# TUTORIAL VOZ SOBRE IP (VOIP)

**CÉSAR ADOLFO LÓPEZ MORANTE**

**ADALBERTO JOSE OSPINO CASTRO**

**UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**FACULTAD DE INGENIERÍA ELECTRICA Y ELECTRONICA**

**CARTAGENA DE INDIAS**

**2005**

# TUTORIAL VOZ SOBRE IP (VOIP)

**CÉSAR ADOLFO LÓPEZ MORANTE**

**ADALBERTO JOSE OSPINO CASTRO**

**Monografía, presentada como requisito de aprobación del Minor en Comunicaciones y Redes 2005**

**Director**

**DAVID ELIÉCER SEÑIOR ELLES**

**Ingeniero Electrónico**

**UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**FACULTAD DE INGENIERÍA ELECTRICA Y ELECTRONICA**

**CARTAGENA DE INDIAS**

**2005**

**Nota de Aceptación**

_____

_____

_____

_____

_____

_____

**Firma del presidente del jurado**

_____

**Firma del jurado**

_____

**Firma del jurado**

**Cartagena, 23 de  octubre del 2005**

*El agradecimiento es una de las virtudes menos practicada por los seres humanos, como decía Ortega y Gasset, somos lo que somos y nuestras circunstancias, y dentro de todo lo que nos rodea, un factor determinante es el ser humano. Pasamos la vida rodeado de diferentes personas a quienes vamos clasificando como amigos, enemigos, extraños, conocidos, simpáticos, antipáticos y muchos otros rótulos, pero, de una u otra manera, todas estas personas colaboran con nosotros y con ellas interrelacionamos para ser el individuo que somos.*

*Este es un agradecimiento general, pero no por eso menos sentido. Primero: A DIOS, por darme vida, salud y permitir que me dedique a lo que me gusta.....un agradecimiento celestial...*

*A mis padres: CÉSAR ADOLFO LÓPEZ LUNA Y BETTY LUZ MORANTE, quienes, aparte del amor, la dedicación y el interés, me infundieron la ética y el rigor que guían mi transitar por la vida.*

*Al Ingeniero GONZALO LÓPEZ VERGARA por su predisposición permanente e incondicional en aclarar mis dudas y por sus substanciales sugerencias durante la redacción de la Monografía, así como en sus observaciones críticas en la redacción del trabajo, por su amistad.*

*A nuestro Director de Monografía: Ingeniero DAVID SEÑOR ELLES por su asesoramiento Técnico y estímulo para seguir creciendo intelectualmente.*

*CÉSAR ADOLFO LÓPEZ MORANTE*

*Mis agradecimientos a Dios por haberme dado el ser, el entendimiento la salud, por brindarme la fortaleza para superar y enfrentar en la vida. todos los momentos buenos y todos aquellos que quisiera olvidar.*

*A mi padre ADALBERTO OSPINO OSPINO, aunque DIOS no nos brindo la oportunidad de pasar más tiempo juntos, sé que siempre te has sentido y te sentirás orgulloso de mí, sé que siempre has estado junto a mí, en cada momento de mi vida, por estas razones y muchas otras más te dedico este logro.*

*A mi madre CARMEN CASTRO DE OSPINO por el amor, ejemplo de conducta y sacrificio personal que me permitieron una educación de excelencia y un apoyo y estímulo constante.*

*A mis familiares más íntimos por la comprensión demostrada en relación a mi quehacer académico y laboral 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 director de monografía DAVIS SEÑOR ELLES y al ingeniero GONZALO LÓPEZ VERGARA.*

*ADALBERTO JOSE OSPINO CASTRO*

**CONTENIDO**

**Pág.**

## LISTA DE FIGURAS

## LISTA DE ANEXOS

**Pág.**

# GLOSARIO

| Términos | Descripción |
|---|---|
| **Access Gateway** | Gateway de acceso<br><br>Un gateway (pasarela) es un elemento de la red que actúa como punto de entrada a otra red. Un access gateway es un gateway entre la red telefónica y otras redes como Internet. |
| **ACD** | **A**utomatic **C**all **D**istributor<br><br>Distribuidor automático de llamadas. Sistema telefónico especializado que puede manejar llamadas entrantes o realizar llamadas salientes. Puede reconocer y responder una llamada entrante, buscar en su base de datos instrucciones sobre qué hacer con la llamada, reproducir locuciones, grabar respuestas del usuario y enviar la llamada a un operador, cuando haya uno libre o cuando termine la locución. |

**ACTA** **A**merica's **C**arriers **T**elecommunications **A**ssociation

Agrupación de pequeñas operadoras de larga distancia. Con sede en Casselberry (Florida), fundada en 1985 por 15 pequeñas compañías de larga distancia para "proporcionar una representación nacional antes los cuerpos legisladores y reguladores, además de contribuir a la mejora de las relaciones comerciales de la industria". Actualmente cuenta con más de 165 miembros.

**ADPCM** **A**daptive **D**igital **P**ulse **C**ode **M**odulation

Forma de codificar el sonido de forma que ocupe menos espacio.

**ADSL** **A**symmetric **D**igital **S**ubscriber **L**ine

Método para aumentar la velocidad de transmisión en un cable de cobre. ADSL facilita la división de capacidad en un canal con velocidad más alta para el suscriptor, típicamente para transmisión de vídeo, y un canal con velocidad significativamente más baja en la otra dirección.

**AMPS** **A**dvanced **M**obile **P**hone **S**ervice

Son las especificaciones del estándar original de los sistemas analógicos. Hoy en día se utiliza principalmente en Norteamérica, Latinoamérica, Australia, así como parte de Rusia y Asia.

**ANI** **A**utomatic **N**umber **I**dentification

Detección del número que llama.

**ANSI** **A**merican **N**ational **S**tandards **I**nstitute

Organización que desarrolla y publica voluntariamente estándares para un amplio sector de industrias en USA.

**API** **A**pplication **P**rogramming **I**nterface

API especifica el formato de los mensajes y el lenguaje utilizado por un programa para comunicarse con el sistema operativo o con otro programa.

**ASP** **A**pplication **S**ervice **P**rovider

Compañía que proporciona acceso remoto a aplicaciones, normalmente sobre Internet. Son útiles cuando una organización encuentra más rentable que otro se encargue de instalar, implementar y mantener las aplicaciones que utiliza. Las aplicaciones pueden ser tan sencillas como el acceso a un servidor de ficheros, o tan complejas como el acceso a través de navegador a un sistema de apoyo a las decisiones empresariales. La mayoría de los ASPs proporcionan los servidores, el acceso a la red y las aplicaciones en forma de suscripción mensual o anual.

**ATM** **A**synchronous **T**ransfer **M**ode

ATM es una tecnología de conmutación de red que utiliza celdas de 53 bytes, útil tanto para LAN como para WAN, que soporta voz, vídeo y datos en tiempo real y sobre la misma infraestructura. Utiliza conmutadores que permiten establecer un circuito lógico entre terminales, fácilmente escalable en ancho de banda y garantiza una cierta calidad de servicio (QoS) para la transmisión. Sin embargo, a diferencia de los conmutadores telefónicos, que dedican un circuito dedicado entre terminales, el ancho de banda no

utilizado en los circuitos lógicos ATM se puede aprovechar para otros usos.

**BCP** **B**roadband **C**ommunications **P**rovider

Un nuevo tipo de compañías de telecomunicaciones que combinan lo mejor de los tres proveedores tradicionales de voz y datos:

- CLECs: Competitive Local Exchange Carriers.
- ICPs: Integrated Communications Providers.
- ISPs: Internet Service Providers.

para implementar servicios multimedia sobre redes de banda ancha.

**Bluetooth** Tecnología de radio desarrollada por Ericsson y otras compañías. Construida alrededor un novedoso chip que hace posible transmitir señales en distancias cortas, sin el uso de cables, entre teléfonos, computadoras y otros dispositivos.

**Broadband** Servicios en red de datos, audio y vídeo de alta velocidad que son digitales, interactivos y basados en paquetes. El ancho de banda es 384 Kb o mayor, que es el mínimo ancho

de banda requerido para transmitir vídeo digital de calidad.

**C7** Common **C**hannel Signaling System No. **7** Ver **SS7**.

**Call me** Servicio integrado en la sede web del cliente, que permite a los usuarios que lo soliciten recibir la llamada de un agente.

**CCITT ley-A y ley-u** Codec de audio (tanto ley-A como ley-u). Son estándares del CCITT de aplicación en comunicaciones telefónicas. Incluyen la codificación y la compresión de la señal y también se utilizan en Telefonía IP.

**CDMA** **C**ode **D**ivision **M**ultiple **A**ccess

Es una tecnología de banda ancha para transmisión digital de señales de radio entre, por ejemplo, un teléfono móvil y una estación radiobase. En CDMA, una frecuencia se divide en un número de códigos. Este estándar se utiliza en Norteamérica, Latinoamérica, Europa del Este, Asia y

Oriente Medio.

**CIM** **C**ustomer **I**nteraction **M**anagement

Reciben este nombre la tecnología y los procesos asociados que permiten manejar de forma coordinada múltiples sistemas de relación con los clientes, incluyendo telefonía, email e interacción con el sitio Web.

**CLEC** **C**ompetitive **L**ocal **E**xchange **C**arrier

Creado por el Acta de Telecomunicaciones de 1996, un CLEC es un proveedor de servicios que está en competencia directa con un proveedor de servicios ya establecido. CLEC se utiliza a menudo para designar de forma general a cualquier competidor, pero el término tiene realmente implicaciones legales. Para ser considerado un CLEC, un proveedor de servicio debe obtener ese reconocimiento de algún organismo oficial o estatal. Como compensación al tiempo y dinero invertido en ganarse ese reconocimiento, el CLEC obtiene autorización para colocar sus equipos en las dependencias del proveedor de servicios ya establecido.

**Codec** Codec

Algoritmos de Compresión/Descompresión. Se utilizan para reducir el tamaño de los datos multimedia, tanto audio como vídeo. Compactan (codifican) un flujo de datos multimedia cuando se envía y lo restituyen (decodifican) cuando se recibe.

Si alguna vez recibes un fichero o una llamada telefónica y no puedes escuchar nada, lo más probable es que la aplicación que utilizas no soporte el codec con el que se han codificado los datos.

Entre los codec de audio más extendidos se encuentran: GSM (Global Standard for Mobile Communications), ADPCM, PCM, DSP TrueSpeech, CCITT y Lernout & Hauspie. Y entre los codec de vídeo tenemos a Cinepak, Indeo, Video 1 y RLE.

