Migration of VOIP/SIP Enterprise Solutions towards IMS

by

Lian Wu
Anders Hagelskjær Aasgaard

Thesis in partial fulfilment of the degree of
Master in Technology in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad
Norway

May 2006

Abstract

Voice-over-IP solutions based on SIP and Skype are now widely spread and accepted by end-users. "Traditional Circuit Switched" voice services suffer from declining revenues, high maintenance cost, and a lack of integration with Internet applications.

For an enterprise customer it is increasingly difficult to make a decision about which VoIP solution to select. For fixed and mobile operators new solutions based on IMS are on the horizon, and investment strategies for VOIP solutions are difficult.

The research project will investigate VoIP/SIP solutions based on open source as a starting point, and outline their possible migration towards IMS for enterprise customers. Major differences between current VoIP/SIP solutions and IMS will be outlined.

Architecture components that allow interconnection, extension and migration of VoIP solutions towards IMS shall be proposed. Possibly “proof-of-concept” demonstrations will also be built to verify interoperability aspects.

We have proposed four IMS migration solutions that connect a VoIP/SIP enterprise solution together with the upcoming IMS technology. We also outlined a possible migration roadmap that shows in what stage of IMS development the solutions can be implemented. Furthermore this thesis shows the design and implementation of a working state-of-the-art VoIP/SIP enterprise solution.

Preface

This thesis concludes the two-year Master of Science program in Information and Communication Technology (ICT) at Agder University College (AUC), Faculty of Engineering and Science in Grimstad, Norway. The workload of this thesis equals 30 ECTS and the project has been carried out from January to June 2006.

First of all, we would like to thank Professor Dr. Frank Reichert, our supervisor at Agder University College, for excellent supervision and guidance throughout the project period. The thesis has been developed in co-operation with Teleca Wireless Solutions AS (TWS) in Grimstad, Norway. In this context we will also thank our supervisors at TWS, chief technical officer, Jøran Bøch, for very good support and advices, and Senior Tester Elis Johannsson for good help on our IMS part research.
In the VoIP/SIP part of our research we would like to thank co-student Erling Reizer, he has been a valuable asset in the testing of our Teleca/HiA testbed.
Thanks to Sjur Eivind Usken from Phonect that helped us with free VoIP/PSTN testing accounts for our testbed.
Finally we would like to thank Head of Studies, Stein Bergsmark, for his contributions, and our co-students for helpful feedback on our thesis.

Grimstad, May 2006

Lian Wu

Anders Hagelskjær Aasgaard

Table of contents

Table List

Figure list

1 Introduction

1.1 Background

Following the wide spreading of Internet, VoIP became very popular, especially amongst global enterprise businesses. Instead of traditional telephony services, many enterprises have adopted or plan to use VoIP. VoIP promises to provide more flexibility and cost-efficiency.

Different VoIP protocols and solutions created compatibility and interoperability obstacles. Security and QoS are very important for enterprises to choose the right solution. IMS is the key element in next generation network and provides a reference architecture for operators to realize real-time communication services offering key features such as QoS, security, group management, and instant voice messaging. IMS supporters claim that this technology will replace today's solutions, and it will be important to make decisions now that make the transition to IMS easier. SIP promises to make the migration to IMS less complicated, and most IMS functions can be recognized as part of a SIP-based next generation VoIP service platform.

This thesis is introduced by Teleca Wireless Solutions AS, which is one of the world's leading independent 2.5G/3G competence centers, working with major Network Equipment Providers and global Mobile Operators. They are working with GPRS/UMTS/IMS Software development for Ericsson and offer professional services and products for international Mobile Operators. Since its major customers are migrating to an All-IP infrastructure, it is important for Teleca to keep up with this area and to have the knowledge to explore new and promising business opportunities, e.g., in enterprise solutions in the VoIP/SIP/IMS area.

1.2 Thesis definition

The research project will investigate migration of VOIP/SIP Enterprise Solutions towards IMS.

The final thesis definition is formulated like this:
"Study and evaluate possible VoIP/SIP solutions for enterprise customers, and build a HiA-Teleca VoIP/SIP test-bed. Study and evaluate possible IMS solutions for enterprise. Compare major differences between current VoIP/SIP solution and IMS solution, and then propose an architecture that allows interconnection/extension/migration of VoIP solutions towards IMS"

1.3 Problem statement

The project will focus on the technical aspects of VoIP/SIP and IMS solutions based on standards or widely accepted solutions. Open source VoIP/SIP implementations will be used as a starting point to save time and cost. This will also give us a well-

documented and well-tested starting point for our project. If it's necessary the source code will be modified to reach our project goals.
The study will not evaluate the Skype solution or other proprietary protocols that are not disclosed nor standardized. We assumed the enterprise customer has broadband Internet access, and an Intranet that can host new services, if required.

Nowadays there are already some VoIP/SIP solutions available, and our first challenge is to identify State-Of-the-Art Enterprise SIP Solutions. Many enterprises aren't satisfied with only using traditional telephone services. Rich features like presence, instant messaging, voicemail, video conference, etc are interesting and may increase productivity. Interconnecting applications like e-mail with the enterprise PBX will provide more convince and efficiency for users. For example; a user can dial other users by simply selecting them from his address book. How to implement these enhanced features in our test-bed is our second task.
Since most enterprises have firewall and NAT for security reasons, traversal issues should be considered in our solution. For example; call between SIP clients behind different NAT domains, or how-to access phone resources from outside the enterprise domain. Hence our next challenge is achieving roaming across business domains.

The next and final problem involves IMS research. It's time consuming for enterprise users to update their terminals to SIP/IMS phones. How can we integrate these legacy non IMS/SIP phones and legacy mobile phones into our IMS migration solution?

Our vision; Inside an enterprise domain, a user will be reachable at sip:user@enterprise.com. Multiple SIP or mobile phones can be used to receive calls.

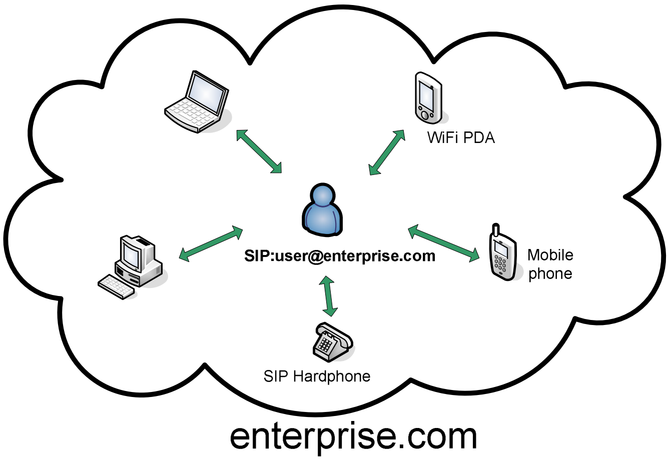


Figure 1 SIP Enterprise

When the user leaves the enterprise domain, he will use his mobile phone to register with operator.com domain. Then we face a problem, how can the user still receive calls referring to sip:user@enterprise.com?

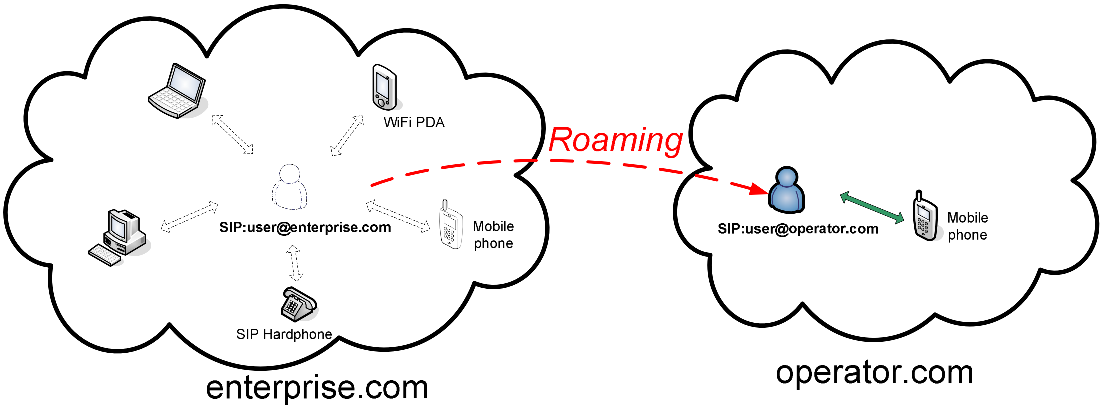


Figure 2 IMS Migration

The list below contains possible enterprise requirements:

- VoIP/SIP solution
- NAT Traversal
- Presence
- IM
- Conference
- Video support
- SIP client
- Roaming support
- Integrate Mobile phone
- Integration of legacy mobile and non-SIP ,non-IMS phone support

1.4 Importance of study

Voice-over-IP services based on SIP are widely spread and accepted by end-users; furthermore, fixed and mobile operators are investigating solutions based on IMS. Who will need solutions based on our project?

- Enterprises will need to select the right strategy for cost-efficient and flexible voice and application services as well as being prepared for future business.
- Operators need to address the enterprise market with new services,
- Manufacturers have to invest in the right product portfolio.

The project is of interest to ourselves because it gives us a good theoretical and practical experience with VoIP/SIP/IMS, and a chance to demonstrate our capabilities to solve complex system engineering problems. Building up a test-bed from scratch, enhanced with rich features, and demonstrating them to our "customers", will be very rewarding.

1.5 Report outline

This report is structured as followed:

Chapter 1 gives an introduction to the master thesis which is the current chapter.

Chapter 2 provides the basic theory about VoIP/SIP/IMS and related technology for building enterprise VoIP network. This will establish a foundation for understanding the later proposed solutions.

Chapter 3 evaluates which SIP solutions that will be used in the testbed.

Chapter 4 proposes the VoIP/SIP solution and describes how we implement the HiA-Teleca testbed.

Chapter 5 extends the solution with IMS migration.

Chapter 6 discusses all the results we have achieved in this project.

Chapter 7 gives the conclusion of our project work and point out possible further work based on this thesis.

2 Theory and State of Art

2.1 Theory

2.1.1 Voice over Internet Protocol

Using your broadband connection or any other computer network to transfer human speech was first developed in 1973 by the Internet researcher Danny Cohen. He defined a two part structure which is used in VoIP applications to this day. A control protocol and a data transport protocol. The first one is used to handle the initiation of a call and any other requirement, while the last one is responsible for transferring the voice data. [2.1][2.2]

Voice over Internet Protocol (VoIP) has since then evolved into a wide spectrum of different services over media protocols such as SIP [RFC 3261][2.3] and H.323[2.4]. Some services restrict you to only call other people using the same services or application, while others give you the same functionality as a normal telephone.[2.5][2.6]

2.1.2 Quality of Service

Quality of Service (QoS) refers to a way of guaranteeing that a packet will not be dropped between to points in the network. [2.7]
In today's packet switched network, we have no guaranties for when or how data reaches its destination. The internet is based on a "best effort" strategy that will work just fine with web browsing and mail transfer. Because if a request for a webpage fails, the packet would just be re-sent. This is not practical for VoIP communication. We need a way of negotiating the possible bandwidth speed when a call is initiated.

2.1.3 Session Initiation Protocol

Quote from The IMS – IP multimedia Concept and Services [2.8]:"*SIP is an application layer protocol that is used for establishing, modifying and terminating multimedia sessions in an Internet Protocol (IP) network*"

The Internet Engineering Task Force (IETF) is in the processes of continuously standardizing this protocol, and has been using it for a while to distribute multimedia content. It was later adapted to VoIP because of its extensibility.

SIP has inherited its simplicity from Hypertext Transport Protocol (HTTP) and Simple Mail Transfer protocol (SMTP), which is one of the most successful designs of the Internet. Therefore SIP has the same basic design goals. But most important for this project is the focus on personal mobility. [2.2][2.9][2.10]
More about SIP functionality in roaming theory (2.1.8)

2.1.4 Private Branch eXchange

A Private Branch eXchange (also called PBX or Private Business eXchange) is a privately owned telephone service that connects all the enterprise telephones to the public telephone system. A PBX will handle telephone number's and call routing inside the enterprise like the old telephone switching services where people manually connected each individual to a certain phone number. The difference is that everything is handled automatically. It may also handle the voicemail and many other common services, like internal enterprise calls.[2.11]

2.1.5 IP Multimedia Subsystem

Quote from The IMS – IP multimedia Concept and Services [2.8]:"*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*"

IMS is the new technology that will connect the existing infrastructure with the next generation of phone systems. Telecom operators may use this architecture to tie together fixed and mobile multimedia services. IMS will tie together exciting services, and give support for all of them from any terminal in any location. It's based on the standard IP protocol, defined by the IETF, and IP will be used regardless of the interface initiating or accepting the call. [2.12]

IMS is regarded by many as the leading new technology because it merges the internet with the cellular world and keeps the main advantages of each system.[2.13]

IMS will be discussed more thoroughly in chapter 5 and appendix D.

2.1.6 Firewall

Definition according to Wikipedia [2.14]: "*A firewall in computing is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy.*"

If a request comes from an outside computer to a firewall and was not initiated from inside the private network, the default action is to drop the request immediately. So call requests from the outside are almost impossible.
When a computer inside a firewall domain initiates any form of request, the router/firewall keeps track of the communication and keeps a channel open for that specific computer.

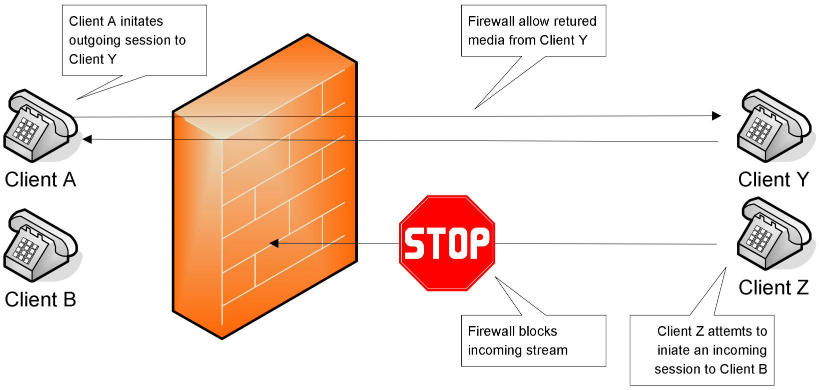

Client A initates outgoing session to Client Y
Firewall allow retured media from Client Y
Client A
Client B
Client Y
STOP
Client Z
Firewall blocks incoming stream
Client Z attemts to iniate an incoming session to Client B

Figure 3 Firewall traversal

2.1.7 NAT

To understand NAT we first have to define the difference between a private and a public network (the Internet). In Internet terminology, a private network is a network that uses private IP address space not routable on the public Internet. [2.16] From Wikipedia[2.17]: “*Computers may be allocated addresses from this address space when it's necessary for them to communicate with other computing devices on an internal (non-Internet) network but not directly with the Internet.*“
A NAT takes private IP addresses and ports and translates them into public ones. Because of this a limited number of public IP addresses are sufficient for a large corporate network.
Another reason is to hide the computer from public access and thus making it more secure. This added security comes at a price, especially for VoIP/SIP services.

In order to make the computer address private but still allowing it to access remote services, the NAT router keeps a table that links the private addresses and port numbers to the public IP addresses and port numbers. This table contains links of communication that has been started from inside the NAT; therefore communication initiated from the outside will fail.

When a call is initiated the request is transferred with SIP, while the actual audio is transferred over the Real-time Transport protocol (RTP) on another port.
This causes problems for both Firewall and NAT environments. The end-to-end media transfer (RTP) contains only details of the private addresses and ports from the computer it was sent from. So when the client on the other side tries to return the media information it will fail, because the private address doesn’t mean anything on the public network. [2.15]

NAT traversal methods are shown in Appendix E.

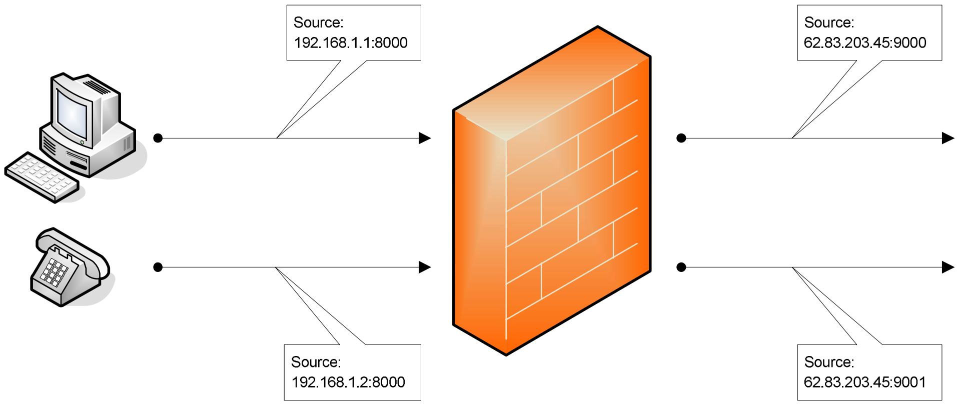


Figure 4 NAT Traversal

2.1.8 Roaming

Introduction

The concept of a stationary office is fading in today's enterprise environment. Users will work from home, another office or from their cell phone. All of these environments will have a static reachable address or phone number. But addresses to reach these environments will be different Trying to reach an individual may require you to try several telephone/URI extensions. This is time consuming and expensive. Can SIP technology make all this change?

What is roaming?
According to Wikipedia [2.18]:"*Roaming is a general term in wireless telecommunications, which refers to the extending of connectivity service in a location that is different from the home location where the service was registered.*"

So when you are trying to use the phone resources located on an enterprise PBX or SIP server that is different from the one you are currently using, you are a roaming user. Another example used in this text; if you are outside of the normal environment used to access the enterprise PBX or SIP Server but still is allowed access to it.

2.1.8.1 Registrar Server

From voip-info.org[2.19]: "*A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.*"

So a registrar is responsible for one or more public host's that defines user identities. In this case the userA has sip:userA@teleca.no as his main identity. When userA moves to another location he receives another sip identity: sip:userA@hia.no. This is where the registrar server comes in handy. The user or server responsible for hia.no will pass along location information to the registrar at Teleca.no. So when a call arrives at userA@teleca.no the registrar will know where the call should be forwarded.

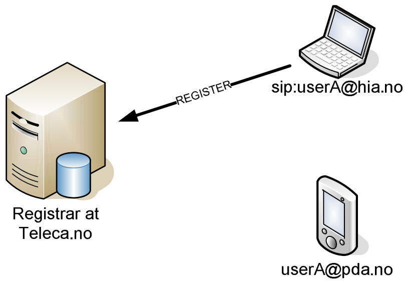


Figure 5 Registrar Server

2.1.8.2 Proxy Server

Based on the information in the location server, (which is stored and handled by the registrar) the proxy server plays the role of routing the requests to the specified location. The proxy will rewrite the received SIP message and forwarding it to its new location.[2.20]

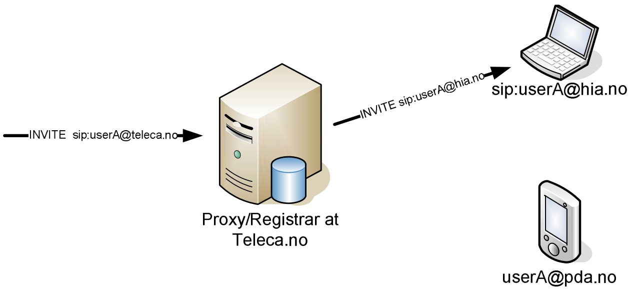


Figure 6 Proxy Server

2.1.8.3 Redirect Server

From voip-info.org[2.21]: “*A redirect server is a user agent server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URI’s.*”
Rather than directly transferring the call like a proxy, the redirect server will send location information back to the client that initiated the call. The client will then know the location of the user he wants to get in touch with and can contact this user directly. This will reduce the load of the SIP server.

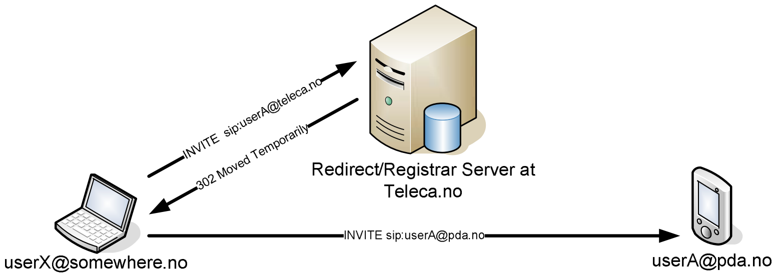


Figure 7 Redirect Server

2.1.9 Presence

Presence is a way to display your status or availability to system users. A client will send information to a server to show if he is busy, on the phone, in a meeting or just online. This is widely used in VoIP and IM applications to show a user’s willingness or possibility to communicate. [2.22]
Appendix D shows presence architecture and procedures in SIP and IMS.

2.1.10 Instant messaging

Instant messaging (IM) is a way of instantly communicating between two or more people over a network. A user will connect to a server that may have presence status about all the users on that system or a in a private “buddy list”. From the presence status it is visible who can be reached by instant messaging. [2.23]

2.2 “VOIP to IMS Migration” - Literature Review

The implementation of SIP features for VoIP services has been going on for some years. Hyun et al. [2.24] address the design and implementation of SIP server components. The features supported include call establishment, termination, registration, and capability negotiation. S. Zeadally and F. Siddiqui has written an article about implementing SIP features and they have with great success implemented a range of functionality, example: point-to-point, and multi-point audio conferencing.[2.25]

IP Multimedia System (IMS)[2.26][2.27][2.28], namely an overlay architecture for the provision of multimedia services, such as VoIP and videoconferencing on top of globally emerging 3G broadband packet networks. There is an overall agreement that the way to merge today’s different mobile and fixed communication architectures is thru IMS. T. Magedanz, D. Witaszek, K. Knuettel has written an article called THE IMS PLAYGROUND @ FOKUS[2.29]. They conclude that to develop VoIP/SIP and IMS services we need an open testbed where manufactures and enterprises can test out there new applications. A testbed should expose NGN enabling technology and the related technical know how in an encouraging way to the academia and industry.

Today, there are many IMS pre-products originating from the VoIP and wireless telecommunications market. But, there is not yet any commercial IMS deployment within operator networks. However, first “Push To Talk” (PTT) service implementations that are mushrooming around the globe can be regarded as the first big trials for IMS technologies. There are also some more specific articles about the function of specific parts of an IMS network: Peter Kim et al has written a paper about implementing a IMS PTT feature on a GPRS/UMTS network [2.30]

3 Evaluate VoIP/SIP Enterprise Solutions

To build a successful VoIP/SIP testbed extensive research has to be done to make sure all the necessary functionality will be available to us. The testbed will be time-consuming as there are an incredible amount of different aspects to take into consideration. We will start with our requirements and from that we will choose all the necessary software and hardware.

3.1 Requirements

To qualify as a valid VoIP/SIP enterprise solution we have these requirements:

- Support for wide array of operating systems
- Interoperability with standard hardware
- Compatible with wide array of soft/hard-phones
- SIP support
- NAT/firewall traversal support
- Voicemail
- Presence and Instant Messaging
- Video Support

3.2 Evaluate SIP Clients

A client is the only equipment a user will relate to. It's important to find one that is simple to use and still supports advanced functions.

3.2.1 SIP Softphone

A softphone is fully functional IP Telephone running as an application on a computer. It requires appropriate audio hardware to work. Their main advantage is that most of them are available as free download and can with ease support video and presence.

3.2.1.1 SJphone v.1.60

SJphone[http://www.sjlabs.com] supports multiple operating systems; Windows, Linux and MAC. In 2005 it got “Internet telephony – Product of the year” award [http://www.tmcnet.com/]. It's well known for great audio quality and ease of use. Further more it's fully interoperable with most major Internet Telephony Service Providers (ITSP) and software and hardware manufacturers. Free download from SJlabs web site.

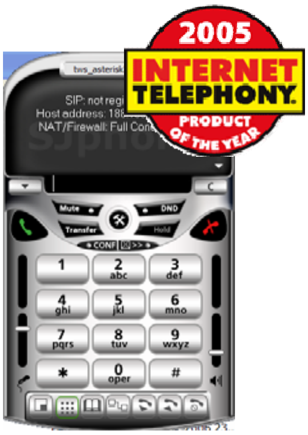


Figure 8 SJphone

Functionality:

- Protocol: SIP/H.323
- Audio codec: G.711, GSM, iLBC

- Automatic NAT detection by STUN
- PDA Support

3.2.1.2 Xten EyeBeam v1.1.3006

Xten eyebeam [http://www.xten.com/] softphone made by Counterpath is the commercial version of free “X-Lite” softphone made by the same company. It has an incredible amount of features, including Presence, IM and video support. For 2-9 users it costs 40$.

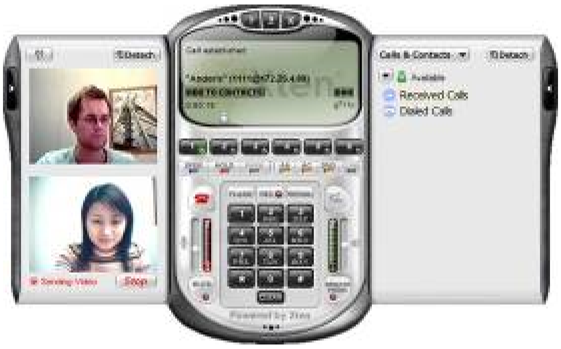


Figure 9 Xten EyeBeam

Functionality:

- Protocol: SIP
- Audio codec:
  DVI4, G.711, G.729A, GSM, iLBC, Speex, L16 PCM & Speex
- Video Codec: Basic H.263,H.263+,H.263++CIF
- Presence & Instant Messaging
- NAT Traversal using STUN, ICE & Xtunnels (v1 & 2)

3.2.2 SIP Hardphone

A SIP hardphone will look very similar if not identical to a normal phone. The difference is on the inside where we find a small CPU that interprets SIP instead of PSTN/ISDN messaging.

3.2.2.1 Grandstream GXP-2000

Another winner of the 2005 Internet Telephony – Product of the year award is Grandstream GXP-2000 [http://www.tmcnet.com/].
It supports SIP, NAT, Presence and CallerID. In addition gradstream has a higly dedicated firmware development unit.

Figure 10 GXP-2000

Functionality:

- Protocol: SIP
- Support NAT traversal (STUN, etc)
- SIP presence (SIMPLE)
- Multi-line support of up to 11 lines indicators (expandable to a few dozen more through expansion key-module)
- Graphical LCD to display up to 8 lines and 22 characters per line
- Support Caller ID display or block, per call or permanent

3.3 Evaluate Software SIP PBX

To have a successful SIP/VoIP testbed we needed to choose a SIP PBX that had all the features we needed for testing. We also needed to find one that had an active development community so the testbed would continue to be developed. This would insure that it would be useful in future testing and development.

