_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

CONFIGURACIÓN, IMPLEMENTACIÓN Y EVALUACIÓN DEL SERVICIO DE VOIP.

Álvaro Ortolá Gaona

Tutor: Juan Carlos Guerri Cebollada

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2016-17

Valencia, 12 de septiembre de 2017

Resumen

Este proyecto de fin de grado tiene como objetivo el estudio de Voz sobre IP. Se detallará todos los diferentes protocolos para su utilización, los parámetros a tener en cuenta como los códecs, retardos y pérdidas. Nos centraremos en analizar el protocolo SIP, los elementos SIP de red, los mensajes de dicho protocolo como también como se establece una sesión.
Se instalará en el laboratorio un servidor Asterisk para administrar una central telefónica de forma sencilla. Una vez instalado dicho servidor se realizarán distintas pruebas con ayuda del softphone Jitsi para poder estudiar los diferentes escenarios y así entender los distintos procesos y protocolos para una correcta realización de una llamada. Utilizaremos el Wireshark para la monitorización de los distintos medios y así poder detallar la calidad de servicio y la calidad de experiencia por el usuario. Se utilizará el programa NetLimiter y Clumsy para reducir el ancho de banda del programa y así analizar las perdidas y poder llegar a una conclusión optima del estudio.

Resum

Aquest projecte de fi de grau té com a objectiu l'estudi de Veu sobre IP. Es detallarà tots els diferents protocols per a la seva utilització, els paràmetres a tenir en compte com els còdecs, retards i pèrdues. Ens centrarem en analitzar el protocol SIP, els elements SIP de xarxa, els missatges d'aquest protocol com també com s'estableix una sessió.
S'instal·larà al laboratori un servidor Asterisk per administrar una central telefònica de forma senzilla. Un cop instal·lat aquest servidor es realitzaran diferents proves amb ajuda del softphone Jitsi per poder estudiar els diferents escenaris i així entendre els diferents processos i protocols per a una correcta realització d'una trucada. Utilitzarem el Wireshark per a la monitorització dels diferents mitjans i així poder detallar la qualitat de servei i la qualitat d'experiència per l'usuari. S'utilitzarà el programa NetLimiter i Clumsy per reduir l'ample de banda del programa i així analitzar les perdudes i poder arribar a una conclusió òptima de l'estudi.

Abstract

This end-of-degree project aims to study Voice over IP. All of the various protocols for its use will be detailed and the parameters to take into account such as codecs, delays and losses. We will focus on analysing the SIP protocol, the SIP network elements, the protocol's messages and also how a session is established.
An Asterisk server will be installed in the laboratory to easily manage a telephone centre. Once installed the server will perform different tests with the help of softphone Jitsi to be able to study the different scenarios and thus understand the different processes and protocols for a correct execution of a call. We will use the Wireshark for the monitoring of the various means and thus be able to detail the quality of service and the quality of user experience. The NetLimiter program and Clumsy will be used to reduce the bandwidth of the program and therefore analyse the losses and reach an optimal conclusion of the study.

ÍNDICE

Capítulo 1: OBJETIVO DEL PROYECTO.

A medida que van pasando los años se ha producido un elevado incremento en el uso de tecnologías de Voz sobre IP (VoIP), esta tecnología empezó a desarrollarse en 1973 cuando se implementó el protocolo Network Time Protocol, que permitía transmitir voz en tiempo real dentro de la red Arpanet, precursora de Internet. No obstante no fue a partir de 1995 cuando empezó a surgir los distintos protocolos de señalización de internet como H.323 o SIP. En 2004 comienza a proliferar una gran cantidad de aplicaciones, gratuitas como de pago, que permiten la transmisión de audio y vídeo a través de Internet dando lugar a la comunicación entre millones de personas en todo el mundo con un coste económico bajo.

Actualmente en España la VoIP está experimentando un crecimiento notable gracias, sobre todo, al aumento del ancho de banda, a la pérdida del miedo de los consumidores y al interés por el ahorro que ofrecen las llamadas telefónicas utilizando operadores IP.

El objetivo de este proyecto es la instalación de un servidor Asterisk que permite ejecutar, configurar y administrar una Central Telefónica de forma rápida y sencilla.
Se utilizará un softphone gratuito para poder realizar las distintas comunicaciones entre los usuarios y así poder estudiar los distintos escenarios y protocolos intervenidos, concretamente nos centraremos en analizar el protocolo SIP (Session Initiation Protocol).
Una vez realizado los distintos escenarios se monitorizará con Wireshark los distintos procesos para la correcta realización de la llamada y así poder estudiar la calidad de servicio (QoS) y la calidad de experiencia (QoE) del usuario.

Además, la realización de este proyecto tiene como objetivo una función educativa debida que los futuros alumnos podrán realizar distintas pruebas en el laboratorio y así asentar los distintos conocimientos adquiridos en clase sobre VoIP.

Capítulo 2: SIP

2.1 VoIP:

El principal objetivo es analizar los distintos protocolos de internet que permiten que la señal de voz viaje a través de internet empleando el protocolo IP.
VoIP (Voice Over Internet Protocol) permite enviar la señal de voz en paquetes de datos, en vez de enviarla de forma analógica como estaba siendo utilizada la telefonía convencional y empleará un conjunto de recursos para que la señal de voz viaje a través de Internet utilizando el protocolo IP (Protocolo de Internet).

Los elementos que dispone una red de VoIP son:

- **Cliente:** será el responsable de originar y establecer las llamadas. La información será recibida a través del micrófono del usuario y codificada, se empaquetará para después decodificarla y reproducirse.
- **Servidor:** se encargará de las operaciones de base de datos. Dichas operaciones pueden ser la contabilidad, la recolección, el enrutamiento, la administración y control del servicio, el registro de los usuarios, etc.
- **Gateways:** puente de unión entre todos los usuarios, su función principal es la de proveer interfaces con la telefonía tradicional adecuada, la cual funcionara como una plataforma para los clientes.

2.2 Protocolos de VoIP:

- **H.323:** es un conjunto de estándares creado por ITU-T para la propagación de voz, vídeos y datos multimedia sin proporcionar calidad de servicio a través de redes basadas en conmutación de paquetes.Es el estándar que más difusión cuenta en telefonía IP. Dicho protocolo en un inicio se diseñó para transportar voz y vídeo en redes de área local pero posteriormente se expandió a redes amplias como Internet.
  La arquitectura de H.323define componentes, protocolos, señalización y códecs que hacen posible la comunicación y garantizar la compatibilidad entre los dispositivos.
- **SIP:** Session Initiation Protocol (SIP) es un protocolo desarrollado por el IETF en 1999 utilizado para el dominio de llamadas multimedia y servicios telefónicos de VoIP. Tiene una estructura cliente/servidor basada en un modelo de petición/respuesta.
  Posteriormente se explicará con más detalle este protocolo debido a que será el utilizado para las pruebas del laboratorio.
- **Megaco o H.248:** complementa a H.323 y SIP. Se utiliza para que las Media Gateway puedan controlar las puertas de enlace para el soporte de llamadas de voz entre redes IP-IP o RTC-IP.
- **IAX:** actualmente se utiliza la versión 2 de este protocolo IAX2. Es utilizado para conexiones de VoIP entre servidores Asterisk, y entre servidores o clientes que utilizan IAX. Es un protocolo simple y requiere poco ancho de banda. Dispone de una multitud de códecs para audio como también permite manejar diversos streams multimedias en el mismo flujo, puede ser beneficioso para multiconferencias. El tráfico de datos va sobre UDP.

- **SKINNY:** muestra una arquitectura del tipo cliente servidor, utiliza el Call Manager que es un elemento encargado de realizar la gestión de las llamadas donde los clientes se conectaran a través de TCP y para el tráfico de datos utilizará RTP/UDP/IP. Actualmente es propiedad de Cisco y destaca por su ligereza por su reducida capacidad de procesamiento.

2.3 Parámetros de VoIP:

2.3.1 Códecs:

Para poder transmitirse la voz por la red IP habrá que codificarse, para ello se hará uso de códecs que asegurará la codificación y comprensión para después poder decodificarlo y descompresionar de forma adecuada. Según el códec que se utiliza en la transmisión, se utilizará mayor o menos ancho de banda. Los principales códecs utilizados para VoIP son:

- **G.711:** es un estándar utilizado para la codificación de audio en telefonía. Proporciona un flujo de datos de 56 kbit/s o 64 kbit/s.
- **G.723:** se utiliza sobretodo en VoIP debido al bajo requerimiento de ancho de banda. Suministra una tasa de 5.3 Kbit/s o 6.4 Kbit/s
- **G.729:** algoritmo de compresión de datos de audio que comprime en trozos de 10 milisegundos. Se utiliza en VoIP debido a su reducido requerimiento de ancho de banda. Opera a una tasa de 8 kbit/s pero también puede suministrar a 6.4 kbit/s y de 11.8 kbit/s para peor o mejor calidad.

2.3.2 Latencia o retardos:

El retardo es la cantidad de tiempo para que se transmita un paquete desde un punto de la red a otro, es decir, es la suma de los retardos siguientes:

- Retardo algorítmico: introducido por el códec usado y es inherente al algoritmo de codificación.
- Retardo de empaquetamiento: hace referencia al tiempo que se requiere para rellenar un paquete de información, es decir la carga útil del paquete sin cabeceras, con los datos ya codificados y comprimidos. Depende directamente del tamaño de trama definido por cada códec y el número de tramas por paquetes.
- Retardo de serialización: relacionado con la tasa del reloj de transmisión.
- Retardo de supresión de jitter: se debe al almacenamiento temporal del flujo de paquetes en un buffer del extremo receptor.
- Retardo de propagación: tiempo requerido por el paquete para llegar desde su origen al destino.
- Retardo de encolado: tiempo que esperan los paquetes almacenados en una cola de salida antes de ser transmitidos por la red.

Por debajo de los 150 ms una conversación se puede considerar aceptable, en caso contrario ya se produciría retardos importantes.

2.3.3 Pérdidas:

Frame Lost o Perdidas es debido a la congestión de la red o corrupción de datos las tramas se pueden perder. Además, para tráfico de tiempo real como la voz, la retransmisión de tramas perdidas en la capa de transporte no es práctico por ocasionar retardos adicionales. Por consiguiente, los terminales de voz tienen que retransmitir con muestras de voz perdidas, también llamadas Frame Erasures. El efecto de las tramas perdidas en la calidad de voz depende de cómo los terminales gestionen las Frame Erasures. [1]

En el caso más simple si se pierde una muestra de voz el terminal dejará un intervalo en el flujo de voz. Si muchas tramas se pierden, sonará grietoso con sílabas o palabras perdidas. Una posible estrategia de recuperación es reproducir las muestras de voz previas. Esto funciona bien si sólo unas cuantas muestras son perdidas. Para combatir mejor las ráfagas de errores usualmente se emplean sistemas de interpolación. Basándose en muestras de voz previas, el decodificador predecirá las tramas perdidas. Esta técnica es conocida como Packet Loss Concealment (PLC).

La ITU-T G.113 apéndice I provee algunas líneas de guía de planificación provisional en el efecto de pérdida de tramas sobre la calidad de voz. El impacto es medido en términos de Ie, el factor de deterioro. Este es un número en el cual 0 significa no deterioro. El valor más grande de Ie significa deterioro más severo. La siguiente tabla está derivada de la G.113 apéndice I y muestra el impacto de las tramas perdidas en el factor Ie.

2.3.4 Calidad de servicio:

La calidad de servicio o Qos es el rendimiento promedio de una red, es decir, mide la calidad de los servicios teniendo en cuenta la tasa de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc.

Para mejorarla se ha propuesto disminuir los anchos de banda, para ello se suprime los silencios se aprovechará mejor el ancho de banda al tener que transmitir menos información como también comprimir las cabeceras aplicando RTP/RTCP.

Se pueden distinguir tres tipos de QoS:

- Servicio Best Effort: los usuarios recibirán la mejor calidad de servicio posible en ese momento, el ancho de banda variará como también los tiempos de respuesta. No se garantiza que los datos lleguen a su destino ni ofrecer una determinada QoS.
- Servicios Integrados: gestiona los recursos necesarios para garantizar la QoS. Funciona reservando recursos de extremo a extremo de la red. RSVP es un protocolo que fue desarrollado para programar y reservar ancho de banda requerido.
- Servicios Diferenciados: intenta garantizar la calidad de servicio en redes de gran tamaño como Internet. Permite tratar cada paquete de manera individual, además cada router o switch puede configurar distintas políticas de QoS. [2]

2.4 Definición SIP:

SIP (Session Initiation Protocol) es uno de los protocolos de señalización más conocidos de VoIP. Es un protocolo de señalización simple, desarrollado por el grupo de trabajo MMUSIC del IETF con la finalidad de ser el estándar de iniciación, modificación y finalización donde intervienen elementos multimedia como por ejemplo voz, vídeo, etc.

Se caracteriza por tener una sintaxis parecida a los protocolos HTTP (protocolo de transferencia de hipertexto) y SMTP (protocolo para transferencia simple de correo).
SIP se apoya en una arquitectura cliente servidor en la cual los clientes inician las llamadas y los servidores las responden, es un protocolo abierto basado en estándares, ampliamente soportado y no es dependiente de un solo fabricante de equipos. La arquitectura SIP es abierta, escalable, flexible y distribuida. La función distribuida permite incorporar nuevas funciones sin verse afectados otros componentes. También mantiene información sobre el estado de los extremos permitiendo recuperarse de fallos de alguno de los componentes.

Algunas de las características que ofrece este protocolo son:

- Localización del usuario: registro y localización de participantes y gestión de movilidad.
- Disponibilidad del usuario: determina la voluntad del receptor de la llamada en participar en las comunicaciones.
- Capacidad del usuario: descripción de características de las sesiones y negociación de las capacidades de los participantes.
- Establecimiento de sesión: establece los parámetros de sesión de ambos extremos.
- Gestión de sesión: incluyendo transferencia, terminación de las comunicaciones, modificación de los parámetros y la invocación de servicios.

