## línea horizontal



Trabajo Practico Redes Administrativas

**Redes Administrativas** - 2do Cuatrimestre - Año 2022

**Profesor:** Milio Claudio

**─**

**Autores**

ALFANO, Laura Magali

DOME, Martín

RODRÍGUEZ ARATA, Damián Agustín

VILLANOVA, Pablo Emmanuel

# Índice

[**Índice**](#_heading=h.2et92p0) **1**

[**Consigna**](#_heading=h.3dy6vkm) **1**

[**Desarrollo de la actividad**](#_heading=h.1t3h5sf) **1**

[**VOIP**](#_heading=h.4d34og8) **1**

[VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.](#_heading=h.opk120den9o4) 2

[VoIP Retardo.](#_heading=h.50gb8j8qy3ep) 2

[CAUSAS DEL DELAY.](#_heading=h.alunql44c3hp) 2

[Jitter.](#_heading=h.sde3qz7redup) 3

[JITTER: BUFFER ADAPTATIVO.](#_heading=h.l7oxiwddehgz) 4

[Pérdida de Paquetes.](#_heading=h.zaywjyv512dc) 4

[CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS.](#_heading=h.bgaylroy6u7t) 5

[LATENCIA.](#_heading=h.7qlcw5qcx2bo) 5

[**PARÁMETROS DE LA VOZ.**](#_heading=h.c8aqv3m8uv7u) **6**

[Calidad de la Voz VSQ.](#_heading=h.skrvkussxlv5) 6

[**PROTOCOLOS VOIP.**](#_heading=h.cbdy25x7j45q) **8**

[TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP.](#_heading=h.pl1f0srivwbh) 8

[REAL TIME TRANSPORT PROTOCOL](#_heading=h.8i3ddeyto50j) 9

[PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL).](#_heading=h.b5g8nxkqg1hu) 13

[SEÑALIZACIÓN Y CONTROL DE LLAMADA H.323 y SIP](#_heading=h.h9a9z9502dtz) 14

[PROTOCOLO DE SEÑALIZACIÓN H.323](#_heading=h.i8k31k5ftnns) 15

[EL ESTABLECIMIENTO DE LLAMADAS EN H.323.](#_heading=h.34fwbmd26cn7) 18

[PROTOCOLO DE SEÑALIZACIÓN SIP](#_heading=h.tmmjo4lpmvfl) 21

[SERVIDORES DE REDIRECCIÓN.](#_heading=h.74ppn9neh9ku) 22

[SERVIDORES PROXY.](#_heading=h.vbjno165oe5b) 23

[SERVIDORES DE REGISTRO.](#_heading=h.gte5krqoeh1b) 23

[**Bibliografía consultada**](#_heading=h.3rdcrjn) **28**

# Consigna

# Desarrollo de la actividad

## VOIP

IP ha tenido su origen en transmisión de datos y no estaba adaptada a la transmisión de voz e imágenes. La tecnología de transmisión de paquetes, en la que está basada IP, ofrece tamaño de celdas variable, que en comparación con tecnologías de tamaño de celda fija como ATM, introduce ineficiencias y necesidad de proceso extra. IP es un protocolo que en principio ofrece un tipo de calidad de servicio (QoS) basado en proporcionar el mejor rendimiento posible en el enlace disponible. (Best Effort)

VoIP es una tecnología que permite enviar y recibir llamadas o videollamadas por internet. Recopila la voz humana para codificarla en datos digitales y mandarla a otro dispositivo que los traduce de nuevo en voz, en tiempo real. Su nombre proviene del inglés voice over IP y significa «voz sobre protocolo de internet».

La configuración de las llamadas VoIP permite que estas se realicen con teléfonos o celulares y también por medio de computadoras, laptops o adaptadores telefónicos. Se puede realizar entre dos o más dispositivos conectados a la red. Entre las aplicaciones más populares que utilizan esta tecnología están WhatsApp, Messenger de Facebook, Telegram, Skype y Zoom, entre otras.

Existen además proveedores de VoIP privados que ofrecen más funciones y ventajas que las de uso común, como una red más segura que protege el servicio de software maliciosos, robos de base de datos, intentos de hackeo de las cuentas y fraudes.

### VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

◼ Retardos de los paquetes: una red IP no asegura el retardo de un paquete. Solamente a través del control y gestión global extremo a extremo, y la disponibilidad de suficiente ancho de banda, así como la tecnología de switching-routing necesaria, es posible asegurar unos niveles de retardo máximos.

◼ Jitter: es muy dependiente del retardo de los paquetes, y consiste en el tiempo de variación en la llegada de paquetes. Este parámetro tiene los mismos problemas y dificultades que el retardo, por lo que las soluciones van en la misma línea.

◼ Pérdida de paquetes: al estar basados sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión.

### VoIP Retardo.

El retardo produce dos problemas:

◼ La presencia de Eco

◼ Talking Overlap

El eco es causado por la reflexión de la señal de voz del que habla y que vuelve a su oído. Es producida por las desadaptaciones en el terminal receptor del equipo lejano. Se convierte en un problema importante cuando el retardo de ida y vuelta es mayor a 50 mseg. Como el eco es percibido como problema significativo desde el punto de vista de la calidad, se debe corregir con la utilización de canceladores de eco. La presencia de Eco - Talking Overlap (Solapamiento de hablantes ) Se produce cuando los dos interlocutores hablan simultáneamente, particularmente cuando uno está hablando y el otro se superpone. Se convierte en un problema importante cuando el retardo extremo a extremo es mayor a 150 mseg.

Por esto, el retardo “end to end”, es el mayor condicionante para el diseño de una red de VoIP, para asegurar un nivel de calidad acorde a los requerimientos de los clientes.

### CAUSAS DEL DELAY.

◼ Demora de trama (demora de algoritmo o de acumulación)

◼ Demora de procesamiento (depende del hardware)

◼ Demora de red.

Es causada por el modo de operación de los codificadores de voz. Estos requieren una o más tramas completas de muestra por lo que es necesario un “buffering”. Esto implica cierta demora inevitable, y que es inherente al proceso de codificación. El codificador acorde a la norma G.729 CS-ASELP que comprime la voz a 8 Kbits/seg introduce un retardo de 10 mseg. Es el tiempo que toma el codificador en “analizar” la voz, esto es, la toma de las muestras de voz, más el tiempo que consume el decodificador en reconstruirla y es dependiente del hardware. Esta demora es causada por el medio físico de la red, de la capacidad de los links de la misma y los protocolos usados en la transmisión de la VoIP y además por los buffers utilizados para remover el jitter en el extremo receptor. Es una parte significativa en la suma de la demora total extremo a extremo.

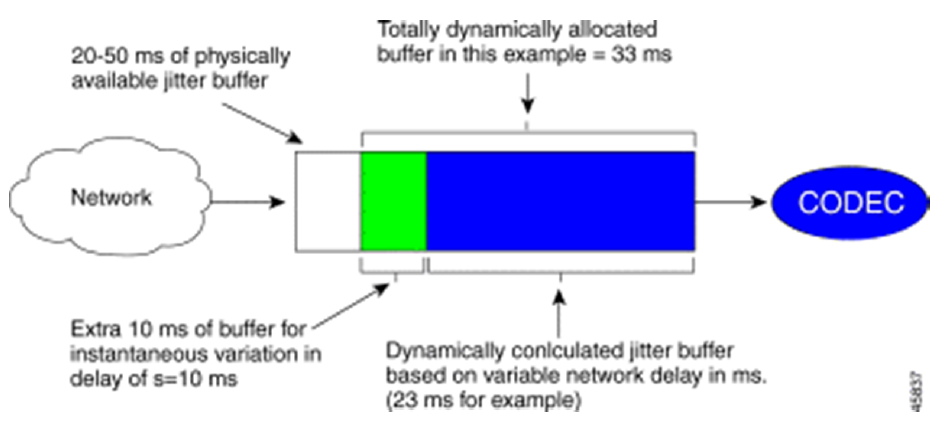
### Jitter.