Asterisk

Asterisk is an open source software implementation of a PBX. It supports the SIP protocol but also many others like IAX[3.1] and H.323. The wide protocol support and the many features are the main reasons for its popularity. This is visible from the large amount of community sites supporting and documenting Asterisk functionality.
[3.2]

sipX

Like Asterisk, sipX is also an open source software implementation of a PBX, but it's not a strict PBX solution. SipX is more of a native SIP server with PBX functionality. Some of the more advanced telephony features is therefore missing in the sipX distribution.
[3.3]

3.3.1 Hardware

In software SIP PBX solution the maximum number of users and concurrent calls is mainly limited by available CPU power and RAM capacity. But hard drive capacity is also important in systems supporting Voicemail. We would also recommend implementing a hard drive mirror solution (software/hardware RAID) to make sure that data and system settings is safe. To keep system stable and available we would recommend some sort of power backup solution.

3.3.1.1 Minimum Requirements:

- 1Ghz CPU
- 512 RAM
- 80GB Hard Drive (2x80GB)
- Ethernet card (10/100/1000 Mbit/s)

These requirements were defined by us for our Testbed solution. This was sent to HiA and Teleca when we requested the necessary equipment.

3.3.1.2 Two Servers donated by HiA:

- 2GHz P4 HT
- 1GB DDR2 RAM
- 2x80GB Hard Drive

- Gigabit Ethernet Card

3.3.1.3 Two Servers donated by Teleca:

- AMD Athlon(tm) 64 Processor 3000+
- 1GB DDR RAM
- 1x100GB Hard Drive
- 100Mbit Ethernet Card

3.3.2 Asterisk vs. sipX

Table 1 Asterisk vs. sipX

		Asterisk 1.2.7.1 from Digium	**sipX 3.0.1 from Pingtel**
Platform		Asterisk is primarily developed on GNU/Linux for x/86. It is known to compile and run on GNU/Linux, OpenBSD, FreeBSD, and Mac OS X Jaguar.	Pingtel's binary distribution of sipX runs on Red Hat Linux, and is compatible with most commercially available SIP-based IP phones.
Features	**Presence**	Asterisk provides limited SIP presence support. SIP subscriptions are used to show Online/Offline status. It’s limited in the way that you can’t see busy or away status. Presence with full functionality can be implemented in Asterisk with a third party IM services called Wildfire. The connection between these systems is a plug-in called Asterisk-IM.	SipX has support of presence. It’s clearly defined and is a separate module in the sipX architecture.
	IM	Asterisk support IM thru the Asterisk-IM project.	SipX has support of IM thru The reSIProcate Project.

	SIP proxy	Asterisk is not a SIP proxy. A SIP proxy handles call control on behalf of other user agents and usually does not maintain state during a call and therefore is never the endpoint of a call. Asterisk, as a server, is a SIP registrar and location server and also acts as a user agent endpoint (soft phone).	Natively built on standard SIP, sipX is a full SIP proxy with all the architectural advantages that entails.
	Protocols	Asterisk supports a wide array of different protocols: • IAX • H.323 • SIP • MGCP (Media Gateway Control Protocol) • SCCP (Skinny Client Control Protocol)	sipX basic free version supports SIP, but additional protocol support is available for paying customers.
Open Source		Asterisk is pure open source. No cost to download Asterisk software; support available from Digium for US$150 per hour.	Pingtel's SIPxchange has a more commercial flavour. It's still an open source product, the base PBX, sipX, can be downloaded from the SIPfoundry Web site for free, but if you pay Pingtel's modest price, you get additional support, plus plug-ins and tools such as media gateway services. $1,000 per CPU, including support and some commercial plug-ins; sipX software available as free download
Management		Configuration in Asterisk is text based. This is fast and effective, but requires more knowledge from staff.	SipX has a web based graphical management system that makes everyday jobs more user-friendly.

Scalability	The number of users in Asterisk is not defined, but is thought to be CPU bound.	The sipX system has clearly defined modules that can be split over different systems. This allows you to share the load over several servers. Sadly the only real CPU intensive task is that of the media server. And that can not be divided. And this is the part that limits active users on a system. Multiple CPU systems will increase this limit.
Community support	Asterisk has been around for a long time, and has enormous support from the open source community. It is the classical open source solution.	Despite the positive facts about sipX, the documentation and support seems lacking.
Installation	• Need extensive Linux knowledge to get the system up and running with source install. • No binary support • Maintainers of package based Linux systems like (apt and yum) make's is possible to install and update the system with one simple command. • Very good install documentation • Easy to add phones. Username and password is the only requirement.	• SipX has binary support for Fedora. • Maintainers of package based Linux systems like (apt and yum) make's is possible to install and update the system with one simple command. • Install documentation is limited • Hard to get the system fully functional. Dependent on DNS support. • Need MAC address in addition to username and password. If the phone doesn't support sipX security requirement, a special hash of the password will be required.

[3.4][3.5] [3.6] [3.7] [3.8] [3.9]

4 Implementation and Design of VoIP/SIP Enterprise Solution

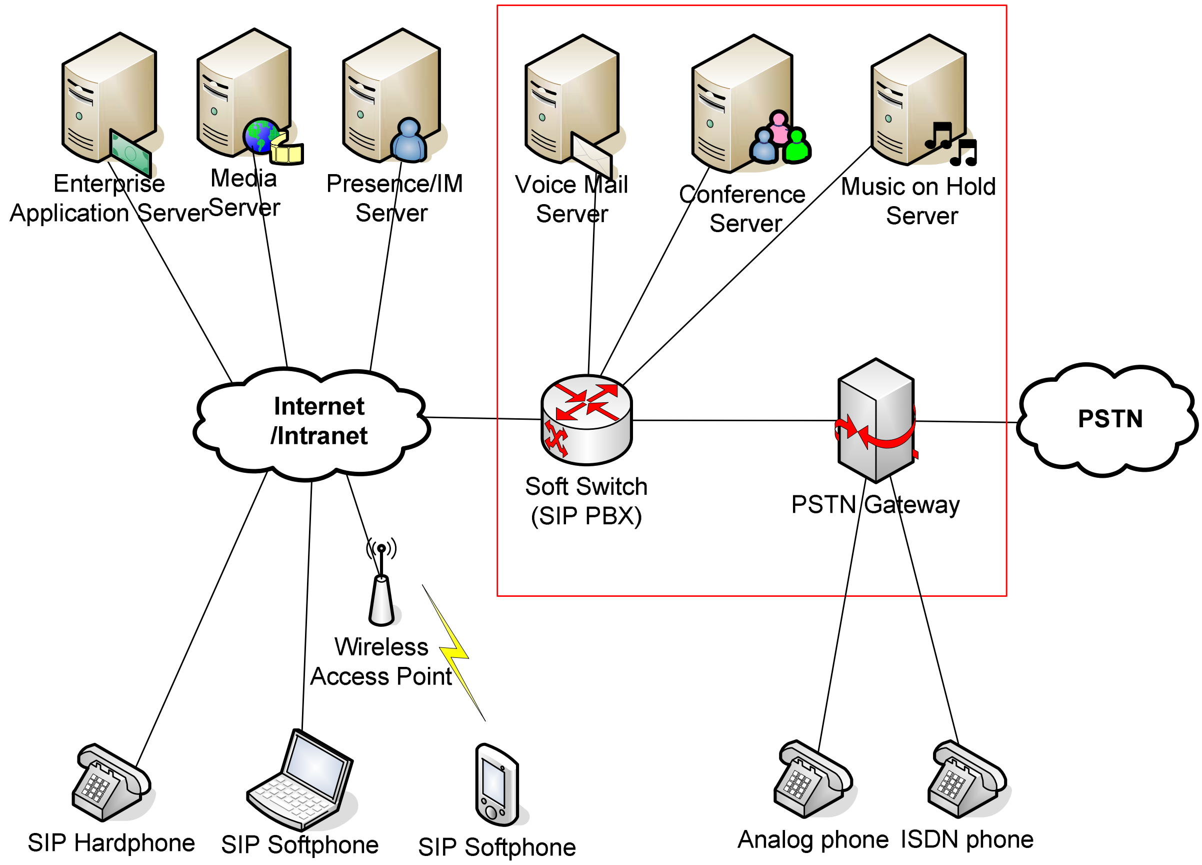
4.1 Purpose

Creating a state-of-the-Art research platform from scratch will give HiA and Teleca a common VOIP/SIP/IMS test-bed. The purpose is to build and develop competence in VOIP/SIP/IMS area and establishing an environment for development in future "All-IP" products and services. This task will be done by our master thesis.

4.2 Architecture

4.2.1 Logical Architecture

Basic logical architecture of our SIP testbed is shown in the figure below:



The key element is the soft switch, which is also known as a SIP PBX. It plays central role in the architecture. According to different session control requirements, it might be implemented as a combination of several SIP entities [RFC 3261], such as SIP registrar, proxy server, redirect server, forking server, Back-To-Back User Agent (B2BUA) [4.1] etc.

SIP clients consist of SIP hardphones and softphones on PC, PDA etc. They are connected to SIP PBX through Internet or Intranet.

Legacy non-IP phones, like analog phones or ISDN phones can be connected to SIP PBX through PSTN gateway. PSTN gateway links SIP PBX to PSTN network.

Enterprise application server, media Server, presence server are connected to the SIP PBX through Internet/Intranet. They provide respective services to SIP clients.

Remember that the figure is a logical architecture; these components can be deployed in different ways.
We are planning to put SIP PBX, voice mail server, conference server, music on hold server and PSTN gateway to same machine as the red square in the picture indicates. Due to economy reason, we will use a VOIP provider on Internet as PSTN gateway.

4.2.2 Security

Based on decisions made from evaluating VoIP/SIP enterprise solutions we found the initial structure for making successful calls inside the testbed. We had very little knowledge of the restrictions that was in place at each location and if it was possible to get around them without compromising the security.
The initial thought was that we would setup the equipment in an independent network area with no contact with other enterprise data equipment. At Teleca this was not possible and we had to make it work behind the existing firewall solution. Because of the active development at Teleca, there is very restrictive security layout. Initial testing with SIP was impossible.
We decided to try and make this work under the given circumstances. To make a SIP PBX work here would be a really hard task and a big learning experience.

This also means that we have to depend on the help of a lot of other members of the Teleca community, especially with the firewall. This will be time-consuming, but is a relevant problem in any enterprise situation.

4.3 Setup

First task was to install a Linux OS on the servers. Here we used Debian GNU/Linux 3.1 (r1) [http://www.debian.org/]. We installed software raid 1 on the servers which had two hard drives. Then we used the apt-get feature to bring all the software up to date. Debian uses three different definitions on how to update its software; Sarge, Etch and Sid. The names stand for stable, testing and development in the same order. To get access to the latest version of Asterisk we used Etch. This may sound risky, but Debian has a very high level off testing before software qualifies as stable. So in most cases it is very secure to use.

Apt-get was used to install Asterisk PBX also. We used Asterisk 1.2.4. The configuration files in Asterisk works as a how-to to explain all the possible

functions/options. We made our own limited version of these files; including only the functionality we required.
After exchanging the configuration files with our own we could run the servers.

Presence was implemented with the Wildfire IM v2.6.2 server from Jivesoftware [http://www.jivesoftware.org]. Presence clients along with configuration are explained in chapter 4.7.3.4.

Firewall/NAT and DHCP services were implemented with Smoothwall Express 2.0 [http://www.smoothwall.org/]. We will not go into detail about the firewall and NAT configuration as this can be dangerous to the security at each location.

We used clients with a dual install of both Linux and Windows. On the clients we used SJphone and Eyebeam Xten as soft phones. We also had two Grandstream GXP-2000 hard phones that we used as SIP clients.

We made contact with VoIP Company called Phonect which provides VoIP services mainly for enterprises. They gave us two free accounts that we could use to reach the PSTN.

Figure below shows that we have implemented an OpenSER [4.2][4.3] SIP Server. This is a very new SIP server solution that has hit a stable release in the last month of this project. We included this at a late stage in the project and haven't got a chance to do extensive testing on this distribution. The main problem with OpenSER is the documentation and overall ease of use.
But we have realized that it will be a major SIP server solution for the future. It can support 10 times the users as a similar Asterisk PBX setup and also have more of the complex SIP functionality that Asterisk lacks.

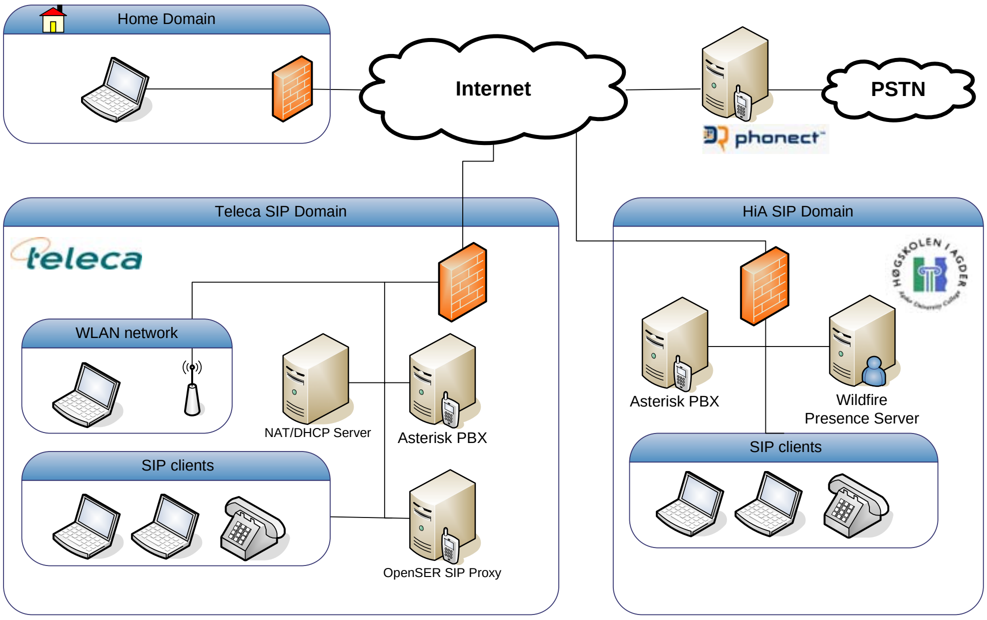


Figure 11 HiA/Teleca Testbed

4.4 Test Case Specification for SIP Test-bed

4.4.1 Introduction

To verify whether our testbed is fully functional and if it can handle different environments we need to test it. And a good way to test a SIP testbed is to see how it deals with factors that generally make SIP communication complicated.
Some of these factors are NAT, firewall and roaming.

And if we run into trouble we can try the techniques described in appendix E to work around it.

4.4.2 Environment

- Internet connection with a firewall solution that we can control.
- DHCP server with minimum 2 public IP addresses.
- Minimum 2 servers running Asterisk PBX with SIP signaling.
- Minimum 2 SIP Clients. Suggest use SJPhone as softphone and Grandstream GXP-2000 as hardphone.

4.4.3 Test tools

- Ethereal will be used to analyze SIP protocol.

4.4.4 Firewall/NAT Test Case

Test scenario:

1. UserA call userB
2. UserB answer.
3. UserA disconnect.

4.4.4.1 Single Domain

Description: Calling inside local area network.

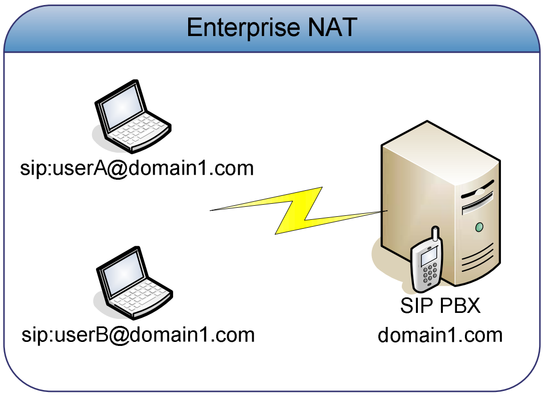


Figure 12 Single Domain

4.4.4.2 Dual Domain

Description: Calling behind NAT through local enterprise PBX.

Here we have a NAT environment protecting each domain. All the users will have a private address which makes point to point communication with SIP and RTP difficult.

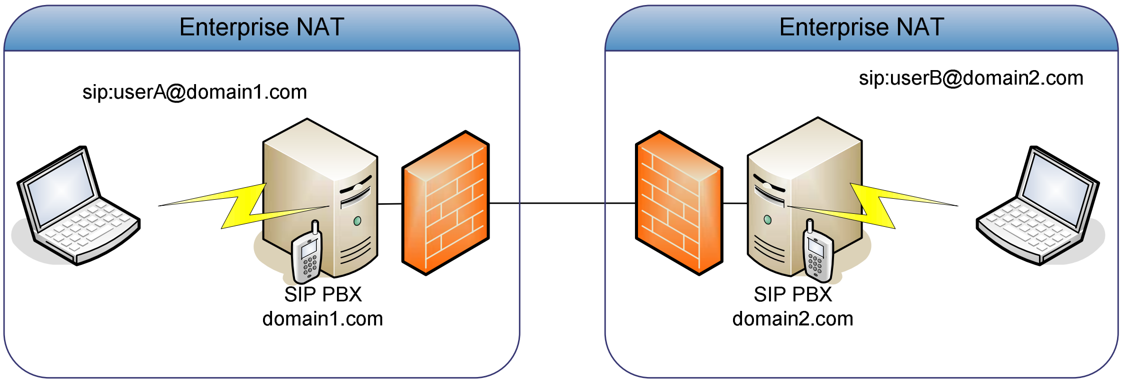


Figure 13 Dual Domain 1

4.4.4.3 Quadric-domain 1

Description: Calling between public computers through enterprise PBX

UserA and UserB is now located outside the enterprise network. But they will still connect to the enterprise VoIP PBX. More en more users work from home or another location outside of the normal office environment. But to be productive they may want to be available at the same telephone number and have access to their voicemail.

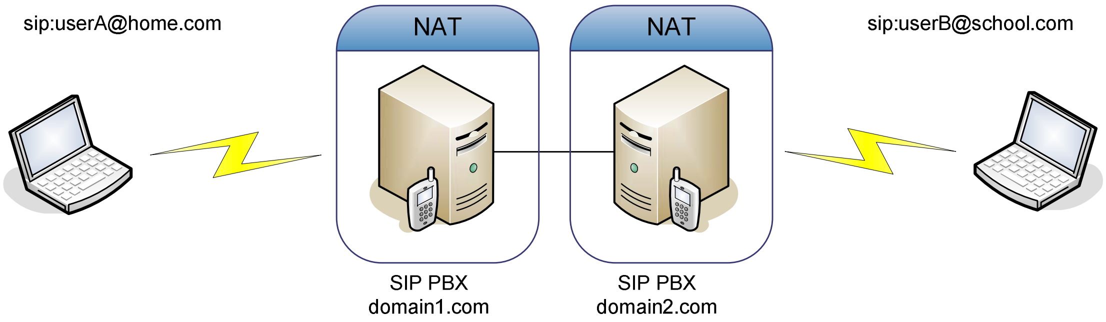


Figure 14 Quadric-domain 1

4.4.4.4 Quadric-domain 2

Description: Calling between different enterprise computers through other enterprise PBXs.

This is very similar to the previous example but now the users who are still working outside the enterprise network behind NAT as well. For every domain we now have a set of private and public addresses.

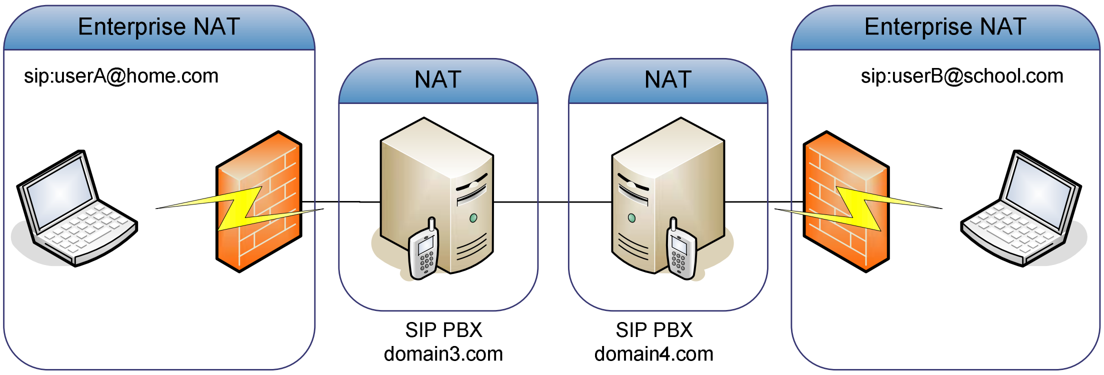


Figure 15 Quadric-domain 2

4.4.5 Roaming Test Case

Test scenario:

1. UserA turns off SIP phone
2. UserA change location and turns on SIP phone.
3. UserA registers to available SIP PBX

4.4.5.1 Access point roaming

Description: UserA is moving between different phone terminals connected to the same SIP PBX.

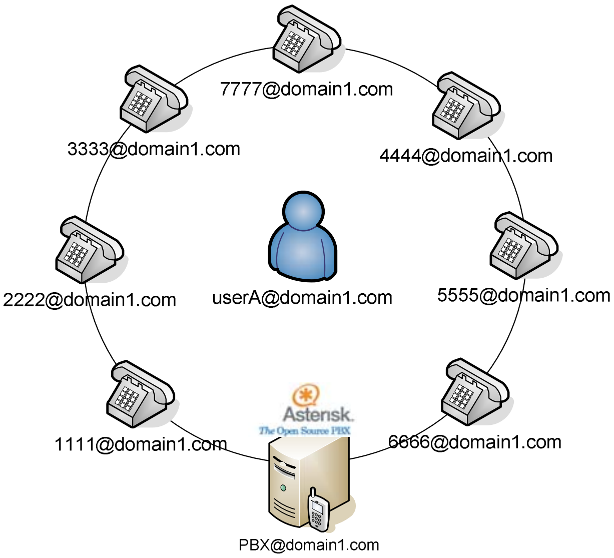


Figure 16 AP Roaming

4.4.5.2 Domain roaming

Description: UserA changes domain and SIP PBX. Because of this UserA will get a new SIP address. But UserA still want to be available on his normal SIP identity at domain.com.

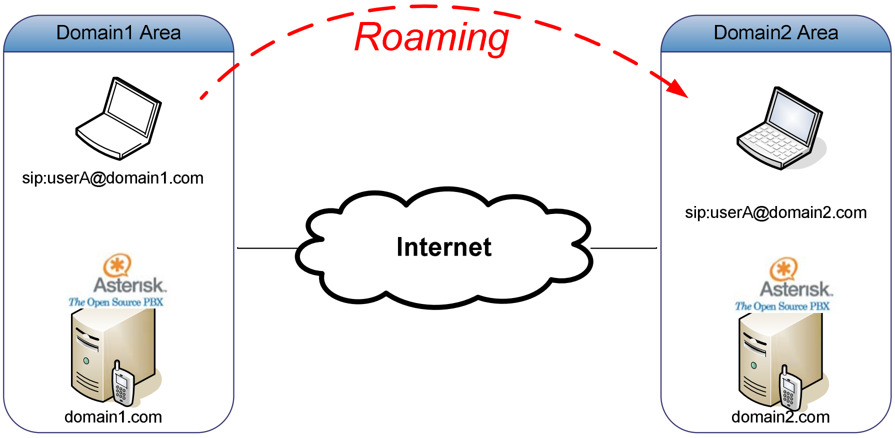


Figure 17 Domain Roaming

4.5 NAT Solutions

In this part of the document we will discuss the different methods of solving these problems. How can we make incoming calls easy, while keeping the overall security of the network?

These are the solutions we will discuss:

- Manual Configuration
- Universal Plug and Play (UPnP)
- Simple Traversal of UDP Through Network Address Translation devices (STUN)
- Traversal Using Relay NAT (TURN)
- Application Layer Gateway
- Tunnel Techniques

The technical overview of these different NAT traversal solutions is available in Appendix D.

4.5.1 Overview

Table 2 NAT Solutions

Manual configuration	+	Very simple in a single user environment. Need no special support from firewall, client or server.
	–	But in a large scale enterprise network this will mean a huge amount of work, so this is only suitable for very small networks.
UPnP	+	It is very easy to use and needs a small amount of knowledge to make it work. And this is the idea behind the software to. Not just for VoIP, but for a wide array of services to need to-way access in a NAT environment. This technology is heavily supported by Microsoft and a lot of other hardware vendors, so the availability of hardware/software that support this feature should not be a problem.
	–	But the security is; UPnP needs dynamic control over the firewall and that will be unacceptable by most enterprise administrators.
STUN	+	Very simple and stable solution supported by the majority of VoIP clients.
	–	STUN needs to be supported by the clients in the network. Will not work on Symmetric NAT which is very common in enterprise networks.

TURN	+	This fulfils the demands for symmetric NAT because there is no change in destination address.
	—	This will come at a high price for the provider of the TURN functionality since all the traffic will flow thru the TURN server. The TURN protocol hasn’t taken into consideration that service providers would like to change certain aspects of the SIP/SDP negotiation. QoS and Security is an example of specifications that are not revealed in the TURN protocol. Like STUN, TURN needs to be supported by the clients in the network. TURN is still an Internet draft.
ALG	+	ALG is an active part of the enterprise firewall that can filter the traffic based on signaling. It can investigate the contents of a packet and make a decision on a higher level than the basic accept/deny filters of a common firewall.
	—	This requires upgrading the software of your NAT/firewall or in a worst case scenario upgrading the hardware.
Tunnel	+	With this infrastructure there will be no violation of the firewall policy that we have discussed before.
	—	But the external server will be a good point of attack for anyone that wants to harm the system. If this server would be compromised the attackers will have an attack way straight into the internal network.

4.5.2 Single Domain

In a single domain we would normally have no restrictions like firewall or NAT. This should make normal calling scenarios very simple, and our testing shows the same.

No firewall or NAT traversal technology should be necessary.

4.5.3 Dual Domain

If the clients are allowed to make direct connections out of the network to other users, we may have to implement advanced firewall/NAT traversal technology. Each client will have to be available for outgoing and even more complicated, incoming calls. This forces the administrators to make compromises to enterprise firewall.

A good workaround is to let the SIP PBX handle all the communication. All traffic (both SIP and RTP) in and out of the NAT will pass through the server. This will keep the confusion about which client the traffic is headed to a minimum.

But the SIP PBX still have a private address and will need to traverse both the firewall and NAT to get to the public internet. This will be very easy if you use the PBX as a strict outbound proxy. A simple firewall that redirects of all the SIP traffic into the SIP PBX will accomplish this with ease.

4.5.4 Quadric-domain 1

Allowing users working from a location outside the enterprise is a tricky situation. The users are directly connected to the public network without NAT restrictions. This will make point to point RTP communication easier. So allowing only SIP communication into the enterprise is possible. The SIP protocol will exchange RTP information among the users. This will save the enterprise bandwidth as well.

4.5.5 Quadric-domain 2

This is similar to Quadric-domain 1, but now the users are behind NAT as well.

