

INSTITUTO POLITÉCNICO NACIONAL
CENTRO DE INVESTIGACIÓN Y DESARROLLO
DE TECNOLOGÍA DIGITAL



MAESTRÍA EN CIENCIAS CON
ESPECIALIDAD EN SISTEMAS DIGITALES

**“ANÁLISIS E IMPLEMENTACION DE UN SISTEMA
EXPERIMENTAL DE VOZ SOBRE IP EMPLEANDO EL
PROTOCOLO SIP”**

TESIS

**QUE PARA OBTENER EL GRADO DE
MAESTRO EN CIENCIAS**

P R E S E N T A:

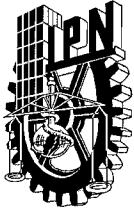
EVA GUADALUPE ALVAREZ HERNANDEZ

BAJO LA DIRECCIÓN DE:

DR. MOISES SANCHEZ ADAME Y DR. MIGUEL AGUSTIN ALVAREZ CABANILLAS

ENERO 2009

TIJUANA, B.C., MÉXICO



INSTITUTO POLITÉCNICO NACIONAL SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de Tijuana, B.C. siendo las 15:00 horas del día 15 del mes de enero del 2009 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de CITEDI para examinar la tesis de grado titulada:

ANÁLISIS E IMPLEMENTACIÓN DE UN SISTEMA EXPERIMENTAL DE VOZ SOBRE IP EMPLEANDO EL PROTOCOLO SIP.

Presentada por el alumno:

ÁLVAREZ

Apellido paterno

HERNÁNDEZ

materno

EVA GUADALUPE

nombre(s)

Con registro:

B0	6	1	1	9	0
----	---	---	---	---	---

aspirante al grado de:

MAESTRÍA EN CIENCIAS EN SISTEMAS DIGITALES

Después de intercambiar opiniones los miembros de la Comisión manifestaron **SU APROBACIÓN DE LA TESIS**, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISION REVISORA

Director de tesis


DR. MIGUEL AGUSTIN ALVAREZ CABANILLAS

Director de tesis


DR. MOISÉS SÁNCHEZ ADAME



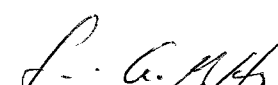

M. C. ERNESTO EDUARDO QUIROZ MORONES

S. E. P.
INSTITUTO POLITÉCNICO NACIONAL
CENTRO DE INVESTIGACIÓN Y DESARROLLO
DE TECNOLOGÍA DIGITAL
DIRECCIÓN


M. C. JOSE ABEL HERNANDEZ RUEDA

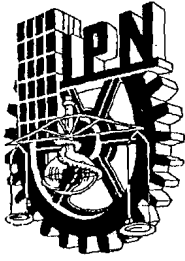
DR. ROBERTO HERRERA CHARLES

EL PRESIDENTE DEL COLEGIO


DR. LUIS ARTURO GONZALEZ HERNANDEZ



S. E. P.
INSTITUTO POLITÉCNICO NACIONAL
CENTRO DE INVESTIGACIÓN Y DESARROLLO
DE TECNOLOGÍA DIGITAL
DIRECCIÓN




INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de Tijuana, Baja California, el día 16 del mes Enero del año 2009, el (la) que suscribe Eva Guadalupe Álvarez Hernández alumno (a) del Programa de MAESTRÍA EN CIENCIAS EN SISTEMAS DIGITALES con número de registro B061190, adscrito al CENTRO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA DIGITAL, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de Dr. Miguel A. Álvarez Cabanillas y Dr. Moises Sanchez Adame y cede los derechos del trabajo intitulado Análisis e implementación de un sistema experimental de voz sobre IP empleando el protocolo SIP, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección: Av. del Parque No. 1310, Mesa de Otay, Tijuana, Baja California, México CP 22510. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.


Nombre y firma

DEDICATORIA

*A **Dios** por ser mi fuerza cada día.*

*A mis padres **Arturo** Álvarez y **Martha** Hernández que con su esfuerzo y esmero me enseñaron a luchar por ser una mejor persona en todos los sentidos, gracias los amo con todo mi corazón.*

*Al amor de mi vida y el que ahora es mi esposo: **Rafael**, por tener fe en mí, por no dejarme vencer en los momentos difíciles, por el apoyo que siempre me ha brindado, por comprender y acompañarme en este largo camino y por dejarme compartir mi vida a su lado.*

AGRADECIMIENTOS

A mis hermanos Argel, Hiram y Jorge porque siempre me han cuidado y por darme unos sobrinos hermosos: Argelito, Ayrton, Aarón, Christian, Hiramí, a la hermosa flaquita y la que está por llegar.

A mi familia en la Ciudad de México que me brindó su casa durante las jornadas de Consejo en el INP, pero sobre todo por su caluroso recibimiento.

A mis mejores amigos Carmen, Marthys, Roy y Christian con los cuales tuve la fortuna de cursar la universidad y con los que ahora compartiré un logro más. A Diego, Gabo e Isma por dejarme pertenecer al grupo selecto de los “Chuchis”, pero sobre todo por brindarme su amistad.

A todos mis compañeros, a mis maestros, al personal administrativo por su ayuda y colaboración. Gracias a Yazmin, José Ángel, Perla, Miguel, Narce, Oriol, Sonia, Camacho, Lulu, Yara, Oscar, Blanquita, Juan y al Ing. Enrique Cárdenas.

*Mi más sincero agradecimiento a los que me guiaron con mucha paciencia en este camino, los que dedicaron su tiempo y de los que aprendí mucho, mis directores de tesis:
Dr. Moisés Sánchez Adame
Dr. Miguel Agustín Álvarez Cabanillas*

*A mi Comité Tutorial que desde el inicio me brindo el apoyo para mi trabajo y de los que recibí excelentes comentarios, gracias por su paciencia y por sus consejos:
MC. Ernesto Quiroz Morones
Dr. Roberto Herrera Charles
MC. José Abel Hernández Rueda*

Gracias al CITEDI por permitirme realizar mis estudios de Maestría, al Programa de Becas del Instituto Politécnico Nacional y a CONACYT por su apoyo económico brindado durante estos dos años y medio.

A todas y cada una de las personas que directa o indirectamente contribuyeron en este trabajo, mil gracias, sin ustedes esto hoy no hubiese concluido.

RESUMEN

En este trabajo se analiza la trayectoria de los mensajes empleados por el Protocolo de Inicio de Sesión (*Session Initiation Protocol: SIP*) de Voz por IP (*Voice over IP: VoIP*). Se inicia con la revisión de la evolución de este nuevo tipo de telefonía; así también se revisa los elementos principales que la componen los cuales son: el Protocolo de Internet, conversión analógica-digital y codecs (codificador-decodificador). Además se analizaron los factores que determinan la Calidad del Servicio (*Quality of Services: QoS*). Posteriormente se efectúa un análisis del funcionamiento del Bloque de Protocolos para Multimedia por Internet (*Internet Multimedia Protocol Stack*), así como el análisis de los principales protocolos que intervienen en el proceso de telefonía los cuales son: Protocolo de Descripción de Sesión (SDP), Protocolo de Inicio de Sesión (SIP), Protocolo de Transporte en Tiempo Real (RTP), Protocolo de Datagrama de Usuario (UDP), Protocolo de Internet (IP) y Ethernet. En particular se realiza un análisis más extenso al protocolo SIP que es el centro de este trabajo y que permite la administración de la comunicación telefónica entre usuarios a través de Internet. Se describe la implementación de un sistema experimental de Voz sobre IP mediante un servidor tipo *softswitch* en una topología de red local con dos terminales. Esta red local se conecta a la red pública de Internet a través de un Servidor de Registros que contienen el Sistema de los Nombres de Dominio (*Domain Name System: DNS*). De esta forma es posible establecer la telefonía VoIP entre usuarios en la red pública con usuarios en la red local. Finalmente se verifica la intervención de los protocolos descritos anteriormente en el proceso de telefonía VoIP, analizando la transferencia de paquetes en una llamada en tiempo real entre dos usuarios SIP, en la red experimental implementada.

Palabras clave: VoIP, IP, SIP, RTP, UDP, Ethernet.

ABSTRACT

In this work, we analyze the messages trajectory used by the Session Initiation Protocol on Voice over IP (*VoIP*). It initiates with a survey of the evolution of this new type of telephony; it also reviews the important elements of VoIP as: the Internet Protocol, analog-digital conversion and codecs (*coder-decoder*). The factors which determine the Quality of Service (*QoS*) are also analyzed. Then it analyses the Internet Multimedia Protocol Stack work, it also analyses the top Protocols that intervene in the telephony process which they are: Session Description Protocol, Session Initiation Protocol, Real Time Transport Protocol, User Datagram Protocol, Internet Protocol and Ethernet. In particular we made a more extended analysis of the SIP Protocol that is the core of this work, because it allows the administration of the telephone communication between users in the Internet. It describes the experimental implementation of a voice system over the IP made possible by a softswitch type server with a local net topology with two terminals. This local Net is connected to the public Internet by a Register Server that contains a Domain Name System DNS. This makes possible to establish the VoIP telephony between users in the Public Network with users in the local Network. Finally we verify the application of the Protocols described previously in the VoIP Telephony, analyzing the transfer of packages in a real time call between two SIP users in the implemented experimental Network.

Keywords: VoIP, IP, SIP, RTP, UDP, Ethernet.

Lista de tablas

Tabla 2. 1 Métodos de compresión.	- 9 -
Tabla 2. 2 Parámetros de MOS.	- 10 -
Tabla 2. 3 Codecs de audio de la ITU.....	- 11 -
Tabla 3. 1 Tipos de respuestas SIP.	- 28 -
Tabla 3. 2 Campos de formato de mensajes de peticiones y respuesta.....	- 30 -
Tabla 4. 1 Lista de campos SDP según el orden requerido.	- 36 -
Tabla 4. 2 Valor de los atributos de SDP.....	- 37 -
Tabla 4. 3 Tipos de paquetes RTCP.....	- 40 -
Tabla 4. 4 Tipo de carga útil de audio y video RTP/AVP.	- 40 -
Tabla 4. 5 Tipos de servicios.	- 44 -
Tabla 4. 6 Parámetros del campo Bandera del encabezado de IP.....	- 45 -
Tabla 4. 7 Mensajes de error y de consulta del protocolo ICMP.....	- 48 -
Tabla 4. 8 MTU para distintas redes.	- 49 -
Tabla 5. 1 Requerimientos para el uso del softphone X-Lite	- 67 -
Tabla 5. 2 Nueva dirección IP del servidor.....	- 72 -
Tabla 5. 3 Tipo A.	- 73 -
Tabla 5. 4 Tipo B.	- 73 -

Lista de figuras

Figura 2. 1 Red VoIP en conexión con una red tradicional.	- 5 -
Figura 2. 2 Proceso de Codificación.	- 9 -
Figura 2. 3 Aplicaciones de VoIP.	- 12 -
Figura 2. 4 Latencia.	- 13 -
Figura 2. 5 Variación de retraso.	- 13 -
Figura 3. 1 Bloque de Protocolos para Multimedia por Internet.	- 18 -
Figura 3. 2 Usuario C invita a una sesión de voz al usuario A y usuario B.	- 19 -
Figura 3. 3 El usuario registra en el servidor su posición actual.	- 20 -
Figura 3. 4 Servidor de Registro.	- 23 -
Figura 3. 5 Ejemplo de un Servidor de Re-direccionamiento.	- 25 -
Figura 3. 6 El Request-URI contiene el siguiente salto del camino.	- 31 -
Figura 3. 7 Formato de Petición y Respuesta de SIP.	- 32 -
Figura 4. 1 Formato de SDP.	- 35 -
Figura 4. 2 Encabezado de RTP.	- 38 -
Figura 4. 3 Ejemplo de la negociación de un codec empleando el protocolo SIP.	- 39 -
Figura 4. 4 Encabezado de UDP.	- 41 -
Figura 4. 5 Encabezado del Protocolo de Internet.	- 43 -
Figura 4. 6 Encabezado del Protocolo ARP.	- 47 -
Figura 4. 7 Encapsulamiento de un paquete de petición o consulta ARP.	- 47 -
Figura 4. 8 Encabezado ICMP.	- 47 -
Figura 4. 9 Encabezado de Ethernet.	- 50 -
Figura 4. 10 Protocolos que interviene con SIP.	- 51 -
Figura 4. 11 Diagrama de casos de los elementos principales para SIP.	- 51 -
Figura 4. 12 Diagrama de flujo de una conversación empleando SIP.	- 53 -
Figura 4. 13 Diagrama de secuencia de una transacción de invitación (<i>Invite</i>).	- 55 -
Figura 4. 14 Diagrama de secuencia de la finalización de una llamada.	- 56 -
Figura 5. 1 Red inicial del sistema experimental.	- 59 -
Figura 5. 2 Selección del tipo de teclado.	- 60 -
Figura 5. 3 Selección de zona horaria.	- 61 -
Figura 5. 4 Asignación de contraseña para la cuenta root.	- 61 -
Figura 5. 5 Configuración de la red.	- 62 -
Figura 5. 6 Configuración manual o dinámica de la red.	- 62 -
Figura 5. 7 Pantalla de inicio de la interfaz de TrixBos.	- 63 -
Figura 5. 8 Pantalla de inicio de FreePBX.	- 63 -
Figura 5. 9 Creación de una extensión por el administrador.	- 65 -
Figura 5. 10 Parámetros requeridos para la configuración de un softphone.	- 66 -
Figura 5. 11 X-Lite versión 3.0.	- 67 -
Figura 5. 12 Softphone SJphone.	- 68 -
Figura 5. 13 Servidor y terminal administradora.	- 69 -
Figura 5. 14 Mensaje alertando de que está entrando una llamada.	- 69 -

Figura 5. 15 Información de la conversación realizada.	- 69 -
Figura 5. 16 Estadística de llamadas por mes durante el periodo abril-diciembre 2008.	- 71 -
Figura 5. 17 Topología de red con acceso desde el exterior a la red local de CITEDI.	- 73 -
Figura 5. 18 Flujo de mensajes en una llamada VoIP empleando SIP.	- 74 -
Figura 5. 19 Mensaje de inicio de la llamada.	- 75 -
Figura 5. 20 Mensaje de autenticación	- 76 -
Figura 5. 21 Envío de mensaje ACK de confirmación.	- 76 -
Figura 5. 22 Envío del mensaje ‘100 Trying’	- 77 -
Figura 5. 23 Envío de mensaje ‘180 Ringing’	- 77 -
Figura 5. 24 Envío de mensaje ‘200 OK’	- 78 -
Figura 5. 25 Mensaje fin (<i>bye</i>) para finalizar la llamada.	- 79 -
Figura 5. 26 Mensaje de aceptación ‘200 OK’	- 79 -
Figura 5. 27 Protocolos que intervienen en la transmisión empleando SIP.....	- 80 -
Figura 5. 28 Campos del Protocolo SDP.	- 80 -

Lista de símbolos y acrónimos

ARP	<i>Address Resolution Protocol</i>	Protocolo de Resolución de Direcciones
ATA	<i>Analog telephone adapter</i>	Adaptador para teléfono analógico
BIT RATE	<i>Bit rate</i>	Tasa de Bit
BITS	<i>Binary Digit</i>	Digito Binario
BW	<i>Band width</i>	Ancho de Banda
CODEC	<i>COder-DECoder</i>	Codificador-Decodificador
DNS	<i>Domain Names System</i>	Registro de Nombres de Dominio
Gbps	<i>Gigabits per seconds</i>	Gigabit por segundo
GSM	<i>Global System for Mobile communications</i>	Sistema Global para Comunicaciones Móviles
HTTP	<i>Hypertext Transfer Protocol</i>	Protocolo de Transferencia de Hipertexto
ICMP	<i>Internet Control Message Protocol</i>	Protocolo de Mensajes de Control de Internet
IETF	<i>The Internet Engineering Task Force</i>	Grupo de tareas de Ingeniería de Internet
IP	<i>Internet Protocol</i>	Protocolo de Internet
ITU	<i>Internacional Telecommunication Union</i>	Unión Internacional de Telecomunicación
LAN	<i>Local area network</i>	Red de area local
LLC	<i>Logical Link Control</i>	Control de Enlace Lógico
MAC	<i>Medium Accesess Control Address</i>	Control de Acceso al Medio
Mbps	<i>Megabits per seconds</i>	Megabits por Segundo
MGC	<i>Media Gateway Control Protocol</i>	Protocolo de Control de Entrada de los Medios
MOS	<i>Mean opinion Score</i>	Valor de Opinión Promedio
ms	<i>Miliseconds</i>	Milisegundos
MTU	<i>Maximum Transfer Unit</i>	Unidad Máxima de Transferencia
PCM	<i>Pulse Code Modulation</i>	Modulación por Codificación de Pulsos
PDU	<i>Protocol Data Unit</i>	Unidad de Datos de Protocolo
QoS	<i>Quality of Service</i>	Calidad de Servicio
RFC	<i>Request for Comments</i>	Petición de Comentarios
RTCP	<i>Real-time Transport Control Protocol</i>	Protocolo de Control de Transporte en Tiempo Real
RTP	<i>Real-time Transport Protocol</i>	Protocolo de Transporte en Tiempo Real
RTT	<i>Round-trip time</i>	Tiempo de Viaje de Ida y Vuelta
SCCP	<i>Skinny Client Control protocol</i>	Protocolo de Control de Cliente
SDP	<i>Session Description Protocol</i>	Protocolo de Descripción de Sesión
SID	<i>Silence insertion description</i>	Descripción de Paquetes de Silencio
SIP	<i>Session Initiation Protocol</i>	Protocolo de Inicio de Sesión
SMTP	<i>Simple Mail Transfer Protocol</i>	Protocolo Simple de Transferencia de Correo

UA	<i>User Agent</i>	Agente Usuario
UDP	<i>User Datagram Protocol</i>	Protocolo de Datagrama de Usuario
URI	<i>Uniform Resource Identifier</i>	Identificador de Recursos Uniformes
VAD	<i>Voice activity detection</i>	Detección de Actividad de Voz
VoIP	<i>Voice over IP</i>	Voz sobre IP
WWW	<i>World Wide Web</i>	Red Mundial

CONTENIDO

RESUMEN.....	I
ABSTRACT.....	II
LISTA DE TABLAS.....	III
LISTA DE FIGURAS.....	IV
LISTA DE SÍMBOLOS Y ACRÓNIMOS	VI
1 INTRODUCCIÓN	- 1 -
2 TELEFONÍA IP.....	- 3 -
2.1 VOZ SOBRE IP	- 4 -
2.1.1 Protocolo de Internet.....	- 5 -
2.1.2 Equipamiento para VoIP	- 7 -
2.2 CODIFICACIÓN	- 8 -
2.2.1 Codec	- 10 -
2.3 CALIDAD DE SERVICIO.....	- 11 -
2.3.1 Latencia.....	- 13 -
2.3.2 Variación del retraso	- 13 -
2.3.3 Ancho de banda.....	- 14 -
2.3.4 Supresión de silencios.....	- 14 -
2.3.5 Eco	- 15 -
3 PROTOCOLO DE INICIO DE SESIÓN	- 17 -
3.1 DEFINICIÓN	- 18 -
3.1.1 Establecimiento, modificación y terminación de sesión.....	- 18 -
3.1.2 Movilidad del usuario	- 19 -
3.1.3 Registros	- 20 -
3.2 ARQUITECTURA	- 21 -
3.2.1 Elementos de la arquitectura.....	- 21 -
3.2.2 Agentes de Usuario.....	- 22 -
3.2.3 Servidores	- 22 -
3.3 OPERACIÓN DEL PROTOCOLO SIP	- 25 -
3.3.1 Mensaje de Peticiones.....	- 26 -
3.3.2 Métodos.....	- 26 -
3.3.3 Mensaje de Respuesta.....	- 28 -
3.3.4 Tipos de respuestas	- 28 -
3.4 FORMATO DE LOS MENSAJES SIP.....	- 30 -
3.4.1 Petición	- 31 -
3.4.2 Respuestas.....	- 32 -
3.4.3 Cuerpo del mensaje SIP.....	- 32 -

4 ANÁLISIS DE LOS PROTOCOLOS EMPLEADOS EN VOIP	- 34 -
4.1 PROTOCOLO DE DESCRIPCION DE SESIÓN (SDP)	- 34 -
4.1.1. <i>Función de SDP</i>	- 35 -
4.1.2 <i>Formato SDP</i>	- 35 -
4.2 PROTOCOLO DE TRANSMISION EN TIEMPO REAL	- 37 -
4.2.1 <i>Función de RTP</i>	- 38 -
4.2.2 <i>Encabezado RTP</i>	- 38 -
4.3 PROTOCOLO DE DATAGRAMA DE USUARIO (UDP).....	- 41 -
4.3.1 <i>Función de UDP</i>	- 41 -
4.3.2 <i>Encabezado UDP</i>	- 41 -
4.4 PROTOCOLO DE INTERNET (IP)	- 42 -
4.4.1 <i>Función de IP</i>	- 42 -
4.4.2 <i>Encabezado IP</i>	- 43 -
4.5 ETHERNET	- 49 -
4.5.1 <i>Función de Ethernet</i>	- 49 -
4.5.2 <i>Encabezado Ethernet</i>	- 50 -
4.6 COMPORTAMIENTO DE SIP	- 50 -
4.6.1 <i>Elementos básicos en el empleo del Protocolo SIP</i>	- 51 -
4.6.2 <i>Establecimiento de una llamada de Voz sobre IP</i>	- 52 -
5 IMPLEMENTACIÓN EXPERIMENTAL	- 58 -
5.1 ARQUITECTURA DE RED.....	- 58 -
5.2 INSTALACION DEL SOFTWARE DEL SISTEMA	- 59 -
5.2.1 <i>Configuración del Servidor</i>	- 60 -
5.2.2 <i>Configuración de la Interfaz</i>	- 63 -
5.2.3 <i>Instalación y configuración del Softphone</i>	- 65 -
5.3 PRUEBAS DE COMUNICACION	- 68 -
5.3.1 <i>Acceso fuera de la red local</i>	- 71 -
5.4 ANÁLISIS DEL TRAFICO DE VOZ EN TIEMPO REAL.....	- 74 -
6 CONCLUSIONES	- 82 -
REFERENCIAS.....	- 84 -
APÉNDICE.....	- 88 -

CAPITULO 1

INTRODUCCIÓN

La tecnología de Voz sobre IP (*Voice over IP: VoIP*) ha evolucionado de manera rápida y los servicios que actualmente se proveen son de mayor calidad con respecto a años anteriores. El auge se debe principalmente a que el uso de Internet se ha convertido cotidianamente en una necesidad y con este servicio se pueden realizar numerosas actividades sin salir del trabajo o del hogar como: realizar pagos, hacer llamadas telefónicas o incluso mantener una videoconferencia.

Es así como los usuarios de Internet aumentan cada día, en el 2008 el porcentaje llegó a 16.6 % de la población total en América del Norte, concentrándose el mayor porcentaje en Asia con el 40.0 %. Otro países con alto uso son Dinamarca, Alemania, Japón, EUA, Francia, Italia, España [1]. En México 1.6 millones de habitantes tienen acceso a Internet de una población estimada de 103,263,388 hasta el 2005 [2].

De los usuarios a nivel mundial conectados a Internet, 11 millones son usuarios VoIP [3] hasta el 2005, lo cual indica un crecimiento en el uso de llamadas mediante el servicio de Internet. Existen infinidad de proveedores VoIP en todo el mundo, pero los que tienen mayor demanda en Norteamérica son AOL, AT&T, Avaya, CISCO System [4]. En el ámbito empresarial el 80% de las empresas encuestadas están utilizando, probando o pensando en instalar un sistema VoIP y de aquellos que ya son usuarios el 63% piensa invertir más [5].

Con lo anterior, se reafirma que la tecnología de Voz sobre IP crece de manera constante, siendo un servicio tanto para empresas como para los hogares. Esto indica que hay mayor demanda en

1. INTRODUCCIÓN

equipos, proveedores y técnicos abriendo el espectro para el desarrollo de nuevas y mejores oportunidades de empleos, negocios, herramientas, aplicaciones etc.

Lo anterior justifica la realización de proyectos de investigación en esta área tan dinámica y por tal razón este trabajo plantea el siguiente objetivo el cual es: “Análisis que sigue la transmisión de un mensaje de VoIP empleando el Protocolo de Inicio de Sesión (SIP) en una arquitectura de red específica implementada en una plataforma experimental de voz sobre IP”

Para cumplir con lo anterior fue necesario plantear objetivos específicos en cada etapa los cuales fueron:

- Estudio del proceso que sigue la voz analógica de las comunicaciones de Voz sobre IP.
- Analizar la función y comportamiento del Protocolo de Inicio de Sesión en una red VoIP y de los protocolos que intervienen en el proceso de comunicación.
- Implementar un sistema experimental Voz sobre IP en una plataforma económica. Logrando la comunicación entre terminales SIP.

La tesis está estructurada de la siguiente manera: el Capítulo I, describe el estado actual de la tecnología de Voz sobre IP, así como las estadísticas que demuestran su evolución. En el Capítulo 2, se presenta el concepto de VoIP, las funciones que lleva a cabo, los elementos necesarios para la transmisión como el equipo y la calidad de servicios, así como conceptos relacionados con el tema. En el Capítulo 3, se presenta la función del Protocolo de Inicio de Sesión, sus elementos y arquitectura dentro del sistema de comunicación, así como el formato de mensajes SIP, tanto para peticiones como respuesta. En el Capítulo 4, se analizan los protocolos que intervienen en la trayectoria de un mensaje de voz utilizando SIP los cuales pertenecen al Bloque de Protocolos para Multimedia por Internet. En el Capítulo 5, se explica la implementación del sistema experimental de Voz sobre IP, los pasos para la configuración del software y hardware utilizado en la topología de red y los recursos necesarios para poder establecer una llamada de voz en tiempo real. En el Capítulo 6, se finaliza con las conclusiones que se obtuvieron en el desarrollo del trabajo así como las limitaciones actuales y una propuesta para trabajo a futuro.

CAPÍTULO 2

TELEFONÍA IP

En este capítulo se realiza una revisión de la telefonía de Voz sobre IP (*Voice over Internet Protocol: VoIP*), y los principales elementos que la componen los cuales son: Protocolo IP, conversión analógica-digital, tipos de codecs (codificador-decodificador), factores que impactan en la Calidad de Servicio (*Quality of Services: QoS*) y diferentes aplicaciones que existen.

En la telefonía VoIP la voz es digitalizada por el proceso de conversión analógica-digital, el cual tiene tres pasos: muestreo, cuantificación y codificación. Después se hace uso del protocolo de Internet (*Internet Protocol: IP*), que tiene como función encaminar los paquetes de voz hacia su destino. IP se sirve de varios protocolos para brindar un mejor servicio puesto que actúa bajo el método de mejor esfuerzo (*best effort*) en el cual no cuenta con un mecanismo que le permita verificar si un mensaje llegó a su destino de manera correcta y no asegura la calidad de información. Es conveniente reducir el tamaño de la información para que la transmisión sea en menor tiempo, para eso existen varios esquemas de compresión o codec (codificador-decodificar), que funcionan aplicando algún tipo de algoritmo que disminuya el tamaño sin comprometer la calidad, algunos son mejores que otros y eso depende de la aplicación que se esté utilizando.