Es la variación del tiempo de arribo de los frames del codec. Se producen por los distintos caminos que puede tomar el paquete al cruzar la red y afecta la calidad. Si la muestra entra en el buffer introduce retardo y si no entra en el buffer afecta por el descarte de paquetes. Para contrarrestarlo se utilizan Buffers Anti-jitter Adaptativos: el Gateway sensa el Jitter de la red (RTP) y ajusta el tamaño del “de-jitter buffer” para compensar las diferencias de tiempo de arribo de paquetes. Esto afecta la latencia pues introduce retardos en la red.

## 

### JITTER: BUFFER ADAPTATIVO.

El buffer adaptativo es calculado dinámicamente tomando como variable el delay de la red en milisegundos.



### Pérdida de Paquetes.

Al estar basado VOIP sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión. La pérdida de paquetes introduce tasa de error en las comunicaciones.

**Se minimiza:**

◼ Sobredimensionando las redes de modo que no se tengan que descartar paquetes en forma preventiva en los routers (WRED)

◼ Marcando los paquetes de VoIP como prioritarios (Diffserv)

**El oído humano tolera no más de 1% al 3% de paquetes perdidos**

### CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS.

Se debe tener en cuenta los “silencios” de la conversación, para una mejor explotación del ancho de banda. Para ello se emplean “algoritmos de compresión del silencio” en la codificación de voz.

Por ello se requiere la utilización de:

◼ Algoritmos de detección de la actividad de voz (VAD)

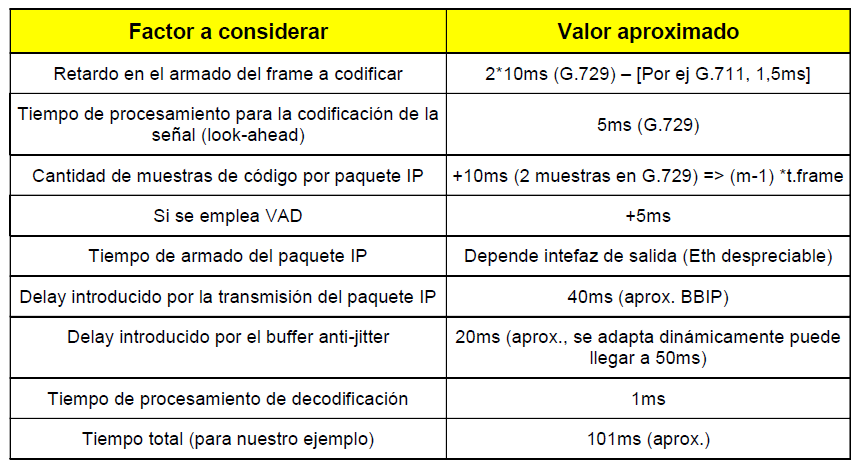
◼ Algoritmos de generación de ruido de confort (CNG)

La señal de voz codificada resultante se transmite con una velocidad no uniforme en función del nivel de actividad que presente la fuente generadora.

El mecanismo de compresión del silencio es crítico en las prestaciones de la codificación de voz. Una implementación inadecuada conlleva a un deterioro significativo de la inteligibilidad de la voz.

### LATENCIA.

Es el retardo one-way entre ambos extremos No debe superar los 150ms para no afectar la interactividad.



## PARÁMETROS DE LA VOZ.

### Calidad de la Voz VSQ.

La calidad de la voz (Voice Speach Quality) es evaluada por medio de dos parámetros:

◼ Claridad: que refleja el grado de palabras y frases entendidas

◼ Fidelidad: califica el grado de reconocimiento de la personal que habla.

La VSQ se puede medir en mediciones subjetivas o mediciones objetivas.

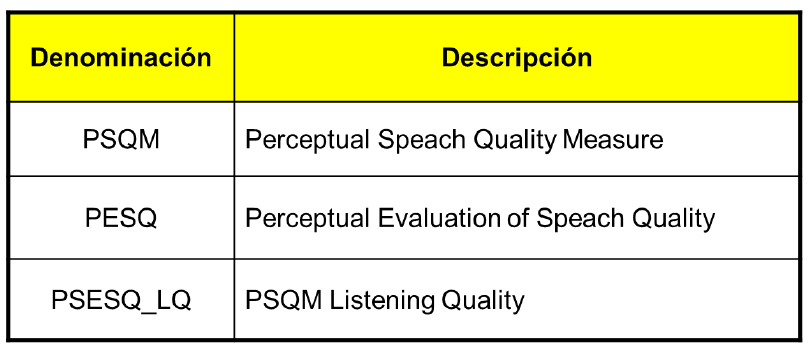
Las medidas objetivas de la ejecución de servicios, como la pérdida de información y el retardo contribuyen a la QoE (calidad de experiencia). Para realizar estas mediciones habitualmente se utilizan sistemas electrónicos, los cuales están basados en algoritmos y fórmulas matemáticas que miden la QoE en sistemas de IPTV, algunas de las técnicas que estos equipos electrónicos implementan son:

◼ Técnicas basadas en modelos de percepción humana de vídeo.

◼ Técnicas basadas en parámetros que indican el grado de deterioro de la red.

◼ Técnicas basadas en el tiempo del deterioro de la señal de vídeo.

◼ Técnicas basadas en los parámetros de las señales de vídeo.



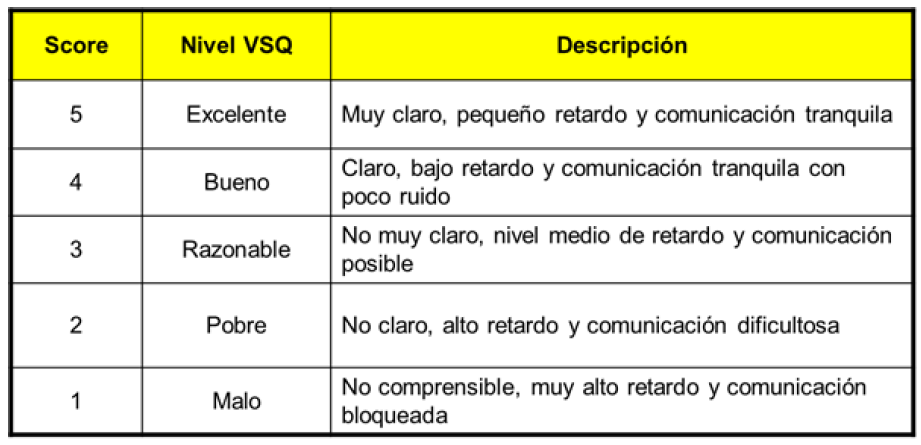
En las mediciones subjetivas se aplica la Recomendación P.830 del ITU en la que se aplica el método Mean Option Score (MOS). Estas medidas se realizan en entornos donde participan grupos de personas, las cuales realizan un conjunto de pasos como los que se listan a continuación:

◼ Elegir las secuencias de vídeo a evaluar.

