ESTUDIO DE LOS ESTANDARES SIP Y H.323 COMO RESPALDO A LA TECNOLOGÍA EMERGENTE DE VOZ SOBRE IP (VoIP)

CARLOS ALBERTO PIMENTEL NAVARRO

LUIS CARLOS GUZMAN BARRIOS

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2003

ESTUDIO DE LOS ESTANDARES SIP Y H.323 COMO RESPALDO A LA TECNOLOGÍA EMERGENTE DE VOZ SOBRE IP (VoIP)

CARLOS ALBERTO PIMENTEL NAVARRO

LUIS CARLOS GUZMAN BARRIOS

Monografía, presentada como requisito de aprobación del Minor en Comunicaciones y Redes

Director

GONZALO LOPEZ

Ingeniero Electrónico

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2003

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena, 23 de mayo del 2003

Le doy gracias a Dios por haber dado vida y salud para lograr una de mis metas en este largo camino.

Le agradezco a mi familia en especial a las dos personas que se preocuparon por darme una formación, mi madre LEOPOLDINA NAVARRO que me apoyo como toda madre le brinda apoyo a sus hijos en los momentos buenos y en los momentos difíciles, a mi padre RAMIRO PIMENTEL por enseñarme los valores para surgir en la vida, por que me brindo la oportunidad de estudiar a pesar de los sacrificios que pudo tener.

A Glenda Hernández por ser tan especial, por comprenderme y brindarme ese apoyo sentimental que en la vida es muy importante, a mis hermanos en especial a Ramiro J. Pimentel C., compañeros, amigos y docentes por que fueron ellos los que estuvieron presente en este logro de mi vida.

Carlos Alberto Pimentel Navarro

Gracias a DIOS, por brindarme la fortaleza para superar y enfrentar en la vida, todos los momentos buenos y todos aquellos que quisiera olvidar, así como por toda esa cantidad de personas que siempre se han preocupado por mí.

Gracias a mi familia, por todo su respaldo y apoyo, en especial a tres personas, Mi madre CARMEN A. DE GUZMÁN, por su constante apoyo y paciencia, por su generosidad y preocupación, por ese rostro de satisfacción y de orgullo que siempre comparte conmigo. GILMA C. GUZMÁN por todo su apoyo, preocupación y por su interés en ofrecerme siempre las mejores cosas. Mi padre LUIS E. GUZMÁN, por ser una persona vital en mi vida, por su apoyo y respaldo, por la oportunidad que me brindo de estudiar a pesar de todos los sacrificios y por sentirse tan orgulloso de su hijo así como yo me siento de él.

A mi madre LUZ MARINA BARRIOS A. aunque DIOS no nos brindo la oportunidad de pasar más tiempo juntos, sé que siempre te has sentido y te sentirás orgullosa de mí, sé que en mi corazón siempre estás presente y que siempre has estado junto a mí, en cada momento de mi vida, por estas razones y muchas otras más te dedico este logro, uno de los mas importantes de mi vida hasta el momento.

A CLAUDA M. PALENCIA por su paciencia, por brindarme su amor sin reserva y por tener ese algo que la hace un ser excepcional,

A mis hermanos en especial ANDRES FELIPE y a todas las personas que dentro del ambiente universitario me apoyaron y me ofrecieron su ayuda sin esperar nada a cambio, en especial a mi tío JOSÉ I. BARRIOS A.

Luis Carlos Guzmán Barrios

.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACRONIMOS.

ACF *Admissions Confirm Message* (Mensaje de Confirmación de Acceso)**; H.323**

ACK *Acknowledgement* (Acuse de Recibo)

ADPCM *Adaptive Differential Pulse Code Modulation* (Modulación por pulsos codificados diferencial y adaptable)

ARJ *Admissions Reject Message* (Mensaje de Rechazo de Acceso)**; H.323**

ARQ *Admissions Request Message* (Mensaje de Petición de Acceso)**; H.323**

ANR *Automatic Noise Reduction* (Reducción Automática de Ruido)

ATM *Asynchronous Transfer Mode* (Modo de Transferencia Asíncrona)

AVP *Audio/vides Profile (Perfil de Audio/video);* **SIP - RFC 1890**

B-ISDN *Broadband Integrated Services Digital Networks* (Red Digital de Servicios Integrados de Banda Ancha)

CS-ACELP *Conjugate Structure Algebraic Codebook Excited Linear Prediction* (Predicción Lineal con excitación por código algebraico de Estructura Conjugada)**; H.323 – G.729**

DCF *Disengage Confirmation* (Confirmación de Desconexión)**; H.323**

DiffServ *Differentiated Services Internet QoS model* (modelo de Calidad de servicio en Internet basado en Servicios Diferenciados)

DRQ *Disengage Request* (Petición de Desconexión)**; H.323**

DNS *Domain Name System* (Sistema de Nombres de Dominio)

E.164 Recomendación de la ITU-T para la numeración telefónica internacional, especialmente para ISDN, BISDN y SMDS.

ENUM *Telephone Number Mapping* (Integración de Números de Teléfono en DNS)**; H.323**

GCF *Gatekeeper Confirm* (Confirmación de Gatekeeper); **H.323**

GRJ *Gatekeeper Reject* (Rechazo de Gatekeeper); **H.323**

GRQ *Gatekeeper Request* (Petición de Gatekeeper); **H.323**

H.323 Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real en redes de área local, LAN, e Internet; **H.323**

HTTP *Hypertex Transfer Protocol* (Protocolo de Transferencia de Hipertexto)

IETF *Internet Engineering Task Force* (Grupo de Trabajo de Ingeniería de Internet)

IGMP *Internet Group Management Protocol* (Protocolo de Gestión de Grupos en Internet)

IntServ *Integrated Services Internet QoS model* (modelo de Calidad de Servicio en Servicios Integrados de Internet)

IP *Internet Protocol* (Protocolo Internet)

IPBX *Internet Protocol Private Branch Exchange* (Central Privada basada en IP)

IPSec *IP Security* (Protocolo de Seguridad IP)

IPX *Internet Packet Exchange* (Intercambio de Paquetes Entre Redes)

ISDN *Integrated Services Digital Network* (Red Digital de Servicios Integrados, RDSI)

IVR *interactive voice response* (Respuesta de Voz Interactiva)**; H323**

ITU-T *International Telecommunications Union -Telecommunications* (Unión Internacional de Telecomunicaciones- Telecomunicaciones)

LD-CELP *Low Delay Codebook Excited Linear Prediction* (Predicción Lineal con Excitación por Código Bajo Retardo)**; H.323 – G.728**

MC *Multipoint Controller* (Controlador Multipunto); **H.323**

MCU *Multipoint Control Unit* (Unidad de Control Multipunto); **H.323**

MOS *Mean Opinion Score* (Media de Resultados de Opinión)

MP *Multipoint Processor* (Procesadores Multipuntos)**; H.323**

MPLS *Multiprotocol Label Switching* (Conmutación de Etiquetas Multiprotocolo)

PBX *Private Branch Exchange* (Central Telefónica Privada)

PCM *Pulse Code Modulation* (Modulación por Código de Pulso)

PPP *Point to Point Protocol* (Protocolo Punto a Punto)**; TCP/IP**

PSTN *Public Switched Telephone Network* (Red de Telefonía Conmutada Pública)

QoS *Quality of Service* (Calidad de Servicio)

RAS *Registration, Admission and Status* (Registro, acceso y Estado); **H.323**

RCF *Registration Confirmation* (Confirmación de Registro); **H.323**

RRJ *Registration Reject* (Rechazo de Registro); **H.323**

RRQ *Request Registration* (Petición de Registro); **H.323**

RSVP *Resource Reservation Protocol* (Protocolo de Reserva)

RTCP *Real Time Control Protocol* (Protocolo de Control en Tiempo Real)

RTP *Real Time Transfer Protocol* (Protocolo de Transferencia en Tiempo Real)

RTSP *Real Time Streaming Protocol* (Protocolo de Flujo en Tiempo Real)

RTT *Round Trip Time* (Tiempo de ida y vuelta)

SAP *Session Annunciation Protocol* (Protocolo de Anuncio de Sesión)

SB-ADPCM *Sub-Band Adaptive Differential Pulse Code Modulation* (Modulación por pulsos codificados diferencial adaptable de banda baja) **; H.323 – G.722**

SCN *Switched Circuit Network* (Red de Circuitos Conmutados)

SDP *Session Description Protocol* (Protocolo de Descripción de Sesión)

SIP *Session Initiation Protocol* (Protocolo de Inicio de Sesión)

SNMP *Signaling Network Management Protocol* (Protocolo de administración de red)**; H.323**

SS7 *Signalling System Number 7* (Sistemas de Señalización número 7)

STMR *Side Tone Masking Rating* (Índice de Enmascaramiento para el Efecto Local)

TCP *Transmission Control Protocol* (Protocolo de Control deTransmisión)**; TCP/IP**

UA *User Agent* (el Agente de Usuario); **SIP**

UAC *User Agent Client* (Cliente de Agente de Usuario); **SIP**

UAS *User Agent Server* (Servidor de Agente de Usuario)**; SIP**

UCF *Unregister confirmation* (Confirmación de Cancelación de registro); **H.323**

UDP *User Datagram Protocol* (Protocolo de Datagramas de Usuario)**; TCP/IP**

URI *Uniform Resource Identifier* (Identificador Unificado de Recursos)**; SIP**

URJ *Unregister Reject* (Rechazo de Cancelación de Registro); **H.323**

URL *Uniform Resource Locators* (Localizador Unificado de Recursos)**; SIP**

URQ *Unregister Request* (Petición de Cancelación de Registro); **H.323**

TÉRMINOS.

Checksum. Esquema simple de detección de errores, donde cada mensaje transmitido es acompañado por un valor numérico basado en el número de grupo de bits del mensaje; **TCP/UDP**

Circuit Switching (conmutación de circuitos). Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación de circuitos más representativa es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, «ranuras»de tiempo o frecuencias) dedicados para cada llamada telefónica.

Codec (codec). Algoritmo software usado para comprimir/descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (*frame*), los retardos de proceso, etc. Algunos ejemplos de *codecs* típicos son G.711, G.723.1, G.729 o G.726.

DIV 14 Codec utilizado para el tratamiento de las señales de video. **; SIP**

Gatekeeper Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, Gateways y MCUs H.323. Puede proporcionar otros servicios de valor agregado a la red. **; H.323**

Gateway Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. **; H.323 - SIP**

GSM. Codec utilizado para pasar una señal analógica a digital, El codec GSM elimina la redundancia inherente a la señal de voz. Tiene una calidad de servicio aceptable. Reconoce los lapsos de silencio para no enviarlos. **; SIP**

Intranet (intranet). Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

Jitter (variación de retardo). Es un término que se refiere al nivel de variación de retado que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio o video, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos ininteligibles.

OSPF (Abrir la ruta más corta primero). Algoritmo de estado de enlace de enrutamiento IGP jerárquico propuesto como sucesor del RIP en la comunidad de la Internet. Entre las características de OSPF se incluyen enrutamiento más económico, enrutamiento multiruta y equilibrio de carga.

Packet Switching (conmutación de paquetes). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

Proxy Server (Servidor *Proxy*). Es el único punto de contacto del UA para los mensajes de señalización, recibe peticiones de los clientes y los dirige a otros servidores o al cliente destino. **; SIP**

Redirect Server (Servidor de Redireccionamiento). Acepta peticiones SIP y da a conocer la dirección del UA llamado, no interviniendo más en la sesión. **; SIP**

Router (encaminador, enrutador). Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Es el nodo básico de una red IP.

Softswitch (conmutación por software). Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.

T.120 Es un conjunto independiente de estándares de redes, que proporcionan una interfase general de distribución de datos a los diseñadores de

aplicaciones. Esta especificación soporta transferencias confiables de datos punto a punto y multipunto. T.120 se incorpora en los UA, terminales y MCU, en SIP y H.323 respectivamente.¸ **H.323 - SIP**

URL, URI (Localizador Unificado de Recursos, identificador unificado de Recursos). URL, Es el mecanismo con el cual el World Wide Web asigna una dirección única a cada uno de los recursos de información de cualquier lugar de Internet. El URL de un recurso de información es su dirección en Internet, la que permite que el navegador la encuentre y la muestre de forma adecuada. Mientras que el URI es un texto corto que identifica cualquier recurso (servicio, página, documento, dirección de correo electrónico, enciclopedia...) accesible en una red. **; SIP**

VoIP*, Voice over IP* (Voz sobre IP). Método de envío de voz por redes de conmutación de paquetes utilizando TCP/IP, tales como Internet.

RESUMEN

La Voz Sobre IP es una tecnología emergente para las comunicaciones de voz sobre redes basadas en conmutación de paquetes, Como su nombre lo indica la tecnología de red de paquete sobre la que trabaja es la red IP, que tiene un gran fortaleza, la Internet esta basada en esta tecnología, por lo que ya se encuentra una plataforma lo suficientemente amplia para las aplicaciones de comunicaciones de voz.

El respaldo a esta tecnología esta definido por diversos protocolos entre los cuales se destacan como máximos exponentes H.323 y SIP, que son los protocolos representativos de VoIP.

ESTANDAR H.323

Este estándar es la piedra angular para las tecnologías de transmisión de audio, video y comunicaciones de datos sobre redes de paquetes en tiempo real. Por medio de este estándar se especifican los componentes, protocolos y procedimientos necesarios para proveer un sistema de comunicaciones multimedia en redes de paquetes.

El estándar H.323 especifica cuatro clases de componentes: terminales, los Gateways, Gatekeeper y las MCU.

SIP

SIP es un protocolo de señalización de llamadas basado en texto. Está diseñado teniendo en cuenta protocolos textuales, tales como SMTP y HTTP, con codificación normalizada flexible y extensible. Comparte elementos comunes a Internet, como los nombres DNS y direcciones de correo electrónico. Utiliza, como en HTTP, el modelo “petición-respuesta” en la iniciación de una llamada.

Las entidades principales en SIP son el Agente de Usuario (AU), o terminal y el Servidor SIP que puede ser de dos tipos posibles: Servidor *Proxy* y el Servidor de Redireccionamiento.

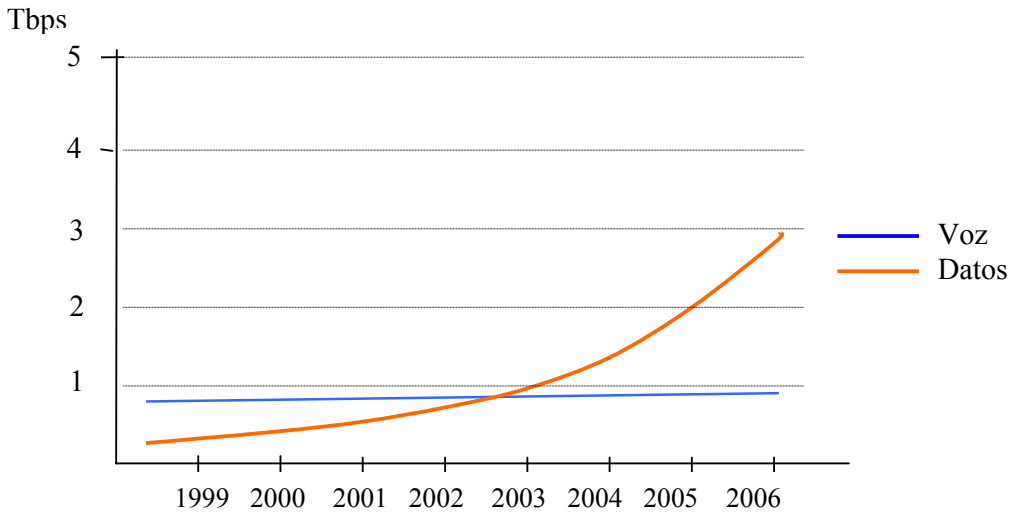
INTRODUCCION

Nuestro sistema telefónico actual, la red telefónica publica conmutada (PSTN), a pesar de lo que muchas personas tienden a creer, no se ha sometido a cambios radicales desde la época de los ochenta, es decir, se ha quedado rezagada en relación a los avances tecnológicos en el campo de las telecomunicaciones, con respecto a otras aplicaciones, como lo son las redes de datos; que a diferencia de la red telefónica conmutada ha experimentado fuertes y drásticos cambios que la han llevado a un desarrollo de grandes proporciones en muy pocos años. Esto se debe en gran parte al manejo efectivo que este tipo de redes le dan al ancho de banda (por ejemplo para la transmisión de voz en estas redes se suprimen los tiempos de silencio) y Como consecuencia de este desarrollo se ha obtenido una de las aplicaciones de las que se destaca como el avance más importante y significativo de este campo en el siglo XX, las redes IP, que se han desarrollado de tal manera que son la base de Internet, es una relación tan estrecha que se puede afirmar que hablar de Internet es hablar de una red IP. En la actualidad, Es tal la importancia de la Internet que es uno de los fenómenos que capta mayor interés dentro del mundo de las telecomunicaciones, y prueba de ello es el crecimiento experimentado en el número de usuarios que utilizan y están por utilizar este servicio.

Las predicciones mas generales, respecto a este tema no se han hecho esperar y apuntan a un crecimiento del 90% en el trafico de datos, que si se compara con las predicciones del aumento de la telefonía (fija), se observa la diferencia de forma inmediata, no se apunta a que esta crezca más del 5%. (Ver Figura 1)

Todos estos adelantos en las redes de datos y sobretodo en las redes IP, se pueden empezar a aplicar a las comunicaciones de voz y es en este momento donde aparece el concepto de Voz sobre IP (VoIP), como tecnología emergente para el soporte de las comunicaciones de voz.

Figura1. Crecimiento del Tráfico Voz –Datos



Fuente: A.D.Little

La Voz sobre IP (VoIP), es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permite la realización de

llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, *gateway's* y teléfonos estándares, entre otros dispositivos. En general, servicios de comunicación de voz, fax, aplicaciones de mensajes de voz son transportados vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

La VoIP, como una solución a los servicios de telecomunicaciones es atractiva en la manera que ofrezca ventajas sobre su competencia, la PSTN, y en realidad esto es lo que esta ofreciendo, por ejemplo y solo por destacar dos de ellas que en el orden de prioridades están en los primeros lugares, se tiene que la VoIP brinda:

- Integración de servicios y unificación de estructura. Integración de la voz como un servicio mas de la red, lo que tiene como consecuencia el manejo de una sola red integrada de voz y datos (multimedia).
- Ahorro de costos de comunicaciones. Un ejemplo sencillo una llamada de larga distancia no costaría mas que una llamada local, ya que esta viaja por una red IP (Internet normalmente) y no se tiene que pagar mas de lo que se paga a un ISP por brindar este servicio.

Pero para llegar a brindar este servicio con la calidad que se exige por parte del usuario final, fue necesario desarrollar estándares que permitan cumplir con esta cualidad (QoS), y es en este momento donde la VoIP, se empieza a observar como una tecnología emergente garantizada y con un gran respaldo tecnológico, demostrado en sus estándares como el H.323 y el protocolo SIP que se han destacado entre otros por su funcionalidad y acogida.

1. VOZ SOBRE PAQUETES

1.1 FUNDAMENTOS DE REDES IP

Las redes de conmutación de paquetes y en particular las redes IP constituyen, por su despliegue y funcionalidad, un objetivo interesante y de gran importancia en la evolución de las redes tradicionales de conmutación de circuitos. Aunque para lograr esta migración de forma excepcional, se debe esencialmente avanzar en características o aspectos como la capacidad de procesado, eficiencia de ancho de banda y disminución de la latencia, tanto en el establecimiento como en el flujo de la comunicación, buscando de esta forma minimizar los efectos debidos a la congestión y retardo de paquetes.

1.1.1 El conjunto TCP/IP. El conjunto de protocolos TCP/IP (Protocolo de Control de *Transmisión/Protocolo* Internet) se desarrolló como parte de la investigación realizada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA). Aunque Originalmente, se desarrolló para suministrar comunicaciones a través de DARPA, actualmente TCP/IP permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones de Lan como de WAN, por esta razón, TCP/IP es hoy

el estándar de facto para las comunicaciones de *internetwork* y sirve como el protocolo de transporte para Internet, permitiendo que millones de computadores se comuniquen a nivel mundial.

Los dos protocolos más importantes dentro de TCP/IP son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto.

La arquitectura del TCP/IP consta de cuatro niveles o capas en las que se agrupan los protocolos, manteniendo una relación muy estrecha con las capas del modelo de referencia OSI.

Figura 2. Pila de Protocolos TCP/IP

- **Capa de Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).

- **Capa de Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la confiabilidad necesaria en el transporte de los mismos.
- **Capa de Internet (Red):** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes, otros protocolos que operan en esta capa son el ICMP, ARP, RARP.
- **Capa de Acceso a red:** En esta capa TCP/IP soporta todas las funciones de las capas de enlace de datos y física del modelo OSI.

❖ En el nivel más alto se encuentran los programas de comunicaciones tales como Telnet, FTP o SMTP para entrega de correo electrónico. Se observa en la capa de trasporte los protocolos pertenecientes a este nivel, TCP y UDP que serán descritos en el ítem .1.1.1.2

❖ **IP** (*Internet Protocol*) Es el protocolo principal de la capa de red, encargado de enviar bloques de datos (datagramas) de un punto a otro de la red; para ello emplea un campo de direcciones de cuatro octetos que forman la dirección IP. Además este protocolo se encarga de la fragmentación y re-ensamblado de datagramas cuando sea necesario.

❖ Para convertir las direcciones IP en direcciones físicas (necesarias para conocer a donde enviar un mensaje) en TCP/IP se incluye el protocolo de

enlace ARP *(Address Resolution Protocol).* ARP averigua una dirección física difundiendo un mensaje de petición, al cual solamente responde de manera positiva el dispositivo (*host*) buscado que posee la dirección IP incluida en el mensaje de petición difundida. De manera similar, también se puede conocer la dirección IP correspondiente a una dirección física mediante ARP inverso (RARP).

- Otros protocolos de enlace relacionados directamente con TCP/IP son los de punto a punto y de línea serie (PPP, SLIP), que utilizan encapsulamiento de paquetes en las conexiones de red sobre líneas telefónicas vía modem.

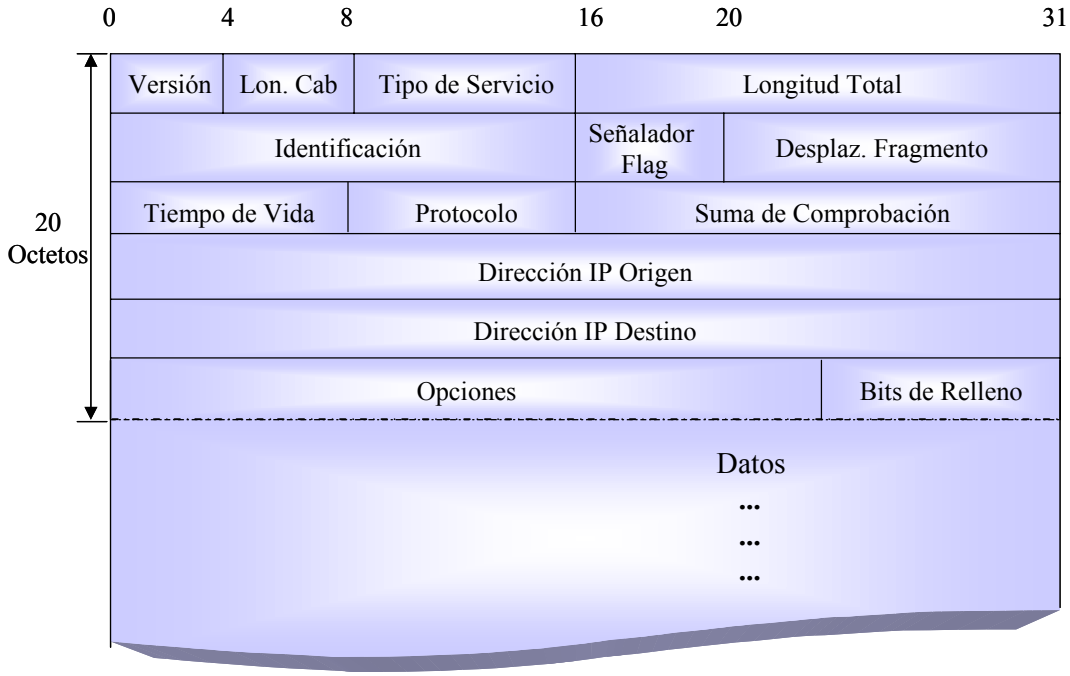
1.1.1.1 Capa de red. Encaminamiento IP. El protocolo IP está directamente relacionado con el concepto de encaminamiento de la información entre subredes, de ahí su nombre: protocolo inter-net. IP no está orientado a conexión (realiza el mejor esfuerzo), lo cual implica que el encaminamiento de los paquetes no sigue un camino preestablecido.

Desde su desarrollo original, IP ha tenido varias versiones, y aunque actualmente está aprobado IPv6, la versión más utilizada es la 4, que es la que se describe a continuación.

Un datagrama IP consiste en un mínimo de 160 bits de cabecera y un número variable de octetos para datos. La cabecera incluye los campos de número de

versión de protocolo (4 bits), longitud de cabecera, tamaño total del paquete (16 bits) y campos de control y de comprobación de errores.

Figura 3. Formato de Paquete IP



De los 20 octetos de cabecera que contiene un paquete IP, son de especial interés los campos denominados **Protocolo** y **Tiempo de Vida** (*Time To Live,* TTL). El primero indica con que protocolo de la capa superior (TCP/UDP) se comunica (recibe o envía los datos IP). El campo TTL contiene un valor inicial asignado por el origen que se decrementa en uno por cada enrutador por donde va pasando el paquete, hasta que al alcanzar el valor nulo éste es descartado. Otro campo que puede servir para discriminar clases de servicio, importante para la transmisión de voz, es el Tipo de Servicio, que incluye 3 bits de prioridad (0 = baja prioridad hasta 7 = datagrama de control de red) y otros 3

bit (D, T, R) que si se activan indican que se solicita datagrama con bajo retardo, alta capacidad y alta confiabilidad respectivamente.

Los campos de dirección son de 32 bits, tanto de origen como destino. En una red IP, un enrutador debe examinar cada datagrama para comprobar primero si el identificador de red de la dirección IP de destino está ubicada en su propia red, y en caso afirmativo lo envía al destinatario (encaminamiento directo). En otro caso se ha de comparar la dirección de destino con una tabla de direcciones que mantiene el enrutador en memoria, llamada tabla de encaminamiento IP. Si se encuentra una dirección de host en su misma red o de subred que coincide con la misma, el datagrama se envía a la dirección de la red destino o la del siguiente enrutador de acuerdo con la mencionada tabla. Si no encuentra una coincidencia, mira la parte de dirección de red por si existe coincidencia con la tabla de redes, y de nuevo intenta enviar el paquete a esa dirección (encaminamiento indirecto).

En último caso, y si no hay coincidencia, el enrutador busca una dirección por defecto para el siguiente salto. Solo en caso de que no exista dirección por defecto, éste envía un mensaje de fallo a la red. Para los mensajes de notificación de red (fallo en la ruta, paquete descartado, host inalcanzable, etc.) se emplea el protocolo de control de mensajes ICMP (Internet Control Mensaje Protocol).

La tabla de direccionamiento de un enrutador puede ser estática, o dinámica. La primera se usa en redes sencillas y generalmente se carga de un archivo al arrancar, o está en memoria semipermanente (memoria flash, EEPROM, firmware…). Sin embargo, si la tabla es dinámica como es el caso de las redes de cierta entidad, es necesario difundir un mensaje ICMP de petición de direcciones, al que deberán responder los enrutadores implicados. Mediante protocolos de encaminamiento se averiguan los caminos más cortos hacia un destino, y también se actualizan las tablas de direcciones según criterios de tráfico, velocidad, disponibilidad, etc.

1.1.1.2 TCP Y UDP. Dentro del conjunto TCP/IP, los protocolos de la capa de transporte: TCP y UDP son usados directamente para pasar datos a la capa superior, constituida por las aplicaciones de comunicaciones.

ASPECTOS COMUNES A LA CAPA DE TRANSPORTE

Los protocolos de la capa de transporte correspondientes a la pila TCP/IP tienen las siguientes funciones en común:

- Comunicación entre procesos. (Puertos)

Cada proceso de capa superior que quiera comunicarse con otro se identifica él mismo en el conjunto de protocolos TCP/IP por uno o más puertos. El puerto es un número de dos octetos, utilizado para identificar a qué protocolo o aplicación

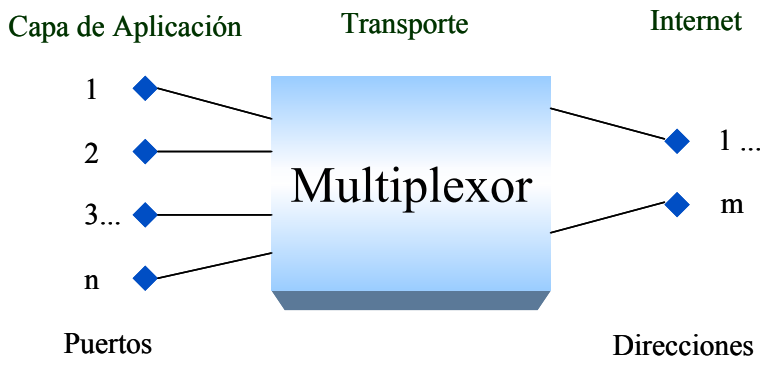
de capa superior (proceso) se deben pasar los mensajes. Existen puertos asignados de antemano por el IANA *(Internet Assigned Numbers Authority)* para aplicaciones conocidas, como Telnet (puerto 23) o SMTP (puerto 25), todas ellas en el rango de 0 a 1023. Por otro lado los programas de usuario pueden utilizar el resto de los puertos no asignados que van hasta el 65535 (limitado por el campo de 16 bits).

- Multiplexación en las capas de transporte.

Según el valor del puerto asignado, la capa de transporte pasa su contenido a la aplicación de red correspondiente. Una dirección puede comunicarse con distintos protocolos (puertos) de mayor nivel. En función de que el flujo de datos vaya de la capa superior a la inferior o viceversa, existe multiplexación (demultiplexación) 1-n.

También existe la posibilidad de multiplexación m-n, cuando un host tiene más de un adaptador de red (como en un PC router), de tal forma que existe más de una entrada de la capa inferior (dirección IP).

Figura 4. Multiplexación de Puertos



Una dirección IP con su puerto asociado identifica un servicio o aplicación que se está ejecutando en un host, y a esta combinación se le denomina *socket* o conexión TCP/IP.

UDP

El protocolo UDP *(User Datagram Protocol*) es un protocolo de nivel transporte muy simple, y básicamente añade a IP el concepto de multiplexado de puertos que se acaba de exponer. Al igual que el protocolo IP, UDP no está orientado a conexión, y por tanto no existen mecanismos de recuperación de datos (en caso de pérdidas o errores de transmisión).

La unidad de datos UDP es el datagrama. UDP añade 8 octetos a los datos que recibe de la capa de aplicación, en los que se incluye los puertos de origen/destino y los campos de tamaño (del datagrama) y suma de comprobación de errores.

Aunque UDP no es un protocolo que proporciona confiabilidad, su estructura y funcionamiento lo hacen sin embargo apropiado para aplicaciones en “tiempo real” donde la latencia es un requerimiento importante como es el caso del transporte multimedios y específicamente en VoIP. También se utiliza en comunicaciones breves o de pocos datos como las usadas en el protocolo SNMP de supervisión de redes, donde prima la sencillez frente a la fiabilidad de los datos.

Como protocolo de uso general, UDP es adecuado para la difusión de mensajes a toda la red (local) o envíos a múltiples destinos (*multicast*), ya sean de la red propia o de otras subredes.

Para controlar los mensajes de multidifusión se utiliza el protocolo IGMP *(Internet Group Management Protocol),* que informa sobre los *hosts* que quieren recibir *multicast*, es decir, comunicaciones dirigidas a un grupo.

TCP

El protocolo TCP *(Transmission Control Protocol)* es el más utilizado por las aplicaciones de Internet: HTTP, FTP, Telnet, etc. TCP está orientado a conexión, lo cual indica que un host (cliente) debe establecer una conexión con otro (servidor) antes de solicitar una transferencia de datos.

TCP se diferencia de UDP principalmente porque proporciona confiabilidad de los datos mediante funciones de control de flujo. Es decir, si el origen no recibe una confirmación de que los datos han llegado a su destino durante un periodo de tiempo, estos se envían de nuevo. Además, TCP incorpora mecanismos para reordenar los datos cuando estos llegan fuera de secuencia.

Los bloques TCP se denominan segmentos y son de longitud variable. Cada segmento contiene 20 octetos (opcionalmente hasta 60) de cabecera. La cabecera TCP contiene los puertos origen y destino, campos de control de secuencia, tamaño, indicadores de estado y una suma de comprobación. El

campo de secuenciamiento permite controlar el orden en el que llegan los segmentos de datos, y junto con el campo ACK de confirmación informan de que los datos se han recibido correctamente.

