UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Implementación de Servicios de Voz sobre el Protocolo de Internet bajo los Protocolos SIP y H.323

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE
Ingeniero en Redes

PRESENTA
Br. Edwin José López Canul

SUPERVISORES

Dr. Homero Toral Cruz

Dr. Freddy Ignacio Chan Puc

M.C. Francisco Méndez Martínez

CHETUMAL QUINTANA ROO, MÉXICO, DICIEMBRE DE 2016

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

Comité de Trabajo Monográfico

SUPERVISOR:

Dr. Homero Toral Cruz

SUPERVISOR:

Dr. Freddy Ignacio Chan Puc

SUPERVISOR:

M.C. Francisco Méndez Martínez

CHETUMAL QUINTANA ROO, MÉXICO, DICIEMBRE DE 2016

Resumen

La voz sobre el protocolo de Internet (VoIP) es una de las tecnologías más populares e innovadoras que está comenzando a abrirse paso a través de muchos ámbitos, tales como: sociales, comerciales, tecnológicos, académicos, investigación, etc.

Se trata de una tecnología de menor costo de tarificación en comparación con la telefonía convencional, debido a que utiliza Internet en lugar de la red tradicional de conmutación por circuitos para transportar la información.

Internet es una de las redes más importantes en el área de las telecomunicaciones y últimamente ha evolucionado a un ritmo muy acelerado; a tal grado de convertirse en la red convergente, sobre la cual, múltiples aplicaciones transmiten información de diversas naturalezas. Sin embargo, Internet ofrece un servicio de mejor esfuerzo y no garantiza calidad de servicio y la voz sobre el protocolo de Internet es una tecnología que demanda cierto nivel de calidad de servicio. Por otro lado, en muchas de las ocasiones no se realiza la configuración adecuada de ciertos parámetros del sistema en función de los recursos de la red y en consecuencia la calidad de servicio (QoS) se ve afectada. Por tal motivo, es importante una adecuada configuración de parámetros en el sistema VoIP a la hora de realizar su implementación, tales como: uso de detectores de actividad de voz y tipo de códec; esto con el objetivo de garantizar cierto nivel de QoS en la transmisión de voz a través de la redes de datos como Internet.

En este trabajo monográfico se realizará la implementación de servicios de voz sobre el protocolo de Internet bajo dos de los más importantes protocolos de VoIP: SIP y H.323, en dos redes LAN interconectadas por un Router.

Agradecimientos

A esta gran casa de estudios, mi querida universidad de Quintana Roo por formarme con los más altos estándares de calidad, a mi madre por su filosofía de lucha que imprimió en mi persona.

Dedicatoria

Para mi madre, Jesusa Canul Cohuo, mi esposa Wendy Irazú Brito Valle y mi hijo Edwin Alexander López Brito por ser los grandes pilares que me llenan de alegría, quienes con su compañía me motivan a disfrutar la vida y seguir alcanzando mis metas.

Gracias por acompañarme en este camino de grandes sacrificios donde cada uno de ustedes me proporciono su ayuda y consejos para salir avante en estos cinco años de formación académica, este logro es compartido ya que no lo hubiera logrado sin ustedes.

Contenido

Contenido

Agradecimientos 4
Dedicatoria 5
Introducción 13
Justificación 14
Objetivos 14
Desarrollo 15
Capítulo 1: Conceptos básicos de voz sobre el protocolo de internet 15
1.1.-Antecedentes de telefonía 16
1.2.-¿Que es VoIP? 17
1.3.-Funcionalidades de VoIP 17
1.3.1 Señalización 17
1.3.2 Códec 17
1.4.-Protocolo de internet (IP) 18
1.4.1 Direccionamiento IP 18
1.4.2.- Funcionamiento del protocolo IP 19
1.4.3.-Protocolos de transporte IP. 21
1.4.3.1.-TCP 23
1.4.3.2.- UDP 24
Capítulo 2: Calidad en el servicio en sistemas VoIP. 25
2.1 Concepto 26
2.2.- Factores que influyen en la calidad 27
2.2.1. Disponibilidad 28

2.2.2. Jitter 29
2.2.3. Perdidas 30
2.2.4. Retardo 31
2.2.5. ECO 35
2.2.6. Ancho de Banda 39
2.2.6.1 Supresión de silencios 40
2.3.-Medida de la calidad de la voz 42
2.3.1 ITU-T P.800 (Escalas MOS) 45
2.3.2 Modelado perceptual de la voz 47
2.3.2.1. Psicoacustica 48
2.3.2.2. ITU-T P.861 (PSQM) 51
..... 52
2.3.2.3. ITU-T P.862 (PESQ) 52
2.4. Modelo E 54
2.5. VQMon 57
Capitulo III: Protocolos de señalización H.323 y SIP. 59
3.1. INTRODUCCION 60
3.2. H.323 60
3.2.1 Descripción del sistema 62
3.2.1.1. Terminal. 63
3.2.1.2. Gateway 64
3.2.1.3. Gatekeeper 65
3.2.1.4. EL MCU y elementos 66
3.2.1.5. Servidor proxy H.323 66
3.2.3. Conjunto de protocolos H.323 67
3.2.3.1 Señalización RAS 68
3.2.3.2. Descubrimiento de gatekeeper 68

3.2.4. Registro..... 69
3.2.4.1. Localización del punto final. 71
3.2.4.2 Admisiones 71
3.2.4.3. Información de Estado. 72
3.2.5. Control de ancho de banda. 72
3.3 SIP..... 73
3.3.2 Arquitectura SIP..... 74
3.3.3 Operación del protocolo SIP 76
3.3.3.1 Transacciones Cliente / Servidor 76
3.3.4 RESPUESTAS SIP 76
3.3.5 Las solicitudes SIP..... 78
3.3.5.1¿Por qué SIP utiliza un saludo de tres vías? 81
..... 87
3.3.6 Formato de los mensajes SIP 87
3.3.7 Formato de respuesta SIP 89
Capitulo IV: Implementación de servicios de VoIP. 98
4.1 Implementación de servicio de voz sobre el protocolo de internet bajo el protocolo SIP..... 99
4.1.1 Características de los equipos..... 100
4.1.2 Configuración de los Equipos SIP. 102
4.1.2.5 Configuración Troncal SIP..... 108
4.1.3 Comprobación de llamadas. 113
4.2 Implementación de servicio de voz sobre el protocolo de internet bajo el protocolo H.323. 115
4.2.1.- Características de los equipos H.323. 116
4.2.2 Configuración de los equipos H.323..... 116
4.2.3 Comprobación de llamada..... 123
Capitulo V.- Resultados de la implementación. 127

5.1 Resultados de la implementación SIP 128
5.2 Resultados de la implementación H.323 129
Conclusiones 130
Bibliografía 132
Abreviaturas 133
Anexos 136

Índice de Figuras

Figura 1- 1. Red básica de 4 teléfonos. 16
Figura 1- 2. Formato de dirección de clase A, B, y C. 19
Figura 1- 3. Campos de paquetes IP. 21

Figura 2- 1. Relación entre la inteligibilidad y la calidad de la codificación de la voz 27
Figura 2- 2. Relación entre retardo y jitter. 30
Figura 2- 3. Relación entre el retardo en un solo sentido. 32
Figura 2- 4. Procesamiento de la señal de voz entre los extremos. 33
Figura 2- 5. Características de algunos códec. 34
Figura 2- 6. Conversión 2H/4H en la bobina hibrida. 36
Figura 2- 7. Comunicación VoIP sin eco. 37
Figura 2- 8. Solución de voz sobre paquetes con eco. 38
Figura 2- 9. Funcionamiento de un cancelador de eco. 38
Figura 2- 10. Puntos en los que se puede activar el VAD. 41
Figura 2- 11. Medida intrusiva o active. 42
Figura 2- 12. Medidas no intrusivas o pasivas. 43
Figura 2- 13. Comparación entre estándares de la calidad de voz. 44
Figura 2- 14. Generación de las escalas MOS. 45
Figura 2- 15. Modelo perceptual de la voz. 48
Figura 2- 16. Área de audición del ser humano. 49
Figura 2- 17. Tipos de enmascaramiento. 50

Figura 2- 18. Algoritmos PSQM. 52
Figura 2- 19. Algoritmo PESQ. 53
Figura 2- 20. Id en función del retardo. 55
Figura 2- 21. Evaluación de la calidad de la voz a partir del modelo E. 56
Figura 2- 22. Relación entre el modelo E y las escalas MOS en paquetes IP. 57

Figura 3- 1. Características y protocolos de H.323 61
Figura 3- 2. Elementos de la red H.323. 62
Figura 3- 3. Relaciones de los componentes de H.323. 63
Figura 3- 4. Elementos de un Gateway de H.323. 65
Figura 3- 5. Capas de la suite de protocolos H.323. 67
Figura 3- 6. Descubrimiento automático de Gatekeeper. 69
Figura 3- 7. roceso de mensajería y secuenciación para el registro de un gatekeeper y punto final. 70
Figura 3- 8. Arquitectura de red SIP. 75
Figura 3- 9. Laura emite una respuesta final (200 OK) por a invitación recibida. 80
Figura 3- 10. Saludo de tres vías: Invite-200 OK-ACK. 81
Figura 3- 11. Bob cancela su INVITE (invitación). 82
Figura 3- 12. Proxy Cancelando la transacción INVITE 84
Figura 3- 13. Laura envía un BYE cuando cuelga. 85
Figura 3- 14. Bob se registra en el registro Company.com 85
Figura 3- 15. Bob consulta al servidor sobre sus capacidades. 87
Figura 3- 16. SIP no garantiza que se reciban respuestas provisionales. 90
Figura 3- 17. Call-ID ayuda a distinguir entre diferentes sesiones. 92
Figura 3- 18. Los encabezados de CONTACTO pueden omitir un servidor proxy, una vezque el usuario final se encuentre. 93
Figura 3- 19. Cseq ayuda a distinguir las transacciones dentro de una sesión. 94
Figura 3- 20. El nombre del método en el Cseq permite diferenciar las respuestas INVITE y CANCEL. 95
Figura 3- 21. Los encabezados de ruta tienen un proxy permaneciendo en la ruta de señalización durante toda la sesión. 97

Figura 4- 1. Escenario de medición SIP 99
Figura 4- 2. Agregar Extensión SIP. 102
Figura 4- 3. Parámetros de extensión SIP. 103
Figura 4- 4. Creación de las extensiones SIP1 (1001-1004). 105
Figura 4- 5. Creación de las Extensiones SIP1 (1005-1008). 105
Figura 4- 6. . Creación de las Extensiones SIP2 (101-104). 106
Figura 4- 7. . Creación de las Extensiones SIP2 (105-108). 107
Figura 4- 8. Imagen de la configuración del router 1841. 108
Figura 4- 9. Troncal SIP para el servidor SIP1 109
Figura 4- 10. Troncal SIP para el servidor SIP2. 110
Figura 4- 11. Ruta de salida de SIP1 111
Figura 4- 12. Ruta de salida de SIP2. 112
Figura 4- 13. Selección de códec y modo de comprensión de voz. 113
Figura 4- 14. Extensiones del servidor SIP1 llamando a las extensiones del servidor SIP2 114
Figura 4- 15. Extensiones del servidor SIP-2 llamando a las extensiones del servidor de SIP1 114
Figura 4- 16. Escenario de medición H.323. 115
Figura 4- 17. . Contenido de la carpeta GNU. 116
Figura 4- 18. Contenido del archive Gatekeeper.ini del GK1. 117
Figura 4- 19. Contenido del archive Gatekeeper.ini del GK2. 118
Figura 4- 20. Inicio del Gatekeeper.exe a través del ms-dos. 120
Figura 4- 21. Creación de las extensiones del GK1 (1001-1004) 120
Figura 4- 22. Creación de las extensiones GK1 (1005-1008) 121
Figura 4- 23. Creación de las extensiones GK1 (101-104), para el GK2, (105-108). 122
Figura 4- 24. Selección de códec y modo de comprensión de voz. 123
Figura 4- 25. Estado del Gatekeeper. 124
Figura 4- 26. Establecimiento de llamada de GK1 a GK2. 125
Figura 4- 27. Establecimiento de llamada de GK2 a GK3. 126

Tablas

Tabla 1. Escala MOS utilizada para medir la calidad de la voz. 46

Tabla 2. Escala MOS para medida del esfuerzo de interpretacion del mensaje46. .....
Tabla 3. Escala MOS de calidad para los codecs más comunes. 47
Tabla 4. Clases de respuesta SIP 77
Tabla 5. Codigos de respuesta SIP 77
Tabla 6. Codificación binaria de los meses. 88
Tabla 7. Codificación binaria de los meses. 89
Tabla 8. Encabezados SIP. 91
Tabla 9. Administración de las llamadas escalonadas SIP 128
Tabla 10. Administración de las llamadas escalonadas H.323 129

Introducción

El avance de la tecnología permitió que se construya una plataforma donde todas las redes se integren en una sola, y con el nacimiento de nuevas aplicaciones y servicios, tal como VoIP, se dio el inicio de la convergencia de redes.

Actualmente existen dos protocolos dominantes en el mercado para la implementación de la VoIP, el primero es el protocolo de inicio de sesión (SIP) basado la arquitectura cliente-servidor, desarrollado por la IETF (Internet Engineering Task Force) y el segundo es H.323 que está orientado a la red de circuitos, desarrollado por la ITU (Internacional Telecommunications Union), ambos protocolos son implementados para soluciones diferentes y necesidades diferentes, en base a esto es necesario entender a profundidad el funcionamiento de ambos protocolos. La presente monografía, proporcionará a los lectores los conceptos básicos referentes a H.323 y SIP, y además ir un paso más adelante al comprender la importancia del uso de los detectores de actividad de voz (VAD) y diversos codificadores de voz.

Por otro lado, se detalla de una forma clara, la forma de cómo implementar servicios de voz sobre el protocolo de Internet bajo el protocolo SIP y la recomendación H.323, así también como las configuraciones necesarias para establecer la comunicación entre diversos usuarios que se encuentren en distintas redes LAN.

El trabajo monográfico está compuesta por cinco capítulos:

El primer capítulo está conformado por los conceptos básicos de voz sobre el protocolo de internet, en donde se explica el protocolo de internet (IP) y los conceptos asociados a la transmisión de voz.

El segundo capítulo contiene los conceptos referentes a la calidad de servicio en sistemas VoIP, se mencionan las diversas variables que inciden en la calidad de VoIP en su implementación, como jitter, ancho de banda, buffer, detección de voz, códec, todo esto es abordado en el capítulo dos.

El tercer capítulo está compuesto por los protocolos de señalización H.323 y SIP en el cual se mencionan sus arquitecturas y componentes para poder comprender el funcionamiento de cada uno de ellos.

El capítulo cuarto contiene la metodología usada en la implementación de servicios de VoIP, se detalla cada paso de la implementación.

El capítulo quinto nos proporciona los resultados de la implementación.

Justificación

Dentro de la constante tendencia de evolución de las tecnologías de información y redes de comunicación, Internet es una de las redes de mayor impacto en la vida cotidiana de millones de personas y es de singular importancia mencionar el gran crecimiento que han tenido en estos últimos años. Internet, puede considerarse como base para el desarrollo de nuevos servicios y aplicaciones no restringidos no sólo al transporte de datos, sino a la integración de múltiples medios (voz, datos, video, fax, etc.) sobre una misma infraestructura de red. Esta integración de múltiples medios es mejor conocida como convergencia de redes de comunicación.

Una de las piezas clave que ha permitido dicha convergencia ha sido el desarrollo de la tecnología VoIP. La cual es una de las aplicaciones más importantes sobre Internet, derivado de su disponibilidad multiplataforma que permite a cualquier usuario hacer uso de esta tecnología independientemente del sistema operativo que utilice, ofrece servicios más atractivos de comunicación a un menor costo a diferencia de la red telefónica pública conmutada y en la actualidad su infraestructura de red permite la integración de múltiples servicios de comunicación.

Objetivos

Implementar servicios de voz sobre el protocolo de Internet bajo los protocolos SIP y H.323, en dos redes LAN interconectadas por un Router.

Desarrollo

Capítulo 1: Conceptos básicos de voz sobre el protocolo de internet

1.1.-Antecedentes de telefonía

La primera transmisión de voz, enviado por Alexander Graham Bell, se llevó a cabo en 1876 a través de lo que se llama un circuito de generación de llamada, esto quiere decir que no hubo marcación de números, en cambio, si un cable físico conectado a dos dispositivos en comunicación [1].

Con el tiempo, este diseño simple evolucionó de una transmisión de voz en un solo sentido, por el que sólo un usuario podía hablar, a una transmisión de voz bidireccional, en el que ambos usuarios podían hablar. Para mover la voz a través del cable era necesario un micrófono de carbón, una batería, un electroimán y un diafragma de hierro. También requiere un cable físico entre cada lugar que el usuario quería llamar.

Para ilustrar mejor los inicios de la PSTN, ver la red básica de cuatro teléfonos que se muestra en la Figura 1-1. Como se puede ver, existe un cable físico entre cada ubicación [1].

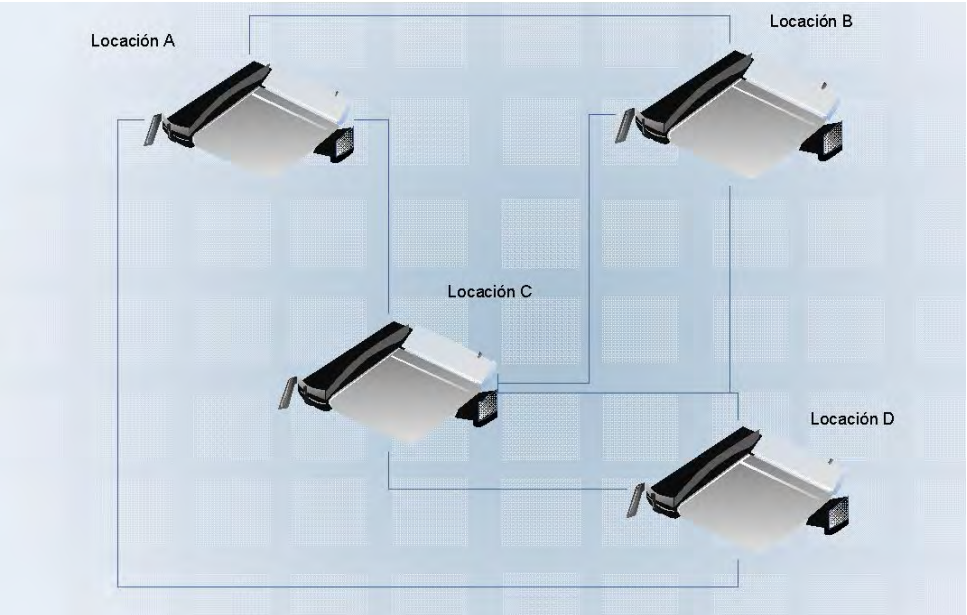


Figura 1- 1. Red básica de 4 teléfonos.

Con la evolución del internet y el surgimiento de diversos protocolos de VoIP, es posible implementar una red de telefonía sobre la red de paquetes en lugar de una red de telefonía basada en la conmutación de circuitos [1].

1.2.-¿Que es VoIP?

VoIP es una tecnología que permite que las redes IP se utilicen para la transmisión de los servicios de voz. VoIP define una alternativa para realizar llamadas de voz a través de una red IP, incluyendo la digitalización, paquetización y señalización [2].

VoIP proporciona ahorro de costos mediante la utilización de la red IP existente para transportar voz, especialmente donde las empresas han subutilizado la red IP, y es posible transportar VoIP sin costo adicional.

VoIP comparte el ancho de banda a través de múltiples conexiones lógicas, lo que da como resultado un uso más eficiente del ancho de banda [2].

1.3.-Funcionalidades de VoIP

1.3.1 Señalización

Señalización es la capacidad de generar información de control que se utilizará para establecer, controlar y liberar las conexiones entre dos puntos finales. SIP y H.323 son ejemplos de protocolos de señalización, donde los dispositivos finales contienen la inteligencia para iniciar y terminar las llamadas [2].

1.3.2 Códec

Los Códecs proporcionan la traducción de codificación y decodificación entre formatos analógicos y digitales. Cada tipo de códec define el método de codificación de voz y el mecanismo de compresión que se utiliza para convertir el flujo de voz. El códec más utilizado en un entorno WAN es G.729, que comprime el flujo de voz a 8 kbps [2].

1.4.-Protocolo de internet (IP)

James peter (2000) afirma que los beneficios de Voz sobre IP (VoIP) se derivan de la utilización del Protocolo de Internet (IP) como mecanismo de transporte, lo que hace al final de cuentas que realmente exista una comunicación.

1.4.1 Direccionamiento IP

Para *james Peter (2000),* de los diferentes esquemas de direccionamiento, el direccionamiento IP es el más importante de entender, ya que debe conceptualmente comprender cómo estos dispositivos se comunican para construir efectivamente las redes.

Existen muchos protocolos, y cada uno tiene un esquema de direccionamiento diferente. La capa de red de direccionamiento es normalmente jerárquica.

Clasificación de redes.

• Redes de clase A están destinados principalmente para uso con algunas grandes redes, ya que proporcionan sólo siete bits para el campo de dirección de red.

• Las redes de clase B asignan 14 bits para el campo de la dirección de red y 16 bits para el campo de la dirección de host. Esta clase de dirección ofrece un buen compromiso entre la red y el espacio de direcciones de host.

• Las redes de clase C asignan 21 bits para el campo de dirección de red. Ellos proporcionan sólo 8 bits para el campo de acogida, sin embargo, el número de hosts por la red puede ser un factor limitante.

• Las direcciones de clase D están reservadas para grupos de multidifusión, como se describe formalmente en la RFC 1112. En las direcciones de clase D, los cuatro bits de más alto orden se establecen en 1, 1, 1 y 0.

• Las direcciones de clase E también se definen por la propiedad intelectual, pero se reservan para uso futuro. En las direcciones de clase E, los cuatro bits de más alto orden se establecen en 1, y el quinto bit es siempre 0.

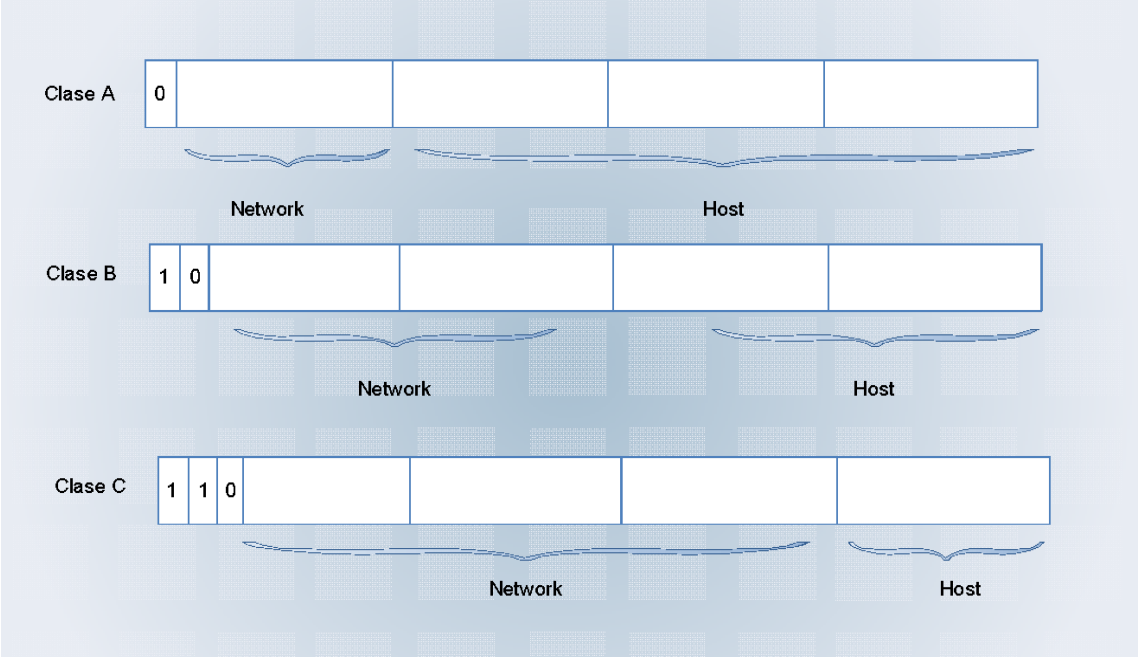


Figura 1- 2. Formato de dirección de clase A, B, y C.

1.4.2.- Funcionamiento del protocolo IP

James peters (2000) define en sí que el protocolo de internet IP es un protocolo sin conexión que reside en la capa 3 (la capa de red), lo que deriva de la inexistencia de fiabilidad en sus mecanismos, control de flujo, secuenciación, o reconocimientos. Otros protocolos como TCP, puede estar en la parte superior de IP (capa de sesión) y estos si pueden agregar el control de flujo, la secuenciación, y otras características que garanticen estos controles de flujo.

Puede usar IP en una casa o en un negocio a través de cualquier medio que sea necesario (por ejemplo, inalámbrica, banda ancha). Esto no necesariamente

significa que cuando se diseña una red puede ignorar las capas de abajo, solo que son independientes de cualquier aplicación basada en IP.

IP se considera el protocolo de ráfaga, lo que significa que las aplicaciones que residen por encima de IP experimentan largos periodos de silencio, seguidas por una necesidad de un ancho de banda grande. Un buen ejemplo de esto es el correo electrónico, si tú configuras tu correo para descargar un paquete del correo electrónico cada 20 minutos, alrededor de 20 minutos silencio existe, durante el cual no se requiere ancho de banda, *James Peters (2000).*

Se aborda un paquete IP en tres formas generales: a través de los mecanismos de unicast, multicast, o broadcast, estos conceptos manejados muy ampliamente en el protocolo de internet son necesario comprenderlos para que al final de cuentas se puedan tener los elementos claves, como se ha dicho en líneas anteriores, IP es la base de la tecnología Voz sobre IP, James Peters (2000).

Brevemente explicado James Peters (2000), menciona que estos tres mecanismos proporcionan los medios para que todos los paquetes IP puedan marcarse con una dirección IP, cada uno a su manera única, estos tres se explican de manera breve y concisa a continuación:

1. **Unicast** es bastante simple, ya que identifica a una dirección específica y el nodo va enviar el paquete a las capas más altas del modelo de referencia OSI.
2. **Paquetes de difusión** (broadcast) se envían a todos los usuarios de una subred local. Las transmisiones pueden a travesar puentes e interruptores, pero no se pasan a través de routers (a menos que estén configurados especialmente para hacerlo).
3. **Paquetes de multidifusión** utilizan una gama especial de abordar a un grupo de usuarios para recibir el mismo flujo. Esto permite al remitente enviar un solo paquete a varios remitentes.

Unicast, multicast y broadcast cada uno tiene un propósito, el unicast permite la comunicación entre dos estaciones, independientemente de la ubicación física. Los broadcast se utiliza para comunicarse con todos en una subred simultáneamente, los de multidifusión son los que permiten a las aplicaciones, tales como videoconferencias, que tiene un transmisor y varios receptores, en

voz sobre IP una de las opciones puede ser la videoconferencia por lo tanto utiliza multicast, con esta explicación más detallada se deja claro cuáles son las funciones de cada uno *James peters (2000).*

1.4.3.-Protocolos de transporte IP.

TCP y UDP tienen diferentes características que varias aplicaciones pueden usar. Si fiabilidad es más importante que la demora, por ejemplo, puede utilizar TCP para garantizar la entrega de paquetes. UDP no utiliza paquetes retransmisores, sin embargo esto puede reducir la fiabilidad pero en algunos casos no se le da una utilidad importante.

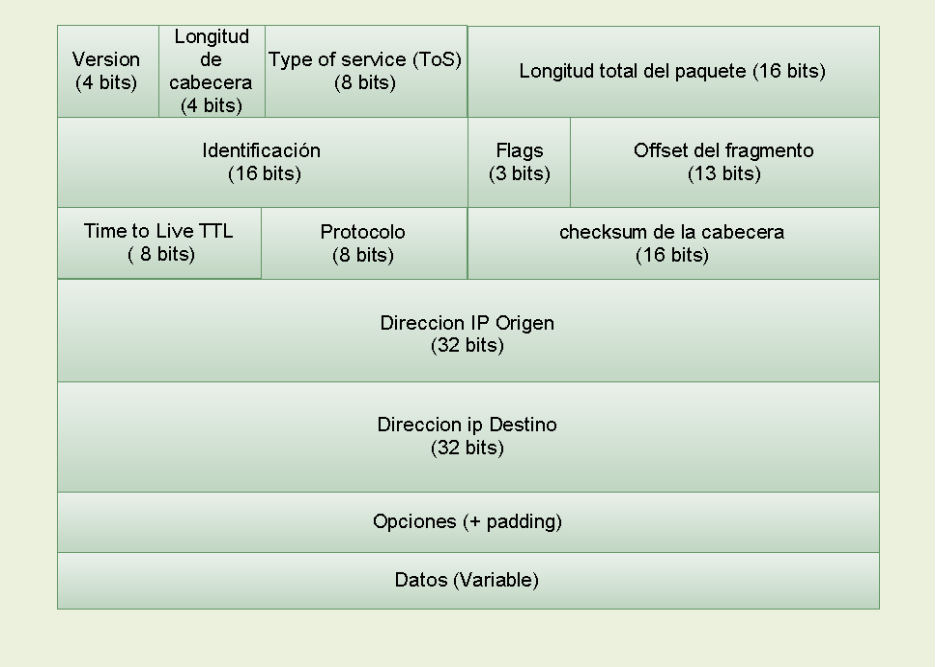


Figura 1- 3. Campos de paquetes IP.

Los campos de paquetes IP que se muestran en la figura 1-3 de arriba se definen a continuación:

Versión: Indica si es la versión IPv4 o IPv6

Longitud de la cabecera IP (DIH): indica la longitud de la cabecera del datagrama en palabras de 32 bits.

Tipo de servicio: especifica como un protocolo de capa superior en particular quiere el datagrama actual a ser manejado. Puede asignar varios paquetes de calidad (QoS) los niveles de servicio basados en este campo.

Longitud Total (total lenght): Especifica la longitud de todo el paquete IP, incluyendo datos y el encabezado, en bytes.

Identificación (identification): Contiene un entero que identifica el datagrama actual. Este campo ayuda a unir las piezas de los datagramas.

Banderas (flags): Un campo de 3 bits de los cuales lo de bajo de orden de 2 bits de control de la fragmentación. El bit de orden en este campo es no utilizado, un bit especifica si se puede fragmentar el paquete, el segundo bit si el paquete es el último fragmento de una serie de paquetes fragmentados.

Time-to-live: Mantiene un contador que disminuye gradualmente hasta llegar a cero, momento en el que el datagrama se descarta. Esto evita que los paquetes estén en un bucle sin fin.

Protocol (protocolo): Indica que protocolo de cada superior recibe el paquete entrante después del procesamiento IP está completa.

Cabecera Checksum: Verifica que la cabecera no este dañada.

Soure Addres: La dirección Origen.

Destination Addres: La dirección destino que recibe el datagrama.

Options (Opciones): Permite IP para apoyar las diversas opciones, como la seguridad.

Datos: Contiene datos de la aplicación, así como información de protocolo de capa superior.

1.4.3.1.-TCP

TCP incorpora mecanismos para la reacción en un caso de pérdidas de paquetes. Principalmente a casusa de la congestión en los nodos de la red (enrutadores, interruptores), debido al principio de servicio de mejor esfuerzo y la naturaleza a ráfagas de trafico IP.

Cuando TCP descubre que se han perdido datos en la red, se recupera de ella mediante la retransmisión de los segmentos que faltan. TCP descubrirá la perdida mediante la recepción de akcnowledgement del emisor, o si el emisor no recibe akcnowledgement en el periodo de tiempo más largo que el predefinido.

Porque TCP fue creado originalmente para redes de paquetes por cable, siempre asume que las pérdidas se están produciendo debido a la congestión únicamente. Reacciona a la congestión disminuyendo su velocidad de datos basado en un mecanismo para evitar la congestión.

TCP utiliza para evitar la congestión la herramienta basada en ventanas, básicamente con dos ventanas:

La congestión ventana (cwnd) y el receptor anunciando ventana de congestión (rcvwnd). El receptor anuncia el tamaño de la ventana de congestión en el remitente. El remitente determina la congestión de la ventana del receptor y la congestión (por ejemplo, el reconocimiento de los paquetes enviados faltante). Para la explicación de evitar la congestión, conveniente introducir el mecanismo de arranque lento TCP primero. (traffic and design of wireless ip p.59)

Retransmisión rápida: Se propone este mecanismo de TCP para hacer frente a ACKs duplicados debido a la reordenación de segmentos. Desde TCP no se sabe si un ACKs es duplicado debido a un segmento perdido o un reordenamiento de los segmentos, la retransmisión rápida debe esperar por un pequeño número de ACKs duplicados sean recibidas por el remitente.

Recuperación rápida: La recuperación rápida permite la invocación de evitar la congestión en lugar de comienzo lento después de la retransmisión del segmento faltante por el algoritmo de retransmisión rápida.

James Peters nos dice que dentro de la señalización de VoIP, TCP se utiliza para garantizar la fiabilidad de la configuración de una llamada. Debido a los métodos por los cuales opera TCP y que hemos mencionado en este tema, no es factible utilizar este protocolo de transporte para transmitir voz en tiempo real en una llamada VoIP.

1.4.3.2.- UDP

Es un protocolo mucho más sencillo que el protocolo anterior TCP y es útil cuando la confiabilidad de TCP no es necesarias, UDP es un protocolo orientado a la no conexión y tiene una cabecera más pequeña lo que ese traduce en una sobre carga mínima haciendo más rápido el proceso.

Solo consta de cuatro campos: Puerto de Origen, puerto de destino, la longitud y la suma de comprobación UDP. La fuente y los campos de puerto destino sirven para las mismas funciones del protocolo TCP.

UDP se utiliza en VoIP para transportar el tráfico de voz en tiempo real (los canales portadores), TCP no se utiliza porque el flujo de control y la retransmisión de paquetes de audio de voz son innecesarios. Debido a que UDP se utiliza para llevar el audio este se sigue transmitiendo sin importar si se han perdido pocos paquetes o una gran cantidad de estos.

Si se utilizara TCP para VoIP, la calidad de la voz sería inaceptable debido a la latencia, la espera de reconocimientos (aknowledgmenrs) y retransmisiones. James Peters (2000).

Capítulo 2: Calidad en el servicio en sistemas VoIP.

2.1 Concepto

El concepto de calidad de servicio o QoS (Quality of Service) es demasiado amplio, y por ello, su interpretación depende del contexto concreto en que se emplee el término. En este capítulo nos centraremos en la calidad de la voz desde el punto de vista del usuario, es decir, de como de bien se escuchan los interlocutores de una conversación telefónica a través de una red de voz sobre paquetes [3].

Las consideraciones generales sobre la evaluación de la calidad del servicio telefónico se encuentran en la recomendación E.240 de la ITU-T. Esta recomendación subraya los aspectos que mayor influencia ejercen sobre la percepción de la calidad del servicio de telefonía por parte de los usuarios [3].

Algunos aspectos importantes son:

Tasa de conectividad: Hace referencia a la probabilidad de la disponibilidad de recursos de la red para cursar un intento de llamada [3].

Inteligibilidad de la voz: Un requisito, previo a todos los demás es que cada extremo sea capaz de entender claramente las palabras de su interlocutor. En este sentido, juega un papel fundamental la claridad de la voz [3]. La claridad de la voz es un parámetro subjetivo que puede definirse como la fidelidad con que la voz es percibida por el extremo remoto e indica cuanta información puede extraerse de las palabras del otro extremo. Depende de la distorsión introducida por los componentes de la red. Sin embargo, es independiente del retardo (aunque el jitter si ejerce gran influencia) y del eco (puesto que este es escuchado por el emisor y la claridad se evalúa en el receptor) [3]. La inteligibilidad depende de una gran variedad de factores, aunque únicamente son bien conocidos unos pocos. Por ejemplo, se sabe que ciertas bandas de frecuencias (200-800 Hz) son más importantes para la inteligibilidad que otras (1000-1200 hz) [3].