◼ Evaluación y calificación numérica por parte de los observadores.

◼ Depuración de los observadores por fallos en el proceso.

◼ Cálculo de la calidad subjetiva media, mediante el análisis estadístico de los resultados encontrados por los observadores, este valor es conocido como MOS (Mean Opinion Scale).



## PROTOCOLOS VOIP.

Las tecnologías "IP" hacen referencia a un conjunto de protocolos que conforman la red IP.

Los protocolos de transporte más usados son:

◼ TCP: capaz de proporcionar conexiones garantizadas para paquetes de datos sobre IP

◼ UDP: que proporciona un servicio de entrega no garantizado

Ninguno de estos protocolos por sí mismos pueden proporcionar el soporte de aplicaciones en tiempo real como la voz.

Existen una serie de protocolos que proporcionan servicios en tiempo real sobre IP

◼ RTP (Real Time Transport Protocol)

◼ RTCP (Real Time Control Protocol)

◼ RSVP (Resource Reservation Protocol)

◼ RTSP (Real Time Streaming Protocol)

Existen a su vez protocolos de señalización, que permiten el inicio, mantenimiento y fin de cada comunicación:

◼ Modelo H.323 (solución UIT)

◼ Modelo SIP (solución IETF)

◼ Modelo MEGACO (H.248)

### TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP.

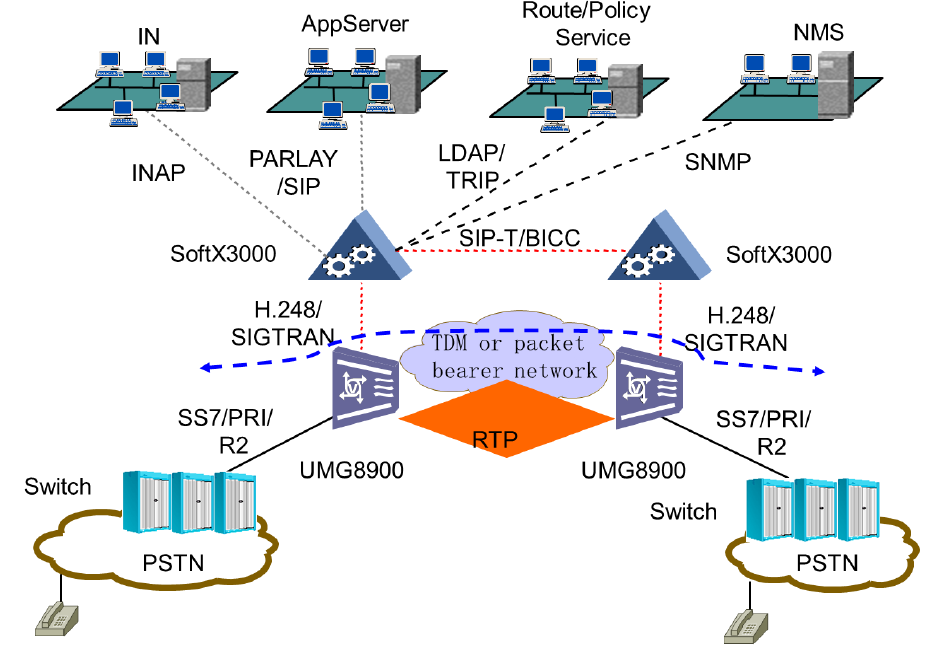
Se requiere un protocolo, o conjunto de ellos, que se ocupe de esta tarea y garantice la entrega de los paquetes de “medios” en tiempo real, o casi en tiempo real, siempre y cuando el deterioro de la calidad no sobrepase lo humanamente admisible, según el caso.

En relación con esto hay que señalar que la red IP no solo “mueve” a través de ella paquetes de información de usuario propiamente dicha, sino también “mueve” paquetes de control, es decir paquetes de señalización.

El término señalización en Telefonía IP tiene una connotación algo más amplia que el concepto correspondiente en las redes clásicas de Telecomunicaciones modo circuito.

Se trata ahora no sólo de la señalización necesaria para el control de la llamada en el sentido clásico (establecimiento, mantenimiento-modificación y terminación de la “conexión”), sino también señalización para garantizar QoS.

En correspondencia con esto, hay que hacer la distinción entre “transporte de medios”, en alusión a la información de usuario (voz, imágenes, etc.), y “transporte de información de control”, es decir, señalización.



El transporte de los medios (voz, vídeo, datos, etc.) por la red IP no sólo se traduce en mover por la misma secuencia de bits empaquetados, sino que también se requiere adicionarles a éstos cierta información de control, por ejemplo:

◼ Tipo de información transportada

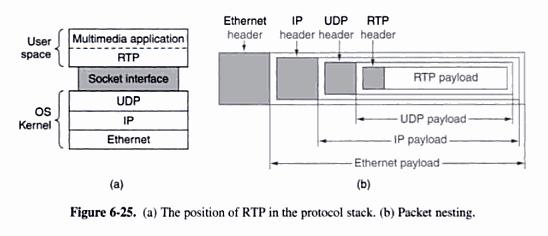
◼ Números de secuencia

◼ Marcas de tiempo, etc.

Esto supone una manera de “formatear” los paquetes IP y hacerlos aptos para el transporte de información con requerimientos de tiempo real.

### REAL TIME TRANSPORT PROTOCOL

RTP – significa “Real Time Transport Protocol” (Protocolo de transporte en tiempo real), y define un formato de paquete estándar para el envío de audio y video sobre Internet. Es definido en el RFC1889. Fue desarrollado por el grupo de trabajo de transporte de audio y video y fue publicado por primera vez en 1996. RTP se utiliza en los sistemas de comunicación y entretenimiento que involucran medios de transmisión, tales como la telefonía, aplicaciones de videoconferencias, servicios de televisión y web basado en funcionalidades push-to-talk.



**Posición de RTP en el stack de protocolos**

El transporte de medios exige cumplir una serie de requisitos:

◼ Caracterización de la carga útil, su identificación, cómo ha sido codificada, su formato, cuántas tramas por paquete, etc.

◼ Información de tiempo que posibilite su reconstrucción temporal en el receptor o los receptores, y la sincronización de diferentes flujos de medios en el tiempo.

◼ Secuenciamiento de los paquetes que constituyen los streams de medios, para posibilitar su reproducción en orden correcto y la detección de paquetes perdidos

Todo esto posibilita la gestión adecuada de los streams de medios en el receptor.

Concebido para compensar el jitter y la pérdida de secuencia de los paquetes que introducen las redes IP. Puede ser empleado para el transporte de streams de datos sensibles al tiempo, p.e. voz y vídeo.

RTP se utiliza junto con el protocolo de control de RTP (RTCP). Mientras que RTP transporta los flujos de medios (por ejemplo, audio y vídeo), RTCP se usa para supervisar las estadísticas de transmisión y calidad de servicio (QoS) y ayuda a la sincronización de múltiples flujos. RTP es originado y recibido en número de puerto par y la comunicación asociadas a RTCP utilizan el próximo número de puerto impar superior. RTP es uno de los fundamentos de VoIP y se utiliza conjuntamente con SIP el cual ayuda a establecer las conexiones a través de la red.

