ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

ANÁLISIS DE LA PAQUETIZACIÓN DE VOZ SOBRE IP EMPLEANDO EL PROTOCOLO DE INICIO DE SESIONES SIP CON BACK TO BACK USER AGENT (B2BUA) EN UNA APLICACIÓN SOBRE REDES WI-FI

VÍCTOR HUGO LÓPEZ CHALACÁN

SANGOLQUÍ – ECUADOR

2011

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: “Análisis de la paquetización de Voz sobre IP (VoIP) empleando el protocolo de inicio de sesiones SIP con Back To Back User Agent (B2BUA) en una aplicación sobre redes Wi-Fi”, fue realizado en su totalidad por el señor Víctor Hugo López Chalacán, bajo nuestra dirección.

Ing. Freddy Acosta	Ing. Darío Duque
DIRECTOR	CODIRECTOR

RESUMEN

En el desarrollo del presente proyecto se ha realizado un análisis de la paquetización de Voz sobre IP, empleando el protocolo de señalización de comunicación más ampliamente utilizado en la tecnología Voz sobre IP, denominado: Protocolo de Inicio de Sesiones (SIP), obteniendo la comunicación de voz directa de persona a persona en tiempo real a través del gran uso de la Internet. La aplicación del proyecto permite realizar y recibir llamadas, desde y hacia Estados Unidos, mediante la Internet. Utilizando dispositivos terminales de VoIP basados en SIP tanto en *hardware* como en *software*, sobre una red inalámbrica Wi-Fi.

El proyecto fue dividido en tres bloques principalmente: la suscripción con el proveedor de servicio VoIP o ITSP (*Internet Telephony Service Providers)*, configuración del router inalámbrico, y la configuración de los dispositivos terminales SIP.

Para el presente proyecto se utilizó el proveedor CallCentric (*Internet Phone Service*), el cual ofrece VoIP basado en el servicio de teléfono de banda ancha utilizando el protocolo SIP. Los servicios incluyen llamadas salientes y llamadas entrantes en los Estados Unidos.

Para el desarrollo de la red inalámbrica Wi-Fi se utilizó router *Linksys* por Cisco *Wireless N Gigabit* modelo WRT310N v2.

En el proyecto se utilizó: el dispositivo terminal SIP en *hardware: WLAN660S Wi-Fi SIP Phone*, y una computadora laptop Wi-Fi en la cual se encuentra instalada la aplicación para realizar llamadas VoIP: el dispositivo terminal SIP en *software:* el *Softphone* X-Lite versión 4.0. Además para la captura y análisis de los paquetes SIP la computadora contiene el analizador de protocolos *Wireshark*. Con la información proporcionada por el proveedor de servicio VoIP se configuran los parámetros requeridos por los terminales SIP.

DEDICATORIA

Esencialmente quiero dedicar este trabajo a mi Dios, puesto que todo es de Dios, todo es por Él y para Él.

A mis amados padres, José y Gladis, por su profundo amor para con todos sus hijos, y por enseñarnos a ser verdaderamente una familia unida.

A mis lindos hermanos: Jeanneth, Mireya, y José Luis (yo soy el “ultimito”), ellos son realmente mi orgullo y son mi ejemplo a imitar, ustedes son mi fuerza, mi motivación, mi respaldo.

A mis preciosos sobrinos: Andrés Sebastián y Fernanda Antonela, ellos son el motor que mueve vida, son mis tesoros.

A todo aquel que esté interesado en consultar e investigar, en el fascinante mundo de Voz sobre IP.

AGRADECIMIENTO

De todo corazón, quiero dar el agradecimiento principal y más importante a Dios, *El ingeniero por excelencia*, por darme las fuerzas, la inteligencia, la sabiduría, los recursos tanto materiales como humanos, necesarios en todo el proceso para finalizar mi carrera profesional. Porque no es por mis fuerzas, ni por mis capacidades, todo es por la tierna gracia de Dios. Siempre he podido ver su mano poderosa ayudándome en mis estudios, reconociendo que: todo es de Dios, todo es por Él y para Él.

Gracias mí Dios por los estudios que me has dado, ayúdame Dios a glorificar tu nombre en mi vida profesional, y que cada día aplique tu palabra en mi forma de pesar. Toda la gloria y honra sean dadas a ti.

Nuevamente quiero dar las gracias a Dios por darme la mejor familia del mundo, ya que sin ellos no sería nada ni nadie.

Un especial agradecimiento a mis amados padres, José y Gladis, por su inmenso amor, cariño, compresión, cuidado, y bueno faltarían hojas para describirlos ☺, ellos han sido realmente un pilar fundamental en mi vida, los amo mucho.

De la misma forma un agradecimiento muy especial a mis lindos hermanos: Jeanneth, Mireya, y José Luis. Gracias por quererme y ayudarme siempre de una manera muy especial, son lo máximo, los quiero ñaños.

Gracias a toda mi familia en general: abuelitos Teresita y Humbertito, cuñados, sobrinos, tíos, primos, entre otros, gracias por siempre apoyarme, por su preocupación, por sus bendiciones, por sus hermosas palabras que me infunden aliento cada día.

A mis compañeros y amigos, gracias por su ayuda incondicional en cada momento, a mis compañeros gracias por ser un grupo unido, por apoyarnos y porque son un excelente grupo de trabajo.

A una persona muy especial Christine Bullock, gracias por su ayuda, oraciones y apoyo incondicional en el todo el transcurso de este trabajo.

A mi querido grupo pequeño, a todos y cada uno de ustedes muchísimas gracias por sus oraciones, buenos deseos, por su preocupación, por estar “monitoreándome”, ustedes son una gran bendición en mi crecimiento espiritual, a la cabeza de nuestra querida facilitadora Gabita Espín.

A los ingenieros Freddy Acosta y Darío Duque, por su apoyo y colaboración en la realización de este proyecto.

A todos y cada uno de usted mil gracias, Dios les pague.

Víctor Hugo López.

PRÓLOGO

Con el paso del tiempo, las tecnologías de comunicación sobre redes, concretamente en el campo de la telefonía, han obtenido grandes logros, a partir de la creación del telégrafo hasta nuestros días, como resultado del desarrollo de la tecnología en la informática y telecomunicaciones, es posible transmitir la señal de voz humana en paquetes sobre las redes de datos IP, esto en nuestros días se lo conoce como Voz sobre IP (VoIP). Mediante VoIP permite unir la transmisión de voz con la transmisión de datos.

La Voz sobre IP, permite la transmisión de la señal de voz, para conseguir esto la señal es comprimida y digitalizada de manera muy eficiente, estableciendo un modelo o sistema que permita "*empaquetar*" la señal de la voz, en las cuales la información a transmitir se divide en unidades de información denominados *paquetes*, para que puedan viajar a través de redes de datos.

Teniendo en cuenta que la red de Internet es la "red de redes", nos dirige claramente al protocolo IP (*Internet Protocol*), en la cual se aprovecha el ancho de banda y la infraestructura de redes alámbricas e inalámbricas existentes (redes Wi-Fi), consiguiendo un ahorro importante en costos, tanto para empresas de telecomunicaciones como a personas particulares.

SIP (es el acrónimo en inglés de *Session Initiation Protocol* o en español Protocolo de Inicio de Sesiones) es un protocolo de señalización de comunicación ampliamente utilizado en la tecnología Voz sobre IP, para la comunicación por voz y vídeo directa de persona a persona en tiempo real a través de Internet. Permitiendo mensajería instantánea, presencia (si están *online* o no), voz, video, intercambio de archivos instantáneamente, compartir aplicaciones y mucho mas. El protocolo SIP contiene una entidad lógica denomina Back to Back User Agent (B2BUA), encargada del control, gestión de llamadas entre usuarios SIP, interconexión de red, transcodificación entre los puntos terminales de la llamada, entre otros.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

3PCC: Third party call controller.

ACK: Acknowledgement.

ADC: Analog to digital converter.

ADPCM: Adaptive Differential Pulse Code Modulation.

AES: Advanced Encryption Standard.

ARP: Address Resolution Protocol.

ARP: Address Resolution Protocol.

ARPANET: Advanced Research Projects Agency Network.

AVP: Audio Video Profiles.

B2BUA: Back to Back User Agent.

CELP: Code Excited Linear Prediction.

CoS: Class of Service.

CS-ACELP: Conjúgate Structure Algebraic Code Excited Linear Prediction.

DAC: Digital to analog converter.

DARPA: Defense Advanced Research Projects Agency.

DNS: Domain Name System.

DSCP: DiffServ Código Point.

DSP: Digital Signal Processor.

FDM /MDF: Frequency Division Multiplexing, Multiplexación por División de Frecuencia.

FTP: File Transfer Protocol.

HTTP: HyperText Transfer Protocol.

IANA: Internet Assigned Numbers Authority.

ICMP: Internet Control Message Protocol.

IEEE: Institute of Electrical and Electronics Engineers.

IETF: Internet Engineering Task Force.

IGMP: Internet Group Management Protocol.

IP: Internet Protocol.

ISDN: Integrated Services Digital Network.

ITSP: Internet Telephony Service Providers.

ITU: International Telecommunication Union.

LAN: Local Area Network.

LD-CELP: Low-Delay Code Excited Linear Prediction.

MAC: Media Access Control.

MIC: Modulación por Impulsos Codificados.

MOS: Mean Opinion Score.

MTU: Unidad de Transmisión Máxima.

NAT: Network Address Translation.

NIC: Network Interface Card.

OUI: Organizationally Unique Identifier.

PBX: Private Branch Exchange.

PCM: Pulse Code Modulation.

PDA: Personal digital assistant, Asistente digital personal.

PDU: Protocol Data Unit.

POP: Post Office Protocol.

POTS: Plain Old Telephone Service.

PSK: Pre Shared Key.

PSTN/RTPC: Public Switched Telephone Network, Red Telefónica Pública Conmutada.

QoS: Calidad de Servicio.

RARP: Reverse Address Resolution Protocol.

RAS: Registration, Admission and Status.

RFC: Request for Comments, Petición De Comentarios.

RPE-LTP: Regular Pulse Excitation LongTerm Predictor.

RTB: Red Telefónica Básica.

RTC: Red Telefónica Conmutada.

RTCP: Real-time Transport Control Protocol.

RTP: Real-time Transport Protocol.

SDP: Session Description Protocol.

SIP: Session Initiation Protocol.

Smartphone: Teléfono inteligente.

SMTP: Simple Mail Transfer Protocol.

SSID: Service Set IDentifier.

TCP: Transmission Control Protocol.

TDM /MDT: Time Division Multiplexing, Multiplexación por división de tiempo.

TELNET: Telecommunication Network.

TKIP: Temporal Key Integrity Protocol.

ToIP: Telefonía sobre IP.

TOS: Tipo de Servicio.

UA: Agente de Usuario.

UAC: Agente de Usuario Cliente.

UAS: Agente de Usuario Servidor.

UDP: User Datagram Protocol.

URI: Uniform Resource Identifier.

URL: Uniform Resource Locator

URN: Uniform Resource Name

UUIE: User to User Information Element.

VAD: Voice Activity Detection.

VoIP: Voice Over Internet Protocol, Voz sobre IP.

WAN: Wide Area Network.

WECA: Wireless Ethernet Compatibility Alliance.

WEP: Wired Equivalent Privacy.

WMM: Wi-Fi Multimedia.

WPA: Wi-Fi Protected Access.

WPA2: Wi-Fi Protected Access 2.

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

Con el paso del tiempo, las tecnologías de comunicación sobre redes, concretamente en el campo de la telefonía, han obtenido grandes logros, a partir de la creación del telégrafo hasta nuestros días, como resultado del desarrollo de la tecnología en la informática y telecomunicaciones, es posible transmitir la señal de voz humana en paquetes sobre las redes de datos IP, esto en nuestros días se lo conoce como Voz sobre IP (VoIP).

1.1.1 Historia de la red telefónica tradicional

El término telefonía proviene del griego "tele" (lejos, distancia) y "fonia" (sonidos), que aparece a finales del siglo XIX con la invención del teléfono, inicialmente fue considerado como inventor del teléfono a Alexander Graham Bell, ya que él fue el primero en patentarlo, pero más tarde correctamente se le reconoció como inventor del teléfono a Antonio Meucci en el 2002.

Este artefacto (llamado teléfono), consistía principalmente de un altavoz y un micrófono, que se encontraban conectado con otro teléfono de similares características, ubicado a cierta distancia, Esta conexión se la realizó a través del cable, por medio de dicho cable se transmitía y recibía la señal de voz de cada uno de los teléfono situados en los extremos, por medio de esto se consiguió mantener conversaciones a cierta distancia.

En su fase inicial, cada persona que tenía este teléfono debía conectarlo por medio del cable, con el teléfono de la persona con la que desearía mantener una comunicación a distancia. En sus inicios el medio de transmisión se realizó a través de un hilo de hierro, además no disponían de circuitos de marcación.

El despliegue de esta red telefónica no fue ordenado. Porque comenzó como una simple agrupación de conexiones entre clientes, es decir una comunicación punto a punto, como se aprecia en la Figura 1.1.

Figura. 1.1. Agrupación de conexiones entre clientes.

Formando una topología de red telefónica completamente tipo malla, entre todos los usuarios que tenían teléfono, como se aprecia en la Figura 1.2.

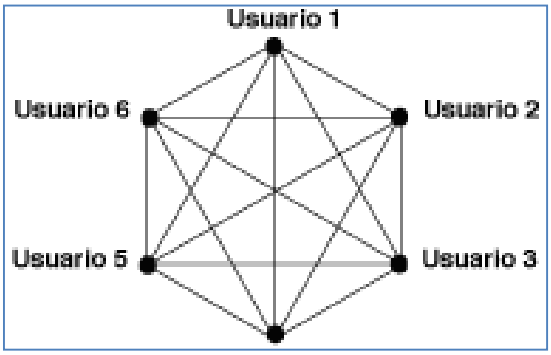

Figura. 1.2. Topología de red telefónica completamente tipo malla.

Esto dio lugar a la aparición de montones de cables tendidos por las ciudades conectando teléfonos como se aprecia en la Figura 1.3.

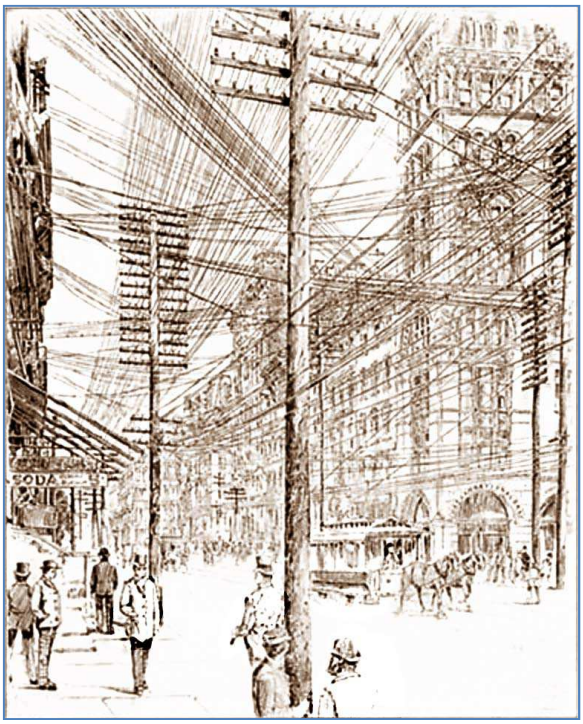

Figura 1.3. Tendidos de cable en Nueva York 1890.

Con el crecimiento del número de clientes esta situación en poco tiempo se volvió inmanejable, consecuentemente surgió la necesidad de crear una solución. Una entidad general que se encargue de gestionar los cables, llevando a la creación de centralitas, como sitios donde se establecen conexiones entre los abonados, de modo que cada teléfono se conectó a una centralita, a las que llegaban los cables que provenían de todos los aparatos de una determinada zona, como se aprecia en la Figura 1.4.

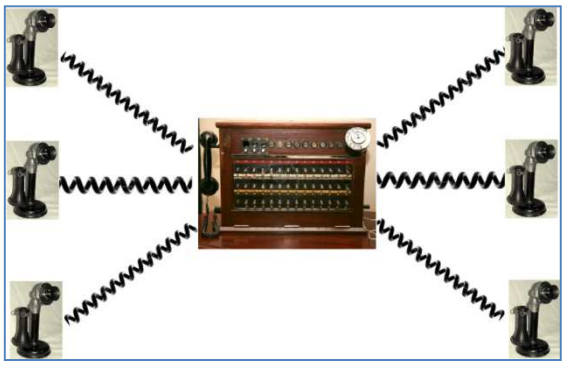

Figura. 1.4. Conexión de teléfonos a la centralita.

Aquellas primeras centralitas telefónicas no eran automáticas, la conexión entre el origen y el destino de la llamada, se realizaba de forma manual en las centrales telefónicas, es decir debían estar controladas por un operador humano.

Para realizar una llamada telefónica, un abonado descolgaba el teléfono y se requería al operador la comunicación con la persona deseada, esto permitía hablar con cualquier teléfono que estuviera conectado a la centralita; La operadora pinchaba la clavija de comunicación en grandes paneles con cuantiosos conectores, como se aprecia en la Figura 1.5.

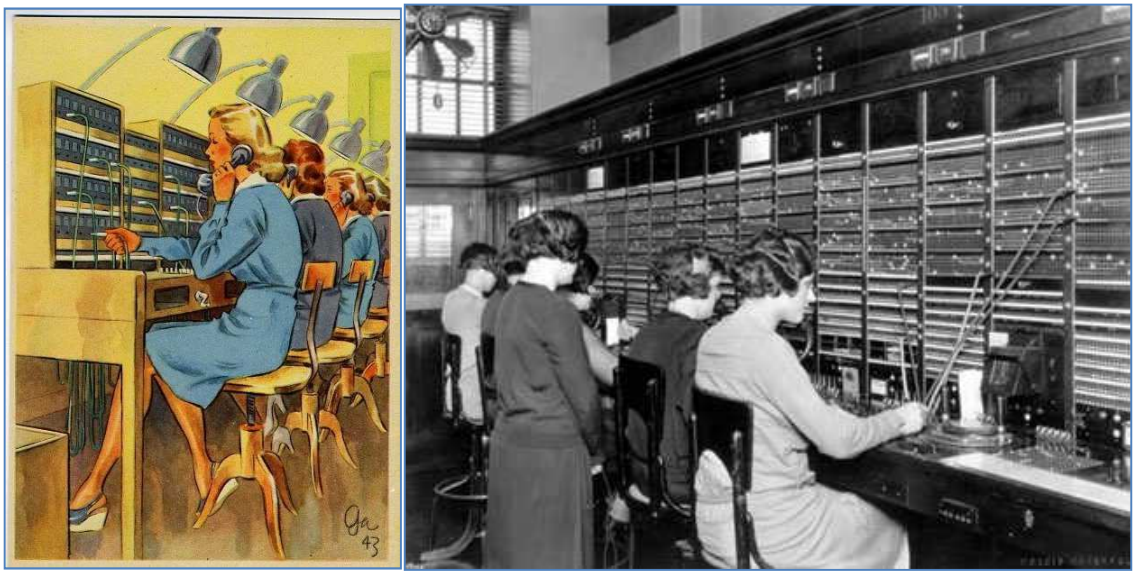

Figura. 1.5. Operadora manual en su panel.

En la cual las operadoras unían los cables de ambos teléfonos, si la llamada era local, en el caso de que la comunicación con la persona deseada, se encuentre en otra zona, el operador se conectaba con otra centralita, y el nuevo operador continuaba con la petición para poder realizar la llamada, formando una conexión entre topologías de red tipo estrella, como se aprecia en la Figura 1.6, para lograr esto, fue necesario identificar cada teléfono con un número único.

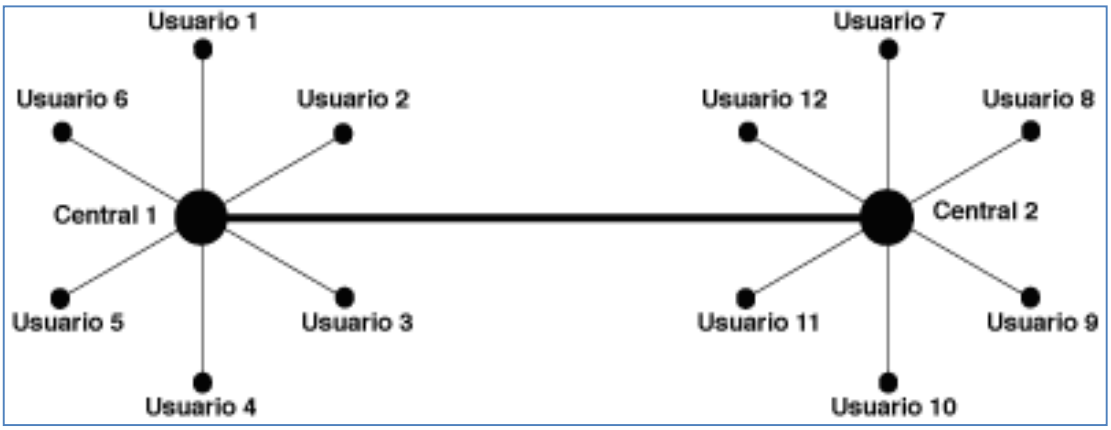

Figura. 1.6. Interconexión entre centrales o topologías de red tipo estrella.

En las organizaciones, se comienza a utilizar el término PBX[1], que no es más que un panel de conmutaciones o conexiones a cargo de un operador humano.

Con este proceso, una llamada de costa a costa en los EE UU podía llegar a tardar dos horas en establecerse, por la cantidad de operadores que estaban involucrados (sin embargo la espera promedio era de de 15 minutos).

Este problema se solucionó con el invento de Almon Brown Strowger, que después de tener conocimiento de que la operadora o la telefonista encargada de la conmutación manual de las llamadas, había desviado la de un cliente hacia el negocio de un competidor, Strowger no descansó hasta inventar un sistema que pudiera evitar la intervención de operadores manuales.

Strowger inventó un determinado sistema de marcado en los teléfonos, para que la llamada se conmute automáticamente al destino requerido, con el apoyo de su sobrino Walter S. Strowger realizaron un sistema de conmutación del que solicitó una patente en 1889, que le fue concedida con el número US447918 en 1891. [1]

[1] PBX (Private Branch Exchange) literalmente rama privada de intercambio, dispositivo que permite la interconexión de teléfonos (en este contexto extensiones), que interconectan una o varias salidas a la PSTN con estas extensiones.

En 1960 empiezan a surgir las primeras centralitas telefónicas automáticas electrónicas analógicas que realizaban la conmutación a través de relés. Con la invento de centrales telefónicas automáticas se consiguió eliminar los operadores humanos y acelerar el proceso de conmutación. En la actualidad, todo el proceso se ha automatizado, Las modernas centrales se encargan de recibir todas las llamadas y realizan las conexiones de forma casi instantánea.

Por muchos años la red telefónica fue analógica, lo que se enviaba y recibía, por medios de los cables, era la transformación directa de la voz en voltaje. La señal transmitida, desde el origen hasta llegar a su destino, tenía que pasar por varios filtros analógicos, como amplificadores, repetidores, etc., debido a que generalmente en sistemas de transmisión analógica se utilizaba multiplexación por división de frecuencia (MDF) o (FDM)[2] (Figura 1.7).

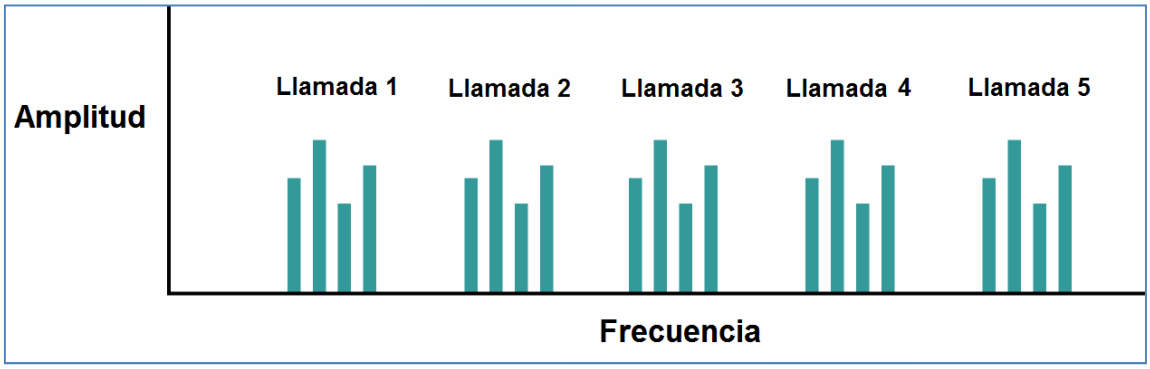

Figura. 1.7. Multiplexación por división de frecuencia (MDF) o (FDM).

Estos dispositivos insertaban ruido en la señal original, además la señal era muy susceptible a interferencias por problemas en los cables; El ruido introducido por estos dispositivos y la interferencia, no podían ser eliminados fácilmente, generando una baja calidad en la comunicación.

2 Multiplexación por división de frecuencia (MDF) o (FDM) del Inglés Frequency Division Multiplexing, es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos.

Se alcanzó eliminar completamente el ruido, mediante el desarrollo de la telefonía digital, utilizando conversores analógico/digital y digital/analógico consiguiendo una importante mejora en la comunicación, porque la señal de voz ya no se enviaba convertida en voltaje, lo que se enviaba ahora es la voz digitalizada, y al momento de pasar por los diversos dispositivos como repetidores, centrales, etc., la señal original es reconstruida totalmente.

Después de la invención del transistor y el avance de la electrónica digital se empieza a transformar las redes telefónicas en digitales, poco a poco en diversos países se han ido convirtiendo las redes telefónicas de análogas en digitales, sobre todo la conexión entre centralitas lo que se conoce como *trunking*[3], aunque la conexión entre el equipo de abonado (teléfonos) y la centralita continua siendo analógica, las centralitas digitalizan las señales análogas, para eliminar el ruido sobre todo en la conexión entre centrales.

Para la transmisión de señales analógicas utilizábamos la multiplexación por división de frecuencia, en la transmisión de señales digitales se modifica el modo de multiplexación por división de tiempo (*MDT*) o (*TDM*)[4], de esta forma se logra eliminar la presencia de filtros analógicos y un mejor aprovechamiento del medio de trasmisión, porque ocupa un canal de trasmisión (por lo general de gran capacidad) a partir de distintas fuentes o canales, el ancho de banda total del medio de transmisión es asignado a cada canal durante un intervalo de tiempo, como se aprecia en la Figura 1.8.

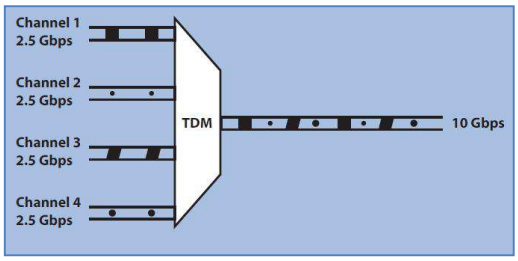

Figura. 1.8. Multiplexación por división de tiempo, un canal de trasmisión.

3 Llamada entre centralitas, canal de señalización compartido.

4 La multiplexación por división de tiempo (MDT) o (TDM), del Inglés Time Division Multiplexing, es el tipo de multiplexación más utilizado en la actualidad, especialmente en los sistemas de transmisión digitales.

En la multiplexación por división de tiempo podemos enviar un fragmento de la cierta conversación en menor tiempo que el original, la idea es poder comprimir la señal original, pensemos en la posibilidad de enviar un fragmento de una conversación que se originó en un extremo es de un segundo, mediante un cable tan solo ocupamos medio segundo, el medio de transmisión (el cable) se encuentra disponible en resto del medio segundo, lo cual se puede aprovechar el medio de transmisión para enviar un fragmento de otra conversación de duración medio segundo, con esto se consigue por medio de un solo cable obtener dos conversaciones simultáneas.

El proceso se obtiene "intercalando" muestras de diferentes señales, para transmitirlas en forma secuencial por el mismo canal como se aprecia en la Figura 1.9.

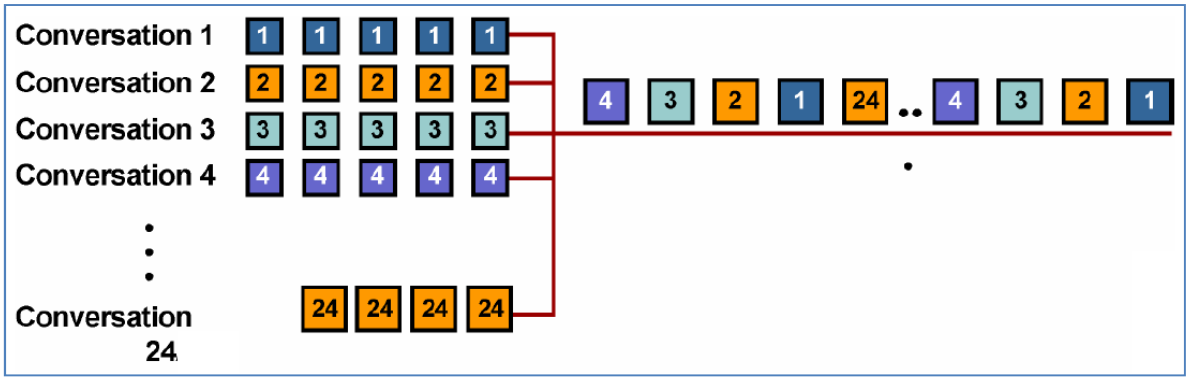

Figura. 1.9. Transmisión en forma secuencial, intercalando muestras de diferentes conversaciones.

Gracias a la digitalización de la voz, por ejemplo se puede dividir la conversación en fragmentos de milésimas de segundos y que pueden ser enviados a través del medio de transmisión (el cable) en menor tiempo, de esta manera se puede optimizar el medio de transmisión, es decir a través de un solo cable tener numerosas conversaciones simultáneas.

1.1.2 Funcionamiento básico de la red de telefonía básica RTB

La Red Telefónica Básica (RTB) se define como la agrupación de todos los medios de transmisión y conmutación necesarios, para conectar dos equipos terminales a través de un circuito físico que nos permite establecer una comunicación, este circuito físico es temporal que se desconecta al finalizar la llamada, este proceso realizan las redes de telecomunicaciones conmutadas. La Red Telefónica Conmutada RTC, también se la llama Red Telefónica Básica RTB, en su esencia es diseñada para la transmisión de la señal de la voz humana, además puede ser utilizada para transportar datos.

En la red telefónica clásica, los equipos terminales (teléfonos) se comunican por medio del par de cobre (un cable de dos hilos, uno de transmisión y el otro de recepción T y R) a una central de conmutación, este cableado entre la central telefónica y equipo terminan es denominado como *Bucle de Abonado*, en donde la información o señal de control, se transmite por el mismo canal por el que se está llevando a cabo la comunicación.

Desde el inicio de la telefonía automática existen señales de control, como la de descolgar, marcar y colgar, esto se realizaba mediante la apertura y cierra del bucle de abonado, actualmente la señal de control de marcación se realiza mediante tonos que son enviados por el equipo terminal telefónico hacia la central de conmutación, a través del mismo par de cobre por el que se realiza la conversación. Para la comunicación de dos usuarios o abonados de una red telefónica conmutada, se realiza por medio de la conmutación de circuitos, mediante esto se forma un canal dedicado para la conexión entre dos abonados, este proceso es diferente en la conmutación de paquetes. La conmutación de circuitos es una clase de conexión que se ejecuta en todos los diferentes puntos o nodos de la red, estos nodos deben estar en la capacidad de conmutar y de gestionar el canal necesario para establecer un canal dedicado con el fin de conseguir la conexión solicitada, mientras dure la conexión, la red reserva recursos para transmisión y conmutación, los conmutadores deben tener la inteligencia necesaria para realizar estas reservas y establecer una ruta a través de la red.

Estos recursos son utilizados exclusivamente en el circuito de comunicación, esta conexión es transparente, esto quiere decir que después de establecer la conexión, parece como que los dispositivos realmente estuvieran conectados. Con el avance tecnológico el funcionamiento básico de las redes de telefonía en su esencia no ha cambiado, propiamente dicho en la conmutación de circuitos, que se componen de tres frases: el establecimiento del circuito, la transferencia de voz/datos y la desconexión del circuito. Después del establecimiento del circuito para comunicarse entre el origen y destino, se fija un ancho de banda hasta que se termine la comunicación, para realizar otra comunicación con un diferente destino, primero se debe terminar la comunicación establecida.

1.2 SITUACIÓN ACTUAL

1.2.1 Introducción de Voz sobre IP (VoIP) y el protocolo SIP

Hoy por hoy es posible transmitir la señal de voz humana en paquetes sobre las redes de datos IP, esto en nuestros días se lo conoce como Voz sobre IP (VoIP). Mediante VoIP permite unir la transmisión de voz con la transmisión de datos. La Voz sobre IP, permite la transmisión de la señal de voz, para conseguir esto la señal es comprimida y digitalizada de manera muy eficiente, estableciendo un modelo o sistema que permita "*empaquetar*" la señal de la voz, en las cuales la información a transmitir se divide en unidades de información denominados *paquetes*, para que puedan viajar a través de redes de datos.

Actualmente el Protocolo de Inicio de Sesiones (SIP), es uno de los protocolos de señalización más utilizados en tecnología voz sobre IP. SIP ha sido estandarizado y dirigido principalmente por el IETF mientras que el protocolo de VoIP H.323 ha sido tradicionalmente más asociado con la Unión Internacional de Telecomunicaciones. Sin embargo, las dos organizaciones han promocionado ambos protocolos del mismo modo. SIP fue inicialmente publicado como un proyecto orientado a la integración y servicios de internet por el IETF en 1996, con su primer RFC en 1999, las especificaciones más reciente de SIP están publicadas en el RFC 3261.

SIP parece muy sencillo, y realmente lo es. Pero detrás de su sencillez se oculta su gran fortaleza; SIP posee un diseño “modular”, el cual es considerado como la fortaleza del protocolo SIP, esto le ha permitido ser utilizado en muchas aplicaciones. El alcance del protocolo SIP es relativamente amplio, incluyendo el establecimiento de prácticamente cualquier tipo de sesión entre dos partes. SIP interviene en la parte de señalización al establecer la sesión de comunicación, pero este protocolo trabaja conjuntamente con SDP y RTP/RTCP, donde SDP propiamente está diseñado para transportar información referente a las características de las sesiones, y parámetros de capacidades de negociación entre los integrantes de la sesión, como por ejemplo el listado de *Codecs* que están en la capacidad de soportar los integrantes de la sesión. Por otro lado RTP/RTCP se encarga de transportar los media streams o datos multimedia, propiamente dicho transporta el audio o video.

Hoy por hoy Voz sobre IP se encuentra generando grandes oportunidades para el desarrollo tecnológico de nuevos proyectos considerándolo como un problema dominante de investigación.

Los distribuidores de VoIP, telefonía IP, mensajería instantánea (como el Microsoft MSN Messenger), están todos normalizados sobre SIP. En Noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP[5] (*3rd Generation Partnership Project*) y elemento permanente de la arquitectura IMS (*IP Multimedia Subsystem*).

Hoy en día se está empezando a afirmar que lo que fue el protocolo HTTP para la Web, lo hará SIP para las telecomunicaciones [2]. SIP tiene grandes repercusiones en la industria de las telecomunicaciones. Las empresas de celulares han decidido normalizar sobre SIP todas las aplicaciones futuras. La comunicación en tiempo real de persona a persona ahora es posible al gran uso del internet, hoy por hoy el estándar de internet para comunicación, es el protocolo SIP.

5 3rd Generation Partnership Project (3GPP) es un acuerdo de colaboración en tecnología de telefonía móvil que fue establecido en diciembre de 1998.

SIP (es el acrónimo en Inglés de *Session Initiation Protocol* o en Español Protocolo de Inicio de Sesiones) es un protocolo de señalización de comunicación ampliamente utilizado en la tecnología Voz sobre IP, para la comunicación por voz y vídeo directa de persona a persona en tiempo real a través de Internet. Permitiendo mensajería instantánea, presencia (si están *online* o no), voz, video, intercambio de archivos instantáneamente, compartir aplicaciones y mucho mas.

Al igual que HTTP fue creado para la web y SMTP creado para el correo electrónico, SIP esta creado a través del gran uso del Internet para la comunicación en tiempo real entre personas, SIP es actualmente el protocolo de elección para realizar las nuevas instalaciones de VoIP, lo cual esta evidenciado por el apoyo de Microsoft, MCI, AT&T y muchos otros. Los Usuarios SIP en la red LAN tienen un alcance global y de todos los clientes SIP conectados a Internet, como se presenta en la Figura 1.10.

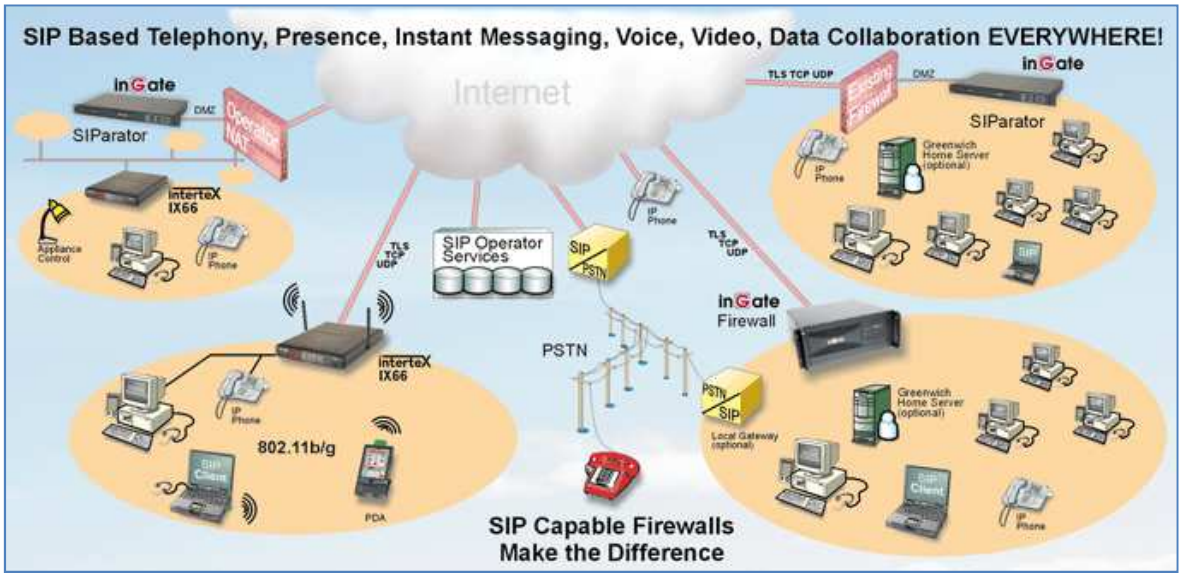

Figura. 1.10. Usuarios SIP tienen un alcance global de todos los clientes SIP conectados a Internet.

Actualmente existen una gran cantidad de dispositivos terminales que soportan aplicaciones VoIP basados en SIP, estas aplicaciones se encuentran tanto en hardware como en software, los cuales están disponibles comercialmente gracias a muchos fabricantes. Estos dispositivos terminales son teléfonos que permiten hacer llamadas utilizando tecnología VoIP, soportando SIP.

Los terminales físicos (hardware) tienen una apariencia como un teléfono convencional muy profesional. Los teléfonos SIP pueden también estar basados en software denominados *Softphone*, que no es otra cosa que un software que emula las funciones de un teléfono físico tradicional, permitiendo que cualquier computador pueda ser utilizado como teléfono.

1.2.2 Beneficios de VoIP (Voz sobre IP) y la telefonía IP

Las principales razones de las empresas, organizaciones y consumidores para elegir la telefonía IP en lugar de la telefonía tradicional son las siguientes:

- ✓ **Efectividad en costos**

  Las empresas nacionales y organizaciones pueden ahorrar hasta un 30-40% de sus gastos de teléfono utilizando VoIP. Las empresas internacionales pueden ahorrar drásticamente más, quizás hasta un 90%.

- ✓ **Funcionalidad**

  La telefonía IP es solo el comienzo. Con Voz sobre IP se puede beneficiar de la videoconferencia, mensajería instantánea, presencia, compartir archivos instantáneamente, entre otros.

- ✓ **Administración / Control**

  Con la telefonía tradicional (POTS) es el operador quien controla lo que puede y no puede hacer, y quien cobra incluso por una pequeña configuración del sistema. Con VoIP se podría tener el control completo al instante.

- ✓ **Trabajo con mayor eficiencia**

  Con VoIP se puede dirigir las llamadas entrantes para satisfacer necesidades específicas y forma de trabajo. Por ejemplo en un instante su oficina puede convertirse en centro de llamadas (*Call Center*).

1.2.3 Ventajas de Voz sobre IP

Las principales ventajas de la tecnología Voz sobre IP son las siguientes:

- Voz sobre IP permite transmitir más de una llamada telefónica por el mismo canal o circuito virtual, optimizando recursos de infraestructura, ancho de banda. De esta manera es más sencillo incrementar una línea de telefónica para el hogar u oficina.

- VoIP proporciona movilidad, es decir es extremadamente flexible, en VoIP es independiente la ubicación del usuario, el usuario puede llevar su teléfono VoIP a cualquier lugar, siempre y cuando disponga de una conexión a la Internet, estará en la capacidad de recibir llamadas.

- Si se desea implementar un sistema telefónico completo, con VoIP no existe la necesidad de instalar un cableado telefónico dedicado, porque funciona por medio de la red informática existente. De la misma manera no es necesario instalar módems especiales de voz o tarjetas de telefonía.

1.2.4 ¿Por qué elegir el protocolo SIP y no otro protocolo?

Las principales razones para elegir SIP en lugar de otra tecnología son las siguientes:

1. **Oportunidades con SIP**

   El protocolo SIP es un estándar para la comunicación de persona a persona, que le permite beneficiarse del servicio de telefonía IP, mensajería instantánea, presencia, videoconferencia, intercambio de archivos instantáneamente, entre otros. Ya que es un estándar abierto que solo la imaginación es lo que limita a la gran variedad de aplicaciones que los proveedores de todo el mundo pueden dar.

2. **Estándar vs propiedad tecnológica de cada protocolo**

Existen muchos protocolos para la tecnología VoIP y telefonía IP. Algunas marcas utilizan la propiedad tecnológica, la cual prohíbe a los usuarios mezclar y combinar productos de diferentes fabricantes. SIP es un estándar mundial abierto. La elección de productos basados en el estándar SIP asegura que se pueden mezclar productos de diferentes fabricantes y que va a ser parte del mundo VoIP en el futuro.

3. **SIP vs H.323, MGCP, y otros protocolos**

SIP es un protocolo nuevo, y más simple que el protocolo H.323, y mucho más adecuado para VoIP y otras aplicaciones de internet. Por lo tanto se observará una gran cantidad de aplicaciones basadas en SIP que en H.323. MGCP es un protocolo basado en ideas de un simple teléfono tradicional, donde el operador tiene el control total. SIP permite a los usuarios finales tener un control total.

4. **SIP es el futuro**

Más y más empresas y organizaciones alrededor del mundo eligen equipos compatibles con SIP, *Gartner Group* estimó que en el año 2008, el 90% de todas las redes de telefonía corporativa serán habilitadas para IP y se basan en el protocolo SIP.

1.3 EL PROTOCOLO SIP EN EL DESARROLLO DEL PROYECTO

El presente proyecto pretende analizar la paquetización de Voz Sobre IP en una llamada internacional hacia USA, empleando el Protocolo de Inicio de Sesiones (SIP), con *Back To Back User Agent* (B2BUA), sobre una red inalámbrica Wi-Fi. Para una mejor comprensión del proyecto se ilustra en la Figura 1.11 el diagrama funcional por bloques.

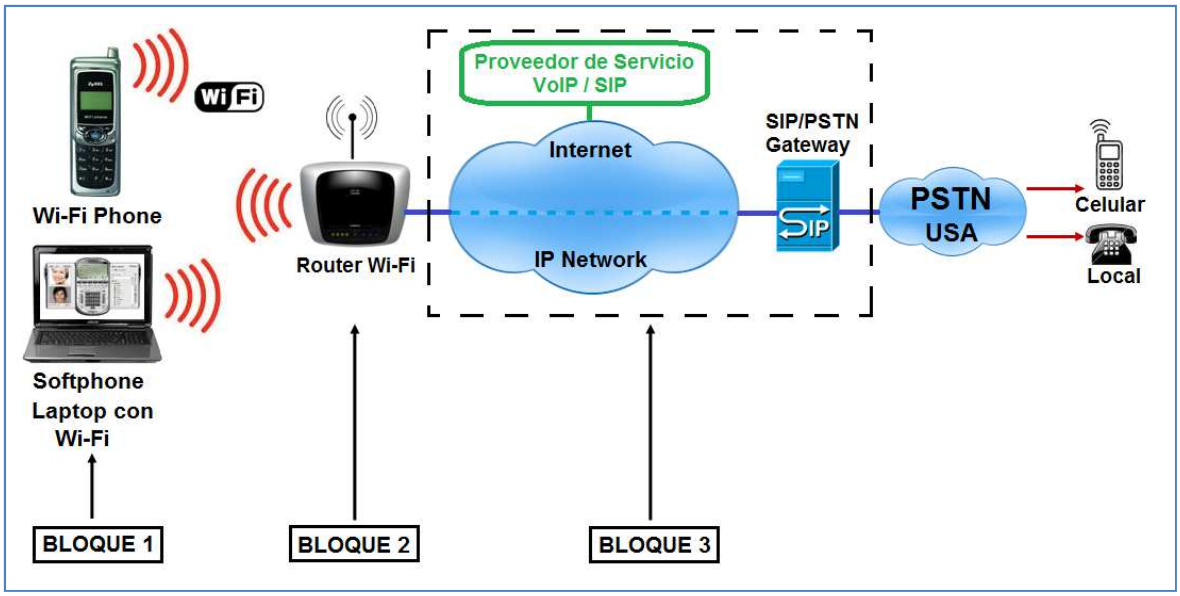

Figura. 1.11. Sistema VoIP empleando el protocolo SIP: Diagrama funcional por bloques.

- ✓ **Bloque 1.** Configuración de los dispositivos terminales SIP.

  Las aplicaciones VoIP basados en SIP se encuentran en dispositivos terminales tanto en *hardware* como en *software*, es por esto que este bloque contiene un celular Wi-Fi *Phone* (*hardware*), y una computadora laptop Wi-Fi en la cual se encuentra instalada la aplicación para realizar llamadas VoIP denominada *Softphone* (*software*). Además para la captura y análisis de los paquetes SIP la computadora contiene el analizador de protocolos *Wireshark*. Con la información proporcionada por el proveedor de servicio VoIP se configuran los parámetros requeridos por los terminales SIP.

- ✓ **Bloque 2.** Configuración del router inalámbrico.

  Este bloque contiene la configuración de la red inalámbrica.

- ✓ **Bloque 3.** Proveedor de servicio VoIP / SIP, Gateway SIP/PSTN.

  Para poder realizar llamadas desde de la Internet hacia teléfonos convencionales o fijos, es necesario suscribirse con un proveedor de servicio VoIP / SIP (*VoIP Internet Phone Service*). Estos proveedores ofrecen Voz sobre IP basados en el servicio de telefonía de banda ancha utilizando el protocolo SIP para los usuarios. A estos proveedores se los denomina ITSP (*Internet Telephony Service Providers)*. Estos proveedores ofrecen servicios de puerta de enlace o *Gateway* VoIP (*Gateway* SIP/PSTN). Además proveedores permiten realizar y recibir llamadas desde los números de teléfonos analógicos tradicionales y números celulares. La puerta de enlace o *Gateway* proporciona un número de teléfono en el área solicitada (en el presente proyecto USA), para recibir llamadas desde los números de teléfonos convencionales y celulares.

1.4 OBJETIVOS

General

- Analizar la paquetización de Voz Sobre IP empleando el Protocolo de Inicio de Sesiones SIP con *Back To Back User Agent* (B2BUA), en una aplicación sobre redes Wi-Fi.

Específicos

- Analizar el estado del arte sobre la tecnología Voz sobre IP (VoIP).
- Analizar el estado del arte de la utilización del protocolo SIP, como protocolo más utilizado en tecnología Voz Sobre IP.
- Clasificar los protocolos de Voz sobre IP.
- Evaluar el funcionamiento del teléfono WLAN660-S Wi-Fi SIP Phone, en una llamada telefónica.
- Evaluar el funcionamiento del Softphone X-Lite, en una llamada telefónica internacional (USA).
- Analizar la paquetización en una llamada de Voz sobre IP con el protocolo SIP, utilizando el analizador de protocolos *Wireshark.*
- Determinar alcances y limitaciones de la aplicación implementada.

1.5 ORGANIZACIÓN DEL DOCUMENTO

Para el desarrollo del proyecto se lo presentará dentro de seis capítulos, distribuidos de la siguiente forma:

CAPÍTULO I: Introducción. Constituye los antecedentes del proyecto, objetivos y situación actual, detallando la importancia y aplicación funcional al que se debe llegar al concluir el presente proyecto.

CAPÍTULO II: Fundamento Teórico. Está compuesto por todo el fundamento teórico, conceptos y parámetros relacionados, necesarios en la realización del presente proyecto, en el cual se explica los aspectos generales sobre las redes las redes de computadoras que utilizan el protocolo IP. Seguido de esto, se describe todo lo relacionado en Voz sobre IP (VoIP), realizando un análisis detallado y clasificación de los protocolos más utilizados en VoIP, analizando sus características y ventajas, mediante estos argumentos, permitió en el capítulo posterior seleccionar al protocolo SIP para la realización del presente proyecto.

CAPÍTULO III: Protocolo de Inicio de Sesiones (SIP). Contiene todo el fundamento teórico explícitamente detallando el protocolo SIP, siendo SIP uno de los protocolos de señalización más utilizados en tecnología Voz Sobre IP.

CAPÍTULO IV: Materiales y Métodos. Se especifica en detalle los materiales utilizados en la aplicación del presente proyecto, y los procedimientos para implementar dicha aplicación, como la suscripción del proveedor de servicio VoIP (*VoIP Internet Phone Service*), como también las configuraciones del router inalámbrica y del los equipos terminales SIP.

CAPÍTULO V: Obtención y Análisis de Resultados. Contiene la obtención y el análisis de los resultados de la aplicación.

CAPÍTULO VI: Conclusiones y Recomendaciones. Se presenta las conclusiones y recomendaciones que se obtuvo durante el desarrollo del proyecto.

CAPÍTULO II

FUNDAMENTO TEÓRICO

2.1 GENERALIDADES DE VOZ SOBRE IP (VoIP)

2.1.1 ¿Qué es la VoIP?

La sigla VoIP proviene de las palabra en Inglés: *Voice Over Internet Protocol*, que significa “voz sobre un protocolo de internet o voz sobre IP”, por medio de VoIP permite unir la transmisión de voz con la transmisión de datos, que antiguamente eran dos mundos completamente separados, es por esto que se considera a la VoIP como una tecnología y no como un servicio.

La Voz sobre IP, permite la transmisión de la señal de voz, para conseguir esto la señal es comprimida y digitalizada de manera muy eficiente, estableciendo un modelo o sistema que permita “empaquetar” la señal de la voz, en las cuales la información a transmitir se divide en unidades de información (paquetes), para que puedan viajar a través de redes de datos, a diferencia de la Red Telefónica Publica Conmutada RTPC o PSTN *Public Switched Telephone Network*, que se fundamenta en la conmutación de circuitos, en la cual se establece un circuito o canal dedicado durante el tiempo que demore la comunicación, como se estudio anteriormente, esto significa que los recursos que intervienen en la comunicación no pueden reutilizados en otra comunicación hasta que finalice la primera.

Para que estos paquetes puedan ser transmitidos en una red de datos y teniendo en cuenta que la red de Internet es la "red de redes", nos dirige claramente que utiliza al protocolo IP (*Internet Protocol*), en la cual se aprovecha el ancho de banda y la infraestructura de redes alámbricas e inalámbricas existentes, consiguiendo un ahorro importante en costos, tanto para empresas de telecomunicaciones como a personas particulares.

No obstante, ésta tecnología de la VoIP tiene una desventaja, es que en el protocolo IP no ofrece QoS (Calidad de Servicio), cuando se transmite voz sobre una red IP como la red de Internet, existen varios factores que afectan la calidad de la comunicación, como bajas velocidades de conexión a Internet, aumento de tráfico del Internet, por lo tanto se pueden tener retardos en las transmisiones de paquetes, esta desventaja está siendo superada mediante la evolución de la tecnología y al aumento de las tasas de transmisión que están siendo ofrecidas actualmente, en otras palabras, la constante expansión de las conexiones de banda ancha, han conseguido que la calidad de servicio de esta tecnología, llegue a un excelente nivel, lo cual podría llegar a convertirse en una gran competencia para las empresas de telefonía tradicional.

Está claro que VoIP es una tecnología, que convierte la señal analógica de la voz en paquetes de datos, y no es un servicio propiamente dicho, con esta tecnología pueden proporcionarse servicios de Telefonía, videoconferencia, entre otros. La prestación de un servicio de telefonía en donde la señal de la voz es empaquetada y viaja a través de una red de datos utilizando el protocolo IP, es conocida como Telefonía sobre IP o ToIP, además la telefonía IP se refiere a servicios de comunicaciones como aplicaciones de la voz, fax, diferente al concepto de la VoIP. *El Servicio de la Telefonía IP es una aplicación indudable de la tecnología VoIP*. La telefonía IP dispone de equipos que convierten la señal de voz analógica del teléfono en digital, posteriormente comprimen la información y la introducen en paquetes IP, los cuales son transmitidos sobre una red IP (Intranet o Internet), estos equipos se encuentran en: tarjetas especificas para ordenador, servidores, software específicos, entre otros, los cuales también pueden realizar el proceso inverso al momento que el paquete llega a su destino.

Inicialmente se utilizó el protocolo IP para el envío exclusivamente de datos, pero gracias al desarrollo tecnológico es factible convertir la señal de la voz analógica en digital y comprimirla en paquetes de datos, los cuales pueden ser transmitidos por medio de las diferentes tecnologías existentes como ATM, Frame Relay, Satélites, entre otras.

2.1.2 Principio de funcionamiento de la VoIP

La Voz sobre IP no está basada en la conmutación de circuitos, en la cual establece un circuito físico o canal dedicado como en la red telefónica convencional, a diferencia que la VoIP está basada en la *conmutación por paquetes,* en la cual se establece un circuito virtual, por el cual se envían múltiples comunicaciones por medio del mismo canal o circuito virtual, esto implica un uso más eficiente de la red, optimizando recursos de infraestructura, ancho de banda, se logra prestar más servicios de telecomunicaciones.

En la *Conmutación de paquetes*, la información a transmitir se divide en unidades de información llamados paquetes, en los cuales se aumenta información relevante (la dirección a la que se dirige y la dirección del origen del paquete, dicho de otra manera dirección origen y dirección destino).

Estos paquetes viajan por flujos independientes, no existe una ruta predeterminada, es decir los paquetes pueden viajar por el mejor camino entre dos puntos, donde siempre tienen más de un camino o ruta disponible, con mayores opciones por donde llegar a su destino, esto es una *característica intrínseca de las redes IP*, cuando los paquetes ya han llegado a su destino son re ensamblados para reconstruir la información original, por lo tanto se puede mencionar que la conmutación por paquetes es más inteligente en aprovechar los recursos de la red.

Existen dos procesos básicos para el funcionamiento de la VoIP (Figura 2.1), estos son:

- Conversión de la señal analógica en formato digital.
- Compresión de la señal digital y divida en paquetes.

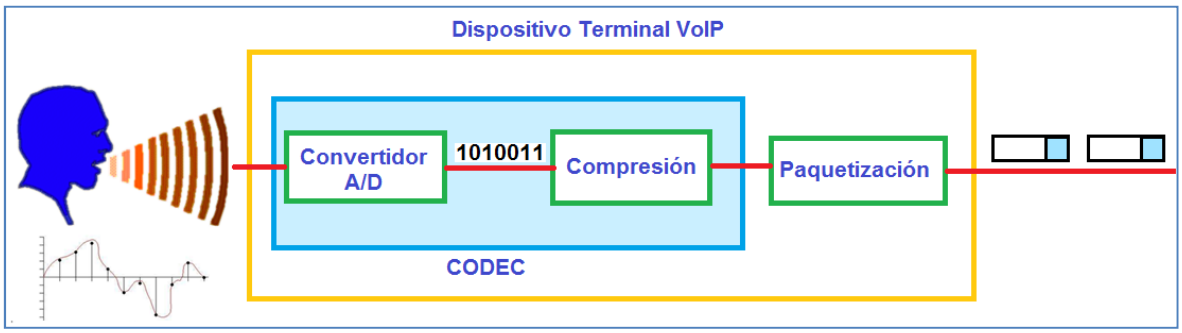

Figura. 2.1. Procesos básicos de la VoIP, conversión y compresión.

En la Voz sobre IP se convierte la señal de voz analógica del teléfono en digital es decir la digitalizamos de manera muy eficiente, mediante un convertidor análogo/digital (ADC *analog to digital converter*), la información a transmitir se divide en unidades de información (paquetes) a través de la red IP, al momento que el paquete llega a su destino se realiza el proceso inverso, es decir la reconversión mediante un convertidor digital/análogo (DAC *digital to analog converter*), como se aprecia en la Figura 2.2.

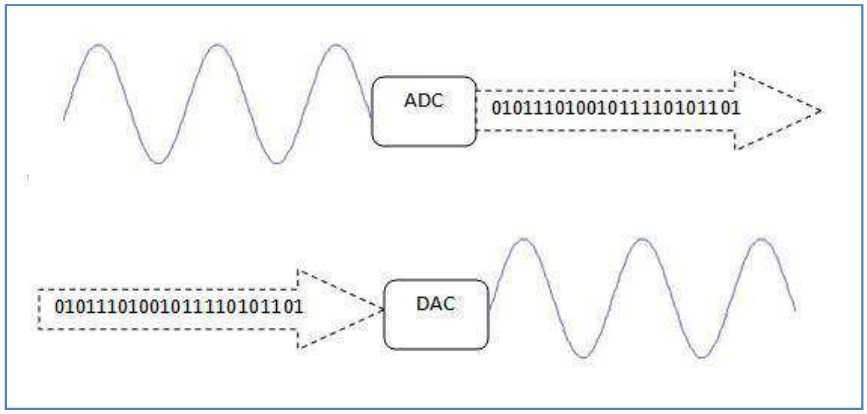

Figura. 2.2. Conversión mediante ADC y reconversión mediante DAC.

El funcionamiento comienza con la digitalización de la señal de la voz análoga del teléfono, por ejemplo aplicando PCM (*Pulse Code Modulation*) con un *codec* codificador-decodificador obteniendo muestras PCM, estas muestras pasan el algoritmo de compresión, en donde la información es comprimida y además para poder transmitir se divide en unidades de información, es decir en paquetes, que viajan a través de redes IP, posteriormente a la nube red IP se realizan el mismo proceso en sentido inverso, como se aprecia en la Figura 2.3.

