IPv6@ESTG-LEIRIA: VOIP OVER IPV6

HUGO OLIVEIRA, ANTÓNIO PEREIRA, MÁRIO ANTUNES, NUNO FONSECA

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO DE LEIRIA – ESTG

Morro do Lena – Alto do Vieiro, 2401-951 Leiria, Apart. 3063

Tel. +351 244820300, Fax. +351 244820310, http://www.estg.ipleiria.pt

Email: eic08705@student.estg.ipleiria.pt, apereira@estg.ipleiria.pt ,

mario.antunes@estg.ipleiria.pt , nfonseca@estg.ipleiria.pt

Abstract **- This article presents a method for the integration of Voice over IPv4 (VoIPv4) solution over an IPv6 backbone, using translation mechanism IPv4 to IPv6 know as the GRE tunnel. Quality of service (QoS) was also tested on the IPv6 backbone, because voice over IP is very sensitive to traffic that passes through the IPv6 network. The solution for the QoS used was traffic prioritization. Another scenario, is the implementation of a native Voice over IPv6 (VoIPv6) solution using an Open Source solution. Finally, the presentation of results of the implementation of these scenarios.**

Keywords: **IP telephony, Protocols, Voice over IP; QoS; IPv4 to IPv6 translation mechanisms**

1. INTRODUCTION

IP telephony has came a long way, and in these last few years, there has been a great boom in its utilization, because it's cost effective, on both Local Area Network (LAN) and Wide Area Network (WAN) (especially for external phone calls). Thanks to broadband, applications like audio and video (bandwidth on demand) are now possible, and have better quality. Traditional services like fax and Plain Old Telephone Service (POTS) telephony can be integrated over the IP network. The Session Initiation Protocol (SIP) can easily be integrated for the Internet, and is responsible for session initiations of audio (especially VoIP), video, instant messaging, and other formats.

The Cisco Systems [1] company has its own session control protocol, called the Skinny Client Control Protocol or SCCP, but they also support SIP, and other protocols, like the H.323. The H.323 is important for the interoperability of legacy telephony like Integrated Services Digital Network (ISDN) and POTS.

Implementing IP telephony is easy because it uses the existing IP infrastructure of the institution or company.

Nowadays, voice over IPv6 still has a long way to go, Cisco Systems for example, does not support IPv6 on any of its VoIP solutions. There are no or very few commercial solutions for VoIPv6. However there are one or two Open Source servers (IPTEL [2] and VOCAL [3]) that use the SIPv6 protocol. There are very few SIPv6 terminals most of them are difficult to install, and are full of application bugs.

2. TECHNOLOGY AND IP TELEPHONY PROTOCOLS

This section will describe the basic components of IP telephony and their protocols. There are two types of IP telephony protocols, the signalling protocols and transport protocols.

2.1. BASIC COMPONENTS [5]

An IP Telephony infrastructure usually consists of different types of components. This section gives an overview of typical components without describing them in a protocol-specific context.

Terminal - A terminal is a communication endpoint that terminates calls and their media streams. Most commonly, this is either a hardware or a software telephone (installed on the computer) or videophone, possibly enhanced with data capabilities. There are terminals that are intended for user interaction and others that are automated, e.g., answering machines. This equipment needs an IP address to work.

Server - Placing an IP Telephony call requires at least two terminals, and the knowledge of the IP address and port number of the terminal to call. Obviously, forcing the user to remember and use IP addresses for placing calls is not ideal and dynamic IP addressing schemes (DHCP) make this requirement even more intolerable. As mentioned before, terminals usually register their addresses with a server. The server stores these telephone addresses along with the IP addresses of the respective terminals, and is thus able to map a telephone address to a host.

Finally, a telephony server is responsible for authenticating registrations, authorising calling parties and performing the accounting.