Existen otros factores en la telefonía VoIP como: el ancho de banda, latencia, variación de retardo y que impactan la calidad de lo transmitido. Debido a que la voz tiene que enviarse en tiempo real las dificultades aumentan.

2.1 Voz sobre IP

Dado que la tecnología de Voz sobre IP transporta de conversaciones telefónicas a través de una red bajo el Protocolo IP esto se realiza mediante el envío de tramas de información. Todas las tramas deben reconstruirse en el orden correcto, y prácticamente de forma inmediata, a diferencia de lo que ocurre con otras transmisiones sobre IP. Estas tramas cuando están reordenadas, forman un mensaje de voz para el usuario final [5].

En VoIP, es necesaria la prioridad, ya que es preciso que la información llegue en tiempo real. En algunas aplicaciones por ejemplo el correo electrónico no es indispensable que la información se transmita de esa forma, puesto que son datos y no voz.

El tiempo de llegada de mensajes en VoIP, es crítico, este factor es uno de los tantos que determinan la calidad de la llamada. El ancho de banda, puede afectar la calidad de la conversación que puede ver degradada, el retraso de la voz del transmisor al receptor distorsiona la secuencia de la conversación. Estos factores determinan la calidad de servicio (*Quality of Service: QoS*) la cual es imprescindible para sostener una plática telefónica aceptable.

En la figura 2.1 se aprecia la arquitectura VoIP, que marca tres elementos importantes:

1. Terminales
2. *Gatekeepers* o servidores
3. *Gateway*.

1.- **Terminales:** definidas como los sustitutos de los teléfonos tradicionales, se clasifican en los en tres dispositivos: teléfono basado en software, teléfono basado en hardware y teléfono VoIP. También podemos utilizar un teléfono analógico mediante un adaptador (*Analog Telephone Adapter: ATA*).

2.- ***Gatekeepers*** (H.323) o **servidores** (SIP) son el centro de toda la organización VoIP, serían el sustituto para las actuales centrales, puesto que gestionan la administración de los usuarios incluyendo la creación, modificación y eliminación de registros, realizan la señalización entre

2. TELEFONÍA IP

dos usuarios y monitorean en todo momento la llamada, normalmente implementados en software o hardware.

3.- **Gateway** su función es enlazar con la red telefónica tradicional, actuando de forma transparente para el usuario. Es preciso destacar el uso de protocolos en estas aplicaciones, que son un conjunto de reglas que controlan la continuidad de mensajes que suceden durante una comunicación entre entidades que forman una red. VoIP trabaja con varios protocolos por ejemplo: el Protocolo de Inicio de Sesión (*Session Initiation Protocol: SIP*), Protocolo H.323, Protocolo IAX (*Inter Asterisk Exchange: IAX*), Protocolo de Control de Entrada de los Medios (*Media Gateway Control Protocol: MGC*), Protocolo de Control de Cliente (*Skinny Client Control Protocol: SCCP*) [6]. En el capítulo III abordaremos el protocolo SIP con mayor detalle.

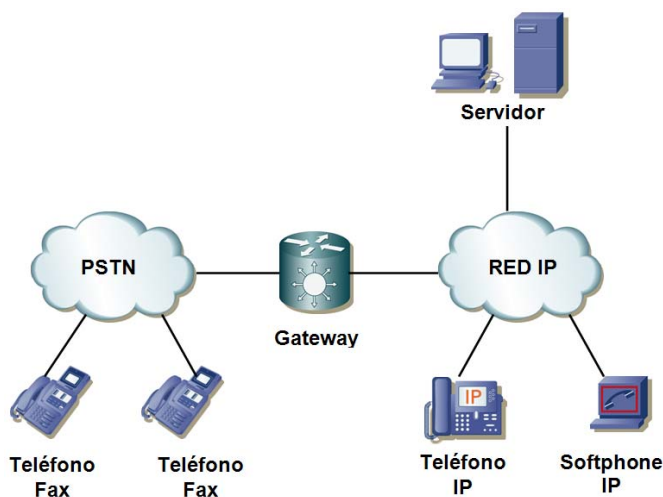


Figura 2. 1 Red VoIP en conexión con una red tradicional.

2.1.1 Protocolo de Internet

El protocolo de Internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son 'hosts' identificados por direcciones de longitud fija. El protocolo Internet también se encarga, si es

2. TELEFONÍA IP

necesario, de la fragmentación y el ensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos host a host. El protocolo Internet puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

Operación

El Protocolo de Internet implementa dos funciones básicas: direccionamiento y fragmentación.

Direccionamiento

Se establece una distinción entre nombres (dominio), direcciones (IP) y rutas (recorrido de un emisor a un receptor), el módulo de Internet hace corresponder los nombres con las direcciones IP, es tarea de los procedimientos de la capa superior (es decir, redes locales o 'gateway') realizar la correspondencia entre direcciones de red local y rutas. Las direcciones son de longitud fija de 4 octetos (32 bits).

Fragmentación

La fragmentación de un datagrama Internet es necesaria cuando éste se origina en una red local que permite un tamaño desmedido y debe atravesar una red externa que limita los paquetes a un tamaño inferior. Es necesario dividir el paquete de modo que se disminuya el tamaño y pueda atravesar por la red.

El protocolo de Internet utiliza cuatro mecanismos clave para suministrar su servicio:

- Tipo de servicio
- Tiempo de vida
- Opciones
- Suma de control de encabezado.

2. TELEFONÍA IP

El **Tipo de servicio** se utiliza para indicar la calidad del servicio deseado. Es un conjunto generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet.

El **Tiempo de vida** es una indicación de un límite superior en el periodo de vida de un datagrama. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado.

Las **Opciones** proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y enrutamiento especial.

La **Suma de control de encabezado** proporciona una verificación a la información utilizada al procesar el datagrama, siendo ésta transmitida correctamente.

El protocolo de Internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo, ni entre extremos ni entre saltos. No hay control de errores para los datos, sólo una suma de control de encabezado. No hay retransmisiones. No existe control de flujo [7],[8].

2.1.2 Equipamiento para VoIP

Teléfonos VoIP

Llamado teléfono IP, permite al usuario hacer llamadas a cualquier otro teléfono por medio de la tecnología de voz sobre IP, de esta manera la voz es transmitida sobre la red de Internet, basado en software como el *softphone* ó un aparato telefónico. Algunas de las funciones más comunes de un teléfono VoIP son: identificador de llamadas, transferencia de llamadas, llamada en espera.

Algunas de las características de teléfonos VoIP son:

- Ancho de banda reducido: inclusión de codecs de alta compresión (ejemplo: G.729, GSM, Speex).

2. TELEFONÍA IP

- Buena interfaz de administración: inclusión de interfaz web.
- Salida de audio: inclusión de salida externa de audio y soporte de manos libres (para educación a distancia).

Telefonía implementa mediante Software

Una alternativa al uso de equipos dedicados (físicos) de VoIP es el uso de programas para emularlos. Estos programas se conocen como *softphones* y funcionan en cualquier dispositivo, en este caso una computadora. El único requerimiento es tener una tarjeta de sonido en funcionamiento y estar seguro de que el cortafuegos instalado en la máquina, no está bloqueando a la aplicación.

Adaptador para Teléfonos Analógicos

Un adaptador para teléfonos analógicos (ATA) o adaptador telefónico (TA) conecta un teléfono ordinario a una red de Internet. Un ATA tiene un conector RJ11 (el conector de teléfono) y un RJ45 (el conector de red o Ethernet), solo es necesario tener conexión a Internet. A comparación del *softphone* tiene mejor calidad de sonido y no se ve afectado por problemas del sistema operativo [9].

2.2 Codificación

Representar una forma de onda analógica como es la voz en forma digital, requiere de contar con un número discreto de muestras de la señal analógica y entonces representar cada muestra con un número de bits. Al recuperar la señal, se podrían tomar un número infinito de muestras, sin embargo el Teorema de Nyquist [10] indica que para poder reconstruir una señal conviene que ésta sea muestreada como mínimo al doble de la frecuencia más alta contenida en la señal original. De esta manera si la señal de voz tiene como frecuencia máxima 4000 Hertz, es necesario tomar 8000 muestras por segundo para reconstruir dicha señal [11]. Una vez que se cuenta con la muestra de la señal original, se discretiza en amplitud esto es, otorgarle a cada muestra un valor discreto de voltaje; el número de bits depende del estándar a utilizar, son 7 bits

2. TELEFONÍA IP

para el americano y 8 bits para el europeo, a este proceso se le conoce como cuantificación. Para finalizar, en el proceso de codificación se le asigna un valor binario a cada valor de voltaje.

La figura 2.3 muestra los procesos que la voz tiene que pasar antes de poder ser enviada a su destino.

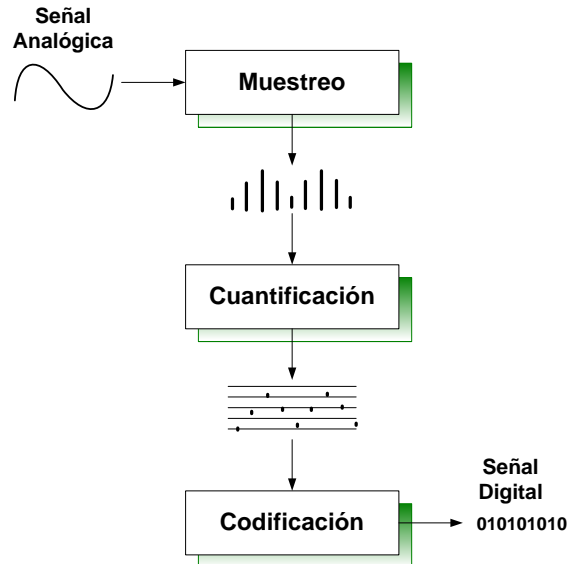


Figura 2. 2 Proceso de Codificación.

Ya que se tiene la señal analógica digitalizada se procede a decidir qué tipo de codificación se requiere para la transmisión, en lo cual se emplea un codec (codificador-decodificador) para la fuente y destino. Una de las funciones del codec es comprimir la información de tal manera que reduzca el tamaño de la señal digitalizada y ésta se transmita con mayor facilidad por la red.

Tabla 2. 1 Métodos de compresión.

METODO DE COMPRESION	CODEC	BIT RATE	
PCM	Pulse Code Modulation	G.711	64 Kbps
ADPCM	Adaptive Differential Pulse Code Modulation	G.726	32 Kbps
LDCELP	Low-Delay Code Excited Linear Prediction	G.728	16 Kbps
CS-ACLEP	Conjugate-Structure Algebraic-Code-Excited-Linear-presition	G.729,a	8 Kbps

2.2.1 Codec

Existen varios tipos de codecs los cuales se pueden clasificar en tres grupos: codecs de forma de onda, codecs fuente o vocoders y los codecs híbridos. Los codecs de forma de onda funcionan muestreando y codificando la señal analógica sin ningún conocimiento de la señal, los codecs fuente intentan aproximar la señal analógica entrante a un modelo matemático y los codecs híbridos proporcionan lo mejor de los dos anteriores [11]. La Unión Internacional de Telecomunicaciones (*International Telecommunication Union: ITU*) [12] tiene varias recomendaciones acerca de los codecs de onda, los cuales se encuentran en la tabla 2.3 y descritos más adelante.

La calidad de los codecs se mide de acuerdo a una prueba llamada “Valor de Opinión Promedio” (*Mean Opinion Score: MOS*). Esto se lleva a cabo, con un grupo de personas que escuchan un determinado audio comprimido por el codec. Como la calidad de la voz y el sonido en general es subjetiva, es necesario contar con numerosos oyentes y un material de muestra. Los oyentes de cada muestra de audio, tienen un rango del uno (malo) al cinco (excelente) para calificar. El resultado final, es el promedio de la cantidad de oyentes y las calificaciones dadas por los mismos. La Tabla 2.2 da a conocer el rango de valores, desde uno siendo la puntuación más baja, hasta cinco que es la puntuación más alta [11], [13].

Tabla 2. 2 Parámetros de MOS.

PUNTUACION	CALIDAD	NIVEL DE DISTORCION
5	Excelente	Imperceptible
4	Buena	Perceptible, pero no molesto
3	Aceptable	Perceptible y ligeramente molesto
2	Pobre	Molesto
1	Insatisfactoria	Muy molesto

La tabla 2.3 muestra los principales codec de onda y detalla las siguientes cualidades: ‘bit rate’ (*número de bits transmitidos en un segundo*), tamaño de muestra en milisegundo y parámetro de puntuación de MOS.

Tabla 2. 3 Codecs de audio de la ITU.

CODEC	BIT RATE KBPS	TAMAÑO DE MUESTRA (ms)	MOS
G.711	64	0.125	4.1
G.726	32	0.125	3.85
G.728	16	0.625	3.61
G.729	8	10	3.92 – 3.7
G.723	6.3 y 5.3	30	3.9 y 3.65

El codec que según la tabla 2.3 reúne las mejores características es el codec G.711 y este describe la técnica de codificación de forma de onda, con una frecuencia de muestro de 8000 Hertz utilizada en la telefonía tradicional. Tiene dos variantes: Ley μ (en EUA) y Ley a (en Europa), las dos proveen buena calidad de acuerdo a MOS, el inconveniente es el uso de 64 Kbps de ancho de banda.

Dependiendo de la aplicación es el tipo de codec a utilizar, si la muestra es muy grande y se requiere del uso de varios envíos a la vez, entonces se puede optar por codecs como G.723 en sus dos variantes [11], [13]. Esto tiene cierta importancia en la calidad de servicio puesto que si se minimiza demasiado el tamaño de un paquete puede que la calidad se vea comprometida para el usuario final. A continuación se presentan algunos de los factores principales en la Calidad de Servicio (QoS).

2.3 Calidad de servicio

Internet y el protocolo de Internet se diseñaron para proporcionar un servicio que realice el mejor esfuerzo en la entrega. En este mecanismo del mejor esfuerzo (*Best Effort*), Internet o una Intranet privada tratan por igual a todos los paquetes de datos. Conforme crece el nivel de tráfico en las redes, y se produce la congestión, la entrega de todos los paquetes se vuelve lenta. Si la congestión llega a ser severa, se descartan paquetes más o menos de forma aleatoria para aliviar dicha congestión. No se hace ninguna distinción en términos de la importancia relativa de ningún tipo de tráfico o en sus requisitos de temporización.

2. TELEFONÍA IP

Con el tremendo incremento del volumen de tráfico, y con la introducción de nuevas aplicaciones en el tiempo real, multimedia y multidifusión, los protocolos y servicios tradicionales de Internet son lamentablemente inadecuados. Pero las necesidades de los usuarios han cambiado.

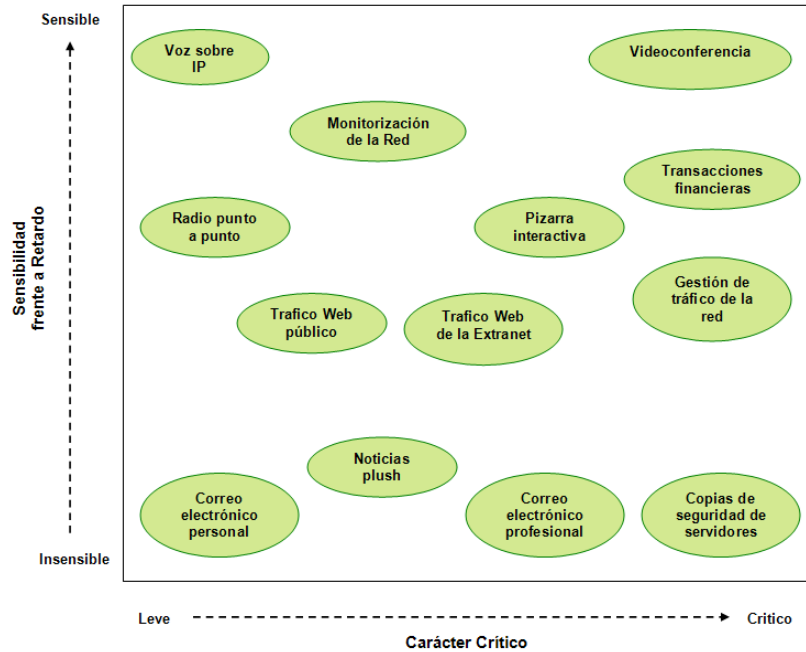


Figura 2. 3 Aplicaciones de VoIP.

La figura 2.3 muestra varias aplicaciones que son sensibles a retardos y que son de carácter crítico como en el caso de la videoconferencia, donde la conexión es en tiempo real y requiere de un ancho de banda satisfactorio en los dos sentidos, de no ser así la comunicación puede llegar a ser molesta y no perceptible. Los correos electrónicos son insensibles puesto que el retardo no es una desventaja, ya que no tienen un tiempo exacto de llegada, además, su uso conlleva la pérdida de paquetes o errores al recibir y por lo tanto los usuarios tienen noción de que el proveedor puede fallar. Algunos factores que pueden impactar la calidad de servicio de voz son:

- Latencia
- Variación del retraso
- Ancho de Banda
- Supresión de Silencios
- Eco

Con mayor detalle son presentados a continuación [8].

2.3.1 Latencia

Corresponde al tiempo que le toma a un mensaje viajar de un extremo de la red a otro, se mide en términos de tiempo, algunas situaciones también requieren el tiempo que tarda en regresar el mensaje, en otras palabras un viaje de ida y de regreso, a este tipo de latencia se le llama Tiempo de Viaje de Ida y Vuelta (*Round-Trip Time: RTT*). En la figura 2.4, se muestra la distancia que recorre un paquete a través de Internet hasta que llega a su destino, al salir el paquete es cero conforme transcurre su recorrido ésta aumenta, llegado a su destino el total del tiempo es el valor de la latencia en milisegundos [14], [15].

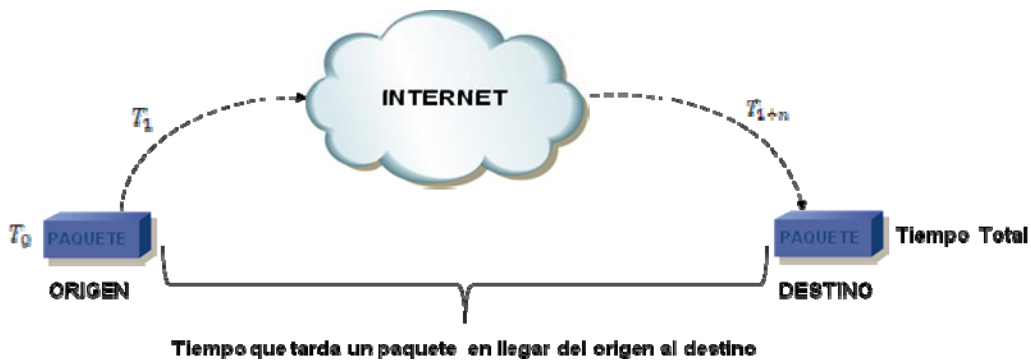


Figura 2. 4 Latencia.

2.3.2 Variación del retraso

Es la variación del tiempo de retraso entre un paquete y otro, ocurre porque la velocidad de propagación de la señal por un medio guiado varía con frecuencia. En la figura 2.5, un mensaje es enviado en la red con cierto retraso, el siguiente paquete puede tener diferente retraso debido a factores como el tráfico; esta variación del retraso ocasiona que se distorsione la voz.



Figura 2. 5 Variación de retraso.

2.3.3 Ancho de banda

El ancho de banda (*BandWidth: BW*) de una red puede definirse como la cantidad máxima de información que la red es capaz de transportar (por unidad de tiempo). El primer requisito que debe cumplir una red de voz sobre paquetes para ofrecer la calidad adecuada es disponer del ancho de banda suficiente para cursar las comunicaciones de voz. En general el ancho de banda debe ser tal como se muestra en la siguiente ecuación [14].

$$BW = \frac{BW_{VOZ} + BW_{VID} + BW_{DAT}}{0.75} \quad (2.1)$$

donde:

BW = ancho de banda.

BW_{VOZ} = ancho de banda de la voz.

BW_{VID} = ancho de banda de video.

BW_{DAT} = ancho de banda de los datos.

El margen para posible congestión de tráfico es del 25%. Al dimensionar una red, según este criterio, se garantiza que habrá ancho de banda suficiente para cursar las comunicaciones, se reduce las probabilidades de que el retardo y las pérdidas tengan un impacto considerable.

2.3.4 Supresión de silencios

Es un mecanismo complementario al empleo de codecs compresores para reducir el ancho de banda. Se trata de aprovechar el que en una conversación existan tiempos en donde el emisor y receptor no emiten ningún sonido, estadísticamente el 60% del tiempo es de esta manera, debido a las pausas y al turno en la conversación. La función de la supresión de silencios consiste en utilizar estos tiempos muertos en donde el canal esta libre para, entonces aprovecharlos en otras conversaciones de voz. Obteniendo el 60% de ahorro en el flujo de paquetes. Estas técnicas

2. TELEFONÍA IP

reciben el nombre de detección de actividad o supresión de silencios (*Voice Activity Detection: VAD*).

Con el fin de evitar que el interlocutor piense que se ha cortado la comunicación durante los intervalos de silencio se envían periódicamente paquetes de silencio (*Silence Insertion Description: SID*) durante la pausa. Estos paquetes proporcionan una indicación de ruido que existe en el origen para que el receptor lo simule en el terminal remoto mediante un generador de ruido

Cabe destacar que aunque esta técnica proporcione una posibilidad de reducir el ancho de banda también provoca ciertas desventajas. Como el llamado fenómeno *clipping*; que consiste en que la voz del interlocutor parece recortada. Las pérdidas de paquetes, la latencia y variación del retraso pueden producir este fenómeno.

2.3.5 Eco

Se produce cuando el emisor escucha parte de su propia voz junto con la voz del otro interlocutor o en ausencia de ella. Las causas del eco son muy variadas las cuales se mencionan a continuación:

- Eco acústico
- Eco eléctrico

El primero se refiere a un acoplamiento entre el micrófono y el auricular, se puede solucionar adquiriendo equipos de mayor calidad, pero a la vez de mayor precio. El segundo eco es consecuencia de un desacople de impedancias en el extremo receptor [14], [15].

En este Capítulo se presentó una breve introducción a la tecnología de VoIP. Así como las características, elementos (hardware y software) y conceptos relacionados al tema. De acuerdo a VoIP, existen varios protocolos de señalización, en el capítulo 3 “Protocolo de Inicio de Sesión”

2. TELEFONÍA IP

se muestra de manera más detallada las funciones, la arquitectura, el formato y método de envío de mensajes, la relación con otros protocolos y ejemplos de registro y establecimiento de una sesión SIP .

CAPÍTULO 3

PROTOCOLO DE INICIO DE SESIÓN

Actualmente se desarrolla e inicia el surgimiento de un conjunto de protocolos y tecnologías de red, con las que se pretende sentar las bases necesarias para que la comunicación multimedia en tiempo real a través de Internet tenga una amplia disponibilidad como la comunicación de texto y datos. Además, se pretende que estos nuevos sistemas puedan interoperar con la red de Internet.

El propósito de lograr un sistema de telecomunicaciones universal es que tengan cabida contenidos tan diversos como correo electrónico, voz o fax entre otros, para eso es necesario avances en diversos campos. Este capítulo se centrará en la arquitectura y los protocolos propuestos por El Grupo de Tareas de Ingeniería de Internet (*The Internet Engineering Task Force: IETF*) [16] en particular, con el Protocolo de Inicio de Sesión.

El protocolo SIP es el encargado de la señalización dentro de una conversación de voz sobre IP. Cuenta con dos elementos principales: agentes usuarios y agentes servidores, está basado en el Protocolo de Transferencia de Hipertexto (*Web Hypertext Transfer Protocol: HTTP*), el cual utiliza el método de petición-respuesta. El usuario cuenta con un registro, así como un número único con el cual puede comunicarse con otro si lo desea y entablar, modificar o terminar una conversación.

3. PROTOCOLO DE INICIO DE SESIÓN

3.1 Definición

El Protocolo de Inicio de Sesión (*Session Initiation Protocol: SIP*) es una forma de señalización, las funciones de éste protocolo son: establecer modificar y terminar sesiones. Así como, solicitar (petición) y enviar (respuesta) mensajes en tiempo real sobre Internet.

Fue desarrollado por el IETF y publicado en 1999 en el RFC 2543 [17] y eventualmente se publicó el crecimiento de SIP y sus cambios en el RFC 3261 [18].

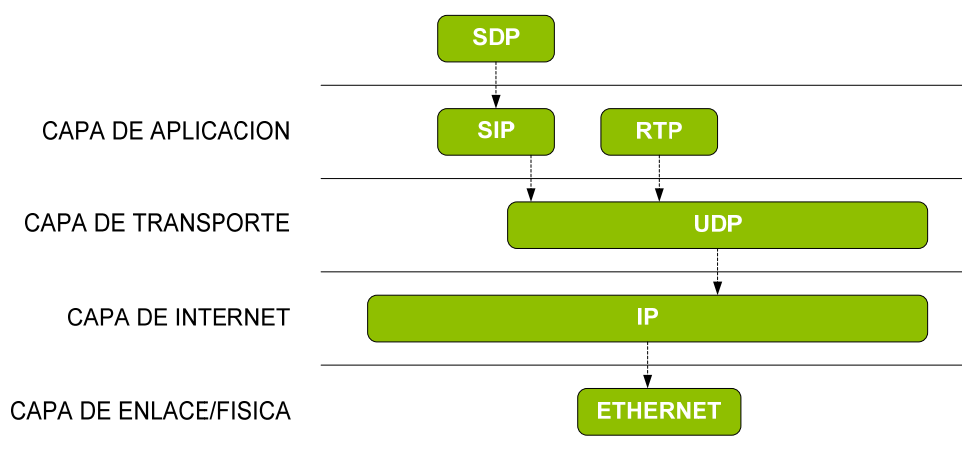


Figura 3. 1 Bloque de Protocolos para Multimedia por Internet.

3.1.1 Establecimiento, modificación y terminación de sesión

El protocolo SIP es independiente del tipo de sesión multimedia y del mecanismo utilizado para describirla; es igualmente utilizado para videoconferencias, llamadas, compartir recursos o sesiones de juego, en resumen, SIP es utilizado para distribuir la descripción de las sesiones entre los participantes potenciales, como se muestra en la figura 3.2. Una vez que la descripción de la sesión es distribuida, el protocolo SIP puede ser usado para negociar y modificar los parámetros así como terminar la sesión.

3. PROTOCOLO DE INICIO DE SESIÓN



Figura 3. 2 Usuario C invita a una sesión de voz al usuario A y usuario B.

El inicio de sesión entre dos o más usuarios depende principalmente de la oferta de medios, ya que es un factor imprescindible, sin ella no puede existir la comunicación. Lleva implícito el tipo de codec que el usuario transmisor desea utilizar. El usuario receptor puede o no aceptar e incluso ofrecer otro tipo de codec. Esta negociación tiene que ser resuelta para que la conversación sea establecida, se puede dar el caso, en que un usuario determine ya no utilizar más el codec o tal vez abrir una videoconferencia. Para esto, se inicia de nuevo una negociación, sin perder el canal de comunicación y ambos usuarios ofertan sus medios.