Para evitar un reconocimiento de cada segmento enviado se utiliza el campo ventana de recepción, cuyo valor indica cuantos bytes se pueden enviar antes de ser validados por el receptor. La ventana de recepción determina la máxima cantidad de información que puede ser transmitida antes de que el asentimiento sea enviado, y su objetivo es conseguir una transmisión de información continua. El receptor anuncia al transmisor el tamaño de la ventana durante el establecimiento de la conexión TCP.

Para establecer una conexión, el cliente envía una solicitud TCP al servidor, con empleo de los bits indicadores de estado, y el servidor permite la conexión enviando un segmento de forma similar. Una vez establecida, el emisor manda una serie de segmentos de datos antes de recibir un control de su recepción correcta, número determinado por el valor de la ventana.

En caso de tener que enviar cantidades reducidas de datos (por ejemplo una pulsación de tecla), existen mecanismos para agruparlos hasta que igualan el tamaño de la ventana o bien se recibe una confirmación del segmento previo recibido.

Las comunicaciones TCP están orientadas por tanto a conexión, con establecimiento y liberación de la misma y control de flujo de datos. Ello

permite fiabilidad en la comunicación (adecuado típicamente para la transmisión de archivos binarios), a costa de una mayor latencia (tiempo) y complejidad en el protocolo.

1.1.1.3 Protocolos de aplicación. Dentro de la pila de protocolos TCP/IP, en la capa de aplicación se encuentran los siguientes:

- **HTTP** es el protocolo utilizado para poder navegar por las páginas web.

- Con **FTP** (*File Transfer Protocol*) es posible la transferencia de archivos entre dos equipos conectados a Internet.

- **TELNET** nos permite acceder a un equipo remoto y crear, modificar y ejecutar archivos tal y como si estuviéramos delante del computador al que nos hemos conectado.

- **SMTP** *(Simple Mail Transfer Protocol*) también requiere transporte TCP y se encarga del envío de correo electrónico.

- **DNS** es el mecanismo que establece la correspondencia entre nombres de dominio y direcciones IP.

1.1.1.3.1 Servidores de nombres. DNS. Para dirigirse a un nodo Internet se utilizan por lo general nombres en lugar de direcciones IP numéricas, pues resulta más práctico y fácil de recordar. Un nombre completo consta de dos partes: el nombre del host y el dominio o red local al que pertenece. Mediante el protocolo DNS (*Domain Name System*), se convierte un nombre a dirección IP.

Los servidores DNS reciben las peticiones de clientes conteniendo el nombre de una máquina y resuelven su dirección IP. Los servidores de nombres pueden ser desde servidores locales tipo *proxy*, que guardan peticiones ya resueltas en memoria caché, a otros servidores de mayor nivel que contienen bases de datos, hasta llegar si es necesario al servidor maestro, que gestiona todos los nombres de un dominio como .org o .com.

Por ejemplo, para obtener la dirección IP de **www.voip.org.co**, el primer paso es dirigirse a un servidor de nombres local (red local o la del proveedor de acceso a Internet); en caso de que no resuelva la dirección, se dirige al servidor maestro que gestiona todos los dominios tipo .co, y que previamente han sido registrados en el país. Una vez resuelta la dirección de primer nivel puede ser necesario otro servidor para resolver el dominio de segundo nivel (.org) hasta llegar a la dirección de destino.

1.1.1.4 IP versión 6 (IPv6). El principal acontecimiento impulsor para convertir la versión actual del Protocolo Internet (IPv4) a la versión seis es el rápido crecimiento de la Internet. IPv6 se está introduciendo para superar las restricciones de la anterior versión, y aunque en principio pueda parecer que añade complicaciones al espacio de direccionamiento actualmente utilizado, hay que pensar que ha sido especificado pensando en las necesidades futuras de unas redes que van a transportar no solo datos sino servicios multimedios de entretenimiento y otros apenas concebidos ahora, pero que van a permitir el acceso virtualmente a cualquier dispositivo electro-mecánico que podamos imaginar. Todo ello teniendo en cuenta la interoperabilidad entre versiones IP.

Se ha previsto que habrá más transacciones en tiempo real en la Internet e intranets según se vayan transformando en redes más complejas y transportando una mayor riqueza y variedad de datos (servicios, entretenimiento, video...). Por otro lado, el número de posibles caminos entre extremos aumenta con el cuadrado del número de direcciones IP, mientras que el número de enrutadores intermedios puede aumentar a un ritmo aún mayor.

Las modificaciones en direccionamiento que serán necesarias para manejar el tráfico que comienza a aparecer en las redes IP globalmente han influido en la elección de un espacio de direccionamiento de 128 bits para la nueva versión que en principio puede parecer excesivo. Sin embargo, se ha tenido en cuenta el establecimiento de niveles jerárquicos de direccionamiento, para simplificar en gran medida las tablas de direccionamiento de los enrutadores.

En un escenario de red complejo, la necesidad de configurar automáticamente un enrutador se convierte en prioritaria si el administrador de red tiene que asignar una gran cantidad de direcciones de red propias y de su entorno, todo ello sin tener en cuenta que no siempre es factible contar con personal cualificado para estas tareas. IPv6 está diseñado con el objetivo de que un terminal pueda obtener automáticamente toda la información necesaria para conectarse a Internet, sin intervención humana directa.

1.1.1.4.1 Breve historia de IPv6. Desde 1991 ha estado estudiando el Grupo de Trabajo de Arquitecturas Internet el problema del crecimiento de usuarios y el número de direcciones que serían necesarias en el futuro. Desde entonces, los requerimientos han aumentado por las necesidades de asignación de direcciones IP a dispositivos diversos como teléfonos IP, *Gateways* e incluso para interfaces de diagnóstico de elementos mecánicos como motores de vehículos.

En 1995 se finalizó un primer documento de trabajo, RFC6 1752, conocido como "*IP NextGen*" que pretendía mejorar IP y su compatibilidad con otros protocolos (como IPX).

Después de varias deliberaciones se documentaron las primeras propuestas sobre el protocolo base y otros relacionados con su implantación.

Tabla 1. RFCs con propuestas detalladas para el despliegue de IPv6.

RFC 2460 – Especificación base IPv6. RFC 2373 – Arquitectura de direcciones IPv6. RFC 2462 – Autoconfiguración de direcciones IP. RFC 1886 – Problemas de un Servicio DNS mejorado. RFC 2893 – Mecanismos de transición para nodos IP

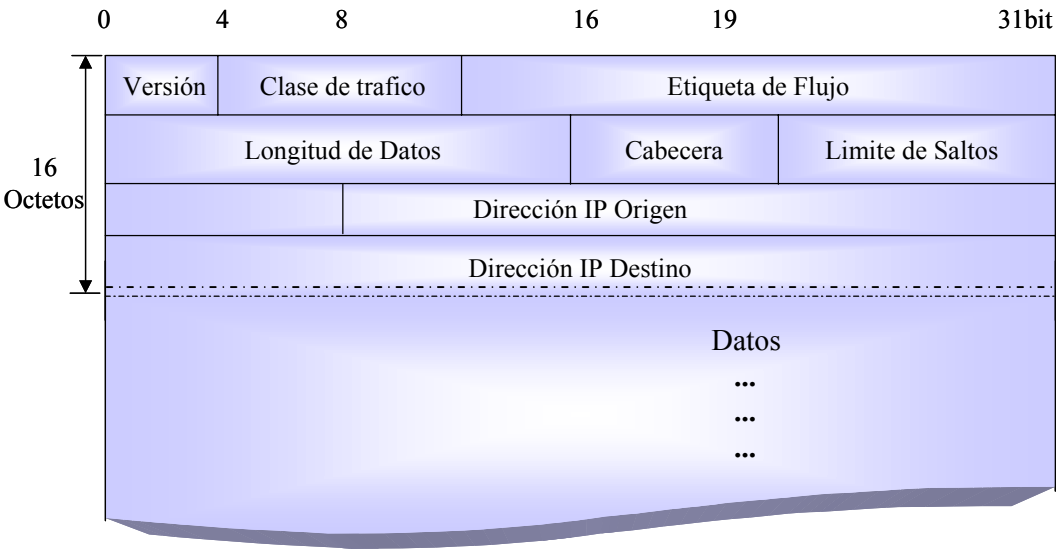
Formato

Esta versión tiene varias mejoras sobre la anterior, que esencialmente son

- Tamaño de dirección IP de 16 octetos (128 bits)
- Formato de cabecera más simple
- Etiqueta de flujo
- Configuración de direcciones IP más automatizada
- Mejora en las extensiones y opciones
- Extensiones para la autenticación y seguridad
- Enrutamiento múltiple mejorado, añadiendo un campo en la dirección de multidifusión.
- Direccionamiento a cualquier sitio (*anycast*).

En la figura 5 se representan los campos de la cabecera IPv6.

Figura 5. Formato de IPv6



La cabecera IPv6 incluye los campos:

- Clase de Tráfico (8 bits) para establecer prioridades en la entrega de tráfico de datos. Equivale al campo tipo de servicio (TOS), y permite la implantación de servicios diferenciados.

- Etiqueta de Flujo (20 bits) para indicar el tratamiento especial del encaminamiento de una secuencia de paquetes.

- Cabecera Siguiente (8 bits), especifica el siguiente protocolo encapsulado. Compatible con el campo de protocolo de IPv4.

- Límite de saltos (8bits), valor que se va decrementando por cada salto; sustituye al campo TTL en la cabecera IPv4.

Las principales ventajas derivadas del uso de IPV6 son:

- **Escalabilidad**, al poseer un espacio de direccionamiento de 4x32 bits, pueden establecerse jerarquías de direccionamiento de diversos niveles, y facilitar las rutas de acceso.

- **Seguridad**, la especificación incluye codificado de paquetes (ESP) y cabecera de autenticación de la fuente. Con IPSec se puede también prevenir los problemas de autenticación para los paquetes dirigidos a su destino predeterminado.

- **Calidad de Servicio (QoS)**, la etiqueta de flujo en IPv6 indica a qué flujo extremo a extremo pertenece un paquete, y así se puede encaminar con mayor eficiencia.

- **Autoconfiguración** de la dirección, al establecerse una configuración automática de direcciones se facilita la gestión de terminales y enrutadores. En caso de unión de dos redes IPv6, también se pueden renumerar las direcciones automáticamente.

- **Descubrimiento del próximo (ND),** es un protocolo que sustituye a ARP, y a diferencia de éste utiliza direcciones *multicast*, lo cual implica que no se difunden indiscriminadamente los datos a todas las direcciones como en ARP.

- **Fragmentación de paquetes.** A diferencia de IPv4, la cabecera puede estar encadenada, indicando si el siguiente paquete contiene cabecera o datos. La fragmentación entonces ocurre extremo a extremo, no a través de los enrutadores.

La cuestión de interoperabilidad entre redes IPv4 e IPv6 está también resuelta, y se han considerado los casos de envío y de datos entre una y otra red, así como entre redes IPv6 a través de una red IPv4 mediante “túnel”.

En definitiva, IPv6 amplía y mejora el espacio de direccionamiento IP, facilita la configuración de redes y proporciona seguridad y calidad de servicio.

2. ESTANDARES DE VoIP

La Voz sobre IP, como tecnología emergente esta basada en estándares que permiten que su aplicación como servicio adicional de las redes de datos, tenga una gran aceptación entre los usuarios, que como se ha proyectado e investigado es un sector que ha estado en constante crecimiento.

Este grado de aceptación que ha recibido la voz sobre IP se debe en gran parte a estos estándares que se han estado desarrollando, que a su vez han permitido manejar un alto porcentaje de calidad de servicio (QoS) que es entre otras cualidades el atractivo de Voz sobre IP.

Los estándares de mayor aplicación e importancia en esta tecnología son, el estándar H.323 y el protocolo SIP (*Session Initiation Protocol*), que se han destacado por su versatilidad y confiabilidad.

2.1 ESTANDARES DE LA FAMILIA H.32x

Los estándares que hacen parte de la recomendación H.32x especificada por la ITU-T, están desarrollado para respaldar los servicios de comunicaciones multimedia sobre diferentes tipos redes:

H.324 Trabaja sobre SCN (*Switched Circuit Network*).

H.320 Trabaja sobre ISDN (*Integrated Services Digital Networks*).

H.321 y H.310 Trabajan sobre B-ISDN (*Broadband Integrated Services Digital Networks*).

H.322 Trabaja sobre LANs que garantizan calidad de servicio.

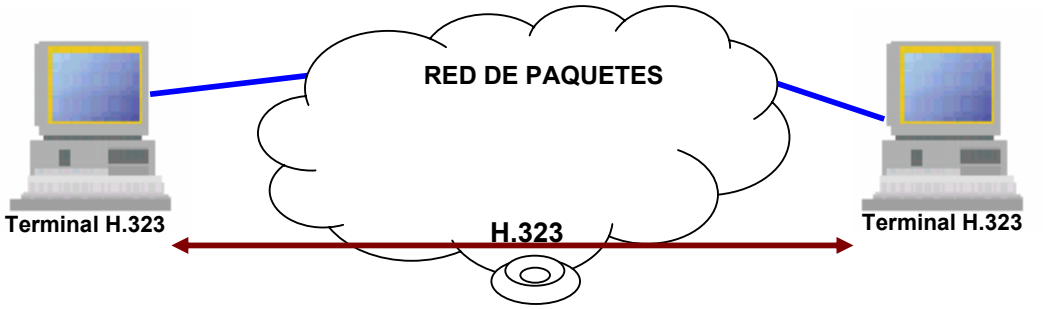
H.323 Trabaja sobre IP

H.323 ha sido uno de los más desarrollados gracias a que este estándar garantiza interoperabilidad con otras redes de servicios de multimedia. Esta característica es alcanzada a través del uso de un *Gateway*. El *Gateway* es utilizado para interpretar cualquier red o señal requerida para la interoperabilidad.

2.1.1 Estándar H.323. Este estándar es la piedra angular para las tecnologías de transmisión de audio, video y comunicaciones de datos sobre redes de paquetes en tiempo real. Por medio de este estándar se especifican los

componentes, protocolos y procedimientos necesarios para proveer un sistema de comunicaciones multimedia en redes de paquetes (ver Figura 6). Cuando se especifica redes de paquetes se debe tener en cuenta que esta puede estar basada en, el protocolo IP (*Internet Protocol*) o el IPX (*Internet Packet Exchange*).

Figura 6. Terminales H.323 en una Red de Paquetes.



H.323 puede ser utilizado en diferentes aplicaciones como son, solo audio (Telefonía IP), audio y video (video telefonía), audio y datos, y audio video y datos. También puede ser aplicado para comunicaciones multimedia multipunto.

Este estándar, como se observa brinda incontables servicios que pueden ser aplicados en diversas áreas, como lo son, negocios, aplicaciones de entretenimientos, consumidores directos, entre otras áreas. Es por esta razón que ha sido desarrollado para trabajar bajo diferentes clases de redes, que van desde las redes de área local (LANs), redes empresariales (ENs), redes de área metropolitana (MANs) hasta las redes de área extensa (WANs).

2.2 PROTOCOLO DE INICIO DE SESIÓN (SIP)

Aunque H.323 es la referencia para interoperabilidad en el mundo de la VoIP, existen otros protocolos alternativos de menor complejidad que también se utilizan en aplicaciones de telefonía sobre IP. El protocolo SIP (*Session Initiation Protocol*) es uno de ellos, fue desarrollado por la IETF (*Internet Engineering Task Force*) y se caracteriza por ser relativamente simple, claro y familiar en el ámbito de las aplicaciones Internet está siendo utilizado cada vez con mayor frecuencia.

SIP es un protocolo de señalización de llamadas basado en texto. Está diseñado teniendo en cuenta protocolos textuales establecidos por el IETF en Internet, tales como SMTP y HTTP, con codificación normalizada flexible y extensible. Comparte otros elementos comunes a Internet, como los nombres DNS y direcciones de correo electrónico. Utiliza, como en HTTP, el modelo "petición-respuesta" en la iniciación de una llamada, que puede ser establecida estrictamente sin la mediación de un agente de llamada.

Las entidades principales en SIP son el Agente de Usuario (AU), o terminal (puede ser un teléfono IP, *Gateway* o un programa de telefonía), y el Servidor SIP.

2.3 MGCP (*Media Gateway Control Protocol*) / H.248 (MEGACO).

MGCP es un protocolo tipo maestro-esclavo para comunicaciones entre elementos de control de llamada y *Gateway* de telefonía IP. MGCP surgió con el objeto de facilitar la integración del protocolo de señalización número 7 (SS7) con la VoIP, ya que la arquitectura definida en H.323 es incompatible con el mundo de los servicios de telefonía publica. Las soluciones de VoIP basadas en MGCP separan la inteligencia de la llamada (funciones de control) del manejo de los medios, lo cual lo hace bastante apropiado para la tecnología de conmutación por software (*softswitch*).

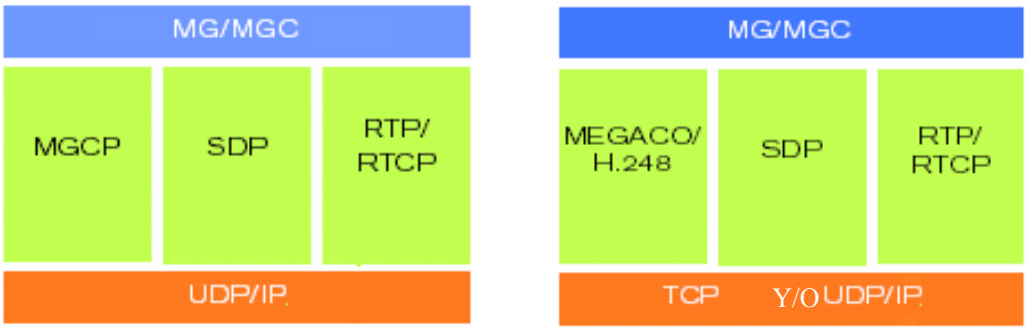
Megaco (o su equivalente la recomendación H.248 de la UIT) es bastante similar a MGCP desde el punto de vista de la arquitectura y la relación controlador-*Gateway*, pero también soporta otras redes como ATM. Propuesto conjuntamente por el Grupo 16 de UIT y el IETF, Megaco añade a MGCP capacidades de interoperabilidad entre iguales, y proporciona un medio de control apropiado para dispositivos telefónicos IP que operen como maestro/esclavo.

Megaco explota el modelo *Gatekeeper* y desplaza el *Gateway* de control de señalización, hacia un " *Gateway* de control de medios " o "softswitch". MGCP/Megaco es el protocolo usado para comunicaciones entre el controlador (MGC) y el *Gateway* de medios (MG), y está diseñado para el control remoto intradominio de dispositivos orientados a conexión o a sesión,

tales como *Gateway* VoIP, servidores de acceso, multiplexores de acceso DSL (DSLAMs), dispositivos enrutadores, MPLS, etc.

Mediante el protocolo Megaco, el MG, al detectar un descuelgue (cuando una persona levanta el teléfono para hacer una llamada), se lo comunica al MGC. Este puede responder con un comando de instrucción al MG para que envíe tono de marcación y 'escuche' los tonos del número marcado. Después de detectar el número, el MGC determina como enrutar la llamada y, usando un protocolo de señalización inter-MGC como H.323 o SIP, contacta con el MGC del terminal distante.

Figura 7. Arquitecturas MGCP/MEGACO



Arquitectura MGCP **Arquitectura MEGACO**

El estándar H.323 Será analizado en forma detallada en el capitulo 3 y el Protocolo SIP en el capitulo 4 respectivamente, por ser estas dos recomendaciones las más utilizadas y más representativas de la normativa establecida

3. ESTANDAR H.323

Este estándar pertenece a la familia de recomendaciones H.32x desarrollada por la ITU-T, que especifica las recomendaciones para los servicios de comunicaciones multimedia sobre diferentes tipos de redes. Para el caso del estándar H.323 se trabajan estos servicios sobre las redes IP.

3.1 PROTOCOLOS ESPECIFICADOS POR H.323

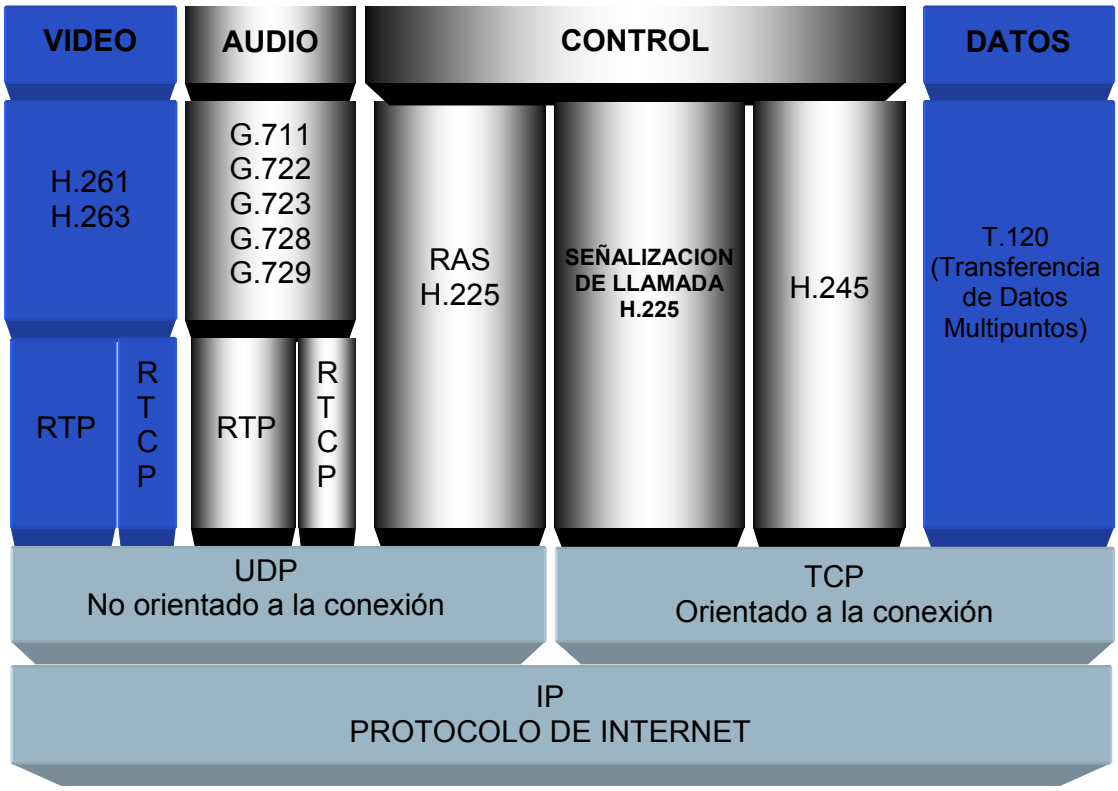
H.323 especifica cuatro pilas de protocolos básicamente, que son: Audio, Video, Control y Datos (ver figura 8). Para la aplicación de VoIP la parte sombreada de la tabla (Control y Audio), es la que se utiliza. Los protocolos especificados son los que están sombreados y de color azul.

Dentro de estos protocolos se definen los siguientes:

- *CODECs* de Video.
- *CODECs* de Audio.
- H.225 RAS (Registro, Acceso y Estado).

- H.225 Señalización de Llamadas.

Figura 8. Protocolos H.323



- H.245 Señalización de Control.

- RTP (Protocolo de Transferencia en Tiempo Real).

- RTCP (Protocolo de Control en Tiempo Real)

3.1.1 *CODECs* de video. La función de este protocolo es codificar el video proveniente de la cámara para la transmisión de la terminal H.323 que se encuentra enviando información, decodificar el video que se recibe y que es enviado al reproductor de video en la terminal H.323 que recibe la información. Ya que H.323 especifica el soporte de video de manera opcional, no es vital para una red H.323 que maneja únicamente VoIP. Sin embargo cualquier terminal qué desee comunicación de video, debe soportar los codificadores y decodificadores de video especificados en la recomendación ITU-T H.261.

3.1.2 *CODECs* de audio. Un *Codec* de audio codifica la señal proveniente del micrófono para la transmisión de la terminal H.323 que se encuentra enviando información, y decodifica el *Codec* de audio recibido que es enviado al dispositivo de salida de audio (altavoz) de la terminal que recibe la información. Como el mínimo servicio proporcionado en el estándar H.323 es el de audio, todas las terminales H.323 deben tener al menos el soporte de un *Codec* de audio, entre los que se encuentran los siguientes:

3.1.2.1 Estándar G.711. Utiliza la técnica PCM (*Pulse Code Modulation*) para la digitalización de la señal de voz. La tasa de transmisión es de 64 Kbps. El estándar G.711 es reconocido internacionalmente, es extensamente utilizado en la conversión de señales de voz para la transmisión en redes digitales. La calidad resultante de las señales de voz después de la conversión es adecuada

para las señales de voz, pero no es considerada lo bastante buena para las señales de audio.

3.1.2.2 Estándar G.722. Utiliza una variante de la técnica ADPCM (*Adaptive Differential Pulse Code Modulation*), denominada SB-ADPCM (*Sub-Band Adaptive Differential Pulse Code Modulation*). Es utilizado en los canales de 64Kbps de ISDN Para la transmisión de señales de audio de calidad media (frecuencias de hasta 7 Khz.).

3.1.2.3 Estándar G.723.1. El estándar ITU-T G.723.1 (combinación de G.721 y G.723), produce niveles de compresión digital de voz de 10:1 y de 12:1, operando respectivamente a 6.3 Kbps y 5.3 Kbps, con mejor cualidad para la tasa más alta. La característica de reducción de uso de ancho de banda es ideal para la telefonía sobre Internet en tiempo real y para aplicaciones sobre líneas telefónicas convencionales. G.723.1 se desarrollo y se ha convertido en un estándar emergente para la interoperabilidad de la transmisión de la voz en plataformas distintas.

3.1.2.4 Estándar G.728. Utiliza la técnica de LD-CELP (*Low Delay Codebook Excited Linear Prediction*), que es una técnica híbrida de *vocoder* (codificación

por vocalización) y de codificación de forma de onda. La señal de voz esta limitada a 4 Khz y digitalizada a 16 Kbps.

3.1.2.5 Estándar G.729. Utiliza la técnica de codificación denominada CS-ACELP (*Conjugate Structure Algebraic Codebook Excited Linear Prediction*), para codificar una señal analógica de voz en una señal digital de 8 kbps.

3.1.3 H.225 RAS (Registro, Acceso y Estado). Este protocolo es utilizado entre los dispositivos terminales de una red H.323 (Terminales H.323 y *Gateways*) y los *Gatekeeper*. RAS es utilizado para ejecutar procedimientos de registro, control de admisión, cambios de ancho de banda, estado y finalización de sesión entre los dispositivos terminales y los *Gatekeeper*. Un canal RAS es utilizado para el intercambio de mensajes RAS y es este canal de señalización el que se establece antes de abrir algún otro canal entre los dispositivos terminales de la red H.323 y el *Gatekeeper*.

El H.225 RAS es utilizado entre estos dispositivos para lo siguiente:

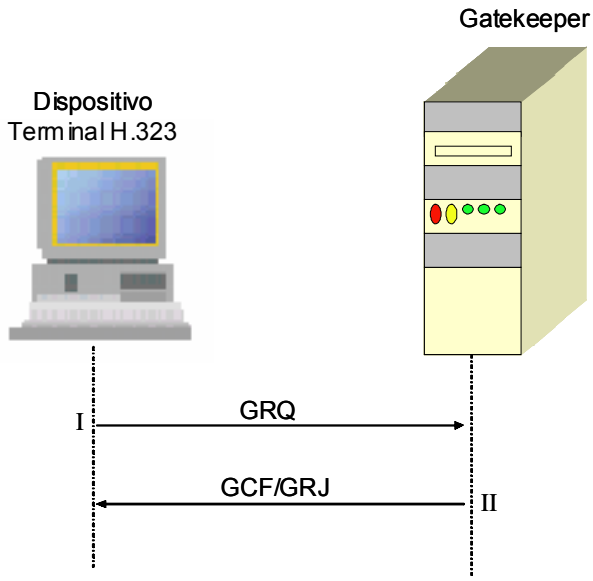
- Detección del *Gatekeeper*.

- Registro y localización de dispositivos terminales.

3.1.3.1 Detección del *Gatekeeper*. La detección del *Gatekeeper* es el proceso mediante el cual un dispositivo terminal determina en cual *Gatekeeper* se debe registrar. Este procedimiento puede ser realizado de forma dinámica o estática. En la detección de forma estática, el dispositivo es pre-configurado con la dirección del *Gatekeeper* asociado a él. En el procedimiento dinámico la asociación dispositivo-*Gatekeeper* se puede alterar con el tiempo, debido a diversas razones como por ejemplo una falla en el *Gatekeeper*.

En el procedimiento dinámico un dispositivo que no ha establecido cual es su *Gatekeeper* asociado, inicia un procedimiento de auto-detección, el cual consiste en el envió de un mensaje *multicast* de petición de *Gatekeeper* (GRQ [*Gatekeeper Request*]), este mensaje es enviado a las direcciones *multicast* de detección de *Gatekeeper*. Uno o más *Gatekeeper* pueden responder con un mensaje de confirmación de *Gatekeeper* (GCF [*Gatekeeper Confirm*]). Este mensaje contiene la dirección de transporte del canal RAS del *Gatekeeper*. Si un *Gatekeeper* no deja registrar un dispositivo debe enviar un mensaje de rechazo de *Gatekeeper* (GRJ [*Gatekeeper Reject*]). Si más de un *Gatekeeper* responde el dispositivo esta en capacidad de escoger cual de los *Gatekeeper* desea utilizar (en este punto el dispositivo sabe cual es el *Gatekeeper* en el que debe hacer su registro) este proceso se ilustra en la figura 9.

Figura 9. Detección Dinámica del *Gatekeeper*



Si ninguno de los *Gatekeeper* responde después de haber transcurrido cierto tiempo, el dispositivo puede reenviar un mensaje GRQ (este reenvió lo hace 5 segundos después de haber enviado el mensaje anterior).

Si un dispositivo, en cualquier momento, determina que su registro de *Gatekeeper* no es valido, el debe redectectar su *Gatekeeper*. La condición de registro inválido puede ser caracterizada por las siguientes situaciones: El dispositivo envía un mensaje de RRQ (*Request Registration*) al *Gatekeeper* y recibe de este un mensaje de RRJ (*Registration Reject*) o no recibe ninguna respuesta.

3.1.3.2 Registro y Localización de Dispositivos Terminales. El procedimiento de registro es por medio del cual un dispositivo terminal se une a

una zona y le informa al *Gatekeeper* la dirección de transporte y nombre de identificación (*alias*) de la zona. Como parte del proceso de configuración todos los dispositivos se deben registrar con el *Gatekeeper* identificado a través del procedimiento de detección. Este registro debe ocurrir antes de que cualquier llamada sea realizada y debe ocurrir periódicamente cuando sea necesario. Por su parte el proceso de localización es mediante el cual la dirección de transporte de un dispositivo Terminal es determinada y se la asigna su nombre de identificación o una dirección E.164.

"Un *Gateway* o una MCU puede registrar una o mas direcciones de transporte. El uso de múltiples direcciones puede simplificar el enrutamiento de llamadas".

Un RRQ puede ser repetido periódicamente de tal forma que el *Gatekeeper* puede manejar múltiples peticiones del mismo equipo. Cuando un mensaje RRQ llega al *Gatekeeper* pueden ocurrir las siguientes situaciones en cuanto al contenido de la dirección del dispositivo que envía el mensaje:

- Las direcciones de transporte y nombre de identificación idénticos a un RRQ anterior: El *Gatekeeper* responde con un RCF (*Registration Confirmation*).

- Nombre de identificación igual al RRQ anterior y dirección de transporte diferente: El *Gatekeeper* puede confirmar la petición de acuerdo con las

políticas de seguridad del mismo o puede rechazar indicando que hay duplicación de registro.

- Dirección de transporte igual a un RRQ anterior y nombre de identificación diferente: El *Gatekeeper* debe modificar el contenido de la tabla de conversiones o puede establecer algún método de autenticación de estos cambios.

El registro que el dispositivo realiza con el *Gatekeeper* puede tener un tiempo finito, este tiempo en el que el registro será valido puede ser indicado por el dispositivo por medio de un mensaje RRQ enviado al *Gatekeeper* y este puede responder con un mensaje RCF que contenga el mismo valor o un valor menor que será el tiempo de vida del registro en el *Gatekeeper*. Antes de que el tiempo de vida expire el dispositivo debe enviar un mensaje RRQ con características especiales para hacer que el contador de tiempo de vida sea reiniciado. En caso que el tiempo de vida expire el dispositivo deberá registrarse nuevamente con el *Gatekeeper* a través de un mensaje RRQ normal.

