



UNIVERSIDAD DE QUINTANA ROO  
DIVISIÓN DE CIENCIAS E INGENIERÍA

---

**Análisis del Comportamiento de la Pérdida de Paquetes a Ráfagas en una Comunicación VoIP y sus Implicaciones en la Calidad de Servicio**

---

TRABAJO DE TESIS  
PARA OBTENER EL GRADO DE  
**Ingeniero en Redes**

PRESENTA

**Br. Erika Eunice Briceño Arceo**

DIRECTOR DE TESIS  
**Dr. Homero Toral Cruz**

ASESORES

**Ing. Pablo Velarde Alvarado**

**Dr. Freddy Ignacio Chan Puc**

**L. I. Luis Fernando Mis Ramírez**

**Ing. Francisco Méndez Martínez**



CHETUMAL QUINTANA ROO, MÉXICO, DICIEMBRE DE 2016



**UNIVERSIDAD DE QUINTANA ROO**  
**DIVISIÓN DE CIENCIAS E INGENIERÍA**


---

**TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL COMITÉ  
DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA  
OBTENER EL GRADO DE:  
INGENIERO EN REDES**

---

**Comité de Trabajo de Tesis**

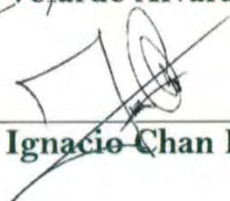
**DIRECTOR:**

  
\_\_\_\_\_  
**Dr. Homero Toral Cruz**

**ASESOR:**

  
\_\_\_\_\_  
**Ing. Pablo Velarde Alvarado**

**ASESOR:**

  
\_\_\_\_\_  
**Dr. Freddy Ignacio Chan Pue**



CHETUMAL QUINTANA ROO, MÉXICO, DICIEMBRE DE 2016

## **Agradecimientos**

A Dios por haberme brindado salud, vida y por acompañarme en todo momento.

A mis padres y hermano por su apoyo, amor, comprensión y ayuda que me han brindado durante toda mi vida.

A la Universidad de Quintana Roo por darme la oportunidad de estudiar la carrera de Ingeniería en Redes y formar parte de ésta.

A mi director de tesis, el Dr. Homero Toral Cruz por su apoyo y guía durante el proceso de éste y durante la carrera.

A mis maestros que me han ayudado a orientarme y por su atención durante mi carrera.

A mis amigos y compañeros que fui conociendo durante este transcurso de mi preparación profesional y que compartimos buenos momentos dentro y fuera de la universidad.

## **Dedicatoria**

A Dios, a mis padres y hermano

## RESUMEN

La tecnología de voz sobre IP o también conocida como VoIP, constituye una forma de transmitir voz sobre una red de conmutación de paquetes, ésta tecnología está en constantes cambios, evolución, y permite la convergencia de diferentes medios, tales como: voz, datos, y video.

Hace aproximadamente una década, la calidad de servicio de aplicaciones en tiempo real (tales como la voz) sobre redes de datos, se veía afectada principalmente por el ancho de banda y otros parámetros de calidad de servicio, tales como: retardos y pérdida de paquetes. Actualmente, el incremento y uso óptimo del ancho de banda es una tarea mucho más sencilla, utilizando técnicas avanzadas de compresión de voz, usando enlaces de banda ancha o haciendo uso de novedosas técnicas de multiplexación, entre otras.

Sin embargo, el problema de calidad de servicio en estos sistemas en tiempo real persiste y el reto se centra en disminuir los retardos y prevenir o atenuar los efectos de la pérdida de paquetes.

Una de las principales métricas bajo estudio es la pérdida de paquetes, la cual se puede presentar de forma homogénea o uniforme y a ráfagas.

La pérdida de paquetes se puede presentar de manera homogénea o uniforme, lo cual implica que la pérdida de un paquete en particular es independiente de si se pierden o no paquetes anteriores. Sin embargo, diversos estudios han demostrado que la pérdida de paquetes presenta naturaleza ráfagoza y muestra una dependencia temporal. Por lo tanto, si el paquete  $n$  se pierde, entonces existe una mayor probabilidad de que el paquete  $n + 1$  también se pierda.

En base a los puntos anteriores, en esta tesis, se propone realizar un estudio sobre el comportamiento temporal de la pérdida de paquetes en una comunicación VoIP y sus implicaciones en la calidad de servicio percibida por el usuario final.

## Lista de Abreviaturas

ACK	Acknowledgement
ATM	Asynchronous Transfer Mode
CODEC	Coder-Decoder
CPU	Central Processing Unit
FEC	Forward Error Correction
GSM	Global System for Mobile
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU-T	International Telecommunication Union
MCU	Multipoint Control Unit
MIPS	Millions of Instructions Per Second
MOS	Mean Opinion Score
PLC	Packet Loss Concealment
PLR	Packet Loss Rate
PSTN	Public Switched Telephone Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Registration, Admission and Status
RTCP	Real Time Control Protocol

RTP	Real-Time Transport Protocol
SID	Silence Insertion Description
SIP	Session Initiation Protocol
SONET	Synchronous Optical Networking
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VAD	Voice Activity Detection
VoIP	Voice over Internet Protocol

## Contenido

<b>CAPÍTULO 1. INTRODUCCIÓN</b> .....	1
Justificación.....	2
Objetivos.....	3
Objetivo general.....	3
Objetivos particulares.....	3
Planteamiento del Problema.....	3
<b>CAPÍTULO 2. Tecnología de VoIP</b> .....	5
2.1 Ventajas de VoIP.....	5
2.2 Redes de conmutación de circuitos.....	8
2.2.1 Red telefónica pública conmutada.....	9
2.3 Redes de conmutación de paquetes.....	10
2.4 Protocolos de Internet.....	12
2.4.1 IP.....	14
2.4.2 TCP.....	15
2.4.3 UDP.....	16
2.4.4 RTP.....	17
2.4.5 RTCP.....	18
2.5 Protocolos de señalización.....	19
2.5.1 H.323.....	20
2.6.2 SIP.....	27
<b>CAPÍTULO 3. QoS</b> .....	33
3.1 Concepto de calidad de la voz.....	33
3.2 Factores que influyen en la calidad.....	35
3.2.1 Disponibilidad.....	35
3.2.2 Jitter.....	36
3.2.3 Pérdidas.....	37
3.2.4 Retardo.....	38
3.2.5 Eco.....	41
3.2.6 Ancho de banda.....	42
3.3 Medición de la calidad de la voz.....	44
3.4 Método subjetivo: MOS.....	45



3.5 Modelo E .....	46
<b>CAPÍTULO 4. PÉRDIDAS DE PAQUETES</b> .....	49
4.1 Distribución de pérdida de paquetes: Gaps y Bursts .....	50
4.2 Comportamiento de la pérdida de paquetes: microscópico y macroscópico .....	51
4.4 Modelos de pérdida de paquetes: Cadenas de Markov .....	52
4.5 Mecanismos para atenuar la pérdida de paquetes .....	55
<b>CAPÍTULO 5. MEDICIONES</b> .....	58
5.1 Metodología para emular pérdida de paquetes .....	58
5.2 Escenario de medición.....	60
5.3 Realización de las mediciones .....	61
<b>CAPÍTULO 6. ANÁLISIS DE RESULTADO</b> .....	69
6.1 Análisis de MOS.....	69
6.2 Análisis de PLR.....	71
<b>CAPÍTULO 7. CONCLUSIONES</b> .....	77
<b>Referencias</b> .....	79

## Índice de Tablas

Tabla 1 Algunos CODECs más comunes para telefonía.....	27
Tabla 2 Relación entre el retardo en un solo sentido y la calidad de la voz .....	39
Tabla 3 Características de algunos CODECs .....	40
Tabla 4 Evaluación de la calidad de la voz a partir del modelo E.....	47

## Índice de Figuras

Figura 1 Red de conmutación de circuitos.....	9
Figura 2 Conmutación de paquetes .....	11
Figura 3 Modelo de referencia TCP/IP .....	13
Figura 4 Estructura IP .....	14
Figura 5 Estructura TCP .....	15
Figura 6 Estructura UDP .....	16
Figura 7 Encapsulamiento de paquetes de voz.....	18
Figura 8 Estructura de Terminal H.323 .....	21
Figura 9 Elementos de una red H.323 .....	22

Figura 10 Señalización H.323 .....	25
Figura 11 Ejemplo de llamada SIP .....	31
Figura 12 Relación entre la inteligibilidad de la codificación de la voz .....	35
Figura 13 Procesamiento de la señal de voz entre los extremos.....	39
Figura 14 Puntos en los que se puede activar la VAD .....	43
Figura 15 Comportamiento microscópico y macroscópico.....	52
Figura 16 Cadena de Markov de 2 estados .....	53
Figura 17 Método interleaving.....	56
Figura 18 a) Escenario de medición real, b) Escenario de medición emulada.....	61
Figura 19 Creación de nueva sesión.....	62
Figura 20 Configuración de una sesión .....	62
Figura 21 Selección de interfaz de captura .....	63
Figura 22 Iniciar comunicación.....	63
Figura 23 Captura de los patrones de tráfico.....	64
Figura 24 Selección de flujo .....	64
Figura 25 Decodificación de flujos UDP .....	65
Figura 26 Mostrar todos los flujos RTP .....	65
Figura 27 Flujo RTP.....	66
Figura 28 Configuración, para el tamaño de paquetes de 40 ms .....	67
Figura 29 Evaluación del MOS ( $PS = 20\ ms$ ) .....	70
Figura 30 Evaluación del MOS ( $PS = 40\ ms$ ) .....	70
Figura 31 Distribución temporal del $PLR$ .....	72
Figura 32 Número de ráfagas de pérdida de paquetes ( $PS = 40\ ms$ ).....	73
Figura 33 Longitud promedio de paquetes perdidos durante las ráfagas ( $PS = 40\ ms$ ) .....	74
Figura 34 Número de gaps entre las ráfagas de pérdida de paquetes ( $PS = 40\ ms$ ).....	75

# CAPÍTULO 1

## CAPÍTULO 1. INTRODUCCIÓN

Hace aproximadamente una década, la calidad de servicio de aplicaciones en tiempo real sobre redes de datos, se veía afectada principalmente por el ancho de banda y otros parámetros de calidad de servicio, tales como: retardos y pérdida de paquetes. En esa época, se creía que, si se incrementaba el ancho de banda, se podrían solucionar estos problemas de calidad. Actualmente, el incremento y uso óptimo del ancho de banda es una tarea mucho más sencilla, utilizando técnicas avanzadas de compresión de voz, usando enlaces de banda ancha o haciendo uso de novedosas técnicas de multiplexación, entre otras. Sin embargo, el problema de calidad de servicio en estos sistemas en tiempo real persiste y el reto se centra en disminuir los retardos y prevenir o atenuar los efectos de la pérdida de paquetes [1].

Entre los diferentes elementos de calidad de servicio, la pérdida de paquetes es el deterioro principal que hace a la voz sobre el protocolo de Internet perceptualmente diferente de la red telefónica pública conmutada, [2]. Debido al comportamiento dinámico de las redes de paquetes, la pérdida de paquetes puede mostrar una gran variedad de distribuciones. La distribución de paquetes perdidos más estudiada en pruebas de calidad de voz es la de Bernoulli (pérdida de paquetes homogénea o uniforme), [3]. La pérdida de paquetes se puede presentar de manera homogénea o uniforme, lo que implica que la pérdida de un paquete en particular es independiente de si se pierde o no paquetes anteriores. Sin embargo, diversos estudios han demostrado que la pérdida de paquetes presenta naturaleza ráfaga y muestra una dependencia temporal. Por lo tanto, si el paquete  $n$  se pierde, entonces existe una mayor probabilidad de que el paquete  $n + 1$  también se pierda. Por consiguiente, existe una fuerte correlación entre la pérdida de paquetes consecutivos, lo que resulta en un comportamiento de pérdida de paquetes a ráfagas, [4].

Por otro lado, para evaluar la calidad de servicio, existen diversas herramientas basadas principalmente en el MOS y el Modelo E. Dichos modelos no contemplan

el comportamiento de pérdida de paquetes a ráfagas, es decir, sólo consideran el valor numérico de pérdida.

En base a los puntos anteriores, en el presente trabajo, se propone realizar un estudio sobre el comportamiento de pérdida de paquetes a ráfagas en una comunicación VoIP y sus implicaciones en la calidad de servicio percibida por el usuario final.

## Justificación

Una estrategia para mejorar el desempeño de los servicios de voz sobre las redes de datos que no garantizan calidad de servicio, es mediante el diseño adecuado de aplicaciones VoIP y mecanismos de QoS. Para lograr un diseño adecuado de aplicaciones VoIP y mecanismos de QoS, es necesario conocer el comportamiento de los principales parámetros que determinan la calidad de servicio que percibe el usuario final. Para caracterizar dichos parámetros se requiere realizar extensivas mediciones de tráfico de voz bajo diversos escenarios de red. En base a lo mencionado anteriormente, en este proyecto, se realizará un análisis y caracterización del comportamiento de pérdida de paquetes en una comunicación VoIP y su impacto en la calidad de servicio percibida por el usuario final. Dicho análisis, puede servir como referencia para proponer mejoras en los modelos utilizados para evaluar la calidad de servicio de aplicaciones VoIP que no consideran el fenómeno de pérdida a ráfagas y el diseño adecuado de aplicaciones VoIP y mecanismos de QoS.

## Objetivos

### Objetivo general

Analizar el comportamiento de pérdida de paquetes a ráfagas en una comunicación VoIP y sus implicaciones en la calidad de servicio percibida por el usuario final.

### Objetivos particulares

- Generar tráfico de voz mediante una aplicación VoIP en software
- Capturar el tráfico utilizando la herramienta Wireshark
- Procesar los patrones de tráfico capturados
- Generar vectores de pérdida de paquetes a partir de los números de secuencia

## Planteamiento del Problema

Como se mencionó anteriormente, en los sistemas VoIP es de gran importancia analizar el comportamiento temporal de la pérdida de paquetes bajo diversos porcentajes y distribuciones. Sin embargo, supongamos que en una comunicación real de VoIP se desea obtener un porcentaje específico de pérdida de paquetes; esto podría tardar mucho tiempo en suceder o tal vez nunca pasaría. No obstante, es posible emular diferentes condiciones de pérdida de paquetes en un sistema de VoIP mediante cadenas de Markov, para representar diversas condiciones de tráfico de red y evaluar sus implicaciones en la calidad de servicio percibida por el usuario final.

# CAPÍTULO 2

## CAPÍTULO 2. Tecnología de VoIP

La voz sobre IP o VoIP es una tecnología que permite transmitir voz sobre redes de conmutación de paquetes. Las redes de conmutación de paquetes también son conocidas como redes IP [5]. Voz sobre IP representa un gran cambio significativo respecto a la manera tradicional de realizar llamadas telefónicas. La tecnología de VoIP se puede utilizar en diferentes redes de comunicación, tales como redes de banda ancha (DSL/ cable), WLAN (IEEE 82.11) y 3G celular [6].

### 2.1 Ventajas de VoIP

La tecnología VoIP presenta un conjunto de ventajas respecto a la transmisión de voz sobre la red telefónica pública conmutada (PSTN, Public Switched Telephone Network), las más importantes se describen a continuación:

- **Disminución de costos:** Debido a que VoIP emplea Internet como medio de transporte, el único costo que se genera es el correspondiente a la facturación mensual de Internet del proveedor de servicio (ISP, Internet Service Provider) Hoy en día el servicio de Internet más común es mediante ADSL que se puede emplear de forma ilimitada y conlleva un costo fijo o tarifa plana mensual.
- **Uso más eficiente del ancho de banda.** Sobre una línea física de teléfono en la PSTN, únicamente dos personas pueden hablar al mismo tiempo. Mientras que, con la tecnología VoIP, sobre una línea física es posible transmitir un conjunto de llamadas a la vez. VoIP utiliza un conjunto amplio de codificadores de voz, para comprimir los paquetes de voz durante la transmisión, lo cual permite transferir una cantidad mayor de información sobre una línea física. Como resultado, se puede establecer más llamadas a través de una única línea de acceso.



- **Hardware y software más accesibles.** Una opción para realizar una comunicación VoIP es mediante el uso de hardware básico como una computadora, una tarjeta de sonido, altavoces y un micrófono. Por otro lado, existen diferentes aplicaciones en software que pueden ser usadas para establecer comunicaciones de voz sobre la red de paquetes. Algunos ejemplos de aplicaciones ampliamente utilizadas son Skype o Net2Phone. Además, en la mayoría de los casos no será necesario hacer nuevas instalaciones de cableado telefónico, ya que VoIP se integra con la red de datos existente en la gran mayoría de empresas y hogares.
- **Servicios más atractivos.** La tecnología VoIP permite realizar llamadas en cualquier lugar del mundo únicamente empleando tu cuenta VoIP. De esta forma, el servicio de telefonía puede ser tan portable como el e-mail, es decir, no limita la movilidad del abonado. Otras prestaciones que ofrece VoIP son el reconocimiento de llamada, posibilidad de crear números virtuales o el contestador automático, por poner algunos ejemplos.  
Al estar basada en la tecnología de conmutación de paquetes, es posible transmitir imágenes, video o texto a la vez que la voz. De esta forma, puedes hablar con alguien a la vez que le envías archivos o incluso que te está viendo a través de una webcam (videollamadas).
- **Esquema de red flexible.** La red que proporcionará servicio de VoIP no necesita tener un esquema o topología en concreto. Esto hace posible que una organización pueda hacer uso de diversas tecnologías, tales como ATM, SONET o Ethernet. Cuando empleamos VoIP, la complejidad de la red inherente en las conexiones de la PSTN es eliminada, creándose una infraestructura flexible que puede soportar muchos tipos de comunicación. El sistema estará más estandarizado, requerirá menos equipamiento y su tolerancia a fallos será mayor.
- **Teletrabajo.** Si trabaja en una organización que emplea una intranet o extranet, podrás acceder a tu oficina desde casa a través de VoIP. Puedes convertir tu hogar en una parte de la oficina y usar remotamente la voz, el fax o los servicios de datos de tu lugar de trabajo a través de la intranet de

la oficina. La naturaleza portátil de la tecnología VoIP está provocando que gane popularidad, ya que proporciona una gran cantidad de comodidades impensables hace unos años. La portabilidad tanto de hardware como de servicios se está convirtiendo cada día en algo más normal, y en ese contexto VoIP encaja perfectamente.

- **Fax sobre IP.** Los problemas de los servicios de fax sobre la PSTN son el alto costo que conllevan para largas distancias, la atenuación de la calidad en las señales analógicas y la incompatibilidad entre algunas máquinas cuando se comunican. La transmisión de fax en tiempo real sobre IP simplemente utiliza una interfaz de fax para convertir los datos en paquetes y asegura que éstos serán entregados completamente y de forma segura. Otra ventaja de este sistema es que ni siquiera necesitamos una máquina fax para enviar y recibir fax.
- **Desarrollo de software más productivo.** VoIP puede combinar diferentes tipos de datos, enrutándolos y señalizándolos de forma muy flexible y robusta. Como resultado de esto, los desarrolladores de aplicaciones de red encontrarán más fácil crear y desplegar aplicaciones que realicen comunicaciones de datos empleando VoIP. Además, la posibilidad de implementar VoIP en navegadores web y servidores proporciona un beneficio tanto productivo como competitivo a esta tecnología [7].

