Kood: IRT70LT

IMS NETWORK CSCF NODE TESTING

IMS VÕRGU SEANSIJUHTIMISE SÕLME (CSCF) TESTIMINE

Jelizaveta Kornejeva

Töö on tehtud telekommunikatsiooni õppetooli juures
Juhendaja Avo Ots
Kaitsmine toimub raadio- ja sidetehnika instituudi kaitsmiskomisjonis
Autor taotleb tehnikateaduse magistri kraadi

Esitatud: 30.03.2009
Kaitsmine:
Abstract

Keywords: IMS network, CSCF, SIP, SIP signaling in IMS, CSCF testing.

IP Multimedia Subsystem (IMS) is a generic architecture for offering multimedia and voice over IP services defined by 3GPP. IMS is access independent as it supports multiple access types. The implementation of the IMS promises good revenues to the operators. IMS is a key enabler for fixed-mobile convergence.

This Master thesis outlines the benefits of IMS, its architecture and protocols emphasizing the role of Session Initiation Protocol (SIP). It also outlines the SIP signaling and routing mechanisms in the IMS.

The thesis tells about the necessity of IMS testing, describes the possible way of testing the IMS main network element-Call Session Control Function (CSCF) by the means of the special software-Spirent Protocol Tester. The two test cases are given as examples to demonstrate the process of finding an error in the equipment by the person performing as a tester.

This Master thesis is written in English and consists of 91 pages, including 44 figures, 1 table and an attachment.
Referaat

Võtmesõnad: IMS vörk, CSCF, SIP, SIP signaliseerimine IMS-vörgus, CSCF testimine.

IP Multimedia Subsystem (IMS) on 3GPP poolt standardiseeritud võrguarhitektuuri raamistik mis saab pakkuda erinevaid multimeedia ja VoIP teenuseid sõltumatult võrguühenduse tüübist. IMS platvorm lubab sideoperaatoritele häid võimalusi innovatiivsete teenuste loomiseks ja selle abil lisatulu teenimiseks. IMS on peamine FMC (Fixed Mobile Convergence) realiseerimise võimaldaja.

Magistritöö annab ülevaate IMS'i eelistest, arhitektuurist, selgitab erinevate komponentide funktsioone, peatub IMS võrgus kasutatavatel protokollidel, fokusseerides SIP (Session Initiation Protocol) protokollil. Töö kirjeldab SIP signaliseerimise ja suunamise mehhanisme.

Magistritöö rõhutab IMS, eriti põhielemendi CSCF (Call-Session Control Function) testimise vajalikkust. Töö keskendub ühele võimalikule testimise viisile, kasutades spetsiаalset programmi-Spirent Protocol Tester. Kaks testi on toodud demonstreerivaks näiteks, kuidas inimene-tester saab avastada seadmete vigu.

Magistritöö on koostatud inglise keeles, koosneb 91 lehest, sisaldab 44 joonist,1 tabelit ja 1 lisa.
Preface

This master thesis embodies the result of my studies at Tallinn University of Technology and my work experience in Softronic Baltic AS.

I am grateful to my supervisor Avo Ots, my colleague Margus Rohtla for their advices and encouragement. I would also like to thank Softronic Baltic AS SIP developers’ team for our pleasant cooperation.
# Table of Contents

1. **Introduction** .................................................................................................................. 14
   1.1. The Contents of the Thesis ......................................................................................... 15
   1.2. The Structure of the Thesis ....................................................................................... 17

2. **Overview of the IMS** ................................................................................................. 18
   2.1. Convergence of Networking Paradigms .................................................................... 18
   2.2. IMS Benefits ............................................................................................................. 20
   2.3. Architectural Requirements ....................................................................................... 23
   2.4. Overview of IMS Architecture .................................................................................. 24
      2.4.1. Call/Session Control Function – CSCF .............................................................. 25
      2.4.2. Databases ........................................................................................................... 29
      2.4.3. Other IMS entities ............................................................................................. 30
      2.4.4. PSTN Interworking Functions ............................................................................ 32
      2.4.5. Support Functions .............................................................................................. 33
      2.4.6. GPRS Entities .................................................................................................. 34
      2.4.7. IPv4/IPv6 Interworking Functions .................................................................... 35
   2.5. Overview of Key Protocols Used in IMS Network .................................................... 36
      2.5.1. Session Initiation Protocol (SIP) ....................................................................... 36
      2.5.2. Diameter ............................................................................................................ 36
      2.5.3. H.248(Megaco or Gateway Control Protocol) .................................................. 37
      2.5.4. Session Description Protocol (SDP) .................................................................. 37
      2.5.5. Real-Time Transport Protocol (RTP) ................................................................. 37
      2.5.6. RTP Control Protocol (RTCP) ......................................................................... 37
      2.5.7. IPv6 .................................................................................................................. 37

3. **SIP in the IMS** .............................................................................................................. 38
   3.1. SIP Place in the Internet Multimedia Protocol Stack ................................................. 38
   3.2. Session Control ......................................................................................................... 39
3.2.1. SIP and User Mobility ................................................................. 39
3.2.2. SIP Logical Entities ................................................................. 39
3.2.3. Session Establishment ............................................................. 42
3.2.4. Requests .................................................................................. 44
3.2.5. Responses ................................................................................. 45
3.2.6. Header Fields ........................................................................... 47
3.2.7. The Message Body ................................................................. 49
3.3. Routing ....................................................................................... 49
  3.3.1. Processing INVITE ................................................................. 51
  3.3.2. Routing of Subsequent Requests in a Dialog ......................... 54
  3.3.3. Routing from the S-CSCF to the AS ........................................ 54
  3.3.4. Routing from AS back to the S-CSCF ..................................... 55
4. IMS Core Network Testing................................................................. 56
  4.1. The Purpose of the CSCF Testing ............................................... 56
  4.2. Possible Testing Environment .................................................... 57
  4.3. Spirent Protocol Tester .............................................................. 59
  4.4. Example .................................................................................... 61
    4.4.1. SPT Two Proxy Simulation ............................................... 61
  4.5. TTCN-3 ................................................................................... 72
5. Conclusion .................................................................................... 75
6. References ..................................................................................... 76
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ericsson vision of a new multimedia experience across diverse networks [14]</td>
</tr>
<tr>
<td>2</td>
<td>IMS in converged networks [12]</td>
</tr>
<tr>
<td>3</td>
<td>Vertical service versus horizontal service implementations [4]</td>
</tr>
<tr>
<td>4</td>
<td>The difference in service interconnect between a non-IMS network and IMS-enabled operators [4]</td>
</tr>
<tr>
<td>5</td>
<td>IMS standardization [4]</td>
</tr>
<tr>
<td>6</td>
<td>IMS and layered architecture [16]</td>
</tr>
<tr>
<td>7</td>
<td>3GPP IMS architecture overview [13]</td>
</tr>
<tr>
<td>8</td>
<td>Typical IMS core overview [4]</td>
</tr>
<tr>
<td>9</td>
<td>S-CSCF routing and basic IMS session setup [12]</td>
</tr>
<tr>
<td>10</td>
<td>Structure of HSS [12]</td>
</tr>
<tr>
<td>11</td>
<td>Three types of Application Servers [12]</td>
</tr>
<tr>
<td>12</td>
<td>The PSTN/CS gateway interfacing a CS network [13]</td>
</tr>
<tr>
<td>13</td>
<td>The example of GPRS entities and the IMS [13]</td>
</tr>
<tr>
<td>14</td>
<td>The IMS-ALG and the TrGW [13]</td>
</tr>
<tr>
<td>15</td>
<td>The Internet Multimedia Protocol stack [23]</td>
</tr>
<tr>
<td>16</td>
<td>Application Server acting like a SIP proxy</td>
</tr>
<tr>
<td>17</td>
<td>SIP Trapezoid [23]</td>
</tr>
<tr>
<td>18</td>
<td>Application Server acting like a B2B-UA</td>
</tr>
<tr>
<td>19</td>
<td>A simple SIP session establishment example [27]</td>
</tr>
<tr>
<td>20</td>
<td>An INVITE message example [27]</td>
</tr>
<tr>
<td>21</td>
<td>A SIP message format [12]</td>
</tr>
<tr>
<td>22</td>
<td>180 Ringing response on INVITE [27]</td>
</tr>
<tr>
<td>23</td>
<td>200 OK response on INVITE [27]</td>
</tr>
<tr>
<td>24</td>
<td>The example scenario [12]</td>
</tr>
<tr>
<td>25</td>
<td>IMS session establishment call flow [12]</td>
</tr>
</tbody>
</table>
Figure 26. Routing an initial INVITE request and its responses [12] ..............................................51
Figure 27. Routing of subsequent requests and their responses [12] ..............................................54
Figure 28. Example of possible testing environment [32] .................................................................58
Figure 29. Example of the CSCF configuration [32] .................................................................58
Figure 30. Spirent Protocol Tester [10] .........................................................................................59
Figure 31. Spirent client architecture [10] .......................................................................................60
Figure 32. Two proxy applications simulation [32] ............................................................................61
Figure 33. Test case signaling with two stateful proxies [32] ............................................................62
Figure 34. State machine simulating the stateful Proxy Application Server with call forwarding [32] ..............................................................................................................................63
Figure 35. The test case with two stateful Proxy Application Servers ready to be executed [32] 64
Figure 36. Two stateful proxies call flow in Spirent [32] .................................................................65
Figure 37. The INVITE request [32] ...............................................................................................66
Figure 38. Test case signaling with two stateless proxies [32] ..........................................................67
Figure 39. State machine simulating the stateless Proxy Application Server with call forwarding [32] ..............................................................................................................................68
Figure 40. The test case with two stateless Proxy Application Servers ready to be executed [32] ..............................................................................................................................................69
Figure 41. Two stateless proxies call flow in Spirent [32] ...............................................................70
Figure 42. The failed state machine in Spirent. The test case fails because the UE receives the ACK message from the wrong port [32] .................................................................................................71
Figure 43. Test suite execution [32] ...............................................................................................72
Figure 44. General structure of a TTCN-3 Test System [30] ..........................................................74
List of Tables

Table 1. SIP response classes [23]........................................................................................................47
## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G/2G/3G</td>
<td>First/second/Third-Generation Cell-Phone Technology</td>
</tr>
<tr>
<td>3GPP</td>
<td>Third Generation Partnership Project</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>AMR</td>
<td>Adaptive Multi-Rate</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AS</td>
<td>Application Server</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>AUC</td>
<td>Authentication Center</td>
</tr>
<tr>
<td>AUTOSAR</td>
<td>Automotive Open System Architecture</td>
</tr>
<tr>
<td>B2BUA</td>
<td>Back-To-Back User Agent</td>
</tr>
<tr>
<td>BGCF</td>
<td>Breakout Gateway Control Function</td>
</tr>
<tr>
<td>BICC</td>
<td>Bearer Independent Call Control</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CAMEL</td>
<td>Customized Applications for Mobile Network Enhanced Logic</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CS</td>
<td>Circuit Switched</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Session Control Function</td>
</tr>
<tr>
<td>CSE</td>
<td>CAMEL Service Environment</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data for GSM Evolution</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>ISUP</td>
<td>Integrated Services User Part</td>
</tr>
<tr>
<td>GGSN</td>
<td>Gateway GPRS Serving/Support Node</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IBCF</td>
<td>Interconnect Border Control Function</td>
</tr>
<tr>
<td>I-CSCF</td>
<td>Interrogating Call Session Control Function</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IMS-ALG</td>
<td>IP Multimedia Subsystem Application-Level Gateway</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IMS-MGW</td>
<td>IP Multimedia Subsystem Media Gateway</td>
</tr>
<tr>
<td>IM-SSF</td>
<td>CAMEL IP Multimedia Service Switching Function</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPSec SAs</td>
<td>IPSec security associations</td>
</tr>
<tr>
<td>ISC</td>
<td>IP Service Control interface</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>ITU-T</td>
<td>International Telecommunication Union-Telecommunication</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MGCF</td>
<td>Media Gateway Control Function</td>
</tr>
<tr>
<td>MGW</td>
<td>Media Gateway</td>
</tr>
<tr>
<td>MOST</td>
<td>Media Oriented Systems Transport</td>
</tr>
<tr>
<td>MRFC</td>
<td>Multimedia Resource Function Controller</td>
</tr>
<tr>
<td>MRFP</td>
<td>Multimedia Resource Function Processor</td>
</tr>
<tr>
<td>MSC/MSC</td>
<td></td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number</td>
</tr>
<tr>
<td>MTP</td>
<td>Media Transfer Protocol</td>
</tr>
<tr>
<td>OSA</td>
<td>Open Service Access</td>
</tr>
<tr>
<td>PCRF</td>
<td>Policy and Charging Rules Function</td>
</tr>
</tbody>
</table>