**CPCI, CompactPCI** **C**ompact **P**eripheral **C**omponent **I**nterface

CPCI es una combinación del bus PCI contenido en una tarjeta con formato Eurocard (varios tamaños disponibles). Eurocard proporciona mayor robustez y fiabilidad a la hora

de conectar dispositivos en sistemas embebidos que las tarjetas PCI estándar utilizadas en equipos de sobremesa. Se pueden intercambiar sin apagar el equipo y tienen mayor rendimiento (32-bit, 33MHz) que el bus ISA.

**CPSB** **C**ompactPCI **P**acket **S**witching **B**ackplane

Todavía es una propuesta (subcomité técnico PICMG 2.16). Se trata de una red Ethernet conmutada redundante 10/100/1000 en un chasis CompactPCI proporcionando conectividad IP entre todos los slots cPCI/cPSB utilizando una topología en estrella.

**CRM** **C**ustomer **R**elationship **M**anagement

La forma en que una compañía maneja las relaciones con sus clientes. Una solución CRM exitosa depende de la habilidad para interactuar con los clientes a través de cualquier canal que ellos elijan, así como seguir la pista y mantener información en todo momento de las interacciones de los clientes con dichos canales, de forma que podamos tener siempre una visión de conjunto completa del cliente.

**CRS** **C**hannelized **R**eserved **S**ervices

Una arquitectura basada en estándares que permite el autoaprovisionamiento de aplicaciones de próxima generación en redes ópticas. Los servicios se reservan utilizando ciertos canales del ancho de banda disponible 'al vuelo', de forma que se ajusten a los requerimientos de la aplicación. Diseñado para reducir costes y tiempos de puesta en servicio de los proveedores de servicio, la arquitectura CRS integra redes IP con transporte óptico inteligente, permitiendo capacidades de multidifusión y reserva dinámica de ancho de banda.

**CSLIP** **C**ompressed **S**erial **L**ine **I**nterface **P**rotocol

Una versión optimizada del protocolo SLIP (Serial Line Interface Protocol), utilizado habitualmente para conectar PCs a Internet a través de líneas telefónicas. Incluye compresión, lo que permite aumentar el flujo de datos.

**CT** **C**omputer **T**elephony

Añadir las posibilidades que ofrecen los ordenadores a la

realización, recepción y manejo de las llamadas telefónicas.

**CT Server** **C**omputer **T**elephony **Server**

Un servidor de comunicaciones abierto basado en estándares para proporcionar servicios en un entorno empresarial o en una centralita. Basado en software, permite que diferentes tecnologías y aplicaciones de varios vendedores ínter operen sobre un único servidor.

**DECT** **D**igital **E**nhanced **C**ordless **T**elecommunications

Una norma común para telefonía personal inalámbrica. Originalmente establecida por ETSI, un ente europeo de estandarización. DECT es un sistema para negocios de comunicaciones inalámbricas.

**DNIS** **D**ialed **N**umber **I**dentification **S**ervice

Un servicio telefónico que permite al llamado saber el número marcado por el llamante. Es una prestación habitual en los números gratuitos (800 y 900), y permite identificar el número originalmente marcado cuando varios números

900 acaban en un mismo circuito. Funcionan pasando el número marcado al dispositivo destino de la llamada, que puede actuar en función de ese dato a la hora de enrutar, encolar o tratar la llamada en general. Un uso típico consiste en dar un tratamiento diferenciado a los usuarios llamantes en campañas de marketing o simplemente en las llamadas a un centro de llamadas (Call Center).

**DSL** **D**igital **S**ubscriber **L**ine

Tecnología que permite a un proveedor usar el exceso de ancho de banda de sus líneas de pares de cobre para proporcionar servicios de datos. En principio se pensó como una tecnología de transición hasta que estuvieran disponibles las infraestructuras de fibra óptica, pero ha llegado a convertirse en una industria en si misma. xDSL se utiliza para describir distintas variantes del DSL general.

**DSP** **D**igital **S**ignal **P**rocessor

Un microprocesador digital especializado que realiza cálculos o digitaliza señales originalmente analógicas. Su gran ventaja es que son programables. Entre sus principales usos está la compresión de señales de voz. Son la pieza clave de

los codec.

**DTM** **D**ynamic Synchronous **T**ransfer **M**ode

Tecnología de conmutación de circuitos dinámica que proporciona transporte entre routers a través de canales, y permite el transporte óptico de información a altas velocidades.

En DTM, un canal tiene un ancho de banda dedicado, y forma una ruta dinámica entre emisor y receptor, pasando a través de routers en su camino. Canales con cierta calidad de servicio (QoS) son establecidos 'al vuelo' y fijados de forma extremadamente rápida.

**DTMF** **D**ual-**T**one **M**ultifrequency

Una forma de señalización consistente en uno o varios botones, o un teclado numérico completo como en el caso de los teléfonos, que envía un sonido formado por dos tonos discretos, sonido que es recogido e interpretado por los sistemas telefónicos (centrales, centralitas o conmutadores).

**E1** Conexión por medio de la línea telefónica que puede

transportar datos con una velocidad de hasta 1,920 Mbps. Según el estándar europeo (ITU), un E1 está formado por 30 canales de datos de 64 kbps más 2 canales de señalización. E1 es la versión europea de T1 (DS-1). Velocidades disponibles:

| | | | | |
|---|---|---|---|---|
| E1: | 30 | canales, | 2,048 | Mbps |
| E2: | 120 | canales, | 8,448 | Mbps |
| E3: | 480 | canales, | 34,368 | Mbps |
| E4: | 1920 | canales, | 139,264 | Mbps |
| E5: | 7680 | canales, | 565,148 | Mbps |

**ECTF** **E**nterprise **C**omputer **T**elephony **F**orum

Organización sin ánimo de lucro, con sede en California, que desarrolla estándares de telefonía por ordenador. Fundada por Dialogic, Digital Equipment Corporation, Ericsson, Hewlett-Packard y Nortel, el ECTF tiene ahora 36 miembros principales, incluyendo a AT&T, IBM y Sun Microsystems.

**EDGE** **E**nhanced **D**ata **G**SM **E**nvironment

Tecnología que da a GSMA y TDMA una capacidad similar para el manejo de servicios de tercera generación de telefonía móvil. EDGE fue desarrollado para permitir la transmisión de grandes cantidades grandes de datos a alta velocidad, 384 kilobits por segundo.

**Edge Switch** Un dispositivo de conmutación de red diseñado para realizar funciones normalmente asociadas con un router en un entorno de LAN o WAN.

**Embedded System** Conjunto software y hardware que forma parte de algún sistema mayor y que se funciona sin intervención humana. Un sistema embebido típico sería una tarjeta microcomputadora con software en ROM, que realiza cierta tarea de forma ininterrumpida. Puede incluir algún tipo de sistema operativo (muy sencillo normalmente), no suele contar con periféricos (teclado, monitor o discos) y raramente tienen interfaz con el usuario. En muchos casos debe proporcionar respuesta en tiempo real.

**EPOC** Sistema operativo para terminales móviles, desarrollado por Symbian (alianza estratégica de Ericsson, Matsushita, Motorola, Nokia y Psion).

**ETSI** **E**uropean **T**elecommunications **S**tandards **I**nstitute

Organismo europeo de estandarización para telecomunicaciones.

**FCC** **F**ederal **C**ommunications **C**ommission

La agencia federal de USA responsable de regular las comunicaciones interestatales e internacionales por radio, televisión, cable y satélite.

**Frame Relay** Es un protocolo estándar para interconectar LANs. Proporciona un método rápido y eficiente para transmitir información desde dispositivos de usuario a bridges y routers. Se utiliza el ancho de banda disponible sólo cuando se necesita. Para transmitir la información se divide en paquetes, este método de transmisión resulta eficiente al transmitir comunicaciones de voz, con un adecuado control.

**G.lite** Una versión de ADSL (ver DSL) que ofrece 1.5 Mbps de bajada y 640 Kbps de subida y está diseñada especialmente para el mercado de consumo. G.lite hace innecesario en muchos casos enviar personal especializado por parte de las operadoras para instalar nuevo cableado al cliente o un 'splitter', que es un dispositivo que separa las señales de voz y datos en casa del usuario.

**Gatekeeper** Un componente del estándar ITU H.323. Es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia. Los Gatekeepers proporcionan la inteligencia de red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de los detalles de las llamadas para tarificar y comunicación con el sistema de gestión de la red. También monitorizan la red para permitir su gestión en tiempo real, el balanceo de carga y el control del ancho de banda utilizado.

**Gateway** En general se trata de una pasarela entre dos redes. Técnicamente se trata de un dispositivo repetidor electrónico

que intercepta y adecua señales eléctricas de una red a otra. En Telefonía IP se entiende que estamos hablando de un dispositivo que actúa de pasarela entre la red telefónica y una red IP. Es capaz de convertir las llamadas de voz y fax, en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet.

**GPRS** **G**eneral **P**acket **R**adio **S**ervice

Se trata de una mejora al sistema de comunicaciones móvil GSM para permitir paquetes de datos. GPRS permite un flujo continuo de paquetes IP de datos permitiendo servicios como la navegación por Internet o la transferencia de ficheros. GPRS mejora el servicio de mensajes cortos disponible en GSM (GSM-SMS), ya que éste limita los mensajes a 160 bytes de longitud.

**GSM** **G**lobal **S**ystem for **M**obile Communications

GSM es la tecnología telefónica móvil digital basada en TDMA predominante en Europa, aunque se usa en otras zonas del mundo. Se desarrolló en los años 80 y se desplegó en siete países europeos en 1992. Se utiliza en Europa,

Asia, Australia, Norteamérica y Chile. Opera en las bandas de 900MHz y 1.8GHz en Europa y en la banda de 1.9GHz PCS en U.S.A.

GSM define el sistema celular completo, no sólo el interface radio (TDMA, CDMA, etc.). En 2000 había más de 250 millones de usuarios GSM, lo que representa más de la mitad de la población mundial de usuarios de telefonía móvil.

**H.110** Una especificación de bus TDM o una capa física de la telefonía por ordenador, utilizada para conectar recursos a nivel de tarjeta dentro de un chasis CompactPCI.

Por ejemplo, un bus H.110 se puede utilizar para llevar canales entre una tarjeta de interfaz T-1/E-1 y otra tarjeta con DSPs. El bus H.110 soporta hasta 4.096 canales simultáneos.

**H.323** H.323 es la recomendación global (incluye referencias a otros estándares, como H.225 y H.245) de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para las comunicaciones multimedia sobre redes

basadas en paquetes que no proporcionan una Calidad de Servicio (QoS, Quality of Service) garantizada.