## 2.2 Redes de conmutación de circuitos

Las comunicaciones mediante la conmutación de circuitos implican la existencia de un camino o canal de comunicaciones dedicado entre origen y destino, que es una secuencia de enlaces físicos conectados entre nodos de red los cuales son a través de conmutadores. Un conmutador es un dispositivo con  $n$  entradas y  $m$  salidas, el cual crea una conexión física temporal entre un enlace de entrada y un enlace de salida. El número de entradas no tiene que coincidir con el de salidas [8] y [9].

La comunicación vía la conmutación de circuitos implica tres fases:

- 1. Establecimiento del circuito**
- 2. Transferencia de datos**
- 3. Desconexión del circuito**

La comunicación de las redes de conmutación se empieza estableciendo un circuito virtual, es decir, un camino entre origen y destino por el que circularán los paquetes, (ver Figura 1), seguidamente empieza la transferencia de datos donde los paquetes van pasando por el circuito virtual que se creó entre los conmutadores, de manera que todos los paquetes llegaran exactamente en el mismo orden en que se generaron. Una vez que todos los paquetes sean enviado y no haya más paquetes que enviar o se haya finalizado la conexión, prosigue la desconexión del circuito, es decir, que los conmutadores liberan sus entradas y salidas para otra conexión, [10].

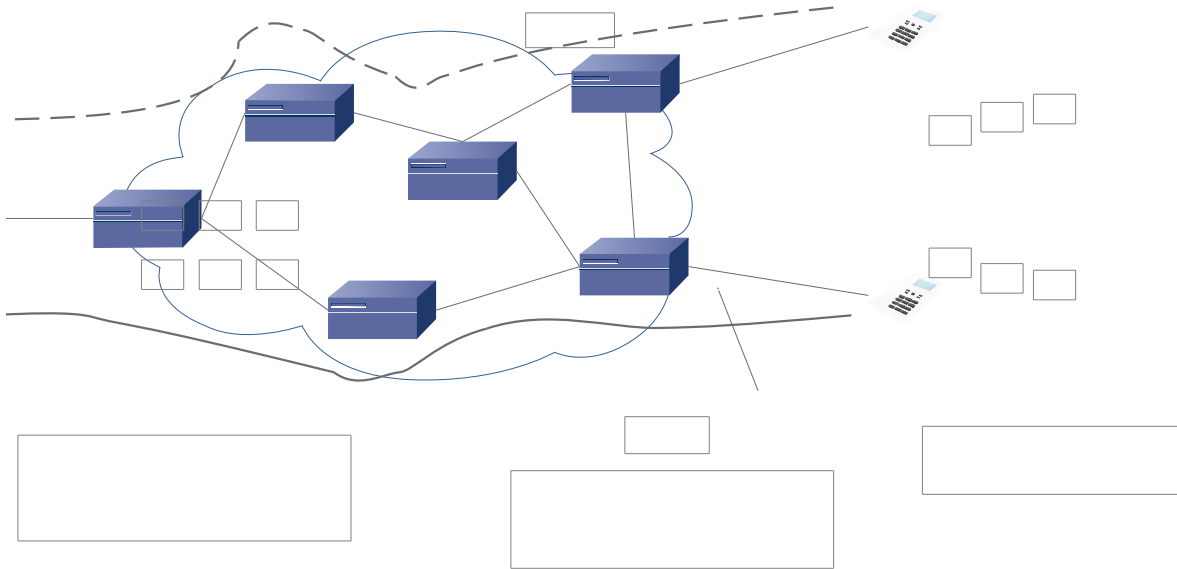


Figura 1 Red de conmutación de circuitos

### 2.2.1 Red telefónica pública conmutada

La red telefónica pública conmutada o mejor conocida como PSTN (por sus siglas en inglés) es básicamente una red basada en circuitos. Esta red tiene la capacidad de soportar o cubrir telefonía fija y móvil; originalmente fue una red analógica, sin embargo, actualmente es una red en su mayoría digital [11].

La red telefónica está compuesta básicamente por los siguientes elementos:

- **Nodos de conmutación.** Existen dos tipos de nodos: los que se denominan centrales locales, en los cuales se conectan los usuarios de la red y los que se denominan centrales de tránsito que son los encargados de encaminar las comunicaciones permitiéndoles que puedan llegar a los destinos solicitados.

- **Enlaces.** Los enlaces que se usan en la PSTN para interconectar las centrales locales entre sí, y con las centrales de tránsito, se suelen denominar enlaces troncales por la cantidad de canales de voz.
- **Enlaces de abonado.** Es un canal de comunicación que conecta al equipo, o los equipos terminales del usuario, con la central local, de que será tributario. También conocido como par de abonado o como “local loop”.
- **Equipos terminales.** Son los equipos que cada usuario podrá conectar a la red de acuerdo con las prestaciones que la misma pueda brindar, el primero y más importante que debe considerarse en esta red es precisamente el teléfono [12].

### 2.3 Redes de conmutación de paquetes

Las redes de conmutación de paquetes, funciona de una manera muy diferente a la red de conmutación de circuitos. Los datos son transmitidos en unidades discretas formadas por bloques de longitud variable denominados paquetes. Por lo cual la red establece la longitud máxima del paquete, y si en una transmisión se presenta paquetes de gran tamaño, éstos se dividen en paquetes más pequeños. Cada paquete es tratado de forma independiente en cada nodo de la red, por lo que cada paquete contiene no sólo datos, sino también una cabecera con información de control (como códigos de prioridad y las direcciones origen y destino), de esta manera, el nodo podrá tomar decisiones de encaminamiento más adecuadas a cada caso. La implicación inmediata es que los paquetes pueden llegar desordenados al destino. Sobre este tipo de redes, el servicio suele ser no orientado a la conexión, es decir, que al no haber una reserva de recursos previa es posible que algunos paquetes se pierdan, por ejemplo, al ser descartados por los nodos de la red en caso de congestión [10] y [9].

En la Figura 2, podemos observar que un terminal A quiere establecer conexión con los terminales B y C de manera independiente.

Lo primero que hace el terminal A es generar la información que le quiere enviar a cada terminal respectivamente, ésta información es dividida en paquetes que llevan la dirección destino. Los paquetes no seguirán un camino fijo, es decir, que éstos viajarán por diferentes nodos hasta llegar al destino, pero los paquetes no siempre llegan en el mismo orden en que fueron emitidos, también se puede presentar que algún o algunos se pierdan en el camino.

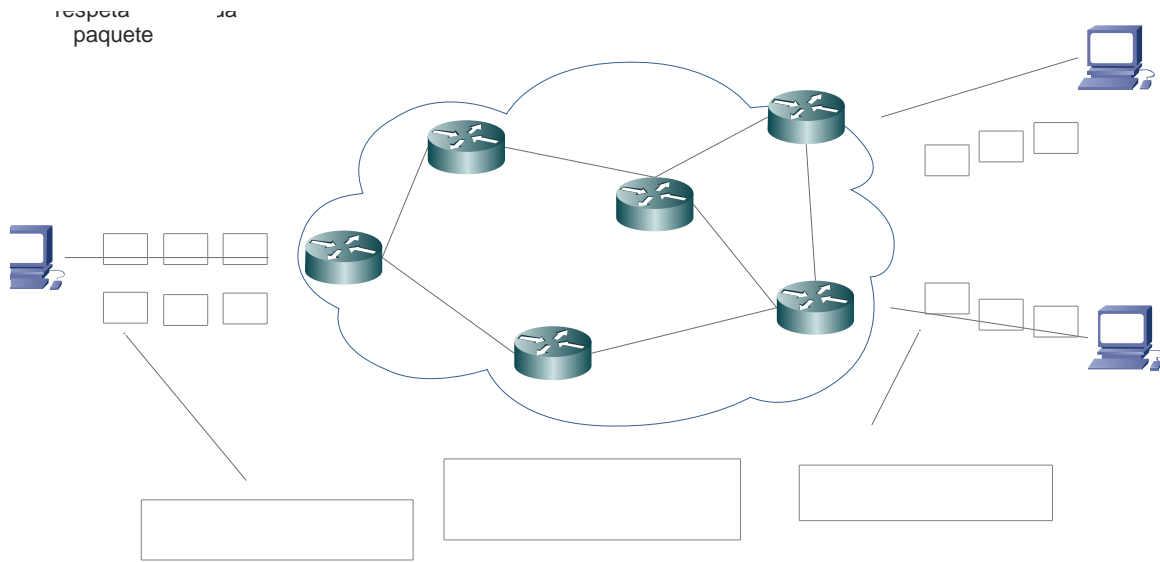


Figura 2 Conmutación de paquetes

## 2.4 Protocolos de Internet

La familia de protocolos de Internet es un conjunto de protocolos de red en la que se basa la red de redes y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los primeros en definirse, y que son los más utilizados.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI el cual consta de diferentes capas (ver Figura 3), donde cada una de estas capas es responsable de una función diferente para la comunicación, cada capa tiene una función bien definida [13]:

1. **Nivel Físico:** Se encarga de las tareas de transmisión física de las señales eléctricas entre los diferentes sistemas [14].
2. **Nivel de Enlace de datos:** Lo que hace la capa es aceptar un flujo de bits puros e intentar entregarlo al destino. No garantiza que este flujo de bits esté libre de errores, es responsabilidad de la capa de enlace de datos detectar y corregir errores. Para ello, añade bits adicionales a los que forman el mensaje para poder detectar errores de transmisión en el mismo y poder pedir su retransmisión. Agrupa los bits en bloques denominados tramas, que contienen los bits de mensajes, los bits añadidos para detectar errores y diferentes campos de control [14].
3. **Nivel de Red:** Se encarga de llevar los paquetes (tomando en cuenta la mejor ruta) desde el origen hasta el destino. La capa de red es la capa en la que residen los protocolos de enrutamiento [14].
4. **Nivel de Transporte:** la función principal de este nivel consiste en proporcionar un flujo de datos entre los sistemas que contienen las aplicaciones de la capa superior. Existen dos protocolos de transporte TCP y UDP. TCP provee un flujo de datos confiable entre dos hosts. Le conciernen cosas como fragmentar los datos que le son pasados desde la

aplicación a un tamaño apropiado para su manejo en la capa de red inferior, reconocimiento de los paquetes recibidos, y establecer tiempo de espera para asegurarse que el otro extremo de la comunicación puede reconocer los paquetes enviados. UDP, por otra parte, proporciona un servicio mucho más simple a la capa de aplicación. Envía paquetes de datos llamados datagramas de un servidor a otro, pero no existe garantía de que el datagrama alcance el otro extremo de la comunicación. Cualquier fiabilidad deseada debe ser añadida por la capa superior [14].

5. **Nivel de Aplicación:** El nivel de aplicación es el nivel que los programas más comunes para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar [13] .

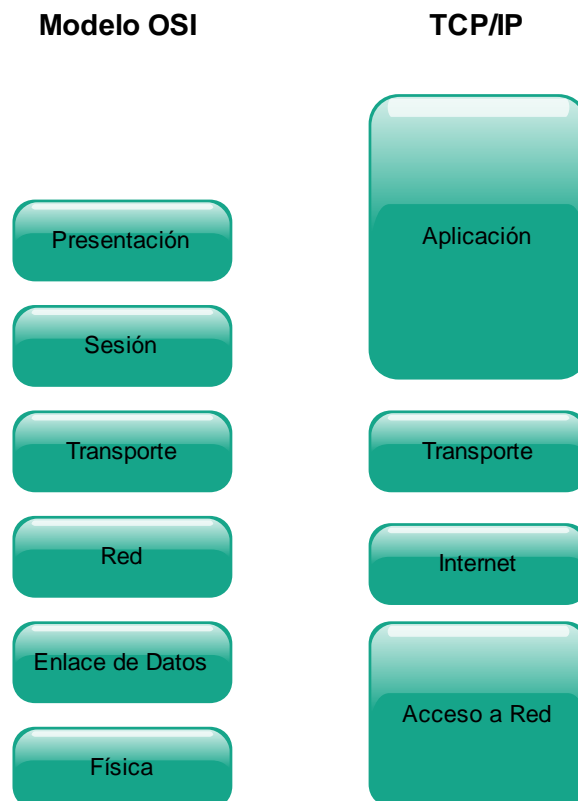


Figura 3 Modelo de referencia TCP/IP



### 2.4.1 IP

El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de conmutación de paquetes, este protocolo se encuentra descrito en el RFC 791.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente).

El Protocolo de Internet provee un servicio de datagramas no fiable, también llamado *best-effort*, es decir, hará lo mejor posible, pero la QoS no está garantizada. IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino, únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. La Figura 4 muestra la estructura del protocolo IP [13].

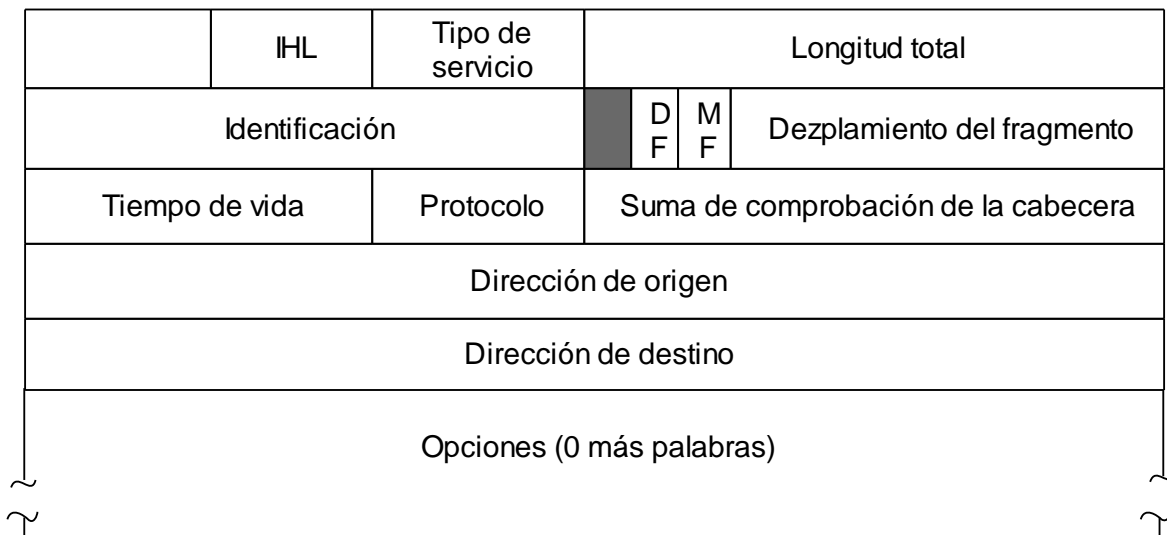


Figura 4 Estructura IP

### 2.4.2 TCP

Es uno de los protocolos fundamentales en Internet de la capa de transporte orientado a la conexión [15]. Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. En la Figura 5 se muestra su estructura.

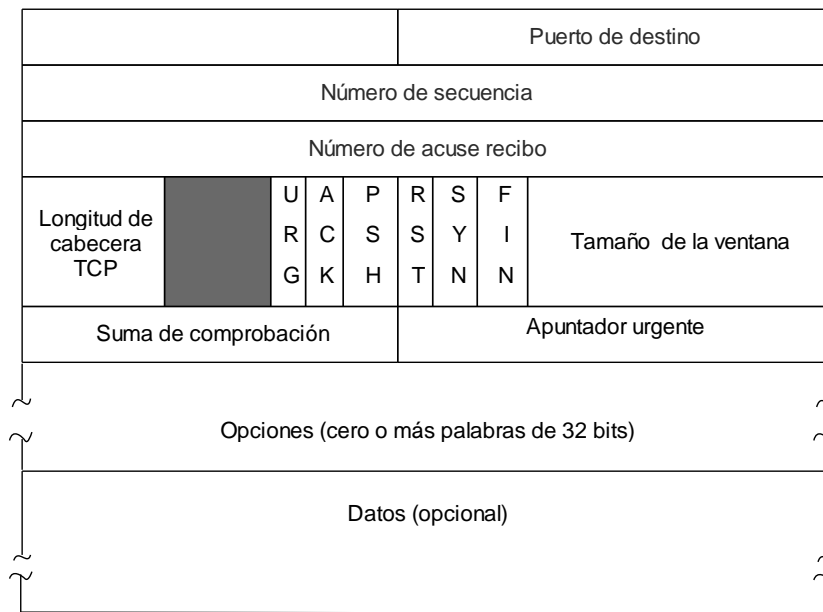


Figura 5 Estructura TCP

### 2.4.3 UDP

UDP (User Datagram Protocol), definido en el RFC 768, es un protocolo de transporte no orientado a la conexión. Este protocolo proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión [16]. Ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros, y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

Al no realizar control de flujo, confirmación y retransmisiones, convierte a UDP en un protocolo muy rápido y eficaz para aplicaciones que no requieren una garantía de entrega y en los cuales es más importante el tiempo de entrega que la pérdida de datos.

UDP transmite segmentos que consiste en un encabezado de 8 bytes seguido por la carga útil [16]. En la Figura 6 se muestra su estructura.

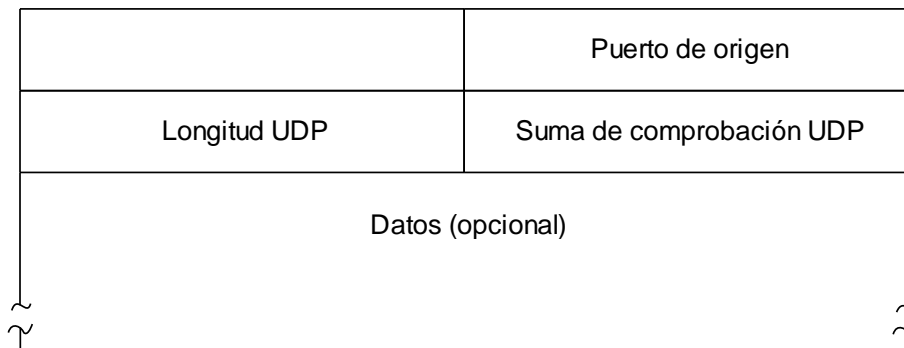


Figura 6 Estructura UDP

#### 2.4.4 RTP

RTP (Real Time Protocol) es el estándar que define las comunicaciones de audio y video en tiempo real sobre redes IP, asumiendo, por tanto, la existencia de pérdidas y retardos y la posibilidad de variación dinámica de las características de la red en el transcurso de la comunicación. Suministra funciones de transporte extremo a extremo y ofrece servicios tales como identificación del tipo de carga, numeración de secuencia, *timestamping*, etc. No garantiza la entrega del tráfico en tiempo real, pero sí suministra los recursos para que éste se entregue de manera sincronizada. Como se indica, está orientado a la transmisión de información en tiempo real, como la voz o el video.

Los paquetes RTP están divididos en dos grandes bloques (ver Figura 7). Por un lado, encontramos la cabecera que contiene la información necesaria para reconstruir el flujo de bits generado por el códec del emisor y, otro, la carga útil, es decir, el propio flujo de bits.

RTP permite al tipo de información transportada, añadir marcas temporales (*time stamp*) y números de secuencia y controlar la llegada de los paquetes. Toda esta información es utilizada por los receptores para reconstruir el flujo de paquetes que generó el receptor eliminando, en la medida de lo posible, los efectos de las pérdidas y retardos (variables y fijos). En este sentido, hay que destacar que RTP no lleva a cabo ninguna reserva de recursos, sino que ofrece al receptor los mecanismos necesarios para recobrar la información en presencia de éstos [10].