Many enterprises use a tunnel into the enterprise to get access to office resources like mail and files stores on company servers. This could be used to get access to the SIP PBX also. This could be implemented in many ways, but the most common is to give access to all resources (Virtual Private Network). With this solution you have access to everything you normally would if you were working inside the enterprise. The client should therefore have very strict security. A good idea is to map the specific hardware (Ethernet card) to the username allowed to use tunnel. From a VoIP point-of-view allowing a client access to all resources seems like overkill. So if the users only need access to phone resources this should be specified.

4.6 Roaming Solutions

4.6.1 Access Point Roaming

4.6.1.1 Agent Mobility

Agent Mobility occurs when you use different phones, that all are connected to the same SIP PBX. This is the simplest form of roaming, and if we look at how we described roaming in the theory chapter, one could argue that it isn't a roaming scenario at all.

Example: The Call center situation; the people working at the call center have no permanent seating situation. So they are forced to work at different locations each day.

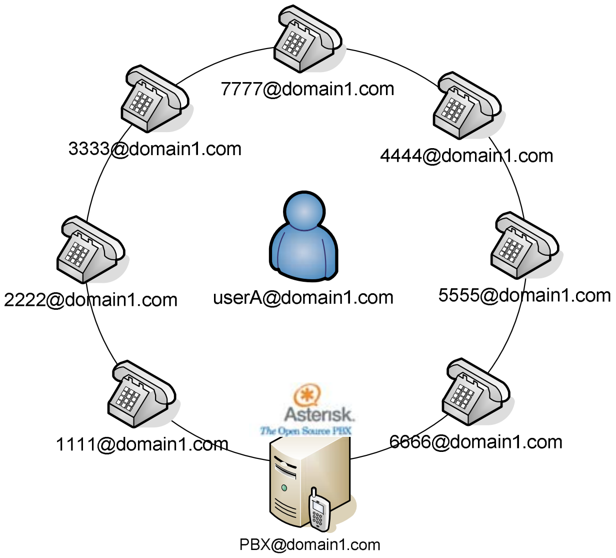


Figure 18 Agent Mobility

We have a predefined network with multiple static nodes connected to the PBX. Each phone has a static address where it can be reached. The user can move from phone to phone and use his roaming identity/address on the node he is currently using.

Example: The user at the call center starts his shift and is assigned a phone for the day. The phone has the address 3333@domain1.com. The user has a roaming identity; userA@domain1.com. He can then use his assigned phone to register his roaming identity with the static phone address. Calls arriving at userA@domain1.com will be redirected to 3333@domain1.com.

4.6.2 External Domain Mobility

In chapter one we talked about that the idea of a static workplace was changing. People will always be on the move, contacting partners or business customers. But we still need to be available.

What if we had a public user id/address that everyone that needs to get in touch with us knows? It could be printed on our business card or on your webpage. Let's call that address userA@public.com. We also have a laptop (userA@laptop.com), cell phone (userA@cell_phone.com), PDA (userA@pda.com) and an office phone (userA@office.com). Any call to the public user ID should be directed to the device we are currently using.

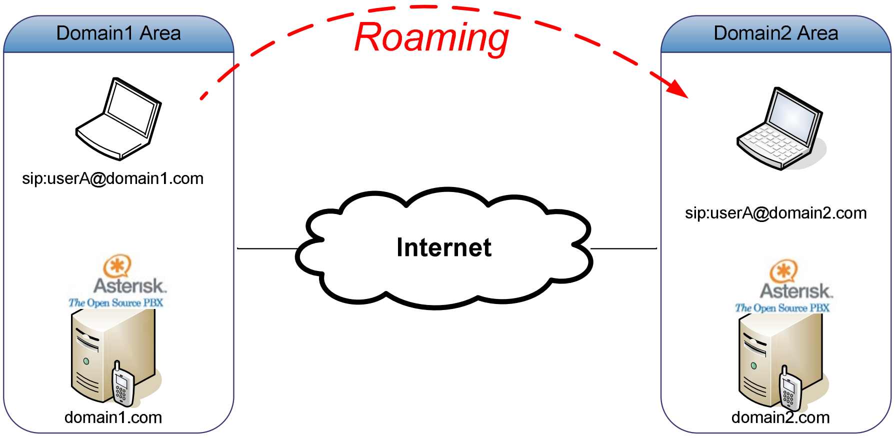


Figure 19 Domain Roaming

4.6.2.1 Client Initiated - Multiple Register

When the user is logged on in the office environment he has access to voicemail and private extensions (short telephone numbers that are valid in office environment) to his fellow workers. When a user has grown accustomed to these functions he may want to use the same functionality at home or at the internet cafe. This can be accomplished by allowing the user access to the Office PBX from the outside.

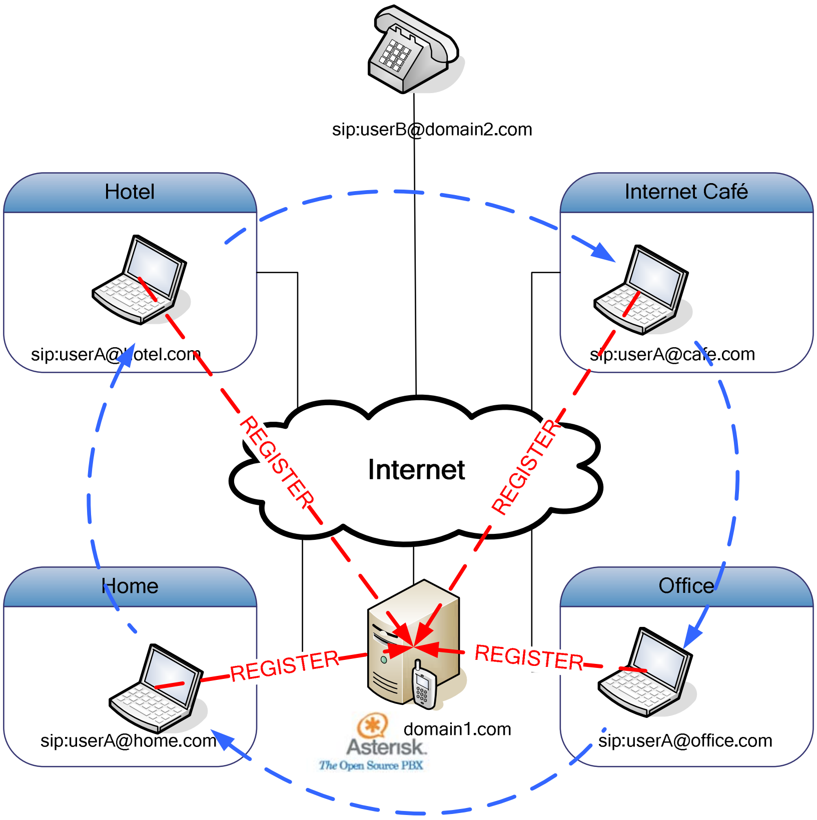


Figure 20 Access Point Roaming

4.6.2.2 Proxy Server

UserA moves from Teleca domain to HiA domain. UserA registers with Teleca proxy server and gives the new address where further contact should be directed. All calls to userA@teleca.no will be forwarded thru the Teleca proxy server to HiA proxy server. [4.4] [4.5]

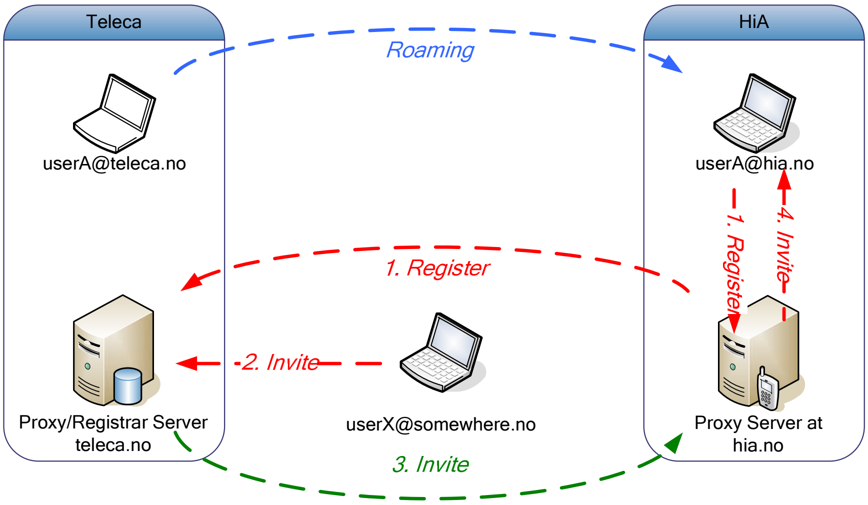


Figure 21 Proxy Scenario

4.6.2.3 Redirect Server

In some architecture's it may be desirable to reduce the processing load on proxy servers that are responsible for routing requests, and improve signaling path robustness, by relying on redirection.

UserA moves from Teleca domain to HiA domain. UserA registers with Teleca redirect server and gives the new address where further contact should be directed. A call arrives at Teleca domain, the redirect server will inform the caller of userA's new location and userX will make a new INVITE request to the given domain (HiA). [4.4] [4.5]

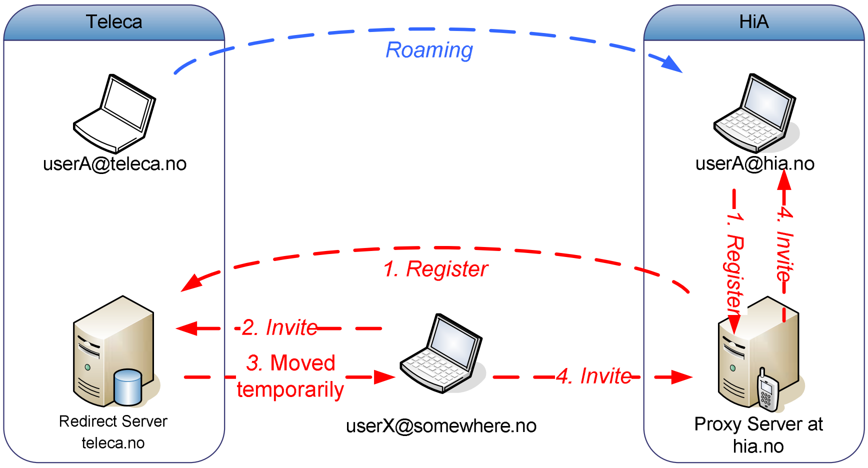


Figure 22 Redirect Scenario

4.6.2.4 Forking Proxy Server

A forking proxy will initiate calls to all the registered URI's. This is one of the simplest ways of finding the active user when there are several registered domains for a URI. The calls can be initiated in parallel or in sequence. [4.4] [4.5]

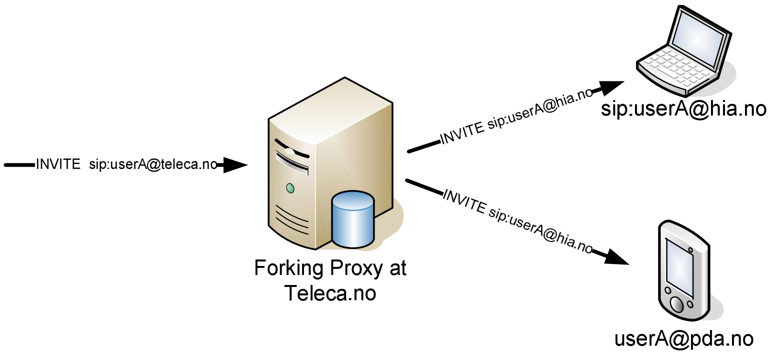


Figure 23 Forking Proxy Server

UserA is registered with userA@pda.no and userA@hia.no. He is moving around in an office environment. When a call arrives at userA@teleca.no both URI's will be invited to the call. UserA is currently at his laptop and accepts the call on userA@hia.no. The call will be accepted on userA@hia.no and dropped on userA@pda.no.

4.6.2.5 Presence Server

Requirement: Teleca must be able to read HiA presence status for this user.

UserA logs on the visited domain (HiA). The presence server at the visited domain will then be updated with the user's current status and location. When a call arrives at home domain (Teleca), the proxy/redirect server will check the user's status as reported by the presence server. This status will tell the proxy/redirect server where the user is located, and if he is available (busy, away or at lunch). From this information the server could decide to not forward the call. This will give the user more privacy in the case that he doesn't want to give away his current location or if he isn't available for a call.

The green line shows how the call will be forwarded if the Teleca domain uses a proxy server instead of a redirect server.

This solution will be thoroughly discussed in the IMS chapter.

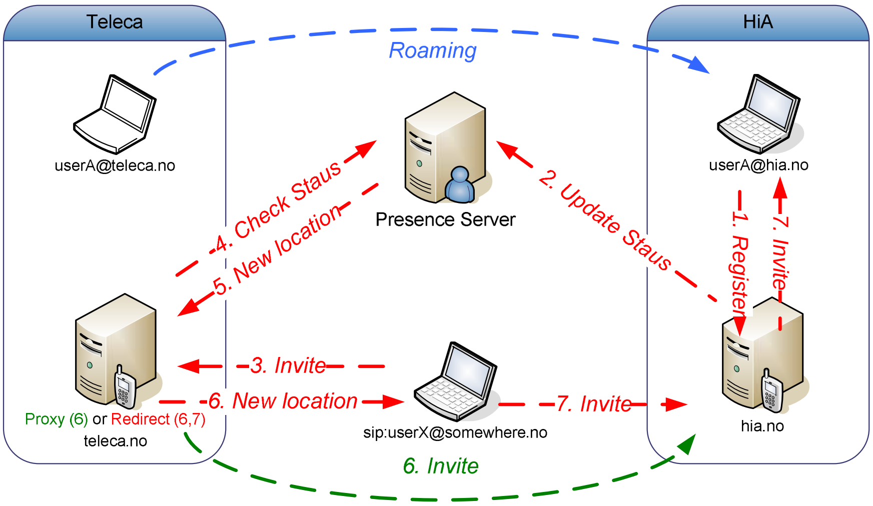


Figure 24 Presence Server Scenario

4.7 Enhancements

4.7.1 Multiple servers to link sub-domains

Large enterprises may have sub departments in different locations; they could even be in different countries. Administrators may want to use dedicated VoIP servers at each location to handle the communication. There are several reasons for this:

- To avoid delay of internet and achieve better VoIP performance.
- Avoid overloading the SIP PBX, by dividing the user database over several servers.
- To achieve roaming between different SIP PBX domain.

Multiple server issues should be taken into consideration while making VoIP/SIP solutions for enterprises. This project will discuss how to interconnect two Asterisk servers.

4.7.2 TAPI

The purpose of the TAPI interface is to interconnect your mail client with your telephone. Many people use the Outlook address book to store their contact information. So the normal process would be to look up the information and dial the telephone number on your telephone. But what if we could interconnect the address book with the telephone? This is exactly what the TAPI driver does.
With the TAPI function installed you can send the call information directly to your telephone. When you pick up the telephone the call will be transferred.

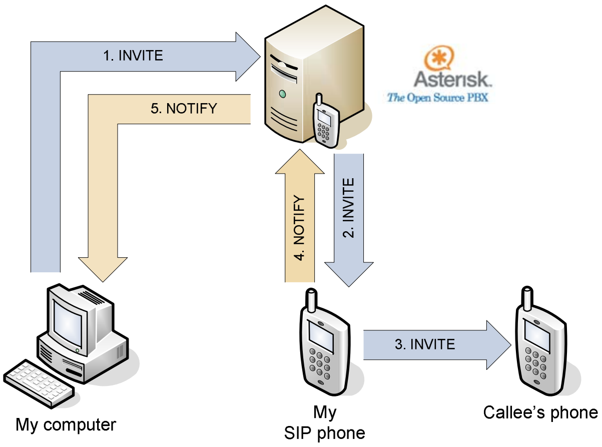


Figure 25 TAPI

4.7.3 Presence and Instant Messaging

VoIP is in many cases not sufficient in a complete communication layout for an enterprise. Presence information and instant messaging are great tools for availability and exchange of information.
We will first evaluate support for Presence and IM in our chosen SIP PBX; Asterisk. Next we will study other ways of implementing this onto exciting VoIP implementation using Asterisk.

4.7.3.1 Current Presence Support in Asterisk:

Till now (May 2006) there are no clients that will show complete presence information for Asterisk users. And this is simply because Asterisk doesn't support this to a full extent. But it provides some support of SIP presence as defined in RFC 3856 [4.5][4.6].
Asterisk does not currently support "publish" method for publishing presence documents in Presence Information Data Format (PIDF) defined in RFC 3863[4.7], but it can generate "notify" to "subscribe" users when "register" occurs and also when the client disconnects.
Due to the lack of "publish" method support, there's no support of extended states (Away, Do not disturb, Busy). You can subscribe to extension state for any channel that supports device state notification. In order to fix this, we need a user abstraction in Asterisk, something that will be worked on in development version 1.3.

4.7.3.2 Phones known to work with SIP Presence in Asterisk

- Snom (various models)
- Polycom IP30x/IP50x/IP600
- Xten EyeBeam (softphone)
- Grandstream GXP2000 (Firmware >= 1.0.1.13)
- Aastra 480i
- Aastra 9133i

All of the listed phones above are hardphones except for the Xten Eyebeam. A hardphone is not the ideal way of using presence and IM together. Consider these scenarios:

- Overview of online/busy users
- Sending quick messages to specific users/groups

It's not hard to realize that an IM/Presence solution is best controlled from the desktop of your computer. And if you want to transfer or setup a call to your hardphone this can be controlled from the computer too.

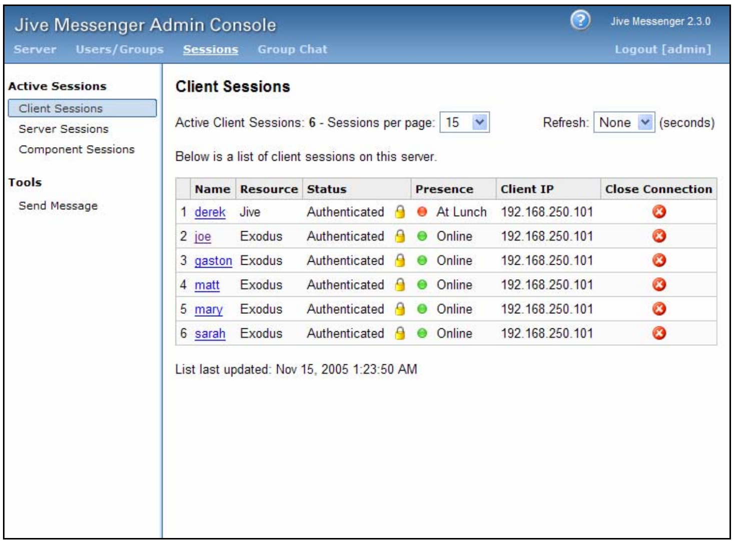
4.7.3.3 Current Instant messaging support in Asterisk:

Asterisk has no support for instant messaging in their current development. It exists ways to get it working with third party patches to the Asterisk source code. But this involves recompiling of the Asterisk source code. This method is very complicated and not a recommended way of maintaining your PBX. It may also cause potential problems with further upgrades.

4.7.3.4 Wildfire / Spark / Asterisk-IM

In Xten Eyebeam the client controls much of the functionality and it is quite complex. Many system operators would prefer a solution where the clients are connected to a separate server that they can control all functions that are available to the users.

Wildfire (The figures in this section are from wildfire.org.)
Wildfire is a standalone open source IM server which also can be bought with commercial support. It uses the only widely adopted open protocol for instant messaging; XMPP (also called Jabber). It features SSL/TLS encryption and is controlled with a built in web server functionality. It is built on java and supports Windows, Unix/Linux, and Mac OSX.



Client Sessions

Active Client Sessions: 6 - Sessions per page: 15   Refresh: None (seconds)

Below is a list of client sessions on this server.

	Name	Resource	Status	Presence	Client IP	Close Connection
1	derek	Jive	Authenticated	● At Lunch	192.168.250.101	✕
2	joe	Exodus	Authenticated	● Online	192.168.250.101	✕
3	gaston	Exodus	Authenticated	● Online	192.168.250.101	✕
4	matt	Exodus	Authenticated	● Online	192.168.250.101	✕
5	mary	Exodus	Authenticated	● Online	192.168.250.101	✕
6	sarah	Exodus	Authenticated	● Online	192.168.250.101	✕

List last updated: Nov 15, 2005 1:23:50 AM

Figure 26 Wildfire Admin Console

Spark
Spark is a free, cross-platform IM client. It features built-in support for group chat, telephony integration, and strong security. It also offers an end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations.

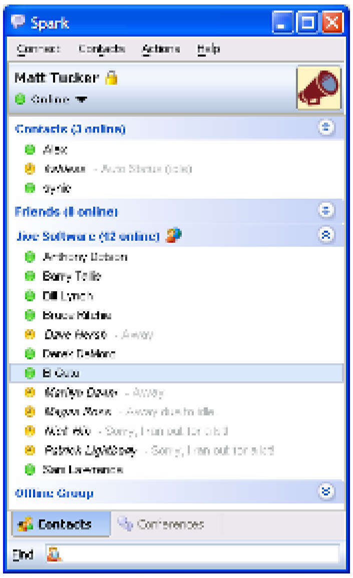


Figure 27 Spark IM Client

Asterisk-IM

Asterisk-IM is one of the many available plug-in's for the Wildfire server. The purpose of this plug-in is to integrate Asterisk with Wildfire and exchange information between them. With this plug-in installed the Asterisk users can be mapped with the Wildfire users. And Wildfire will receive events from Asterisk about the status of users and incoming calls. It is also possible to initiate a call to a user via the spark IM client thru the Asterisk PBX.

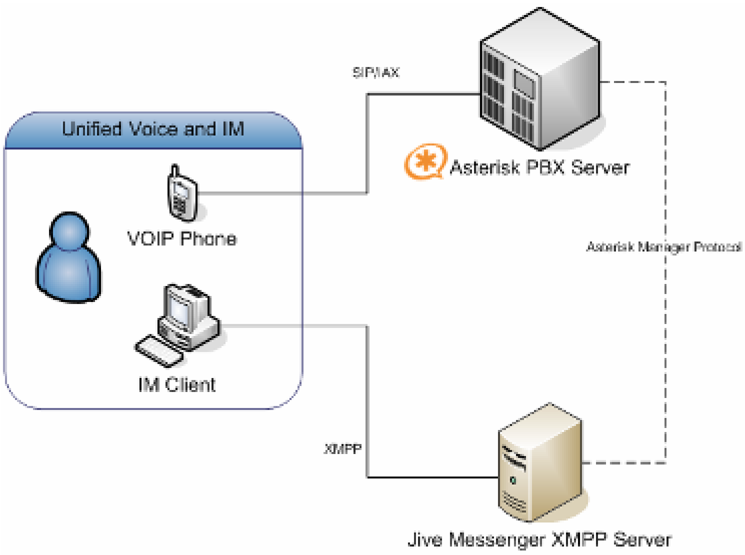


Figure 28 Asterisk-IM Architecture

Spark-Manager

Spark Manager is another plug-in for Wildfire. With this you can control the distribution and configuration of the spark clients on your network. Administrators use the web-based admin console to configure which Spark client version they wish to activate. Then, the next time users log in they will be notified to upgrade.

4.7.4 Conference and Video Support

It is no doubt that audio/video conferences brings great convenience for enterprise users and reduce traveling costs. We chose to use Asterisk own simple conferencing functionality. By using 'MeetMe' application, multiple callers can meet in a virtual conference room and communicate with all other callers.

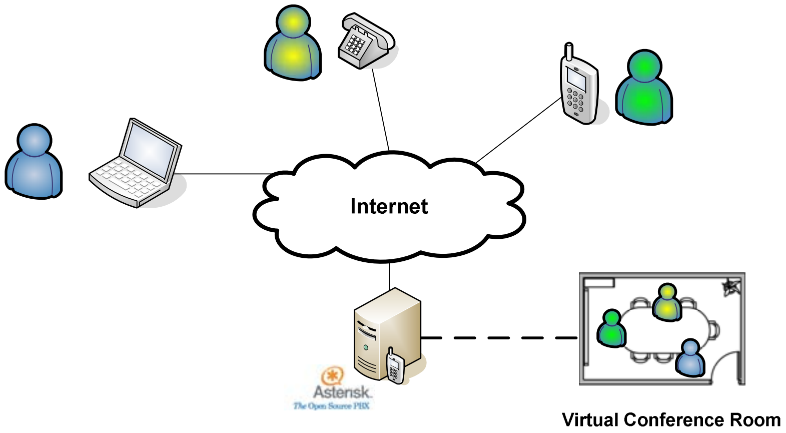


Figure 29 Conference enhancement

By enabling Asterisk video support, we can see each other when we talking. The SIP videophone we use is Xten eyeBeam softphone. See Figure 9 in chapter 3.2.1. It makes it possible for enterprises to have a video conferences.

4.8 Results:

Our second and probably most time-consuming project was to setup a complete SIP/VoIP testbed.

We choose a variety of equipment and software based on our research and implemented them as we saw fit. We worked around the security architecture at each location with help from NAT/firewall traversal tools.

Our testbed implementation consisted of these parts:
SIP PBX: Asterisk 1.2.4 from Digium
Alternative SIP Server: openSER v1.0.1
NAT/DHCP Server: Smoothwall Express 2.0
SIP Hardphone: Grandstream GXP-2000
SIP Softphone:

- Xten EyeBeam v1.1.3006 from Countherpath
- SJphone 1.60.289a from SJlabs

Presence Server: Wildfire IM v2.6.2 server
Presence Client: Spark IM Clients v1.1.4

Our Teleca/HiA testbed primarily consists of an Asterisk PBX at each location. They are both interconnected and can call defined private users with private short number extensions. The clients and servers can be moved in and out of NAT and firewall protection to test their performance in each case.

The company's existing internet connection was used for all testing with delay. The voice quality was well within what you would expect from a normal circuit switched PBX and PSTN provider. We also used our home domain to test NAT, firewall and roaming.