Gateways - are telephony endpoints that facilitate calls between endpoints that usually would not interoperate. Usually this means that a gateway translates one signalling protocol into another (e.g. SIP/ISDN signalling gateways), but translating between different network addresses (IPv4/IPv6) or codecs (media gateways) can be considered gatewaying as well. Of course, it is possible that multiple functionalities exist in a single gateway. Finding gateways between VoIP and a traditional PBX is usually quite simple.

Gateways that translate different VoIP protocols are harder to find. Most of them are limited to basic call functionality.

Figure 1 show a scenario with each of theses basic components mentioned (server, terminal and gateway).

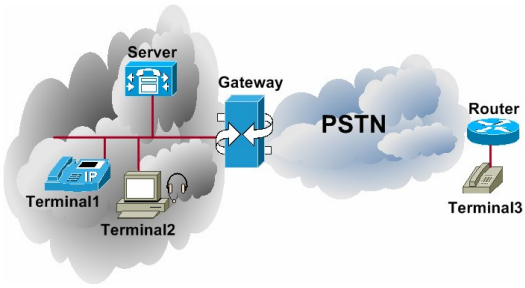

Figure 1 IP telephony components

2.2. PROTOCOLS

There are two types of telephony protocols, the signalling protocols and the transport protocols. The next figure show terminals A and B, and the server C. When terminal A wishes to communicate with terminal B, he needs to inform C that he wishes to speak with terminal B, and get the call to be established between them. Because terminals A and B are register on C, C can then contact terminal B and say that A is calling him.

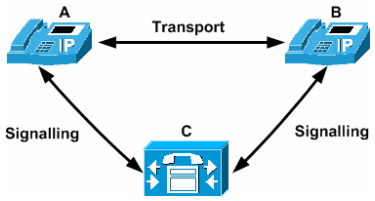

Figure 2 IP telephony protocols

The signalling protocol always is exchange between the IP telephony server (like the Call Manager) and the terminals. After the session has been established, communication is point-to-point between terminals, for the carry audio using the Real Time Protocol (RTP).

In 1995, the first VoIP product reached the market, with the objective of reducing costs. The most relevant signalling protocols are the following:

- Session Initiation Protocol (SIP)
- Skinny Client Control Protocol (SCCP)
- H.323

Other:

- Media Gateway Control Protocol (MGCP)
- H.248/Media Gateway Control (MEGACO)

As mentioned earlier, the signalling protocol is only to initiate the session, then the transport protocol use to transport media like the *Real-Time Transport Protocol* (RTP), *Real-time Transport Control Protocol* (RTCP), and *Resource Reservation Protocol* (RSVP).

Signalling Protocols

SIP [6] - The Session Initiation Protocol (SIP) is client-server session signalling protocol. The sessions range from audio (or VoIP), video, instant messaging, and many other formats. That is why it has been widely used, because it resembles the web protocols like the Hypertext Transfer Protocol (HTTP). Therefore, it is a text-based protocol, which makes it easy for developers to write application and service providers to deploy services.

SIP was designed by IETF as a multimedia protocol that could take advantage of the IP service model architecture.
A SIP address is a type of *Uniform Resource Identifier* (URI) called a SIP URI. It has a similar form to an email address, and so the Universal Resource Locators (URLs) are used as address data format. The general form of a SIP URI is:

sip: user:password@host:port;uri-parameters?headers

SIP also uses SDP, SDP is used for describing multimedia session for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. SDP was standardized by IETF. SDP conveys sufficient information in a multimedia session in a textual format. SDP includes description of:

- Media to use (audio or video, codec, sampling rate, and transport protocol)
- Media destination (IP address and port number)
- Session name and purpose
- Times the session is active
- Contact information

Because SIP is based on URL, so Domain Name Systems (DNSs) is needed and the Telephony Routing Over IP (TRIP) is used for routing the calls.

The Cisco's Skinny protocol - The Skinny Client Control Protocol (SCCP) is used by Cisco's IP telephony products, like the Cisco's Call Manager and Cisco's IP phones. Their is another server that supports this protocol the Asterisk server.