Los protocolos RTP y RTCP no ejercen ningún tipo de influencia en las condiciones de la red IP, no controlan la calidad de servicio, sólo posibilitan que los receptores puedan “resolver” apropiadamente las “perturbaciones” (jitter, pérdida de secuencia) a que son sometidos los paquetes IP con contenidos de tiempo real al atravesar la red.

Los paquetes RTP transportan streams de datos sensibles a:

◼ A las demoras de la red

◼ A sus fluctuaciones

◼ A las pérdidas de paquetes,

◼ A las pérdidas de información adicional que posibilite su recuperación y entrega adecuada.

Con respecto a las pérdidas de información adicional:

◼ La identificación de la fuente

◼ Tipo de carga útil que transporta el paquete

◼ La secuenciación de paquetes

◼ La información de temporización

El protocolo RTP provee monitorización, diagnóstica y realimenta al emisor de la calidad de la transmisión; soporta también la integración de tráfico transmitiendo múltiples fuentes en un simple flujo.

**RTP Provee:**

◼ Sincronismo

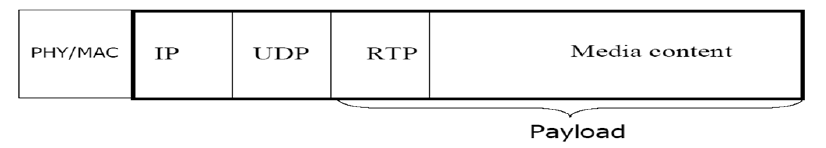
◼ Secuenciamiento y Detección de pérdida de paquetes

◼ Segmentación y rearmado

Cada flujo RTP es unidireccional y tiene asociado un flujo RTCP en el port UDP n+1.

El lado origen envía: información sobre los datos enviados, sincronización y timestamp

El lado receptor envía: información sobre los datos recibidos, pérdida de paquetes, jitter y delay.



RTP posibilita el transporte de datos isócronos a través de redes de paquetes

Ha sido optimizado para transferencias con requisitos de tiempo real, tanto unicast como multicast, soportando servicios extremos a extremo.

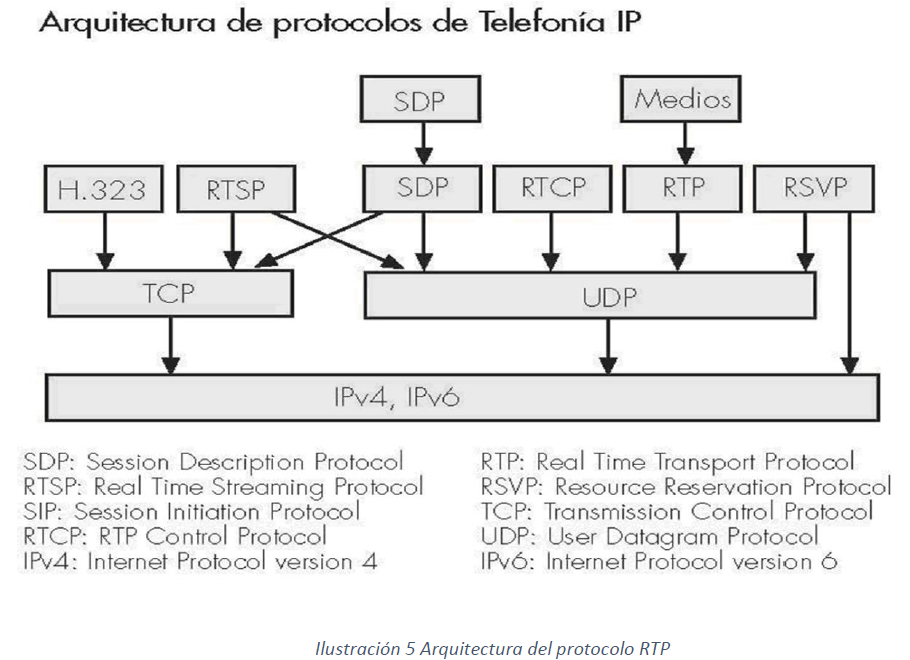
Pero no garantiza:

◼ Reserva de recursos ni da garantía de calidad de servicio

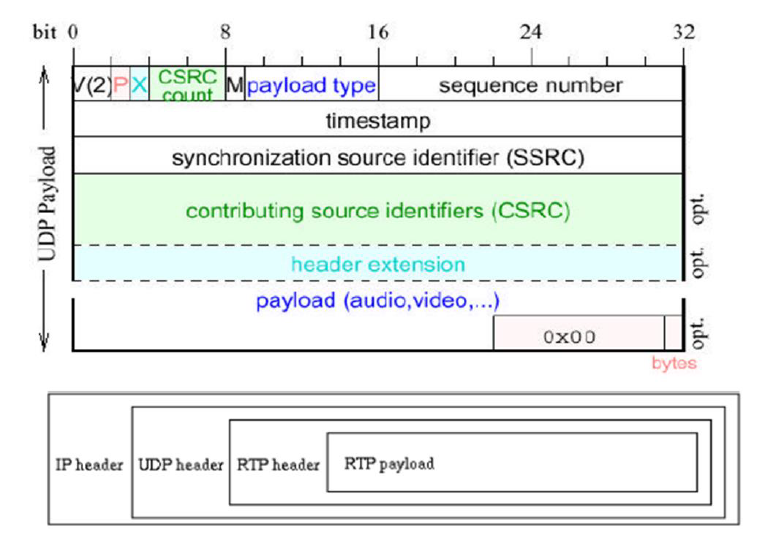
◼ Provisión de mecanismos para garantizar la entrega en tiempo

◼ Asume que la red es segura y entrega los paquetes en secuencia.

Su papel fundamental es actuar como una interfaz entre aplicaciones de tiempo real y los protocolos de la capa de transporte, sin establecer qué protocolo debe ésta usar, aunque típicamente se soporta sobre UDP.



A continuación, se muestra la trama RTP:



### PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL).

RTCP es un protocolo de control que “acompaña” al protocolo RTP para la transferencia entre fuentes y destinos de streams multimedia. Proporciona información de la calidad de la transmisión en la red, posibilitando adaptar las fuentes al estado de la red.

RTCP se basa en la transmisión periódica de paquetes de control a todos los participantes en la sesión, empleando el mismo mecanismo de distribución que los paquetes de datos, por lo que debe proveer la multiplexación de paquetes de datos y paquetes de control RTCP, p.e., mediante el empleo de puertos diferentes del protocolo UDP.

RTCP es imprescindible en sesiones multicast, como realimentación de cómo reciben los streams de datos los destinatarios, posibilitando así homogeneizar la calidad. En comunicaciones unicast no es necesario, pero si es útil su uso.

Sus funciones son las de suministrar información respecto a la calidad de la distribución de los datos, “realimentación” que posibilita a la fuente de los datos:

◼ aplicar control de flujo

◼ aplicar control de congestión

◼ aplicar codificación adaptativa

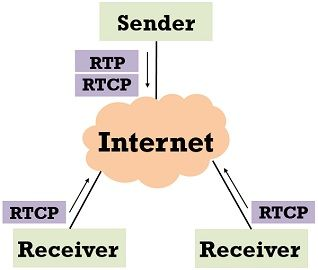
◼ diagnosticar fallos en la distribución multicast

◼ posibilita obtener información útil para diagnóstico y gestión de la red.