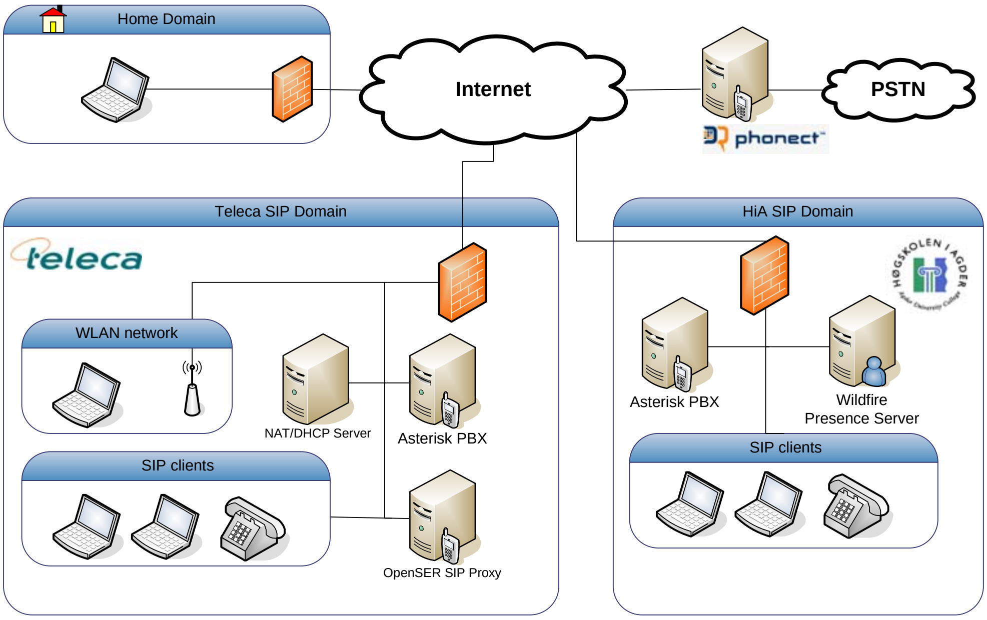


Figure 30 HiA/Teleca Testbed

4.8.1 Firewall/NAT Solutions

We have explained and evaluated many of the possible solutions and given a summary of what each solution has to offer.
Manual configuration will be to time consuming, and UPnP will not be acceptable in a large enterprise environment. STUN has major difficulties with the most common enterprise NAT systems and requires support from the clients. ALG and Tunnel is the best solutions when it comes to preserving firewall security and allowing incoming calls, but they are also the most complex. TURN is less complex and will work an all types of NAT, but is still on the drawing board and has fewer options for a service provider. There is no clear winner in this discussion. There are many different types of enterprises and each will need a different solution.
Our solution used a combination of STUN and TCP/UDP tunneling to get the testbed working. A more detailed overview of the different NAT traversal technologies can be found in Appendix D.

4.8.2 Roaming Solutions

The Roaming chapter (4.6) proposed multiple ways for an enterprise to make their public identities accessible from different locations. They were divided them into two categories; Access Point Roaming and External Domain Mobility.

Access Point Roaming is a useful tool in enterprise that has users moving around inside the enterprise domain, while External Domain Mobility is useful outside the enterprise domain. We have proposed multiple solutions and have tested everyone except for the presence solution.

4.8.3 Enhancements

4.8.3.1 Multiple Servers to link sub-domains

Multiple linked SIP PBX servers was tested and successfully implemented in our testbed. This was a representation of a multi-department enterprise scenario. Private extensions and short numbers were used to call from Teleca to HiA and vice versa. Centralized Voicemail handling and roaming users was also one of the successful results of this implementation.
Appendix A will show a detailed explanation of how you achieve dual server communication in Asterisk.

4.8.3.2 TAPI

We proposed a solution with TAPI that will greatly simplify the daily work of anyone that uses a telephone. Almost everyone today needs to use an electronic address book of some sort. With the TAPI driver you can transfer the numbers from your screen directly to your telephone. The TAPI driver was implemented in our VoIP solution and tested with Microsoft Office. Demonstration showed that this worked very well. How-to configure a TAPI solution is shown in appendix B.

4.8.3.3 Presence and instant messaging

The presence functionality in Asterisk PBX is limited and the Instant Messaging is non-existent. This was a concern in the initial SIP PBX research, but Asterisk had too many other positive factors that we couldn't ignore.
Presence and IM functionality was therefore incorporated into the Asterisk PBX with use of 3-party software.

Wildfire / Spark / Asterisk-IM:
With help from the Asterisk-IM interface we combined the Wildfire IM server with the Asterisk PBX. This gave us a complete Presence/IM solution with call support. The solution is controlled with a simple and highly configurable web interface. The administrators also have the ability to remotely upgrade and configure the Spark Clients. All these functions are incorporated and tested in our SIP solution.

In appendix C we have described in detail how to configure a working Wildfire server in Debian.

4.8.3.4 Conference and video support

We have successfully configured Asterisk PBX to support conference and video calls. These enhanced functionalities have been demonstrated on out test-bed.

The basic configuration of conference is quite simple. For example, the virtual conference room number is 101, and phone number for accessing this conference room is 2999. Two asterisk configuration files should be changed.

- "conf => 101" is added to meetme.conf.
- "extern =>2999,1, MeetMe(101)" is added to extensions.conf.

More advanced setting for MeetMe application can be found in Asterisk handbook from Digium [4.9].

To turn on video support, we add three lines in asterisk SIP configuration file sip.conf.

- "allow=h263" is added to enable video codec
- "allow=h263p" enables another advanced video codec
- "videosupport=yes" enables support for SIP video

5 Migration towards IMS

5.1 Overview

As we mentioned in chapter 2.1.5, IMS is a new architecture to provide multimedia services based on open standards of the Internet Protocol. The idea behind IMS is to offer Internet services everywhere and at anytime by using multiple access technologies. [5.3] But any 2G/3G cellular user can access internet by using a data connection. This is especially true for 3G, which high data rate makes the cellular users enjoy all the services of the internet. Furthermore, almost all IMS services can be accomplished without IMS. So why do we need it?

After the literature review [5.2][5.4] etc, we will summarize the answers below:

1) **QoS(Quality of Services)**
QoS means that the network offers guarantees about the amount of bandwidth a user gets for a particular connection or the delay the packets experience. This is key component of IMS, which packet switched domains are missing.

2) Charging of multimedia services
IMS makes it possible to charge multimedia sessions appropriately. IMS does not mandate any particular business model, but let operators decide how to charge.

3) Integration of different services
Without IMS, service creation can be complex and expensive for the operator and the user. The key is integrating different services (e.g., multimedia, presence, instant messaging, web browsing, location, personalized services) within a single technology.

4) Security
Fixed network today don’t have the security that is implemented in mobile networks. IMS will resolve these problems in a common way by introducing authentication with ISIM (IP multimedia Services Identity Module).

5) Standardized Interface
The benefit of standardized interface is openness and interoperability. IMS architecture defines standardized interfaces to link a collection of functions. Common components, such as call control and configuration storage, make it possible to reuse the existing infrastructure and reduce repeating work while developing new services. Therefore less development work is needed, and new services can be rolled out to market faster and cheaper than before. [5.7]

6) Fixed-mobile convergence (FMC)
IMS is independent of the underlying media transport, so that the same IMS-based application services will be available for both fixed-line and mobile networks. I.e. subscribers can use the same service with all of their different access devices.

These are the major differences between IMS and non-IMS.

It seems that IMS is the promising new architecture that fulfills all of our needs, then why do we need an IMS migration solution?
It is no doubt that IMS will play a key role in the future All-IP infrastructure, but it is still in the development stage. It should be pointed out that it takes time for all 3G mobile networks to upgrade to 3GPP Release 5 network and same for fixed network to migrate from PSTN to IMS based NGN. It will take several years before the full IMS functionality is realized. So IMS solution for enterprises can't be implemented yet.
Enterprises don't have the patience to wait for IMS; they want to get the benefits of VoIP now. Some enterprises have already started to use SIP VoIP soft-switch solutions. So how can we make a VoIP solution that works now and that can be easily and efficiently migrated to a complete IMS solution in the future?

5.2 IMS architecture

5.2.1 IMS Architecture Overview

To achieve greater flexibility, IMS has a layered architecture.[5.1] Figure below provides a simple representation of IMS architecture in three layers. The middle IMS signaling layer is used to separate the top services/application layer from the bottom transport layer. The layered approach helps introducing new access networks into existing IMS architecture. Three User Equipments (UEs) representing different 3GPP release are shown in the figure below. Now IMS is not just for cellular access (3GPP R5), but will also support WLAN (3GPP R6), fixed line (3GPP R7).

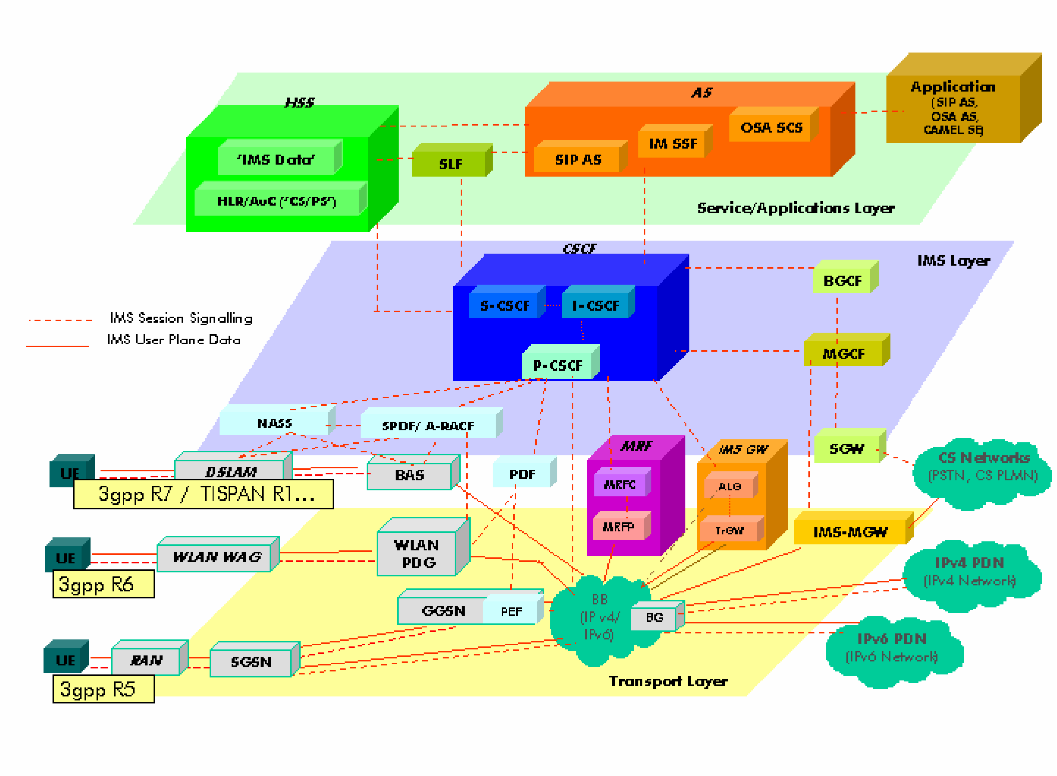


Figure 31 Overview IMS architecture

[5.1]

From the figure, we can see the database (HSS, SLF), essential node for Session management and routing (CSCF), Interworking elements (BGCF, MGCF, MGW, SGW), and services related nodes (Application Server, MRFC, MRFP). Now we can take a close look at each layer.[5.3] [TS 23.228]

1) **Transport Layer**
   Through the Transport Layer, end users connect to the IMS infrastructure by using some form of User Equipment (UE), e.g.3G wireless handset, WiFi-enabled PDA, or a broadband connection. UEs can be an IMS enabled device or non-IMS device which interfaces with the IMS infrastructure through a gateway.
   There are several types of gateways defined within the IMS that provide non-IMS terminals access to the IMS domain or inter-working between the PSTN and the IMS. Here are some key elements in Transport layer:
   - **BG (Breakout Gateway)**
     A BGCF (Breakout Gateway Control Function) is a SIP server that includes routing functionality based on telephone numbers. It's only used when calling from the IMS to a phone in a circuit switched network, such as the PSTN or the PLMN.
   - **MRFP (Media Resource Function Processor)**
     MRFP is a part of **MRF (Media Resource Function)**. MRF provides a source of media in the home network.It devided into MRFP which are media layer node and MRFC (Media Resource Function Controller) which are signaling node. An MRFP implements all media-related functions.
   - **MGW (Media gateway)**
     The MGW interfaces with the media plane of the PSTN or CS network, by converting between RTP and PCM. It can also transcode when the codec’s don't match (e.g. IMS might use AMR, PSTN might use G.711).
2) **IMS Layer**
   The IMS layer is also known as a control/signaling layer which comprises network control servers for managing call or session set-up, modification and release.
   - **CSCF(Call Session Control Function)**
     CSCF plays a central role in the session control and uses the SIP protocol for call control. There are three types of CSCF, known as P(Proxy)-CSCF, I(Interrogating)-CSCF and S(Serving)-CSCF.
     P-CSCF is a SIP proxy that is the first point of contact for the IMS terminal. It handles all of the SIP signaling requests to/from the end-user and forwards them as appropriate.
     I-CSCF provides location services for when a message or service must traverse multiple IMS domains.
     S-CSCF The S-CSCF (Serving) routes the SIP signaling to and from subscribers via Application Servers, according to the service profile information held for each subscriber in the Home Subscriber Server (HSS).
   - **HSS(Home Subscriber Server)**

The HSS is a centralized database that stores user-related information, such as home network location, security information, and user profile information.

- **SLF(Subscriber Location Function)**
  SLF is a database that maps users' addresses to HSSs. IMS networks more than one HSS need an SLF.
- **BGCF(Breakout Gateway Control Function)**
  A BGCF is a SIP server that includes routing functionality based on telephone numbers. BGCF is invoked when a session needs to exit the IMS domain and enter the PSTN or Circuit Switched network.
- **SGW (Signaling Gateway)**
  Interfaces with the signaling plane of the CS(circuit switched) network. It transforms lower layer protocols as SCTP (which is an IP protocol) into MTP (which is a SS7 protocol), to pass ISUP from the MGCF to the CS network.
- **MGCF (Media Gateway Control Function)**
  MGCF does call control protocol conversion between SIP and ISUP, and interfaces with the SGW over SCTP. It also controls the resources in an MGW with a H.248 interface.
- **MRFC (Media Resource Function Controller)**
  MRFC is a part of MFR, acts as a SIP User Agent to the S-CSCF, controls the MRFP with a H.248 interface

3) **Service/Application Layer**
The application layer comprises application and content servers to execute value-added services for the user.
Application servers (AS) host and execute services, and interfaces with the S-CSCF using SIP. This allows third party providers an easy integration and deployment of their value added services to the IMS infrastructure. Depending on the service the AS can act as a SIP Proxy, SIP User Agent, SIP Back-to-Back User Agent. There are several different types of AS:

- SIP AS : native IMS application server
- OSA-SCS : an Open Service Access - Service Capability Server interfaces with OSA Application Servers using Parlay
- IM-SSF : an IP Multimedia Service Switching Function interfaces with CAMEL Application Servers using CAP

5.2.2 Protocols in IMS

IMS have chosen SIP as session control protocol. SIP is a text based protocol and is very similar to HTTP. It is easy to program compared to mobile network protocols and widely used in the internet. It also enables convergence of fixed and mobile internet, and can be used to implement all types of peer-to-peer applications.

AAA protocol, short for Authentication, Authorization and Accounting protocol, is widely used on IP network to provide the required protection and access control. IMS uses Diameter [RFC 3588] which is en evolution of RADIUS [RFC 2865].

RTP (Real-time Transport Protocol) and RTCP (Real-time Transport Control Protocol) are used to transport real-time media; such as video and audio. All protocols in IMS are adopted from Internet standards (IETF).

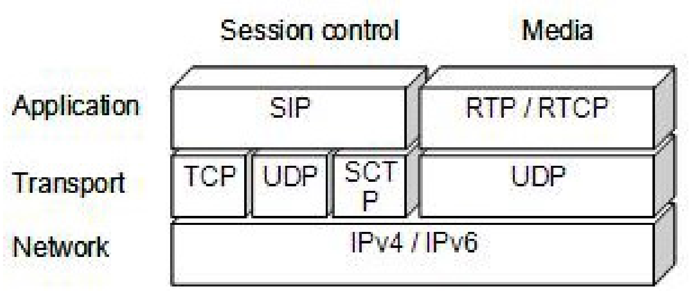


Figure 32 Protocols used in IMS

5.2.3 Identifications in IMS

5.2.3.1 Public User Identities

Each IMS user has one or several public identities, which are used to route SIP signaling. The format will be a SIP URI (as defined in RFC3261,e.g. sip:lian@teleca.no), or a TEL URI (as defined in RFC3966,e.g. tel:+471234567). Public User Identities are allocated to the IMS subscriber by home operator.

5.2.3.2 Private User Identities

Each IMS user has one or several private identities which are not known to other users, and used for subscription identification and authentication. It uses a NAI(Network Access Identifier, as defined in RFC2486) format , like username@operator.com.

In 3GPP R5, an IMS subscriber is assigned one Private User Identity and a number of Public User Identity, as shown in following figure.

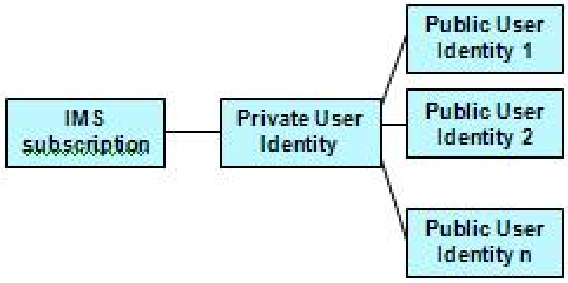


Figure 33 IMS user identity

Considering one user may have different smart cards in different IMS terminals, in 3GPP R6 an IMS subscriber may have a number of private user Identities.

5.3 Future IMS solution vision

IMS aims to provide ubiquitous cellular access to all the services that Internet provides. It seems that introducing IMS domain will solve the problem how to integrate mobile phone to overall enterprise communications solutions.
With mobile integration based on IMS, users can enjoy the flexibility and "take their office with them" anywhere.

Because of the complexity of a core IMS network implementation, most enterprises will use IMS solutions provided by a telecom operator.
Below is a possible IMS solution for enterprises in the future:

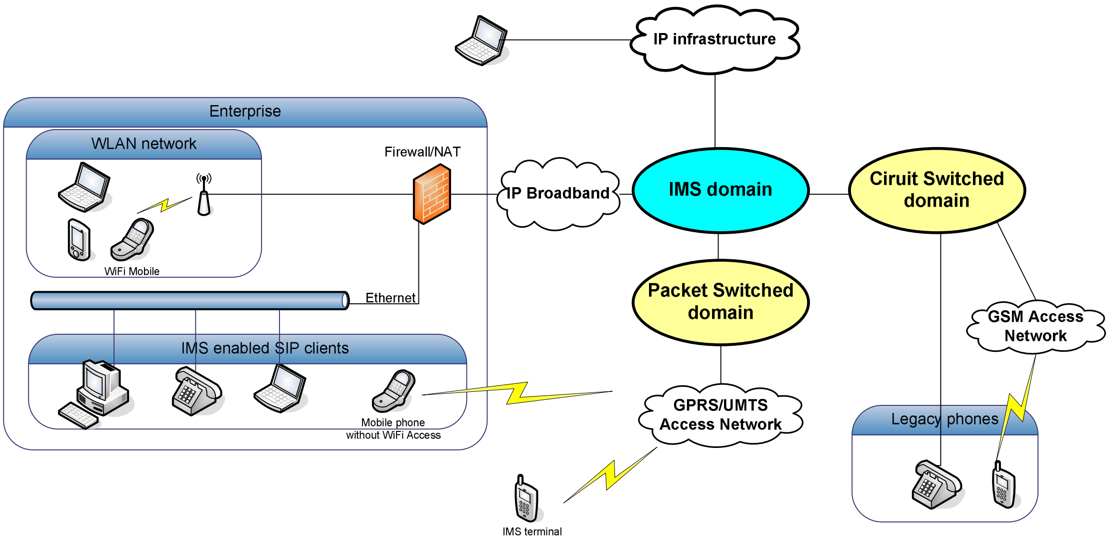


Figure 34 Possible future IMS enterprise solution

From the figure, we can see that mobile phones with WiFi access can connect to IMS domain either through normal GPRS/UMTS access network or through enterprise's WLAN. Mobile phones without WiFi access can just use GPRS/UMTS radio access. The mobile phone should be IMS enabled to be able to make use of IMS rich services. In the future, you may not see a PSTN telephone inside an enterprise, but instead you will find SIP hard-phones which are directly connected to ethernet ports. People also use softphones with rich multimedia features on workstations, portable PC, PDAs etc. These devices are connected to IMS domain through ethernet or WLAN. Outside of the enterprises, people can connect to the IMS domain through any access method for both IP infrastructure and mobile network. To connect with the legacy phones, IMS domain will take responsible by interfacing with the circuit switched domain.

5.4 Possible IMS migration solution

As we mentioned, it takes time for a complete IMS network is realized. We have to make a solution that can migrate to IMS easily and efficiently.
In the migration stage, we assume that the IMS domain is called "operator.com". Some users in the enterprise have changed to IMS enabled terminals, so that they can directly connect to IMS. But others still use their legacy non-IMS SIP clients which are connected to enterprise SIP PBX (non-IMS). Furthermore, some users may still use legacy non-SIP mobile phones.

The figure below shows the network infrastructure in an IMS migration stage.

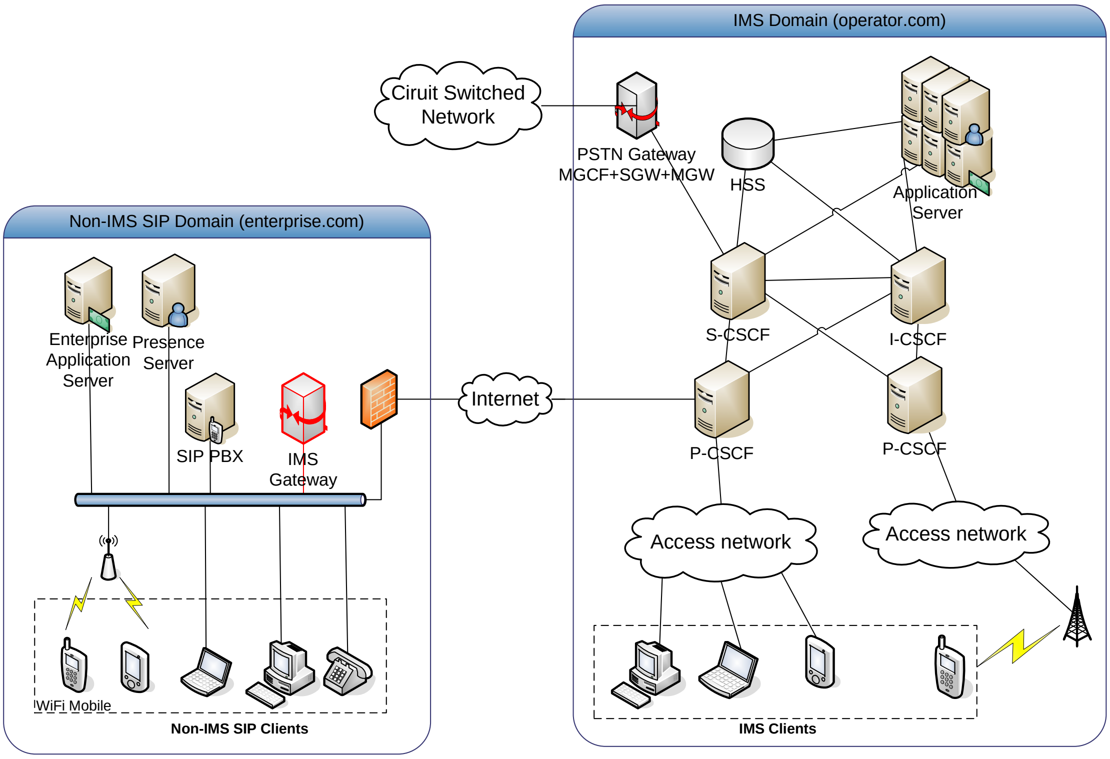


Figure 35 Network infrastructure in IMS migration stage

IMS uses the 3GPP variant of SIP, which need to interoperate with the IETF SIP because IETF SIP entities on the Internet do not support some of the extensions used in the IMS (e.g. preconditions).
To use special IMS services, like “push to talk”, a SIP client need to support IMS functionality.
The IMS Gateway plays the key role of interconnecting the IMS network and the non-IMS SIP based network. But how to implement the gateway is still an issue. Inter-working with IMS and Non-IMS SIP-based networks (specified in 3GPP TS 29.162) is not possible at this stage.

In the migration solution, an enterprise user may have two identities: one is sip:userA@operator.com in IMS domain and the other is sip:userA@enterprise.com in enterprise domain. When he turns his IMS-enabled terminal on, he registers on IMS domain, and use operator.com identity. But his fixed IP phone and his softphone which are registered on enterprise SIP PBX use another identity: sip:userA@enterprise.com.
Now we face a problem. When someone calls sip:userA@enterprise.com, the user with IMS-enabled terminal (sip:userA@operator.com) needs to be reached. It seems enterprise domain and operator domain should interoperate, but how can we make this possible?

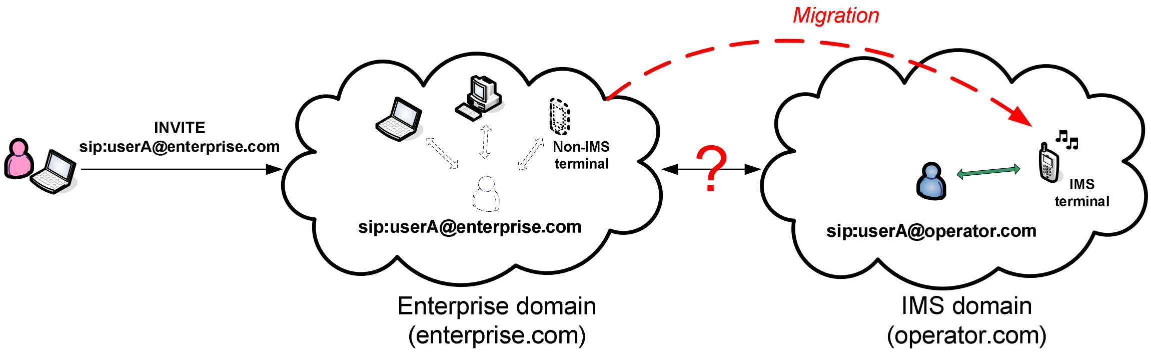


Figure 36 Interoperate problem in migration towards IMS

On the following pages are four possible solutions we have discussed based on forking, client, presence and registration. A detailed discussion of these solutions can be found in chapter 6.3.

5.4.1 Forking

In this solution, enterprise.com always forks incoming calls to operator.com. Enterprises SIP PBX worked as a forking proxy.

(a)Registration

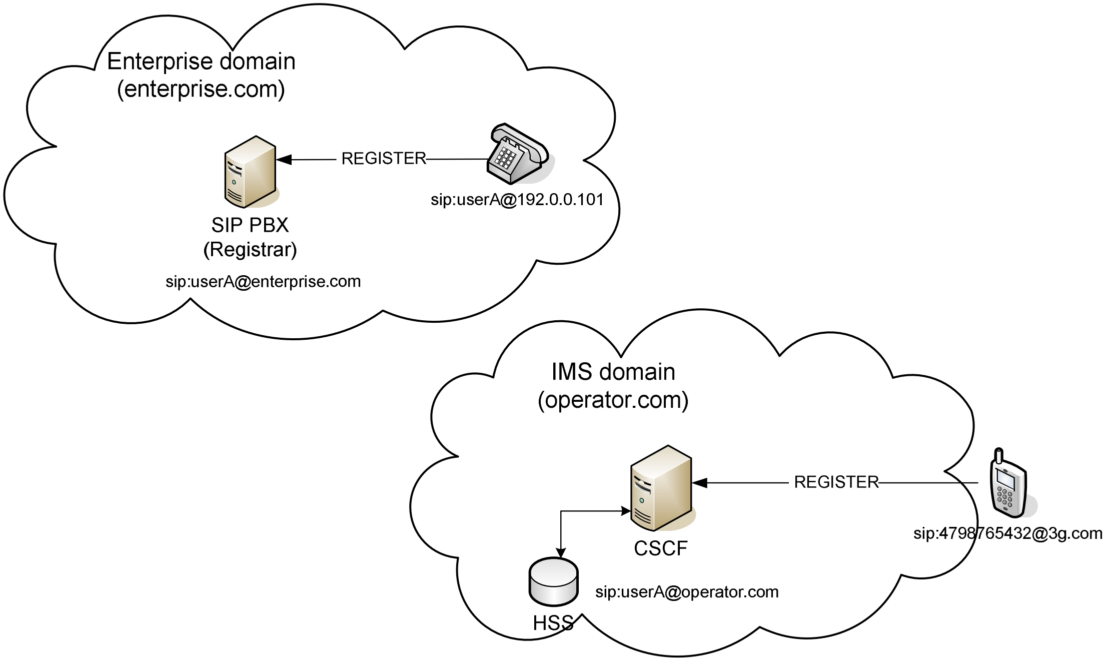


Figure 37 Registration in forking solution

Enterprise SIP client and IMS client is registered on their own domain independently. For example, userA has a fixed SIP phone in his office, which is registered with SIP PBX as sip:users@enterprise.com. When userA turn on his IMS terminal, it is registered with IMS domain as sip:userA@operator.com.