The Skinny client uses the TCP/IP protocol and port number 2000 to establish and terminate the calls and uses RTP/UDP/IP to transport multimedia information to the Skinny clients or H.323 terminals. A gateway is necessary used to guarantee interoperability between Skinny and H.323 equipments.

H.323 [7] - H.323 is an International Telecommunications Union-Telecommunications (ITU-T) standard that defines a packet-based multimedia communications system. H.323 defines a distributed architecture for transporting multimedia applications over LANs. Because of its early availability and its evolution to address the needs of VoIP, H.323 is currently the most widely used VoIP signalling and call-control

protocol. International and domestic carriers rely on H.323 to handle billions of minutes of use each year.

H.323 is considered an umbrella protocol because it defines all aspects of call transmission. H.323 defines the Registration, Admission, and Status (RAS) protocol for call routing, H.225 protocols for call set-up, and H.245 protocols for capabilities exchange. H.323 is based on the Integrated Services Digital Network (ISDN) Q.931 protocol, which allows it to easily interoperate with legacy voice networks such as the PSTN and Signalling System 7 (SS7).

Transport Protocol

Real Time Transport Protocol (RTP) [6] - RTP is an end-to-end protocol and provides various mechanisms for the transmission of multimedia data such as video and audio streams. It is network and transport protocol independent; however it is used over UDP. RTP can be used over both unicast and multicast network services, where the network is responsible for transmitting the data to multiple locations.
It is used by session protocols like SIP, H.323 and SCCP.

3. Transition Mechanisms

The IPv6 protocol was developed a few years ago, by the Internet Engineering Task Force (IETF) and is gaining maturity in the core networks, but only recently, implementations for voice are available. In the future, IPv4 will no longer be the core of the internet, and there will be more networks using IPv6. In the meantime, it is necessary to integrated IPv4 services in IPv4 networks, so that they can coexist. There are many methods explain in RFCs, but there are not many implementations out there. The RFC 4213 (October of 2005) “Basic Transition Mechanisms for IPv6 Hosts and Routers” specifies the mechanisms for compatibility with IPv4, implemented on hosts and Routers IPv6. There are two mechanisms specified on this RFC dual stack and tunnelling. The RFC 2185 specifies routing in the infrastructures and the RFC 2473 specifies the techniques of tunnelling. Other mechanisms are specified on the RFC 2529.

This Project only implemented a GRE tunnel.

GRE [9] - O GRE (Generic Routing Encapsulation) is a protocol used for tunnelling, developed initially by Cisco Systems, this protocol encapsulates one layer three (network layer of the OSI model) protocol in another. For example is possible to transport multicast traffic IPv6 in unicast IPv4 networks.

A GRE encapsulated packet has the form:

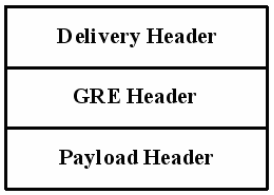

Figure 3 Structure of the GRE encapsulation

All the packet headers can be divided into three headers the Delivery header, GRE header, and Payload Header.

The Delivery header is responsible for transporting the entire packet to its destination. The GRE header is the intermediate header. The Payload Header has the protocol that needs transporting by the delivery protocol.

When the IPv4 protocol is transported in the payload of the GRE, the Protocol type field must have the value 0x800.

This protocol is specified in the following RFCs: RFC 2784 RFC1701 RFC2784 and RFC 2460.

Figure 4 show an example of a GRE encapsulation, with an IPv4 over IPv6 encapsulation.

The IPv6 protocol is responsible for transporting the IPv4 protocol. Only when the packet reaches the other end of the packet, the packet is unencapsulated and IPv4 header used.