Codificación de la voz: Una vez que la llamada ha sido establecida y que la voz del otro extremo puede entenderse con claridad el siguiente paso es codificar la voz, transmitirla a través de la red y ver qué tal se escucha. El resultado será una medida de la bondad del esquema de codificación empleado [3]. La calidad de la codificación y la inteligibilidad de la voz están relacionadas entre sí y ambas

dependen de la tasa binaria y de la tasa de error (ver figura 2-1). Como puede verse, cuanto mayor es la tasa binaria, tanto más probable es obtener una buena calidad en la codificación (no solo inteligibilidad). Por otro parte, el incremento de la tasa de error es mayor cuanto menor es la tasa binaria debido a la disminución en la información de redundancia por la compresión [3].

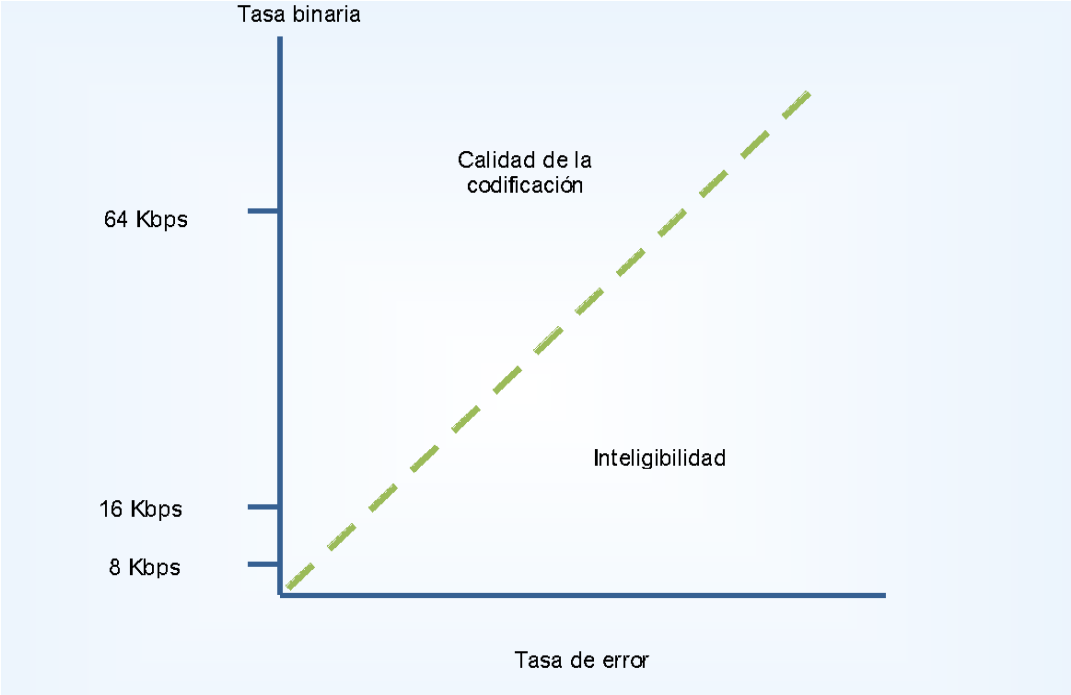


Figura 2- 1. Relación entre la inteligibilidad y la calidad de la codificación de la voz

2.2.- Factores que influyen en la calidad

Para los usuarios de las redes de voz sobre paquetes las diferencias tecnológicas existentes entre las redes de conmutación de circuitos y de paquetes deben ser totalmente transparentes. Es decir, que de alguna manera hay que conseguir que las redes de conmutación de paquetes ofrezcan una calidad de servicio telefónico similar a las redes de conmutación de circuitos sin perder sus características propias. En general, las factores que determinan esta calidad, por orden de importancia, la disponibilidad, el jitter, las perdidas, el retardo y el ancho de

banda. Además, en comunicaciones telefónicas otra limitación tecnológica que hay que tener en cuenta es el eco [3].

En este capítulo estudiaremos, precisamente, la influencia de estas limitaciones tecnológicas [3].

2.2.1. Disponibilidad

La disponibilidad de un sistema es una medida de la probabilidad con que se encontrara en condiciones de funcionamiento, de manera que cuanto mayor es dicha probabilidad mayor será la disponibilidad [3].

A la hora de diseñar cualquier sistema debemos analizar, en primer lugar, el tiempo que el sistema puede dejar de estar operativo debido a los fallos inesperados en el hardware y el coste que ello supone para contratarlo con el costo de la inversión necesaria para prevenir dichos fallos. Para VoIP los componentes críticos son los servidores. Los gateways y los terminales de usuario [3].

La clave de la tolerancia es la redundancia, cuyo propósito es simple, cualquier parte del sistema que resulte crítico para su funcionamiento deberá estar replicada, de tal modo, que el sistema de reversa reemplace al principal en caso de fallo de este último. Replicar absolutamente todos y cada uno de los componentes de la red no tiene sentido y, además, no es viable económicamente, por lo que se opta por duplicar única y exclusivamente aquellos que realmente son críticos para el funcionamiento de la red, generalmente, los servidores encargados del control de llamadas, la señalización y la señalización y los gateways [3].

Por otra parte, se suele configurar los terminales de usuarios para que si ocurriera que la llamada no puede cursarse por carecer de recursos o por estar la red fuera de servicio, dicha llamada se encamine por la red telefónica publica conmutada (RTPC) o la red digital de servicios integrados (RDSI). Es lo que se conoce como encaminamiento de backup [3].

Además, es recomendable utilizar los sistemas de alimentación ininterrumpida (SAI) que reducen el impacto de los cortes de suministro eléctrico. Estos

sistemas, si son de pequeña potencia, constan de una batería que acumula energía y de un ondulador que transforma la corriente continua en alterna a 220 v/ 50 Hz para alimentar al equipo durante un periodo de tiempo (por ejemplo, 30 minutos) que da lugar para poder cerrar las aplicaciones y evitar la pérdida de datos. En caso de sistemas de gran potencia se tienen generadores con motores de gasolina, con lo que el sistema puede presentar gran autonomía. En ambos casos entran en funcionamiento ante los cortes de energía y también realizan un filtrado/estabilidad de la corriente, para eliminar los picos de tensión y micro cortes [3].

2.2.2. Jitter

En general a la hora de analizar las prestaciones de una red se habla de retardo en valores medios. Sin embargo, el tráfico de voz es muy sensible a las variaciones de retardo y, por ello, trabajar con valores medios no resulta suficiente [3].

En redes IP, y en general en cualquier red de paquetes, no es posible garantizar que todos los paquetes de una misma comunicación sigan el mismo camino (de hecho, lo más probable es que no lo hagan), al contrario de lo que ocurre en las redes de conmutación de circuitos. Como consecuencia, cada paquete llegara al destino atravesando un número distinto de nodos en la red, por tanto alcanzaran su objetivo con un retardo diferente. Esta variabilidad del retardo recibe el nombre del jitter [3].

Los paquetes se generan en el origen con una cadena fija, por ejemplo, un paquete de voz cada 20 ms. Sin embargo, al llegar al destino, este tiempo es variable debido a las diferencias en los retardos de encolamiento y propagación fundamentalmente [3].

Para absorber estas variaciones se utilizan los llamados buffers de supresión de jitter. La supresión consiste en el almacenamiento de los paquetes durante un tiempo suficiente para que los paquetes que han llegado fuera de secuencia puedan reordenarse y reproducirse en el orden correcto, tal y como lo muestra la figura 2-2. Por tanto, cuanto mayor es el jitter de los paquetes, mayor es el tamaño del buffer de supresión de jitter necesario para reducir su impacto en la calidad [3].

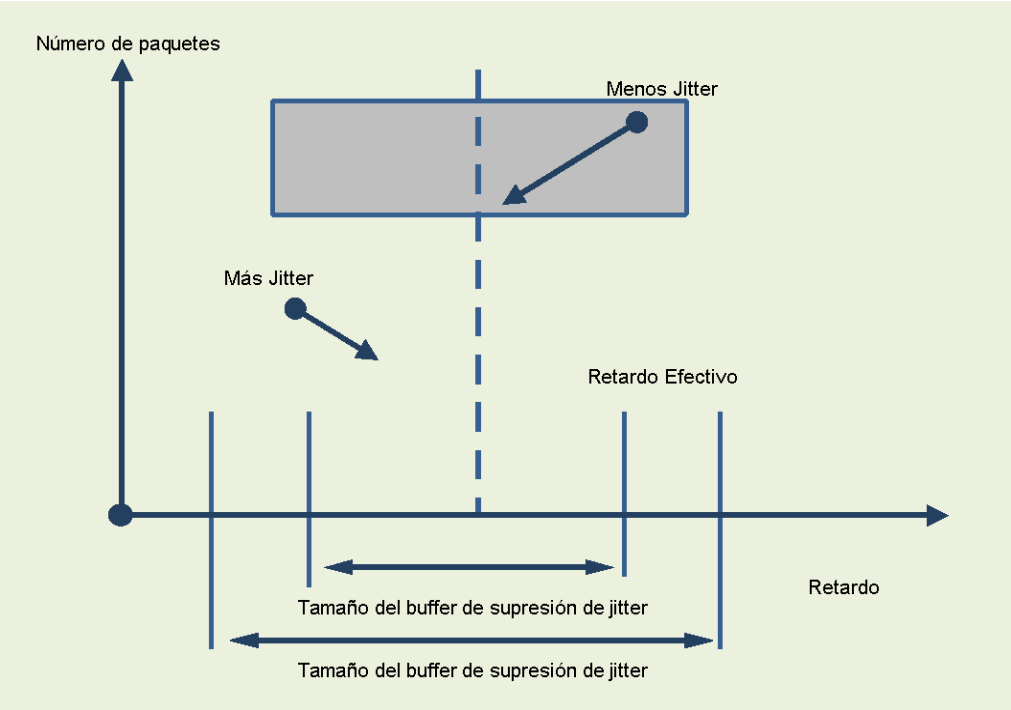


Figura 2- 2. Relación entre retardo y jitter.

2.2.3. Perdidas

Las pérdidas de paquetes son el resultado del descarte de paquetes que se produce en los nodos de la red como consecuencia de la congestión de dichos nodos. Puesto que las redes de conmutación de paquetes no se producen una reserva de recursos previa al envío de información de usuario, las pérdidas son inevitables. El efecto de las pérdidas es una disminución de la calidad de la voz, puesto que faltan paquetes a la hora de reconstruir la señal vocal. Esta disminución de la calidad es tanto mayor cuanto mayor sea la compresión del códec [3].

La soluciona más inmediata al problema de las perdidas es la mejora de la arquitectura de la red. En efecto, puesto que las pérdidas son, básicamente, una cuestión de capacidad, si se sustituyen las líneas y los routers por otros de mayor capacidad el problema queda aparentemente resuelto. Sin embargo, esta solución no es definitiva puesto que en cuanto aumente ligeramente el tráfico de la red, los efectos nocivos de las perdidas volverán a aparecer [3].

La alternativa que puede parecer más obvia es solicitar la retransmisión de los paquetes perdidos. Sin embargo, esto introducirá un retardo adicional que todavía empeora más la calidad de la voz. Son necesarias, por tanto, otro tipo de técnicas que atenúan efectos de las perdidas. Para este fin, se han desarrollado tres medidas [3]:

Corrección de errores (FEC, Forward Error Control): en este tipo de técnicas, junto con los paquetes, se incluye información de redundancia que permite recuperar el valor del paquete perdido a partir del valor de los paquetes perdidos. Su principal inconveniente es el retardo puesto que para decodificar un paquete son necesarios paquetes vecinos [3].

Distribución de errores: Consiste en provocar de forma intencionada que las pérdidas se presenten de manera aleatoria para dispersar sus efectos. De nuevo, el inconveniente es el retardo adicional que introducen y que consumen un mayor ancho de banda [3].

Recuperación de errores (Packet Lost Concealment): Sustituyen el paquete perdido por otro. Esta sustitución puede ser tan simple como emplear un paquete perdido, un silencio o un ruido blanco, o tan compleja como el resultado de una técnica de predicción a partir de anteriores y posteriores. En este sentido, conviene tener en cuenta que a mayor complejidad, mayor costo de procesamiento y mayor retardo introducido [3].

2.2.4. Retardo

El retardo o latencia es el tiempo invertido por la señal de una voz en su viaje desde el origen hasta el destino. Una de las características más importantes de la voz es su temporalidad, no solo porque el intervalo de pronunciación de dos silabas determina su pertenencia a una misma palabra, sino que la conversión entre dos interlocutores sigue un esquema temporal de escucha-respuesta cuya

alteración puede convertir la conversación en inteligible (piense en dos interlocutores hablando a la vez) [3].

Por otra parte, uno de los problemas de las redes telefónicas es el eco, consecuencia de las reflexiones que sufre la señal en el otro extremo. Las redes telefónicas convencionales se diseñan para el retardo no supere los 50 ms y, en estas circunstancias, el eco es enmascarado por la voz de los interlocutores [3].

El retardo máximo aceptable máximo aceptable marca un umbral por encima del cual la calidad de la voz resulte es inaceptable y conversación resulta imposible. La recomendación G.144 de la ITU-T establece este umbral entorno a los 150 ms (ver figura 2-3) [3].

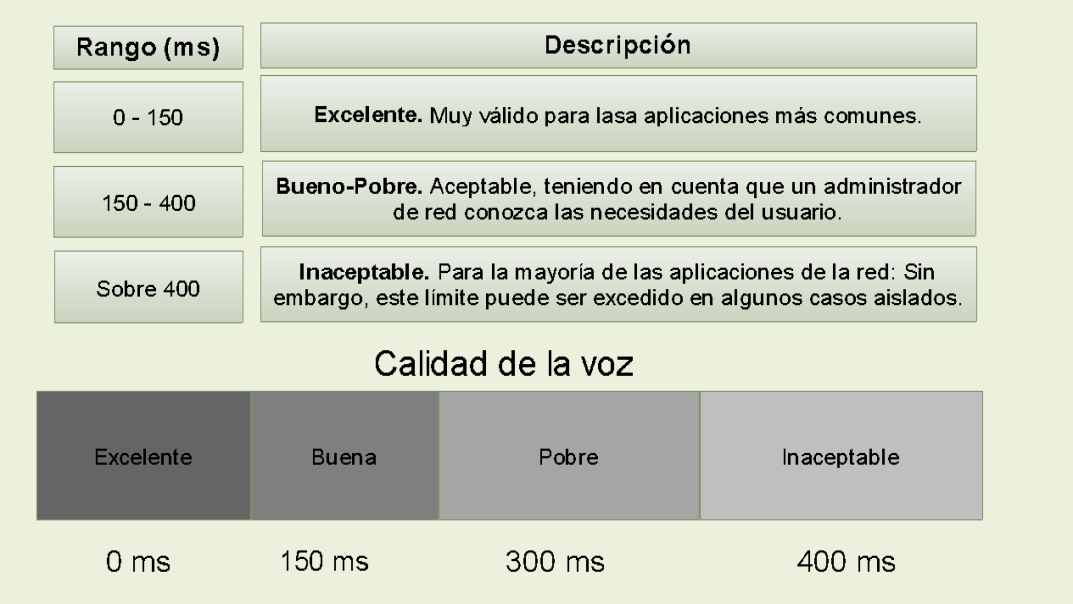


Figura 2- 3. Relación entre el retardo en un solo sentido.

Una vez que ya se dispone de un objetivo de diseño en cuanto al retardo se refiere, el paso siguiente es estudiar las distintas fuentes de retardo con el fin de optimizar su comportamiento. Para ello, conviene analizar todo el proceso que sufre la señal de voz desde que es emitida por un extremo hasta que llega a su receptor (ver figura 2-4) [3].

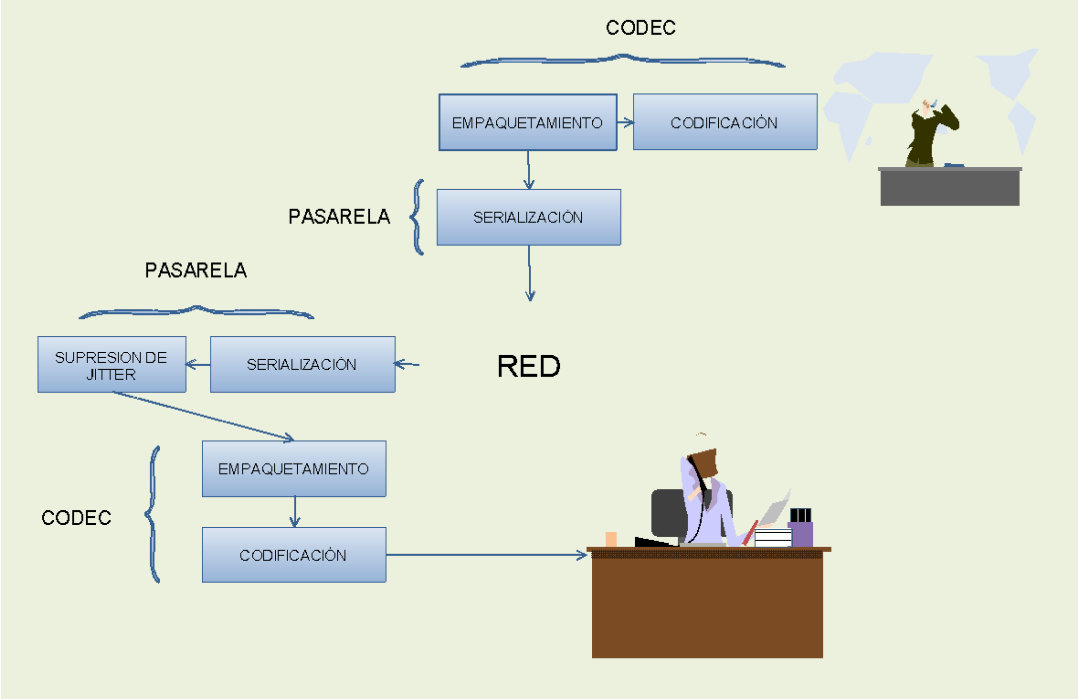


Figura 2- 4. Procesamiento de la señal de voz entre los extremos.

En primer lugar, la voz del usuario debe digitalizarse ya que su formato natural es analógico y para su transmisión por la red de paquetes debe tener un formato digital. Junto con la digitalización, algunos códec realizan, además una compresión que reduce el ancho de banda consumido por la comunicación vocal. El paso siguiente es empaquetar las muestras de voz antes de su transmisión por la red. El retardo introducido en todos estos procesos depende del códec. La tabla de la figura 2-5 muestra los parámetros de algunos de los códec más empleados en VoIP, aunque algunos pueden variar ligeramente, dependiendo del fabricante [3].

Una vez que los paquetes llegan al gateway, esta invertirá un cierto tiempo en transmitirlos por una determinada línea. Este tiempo es lo que se conoce como retardo de serialización y depende de la velocidad de la línea y el tamaño de la trama. El retardo de serialización debe contabilizarse cada vez que el paquete atraviese un dispositivo store-and-forward como un router o switch [3].

	G.711	G.729	G.723.1
Tasa binaria (kbps)	64	8	6,3 / 5,3
Complejidad (MIPS)	0,1	22	16 / 18
Retardo codificador (ms)	0,125	15	37,5
Tiempo entre paquetes (ms)	20	20	30
Retardo de empaquetamiento (ms)	1,5	15	37,5
Tamaño de buffer de supresión de jitter (ms)	40	40	60
Calidad (MOS)	4,4	4,1	3,5 - 3,9

Figura 2- 5. Características de algunos códec.

Los paquetes serializados viajaran por la red hasta llegar al destino. El tiempo invertido en este viaje deriva, fundamentalmente, de dos contribuciones, una fija y otra variable. La componente fija se corresponde con el retardo de propagación, que es el tiempo que tarda la señal en alcanzar su destino. Depende de las características del medio físico de transmisión y de la velocidad de la luz, por lo que suele ser muy pequeño (la recomendación G.114 aconseja un valor de 6 μs/km). Por otro lado, los paquetes son encolados en los nodos de la red un tiempo variable que depende de la carga de la misma y la capacidad de dichos

nodos. Puesto que el número de paquetes en espera en la cola de transmisión depende de la caracterización estadística del tipo de tráfico al que pertenezcan dichos paquetes, el retardo de encolamiento varía mucho de un paquete a otro. En cualquier caso, generalmente, el retardo de la red se encuentra comprendido entre 70 ms y 100 ms y es, por tanto, una de las contribuciones más importantes al retardo total [3].

Como consecuencia de la variabilidad del retardo de paquetes, se produce un fenómeno conocido como jitter. En cualquier caso para reducir la influencia del jitter se utilizan unos buffers que almacenan los paquetes de voz durante cierto tiempo. Este almacenamiento introduce un retardo adicional, por lo que habrá que llegar a una solución de compromiso [3].

2.2.5. ECO

El eco es un fenómeno común a las redes telefónicas convencionales y a las redes de voz sobre paquetes. Se produce cuando el emisor escucha parte de su propia voz junto con la voz de su otro interlocutor o en ausencia de ella [3].

Las causas del eco son muy variadas. En primer lugar se encuentra el eco acústico, debido a un acoplamiento entre el micrófono y el auricular del teléfono. Debe considerarse, sobre todo, en teléfonos manos libres o inalámbricos y se suele solucionar utilizando terminales de gran calidad y mayor precio. El otro tipo de eco es el eco eléctrico, consecuencia de una desadaptación de impedancias en el extremo receptor. Este es el más importante y el que se tratara en este apartado [3].

En redes telefónicas convencionales se usan dos pares de hilos (uno para la transmisión y uno para la recepción) entre el bucle telefónico del usuario y la central de conmutación del operador. Sin embargo, al teléfono del usuario llega un par. Por tanto, es necesaria una conversión que se lleva a cabo en un dispositivo llamado bobina hibrida (ver figura 2-6) [3].

En la conversión 2H/4H se produce una desadaptación de impedancias que refleja parte de la señal incidente y que viajara junto con la voz del otro extremo, dando lugar al fenómeno conocido como eco. En realidad, se trata de un fenómeno inevitable aunque, de manera controlada, resulta imperceptible. De hecho, en redes telefónicas convencionales si la amplitud es suficientemente baja

y el retardo es un solo sentido es menor de 50 ms, el eco queda enmascarado por la conversación normal [3].

Además del retardo del eco, que debe mantenerse en torno a los 16 ms, también es importante su amplitud. La magnitud de la señal reflejada recibe el nombre de ERL (Eco Return Loss) y se define como [3]:

ERL= Amplitud de la señal fuente –Amplitud del eco.

La recomendación G.168 ESTABLECE QUE El ERL debe ser mayor a 55 dB

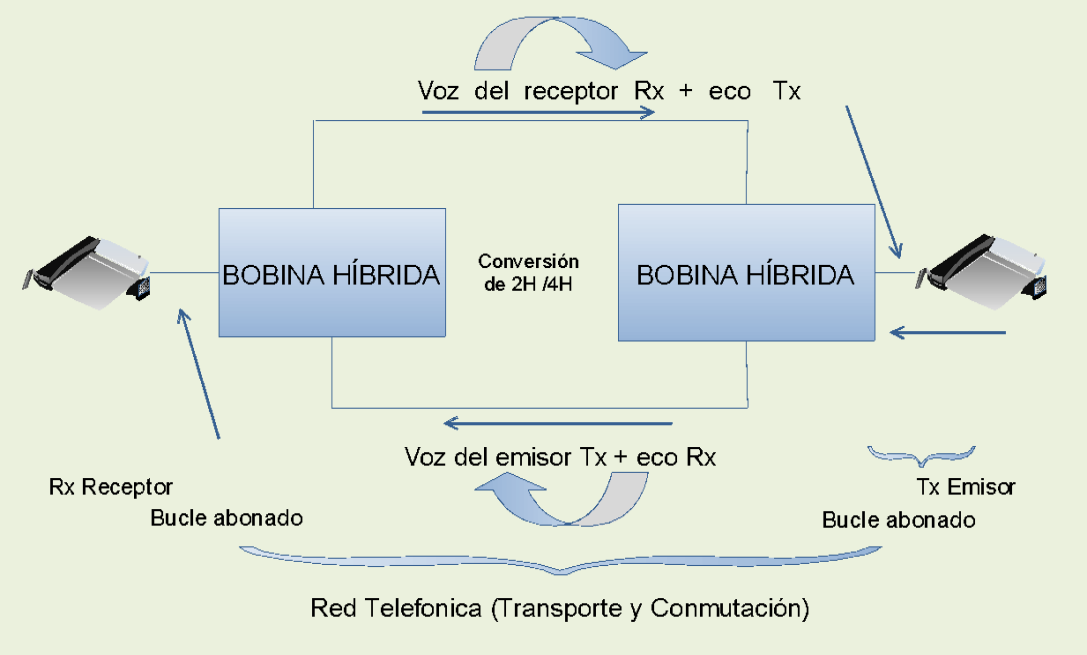


Figura 2- 6. Conversión 2H/4H en la bobina hibrida.

A la hora de estudiar el eco en redes de voz sobre paquetes, se debe tener en cuenta que este únicamente se produce en los segmentos analógicos de la red y no en los digitales. Estos segmentos susceptibles de sufrir eco reciben el nombre de circuitos de cola. Por ejemplo, cuando el ámbito de la voz sobre paquetes abarca toda la red completa (IP extremo a extremo) no se produce eco puesto que toda la comunicación tiene lugar a través de la red de datos (fig. 2-7) [3].

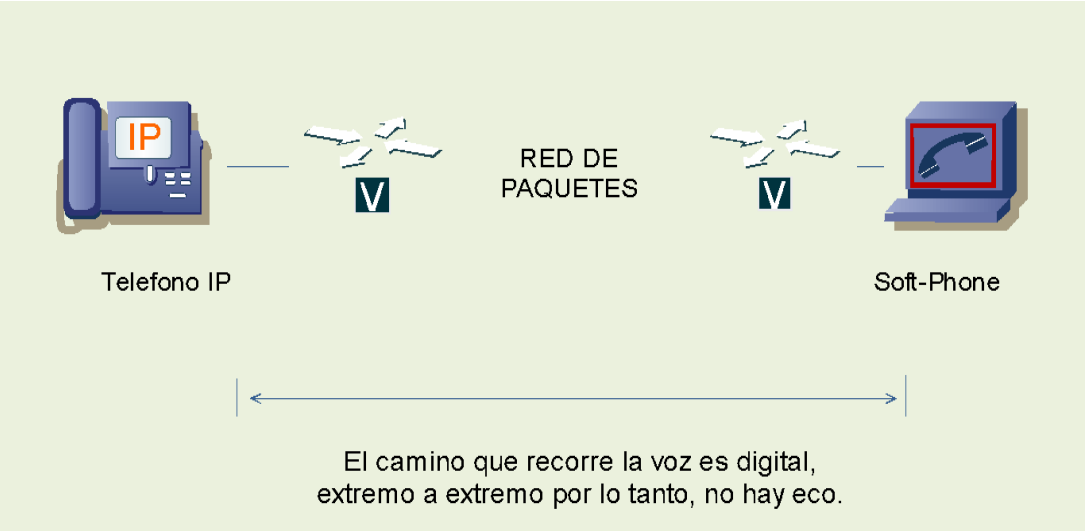


Figura 2- 7. Comunicación VoIP sin eco.

Sin embargo, esta situación es muy poco común. Generalmente, la voz sobre paquetes debe interactuar con teléfonos convencionales y PBX (ver figura 2-8) en los que sí existe circuito de cola y por tanto, en los que se produce cierta cantidad de eco que habrá que eliminar o al menos reducir a unos niveles tolerables [3].

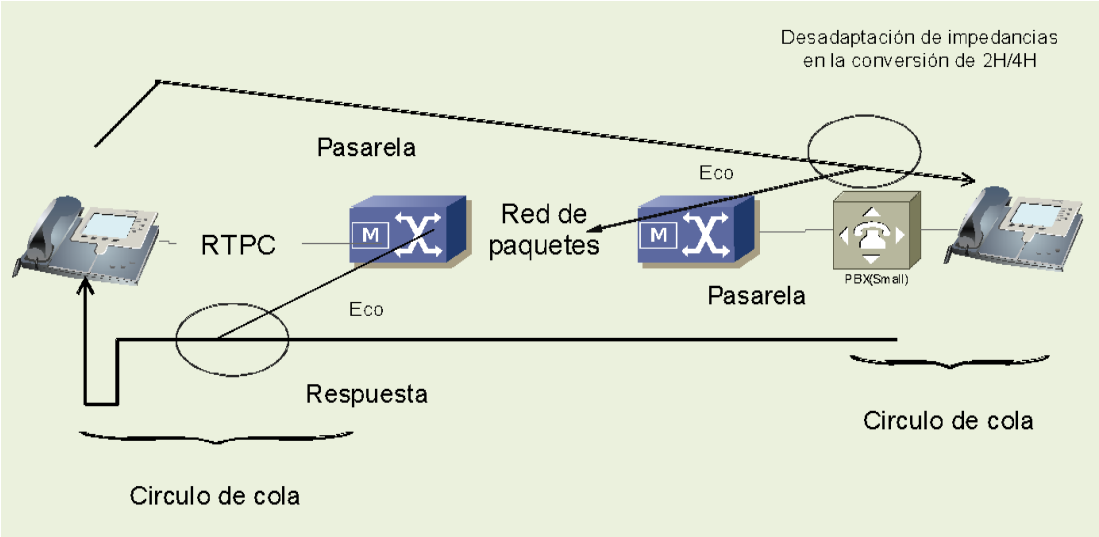


Figura 2- 8. Solución de voz sobre paquetes con eco.

Para disminuir los efectos del eco, algunos gateways y teléfonos IP incluyen canceladores de eco. Un cancelador de eco (ver figura 2-9) lleva a cabo un filtrado adaptativo de la señal recibida (eco + voz del otro extremo) que estima el valor del eco que contiene e intenta neutralizarlo [3].

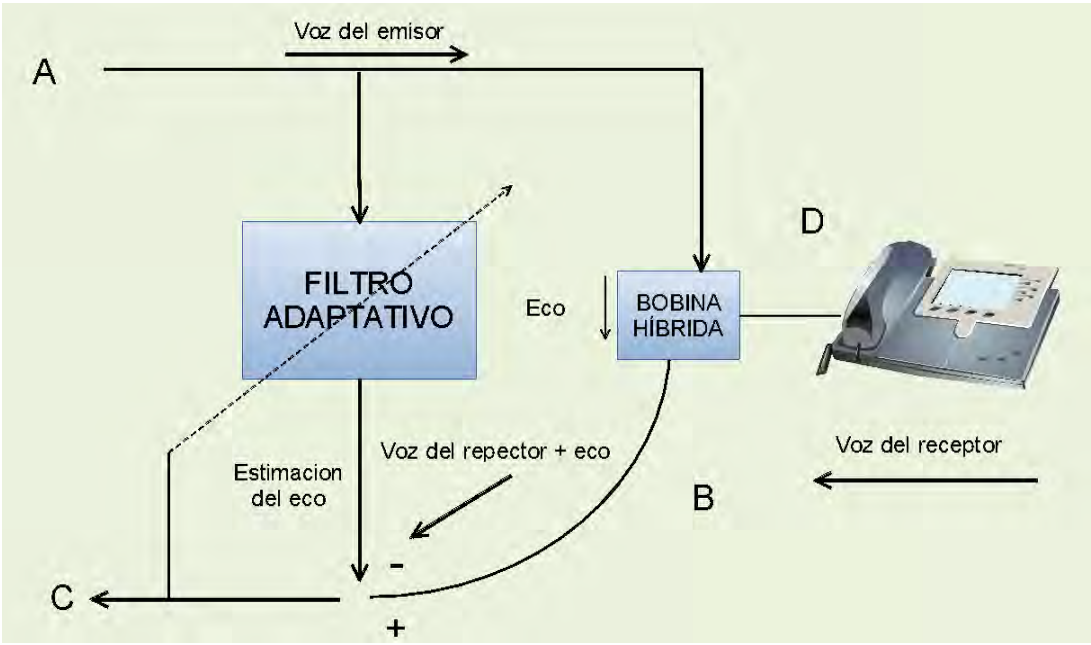


Figura 2- 9. Funcionamiento de un cancelador de eco.

En primer lugar, se produce un almacenamiento de la señal cuyo objetivo es calcular los valores de los coeficientes del filtrado adaptativo y, a partir de ellos, una estimación del eco. El tamaño de la memoria del almacenamiento depende del retardo de eco previsto. La señal entrante (rama A) llega, finalmente, a la bobina hibrida donde , debido a la conversión 2H/4H parte de ella se refleja y se suma la señal del receptor (rama D), de manera que por el hilo e recepción (rama B), viajaran tanto la voz del receptor como el eco. Es precisamente en este punto donde entra en juego el cancelador de eco, restando a este conjunto la estimación del eco calculada a partir de la voz del hablante almacenada. El resultado es que, el eco es menor que el que había, obviamente, cuanto mejor sea la estimación del eco, mucho menor será este y mayor calidad se percibirá en la señal recibida por el origen. Sin embargo, una mejor estimación supone un mayor procesamiento de la señal, es decir, un mayor retardo y un mayor coste. Algunas recomendaciones de la ITU-T que abordan la cancelación del eco empleando filtros adaptativos son las recomendaciones G.165 Y g.168 [3].

2.2.6. Ancho de Banda

El ancho de banda (BW, BandWith) 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. Aunque los cálculos necesarios se estudiaran en una capitulo posterior, en general, el ancho de banda medio de la red debe ser tal que [3]:

$$BW = \frac{BW_{VOZ} + BW_{VIDEO} + BW_{DATOS}}{0{,}75}$$

De esta manera, nos dejamos un 25 % de margen para hacer frente a posibles picos de tráfico. Al dimensionar la red según este criterio, es decir, al garantizar que habrá ancho de banda suficiente para cursar las comunicaciones, se reduce la probabilidad de que el retardo, el jitter o las pérdidas tengan un impacto considerable. Sin embargo, esto no quiere decir, ni mucho menos, que sobredimensionando la red en cuanto a ancho de banda se refiere se resuelvan definitivamente los problemas de calidad. En todo caso, deberá hacerse un estudio de cada uno de los factores para tomar las medidas adecuadas [3].

Una comunicación de voz sin comprimir, por cada sentido de la comunicación consume 64 Kbps. Sin embargo, puesto que el ancho de banda es un recurso escaso (sobre todo porque se paga), sería deseable poder comprimir la voz y aumentar la eficiencia de utilización del ancho de banda cursando un mayor número de comunicaciones. Sin embargo, el precio a pagar es una disminución de la calidad. Aunque no existe ninguna relación directa entre el ancho de banda y calidad de la voz, en general, cuanto mayor es la compresión, menor es la calidad de la voz ya que la señal es más sensible a las perdidas y al retardo [3].

2.2.6.1 Supresión de silencios

Es un mecanismo complementario al empleo de los códec compresores para reducir el ancho de banda. Se trata de aprovechar el hecho de que en una conversación normal el 60 % del tiempo lo ocupan silencios debidos a las pausas para respirar y a la espera del turno en la comunicación. La idea es utilizar estos instantes en que el canal está libre, para introducir tráfico de otras conversaciones. De esta manera, se pueden obtener reducciones de hasta el 60 % en el flujo de paquetes. Estas técnicas reciben el nombre de detección de actividad de voz, supresión de silencios o VAD (Voice Activity Detection) [3].

La detección de actividad puede activarse en varios componentes de la red. Supongamos una red con una arquitectura toll by pass, una de las

configuraciones más comunes (ver figura 2-10). En este caso, existen seis puntos en los que podría activarse la VAD [3].