Tallinn 2009
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-CSCF</td>
<td>Proxy Call Session Control Function</td>
</tr>
<tr>
<td>PDF</td>
<td>Policy Decision Function</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone System/Service</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PS</td>
<td>Packet Switched</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>PTT</td>
<td>Push-to-Talk</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality Of Service</td>
</tr>
<tr>
<td>RTCP</td>
<td>Real-time Transport Control Protocol</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Transport Protocol</td>
</tr>
<tr>
<td>SCS</td>
<td>OSA Service Capability Server</td>
</tr>
<tr>
<td>S-CSCF</td>
<td>Serving Call Session Control Function</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Description Protocol</td>
</tr>
<tr>
<td>SEG</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SGW</td>
<td>Signaling Gateway</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLF</td>
<td>Subscription Locator Function</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>THIG</td>
<td>Topology Hiding Inter-network Gateway</td>
</tr>
<tr>
<td>TETRA</td>
<td>TErrestrial Trunked RAdio</td>
</tr>
<tr>
<td>TISPAN</td>
<td>Telecommunications and Internet Converged Services and Protocols for Advanced Network</td>
</tr>
<tr>
<td>TrGW</td>
<td>Translation Gateway</td>
</tr>
<tr>
<td>TTCN-3</td>
<td>Testing and Test Control Notation version 3</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
</tr>
<tr>
<td>V.90</td>
<td>Modem connection protocol; allowing for speeds up to 56Kbps using standard phone line</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>WCDMA</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
1. Introduction

Networks of the future will be more about users rather than a particular infrastructure, allowing subscribers to link with any available service while using any device or access method. Now fixed/wireless convergence is a growing trend, and service providers operating intelligent IP networks are looking for a way to deliver seamless access to their applications and content, regardless of the subscriber’s location.

IP Multimedia Subsystem (IMS) has received a lot of attention in the industry recently. IMS refers to a network architecture consisting of an IP-based core network connected to a multiple access networks to provide a converged service to wireless, wire line and cable subscribers. IMS standard was defined for 3G UMTS (Universal Mobile Telephony System) wireless networks (next generation of GSM mobile systems). But, the flexibility of the IMS network architecture has made it attractive to connect other access networks like GSM and CDMA mobile networks, cable TV networks, WiFi networks, WiMAX networks, enterprise and residential networks, etc. [1]. Direct IMS terminals (such as mobile phones, personal digital assistants (PDAs), computers, etc.) can register directly on an IMS network, even if they are roaming in another network or country. The only requirement is that they can use IPv4/IPv6 and run Session Initiation Protocol (SIP) user agents [2]. SIP is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions. SIP was accepted by 3GPP as a signaling protocol and permanent element of the IMS architecture for IP-based multimedia services in mobile systems [3].

IMS offers a standardized way to deliver convenient IP-based services to wire line, wireless or cable community—enabled by one common core and control. It is the cornerstone of the evolutions of current networks to a single, all-IP based network where all types of services (messaging, telephony, etc.) and multimedia (voice, video, pictured, text, etc.) can be integrated into a single user experience [4]. IMS enables the service and network convergence and device convergence. For example, a user may want to use a single device that can perform multiple functions over multiple networks like a PDA-based mobile phone that can access mobile as well as wireless broadband networks (like WiFi or WiMAX networks). Likewise, a user may use multiple devices accessing a common service over multiple devices with the application seamlessly handing over between the different access networks and different devices—for example, a user may start an application (a call, conference, video call, etc.) on his computer, hand the session off to his mobile phone as he drives to work and then hand off the session to his work computer when he arrives. This convergence will allow operators to offer converged services to their subscribers providing access anywhere whether they are home, at the office, in the car, traveling, etc.

An important aspect of this converged solution is the ability to flexibly launch new services in a fast and scalable manner. Having a mechanism to cost-effectively roll-out new service offerings across multiple access networks is a key requirement.

The IMS core network is defined as a layered network consisting of a media transport layer (voice, video, data, etc.), call control layer (SIP control, transport control, etc.) and applications layer (to provide added
functionality to the IMS core network). A key benefit of the IMS core network is the use of this common application layer while reusing common transport and call control layers to provide multiple services to users across multiple access networks. This will allow operators to provide their subscribers with access to common applications across divergent networks. More important is that new applications that are developed can be added to this common application layer cost-effectively reusing the existing network elements and existing access networks, effectively lowering the initial costs to deploy new features [1].

Service providers expect and require that their significant investments in IMS will quickly reap new business opportunities and lower operational costs without placing existing services at risk.

But before the new multimedia services become a strong revenue contributor, service providers and network equipment developers must have strong confidence in the reliability, availability and security of the underlying IMS infrastructure [5]. Testing of the IMS core network before the market release plays a big role in development process.

The IMS core network predominantly consists of the HSS -Home Subscriber Server [6] and the CSCF - Call Session Control Function [6]. The HSS plays the role of a location server in IMS, in addition to acting as an AAA server. The HSS also serves as a single point of provisioning for IMS subscribers and their services. The Call session control function also plays an important role in IMS. The CSCF node facilitates SIP session setup and teardown. The Call Control Function is divided into three logical entities [7]:

- Proxy CSCF (P-CSCF)
- Interrogating CSCF (I-CSCF)
- Serving CSCF (S-CSCF)

Each of them has its own function in processing SIP requests and responses. Testing the CSCF functionality is of a primary concern, because it is the most important part of IMS [8].

Function test in simulated environment is a necessity in testing process since the costs of the testing in a real environment are very high. At this level of testing many faults and errors can be discovered before the software testing goes to system on real nodes. This shortens the period of system test which reduces the final cost [9].

Different companies provide their solutions of software for network equipment testing and the developers can choose the most convenient and efficient way of testing according to their needs and purposes.

1.1. The Contents of the Thesis

This thesis has two main goals. The first one is to give an introduction to the IMS and describe what benefits it brings to the operators and customers. An overview of IMS architecture and the protocols that are used in the IMS, especially SIP protocol, is required to fulfill the second goal of the thesis, which is to
present one of the alternatives for testing the IMS core network elements’ behavior in different call flow scenarios.

The thesis gives an example of the IMS CSCF testing using Spirent Protocol Tester as a testing environment. Spirent Protocol Tester (SPT) developed by Spirent Communications provides comprehensive support for all major VoIP and IMS protocols and media formats, including conformance, protocol, functional and interoperability testing, while simultaneously providing high-performance signaling and media load generation. Spirent Protocol Tester has a state machine – based architecture and can test and emulate virtually any VoIP and IMS network element, function or service. The Spirent Protocol Tester is the ideal tool for addressing IMS interoperability testing challenges by allowing users to add, remove and customize protocol message headers and payloads. With the Spirent Protocol Tester engineers can define and create any protocol call flow using any mix of protocols. The SPT provides this needed flexibility via a modern graphical user interface necessary for rapid test case creation and easy troubleshooting [10].

The main target of such testing is making sure that CSCF is capable to handle different sometimes complex SIP flow scenarios according to the standards, to test the interoperability among different core network components and to check the accuracy of routing procedure within the network. Each CSCF that is traversed during the call session establishment procedure participates in the routing mechanism. In IMS core network testing the routing part is the most complex issue. This work also gives an overview of the routing mechanism within the IMS core network.

If the test case fails, the person performing as a tester has to find the reason for that. Before test case implementation the testers work with standards and prepare the theoretical part which covers the test case call flow that includes the signaling of the SIP messages, the contents of the SIP messages and the routing of the SIP messages. After running the test case on the device under test, which in this case is the IMS core network, the tester can compare the theoretical version of the call flow with a “real” implementation. The comparison of the real CSCF equipment’s behavior with the behavior defined in the standard can reveal CSCF equipment faults. After revealing the faults the CSCF developers are informed about it, and they tend to improve the next release of the equipment. This work demonstrates the process of finding the bug in the equipment.

The future trend of SIP testing is also mentioned in the thesis. The Testing and Test Control Notation TTCN-3 is a modern, powerful test specification and test implementation language that supports all kinds of black-box testing. TTCN-3 was developed at the European Telecommunications Standards Institute (ETSI) and is the only standardized test specification language (also adopted at ITU-T). Recent development show, that the industry and research start focusing more and more on testing with TTCN-3 [11]. It is declared to become a standard for next-generation testing.
1.2. The Structure of the Thesis

The thesis consists of three parts. The first part gives an overview of the IP Multimedia Subsystem. It explains the idea of convergence of networking paradigms, gives the reasons why IMS is necessary and what benefits it brings, describes the architecture of IMS and the functionalities of the IMS nodes, gives a short overview of the protocols used in the IMS.

The main scope of the second part is the role of the session initiation protocol (SIP) in the IMS. This part explains the concepts of the SIP and its functions within the IMS network, lists SIP logical entities, illustrates the session establishment process using SIP, describes the SIP request’s and response’s structure and gives an idea how SIP routing works. This part of thesis contains figures that illustrate the SIP requests/ responses routing process in the IMS network.

And, finally, the third part focuses on the testing of the call session control functions- the main IMS functional nodes. This part explains why testing of the IMS core is essential, gives an overview of the possible testing environment which is practically implemented, tells about Spirent Protocol Tester and its use while testing the IMS core network, gives examples of two test case implementations and analysis of the received results. This part also tells about the future trend in the IMS testing – which is the use of the programming language TTCN-3 -Testing and Test Control Notation Version 3 [6].

The attachment contains the signaling flow of the two test cases which results are analyzed in this thesis. The theoretical part made in excel document consists of the SIP request/responses flow between the IMS core nodes. Comments contain the important headers taken from the Spirent Protocol Tester to compare the routing within the real IMS core network and theoretical part that respond to the standard.
2. Overview of the IMS

2.1. Convergence of Networking Paradigms

Fixed, mobile and Internet networks have gone through a major transition in the past 20 years.

In the fixed side, traditional Public Switched Telephone Network (PSTN) and Integrated Services Digital Network (ISDN) traditional voice and video communication have been dominating.

In the mobile world, first generation (1G) systems were introduced in the mid-1980. The main emphasis was on speech and speech-related services. Second-generation (2G) systems in the 1990 brought some data services. The circuit-switched domain is an evolution of the technology used in 2G networks. The third generation networks (3G) that have a packet-switched domain are now enabling faster data rates and different multimedia services [12]. These services include, of course, telephone calls, messaging services ranging from simple text messages (SMS, Short messaging Service) to fancy multimedia messages that include video, audio, and text (MMS, Multimedia Messaging Service). Users can surf the web, read emails, download videos, and do virtually everything they can do over the Internet. Technically, any user can install a VoIP client in his 3G terminal and establish VoIP calls over the packet-switched domain.

The Internet has experienced dramatic growth over the last few years- from a small network linking a few research sites to a massive worldwide network. The main reason for its rapid growth has been the ability to provide a number of extremely useful services that millions of users like. The best known examples are the World Wide Web, email, instant messaging, presence, VoIP, videoconferencing, and shared whiteboards. The Internet is able to provide various new services because it uses open protocols that are available on the web for any service developer [13].

What challenges are we facing now? The Figure 1 demonstrates Ericsson vision of a new “converged user experience that leverages the best from the telecoms, media and internet worlds”.