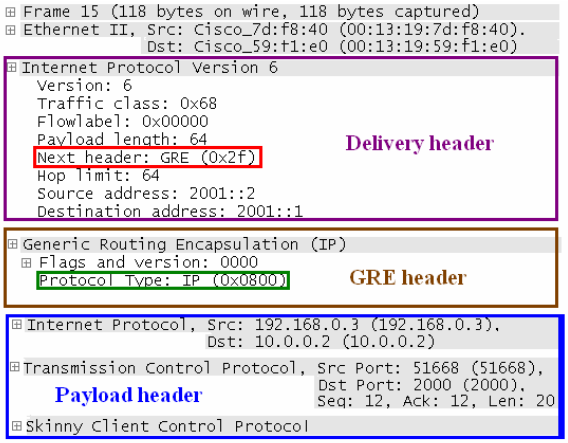

Figure 4 Example of a GRE encapsulation

4. QoS

The Internet Protocol IP is responsible for the success of the internet, and offers best effort (BE) for the packets and is able to work on any type of media, and platform. Applications like streaming of video, voice over IP (VoIP), e-mail, and other need Quality of Service (QoS). There are different parameters to consider latency, jitter, bandwidth, packet loss, and availability.

QoS for IPv6

QoS for IPv6 is divided in to fields: the Traffic Class field ad the Flow label field. The first one is for DiffServ and the second one is for IntServ. The Traffic Class field has the same functionally as the Type of Service for IPv4.

4.1. RESTRICTIONS FOR QOS FOR IPV6 ON CISCO IOS[1]

The following QoS features are supported on Cisco's IOS for managing IPv6 traffic [13] :

Supports:

- Packet classification
- Queuing with **LLQ** support
- Traffic shaping
- WRED
- **Class-based packet marking, CBWFQ**
- Policy-based packet marking

Doesn't support:

- Compressed Real-Time Protocol (CRTP)
- Network-Based Application Recognition (NBAR)
- Committed Access Rate (CAR)
- Priority Queuing (PQ)
- Custom Queuing (CQ)
- RSVP
- IP RTP priority

Traffic prioritization [14]

In choosing from the many available prioritization schemes, the major factors to consider include the type of traffic involved and the type of media on the WAN. For multi-service traffic over an IP WAN, Cisco recommends low-latency queuing (LLQ) for all links. This method supports up to 64 traffic classes, with the ability to specify, for example, priority queuing behaviour for voice and interactive video, minimum bandwidth class-based weighted fair queuing for voice control traffic, additional minimum bandwidth weighted fair queues for mission critical data, and a default best-effort queue for all other traffic types.
Figure 5 shows an example prioritization scheme.

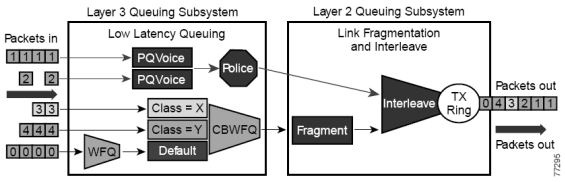

Figure 5 Optimized Queuing for VoIP over the WAN

Cisco recommends the following prioritization criteria for LLQ:

• The criterion for voice to be placed into a priority queue is the differentiated services code point (DSCP) value of 46, or a per-hop behaviour (PHB) value of EF.

• The criterion for video conferencing traffic to be placed into a priority queue is a DSCP value of 34, or a PHB value of AF41. However, due to the larger packet sizes of video traffic, these packets should be placed in the priority queue only on WAN links that are faster than 768 Kbps. Link speeds

below this value require packet fragmentation, but packets placed in the priority queue are not fragmented, thus smaller voice packets could be queued behind larger video packets. For links speeds of 768 Kbps or lower, video conferencing traffic should be placed in a separate class-based weighted fair queue (CBWFQ).

Note: One-way video traffic, such as the traffic generated by streaming video applications for services such as video-on-demand or live video feeds, should always use a CBWFQ scheme because that type of traffic has a much higher delay tolerance than two-way video conferencing traffic

• As the WAN links become congested, it is possible to starve the voice control signalling protocols, thereby eliminating the ability of the IP phones to complete calls across the IP WAN. Therefore, voice control protocols, such as H.323, MGCP, and Skinny Client Control Protocol (SCCP), require their own class-based weighted fair queue. The entrance criterion for this queue is a DSCP value of 24 or a PHB value of CS3.