**Handshake** Protocolo que permite al emisor y receptor ponerse de acuerdo a la hora de intercambiar datos entre ellos. Permite negociar la velocidad de transferencia inicial y variarla a medida que transcurre el intercambio de datos.

**HDLC** **H**igh Level **D**ata **L**ink **C**ontrol

Protocolo desarrollado por ISO y basado en trabajos previos realizados por IBM sobre SDLC.

**Hot Swap** Retirar un componente de un sistema e introducir uno nuevo sin apagarlo y mientras el sistema sigue funcionando con normalidad. En los sistemas redundantes es posible hacerlo con muchos de sus componentes: discos, tarjetas, fuentes de alimentación, en general con todos aquellos componentes que hayan sido duplicados dentro del sistema.

**HSCSD** **H**igh **S**peed **C**ircuit **S**witched **D**ata

Mejora al sistema de comunicaciones móvil GSM que

permite combinar hasta cuatro canales de 14.4 Kbps y conseguir así transferencias de datos de 57.6 Kbps. Parte de la fase 2 de GSM, HSCSD es adecuado para videoconferencia y transmisiones multimedia.

**IAD** **I**ntegrated **A**ccess **D**evice

Dispositivo que procesa voz y tráfico de datos en un único punto de una red local (LAN) o de área extendida (WAN).

**ICP** **I**ntegrated **C**ommunications **P**rovider

Un proveedor de servicios que proporciona tanto facilidades generales de red como facilidades a medida para empresas y particulares, como voz, datos y aplicaciones. Estos servicios se proporcionan simultáneamente sobre el mismo canal (red telefónica, cable, DSL). Utilizando un ICP, los usuarios pueden resolver todas sus necesidades de comunicación a través de un sólo proveedor y con una factura única.

**IETF** **I**nternet **E**ngineering **T**ask **F**orce

Se reúne tres veces al año para fijar estándares técnicos

sobre temas relacionados con Internet.

**IFRF** **I**nternet **F**ax **R**outing **F**orum

Grupo que ha publicado una especificación que permite a las empresas interconectar sus servidores de fax a Internet, de forma que los proveedores de servicio puedan enrutar y transmitir sus faxes.

**IMAP** **I**nternet **M**essaging **A**pplication **P**rotocol

Protocolo que permite a un servidor central de correo proporcionar acceso remoto a los mensajes de correo. IMAP4 es la última versión y es más sofisticado y versátil que POP3 (Post Office Protocol).

**IMTC** **I**nternational **M**ultimedia **T**eleconferencing **C**onsortium

Organización sin ánimo de lucro dedicada a desarrollar y promover estándares para videoconferencia.

**IP** **I**nternet **P**rotocol

La parte IP del protocolo de comunicaciones TCP/IP. Implementa el nivel de red (capa 3 de la pila de protocolos OSI), que contiene una dirección de red y se utiliza para enrutar un paquete hacia otra red o subred. IP acepta paquetes de la capa 4 de transporte (TCP o UDP), añade su propia cabecera y envía un datagrama a la capa 2 (enlace). Puede fragmentar el paquete para acomodarse a la máxima unidad de transmisión (MTU, Maximum Transmission Unit) de la red.

**IP PBX** **IP P**rivate **B**ranch e**X**change

Centralita IP. Dispositivo de red IP que se encarga de conmutar tráfico telefónico de VoIP.

**IP Telephony** **Telefonía IP**

Tecnología para la transmisión de llamadas telefónicas ordinarias sobre Internet u otras redes de paquetes utilizando un PC, gateways y teléfonos estándar.

En general, servicios de comunicación - voz, fax,

aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional. Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

**IRC** **I**nternet **R**elay **C**hat

Red de canales temáticos donde puedes hablar y conocer a otras personas. Para utilizarlo necesitarás algún cliente IRC y conexión a un servidor IRC. Muchos ISP disponen de servidores IRC y permiten el acceso a través de Web, lo que evita tener que utilizar un programa específico.

**IS-95** **I**nterim **S**tandard**-95**

Una norma de telefonía móvil digital basada en tecnología CDMA.

**IS-136** **I**nterim **S**tandard**-136**

Una norma de telefonía móvil digital basada en tecnología TDMA.

**ISDN** **I**ntegrated **S**ervices **D**igital **N**etwork (**RDSI, R**ed **D**igital de **S**ervicios **I**ntegrados)

Red telefónica pensada para mejorar los servicios de telecomunicaciones a nivel mundial. Proporciona un estándar aceptado internacionalmente para voz, datos y señalización. Todas las transmisiones son digitales extremo a extremo, utiliza señalización fuera de banda, y proporciona más ancho de banda que la red telefónica tradicional.

**IsoEthernet** **Iso**chronous **Ethernet**

Una extensión del estándar Ethernet propuesto por IBM y National Semiconductor, que permite transportar tanto llamadas de voz o vídeo junto a los paquetes de datos sobre

el mismo cable.

**ISUP** **I**ntegrated **S**ervices Digital Network **U**ser **P**art

ISUP es una capa del protocolo SS7. Los mensajes ISUP (orientados a conexión) se utilizan para establecer y liberar llamadas telefónicas. ISUP define un protocolo que permite iniciar la llamada, reservar un camino para la voz y los datos entre los dispositivos y liberar la llamada. A pesar de tratarse de una capa del protocolo SS7, su uso no se limita a las llamadas RDSI.

**ITU-T** **I**nternational **T**elecommunications **U**nion - **T**elecommunication

Antes conocida como CCITT (Comite Consultatif Internationale de Telegraphie et Telephonie). Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones: crea estándares, reparte frecuencias para varios servicios, etc.

**IVR** **I**nteractive **V**oice **R**esponse

IVR consiste en un conjunto de mensajes de voz y marcación de tonos desde un teléfono, de este modo se obtiene información del usuario llamante que en el destino sirve para la autenticación e identificación del mismo. También permite realizar transacciones totalmente automatizadas.

Ultimamente las tecnologías de reconocimiento del habla están reemplazando a la detección de tonos DTMF, debido a la mejora en la fiabilidad que se ha conseguido.

**J1** La versión japonesa del sistema E en Europa o T en Norteamérica.

| | | | | |
|---|---|---|---|---|
| J1: | 24 | canales, | 1.544 | Mbps |
| J2: | 96 | canales, | 6.312 | Mbps |
| J3: | 480 | canales, | 32.064 | Mbps |
| J4: | 1440 | canales, | 97.728 | Mbps |
| J5: | 5760 | canales, | 400.352 | Mbps |

**LAN** **L**ocal **A**rea **N**etwork

Red de área local. Una red pequeña de datos que cubre un

área limitada, como el interior de un edificio o un grupo reducido de edificios.

**LAPD** **L**ink **A**ccess **P**rotocol - Channel **D**

LAPD es un protocolo de nivel 2 definido en CCITT Q.920/921. LAPD funciona en Modo Asíncrono Balanceado (ABM, Asynchronous Balanced Mode), siendo este modo totalmente balanceado, es decir, no hay relación maestro/esclavo.

**LDAP** **L**ightweight **D**irectory **A**ccess **P**rotocol

Es un protocolo software que permite localizar a personas, organizaciones y otros recursos como ficheros o dispositivos en una red, bien en Internet o en una intranet. LDAP es una versión *ligera* del Protocolo de Acceso a Directorio (DAP), que a su vez es parte del protocolo X.500, un estándar para servicios de directorio en red. LDAP es más ligero porque es su versión inicial no incluía características de seguridad.
Desarrollado originalmente en la Universidad de Michigan, actualmente lo utilizan más de 40 compañías en sus

productos: Netscape lo incluye en la última versión del Comunnicator, Microsoft lo utiliza en su Directorio Activo y en Outlook Express. Novell en sus servicios de directorio NetWare y Cisco en sus equipos para redes.

**LEC** **L**ocal **E**xchange **C**arrier

Compañía que proporciona servicios telefónicos a nivel local.

**Media Gateway** Denominación genérica para referirse a varios productos agrupados bajo el protocolo MGCP (Media Gateway Control Protocol). La principal misión de un Media Gateway es la conversión IP/TDM bajo el control de un Softswitch.

**Media Server** Dispositivo que procesa aplicaciones multimedia como distribución de llamadas, fax bajo demanda y programas de respuesta a emails automática. Facilitan el mantenimiento y la administración, ofrecen menores costes y aportan mayor flexibilidad a la hora de desarrollar nuevas aplicaciones.

**MEGACO** **Me**dia **Ga**teway **Co**ntrol

MEGACO es un protocolo de VoIP, combinación de los protocolos MGCP e IPDC. Es más sencillo que H.323.

**MGCP** **M**edia **G**ateway **C**ontroller **P**rotocol

MGCP es un protocolo de control de dispositivos, donde un gateway esclavo (MG, Media Gateway) es controlado por un maestro (MGC, Media Gateway Controller).

**Modem** **MO**dulator - **DEM**odulator

Este término proviene de las palabras Modulador - Demodulador. Equipo que convierte señales digitales en analógicas y viceversa. Los modems se utilizan para enviar datos digitales a través de la red telefónica (PSTN), que normalmente es analógica. Un módem realiza una modulación del mensaje digital, convirtiéndolo en tonos que pueden ser enviados a través de la red telefónica. Al otro extremo, el demodulador del módem vuelve a convertir los tonos en una secuencia binaria (mensaje digital).

**Module** Módulo

Una tarjeta que no puede trabajar sola, debe conectarse a otra tarjeta.

**MTP** **M**essage **T**rasfer **P**art

MTP forma parte del protocolo SS7. Se divide en tres niveles (ver MTP-1, MTP-2 y MTP-3).

**MTP-1** **M**essage **T**rasfer **P**art **- 1**

El nivel 1 de MTP es equivalente a la capa de nivel físico de OSI. Define las características funcionales, eléctricas y físicas del enlace de señalización digital. Entre los interfaces físicos definidos se incluyen los siguientes: E-1 (2048 kb/s; 32 canales de 64 kb/s), DS-1 (1544 kb/s; 24 canales de 64kb/s), V.35 (64 kb/s), DS-0 (64 kb/s), y DS-0A (56 kb/s).

**MTP-2** **M**essage **T**rasfer **P**art **- 2**

El nivel 2 de MTP es equivalente a la capa de enlace de OSI. Asegura la transmisión sin errores extremo a extremo de un mensaje a través del enlace de señalización. Implementa control de flujo, validación de la secuencia de los mensajes y

control de errores. Cuando se produce un error en un enlace de señalización, el mensaje (o el conjunto de mensajes) es retransmitido.