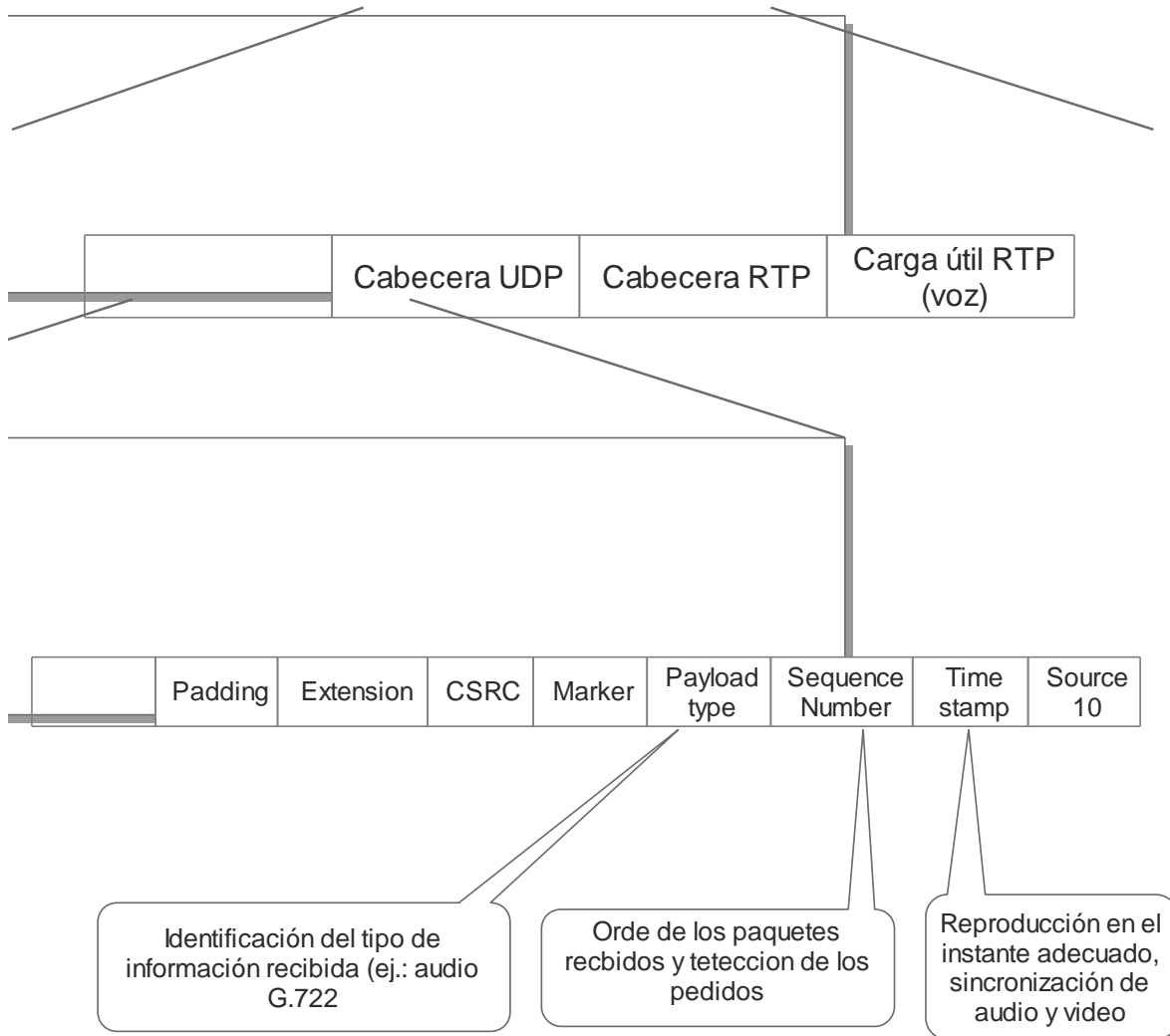


Figura 7 Encapsulamiento de paquetes de voz

### 2.4.5 RTCP

RTP dispone de medios para, en presencia de pérdidas, jitter o retardos, perder continuar con la reproducción del flujo de paquetes. Sin embargo, no especifica ningún medio para estimar los valores de dichos parámetros. De esto, precisamente, se encarga su protocolo de control asociado, RTCP (Real Time Control Protocol), definido en al FFC 1889.

RTCP describe el intercambio de mensajes de control relacionados, fundamentalmente, con la calidad de servicio (retardo, jitter, tasa de pérdidas, etc.), aunque opcional, su utilización es recomendable porque proporciona información de estado de la comunicación con el fin de detectar, por ejemplo, situaciones en las que la calidad de la transmisión no es suficiente, aunque no provee de los mecanismos necesarios para mejorar las presentaciones de la red (reserva de ancho de banda, control de la congestión, etc.).

Además de la información relacionada con la calidad de servicio, RTCP proporciona otras funciones adicionales como la identificación de la fuente, la sincronización entre medios o el control de la sesión [10].

## 2.5 Protocolos de señalización

Los protocolos de señalización en redes de voz sobre paquetes realizan muchas funciones similares a las que llevan a cabo en redes telefónicas (establecimiento de la sesión, señales de progreso de llamadas, gestión de los participantes en la llamada, etc.). Sin embargo, dadas las características particulares de las redes de paquetes deben encargarse, junto con las anteriores, de otras tareas específicas. Por otra parte, las expectativas de calidad del usuario exigen a una red de señalización de altas prestaciones, pues la disponibilidad de la red debe ser similar a la de PSTN (99.999%). Esta es la razón en la que la fiabilidad no sólo deba residir en los elementos de la red sino también en la arquitectura de señalización empleada.

Al igual que ocurría en las redes telefónicas convencionales en las que es posible distinguir entre señalización de usuario y señalización de redes, en redes de voz sobre paquetes tenemos protocolos de señalización entre terminales y protocolos de señalización en la red IP.

En realidad, los protocolos de señalización entre terminales son comunes a cualquier tipo de comunicaciones multimedia (voz, vídeo y audio) a través de las

redes de paquetes. Aplicadas a la voz sobre paquetes, tienen como objetivo mantener la interfaz con el usuario típica de las redes telefónicas, es decir, generar los tonos y señales necesarios para que el usuario no perciba la tecnología de soporte de las llamadas telefónicas ha cambiado [10]. Dos de los protocolos de señalización más importantes en sistemas VoIP son: H.323 y SIP.

### 2.5.1 H.323

La recomendación H. 323 de la Unión Internacional de Telecomunicaciones (ITU en sus siglas en inglés) se ocupa de la transmisión de servicios de comunicación multimedia sobre redes basadas en paquetes, que pueden no proporcionar una calidad de servicio (QoS) garantizada. Esta recomendación es el resultado del trabajo del grupo de estudio número 16 de la ITU-T, el cual se ocupa de las cuestiones relacionadas con la telefonía basada en paquetes y las comunicaciones multimedia [17].

La arquitectura de H.323 define un conjunto de componentes, protocolos, señalización, CODECs, etc., para llevar a cabo la comunicación y garantizar así la compatibilidad entre dispositivos [13].

H.323 soporta los siguientes protocolos [13]:

- H.225 para el direccionamiento (RAS: registro, admisión y estado) y señalización de la llamada (H.225.0).
- H.235 para la seguridad y cifrado.
- H.245 para la señalización de control y la apertura/cierre de canales lógicos.
- H.250 para los servicios suplementarios,
- RTP/RTCP para el transporte de medios en tiempo real.
- T.120 como protocolo de datos para conferencias multimedia.
- CODECs de voz: G.711, G.722, G.723, G.728 y G.729.
- CODECs de vídeo: H.261, H.263, H.264.

2.5.1.1 Componentes H.323

Dado que muchas de las prestaciones de los terminales de H.323 son opcionales, es interesante conocer que bloques integran una terminal H.323. Por ello, a la hora de adquirir un equipo que soporte la normatividad H.323, habrá que valorar qué funcionalidades necesitamos para decidir si el equipo que se ajusta a nuestras necesidades debe incorporarlas o no. La Figura 8 muestra un ejemplo de terminales H.323 [17].

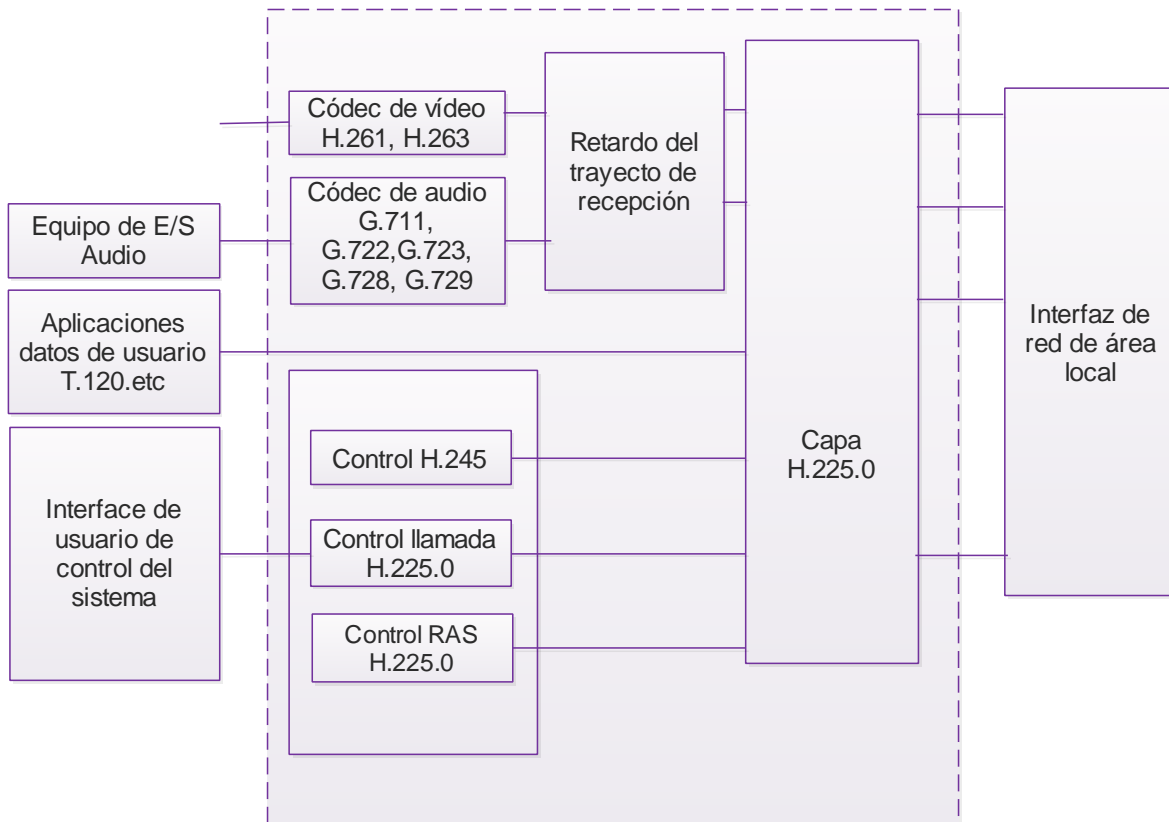


Figura 8 Estructura de Terminal H.323



Una red h.323 está compuesta por cuatro tipos de elementos, tal y como muestra la Figura 9, que son Terminales, Gateways, Gatekeepers y Unidades de control.

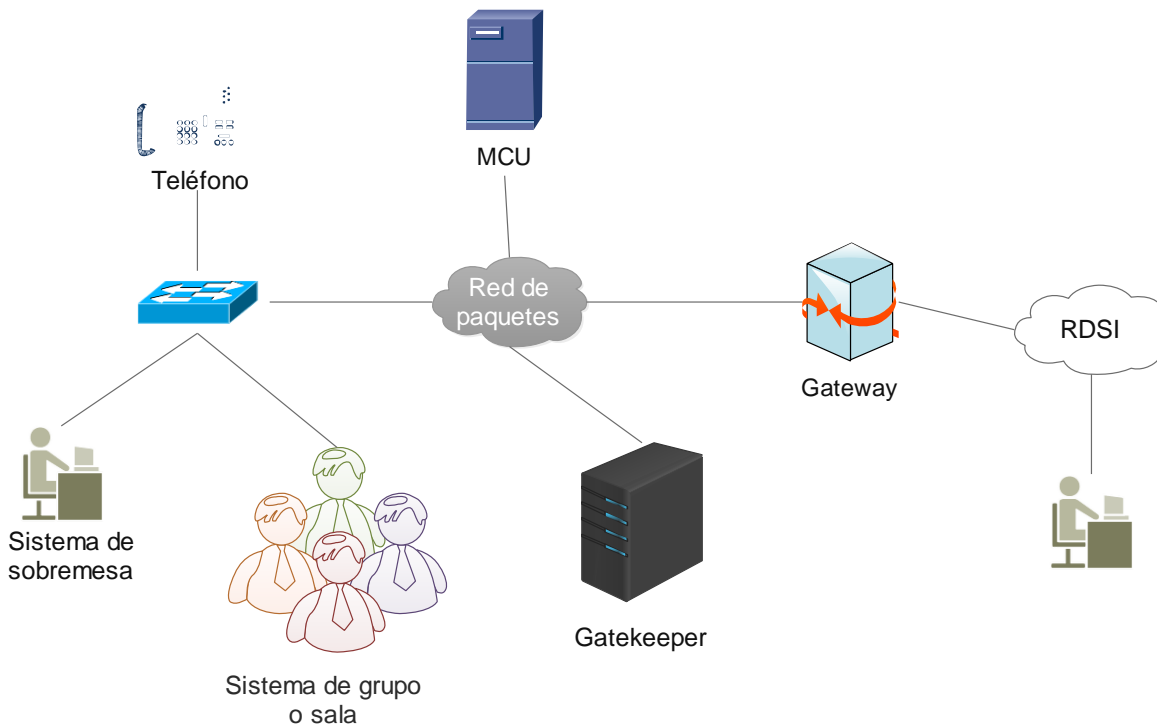


Figura 9 Elementos de una red H.323

- **Terminales.** Son los equipos utilizados por los usuarios finales y abarcan desde teléfonos tradicionales (analógicos, ISDN, GSM, etc.), hasta teléfonos IP pasando por hosts (equipos con tarjeta de sonido, micrófono y altavoces) y sistemas de grupo o sala. Todos los terminales deben soportar H.245, Q.931, RAS y RTP.
- **Gateways.** Los Gateways se encargan de la interconexión entre redes heterogéneas, por ejemplo la interconexión entre la red de circuitos y la red de paquetes. Sus funciones básicas son la traducción de protocolos de establecimiento y liberación de llamadas y la conversión de los formatos de la información entre diferentes tipos de redes. Son elementos opcionales

cuando las comunicaciones multimedia se establecen entre equipos de una misma red local.

- **Gatekeepers.** El Gatekeeper, de los que puede haber más de uno, es el componente más crítico en una red H.323, cuando está presente, puesto que se encarga de las tareas de control de en su zona de influencia. Dentro de su zona, el gatekeeper provee una serie de servicios a entidades registradas, entre lo que se encuentra la gestión de zona, el control de admisión, la gestión del ancho de banda y la traducción de direcciones (IP-números de teléfono).
- **Unidad de Control Multipunto.** Las unidades de control multipunto (MCU, Multiconference Control Unit), se emplea en comunicaciones simultáneas entre más de dos usuarios (multiconferencias). Se encarga de mezclar los flujos de audio y video y distribuir dichos flujos entre los participantes [10].

#### 2.5.1.2 Pila de protocolos

Las comunicaciones en H.323 son una combinación de señales de audio, video, datos y señalización. Las capacidades de audio, señalización de llamada Q.931, señalización RAS y señalización H.245 son obligatorias en todos los terminales.

Las funciones de señalización son el núcleo de un terminal H.323. Estas funciones incluyen señalización para establecimiento de llamada, intercambio de capacidades, señalización de comando e indicaciones y mensajes de apertura y descripción del contenido de los canales lógicos. Estas son las funciones que llevan a cabo los protocolos H.225, RAS y H.245:

- H.225: Es un protocolo de señalización de llamada, se utiliza para establecer llamadas entre entidades H.323, se deriva del protocolo de control de llamada para la ISDN, Q.931/Q.932, aunque se ha modificado para adaptarse a redes de paquetes. El objetivo de H.225 es el establecimiento, control y finalización de una llamada H.323.

Los mensajes más comunes de Q.931/Q.932 son:

- **Setup:** Es enviado para iniciar una llamada y establecer una conexión con una entidad H.323. La información principal que contiene el mensaje es el puerto, dirección IP y alias del llamante o la dirección IP y puerto de llamado.
  - **Call Proceeding:** Enviado por el gatekeeper a un determinado terminal advirtiéndolo del intento de establecer una llamada.
  - **Alerting:** Indica el inicio de la fase de generación de tono.
  - **Connect:** indica el comienzo de la conexión.
  - **Reléase Complete:** Enviado por el terminal para iniciar la desconexión.
  - **Facility:** Mensaje de la forma Q.932 usando como petición o reconocimiento.
- H.245: Es el protocolo de control de medios, se encarga de la negociación de las capacidades de la sesión y creación del canal lógico, así como también de la liberación de conexión. H.245 es una señalización que debe realizarse en paralelo con H.225 y, de preferencia antes del mensaje Connect (si no, podría perderse algunos de los datos transmitidos). H.245 controla sesión encargándose de:
    - El intercambio de capacidades de los terminales.
    - La determinación del maestro y el esclavo de la comunicación.
    - El control y composición de la señalización del canal lógico.

Estos protocolos son ejecutados en orden estricto. Primero, el registro de los terminales ocurre a través de RAS, posteriormente el establecimiento de la llamada ocurre a través de H.225 (Q.931) sobre TCP, después, los mensajes son intercambiados entre la entidad que llama y la entidad llamada por medio de H.245, que también es transportado por TCP. Finalmente, los flujos RTP son enviados por UDP. Posteriormente para terminar la comunicación, se emplea H.245 para la liberación de la conexión, y RAS para la liberación de terminales [14].

La Figura 10 muestra un diagrama de llamada H.323 completo, contemplando todos los protocolos involucrados en ella.