2.4.1 Diseño del Protocolo:

SIP puede utilizar en su **capa de transporte** tanto UDP (User Datagram Protocol) como TCP (Transmission Control Protocol). UDP es un protocolo de nivel de transporte para el intercambio de datagramas sin que se haya establecido previamente una conexión, el propio datagrama contendrá la información necesaria de direccionamiento en la cabecera.
TCP es un protocolo que garantiza que los datos serán entregados a su destino sin errores y en el mismo orden que se ha transmitido.

También podrá utilizar un protocolo seguro TLS que irá encapsulado sobre TCP para encriptar la información y no sea transmitido en texto plano.

Los clientes SIP usan el puerto 5060 en TCP y UDP para conectar con los servidores SIP, en caso de utilizar TLS el puerto a utilizar es el 5061.

Cabe destacar que en una comunicación ambos extremos deben soportar los mismos protocolos de transporte sino la sesión no se podrá establecer desembocando un mensaje ICMP de "*Not Supported*".

Otro punto importante es el tamaño máximo de segmento ya que está involucrado directamente con el códec a utilizar. La negociación de códecs, puertos y servicios multimedia se complementa con el protocolo SDP y el portador del contenido de voz y vídeo que intercambian los participantes en una sesión establecida es RTP.

Si nos centramos en **nivel de aplicación** SIP se complementa con distintos protocolos para realizar su funcionamiento como:

- SDP: es un protocolo que describe sesiones de comunicación multimedia cubriendo aspectos como anuncio de sesión, invitación a sesión y negociación de parámetros. SDP no se encarga de entregar los contenidos propiamente dichos sino de entablar una

negociación entre las entidades que intervienen en la sesión como tipo de contenido, formato, y todos los demás parámetros asociados. Este conjunto de parámetros se conoce como perfil de sesión.

- RTP: es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia. Va de la mano de RTCP y se sitúa sobre UDP.
- RTCP: es un protocolo que se encarga de monitorizar la calidad del servicio y proporciona información sobre los participantes de una sesión. La principal función es proporcionar una retroalimentación útil para mantener una calidad de distribución adecuada, es decir, los receptores informan al emisor sobre la calidad de su recepción, incluyendo el número de paquetes perdidos, *jitter* y RTT.
- RSVP: es un protocolo para manejar la calidad de servicio de la comunicación, ya que hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Uno de los objetivos de RSVP es eliminar situaciones en las que la voz se pierde, para ello reserva ancho de banda y da prioridad a los paquetes de voz. Es importante tener en cuenta que este protocolo no garantiza una calidad de servicio.[3]

En **nivel de red** se tendrá el protocolo IP (v4 y v6) tiene como función el uso bidireccional en origen y destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión.

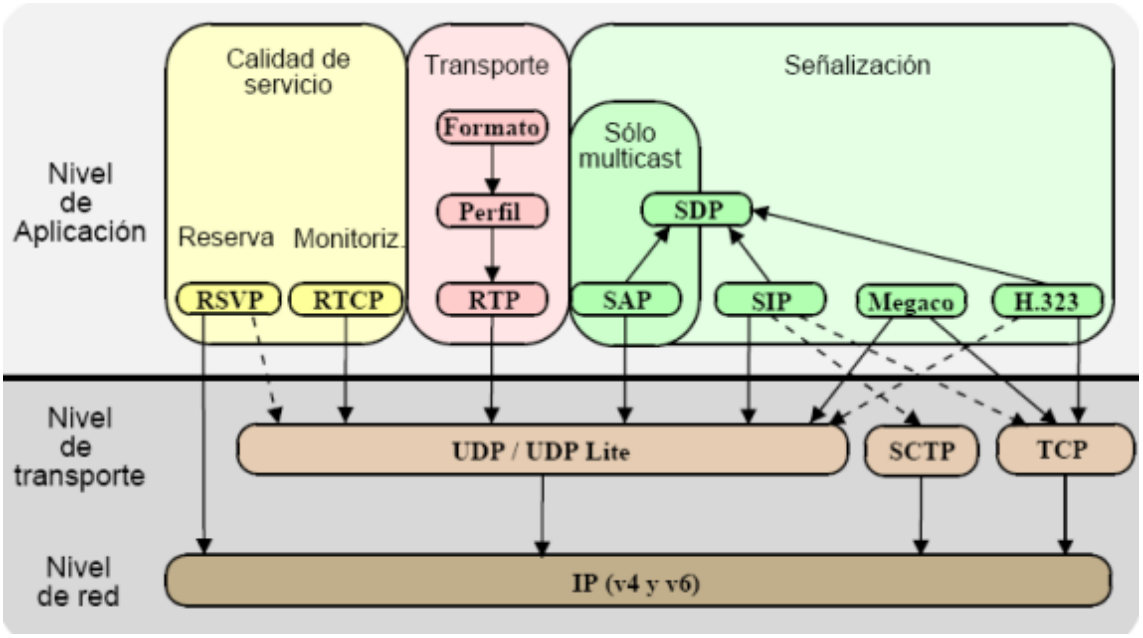


Figura 1. Diseño del protocolo.

2.4.2 Elementos SIP de red

SIP define dos tipos de entidades: los clientes y los servidores.

· Los terminales físicos conocidos como agentes usuarios (UA) pueden ser dispositivos en sí o softwares instalados en un PC pero que usan SIP y RTP para la comunicación. Estos son los puntos extremos del protocolo, es decir los que emiten y reciben los mensajes del protocolo SIP.

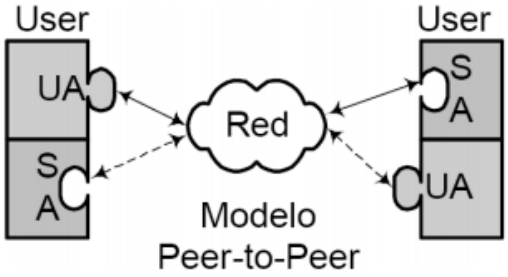


Figura 2. Agentes usuario.

Los UA pueden ser de dos tipos:

- User Agent Client (UAC) entidades que inician la sesión.
- User Agent Server (UAS) entidades que reciben la sesión.
-

Además de los agentes de usuario existen otras entidades que intervienen en el protocolo, estos son los servidores de registro, los proxy y los redirectores.

- Proxy Server: sirve para encaminar un mensaje entre un agente de usuario cliente y un agente de usuario servidor, él se encargará de enviar directamente el mensaje hacia el destino. Este punto intermedio puede ofrecer varias funciones como el control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, etc.

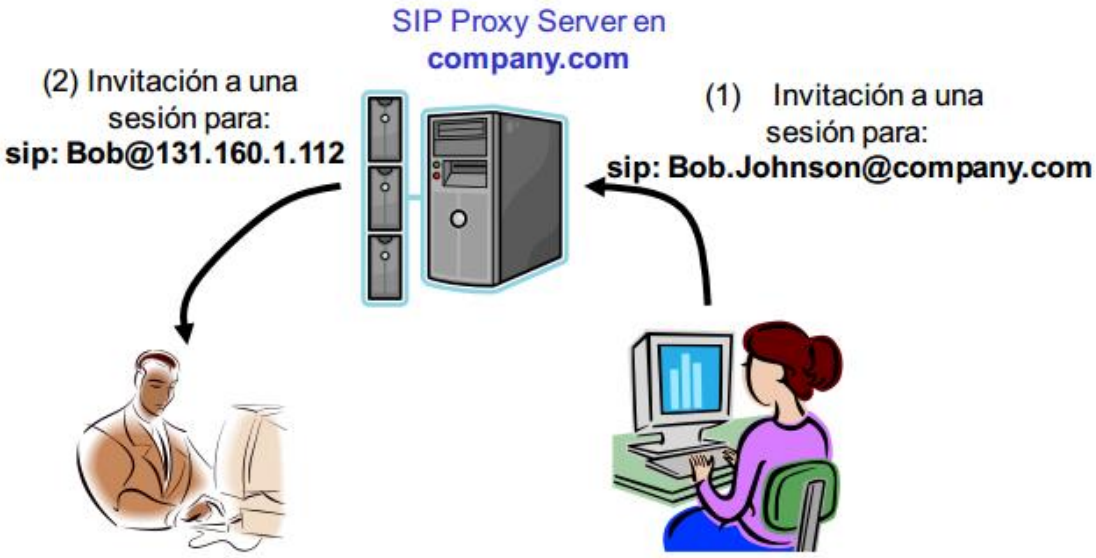


Figura 3. Proxy Server.

- Redirect Server: servidor que acepta un request SIP, mapea la dirección a nuevas direcciones y retorna estas direcciones al cliente. Al contrario que un proxy server el redirect server no inicia sus propios mensajes de SIP, sólo responde.

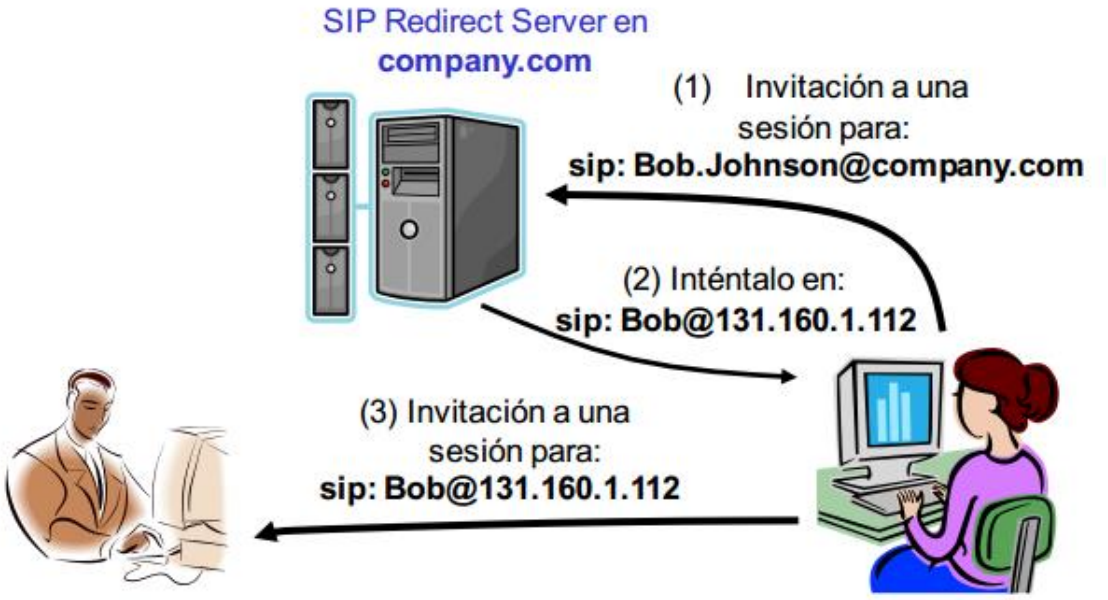


Figura 4. Redirect Server.

- Registrar Server: Es un servidor que acepta mensajes del tipo de REGISTER, el usuario puede estar registrado con múltiples dispositivos y un dispositivo puede tener registrado varios usuarios. El protocolo SIP permite establecer la ubicación física de un usuario determinado, esto es, en qué punto de la red está conectado. Cada usuario tiene una dirección lógica que es invariable respecto de la ubicación física del usuario. Las direcciones SIP están identificadas por una URI (Uniform Resource Identifier) con la forma *user@host*.
  La dirección física (denominada "dirección de contacto") es dependiente del lugar en donde el usuario está conectado (de su dirección IP). Cuando un usuario inicializa su terminal el usuario SIP envía una petición con el método REGISTER a un Registrar Server informando a qué dirección física debe asociarse la dirección lógica del usuario. El servidor de registro realiza entonces dicha asociación (denominada binding). Esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante un desregistro. La forma en que dicha asociación es almacenada en la red no es determinada por el protocolo SIP, pero es vital que los elementos de la red SIP accedan a dicha información.

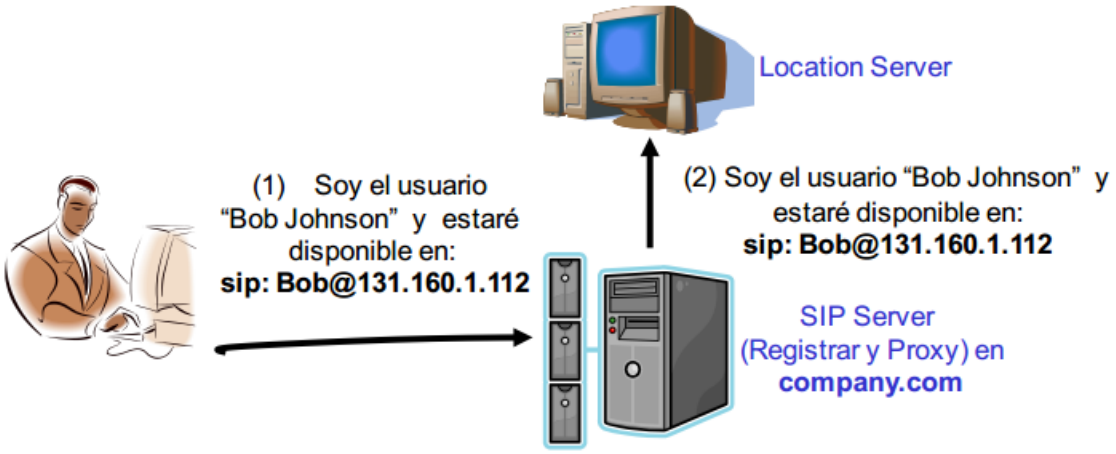


Figura 5. Registrar Server.

- Location server: es un servidor que es utilizado por un Redirect o Proxy server SIP para obtener información acerca de las posibles localizaciones de un usuario llamado. Tendrá una base de datos actualizada por el Registrar Server o por otro tipo de mecanismos. No utiliza SIP para comunicarse con otros servidores.