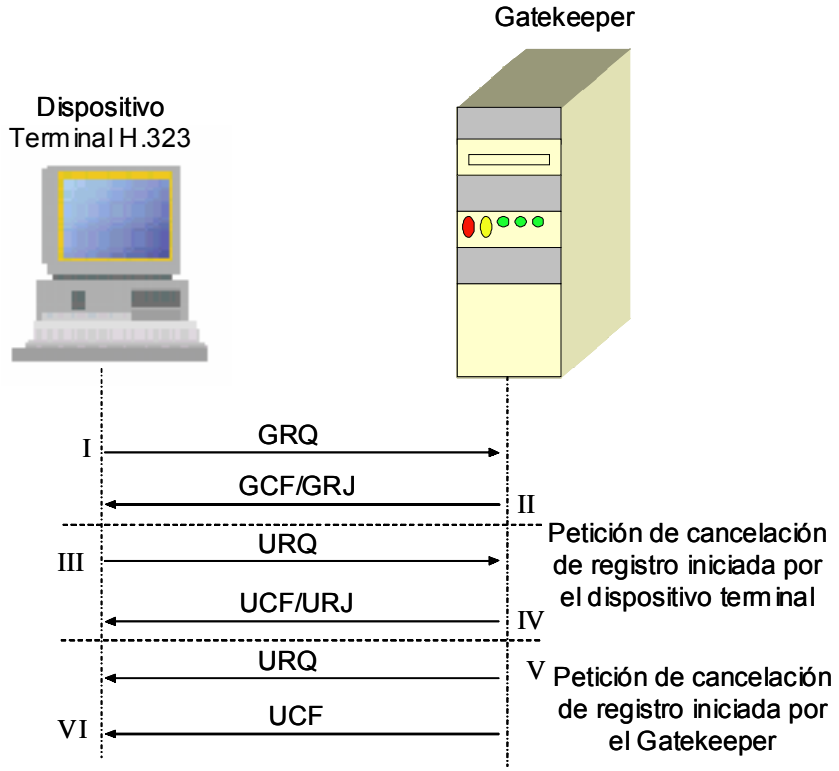
Un dispositivo puede cancelar su registro con el *Gatekeeper* enviando un mensaje URQ (*Unregister Request*) que será respondido por el *Gatekeeper* con un mensaje UCF (*Unregister confirmation*). Si el dispositivo aún no estaba registrado en el *Gatekeeper* este responderá con un mensaje de URJ (*Unregister Reject*). La cancelación de un registro permite a un dispositivo

alterar el nombre de identificación asociado a una dirección de transporte o viceversa.

El *Gatekeeper* por su parte también puede tomar la iniciativa de cancelar el registro de un dispositivo, en este caso el *Gatekeeper* envía un mensaje URQ al dispositivo, que responde con un mensaje UCF. En el caso que el dispositivo desee iniciar una nueva llamada, este debe antes registrarse de nuevo a un *Gatekeeper*.

3.1.4 H.225 Señalización de Llamadas. H.225 señalización de llamadas es utilizado para el establecimiento de conexiones entre dispositivos terminales H.323 (Terminales y *Gateways*). Existen dos casos o formas para el intercambio de mensajes H.225 señalización de llamadas. La primera forma es la señalización de llamadas directa, en este caso durante la confirmación de acceso el *Gatekeeper* indica que los dispositivos terminales pueden intercambiar los mensajes de señalización directamente "sin intervención de *Gatekeeper*" (ver figura 11), esto lo realizan por medio del canal de señalización de llamadas. La segunda forma es la señalización de llamadas enrutadas por el *Gatekeeper*, en este caso los mensajes H.225 son intercambiados entre los dispositivos terminales y el *Gatekeeper*, donde el *Gatekeeper* recibe los mensajes de señalización de llamadas, por medio del

Figura 10. Procedimiento para Registro/Cancelación de Registro en el *Gatekeeper*



canal de señalización de llamadas provenientes desde un dispositivo terminal y lo enruta hacia el otro dispositivo terminal por medio del canal de señalización llamadas del otro dispositivo (ver figura 12).

Figura 11. Señalización de Llamada en Forma Directa

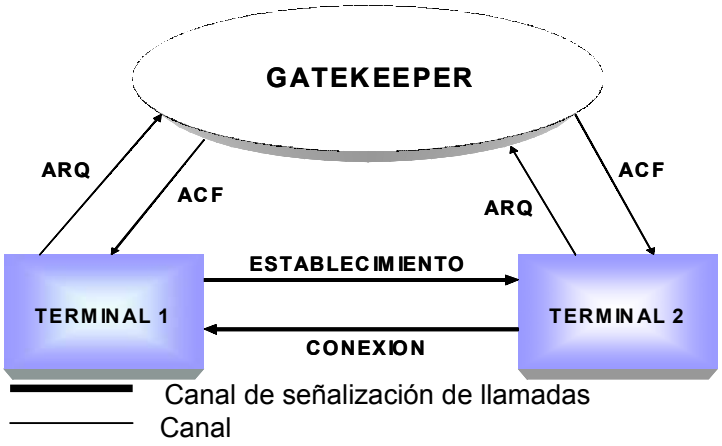
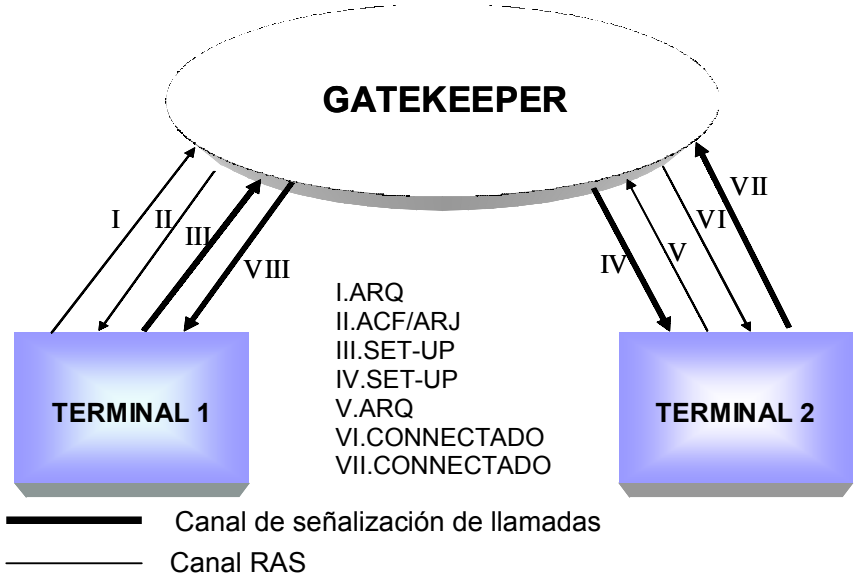


Figura 12. Señalización de Llamadas Enrutadas por el *Gatekeeper*



3.1.5 H.245 Señalización de control. H.245 Señalización de Control consiste en el intercambio *end-to-end* de mensajes de control dirigiendo las operaciones de los dispositivos terminales H.323. Los mensajes de control H.245 son enviados a través del canal de control H.245, este es un canal lógico permanentemente abierto y es diferente a los canales de medios. Estos mensajes de control contienen información con relación con los siguientes puntos:

- Intercambio de capacidades

- Apertura y cerrado de canales lógicos utilizados para cargar el flujo de medios

- Mensajes de control de flujo

- Indicaciones y mensajes generales

El intercambio de capacidades es un proceso que se da las terminales que se están comunicando con el fin de intercambiar mensajes para proporcionar a las mismas la característica de recibir y transmitir las capacidades de los dispositivos con que se esta en la comunicación.

El canal lógico carga la información de un dispositivo terminal a otro dispositivo terminal (el caso de una comunicación punto a punto) o múltiples dispositivos finales (en caso de una comunicación punto a multipunto). Este canal lógico es unidireccional y H.245 proporciona mensajes para abrir o cerrarlo.

3.1.6 Protocolo de transporte en tiempo real (RTP y RTCP). El protocolo de transporte en tiempo real es utilizado para proporcionar entrega de servicios de tiempo real audio y video *end-to-end*. Mientras que en H.323 es utilizado para transportar datos basados sobre redes IP. RTP es típicamente para transportar datos por medio de UDP (*User Datagram Protocol*). RTP junto con UDP, proporcionan funcionalidad de protocolo de transporte. RTP proporciona identificación de tipo de carga útil (*payload*), numeración secuencial, *timestamping* y control de entrega. UDP proporciona servicios de

multiplexación y *checksum*. RTP también puede ser utilizado con otros protocolos de transporte.

3.1.6.1 Identificación del *Payload*. Es esencial que los paquetes RTP entregado al destino sean decodificados según las mismas reglas utilizadas en el proceso de codificación. Es por esto que el RTP identifica la información que esta siendo transportada asociándola a un identificador de tipo de *payload* para cada paquete. Los tipos de *payload*, son esencialmente *codecs* que se utilizan para la digitalización de audio y video.

3.1.6.2 *Timestamping*. El atraso variable entre fuente y destino en una red basada en paquetes, tiene como resultado que los paquetes lleguen al destino con intervalos irregulares entre paquetes. Este efecto es llamado Jitter y puede conllevar a unas perdidas significativa de calidad en cuanto al tráfico de video o voz. RTP actúa como ayuda a este problema incluyendo en su cabecera un campo de 32 bits llamado *Timestamp.*

3.1.6.3 Numeración secuencial. Las características de las redes de paquetes como Internet, no garantiza la llegada en orden de los paquetes al destino. De modo que para permitir la reordenación de los paquetes RTP asocia un número

de secuencia para cada paquete enviado. Este número de secuencia también puede ser utilizado para detectar la perdida de paquetes en la red.

El RTP esta constituido por una parte de datos (RTP) y una parte de control denominada **RTCP**. La cuya función principal es proporcionar realimentación de la calidad de distribución de los datos. RTCP también proporciona soporte para conferencia en tiempo real con grupos de cualquier tamaño, así mismo también proporciona soporte para la sincronización de diferentes flujos de medios.

RTCP se basa en la transmisión periódica de paquetes control para todos los participantes de una sesión, utilizando los mismos mecanismos de distribución de paquetes de datos. Los paquetes RTCP contienen información importante para monitoreo de entrega paquetes de audio, tales como: *Jitter* entre llegadas de paquetes, número de paquetes perdidos, numero total de paquetes y octetos transmitidos y otros datos útiles para diagnostico, monitoreo y corrección de algunos tipos de condiciones e error en la red.

3.2 COMPONENTES BASICOS DE H.323

El estándar H.323 especifica cuatro clases de componentes, los cuales, al trabajar en conjunto en una red, están en capacidad de proveer servicios de comunicaciones multimedia punto a punto y punto a multipunto.

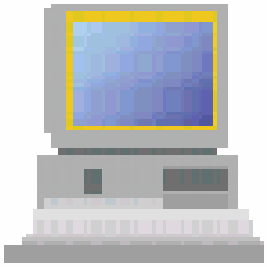
- Terminales
- *Gateways*
- *Gatekeeper*
- Multipoint Control Units (MCU)

3.2.1 Terminales. Es el extremo de cliente que proporciona comunicaciones multimedia bidireccionales en tiempo real; una terminal de H.323 puede ser un computador personal (PC) o un dispositivo independiente (teléfono) en el cual esté corriendo H.323 y aplicaciones multimedia. El terminal H.323 soporta comunicaciones de voz y puede soportar de forma opcional datos o videos. Ya que el servicio básico que se provee en una terminal H.323 es de comunicaciones de voz.

Como una de las características primarias de H.323 es la interoperabilidad, las terminales H.323 son compatibles con terminales H.324 (SCN y *wireless*), terminales H.310/H.21 (B-ISDN), terminales H.320 (ISDN) y terminales H.322 (QoS LANs). Se debe destacar que las terminales H.323 se pueden utilizar en conferencias multipuntos.

Figura 13. Terminales H.323

Teléfono IP



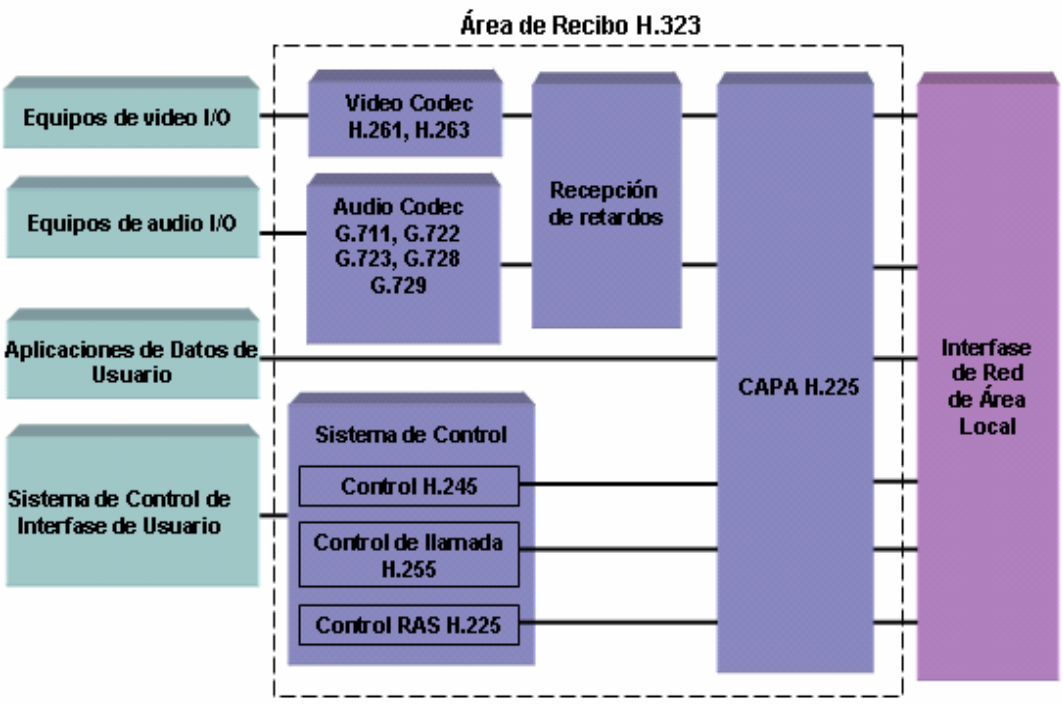
Computador Personal (PC)

3.2.1.1. Características de los terminales H.323. Los terminales H.323 deben trabajar con los siguientes protocolos:

- **H.245** Para la capacidad de intercambio entre terminales y creación de canales.
- **H.225** Para el establecimiento y señalización de llamadas.
- **RAS** Para registro y otros controles de admisión con un *Gatekeeper*.
- **RTP/RTCP** Para ordenar los paquetes de audio y video

Los terminales H.323 deben de igual manera trabajar con el *CODEC* de audio G.711. Otros componentes opcionales con los que puede trabajar un terminal H.323 son los *CODEC* de video, protocolo para transmisión multipunto de datos T.120 y poseer características de MCU (sección 3.2.4).

Figura 14. Arquitectura del Terminal H.323



3.2.2 *Gateway*. Este es un dispositivo diseñado para brindar conectividad y la posibilidad de comunicación entre dos redes diferentes. El *Gateway* como componente básico de H.323 tiene como objetivo primordial, hacer compatibles las características de una terminal de H.323 y una terminal perteneciente a una red de circuitos conmutados y viceversa. En general un *Gateway* está diseñado para realizar conversiones entre formatos de transmisión (por ejemplo: H.225 a H.221), procedimientos de comunicación (por ejemplo: H.245 a H.242), y

formatos de audio, video y datos (por ejemplo: G.711 a G.729). Además de estas características este dispositivo en conjunto con un *Gatekeeper* (sección 3.2.3), esta en capacidad de ejecutar funciones de establecimiento y finalización de llamadas entre una red H.323 y una SCN.

Para establecer una comunicación entre un terminal H.323 y otro terminal H.323, no es necesario el uso de un *Gateway*, siempre y cuando los dos terminales se encuentren en la misma red; ya que no serian necesarias las características de conversión que este posee. Aunque se podría utilizar en el caso en que se quiera evitar un *Router* o un enlace de baja velocidad, estableciendo una llamada de salida a través de un *Gateway* y retornando a la misma red a través de otro *Gateway*.

3.2.2.1 Características del *Gateway*. Una aplicación directa del *Gateway* de la norma H.323 es en la telefonía IP, donde este conecta una red IP y una red SCN, de la siguiente forma:

En la parte correspondiente a la red H.323, en el *Gateway* se maneja el protocolo de señalización de control para capacidad de intercambio H.245, el protocolo de señalización de llamadas H.225 para el establecimiento y finalización de las mismas, y H.225 registro, admisión y estado (RAS), para registro con el *Gatekeeper*. En la parte correspondiente a la SCN, en el

Gateway se manejan protocolos específicos par a este tipo de redes, por ejemplo: ISDN y SS7.

Los terminales H.323 se comunican con el *Gateway* utilizando el protocolo de señalización de control H.245 y el protocolo de señalización de llamada H.225. El *Gateway* convierte estos protocolos de manera transparente a las respectivas contrapartes en la SCN y viceversa. El *Gateway* también realiza el establecimiento y finalización de llamadas en ambas redes y como se explicó anteriormente la conversión entre formatos de audio, video y datos. En algunos casos la conversión de audio y video no es requerida y esto ocurre cuando ambas terminales (terminal H.323 y la terminal de la otra red diferente a H.323) utilizan un mismo modo de comunicación.

Los *Gatekeeper* reconocen a cada uno de sus puntos terminales como *Gateway*, ya que estos se han registrado a él por medio del protocolo H.225. Los *Gateway* además de todas estas características ya mencionadas están en condiciones de soportar un número considerable de llamadas simultáneas entre una red H.323 y otra diferente. Se debe tener en cuenta que el *Gateway* es un componente lógico de H.323 y puede ser implementado como parte de *Gatekeeper* o de una MCU.

Figura 15. Pila de Protocolos del *Gateway*

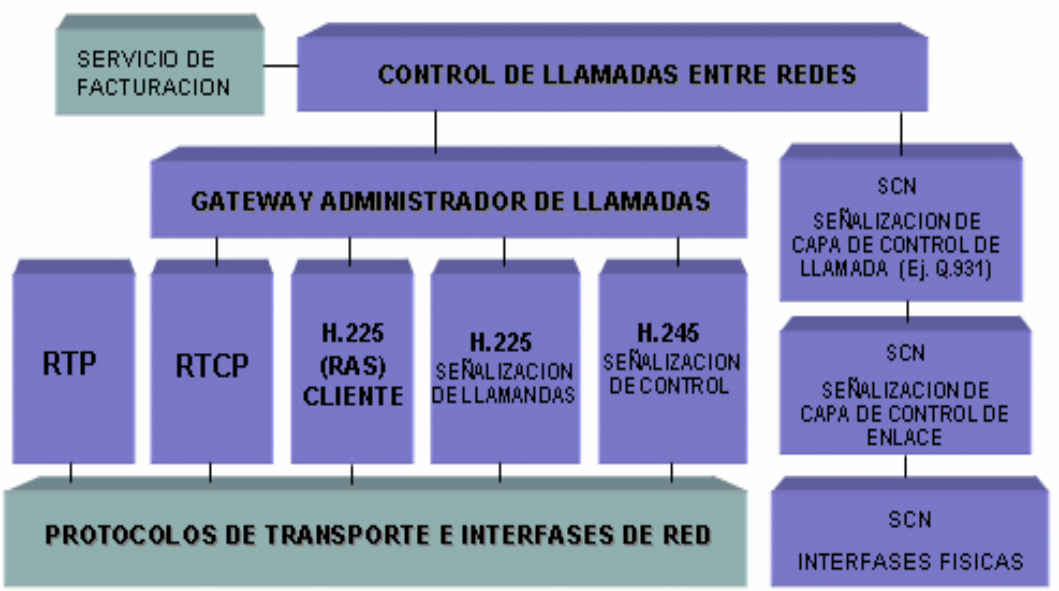
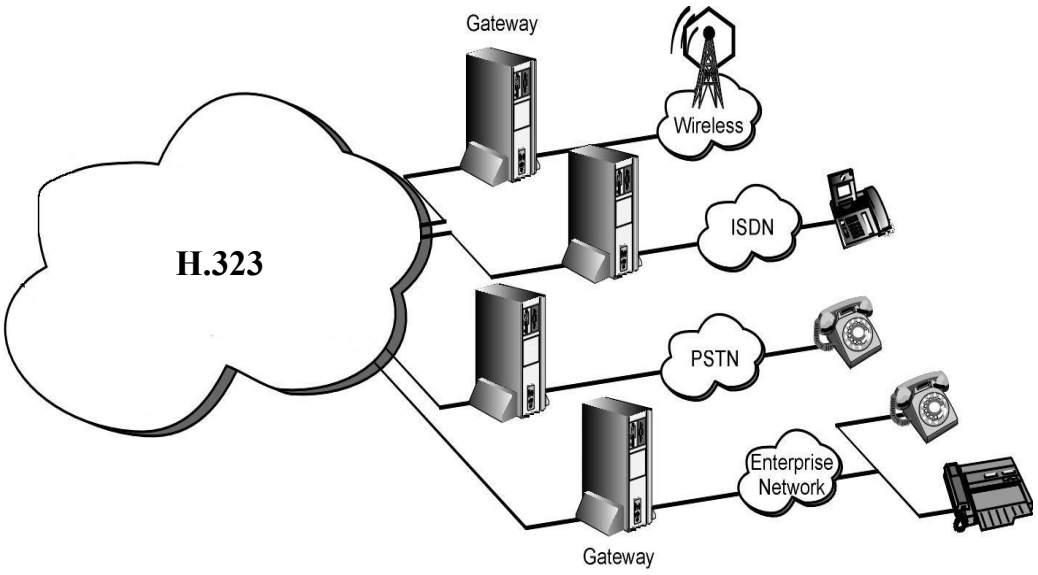


Figura 16. Localización Lógica del *Gateway*



3.2.3 *Gatekeeper*. El *Gatekeeper* es la herramienta de gestión más poderosa disponible para una red multimedia H.323. Este dispositivo es en realidad el cerebro de las redes H.323. Es el punto focal para todas las llamadas dentro de una red H.323, su aplicación brinda esencialmente las funciones de control y administración requeridas para mantener la integridad de las redes en cada uno de los medios donde esta se desenvuelven.

Como dispositivo de importancia crucial dentro de H.323 el *Gatekeeper* proporciona las siguientes funciones:

- Autorización.
- Autenticación.
- Contabilización y registro.
- Control y enrutamiento de llamadas.
- Servicios telefónicos básicos como la guía telefónica y funciones de PBX.
- Control del ancho de banda usado para suministrar QoS y proteger otras aplicaciones criticas de la red del trafico H.323.

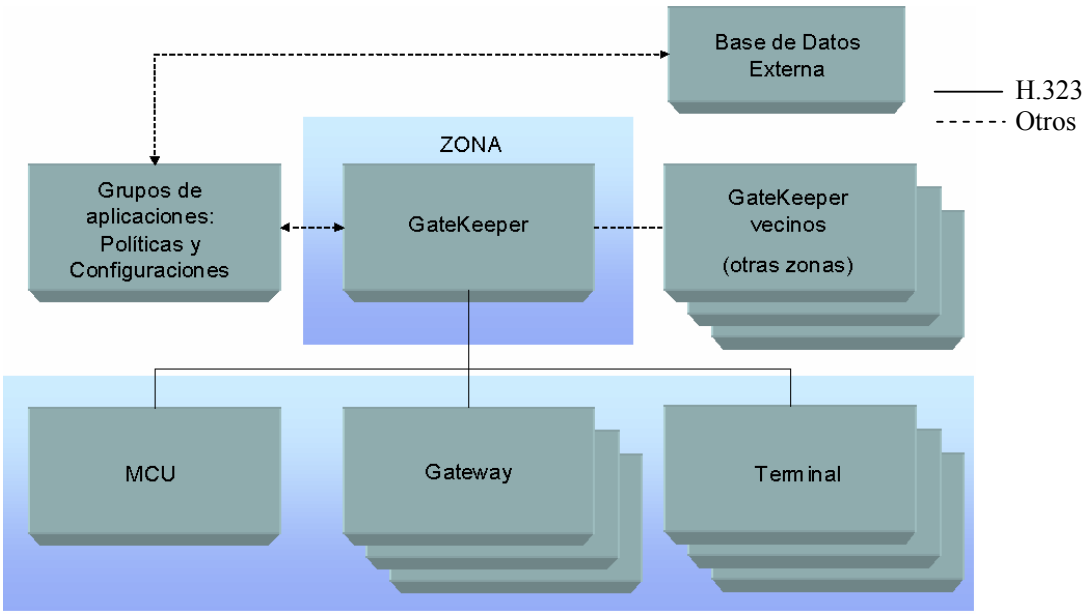
- Control total del uso de la red.

- Sistema de administración global y políticas de seguridad.

3.2.3.1 Entorno del *Gatekeeper*. El estándar H.323 es implementado en las redes a través de zonas, que están relacionadas de forma intrínseca con el *Gatekeeper*. Las zonas son el conjunto de todas las terminales, *Gateways* y MCUs manejados por un solo *Gatekeeper* es decir, es el conjunto de puntos finales sobre los cuales solo un único *Gatekeeper* tiene jurisdicción. Las zonas pueden ser definidas de acuerdo a la ubicación geográfica, a la topología de la red, a un prototipo funcional (organizacional), en fin la característica principal de las zonas es que se debe tener un solo *Gatekeeper* aditivo y debe ser comprendida como múltiples segmentos de red conectados por medio de *routers* u otros dispositivos

El *Gatekeeper* maneja todas las actividades de la zona. Si se desea integrar a la red un nuevo componente (Terminal, *Gateway*, Etc.), este enviara una pregunta a la red con el objetivo de identificar cual de los *Gatekeeper* está presente y si acepta la petición de registro de este componente o envía la petición de registro a un *Gatekeeper* predeterminado. Este proceso de identificación y registro de cualquier componente terminal es un prerrequisito para la zona de administración del *Gatekeeper*.

Figura 17. Entorno del *Gatekeeper*



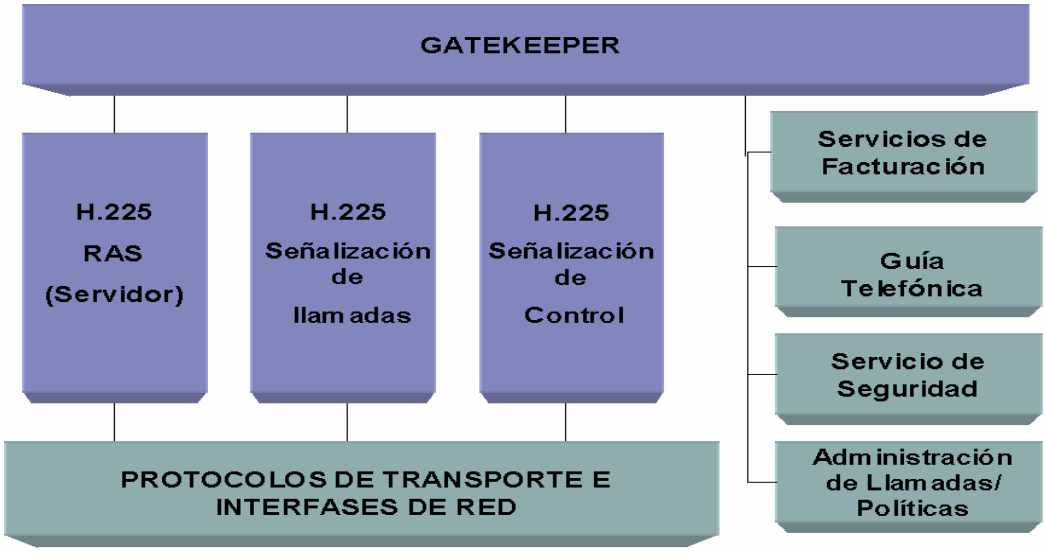
La elección del *Gatekeeper* es crítica para la operación óptima del total de la red H.323. El *Gatekeeper* no es un obstáculo para los diseñadores en relación a la capacidad de la escalabilidad de sistema para un mayor número de usuarios.

La identificación de puntos terminales en una zona es realizada utilizando versiones IP, identificación de nombres (como identificadores H.323, direcciones de *e-mail* y *URLs* [*Universal Resource Locators*]) o números telefónicos. El *Gatekeeper* puede ser configurado y controlado remotamente por medio de un grupo de aplicaciones independientes, utilizando HTTP (*Hypertex Transfer Protocol*) o SNMP (*Signaling Network Management Protocol*). Por ejemplo el diseñador de la red puede configurar el *Gatekeeper*

para permitir un conjunto específico de componentes terminales dentro de la red y proveer usuarios con un único grupo de políticas y procedimientos.

Los servicios ofrecidos por el *Gatekeeper* están definidos por el Protocolo H.225 e incluyen traslación de direcciones, control de admisión, control de ancho de banda y administración de zonas; y a pesar de todas estas características el *Gatekeeper* es opcional en un sistema H.323. Las redes H.323 que no tienen *Gatekeeper* no tendrán la posibilidad de brindar estos servicios, pero en el caso de redes H.323 que tienen *Gateway* de telefonía IP podrían contener también un *Gatekeeper* para trasladar direcciones telefónicas entrantes E.164 en direcciones de transporte. El *Gatekeeper* es un componente lógico de H.323 pero puede ser implementado como parte de un *Gateway* o MCUs.

Figura 18. Componentes del *Gatekeeper*



3.2.3.2 Funciones del *Gatekeeper*. El *Gatekeeper* como dispositivo reglamentado en el estándar H.323 de la ITU-T, incluye funciones que son de carácter obligatorio y funciones que pueden ser opcionales dependiendo de las especificaciones de la red en la que se va a realizar la aplicación de VoIP.

3.2.3.2.1 Funciones de carácter obligatorio. Las funciones de carácter obligatorio especificadas en el estándar H.323 para los *Gatekeeper* son las siguientes:

- Conversión de direcciones.
- Control de acceso.
- Control de ancho de banda
- Administración de zonas.

3.2.3.2.1.1 Conversión de direcciones. El *Gatekeeper* permite el uso local de esquemas de direccionamiento privado, tales como *nickname*, direcciones de *e-mail*, números telefónicos, etc. Por lo tanto debe proveer la conversión de estas direcciones en direcciones necesarias para el establecimiento de una comunicación sobre una red IP. Esto sucede ya que los usuarios típicamente

no conocen las direcciones IP de las otras terminales con las que se desean comunicar. Este proceso de conversión de direcciones se realiza por medio de una tabla de conversión. Que se puede actualizar por medio de diferentes mecanismos, uno de ellos es el uso del canal de registro, admisión y estado (RAS). Para las terminales que no utilizan el canal RAS se puede implementar otros mecanismos para el enrutamiento de sus comunicaciones.

Otro caso en el que se aplica este servicio es para las llamadas originadas fuera de las redes H.323, que son recibidas por el *Gateway*, estas típicamente utilizan números telefónicos E.164 para identificar el terminal de destino. Para poder establecer la comunicación en la red IP es necesaria la conversión de este número telefónico en direcciones IP.

3.2.3.2.1.2 Control de acceso. El *Gatekeeper* autoriza el acceso a la red basado en lineamientos H.323 y otros criterios, utilizando ARQ (*Admissions Request Message*), ACF (*Admissions Confirm Message*) y ARJ (*Admissions Reject Message*). Estas políticas o lineamientos son seleccionadas por el administrador de la red cuando esta configurando el *Gatekeeper* y/o las zonas. El acceso a la red y a los servicios especiales (Ej. Uso de un *Gateway*), pueden ser configurado por medio de autorización de llamadas, utilización y disponibilidad de ancho de banda, identificación de usuario, hora del día, direcciones de origen y destino u otros criterios. Se debe tener en cuenta que como resultado de la limitada cantidad de recursos, no todos los usuarios

estarán en capacidad de acceder a la red al mismo tiempo y que esta función puede ser nula, es decir que se admiten todas las peticiones de ingreso a la red.

3.2.3.2.1.3 Control de ancho de banda. El *Gatekeeper* monitorea y controla el consumo de ancho de banda de la red y garantiza que el tráfico de video y/o audio no exceda la carga máxima de la red definida por el administrador de la red. El administrador tiene la capacidad de restringir el consumo de ancho de banda del tráfico H.323 con el fin de ofrecer calidad de servicio (*QoS*) a otras aplicaciones más críticas y de mayor importancia. Este control lo realiza el *Gatekeeper* utilizando mensajes RAS, BRQ (*Bandwidth Request*), BCF (*Bandwidth Confirm*) y BRJ (*Bandwidth Reject*). Por ejemplo si el administrador de red ha especificado un límite para el un número de conexiones simultaneas en la red H.323, el *Gatekeeper* puede rechazar el establecimiento de nuevas conexiones una vez que este limite ha sido alcanzado. El control de ancho de banda al igual que el control de admisión puede ser una función nula, por lo tanto en este caso se aceptarían todas las peticiones para modificación del ancho de banda.

3.2.3.2.1.4 Administración de zonas. El *Gatekeeper* brinda las funciones mencionadas anteriormente (conversión de direcciones, control de acceso y control de ancho de banda), para los terminales, *Gateway* y MCUs localizados

dentro de su zona de control. Como un ejemplo de aplicación se puede requerir que no más de 15 llamadas sean permitidas en un enlace de baja velocidad, de modo que la QoS no sea degradada. Este tipo de administración puede de igual forma permitir aplicaciones como distribución automática de llamadas y otros servicios asociados a un centro de llamadas (*Call Center*).