También controla la velocidad de emisión de paquetes RTP, para que éste sea escalable en cuanto al número de participantes.

RTCP debe ser utilizado por todos los participantes de una sesión RTP, enviando cada uno de ellos paquetes RTCP periódicamente.

Se debe dejar una pequeña parte (5 %) del ancho de banda asignado a RTP para RTCP, y se reparte entre todos los participantes.



### SEÑALIZACIÓN Y CONTROL DE LLAMADA H.323 y SIP

Por las propias características de las redes IP, que no asignan recursos en exclusividad para cada comunicación, sino que existe una compartición máxima de los mismos, se hace necesario que los sistemas de VoIP requieran señalizar, con los protocolos adecuados, todo el control de la comunicación, por ejemplo:

◼ Negociar el tipo de codificador a utilizar

◼ Negociar los parámetros de empaquetado de la voz (y vídeo)

◼ Negociar la calidad de servicio con la red (demoras, pérdida de paquetes)

◼ Intercambiar N° de Puertos por los que se llevará a cabo la comunicación.

La señalización de VoIP y demás medios sobre IP debe garantizar los servicios clásicos que brindan las redes telefónicas, sumar la potencialidad que presentan las redes IP para la integración de servicios de voz, datos y vídeo.

También debe dar solución a la problemática particular de manejar tráfico con requerimientos de tiempo real sin que la QoS se deteriore más allá de lo admisible.

El flujo de la información de usuario y el flujo de señalización siguen trayectorias diferentes en su paso por las redes IP

En la señalización intervienen elementos funcionales que no intervienen en el manejo de los paquetes de la información del usuario.

La voz (información de usuario) y la señalización no presentan los mismos requerimientos de transporte por la red, la voz tiene que ser tratada con demora y jitter mínimos, pues pierde “valor” con el tiempo, dados sus requerimientos de tiempo real. La señalización carece de requerimientos de tiempo real.

Los “momentos” de la señalización no tienen coincidencia total con los “momentos” de la conversación, en lo fundamental la señalización precede y sucede a la conversación.

Según el caso también puede coincidir en el tiempo con ésta, es decir, que durante el trasiego por la red de paquetes de voz también se transfieran paquetes de señalización de una comunicación ya establecida.

El tráfico de información de usuario (voz, etc.) es tratado por la red IP de manera diferente a como lo hace con el tráfico de señalización.

Los protocolos de señalización son los que se usan para garantizar el establecimiento, mantenimiento, modificación y terminación de llamadas de voz sobre las redes IP: señalización de control de llamadas.

También intervienen en la QoS, seguridad y control de medios.

Se han desarrollado diferentes soluciones para la problemática de la señalización de control de llamada en sistemas de VoIP:

◼ Modelo H.323 (solución UIT)

◼ Modelo SIP (solución IETF)

◼ Modelo MEGACO (H.248)

Son tres soluciones diferentes a la misma problemática, la señalización de control de llamada para el servicio de VoIP, cada una con una arquitectura funcional y protocolos que las caracterizan.

### PROTOCOLO DE SEÑALIZACIÓN H.323

H.323 es el protocolo internacional para conferencia sobre redes de paquetes que ha sido aprobado por la UIT en 1996. Esto garantiza la Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con ISDN y PSTN.

H.323 se define como el estándar que permite que el tráfico multimedia en tiempo real sea intercambiado sobre una red de paquetes, por ejemplo, la red IP. También define una serie de entidades en una red cada una de ellas con una serie de funcionalidades.

H.323 incluye las siguientes recomendaciones:

◼ H.225.0: paquetización, sincronización, señalización (Contiene el protocolo RAS)

◼ H.245 : control de canal

◼ H.261 y H.263: codificación de vídeo

◼ G.711, G.722, G.723.1, G.728, G.729: codificación de audio

◼ T.120: conferencias de datos en tiempo real, punto a punto y multipunto.

COMPONENTES H.323. H.323 define los siguientes componentes: Terminal, Gateway, Gatekeeper, Unidad de Control Multipunto, etc.

Gateways: son los sistemas encargados de permitir que los equipos H.323 puedan operar con otras redes.

Las pasarelas (Gateways) sirven de “puente” entre redes H.323 y otras redes, por ejemplo, con las redes de conmutación de circuitos de telefonía.

Desarrollan la “traducción” de la señalización, y la formación del control e información de usuario, según requerimientos de las redes que interconecta, posibilitando así la interoperabilidad entre redes, terminales y servicios, haciendo viable la integración de servicios aún con plataformas dispares (p.e., PSTN y redes IP).

Los Gateways cursan información de usuario, soportada ésta en RTP/UDP/IP.

Los Gateways, “vistos” desde cada una de las redes que interconecta, se comportan como un elemento más de las mismas, es decir, vista desde la red telefónica se comporta como una central de conmutación más de ésta, y vista desde una red IP como un nodo más de ésta.

Los Gateways son elementos funcionales opcional en entornos H.323, sólo son necesarios cuando se requiere interconexión entre entornos H.323 y entornos no H.323.

Así tenemos:

◼ Gateways H.320, para redes N-ISDN

◼ Gateways H.321, para redes B-ISDN

◼ Gateways H.322, para redes LAN con calidad de servicio

◼ Gateways H.324, para redes GSTN e inalámbricas

Y realizan funciones como la Traducción de formatos de transmisión, traducción de procedimientos de comunicación, transcodificación de audio y video y el establecimiento y liberación de llamadas.

Gatekeepers: Dentro de su zona LAN actúa de monitor de la red, proporcionando los servicios de resolución de direcciones (por ejemplo, asignación de la dirección IP a su alias, ya sea número telefónico o nombre) y de conceder permisos de llamadas.

Son entidades de control y señalización y constituyen los elementos funcionales más complejos en el marco H.323.

Proveen aquellos servicios que no pueden ser descentralizados e implementados en los “endpoints” (terminales, pasarelas, MCU´s).

Las funciones que lleva a cabo un gatekeeper se clasifican en funciones básicas y opcionales.

Entre las funciones básicas encontramos:

◼ Traducción de direcciones.

◼ Control de admisión.

◼ Control del ancho de banda.

◼ Gestión de Zona H.323.

Traducción de direcciones: Entre direcciones de transporte y alias de direcciones

Control de admisión: controla el acceso sobre la base de diferentes criterios, p.e., autorización, ancho de banda, etc. Puede no existir, esto es, se admiten todas las solicitudes de acceso

Control del ancho de banda: puede basarse en la gestión del ancho de banda. Puede no estar presente, admitiéndose todas las solicitudes de ancho de banda

Gestión de Zona H.323: se refiere a las funciones anteriores para los terminales, Gateways y MCU´s registrados en su zona de control.

**Como funciones opcionales tendremos:**

Señalización de control de llamada: en conferencias punto a punto el GK puede procesar mensajes Q.931

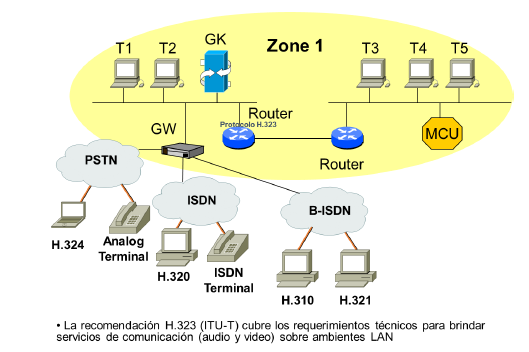
Autorización de llamadas: sobre la base de la especificación Q.931 el GK puede rechazar llamadas, p.e., acceso restringido a y desde determinados terminales o Gateways, restringir el acceso durante ciertos periodos de tiempo, etc.