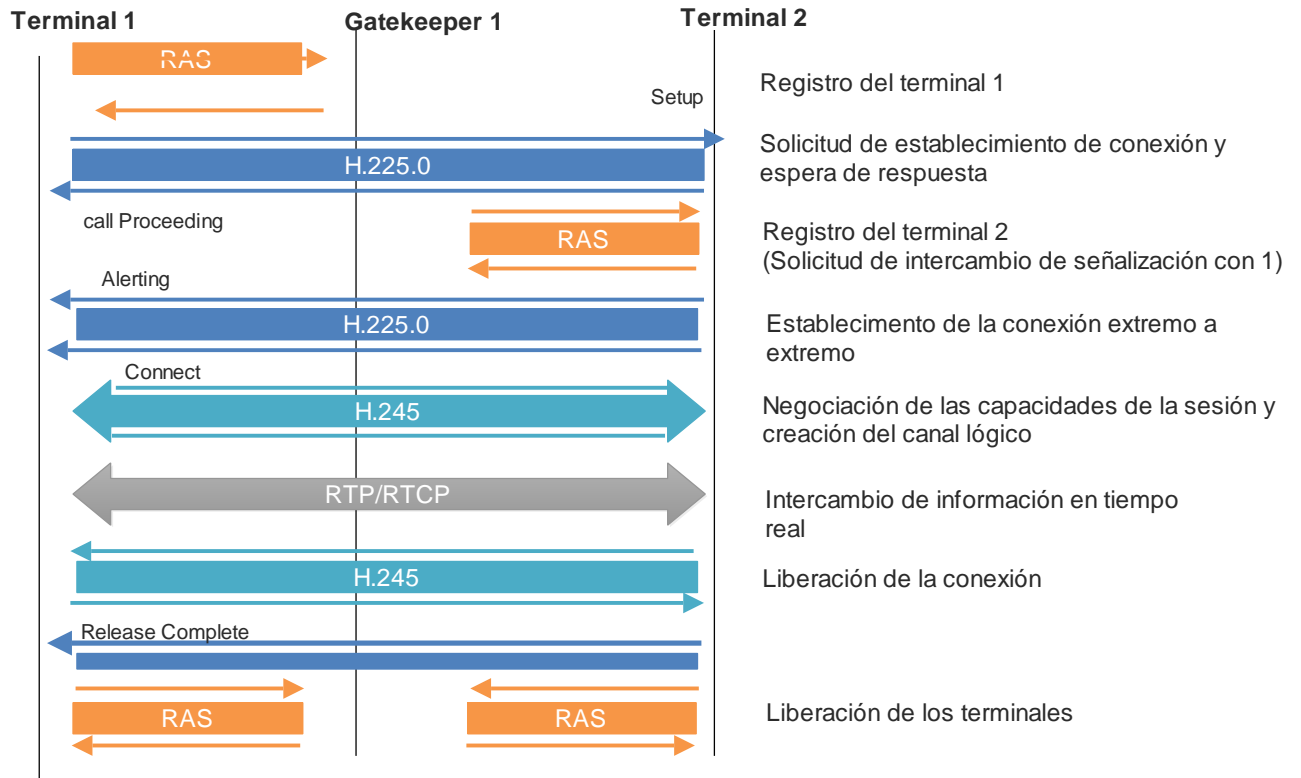


Figura 10 Señalización H.323

### 2.5.1.3 CODECs

En VoIP además de codificar la voz se busca tener más eficiencia incluso al momento del muestreo, por lo tanto, cuando se quiere reducir el ancho de banda de una señal de voz, se utilizan esquemas de codificación y muestreo avanzados que permiten mantener cierto nivel de calidad y disminuir los requisitos de ancho de banda.

De esta tarea se encargan los Codificadores-Decodificadores (CODECs) los cuales constituyen una serie de especificaciones basadas en hardware y/o software para la codificación y decodificación de señales digitales. Es decir, un CODEC realiza la tarea de codificar una señal o flujo de datos y posteriormente decodificarla y recuperar así la señal original.

Los CODECs se utilizan para tener una compresión de los datos y para proporcionar otras capacidades adicionales, pueden permitir ahorrar ancho de banda, esto es sumamente necesario especialmente en conexiones de baja capacidad donde se necesita tener buena calidad de llamadas y el establecimiento de múltiples llamadas VoIP simultáneamente [5].

La Tabla 1 muestra algunos de los estándares de codificación más importantes cubiertos por la ITU y, como se puede ver, la calidad es menor cuanto mayor es la compresión, además que se requiere mayor consumo de CPU (MIPS).

Algunos esquemas de compresión, tales como el G.729 y el G.723.1, consiguen una baja tasa de bits, reduciendo considerablemente la necesidad de ancho de banda, por lo que resultan apropiados para Internet. Por ejemplo, el G.723.1, aparecido en noviembre de 1988, incluye un esquema de compresión basada en la supresión de silencios y VAD (*Voice Activity Detection*) [10].

Tabla 1 Algunos CODECs más comunes para telefonía

CODEC	Ancho de banda kHz)	Frecuencia de Muestreo kHz	Duración muestras/tramas (ms)	MOS	Aplicación
G.711 (PCM)	64	8	0.125	4.4	Telefonía
G.721 (ADPCM)	32	8	0.125	4.2	Telefonía
G.722 (SB-ADPCM)	48/56/64	16	0.250		Videoconferencia
G.728 (LD-CELP)	16	8	0.625	4.2	Telefonía/ Videoconferencia
G.729 (CS-ACELP)	8	8	10	4.1	Telefonía
G.723.1 (MP-MLQ)	6.3	8	30	3.9	Telefonía Internet
G.723.1 (ACELP)	5.3		30	3.6	Telefonía Internet

### 2.6.2 SIP

El protocolo SIP (Session Initialization Protocol) es un protocolo de señalización (application-layer control) creado para administrar sesiones multimedia entre dos o más partes. Muchos confunden pensando que el protocolo SIP es quien transporta la voz propiamente dicha, pero no es así, esta labor la hace otro protocolo, de lo que sí se encarga SIP es de la señalización necesaria para establecer una llamada, modificarla, así como para finalizarla.

El protocolo SIP fue diseñado con la premisa de la simplicidad en mente, se trata de un protocolo de texto con mensajes de comunicación sencillos. Inclusive SIP comparte algunos códigos de estatus con HTTP como el familiar *404: Not found* [11].

SIP es independiente del tipo de sesión multimedia manipulado y del mecanismo utilizado para describir la sesión. Es igualmente útil para videoconferencias, llamadas de audio, pizarras compartidas, y sesiones de juego. Las sesiones consisten en llevar flujos RTP de audio y vídeo por lo general se describen utilizando SDP, pero algunos tipos de sesión pueden ser descritas con otros protocolos de descripción.

En resumen, el SIP se utiliza para distribuir descripciones de la sesión entre los participantes potenciales. Una vez que la descripción de la sesión se distribuye, SIP puede utilizarse para negociar y modificar los parámetros de la sesión y terminar la sesión [18].

#### 2.6.2.1 Arquitectura SIP

SIP define cuatro componentes lógicos. Estos componentes se pueden implementar en dispositivos físicos, tal como teléfonos IP, o bien como aplicaciones software; en cualquier caso, un mismo dispositivo físico puede incluir uno o más componentes lógicos. Todos los elementos SIP deben implementar obligatoriamente TCP y UDP. En ambos protocolos escucha en el puerto 5060 [13].

- **Servidor Proxy.** Se encarga de encaminar peticiones/respuestas hacia el destino final. El encaminamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final.
- **Servidor de Redirección.** Realiza una función equivalente al servidor proxy, pero a diferencia de éste no progresa la llamada, sino que contesta a un INVITE con un mensaje de redirección, indicándole en el mismo como contactar con el destino.
- **Servidor de Registro.** Mantienen la localización actual de un usuario. Se utiliza para que los terminales registren la localización en la que se

encuentran. Este servidor facilita la movilidad de usuarios, al actualizar dinámicamente la misma.

- **Agente de llamada (Call Agent).** Realiza las funciones de los tres servidores anteriores, además de poder realizar las siguientes acciones:
  - Localizar a un usuario mediante la redirección de la llamada a una o varias localizaciones.
  - Implementar servicios de redirección como reenvío si ocupado, reenvío si no contesta, etc.
  - Implementar filtrado de llamada en función del origen o del instante de la llamada.
  - Almacenar información de administración de llamadas.
  - Realizar cualquier otra función de gestión [19].

#### 2.6.2.2 Peticiones y respuestas SIP

##### Peticiones SIP

- INVITE – Mensaje inicial de invitación enviado por el extremo llamante.
- ACK – Respuesta del agente llamante ante el mensaje de aceptación de la llamada por parte del destino.
- BYE – Señal de terminación de la sesión por parte de uno de sus participantes.
- CANCEL – Cancela una petición pendiente.
- REGISTER – Empleado por los usuarios para registrar su dirección de contacto actual.
- OPTIONS – Consulta a un agente de usuario acerca de sus capacidades (ej. CODEC)
- INFO – Contiene información fuera de banda, como dígitos DTMF.

##### Respuestas SIP

- 1xx – Mensajes de información.
- 2xx – Éxito.



- 3xx – Mensaje de desvío.
- 4xx – Error de la petición.
- 5xx – Error en el servidor.
- 6xx – Error general.

Los seis pasos básicos implicados en el manejo de sesiones SIP son los siguientes (ver Figura 11):

- Registro, iniciación y localización del usuario.
- Descripción de la sesión multimedia que se presente establecer.
- Aceptación de la petición de conexión del otro extremo.
- Establecimiento de la llamada.
- Comunicación.
- Terminación de la llamada.

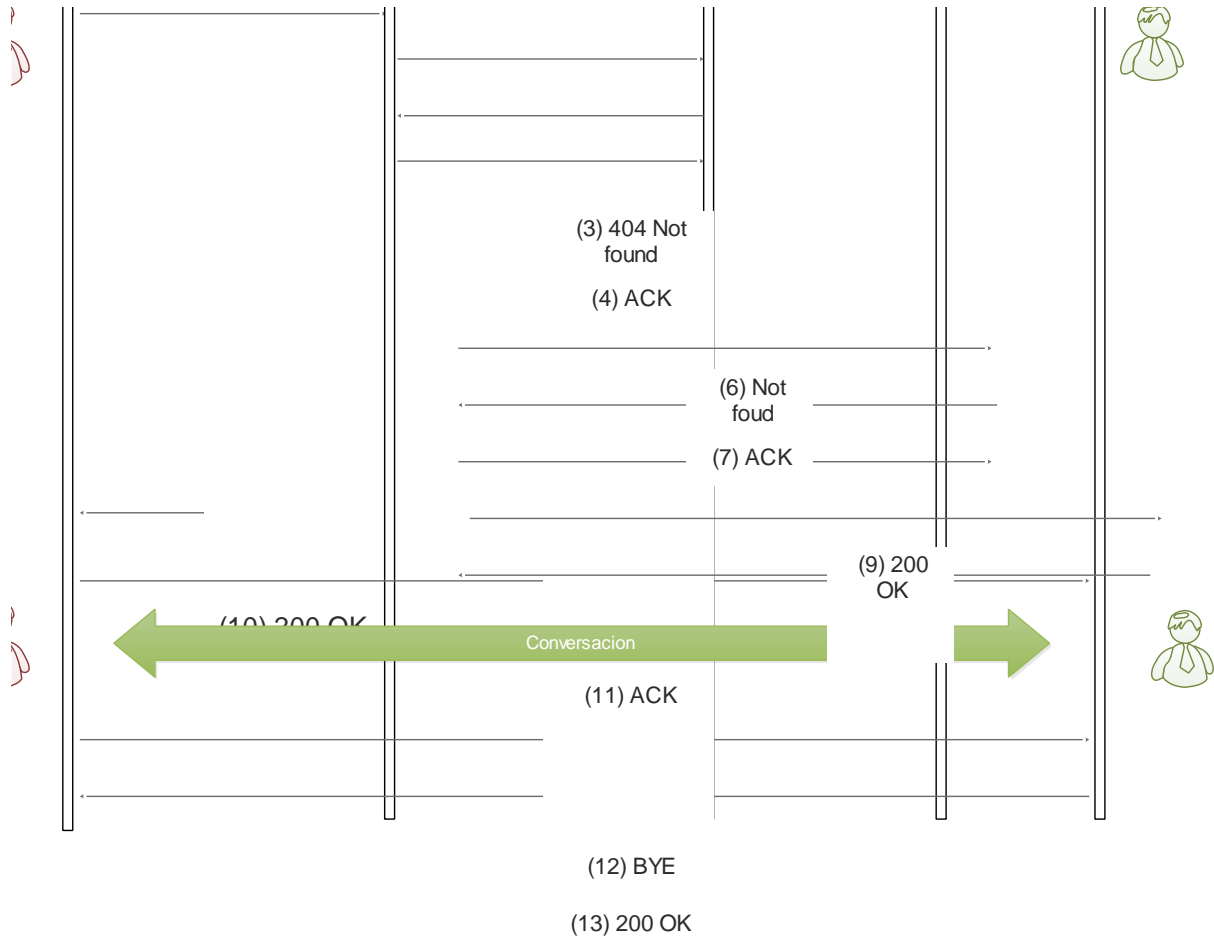


Figura 11 Ejemplo de llamada SIP

# CAPÍTULO 3

## CAPÍTULO 3. QoS

En los últimos años, la importancia de la calidad de servicio (QoS) para las tecnologías de redes de paquetes ha aumentado rápidamente. Hoy en día la QoS es sin duda una de las piezas principales de las tecnologías de red de paquetes, sobre todo en aplicaciones en tiempo real, como la VoIP.

### 3.1 Concepto de calidad de la voz

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. La calidad de la voz desde el punto de vista del usuario, es decir, en función del grado de satisfacción del usuario final; la calidad de servicio desde el punto de vista de la red, dicho de otra manera, en función de los mecanismos que proporcionan las redes de telecomunicaciones para garantizar a un flujo de voz, cierto nivel de QoS, en función del ancho de banda, retardo, jitter y pérdidas.

Las consideraciones generales sobre la evaluación de la calidad del servicio telefónico se encuentran en la recomendación E.420 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. Algunas son tan curiosos como la posibilidad de comunicarse con usuarios que se encuentren en otros países o que la facturación esté libre de errores. Otros aspectos importantes son:

- **Tasa de conectividad:** Hace referencia a la probabilidad con la que la red dispondrá de recursos para cursar un intento de llamada.
- **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. Es este sentido, juega un papel fundamental la claridad de la voz.

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 cuánta 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 sí ejerce gran influencia) y del eco (puesto que éste es escuchado por el emisor y la claridad se evalúa en el receptor).

- **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.

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 12. Como puede verse, cuanto mayor es la tasa binaria, tanto más probable es de obtener una buena calidad de la codificación (no sólo inteligibilidad). Por otra parte, el incremento de la tasa de error mayor cuanto menor es la tasa binaria debido a la disminución en la información de redundancia por la compresión [10].

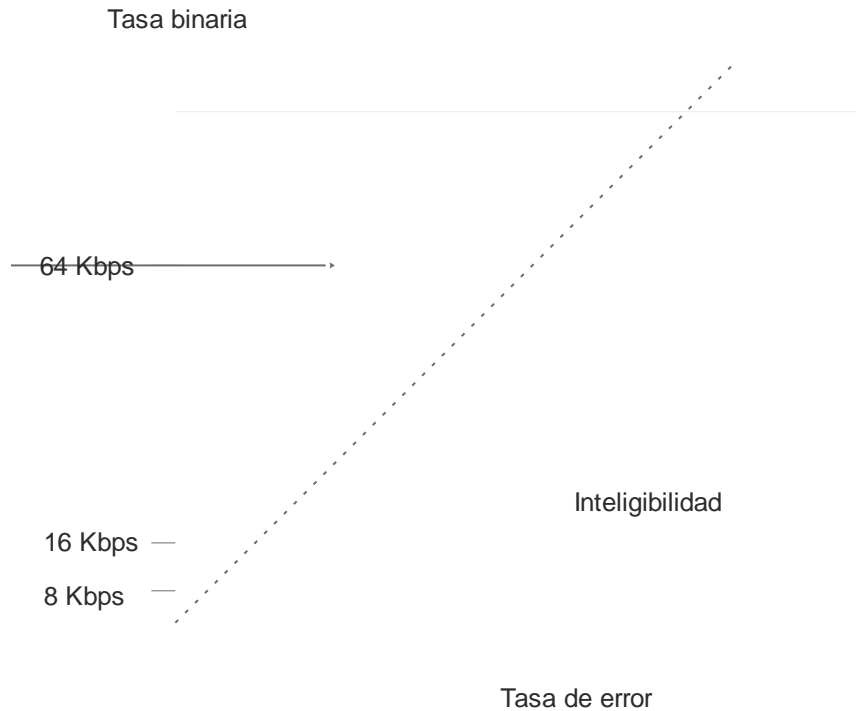


Figura 12 Relación entre la inteligibilidad de la codificación de la voz

## 3.2 Factores que influyen en la calidad

### 3.2.1 Disponibilidad

La disponibilidad de un sistema es una medida de la probabilidad con que se encontrará en condiciones de funcionamiento, de manera que cuanto mayor es la disponibilidad mayor es dicha probabilidad.

Las redes telefónicas convencionales como la PSTN o la ISDN presentan valores de disponibilidad muy elevados, en torno al 99.999% (los llamados 5 niveles), es decir 5.25 minutos fuera de servicio al año. Sin embargo, las redes de datos no alcanzan, ni de lejos estos niveles de disponibilidad. Al contrario, sufren de las pérdidas de servicio periódicas causadas, por ejemplo, por errores de usuarios o del software.

A la hora de diseñar cualquier sistema debemos analizar, en primer lugar, el tiempo que el sistema puede dejar de estar operativo debido a fallos inesperados en el hardware y el costo 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 usuarios.

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 PSTN o ISDN. Es lo que se conoce como encaminamiento de *backup*.

Además, es recomendable utilizar sistemas de alimentación ininterrumpida (UPS) 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 convertidor que transforma la corriente continua en alterna a 200 V/50 Hz para alimentar al equipo durante un cierto tiempo (por ejemplo 30 minutos) que dé lugar a 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 una gran autonomía. En ambos casos, entran en funcionamiento ante los cortes de energía y también realizan un filtrado/establecido de la corriente, para eliminar los picos de tensión y los microcortes [10].

### 3.2.2 Jitter

En general, a la hora de analizar las prestaciones de una red se habla de retardos en valores medios. Sin embargo, el tráfico de voz es muy sensible a las variaciones del retardo y, por ello, trabajar con valores medios no resulta suficiente. En redes IP, y en general en cualquier red de paquetes, no se puede garantizar que todos los paquetes de una misma comunicación sigan el mismo camino, al contrario de lo que ocurre en las redes de conmutación de circuitos.

Como consecuencia, cada paquete llegará al destino atravesando un número distinto de nodos de la red y, por lo tanto, alcanzaran su objetivo con un retardo diferente. Esta variación del retardo recibe el nombre de jitter.

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

Para absorber estas variaciones se utilizan los llamados *buffers* de supresión de jitter. La supresión consiste en el almacenamiento de los paquetes durante el tiempo suficiente para que los paquetes que hayan llegado fuera de secuencia o tiempo puedan reordenarse y reproducirse en el orden correcto. Por tanto, cuanto mayor es el jitter de los paquetes, tanto mayor es el tamaño del *buffer* de supresión de jitter necesario para reducir su impacto en la calidad.

La supresión de jitter introduce un retardo adicional que puede afectar a la calidad de la voz resultante. Por ello, es necesario encontrar una solución de compromiso entre el tamaño del *buffer*, el retardo y las pérdidas. La situación ideal es aquella en la que el tamaño del *buffer* varía dinámicamente con las condiciones de la red durante su funcionamiento [10].

### 3.2.3 Pérdidas

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 en las redes de conmutación de paquetes no se produce una reserva de recursos previa al envío de la 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. Por otro lado, esta disminución de la calidad es tanto mayor cuanto mayor sea la tasa de compresión del códec [10].



### 3.2.4 Retardo

El retardo es el tiempo invertido por la señal de voz en su viaje desde el origen al destino. Una de las características más importantes de la voz es su temporalidad, no sólo porque el intervalo de pronunciación de dos sílabas determina su pertenencia a una misma palabra, sino porque la conversación entre dos interlocutores sigue un esquema temporal de escucha-respuesta cuya alteración puede convertir la conversación en inteligente (piénsese en dos interlocutores hablando a la vez).

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 50ms y, en estas circunstancias, el eco es enmascarado por la voz de los interlocutores.

Al estudiar la influencia del retardo en las comunicaciones de voz sobre paquetes son dos los aspectos que a determinar; el retardo máximo aceptable y las fuentes de retardo.