**MTP-3** **M**essage **T**rasfer **P**art **- 3**

El nivel 3 de MTP es equivalente a la capa de red de OSI. Proporciona enrutamiento entre puntos de señalización de la red SS7. Es capaz de re-enrutar tráfico evitando enlaces y puntos de señalización averiados, y aplicar control de tráfico cuando ocurren congestiones en la red.

**Multi-Service Router** Un tipo de router que examina las llamadas en la red telefónica antes de que sean enviadas a un destino concreto. Se basa en un enlace especial de señalización que llega de la centralita y permite que un sistema de pre-enrutamiento reciba dicha señalización, examine el estado actual del call center y le devuelva una notificación a la centralita para que ésta envíe la llamada al destino elegido. La ventaja es que la llamada es enrutada o desviada antes de aceptarla.

**NAT** **N**etwork **A**ddress **T**ranslation

Un estándar definido en la RFC 1631 que permite a una red de área local (LAN) utilizar un conjunto de direcciones IP internamente y un segundo conjunto de direcciones externamente. El dispositivo que hace NAT se sitúa en el punto de salida a Internet y realiza todas las traducciones de direcciones IP que sean necesarias.

NAT tiene básicamente tres propósitos:
1.-Proporcionar funcionalidad de firewall al ocultar las direcciones IP internas.
2.-Permitir a una compañía utilizar todas las direcciones IP internas que desee sin posibilidad de conflicto con otras compañías y un conjunto limitado de direcciones externas.
3.-Combinar varios tipos de conexiones (normalmente RDSI) en una única conexión a Internet.

**NMT** **N**ordic **M**obile **T**elephone

Normativa Nórdica para la telefonía móvil analógica. Establecida por las administraciones de telecomunicaciones en Suecia, Noruega, Finlandia y Dinamarca a principios de

los años 80. Los sistemas NMT han sido instalados también en otros países europeos, incluyendo parte de Rusia, Medio Oriente y Asia.

**OpenVoB** **Open V**oice **o**ver **B**roadband

Organización sin ánimo de lucro creada para promover y acelerar el desarrollo de la tecnología de voz sobre redes de banda ancha, sus aplicaciones y los servicios relacionados.

Su objetivo es utilizar estándares abiertos existentes para que productos y servicios de distintos fabricantes puedan interoperar entre ellos.

**PBX** **P**rivate **B**ranch e**X**change

Centralita, central privada. Un sistema telefónico utilizado en compañías y organizaciones, privado por tanto, para manejar llamadas externas e internas. La ventaja es que la compañía no necesita una línea telefónica para cada uno de sus teléfonos. Además las llamadas internas no salen al exterior y por tanto no son facturadas.

**PCI** **P**eripheral **C**omponent **I**nterconnect

Se trata de un bus para periféricos utilizado en PCs, Macintoshes y Workstations. Proporciona un enlace de datos de alta velocidad entre la CPU y los periféricos (tarjetas de vídeo, discos, red, etc.).
PCI proporciona facilidades *conectar y listo* (plug and play), configurándose las tarjetas PCI automáticamente en el arranque del equipo. También permite compartir interrupciones (IRQs), lo que alivia el problema del limitado número de IRQs disponibles en un PC.
PCI soporta una velocidad de 33 MHz, puede mover datos a 32 y 64 bits y soporta *bus mastering*. La versión 2.1 de PCI llega hasta 66 MHz, por lo que duplica el rendimiento.

**PCM** **P**ulse **C**ode **M**odulation

Convierte una señal analógica (sonido, voz normalmente) en digital para que pueda ser procesada por un dispositivo digital, normalmente un ordenador. Si, como ocurre en Telefonía IP, nos interesa comprimir el resultado para transmitirlo ocupando el menor ancho de banda posible, necesitaremos usar además un codec.

**PCS** **P**ersonal **C**ommunications **S**ervices

PCS se refiere a servicios inalámbricos que surgieron después de que el gobierno de U.S.A. subastara licencias comerciales en 1994 y 1995. Se trata de la banda 1.8-2GHz y se suele utilizar para transmisión celular digital que compite con los servicios tanto analógicos como digitales en las bandas de 800Mhz y 900MHz.

**PDC** **C**elular **P**ersonal **D**igital

Estándar japonés para telefonía móvil digital.

**Policy Manager** Un elemento de una red IP que impone ciertas reglas, definidas por el usuario o por un proveedor de servicios, a la hora de asignar ancho de banda para determinados servicios con el objetivo de garantizar cierta calidad de servicio (QoS, Quality of Service) en la red.

**POP** **P**oint **o**f **P**resence

Punto de presencia en la red telefónica.

**PPP** **P**oint-to-**P**oint **P**rotocol

Protocolo punto a punto. Es el estándar utilizado en comunicaciones serie en Internet. Más moderno y mejor que SLIP, PPP define cómo intercambian paquetes de datos los modems con otros sistemas en Internet.

**PSTN** **P**ublic **S**witched **T**elephone **N**etwork

Red telefónica convencional.

**Router** Un dispositivo físico, o a veces un programa corriendo en un ordenador, que reenvía paquetes de datos de una red LAN o WAN a otra. Basados en tablas o protocolos de enrutamiento, leen la dirección de red destino de cada paquete que les llega y deciden enviarlo por la ruta más adecuada (en base a la carga de tráfico, coste, velocidad u otros factores).

**RTP** **R**outing **T**able **P**rotocol

Protocolo telefónico que hace uso de una lista de instrucciones o tabla que le indica cómo manejar llamadas

telefónicas entrantes.

**RTP** **R**eal-**T**ime **T**ransport **P**rotocol

El protocolo estándar en Internet para el transporte de datos en tiempo real, incluyendo audio y vídeo. Se utiliza prácticamente en todas las arquitecturas que hacen uso de VOIP, videoconferencia, multimedia bajo demanda y otras aplicaciones similares. Se trata de un protocolo *ligero* que soporta identificación del contenido, reconstrucción temporal de los datos enviados y también detecta la pérdida de paquetes de datos.

**SBus** Originalmente era un bus propietario de Sun, que fue liberado como de dominio público. El IEEE estandarizó una versión de 64 bits en 1993.

**SCCP** **S**ignaling **C**onnection **C**ontrol **P**art

SCCP proporciona servicios de red, tanto orientados a conexión como no orientados a conexión, sobre el nivel 3 de MTP.

**SCSA** **S**ignal **C**omputing **S**ystem **A**rchitecture

Una arquitectura abierta pensada para transmitir señales de voz y vídeo desarrollada por Dialogic. Soporta transferencia de datos a 131 Mbps y proporciona hasta 2.048 time slots, el equivalente a 1.024 conversaciones bidireccionales simultaneas a 64 Kbps.

**SCSI** **S**mall **C**omputer **S**ystem **I**nterface

Es un interfaz hardware que permite la conexión de hasta 7 ó 15 periféricos a una tarjeta que se conecta al PC o Workstation y se suele llamar "SCSI host adapter" o "SCSI controller". Los periféricos SCSI se conectan encadenados, todos ellos tienen un segundo puerto que se utiliza para conectar el siguiente periférico en línea. También hay tarjetas SCSI que disponen de dos controladores y soportan hasta 30 periféricos.

**SCTP** **S**imple **C**ontrol **T**ransmission **P**rotocol

SCTP es un protocolo de transporte fiable, diseñado para trabajar sobre redes de paquetes no orientadas a conexión,

como IP.

**SDH** **S**ynchronous **D**igital **H**ierarchy

Jerarquía Digital Síncrona. Una norma para la transmisión digital de señales en redes de transporte. SDH es la versión europea de SONET.

**SDP** **S**ession **D**escription **P**rotocol

SDP lo utiliza SIP para describir las capacidades multimedia de los participantes en la llamada y negociar un conjunto común de capacidades multimedia a utilizar.

**SDSL** **S**ymmetrical **D**igital **S**ubscriber **L**ine

Una línea DSL en la que la velocidad de bajada y subida es la misma. Se utiliza casi exclusivamente en entornos empresariales, ya que los clientes residenciales normalmente necesitan una velocidad de bajada mayor que de subida.

**SGCP** **S**imple **G**ateway **C**ontrol **P**rotocol

SGCP es un protocolo utilizado con SGCI para controlar Gateways VOIP desde elementos de control de llamada externos.

**SIP** **S**ession **I**nitiation **P**rotocol

SIP es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet.

Un estándar de la IETF (Internet Engineering Task Force) definido en la RFC 2543. SIP se utiliza para iniciar, manejar y terminar sesiones interactivas entre uno o más usuarios en Internet. Inspirado en los protocolos HTTP (web) y SMTP (email), proporciona escalabilidad, flexibilidad y facilita la creación de nuevos servicios.

**SLIP** **S**erial **L**ine **IP**

Uno de los primeros estándares desarrollados para conectar un ordenador a Internet utilizando un modem conectado a una línea telefónica. Ha sido superado por CSLIP y PPP.

**Softswitch** Término genérico para cualquier software pensado para actuar de pasarela entre la red telefónica y algún protocolo de VOIP, separando las funciones de control de una llamada del media gateway.

**Software PBX** **Software P**rivate **B**ranch e**X**change

Sistema telefónico que hace converger voz y datos en una plataforma estándar haciendo uso de componentes relacionados con la Telefonía IP. Al estar basado en estándares se asegura la interoperabilidad entre componentes de distintos fabricantes.

**SS7** Common Channel **S**ignaling **S**ystem Nº **7**

SS7 es un estándar global para telecomunicaciones definido por la Unión Internacional de Telecomunicaciones (Sector de Estandarización de Telecomunicaciones). Define los procedimientos y protocolos mediante los cuales los elementos de la Red Telefónica Conmutada (RTC o PSTN, Public Switched Telephone Network) intercambian información sobre una red de señalización digital para establecer, enrutar, facturar y controlar llamadas, tanto a

terminales fijos como móviles.

**T1** Un circuito digital punto a punto dedicado a 1,544 Mbps proporcionado por las compañías telefónicas en Norteamérica. Ver E1 y J1 para los equivalentes europeos y japonés, respectivamente. Permite la transmisión de voz y datos y en muchos casos se utilizan para proporcionar conexiones a Internet.

T1 (DS1): 24 canales, 1,544 Mbps
T2 (DS2): 96 canalels, 6,312 Mbps
T3 (DS3): 672 canales, 44,736 Mbps
T4 (DS4): 4032 canales, 274,176 Mbps

**TACS** **T**otal **A**ccess **C**ommunication **S**ystem

Una norma de teléfonos móviles, originalmente utilizada en Gran Bretaña. Utiliza la banda de frecuencia de 900 MHz.