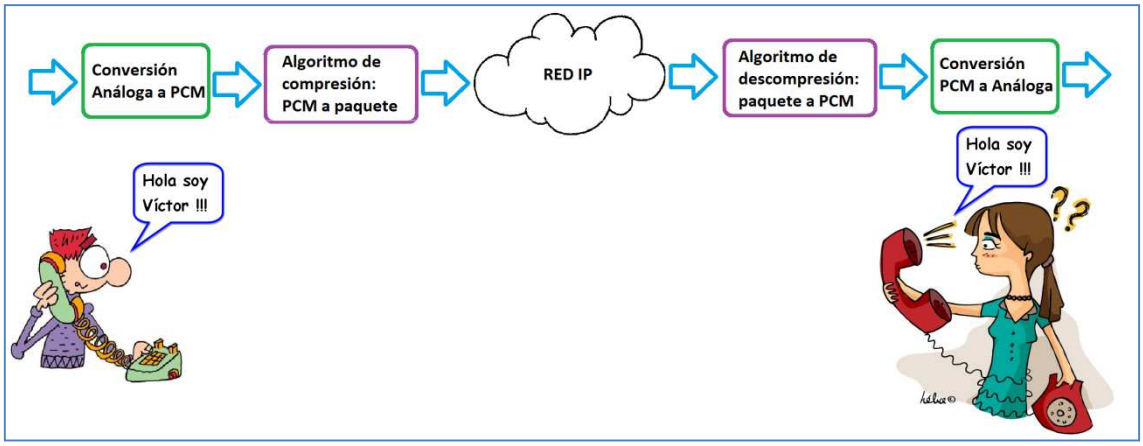

Figura. 2.3. Funcionamiento Voz sobre IP.

2.1.3 Elementos fundamentales en una arquitectura VoIP

Los Principales elementos en una arquitectura VoIP son los siguientes:

2.1.3.1 Gateway

El Gateway es un elemento fundamental en las redes VoIP, su objetivo fundamental es acoplar la red de datos IP con la Red Telefónica Publica Conmutada RTPC (PSTN *Public Switched Telephone Network*) y también con redes de telefonía tradicional.

2.1.3.2 Servidor / Gatekeeper / Servidor SIP / Agente de llamadas

El Gatekeeper es un elemento optativo en la red, pero cuando disponemos de este elemento, los demás elementos tienen que utilizar sus funciones administrativas, de gestionar y controlar los recursos de la red, soporta enrutamiento de llamadas.

Dependiendo del sistema en el cual se encuentre basado este elemento obtiene su nombre, es decir en un sistema en el cual se encuentre basado en H.323 el servidor se lo conoce como Gatekeeper, en un sistema SIP: servidor SIP, en un sistema MGCP o MEGACO: Agente de llamadas (*Call Agent*), estos sistemas se estudiarán más adelante.

Es bastante frecuente encontrar que el Gatekeeper y Gateway se encuentren trabajando juntos; Este equipo tiene interfaces LAN y además puede tener uno o todas las siguientes interfaces:

"FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
E&M. Para conexión específica a centralitas.
BRI. Acceso básico RDSI (2B+D)
PRI. Acceso primario RDSI (30B+D)
G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps". [3]

2.1.3.3 Terminales VoIP

Un teléfono IP es un equipo terminal que naturalmente soporta VoIP, en cual podría conectarse directamente a una red de dados IP.

Entendiendo que una red de datos IP puedes ser: una red IP privada, la red de Internet, o una red Intranet, definitivamente, la red de datos IP proporciona conectividad

entre todos los terminales, en la Figura 2.4 se aprecian los principales elementos en una arquitectura VoIP.

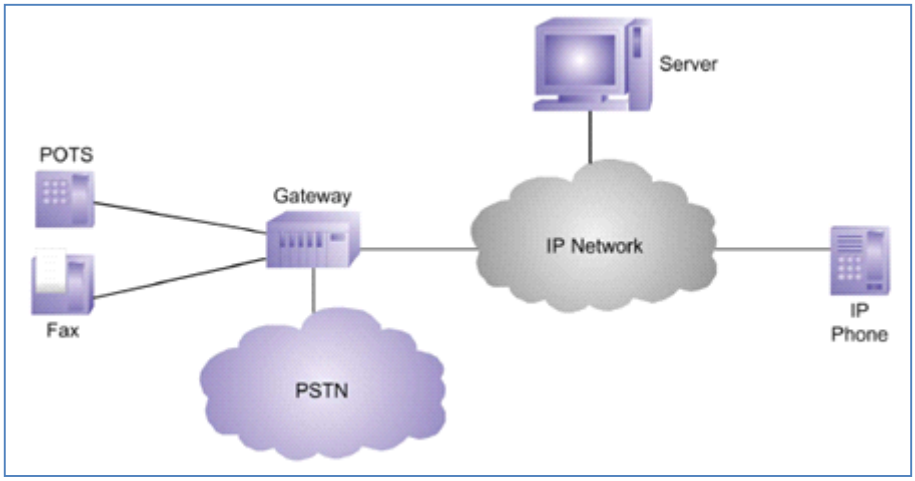

Figura. 2.4. Elementos fundamentales de una red VoIP.

- **Agente de Usuario**

Los terminales de telefonía IP poseen indudablemente cierta inteligencia, que es suministrada por un Agente de Usuario (UA), se fundamenta en un programa informático el cual siempre se encuentra en estado activo, expresado en otras palabras los Agentes de Usuario (UA) son las entidades que se encuentran al final de la red, y son los que "conversan" con otras entidades. Los Agentes de Usuario son los que inician y finalizan las sesiones o comunicaciones, empleando mensajes para solicitar algún servicio, además están en la capacidad de responder solicitudes y también solicitan respuestas.

2.2 DESCRIPCIÓN GENERAL DE REDES DE COMPUTADORES Y PROTOCOLO IP

El funcionamiento de la telefonía IP se fundamenta sobre redes de computadoras o redes de datos IP o dispositivos similares, de la misma manera en la red de Internet, teniendo en cuenta que la red de Internet es la "red de redes", nos dirige claramente que utilizan al protocolo IP (*Internet Protocol*), en el presente tema del capítulo se definirán los aspectos generales sobre las redes las redes de computadoras que utilizan el protocolo IP

2.2.1 Modelo OSI

La organización internacional para la estandarización ISO, que es el acrónimo de International *Organization for Standardization*, en el año de 1984 aceptó la necesidad de crear un modelo para las redes de computadoras, para facilitar a los distintos fabricantes en la creación de diversas implementaciones que sean interoperables[6] y abiertas. De este modo nace el modelo de referencia OSI que es el acrónimo de *Open Systems Interconnection*, creada por la ISO, en la cual presenta una arquitectura de red que está formada por 7 niveles o capas como se presenta en la Figura 2.5.

Figura. 2.5. Capas del modelo de referencia OSI.

6 La interoperabilidad es la capacidad que tiene un producto o un sistema, cuyas interfaces son totalmente conocidas, para funcionar con otros productos o sistemas existentes o futuros y eso sin restricción de acceso o de implementación.

Por lo tanto cada capa debe tener funciones específicas además de seguir estándares internacionales, cada capa posee una interfaz la cual esta interconectada con la capa superior. Se entiende por interfaz al conjunto de procedimientos que definen al servicio que la capa está en condiciones de realizar para entregar a quien lo necesite.

Cuando un computador A (origen) desea enviar información a otro computador B (destino), empezando en el origen, conforme los datos se desplazan atravesando las diferentes capas del modelo OSI, cada capa va agregando información de control a los datos, es decir los datos se empaquetan por medio de un proceso que se denomina encapsulamiento; En el destino cada capa analiza y va eliminando la información de control de los datos, como se presenta en la Figura 2.6.

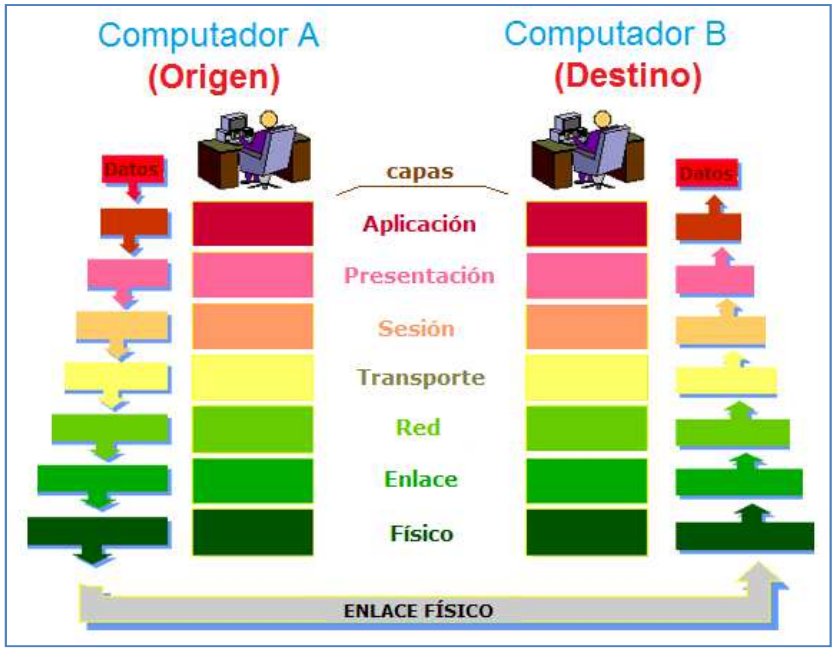

Figura. 2.6. Encapsulamiento atravesando las capas del modelo OSI.

Al momento de enviar un paquete de datos desde el origen hacia su destino, el paquete atraviesa de una capa a otra, existen protocolos que trabajan en cada capa (un protocolo, es un conjunto de normas o reglas que rigen en el proceso de comunicación entre computadoras, de la misma forma es un lenguaje común para evitar problemas de incompatibilidad), estos protocolos le van agregando información a al paquete, esta información será procesada por los respectivos protocolos de la misma capa en el equipo destino como se presenta en la Figura 2.7.

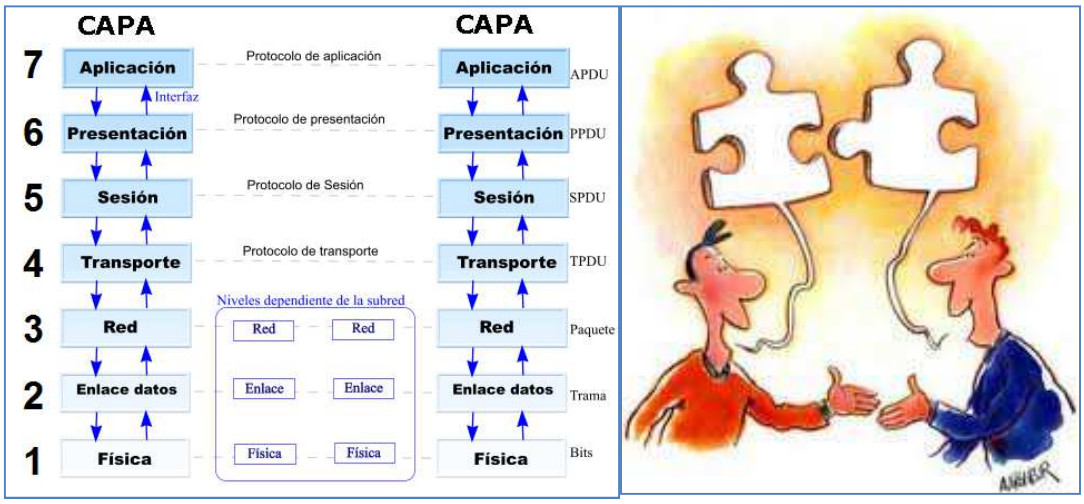

Figura. 2.7. Protocolos que trabajan en cada capa en el modelo OSI.

A la información que se agrega a los paquetes de datos se la denomina "*header*" o cabecera, mediante el proceso de encapsulamiento, es decir se va re empaquetando, en cada capa se agrega su propia cabecera, exceptuado en la capa física, cada capa del computador origen se comunica con su respectiva capa del computador destino, dicho de otra manera se comunica con su capa par o igual, a esto se le denomina comunicación *Peer to Peer* o comunicación Par a Par, durante esta comunicación, entre las capas pares los protocolos intercambian información en unidades de datos que les denomina PDU (*Protocol Data Unit*), como se presenta en la Figura 2.8.

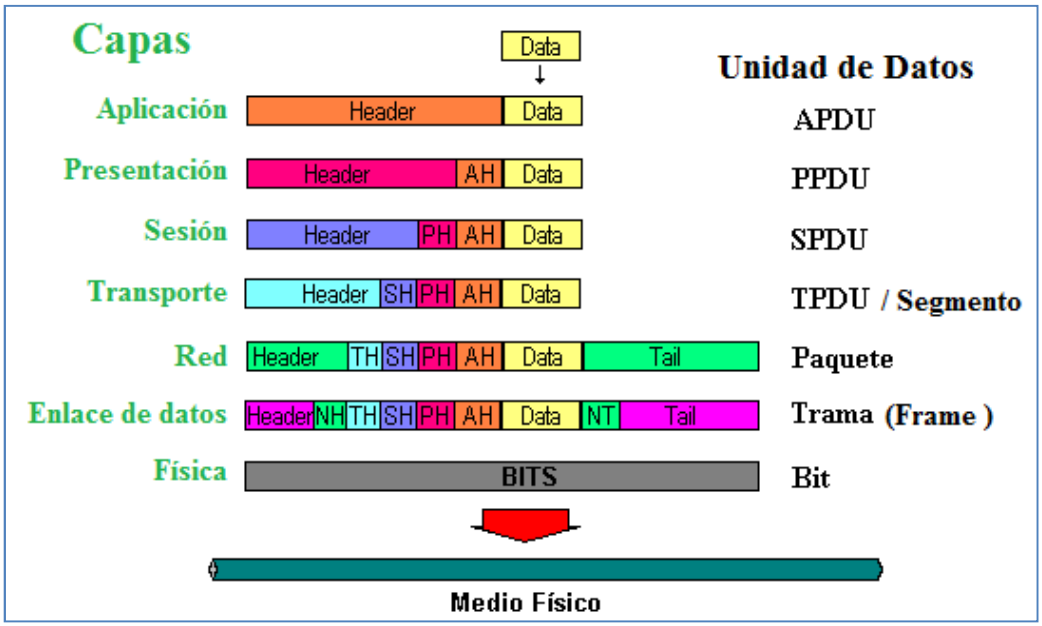

Figura. 2.8. Aumento de header en los datos / unidad de datos

2.2.1.1 Capa Física

Esta capa es la encargada de las conexiones físicas del ordenador hacia la red de datos, entre sus principales funciones se tiene la de definir el medio o los medios físicos por donde la comunicación va a viajar, también define las características de materiales, eléctricas, mecánicas, que van a ser utilizadas en la transmisión de los datos, de igual forma define las características funcionales de la interfaz, además esta capa se encarga de la transmisión del flujo de bits a través del medio físico o de los circuitos de comunicaciones. A continuación se presentan en la Figura 2.9 ejemplos de equipos que trabajan en esta capa como repetidores, hubs.

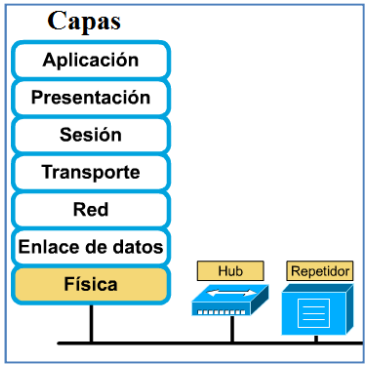

Figura. 2.9. Dispositivos que trabajan en la capa física.

2.2.1.2 Capa de enlace de datos

Esta capa es la encargada del direccionamiento físico o plano, que corresponde a las direcciones MAC que en Inglés es acrónimo de *Media Access Control* o control de acceso al medio, la dirección MAC es un identificador a un dispositivo de red, esta dirección se encuentra grabada en las tarjetas de red o también llamada NIC (por *network interface card* o tarjeta de interfaz de red), como se presenta en la Figura 2.10 ejemplos de dispositivos de red, cada dispositivo tiene su propia dirección MAC determinada, que esta forma por 48 bits codificados en bloques hexadecimales, los primeros 24 bits son utilizados por el OUI (siglas en Inglés de *Organizationally Unique Identifier* o Identificador Único Organizacional) que es la identificación única del fabricante, y los últimos 24 bits determinada y configurada por el IEEE (siglas en Inglés de *Institute of Electrical and Electronics Engineers* o Instituto de Ingenieros Eléctricos y Electrónicos).

Asimismo se ocupa de la topología de la red, acceso al medio, igualmente se encarga de la detección de errores, de una ordenada transmisión de las tramas y controlar el flujo. En esta capa se agrupan los bits de la capa física y dividiéndolos en tramas de datos, identificando un principio y fin de la trama, también transmite las tramas en forma secuencial y procesa las tramas para la capa superior.

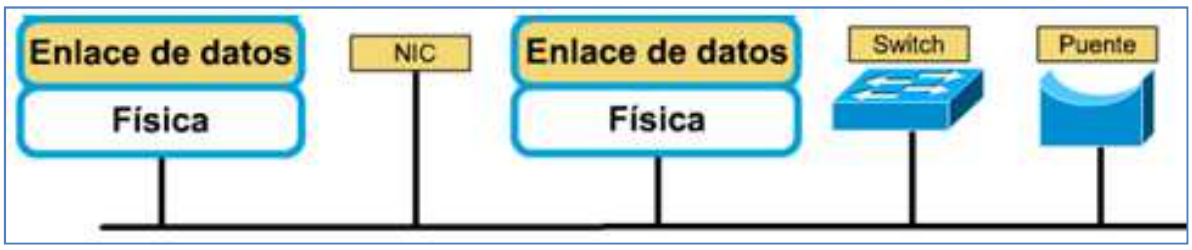

Figura. 2.10. Dispositivos que trabajan en la capa enlace de datos, switch, puente o bridge.

2.2.1.3 Capa de red

En la capa de red el objetivo principal es lograr que los datos lleguen a su destino desde su origen, existen dispositivos que se encargan de realizar estos trabajos denominados en caminadores, enrutadores o en Inglés llamados *routers*, como se presenta en la Figura 2.11, también se los denomina dispositivos de capa 3, esta capa es la encargada del direccionamiento lógico y del enrutamiento, dicho de otra manera, determina la ruta de los paquetes hasta llegar a su destino final.

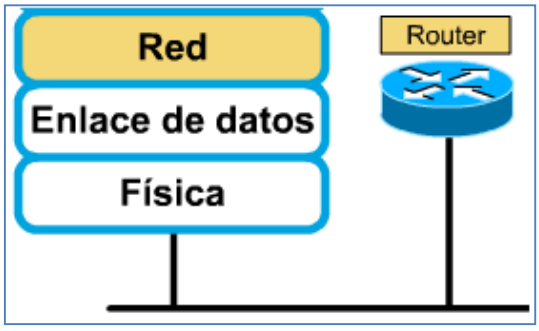

Figura. 2.11. Equipo Router o dispositivo de capa 3.

2.2.1.4 Capa de Transporte

Esta capa es la encargada de la transmisión de los segmentos, los segmentos son la PDU de esta capa, además en esta capa establece, mantiene y termina las conexiones lógicas entre los host[7], esta capa es la responsable de la entrega confiable de datos, también ofrece control de flujo. Los protocolos en esta capa son TCP y UDP; "Transmission Control Protocol" y "User Datagram Protocol" respectivamente.

TCP es un circuito orientado a la conexión, es decir, antes de la trasmisión de datos, se establece un circuito virtual lógico, es un protocolo estándar, de estatus recomendado, sus especificaciones se encuentran en la RFC 793. TCP es un protocolo seguro, además ofrece corrección de errores, también reordena los paquetes cuando están desordenados, simultáneamente envía una confirmación de recepción de paquetes.

UDP es no orientado a la conexión es decir solo despacha información, es un protocolo estándar, de estatus recomendado, sus especificaciones se encuentran en la RFC 768. UDP es un protocolo rápido, la información llega en el menor tiempo posible, por lo tanto es utilizado en aplicaciones en tiempo real, como voz, video entre otros.

Por lo tanto trabajan con puertos, un puerto es una interfaz lógica, dicho de otra manera, es un numero de 16 bits que permite identificar unívocamente (solo a el) a una determinada aplicación o proceso, como se presenta en la Figura 2.12. Un puerto es de 16 bits, si realizamos la operación x^y, donde x es 2 y y es 16 se obtiene 65536 puertos, tomando en cuenta al 0 se tienen del 0 al 65535 puertos, los cuales se clasifican en dos grupos, el primer grupo se los llama *Puertos Bien Definidos*, estos sirven para aplicaciones ya definidas o estándar, van desde puerto 0 hasta el puerto 1023, los cuales son administrados por la Agencia de Asignación de Números de Internet cuyo acrónimo es IANA (Internet Assigned Numbers Authority). El segundo grupo se los llama *Puertos Efímeros*, que son utilizados por el host local, van desde puerto 1024 hasta el puerto 65535.

[7] Literalmente host significa anfitrión, que es un ordenador que se encuentra directamente conectado a una red.

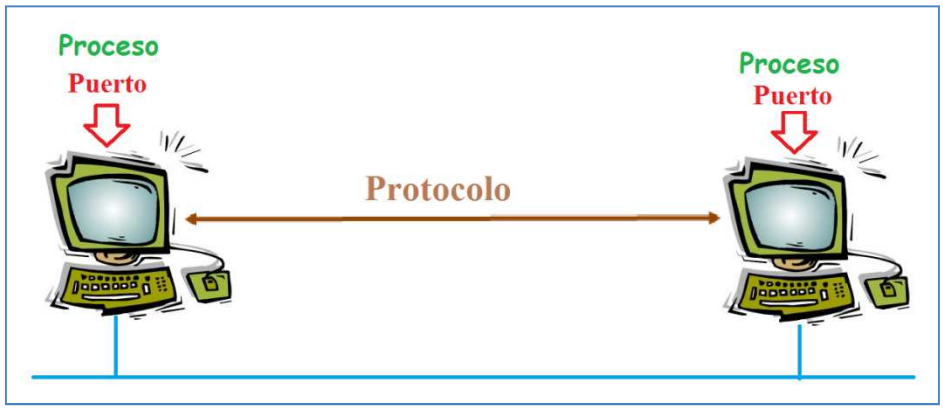

Figura. 2.12. Puerto identifica unívocamente a un determinado proceso

El intercambio de datos entre procesos es a través de los denominados *Sockets*, los procesos pueden estar en el mismo ordenador o en diferentes ordenadores que se encuentren conectados en una red de datos. Después que se establece la conexión de socket, los datos están en la capacidad de enviarse desde el origen hacia el destino y viceversa.

Un socket está conformado por: < Protocolo, Dirección Lógica local, Puerto >

Una conversación es un *link* de comunicación entre dos procesos. La identificación de una conversación se denomina *Asociación*. Una Asociación está conformada por:

< Protocolo, dirección lógica origen, puerto origen, dirección lógica destino, puerto destino>

A continuación se presenta en la Figura 2.13 un ejemplo de asociación.

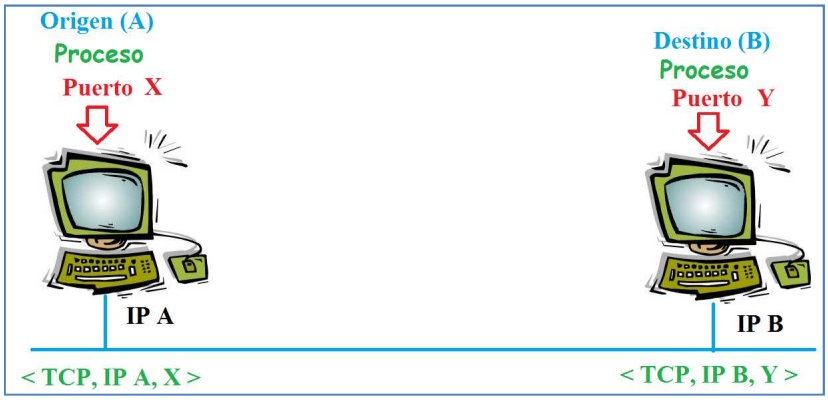

Figura. 2.13. Ejemplo de asociación.

Según el ejemplo de la Figura 2.9 la asociación es la siguiente:

< TCP, IP A , X , IP B , Y >

2.2.1.5 Capa de Sesión

En esta capa como su nombre lo indica, es la encargada de iniciar, mantener y finalizar sesiones entre aplicaciones, permitiendo que dos diferentes ordenadores establezcan conversaciones o sesiones, también en esta capa se definen mecanismos para el control del dialogo, sincroniza el dialogo entre las capas de presentación de diferentes ordenadores administrando el intercambio de datos.

2.2.1.6 Capa de Presentación

Esta capa define el formato de los datos en que se intercambia la información entre aplicaciones y también la sintaxis que usan las aplicaciones.

Además proporciona seguridad en la red utilizando encriptación y des encriptación, igualmente se encarga de la compresión (*code formatting*), garantizando que los datos enviados por la capa aplicación sean entendibles en el destino, se tiene por ejemplo los formatos de texto, imágenes, sonido, códigos ASCII entre otros, Ej.: JPEG, ASCII, GIF, TIFF, MPEG, etc.

2.2.1.7 Capa de Aplicación

Esta capa es la más cercana al usuario, porque interactiva con el usuario, proporcionando servicios de red a las aplicaciones del usuario, como por ejemplo navegadores web, correo electrónico, transferencia de archivos, entre otros, Ej.: Telnet, HTTP, FTP, Browsers, SMTP, etc.

2.2.2 Modelo TCP/IP

El modelo TCP/IP, fue definido en los años 70 por DARPA (que es acrónimo en Inglés de *Defense Advanced Research Projects Agency* o Agencia de Investigación de Proyectos Avanzados de Defensa), años más Departamento de Defensa de los Estados Unidos creó a ARPANET (*Advanced Research Projects Agency Network*), en el año de 1975, ARPANET empezó a funcionar como la primera red de área ampliada (WAN, que es el acrónimo en Inglés de *Wide Area Network*), esto sirvió como base para unificar los centros de investigaciones militares y universidades, trabajando en protocolos más avanzados y específicos para ordenadores, en 1983 se adoptó a TCP/IP como estándar principal para las comunicaciones.

En base a la historia y al análisis técnico, se puede mencionar que, el estándar abierto de Internet es TCP/IP (*Protocolo de control de transmisión/Protocolo Internet*), el modelo de referencia TCP/IP y la familia de protocolos de TCP/IP, hacen posible la comunicación entre ordenadores, es decir permite la transmisión de datos en redes de computadoras, alcanzando a ser la base de la red Internet, utilizando direcciones IP, cada equipo de red tiene una dirección IP, por lo tanto es posible direccionar los paquetes de datos desde el origen hacia su destino.

TCP/IP describe un conjunto o familia de protocolos de red, primordialmente porque hace referencia a los dos protocolos más importantes y utilizados de esta familia los cuales son: el Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP). Existen más de 100 diferentes protocolos, entre los más sonados se tiene: El utilizado para acceder a páginas web: HTTP (HyperText Transfer Protocol), para transferencia de archivos: FTP (File Transfer Protocol), para la resolución de direcciones: ARP (Address Resolution Protocol), para correo electrónico: SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol), para acceder a equipos distantes: TELNET (Telecommunication Network), entre otros.

El modelo en esta arquitectura de protocolos es más simple que el modelo OSI, en esta arquitectura se ha agrupado diversas capas para forma una sola, incorporando sus funciones, de esta manera el modelo TCP/IP está conformado por 4 capas, a continuación se presenta en la Figura 2.14 el modelo TCP/IP en analogía con el modelo OSI.

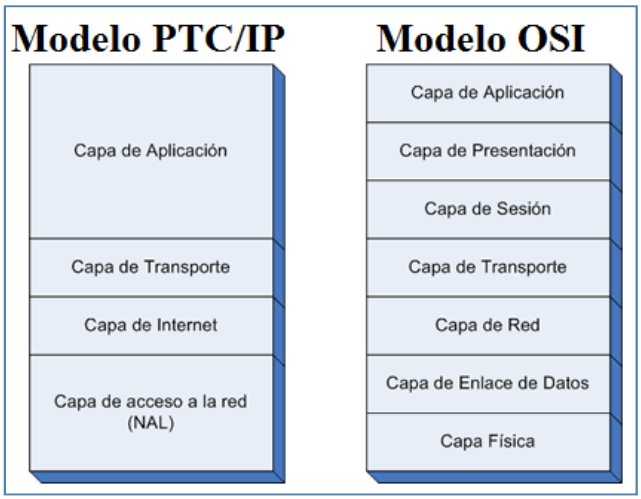

Figura. 2. 14. Modelo TCP/IP en analogía con el modelo OSI.

Semejante al modelo OSI, para el envió de datos, cada capa añade información de control a los datos, esta información se denomina *cabecera* empleando encapsulación. Para recepción se realiza el proceso inverso, por lo tanto cuando los datos ascienden atravesando cada capa, se elimina la cabecera correspondiente, como se presenta en la Figura 2.15. [5].

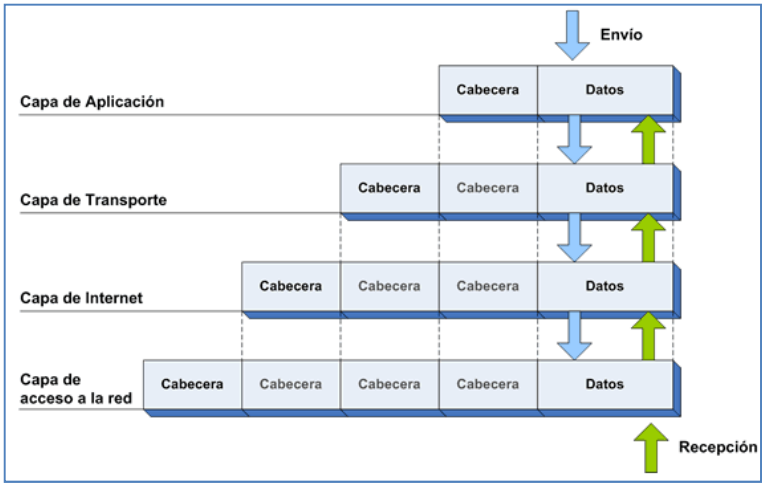

Figura. 2.15. Encapsulación en el modelo TCP/IP.

A continuación se presenta en la Tabla 2.1 los términos que cada capa interpreta con los datos, con respecto a TCP y UDP.

Tabla. 2.1. Términos que cada capa interpreta con los datos.

CAPAS	TCP	UDP
Aplicación	Flujo	Mensaje
Transporte	Segmento	Paquete
Internet	Datagrama	Datagrama
Acceso a la Red	Trama	Trama

2.2.2.1 Capa de acceso a la red o Network

Esta es la primera capa del modelo TCP/IP, esta capa está en la capacidad de acceder a cualquier red física, aceptando arquitecturas WAN[8], LAN[9]. En esta capa se especifica todo lo relacionado con la transmisión de los datos en una red física, además se especifica el mecanismo de encapsular datagramas sobre el tipo de red física especificado, por ejemplo se tiene: *Ethernet, Wi-Fi, Wimax, Token Ring, X25, Frame Relay, ATM, SDH,* entre otros.

2.2.2.2 Capa de Internet o Internetwork

Todas las capas son importantes en esta arquitectura, pero la capa de Internet o Internetwok es esencial, ya tiene como propósito principal de enviar paquetes desde el origen hacia su destino sobre una red de datos, independientemente de la ruta que el paquete viaja para llegar a su destino, generando la mejor ruta mediante la conmutación de paquetes.

8 WAN (Wide Area Network o Red de Área Extensa).

9 LAN (Local Area Network o Red de Área Local).

El protocolo fundamental de esta capa es el IP, el protocolo IP define el formato del paquete llamado *datagrama*, un datagrama es la unidad básica de transmisión sobre la red Internet. Esta capa es la encargada de administrar el direccionamiento lógico o direcciones IP. También ofrece un servicio de datagramas, permitiendo el enrutamiento de datagramas, además realiza la fragmentación y re ensamblaje de datagramas. Entre sus principales protocolos en esta capa se tiene: IP, ARP[10], RARP[11], ICMP[12], IGMP[13].

2.2.2.3 Capa de Transporte

En esta capa se fundamenta en los aspectos de calidad del servicio, ofreciendo comunicación *end to end* con confiabilidad entre origen y destino, control de flujo, control de errores, secuenciamiento de paquetes. En esta capa existen dos protocolos TCP y UDP.

El protocolo TCP es un protocolo estándar de estatus recomendado, es un servicio orientado a la conexión, es confiable mediante el establecimiento de un circuito lógico, para la transmisión de datos entre procesos. Cuando los datos son transmitidos, en el origen espera recibir una confirmación por parte del destino, y cuando no recibe una confirmación genera una retransmisión de los datos. TCP realiza la transmisión de la información vía *streams*, es decir por grupos de bytes y el origen espera recibir la confirmación de ese grupo de bytes. Otra característica de TCP es que coloca números de secuencia en cada segmento de datos que es transmitido, el número de secuencia corresponde al primer octeto de los datos, dicho de otra manera es el primer byte de datos. También. Además se encarga del control de flujo controlando la congestión en la red. TCP ofrece multiplexación ya que está en capacidad de levanta varias conexiones porque TCP dispone de varios puertos. Cada vez que se levanta una conexión, se establece un canal de comunicación bidireccional, en el cual ambos procesos pueden enviar y recibir información al mismo tiempo, dicho de otra manera la conexión es *full-dúplex*.

10 ARP (Address Resolution Protocol, Protocolo de resolución de direcciones).

11 RARP (Reverse Address Resolution Protocol, Protocolo de resolución de direcciones inverso).

12 ICMP (Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet).

13 IGMP (Internet Group Management Protocol).

El protocolo UDP es un protocolo estándar de estatus recomendado, es un servicio no orientado a la conexión, es decir, no se establece una conexión previa con el destino para transmitir un mensaje UDP, los mensajes pueden llegar desordenados al destino. Además UDP no ofrece control de errores, ni confiabilidad en el despacho de datos, estos mensajes se pueden perder o llegar dañados. UDP trabaja con datagramas, realiza un servicio de mejor esfuerzo (best effort), UDP opera como interfaz entre la capa Aplicación y la capa *Internetwork*, trabajando como MUX y DEMUX de datagramas como se presenta en la Figura 2.16.

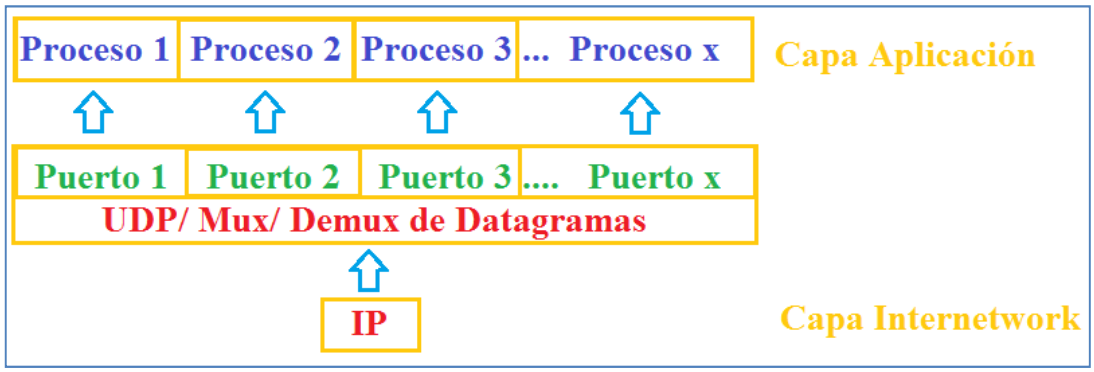

Figura. 2.16. UDP opera entre la capa Aplicación y la capa Internetwork.

Para transportar un mensaje de un computador a otro, UDP utiliza el protocolo de Internet IP porque este ofrece un servicio de entrega, como se presenta en la Figura 2.17. [6].

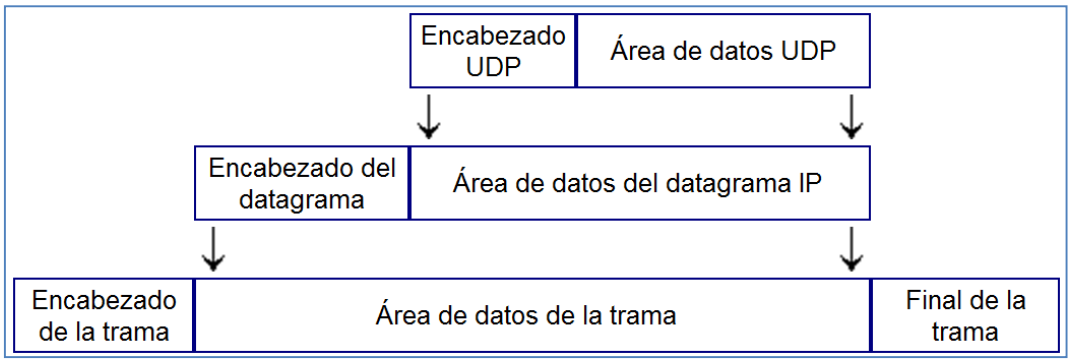

Figura. 2.17. UDP utiliza al protocolo IP.

Para poder distinguir entre los muchos programas que se están ejecutando en un mismo ordenador, UDP proporciona puertos de protocolo, conjuntamente con los datos, cada mensaje UDP contiene el número del puerto de origen y el número del puerto de destino, como se presenta en la Figura 2.18, por lo tanto como UDP opera como MUX y DEMUX de datagramas, hace que un determinado puerto trabaje con un proceso especifico.

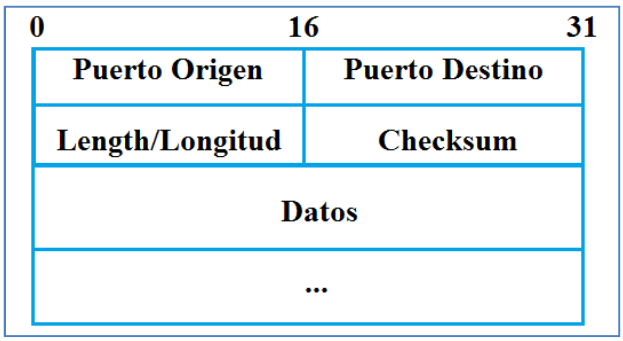

Figura. 2.18. Formato del mensaje UDP.

- **Puerto UDP de origen:** (16 bits), número de puerto del equipo origen.
- **Puerto UDP de destino:** (16 bits), número de puerto del equipo destino.
- **Length/Longitud del mensaje UDP:** (16 bits), detalla la longitud medida en bytes del mensaje UDP.
- **Checksum:** (16 bits). Se lo conoce por *Frame Check Sequence*, es cuando una trama es recibida y tienen una secuencia de verificación incorrecta, por lo tanto verifica la integridad física de los datos a procesar.
- **Datos**. Son los datos que se envían las aplicaciones.

Los procesos de la capa Aplicación utilizan estos puertos para poder recibir y transmitir mensajes. Cuando una aplicación cliente desea comunicarse con un servidor, la aplicación busca un puerto libre para utilizarlo, este número de puerto es asignado dinámicamente, es decir estos puertos son utilizados por el host local, van desde puerto 1024. A diferencia que para aplicaciones ya definidas o estándar de servidores, utilizan los números de puertos registrados, estos puertos se definen en la RFC 1700, a continuación se presenta en la Tabla 2.2 los números de puertos más comunes utilizados por TCP y UDP.

Tabla. 2.2. Puertos más comunes por TCP y UDP.

Nombre	Puerto / Protocolo	Descripción
Puertos Bien Conocidos		
echo	7/tcp/udp	Echo
ftp-data	20/tcp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
telnet	23/tcp	Telnet
smtp	25/tcp	Simple Mail Transfer
time	37/tcp/udp	Time
nameserver	42/tcp/udp	Host Name Server
nicname	43/tcp/udp	Who Is
domain	53/tcp/udp	Domain Name Server
tftp	69/udp	Trivial File Transfer
www-http	80/tcp	World Wide Web HTTP
pop3	110/tcp	Post Office Protocol - Version 3
nntp	119/tcp	Network News Transfer Protocol
netbios-ssn	139/tcp/udp	NETBIOS Session Service
irc	194/tcp	Internet Relay Chat Protocol
rip	520/udp	Routing Information Protocol
Puertos Registrados		
msn	1863/tcp	Messenger
http-alt	8008/tcp	Transferencia de hipertexto (HTTP) alterno
http/webcache	8080/tcp	Servicio de caché del World Wide Web (WWW)
radius	1812/udp	Contabilidad y autenticación de marcado Radius
SIP	5060/udp	Session Initiation Protocol

2.2.2.4 Capa de Aplicación

La capa aplicación es la que ofrece servicios específicos al usuario, es decir es la interfaz con el usuario, entre los protocolos más conocidos se tiene por ejemplo: a *Telnet* que permite la conexión remota de terminales, *FTP* para transferencias interactivas de ficheros, SMTP para enviar correos por medio de la red de datos, DNS, HTTP, NFS, RIP, entre otros.

2.2.3 Protocolo de Internet (IP)

El Protocolo de Internet (IP), este protocolo es fundamental en la capa de Internet o *Internetwok* del modelo TCP/IP, es un protocolo estándar, de estatus requerido, es decir siempre debe estar presente, sus especificaciones se encuentran en la RFC 791, este protocolo permite el envío de paquetes o datagramas de información desde un origen a un destino a través de redes interconectadas. También IP es no orientado a la conexión, realiza un servicio de datagramas no fiable denominado *mejor esfuerzo (best effort)*, dicho de otra manera no garantiza que el paquete llegue a su destino, puesto que no tiene mecanismos de control, ni secuenciamiento de paquetes, es decir los paquetes pueden llegar a su destino desordenados, por lo tanto no es confiable. Para aspectos de calidad del servicio, confiabilidad, es proporcionado por los protocolos de la capa de aplicación, como por ejemplo TCP.

El protocolo IP define el formato del paquete llamado *datagrama IP*, el datagrama IP es la unidad básica de transferencia sobre la red de datos como por ejemplo la red de Internet. El Datagrama IP básicamente tiene dos áreas, cabecera y datos, este datagrama se encapsula en el Área de datos dentro de la Trama, como se presenta en la Figura 2.19.

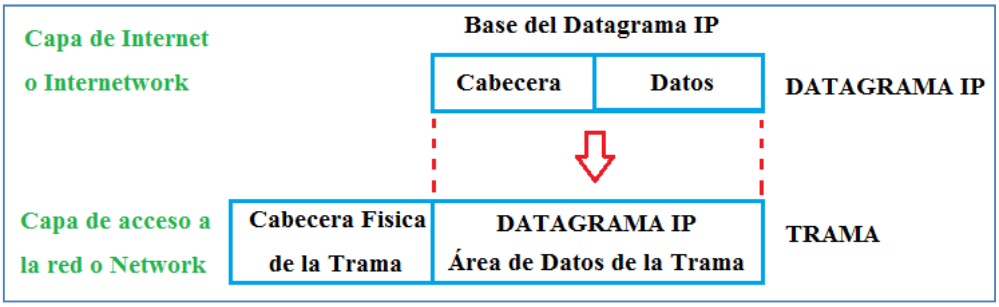

Figura. 2.19. El Datagrama IP se encapsula dentro de la Trama.

La trama tiene una longitud máxima, dependiendo del tipo de red o hardware que se esté utilizando, por ejemplo la mayoría de las redes de área local Ethernet utilizan un MTU de 1500 bytes. El tamaño máximo de una trama se denomina MTU (Unidad de transmisión máxima). IP establece que todas las redes deberán ser capaces de manejar datagramas de al menos 576 bytes.

Cuando el datagrama es más grande que la MTU de la red, se fragmenta, el protocolo IP ofrece un mecanismo de fragmentación de datagramas, esto se lleva a cabo a nivel de dispositivos de capa 3 o *routers* (del modelo OSI), esto sucede durante la transmisión de una red con MTU grande a una red con MTU más pequeña, el *router* divide al datagrama en fragmentos más pequeños que la MTU de la red. Estos fragmentos son encapsulados en tramas, agregando una cabecera a cada fragmento, estas tramas pueden ser enviadas a su destino por distintas rutas, además IP ofrece reensamblado de datagramas, agregando información, para que el equipo receptor este en la capacidad de reensamblar los fragmentos en orden correcto, por lo tanto el formato del datagrama IP dispone varios campos que permiten que la fragmentación y el reensamblado sean posibles, el formato del datagrama IP se presenta en la Figura 2.20 [7].

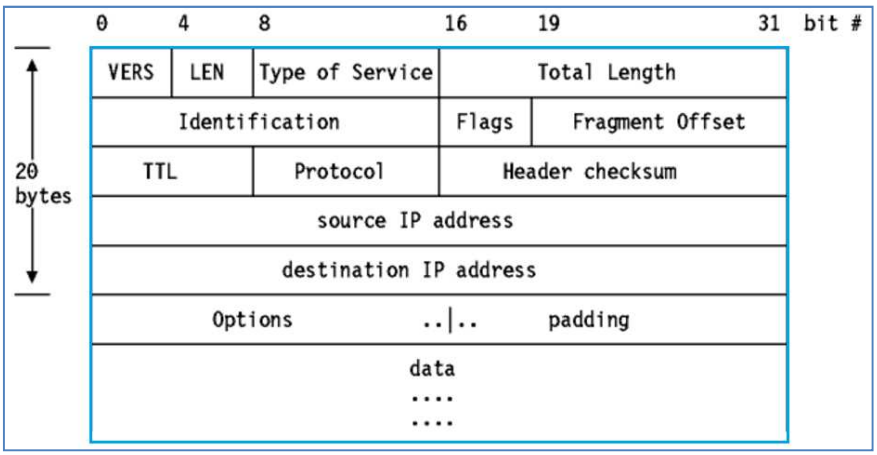

Figura. 2.20. Formato del datagrama IP.

A continuación se describe cada campo del datagrama IP:

- **VERS:** Contiene información de la versión del protocolo IP.
- **LEN:** Indica la longitud de la cabecera del datagrama IP, contada en cantidades de 32 bits.
- **Type of Service (ToS):** Indica la calidad del servicio requerido por el datagrama IP, este campo se detalla en la Figura 2.21.

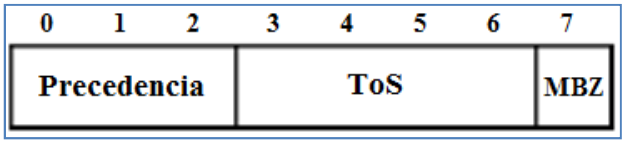

Figura 2.21. Campo Type of Service.

Donde la Precedencia indica la medida de naturaleza y prioridad del datagrama, MBZ es un bit reservado para uso futuro.

- **Total Length:** Es un campo de 16 bits que indica la longitud total del datagrama incluido cabecera y datos.
- **Identification:** Es un número único asignado por el origen, utilizado para el reensamblaje de un datagrama fragmentado, los fragmentos este datagrama tienen el mismo número de identificación.
- **Flags:** Banderas de control es de 3 bits, este campo se detalla en la Figura 2.22.

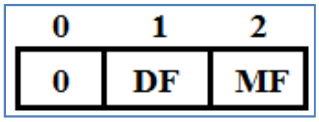

Figura. 2.22. Campo Flags.

Donde el primer bit debe ser 0, DF (*Don't Fragment*) o no fragmentar = 1 y para permitir fragmentar = 0, MF (More fragments) o mas fragmentos se especifica = 1 para decir que existen más fragmentos y = 0 significa que es el último fragmento del datagrama.

- **Fragment Offset:** Es utilizado para reensamblar todo un datagrama fragmentado, dicho de otra manera es un contador para dar orden al datagrama fragmentado, el primer fragmento es 0, este valor indica el número de segmentos de 64 bits.
- **TTL (Time to Live):** Es el tiempo en segundos que el datagrama está permitido para viajar dentro de la red, es decir es el número de saltos permitidos, con el fin de que el datagrama no se encuentre circulando infinitamente, cada router disminuye en una unidad el valor del TTL, cuando este valor llega a 0 el router informa al dueño del datagrama, mediante un mensaje ICMP que el datagrama fue eliminado.
- **Protocol:** Especifica el protocolo de nivel superior que se encuentra encapsulado en el datagrama IP, por ejemplo se tiene el valor para ICMP =1, para IGMP =2, para TCP =6, para UDP = 17, entre otros.
- **Header Checksum:** Verifica la integridad de la cabecera, es decir es el resultado de aplicar un código de protección de errores a la cabecera del datagrama.
- **Source IP Address:** Contiene la dirección IP de 32 bits de origen del datagrama.
- **Destination IP Address:** Contiene la dirección IP de 32 bits de destino del datagrama.

- **Options:** Es un campo opcional, cuando existe esta información, es utilizada para realizar un registro de ruta.
- **Padding:** Campo de relleno, cuando existe información en el campo Options, padding se utiliza para completar palabras de 32 bits con ceros.
- **Data:** Se especifican los datos del protocolo.

Para identificar de manera lógica y jerárquica a una red y también a una unidad de procesamiento dentro de una red, se realiza a través de *direcciones IP*, a cada interfaz de red se asigna una dirección IP, si un ordenador se encuentra conectado a mas de una red se llama *multi-homed*, cada interfaz de red tendrá su propia dirección IP, una dirección IP está constituida por un par de números:

Dirección IP = < # dirección de red > < # dirección de host >.

Las direcciones IP versión 4 se representan por un número de 32 bits, los 32 bits se dividen en 4 octetos (un octeto = 8 bits) separados por puntos, que se expresan como números de notación decimal, el valor decimal de cada octeto está comprendido en el rango de 0 a 255, como por ejemplo: 128.3.0.253, donde 128.3 es el número de red y 0.253 es el numero de la interfaz de red o host, para diferenciar que parte de la dirección pertenece a la red y que parte de la dirección pertenece al host, las direcciones se dividen en clases, cada clase tiene una porción determinada en los octetos para red y host, como se presenta una Tabla 2.3.

Tabla. 2.3. Clasificación en clases a las direcciones IP.

Clase	1.- Octeto	2.- Octeto	3.- Octeto	4.- Octeto
A	0 RED	HOST	HOST	HOST
B	10 RED	RED	HOST	HOST
C	110 RED	RED	RED	HOST
D	1110 RED	Direcciones multicast o multidifusión		
E	11110 RED	Reservado		

A continuación se presenta en la Tabla 2.4 el rango de direcciones de red en cada clase, y el número de direcciones de red posibles.

Tabla. 2.4. Rango de direcciones de red.

Clase	Dirección mínima de red	Dirección máxima de red	Número de direcciones de red posibles
A	1.H.H.H	126.H.H.H	2^7 - 2
B	128.0.H.H	191.255.H.H	2^14 - 2
C	192.0.0.H	223.255.255.H	2^21 - 2
D	224.0.0.H	239.255.255.H	2^20 - 2

Tanto para direcciones de red como para direcciones de host, existen dos direcciones las cuales están preasignadas, cuando tienen todos los demás bits 0 son para red, y direcciones que tienen todos los demás bits 1 se utilizan para mensajes de *broadcast*, existe otra dirección de particular importancia en la clase A, las direcciones que tienen en su primer octeto 127, son denominadas como *direcciones de loopback*, utilizadas para pruebas locales o test de *hardware*, a continuación se presenta en la Tabla 2.5 el número de host disponibles para cada red en cada clase.

Tabla. 2.5. Número de host disponible para cada red.

Clase	Octetos				# de bits para HOST	# de HOST para cada Red
	1	**2**	**3**	**4**		
A	R	H	H	H	24	16,777,214
B	R	R	H	H	16	65534
C	R	R	R	H	8	254

Para optimizar el uso de las direcciones IP, se introdujo el concepto de *Subredes*, en el cual la porción de host se subdivide para formar una subred, por lo tanto el formato es el siguiente:

Dirección IP = < # dirección de red > < # de dirección de sub red > < # dirección de host >.

Para poder identificar en una dirección IP cual es la porción de red y cuál es la de host, se utiliza una *máscara de subred*, en la cual es un número de 32 bits, que indica posiciones de bits, cuando los bits son 1 identifica la porción de red, y cuando los bits son 0 identifica la porción de los host, también este número se expresa en notación decimal.

En la cabecera del datagrama IP se encuentran las direcciones IP de los ordenadores origen y destino, estas direcciones son utilizadas por los enrutadores o *routers* para definir por cual tramo de red deben enviar los paquetes. Cuando la dirección de Origen y la dirección de destino se encuentran en la misma dirección de red se denomina enrutamiento *Directo*, y cuando la dirección de origen y destino se encuentran en distinta dirección de red se denomina enrutamiento *Indirecto*, en la cual los paquetes son enviados al Gateway para realizar su respectivo despacho, considerando que las subredes son independientes de la red.

2.3 INTRODUCCIÓN A LOS PROTOCOLOS DE VOZ SOBRE IP (VoIP)

En la actualidad existen un sin número de protocolos que definen distintas maneras en el establecimiento y control de las comunicaciones de voz sobre IP. En este tema del presente capítulo, se estudiará de manera sucinta los conceptos elementales sobre señalización y funciones básicas de los protocolos que son utilizados para el transporte de audio, a través de las redes de datos IP, estos conceptos se profundizaran en los siguientes temas del presente capítulo.

2.3.1 Clasificación de los protocolos

Para poder clasificar los protocolos utilizados en todo el proceso del establecimiento de una comunicación de voz entre dos terminales a través de una red de datos IP, primeramente se definirán los diferentes tipos de negociaciones que intercambian los terminales para poder establecer una comunicación. El primer concepto que aparece es el de informar al terminal llamado que deseo establecer una comunicación de voz, inmediatamente el terminal llamado debe responder de cierta manera aceptando o rechazando establecer la comunicación, dicho de otra manera, a este tipo de negociación en la cual el terminal llamante intercambian información con el terminal llamado, se denomina *Señalización de Llamada o en Inglés Call Signalling* .

La señal de voz se trasmite codificada y se divide en unidades de información, es decir en paquetes, los codificadores más utilizados son: G.729, G.711, GSM, entre otros, principalmente para el transporte de voz se realiza sobre segmentos UDP, esto implica la negociación de puertos UDP es decir donde el receptor espera recibir el audio, estos y otros parámetros son necesarios intercambiar entre los terminales, empleando mensajes, al intercambio de este tipo de información se denomina los protocolos de *Control de Señalización de Llamada o en Inglés Call Control Signaling.*

Después de establecer la comunicación, el audio se envía codificado en paquetes IP, las redes de datos por lo general tienen mayor variación de retardo que las redes de telefonía tradicional, porque la red de datos no fue diseñada para transportar señales de voz, y teniendo en cuenta que, una característica intrínseca de las redes IP, es que los paquetes con la señal de voz pueden llegar desordenados a su destino, por lo tanto es necesario empaquetar la información de la señal de voz, mediante un protocolo que disminuya o este en la capacidad de controlar estos efectos. A esta clase de protocolos se los llama *Protocolos de Transporte de Media o en Inglés Media Transport Protocols.* Estos protocolos trabajan en conjunto con los denominados *Protocolos de Control de Transporte de Media, en Inglés Media Transport Control Protocols*, cumpliendo con la función de informar a los terminales que intervienen en la comunicación, estadísticas de conexión y también información de jitter, paquetes recibidos, paquetes enviados, paquetes perdidos, entre otros. Los protocolos más utilizados para el transporte y control de media son: RTP (*Real-time Transport Protocol*), que trabaja en conjunto con RTCP (*Real-time Transport Control Protocol*), Cuando RTP lleva los media streams como audio o video, RTCP se encarga de monitorear, es decir provee información sobre estadísticas de transmisión y calidad de servicio (QoS), y ayuda a sincronizar los múltiples streams. Las especificaciones de estos protocolos se encuentran en la RFC 3550.

Con toda esta información recopilada parecería que se dispone de todos los elementos necesarios para establecer y lograr controlar una comunicación de voz entre dos ordenadores, esto es verdad para ciertas topologías en donde la red es pequeña, pero cuando se empieza a expandir la red o existe la necesidad de interconectarse con la PSTN mediante *Gateways*, es fundamental centralizar cierta clase de información, logrando que la red sea escalable, por lo tanto es necesario un dispositivo de control, que tenga funciones de: enrutamiento, trascoding de señalización, localización entre otros. Este dispositivo se denomina *Softswitch*, por lo tanto es necesario realizar la comunicación entre: equipos terminales, gateways, softswitch, entre otros, a los protocolos que intervienen en este tipo de comunicación se les denomina *protocolos de registración y control*, frecuentemente esta clasificación se encuentra dentro de los parámetros en los protocolos de señalización de llamadas.

A continuación se presenta en la Tabla 2.6 la clasificación de los cuatro protocolos más utilizados para VoIP existentes en la actualidad, con su respectiva función, y la entidad que lo define, como por ejemplo la ITU-T (*International Telecommunication Union*) en el sector de normalización de las Telecomunicaciones, otra entidad es el IETF (*Internet Engineering Task Force* o en español Grupo Especial sobre Ingeniería de Internet) esta entidad es mundialmente reconocida por regular las propuestas y estándares de internet, mediante los mencionados RFC.

Tabla. 2.6. Clasificación de los cuatro protocolos más utilizados para VoIP.

Nombre del Protocolo	**SIP**	**H.323**	**Megaco/H.248**	**MGCP**
Entidad	IETF	ITU-T	IETF/ITU-T	IETF
Función que realiza				
Señalización de llamada	SIP	H.225/Q.931	Megaco	MGCP
Control de Señalización de llamada	SDP	H.245	SDP	SDP
Registración y control	SIP	H.225/RAS	Megaco	MGCP
Transporte de audio	RTP	RTP	RTP	RTP
Control de transporte de audio	RTCP	RTCP	RTCP	RTCP
Nombre del dispositivo de control (SoftSwitch)	SIP server	Gatekeeper	Call Agent o MGC	Call Agent o MGC

Los cuatro protocolos actualmente más utilizados para VoIP son: SIP, H.323, Megacoy MGCP. Obsérvese que independientemente del protocolo de señalización utilizado todos emplean RTP para el transporte de audio. En el área de registración y control, SIP emplea mensajes específicos para la registración, y para el control utiliza los mensajes de señalización de llamada, en esta área H.323 define un protocolo independiente, para el caso de Megaco y MGCP no permiten llamadas sin el dispositivo de control como el softswitch, puesto que no pueden intercambiar mensajes de señalización entre gateways porque su topología es maestro esclavo. El nombre del dispositivo de control lo define cada protocolo, cada dispositivo de control está en la capacidad de trabajar con los distintos protocolos de señalización, para realizar la comunicación entre terminales y gateways.

A continuación se presenta en la Figura 2.23 la clasificación entre los protocolos de: señalización, calidad de servicio, transporte de media, que se encuentran dentro de la capa aplicación. Además se presentan los protocolos que trabajan en las diferentes capas del modelo TCP/IP.