5. TESTS

This section will explain the results of tests made during the Project.

5.1. IMPLEMENTATION OF A GRE TUNNEL "4TO6"

The objective of this scenario is the implementation of a GRE tunnel, verification of the encapsulation process and overhead. The GRE tunnel "4to6" is support in the Cisco IOS version 12.3(7)T, 12.4 or 12.4(2)T.

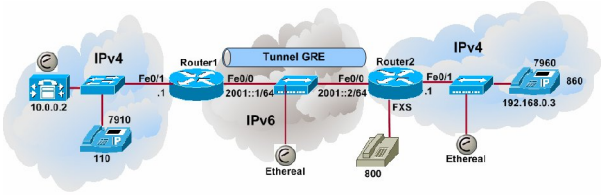

Figure 6 GRE tunnel IPv4 over a IPv6 backbone

To determine the overhead, Ethereal was used to capture the packets. Figure 6 describes where Ethereal was installed.

Ethereal was installed half way thought the tunnel and at the Call Manager and between the IP phone 7960 and Router2 (by means of a hub).

Results – During the GRE encapsulation process, the value of the Differentiated Services (DSCP or TOS – IPv4) field of IPv4 is copied to the Traffic Class field of IPv6. So it's not necessary to mark the packet for QoS on the Router. The process has the following order in terms of protocols:

RTP, UDP, IPv4, GRE, IPv6, Ethernet.

[1] Nas versões 12.2(13)T, 12.3, 12.3(2)T, 12.0(28)S , 12.4, 12.4(2)T

GRE Overhead – There are two more headers the IPv6 header and the GRE header. The IPv6 header occupies 40 bytes and the GRE header occupies 4 bytes, which gives a more 44 bytes than the original IPv4 frame.

QoS test on the scenario

Figure 7 was implemented to test QoS. Chariot was used to generate streams VoIPv4, and MGEN was used to generate IPv6 traffic for best effort. MGEN was used because Chariot doesn't support IPv6 on version 4.1.

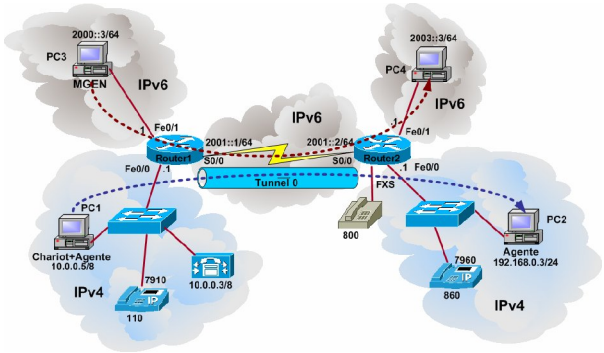

Figure 7 QoS test over the GRE tunnel

All the IPv4 traffic will suffer encapsulation and pass though the tunnel interface, and all the IPv6 traffic will pass thought the serial interface.

The tunnel interface is a logical interface that uses the serial link, so all policies are applied to the serial interface.

Traffic is always generated from Router1 to Router2, so Router1 is a bottleneck. Router1 will be the one discarding packets in case of congestion.

For this scenario, two queues were created. The first queue is for the RTP protocol (any packets marked with value DSCP EF or 46). The second for the signalling protocol in this case Skinny (packets marked with DSCP/PHB value 26/AF31 or 24/CS3).

Bandwidth was allocated for each of theses queues.

The bandwidth for RTP protocol defers depending on the codec used, for the Cisco IP phones use the G.729 codec. Not forgetting the overhead caused by the GRE encapsulation, it's possible to determine the bandwidth by the following formula.

Normally the packet will have 74 bytes, but because of the overhead which is 44bytes. The frame will have 118 bytes instead of 74 bytes.