Estos equipos de voz sobre Internet, ya sea softphone o teléfono IP son casi idénticos a los de uso analógico, ambos tienen alertas de sonidos para dar a conocer que la llamada está en curso, que se encuentra ocupado o tal vez que la llamada tuvo una falla.

3.1.2 Movilidad del usuario

El protocolo SIP no puede establecer una sesión con un participante hasta que este sea ubicado, frecuentemente el mismo usuario puede ser localizado en diferentes lugares.

SIP provee movilidad a los usuarios y es proporcionada por el Identificador de Recursos Uniformes (*Uniform Resource Identifier: URI*), mediante el cual los usuarios pueden ser identificados. La sintaxis y semántica de URI se deriva del concepto introducido por la Red

3. PROTOCOLO DE INICIO DE SESIÓN

Mundial Amplia (*World Wide Web: WWW*) que utilizan estos identificadores desde la década de los 90.

El formato URI para SIP contiene en primera instancia a SIP separada del elemento ubicación por dos puntos (:), el elemento ubicación es la dirección donde podemos localizar al usuario, es similar a una dirección de e-mail. Un ejemplo de URI es SIP: usuario.a@dominio.com. URI provee una identificación de cada usuario en SIP, se puede comparar con un número telefónico, siendo ambos un identificador único, con esto cada usuario puede ser localizado y localizar a cualquier usuario [19].

3.1.3 Registros

Un usuario tiene que estar registrado para que pueda establecer comunicación con otro usuario, para esto la información principal es la dirección IP, el nombre o extensión y el dominio. Estas son enviadas al servidor de registro donde se guardan en una base de datos, como se muestra en la figura 3.3. Este servidor tiene la función de actualizar, mantener y dar a conocer la ubicación del usuario que sea requerido por otro usuario o servidor.



Figura 3. 3 El usuario registra en el servidor su posición actual.

Si el usuario A quiere establecer una comunicación con el usuario B. El usuario A tiene su dirección SIP pública (USUARIO.B@dominio.com) por lo que, cuando el servidor de dominio.com es contactado para preguntar por usuario B, el servidor sabe donde puede ser contactado y la conexión es establecida.

3.2 Arquitectura

La recomendación de H.323 y el protocolo SIP definen mecanismos de señalización para establecer y terminar llamadas, así como otras funciones de control de conferencia, negociación de capacidades y servicios adicionales sobre redes de conmutación de paquetes. SIP se ha diseñado con la pretensión de que, desde la perspectiva de los estándares y prácticas habituales en Internet, presente las siguientes ventajas frente a H.323.

- Implementación más fácil de realizar y depurar, ya que utiliza menor cantidad de mensajes para establecer una conversación.
- Mayor flexibilidad para incorporar nuevas funciones debido a que interactúa con protocolos independientes.
- Mayor integración con otras aplicaciones y servicios Internet, ya que está basado en el método de petición respuesta de HTTP.

3.2.1 Elementos de la arquitectura

Aunque SIP se creó como un protocolo de inicio de sesiones, al igual que otros protocolos ha evolucionado, mediante la definición de nuevas funciones y servicios en forma de módulos complementarios basados en un núcleo de funciones básicas flexibles y ampliables, hasta constituirse en el protocolo de señalización y control propuesto por el IETF, como base para los servicios de telefonía y comunicación multimedia en general en Internet, así como el protocolo de señalización de la red telefónica de tercera generación y la base de algunos de los sistemas de mensajería instantánea más extendidos [20].

SIP es un protocolo de señalización cliente-servidor de nivel de aplicación válido para redes unicast y multicast, generalmente, los mensajes SIP constan de un conjunto de encabezados y un cuerpo que contiene descripciones de sesiones multimedia, siendo el Protocolo de Descripción de Sesión (*Session Description Protocol: SDP*) el formato utilizado en la actualidad.

3. PROTOCOLO DE INICIO DE SESIÓN

Puesto que el formato de los mensajes SIP es textual, basado en el Protocolo de Transferencia de Hipertexto (*Web Hypertext Transfer Protocol: HTTP*) y Protocolo Simple de Transferencia de Correo (*Simple Mail, Transfer Protocol: SMTP*) es posible desarrollar servicios SIP mediante los procedimientos extendidos en la Web. Los dos tipos de elementos presentes en la arquitectura SIP son:

- Agentes de usuario (UA)
- Servidores.

A continuación se amplía la información de los conceptos anteriores.

3.2.2 Agentes de Usuario

El agente de usuario (*User Agent*) es el software de SIP en el punto terminal o estación terminal, funciona como un cliente cuando hace las peticiones de inicio de sesión (UAC) y también actúa como un servidor cuando responde a las peticiones de sesión (UAS); por lo tanto, la arquitectura básica es de naturaleza cliente-servidor. El Agente de Usuario (UA) es inteligente, es el sentido que almacena y administra el estado de la llamada. El UA establece las llamadas usando un número y una dirección parecida al correo eléctrico.

3.2.3 Servidores

Las funciones básicas de los servidores SIP son la localización de usuarios y la resolución de nombres. Puesto que los agentes de usuario-cliente no conocen la dirección IP del destinatario de una llamada, sino su nombre de usuario SIP o un número de teléfono al que habrá de acceder a través de una gateway, necesitan enviar en primer lugar un mensaje de invitación al servidor correspondiente al nombre o número para que localice al destinatario, el servidor puede conocer la dirección del destinatario o recurrir a otros servidores para continuar la búsqueda. Cuando las llamadas se redirigen, la ruta seguida se registra en los mensajes SIP, de modo que al momento de generar respuestas se pueda conocer el camino de retorno hasta el origen del mensaje inicial.

3. PROTOCOLO DE INICIO DE SESIÓN

Los servidores SIP actúan generalmente como varios tipos de servidores de forma simultánea, debido a la infraestructura de servidores SIP, es posible gestionar las llamadas de forma distribuida entre equipos personales, equipos de proveedores de servicios y pasarelas corporativas, con la consiguiente flexibilidad y control por parte del usuario, que puede mantener la privacidad de sus datos personales en todo momento. Asimismo un mensaje SIP puede pasar por un número indeterminado de servidores desde que un agente de usuario-cliente lo envía hasta que llega al agente de usuario servidor destinatario.

Los servidores SIP pueden ser de tres tipos:

Servidor de registro

El uso de estos servidores es registrar un dispositivo después de su arranque, de modo que cuando lleguen invitaciones destinadas a él, los servidores SIP puedan proporcionar su dirección. Se contempla la existencia de un tiempo máximo de validez en un intervalo de 90 a 3600 segundos esto depende de la configuración que manualmente realice el administrador del sistema, por defecto el valor estándar es de 1800 segundos, dentro de este tiempo definido por el servidor se debe de renovar el registro [20].

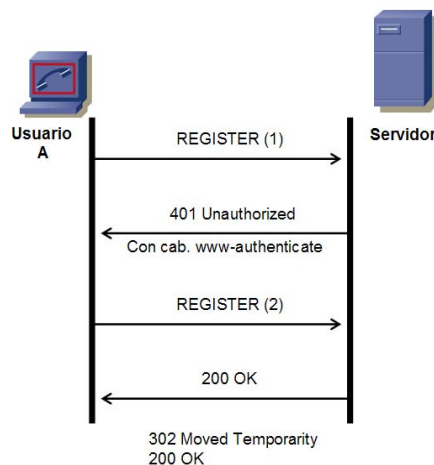


Figura 3. 4 Servidor de Registro.

Servidor Proxy

Los servidores Proxy reenvían peticiones desde el Agente de Usuario hacia el siguiente Servidor SIP y retienen la información por cuestiones de contabilidad o facturación. Adicionalmente puede operar en forma constante o dependiente de la conexión. El Servidor constante puede dirigir las llamadas entrantes hacia diversas extensiones que están activas a la vez y la primera en responder tomará la llamada. Esta capacidad significa que se puede buscar en los diferentes teléfonos SIP: de escritorio, móvil o en casa y todos “timbrarían” cuando llegue una llamada, de tal forma que al contestar en cualquiera de ellos se inicia la conversación y los otros dispositivos dejan de timbrar.

Los Servidores Proxy pueden usar varios métodos para intentar resolver la dirección de destino solicitada, incluyendo búsquedas en el Registro de Nombres de Dominio (*Domain Name System: DNS*), en bases de datos o relevando la labor hacia el siguiente Servidor Proxy.

Servidor de redirección

A diferencia de los Proxy no inician transacciones, cuando reciben solicitudes desde un agente de usuario-cliente, remiten al mismo agente un mensaje indicado los servidores con los que debe ponerse en contacto, en un procedimiento similar al de búsqueda iterativa del Registro de Nombres de Dominio. Asimismo, a diferencia de los agentes de usuarios servidores no aceptan llamadas.

Normalmente, los servidores de redirección gestionan mayor número de mensajes que los proxys puesto que en sesiones controladas por SIP la redirección se realiza mediante mensajes SIP, las respuestas se pueden generar con flexibilidad y adecuación a servicios de conferencia multimedia, codificándose en función de parámetros tales como la hora del día, origen o urgencia de la llamada, o cualquier otro criterio específico aplicado por el servidor SIP.

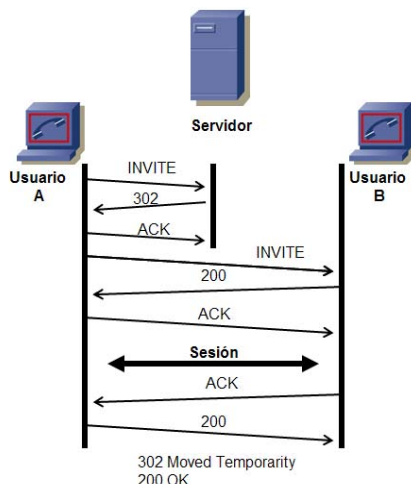


Figura 3. 5 Ejemplo de un Servidor de Re-direccionamiento.

3.3 Operación del Protocolo SIP

El protocolo SIP está basado en el protocolo HTTP y como tal SIP se basa en el método petición-respuesta, para entender este mecanismo se requiere de los conceptos cliente y servidor que colaboran en este procedimiento.

Un cliente es una entidad de SIP que genera peticiones y un servidor es una entidad de SIP que recibe peticiones y las responde. Es parecido a la búsqueda de páginas en Internet, un cliente teclea <http://www.citedi.mx> y la petición es enviando a un servidor Web; éste regresa una respuesta con la información solicitada: la pagina Web.

El protocolo SIP utiliza el mismo procedimiento, siguiendo la misma terminología cuando dos agentes de usuario intercambian mensajes de SIP, el agente de usuario que envía peticiones se considera el agente de usuario cliente y el agente de usuario que responde a esas peticiones, es el agente de usuario servidor. A esta petición junto con la respuesta que produce es conocida como una transacción SIP [21].

3.3.1 Mensaje de Peticiones

Las especificaciones SIP definen seis tipos de peticiones conteniendo un campo llamado método, denotando su propósito. Un mensaje de SIP ya sea peticiones o respuestas, contiene una carga útil que usualmente consiste en la descripción de la sesión (SDP).

3.3.2 Métodos

En el protocolo las peticiones SIP especifican una acción para ser tomadas por otro agente usuario o servidor. Los métodos invitación (*invite*), registro (*register*), fin (*bye*), reconocimiento (*acknowledgement: ack*), cancelar (*cancel*) y opciones (*options*) son los principales en SIP. Los métodos referir (*refer*), suscribirse (*subscribe*), notificar (*notify*), mensaje (*message*), actualización (*update*), información (*information: INFO*) y ruptura (*crack*) no son utilizados en este trabajo, su descripción esta en cada uno de los RFC correspondientes. A continuación se describe el significado de cada método.

Invitación (*invite*)

Este método describe las características del usuario que desea entablar una conversación con otro usuario. Por ejemplo cuando el usuario A llama al usuario B, se envía una invitación con una descripción de la sesión.

Registro (*register*)

El mensaje de petición de registro se utiliza para informar a un servidor de la localización actual de un usuario, conteniendo el tiempo que el registro permanecerá vigente. Un usuario puede registrarse en diferentes lugares al mismo tiempo, indicando al servidor que debe buscarlo en cualquiera de esas direcciones hasta ser contactado.

3. PROTOCOLO DE INICIO DE SESIÓN

Fin (*bye*)

La petición de fin es utilizada para abandonar la sesión, es decir en una conversación con dos usuario o más, con uno que abandone la sesión indica que ésta ha sido terminada. Por ejemplo, cuando el usuario A le envía un mensaje de fin al usuario B, su sesión es terminada, esto no sucede en conversaciones entre tres o más personas, cuando un usuario manda la petición de fin indica que únicamente ese participante abandona la sesión.

Reconocimiento (*acknowledgement: ack*)

La petición de reconocimiento se usa para confirmar la recepción de una respuesta final a una petición.

Cancelar (*cancel*)

La petición de cancelar como su nombre lo indica, se utiliza para cancelar transacciones pendientes. Si un servidor SIP recibe una invitación pero no ha enviado una respuesta final, podrá detener el proceso de invitación si recibe una petición de cancelar. Si aún recibéndola el servidor envía una respuesta final, entonces la transacción se llevará a cabo y la petición de cancelar no tendrá ningún efecto.

Opciones (*options*)

Las peticiones de opciones sirven para determinar las capacidades del servidor, incluyendo cuales sus métodos y protocolos de descripción de sesión soporta; regresando información especificando tipos de esquema de codificación de medios.

3.3.3 Mensaje de Respuesta

Sobre la recepción de una petición, un servidor emite una o varias respuestas, cada respuesta tiene un código que indica el estado de la transacción. Los códigos de estado son números enteros de tres dígitos, en un rango de 100 al 699, están agrupados en clases como se muestra en la tabla 3.1 siguiente:

Tabla 3. 1 Tipos de respuestas SIP.

RANGO	TIPO DE RESPUESTA
100-199	Informativa
200-299	Exitoso
300-399	Redirección
400-499	Error del cliente
500-599	Error del servidor
600-699	Falla Global

Una respuesta con un código de estado de 100 a 199 es considerada como provisional. Respuestas entre 200 y 699 son respuestas finales. Una transacción SIP entre un cliente y un servidor, está formada generalmente por: una petición del cliente, una o más respuestas provisionales y una respuesta final.

Junto con el código de estado, las respuestas de SIP llevan consigo información que permite a una persona entender este código de estado. Por ejemplo, el código 180 significa que el usuario invitado a una sesión ha sido alertado y que pertenece al rango de respuestas informativas. La frase a esta respuesta es timbrando (*ringing*) y simplemente es descriptiva.

3.3.4 Tipos de respuestas

Informativa

Los tipos de respuesta información se utilizan para indicar el proceso de la llamada y contienen el cuerpo del mensaje. La excepción para esto es la respuesta ‘100 Trying’ que es solo una respuesta temporal.

3. PROTOCOLO DE INICIO DE SESIÓN

Las respuestas informativas son opcionales, un UAS puede enviar una respuesta final sin necesidad de enviar una respuesta informativa, mientras las respuestas finales a una invitación reciben un mensaje de reconocimiento para confirmar de recibido.

Éxito

Las respuestas de clase de éxito indican que la petición ha tenido éxito o ha sido aceptada.

Redirección

Las respuestas son generalmente enviadas por un servidor de Redirección en respuesta a una invitación, un agente usuario servidor, puede también enviar una respuesta de tipo redirección para implementar tipos de características de envío de llamada.

Error del cliente

Esta clase de respuesta es usada por el servidor o el agente usuario servidor para indicar que la petición no puede ser cumplida como fue presentada. La respuesta de error del cliente debe indicar al agente usuario cliente la naturaleza del error y la manera en que la petición puede ser reformulada, típicamente las respuestas de error de cliente requerirán la intervención del usuario antes de que una nueva petición pueda ser generada.

Error del servidor

Este tipo de respuesta indica que la petición no puede ser procesada debido a un error con el servidor, pero se puede intentarse de nuevo en otro tiempo. Para más información acerca de los tipos de campos que integran los formatos de petición- respuesta, consultar el Apéndice A.

La tabla 3.2 muestra los campos que están contenidos en los formatos, tanto en mensajes de petición como en mensajes de respuesta.

3. PROTOCOLO DE INICIO DE SESIÓN

Tabla 3. 2 Campos de formato de mensajes de peticiones y respuesta.

CAMPOS		
Accept	Join	Reject-Contact
Accept-Contact	Max-Forward	Replaces
Accept-Encoding	Mime Versión	Reply-To
Accept-Language	Min-Expires	Request-Disposition
Alert-Info	Min-SE	Requiere
Allow	Organization	Retry-After
Allow-Events	P-Access-Network-Info	Route
Authentication-Info	P-Asserted-Identity	Rseq
Authorization	P-Called-Party-ID	Server
Call-Id	P-Charging-Function-Addresses	Service-Route
Contact	P-Charging-Vector	Session-Expires
Contact-Disposition	P-Preferred-Identity	SIP-Etag
Contact-Encoding	Priority	SIP-If-Match
Content-Length	Privacy	Subject
Content-Type	Proxy-Authenticate	Subscription-State
Cseq	Proxy-Authentication-Info	Supported
Date	Proxy-Authorization	Timestamp
Diversion	Proxy-Require	To
Error-Info	Rack	Unsupported
Event	Reason	User-Agent
Expires	Record-Route	Vía
From	Referred-By	Warning
In-Reply-To	Refer-To	WWW-Authenticate

3.4 Formato de los mensajes SIP

Una vez que se ha seleccionado qué información deberá ser intercambiada en una sesión SIP, el siguiente paso es decidir cómo debe ser codificada ésta información. Esta decisión tiene básicamente dos aproximaciones: binaria o basada en texto.

El protocolo SIP utiliza la codificación basada en texto, lo que ha creado una fuerte controversia ya que los partidarios de esta idea proponen que su utilización es más sencilla porque puede ser leída fácilmente, además de que los protocolos basados en texto son más flexibles y escalables.

3. PROTOCOLO DE INICIO DE SESIÓN

Dicha codificación tiene como desventaja el tamaño de la información y en la codificación binaria esto es una ventaja.

3.4.1 Petición

En una petición de SIP se describe lo siguiente: línea de petición, varias líneas de encabezado, una línea vacía y un cuerpo de mensaje; el cuerpo de mensaje es opcional, algunas peticiones no lo contienen, puesto que no son necesarias para la transmisión.

Línea de petición: esta línea contiene tres elementos: método, dirección URI y la versión del protocolo.

- El método indica el tipo de petición.
- La dirección URI indica el destino de llegada a dónde la petición tiene que ser enrutada.
- La versión SIP en la actualidad es 2.0.

En la figura 3.6 el SIP Proxy en dominio.com recibe una invitación con la dirección URI SIP:usuario.a@dominio.com, ese Proxy sabe que el usuario B puede ser localizada en dos direcciones por lo que genera dos invitaciones; una contiene como dirección URI SIP:usuario.b@citedi.mx y es enviada al servidor citedi.mx, la segunda invitación tendrá SIP:usuario.a@131.160.1.112.

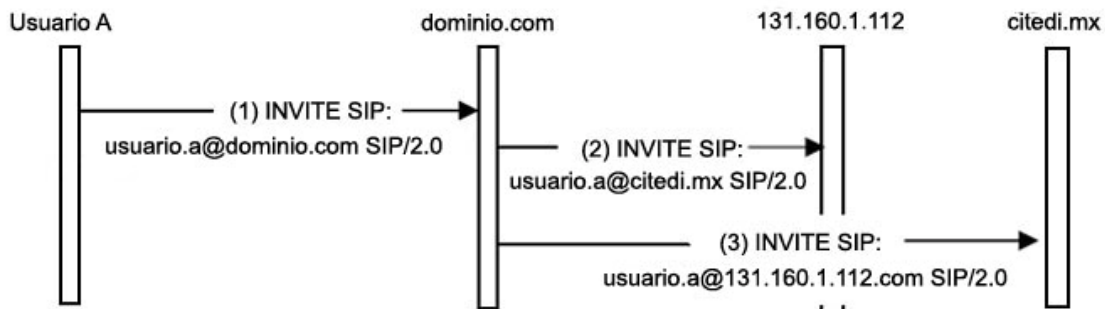


Figura 3. 6 El Request-URI contiene el siguiente salto del camino.

3.4.2 Respuestas

Una respuesta de SIP consiste en: línea de estado, varias líneas de encabezado, línea vacía y un cuerpo de mensaje. Al igual que la petición SIP, el cuerpo del mensaje es opcional.

Línea de estado: Esta línea contiene tres elementos: la versión del protocolo, el código de estado y la frase de estado. La versión actual del protocolo se escribe SIP/2.0, el código de estado reporta el estado de la transacción y la frase de estado la descripción del código.

3.4.3 Cuerpo del mensaje SIP

Tanto peticiones como respuestas pueden contener cuerpos de mensaje separados de los encabezados por una línea, el cuerpo del mensaje que llevan los paquetes de SIP es usualmente una descripción de sesión. Los SIP proxys no necesitan examinar el cuerpo del mensaje que reciben, esta información es transparente para ellos por lo que las descripciones de sesión son transmitidas entre usuarios finales (agente usuario).

Así como un e-mail puede llevar varios archivos adjuntos, los mensajes de SIP pueden llevar varios cuerpos de mensaje. Por ejemplo, el usuario A puede enviar una invitación con dos cuerpos: una descripción de sesión y su foto, de esta forma el agente usuario B puede mostrar la fotos en la pantalla mientras que está siendo alertado [17], [18], [22]; el formato general de los mensajes SIP se muestra en la figura 3.7.



Figura 3. 7 Formato de Petición y Respuesta de SIP.

3. PROTOCOLO DE INICIO DE SESIÓN

En este capítulo se concentra la información más importante del Protocolo SIP, indicando su definición, arquitectura, comportamiento, la función dentro de la comunicación entre dos usuarios y el formato de los mensajes petición-respuesta; esta investigación fortalece el conocimiento para el capítulo “Análisis de los Protocolos empleados en VoIP” ya que SIP tiene una relación directa y algunas de las funciones y campos que utiliza están relacionados con los protocolos de comunicación VoIP que se verán a continuación.

CAPÍTULO 4

ANÁLISIS DE LOS PROTOCOLOS EMPLEADOS EN VOIP

Como se presento en el Capítulo 3 “Protocolo de Inicio de Sesión”, SIP necesita de otros protocolos para concretar una llamada de voz. En necesario entonces, conocer el comportamiento de cada uno de los protocolos que intervienen en el proceso de establecimiento de una llamada de Voz sobre IP. En este capítulo se analizara la función y el encabezado de los protocolos: SDP, RTP, UDP, IP Ethernet; además se presenta, el procedimiento para que un usuario pueda contactarse con otro mediante la tecnología de Voz sobre IP.

4.1 PROTOCOLO DE DESCRIPCION DE SESIÓN (SDP)

El Protocolo SDP, definido por el RFC 2327 [23] y RFC 4566 [24] fue desarrollado por el grupo de trabajo IETF. Se considera más como una descripción de sintaxis que un protocolo ya que no provee una capacidad de negociación, el propósito original de SDP fue detallar las sesiones multidifusion bajo Internet.

4.1.1. Función de SDP

Tiene como principales funciones el informar la existencia del inicio de una sesión, brindando características de los medios de transmisión, permitiendo la unión y participación de los usuarios mediante el modelo de Petición-Respuesta.

4.1.2 Formato SDP

La figura 4.1 describe los campos del formato SDP, el “Tipo” se refiere a una letra que simboliza una característica de la sesión, el “Valor” puede ser numérico o descriptivo.

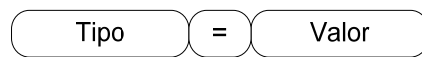


Figura 4. 1 Formato de SDP.

Contenido de la información en una sesión:

- Dirección IP (IPv4 o nombre del servidor).
- Número de puerto (UDP).
- Tipo de medio (audio, video).
- Esquema de codificación.

Entre la información que contiene el cuerpo de mensaje de SDP se muestra la siguiente:

- Asunto de la sesión.
- Tiempos de inicio y término de la sesión.
- Información del contacto acerca de la sesión.

El protocolo SDP básicamente conecta al usuario fuente con el usuario origen, brindando información básica de ambos [22]. La tabla 4.1 contiene los campos del formato junto con su nombre y descripción. Esta información va incluida en los mensajes del Protocolo SIP con los datos del usuario que desea iniciar una conversación telefónica de voz sobre IP. Uno de los campos importantes para la negociación de esquemas de compresión es ‘a’, éste se refiere al tipo de medio ya sea voz o video con el que se establece la sesión.

4. ANALISIS

En la tabla 4.2 se muestra la extensión de los tipos de parámetros para este campo y la descripción de cada uno. Para ejemplificar se tiene lo siguiente

a = rtpmap: 0 PCMU/8000

donde 'rtpmap' representa la lista de audio y video del protocolo RTP, '0' significa el identificador del tipo de carga, PCMU/8000 es el codec a utilizar; lo anterior esta referenciado en la tabla 4.4.

Tabla 4. 1 Lista de campos SDP según el orden requerido.

CAMPO	NOMBRE	DESCRIPCION
V	Número de versión del protocolo	Versión actual: 0
O	Creador e identificador de sesión	Nombre de usuario, identificador de sesión, versión, tipo de red y tipo de dirección
S	Nombre de sesión	Cualquier número de caracteres diferentes de cero
I	Información de sesión	Cualquier número de caracteres
U	Identificación de fuente uniforme	Dirección URI
E	Dirección de correo	Caracteres variables
P	Número de teléfono	Caracteres numéricos
C	Información de conexión	Tipo de red, tipo de dirección y conexión de dirección
B	Información de Ancho de Banda	Información del ancho de banda usado
T	Tiempo de inicio y fin de sesión	Tiempo de inicio: determinado, tiempo final: indefinido
A	Medios	Extensión del Protocolo SDP (Tabla 2.2)
M	Medios de información	Medio, puerto, transporte y formato de lista

4. ANALISIS

La tabla 4.2 describe lo que representa cada valor del campo 'a'.

Tabla 4. 2 Valor de los atributos de SDP.

ATRIBUTO	DESCRIPCION
a = rtpmap	Lista RTP/AVP
a = cat	Categoría de la sesión
a = keywds	Palabra clave de sesión
a = tool	Nombre de la herramienta usada para crear SDP
a = ptime	Longitud del tiempo en milisegundos para cada paquete
a = sendonly	Modo de solo enviar
a = reconly	Modo de solo recibir
a = orient	Orientación para sesión de pizarra virtual
a = type	Tipo de conferencia
a = rtcp	Puerto RTCP explícito
a = quality	Sugerencia de calidad de codecs

Otro protocolo que es fundamental para abrir el flujo de información es el Protocolo de Transporte en Tiempo Real (*Real-Time Transport Protocol: RTP*), ya que sin este protocolo no se lleva a cabo la negociación de oferta de medios que los usuarios proponen para establecer una conversación, así mismo, el Protocolo de Control de Transporte en Tiempo Real (*Real-Time Transport Control Protocol: RTCP*) colabora con el servicio de calidad, pues la tecnología de Voz sobre IP lleva a cabo su transporte de paquetes principalmente, mediante el Protocolo de Datagrama de Usuario (*User Datagram Protocol: UDP*). El servicio de voz requiere ser enviada en tiempo real y UDP no brinda fiabilidad. Lo anterior quizás parezca una desventaja. Pero, las retransmisiones de un paquete sin confirmación producen un retardo que es inadecuado en el servicio de voz.