Figure 1. Ericsson vision of a new multimedia experience across diverse networks [14]

At the moment we are experiencing the fast convergence of fixed and mobile worlds and the Internet. The popularity of mobile devices is increasing and soon there will be more that 2 billion mobile devices in use. These mobile devices have large, high-precision displays; they have build-in cameras and a lot of
resources for applications. They are always-on always-connected application devices. This redefines applications. They are no longer isolated entities exchanging information only with the user interface. The next generation applications are peer-to-peer entities, which facilitate sharing: shared browsing, shared whiteboard, shared game experience, shared two-way radio session, for example Push to talk Over Cellular. Dialing a number and talking isn’t already enough. The ability to establish a peer-to-peer connection between the new Internet Protocol (IP) enabled devices is the key requirement. This new paradigm of communications reaches far beyond the capabilities of the Plain Old Telephone Services (POTS) [13].

In order to communicate, IP-based applications must have a mechanism to reach the correspondent. The telephone network entirely fulfils this task. By dialing the peer, the network can establish connection between any two terminals over the IP network. Nowadays, this critical IP connectivity capability is offered only in isolated and single-service provider environments in the Internet; closed systems compete on user base, where user lock-in is a key target and interworking between service providers is an unwelcome feature. Therefore, there is a great necessity for a global system that allows applications in IP-enabled devices to establish peer-to-peer and peer-to-content connections easily and securely.

![Figure 2. IMS in converged networks [12]](image)

Many companies that belong to telecom operators, internet companies and the media world are limiting their business opportunities by being unable or unwilling to work with the others. However, there is the hope on the horizon: IMS (IP Multimedia Subsystem) can provide a framework to bridge the perspective business models [15]. The definition for the IMS is:

**IMS is a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end-users using common Internet-based protocols [12].**
The integration of voice and data services increases productivity, while the development of innovative applications integrating voice, data and multimedia will create demands for new services [12]. The combination of mobility and the IP network will be a key factor for the service success in the future.

Figure 2 shows a converged communication network for the fixed mobile environment. The IMS introduces multimedia session control in the packet-switched domain and at the same time brings circuit-switched functionality in the packet-switched domain. The IMS is a key technology for such network paradigm that enables a “converged user experience that leverages the best from the telecoms, media and internet worlds” [15].

Usually industries tend to hold a negative perspective on change, but sometimes change cannot be avoided, and companies that accept the changed circumstances are more likely to overcome the challenges those circumstances bring. Now many telecom operators, vendors and such telecom giants like Ericsson, Nokia Siemens, Alcatel-Lucent, Motorola, Nortel, Cisco, NEC, etc dedicate a lot of their attention to the IMS. IMS is still a new technology in deployment and that means that there is a great opportunity for the first movers to establish dominant positions in the IMS-enabled services. At the beginning of the 2008 year Ericsson estimated that there were approximately 40 commercial deployments of IMS around the world, and over 130 contracts for IMS network installations [15].

### 2.2. IMS Benefits

“Why do we need the IMS?” is major strategic questions for any operator these days. There are plenty of possible answers on this question, but perhaps the key one is that IMS delivers innovative multimedia services over fixed and mobile networks using open standards. IMS covers key issues such as convergence, service creation and delivery, service interconnection and open standards. It allows an operator to retain existing business models and evolve towards new ones.

Here are the reasons why do we need IMS:

- **IMS is an enabler for convergence.**

IMS enables convergence and interworks in several dimensions—across fixed and mobile access—in the service layer, control layer and connectivity layer. The IMS architecture provides a number of common functions that are generic in their structure and implementation, and can be reused by virtually all services in the network (for example, group/list management, presence, provisioning, operation and management, directory, charging and deployment (Figure 3). By securing these common functions less parallel development is required, more reliable systems are introduced, developers can focus on the actual application and not the surrounding details. The traditional network—with its service-unique functionality—is very complex and expensive to build.
On the Figure 3 we can see that for the traditional network structure separate implementations of each layer must be built for every service and the structure is replicated across the network.

- **IMS allows fast and efficient service creation and delivery.**

As it was mentioned above, many functions can be reused for service creation. IMS services are hosted by Application Servers and many aspects of service control are defined through standardized means. For example, IMS defines how service request are routed, which protocols are supported, how charging is performed and how service composition is enabled. IMS systems are designed to support multiple Application Servers. This means, that the same infrastructure can be utilized for new services and the implementation effort is focusing on actual service. Operators can benefit a lot from this solution, because they will be able to use services developed from the third parties, combine them, integrate them with other services and provide the user with a completely new service. Operators can take advantage of a powerful multi-vendor service creation industry.

- **With IMS service interconnection can be provided.**

The IMS standard helps to create and secure interconnect agreements of a multitude of services and to enable the industry to agree a few key mechanisms for interconnection (Figure 4). A key concept in IMS is Communication Services: standardizing a few basic communication patterns that can then be provided as application building blocks. Communication Services span the whole operator network, from the network–network interface (NNI) to the user–network interface (UNI). Third-party applications will be connected through APIs built on Communication Services.
As shown in Figure 4, instead of establishing separate interconnect agreements per service, the operators can agree on a small set of basic agreements. In this way, the process of agreeing Service Layer Agreements (SLAs) and settlement rules for each new service is avoided.

- **IMS uses open standards.**

The IMS standard (Figure 5) is an international recognized standard, first specified by the 3GPP/3GPP2 and now being embraced by other standard bodies such as ETSI/TISPAN, CableLabs, JCP, OMA and WiMAX Forum. The IMS standard supports different access types: GSM, WCDMA, CDMA200, cable, wireline broadband access, WLAN/WiFi and WiMAX. It defines “horizontal” architecture, where services and common functions can be reused for multiple applications. This attitude allows eliminating the costly and complex traditional network structure. Standardization makes it work end to end and enables an attractive, convenient user experience.

- **IMS provides QoS “better than best-effort”.**

IMS provides QoS that would suit the different requirements of different conversational, streaming and interactive classes of services. Modern packet-switched domain networks does not guarantee the amount of bandwidth a user gets for a particular connection, or the maximum delay the packets experience. The IMS takes care of synchronizing session establishment with QoS provision so that users have a predictable experience. The IMS network elements at the borders with access networks isolate the IMS core from specific access network QoS aspects, plus, they provide access-specific policy control such as fraud protection, QoS assurance and user address reachibility.

- **IMS enables appropriate charging of multimedia sessions.**

Now 3G operators charge for the amount of data transferred and that may bring large expenses to the user. The operator can not use a different business model to charge the user, because the operator is not
aware of the contents of those bites: they could belong to a VoIP session, to an instant message, to a web page or to an email. If the operator is aware of the actual service that the user is demanding, it can suggest an alternative charging scheme that may be more beneficial to the user. For example, the operator may charge for a multimedia session based on its duration. The IMS provides information about the service being used and the operator decides whether to use a flat rate for the service, apply time-based charging, apply QoS-based, or perform any new type of charging. IMS provides network operators and developers more choice in business models [4].

### 2.3. Architectural Requirements

There is a set of basic requirements which define the way in which the IMS architecture has been created and how it should evolve in the future:

- Support for establishing IP Multimedia Sessions
- Support for a mechanism to negotiate QoS
- Support for interworking with the Internet and circuit-switched networks
- Support for roaming
- Support for strong control imposed by the operator with respect to the services delivered to the end-user
- Support for rapid service creation without requiring standardization
- Access independence of the IMS: The release 6 version of 3GPP TS 22.228 added a new requirement to support access from networks other than GPRS
- Support of a layered design [13] (Figure 6).

![Figure 6. IMS and layered architecture [16]](image)
Figure 6 demonstrates the IMS layered architecture. Services are run on the top of the IMS signaling network (control layer). The layered approach increases the importance of the application layers because all the services are designed independent of the access network and the IMS aim is to bridge the gap between them.

### 2.4. Overview of IMS Architecture

IMS entities can be classified in main categories:

- Session management and routing (CSCFs)
- Databases (HSS, SLF)
- Services (application server, MRFC, MRFP)
- Interworking functions (BGCF, MGCF, IMS-MGW, SGW, etc)
- Support functions (PDF, SEG, THIG, etc)
- Charging

IMS specifications do not standardize nodes, but functions. IMS architecture is a collection of functions linked by standardized interfaces. Implementers are free to combine two functions into one single node or instead, to split a single function into two or more nodes. Mostly, vendors follow the IMS architecture closely and implement each function into a single node[13].

The Figure 7 gives an overview of the IMS architecture.

![3GPP IMS architecture overview](image)

*Figure 7. 3GPP IMS architecture overview [13]*

The Figure 7 also shows most of the signaling interfaces in the IMS.
The IMS core is access independent and same services can be delivered over different types of access technologies. In the IMS specification the “core network” includes two main nodes: the Call Session Control Function (CSCF) and the Home Subscriber Server (HSS) [9].

2.4.1. Call/Session Control Function – CSCF

The Call/Session Control function (CSCF, (Figure 8)) is the heart of the IMS architecture and it is used to process SIP signaling. The main function is to provide session control for terminals and applications using the IMS network including routing of the SIP messages, monitoring of the SIP sessions and communicating with the policy architecture to support media authorization. It is also responsible for interacting with the HSS [9]. There are three types of CSCF, depending on the functionality they provide:

- P-CSCF (Proxy- Call/Session Control Function)
- I-CSCF (Interrogating- Call/Session Control Function)
- S-CSCF (Serving-Call/Session Control Function)

![Figure 8. Typical IMS core overview [4]](image)

Proxy Call Session Control Function (P-CSCF)

P-CSCF is the first contact point for users within the IMS, all the traffic from the UE at first is sent to the P-CSCF. Similarly, all terminating SIP signaling from the network is sent from the P-CSCF to the UE. P-CSCF realizes four tasks [12]:

- SIP compression
SIP protocol is a text-based signaling protocol, it contains a large number of headers and header parameters, which means that SIP messages can be large. 3GPP has mandated the support of SIP compression and decompression between the UE and the P-CSCF. If the UE has indicated that it wants to receive compressed messages, the P-CSCF has to compress them.

- **IPSec security association**

P-CSCF is responsible for establishing a number of IPSec security associations toward the IMS terminal. These IPSec security associations (SAs) are applying integrity protection (i.e., the ability to detect whether the contents of the message has changed since its creation) and confidential protection of SIP signaling. This is achieved during SIP registration as the UE and P-CSCF negotiate IPSec SAs. Once P-CSCF authenticates the user, the P-CSCF asserts the identity of the user to the rest of the nodes in the network, which trust the P-CSCF and use this identity for a number of purposes, such as providing personalized services and generating account records.

- **Interaction with Policy Decision Function(PDF)**

The P-CSCF may include PDF, which can be integrated with the P-CSCF or be implemented as a stand-alone device. The PDF authorizes media plane recourses and manages QoS over the media plane. Based on the received information the PDF is able to derive authorized IP QoS information that will be passed to the GGSN when the GGSN needs to perform Service-Based Local Policy. Additionally, via the PDF the IMS is able to deliver IMS charging correlation information to the GPRS network and to receive GPRS charging correlation information from the GPRS network. This makes possible to merge charging data records coming from the IMS and GPRS networks in the billing system.

- **Emergency session detection**

IMS emergency sessions are still not fully specified. It is important that P-CSCF of the IMS network detects emergency session attempts and guides a UMTS UE to use the CS network for emergency calls. P-CSCF should be able to select an emergency CSCF to handle an emergency call. This is needed because in the IMS roaming cases, the assigned S-CSCF is in the home network and the home S-CSCF is unable to route the request to the correct emergency centre.

An IMS network can include several P-CSCFs for the sake of scalability and redundancy. Each of them serves a number of IMS terminals, depending on the capacity of the node.

The P-CSCF can be located in the home network or in the visited network. When the underlying network is based on GPRS, the P-CSCF is always located near the GGSN (Gateway GPRS Support Node). It is expected that the first IMS networks will be configured with GGSN and P-CSCF [13].