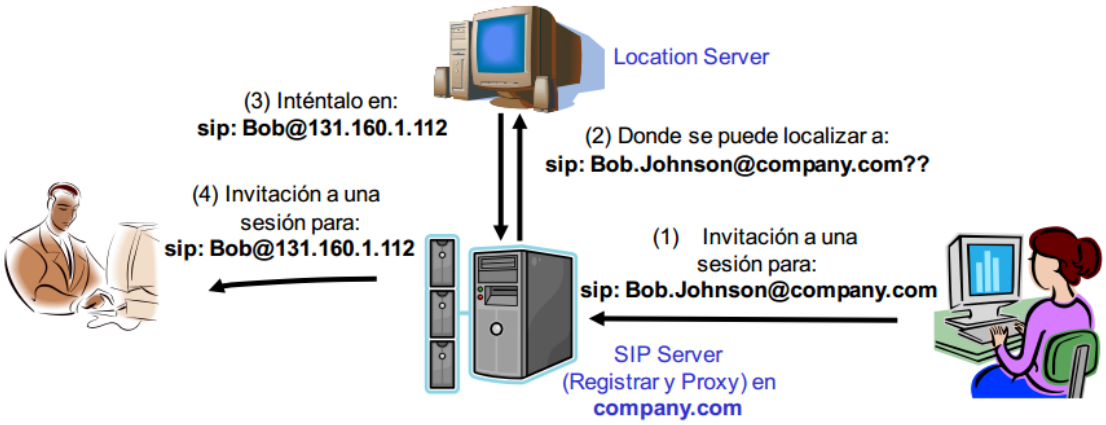


Figura 6. Location Server.

2.4.3 Mensajes del protocolo SIP:

- Direcciones SIP: Los clientes son identificados por direcciones únicas definidas como URL's, es decir las direcciones vienen en un formato muy similar a una dirección de correo electrónico. Tendrá el formato user@host.com, siendo el user el nombre del usuario, número de teléfono… y el host el dominio DNS o dirección IP.

- Métodos de SIP: SIP usa mensajes para la conexión y control de llamadas. Tendrá dos tipos mensajes de petición y mensajes de respuesta.
  Las peticiones están compuestas por una línea de petición, una serie de encabezados y un cuerpo, las respuestas por una línea de respuesta donde se indica el código de estado de la respuesta, que es un número que indica el resultado del procesamiento de la petición, una serie de encabezados y un cuerpo.
  Los encabezados de peticiones y respuestas se utilizan para diversas funciones del protocolo relacionadas con el encaminamiento de los mensajes, autenticación de los

usuarios, entre otras y el cuerpo de los mensajes es opcional y se utiliza entre otras cosas para transportar las descripciones de las sesiones que se quieren establecer, utilizando la sintaxis del protocolo SDP.

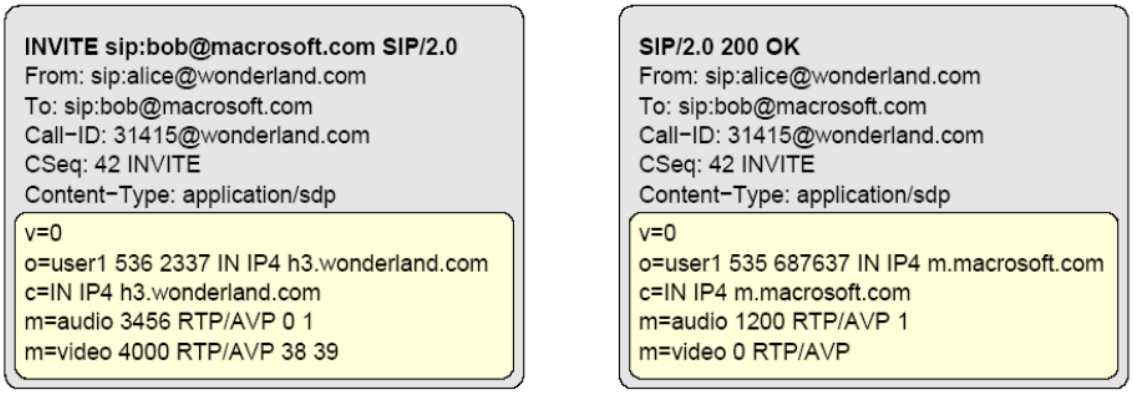


Figura 7. Mensajes SIP.

Los métodos que utiliza SIP son los siguientes:

- **INVITE:** Solicita el inicio de una llamada. Los campos de la cabecera contienen dirección origen y dirección destino, asunto de la llamada, prioridad de la llamada, peticiones de enrutamiento de llamada, preferencias para la ubicación de usuario y características deseadas de la respuesta.
- **TRYING:** Indica que el servidor Proxy está tratando de establecer la comunicación.
- **RINGING:** Indicación de aviso de llamada.
- **ACK:** Usado para facilitar un intercambio confiable de mensajes entre los pares. Confirmación de diferentes campos del mensaje INVITE.
- **CANCEL:** Cancela una solicitud pendiente.
- **OPTIONS:** Solicita información a una Host acerca de sus propias capacidades. Se utiliza antes de iniciar la llamada a fin de averiguar si ese host tiene la capacidad de transmitir VoIP, etc.
- **INFO:** Transporte de información de la llamada.
- **PRACK:** Reconocimiento provisional.
- **COMET:** Notificación de precondición.
- **REFER:** Transferencia a otra URL.
- **SUSCRIBE:** Requerir notificación de Evento.
- **UNSUSCRIBE:** Cancelar notificación de Evento.
- **NOTIFY:** Notificación de Evento.
- **MESSAGE:** Mensaje instantáneo.

Las respuestas se pueden clasificar: [4]

1xx – Mensajes provisionales

- 100 Trying
- 180 Ringing
- 183 Session Progress

2xx – Respuestas de éxito

- 200 OK

- 202 Accepted

3xx – Respuestas de redirección
- 300 Multiples Choices
- 301 Moved Permanently
- 302 Moved Temporarily

4xx – Error en el cliente (error en la petición)
- 400 Bad Request
- 401 Unauthorized
- 404 Not found
- 407 Proxy Authentication required
- 486 Busy here
- 487 Request terminated

5xx – Error en el servidor
- 500 Server internal error
- 502 Bad Gateway

6xx – Respuestas de fallo global
- 600 Busy everywhere
- 603 Decline

2.4.4 Establecimiento de una sesión:

El cliente cada vez que enciende su dispositivo o modifica su localización tendrá que registrarse para ello utilizará el registrar server.
Los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor consulta si el usuario puede ser autenticado y enviará un mensaje de OK en caso de ser correcto. La información de registro se refresca periódicamente.

El flujo habitual del establecimiento de una conexión mediante el protocolo SIP es el siguiente:

i. El agente de usuario SIP que reside en el terminal, actuando como UAC envía la petición **INVITE** al servidor que tiene configurado (en este caso *Proxy*). Este servidor se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario. Una vez obtenida la dirección del servidor del dominio destino, encamina hacia allí la petición. El servidor del dominio destino establece que la petición es para un usuario de su dominio y entonces se vale de la información de registro de dicho usuario para establecer su ubicación física. Si la encuentra, entonces encamina la petición hacia dicha dirección.

   Normalmente la petición con el método INVITE lleva un cuerpo donde viaja una descripción de la sesión, esta descripción es realizada con el protocolo SDP. En ella se indica el tipo de contenido a intercambiar (voz, video, etc.) y sus características (códecs, direcciones, puertos donde se espera recibirlos, velocidades de transmisión, etc.). Esto se conoce como "oferta de sesión SDP". La respuesta a esta oferta viaja, en este caso, en el cuerpo de la respuesta definitiva a la petición con el método INVITE. La misma contiene la descripción de la sesión desde el punto de vista del

destinatario. Si las descripciones fueran incompatibles, la sesión debe terminarse mediante una petición con el método BYE.

ii. El agente de usuario destino si se encuentra desocupado comenzará a alertar al usuario destino y envía una respuesta hacia el usuario origen con un código de estado que indica esta situación **180 Ringing**.

iii. La respuesta sigue el camino inverso hacia el usuario origen. Cuando el usuario destino finalmente acepta la invitación, se genera una respuesta con un código de estado **200 OK** que indica que la petición fue aceptada.

iv. La recepción de la respuesta final es confirmada por el UAC origen mediante una petición con el método **ACK**, esta petición no genera respuestas y completa la transacción de establecimiento de la sesión.

v. Al terminar la sesión, que lo puede hacer cualquiera de las partes, el agente de usuario de la parte que terminó la sesión, actuando como UAC, envía hacia la otra una petición con el método **BYE**.

vi. Cuando lo recibe el UAS genera la respuesta con el código de estado correspondiente **200 OK**.

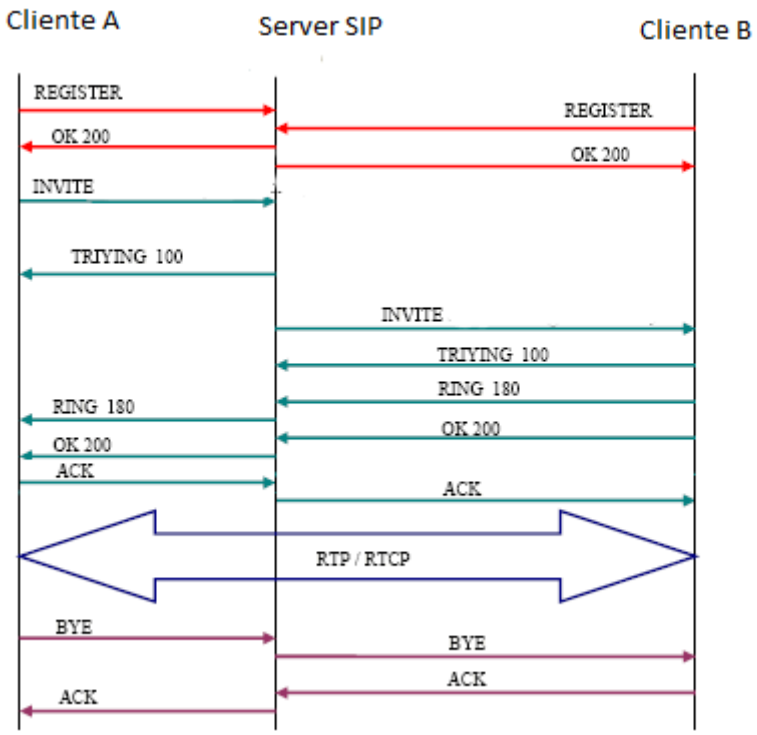


Figura 8. Establecimiento de sesión SIP.

SIP permite modificar la llamada una vez se está realizando, para ello utiliza SDP para definir las características de la comunicación utilizando un modelo de oferta y respuesta. En la oferta se ofrecen los distintos tipos de protocolos, payloads, direcciones y puertos para la comunicación. En las respuestas se define cuáles serán los utilizados. Mientras se negocia nuevamente las

características de la comunicación, se continúa con los parámetros anteriores. Sólo se puede renegociar después del primer establecimiento.

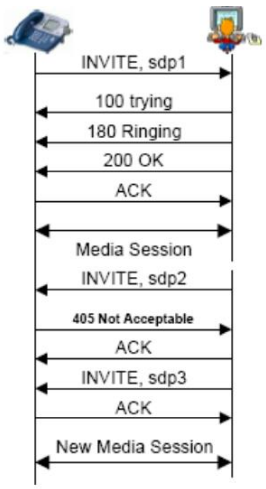


Figura 9. Negociación SIP.

2.4.5 Aplicaciones que utilizan SIP:

Algunos de los programas de audio/videoconferencia que usan SIP: Jitsi, Ekiga, Twinkle, Tapioca, SipX, KPhone, KCall, WxCommunicator, Linphone, Xlite, Zoiper, SJPhone, entre otros.

Capítulo 3: SERVIDOR ASTERISK

3.1 Elección del servidor:

El servidor utilizado para la realización de esta práctica es Asterisk, debido a la gran flexibilidad que ofrece como también a las diversas aplicaciones empleadas. Permite instalar, ejecutar, configurar y administrar una Central Telefónica de forma rápida y sencilla. Se instalará dicho servidor debido a que es un software libre, no representa gasto alguno en cuanto a licencias de uso, no requiere de un PC potente para ser ejecutado dado que se puede administrar vía web y utilizar el mismo hardware existente.

3.2 Instalación del servidor:

El servidor Asterisk necesita ejecutarse con el sistema operativo Linux y en el laboratorio dónde va a ser instalado se utilizará Microsoft Windows, para ello se instalará el programa Oracle VM VirtualBox, el cual consiste en la virtualización para arquitecturas x86/amd64, gracias a esto es posible instalar sistemas operativos adicionales "invitado" dentro de otro sistema operativo "anfitrión".

Una vez el programa ha sido correctamente instalado procederemos a descargar la imagen ISO de AsteriskNow, para ello descargaremos la versión 10.13 de 64 bits.

Se crea una nueva máquina virtual de nombre Asterisk, tipo Linux con la versión Ubuntu de 64bits y un tamaño de memoria RAM de 1024 MB y crearemos un disco duro virtual de 8 Gb del tipo VDI.

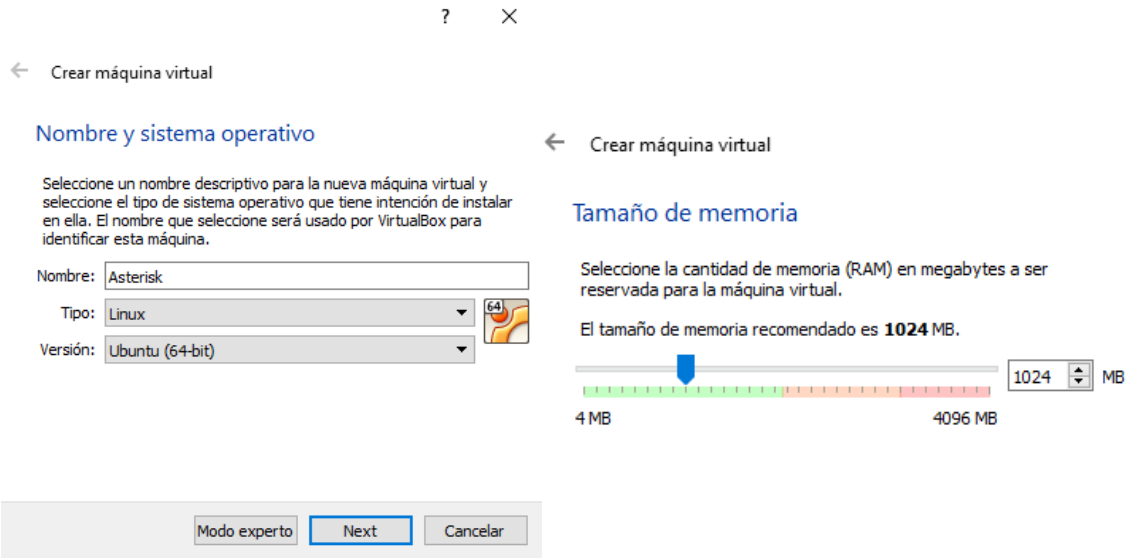


Figura 10.Sistema operativo y memoria de la máquina virtual.