4.2 PROTOCOLO DE TRANSMISION EN TIEMPO REAL

El Protocolo de Transporte en Tiempo Real fue desarrollado para permitir el transporte de paquetes: de voz y video, en tiempo real sobre IP. Descrito en el RFC 1889 [22], [25], [26]. Sin asegurar algún tipo de calidad de servicio. A continuación se presenta la función, algunas características y el encabezado de RTP.

4. ANALISIS

4.2.1 Función de RTP

Permite el transporte en tiempo real de paquetes que contengan voz, video u otra información sobre IP. No provee una calidad de servicio bajo la red IP.

Detecta lo siguiente:

- Pérdida de paquetes: mediante el campo número de secuencia verifica que todos los paquetes tenga un número secuencial entre sí.
- Variación de retraso: el campo marca de tiempo indica la llegada entre un paquete y otro.
- Ruteo asimétrico: se identifica la ruta de cada paquete, aunque en ocasiones la ruta sea diferente.

Provee funciones de extremo a extremo en aplicaciones comunes, como audio y video.

- Comunicar la elección del esquema de codificación de los datos.
- Determinar la relación temporal entre los datos recibidos.
- Sincronizar los distintos medios.
- Indicar la pérdida de paquetes.
- Indicar límites de tramas de los datos.
- Identificación amigable de usuarios.

4.2.2 Encabezado RTP

En la figura 4.2 se presentan los campos con los que cuenta RTP y su función de acuerdo al tipo de transmisión que se realice. El encabezado tiene una longitud de 96 bits o 12 bytes.

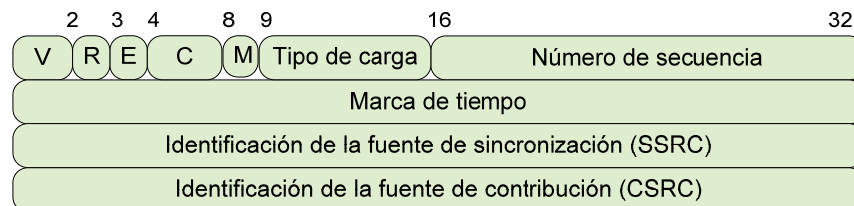


Figura 4. 2 Encabezado de RTP.

4. ANALISIS

El primer campo **V** se trata de la versión de RTP (2 bits), **R** relleno (*padding*) (1 bit) este campo indica que el paquete contiene uno o más bytes de relleno que no son parte de la carga útil, el campo **E** significa extensión, cuando este bit está en 1 se indica que está seguido de una extensión de encabezado (1 bit), **C** representa el conteo y especifica el número de CSRC que siguen al encabezado (4 bits), **M** indica marca de inicio de una trama de audio o video (1 bit), **Tipo de carga** define el codec en uso, el valor de este campo corresponde al listado en SDP (7 bits), **Número de secuencia** es incrementado para cada paquete RTP enviado y usado para detectar pérdidas fuera de secuencia (16 bits), **Marca de tiempo** refleja el instante de muestro del primer byte del paquete RTP (carga útil), basado en un reloj que se incrementa periódicamente y se utiliza para sincronización y cálculo la variación del retraso (32 bits), el campo **SSRC** indica el número que identifica la fuente (32 bits) y por ultimo **CSRC** contiene de 0 a 15 tipos de (32 bits) cada uno de los cuales especifica la fuente que ha contribuido a la carga útil del paquete.

El protocolo RTCP definido en el RFC 3605 [22], [26] es un protocolo que permite a los participantes el envío de reportes y estadísticas de calidad e intercambia información de identidad básica, el uso de reportes permite la retroalimentación sobre la calidad de conexión incluyendo la siguiente información:

- Número de paquetes enviados y recibidos.
- Número de paquetes perdidos.
- Paquetes de variación de retraso.

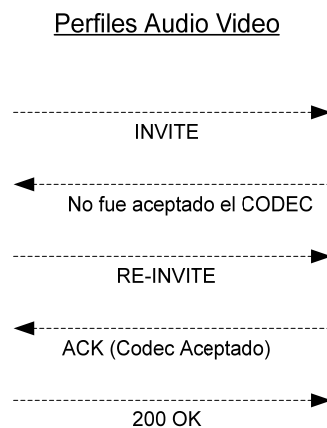


Figura 4. 3 Ejemplo de la negociación de un codec empleando el protocolo SIP.

4. ANALISIS

En la tabla 4.3 se muestra el tipo y nombre del paquete que el Protocolo RTCP utiliza en el envía y comunicación con RTP. Estos mensajes describen, características de conexión entre usuarios en una conversación, los cuales funcionan para crear estadísticas de calidad de servicio.

Tabla 4. 3 Tipos de paquetes RTCP.

TIPO DE PAQUETES	NOMBRE DEL PAQUETE	DESCRIPCION
SR	Reporte emisor	Un participante envía y recibe paquetes
RR	Reporte receptor	Envío de un participante que solo recibe paquetes RTP
SDES	Descripción de origen	Contiene información acerca del participante: correo electrónico, número de teléfono y host
BYE	Fin (<i>Bye</i>)	Finalización de la sesión
APP	Especificación de aplicación	Definido por perfil en particular
XR	Reposte extendido	Reporte extendido y resumen

En la tabla 4.4, se presentan una serie de parámetros sobre los tipos de codec más utilizados. El tipo de carga es un valor que SIP y SDP utilizan dentro de sus mensajes de petición dando a conocer el tipo de codec que tiene un usuario.

Tabla 4. 4 Tipo de carga útil de audio y video RTP/AVP.

TIPO DE CARGA	CODEC	RELOJ	DESCRIPCION
0	PCMU	8000	ITU G.711 PCM, audio 64 Kbps
1	1016	8000	CELP, audio 4.5 Kbps
2	G721	8000	ITU G.721 ADPCM, audio 32 Kbps
3	GSM	8000	Estándar Europeo GSM, audio 13 Kbps
5	DV14	8000	DVI ADPCM, audio 32 Kbps
6	DV14	16000	DVI ADPCM, audio 64 Kbps
7	LPC	8000	Audio experimental LPC
8	PCMA	8000	ITU G.711 OCM Law-a, audio 64 Kbps
9	G.722	8000	Audio ITU G.722
10	L16	44100	Lineal de 16 bits, audio 704.6 Kbps

4. ANALISIS

El siguiente protocolo está en la capa de transporte y es el encargado de enviar su encabezado y los datos hacia la capa enlace.

4.3 PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

Hace disponible un tipo de datagrama para la transmisión, permite el envío a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su encabezado, esto se encuentra definido en RFC 768 [27].

4.3.1 Función de UDP

Provee servicio sin conexión, envía los paquetes sin detección de errores y sin acuse de recibo. Se utiliza en aplicaciones sencillas que no requieran una alta confiabilidad o en los entornos locales de alta confiabilidad con el fin de reducir los retardos.

4.3.2 Encabezado UDP

El encabezado de este protocolo es mostrado en la figura 4.4. El puerto origen y el puerto destino tienen un longitud de 16 bits y contiene el puerto de la computadora ya sea origen o destino respectivamente. La longitud de 16 bits corresponde a la longitud total del datagrama de usuario, con el encabezado y los datos. Esta longitud no puede pasar 65,536 bytes debido a que IP encapsula el paquete de un tamaño fijo. La suma de control de 16 bits realiza una verificación de error del paquete [10].

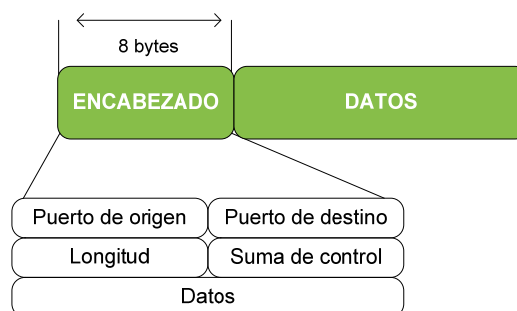


Figura 4. 4 Encabezado de UDP.

4. ANALISIS

La capa de Internet es la encargada del envío de datagramas a la capa inferior, como se vio en el Capítulo 2 en la sección 2.1.1, IP provee servicios para la transmisión de datos, voz y video. Por lo tanto las aplicaciones son innumerables, en el caso de VoIP lo que se transmiten son conversaciones sobre Internet. En la siguiente sección se explica más a detalle.

4.4 PROTOCOLO DE INTERNET (IP)

El Protocolo de Internet, que es utilizado en múltiples aplicaciones, está definido en el RFC 791 [7], proporciona los medios necesarios para el transporte de datagramas desde el origen hasta su destino. También se encarga si es necesario de la fragmentación y reensamble de grandes datagramas que no pueden ser recibidos en pequeñas redes.

4.4.1 Función de IP

Proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas, puede haber envío sin que exista una previa conexión y ofrece un servicio de mejor esfuerzo (*best effort*) que significa que hará el mejor servicio posible a su alcance en el momento de enviar los paquetes, pero en realidad garantizando poco ya que carece de un mecanismo para determinar si un paquete alcanza o no su destino.

Operación:

- Direcccionamiento.
- Fragmentación.

Mecanismo:

- Tipo de servicio: QoS deseado.
- Tiempo de vida: período de vida de un datagrama.
- Opciones: funciones de control.
- Suma de control de encabezado (verificación de que la información ha sido transmitida correctamente).

4. ANALISIS

No proporciona:

- Mecanismo de comunicación fiable.
- Acuses de recibo (ni en extremos ni en saltos).
- Control de errores para los datos.
- Retransmisiones.
- Control de Flujo.

4.4.2 Encabezado IP

IP contiene campos que colaboran de distinta forma para lograr que la información llegue del origen al destino, la longitud del encabezado es de 32 bits pero el tamaño de éste depende de la red por la cual se desea transmitir.

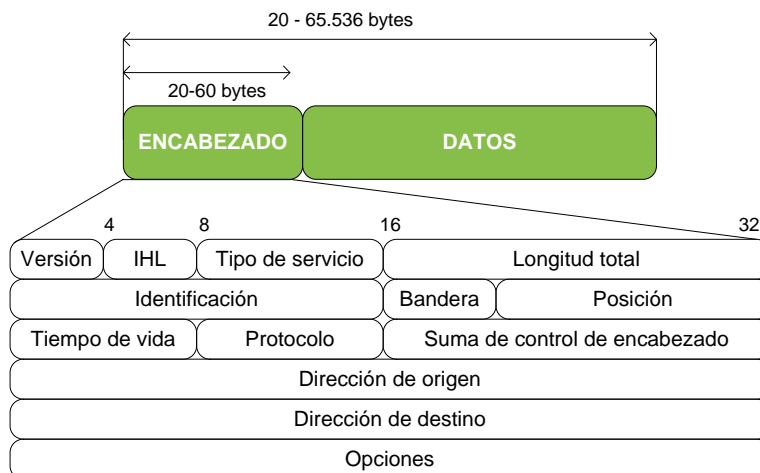


Figura 4. 5 Encabezado del Protocolo de Internet.

El encabezado de la figura 4.5 muestra algunos de los campos más importantes del Protocolo de Internet, el Tipo de Servicio (8 bits) se utiliza para indicar la calidad del servicio deseado. Es un conjunto de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. La tabla 4.5 muestra los bits que representan el tipo de servicio que se coloca en el encabezado de IP.

Tabla 4. 5 Tipos de servicios.

BIT 0-2	PRIORIDAD	
Bit 3	Demora normal.	0
	Baja demora.	1
Bit 4	Rendimiento normal.	0
	Alto rendimiento.	1
Bit 5	Fiabilidad normal.	0
	Alta fiabilidad.	1
Bit 6-7	Reservado para uso futuro.	0

La Suma de control de encabezado (16 bits) proporciona una verificación de que la información utilizada al procesar el datagrama Internet, ha sido transmitida correctamente. Si la suma de control de encabezado falla, el datagrama Internet es descartado inmediatamente por la entidad que detecta el error.

El protocolo de Internet no proporciona ningún mecanismo de comunicación fiable. No hay retransmisiones, control de flujo, control de errores para los datos, sólo una suma de control de encabezado, mucho menos existen acuses de recibo, ni entre extremos ni entre saltos. Los errores detectados pueden ser notificados por medio del Protocolo de Mensajes de Control de Internet (*Internet Control Message Protocol: ICMP*), el cual está implementado en el módulo del protocolo de Internet esto se explicará brevemente más adelante [8].

Los paquetes que se originan deben de ser encapsulados en datagramas para pasar del nivel de red al nivel más bajo, los datagramas son encaminados desde un enrutador a través de redes basándose en la interpretación de una dirección de Internet. El enrutamiento de mensajes en ocasiones requiere de cruzar por redes donde el tamaño máximo de paquete es mayor que el datagrama, para solucionar este inconveniente IP proporciona un mecanismo de fragmentación; la fragmentación se origina cuando el tamaño de un datagrama es mayor que el permitido en una red y que cuando requiere salir de la red local hacia otra red exterior es necesario que atraviese por varios enrutadores que en ocasiones están limitados en el tamaño de recepción, entonces es necesario dividir el datagrama cuantas veces sea necesario para poder llegar al destino.

4. ANALISIS

En el encabezado de IP se utilizan varios campos como Bandera (3 bits), donde se indica si es posible fragmentar o no un datagrama, si existen más fragmentos o si es el último. Los parámetros de Bandera son mostrados en la Tabla 4.6.

Tabla 4. 6 Parámetros del campo Bandera del encabezado de IP.

	DESCRIPCION	
Bit 0	Reservado	
Bit 1	DF: No fragmentar (<i>Don't fragment</i>)	1
	Puede fragmentarse	0
Bit 2	MF: Mas fragmentos (<i>More fragment</i>)	1
	Ultimo Fragmento	0

El tamaño usual de un datagrama es de 576 bytes que incluye el encabezado y los datos del datagrama, donde el encabezado tiene un margen de 20 a 64 bytes y el resto es para los datos, si el encabezado (figura 4.5) no tiene opciones se utilizan solo 20 bytes. Las redes están capacitadas para procesar un máximo tamaño de 65,536 bytes, (dependiendo de la red).

El campo **Identificador** (16 bits) se encarga de distinguir entre los fragmentos de un datagrama y otro, asignado por el emisor para facilitar el acomodo de los datagramas cuando lleguen al receptor. El campo de **Posición** (13 bits) es el encargado de indicar a qué parte del datagrama pertenece el fragmento, el receptor se guiará con los campos: identificador, origen, destino y protocolo; estos campos contienen los mismos datos en cada fragmento, así que todos los que sean similares van a pertenecer a un datagrama. Para reordenar los fragmentos sin errores, en el encabezado de IP se tiene un campo de posición.

Otro campo importante es **Suma de comprobación** (16 bits), existen varios algoritmos para realizar la suma, por ejemplo el complemento a 1 de 16 donde se suma los complementos del encabezado y si es correcta se envían 0's y si alguna parte del datagrama tiene errores entonces aparecerán 1's, esta verificación se realiza sólo para el encabezado. Por su parte los datos son verificados en los niveles superiores, si la suma de control fuese hecha para ambos, encabezado y datos, el procesamiento seria incrementado teniendo como consecuencia más tiempo de ejecución.

4. ANALISIS

El campo de **Opciones** (tamaño variable) proporciona funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las redes más comunes. Las Opciones incluyen recursos para marcas de tiempo, seguridad y enrutamiento especial, se clasifica en; no operación, fin de operación, registrar ruta, campo estricto y no estricto y marca de tiempo. Este campo puede ocupar un máximo de 40 bytes aproximadamente y es opcional; si alguna red local utiliza las opciones mencionadas, las demás redes por donde tenga que cruzar están obligadas a procesarlas.

Después del proceso de fragmentación donde varios campos colaboran para ese proceso, existe otro proceso que realiza IP: el direccionamiento. El cual requiere varios parámetros para identificar el origen y el destino de las direcciones, dentro de la dirección se debe conocer si es unicast (envío de un usuario a un receptor), multicast (envío de un usuario a varios receptores de un mismo grupo) o broadcast (envío de un usuario a todos los receptores posibles), en cada caso la dirección es específica y esto hace que el envío a su destino sea más fácil ya que el primer bit es el que alerta el tipo de dirección.

Existen varios protocolos que colaboran para la transmisión, para esto los parámetros importantes son la dirección lógica (dirección IP) y la dirección física o MAC (*Media Access Control Address*); es necesario que exista una asociación entre ellas, ya que de no ser así, no es posible que el datagrama llegue a su destino [10]. Existen dos tipos de asociación: estática y dinámica, ambas crean tablas de direcciones de asociación. Estas tablas de enrutamiento se guardan en cada nodo de una red y enrutador, si un nodo desea llegar hasta otro conociendo solo su dirección lógica, entonces busca en la tabla la dirección que coincida con la que conoce y con eso obtiene la dirección física; lo anterior tiene varias desventajas debido a que la tarjeta de red puede cambiar o el usuario puede moverse de lugar. En cambio la asociación dinámica, cada vez que conoce una dirección cualquiera que sea, lógica o física, utiliza un protocolo para conocer la restante.

El datagrama contiene la dirección lógica del receptor, ésta es obtenida de la tabla de enrutamiento, pasa al siguiente nivel físico y para esto se encapsula en una trama, pero es necesario conocer su dirección física; así que envía un paquete de consulta del Protocolo de

4. ANALISIS

Resolución de Dirección (*Address Resolution Protocol: ARP*) a todos los nodos de la red, que contiene su dirección lógica, dirección física y la dirección lógica del receptor. El nodo que coincida envía de vuelta el paquete de consulta ARP por medio de la dirección lógica del emisor con la dirección física de él. El paquete de consulta es mostrado en la figura 4.6 donde se coloca la información que se tiene y se deja vacío el campo dirección hardware del receptor. Los otros campos son llenados de acuerdo al protocolo IP.

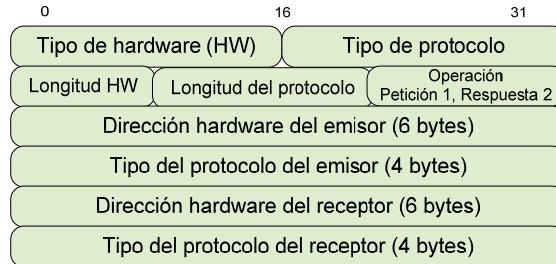


Figura 4. 6 Encabezado del Protocolo ARP.

El paquete ARP es encapsulado en una trama Ethernet, como se muestra en la figura 4.7 para ser enviado a buscar el destino, ya que sólo se tiene la dirección lógica. El datagrama ahora que tiene la dirección física es encapsulado en Ethernet y transmitido a su destino, el significado de cada campo de Ethernet se mostrará más adelante.

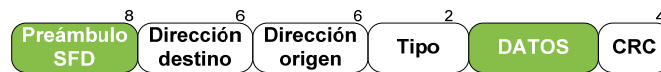


Figura 4. 7 Encapsulamiento de un paquete de petición o consulta ARP.

Si existe algún error en cuanto a los datagramas, IP se sirve del Protocolo ICMP que envía mensajes de tipo informe de error y de consulta, tiene como objetivo el informar sobre problemas con enrutadores o consultar quienes están cerca de él, la figura 4.8 muestra los campos que contiene el encabezado del protocolo ICMP [10].

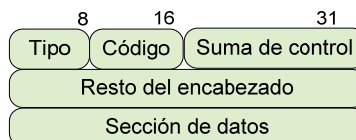


Figura 4. 8 Encabezado ICMP.

4. ANALISIS

Los mensajes del protocolo ICMP van en el campo tipo, la razón de un mensaje en particular va en el campo código, la verificación del encabezado se realiza en el campo suma de control, el campo resto del encabezado se especifica para cada mensaje en particular y el campo de sección de datos depende si es un mensaje de error o consulta, los tipos de mensajes se muestran en la Tabla 4.7

Tabla 4. 7 Mensajes de error y de consulta del protocolo ICMP.

DESCRIPCION DE ERROR	TIPO
Destino inalcanzable.	3
Frenar origen.	4
Tiempo excedido.	11
Problemas con parámetros.	12
Redirección.	5
DESCRIPCION DE CONSULTA	TIPO
Petición de eco y de respuesta.	8 y 0
Petición de marca de tiempo y respuesta.	13 y 14
Petición de redirección de máscara y respuesta.	17 y 18
Petición de enrutador y anuncio.	10 y 9

A nivel de enlace cada protocolo tiene su propio formato de trama, uno de los campos es el tamaño máximo de los datos. Cuando el datagrama se encapsula en una trama, el tamaño total del datagrama debe ser menor al tamaño máximo, que está definido por restricciones del hardware y software utilizado en la red, a este parámetro se le llama Unidad Máxima de Transferencia (MTU). En la tabla 4.8 se presenta el tamaño de algunas redes.

Tabla 4. 8 MTU para distintas redes.

PROTOCOLO	MTU
Hypercanal	65,536 bytes
Token ring (16 Mbps)	17,914 bytes
Token ring (4 Mbps)	4464 bytes
FDDI	4352 bytes
/Ethernet	1500 bytes
X.25	576 bytes
PPP	296 bytes

4.5 ETHERNET

Fue creado en 1976, por Xerox's en el Centro de Investigación de Palo Alto (*Palo Alto Research Center: PARC*). Ethernet está clasificado de acuerdo a la velocidad que puede transmitir: Ethernet Estándar (10 Mbps), Fast Ethernet (100 Mbps), Ethernet Gigabit (1 Gbps), Ethernet 10 Gigabit (10 Gbps) y Ethernet Experimental (100 Gbps).

En el caso del Ethernet Estándar, es dividido en dos subniveles. El subnivel Control de Acceso Medio (*Media Access Control: MAC*) que controla la operación de los métodos de acceso, realiza tramas con la información recibida de la capa superior y la pasa a la capa físico. El subnivel de Control de Enlace Lógico (*Logical Link Control: LLC*) define un encabezado de unidad de datos de protocolo (*Protocol Data Unit: PDU*), los campos son utilizados para control de flujo y error y definen el protocolo de la capa superior [10]

4.5.1 Función de Ethernet

- Las transmisiones son difundidas por un canal compartido y quien sea destinatario de la información, responderá al mensaje.
- Tiene la facilidad de ampliar la red (LAN) debido a su tipo conexión.

4. ANALISIS

- Ha evolucionado a tal nivel que sus implementaciones son interoperables, lo que hace fácil la migración a otro tipo de cable o de velocidad.

4.5.2 Encabezado Ethernet

La figura 4.9 muestra los campos del encabezado de Ethernet entre los cuales destacan: el campo **Preámbulo** (7 bytes) permite al receptor saber cuándo una trama está llegando, el **Delimitador de Comienzo de Trama** (*Start of frame delimiter: SFD*) (1byte) como su nombre lo indica da aviso del inicio de una trama y sobre la sincronización.

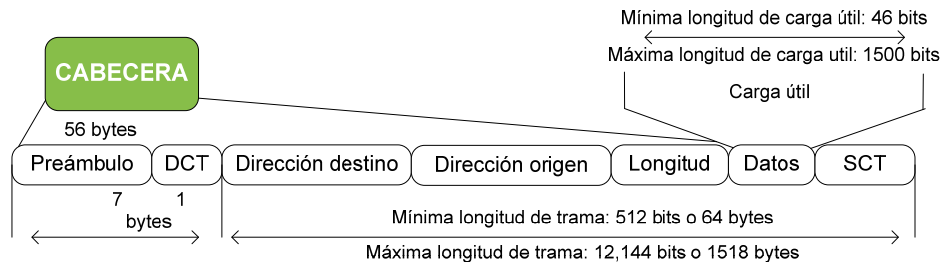


Figura 4. 9 Encabezado de Ethernet.

Los últimos dos bits se refieren a que la dirección destino es el siguiente campo, la dirección destino y origen (6 bytes) contiene la dirección de quien lo recibe y quien manda el mensaje, respectivamente, el campo longitud (2 bytes) está presente para dar a conocer el número de bytes en el campo de datos, el campo datos (46 - 1500 bytes) contiene los datos encapsulados del nivel superior, el campo de **Secuencia de comprobación de trama** (*Frame check sequence: FCS*) contiene la información detección de errores [10].

4.6 COMPORTAMIENTO DE SIP

SIP está relacionado con los protocolos mencionados anteriormente, cada uno de los cuales transporta la carga hacia el siguiente nivel como se muestra en la figura 4.10.

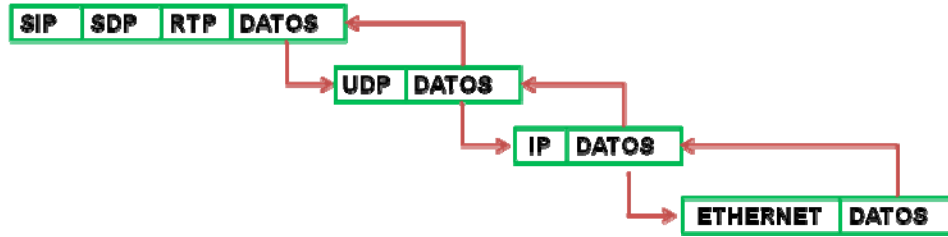


Figura 4. 10 Protocolos que interviene con SIP.

4.6.1 Elementos básicos en el empleo del Protocolo SIP

El protocolo SIP, como se mencionó en el capítulo 3, contiene dos elementos: usuarios y servidores; no obstante para poder enlazar a un usuario con el otro, primero cada usuario debe de estar registrado, para eso se cuenta con un administrador, éste se encarga de enviar los datos necesarios para crear el registro en el servidor y guardar la información en una base de datos; cada elemento tiene su función básica, las cuales se presentan en el diagrama de caso de uso, en la figura 4.11.