3.2.3.2.2 Funciones Opcionales. Estas características adicionales que pueden ser incorporadas al *Gatekeeper* fueron desarrolladas e implementadas para ofrecer una mejor calidad y variedad de servicios dentro de una red H.323, añadiendo de esta forma un valor agregado a la red. Las funciones opcionales que se brindan son las siguientes:

- Control de enrutamiento de llamada.
- Autenticación de llamadas.
- Acceso/autorización de llamadas.
- Contabilización de llamadas.
- Administración de ancho de banda.
- Servicios de administración de llamadas.

- Servicios adicionales.

- Servicios de guía telefónica.

3.2.3.2.2.1 Control de enrutamiento de llamada. Existen dos modelos diferentes para el enrutamiento de llamadas, el modo directo y el modo de enrutamiento. El modo enrutamiento es el más utilizado y preferido. En este modo el *Gatekeeper* proporciona su propia dirección como la dirección destino, es decir él recibe todos los mensajes de señalización de llamadas y maneja el enrutamiento de las llamadas entre los terminales y el mismo durante la sesión. En este caso el *Gatekeeper* deja un canal de señalización abierto mientras enruta la llamada durante el tiempo de duración de esta. El modo de enrutamiento es fundamental para la administración de llamadas, ya que ejecuta funciones de búsqueda de tramos que proporciona un control separado sobre cada uno de los tramos de la llamada, conectando o desconectando cada uno de estos por separado (ver figura 19).

En el modo directo, el *Gatekeeper* proporciona el terminal que coincide con la dirección de destino y los dirige (el terminal origen se dirige hacia el terminal destino) al canal de señalización de llamadas de tal manera que todos los mensajes pueden ser intercambiado directamente sin la intervención del *Gatekeeper*

Figura 19. Enrutamiento de Llamada

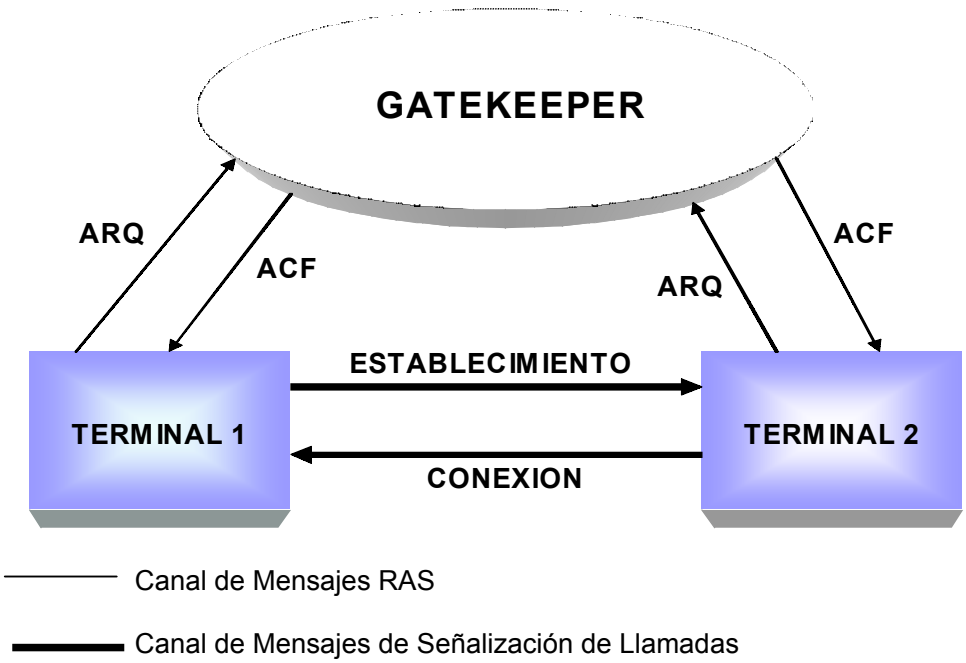


Tabla 2. Modo de Señalización Directa de Llamadas

PROCEDIMIENTOS REQUERIDOS PARA LA ADMINISTRACION DE LAS ZONAS	POLITICAS Y PROCEDIMIENTOS OPCIONALES
Conversión de Direcciones	Autorización de Llamadas
Control de Acceso	Administración de Ancho de Banda
Control de Ancho de Banda	Servicios Adicionales
	Servicio de Guía Telefónica
	Servicio de Administración de Llamadas
PROCEDIMIENTOS OPCIONALES	
Señalización de Control de Llamadas	

3.2.3.2.2.2 Autenticación de llamada. Esta función es identificada dentro del *Gatekeeper* como un servicio adicional, cuando este tiene la capacidad de identificación de usuario o de proveer una determinada clave de acceso.

3.2.3.2.2.3 Acceso/Autorización de llamadas. El *Gatekeeper* autoriza una llamada basándose específicamente en los derechos de acceso de cada uno de los usuarios. Este puede rechazar una llamada proveniente de un terminal como resultado de una anomalía o falla de la autorización. La razón para un rechazo puede incluir la restricción del acceso hacia una terminal o de una terminal o *Gateway*. También se puede restringir el acceso durante ciertos periodos de tiempo pero no se limita solamente a estas acciones en particular.

El administrador de la red puede escoger la acción de admitir todas las peticiones bajo ciertas circunstancias de fuerza mayor. Es de gran importancia resaltar que el control de admisión es la vía para preservar la integridad de las llamadas y sesiones que están en progreso cuando un usuario solicita acceso a la red. Estas políticas de control también pueden ser implementadas para finalizar una llamada ordinaria, para procesar una petición de llamada de mayor prioridad.

3.2.3.2.2.4 Contabilización de llamadas. Una vez que la llamada es finalizada el *Gatekeeper* notifica a la entidad de contabilización los detalles de la llamada.

El *Gatekeeper* también puede generar en cooperación con un sistema de respaldo (base de datos) facturaciones. La información contenida en esta puede incluir muchos detalles como la duración de la llamada, origen, destino y *QoS*.

3.2.3.2.2.5 Administración de ancho de banda. El *Gatekeeper* puede controlar y limitar el número de terminales H.323 permitidos para utilizar la red simultáneamente. A través de H.225 el *Gatekeeper* esta en capacidad de limitar el ancho de banda de las llamadas con el fin de finalizar o rechazar una llamada si determina que no hay suficiente ancho de banda en la red para soportarla. El *Gatekeeper* puede trabajar en conjunto con el servidor de *QoS* para obtener una mejor *QoS* para las llamadas. Esta función puede de igual manera operar durante una llamada activa cuando un usuario terminal solicita ancho de banda adicional.

3.2.3.2.2.6 Servicios de administración de llamadas. El *Gatekeeper* esta en capacidad de mantener una lista de las llamadas H.323 en curso, que es similar a la lógica de una PBX. Esta información es necesaria para indicar que un terminal esta ocupado y proveer información para la función de administración de ancho de banda.

3.2.3.2.2.7 Servicios adicionales. Los servicios adicionales están definidos en el estándar H.324, estos pueden ser entre otros el reenvío y la transferencia de llamadas, que son servicios telefónicos críticos en áreas como las redes empresariales, en donde los usuarios esperan que su red tenga la capacidad de proveerlos de forma transparente. En estos casos tanto el *Gatekeeper* como los terminales pueden proveer el soporte necesario para estos servicios; sin embargo el *Gatekeeper* los ejecuta con menos complejidad computacional y carga sobre el cliente.

3.2.3.2.2.8 Servicios de guía telefónica. Las bases de datos de los *Gatekeeper* deben contener los perfiles de los usuarios para suministrar la información necesaria para implementar este servicio, con el fin de ayudar a los usuarios a encontrar a otros. De igual manera se puede acceder a otros servicios de guía telefónica (como ILS [*Internet Locator Service*]), que son actualizados o configurados con la información necesaria para conectar las llamadas.

3.2.3.3 Papel actual. Aunque originalmente fue considerado como un componente opcional en las redes H.323 por la ITU, el *Gatekeeper* se ha convertido en una herramienta esencial para los proveedores de servicio. Generando un nuevo flujo de ingresos con la aplicación de este en la

comunicación entre la PSTN y las redes IP, respondiendo por consiguiente a la urgente necesidad de la interoperabilidad entre las redes de comunicaciones.

En cuanto a las redes empresariales, el *Gatekeeper* se ha convertido en una gran ayuda para las organizaciones que deben mantener su ventaja competitiva en un mercado de características muy reñidas. El *Gatekeeper* se ha convertido en un instrumento básico en el crecimiento y ha mejorado la calidad de las estructuras de las Intranet para soportar un entorno IP y las capacidades de comunicaciones multimedia en tiempo real. Por medio de la incorporación de este dispositivo las compañías se han estado beneficiando de una mejoría en la producción e incrementado las ganancias como resultado de la colaboración eficiente y eficaz entre empleados, clientes y las cadenas de proveedores. Además, las organizaciones ahora se benefician de los ahorros cosechados por la implantación de la telefonía IP y la simplificación de la administración de la red.

3.2.4 MCU (*Multipoint Control Units*). Las MUCs proporcionan el soporte necesario para las sesiones establecidas entre tres o más terminales H.323. Todas las terminales que participan en esta sesión establecen una conexión con la MCU. La MCU administra todos los recursos de la sesión, las negociaciones entre las terminales con el fin de determinar el codificador/decodificador (*CODEC*) de audio o video a utilizar y puede manejar de igual manera el flujo de información del medio.

Una MCU consta de un MC (*Multipoint Controller*), de carácter obligatorio y uno o más MP (*Multipoint Processor*), que es de carácter opcional por lo tanto una MCU puede carecer de MPs.

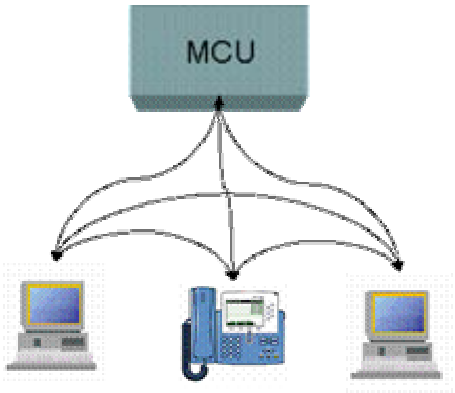
El MC realiza negociaciones H.245 entre todas las terminales para determinar las capacidades de cada uno de ellas y así establecer un nivel común de procesamiento de audio y vídeo, El MC envía o informa a las terminales este conjunto de "capacidades", para de esta forma mantener la interoperabilidad entre ellas indicando la forma o modo en que estas deben transmitir. Este conjunto de capacidades puede ser revisado periódicamente por el MC y reenviado a todas las terminales en la sesión con el objetivo de añadir nuevas terminales a la sesión o actualizar la información para saber cuales terminales han salido de la sesión. Mientras que el MP es el responsable de enrutar y procesar las secuencias de audio, vídeo y datos entre extremos de terminales.

Las posibilidades de establecer una conferencia multipunto en H.323, están divididas en dos conceptos fundamentales, Conferencia centralizadas y descentralizadas.

Las conferencias multipunto centralizadas exigen la presencia de un MCU. En este caso todos lo terminales involucrados en la conferencia envían los flujos de datos, video, audio y control ha la MCU en una forma punto a punto. EL MC administra la conferencia a través de las funciones de control H.245, que también definen las capacidades de cada una de las terminales. El MP recibe,

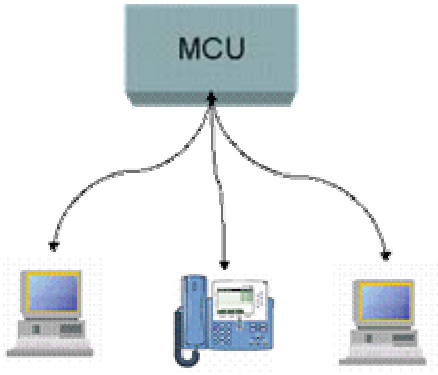
envía y procesa las señales de voz, video o datos de cada uno de los dispositivos participantes. También puede ofrecer conversión de diferentes códigos y tasas de bits, permitiendo la participación de dispositivos con diferentes modos de comunicación. La MCU puede utilizar Multicast para distribuir los flujos de audio y video si los dispositivos participantes en la conferencia tienen la capacidad de recibir transmisiones multicast.

Figura 20. Conferencia Multipunto Descentralizada



Las conferencias multipunto descentralizadas pueden hacer uso de la tecnología multicast de forma que las terminales H.323 se comuniquen sin enviar los datos a una MCU. El MC en este caso puede proveer algunas funciones de control, tales como la administración de la conferencia, *broadcast* de video y señalación de video. Esto puede ser realizado utilizando H.245, en donde el MC recibe mensajes H.245 de los participantes de la conferencia y envía los controles apropiados para los otros dispositivos con el fin de habilitar o deshabilitar sus sistemas de *multicast* de video. De igual manera se pueden utilizar comandos T-120 que proporcionan las mismas funciones.

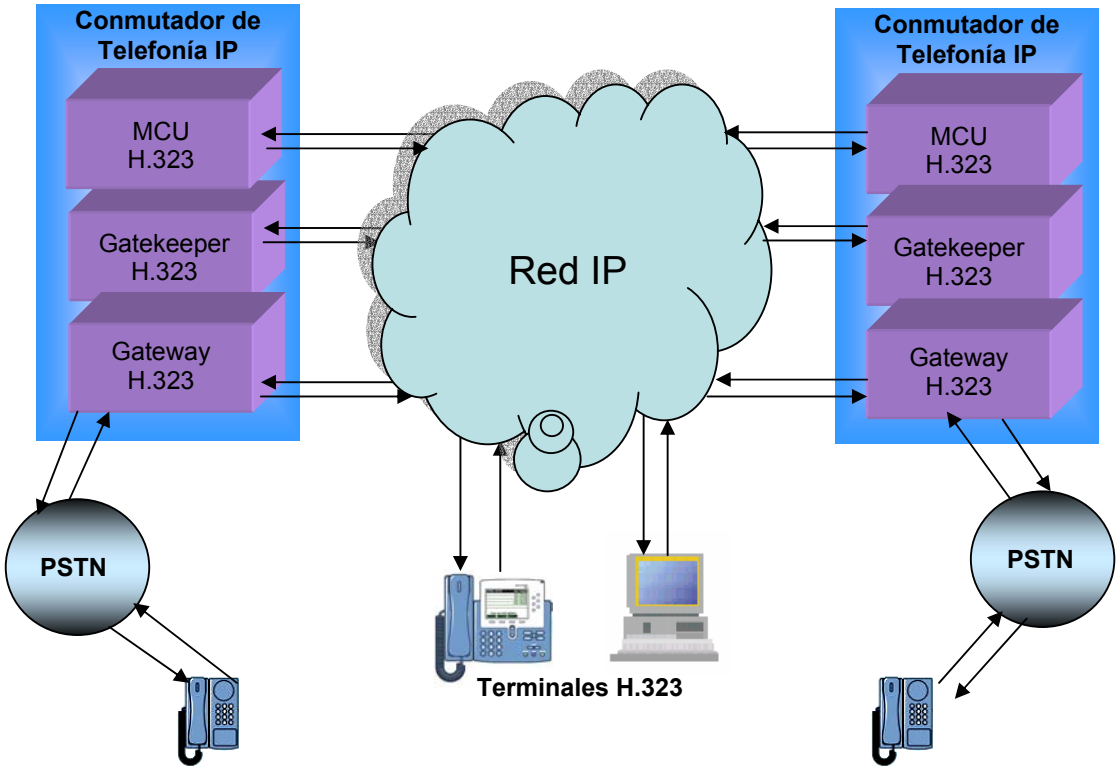
Figura 21. Conferencia Multipunto centralizada



Otra posibilidad de implementación son las conferencias multipunto híbridas, que combinan características de tipo centralizadas y descentralizadas. Las opciones disponibles son: conferencia multipunto con audio centralizado y conferencias multipunto con video centralizado, en ambos casos los dispositivos participantes en la conferencia se comunican con un MC de modo punto a punto utilizando un canal de control H.245.

Como se observa los *Gatekeeper*, *Gateway* y MCUs son lógicamente componentes separados dentro del estándar H.323, pero los tres pueden ser implementados como un único dispositivo físico.

Figura 22. Distribución Lógica de los Componentes de una Red H.323 Durante una Llamada VoIP



3.3 VERSIONES H.323

El estándar H.323 esta especificado por la ITU-T (grupo de estudio 16). La versión número uno de la recomendación H.323 fue aceptada en Octubre de 1996, se caracteriza por no garantizar la calidad de servicio (QoS) para los equipos de redes de área local (LANs) y sistemas telefónicos con visualizadores de video.

El desarrollo de la Voz sobre IP y de las aplicaciones que están inherentes a esta como lo es la telefonía IP, dieron el primer paso para llevar a una revisión la especificación H.323. La ausencia de un estándar para la voz sobre IP resultó en productos que eran incompatibles y con el avance esta, nuevos requerimientos fueron emergiendo, como por ejemplo proveer comunicación entre telefonía basada en computadores y un teléfono tradicional basado en la red telefónica conmutada. Estos requerimientos forzaron al desarrollo de un estándar para telefonía IP.

3.3.1 Versión número dos. En Enero de 1998 nace la versión número dos del H.323 que fue definida para respaldar estos requerimientos adicionales. Esta identifica muchas deficiencias en la versión numero uno e introduce nuevas funcionalidades dentro de los protocolos existentes como H.245 y H.225, así como nuevos protocolos.

Dentro de las nuevas funcionalidades, protocolos y características establecidas se logran destacar las siguientes:

Seguridad: Se hace referencia a tres características cuando se esta tratando de seguridad, autenticación, integridad y privacidad. Autenticación es un mecanismo para asegurar que los dispositivos terminales participantes en una sesión o conferencia sean en realidad quienes dicen ser. La Integridad proporciona un medio para confirmar que los datos dentro de un paquete no

han cambiado. La privacidad/confidencialidad es proporcionada por medio de mecanismos de codificación y decodificación, ya que si los datos son interceptados no podrán ser leídos.

***Fast Connect*:** Es un nuevo método para el establecimiento de llamadas, que evita algunos de los pasos (sección 2.4) con el fin de hacerlo de forma más rápida. Fast Conect permite que el canal de medios (audio, video, datos) que se establece sea operacional después del que el mensaje CONECTADO es enviado, lo que es de gran importancia sobre todo para ciertos procesos de facturación.

Lista de Conferencia: Si una MCU maneja múltiples sesiones o conferencias y desea proporcionar a un dispositivo Terminal que se encuentra llamando o intentando iniciar una sesión la capacidad de elegir una de ellas, la MCU puede enviarle una lista de las conferencias. Este servicio solo es proporcionado para dispositivos terminales pertenecientes a la versión dos o a una más reciente.

***Gatekeeper* Alterno:** Con el fin de proporcionar redundancia en el sistema que utiliza un Gatekeeper, este puede indicar *Gatekeepers* alternos que pueden ser utilizados en el caso de una falla en el Gatekeeper primario. Los usuarios están en capacidad de utilizar estos *Gatekeeper* alternos, si una petición hecha al Gatekeeper primario no es respondida o en otros casos configurados previamente por el administrador de la red.

Otras Características: Integración T.120/H.323, *Tunneling*, identificador de llamadas, reemplazo dinámico de canales, progreso del mensaje, conmutación remota lógica, entre otras características que han sido definidas como un respaldo a la calidad de servicio de VoIP, en particular a la telefonía IP.

3.3.2 Versión número tres. Esta versión de H.323 fue aprobada el 3 de Septiembre de 1999, la versión tres hace unas mejoras modestas a la versión dos, introduciendo solo algunas características al documento base. Sin embargo se progresó mucho en relación sobre todo a los nuevos anexos con respecto a H.323 y a H.225 que añaden un valor considerable a la arquitectura global de H.323.

Dentro de las mejoras y características en las que se hace hincapié en esta versión están:

Mantener y Volver a Usar Conexiones: Con el fin de proporcionar un mejor funcionamiento y de preservar los recursos del sistema, la versión tres introduce la habilidad para un dispositivo terminal de especificar si tiene la capacidad de volver a usar una conexión de señalización de llamada y si puede soportar el uso del mismo canal de señalización de llamada para llamadas múltiples. Estas características son de vital importancia para los *Gateway*, que pueden tener miles de llamada corriendo simultáneamente. Utilizando estas dos características el Gateway puede mantener una sola

conexión TCP entre el y el Gatekeeper con el propósito de ejecutar todas las señalizaciones de llamada.

Conferencia o sesión fuera de consulta: Para explicar esta característica, se propone este ejemplo, se realiza una llamada y un recepcionista contesta el teléfono. Como sucede típicamente, él colocara la llamada en espera mientras el llama a la persona con quien se desea comunicar. Luego el recepcionista conecta la llamada a otra parte, dejando en la línea a la persona que realizó la llamada y la que se estaba llamando únicamente. Este caso es introducido en la versión tres de H.323 y es llamado conferencia fuera de consulta.

Preferencia de Lenguaje: Con la versión H.323 las personas que llaman, tiene la capacidad de especificar un lenguaje de preferencia. Esta información es importante y puede ser utilizada en un centro de llamadas (*call center*), para ayudar a enrutar la llamada hacia un operador que pueda manejar el lenguaje especificado o también puede ser utilizado un sistema IVR (*interactive voice response*).

Otras Características: En los anexos creados en esta versión se resaltan características como el control remoto de dispositivos, capacidades genéricas, identificación de llamadas, diferentes clases de servicios complementarios, entre otras.

3.3.3 Versión número cuatro. Esta versión fue aprobada en Noviembre 17 del año 2000 y contiene mejoras en un número importante de áreas, incluyendo confiabilidad, escalabilidad y flexibilidad. Nuevas características ayudaran a facilitar la aplicación de soluciones por medio de *Gateways* y MCUs al creciente mercado de servicios requeridos por los usuarios. H.323 ha sido el líder indiscutible en el tratamiento e intercambio de voz, video y datos sobre redes de paquetes, y la versión cuatro da pasos agigantados para mantener a H.323 en la cabeza de la competencia.

Dentro de las características desarrolladas para las mejoras de H.323 en esta versión se encuentran las siguientes:

Gatekeeper Alternos: Uno de los más importantes aspectos en cualquier sistema telefónico es el tiempo productivo "*up-time*", los usuarios no permiten un sistema telefónico con fallas de servicio y los proveedores de servicios no quieren perder usuarios. Las fallas del *Gatekeeper* resultan algunas veces en llamadas perdidas, perdidas de facturación o ambas. Por lo tanto se ha intentado proveer redundancia de *Gatekeeper*, campo que ya fue introducido en la versión dos de H.323, pero la utilización de este campo nunca fue explicada de forma concisa, por lo tanto, la versión cuatro introduce una nueva sección que detalla los procedimientos que los dispositivos terminales deben seguir con el fin de proveer cierta robustez al sistema.

Transmisión de flujo multiplexado: Una debilidad con el uso actual de RTP es la dificultad al sincronizar el flujo de audio y video separado. La versión 4 incluye ahora un procedimiento opcional que permite a ambos video y audio ser multiplexado en un mismo flujo, esto ayudará a los dispositivos terminales en la sincronización de video y audio con el fin que la presentación de la información al usuario se observe de forma más natural

Ofrecimiento de llamada (H.450.10): Este servicio permite a un terminal que se encuentra llamando a otro terminal que se encuentra ocupado en el momento, la posibilidad de identificar que esta siendo llamado por otro terminal. Por lo tanto la llamada se establecerá una vez que el usuario ocupado la acepte.

Reportes de utilización: Para ayudar a proporcionar la información exacta para el servicio de facturación, el *Gatekeeper* puede pedir a los los dispositivos terminales que le proporcionen reporte de utilización de recursos varias veces durante una llamada, incluyendo al comienzo, durante y al final de la llamada. Esta nueva característica puede ser utilizada por los *Gatekeeper* alternos. Los reportes de utilización incluyen el tiempo de establecimiento y finalización de una llamada, la causa de la finalización y diferentes características que pueden diferenciar una llamada de otra.

Administración de ancho de banda: Una prioridad para la versión cuatro de H.323. Un dispositivo terminal puede demandar más ancho de banda del que

en realidad este necesitando, lo que causa que los recursos de la red sean desaprovechados. Con la versión cuatro, es ahora obligatorio que el dispositivo terminal realice peticiones de ancho de banda con un valor inferior si, ciertamente, el dispositivo terminal este utilizando menos ancho de banda que el indicado en el ARQ inicial.

Otras características: Dentro de esta versión se destaca entre otras características como: capacidad de los dispositivos terminales, nuevos servicios de identificación de llamadas, servicio de identificación de nombre (H.450.8), tonos y anuncios.

3.4 PROCEDIMIENTO DE CONEXIÓN

A continuación se describen los pasos involucrados en el establecimiento y finalización de una llamada H.323. La red utilizada en la descripción esta compuesta por dos terminales H.323 (T1 y T2) registrados a un mismo *Gatekeeper*. Se utiliza el método directo para el enrutamiento del canal de señalización de llamada (mensajes H.225) y para el enrutamiento del canal de control (Mensajes H.245). Se asume la encapsulación RTP para el flujo de medios.

Pasos.

1. El dispositivo terminal T1 envía una petición de acceso (RAS-ARQ), por medio del canal RAS al *Gatekeeper*. T1 solicita el uso del método de señalización de llamada en forma directa.

2. El *Gatekeeper* confirma el acceso de T1 enviándole un mensaje a ACF. El *Gatekeeper* en este mensaje le indica que puede utilizar la señalización de llamada en forma directa.

3. T1 envía un mensaje H.225 de señalización de llamada (establecimiento) a T2 solicitando una conexión.

4. T2 responde con un mensaje de proseguimiento de llamada.

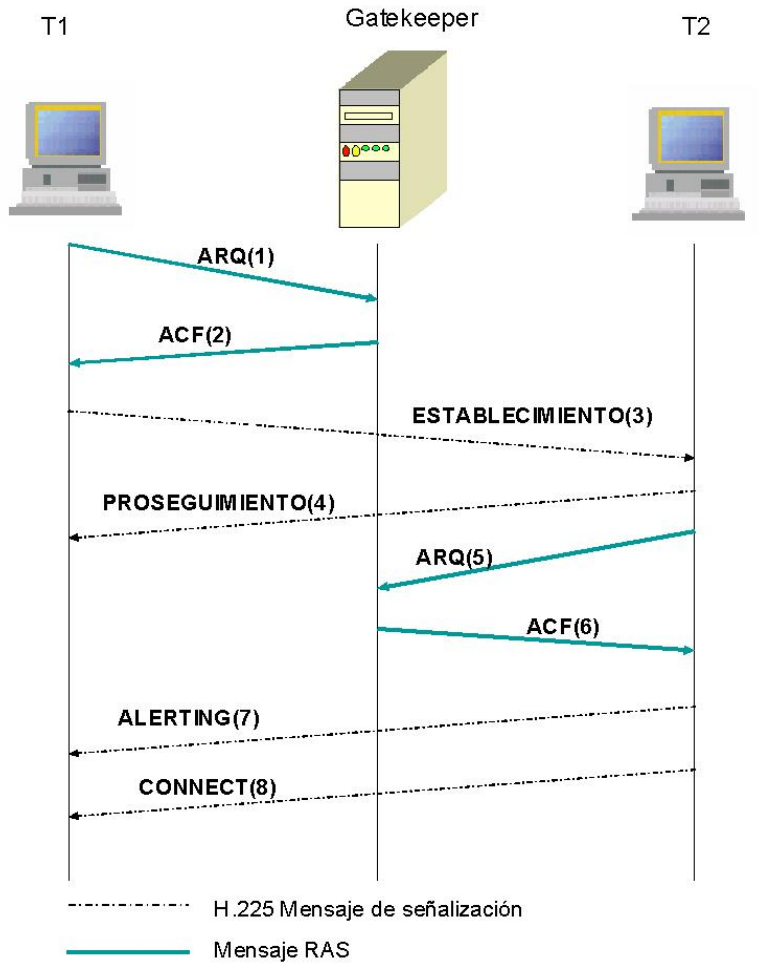
5. Ahora T2 debe registrarse con el *Gatekeeper*. Por lo cual envía una petición de acceso (RAS-ARQ) por medio del canal RAS al *Gatekeeper*.

6. El *Gatekeeper* confirma el acceso enviando un mensaje ACF a T2.

7. T2 alerta a T1 del establecimiento de la conexión enviándole un "*Alerting Message*".

8. Entonces T2 confirma el establecimiento de la conexión enviando a T1 un mensaje H.225 de conectado (*connect message*) y la llamada es establecida. Este mensaje contiene la dirección de transporte del canal de control H.245, que será utilizado para la señalización H.245

Figura 23. Establecimiento de Llamada H.323 (Pasos 1-8)



9. El canal de control H.245 es establecido entre T1 y T2. T1 envía un mensaje H.245 de conjunto de capacidades de terminal (H.245 *Terminal*

CapabilitySet message) a T2, iniciando así el intercambio de información sobre sus capacidades.

10. T2 envía un mensaje de reconocimiento de capacidades de T1, enviándole un mensaje H.245 de conjunto de capacidades de terminal recibido (H.245 *Terminal CapabilitySetAck message*).

11. T2 informa sus capacidades a T1 enviando un mensaje H.245 de conjunto de capacidades de terminal (H.245 *Terminal Capability Set message*).

12. T1 envía un mensaje de reconocimiento de capacidades de T2, enviándole un mensaje H.245 de conjunto de capacidades de terminal recibido (H.245 *Terminal Capability Set Ack message*)

13. T1 abre un canal (*media chane*l) con T2 enviando un mensaje H.245 de apertura de canal lógico (*Open Logical Chanel Message*). La dirección de transporte del canal RTCP es incluida en el mensaje

14. T2 reconoce el establecimiento del canal lógico unidireccional desde T1 a T2 enviando un mensaje H.245 *Open Logical Chanel Akc*. Incluida en este mensaje esta la dirección de transporte RTP asignada por T2, que será utilizada por T1 para el envío de flujos de audio (y/o video) RTP y la dirección RTCP recibida de T1anteriormente.

15. Luego, T2 abre un canal (*media chanel*) con T2 enviando un mensaje H.245 de apertura de canal lógico (*Open Logical Chanel Message*). La dirección de transporte del canal RTCP es incluida en el mensaje

16. T1 reconoce el establecimiento del canal lógico unidireccional desde T2 a T1 enviando un mensaje H.245 *Open Logical Chanel Akc*. Incluida en este mensaje esta la dirección de transporte RTP asignada por T1, que será utilizada por T2 para el envío de flujos de audio (y/o video) RTP y la dirección RTCP recibida de T2 anteriormente. En este momento la comunicación bidireccional de medios (audio y/o video) esta establecida.

- A partir de este momento los paquetes de audio (y/o video) pueden ser enviados a través del protocolo RTP, con el control del protocolo RTPC. En la figura 25 se muestra el flujo de los paquetes de audio (y/o video) y el flujo de control RTPC, como los pasos 17-20.

- Ya finalizado el intercambio de información entre T1 y T2, la llamada es finalizada. En este procedimiento se involucra el intercambio de mensajes H.225, H.245 y RAS. Se continúa con los pasos 21-25.

21. T2 inicia la desconexión, Este envía un mensaje H.245 *End Session Command* a T1.

22. T1 confirma la desconexión enviando un mensaje H.245 End Session Command a T2.

23. T2 completa la desconexión de la llamada enviando a T1 un mensaje H.225 Release complete a T1.

24. T1 y T2 se desconectan del *Gatekeeper*, enviando un mensaje RAS de petición de desconexión DRQ (*Disengage Request*).