Gestión de ancho de banda: el GK puede rechazar llamadas si el ancho de banda que éstas solicitan no está disponible, bien en nuevas llamadas o en llamadas en curso que soliciten ancho de banda adicional.

Gestión de llamadas: el GK puede, mediante una tabla propia, disponer del estado de las llamadas H.323, pudiendo saber el estado de un terminal dado y el “gasto” de ancho de banda asociado a las llamadas en curso, y proceder en consecuencia respecto a las nuevas solicitudes.

Terminales: son los dispositivos que se pueden conectar directamente a IP y soportan H.323

MCUs: (Multipoint Control Unit): es el sistema encargado del control de las conferencias múltiples, proporciona todos los servicios para establecer comunicaciones multipunto.



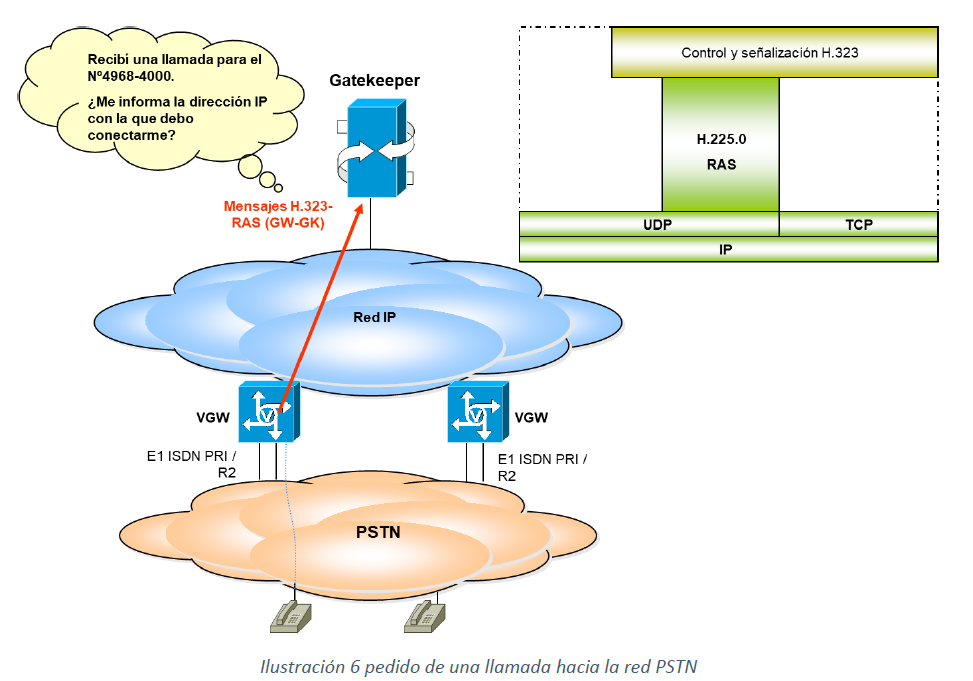
### EL ESTABLECIMIENTO DE LLAMADAS EN H.323.

El establecimiento de la llamada se lleva a cabo en tres fases.

◼ Fase RAS: intercambio de mensajes entre gatekeeper y endpoint, para traducción de direcciones, autorización (o rechazo) de llamadas y gestión de ancho de banda.

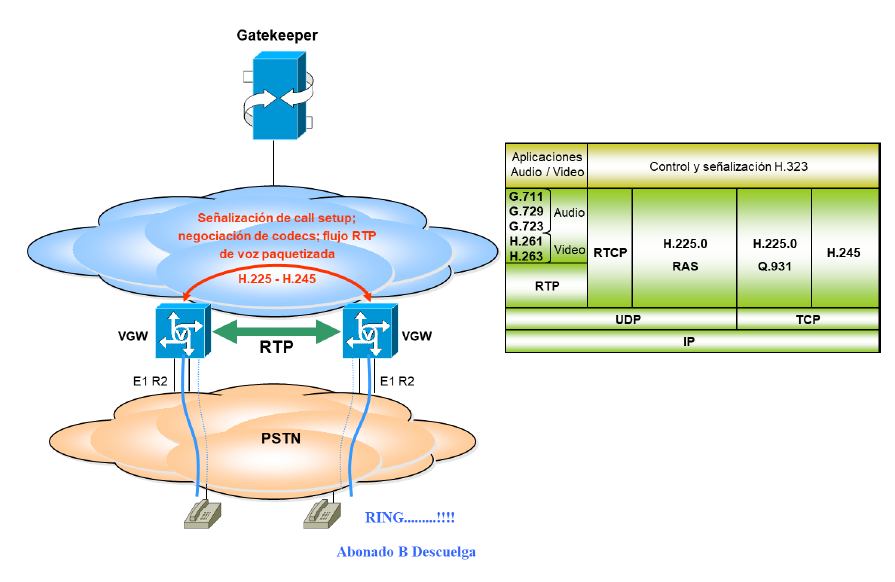
◼ Fase Q.931: intercambio de mensajes entre endpoints para el establecimiento de conexiones lógicas

◼ Fase H.245: intercambio de mensajes entre endpoints para “acordar” el intercambio de información de usuario.

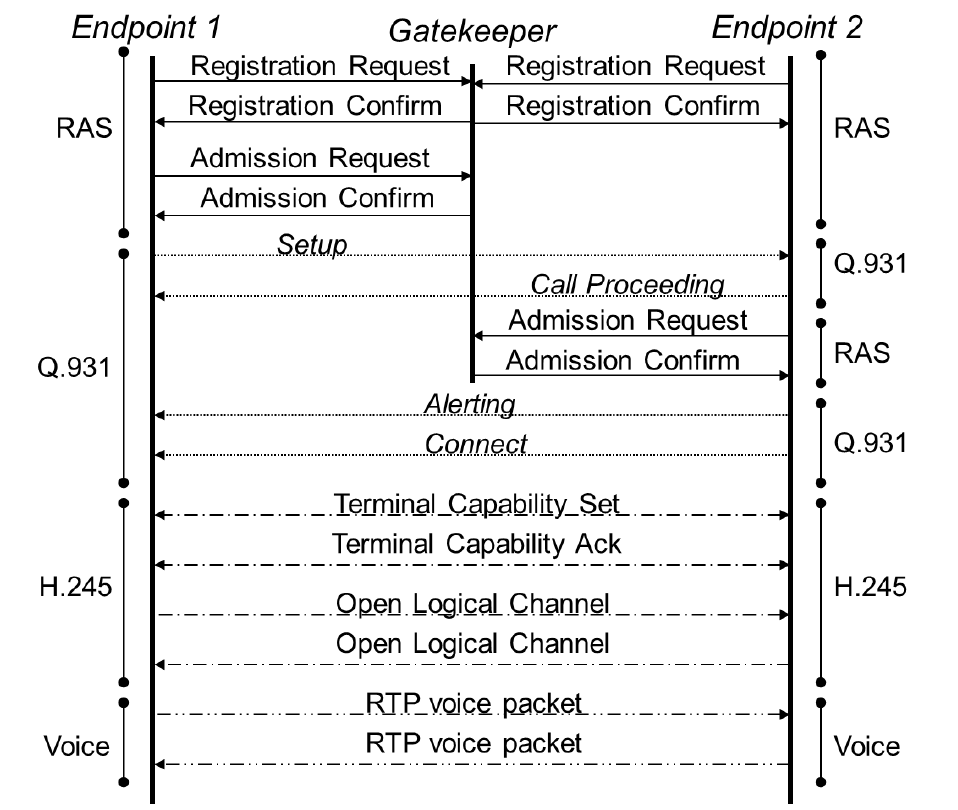


A continuación, el gatekeeper verifica las listas de numeración y la tabla de enrutamiento IP y le indica a que IP debe conectarse para establecer la llamada.