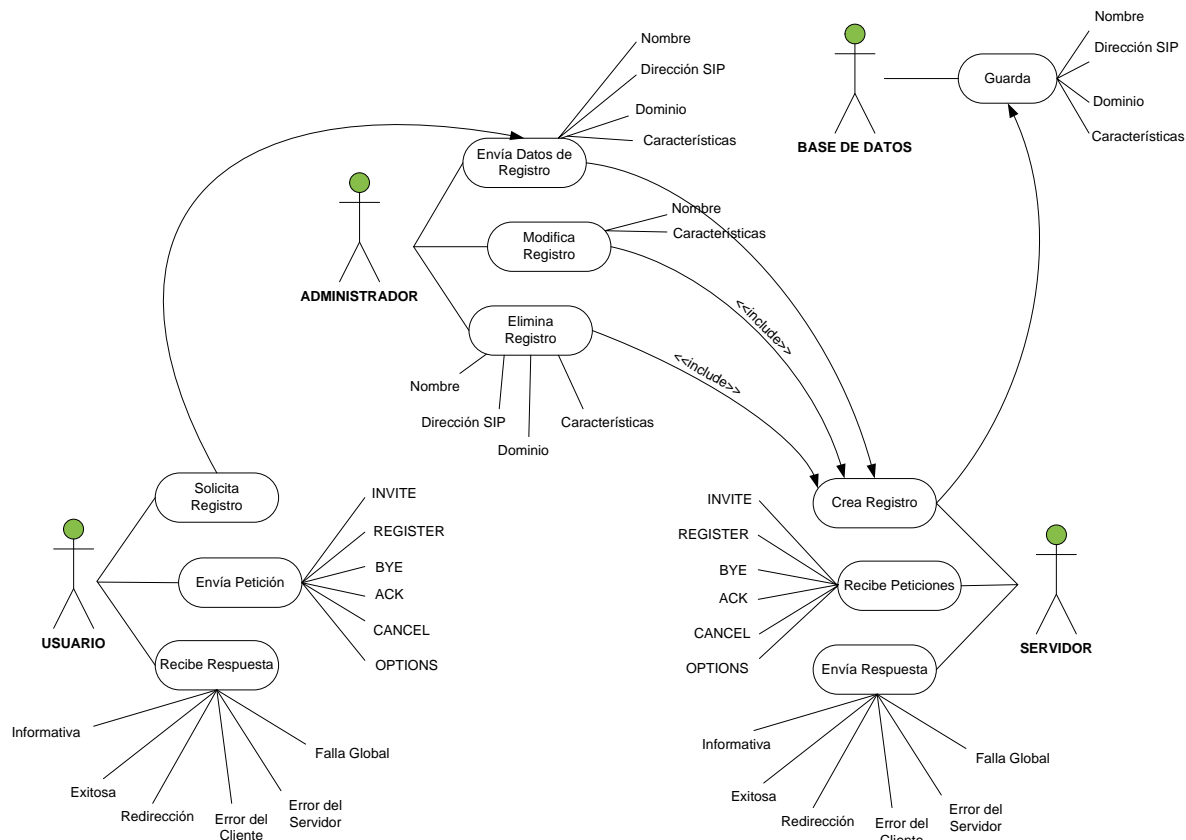


Figura 4. 11 Diagrama de casos de los elementos principales para SIP.

4.6.2 Establecimiento de una llamada de Voz sobre IP

Para una comunicación simple de un transmisor a un receptor utilizando el protocolo SIP, es necesaria la apertura de un medio o canal por el cual se transmitan los mensajes. La figura 4.12 muestra el inicio con una petición de Invitación (*Invite*) que envía el transmisor al Servidor Proxy, este servidor busca al usuario hasta encontrarlo, haciendo uso de bases de datos y servidores de localización.

De no ser encontrado se envía un mensaje al transmisor. Si se encontró se le envía la petición de invitación, en caso de que el servidor haya arrojado varias ubicaciones de usuarios, el mensaje se envía a todos, de tal manera que el primero que conteste continua con el establecimiento de sesión. Los otros usuarios reciben un mensaje de cancelación, el usuario receptor envía un mensaje que la llamada está entrando, si contesta entonces comienza la negociación de codec y si ambos usuarios están de acuerdo finaliza la transacción de invitación (*Invite*) e inicia el flujo de paquetes RTP.

El servidor estará monitoreando la sesión en todo momento, guardando las rutas y parámetros necesarios para mantener la sesión. Si alguno de los dos usuarios desea modificar el tipo de medio, es enviado entonces una re-invitación (*Re-Invite*). Este método tiene como función mantener la sesión mientras se realiza la negociación. La llamada termina cuando un usuario cuelga, para el flujo de paquetes RTP y es enviando un mensaje de BYE. El usuario responde con una aceptación (200 OK).

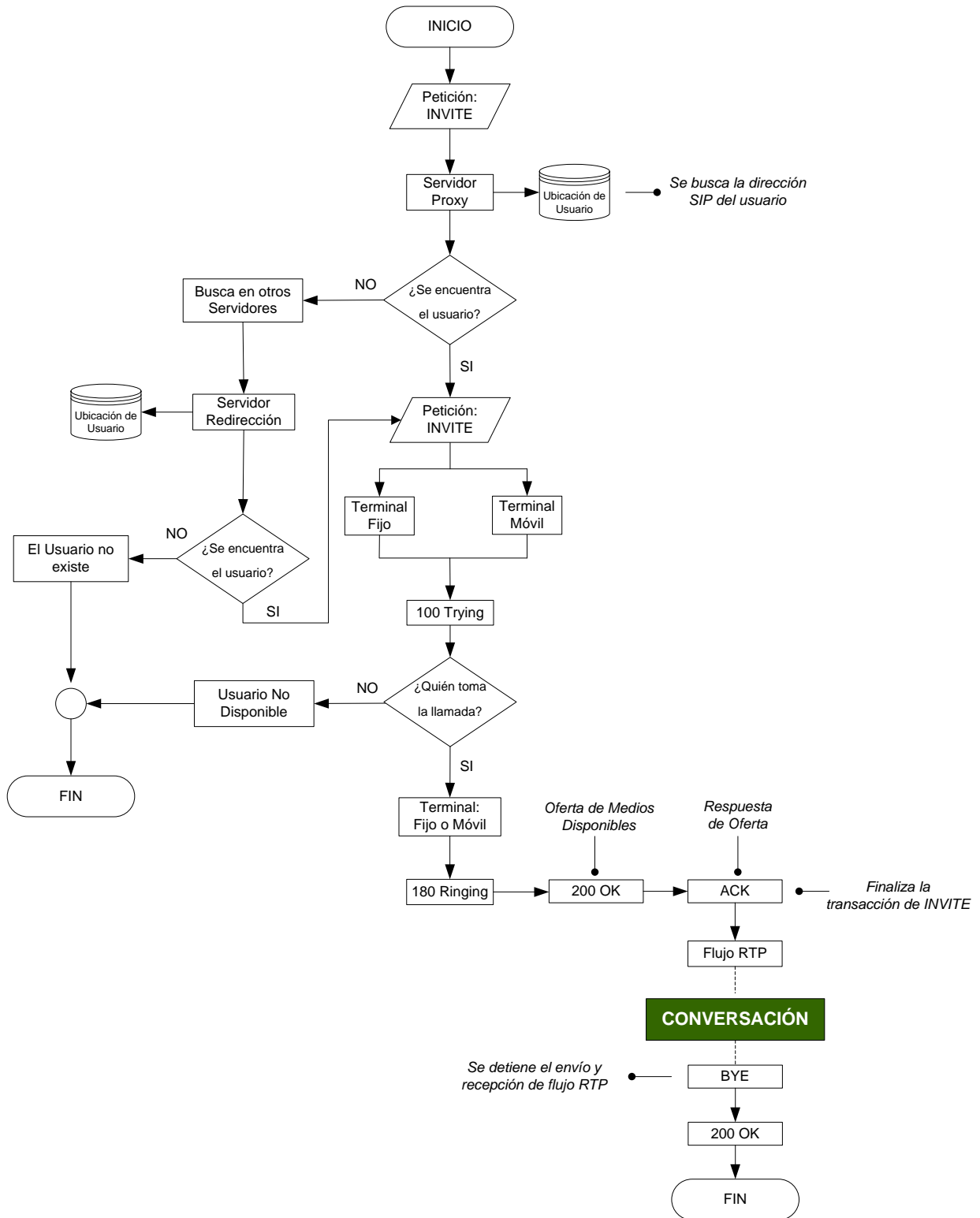


Figura 4. 12 Diagrama de flujo de una conversación empleando SIP.

4. ANALISIS

Otra alternativa, puede ser que el usuario sea hallado en el servidor Proxy, por tal motivo no es necesario buscarlo, el servidor Proxy puede pedir la autenticación del usuario. Esto es, porque pueden darse un caso diferente, dependiendo del tamaño de la red, el servidor o las terminales.

Para detallar de mejor manera este caso, se establece la sesión de un usuario transmisor a un usuario receptor, como sigue en el pseudocódigo.

1. Inicio.
2. Se envía una petición de Invitación (*Invite*) por parte de un usuario transmisor al servidor Proxy.
3. El servidor Proxy la procesa y pide al usuario transmisor la autenticación.
4. El usuario transmisor, le envía una aceptación con la autenticación.
5. El usuario transmisor, de nuevo envía otra transacción de invitación (*Invite*) al servidor Proxy.
6. El servidor Proxy verifica el dominio del usuario en un servidor DNS.
7. El servidor DNS envía su contestación al usuario.
8. El servidor Proxy envía la petición de Invitación (*Invite*) al usuario receptor.
9. El usuario receptor le hace saber al servidor Proxy que el teléfono está sonando.
10. El servidor Proxy le hace saber al usuario transmisión que el teléfono está sonando.
11. El usuario receptor toma la llamada y se lo hace saber al servidor Proxy.
12. El servidor Proxy le hace saber al usuario transmisor que se tomó la llamada.
13. El usuario transmisor envía una aceptación de confirmación al servidor Proxy.
14. El servidor Proxy, envía una aceptación de confirmación al usuario receptor.

En el último paso (14) se inicia la conversación, entre el usuario transmisor y el usuario receptor, entonces comienza el flujo de paquetes RTP. La transacción de invitación (*Invite*) se ha completado, pero en todo momento el servidor Proxy esta monitoreando la conversación, el diagrama de secuencia, se muestra en la figura 4.13.

Cuando un usuario ya sea el transmisor o receptor decide finalizar la conversación, entonces sucede lo siguiente.

4. ANALISIS

15. El usuario receptor envía un mensaje de finalización al servidor Proxy.
16. El servidor Proxy envía un mensaje de finalización al usuario transmisor.
17. El usuario transmisor le envía una aceptación de confirmación al servidor Proxy.
18. Finalmente, el usuario receptor recibe una aceptación de confirmación por parte de servidor Proxy.
19. Fin.

Ya finalizada la conversación los recursos utilizados y los usuarios son liberados, lo cual indica que están disponibles para una nueva conversación, el diagrama de secuencia, para la finalización de una conversación aparece en la figura 4.14.

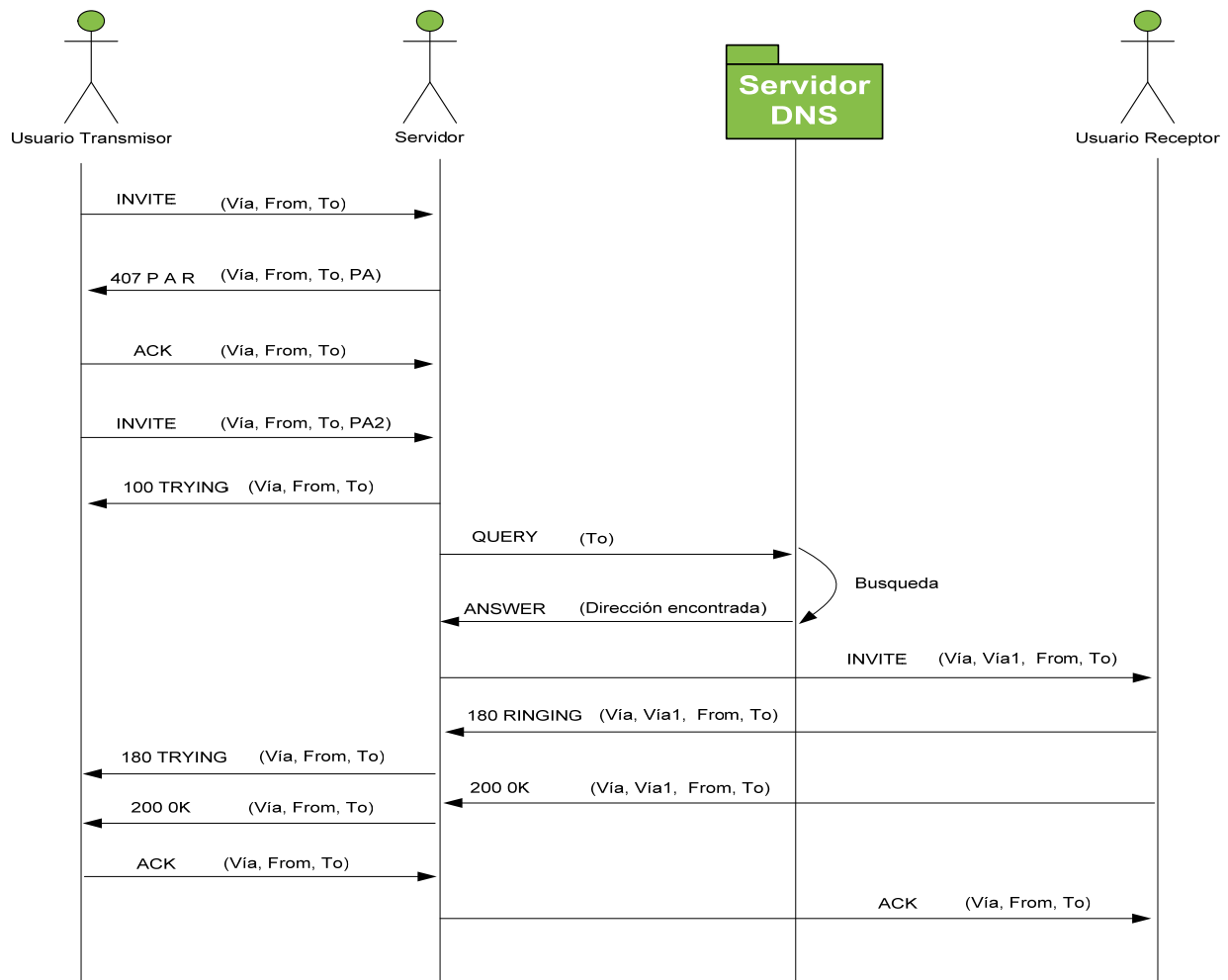


Figura 4. 13 Diagrama de secuencia de una transacción de invitación (Invite).

4. ANALISIS

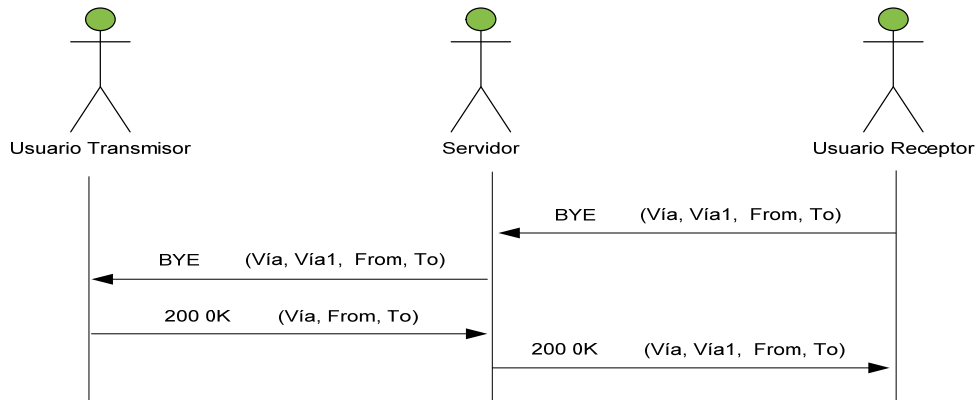


Figura 4. 14 Diagrama de secuencia de la finalización de una llamada.

Resumiendo lo antes mencionado, se considera la aplicación del protocolo SIP realizada como indica en la figura 4.12, donde dos usuarios inician una sesión, hasta este momento la voz viaja bajo algún tipo de codec (que fue negociado previamente mediante el RTP) y la información de los protocolos de la capa de aplicación en encabezados SIP. Los datos son enviados al protocolo de la capa de transporte, UDP, el cual ofrece un servicio sin conexión y no confiable pero práctico para aplicaciones de tiempo real, el datagrama UDP se envía a la capa de Internet, donde IP suministra los medios necesarios para la transmisión de datagramas a la siguiente capa de enlace de datos (LLC y MAC), la capa física recibe tramas de tamaño variable. La longitud promedio de la trama es de 1518 bytes y la mínima es de 64 bytes; la carga útil, donde va la voz que se quiere transmitir tiene una longitud máxima de 1500 bytes y mínima de 46 bytes.

Esta trama contiene todos los datos del encabezado de los protocolos anteriores y los mensajes del protocolo SIP [28], ya que la voz llegó hasta el otro extremo de forma digital y para eso fue necesario el procedimiento anterior, ahora comienza a extraer la información del encabezado, esto es cuando se inició, la voz pasó por un proceso de conversión analógico-digital se comprimió y se transmitió utilizando el Protocolo IP, para el transporte se utilizó UDP, RTP para la transmisión en tiempo real y SIP se encargó de la señalización, la información pasó a través de los protocolos mencionados y al final se envió la señal eléctrica mediante medios físicos. Ahora el proceso es inverso, la información se extrae del encabezado de los protocolos y se reconstruye los datos digitales a señales audibles [10].

4. ANALISIS

De acuerdo a lo anterior, cada protocolo tiene en su encabezado campos dedicados a las diferentes formas de transmisión, ya sea datos, video o voz. Este trabajo está enfocado a la telefonía IP, por lo tanto requiere de la utilización de un protocolo de señalización que enlace a usuarios en una conversación dentro de una red de Internet, esta función la realiza el Protocolo de Inicio de Sesión (SIP). También se requiere de un protocolo que describa las características más sobresalientes de los medios y ubicación de usuarios de modo que exista una comunicación, de eso está encargado el Protocolo de Descripción de Sesión (SDP). El Protocolo de Transporte en Tiempo Real tiene dos funciones importantes en el proceso: primero detecta la pérdida de paquetes y segundo tiene registros de la marca de tiempo entre un paquete y otro; esto genera control en el envío. En el transporte, el Protocolo de Datagrama de Usuario (UDP) permite el envío de datos y el Protocolo IP (IP) realiza el transporte hacia el destino final. El enlace físico puede realizarse por distintos medios, en este caso se utiliza Ethernet.

Ya que se tiene un espectro más amplio de la comunicación VoIP, en el capítulo 5 “Implementación Experimental” se presenta una plataforma de red local que mediante un servidor realiza la función de “*call center*”, con la cual se pueden gestionar llamadas entre usuarios dentro de la red local y en la red de Internet. Finalmente, con un software de nombre “*Ethereal*” se compara el análisis hecho en este capítulo con el flujo de mensajes en tiempo real de una llamada entre usuarios SIP que se realiza en la plataforma experimental.

CAPÍTULO 5

IMPLEMENTACIÓN EXPERIMENTAL

En este capítulo se presenta la implementación de un servidor en una topología de red que esta enlazado con dos terminales. El servidor tiene la función de registrar a cada terminal con un número de extensión. En las terminales se instaló un programa que funciona como un teléfono tradicional pero instalado en un dispositivo, en este caso una computadora. El usuario de cada terminal puede solicitarle al servidor una conversación con el usuario de la otra terminal y entonces el servidor enlaza a los dos usuarios. Lo anterior fue hecho dentro de la red local.

Se modificó la configuración del servidor con una dirección IP pública para un acceso de usuarios fuera de la red. Esto significa que un usuario puede realizar una conversación con otro usuario que se encuentre en otra localidad. Se realizaron pruebas de conexión con el servidor y de usuario a usuario, se empleo el Protocolo de señalización SIP en cada terminal.

Se consideró por medio de un software de nombre “Ethereal” si los resultados obtenidos en una conversación real de Voz sobre IP corresponde a los resultados del estudio realizado en el capítulo 4 Análisis.

5.1 ARQUITECTURA DE RED

Para diseñar la red fue necesario varios elementos: 1er. una máquina que tuviera la función de servidor, 2do. una máquina administradora que funcione como interfaz gráfica, 3ro. una máquina

5. IMPLEMENTACION EXPERIMENTAL

terminal para la elaboración de pruebas, 4to. un hub para la topología tipo estrella, 5to. un switch el cual brindará el servicio de conexión de Internet, 7mo. micrófonos externos y 7mo. cableado.

Como se muestra en la figura 5.1, se muestra claramente la conexión del servidor con las dos terminales y la comunicación con el hub y el switch. Las características técnicas de cada elemento, son las siguientes:

- Máquina Servidor: procesador Pentium III, 500 MHz, 256Mb. RAM, disco duro de 6 GB tarjeta de red 10 Mbps y unidad de disco.
- Máquina Terminal: procesador AMD Turion 64X2, 1.60 GHz, 2 GB RAM, disco duro de 160 GB, tarjeta de red 100 Mbps, tarjeta inalámbrica y unidad de disco.
- Hub ARK de 8 puertos 10/100.
- Switch Linksys Wireless-G 2.4 GHz, 4 puertos [29].

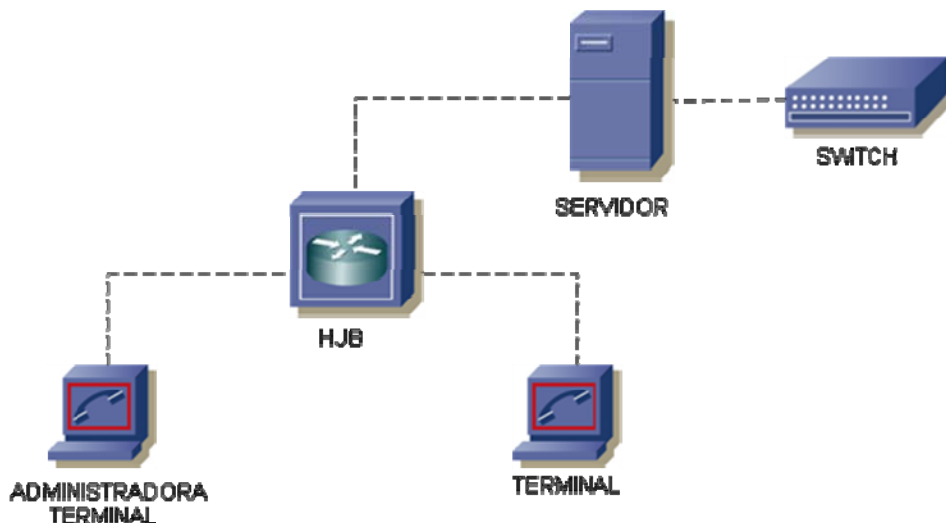


Figura 5. 1 Red inicial del sistema experimental.

5.2 INSTALACION DEL SOFTWARE DEL SISTEMA

Para la instalación del software en la máquina servidor, es necesario descargar de la página oficial [30] el paquete de nombre TrixBox, basado en Linux en su versión 2.2.4 CE el cual cuenta con varios elementos: Linux CentOS, Asterisk, FreePBX.

5. IMPLEMENTACION EXPERIMENTAL

- Linux está basado en ‘Red Hat Enterprise’.
- Asterisk es el núcleo propio de la telefonía.
- FreePBX es el entorno gráfico que facilita la configuración de Asterisk; no a través de la edición de archivos de texto, sino a través de interfaces Web.

TrixBos es similar a una central telefónica la cual puede manejar hasta diez extensiones, incluye un servidor Web Apache con soporte de lenguaje PHP y MySQL para bases de datos, este servidor tiene la función de fungir como servidor de Registro, Redirección (en caso de ser necesario) y Proxy; cuenta con una base de datos interna de todas las extensiones, las características de cada una de ellas y guarda los detalles de conversaciones [29].

5.2.1 Configuración del Servidor

En la máquina servidor que de aquí en adelante llamaremos simplemente servidor, se procede a configurar el software de TrixBos. Los parámetros que solicita el servidor son:

- Selección del tipo de teclado (figura 5.2).
- Selección de zona horaria (figura 5.3).
- Asignación de contraseña para la cuenta root (figura 5.4).

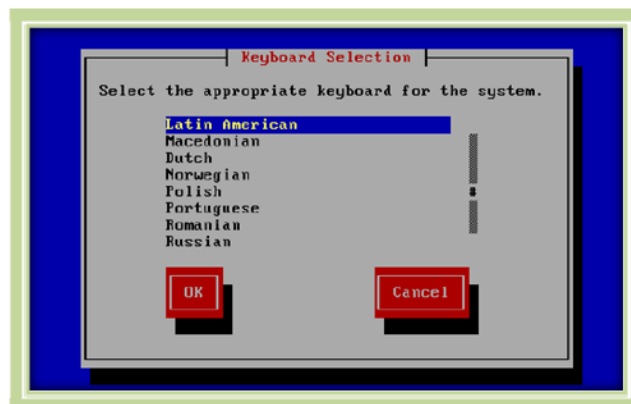


Figura 5. 2 Selección del tipo de teclado.

5. IMPLEMENTACION EXPERIMENTAL

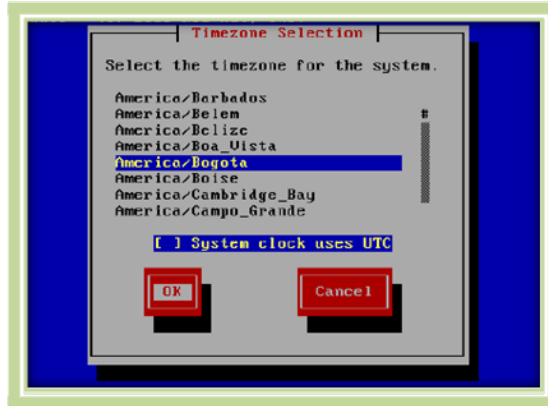


Figura 5. 3 Selección de zona horaria.

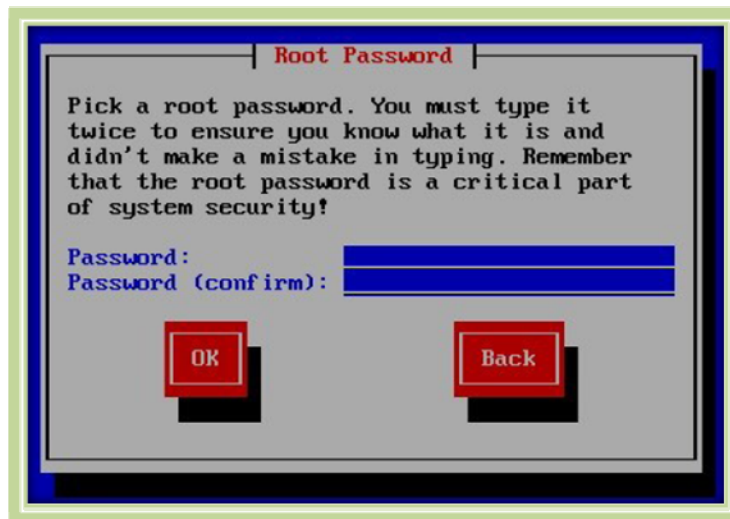


Figura 5. 4 Asignación de contraseña para la cuenta root.

El proceso comienza con la instalación de los paquetes Linux, después se inicia la instalación de Asterisk y demás componentes propios de TrixBos, finalmente se reinicia el equipo y ya iniciado está listo para desempeñar su función de servidor; es recomendable como en todo equipo que las contraseñas sean seguras.

Existen varios comandos de Linux con los que podemos modificar algunas características del servidor TrixBos, en él introducimos el comando **'help'** y nos proporciona una lista con los comandos más importantes para Linux.

5. IMPLEMENTACION EXPERIMENTAL

Ahora, se modifica la dirección IP con la red que se tiene, se introduce el comando **'netconfig'**, aparece una pantalla que indica si se desea modificar la red (figura 5.5). Se indica que si y la siguiente pantalla pide que se configure la red de forma dinámica o aleatoria. En este caso, se opta por hacerlo de manera dinámica, en la figura 5.6, se presentan las dos opciones para la configuración de la red.