(b)Basic call setup

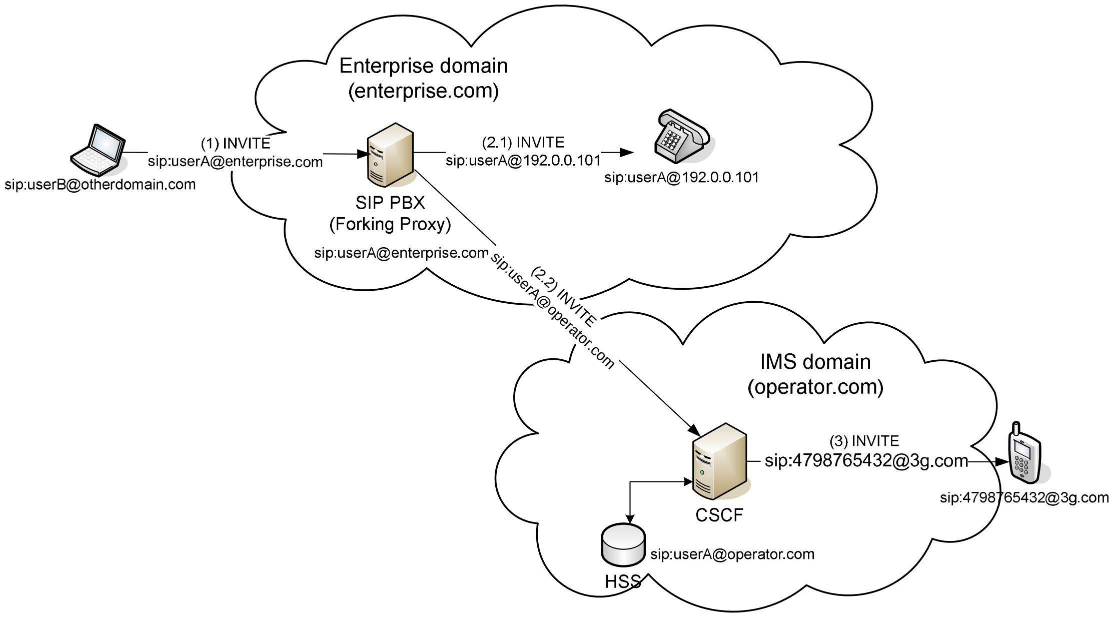


Figure 38 Basic call setup in forking solution

There are two types of forking. One is parallel forking which calls all clients in forking list simultaneous. For example, when someone calls sip:userA@enterprise.com, both his fixed IP phone and his IMS terminal will be ringing. When he picks up his IMS terminal, the communication will go through this terminal and the fixed IP phone will stop ringing.
The other is sequential forking which try clients one by one after a certain period of time until one phone is picked up. The Forking sequence and time interval are pre-configured and stored in the forking server. For example, when someone calls sip:userA@enterprise.com, his fixed IP phone starts ringing since it is the first element on his forking list. UserA doesn't take the phone, because he is out of office. After e.g. 5 second, fixed IP phone stops ringing, then his IMS terminal (registered as sip:userA@operator.com) starts ringing, he picks up the IMS terminal, then he can be reached by userB .

5.4.2 Client based

This solution requires an advanced client to inform enterprise SIP PBX that his location has moved to another domain, all incoming call to sip:userA@enterprise.com should be redirected to sip:userA@operator.com.

(a)Registration

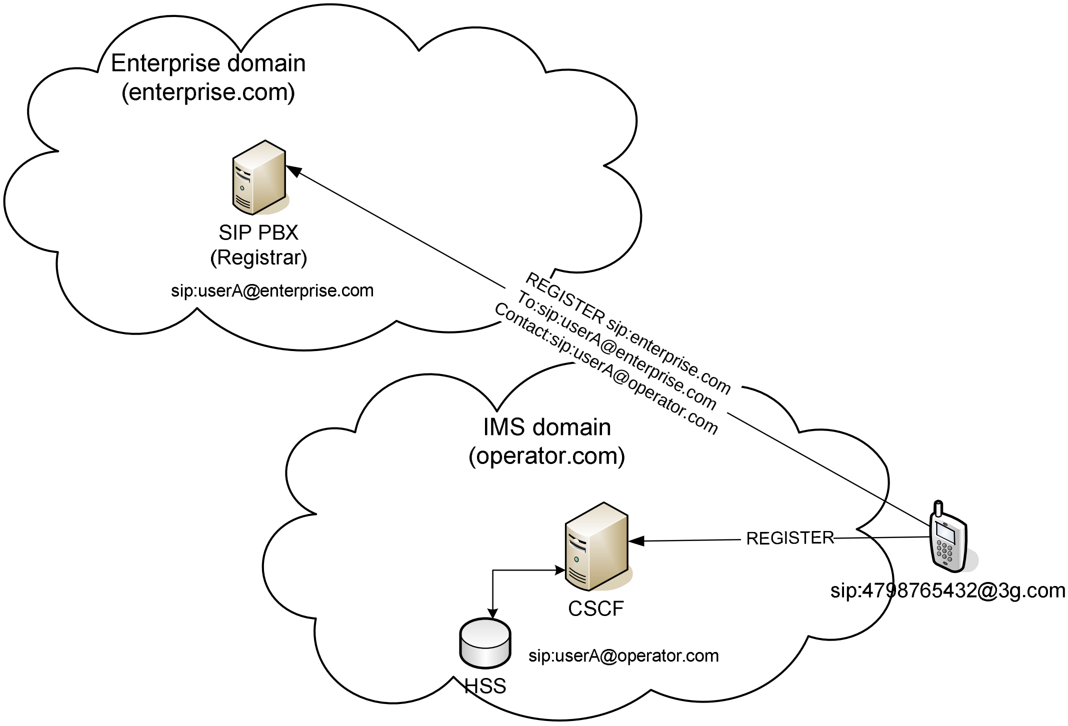


Figure 39 Registration in client based solution

When user turns on the IMS terminal, it will register on IMS domain as sip:userA@operator.com. Then it will register on the enterprise SIP PBX as sip:userA@enterprise.com and inform SIP PBX about the location change.

(b)Basic call setup

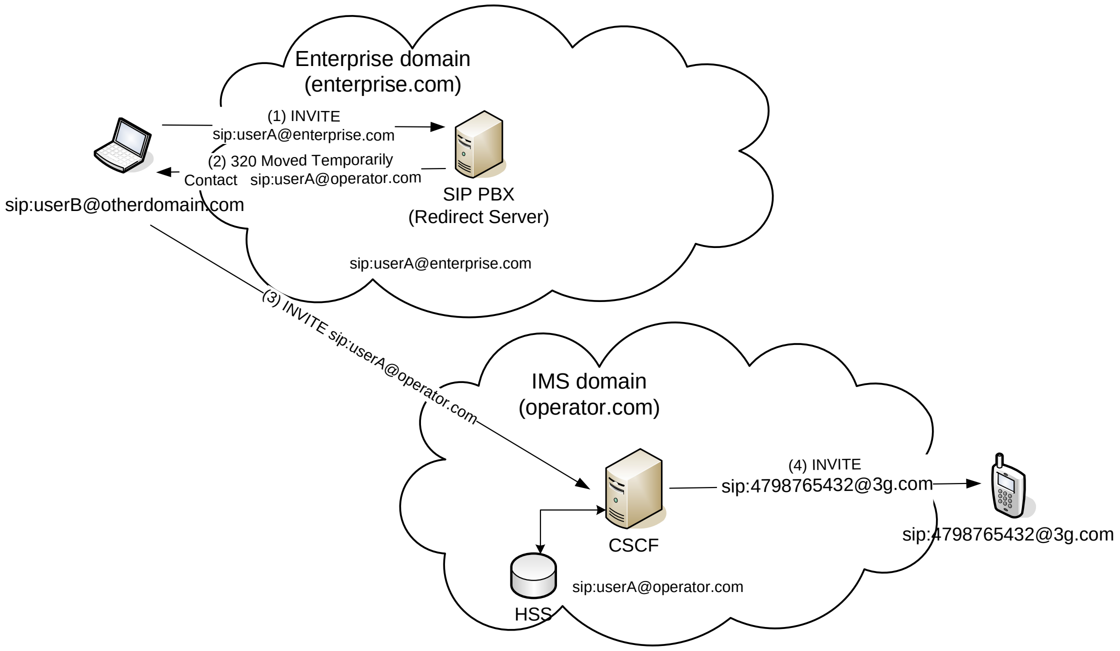


Figure 40 Basic call setup in client based solution

When an incoming call from sip:userA@enterprise.com reaches SIP PBX, the SIP PBX will acts as a redirect server and sends a “302 Moved Temporarily” SIP message to caller userB and instruct userB to try userA’s new location sip:userA@operator.com. Then userB will initiate a new call to sip:userA@operator.com which is directly sent to IMS domain, and userA’s terminal.

5.4.3 Presence

In the future, presence is one of those basic services that are likely to become omnipresent [5.3]. In the IMS architecture we find a presence solution. If the enterprise would include a similar presence service in its own domain, they could exchange information about the enterprise users and their location.

In this solution, both domains have their own presence server. These two domains have a presence link agreement so that they can get the presence status of each others servers. When the IMS terminal is turned on, the presence server in the IMS domain updates the user's status to be "online". It will update the presence server at the enterprise with the current status and location: sip:userA@operator.com. When enterprise SIP PBX get an incoming call to sip:userA@enterprise.com, the call will redirected to operator.com.

(a)Registration

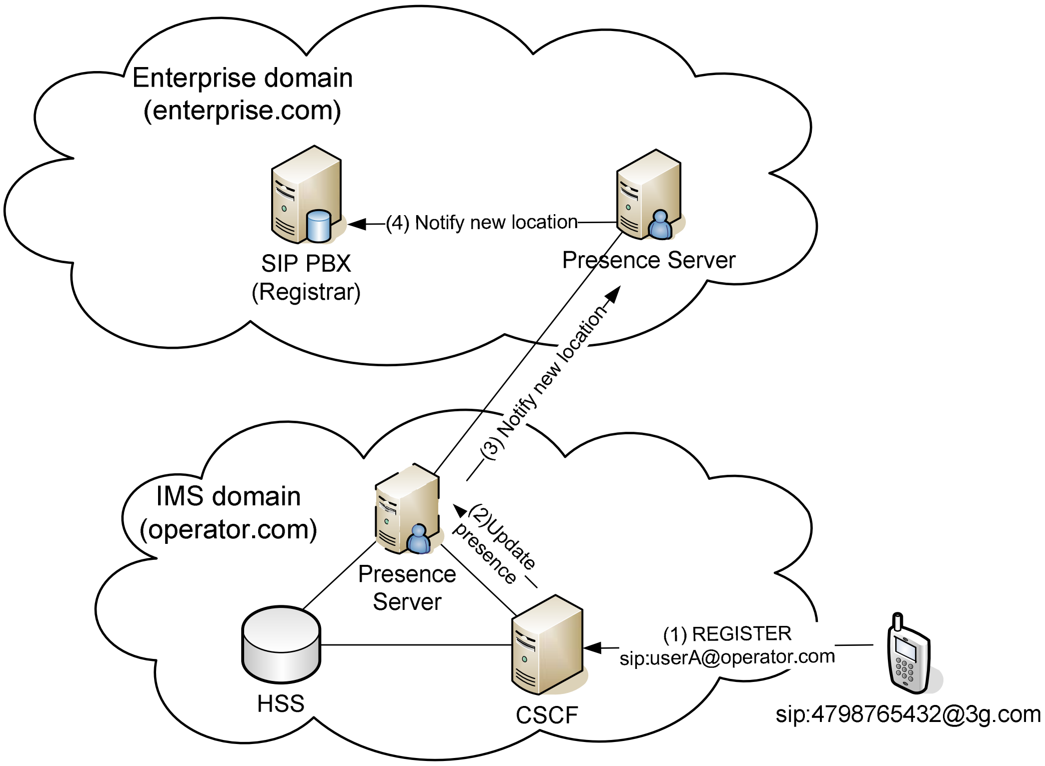


Figure 41 Registration in presence solution

According to the SIP presence architecture [Appendix-D], the SIP PBX plays the role as watcher of its Presence Agent (PA), which is the presence server in the enterprise domain. The presence server in enterprise domain works as a watcher of the presence server in IMS domain, and IMS terminal works as a Presence User Agent (PUA). When userA starts using the IMS domain, he will be registered as sip:user@operator.com. At the same time; the IMS domain updates userA presence status to online (according to filter criteria for presence service in user profile which stored in HSS, CSCF). It will also update his new location in the IMS presence server. Then the IMS presence server will notify its PUA, i.e. enterprise presence server about the new presence location. Furthermore, enterprise presence server will notify the new location to its PUA, i.e. enterprise SIP PBX which works as a SIP Registrar.

(b)Basic call setup

From the registration procedure above, we can see the registrar in enterprise domain is always updated to the user’s current location by linking two presence servers. To setup the basic call, it doesn’t need to involve the presence servers. SIP PBX will work as a redirect server and the sequence will look exactly like the basic call setting in client based solution. See figure 39.

5.4.4 Link Registration

Instead of using presence servers as mentioned above, this solution links two enterprise application servers so that registration procedure in two domains can be linked.
This solution needs some pre-requisites:

- IMS domain has an enterprise AS to handle link registration.
- It has a database which has a mapping of the user's SIP URI to the enterprise SIP domain.
- It knows that userA belongs to enterprise.com. Then it can provide link-register service.

In enterprise domain there is an application server that handles the link registration. It uses subscribe-notify mechanism to do link-register service subscription. The user profile which is stored in HSS contains a service profile with filter criteria for link register. The filter criteria help S-CSCF to decide when to involve a particular AS to provide a service. More information about filter criteria can be found at 3GPP TS 23.218.

(a)Registration

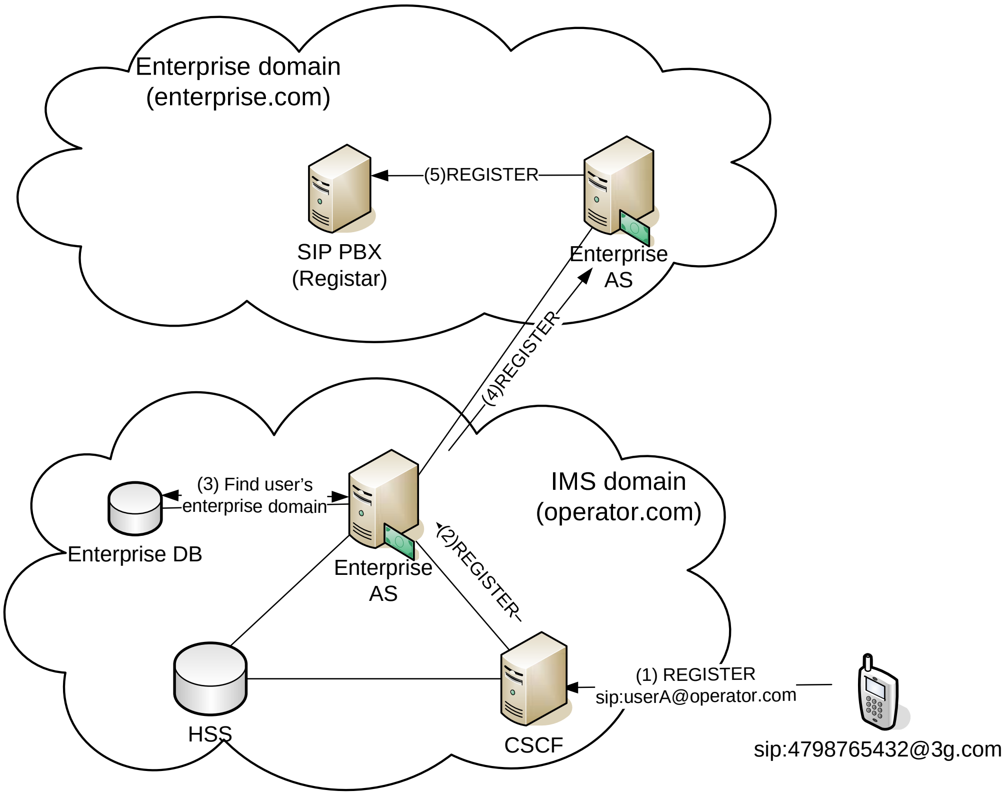


Figure 42 Registration in link presence solution

When the IMS client is turned on, it registers with IMS domain. Based on the filter criteria in User Profile which is stored in HSS, the S-CSCF will send register information to the Enterprise AS. It will then perform service control procedures, i.e. CSCF will send REGISTER message to Enterprise AS, and it will check the database to find user’s enterprise domain and send REGISTER message to Enterprise AS. Now the SIP PBX in the enterprise domain knows the user is currently registered in IMS domain as sip:userA@operator.com.

(b)Basic call setup

From the registration procedure above, we can see that the registrar in the enterprise domain is always updated to the user’s current location by linking two enterprise servers. SIP PBX will work as a redirect server; hence basic call setting procedure will look just like the basic call setup in the client based solution. See figure 39.

5.5 Results

For the purpose of integrating a mobile phone into an enterprise VoIP/SIP communication solution, we introduced IMS research. Because IMS is a promising architecture for offering IP multimedia services through ubiquitous cellular access, WLAN and fixed line etc.

First we pointed out why we need IMS in six aspects:

- QoS(Quality of Services)
- Charging of multimedia services
- Integration of different services
- Security
- Standardized Interface
- Fixed-mobile convergence (FMC)

These are major difference from IMS and non-IMS solutions.

After learning the IMS architecture in details we gave a possible IMS enterprise solution for the future. Since IMS is still in a developing phase and it is not put into commercial use, it needs a smooth and effective way for migrating an enterprise towards IMS. By studying detailed procedures in SIP and IMS, we discussed the interoperability between SIP domain and IMS domain in different cases, such as registration, basic call setup and presence. [Appendix D] Then we outlined the network infrastructure for enterprise solution in the IMS migration stage.

Furthermore, we faced a new problem. An enterprise user migrates to use IMS by using IMS operator's domain SIP URI, he still need to be reached by old enterprise domain SIP URI. We proposed these four solutions to resolve it:

- Forking solution
- Client based solution
- Presence solution
- Link Registration solution

The idea behind these solutions came from roaming research in different SIP domains at an early stage in our project. Because of time limitation and since we don't have IMS domain for testing, we tested a forking solution by using two different SIP domains instead. This test was successful.

6 Discussion

6.1 VoIP/SIP Enterprise Solutions

"Study and evaluate possible VoIP/SIP solutions for enterprise customers"

6.1.1 Evaluate SIP Clients

Basic Requirements for SIP client:

- Easy user interface
- Easy configuration
- NAT traversal
- No need for special external/internal hardware
- Windows/Linux support
- Not bound to a specific service (e.g. Skype)

6.1.1.1 SJphone:

SJphone has a nice and simple user interface. It doesn't support multiple simultaneous connected accounts, but for testing this may be an advantage. Basically it is a very good and simple client with excellent audio quality. It also identifies NAT type with help of STUN technology and has a configuration wizard to setup audio hardware. The fact that it's free makes it even better.

6.1.1.2 Xten EyeBeam:

We have tested the Xten eyebeam with Asterisk and it was quite impressive to use. You have a very nice and easy user interface with all the common controls. The possibility to hide user list and video output is also a nice feature.
Earlier we have tried the free version of eyebeam (X-Lite). We found the free version to be quite resource intensive and sometimes unstable. Eyebeam is more stable, but still use a lot of resources. Both of them have the possibility to communicate with up to 10 VoIP services simultaneously. The hardware configuration (for external hardware) also worked very well.

6.1.1.3 Grandstream GXP-2000

GXP-2000 is an excellent SIP hardphone for enterprise environments. It features a web interface that can be used to configure general, advanced settings and up to four accounts. It supports STUN and keep-alive to help with NAT traversal.

But the most impressive fact is the available firmware updates for the Grandstream phones. Problems reported to Grandstream or to various know VoIP forums are dealt with very quickly. We are very satisfied with the phone and the support staff. The only negative aspect is the poor availability.

6.1.2 Software SIP PBX

Table 3 SIP PBX comparison

	Asterisk	SipX
+	+Large community + Good documentation + Already used at Teleca + Platform independent +Many useful Add-ons	+ Management and operation + pure SIP
-	- Management is console based - Support for IM and Presence	- Platform dependent - Small community - Poor Documentation

Conclusion on Platform: Asterisk
Conclusion on Features: sipX
Conclusion on Management: sipX
Conclusion on Scalability: sipX
Conclusion on Installation: Asterisk
Conclusion on Community support: Asterisk

The first major task in this thesis was to evaluate the limited amount of SIP PBX servers that was available. It was soon clear to us that there were only two main distributions that had the flexibility and configuration options that were necessary.

On one hand we have the older and more mature Asterisk PBX which has got wide support from the open source community and is widely used in enterprise environments. It has a wide array of add-on and supported hardware.
On the other we have SipX which uses pure SIP and clearly defined architecture. The everyday management and scalability of the system will impress the administrators as well as system developers.

It's important to notice here that there is no totally wrong choice. We have been looking for one decisive fact that will rule out one or the other, but we have yet to find one.
But after implementing and testing both these solutions, we came to the conclusion that Asterisk PBX was the better choice. This was based on the mature software and support from the open source community. Asterisk PBX has a wide array of add-ons and clearly defined configuration settings for the different parts of the system layout.

6.2 Implementation and Design of VoIP/SIP Enterprise Solution

"Build a HiA-Teleca VoIP/SIP test-bed"

The testbed architecture was in constant change but we finally found a solution that would satisfy our test cases. Implementation was as mentioned before very time-consuming. There are many problems to consider in any Linux implementation not to mention the basic Asterisk configuration. The apt-get feature in Debian was a very helpful feature, but makes it very hard to make custom changes to the source code. But in a normal enterprise environment this should not be necessary. And if it is necessary you can download the CVS source and compile from the start. There exist step-by-step tutorials on how to do this.

The presence server configuration will also need good knowledge of the Linux operating system. As an example it requires java support which is not trivial to get working in a Linux environment. We have added a configuration how-to for this in the Appendix section. But the part that gave us the most headaches is interlinking Asterisk with Wildfire IM Server. The software that makes this possible is the Asterisk-IM plug-in. The Wildfire server comes with a nice web based configuration system. With the plug-in installed you can interlink users from the presence system with the users from Asterisk. The advantage here is realized with the presence client, Spark IM. This client connects to the presence server and shows the status of every user on the Wildfire server. But when the Asterisk is connected you get status from this system as well. The possibility to initiate calls directly from the Spark client through the Asterisk PBX is also possible. All in all this makes a complete VoIP/SIP testbed which include presence and IM support. This will give the testbed added potential when we start with IMS research.

In the latest stage of our project we incorporated openSER. While Asterisk is made to replace the enterprise PBX, openSER is a complex SIP server with all the functionality one would expect. It includes presence and IM functionality as well as NAT traversal technology, but it lacks the Asterisk media translation. Asterisk connects to a wide array of different signaling protocols (SIP, H.323, PSTN, +++).

So if we would make a new testbed implementation we would use a combination of openSER and Asterisk. OpenSER would handle SIP communication while Asterisk will handle communication to other communication media. This will give us the best of two worlds, it can support a lot of users while still have the flexibility of connection to other mediums.

6.2.1 Firewall/NAT Solutions

NAT is one of the biggest concerns for VoIP Implementations for VoIP services. It destroys the transparency which VoIP services relies on. Our project deals with NAT/firewall issues and shows the best solutions in different scenarios.

We would have liked to try all of the possible NAT traversal techniques but due to the limited time and resources that are available to us this will not be possible. And some of these techniques are sadly not in development yet.
Most of all we would like to try an ALG which will give an enterprise a unique possibility to control protocol communication moving in and out of the enterprise domain. But we managed to communicate with all of our SIP servers with the techniques that were available to us without violating the security at each location.

6.2.2 Roaming Solutions

We have evaluated solutions for many different scenarios. The simplest is the “call center solution” and we also added a proxy/redirect scenario. The most complex, but also the most interesting case is roaming with non-SIP phones. We proposed Presence solution to support this case. There exists no solution like this today and we are looking forward to developing it further in the migration to IMS chapter.

While a firewall/NAT solution is something that most enterprises will take into consideration, a roaming solution may not be necessary. The idea of allowing outside users to use phone resources located is troublesome at best and should be avoided if the there are no substantial gain for the enterprise.

We can see a lot of potential in an enterprise roaming solution. As stated before; a modern enterprise will have employees that need to be available outside of the normal office environment. And business relations that need to get a hold of a certain user should not be forced to handle multiple addresses and telephone numbers.

6.2.3 Enhancements

We choose the Asterisk PBX as our main SIP PBX server. But this server also has shortcomings that a modern enterprise may want to make everyday use easier and more practical.

6.2.3.1 Multiple Servers to link sub-domains

Multi-department enterprises are very common. And having all the different departments connecting to one PBX is very unnecessary and complicated. With one PBX in each domain you can handle NAT/firewall issues and save money on inter-company calling. We feel that multiple PBX solutions are essential in any multi-department enterprise.

6.2.3.2 TAPI

This enhancement greatly simplifies the calling procedure. To be efficient while making calls you should eliminate the step of dialing the number manually on your telephone. This is not only useful in an enterprise, but in any case where a telephone is used together with a computer.

6.2.3.3 Presence and instant messaging

It is possible to have a complete Presence/IM solution that works just fine even without Asterisk. And this is also why this solution will include a lot of extra work. All the users must be added twice (i.e. once on Asterisk server and once on IM server). And the mappings between Asterisk and Wildfire must be done manually. But after the initial mapping was done everything worked as expected.

The key argument for this solution is control. It’s a centralized solution where administrators have complete control over clients and security. The Wildfire solution can be run on an independent server, and this will free up resources on the Asterisk system.