El retardo máximo aceptable marca un umbral por encima del cual la calidad de la voz resultante es inaceptable y la conversación resulta imposible, la recomendación G.144 de la ITU-T establece estos umbrales, ver Tabla 2. Sin embargo, la influencia del retardo depende tanto de factores objetivos como de factores subjetivos, por ello, en algunas ocasiones como es el caso de las comunicaciones vía satélite en que los usuarios se encuentran predispuestos a tolerar una menor calidad, podría llegar a soportarse retardo de unos 400ms.

Tabla 2 Relación entre el retardo en un solo sentido y la calidad de la voz

Rangos(ms)	Descripción
0 – 150ms	<b>Excelente.</b> Muy válido para las aplicaciones más comunes.
150 - 400ms	<b>Buena-pobre.</b> Aceptable, teniendo en cuenta que un administrador de red conozca las necesidades del usuario.
<b>Sobre 400ms</b>	<b>Inaceptable</b> para la mayoría de aplicaciones de red; sin embargo, este límite puede ser excedido en algunos casos aislados.

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 13.

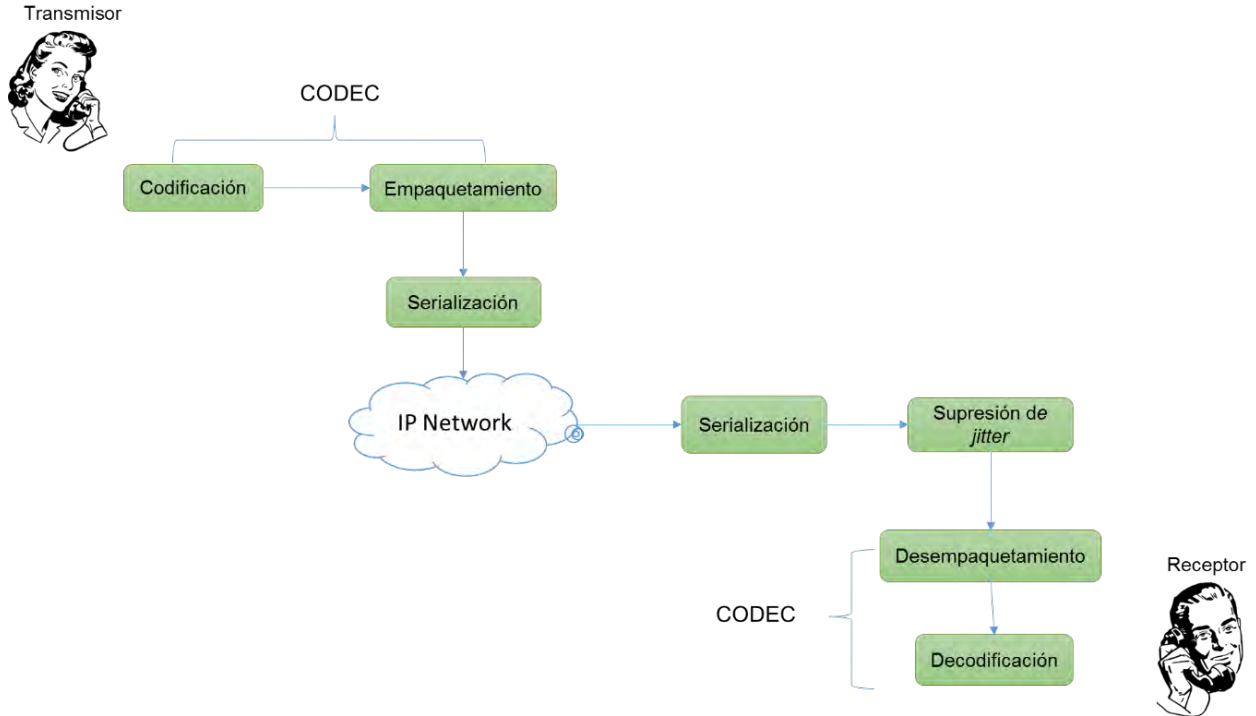


Figura 13 Procesamiento de la señal de voz entre los extremos

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 CODECs 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 3 Recoge los parámetros de algunos de los CODECs más empleados en VoIP, aunque algunos puedes variar ligeramente, dependiendo del fabricante.

Tabla 3 Características de algunos CODECs

	<b>G.711</b>	<b>G.729</b>	<b>G.723.1</b>
<b>Tasa binaria (kbps)</b>	64	8	6.3/5.3
<b>Complejidad (MIPS)</b>	0.1	22	16/18
<b>Retardo codificador (ms)</b>	0.125	15	37.5
<b>Tiempo entre paquetes (ms)</b>	20	20	30
<b>Retardo de empaquetamiento (ms)</b>	1.5	15	37.5
<b>Tamaño del <i>buffer</i> de supresión de jitter (ms)</b>	40	40	60
<b>Calidad (MOS)</b>	4.4	4.1	3.5-3.9

Una vez que los paquetes llegan al gateway, ésta 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 del tamaño de la trama. El retardo de serialización debe contabilizarse cada vez que un paquete atraviese un dispositivo store and forward como *router* o un *switch*.

Los paquetes serializados viajarán 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. 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 de 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 pertenece dichos paquetes, el retardo de encolamiento varía mucho de un paquete a otro. En cualquier caso, generalmente, el retardo se encuentra comprendido entre 70 ms y 100 ms y es, por tanto, una de las contribuciones más importantes al retardo total [10].

### 3.2.5 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 del otro interlocutor o en ausencia de ella.

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 electrónico, consecuencia de una desadaptación de impedancias en el extremo receptor.

En redes telefónicas convencionales se emplean dos pares de hilos (uno para transmisión y uno para para 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 denominado bobina híbrida.

En la conversión 2H/4H se produce una desadaptación de impedancias que refleja parte de la señal incidente y que viajará 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 en un solo sentido es menor de 50ms, el eco queda enmascarado por la conversión normal [10].

### 3.2.6 Ancho de banda

El ancho de banda (BW, BandWidth) 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, el ancho de banda medio de la red debe ser tal que:

$$BW = \frac{BW_{VOZ} + BW_{VIDEO} + BW_{DATOS}}{0.75}$$

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, sobredimensionado 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.

Una comunicación de voz sin comprimir, por cada sentido de la comunicación, consume 64kbps, sin embargo, puesto que el ancho de banda es un recurso escaso, sería deseable poder comprimir la voz y aumentar la eficiencia de utilización del ancho de banda causando 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 pérdidas y al retardo [10].

### 3.2.6.1 Supresión de silencios

Es un mecanismo complementario al empleo de CODECs compresores para reducir el ancho de banda. Se trata de aprovechar el hecho de que en una conversación normal aproximadamente el 60% del tiempo lo ocupan los silencios debido 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, supresión de silencios o VAD (*Voice Activity Detection*).

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 14. En este caso, existen seis puntos en los que podría activarse la VAD.

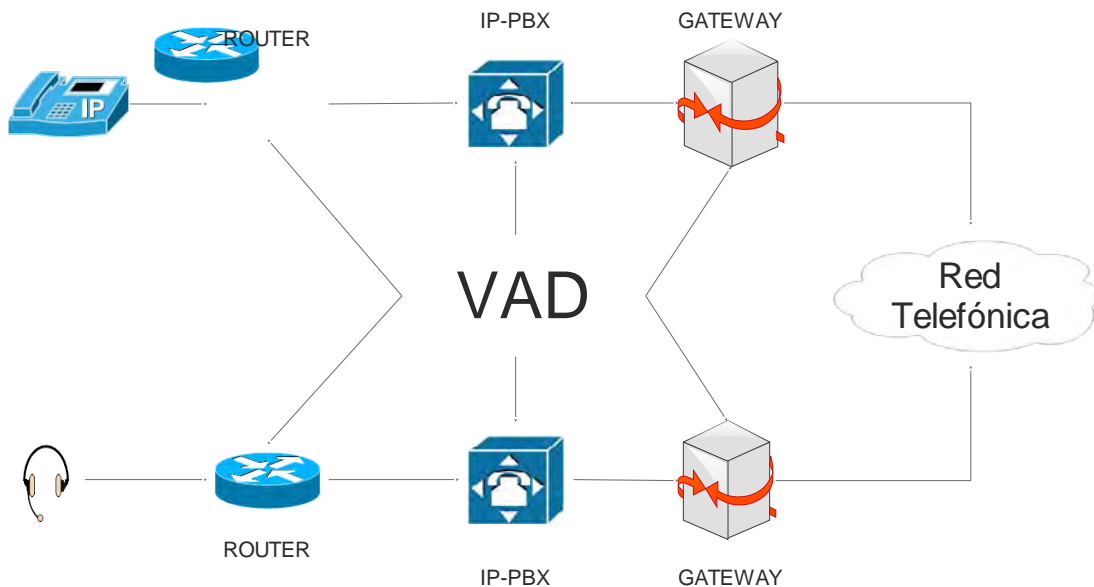


Figura 14 Puntos en los que se puede activar la VAD

Para evitar que el interlocutor piense que se ha cortado la comunicación durante los intervalos de silencio se envían periódicamente paquete 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 (recomendación ITU-T I.366.2).

Sin embargo, pese a que la supresión de silencios aporta beneficios en cuanto al ancho de banda empleado, también suele ser la responsable que un fenómeno conocido como *clipping* y que consiste en que la voz del interlocutor parece “recortada”. También las pérdidas, la latencia y el jitter pueden producir este fenómeno [10].

### 3.3 Medición de la calidad de la voz

Una de las características más importantes de los distintos sistemas de codificación y decodificación de la voz es la calidad de sonido inteligible conseguido en distinto. La finalidad de la tecnología de voz sobre IP es conseguir una comunicación mediante el empleo del habla, por tanto, más que la fidelidad del sonido importa la inteligibilidad del mismo. Esto es lo que se conoce como calidad de la voz. En general, cuando se mide la calidad de la voz en comunicaciones telefónicas, no se habla de fidelidad del sonido, sino de tres parámetros básicos:

- Calidad de audición: Cómo se escucha, si se entiende bien.
- Calidad de conversación: Cómo interactúa.
- Calidad de transmisión: Calidad de red.

En cualquier caso, el objetivo de las mediciones es poder medir las mejoras de un sistema concreto o realizar comparaciones entre sistemas distintos. Para ello, suele ser suficiente con medir uno o dos de los parámetros anteriores.

Aunque parece una tarea complicada, el hecho es que existen diversos métodos normalizados para realizar mediciones de la calidad de la voz. Los más conocidos son: MOS, Modelo E, PSQM y PAMS [20].

### 3.4 Método subjetivo: MOS

MOS (Mean Opinion Score, “Valoración media de opinión”) fue uno de los primeros métodos de medición de la calidad de voz. Se trata de un sistema de valoración subjetiva que consiste en evaluar la calidad de distintas muestras y ponderar los resultados para obtener una puntuación media. El sistema MOS dispone de una escala de cinco puntos con el siguiente significado:

1. **Mala.** Distorsión muy molesta
2. **Pobre.** Distorsión molesta
3. **Regula.** Distorsión perceptible y ligeramente molesta
4. **Buena.** Nivel de distorsión perceptible pero no molesta
5. **Excelente.** Sin distorsión

El método del MOS se encuentra descrito en la recomendación P.800 de la ITU-T. Para asegurar en lo posible la objetividad de la medición, esta recomendación incluye una serie de indicaciones relativas a la sección de participantes, el entorno donde se deben realizar las pruebas, explicación de la valoración, análisis de resultado, etc. Idealmente, si se realizasen dos evaluaciones distintas a un mismo sistema debieran obtenerse puntuaciones similares.

Desde el punto de vista práctico, una puntuación MOS de 4 o superior supone una alta calidad de voz [20].



### 3.5 Modelo E

El modelo E es una aproximación matemática de la medida de la calidad de la voz basada en la evaluación de las características de transmisión de voz sobre la red de paquetes y cuyo objetivo es predecir la calidad de la voz en función del retardo, las pérdidas y tipo de CODEC utilizado [10].

El modelo E toma las degradaciones debidas a eco para el hablante y el retardo de transmisión en consideración y por lo tanto se pueden aplicar a la predicción de la calidad en una situación conversacional. Fue compilado con una combinación de diferentes modelos de predicción de la calidad en el marco del ETSI (European Telecommunications Standards). El modelo E es ampliamente utilizado para estimar la calidad durante la planificación de redes, y también durante su operación. Este modelo ha sido objeto de una amplia validación, y se ha encontrado para proporcionar estimaciones de calidad realistas para el individuo y también dentro de los límites de las degradaciones combinados [2].

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:

$$R = R_0 - I_s - I_d - I_e + A$$

El término  $R_0$  hace referencia a la relación señal-a-ruido mientras que  $I_s$  modela la degradación que sufre la señal como consecuencia de su conversión a un formato adecuado para su transmisión por la red. Los otros tres términos son el efecto de las pérdidas ( $I_e$ ) del retardo ( $I_d$ ) y el margen de seguridad ( $A$ ), que ahora 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:

$$I_d = 0.024 \cdot d + 0.11 - (d - 177.3) \cdot H(d - 177.3)$$

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, 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 200ms.

Otro de los factores que influyen en la calidad de la voz son las pérdidas cuyo impacto se modela a través de parámetro  $I_e$ , tanto mayor es la disminución de la calidad.

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 la Tabla 4.

Tabla 4 Evaluación de la calidad de la voz a partir del modelo E

Modelo E (Factor R)	Satisfacción del usuario	Escala MOS
$94 \leq R < 100$	Muy satisfecho	4.3 - 4.4
$80 \leq R < 90$	Satisfecho	4.0 - 4.3
$70 \leq R < 80$	Algunos insatisfechos	3.6 - 4.0
$60 \leq R < 70$	Muchos insatisfechos	3.1 - 3.6
$50 \leq R < 60$	Casi todos insatisfechos	2.6 - 3.1
$0 \leq R < 50$	No Recomendado	1.0 - 2.6

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

$$MOS = \begin{cases} 1 & R < 0 \\ 1 + 0.035 \cdot R + 7 \cdot R(R - 60) \cdot (100 - R) \cdot 10^{-6} & 0 < R < 100 \\ 4.5 & R > 100 \end{cases}$$

# CAPÍTULO 4

## CAPÍTULO 4. PÉRDIDAS DE PAQUETES

En una red IP, es posible que algunos paquetes puedan llegar fuera de orden o no llegar nunca. La pérdida de paquetes es causada por la congestión, la inestabilidad de enrutamiento, enlaces perdidos, como los enlaces inalámbricos o fallo del enlace. La pérdida por congestión es la causa más común. Los paquetes IP de muchas fuentes se ponen en cola para su transmisión en router. Cuando la cola se llena, los paquetes entrantes se pierden.

Además, debido a sensibilidad de la transmisión de voz, UDP representa la capa de transporte adecuada, ya que no proporciona ninguna facilidad para la retransmisión de paquetes perdidos minimizando los retardos de transmisión. Sin embargo, al mismo tiempo permite que se produzcan pérdidas de paquetes durante la congestión de la red.

Este comportamiento puede causar la pérdida de información útil de voz. Cada paquete puede contener 10-50ms de información de voz. Cuando se produce demasiadas perdidas de paquetes, el receptor no podría ser capaz de realizar la tarea de reconocimiento [21].

Por otro lado, diversos estudios han demostrado que la pérdida de paquetes presenta naturaleza rafagoza, es decir, si un paquete se pierde, existe una alta probabilidad que el siguiente paquete también se pierda. A este fenómeno se le conoce como pérdida de paquetes a ráfagas. Un modelo que permite capturar este fenómeno es mediante cadenas de Markov de estados infinitos. Una cadena de Markov de dos estados puede ser utilizada para representar una ráfaga de paquetes perdidos (bursts) o una ráfaga de paquetes que llegaron correctamente a su destino (gaps). Para lograr un comportamiento similar al que ocurre en Internet, es necesario usar una cadena de Markov de 4 estados. Así podremos tener varias transiciones entre burst y gaps.

## 4.1 Distribución de pérdida de paquetes: Gaps y Bursts

Con la finalidad de evaluar adecuadamente la calidad de una llamada de voz sobre IP, es conveniente tener en cuenta el grado de rafagosidad (burstiness) de la pérdida de paquetes.

Debido a lo dinámico del Internet, es decir, el comportamiento es variable en el tiempo de paquetes de red, la pérdida de paquetes puede mostrar una variedad de distribuciones. Una de las distribuciones más utilizadas para representar la pérdida de paquetes es mediante el modelo de Bernoulli o Gilbert-Elliott, en el cual, un periodo de tiempo, delimitado por paquetes perdidos y/o desechados con una tasa alta, es conocido como un “burst”, y un periodo entre dos *bursts* es un llamado “gap”, en el cual, los paquetes son recibidos correctamente.

Los “bursts” corresponden a los periodos de tiempo durante el cual la tasa de pérdida de paquetes es lo suficientemente alta para producir la degradación notable de la calidad de audio.

Los “gaps” corresponden a los periodos de tiempo durante el cual pueden ocurrir sólo paquetes perdidos aislados, y en general, estos pueden ser enmascarados por alguna técnica de ocultamiento de pérdida de paquetes [22].

Un burst se define, en términos de un valor denominado “Gmin”, como la secuela más larga que: (a) comienza con un paquete perdido o descartado, (b) no contiene ocurrencias de Gmin o más paquetes perdidos consecutivos (y no descartados), y (c) termina con un paquete perdido o descartado.

Formalmente, un gap se define como cualquiera de los siguientes: (a) el periodo desde el inicio de una sesión de RTP al tiempo de la recepción del último paquete recibido antes del primer burst, (b) el periodo desde el final del ultimo burst, ya sea a la hora del informe o al final de la sesión RTP, lo que ocurra primero, o (c) el periodo de tiempo entre dos bursts [22].

Como se mencionó anteriormente, la distribución de pérdida más estudiada en pruebas de la calidad de voz es la de Bernoulli, definida por  $P_{pl}$  o probabilidad global de pérdida de paquetes ( $P_{pl}$  - *overall packet loss probability*). Los porcentajes de pérdida de paquetes y la probabilidad global de pérdida pueden ser representados mediante:

$$\frac{P_{pl}}{\%} = P_{pl} \cdot 100$$

## 4.2 Comportamiento de la pérdida de paquetes: microscópico y macroscópico

En el presente trabajo, usaremos una descripción de paquetes perdidos en un sistema VoIP basados en ventanas de tiempo angostas y amplias. Donde, el comportamiento de los paquetes perdidos en una ventana de tiempo angosta será llamada Microscópica, y el comportamiento de pérdida de paquetes en una ventana de tiempo amplia será llamado Macroscópica.

Por comportamiento microscópico entenderemos al periodo de pérdida de paquetes observado en una ventana de tiempo  $W_1$  de una traza de tráfico VoIP; donde este periodo de paquetes perdidos tiene un específico  $PLR_1$ .

Por otra parte, el comportamiento macroscópico se refiere al conjunto de periodos microscópicos ( $W_1, W_2, W_3, \dots, W_n$ ) observado en toda la traza de pérdida de paquetes de tráfico VoIP; en el que cada periodo microscópico tiene su propio  $PLR$  ( $PLR_1, PLR_2, PLR_3, \dots, PLR_n$ ), como se muestra la Figura 15. En este comportamiento existen diferentes niveles de  $PLR$  para cada periodo microscópico, es decir, las pérdidas de paquetes no suceden de manera homogénea o uniforme, sino que se concentran en algunos intervalos de tiempo (los paquetes se pierden por ráfagas). El  $PLR_T$  es calculado sobre el conjunto de trazas ( $W_T = W_1 + W_2 + W_3 + W_4 + W_5$ ).