Tallinn 2009
Interrogating Call/Session Control Function (I-CSCF)

I-CSCF is a contact point within an operator’s network for all connections destined to a subscriber of that network operator. When a SIP entity needs to send a SIP message to particular domain, it performs a DNS lookup to obtain the address of the SIP server of that domain. A domain’s DNS records point to the domain’s I-CSCF. Therefore, the I-CSCF handles the domain’s incoming traffic. There are four tasks assigned to the I-CSCF [12]:

- To obtain the name of the next hop (it can be S-CSCF or application server) from the Home Subscriber Server (HSS).

The interface between I-CSCF and the HSS or SLF is based on Diameter protocol.

- To assign S-CSCF based on received capabilities from the HSS.

The assignment of the S-CSCF takes place when a user is registered in the network or a user received a SIP request while being unregistered in the network but having services related to an unregistered state (e.g., voice mail).

- To route incoming requests further to an assigned S-CSCF or the application server.

- To provide Topology Hiding Inter-network gateway (THIG) functionality which means that optionally I-CSCF may encrypt the part of the SIP messages that contain sensitive information about the domain, for example, the number of servers in the domain, their DNS names or their capacity.

An IMS network can include several I-CSCFs for the sake of scalability and redundancy.

I-CSCF is usually located in the home network, but in some cases (like I-CSCF (THIG)) it can be located in a visited network [13].

Serving Call/Session Control Function (S-CSCF)

S-CSCF is the central node; it can be called “an IMS brain”. S-CSCF is a SIP server which is responsible for handling registration processes, making routing decisions, maintaining session states and storing the service profiles.

When a user sends a registration request it will be routed to the S-CSCF, and in its turn S-CSCF downloads authentication data and a service profile from the HSS using a Diameter. Based on the authentication data it generates a challenge to the UE. After receiving the response and verifying it the S-CSCF accepts the registration and starts supervising the registration status. After registration the user can initiate receive IMS services.
A service profile is a collection of user-specific information that is stored in the HSS; it is a set of triggers that may cause a SIP message to be routed through one or more applications. The S-CSCF download the service profile associated with a particular public user identity (e.g., joe.doe@ims.example.com) when this public user identity is registered in the IMS. The information from the service profile can be used for S-CSCF to decide when and, which application server(s) is contacted when a user sends a SIP request or receives a request from somebody. The service profile may contain instructions about what kind of media policy the S-CSCF needs to apply.

The S-CSCF is responsible for the routing decisions as it receives all UE-originated and UE-terminated sessions and transactions. When it receives a UE-originating request via the P-CSCF it needs to decide if application servers are contacted or not. After possible application server(s) interaction the S-CSCF either continues a session in IMS or breaks to other domains. Moreover, if the UE uses a Mobile Station ISDN (MSISDN) number to address a called party then the S-CSCF converts the MSISDN number (i.e., a tel URI) to SIP Universal Resource Identifier (URI) format (typically based on DNS E. 164 Number Translation, RFC 2916[143]) before sending the request further. Similarly, the S-CSCF receives all requests which are terminated at the UE. Although, the S-CSCF knows the IP address of the UE from the registration, it routes all requests via the P-CSCF, as the P-CSCF takes care of the SIP compression and security functions.

In addition, the S-CSCF is able to send accounting-related information to the Online Charging System for online charging purposes (i.e., supporting pre-paid subscribers) [12].

An IMS network usually includes several S-CSCFs for the sake of scalability and redundancy. Each S-CSCF serves a number of terminals, depending on the capacity of the node.

The S-CSCF is always located in the home network [13].

![Figure 9. S-CSCF routing and basic IMS session setup [12]](image-url)
Figure 9 illustrates the S-CSCF’s role in routing decisions.

### 2.4.2. Databases

There are two types databases defined in IMS: Home Subscriber Server (HSS) and the Subscription Locator Function (SLF) [12].

**Home Subscriber Server (HSS)**

HSS is the main data storage for all subscribers and service-related data of the IMS. It is very similar to the HLR (Home Location Register) in GSM. The data in the HSS includes user identities, registration information, access parameters and service-triggering information. [3GPP TS 23.002].

User identities consist of two types: private (is assigned by the home network, used for registration and authorization) and public (that users can use for requesting communication with the end-user) user identities.

IMS access parameters are used to set up sessions and include parameters like user authentication, roaming authorization and allocated S-CSCF names.

Service-triggering information enables SIP service execution.

The HSS also gives user-specific requirements for S-CSCF capabilities.

HSS also contains the subset of Home Location Register and Authentication Center (HLR/AUC) functionality required by the packet-switched (PS) domain and the circuit-switched (CS) domain (Figure 10). HLR functionality is required to provide support to PS domain entities, for example SGSN and GGSN for enabling the user’s access to PS domain services. HLR provides support for CS domain entities, like MSC/ MSC services for enabling the user’s access to CS domain services and support roaming to GSM/ UMTS CS domain networks.

The AUC stores a secret key for each mobile subscriber. Data is used for mutual authentication of the IMSI and the network.

![Figure 10. Structure of HSS [12]](image)

There may be more that one HSS in a home network, depending on the number of subscribers, the capacity of the HSS and the organization of the network [12].
Subscription Locator Function (SLF)

The SLF is a database that maps users to HSS, it uses a resolution mechanism that enables the I-CSCF, S-CSCF and AS to find the address of the HSS that holds the subscriber information for a specific user identity when there are several HSSs deployed in one IMS network [12].

Both HSS and SLF implement the Diameter protocol [13].

2.4.3. Other IMS entities

Service functions:

- Multimedia Resource Function Controller (MRFC)
- Multimedia Resource Function Processor (MRFP)
- Application Server (AS) [12]

Media Resource Function (MRF)

MRF provides a source of media in the home network [13].

Multimedia Resource Function Controller (MRFC) and Multimedia Resource Function Processor (MRFP) are used to provide mechanisms for bearer-related services like conferencing, announcements to a user or bearer transcoding in the IMS architecture. The MRFC handles SIP communication from and to the S-CSCF and controls MRFP. The MRFP provides user-plane resources that are requested and instructed by MRFC. MRFP performs the functions of:

- Mixing of incoming media streams
- Media stream source
- Media stream processing [12]

The MRF is always located in the home network.

Currently, MRFC and MRFP are not widely used [13].

Application Servers (ASs)

ASs are not entirely IMS entities. Due to the layered IMS design they are rather functions on top of IMS, which provide value-added multimedia services in the IMS, for example presence, Push to talk Over Cellular, etc.

The main functions of the application servers are:

- The ability to process and impact an incoming SIP session received from the IMS.
- The ability to originate SIP requests.
- The ability to send accounting information to the charging functions.

ASs services are not only SIP-based services, an operator can offer an access to services based on the Customized Application for Mobile network Enhances Logic (CAMEL) Service Environment (CSE) and the Open Architecture (OSA) for its IMS subscribers. Application Server is the term usually used for capturing the behavior of the SIP AS, OSA Service Capability Server (SCS) and CAMEL IP Multimedia Service Switching Function (IM-SSF) [12] (Figure 6).

**SIP AS**

A SIP AS is a SIP-based server that realizes a wide range of value-added multimedia services such as presence, PTT, conferencing servers.

**OSA Service Capability Server (OSA-SCS)**

With the help of OSA an operator can realize such service capabilities like call control, user interaction, user status, data session control, terminal capabilities, account management, charging and policy management for developing services. It can be used as a standardized mechanism for providing third-party ASs in a secure manner to the IMS, because it contains initial access, authentication, authorization, registration and discovery features in multiple entities. OSA SCS is used to terminate SIP signaling from the S-CSCF. The OSA SCS uses an OSA Application Programming Interface (API) to communicate with an actual OSA application server.

**IP Multimedia Service Switching Function (IM-SSF)**

With the help of IM-SSF in the IMS the legacy services that are developed in the CSE can be supported. It hosts CAMEL network features (trigger detecting points, CAMEL Service Switching Finite State Machine, etc.) and interworks with the CAMEL Application Part (CAP) interface [12].

![Figure 11. Three types of Application Servers [12]](image)

Figure 11 shows three types of ASs and their connections.
There might be one or more ASs per subscriber. One or more ASs can be involved in a single session. An example can be the following: An operator has one AS to control terminating traffic to a user based on his preferences (such as redirection of incoming calls to an answer machine between 1 p.m. and 6 p.m.) and another AS is used for adapting the content of instant messages according to the capabilities of the UE(such as screen size, number of colors, etc.) [12].

ASs can be located in the home network or in the external third-party network to which the home operator maintains a service agreement [13].

2.4.4. PSTN Interworking Functions

The IMS provides interworking with circuit switched telephony networks through a set of nodes (Figure 11).

**Breakout Gateway Control Function (BGCF)**

The BGCF is a SIP server that includes routing functionality based on telephone numbers. It is used when the session initiated by an IMS terminal is addressed to a user in a circuit-switch network, such as PSTN or the PLMN. BGCF decides which MGCF handles a particular session that will terminate in the circuit switched network. If the BGCF decides that an MGCF in a different domain should handle the session, it can relay the SIP message it received to a BGCF in that domain [12][13].

**Media Gateway Control Function (MGCF)**

The MGCF is a central node of the PSTN/CS gateway. It performs the protocol translation between SIP and the signaling protocol used in the circuit switched network (ISUP or BICC). The MGCF also controls a Media Gateway (MGW). The protocol used between the MGCF and the MGW is H248 (ITU Recommendation H.248 [189]) [12][13].

**Media Gateway (MGW)**

The MGW interfaces the media plane of the PSTN or CS network. It realizes the translation between the RTP-based media used in the IMS and the media format used in the circuit switched network. The common scenario is when the IMS terminal is using the AMR (3GPP TS 26.071[7]) codec and the PSTN terminal is using the G.711 codec (ITU-T Recommendation G.711[177]) [12][13]

**Signaling Gateway (SGW)**

The MGCF interworks with the circuit switched network through a signaling gateway- SGW-Signaling Gateway.
The SGW interfaces the signaling plane of the CS network. It performs lower-layer protocol conversion. For example, SGW is responsible for replacing the lower MTP (ITU-T Recommendations Q.701 [179]) transport with SCTP (Stream Control Transmission Protocol, defined in RFC 2960[308]) over IP.

SGW transforms ISUP (ITU-T Recommendation Q. 761[185]) or BICC (ITU-T Recommendation Q.1901 [186]) over MTP into ISUP or BICC over SCTP/IP [12][13]

![Diagram of PSTN/CS gateway interfacing a CS network](image)

Figure 12. The PSTN/CS gateway interfacing a CS network [13]

Figure 12 shows a BGCF and a decomposed PSTN gateway that interfaces the PSTN.

### 2.4.5. Support Functions

**Policy Decision Function (PDF)**

PDF (Also known as Service-based Policy Decision Function in TISPAN). This function takes a service level policy request from the application layer (for example P-CSCF) and translates it into IP QoS parameters. For example, a G.711 call would be translated into real-time priority with 80 kbps IP bandwidth requirement. The access network is then asked if it can provide this QoS, and it will depend on the type of access network used [12][13].

**Security Gateway (SEG)**

SEG has the function of protecting control-plane traffic between security domains. The security domain is a network that is managed by a single administrative authority. The SEG is placed at the border of the security domain and it enforces the security policy of a security domain toward other SEGs in the destination security domain. In the IMS all traffic within the IMS is routed via SEGs, especially when the traffic is interdomain, meaning that it originates from a different security domain from the one where it is
received. When, protecting inter-domain IMS traffic, both confidentiality as well as data integrity and authentication are mandated [12][13].

**Topology Hiding Inter-network Gateway (THIG)**

THIG functionality could be used to hide the configuration, capacity and topology of the network from outside an operator’s network. If an operator wants to use hiding functionality then the operator must place a THIG function in the routing path when receiving requests or responses from other IMS networks. Similarly, the THIG must be placed in the routing path when sending requests or responses to other IMS networks. The THIG performs the encryption and decryption of all headers which reveal topology information about the operator’s IMS network [12][13].

**2.4.6. GPRS Entities**

**Serving GPRS Support Node (SGSN)**

SGSN is responsible for performing both control and traffic-handling functions for the packet switched domain.