6.2.3.4 Conference and video support

Asterisk has already included simple conference functionality and video support. With correct configuration, these features can be easily implemented.

6.3 Migration towards IMS

"Study and evaluate possible IMS solutions for enterprises,
Compare major differences between current VoIP/SIP solution and IMS solution, and then propose an architecture that allows interconnection/extension/migration of VoIP solutions towards IMS"

6.3.1 Forking

This is the simplest solution. SIP PBX works as a forking proxy. In advance, the IMS domain SIP URI (e.g. sip:userA@operators.com) has to be added to the user's forking list in SIP PBX. Neither extra application servers are needed, nor is an agreement between operator and enterprise needed. Simplicity is the advantage.

As for disadvantage, maintenance of forking list manually is time-consuming. Furthermore, if the forking list becomes large, network signaling traffic will be increased for parallel forking while calling delay time would be very long for sequential forking.

6.3.2 Client based

The advantage is that we avoid unnecessary signaling to figure out if the user can be reached by the IMS domain. Hence network signaling traffic load may be reduced. It's also a simple solution, but it requires more functionality from the client. The client has to be SIP enabled. Legacy mobiles can not send SIP messages to SIP PBX to inform location changing, so they are not supported by this solution.

We can work around its shortcoming in some situations. For example, if a user knows that he will only use a certain IMS domain later, he may change enterprise registrar manually before roaming to IMS domain. If the enterprise SIP PBX has a web GUI to maintain registrar, the current location can be updated through the internet. But it's not very flexible and requires more knowledge from the user.

6.3.3 Presence

The advantage of this solution is that it's a network based solution which has no requirements for the client, i.e., it can supports legacy telephone. Compared to forking, it avoids unnecessary signaling traffic in network.

Disadvantage is that it is a somewhat complex solution. Enterprise and IMS operator should have a presence agreement so that they know each peer's presence status.

6.3.4 Link Registration

The advantage of this solution is the same as for linking presence solutions. Based on the network, the solution has no requirement to the client, and it can avoid unnecessary signaling traffic.

The shortcoming of this solution is quite like linking presence too. It is a little complex and in stead of a presence agreement, it needs registration agreement between these two domains.

6.3.5 Summary of migration road map

Table below shows the evaluation of the 4 solutions we have proposed. They are proposed to resolve the interoperating problem in migration towards IMS, i.e., when enterprise user migrates to IMS domain he may not be reachable with enterprise SIP URI.

Table 4 Migration solutions comparison

	Forking	Client based	Presence	Link registration
Terminal requirement	No	Terminal should be SIP enabled and domain settings configurable.	No	No
Server requirement	Enterprise SIP PBX act as a SIP forking proxy	no	Presence server is required for both domains.	Application server for providing link registration service is required.
Contract requirement	No	No	Presence contract for exchange of presence information between Enterprise domain and operator domain is needed.	Enterprise subscribes to “subscriber registration update service” which is provided by operator.
Total Discussion	It is simplest solution, but parallel forking will cause more network signaling traffic, sequential forking will cause call delay. It is suitable for enterprise with small forking list.	It is simple, and operator independent. It requires no complex SIP-IMS setup. It requires a more complex client. It also needs more advanced terminal configuration.	It is a little complex, but supports legacy phone. It is suitable for all enterprises, especially for those who have an own presence server already.	It is the most complex solution. It requires installation of a SIP to IMS gateway. In an early phase of SIP/IMS introduction not many operator may support registration updates across business borders

Figure below shows the possible migration road map of enterprise solutions towards IMS. Considering the amount of IMS-enabled operators and functionality features, we proposed four migration solutions that may appear in different migration stages.

Our opinion is that forking may appear first since forking solution is the simplest solution. Forking proxies are the basic SIP entities defined in SIP [RFC 3261]. It requires nothing special from operator and client to implement the solution. IMS is still not put into commercial use. Forking solution is therefore suitable for the first migration stage.

It is no doubt that some operators will deploy IMS in their network, and IMS-enabled clients will become more and more popular. Then presence and client based solutions will then be suitable. We don't know which will come first. Client based solutions need an advanced client and don't support legacy phones, whereas presence solution is network based. Presence solution have no special client requirements and support legacy phones. Hence in the road map, we show that the presence solution have more functionality than client based solution.

Link Registration is a relative complicated solution. Like the presence solution this is a network based solution. It requires an IMS-enabled operator to support registration updates across business borders. This kind of support may not be added for many operators in an early phase of SIP/IMS introduction. So it seems that the link registration solution will appear in the later phase of migration towards IMS.

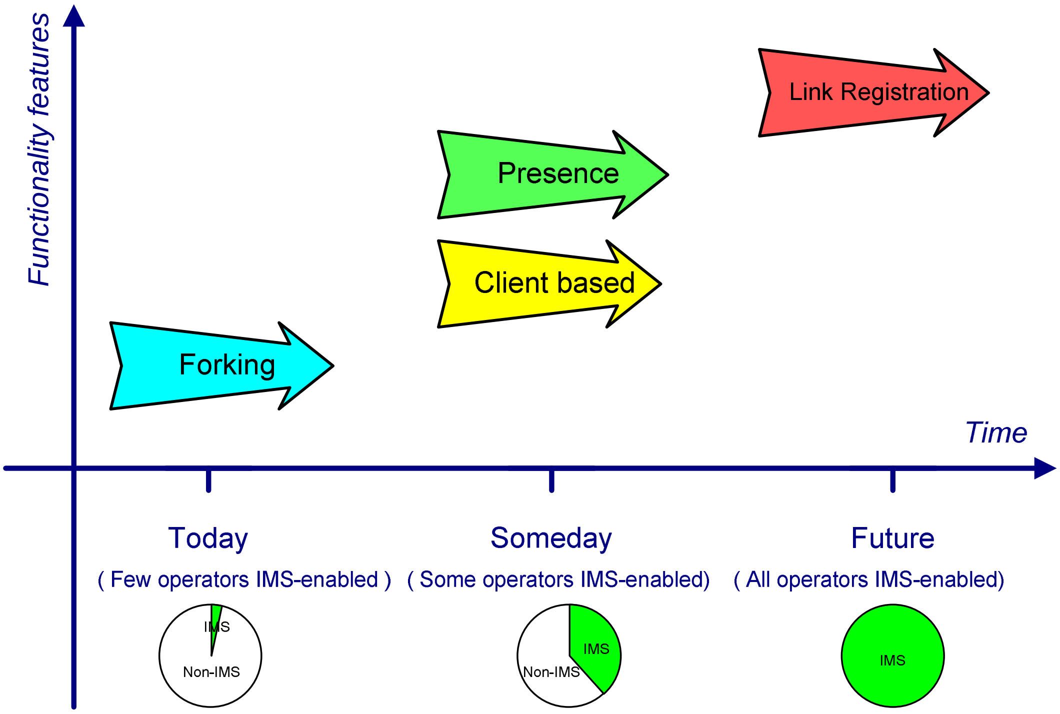


Figure 43 Possible Migration Roadmap towards IMS

7 Conclusion and Further work

7.1 Conclusion

In this thesis we discussed and integrated a suitable enterprise VoIP/SIP solution. A research platform “HiA-Teleca test-bed” with enhanced features was built from scratch. Based on studying interoperability between enterprise domain and operator domain on test-bed, we proposed and evaluated four possible migration solutions from VoIP/SIP towards IMS for enterprise. An IMS migration roadmap with these four solutions was given.

We began with researching “state-of-the-art” technology related to enterprise VoIP/SIP solutions. It is important for us to define possible enterprise requirements and integrate a suitable VoIP/SIP solution into an existing enterprise network.

To approve our concept and research the possibilities of SIP technology, we established the “HiA-Teleca test-bed”. It will be a common research platform for HiA and Teleca to build and develop competence in VOIP/SIP/IMS area. It will contribute development in future “All-IP” products and services.

By further researching the test-bed, our solution was enhanced with a wide array of new services, such as presence, instant message, conference, and video calls. It will also support firewall/NAT traversal and roaming.

To integrate cellular phones and legacy phones into an overall enterprise solution, we introduced IMS research. We pointed out the six major differences of IMS and non-IMS solutions. Future possible IMS solutions were proposed. IMS is still not in commercial use and it will still take several years for the full IMS vision to become a reality. VoIP/SIP solution and IMS solution will co-exist and develop over a long period into the future. How to interoperate existing VoIP/SIP enterprise domains and IMS operator domains is very important in IMS migration phase, but not addressed sufficiently in the literature.
Our thesis proposed and evaluated four migration solutions:

- Forking solution
- Client based solution
- Presence solution
- Link Registration solution

Our solutions tied the VoIP/SIP solution together with the overall communication system of an enterprise. So that each user can be accessible from a single telephone number or SIP URI without restricting his movement inside or outside of the enterprise environment.

According to complexity, functionality and dependency of IMS deployment, these four solutions might appear in different IMS migration phases. Our solutions make it possible for enterprise users to smoothly migrate towards a future IMS infrastructure.

7.2 Future work

Based on our work, following issues can be interesting for further research:

- The testbed will continue to be used as a development platform for new SIP/IMS based solutions and for demonstration purposes.
- Evaluate QoS and security for the testbed we have built.
- Combine openSER and Asterisk to increase user capability and SIP functionality.
- Authentication between SIP and IMS might be an interesting issue for further research.
- Implement/Simulate IMS core for testbed.
- We have proposed four enterprise IMS migration solutions. We have only tested the forking solution because of project time limitation. Maybe in the future, more solutions can be implemented.
- We have made a sip soft phone base on the open source client sipXezphone; this could be a base source for future IMS client development.
- We didn’t have time to implement the IMS gateway, maybe it can be a potential business product for future study.

Abbreviations

3GPP	3rd Generation Partnership Project
ALG	Application Layer Gateway
AS	Application Server
BAS	Broadband Access Server
BG	Border Gateway
BGCF	Breakout Gateway Control Function
CAMEL	Customized Application for Mobile Network Enhanced Logic
CS	Circuit Switched
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR/AuC	Home Location Register/Authentication Center
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IM	Instant Messaging
IM SSF	IP Multimedia-Services Switching Function
IMS	IP Multimedia Subsystem
IMS	IP Multimedia Subsystem
IMS-MGW	IP Multimedia Subsystem Media Gateway
IP	Internet Protocol
IPv4 PDN	Internet Protocol Version 4 Packet Data Network
IPv6 PDN	Internet Protocol Version 6 Packet Data Network
LCD	Liquid crystal display
MGCF	Media Gateway Control Function
MPLS	Multiprotocol Label Switching
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NGN	Next Generation Networking
OSA AS	Open Service Architecture Application Server
OSA SCS	Open Service Architecture
P2P	Peer-to-Peer
PBX	Private Branch eXchange

P-CSCF	Proxy-Call Session Control Function
PA	Presence Agent
PDA	Personal digital assistants
PDF	Policy Decision Function
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
PTT	Push To Talk
PUA	Presence User Agent
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request for Comments
RTP	Real-time Transport Protocol
SGSN	Serving GPRS Serving Node
SGW	Signaling Gateway
SIP	Session Initiation Protocol
SIP AS	Session Initiation Protocol Application Server
SMTP	Simple Mail Transfer Protocol
SPDF	Service Policy Decision Function
SS7	Signaling System #7
STUN	Simple Traversal of UDP over NATs
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TrGW	Translation Gateway
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol
WLAN PDG	Wireless LAN Packet Data Gateway
WLAN WAG	Wireless LAN Wireless Access Gateway

References

Theory and State of Art

[2.1] "Voice over IP" from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/VoIP

[2.2] "FAQ about Voice over IP" from FCC. (Visited Feb. 2006)
URL: http://www.fcc.gov/voip/

[2.3] "SIP" from Wikipedia. (visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/ Session_Initiation_Protocol

[2.4] "H.323" from Wikipedia. (visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/H.323

[2.5] "Network Voice Protocol" from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/Network_Voice_Protocol

[2.6] "Specifications for the Network Voice Protocol" from RFC741
URL: http://tools.ietf.org/html/741

[2.7] "Quality of service" from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/Quality_of_service

[2.8] M. Poikselkä et al., Wiley, "The IMS – IP multimedia Concepts and Services", 2004 ISBN 0-470-87113-X

[2.9] "What Is SIP Introduction" from SIP center. (Visited Feb. 2006)
URL:
http://www.sipcenter.com/sip.nsf/html/What+Is+SIP+Introduction

[2.10] Gonzalo Camarillo, McGraw Hill "SIP Demystified", 2002
ISBN 0-07-137340-3

[2.11] Private branch exchange from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/PBX

[2.12] "IP Multimedia Subsystem" from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem

[2.13] Gonzalo Camarillo and Miguel A. Garc´ıa-Mart´ın c 2006 John Wiley & Sons, Ltd "IMS Vision: Where Do We Want to Go?"

[2.14] Firewall (networking) from Wikipedia. (Visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/Packet_filter

[2.15] "NAT Traversal for Multimedia over IP Services" (visited Feb. 2006)
URL: http://www.newport-networks.com/whitepapers/nat-traversal1.html

[2.16] Y. Rekhter "Network Working Group - Address Allocation for Private Internets" (visited Feb. 2006)
URL: http://www.ietf.org/rfc/rfc1918.txt February 1996

[2.17] "Private network" from Wikipedia (visited Feb. 2006)
URL:http://en.wikipedia.org/wiki/Private_IP_address

[2.18] "Roaming" from voip-info.org (visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/Roaming

[2.19] "SIP Registrar server" from voip-info.org (visited Feb. 2006)
URL: http://www.voip-info.org/wiki/index.php?page=SIP+registrar+server

[2.20] "SIP Proxy server" from voip-info.org (visited Feb. 2006)
URL: http://www.voip-info.org/wiki/index.php?page=SIP+proxy

[2.21] "SIP redirect server" from voip-info.org (visited Feb. 2006)

URL: http://www.voip-info.org/wiki/view/SIP+redirect+server

[2.22] "Presence information" from voip-info.org (visited Feb. 2006) URL: http://en.wikipedia.org/wiki/Presence_information

[2.23] "Instant messaging" from voip-info.org (visited Feb. 2006) URL: http://en.wikipedia.org/wiki/Instant_messaging

[2.24] "An Implementation of SIP Servers for Internet Telephony", Proc. of the 5th International Conference on High Speed Networks and Multimedia Communication, 2002

[2.25] "Design and Implementation of a SIP-based VoIP Architecture" by S. Zeadally and F. Siddiqui, 2004

[2.26] White Paper IMS - "IP Multimedia Subsystem from Ericsson" URL:http://www.ericsson.com/technology/whitepapers/ims_ip_multimedia_subsystem.pdf (visited Feb. 2006)

[2.27] Gonzalo Camarillo and Miguel a. Garcia-Martin – "The 3G IP Multimedia Subsystem, Merging the Internet and the cellular worlds" (2004)

[2.28] "The Role of IMS in PSTN-to-VOIP Migration" by Tim Hills (2005) URL:http://www.lightreading.com/document.asp?doc_id=83597&page_number=8

[2.29] MagedanWitaszek, K. Knuettel Fraunhofer, "THE IMS PLAYGROUND @ FOKUS – AN OPEN TESTBED FOR NEXT GENERATION NETWORK MULTIMEDIA SERVICES T. FOKUS", Technical University of Berlin, Germany

[2.30] Peter Kim, Andras Balazs, Eddy van den Broek, Gerhard Kieselmann, Wolfgang Bohm "IMS-based Push-to-Talk over GPRS/UMTS" 2005

Evaluate VoIP/SIP Enterprise Solutions

[3.1] "IAX" from Wikipedia. (Visited Feb. 2006) URL: http://en.wikipedia.org/wiki/IAX

[3.2] "Asterisk PBX" from Wikipedia. (Visited Feb. 2006) URL: http://en.wikipedia.org/wiki/Asterisk_PBX

[3.3] "sipX" from Wikipedia. (Visited Feb. 2006) URL: http://en.wikipedia.org/wiki/sipX

[3.4] "Open source PBXes offer free flexibility" from Wayne Rash, InfoWorld. (Visited Feb. 2006) URL: http://www.linuxworld.com.au/index.php/id;840466049;fp;4;fpid;4

[3.5] "How to Compare sipX ECS with the Asterisk PBX (sipX vs. Asterisk)" from Sipfoundry. (Visited Feb. 2006) URL: http://sipxwiki.calivia.com/index.php/Comparing_sipX_with_Asterisk

[3.6] "Asterisk Features" from Digium. (Visited Feb. 2006) URL: http://www.Asterisk.org/features

[3.7] "SIPfoundry sipX Projects - Open Source IP PBX Solution (VoIP)" from pingtel. (Visited Feb. 2006) URL: http://www.sipfoundry.org/sipX/

[3.8] "Asterisk" from voip-info.org. (Visited Feb. 2006) URL: http://www.voip-info.org/wiki-Asterisk

[3.9] SipX from voip-info.org. (visited Feb. 2006)

URL: http://www.voip-info.org/wiki-sipx

Implementation and Design of VoIP/SIP Enterprise Solution

[4.1] ”Bringing Telephony Features into SIP Networks with Back To Back User Agent”
URL:http://www.sipcenter.com/sip.nsf/html/Bringing+Telephony+Features+into+SIP+Networks+with+Back+To+Back+User+Agent

[4.2] “openSER” from openSER.org. (Visited April 2006)
URL: http://openSER.org

[4.3] “openSER” from voip-info.org. (Visited April 2006)
URL: http://www.voip-info.org/wiki/view/OpenSER

[4.4] Gonzalo Camarillo and Miguel a. Garcia-Martin – The 3G IP Multimedia Subsystem, Merging the Internet and the cellular worlds (2004) P.51-70

[4.5] Gonzalo Camarillo – SIP DEMYSTIFIED (2002) P.98-106

[4.6] RFC 3856 - “A Presence Event Package for the Session Initiation Protocol by Network Working Group(SIP)” (visited Mars. 2006)
URL:http://www.faqs.org/rfcs/rfc3856.html

[4.7] Asterisk presence from http://www.voip-info.org (visited Feb. 2006)
URL:http://www.voip-info.org/wiki/view/Asterisk+presence

[4.8] RFC 3863 - Presence Information Data Format (PIDF) by H. Sugano el al. (visited mars. 2006)
URL:http://www.rfc-archive.org/getrfc.php?rfc=3863

[4.9] Asterisk handbook from Digium (visited Feb. 2006)
URL:http://www.digium.com/en/docs/asterisk_handbook/meetme_meetmecount.html

Migration towards IMS

[5.1] IP Multimedia Subsystem from Wikipedia. (visited Feb. 2006)
URL: http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem

[5.2] “The 3G IP Multimedia Subsystem”,
G. Camarillo et al., McGraw Hill, 2004 ISBN 0470 87156 3

[5.3] “The IMS”, M. Poikselkä et al., Wiley, 2004
ISBN 0-470-87113-X

[5.4] IMS Migration Challenges and Solutions: Towards a Multimedia-Enhanced Telephony Architecture, MetaSwitch White Paper
URL: http://www.metaswitch.com/rescenter/whitepapers.htm

[5.5] IMS - IP Multimedia Subsystem, Ericsson White Paper
URL: http://www.ericsson.com/technology/whitepapers/ims_ip_multimedia_subsystem.pdf

[5.6] Cisco Service Exchange Framework: Supporting the IP Multimedia Subsystem for Mobile, Wireline, and Cable Providers,
Cisco Systems white paper

URL:http://www.cisco.com/application/pdf/en/us/guest/netsol/ns549/c654/cdccont_0900aecd80395cb0.pdf

[5.7] IMS architecture from Data Connection.
URL: http://www.dataconnection.com/sbc/imsarch.htm

Appendix

[A.1] "Asterisk - dual servers" from voip-info.org (visited mars. 2006)
URL: http://www.voip-info.org/wiki-Asterisk+-+dual+servers

[B.1] "The Asterisk TAPI project" by Omniis (visited Feb. 2006)
URL: http://www.omniis.com/ntsgr/cms/page.asp?688

[C.1] "Wildfire Installation Guide" from jivesoftware. (Visited Feb. 2006)
URL: http://www.jivesoftware.org/builds/Wildfire/docs/latest/documentation/install-guide.html#unix

[E.1] "Best practices for SIP NAT traversal" by Adrian Georgescu
URL: http://ag-projects.com/docs/PressArticles/NATtraversal-BestPractices.pdf

[E.2] RFC 3489 – "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)". By J. Rosenberg URL:http://www.faqs.org/rfcs/rfc3489.html

[E.3] "Peer-to-Peer Communication across Network Address Translators" (Visited Jan. 2006) by Dan Kegel
URL: http://www.brynosaurus.com/pub/net/p2pnat/

[E.4] "STUN" from Wikipedia, the free encyclopedia (Visited Jan. 2006)
URL: http://en.wikipedia.org/wiki/STUN

Standard References

IETF Specification

RFC 2327 Session Description Protocol (SDP)
RFC 3261 Session Initiation Protocol (SIP)
RFC 3265 SIP-Specific Event Notification
RFC 3310 HTTP Digest Authentication using Authentication and Key Agreement (AKA)
RFC 3327 extension header field for registering non-adjacent contacts (path header)
RFC 3428 SIP Extension for Instant Messaging
RFC 3455 private header extensions for SIP
RFC 3489 Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
RFC 3515 the SIP REFER method
RFC 3550 Real-time Transport Protocol (RTP)
RFC 3574 Transition Scenarios for 3GPP Networks
RFC 3588 DIAMETER base protocol
RFC 3608 extension header field for service route discovery during registration
RFC 3665 SIP Basic Call Flow Examples
RFC 3680 SIP event package for registrations
RFC 3842 SIP event package for message waiting indication and summary
RFC 3856 SIP event package for presence
RFC 3857 SIP event template-package for watcher info
RFC 3858 XML based format for watcher information
RFC 3863 Presence Information Data Format (PIDF)
RFC 3891 the SIP Replaces Header
RFC 3903 SIP Extension for Event State Publication
RFC 4235 an INVITE-Initiated dialog event package for SIP

3GPP Specification

TS 22.101 Service Aspects; Service Principles
TS 22.141 Presence Service; Stage 1
TS 22.800 IMS Subscription and access scenarios
TS 23.002 Network Architecture
TS 23.003 Numbering, Addressing and Identification
TS 23.141 Presence Service; Architecture and functional description; Stage 2
TS 23.218 IMS session handling; IM call model; Stage 2
TS 23.228 IMS stage 2
TR 23.981 Interworking aspects and migration scenarios for IPv4-based IMS implementations (early IMS)
TS 24.141 Presence Service using the IMS Core Network subsystem; Stage 3
TS 24.229 IMS call control protocol based on SIP and SDP; Stage 3
TS 29.162 Interworking between the IMS and IP networks
TS 29.163 Interworking between the IMS and Circuit Switched (CS) networks
TS 29.162 Interworking between the IMS and IP networks
TS 29.163 Interworking between the IMS and Circuit Switched (CS) networks
TS 29.962 Signaling inter-working between the 3GPP SIP profile and non-3GPP SIP usage

Appendix A - Asterisk dual servers Configuration

After literature review [A.1] we experimented with dual server functionality.
There exist several ways of interconnecting Asterisk PBX servers. One way is with the IAX protocol, which actually has a better way of dealing with NAT-to-NAT environments. But our project deals with SIP, so we will concentrate on this solution. This may seem like an odd choice considering that IAX is better with NAT traversal, but our project will also deal with IMS. And SIP is a permanent element of the IMS architecture.

While two PBX servers are connected, it is necessary to share their dial plan as well. The dial plan should be designed on each server so that it becomes immediately clear which VoIP PBX should receive the call, e.g. use 1xxx for Location 1, 2xxx for Location 2.

Here we give our successful example to show how it works.
We have two Asterisk servers in different location.

Location	Location 1	Location 2
Server name	Asterisk 1	Asterisk 2
Server IP Address	172.25.4.124	172.25.4.99
User A extension	1111	2111
User B extension	1222	2222

It is not necessary to have extension numbers for each user in both servers; it is only used for roaming users. For example, User A travel from Location 1 to Location 2, when he turns on his SIP phone, he will register on Location 2 PBX server.
And his colleagues in Location2 can call him 2111. User B in Location1 don’t know User A has moved to a new location, so she is still calling him on 1111, this call will be forward to 2111.

In the configuration files on each server, it should be an entry to define peer server’s IP address so that they can communicate to each other. e.g. sip.conf on Asterisk 1 has en entry[asterisk2].

```
[asterisk2]
type=friend
host=172.25.4.124
context=default
```

And this entry name will be used in extension.conf. For example extension.conf has this line:

```
exten => _”prefix”XXX,1,Dial(SIP/”Peer defined in sip.conf”/${EXTEN},30,r)
```

This means if a user on this server dial the extension (the amount of numbers in the extension is defined by the number of X's and the prefix), the call will be transferred to peer defined in sip.conf.

Configuration files for Asterisk 1:

(1)sip.conf

```
[general]
context=default
port=5060
bindaddr=0.0.0.0
srvlookup=yes

[anders]
type=friend
host=dynamic
username=anders
secret= SecretOfAnders
context=default

[wulian]
type=friend
host=dynamic
username=wulian
secret= SecretOfWulian
context=default

[asterisk2]
type=friend
host=172.25.4.124
context=default
```

(2)extension.conf

```
[general]
static=yes
writeprotect=no

exten => 1111,1,Dial(SIP/anders,20,tr)
exten => 1111,2,Voicemail,u1111
exten => anders,1,goto(1111,1)

exten => 1222,1,Dial(SIP/wulian,20,tr)
exten => 1222,2,Voicemail,u222
exten => wulian,1,goto(1222,1)

exten => _2XXX,1,Dial(SIP/Asterisk2/${EXTEN},30,r)
exten => _2XXX,2,Congestion

exten => 1000,1,voicemailMain
```

Configuration files for Asterisk 2:

(1)sip.conf

```
[general]
context=default
port=5060
bindaddr=0.0.0.0
srvlookup=yes

[wulian]
type=friend
context=default
username=wulian
secret=SecretOfWulian
host=dynamic

[anders]
type=friend
context=default
username=anders
secret= SecretOfAnders
host=dynamic

[asterisk1]
type=friend
context=default
host=172.25.4.99
```

(2)extension.conf

```
[general]
static=yes
writeprotect=no

exten => 2222,1,Dial(SIP/wulian)
exten => 2222,2,Voicemail,u2222
exten => wulian,1,goto(2222,1)
exten => 4444,1,Dial(SIP/wulian)

exten => 2111,1,Dial(SIP/anders)
exten => 2111,2,Voicemail,u2111
exten => anders,1,goto(2111,1)

exten => _1XXX,1,Dial(SIP/Asterisk1/${EXTEN},30,r)
exten => _1XXX,2,Congestion

exten => 2000,1,VoicemailMain
```

Appendix B - TAPI Configuration

After literature review [B.1] we experimented with TAPI functionality on our testbed. First we need to download the TAPI driver. There exist different types, but for this example we will use Asterisk TAPI. It can be downloaded from asttapi's page located at sourceforge.net . [https://sourceforge.net/projects/asttapi/].
Install and reboot.
Now it's time to configure the manager API in Asterisk:
Edit this file: manager.conf

```
; Asterisk Call Management support

[general]
enabled = yes                              ;Set to yes to enable the Call Management
port = 5038                                ;Listening port
bindaddr = 0.0.0.0                         ;Listen to every IP

[nick]                                     ;Replace with your username
secret = mysecret                          ;Your password
deny = 0.0.0.0/0.0.0.0                     ;deny every IP
permit = 192.168.1.5/255.255.255.0         ;Allow one IP
read = system,call,log,verbose,command,agent,user      ;User rights
write = system,call,log,verbose,command,agent,user     ;More of the same
```

You have to restart the Asterisk server after this, a simple reload will not do.
Next we have to configure the TAPI driver. Go to control panel→Phone and modem options →Advanced → Omniis TAPI driver for Asterisk → Configure

Host – this is the host name or IP address of the server running the Asterisk manager
Port – 5038 – default
User – the user you set-up in manager.conf
Password – the users secret you set-up in manager.conf
User Channel – this is the your extension, it terms of the channel name in my case it is Sip/nick (nick being your defined user)
Dial by 'context' – check this one
Context – the context that is defined in the sip.conf for your user
Caller ID – The identification number/name associated with your user
Outgoing Chan – this is the channel which external calls are placed over, you can get this information from extensions.conf, in here you will find a section which defines external calls.