Una vez creada la máquina virtual se configura el adaptador de red conectándolo a Adaptador Puente. En opciones avanzadas, se permitirá todo en modo promiscuo y añadiremos la dirección MAC 0800274F8A68, dada por la Universidad Politécnica de Valencia, se especifica con mayor precisión en la imagen siguiente.

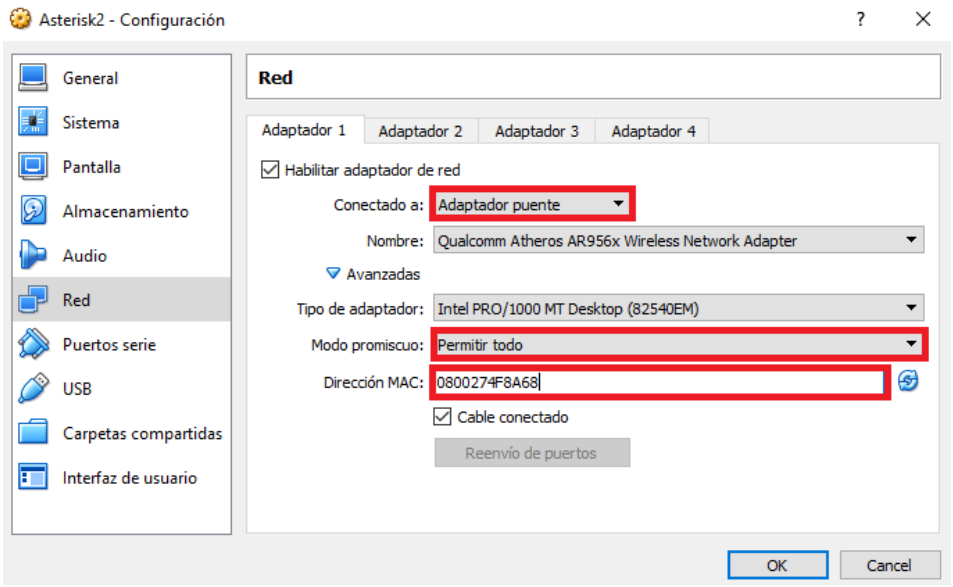


Figura 11. Configuración red de la máquina virtual.

En Almacenamiento se añadirá dentro del controlador IDE la imagen ISO descargada, como se observa en la imagen siguiente.

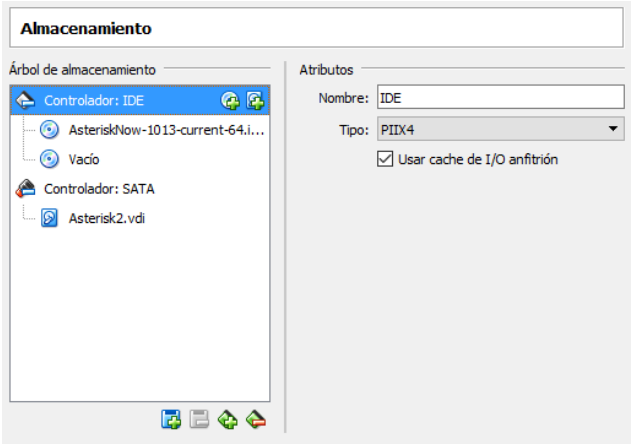


Figura 12. Configuración de la imagen ISO.

3.3 Configuración del servidor:

Una vez iniciado la máquina virtual se procede a la configuración del servidor. Primeramente, aparecerán las opciones de red donde se configurará la IP de forma manual y se desactivará el soporte de IPv6 como se muestra en la imagen siguiente. [5]

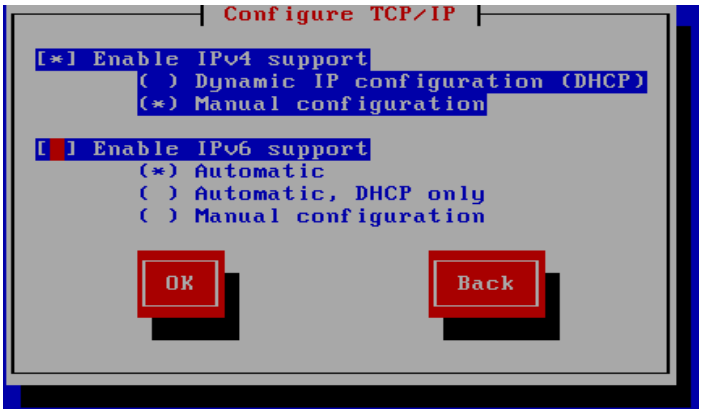


Figura 13. Configuración del servidor Astersik.

En segundo lugar, la dirección IP que se introducirá es 158.42.188.166 con máscara 255.255.255.0 proporcionada por la Universidad Politécnica de Valencia, para poder acceder a dicho servidor desde los demás ordenadores del laboratorio los cuales están en el mismo dominio de red. El nombre del servidor será pracservitel y con el Gateway se pondrá la dirección IP 158.42.188.250.

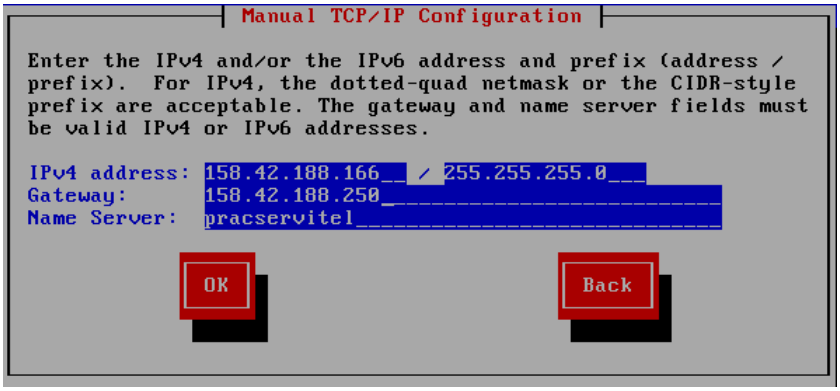


Figura 14. Configuración manual TCP/IP.

Se seleccionará la zona horaria pertinente a la localización de dicho servidor, en este caso Europa/Madrid.

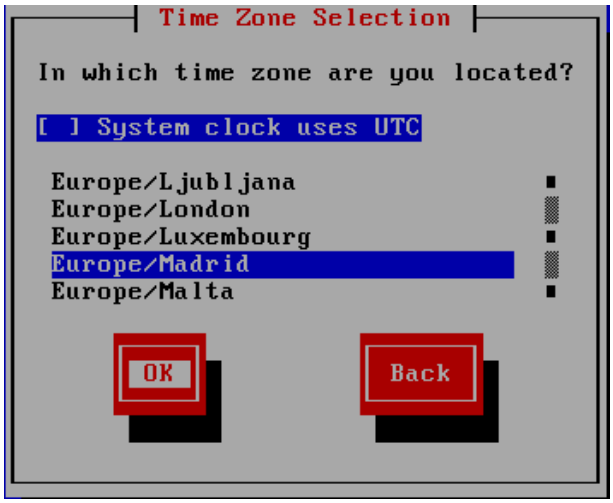


Figura 15. Zona horaria.

Y por último se pide una contraseña para el usuario root. La contraseña de root es la contraseña que se utilizará para iniciar sesión en el símbolo del sistema Linux más tarde.

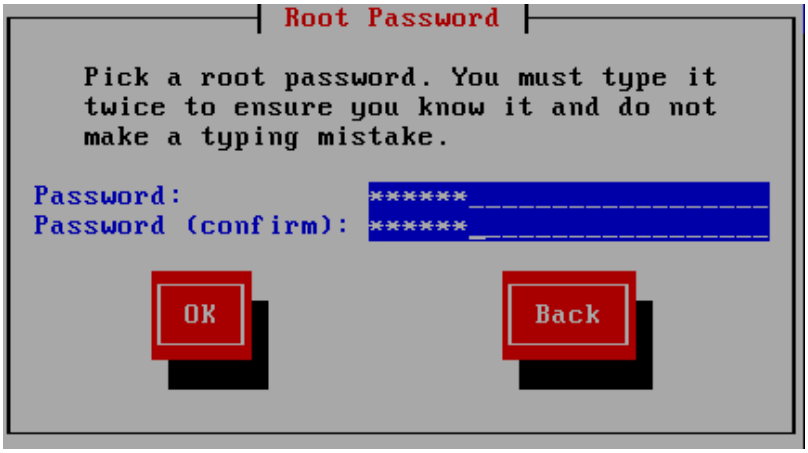


Figura 16. Contraseña del servidor.

Posteriormente, efectuada toda la configuración del servidor, solo habrá que identificarse y observar que no sale ningún mensaje de error.

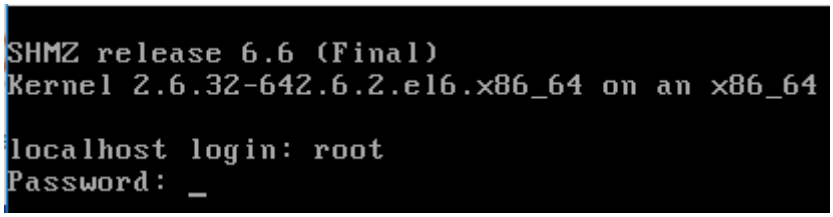


Figura 17. Identificación del servidor.

Más adelante, se introducirá la dirección IP del servidor en el navegador web con otro equipo de la misma red. La primera vez se pedirá para crear el administrador un nombre de usuario y la

contraseña de administrador. Este nombre de usuario y contraseña serán utilizados en el futuro para acceder a la pantalla de configuración de FreePBX.

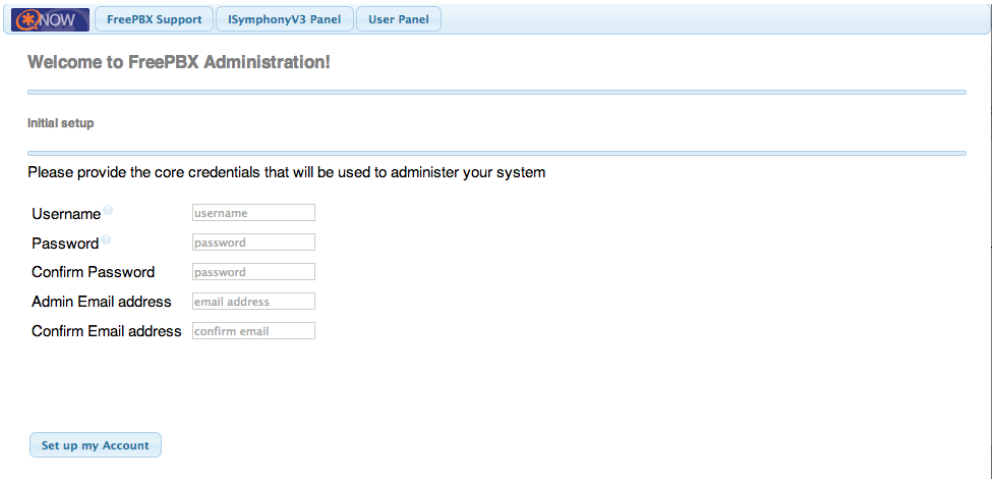


Figura 18. Administrador FreePBX.

La pantalla principal de FreePBX ofrecerá cuatro opciones:

- Administrador FreePBX: permite configurar PBX el cual te autoriza a acceder introduciendo el nombre de usuario y la contraseña de administrador que se configuró en el paso anterior para iniciar sesión.
- Panel de Control de Usuario: se detallará las cuentas de los usuarios.
- Panel de Control del Operador: permitirá al operador controlar las llamadas.
- Soporte de Ayuda: proporcionará ayuda al usuario.

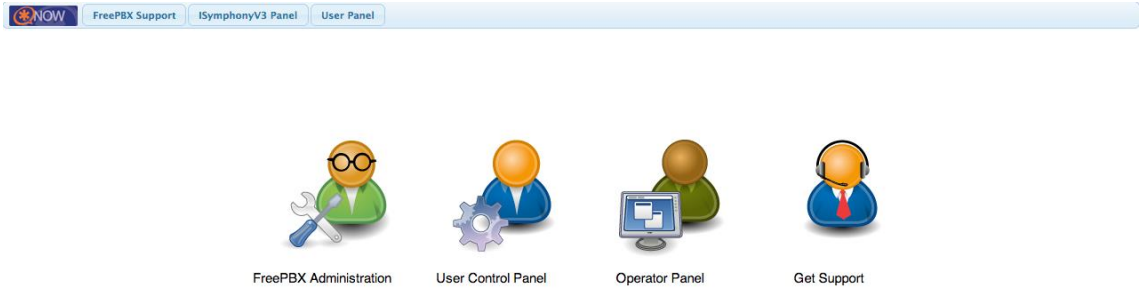


Figura 19. Pantalla principal FreePBX.

Para crear las diferentes extensiones, se seleccionará en el menú Applications y se dará clic en Extensions. Se completará los datos correspondientes a User Extension y Secret que son los datos mínimos necesarios, en donde User Extension es el número de Anexo y Secret es la contraseña del número de Anexo a crear.