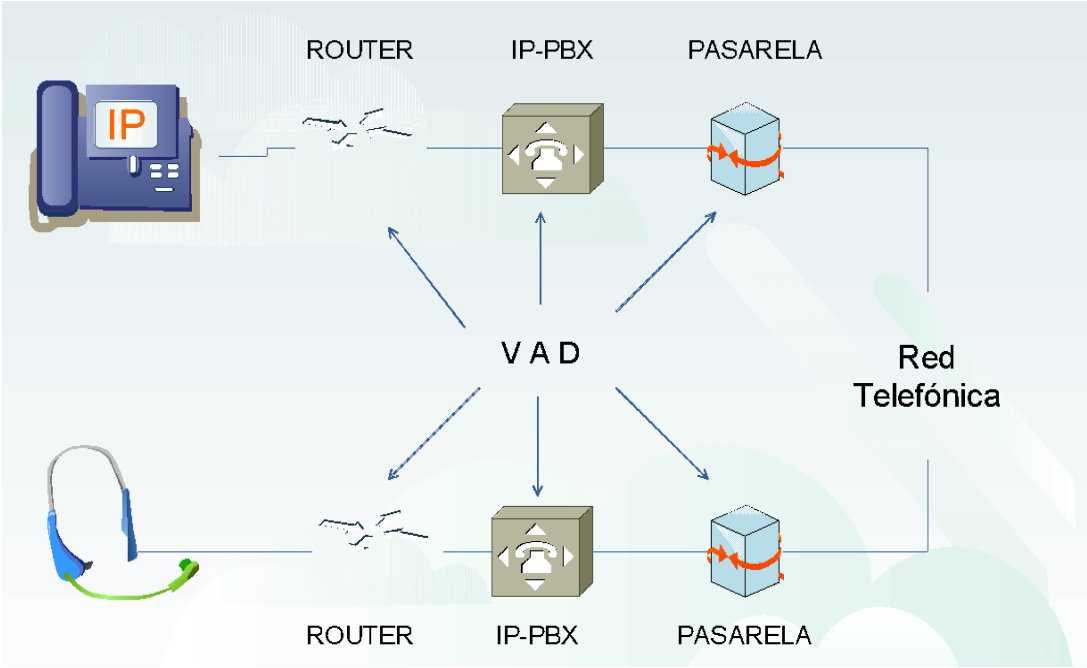


Figura 2- 10. Puntos en los que se puede activar el VAD.

Para evitar que el interlocutor piense que se ha cortado la comunicación durante los intervalos de silencio se envían periódicamente paquetes de silencio (SID, silence Insertion Description) durante la pausa. Estos paquetes proporcionan una indicación del nivel de ruido que existe en el origen para que el receptor lo simule en el terminal remoto mediante un generador de ruido (recomendaciones ITU-T I.366.2) [3].

Sin embargo, pese a que la supresión de silencios aporta beneficios en cuanto al ancho de banda empleado, también suele ser la responsable de un fenómeno conocido como clipping que consiste en que la voz del interlocutor parece

“recortada”. También las perdidas, la latencia y el jitter pueden producir este fenómeno [3].

2.3.-Medida de la calidad de la voz

Como veremos, la variedad de métodos y técnicas existentes que tienen como objetivo determinar la calidad de la voz es enorme. En general, todas ellas se suelen clasificar según dos criterios: su grado de intrusión en la red y su objetividad [3].

El grado de intrusión en la red hace referencia al modo en que el proceso de medida interacciona con dicha red. Según este criterio, podemos encontrar sistemas de medida intrusivos o activos y sistemas no intrusivos o pasivos [3].

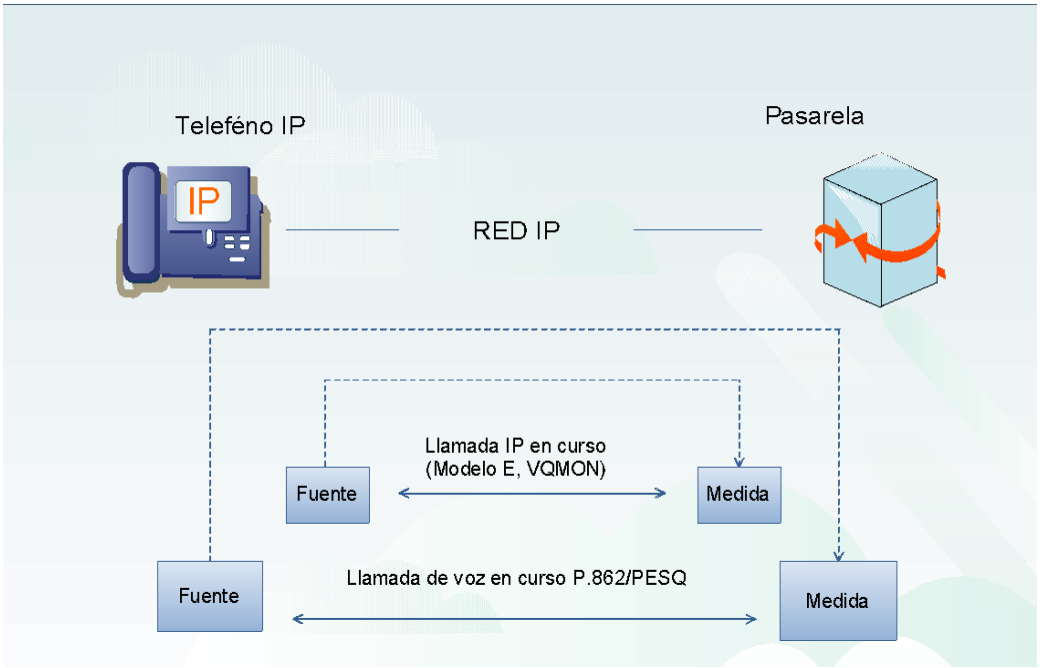


Figura 2- 11. Medida intrusiva o activa.

Los sistemas intrusivos consisten en el envío de una señal conocida a través de la red (llamada de prueba) y en la comparación entre la señal recibida y la transmitida para estudiar la degradación que introduce la red en la señal transmitida. Debido a la complejidad y al elevado coste de este tipo de técnicas,

no permiten su utilización para medidas en tiempo real aunque son ideales para la medida de prestaciones de un códec en el laboratorio. Además, durante el periodo de pruebas de red no transporta tráfico de usuarios y, por tanto, no genera negocio. Pertenecen a este grupo los estándares PSQM, PESQ y PAMS, entre otros (ver Figura 2-11) [3].

Los sistemas no intrusivos o pasivos, por su parte, efectúan medidas en tiempo real, mientras el sistema sigue en explotación sin interferir en las llamadas existentes, y sin necesidad de señal de interferencia (ver figura 2-12). El inconveniente es que por lo general, son menos exactas que las anteriores. Una variante muy útil de los sistemas de medición pasivos son los agentes embebidos que, por ejemplo, pueden incorporarse directamente en el gateway o en el propio teléfono IP. Medidas pasivas son las escalas MOS, el modelo E y VQMon [3].

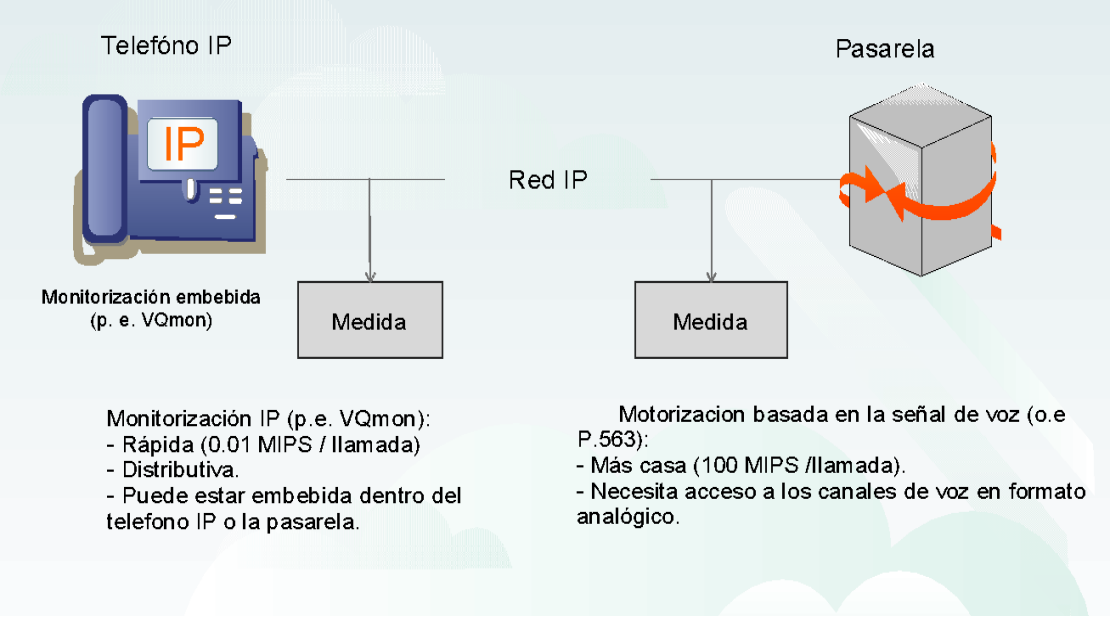


Figura 2- 12. Medidas no intrusivas o pasivas.

En cuanto a la objetividad de las medidas hace referencia a que tan independiente de la opinión de los sujetos es la calidad de la voz medida en un determinado conjunto de pruebas. Las primeras que aparecieron fueron las

medidas subjetivas consistentes simplemente en evaluar la calidad de la voz en base a las opiniones de un grupo lo suficientemente extenso de usuarios como para que los resultados sean estadísticamente relevantes. Sin embargo, se necesitaba una aproximación más ingenieril al problema que, por otra parte, permita evaluar la calidad de la voz en el laboratorio. La solución son modelos perceptuales de la voz que hacen posible la definición de modelos objetivos de evaluación de la calidad de la voz [3].

La figura 2-13 recoge una comparación entre las medidas de calidad de audio estandarizadas más extendidas. En las redes de telecomunicaciones en general y en las redes de voz sobre paquetes en particular, interesa utilizar códec de reducida tasa binaria ya que el ancho de banda es un recurso escaso [3].

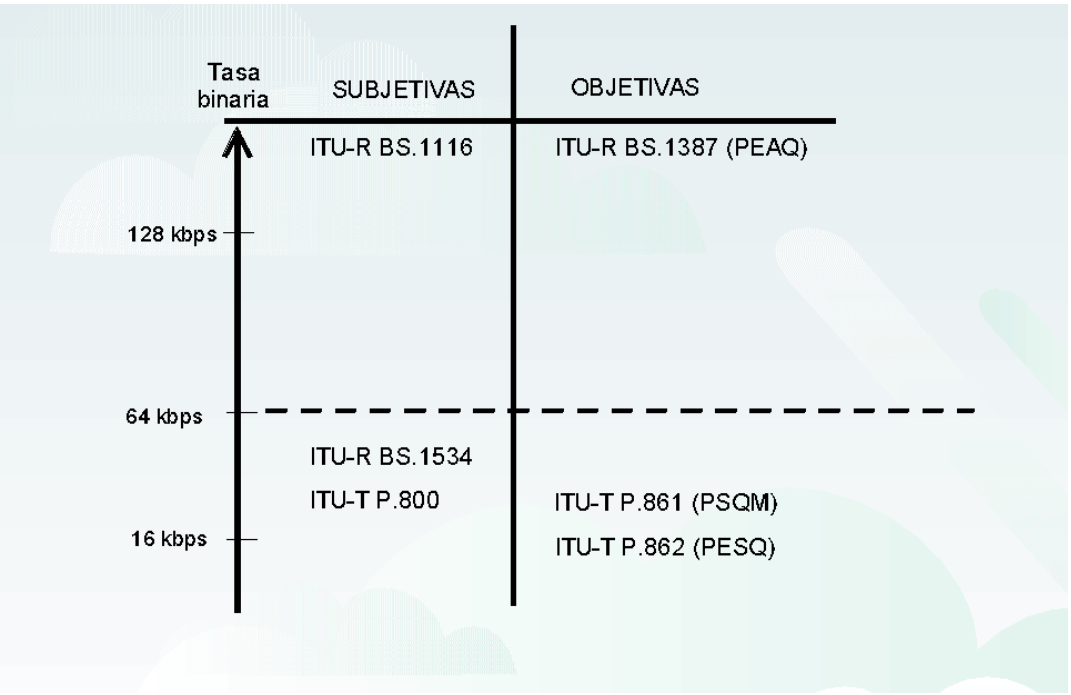


Figura 2- 13. Comparación entre estándares de la calidad de voz.

2.3.1 ITU-T P.800 (Escalas MOS)

Los mecanismos tradicionales empleados para la evaluación de la calidad de la voz en redes de telefonía fueron estandarizados por la ITU-T. Uno de ellos es la recomendación ITU-T P.800 que describe las escalas MOS y que se han venido utilizando para los códec de voz desde 1993. Se trata de un conjunto de técnicas subjetivas de la medida de la calidad de la voz reciben el nombre de test ACR (Absolute Category Rating) y que tienen el mismo esquema general: Se reúne a una muestra de usuarios a los que se pide que opinen sobre la calidad que en algún aspecto en concreto ofrece un determinado sistema de transmisión de la voz (ver figura 2-14) [3].

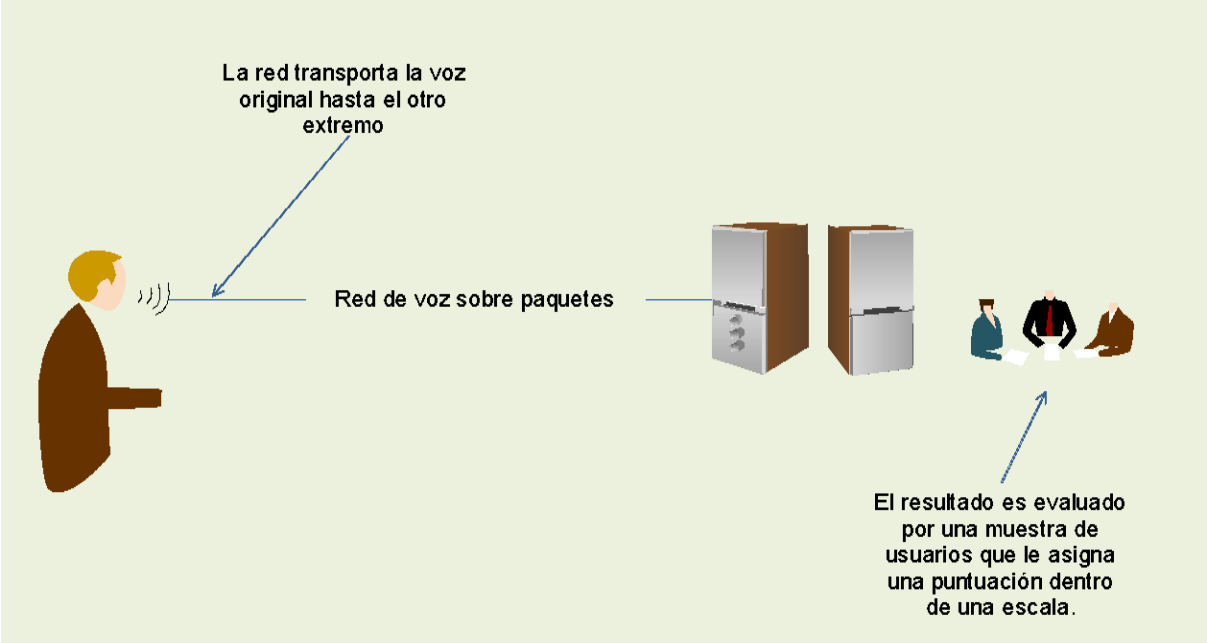


Figura 2- 14. Generación de las escalas MOS.

Los test ACR, a diferencia de lo que ocurren en el modelado perceptual, no utilizan la comparación con una señal de referencia. En realidad, esto es precisamente lo que ocurre en una conversación telefónica, en donde los

extremos no disponen de la voz original del otro extremo. Sin embargo, es necesario ajustar las opiniones de los distintos usuarios a una escala absoluta y por ello, previamente, se presenta a los usuarios unos ejemplos predefinidos que les proporcionan una base a la hora de evaluar la calidad de la voz. Estos ejemplos están recogidos en la recomendación P.810 (MNRU, Modulated Noise Reference Unit) [3].

Los aspectos que evalúan las escalas MOS son muy variados, sin embargo, los más comunes son, quizá, el de la calidad de la voz (tabla 1) y el que evalúa el esfuerzo requerido para entender el significado del mensaje pronunciado por el otro extremo (tabla 2) [3].

Tabla 1. Escala MOS utilizada para medir la calidad de la voz.

Puntuación	Calidad
5	Excelente
4	Buena
3	Aceptable
2	Pobre
1	Mala

Tabla 2. Escala MOS para medida del esfuerzo de interpretacion del mensaje.

Puntuación	Esfuerzo
5	Relajación completa: no es necesario ningún esfuerzo
4	Necesario prestar atención: no se requiere esfuerzo apreciable
3	Esfuerzo moderado
2	Esfuerzo considerable
1	Imposible de entender

Tabla 3. Escala MOS de calidad para los codecs más comunes.

Estándar de codificación	Valor MOS (velocidad)
G.711	4,4 (64 kbps)
G.726	3,8 (32 kbps)
G.728	3,6 (16 kbps)
G.729	3,7 (8 kbps)
G.723.1	3,9 (6,3 kbps)
	3,6 (5,3 kbps)

El principal inconveniente de las escalas MOS deriva de su propia concepción. En efecto par que sean realmente significativas es imprescindible que la muestra de usuarios sea suficientemente grande y ello encarece el proceso de elaboración. Además, al ser subjetivas dependen en gran cantidad de factores como la predisposición la actitud de los usuarios frente a la prueba o el nivel cultural de los individuos. Sin embargo, tienen la ventaja de que los patrones de comportamiento humanos son sobradamente conocidos y, en algunos casos, resulta sencillo determinar los efectos de las perdidas y del retardo en una muestra de usuarios relativamente reducida.

2.3.2 Modelado perceptual de la voz

Las técnicas preceptúales o psicoacusticas se basan en el modelado de la respuesta del oído humano y la introducción a dicho del modelo de una señal de referencia y de la señal de entrada cuya calidad desea evaluarse y que proporciona una representación paramétrica de ambas señales (ver figura 2-15). Seguidamente, se someten a un proceso de comparación del que se obtiene una estimación de la diferencia audible. Esta debe ser procesada de la misma manera en que lo haría el odio humano en un test con individuos y para ello se utiliza un modelo cognitivo que, finalmente, dará como resultado la calidad de la voz [3].

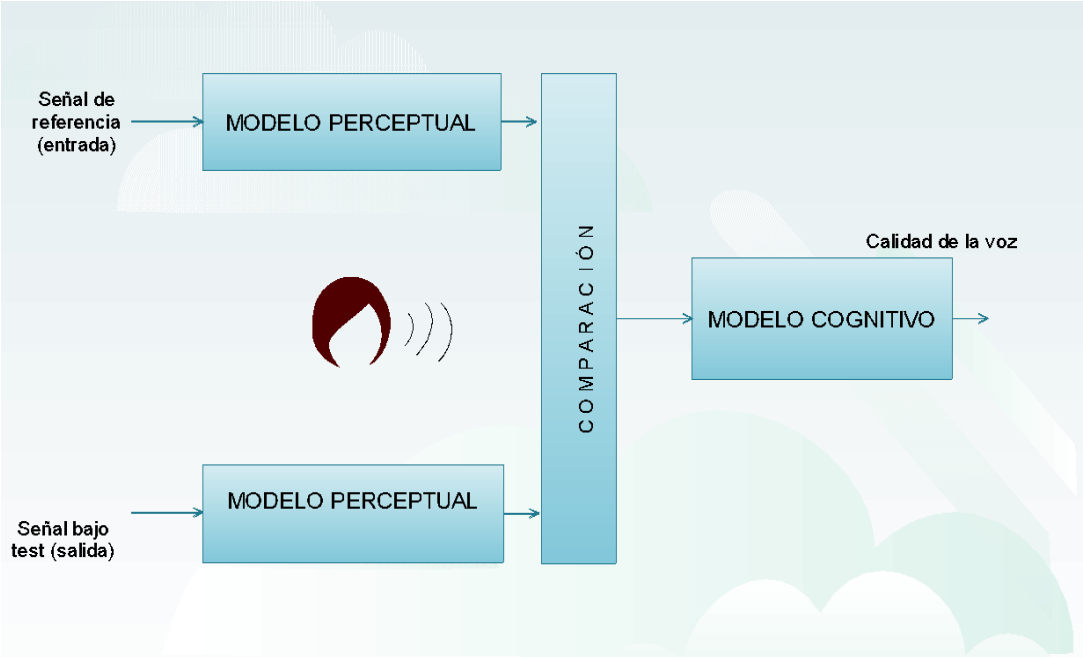


Figura 2- 15. Modelo perceptual de la voz.

2.3.2.1. Psicoacustica

El comportamiento del sistema auditivo humano es altamente no lineal. En efecto, únicamente somos sensibles a aquellos sonidos comprendidos dentro de un rango de amplitudes y frecuencias (rango dinámico) muy concreto, siendo esta sensibilidad dependiente de la frecuencia, de manera que se define un área de audición (ver figura 2-16) [3].

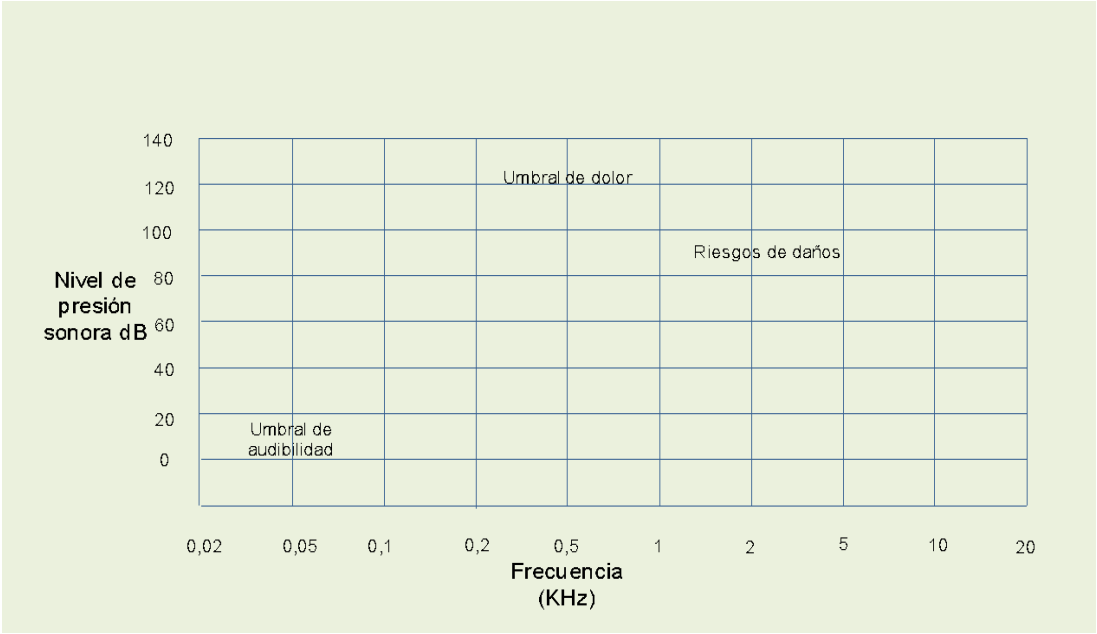


Figura 2- 16. Área de audición del ser humano.

Por otra parte, el espectro audible se divide en zonas denominadas bandas críticas o bark, hasta un total de 25 bark. Cada uno de estos bark se caracteriza porque el nivel de sonoridad es constante en toda la banda de frecuencias que comprende. El ancho de cada banda crítica es aproximadamente constante e igual a 100 Hz por debajo de los 500 Hz y de alrededor del 20 % de la frecuencia central, para valores por encima de los 500 Hz [3].

La precepción de un sonido es un fenómeno muy complejo y en el que se ven implicados gran cantidad de parámetros. El primero de ellos es el umbral de audición, que se define como el nivel de presión sonora mínimo para producir una sensación en el oído humano. Por debajo de ese valor, el sonido pasara desapercibido [3].

El umbral de audición no es constante, ni siquiera para el mismo sujeto, que varía en función de la frecuencia y de la presencia o ausencia de otros sonidos. Esta posibilidad de que un sonido quede oculto por la ocurrencia de otros se conoce

con el nombre de enmascaramiento y puede ser de tres tipos (ver figura 2-17) [3].

Enmascaramiento simultaneo: Las señales enmascarante y enmascarada ocurren el mismo instante de tiempo o con una diferencia tan pequeña que puede considerarse despreciable [3].

Pre-enmascaramiento: El sonido enmascarado ocurre entre 5 y 20 ms antes que el enmascarante [3].

Postenmascaramiento: El sonido enmascarado ocurre entre 50 y 200 ms después que el enmascarante [3].

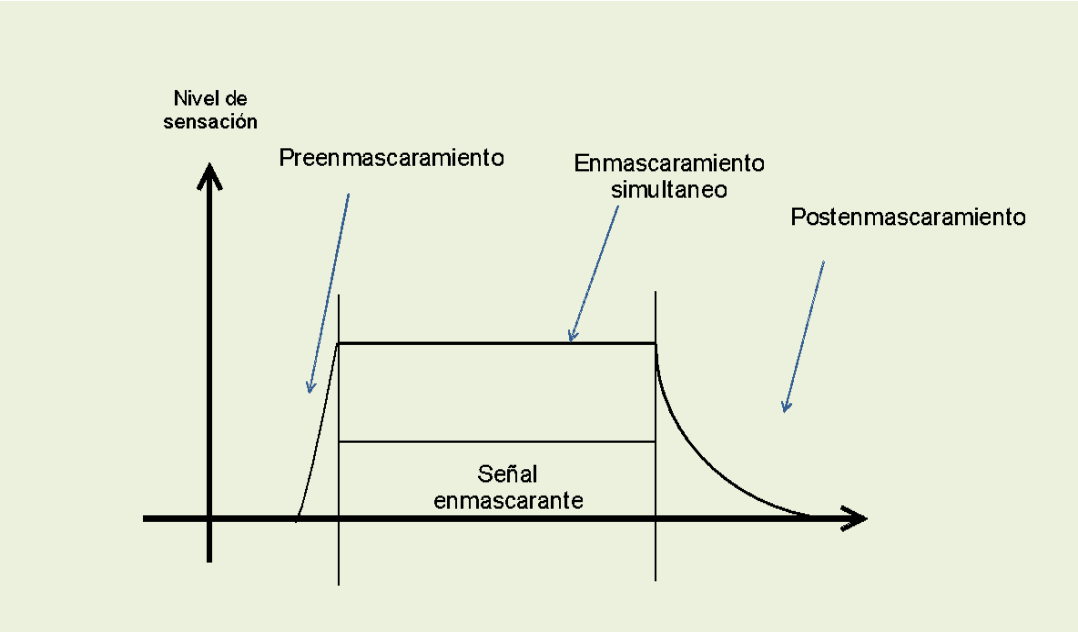


Figura 2- 17. Tipos de enmascaramiento.

Este fenómeno se aprovecha en algunos codificadores para comprimir, todavía más la señal, evitando transmitir las señales enmascaradas puesto que no se oirán [3]. Tal es el caso de la codificación de audio MPEG.

Además de los parámetros anteriores, existen algunos otros que también se emplean en la caracterización subjetiva de la percepción sonora, los más importantes son los siguientes [3]:

Roughness y fluctiation strength: Miden el índice de modulación de señal en amplitud y frecuencia [3].

Sharpness: Indica el contenido de alta frecuencia del sonido (es decir, su color), de tal manera que cuanto mayor es el sharpness, tanto mayor es aquel [3].

Toality: Representa la riqueza total del sonido y suele ser proporcional a la percepción sonora [3].

2.3.2.2. ITU-T P.861 (PSQM)

En 1996 el grupo de estudio SG12 de la ITU acabo la recomendación P.861 para el análisis objetico de los códec de voz basado en un algoritmo denominado PSQM (Perceptual Speech Quality Mesaure). PSQM es una versión de otro algoritmo con carácter más general, el PAQM (perceptual Audio Quality Audio Measure), utilizado en señales telefónicas. A diferencia de este último, PSQM considera los efectos psicoacusticos en la percepción de la calidad del sonido [3].

El diagrama de bloques de la figura 2.18 muestra cómo se calcula la calidad de la voz según el algoritmo empleado por PQSM. En primer lugar, se convierte la representación temporal de las señales x, y al dominio de la frecuencia dividiéndolas en bloques y obteniendo su FFT (Fast Fourier transform). Seguidamente, las muestras de frecuencia se enventanan y la escala frecuencial se transforma a barks o bandas críticas, proceso que se conoce con el nombre de frequency warping. Una vez hecho esto, tanto la señal bajo test como la señal de referencia se filtran con un modelo del dispositivo receptor (auriculares, altavoces, etc.) y se añade al resultado un ruido Hoth que simula el ambiente de oficina convencional. Restando las dos representaciones de la señal, se dispone de una estima del error audible en función del timbre y del tiempo [3].

Este algoritmo se utiliza para códecs con tasas binarias comprendidas entre los 8 Kbps y los 16 Kbps. Sin embargo, las medidas PSQM fueron diseñadas para analizar solo los efectos de la comprensión / descomprensión llevadas a cabo por el códec y no tiene en cuenta las degradaciones causadas por la red como consecuencia de las pérdidas o el jitter de paquetes [3].

Figura 2- 18. Algoritmos PSQM.

2.3.2.3. ITU-T P.862 (PESQ)

Cuando se estandarizo PSQM como la recomendación P.861 los esfuerzos se centraban, sobre todo, en los códec de voz empleados en comunicaciones móviles como GSM y su aplicación a VoIP se consideraba algo lejana. Sin embargo, las redes de próxima generación, como son las de voz sobre paquetes, han cambiado drásticamente las necesidades y la ITU se ha visto obligada a revisar estándares de medición de la calidad, dado que en este tipo de redes el efecto predominante es el retardo y no a distorsión, como ocurre en los códec GSM. El resultado fue el algoritmo PESQ (Perceptual Evaluation of Speech Quality) y que fue incluido en 2001 dentro de la recomendación P.862 [3].

PESQ, en realidad, es una evolución de otro algoritmo, el PSQM+. Este último resolvía las distorsiones producidas por las ráfagas de error, pero todavía

presentaba problemas a la hora de compensar las variaciones del retardo. Por otro lado, MT desarrollo un algoritmo, el PAMS, que manejaba la variabilidad del retardo a la perfección. PESQ combina ventajas de ambos aunque tiene el inconveniente de que no está concebido para aplicaciones de streaming. La Figura 2-19 muestra el diagrama de PESQ [3].

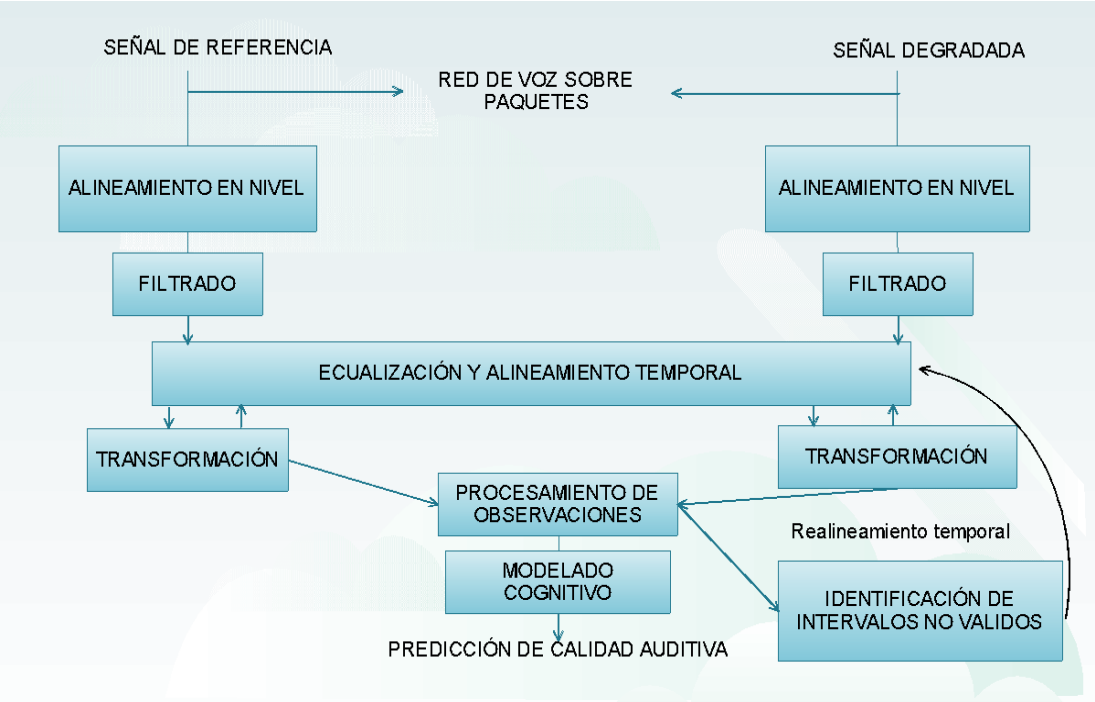


Figura 2- 19. Algoritmo PESQ.

Su principal inconveniente es que no está diseñado para aplicaciones de streaming. Sin embargo, las medidas PESQ son directamente trasladables a las escalas MOS con muy pocas manipulaciones. En realidad, las escalas PESQ están comprendidas entre 1,0 (peor puntuacion) y 4,5 (mejor puntuacion), ya que los usuarios, en general, son bastantes cautos a la hora de asignar el 5, es decir, calidad excelente, incluso cuando no existe degradación alguna en la señal [3].

2.4. Modelo E

El modelo E es una aproximación matemática a la medida de la calidad de la voz basada en la evaluación de las características de transmisión de la red de voz sobre paquete y cuyo objetivo es predecir la calidad de la voz en función del retardo, el jitter , las perdidas y otras características de la red [3].

El modelo E está especificado en la recomendación ITU-T G.107 y estipula que la calidad de la voz puede evaluarse a través del parámetro R, definido como

$$R = R_0 - I_S - l_d - I_e + A$$

El termino R_0 hace referencia a la relación señal-a-ruido mientas que I_s modela la degradación que sufre la señal como consecuencia de su conversión a un formato adecuado para su transmisión en la red. Los otros tres términos son el efecto de las perdidas (I_E), del retardo (I_d), y el margen de seguridad (A), que hora analizaremos con más detalle. En cualquier caso, la recomendación proporciona una expresión mucho más simple si se considera en la anterior los valores por defecto y que es [3]:

$$R = 94{,}2 - l_d - I_e$$

Como se verá en un apartado posterior, el retardo es uno de los factores más importantes a considerar cuando se estudia la calidad de la voz. Su impacto en el modelo E está representado por el parámetro I_d que en redes IP es función del retardo extremo a extremo [3]:

$$I_d = 0.024 * d + 0.11 * (d - 177.3) * (d - 177{,}3)$$

Donde H(x) es la función de Heavyside:

$$H(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}$$

Si se representa gráficamente esta relación (ver figura 2.20), se concluye que en torno a los 175 ms un aumento del retardo supone una disminución drástica de

la calidad de la voz, algo que concuerda con la recomendación ITU-T G.114 en la que se aconseja que los valores del retardo en un solo sentido no superen valores comprendidos entre 150 ms y 200 ms [3].

Otro de los factores que influyen en la calidad de la voz son las perdidas cuyo impacto se modela atravesó del parámetro I_e (recomendación ITU-T G.133). En general, cuanto mayor es el valor de I_e, tanto mayor es la disminución de la calidad [3].

Por fin, la salida del modelo E es el factor de transmisión, R a partir del cual puede obtenerse un valor en la escala MOS de la calidad de la voz (ver figura 2.20) [3].