El comportamiento microscópico puede ser modelado por una cadena de Markov en pocos números de estados, mientras que el comportamiento macroscópico puede ser modelado por una cadena de Markov de varios estados.

Con el fin de simplificar esta descripción de paquetes perdidos, los periodos microscópicos pueden ser clasificados en dos conjuntos; uno para bajas pérdidas y otra para altas pérdidas de paquetes. El umbral usado para delimitar los dos conjuntos, es una función de la percepción de la calidad, buena o mala, de acuerdo al cálculo de valores MOS [23].

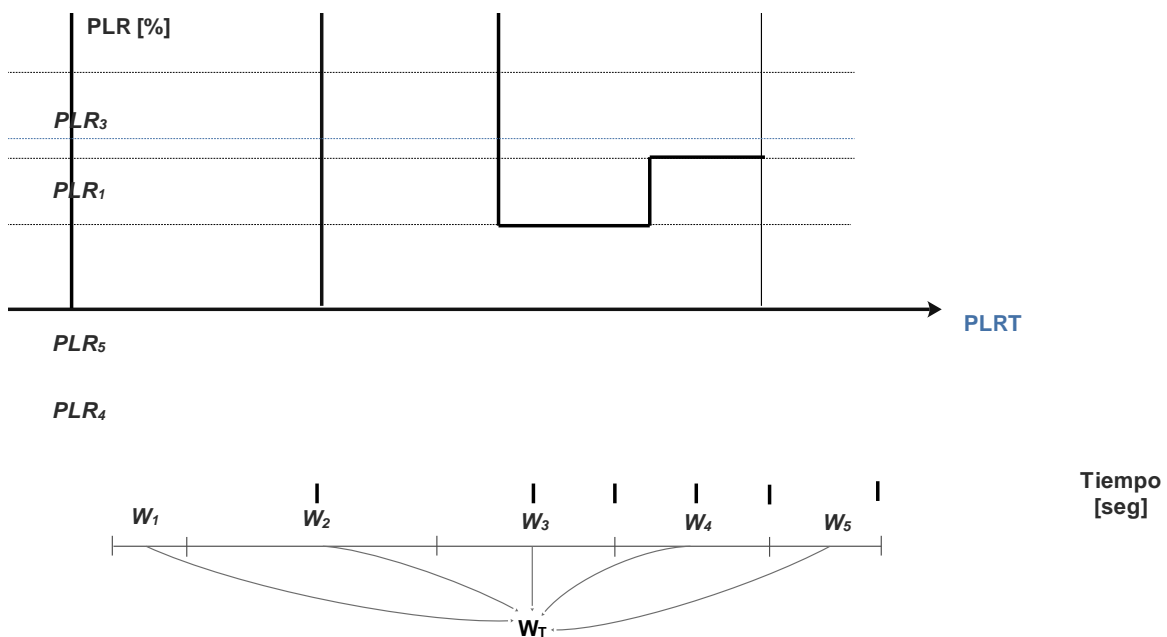


Figura 15 Comportamiento microscópico y macroscópico

#### 4.4 Modelos de pérdida de paquetes: Cadenas de Markov

Las trazas de paquetes perdidos en sistemas VoIP pueden ser modelados adecuadamente mediante cadenas de Markov. Se puede obtener un modelo simplificado de una traza de pérdida, utilizando únicamente una cadena de Markov de dos estados, ver Figura 16.

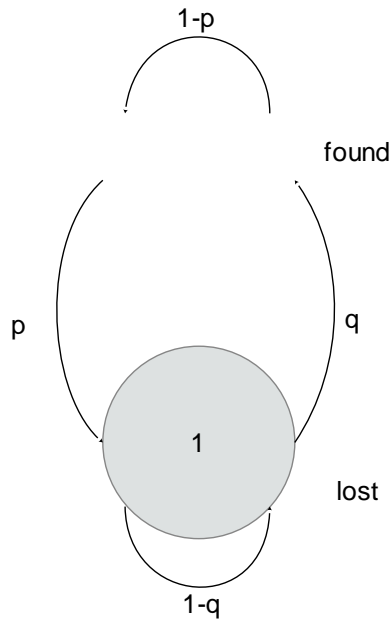


Figura 16 Cadena de Markov de 2 estados

Para una cadena de Markov de 2-estados,  $P_{pl}$  se pueden calcular mediante la siguiente ecuación:

$$P_{pl} = \frac{P}{p + q}$$

Donde  $P_{pl}$  corresponde a la probabilidad de ocupar el estado “1”, es decir, el estado perdido.

La distribución de las pérdidas relacionadas con un modelo de Markov de 2-estados, se puede caracterizar mediante el número de paquetes que se pierden o se encuentran en una fila. Por ejemplo, la probabilidad de que la transición de “1” (perdido) a “0” (encontrado) se produce después de las etapas  $k$ , se puede expresar como:

$$p(k, q) = q(1 - q)^{k-1}$$



De acuerdo a la ecuación anterior, el número de pasos necesarios para el tránsito  $k$  de la pérdida encontrada, es decir, el número de paquetes consecutivamente perdidos, es una variable aleatoria distribuida geoméricamente. Esta distribución geométrica de las pérdidas consecutivas hace que el modelo de Markov de 2-estados sea aplicable a la descripción de los eventos de pérdida observada en Internet. El número medio de paquetes perdidos en una fila se puede calcular como la esperanza (expectativa) de  $k$ .

$$\mu_{10} = E\{k\} = \sum_{k=1}^{\infty} k \cdot q (1 - q)^{k-1}$$

Esta expresión puede estar reescrita como una fila geométrica, de modo que la esperanza se puede calcular como:

$$\mu_{10} = \frac{1}{q}$$

Del mismo modo, el número medio de paquetes consecutivos es encontrado mediante:

$$\mu_{01} = \frac{1}{p}$$

De ello se desprende intuitivamente a partir de  $P_{pl} = \frac{P}{p+q}$  la siguiente ecuación:

$$P_{pl} = \frac{\mu_{10}}{\mu_{10} + \mu_{01}}$$

## 4.5 Mecanismos para atenuar la pérdida de paquetes

La pérdida de paquetes puede ser atenuada mediante diversos mecanismos, dentro de los más utilizados podemos mencionar los siguientes:

- **Corrección de errores (FEC):** en este tipo de técnica, junto con los paquetes, se incluye información de redundancia que permite recuperar el valor del paquete perdido a partir de las redundancias incluidas.
- **Recuperación de errores (PLC):** sustituyen el paquete perdido por otro. Esta situación 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 paquetes anteriores y posteriores. En este sentido, conviene tener en cuenta que, a mayor complejidad, mayor costo de procesamiento y mayor retardo introducido [10].
- **Interleaving:** Este método intenta reducir la degradación de la calidad de audio perceptual mediante la distribución de la pérdida de paquetes en varios gaps pequeños en lugar de tener un burst de gran tamaño. Muchos investigadores creen que puede pasar desapercibido el efecto de la pérdida si se dispersa en varios burst pequeños. Una desventaja es el aumento en el retardo extremo a extremo, debido al tiempo de procesamiento de esta técnica [13] y [24].

En la Figura 17, se muestra el funcionamiento del método de interleaving, como se puede observar el flujo original de paquetes a transmitir en una comunicación se encuentran ordenados en una secuencia, mediante el mecanismo de interleaving se busca cambiar el orden bajo un patrón específico, evitando pérdidas consecutivas por si se presenta alguna congestión o anomalía en la red. Finalmente, es necesario reordenar en la secuencia original en el lado del receptor.

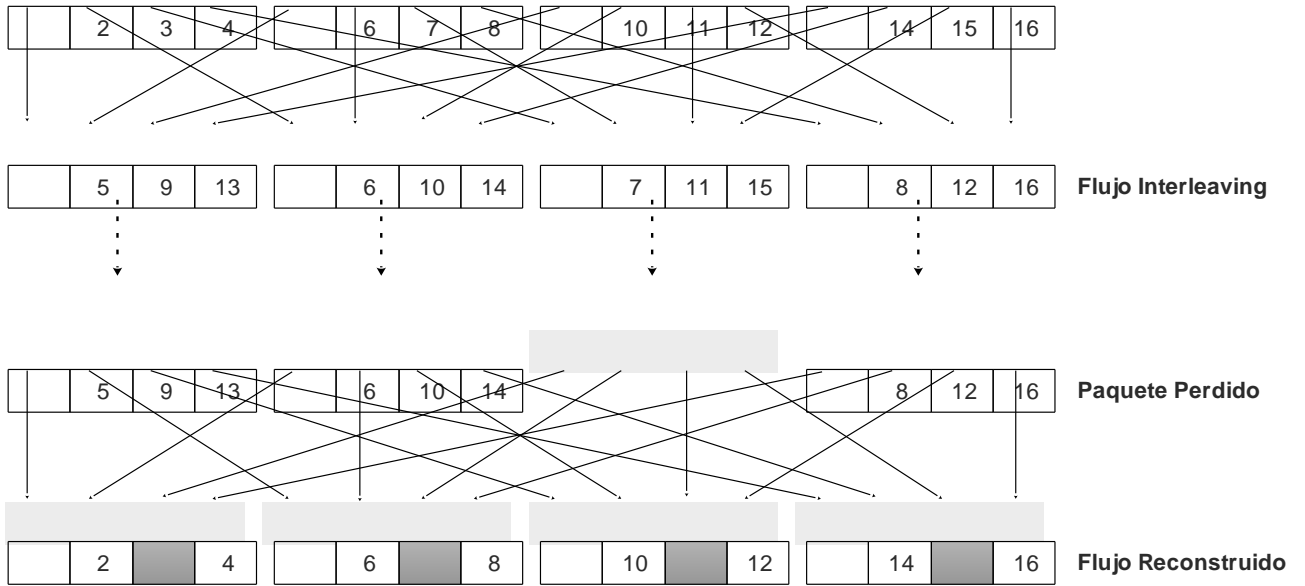


Figura 17 Método interleaving

# CAPÍTULO 5

## CAPÍTULO 5. MEDICIONES

En este capítulo, se abordará el análisis de diferentes escenarios creados. Cada escenario tendrá diferente nivel de  $PLR$  ( $PLR = \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5\}$ ) y diferente nivel de rafagosidad  $w$  ( $w = 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1$ ). En una comunicación real se sabe que, para fines de estudio, es casi imposible obtener un comportamiento de la red con ciertos niveles de  $PLR$  deseado. Supongamos que en una comunicación de VoIP se desea obtener un  $PLR$  de 3%; esto podría tardar mucho tiempo en suceder o tal vez nunca pasaría. Sin embargo, es posible emular diferentes escenarios con diversos niveles de  $PLR$  deseado por medio de la siguiente metodología que se describirá en este capítulo.

### 5.1 Metodología para emular pérdida de paquetes

Las actuales metodologías para simular paquetes perdidos consisten solamente en generar patrones de pérdidas por medio de cadenas de Markov de diferentes estados [3]. La metodología propuesta para emular paquetes perdidos estará basada en dos etapas: primero se genera un conjunto de vectores de pérdida de paquetes y después se introducirá este vector a una aplicación VoIP en software (*VoIPAS*) [13], con el objetivo de emular las pérdidas en la comunicación.

La metodología está basada en los siguientes puntos:

1. Se crearán vectores de pérdida de paquetes mediante una cadena de Markov de 2-estados, los cuales estarán representados por una secuencia binaria:

$$X = \{X_t: t = 1, \dots, N\}$$

Donde,  $X_t = 1$  quiere decir que un paquete se perdió y  $X_t = 0$  que un paquete llegó a su destino y  $N$  es la longitud del patrón de pérdidas o el número de paquetes de voz en una comunicación VoIP.

2. Puesto que los paquetes se pierden en Internet a ráfagas, los valores generados ( $X_t = 1$  o  $X_t = 0$ ) mediante la cadena de Markov de 2-estados con un determinado valor de  $PLR$  ( $PLR = \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5\}$ ) estarán contenidos dentro de una ventana de tiempo  $W_l^u$  de tamaño  $wN$  ( $w = 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1$ ) dentro del vector  $X$ .

Donde:

$W_l^u = \{X_l, X_{l+1}, \dots, X_u : l = 1, 2, \dots, N - [wN] + 1 \quad u = l + [wN] - 1 \quad l < u\}$ ,  $X_l$  y  $X_u$  son el  $l$ -ésimo y  $u$ -ésimo elemento de la serie de tiempo  $X$  y representa la ventana de tiempo desde su comienzo hasta su fin.

Por otro lado, los valores en el vector  $X$  que corresponden a los  $N(1 - w)$  elementos situados fuera de la ventana de tiempo  $W_l^u$  serán rellenados con ceros ( $X_t = 0$ ).

3. Para concluir, se pone en práctica esta metodología, sobre una aplicación en software VoIP. La emulación se realiza de la siguiente manera: a) se introduce en la aplicación VoIP un vector de pérdida  $X$  antes de iniciar la llamada de prueba; b) cuando la aplicación VoIP detecta un “uno” en el vector ( $X_t = 1$ ), el paquete de voz no se envía; y c) cuando la aplicación VoIP detecta un “cero” en el vector ( $X_t = 0$ ), el paquete de voz es enviado.
4. Cada vector tendrá una longitud correspondiente a una llamada de 10 minutos de duración. En este trabajo se utilizará el CODEC G.711, porque es el más utilizado en los servicios de telefonía. El número de paquetes creados en una comunicación de 10 minutos de duración, dependerá del tamaño de paquete utilizado. Para este trabajo se utilizará dos tamaños de

paquetes: 20 ms y 40 ms, utilizaremos de 20 ms ya que es el tamaño más utilizado en sistemas VoIP y el de 40 ms para evaluar el comportamiento de ambos.

## 5.2 Escenario de medición

La Figura 18 a) y b) muestran el escenario de medición real y el escenario de medición emulada, respectivamente. Cabe mencionar, que el escenario real consta de dos computadoras A y B, las cuales se encuentran conectadas únicamente por un cable Ethernet, teniendo así una configuración punto a punto; se sabe que no habría ninguna pérdida de paquetes adicionales a las emuladas en una red punto a punto como esta.

Para generar un conjunto de trazas de tráfico VoIP, se estableció un conjunto de llamadas de prueba mediante la aplicación VoIPAS y para lograr emular el escenario de la Figura 18 b), bajo diferentes condiciones de pérdidas de paquetes (*PLR*), y niveles de rafagosidad ( $w$ ) se aplicó la metodología presenta en la sección (5.1 Metodología para simular paquetes Perdidos)

A continuación, se describen las características de los equipos usados en el escenario de medición:

- La computadora A tiene instalado Windows XP Professional, una IP 192.168.10.4. En esta PC se introducen los vectores de pérdida mediante la aplicación VoIPAS, como se mencionó anteriormente, esta aplicación va a leer cada elemento del vector de pérdida a la misma tasa que transmite los paquetes de voz en la llamada de prueba y enviará el paquete de voz si encuentra un 0 ó no lo enviará si encuentra un 1.
- La computadora B tiene instalado Windows 7 Ultimate x86 con la IP 192.168.10.3. En esta PC también se instaló la aplicación VoIPAS para que se pueda llevar a cabo la comunicación con la computadora A, y para capturar los patrones de tráfico (pérdidas) generados durante la

comunicación entre A y B se utilizó el analizador de protocolos Wireshark y la aplicación de VQcapture [25] (para analizar los bursts y gaps).

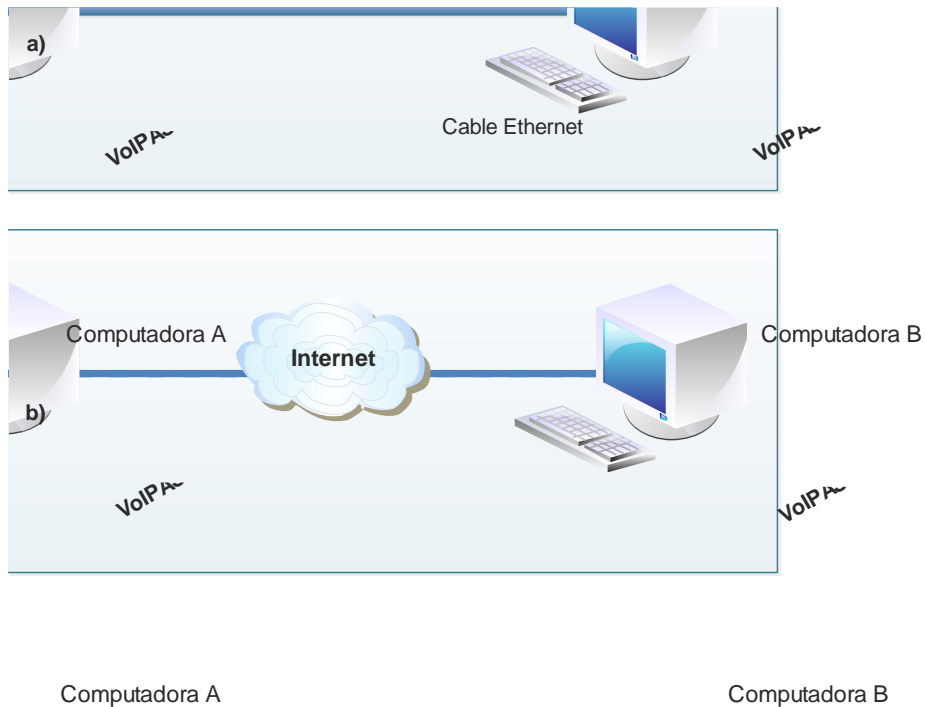


Figura 18 a) Escenario de medición real, b) Escenario de medición emulada

### 5.3 Realización de las mediciones

En esta sección, se describen los pasos seguidos para la realización de la medición de los patrones de tráfico, para los tamaños de paquetes de 20 ms y 40 ms.

Primer paso, configuración de la Computadora A: Ejecutar el VoIPAS, seguidamente crear una nueva sesión dando clic en la opción New Session, como se muestra en la Figura 19.



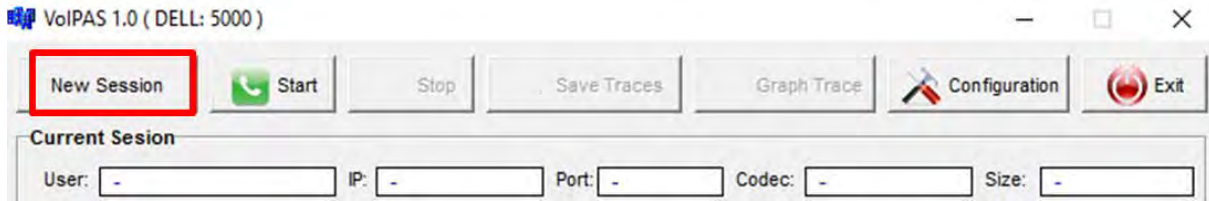


Figura 19 Creación de nueva sesión

Como se muestra en la Figura 20, se configura la IP de la computadora destino, el puerto destino lo dejamos por defecto en 5001, se selecciona el tipo de CODEC (G711 A Law) con un tamaño de paquete(20 ms), se carga el vector de pérdida con la opción Load y las demás opciones no se modifican, clic a OK para terminar la configuración de la Computadora A e iniciar la sesión.