Para utilizar mediante softphone un Anexo tanto para un Smartphone como para un PC se debe:

- Configurar el SmartPhone o PC para que se encuentre dentro de la misma red LAN en la que se encuentra nuestro servidor Asterisk.
- Instalar una aplicación que permita realizar llamadas VoIP, en este caso se utilizará el softphone Jitsi para hacer las diferentes pruebas.
- Configurar la aplicación con la información correspondiente al Anexo previamente creado.

3.4 Configuración del Softphone:

Sin importar la aplicación que se vaya a utilizar habrá que ir al apartado de configuración y seleccionar la opción Cuentas donde les pedirán los siguientes datos: *Username/Extension*, donde se debe de ingresar el número del Anexo, *Password*, donde se debe de ingresar la contraseña del Anexo y *Domain*, donde se debe de ingresar la dirección IP del servidor Asterisk.

Concretamente, se configurará la aplicación softphone Jitsi en los ordenadores del laboratorio, donde se pedirá los datos que se ha introducido en la creación de la extensión. Cada PC tendrá que configurar su softphone con las diferentes extensiones creadas.

En Jitsi específicamente en Archivo se seleccionará el apartado de Agregar una nueva cuenta SIP, se insertará como identificador SIP el número de la extensión seguido por la dirección del servidor y la contraseña, como se observa en la siguiente imagen.

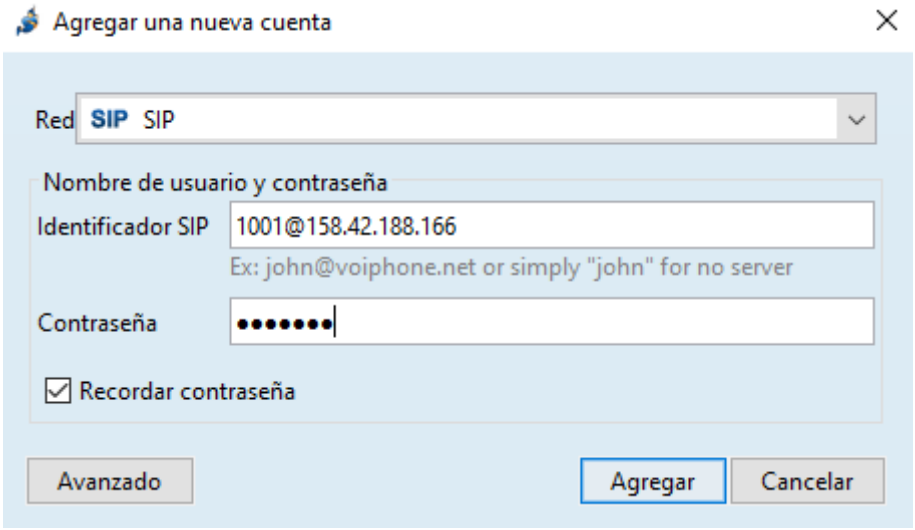


Figura 20. Configuración de Jitsi.

Una vez la configuración haya sido correcta, el sistema está listo para enviar y recibir llamadas de voz y vídeo.

Capítulo 4. SIMULACIONES

4.1 Llamada de voz.

La primera simulación obtenida es una llamada de voz entre dos clientes sin cambiar ningún parámetro, el programa utilizado para estudiar el tráfico de paquetes es Wireshark, un software analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones.

El cliente con dirección IP 158.42.188.119, con número de extensión 1001, quiere iniciar una conversación con el cliente 158.42.188.123, con extensión 1002, para hacer posible esta conexión se utilizará el servidor instalado en el laboratorio con dirección IP 158.42.188.166 que será el encargado de establecer dicha comunicación. El protocolo de transporte utilizado es UDP y el número de puerto que se utiliza para SIP es 5060.

Como se observa en las siguientes imágenes primeramente se utiliza el método INVITE con el fin de establecer el inicio de una llamada. El servidor recibirá un trying y ringing que es para intentar establecer la conexión, es decir, el destinatario recibirá un aviso de llamada.
La respuesta final a la invitación viene dada por el Status: 200 OK, el emisor enviará un ACK confirmando que la invitación ha sido aceptada.
El protocolo SDP se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones. Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet.
Por último tenemos el método BYE para liberar la sesión establecida producido en este caso por el emisor y el receptor le contestará con un ACK 200 OK para confirmar el fin de la llamada.

127	4.664841	158.42.188.119	158.42.188.166	SIP/SDP	1476 Request: INVITE sip:1002@158.42.188.166 |
128	4.666624	158.42.188.166	158.42.188.119	SIP	608 Status: 401 Unauthorized |
129	4.668991	158.42.188.119	158.42.188.166	SIP	419 Request: ACK sip:1002@158.42.188.166 |
131	4.670954	158.42.188.119	158.42.188.166	SIP/SDP	252 Request: INVITE sip:1002@158.42.188.166 |
132	4.675327	158.42.188.166	158.42.188.119	SIP	403 Status: 100 Trying |
133	4.899875	158.42.188.166	158.42.188.119	SIP	647 Status: 180 Ringing |
134	4.959238	158.42.188.166	158.42.188.119	SIP	647 Status: 180 Ringing |
219	8.649868	158.42.188.166	158.42.188.119	SIP/SDP	1015 Status: 200 OK |
221	8.675309	158.42.188.119	158.42.188.166	SIP	793 Request: ACK sip:158.42.188.166:5060 |
794	13.599168	158.42.188.119	158.42.188.166	SIP	793 Request: BYE sip:158.42.188.166:5060 |
795	13.600564	158.42.188.166	158.42.188.119	SIP	437 Status: 200 OK |

Figura 21. Métodos llamada de voz.

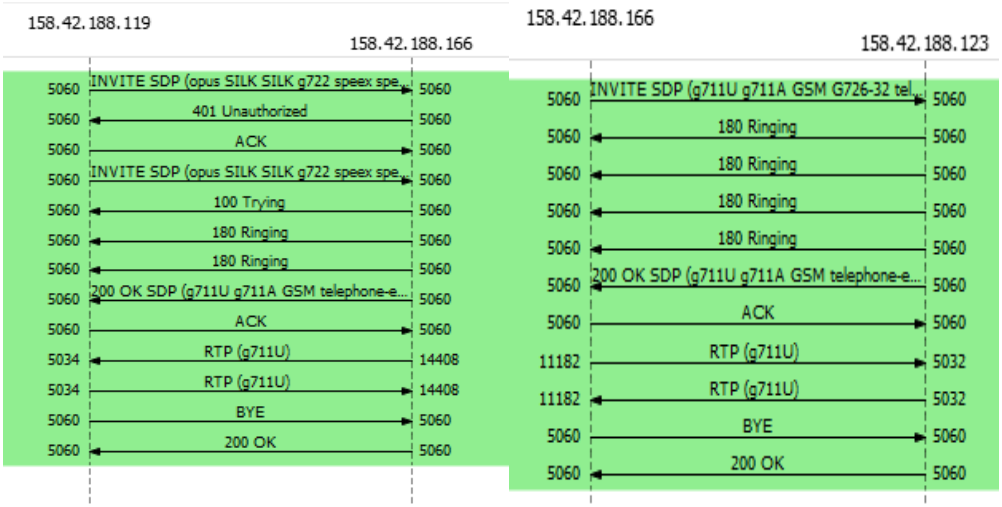


Figura 22. Intercambio de mensajes de llamada de voz.

Se analiza los códecs disponibles por el extremo que son GSM, G.711 (PCMA, PCMU) y DyinamicRTP como se muestra en la siguiente imagen.

```
Media Description, name and address (m): audio 5014 RTP/AVP 96 97 98 9 100 102 0 8 103 3 104 4 101
    Media Type: audio
    Media Port: 5014
    Media Protocol: RTP/AVP
    Media Format: DynamicRTP-Type-96
    Media Format: DynamicRTP-Type-97
    Media Format: DynamicRTP-Type-98
    Media Format: ITU-T G.722
    Media Format: DynamicRTP-Type-100
    Media Format: DynamicRTP-Type-102
    Media Format: ITU-T G.711 PCMU
    Media Format: ITU-T G.711 PCMA
    Media Format: DynamicRTP-Type-103
    Media Format: GSM 06.10
    Media Format: DynamicRTP-Type-104
    Media Format: ITU-T G.723
    Media Format: DynamicRTP-Type-101
```

Figura 23. Códecs disponibles.

Estudiamos los paquetes enviados durante la conversación y vemos que el valor del jitter entra dentro de los parámetros normales ya que es a partir de 100 ms cuando puede sufrir alteraciones o pérdidas de datos como era de esperar no ha habido ninguna pérdida de paquetes de los 1470 enviados.

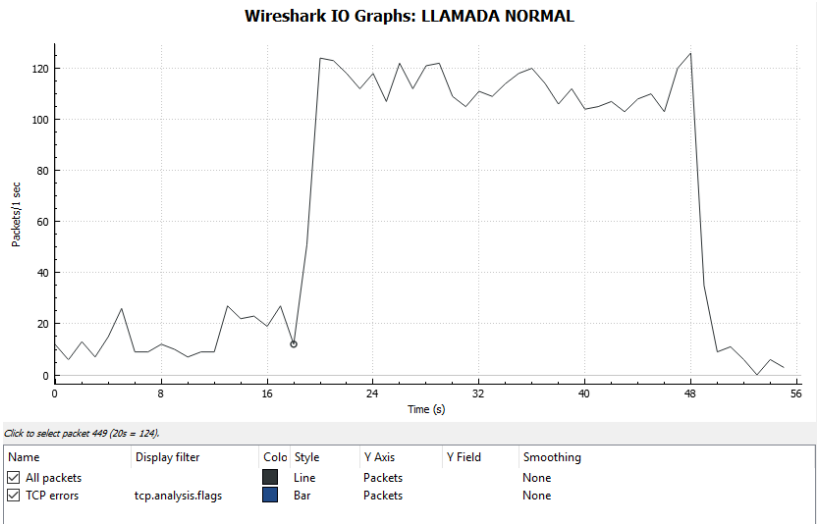


Figura 24. Paquetes enviados llamada de voz.

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
158.42.188.119	5014	158.42.188.166	18064	0x6d3c91ca	g711U	1470	0 (0.0%)	35.418	6.020	4.693	
158.42.188.166	18064	158.42.188.119	5014	0x46ada0b0	g711U	1470	0 (0.0%)	40.538	6.250	4.827	

Figura 25. Paquetes perdidos llamada de voz.

Una de las funcionalidades de Wireshark es que nos permite reproducir la conversación mantenida como también ver su gráfico.

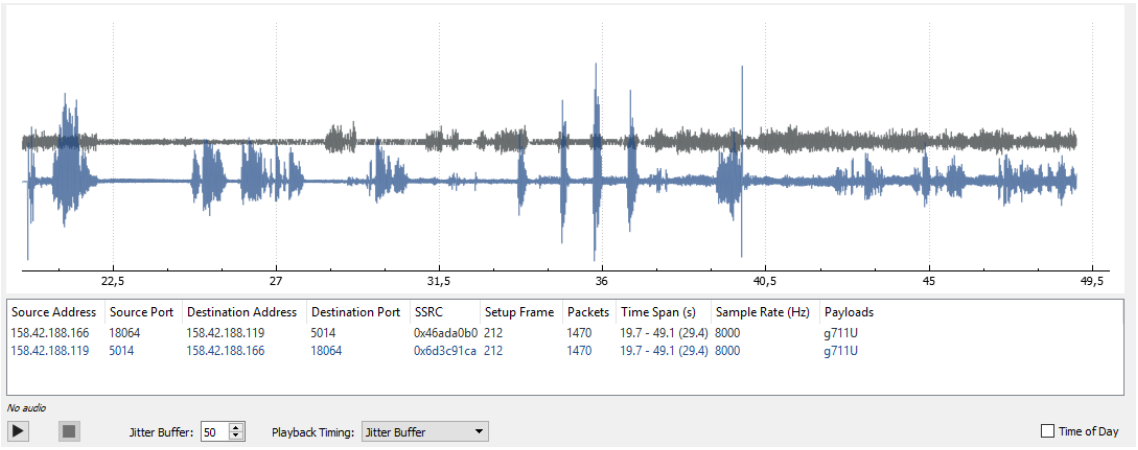


Figura 26. Gráfico de la conversación.