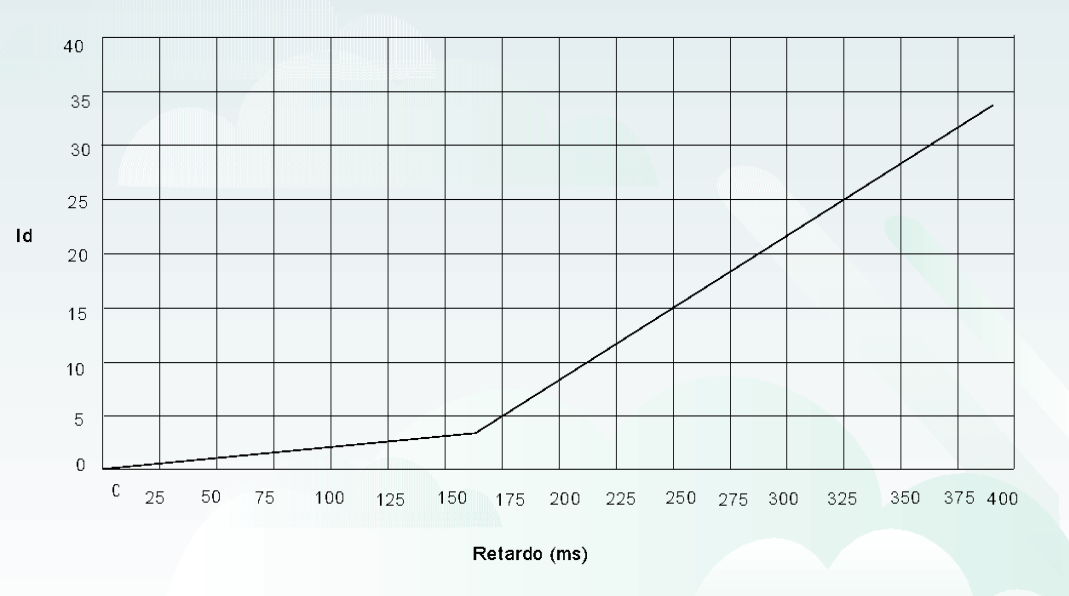


Figura 2- 20. Id en función del retardo.

Figura 2- 21. Evaluación de la calidad de la voz a partir del modelo E.

En el caso concreto de redes IP, el factor de transmisión R y la escala MOS están relacionados a través de la siguiente expresión [3]:

$$MOS = \begin{cases} 1 & R < 0 \\ 1 + 0{,}035 * R + 7 * R * \ (R - 60) * M\ (100 - R) * 10^{-6} & 0 < R < 100 \\ 4{,}5 & R > 100 \end{cases}$$

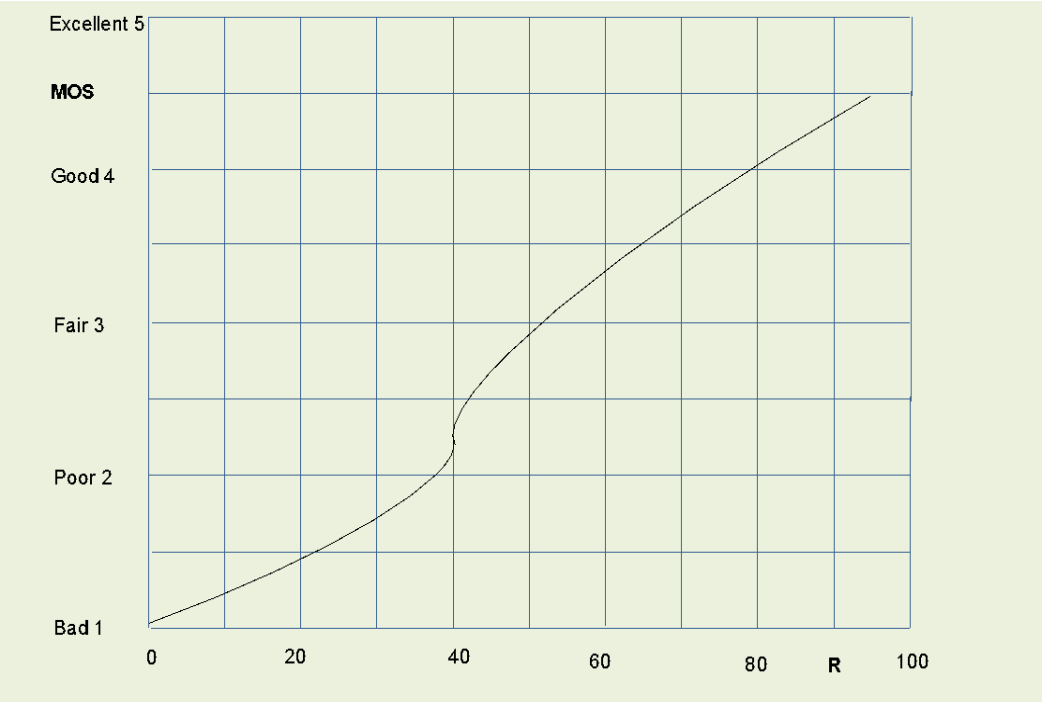


Figura 2- 22. Relación entre el modelo E y las escalas MOS en paquetes IP.

De la gráfica de la Figura 2-22 se deduce que, puesto que el valor máximo de R es 94,2 la calidad nunca podrá ser mayor de 4,4 y que cualquier procesamiento de la voz produce una degradación de la calidad [3].

2.5. VQMon

De todas las medidas vistas hasta ahora, ninguna satisface adecuadamente las necesidades de proveedores de servicios de VoIP. Gran parte de ellas se basan en comportamiento en medida de la red obtenido tras mediciones de largo plazo de parámetros como el jitter, las perdidas y el retardo que, por otro lado, son difíciles de relacionar con la calidad que perciben los usuarios en llamadas individuales. Son necesarios, pues, otros tipos de medidas que superen estos inconvenientes [3].

Uno de los más recientes es VQMon (Voz Quality Monnitoring) desarrollado por la empresa Telchemy. No tiene en cuenta directamente los aspectos de la codificación de la señal, pero analiza la degradación que introduce la red (jitter,

pérdidas y retardo) y predice el impacto en la señal de voz reconstruida. VQMon permite medir, en tiempo real, la calidad de la voz para todas las llamadas que estén en curso en un determinado instante [3].

Generalmente, las medidas de calidad suelen hacerse en los puntos finales de la comunicación de VoIP, es decir, en los gateways, en el caso de una arquitectura toll-by-pass o en los propios terminales de usuarios si la VoIP esta implementada extremo a extremo. Esta información resulta extremadamente importante, no solo porque la calidad determina la percepción que los usuarios tienen del servicio que les ofrece la red, sino también porque es un dato necesario a la hora de llevar a cabo el correcto dimensionamiento del sistema [3].

Una de las características más interesante de VQMon es que emplea un modelo estadístico para el análisis de las degradaciones que introduce la red que considera la voz tal y como el usuario la percibe, en lugar de emplear valores medios en la red entera o en un segmento de la misma. Por ejemplo, VQMon, no mide la tasa de perdidas si no también la distribución. Varios estudios han concluido que para una cierta tasa de perdidas, la degradacion de la calidad de la voz es mucho mayor si las pérdidas se producen a ráfagas. Además, VQMon tambien explota la memoria a corto plazo de los seres humanos que nos lleva a conceder mayor importancia a las degradaciones recientes frente a las que ocurrieron antes [3].

Capitulo III: Protocolos de señalización H.323 y SIP.

3.1. INTRODUCCION

En este capítulo se describe el funcionamiento de los protocolos de señalización H.323 y SIP, con el fin de que en un entorno laboral o de investigación se puedan comprender los mensajes que cada protocolo de señalización pudiera enviar.

Primeramente, empezamos con el protocolo H.323 que es una especificación de la unión internacional de telecomunicaciones (UIT.T) se define que es H.323 cuál es su arquitectura y cuáles son sus elementos más importantes con la explicación de sus características o más bien que papel tienen estos elementos dentro de la red H.323 y como se logra el funcionamiento de este protocolo.

Seguidamente tenemos el siguiente protocolo de señalización en este caso el protocolo SIP que actúa en una relación de cliente servidor, este es un protocolo desarrollado por MMUSIC DEL IETF (Internet Engeneering task force) una organización internacional que tiene como objetivo contribuir a la ingeniería de internet en diferentes áreas, también se explica a detalle los elementos de SIP así como sus funciones básicas y los mensajes que se proporcionan durante la transmisión de una llamada, esto con el fin de que se pueda saber su significado a la hora de establecer el escenario controlado para las pruebas pertinentes.

3.2. H.323

H.323 es una especificación del sector de normalización de las telecomunicaciones Unión Internacional de Telecomunicaciones (UIT-T) para la transmisión de audio y video y datos a través de una red de protocolo de internet (IP), incluyendo el internet. Cuando se cumple con H.323, los productos y aplicaciones de los vendedores pueden comunicarse entre sí. El estándar H.323 se ocupa de la señalización y el control de llamadas y el control del ancho de banda para conferencias punto a punto y multipunto. La serie H de recomendaciones también especifica H.320 para la red digital integrada (ISDN) y H.324 para el servicio telefónico antiguo (POTS) como mecanismo de transporte [1].

El estándar H.323 consiste en los siguientes componentes (Figura 3-2) y protocolos que se muestran (Figura 3-1).

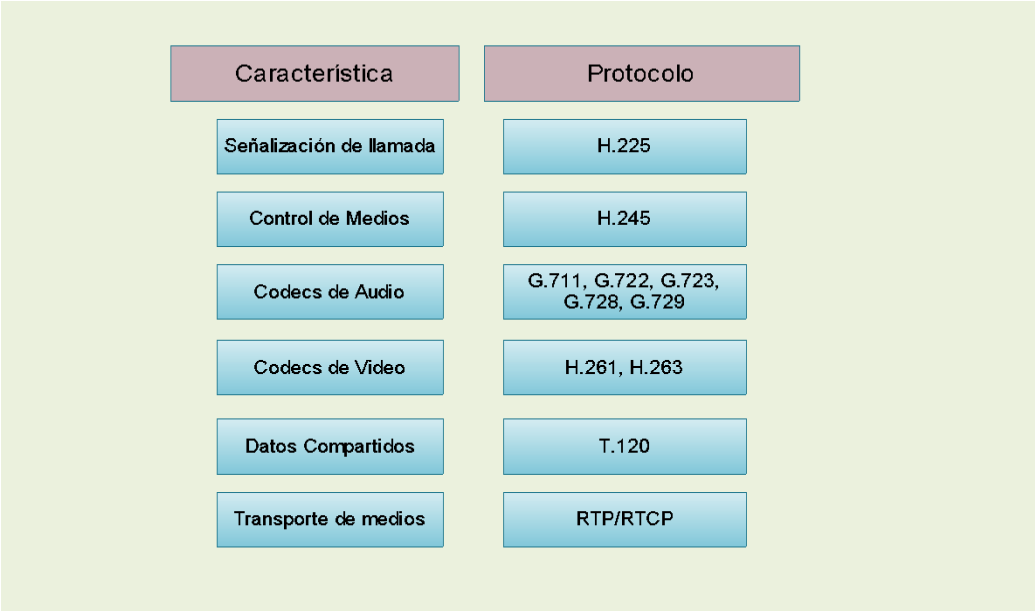


Figura 3- 1. Características y protocolos de H.323

El sistema H.323 se discute en las siguientes 3 secciones.

-
- Elementos H.323
- Conjunto de protocolos H.323
- H.323 Flujos de llamadas

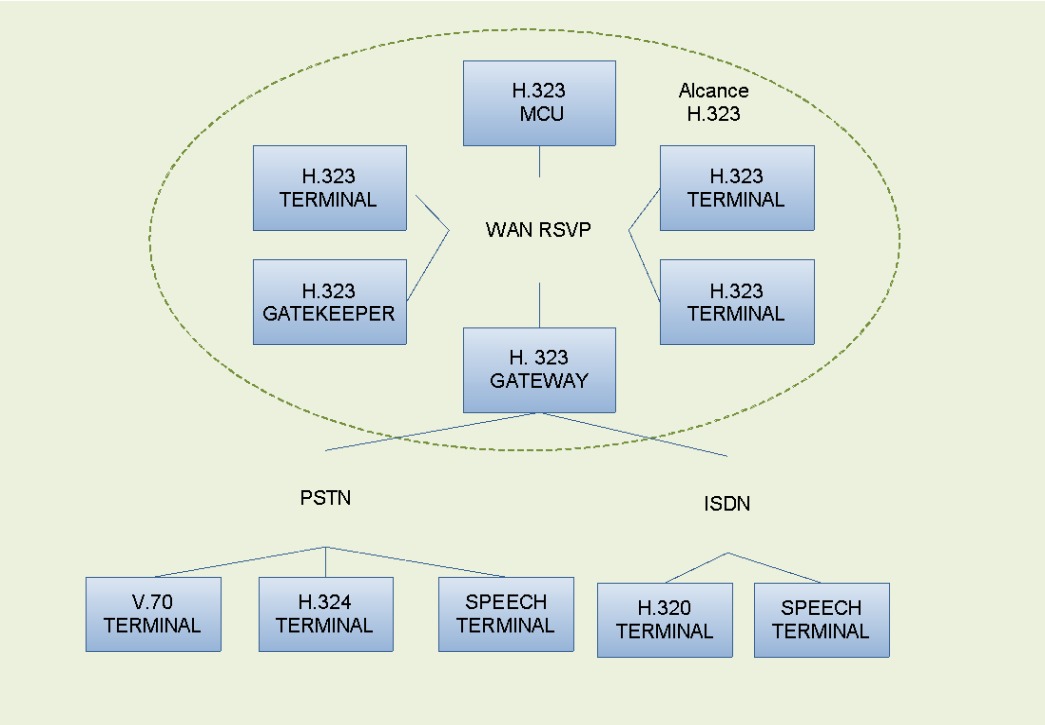


Figura 3- 2. Elementos de la red H.323.

3.2.1 Descripción del sistema

A menudo se refiere como criterios de valoración, las terminales proporcionan audio para conferencias punto a punto y multipunto, opcionalmente, video y datos. Los Gateways se interconectan con la red telefónica publica conmutada (PSTN) o redes RDSI H.323 para el interfuncionamiento del punto final. Los Gatekeepeer proporcionan el control de admisión y servicios de traducción de dirección de terminales o Gateway. MCUs son dispositivos que permiten a dos o más terminales o gateway que permite a dos o más terminales o gateway conferencias ya sea con sesiones de video o audio [1].

3.2.1.1. Terminal.

Es el elemento de la red que se ilustra en la figura 3-3 debe tener una unidad de control del sistema, la transmisión de medios de comunicación, códec de audio, y la interfaz de red de paquetes. Requisitos opcionales incluyen un códec de video y aplicaciones de datos de usuario [1].

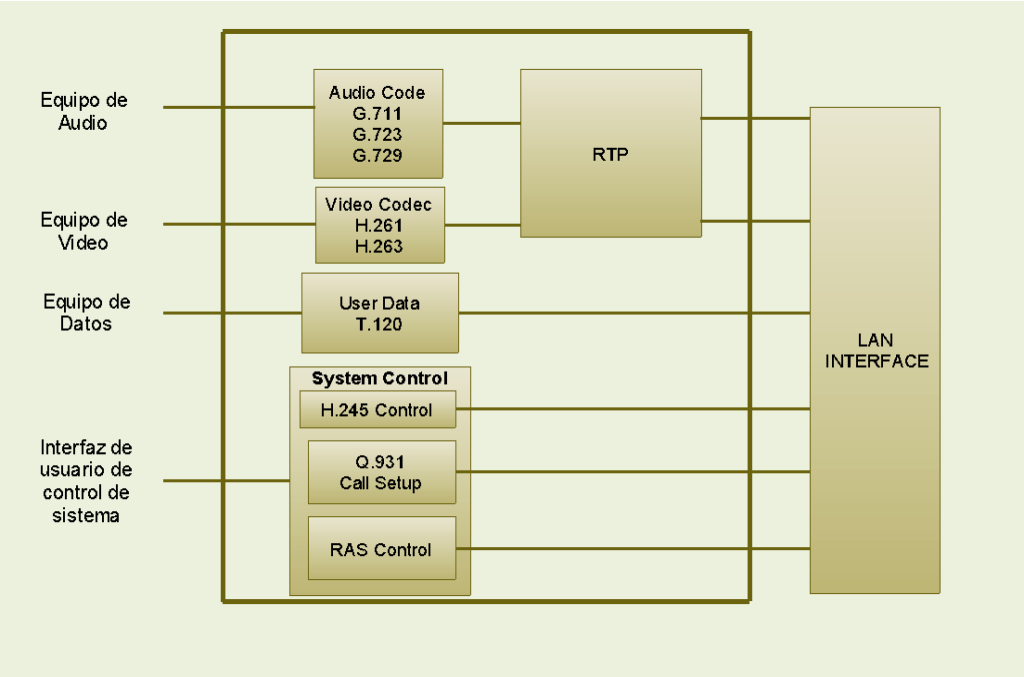


Figura 3- 3. Relaciones de los componentes de H.323.

System Control Unit (Unidad de control del sistema): Proporciona H.255 y H.245 llamada de control, intercambio de capacidades, mensajería, y la señalización de comandos para el correcto funcionamiento del terminal [1].

Media transmisión (Medios de transmisión). Formatos del video, datos, flujos de control y mensajes de interfaz de red de audio transmitidos. Media transmisión

también recibe el audio y video, datos flujos de control y los mensajes de la interfaz de red [1].

Audio Códec (Códec de audio). Codifica la señal desde el equipo de audio para la trasmisión y decodifica el código del audio entrante, funciones requeridas incluyen la codificación y decodificación de voz G.711 y transmitir y recibir law-a y law-u opcionalmente, G.722, G.723.1, G.728, G.729 y la codificacion y decodificación son soportados [1].

Network interface (Interface de red). Una interfaz basada en paquetes puede soportar el protocolo de control de transmision (TCP) y el unicast user datagram (UDP) y los servicios de multidifusión [1].

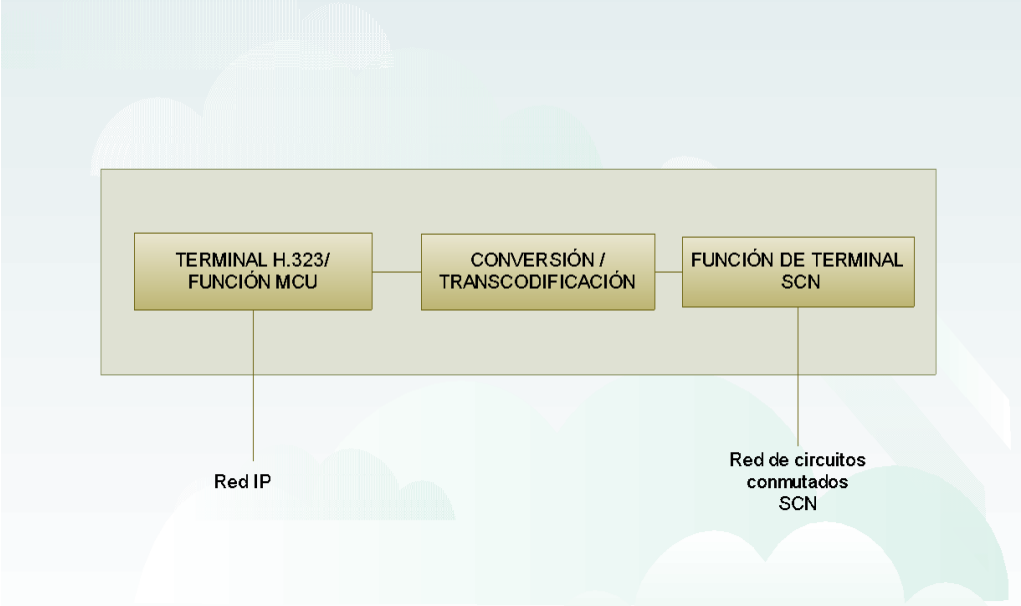
Video Códec (Códec de video). Opcional, pero si existe, debe ser capaz de codificar y decodificar video de acuerdo con Quarter Comment Intermediate Format H.261 (QCIF) [1].

Data Channel (Canal de datos). Soporta aplicaciones tales como acceso a la base de datos, transferencia de archivos, y las conferencias audiograficos (La capacidad de modificar una imagen comun sobre los ordenadores de varios usuarios simultaneamente). Tal como se especifica en la recomendación T.120 [1].

3.2.1.2. Gateway

El Gateway H.323 refleja las características de un punto final en la red conmutada de circuitos (SCN) y el punto final H.323. Se traduce entre audio, video y formatos de transmisión de datos, así como los sistemas de comunicación y protocolos. Esto incluye el establecimiento de llamada y el desmontaje tanto en la red IP y el SCN [1].

No se necesitan puertas de enlace a no ser que se requiera la interconexión con la red SCN. Por lo tanto, los puntos extremos H.323 pueden comunicarse directamente a través de la red de paquetes sin necesidad de conectarse a un gateway. El gateway actúa como un terminal H.323 o MCU en la red y un terminal SCN o MCU en el SCN, como se ilustra en la Figura 3-4 [1].



3-4. Elementos de un Gateway de H.323

3.2.1.3. Gatekeeper

Una función opcional, el gatekeeper proporciona servicios de control pre llamada y de nivel de llamada a los puntos extremos H.323. Los gatekeepers están separador lógicamente de los otros elementos de la red en entornos H.323 si se implementa más de un Gatekeeper, la intercomunicación se lleva a cabo de forma indeterminada [1].

Un gatekeeper si está presente en un sistema H.323, debe realizar lo siguiente:

Traducción de direcciones: Proporciona direcciones IP de punto final de alias H.323 (como pc1@cisco.com) o direcciones E.164 (números de teléfono estándar) [1].

Admisión de control. Proporciona acceso autorizado a H.323 utilizando la solicitud / admisión, confirmación/ admisión, rechazo/ admisión (ARQ/ACF/ARJ) los mensajes analizados en la sección “Señalización RAS” más adelante en este capítulo [1].

Zone Management (Manejo de la zona). Provista de terminales registradas, Gateway, MCUs se analiza en la sección RAS más adelante del capítulo. [1].

3.2.1.4. EL MCU y elementos

El controlador multipunto (MC) soporta conferencias entre tres o más puntos extremos en una conferencia multipunto. MCs transmiten el conjunto de capacidades a cada punto final de la conferencia multipunto y pueden revisar las capacidades durante la conferencia. La función MC puede ser residente en un terminal, Gateway, gatekeeper o MCU [1].

El proceso multipunto (MP) recibe audio, video y/o datos de flujos y los distribuye a los puntos finales que participan en una conferencia multipunto [1].

La MCU es un punto final que soporta conferencias multipunto y, como mínimo, consiste en un MC y uno o más MPs. Si soporta conferencias multipunto centralizadas, una MCU típica consta de un MC y un audio, video y datos MP [1].

3.2.1.5. Servidor proxy H.323

Un servidor proxy H.323 es un proxy diseñado específicamente para el protocolo H.323. El proxy opera en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los proxis pueden determinar el destino de una llamada y realizar la conexión si se desea. El proxy es compatible con las siguientes funciones principales [1].

Las terminales que no soportan el protocolo de reserva de recursos (RSVP) se puede conectar a través de las redes de acceso o de área local (LAN) con relativamente buena calidad de servicio (QoS) para el proxy. Pares de proxys pueden negociar QoSs adecuada para hacer un túnel a través de la red IP. Proxies pueden administrar QoS con trozos de RSVP y/o de procedencia IP [1].

La representación de apoyo al transporte de trafico H.323 a través del enrutamiento de aplicación específica (ARS) [1].

Un proxy es compatible con la traducción de las direcciones de red, permitiendo a los nodos H.323 para ser desplegado en redes con espacio de direcciones privadas [1].

Un proxy desplegado sin un servidor de seguridad o de forma independiente de un servidor de seguridad proporciona seguridad de forma que solo el trafico H.323 pasa a través de él. Un proxy desplegado en conjunción con un servidor de seguridad para configurar simplemente para pasar todo el tráfico H.323 trata

al proxy como un nodo de confianza. Esto permite que el servidor de seguridad proporcionar redes de datos de seguridad y el proxy para proporcionar seguridad H.323 [1].

3.2.3. Conjunto de protocolos H.323

El conjunto de protocolos H.323 se basa en varios protocolos, como se ilustra en la figura 3-5. La familia de protocolos de admisión de llamadas, es compatible con la configuración, el estado, el desmontaje, los flujos de medios y mensajes en los sistemas H.323. Estos protocolos son compatibles con ambos mecanismos de entrega de paquetes fiables y no fiables a través de redes de datos [1].

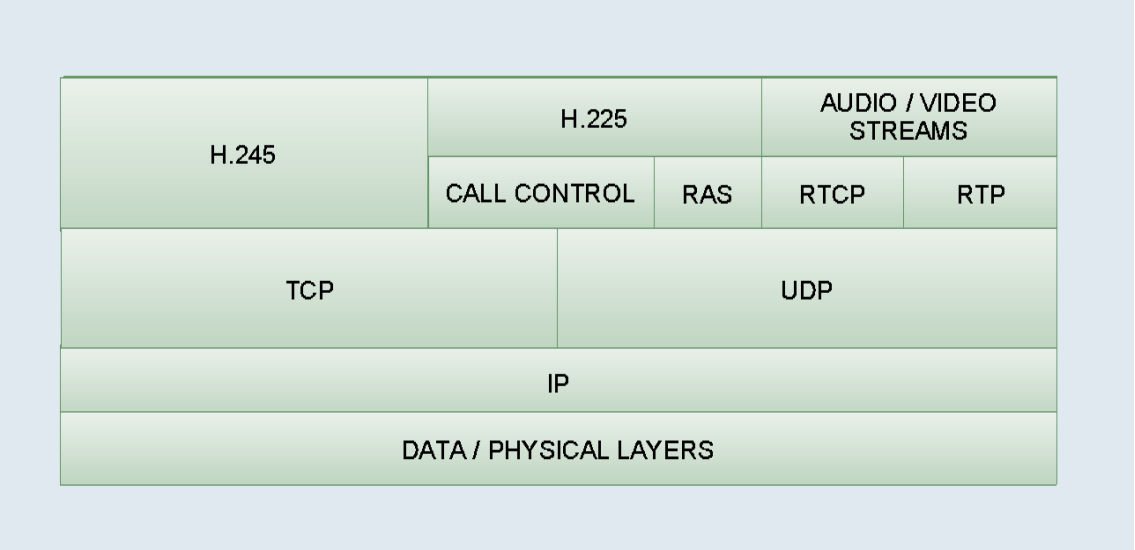


Figura 3-5. Capas de la suite de protocolos de H.323

Aunque la mayoría de las implementaciones H.323 hoy utilizan TCP como mecanismo de transporte para la señalización la versión H323 versión 2 no permite UDP básica [1].

Registro, admisión y estado señalización (RAS): proporciona control pre llamada en las redes basadas en gatekeeper H.323 [1].

Control de señalización de llamada. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales [1].

Control de medios de comunicación y transporte. Proporciona el canal H.245 fiable que lleva los mensajes de control de los medios de comunicación. El transporte se produce con un flujo UDP no fiable [1].

3.2.3.1 Señalización RAS

La señalización RAS proporciona un control pre llamada en las redes H.323 en las que existen Gatekeeper y una zona. Se establece el canal RAS entre los puntos finales y los Gatekeeper a través de una red IP. El canal de RAS se abre antes de establecer cualquier otro canal y es independiente de los canales de transporte de señalización de control de llamadas y medios de comunicación. Esta conexión UDP no fiable lleva los mensajes RAS que realizan el registro, admisión, cambios de ancho de banda, y el estado [1].

3.2.3.2. Descubrimiento de gatekeeper

El descubrimiento de un gatekeeper es un proceso manual o automático que usan para identificar que Gatekeeper los puntos finales. En el método manual, los puntos finales están configurados con la dirección IP del Gatekeeper y por lo tanto, se puede intentar el registro de inmediato, pero solo con el Gatekeeper predefinido. El método automático permite que la relación entre los puntos finales y los gatekeepers cambiar con el tiempo y requiere un mecanismo conocido como la detección automática [1].

La detección automática permite a un punto final, que puede no conocer Su gatekeeper, para descubrir su gatekeeper utiliza un mensaje de multidifusión. Debido a que los puntos finales no tienen que ser configurados o reconfigurados de forma estática para gatekeeper, este método tiene menos gastos administrativos. La dirección de descubrimiento multidifusión para gatekeeper es 224.0.0.41, el puerto de descubrimiento de gatekeeper es 1718, y el registro del gatekeeper es 1719 [1].

Los siguientes tres mensajes RAS se utilizan para el descubrimiento automático de H.323 gatekeeper [1].

Solicitud Gatekeeper (GRQ). Un mensaje de multidifusión enviado por un punto extremo que mira para el gatekeeper [1].

Confirma Gatekeeper (GCF). La respuesta a un punto final GRQ indica la dirección de transporte de canal RAS del Gatekeeper.

Rechazar Gatekeeper (GRJ). Avisa a un punto final que el gatekeeper no quiere aceptar su registro. Esto es generalmente debido a una configuración en el Gateway o en el gatekeeper [1].

La figura 3-6 ilustra los procesos de mensajería y de secuenciación para la detección automática [1].

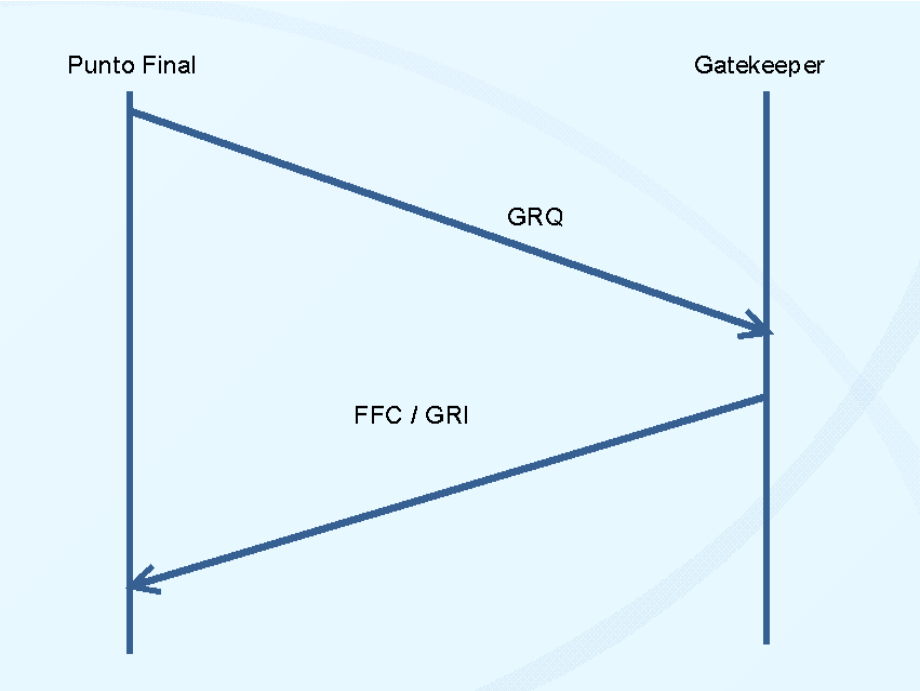


Figura 3-6. Descubrimiento automático de Gatekeeper.

3.2.4. **Registro**

El registro es el proceso que permite a los gateways, puntos finales, y MCUs unirse a una zona e informar al Gatekeeper de sus direcciones IP y alias. Un proceso necesario, el registro se produce después de que el proceso de descubrimiento, pero antes de que se pueda intentar alguna llamada. Se pueden

utilizar los siguientes seis mensajes para permitir que un punto final se registre y cancele el registro [1].

Solicitud de registro (RRQ). Se envía desde el punto final a la dirección de canal del gatekeeper.

Confirmar El registro (RCF). Enviado por el gatekeeper y confirma un registro por puntos finales [1].

Rechazar el registro (RRJ). Enviado por el gatekeeper y rechaza el registro de puntos finales [1].

Eliminar registro de solicitud (URQ). Enviado desde un punto final o gatekeeper para cancelar un registro [1].

Confirmar cancelar registro (UCF). Enviado desde el punto terminal o gatekeeper para confirmar una anulación [1]. Anular el registro rechazar (URJ). Indica que el punto final no fue registrarse previamente con el gatekeeper [1].

La figura 3-7 ilustra los procesos de mensajería y de secuenciación para el registro de un punto final y punto final [1].

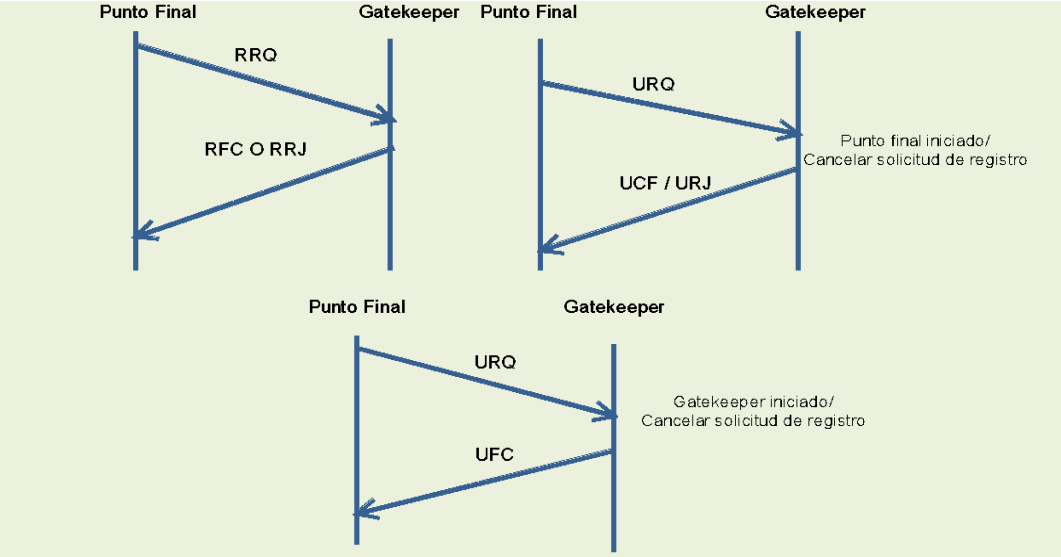


Figura 3-7. Proceso de mensajería y secuenciación para el registro de un gatekeeper y punto final.

3.2.4.1. Localización del punto final.

Los puntos finales y los gatekeepers usan la localización de puntos finales para obtener información de contacto cuando solo la información de alias está disponible. Ubica los mensajes que son enviados a la dirección del canal RAS del gatekeeper o multicas del descubrimiento de la dirección multicast del gatekeeper [1].

El gatekeeper es responsable de la respuesta de punto final deseado, con indicación de su cuenta o información de contacto de punto final [1].

El punto final o gatekeeper puede incluir una o más direcciones E.164 fuera de la zona en la solicitud. Se pueden utilizar los siguientes tres mensajes para localizar los puntos finales [1]:

LRQ. Enviado para solicitar la información de contacto de punto final o Gatekeeper de una o más direcciones E.164 [1].

LCF. Enviado por el gatekeeper y contiene el llamado canal de señalización o la dirección del canal RAS de si mismo el punto final deseado.

Rechazar Ubicación (LRJ). Enviado por gatekeeper que reciben un LRQ para los cuales la solicitud de puntos finales no registrados o no tiene recursos disponibles [1].

3.2.4.2 Admisiones

Los mensajes de admisión entre los puntos finales y los gatekeeper proporcionan la base para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a las redes H.323 mediante la confirmación o rechazo de una solicitud de admisión. Una solicitud de admisión incluye el ancho de banda solicitado, que el gatekeeper puede reducir en la confirmación [1].

Los siguientes mensajes proporcionan admisión y controlan las redes H.323 [1].

ARQ. Un intento por parte de un punto final por iniciar una llamada.

ACF. Una autorización por el gatekeeper para admitir una llamada.

ARJ. Niega la petición del punto final para obtener acceso a la red para esta llamada.

El mensaje ACF contiene la dirección IP de la puerta del Gateway o del gatekeeper y permite al Gateway de origen para iniciar de inmediato los procedimientos de señalización de control de llamadas [1].