25. El *Gatekeeper* desconecta T1 y T2 y lo confirma enviando un mensaje DCF (*Disengage Confirmation*).

Figura 24. Flujo de Señalización de Control H.323 (Pasos 9-16)

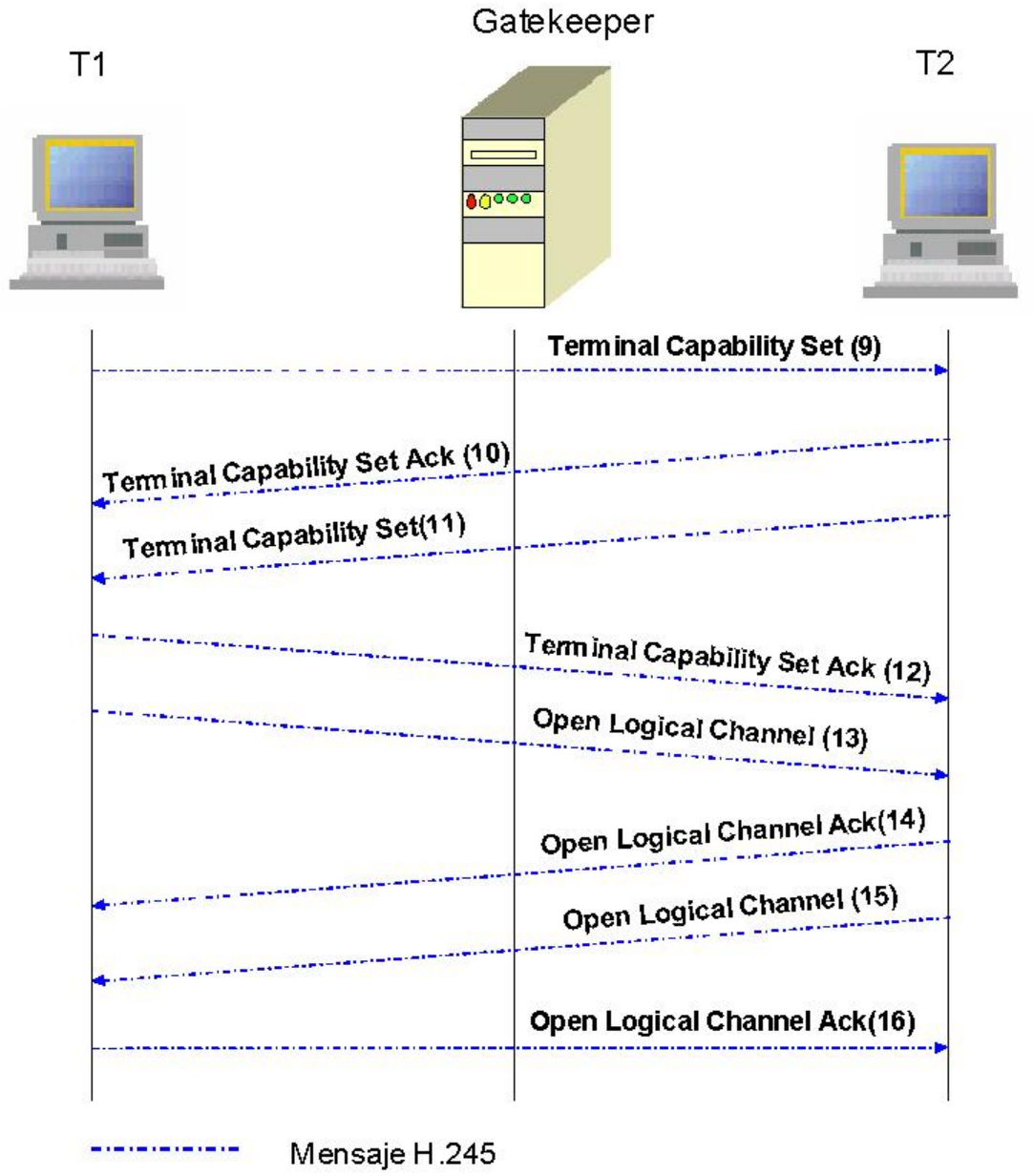


Figura 25. Flujo y Control de Medios (audio y/o video, pasos 17-20)

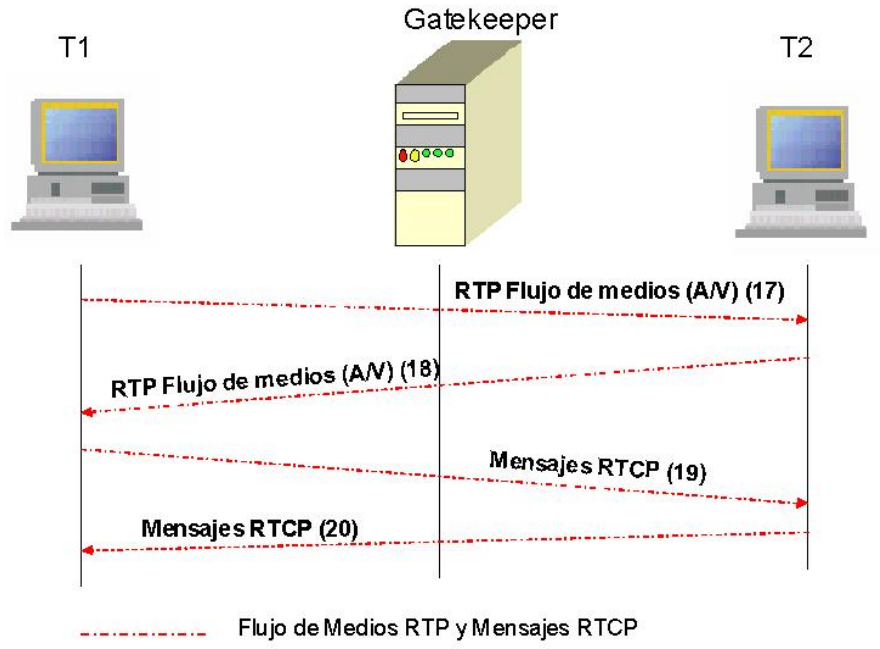
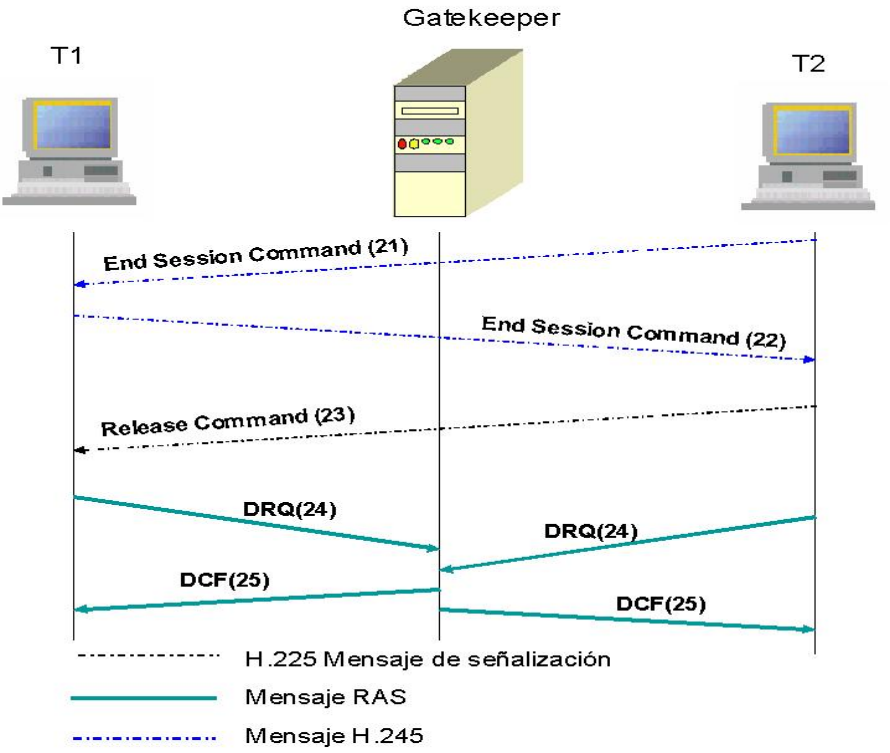


Figura 26. Finalización de la Llamada H.323



3.5 NUMERACION EN VoIP. ENUM

Dentro de VoIP se plantea una cuestión cuando se trata de integrar las redes de conmutación de circuitos con las redes de conmutación de paquetes, referente al direccionamiento de las llamadas que pasan de una red a la otra. En este sentido, sería deseable que existiera un único sistema integrado de numeración o direccionamiento global (plan de acceso de abonado).

En la actualidad las llamadas provenientes desde redes basadas en direcciones IP se terminan generalmente en otras redes (*PSTN*); sin embargo no es frecuente el caso contrario: terminar llamadas en redes IP. Esto conlleva a que el usuario llamado solo pueda utilizar terminales conectados a la red telefónica convencional, aunque cada vez existen más usuarios con conexión IP permanente (*always on*), vía cable o ADSL.

Para poder acceder a un usuario en una red basada en direcciones IP se requiere por tanto el desarrollo e implantación de algún tipo de esquema de direccionamiento/ numeración global, de tal manera que un usuario se pueda dirigir a otro a través tanto de la Red Telefónica Pública Conmutada (*PSTN*) como de la red IP.

Actualmente el Grupo de Estudios nº2 de la ITU (SG2) está estudiando un número de posibles opciones por las cuales los usuarios de redes basadas en

direcciones IP puedan ser accedidos desde redes *SCN*. Una posibilidad es asignar a los dispositivos IP recursos de numeración según la Rec. E.164 de ITU-T

Otro planteamiento potencial para la integración de los diferentes sistemas de acceso de abonado de la red *SCN* y de la basada en direcciones IP es el protocolo ENUM. Adoptado por la IETF, ENUM utiliza una arquitectura basada en un sistema de nombres de dominio (DNS) para asignar números telefónicos según la Rec. E.164 a direcciones Web o identificadores universales de recursos (URL). Como los números E.164 pueden sincronizarse con el DNS, el protocolo ENUM tiene, al parecer, importantes repercusiones para las administraciones a cargo de las políticas de numeración en lo que concierne a los "distintivos de país". El SG2 opina que las entidades administrativas, incluidos los administradores del DNS, deberían observar las recomendaciones aplicables vigentes del ITU-T referente a la inclusión de información de recursos E.164 en el DNS.

3.5.1 Identificación de usuario VoIP.

- NOMBRE: Etiqueta alfanumérica empleada como referencia al servicio por los usuarios finales. Es portable.
- NÚMERO : Cadena de dígitos decimales de un plan de numeración reconocido (E.164)

- DIRECCIÓN: Cadena de números, símbolos e información adicional que identifica puntos de terminación específicos en una conexión de redes. (E.164).

Fig. 27 Numeración E.164

Esquema de Numeración E.164

CC → Código de pais

NDC → Número de Area

El documento RFC 2916 proporciona una guía para el uso global de ENUM, y designa e164.arpa como el dominio exclusivo asociado a ENUM Global. Con ello se asegura el acceso a una única base de datos Internet de registros para la resolución de URLs.

El extremo con dirección ENUM puede ser tanto un terminal telefónico como un sitio web o una dirección de correo electrónico, según como esté definido en el nombre de dominio cualificado. La funcionalidad ENUM permite asociar a un número de teléfono los servicios o dispositivos que se quieran.

Como ejemplo de conversión a ENUM, se toma un número telefónico de 9 dígitos (mas el código del país). Para este caso se escoge el número +33 1 40

20 51 51, que corresponde a un número telefónico en Paris Francia. El proceso en ENUM para convertir este número de teléfono en una dirección de DNS es el siguiente:

- Quitar todos los caracteres numéricos con excepción del encabezado “+”
  Ejemplo: +33140205151

- Quitar todos los caracteres excepto los dígitos
  Ejemplo : 33140205151

- Colocar puntos entre cada uno de los dígitos
  Ejemplo: 3.3.1.4.0.2.0.5.1.5.1

- Invertir el orden de los dígitos
  Ejemplo: 1.5.1.5.0.2.0.4.1.3.3

- Se coloca al final el dominio de ENUM “e164.arpa”
  Ejemplo: 1.5.1.5.0.2.0.4.1.3.3.e164.arpa

El número de teléfono básico, en este ejemplo el 33 1 40 20 51 51, es la entrada. La salida es el Nombre de Dominio Totalmente Cualificado, que en este ejemplo es 1.5.1.5.0.2.0.4.1.3.3.e164.arpa, y puede usarse como DNS en las llamadas de telefonía IP.

- Por otro lado, una solución real al problema de direccionamiento y su posible escasez de rangos vendría dado con el despliegue de IPv6, al pasar el espacio de direccionamiento a 128 bits.

4. PROTOCOLO DE INICIO DE SESION (SIP)

SIP (*Session Initiation Protocol)* es un protocolo "cliente–servidor", similar a HTTP (*Hypertex Transfer Protocol*), utilizado para establecer, modificar y finalizar sesiones con uno o más participantes. De forma similar a la que un *browser* realiza peticiones a un servidor *web*, el cliente o usuario SIP realiza peticiones a una entidad receptora (servidor) que las procesa y luego, envía de regreso al cliente respuestas a su petición. Aun cuando SIP es similar a HTTP en la sintaxis y semántica, tiene características especiales que le permiten proporcionar el soporte necesario para el establecimiento y control de llamadas (VoIP).

4.1 DEFINICION

SIP fue desarrollado por la IETF (*Internet Engineering Task Force* [RFC 2543]). Es un protocolo de control que hace parte de la capa de aplicación, que esta en capacidad de establecer, modificar y finalizar sesiones con uno o más participantes. Las sesiones incluyen conferencias multimedia y llamadas telefónicas (Internet).

SIP soporta cinco aspectos básicos dentro del establecimiento y finalización una sesión:

- **Ubicación de usuario:** Determinación del dispositivo terminal que será usado para el establecimiento de la comunicación.

- **Disponibilidad de usuario:** Determinación de la disposición del usuario o cliente llamado para establecer la comunicación.

- **Capacidades de usuario:** Determinación del medio y de los parámetros del medio que serán utilizados.

- **Establecimiento de sesión:** Establecimiento de los parámetros de la sesión en ambas partes tanto el usuario que llama como el llamado.,

- **Manejo de sesión:** En esta faceta esta incluida la transferencia de información y la finalización de sesiones, la modificación de los parámetros de la sesión y servicios requeridos en la sesión.

4.2 ENTIDADES SIP

Dentro de SIP se definen dos tipos de entidades principales que son el Agente de Usuario (UA [*User Agent*]) y el servidor SIP. El agente de usuario es una entidad lógica y esta basado en dos componentes: el Cliente de Agente de Usuario (UAC [*User Agent Client*]) que esta encargado de enviar las peticiones SIP y el Servidor de Agente de Usuario (UAS [*User Agent Server*]) que esta encargado de responder las peticiones SIP. Mientras que el servidor SIP puede ser de dos tipos posibles: Servidor *Proxy* (*Proxy Server*), que es el único punto de contacto del UA para los mensajes de señalización, recibe peticiones de los clientes y los dirige a otros servidores o al cliente destino. Puede ramificar una petición de llamada hacia varias direcciones simultáneamente y el Servidor de Redireccionamiento (*Redirect Server*), acepta peticiones SIP y da a conocer la dirección del UA llamado, no interviniendo más en la sesión. La configuración básica del SIP consiste de al menos dos terminales (UA) conectados a una red de área local. Sin embargo, en aplicaciones prácticas es necesario añadir algunas de las otras entidades SIP con el fin de obtener un sistema de comunicaciones eficiente al estar conectado con el mundo exterior. Estas entidades brindan mayor funcionalidad a la red.

4.2.1 Agente de usuario (UA). Son los puntos finales (clientes o usuarios) que están en capacidad de recibir o establecer llamadas. Reciben y generan flujos

de información direccional en tiempo real. Un AU puede ser un *software* instalado en una computadora personal (PC) o un dispositivo *Hardware* dedicado a esta función. El UA debe estar en capacidad de soportar tráfico de voz, mientras que el tráfico de videos y de datos es una característica opcional.

Un caso especial dentro de esta entidad de SIP, son los *Gateways*, que son los que conectan la red SIP, con una red de conmutación de circuitos como la *PSTN*. El *Gateway* es implementado como un UAS que esta encargado de recibir y de establecer sesiones o llamadas de cada lado de la red y traducir el flujo de información asi como la información de control.

4.2.2 Servidores SIP. Las llamadas SIP son establecidas a través de estas entidades o dispositivos, que proveen resolución de direcciones y enrutamiento de llamadas. También pueden proporcionar servicios de seguridad y métodos de control del tráfico de la red a través del control de admisión y de la administración del ancho de banda.

Los servidores SIP, pueden funcionar como se aclaró anteriormente de dos formas como un Servidor *Proxy* o como un Servidor de Redireccionamiento, la diferencia entre ellos se identifica en la forma de responder a una petición si el usuario que es solicitado no se encuentra localizado en el servidor contactado. Un Servidor de Redireccionamiento informa al usuario que esta intentando establecer la sesión para que contacte otro servidor directamente. Un Servidor

Proxy contacta por sí mismo uno o más servidores interconectados a él y pasa la petición de inicio de sesión hacia delante. El Servidor *Proxy* debe mantener el estado de la llamada mientras que el Servidor de Redireccionamiento "olvida" la petición de establecimiento de sesión después de ser procesada. Conociendo estas características es aconsejable por lo tanto que los servidores SIP puedan operar de las dos formas.

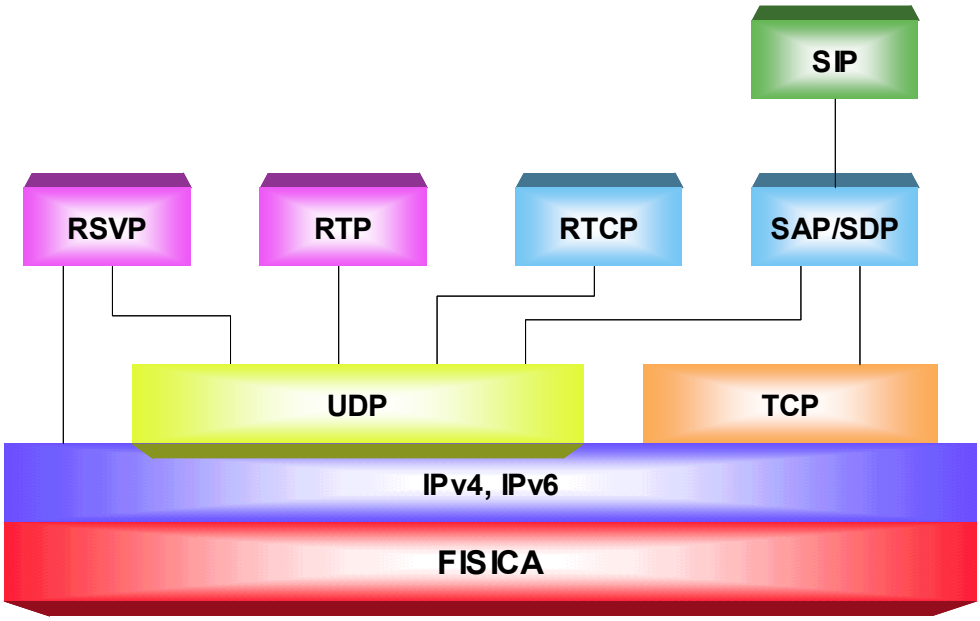
4.3 ARQUITECTURA

La funcionalidad de SIP esta concentrada en la señalización, SIP incluye como protocolo, señalización básica de las llamadas, ubicación de usuarios, registro y como una extensión incluye también características de señalización avanzadas. Los otros servicios como calidad de servicio, acceso a servicios de directorio, descripción del contenido de una sesión y control de sesiones son prestados por SIP, respaldado por otros protocolos. SIP tiene una arquitectura modular, en donde diferentes funciones son desarrolladas en diferentes protocolos.

SIP forma parte de la arquitectura global de datos multimedia y de control desarrollada por el IETF que incorpora protocolos como: RSVP (*Reservation Protocol* [4.9]) que es utilizado para la reserva de recursos de la red, RTP (*Real Time Transfer Protocol* [3.1.6]) que es utilizado para el trasporte de datos

en tiempo real y proporcionar un respaldo de QoS, RTSP (*Real Time Streaming Protocol* [4.10]) utilizado para el control de la entrega de flujos de medios (voz, datos, video), SAP (*Session Annunciation Protocol* [4.8]) usado para el anuncio de sesiones multicast y el SDP (*session description protocol [4.7]*) que se encarga de la descripción de las sesiones multimedia. SIP puede ser usado en conjunto con estos protocolos con el fin de brindar un mayor respaldo y servicios completos a los usuarios, sin embargo la funcionalidad y operación básica de SIP, no depende de ninguno de estos protocolos. En la figura 28 se observa la arquitectura de SIP en base a la pila de protocolos manejados.

Figura. 28 Pila de Protocolos SIP



4.3.1 Transporte de Flujo de Medios en Tiempo Real. SIP es utilizado sobre redes de paquetes que no proporcionan calidad de servicio (QoS), la telefonía y

las videoconferencias, son aplicaciones en tiempo real que requieren de muy poco retardo, asi como muy poca variación de retardo, también exigen que se manejen paquetes pequeños y con pequeñas cabeceras (*overhead*), además si se manejan datos en la red hay que agregar que estos requieren manejo de tiempo y sincronización. Por tal razón SIP, utiliza protocolos de transporte en tiempo real como el RTP y el RTCP definidos en el capitulo 3 y el protocolo RSVP definido en la sección 4.9 Que le permiten mantener y asegurar una calidad de servicio a los usuarios.

4.4 ESTRUCTURA DEL MENSAJE

Existen dos clases de mensajes SIP, solicitudes y respuestas. Los mensajes SIP utilizan la estructura de mensajes que se usa en HTTP (codificación en formato de texto). Una solicitud SIP comienza con una línea de inicio seguida por varios encabezados y opcionalmente un cuerpo de mensaje que puede contener una descripción de la sesión. La línea de inicio esta compuesta por el comando SIP, EL URI solicitado y la versión del protocolo SIP. Una respuesta SIP comienza con una línea de estado seguida de igual manera por varios campos de cabecera. La línea de estado esta compuesta por la versión del protocolo SIP, el código numérico de estado y la frase asociada con el código numérico de estado. El código de estado esta clasificado en seis clases

(similar a la codificación en HTTP): 1xx, 2xx, 3xx, 4xx, 5xx y 6xx, que serán definidas en la sección 4.11.

Los encabezados SIP, pueden estar divididos en cuatro grupos diferentes.

- Campo de encabezado general, que es aplicado a ambos tipos de mensajes: solicitudes y respuestas.
- Campo de encabezado de entidad, en este campo se define información acerca del cuerpo del mensaje o si en el mensaje no se ha establecido un cuerpo, en el mensaje se define entonces información acerca de los recursos identificados por la solicitud.
- Campo de encabezado de solicitud o petición, este campo actúa como modificador de la solicitud y permite que el usuario pase información adicional sobre la solicitud al servidor.
- Campo de encabezado de respuesta, permite al servidor pasar información adicional acerca de la respuesta, que no pudo ser colocada en la línea de estado.

SIP utiliza muchos de los campos de encabezado usados en HTTP, como lo son el encabezado de entidad y de autenticación. Esto es muy importante dentro de la estructura del protocolo ya que facilita la integración de los servidores SIP y los servidores *Web*.

SIP define seis comandos principales con el fin de establecer una llamada o una conexión:

Invite, invita un usuario a una sesión.

Bye, termina una conexión entre dos usuarios.

Options, señala información acerca de las capacidades (recursos).

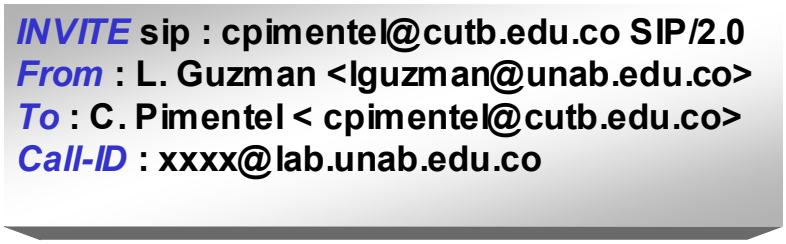
Status, informa al servidor acerca del progreso de la señalización.

Ack, es utilizado para el intercambio de mensajes confiables.

Register, da a conocer información de ubicación a un servidor SIP.

Dentro de un mensaje SIP, se destacan varios campos definidos de la siguiente manera: *"From"* es el campo de encabezado que transporta la fuente lógica de la llamada, la cual indica a la entidad que esta solicitando la llamada (el iniciador). La destinación lógica de la llamada esta contenida dentro del campo *"To",* esta nombra la parte a quien el iniciador desea contactar (el receptor). Cada llamada es identificada, esto se realiza por medio de un identificador único llamadas, que es cargado en el campo *"Call ID"*. El identificador de llamada es creado por el iniciador de la llamada y es usado por todos los participantes en esta. Consiste de un número que identifica la llamada y además puede Servir para procesos de facturación.

Figura. 29 Mensaje de invitación SIP



4.4.1 Establecimiento de Una Llamada SIP. El establecimiento de una llamada de forma exitosa, consiste de una solicitud de invitación (*INVITE*) de un usuario y una respuesta *Ack* desde el terminal que ha sido llamado. Una respuesta negativa puede ser enviada con una contestación *BYE*. La solicitud de invitación usualmente contiene una descripción de la sesión, escrita en el formato SDP. En la descripción de la sesión se proporciona información acerca de que características y formato de medios soporta el cliente o usuario.

La invitación puede pasar por varios servidores mientras va camino al usuario llamado. Estos servidores como se especifico anteriormente son de tres tipos, el Servidor *Proxy*, que recibe la solicitud y la remite hacia la ubicación del usuario llamado. Puede también remitir la solicitud hacia múltiples servidores a la vez con el fin de contactar al usuario en una de las localizaciones, o para un grupo *multicast*. El Servidor de Redireccionamiento solo informa al usuario que realiza la invitación sobre hacia donde debe dirigirse y el usuario envía una nueva solicitud al receptor (usuario llamado) directamente. El UAS reside en el *host* donde el usuario esta situado e informa al usuario acerca de las llamadas y espera por una respuesta de que hacer: aceptar, rechazar o seguir (ignorar).

En un sistema SIP también se pueden incluir servidores de ubicación, que mantienen una base de datos de las ubicaciones de los usuarios. Esto permitirá a los usuarios moverse entre un número de diferentes sistemas finales con el transcurso del tiempo. Los servidores de ubicación envían mensajes de registro (*Register*) a los servidores para informar a cerca de cambios.

Cuando el usuario llamado ha sido contactado, envía una respuesta al usuario que inicia la llamada la cual consiste como se explico anteriormente en una línea de estado compuesta entre otros campos (sección 4.3) por un código numérico de estado de tres dígitos jerárquica mente organizado, clasificado en seis clases: 1xx, esta clase indica el progreso de llamada y siempre va estar seguido por otras respuestas indicando el resultado final. 2xx, esta clase indica mensaje exitoso (200 *OK*). 3xx, indica reexpedición, 4xx, 5xx, 6xx, indican fallas del cliente, servidor y globales respectivamente. Las respuestas son siempre enviadas a la entidad que enviaba el mensaje al servidor, no al creador de la solicitud.

Una respuesta positiva, a un mensaje de establecimiento, contiene además una descripción de sesión, describiendo los tipos de medio soportados. Los identificadores de llamada son utilizados para indicar los mensajes pertenecientes a la misma sesión.

4.4.2 Intercambio de Capacidades. Para realizar este procedimiento SIP, utiliza SDP con el fin de describir las capacidades (recursos), el intercambio de capacidades en SIP es simple, el usuario que inicia la llamada proporciona una lista de las características y tipos de medio que soporta y el usuario llamado escoge de la lista cuales soporta y envía un mensaje SDP de regreso. SIP puede utilizar cualquier protocolo de descripción de sesión incluido H.245 (sección 3.1.5).

Se debe tener en cuenta que los parámetros de los medios pueden cambiar durante la sesión, SIP realiza esto enviando un nuevo mensaje de invitación con una nueva descripción de medios.

Como se logra apreciar SIP, se vale de un proceso muy simple para cumplir con el intercambio de capacidades de los UA, por medio de una lista de los recursos disponible que se envía de un UA a otro.

4.5 FLUJO DE MEDIOS (AUDIO, VIDEOS, DATOS)

4.5.1 *Codecs* de audio. En este campo SIP, recomienda un conjunto mínimo de *codecs* de audio para un UA, este conjunto consiste de los *codecs,* G. 711, GSM y DIV 14. El soporte de otros *codecs* es opcional y se haría con el fin de brindar mayor soporte a las transmisiones de audio lo que garantizaría una mayor calidad de servicio (QoS).

4.5.2 *Codecs* de Video. La función que desempeñan estos *codecs* es la de manejar y codificar el video proveniente de la cámara para la transmisión del UA que se encuentra enviando información, decodificar el video que se recibe y que es enviado al reproductor de video en el UA que recibe la información. SIP especifica el soporte de video de manera opcional, por lo tanto no es vital para

una red SIP que maneja únicamente VoIP. Sin embargo cualquier UA qué desee comunicación de video, debe soportar los codificadores y decodificadores de video especificados en la recomendación ITU-T H.261.

4.5.3 Canales de Datos. Los canales de datos son tratados en aplicaciones multipunto de tiempo real, como la transferencia de archivos, realidad virtual y juegos en los que participan múltiples jugadores. SIP puede establecer comunicaciones de datos por medio de la especificación T.120 o cualquier otra especificación. SIP no especifica cual protocolo o especificación debe ser utilizado para los canales de datos.

4.6 SESIONES (CONFERENCIAS) MULTIPUNTO

En SIP las conferencias multipuntos, se pueden agrupar de tres formas: conferencias *multicats* (M*ulticast Conferences*), conferencias unidas (*bridged conferences*) y conferencias de malla completa *(full-mesh conferences*). Las conferencias de malla completa son descentralizadas (Capitulo 3 [MCU]), donde cada participante envía la información hacia cada uno de los otros participantes y la información o el flujo de información que se recibe es tratado o manejado localmente. Este método es adecuado para conferencias en donde participen tres o más UA. En las Conferencias unidas, cada usuario esta

conectado a un puente que mezcla el flujo de información de cada uno de los usuarios y luego transmite el flujo resultante. Las conferencias *multicast* ofrecen un método más eficiente con respecto al ancho de banda, este tipo de conferencias puede ser utilizada en redes que soporten trafico *multicast*.

En la práctica estos métodos son combinados, En las conferencias los UA que se encuentran en la red que permita *multicast*, utilizan el método *multicast*. Los UA buscan de forma automática las características de cada uno de ellos e identifican cuales tiene la capacidad de *multicast*, luego se invita a estos que tiene la capacidad de *multicast* a un grupo *multicast*. Los UA que no posean esta capacidad continuaran utilizando *unicast*, Los UA que entren nuevos en una conferencia siempre lo harán el modo *unicast*.

4.6.1 Señalización *Multicast*. SIP al igual que otros protocolos puede utilizar las capacidades *multicast* de la red para la transmisión de flujos de información; Pero la técnica de señalización *multicast* es únicamente soportada dentro de los protocolos y estándares de VoIP por SIP. Un usuario puede enviar una solicitud por medios *multicast* a un grupo de receptores para alcanzar a todos o para alguno de los miembros, en el segundo caso la conexión es establecida entre el usuario que envía la solicitud o petición y el primer de los miembros en responder. Las conferencias *multicast* pueden ser anunciadas. SIP utiliza un protocolo especial para el anuncio de las conferencias *multicast*, este protocolo es el SAP.

4.7 PROTOCOLO DE DESCRIPCIÓN DE SESION (SDP)

Este protocolo fue desarrollado expresamente para la descripción de sesiones multimedia para propósitos de anuncio de sesión, invitación de sesión y otras formas de iniciación de sesiones multimedia. La carga útil (*payload*) de los mensajes SIP puede ser SDP. SDP también puede ser utilizado por otros protocolos como SAP. SDP proporciona un medio para transportar suficiente información con el fin de permitir que los usuarios se unan y participen en la sesión.

La carga útil de SDP, incluye:

- Nombre y propósito de la sesión.
- Tiempo de duración de la sesión.
- Los Medios que comprenden la sesión (audio, video, datos)
- Información para recibir estos medios (puertos, direcciones, formatos, etc.)

Como los recursos necesarios para participar en una sesión pueden ser limitados, SDP puede proporcionar información adicional como:

- El ancho de banda que será usado en la sesión.

- Información para contactar a la persona responsable de la sesión.

El tiempo de duración de una sesión puede ser limitado o ilimitado, independientemente de esta característica una sesión puede ser activada únicamente a horas específica. La información de medios que se transporta en SDP, es muy completa. Este describe el tipo de medio (por ejemplo audio), el protocolo de transporte utilizado, el formato del medio (MPEG video), la dirección IP a contactar, el puerto a contactar y finalmente información especifica del medio (por ejemplo descripción del ancho de banda).

El contenido de SDP, esta constituido por campos o líneas de texto con la siguiente estructura:

<Tipos de Campo> = < Valor>

Los tipos de campos están estructurados de tres formas : el campo de descripción de sesión, que describe la sesión en general, el campo de descripción de tiempo, que esta encargado de describir específicamente el registro del tiempo y el campo de descripción de los medios, que describe el tipo de medio que es transportado en la sesión.

Tabla 3. Campos de Descripción de Tiempo.

Field Name	Descripción
t	Tiempo en que la sesión esta activa
r*	tiempos de repetición

Tabla 4. Campos de Descripción de Medios

Field Name	Descripción
m	Nombre de medios y dir. de transporte
i*	Material multimedia
c*	Información de conexión
b*	Información de ancho de banda
a*	Atributos de los medios

Tabla 5. Campos Principales Que Puede Contener Un Mensaje Con Cuerpo SDP.