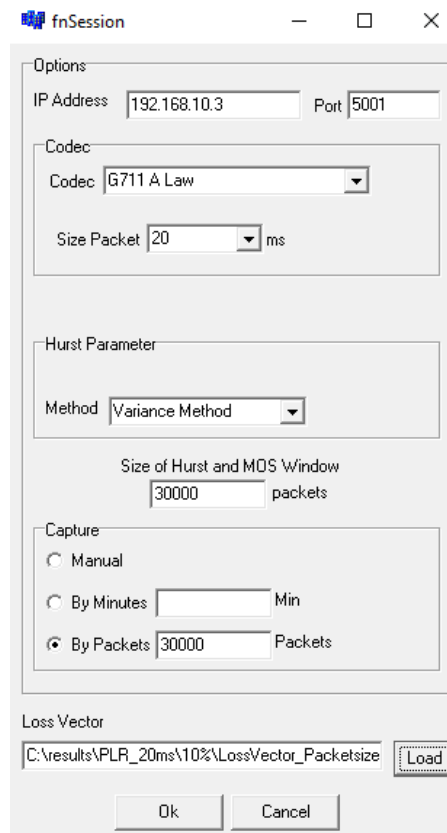


Figura 20 Configuración de una sesión

Segundo paso, configuración de Computadora B: Ejecutar VoIPAS, y como esta computadora funcionará como receptor, no es necesario hacer ninguna configuración. Entonces ya configuradas la computadora emisor y computadora receptor (A y B), se prosigue a realizar la captura de los patrones de tráfico, es necesario abrir Wireshark, seleccionar la interfaz de red utilizada y le damos clic a Start para iniciar a la captura de paquetes, como se muestra en la Figura 21 y al mismo tiempo le damos Start en la aplicación VoIPAS , como se muestra en la Figura 22.

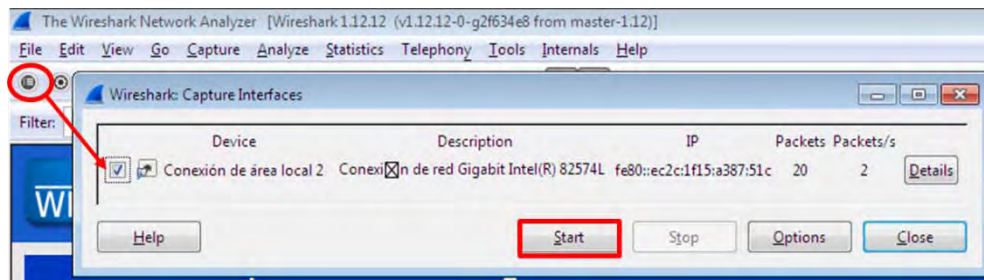


Figura 21 Selección de interfaz de captura

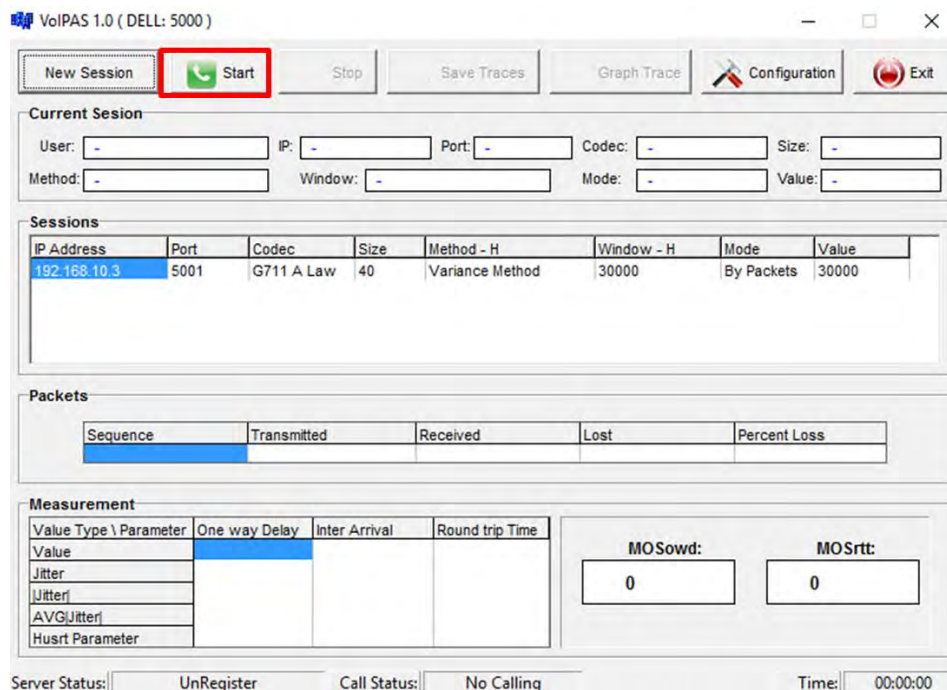


Figura 22 Iniciar comunicación

Una vez establecida la comunicación entre A y B, se iniciará de forma paralela la captura mediante Wireshark en B, como se muestra en la Figura 24

No.	Time	Source	Destination	Protocol	Length	Info
101	0.72368300	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
102	0.72434800	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
103	0.73319000	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
104	0.73336100	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
105	0.74368600	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
106	0.74451800	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
107	0.75363900	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
108	0.75381000	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
109	0.76368200	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
110	0.76465300	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
111	0.77307600	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
112	0.77324200	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
113	0.78368400	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
114	0.78440400	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
115	0.79331800	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
116	0.79349600	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
117	0.80368900	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
118	0.80434300	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
119	0.81406800	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
120	0.81424000	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
121	0.82368500	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
122	0.82439700	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
123	0.83234500	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001
124	0.83252000	192.168.10.3	192.168.10.4	UDP	58	Source port: 5002 Destination port: 5002
125	0.84368500	192.168.10.3	192.168.10.4	UDP	218	Source port: 5001 Destination port: 5001
126	0.84426500	192.168.10.4	192.168.10.3	UDP	60	Source port: 5002 Destination port: 5002
127	0.85258500	192.168.10.4	192.168.10.3	UDP	218	Source port: 5001 Destination port: 5001

Figura 23 Captura de los patrones de tráfico

En este trabajo las llamadas de prueba tuvieron una duración de 10 minutos. Al finalizar los 10 minutos de la comunicación (o recibidos los 30,000 paquetes en B o en el otro caso recibidos los 15,000 paquetes en B), se procede a identificar los flujos RTP entre A (192.168.10.4) y B (192.168.10.3), como se muestra en la Figura 24.

No.	Time	Source	Destination	Protocol
101	0.72368300	192.168.10.3	192.168.10.4	UDP
102	0.72434800	192.168.10.4	192.168.10.3	UDP
103	0.73319000	192.168.10.4	192.168.10.3	UDP
104	0.73336100	192.168.10.3	192.168.10.4	UDP
105	0.74368600	192.168.10.3	192.168.10.4	UDP
106	0.74451800	192.168.10.4	192.168.10.3	UDP

Figura 24 Selección de flujo

Como se puede observar en la Figura 23, en la captura realizada sólo existen flujo de datagramas UDP, para poder visualizar los flujos RTP, es necesario realizar la

decodificación de dichos datagramas; para lograr esto se selecciona un flujo UDP clic derecho y seleccionando la opción Decode As.. y luego RTP, clic en ok para finalizar la decodificación, como se muestra en la Figura 25.

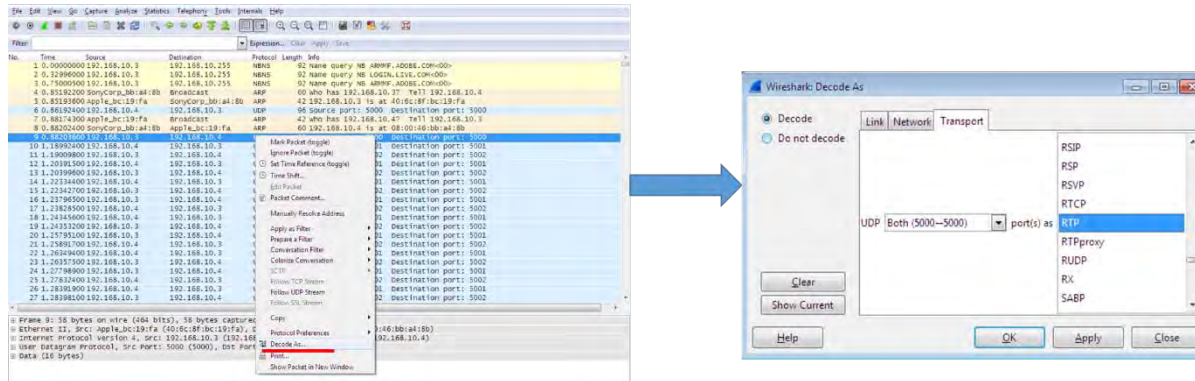


Figura 25 Decodificación de flujos UDP

Después de que se decodificaron los datagramas UDP, seleccionamos la opción Telephony en el menú y dentro de la lista que despliega seleccionamos RTP y le damos clic a Show All Streams para visualizar los flujos RTP, como se muestra en la

Figura

26.

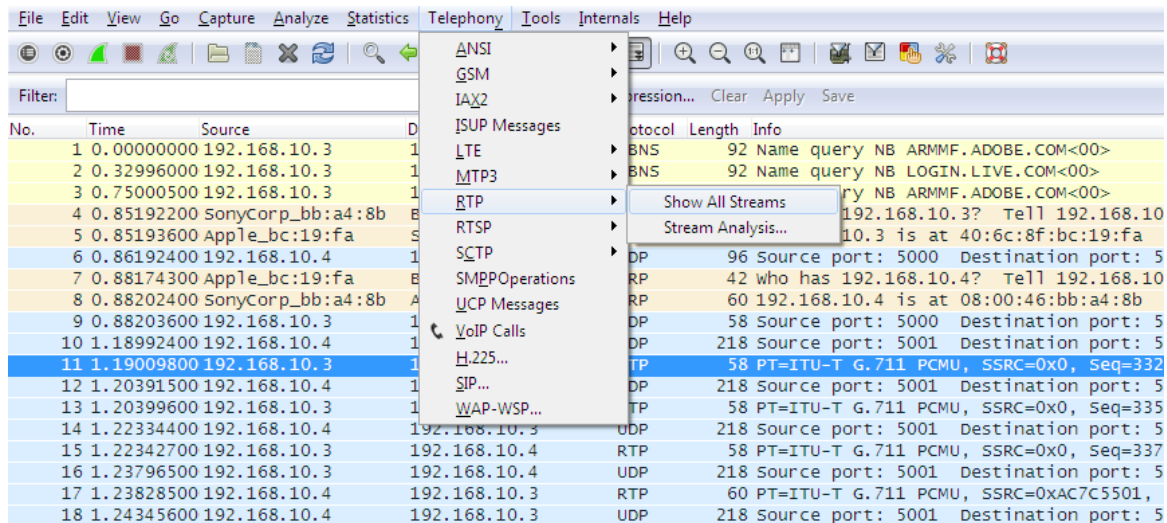


Figura 26 Mostrar todos los flujos RTP

En este paso se puede verificar que el porcentaje de paquetes perdidos medidos durante la comunicación, coincida con el porcentaje de paquetes perdidos (PLR) del vector de pérdida que se introdujo en la aplicación de VoIPAS (PLR simulado),

por ejemplo, para este caso se requiere que en el vector se pierda 90 paquetes (240 unos en el vector de pérdida), que equivale al 0.3% del total de paquetes transmitidos (30,000 paquetes) de la ventana de 10% ( $w = 0.1$ ). En la Figura 27, se observa que se han perdido 95 paquetes (0.32%), lo cual es una buena aproximación de lo esperado, es decir, que el error es muy pequeño.

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
192.168.10.3	5001	192.168.10.4	5001	0x24	g711U	30014	0 (0.0%)	25.328	17.795	17.500	
192.168.10.4	5001	192.168.10.3	5001	0x0	g711U	29925	95 (0.3%)	122.619	25.506	17.583	•

2 streams, 1 selected, 29925 total packets. Right-click for more options.

Close Find Reverse Prepare Filter Export... Copy Analyze Help

Figura 27 Flujo RTP

Este procedimiento se realizó para los diferentes niveles de pérdida  $PLR = \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5\}$ , así mismo, para cada tamaño de ventana ( $wN$ ), es decir, 10 ventanas por tamaño de paquete (para los tamaños de paquete de 20 ms y 40 ms), por lo tanto se generaron 440 llamadas de prueba que representan diferentes condiciones de red en función de la pérdida de paquetes.

Para el tamaño de paquete de 40 ms, se realiza el mismo procedimiento desde el principio, lo único que cambia es cuando se configura la opción de Size Packet, se selección 40 ms, como se muestra en la Figura 28.



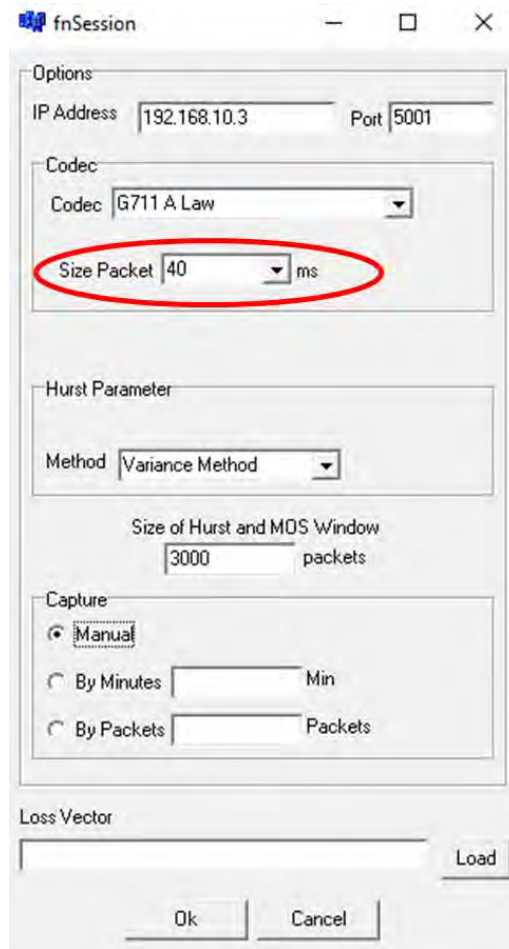


Figura 28 Configuración, para el tamaño de paquetes de 40 ms

# CAPÍTULO 6

## CAPÍTULO 6. ANÁLISIS DE RESULTADO

### 6.1 Análisis de MOS

En la Figura 29 y Figura 30 se pueden ver las diferentes curvas del *MOS vs PLR* para los diferentes tamaños de ventanas (10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%), en las cuales, se introdujeron diferentes niveles de *PLR* (0.1%, 0.2%, 0.3%, 0.4%, 0.5%, 0.6%, 0.7%, 0.8%, 0.9%, 1%, 1.1%, 1.2%, 1.3%, 1.4%, 1.5%, 2%, 2.5%, 3%, 3.5%, 4%, 4.5%, 5%). En las Figuras 30 y 31, se puede observar que a medida que incrementa el *PLR*, la calidad de servicio en la comunicación presenta un decremento y de igual manera, estas figuras muestran que aunque los tamaños de ventanas son diferente, presentan la misma tendencia, es decir, las curvas se sobreponen, esto se presenta para ambos tamaños de paquetes (*PS – Packet Size*) de 20 ms y 40 ms.

Por lo que podemos decir, que el *MOS* no toma en cuenta el comportamiento de las pérdidas de paquetes a ráfagas, sin embargo, de manera perceptual, es lógico pensar que mientras mayor es el nivel de rafagosidad, menor será la calidad de servicio percibida por un usuario final.



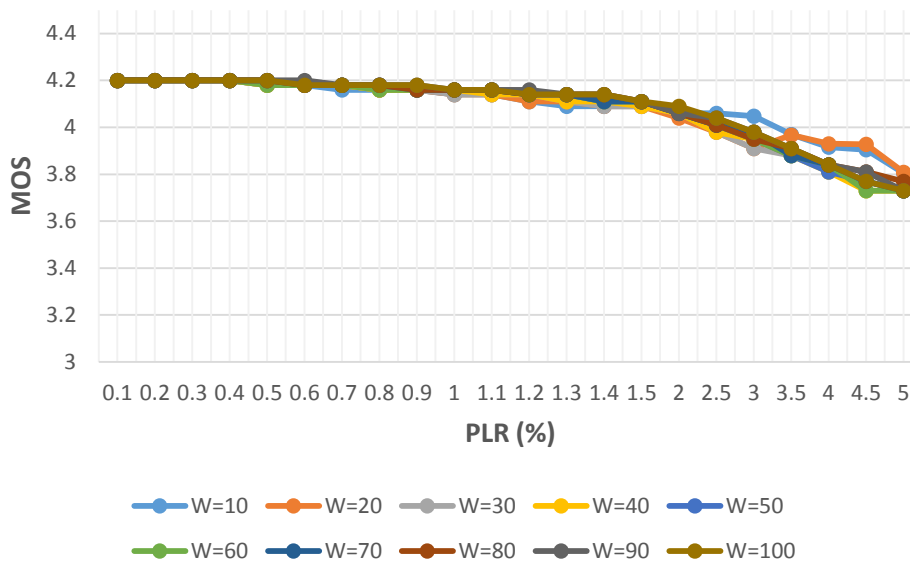


Figura 29 Evaluación del MOS ( $PS = 20 ms$ )

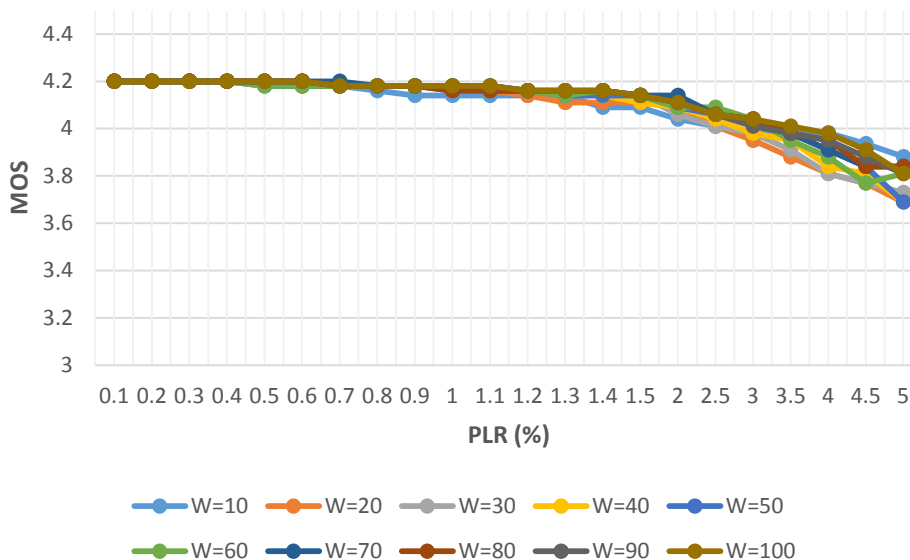


Figura 30 Evaluación del MOS ( $PS = 40 ms$ )

En otras palabras, podemos decir que el nivel de rafagosidad tiene un efecto nulo en la QoS que percibe el usuario final de acuerdo a la evaluación del *MOS*, es decir, para realizar el cálculo de la QoS, el *MOS* sólo toma en cuenta el valor del porcentaje del *PLR* y no su comportamiento temporal.

## 6.2 Análisis de PLR

En la Figura 31, se muestran de manera gráfica los vectores de pérdida de paquetes que se introdujeron a la aplicación de voz sobre el protocolo de Internet denominada VoIPAS para dos diferentes tamaños de ventana ( $W = 10\%$  y  $W = 100\%$ ) y para dos valores de  $PLR$  ( $PLR = 0.1\%$  y  $PLR = 5\%$ ).