3.2.4.3. Información de Estado.

El gatekeeper puede utilizar el canal RAS para obtener información de estado desde un punto final. Puede utilizar este mensaje para supervisar si el punto final está en línea y fuera de línea debido a una condición de fallo. El periodo de votación típico de los mensajes de estado es de 10 segundos. Durante la ACF, el gatekeeper también puede solicitar enviar que el punto final envía mensajes de estado durante una llamada. Se pueden utilizar los siguientes tres mensajes [1]:

Solicitud de información (IRQ). Enviado desde el gatekeeper a la condición de punto extremo solicitante [1].

Respuesta de solicitud de información (TIR). Enviado desde el punto final al controlador de acceso en respuesta a un IRQ. Este mensaje también se envía desde un punto final si el gatekeeper solicita actualizaciones periódicas de estado [1].

Consulta de estado. Enviado fuera del canal RAS en el canal de señalización de llamada. Un punto extremo o el gatekeeper pueden enviar mensajes de estado una solicitud a otro punto final para verificar el estado de la llamada. Los gatekeeper suelen utilizar estos mensajes para verificar si las llamadas están todavía activos [1].

3.2.5. Control de ancho de banda.

El control de ancho de banda se logró inicialmente a través del intercambio de admisión entre un extremo y el gatekeeper dentro de la secuencia ARQ/ACF/ARJ. El ancho de banda puede cambiar durante la llamada, sin embargo. Se pueden utilizar los siguientes mensajes para cambiar el ancho de banda [1].

BRQ. Enviado por un punto final al controlador de acceso que solicita un aumento o disminución en el ancho de banda de la llamada.

BCF. Enviado por el Gatekeeper confirmando la aceptación de la solicitud de cambio de ancho de banda.

OIJ. Enviado por el Gatekeeper donde rechaza la solicitud de cambio de ancho de banda (enviado si el ancho de banda no está disponible).

Nota.

El control de ancho de banda está limitado en su alcance a solo el gatekeeper y Gateway y no toma en cuenta el estado de la red en sí misma. El gatekeeper actualmente solo se fija en su tabla de ancho de banda estática para determinar si debe aceptar o rechazar la solicitud de cambio de ancho de banda [1].

3.3 SIP

SIP es el protocolo especificado IETF para iniciar una comunicación de dos vías sesión. Es considerado por algunos como más simple que H.323, a pesar de que es ahora el RFC más grande en la historia del IETF. SIP está basado en texto; evitando así la Cuestiones de análisis ASN.1 asociada que existen con el conjunto de protocolos H.323, siS / MIME no se usa como parte de SIP medidas de seguridad inherente . Además, SIP es un protocolo de nivel de aplicación, es decir, que se desacopla de la capa de protocolo que es transportados a través. Se puede realizar por TCP, UDP, SCTP . UDP se puede utilizar para disminuir los gastos generales y aumentar la velocidad y la eficiencia, o TCP puede ser utilizado si SSL / TLS se incorpora a los servicios de seguridad. Implementaciones más nuevas pueden utilizar protocolo de transmisión de control de flujo (SCTP), desarrollado en el SIGTRAN del IETF grupo de trabajo (RFC 2,960) específicamente para el transporte de los protocolos de señalización. SCTP ofrece una mayor resistencia a ataques DoS a través de un método de protocolo de enlace de cuatro vías, la capacidad de multi-hogar, y la agrupación opcional de múltiples mensajes de usuario en un paquete SCTP sola. Servicios de seguridad adicionales pueden ser usados con SCTP a través de RFC 3436 (TLS SCTP) o 3554 (SCTP sobre IP Sec). A diferencia de H.323, un solo puerto se utiliza en SIP (H.323 en cuenta que también se puede utilizar de

una manera que utiliza un solo puerto - Dirigir las llamadas enrutadas). El valor predeterminado para este puerto es 5060 [2].

3.3.2 Arquitectura SIP

La arquitectura de una red SIP es diferente de la estructura H.323. Una red SIP se compone de puntos finales, un proxy y/o un servidor redirector, servidor de localización y registrador. Un diagrama se proporciona en la figura 3-8, EN el modelo de SIP, un usuario no está unido a un host especifico (ni es el caso de H.323, gatekeeper ofrece resolución de direcciones). El usuario reporta inicialmente su ubicación a un registrador, que pueden ser integrados a un proxy o a un proxy redirector. Esta información a su vez está almacenada en el servidor de localización externo [2].

Los mensajes de los puntos finales deben direccionarse a través de un proxy o al servidor de redirección. Intercepta los mensajes de los puntos el servidor proxy u otros servicios, inspecciona su “para”. El campo contacto para resolver el nombre de usuario dentro de una dirección para resolver el nombre de usuario y enviar los mensajes a lo largo del apropiado punto final o algún otro servidor [2].

Los servidores de redirección realizan la misma funcionalidad de resolución, pero la responsabilidad es colocada en los puntos finales para llevar a cabo la transmisión real. Es decir, de re direccionamiento de servidores de obtener la dirección real de destino desde el servidor de localización y devolver esta información al remitente original, que luego debe enviar su mensaje llamadas enrutadas directos directamente a esta dirección resulta (similares a H.323 con portero) [2].

El propio protocolo SIP se basa en el método de protocolo de enlace de tres vías implementado en TCP (ver Figura 3-10).

Tendremos en cuenta la configuración aquí cuando un servidor proxy se utiliza para mediar entre los puntos finales. El proceso es similar con un servidor de redirección, pero con el paso adicional de devolver la dirección resuelta al punto

final de origen. Durante el proceso de instalación, detalles de comunicación se negocian entre los puntos extremos utilizando sesión descripción protocolo SDP, que contiene campos para el códec utilizado, el nombre de la persona que llama, etc [2].

Si Bob desea realizar una llamada a Alice él envía una petición INVITE al servidor proxy que contiene información SDP para el periodo de sesiones, que luego es enviada al cliente Alice por el servidor proxy de Bob. Finalmente, en el supuesto de que Alice quiere hablar con Bob, se enviara un mensaje OK de nuevo que contiene sus preferencias de llamada en formato SDP [2].

Entonces Bob responderá con un “ACK”. SIP prese la ACK para contener en lugar SDP de la invitación, por lo que un INVITE puede verse sin protocolo específico de información. Después de que se recibió el “ACK”, la conversación puede comenzar a lo largo de los puertos RTP/RTCP previamente acordados. Tenga en cuenta que todo tráfico era transportado a través de un puerto en un formato simple (texto), sin ningún complicado cambio de canal / puerto asociado con H.323, Todavía SIP presenta varios desafíos para los firewalls y NAT.

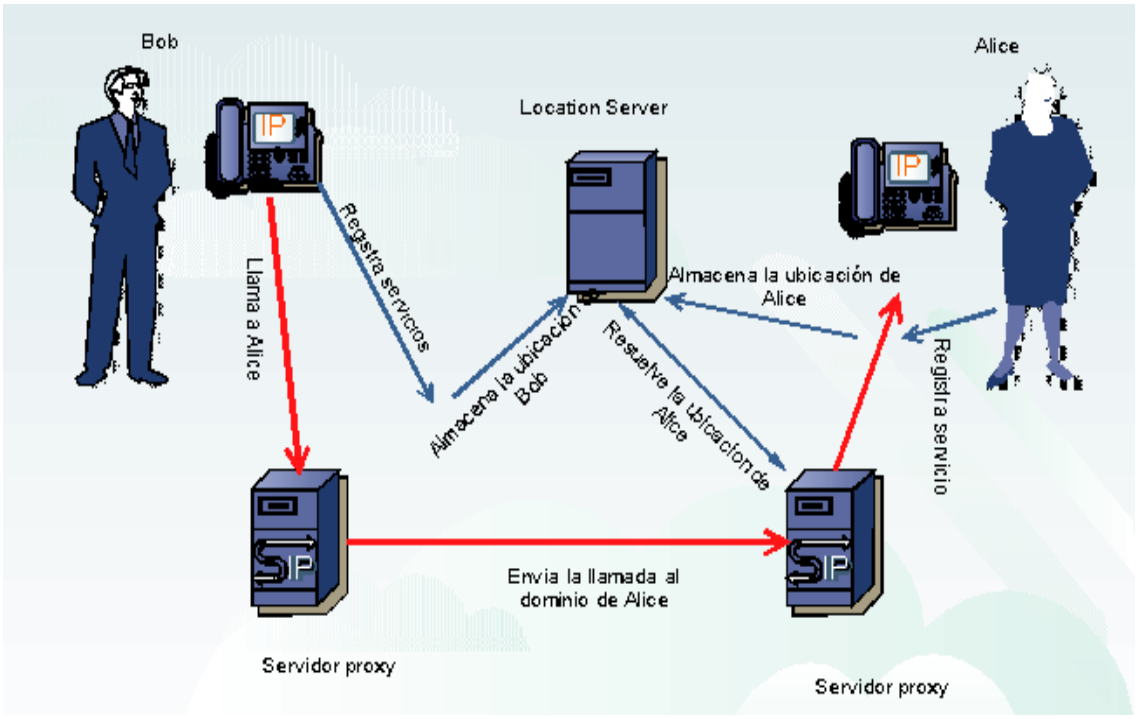


Figura 3-8. Arquitectura de red SIP.

3.3.3 Operación del protocolo SIP

Este subtema describe a SIP con detalle, describe como la funcionalidad de SIP se logra: Es decir, los mensajes que intercambian entre las diferentes entidades SIP y cuáles son sus formatos de mensaje. Se examinarán múltiples ejemplos de cómo funciona SIP. Estos ejemplos suelen consistir en un flujo de mensajes que le dan una imagen global de la operación SIP [5].

Sin embargo, también se incluye ejemplo en el que el lector puede ver todos los mensajes a detalle, incluyendo cabeceras de los mensajes, parámetros y descripción de sesiones [5].

3.3.3.1 Transacciones Cliente / Servidor

SIP se basa en el protocolo Web Hypertext Transfer Protocol (HTTP) y como HTTP, SIP en un protocolo de petición / respuesta. Para entender utilizado en SIP, tendremos que examinar las siguientes definiciones del cliente y el servidor [5].

Un cliente es una entidad SIP que genera peticiones. Un servidor es una entidad SIP que recibe las solicitudes y devuelve respuestas. Esta terminología se hereda de HTTP, en el que el navegador web contiene un cliente HTTP. Cuando escribo una dirección en mi navegador WEB como http://www.accessmhtelecom.com, estoy enviando una solicitud a un servidor WEB en particular. El servidor WEB envía de nuevo una respuesta a la información solicitada, es decir la pagina WEB de grupo editorial de telecomunicaciones de McGraw-Hill [5].

SIP se ajusta a los mismos procedimientos siguiendo la misma terminología, cuando dos agentes de usuario intercambian mensajes SIP, el agente de usuario (UA) ENVIA SOLCITUDES ES EL CLIENTE DE AGENTE DE usuario (UAC) y la UA regresa respuestas de del Servidor de agente de usuario (UAS), estas se llaman transacción SIP [5].

3.3.4 RESPUESTAS SIP

Tras la recepción de una solicitud, el servidor emite una o varias respuestas. Cada respuesta tiene un código que indica el estado de la transacción. Estados de los códigos son números enteros que van desde 100 a 699 y se agrupan en clases como se muestran en la tabla 4 [5].

Tabla 4. Clases de respuesta SIP

SIP: Operación de Protocolo	
Rango	Clase de respuesta
100-199	Informativo
200-299	Éxito
300-399	Redirección
400-499	Error del cliente
500-599	Error de servidor
600-699	Falla global

Una respuesta con un código de estado 100 a 199 se considera provisional. Las respuestas 200 a 699 son respuestas finales. Una transacción SIP entre cliente y un servidor comprende una solicitud desde el cliente, uno o más respuestas provisionales, y una respuesta final [5].

Junto con el código de estado, las respuestas SIP llevan una frase razón. Este último contiene información legible sobre el código de estado. Por ejemplo, un código de estado de 180 significa que el usuario invitado a una sesión es ser alertados. Por lo tanto, la frase razón podría contener un “Ringing”. [5].

La tabla 5-2 contiene todos los códigos de estado definidos actualmente con sus frases asociados por defecto [5].

Tabla 5. Codigos de respuesta SIP

100	**trying (Tratando)**	**413**	**Request entity too large**
180	Ringing	414	Request URL too large
181	call is being forwarded	415	Unsupported media type
182	Queued	420	Bad extension
183	Session progress	480	Temporarily not avaliable
200	ok	481	Call leg / transaction does not exist
202	Acepted	482	Loop detected
300	Multiple choices	483	Too many hops
301	Moved permanently	484	Address incomplete
302	Moved temporarily	485	Ambiguous
305	Use proxy	486	Busy here

380	Alternative service	487	Request cancelled
400	Bas request	488	Not acceptable here
401	Unauthorized	500	Internal server error
402	Payment required	501	Not implemented
403	Forbidden	502	Bad gateway
404	Not found	503	Servide unavaliable
405	Method not allowed	504	gateway time-out
406	Not acceptable	505	SIP version nos supported
407	Proxy authentication required	600	Busy everywhere
408	Request time-out	603	Decline
409	Conflict	604	Does not exist anywhere
410	Gone	606	Not aceptable
411	Length required		

3.3.5 Las solicitudes SIP

Las especificaciones núcleo de SIP definen 6 tipos de solicitudes, cada uno de ellos con un propósito diferente. Cada petición SIP contiene un campo. Llamado método, que denota u propósito. La lista muestra los seis métodos [5].

- INVITE
- ACK
- OPTIONS
- BYE
- CANCEL
- REGISTER

Ambas solicitudes y respuestas pueden contener organismos SIP. El cuerpo de un mensaje es su carga útil. Cuerpos SIP suelen consistir en una descripción de la sesión [5].

INVITE INVITE las solicitudes invitan a los usuarios a participar en una sesión. Los cuerpos de las solicitudes de INVITE contiene la descripción de la sesión. Por ejemplo, cuando Bob llama a Laura, su UA envía un INVITE con una descripción de la sesión a la UA de Laura. Supongamos que la UA de Bob utiliza Sesion Desription Protocol (SDP) para describir el periodo de sesiones. Su UA recibe el INVITE con la siguiente descripción de la sesión [5].

o=Bob 2890844526 2890842807 IN IP4 131.160.1.112
s=I want to know how you are doing
c=IN IP4 131.160.1.112
t=0 0
m=audio 49170 RTP/AVP 0

La invitación recibida por la UA de Laura significa que Bob está invitando a Laura a unirse a una sesión de audio. A partir de la descripción de la sesión realizada en el INVITE, UA de Laura sabe que Bob quiere recibir paquetes del protocolo de transporte en tiempo real (RTP) que contiene la voz de Laura en 131.160.1.112 datagramas de usuario Numero de puerto de protocolo (UDP) 49170 [5].

Su UA también sabe que Bob puede recibir un Pulse Code Modulation (PCM) de voz codificada. (RTP/AVP0 en la línea m indica PCM) UA de Laura comienza alertando a Laura y devuelve una respuesta “180 timbre” para la UA de Bob. Cuando Laura finalmente acepta la llamada, su UA devolverá un “200 Aceptar la respuesta”, con una descripción de la sesión en el mismo [5].

v=0
o=Laura 2891234526 2812342807 IN IP4 138.85.27.10
s=I want to know how you are doing
c=IN IP4 138.85.27.10
t=0 0
m=audio 20000 RTP/AVP 0

En este punto, Laura acepta la llamada e informa a Bob que lo hara recibir paquetes RTP en 138.85.27.10 puerto UDP 20.000 (Figura 3-9) [5].

Si, cuando Laura y Bob están en medio de la sesión, uno de ellos desea modificar el periodo de sesiones, solo tienen que emitir un nuevo INVITE. Este tipo de INVITE, llamado re-INVITE, lleva una descripción de sesión actualizada [5].

Podría consistir en nuevos parámetros tales como números de puerto para el vigente medio de comunicación, o podría añadir nuevos flujos de medios. Por ejemplo, Bob y Laura puede agregar una secuencia de video a su conversación de voz a través de una re-INVITE [5].

Significativamente, SIP solo se ocupa de la invitación para el usuario y la aceptación del usuario invitado [5].

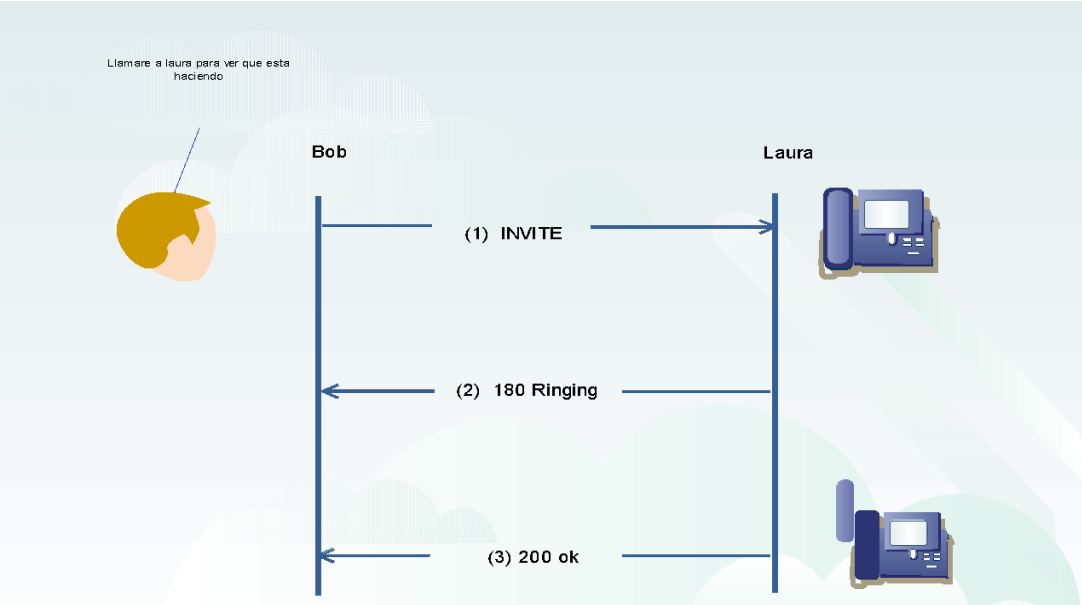


Figura 3- 9. Laura emite una respuesta final (200 OK) por a invitación recibida.

ACK las solicitudes ACK se utilizan para reconocer la recepción de una respuesta final a una invitación. Así, un cliente que origina una solicitud INVITE emite una solicitud de ACK cuando recibe una respuesta final para el INIVITE, proporcionando un saludo de tres vías: INVITE de respuesta final ACK (Figura 3-10) [5].

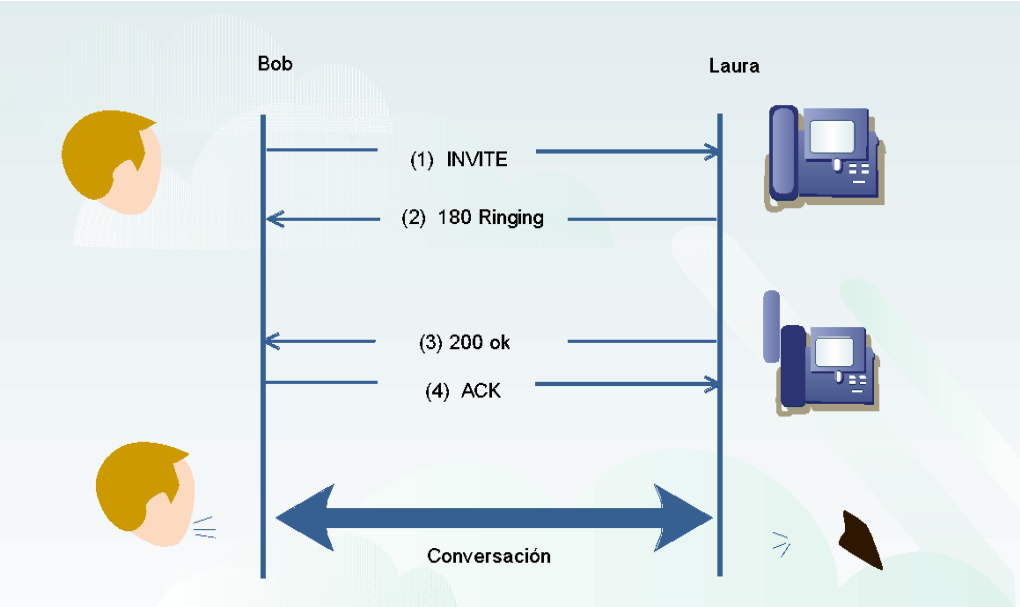


Figura 3- 10. Saludo de tres vías: Invite-200 OK-ACK.

3.3.5.1¿Por qué SIP utiliza un saludo de tres vías?

INVITE es el único método que utiliza el saludo de tres vías en lugar de un enlace de dos vías (Método de respuesta final). Ciertas características marcan el método INVITE, aparte de otro método. Cuando un cliente envía una solicitud de otro INVITE, que espera una respuesta rápida del servidor. Sin embargo, la respuesta de una solicitud INVITE puede tardar mucho tiempo [5].

Cuando Bob llama a Laura, ella puede tener que demorar en tomar su teléfono SIP y pulsar los botones, así que el “200 ok” respuesta que vendrá más o menos retrasado. Él envió ACK desde el cliente al servidor permite saber que el cliente todavía está allí y que la sesión se ha establecido con éxito [5].

El saludo de 3 vías también permite la implementación de la bifurcación proxy. Cuando uno estos tenedores de una solicitud, el cliente emitió que la solicitud obtendrá varias respuestas de diferentes servidores. Él envió de un ACK para todos los destinos que han respondido es esencial para el funcionamiento de SIP y para asegurar a través de protocolos no fiables como UDP [5].

CANCEL cancelar peticiones, cancelar transacciones pendientes. Si un servidor SIP ha recibido una invitación, pero aún no ha devuelto una respuesta final, se detendrá el procesamiento de la invitación a la recepción de un CANCELAR. Si, sin embargo, tiene ya una respuesta final para la solicitud INVITE, CANCEL no tendrá ningún efecto en la transacción [5].

En la Figura 3-11 Bob llama a Laura y su teléfono SIP comienza a sonar, pero nadie contesta a tiempo. Bob decide colgar. EL envía CANCEL de su solicitud INVITE anterior. Tras la recepción del CANCEL, Deja de sonar el teléfono SIP de Laura. El servidor devuelve una respuesta OK 200 para cancelar, lo que indica que se ha procesado correctamente [5].

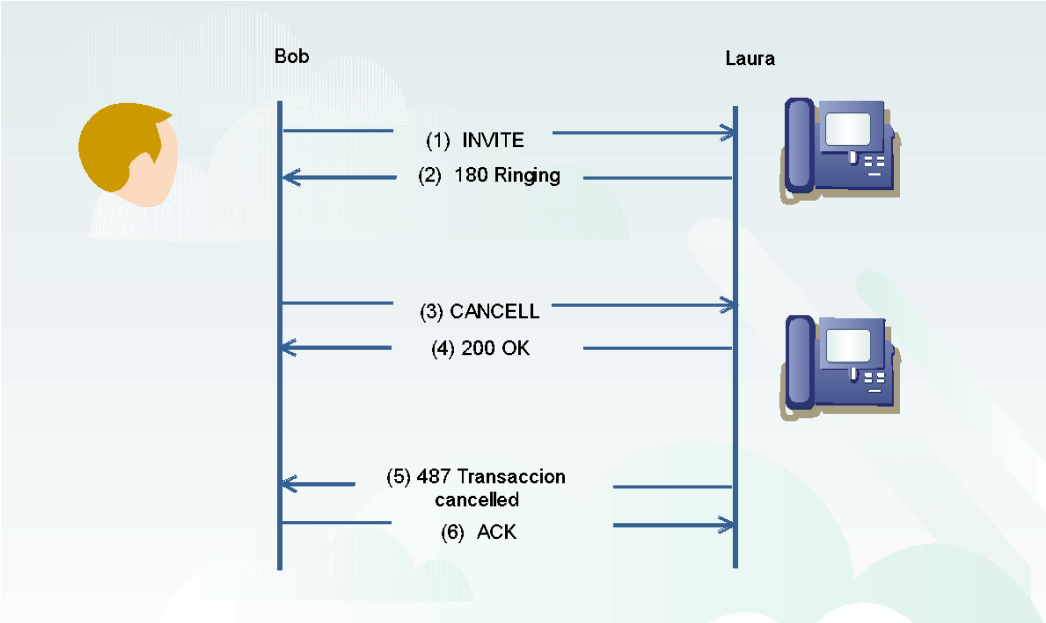


Figura 3-11. Bob cancela si INVITE (Invitación).

Es importante señalar que después de que el servidor ha respondido a la solicitud CANCEL, responde a la anterior INVITE, se envía una “487 transacción cancelada” y el cliente termina el saludo de 3 vías enviando un ACK (INVITE-487 Transacción Cancelada-ACK). Por lo tanto, el INVITE de 3 vías se realiza siempre, incluso cuando se cancela la operación [5].

Cancelar las solicitudes son útiles cuando se bifurcan los proxis (proxis que emiten más de un INVITE al recibir solo un INVITE). Cuando las representaciones se bifurcan está realizando una búsqueda paralela, trata varios lugares el mismo tiempo. Por ejemplo, un proxy bifurcación sabe que los tres posibles lugares donde Bob podría ser alcanzado son SIP: Bob@131.160.1.112, SIP: Bob.johnson@company.com, y SIP:Bob.university.com. Cuando este proxy recibe un INVITE de Laura a Bob, que tratara estos tres lugares en paralelo (Al mismo tiempo). El proxy bifurcación envía tres invitaciones, una para cada ubicación. Bob, que está trabajando actualmente en 131.160.1.112, responde a la llamada, los proxy bifurcan recibe un 200 OK de SIP: Bob@131.160.1.112 y hacia adelante esta respuesta a la UA de Laura debido a la sesión que ya se ha establecido entre Laura y Bob, el proxy bifurcación quiere parar las otras búsquedas iniciadas, por lo que envía dos CANCEL, uno para cada lugar para cerrar las búsquedas (Figura 3-12) [5].

Recuerde que una petición de CANCEL no afecta a una transacción una vez que la respuesta final ha sido enviada. Por lo tanto en nuestro ejemplo, incluso la bifurcación envía un CANCELAR para SIP: Bob@131.160.1.112 , la sesión entre Bob y Laura si persiste , y CANCEL no puede terminar la transacción en curso, se ignora por transacciones completadas [5].

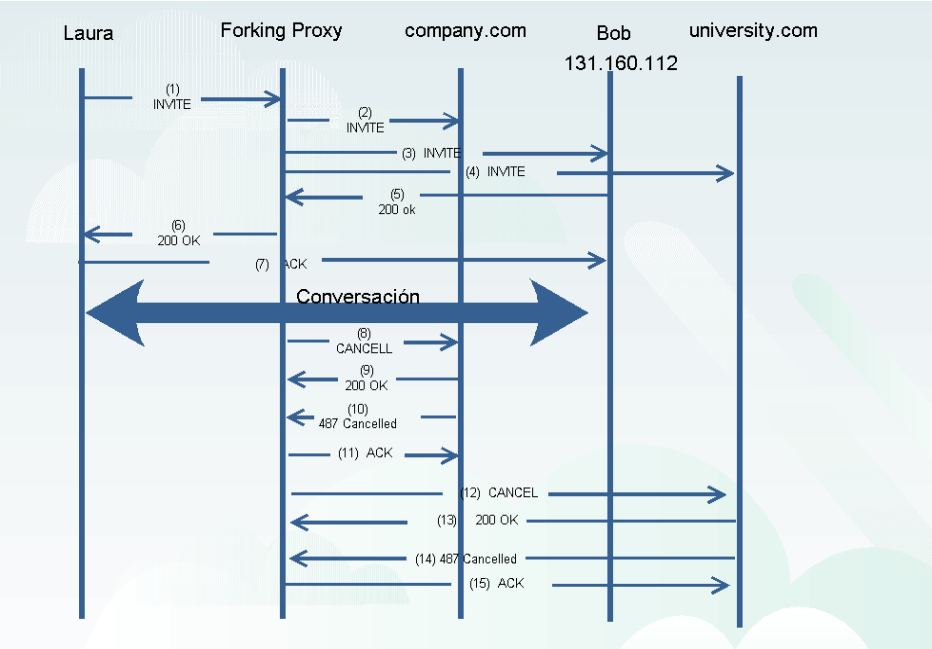


Figura 3- 12. Proxy Cancelando la transacción INVITE

BYE las peticiones BYE se utilizan para abandonar las sesiones. En las sesiones de dos partidos, el abandono por alguna de las partes implica que la sesión se termina. Por ejemplo Cuando Bob envía un pase directo a Laura, su sesión es automáticamente terminado (Figura 3-13). En los escenarios de multidifusión, sin embargo, una petición de BYE de uno de los participantes solo significa que un participante en particular sale de la conferencia. La sesión en si no se ve afectada. De hecho, es una práctica común en las grandes sesiones de multidifusión que no envía un BYE la salir de la sesión [5].

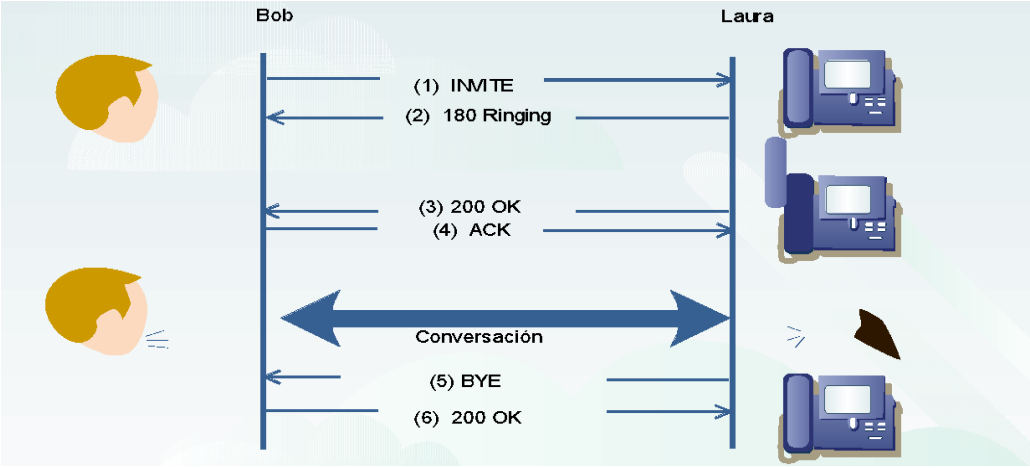


Figura 3-13. Laura envía un BYE cuando cuelga.

Figura 3-14. Bob se registra en el registro Company.com.

REGISTER Los usuarios envían solicitudes de registro para informar a un servidor (en este caso, se refiere a un registrador) sobre su ubicación actual. Bob puede enviar un registro al registrador en Company.com ordenando todas las solicitudes entrantes para SIP: Bob.johnson@company.com deben ser proxy, o redirigidos a SIP: Bob@131.160.112 (Figura 3-14). Los servidores SIP están generalmente ubicados conjuntamente como registradores SIP. Un registrador SIP puede enviar toda la información recibida de diversas peticiones REGISTER a un solo servidor de localización, poniéndolo a disposición de cualquier servidor SIP tratando de encontrar un usuario [5].

REGISTER también contiene los tiempos en que el registro se refiere. Por ejemplo, Bob puede registrar su ubicación actual hasta las cuatro de la tarde, porque sabe que es cuando va a salir de la oficina, Un usuario también puede registrar en varios lugares al mismo tiempo, lo que indica al servidor que debe buscar al usuario en todas las localidades registradas hasta que el o ella se alcanza [5].

OPTIONS

Las peticiones opciones de consulta un servidor sobre sus capacidades (Figura 3-15), incluyendo que métodos y que descripción de protocolos de sesión soporta. Un servidor SIP puede responder a solicitudes de OPCIONES que apoya a SDP como protocolo y cinco de descripción de métodos de sesión: INVITE, ACK, CANCELAR, BYE y OPTIONS. Debido a que el servidor no es compatible con el método de REGISTRO, puedo deducir que no es un registrador. El método OPCIONES podría no ser útil ahora, pero a medida que hay nuevas extensiones agregan métodos SIP, el método OPCIONES es una gran manera de descubrir que métodos de cierto servidor soporta [5].

Un método OPCIONES también devuelve los datos que especifica cuales codificaciones para el cuerpo de los mensajes el servidor entiende. Si un determinado servidor entiende, por ejemplo, un esquema de comprensión determinado, el cliente será capaz de enviar las descripciones de las sesiones comprimidas y aprovechar la oportunidad de ahorrar algo de ancho de banda [5].

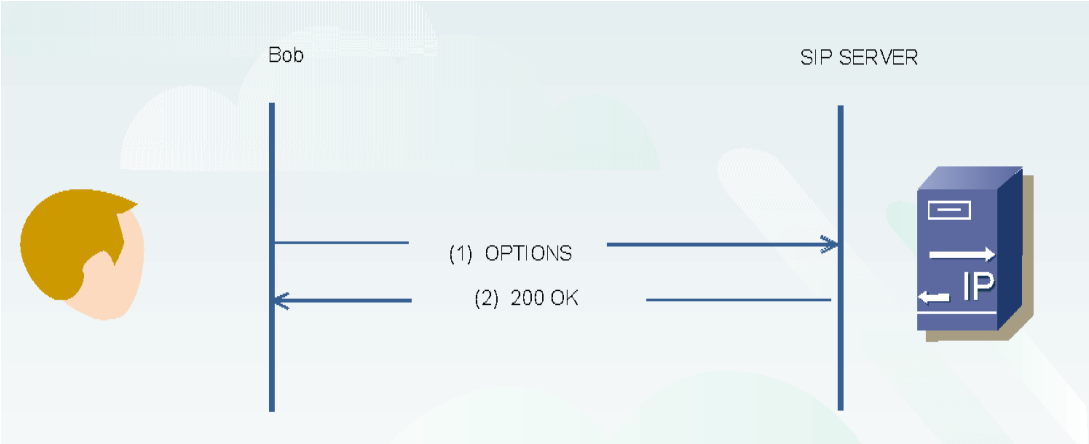


Figura 3-15. Bob consulta al servidor sobre sus capacidades.

3.3.6 Formato de los mensajes SIP

El diseño del protocolo procede en etapas discretas. Cuando se ha decidido que información será intercambiada entre sistemas distribuidos, el siguiente paso es decidir cómo esta información debe ser codificada. Esta decisión tiene básicamente dos enfoques: Binario, que utiliza campos de bits para codificar la información y textual, que usa cadena de caracteres. El siguiente ejemplo ilustra las diferencias entre los dos enfoques [5].

Los usuarios necesitan para realizar un seguimiento del mes en curso en sus equipos, y un servidor en la red tiene esa información. Necesitamos un protocolo que pueda transferir esta información desde el servidor al escritorio [5].

El campo actual del mes puede tomar exactamente 12 valores posibles: Enero, febrero, Marzo, Abril, Mayo, Junio, Julio, Agosto, Septiembre, Octubre, Noviembre, Diciembre [5].

Un protocolo basado en texto transmitiría el nombre del mes entre sistemas. Digamos que el contenido del mensaje es enero. Cada carácter (Letra) es típicamente codificado usando un byte (8 bits). Por lo tanto, el mensaje de enero será codificado con 49 bits (7 letras tiempos de 8 bits) [5].

Un protocolo binario, por otra parte, seria definir una tabla con posibles valores y su codificación correspondiente, como se muestra en la Tabla 5-3 [3].

Por lo tanto, para transmitir el mes en curso, el protocolo binario enviaría el 4 bit mensaje que contiene 0000 [5].

SIP utiliza la codificación de texto en lugar del binario. Este problema ha ocasionado acaloradas discusiones. Texto vs Binario parece ser un debate cuasi-religiosa en que es imposible mantener una opinión moderada [5].

Proponentes de texto afirman que los protocolos basados en texto se depuran con mayor facilidad, ya que pueden leerse directamente por un ser humano y que los protocolos de texto más flexibles y más fácil de extender con nuevas características [5].