Control part consists of mobility management that deals with the location and state of the UE and its authentication, and of session management, that deals with connection admission control and any changes in the existing data connections. It also supervises 3G network services and resources.

Traffic handling part is session management that is executed. The SGSN acts as a gateway for user data tunneling, it relays user traffic between the UE and the GGSN. It also assures that connections have the appropriate QoS. Plus, it generates charging information [12][13].

**Gateway GPRS Support Node (GGSN)**

GGSN provides interworking with external packet data networks, where IP-based applications and services reside. For example, the external data network can be the IMS or the Internet. GGSN routes IP packets containing SIP signaling from the UE to the P-CSCF and vice versa. Plus, it takes care of routing IMS media IP packets toward the destination network. The interworking service provided is realized as access points that relate to the different networks the subscriber wants to connect. In most cases the IMS has its own access point. When the UE activates a PDP context toward an access point (IMS), the GGSN allocates a dynamic IP address to the UE. This allocated IP address is used in IMS registration and when the UE initiates a session as a contact address of the UE. Additionally, the GGSN polices and supervises the PDP context usage for IMS media traffic and generates charging information [12][13].
Figure 13 shows the connection between the P-CSCF and the GGSN.

### 2.4.7. IPv4/IPv6 Interworking Functions

IMS support two IP versions, IPv4 and IPv6. This means that there will be IMS sessions between IPv4 and IPv6 clients.

IPv4-IPv6 conversion is performed at the Interconnect Border Control Function (IBCF) (Figure 14). The IMS Application Layer Gateway (IMS-ALG) modifies SIP messages in order to perform IPv4-IPv6 conversion. It also controls the Translation Gateway (TrGW), which performs IPv4-IPv6 conversions at the media level [12][13].

Figure 14. The IMS-ALG and the TrGW [13]
2.5. **Overview of Key Protocols Used in IMS Network**

While designing the IMS 3GPP decided to reuse protocols that had already been developed by IETF and the ITU-T. Doing this, 3GPP took advantage of the experience of the IETF and the ITU-T in designing robust protocols, reducing the time for developing and the cost [13]. The list of the key protocols used in the IMS network:

### 2.5.1. Session Initiation Protocol (SIP)

SIP is the main protocol used in IMS networks. SIP was developed by IETF and selected as a standard for IMS by 3GPP [4]. The latest version of the specification is RFC 3261 from the IETF SIP Working Group. SIP inherits most of its principles from SMTP (Simple mail Transfer Protocol (RFC 2821[201]) and HTTP (Hypertext Transfer Protocol (RFC 2616[144]), which are the most successful protocol on the Internet [18]. SIP is:

*Transport-independent; SIP can be used with UDP, TCP, SCTP, etc.*

*Text-based, allowing for humans to read and analyze SIP messages.*

The function of SIP is to establish, modify and terminate multimedia sessions- with media such as voice, video and chat-over IP networks, where the media delivery part is handled separately [3].

In SIP there is just one single protocol, which works end-to end and supports the establishment and termination of user location, user availability, user capability, session set-up and session management. It is also enabling additional multimedia sessions and participants to be dynamically added or removed from a session. SIP is considered to be flexible and secure. All these reasons make SIP very convenient for using in IMS [4].

### 2.5.2. Diameter

Authentication, Authorization and Accounting Protocol

Diameter (defined in RFC 3588), which was developed from the current version of RADIUS protocol (RFC 2865) by the IETF, is the protocol of the policy support, Accounting, Authentication, Authorization (AAA) for IMS [17][19]. Diameter is used by the S-CSCF, I-CSCF and the SIP application servers in the Service Layer, and in their exchange with the HSS containing the user and subscriber information. Compared with RADIUS, Diameter has improved transport- it uses Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP), and not UDP, as transport-improved proxy, enhanced session control and higher security[4].
2.5.3. **H.248(Megaco or Gateway Control Protocol)**

H.248 protocol is a result of joint work of the IETF’s MEGACO working group and the ITU-T Study Group 16, it is defined in RFC 3525 and ITU-T Recommendation H.248. Megaco is a control protocol used between media control functions and media resources, for example between MGCF (Media Gateway Control Function) or MRFC (Media Gateway Function Controller) and MRFP (Media Resource Function Processor) [20].

2.5.4. **Session Description Protocol (SDP)**

SDP was developed by IETF and published in the RFC 4566. It is a format for describing multimedia communication sessions for the purposes of session announcement, session invitation, and the other forms of multimedia session initiation. SDP does not provide the content of the multimedia form itself but it provides a negotiation between two end points to allow them to agree on a media type and format [21].

2.5.5. **Real-Time Transport Protocol (RTP)**

RTP was developed by the Audio-Video Transport Working Group of the IETF and is specified in RFC 3550. RTP defines a standardized packet format for delivering audio and video over the Internet [22].

2.5.6. **RTP Control Protocol (RTCP)**

RTCP is a sister protocol of the RTP. It is defined in RFC 3550. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP [22].

2.5.7. **IPv6**

Internet protocol version 6 is a network-layer IP standard used by devices to exchange data across a packet-switched network. Originally, IMS was specified to use IPv6, but with 3GPP Release 6, IMS does provide support for IPv4 and private address scheme [4].
3. SIP in the IMS

3.1. SIP Place in the Internet Multimedia Protocol Stack

Figure 15 shows the four-layer Internet Multimedia Protocol stack and the SIP place in it.

![Figure 15. The Internet Multimedia Protocol stack [23]](image)

**Physical layer**

The very lowest layer is the physical layer and link layer, which could be Ethereal local area network (LAN), a digital subscriber line (DSL), a wireless 802.11 network, etc. This layer performs such functions as a symbol exchange, frame synchronization, and a physical interface specification [23].

**Internet layer**

The next layer is the Internet layer. IP –Internet Protocol, which is a connectionless, best-effort packet delivery protocol, is used at this layer to route a packet across the network using the destination IP address [23].

**Transport layer**

Then comes the transport layer. There are three commonly used transport layer protocols: Transmission Control Protocol-TCP, Transmission Layer Security-TLS and User Datagram Protocol-UDP [23].

**Application layer**

The top layer shown on figure 15 is the application layer. This layer includes SIP and media transport protocols like RTP (Real-time Transport Protocol), H.323 (an alternative signaling protocol to SIP). SDP –Session Description Protocol is shown above SIP in the protocol stack (Figure 15) because it is carried in a SIP message body [23].

As shown on the Figure 15 SIP can use any transport protocol.
3.2. **Session Control**

This part explains the concepts of the Session Initiation Protocol (SIP) that is used in the IMS to set up, modify and release the multimedia sessions.

SIP supports five facets of establishing and terminating multimedia communications:

- **User location:** determination of the end system to be used for communication;
- **User availability:** determination of the willingness of the called party to engage in communication;
- **User capabilities:** determination of the media and media parameters to be used;
- **Session setup:** “ringing”, establishing of session parameters at both called and calling party;
- **Session management:** including transfer and termination of sessions, modifying session parameters, and invoking services [24].

3.2.1. **SIP and User Mobility**

SIP – session initiation protocol is the main signaling protocol of the IMS. SIP provides user mobility through registrations, which makes the user always reachable under the same identifier regardless of the user’s current location. Every time a user becomes available at a user agent, the user agent registers its location with the user’s registrar, which is located in the user’s domain. This way, the home domain is informed about how to route incoming session requests to the user agent where the user is currently available. This kind of mobility can be managed across various networks and devices using SIP.

In SIP users are identified by URIs, which are very similar to e-mail addresses (for example: sip:liza@example.com) and they are not tied to a single physical device.

SIP also supports multicast. In the multicast routing, a single packet is routed to set of destinations [25].

3.2.2. **SIP Logical Entities**

**User Agent**

User agent is a logical entity, a terminal or software that users use to connect to the SIP network. UAs can act as both a user agent client, while generating SIP requests, and user agent server while generating a response to a SIP message [23].

**Proxy Server**

Proxy server is an intermediary entity that acts as both server and a client for the purpose of making requests on behalf of the clients.
Proxy helps to route SIP messages towards their destination, which means its job is to ensure that a request is sent to another entity “closer” to the targeted user. Proxy can also be useful for enforcing policy (for example, making sure a user is allowed to make a call). It can interpret or re-write certain parts of SIP messages; it can also send a request to a number of locations at the same time (this entity is called a “forking proxy”).

A proxy server is different from a user agent or gateway in three key ways:

- A proxy server does not issue requests; it only responds to requests from a user agent. (A CANCEL request is an exception to this rule.)
- A proxy server has no media capabilities.
- A proxy server does not parse message bodies; it relies exclusively on header fields.
Figure 17 shows a common network topology known as the SIP Trapezoid. A pair of user agents in different domains establishes a session using a pair of proxy servers, one in each domain. In this configuration, each user agent is configured with a default outbound proxy server, to which is sends all the requests [23].

Proxy servers can be:

**Stateful proxy:** A logical entity that keeps track of requests and responses received in the past and uses that information in processing future requests and responses. For example, a stateful proxy server starts a timer when a request is forwarded. If there is no response on the request within the timer period, the proxy will retransmit the request, relieving the user agent of this task. Stateful proxy can also require user agent authentication.

**Stateless proxy:** A logical entity that processes each SIP request or response based only on the message contents. Once the message has been parsed, processed and forwarded or responded to, no information about the message is stored-no dialog information stored. A stateless proxy never retransmits a message and does not use SIP timers. Technically, stateless proxy only forwards every request it receives downstream and every response it receives upstream [18].

**Back-to-Back User Agents**

B2BUA is a logical entity that receives a SIP request reformulates it and sends it out as a new request. Responses to the request are also reformulated and sent back in the opposite directions. For example, B2BUA can be used to implement an anonymizer service, when two parties involved in the session can communicate without either party learning the other party’s URI, IP address, or any other information.

![Diagram of Application Server acting like a B2B-UA](image)

**Redirect Servers**

Redirect server is a logical entity that generates 3xx responses to requests it receives, directing the client to contact an alternative set of URIs.
Registrar

Registrar is a server, that accepts SIP REGISTER requests and places the contact information it receives in those requests into the location service for the domain it handles. Technically, it means that the contact information from the request is available to other SIP servers within the same administrative domain, such as proxies and redirect servers.

Application Server

Application server is an entity in the network that provides end-users with a service, for example, presence service and conferencing servers [18][26].

There are other SIP clients and Servers but they are not in the scope of this work.

3.2.3. Session Establishment

SIP provides session establishment through a two-way session description exchange called the offer/answer model. A user agent generates session description that contains the information needed to establish the session and sends it to the remote user agent. This session description is referred to as the offer (request). On receiving the offer, the remote user agent generates its own session description, which is referred to as the answer (response). Once the offer/answer exchange completes, the user agent can start exchanging media between them. The session is considered to be established [25].

![A simple SIP session establishment example](image)

Figure 19. A simple SIP session establishment example [27]
The Figure 19 shows a simple exchange of SIP messages between two SIP-enabled devices, which can be SIP phones, softphones, hand-helds, palmtops, cell phone, etc. Both devices are connected to an IP network such as the Internet.

On the figure 20 we can see that Alice begins the message exchange by sending a SIP INVITE message to the called party, Bob.

![Figure 20. An INVITE message example [27]](image)

SIP message consists of: start line, a number of header fields and optionally the message body (Figure 21).

![Figure 21. A SIP message format [12]](image)

SIP messages can be either requests or responses.
### 3.2.4. Requests

**Request**: A SIP message sent from a client to a server to invoke a particular operation.

SIP requests are distinguished from responses using the start line, which is often referred to as the request line.

The start line consists of:
- Method name
- Request URI
- Protocol version

#### Methods

There are six original methods in SIP that are described in RFC 3261:

**INVITE**: used to establish media sessions between user agents. An INVITE usually has message body that contains the media information -SDP. Responses to INVITE are always acknowledged with the ACK method. A successful INVITE request establishes a dialog which continues until a BYE is sent by one of the parties.