Field Name	Descripción
v	Versión del Protocolo
o	Creador e identificador de sesión
s	Nombre de la sesión
i*	Información de la sesión
u*	Descripción de URI
e*	Dirección de e-mail
p*	Numero telefónico
c*	Información de conexión
b*	Información de ancho de banda
z*	Zona de ajuste de tiempo

Figura. 30 Ejemplo de Mensaje SIP *INVITE* Con Cuerpo SDP

```
INVITE sip:cpimentel@cutb.edu.co SIP/2.0
From: L. Guzman <lguzman@unab.edu.co>
To: C. Pimentel < cpimentel@cutb.edu.co>
Call-ID: xxxx@lab.unab.edu.co


v=0
o=lguzzy 810120790921 800217 IN IP4 128.10.20.30
c=IN IP4 140.170.67.20
m=audio 500 RTP/AVP 0
```

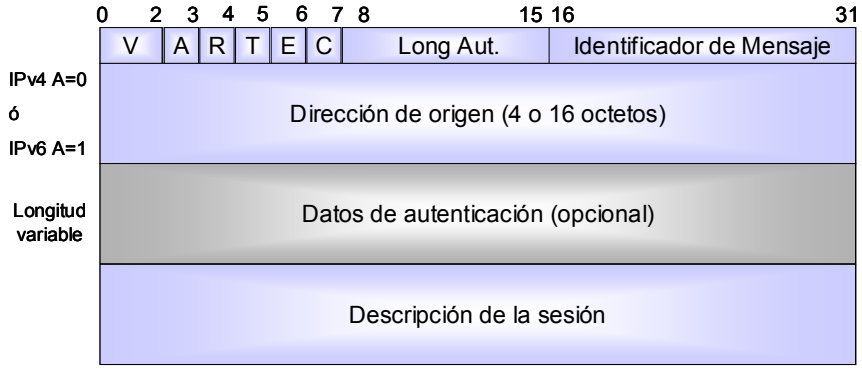
Dentro de este mensaje, el campo “o”, como se observa esta compuesto por seis sub-campos: el primero es el *login* del usuario en el *host* que envía el mensaje (lguzzy), El segundo es el identificador de sesión (810120790921), el tercero es el número de la versión para esta sesión (este cambia con los cambios que se puedan realizar a la sesión), el cuarto es el tipo de red (IN, que es la identificación de Internet, no para red inteligente [IN]), el quinto es el tipo de dirección (IP4), que en este caso es IP versión 4, finalmente el sexto es la dirección de la maquina en la cual la sesión fue creada. El campo “c” tiene la misma estructura que el campo “o” (tipo de red, tipo de dirección y dirección de conexión). El campo “m”, describe el tipo de medio que será transportado en la sesión, está formado por cuatro sub-campos, el primero es el tipo de medio (en este caso es audio, pero otros tipos son definidos dentro de este, como video, aplicación, etc.), el segundo es el puerto de transporte a utilizar, existe la posibilidad de especificar múltiples puertos, el tercer sub-campo es para especificar el protocolo de trasporte. Este sub-campo tiene una relación directa

con el sub-campo de tipo de dirección en el campo“c”. De tal forma que el sub-campo “c” de IP4 significa que el protocolo de transporte corre sobre IPv4, con perfil para sonido y vídeo (RTP/AVP), sonido en formato PCM de ley μ (tipo de datos 0).

4.8 PROTOCOLO DE ANUNCIO DE SESION (SAP)

El protocolo de anuncio de sesión (SAP), es uno de los protocolos mas simples desarrollados para el anuncio de sesiones *multicast***,** con la utilización de este protocolo, el usuario que establece la sesión multicast, simplemente envía paquetes de forma *multicast* hacia un grupo *multicast* transportando en ellos una descripción SDP, de la sesión que se establecerá. Los usuarios que deseen conocer que sesión será activada solo deben “escuchar” en dirección al grupo multicast al cual se están enviando los anuncios de sesión y recibir estos paquetes de anuncio, con el fin de activar las herramientas necesarias para poder participar en la sesión que será activada. En pocas palabras este es el principio básico del funcionamiento de SAP, claro está que el protocolo se torna un poco mas complejo cuando se le agregan características como por ejemplo seguridad.

Figura. 31 Estructura de los Anuncios SAP.



Los bits del 0-2 conforman el campo que identifica a la versión, el bit “R” es un campo reservado cuyo valor debe ser 0, el bit “T” indica si el anuncio corresponde a la creación de una sesión (valor 1), o se trata de una solicitud de eliminación de un anuncio previo (valor 0), el bit “C” indica si el contenido del anuncio está o no comprimido, el bit “A” indica el tipo de versión IP que se está utilizando (0 = IPv4 y 1= IPv6) , el bit “E” indica si el anuncio SAP esta o no codificado, la codificación de los anuncios SAP, no se recomienda, dado que los escenarios en los que se puede necesitar probablemente requieren otros mecanismos de anuncio, de este modo se evita el desperdicio de ancho de banda que puede suponer transmitir anuncios codificados que algunos receptores no están en capacidad de descifrar. Los bits R, A y T en conjunto conforman el campo “MT”, tipo de mensaje.

4.9 RSVP (*RESOURCE RESERVATION PROTOCOL*)

RSVP es un protocolo de control de red que aporta calidad de servicio (QoS) *end to end* a un flujo de datos IP. Las aplicaciones de comunicaciones en tiempo real reservan los recursos necesarios de encaminamiento, de tal manera que durante la transmisión pueda ser disponible el ancho de banda necesario. Es una solución distribuida, que permite a múltiples receptores de diferentes características efectuar reservas específicamente dimensionadas a sus propias necesidades.

Cuando el receptor de datos requiere una calidad de servicio específica, utiliza RSVP para solicitar reserva de recursos a los enrutadores a lo largo del trayecto de los datos. El protocolo negocia los parámetros de conexión con los enrutadores y mantiene los estados de éstos y de los *host*. El modo de atribución de recursos tiene la ventaja de que, al ser efectuado por el receptor, puede demandar una QoS adecuada a sus necesidades y al consumo deseado, por lo que se puede garantizar una QoS.

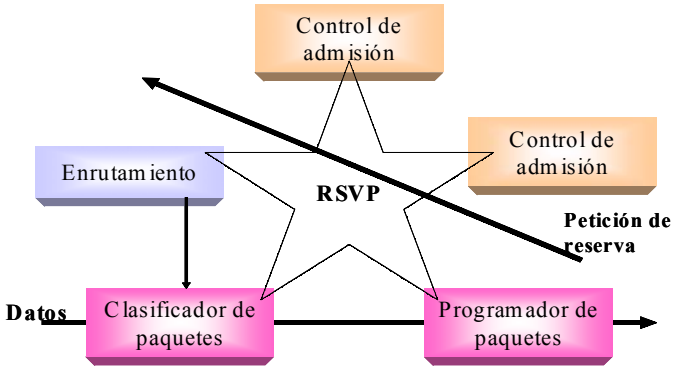
RSVP no es un protocolo de enrutamiento, pues en el proceso de reserva no transmite los datos simultáneamente, y exige que los sistemas terminales funcionen en modo conectado. Sin embargo, para garantizar un ancho de banda determinado debe conocer previamente a donde dirigir las peticiones de reserva de recursos. Los flujos se transmiten en modo *simplex*, es decir, que

solamente reserva recursos para transmisión en un sentido (hacia el receptor que solicita la reserva).

En la figura 32 se resumen los procedimientos que utiliza el protocolo para reserva y estado de los recursos. Se aprecian dos caminos: uno de petición de reserva y otro en sentido contrario de envío de mensajes que indican el trayecto a seguir por los datos para que el receptor (o los receptores, pues los mensajes se pueden enviar en modo *multicast*) pueda determinar los recursos que se deben reservar, según el trayecto seguido desde el origen de los datos. El control de usuarios incluye los permisos de acceso y autenticación. El control de admisión se refiere al control de los recursos necesarios para suministrar la calidad de servicio (QoS) solicitada.

RSVP comprueba el estado de los procedimientos de control de usuarios y admisión, y si son válidos manda los parámetros correspondientes al clasificador de paquetes (para ordenarlos según prioridad) y al programador de paquetes (para transmitirlos una vez clasificados). También se comunica con el proceso de enrutamiento para determinar el trayecto por medio del cual se enviarán sus peticiones de reserva, manejo de usuarios y rutas.

Figura. 32 Procedimientos de RSVP



Al ser RSVP un protocolo diseñado para multicast, los receptores que inician la petición de reserva pueden cambiar dentro de un grupo, y también las rutas reservadas pueden ser modificadas sin gran sobrecarga para el emisor.

En definitiva, RSVP está orientado a recepción, es compatible con IPv6 y se acondiciona sin dificultad a diferentes calidades de servicio requeridas para un mismo emisor.

4.10 RSTP (*REAL TIME STREAMING PROTOCOL*)

RTSP es un protocolo de nivel de aplicación, utilizado principalmente para el control en la entrega de los flujos de medios en tiempo real. Fue diseñado para trabajar con medios sensibles al tiempo, fundamentalmente con los flujos de

video y de audio y donde existan las aplicaciones de tiempo real. Al igual que SIP, RTSP es muy similar en estructura y operación a HTTP.

4.11 PROCEDIMIENTO DE ESTABLECIMIENTO DE UNA LLAMADA SIP: SOLICITUD, RESPUESTA, SESION.

Para establecer una llamada SIP, el paso más importante es enviar una solicitud de establecimiento de llamada a un usuario (*INVITE*). Para realizar la invitación, el usuario que solicita el establecimiento de la llamada debe obtener la dirección del usuario a llamar (comúnmente, nombre@dominio). Después de obtenerla el usuario envía un mensaje *INVITE*. Con el fin de que este proceso de establecimiento de llamada pueda llevarse acabo, el usuario llamado, debe estar registrado o se debe registrar con su servidor local, en este proceso de registro entran en función los protocolos TCP o UDP.

El proceso de registro en el servidor SIP por parte del usuario llamado es realizado por medio del siguiente mensaje SIP (mensaje de solicitud de registro SIP).

- Con el fin de explicar el proceso de establecimiento de la llamada, se hará uso de dos usuarios SIP, el usuario que solicita el establecimiento de la llamada, que se representara por medio de L. Guzmán

(lguzman@unab.edu.co) y el usuario llamado que se representara por medio de C. Pimentel (cpimentel@cutb.edu.co).

REGISTER sip:cutb.edu.co SIP/2.0
Via: SIP/2.0/UDP lab.cutb.edu.co
From: C. Pimentel <sip:cpimentel@ cutb.edu.co >
To: C. Pimentel < sip:cpimentel@ cutb.edu.co>
Call-ID: xxxxxx@lab.cutb.edu.co
CSeq: 1 *REGISTER*
Contact: <sip:cpimentel@ lab.cutb.edu.co:5000;*transport*=udp>
Expires: xxxx

En este procedimiento de registro, C. Pimentel, esta utilizando el terminal SIP o UA (teléfono o computador) lab.cutb.edu.co, y se registra a su servidor local cutb.edu.co. (Servidor de Ubicación a la vez).

Como se observa el mensaje de registro esta compuesto por varios campos, el primero es la línea de inicio, (sección 4.4), esta línea está seguida de varios campos de encabezado que transportan la siguiente información:

- **Via**, contiene la dirección del terminal utilizado (lab.cutb.edu.co) y el protocolo de transporte utilizado (UDP). Utilizado para indicar a las otras entidades donde enviar las repuestas.

- ***From***, contiene el nombre que se despliega (C. Pimentel) y la URI SIP (sip:cpimentel@ cutb.edu.co) que indica al usuario que inicia la solicitud.

- ***To***, contiene al igual que *from*, el nombre que se despliega (C. Pimentel) y la URI SIP (sip:cpimentel@ cutb.edu.co) que indica el usuario al que se dirige la solicitud, en este caso coincide con el campo *from*, por ser un mensaje de registro.

- ***Call-ID***, contiene un número que identifica la llamada (xxxx), creado por el usuario que envía la solicitud, además de la dirección del UA que está utilizando (lab.cutb.edu.co), para este caso se escogerá como numero dentro de *call-ID* el siguiente (20031015).

- ***CSeq***, (Comando de Secuencia), contiene un número entero y el nombre de un código, el número en este comando es incrementado por cada nueva petición y el código identifica que clase de solicitud se esta realizando,

- ***Contact****,* contiene la URI SIP (cpimentel@ lab.cutb.edu.co) que representa una ruta directa para contactar el usuario que envía la solicitud. (en este caso C. Pimentel)

- ***Expires***, indica el tiempo de vida (xxxxx) del registro en el servidor, el tiempo está especificado en segundos. para este caso se escogerá un tiempo de vida de 5 Horas (1800).

Con estas características el mensaje de registro queda entonces definido de la siguiente forma:

REGISTER sip:cutb.edu.co SIP/2.0
Via: SIP/2.0/UDP lab.cutb.edu.co
From: C. Pimentel <sip:cpimentel@ cutb.edu.co >
To: C. Pimentel < sip:cpimentel@ cutb.edu.co>
Call-ID: 20031015@lab.cutb.edu.co
CSeq: 1 *REGISTER*
Contact: <sip:cpimentel@ lab.cutb.edu.co:5000;*transport*=udp>
Expires: 1800

Por lo tanto, el registro define que expira en 5 horas, cualquier solicitud futura para cpimentel@ cutb.edu.co será redireccionada hacia lab.cutb.edu.co, el puerto del terminal es el 5000 y el protocolo de transporte es el UDP.

Desde este momento si se puede proceder con el establecimiento de la llamada, que comienza con la solicitud (I*NVITE*), la respuesta, la sesión y la finalización.

1. L. Guzmán solicita el establecimiento de una llamada a C. Pimentel, por medio del siguiente mensaje de solicitud SIP (*INVITATION*).

INVITE sip:cpimentel@ cutb.edu.co SIP/2.
From: L. Guzman <sip:lguzman@unab.edu.co>

To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20030108@off.unab.edu.co

El mensaje de solicitud se enviará al servidor que corresponde al próximo salto del servidor local de L. Guzman (unab.edu.co), que puede ser *Proxy* o de Redireccionamiento, para este caso se escogió un servidor *Proxy*. Que contacta por si mismo a otro servidor interconectado a él (cutb.edu.co) y pasa la petición de establecimiento de llamada hacia delante [2], el servidor (cutb.edu.co) localiza al usuario requerido (C. Pimentel) y envía su dirección (cpimentel@lab.cutb.edu.co) al servidor Proxy [3], que a la vez envía la solicitud de establecimiento de llamada hacia el usuario llamado [4], para lograr esto, el servidor *Proxy*, cambia el campo *INVITE*, con la dirección obtenida del servidor cutb.edu.co. (dirección de contacto del usuario llamado) El mensaje que llega al usuario es el siguiente.

INVITE sip:cpimentel@ lab.cutb.edu.co SIP/2.
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20030108@off.unab.edu.co

5. Ya resuelta, la dirección del usuario llamado (C. Pimentel) y el mensaje ha llegado exitosamente a él, este envía su dirección IP al usuario que intenta establecer la llamada (L. Guzman). Por medio del siguiente mensaje.

200 OK
From: C. Pimentel <sip: cpimentel@ cutb.edu.co >
To: L. Guzman <sip:lguzman@unab.edu.co>

Call-ID: 20030108@off.unab.edu.co

6. El próximo mensaje es el acuso de recibo (de L. Guzman a C. Pimentel), que se envía por medio del servidor *Proxy*.

ACK sip: cpimentel@ cutb.edu.co
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20030108@off.unab.edu.co

7. El servidor *Proxy*, envía el acuso de recibo a C. Pimentel

ACK sip: cpimentel@ lab.cutb.edu.co
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20030108@off.unab.edu.co

8. El usuario llamado (C. Pimentel), envía un mensaje a el usuario que intenta establecer la llamada (L. Guzman) que indica que el acuso de recibo llego exitosamente. Se ha establecido la llamada y se inicia la sesión.

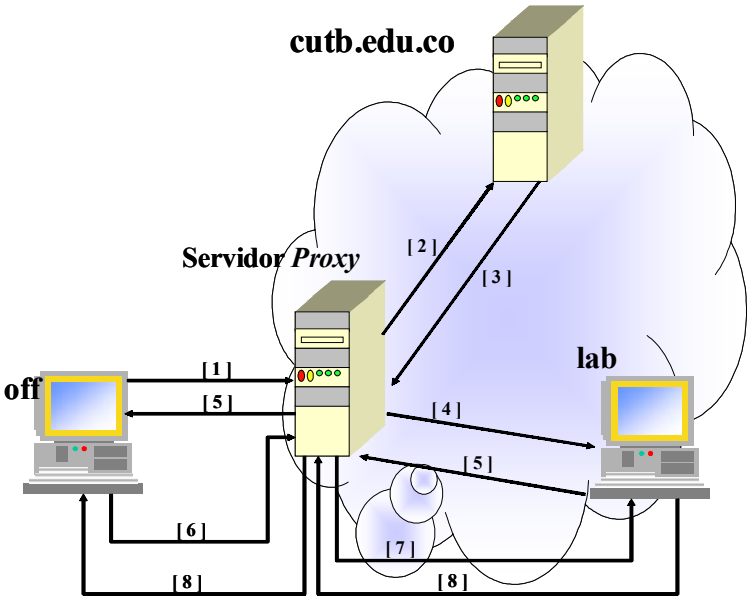
200 OK
From: C. Pimentel <sip: cpimentel@ cutb.edu.co >
To: L. Guzman <sip:lguzman@unab.edu.co>
Call-ID: 20030108@off.unab.edu.co

9. Para terminar la sesión se envía un mensaje *BYE¸* en este caso L. Guzman

finaliza la sesión, envía el mensaje a C. Pimentel.

BYE sip:cpimentel@ cutb.edu.co SIP/2.
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20030108@off.unab.edu.co

Figura. 33 Establecimiento de Llamada SIP (Servidor *Proxy)*



Con el fin de ilustrar una de las características de SIP, como es la de la posibilidad de que el usuario tenga movilidad, se desarrolla el siguiente caso de establecimiento de llamada.

Con los mismos usuarios especificados en el caso anterior (L. Guzman y C. Pimentel), con la misma acción para cada uno de ellos, es decir, L. Guzman es el usuario que inicia el establecimiento de la llamada y C. Pimentel es el usuario llamado; pero la particularidad del ejemplo es que ahora se utilizara un Servidor de Redireccionamiento en vez de un servidor *Proxy* y se tomara el caso en que el usuario llamado a cambia de sitio.

Para el desarrollo de este caso, el usuario C. Pimentel se trasladará a su casa (servidor, casa.com). Pero para que cualquier petición que se dirija a C. Pimentel pueda llegarle en su nueva ubicación, el usuario debe primero y antes que nada cancelar cualquier ubicación existente [1], luego debe actualizar su registro [2].

1. Este mensaje cancela cualquier ubicación existente.

REGISTER sip:cutb.edu.co SIP/2.0
Via: SIP/2.0/UDP lab.cutb.edu.co
From: C. Pimentel <sip:cpimentel@ cutb.edu.co >
To: C. Pimentel < sip:cpimentel@ cutb.edu.co>
Call-ID: 20031015@lab.cutb.edu.co
CSeq: 2 *REGISTER*
Contact: *
Expires: 0

2. Este mensaje crea un nuevo registro.

REGISTER sip:cutb.edu.co SIP/2.0
Via: SIP/2.0/UDP comp1.casa.com
From: C. Pimentel <sip:cpimentel@ cutb.edu.co >
To: C. Pimentel < sip:cpimentel@ cutb.edu.co>
Call-ID: 20031015@comp1.casa.com
CSeq: 3 *REGISTER*
Contact: <sip:cpimentel@ comp1.casa.com:5000;*transport*=udp>
Expires: 1800

Ahora el servidor (cutb.edu.co), enviará cualquier solicitud para C. Pimentel al servidor casa.com. Para que el servidor casa.com pueda reconocer y hacer llegar las peticiones para C. Pimentel este deberá registrarse a él por medio de un mensaje *REGISTER*.

Con todos los registros establecidos, se inicia un proceso de solicitud de establecimiento de llamada de parte del usuario L. Guzman hacia el usuario C. Pimentel, esto se realiza en el modo de redirrecionamiento.

[1] INVITE sip:cpimentel@ cutb.edu.co SIP/2.
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20032001@off.unab.edu.co

El mensaje de solicitud se enviará al servidor que corresponde al próximo salto del servidor local de L. Guzman (unab.edu.co), en este caso un servidor de

redireccionamiento. Que contacta a otro servidor interconectado (cutb.edu.co [servidor de ubicación]) y pasa la petición de establecimiento de llamada hacia delante [2], el servidor (cutb.edu.co) localiza al usuario requerido (C. Pimentel) y envía su dirección (cpimentel@comp1.casa.com) al servidor de redirrecionamiento [3], este envía esta dirección del usuario que se desea contactar (C. Pimentel) al usuario que intenta establecer la llamada (L. Guzman)[4] y no interviene mas en el proceso, mientras que la llamada se establece directamente entre los dos usuarios. El mensaje enviado a L. Guzman es el siguiente.

[4] SIP/2.0 302 *Moved temporarily*
Via: SIP/2.0/UDP off.unab.edu.co
From: L. Guzman <sip:lguzman@unab.edu.co
To: C. Pimentel < sip:cpimentel@ cutb.edu.co>
Call-ID: 20032001@comp1.casa.com
CSeq: 1 *INVITE*
Contact : <sip:cpimentel@ comp1.casa.com:5000; *transport*=udp>

5. L. Guzman envía el mensaje *INVITE*, para el establecimiento de la llamada al usuario C. Pimentel directamente,

INVITE sip:cpimentel@ comp1.casa.com SIP/2.
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20032001@off.unab.edu.co

6. El usuario llamado (C. Pimentel), envía un mensaje ACK a el usuario que intenta establecer la llamada (L. Guzman) que indica que su mensaje de establecimiento de llamada llego exitosamente.

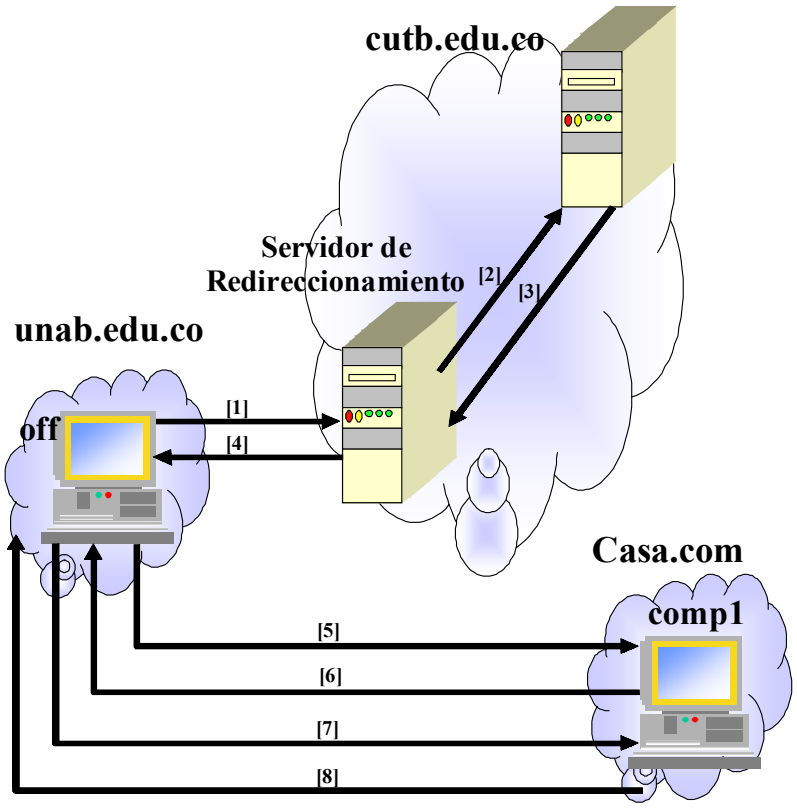
200 OK
From: C. Pimentel <sip: cpimentel@ cutb.edu.co >
To: L. Guzman <sip:lguzman@unab.edu.co>
Call-ID: 20032001@comp1.casa.com
7. El próximo mensaje es el acuso de recibo. (de L. Guzman a C. Pimentel)

ACK sip: cpimentel@ comp1.casa.com
From: L. Guzman <sip:lguzman@unab.edu.co>
To: C. Pimentel <sip: cpimentel@ cutb.edu.co >
Call-ID: 20032001@off.unab.edu.co

8. El usuario llamado (C. Pimentel), envía un mensaje a el usuario que intenta establecer la llamada (L. Guzman) que indica que el acuso de recibo llego exitosamente. Se ha establecido la llamada y se inicia la sesión.

200 OK
From: C. Pimentel <sip: cpimentel@ cutb.edu.co >
To: L. Guzman <sip:lguzman@unab.edu.co>
Call-ID: 20032001@off.unab.edu.co

Figura. 34 Establecimiento de llamada SIP (Servidor de Redireccionamiento)



5. COMPARACIONES

5.1 COMPARACION ENTRE LA TRANSMISIÓN DE LA VOZ POR CONMUTACIÓN DE CIRCUITO (PSTN) Y LA TRANSMISIÓN DE LA VOZ POR PAQUETES (VOIP)

La primera diferencia que sale a la luz entre estos dos tipos de transmisión es el tipo tecnología de conmutación sobre la que están basada y el tiempo que han estado entre nosotros, por un lado está la tecnología de conmutación de circuitos y su representativo máximo la Red Telefónica Publica Conmutada (PSTN), que ha estado muchos años entre nosotros y por el otro está la tecnología de conmutación de paquetes con su representativo máximo las redes de paquetes IP, base de la Internet, que lleva muy poco tiempo entre nosotros comparándola con la PSTN pero que se ha desarrollado de forma de forma continua y cada vez con una mayor rapidez y flexibilidad.

5.1.1 Características principales de la conmutación de circuitos (PSTN). Existen muchas características que destacar en esta tecnología de conmutación, dentro de las cuales se ha resaltado las siguientes:

- Para cada comunicación se establece un camino físico, mientras dure el intercambio de información. Se establece un canal lógico a través del cual se envían información los interlocutores, aunque la información sea nula (espacios de silencio).

- La información se envía en tiempo real.

- Bajo rendimiento de los medios de transmisión utilizados; en la práctica hay muchos periodos de silencio en los que el canal está ocupado y no está siendo utilizado.

- Posee alto grado de confiabilidad, con disponibilidad de red típicamente mejor que 99.99%

- Calidad de servicio excelente, bajo retardo y fluctuación limitada, alta inteligibilidad, etc.

5.1.2 Características principales de la conmutación de paquetes (VoIP). La conmutación de paquetes que es una tecnología que se ha desarrollado

muy rápidamente, obedece varias características como por ejemplo el uso efectivo del ancho de banda, entre otras como las que se exponen a continuación.

- Envío de bloques de información que son fragmentos de lo que se desea transmitir. Tendrán una longitud máxima.

- En los centros de conmutación existirá almacenaje de los mensajes hasta que se pueda retransmitir al centro posterior.

- Los paquetes permanecen muy poco en memoria, es muy rápido, y por tanto se consiguen comunicaciones en prácticamente tiempo real.

- Se utiliza su división en circuitos virtuales; por un mismo medio se establecen distintos canales de comunicación. Los canales ocupan el medio únicamente cuando tienen información que transmitir; Si solo un canal tiene que transmitir, lo hará continuamente ocupando todo el medio.

- Cuando el mensaje es demasiado grande, es dividido en paquetes más pequeños.

Tomando como base estas características se realiza una comparación general de estas dos tecnologías teniendo como base la eficiencia y la forma de transmitir la información, por lo tanto se concluye que la conmutación de

circuitos es muy ineficiente, dado que mantiene las líneas mucho tiempo ocupadas, incluso cuando no hay información circulando por ellas, requiere que los dos sistemas conectados trabajen con las mismas características. En conmutación de paquetes se transmiten paquetes cortos. Para transmitir grupos de datos grandes, se divide en paquetes más pequeños y se les añade una serie de bits de control, lo que permite que el transporte de información tenga una gran flexibilidad.

Por todo esto se logran obtener muchas ventajas de la transmisión por conmutación de paquetes sobre la transmisión por conmutación de circulitos como son: Mayor eficiencia de la línea, Se permiten conexiones entre estaciones de diferentes características, Se pueden usar prioridades para el transporte de información que necesite de esta característica.

5.1.3 Comparación entre PSTN y VoIP. Luego de haber discutido las características que identifican a cada una, se describirá la arquitectura que las define, en primer lugar se tiene a la PSTN, que está compuesta de dos capas que son la de transporte y la de control, La primera está constituida por el medio de comunicación telefónica, que incluye las centrales de conmutación locales y las centrales de tránsito para interconexión entre centrales (centrales interurbanas o internacionales), así como los enlaces entre las mismas que establecen la llamada entre dos partes. La capa de control está formada por los Puntos de Transferencia de Señalización (PTS), las bases de datos o Puntos

de Control de Servicio (PCS) y los nodos de servicio. Esta segunda capa controla el comportamiento de los conmutadores de la capa de transporte, y actúa sobre los mismos para proporcionar todos los servicios de la RTPC. Mientras que la VoIP, esta compuesta de tres elementos, el Gateway, Situado en los extremos de la red, transforma el tráfico de circuitos en paquetes y viceversa. En el proceso de paquetización, y mediante la compresión y la supresión de eco, el Gateway adapta el tráfico en paquetes, crea y añade una cabecera para su control y envía el paquete a través de la red según las instrucciones proporcionadas por el elemento de control y señalización. El segundo elemento es el de control y señalización, que puede ser un Gatekeeper o un Servidor (H.323 y SIP respectivamente), que es el encargado de Proporcionar control y la señalización de la red. El control de llamada se refiere a su establecimiento y finalización, selección de servicio, enrutamiento, autenticación de llamada, autorización y contabilidad de llamadas

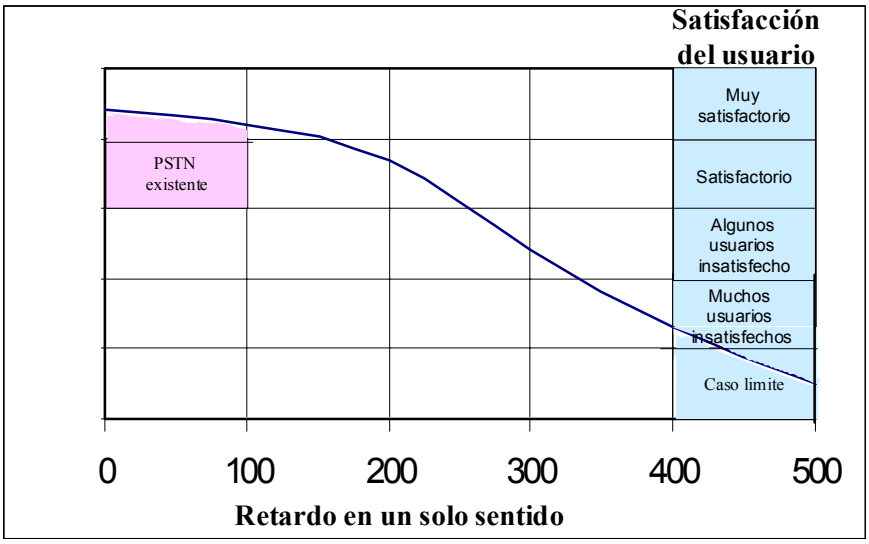
El elemento de control mueve la inteligencia de servicio fuera de la central hacia una base de datos o servidor de aplicaciones aunque, a veces, puede soportar algunos de los servicios más populares (sin requerir una plataforma de aplicaciones independiente) como la identificación de llamada, número abreviado, etc. Precisamente el tercer elemento es el servidor de aplicaciones, Soporta los servicios más complejos y que necesitan una cierta inteligencia como la llamada a tres, transferencia de llamada, creación de registros de llamada y, en general, todos los servicios que actualmente ofrecen las centrales de conmutación.

5.1.4 Comparación de QoS entre la PSNT y la VoIP con base en los *codecs* de audio utilizados por VoIP y la satisfacción de los usuarios. La comparación que se realizará en esta sección será basada en diferentes gráficas que tienen como variable la satisfacción de usuario con el servicio, el retardo en un solo sentido de transmisión y la perdida de paquetes en la red.

En la figura 35, se muestra el comportamiento de la red telefónica pública conmutada con respecto al retardo en un solo sentido y la satisfacción del usuario, claro está que en este caso no existe la perdida de paquetes.

Los resultados obtenidos indican que en el caso cuando el retardo (RTT) comienza a aumentar sobre 300ms, se convierte en perceptible al usuario, y los niveles de satisfacción comienzan a caer de forma rápida a partir de ese punto.