El destino solicita permiso al gatekeeper para establecer la llamada y al autorizar se produce el enlace con la red PSTN.



En la siguiente ilustración pueden verse los mensajes entre los componentes de H.323.



### PROTOCOLO DE SEÑALIZACIÓN SIP

(Session Initiation Protocol) es un protocolo de control del nivel de aplicación que maneja la señalización y el control de llamadas.

Controla el establecimiento, modificación y terminación de sesiones o llamadas multimedia, directa o indirectamente.

SIP se cataloga como un protocolo de señalización y forma parte de las especificaciones del IETF para comunicaciones multimedia, juntamente con otros protocolos como RSVP, RTP, RTSP, SAP, SDP, pero su funcionalidad no depende de ninguno de éstos.

Soporta comunicaciones entre usuarios pertenecientes a redes IP, como también con usuarios de las redes telefónicas por intermedio de pasarelas (gateways).

Debemos notar que es neutral en relación con los protocolos de las capas inferiores, por lo que puede soportarse sobre TCP o UDP, igualmente sobre IP, IPX, ATM AAL5, F-R o X.25.

Provee por sí mismo sus propios mecanismos de seguridad.

Por otra parte, SIP es un protocolo basado en texto, emplea el juego de caracteres ISO 10646 con codificación UTF-8 (RFC 2279), lo que posibilita una fácil implementación y depuración, lo hace flexible y extensible.

El sobre encabezamiento que implica usar un protocolo basado en texto no tiene aquí mayores trascendencias, pues SIP es un protocolo de señalización, no es un protocolo para transmisión de datos de usuario donde sí tendría consecuencias su orientación a texto.

Los elementos funcionales de SIP son:

◼ Agentes de Usuario (User Agent, UA),

◼ Servidores de Red.

◼ Agentes de Usuario Clientes (User Agent Client, UAC)

◼ Agentes de Usuario Servidores (User Agent Server, UAS).

Los UAC originan las solicitudes SIP (asociados al extremo que origina la llamada).

Los UAS responden a estas solicitudes, es decir, originan respuestas SIP (asociados al extremo que recibe la llamada).

Los UAC y UAS por sí solos son capaces, sin los servidores de red, de soportar una comunicación básica (modelo de llamada básico, directamente entre endpoints).

La potencialidad del Modelo SIP se aprovecha con el empleo de los Servidores de Red (modelo de llamada con servidores proxy y modelo de llamada con servidores de redirección).

Los UA deben implementar el transporte tanto sobre TCP como sobre UDP.

Los Servidores de Red se pueden clasificar de la siguiente manera:

◼ Servidores de Redirección

◼ Servidores Proxy

◼ Servidores de Registro

### SERVIDORES DE REDIRECCIÓN.

◼ Redireccionan las solicitudes de llamadas (mensajes INVITE), que son solicitudes SIP

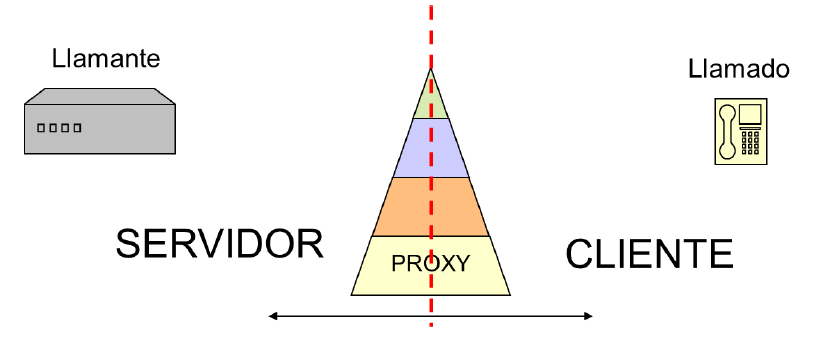
◼ Retorna la dirección (o direcciones) de la parte llamada, (SIP-URL), o cómo contactar con ella (respuesta 3xx).

◼ Rechazan la llamada error de cliente, enviando una (respuesta 4xx)

◼ Rechazan la llamada error de servidor, enviando una (respuesta 5xx)

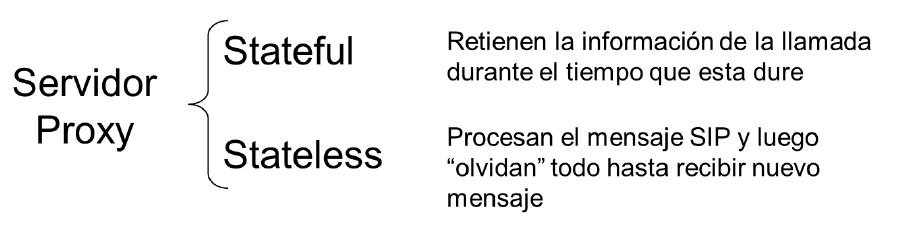
### SERVIDORES PROXY.

Corren un programa “intermediario” que actúa como servidor y como cliente. Respecto al llamante se comporta como servidor y, al llamado como cliente.



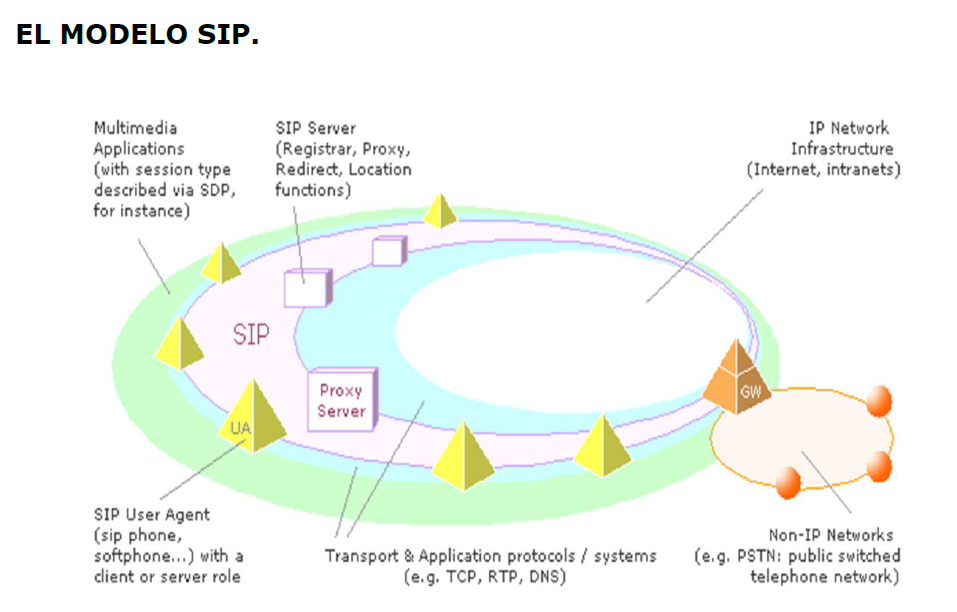
Un servidor proxy puede enviar solicitudes hasta el destino final sin efectuar cambio alguno en ellas.