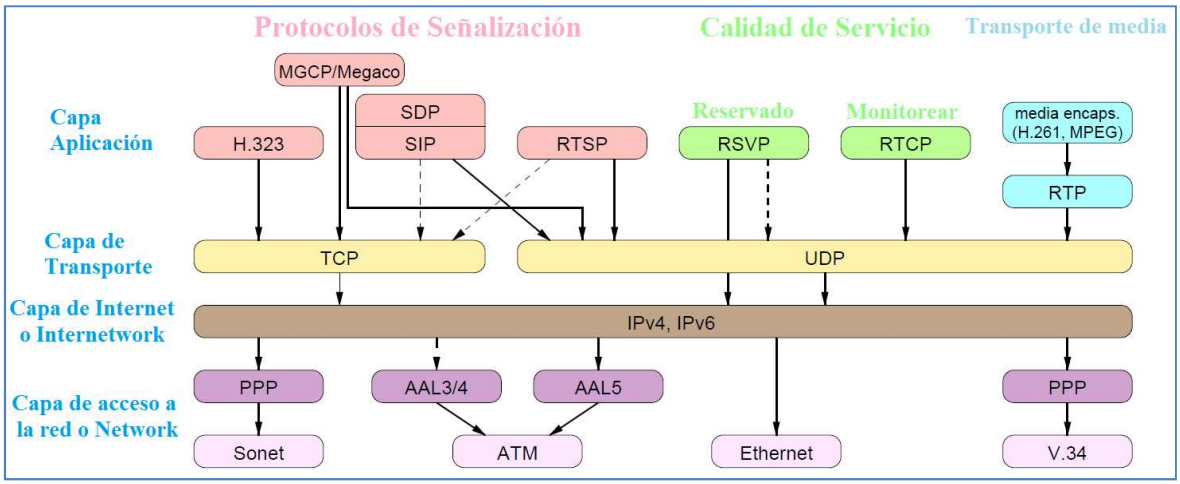

Figura. 2.23. Clasificación de protocolos para VoIP en la capa Aplicación.

2.3.2 Protocolos de señalización de llamada

Para explicar los protocolos de señalización de llamada, se cometerá mediante un ejemplo en el cual se realizará una llamada directa entre dos equipos terminales, estos puedes teléfonos IP, softphones, entre otros. El usuario *Origen* desea establecer una comunicación con el usuario *Destino*, mediante una llamada, digitando la dirección IP del usuario destino (esto no es común, porque existen dispositivos de control que traducen nombres, números en direcciones IP). El equipo terminal del usuario origen envía un paquete con un mensaje *Solicitud* al equipo terminal del usuario destino, diciéndole que desea establecer una comunicación, el equipo destino responde con otro mensaje *Respuesta* diciéndole que: recibió y está procesando la llamada, instantáneamente el equipo destino esta timbrando (ringing) y envía otro mensaje diciendo que el equipo esta timbrando, precisamente después de contestar el teléfono o atender la llamada, el equipo destino envía otro mensaje diciendo que atendió la llamada, y la comunicación se establece, es decir el audio o video se establece mediante RTP.

Todo este proceso de mensajes solicitud-respuesta se realiza por medio de los protocolos de señalización de llamada, por ejemplo el protocolo SIP, H.323, en la Figura 2.24 se presenta el ejemplo utilizado con el intercambio de mensajes solicitud-respuesta.

Figura. 2.24. Intercambio de mensajes solicitud-respuesta.

En el protocolo H.323 utiliza mensajes que habían estado definidos por el protocolo de control de conexiones Q.931 para la ISDN (Integrated Services Digital Network o en español Red Digital de Servicios Integrados), que es una recomendación de la ITU, puesto que estos mensajes inicialmente no fueron definidos para voz sobre IP, porque no poseen parámetros relacionados con IP, por lo tanto se definió al protocolo H.225 ya que tiene parámetros IP, que trabaja en conjunto con el protocolo Q.931 para el transporte de estos parámetros, en el área de UUIE (*User to User Information Element*). Este protocolo se señalización H.225/Q.931 utiliza al protocolo TCP de la capa de transporte, como se estudió TCP es un servicio orientado a la conexión, estableciendo un circuito lógico inicial, para esta clase de llamadas el equipo terminal origen trabaja como cliente, y el equipo terminal destino trabaja como servidor utilizando el puerto 1720 de TCP, como se presenta en la Figura 2.25, el intercambio de mensajes en el proceso de una llamada utilizando el protocolo H.323. [8].

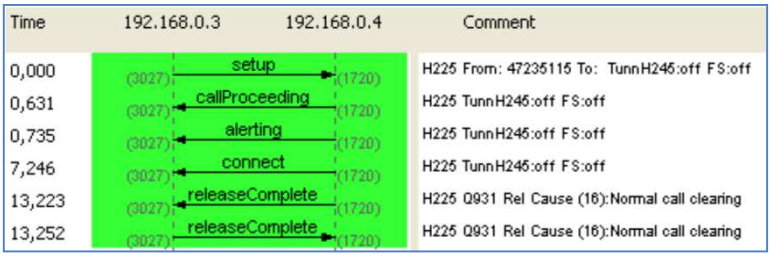

Figura. 2.25. Intercambio de mensajes en una llamada con H.323.

El protocolo SIP utiliza sus propios mensajes ya que inicialmente si fueron definidos para escenarios IP propiamente dicho para voz sobre IP, a diferencia de H.323, SIP trabaja sobre el protocolo UDP de la capa de transporte, por tal razón aparece un nuevo mensaje de confirmación denomina ACK (Acknowledgement o en español acuse de recibo) para indicar que: si ha llegado el mensaje y además ha llegado correctamente, este mensaje ACK es enviado como respuesta al mensaje 200OK.

SIP también trabaja en un modelo cliente-servidor, donde el terminal origen trabaja como cliente, y el equipo terminal destino trabaja como servidor utilizando el puerto 5060 de UDP, se presenta en la Figura 2.26 el intercambio de mensajes en el proceso de una llamada utilizando el protocolo SIP. [8].

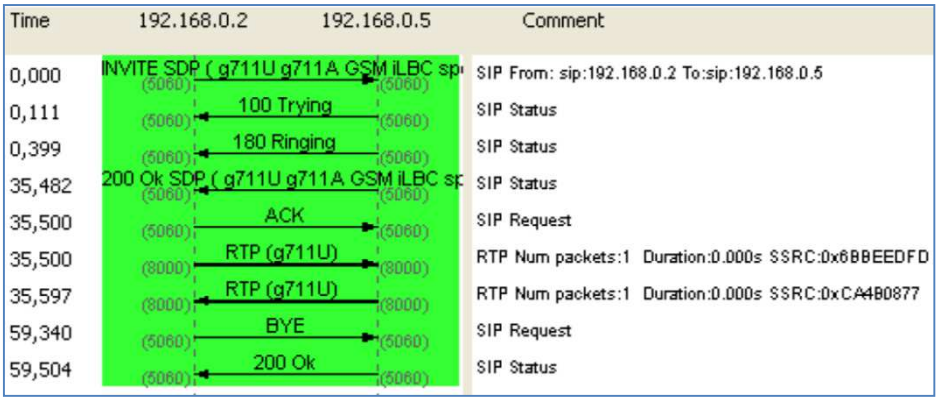

Figura. 2.26. Intercambio de mensajes en una llamada con SIP.

A continuación se presenta en la Tabla 2.7 un resumen con los nombres de mensajes básicos que utiliza SIP y H.323 con su respectivo significado.

Tabla. 2.7. Nombres de mensajes básicos que utiliza SIP y H.323.

PROTOCOLO	**SIP**		**H.323**	
Se envía desde	Origen	Destino	Origen	Destino
Deseo establecer una comunicación	INVITE		SETUP	
Recibí y estoy procesando la llamada		100 TRYING		CALL PROCEDING
El terminal esta timbrando (ringing)		180 RINGING		ALERTING
Atendí la llamada	ACK	200 OK		CONNECT

2.3.3 Protocolos de control de señalización de llamada

En los protocolos de señalización de llamada transportan en los mensajes información referente a indicadores de llamada, como por ejemplo datos del terminal origen, del terminal destino, pero no transportan información referente a como se debe enviar el audio, el audio o video se establece mediante RTP, que trabaja sobre UDP que utiliza puertos efímeros, que deben ser negociados entre los terminales, además se debe negociar parámetros como el codificador de audio, ya que existe un gran conjunto de codificadores para enviar el audio.

Por lo tanto se necesitan mensajes para negociar dos parámetros importantes, el primer parámetro es el puerto de UDP, el segundo parámetro es el *Codec* que se va a utilizar en la llamada. En la Figura 2.27 se presenta un ejemplo explicito de mensajes, con las funciones que realizan los protocolos de control de señalización de llamada.

Figura. 2.27. Ejemplo explicito de mensajes de los protocolos de control de señalización de llamada.

SIP para el control de señalización de llamada utiliza al protocolo SDP (*Session Description Protocol*), y en el caso de H.323 utiliza al protocolo H.245. En el intercambio de mensajes en una llamada SIP, SDP se envía conjuntamente con los mensajes *INVITE* y *200OK*, cabe aclarar que: el mensaje *INVITE* se envía desde el origen hacia el destino, y el mensaje *200OK* se envía desde el destino hacia el origen.

Dentro del mensaje SDP se envían los parámetros a negociar como por ejemplo el listado de *Codecs* que soporta o está en la capacidad de trabajar tanto el terminal origen como destino, este códec se envía en orden de prioridad (g711U, g711A, GSM, entre otros). También se envía la IP, el puerto en el cual se desea recibir el audio mediante RTP. En el caso del mensaje *200OK* no siempre se envía SDP, porque existió un mensaje anterior que ya negoció estos parámetros, como se resalta en la Figura 2.28.

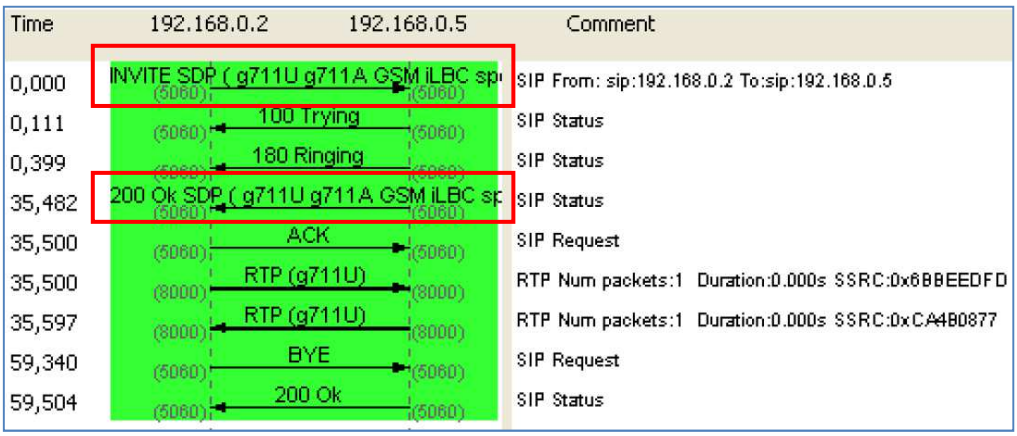

Figura. 2.28. SDP se envía en el mensaje INVITE y 200OK.

En H.323 los parámetros como códec, IP, puerto UDP, se negocian después de establecer la llamada, por lo tanto esto generó un retardo para iniciar el envío del audio, por tal razón se definió un proceso que trabaja de manera similar a SIP, denominado *Fast Start o Fast Connect*, H.323 trabaja con H.245 como protocolo de control de señalización de llamada, sobre mensajes H.225. El protocolo H.245 tiene tres mensajes básicamente para el establecimiento de la llamada:

- TCS (Terminal Capability Set), básicamente negocian las tablas de codecs.
- MSD (Master Slave Determination).
- OLC (Open Logical Channel), básicamente se establece el canal lógico, negociando puertos UDP en el cual se va a recibir el audio.

A continuación se presenta en la Figura 2.29 intercambio de mensajes del protocolo H.245 que trabaja en conjunto con H.225, en una llamada con H.323. Cabe aclara que además de mensajes para el establecimiento de la llamada, existen mensajes para mantener y finalizar una llamada.

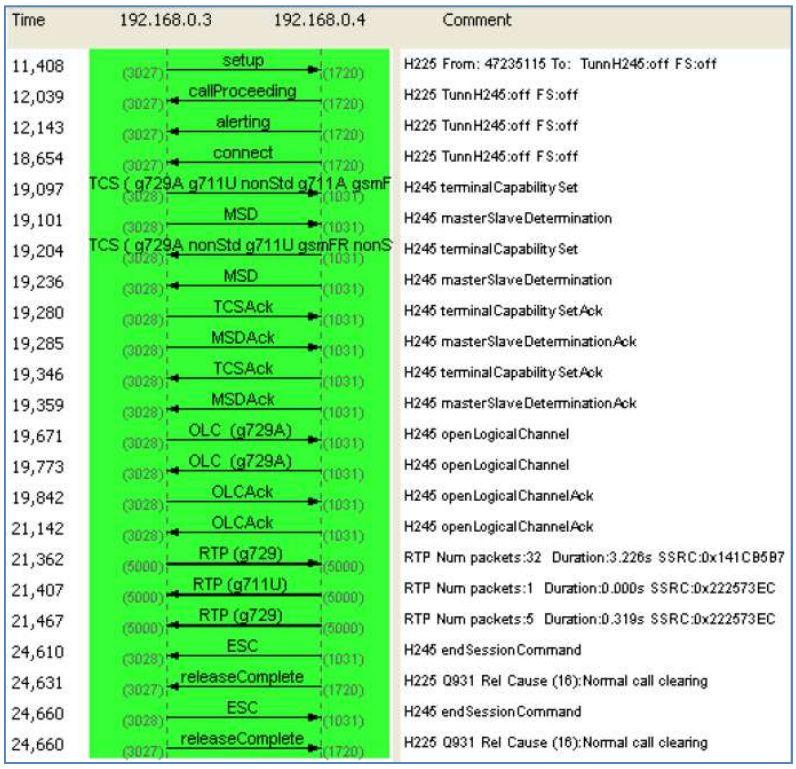

Figura. 2.29. Intercambio de mensajes del protocolo de control de señalización de llamada H.245.

A continuación se presenta en la Tabla 2.8 una comparación entre los protocolos de control de señalización, en una llamada SIP y H.323.

Tabla. 2.8. Comparación entre los protocolos de control de señalización de SIP y H.323.

Nombre del Protocolo	SIP	H.323
Protocolo de Control de Señalización de llamada	SDP	H.245
Capacidad de Negociación de codecs	Dentro del mensaje SDP	TCS
Determinación Maestro Esclavo	No negocia	MSD
Establece el canal lógico	Dentro del mensaje SDP	OCL

2.3.4 Protocolos de transporte de media

El protocolo más utilizado para el transporte de los media streams (audio, video) es RTP, independientemente del protocolo que se está utilizando para el establecimiento de la llamada. La función principal de RTP es la de transportar los media streams, propiamente dicho transportar el audio o video codificados mediante UDP, para conseguir esto existen básicamente dos campos esenciales en la cabecera del formato del mensaje RTP, los cuales están definidos en la RFC 3550:

- *Timestamp* o etiqueta de tiempo, en este campo se mide el tiempo en unidades de 125us, con esto el receptor tiene la capacidad de saber en qué instante de tiempo va a reproducir el audio recibido.
- *Sequence number* o número de orden, este campo es un número que se incrementa en una unidad por cada paquete RTP enviado, puede ser utilizado por el receptor para detectar paquetes perdidos, y para restaurar el orden de los paquetes, como se presenta en la Figura 2.30.

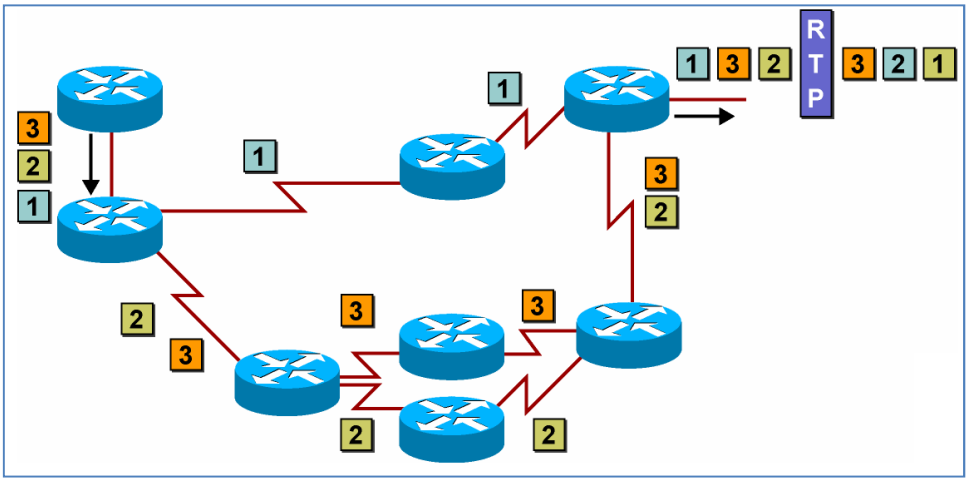

Figura. 2.30. RTP restaura el orden de los paquetes.

RTP trabaja en conjunto con RTCP, cuando RTP lleva los media streams, RTCP se encarga de monitorear estadísticas de transmisión y calidad de servicio (QoS), como jitter, paquetes recibidos, paquetes enviados, paquetes perdidos, entre otros, informando a los terminales que intervienen en la comunicación.

2.3.5 Protocolos de registración y control

En los ejemplos presentados anteriormente, la llamada se realizaba en forma directa entre los terminales, excluyendo al dispositivo de control, a continuación se presentan tres razones primordiales porque es necesario utilizar un dispositivo que permita controlar y direccionar las llamadas:

- Cuando un usuario quiere establecer una llamada, es poco manejable tener que recordar y digitar la dirección IP, del terminal destino al que se desea llamar, y además su dirección IP puede estar cambiando temporalmente, por ejemplo cuando a un computador se le asigna una dirección IP mediante DHCP.
- Es fundamental controlar entre que segmentos de usuarios están permitidos realizar llamadas, sobre todo cuando el terminal destino se encuentra dentro de una red tarifada, también es importante controlar el tiempo de duración de la llamada, para realizar la respectiva tarifación de ser necesaria.
- Cuando la red se encuentra interconectada a la PSTN, es esencial utilizar un dispositivo que realice la función de direccionar a los números telefónicos marcados, por lo tanto es necesario centralizar la información referente a ruteo, caso contrario cada terminal IP o Gateway debería estar en la capacidad de procesar tablas completas con información de ruteo, esto no es optimo, es decir deberían saber por cual Gateway deben ingresar a la PSTN en función al número telefónico marcado.

El dispositivo de control se lo denomina con distintos nombres, depende del protocolo de VoIP con el que se está comunicando, es decir en una comunicación en la cual se encuentra basada en SIP, al dispositivo de control se lo denomina: Servidor SIP (*SIP Server, SIP Proxy, Location Server, Redirect Server, Registrar*). Si la comunicación es mediante H.323 al dispositivo se lo denomina *Gatekeeper*, y para el caso de MGCP y Megaco al dispositivo de control se lo denomina *Media Gateway Controller o Call Agent*, habitualmente al dispositivo de control se lo denomina Softswitch, el cual puede trabajar como *SIP Proxy, Gatekeeper, Call Agent*, dicho de otra manera realiza funciones de ruteo, transcoding de señalización, (cabe aclarar que no realiza transcoding de audio, porque en esta clase de topologías, el audio no atraviesa por los dispositivos de control).

Ahora la llamada no se realiza en forma directa entre los terminales, porque interviene el dispositivo de control, por lo tanto también cambia la forma de trabajo, dependiendo del protocolo de VoIP que se está utilizando (SIP, H.323, MGCP, Megaco).

El primer paso es *Registrar* el equipo Terminal o Gateway, al dispositivo de control o Softswitch. Después que el equipo terminal se ha registrado, el dispositivo de control coloca al terminal dentro de su tabla de usuarios en línea, es decir el terminal ya está listo o esperando establecer una llamada. Además el dispositivo de control ya conoce la ubicación del terminal, es decir posee información como: dirección de transporte, IP, puerto. Cuando se menciona *Registrar* un terminal, se refiere a relacionar un número o nombre con una dirección de transporte, y cuando se menciona *Registrar* a un *Gateway*, se refiere a que el dispositivo de control conoce que el *Gateway* está en línea y que puede ser utilizado para rutear las llamadas en función al número telefónico marcado. Dependiendo si el número telefónico marcado (prefijos) corresponde a su tabla de ruteo, la llamada saldrá por un determinado *Gateway.*

En una comunicación con H.323, se utiliza el protocolo H.225.0 mediante un canal RAS (*Registration, Admission and Status*) para llevar mensajes que utiliza el Gatekeeper para comunicarse con los terminales y Gateway, como se presenta en la Figura 2.31, los equipos terminales tienen las direcciones IP: 192.168.0.3 y 192.168.0.5 respectivamente, los terminales realizan el proceso de registración en el *Gatekeeper* que tiene la dirección IP: 192.168.0.4, utilizando mensajes de *registración.*

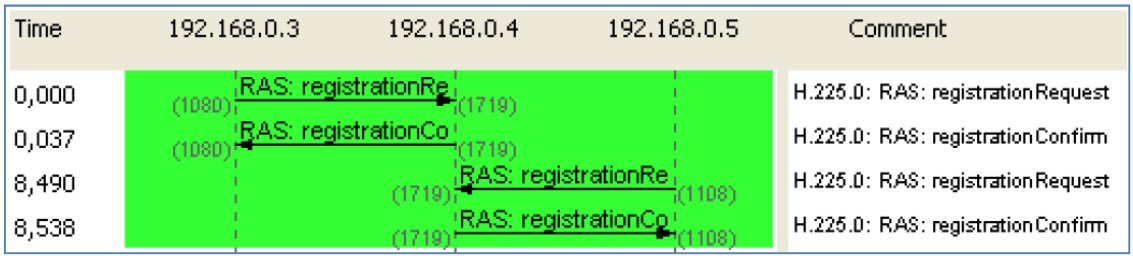

Figura. 2.31. Mensajes de registración de los terminales al Gatekeeper en una llamada con H.323.

Asimismo cuando se desea realizar una llamada existen mensajes de *admisión*, y para conocer el estado de una llamada activa existen los mensajes de *status*. En la Figura 2.32 se presenta un modelo de llamada utilizando H.323, cuando el terminal origen con dirección IP: 192.168.0.3 desea realizar una llamada al terminal destino con dirección IP: 192.168.0.5, antes de empezar a establecer la llamada mediante el mensaje *SETUP*, el terminal origen solicita permiso al *Gatekeeper*, enviando un mensaje *admission Request* (solicitud de admisión), el *Gatekeeper* responde con un mensaje *admission Confirm* (admisión confirmar) y envía la dirección de transporte del terminal destino. De la misma manera el terminal destino solicita permiso al *Gatekeeper*, antes de atender la llamada mediante el mensaje *CONNECT*.

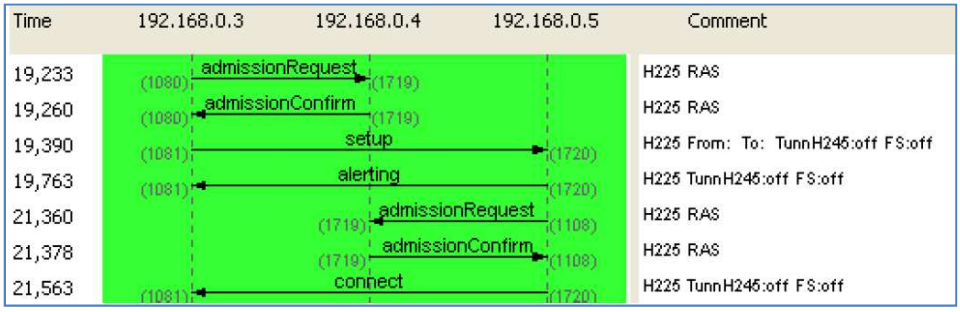

Figura. 2.32. Mensajes de admisión de los terminales al Gatekeeper en una llamada con H.323.

El protocolo SIP para realizar el proceso de registración, lo hace mediante un mensaje denominado *REGISTER*, antes de empezar a establecer la llamada mediante el mensaje *INVITE*. En una comunicación con SIP, se define un dispositivo en el cual los terminales (usuarios) deben registrarse, denominado *REGISTRAR Server*. A continuación se presenta en la Figura 2.33 un ejemplo de dos terminales o usuarios registrándose en *REGISTRAR*.

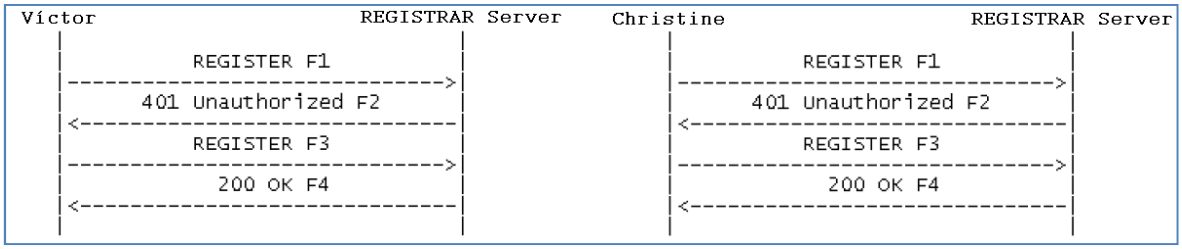

Figura. 2.33. Dos usuarios registrándose en REGISTRAR mediante SIP.

Cuando el terminal origen desea establecer una llamada al terminal destino, se empieza mediante el mensaje *INVITE*, el mensaje *INVITE* no va directamente al terminal destino, primero tiene que pasar por uno o varios dispositivos denominados *SIP PROXY*, porque el *SIP PROXY* posee información de ruteo de llamadas, además puede o no solicitar autenticación para establecer la llamada. Cabe mencionar que es muy frecuente encontrar en muchas topologías de red, que el SIP PROXY y el REGISTRAR Server se encuentran ubicados en un mismo dispositivo.

Cuando el mensaje *INVITE* atraviesa al *SIP PROXY*, este no genera una respuesta de vuelta hacia el terminal origen, esencialmente el *SIP PROXY* reenvía el mensaje *INVITE* (modificando ciertos campos) hasta llegar al terminal destino, dicho de otra manera se podría decir que el *SIP PROXY* trabaja como si fuera un router a nivel de SIP. Este ejemplo se presenta en la Figura 2.34.

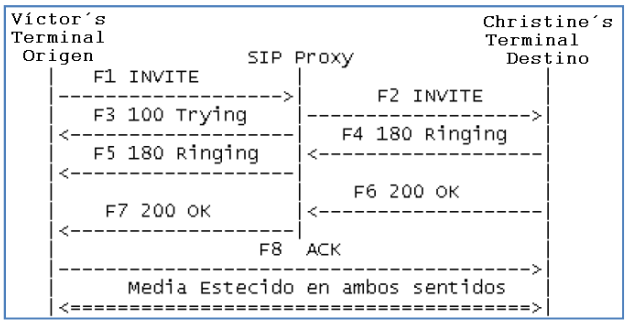

Figura. 2.34. Establecimiento de una llamada atravesando un SIP PROXY.

Los protocolos *MGCP* y *Megaco* trabajan en topologías Maestro-Esclavo, dicho de otra manera estos protocolos necesitan utilizar un dispositivo de control, en este caso el *Softswitch.* A diferencia de los protocolos SIP y H.323 que son *peer to peer*, que están en la capacidad de establecer llamadas entre terminales, sin la necesidad de utilizar un dispositivo de control. Los protocolos *MGCP* y *Megaco* fueron diseñados exclusivamente para *Gateways* y no para equipos terminales. La idea principal es de simplificar o reducir la cantidad de procesamiento de los *Gateways*, y centralizar la mayor cantidad de información en el *Call Agent o Softswitch,* es decir toda la "inteligencia" se concentra en este dispositivo. Por lo tanto el Gateway constantemente debe estar esperando recibir instrucciones del *Call Agent*, es por esto que con una arquitectura MGCP y Megaco no podría existir una comunicación peer to peer.

Consecuentemente se podría decir que los protocolos MGCP y Megaco definen mensajes para la señalización de la llamada y además para registración y control. Cabe recordar que estos protocolos utilizan a SDP como protocolo de control de señalización de la llamada, y de la misma forma utiliza a RTP como protocolo para el transporte de media (audio). A continuación se presenta en la Tabla 2.9 una comparación entre los cuatro protocolos más utilizados para VoIP.

Tabla. 2.9. Comparación entre los cuatro protocolos más utilizados para VoIP.

Nombre del Protocolo	**SIP**	**H.323**	**Megaco/H.248**	**MGCP**
Entidad	IETF	ITU-T	IETF/ITU-T	IETF
Presenta una arquitectura	Distribuida	Distribuida	Centralizada	Centralizada
Versión Actual	SIP 2.0 RFC 3261	H.323v6	H.248.1 RFC 3525	MGCP 1.0 RFC 2705
Transporte de señalización	TCP o UDP siendo UDP el más utilizado	UDP (canal RAS), TCP para lo demás	TCP o UDP	UDP
Codificación	Texto	ASN.1	ASN.1 o Texto	Texto

El protocolo H.323 fue el primero en constituirse como líder por el hecho de ser escalable y maduro, su principal competidor es el protocolo SIP, puesto que estos protocolos trabajan con el mismo tipo de arquitectura (Distribuida), actualmente SIP está ganando mucho protagonismo, y aceptación por parte de varios proveedores de servicios para el transporte de tráfico en VoIP, gran parte de las nuevas soluciones se están implementando con SIP. Los protocolos MGCP y Megaco son utilizados esencialmente por los proveedores de servicios de telefonía, puesto que tienen la capacidad de controlar de manera muy eficiente a muchos Gateways, ya que cada Gateway posee gran cantidad de abonados POTS[14], Megaco ha ganado terreno en soluciones con troncales, por manejar grandes cantidades de abonados POTS. Ya no se desarrollan más especificaciones para MGCP, las modificaciones en este tipo de arquitectura (Centralizada) se realizan en las especificaciones de Megaco/H.248.

14 POTS es el acrónimo de *Plain Old Telephone Service*, que es el servicio de línea telefónica convencional (analógica), tradicional o red telefonía básica RTB, por medio del cableado de cobre.

2.4 INTRODUCCIÓN A CALIDAD DE SERVICIO (QoS), CODECS, Y Wi-Fi

Para el desarrollo del presente proyecto es necesario conceptualizar los siguientes parámetros que se relacionan con Voz sobre IP: *Calidad de Servicio (QoS), Codecs y Wi-Fi*, los cuales se describen a continuación.

2.4.1 Calidad de servicio (QoS) en VoIP

Con el paso del tiempo, se podría pensar que VoIP lograría reemplazar a la red de telefonía tradicional (PSTN), por lo tanto los clientes necesitan recibir la misma calidad de transmisión de voz que reciben con los servicios de telefonía básica, esto significa una consistente alta calidad en la transmisión de voz. Al igual que otras aplicaciones en tiempo real, VoIP es extremadamente sensible al ancho de banda y a los retrasos.

Las transmisiones de VoIP para ser inteligibles al receptor, es decir para que pueda entender el receptor necesita que: no exista perdidas de paquetes de voz, tampoco debería existir un retardo excesivo, ni sufrir variaciones de retardos (conocido como *Jitter*), por ejemplo los siguientes estándares deben cumplirse:

- El codec por defecto G.729, requiere la pérdida de paquetes por lo menos de 1 por ciento para evitar errores audibles. Idealmente, no debería haber ninguna pérdida de paquetes en VoIP.

- La especificación ITU G.114 recomienda un retardo, inferior a 150 milisegundos (ms) en una vía o en un solo sentido, de extremo a extremo, para obtener alta calidad en tráfico de tiempo real, como la voz. Para llamadas internacionales, en un solo sentido, retardo de hasta 300 ms es aceptable, especialmente para transmisiones vía satélite. Este retraso en un solo sentido posee un retardo de propagación, en consideración al tiempo que necesita la señal en recorrer su distancia.

- Jitter buffers (para compensar la variación de retardo) añade aún más el retardo de extremo a extremo, y son generalmente efectivos solo en variaciones de retardo inferior a 100 ms. Por lo tanto el Jitter debe ser minimizado.

VoIP puede garantizar una alta calidad en la transmisión de voz, si los canales de señalización y de audio, tienen prioridad sobre otros tipos de tráfico de la red. Para que los usuarios reciban un nivel aceptable de calidad de la voz, el tráfico de VoIP debe garantizar ciertas compensaciones de: ancho de banda, latencia, y requisitos de Jitter. QoS asegura que los paquetes de voz de VoIP reciban el tratamiento preferencial que requieren.

Es bastante evidente el desarrollo de la telefonía IP, porque principalmente aprovecha los recursos existentes y disminuye el costo de las llamadas por medio de la Internet. El éxito de cualquier producto/servicio es directamente proporcional a la calidad que mantiene. Con referencia a la telefonía IP, la calidad y el costo son dos factores importantes que pueden afectar el atractivo de este servicio. VoIP todavía adolece con respecto a la calidad de transmisión de voz que presentan los servicios de telefonía tradicional, pero con la constante expansión de las conexiones de banda ancha, han conseguido que la calidad de servicio de esta tecnología, llegue a un excelente nivel, lo cual podría llegar a convertirse en una gran competencia para las empresas de telefonía tradicional.

En una red VoIP presenta ciertos problemas con respecto a la calidad de servicio (QoS), los principales son: la Latencia, el Jitter, el Eco, y pérdida de paquetes. Estos problemas son resueltos mediante diversas técnicas, que se analizarán en los siguientes temas del presente capitulo. Estos problemas se originan principalmente por dos factores:

1. La red de internet es un sistema fundamentado en la conmutación de paquetes, es decir los paquetes pueden viajar por el mejor camino entre dos puntos, donde siempre tienen más de un camino o ruta disponible, con mayores opciones por donde llegar a su destino (característica intrínseca de las redes IP), por lo tanto se puede producir efectos de pérdida de paquetes o Jitter.

2. En las comunicaciones VoIP se transportan los datos en tiempo real, por lo tanto se producen efectos como: eco, pérdida de paquetes, retardos, latencia, los cuales pueden llegar a ser muy incómodos para mantener una conversación. Por lo tanto deben ser minimizados.

2.4.1.1 Retardo

El Retardo es el tiempo de tránsito que necesitan los paquetes en recorrer su distancia, desde el origen hacia el destino y vuelta. Los usuarios tienen la capacidad de mantener una conversación cómodamente aunque exista cierto retardo, no obstante puede llegar a un umbral en el cual empieza a ser incómodo para mantener una conversación.

2.4.1.2 Latencia

La Latencia se puede definir como los retardos acumulados, por ejemplo: existen retardos en los *switches* (proceso *store and forward*), retardos de procesamiento (se realiza cambios en los encabezados de los paquetes), entre otros. Adicionalmente se añaden los retardos propios sobre el proceso de compresión vocal.

La latencia se define técnicamente en VoIP, como la cantidad de tiempo necesario para transmitir un paquete desde el origen hasta el destino. Se trata de un retardo de extremo a extremo que se produce en el intercambio de información entre dos nodos. Simplemente, puede ser referido como la velocidad de la red que puede afectar la calidad general del servicio. Las comunicaciones en tiempo real como VoIP son sensibles a este efecto, es un problema frecuente en enlaces lentos o congestionados.

- Valores recomendados

La Latencia entre extremo a extremo de la comunicación, se recomienda ser inferior a 150 ms.

- Potenciales soluciones

Generalmente depende de los equipos por los que atraviesan los paquetes, es decir, de la red propiamente dicha. Se podría reservar un ancho de banda desde el origen hacia el destino, también señalizar los paquetes con valores de TOS (Tipo de Servicio), para priorizar el trafico de tiempo real.

2.4.1.3 Jitter

El Jitter se define técnicamente como la variación de tiempo en la llegada de los paquetes, es decir, el Jitter es un efecto en el cual el retardo entre paquetes no es constante, por lo tanto existe una variación en los retardos, producida por congestión de tráfico en la red o en el *backbone*[15] de red. Se podría minimizar este efecto proporcionando: prioridad al tráfico de voz con respecto al de datos, enlaces de mayor velocidad.

El Jitter es un efecto de las redes de datos IP no orientadas a conexión, las cuales son fundamentadas en conmutación de paquetes, consecuentemente los paquetes pueden seguir rutas distintas para llegar a su destino.

- Potenciales soluciones

La principal solución considerablemente adoptada es utilizar *Jitter buffers*, los *Jitter buffers* básicamente asignan una cola o almacén, para ir recibiendo los paquetes y añadiendo un pequeño retraso, generalmente en los teléfonos IP tanto en hardware como en software, se pueden modificar o configurar los *buffers*. Una disminución del *buffer* significa menos retardo pero más pérdida de paquetes, caso contrario, un aumento del *buffer* significa menos pérdida de paquetes pero más retardo.

15 Backbone se refiere a las principales conexiones troncales de Internet.

2.4.1.4 Eco

Básicamente el eco es un fenómeno técnico producido por la desadaptación de impedancias en el circuito híbrido que convierte de 4 a 2 hilos en los sistemas telefónicos, también es producido por el retorno de la señal, es decir el sonido sale por los altavoces y regresa nuevamente al micrófono, obteniendo una ligera permanencia del sonido, este fenómeno es también conocido como reverberación. El eco se define como una reflexión retardada de la señal acústica original.

- Valores recomendados

La intensidad del eco es un factor importante, puesto que normalmente la señal de vuelta tiene menor potencia que la original. Un valor tolerable es que la señal llegue a 65 ms y con una atenuación de 25 a 30 dB.

2.4.1.5 Pérdidas de paquetes (Packet Loss)

Esto se refiere a la tasa de pérdida de paquetes, en la cual representa el porcentaje de paquetes transmitidos que se descartaron en la red. Estos descartes pueden ser ocasionados por altas tasas de error en algún medio de enlace, o también por sobrepasar la capacidad de un buffer de una interfaz en momentos de congestión. La perdida de paquetes máxima admitida para que no se degrade la comunicación en aplicaciones de voz deber ser inferior al 1%.

2.4.1.6 Calidad de servicio (QoS) en un dispositivo de red

La calidad de servicio (QoS) en un dispositivo de red ayuda a las aplicaciones tales como voz, video *streaming*, y otras aplicaciones sensibles al tiempo, proporcionando una apropiada prioridad, y un ancho de banda adecuado al tráfico durante la congestión de la red.

Las llamadas de voz y video *streaming*, pueden sufrir efectos de Jitter, latencia, paquetes perdidos, cuando el tráfico en general excede la capacidad de la red, por lo tanto el tráfico de voz y video deben recibir un trato prioritario, lo cual es proporcionado la clasificación de QoS.

Adicionalmente, QoS puede proporcionar configuraciones de cantidades de ancho de banda, para aplicaciones importantes como voz y video, asegurando la continuidad de dichas aplicaciones. La calidad de servicio es de vital importancia en un router WAN, o en un *switch* LAN, por lo tanto requieren de una configuración de QoS para evitar alguna potencial degradación de la calidad de voz o vídeo.

2.4.1.7 ¿Cómo trabaja la QoS en un dispositivo de red?

El dispositivo de red realiza un procedimiento para ofrecer calidad de servicio, este procedimiento que se detalla a continuación:

1. Establecimiento de prioridades.
   - ✓ Clasificar y marcar los tipos de tráfico.
   - ✓ Primero voz, después video, a continuación datos.

2. Poner en cola a los paquetes.
   - ✓ Clasificar el tráfico en colas/grupos.
   - ✓ Transmitir primero el tráfico de mayor prioridad.

3. Regulación de tráfico.
   - ✓ Control de la tasa de transmisión, garantizar ancho de banda.
   - ✓ Bajar la prioridad del tráfico cuando sea necesario.

A continuación se presenta en la Figura 2.35 el procedimiento de cómo trabaja la QoS en un dispositivo de red, con cuatro diferentes tipos de paquetes (aplicaciones). Los paquetes de color AZUL tienen la primera prioridad es decir la más alta, porque representan a los paquetes de gestión de red y voz. Los paquetes de color ROJO tienen la segunda prioridad, estos paquetes son de video. Los paquetes de color VERDE tienen la tercera prioridad, estos son paquetes esenciales (*core*) de la red, por ejemplo: las consultas de base de datos, etc. Los paquetes de color AMARILLO tienen la prioridad más baja "mejor esfuerzo", estos paquetes representan los paquetes de datos, por ejemplo Internet o correo electrónico.

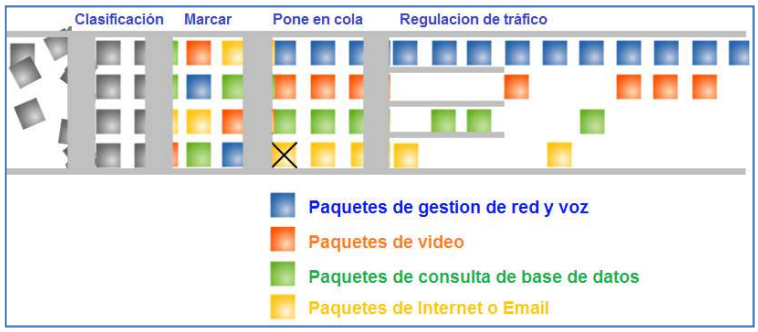

Figura. 2.35. Procedimiento para ofrecer QoS en un dispositivo de red.

Las aplicaciones de voz y vídeo son más sensibles a retardos y al Jitter, estas aplicaciones comúnmente son compartidas en las redes de datos, por lo tanto los paquetes de voz y video deben ser identificados (frecuentemente denominados clasificados), marcados mediante los métodos 802.1p (layer 2) o DSCP (layer3) (*DiffServ Código Point*, son los seis bits más significativos del byte ToS en la cabecera del paquete IPv4, los otros dos bits se utilizan para control de flujo). La implementación de QoS minimizar los retardos y Jitter.

El método 802.1p utiliza el campo *user priority* (PRI, prioridad de usuario) también denominado Clase de Servicio (CoS) en *layer* 2 (*Class of Service*), PRI se encuentra dentro del campo TAG de la trama Ethernet, utilizado para identificar la aplicación. Los diferentes tipos de tráfico (aplicaciones) son asignados un valor diferente de CoS. Existen valores predeterminados los cuales son recomendados para utilizar CoS, estos valores se presentan en la Tabla 2.10.

Tabla. 2.10. Valores recomendados para CoS.

CoS	Aplicación
7	Reservado
6	Routing
5	Voz
4	Video
3	Señalización de llamada
2	Datos críticos
1	Datos de forma masiva
0	Datos mejor esfuerzo

2.4.1.8 Resumen de los requisitos de QoS para Voz sobre IP

En voz sobre IP la señal analógica de voz debe que pasar por un proceso de codificación, posteriormente tiene atravesar por varios componentes de la red, como se presenta en la Figura 2.36. Básicamente los requisitos para transportar voz sobre IP en un solo sentido son los siguientes:

- La latencia entre extremo a extremo de la comunicación, se recomienda ser menor o igual a 150 ms.
- El Jitter se recomienda ser menor o igual a 30 ms.
- Paquetes perdidos se recomienda ser menor o igual al 1%.
- Garantizar un ancho de banda necesario para aplicaciones de voz.

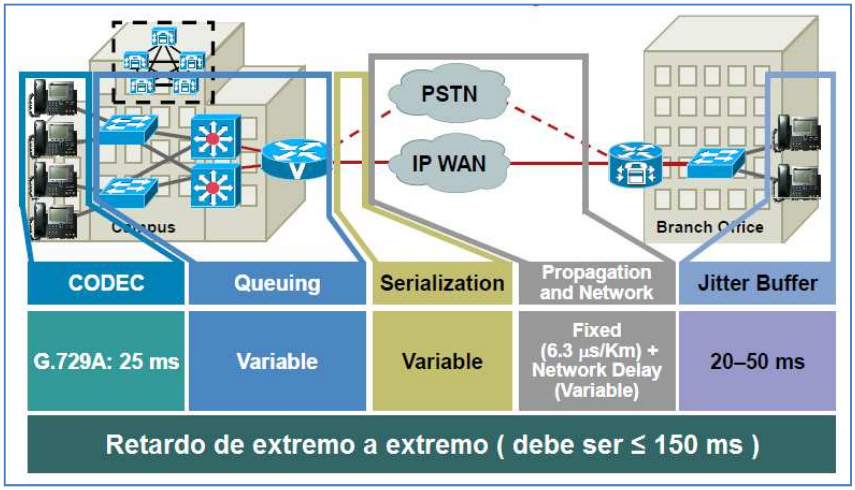

Figura. 2.36. Requisitos de QoS para Voz sobre IP.

2.4.2 Codecs

Un codec, que proviene del Inglés coder-decoder, (codificador / decodificador) convierte las señales analógicas a un flujo de bits (*bitstream*) digitales (formato de audio digital), y otro codec idéntico en el otro extremo de la comunicación convierte el flujo de bits digitales en una señal analógica, para poder reproducir la señal. Básicamente VoIP se fundamenta en la conversión de señales analógica – digital, como se ilustra gráficamente en la Figura 2.37.

Figura. 2.37. Codec convierte las señales analógicas a un flujo de bits (*bitstream*).

En el mundo de VoIP, los codecs se utilizan para codificar la voz para su transmisión a través de redes IP. Codecs en VoIP también se les conoce como vocoders, para "codificadores de voz". Los codecs generalmente ofrecen una capacidad de compresión para ahorrar ancho de banda de red. Algunos codecs también apoyan la supresión de silencio, donde el silencio no está codificado o transmitido.

2.4.2.1 Funcionamiento de los codecs en VoIP

Los codecs trabajan utilizando algoritmos avanzados permitiendo tomar las muestras, ordenas, comprimir y empaquetar los datos. El algoritmo más común en aplicaciones VoIP es el algoritmo *CS-ACELP (Conjúgate Structure Algebraic Code Excited Linear Prediction*), este algoritmo también ayuda a organizar el ancho de banda disponible. En el anexo B del algoritmo CS-ACELP aplica una regla en comunicaciones VoIP, la cual indica que: si nadie está transmitiendo, no mandar ninguna información, consiguiendo una gran eficiencia, característica de las redes basadas en la conmutación de paquetes.

Los codecs cumplen el trabajo de convertir las señales analógicas a un flujo de bits digitales, tomando muestras de la señal de voz (audio) miles de veces por segundo, lo que se conoce como Muestreo (*sampling*), por ejemplo, el codec G.711 toma 8,000 muestras por segundo, convirtiendo cada pequeña muestra a un formato digital, es decir las muestras se convierten en un flujo de bits (*bitstream*) digitales. Adicionalmente a la conversión el codec también comprime el flujo de bits, y para su transmisión se los divide en unidades de información denominados *paquetes*, como se presenta en la Figura 2.38.

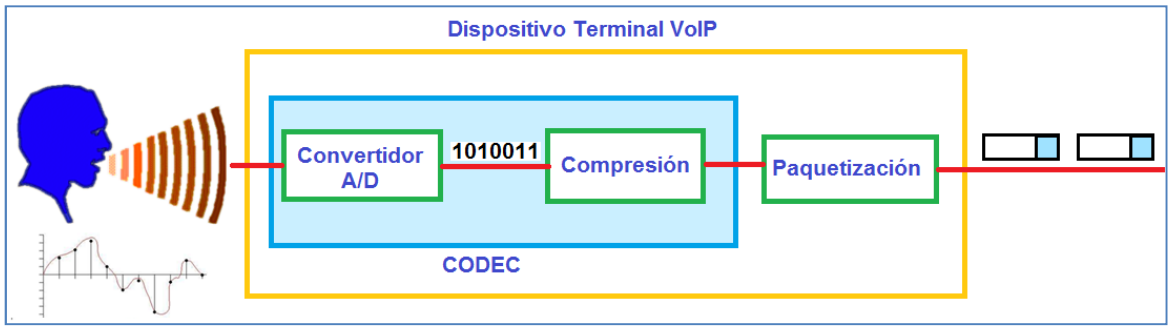

Figura. 2.38. Proceso de conversión de la señal de voz para su transmisión.

En el proceso de conversión, existen muchas formas de transformar la señal analógica de la voz a información digital, los cuales se rigen por varios estándares. El proceso de conversión generalmente se basa en la *modulación por impulsos codificados (MIC o PCM* por sus siglas en Inglés *Pulse Code Modulation*), o en alguna variante.

Para comprender de mejor manera los principales parámetros que caracterizan un codec, se analizará brevemente el funcionamiento del codec G.711, este codec para la conversión utiliza *PCM*, el cual se basa principalmente en tres procesos:

1. Muestreo (*sampling*).
   Toma valores instantáneos de una señal analógica en intervalos iguales de tiempo, a estos valores tomados se los denomina muestras.
2. Cuantificación (*quantization*).
   Asigna valores discretos a las amplitudes de las muestras.
3. Codificación (*codification*).
   Representa una muestra cuantificada en un número binario, es decir mediante códigos preestablecidos, la señal analógica se transformará en un tren de impulsos de señal digital (sucesión de ceros y unos).

- Muestreo (*sampling*)

El proceso de muestreo se fundamenta en tomar valores instantáneos de una señal analógica, estos valores se toman en intervalos iguales de tiempo, este proceso se ilustra en la Figura 2.39.

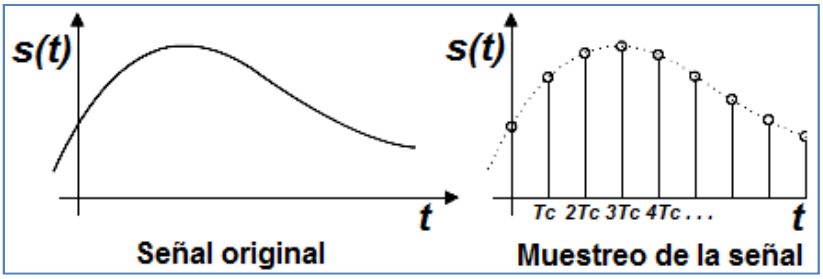

Figura. 2.39. Proceso de muestreo.

El proceso de muestreo se realiza a un ritmo uniforme, representado por la tasa o frecuencia de muestreo (fm) o en Inglés *sampling rate*. Que es el número de muestras por unidad de tiempo que se toman de una señal continua para producir una señal discreta, las frecuencias generalmente se expresan en hercios (Hz, ciclos por segundo) o múltiplos, como por ejemplo el kilohercio (kHz).

La frecuencia de muestreo debe cumplir con una condición, la cual está basada en el *Teorema de muestreo o de Nyquist-Shannon*, afirmando que: para poder replicar con exactitud una señal con una frecuencia máxima (f), (es decir, siendo matemáticamente reversible en su totalidad) es necesario que la frecuencia de muestreo (fm) sea por lo menos el doble de la frecuencia máxima (2f).

La voz humana es una señal analógica no periódica, su rango de operación en frecuencia está entre 20 y 20.000Hz, no obstante, su ancho de banda útil es decir donde está concentrada la mayor información está entre 300 a 3.400Hz, de acuerdo con el teorema del muestreo, es necesario tomar muestras a una frecuencia por lo menos a 6.800Hz (2*3.400).

Prácticamente la frecuencia de muestreo o *sampling rate* es de 8.000Hz, este valor quiere decir que: se toman 8.000 muestras por segundo, que corresponde a una separación entre muestras o propiamente dicho periodo de muestreo (T) de: T=(1/fm), T=(1/8000), T=0.000125segundos, es decir T=125us. Por lo tanto en este ejemplo dos muestras consecutivas de una misma señal se encuentran separadas 125us.

En el otro extremo de la comunicación, un codec idéntico convierte el flujo de bits digitales en una señal analógica, es decir las 8,000 muestras son reconstruidas, los pedazos de audio que se perdieron entre el medio de estas muestras, son tan pequeños que es imposible ser percibido por el oído humano, prácticamente se escucha como una sucesión continua de audio. La frecuencia de muestreo (fm) en VoIP depende del codec que se esté utilizando, por lo general existen las siguientes frecuencias de muestreo:

- ✓ 64.000 muestras por segundo (fm = 64 kHz).
- ✓ 32.000 muestras por segundo (fm = 32 kHz).
- ✓ 8.000 muestras por segundo (fm = 8 kHz).

2.4.2.2 Codecs utilizados en VoIP

A continuación se presenta en las Tablas 2.11, 2.12, 2.13, un resumen con los codecs más utilizados en VoIP, además se indican los principales parámetros que los caracterizan, estos parámetros son los siguientes:

- Bit rate (Kbps)

  Basado en el codec, este es el número de bits por segundo que deben ser transmitidos para entregar una llamada de voz. (Codec Bit rate = tamaño de la muestra / intervalo de la muestra).

- Tamaño de la muestra (Bytes)

  Basado en el codec, este es el número de bytes capturados por el Procesador Digital de Señales o DSP (*Digital Signal Processor*), en cada intervalo de muestreo del codec. Por ejemplo, el codificador G.729 opera en intervalos de muestreo de 10 ms, lo que corresponde a 10 bytes (80 bits) por muestra, por lo tanto su Bit rate es de 8 Kbps.

- Intervalo de la muestra (ms)

  Este es el intervalo de muestreo en el que el codec opera. Por ejemplo, el codificador G.729 opera en intervalos de muestreo de 10 ms.

- Sampling rate (KHz)

  Es la frecuencia de muestreo de la señal de voz.

- Frame size

  Representa cada cuantos milisegundos se envía un paquete con información sonora.

- MOS (Mean Opinion Score)

  Indica una calificación numérica de la calidad de la señal de voz en el destino final de la comunicación, este esquema utiliza pruebas subjetivas (medidas de opinión), esta calificación es expresada con un número en el rango de 1 a 5, donde 1 es la más baja calidad de audio recibido, y 5 es la más alta medición de la calidad de audio recibido, esta medida posteriormente es calculada matemáticamente, obteniendo como resultado un indicador cuantitativo de las cualidades técnicas del codec utilizado.

Tabla. 2.11. Información del codec.

Codec	Bit Rate (Kbps)	Tamaño de la muestra (Bytes) (1Byte = 8 bits)	Intervalo de la muestra (ms)	Mean Opinion Score (MOS)
G.711	64	80	10	4.2
G.729	8	10	10	4.0
G.723.1	6.3	24	30	3.9
G.723.1	5.3	20	30	3.8
G.726	32	20	5	3.85
G.726	24	15	5	
G.728	16	10	5	3.61
G722	64	80	10	4.13
ilbc mode 20	15.2	38	20	NA
ilbc mode 30	13.33	50	30	NA

Tabla. 2.12. Codecs más utilizados en VoIP.

Nombre	Estandarizado	Bit rate (kb/s)	Muestreo Sampling rate (KHz)	Frame size (ms)	MOS
G.711	ITU-T	64	8	20	4.2
	Descripción	Pulse code modulation (PCM).			
	Observaciones	Tiene dos versiones u-law (US, Japón) y a-law (Europa y resto del mundo) para muestrear la señal. Entrega precisa en la transmisión de voz. Los requisitos muy bajos de procesador. Necesita por lo menos 128 kbps para dos vías.			
G.721	ITU-T	32	8		
	Descripción	Adaptive differential pulse code modulation (ADPCM).			
	Observaciones	Obsoleta. Se ha transformado en la G.726.			
G.722	ITU-T	64	16		
	Descripción	7 kHz audio-coding within 64 kbit/s.			
	Observaciones	Divide los 16 Khz en dos bandas cada una usando ADPCM. Se adapta a diferentes compresiones de ancho de banda.			
G.722.1	ITU-T	24/32	16	20	
	Descripción	Codificación a 24 y 32 kbit/s para sistemas sin manos con baja perdida de paquetes.			
G.723	ITU-T	24/40	8		
	Descripción	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones en circuitos digitales.			
	Observaciones	Obsoleta por G.726. Es totalmente diferente de G.723.1.			
G.723.1	ITU-T	5.3/6.3	8	30	3.8-3.9
	Descripción	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.			
	Observaciones	Parte de H.324 video conferencing. Codifica la señal usando linear predictive analysis-by-synthesis coding. Para el codificador de high rate utiliza Multipulse Maximum Likelihood Quantization (MP-MLQ) y para el de low-rate usa Algebraic-Code-Excited Linear-Prediction (ACELP).			
G.726	ITU-T	16/24/32/40	8	20	3.85
	Descripción	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM).			
	Observaciones	ADPCM; reemplaza a G.721 y G.723.			
G.727	ITU-T	variable rate ADPCM 16-40			
	Descripción	5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM).			
	Observaciones	ADPCM. Relacionada con G.726.			

Tabla. 2.13. Codecs más utilizados en VoIP.

Nombre	Estandarizado	Bit rate (kb/s)	Muestreo Sampling rate (KHz)	Frame size (ms)	MOS
G.728	ITU-T	16	8	2.5	3.61
	Descripción	Coding of speech at 16 kbit/s using LD-CELP (Low-Delay Code Excited Linear Prediction).			
	Observaciones	CELP.			
G.729	ITU-T	8	8	10	4.0
	Descripción	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP).			
	Observaciones	Excelente utilización del ancho. Error tolerante. Se requiere licencia. Bajo retardo (15 ms).			
GSM 06.10	ETSI	13	8	22.5	
	Descripción	Regular Pulse Excitation LongTerm Predictor (RPE-LTP).			
	Observaciones	Gratuito y está disponible en muchos hardware y software plataformas. Se utiliza en teléfonos móviles con tecnología GSM.			
LPC10	Gobierno de USA	2.4	8	22.5	
	Descripción	Linear-predictive codec.			
	Observaciones	10 coeficientes. La voz suena un poco "robótica".			
Speex		8, 16, 32	2.15-24.6 (NB), 4-44.2 (WB).	30 (NB), 34 (WB).	
	Descripción	CELP (Code Excited Linear Prediction).			
	Observaciones	Minimizar el uso de ancho de banda mediante el uso variable del bit rate.			
iLBC		13.33, 15.20	8	30	
	Descripción	Internet Low Bitrate Codec.			
	Observaciones	Robusto en perdidad de paquetes.			
DoD CELP	American Department of Defense (DoD) Gobierno de USA.	4.8		30	
EVRC	3GPP2	9.6/4.8/1.2	8	20	
	Descripción	Enhanced Variable Rate CODEC.			
	Observaciones	Se usa en redes CDMA.			
DVI	Interactive Multimedia Association (IMA).	32	Variable		
	Descripción	DVI4 uses an adaptive delta pulse code modulation (ADPCM).			
L16		128	Variable		
	Descripción	Uncompressed audio data samples.			

Cuando se selecciona un codec, afecta directamente a la calidad de la voz, debido a los diferentes algoritmos de compresión utilizados y a la cantidad de ancho de banda que necesita.

Los codecs más utilizados para transmitir Voz sobre IP son los siguientes:

- G.711

  Este codec es un estándar de la ITU-T, codifica la voz a 64 Kbps utilizando PCM. G.711 usualmente esta descrito como un descompresor que utiliza la misma frecuencia de muestreo de la telefonía tradicional, además este codec posee una calificación MOS de 4.2, sin embargo utiliza una gran cantidad de ancho de banda para su transmisión, puede ser utilizado en entornos LAN por ejemplo teléfonos IP conectados en redes de 100Mbps. Existen 2 algoritmos principales que definen este estándar, el algoritmo mu-law (utilizado en Norte América y Japón) y el algoritmo a-law (utilizado en Europa y el resto del mundo).