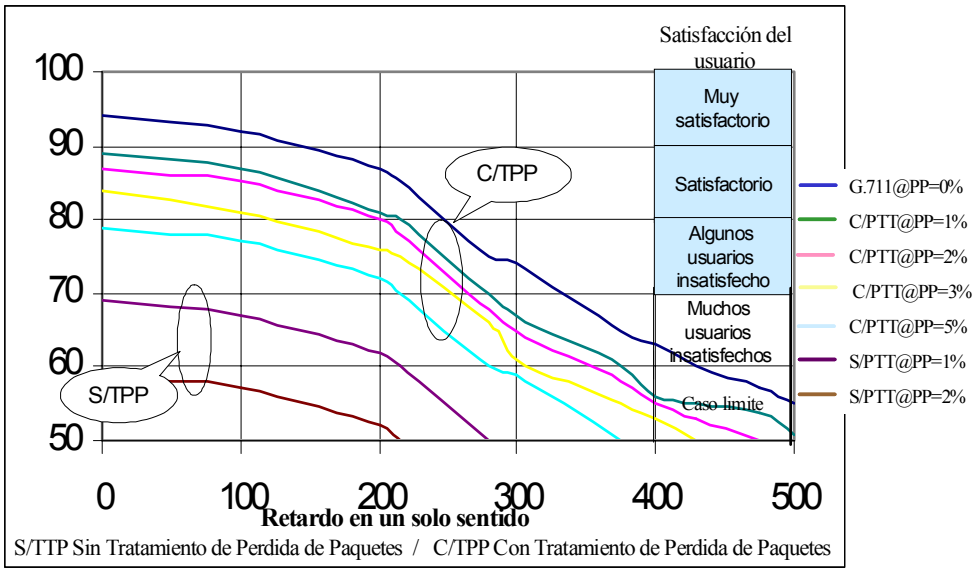
Figura 35. Comportamiento de la PSTN (Retardo en un sentido vs Satisfacción)



Fuente TIA (*Telecommunications Industry Association*)

Si se utiliza el *codec* de audio especificado como básico dentro de los estándares de VoIP el G.711, sin perdidas de paquetes los resultados son idénticos a los obtenidos anteriormente con la PSTN. Sin embargo una vez introducida la perdida de paquetes, la QoS empieza a caer dramáticamente, especialmente si dentro de la red no se l realiza ningún tratamiento de perdida de paquetes. Aunque con tratamiento de perdida de paquetes, una perdida de paquetes debajo del 3% y un retardo bajo los 100ms, la calidad sigue siendo satisfactoria. (Figura 36)

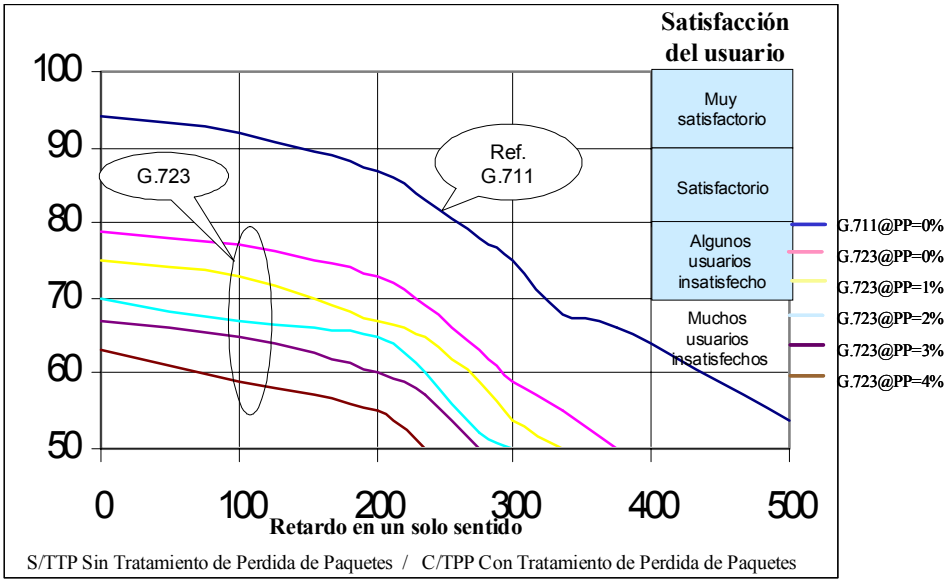
Figura 36. Desempeño del *codec* G.711



Fuente TIA (*Telecommunications Industry Association*)

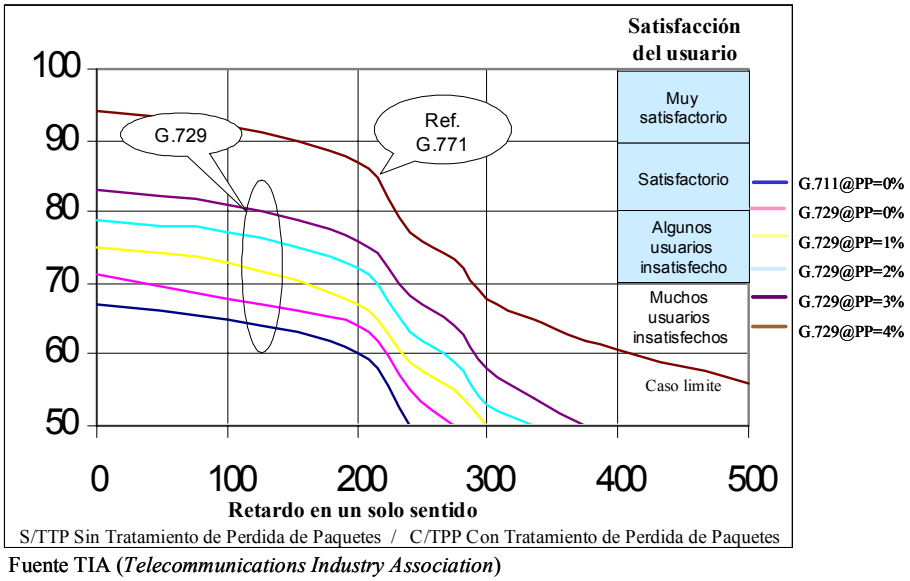
Los datos comprimidos son otra historia, si se observa la figura 37, donde se utiliza únicamente el *codec* G.723 (6.3 Kbits/s), la calidad de audio nunca alcanza los niveles de satisfacción del usuario, ni en el caso en que se tiene 0% de perdidas de paquetes. El protocolo G.729, que es comprimido a 8Kbits/s, es ligeramente mejor, entrando en la zona satisfactoria pero bajo la condición de que el retardo no sobrepase los 200ms y que se sostenga una perdida muy pequeña de paquetes.(ver figura 38)

Figura 37. Desempeño del *codec* G. 723



Fuente TIA (*Telecommunications Industry Association*)

Figura 38. Desempeño del *codec* G. 729



Fuente TIA (*Telecommunications Industry Association*)

5.2 COMPARACIÓN ENTRE H.323 Y SIP

Estos dos son los estándares que predominan en la transmisión de voz sobre paquetes, por lo tanto son en ellos en los que se ha centrado la investigación y con el fin de brindar una comparación entre estos dos, se tendrán en cuenta la funcionalidad, la calidad de servicio, la escalabilidad, la flexibilidad y la interoperabilidad.

5.2.1 Funcionalidad. Para desarrollar este término se expondrán los procedimientos para el establecimiento de una llamada, asi como los servicios complementarios y el intercambio de capacidades que cada uno de estos estándares manejan.

Para este caso de referencia se presenta la siguiente tabla con las características más representativas de la funcionalidad de ambos de los protocolos

Tabla 6. Características de Funcionalidad en H.323 y SIP.

Servicio de control de llamadas
Llamada en espera
Transferencia de llamadas
Características avanzadas
Control a terceros
Conferencia
Intercambio de Capacidades

5.2.1.1 Establecimiento de llamada. En este procedimiento ambos protocolos son similares, en la figura 39 se representa en forma básica el establecimiento de una llamada H.323, mientras que en la figura 40 se representa el establecimiento en forma básica de una llama SIP

Figura. 39 Establecimiento de llamada H.323

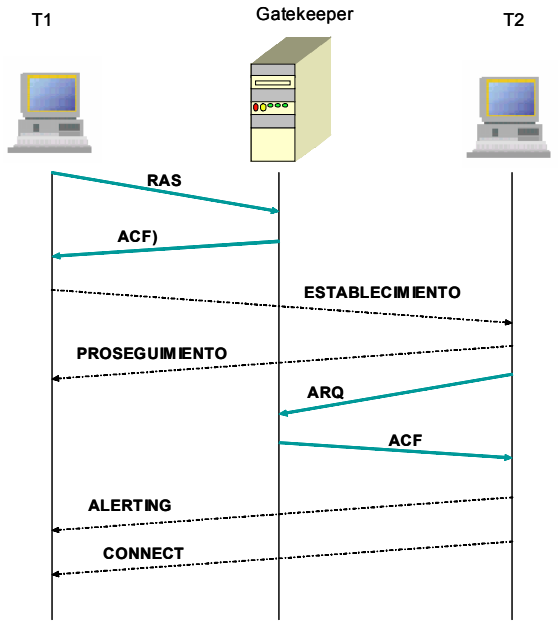
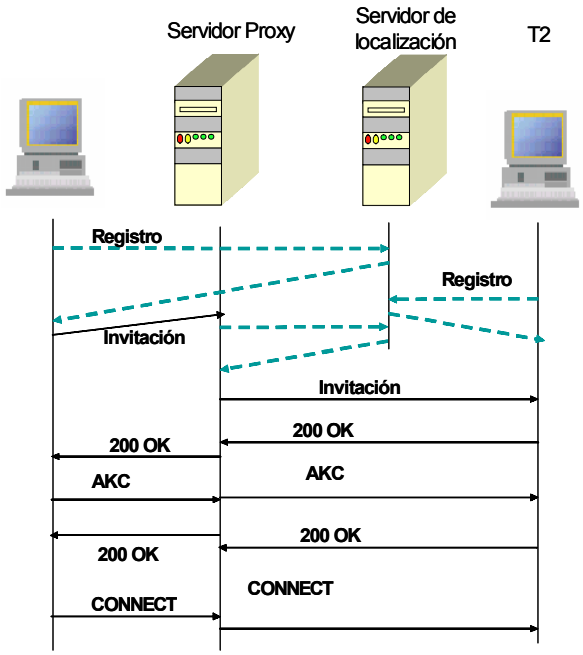


Figura. 40 Establecimiento de llamada SIP



5.2.1.2 Transferencia de llamada. En este proceso de transferencia de llamada se habilita a un usuario para transferir una llamada que ya esta establecida hacia otro tercer usuario. Ambos SIP y H.323 soportan tres tipos de transferencia de llamada: transferencia ciega, transferencia alternativa y transferencia asistida por operador. Las figuras 41 y 42, muestran el flujo de señalización para una transferencia ciega en H.323 y SIP respectivamente.

Figura. 41 Transferencia ciega de llamada en H.323

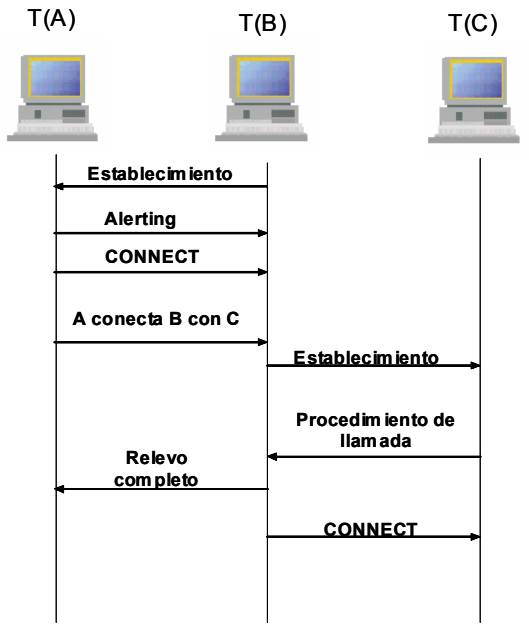
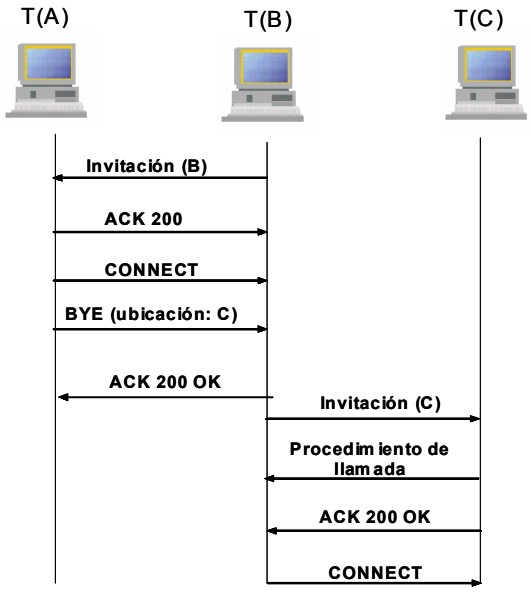


Figura. 42 Transferencia ciega de llamada en SIP



5.2.1.3 Control de terceros El control de terceros es definido como la habilidad que tiene una entidad de establecer una llamada entre otras dos entidades sin que necesariamente tenga que participar en la sesión. Esta característica es actualmente disponible únicamente en SIP, aunque no se descarta que en las próximas versiones de H.323 sea añadida la misma funcionalidad.

5.3 CALIDAD DE SERVICIO (QOS)

En la tabla 7 se presentan las diferentes características que se deben tener en cuenta cuando se está hablando de calidad de servicio en VOIP, estas características y su rendimiento dentro de las redes H.323 y SIP, son las que permiten establecer una diferencia entre estos dos estándares.

Tabla7. Características de QoS En redes H.323 y SIP

Calidad de servicio
Retardo de establecimiento de llamada
Confiabilidad
Recuperación paquetes perdidos
Detección de fallas
Tolerancia de fallas

El retardo del establecimiento de llamada, se debe entender como el número de recorridos de ida y vuelta, necesarios para el establecimiento de una llamada, en la primera versión de H.323 eran muchos los pasos para el establecimiento, pero se ha ido mejorando con el desarrollo de nuevas versiones. En SIP como en H.323v3, este factor está bajo los niveles adecuados y son iguales, pero H.323 tiene varia ventajas sobre SIP en cuanto al establecimiento de conexiones para los protocolos usados (UDP y TCP) para el transporte de mensajes de establecimiento de llamada.

Dentro del campo de calidad de servicio está incluida la confiabilidad de la red, que depende, como se observa de tres factores primordiales, detección de fallas, tolerancia de fallas y recuperación de perdida de paquetes, donde H.323 tiene alternativas mucho mas complejas que SIP, que en algunos casos se pueden tornar en ventajas o desventajas frente a SIP.

5.4 ESCALABILIDAD

Muchos son los aspectos que se deben tener en cuenta para hablar de escalabilidad en estos dos sistemas (H.323 y SIP), estos aspectos afectan de manera directa la escalabilidad y se describen en términos de complejidad, comunicaciones multipunto, procesamiento de los servidores o Gatekeeper, comunicación interna entre servidores, etc.

En muchos de estos términos SIP, ha demostrado ser igual de funcional que H.323, sin la necesidad de ser tan complejo como este. Por ejemplo, H.323 incluye H.225 para la señalización de las llamadas, H.245 para el control de las llamadas, H.450.X para servicios complementarios, etc. Mientras que SIP se apoya de SDP y de una manera menos complicada cumple con las mismas tareas solo con el uso de cuatro cabeceras (*To, From, Call-ID* y *Cseq)* y tres tipos de peticiones (*INVITE, ACK* y *BYE*), lo que trae como consecuencia que SIP consiga una mayor escalabilidad basada en la simplicidad de su estructura.

5.5 FLEXIBILIDAD

Este término al igual que los anteriores está basado en las diferentes características que maneja SIP y H.323, en este caso la flexibilidad viene ligada con el concepto de fácil adaptación en donde SIP, lleva la delantera ya que la codificación basada en texto de SIP hace que la adaptación a cambio producidos como por ejemplo en una sesión sea mucho mas fácil que en H.323 ya que este ultimo requiere de mayor interacción entre sus sub-protocolos.

5.6 INTEROPERABILIDAD

En este caso hay muchos aspectos por tener en cuenta y por desarrollar en estos estándares. La interoperabilidad es definida como la capacidad de los diferentes estándares de VoIP para trabajar con diferentes versiones, implementaciones y otros protocolos de señalización. H.323 tiene la delantera en este campo de la interoperabilidad ya que ha demostrado tener un gran acople entre todas sus versiones y además como característica principal es un estándar que nació como una familia de recomendaciones para lograr el trabajo e interoperabilidad entre diferentes tipos de redes, como lo demuestra la especificación H.32x, en donde se encuentran: H.324 Trabaja sobre SCN (*Switched Circuit Network*), H.320 Trabaja sobre ISDN (*Integrated Services Digital Networks*), H.321 y H.310 Trabajan sobre B-ISDN (*Broadband Integrated Services Digital Networks*) y H.323 que trabaja sobre IP.

6. CALIDAD DE SERVICIO QoS EN VoIP

6.1 INTRODUCCION

Las redes basadas en paquetes IP harán posible realizar llamadas de bajo costo, además de generar servicios de telecomunicaciones innovadores, aumentando así la competencia. Este proceso se verá acelerado por los numerosos avances que se están produciendo en la tecnología VoIP, que permiten obtener mejores rendimientos. Ahora la voz podrá ser transmitida sobre redes de datos con la misma calidad que las llamadas realizadas sobre la red telefónica convencional, debido a las nuevas tecnologías de compresión de voz y el mayor ancho de banda disponible.

La telefonía IP, a diferencia de la *PSTN*, soporta diferentes niveles de Calidad de Servicio (QoS); ello permite a los operadores y proveedores de servicio dirigirse a distintos segmentos del mercado, con diferentes ofertas de calidad, dependiendo del precio que los clientes estén dispuestos a pagar por cada nivel de QoS.

En este capitulo se hace una visión global de la QoS junto con un repaso de las técnicas de ingeniería de tráfico que se usan para asegurar la entrega de paquetes en las redes IP.

6.2 CALIDAD DE SERVICIO. NIVELES DE SERVICIO

La evolución de las redes a una infraestructura convergente o de red única plantea nuevas cuestiones en cuanto a calidad de servicio (QoS). Generalmente, las necesidades del tráfico asociadas con las aplicaciones de datos son muy diferentes de las que corresponden a las llamadas telefónicas y a otros servicios suministrados en tiempo real. Los servicios pueden variar desde los más tolerantes a fallos de transmisión, como el fax o la escucha de una transmisión de audio, hasta los más estrictos, como una aplicación interactiva de juegos, y por esta razón gran parte de la investigación se centra en posibilitar diferentes clases de servicio para diferentes tipos de tráfico

La calidad de servicio debe estar enfocada a la satisfacción del usuario final mediante una operativa eficiente que ahorre costos. Como ya se ha comentado, la consideración de la QoS en voz sobre paquetes y, particularmente, en telefonía IP es un factor fundamental para su desarrollo a gran escala.

La calidad de funcionamiento debe considerar varios aspectos; entre otros, la fiabilidad, el flujo y la seguridad. No obstante, el hecho de que para el público la calidad de transmisión de voz a través de Internet pública sea deficiente explica por qué no se suele considerar la telefonía Internet como un servicio con calidad de operador. En general existen dos formas de mejorar la calidad de transmisión IP:

- Aumentar la capacidad disponible (ancho de banda).

- Implementar un soporte de QoS para mejorar la calidad de funcionamiento.

Con respecto a estos puntos, se está investigando para lograr un encaminamiento de conmutación mejorado y ordenado por prioridades, además de invertir para incrementar la capacidad de las redes de datos mundiales. De hecho, ciertos observadores sostienen que aumentar la capacidad disponible es un método mucho más práctico que mejorar la calidad para acelerar la implantación de Internet, ya que no requiere una actuación coordinada de los proveedores de servicios Internet.

Si se implementara una infraestructura de clase de servicio en una conexión a través de Internet (pública), la falta de un régimen global de QoS a través de Internet significaría que no se pueden ofrecer garantías de QoS. En general se plantean menos problemas cuando se utilizan redes IP gestionadas (privadas), ya que éstas cuentan con una mayor capacidad, transmisión más rápida y una

mejor calidad de la voz que satisfacen a los clientes. Por consiguiente, la capacidad de tráfico explotada en redes privadas es por regla general un factor determinante para garantizar la viabilidad de la telefonía IP de nuestros días y resulta más importante en este sentido que la calidad de servicio.

Existen diferentes técnicas y normas para soportar la QoS en telefonía IP. La solución particular depende en cada caso de aspectos como los requerimientos de usuario, necesidad de integrar la infraestructura convencional o la interoperabilidad con otras redes.

Una manera que tiene un operador de asegurar la calidad de un servicio de voz es establecer a su vez acuerdos de nivel de servicio con los proveedores. Los niveles de servicio se refieren a las capacidades reales de QoS extremo a extremo, es decir, la capacidad de una red de entregar un servicio requerido por el tráfico específico de red, especificando parámetros como capacidad de transferencia de datos (*throughput*), pérdida de paquetes, latencia y variación de retardo máximo.

Existen tres niveles de servicio básicos:

- **Servicio de mejor esfuerzo** (best effort), es simplemente conectividad sin garantía, como en la Internet.

- **Servicio diferenciado**, en el que un tráfico determinado es tratado mejor que el resto, siendo en promedio más rápido y con menor tasa de pérdidas.

- **Servicio garantizado**, con absoluta reserva de recursos de red para el tráfico específico.

6.3 CALIDAD PERCIBIDA EN VoIP

La calidad de la voz es un concepto subjetivo, pues no se puede medir con objetividad sino es con referencia a una persona que escucha y experimenta como percibe la voz. La calidad percibida de una llamada VoIP está limitada por diversos factores, como el retardo y sus variaciones, pérdidas de paquetes y el eco. Para evaluar la calidad se suelen utilizar medidas subjetivas y formar índices de percepción, como el conocido índice MOS (*Mean Opinion Score*).

Los factores que influyen en la calidad de la voz, se pueden clasificar en dos grupos:

- Los relacionados con la transmisión de paquetes y que pueden afectar a la claridad de la voz (fidelidad, inteligibilidad). Entre ellos se encuentran la latencia, pérdida de paquetes, variación de retardo (jitter) y distorsión de codificación.

- Los que afectan a las redes en general, como el eco, retardo de propagación, niveles variables de señal y ruido de fondo.

La combinación de estos efectos puede dar lugar a un entorno de llamada inaceptable, por lo que deben ser controlados en su conjunto. A continuación se comentan estos efectos y su posible atenuación o compensación para mejorar la calidad de la conversación.

6.3.1 Latencia. Un área importante en la percepción de la calidad de la voz, particularmente en redes que usan tecnologías de VoIP, es la latencia, o retardo acumulado. Esto es debido a una serie de factores, entre los que se pueden señalar:

- Retardo propio del algoritmo de compresión de voz.

- Retardo por la carga del proceso de compresión/descompresión y paquetización de voz en el *Gateway*.

- Latencia propia de los dispositivos de enrutamiento y encolado de paquetes.

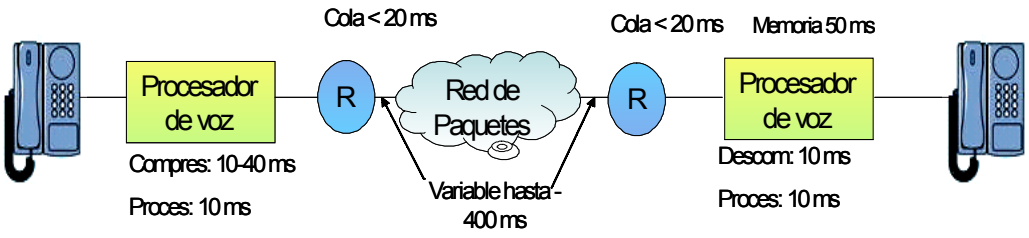
- Tiempo de propagación (proporcional a la distancia entre extremos de usuario).

El *Gateway* comprime y empaqueta la voz, y luego se transporta a través de la red hasta el *Gateway* distante. Los paquetes pasan a través de diferentes

medios físicos que se interconectan: enrutadores y otros dispositivos de enrutamiento con mecanismos de colas que introducen retardos adicionales.

Para ver como influye la transmisión de VoIP en el retardo, tomemos un ejemplo de voz codificada a 8 kbps según la recomendación G.729. El paquete contiene una trama de datos de 10 ms (latencia de paquetización), con una latencia de algoritmo de compresión de unos 25 ms, a los que se debe añadir un retardo de memoria de compensación de jitter de unos 15 ms, tiempo de decodificación 10 ms y otros como retardo de transmisión, encolado (enrutamiento), etc. Llegamos a un retardo mínimo total de unos 70 ms.

Figura 43. Contribuciones a la Latencia en VoIP



A partir de una latencia de unos 200 ms, el hablante debe dar tiempo a su interlocutor para no interferirlo, la audición comienza a ser molesta a los 250 – 300 ms y ya no es posible la comunicación en modo dúplex, apareciendo el conocido efecto *walkie-talkie*. (*Half dúplex*)

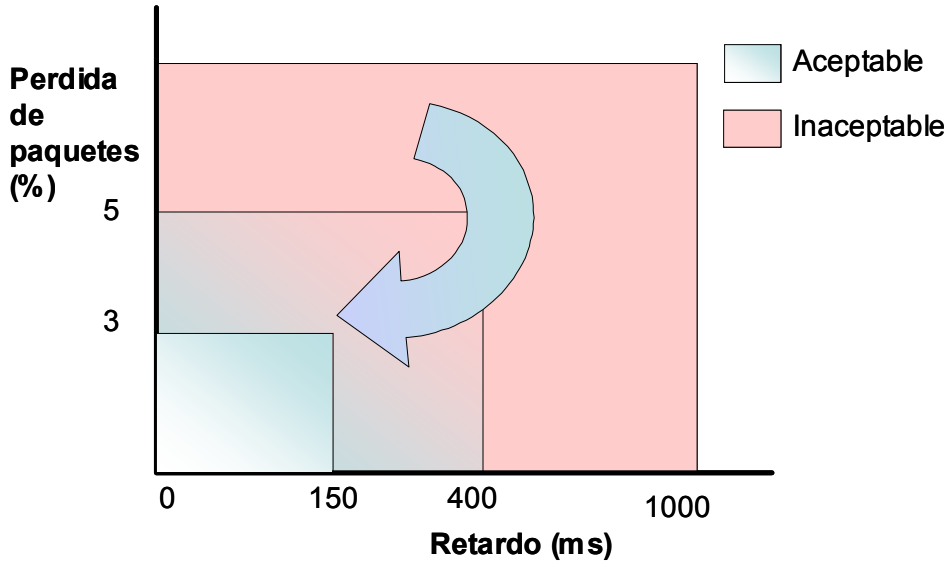
El efecto empeora cuando además se pierden paquetes de voz a lo largo del trayecto a su destino, pues ello afecta a la calidad del sonido. El efecto de la pérdida de paquetes depende de factores como el tamaño del paquete, tipo de

codec de voz usado y duración de la pérdida entre otros. Los paquetes que se pierden afectan no solo a la conversación sino también a la efectividad de los mensajes de señalización de las llamadas.

En general, a partir de un 5% de pérdida de paquetes la voz tiene un sonido metálico, y si el porcentaje de pérdidas supera el 10% parece que se habla con un robot. No obstante, para una conversación telefónica la pérdida medida entre extremos no debiera superar el 3-5%, para no interferir la señalización.

La figura siguiente muestra zonas de funcionamiento admisible, tolerable y no aceptable en VoIP en función de la latencia.

Figura 44. Áreas de Funcionamiento en Telefonía IP



Para solventar los problemas de pérdidas de paquetes se utilizan protocolos y técnicas de ingeniería de tráfico, como RSVP, DiffServ, o MPLS.

6.3.2 Variación del retardo (Jitter). Sin mecanismos de provisión de QoS, los enrutadores manejan los paquetes a medida que van llegando, y dependiendo de lo que ocurre en ese instante, los despacha con más o menos rapidez.

Debido a ello los paquetes que van por la red llegan a su destino con variaciones de retardo, lo que es poco tolerable para que haya una conversación con cierta fluidez.

La solución consistirá en poner los paquetes recibidos en una memoria intermedia en recepción y leerlos a una velocidad regular mediante un proceso separado, aunque esto introduce un retardo adicional proporcional a la variación del retardo.

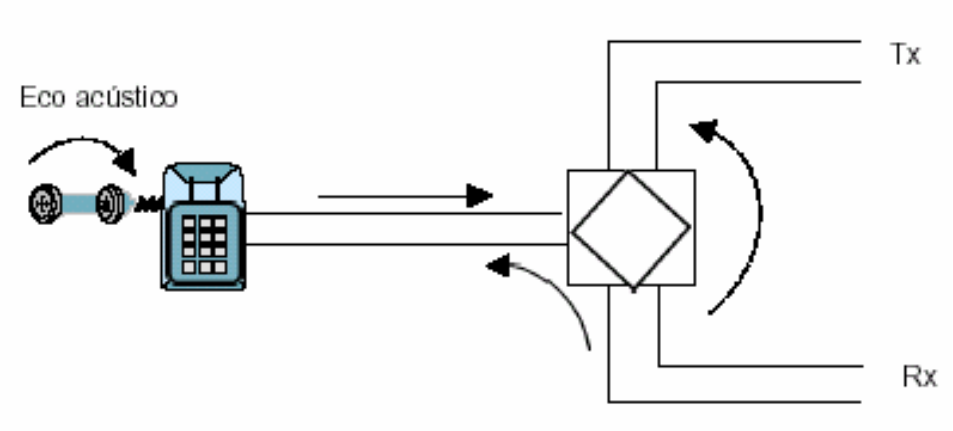
Las memorias (buffer) que compensan estas fluctuaciones de retardo pueden ser dinámicas, adaptables a las variaciones, o estáticas, con un tamaño fijo. Las primeras pueden proporcionar mejor calidad del servicio al reducir el tamaño de la memoria si la red lo permite. La topología de red también influye en el retardo variable, así en una red de datos conmutada hay menos colisiones de paquetes que en una basada en concentradores (HUB).

6.3.3 ECO. Otro factor importante que afecta a la calidad percibida de voz en las llamadas es el eco de la persona que habla. Cualquier discontinuidad a lo largo de la línea de transmisión puede causar eco, como el producido al pasar

en un extremo la línea de dos a cuatro hilos (bobina híbrida), pues parte de la señal recibida desde el extremo lejano se vuelve a transmitir junto con la señal deseada, por lo cual la persona que habla escucha su propia voz con cierto retardo, perceptible a partir de unos 30 ms. Otro tipo de eco (eco acústico) se puede producir por realimentación de la salida del auricular al micrófono cercano (ver figura 45).

Las recomendaciones G.164 (supresores de eco), G.165 y G.168 de la ITU proporcionan unos métodos de medida y límites en los niveles y retardos de eco que se deberían seguir con criterio de cumplimiento mínimo. Las posibilidades de terminación de llamadas en redes fijas, celulares o inalámbricas hacen que los requerimientos de control de eco sean más exigentes.

Figura 45. Fuentes de Eco



El efecto del eco se puede corregir con un cancelador, que hace una predicción del eco en función de la señal recibida y la sustrae de la señal de audio a

transmitir, consiguiendo que el efecto sea imperceptible. Para ello se requiere que cumplan con los límites de la recomendación G.168 de la ITU, aunque normalmente los canceladores de eco tienen una capacidad de supresión mucho mayor, pues deben responder a los posible retardos producidos en las redes actuales, que pueden incluir teléfonos celulares en los extremos, redes ATM y codificación de VoIP. Una capacidad añadida que se espera de un cancelador es la posibilidad de controlar el nivel de audio para compensar sus variaciones. La naturaleza dinámica de las redes puede causar variaciones de retardo y las características del extremo del circuito. Es por ello muy importante que el cancelador converja rápidamente antes de que se produzca el eco, aunque también puede generar un ruido molesto al tratar de adaptarse al eco con rapidez.

También se requiere que tenga en cuenta el ruido de fondo o ruido estacionario, mediante algún tipo de análisis espectral, para poder minimizarlo y que no influya negativamente en la codificación de la voz.

6.3.4 Ruido. El ruido de fondo es otro potencial problema de calidad percibida. Este ruido es captado por el teléfono y se distorsiona tras la codificación de voz en el *Gateway* VoIP, y si el ruido es similar a la conversación, el impacto en los codificadores es mayor. El resultado puede ser un molesto ruido que origina quejas de los usuarios VoIP a los operadores. De nuevo la tecnología puede ayudar a resolver esta cuestión mediante el uso en los canceladores de eco de

un mecanismo de reducción automática de ruido (ANR) mediante técnicas de filtrado espectral, lo cual puede disminuir el ruido de fondo hasta un 75% cuando es estacionario (no variable).

También existen mecanismos de supresión de silencio cuando no hay actividad, con objeto de no transmitir paquetes y ahorrar ancho de banda, e incluso pueden enviar información de ruido de inactividad para que el extremo lejano lo genere como "ruido confortable" en periodos de silencio. Los detectores de voz se usan para restablecer la codificación.

Se ha descubierto que cuando se mueve una salva de ruido desde el principio al final de una conversación la calidad percibida es bastante afectada, sugiriendo un efecto memoria en la llamada y que si se retarda el ruido no se tiene en cuenta.