BW (RTP) = 74 (size of the frame in bytes)*8 bits per byte*50PPS = 29.6 Kbps (outside the tunnel)

BW (RTP) = 118 (size of the frame in bytes)*8 bits per byte*50PPS = 47.2 Kbps (inside the tunnel)

The signalling protocol needs less bandwidth, and because there is no encryption, the bandwidth is calculated in the following manner:

BW (skinny)(bps) = 265 * (nº of IP Phones and gateways)

On Cisco Router is only possible to allocate at least 8kbps, so that's the value used.

Call Admission on the Call Manager is important because when allocating bandwidth for N voice stream, if there is congestion it not possible to have N+1 voice streams. If there are N+1 streams there will be no QoS because of congestion in the LLQ queue.

Results – Various tests were performed on a 256 kbps link, with 1, 2, 3 e 4 streams VoIP (Chariot) generated. Traffic best effort (BE) was generate for each test using MGEN and with the following values: 64kbps, 128kbps, 256kbps and 512kbps. The following table shows the results for test with three VoIP streams.

Packet loss (voice)	Average Jitter (ms)	MGEN BE (throughput in kbps)	Drop rate BE on router1 (bps)
0	7.078	64	0
0	10,675	128	31000
0	10,536	256	100000
0	11,530	512	260000

Table 1 Three voice streams generated on Chariot NetIQ

Available BW BE (without BE traffic) = totalBW - *priority* +BW for signalling = 256-150=106

Effective BW = available BW BE – MGEN traffic =106-64=96 kbps (a positive value indicates that there are any losses because the is still bandwidth available, as we can see from table 1 this value was expected)

Effective BW = available BW BE – MGEN traffic = 106-128= **- 22 kbps** (negative value indicate that there is no bandwidth available, so there will be losses, the results from table 1 have losses and were expected).

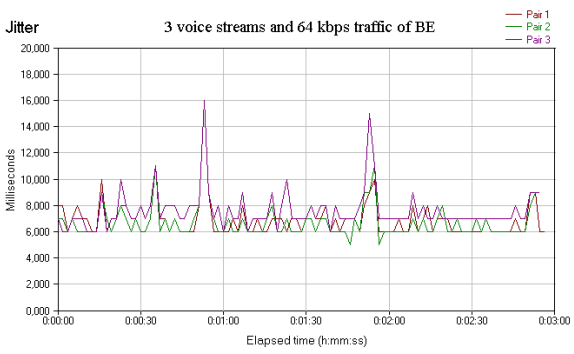

Figure 8 Jitter, 3 voice streams and 64kbps traffic of BE

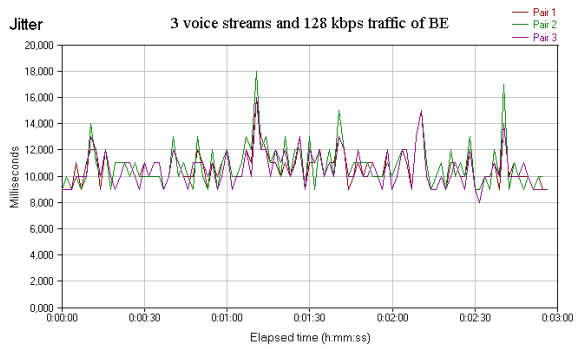

Figure 9 Jitter, 3 voice streams and 128 kbps traffic of BE

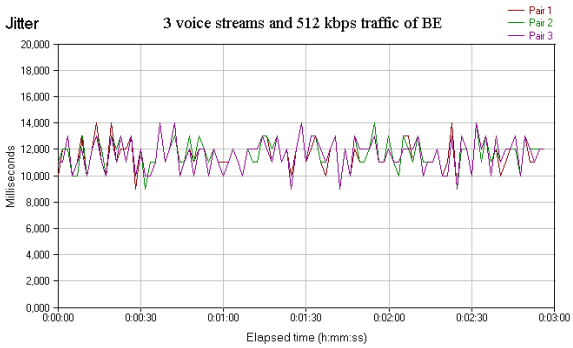

Figure 10 Jitter, 3 voice streams and 512 kbps traffic of BE

The test performed with four streams isn't presented in this article and shouldn't be used in a real scenario, because it exceeds the 75% of the total bandwidth available, Cisco [15] recommends it (in this case 190+8=198/256=77%).