**TAPI** **T**elephony **A**pplication **P**rogramming **I**nterface

Permite a los programadores escribir aplicaciones para PC

que hagan uso de servicios proporcionados por los fabricantes de telefonía. Estas aplicaciones pueden controlar desde un simple teléfono hasta una centralita. Ejemplos de sus posibilidades son la marcación automática, detección del número llamante incluyendo conexión con la agenda personal, marcación desde la agenda, contestador telefónico e incluso sistemas con reconocimiento vocal integrado.

**TASP** **T**elephony **A**pplication **S**ervice **P**rovider

Proveedor de aplicaciones de telefonía que facilita la tecnología, la infraestructura y los servicios de telefonía de nueva generación a empresas a través de redes privadas virtuales (VPNs, virtual private networks). Los usuarios de estos servicios tienen así acceso a plataformas basadas en estándares abiertos y utilizando XML y VoiceXML pueden hacer uso de las aplicaciones telefónicas y servicios disponibles e integrarlos en su red.

**TCAP** **T**ransaction **C**apability **A**pplication **P**art

Los mensajes TCAP se utilizan para intercambiar información, no orientada a conexión, no relacionada

directamente con la red telefónica. Por ejemplo, se utilizan para enviar peticiones a bases de datos y recibir los resultados.

**TCP** **T**ransmission **C**ontrol **P**rotocol

Protocolo de comunicación que permite comunicarse a los ordenadores a través de Internet. Asegura que un mensaje es enviado completo y de forma fiable. Se trata de un protocolo orientado a conexión.

**TDMA** **T**ime **D**ivision **M**ultiple **A**ccess

Tecnología para la transmisión digital de señales de radio; por ejemplo, entre un teléfono móvil y una estación radiobase. En TDMA, la banda de frecuencia se divide en un número de canales que a la vez se agrupa en unidades de tiempo de modo que varias llamadas pueden compartir un canal único sin interferir una con otra.

**UMTS** **U**niversal **M**obile **T**elecommunications **S**ystem

Nombre de la normativa para la tercera generación de

telefonía móvil en Europa, fue estandarizada por ETSI.

**URL** **U**niform **R**esource **L**ocator

Es el formato fijo utilizado para especificar y obtener documentos y otros recursos disponibles en Internet. Por ejemplo, una URL puede ser: http://www.sitio.com. Si la desglosamos vemos que consta del protocolo http (hyper-text transfer protocol), www (world-wide web), sitio (nombre del dominio), com (company). Las URLs también se utilizan para indicar otros protocolos, como ftp, news, WAIS.

**VAT** Herramienta de teleconferencia audio del entorno UNIX que permite hablar con varias personas simultáneamente utilizando Internet. Todo lo que necesitas es el programa VAT, una conexión IP y una tarjeta de sonido full-duplex.

En el entorno Windows el programa más popular para telefonía IP es NetMeeting, de Microsoft.

**VME** **V**ersa **M**odule **E**urocard bus

VME es un bus de 32 bit bus desarrollado por Motorola,

Signetics, Mostek y Thompson CSF. Muy utilizado en aplicaciones industriales, comerciales y militares. Existen más de 300 fabricantes de productos para bus VME en todo el mundo. VME64 es una versión mejorada que soporta transferencias y direccionamiento de datos de 64-bit.

**VoATM** **V**oice **O**ver **ATM**

La voz sobre ATM permite a un enrutador transportar el tráfico de voz (por ejemplo llamadas telefónicas y fax) sobre una red ATM. Cuando se envía el tráfico de voz sobre ATM éste es encapsulado utilizando un método especial para voz multiplexada AAL5.

**VoFR** **V**oice **O**ver **F**rame **R**elay

Permite a un enrutador transportar el tráfico de voz (por ejemplo llamadas telefónicas y fax) sobre una red de Frame Relay. Cuando se envía el tráfico de voz sobre Frame Relay el tráfico de voz es segmentado y encapsulado para su tránsito a través de la red Frame Relay utilizando FRF.12 como método de encapsulamiento.

**VoHDLC** **V**oice **O**ver **HDLC**

Permite a un enrutador transportar tráfico de voz en vivo (por ejemplo llamadas telefónicas y fax) hacia un segundo enrutador sobre una línea serie.

**Voice Portal** Portal de voz.

Servicios que ofrecen acceso a información diversa normalmente utilizando números gratuitos (900 ó 800) desde cualquier teléfono. Se facilita información de interés general, como noticias, el tiempo, cotizaciones de bolsa, deportes, tráfico, etc.

**Voice Web** Sitio web accesible a través del teléfono. Desde cualquier teléfono, y utilizando la voz es posible acceder a contenidos en Internet y realizar transacciones comerciales.

**VoiceXML** Un nuevo estándar que permite el acceso al contenido web a través del teléfono. VoiceXML utiliza XML para representar el flujo de la llamada y del diálogo, y permite tanto el acceso,

la navegación y la recuperación de contenidos de sitios web que cumplan este estándar utilizando cualquier teléfono, incluyendo los móviles.

**VoIP** **V**oice **O**ver **IP** (Voz sobre IP)

Tecnología que permite la transmisión de la voz a través de redes IP, Internet normalmente. La Telefonía IP es una aplicación inmediata de esta tecnología.

**WAN** **W**ide **A**rea **N**etwork

Una red de comunicaciones utilizada para conectar ordenadores y otros dispositivos a gran escala. Las conexiones pueden ser privadas o públicas.

**WAP** **W**ireless **A**pplication **P**rotocol

Un protocolo gratuito y abierto, sin licencia, para comunicaciones inalámbricas que hace posible crear servicios avanzados de telecomunicación y acceder a páginas de Internet desde dispositivos WAP. Ha tenido gran

aceptación por parte de la industria.

**WAV** Formato Windows, y también la extensión de los ficheros, para ficheros de audio.

**WCDMA** **W**ideband **C**ode-**D**ivision **M**ultiple **A**ccess

Una tecnología para radiocomunicaciones digitales de banda ancha para Internet, multimedia, amplitud y otras aplicaciones que demandan capacidad. WCDMA fue desarrollado por Ericsson y otros. Ha sido seleccionado para la tercera generación de sistemas de telefonía móvil en Europa, Japón y Estados Unidos.

**WDM** **W**avelength **D**ivision **M**ultiplexing

Tecnología que usa señales ópticas en diferentes longitudes de onda para aumentar la capacidad de redes de fibra óptica, a fin de manejar ciertos grados de servicios simultáneamente.

**Wire speed** El ancho de banda de un sistema concreto de interconexión o transmisión. Por ejemplo, para una Ethernet 10BaseT es de 10 Mbps. Cuando se dice que los datos van a "wire speed" o "wire rate", se está queriendo indicar que hay poco o ninguna sobrecarga software asociada con la transmisión, por lo que los datos viajan a la máxima velocidad que permite el hardware.

**WLAN** **W**ireless **LAN**

Versión inalámbrica del LAN. Provee el acceso al LAN incluso cuando el usuario no está en la oficina.

**X.25** X.25 es una recomendación del CCITT para el interfaz entre un DTE y un DCE sobre la Red Telefónica Conmutada (RTC o PSTN, Public Switched Telephone Network). Generalmente, X.25 cubre las capas 1 a 3 del modelo de comunicaciones ISO, aunque muchas veces se utiliza este término para referirse específicamente a la capa de paquetes 3. X.25 se transporta dentro del campo *Información* de las tramas LAPB.

**XML** e**X**tensible **M**arkup **L**anguage

Sistema de codificación que permite intercambiar cualquier tipo de información a través de Internet de forma estructurada. Se trata de un metalenguaje y, por tanto, contiene reglas que permiten la construcción de otros lenguajes y la creación de elementos que expanden el tipo y la cantidad de información que se puede distribuir en los documentos que sigan este estándar.

**XModem** Un protocolo asíncrono de dominio público para transferencia de ficheros para ordenadores que facilita la transferencia sin errores de ficheros a través de líneas telefónicas. Desarrollado por Ward Christiansen para ordenadores de 8 bit sobre CP/M (Control Program for Microprocessors). Actualmente está soportado por la mayoría de los programas de comunicaciones para ordenadores.

**YModem** Una versión mejorada del protocolo XMODEM-1K. YMODEM transfiere datos en bloques de 1.024 bytes e incluye CRC (Cyclic Redundancy Check, Chequeo de Redundancia Cíclica)

en cada trama. También soporta el envío de más de un fichero en secuencia. Ver XMODEM y ZMODEM.

**ZModem** Evolución de los dos anteriores, se trata de un protocolo muy rápido que permite utilizar caracteres comodín a la hora de indicar los ficheros a transferir. También es capaz de reanudar transferencias de ficheros interrumpidas. Es el protocolo de comunicaciones más extendido y se incluye en la mayoría de los programas de comunicaciones actuales.

# RESUMEN

El desarrollo de las telecomunicaciones y en particular de Internet ha hecho que tecnologías como la telefonía IP (Internet Protocol) comiencen a ser una realidad tanto en el mundo de los negocios como del ocio. Originalmente la voz y los datos se han transmitido a través de sistemas completamente separados. Sin embargo, hoy en día es posible realizar las comunicaciones de voz en las redes internas de las organizaciones utilizando el protocolo IP de Internet, de forma que, al menos en nuevos edificios, ya no existe la necesidad de instalar una red telefónica. En las comunicaciones que se realizan actualmente en las oficinas, el acceso a las redes de datos es tan importante como las comunicaciones telefónicas. En ambos casos, la información se transmite como señales digitales. Sin embargo, voz y datos son transportados sobre sistemas completamente separados, una vestigio de los tiempos en que la telefonía se basaba en la transmisión de señales analógicas y los ordenadores se encontraban en su etapa inicial de desarrollo.

Este TUTORIAL presenta VOIP (VOICE OVER INTERNET PROTOCOL) como una posible solución a este problema. Desarrolla también una primera aproximación al concepto y la terminología de la convergencia de redes, para a continuación establecer una comparativa entre la Telefonía IP y la Telefonía convencional. Se aportan además detallados análisis de los requerimientos de

la Telefonía IP, de su situación en el ámbito legal y de los distintos estándares que se utilizan en su desarrollo.

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**

Es un estándar que especifica los componentes, los protocolos y los procedimientos que proporcionan redes del paquete del excedente de los servicios de la comunicación de los multimedia (audio, vídeo, y comunicaciones de datos en tiempo real), incluyendo redes basadas del Internet Protocol (IP). H.323 es parte de una familia de las recomendaciones de Itu-t llamadas H.32x que proporcione servicios de la comunicación de los multimedia sobre una variedad de redes.

**SIP (Protocolo de inicio de sesión)**

Un protocolo de señalización de capa de aplicación que define la iniciación, modificación y la terminación de sesiones interactivos de comunicación multimedia entre usuarios.