De la Figura 31, se observa la distribución temporal de la pérdida de paquetes sobre las ventanas de tiempo de  $W = 10\%$  y  $W = 100\%$ , en las cuales se puede observar diferentes niveles de rafagosidad, representativos de diversos escenarios de red. Por otro lado, se muestra que cuando la ventana  $W$  es más pequeña y se incrementa el nivel de  $PLR$  el número de ráfagas son menores, sin embargo, estas presentan una longitud mayor, es decir que el número de paquetes que se pierden de forma consecutiva por cada ráfaga es mayor o el nivel de rafagosidad es mayor; sin embargo, cuando la ventana  $W$  es de mayor tamaño, se presentan más ráfagas, pero estas son de menor tamaño, en otras palabras, las pérdidas se presentan de una manera uniforme.

Como se mencionó anteriormente, mientras mayor es el nivel de rafagosidad, menor será la calidad de servicio percibida por un usuario final, es decir, la calidad de servicio percibida por el usuario es menor en la comunicación donde el  $PLR$  se presenta en una ventana de  $10\%$  que cuando se presenta en una ventana de  $100\%$ , esto, debido a que en  $W = 10\%$  se puede perder palabras, mientras que en  $W = 100\%$  las pérdidas se distribuyen de manera uniforme en toda la comunicación y pueden pasar desapercibidas.

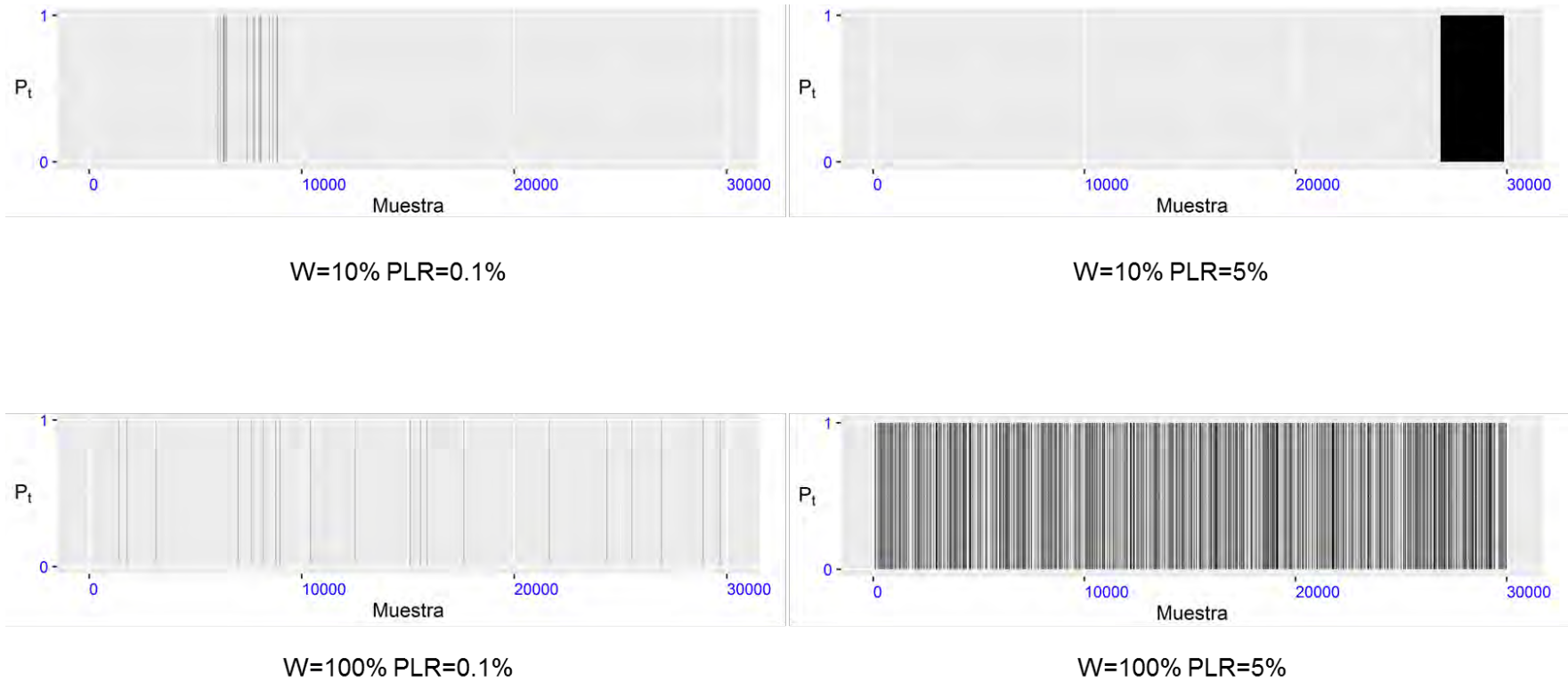


Figura 31 Distribución temporal del *PLR*

La Figura 32 muestra el número de ráfagas de pérdidas de paquetes (burst count) que hubo en el conjunto de llamadas de prueba realizadas bajo diferentes tamaños de ventanas (10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%) y diferentes niveles de *PLR* (0.1%, 0.2%, 0.3%, 0.4%, 0.5%, 0.6%, 0.7%, 0.8%, 0.9%, 1%, 1.1%, 1.2%, 1.3%, 1.4%, 1.5%, 2%, 2.5%, 3%, 3.5%, 4%, 4.5%, 5%).

Como se puede observar, mientras mayor es el valor de *W* y *PLR*, mayor es el número de ráfagas que se presentan en la comunicación.

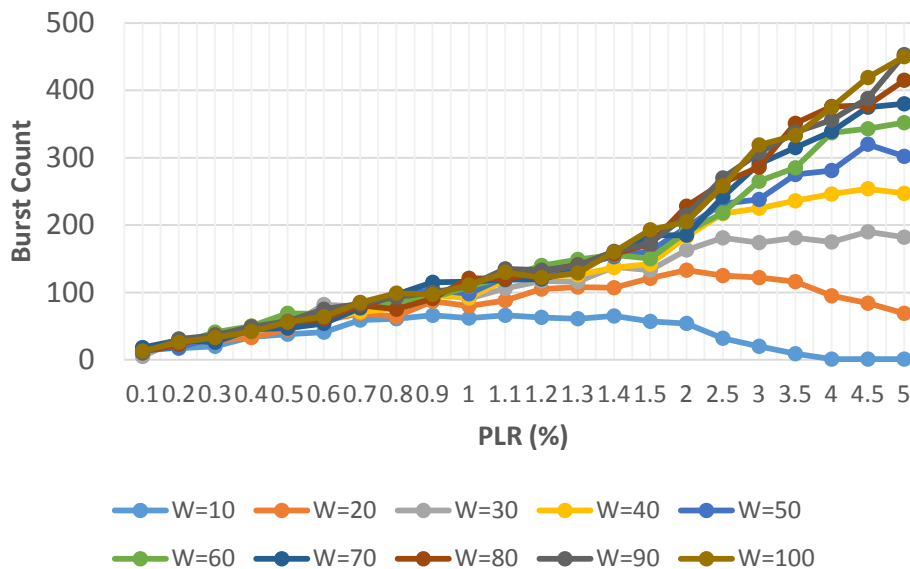


Figura 32 Número de ráfagas de pérdida de paquetes (*PS* = 40 ms)

La Figura 33, muestra la longitud promedio de paquetes perdidos durante las ráfagas (burst length) que se presentaron para el conjunto de llamadas de prueba realizadas bajo diferentes tamaños de ventanas *W* y diferentes niveles de *PLR*.

En la Figura 33 se puede observar que, mientras menor es el valor de *W* y mayor es el valor de *PLR*, mayor es la longitud de las ráfagas que se presentan en la comunicación.

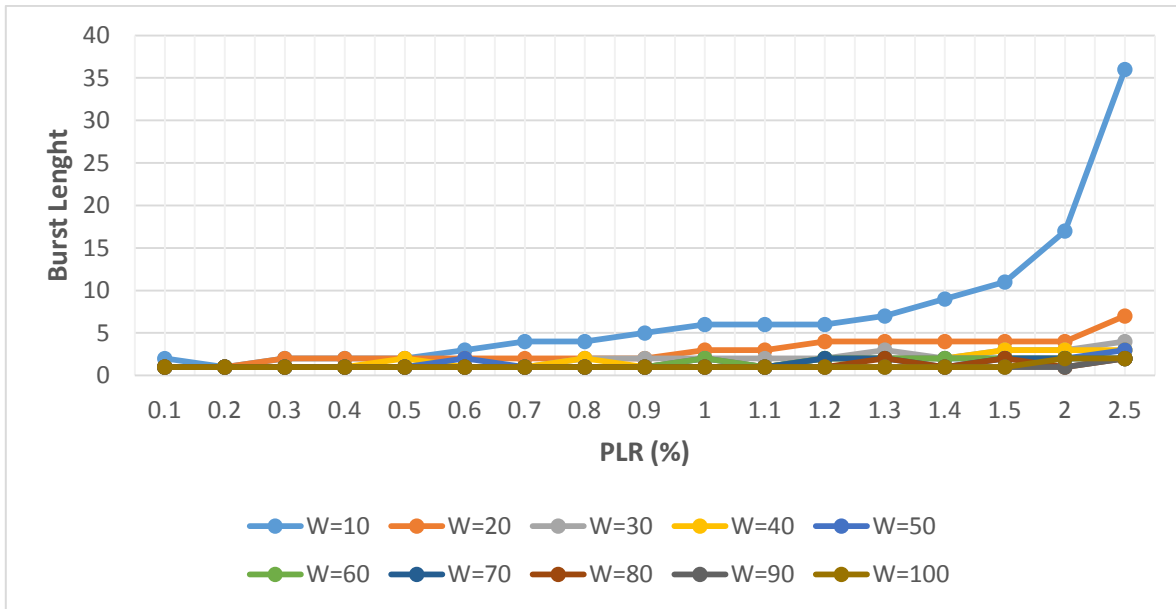


Figura 33 Longitud promedio de paquetes perdidos durante las ráfagas ( $PS = 40\ ms$ )

En la Figura 34, se observa el número de gaps entre las ráfagas de pérdida de paquetes (gap count), es decir, espacios donde no se presentaron pérdidas de paquetes o los paquetes fueron recibidos.

De la Figura 34 Figura 35 observamos que mientras menor es el valor de  $W$  y mayor es el valor de  $PLR$ , mayor es el número de gaps entre las ráfagas que se presentan en la comunicación.

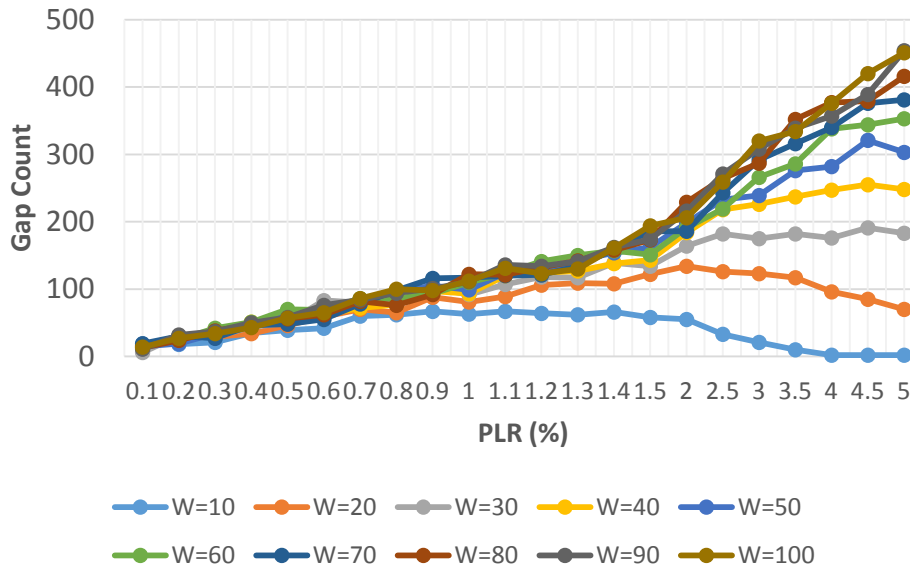


Figura 34 Número de gaps entre las ráfagas de pérdida de paquetes ( $PS = 40\ ms$ )

El presente análisis nos muestra las debilidades que presenta el Modelo E utilizado para evaluar la calidad de servicio percibida por el usuario final mediante el MOS; el cual no considera el comportamiento temporal de la pérdida de paquetes en una comunicación. Es decir, el Modelo E solo utiliza el porcentaje de pérdida de paquetes para realizar el cálculo de la QoS, sin considerar la forma como se presentó el *PLR* (a ráfagas o de forma uniforme). Sin embargo, mediante el estudio del comportamiento temporal del *PLR* es posible presentar un análisis más profundo, a través de las siguientes métricas: número de ráfagas de pérdida de paquetes, longitud promedio de paquetes perdidos durante las ráfagas y número de gaps entre las ráfagas de pérdida de paquetes. Dichas métricas permiten visualizar ciertas variaciones en función del tamaño de ventana  $W$  (nivel de rafagosidad) y del valor de la pérdida de paquetes (*PLR*). Por lo tanto, las métricas mencionadas anteriormente pueden ser usadas para mejorar el Modelo E al considerar diferentes ponderaciones en la QoS en función de  $W$  y *PLR*.

# CAPÍTULO 7

## CAPÍTULO 7. CONCLUSIONES

En la actualidad VoIP es una de las aplicaciones más atractivas dentro de las redes de telecomunicaciones, sin embargo, debido a que opera sobre las redes IP, la calidad de servicio no está garantizada, lo cual implica que existan retardos, jitter y pérdida de paquetes. Las métricas mencionadas anteriormente, son las más importantes que determinan la QoS en una transmisión de voz sobre redes IP.

Por otro lado, la pérdida de paquetes es el principal deterioro que presenta VoIP y que lo hace diferente a la red telefónica pública conmutada, debido al comportamiento dinámico de las redes IP.

Motivados de los puntos mencionados anteriormente, en este trabajo se presenta un análisis del comportamiento temporal de la pérdida de paquetes en una comunicación VoIP y sus implicaciones en la calidad de servicio percibida por el usuario final. Para realizar dicho análisis se generó tráfico VoIP mediante una aplicación en software (VoIPAS) y se emularon diferentes condiciones de pérdida de paquetes, el tráfico generado fue capturado con el analizador de protocolos Wireshark y posteriormente fue procesado mediante la herramienta VQcapture.

Como resultado del análisis realizado en esta tesis, se muestra las debilidades que presenta el Modelo E utilizado para evaluar la calidad de servicio percibida por el usuario final mediante el MOS; el cual no considera el comportamiento temporal de la pérdida de paquetes en una comunicación. Es decir, el Modelo E solo utiliza el porcentaje de pérdida de paquetes para realizar el cálculo de la QoS, sin considerar la forma como se presentó el *PLR* (a ráfagas o de forma uniforme). Sin embargo, mediante el estudio del comportamiento temporal del *PLR* es posible presentar un análisis más profundo, a través de las siguientes métricas: número de ráfagas de pérdida de paquetes, longitud promedio de paquetes perdidos durante las ráfagas y número de gaps entre las ráfagas de pérdida de paquetes. Dichas métricas permiten visualizar ciertas variaciones en función del tamaño de ventana  $W$  (nivel de rafagosidad) y del valor de la pérdida de paquetes (*PLR*). Por lo tanto, las métricas mencionadas anteriormente pueden ser usadas para mejorar



el Modelo E al considerar diferentes ponderaciones en la QoS en función de  $W$  y  $PLR$ .

Como trabajo futuro se podría proponer alguna mejora del Modelo E, mediante la adición de las métricas de contador de ráfagas, contador de gaps y tamaños de ráfagas.

## Referencias

- [1] F. Gebali, *Analysis of Computer and Communication Networks*, Springer, 2008.
- [2] A. Raake, *Speech Quality of VoIP*, John Wiley & Sons, Ltd, 2006.
- [3] A. Raake, «Short and Long-Term Packet Loss Behavior Towards Speech Quality Prediction for Arbitrary Loss Distributions,» *IEEE Transactions on Audio, Speech, and Language Processing*, vol. XIV, nº 6, 6 Noviembre 2006.
- [4] H. Toral Cruz, A.-S. Khan Pathan y J. C. Ramírez Pacheco, «Accurate Modeling of VoIP Traffic QoS Parameters in Current and Future Networks with Multifractal and Markov Models,» *Mathematical and Computer Modelling Jourba*.
- [5] A. A. Domínguez Hernández, *Análisis de Implementación y Recomendaciones de Soluciones Corporativas de Comunicaciones Unificadas NGG BASED con Business Communications Manager (BCM) de Nortel*, Quito, 2009.
- [6] D. Soldani, M. Li y R. Cuny, Edits., *QoS and QoE Management in UMTS Cellular Systems*, JOHN WILEY & SONS. LTD, 2006.
- [7] J. Gómez López y F. Gil Montoya, *Volp y Asterisk. Redescubriendo la telefonía*, Primera ed., Madrid: Alfaomega, 2008, p. 348.
- [8] W. Stallings, *Comunicaciones y redes de Computadores*, Sexta, Ed., Prentice Hall, 2007.
- [9] B. A. Forouzan, *Transmisión de Datos y Redes de Comunicaciones*, Segunda ed., C. Fernández Madrid, Ed., McGraw Hill, 2002.
- [10] J. M. Huidobro Moya y D. Roldán Martínez, *Tecnología VoIP y Telefonía IP*, Primera ed., Alfaomega, 2006.
- [11] E. Landívar, *Comunicaciones Unificadas con Elastix*, Primera ed., vol. I, 2008.
- [12] A. R. Castro Lechtaler y R. J. Fusario, *Teleinformática para Ingenieros en Sistemas de Información*, vol. II, Barcelona: Reverté, 1999.
- [13] J. A. Argáez Xool, *Software para análisis de QoS en VoIP*, CINVESTAV Unidad Guadalajara, Jalisco, 2009.
- [14] G. d. R. Almeyda Torres, *Desarrollo de un Generador de Tráfico Sintético de VoIP*, Chetumal, Quintana Roo, 2013.

- [15] J. Postel, *TCP: Transmission Control Protocol*, 1981.
- [16] A. S. Tanenbaum y D. J. Wetherall, *Computer Networks*, Quinta ed., Prentice Hall, 2011.
- [17] M. Faúndez Zanuy, *Tratamiento digital de voz e imagen y aplicaciones de la multimedia*, Barcelona: Marcombo, 2000.
- [18] G. Camarillo, *SIP Demystified*, McGraw-Hill, 2002.
- [19] J. I. Moreno, I. Soto y D. Larrabeiti, «Protocolos de Señalización para el transporte de Voz sobre redes IP».
- [20] J. A. Caballar, *VoIP. La telefonía de Internet*, Madrid: Thomson, 2008.
- [21] D. Quercia, *A Simulative Study of Distributed Speech Recognition Over Internet Protocol Networks*, Illinois, Chicago, 2002.
- [22] Network Working Group, *RFC 3611*, 2003.
- [23] H. Toral Cruz, *Modelado de los Parámetros de QoS de tráfico VoIP Auto-similar y una Mejora al Modelo E*, CINVESTAV Unidad Guadalajara, Jalisco, 2010.
- [24] T.-K. Chua y D. C. Pheanis, «Qos Evaluation of Sender-Based Loss-Recovery Techiques for VoIP,» *IEEE Network*, 2006.
- [25] I. Telchemy, «Telchemy,» [En línea]. Available: <https://www.telchemy.com/vqcapture.php>. [Último acceso: 2016].