The jitter value in all the tests never passed 15 ms, the maximum value was 18 ms. The standard ITU-T G.114, says that jitter may between 20 to 50 ms, giving good results.

At the end of each test the command **sh policy-map interface serial 0/0** was executed on the Router1, to check the drop rate of the BE traffic, and on the voice class. No losses where found for the voice class on the Router1, nor on Chariot.

5.2. IMPLEMENTATION OF A VOIPV6 SCEANRIO

The SIP protocol uses a distributed architecture, but also supports point-to-point communication, but there are many advantages of having a server, because of the authentication of users and other many other features.

For the native VoIPv6 scenario, a SIP Express Router (SER) of IPTEL, and Linphone soft phones as terminals were installed on a Linux (Fedora Core 4) operating system. DNSv6 was installed, because on the soft phone didn't support and crashed when using the static IPv6 address, only the SIP URI worked so DNSv6 was mandatory.

Linphone [16] only supports VoIP and instant messaging. The SIP Communicator supports also video. There are two versions of the SIP communicator

The older version is available on this site (see ref.)[17], and another version is being developed (see ref.) [18].

Linphone version 1.2 was used, version 1.1 doesn't work with IPv6. In the next figure we have theVoIPv6 scenario.

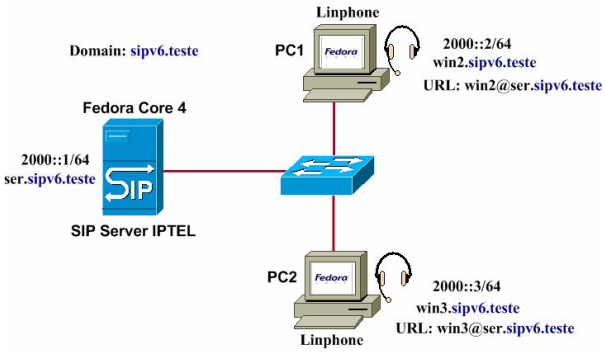

Figure 11 The native VoIPv6 scenario

Ethereal was installed on each computer to determine the messages exchange.

Results – The skinny messages are Exchange between the CallManager and the terminals, the RTP messages are exchanged point-to-point. In the following figure, we also can see SIP/SDP messages.

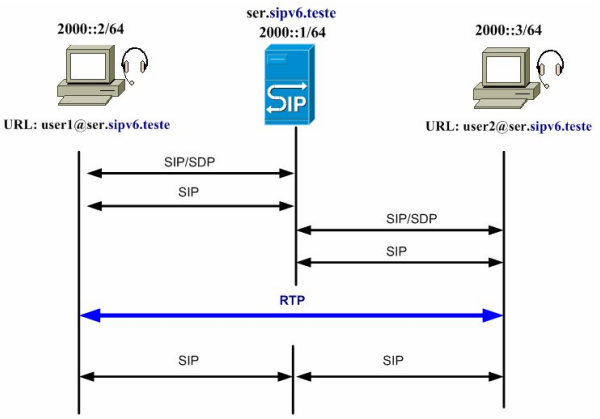

Figure 12 SIP messages

6. CONCLUSION

This article briefly explained the VoIP architectures, QoS mechanisms and its support for IPv6, and the implementation of scenarios. During the project VoIPv6, solutions using Open Source were investigated, because Cisco or commercial versions only support IPv4, in their voice solutions. During the project, all the VoIP messages were analysed when using Cisco and Open Source VoIP solutions. Lots of IPv6 to IPv4 translation mechanisms were investigated, but only GRE tunnel was chosen for implementation. After configuring the GRE tunnel, the encapsulation process was analysed and overhead accounted for. Because voice traffic is sensitive to traffic on the network, a QoS solution was investigate and configured for the scenario. To test QoS two software applications were used Chariot (to generate VoIPv4 streams) and MGEN (to generate IPv6 streams for Best effort).