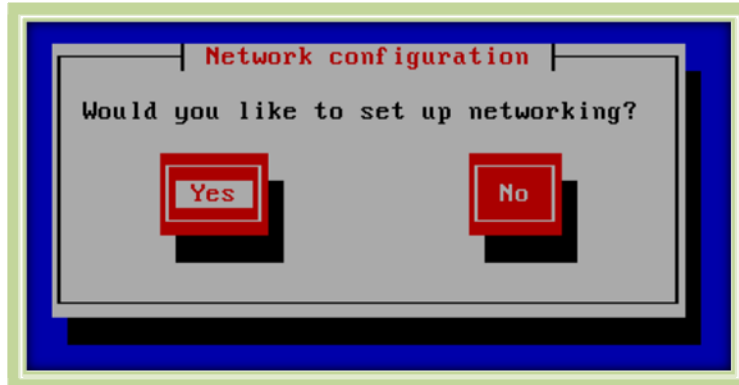


Figura 5. 5 Configuración de la red.

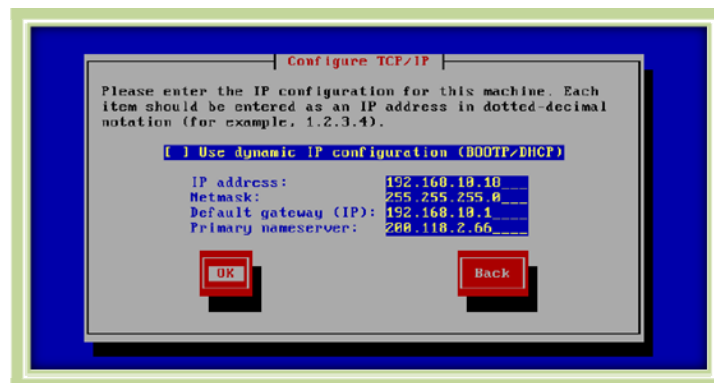


Figura 5. 6 Configuración manual o dinámica de la red.

La dirección IP registrada aparece después de que se guardan los cambios y se reinicia el servidor. En la terminal administradora se abre una página de Internet y en el buscador se coloca la dirección IP que nos fue proporcionada por el servidor al inicio, en la pantalla siguiente se muestra en el recuadro negro la dirección IP.

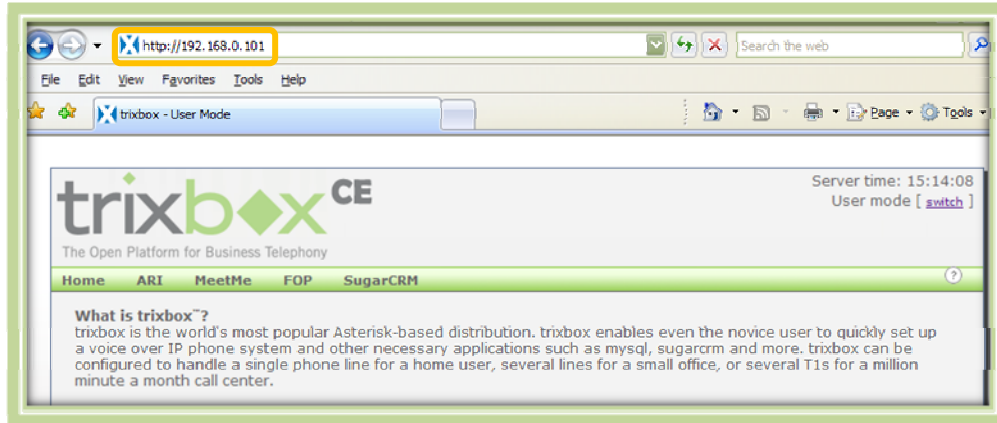


Figura 5. 7 Pantalla de inicio de la interfaz de TriBox.

5.2.2 Configuración de la Interfaz

En la interfaz se ingresa a FreePBX modulo del cual se puede gestionar la creación, modificación y eliminación de extensiones, así como se dispone de reportes y estadísticas de llamadas, también muestra las características del servidor, el estatus de la memoria y el tiempo de inicio del servidor. En la figura 5.8 se muestra la versión y los apartados con los que cuenta.

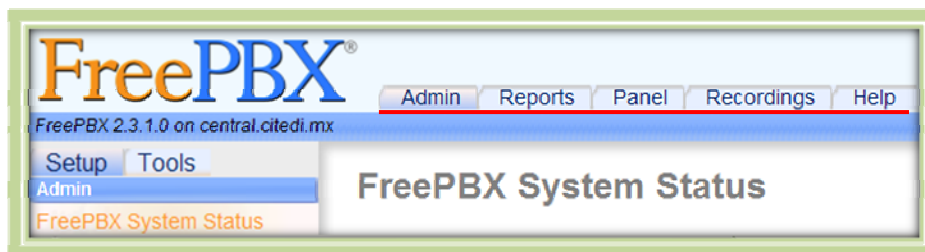


Figura 5. 8 Pantalla de inicio de FreePBX.

La pantalla principal se divide en cinco módulos: administración, reporte, panel, grabaciones y ayuda.

En Administración (*admin*), se encuentran las secciones de Administración, Básicas, Control de llamadas internas y Configuración y opciones internas. En cada una de ellas se puede realizar diferentes actividades, desde actualizar la versión de FreePBX, así como también crear administradores, extensiones, modificar las características de llamadas y grabar música de espera

5. IMPLEMENTACION EXPERIMENTAL

En Reportes (*reports*), se localizan un programa para sacar estadísticas de acuerdo al flujo de llamadas del día, mes o año y la descripción de las llamadas. Estos reportes se pueden obtener en archivo Excel o PDF en línea.

En Panel (*panel*), se enlistan las extensiones creadas, su actividad y si tienen algún mensaje pendiente.

En Grabaciones (*recordings*), se tiene un enlace el cual nos brinda el servicio de correo de voz, es necesario tener extensión y contraseña.

En Ayuda (*help*), auxilia en el caso de tener alguna duda o conflicto con el servidor.

El FreePBX es utilizado como enlace al servidor ya que TrixBox no cuenta con su propia interfaz dentro del sistema operativo. Por tal razón, como se mencionó al inicio de este capítulo es necesario contar con una terminal administradora, desde la cual se gestione toda la administración del servidor, al que también podemos llamar central telefónica.

En el apartado de administración se ingresa a extensiones, creándose una para cada terminal, los datos más importantes son: extensión (recomendada con tres dígitos), contraseña, nombre de despliegue y otros servicios agregados. El administrador guarda el servidor guarda un registro en la base de datos (figura 5.9). Se tiene entonces, dos cuentas [29]:

- Usuario A con el número 200.
- Usuario B con el número 201.

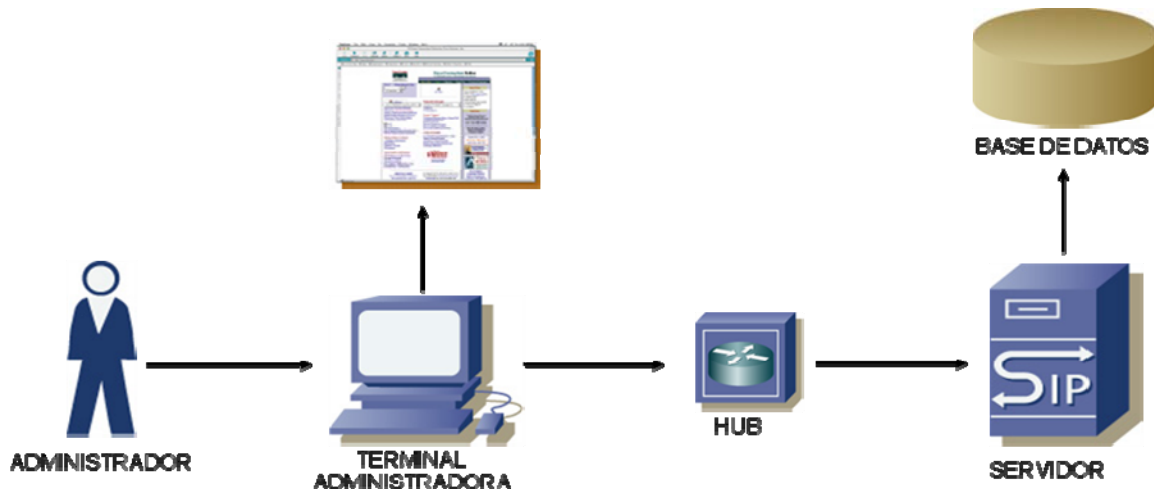


Figura 5.9 Creación de una extensión por el administrador.

Después de que el administrador dio de alta la cuenta por medio de la interfaz FreePBX de manera sencilla, se procede a realizar pruebas de conexión con el objetivo de limitar los errores en comunicación [31].

5.2.3 Instalación y configuración del Softphone

De acuerdo a lo anterior es necesario contar con un softphone, este dispositivo funciona como teléfono ordinario, su interfaz suele ser diferente para cada marca de softphone. En general se trata de simular un teléfono en pantalla, solo que mediante la ayuda física de un monitor y un teclado.

Para la instalación del softphone se requiere de bajar el ejecutable de la página oficial en Internet (www.counterpath.com) [32] y configurarlo de acuerdo a los parámetros que tiene el servidor, los cuales son: nombre a desplegar, nombre de usuario, contraseña, servidor Proxy y dominio, tal como aparece en la figura 5.10. Los codecs de audio que se utilizan es G.711 a-Law, G711 u-Law y GSM y de video H.63.

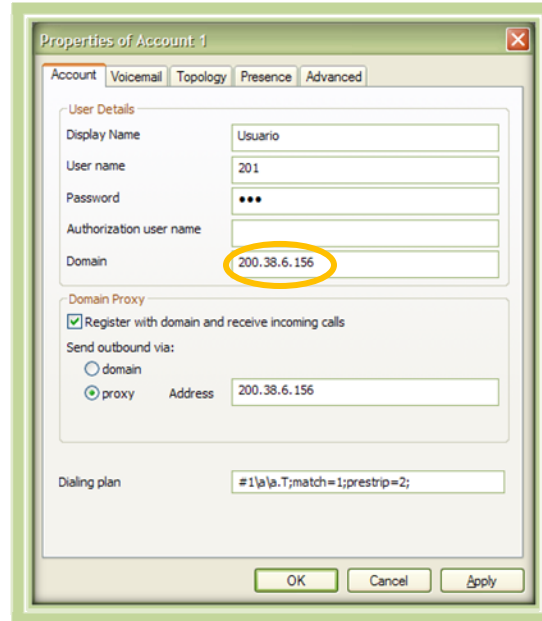


Figura 5. 10 Parámetros requeridos para la configuración de un softphone.

El nombre del softphone es X-Lite versión 3.0 de la compañía Counterpath [33]. Este softphone es muy popular en el mercado, está dentro de los diez softphone más usado en la actualidad que no requieren licencia [34]. Los requerimientos para su instalación se presentan en la tabla 5.1. Las características más importantes se mencionan a continuación:

Características

- Utiliza el Protocolo de Inicio de Sesión para todas las sesiones interactivas.
- Libro de direcciones personal, incluyendo listas de llamadas e historial.
- Integración con Microsoft Outlook permitiendo que los usuarios importen su libro de dirección en su lista de contactos.
- Grabación de llamada de la voz y del vídeo
- Facilidad de recibir y hacer llamadas al permitir la selección de llamadas entrantes.

5. IMPLEMENTACION EXPERIMENTAL

Tabla 5. 1 Requerimientos para el uso del softphone X-Lite

DISPOSITIVO	MÍNIMO	MÁXIMO
Procesador	Intel Pentium III 700 MHz o equivalente	Pentium 4® 2.0 GHz o equivalente
Memoria	256 MB	256 MB
Espacio en el disco duro	30 MB	30 MB
Sistema Operativo	Windows 2000 Windows XP	
Conexión	Conexión de Red IP (Banda ancha, LAN, wireless)	
Adaptador de sonido	Full-duplex, 16-bit	

Una ventaja es la interfaz sencilla, con la que se puede realizar y recibir llamadas, tener comunicación en videoconferencia y mensajería instantánea. Es compatible con otros estándares de telefonía y con protocolos de señalización diferentes. En la figura 5.11 se muestra la imagen de la interfaz del softphone.



Figura 5. 11 X-Lite versión 3.0

También fue usado el softphone Sjphone para realizar pruebas de compatibilidad, el cual provee servicio empleando el Protocolo SIP, tiene características similares al softphone X-Lite, solo que la interfaz está diseñada de manera diferente; también está dentro de los 10 más utilizados en la actualidad. En la figura 5.12 se muestra el softphone Sjphone [35].



Figura 5. 12 Softphone SjPhone.

Tanto el softphone X-Lite como Sjphone fueron utilizados para las pruebas realizadas, ya configurado los dos softphone y el servidor se realizan pruebas para el funcionamiento correcto. Probando que el servidor despliegue su enlace se introduce la dirección IP pública, asimismo el softphone o terminal en primera instancia se inicializa, busca al servidor por medio del parámetro que introducimos en el servidor Proxy.

Una vez que el servidor ya que tiene el registro de ese softphone abre un puerto (indicado en el registro) por donde tendrá contacto toda vez que se requiera. Si algún usuario solicita tener contacto con otro usuario y ya hizo su búsqueda en el servidor Proxy, este también funciona como servidor de redirección, le indicará por medio de un mensaje la ubicación en dónde puede localizar al usuario solicitado.

5.3 PRUEBAS DE COMUNICACION

Hasta este momento las dos terminales tienen comunicación con el servidor como aparece en la figura 5.1, en la figura 5.13 se observa a una de las terminales y el servidor teniendo comunicación en la red local.

5. IMPLEMENTACION EXPERIMENTAL



Figura 5. 13 Servidor y terminal administradora.

Cuando una terminal desea hacer una llamada con otra terminal, la terminal transmisora despliega un mensaje en la pantalla de la terminal receptora que está entrando una llamada, en la figura 5.14 se observa dicho mensaje.

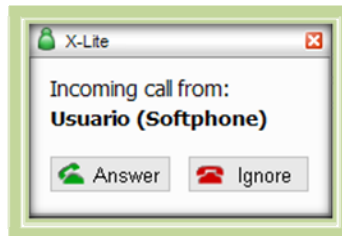


Figura 5. 14 Mensaje alertando de que está entrando una llamada.

La terminal receptora contesta la llamada y se inicia la conversación, se puede comprobar que la llamada fue contestada, entrando a la interfaz FreePBX y en el apartado de reportes se muestra la información de la llamada (figura 5.15), la cual muestra la fecha, hora, canal, fuente o terminal transmisora así como su descripción, el número del destino, la disposición de la llamada y la duración.

	Calldate	Channel	Source	Clid	Dst	Disposition	Duration
1.	2008-08-29 14:06:15	SIP/200-09..	200	"Usuario" <200>	201	ANSWERED	00:17
2.	2008-08-29 14:05:58	SIP/201-09..	201	"Usuario" <201>	200	ANSWERED	00:13
3.	2008-08-29 14:03:19	SIP/201-09..	201	"Usuario" <201>	200	ANSWERED	00:04

Figura 5. 15 Información de la conversación realizada.

5. IMPLEMENTACION EXPERIMENTAL

En el sistema local se realizaron 100 llamadas de las cuales 75 no fueron exitosas, 21 fueron contestadas y 4 tenían tono de ocupado. El porcentaje de fallos es muy alto debido a que el sistema y las terminales se encontraban en pruebas teniendo dificultades para enlazar por medio de la dirección IP al transmisor y receptor.

Posteriormente con el sistema en con conexión al exterior se realizaron 778 llamadas, la disposición de contestación fue diferente en algunos casos, como los siguientes:

- Contestada (354)
- No contestada (419)
- Fallo (1)
- Ocupado (5)

Durante el periodo de pruebas se realizaron las siguientes llamadas por mes que se presenta en la gráfica.

5. IMPLEMENTACION EXPERIMENTAL

Tabla 5. 2 Nueva dirección IP del servidor.

CENTRAL.CITEDI.MX	
Dirección IP	200.38.6.156
Máscara de subred (Subset mask)	255.255.255.128
Puerta de enlace (Gateway)	200.38.6.190
Servidor DNS	200.38.6.129

Cualquier terminal exterior puede acceder al servidor mediante la dirección IP pública, esto es, que podemos tener servicio fuera de la red. Dentro de la red del CITEDI se tienen varias computadoras, las cuales tienen acceso a Internet y únicamente una dirección IP; pero al salir hacia el exterior pasan por el servidor DNS, el cual envía la información con una IP pública. Cuando la información se envía de vuelta a la red del CITEDI, llega al servidor DNS y éste busca quien es el destinatario por medio de la única dirección IP. Lo mismo sucede con el servidor TrixBos, la red interna tiene una dirección IP pero en el exterior se identifica con la dirección IP pública 200.38.6.156 o el dominio central.citedi.mx [37].

La topología que se tiene ahora aparece en la figura 5.16, la cual muestra la red del CITEDI. Se observa el servidor DNS, los enrutadores tanto el interno como externo, dos switches, el servidor TrixBos y las terminales.

5. IMPLEMENTACION EXPERIMENTAL

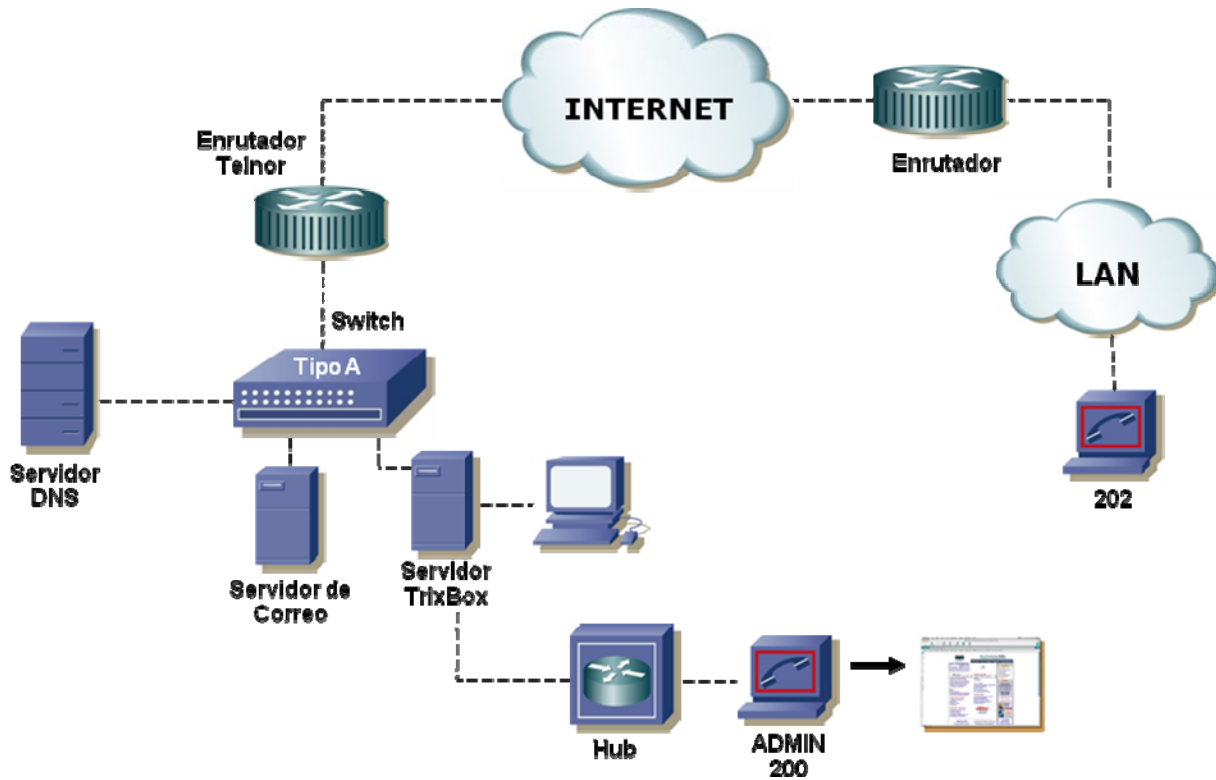


Figura 5. 17 Topología de red con acceso desde el exterior a la red local de CITEDI.

El switch tipo A y B respectivamente, son el grupo de direcciones que están asignadas a CITEDI.

Tabla 5. 3 Tipo A.

PARAMETROS	
Dirección IP	200.38.6.130 a 192
Máscara de subred (<i>Subset mask</i>)	255.255.255.192
Puerta de enlace (<i>Gateway</i>)	200.38.6.190
Servidor DNS	200.38.6.129

Tabla 5. 4 Tipo B.

PARAMETROS	
Dirección IP	200.38.6.130
Máscara de subred	255.255.255.192
Puerta de enlace	200.38.6.190
Servidor DNS	200.38.6.129

5.4 Análisis del tráfico de Voz en Tiempo Real

Para verificar que el análisis fue desarrollado satisfactoriamente se recurrió a un software de redes llamado “Ethereal”, en su versión gratuita, este software tiene como principal característica que captura el tráfico de una red, ya sea Ethernet o wireless o despliega en pantalla los protocolos que intervienen en la transmisión. En este caso, se analiza la llamada de un softphone a otro en la misma red, se acepto la llamada y después de unos segundos se finalizó. La figura 5.17 muestra el intercambio de mensajes en la captura desde la terminal donde se encuentra el softphone.

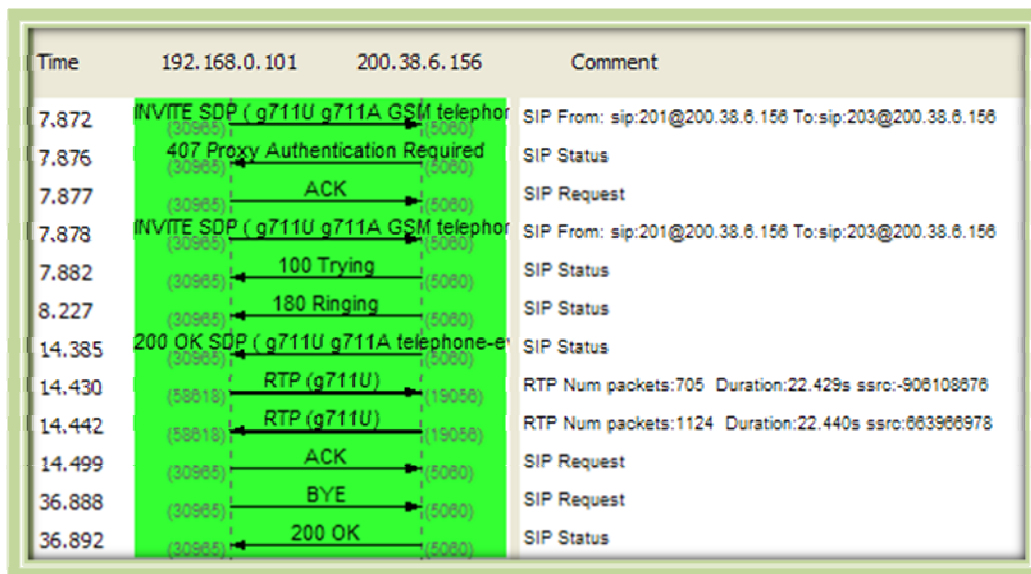


Figura 5. 18 Flujo de mensajes en una llamada VoIP empleando SIP.

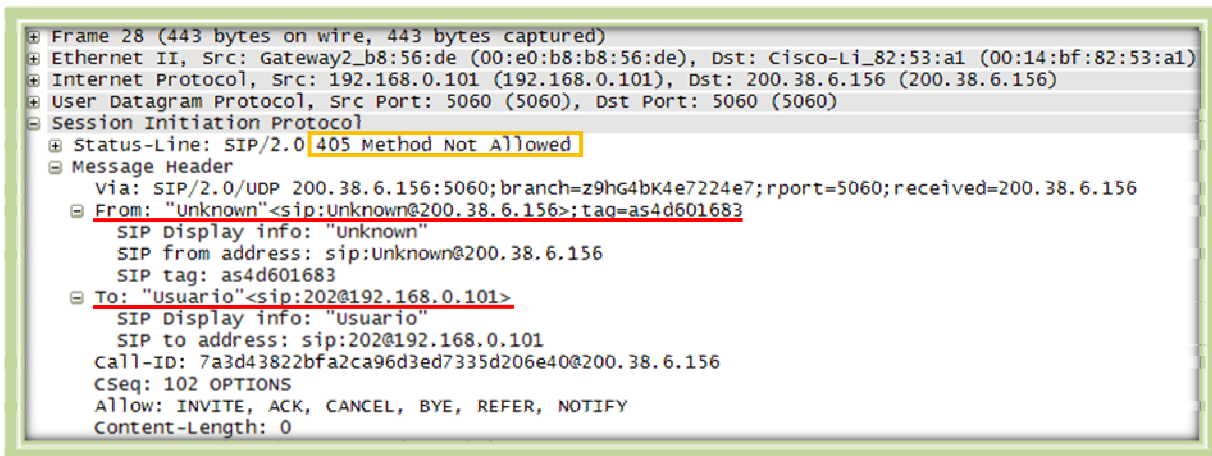
Se puede apreciar que la comunicación entre un usuario y otro es equivalente a las figuras 4.12 y 4.13 del capítulo anterior, los parámetros que intervienen son: el tiempo, la dirección IP fuente, dirección IP destino y comentario.

El establecimiento comienza con un mensaje de ‘invite’ por parte del softphone, donde se envía encapsulado sobre el protocolo SIP un mensaje del protocolo SDP, para negociar los codecs (G711 U, G711A GSM). El siguiente mensaje es un ‘100 Trying’ enviado por el teléfono SIP en respuesta a la invitación recibida, luego en el mismo sentido se envía un mensaje de sonando ‘180 Ringing’, para confirmar que se está dando aviso de la llamada entrante. Al aceptar la

5. IMPLEMENTACION EXPERIMENTAL

comunicación, el softphone envía un mensaje de '200 OK' con un mensaje de SDP, encapsulado sobre SIP con el codec a utilizar (G.711 U), después los siguientes mensajes son de RTP para el intercambio de audio, se confirma con un mensaje reconocimiento (*ack*) la utilización del protocolo y el codec. Finalmente, se termina la comunicación por parte del softphone y envía un mensaje de fin (*bye*) y el otro extremo responde con un '200 OK' para confirmar el fin de la llamada.

El análisis comienza con el primer mensaje de invitación, la figura 5.18 muestra los campos de SIP, enlista en jerarquía los protocolos utilizados comenzando con Ethernet hasta llegar a SDP. Los datos marcados es el estatus del mensaje, usuario origen y usuario destino.