Start Microsoft Outlook and go to the address book. Right click on a contact and choose "call contact". A new window will appear with the name of the person you are calling and his telephone number. Click the button that says dialing options. In this window you will see a pull down list that says "connect using line". Choose the one that says Asterisk. You can press "Line properties and check that everything is setup correctly, or you can just press ok and initiate the call.
If you have done everything right you will now be able to call using the TAPI driver. Your telephone will start to ring. And when you pick up the phone the call will be initiated to the person/party you defined in Outlook.

Appendix C - Installation of Wildfire / Spark / Asterisk-IM on Debian

Detailed instructions for Wildfire / Spark / Asterisk-IM installation on Debian are shown bellow. [C.1]

1. Open a command interface.
2. Choose were to put the files.
3. Login as root
4. Download the latest version of Wildfire from: http://www.jivesoftware.org.
5. Uncompress downloaded file.
6. Move Wildfire directory to /opt/
7. Download java-runtime from: http://java.sun.com/
8. Remove root privilege (necessary to configure java)
9. Make suitable Debian package
10. Change to root
11. Install newly made Java-Debian package
12. Install Mysql server and client
13. Change Mysql server password
14. Login to mysql server interface
15. Create database
16. logout of mysql server interface
17. Change directory
18. Import necessary database structure into our new database
19. Change directory
20. Download Asterisk-IM plug-in
21. Change directory
22. Start Wildfire
23. Open a web-browser and go to: http://localhost:9090/

```
1.    (open terminal)
2.    cd /usr/local/src/
3.    su
4.    wget http://www.jivesoftware.org/servlet/download/builds/Wildfire/Wildfire_2_5_0.tar.gz
5.    tar zvxf Wildfire_2_5_0.tar.gz
6.    mv Wildfire/ /opt/
7.    Download java-runtime from: http://java.sun.com/
8.    Add contrib to each line in /etc/apt/sources.list
9.    apt-get update
10.   apt-get install fakeroot java-package
11.   exit
12.   fakeroot make-jpkg jre-1_5_0_06-linux-i586.bin
13.   su
14.   dpkg -i sun-j2re1.5_1.5.0+update06_i386.deb
15.   apt-get install mysql-server mysql-client libmysqlclient12-dev
16.   mysqladmin -u root password secret (secret=your own password)
17.   mysql -u root –p
18.   create database imserver;
19.   exit
20.   cd /opt/Wildfire/resources/database/
21.   mysql -u root -p imserver < Wildfire_mysql.sql
22.   cd /opt/Wildfire/plugins/
23.   wget http://www.jivesoftware.org/Wildfire/plugins/Asterisk-im.jar
24.   cd /opt/Wildfire/bin/
25.   ./Wildfire start
26.   (open a web-browser and goto: http://localhost:9090/)
```

Appendix D - Case study for registration, basic call setup and presence

This appendix consists of SIP and IMS studying of three cases, which are registration, basic call setup and registration. We have searched many related IETF and 3GPP specifications; see Standard References. For the purpose of understanding our IMS migration solutions, we summarized our study in this appendix. Most SIP resources comes from [5.2] and IETF [RFC 3261]; and most IMS resources comes from [5.3] and 3GPP [TS 23.228], [TS 24.229].

Case study – Registration

SIP Registration

SIP Registration is used for SIP User Agent to inform a registrar (e.g. in Teleca.no) about their current location by send REGISTER request. All incoming request for sip:lian@teleca.no will be proxied or redirected to current location (e.g. sip:lian@188.188.188.102). Registration can be done with or without authentication. Below shows these two types of registration sequence.

a) SIP registration without authentication

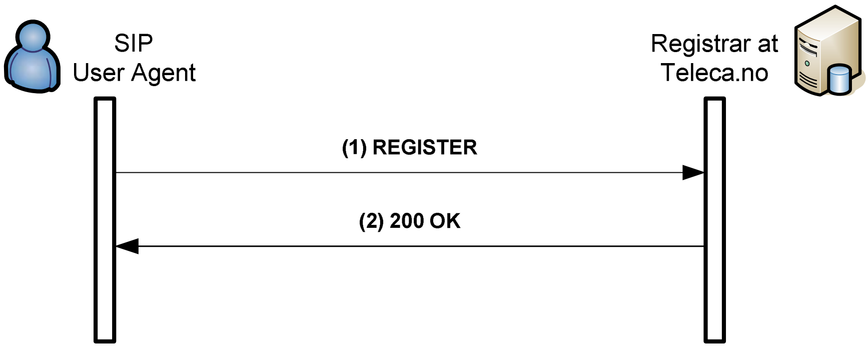


Figure 44 SIP registration without authentication

b) SIP registration with authentication

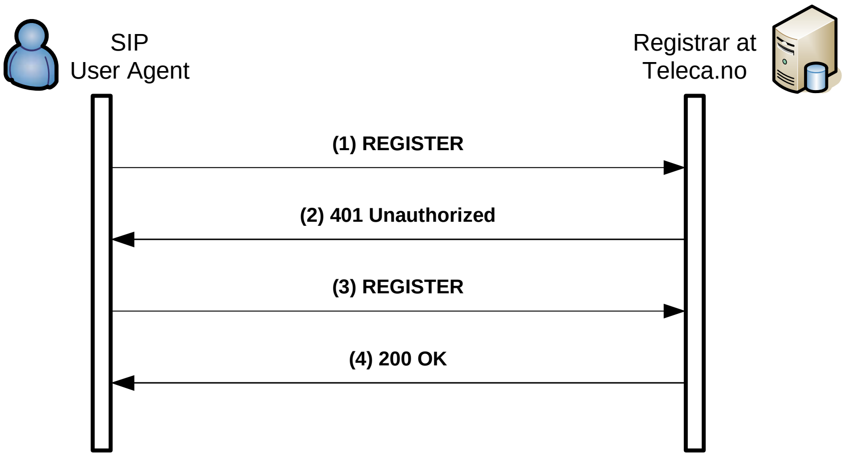


Figure 45 SIP registration with authentication

IMS Registration

IMS prerequisites

Before any IMS activities can be performed, the following has to be accomplished:

- IMS subscription,
- Access to IP network (e.g. GPRS, ADSL, WLAN),
- P-CSCF address discovery (there are two ways: Integrated into IP Connectivity Access Network (IP-CAN) and Standalone procedure)
- IMS level registration.

Acquire an IP address are different for different access networks, here we mainly talking about IMS registration.

Detail IMS registration message

Registration is IMS mandatory, not SIP mandatory. IMS Registration is accomplished by a SIP REGISTER request. First IMS terminal retrieves from ISIM the Private User Identities, Public User Identities and home network domain URI, then it creates a SIP REGISTER request like below.

```
REGISTER sip:teleca.no SIP/2.0
Via: SIP/2.0/UDP 192.0.0:5060
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD
                     utran-cell-id-3gpp=C359A3913
From: <sip:twswuli@teleca.no>
To: <sip:twswuli@teleca.no>
Contact: <sip:[1080::8:800:200C:417A];comp=sigcomp>;
          expires=600000
Call-ID: 748923400@432423dfad
Authorization: Digest username="lian@teleca.no",
          realm="teleca.no", nonce="",
          uri="sip:teleca.no",response=""
Security-Client: ipsec-3gpp,alg=hmac-sha-1-96
          spi-c:=3929102; spi-s=0293020;
          port-c:3333; port-s=5059
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Content-Length: 0
```

The REGISTER request includes these four parameters:

1. Registration URI: Identifies home network domain to address the SIP REGISTER request
2. Public User Identity: the SIP URI that represents the user ID under registration (address that users prints in their business cards)
3. Contact address: SIP URI that includes the IP address of the IMS terminal or a host name where the user is reachable.
4. Private User Identity: used for authentication only, not routing. Same as IMSI in GSM

IMS registration with authentication

Since IMS based on SIP, it can support SIP registration without authentication as we mentioned above for testing, but in practice, registration with authentication will always be used.

3GPP IMS terminals need to be equipped with a removable UICC (Universal Integrated Circuit Card) for authentication when accessing IMS network. The UICC is a removable smart card, which may contain SIM (Subscriber Identity Module), USIM (UMTS Subscriber Identity Module), and ISIM (IP multimedia Services Identity Module). SIM is used for GSM/GPRS networks; USIM is used to access UMTS networks. ISIM is IMS specific, which contains the collections of parameters for user identification and authentication, such as Private User Identity, Public User Identity, Home Network Domain URI, Long-term secret …

IMS registration can use an ISIM or use an USIM. But the registration procedure is quite similar, independently of the presence of an ISIM or USIM, shown as below.

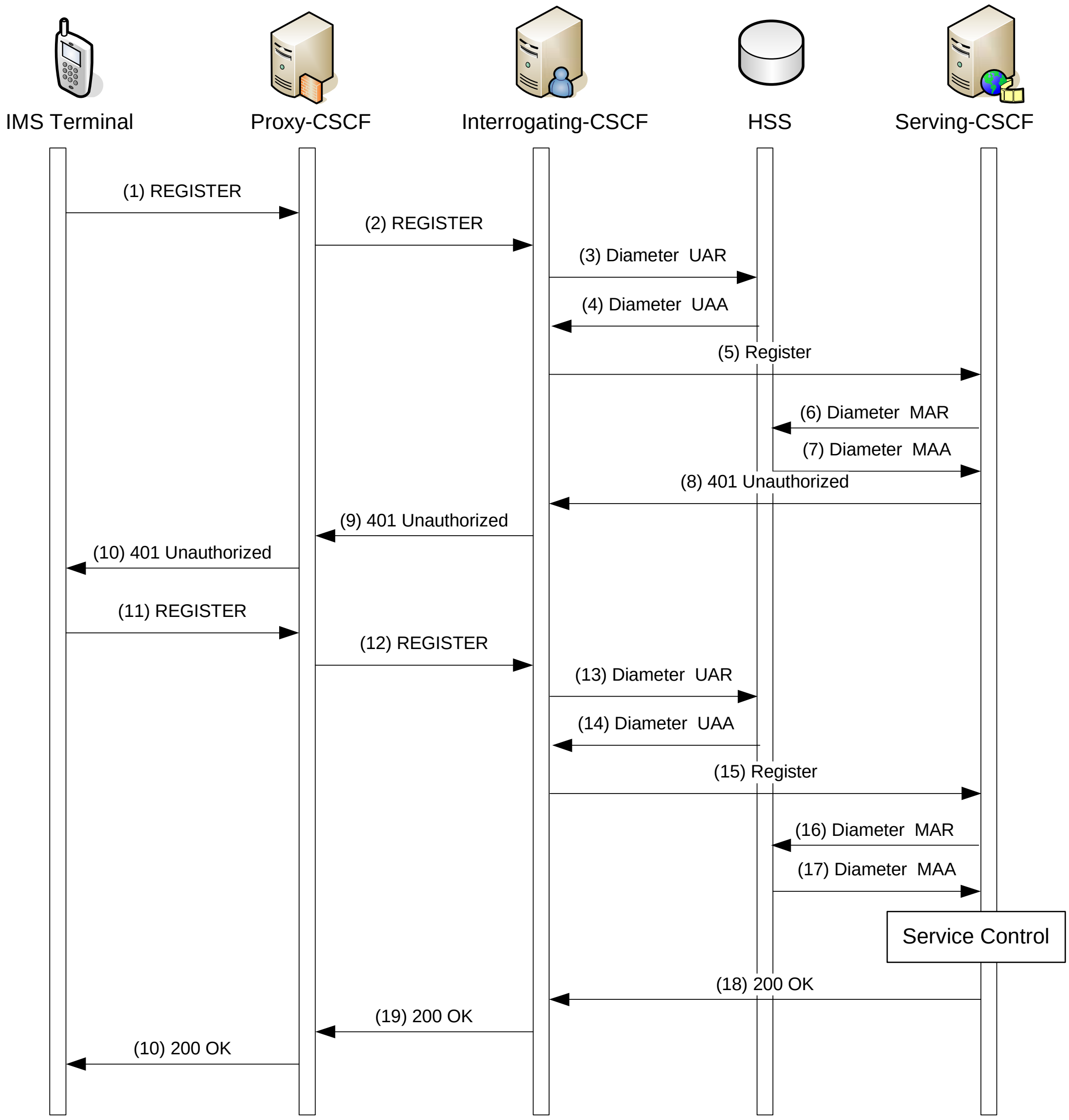


Figure 46 IMS registration procedure with authentication

One of the IMS requirement is the user should be informed whether he is reachable or not (i.e. whether the terminal is under radio coverage and whether the user is registered with the network or not). The registration can be removed by shutdown of S-CSCF or manually deregistering.
Basic SIP protocol does not inform IMS terminal if subscription is removed. IMS solve the problem by doing a subscription to the reg event. NOTIFY is sent when subscription state has changed. Figure below shows the sequence.

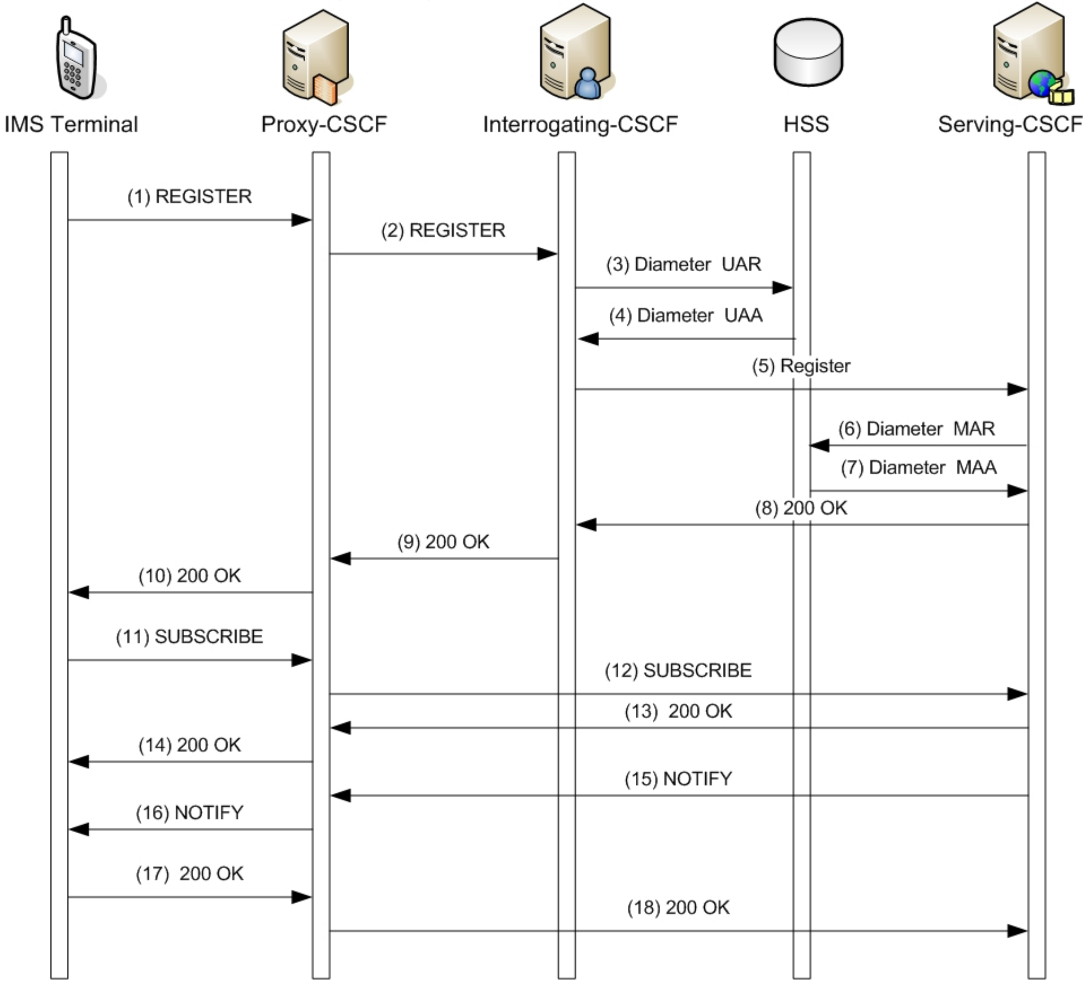


Figure 47 IMS registration including subscription to the reg event state

Interoperability Discussion

From the above studying, we can see non-IMS SIP client and IMS client use the same registration procedure but IMS client can have an extra subscription of the reg event state.

- Non-IMS SIP Client can register on IMS domain when using the account IMS domain provided and support the authentication algorithm (e.g. AKAv1-MD5) IMS domain used. From the ethereal log we got from Ericsson IMS tester proved that.
- Theoretically IMS client can register on Non-IMS SIP VoIP domain without doing subscribe reg event. Of course IMS client should be configured to have the same authentication method as Non-IMS SIP PBX needed .But the IMS client may not use the IMS rich services as it was registered in IMS domain.

Case study - Basic Call Setup

SIP basic call setup

To establish a basic call, INVITE Request is sent from caller (e.g. Lian) to invite other user (e.g. Anders) to join a call session. INVITE Request consists of the session description, e.g. the Lian's IP address, the media type, and media received port etc. Then Anders's phone ringing and send status "180 Ringing" response back. When Anders pick up the phone, "200 OK" with a session description is sent back to Lian to show Anders accept the session. This session description contains Anders's IP address, port, protocol etc for media transaction. Then Lian will return ACK response if she does not give up waiting. Finally with the three-way handshake "INVITE-final response-ACK", the basic call session is established. If end users know each other's SIP address, they can establish call at once. But actually proxy server is quite common used within call setup. Following figures shows the message sequences of SIP basic call setup with and without SIP proxy.

a) Call setup without SIP proxy

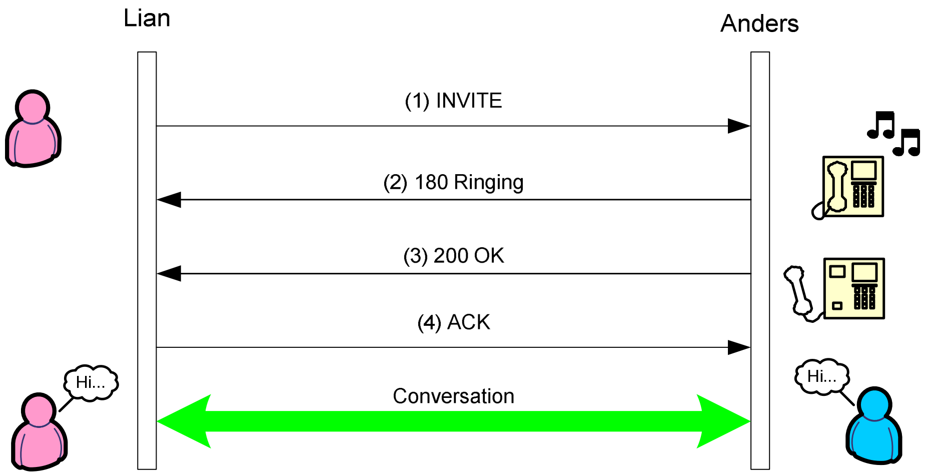


Figure 48 Call setup without SIP proxy

b) Call setup with SIP proxy

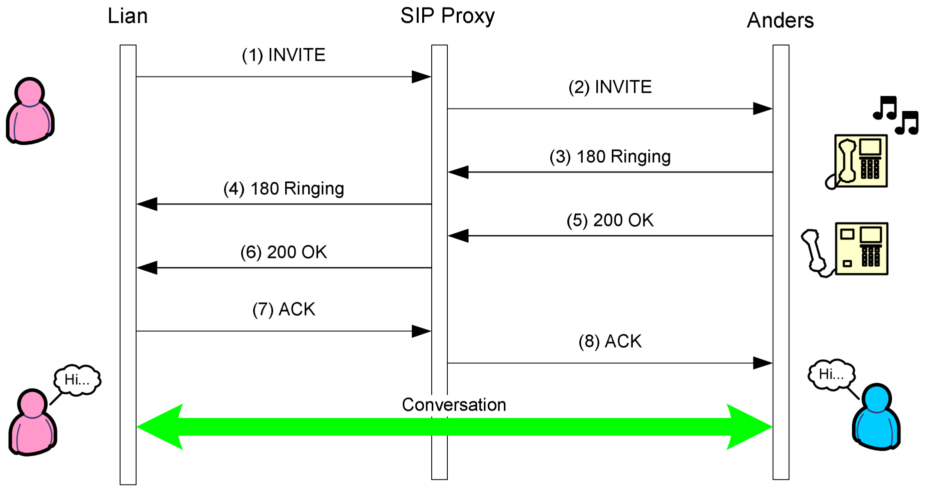


Figure 49 Call setup with SIP proxy

IMS basic call setup

The precondition for basic call setup is both users are registered.
An Basic Session includes Client to client session starts by doing an INVITE method, The INVITE message will be forwarded to the S-CSCF for the originating home network and then sent further to the S-CSCF for the terminating home network.
The procedure is shown as below. In this figure we assume that both users are roaming outside their respective home network. And we simplified the figure without showing the resource reservation which sometimes known as preconditions. In 3GPP Release 5, preconditions was mandatory, but Release 6 allows session establishment without preconditions when the remote terminal does not support them or when service does not required them.

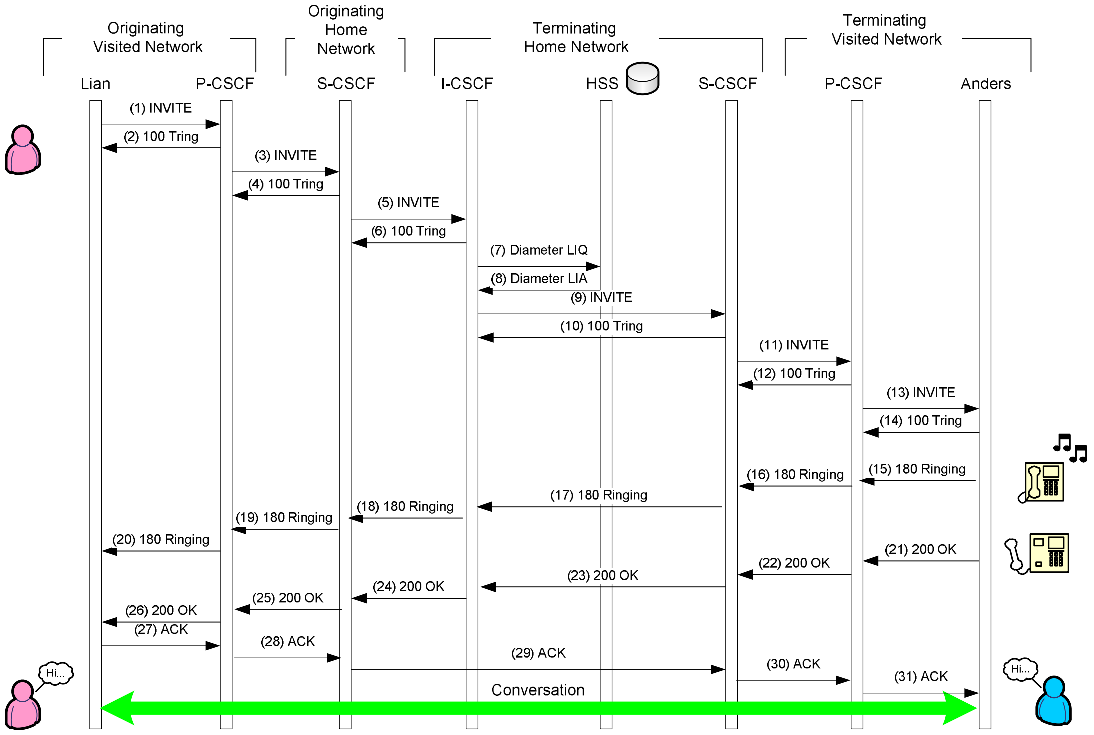


Figure 50 IMS basic call setup

From the figure we can see:
(1-6)Lian will call Anders; she send an INVITE request includes a Request-URI with the SIP URI of destination subscriber. The INVITE request contains a Route header that helps the P-CSCF to route the INVITE request to the home S-CSCF. The S-CSCF evaluates the filter criteria for subscriber. Then the S-CSCF inspects the Request-URI to find the destination network. With the help of DNS, the S-CSCF finds the entry point (I-CSCF) of Anders's Home network. The S-CSCF forwards the INVITE request to that I-CSCF.
(7-8) The I-CSCF queries the HSS to find out which S-CSCF is serving the destination subscriber Anders and HSS returns the S-CSCF address. Protocol Diameter is used between I-CSCF and HSS.

(9-14) The I-CSCF forwards the INVITE request to that S-CSCF. The S-CSCF evaluates the service criteria for subscriber Anders, and inspects the Contact information (at registration), forwards the INVITE request to the P-CSCF. Then The P-CSCF forwards the INVITE request to the Anders.
(15-20) Anders's phone ringing, forward status "180 Ringing" message back to Lian.
(21-26) When Anders's pick up the phone, message "200 OK" is forwarded back.
(27-31) Lian's phone forward ACK to Anders. With three-way handshake, conversation is established successfully. Lian can talk with Anders now.

Interoperability Discussion

From the above studying, we can see non-IMS SIP client and IMS client use the same registration procedure when IMS client don't use precondition functionality. Non-IMS SIP Client can make basic call with IMS Client without enable precondition (e.g. QoS reservation). Of course they should use same algorithm for authentication.

Case study – Presence

SIP Presence

By using presence service, a user can inform its reachability, availability and willingness of communication to another user. [5.2] Figure below shows the SIP presence Architecture.