- G.729

  Este codec es un estándar de la ITU-T, codifica la voz a 8 Kbps utilizando CS-ACELP (predicción lineal de código algebraico excitado en estructura conjugada), G.729 posee una frecuencia de muestreo de 8 KHz y utiliza un tamaño de cuadro de 10ms. Este codec posee una calificación MOS de 4.0. Este es el codec habitualmente utilizado en aplicaciones de Voz sobre IP, debido a que brinda una alta compresión, esto quiere decir que utiliza poco ancho de banda para su transmisión, dicho de otra manera, tiene el balance justo entre una buena calidad de voz (sonido) y eficiencia en el uso de ancho de banda.

- G.723

  Este codec es un estándar de la ITU-T, presenta un algoritmo de baja tasa de compresión, posee dos versiones, 5.3 Kbps, 6.4 Kbps, G.723 brinda bajo ancho de banda para su transmisión. Este codec posee una calificación MOS de 3.9. Este codec es adecuado en conexiones WAN de bajo ancho de banda.

A continuación se presenta en la Tabla 2.14, una referencia del consumo aproximado de ancho de banda que tienen los diferentes tipos de codecs más utilizados en Voz sobre IP. Cabe resaltar que el ancho de banda es calculado sin *Supresión de Silencio*, es decir, por ejemplo existen codecs que permiten que la conexión RTP siempre este en línea, pero existen otros codecs que permiten *Voice Activity Detection* (VAD), básicamente, esto quiere decir que solo se va a transmitir la voz cuando se detecte, por lo tanto nos permite ahorrar ancho de banda. El uso de *Supresión de Silencio* puede reducir el consumo de ancho de banda hasta en un 30%.

Tabla. 2.14. Ancho de banda aproximando utilizado en una llamada externa.

Codec	Bit rate (Kbps)	Ancho de Banda Aproximado usado en una conversación	2 Calls (Kbps)	4 Calls (Kbps)	6 Calls (Kbps)	8 Calls (Kbps)
G.711	64	110 Kbps	220	440	660	880
G.726-40	40	87 Kbps	174	348	522	696
G.726-32	32	79 Kbps	158	316	474	632
G.726-24	24	71 Kbps	142	284	426	568
G.726-16	16	63 Kbps	126	252	378	504
G.729	8	55 Kbps	110	220	330	440
G.723.1	5.3	36 Kbps	73	145	218	290
	6.4	37 Kbps	74	150	224	299

2.4.3 Wi-Fi

2.4.3.1 ¿Qué es Wi-Fi?

En palabras sencillas, Wi-Fi es conectividad. En casa, Wi-Fi permite conectarse a un contenido favorito, además permite comunicaciones sobre: teléfonos celulares, computadoras, reproductores multimedia, y otros dispositivos, todo esto sin los molestosos cables. Además cuando el dispositivo está en el movimiento, Wi-Fi permite conectarse a la Internet para desempeñar cualquier actividad cotidiana, con facilidad y rapidez, sin preocuparse por buscar una conexión de red cableada, eso es Wi-Fi.

2.4.3.2 Funcionamiento de la tecnología Wi-Fi

Las redes Wi-Fi utilizan las tecnologías de radio denominada 802.11, para ofrecer acceso seguro, confiable, rápida conectividad inalámbrica (*wireless*). Una red Wi-Fi puede ser utilizar para conectar dispositivos electrónicos entre sí, a la Internet, y redes de cable que utilizan la tecnología *Ethernet*. Las redes Wi-Fi operan en las bandas de radio: 2.4GHz y 5GHz, algunos productos contienen las dos bandas (*dual band*). Proporcionando un desempeño similar a las redes básicas de cable.

Los productos Wi-Fi son fáciles de conectar entre sí. La Alianza Wi-Fi (*Wi-Fi Alliance*) ha otorgado más de 10.000 productos certificados, a los dispositivos que han sido probados en interoperabilidad, y aseguran ser “buenos vecinos” con otros equipos Wi-Fi. Esto significa que no van a interferir con el funcionamiento de otros productos. La interoperabilidad significa que los productos de diferentes compañías funcionen en conjunto de manera compatible, lo que significa que existe una gran variedad de opciones en productos, y se pueden mezclar y combinar productos CERTIFICADOS Wi-Fi (*Wi-Fi CERTIFIED*), con la confianza de que van a trabajar en conjunto. Cuando se compra productos *Wi-Fi CERTIFIED*, se puede estar seguro que han sido probados para funcionar fielmente en una red inalámbrica, y contienen las últimas características de la seguridad.

Dicho de Otra manera, Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente conocida como la *WECA: Wireless Ethernet Compatibility Alliance*), esta organización comercial que adopta, prueba y certifica que los equipos cumplen con los estándares 802.11 de interoperabilidad y seguridad, relacionados a redes inalámbricas de área local.

2.4.3.3 Tecnología Wi-Fi

Hoy en día los productos Wi-Fi puede hacer de todo, desde el envío de correo electrónico hasta envió de *streaming* de video y enlaces internacionales de llamadas de vídeo conferencia, inclusive enlaces a la red de Internet desde un avión que se encuentra a 10.000 pies de altura, o simplemente el enlace en el hogar.

Para el indudable gran desarrollo de Wi-Fi fue necesaria la cooperación de miles de empresas, investigadores e ingenieros para desarrollar productos que funcionen en conjunto de manera compatible sin problemas. A mediados de la década de 1990, un consorcio internacional de expertos en ingeniería de muchas compañías de tecnología, comenzaron a trabajar juntos a través de una organización llamada IEEE (Instituto de Ingenieros Eléctricos y Electrónicos, conocido como "I triple E"), para desarrollar estándares, como por ejemplo estándares para nuevos productos inalámbricos que deben interactuar unos con otros.

- **Banda de Frecuencia**

Los productos Wi-Fi operan sobre las ondas de radio, de la misma manera que un teléfono celular, la puerta del garaje, TV, radio, sistema de navegación GPS, microondas, entre otros. Cada uno de estos diferentes productos operan en un sector específico, o banda de frecuencia, del espectro radioeléctrico. Los productos Wi-Fi operan en las bandas de 2.4 GHz o 5GHz. Estas bandas se denominan de “licencia libre o bandas no licenciadas", esto indica que los usuarios pueden utilizar productos diseñados para estas bandas sin licencia del gobierno, como las que se conceden para las transmisiones de radio o televisión en las bandas licenciadas. Debido a que las bandas de Wi-Fi son de "licencia libre", se vuelve más importante para los fabricantes asegurar que sus productos pasen los estándares de interoperabilidad establecidos por la certificación Wi-Fi. Las pruebas de certificación aseguran que los productos Wi-Fi son buenos vecinos y no interfieren con las señales de otros dispositivos.

2.4.3.4 ¿Qué es 802.11?

Hoy en día los productos Wi-Fi son designados por un sistema decimal *Dewey* (*Dewey Decimal System*), desarrollado por el IEEE para diferenciar entre diversas familias de tecnologías. Los productos Wi-Fi son identificados como 802.11, además son identificados por una letra minúscula que identifica cual tecnología específica esta en operación, como por ejemplo 802.11a.

Hasta la fecha ha habido cuatro generaciones Wi-Fi de productos disponibles, y más estándares se están trabajando para añadir nuevas características y también mejorando el desempeño y seguridad. Cada generación está definida por un conjunto de características que se relacionan con el desempeño, la frecuencia y ancho de banda, como se presenta en la Tabla 2.15. También cada generación promueve mejoras en la seguridad y pueden incluir otras nuevas características que los fabricantes pueden implementar.

Tabla. 2.15. Generaciones Wi-Fi.

Tecnología Wi-Fi	Banda de frecuencia	Ancho de Banda (Bandwidth) o velocidad máxima de datos
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz, 5 GHz, 2.4 ó 5 GHz (seleccionable), o 2.4 y 5 GHz (concurrente)	450 Mbps

Los productos *Wi-Fi CERTIFIED* son probados para asegurar que estos trabajan con generaciones anteriores de productos Wi-Fi, que operan en la misma banda de frecuencia. Por ejemplo, la denominación *Wi-Fi CERTIFIED* 802.11g indica que el producto ha sido certificado para cumplir con los estándares de 802.11g, y operará con dispositivos *Wi-Fi CERTIFIED* en 802.11b o 802.11n (porque trabajan en la banda de frecuencia 2.4 GHz). Los productos *Wi-Fi CERTIFIED* incluyen un logotipo que los identifica, indicando qué características han sido probadas, y que el producto ha cumplido con todos los estándares de la notación, como se presenta en la Figura 2.40.

Figura. 2.40. Logotipo Wi-Fi CERTIFIED.

2.4.3.5 Métodos de seguridad en Wi-Fi.

Un método básico para impedir que usuarios no autorizados ingresen a una red inalámbrica, es suprimir la transmisión (*broadcast*) del SSID (*Service Set IDentifier*) del punto de acceso. A menudo al SSID se le conoce como nombre de la red.

Otro método es el filtrado de MAC, es decir solo se permite el acceso a la red a los equipos con direcciones MAC autorizadas. Esto es lo más recomendable cuando se utilizan los mismos equipos.

En la actualidad existen varias alternativas para garantizar la seguridad en redes Wi-Fi. Habitualmente se utiliza la encriptación de los datos o cifrado de datos, para garantizar la seguridad en estas redes, que se encarga de codificar la información transmitida, estas seguridades ofrecen los equipos inalámbricos. Las encriptaciones inalámbrica más comunes son:

- WEP (*Wired Equivalent Privacy* / Privacidad Equivalente a Cableado)

Permite cifrar la información que se transmite. Proporciona un cifrado en dos niveles de seguridad, los cuales utiliza claves de 64 y 128 bits. En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida. Este tipo de cifrado no está muy recomendado, debido a las altas vulnerabilidades que presenta.

- WPA (*Wi-Fi Protected Access* / Acceso Protegido Wi-Fi)

Ofrece mayor seguridad al viejo protocolo WEP, además ofrece mejoras en generación dinámica de la clave de acceso, es decir WPA permite la autenticación mediante una clave compartida (*PSK, Pre Shared Key*), este proceso es similar al WEP, en el cual requiere introducir la misma clave en los equipos que intervienen en la red.

Básicamente WPA se fundamente en la simplicidad de la distribución de claves de autentificación y en el protocolo de cifrado que utiliza. Normalmente utiliza el protocolo de cifrado *TKIP (Temporal Key Integrity Protocol*), en el cual se utiliza una clave de 128 bits por paquete, lo que significa que genera dinámicamente una nueva clave para cada paquete.

- WPA2 (*Wi-Fi Protected Access 2* - Acceso Protegido Wi-Fi 2)

WPA2 está basada en el estándar 802.11i, es por esta razón que se le conoce a WPA2 como IEEE 802.11i-2004, creado para corregir las vulnerabilidades detectadas en WPA, WPA2 utiliza el algoritmo de cifrado AES (*Advanced Encryption Standard*). Con este algoritmo es posible cumplir con los requerimientos de seguridad, para proteger las redes inalámbricas Wi-Fi.

WPA2 requiere pruebas y certificación por la Alianza Wi-Fi. La certificación se inició en septiembre de 2004, desde 13 de marzo de 2006, la certificación WPA2 es obligatoria para todos los nuevos dispositivos para llevar la marca Wi-Fi.

En WPA2 reemplaza el protocolo de cifrado TKIP por CCMP para proporcionar seguridad adicional. Esto es obligatorio para los dispositivos certificados Wi-Fi desde el año 2006. CCMP, es un mecanismo de encriptación/cifrado basado en AES, el cual es más fuerte que TKIP, comúnmente se denomina AES en lugar de CCMP.

En la práctica, el router o el punto de acceso (*access point*) de un típico usuario domestico, soportan WPA en modo WPA-PSK con encriptación TKIP. Cuando los routers son actualizados, admiten WPA2 en modo WPA-PSK con cifrado CCMP.

2.4.3.6 Voz sobre Wi-Fi

Voz sobre Wi-Fi permite a los usuarios hacer y recibir llamadas de voz a través de las redes Wi-Fi. Esto está ganando rápidamente popularidad como la voz sobre IP (VoIP), que goza de una popularidad cada vez mayor, gracias al surgimiento de nuevos dispositivos de voz, como teléfonos de modo dual con tecnología celular y Wi-Fi, con una amplia disponibilidad. En los últimos años, los fabricantes de dispositivos Wi-Fi han ampliado y mejorado la funcionalidad de voz, para satisfacer la demanda de los usuarios y para acelerar el crecimiento del mercado de voz sobre Wi-Fi.

En la actualidad existe una gran variedad y cantidad de dispositivos celulares solo con tecnología Wi-Fi y modo dual con tecnología celular y Wi-Fi, los cuales son productos *Wi-Fi CERTIFIED*, basados en Wi-Fi interoperabilidad y seguridad. También existen muchos otros dispositivos *Wi-Fi CERTIFIED* que soportan aplicaciones de voz, como las computadoras portátiles. Adicionalmente, los programas de certificación para WMM[16] (*Wi-Fi Multimedia*) y WMM *Power Save* (Ahorro de energía), han introducido características avanzadas en Calidad de Servicio (QoS), eso ha mejorado la capacidad de voz de redes Wi-Fi.

La Alianza Wi-Fi (*Wi-Fi Alliance*) se encuentra garantizando buena calidad de voz en equipos certificados (*Wi-Fi CERTIFIED*), mediante el programa de certificación *Wi-Fi CERTIFIED Voice-Personal*.

Este programa dirige los requisitos específicos de las aplicaciones de voz en entornos domésticos y pequeñas oficinas, que requieren los dispositivos terminales y los puntos de acceso, para cumplir con los niveles de desempeño adecuados, referentes a perdida de paquetes, latencia, Jitter, entre otros, para garantizar una buena calidad de voz.

16 WMM permite a las redes Wi-Fi priorizar el tráfico generado por las diferentes aplicaciones.

Las aplicaciones de voz en redes Wi-Fi son atractivas para muchos usuarios en entornos domésticos y pequeñas oficinas, por las siguientes razones:

- Dispositivos con capacidad de voz

La tecnología Wi-Fi ofrece a los usuarios una amplia gama de dispositivos que soportan aplicaciones de voz, lo que incluye, pero no está limitado a los teléfonos móviles. Las computadoras portátiles han sido los primeros dispositivos en soportar voz sobre Wi-Fi, pero los teléfonos celulares solo con tecnología Wi-Fi y modo dual celular/Wi-Fi, están creciendo rápidamente, ofreciendo a los usuarios de VoIP sin cables.

- Conveniencia.

Voz sobre Wi-Fi opera dentro de una red accesible y de gran confianza que los usuarios saben cómo manejar. Los equipos Wi-Fi son fáciles de instalar y puede ser utilizado por diversos dispositivos en toda la casa u oficina (por ejemplo, teléfonos, computadoras portátiles, consolas de videojuegos, impresoras, entre otros.)

- Buena calidad de voz.

La certificación *Wi-Fi CERTIFIED Voice-Personal*, comprueba que los dispositivos y puntos de acceso entreguen buena calidad de voz dentro de una red Wi-Fi, que es compartida por varios dispositivos (por ejemplo, teléfonos, computadoras portátiles, consolas de juegos e impresoras).

- Ahorro de costos.

Voz sobre Wi-Fi extiende la opción de servicios disponibles para los usuarios a través de su actual o un nuevo proveedor de servicio, lo cual puede resultar un ahorro en costos.

Voz sobre Wi-Fi es una de las áreas más interesantes de crecimiento en la industria Wi-Fi. Los usuarios están dispuestos a utilizar sus dispositivos Wi-Fi certificados, para aplicaciones de voz y para explorar nuevos servicios que les traen funcionalidad y conveniencia. La propuesta de valor es convincente: Voz sobre Wi-Fi proporciona a los usuarios un acceso cómodo y sencillo a las aplicaciones móviles de voz, disponible a través de su conexión a Internet de banda ancha, por medio de una gran variedad de dispositivos terminales.

CAPÍTULO III

PROTOCOLO DE INICIO DE SESIONES (SIP)

3.1 INTRODUCCIÓN

Hay muchas aplicaciones de Internet que requieren la creación y gestión de sesiones, donde una sesión es considera como un intercambio de datos entre una asociación de participantes. La implementación de estas aplicaciones se complica por las varias características de los participantes, por ejemplo los usuarios o entidades finales pueden moverse entre los extremos o puntos finales, también los usuarios pueden ser direccionables por varios nombres, asimismo los usuarios pueden comunicarse en varios medios diferentes en ocasiones simultáneamente.

Numerosos protocolos han sido diseñados para llevar los distintos tipos de datos en tiempo real en sesiones multimedia, datos como voz, video, mensajes de texto, entre otros. El Protocolo de Inicio de Sesiones (SIP) trabaja en conjunto con estos protocolos para permitir que las entidades finales (llamados agentes de usuario) localicen su ubicación el uno al otro, y además se ponen de acuerdo sobre las características de las sesiones, y parámetros de capacidades de negociación que les gustaría compartir entre los participantes de la sesión.

Para localizar la ubicación de los posibles participantes de la sesión, y para otras funciones, SIP permite la creación de una infraestructura de hosts de red (llamados servidores proxy) para que los agentes de usuario puedan enviar los registros, las invitaciones de sesiones, y otras solicitudes.

SIP es una herramienta ágil de propósito general, para establecer o crear, modificar y finalizar sesiones que trabaja independientemente de los fundamentales protocolos de transporte y sin dependencia sobre el tipo de sesión que se está estableciendo.

3.2 RESUMEN DE FUNCIONALIDAD DEL PROTOCOLO SIP

El Protocolo de Inicio de Sesiones (SIP es el acrónimo de *Session Initiation Protocol*) es un estándar del IETF para establecer o iniciar , modificar, y finalizar sesiones multimedia (conferencias), tales como las llamadas de telefonía sobre internet, además estas sesiones pueden ser utilizadas para audio, video, mensajería instantánea, o para sesiones de comunicación con datos en tiempo real. SIP también puede invitar a participantes a una sesión ya establecida como una conferencia *multicast* (multidifusión o grupo). SIP soporta transparentemente la asignación de nombre y servicios de redirección, por ejemplo soporta movilidad de los usuarios, los usuarios pueden mantener un único identificador, independientemente de su ubicación en la red.

SIP soporta 5 facetas para el establecimiento y terminación de comunicaciones multimedia:

- ✓ Localización del usuario.
- ✓ Disponibilidad del usuario.
- ✓ Capacidades del usuario.
- ✓ Configuración de la sesión.
- ✓ Gestión de la sesión.

Para la construcción de un sistema que utiliza al protocolo SIP, requiere que los implementadores lean las bases de las especificaciones de SIP, y los protocolos que intervienen en una aplicación particular. Por ejemplo, el uso de SIP para mensajería instantánea se define por separado de las especificaciones de SIP, para el uso de SIP en Voz sobre IP requiere que el implementador esté familiarizado con SDP, los cuales están definidos en una RFC totalmente independiente. El diseño “modular” es considerado como la fortaleza del protocolo SIP.

El alcance del protocolo SIP es relativamente amplio, incluyendo el establecimiento de prácticamente cualquier tipo de sesión entre dos partes. SIP también es totalmente independiente del mecanismo de transporte, aunque TCP y UDP son utilizados casi exclusivamente. SIP fue inicialmente publicado como un proyecto orientado a la integración y servicios de internet por el IETF en 1996, con su primer RFC en 1999, las especificaciones más reciente de SIP están publicadas en el RFC 3261.

Este protocolo posee mayor flexibilidad para agregar nuevas funciones y su implementación es relativamente más simple.

El protocolo SIP es un protocolo de señalización para VoIP, que se encuentra dentro del *Stack* de protocolos en la capa aplicación del modelo TCP/IP. Este protocolo guarda una estrecha relación con el protocolo SDP, como se presenta en la Figura 3.1.

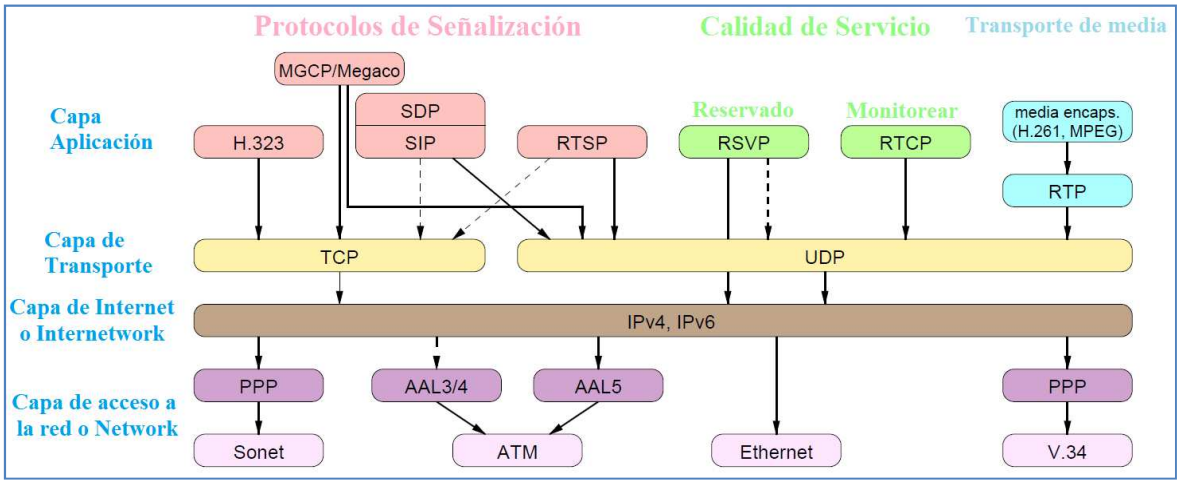

Figura. 3.1. SIP protocolo de señalización dentro de la capa aplicación del modelo TCP/IP.

SIP es un protocolo de señalización de la capa aplicación, para iniciar, gestionar o modificar, y finalizar sesiones comunicación interactiva, multimedia (voz, video) entre usuarios, a través de las redes de datos o redes de paquetes. SIP utiliza una sintaxis similar a los protocolos de internet como HTTP y SMTP, SIP es un texto codificado y altamente extensible, SIP puede trabajar en características y servicios como: los servicios de control de llamadas, movilidad, interoperabilidad con los sistemas de telefonía existentes.

Principales funciones de SIP:

- ✓ Establecer, modificar o gestionar, y finalizar sesiones entre dos o más integrantes.
- ✓ Realizar la registración y localización de integrantes.
- ✓ Gestionar del conjunto de integrantes y entidades lógicas SIP que componen el sistema.
- ✓ Describe las características de las sesiones, y parámetros de capacidades de negociación (dentro del mensaje SDP).

Principales características de SIP:

- ✓ Se basa codificación en texto y altamente extensible.
- ✓ Sintaxis similar a los protocolos HTTP y SMTP.
- ✓ Para identificar una entidad SIP utiliza los URIs (esquemas: sip, sips, tel).
- ✓ Mensajes básicos de SIP: INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, entre otros.
- ✓ Los mensajes se utilizan para: iniciar, gestionar, y finalizar sesiones (llamadas).
- ✓ Dentro del mensaje SDP contiene parámetros multimedia.
- ✓ Mensajes de respuesta similares a HTTP (por ejemplo el mensaje 200 OK).
- ✓ La localización se establece mediante el DNS[17].

Principales aplicaciones de SIP:

- ✓ Establecimiento de llamadas de Voz sobre IP.
- ✓ Establecimiento de conferencias multimedia.
- ✓ Notificación de eventos (*Suscribe, Notify*).
- ✓ Protocolo de señalización.

17 DNS es el acrónimo de Domain Name System (en español sistema de nombres de dominio), su principal función es la resolución de nombres de dominio. Usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

SIP trabaja conjuntamente con otros protocolos, como: SDP y RTP/RTCP, donde SDP describe las características de las sesiones, y parámetros de capacidades de negociación entre los integrantes de la sesión, por otro lado RTP/RTCP se encarga de transportar los media streams o datos multimedia, propiamente dicho transporta el audio o video.

El protocolo SIP está orientado a conexiones *peer to peer*, dos usuarios pueden establecer una sesión entre ellos, mediante dos canales de comunicación, como se presenta en la Figura 3.2. Los dos canales de comunicación son los siguientes:

- Señalización SIP, para establecer, modificar, y finalizar sesiones entre dos o más integrantes.
  (Puerto UDP 5060).

- Transporte y control de media, RTP lleva los media streams, RTCP se encarga de monitorear estadísticas de transmisión y calidad de servicio (QoS).
  (Puerto UDP 10000-20000 generalmente).

Figura. 3.2. Esquema de funcionamiento del protocolo SIP, orientado a conexiones *peer to peer*.

La lógica se encuentra guardada en los dispositivos terminales o finales, exceptuando el ruteo de mensajes SIP, la ventaja de este protocolo es su gran escalabilidad y modular, porque los servidores no son saturados con el envió de menajes SIP.

Cada paquete puede viajar por un camino completamente diferente, los paquetes de señalización viajan por un camino diferente que los paquetes que transportan los media streams. Tanto la señalización, como el transporte de media, asimismo como otras aplicaciones (FTP, web, email, entre otros), parecen semejantes a nivel de la capa de transporte, y comparten el mismo destino, como se presenta en la Figura 3.3.

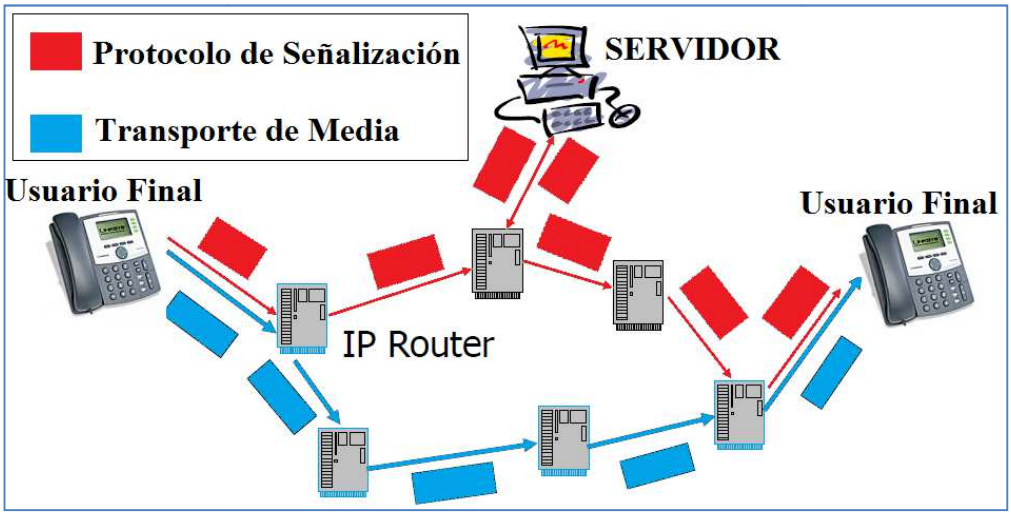

Figura. 3.3. Paquetes de señalización viajan por diferente camino.

3.2.1 Direccionamiento SIP

Para identifica a una entidad SIP, se realiza de la misma forma para identificar a una cuenta de correo electrónico, esta forma es mediante URI (*Uniform Resource Identifier* o identificador uniforme de recurso). Se puede clasificar un URI como localizador URL (*Uniform Resource Locator*) o como nombres URN (*Uniform Resource Name*) o como ambos, como se presenta en la Figura 3.4.

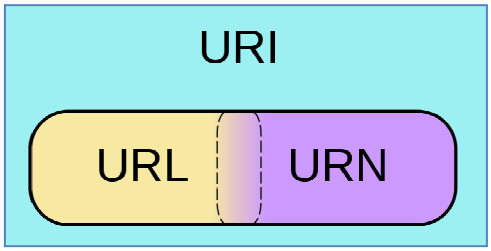

Figura. 3.4. Esquema URI.

Un SIP URI es el esquema de *Direccionamiento SIP* para llamar a otra persona vía SIP. Dicho de otra manera, un SIP URI es un número telefónico SIP de un usuario. El SIP URI es similar a una dirección de correo electrónico y se describe en el siguiente formato:

sip: [userinfo] hostport [parameters]

Donde:

- *userinfo*: contiene información referente al usuario, seguido del carácter "@".
- hostport: contiene un nombre de dominio o una dirección IP, adicionalmente, puede incluir un número de puerto.
- *parameters*: contiene parámetros adicionales. Que se indican después del carácter ";".

Dicho de otra manera:

sip:x@y:puerto

Donde:

- x es el nombre del usuario o numero de usuario SIP.
- y es el equipo (Servidor SIP) o dominio o IP.

El URL puede ser una combinación de FQDNs[18] o E.164[19] números o incluso ambos.

Ejemplos:

- ✓ Soporta FQDNs (nombres) utilizando sip: URLs
  "Victor Lopez" sip:victorlopez@domain.com

- ✓ Soporta para direcciones E.164 (números)
  Aplicación:
  - Servidor SIP: a2b1.nuestroserver.com
  - Usuario SIP: 0466369998

  El SIP URI de la aplicación es el siguiente:
  sip:0466369998@a2b1.nuestroserver.com

18 FQDN (Fully Qualified Domain Name) es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.

19 E.164 es una recomendación ITU-T que define el plan de numeración pública internacional de telecomunicaciones utilizado en la PSTN y en algunas redes de datos, También define el formato de los números telefónicos.

- ✓ Soporta para direcciones mezcladas
  sip:10543868451@10.0.0.5; user=phonesip:marksmith@10.1.1.1

- ✓ Soporte para direcciones E.164 utilizando tel: URLs
  tel:11234567890

Cuando se desea realizar una llamada mediante SIP, se puede tener un nombre o un número, sin embargo el nombre se debe de traducir a un número que está en un formato E.164. Cuando un usuario se registra en el servidor con un nombre, en realidad es un número, es decir el servidor realiza una traducción, prácticamente el formato que se maneja es el E.164.

A continuación se presenta en la Tabla 3.1 los esquemas URI, con su respectiva función, y la RFC que define sus especificaciones.

Tabla. 3.1. Esquemas URI.

Esquema	USO	RFC
sip: sips:	Direcciones SIP (segura y no segura).	3261
tel:	Números de teléfono.	3999
pres:	Presencia de recurso.	3861
im:	Recurso de mensajería instantánea.	3861
http:	Protocolo de transporte de Hipertexto para páginas web.	2616
xmpp:	Jabber IM y presencia de URIs.	
H323:H323	URL H323.	3508

3.3 ENTIDADES SIP

En la arquitectura SIP existen dos componentes esenciales, los *Agentes de Usuario y* los *Servidores* (User Agente UA y Server). Cada entidad tiene funciones específicas y participa en la comunicación SIP como *cliente* (inicia las solicitudes), o como *servidor* (responde a las solicitudes) estos pueden ser *Proxies*, *Redirect*, *Registrar*, o realizar ambas cosas, como se presenta en la Figura 3.5.

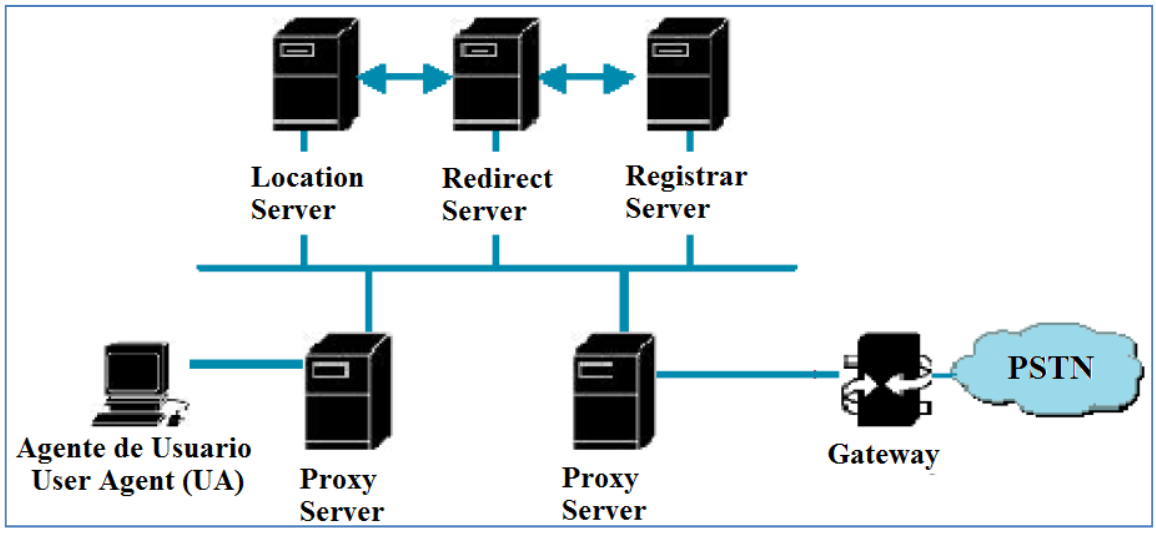

Figura. 3.5. Arquitectura SIP dos componentes esenciales Agentes de Usuario y Servidores.

Una red SIP está compuesta principalmente por cinco entidades lógicas SIP.

Las entidades lógicas SIP son:

- *User Agent* (Agente de usuario)
- *Proxy server* (Servidor proxy)
- *Redirect server* (Servidor de redirección)
- *Registrar server* (Servidor de registro)
- *Back to Back User Agent* (B2BUA)

En una arquitectura funcional y física, un “dispositivo físico” puede tener funciones uno o más entidades lógicas SIP. Por ejemplo, un servidor de red puede trabajar como *Server Proxy* y también puede funcionar como *Registrar* al mismo tiempo, como se presenta en la Figura 3.6.

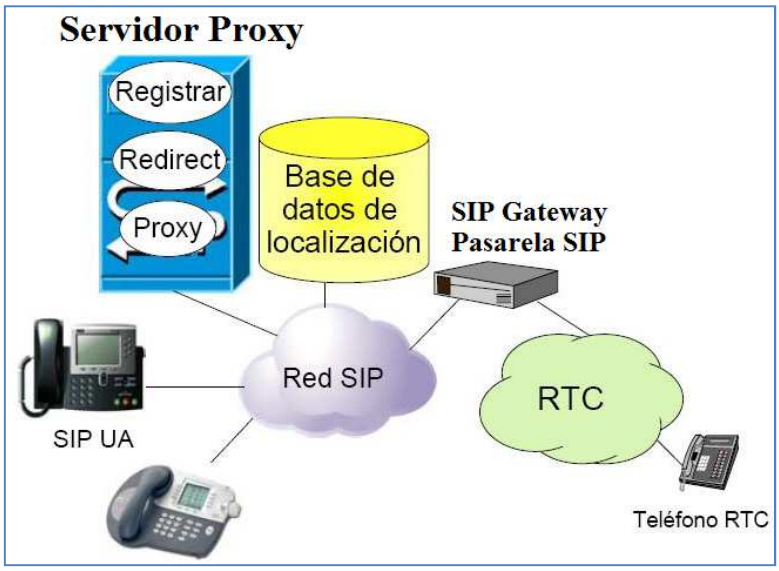

Figura. 3.6. Arquitectura SIP funcional y física.

3.3.1 User Agent (Agente de usuario)

En SIP, los Agentes de Usuarios (UA: *User Agent*) son entidades finales, los Agentes de Usuario inician y terminan sesiones mediante el intercambio de mensajes de solicitud y respuesta.

En la RFC 3261[20] se define al Agente de Usuario como una aplicación que posee dos elementos fundamentales, un es el Agente de Usuario Cliente (UAC: *User Agent Client*) y el otro es el Agente de Usuario Servidor (UAS: *User Agent Server*), estas entidades se localizan en un *Softphone*, teléfonos celulares SIP, terminales IP, *Hard-IP phones*, entre otros. UAC y UAS se definen a continuación: [4]

20Se abrevia como RFC de las palabras en Inglés: Request for Comments o "Petición De Comentarios" en español, cada RFC es un documento cuyo contenido es una propuesta oficial sobre algún tema especifico de la red Internet, en la cual ese explica con todo detalle. Cada RFC tiene un título y un número asignado, que no puede repetirse ni eliminarse aunque el documento quede obsoleto.
RFC Request for Comments: 3261, SIP: Session Initiation Protocol

- El Agente de Usuario Cliente (UAC) es una aplicación en la cual el cliente inicia o envía solicitudes SIP hacia la red IP, y recibe respuestas a estas solicitudes.
- El Agente de Usuario Servidor (UAS) es una aplicación que al momento de recibir una solicitud SIP de la red IP, realiza el contacto con el usuario o cliente y devuelve la respuesta a la solicitud, como se aprecia en la Figura 3.7.

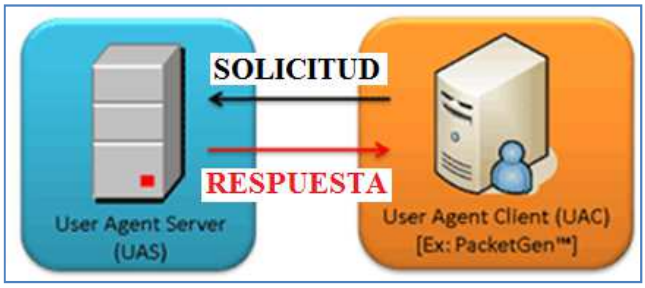

Figura. 3.7. UAS recibe mensajes desde UAC.

Los procesos que realizan los UAC y UAS fundamentalmente dependen de dos factores: el primero es verificar que el mensaje (solicitud/respuesta) forma parte de un dialogo, y depende la solicitud realiza un método apropiado.

Los diálogos se especifican con todo detalle en la sección 12 del RFC 3261, lo que significa una relación punto a punto entre los Agentes de Usuario (UA), estableciendo mediante mensajes del método SIP como por ejemplo el mensaje INVITE, como se aprecia en la Figura 3.8.

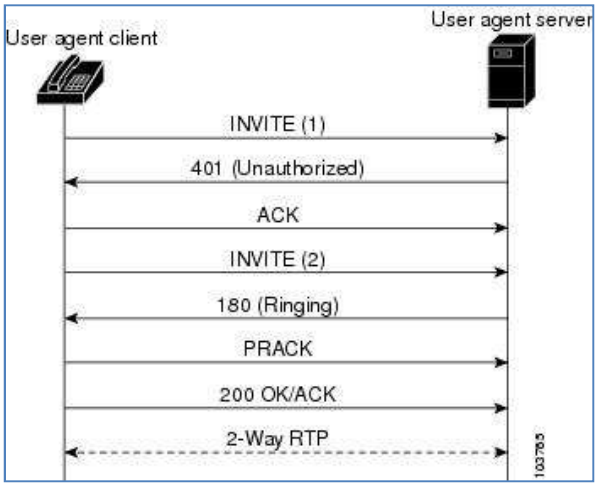

Figura. 3.8. Flujo de llamada desde UAC hacia UAS con mensaje INVITE.

Existen varios dispositivos que están en la capacidad de tener funciones de Agente de Usuario (UA) como por ejemplo: teléfonos IP, computadoras con *Softphone*, sistemas automáticos de mensajería, pasarelas telefónicas entre otros, estos dispositivos en el punto de red que estén instalados, poseen cierta inteligencia para interaccionar con el usuario, dicho de otro modo tienen capacidad de proceso para saber actuar como UAC y UAS.

Hay que tener presente que para poder utilizar un terminal IP y que este pueda realizar comunicaciones, se debe hacer una configurarlo previa, con los parámetros que indica el operador del servicio.

- **Softphones**

Los *Softphones* son otro tipo de terminal de telefonía IP plasmados en un software, el cual debe ser instalado en nuestro ordenador personal, en un PDA[21], asimismo en un teléfono celular denominados *smartphone*[22], el cual debe tener los recursos informáticos necesarios para funcionar. Dicho de Otra manera un *Softphone* no es otra cosa que un software que emula las funciones de un teléfono físico tradicional, que permite marcar, transferir o recibir llamadas, desde nuestro computador personal o portátil.

Su apariencia o interfaz grafica es muy amigable para el usuario, porque se parece a un teléfono regular, también a programas de mensajería, varios de estos Softphone están exclusivamente diseñados solo para telefonía IP, otros incluyen telefonía IP, videoconferencia y mensajería, además de trabajar con el protocolo SIP se pueden configurar con diferentes protocolos.

21 Se abrevia como un PDA del Inglés personal digital assistant (asistente digital personal), también denominado ordenador de bolsillo o computadora de mano.

22 Smartphone en Inglés (teléfono inteligente) es un término comercial para mencionar a un teléfono móvil que ofrece más funciones que un teléfono celular común.

A continuación se presenta en la Figura 3.9 imágenes de un Softphones X-Lite y un teléfono celular con aplicación SIP.

Figura. 3.9. Softphone X-Lite para PC y teléfono celular con aplicación SIP.

- **Terminales IP**

Su apariencia es como un teléfono convencional muy profesional, dispone con una pantalla o display juntamente con teclas de funciones, se aprecia en la Figura 3.10, estos dispositivos están en la capacidad de tener funciones de Agente de Usuario (UA), por lo tanto exige que tenga instalado un pequeño procesador, el cual es usual encontrar que funcione en alguna versión de Linux, además existe un grupo de dispositivos terminales que poseen un servidor web, para realizar configuraciones remotas ingresando a páginas web.

Figura. 3.10. Ejemplos de terminales IP.

- **Adaptadores ATA**

Un adaptador ATA es un dispositivo que transforma la telefonía analógica convencional en telefonía IP, este dispositivo permite utilizar el teléfono convencional para realizar llamadas a través de una red de datos IP. Estos dispositivos tienen funciones de Agente de Usuario (UA) para la señalización SIP, además disponen de un circuito electrónico, para que la información pueda ser transmitida a través de la red de datos, convirtiendo la información analógica del teléfono en digital utilizando un códec.

Los circuitos electrónicos de los adaptadores ATA son muy similares a la de los teléfonos IP, porque son instalados con un pequeño procesador, asimismo cuentan con un sistema operativo, y un servidor web para realizar configuraciones remotas, es muy usual encontrar que estos dispositivos están pre configurados por el operador de telefonía IP, a continuación se presenta en la Figura 3.11 como ejemplo un adaptador ATA *Linksys* con sus respectivos puertos.

Figura. 3.11. Adaptador ATA Linksys.

Por lo tanto se presenta en la Figura 3.12 un esquema básico de instalación.

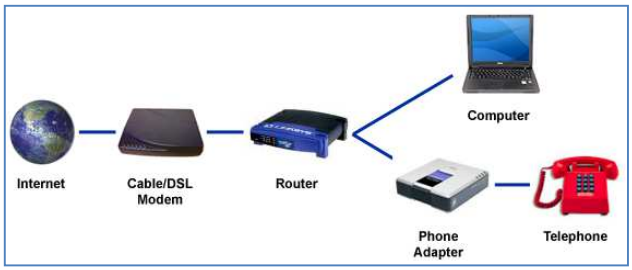

Figura. 3.12. Esquema básico de instalación.

3.3.2 Proxy Server (Servidor proxy)

La palabra *Proxy* posee un origen jurídico, en Inglés significa “poder de representación, apoderado o representante para que actué en mi nombre” [9], es por esto que un *Proxy Server* es una entidad intermediaria, dicho en palabras sencillas se puede decir que un *Proxy* es un intermediario que nos realiza un mandado.

Un *Proxy* está en capacidad de actuar como servidor y cliente, con el fin de generar solicitudes en nombre de otros clientes, es decir a nombre de un UA, estas solicitudes se dirigen hacia otro UA u otro *Proxy*. Dicho de otra manera un *Proxy Server* recibe las solicitudes SIP, de un UA (u otro *Proxy*) como si fuese un servidor, y devuelve una respuesta. En muchas ocasiones un *Proxy* tiene que consultar a otros *Proxies*, en este caso actúa como cliente (frente a otros *Proxies*) reenviando la solicitud.

Los *Proxy Server* también son utilizados para funciones de enrutamiento, esta es su principal tarea, es decir se encarga de encaminar las solicitudes o propiamente dicho las invitaciones de sesión, hasta llegar al UA llamado o destino. Generalmente una invitación de sesión (solicitud), atraviesa por varios *Proxies Servers* hasta llegar a aquel que conozca la localización precisa del UA destino, como se presenta en la Figura 3.13 [10]. Los *Proxies* también son útiles para aplicar cierto tipo de control, como por ejemplo, verifica que un usuario está autorizado para hacer una llamada,

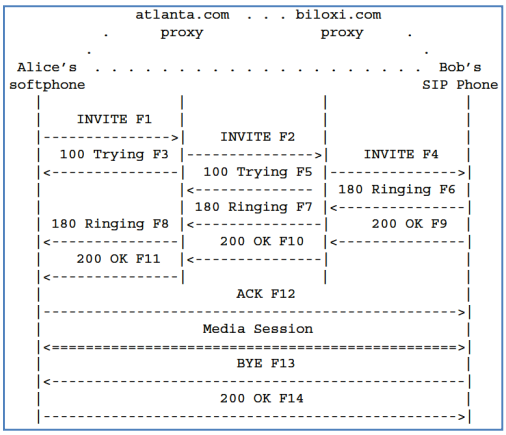

Figura. 3.13. SIP proxy server.

Existen dos tipos básicos de *SIP Proxy Server*: *stateless* (sin memoria) y *stateful* (con memoria). El *stateless proxy* no mantiene un estado de las transacciones cuando se están procesando las solicitudes, simplemente reenvían los mensajes SIP.

El *stateful proxy* si mantiene un estado de las transacciones cuando se están procesando las solicitudes, hasta que la transacción finalice, además está en la capacidad de enviar un mismo mensaje SIP con destino a dos UA o *Proxies* diferentes, dicho en otras palabras, divide una solicitud en varias a esto se denomina *forking*, con el propósito de optimizar la localización de un usuario específico, es decir se realiza una localización simultánea o en paralelo, como se presenta en la Figura 3.14.

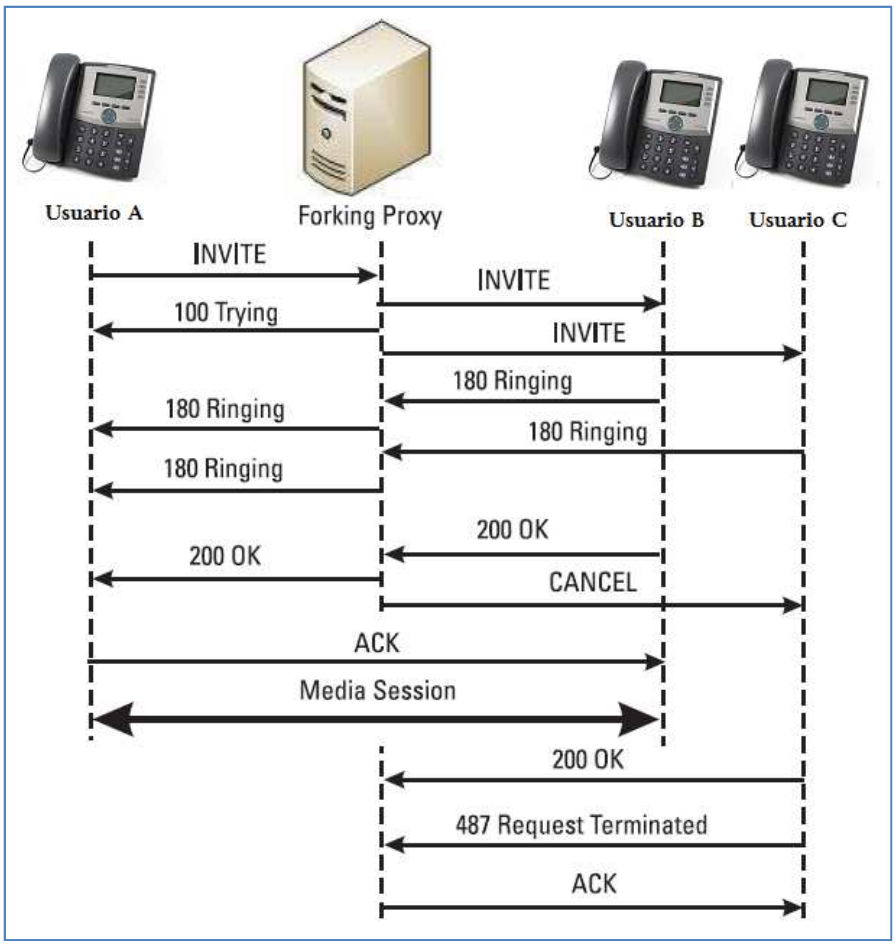

Figura. 3.14. Funcionamiento del forking proxy.

3.3.3 Redirect Server (Servidor de redirección)

Un servidor de redirección es un agente de usuario servidor (UAS), que genera respuestas a las solicitudes que recibe, mediante mensajes con código 3xx, con la dirección del contacto, dirigidas al cliente. Un servidor de redirección tiene la característica de responder a las solicitudes, pero no puede reenviar solicitudes.

Cuando un servidor de redirección recibe una solicitud (mensaje *INVITE sip:B@sipserver.net*) de parte del cliente (usuario A), el servidor de redirección realiza la búsqueda en la base de datos o un servicio de ubicación con información de localización, para saber la localización del usuario al que se desea llamar (usuario B), creada por *Registrar Server*. Esta información de localización es enviada al cliente (usuario A) mediante un mensaje con código 3xx (*302 Moved Temprary*, *Contact: sip:B@sipserver.org*), a continuación el cliente (usuario A) extrae la información y responde con un mensaje *ACK* al servidor de redirección, posteriormente el cliente envía una nueva solicitud (mensaje *INVITE sip:B@sipserver.org*) directamente al resultado del la búsqueda (usuario B), como se presenta en la Figura 3.15.

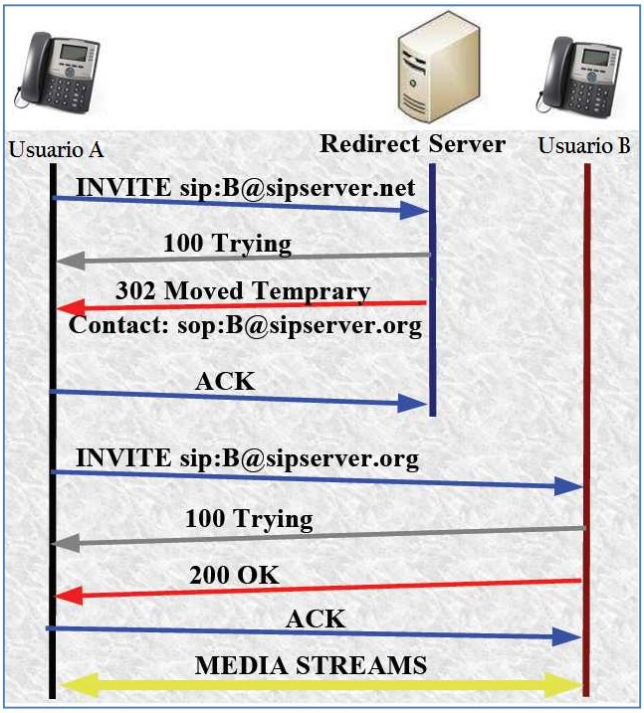

Figura. 3.15. Funcionamiento del servidor de redirección.

3.3.4 Registrar Server (Servidor de registro)

Un servidor de registro es aquel que recibe solicitudes (mensaje REGISTER), y coloca o actualiza la información que recibe de esas solicitudes dentro una base de datos de ubicación o un servicio de ubicación o localización, dicho de otra manera, estos servidores de registro son bases de datos que contienen la ubicación de todos los agentes de usuario (UA), que se encuentran dentro de un determinado dominio. En mensajería SIP, estos servidores recuperan y envían direcciones IP de los participantes, asimismo envían otra información pertinente al servidor *proxy*. El servidor de registro usualmente es una entidad lógica que se encuentra junto al servidor *proxy*. Al servidor de registro en Inglés se lo denomina *SIP Registrar*, y su función se basa en asociar una SIP URI con una o varias direcciones IP, que comúnmente son del tipo *sip:*, sin embargo también son del tipo tel:, es posible que se asocie una SIP URI a varias direcciones IP, (por ejemplo cuando existen routers intermedios) en este caso, cuando se realice una llamada a este SIP URI sonarán las direcciones IP asociadas simultáneamente.

En el momento que un usuario se conecta a la red, y ejecuta su *Softphone* en su ordenador, o enciendo su teléfono IP, entre otros agentes de usuario, estos UA envían mensaje *REGISTER*, hacia el llamado *SIP Registrar* con el propósito de que éste conozca su ubicación. El *SIP Registrar* atiende estos mensajes (*REGISTER*), inmediatamente autentifica y valida la cuenta del usuario en una base de datos, que puede ser interna o externa, realizando un registro de la localización actual del usuario, como se presenta en la Figura 3.16.

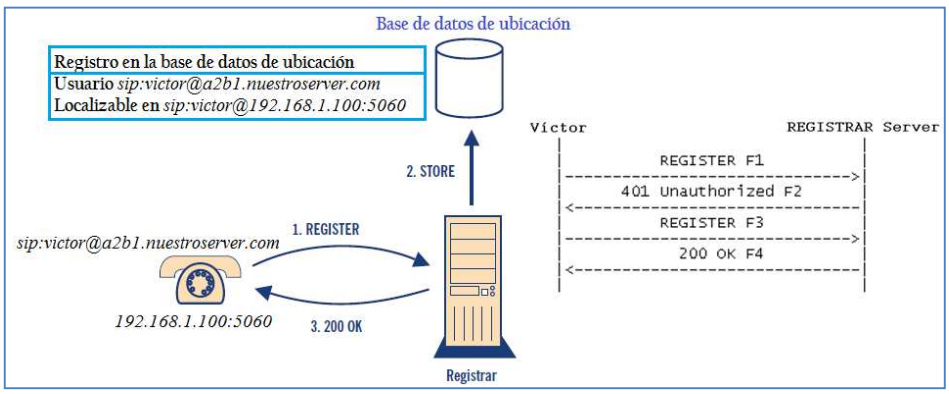

Figura. 3.16. Funcionamiento del servidor de registro (Registrar).

3.3.5 SIP Gateway

Un *gateway* es el responsable de interconectar la red de telefonía IP con otros tipos de redes. El *gateway* realiza la traducción entre diferentes formatos de transmisión y procedimientos de comunicación, como la señalización, paquetes multimedia, entre otros.

Un *Gateway SIP* es una entidad que puede realizar la unión o es la interfaz entre SIP y otro protocolo, como se presenta en la Figura 3.17, por ejemplo el *gateway SIP* puede conectar una red basada en SIP con la red H.323, transformando la señalización SIP en señalización H.323, en este proceso los paquetes multimedia no finalizan en el *gateway SIP*, estos paquetes están permitidos traspasar el *gateway SIP* directamente a la red H.323, porque se encuentran en el mismo tipo de red (red de datos IP), relacionado con la conmutación de paquetes.

El *gateway SIP* también puede conectarse con la PSTN, asimismo con la RDSI (Red Digital de Servicios Integrados o en Inglés ISDN), en este proceso la señalización y los paquetes multimedia finalizan en el gateway SIP, para ser transformados, porque son redes que presentan distinta tecnología, relacionado con la conmutación de circuitos.

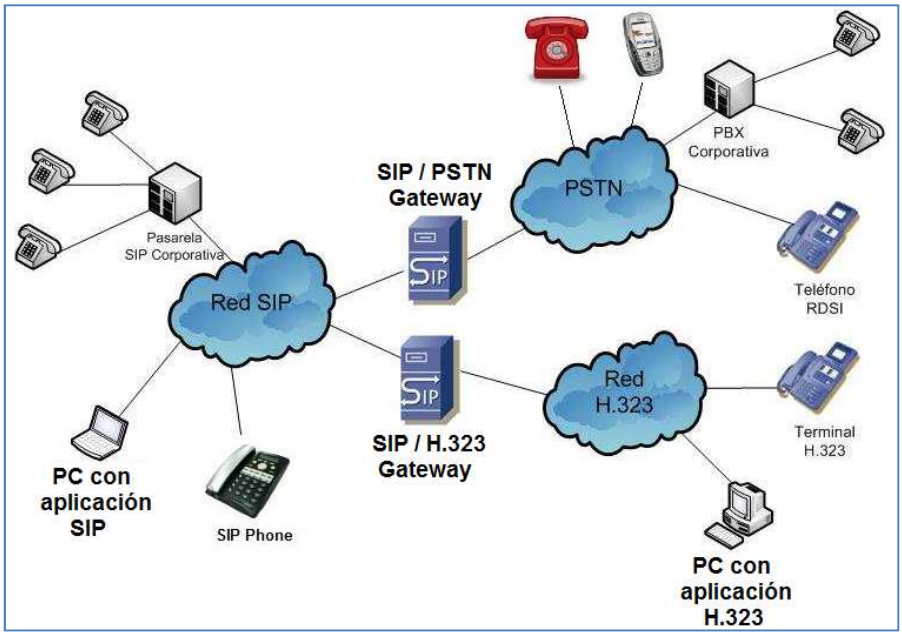

Figura. 3.17. SIP Gateway.

3.4 SIP BACK TO BACK USER AGENT (B2BUA)

El Back to Back User Agent (B2BUA) es una entidad lógica en aplicaciones SIP, dicho en otras palabras B2BUA es un elemento o componente lógico del protocolo SIP, para el control de llamadas entre usuarios SIP.

El B2BUA opera entre los dos puntos extremos de una llamada telefónica o entre una sesión de comunicación, y divide el canal de comunicación en dos sesiones, es decir negocia toda la señalización SIP entre los dos puntos extremos de la llamada, desde el establecimiento hasta la finalización de la llamada, es decir el B2BUA está involucrado en el establecimiento, administración y finalización de la llamada.

El B2BUA es utilizado típicamente como un servidor de aplicaciones SIP, que proporciona una mayor funcionalidad, mediante el manejo de toda la señalización SIP, de la llamada como también entre las entidades que participan, permitiendo realizar un seguimiento desde el establecimiento hasta la finalización de la llamada.

A diferencia de un servidor *Proxy* SIP, en que este solo gestiona el estado de una llamada, en cambio el B2BUA mantiene el estado completo de las llamadas y participa en todas las solicitudes de la llamada. Manteniendo las llamadas está en la capacidad de conseguir información en determinados escenarios como por ejemplo la exacta contabilidad de la llamada, prepago y facturación, re direccionamiento de las llamadas, entre otros.

Como todos los mensajes de control para cada flujo de llamada a través de B2BUA, el proveedor de servicio VoIP puede llevar a cabo funciones de valor agregado disponible durante la llamada.

El B2BUA puede proporcionar las siguientes funciones:

- Gestión o administración de llamadas (facturación, desconexión automática de llamadas, transferencia de llamadas, etc).
- Grabación de la comunicación.
- Interconexión de red (adaptación de protocolos).
- Ocultar información de la red entre los agentes de usuario (direcciones privadas, topología de red, etc).
- Transcodificación, es decir traduce codecs entre los puntos extremos de la llamada, permitiendo que un agente de usuario trabaje con un codec, y en el otro extremo el agente de usuario trabaje con un codec diferente.