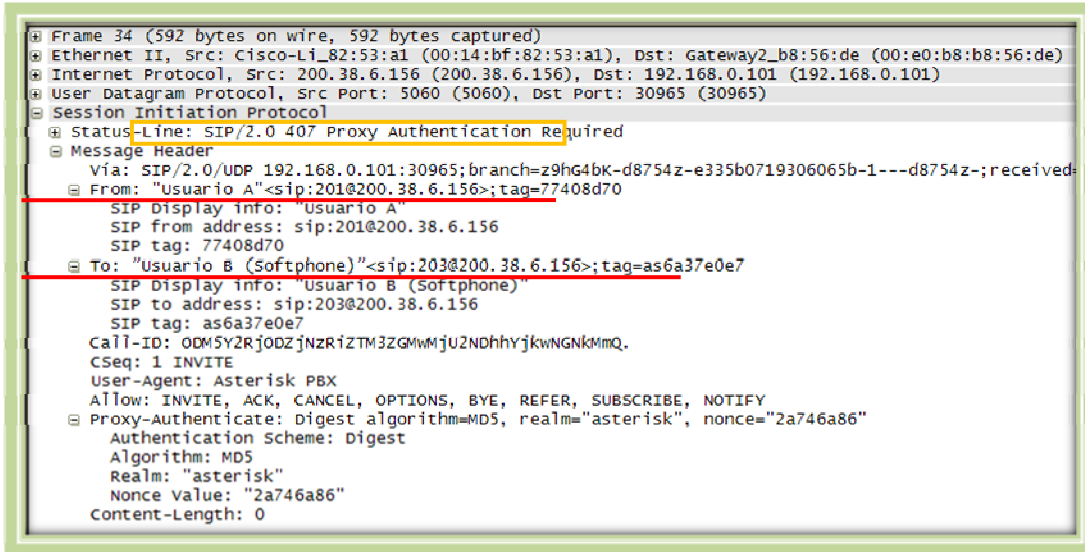


```
⊕ Frame 28 (443 bytes on wire, 443 bytes captured)
⊕ Ethernet II, Src: Gateway2_b8:56:de (00:e0:b8:b8:56:de), Dst: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1)
⊕ Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 200.38.6.156 (200.38.6.156)
⊕ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊖ Session Initiation Protocol
  ⊕ Status-Line: SIP/2.0 405 Method Not Allowed
  ⊖ Message Header
    Via: SIP/2.0/UDP 200.38.6.156:5060;branch=z9hg4bk4e7224e7;rport=5060;received=200.38.6.156
    ⊖ From: "Unknown"<sip:unknown@200.38.6.156>;tag=as4d601683
      SIP Display info: "Unknown"
      SIP from address: sip:Unknown@200.38.6.156
      SIP tag: as4d601683
    ⊖ To: "Usuario"<sip:202@192.168.0.101>
      SIP Display info: "Usuario"
      SIP to address: sip:202@192.168.0.101
    Call-ID: 7a3d43822bfa2ca96d3ed7335d206e40@200.38.6.156
    Cseq: 102 OPTIONS
    Allow: INVITE, ACK, CANCEL, BYE, REFER, NOTIFY
    Content-Length: 0
```

Figura 5. 19 Mensaje de inicio de la llamada.

En la figura anterior se puede apreciar que el usuario aún no ha sido autenticado, lo cual indica que no se despliega el nombre del usuario hasta que este usuario envíe sus datos de nueva cuenta y se sometan a un algoritmo de autenticación, como lo muestra la figura 5.19.

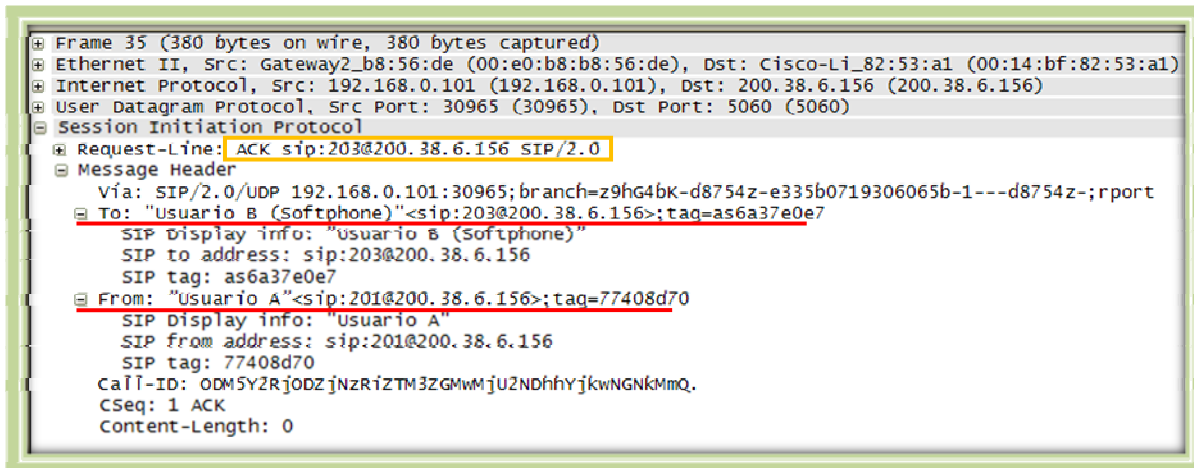
5. IMPLEMENTACION EXPERIMENTAL



```
# Frame 34 (592 bytes on wire, 592 bytes captured)
# Ethernet II, Src: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
# Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
# User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
# Session Initiation Protocol
# Status-Line: SIP/2.0 407 Proxy Authentication Required
# Message Header
  Vía: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hG4bK-d8754z-e335b0719306065b-1---d8754z-;received=
  From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
  SIP Display info: "Usuario A"
  SIP from address: sip:201@200.38.6.156
  SIP tag: 77408d70
  To: "Usuario B (Softphone)"<sip:203@200.38.6.156>;tag=as6a37e0e7
  SIP Display info: "Usuario B (Softphone)"
  SIP to address: sip:203@200.38.6.156
  SIP tag: as6a37e0e7
  Call-ID: ODM5Y2RjODZjNzRlZTM3ZGMwMjU2NDhhYjkwNGNkMmQ.
  CSeq: 1 INVITE
  User-Agent: Asterisk PBX
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
  Proxy-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="2a746a86"
  Authentication Scheme: Digest
  Algorithm: MD5
  Realm: "asterisk"
  Nonce Value: "2a746a86"
  Content-Length: 0
```

Figura 5. 20 Mensaje de autenticación

En la figura 5.20 el usuario envía una confirmación con el mensaje de reconocimiento respondiendo al mensaje anterior.



```
# Frame 35 (380 bytes on wire, 380 bytes captured)
# Ethernet II, Src: Gateway2_b8:56:de (00:e0:b8:b8:56:de), Dst: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1)
# Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 200.38.6.156 (200.38.6.156)
# User Datagram Protocol, Src Port: 30965 (30965), Dst Port: 5060 (5060)
# Session Initiation Protocol
# Request-Line: ACK sip:203@200.38.6.156 SIP/2.0
# Message Header
  Vía: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hG4bK-d8754z-e335b0719306065b-1---d8754z-;rport
  To: "Usuario B (Softphone)"<sip:203@200.38.6.156>;tag=as6a37e0e7
  SIP Display info: "Usuario B (Softphone)"
  SIP to address: sip:203@200.38.6.156
  SIP tag: as6a37e0e7
  From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
  SIP Display info: "Usuario A"
  SIP from address: sip:201@200.38.6.156
  SIP tag: 77408d70
  Call-ID: ODM5Y2RjODZjNzRlZTM3ZGMwMjU2NDhhYjkwNGNkMmQ.
  CSeq: 1 ACK
  Content-Length: 0
```

Figura 5. 21 Envío de mensaje ACK de confirmación.

El usuario envía una invitación de nuevo ya que el primer mensaje no estaba permitido aún porque el usuario no estaba autenticado, entonces envía un '100 trying' para confirmar que sigue en la transacción (figura 5.21).

5. IMPLEMENTACION EXPERIMENTAL

```

* Frame 37 (509 bytes on wire, 509 bytes captured)
* Ethernet II, Src: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
* Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
* User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
* Session Initiation Protocol
  * Status-Line: SIP/2.0 100 Trying
  * Message Header
    Via: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hg4bk-d8754z-f01f1370b0017930-1---d8754z-;received=200.38.6.129;rport=30965
    From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
      SIP Display info: "Usuario A"
      SIP from address: sip:201@200.38.6.156
      SIP tag: 77408d70
    To: "Usuario B (Softphone)"<sip:203@200.38.6.156>
      SIP Display info: "Usuario B (Softphone)"
      SIP to address: sip:203@200.38.6.156
      Call-ID: 0dM5Y2Rj0DZjNzRiZTM3ZGMwMjU2NDhhYjkwNGNkMmMq.
      CSeq: 2 INVITE
      User-Agent: Asterisk PBX
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
    Contact: <sip:203@200.38.6.156>
    * Contact Binding: <sip:203@200.38.6.156>
    Content-Length: 0

```

Figura 5. 22 Envío del mensaje '100 Trying'.

La figura 5.22 muestra el envío de un mensaje '100 Trying', el cual significa que el softphone al que se llama está sonando, en seguida del mensaje anterior, se envía '200 OK' el cual parece en la figura 5.23.

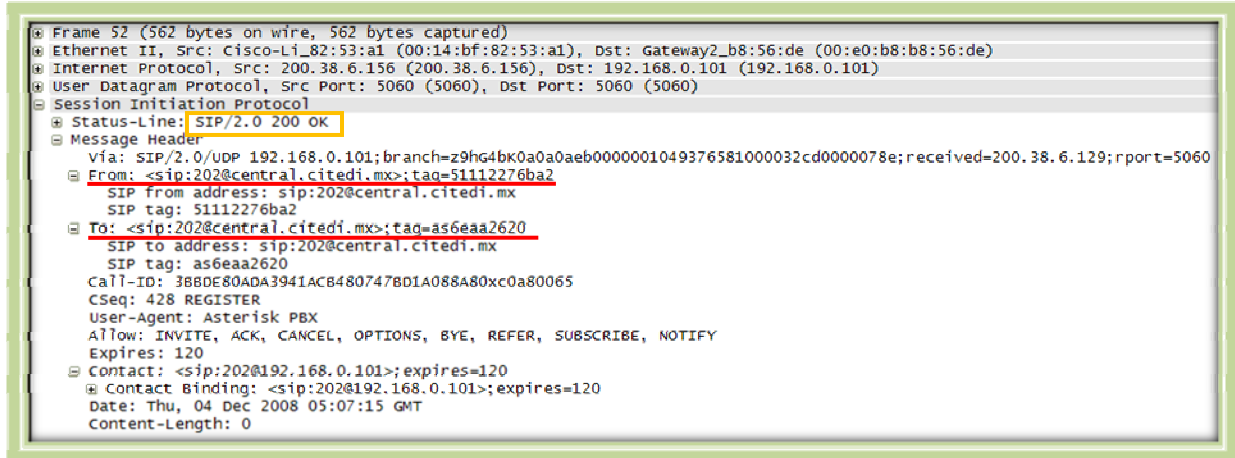
```

* Frame 39 (525 bytes on wire, 525 bytes captured)
* Ethernet II, Src: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
* Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
* User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
* Session Initiation Protocol
  * Status-Line: SIP/2.0 180 Ringing
  * Message Header
    Via: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hg4bk-d8754z-f01f1370b0017930-1---d8754z-;received=200.38.6.129;rport=30965
    From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
      SIP Display info: "Usuario A"
      SIP from address: sip:201@200.38.6.156
      SIP tag: 77408d70
    To: "Usuario B (Softphone)"<sip:203@200.38.6.156>;tag=as5df0ac44
      SIP Display info: "Usuario B (Softphone)"
      SIP to address: sip:203@200.38.6.156
      SIP tag: as5df0ac44
      Call-ID: 0dM5Y2Rj0DZjNzRiZTM3ZGMwMjU2NDhhYjkwNGNkMmMq.
      CSeq: 2 INVITE
      User-Agent: Asterisk PBX
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
    Contact: <sip:203@200.38.6.156>
    * Contact Binding: <sip:203@200.38.6.156>
    Content-Length: 0

```

Figura 5. 23 Envío de mensaje '180 Ringing'.

5. IMPLEMENTACION EXPERIMENTAL



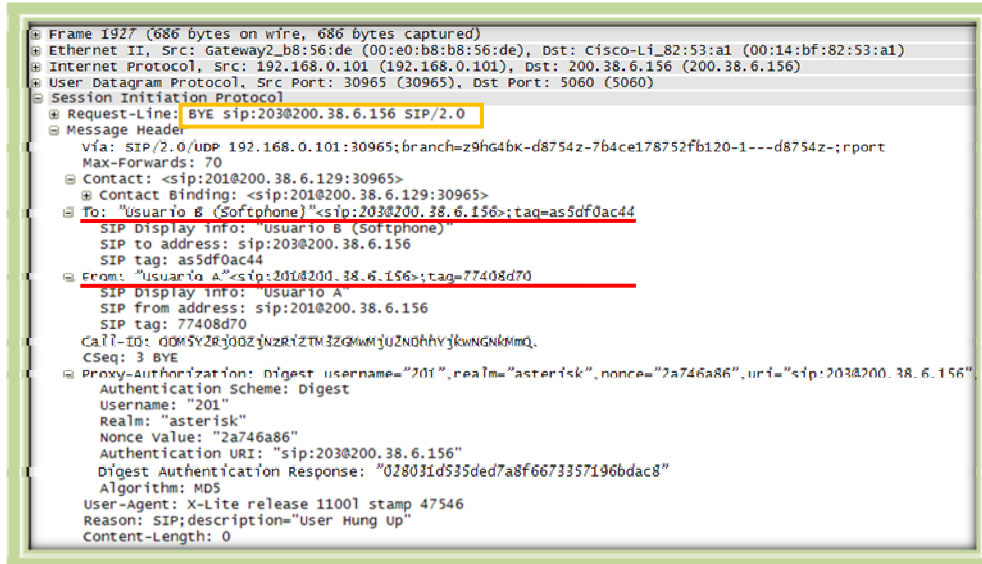
```
Frame 52 (562 bytes on wire, 562 bytes captured)
Ethernet II, Src: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Message Header
Via: SIP/2.0/UDP 192.168.0.101;branch=z9hg4bk0a0a0aeb0000001049376581000032cd0000078e;received=200.38.6.129;rport=5060
From: <sip:202@central.citedi.mx>;tag=51112276ba2
SIP from address: sip:202@central.citedi.mx
SIP tag: 51112276ba2
To: <sip:202@central.citedi.mx>;tag=as6eaa2620
SIP to address: sip:202@central.citedi.mx
SIP tag: as6eaa2620
Call-ID: 388DE80ADA394IACB480747BDIA088A80xc0a80065
CSeq: 428 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Expires: 120
Contact: <sip:202@192.168.0.101>;expires=120
Contact Binding: <sip:202@192.168.0.101>;expires=120
Date: Thu, 04 Dec 2008 05:07:15 GMT
Content-Length: 0
```

Figura 5. 24 Envío de mensaje ‘200 OK’.

En la figura 5.22 se observa que cada usuario tiene el nombre del dominio del servidor que es central.citedi.mx en su dirección SIP. Los mensajes anteriores tienen la dirección del dominio, 200.38.6.156.

Después de este mensaje, ambos usuarios usarán el esquema de compresión G.711 U para el intercambio de audio utilizando el protocolo RTP, el servidor sólo va monitorear las conversaciones y el protocolo SIP ya cumplió con su objetivo, que es proporcionar la señalización entre usuarios en una conversación. Si alguno de los dos usuarios decide finalizar la llamada, se envía entonces un mensaje de fin que representa el final de la conversación (figura 5.24). El otro usuario responde con un mensaje de aceptación ‘200 OK’ con el cual los recursos como: rutas, puertos, ancho de banda, quedan libres para su uso (figura 5.25).

5. IMPLEMENTACION EXPERIMENTAL

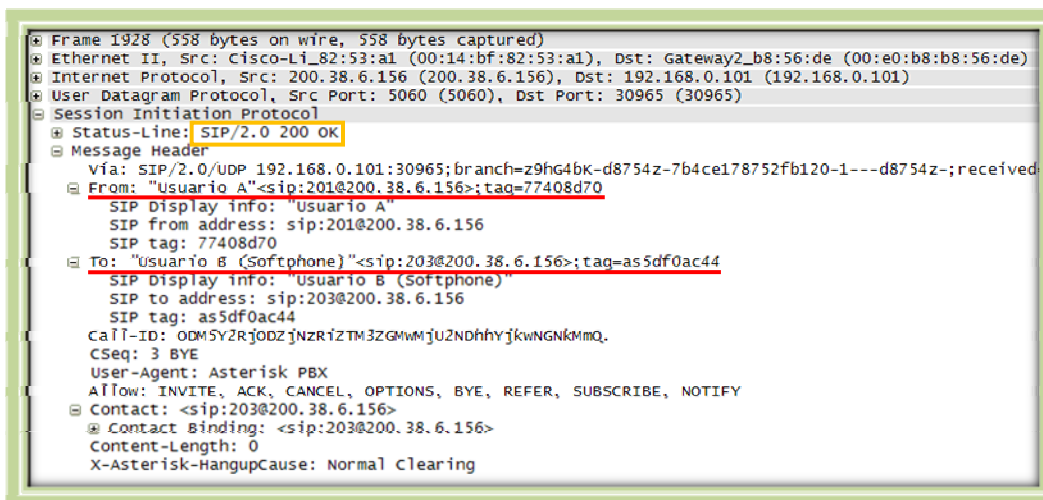


```

* Frame 1927 (686 bytes on wire, 686 bytes captured)
* Ethernet II, Src: Gateway2_b8:56:de (00:e0:b8:b8:56:de), Dst: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1)
* Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 200.38.6.156 (200.38.6.156)
* User Datagram Protocol, Src Port: 30965 (30965), Dst Port: 5060 (5060)
* Session Initiation Protocol
  * Request-Line: BYE sip:203@200.38.6.156 SIP/2.0
  * Message Header
    vfa: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hG4bK-d8754z-7b4ce178752fb120-1---d8754z-;rport
    Max-Forwards: 70
    * Contact: <sip:201@200.38.6.129:30965>
    * Contact Binding: <sip:201@200.38.6.129:30965>
    * To: "Usuario B (Softphone)"<sip:203@200.38.6.156>;tag=as5df0ac44
      SIP Display info: "Usuario B (Softphone)"
      SIP to address: sip:203@200.38.6.156
      SIP tag: as5df0ac44
    * From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
      SIP Display info: "Usuario A"
      SIP from address: sip:201@200.38.6.156
      SIP tag: 77408d70
    Call-ID: ODM5Y2RjODZjNzRiZTM3ZGMwMjU2NDhhYjkwNGNkMmMq.
    CSeq: 3 BYE
    * Proxy-authorization: Digest username="201",realm="asterisk",nonce="2a746a86",uri="sip:203@200.38.6.156"
      Authentication Scheme: Digest
      Username: "201"
      Realm: "asterisk"
      Nonce value: "2a746a86"
      Authentication URI: "sip:203@200.38.6.156"
      Digest Authentication Response: "02803id535ded7a8f6673357196bdac8"
      Algorithm: MD5
      User-Agent: X-Lite release 11001 stamp 47546
      Reason: SIP;description="User Hung Up"
      Content-Length: 0

```

Figura 5. 25 Mensaje fin (*bye*) para finalizar la llamada.



```

* Frame 1928 (558 bytes on wire, 558 bytes captured)
* Ethernet II, Src: Cisco-Li_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
* Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
* User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
* Session Initiation Protocol
  * Status-Line: SIP/2.0 200 OK
  * Message Header
    vfa: SIP/2.0/UDP 192.168.0.101:30965;branch=z9hG4bK-d8754z-7b4ce178752fb120-1---d8754z-;received
    * From: "Usuario A"<sip:201@200.38.6.156>;tag=77408d70
      SIP Display info: "Usuario A"
      SIP from address: sip:201@200.38.6.156
      SIP tag: 77408d70
    * To: "Usuario B (Softphone)"<sip:203@200.38.6.156>;tag=as5df0ac44
      SIP Display info: "Usuario B (Softphone)"
      SIP to address: sip:203@200.38.6.156
      SIP tag: as5df0ac44
    Call-ID: ODM5Y2RjODZjNzRiZTM3ZGMwMjU2NDhhYjkwNGNkMmMq.
    CSeq: 3 BYE
    User-Agent: Asterisk PBX
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
    * Contact: <sip:203@200.38.6.156>
    * Contact Binding: <sip:203@200.38.6.156>
    Content-Length: 0
    X-Asterisk-HangupCause: Normal Clearing

```

Figura 5. 26 Mensaje de aceptación '200 OK'.

En las figuras anteriores se ve reflejado los campos de cada protocolo, sirven para cumplir con la meta de una transmisión que es llegar al destino indicado. En la figura 5.26 se señala los protocolos que interviene dentro de la conversación, cabe señalar que hay varios protocolos que también colaboran, pero este trabajo se limitó al uso de los más relevantes.

Lo señalado en el rectángulo azul es la información que contiene cada trama y es enviada al receptor, el lenguaje es de tipo hexadecimal.

5. IMPLEMENTACION EXPERIMENTAL

The image shows a Wireshark packet capture of a SIP message. The packet structure is as follows:

- Frame 1928 (558 bytes on wire, 558 bytes captured)
- Ethernet II, Src: Cisco-L1_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
- Destination: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
- Source: Cisco-L1_82:53:a1 (00:14:bf:82:53:a1)
- Type: IP (0x0800)
- Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x68 (DSCP 0x1a: Assured Forwarding 31; ECN: 0x00)
- Total Length: 544
- Identification: 0x6927 (26919)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 62
- Protocol: UDP (0x011)
- Header checksum: 0x816e [correct]
- Source: 200.38.6.156 (200.38.6.156)
- Destination: 192.168.0.101 (192.168.0.101)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
- Source port: 5060 (5060)
- Destination port: 30965 (30965)
- Length: 524
- Checksum: 0xd29d [correct]
- Session Initiation Protocol
- Status-Line: SIP/2.0 200 OK
- Message Header

The hex dump at the bottom shows the raw data of the packet, with the SIP message body (SDP) starting at offset 0000.

Figura 5. 27 Protocolos que intervienen en la transmisión empleando SIP.

Dentro del protocolo SIP, se encapsula el protocolo SDP como se muestra en la figura 5.27, con todos los campos que el protocolo utiliza para comunicar a los usuarios las características de cada uno de ellos, incluso los parámetros de RTP para la negociación del esquema de compresión a utilizar.

The image shows a Wireshark packet capture of the SDP message body. The fields are as follows:

- Frame 53 (791 bytes on wire, 791 bytes captured)
- Ethernet II, Src: Cisco-L1_82:53:a1 (00:14:bf:82:53:a1), Dst: Gateway2_b8:56:de (00:e0:b8:b8:56:de)
- Internet Protocol, Src: 200.38.6.156 (200.38.6.156), Dst: 192.168.0.101 (192.168.0.101)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 30965 (30965)
- Session Initiation Protocol
- Status-Line: SIP/2.0 200 OK
- Message Header
- Message body
- Session Description Protocol
- Session-Description-Protocol-Version (v): 0
- Owner/Creator, Session-Id (o): root 3401 3401 IN IP4 200.38.6.156
- Session-Name (s): session
- Connection-Information (c): IN IP4 200.38.6.156
- Time-Description, active-time (t): 0 0
- Media-Description, name-and-address (m): audio 19056 RTP/AVP 0 8 101
- Media-Attribute (a): rtpmap:0 PCMU/8000
- Media-Attribute (a): rtpmap:8 PCMA/8000
- Media-Attribute (a): rtpmap:101 telephone-event/8000
- Media-Attribute (a): fmtp:101 0-16
- Media-Attribute (a): silenceSupp:off - - - -

Figura 5. 28 Campos del Protocolo SDP.

5. IMPLEMENTACION EXPERIMENTAL

Se implementó un sistema experimental de voz sobre IP mediante la instalación de un servidor en una red de topología estrella, un usuario que tenga registrado una extensión puede entablar una conversación en la red local. También se logró que ese mismo usuario tuviera servicio fuera de la red local. Posteriormente, se obtuvieron resultados satisfactorios al analizar los paquetes de voz sobre IP con un software de nombre “Ethereal”, se compararon los resultados del capítulo 4 “Análisis de los protocolos empleados en VoIP” en las figuras 4.13 y 4.14 de la sección 4.6 “Comportamiento de SIP”, que muestran el los mensajes de inicio y fin de una sesión. El software arrojó un diagrama muy similar en la figura 5.18 de la sección 5.4 “Análisis del tráfico de Voz en Tiempo Real”, donde se observa los mensajes que se transmiten durante una conversación. Esta llamada se realizó en la plataforma experimental con dos usuarios SIP que conversaron durante un par de minutos.

Lo anterior demuestra que la investigación teóricamente fue de gran utilidad puesto que ya en la práctica es importante tener un conocimiento del proceso de comunicación para entender cómo y por qué son necesarios tantos mensajes para el inicio de una conversación telefónica VoIP, también resaltar que no es más importante un protocolo que otro dentro de este proceso, cada uno tiene su función y todos están relacionados de tal forma que sin uno de ellos esto no puede llevarse a cabo (es posible realizarlo bajo otros protocolos, pero sería otro tipo de aplicación).

CAPÍTULO 6

CONCLUSIONES

Para entender como inicia la señalización entre dos usuarios que desean mantener una comunicación de voz sobre Internet, se optó por realizar un análisis del comportamiento del Protocolo de Inicio de Sesión (SIP) que desempeña dicha función, de acuerdo a esto se obtuvo el esquema del inicio, modificación y terminación de una conversación.

Dentro de la telefonía de Voz sobre IP (VoIP) se utilizan protocolos en el proceso de comunicación que trabajan en conjunto con SIP, los cuales son: Protocolo de Descripción de Sesión (SDP), Protocolo de Transporte en Tiempo Real (RTP), Protocolo de Datagrama de Usuario (UDP), Protocolo de Internet (IP) y Ethernet. Cada uno de ellos proporciona un mecanismo que colabora en la transmisión de voz siendo primordial que esto se realice en tiempo real y con un servicio de calidad aceptable.

Después de la investigación teórica, se implementó un sistema experimental de voz sobre IP en una topología de red local, ubicada en las instalaciones de CITEDI con los elementos siguientes: un servidor tipo softswitch, dos computadoras, un hub y acceso a internet. El servidor fue configurado con un software de nombre TrixBox que permite gestionar el sistema, crear, modificar y eliminar extensiones telefónicas y generar reportes estadísticos; además se utilizó un software tipo 'softphone' que se instaló en cada computadora. Para las pruebas se realizaron más de 100 llamadas entre dos usuarios SIP dentro de la red local, obteniendo un 25% de llamadas exitosas y un 75 % de llamadas fallidas, esto se debe a que se iniciaba con el proceso de depuración de errores entre el servidor y las terminales. Cuando la red fue enlazada al exterior se realizaron 778 de las cuales 99% fueron exitosas y el 1% no lo fue. Ya que se obtuvieron

6. CONCLUSIONES

resultados satisfactorios; se realizó el estudio de los paquetes en una llamada de Voz sobre IP mediante el empleo de un software analizador, con el cual se pudo comprobar que la explicación teórica proporcionada en el capítulo “Análisis” coincide con los resultados experimentales obtenidos.

Habiendo hecho un análisis exhaustivo de los protocolos que intervienen en el proceso de comunicación de voz sobre IP, se realiza una plataforma con hardware y software a pequeña escala, tipo “*call center*” con recursos mínimos y excelentes resultados. Esto aporta otra alternativa para la telefonía en pequeños negocios y hogares puesto que el costo por instalación es poco a comparación de las ya utilizadas.