Native VoIPv6 is still immature and only available on Open Source, there are project that analyse translation mechanisms IPv4 to IPv6 and vice-versa [20].

The SIP [21] protocol is very important because its very simple and offers a way to initiate session for audio (or VoIP), video, instant messaging, and other formats. The SIP protocol can be used in wireless equipments because it support mobility (VoIP telephone with WiFi) or mobile phones (UMTS), and IPv6 is mandatory. For example, the 3rd Generation Partnership Project (3GPP) specifies that IPv6 is mandatory. [19]

No one knows when Cisco will support IPv6 in the next years. The translation mechanisms can solve that problem but it is only a remedy, and not ideal solution, which is having native VoIPv6. The Japanese government has been investing allot on VoIPv6 solutions. The VoIPv4 solutions are more stable then IPv6 because they have been around for a longer time. They lots of service that work on IPv4, but to become stable in IPv6 will take a while.

In this project, lots of VoIPv6 solutions were investigated which can be consulted in the report of this project [4], mostly Open Source. Lots of the soft phones are a bit difficult to install, and the are full of bugs. There were two SIP server found one is IPTEL called SER and the another one is VOCAL, both Open Source. The Instituto Politécnico de Bragança [22] has implemented this server in there IPv4 network. Another advantage of theses Open Source solutions is that they are compatible with most vendors. For example, the Asterisk server is compatible with the Skinny protocol of Cisco Systems.

7. BIBLIOGRAFIA

[1] **Cisco Systems;** http://www.cisco.com
[2] **IPTEL;** http://www.iptel.org/
[3] **VOCAL;** http://www.vovida.org/
[4] OLIVEIRA, H. – Project report IPv6@ESTG-Leiria: VoIP over IPv6, 2006 (only the Portuguese version is available) www.ipv6.estg.ipleiria.pt
[5] IP Telephony Cookbook, Dr. Margit Brandl, Dimitris Daskopoulos, Erik Dobbelsteijn, Dr. Rosario Giuseppe Garroppo, Jan Janak, Jiri Kuthan, Saverio Niccolini, Dr. J ¨org Ott, Stefan Prelle, Dr. Sven Ubik, Egon Verharen, 9 March 9 2004,http://www.informatik.uni-bremen.de/~prelle/terena/cookbook/main/
[6] Design and Implementation of an OSA/Parlaycompliant Interactive Multimedia Response Unit for Mobile All-IP Networks, Adel Al-Hezmi, Berlin, November 2003
[7] Currículo da Cisco FWL capítulo 12 “Emerging Technologies”
[8] http://www.protocols.com/
[9] **[RFC1701]** Generic Routing Encapsulation (GRE) S. Hanks, T. Li, D. Farinacci, P. Traina, October 1994
[10] **[RFC 2460]** Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, December 1998
[11] **[[RFC2784]** Generic Routing Encapsulation D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000
[12] **[RFC2893]** Transition Mechanisms for IPv4 Hosts and Routers, R. Gilligan, E. Nordmark, IETF, August 2000
[13] http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_qosv6.htm
[14] http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/srnd4_1/ipt4_1/41nstrct.pdf
[15] Cisco IOS Quality of Service Solutions Configuration Guide,(chapter Congestion Management Overview)
[16] http://www.linphone.org/
[17] https://sip-communicator.dev.java.net/index_old.html
[18] http://sip-communicator.org/
[19] 3GPP TS 23.221 V6.3.0, 3rd Generation Partnership Project, June of 2004, http://www.3gpp.org/ftp/Specs/archive/23_series/23.221/.
[20] http://www.6net.org/
[21] [RFC 3261] obsoletes RFC 2543
[22] http://www.ccom.ipb.pt/voip/modules/voip/show_users.php