6.4 CODIFICACION Y COMPRESION DE VOZ. ANCHO DE BANDA

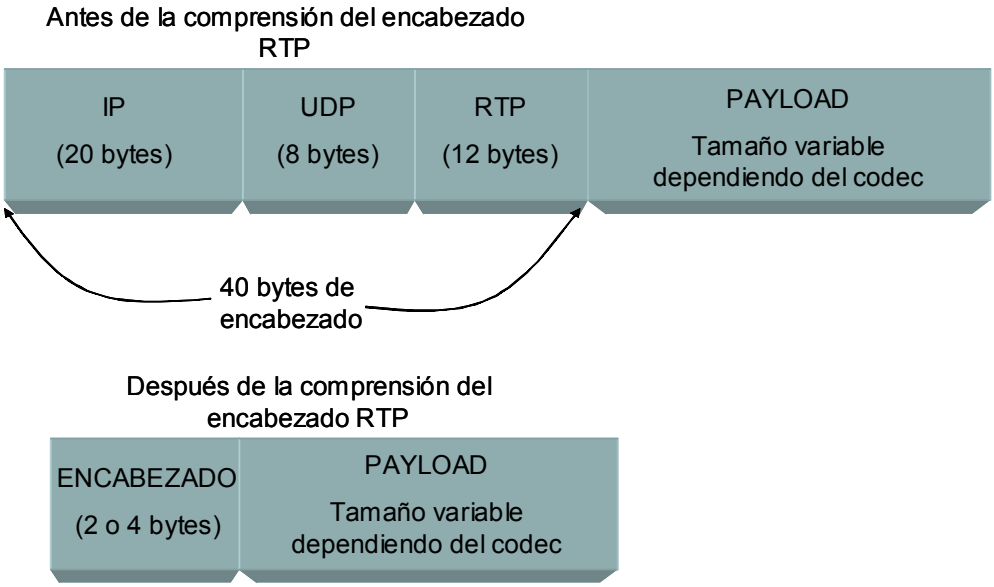
La voz antes de ser convertida en paquetes se ha de codificar (digitalizar si estaba en formato analógico) y comprimir de acuerdo con un esquema generalmente normalizado, utilizando los *codec*s de voz (vocoders). Con ello se obtiene una reducción de la velocidad de bit y, por tanto, del ancho de banda ocupado por la voz, aunque en el proceso posterior de paquetización vuelve a

aumentar al añadirse los campos de cabecera según los protocolos empleados. Así, una llamada VoIP utilizando G.711 (64 kbps) en una comunicación bidireccional (half duplex) a 60 paquetes/seg puede consumir un ancho de banda de pico de 168 kbps. En la utilización de los *codecs* hay que establecer un compromiso entre la reducción de velocidad obtenida, el retardo introducido por el algoritmo de compresión y tamaño de trama y la calidad percibida al comprimir.

Una técnica adicional para reducir el ancho de banda consiste en aprovechar los tiempos de silencio en la conversación para no codificar ni transmitir paquetes, suprimiendo por tanto la transmisión durante esos periodos.

Otra forma de disminuir el ancho de banda ocupado es utilizando compresión de cabeceras. En efecto, los bits de cabecera de los paquetes suponen una sobrecarga adicional que aumentan el ancho de banda. En paquetes RTP, el tamaño de la cabecera puede quedar reducido unas diez veces, como se aprecia en la figura 46.

Figura 46. Comprensión del RTP



6.5 FACTORES QUE AFECTAN LA QoS EN UNA LLAMADA VoIP

Para mejorar la QoS existen aplicaciones y equipos especiales que compensan los principales problemas de envío de voz sobre redes de paquetes: latencia, eco, variaciones de retardo en la llegada y pérdida de paquetes. La verificación de la calidad de una red de VoIP y sus componentes se puede realizar a dos niveles:

- Con medidas de audio extremo a extremo, utilizando herramientas de supervisión para control y registro de eventos.

- Mediante un analizador de protocolos o de paquetes para el seguimiento de llamadas, incluyendo informes detallados de llamadas.

Para tener una idea de los problemas de QoS que se encuentran en VoIP estableceremos a continuación un escenario típico. Supongamos una llamada punto a punto entre dos teléfonos convencionales. Cada extremo está conectado a la red de VoIP mediante una ***Gateway***, y el enrutamiento de llamadas con establecimiento del canal de señalización es realizado por un ***Gatekeeper.***

La llamada se establece siguiendo la recomendación H.323. El proceso de establecimiento sigue, en líneas generales, la siguiente secuencia desde el terminal que llama:

1. Usuario descuelga y, mediante el cambio de estado producido, el terminal informa al controlador (*Gatekeeper*) de su intención de llamar.

2. El usuario obtiene un tono de invitación a marcar y procede a pulsar el número destino.

3. Cuando H.323 conoce mediante señalización la dirección IP de el *Gateway* de destino y se establece como va a ser el proceso de comunicación, ésta ya se puede iniciar, enviando tono de llamada,

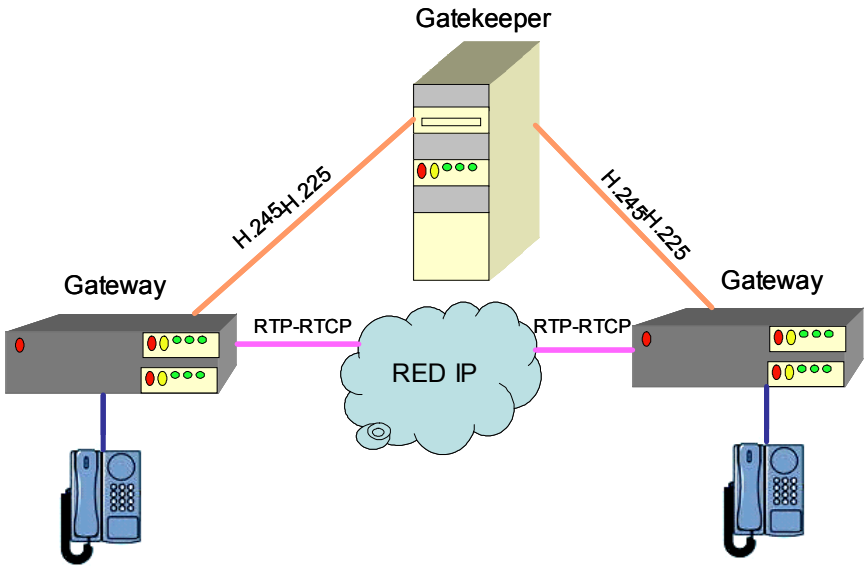
iniciando la conversación o recibiendo tonos de ocupado, congestión, etc.

Para que las secuencias 1 y 2 progresen es necesario establecer los procesos de registro y admisión (RAS) según la recomendación H.225 y los procedimientos de llamada con mensajes basados en Q.931, que también indican el estado de la llamada de manera similar a las realizadas en la *ISDN*.

La última fase del proceso de establecimiento se completa tras negociar los recursos a utilizar (*codecs* de voz, ancho de banda, etc.) a través del canal de control creado para la sesión según la recomendación H.245. Esto se efectúa mediante el intercambio de mensajes usando el protocolo fiable TCP, lo cual puede repercutir en el tiempo de establecimiento en caso de redes próximas a la congestión.

Una vez establecida la comunicación, la voz se transporta en paquetes utilizando el protocolo RTP, con control de estado de transmisión mediante RTCP.

Figura 47. Proceso de una llamada



Aunque descrito de forma resumida, los procesos indicados para establecer una llamada de VoIP típica dan una idea de su complejidad y los posibles problemas de QoS que pueden surgir. En primer lugar, existe un retardo debido a la señalización antes de poder escuchar tono de llamada, pues se debe resolver la dirección IP destino en función de su número de teléfono, admitir luego la conexión y, en fin, negociar los parámetros de interconexión de *Gateway*. Para una adecuada QoS, el tiempo necesario para establecimiento de llamada debe limitarse a unos segundos, cuestión especialmente complicada en llamadas de larga distancia.

Por otro lado, todos los elementos de red introducen un retardo en la transmisión que hay que evaluar y minimizar, desde el *Gateway* con codificador que comprime la voz digitalizada, conversión a paquetes de la voz con inserción de bits de cabecera, enrutamiento de los paquetes, transmisión física

por la red IP y proceso contrario en el otro extremo. Todo ello es susceptible de introducir degradaciones de la QoS, tales como latencia, pérdida de paquetes y fluctuación de retardo (*jitter*).

Para mejorar la calidad de las llamadas por la red se pueden utilizar técnicas de QoS como:

- **Planear la capacidad** necesaria del sistema. Con una adecuada planificación se puede proporcionar un entorno de red controlado.

- **Utilizar herramientas** de gestión para configurar los nodos de red, supervisar y gestionar dinámicamente los flujos de tráfico y realizar estadísticas. Se puede priorizar por tipo de aplicación, por protocolo o bien por situación, y dar preferencia por tanto al tráfico de voz.

- **Añadir mecanismos de control.** Las técnicas de gestión de tráfico, como control de admisión, o la utilización de protocolos de gestión de recursos como RSVP, permiten evitar la sobrecarga de red o, en su caso, mejorar la QoS.

Por otro lado, para compensar la pérdida de paquetes existen técnicas como la **interpolación** de paquetes perdidos, que se sustituyen por el último recibido, la **redundancia** de los paquetes enviados, a costa de un mayor ancho de banda y la **redundancia** híbrida con paquetes comprimidos.

A continuación veremos distintos aspectos sobre ingeniería de tráfico, diferenciación por clase de servicio y gestión de recursos, lo cual nos permitirá obtener una idea general de las técnicas de QoS que se pueden aplicar a la VoIP.

6.5 INGENIERÍA DE TRÁFICO. CoS

Para satisfacer la demanda de servicios de VoIP con calidad de servicio, los operadores deben implantar unos sistemas de gestión y control de red que les permita conectarse con otros, con provisión de QoS a través de redes troncales alternativas y con sistemas de facturación diferenciados por tipo de tráfico.

Como hemos indicado, las redes basadas en IP poseen características que afectan de diversa manera la QoS y que deben ser evaluadas. La forma directa de resolver el problema de congestión de tráfico sería aumentando los recursos, como la instalación de nuevos enlaces, enrutadores o conmutadores más rápidos, lo cual requiere la adecuada planificación, provisión, gestión de recursos, etc. en un tiempo determinado. La ingeniería de tráfico aplica la tecnología y los principios científicos para medir, caracterizar, modelar y controlar el tráfico. Mediante ingeniería de tráfico se puede realizar o controlar aspectos como:

- Gestión de recursos, con control de ancho de banda, equipos y facilidades de red.

- Caracterización y medida de tráfico.

- Gestión de tráfico (por ejemplo, mecanismos de encolado, programación y conformación del tráfico).

- Planeamiento de capacidad de red (*capacity planning*)

- Enrutamiento dinámico y adaptado a necesidades del servicio.

En una red integrada en que distintos tipos de tráfico pueden competir por los recursos disponibles es a menudo deseable asignar prioridad al tráfico en tiempo real. La clase de servicio (CoS) es un método de clasificación que utiliza mecanismos de colas que limitan el retardo y otros factores para mejorar la calidad de servicio.

La ingeniería de tráfico y diferenciación por CoS son características ya conocidas de las redes ATM, basadas en el trabajo de normalización de la ITU sobre *ISDN* banda ancha, entre otros. Por otro lado, la telefonía IP presenta unos retos de QoS, especialmente cuando coexiste con la *PSTN*, por lo que el IETF, el ITU-T y otros organismos han estudiado mecanismos para proporcionar QoS. La mayoría de las normas de calidad de servicio e ingeniería

de tráfico que están preparando los organismos de normalización parece concentrarse en apoyar tecnologías "orientadas a circuitos" tales como IP por ATM o, más recientemente, la conmutación por etiquetas multiprotocolo (MPLS). Estas tecnologías pueden ofrecer soluciones deterministas para la calidad de servicio y la ingeniería de tráfico, y facilitar al mismo tiempo la integración de las actuales redes y las incipientes redes ópticas.

Las primeras iniciativas para proporcionar QoS en redes IP dieron lugar al protocolo RSVP (protocolo de reserva de recursos), surgido en 1990 como un método efectivo para obtener dicha calidad de servicio. Pero el protocolo fue diseñado para una única arquitectura de red, y no para el complejo mundo de múltiples subdominios de hoy. La aparición de nuevas alternativas (estándares) tales como Diff-Serv (*Differentiated Services*) y MPLS (*Multi-protocol Label Switching*) enfocan la gestión de QoS hacia redes que distinguen el tipo de tráfico y pueden acelerar la transmisión a través de enrutadores mediante el uso de etiquetas.

6.6.1 Gestión de recursos. Se han mencionado los servicios de gestión de recursos como un aspecto de la ingeniería de tráfico que busca mejorar la calidad del servicio mediante diferenciación por CoS y gestión de tráfico. La gestión del tráfico incluye ciertas ideas clasificadas tradicionalmente como control de congestión, como las políticas de restricción de acceso a un recurso

o el rebajar de forma dinámica las demandas de usuario para compensar la sobrecarga de red. La gestión de recursos se basa en tareas como:

- Asignación de recursos con reserva de ancho de banda.

- Diferenciación de servicios, con asignación de prioridades según el tipo de tráfico.

- Control de admisión.

- Asignación de tráfico para RPVs.

A continuación se definen los Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ), ambos basados en la gestión de recursos.

6.6.1.1 Servicios integrados. En 1994, el IETF introdujo el concepto IntServ (RFC 1633), en el que se promueve la calidad de servicio con la arquitectura actual de redes mediante reserva de recursos para el tráfico que requiere ancho de banda y bajo retardo. Básicamente, el marco de IntServ define un modelo QoS señalizado, es decir, que las necesidades de recursos son señaladas desde un extremo y el dispositivo correspondiente de red reserva recursos de acuerdo con ello. Para utilizar los Servicios Integrados se emplea como señalizador el protocolo de reserva de recursos RSVP (sección 4.9) , que incluye la posibilidad de control de admisión.

IntServ garantiza niveles de QoS estableciendo tres tipos de servicio, correspondiendo a los tres niveles básicos comentados en la sección 6.2

- Servicios de mejor esfuerzo, para las redes públicas.

- Servicios de carga controlada tolerantes al retardo (recepción de vídeo, audio), para redes menos congestionadas.

- Servicios no tolerantes al retardo, con aseguramiento del ancho de banda y del retardo máximo, para redes gestionadas sin pérdidas. Este sería el nivel de servicio adecuado para telefonía.

Sin embargo, en redes con demanda creciente de ancho de banda estas medidas no suelen ser suficientes, pues los estado de los flujos han de ser mantenidos por los enrutadores, por lo que tiene problemas de escalabilidad y es complicado de desplegar en Internet.

IntServ por RSVP proporciona garantías cuantitativas a cada flujo (conexión IP origen y destino), mientras que DiffServ proporciona aseguramiento cualitativo basado en clases de tráfico.

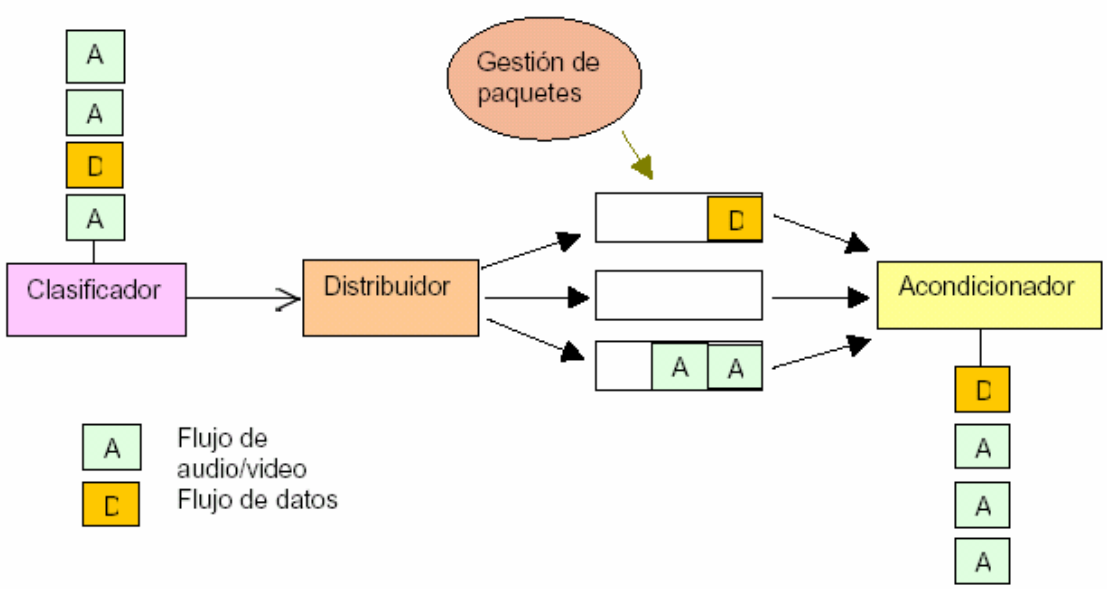
6.6.1.2 Servicios diferenciados. No todos los servicios necesitan realmente garantizar la calidad, pues a veces solo es suficiente ordenar los paquetes de datos mediante algún mecanismo de asignación de prioridades. DiffServ (RFC 2475) define un conjunto de clases de tráfico y unas prioridades para el mismo. La arquitectura de servicios diferenciados contiene dos tipos de elementos funcionales:

- Elemento de borde (*edge function*), que clasifica los paquetes y acondiciona el tráfico. Los paquetes que llegan al borde de la red son clasificados por el campo IP 'Tipo de Servicio' (TOS en IPv4) o 'Tipo de Tráfico' (*TClass* en IPv6).

- Elemento del núcleo de red (*core function*). Se encargan del envío de paquetes según la marca de clasificación realizada anteriormente.

El clasificador de paquetes especifica las clases en el campo de cabecera 'TOS' y posteriormente son leídas para que se marque la prioridad (ver figura 48). Estas comprenden desde las que necesitan un determinado ancho de banda y un máximo retardo estricto hasta las de menos prioridad, y se les asigna un orden de preferencia para el descarte de paquetes. A continuación un distribuidor por clases de paquetes pone en marcha el tratamiento diferenciado que pasa a un proceso acondicionador.

Figura 48. Mecanismo de marcación y diferenciación en Diff Serv



DiffServ hace un tratamiento diferencial de los servicios según su sensibilidad al retardo o pérdida de paquetes. No necesita almacenar los estados de origen y destino de los enrutadores de núcleo como en IntServ, por lo que los enrutadores van más rápido. Sin embargo, hay que tener en cuenta que no es un servicio extremo a extremo ni es predictivo, es decir, no anticipa estados.

Los Servicios Integrados están más orientados a gestionar las redes de acceso, mientras que DiffServ es más adaptable al núcleo de red. Estos servicios son viables para el transporte de VoIP sobre redes bien dimensionadas, donde se puede optimizar el enrutamiento de los paquetes.

6.6.2 Protocolos y Mecanismos De Enrutamiento Con Qos. Así como los Servicios Diferenciados permiten mejorar la entrega de paquetes por

prioridades, actuando sobre los enrutadores, el principio de QOSPF (*QoS Path First*) es el de asegurar una QoS al nivel de enrutamiento. Este protocolo viene a completar OSPF, que permite calcular el camino más corto en función de la topología de red y del estado de los enlaces.

La idea de QOSPF es la de conservar un camino que ya existe dedicado a un flujo en tiempo real. En este caso lo que importa es la estabilidad de la ruta establecida, más que un acortamiento del camino. Con el progreso en la implantación de este tipo de algoritmo en los enrutadores, la QoS de la VoIP en combinación con otros protocolos de mayor nivel se verá mejorada.

En general, el enrutamiento basado en QoS (RFC 2386) persigue principalmente los siguientes objetivos:

1. Determinación de caminos viables. Se trata de elegir el camino, de entre varios disponibles, con mejor posibilidad de acomodo de QoS del flujo dado.

2. Optimización del uso de recursos. Mediante este esquema de enrutamiento se puede utilizar de manera eficiente los recursos de red para una mejor tasa de transferencia.

3. Degradación gradual. El enrutamiento dependiente de estados puede compensar las deficiencias transitorias en los nodos de red (por ejemplo

en una congestión), con mejor velocidad de transferencia y una degradación de prestaciones gradual en comparación con otro esquema intensivo en estados.

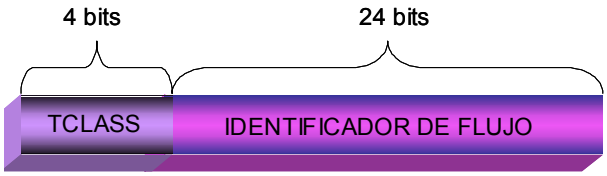
La precedencia IP utiliza los 3 bits de precedencia del campo ToS de cabecera IP para especificar la clase de servicio de cada paquete. Se pueden hasta seis clases de tráfico, según el valor del campo, y las técnicas de encolado de la red pueden utilizar esta señal para dar preferencia al tráfico en tiempo real.

De manera similar al campo ToS en IPv4, la “Etiqueta de Flujo” de una cabecera IPv6 puede ser utilizada para etiquetar paquetes que demanden un tratamiento particular de los enrutadores IP, y asegurar así una QoS. Contiene dos campos:

a) El identificador de flujo (trayectoria a seguir por la red).

b) El campo “TClass” proporciona un medio de identificar la prioridad de distribución deseada de los paquetes que lo contienen. La indicación del tipo de tráfico está dividida en dos grupos: los valores de 0 a 7 se utiliza para etiquetar paquetes con flujo controlado (como una transferencia ftp), mientras que los valores 8 al 15 se usan para etiquetar los paquetes sin control de flujo como los de “tiempo real” (por ejemplo, una sesión de VoIP), siendo el mayor valor el de más prioridad.

Figura 49. Etiqueta de flujo IPv6



Otros mecanismos de enrutamiento permiten de manera indirecta el mantenimiento de una calidad de servicio en una transmisión multimedia. Entre los más utilizados se encuentran:

- **CBWFQ** (*Commited Bandwith Weighted Fair Queueing*). Procedimiento que permite dividir el ancho de banda de manera ponderada entre diferentes clases de servicio, incluyendo una cola de salida de bajo retardo y prioridad absoluta de tráfico sobre otros. Bastante apropiado en caso de tráfico de voz.

- **CAR** (*Commited Access Rate*). Mecanismo para asegurar la velocidad de acceso sobre la interfaz de un enrutador, que puede realizar dos funciones:

    a) limitar la cantidad de tráfico a atravesar la interfaz,

    b) Insertar marcas indicadoras de QoS en paquetes entrantes y eliminarlas en salientes.

- **WRED** (*Weighted Random Early Detection*). Procedimiento de descarga de paquetes de manera aleatoria, en función de la prioridad, para situaciones de carga de la red.

6.7 MPLS

El encaminamiento convencional de los paquetes (protocolo de nivel 3) que viajan a través de enrutadores implica que éstos deben analizar la cabecera de cada paquete para tomar la decisión de envío hacia el siguiente, según un algoritmo de enrutamiento de nivel de red que determina el camino a seguir. Por otra parte, la mayoría de los protocolos de enrutamiento disponibles actualmente se basan en la obtención del camino más corto en la red para los paquetes y no consideran otras métricas de ingeniería de tráfico, tales como el retardo, fluctuaciones y congestión de tráfico, que pueden influir desfavorablemente en las prestaciones globales de la red.

La conmutación de etiquetas multiprotocolo, o MPLS, es un marco de especificación del IETF concebido para la designación, envío, enrutamiento y conmutación de flujos de tráfico de manera eficiente por la red. MPLS agrupa los paquetes de una sesión IP en un solo flujo, y etiqueta cada sesión para permitir su paso inmediato a través de enrutadores, separando el tráfico de

datos con conmutación de etiquetas en el nivel 2 (enlace) de los procedimientos de encaminamiento estándar IP en el nivel de red.

Al ser un protocolo de nivel inferior, MPLS no analiza las direcciones IP, consiguiendo unas características de privacidad y seguridad equivalentes a las de una LAN (Red de Área Local). MPLS se basa en esencia en:

- la separación entre las funciones de control (*routing*) y de envío (*forwarding*) típica en una transmisión asíncrona de datos en red

- El intercambio de etiquetas para el envío de paquetes.

Conceptualmente, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También se puede ver como un protocolo de túneles (sustituyendo a las técnicas habituales de "*tunneling*"), o como una técnica para acelerar el encaminamiento de paquetes, e incluso, como un sustituto de la función de enrutamiento. En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (enlace) y 3 (red), combinando eficazmente las funciones de control de enrutamiento con simplicidad y rapidez.

Mediante la asignación de una etiqueta a un dispositivo enrutador o conmutador y, de acuerdo con unas tablas de enrutamiento, MPLS comunica esta etiqueta a sus vecinos de tal manera que no tengan que analizar las

direcciones y el proceso de envío de paquetes se acelere. Las decisiones sobre asignación de etiquetas se basan en criterios de envío como si es destino único o multicast, ingeniería de tráfico/QoS, etc.

MPLS posee las siguientes características y funcionalidades:

- Especifica mecanismos para manejar flujos de tráfico de varios tipos, como flujos entre distintas máquinas o entre diferentes aplicaciones.

- Es independiente de protocolos de nivel 2 (como ATM o Frame Relay) y nivel 3 (red).

- Proporciona un medio de relacionar direcciones IP con etiquetas de longitud fija, empleadas por diferentes tecnologías de envío y conmutación de paquetes.

- Interfaces con protocolos de enrutamiento tales como protocolo de reserva de recursos (RSVP) y protocolo de camino más corto (OSPF)

CONCLUSIONES

El transporte de la voz tiene su historia en las redes tradicionales de conmutación de circuitos las cuales han estado presentes entre nosotros desde el momento en que se estableció la primera conversación en tiempo real, pero en la actualidad con el desarrollo de los sistemas computarizados y las redes de datos se ha incluido un nuevo concepto en el transporte de la voz, Voz Sobre IP es decir transporte de la voz sobre las redes de conmutación de paquetes y su mayor exponente las redes IP (base de la Internet), que han desarrollado una nueva plataforma para servicios de telecomunicaciones. Con este trabajo se ha demostrado que se está logrando un gran avance en el soporte de estos servicios sobre las redes IP, en especial la transmisión de la voz, que ha llevado a pensar a los operadores de telefonía tradicional en un concepto como es el de la convergencia, con la finalidad de evolucionar (NGN) y poder entrar de forma competitiva en el mercado futuro de las telecomunicaciones por medio de la integración e interoperabilidad con otros tipos de redes, en especial con las redes de conmutación de paquetes.

La ventaja competitiva de la voz sobre IP, en relación con la voz sobre circuitos conmutados, es su versatilidad y arquitectura flexible, lo que proporciona una red multiservicio con capacidad para soportar el tráfico de datos, videos y voz sobre una misma red.

Por medio del desarrollo de H.323 y de SIP, ha mejorado y expandido la utilización de voz sobre IP, actualmente se recomienda la utilización de H.323 por ser un estándar de mayor aplicación, experiencia y con una mayor interoperabilidad con la red telefónica publica conmutada, pero no se descarta que SIP esta tomando una gran acogida gracias a su simplicidad y se espera que con las nuevas investigaciones y pruebas que se están realizando este llegue a obtener la misma aceptación que H.323.

Aunque SIP y H.323 son dos protocolos rivales dentro de este servicio, lo deseable es desarrollar las bases para lograr una interoperabilidad entre los dos, logrando de esta forma mezclar lo simple de uno con la complejidad del otro, obteniendo de esta manera un servicio para la transmisión de voz de forma alternativa a la tradicional, respaldado por un estándar que cualquier otra tecnología desearía tener por ser robusto y a la vez simple al momento de adaptarse a cambios dentro o fuera de la red. Lo que atraería con mucha más fuerza nuevos y potenciales clientes.

La voz sobre IP tiene mucho que brindar, pero al mismo tiempo necesita evolucionar aún más sobre todo en el campo de calidad de servicio, en donde todavía le queda mucho campo por mejorar y demostrar que es un servicio que brinda seguridad y confianza en todos los posibles entornos de aplicación (empresarial, domestico, Internet).

Con relación a la calidad de servicios, la VoIP no está abriendo campo para lograr igualar la calidad de servicios de las redes de conmutación de circuitos, en especial a la de la PSTN. Esta diferencia se debe sobre todo sobretodo a que las redes de conmutación de paquetes tienen que lidiar con una característica que no existe en las redes de conmutación de circuitos que es la pérdida de paquetes, esta característica ha sido un duro reto en el desarrollo de la VoIP, ya que necesita ser reducida a lo mínimo posible para lograr un nivel de servicio satisfactorio.

RECOMENDACIONES

Se recomienda para futuros trabajos, tratar con mayor detenimiento aspectos como las diferentes versiones que se han desarrollado para el estándar H.323, así como para el protocolo SIP y profundizar en temas como convergencia y nueva generación de redes (NGN).

De igual forma se recomienda en futuros trabajos, desarrollar a profundidad temas de suma importancia en las comunicaciones actuales y sobre todo en la voz sobre IP como es el respaldo y la garantía que brinda Internet y su gran desarrollo para los operadores de telefonía que migren completamente a la transmisión de voz por paquetes.

ANEXOS

ANEXO A. CODIGO DE RESPUESTAS COMUNES DEL PROTOCOLO SIP

Respuesta provisional (1xx)	100	continuar
	180	llamando
	181	la llamada se está retransmitiendo
	182	la llamada está en cola
Éxito (2xx)	200	confirmación
	201	aceptación
Redirección (3xx)	300	varias posibilidades
	301	traslado permanente
	302	traslado provisional
Errores en el cliente (4xx)	400	petición incorrecta
	401	no autorizado
	402	ampliación incorrecta
	403	prohibido
	404	no encontrado
	480	no disponible temporalmente
	482	bucle detectado
	484	dirección incompleta
Errores en el servidor (5xx)	500	error interno del servidor
	501	no realizado
	502	pasarela no válida
	503	servicio no disponible
	505	versión no admitida
Errores globales	600	ocupado
	604	no existe
	606	inaceptable

REFERENCIAS BIBLIOGRAFICAS

Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (on line). Disponible en Internet: www.ahciet.net." Proporciona una información bastante actual sobre las telecomunicaciones en los artículos de su revista"

Architecture for Voice, Video and Integrated Data (on line). Cisco Systems, 2002. Disponible en Internet:
http://www.cisco.com/warp/public/cc/so/neso/vvda/iptl/avvid_wp.pdf
"Documento de cisco que describe la arquitectura para videos, datos y voz que utilizan para brindar estrategias de multiservicio y redes convergentes

BUSSE, Ingo; DEFFNER, Bernd y SCHULZRINNE, Henning. Dynamic QoS Control of Multimedia Applications Based on RTP (on line). Disponible en Internet:
http://www.fokus.gmd.de/step/acontrol/ac.htm "Este articulo hace a un mecanismo de tratamiento para el ancho de banda para aplicaciones multimedia, de igual manera hace una descripción puntual a los protocolos RTP y RTCP"

Grupo de Trabajo CDUI/UAT. H.225 (on line). Disponible en Internet: http://telecomunicaciones.uat.mx/h323/documentos como por ejemplo la “Pagina que brinda diferente tipo de información sobre H.225

IETF, Grupo de Network Working. RCF 2543 Session Initiation Protocol (on line). Disponible en Internet: http://www.ietf.org/rfc/rfc2543.txt “Documento publicado por el IETF por medio del grupo de trabajo de red, donde se definen las características del protocolo desarrollado por ellos SIP”.

IETF, Grupo de Network Working. RCF 2974 Session Announcement Protocol (on line). Disponible en Internet: http://www.ietf.org/rfc/rfc2974.txt “Documento publicado por el IETF por medio del grupo de trabajo de red, donde se definen las características del protocolo desarrollado por ellos SAP”.

IETF, Grupo de Network Working. RCF 1889 RTP: A Transport Protocol for Real-Time Applications (on line). Disponible en Internet: http://www.ietf.org/rfc/rfc1889.txt “Documento publicado por el IETF por medio del grupo de trabajo de red, donde se definen las características del protocolo desarrollado por ellos RTP”.

IETF, Grupo de Network Working. RCF 1663 Integrated Services in the Internet Architecture (on line). Disponible en Internet: http://www.ietf.org/rfc/rfc1663.txt " Documento publicado por el IETF por medio del grupo de trabajo de red, donde se definen características como mecanismos de control de tráfico, RSVP, modelo de servicios integrados).

ITU-T. Packet-Based Multimedia Communications Systems, Recommendation H.323, aprobado noviembre 2001 (on line). Disponible en Internet: ttp://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.323. "Plataforma de la ITU-T con la información del estándar H.323"

MONTESINO POUZOLS, Federico. Modelo de Aplicación de Sesión Multimedia. Sevilla, 2002, 116 h. Proyecto de Fin de Carrera (Ingeniero Informático). Universidad de Sevilla. Escuela Técnica Superior de Ingeniería Informática.

Plataforma (on line). Disponible en Internet: www.webproforum.com "Plataforma que sirve de enlace a diferentes e tutoriales y manuales con información sobre H.323 (Gatekeeper, Gateway, etc.), VoIP, QoS en VoIP, etc."

Plataforma (on line). Disponible en Internet: http://www.packetizer.com/. "Plataforma que brinda información muy completa acerca de H.323 y SIP en un mismo lugar".