Puede cambiar alguno de sus parámetros si se requiere y desarrollan el ruteo de las solicitudes y respuestas SIP.



### SERVIDORES DE REGISTRO.

Registran las direcciones SIP (SIP-URL) y las direcciones IP asociadas. Garantizan el “mapping” entre direcciones SIP y direcciones IP. Son servidores que sólo aceptan solicitudes REGISTER, posibilitando el registro correspondiente a la localización actual de los usuarios. Se les denomina servidores de localización, pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada. Deben implementar el transporte sobre TCP y UDP.



El protocolo SIP intercambia mensajes SIP (solicitudes y respuestas) a través de transacciones entre los entes funcionales (Agentes de Usuario y Servidores de Red).

Estos mensajes emplean el formato de mensaje definido en la RFC 822.

Los métodos SIP, esto es, mensajes de solicitud, son:

◼ INVITE

◼ ACK

◼ OPTIONS

◼ BYE

◼ CANCEL

◼ REGISTER

INVITE: invita a un usuario o servicio a participar en una sesión. El cuerpo del mensaje contiene una descripción de la sesión.

ACK: confirma que el cliente llamador ha recibido una respuesta final desde un servidor a una solicitud, p.e. a la solicitud INVITE, reconociendo la respuesta como adecuada.

OPTIONS: posibilita descubrir las capacidades del receptor.

BYE: finaliza una llamada o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.

CANCEL: cancela una solicitud pendiente, pero no afecta una solicitud completada. Este método finaliza una solicitud de llamada incompleta.

REGISTER: se utiliza este método como un servicio de localización que registra la localización actual de un usuario. También es necesario cuando hay varios servidores SIP en un mismo host, en cuyo caso solo uno de los servidores puede usar el número de puerto por defecto. Un servidor SIP que es capaz de aceptar mensajes REGISTER se denomina as register.

Las posibles respuestas a estas solicitudes son códigos de tres enteros, e indican el resultado de comprender y satisfacer una solicitud.

◼ 1xx: Informativo. Solicitud recibida, que continúa para procesar la solicitud. Por ejemplo, 180 RINGING,

◼ 2xx: Sucesos. La acción fue recibida de forma adecuada, comprendida y aceptada. Ej: 200 OK,

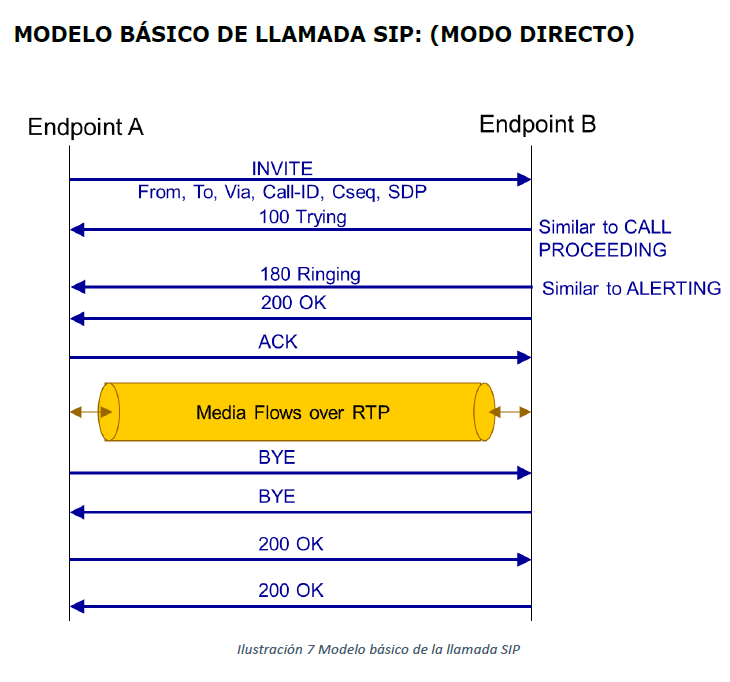
Redes administrativas – Unidad 7 Redes de próxima generación pág. 34

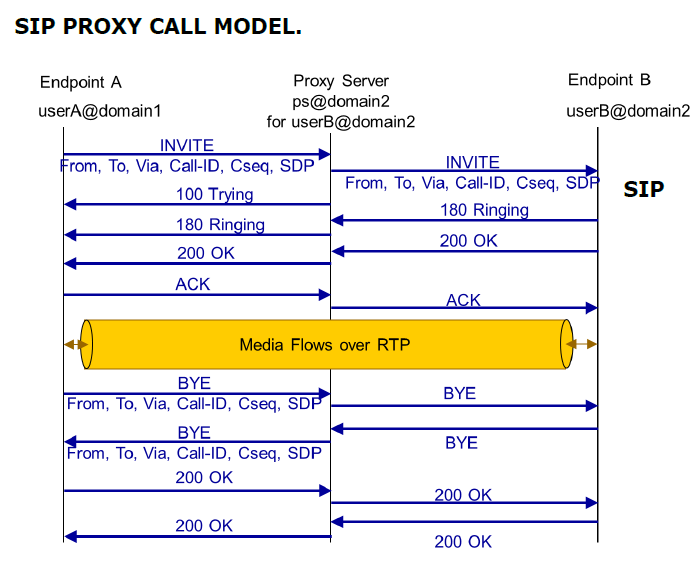
◼ 3xx: Redireccionado. Más acciones deben ser consideradas para completar la solicitud. Ej: 302 MOVED TEMPORARILY,

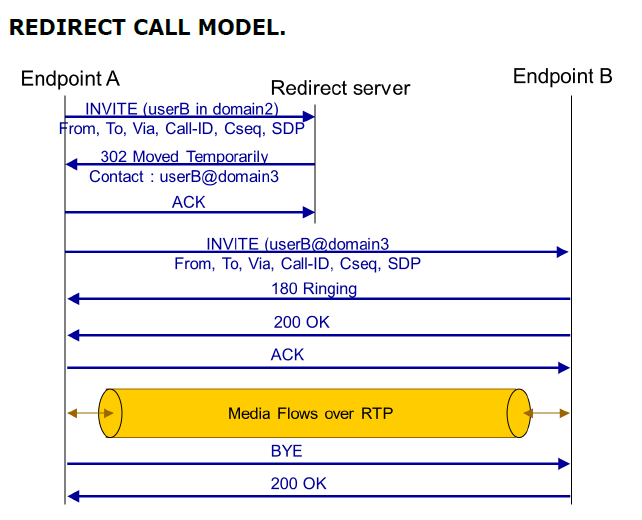
◼ 4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. Ej: 404 NOT FOUND,

◼ 5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. Ej: 501 NOT IMPLEMENTED,

◼ 6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. Ej: 600 BUSY EVERYWHERE.







# Bibliografía consultada