El IETF estándar (RFC 3261) define al *Back to Back User Agent (B2BUA)* como una entidad lógica, que recibe una solicitud y la procesa actuando como si fuese un agente de usuario servidor (UAS), además determina como debe ser respondida la solicitud. También tiene la capacidad de actuar como un agente de usuario cliente (UAC), es decir genera mensajes de solicitud.

Por lo tanto en el segmento que origina la llamada, el B2BUA actúa como un Agente de Usuario Servidor (UAS), y procesa la solicitud como un Agente de Usuario Cliente (UAC) para el destinatario final, como se presenta en la Figura 3.18. Es por tal razón que se podría traducir *Back to Back User Agent* como “un agente de usuario inmediatamente después de otro” o “un agente de usuario tras otro”

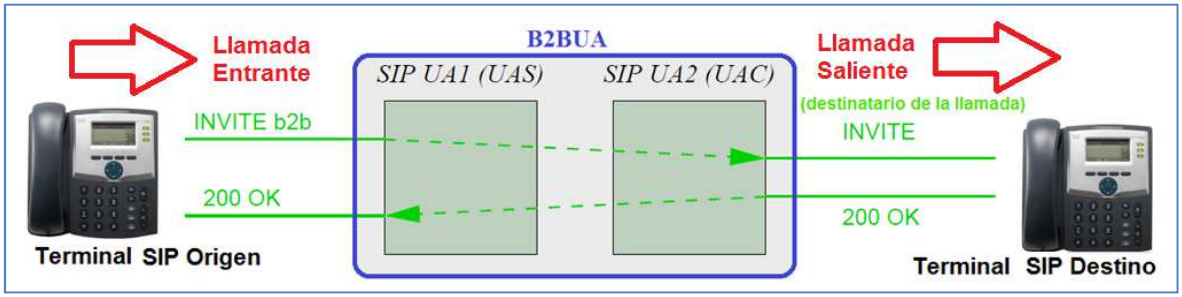

Figura. 3.18. Esquema de un B2BUA.

3.4.1 Arquitectura del B2BUA

Un B2BUA actúa como un agente de usuario (UA) entre los extremos de una llamada SIP. Estos UA son los responsables del manejo de toda la señalización SIP entre los dos extremos de la llamada, empezando desde el establecimiento hasta la finalización de la llamada. Estos agentes permanecen durante todo el transcurso o proceso de la llamada. Un B2BUA se compone lógicamente por dos Agentes de Usuario, los cuales pueden comportarse como UA Servidor o UA Cliente, además estos Agentes de Usuario están enlazados a través de algún tipo de lógica, como se presenta en la Figura 3.19.

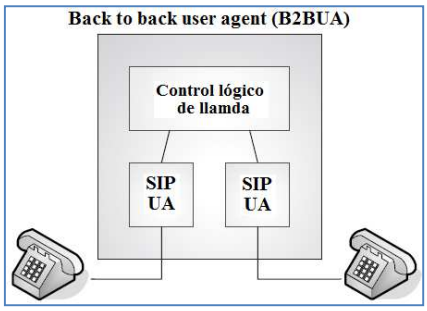

Figura. 3.19. Arquitectura del B2BUA con sus principales componentes.

El B2BUA contiene principalmente los siguientes tres componentes lógicos, como se ilustra en la Figura 3.20.

1. SIP User Agent SERVIDOR.
2. Control lógico de llamada.
3. SIP User Agent CLIENTE.

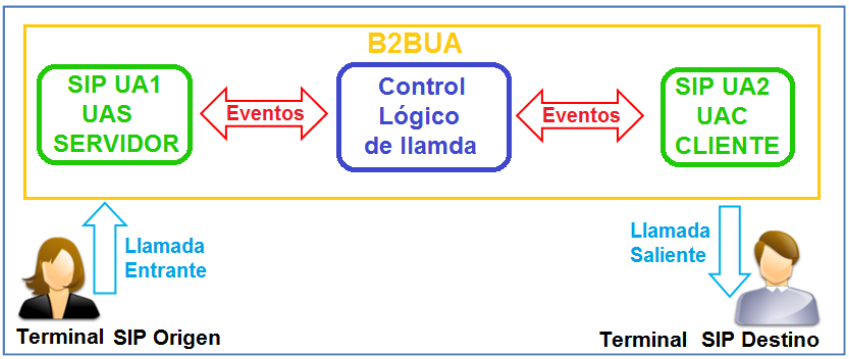

Figura. 3.20. Arquitectura del B2BUA de alto nivel.

3.4.2 Proceso típico de llamada SIP B2BUA

1. Una llamada se inicia cuando el SIP UA Servidor recibe un mensaje *INVITE* (1) (solicitud) entrante, del Terminal SIP de Origen.
2. Después de recibir este mensaje, el SIP UA Servidor genera un evento (respuesta) *TRY* (2) y lo pasa al Control lógico de llamada, como se presenta en la Figura 3.21.

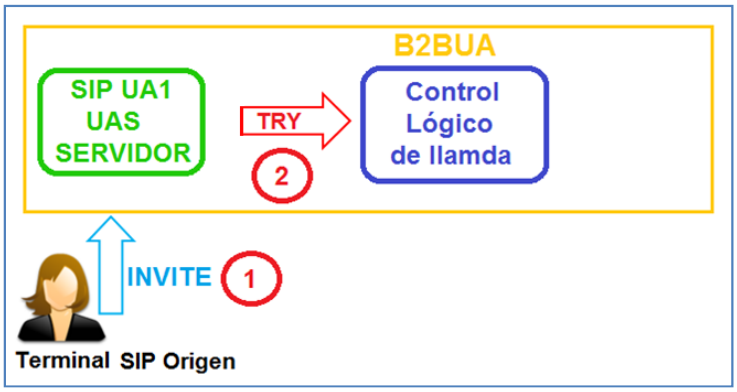

Figura. 3.21. Evento *TRY* pasa al Control lógico de llamada.

3. El Control lógico de llamada recibe el evento *TRY*, realiza la autentificación y autorización, crea el SIP UA Cliente, modifica el evento *TRY*, para adaptarse a cualquier lógica de traducción de parámetros, y lo pasa junto con la información de enrutamiento al SIP UA Cliente (3).
4. El SIP UA Cliente recibe el evento *TRY*, y genera un nuevo mensaje de solicitud *INVITE* (4), como se presenta en la Figura 3.22.

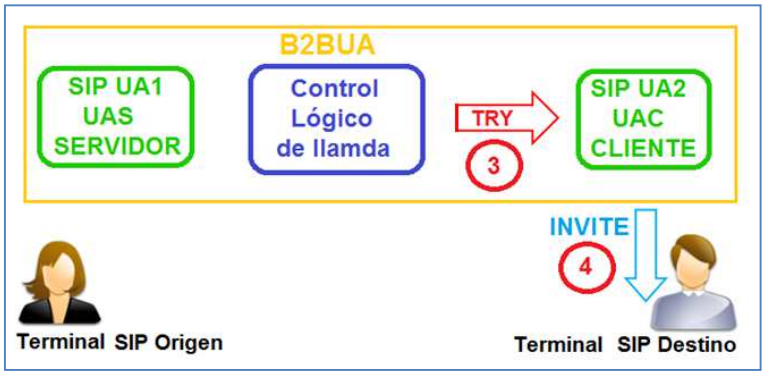

Figura. 3.22. El SIP UA Cliente genera el mensaje de solicitud INVITE.

5. Después que el Terminal SIP Destino recibe el mensaje *INVITE*, empieza a sonar o timbrar y envía un mensaje respuesta SIP provisional *18X Ringing* (5) (el terminal esta timbrando).
6. El SIP UA Cliente recibe el mensaje *180 Ringing*, y genera un evento de llamada (*Ringing*), y lo pasa al Control lógico de llamada (6).
7. El Control lógico de llamada recibe el evento *Ringing*, y lo pasa al SIP UA Servidor (7), el cual envía una respuesta SIP provisional *18X Ringing* al Terminal SIP Origen (8), como se presenta en la Figura 3.23.

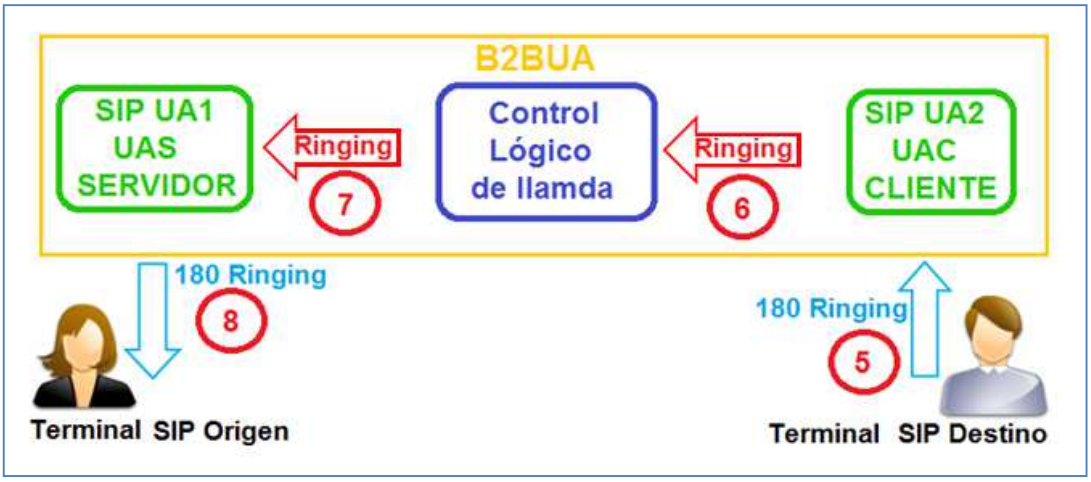

Figura. 3.23. El SIP UA Servidor envía una respuesta al Terminal SIP Origen.

8. Cuando el usuario del Terminal SIP Destino contesta el teléfono, el Terminal genera una respuesta SIP *200 OK* y lo envía nuevamente al SIP UA Cliente (9).
9. El SIP UA Cliente genera un evento *Connect* y lo pasa al Control lógico de llamada (10), posteriormente el Control lógico de llamada pasa el evento *Connect* al SIP UA Servidor (11).
10. El SIP UA Servidor envía el mensaje 200 *OK* al Terminal SIP de Origen (12). En este punto, la sesión se establece, y los Terminales empiezan a intercambiar *media streams RTP* (13), como se presenta en la Figura 3.24.

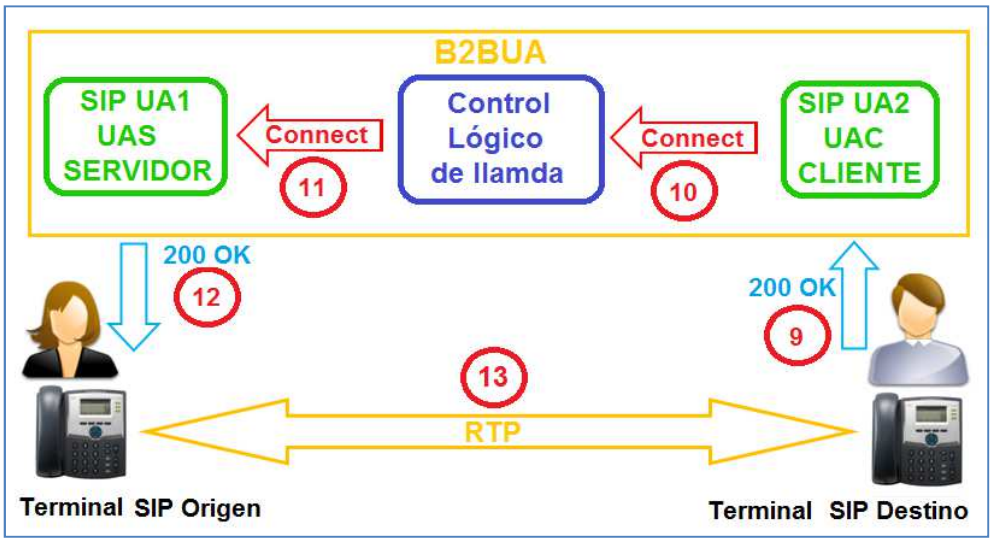

Figura. 3.24. Terminales intercambiar media streams RTP.

11. Cuando cualquiera de los usuarios cuelga el teléfono, el respectivo Terminal SIP genera un mensaje *BYE* (Finaliza una llamada), y envía el mensaje al SIP UA asociado (14).
12. El SIP UA genera un evento de desconexión (*Disconnect*), el cual se propaga hacia el otro lado del B2BUA atravesando el Control lógico de llamada (15), (16), y el resultado es el mensaje *BYE*, el cual es enviado al otro Terminal SIP (17), como se presenta en la Figura 3.25.

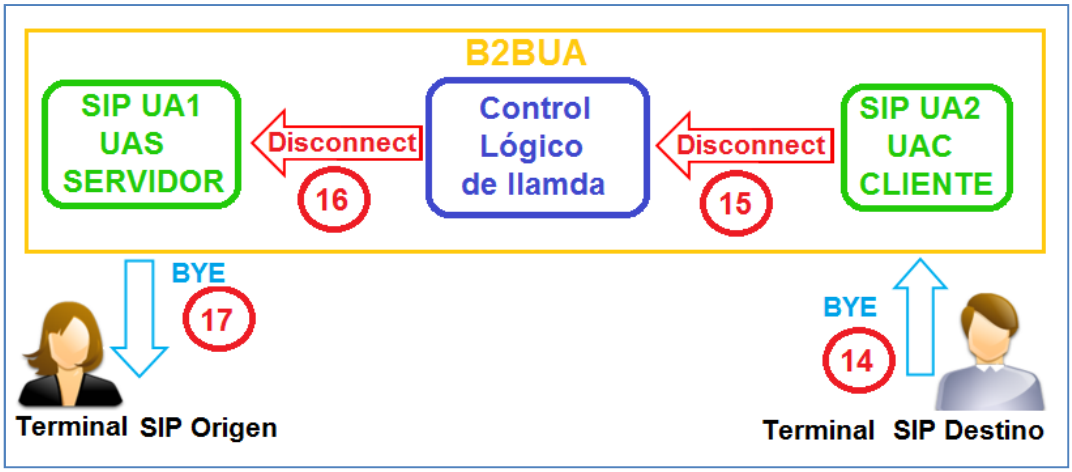

Figura. 3.25. Mensaje BYE enviado hacia el Terminal SIP.

13. La sesión termina.

3.5 MENSAJES SIP

SIP utiliza una sintaxis similar a la del protocolo HTTP, los UAC (UA cliente) general las solicitudes y los UAS (UA servidor) envían respuestas a las solicitudes de los clientes. El protocolo SIP define a la comunicación mediante dos tipos de mensajes. El primer tipo son las solicitudes (*métodos*), y el segundo tipo son las respuestas (*códigos de estado*). Utilizando el formato de mensaje estándar establecido en la RFC 2822, en la cual define su estructura, que consiste en una línea de inicio (*Start line*), seguido de uno o más campos de cabeceras (*Headers*), a continuación una línea en blanco o vacía, la cual indica el final de las cabeceras, y finalmente está constituido por el cuerpo de mensaje (*Message body*), el cual es opcional.

3.5.1 Partes del mensaje SIP

Los mensajes SIP se componen de las siguientes tres partes:

- Línea de inicio (Start line)
- Cabeceras (Headers)
- Cuerpo de mensaje (*Message body*)

El formato del mensaje SIP se presenta en la Figura 3.26.

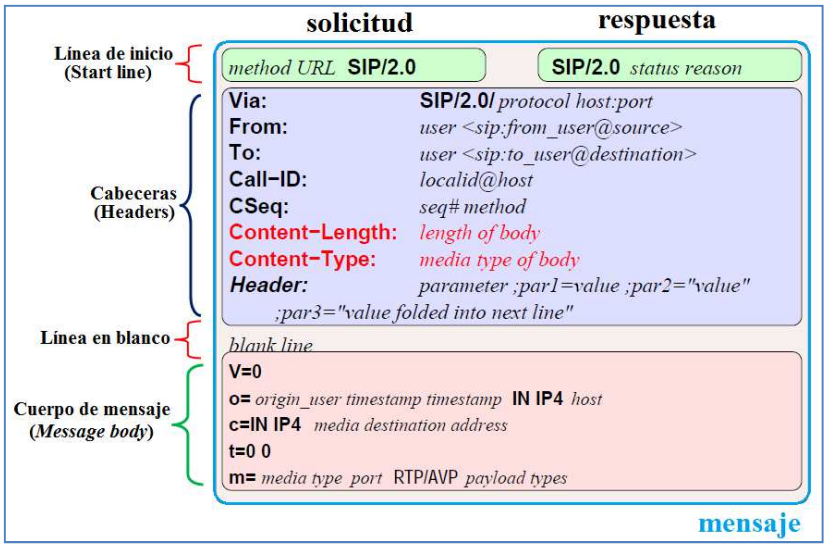

Figura. 3.26. Formato del mensaje SIP.

3.5.1.1 Línea de inicio (Start line)

Todos los mensajes SIP comienzan con una línea de inicio. La línea de inicio transmite el tipo de mensaje [tipo de método (mensaje de solicitud) / código de estado (mensaje de respuesta)] y la versión del protocolo. La línea de inicio puede ser una línea de *Solicitud* (*Request-line*, para solicitudes) o una línea de *Estatus* (*Status-line*, para respuestas), de la siguiente manera:

- La línea de *Solicitud* incluye una Solicitud-URI, que indica a que usuario o servicio se está dirigiendo la solicitud, además incluye las direcciones involucradas en la sesión.
- La línea de Estatus contiene el número del código de estatus (*Status-code*), y su frase textual asociada.

3.5.1.2 Cabeceras (Headers)

En los campos de la cabecera del mensaje SIP, transportan información necesaria a las entidades SIP, información relacionada con la sesión en forma de texto, como por ejemplo indica las direcciones de origen y destino de la solicitud, identificador de llamada entre otros. Dicho de otra forma, en las cabeceras se transmiten los atributos del mensaje, los cuales proporcionan información adicional acerca del mensaje. Estos campos son similares en la sintaxis y semántica a los campos de cabecera del mensaje HTTP (de hecho, algunas cabeceras son tomadas del mensaje HTTP) y por lo tanto siempre tienen el siguiente formato: *<Nombre> : <Valor>*.

Las cabeceras pueden abarcar múltiples líneas. Algunos campos de las cabeceras SIP son por ejemplo*: Via, From, To, Call-ID, CSeq, Contact, User-Agent, Content-Type, Content-Length* entre otros, a continuación se detallan algunos campos:

- ✓ *Via*: Muestra el transporte utilizado para el envió, también identifica la ruta de la solicitud, por lo tanto cada proxy server agrega una línea en este campo.
- ✓ *From*: Indica la dirección del terminal origen de la solicitud.

- ✓ *To*: Indica la dirección del terminal destino de la solicitud.
- ✓ *Call-ID*: Es un identificador único para cada llamada e incluye la dirección del host, este campo debe el mismo para todos los mensajes dentro de una transacción.
- ✓ *CSeq*: Es presentado por un número aleatorio, identificando la secuencia de las transacciones, o de cada solicitud.
- ✓ *Contact*: Indica la o las direcciones que pueden utilizadas para contactarse con el usuario.
- ✓ *User Agent*: Indica el agente de usuario cliente que realiza la transacción.

3.5.1.3 Cuerpo de mensaje (Message body)

El cuerpo del mensaje o carga útil (*payload*) se utiliza para describir la sesión que se iniciará (por ejemplo, en una sesión multimedia puede incluir los tipos de *codecs* de audio y video, también frecuencias de muestreo), es decir en el cuerpo del mensaje transporta información (generalmente SDP ó ISUP[23] cuando va de una troncal hacia la PSTN). Alternativamente puede ser utilizado para datos textuales o binarios de cualquier tipo, que tengan de alguna manera relación a la sesión.

El cuerpo del mensaje puede parecer tanto en mensajes de solicitud como en mensajes de respuesta. SIP hace una clara distinción entre la información de señalización, transmitido en la línea inicio y cabeceras del mensaje SIP.

3.5.2 Tipos de mensajes

Existen dos tipos de mensajes SIP:

- ➢ Solicitudes o métodos (*Requests*): Enviadas desde el cliente al servidor.
- ➢ Respuestas o códigos de estado (*Responses*): Enviadas desde el servidor al cliente.

[23] ISUP es un protocolo de circuitos conmutados, usado para configurar, manejar y gestionar llamadas de voz y datos sobre PSTN.

3.5.2.1 Solicitudes o métodos SIP (Requests)

Las solicitudes SIP son identificadas en la línea de inicio del mensaje (*Start line*), específicamente denominada *Request Line*, la cual contiene el nombre del método, seguido del identificador del destinatario de la solicitud (*SIP URI o Request URI*), seguidamente de la versión del protocolo SIP. A continuación se presenta en la Figura 3.27 un ejemplo de mensaje tipo solicitud SIP.

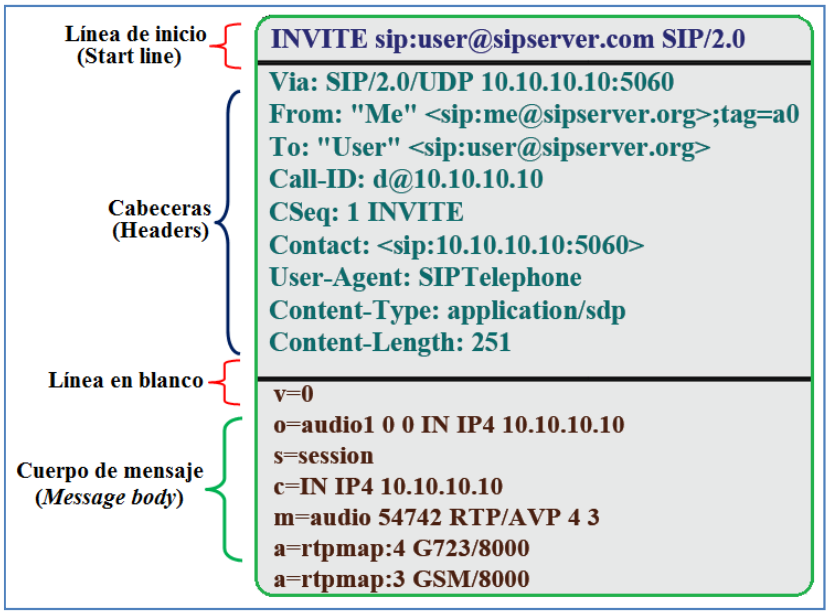

Figura. 3.27. Ejemplo de mensaje tipo solicitud SIP o método SIP.

A continuación se presenta en la Tabla 3.2 ejemplos de métodos de solicitudes SIP.

Tabla. 3.2. Ejemplos de métodos de solicitudes SIP (Requests).

Nombre del método	Descripción
INVITE	Inicia una llamada, cambios en los parámetros de la llamada (re-INVITE)
ACK	Confirma una respuesta final para INVITE
BYE	Finaliza una llamada
CANCEL	Cancela las búsquedas y timbrando (ringing)
OPTIONS	Consulta parámetros de capacidades de negociación, del otro extremo de la llamada
REGISTER	Registra con el Servicio de la Ubicación
INFO	Envía información media de la sesión que no modifica el estado de la sesión

Existen otros métodos adicionales que pueden ser utilizados, denominados *Extensión de los métodos SIP*, se adjunta un listado en el Anexo 1.

- INVITE

El mensaje *INVITE* se utiliza para establecer una sesión multimedia entre dos o más agentes de usuario, es decir invita a un usuario (al que se desea llamar) para establecer una sesión. Este mensaje se envía desde el usuario llamante (origen) hacia el usuario llamado (destino).

- ACK

El mensaje *ACK* (Acknowledgement o en español acuse de recibo), indica que: si ha llegado el mensaje y además ha llegado correctamente, dicho de otra manera, confirma una respuesta final (por ejemplo el mensaje *200 OK*) para *INVITE*, es decir para el establecimiento de una sesión se utiliza el procedimiento llamado *saludo de tres vías* o negociación en tres pasos (*3-way handshake*), debido a la naturaleza asimétrica de la invitación. Se puede tomar un tiempo antes de que el usuario llamado (destino) acepta o rechaza la llamada, entonces el Agente de Usuario (UA) llamado, periódicamente re-transmite una respuesta final positiva hasta que reciba un *ACK* enviado usuario llamante (origen), que indica que el usuario llamante está presente, y listo para comunicarse). Este mensaje *ACK* es enviado como respuesta al mensaje *200 OK*, como se presenta en la Figura 3.28.

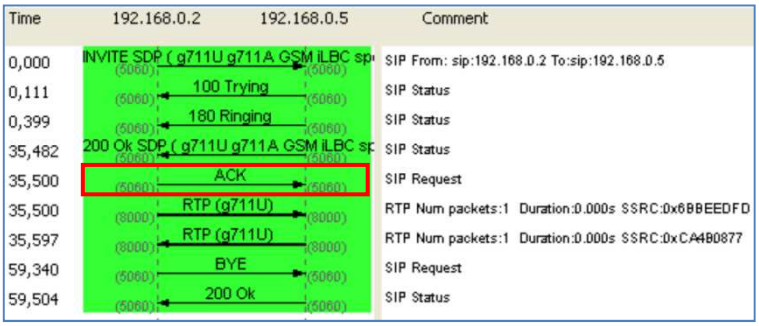

Figura. 3.28. Mensaje ACK confirma una respuesta 200 OK para INVITE.

- BYE

El mensaje *BYE* se utiliza para finalizar las sesiones multimedia. El usuario que desee finalizar la sesión, envía un mensaje *BYE* al otro usuario integrante de la sesión.

- CANCEL

El mensaje *CANCEL* es utilizado para cancelar una sesión que todavía no está completamente establecida. Este mensaje es aplicado cuando el usuario llamado (destino) aún no ha respondido con una respuesta final. Por lo tanto el mensaje *CANCEL* se utiliza cuando el usuario llamante (origen) desea anular la llamada, (típicamente cuando el usuario llamado no responde durante algún tiempo).

- OPTIONS

El mensaje *OPTIONS* se utiliza para consultar a un agente de usuario o servidor sobre sus capacidades y descubre su disponibilidad actual. Dicho de otra manera este mensaje solicita información acerca de sus propias capacidades. La respuesta a esta solicitud, lista las capacidades del agente de usuario o servidor.

- REGISTER

El propósito del mensaje *REGISTER* es de permitir que el *SIP Registrar Server* conozca la ubicación actual del usuario. El mensaje *REGISTER* lleva información sobre la dirección IP actual y el puerto en que un usuario puede ser contactado. El *SIP Registrar Server* extrae esta información y la pone en una base de datos de localización. La base de datos puede ser utilizada por los servidores *proxy SIP* para enrutar las llamadas a los usuarios. Estas registraciones son por tiempo limitado y necesitan ser periódicamente actualizadas.

3.5.2.2 Respuestas o códigos de estado (Responses)

Posteriormente a la interpretación y recepción del mensaje de solicitud SIP, el terminal que recibió este mensaje de solicitud, responde enviando un mensaje de respuesta. El mensaje de respuesta es semejante al mensaje de solicitud, la diferencia se encuentra en la línea de inicio del mensaje (*Start line*), específicamente denominada *Status Line*, la cual contiene la versión del protocolo SIP, seguido del código numéricos de la respuesta (*Status Code*), seguidamente de una pequeña descripción del código correspondiente (*Reason Phrase*), este código numérico de la respuesta está conformado por tres dígitos, los cuales facultan para clasificar los diferentes tipos de respuestas en clases, el primer dígito del código precisa la clase de la respuesta.

Los mensajes de respuesta contienen códigos numéricos de la respuesta. El conjunto de códigos de las respuestas SIP, gran parte se basa en los códigos de respuestas HTTP. Existen dos tipos de respuestas y seis clases:

- Tipos de respuestas
  - Provisionales (clase 1xx), las respuestas provisionales son utilizadas por el servidor para indicar el progreso de las transacciones SIP, pero no finalizan las transacciones SIP.
  - Finales (clases 2xx, 3xx, 4xx, 5xx, 6xx), las respuestas finales si finalizan las transacciones SIP.
- Clases
  - 1xx = Provisional, solicitud recibida, continúa con el proceso de la solicitud.
  - 2xx = Éxito (*Success*), la acción fue recibida con éxito, entendido y aceptado.
  - 3xx = Redirección (*Redirection*), la acción adicional debe ser tomada para completar la solicitud.
  - 4xx = Error del cliente (*Client Error*), la solicitud contiene sintaxis errónea o no puede desempeñarse por este servidor. Respuestas de fallo de método.
  - 5xx = Error del servidor (*Server Error*), el servidor falló al desempeñar una solicitud aparentemente válida.
  - 6xx = Falla global (Global Failure), la solicitud no puede ser cumplida por ningún servidor.

A continuación se presenta en la Figura 3.29 un ejemplo de un mensaje tipo respuesta SIP.

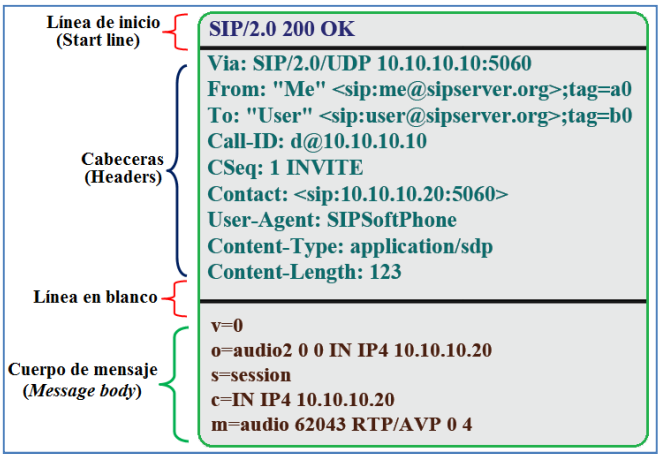

Figura. 3.29. Ejemplo de mensaje tipo respuesta SIP.

A continuación se presenta en la Tabla 3.3 ejemplos de códigos numéricos de respuestas, seguidamente de una pequeña descripción del código correspondiente. Además se adjunta un listado de respuestas SIP en el Anexo 2.

Tabla. 3.3. Ejemplo de Códigos de respuestas.

Número	Significado
100	Trying (Recibí y estoy procesando la llamada)
180	Ringing (El terminal esta timbrando)
200	OK (Atendí la llamada)
300	Multiple choices (Múltiples opciones)
301	Moved permanently (Movido permanentemente)
302	Moved temporarily (Movido temporalmente)
400	Bad request (Solicitud incorrecta)
401	Unauthorized (No autorizado)
403	Forbidden (Prohibido)
408	Request time-out (Solicitud tiempo de espera)
480	Temporarily unavailable (Temporalmente no disponible)
481	Call/Transaction does not exist (La llamada/transacción no existe)
482	Loop detected (Bucle o lazo detectado)
500	Server error (Error del servidor)
600	Busy everywhere (Ocupado en todas partes)
603	Decline (Declive o descenso)
604	Does not exist anywhere (No existe en ninguna parte)
606	Not acceptable (No aceptable)

3.5.3 Ejemplos de mensajes SIP

Los siguientes ejemplos presentan el intercambio de mensajes entre dos agentes de usuario con el propósito de establecer una llamada de voz. El usuario SIP: *alice@radvision.com* (origen), desea establecer una llamada con el usuario SIP: *bob@acme.com* (destino), Alice envía un mensaje de *solicitud INVITE*, que contiene información SDP en el cuerpo del mensaje, Bob responde con un mensaje de *respuesta 200 OK*, que también contiene información SDP. El mensaje de solicitud INVITE se presenta en la Tabla 3.4.

Tabla. 3.4. Ejemplo del mensaje de solicitud INVITE.

Líneas del mensaje de solicitud	Descripción
INVITE sip:bob@acme.com SIP/2.0	Línea de solicitud: nombre del método, Request URI (dirección SIP del destinatario), versión SIP.
Via: SIP/2.0/UDP 172.20.1.1:5060; branch=z9hG4bK-2f059	Identifica la ubicación donde la respuesta debe ser enviada.
Max-Forwards:70	Limita el número de saltos que la solicitud hará en el camino a su destino.
From: Alice A. <sip:alice@radvision.com>;tag=123	Usuario origen de esta solicitud. Incluye una etiqueta única.
To: Bob B. <sip:bob@acme.com>	El usuario a ser invitado, como esta especificado originalmente.
Call-ID: 23889900@alice_ws.radvision.com	Identificador único de esta llamada.
CSeq: 1 INVITE	Comando de secuencia, identifica la transacción.
Contact: <sip:alice@pc33.radvision.com>	Ruta directa para contactarse con Alicia, para nuevas solicitudes.
Subject: Lunch today.	Tema de la llamada.
Content-Type: application/SDP	Tipo del cuerpo del mensaje, en este caso SDP.
Content-Length: 182	Numero de bytes del cuerpo del mensaje.
	La línea en blanco marca fin de la cabecera, para empezar el cuerpo de mensaje.
v=0	Versión de SDP.
o=Alice 53655765 2353687637 IN IP4 128.3.4.5	Propietario o creador, identificador de sesión, versión de la dirección IP de la sesión, dirección IP.
s=Call from Alice.	Tema de la sesión.
c=IN IP4 alice_ws.radvision.com	Información de conexión.
m=audio 3456 RTP/AVP 0 3 4 5	Descripción de media: el tipo, el puerto, diferentes formatos de posibles llamadas, que está dispuesto a recibir y enviar.

Los mensajes de solicitud son utilizados para iniciar alguna acción o para enviar información. Los mensajes de respuesta son utilizados para confirmar que una solicitud fue recibida y está siendo procesada, y posee información sobre el estado del procesamiento. A continuación se presenta en la Tabla 3.5 el mensaje de respuesta 200 OK.

Tabla. 3.5. Ejemplo del mensaje de respuesta 200 OK.

Líneas del mensaje de respuesta	Descripción
SIP/2.0 200 OK	Línea de estado (Status Line): Versión SIP, código de respuesta, descripción del código.
Via: SIP/2.0/UDP 172.20.1.1:5060; branch=z9hG4bK-2f059	Copiado de la solicitud.
From: Alice A. <sip:alice@radvision.com>;tag=123	Copiado de la solicitud.
To: Bob B. <sip:bob@acme.com>;tag=17462311	Copiado de la solicitud. Incluye una etiqueta única para identificar llamadas.
Call-ID: 23889900@alice_ws.radvision.com	Copiado de la solicitud.
CSeq: 1 INVITE	Copiado de la solicitud.
Contact:<sip:bob@172.20.1.77>	Ruta directa para contactarse con Bob.
Content-Type: application/SDP	Tipo del cuerpo del mensaje, en este caso SDP.
Content-Length: 200	Numero de bytes del cuerpo del mensaje.
	La línea en blanco marca fin de la cabecera, para empezar el cuerpo de mensaje.
v=0	Versión de SDP.
o=Bob 4858949 4858949 IN IP4 192.1.2.3	Propietario o creador, identificador de sesión, versión de la dirección IP de la sesión, dirección IP.
s=Lunch	Tema de la sesión.
c=IN IP4 machine1.acme.com	Información de conexión.
m=audio 5004 RTP/AVP 0 3	Descripción de los media streams, que el receptor de la llamada está dispuesto a aceptar.

3.6 TRANSACCIONES SIP

Las transacciones SIP son secuencias de mensajes entre dos entidades SIP, una transacción representa a un mensaje de solicitud y a todos los mensajes de respuesta a esa solicitud, es decir, en una transacción contiene, la solicitud, cero o más respuestas provisionales, y una o más respuestas finales (el mensaje de solicitud *INVITE*, puede ser dividido por un *proxy server*, por tal razón se obtendrá múltiples respuestas finales).

La entidad SIP que almacena o mantiene el estado de las transacciones, es el *stateful proxy*, lo realizan a través del registro de cada transacción por medio de un identificador, el cual se encuentra en el campo Via de la cabecera del mensaje. A continuación se presenta en la Figura 3.30 un ejemplo de los mensajes (solicitud/respuestas) que corresponden a una misma transacción en el establecimiento de una llamada SIP.

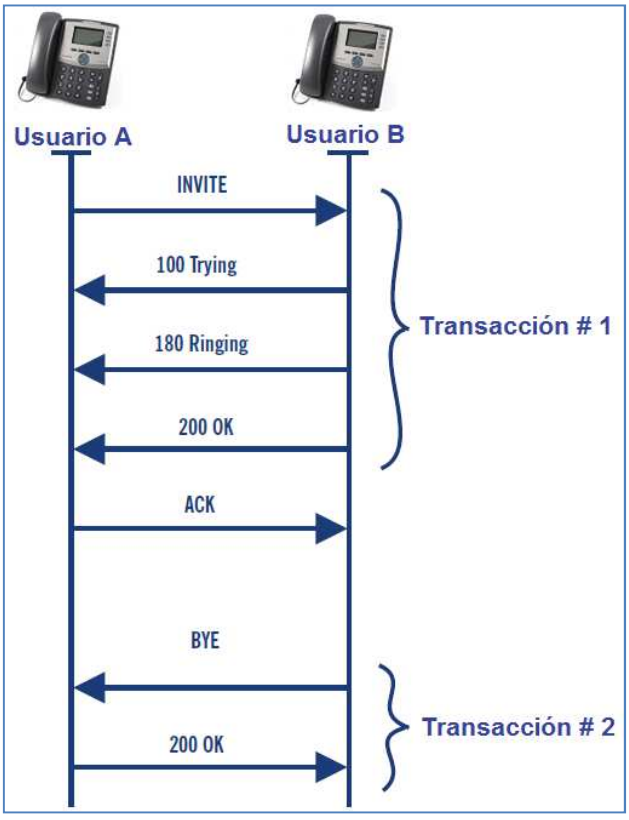

Figura. 3.30. Ejemplo de transacción SIP en el establecimiento de una llamada.

3.6.1 Diálogos SIP

Un dialogo SIP es una conexión *peer to peer* entre dos UA (Agentes de Usuario), que persiste durante algún tiempo. Un diálogo es establecido por menajes SIP, como por ejemplo una respuesta 200 OK a una solicitud *INVITE*.

Un diálogo es identificado por: un identificador de llamada, una etiqueta local, y una etiqueta remota, utilizando los campos *Call-ID* (ID de llamada), *From* (de), *To* (para), de la cabecera del mensaje SIP. Los mensajes en los cuales los campos *Call-ID*, *From*, *To*, contienen la misma información, quiere decir que pertenecen a un mismo diálogo. Adicionalmente el campo *CSeq* identifica la secuencia de las transacciones es decir ordena los mensajes de un diálogo, por lo tanto el *CSeq* representa el número de transacción, Dicho de forma muy sucinta se puede decir que un diálogo es una secuencia de transacciones, como se presenta en la Figura 3.31.

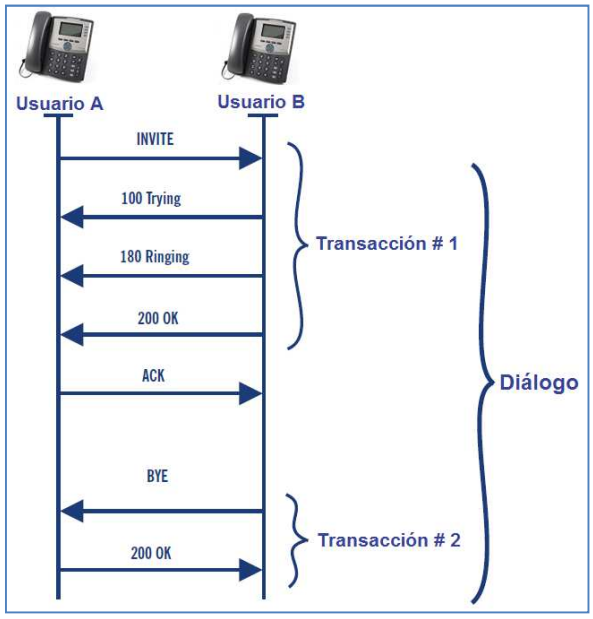

Figura. 3.31. Ejemplo de diálogo SIP.

Los diálogos facilitan el enrutamiento (routing), es decir los diálogos también se utilizan para enrutar los mensajes entre los agentes de usuario, como se describe a continuación.

Se considera que el usuario *sip:alice@radvision.com* (origen), desea establecer una llamada con el usuario *sip:bob@acme.com* (destino), Alice conoce la dirección SIP del usuario destino (*sip:bob@acme.com*), pero esta dirección no dice nada sobre la ubicación actual del usuario, el usuario origen no sabe a qué host debe enviar la solicitud, por lo tanto la solicitud *INVITE* se envía a un servidor *proxy*.

La solicitud se enviará desde un *proxy* hacia otro *proxy* hasta que llega a uno que conoce la ubicación actual del usuario destino, este proceso es denominado *routing*. Una vez que la solicitud llegue al usuario destino, el agente de usuario destino creará una respuesta que será enviada de vuelta al usuario origen. El agente de usuario destino también pondrá información en el campo *Contact* de la cabecera del mensaje de respuesta, este campo contiene la ubicación actual del usuario, es decir este campo indica la o las direcciones que pueden ser utilizadas para contactarse directamente con el usuario. La solicitud original también contiene información en el campo *Contact* de su cabecera, esto significa que, tanto el agente de usuario destino, como el agente de usuario origen, conocen su ubicación actual entre sí.

Debido a que los agentes de usuario conocen la ubicación de cada uno, no es necesario enviar más solicitudes a ningún *proxy*. Ahora los agentes de usuario pueden enviar mensajes (solicitud/respuesta) directamente desde un agente de usuario hacia el otro agente de usuario. Así es exactamente como los diálogos facilitan el enrutamiento (*routing*).

Los mensajes adicionales dentro de un diálogo son enviados directamente desde un agente de usuario hacia otro agente de usuario, esto es una mejora significativa de desempeño, porque los *Proxies* no reciben ni procesan todos los mensajes dentro de un diálogo. En este caso los *Proxies* son utilizados para enrutar solo la primera solicitud que se establece en el diálogo. Los mensajes directos también son entregados con una latencia mucho menor, porque un típico *proxy* generalmente implementa una lógica compleja de enrutamiento.

En la Figura 3.32 se presenta un ejemplo en el cual el mensaje INVITE, por ser la primera solicitud que establece el diálogo, debe atravesar los *Proxies*, a diferencia del mensaje BYE que se envía directamente desde un agente de usuario (origen) hacia otro agente de usuario (destino).

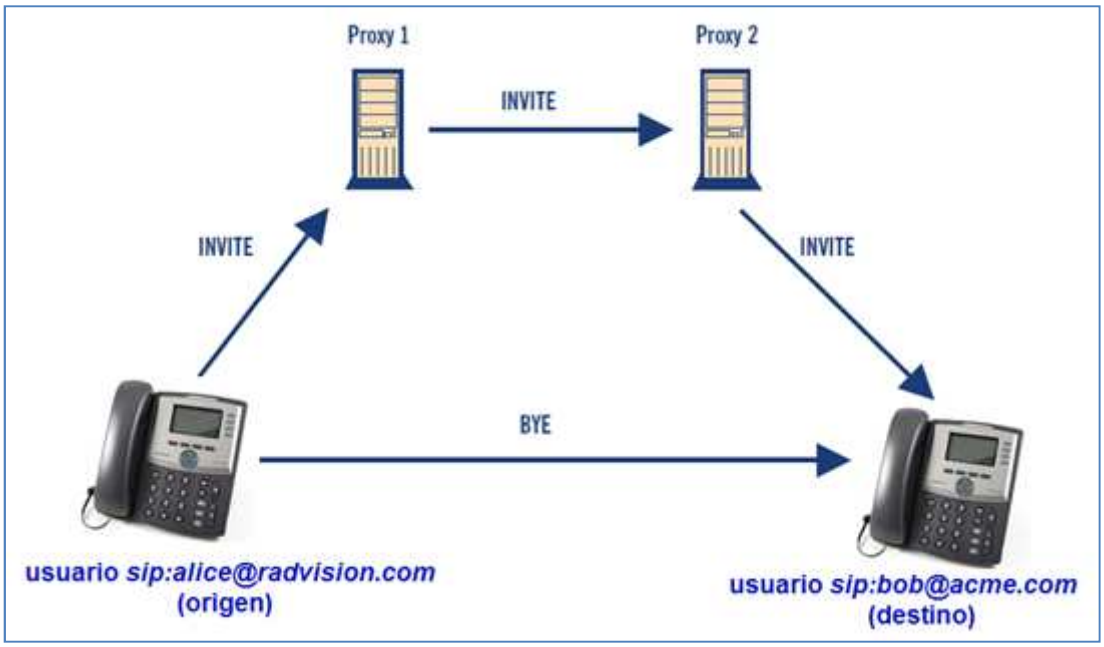

Figura. 3.32. Diálogos facilitan el enrutamiento, SIP trapezoide.

3.7 ESCENARIOS CLÁSICOS DE SIP

En esta sección se presenta un breve resumen de los escenarios clásicos de SIP, que generalmente constituyen el tráfico SIP.

3.7.1 Registro SIP

Los usuarios deben registrarse a la entidad *Registrar* para ser alcanzables por otros usuarios, dicho de otra manera, para que el usuario pueda ser llamado por otros. La solicitud de registro consta de un mensaje *REGISTER*, completando el registro mediante el mensaje de respuesta 200 OK enviado por *Registrar*, si el registro fue exitoso, las registraciones usualmente son autorizadas.

Cuando los usuarios no proporcionan credenciales validas recibirán por respuesta un mensaje 401 ó 407, en este caso el usuario deberá reenviar el mensaje *REGISTER* hasta que el registro haya sido exitoso. La Figura 3.33 presenta un ejemplo de registro SIP.

Figura. 3.33. Registro SIP, flujo de mensajes.

3.7.2 Invitación de sesión SIP

Para el establecimiento de una llamada mediante SIP se debe realizar la invitación de sesión, que consiste en un mensaje de solicitud *INVITE*, que prácticamente es enviado hacia un *proxy*, el *proxy* inmediatamente después de recibir la solicitud *INVITE* envía un mensaje de respuesta *100 Trying* (recibí y estoy procesando la llamada), esto lo realiza para detener las retransmisiones y reenviar la solicitud *INVITE* hacia otro *proxy*. Todas las respuestas provisionales generadas por el usuario destino son enviadas de vuelta al usuario origen, como por ejemplo el mensaje de respuesta *180 Ringing* (el terminal esta timbrando), esta respuesta es generada cuando el teléfono empieza a timbrar.

El mensaje de respuesta *200 OK* (atendí la llamada) es generado una vez que el usuario destino descuelga o contesta el auricular del teléfono, esta respuesta es retrasmitida hacia el usuario origen, hasta que el usuario destino reciba un mensaje de confirmación ACK (atendí la llamada) enviado por el usuario origen, en este punto la sesión se establece y además se establece la conversación (audio/video RTP streams). La Figura 3.34 presenta un ejemplo de invitación de sesión SIP.

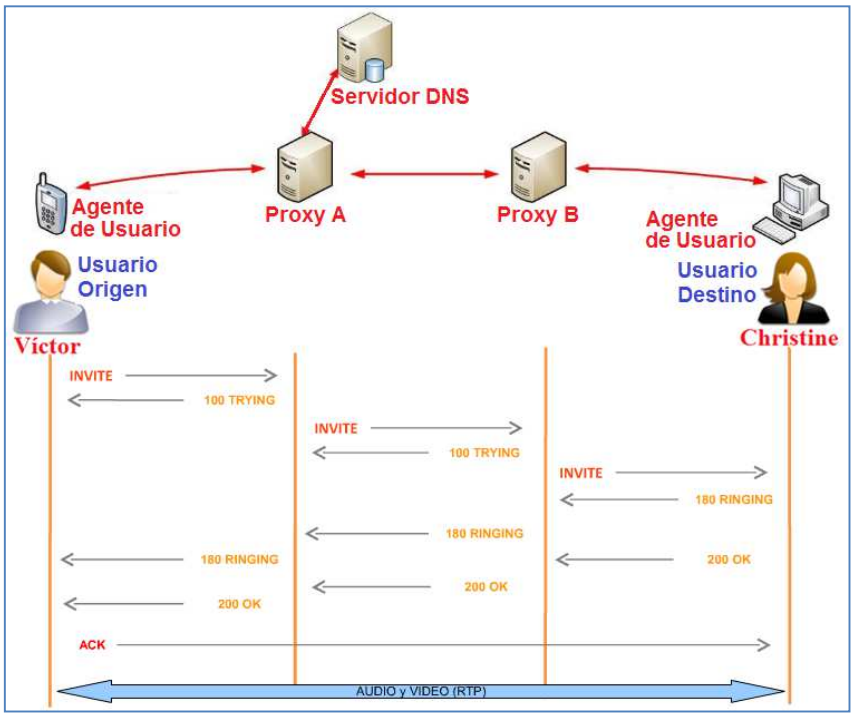

Figura. 3.34. Invitación de sesión SIP, flujo de mensajes.

3.7.3 Finalización de la sesión SIP

La finalización de la sesión se lleva a cabo mediante el envío del mensaje de solicitud *BYE*, dentro del diálogo establecido por *INVITE*. El mensaje *BYE* se envía directamente desde un agente de usuario hacia el otro agente de usuario, a menos que un *proxy* que se encuentra en la trayectoria de la solicitud *INVITE*, haya indicado que desea permanecer en la ruta mediante el establecimiento del proceso *Record Routing (Registro de Ruta).*

El usuario que desea finalizar la sesión, envía la solicitud *BYE* directamente al otro usuario involucrado en la sesión. El usuario que recibe la solicitud *BYE* envía una respuesta 200 OK para confirmar la finalización de la sesión SIP. La Figura 3.35 presenta un ejemplo de finalización de la sesión SIP.

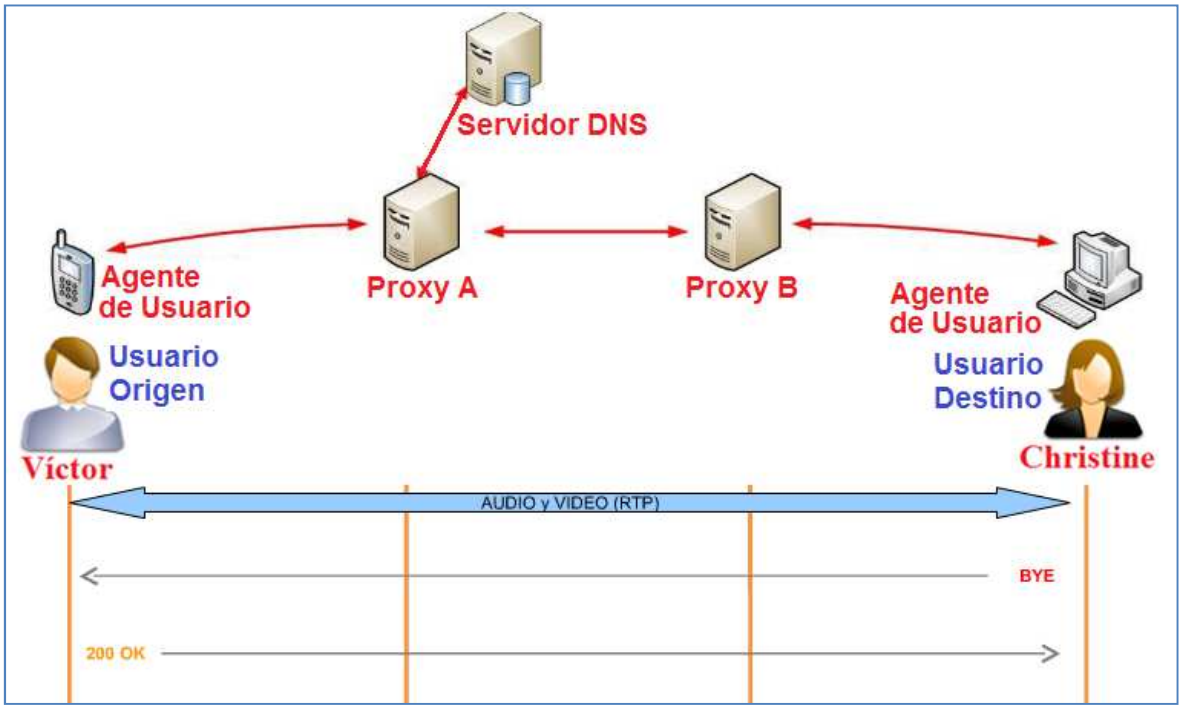

Figura. 3.35. Finalización de la sesión SIP, flujo de mensajes.

3.7.4 Record Routing (Registro de Ruta)

Todas las solicitudes enviadas dentro de un diálogo son por defecto, enviadas directamente desde un agente de usuario hacia otro agente de usuario. Solo las solicitudes que están fuera del diálogo atraviesan los *SIP Proxies,* este enfoque hace que una red SIP sea más escalable, puesto que solo un pequeño número de mensajes SIP atraviesan los *Proxies,* es decir los *Proxies* no reciben ni procesan todos los mensajes dentro de un diálogo.

Existen ciertas situaciones en las cuales los *SIP Proxies* necesitan permanecer en la ruta de todos los mensajes adicionales, con el propósito de controlar el tráfico, por ejemplo los *SIP Proxies* controlan un NAT[24], entre otros.

El mecanismo en el cual un *proxy* informa a los agentes de usuario que desea permanecer en la ruta de todos los mensajes adicionales se denomina *Record Routing (Registro de Ruta).* En este proceso cada *proxy* inserta el campo *Record-Route* en la cabecera del mensaje SIP, que contiene la dirección IP del *proxy.* Los mensajes (solicitud/respuesta) enviados dentro de un diálogo, atravesarán todos los *SIP Proxies* que insertaron el campo *Record-Route* dentro de la cabecera del mensaje SIP. La Figura 3.36 presenta el flujo del mensaje BYE con y sin *Record-Routing.*

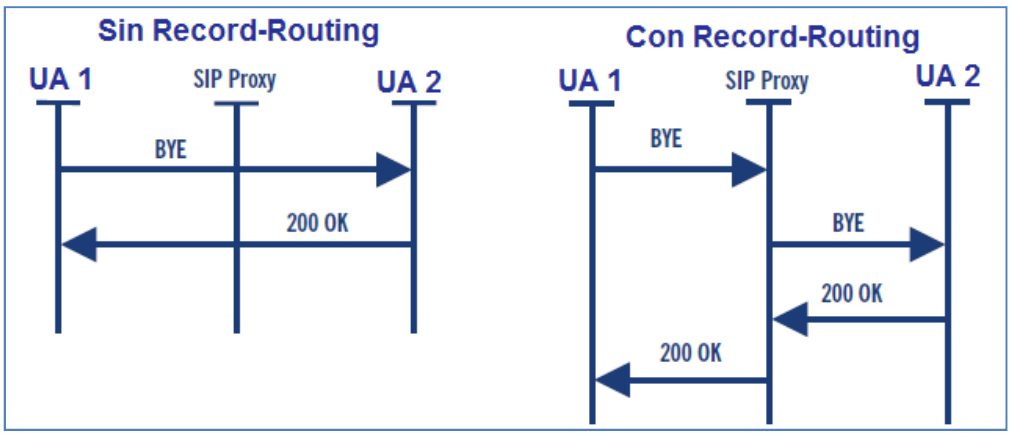

Figura. 3.36. Flujo del mensaje BYE con y sin Record-Routing.

[24] NAT (Network Address Translation - Traducción de Dirección de Red).

3.7.5 Ejemplo de comunicación SIP.

A continuación se analizará de forma sucinta una comunicación SIP, en una llamada SIP existen varias *Transacciones SIP*. Las *Transacciones SIP* son secuencias de mensajes entre dos entidades SIP, es decir, es el intercambio de mensajes entre un cliente y un servidor. Una *Transacción SIP* representa a un mensaje de solicitud y a todos los mensajes de respuesta a esa solicitud, que adicionalmente se ordenan y agrupan en la misma transacción gracias al campo *CSeq*. El ejemplo de comunicación SIP se presenta en la Figura. 3.37.

Una comunicación SIP consta principalmente de las siguientes Transacciones:

1. Las primeras transacciones representadas en color rojo, corresponden al registro de los usuarios.
2. Las siguientes transacciones representadas en color rojo verde, corresponden al establecimiento o invitación de la sesión.
3. En este punto la llamada se encuentra establecida, y empieza el transporte de audio/video, representado en color rojo amarillo, mediante el funcionamiento del protocolo RTP/RTCP.
4. La ultima transacción representada en color rojo azul, corresponde a la finalización de la sesión.

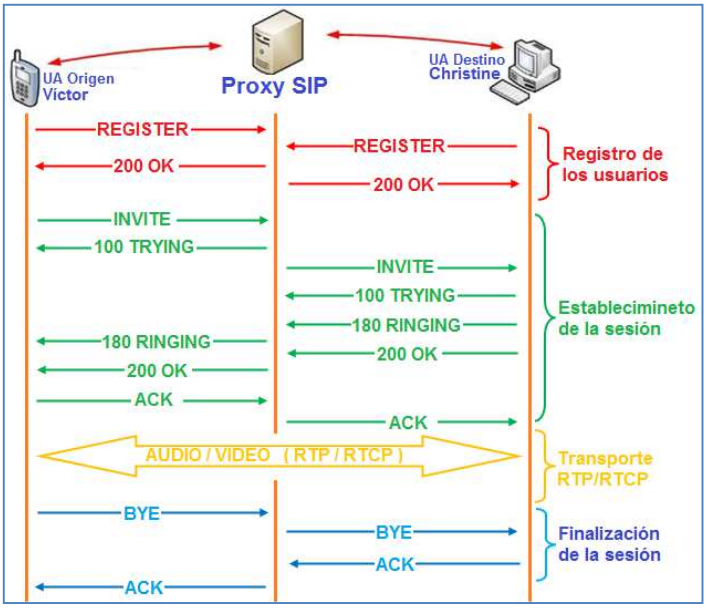

Figura. 3.37. Ejemplo de comunicación SIP.

3.8 PROTOCOLO DE DESCRIPCIÓN DE SESIÓN (SDP)

SDP es el acrónimo en Inglés de *Session Description Protocol* (Protocolo de Descripción de Sesión), que es un formato o un lenguaje para describir los principales parámetros de inicialización que caracterizan a una sesión multimedia, las especificaciones más reciente de SDP están publicadas en la RFC 4566.

SIP trabaja conjuntamente con SDP y RTP/RTCP, donde SDP propiamente está diseñado para transportar información referente a las características de las sesiones, y parámetros de capacidades de negociación entre los integrantes de la sesión, este proceso permite asociar más de un flujo multimedia en una misma sesión, es decir en una misma sesión se puede asociar un flujo para audio, otro flujo para video, o también un flujo para transferir documentos. Por otro lado RTP/RTCP se encarga de transportar los media streams o datos multimedia, propiamente dicho transporta el audio o video.

Dentro del mensaje SDP se envían los parámetros a negociar, como por ejemplo el listado de *Codecs* que están en la capacidad de soportar los integrantes de la sesión, este códec se envía en orden de prioridad (g711U, g711A, GSM, entre otros). También SDP negocia parámetros como la tasa de muestreo de la señal, tamaño de los paquetes, entre otros.