4.2 Desvío de llamadas.

El escenario siguiente es la comunicación entre un cliente con extensión 1001 que inicia la comunicación con 1002 y desvía la llamada a 1005, quedando la conexión establecida entre 1002 y 1005. El flujo de paquetes es el mismo que una llamada normal, se iniciará con un INVITE seguido del Trying y Ringing y su correspondiente ACK seguido con el protocolo SDP para poder establecer la conexión. Cuando se desvía la llamada 1001enviará un REFER proporcionando todos los datos entre la conexión establecida entre 1001 y 1002 para que 1005 pueda iniciar la conexión. Una vez transmitida la llamada se enviará un BYE recibiendo el ACK correspondiente.

```
    90 18.178039    158.42.188.119    158.42.188.166    SIP/SDP  1476 Request: INVITE sip:1002@158.42.188.166 |
    91 18.179905    158.42.188.166    158.42.188.119    SIP       608 Status: 401 Unauthorized |
    92 18.182732    158.42.188.119    158.42.188.166    SIP       419 Request: ACK sip:1002@158.42.188.166 |
    94 18.184170    158.42.188.119    158.42.188.166    SIP/SDP   252 Request: INVITE sip:1002@158.42.188.166 |
    95 18.189044    158.42.188.166    158.42.188.119    SIP       403 Status: 100 Trying |
    96 18.386029    158.42.188.166    158.42.188.119    SIP       647 Status: 180 Ringing |
   103 18.443963    158.42.188.166    158.42.188.119    SIP       647 Status: 180 Ringing |
   142 25.018438    158.42.188.166    158.42.188.119    SIP/SDP  1015 Status: 200 OK |
   143 25.045545    158.42.188.119    158.42.188.166    SIP       793 Request: ACK sip:158.42.188.166:5060 |
   570 28.996844    158.42.188.119    158.42.188.166    SIP       683 Request: OPTIONS sip:158.42.188.166 |
   571 28.998638    158.42.188.166    158.42.188.119    SIP       617 Status: 401 Unauthorized |
  1074 33.853039    158.42.188.166    158.42.188.119    SIP       532 Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
  1077 33.877397    158.42.188.119    158.42.188.166    SIP       722 Status: 200 OK |
  3124 53.636206    158.42.188.166    158.42.188.119    SIP/SDP  1112 Request: INVITE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166, in-dialog |
  3131 53.672425    158.42.188.119    158.42.188.166    SIP/SDP   905 Status: 200 OK |
  3132 53.674901    158.42.188.166    158.42.188.119    SIP       496 Request: ACK sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
  3166 53.997820    158.42.188.119    158.42.188.166    SIP       683 Request: OPTIONS sip:158.42.188.166 |
  3167 53.999537    158.42.188.166    158.42.188.119    SIP       617 Status: 401 Unauthorized |
  5809 79.003163    158.42.188.119    158.42.188.166    SIP       683 Request: OPTIONS sip:158.42.188.166 |
  5811 79.005940    158.42.188.166    158.42.188.119    SIP       617 Status: 401 Unauthorized |
  7317 93.062679    158.42.188.166    158.42.188.119    SIP       520 Request: BYE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
  7319 93.088954    158.42.188.119    158.42.188.166    SIP       542 Status: 200 OK |
  7325 93.851529    158.42.188.166    158.42.188.119    SIP       532 Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
  7326 93.876388    158.42.188.119    158.42.188.166    SIP       722 Status: 200 OK |
  7464 104.004544   158.42.188.119    158.42.188.166    SIP       683 Request: OPTIONS sip:158.42.188.166 |
  7465 104.006222   158.42.188.166    158.42.188.119    SIP       617 Status: 401 Unauthorized |
  7566 128.998621   158.42.188.119    158.42.188.166    SIP       683 Request: OPTIONS sip:158.42.188.166 |
  7567 129.000381   158.42.188.166    158.42.188.119    SIP       617 Status: 401 Unauthorized |
```

Figura 27. Métodos del desvío de llamadas.

Como observamos en la imagen REFER nos da la información de la dirección del emisor, receptor y servidor como también la nueva dirección donde se nos desviará la llamada. También nos proporciona información de puertos, protocolos, identificador de llamada entre otras.

```
Session Initiation Protocol (REFER)
  Request-Line: REFER sip:158.42.188.166:5060 SIP/2.0
  Message Header
    CSeq: 3 REFER
    From: "1001" <sip:1001@158.42.188.166>;tag=100f05df
    To: <sip:1002@158.42.188.166>;tag=4f85cc1b-c5f7-4c70-8368-a68a8258427d
    Call-ID: 7717cd7b3cc1a7a8c4c3d21643e2a4e3@0:0:0:0:0:0:0:0
    Max-Forwards: 70
    Via: SIP/2.0/UDP 158.42.188.119:5060;branch=z9hG4bK-353136-d6ec97a769cf604bc94a869750c0a457
    Contact: "1001" <sip:1001@158.42.188.119:5060;transport=udp;registering_acc=158_42_188_166>
    [truncated]Authorization: Digest username="1001",realm="asterisk",nonce="1498550635/80bee6a0b091e3b97aca484fe4f61ed5",uri="sip:1002@158.42.188.166",response="1afc3636fb27
    User-Agent: Jitsi2.8.5426Windows 7
    Refer-To: <sip:1005@158.42.188.166>
    Referred-By: "1001" <sip:1001@158.42.188.166>
    Content-Length: 0
```

Figura 28. Parámetros del desvío de llamada.

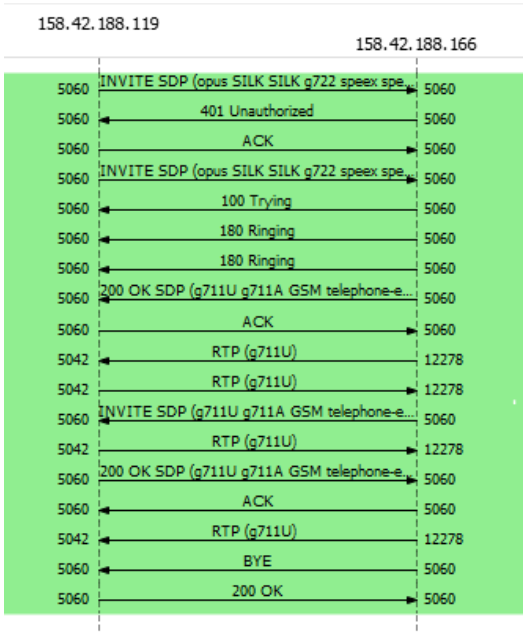


Figura 29. Mensajes del desvío de llamada.

En las siguientes gráficas nos muestra el transcurso de paquetes en el tiempo, como observamos a partir de los 45 segundos es cuando se transmite la llamada de voz. El valor del jitter está situado dentro de los parámetros normales por lo tanto no hay pérdida de paquetes.

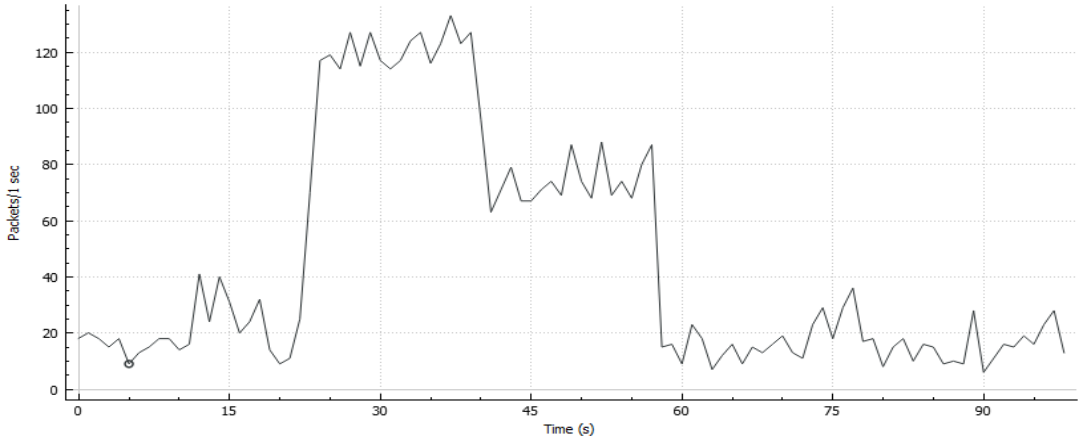
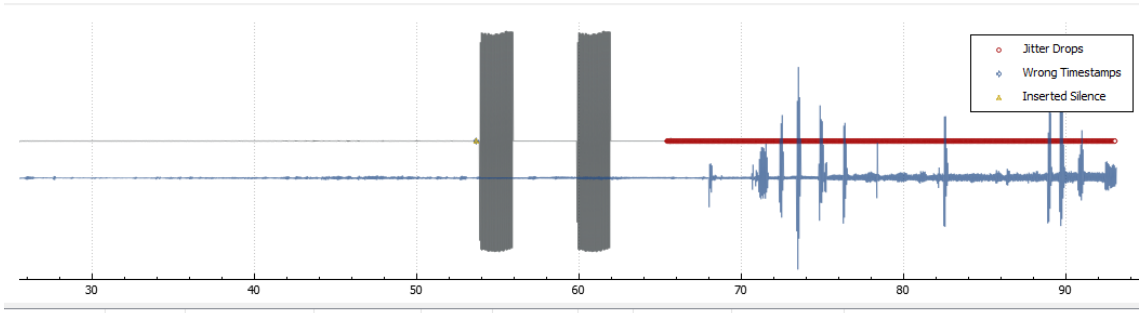


Figura 30. Paquetes enviados del desvío de llamadas.



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
158.42.188.166	12278	158.42.188.119	5042	0x260024be	3124	1956	25.1 - 93 (67.9)	8000	g711U
158.42.188.119	5042	158.42.188.166	12278	0x6557a39d	3124	1974	25.2 - 93.1 (67.9)	8000	g711U

Figura 31. Gráfico conversación durante el desvío de llamadas.

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
158.42.188.119	5052	158.42.188.166	18688	0x32da333d	g711U	1722	0 (0.0%)	40.951	7.372	5.058	
158.42.188.166	18688	158.42.188.119	5052	0x797400e8	g711U	847	0 (0.0%)	36.243	6.243	4.824	

Figura 32. Paquetes perdidos desvío de llamadas.

4.3 Conversación Múltiple.

Primeramente se inicia una conversación entre 1001 y 1002 donde posteriormente se invitará a la comunicación a 1005. Como observamos en la imagen los métodos utilizados son exactos a los de una llamada normal con la diferencia que una vez establecida la conexión se enviará un INVITE a 1005 para unirse a ella.

```
   57  5.789321   158.42.188.119   158.42.188.166   SIP/SDP   1466  Request: INVITE sip:1002@127.0.0.1 |
   58  5.791153   158.42.188.166   158.42.188.119   SIP        603  Status: 401 Unauthorized |
   59  5.793041   158.42.188.119   158.42.188.166   SIP        409  Request: ACK sip:1002@127.0.0.1 |
   61  5.795440   158.42.188.119   158.42.188.166   SIP/SDP    237  Request: INVITE sip:1002@127.0.0.1 |
   62  5.799731   158.42.188.166   158.42.188.119   SIP        398  Status: 100 Trying |
   68  5.975950   158.42.188.166   158.42.188.119   SIP        637  Status: 180 Ringing |
   69  6.022510   158.42.188.166   158.42.188.119   SIP        637  Status: 180 Ringing |
  134 13.763351   158.42.188.166   158.42.188.119   SIP/SDP   1005  Status: 200 OK |
  135 13.788505   158.42.188.119   158.42.188.166   SIP        783  Request: ACK sip:158.42.188.166:5060 |
  859 20.342888   158.42.188.119   158.42.188.166   SIP        683  Request: OPTIONS sip:158.42.188.166 |
  860 20.345032   158.42.188.166   158.42.188.119   SIP        617  Status: 401 Unauthorized |
 1485 30.628125   158.42.188.119   158.42.188.166   SIP/SDP    375  Request: INVITE sip:158.42.188.166:5060, in-dialog |
 1486 30.630454   158.42.188.166   158.42.188.119   SIP/SDP    955  Status: 200 OK |
 1488 30.647033   158.42.188.119   158.42.188.166   SIP        532  Request: ACK sip:158.42.188.166:5060 |
 1481 30.682263   158.42.188.119   158.42.188.166   SIP/SDP   1484  Request: INVITE sip:1005@158.42.188.166 |
 1482 30.684405   158.42.188.166   158.42.188.119   SIP        608  Status: 401 Unauthorized |
 1483 30.686615   158.42.188.119   158.42.188.166   SIP        419  Request: ACK sip:1005@158.42.188.166 |
 1485 30.695761   158.42.188.119   158.42.188.166   SIP/SDP    260  Request: INVITE sip:1005@158.42.188.166 |
 1487 30.701073   158.42.188.166   158.42.188.119   SIP        403  Status: 100 Trying |
 1510 30.911751   158.42.188.166   158.42.188.119   SIP        647  Status: 180 Ringing |
 1514 30.961227   158.42.188.166   158.42.188.119   SIP        647  Status: 180 Ringing |
 2145 41.786168   158.42.188.166   158.42.188.119   SIP/SDP   1015  Status: 200 OK |
 2147 41.810815   158.42.188.119   158.42.188.166   SIP        793  Request: ACK sip:158.42.188.166:5060 |
 2708 45.341987   158.42.188.119   158.42.188.166   SIP        683  Request: OPTIONS sip:158.42.188.166 |
 2709 45.343647   158.42.188.166   158.42.188.119   SIP        617  Status: 401 Unauthorized |
 4247 55.200182   158.42.188.166   158.42.188.119   SIP        532  Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
 4254 55.229788   158.42.188.119   158.42.188.166   SIP        722  Status: 200 OK |
 5686 64.239733   158.42.188.166   158.42.188.119   SIP        508  Request: BYE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
 5691 64.264436   158.42.188.119   158.42.188.166   SIP        530  Status: 200 OK |
 5697 64.304579   158.42.188.119   158.42.188.166   SIP/SDP    377  Request: INVITE sip:158.42.188.166:5060, in-dialog |
 5698 64.307829   158.42.188.166   158.42.188.119   SIP/SDP    960  Status: 200 OK |
 5705 64.336516   158.42.188.119   158.42.188.166   SIP        537  Request: ACK sip:158.42.188.166:5060 |
 5888 66.163923   158.42.188.166   158.42.188.119   SIP        512  Request: BYE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
 5890 66.190309   158.42.188.119   158.42.188.166   SIP        534  Status: 200 OK |
 5901 70.335913   158.42.188.119   158.42.188.166   SIP        683  Request: OPTIONS sip:158.42.188.166 |
 5902 70.337654   158.42.188.166   158.42.188.119   SIP        617  Status: 401 Unauthorized |
```

Figura 33. Métodos enviados conversación múltiple.