No se pretende dejar a un lado la telefonía tradicional puesto que tiene más de 100 años brindando servicio, pero es un hecho que la telefonía de voz sobre IP está en el mercado y ha evolucionado a pasos agigantados ofreciendo un servicio de calidad muy parecido a la telefonía tradicional.

Como trabajo a futuro se plantea la creación de una función que disminuya el tiempo de negociación en una conversación SIP, lo cual significa menos envío de mensajes para completar una transacción. Otra alternativa sería realizar la conexión de la red local con red PSTN, de modo que se puedan generar llamadas de largas distancias o a celulares. Asimismo, continuar con el estudio de los protocolos que intervienen dentro de la comunicación VoIP, para optimizar la transmisión dentro de Internet y eliminar factores que puedan distorsionar la voz.

REFERENCIAS

- [1] Éxito Exportador [en línea], Diciembre 2008.
Disponible en <www.exitoexportador.com/stats.htm>

- [2] Instituto Nacional de Estadística y Geografía, INEGI [en línea], Diciembre 2008.
Disponible en <www.inegi.gob.mx>

- [3] Informe de Investigación de “Point Topic” [en línea], Diciembre 2008
Disponible en <www.vnunet.es/Actualidad/Noticias/Inform%C3%A1tica_profesional/Infomercado/20050711008>

- [4] B. Leader, “World VoIP Market: Telephony services’ wide transformation”; IDATE, Mayo 2006.

- [5] A. IRVINE, “IP Voice: Ventajas y opciones de implantación”; COLT Telecom Group. 2005.

- [6] J. Davidson, J. Peters, M. Bhatia, “Voice over IP Fundamentals”; Cisco Press, 2da Edición, pp. 21-317, Julio 2006.

- [7] J. Postel, “Protocolo de Internet (IP)”; RFC 791 IETF, Septiembre 1981.

- [8] W. Stalling, “Redes de Internet de Alta Velocidad”; Pearson Prentice Hall, 2da. pp. 38-60 Edición, Madrid, 2004 .

REFERENCIAS

- [9] Escudero-Pascual, L. Berthilson, “VoIP para el desarrollo”; Creative Commons, Diciembre 2006.
- [10] B. A. Forouzan, “Transmisión de datos y redes de comunicación”; McGrawHill 2da Edición, pp. 116-120, 658-662, 776-779, Madrid España, 2006.
- [11] R. Rodríguez, “Metodología para una red VoIP de alto tráfico y QoS”, Tesis M.C., CITEDI, Tijuana, B.C., México., 2006.
- [12] ITU, Unión Internacional de Telecomunicaciones [en línea], 2007-2008.
Disponible en <www.itu.int>
- [13] CISCO System, “Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation”, Febrero 2005.
- [14] J. M. Huidobro, “Tecnología VoIP y Telefonía IP”, Alfaomega, pp. 71-88, Julio 2006, México.
- [15] L. Peterson, B. Davie, “Computer Networks”; Morgan Kaufmann 3ra. Edición, 2003, EUA.
- [16] The Internet Engineering Task Force IETF [en línea] 2008.
Disponible en <www.ietf.org>.
- [17] J. Rosenberg, “Session Initiation Protocol”; RFC 2543 IETF, Marzo 1999.
- [18] J. Rosenberg, H. Schulzrinne, G. Camarillo, “Session Initiation Protocol”; RFC 3261 IETF, Junio 2002.
- [19] T. Berners-Lee, R. Fielding, L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax”; RFC 3986 IETF, Enero 2005.

REFERENCIAS

- [20] S. Donovan, J. Rosenberg, “Session Timers in the Session Initiation Protocol”; RFC 4028 IETF, Abril 2005.
- [21] J. Almaraz, G. Vazquez, C. Villanueva, Tesis: “Aplicación de Voz sobre IP para un caso de Telefonía Pública”; Ing. Tesis, UNAM, México, 2006.
- [22] A. Johnston, “Undertanding the Session Initiation Protocol”; Arech House, 2da Edition, EUA 2004.
- [23] M. Handley V. Jacobson, “Session Description Protocol”; RFC 2327 IETF, Abril 1998.
- [24] M. Handley V. Jacobson, C. Perkins, “Session Description Protocol”; RFC IETF 4566, Julio 2006.
- [25] W. Stallings “Data and Computer Communications”, Prentice Hall, 8va. Edicion, New Jersey, US 2007.
- [26] C. Huitema, “Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)”; RFC 3605 IETF, Octubre 2003.
- [27] J. Postel, “User Datagram Protocol”; RFC 768 IETF, Agosto 1980.
- [28] G. Álvarez, M. Sánchez, M. A. Álvarez, “Señalización de Voz sobre IP aplicando el protocolo SIP”, V Congreso Internacional de Ingeniería Electromecánica y Sistemas CIIES, Distrito Federeal, 2008.
- [29] D. Garrison, “TrixBos, Made Easy”, PACKT. B; EUA, Septiembre 2006.
- [30] TrixBos [en linea], 2007-2008.
Disponibile en <www.trixbox.org/>

REFERENCIAS

- [31] A. S Yance, “TrixBos al descubierto”, GECKO EU, GECKO NETWORK, Colombia, 2006.

- [32] Conterpath [en linea], 2007-2008.
Disponible en <www.counterpath.com>

- [33] Counter Path Solutions, Inc. “X-Lite, User Guide”, Canada, 2006.

- [34] Referencia de internet para los softphone [en linea], 2008.
Disponible en < <http://www.clickfornick.com/freephone/2008/12/softphones-best-voip-phones-for-free-voip.html>>

- [35] SJPhone, “Guia Rapida de Configuracion”, Madrid.

- [36] G. Álvarez, M. Sánchez, M. Álvarez, “Análisis e implementación de un sistema experimental de Voz sobre IP empleando el Protocolo SIP”; ELECTRO08, Chihuahua Chihuahua, México.

- [37] G. Álvarez, M. Sánchez, M. Álvarez, “Análisis de la ruta de un mensaje de Voz sobre IP”; ERA08 Tijuana BC, México.

A

APÉNDICE

El Protocolo de Inicio de Sesión (SIP) en la estructura de sus formatos tanto de peticiones como de respuestas, contiene palabras reservadas para el establecimiento de una sesión, que se ubican en los campos del formato y señalan actividades o parámetros. A continuación se presenta las que hasta hoy se encuentran descritas en la literatura.

Métodos del Protocolo SIP

100 *Trying*

Indica únicamente que algún tipo de acción no específica se está llevando a cabo para procesar la llamada, sin indicar si el usuario ha sido localizado.

180 *Ringin*

Esta respuesta se usa para indicar que la transacción de invitación (invite) ha sido recibido por el Agente de Usuario y que el teléfono está sonando. A partir de esa respuesta el agente usuario cliente generara su propio tono de llamada, salvo que se reciba otra indicación.

181 *Call is being forwarded*

Se usa para indicar que la llamada está siendo desviada a otra terminal, se envía cuando esta información puede ser utilizada por el llamante.

182 *Call queued*

Indica que una transacción de invitación (invite) se ha recibido y que se procesará en una fila.

183 *Session Progress*

La respuesta se utiliza para transportar información del progreso de la llamada que no está clasificada de otra manera. Puede estar presente en el texto asociado a la respuesta, en los campos de cabecera o en el flujo de información. Cuando un Agente Usuario Cliente reciba esta respuesta, el terminal no genera tono local, tanto si lleva el cuerpo del Protocolo de Descripción de Sesión (SDP) o no lo lleva.

200 *OK*

Esta respuesta tiene dos usos en SIP: el primero es para aceptar una invitación de sesión y contendrá un cuerpo de mensaje con las propiedades del medio del usuario, el segundo es una respuesta a otras peticiones, indicando que la petición se ha recibido con éxito.

200 *Accepted*

Esta respuesta indica que el Agente Usuario Servidor ha recibido y aceptado la petición, pero la petición puede o no haber sido autorizada o procesada por el servidor.

300 *Múltiple Choices*

Esta respuesta de redirección contiene múltiples direcciones de contacto (campo *Content*), los cuales indican que el servicio de localización ha devuelto diferentes localizaciones posibles para la petición SIP.

301 *Moved Permanently*

Contiene un campo en el encabezado de nombre *Contact*, indica la nueva dirección URI de la parte llamada. El cliente que realiza la petición deberá actualizar su lista de direcciones con la nueva dirección para tenerla en cuneta en las siguientes peticiones.

302 *Moved Temporarily*

La dirección URI incluida en esta respuesta tiene una validez temporal, por el tiempo indicado en el parámetro *expires* del campo *Contact*, y puede ser guardada en el Servidor Proxy para posteriores transacciones durante el tiempo indicado. En caso de que no se indique explícitamente la duración de la validez de la dirección solo será utilizada en el momento sin ser guardada.

305 *Use Proxy*

Contiene la dirección URI que apunta a un Servidor Proxy que tiene información autorizada sobre la parte llamante, es decir, al recurso requerido debe accederse a través del Servidor Proxy. La dirección del Proxy vendrá en el campo *Contact* de la respuesta y será a la que el cliente dirija de nuevo la petición.

380 *Alternative service*

Se producen en situaciones en las que no se ha podido completar la llamada pero existen servicios alternativos, como: el desvío a un buzón de voz. Esta respuesta devuelve una dirección URI en función del tipo de servicio activado por la parte llamada.

400 *Bad Request*

Esta respuesta indica que la petición no la ha entendido el servidor por un error de sintaxis.

401 *Unauthorized*

Indica que la petición requiere llevar a cabo el procedimiento de autenticación.

402 *Payment Required*

Esta respuesta se mantiene para uso futuro.

403 *Forbidden*

Se utiliza para denegar una petición sin dar opción al llamante, en este caso el servidor ha entendido la petición y está correctamente formulada pero no atenderá la petición.

404 *Not Found*

Esta respuesta se proporciona cuando el servidor tiene seguridad de que el usuario identificado por la dirección URI no existe en el dominio especificado en el Request-URI. También se envía si el dominio no es ninguno de los dominios manejados por el receptor de la petición.

405 *Method Not Allowed*

En este caso el método especificado en el Request-Line ha sido comprendido correctamente por el servidor pero no está permitido su uso para la dirección identificada en el Request-URI.

406 *Not Acceptable*

El recurso identificado por la petición es únicamente capaz de responder con características de contenido no aceptables según el campo del encabezado *Accept* incluido en la petición.

407 *Proxy Authentication Required*

Esta respuesta se envía desde un Servidor Proxy para indicar al Agente Usuario Cliente que debe primero autenticarse antes de que la petición pueda ser procesada.

408 *Request Timeout*

Se enviará cuando el servidor de la petición no genere una respuesta a dicha petición en el tiempo adecuado.

410 *Gone*

Es similar a la respuesta 404 pero proporciona la pista de que el usuario requerido no estará disponible en su posición en el futuro. El servidor utilizará esta respuesta cuando tenga la seguridad de que se trata de una condición permanente, en caso de que no exista tal seguridad deberá emplear la respuesta 404.

412 *Conditional Request Failed*

La utiliza el ESC (compositor del estado de eventos) si en una petición *Publish* de actualización, modificación o borrado, el estado de evento al que se refiere ha expirado.

413 *Request Entity Too Large*

Será utilizado por un servidor para rechazar una petición recibida con un cuerpo de mensaje mas largo de lo que es capaz de procesar.

414 *Request-URI Too Long*

Esta respuesta indica que el Request URI de la petición es demasiado largo y no puede ser procesado correctamente.

415 *Unsupported Media Type*

Esta respuesta es enviada desde un Agente de Usuario para indicar que el tipo de medio contenido en la petición no se soporta.

416 *Unsupported URI Scheme*

Se utiliza cuando un Agente Usuario Cliente usa un esquema URI en un *Request-URI* que el Agente Usuario Servidor no entiende.

420 *Bad Extension*

Indica que la extensión especificada en el campo del encabezado *Require* no se soporta en el Agente Usuario o Servidor Proxy, según sea el caso.

421 *Extension required*

Esta respuesta indica que un servidor necesita una extensión que no está presente en el campo del encabezado *Supported* de una petición para el correcto procesamiento de la misma.

422 *Session Timer Interval Too Small*

Se usa para rechazar una petición que contiene en el encabezado un campo de nombre Session-Expires con un intervalo de tiempo demasiado corto. El intervalo de tiempo mínimo permitido es el indicado en el campo *Min-SE* del encabezado.

423 *Interval Too Brief*

El servidor de Registro la utiliza en caso de rechazar una petición debido a que el tiempo en el que expira uno o más contactos es demasiado corto.

429 *Provide Referrer Identity*

Se usa para pedir que en el campo *Referred-By* sea reenviado con seguridad.

480 *Temporarily Unvaible*

Sirve para indicar que la petición ha alcanzado el destino correcto pero el receptor no está disponible por alguna razón (por ejemplo, tiene activado el servicio “ocupado”). El texto asociado dará información más detallada de la causa por la que no está disponible.

481 *Dialog/Transaction Does Not Exist*

Indica que el Agente Usuario Servidor ha recibido una petición para la cual no encuentra una transacción o dialogo existente.

482 *Loop Detected*

Indica que la petición ha entrado en un ciclo, ya que ha sido devuelta a un Servidor Proxy que previamente transfirió la petición.

483 *Too Many Hops*

Señala que la petición ha sido desviada a un número de veces que supera el máximo permitido. El servidor que manda esta respuesta ha recibido en la petición el campo Max Forwards en digito cero.

484 *Address Incomplete*

Indica que el servidor ha recibido en el *Request-URI* de la petición una dirección incompleta.

485 *Ambiguous*

Señala que el *Request-URI* de la petición es ambiguo y debe clasificarse para poder ser procesado.

486 *Busy Here*

Se usa para mostrar que, aunque se ha alcanzado correctamente al receptor, el Agente Usuario no puede aceptar la llamada en la posición cuya dirección se identifica en el *Request-URI*.

487 *Request Terminated*

Se envía como respuesta a un *Bye* o *Cancel*.

488 *Not Acceptable Here*

Indica que el Agente Usuario fue contactado correctamente pero que algunos aspectos descritos en la sesión, tales como medios o ancho de banda o esquema de codificación no son aceptables.

489 *Bad event*

Se usa para rechazar una petición de suscripción o de notificación que contiene un paquete de eventos desconocido o no soportado por el Agente Usuario Servidor. También se usará para rechazar peticiones de suscripciones que no especifican un paquete de evento en la encabezado *Event*.

491 *Request Pending*

Se usa para resolver posibles *Re-Invites* simultáneos realizados por ambas partes del dialogo.

493 *Request Undecipherable*

Esta respuesta es usada por el Agente Usuario Servidor cuando no puede descifrar el cuerpo del mensaje *S/MIME* al no disponer este de la clave pública.

500 *Server Internal Error*

Se envía cuando el Servidor se ha encontrado con un fallo inesperado que no le permite procesar la petición. Se trata de fallos temporales, por tanto el cliente puede hacer un nuevo intento transcurrido algún lapso de tiempo.

501 *Not Implemented*

Indica que el servidor no es capaz de procesar la petición, esta respuesta es apropiada cuando el Agente Usuario Servidor no reconoce el método requerido. La diferencia con la respuesta 405 es que el servidor si reconoce el método pero no es soportado o no está permitido.

502 *Bad Gateway*

Esta respuesta se envía desde un Servidor Proxy que está actuando como *gateway* de otro red e indica que existe algún problema en la otra red que impide procesar la petición.

503 *Service Unavailable*

Indica que el servidor requerido no está disponible temporalmente por congestión o actuaciones de mantenimiento del servidor.

504 *Server Timeout*

Esta respuesta indica que la petición ha fallado debido un vencimiento de la temporización que se ha producido en el Servidor o en la otra red con la que se interconecta el *gateway*.

505 *Versión Not Supported*

Señala que el servidor ha rechazado la petición debido a la versión SIP empleada en la petición.

513 *Message Too large*

Es usada por el Agente Usuario Servidor para indicar que el tamaño de la petición es demasiado grande para ser procesado.

600 *Busy Everywhere*

Esta respuesta es la versión definitiva de la respuesta 486, es decir, tiene el mismo significado pero referido no solo a una dirección sino a cualquier posible dirección del usuario identificado en el *Request-URI*.

603 *Decline*

Es similar a la 600 pero sin dar información del estado de la llamada, simplemente indica que no acepta la llamada.

604 *Does Not Exist Anywhere*

Parecida a la 404 pero el servidor tiene información autorizada para indicar que el usuario identificado no puede ser localizado en ninguna dirección.

606 *Not Acceptable*

Esta respuesta se podrá usar para implementar alguna capacidad de negociación de sesión en SIP. Sirve para indicar que algún aspecto de la sesión requerida no es aceptable por el Agente Usuario Servidor (medio requerido, ancho de banda, esquemas de codificación) y en consecuencia no se puede establecer la sesión.

Contenidos en métodos y respuestas.

Accept

Se usa para indicar tipos de medios aceptables para los cuerpos de mensaje, por parte del Cliente (si se envía en una petición) o del Servidor (si se envía en una respuesta).

Accept-Language

Se usa en las peticiones para indicar los lenguajes preferidos para frases, descripción de sesiones o estado de respuestas, que se incluyan como cuerpo de mensaje en la respuesta.

Alert-Info

Este campo se usa para proporcionar un “tono distintivo”.

Allow

Proporciona una lista con el conjunto de métodos soportados por el Agente Usuario que genera el mensaje.

Allow-Events

Incluye la lista de los paquetes de eventos que soportan el Agente Usuario Cliente (si se envía una petición) o el Agente Usuario Servidor (si aparece en una respuesta).

Call-Id

Actúa como identificador de una petición o de su pertenencia a una dialogo, la respuesta copia el valor de la petición.

Contact

Proporciona uno o varios URI para identificar y facilitar el acceso o contacto con el recurso origen o destino de la petición (dependiendo de si aparece en una petición o en una respuesta). Puede incluir parámetros que describen determinados rasgos o características que contienen la capacidad del dispositivo identificado por el *URI-Contact*.

Cseq

Sirve para ordenar las transacciones dentro de un dialogo, proporciona un medio de identificarlas unívocamente y diferenciar entre métodos nuevo y retransmitidos.

Date

Indica la fecha y hora en que la petición o respuesta se envía por primera vez.

Diversión

Se usa en casos de desvíos de llamada para indicar al llamado quien o quienes han realizado desvíos y porque motivo.

Expires

Proporciona el tiempo relativo tras el cual el mensaje o contenido expira.

From

Indica al usuario que origina la petición.

Min-SE

Indica el valor mínimo, en segundos que puede darse al intervalo de tiempo de expiración de la sesión.

Organization

Se usa para indicar la organización a la que pertenece el que origina el mensaje.

P-Access-Network-Info

Contiene información sobre la red de acceso que el Agente Usuario está utilizando.

P-Asserted-Identity

Transporta entre Proxies de un dominio seguro la identidad de un usuario certificado mediante el proceso de autenticación.

P-Charging-Function-Addresses

Contiene los nombres de los *host* o las direcciones IP de los nodos que reciben la información de facturación.

P-Charging-Vector

Proporciona información para poder correlacionar los registros de tarificación generados por cada una de las entidades de red involucradas en una misma sesión.

P-Preferred-identity

Lo usa un Agente Usuario para comunicar a un Servidor Proxy que identidad prefiere que use en el campo *P-Asserted-Identity* del conjunto de identidades asociadas al Agente Usuario.

Path

Aporta una relación de Servidores Proxies que la petición *Register* recorre entre el Agente Usuario Cliente (origen) y el Servidor (destino)

Privacy

Se utiliza para ocultar información de usuario a efectos de mantener su privacidad, cuando esta transacción debe llevarla a cabo un elemento intermedio de la red, dado que, en general se trata de información que el usuario no puede ocultar por sí mismo.

Reason

Indica la razón por la que la sesión o llamada se termina.

Record-Route

Se usa para forzar el enrutamiento a través de un Servidor Proxy para todas las peticiones enviadas dentro de un dialogo que se establezca entre dos Agentes de Usuario.

Reply-To

Se usa para indicar el SIP o SIP's URI que debería usarse en contestaciones a esa petición, por ejemplo en casos de devolución de llamadas perdidas o sesiones no establecidas y que pueden ser de contenido distinto en el campo *From*.

Require

Este campo enumera las características y extensiones que un Agente Usuario Cliente necesita que soporte un Agente Usuario Servidor para procesar la petición.

Session-Expires

Se usa para indicar el tiempo de expiración de la sesión en segundos.

Supported

Enumera todas las extensiones soportadas por el Agente Usuario Cliente o el Agente Usuario Servidor.

Timestamp

Indica el tiempo exacto en que el Agente Usuario Cliente envía la petición al Agente Usuario Servidor.

To

Indica el receptor lógico de la petición o la dirección pública del usuario o recurso destino de esa petición, puede ser o no el último receptor de la misma.

User-Agent

Contiene información sobre el Agente Usuario que origina la petición (información sobre el fabricante, versión software)

Vía

Indica el transporte usado para la transmisión e identifica la localización donde la respuesta al método va a ser enviada. Puede llevar parámetros como: *comp* y *rport*.

Contenido solo en respuestas.

Authentication-Info

Un Servidor puede incluir este campo en una respuesta exitosa (2XY) generada para una petición que se ha autenticado satisfactoriamente.

Error-Info

Proporciona un puntero hacia una dirección URI que aporte información adicional sobre el estado de error de la respuesta.

Min-Expires

Comunica el mínimo intervalo de actualización en registros, suscripciones, publicaciones manejados por el servidor.

P-Associated-URI

Indica un conjunto de URI's relacionadas con una dirección registrada.

Proxy-Authenticate

Incluye información para que el cliente pueda enviar de nuevo la petición con una acreditación correcta, en caso de que la autenticación la realice un Servidor Proxy.

Proxy-Authentication-Info

Su sintaxis y significado son análogos a los indicados para el campo *Authentication-Info*.

Retry-After

Indica cuando un recurso o servicio puede estar disponible de nuevo.

Rseq

Se utiliza para indicar la secuencia de todas las respuestas provisionales fiables enviadas para una petición,

Server

Contiene información acerca del software usado por el Agente Usuario Servidor para manejar la petición.

Service-Route

La incluye un método *registrar* en la respuesta 200 *OK* al método *Register* indicando una secuencia de Servidores Proxies, dicha secuencia es la que seguirán las peticiones iniciales originadas en el Agente Usuario Cliente cuya dirección está registrada. Para ello, el Agente Usuario Cliente construirá una ruta (*Route*) para futuras peticiones, con el valor del campo *Service-Route* recibida.

SIP-Etag

Este campo es obligatorio en las respuestas exitosas (2XY) enviada para la petición *Publish* por el ESC (compositor del estado de los eventos). La genera este último y contiene un identificador asociado al evento publicado (*entity-tag*).

Unsupported

Lista las características no soportadas por el Agente Usuario Servidor.

Warning

Se usa para proporcionar información adicional sobre el estado de una respuesta.

WWW-Authenticate

Este campo incluye información para que el cliente pueda enviar de nuevo la petición con una acreditación correcta, en caso de que la autenticación la realice un Agente Usuario.

Contenidos solo en métodos.

Accept-Contact

Forma parte de las extensiones de SIP, que permite al usuario que envía la petición establecer preferencias que controlan de algún modo el proceso de la misma por parte de los Servidor Proxy. En concreto, indica un conjunto de rasgos o características correspondientes al Agente Usuario Servidor que se quiere alcanzar.

Authorization

Contiene la acreditación del cliente (incluyendo usuario y contraseña) a efectos de autenticación.

Event

Indica que paquete de eventos está utilizando la petición.

In-Reply-To

Se utiliza en caso de devolución de llamadas perdidas o sesiones no establecidas y enumera los campos *Call-Id* de las llamadas perdidas.

Join

Se usa en una transacción de invitación (*invite*) que solicita la incorporación de un nuevo participante a un dialogo existente.

Max-Forwards

Sirve para limitar el número de saltos de un método.

P-Called-Party-Id

Este campo lo introduce un Servidor Proxy con el valor de la dirección lógica de un usuario registrado, (presente en un *Request-URI*), antes de sustituir este último con la dirección que va a utilizar para encaminar la petición al usuario. De este modo, se asegura que el destino reciba la dirección lógica correspondiente a la petición.

Priority

Señal la urgencia de la petición tal como la percibe el cliente, describiendo la prioridad que la petición debería tener para el usuario o su agente.

Proxy-Authorization

Contiene la acreditación del cliente (incluyendo usuario y contraseña) a efectos de autenticación.

Proxy-Require

Se usa para indicar las características que un Agente Usuario necesita que soporte el Servidor Proxy.

Rack

Se envía en un método *Prack* para soportar la fiabilidad de las respuestas provisionales y sirve para poder relacionar dicho método con la respuesta que acepta.

Refer-To

Solo aparece en el método *Refer* como campo obligatorio, indica el recurso que está siendo referenciado en el método y por lo tanto con el que el receptor debería contactar.

Referent-By

Contiene información sobre el emisor del *Refer*, que debe llegar al receptor de la nueva petición generada como resultado del proceso.

Reject-Contact

Permite al usuario que envíe la petición “establecer preferencias” que controlan de algún modo el proceso de la misma, por parte de los Servidores Proxy, es decir permite al Agente Usuario Cliente especificar al Servidor Proxy que no contacte con un URU cuyas características indicadas explícitamente en el campo *Contact* concuerden con cualquiera de los valores de este campo.

Replaces

Se utiliza para reemplazar a un participante por otro en un dialogo existente, contiene información necesaria para poder identificar dicho dialogo.

Request-Disposition

Permite al usuario que envía la petición establecer preferencias que controlan de algún modo el proceso de la misma por parte de los Servidores Proxy, dicho de otro modo, proporciona una lista de directivas que el Servidor Proxy debería cumplir.

Route

Se usa para proporcionar información de encaminamiento y consta de una lista de URI's a las que, en general se progresara la petición hasta alcanzar el destino.

SIP-If-Match

Solo aparece en el método *Publish*, la introduce el Agente Usuario que enviar dicho método, como actualización de una publicación realizada con anterioridad. Su valor debe de coincidir con

el del identificador del campo *SIP-ETag* recibida de la respuesta 2XY al *Publish* correspondiente a la publicación inicial.

Subject

Indica el asunto de la sesión, permitiendo filtrados sin tener que analizar la descripción de sesión.

Subscription-State

Indica el estado de la suscripción.

Campos del encabezado del cuerpo de los mensajes.

Content-Disposition

Indica como debe un Agente Usuario interpretar el cuerpo del mensaje.

Content-Encoding

Indica que se ha aplicado una codificación al cuerpo de mensaje y por lo tanto deben utilizarse decodificadores para obtener el tipo de medio referenciado en el campo *Content-Type*.

Content-Language

Se usa para indicar el lenguaje del cuerpo del mensaje.

Content-Length

Indica el número de octetos del cuerpo del mensaje, no se incluyen en este computo lo que separan los campos del encabezado.

Content-Type

Indica el tipo de medio del cuerpo de mensaje (tipo/subtipo).

Mime Versión

Proporciona la versión del protocolo MIME utilizada en el cuerpo de mensaje.