Los paquetes SDP usualmente contienen la siguiente información sobre la sesión multimedia:

- ✓ La versión del protocolo.
- ✓ Propietario o creador, identificador de la sesión.
- ✓ Dirección IP (IPv4 o IPv6 direcciones o nombre del host).
- ✓ Nombre de la sesión y su propósito.
- ✓ Información de conexión.
- ✓ Tiempo que la sesión esta activa (tiempos de inicio y finalización de la sesión).

- ✓ Tipo de dato multimedia relacionado con la sesión, (video, audio, formatos, entre otros).
- ✓ RTP perfil (por lo general: RTP/AVP aunque existen otros como: RTP/SAVP).
- ✓ Número de puerto (utilizado por UDP o TCP para el transporte).
- ✓ Esquema de codificación (PCM A-Law, MPEG II video, entre otros).
- ✓ Atributos específicos de la sesión o atributos multimedia, con el siguiente formato: a = <atributo>, a = <atributo>:<valor>

SDP está basado en texto, un mensaje SDP se compone de un conjunto de líneas de texto, de la siguiente forma:

<tipo> = <valor>

Donde <tipo> es un único carácter, y <valor> es un texto estructurado cuyo formato depende el <tipo>. Un ejemplo de mensaje SDP se presenta a continuación:

v = 0
o = alice 2890844526 2890842807 IN IP4 1.2.3.4
s =
c = IN IP4 1.2.3.4
t = 0 0
m = audio 49170 RTP/AVP 0
a = sendrecv

Un mensaje SDP contiene tres niveles de información:

1. Nivel descripción de la sesión: contiene líneas que describen las características de la sesión completa.
2. Descripción del tiempo: contiene líneas que indican aspectos relacionados con el tiempo de la sesión.
3. Descripción multimedia: contiene líneas que caracterizan los diferentes datos multimedia presentes en la sesión.

A continuación se presenta en las Tablas 3.6, 3.7, 3.8, los diferentes tipos de líneas para cada nivel, además se indica si es el campo es Requerido (R) u Opcional (O).

Tabla. 3.6. Nivel descripción de la sesión, SDP líneas.

Campo	Descripción	R/O
v	Versión del Protocolo.	R
o	Propietario o creador, identificador de la sesión.	R
s	Nombre de la sesión.	R
i	Información de la sesión.	O
u	URI de la descripción.	O
e	Dirección email (Email address).	O
p	Número de teléfono (Phone number).	O
c	Información de conexión (Connection information).	O
b	Información de ancho de banda (Bandwidth information).	O
z	Ajuste de la zona de tiempo.	O
k	Clave de cifrado (Encryption key).	O
a	Atributos de la sesión.	O

Tabla. 3.7. Descripción del tiempo, SDP líneas.

Campo	Descripción	R/O
t	Tiempo que la sesión esta activa.	R
r	Repetir el tiempo (Repeat time).	O

Tabla. 3.8. Descripción multimedia, SDP líneas.

Campo	Descripción	R/O
m	Nombre de media y dirección de transporte.	R
i	Titulo de media (Media title).	R
c	Información de conexión (Connection information).	R
b	Información de ancho de banda (Bandwidth information).	O
k	Clave de cifrado (Encryption key).	O
a	Atributos de la sesión.	O

SDP se envía conjuntamente con los mensajes *INVITE* y *200OK*, cabe aclarar que: el mensaje *INVITE* se envía desde el origen hacia el destino, y el mensaje *200OK* se envía desde el destino el hacia origen. En el caso del mensaje *200OK* no siempre se envía SDP, porque existió un mensaje anterior que ya negoció estos parámetros. A continuación se analizará el paquete SIP/SDP dentro del mensaje de solicitud *INVITE*, que se presenta en Figura 3.38.

Para analizar el paquete SIP/SDP se utilizó el programa *Wireshark*, en el cual se ilustran todos los aspectos comentados de SIP, SDP y RTP, en tiempo real. El paquete corresponde a un mensaje SIP tipo *Request* (Solicitud), específicamente con el método *INVITE*, que se refiere al establecimiento de la llamada o sesión.

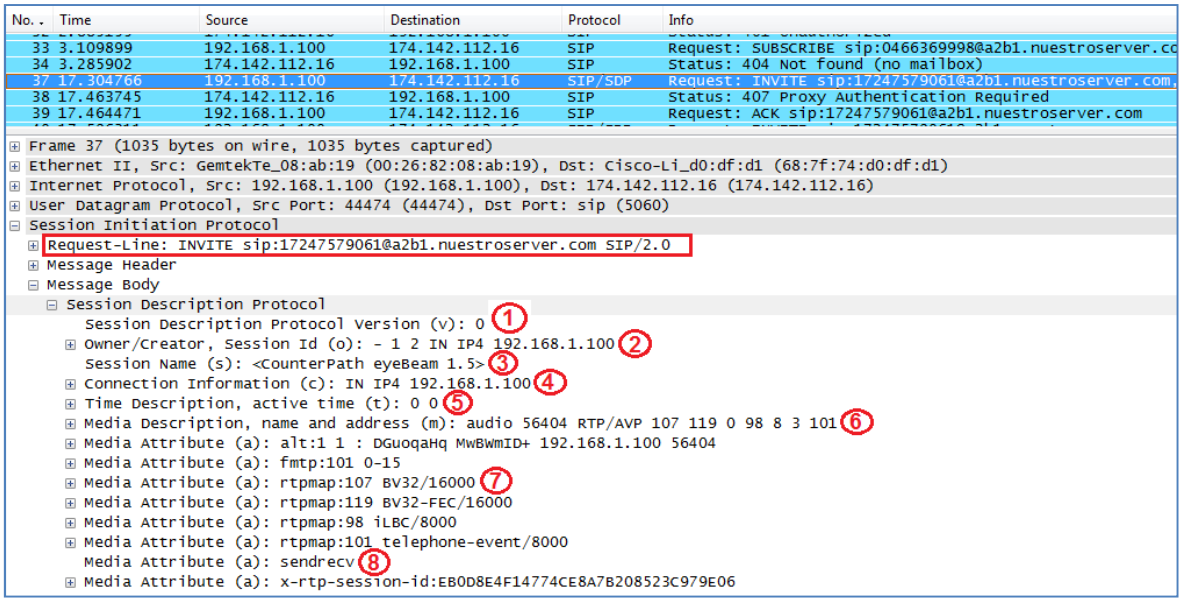

Figura. 3.38. Paquete SIP/SDP dentro del mensaje de solicitud INVITE.

En cuadro rojo se señala el tipo de mensaje SIP (Request-Line), específicamente con el método *INVITE*, mensaje SIP dirigido al usuario: *17247579061@a1b1.nuestroserver.com*, se observa también la versión SIP, la cual es: SIP/2.0.

Message Body o cuerpo del mensaje contiene *Session Description Protocol* (SDP) con los siguientes campos:

1. Versión del protocolo SDP, (v=0).

2. Owner/Creator, Propietario/Creador, identificador de la sesión, además está conformado por:
   (o = <usuario> <Id sesión > <tipo de red> <tipo de dirección IP> <dirección IP>).

3. Nombre de la sesión.

4. *Connection Information*, información sobre la conexión, la información contiene:
   (c = <tipo de red> < tipo de dirección IP> <dirección IP>).

5. *Time Description active time*, se indica el inicio y final de la sesión, en el presente caso se tiene (t): 0 0 , esto quiere decir: Start time = 0, y stop time = 0, lo que significa que es una sesión no limitada y permanente.

6. *Media Description, name and address(m):*, En este campo se presenta información sobre el tipo de datos que se transporta (en presente caso es audio de una sesión telefónica), el puerto UDP utilizado (56404), seguido del protocolo utilizado (RTP/AVP, Real Time Transport Protocol /AVP Audio Video Profiles), y finalmente los formatos de codecs, como se presenta en la Figura 3.39.

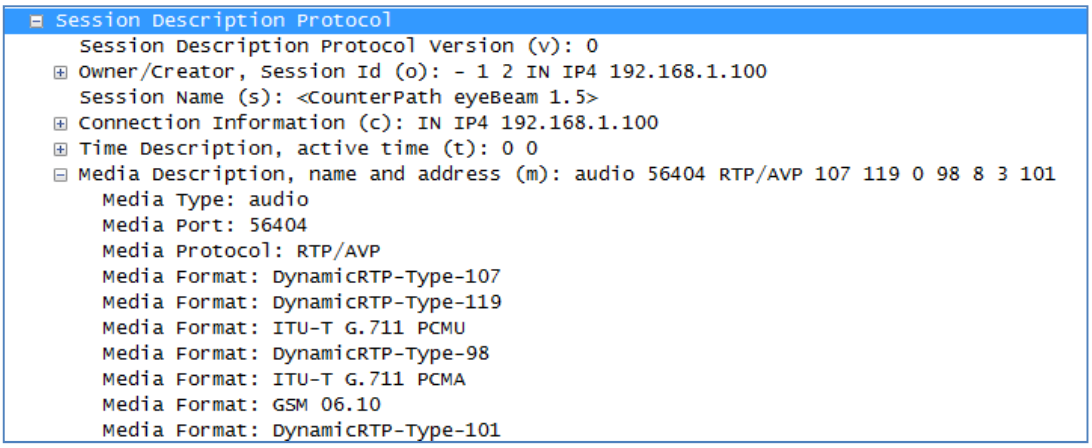

Figura. 3.39. Descripción de los campos multimedia.

7. *Media Attribute (a)*, Se indica una lista de los formato de codes descritos con información de *Sample rate* o frecuencia de muestreo, Fieldname o nombre del campo, entre otros, como se presenta en la Figura 3.40.

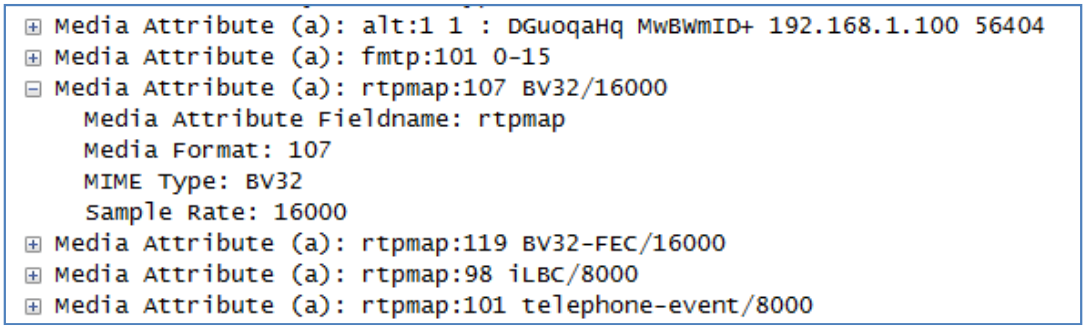

Figura. 3.40. Descripción de los campos atributos de la sesión multimedia.

8. *Media Attribute (a): sendrecv*, es el modo envió/recepción.

9. Atributos propuestos:
   - ✓ Categoría (a): cat: <categoría>.
   - ✓ Palabras clave (a): keywds: <keywords>.
   - ✓ Herramienta (a): tool: <nombre y versión de la herramienta>.
   - ✓ Tiempo de paquete (a): ptime: <packet time>.
   - ✓ Modo sólo recibe (a): recvonly.
   - ✓ Modo envió/recepción (a): sendrecv.
   - ✓ Modo sólo envió (a): sendonly.
   - ✓ Orientación de pizarra (a): orient: <orientación>.
   - ✓ Tipo de conferencia (a): type: <tipo de conferencia>.
   - ✓ Juego de caracteres (a): charset: <juego de caracteres>.
   - ✓ Idioma (a): sdplang: <etiqueta idioma>.
   - ✓ Tasa de frames (a): framerate: <tasa de frames>.
   - ✓ Calidad (a): quality: <calidad>.
   - ✓ Formato específico (a): fmtp: <formato> <parámetros específicos de formato>.

3.9 PROTOCOLOS RTP/RTCP

Inmediatamente después de establecer la sesión, se transportan los datos en tiempo real (audio y/o video). El protocolo más utilizado para el transporte de los *media streams* (audio, video) en telefonía IP es RTP (*Real-time Transport Protocol*), RTP es un protocolo estándar (STD64) definido por el IETF, que proporciona servicios de entrega end-to-end, para datos con características en tiempo real. Su función principal de RTP es la de transportar los *media streams*, o transportar flujos en tiempo real (*Real-time Media Streaming*), codificados mediante UDP.

RTP define el concepto de la sesión RTP, Una sesión RTP está identificada por una dirección de transporte, e incluye solo un tipo de *media streams*. Esto es diferente del concepto de la sesión SDP, que incluye a todos los tipos de *media streams* que fluyen desde el usuario origen (emisor), hasta el usuario destino (receptor). Realmente, una sesión de SDP puede abarcar varias sesiones de RTP. Una sola sesión multimedia SDP podría, por ejemplo incluir una sesión de voz RTP más una sesión video de RTP.

El protocolo RTP "viaja o corre" sobre UDP para el transporte de la información, obteniendo mayor velocidad, puesto que UDP es un protocolo rápido, la información llega en el menor tiempo posible, por lo tanto es utilizado en aplicaciones en tiempo real, como se presenta en la Figura 3.41, además se presenta al paquete RTP encapsulado dentro del paquete UDP/IP.

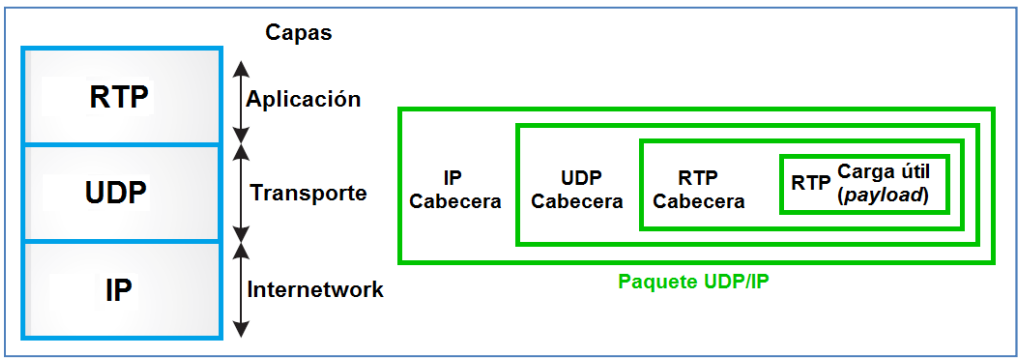

Figura. 3.41. RTP trabaja sobre UDP.

Además aprovecha el campo *Checksum* (suma de verificación, 16 bits) del mensaje UDP, para verificar la integridad de los datos. *Checksum* también se lo conoce por *Frame Check Sequence*, esto es cuando una trama es recibida y tienen una secuencia de verificación incorrecta, por lo tanto verifica la integridad física de los datos a procesar.

Un paquete RTP se compone de una cabecera (*header*) y de los datos o datos carga útil (*payload*), en los datos de carga útil contiene voz o video real codificados, mientras que en la cabecera contiene información necesaria para prestar los servicios que proporciona el protocolo. En la Figura 3.42 se presenta el formato del paquete RTP.

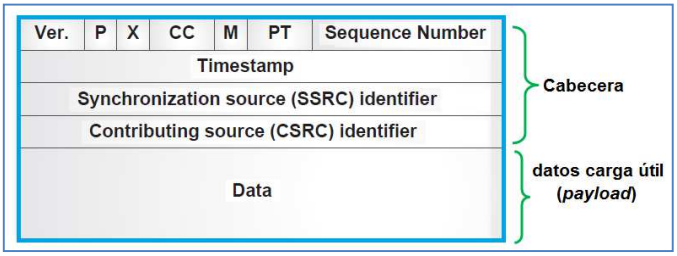

Figura. 3.42. Formato del paquete RTP.

Básicamente existen dos campos esenciales en la cabecera del formato del mensaje RTP, que proporcionan funcionalidades cruciales para transportar los media streams en tiempo real, estos campos son: *Timestamp* o etiqueta de tiempo y *Sequence number* o número de orden. La información del *Timestamp* permite reconstruir la sincronización y eliminar el jitter. La información del campo *Sequence number* es utilizada para verificar la entrega de los paquetes en orden, y en el caso de ser necesario restaurar el orden de los paquetes, es decir permite al receptor reconstruir la secuencia de los paquetes enviados, como se presenta en la Figura 3.43.

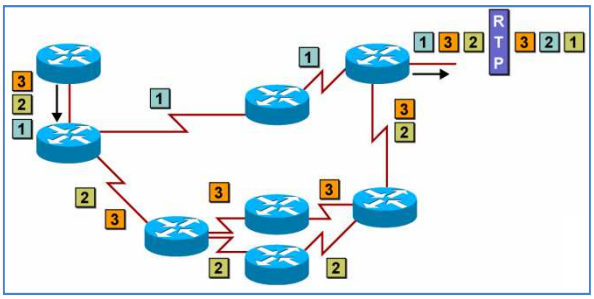

Figura. 3.43. RTP restaura el orden de los paquetes.

Otras cabeceras de interés son:

- Tipo de carga útil o *Payload type* (PT): identifica el formato de la carga útil, es decir, el códec.
- Fuente de sincronización o *Synchronization source* (SSRC): identifica el origen de los paquetes IP.

RTP trabaja en conjunto con RTCP (*Real-time Transport Control Protocol*), cuando RTP transporta los media streams, RTCP se encarga de monitorear, es decir provee información sobre estadísticas de transmisión y calidad de servicio (QoS), como jitter, paquetes recibidos, paquetes enviados, paquetes perdidos, entre otros. Es útil para diagnosticar problemas o incluso provocar un cambio de *codec*. Conjuntamente ayuda a sincronizar los múltiples streams. Las especificaciones más recientes de estos protocolos se encuentran en la RFC 3550.

Principales funciones de RTP/RTCP:

- ✓ Identifica el tipo de carga útil que se transporta (codecs de audio o video).
- ✓ Transporta información de sincronización de los múltiples streams, utilizada para la codificación y decodificación.
- ✓ RTCP monitorear de la entrega de información.
- ✓ RTCP proporciona un seguimiento a la calidad en la distribución de los datos, por ejemplo mantiene el control de los codecs activos.
- ✓ RTCP también se utiliza para transportar un constante identificador de la fuente de RTP que se puede correlacionar con SSRC, (SSRC no es permanente, porque cambia entre sesiones). Este identificador se denomina CNAME, y es transportado en otro tipo de paquetes RTCP denominados SDES (Source Description).
- ✓ Informa el número de participantes por sesión con el propósito de ajustar la tasa de transmisión de datos.

El protocolo RTCP también utiliza al protocolo UDP, para enviar información de control hacia los participantes que intervienen en la sesión, como por ejemplo, estadísticas de transmisión y calidad de servicio (QoS).

CAPÍTULO IV

MATERIALES Y MÉTODOS

4.1 EL PROTOCOLO SIP EN EL DESARROLLO DEL PROYECTO

El presente proyecto pretende analizar la paquetización de Voz Sobre IP en una llamada internacional hacia USA, empleando el Protocolo de Inicio de Sesiones (SIP), con *Back To Back User Agent* (B2BUA), sobre una red inalámbrica Wi-Fi. Para una mejor comprensión del proyecto se ilustra en la Figura 4.1 el diagrama funcional por bloques.

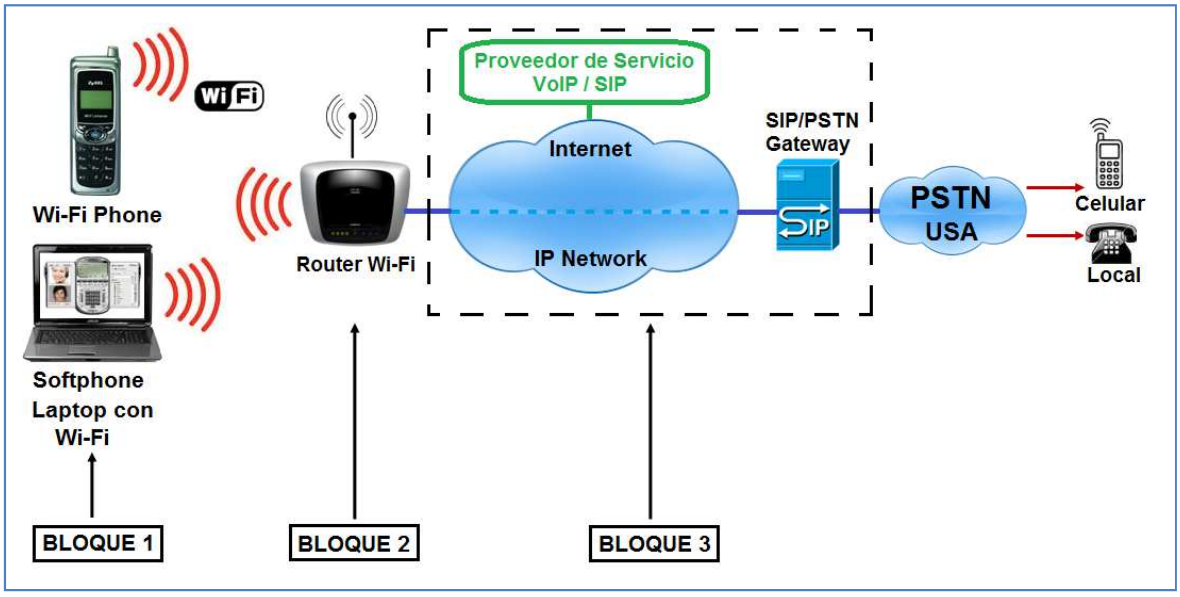

Figura. 4.1. El protocolo SIP en el desarrollo del proyecto: Diagrama funcional por bloques.

- ✓ **Bloque 1.** Configuración de los dispositivos terminales SIP.

  Las aplicaciones VoIP basados en SIP se encuentran en dispositivos terminales tanto en *hardware* como en *software*, es por esto que este bloque contiene un celular Wi-Fi *Phone* (*hardware*), y una computadora laptop Wi-Fi en la cual se encuentra instalada la aplicación para realizar llamadas VoIP denominada *Softphone* (*software*). Además para la captura y análisis de los paquetes SIP la computadora contiene el analizador de protocolos *Wireshark*. Con la información proporcionada por el proveedor de servicio VoIP se configuran los parámetros requeridos por los terminales SIP.

- ✓ **Bloque 2.** Configuración del router inalámbrico.

  Este bloque contiene la configuración de la red inalámbrica.

- ✓ **Bloque 3.** Proveedor de servicio VoIP / SIP, Gateway SIP/PSTN.

  Para poder realizar llamadas desde de la Internet hacia teléfonos convencionales o fijos, es necesario suscribirse con un proveedor de servicio VoIP / SIP (*VoIP Internet Phone Service*). Estos proveedores ofrecen Voz sobre IP basados en el servicio de telefonía de banda ancha utilizando el protocolo SIP para los usuarios. A estos proveedores se los denomina ITSP (*Internet Telephony Service Providers).*

  Estos proveedores ofrecen servicios de puerta de enlace o *Gateway* VoIP (en el presente proyecto es el *Gateway* SIP/PSTN). Habitualmente esto implica un costo por este servicio, sin embargo, generalmente es la opción más económica referente a los precios de las empresas operadoras de telefonía.

  Estos proveedores de Servicios VoIP / SIP permiten realizar y recibir llamadas desde los números de teléfonos analógicos tradicionales y números celulares. Una vez suscrito a este servicio, se puede realizar llamadas a los teléfonos convencionales o fijos, Además la puerta de enlace o *Gateway* proporciona un número de teléfono en el área solicitada, para recibir llamadas desde los números de teléfonos convencionales y celulares.

4.2 PROVEEDOR DE SERVICIO VOIP/SIP, GATEWAY SIP/PSTN

Al momento de elegir un proveedor de servicios VoIP / SIP, la mejor opción es elegir uno que ofrezca servicios especiales en una área determinada, específicamente dentro de un país en particular (en el presente proyecto USA). La elección del proveedor dentro del mismo país que se desea realizar o recibir llamadas constantemente, puede potencialmente reducir los costos en gran manera.

4.2.1 Lista de proveedores de servicio VoIP / SIP

A continuación se presenta una lista de los principales proveedores SIP recomendados, los cuales funcionan bastante bien en aplicaciones de telefonía VoIP.

- ✓ **Call Centric (Canadá, EE.UU.)**

  Callcentric con sede en los Estados Unidos, permite hacer y recibir llamadas telefónicas por Internet sin cuotas de suscripción o mensual. También ofrecen un servicio de pago que permite elegir un número telefónico de EE.UU. o Canadá, y ofrece excelentes precios para llamar a números de teléfonos real.

- ✓ **InPhonex (EE.UU., Reino Unido)**

  InPhonex ofrece un servicio gratuito de número telefónico SIP. Este proveedor posee Gateways PSTN en todas partes del mundo, por lo tanto sólo cobran tarifas locales para ese país. InPhonex también ofrece un número "verdadero" de teléfono para residentes en EE.UU., Canadá y el Reino Unido.

- ✓ **BBPGlobal (Australia, Canadá, Nueva Zelanda)**

  BBPGlobal es una compañía australiana que ofrece tanto servicios gratuitos como de pago. Su servicio gratuito le permite llamar a otros usuarios BBPGlobal o VoIP de PC a PC, y permite recibir llamadas desde un teléfono fijo, si primero se marca a través de un Gateway BBPGlobal.

- ✓ **VoIPtalk (Reino Unido)**

  Es un proveedor popular de Reino Unido, ofrece llamadas gratuitas de PC a PC, además de servicios PSTN gateway.

- ✓ **DrayTEL (UK)**

  Un buen proveedor de Reino Unido que ofrece un servicio básico, sin características adicionales y complementos, brinda llamadas gratuitas de PC a PC, además de servicios PSTN gateway.

4.2.2 Proveedor CallCentric Internet Phone Service

Para el presente proyecto se utilizó el proveedor CallCentric (*Internet Phone Service*), Callcentric ofrece VoIP basado en el servicio de teléfono de banda ancha utilizando el protocolo SIP para usuarios personales, residenciales y comerciales. Los servicios incluyen llamadas salientes (Destino), llamadas entrantes (Origen / DID[25] / DDI) dentro de los EE.UU., Canadá y otros países. Callcentric soporta *Softphones* (*software*), VoIP ATA, teléfonos VoIP (*hardware*), y equipos IP PBX.

Para poder realizar llamadas desde de la Internet hacia teléfonos convencionales o fijos, es necesario suscribirse con un proveedor de servicio VoIP / SIP, para obtener un número SIP, los pasos a seguir son los siguientes:

Paso 1.- **Registrarse en CallCentric**

Ingresar a la página principal: http://www.callcentric.com/ , en la cual la primera opción es *IP FREEDOM*, opción en la cual permite llamadas gratuitas ilimitadas entre todos los miembros CallCentric sin cuotas mensuales. La segunda opción es *PAY PER CALL*, opción en la cual permite realizar llamadas a números fijos, sin cargos mensuales, solo se paga por las llamadas se realiza, a continuación se hace click en *Order Now*, como se presenta en la Figura 4.2.

25 DID (*Direct Inward Dialing*). Es un servicio que ofrecen algunos proveedores VoIP, que permiten tener un número telefónico fijo con el cual recibir llamadas mediante VoIP.

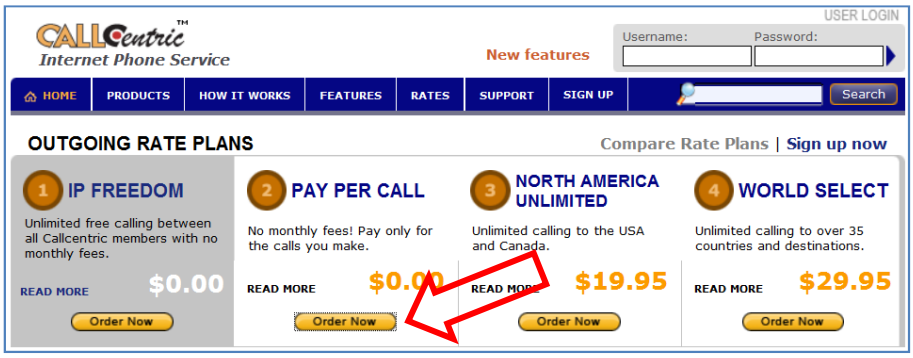

Figura. 4.2. Opción PAY PER CALL.

Se realiza el ingreso de los datos necesarios (nombre, nombre de usuario, *password email*) para registrarse como nuevo cliente (*New customers*), y se hace click en *Continue*, como se presenta en la Figura 4.3.

Figura. 4.3. Ingreso de datos como New customers.

A continuación se enviará un correo electrónico de confirmación a la dirección (*email*) ingresado, que tiene como titulo del mensaje: *Callcentric - Email validation*, en el cual se realiza la validación haciendo click en el enlace proporcionado, como se presenta en la Figura 4.4.

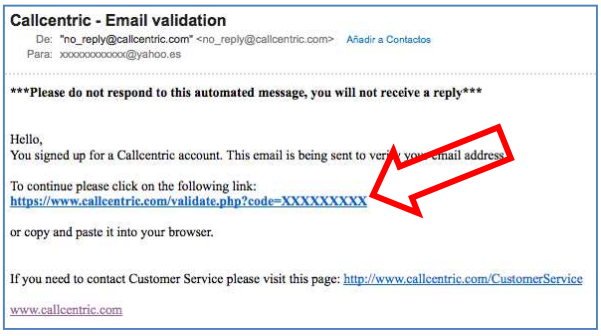

Figura. 4.4. Validación del correo electrónico.

Posteriormente se abrirá una nueva ventana para completar datos del país como: ciudad, estado, código postal, zona horaria. Adicionalmente se marca en el *checkbox* para estar de acuerdo con las condiciones y términos del servicio, y se hace click en *I Agree, Sign Me UP*, como se presenta en la Figura 4.5.

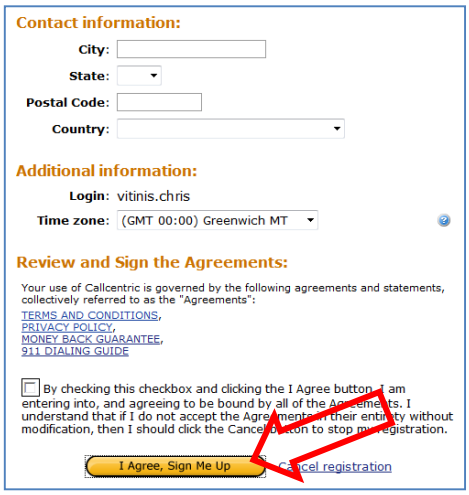

Figura. 4.5. Acuerdo de las condiciones y términos del servicio.

Finalmente aparecerá una nueva ventana en la cual se deberá hacer click en *Go to my Call CallCentric*, en la parte superior izquierda se encuentra la información del usuario, como también el numero SIP asignado que comienza con 1777 precedido por el nombre *Callcentric #*, como se presenta en la Figura 4.6.

Figura. 4.6. Número SIP o número CallCentric.

Para poder realizar llamadas desde de la Internet hacia teléfonos fijos, es necesario añadir fondos (*add funds*) o comprar saldo. De la misma forma para poder recibir llamadas desde teléfonos fijos tradicionales y teléfonos celulares es necesario comprar un número de teléfono, el cual puede ser seleccionado dentro de varias aéreas en los Estados Unidos.

4.3 CONFIGURACIÓN DEL ROUTER INALÁMBRICO

Para el desarrollo de la red inalámbrica Wi-Fi se utilizó router *Linksys* por Cisco *Wireless N Gigabit* modelo WRT310N v2, como se presenta en la Figura 4.7.

Figura. 4.7. Router Linksys Wireless N Gigabit WRT310.

4.3.1 Descripción del router Linksys Wireless N Gigabit WRT310Nv2

Este router cuenta con las siguientes características principales:

- ✓ Ruteador y *switch* de 4 puertos Gigabit para compartir internet, con un sistema incorporado de velocidad y punto de acceso inalámbrico (*Wireless*) con un mejorado rango de alcance.
- ✓ Tecnología *Wireless*-N utiliza múltiples radios por banda para crear señales robustas para maximizar el alcance y velocidad,
- ✓ Mucho más rápido que *Wireless*-G, pero también funciona bien con dispositivos *Wireless*-G y-B.
- ✓ *Switch* de 4 puertos Gigabit que ofrece velocidades de cable que son 10 veces más rápido que las conexiones 10/100 *Fast Ethernet*.
- ✓ *Wi-Fi Protected Setup* ayuda a que la configuración inalámbrica sea segura con simplemente pulsando un botón.
- ✓ Las señales inalámbricas se encuentran protegidas por *industrial-strength* cifrado WPA2, y su red está protegida de los ataques más conocidos de Internet mediante un potente firewall SPI. Encriptación: WEP, WPA, WPA2.

- ✓ Fácil de instalar con una PC con *Windows* o *Mac*, dispone de un asistente de configuración de Cisco.
- ✓ Todos los puertos admiten velocidad Gigabit y una auto negociación (MDI / MDI-X), no hay necesidad de cables cruzados.
- ✓ Cumple con los estándares IEEE 802.11 b, 802.11g y el estándar 802.11n borrador (draft) versión 2.0.
- ✓ Numero de antenas: 3.
- ✓ Potencia RF (EIRP): 17 dBm.
- ✓ Banda Wireless: 2.4 GHz.
- ✓ Clave de seguridad en bits: 64, 128.

4.3.2 Instalación y configuración del router Linksys WRT310Nv2

Este router dispone de un asistente de configuración por Cisco en CD, los pasos a seguir son los siguientes:

Paso 1.- Insertar el asistente de configuración en el dispositivo CD-ROM, y seleccionar *Star Setup* en el menú principal, como se presenta en la Figura 4.8.

Figura. 4.8. Instalación del router Linksys: Paso 1.

Paso 2.- Se selecciona *Next* para continuar con el proceso de instalación, como se presenta en la Figura 4.9.

Figura. 4.9. Instalación del router Linksys: Paso 2.

Paso 3.- Marcar en el *checkbox* (*I accept this agreement*) para estar de acuerdo con las condiciones y términos de la licencia, seleccionar *Next* para continuar, como se presenta en la Figura 4.10.

Figura. 4.10. Instalación del router Linksys: Paso 3.

Paso 4.- Desconectar el actual cable Ethernet (o del Internet) de la computadora y conectar en el puerto amarillo etiquetado “Internet” del nuevo router Linksys, seleccionar *Next* para continuar, como se presenta en la Figura 4.11.

Figura. 4.11. Instalación del router Linksys: Paso 4.

Paso 5.- Este router incluye un cable azul Ethernet, conectar un extremo de este cable en el puerto número 1 del router Linksys, de la misma forma conectar el otro extremo del cable en la computadora, seleccionar *Next* para continuar, como se presenta en la Figura 4.12.

Figura. 4.12. Instalación del router Linksys: Paso 5.

Paso 6.- Conectar el cable de alimentación al router Linksys, seleccionar *Next* para continuar, como se presenta en la Figura 4.13.

Figura. 4.13. Instalación del router Linksys: Paso 6.

Paso 7.- Finalmente conectar el cable de alimentación a la toma eléctrica, seleccionar *Next* para continuar, como se presenta en la Figura 4.14.

Figura. 4.14. Instalación del router Linksys: Paso 7.

Paso 8.- Los pasos siguientes corresponden a la configuración del router. Ingresar un *password* para proteger la administración del router, seleccionar *Next* para continuar, como se presenta en la Figura 4.15.

Figura. 4.15. Configuración del router Linksys: Paso 8.

Paso 9.- Ingresar el nombre de la red inalámbrica, conocido como SSID, esto ayudará a identificar la red, seleccionar *Next* para continuar, como se presenta en la Figura 4.16.

Figura. 4.16. Configuración del router Linksys: Paso 9.

Paso 10.- Se selecciona el método de seguridad para la red inalámbrica. Para el desarrollo de la red inalámbrica se utilizó el método de seguridad WEP, con la clave de seguridad generada aleatoriamente por el router, seleccionar *Next* para continuar, como se presenta en la Figura 4.17.

Figura. 4.17. Configuración del router Linksys: Paso 10.

Paso 11.- Seleccionar *Next* para continuar, como se presenta en la Figura 4.18.

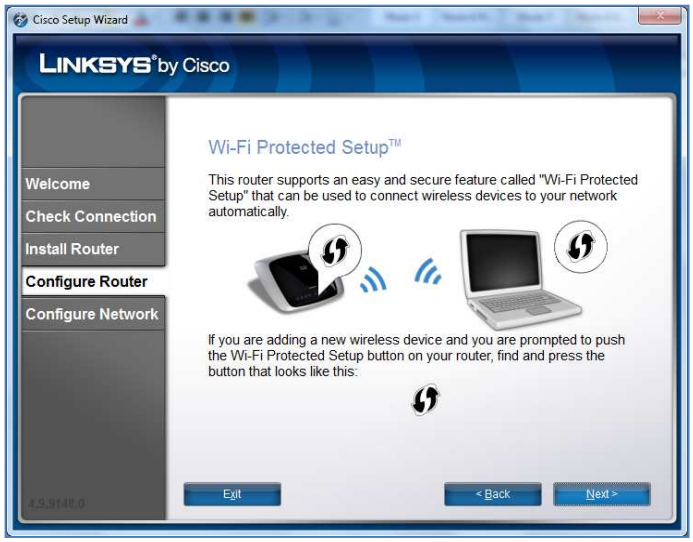

Figura. 4.18. Configuración del router Linksys: Paso 11.

Paso 12.- Seleccionar *Next* para continuar, como se presenta en la Figura 4.19.

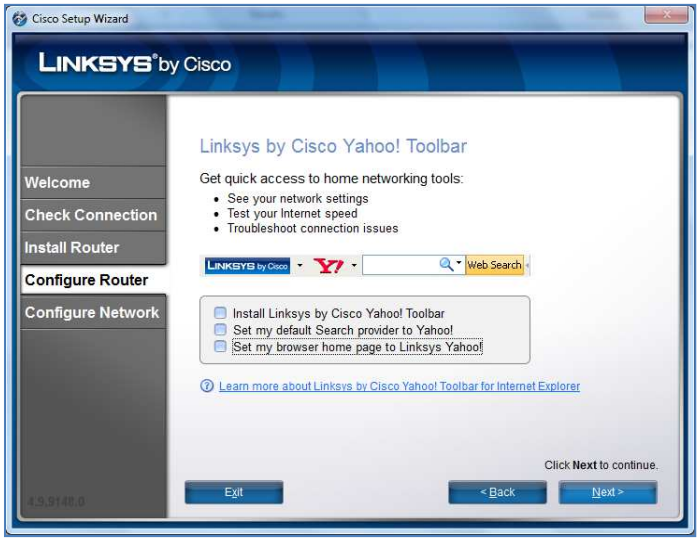

Figura. 4.19. Configuración del router Linksys: Paso 12.

Paso 13.- Se muestran las configuraciones realizadas y se confirma, seleccionar *Next* para finalizar el proceso configuración, como se presenta en la Figura 4.20.

Figura. 4.20. Configuración del router Linksys: Paso 13.

4.3.3 Acceso a la configuración de la red inalámbrica vía Web

Para acceder a la configuración de la red inalámbrica vía web, se debe abrir un navegador web (*web browser*), e introducir la dirección IP del router, por defecto la dirección es: 192.168.1.1, en el campo de Dirección y presionar la tecla *Enter*. Aparecerá una pantalla de inicio, cuando se solicite, dejar en nombre de usuario en blanco y escribir la contraseña por defecto: *"admin"*, seleccionar *Aceptar* para continuar, como se presenta en la Figura 4.21.

Figura. 4.21. Pantalla de inicio de sesión del router Linksys.

A continuación aparecerá una nueva ventana principal de configuración en la cual se deberá hacer *click* en *Wireless* ubicado en el menú principal, como se presenta en la Figura 4.22.

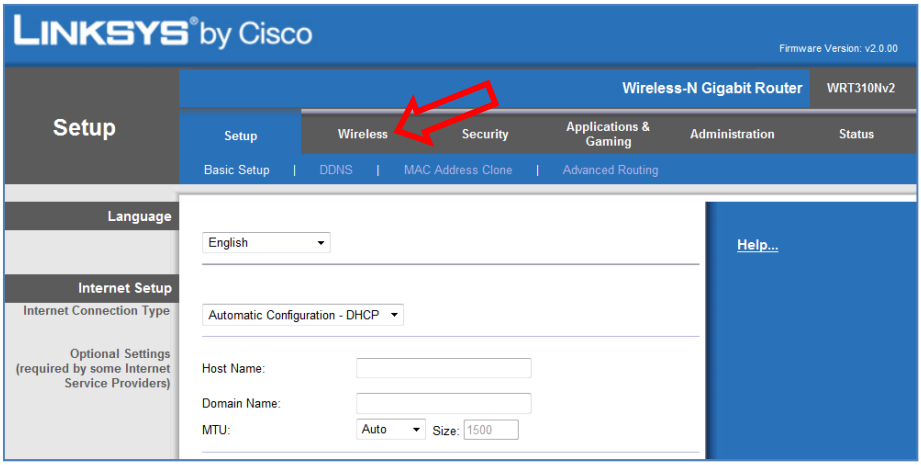

Figura. 4.22. Página principal de configuración.

Dentro del menú *Wireless* se puede gestionar la red inalámbrica, como la configuración inalámbrica básica (*Basic Wireless Settings*), Seguridad inalámbrica (*Wireless Security*), entre otros, como se presenta en las Figuras 4.23 y 4.24.

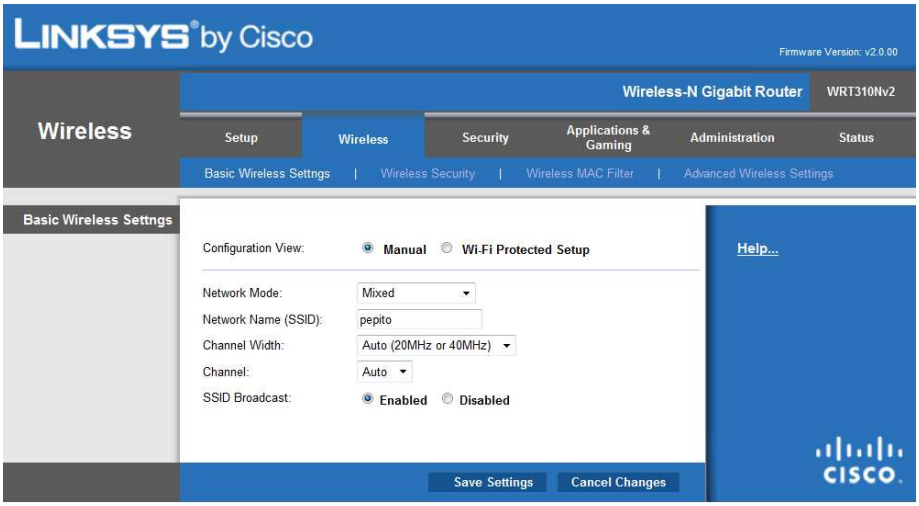

Figura. 4.23. Página Basic Wireless Settings.

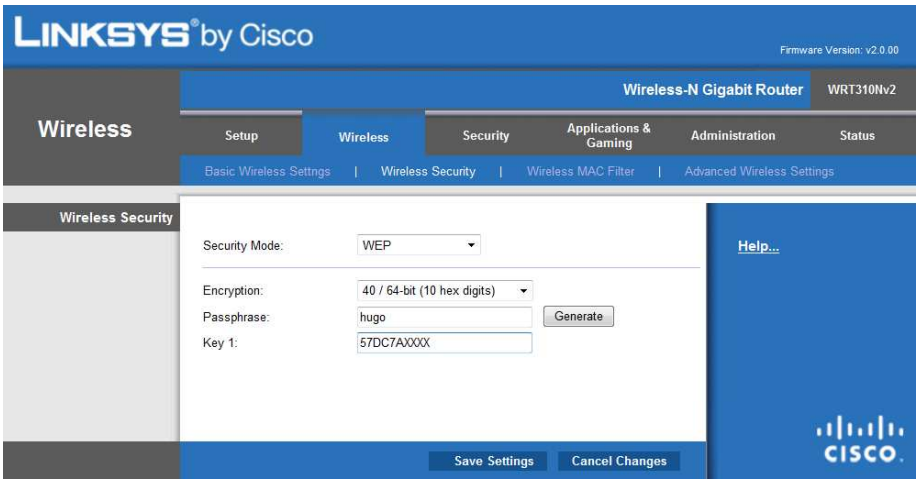

Figura. 4.24. Página Wireless Security.

4.4 CONFIGURACIÓN DE LOS DISPOSITIVOS TERMINALES SIP

Los terminales físicos (hardware) tienen una apariencia como un teléfono convencional muy profesional. Los teléfonos SIP pueden también estar basados en software denominados *Softphone,* que no es otra cosa que un software que emula las funciones de un teléfono físico tradicional, permitiendo que cualquier computador pueda ser utilizado como teléfono.

4.4.1 Lista de dispositivos terminales SIP

Hoy por hoy existe una gran cantidad de dispositivos terminales que soportan aplicaciones VoIP basados en SIP, estas aplicaciones se encuentran tanto en hardware como en software, los cuales están disponibles comercialmente gracias a muchos fabricantes. A continuación se muestra desde la Figura 4.25 hasta la Figura 4.28, una lista con los principales dispositivos terminales SIP, los cuales, el proveedor CallCentric ofrece soporte para cada uno de ellos

- ✓ **Dispositivos en Hardware (IP Phones / ATAs)**

Figura. 4.25. Dispositivos en Hardware (IP Phones / ATAs).

✓ Dispositivos en Software (Softphones)

Figura. 4.26. Dispositivos en Software (Softphones).

✓ Softphones móviles

Figura. 4.27. Softphones móviles.

✓ **Software IP PBX**

Figura. 4.28. Software IP PBX.

4.4.2 Dispositivo en Hardware: WLAN660-S Wi-Fi SIP Phone

Para el desarrollo del proyecto se utilizó el dispositivo terminal SIP en *hardware: WLAN660S Wi-Fi SIP Phone*, como se presenta en la Figura 4.29.

Figura. 4.29. Dispositivo WLAN660-S Wi-Fi SIP Phone.

El WLAN660 es un teléfono SIP inalámbrico (*Wireless*) basado en VoIP, el cual opera a través de internet, proporcionando los beneficios de la telefonía por internet, como por ejemplo, bajo costo en las llamadas, sin limitaciones físicas de una conexión fija a internet (proporcionando movilidad). Este teléfono permite realizar y recibir llamadas de Voz sobre IP, siempre y cuando este dentro de un rango de una red inalámbrica habilitada IEEE802.11b. Este teléfono es fácil de utilizar y configurar a través de su pantalla LCD y teclado. Inclusive es posible administrar la configuración a través de internet, mediante la configuración web del WLAN660.

Este teléfono cuenta con las siguientes características técnicas:

- ✓ Protocolo para el control de llamada: SIP (RFC2543/RFC3261).
- ✓ Codecs de voz: G711, G729.
- ✓ Interfaz de red: *Wireless* IEEE802.11b *Intersil Prism 3.0 CF module*.
- ✓ Rango de frecuencia: 2.4-2.497 GHz.
- ✓ Número de canales: hasta 14 canales.
- ✓ Velocidad de datos: 802.11b secuencia directa escala de 1, 2, 5.5, y 11Mbps.
- ✓ Potencia de salida: 30mW pico.
- ✓ Protocolo de red: TCP/IP, DHCP, IEEE 802.11b (802.11g compatible).
- ✓ Seguridad de red inalámbrica: *Wired Equivalent Privacy* (WEP) 64 y 128 bits.

- **Configuración de red**

En esta sección se configura el modo en que el teléfono accede a la red, el modo que se utilizó fue mediante: DHCP. Puesto que el router inalámbrico *Linksys* dispone de un servidor DHCP. Los pasos a seguir son los siguientes:

Paso 1.- En la pantalla principal, se presiona la tecla superior izquierda correspondiente a *Menú* para ingresar. Paso 2.- Se utiliza la tecla de flecha para desplazarse hacia abajo hasta *Net Settings*, se presiona la tecla correspondiente a *Select* para ingresar. Paso 3.- En la opción *Network Mode*, se presiona *Select*, finalmente se escoge la opción DHCP. Este proceso se presenta en la Figura 4.30.

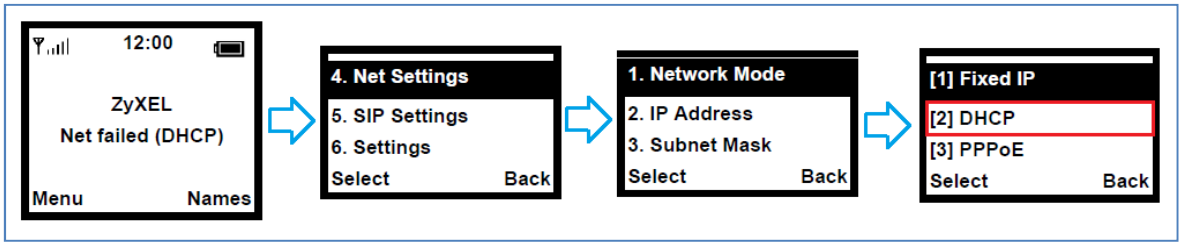

Figura. 4.30. Configuración de red del teléfono WLAN660.

- **Conexión a una red Wireless**

Para acceder a una red inalámbrica específica se realizan los siguientes pasos: Paso 1.- En la pantalla principal, se presiona la tecla superior izquierda correspondiente a *Menú* para ingresar. Paso 2.- Se utiliza la tecla de flecha para desplazarse hacia abajo hasta *Wireless*, se presiona la tecla correspondiente a *Select* para ingresar. Paso 3.- En la opción *Site Survey*, se presiona *Select*, el dispositivo empieza a buscar y muestra una lista de todas las redes inalámbricas disponibles. Finalmente se escoge la red inalámbrica deseada presionando *Select*. Este procedimiento se presenta en la Figura 4.31.

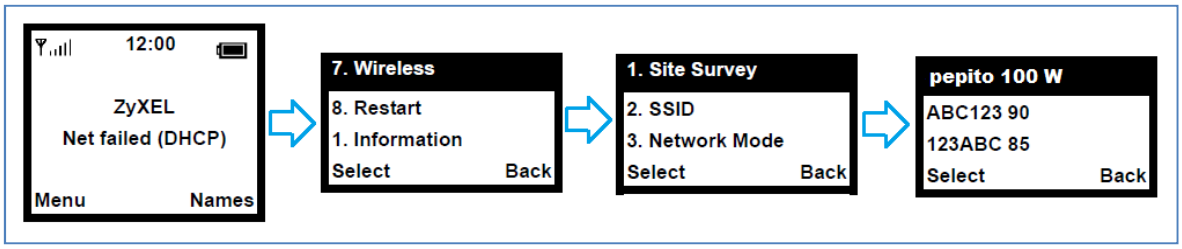

Figura. 4.31. Conexión a una red Wireless del teléfono WLAN660.

- **Configuración para utilizar una clave de encriptación WEP**

Para ingresar una clave WEP se realizan los siguientes pasos: Paso 1.- Dentro del menú *Wireless*, se utiliza la tecla de flecha para desplazarse hacia abajo hasta *WEP Select*, se presiona la tecla *Select* para ingresar. Paso 2.- Se desplaza y se escoge la longitud de la clave WEP (64 ó 128 bits) que utiliza la red inalámbrica, para seleccionar se presiona *Select*. Paso 3.- Se desplaza hacia abajo y se selecciona la clave WEP (*WEP key*) presionando *Select* (la mayoría de las redes utilizan por defecto *WEP key 1*). Paso 4.- Se ingresa la clave WEP de la red inalámbrica. Paso 5.- Se presiona la tecla correspondiente a *OK* para finalizar. Este procedimiento se presenta en la Figura 4.32.

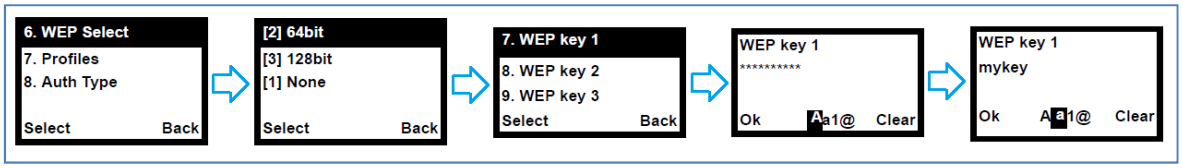

Figura. 4.32. Configuración de una clave WEP del teléfono WLAN660.

Paso 6.- Es posible configurar hasta cuatro claves WEP, pero solo una clave puede ser seleccionada o activada en un momento dado. Paso 7.- Se desplaza hasta *Key Select*, se presiona la tecla *Select* para ingresar. Paso 8.- Se desplaza y se selecciona la clave WEP que la red inalámbrica está utilizando. Se presiona la tecla correspondiente a *Select* para finalizar. Este procedimiento se presenta en la Figura 4.33. Finalmente para guardar todas las configuraciones y regresar a la pantalla principal, se presiona dos veces la tecla superior derecha correspondiente a *Back*.

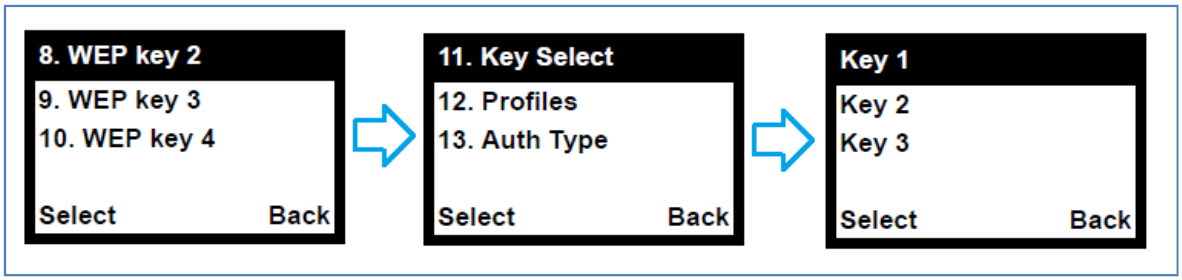

Figura. 4.33. Se selecciona la clave WEP del teléfono WLAN660.

- **Configuración vía Web**

Para acceder a la configuración del teléfono WLAN660 vía web, se debe abrir un navegador web, e introducir la dirección IP del teléfono, (para obtener la dirección IP del teléfono, se presiona la tecla correspondiente a *Menú*, opción *Information*, *IP address*). Aparecerá una pantalla de inicio, ingresar en nombre de usuario: "*voipadmin*", en contraseña: "*admin*", seleccionar *Aceptar* para continuar, como se presenta en la Figura 4.34.

Figura. 4.34. Pantalla de inicio de sesión del teléfono WLAN660.

A continuación aparecerá una nueva ventana la cual contiene información del dispositivo, como por ejemplo la versión software. En el lado derecho se encuentra el menú de opciones, cada opción es un enlace a su correspondiente pantalla, como se presenta en Figura 4.35.

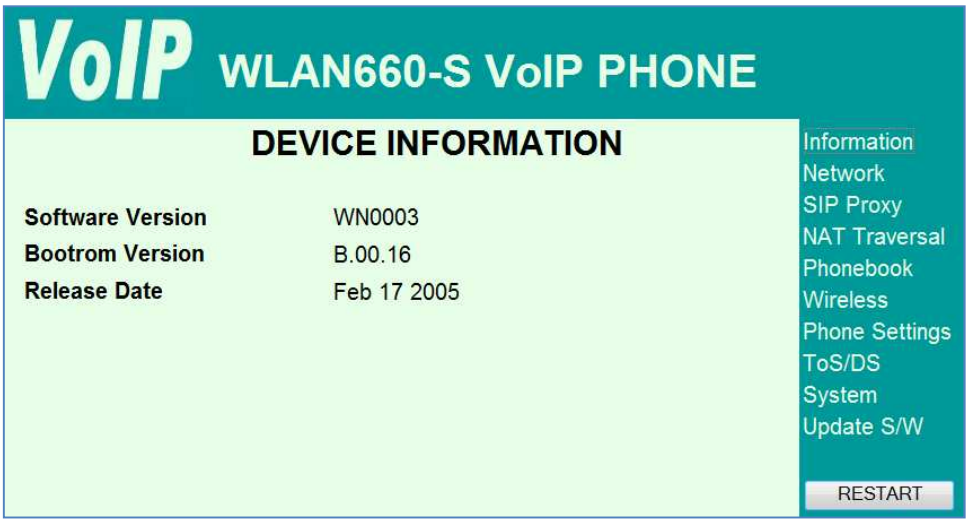

Figura. 4.35. Pantalla configuración web: información del dispositivo.

En la siguiente pantalla se puede realizar la configuración de red, para el proyecto se utilizó DHCP, como se presenta en Figura 4.36.

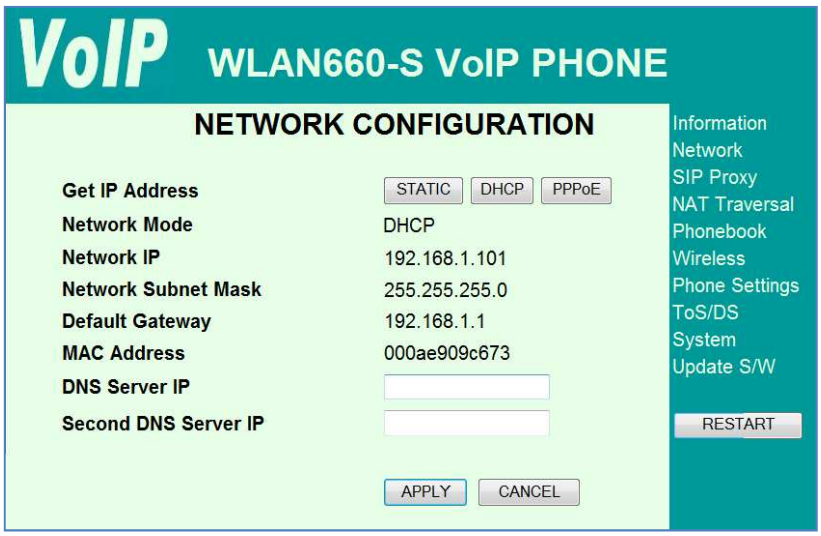

Figura. 4.36. Pantalla configuración web: configuración de red.

En la siguiente pantalla se presenta la configuración SIP, en la cual se ingresa la información proporcionada por el proveedor de servicio VoIP *CallCentric*, esta información es la siguiente:

- *SIP URI sip*: Se ingresa el número de *CallCentric*, este número comienza en 1777 con 7 dígitos adicionales
- *SIP Server Address*: callcentric.com
- *SIP Server Port*: 5060
- *Registrar Server Address*: callcentric.com
- *Registrar Server Port*: 5060
- *Register Expiry Time*: 3600
- *Display name*: Se ingresa el nombre del usuario
- *Registrar Username*: Se ingresa el número de *CallCentric*
- *Registrar Password:* Se ingresa el mismo password que se utilizó para registrarse en la cuenta de *CallCentric*

Después de ingresar la información indica, se hace *click* en *Apply*, posteriormente se puede verificar el estado de la registración del teléfono, esto se muestra con la palabra: *Registered*, como se presenta en Figura 4.37.