**REGISTER**: used by a user agent to notify a SIP network of its current Contact URI (IP address) and the URI that should have requests routed to this Contact.

**BYE**: used to terminate an established media session.

**ACK**: used to acknowledge final responses to INVITE requests.

**CANCEL**: used to terminate pending searches or call attempts. It can be generated by either user agents or proxy servers.

**OPTIONS**: used to query a user agent or server about its capabilities and discover its current availability. The response to this request lists the capabilities of the user agent or server.

The rest methods are described in the separate RFCs.

**REFER**: used by a user agent to request another user agent to access a URI or URL resource.

**SUBSCRIBE**: used by a user agent to establish a subscription for the purpose of receiving notifications (via the NOTIFY method) about a particular event.
**NOTIFY:** used by a user agent to notify about of a particular event. It is always sent when a subscription exists between the subscriber and the notifier.

**MESSAGE:** used to transport instant messages (IM) using SIP. IM usually consists of short message exchanged in real-time by participants of a “conversation”

**UPDATE:** used to modify the state of a session without changing the state of a dialog. Possible uses of UPDATE include muting or placing on hold pending media streams, performing QoS or another end-to-end attribute negotiation prior to session establishment.

**INFO:** used by a user agent to send call signaling information to another user agent with which it has an established media session.

**PRACK:** used to acknowledge receipt of reliably transported provisional responses (1xx)

**PUBLISH:** used by a user agent for uploading information to a server [12] [23].

**Request URI**

The request-URI is a SIP or a secure SIP (SIPS) URI that identifies a resource that the request is addressed to.

**Protocol Version**

The current SIP version is 2.0. All requests within the RFC 3261 must include this version in the request, in the form “SIP/2.0”[23]

#### 3.2.5. Responses

![Figure 22. 180 Ringing response on INVITE][27]
Figure 22 shows the 180 Ringing response on INVITE request from the example depicted on figures 19-20. This response means that Bob’s user agent has started ringing.

![Figure 22. 180 Ringing response on INVITE](image)

Figure 23. 200 OK response on INVITE [27]

Figure 23 shows the 200 OK response on INVITE request from the example depicted on figures 19-20. This response means that Bob has answered the phone.

SIP responses can be distinguished from requests also by looking at the start line. The start line in the response is often referred to as the status line. It consists of:

- Protocol version
- Status code
- Reason Phrase [12]

**Protocol Version**

It is identical to the protocol version in the request line.

**Status Code**

The status code is a three-digit code that identifies the nature of the response. It indicates the outcome of the request. Status codes are classified in six classes (Table1)
Table 1. SIP response classes [23]

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1xx</td>
<td>Informational</td>
<td>Indicates status of call prior to completion. If first informational or provisional response.</td>
</tr>
<tr>
<td>2xx</td>
<td>Success</td>
<td>Request has succeeded. If for an INVITE, ACK should be sent; otherwise, stop retransmissions of request.</td>
</tr>
<tr>
<td>3xx</td>
<td>Redirection</td>
<td>Server has returned possible locations. The client should retry request at another server.</td>
</tr>
<tr>
<td>4xx</td>
<td>Client error</td>
<td>The request has failed due to an error by the client. The client may retry the request if reformulated according to response.</td>
</tr>
<tr>
<td>5xx</td>
<td>Server failure</td>
<td>The request has failed due to an error by the server. The request may be retried at another server.</td>
</tr>
<tr>
<td>6xx</td>
<td>Global failure</td>
<td>The request has failed. The request should not be tried again at this or other servers.</td>
</tr>
</tbody>
</table>

Table 1 shows six possible status codes classes in SIP response messages.

**Reason Phrase**

Reason phrase is a text field giving a short description of the status code, which is aimed to human users [12] [23].

3.2.6. **Header Fields**

After the start line SIP messages contain a set of header fields, which consist of the header field’s name and a header field’s value: *Header-name: header-value*.

**Mandatory Header Fields**

Some headers are mandatory in every SIP request and response. These headers and their formats are listed bellow:

- ✓ To header  
  To: SIP-URI(;parameters)
- ✓ From header  
  From: SIP-URI(;parameters)
- ✓ Call-ID header  
  Call-ID: unique-id
- ✓ CSeq header  
  CSeq: digit method
- ✓ Via header  
  Via: SIP/2.0/[transport-protocol] sent-by(;parameters)
- ✓ Max-Forwards header  
  Max-Forwards: digit

To: contains the URI of the destination of the message, but it is not used to route the message. It is intended for human consumption and for filtering purposes. The tag parameter is used to distinguish, in the case of forking proxies, different user agents that are identified with the same URI.
**From:** contains the URI of the originator of the request. Like To header field it is used for human consumption and filtering. The tag parameter is mandatory.

**Call ID:** is a unique identifier for a SIP message exchange.

**CSeq:** contains a sequence number and a method name. They are used to match request and responses.

**Via:** keeps track of all the proxies a request has traversed. The response uses this Via set to traverse the same proxies as the request did in the opposite direction.

**Max-Forwards:** used to avoid routing loops. Every proxy that handles a request decrements its value by one, when it is zero, the request is discarded [12] [18].

### Header Fields Identifying the Dialog

The user agent that generates the initial INVITE to establish the session generates the unique Call-ID and From tag. In the response to the INVITE, the user answering the request will generate the To tag. The combination of From tag, To tag and the Call-ID uniquely identifies the established session, called “dialog”. This dialog identifier is used by both parties to identify this call because they could have multiple calls set up between them. Subsequent requests within the established session will use this dialog identifier [23].

### Other Important Header Fields in SIP Messages

**Contact:** is mandatory for requests that create dialogs. In the request it is used to convey a URI that identifies the request originator and in the response – the responding resource. Contact header field must be present in INVITE request and 200 OK responses to invitations.

**Route:** The Route header field is used to force routing for a request through the listed set of proxies.

**Record-Route:** is inserted by proxies in a request to force future requests in the dialog to be routed through the proxy.

**User agent:** used to convey information about the user agent originating the request. May contain manufacturer information, software version or comments.

**Server:** used to convey information about the user agent serve generating the response.

**Session-Expires:** used to specify the expiration time of the session.

**Min-SE:** may be present in INVITE that contains Session-Expires field. Contains an integer number of seconds.

**P-Asserted-Identity:** used between trusted proxies to assert the identity of a user that has been authenticated. A proxy receiving P-Asserted-Identity from another proxy that it does not trust will remove this header field.
**Require:** used to list features and extensions that a user agent client requires a user agent server to support in order to process the request.

**Supported:** used to list one or more options implemented by a user or server.

**Allow:** used to indicate the methods supported by the user agent or proxy server sending the response.

**Priority:** may be used by the agent to set the urgency of a request: non-urgent, normal, urgent and emergency.

**Content-length:** used to indicate the number of octets in the message body. Zero indicated that there is no message body.

**Content-Type:** used to specify the Internet media type in the message body.

**Expires:** used to indicate the time interval in which the request or message contents are valid [18] [23].

There are a lot of other possible header fields in SIP.

### 3.2.7. The Message Body

The message body (payload) can carry any text-based information, while the request method and the response status code determine how the body should be interpreted. When describing a session the SIP message body is typically a Session Description Protocol (SDP) message. The detailed description of the SIP message body is out of the scope of this work [12].

### 3.3. Routing

Routing of the SIP messages is one of the most complex issues within IMS. Basic understanding of principles of routing can be achieved through the session flow example.

To make such example, let’s assume the following scenario (Figure 24)

![Figure 24. The example scenario [12]](image)

Figure 24 shows an IMS session between two users. It is based on the assumption that both users are attached to the General packet radio Service (GPRS). Tobias, who is a student from France is currently visiting Finland. He is calling his sister Theresa, who is working in Hungary and currently is on a
business trip to Austria. Tobia’s home operator is located in France. As he is roaming in Finland, the Finish operator provides the P-CSCF, as the home operator, because the Finish operator has signed an IMS roaming agreement. GPRS Support Node (GGSN) that Tobias is using is also located in Finland.

Theresa’s home operator in Budapest has no IMS roaming agreement with the operator in Austria. Therefore, her terminal gets attached to the P-CSCF in her Hungarian home network, where GGSN is also located. Theresa’s access to the IMS is based on the GPRS-level roaming agreement between the operators of her home network and the visited network. It is assumed that both Tobias and Theresa are registered in their home networks.

Then, the scenario is the following: Tobias calls Theresa, her user agent finally starts to ring. Theresa accepts the session. Now they can talk to each other and see each other on the screens of their mobile phones. After Tobias and Theresa have finished their call, they will hang up and one of their UEs will send a BYE request to the other UE [12].

![Figure 25. IMS session establishment call flow [12]](image-url)
This example does not take into consideration such important aspects like media streams agreement between two UEs, security, compression, resource reservation, billing, services initiation, etc. This example will demonstrate only the Routing part of IMS.

Figure 26 demonstrates the routing issues in IMS core network. The main SIP routing mechanisms are the following:

### 3.3.1. Processing INVITE

**Tobias’s UE → P-CSCF**

- Theresa’s SIP URI is indicated as destination in the request URI.
- Tobias’s UE puts its IP address in the Contact header of the request, so that the remote UE can directly reach it.
Tobias’s UE generates Via header and adds its IP address to this Via header in order to receive responses to that request.

Tobias’s UE can add Route headers, if during the registration the route between Tobias’s UE and its S-CSCF in the home network was discovered. P-CSCF Route header will be above, because UE always needs to contact its outbound proxy first.

**P-CSCF→S-CSCF**

When receiving the request P-CSCF:

- Puts its address on the top of the Via header, as it needs to receive all the responses to the requests.
- Adds the first Record-Route header and puts its own address there—this guarantees that all subsequent requests within the dialog will traverse the P-CSCF.
- If there was a Route header list received, removes its own entry from the topmost Route header.

**Tobias’s S-CSCF→ Theresa’s (I-CSCF)**

Receiving the request Tobias’s S-CSCF:

- Adds itself at the topmost Via header
- Adds itself in the Record-Route
- If there was a Route header received, removes its entry from the topmost Route header, so now it is empty.

Now S-CSCF needs to route the request further. S-CSCF takes the host part of the address of Theresa’s public user identity that is indicated in the request URI (i.e., home2.hu) and resolves a SIP server in that domain from the DNS. In return, it receives one or more addresses of I-CSCFs that are located in the home network of Theresa. It takes one of them and sends the request there. The I-CSCF in Theresa’s home network now needs to discover the address of the S-CSCF that is allocated to her. Even if Theresa is not currently registered, the I-CSCF may be able to discover the address of a default S-CSCF as long as Theresa is subscribed to some services as an unregistered user. Information about the S-CSCF currently allocated to a user is stored in the Home Subscriber Server (HSS); as there are several HSSs within the network, the I-CSCF first has to query the Subscription Locator Function (SLF) to discover which HSS holds the data for Theresa. After the SLF returns the address of the HSS, the I-CSCF queries that HSS, which finally returns the address of the S-CSCF that serves Theresa. The I-CSCF now may add a Route entry at the top of the Route list and put the received address of the S-CSCF into it.

**I-CSCF→S-CSCF**

- Adds itself at the topmost Via header
- Does not put its address in the Record-Route, because it does not need to receive any subsequent requests in this dialog-the task of the I-CSCF is to find the S-CSCF of the called user, and, as this is done during initial request processing, there is no need for it to stay in the Route Header.
- Can add Route with Theresa’s S-CSCF.

**S-CSCF→P-CSCF**

When receiving the request S-CSCF:
- Adds itself at the topmost Via header
- Adds itself in the Record-Route
- If there was a Route header received, removes its entry from it.
- May add the P-CSCF address in the Route header.

**P-CSCF→UE**

- Adds itself at the topmost Via header
- Adds itself in the Record-Route
- If there was a Route header received, removes it

After Theresa’s UE has received the INVITE request, it stores the received Contact value and the Record-Route header list, because it will route subsequent requests in the dialog based on them.