Creyentes binarios argumentan que los protocolos binarios argumentan que los protocolos binarios usan el ancho de banda de manera más eficiente y también puede ser fácil depurar y extender con las herramientas adecuadas. Ambos tipos de codificación tienen ventajas y desventajas que no vamos a enumerar en esta discusión, pero tengan en cuenta que SIP es un protocolo basado en texto y exhibe todos los pros y contras de protocolos basados en texto en general [5].

Tabla 6. Codificación binaria de los meses.

0000	**January**	**110**	**July**
0001	February	111	August
0010	March	1000	September
0011	April	1001	Octuber
0100	May	1010	November
0101	June	1011	December

3.3.7 Formato de respuesta SIP

Una respuesta SIP consiste en una línea de estado, varias cabeceras, una línea vacia, y un mensaje body. Tabla 5-5 muestra el formato de una respuesta SIP. El mensaje cuerpo es opcional; Algunas respuestas no lo llevan [5].

Tabla 7. Codificación binaria de los meses.

0000	**January**	**110**	**July**
0001	February	111	August
0010	March	1000	Septembe r
0011	April	1001	Octuber
0100	May	1010	November
0101	June	1011	December

Estado de línea. Una línea de estado tiene tres elementos: la versión del protocolo, el estado código, y una frase razón. La versión del protocolo actual se escribe como SIP/2.0 El código de estado informa sobre el estado de la transacción. Como se describió anteriormente, códigos de estado son números enteros de 100 a 699 y se agrupan en seis diferentes clases (Consulte la tabla 5-1). La frase la razón es para los ojos humanos solamente. No es significativo para las respuestas de procesamiento de los ordenadores SIP. Abajo hay un ejemplo de una línea de estado [5].

SIP / 2.0 180 Ringing

Transmisión fiable de las respuestas. Las respuestas finales fiables se transmiten entre el servidor y el cliente, utilizando las retransmisiones o un protocolo fiable de transporte para garantizar la entrega. Las respuestas tradicionales no lo son. Ellos o bien puede ser recibida por el cliente o perderse en la red. SIP toma este enfoque, ya que está más preocupado por si una sesión se ha establecido o no, y las razones por las que no lo era, que con la forma en la sesión está progresando [5].

En una llamada SIP por ejemplo, las personas que llaman se les garantiza que la notificación de la llamada se ha aceptado, pero puede no saber cuándo

comenzó el destinatario de la llamada de alerta (Figura 3-16). SIP puede ser extendido para la entrega fiable provisional de respuestas si es necesario [5].

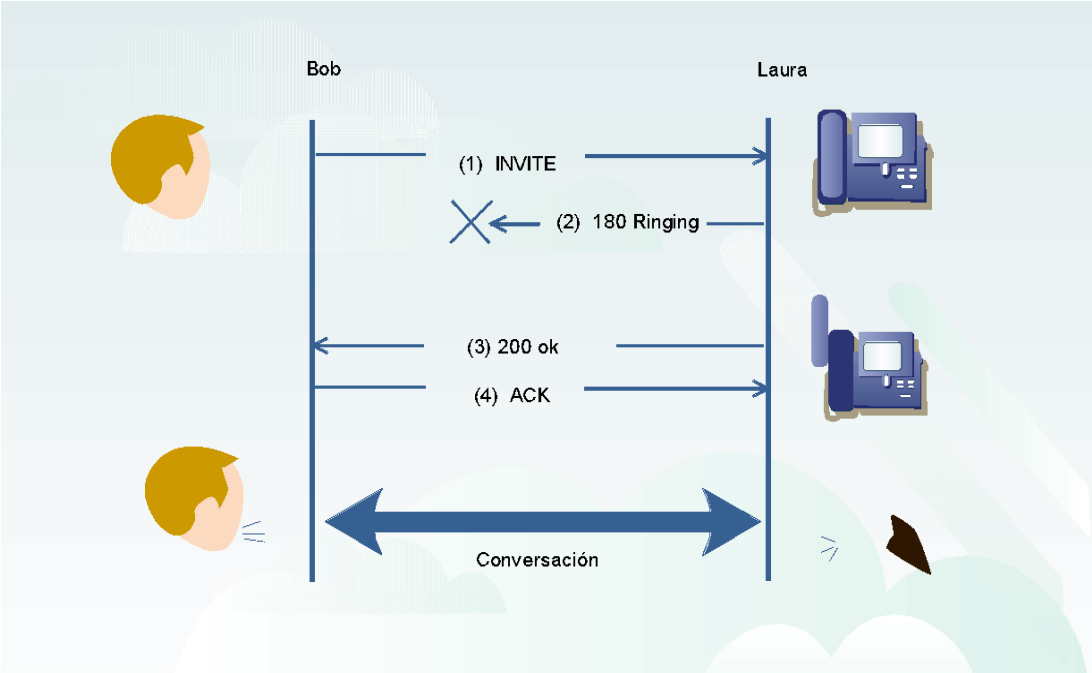


Figura 3-16. SIP no garantiza que se reciban respuestas provisionales.

Cabeceras SIP.

Las solicitudes SIP contienen algunas cabeceras SIP después de la línea de petición, mientras que las respuestas SIP los pusieron después del estado de línea. Las cabeceras proporcionan información acerca de la solicitud (o respuesta) y sobre el cuerpo que contiene. Algunas de las cabeceras pueden ser utilizadas en ambas solicitudes y repuestas, pero otros son específicos de peticiones (o respuestas) solas. La cabecera consiste en el nombre del encabezado, seguido de dos puntos, seguido del valor del encabezado [5].

Por ejemplo, la cabecera llamada De, que identifica el originador de una solicitud en particular, tiene el siguiente aspecto [5]:

From: Bob Johnson <sip:Bob.Johnson@company.com>

En este ejemplo, el encabezado tiene dos campos: el nombre de una persona y su SIP URL tabla 5-6 contiene cabeceras SIP definidos en el protocolo básico [5].

Tabla 8. Encabezados SIP.

Accept	**Content-encoding**	**Max-forwards**	**Route**
Accept-encoding	Content-language	MIME-version	Server
Accept-language	Content-length	Organization	Subject
Alert-info	Content-type	Priority	Supported
Allow	Cseq	Proxy-authenticate	Timestamp
Also	Date	Proxy-authorization	To
Authorization	Encryption	Proxy-require	Unsupported
Call-ID	Error-info	Proxy-route	User-agent
Call-info	Expires	Require	Vin
Contact	From	Response-key	Warning
Content-disposition	In-reply-to	Retry-after	WWW-authenticate

Identificador de llamadas (CALL-ID).

El call-id representa una relación de señalización SIP compartido entre dos o más usuarios. Se identifica una invitación en particular y todas las posteriores operaciones relacionadas con esa invitación en un formato que se ve como la siguiente [5]:

Call-ID: ges456fcdw211kfgte12ax@workstation1234.university.com

Un servidor que está haciendo malabarismos con la señalización SIP para muchas sesiones emplea el identificador de llamada para asociar los mensajes entrantes a la sesión adecuada. Por ejemplo, Bob invita a Laura a una sesión de ajedrez con un call-id particular. UA de Laura acepta y pronto el juego comienza. Después de un rato, Bob pide a Laura hablar con ella, mientras que todavía están jugando al ajedrez. El INVITE desde el UA de Bob tiene una diferente CALL-ID de la anterior. Cuando Bob y Laura terminan de hablar, el UA de Bob envía un pase directo a Laura para finalizar la llamada de teléfono. El UA de Laura utiliza

el Call-ID del mensaje BYE para decidir si termina la partida de ajedrez (Figura 3-17) [5].

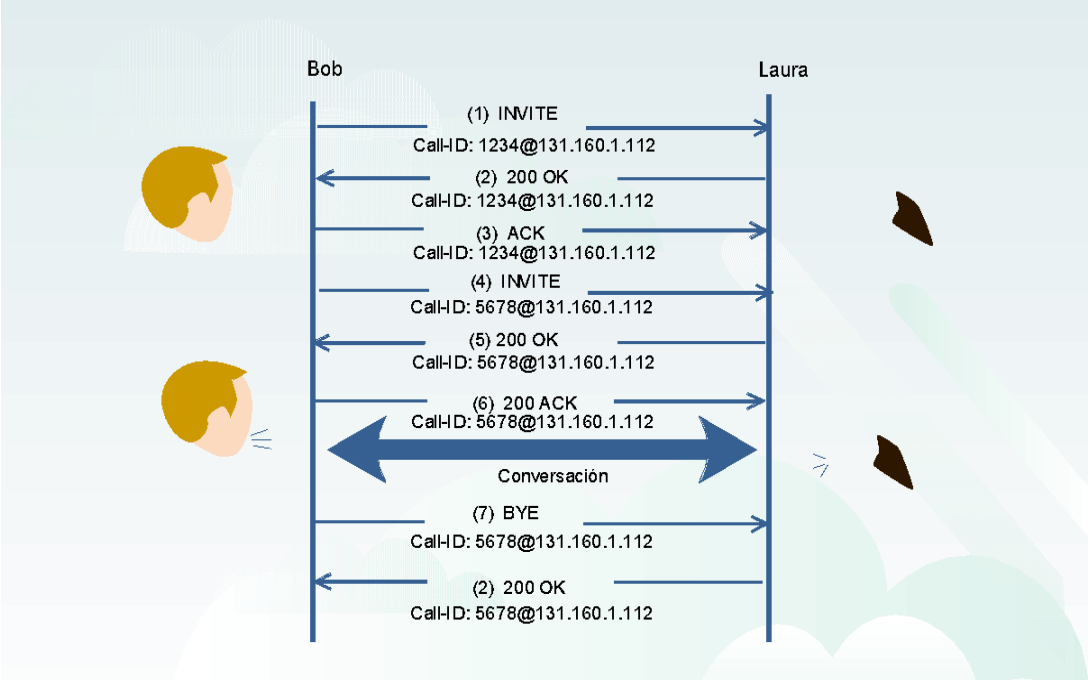


Figura 3-17. Call-ID ayuda a distinguir entre diferentes sesiones.

Contacto (contact).

Una cabecera de contacto proporciona una URL en la que se puede llegar al usuario directamente. Esta característica es importante porque se descarga a los servidores SIP que hacen no necesitar estar en la ruta de señalización de enrutamiento después del primer INVITE [5]..

Por ejemplo, Laura llama a Bob en SIP:Bob.Jhonson@company.com Company.com proxy reenvía el INVITE SIP: Bob@131.160.1.112, donde Bob resulta ser. El acepta la llamada. UA de Bob devuelve un OK la respuesta con una cabecera de contacto [5].

Contact: Bob Johnson <sip:Bob@131.160.1.112>

Cuando UA de Laura recibe esta respuesta 200 OK, envía el ACK del UA de Bob. Debido a la ubicación de Bob se puede encontrar en la cabecera de contacto, el ACK se envía directamente a la SIP: Bob@131.160.1.112 y el ACK no atraviesa el proxy en Company.com Figura 3-18 muestra como las solicitudes posteriores, como el BYE, se envían directamente entre los participantes de la sesión [5].

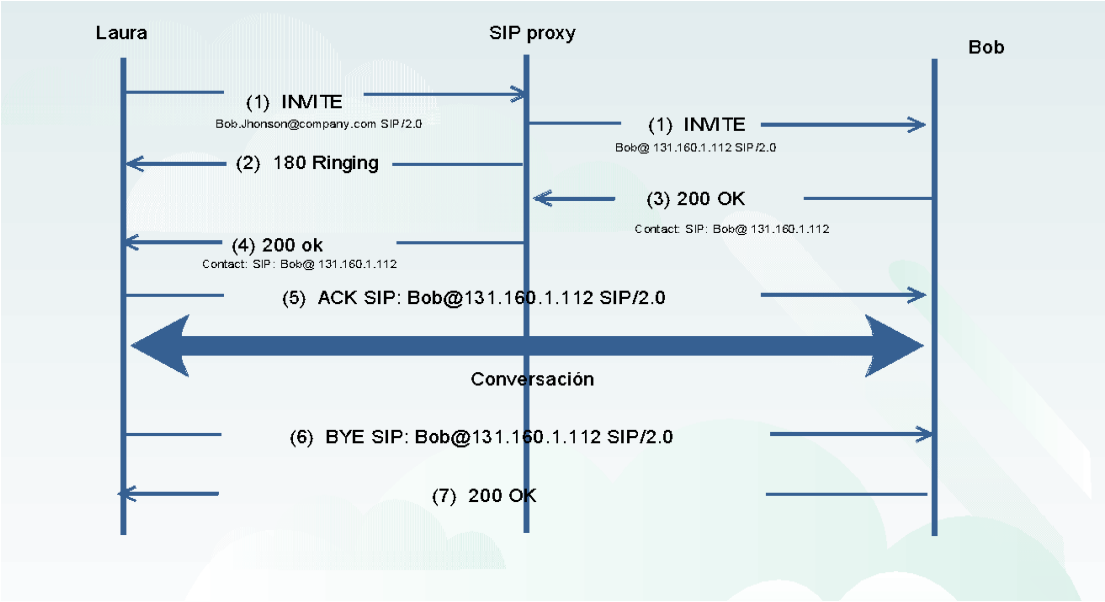


Figura 3-18. Los encabezados de CONTACTO pueden omitir un servidor proxy. Una vez que el usuario final se encuentre.

Cseq.

La secuencia de comandos (Cseq) cabecera tiene dos campos: Un número entero y un nombre de método. La parte numérica de la Cseq se utiliza para ordenar diferentes solicitudes dentro de la misma sesión (definida por un call-id en particular). También se utiliza para que coincida con las peticiones en contra de las respuestas. Por ejemplo, Bob envía una invitación a Laura con la siguiente Cseq [5]:

Cseq: 1 INVITE

Laura devuelve una respuesta 200 OK con el mismo Cseq como el INVITE. Si Bob quiere modificar la sesión ya establecida, se enviará un segundo INVITE (re-INVITE) con la siguiente Cseq [5]:

Cseq: 2 INVITE

Si una retransmisión de la respuesta 200 OK se retrasa por la red y llega a la AU de Bob después de que se ha generado un segundo INVITE, que sabe que se trataba de una respuesta por primer INVITE, gracias a la cabecera CSeq (Figura 3-19) [5].

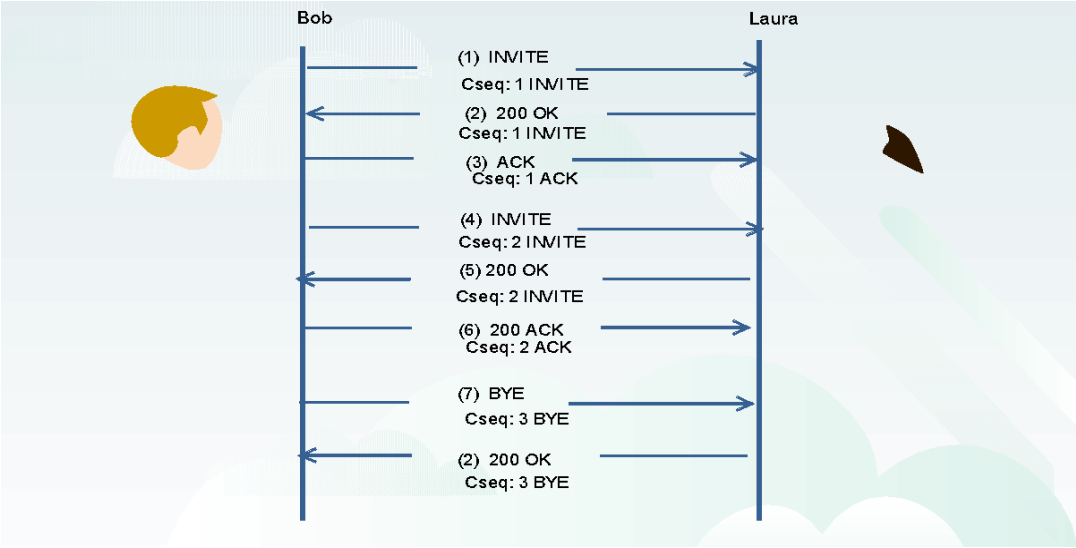


Figura 3-19. Cseq ayuda a distinguir las transacciones dentro de una sesión.

Después de una invitación a todas las solicitudes posteriores (excepto ACK y CANCEL) contener un Cseq es el resultado de incrementar por uno de los Cseq de la solicitud original [5].

Cseq en ACK. Una solicitud de ACK tiene el mismo Cseq como el INVITE se reconoce. Esto permite a los servidores proxy generar los ACK para que no sea un final exitoso de respuestas sin crear nuevas Cseq solo se puede crear por el UA, que asegura que los Cseq sean únicos [5].

Cseq en cancelar. Una solicitud cancelar tiene el mismo Cseq que la solicitud de cancelar. Esto también permite a los servidores proxy para generar CANCELS sin crear nuevos Cseq. Por otra parte, CANCELL es la razón por la cabecera incluye Cseq un nombre de método después de la parte numérica [5].

Debido a que el número Cseq de INVITE y CANCELL es lo mismo, un cliente SIP no podía distinguir las respuestas para cancelar y respuestas para invitar sin un campo adicional. El nombre del método en el interior resuelve Cseq el problema (Figura 3-20) [5].

Desde el encabezado contiene el iniciador de la solicitud y un SIP URL:

```
From: Bob Johnson <sip:Bob.Johnson@company.com>
```

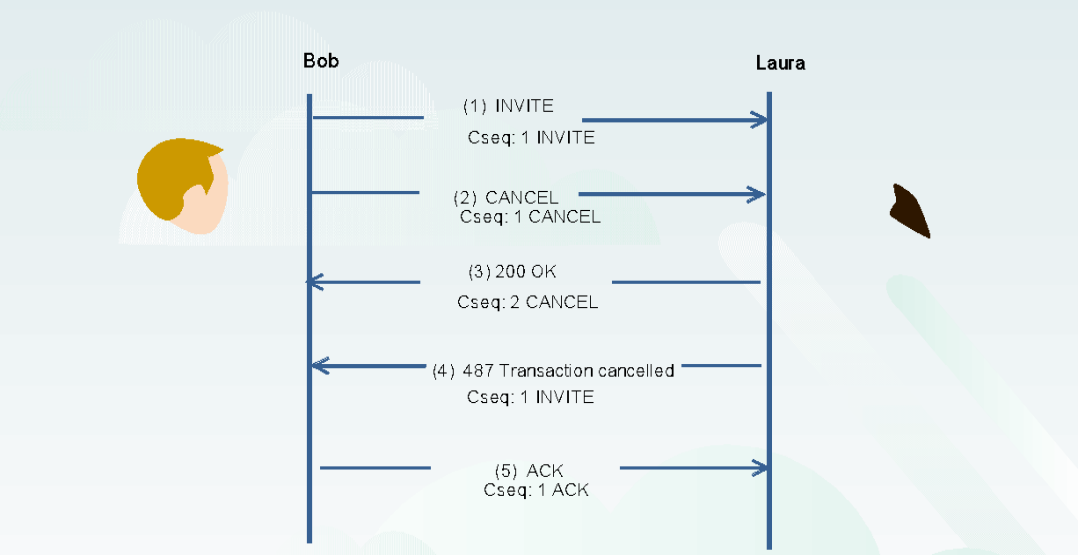


Figura 3- 20. El nombre del método en el Cseq permite diferenciar las respuestas INVITE y CANCEL.

Registro de carreteras y rutas (Record-Route and Route).

Estas dos cabeceras son utilizadas por los proxis que desean estar en la ruta de señalización para toda la sesión. Vimos que la cabecera contacto permiten las UAS enviar solicitudes directamente entre sí. Esta crea proxi que descargan en el camino; que la primera ruta de invitarle al destino correspondiente y luego dejar

que las UAS empiezan a intercambiar señalización SIP. Sin embargo, a veces un proxi necesita permanecer en la ruta de la señalización, para tal caso se necesita un mecanismo para mantener las AU de intercambio de mensajes SIP en sí mismo. Este mecanismo consta de dos cabeceras: Ruta y grabación de ruta [5].

Un proxy puede querer permanecer en la ruta de señalización después del primer INVITE por muchas razones. Uno de ellos es la seguridad. Algunos dominios tienen un proxy de seguridad, un servidor de seguridad, que filtra los mensajes SIP entrantes. Mensajes SIP que no atraviesan con éxito el proxy de seguridad no son aceptados en el dominio. Otra razón es la prestación de servicios. Un proxy que proporciona un servicio de sesión relacionada necesita saber cuándo la sesión se acabó; para nuestros propósitos, esto es cuando un UA envía una petición BYE a otro [5].

La figura 3-21 ilustra el funcionamiento de estas dos cabeceras. Laura envía un INVITE a Bob. El INVITE atraviesa un proxy SIP que desea estar en la ruta de señalización para las solicitudes posteriores entre Laura y Bob. El proxy añade una cabecera de registro de carreteras que contiene su dirección en la INVITE de Bob [5].

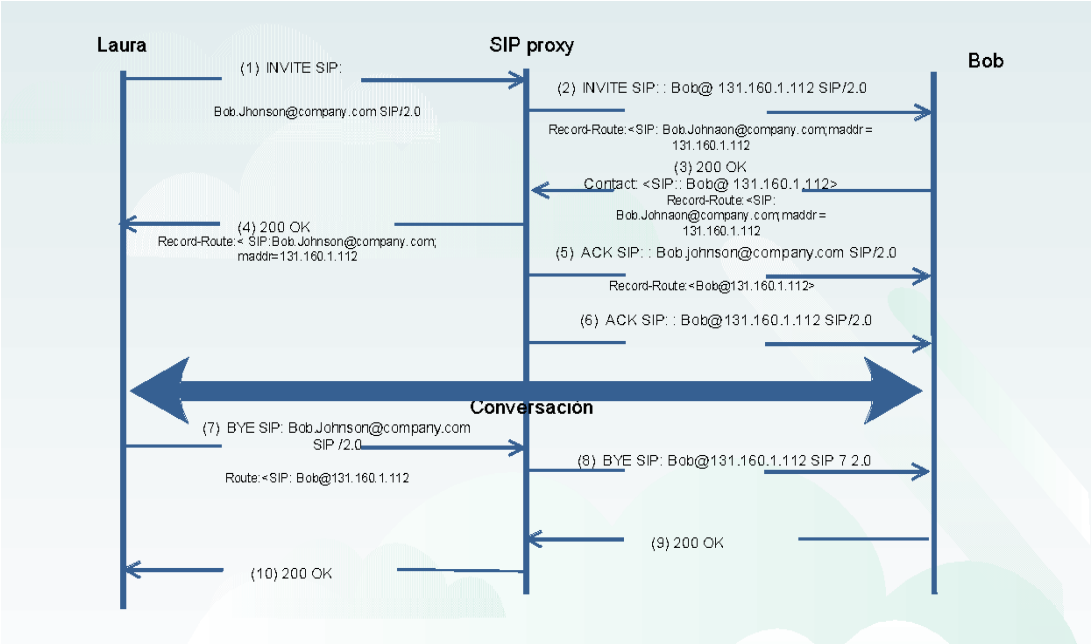


Figura 3-21. Los encabezados de ruta tienen un proxy permaneciendo en la ruta de señalización durante toda la sesión.

UA recibe el INVITE completo con esta cabecera registro de carreteras y lo incluye en la respuesta 200 OK. UA de Bob también añade su encabezado Contact a la respuesta. El parámetro maddr que aparece en el registro de carreteras solo contiene la dirección IP del servidor, que se añade para grabar IP real del servidor, que se añade para grabar IP del servidor para futuras peticiones [5].

UA de Laura recibe la respuesta 200 OK y construye una cabecera de ruta que se utilizara en las solicitudes posteriores. La cabecera de ruta se construye a partir tanto de registro de rutas y la cabecera de contact presente en la respuesta. Debido a que solo uno de proxy tiene que estar en la ruta de señalización, todas las peticiones posteriores de Laura a Bob (ACK Y BYE en este ejemplo) será enviado a la misma y se contiene una cabecera de ruta con la dirección contact Bob. De esta manera, el proxy sabe enviar la solicitud a la dirección que figura en la cabecera de la ruta [5].

Capitulo IV: Implementación de servicios de VoIP.

4.1 Implementación de servicio de voz sobre el protocolo de internet bajo el protocolo SIP.

El escenario en el cual se implementó el servicio VoIP está conformado por dos redes de área local (LAN) 1 y 2, interconectadas mediante un router Cisco entre los servidores Elastix como lo muestra la Figura 4-1.Donde la red LAN 1: es el segmento 192.168.10.0 / 24 y la red LAN 2: es el segmento 10.10.10.0 /24.

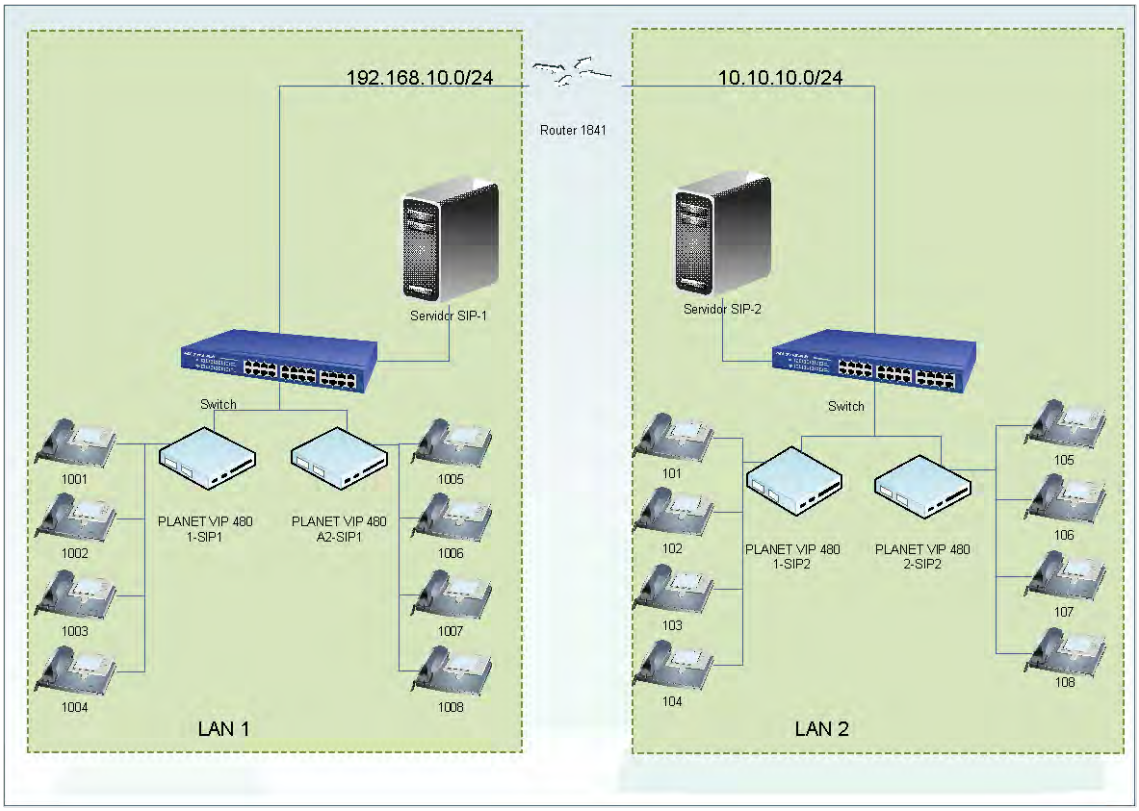


Figura 4- 1. Escenario de medición SIP

La Figura 4-1 muestra una arquitectura SIP formada por dos redes LAN interconectadas a través de un router cisco entre los servidores Elastix, cada red LAN está conformada por un Servidor Elastix, un Switch, y dos equipos Internet

Telephony Gateway Planet VIP-480 con 8 teléfonos cada uno y sus respectivas extensiones.

4.1.1 Características de los equipos

Los equipos utilizados en el escenario SIP son:

- 2 Computadoras.
- 1 Switch.
- 4 PLANET VIP 480-FS.
- 8 Teléfonos VTECH CLIO10B.
- 1 Router cisco 1841.

1 Laptop Gateway NV51 [6].

- Sistema Operativo: Elastix 2.4.0
- Memoria RAM: 4GB DDR3
- Procesador: Intel Pentium Dual Core T4500 (2.30 GHZ)
- Disco duro: 500 GB.
- Intel HD Graphics.

1 Laptop Gateway NE512 [7].

- Sistema Operativo: Elastix 2.4
- Memoria RAM: 2 GB.
- Procesador: Intel Celeron N2840 (2.16 GHz).
- Disco Duro: 320 GB.
- Intel HD Graphics.

2 HP Compac 6000 Pro Small form Factor: Gatekeeper 1 / 2 [8]

- Sistema Operativo: (Elastix 2.4.0)
- Procesador: Pentium (R) Dual-Core CPU E5700 @ 3.00 GHz.
- Memoria RAM: 4 GB.
- Disco Duro: 512 GB.
- Gráficos: Intel (R) Q45/A43 Expres Chipset (Microsoft Corporation-WDDM 1.1).

Planet VIP-480FS [9]

El equipo PLANET VIP-480FS es un Gateway VoIP de cuatro puertos FXS que cumple con los estándares SIP y H.323. Es una solución completa para la integración de redes voz/datos a las redes telefónicas analógicas. No solo provee comunicaciones de alta calidad sino también ofrece capacidades de compartir internet de modo seguro y confiable.

El VIP-480FS es capaz de manejar llamadas tanto SIP como H.323, cuenta con un switch de cuatro puertos y función de ruteador NAT, con estas funcionalidades los usuarios pueden disfrutar de llamadas de voz de alta calidad y acceso seguro a internet sin interferir con sus actividades de rutina.

Con sus clientes PPPoE/DHCP/DDNS, hasta cuatro conexiones concurrentes pueden ser establecidas en cualquier lugar del mundo. El VIP-480FS cuenta con una interfaz de usuario poderosa y amigable (web/telnet), que simplifica la implementación y monitoreo de la red VoIP.

Características

- 4 Ptos FXS + 4 Ptos Ethernet + WAN
- Soporte PPPoE, NAT, QoS
- Cliente DDNS para aplicación con IP dinámica
- Servidor virtual (a través de DDNS)
- Modo de comunicación dúal H.323v4/SIP 2.0
- Codecs de voz: G.711, G.729 AB, G.723
- Detección activa de voz, detección DTMF, cancelador de eco
- Detección de silencios y Modo FAX
- Buffer adaptable para diversas condiciones de jitter
- Display de estatus de canales de voz.

Teléfono VTECH CLIO10B [10]

- Teléfono Alámbrico
- Función radicado
- Timbre encendido/apagado
- Selección pulso/tono
- Tiempo flash disponible (100/300/600 ms).

Router Cisco 1841 [11]

- Procesador de alto rendimiento
- Arquitectura Modular
- Amplia memoria predeterminada
- Puertos LAN Ethernet de alta velocidad integrada.
- Soporte para Cisco IOS 12.3 T, 12.4, 12.4 T y conjunto de funciones.
- Fuente de alimentación estándar integrada.

4.1.2 Configuración de los Equipos SIP.

4.1.2.1 Servidor Elastix

Para la creación de una extensión dar clic en la pestaña PBX, la cual nos enviara a la siguiente ventana y muestra la opción de agregar un nuevo Dispositivo genérico SIP tal y como se muestra en la Figura 4-2.

Figura 4- 2. Agregar Extensión SIP.

En la Figura 4-3 se proporciona un ejemplo de la ventana donde se agrega la nueva extensión SIP y en la cual llenaremos los campos User Extension, Display y Secret.

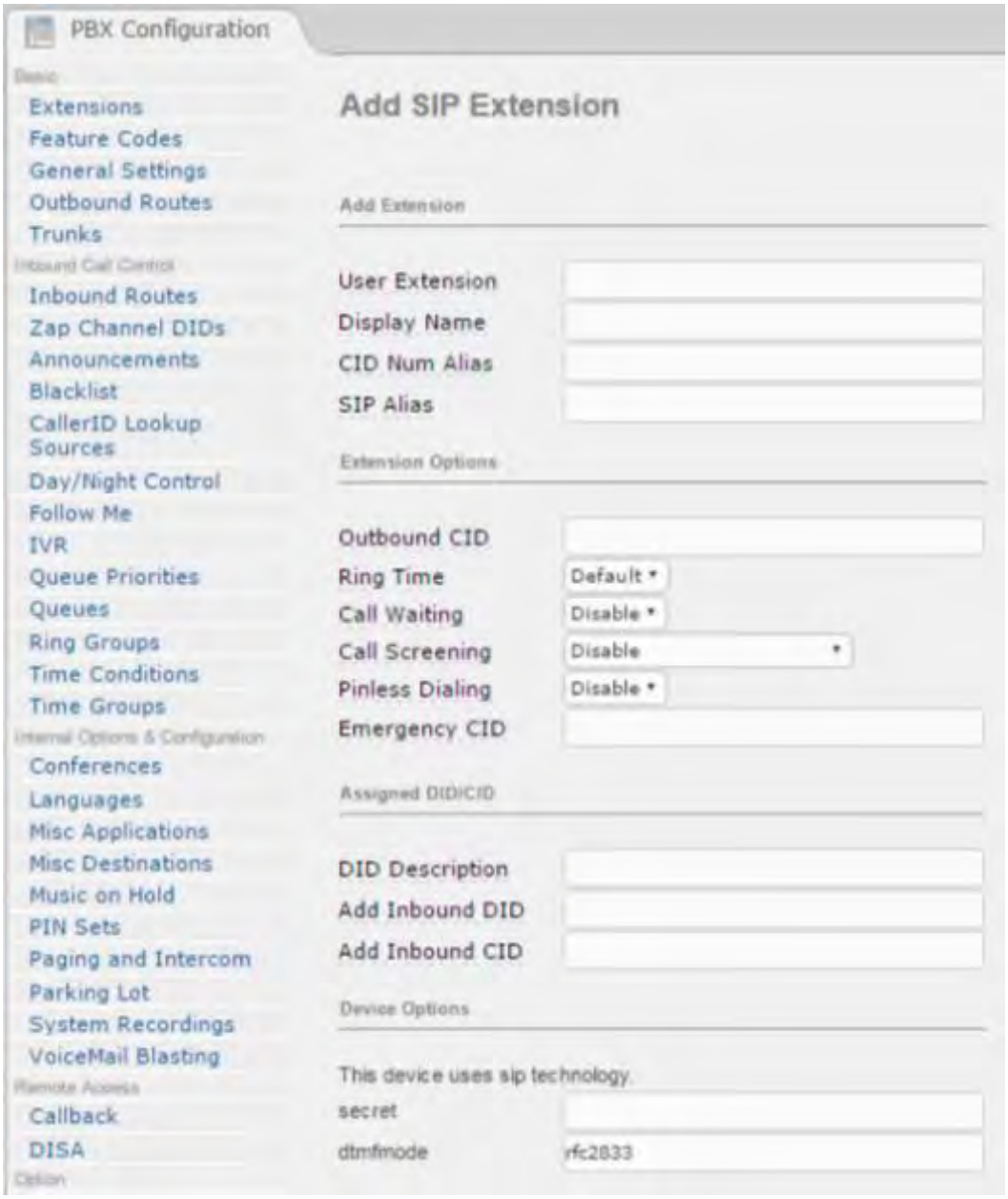


Figura 4- 3. Parámetros de extensión SIP.

Extensión del Usuario: En el Servidor SIP1 se les asignaron las extensiones del 1001 a la extensión 1008 y en el Servidor SIP2 se le asignaron las extensiones del 101 a la extensión 108.

Display Name: Para cada extensión se asignó el nombre de usuario1 hasta el nombre de usuario8, respectivamente en ambos Servidores.

Secret: En el caso del password se establecio el mismo (sip1122) para las 16 extensiones.

4.1.2.3 Internet Telephony Gateway: Planet VIP-480

Para poder dar de alta a los usuarios SIP, se crearon las extensiones en cada Equipo Planet VIP-480, en las Figuras 4-4 y 4-5, se muestra la configuración de las extensiones correspondientes al servidor SIP1 y las Figuras 4-6 y 4-7, las extensiones del servidor SIP2.