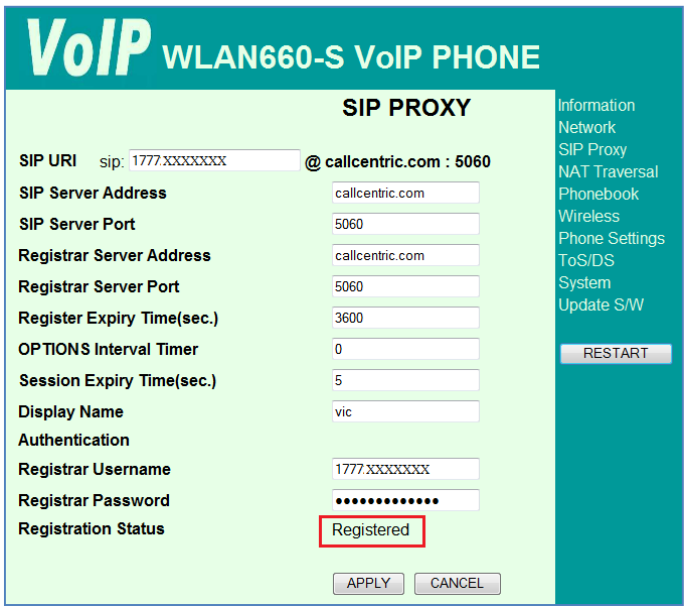

Figura. 4.37. Pantalla configuración web: configuración SIP.

A continuación se presenta en las Figuras 4.38 y 4.39 la configuración Wireless y la configuración del teléfono respectivamente.

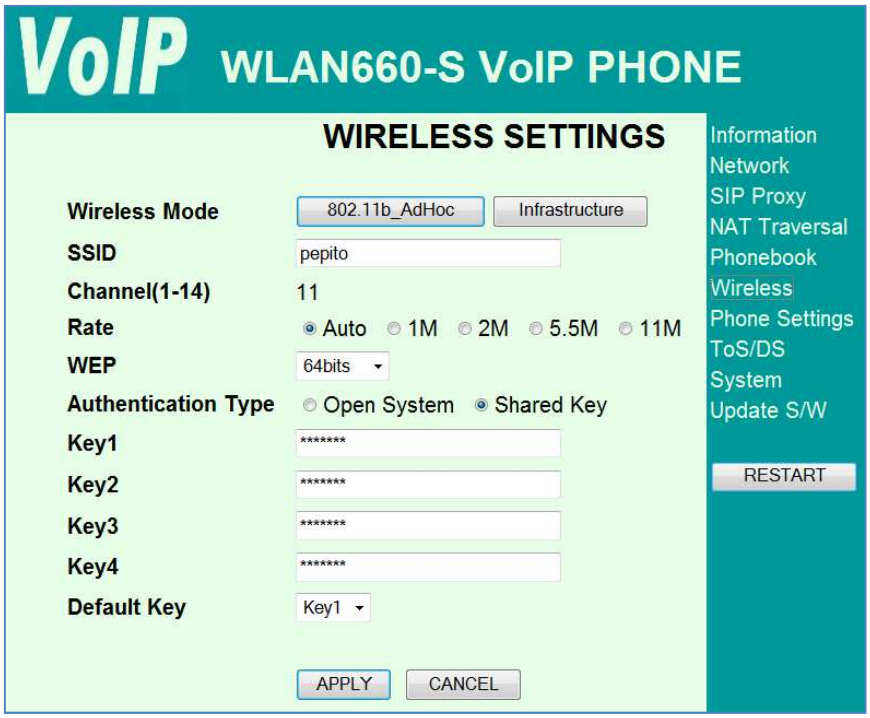

Figura. 4.38. Pantalla configuración web: configuración Wireless.

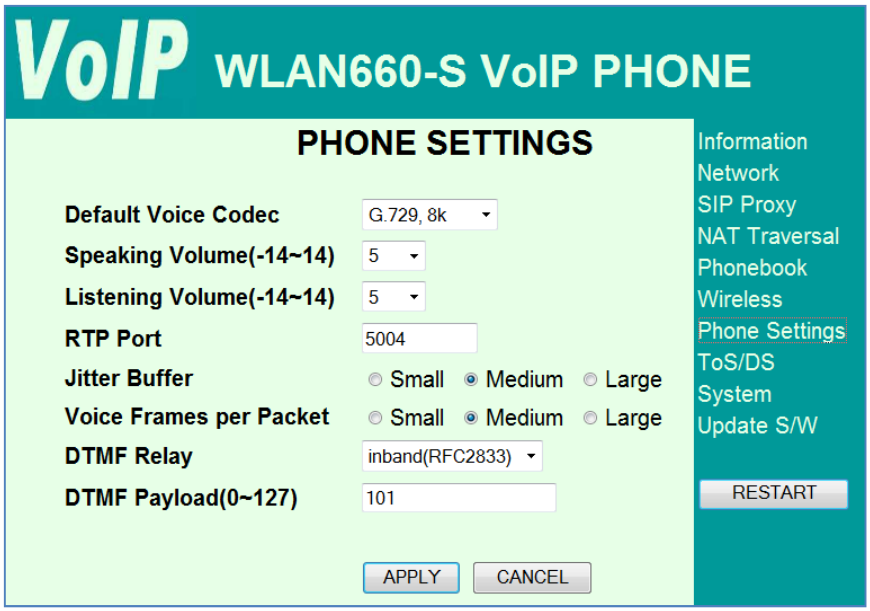

Figura. 4.39. Pantalla configuración web: configuración del teléfono.

4.4.3 Dispositivo en Software: Softphone X-Lite versión 4.0

Para el desarrollo del proyecto se utilizó el dispositivo terminal SIP en *software:* el *Softphone* X-Lite versión 4.0.

X-Lite es un *software* de VoIP que utiliza el Protocolo de Inicio de Sesiones, X-Lite ha sido desarrollado por *CounterPath Corporation*, es una compañía de *software* fundada en Vancouver. *CounterPath* ofrece una serie de *Softphones* los cuales funcional bien con *CallCentric* y están disponibles tanto para *Windows, Mac* OS X y Linux.

En septiembre de 2010 [11], *CounterPath* publicó la disponibilidad de X-Lite 4.0, el cual incorpora muchas características de X-lite 3.0, además cuenta con una interfaz de usuario rediseñada basada en el *Softphone Bria* de *CounterPath*. X-Lite 4.0 se encuentra disponible como una descarga gratuita.

- **Descarga e Instalación del Softphone X-Lite 4.0**

En la Tabla 4.1 se presenta los requerimientos del sistema para poder realizar la instalación del *Softphone* X-Lite 4.0.

Tabla. 4.1. Requerimientos del sistema.

Procesador	Mínimo: Pentium 4, 2.4 GHz o equivalente Optimo: Intel Core 2 Duo o equivalente
Memoria	Mínimo: 1 GB RAM Optimo: 2 GB RAM
Espacio Disco Duro	50 MB
Sistema Operativo	Windows XP Service Pack 2 Windows Vista
Adicional	Microsoft Windows Installer 3.1 Microsoft .NET 3.5 SP1 Microsoft VC 9.0 Runtime Service Pack 1
Conexión	Conexión de red IP (banda ancha, LAN, Wireless)
Tarjeta de Sonido	Full-dúplex, 16-bit o USB auricular

Los pasos para descargar este *Softphone* son muy sencillos, el usuario deberá ingresar al siguiente link:

http://www.counterpath.com/x-lite-download.html

Actualmente para el Softphone X-Lite versión 4.0, existe la posibilidad de descargar para dos sistemas operativos: Windows y Mac, como se presenta en la Figura 4.40.

Figura. 4.40. Sitio web CounterPath, descarga del Softphone.

Después de la descarga, primero, se realiza la ejecución, posteriormente se selecciona *Next* para continuar, seguido a esto, se acepta los términos del acuerdo de la licencia y se selecciona *Next*, *Next*, y finalmente *Install*. Este proceso de instalación se muestra desde la Figura 4.41 hasta la Figura 4.46.

Figura. 4.41. Ejecución del programa X-Lite 4.0.

Figura. 4.42. Inicio de la instalación.

Figura. 4.43. Aceptación de los términos del acuerdo de la licencia.

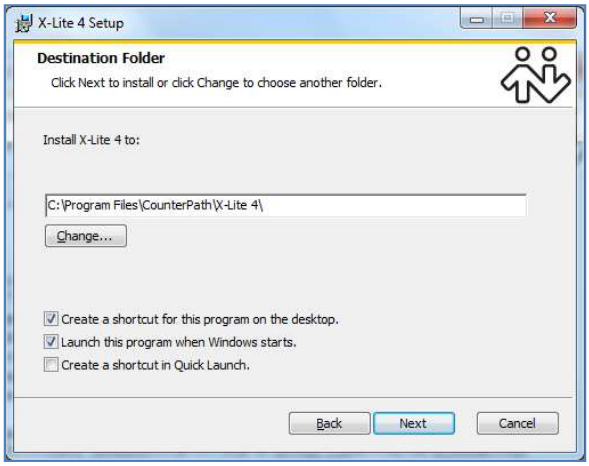

Figura. 4.44. Carpeta que contiene el programa X-Lite.

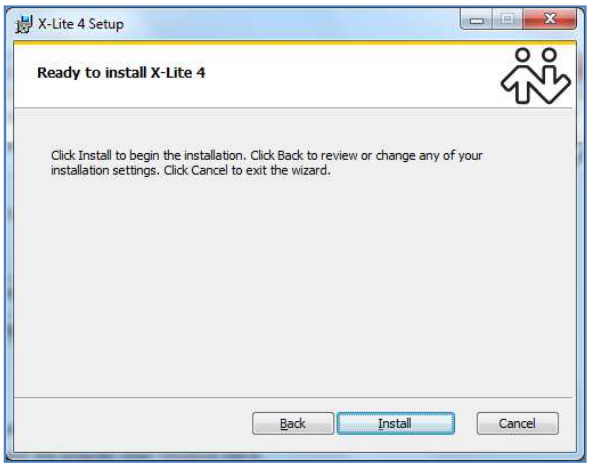

Figura. 4.45. Proceso de instalación.

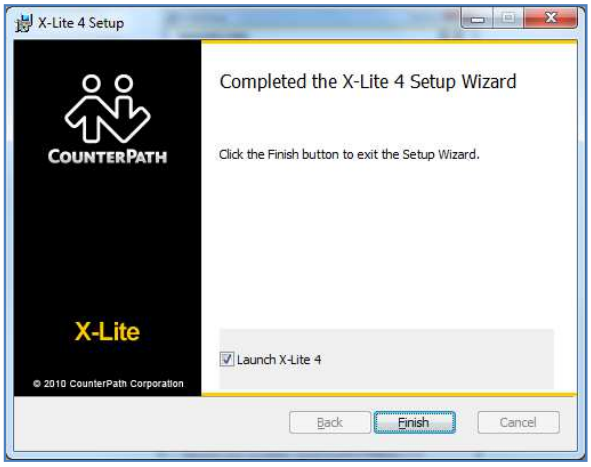

Figura. 4.46. Finalización de la instalación.

Después de instalar el programa se recomienda reiniciar el computador para que los cambios y aplicaciones asociadas al Softphone adquieran efecto y funcione sin problemas.

- **Configuración de la cuenta SIP en el Softphone X-Lite 4.0 para CallCentric**

Para realizar la configuración de la cuenta SIP se realizan los siguientes pasos: Paso 1.- Se selecciona *Softphone* en el menú principal, ubicado en la parte superior del programa, donde aparecerá la opción *Account Settings* y se selecciona, como se presenta en la Figura 4.47.

Figura. 4.47. Configuración de la cuenta SIP en el Softphone X-Lite 4.0.

Paso 2.- Posteriormente aparecerá una ventana denomina *SIP Account*, en la pestaña *Account* (Cuenta), se configura la información proporcionada por el proveedor de servicio VoIP *CallCentric*, esta información es la siguiente: *Account name, User ID, Domain, Password, Display name,*y *Authorization name.*

- *Account name*: Es el nombre del usuario la cuenta.
- *User ID*: Es el número de *CallCentric*, este número comienza en 1777 con 7 dígitos adicionales.
- *Domain*: Es el dominio o Servidor proxy para conectarse a la red de la empresa que provee la Telefonía IP, en este caso es: callcentric.com
- *Password*: Es la misma contraseña que se utilizó para registrarse en la cuenta de *CallCentric.*
- *Display name*: Es la información que aparecerá en la pantalla del *Softphone* X-Lite.
- *Authorization name*: Es el número de *CallCentric*, este número comienza en 1777 con 7 dígitos adicionales.

Adicionalmente debe estar marcado el *checkbox: Register with domain and receive calls*, de misma forma el botón *Domain.* También en el plan de marcación (*Dial plan*) debe estar por defecto: #1\a\a.T;match=1;prestrip=2;. Esta ventana se presenta en la Figura 4.48.

Figura. 4.48. Ventana SIP Account X-Lite 4.0.

Paso 3.- Dentro de la pestaña *Topology*, asegurarse de que las configuraciones estén, como se muestra en la Figura 4.49.

Figura. 4.49. Ventana Topology X-Lite 4.0.

Paso 4.- Dentro de la pestaña *Advanced*, asegurarse de que las configuraciones estén, para guardar y finalizar la configuración se hace *click* en el botón *OK*, como se muestra en la Figura 4.50.

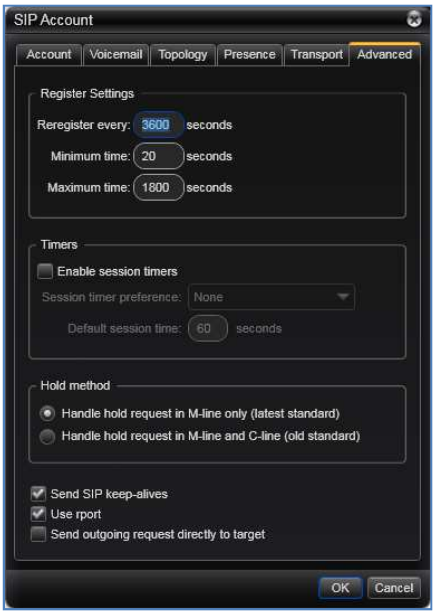

Figura. 4.50. Ventana Advanced X-Lite 4.0.

Paso 5.- A continuación el *Softphone* X-Lite tratará de registrarse (*login*) con el servidor de *CallCentric*. Se puede observar que esto sucede en pocos segundos y si el registro tiene éxito, se observará la siguiente pantalla, la cual se presenta en la Figura 4.51.

Figura. 4.51. Interfaz principal X-Lite 4.0: Registro exitoso.

Paso 6.- Una vez que el registro ha sido exitoso, el usuario está en la capacidad de realizar y recibir llamadas telefónicas.

4.4.4 Analizador de protocolos: Wireshark

Cuando se trabaja en el mundo de la telefonía IP es fundamental utilizar un analizador de protocolos de red, o también conocidos como: analizadores de paquetes, *packet sniffer* o *sniffer*. Con el propósito de entender como está circulando el trafico por la red. Para la captura y el análisis de los paquetes de Voz sobre IP se utilizó el analizador de protocolos *Wireshark.* Esta herramienta multiplataforma antes fue conocida como *Ethereal.*

Wireshark es un analizador de protocolos utilizado para realizar análisis de aplicaciones en tiempo real, como la telefonía IP. Además permite solucionar problemas en redes de comunicaciones, tanto de paquetes enviados como recibidos. *Wireshark* al mismo tiempo de soportar una gran cantidad de protocolos, permite filtrar, con el propósito de analizar específicamente al protocolo SIP.

- **Instalación de Wireshark**

Wireshark es software libre (licencia GPL: *General Public License*), y se ejecuta sobre la mayoría de sistemas operativos. Esta herramienta se puede descargar ingresando al siguiente link:

http://www.wireshark.org/

Se selecciona la opción *Download Wireshark* como se presenta en la Figura 4.52.

Figura. 4.52. Sitio web para descargar Wireshark.

Después de la descarga del instalador, primero, se realiza la ejecución del archivo descargado para iniciar la instalación. Posteriormente se selecciona *Next* para continuar, seguido a esto, se acepta los términos del acuerdo de la licencia seleccionando *I Agree*. A continuación se despliega una ventana para seleccionar los componentes que se desea instalar (se recomienda seleccionar todos los componentes), y se selecciona *Next* para continuar. Seguidamente aparecerá una pantalla en la cual permite seleccionar: crear un acceso directo en el escritorio, crear un menú de inicio y visualizar el icono en la barra de tareas, de la misma manera se permite asociar las extensiones de archivo de rastreo para *Wireshark*, y se selecciona *Next* para continuar. A continuación se selecciona el directorio donde se instalará esta aplicación, se acepta la carpeta indicada por defecto del instalador, y se selecciona *Next* para continuar.

Este instalador contiene una versión de *WinPcap*, se verifica y selecciona para actualizar la versión, y se selecciona *Install* para iniciar el proceso de instalación. Después que se haya finalizado la instalación exitosamente se selecciona *Next*. Finalmente se puede seleccionar correr la aplicación *Wireshark* para ejecutar el programa, seleccionando *Finish.* A continuación se desplegará la pantalla principal del analizador *Wireshark*, como se muestra en la Figura 4.53.

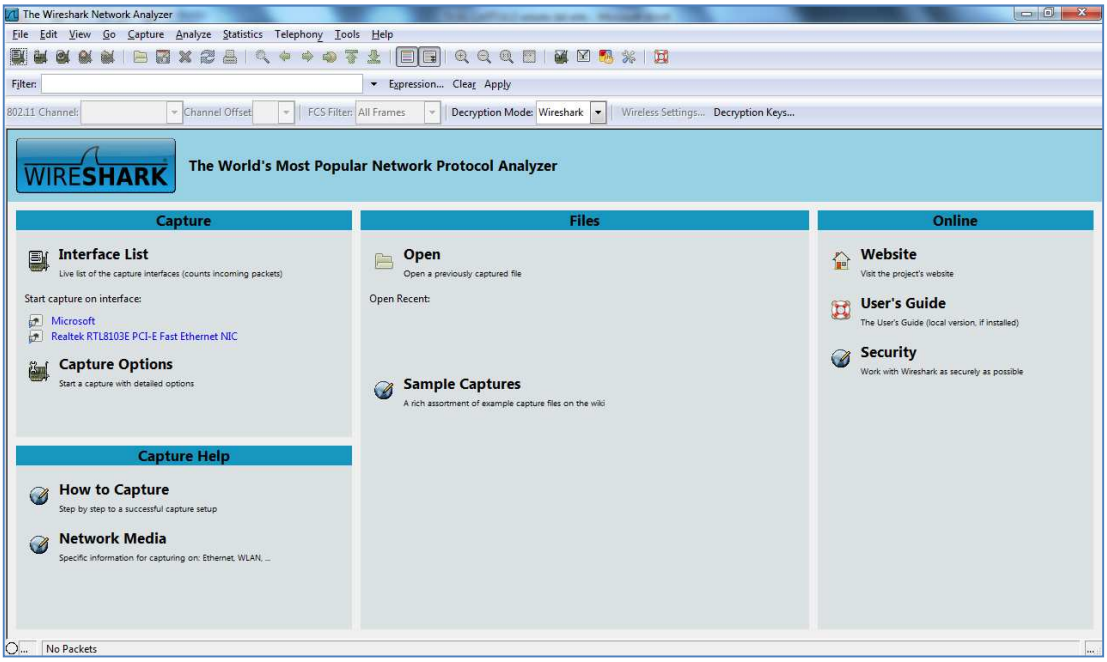

Figura. 4.53. Pantalla principal del analizador Wireshark.

- **Captura de Paquetes**

Antes de iniciar la captura de los paquetes se debe seleccionar una interfaz por donde se desea capturar la información de la red. Se selecciona *Capture* en el menú principal, posteriormente se selecciona *Interfaces*, como se presenta en la Figura 4.54.

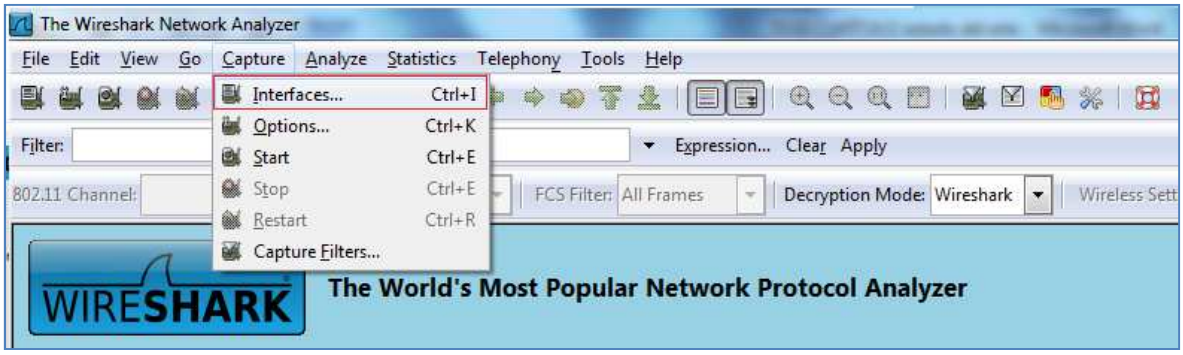

Figura. 4.54. Ingreso a las interfaces.

A continuación se despliega una nueva ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes, en la cual tres botones se presentan por cada interfaz:

- *Start:* para iniciar la captura de paquetes.
- *Options*: para configurar.
- *Details*: proporciona información adicional de la interfaz.

La ventana *Wireshark: Capture Interfaces* se presenta en la Figura 4.55.

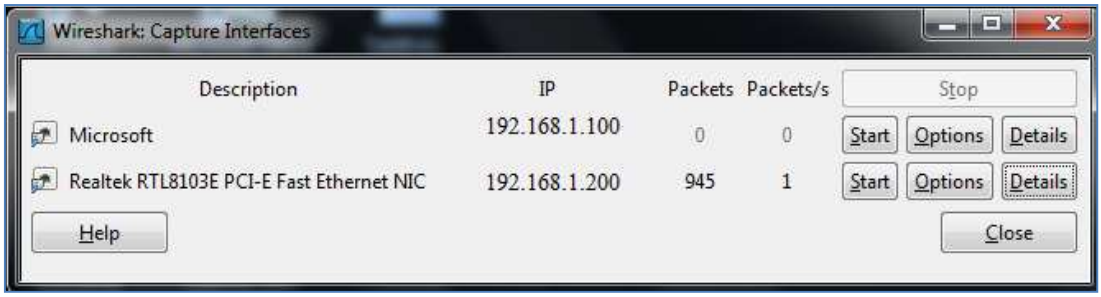

Figura. 4.55. Ventana Wireshark: Capture Interfaces.

CAPÍTULO V

OBTENCIÓN Y ANÁLISIS DE RESULTADOS

En el presente capítulo se describe la obtención y análisis de resultados en las pruebas de funcionamiento realizadas a los dispositivos terminales SIP: en *software* el *Softphone* X-Lite 4.0 y en *hardware* el teléfono WLAN660. Para la captura y el análisis de los paquetes de Voz sobre IP se utilizó el analizador *Wireshark,* la captura se realiza desde la computadora en la cual se encuentra instalado el *Softphone*.

5.1 LLAMADA ENTRE SOFTPHONE X-LITE Y TELÉFONO WLAN660

Este escenario de prueba se presenta en la Figura 5.1, en el cual se realiza el siguiente procedimiento:

- ✓ Empieza la captura de paquetes mediante *Wireshark.*
- ✓ Se realiza una llamada desde el Softphone X-Lite hacia el teléfono WLAN660.
- ✓ Se finaliza la llamada.
- ✓ Se detiene la captura de paquetes.

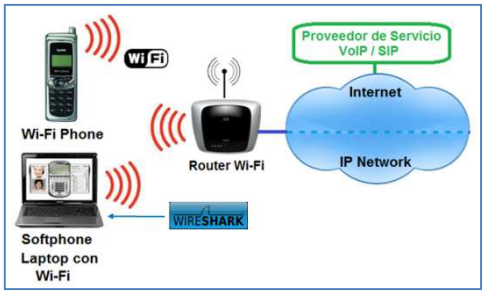

Figura. 5.1. Escenario de prueba: Llamada entre Softphone X-Lite y Teléfono WLAN660.

En las Figuras 5.2 y 5.3 se presenta la grafica del tráfico que está llegando al host (tráfico RTP). Para obtener estas graficas se selecciona *Statistics* en el menú principal de *Wireshark*, posteriormente se selecciona *IO Graphs*.

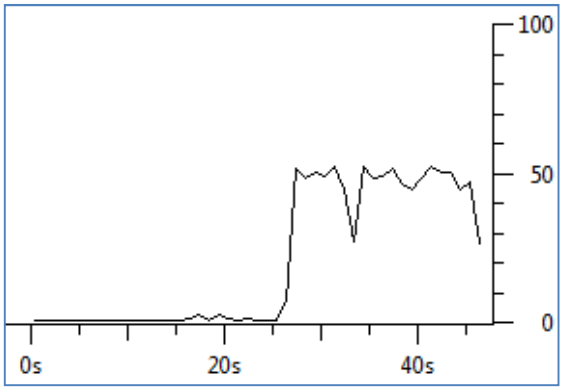

Figura. 5.2. Tráfico recibido en el host (paquetes / segundo).

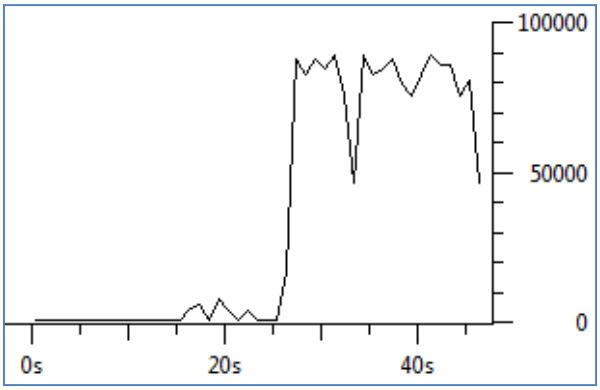

Figura. 5.3. Tráfico recibido en el host (bits / segundo).

- El ancho de banda aproximado de RTP es de 85Kpbs (G.711)

En la Figura 5.4 presenta los RTP Streams de la captura, se presenta dos streams por cada llamada. Para obtener estas ventana se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *RTP* y *Show All Streams*.

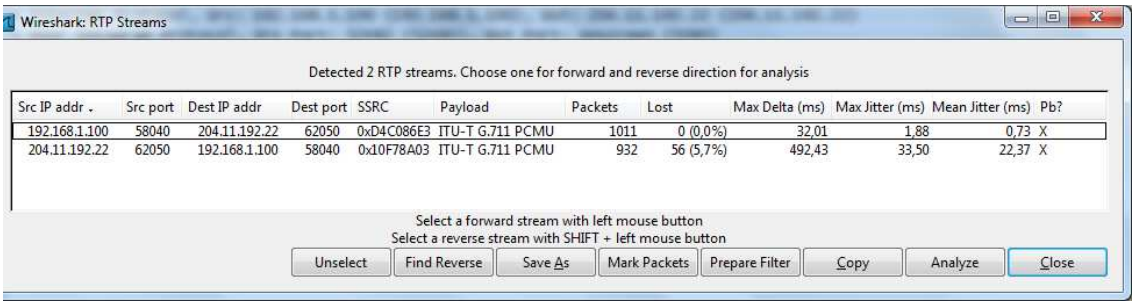

Figura. 5.4. Ventana RTP Streams.

En la tabla 5.1 se presenta los resultados de funcionamiento en el escenario de prueba: Llamada entre Softphone X-Lite y Teléfono WLAN660.

Tabla 5.1. Resultados de funcionamiento: Llamada entre Softphone X-Lite y Teléfono WLAN660.

Direcciones IP		**RTP Streams**				
Fuente	Destino	Paquetes	Perdidos	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.1.100	204.11.192.22	1011	0 (0,0%)	32,01	1,88	0,73
204.11.192.22	192.168.1.100	932	56 (5,7%)	492,43	33,50	22,37

Para obtener gráficamente el flujo de mensajes en una llamada VoIP, se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *VoIP Calls* (Figura 5.5), a continuación se escoge la llamada VoIP y se selecciona *Graph*, esta ventana se presenta en la Figura 5.6.

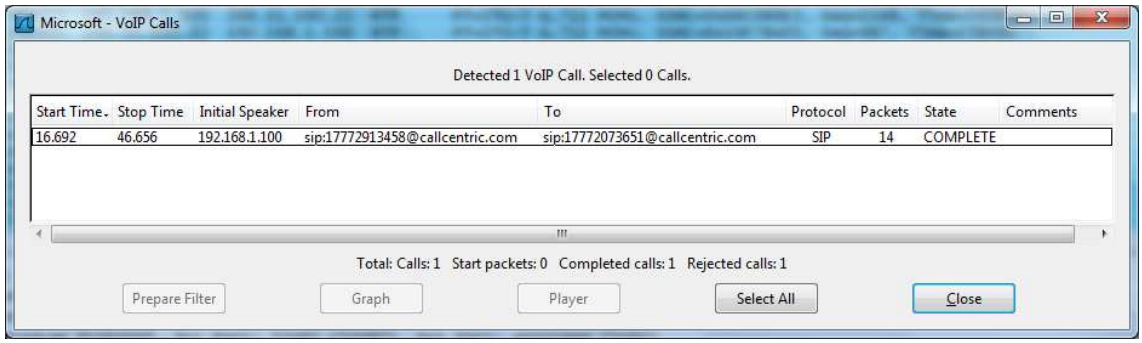

Figura. 5.5. Ventana VoIP Calls.

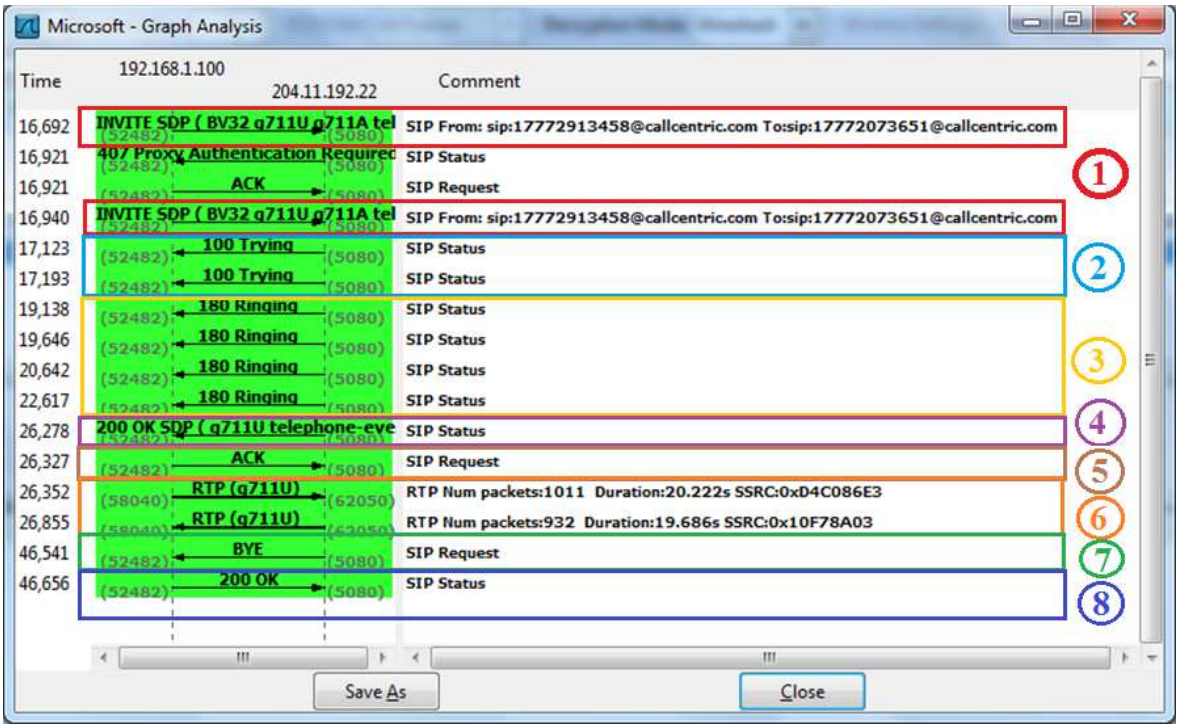

Figura. 5.6. Flujo de mensajes en una llamada VoIP: ventana Graph Analysis.

La Figura 5.6 presenta el intercambio teórico de mensajes SIP. Para el establecimiento de la llamada, se empieza con un mensaje *INVITE* (1) por parte del *Softphone.*

SIP para el control de señalización de llamada utiliza al protocolo SDP, el cual se envía conjuntamente con los mensajes *INVITE* y *200OK*, cabe aclarar que: el mensaje *INVITE* se envía desde el origen hacia el destino, y el mensaje *200OK* se envía desde el destino hacia el origen. Como se mencionó el protocolo SDP se encuentra embebido en SIP, donde usualmente los puertos utilizados por SIP son: el 5060 en texto plano (UDP y TCP) y el puerto 5061 en el caso de TLS[26]. No obstante, prácticamente se puede presentar la utilización de puertos comprendidos entre el 5060 hasta el 5080.

26 TLS (*Transport Layer Security*, en español Seguridad de la Capa de Transporte) es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.

Dentro del mensaje SDP se envían los parámetros a negociar como por ejemplo el listado de *Codecs* que soporta o está en la capacidad de trabajar tanto el terminal origen como destino, este códec se envía en orden de prioridad (BV32, g711U, g711A, GSM, entre otros). También se envía la IP, el puerto en el cual se desea recibir el audio mediante RTP. En el caso del mensaje *200OK* no siempre se envía SDP, porque existió un mensaje anterior que ya negoció estos parámetros.

Inmediatamente después de recibir la solicitud *INVITE,* se envía un mensaje de respuesta *100 Trying* (2) (recibí y estoy procesando la llamada), esto lo realiza para detener las retransmisiones del mensaje *INVITE*. A continuación se envía en el mismo sentido es decir, todas las respuestas provisionales generadas por el usuario destino son enviadas de vuelta al usuario origen, como por ejemplo el mensaje de respuesta *180 Ringing* (3) (el terminal esta timbrando), esta respuesta es generada cuando el teléfono empieza a timbrar.

Al momento de aceptar la comunicación, dicho en otras palabras cuando el usuario destino descuelga o contesta el auricular del teléfono, se retransmite un mensaje de respuesta *200 OK* (4) (atendí la llamada) con un mensaje SDP, proponiendo el codec a utilizarse (*g711U telephone-eve*), hacia el usuario origen, hasta que el usuario destino reciba un mensaje de confirmación *ACK* (5) (atendí la llamada) enviado por el usuario origen. En este punto la sesión se establece y además se establece la conversación mediante el envío de paquetes RTP (6) (audio/video RTP streams). Adicionalmente, en ciertos casos el terminal origen confirma la negociación con un mensaje *ACK*.

Para la finalización de la llamada, se lleva a cabo mediante el envío del mensaje de solicitud *BYE* (7), dentro del diálogo establecido por *INVITE.* El mensaje *BYE* se envía directamente desde un agente de usuario hacia el otro agente de usuario, a menos que un *proxy* que se encuentra en la trayectoria de la solicitud *INVITE,* haya indicado que desea permanecer en la ruta mediante el establecimiento del proceso *Record Routing (Registro de Ruta).* El usuario que desea finalizar la sesión, envía la solicitud *BYE* directamente al otro usuario involucrado en la sesión. El usuario que recibe la solicitud *BYE* envía una respuesta 200 OK (8) para confirmar la finalización de la sesión SIP.

En el establecimiento de la llamada, el primer mensaje enviado es el *INVITE*, a continuación se presenta en la Figura 5.7 la captura de este paquete.

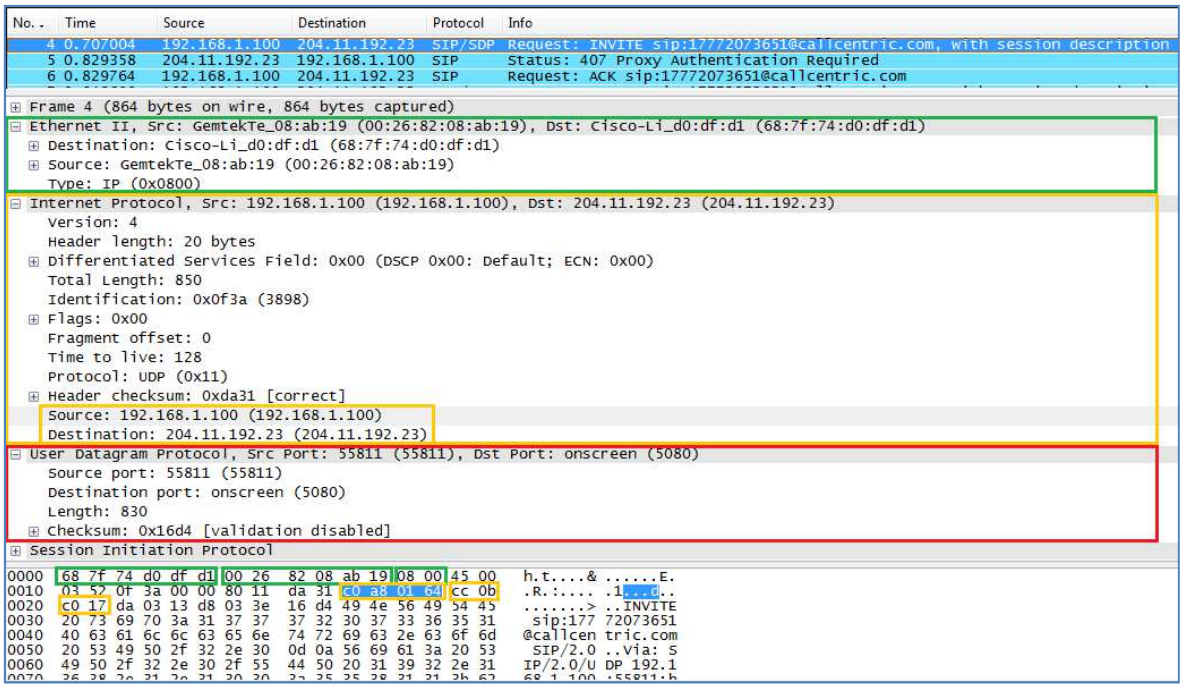

Figura. 5.7. Captura del mensaje INVITE.

En la Figura 5.7, se presenta en el recuadro superior de color verde, el encabezado de la trama en nivel de la capa Enlace, se observa que el protocolo utilizado es *Ethernet*. El término "*Ethernet*" se refiere a la familia de implementaciones de Redes de Área Local (LAN) una de las tres principales categorías es: 10 Mbps Ethernet e IEEE 802.3: especificaciones LAN que operan a 10 Mbps sobre cable coaxial.

En la captura es posible observar los campos de la trama MAC 802.3: dirección destino (*destination 6 bytes*), dirección origen (*source 6 bytes*), Tipo/Longitud (especifica el protocolo de red que encapsula, el cual es IP).

Dirección MAC de destino: 68 7f 74 d0 df d1 (dirección MAC local del *Router Linksys* por *Cisco*).

Dirección MAC de origen: 00 26 82 08 ab 19 (dirección MAC *Wireless* de la computadora)

Tipo/Longitud: 08 00

En el recuadro de color amarillo se presenta todos los campos del encabezado de IP (*Internet Protocol*), como por ejemplo: dirección IP fuente: 192.168.1.100 (dirección IP de la computadora, la cual generó el datagrama), dirección IP destino: 204.11.192.23 (servidor VoIP de *CallCentric*), entre otros.

En el recuadro de color rojo se presenta el encabezado con sus respectivos campos del mensaje UDP (*User Datagram Protocol*), es decir de la capa de transporte. Entre los campos de este mensaje UDP se tiene: puerto origen: 55811, puerto destino: 5080, entre otros.

El siguiente mensaje que se envía como respuesta al mensaje *INVITE* anterior, es el mensaje *TRYING*, a continuación se presenta en la Figura 5.8 la captura de este mensaje.

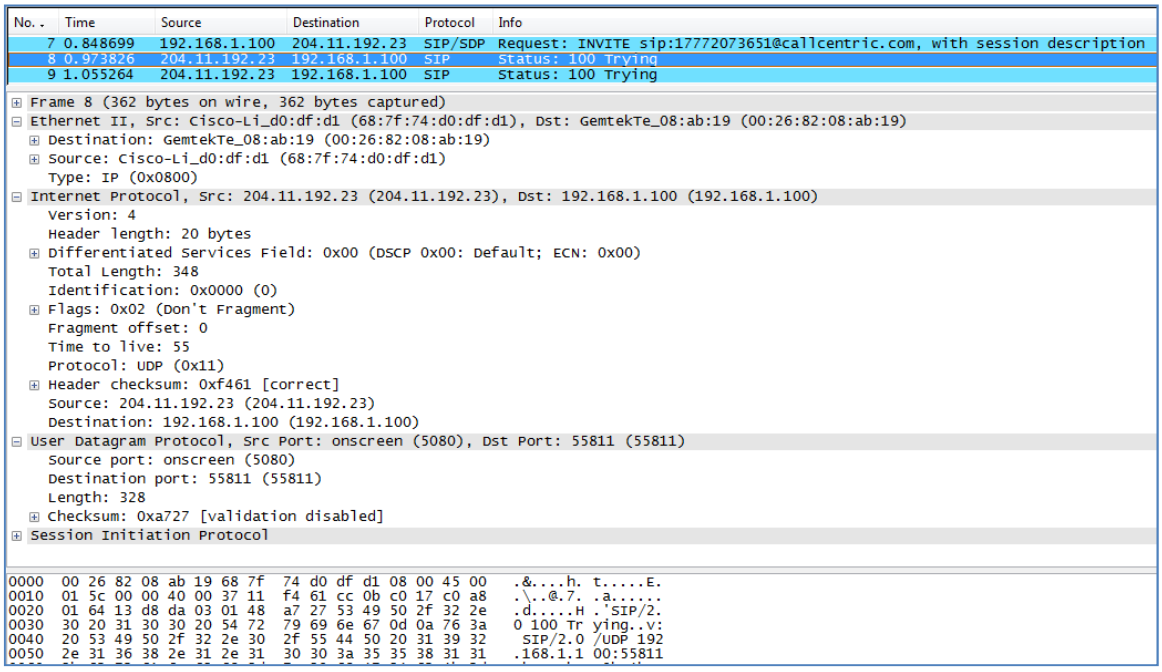

Figura. 5.8. Captura del mensaje TRYING.

En el nivel de enlace se observa que los campos de las direcciones MAC fuente y destino se invierten, puesto que la trama viaja en sentido inverso, desde el servidor VoIP hacia el *Softphone*. De la misma forma en el nivel de red, las direcciones IP han sido invertidas, como también los puertos UDP.

El siguiente mensaje que se envía es el mensaje *RINGING*, el sentido de este datagrama es el mismo que el mensaje anterior (*Trying*), a continuación se presenta en la Figura 5.9 la captura de este mensaje.

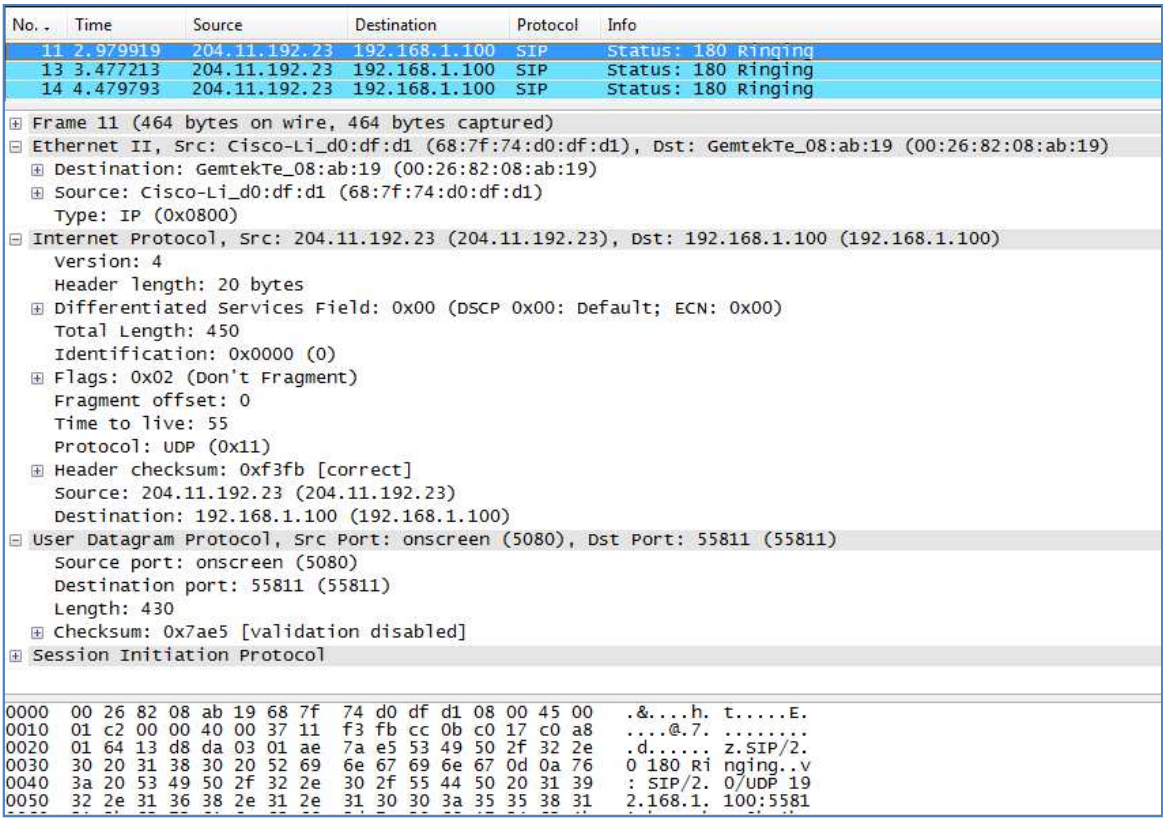

Figura. 5.9. Captura del mensaje RINGING.

Los campos de direcciones MAC, IP y puertos UDP, son los mismos que el mensaje anterior (*Trying*), puesto que el mensaje viaja en el mismo sentido, desde el servidor VoIP hacia el *Softphone*.

El siguiente mensaje que se envía es el mensaje *200 OK*, enviado desde el servidor VoIP, a continuación se presenta en la Figura 5.10 la captura de este mensaje.

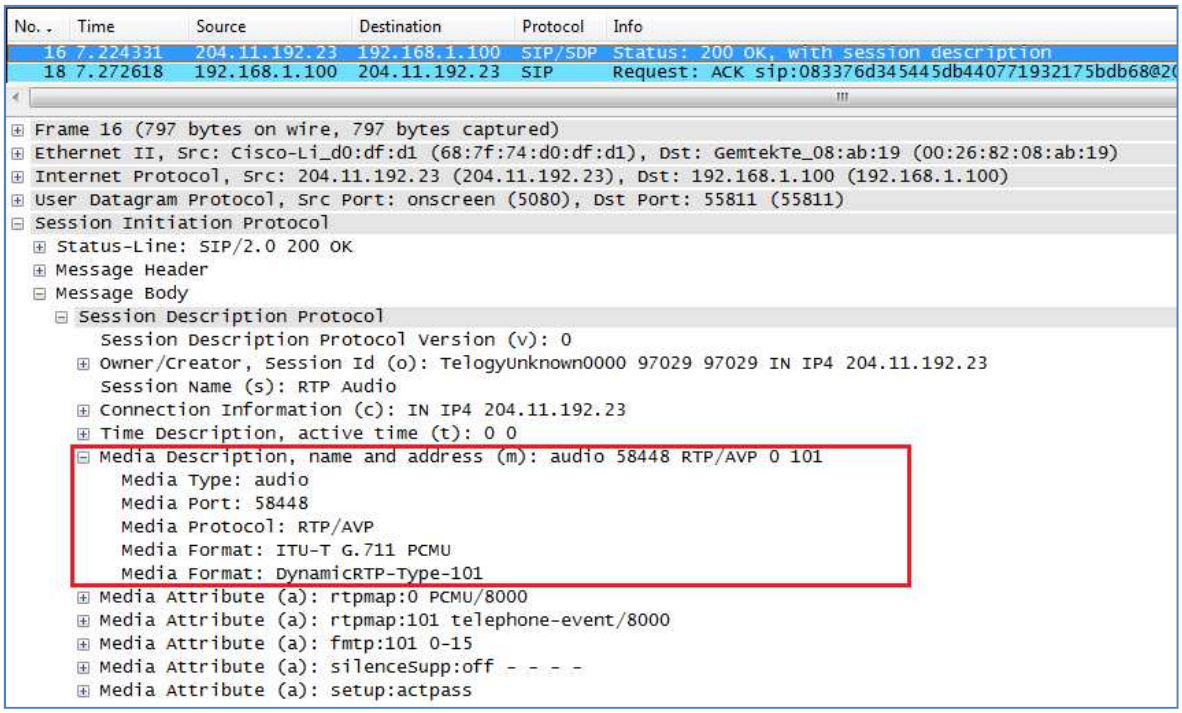

Figura. 5.10. Captura del mensaje 200 OK.

El mensaje de respuesta *200 OK* (atendí la llamada) tiene la función de confirmar que acepta la llamada. Esta respuesta *200 OK* contiene un mensaje SDP encapsulado en SIP con el propósito de confirmar el codec que será utilizado en la comunicación. En este caso el codec se confirma el *G.711 U-Law*.

El siguiente mensaje que se envía es el mensaje *ACK* (atendí la llamada), enviado desde el Softphone, con el propósito de confirmar los diferentes valores de los campos enviados en el mensaje *INVITE*. A continuación se presenta en la Figura 5.11 estos campos, los cuales coinciden entre los dos mensajes (*INVITE y ACK*) de la misma transacción SIP.

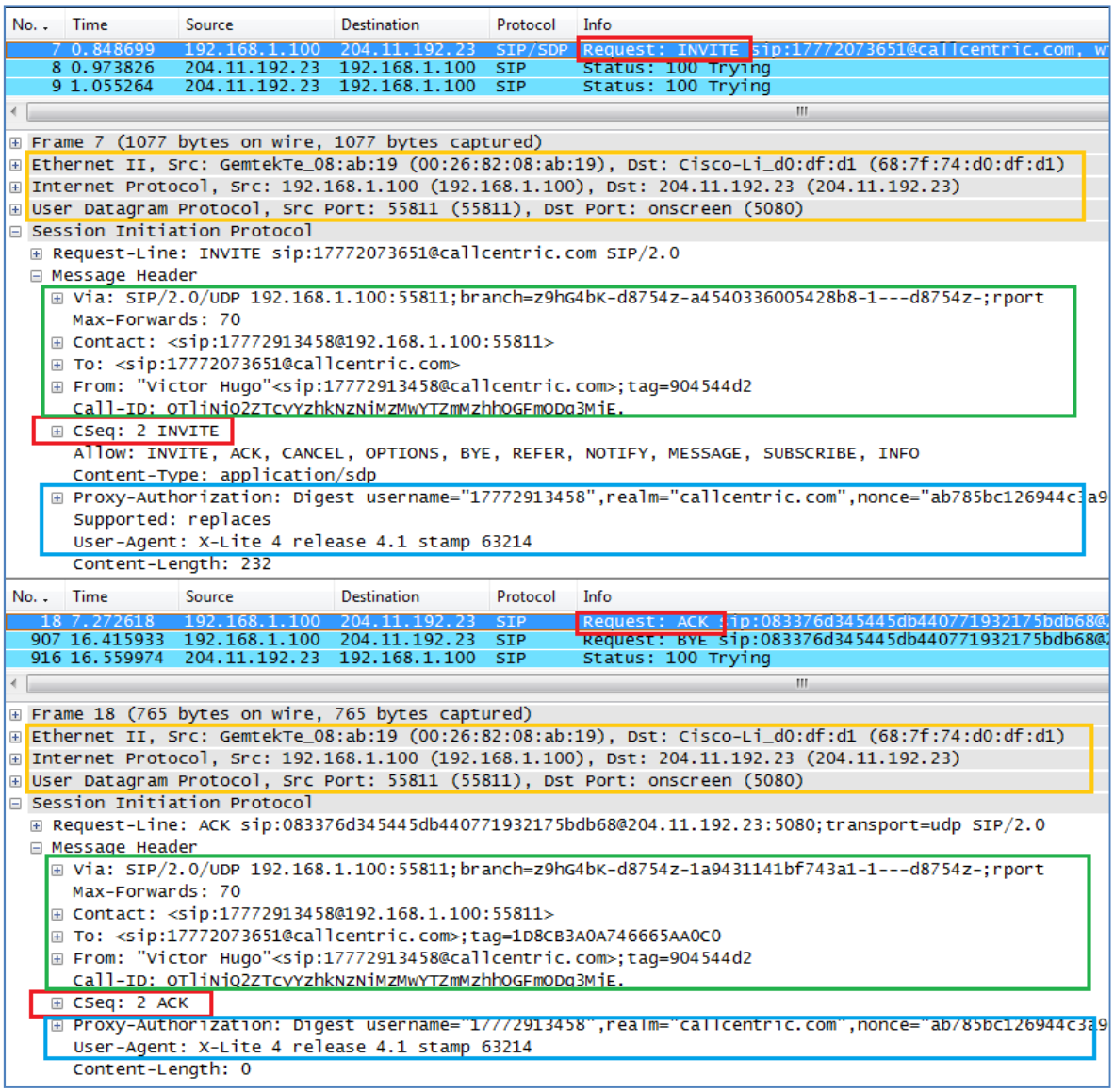

Figura. 5.11. Comparación entre los mensajes INVITE y ACK.

En este punto se establece la conversación o el intercambio de audio, mediante el envío de paquetes RTP. A continuación se presenta en la Figura 5.12 el intercambio de paquetes RTP en los dos sentidos de la conversación.

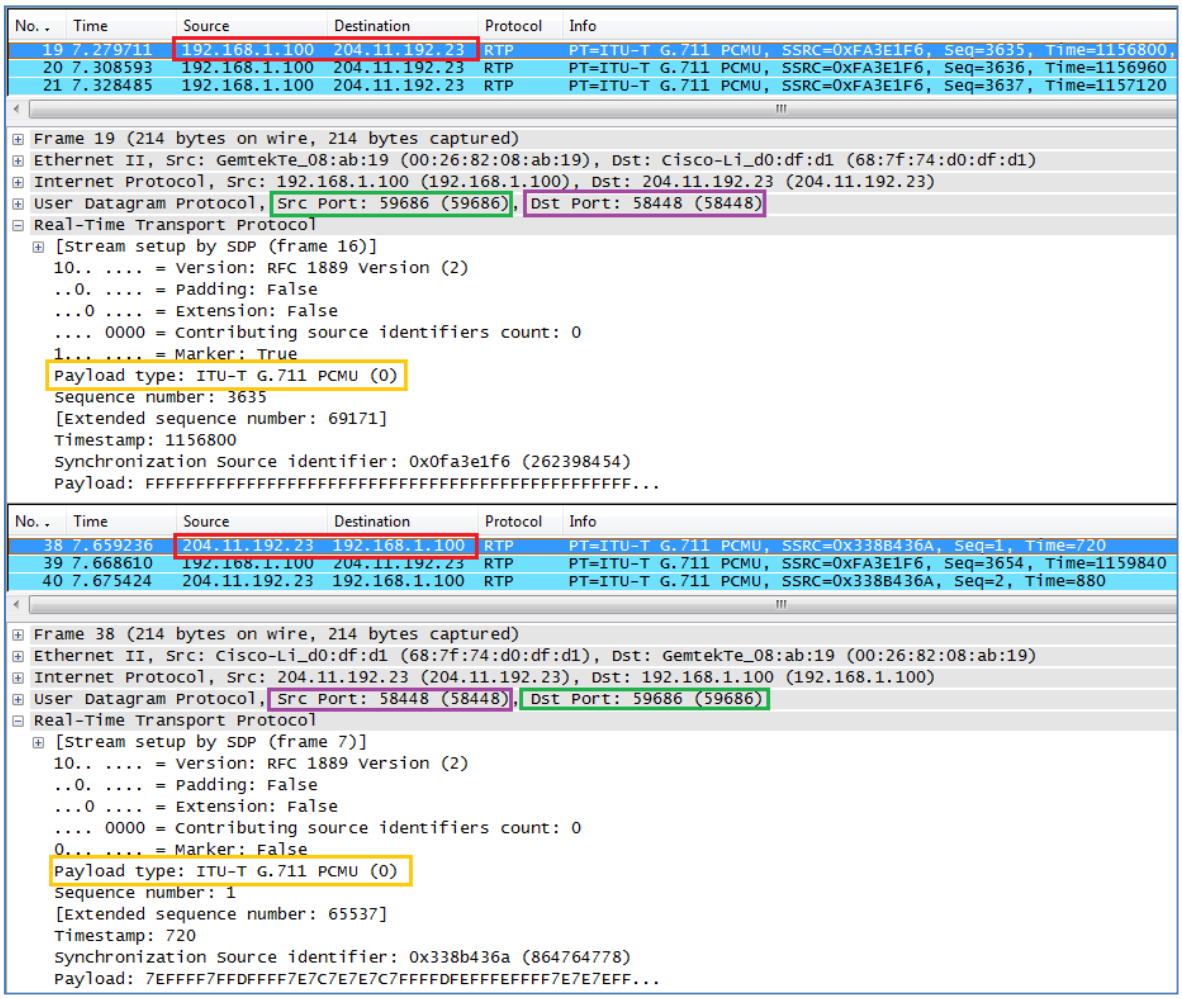

Figura. 5.12. Intercambio de paquetes RTP en los dos sentidos de la conversación.

Para la finalización de la llamada, se lleva a cabo mediante el envío del mensaje de solicitud *BYE*, en el cual se finalizó la llamada desde el *Softphone*, en la Figura 5.13 se presenta la captura del mensaje *BYE*. El usuario que recibe la solicitud *BYE* envía una respuesta *200 OK* para confirmar la finalización de la sesión SIP, como se presenta en la Figura 5.14.

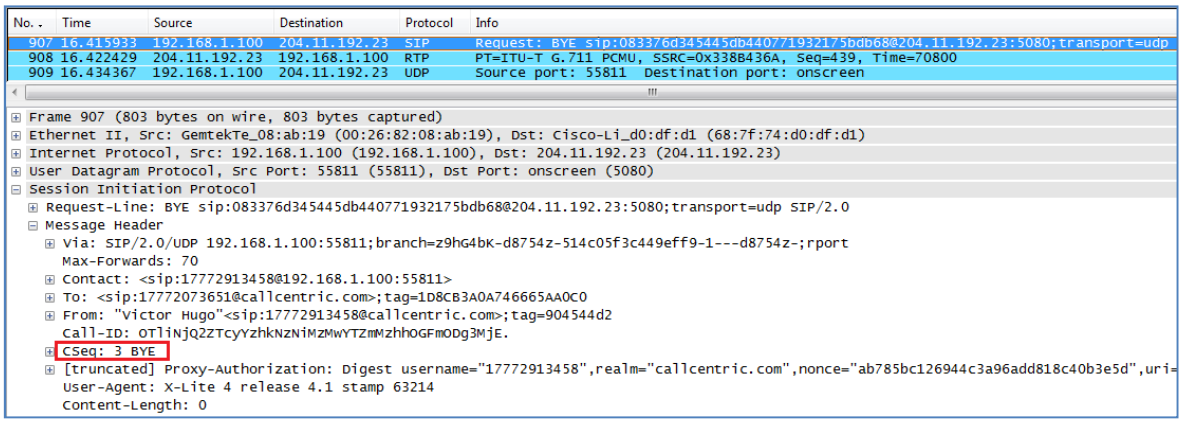

Figura. 5.13. Captura del mensaje BYE.