**Theresa’s UE→P-CSCF**

Theresa’s UE generates 183 (Session in Progress) response. It puts its own IP Address in the Contact Header to indicate the address it wants to use to receive subsequent requests in the dialog. Then Theresa’s UE:
- Puts all Via headers received in INVITE into the response
- Puts all Record-Route headers received in INVITE into the response
- Sends the response to the address and port number of the topmost entry in the Via header.

**Theresa’s P-CSCF→ Tobias’s UE:**

P-CSCF identifies the INVITE transaction the response belongs to by the branch parameter that is set in its own entry in the Via header. Then P-CSCF sends the response to the S-CSCF in Theresa’s network. Theresa’s S-CSCF sends it further to the S-CSCF in the Tobias’s network. Finally Tobias’s S-CSCF sends it to the Tobias’s P-CSCF. Each CSCF entry repeats the following routing steps:
- Removes its own address from the Via header
- Re-writes its own Record-Route entry (changes the port)
- Sends the request to the topmost entry in the Via header until it reaches the UE [12]
3.3.2. Routing of Subsequent Requests in a Dialog

Figure 27. Routing of subsequent requests and their responses [12]

Figure 27 demonstrates the routing of subsequent requests in the IMS core network.

When one of the two UEs needs to send a subsequent request within the dialog, it copies the stored Record-Route entries into the Route header (either reversed or as it is depending on the UE that is sending the new request) of the new requests and the remote UE’s IP address into the request URI. Then the request is routed toward the remote UE by strictly following the entries in the Route header. Every CSCF that is traversed:

- Puts itself in the topmost Via header in order to get all the responses to this request
- Removes own entry from the Route header

3.3.3. Routing from the S-CSCF to the AS

Before sending the request to the AS, S-CSCF:

- Adds own address at the top of the Route headers, in order to receive INVITE request back from the AS
- Adds address of the AS at the top of the Route headers, in order to route the INVITE request to the AS as the next hop
- Adds own address on the top of Record-Route headers, so that it stays on the route for subsequent requests as well.
- Adds its own address on the top of the Via headers, so that it receives all responses to the requests.
3.3.4. Routing from AS back to the S-CSCF

- Removes the topmost entry in the Route header that is pointing to the AS
- Adds its address to at the top of the Via list
- Route the INVITE request based on the topmost Route header back to the S-CSCF [12].
4. IMS Core Network Testing

4.1. The Purpose of the CSCF Testing

The IMS technology is being adopted by all sectors of the telecommunications industry including cellular, landline and cable. Gartner forecasts that the total revenue from the IMS core equipment will exceed that of traditional voice-over-IP control equipment in 2009.

Making IMS work will take a lot of hard work: developing IMS equipment means working in a multi-protocol environment with developing standards and proprietary extensions [28]. Like many new standards, IMS is somewhat fluid and open to interpretation. Although standards have been approved, they are often incomplete, are still evolving. Each of the different standards organizations, which include 3GPP, ETSI, TISPAN and IETF, publishes regular updates. Vendors interpret standards according to their needs and may introduce new innovations which they refer to standards bodies for inclusion in future releases.

IMS promises great revenues, but along with this promise is the threat of unhappy customer’s complaints about network failing, poor media conversation rates and bad service performance.

IMS standards define new network elements, Call Session Control Functions (CSCFs), Home Subscriber Service (HSS), Policy Control and Charging Rules Function (PCRF), ways to handle user authentication, call routing, session establishment, charging, the policy enforcement, etc. This new architecture introduces complexity. The distributed architecture of IMS leads to multi-vendor solutions with a high number of interfaces, differing performance characteristics expressed in a variety of terms.

The equipment vendors and service providers must seriously consider bringing new and high quality products and services to market quickly, avoiding the customer’s dissatisfaction. This requires rapid testing with high performance, scalability and capability to create different custom call flows easily.

IMS networks must be tested end-to-end: from the access to the core, including the myriad network elements, functions and connections/interfaces between them. While the types of tests vary little from those currently used in traditional networks, their number is much higher. IMS testing may contain:

- Functional testing to evaluate the network’s compliance with the specified requirements.
- Interoperability testing to test the interfaces and data carriage between network elements and foster interoperability confidence in the network.
- Capacity testing to ensure network components can handle both sustained traffic levels and surges.
- Media testing to confirm that multimedia traffic is transmitted reliably through the network.
- Proprietary call flow testing to test a non-standard call-flow.
- Trouble shooting and network monitoring to identify anomalies and flag up problems.
Testing of billing accuracy, policy and security issues, QoS, etc.

The CSCFs are the heart of the IMS control structure; along with the HSS they form the IMS “core” (as it was defined in section 2.4, Figure 8). No matter what configuration is implemented, whether the CSCFs are co-located or independently deployed, testing their functionality is of a primary concern. Call/Session Control Functions (CSCFs) process SIP signaling packets in the IMS (as described in section 2.4.1).

The recent thesis gives an example of the SIP functional test case within the IMS. It controls the SIP procedure correspondence to the SIP standards (as described in sections 3.2.2-3.2.7) and the accuracy of the SIP routing mechanism performed by the CSCFs (according to the rules described in section 3.3).

4.2. Possible Testing Environment

The Figure 28 gives an example of possible testing environment. As it can be seen, we have CSCFs and HSS, which can be prototypes or the real equipment that is under development or maintenance process and needs to be tested. CSCFs include P-CSCF, I-CSCF and S-CSCF. The interface between the I-CSCF and the HSS and between the S-CSCF and the HSS is based on Diameter protocol. This interface allows for:

- Location management procedures (exchange of location information)
- User data handling procedures (download user data stored in the server)
- User authentication procedures.

The CSCFs’ configurations can be changed with the help of Simulated Admin Interface. The parameters like “Session-Expires”, “Min-SE”, etc can be set by Simulated Admin Interface using LDAP script files.

The task of a person who performs as a tester is to simulate with the help of the special software User Equipment and Application Server (described in 3.2.2) in order to run different scenarios and test the CSCF behavior in different cases. Both the User Equipment and the Application Server simulators communicate with the CSCF using SIP protocol. Each simulator can be presented with the state machine that sends and receives SIP messages.
Figure 28. Example of possible testing environment [32]

The Figure 29 shows the possible CSCF configuration that consists of the originating and terminating part. Here we have Originating P-CSCF (P₀), Originating I-CSCF (I₀), Originating S-CSCF (S₀), Terminating I-CSCF (I₁), Terminating S-CSCF (S₁) and Terminating P-CSCF (P₁). Due to this structure, Originating User Equipment-UEORIG (a caller) can call to the Terminating User Equipment-EUTERM (a callee). Both UEs are simulated in the special software.

Figure 29 shows all the CSCF ports on originating and terminating side. Each CSCF has two ports (again it can be called “originating” or “ORIG” and “terminating” or “TERM”). As it can be seen the originating and terminating sides have “mirror-like” ports towards each other. Terminating User Equipment sends responses to the Terminating P-CSCF originating port.
On their way, SIP messages can traverse Application Servers (shown on the Figure 29) as Back-to-Back type Application Server (B2B) or Proxy type Application Server (PXY). Application Servers are connected to the S-CSCFs by the ISC interface. Application Servers are also simulated in the special software and can be present at both originating and terminating sides.

Some test companies are being focused on successful deployments and operations of IMS equipment and networks. One of the solutions for testing the IMS core network is suggested by Spirent Communications-Spirent Protocol Tester. This software allows simulating different IMS components and can serve for our purpose which is the simulation of the User Equipment and Application Servers.

4.3. **Spirent Protocol Tester**

Spirent Communications is worldwide provider of integrated performance analysis and service assurance systems for next-generation network technologies. Spirent Communications ([www.spirentcom.com](http://www.spirentcom.com)) has its U.S. headquarters in Sunnyvale, CA. Spirent Communications product Spirent Protocol Tester (SPT) is a state machine-based tester which performs functional and performance testing on IMS equipment and core networks. It is designed to support all protocols used in IMS. What is also important - Spirent is involved with the evolution of IMS architecture to ensure the solutions provide support for the latest iterations and applications.

![Figure 30. Spirent Protocol Tester](image)

**Spirent Protocol Tester Software for Developers**

The SPT software for developers is a software-only version of a complete SPT. This package includes one Windows-based client license, one Windows-based server license, and access to all test case editors, modules and libraries.

The SIP simulation Package adds comprehensive SIP feature and regression testing capabilities to the SPT. This combination creates an ideal simulation tool for testing SIP user agents, proxies, gateways, softswitches, session border controllers, PoC servers, firewalls or any other SIP enabled devices by simulating specific call flows. The SIP simulation Package is a rich library of pre-build messages and test cases that allow users to begin testing quickly and provides advanced developers all the power and flexibility they require. More advanced users can take advantage of the SPT to test even the most
extraordinary scenarios. The integrated message and state machine editors allow for comprehensive customization of every message, parameter and call flow for total flexibility and unlimited negative testing. The integrated database and user defined parameters features allow users to quickly tailor any test case for reuse in different network configurations [10].

**Figure 31. Spirent client architecture [10]**

Figure 31 gives an overview of the Spirent client architecture. It shows the process of creating and running a test case. It consists of these parts:

- **Message Editing and Configuration**
  At first, new test environment should be created: each network component we simulate is presented by the state machine, where we can operate with the SIP messages, configuration files and database.

- **Test case Construction and Execution**
  All the state machines we need for the specific test cases are put together in order to build a test case. The general database needs to be edited for the specific purposes. After that, the test case can be downloaded and executed on the server.

- **Call Trace and Reports**
  Spirent supports monitoring of the call and making reports on the results. Report shows if state machines succeed or fail. If some state machines fail, this means that something went wrong, due to some reason the call was not performed correctly and the error handling was used.

In our case we want to implement state-machines that simulate User Equipment and Application Servers. Basically, we simulate different call flow scenarios with different SIP methods, with different combination of Application Servers, etc. Spirent Protocol Tester also allows simulating CSCF but this is out of the scope of this work.
4.4. Example

The following example will demonstrate the process of finding the equipment’s (CSCF) error by the person testing the system. Two test cases for call forwarding function with two Application Servers—either two stateless or two stateful proxies (described in 3.2.2) were implemented according to the test case specification.

The theoretical part of SIP signaling in the IMS core network was done in Excel document (the part of the attachment document without the comments). The theoretical preparation is necessary for the human tester to compare the result received while the test case execution with the signaling defined by the SIP standard. The tester focused on the SIP procedure call flow, on the contents of the messages (described in 2.3.3-3.2.7) and mainly on the routing part (described in 3.3).

The important message headers (via, record-route, route) taken from Spirent were copied in the Excel document. The test case with two stateful proxies worked fine; the test case with two stateless proxies failed.

4.4.1. SPT Two Proxy Simulation

On figure 32 it can be seen that the User Equipment, two proxy applications and Terminating Half-Call are simulated with SPT.

**Testcase with Two Stateful Proxy Applications**

The purpose of this test case is to verify that the CSCF forwards a call in the correct way. Terminating CSCF should first invoke a stateful proxy (PxyAS w rr) that doesn’t forward the call and then a stateful proxy (PxyAS w rr) that forwards the call by changing the Request URI.

Figure 33 shows the call flow of the test case.
The test case creation process is performed as described in 4.3:

- **Message Editing and Configuration**

The Figure 34 demonstrates the state machine that simulates the stateful proxy that forwards the call by changing the Request URI.
The purposes of the state machine are:

- To perform as a stateful Proxy Application Server (as described in 3.2.2)
- To receive SIP messages
- To check that the received SIP messages were sent from the right port and IP address. If not, indicate the failure
- To check the accuracy of received messages’ contents. If not, indicate the failure
- To store the appropriate information from the received messages’ headers
- To generate additional new data
- To add the routing information to the SIP messages
- To forward correctly modified SIP messages
- To handle the received error messages and to indicate a failure

Basically, all other state machines that are necessary for this test case and are not shown in the thesis are implemented according to the principles written above.

The state machine that simulates the User Equipment generates data and sends SIP requests, receives responses and handles with the error cases.