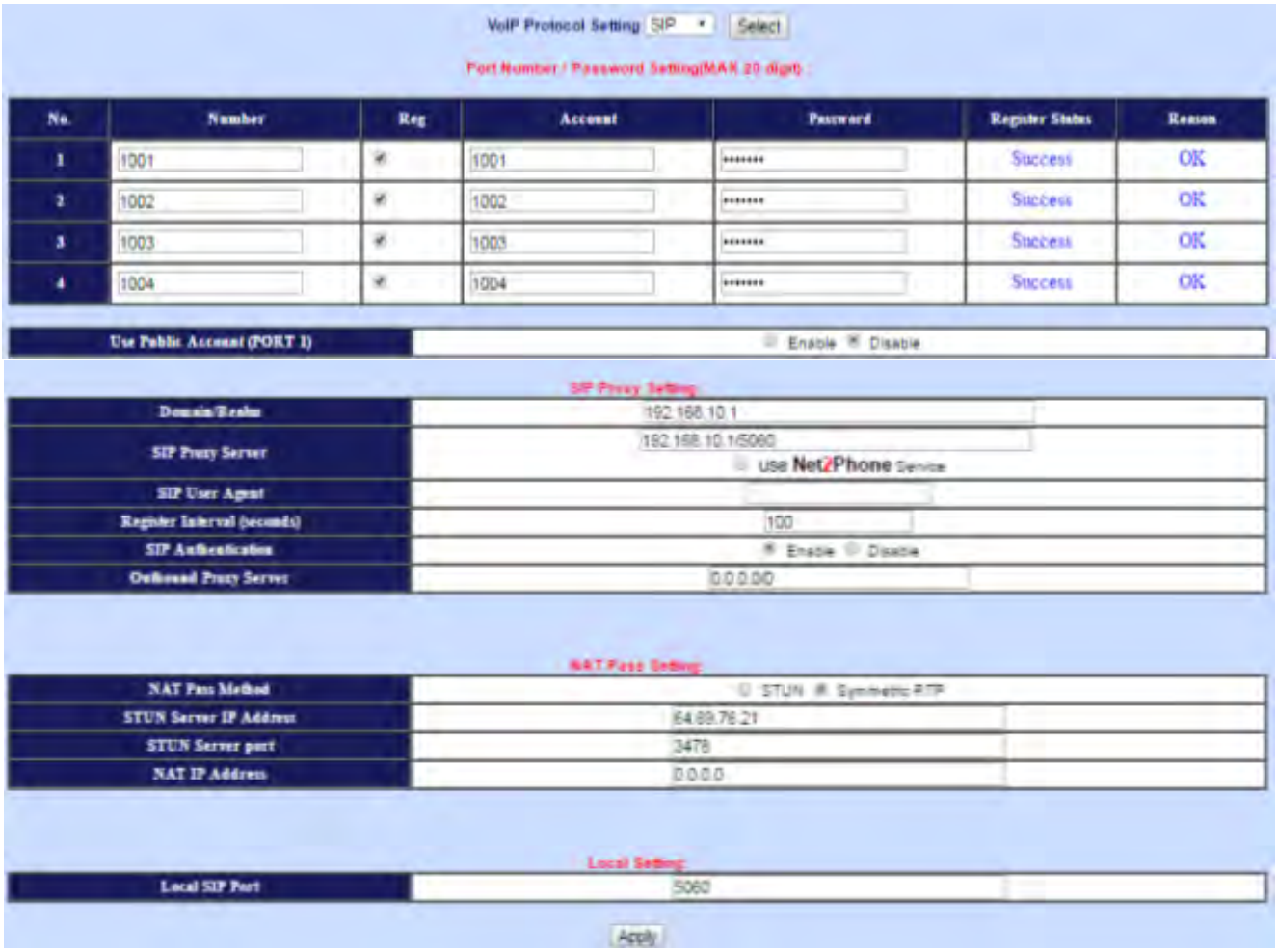


Figura 4-4 Creación de las extensiones SIP1 (1001-1004).

Figura 4-5. Creación de las extensiones SIP1 (1005-1008).

Figura 4-6. Creación de las extensiones SIP2(101-104).

Figura 4-7. Creación de las Extensiones SIP2 (105-108).

4.1.2.4 Router cisco 1841

Para que los servidores SIP-1 y SIP-2 puedan comunicarse fue necesario configurar el router en sus interfaces fastethernet, ya que ambos servidores se encuentran en segmentos de red diferentes fue necesario utilizar el router cisco 1841 para unir las dos redes LAN, el protocolo de enrutamiento implementado fue OSPF tal como lo muestra la figura 4-8.

```
hostname Router
!
interface FastEthernet0/0
 ip address 192.168.10.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.10.254 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
end
```

Figura 4-8. Imagen de la configuración del Router 1841.

4.1.2.5 Configuración Troncal SIP

Para cada Servidor elastix se creó una troncal SIP y para esto nos dirigimos a la pestaña PBX, le damos clic a Trunks y agregamos una troncal SIP, en la Figura

4-9 se muestra la configuración utilizada en el servidor SIP-1 y en la Figura 4-10 se muestra la configuración del servidor SIP-2.

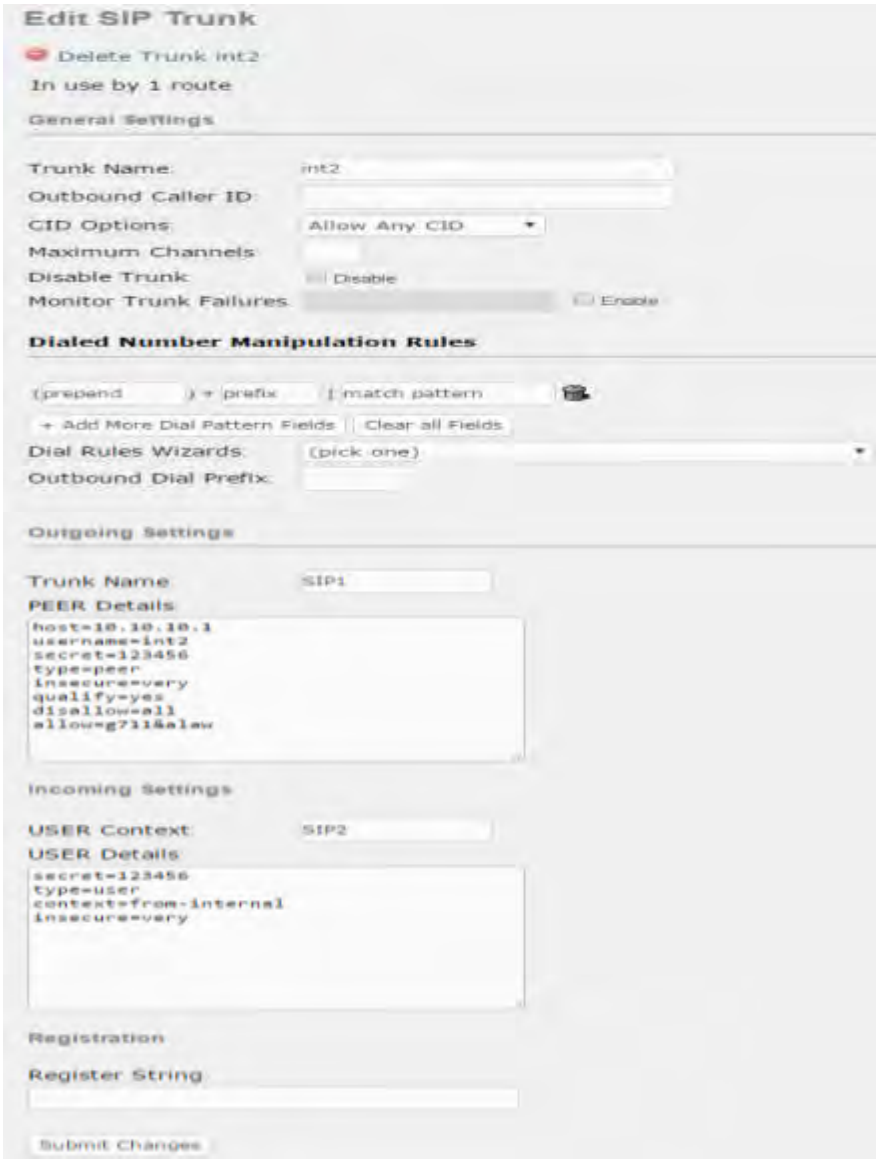


Figura 4-9. Troncal SIP para el servidor SIP1.

Figura 4-10. Troncal SIP para el servidor SIP2.

Para que cada extensión pueda llamar hacia la otra extensión del Servidor Remoto, se debe crear una ruta de salida, en la Figura 4-11 se muestra la configuración del Servidor SIP-A y la Figura 4-12 la del Servidor SIP-B.

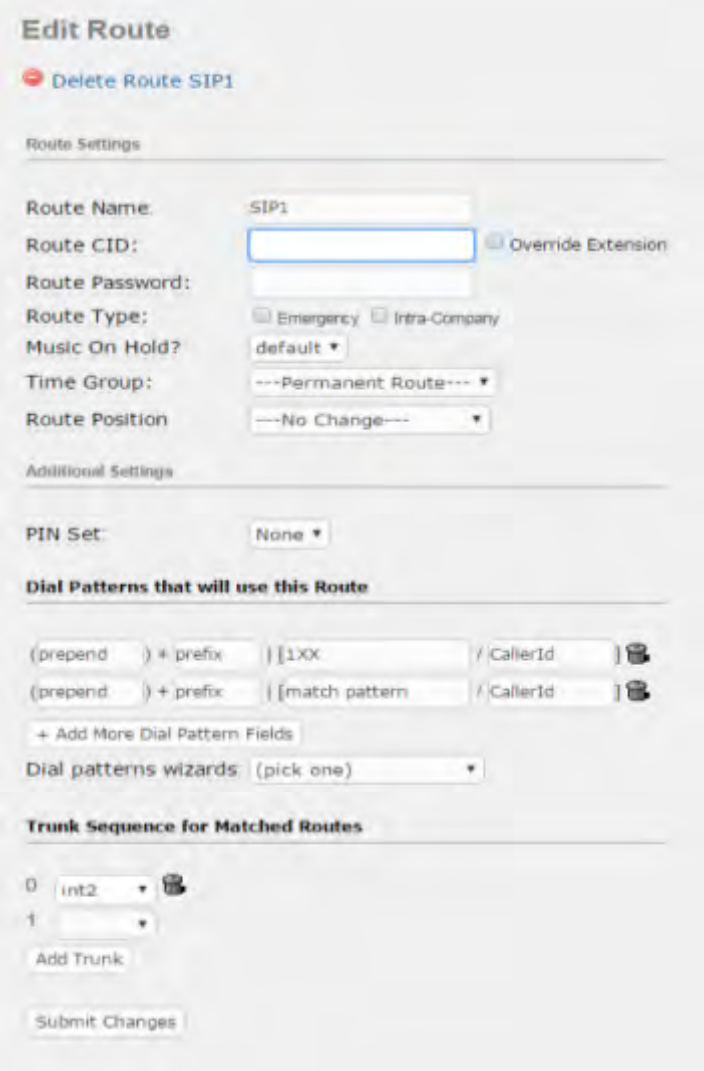


Figura 4-11. Ruta de salida del servidor SIP1.

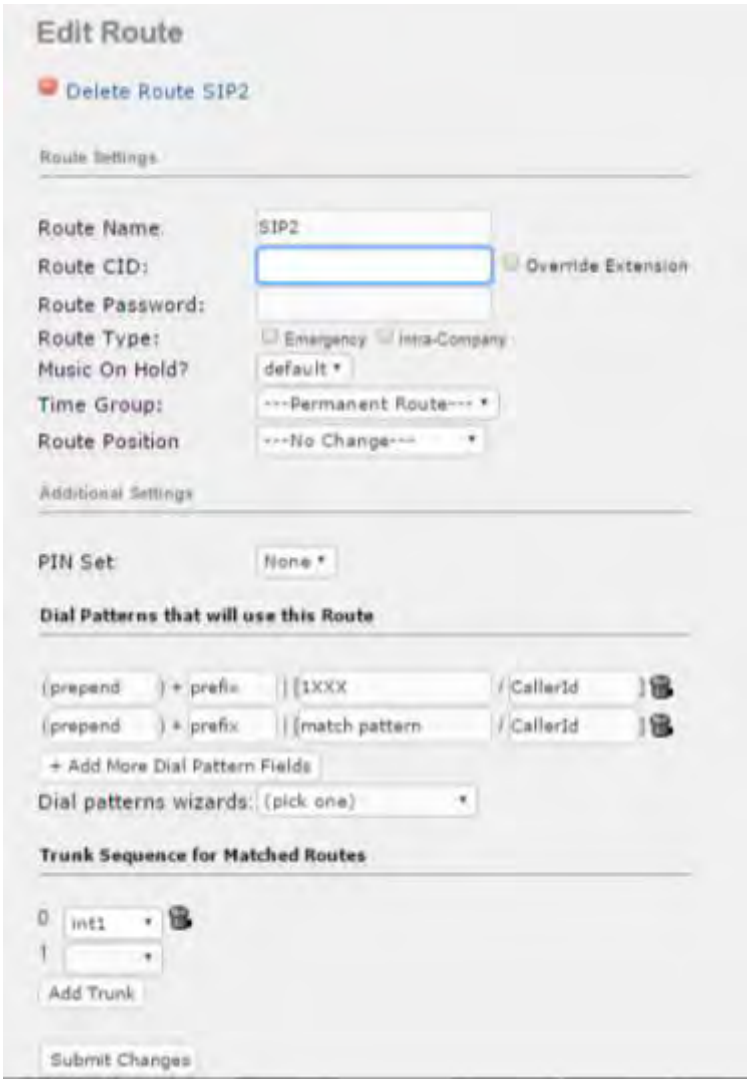


Figura 4-12. Ruta de salida del servidor SIP2.

Para realizar las llamadas con los códecs G.723, g.729 y g.711 y habilitar el VAD, se configuró la sección “Advance Setting” en cada Planet VIP-480 como se muestran en La Figura 4-13:

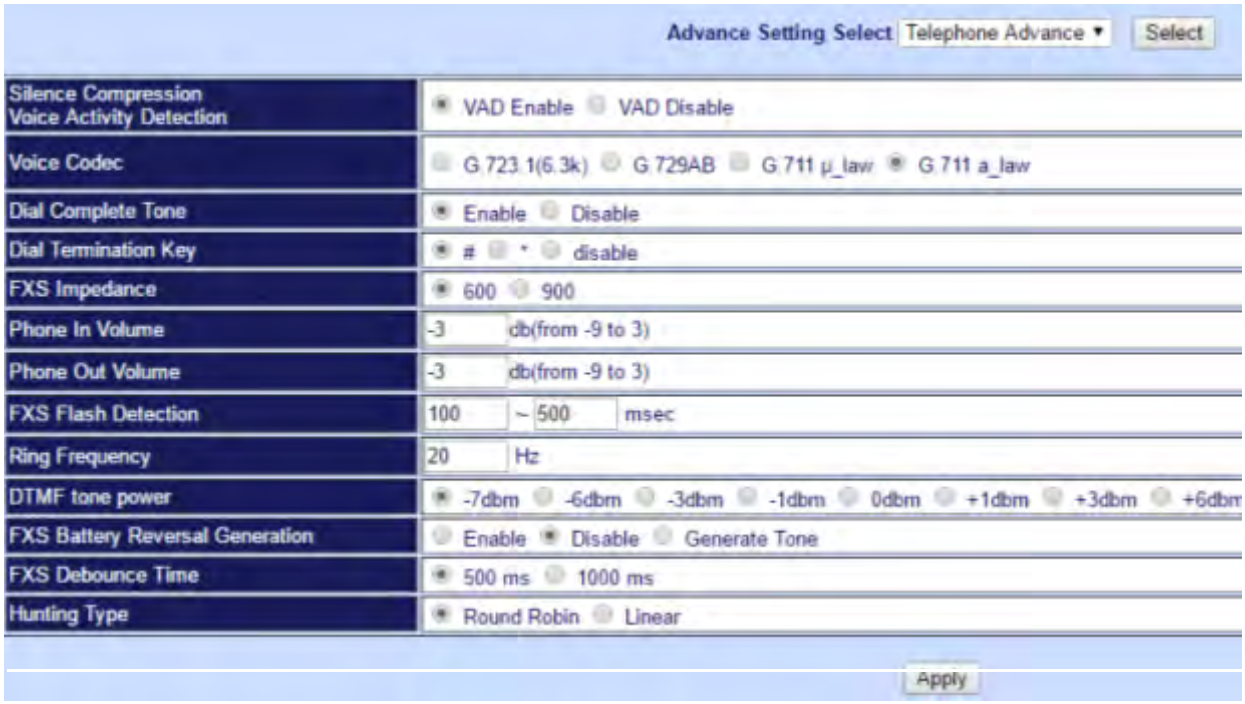


Figura 4-13. Selección de códec y modo de compresión de voz.

4.1.3 Comprobación de llamadas.

Una vez configurados todos los dispositivos se establecieron un conjunto de llamadas como lo muestran las Figuras 4-14 y 4-15.

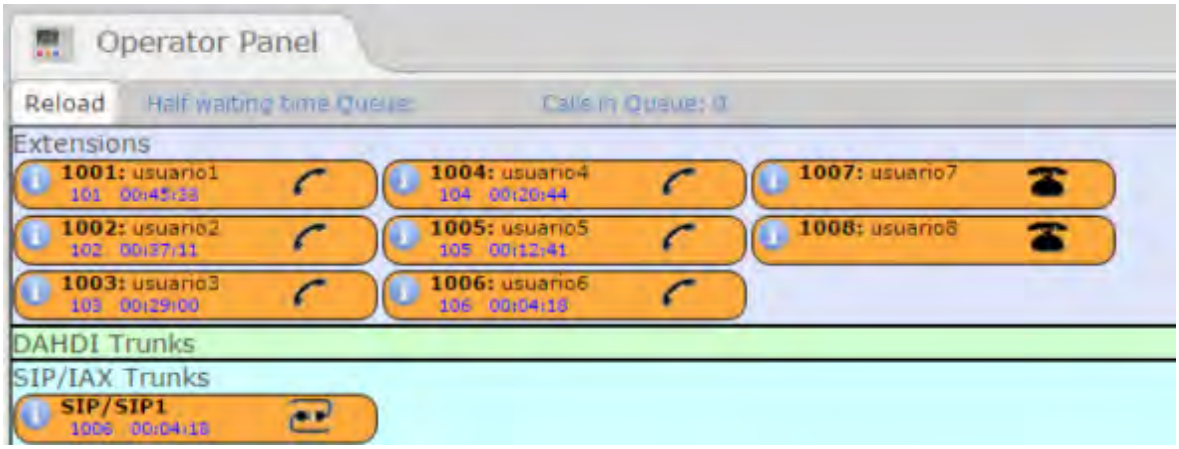


Figura 4-14. Extensiones del servidor SIP1 llamando a las extensiones del servidor SIP2.

Figura 4-15. Extensiones del servidor SIP2 llamando a las extensiones del servidor SIP1.

4.2 Implementación de servicio de voz sobre el protocolo de internet bajo el protocolo H.323.

El escenario en el cual se implementó el servicio VoIP está conformado por dos redes de área local (LAN) 1 y 2, interconectadas mediante un router Cisco entre los servidores Gatekeeper como lo muestra la Figura 4-16. Donde la red LAN 1: es el segmento 192.168.10.0 / 24 y la red LAN 2: es el segmento 10.10.10.0 /24.

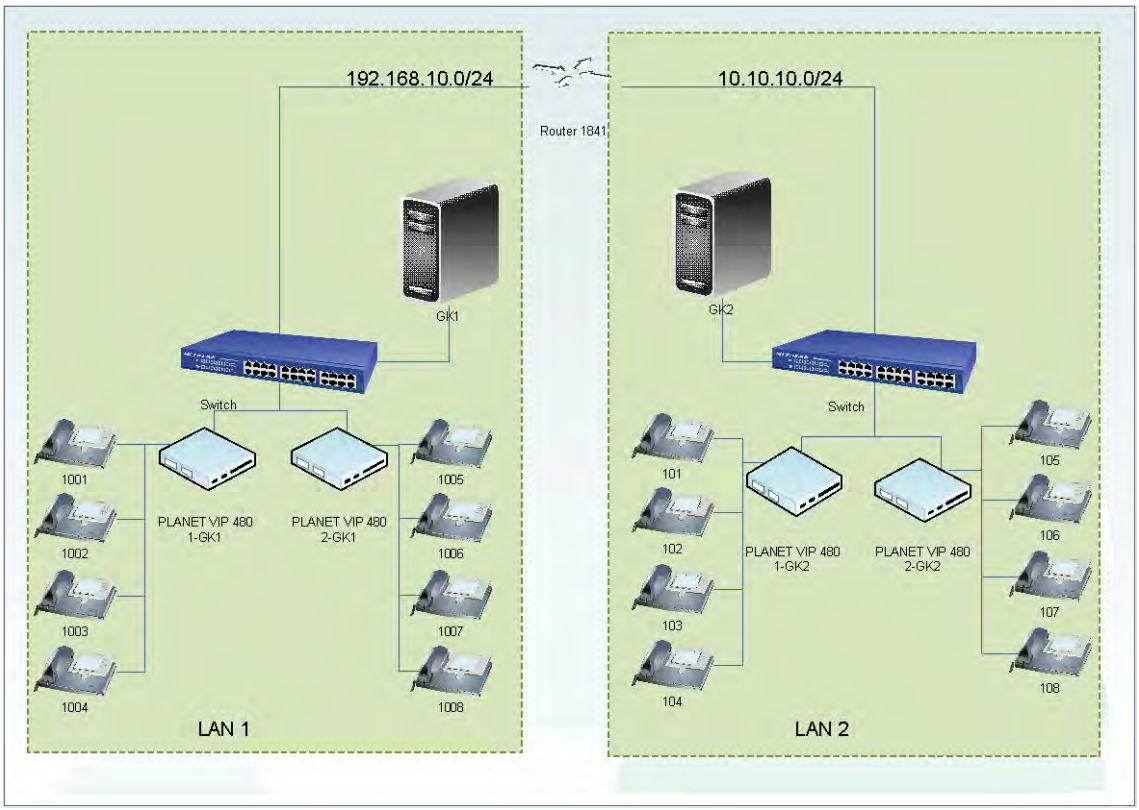


Figura 4- 16. Escenario de medición H.323.

4.2.1.- Características de los equipos H.323.

Los equipos utilizados en el escenario H.323 son:

- 2 Computadoras.
- 1 Switch.
- 4 PLANET VIP 480-FS.
- 8 Teléfonos VTECH CLIO10B.
- 1 Router cisco 1841.

Estos equipos se encuentran descritos en el tema 4.1.1.

4.2.2 Configuración de los equipos H.323

4.2.2.1 Configuración Gatekeeper

En la carpeta GNU se encuentran el archivo gatekeeper.ini necesario para configurar los parámetros, tal como se muestra en la figura.

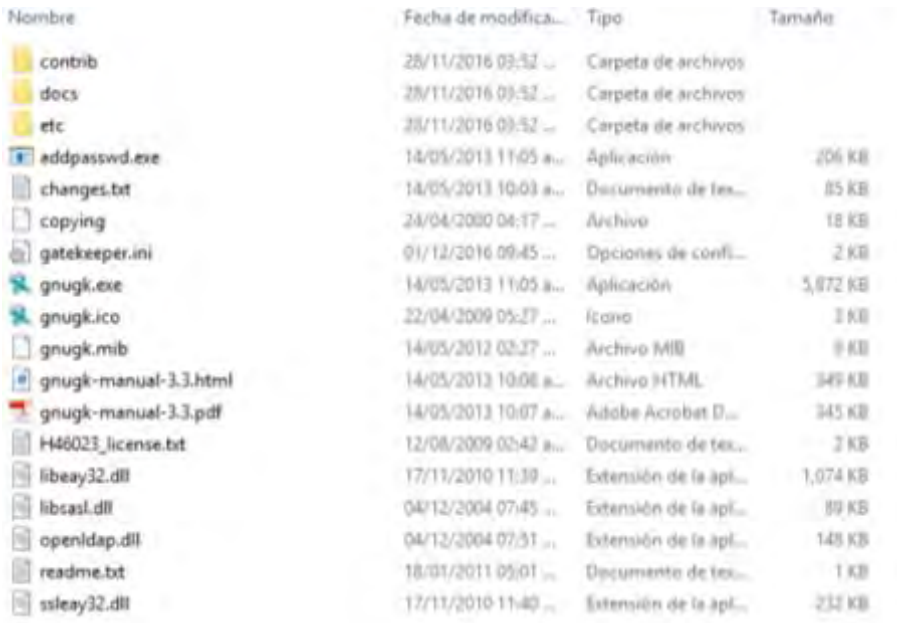


Figura 4- 17. . Contenido de la carpeta GNU.

En la figura 4-18 se muestra la configuración establecida en el archivo Gatekeeper, en este mismo archivo están explicados cada uno de los parámetros.

```
[Gatekeeper::Main]
Fourtytwo=42
Name=GK1
Home = 192.168.10.1
NetworkInterfaces = 192.169.10.0/24

[GkStatus::Auth]
rule=allow


[RasSrv::RRQFeatures]
SupportDynamicIP=1

[Gatekeeper::Auth]
default=allow

[RasSrv::RRQFeatures]
OverwriteEPOnSameAddress=1

[RasSrv::GWPrefixes]
gw1=1001,1002,1003,1004,
gw2=1005,1006,1007,1008

[RasSrv::PermanentEndpoints]
192.168.10.2=gw1
192.168.10.3=gw2

[RasSrv::Neighbors]
GK2=GK2

[Neighbor::gk2]
GatekeeperIdentifier=gk2
Host=10.10.10.1
SendPrefixes=*

AcceptPrefixes=*
```

Figura 4-18. Contenido del archivo Gatekeeper.ini del GK1.

```
[Gatekeeper::Main]
Fourtytwo=42
Name=GK2
Home = 10.10.10.1
NetworkInterfaces = 10.10.10.0/24

[GkStatus::Auth]
rule=allow

[RasSrv::RRQFeatures]
SupportDynamicIP=1

[Gatekeeper::Auth]
default=allow

[RasSrv::RRQFeatures]
OverwriteEPOnSameAddress=1

[RasSrv::GWPrefixes]
gw1=101,102,103,104,
gw2=105,106,107,108

[RasSrv::PermanentEndpoints]
10.1010.2=gw1
10.10.10.3=gw2

[RasSrv::Neighbors]
GK1=GK1

[Neighbor::gk1]
GatekeeperIdentifier=gk1
Host=192.168.10.1
SendPrefixes=*

AcceptPrefixes=*

ForwardLRQ=always
```

Figura 4-19. Contenido del archivo Gatekeeper.ini del GK2.

Fourtytwo=42: Este comando es para identificar que existe un archivo de configuración *.ini*.

- **Name=GK1:** Este es el nombre identificador del gatekeeper.
- **Home = 192.168.10.1:** Este comando se usa para especificar la dirección del gatekeeper.

- **NetworkInterfaces = 192.168.0.0/24:** Aquí especifica la interfaz que tiene disponible el gatekeeper.
- **rule=allow:** Permite todas las conexión vía telnet.
- **default=allow:** Este comando es para la autenticación del gatekeeper.
- **GK2 = GnuGK:** Este comando es para identificar que hay un vecino con el identificador GK2.
- **GatekeeperIdentifier=GK2:** Identificador del vecino.
- **Host=10.10.10.1:** Este comando es para indicar la dirección del gatekeeper del vecino.
- **SendPrefixes=*:** Son las extensiones que enviará el gatekeeper vecino GK2.
- **AcceptPrefixes=*:** Son las extensiones que aceptará el gatekeeper vecino GK2.
- **FowardLRQ=always:** Envía todos los mensajes LRQ sin excepciones.
- gw1=1001,1002,1003,1004
  gw2=1005,1006,1007,1008
  Estos comando son para indicar el Gateway con sus respectivos endpoints configurados.
- **OverwriteEPOnSameAddress=1:** Este comando es para sobrescribir las direcciones en caso que sufra un cambio inesperado y así no se pierda la comunicación.
- **AcceptEndpointIdentifier=1:** Acepta los endpoints identificados dentro del contenido RRQ.
- **AcceptGatewayPrefixes=1:** Acepta los prefijos del Gateway que se declararon previamente en la sección [RasSrv::PermanentEndpoints].

Después de configurar los archivos Gatekeeper.ini en GK1 y GK2 el siguiente paso es iniciar los gatekeeper para se establezcan las llamadas. Cada gatekeeper se inicia con el comando “gnugk.exe –t” en el directorio donde se encuentre, tal como lo ilustra la Figura 4.20.

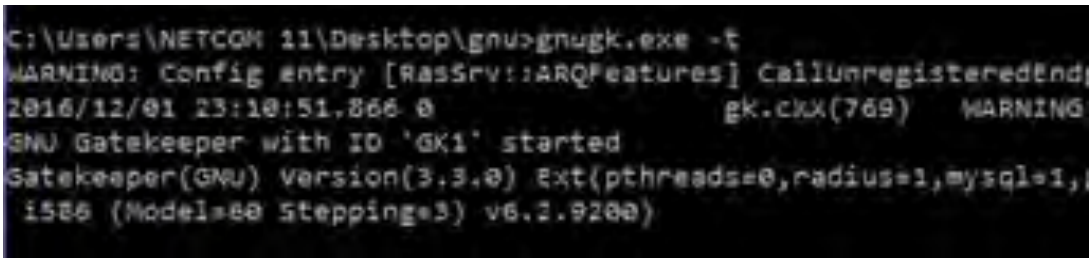


Figura 4-20. Inicio del Gatekeeper.exe a través del ms-dos.

4.2.2.2 Internet Telephony Gateway: Planet VIP-480.

Para poder dar de alta a los terminales H.323, se crearon las extensiones en cada Equipo Planet VIP-480, en las Figuras 4-21 y 4-22, se muestra la configuración de las extensiones correspondientes al GK1 y las Figuras 4-23 y 4-24, las extensiones del GK2.

Figura 4-21. Creation de las extensions del GK1 (1001-1004).

Figura 4-22. Creación de las extensions GK1 (1005-1008).

Figura 4-23. Creación de las extensions GK2 (101-108).

Para realizar las llamadas con los códecs G.723, g.729 y g.711 y habilitar el VAD, se configuró la sección “Advance Setting” en cada Planet VIP-480 como se muestran en La Figura 4-24:

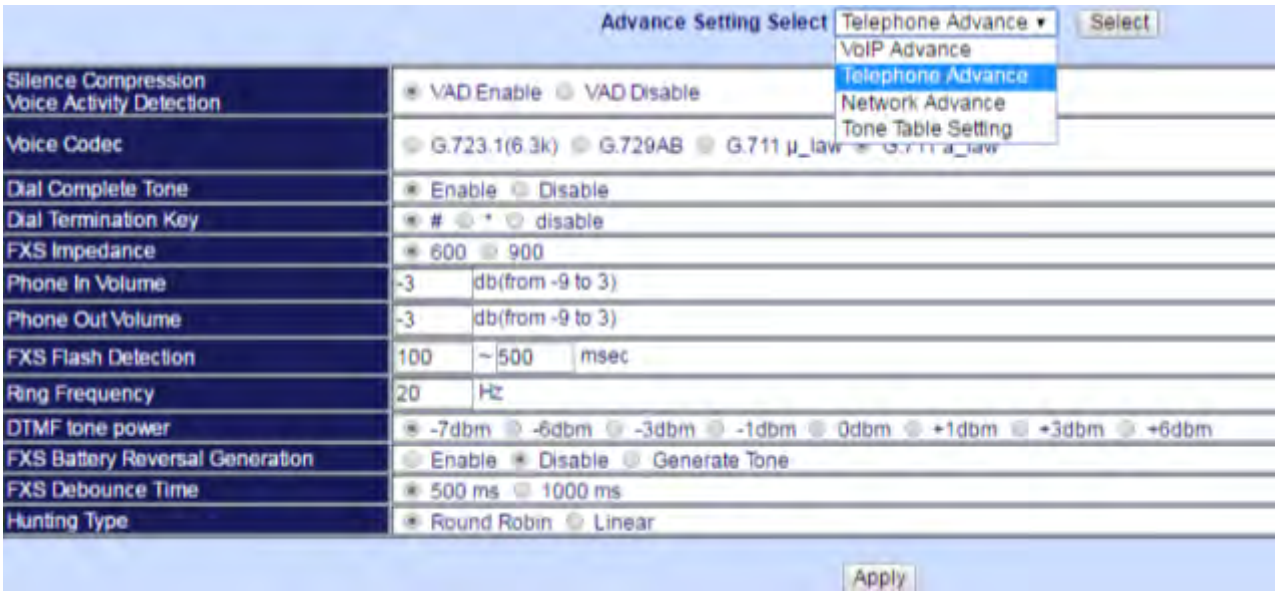


Figura 4- 24. Selección de códec y modo de comprensión de voz.

4.2.2.3. Configuración del router 1841

La configuración del router cisco es la misma que en el tema 4.1.2.4

4.2.3 Comprobación de llamada

En el ms-dos de Windows donde se inició el gatekeeper se muestran mensajes que permiten identificar si existen llamadas. En la Figura 4-25 se ilustra a detalle.

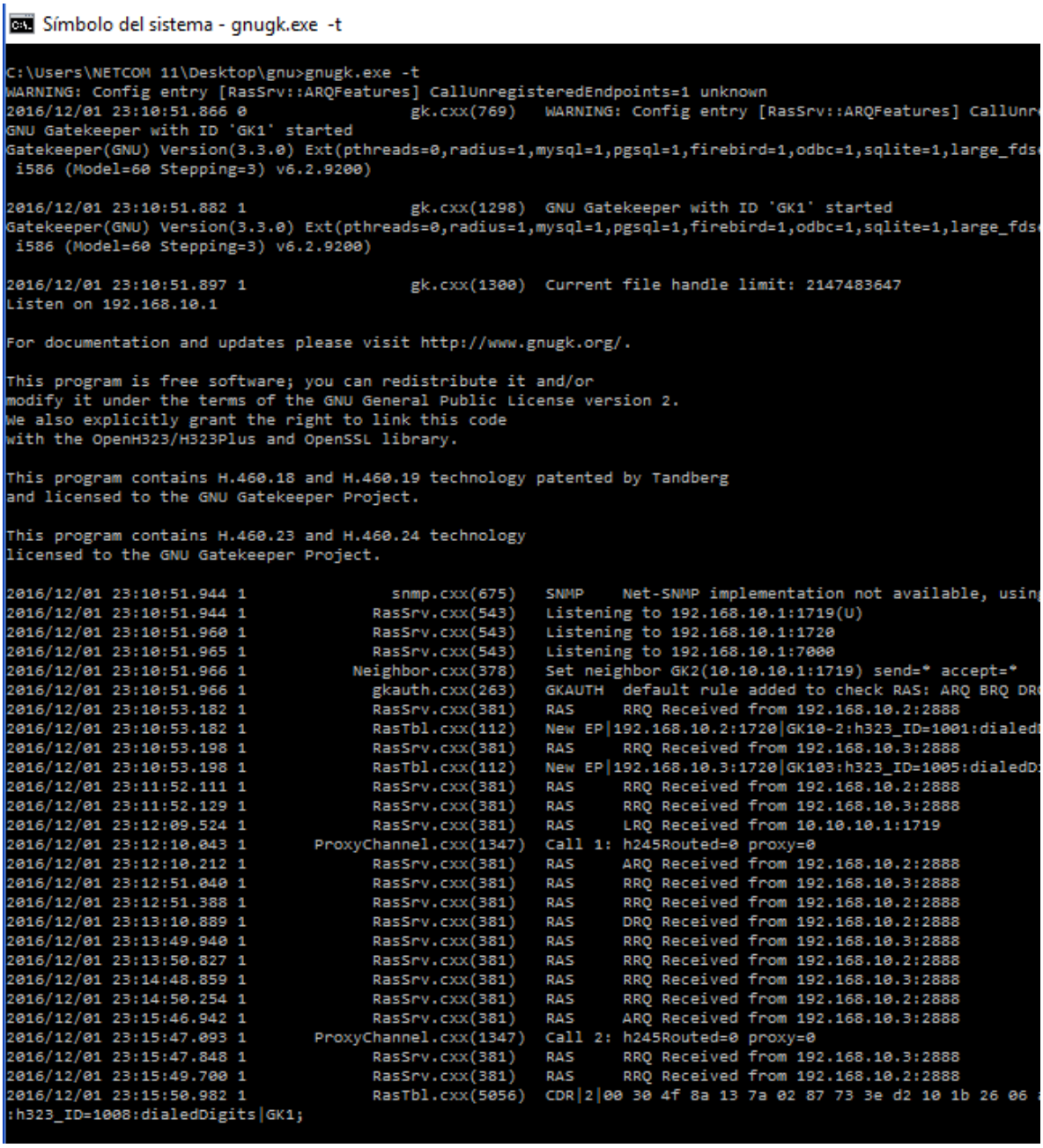


Figura 4- 25. Estado del Gatekeeper.