# INTRODUCCIÓN

La red telefónica de nuestros días, no ha cambiado desde los años ochenta, durante todo este tiempo la tecnología de voz día a día ha tomado fuerza hasta el punto donde el principio de las comunicaciones humanas esta basada en las comunicaciones telefónicas y la transmisión no se pudo quedar atrás en tomar partida hablando de Internet, el ciberespacio y las comunicaciones seguras hoy por hoy la transmisión de voz sobre medios IP es y será dentro de poco el método mas utilizado para llegar hasta los rincones mas escondidos del planeta con la fidelidad de los métodos tradicionales de hoy. los avances en redes de datos han sido muy importantes, tanto en fiabilidad, capacidad como en costos. Todos estos adelantos se pueden empezar a aplicar a nuestras comunicaciones de voz gracias a los últimos desarrollos presentados sobre la tecnología Voz IP.

Como marco para este avance se ha formalizado un estándar que ha permitido aclarar como será el desarrollo de todas las comunicaciones, con la suficiente amplitud como para abarcar todas las posibilidades existentes.

El crecimiento y fuerte implantación de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (gataways), denominadas genéricamente pasarelas VoIP.

La convergencia de las redes de telecomunicaciones actuales supone encontrar la tecnología que permita hacer convivir en la misma línea la voz y los datos. Esto obliga a establecer un modelo o sistema que permita "empaquetar" la voz para que pueda ser transmitida junto con los datos. Teniendo en cuenta que Internet es la "red de redes", desarrollar una tecnología de ámbito mundial nos dirige claramente al protocolo IP (Internet Protocol) y a encontrar el método que nos permita transmitir voz a la vez que datos sobre ese protocolo. El problema tiene una "sencilla" solución: VoIP (Voice Over Internet Protocol).

Algo tan sencillo en principio no lo es en la realidad y para comprobarlo sólo hay que repasar la evolución de los distintos desarrollos comerciales, de los

distintos estándares y las distintas nomenclaturas y acrónimos que utilizan todos los expertos en la materia .
Aunque son conocidas distintas investigaciones en algoritmos avanzados de digitalización de voz desde 1970 (Mañas J.A., VoIP'99, 1999) y distintas experiencias de transmisión de voz sobre redes locales (LAN) en los años 80 (Mañas J.A., VoIP'99, 1999), es en Febrero de 1995 cuando la empresa VocalTec (Canto J., 1999) da el pistoletazo de salida mostrando a través de su producto Internet Phone las posibilidades reales de establecimiento de llamadas telefónicas de Pc a Pc. Se utilizaba entonces un paquete de software instalado en el Pc y como medio de transmisión Internet. Nacía así el término hoy conocido como Telefonía IP.

La evolución en el tiempo ya era imparable y es en 1996 cuando se dan las primeras experiencias de establecimiento de llamadas de Teléfono a Pc (Mañas J.A., VoIP'99, 1999) y de Teléfono a Teléfono. A partir de 1997 empiezan a aparecer nuevos dispositivos y métodos que nos llevan hoy en día a mantener el término XoIP ('X' over Internet Protocol) (Sierra J.C., VoIP'99, 1999) como la verdadera opción de futuro o si se prefiere como la puerta hacia la convergencia de las redes. En este acrónimo X significa cualquier contenido susceptible de ser transmitido por una red (D = data, V = voz, F = fax, M = multimedia).

Este laberinto de tecnologías, de intereses comerciales y de opciones de futuro lleva como toda "revolución" a la confusión y desgaste del público en general. La consecuencia inmediata son las habituales FAQs (Frequently Asked Questions): ¿por qué IP?, diferencia entre Telefonía IP y Voz sobre IP, ¿es VoIP lo mismo que VOFR (Voz sobre Frame Relay )?, ¿qué significa realmente XOIP?, etc.

Es preciso, por tanto, definir de una forma simple y clara la situación actual para que a partir de este momento se puedan identificar claramente tanto los términos como los elementos que de alguna u otra forma intervienen en los distintos niveles del desarrollo de la convergencia de redes. Términos que posiblemente identifican el camino hacia los servicios de VoIP:
· Telefonía: servicios de telecomunicación prestados sobre la Red Telefónica Conmutada (RTC) ya sea Red Telefónica Básica (RTB) o Red Digital de Servicios Integrados (RDSI), a excepción de comunicación de datos.

- **Voz en Internet**: servicios de telefonía prestados sobre la red pública global formada por la interconexión de redes de conmutación de paquetes basadas en IP.

- **Voz sobre IP** (VoIP): servicios de telefonía prestados sobre redes IP "privadas" sin interconexión a la RTC .

- **Telefonía IP**: servicios de telefonía prestados sobre Redes IP "privadas" en interconexión con la RTC.

- **Voz sobre Frame Relay (VOFR):** servicios de telefonía prestados sobre redes soportadas por circuitos Frame Relay, orientados a la transmisión de datos.

- **Voz sobre ATM (Asyncronus Transfer Mode) (VoATM):** servicios de telefonía prestados sobre redes ATM donde existe posibilidad de ofrecer una calidad de servicio (Qos).

- **Multimedia sobre IP (MoIP)**: servicios multimedia (vídeo, audio, imagen, etc) prestados sobre redes IP

- **Fax sobre IP (FoIP):** servicios de transmisión de fax prestados sobre redes IP.

- **XOIP:** en términos globales "todo sobre IP". Se trata de sustituir X por aquella letra que identifique cualquier servicio sobre redes IP (F = fax, M = multimedia, V = voz, D = data, etc).

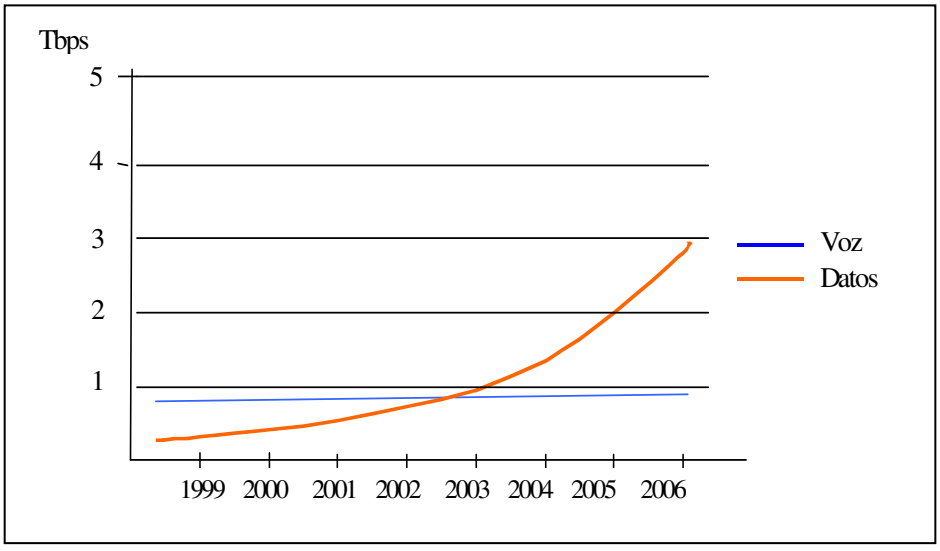



**Figura1.** Crecimiento del Tráfico Voz –Datos

Como conclusión se puede deducir que si el futuro es IP (debido sobre todo a su ámbito de cobertura actual, su aceptación por parte del usuario y la próxima aparición del protocolo IPv6) y que si X es la integración global de todos los servicios actuales y de futuro, XOIP es el verdadero camino que puede abrir las puertas hacia la Convergencia de Redes. Esta Convergencia supone la

unificación sobre una misma estructura de la transmisión de voz y datos. La convergencia supondrá en términos económicos una auténtica "revolución" que afectará desde el entorno empresarial hasta el entorno doméstico. la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema "caliente" y estratégico para las empresas. Hoy, la telefonía sobre IP empieza a ver su hora más gloriosa y es el fruto más legítimo de la convergencia tecnológica.

El concepto original es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red IP (con protocolo Internet, materia que también incluye a las intranets y extranets). Gracias a otros protocolos de comunicación, como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación. La voz puede ser obtenida desde un teléfono común: existen gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Vale decir, se pueden mantener conversaciones teléfono a teléfono.

# 1. REDES CONVERGENTES

Una red convergente no es únicamente una red capaz de transmitir datos y voz sino un entorno en el que además existen servicios avanzados que integran estas capacidades, reforzando la utilidad de los mismos.

A través de la convergencia, una compañía puede reinventar tanto sus redes de comunicaciones como toda su organización. Una red convergente apoya aplicaciones vitales para estructurar el negocio -Telefonía IP, videoconferencia en colaboración y Administración de Relaciones con el Cliente (CRM) que contribuyen a que la empresa sea más eficiente, efectiva y ágil con sus clientes.

## 1.2 ANTECEDENTES

La implementación exitosa de redes convergentes aún se enfrenta a retos, que se manifiestan más claramente cuando estas redes intentan competir con la tradicional red de telefonía basadas en PBXs.

La juventud de las redes convergentes hace que sea difícil aún alcanzar los niveles de disponibilidad y escalabilidad de otras redes pero se trata de campos

en los que dichas redes convergentes están experimentando sustanciales mejoras.

La unión de los nuevos servicios y los avances mencionados están haciendo que estas redes de nueva generación se presenten hoy como la base para el desarrollo de nuevos modelos de negocio tanto en entornos fijos como en móviles.

Ante el desarrollo de las redes de datos durante la década de los 90, se ha planteado la posibilidad de utilizarlas para el envío de información multimedia, como imágenes, voz o incluso música. Estas redes, basadas en el protocolo IP, han conseguido introducirse en el mundo de los negocios.

## 1.3 IMPACTO EN LOS NEGOCIOS

Las empresas descubren que los beneficios de la convergencia afectan directamente los ingresos netos:

Las soluciones convergentes nos hacen más productivos, pues simplifican el usar aplicaciones y compartir información.

Tener una red para la administración significa que el ancho de banda será usado lo más eficientemente posible, a la vez que permite otras eficiencias y ahorros de costos: en personal, mantenimiento, cargos de interconexión, activaciones, mudanzas y cambios.

Los costos más bajos de la red, productividad mejorada, mejor retención de clientes, menor tiempo para llegar al mercado-son los beneficios netos que posibilitan las soluciones de redes convergentes. Reducción de costos de personal para la administración de red y mantenimiento.