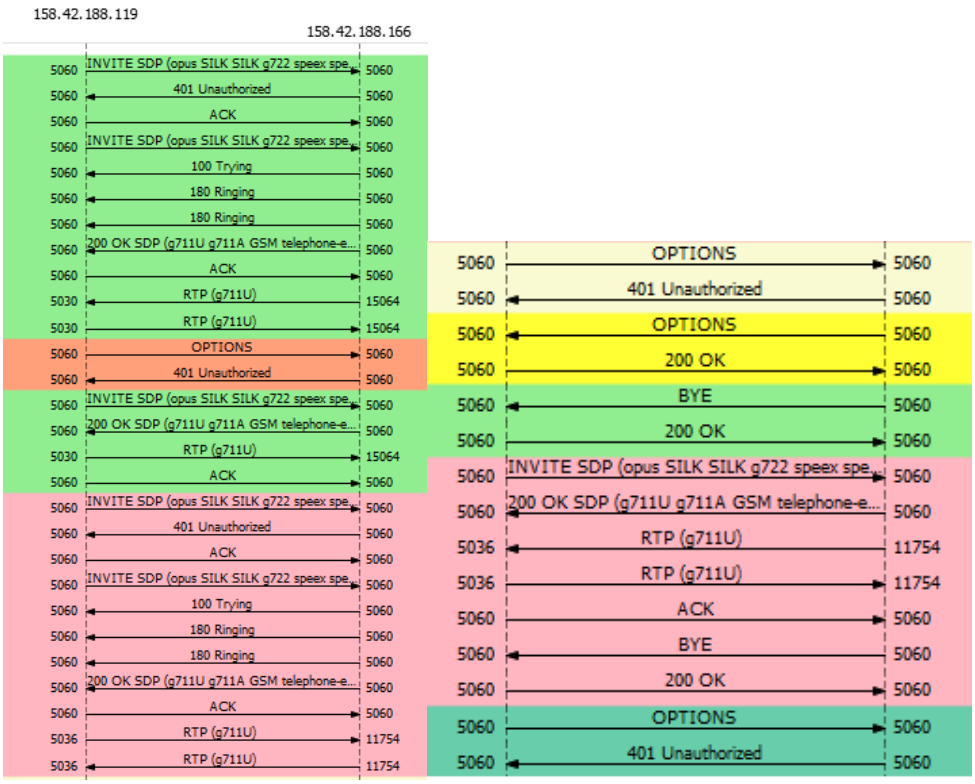


Figura 34. Mensajes enviados conversación múltiple.

Analizamos los paquetes enviados durante la conversación y observamos que no ha habido pérdidas y los valores de los jitters están dentro de la media para mantener una conversación con una calidad de servicio buena.

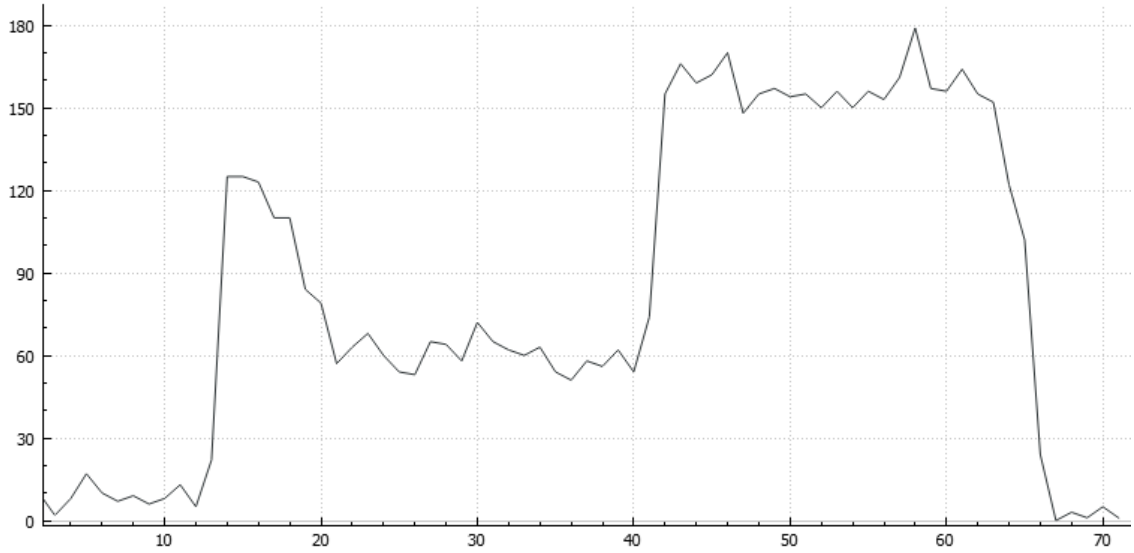
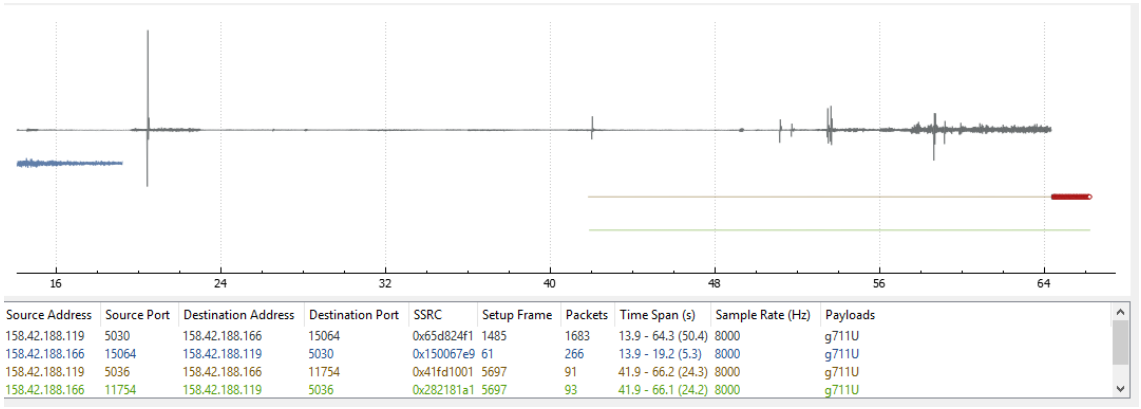


Figura 35. Paquetes enviados conversación múltiple.



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
158.42.188.119	5030	158.42.188.166	15064	0x65d824f1	1485	1683	13.9 - 64.3 (50.4)	8000	g711U
158.42.188.166	15064	158.42.188.119	5030	0x150067e9	61	266	13.9 - 19.2 (5.3)	8000	g711U
158.42.188.119	5036	158.42.188.166	11754	0x41fd1001	5697	91	41.9 - 66.2 (24.3)	8000	g711U
158.42.188.166	11754	158.42.188.119	5036	0x282181a1	5697	93	41.9 - 66.1 (24.2)	8000	g711U

Figura 36. Gráfico de la conversación múltiple.

158.42.188.119	5067	158.42.188.166	16462	0x32106df5	g711U	2064	0 (0.0%)	43.333	7.343	5.246
158.42.188.166	14850	158.42.188.119	5061	0x45266018	g711U	1771	0 (0.0%)	40.010	7.497	5.082
158.42.188.166	16462	158.42.188.119	5067	0xf321905	g711U	2054	0 (0.0%)	42.200	7.851	5.250

Figura 37. Paquetes perdidos conversación múltiple.

4.4 Modificar los códecs.

Para este escenario modificamos los códecs de ambos extremos, tanto de 1001 como de 1002, para que no tengan en común ninguno y poder observar si es posible la comunicación entre ambos. Primeramente se envía un INVITE para establecer la comunicación y es respondido con un error 488 donde nos especifica que no se puede aceptar la llamada. Si analizamos el error podemos observar que es un error en el cliente o en la petición, al establecer la conexión el protocolo SDP se encargará de describir la sesión multimedia, es decir, elegir el códec soportado por ambos extremos y en este caso no es posible adjudicarlo.

132 6.457227	158.42.188.166	158.42.188.119	SIP	532	Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
133 6.482963	158.42.188.119	158.42.188.166	SIP	721	Status: 200 OK |
150 7.414731	158.42.188.119	158.42.188.166	SIP/SDP	904	Request: INVITE sip:1002@158.42.188.166 |
151 7.416428	158.42.188.166	158.42.188.119	SIP	608	Status: 401 Unauthorized |
152 7.418257	158.42.188.119	158.42.188.166	SIP	419	Request: ACK sip:1002@158.42.188.166 |
153 7.419572	158.42.188.119	158.42.188.166	SIP/SDP	1160	Request: INVITE sip:1002@158.42.188.166 |
154 7.421274	158.42.188.166	158.42.188.119	SIP	457	Status: 488 Not Acceptable Here |
155 7.423378	158.42.188.119	158.42.188.166	SIP	408	Request: ACK sip:1002@158.42.188.166 |
346 18.271275	158.42.188.119	158.42.188.166	SIP	684	Request: OPTIONS sip:158.42.188.166 |
347 18.273272	158.42.188.166	158.42.188.119	SIP	618	Status: 401 Unauthorized |

Figura 38. Métodos enviados modificación de códecs.

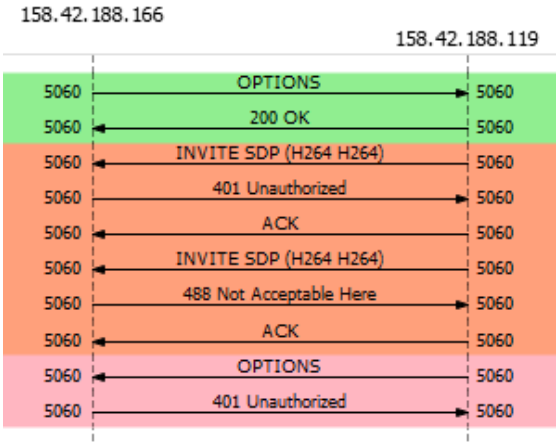


Figura 39. Mensajes enviados modificación de códecs.

4.5 Modificar anchos de banda.

En este escenario haremos uso de un software adicional llamado NetLimiter con el cual nos permite controlar el ancho de banda sobre las aplicaciones. Seleccionaremos el programa softphone utilizado que es Jitsi y limitaremos el ancho de banda a 5 KB/s.

Figura 40.Limitacíon ancho de banda NetLimiter.

Estableceremos la conexión entre 1002 que será quien tenga el ancho de banda modificado y 1001. El transcurso de los paquetes es de una llamada normal donde se utiliza el método INVITE con el fin de establecer el inicio de una llamada. El servidor recibirá un trying y ringing que es para intentar establecer la conexión, es decir, el destinatario recibirá un aviso de llamada. La respuesta final a la invitación viene dada por el Status: 200 OK, el emisor enviará un ACK confirmando que la invitación ha sido aceptada. Para finalizar la llamada utilizará BYE con su correspondiente ACK.

10	2.087637	158.42.188.166	158.42.188.119	SIP	532	Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
11	2.112293	158.42.188.119	158.42.188.166	SIP	722	Status: 200 OK |
29	8.101244	158.42.188.166	158.42.188.119	SIP/SDP	1132	Request: INVITE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
30	8.155936	158.42.188.119	158.42.188.166	SIP	556	Status: 180 Ringing |
34	8.658300	158.42.188.119	158.42.188.166	SIP	556	Status: 180 Ringing |
38	9.660647	158.42.188.119	158.42.188.166	SIP	556	Status: 180 Ringing |
41	10.295176	158.42.188.119	158.42.188.166	SIP/SDP	802	Status: 200 OK |
42	10.297483	158.42.188.166	158.42.188.119	SIP	502	Request: ACK sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
1208	22.277248	158.42.188.119	158.42.188.166	SIP	684	Request: OPTIONS sip:158.42.188.166 |
1209	22.278844	158.42.188.166	158.42.188.119	SIP	618	Status: 401 Unauthorized |
2481	40.937845	158.42.188.166	158.42.188.119	SIP	526	Request: BYE sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
2483	40.960392	158.42.188.119	158.42.188.166	SIP	548	Status: 200 OK |
2517	47.260874	158.42.188.119	158.42.188.166	SIP	684	Request: OPTIONS sip:158.42.188.166 |
2518	47.263398	158.42.188.166	158.42.188.119	SIP	618	Status: 401 Unauthorized |
2705	62.086734	158.42.188.166	158.42.188.119	SIP	532	Request: OPTIONS sip:1001@158.42.188.119:5060;registering_acc=158_42_188_166 |
2706	62.113828	158.42.188.119	158.42.188.166	SIP	722	Status: 200 OK |
2777	72.278591	158.42.188.119	158.42.188.166	SIP	684	Request: OPTIONS sip:158.42.188.166 |
2778	72.280316	158.42.188.166	158.42.188.119	SIP	618	Status: 401 Unauthorized |

Figura 41. Métodos enviados modificación ancho de banda.

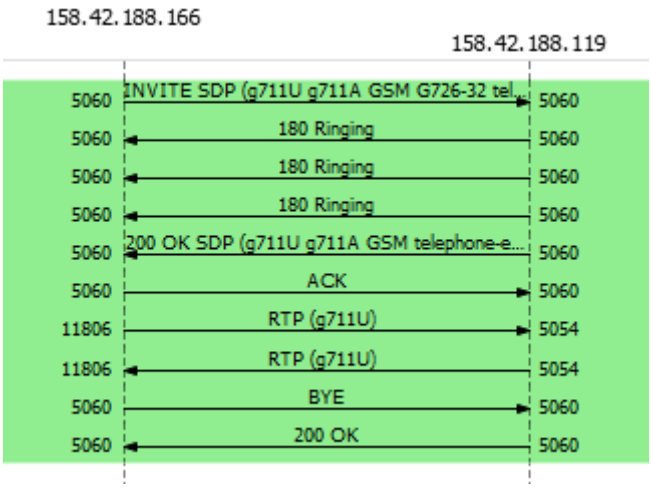


Figura 42. Mensajes enviados modificación ancho de banda.

Analizamos el valor del jitter y observamos que la media estaba entre 112,4 ms, es decir, sobrepasa el valor de los 100 ms y no podía asegurar que no hubiese pérdidas o retrasos. En las pruebas del laboratorio de sonido no hubo ninguna pérdida de paquetes pero si se podía apreciar cierto retraso a la hora de recibir el audio.