En la figura se observa Listening to 192.168.10.1:1719 lo que indica el registro del gatekeeper y el puerto 1720 indica la negociación de llamadas H.323.

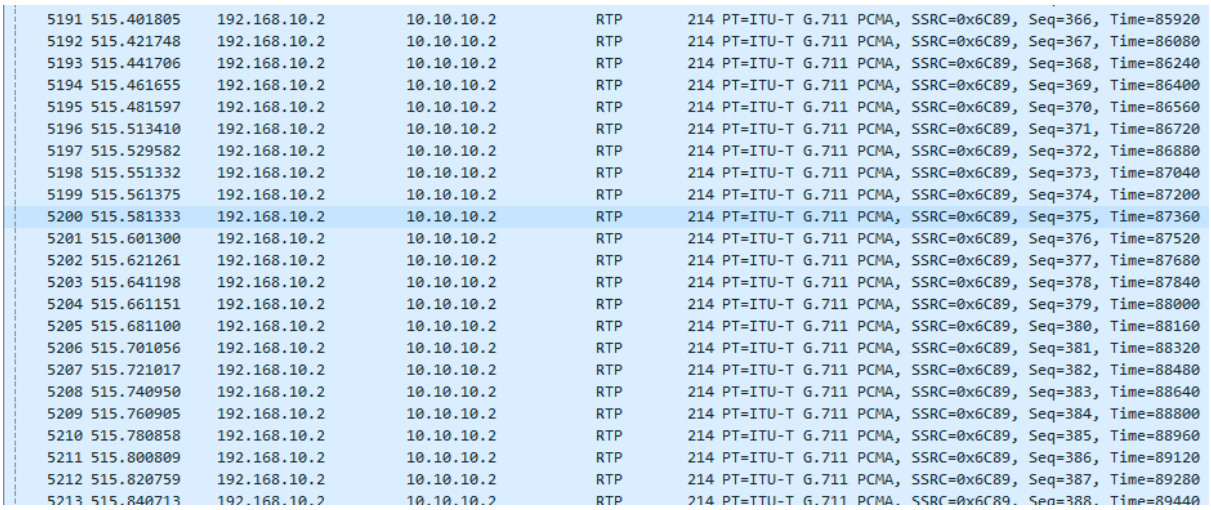
Set Neighbor GK2 (10.10.10.1) indica la dirección IP del Gatekeeper vecino.

send=* accept:* indica que para envío y aceptación de llamadas acepta cualquier extensión.

La solicitud ARQ indica solicitud de admisión de llamada.

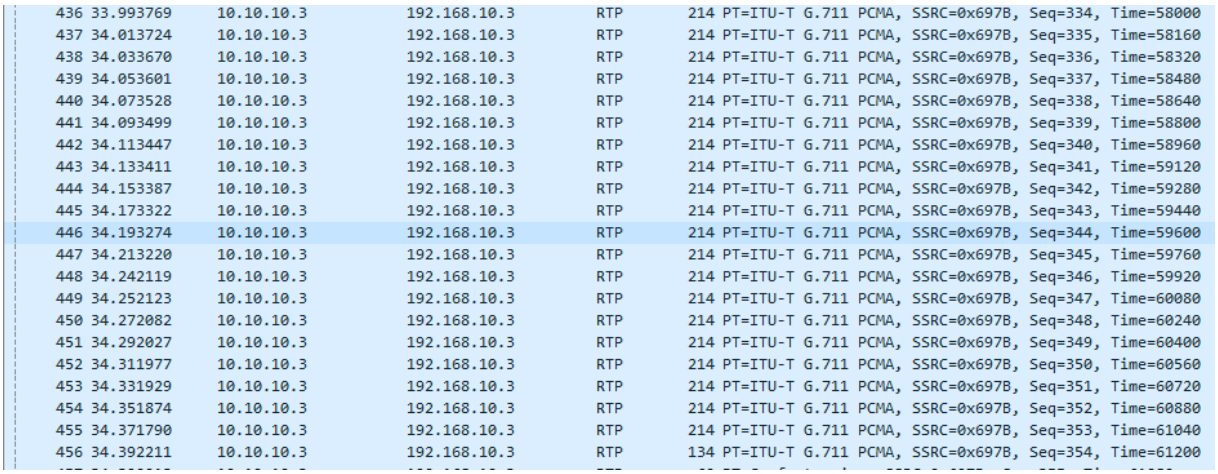
En las figuras 4-26 y 2-27, se capturo los paquetes al momento de establecerse la llamada entre dos terminales.

Puede observarse el trafico RTP (Protocolo de tiempo real), y el tipo de códec utilizado en la llamada de prueba.



5191	515.401805	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=366, Time=85920
5192	515.421748	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=367, Time=86080
5193	515.441706	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=368, Time=86240
5194	515.461655	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=369, Time=86400
5195	515.481597	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=370, Time=86560
5196	515.513410	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=371, Time=86720
5197	515.529582	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=372, Time=86880
5198	515.551332	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=373, Time=87040
5199	515.561375	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=374, Time=87200
5200	515.581333	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=375, Time=87360
5201	515.601300	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=376, Time=87520
5202	515.621261	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=377, Time=87680
5203	515.641198	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=378, Time=87840
5204	515.661151	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=379, Time=88000
5205	515.681100	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=380, Time=88160
5206	515.701056	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=381, Time=88320
5207	515.721017	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=382, Time=88480
5208	515.740950	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=383, Time=88640
5209	515.760905	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=384, Time=88800
5210	515.780858	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=385, Time=88960
5211	515.800809	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=386, Time=89120
5212	515.820759	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=387, Time=89280
5213	515.840713	192.168.10.2	10.10.10.2	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x6C89, Seq=388, Time=89440

Figura 4- 26. Establecimiento de llamada de GK1 a GK2.



436	33.993769	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=334, Time=58000
437	34.013724	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=335, Time=58160
438	34.033670	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=336, Time=58320
439	34.053601	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=337, Time=58480
440	34.073528	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=338, Time=58640
441	34.093499	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=339, Time=58800
442	34.113447	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=340, Time=58960
443	34.133411	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=341, Time=59120
444	34.153387	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=342, Time=59280
445	34.173322	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=343, Time=59440
446	34.193274	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=344, Time=59600
447	34.213220	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=345, Time=59760
448	34.242119	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=346, Time=59920
449	34.252123	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=347, Time=60080
450	34.272082	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=348, Time=60240
451	34.292027	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=349, Time=60400
452	34.311977	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=350, Time=60560
453	34.331929	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=351, Time=60720
454	34.351874	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=352, Time=60880
455	34.371790	10.10.10.3	192.168.10.3	RTP	214 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=353, Time=61040
456	34.392211	10.10.10.3	192.168.10.3	RTP	134 PT=ITU-T G.711 PCMA, SSRC=0x697B, Seq=354, Time=61200

Figura 4- 27. Establecimiento de llamada de GK2 a GK3.

Capitulo V.- Resultados de la implementación.

5.1 Resultados de la implementación SIP

La implementación del protocolo de inicio de sesión (SIP) permitió establecer una arquitectura cliente servidor, en donde el servidor administra las peticiones y los clientes solicitan peticiones, además dentro de esta implementación se sugiere la utilización de detectores de actividad de voz y diversos esquemas de codificación para una configuración adecuada en función de los recursos de la red.

El detector de actividad de voz, también conocido como “supresor de silencios” permite a una red de datos que transporta tráfico de voz a través de una red IP, detectar la ausencia de voz y ahorrar ancho de banda, evitando la generación de paquetes durante los silencios. Las conversaciones incluyen aproximadamente el 60 % del silencio por lo que se concluye que se ahorra aproximadamente el 60 % en el tráfico generado durante una comunicación VoIP.

Para poner a prueba el funcionamiento de todas las extensiones, se generaron llamadas de forma escalonadamente, hasta llegar a las 8 llamadas simultaneas (como se ilustra en la Tabla 9), consiguiendo buena audición sin cortes entre llamadas, lo que nos permitió confirmar que el servicio de implementación llevado a cabo fue exitoso.

Tabla 9. Administración de las llamadas escalonadas SIP

Servidor	Extensión	Códec	Detección de actividad por Voz	Periodo escalonado	Servidor	Extensión
SIP-2	101	G.711	VAD	10 minutos	SIP-1	1001
SIP-2	102	G.711	VAD	10 minutos	SIP-1	1002
SIP-2	103	G.711	VAD	10 minutos	SIP-1	1003
SIP-2	104	G.711	VAD	10 minutos	SIP-1	1004
SIP-2	105	G.711	VAD	10 minutos	SIP-1	1005
SIP-2	106	G.711	VAD	10 minutos	SIP-1	1006
SIP-2	107	G.711	VAD	10 minutos	SIP-1	1007
SIP-2	108	G.711	VAD	10 minutos	SIP-1	1008

5.2 Resultados de la implementación H.323

Durante la implementación del servicio de VoIP mediante la recomendación H.323, se configuraron dos zonas H.323, es decir, lo equivalente a un gatekeeper y dos gateway en modo puente por zona, la comunicación fluyo de manera correcta permitiendo el establecimiento de llamadas entre los terminales H.323 en ambos sentidos (entre las dos zonas H.323).

De igual forma como en el escenario SIP, Para poner a prueba el funcionamiento de todas las extensiones, se generaron llamadas de forma escalonadamente, hasta llegar a las 8 llamadas simultaneas (como se ilustra en la Tabla 10), consiguiendo buena audición sin cortes entre llamadas, lo que nos permitió confirmar que el servicio de implementación llevado a cabo fue exitoso.

Tabla 10. Administración de las llamadas escalonadas H.323

Gatekeeper	Extensión	Códec	Detección de actividad por Voz	Periodo escalonado	Gatekeeper	Extensión
GK2	101	G.711	VAD	10 minutos	**GK1**	1001
GK2	102	G.712	VAD	10 minutos	**GK1**	1002
GK2	103	G.713	VAD	10 minutos	**GK1**	1003
GK2	104	G.714	VAD	10 minutos	**GK1**	1004
Gk2	105	G.715	VAD	10 minutos	**Gk1**	1005
Gk2	106	G.716	VAD	10 minutos	**Gk1**	1006
GK2	107	G.717	VAD	10 minutos	**GK1**	1007
GK2	108	G.718	VAD	10 minutos	**GK1**	1008

Conclusiones

En este trabajo monográfico se presenta una investigación documental que permite conocer a fondo los distintos protocolos y recomendaciones para la implementación de servicios de voz sobre el protocolo de Internet y de igual manera se presenta la implementación práctica de servicios de voz mediante dos de los protocolos VoIP más importantes: SIP y H.323.

Como resultado del presente trabajo se resumen las conclusiones de la siguiente manera:

En cuanto a sus desarrolladores:

SIP es un estándar desarrollado por IETF (Internet Engeneering Task Force), mientras que H.323 fue diseñado por ITU-T (International Telecommunications Union).

En cuanto a su implementación:

SIP es un protocolo de señalización para sesiones interactivas, con características muy parecidas a Internet.

H.323 Proporciona una arquitectura robusta y muy completa, con características muy parecidas a la red de circuitos.

Transporte y control de medios:

La implementación de aplicaciones de voz sobre la red de datos requiere del uso de los protocolos RTP (Real Time Protocol) y RTCP (Real Time Control Protocol) sobre el protocolo UDP por requisitos de tiempo real, aquí se prioriza la rapidez y no la fiabilidad, es decir no se garantiza calidad de servicio.

En cuanto a formato de los mensajes:

H.323 codifica los mensajes en formato binario, al igual que las tramas IP o Ethernet.

SIP emplea formato en texto legible por HTTP o XML.

La codificación binaria permite mayor rapidez mientras que el formato texto tiene un costo computacional elevado lo que reduce el rendimiento y por tanto también consume mayor ancho de banda.

En cuanto a la implementación de los servicios VoIP:

La instalación, configuración y administración de SIP considero que es más cómodo ya que por medio del servidor Elastix permite administrar de manera gráfica cada una de las variables como extensiones, troncales, puertas de salida, contraseñas y direcciones IP.

Por el contrario en H.323 la configuración es a través de un archivo .ini en el cual se tiene que habilitar mediante un conjunto de sentencias tanto el nombre del gatekeeper principal, establecer la zona vecino, Gateway y extensiones, por lo que se tiene que ser muy meticuloso, ya que la ausencia de un punto, una coma y una letra deriva en la caída total de una zona H.323 y con ello todas sus extensiones.

En la implementación de los servicios de VoIP se sugiere la utilización de detectores de actividad de voz y diversos esquemas de codificación para una configuración adecuada en función de los recursos de la red.

La implementación de detectores de actividad de voz permite usar menos ancho de banda ya que no evita la generación de paquetes durante los silencios en la comunicación y con esto hacer uso eficiente del ancho de banda. Por otro lado el usar diversos esquemas de codificación permite hacer uso adecuado del ancho de banda, en función de los recursos de la red.

El uso de una topología exactamente igual en la implementación de los servicios VoIP mediante SIP y H.323, con igual número de teléfonos permitió una comparación más equitativa, en tiempo de instalación, y configuración.

Bibliografía

1.Jonathan Davidson, James Peters. (2002). Voice Over IP: Fundamentals, tercera edición, Estados Unidos de Norteamérica USA: Cisco Company,

2. Kevin Wallace. (2008). Cisco Voice over IP (CVOICE) third edition. USA: Cisco Press.

3. José Manuel Huidobro Moya, David Roldán Martínez. (2006). Tecnología VoIP y telefonía IP. México: Alfaomega.

4. Tony Janevski. (2003). traffic analysis and design of wireless ip networks pdf. Norwood Massachusetts EUA: Artech House.

5. Gonzalo Camarillo. (2002). SIP Demystified . United States of America: McGraw-Hill.

6. http://www.gateway.com/gw/es/AR/content/model/LX.WSS08.001.

7. http://www.gateway.com/gw/es/MX/content/model/NX.Y4VAL.006.

8. http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c01865794

9. http://www.wni.mx/index.php?page=shop.product_details&flypage=flypage_new.tpl&product_id=234&category_id=44&option=com_virtuemart&Itemid=53.

10. http://www.buscalibre.cl/vtech-clio-10b_p_11001123.html

11. http://timerime.com/en/event/2864376/router+cisco+1841

Abreviaturas

VOIP	Voice Over Internet Protocol
QOS	Quality of Service
SIP	Sesion Initiation Protocol
LAN	Local Area Network
ITU	Internacional Telecomunications Union
IFTF	Internet engineering Task Force
PSTN	Public Switched Telephone Network
IP	Internet Protocol
ATM	Asynchronous Transfer Mode
TDM	Time Division Multiplexing
WAN	Wide Area Network
TCP	Transmision Control Protocol
UDP	User Datagram Protocol
ACK:	Acknowledgement
RTP:	Real-time Transport Protocol
RTPC:	Real-time Transport Control Protocol
RDSI:	Integrated Services Digital Network
ERL	Eco Return Loss
PBX:	Private Branch Exchange
BW:	Bandwith

Kbps	kilobit by second
VAD	Voise Activy Detección
SID	Silence Insertion Description
PAQM	Perceptual Audio Quality Audio Measure
PSQM:	Perceptual Speech Quality Measure
PESQ:	Perceptual Evaluation of Speech Quality
MOS:	Mean Opinion Score
ACR	Absolute Category Rating
MNRU	Modulated Noise Reference Unit
FFT	Fast Fourier Transform
VQMon	Voz Quality Mommitoring
ARQ	Admission Request
ACF	Admission Confirm
ARJ	Admission Reject
TCP:	Transmision Control Protocol
UDP:	User Datagram Protocol
GRQ:	Gatekeeper Request
GCF:	Gatekeeper Confirm
RRQ:	Registration Request
RRJ:	Registration Reject
UCF:	Unregistration Confirm
URJ:	Unregistration Request

LRQ:	Location Request
LCF:	Location confirm
LRJ:	Location Rject
IRQ:	Info Request
BRQ:	Banwith Request
SSL:	Secure Sockets Layer
TLS:	Transport Layer Security
SCTP:	Stream Control Transmision Protocol
IETF:	Internet Engineering Task Force
NAT:	Network Adres Translation
HTTP	Hypertext Transfer Protocol
SDP	Sesion Description protocol
UA	User Agents
UAC	User Agent Client
UAS	User Agent Server

Anexos

Instalación de elastix

Para iniciar la instalación en necesario introducir el CD de instalación de Elastix 2.4.0 versión estable, como se muestra en la figura A-1.

Figura A-1. Pantalla de bienvenida del Sistema Operativo Elastix.

La siguiente imagen nos solicita escoger un lenguaje para usar durante el proceso de instalación del sistema operativo, tal como se muestra en la figura A-2.

Figura A-2. Elección de preferencia del proceso de instalación

Se puede observar que el lenguaje ha cambiado al español, la siguiente ventana nos permite elegir el tipo de teclado, la figura A-3 muestra que la opción elegida para el teclado es español.

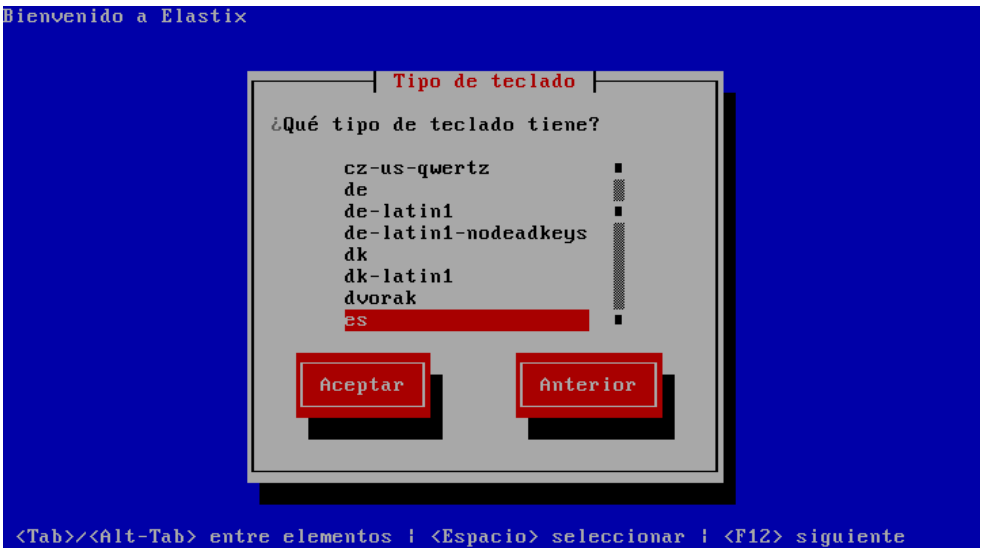


Figura A-3. Elección del tipo de teclado.

En este parte del proceso de instalación se observa la elección del disco duro donde se instalara el s. o. Elastix, en este caso la opción a elegir es Si tal como muestra la figura A-4.

Figura A-4. Aviso

de inicializar la unidad de disco duro.

El siguiente paso es muy importante ya que de esto depende la instalación exitosa del sistema, para este caso seleccionaremos la primera opción de **particiones en dispositivos seleccionados y crear diseño predeterminado** ver figura A-5

Figura A-5.
Selección del Tipo de particionamiento..

La siguiente ventana de aviso requiere confirmación de la acción, ya que se borraran las particiones del disco duro y solo existirá una partición donde se instalara el sistema Elastix ver figura A-6.

Figura A-6. Confirmación de partición.

La figura A-7 muestra la opción de configurar la interfaz de red, debido a que su función principal es ser un servidor, su dirección es fija, por lo tanto durante el proceso se configura, seleccionar la opción Sí.

Figura A-7. Pregunta sobre configuración de interfaz de red.

En la figura A-8 se puede observar que la tarjeta de red es Intel Corporation seleccionar la opción de activar al inicio y activar soporte para IPv4, seleccionar tal como se muestra en la imagen IPv4, enter en Aceptar.

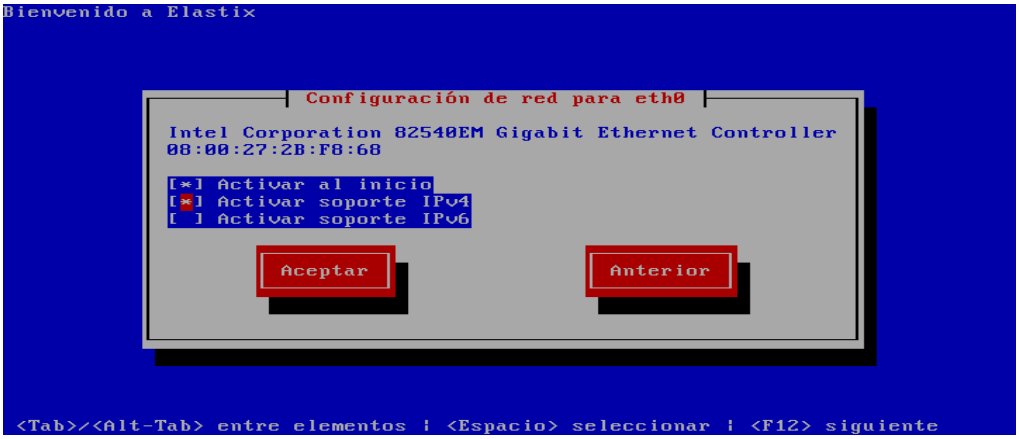


Figura A-8.- Configuración de red para la interfaz eth0.

La figura A-9 muestra la configuración IPv4 para la única interfaz que existe en la PC, seleccionar **configuración manual TCP/IP** y establecer la dirección fija del servidor con su máscara de red.

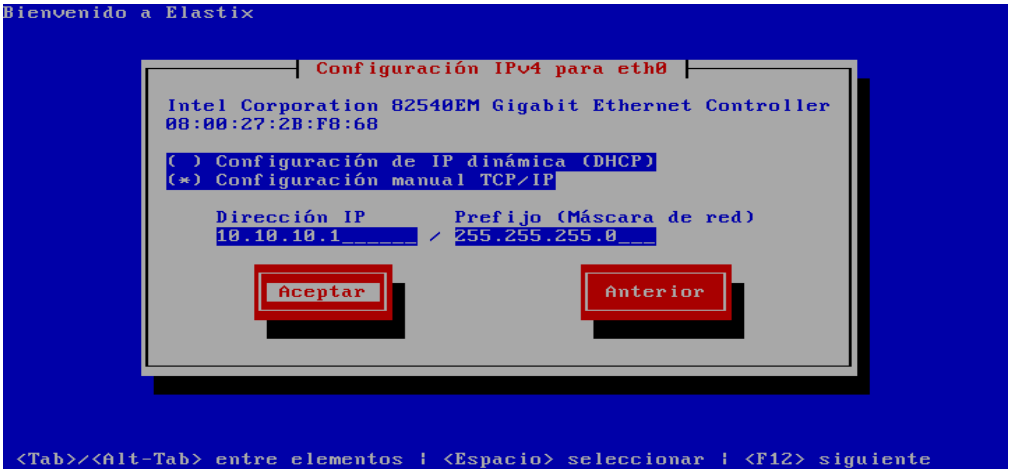


Figura A-9 Configuración IPv4 para eth0.

En esta pantalla se solicita la configuración de red misceláneas, tal como se muestra en la figura A-10 asignar los datos según la configuración específica de cada necesidad, en este caso únicamente se establece la puerta de enlace predeterminada.

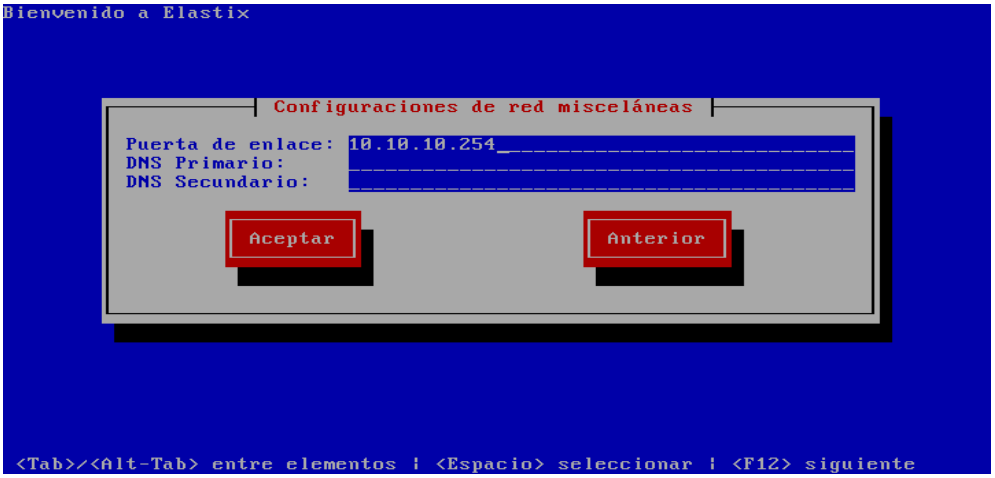


Figura A-10. Configuración de red miscelánea.

En la Figura A-11 se establece el nombre del servidor y el tipo de direccionamiento en este caso manual.

Figura A-11. Configuración del nombre del host.

En la Figura A-12 Se establece la selección del huso horario, seleccionar de acuerdo a la ubicación en este caso **America/Mexico City.**

Figura A-12. Selección huso horario.

La siguiente pantalla solicita establecer la contraseña del root y mediante la cual se tendrá acceso al servidor para su configuración.

Figura A-13. Contraseña del root.

El sistema operativo Elastix solicita obligatoriamente asignar password a la base de datos MySQL, con lo cual se procede a asignarle una, tal como se m,uestra en la figura A-14.

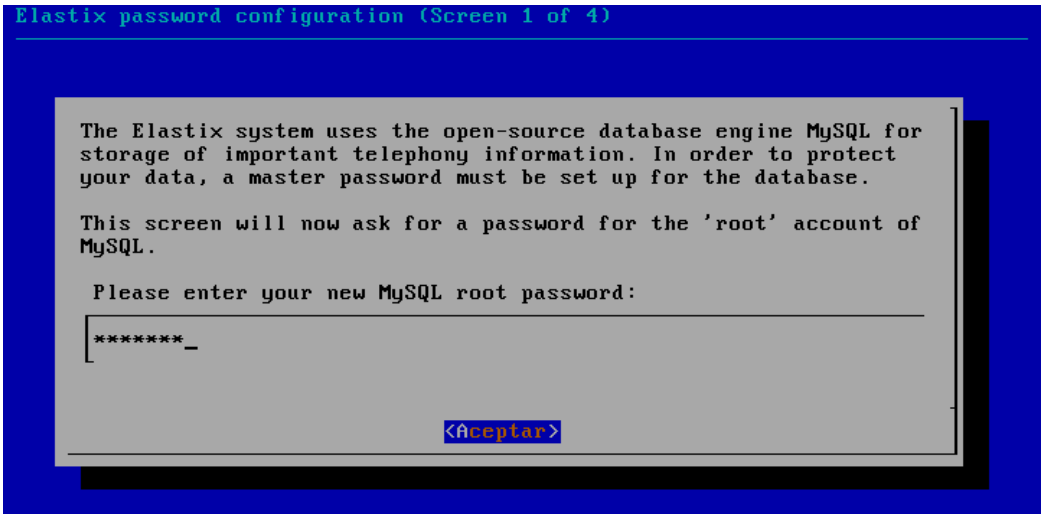


Figura A-14. Asignación de password a MySQL.

En la figura A-15 se solicita password para administrar vía HTTP el PBX de elastix.

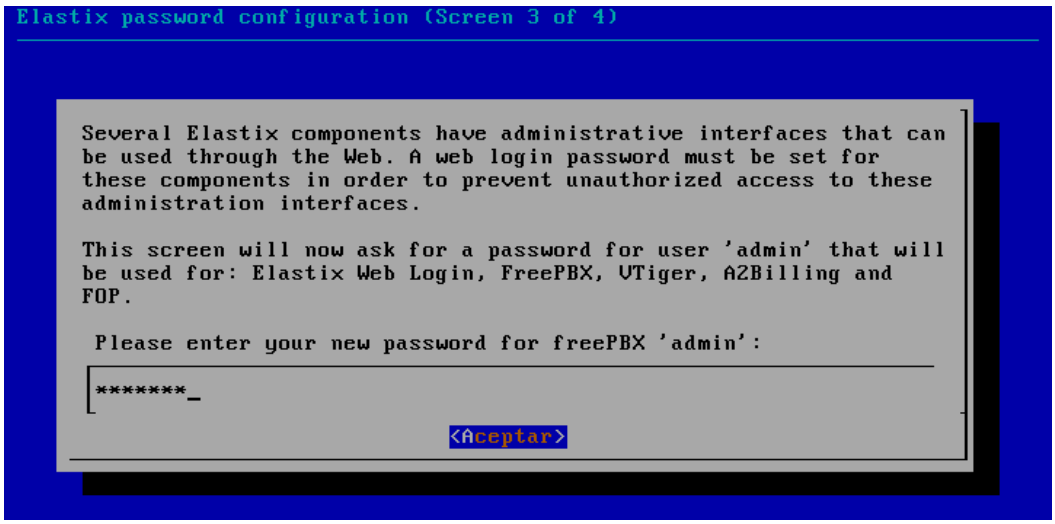


Figura A-15. Asignación de password para la interfaz gráfica.

Configuración de Elastix grafica desde cualquier PC a través de un navegador.

Después de finalizar el proceso de instalación se configura a través del navegador web con la dirección ip fija del servidor, nos manda la siguiente pantalla que muestra la Figura A-16.

Figura A-16. Interfaz gráfica de elastix.

Dashboard (Tablero de instrumentos)

Elastix incorpora por defecto en su Dashboard el monitor de los recursos del sistema a los que se tiene acceso una vez ingresado como root, desde el cual se observa el estado de los procesos y uso de los recursos más importantes del sistema, ver figura A-17.

Dentro de los datos que proporciona están:

- Memoria RAM.
- CPU.
- Disco Duro.
- Nivel de llamadas simultaneas.
- Etc.

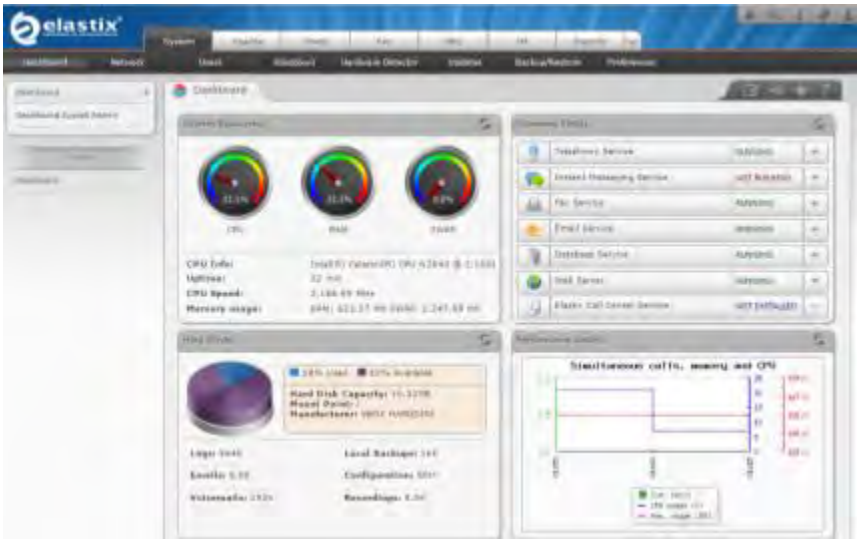


Figura A-17. Dashboard de elastix 2.4.

Network

El menu Network que muestra la Figura A-18 permite observar la direccion IP, el nombre del equipo, puerta de enlace predeterminado y DNS.

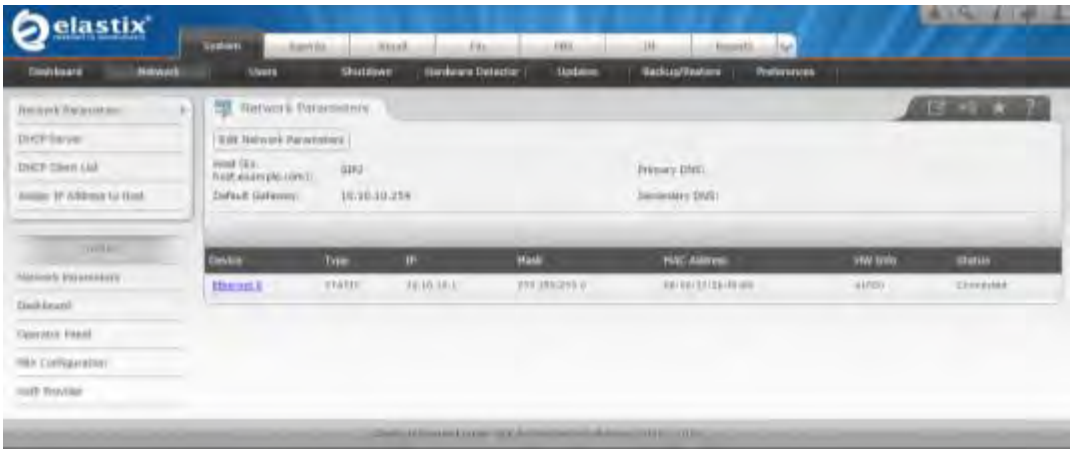


Figura A-18. Network

DHCP

En la figura A-19 se muestra la pestaña DHCP en la cual es posible configurar el direccionamiento automático para dispositivos finales.

Figura A-19. DHCP.

Creación de usuarios.

En el menú que muestra la Figura A-20 se observa que hay un solo usuario el administrador, en esta sección se pueden crear usuarios con diferentes niveles de acceso para utilizar la interfaz gráfica de Elastix.

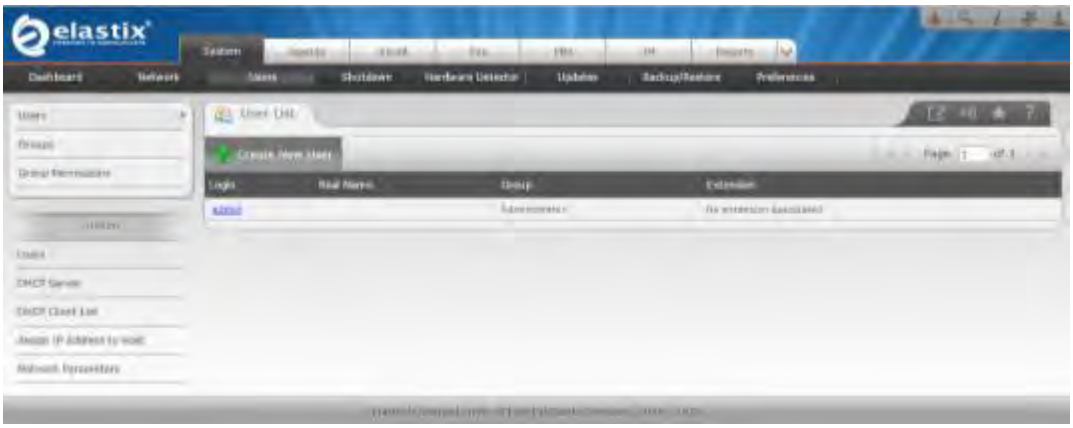


Figura A-20. Creación de usuarios.