## 1.4 Seguridad

Las redes convergentes requieren una seguridad que amplíe las políticas y procesos tradicionales de protección de datos a proteger la privacidad de toda la red, incluyendo el tráfico de IP, debido a la posibilidad de introducir terminales no autorizados a través de la red IP. Las políticas tradicionales de protección de datos pueden influir negativamente en la calidad de la voz si no se diseñan correctamente. Por ello, una red convergente debe ser diseñada para cumplir los requisitos de seguridad para voz y datos, al tiempo que no impida el funcionamiento de aplicaciones críticas para la red.

Los servicios de seguridad empiezan con una Auditoria de Seguridad, para identificar posibles agujeros en la red que pueden ser víctima de intrusos. El Desarrollo de una Política de Seguridad define los procesos, responsabilidades, controles y medidas de seguridad necesarias para proteger los datos en un entorno de convergencia. Este Pre-diseño es clave para el Diseño & Arquitectura de Seguridad, que facilita a los expertos en la compleja tarea de diseño de una infraestructura de información segura en una red convergente. Arquitectura & Diseño aseguran que las medidas de seguridad definidas en una política de seguridad son diseñadas en una estructura segura, además ayuda a cumplir con los requisitos de seguridad corporativa, permitiendo un control de acceso a la red y ofreciendo un mantenimiento remoto seguro y proactivo de todo el entorno de la red. Con este servicio, dispondrá además de la información necesaria para cumplir con las leyes de seguridad, integridad de datos y privacidad. Servicios Gestionados de Seguridad ofrecen un soporte regulatorio adicional mediante el informe de sucesos proactivo y en tiempo real, informes de auditoria, análisis legales, detección de intrusos y respuesta a incidentes, lo que fortalece la seguridad de las redes monitorizadas.

## 2. VOIP

VOIP viene de Voice Over Internet Protocol. Como dice el termino VOIP intenta permitir que la voz viaje en paquetes IP y obviamente a través de Internet. La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información. La voz IP, por lo tanto, no es en sí mismo un servicio, sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales PSTN, las redes desarrolladas a lo largo de los años para transmitir las conversaciones vocales, se basaban en el concepto de conmutación de circuitos, o sea, la realización de una comunicación que requiere el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica. En cambio, la telefonía IP no utiliza circuitos para la conversación, sino que envía múltiples de ellas (conversaciones) a través del mismo canal codificadas en paquetes y flujos independientes. Cuando se produce un silencio en una

conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma. Según esto son evidentes las ventajas que proporciona el segundo tipo de red, ya que con la misma infraestructura podrían prestar mas servicios y además la calidad de servicio y la velocidad serian mayores; pero por otro lado también existe la gran desventaja de la seguridad, ya que no es posible determinar la duración del paquete dentro de la red hasta que este llegue a su destino y además existe la posibilidad de perdida de paquetes, ya que el protocolo IP no cuenta con esta herramienta.

## 2.1 Principio de funcionamiento

Años atrás se descubrió que mandar una señal a un destino remoto también podía hacerse también de manera digital: antes de enviar la señal se debía digitalizar con un ADC (analog to digital converter), transmitirla y en el extremo de destino transformarla de nuevo a formato análogo con un DAC (digital to analog converter).

VOIP funciona de esa manera, digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino.

Básicamente el proceso comienza con la señal análoga del teléfono que es digitalizada en señales PCM (pulse code modulación) por medio del codificador/decodificador de voz (codec). Las muestras PCM son pasadas al algoritmo de compresión, el cual comprime la voz y la fracciona en paquetes que pueden ser transmitidos para este caso a través de una red privada WAN. En el otro extremo de la nube se realizan exactamente las mismas funciones en un orden inverso. El flujo de un circuito de voz comprimido es el mostrado en la figura.

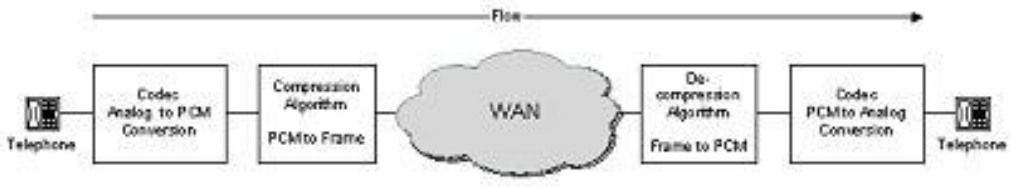



**Figura 2.** flujo de un circuito de voz comprimido

Dependiendo de la forma en la que la red este configurada, el enrutador o el gateway puede realizar la labor de codificación, decodificación y/o compresión. Por ejemplo, si el sistema usado es un sistema análogo de voz, entonces el enrutador o el gateway realizan todas las funciones mencionadas anteriormente de la siguiente manera.

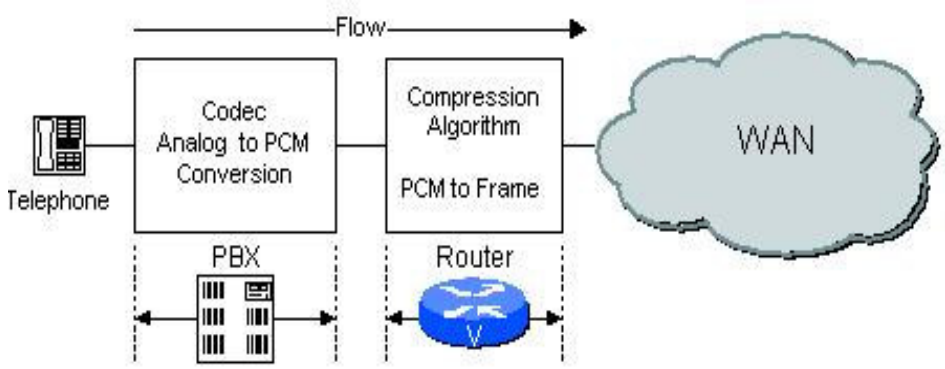



**Figura 3.** Procedimiento de codificación, decodificación

Si, por otro lado, el dispositivo utilizado es un PBX digital, es entonces este el que realiza la función de codificación y decodificación, y el enrutador solo se dedica a procesar las muestras PCM que le ha enviado el PBX**.**

Para el caso en el que el transporte de voz se realiza sobre la red pública Internet, se necesita una interfaz entre la red telefónica y la red IP, el cual se denomina gateway y es el encargado en el lado del emisor de convertir la señal analógica de voz en paquetes comprimidos IP para ser transportados a través de la red, del lado del receptor su labor es inversa, dado que descomprime los paquetes IP que recibe de la red de datos, y recompone el mensaje a su forma análoga original conduciéndolo de nuevo a la red telefónica convencional en el sector de la última milla para ser transportado al destinatario final y ser reproducido por el parlante del receptor.

Es importante tener en cuenta también que todas las redes deben tener de alguna forma las características de direccionamiento, enrutamiento y señalización. El direccionamiento es requerido para identificar el origen y destino de las llamadas, también es usado para asociar clases de servicio a cada una de las llamadas dependiendo de la prioridad. El enrutamiento por su parte encuentra el mejor camino a seguir por el paquete desde la fuente hasta el destino y transporta la información a través de la red de la manera más eficiente, la cual ha sido determinada por el diseñador. La señalización alerta las estaciones terminales y a los elementos de la red su estado y la responsabilidad inmediata que tienen al establecer una conexión.

# 3. INTRODUCCIÓN ESTÁNDARES DE VOIP

Realmente la integración de la voz y los datos en una misma red es una idea antigua, pues desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes WAN de datos de las empresas (típicamente conexiones punto a punto y frame-relay) para la transmisión del tráfico de voz. La falta de estándares, así como el largo plazo de amortización de este tipo de soluciones no ha permitido una amplia implantación de las mismas.

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.

Actualmente existen estándares que regulan este tipo de comunicaciones, estándares que provienen de organismos internacionales de estandarización como el ITU (International Telecommunication Union) que ha establecido unas normas para la interconexión de los distintos elementos que intervienen en una comunicación sobre Telefonía IP.

El estándar que regula este tipo de comunicaciones es el H.323 de la ITU (ITU Standards, 1998). Esta norma realmente es una serie de normas para la transmisión de datos multimedia (audio, vídeo y datos) sobre redes que no garantizan una calidad de servicio (redes IP).

Las funciones cubiertas por el H.323 son acerca del control de llamadas, uso de codificadores de voz y normas de otros organismos que especifican la transmisión en tiempo real de los paquetes de voz.

El protocolo H.323 ha sido adoptado prácticamente por todas las empresas líderes en este sector como Netscape, Microsoft, Intel, Vocaltec. La adopción de este estándar permite la interconexión de equipos y software de cualquier fabricante que lo haya adoptado.

Por tanto es lógico deducir que en la actualidad cualquier empresa que quiera trabajar en servicios de VOIP debe adoptar este estándar en todos sus desarrollos. De esta manera se garantizará una perfecta integración con plataformas hardware y software de distintos fabricantes cuyos productos sigan la misma norma.

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.

## 3.1 ESTANDAR H.323

Es un estándar que especifica los componentes, los protocolos y los procedimientos que proporcionan redes del paquete del excedente de los servicios de la comunicación de los multimedia (audio, vídeo, y comunicaciones de datos en tiempo real), incluyendo redes basadas del Internet Protocol (IP). H.323 es parte de una familia de las recomendaciones de Itu-t llamadas H.32x que proporcione servicios de la comunicación de los multimedia sobre una variedad de redes. H.323 Especifica los componentes, los protocolos, y los procedimientos que proporcionan redes paquete-basadas excedente de la comunicación de los multimedia (véase el cuadro 1). las redes Paquete-basadas incluyen el Internet Protocol (IP) basado (Internet incluyendo) o las redes local-area basadas del intercambio del paquete del Internet (IPX) (LANs), las redes de la empresa (ENs), las redes de área metropolitana (MAN), y las redes de área amplia (WANs). H.323 se puede aplicar en una variedad de mecanismos: audio solamente (telefonía del IP); audio y video (videotelephony); audio y datos; y audio, vídeo y datos. H.323 se puede

también aplicar a las comunicaciones de los de multiples puntos-multipoint-multimedia. H.323 proporciona servicios innumerables y, por lo tanto, se puede aplicar en una variedad amplia de áreas: consumidor, negocio, y usos de la hospitalidad.