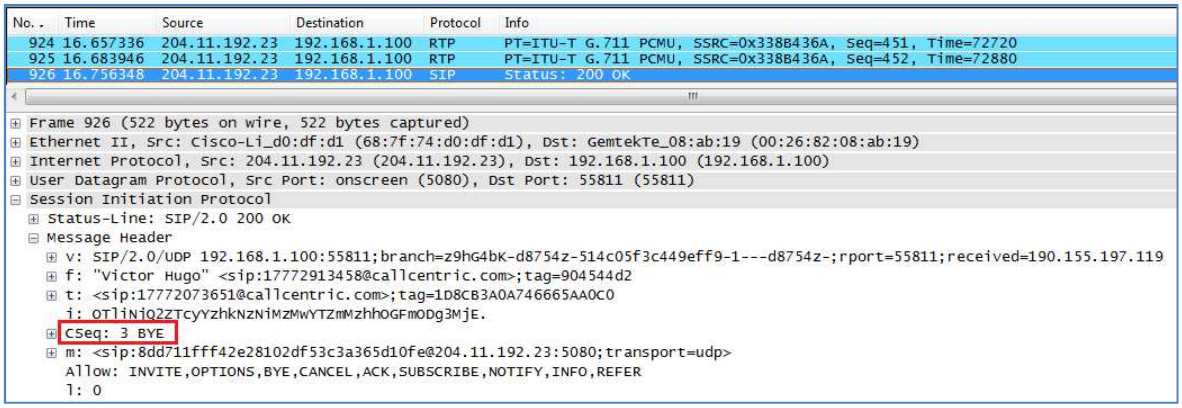

Figura. 5.14. Captura del mensaje 200 OK.

5.2 LLAMADA DESDE SOFTPHONE X-LITE HACIA USA

Este escenario de prueba se presenta en la Figura 5.15, en el cual se realiza el siguiente procedimiento:

- ✓ Empieza la captura de paquetes mediante *Wireshark*.
- ✓ Se realiza una llamada desde el Softphone X-Lite hacia un teléfono celular de USA.
- ✓ Se finaliza la llamada.
- ✓ Se detiene la captura de paquetes.

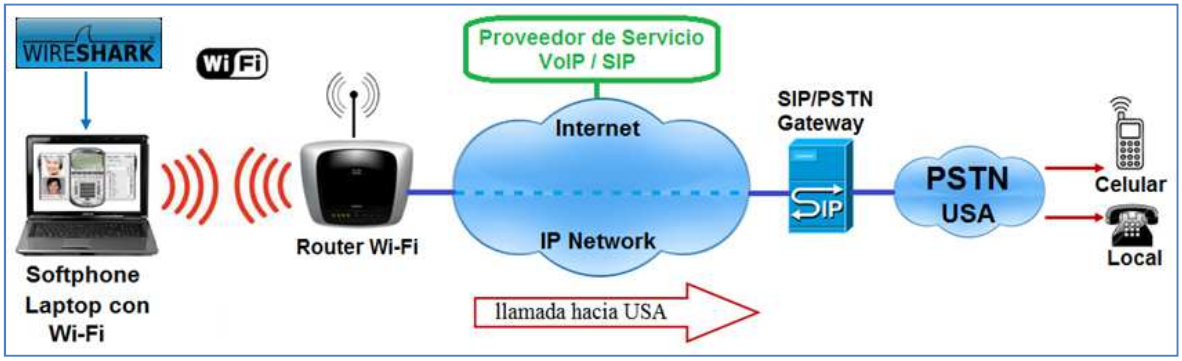

Figura. 5.15. Escenario de prueba: Llamada desde Softphone X-Lite hacia USA.

En las Figuras 5.16 y 5.17 se presenta la grafica del tráfico que está llegando al host (tráfico RTP). Para obtener estas graficas se selecciona *Statistics* en el menú principal de *Wireshark*, posteriormente se selecciona *IO Graphs*.

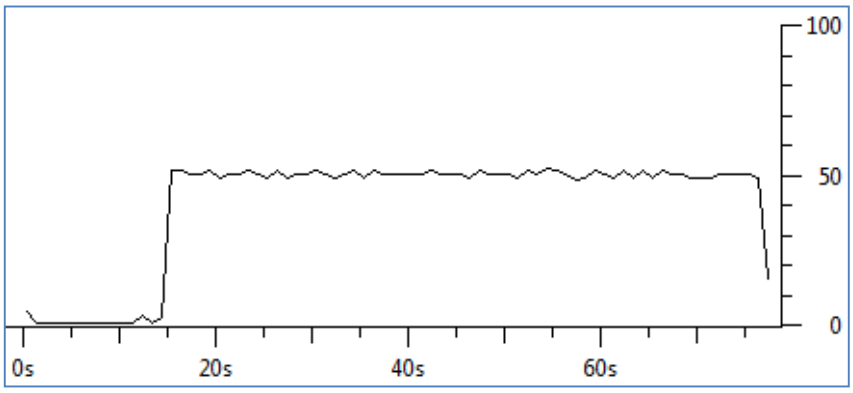

Figura. 5.16. Tráfico recibido en el host (paquetes / segundo).

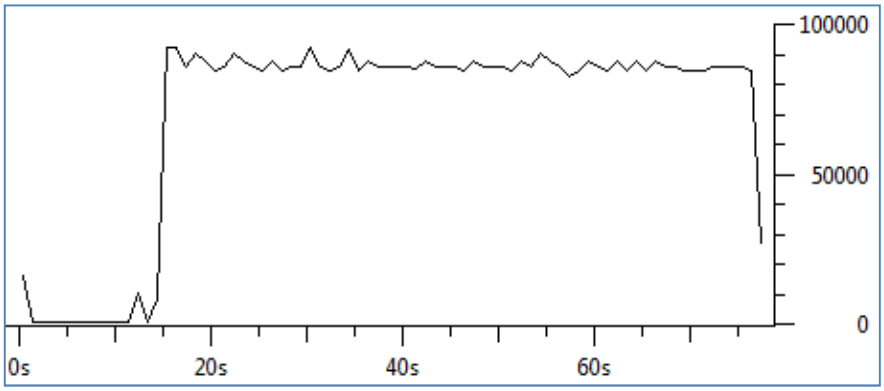

Figura. 5.17. Tráfico recibido en el host (bits / segundo).

- El ancho de banda aproximado de RTP es de 85Kpbs (G.711)

En la Figura 5.18 presenta los RTP Streams de la captura, se presenta dos streams por cada llamada. Para obtener estas ventana se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *RTP* y *Show All Streams*.

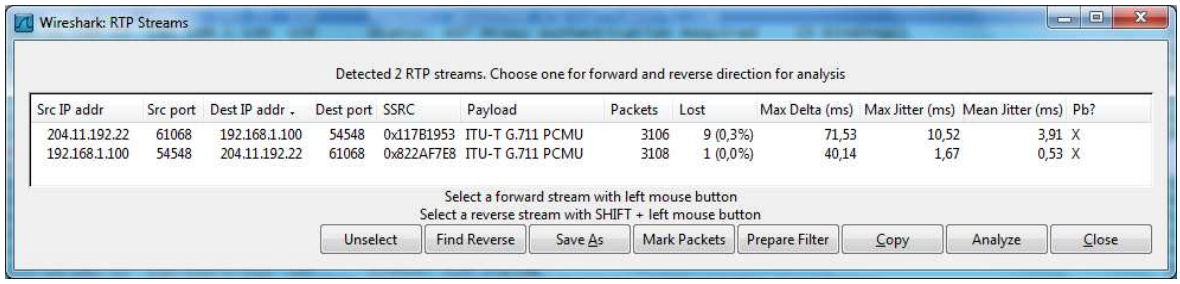

Figura. 5.18. Ventana RTP Streams.

En la tabla 5.2 se presenta los resultados de funcionamiento en el escenario de prueba: Llamada desde Softphone X-Lite hacia USA.

Tabla 5.2. Resultados de funcionamiento: Llamada desde Softphone X-Lite hacia USA.

Direcciones IP		**RTP Streams**				
Fuente	Destino	Paquetes	Perdidos	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
204.11.192.22	192.168.1.100	3106	9 (0,3%)	71,53	10,52	3,91
192.168.1.100	204.11.192.22	3108	1 (0,0%)	40,14	1,67	0,53

Para obtener gráficamente el flujo de mensajes en una llamada VoIP, se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *VoIP Calls* (Figura 5.19), a continuación se escoge la llamada VoIP y se selecciona *Graph*, esta ventana se presenta en la Figura 5.20.

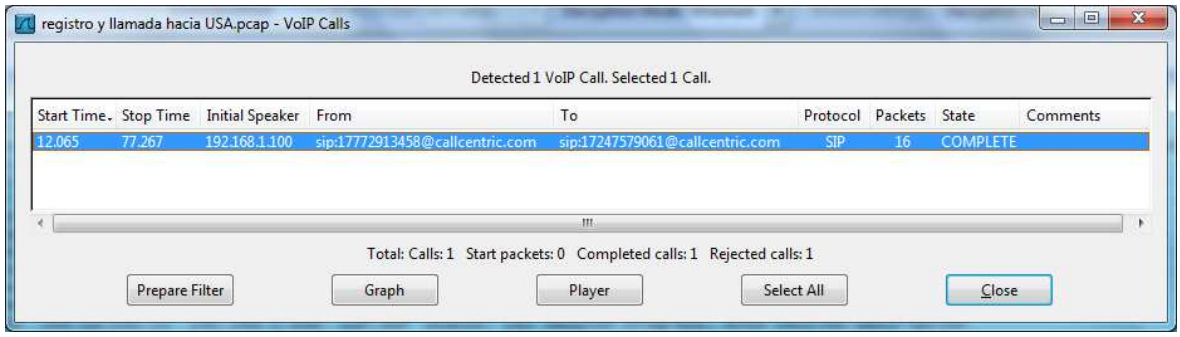

Figura. 5.19. Ventana VoIP Calls.

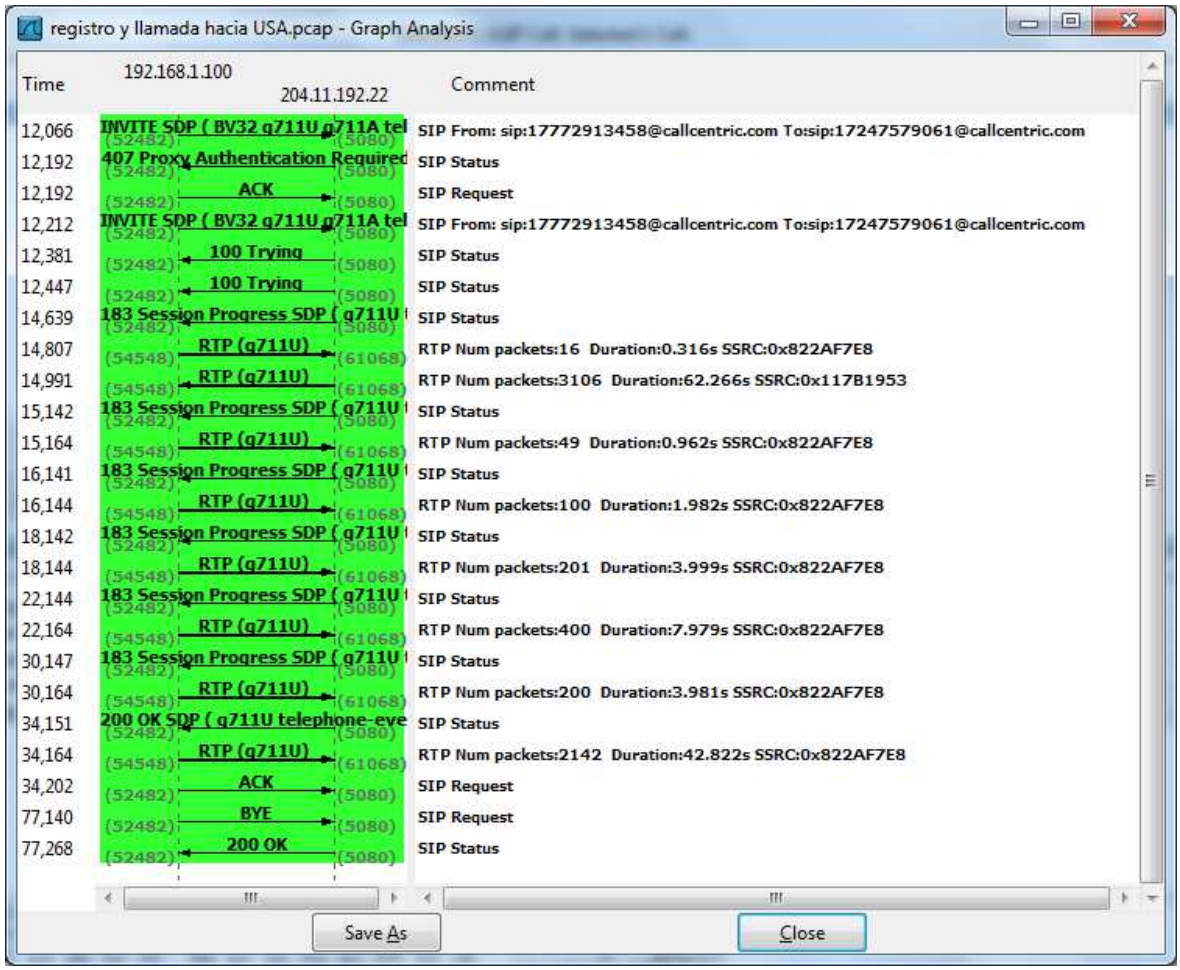

Figura. 5.20. Flujo de mensajes en una llamada VoIP: ventana Graph Analysis.

5.3 LLAMADA DESDE USA HACIA SOFTPHONE X-LITE

Este escenario de prueba se presenta en la Figura 5.21, en el cual se realiza el siguiente procedimiento:

- ✓ Empieza la captura de paquetes mediante *Wireshark*.
- ✓ Se recibe una llamada desde un teléfono celular de USA hacia el *Softphone* X-Lite (Para poder recibir llamadas, se dispone de un número en USA proporcionado por el proveedor de servicio VoIP *CallCentric*).
- ✓ Se finaliza la llamada.
- ✓ Se detiene la captura de paquetes.

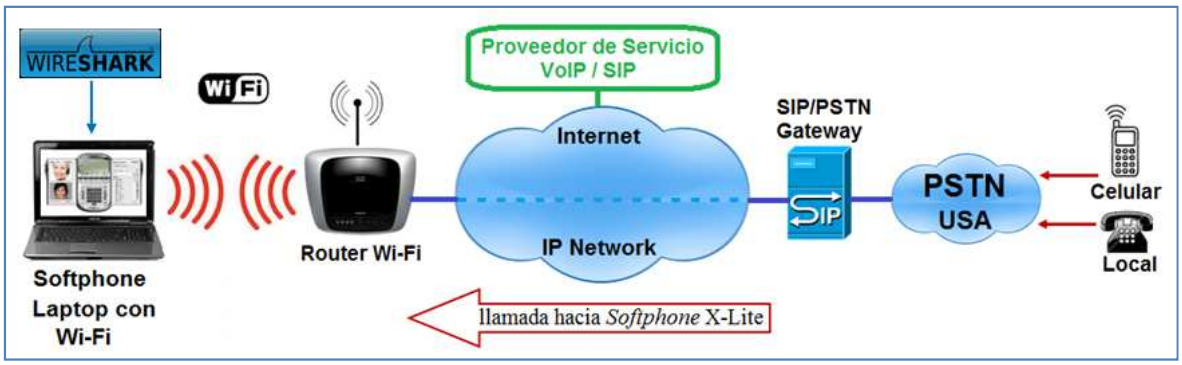

Figura. 5.21. Escenario de prueba: Llamada desde USA hacia Softphone X-Lite.

En las Figuras 5.22 y 5.23 se presenta la grafica del tráfico que está llegando al host (tráfico RTP). Para obtener estas graficas se selecciona *Statistics* en el menú principal de *Wireshark*, posteriormente se selecciona *IO Graphs*.

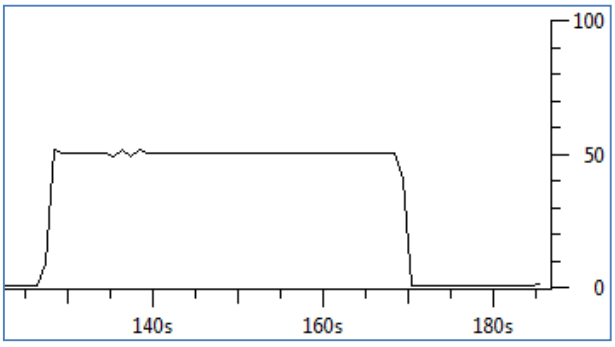

Figura. 5.22. Tráfico recibido en el host (paquetes / segundo).

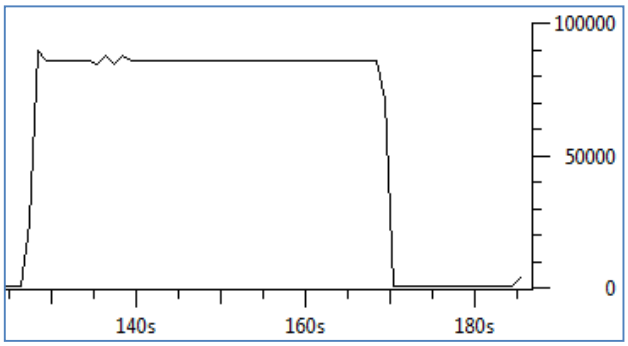

Figura. 5.23. Tráfico recibido en el host (bits / segundo).

- El ancho de banda aproximado de RTP es de 85Kpbs (G.711)

En la Figura 5.24 presenta los RTP Streams de la captura, se presenta dos streams por cada llamada. Para obtener estas ventana se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *RTP* y *Show All Streams*.

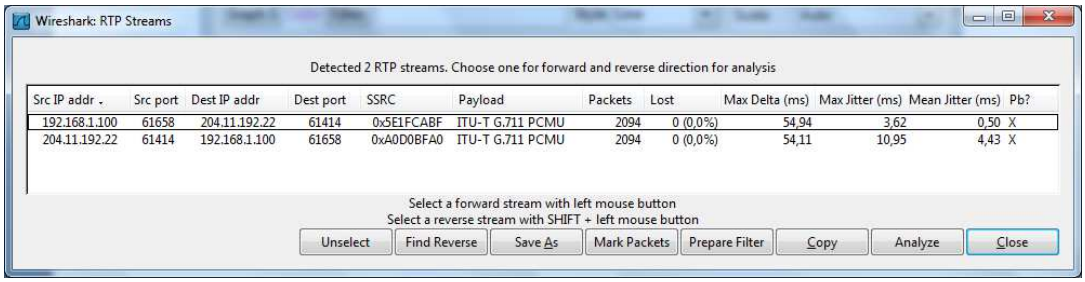

Figura. 5.24. Ventana RTP Streams.

En la tabla 5.3 se presenta los resultados de funcionamiento en el escenario de prueba: Llamada desde USA hacia Softphone X-Lite.

Tabla 5.3. Resultados de funcionamiento: Llamada desde USA hacia Softphone X-Lite.

Direcciones IP		**RTP Streams**				
Fuente	Destino	Paquetes	Perdidos	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.1.100	204.11.192.22	2094	0 (0,0%)	54,94	3,62	0,50
204.11.192.22	192.168.1.100	2094	0 (0,0%)	54,11	10,95	4,43

Para obtener gráficamente el flujo de mensajes en una llamada VoIP, se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *VoIP Calls* (Figura 5.25), a continuación se escoge la llamada VoIP y se selecciona *Graph*, esta ventana se presenta en la Figura 5.26.

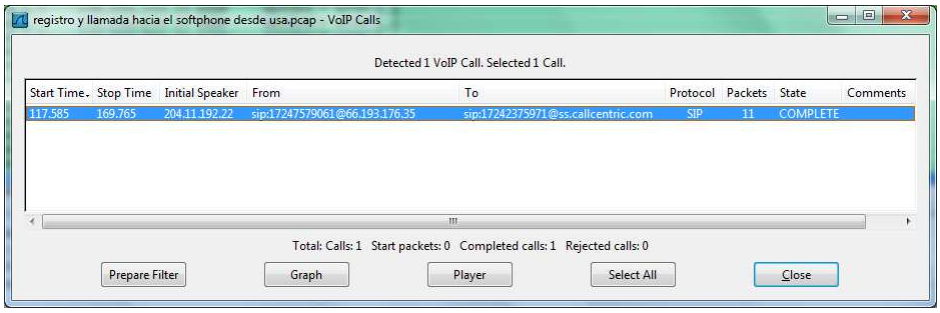

Figura. 5.25. Ventana VoIP Calls.

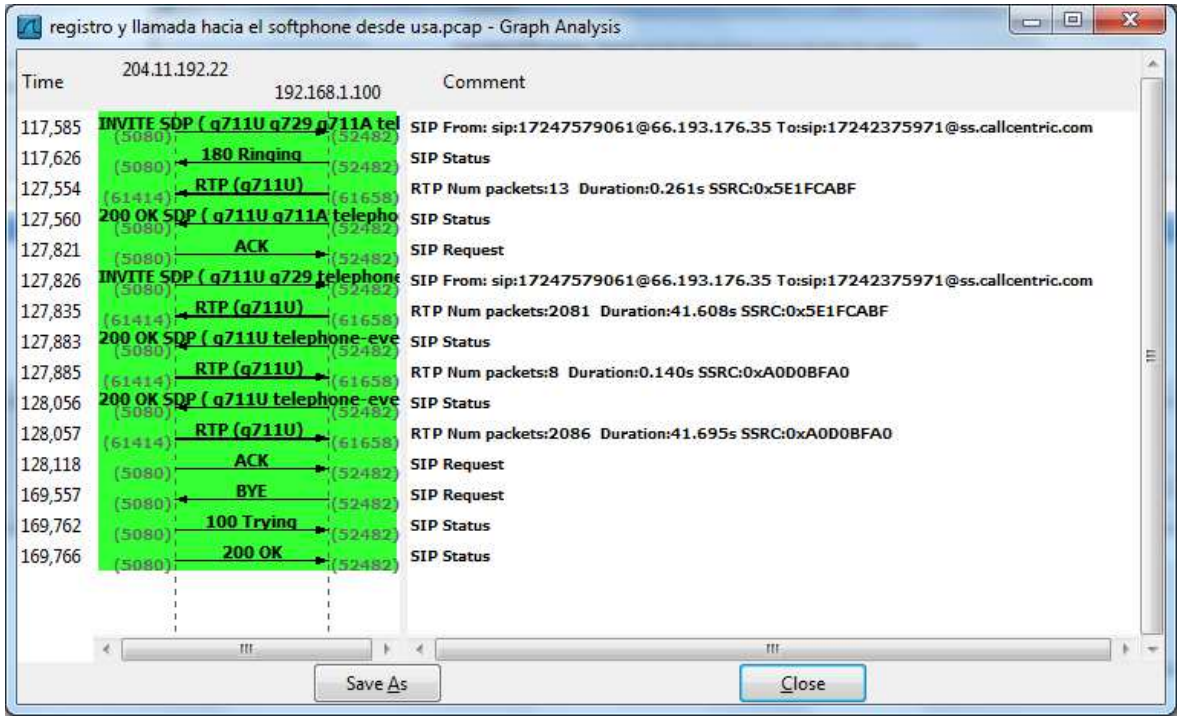

Figura. 5.26. Flujo de mensajes en una llamada VoIP: ventana Graph Analysis.

5.4 TRÁFICO DE VOZ VS TRÁFICO DE DATOS

Este escenario de prueba se presenta en la Figura 5.27, en el cual se realiza el siguiente procedimiento:

- ✓ Empieza la captura de paquetes mediante *Wireshark*.
- ✓ Se genera trafico HTTP descargamos un archivo de la web.
- ✓ Se realiza una llamada mediante el Softphone hacia USA: Llamada 1.
- ✓ Se finaliza la llamada y el trafica HTTP.
- ✓ Se realiza una nueva llamada sin tráfico HTTP, mediante el Softphone hacia USA: Llamada 2.
- ✓ Se finaliza la llamada.
- ✓ Se detiene la captura de paquetes.

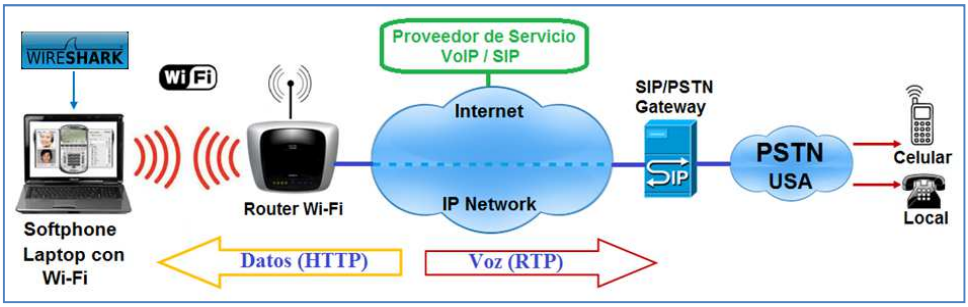

Figura. 5.27. Escenario de prueba: Tráfico de Voz vs tráfico de Datos.

Desde la Figura 5.28 hasta la Figura 5.31, se presenta la grafica del tráfico que está llegando al host (HTTP + RTP). Para obtener estas graficas se selecciona *Statistics* en el menú principal de *Wireshark*, posteriormente se selecciona *IO Graphs*.

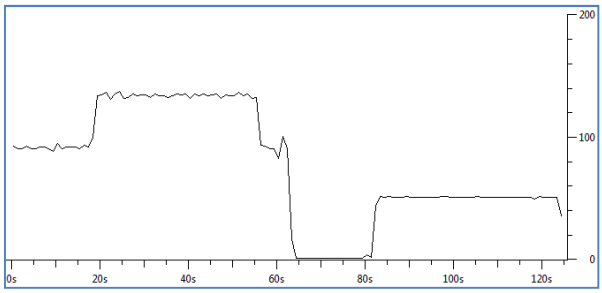

Figura. 5.28. Tráfico recibido en el host (paquetes / segundo).

- Unidades: paquetes / segundo
- Solo tráfico HTTP: 0-20s
- Llamada 1 + Tráfico HTTP: 20-65s
- Tráfico nulo: 65-80s
- Llamada 2: 80-125s

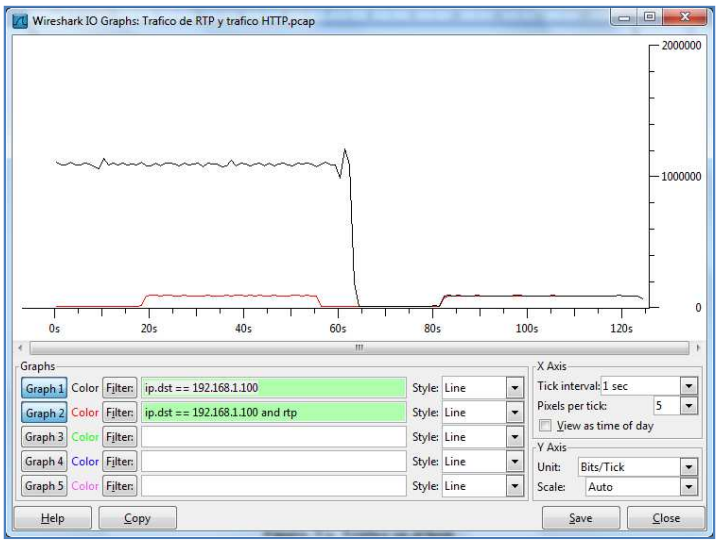

Figura. 5.29. Tráfico recibido en el host (bits / segundo).

- Unidades: bits / segundo
- Ancho de banda promedio de HTTP: 1Mbps
- Ancho de banda RTP<<HTTP
- Tamaño paquete HTTP>RTP

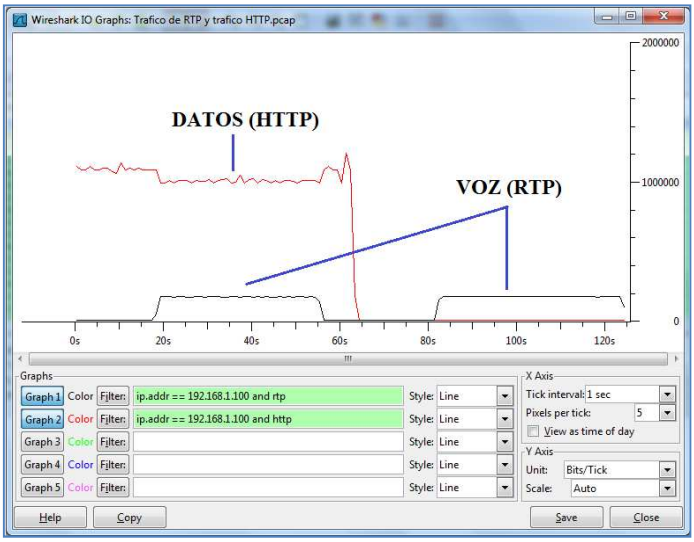

Figura. 5.30. Tráfico recibido en el host (bits / segundo).

- Unidades: bits / segundo
- Se filtra y se observa el tráfico HTTP (color rojo)
- Se filtra y se observa el tráfico RTP (color negro)

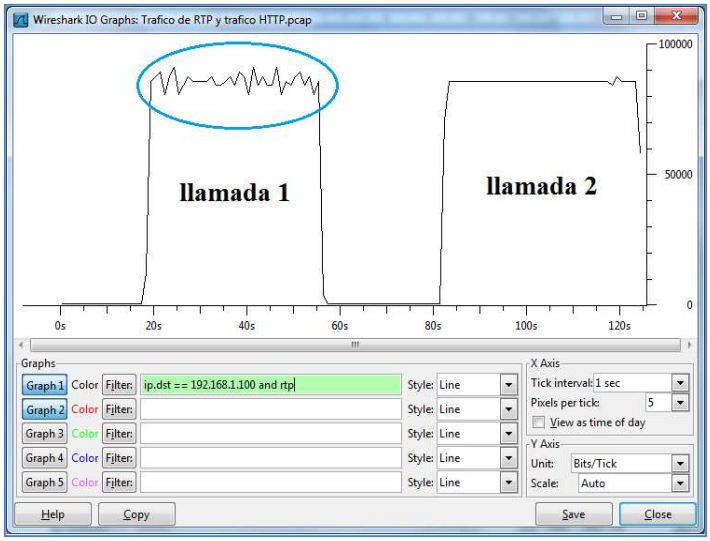

Figura. 5.31. Tráfico recibido en el host (bits / segundo).

- Unidades: bits / segundo
- Se filtra y se observa solo el grafico RTP
- El ancho de banda aproximado de RTP es de 85Kpbs (G.711)
- Se observa el efecto del Jitter en la llamada 1

En la Figura 5.32 presenta todos los RTP Streams de la captura, se presenta cuatro streams, es decir se muestra dos streams por cada llamada. Para obtener estas ventana se selecciona *Telephony* en el menú principal de *Wireshark*, posteriormente se selecciona *RTP* y *Show All Streams*.

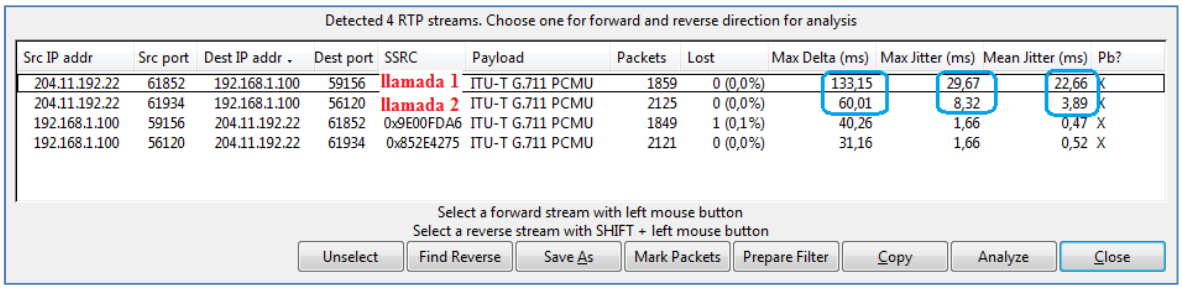

Figura. 5.32. Ventana RTP Streams.

- Posee un codificador G.711
- Muestra la cantidad de paquetes por cada *stream* (*Packets*)
- No existe paquetes perdidos en las dos llamadas (*Lost*)
- Delta: Diferencia entre el tiempo de llegada de un paquete con respecto al siguiente. Si no existe *Jitter* este valor debería ser de 20ms con G.711 y 160bytes/paquete.
- Los valores *Max Jitter* y *Jitter* promedio son mayores en la primera llamada.

A continuación se selecciona la primera llamada y se hace click en *Analyze*, a continuación se presenta una nueva ventana, en la cual se muestra: el detalle de cada paquete, indica el número de secuencia, *Delta*, *Jitter* promedio, ancho de banda, y el estado del paquete. Esta ventana se presenta en la Figura 5.33.

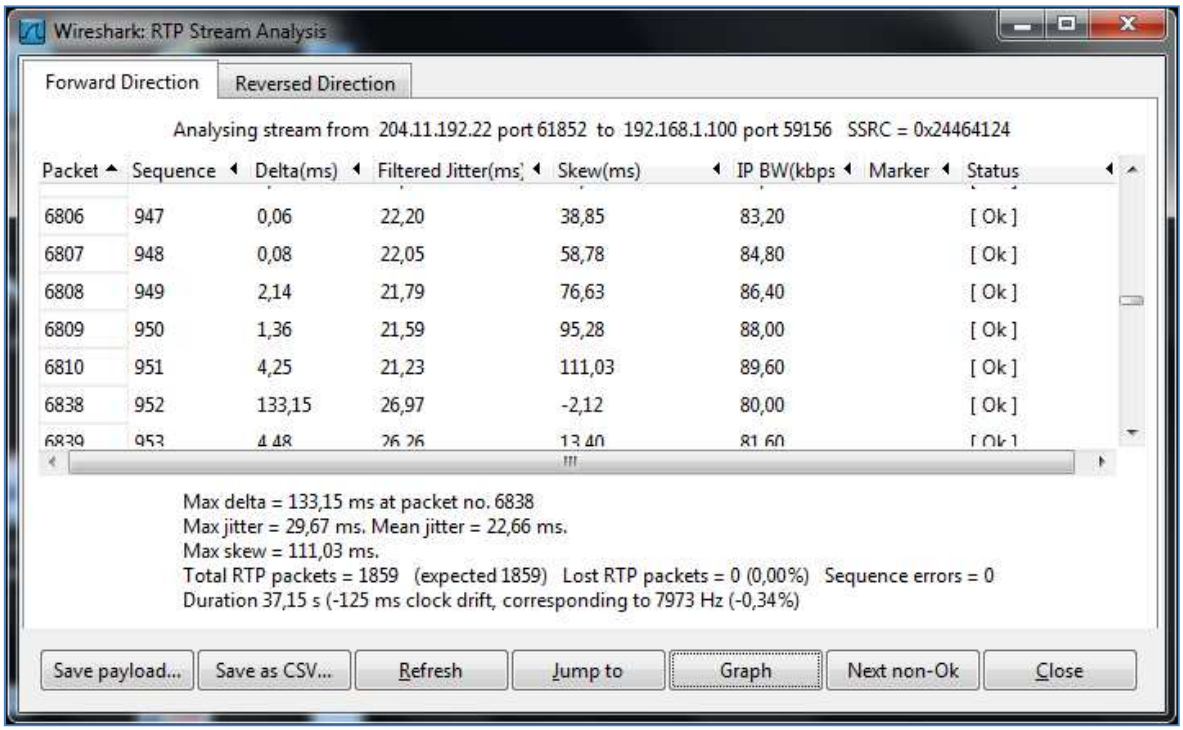

Figura. 5.33. Ventana RTP Streams Analysis.

- Se observa que ancho de banda se encuentra en el rango de: 85Kpbs (G.711)

Posteriormente se selecciona *Graph*, en la cual muestra una ventana que grafica el Jitter o el Delta en función del tiempo, como se presenta desde la Figuras 5.34 hasta la Figura 5.37.

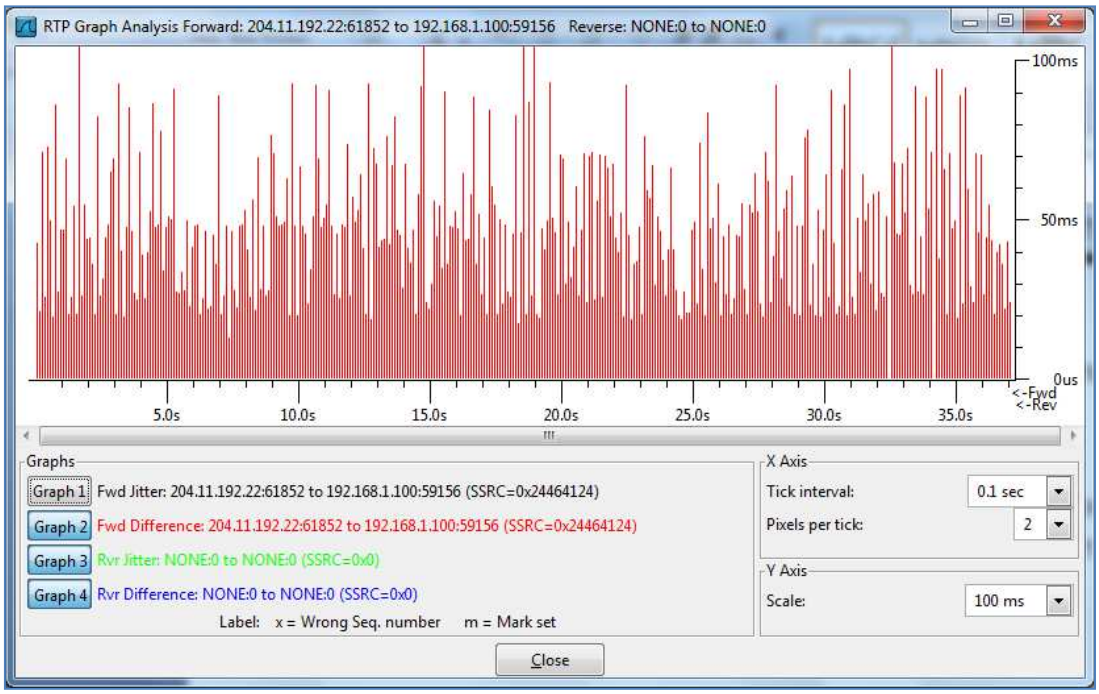

Figura. 5.34. Llamada 1: RTP + HTTP (Delta vs Tiempo).

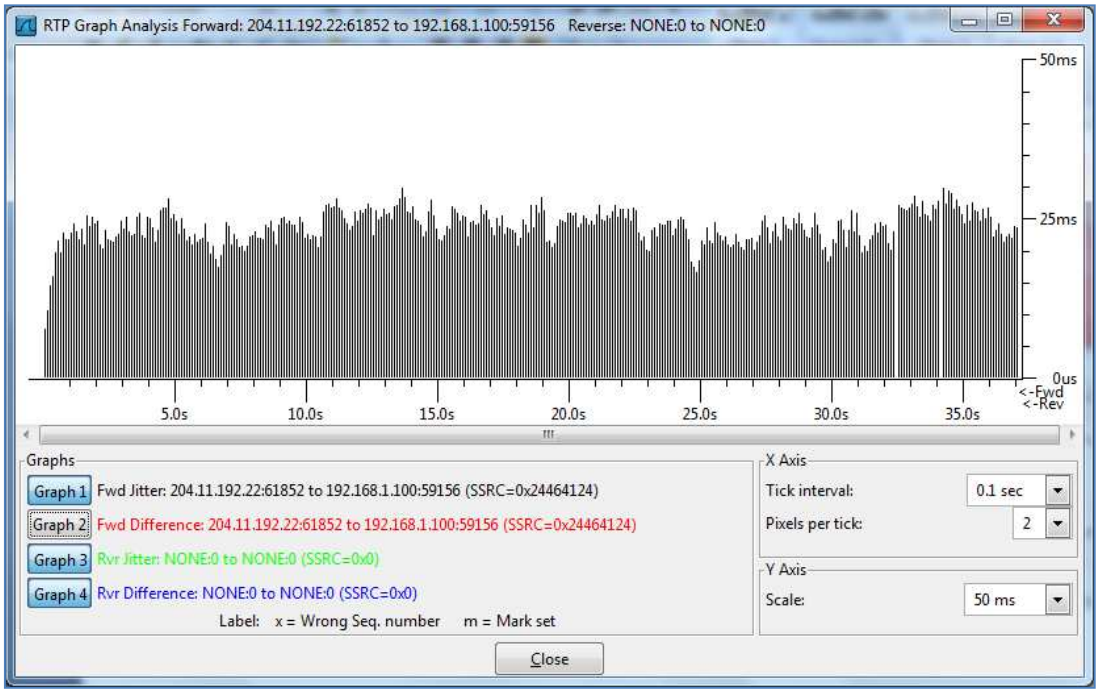

Figura. 5.35. Llamada 1: RTP + HTTP (Jitter vs Tiempo).

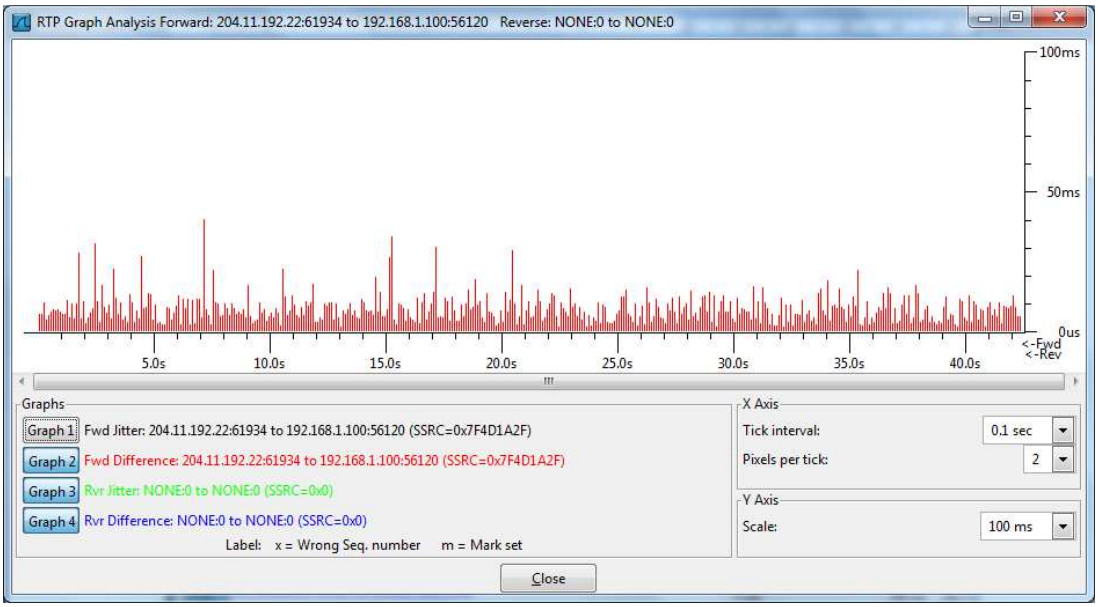

Figura. 5.36. Llamada 2: RTP + HTTP (Delta vs Tiempo).

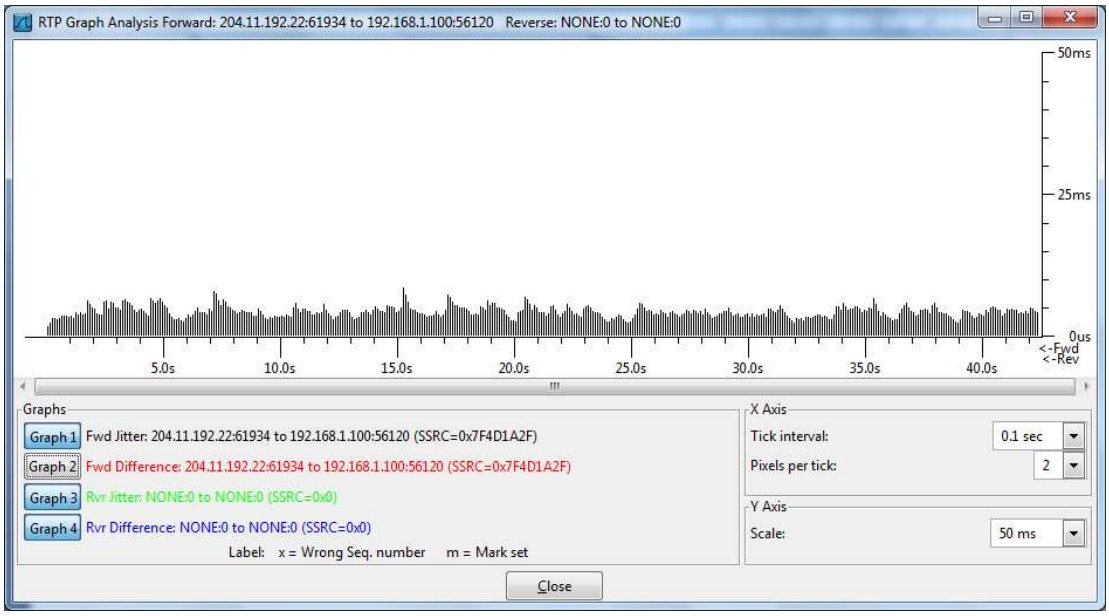

Figura. 5.37. Llamada 2: RTP + HTTP (Jitter vs Tiempo).

A continuación se presenta en la Figura 5.38 una comparación de las graficas Delta y Jitter en función del Tiempo, entre la llamada 1 y la llamada 2.

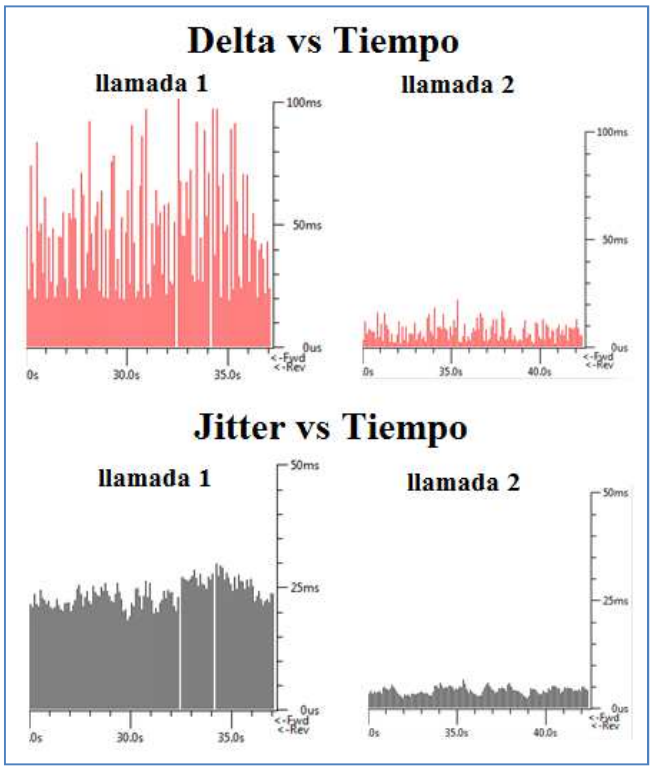

Figura. 5.38. Comparación entre llamada 1 y llamada 2.

- En la llamada 1, cuando existe trafico HTTP, aumenta el Jitter de la voz.
- En la llamada 2, cuando solo existe tráfico de voz, el Jitter disminuye considerablemente.

En las Figuras 5.39 y 5.40 se muestra la estadística de paquetes perdidos debido al Jitter Buffer.

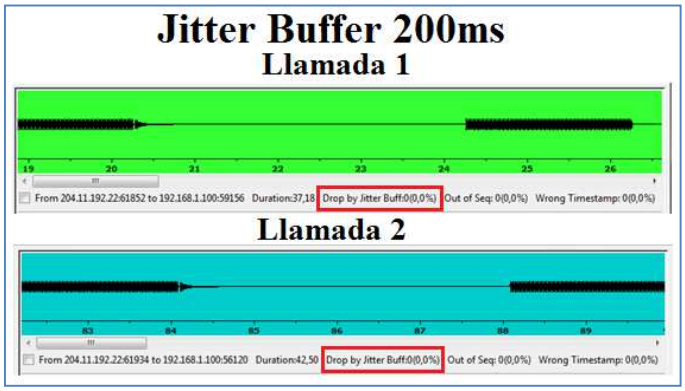

Figura. 5.39. Jitter Buffer de 200ms entre llamada 1 y llamada 2.

- Se observa que en ninguna de las llamadas de voz presenta paquetes descartados.

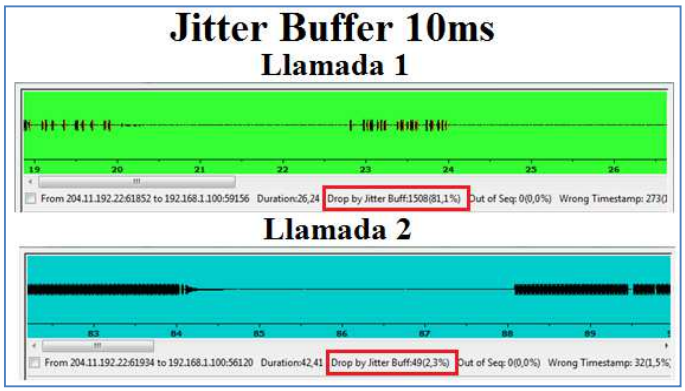

Figura. 5.40. Jitter Buffer de 10ms entre llamada 1 y llamada 2.

- Llamada 1 (HTTP + RTP) presenta 81.1% de paquetes descartados.
- En la llamada 1 la calidad de voz se deteriora drásticamente.
- En la llamada 1 existe más 80 % de paquetes perdidos.
- Llamada 2 (Solo RTP) presenta 2.3% de paquetes descartados.
- En la llamada 2 la calidad de voz se deteriora insignificantemente.
- En la llamada 2 solo existe un 2.3% de paquetes perdidos.

A continuación se presenta en la Tabla 5.4 una comparación de los principales parámetros entre la llamada 1 y la llamada 2.

Tabla. 5.4. Comparación entre llamada 1 y llamada 2.

	Llamada 1	Llamada 2
Max Delta (ms)	133,15	60,01
Max Jitter (ms)	29,67	8,32
Mean Jitter (ms)	22,66	3,89
% de descarte con Jitter Buffer = 200ms	0%	0%
% de descarte con Jitter Buffer = 150ms	0%	0%
% de descarte con Jitter Buffer = 100ms	0,2%	0%
% de descarte con Jitter Buffer = 50ms	7,8%	0%
% de descarte con Jitter Buffer = 30ms	35,7%	0,2%
% de descarte con Jitter Buffer = 20ms	51,3%	0,8%
% de descarte con Jitter Buffer = 10ms	81,1%	2,3%
% de descarte con Jitter Buffer = 8ms	85,5%	9,1%
% de descarte con Jitter Buffer = 5ms	92,1%	28,5%

- Con 50ms de Jitter Buffer en la llamada 1 descarta aproximadamente lo mismo que en la llamada 2 con 8ms de Jitter Buffer.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

Del estudio realizado se determinó que el Protocolo SIP es más simple que otros protocolos, y mucho más adecuado para VoIP y otras aplicaciones de internet. Por lo tanto más y más empresas y organizaciones alrededor del mundo eligen equipos compatibles con SIP. La elección de productos basados en el estándar SIP asegura que se pueden mezclar productos de diferentes fabricantes y que va a ser parte del mundo VoIP en el futuro.

De la investigación realizada se determina que hacer y recibir llamadas de voz a través de las redes Wi-Fi, está ganando rápidamente popularidad como la voz sobre IP (VoIP), que goza de una popularidad cada vez mayor, gracias al surgimiento de nuevos dispositivos de voz, como teléfonos de modo dual con tecnología celular y Wi-Fi, con una amplia disponibilidad. Los fabricantes de dispositivos Wi-Fi han ampliado y mejorado la funcionalidad de voz, introduciendo características avanzadas en Calidad de Servicio (QoS), eso ha mejorado la capacidad de voz de redes Wi-Fi.

La tecnología Wi-Fi ofrece a los usuarios una amplia gama de dispositivos que soportan aplicaciones de voz, lo que incluye, pero no está limitado a los teléfonos móviles. Las computadoras portátiles han sido los primeros dispositivos en soportar voz sobre Wi-Fi, pero los teléfonos celulares solo con tecnología Wi-Fi y modo dual celular/Wi-Fi, están creciendo rápidamente, ofreciendo a los usuarios de VoIP sin cables.

Voz sobre Wi-Fi es una de las áreas más interesantes de crecimiento en la industria Wi-Fi. Puesto que Voz sobre Wi-Fi proporciona a los usuarios un acceso cómodo y sencillo a las aplicaciones móviles de voz, disponible a través de la conexión a Internet de banda ancha, a través de una gran variedad de dispositivos terminales.

VoIP puede garantizar una alta calidad en la transmisión de voz, si los canales de señalización y de audio, tienen prioridad sobre otros tipos de tráfico de la red. Para que los usuarios reciban un nivel aceptable de calidad de la voz, el tráfico de VoIP debe garantizar ciertas compensaciones de: ancho de banda, latencia, y requisitos de Jitter. QoS asegura que los paquetes de voz de VoIP reciban el tratamiento preferencial que requieren.

Del análisis realizado en el escenario de prueba: Tráfico de Voz vs tráfico de Datos, se determinó que los datos HTTP generan un *Jitter* bastante considerable sobre el tráfico de voz. Por lo tanto en la llamada 1, requiere un *Jitter buffer* de 100 ms para obtener un porcentaje aceptable de paquetes descartados. A diferencia que en la llamada 2, no presenta problemas de *Jitter* porque con un *Jitter buffer* de 20ms se obtiene un porcentaje aceptable de paquetes descartados.

El Funcionamiento del presente proyecto es muy satisfactorio, puesto que se cumplió con los objetivos y expectativas planteadas. Por lo tanto, se puede concluir que, el proveedor *CallCentric* (*Internet Phone Service*), es una excelente alternativa en aplicaciones de Voz sobre IP basados en SIP, por su capacidad de funcionamiento y compatibilidad con un sin número de dispositivos terminales SIP, los cuales, el proveedor *CallCentric* ofrece soporte para cada uno de ellos. De la misma forma los dispositivos terminales SIP tanto en *hardware: WLAN660S Wi-Fi SIP Phone*, como en *software:* el *Softphone* X-Lite versión 4.0, presentan un desempeño exitoso. Logrando obtener en gran manera una reducción de costos, con respecto a las llamadas internacionales.

6.2 RECOMENDACIONES

Para garantizar una buena calidad de Voz sobre Wi-Fi, se recomienda que los dispositivos terminales y los puntos de acceso, cumplan con los niveles de desempeño adecuado, referente a perdida de paquetes, latencia, Jitter, entre otros.

Para evitar valores tan altos de *Jitter buffer*, es posible reducir el efecto del *Jitter* proporcionando técnicas de calidad de servicio como: dar prioridad al tráfico de voz con respecto al de datos, enlaces de mayor velocidad, entre otros, teniendo en cuenta que: “Una disminución del *buffer* significa menos retardo pero más pérdida de paquetes, caso contrario, un aumento del *buffer* significa menos pérdida de paquetes pero más retardo”. Prácticamente los valores del *Jitter buffer* pueden ser configurados de forma manual o el equipo terminal (teléfono IP) estime el mejor valor, teniendo en cuenta la relación de compromiso.

Para obtener un porcentaje aceptable de paquetes descartados se recomienda ser menor o igual al 1%.

Al momento de elegir un proveedor de servicios VoIP / SIP, se recomienda elegir uno que ofrezca servicios especiales en una área determinada, específicamente dentro de un país en particular. La elección del proveedor dentro del mismo país que se desea realizar o recibir llamadas constantemente, puede potencialmente reducir los costos en gran manera.

REFERENCIAS BIBLIOGRÁFICAS

[1] Historia de las Telecomunicaciones. Biografía de Almon Brown Strowger. Disponible en: http://histel.com/z_histel/biografias.php?id_nombre=79 [Consulta: 21 enero 2011].

[2] Javier Castillo Ruiz, “Desarrollo de b2bua filter criteria para s-cscf en ims”. Universidad Politécnica de Catalunya, 2006.

[3] VOIP - Voz sobre IP (Voice Over Internet Protocol) Disponible en: Monografias_com.mht [Consulta: 21 enero 2011].

[4] IETF “SIP: Session Initiation Protocol” RFC 3261. J. Rosenberg, dynamicsoft , H. Schulzrinne Columbia U., G. Camarillo Ericsson, A. Johnston WorldCom, J. Peterson, Neustar R. Sparks dynamicsoft, M. Handley ICIR, E. Schooler, AT&T. June 2002.

[5] TCP/IP y el modelo OSI Disponible en: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[6] Tella Llop, Jose Manuel: Fundamentos del TCP/IP. Publicado originalmente en septiembre de 1999 en los grupos de noticias microsoft.public.es.windows98. TCP/IP orientado a Windows Disponible en: http://www.saulo.net/pub/tcpip/b.htm

[7] TCP-IP Tutorial and Technical Overview Tutorial y descripción técnica de TCP/IP Disponible en: http://www.cicei.com/ocon/gsi/tut_tcpip/3376c23.html

[8] Protocolos de Voz sobre IP
Disponible en: www.lairent.com.ar
Julián María Ganzábal [jganzabal@lairent.com.ar]

[9] Entidades básicas de SIP
Disponible en: http://es.wikitel.info/wiki/Entidades_b%C3%A1sicas_SIP

[10] Overview of Operation
IETF “SIP: Session Initiation Protocol” RFC 3261. J. Rosenberg, dynamicsoft , H. Schulzrinne Columbia U., G. Camarillo Ericsson, A. Johnston WorldCom, J. Peterson, Neustar R. Sparks dynamicsoft, M. Handley ICIR, E. Schooler, AT&T. June 2002.

[11] CounterPath Releases X-Lite 4.0
Disponible en: http://www.counterpath.com/counterpath-xlite-4-release.html

FECHA DE ENTREGA: _____

_____

Víctor Hugo López Chalacán

_____

Ing. Gonzalo Olmedo

DIRECTOR DE CARRERA DE INGENIERÍA
EN ELECTRÓNICA Y TELECOMUNICACIONES