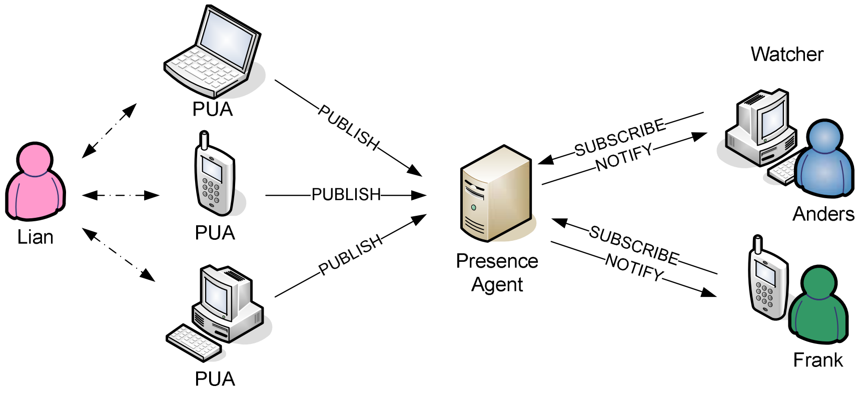


Figure 51 SIP Presence architecture

- Presentity (Presence entity) is the person providing presence information.
- PUA (Presence User Agent) is device to provide information about presence of presentity. Presentity can have several PUAs.
- PA (Presence Agent) gathers all information sent from all the PUAs of presentity.
- Watcher is an entity that requests presence information about presentity.

To identify a presentity or a watcher, a pres URI is used, e.g. pres:lian@teleca.no.

Presence service is built on top of SIP notification framework. RFC 3856 defines the "presence" event. Figures below show the related sequences.

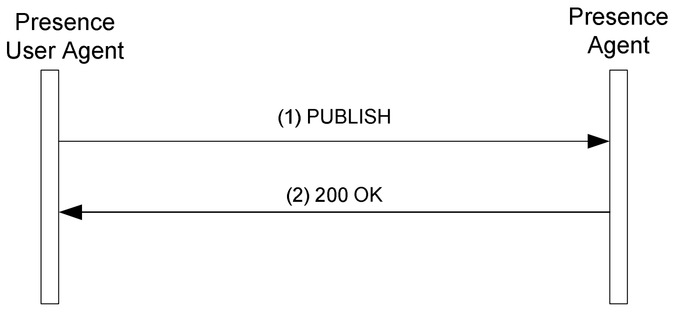


Figure 52 Publication of presence information

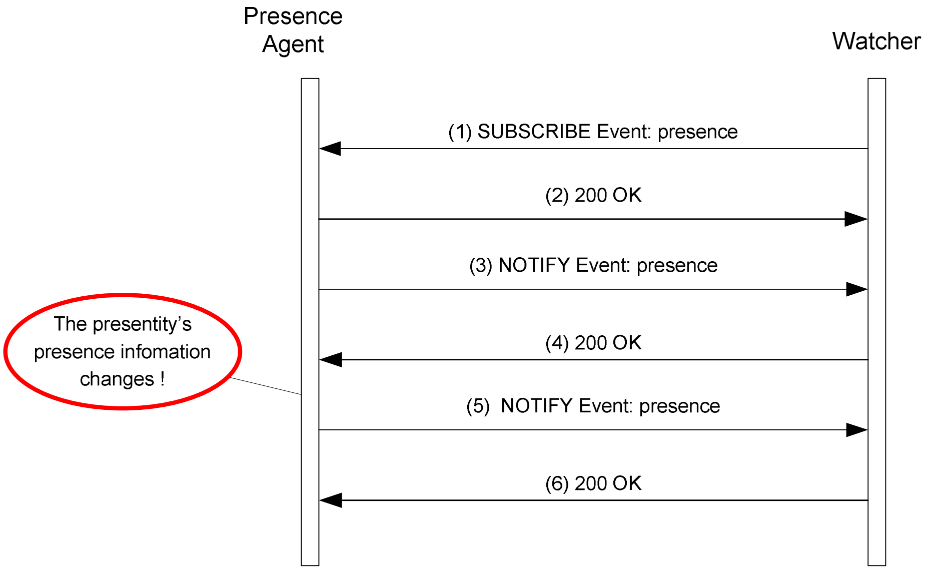


Figure 53 Subscription and notification of presence information

IMS Presence

3GPP TS 23.141 defined architecture to support the presence service in the IMS. It is included in 3GPP Release6.[5.2] Figure below shows the architecture.

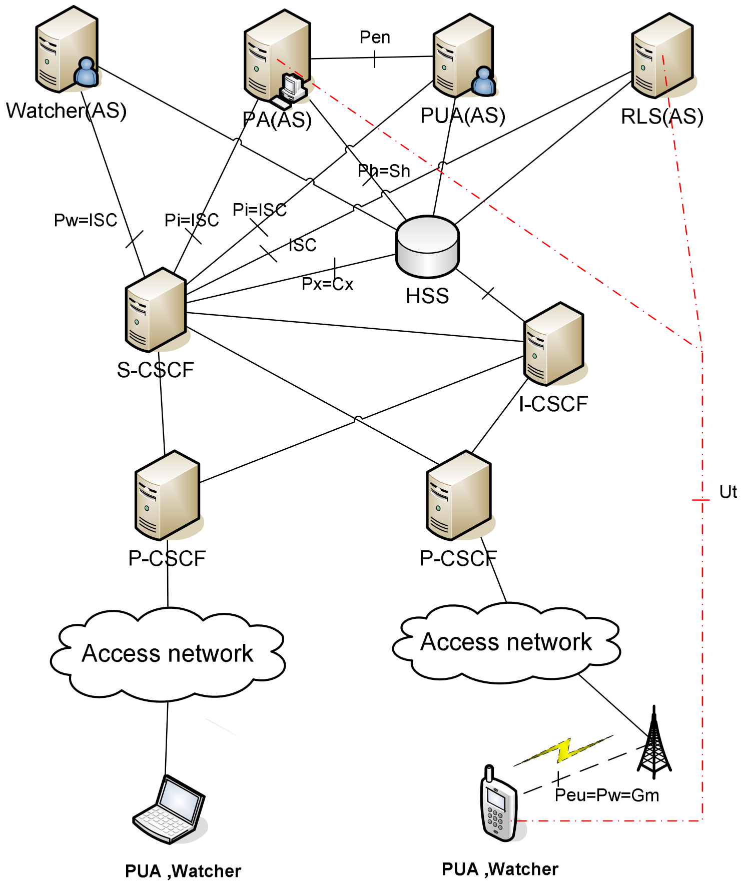


Figure 54 SIP based presence architecture in IMS

From the figure, we can see IMS terminal can act as both watcher and PUA. Since presence is a foundation of other services, other services AS can have a role of watcher or PUA. Presence Server (PS) located in the home network act as PA which is an Application AS. Another AS shown above is Resource List Server (RLS), which provide a URI list service for SUBSCRIBE request. Here the Resource list is a presence list which contains a list of all presentities a watcher is subscribed to. Most of the presence interface just map form existing SIP or Diameter and have a name start with a “P”(e.g. Pw, Pi, Px).Pen is a special interface between PUA(AS) and PA(AS). Ut is new interface between IMS terminal and any AS using XCAP protocol. It allows user to get involved in configuration and data manipulation.

Figure below shows that an IMS terminal acts a PUA to publish its presence to PA.

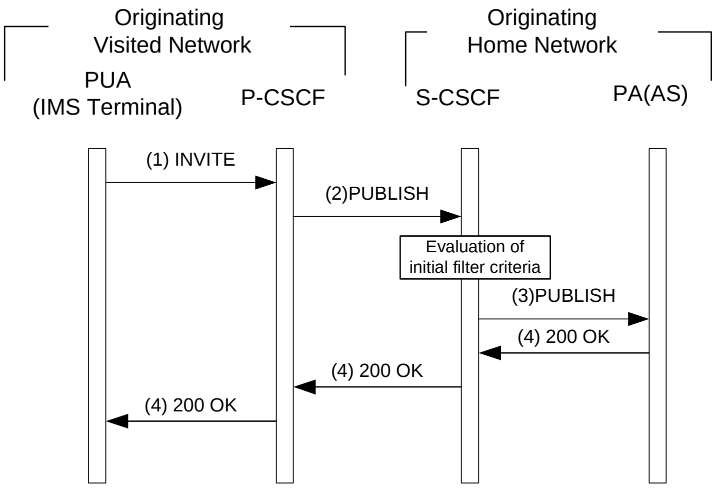


Figure 55 Publishing presence in IMS

Sequence below shows an IMS terminal acts a Watcher to subscribe presence information of presentity from PA. This sequence is presence without RLS service. Sequence with RLS service can be found at [5.2].

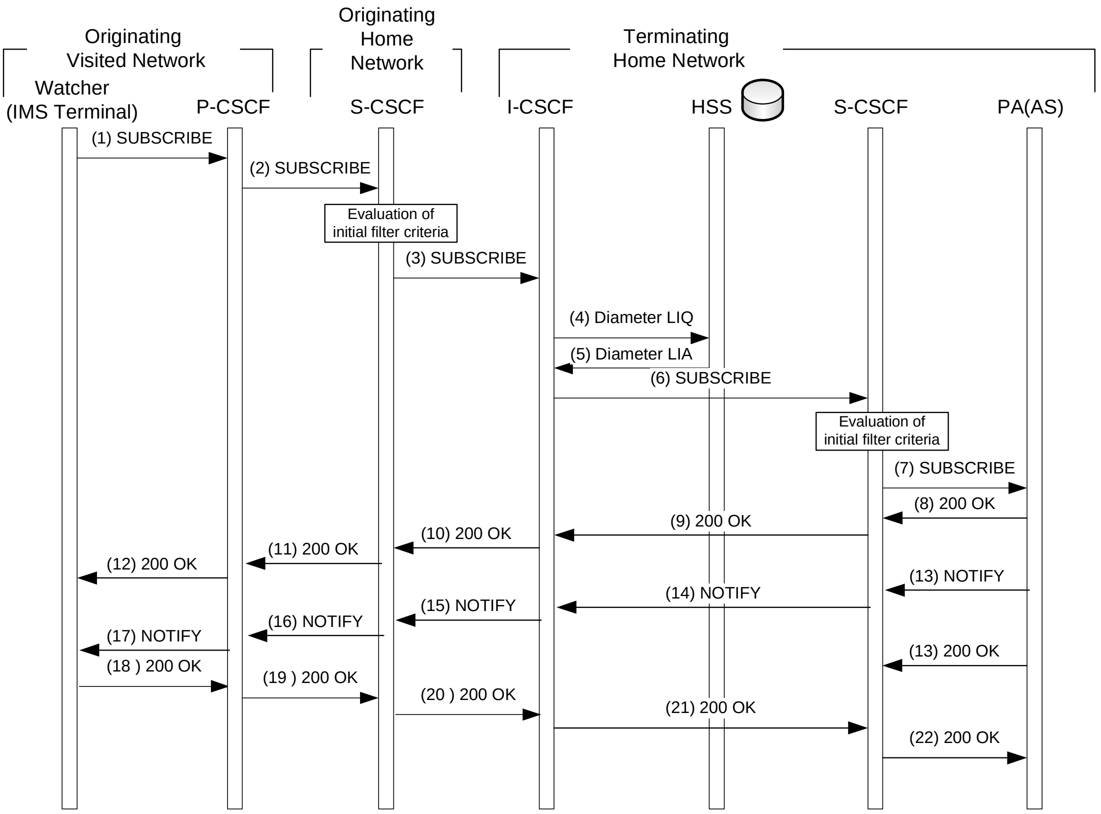


Figure 56 Presence subscription in IMS

Interoperability Discussion

From the above studying, we can see presence service in non-IMS network and IMS network use the same standard for presence publication, subscription and notification. Furthermore, both IETF and 3GPP use the same presence optimizations standard to solve bandwidth problem and terminal-roaming problem for wireless device. Hence it seems presence interoperating between IMS and non-IMS should be OK.

Appendix E - State of the art NAT traversal study

Evaluate Firewall/NAT

Now almost all the enterprises have firewalls and most of them have NAT as well. It is no doubt that enterprises should have firewalls for security. As for NAT (short for Network address translation) , it is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. It is located where the LAN meets the Internet, and makes all necessary IP address translations. NAT can hide the internal IP address for security and is a way to resolve limited
IP addresses in IP v4.

While firewall and NAT traversal gives enterprises more security and cost efficiency, it brings some problems for VoIP/SIP solution for enterprises. Like normal telephony, SIP based communication is two way communication. But for typical firewalls, external client (from un-trusted, public domain) initiated communication will be blocked. The SIP client behind NAT may have problem to communicate with external clients because the routing path of SIP signaling is different from the path of media flow. This document will discuss these issues in details. [E.1]

There are four different types of NAT:
The descriptions of the four types of NAT are from RFC 3489[E.2]:

Full Cone:
A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Basically, a private host is fully readable for outside hosts through a one-to-one mapping of private + public addresses.

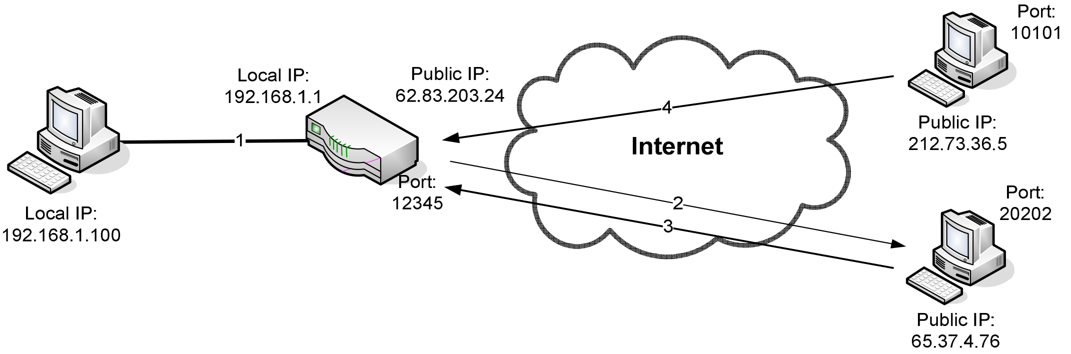


Figure 57 Full Cone NAT

Restricted Cone:
A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an

external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

This version is basically the same, except for this increased security mechanism.

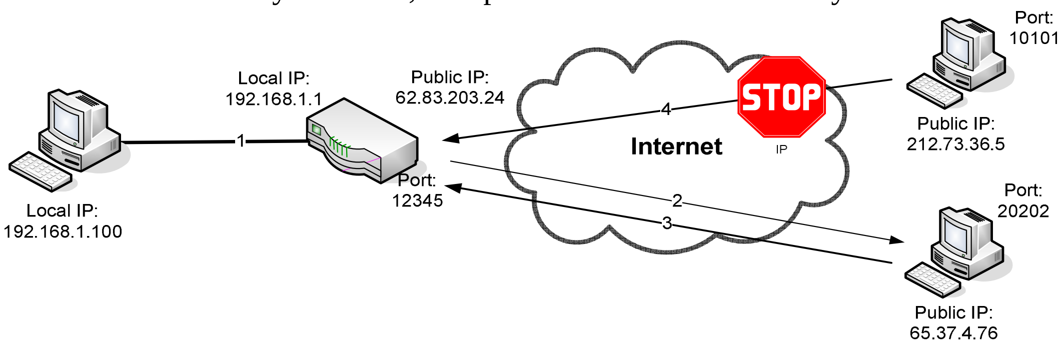


Figure 58 Restricted Cone

Port Restricted Cone:
A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

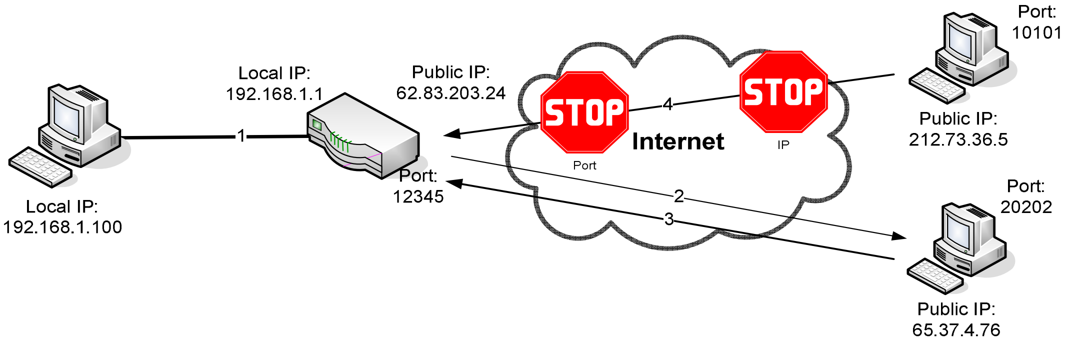


Figure 59 Port Restricted NAT

Symmetric:
A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a packet back to the internal host.

The mapping is done on a “per connection” basis.

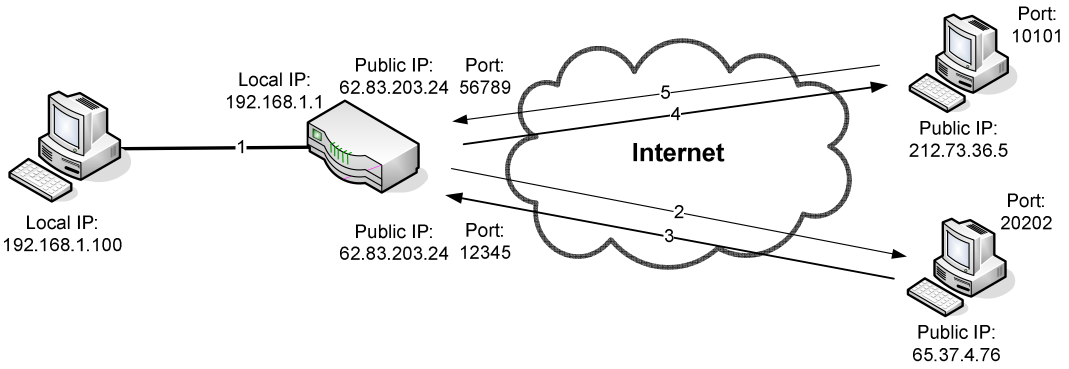


Figure 60 Symmetric NAT

Firewall/NAT traversal

Manual Configuration

One obvious solution is to configure the private computers behind the NAT with different info of what IP’s and ports it will use for connecting to internet. And in the same way configure firewall/NAT with a table that will allow the different clients to communicate with the world.

Universal Plug and Play (UPnP)

This technology is targeted for the small office and home installations.
We have already discussed that the RTP messages uses private IP address when it uses this public address information. UPnP discovers the public IP/port and uses this directly in the client to send information. To make this work both the client and NAT equipment need to have the UPnP feature.

UDP Hole Punching

UDP hole punching enables two clients to setup a direct peer-to-peer UDP session with the help of a well-known third party server. The server has to be trusted and have a valid public IP. This is the technology behind STUN and TURN which we will discuss later.
When the client log on to the server, it will pass on two sets of addresses. Both addresses belong to the client requesting the logon. The address consists of an IP-address and a UDP port. The first address is the client’s private address, or the address it has inside the private network. The second is the public address the client actually uses on the public network after the NAT router has translated them.

Client A wants to make a peer-to-peer connection with Client B; Client A sends a request to Server S. Server S sends B’s private and public address information to A, and A’s private and public address information to B.
If this is a full cone network they can initiate the communication to each other immediately. The clients will try both the public and private address. The first address that sends information back will be used. The private address may seem a bit redundant when we have the public. But it will help performance and security when both clients reside behind the same NAT.

If this is a restricted cone NAT or port restricted cone NAT the first request in the direction of the passive client will be blocked. The active client is the client that initiates the request to Server S. (Client A in this scenario):

Client A initiates the request to Client B. But because of delay, Client B isn't ready to send the request to A. Therefore NAT B will block any attempt from A to reach B. [E.3]

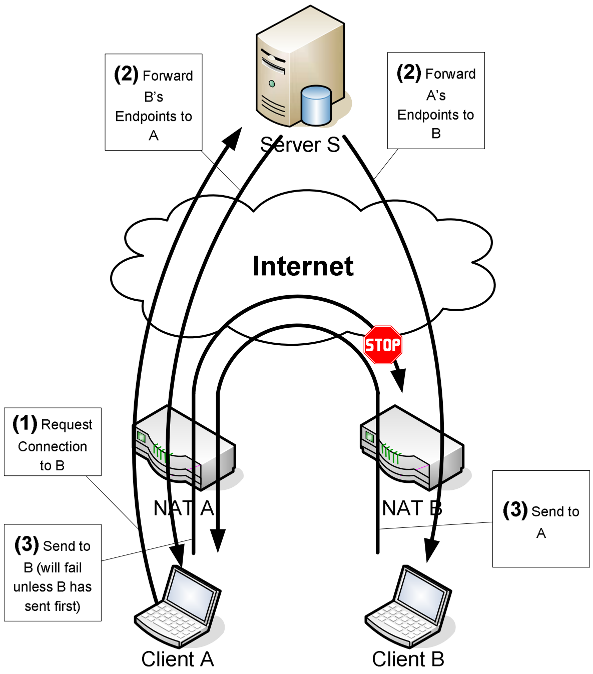

(2) Forward B's Endpoints to A
Server S
(2) Forward A's Endpoints to B
Internet
STOP
(1) Request Connection to B
NAT A
NAT B
(3) Send to A
(3) Send to B (will fail unless B has sent first)
Client A
Client B

Figure 61 UDP Hole Punching

Simple Traversal of UDP over NATs (STUN)
(Based on UDP hole punching)
STUN is a network protocol allowing clients behind NAT (or multiple NATs) to find their public address and the type of NAT it is behind. STUN will use the internet side port associated with the NAT and a particular local port. This information is used to set up UDP communication between two hosts that are both behind NAT routers.

STUN will work with three of four main types of NAT; full cone, restricted cone, and port restricted cone. It will not work with symmetric NAT (also known as bi-directional NAT) which is often found in the networks of large companies. Symmetric NAT unlike the other NAT solutions because it create a mapping based on destination address/port as well as source address/port.
The address of the VoIP client that will be receiving the data is different from that of the STUN server. The NAT table will then make a new entry on a different port for outgoing traffic. This will be different from the data in the call establishment message and the call will fail because of this. To make up for this STUN will accept data from any public IP address on the specified port. This again conflicts with the firewall policy of most system administrators. And therefore will not be accepted. [E.4]

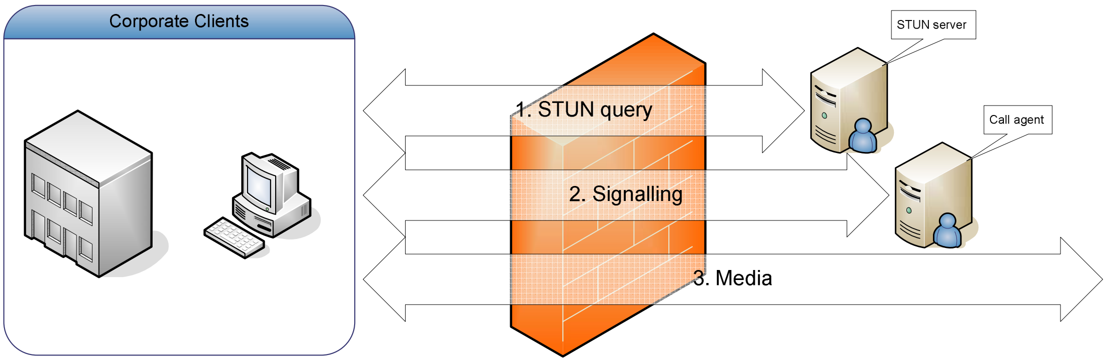


Figure 62 STUN

Traversal Using Relay NAT (TURN)

(Based on UDP hole punching)
TURN was released by the IETF to solve the issues STUN had with Symmetric NAT. As you can see from the picture below, TURN places itself in the middle of the SIP/RTP path. Like with STUN the client sends a request for the public IP and port, and uses this for the rest of the session. [2.15]

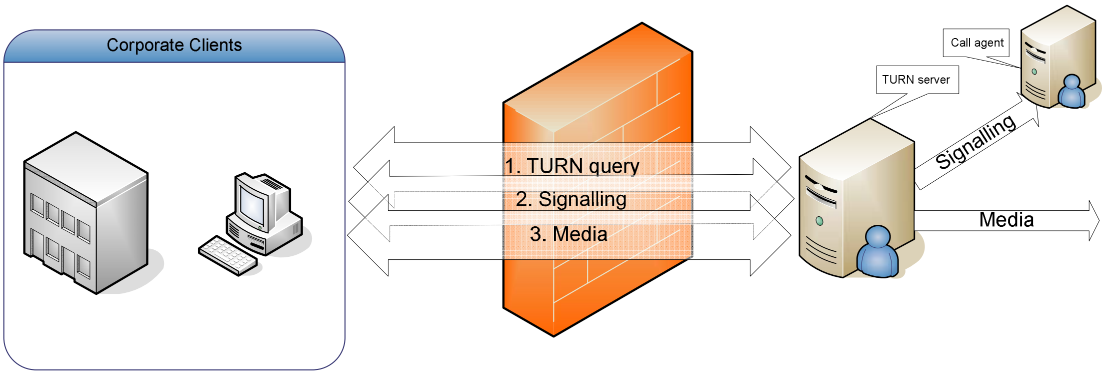


Figure 63 TURN

Application Layer Gateway (ALG)

What if we upgraded the NAT/firewalls to understand the different types of signaling and their relationship with other media flows? This is called an Application Layer Gateway.

Basically a NAT with inbuilt ALG can rewrite information within the SIP messages and can hold address bindings until the session has been terminated. [2.15]

Tunnel Techniques

This method requires a private network server and a public network server. A tunnel will be setup between them and all SIP traffic will be carried thru that tunnel. The external server will change the address labels so the traffic will be routable back to the destination. The server will also make incoming calls available, by use of the same tunnel to carry the traffic back to the internal server. [2.15]

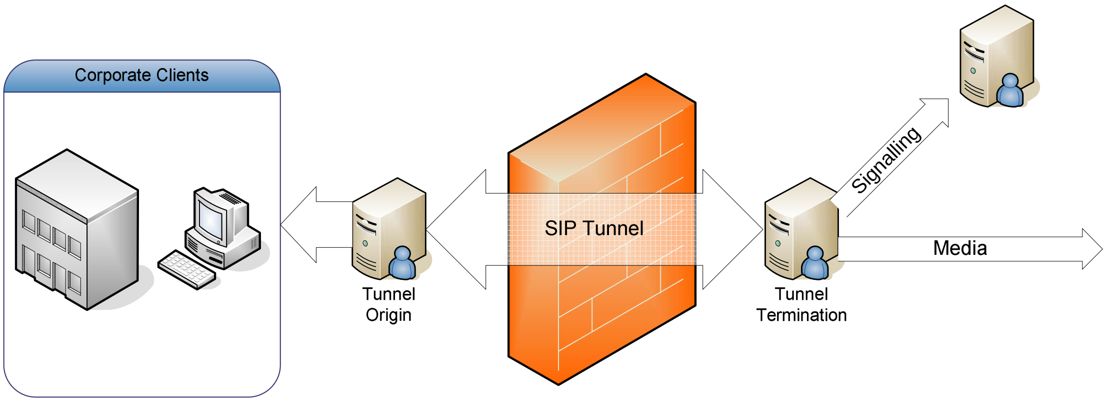


Figure 64 SIP Tunnel