The state machine that simulates the first stateful Proxy Application Server that does not forward the call looks almost like the state machine shown on Figure 34, but it does not perform the call forward function.

The state machine that simulates the Terminating Half-Call receives SIP requests, checks that they were sent from the right port and IP address, generates responses and handles with the error cases.
Test case Construction and Execution

All the state machines we need for this test case are put together as shown on the Figure 35. They are:

*User Equipment simulator (CSCF-O-Invite-O-Bye)*

*Stateful Proxy Application Server without call forwarding (CSCF-PxyAS-Invite)*

*Stateful Proxy Application Server with call forwarding (CSCF-PxyAS-Invite-CallForward)*

*Terminating Half-Call simulator (CSCF-THC-Invite2-O-Bye)*

The global database was build, the IP addresses and ports of the CSCF and other necessary parameters were configured. Figure 29 is very important while configuring of the IP addresses and the ports of the CSCF nodes. Now the test case can be downloaded and executed on the server.

![Figure 35. The test case with two stateful Proxy Application Servers ready to be executed [32]](image)

Call Trace and Reports
Figure 36 demonstrates the flow of the SIP messages. The person implementing the test case can compare the result with the theoretical part prepared beforehand. The tasks of the tester are:

- To follow the SIP call flow in Spirent (From what source to what destination the SIP request goes to)
- To check the call trace (routing) with the Figure 29.
- To compare the SIP call flow in Spirent with the theoretical signaling done in Excel document.

The report did not show failure.

![Figure 36. Two stateful proxies call flow in Spirent [32]](image)
By clicking on the message the tester can view its contents as shown on Figure 37.

![Message Viewer](Image)

**Figure 37. The INVITE request [32]**

Attachment 1 compares the theoretical part of the call flow with the result achieved in Spirent. The SIP headers taken from the messages in Spirent were copied to the Excel document as comments. For making comparison the tester also needs to know the CSCF configuration (Figure 29).

RESULT: The test case works fine, no errors were found.

**Testcase with Two Stateless Proxy Applications**

The purpose of this test case is to verify that the CSCF forwards a call in the correct way. Terminating CSCF should first invoke a stateless proxy (PxyAS wo rr) that doesn’t forward the call and then a stateless proxy (PxyAS wo rr) that forwards the call by changing the Request URI.

Figure 38 shows the call flow of the test case.
• Message Editing and Configuration

The Figure 39 demonstrates the state machine that simulates the stateless proxy that forwards the call by changing the Request URI.
Figure 39. State machine simulating the stateless Proxy Application Server with call forwarding [32]

- **Testcase Construction and Execution**

This state machine has the same purposes as the state machine simulating the stateful Proxy Application Server but it has to perform as a stateless Proxy Application Server.

As it can be seen on Figure 38 and on Figure 39, the ACK and BYE message do not traverse the stateless Proxy Application Server. If the state machine, however, receives ACK, BYE or some other unexpected error message it will indicate the error with the “Fail” state and handle it by using the error path.

The state machines that are necessary for this test case have

- To receive SIP messages
- To check that the received SIP messages were sent from the right port and IP address. If not, indicate the failure
- To check the accuracy of received messages’ contents. If not, indicate the failure
- To store the appropriate information from the received messages’ headers
- To generate additional new data
- To add the routing information to the SIP messages
- To forward correctly modified SIP messages
- To handle the received error messages and to indicate a failure

The state machine that simulates the User Equipment is the same as in the previous test case example.
The state machine that simulates the first stateless Proxy Application Server that does not forward the call looks almost like the state machine shown on Figure 39, but it does not perform the call forward function.

The state machine that simulates the Terminating Half-Call is the same as in the previous test case example.

- Test case Construction and Execution

All the state machines we need for this test case are put together as shown on the Figure 40. They are:

**User Equipment simulator (CSCF-O-Invite-O-Bye)**

**Stateful Proxy Application Server without call forwarding (CSCF-PxyAS-Stateless-Invite)**

**Stateful Proxy Application Server with call forwarding (CSCF-PxyAS-Stateless-Invite-CallForward)**

**Terminating Half-Call simulator (CSCF-THC-Invite2-O-Bye)**

The global database was build, the IP addresses and ports of the CSCF and other necessary parameters were configured. Figure 29 is very important while configuring of the IP addresses and the ports of the CSCF nodes. Now the test case can be downloaded and executed on the server.

![Figure 40. The test case with two stateless Proxy Application Servers ready to be executed][32]
Call Trace and Reports

Figure 41 demonstrates the flow of the SIP messages in Spirent. It can be seen that the state machine simulating the Terminating Half-Call (CSCF-THC-Invite2-O-Bye) fails.

The test case also fails, because one of the state machines fails. The Analysis tool in Spirent shows the path that was taken in the failed state machine, so the developer can find the reason why it is not working properly.

The figure 42 shows the failed state machine. As it can be seen, the test case fails because the ACK message comes to the UE from the wrong port.
Figure 42. The failed state machine in Spirent. The test case fails because the UE receives the ACK message from the wrong port [32]

Attachment 2 compares the theoretical part of the call flow with the result achieved in Spirent. The error can be identified. ACK message that is sent from the terminating S-CSCF to the THC (Terminating half call) should be sent from the terminating port of the S_T-CSCF, which is configured as 7050 (Figure 29). In Spirent we can see that terminating S-CSCF (S_T-CSCF) sends ACK message from the port 7070, which is ISC port. This is totally wrong.

RESULT: It’s clear, that the equipment has a bug.

Different test case scenarios (successful calls, unsuccessful calls, busy, etc) with different requests (UPDATE, CANCEL, INFO, etc) were implemented. All test cases with two stateless proxies failed (Figure 43). The equipment developer was informed about the bug that was found in the CSCF.

Figure 43 demonstrates how the test suite execution works.
4.5. **TTCN-3**

In the past decade, the telecommunication systems to be tested are constantly becoming more dynamic and complex in their nature. To meet these new challenges the new testing technology should be applied. TTCN-3 is proposed to become a new widely spread testing technology. As recent developments show, industry and research start focusing more and more on testing with TTCN-3 [31].

The Testing and Test Control Notation Version 3 (TTCN-3) is an internationally standardized programming language specifically designed for testing of a wide range of computer and telecommunication systems [29].

TTCN-3 has been developed and is maintained by the methods for Testing and Specification technical Committee at ETSI. The TTCN technology has been applied widely and successfully in European industry, ETSI standardization, and certification for more than a decade [30].

TTCN-3 has a powerful, intuitive textual format for defining test scenarios that is similar to conventional procedural programming languages. This textual format if referred to as the TTCN-3 core notation. However, besides typical programming constructs, it contains all the important features to specify test procedures and campaigns for functional, conformance, interoperability, load and scalability tests. These test-specific features are unique compared to traditional scripting or programming languages, and above all technology-independent. TTCN-3 is suited for a large variety of application domains, because it is not tied to any particular application or its interface as well as to any specific test execution environment, compiler or operation system.

This flexibility makes TTCN-3 more preferable than other test tool or vendor proprietary language.
Typical areas of application of TTCN-3 are:

- Protocol and service testing
- Component, integration and system testing
- Testing of embedded, communication-based, and distributed systems

Examples of application domains:

- Mobile communications (LTE, WiMAX, 3G, TETRA, GSM)
- Broadband technologies (ATM, DSL)
- Middleware platforms (WebServices)
- Internet protocols (SIP, IMS, IPv6)
- Smart Cards
- Automotive (AUTOSAR, MOST, CAN) [31]

TTCN-3 is used to specify tests and in which order to execute them, but a TTCN-3 test system is needed to execute TTCN-3 tests (Figure 44). Figure 39 shows the general structure of a TTCN-3 Test System. TRI and TCI standards define test system architecture:

- TTCN-3 tools are required to support internal interfaces
- Allow reuse of test platform components with different tools but also for different System Under Tests (SUTs)

The construction of a TTCN-3 test system requires:

- A TTCN-3 test suite
- A TTCN-3 tool, i.e., a TTCN-3 compiler (or interpreter) plus execution environment.
- Optionally implementations for test execution control, logging and codecs.
- A SUT Adapter implementing the means of communication required by SUT interfaces.
- A Platform Adapter implementing a timing model, e.g., wall clock time, and external functions (if there are any defined in the test suite) [30]
TTCN-3 can be easily applied to test IMS and SIP. ETSI TC TISPAN WG6 has been working on a number of conformance test suites for IMS testing. These standardizes SIP TTCN-3 test suites have been validated by ETSI members. They can be downloaded from ETSI’s official TTCN-3 home page [30].

Using TTCN-3 in IMS testing means using a modern standardized testing technology and the possibility to adapt the same test suites for the different applications (to a simulator, to a smart phone, etc). Besides TTCN-3 test suites can be used across the whole product development cycle. TTCN-3 can provide major benefits in terms of return on investment in testing tools, training and product quality.
5. Conclusion

The thesis has described the key elements comprising IMS SIP technology, including its architecture, network components and protocols, signaling and routing mechanisms.

The telecommunication industry is evolving to the next step in multimedia convergence- IMS. World biggest telecommunication giant like Ericsson, Nokia Siemens, Alcatel-Lucent, Motorola, Nortel, Cisco, NEC are in the process of deploying the IMS network architecture. IMS architecture framework will enable operators to offer new services avoiding high operational expenses. It will also enable a service provider to offer multiple services over the same network due to the IMS layered approach. These are the major reasons why all facets of the industry are rapidly moving toward IMS solutions in order to develop the ultimate next-generation converged platform that will transform the future of voice, video and data communications for consumers and businesses.

The IMS deployment is accompanied with the great challenges, both commercial and technical. The IMS with its varied, diverse and complex technologies and protocols is a quite difficult and complicated solution. In order to avoid different network components’ interconnection problem and other problems that may appear while implementing IMS, the development process should contain the testing part.

The thesis has described the alternative of the IMS CSCF testing using Spirent Protocol Tester. The IMS core network predominantly consists of the Call Session Control Function (CSCF) and the Home Subscriber Server (HSS). The Call Session Control Function plays an important role in IMS. The CSCF node facilitates SIP session setup and teardown. The testing of this component is of a primary concern.

Before the release of the hardware, the developer needs to test the product in a simulated environment to test the functionality, interoperability, and conformance of IMS components. Spirent Protocol Tester is able to fulfill these tasks. The thesis has given an example of testing which is concentrated on SIP signaling path between the IMS CSCFs. The theoretical part based on SIP protocol specifications has been done in the Excel document. Two test cases with the same call flow scenario but different applications servers traversed have been build in Spirent. The test case with two application servers behaving like stateless proxies failed. The result received in Spirent was compared to the theoretical signaling of this test case made in Excel. The error was identified and it happened to be a bug in the CSCF. The developer of the CSCF was informed about the bug that should be fixed in the next CSCF release.

There are plenty of other opportunities to perform the testing of the IMS components. Different companies suggest their software solutions, but the general trend is- using TTCN-3, which is the internationally standardized testing language. Still a lot of research work has to be done for making the transition to TTCN-3 testing.
6. References


2. **IP Multimedia Subsystem.** Wikipedia.[WWW]

3. **Session Initiation Protocol.** Wikipedia.[WWW]


   http://www.mudynamics.com/assets/docs/ims_case_study.pdf

   http://acronyms.thefreedictionary.com/


   http://www.ixiacom.com/solutions/ims/


    http://www.testingtech.com/services/ttcn3_tutorial.php


http://enos.itcollege.ee/~irokk/sissejuhatus.IMSi_s08/IMS_loeng_1.pdf


http://www.ietf.org/rfc/rfc3261.txt


http://www.ietf.org/rfc/rfc3588.txt?number=3588


http://en.wikipedia.org/wiki/Megaco


http://www.ietf.org/rfc/rfc2327.txt


http://www.ietf.org/rfc/rfc3550.txt


http://www.tech-invite.com/Ti-sip-CF3665.html#ref31


30. ETSI official TTCN-3 home page. [WWW]

http://www.ttcn-3.org/


32. Softronic Baltic AS internal documents.