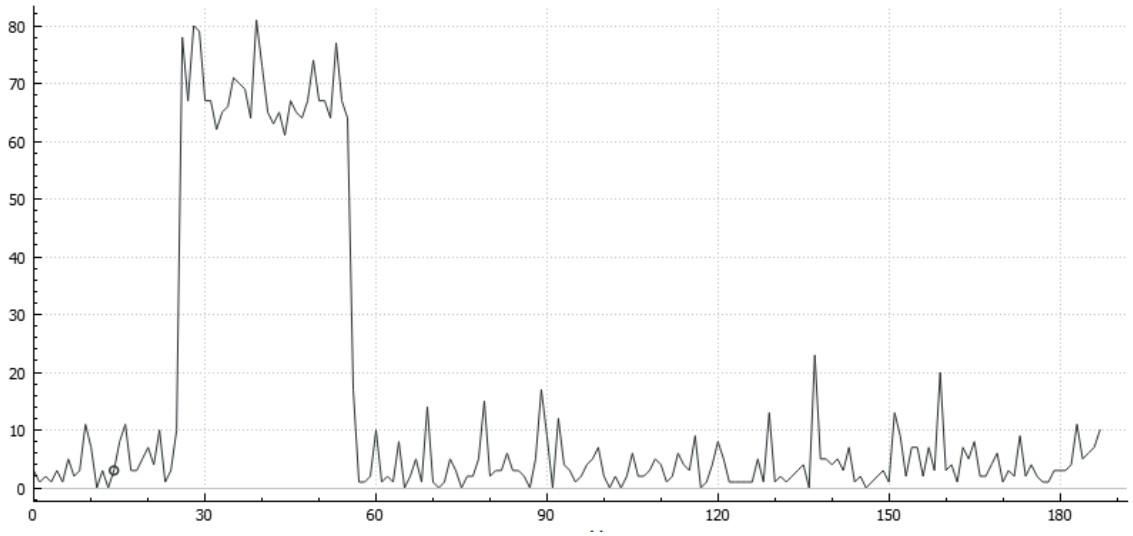


Figura 43. Paquetes enviados modificación ancho de banda.

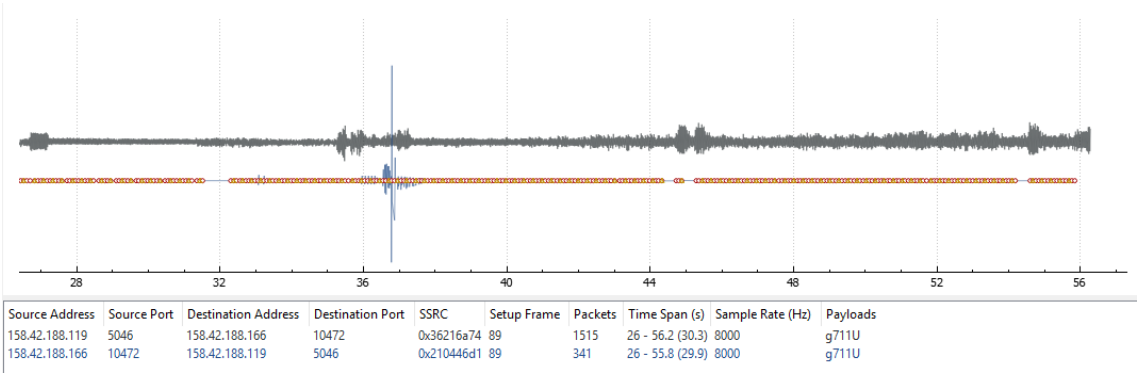


Figura 44. Gráfico de la conversación de la modificación ancho de banda.

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
158.42.188.119	5046	158.42.188.166	10472	0x36216a74	g711U	1515	0 (0.0%)	36.232	6.351	4.728	
158.42.188.166	10472	158.42.188.119	5046	0x210446d1	g711U	341	0 (0.0%)	786.150	112.404	67.909	

Figura 45. Paquetes perdidos modificación ancho de banda.

Ahora configuramos el ancho de banda a 3 KB/s y observamos una pérdida de paquetes considerable como también la calidad del audio llega a ser molesta para mantener una conversación. Podemos observar que el valor del jitter sobrepasa los 100 ms que es el valor establecido para mantener una interlocución satisfactoria.

Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
0 (0.0%)	4413.445	197.412	11.613	
0 (0.0%)	4399.363	38.068	7.699	
5967 (76.5%)	17126.480	197.652	14.986	

Figura 46. Parámetros obtenidos ancho de banda 3KB/s.

Si configuramos el ancho de banda a 2 KB/s vemos que la llamada no se puede realizar y queda a la espera, si desactivamos la opción del control del ancho de banda la comunicación se vuelve a restablecer de forma habitual.

Una vez realizado las distintas restricciones de ancho de banda, obtenemos el gráfico de la red que nos proporciona el programa Netlimiter en concreto para el softphone utilizado. Como podemos apreciar Jitsi ronda sobre los 9 Mb de velocidad de descarga y sobre los 11 Mb de subida. Se puede observar como varía el diagrama si se restringe las distintas velocidades.

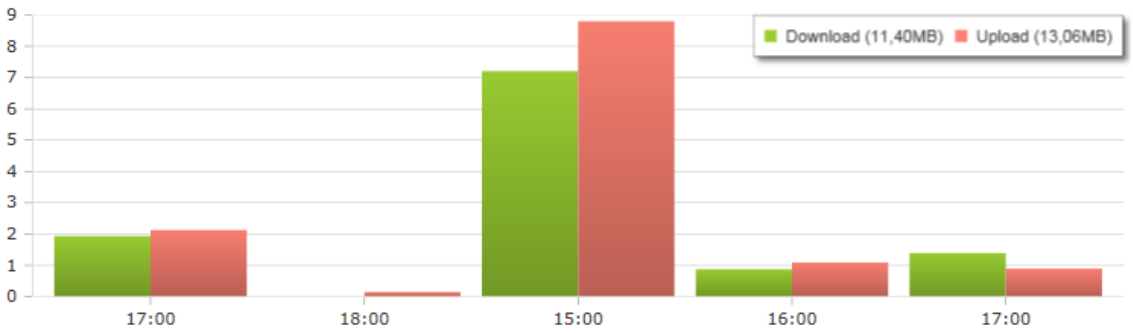


Figura 47. Gráfico ancho de banda utilizado por Jitsi.

4.6 Perdidas:

Con ayuda del software Clumsy se le añadirá distintos porcentajes de pérdidas para así comprobar los valores medios del jitter como también los porcentajes de los paquetes perdidos a lo largo de las diferentes pruebas para la dirección IP del servidor Asterisk. Se utilizará un escenario convencional de emisor y receptor y se grabarán las distintas conversaciones para una comparación de calidad de experiencia del usuario.

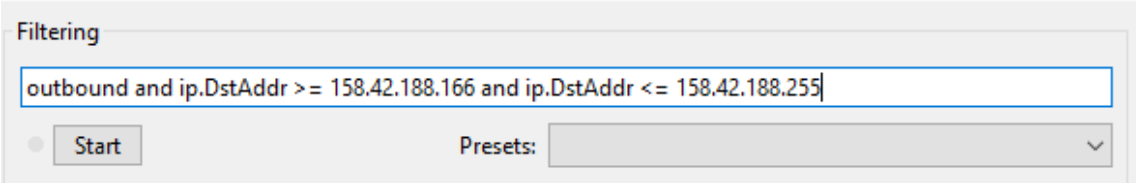


Figura 48. Configuración dirección IP Clumsy

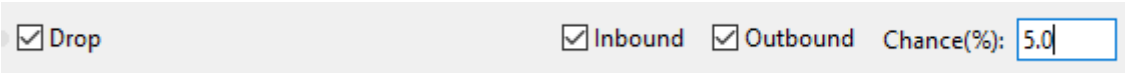


Figura 49. Añadir pérdidas Clumsy.

Primeramente se captura con el Wireshark una conversación sin pérdidas para tener una referencia y así poder comparar los valores adquiridos. Se estudia que el valor del jitter se encuentra entre los valores correctos para mantener una conversación buena y que este valor no supera los 100 ms. El porcentaje de pérdidas es del 0%.

Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
1751	0 (0.0%)	109.507	13.795	6.498	
1719	0 (0.0%)	1277.107	85.366	13.802	
237	0 (0.0%)	32.932	7.542	6.066	

Figura 50. Conversación sin pérdidas.

· **Pérdidas de 5%:**

Se añade un porcentaje de pérdidas del 5% en el software Clumsy y se obtiene que el valor del jitter se encuentre entre los parámetros correctos pero empieza a apreciarse ciertas pérdidas que rondan el 5% y no afecta al usuario a la hora de mantener un dialogo.

Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
g711U	693	0 (0.0%)	63.016	8.347	6.339	
g711U	720	0 (0.0%)	182.391	26.977	10.441	
g711U	123	7 (5.4%)	58.230	7.069	6.101	

Figura 51. Parámetros obtenidos pérdidas 5%.

· **Pérdidas 10%:**

Se añade un porcentaje de pérdidas del 10% en el software Clumsy y como es de esperar obtenemos un porcentaje de pérdidas sobre el 10% y empieza a aprecirase de forma negativa la calidad de experiencia del usuario.

Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
g711U	1602	0 (0.0%)	83.084	9.264	6.506	
g711U	1755	0 (0.0%)	381.394	29.272	12.567	
g711U	211	21 (9.1%)	70.926	7.422	6.486	

Figura 52. Parámetros obtenidos pérdidas 10%.

· **Pérdidas 20%:**

Se añade un porcentaje de pérdidas del 20% y se observa que los resultados obtenidos por Wireshark rondan sobre lo esperado. Si analizamos la calidad de experiencia se va haciendo muy difícil mantener una conversación clara entre ambos.

Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
g711U	1824	0 (0.0%)	4634.081	25.169	8.838	
g711U	1475	0 (0.0%)	4645.437	9.113	6.464	
g711U	195	41 (17.4%)	80.767	6.823	5.865	
g711U	232	651 (73.7%)	13045.680	11.434	7.650	

Figura 53. Parámetros obtenidos pérdidas 20%.

· **Pérdidas 30%:**

Se añade un porcentaje de pérdidas del 30% en el software Clumsy y el porcentaje de pérdidas obtenido es el esperado. Cabe destacar que la conversación entre emisor y receptor es imposible de llegar a un entendimiento.

Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter
g711U	997	36 (3.5%)	2465.798	17.036	6.975
g711U	1478	0 (0.0%)	2435.400	18.536	8.158
g711U	157	79 (33.5%)	112.909	7.143	5.799
g711U	172	1132 (86.8%)	19694.055	12.749	7.030

Figura 54. Parámetros obtenidos pérdidas 30%.

· **Pérdidas 50%:**

Se añade un porcentaje de pérdidas del 50% en el software Clumsy y como se observa en la siguiente figura los paquetes perdidos rondan el 80%. Si se analiza la calidad de conversación es completamente imposible poder recibir una palabra de forma correcta.

Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
0 (0.0%)	2021.765	8.097	6.127	
0 (0.0%)	2001.559	22.690	8.165	
1800 (83.3%)	33821.309	7.191	5.783	
0 (0.0%)	49.252	8.102	6.085	

Figura 55. Parámetros obtenidos pérdidas 50%.

Si añadimos un porcentaje más elevado de pérdidas directamente no deja mantener una conversación, mostrando un mensaje de error por parte del softphone.

Capítulo 5. CONCLUSIONES

Este proyecto tiene como objetivo la instalación en el laboratorio un servidor Asterisk que permita ejecutar, configurar y administrar una central telefónica de forma rápida y sencilla. El principal objetivo es asentar los conocimientos adquiridos en clase de teoría sobre VoIP y SIP, para ello se realizará distintos escenarios y se monitorizará con ayuda de Wireshark los distintos procesos para la realización de una llamada y poder concretar y estudiar la calidad de servicio como la calidad de experiencia del usuario. Para ello se utilizará un softphone gratuito para poder realizar la comunicación entre los usuarios.

El proyecto se ha dividido en dos bloques principales la instalación del servidor y realizar los distintos escenarios y así poder estudiar y comprobar el funcionamiento del servidor.
Después de varias pruebas realizadas se decidió que el servidor que mejor resultados daba en el ámbito de investigación, sencillez y facilidad de instalación fue Asterisk. Su correcta instalación proporciono resultados muy favorables en el estudio de los diferentes escenarios.

Cabe destacar que el softphone utilizado es Jitsi pero se ha comprobado que también funciona correctamente con otros softwares gratuitos.

Si nos centramos en el estudio de las simulaciones podemos observar los distintos procedimientos llevados a cabo para analizar los distintos mensajes intercambiados, los gráficos de los paquetes enviados durante la conversación, el valor de los paquetes perdidos, del jitter como también poder reproducir la conversación mantenida durante la llamada.
Se nos permite realizar desvío de llamadas, conversaciones múltiples, modificar los códecs entre otras opciones más.

También hemos realizado con ayuda del software Netlimiter diferentes pruebas de ancho de banda para poder observar si se realiza la llamada correctamente, si hay retardos o pérdidas de paquetes. También junto con Clumsy hemos forzado a añadir pérdidas para grabar las diferentes conversaciones obtenidas y poder estudiar la calidad de experiencia del usuario. Llegando a la conclusión que a partir del 30% de pérdidas como también que reducir el ancho de banda a más de 2Kb/s no es posible mantener una conversación de forma fluida. Esta parte del proyecto se puede estudiar de mejor forma con los audios grabados de todos los distintos parámetros modificados.

Cabe mencionar que este proyecto queda abierto para posibles futuros estudios con otras simulaciones incluso también una vez establecido el servidor y haber estudiado con los alumnos las diferentes pruebas, posibilita cambiar diferentes comportamientos del servidor para facilitar la investigación de la VoIP y del protocolo SIP.

BIBLIOGRAFÍA

[1] Pérdidas y retardos. https://sites.google.com/site/largadistanciadesdetupcvoip/retardo-o-latencia

[2]Calidad de Servicio. http://elastixtech.com/fundamentos-de-telefonia/voip-telefonia-ip/

[3]Diseño de protocolo a nivel de transporte. https://www.securityartwork.es/2008/02/27/voip-protocolos-de-transporte/

[4] Mensajes del protocolo SIP. https://seguridadyredes.wordpress.com/2010/04/05/wireshark-captura-conversaciones-voip-protocolo-sip-sdp-y-rtp-extraccion-de-audio/

[5] Servidor Asterisk. https://wiki.asterisk.org/wiki/display/AST/Installing+AsteriskNOW