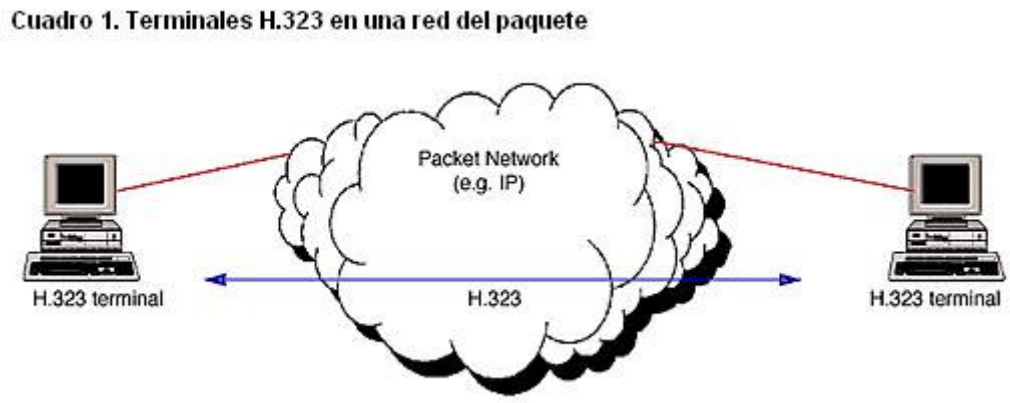



**Figura 4.** Terminales H.323 en una red de paquetes

## 4.1 PROTOCOLOS ESPECIFICADOS POR H.323

H.323 especifica cuatro pilas de protocolos básicamente, que son: Audio, Video, Control y Datos (ver figura 5). 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.

- H.245 Señalización de Control.

- RTP (Protocolo de Transferencia en Tiempo Real).

- RTCP (Protocolo de Control en Tiempo Real)

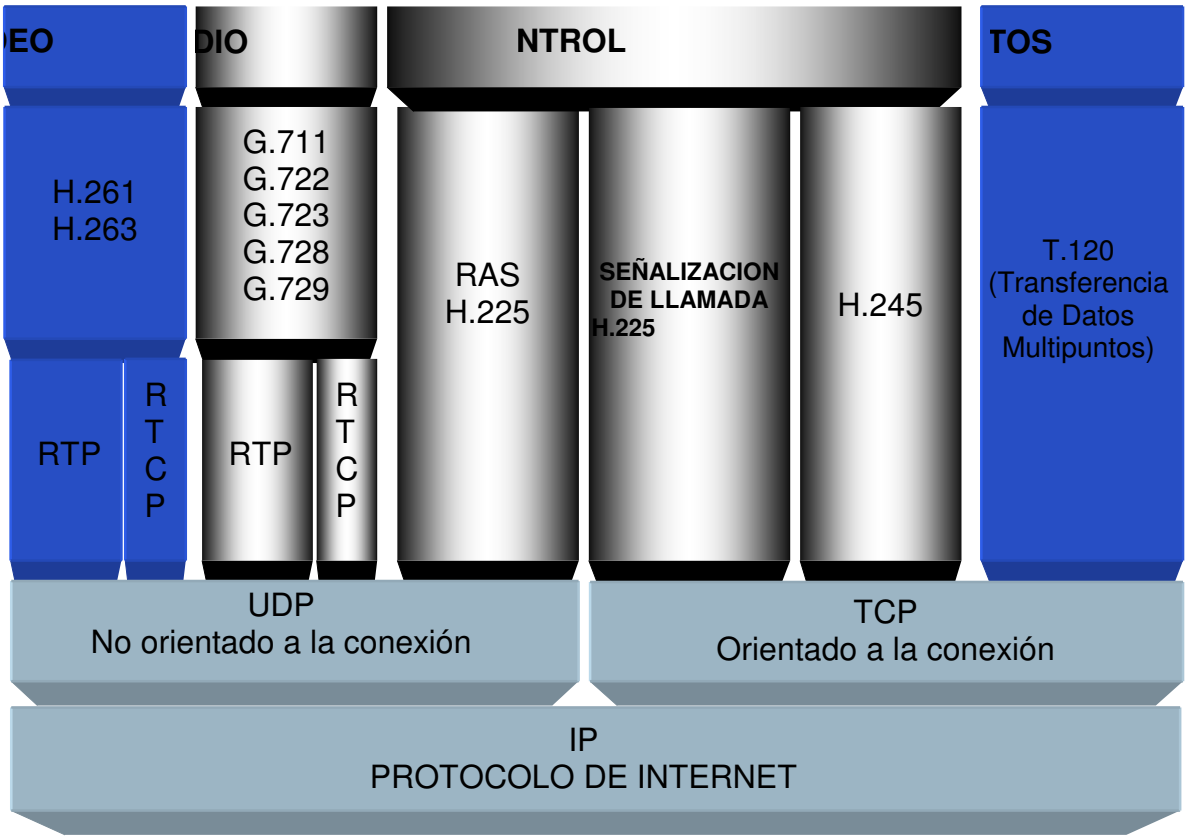



**Figura 5.** Protocolos H.323

### 4.1.1 *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.

### 4.1.2 *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:

#### 4.1.2.1 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.

#### 4.1.2.2 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.).

#### 4.1.2.3 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.

#### 4.1.2.4 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.

#### 4.1.2.5 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.

### 4.1.3 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.

#### 4.1.3.1 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 6.

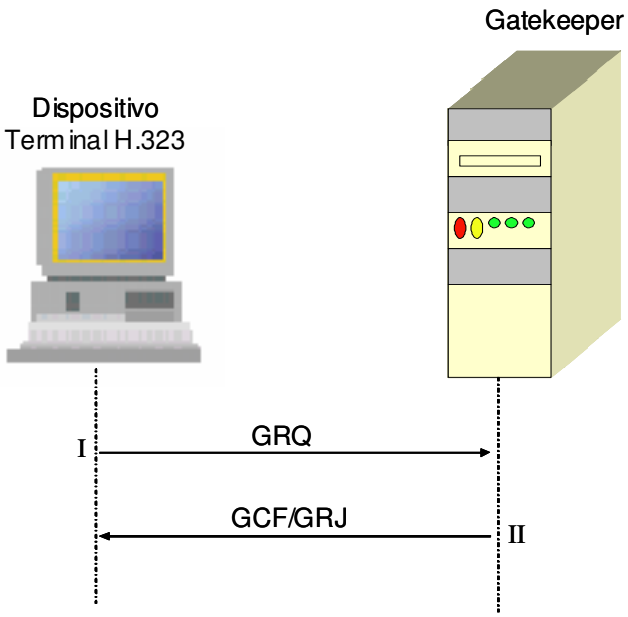



**Figura 6.** Detección Dinámica del *Gatekeeper*

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.

#### 4.1.3.2 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*.

### 4.1.4 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 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

El H.225 RAS se utiliza entre las puntos finales H.323 (los terminales y las entradas) y los porteros para el siguiente:

- descubrimiento del portero (GRQ)
- registro de la punto final
- localización de la punto final
- control de la admisión
- tenga acceso al símbolo

Los mensajes de RAS se continúan un canal de RAS que sea no fiable. Por lo tanto, el intercambio del mensaje de RAS se puede asociar a descansos y a cuentas de la recomprobación.

#### 4.1.4.1 DESCUBRIMIENTO DEL PORTERO

El proceso del descubrimiento del portero es utilizado por las puntos finales H.323 para determinar al portero con quien la punto final debe colocarse. El descubrimiento del portero se puede hacer estáticamente o dinámicamente. En descubrimiento estático, la punto final sabe la dirección de transporte de su portero a priori. En el método dinámico de descubrimiento del portero, los multicasts de la punto final un mensaje de GRQ en la dirección del multicast del descubrimiento del portero: "quién es mi portero?" Unos o más porteros pueden responder con un mensaje de GCF: "puedo ser su portero."

#### 4.1.4.2 REGISTRO DE LA PUNTO FINAL

El registro es un proceso usado por las puntos finales para ensamblar una zona y para informar al portero el transporte y alias las direcciones de la zona. Todas las puntos finales se colocan con un portero como parte de su configuración.

#### 4.1.4.3 LOCALIZACIÓN DE LA PUNTO FINAL

La localización de la punto final es un proceso por el cual la dirección de transporte de una punto final es determinada y dada su dirección nombre del alias o E.164.

#### 4.1.4.4 EL OTRO CONTROL

El canal de RAS se utiliza para otras clases de mecanismos del control, tales como control de la admisión, para restringir la entrada de una punto final en una zona, control de la anchura de banda, y el control de la retirada, donde está una punto final disassociated de un portero y de su zona.

#### 4.1.4.5 EL SEÑALAR DE LLAMADA H.225

El señalar de llamada H.225 se utiliza para instalar conexiones entre las puntos finales H.323 (los terminales y las entradas), sobre las cuales los datos en tiempo real pueden ser transportados. El señalar de llamada implica el intercambio de los mensajes de gestión de protocolo H.225 sobre un canal llamar-que señala confiable. Por ejemplo, los mensajes de gestión de protocolo H.225 son TCP transportados en una red IP-basada H.323.

Los mensajes H.225 se intercambian entre las puntos finales si no hay portero en la red H.323. Cuando un portero existe en la red, los mensajes H.225 se intercambian directamente entre las puntos finales o entre las puntos finales después de ser encaminado a través del portero. El primer caso es el señalar de llamada directa. Se llama el segundo caso el señalar de llamada portero-encaminado. El método elegido es decidido por el portero durante intercambio del mensaje de la RAS-admisio'n.

#### 4.1.4.6 EL SEÑALAR DE LLAMADA PORTERO-ENCAMINADO

Los mensajes de la admisión se intercambian entre las puntos finales y el portero en los canales de RAS. El portero recibe los mensajes llamar-que

señalan en el canal llamar-que señala a partir de una punto final y los encamina a la otra punto final en el canal llamar-que señala de la otra punto final.

#### 4.1.4.7 EL SEÑALAR DE LLAMADA DIRECTA

Durante la confirmación de la admisión, el portero indica que las puntos finales pueden intercambiar llamar-señalar mensajes directamente. Las puntos finales intercambian señalar de llamada en el canal llamar-que señala.

#### 4.1.4.8 INTERCAMBIO DE LAS CAPACIDADES

Las capacidades intercambian son un proceso usando los mensajes del intercambio de los terminales el comunicarse para proporcionar su transmiten y reciben capacidades a la punto final del par. Transmita las capacidades describen la capacidad del terminal de transmitir corrientes de los medios. Reciba las capacidades describen la capacidad de un terminal de recibir y de procesar corrientes entrantes de los medios.

#### 4.1.4.9 EL SEÑALAR DEL CANAL LÓGICO

Un canal lógico lleva la información a partir de una punto final a otra punto final (en el caso de un punto para señalar conferencia) o a las puntos finales

múltiples (en el caso de una conferencia punto-a-de múltiples puntos). H.245 proporciona mensajes para abrir o para cerrar un canal lógico; un canal lógico es unidireccional.

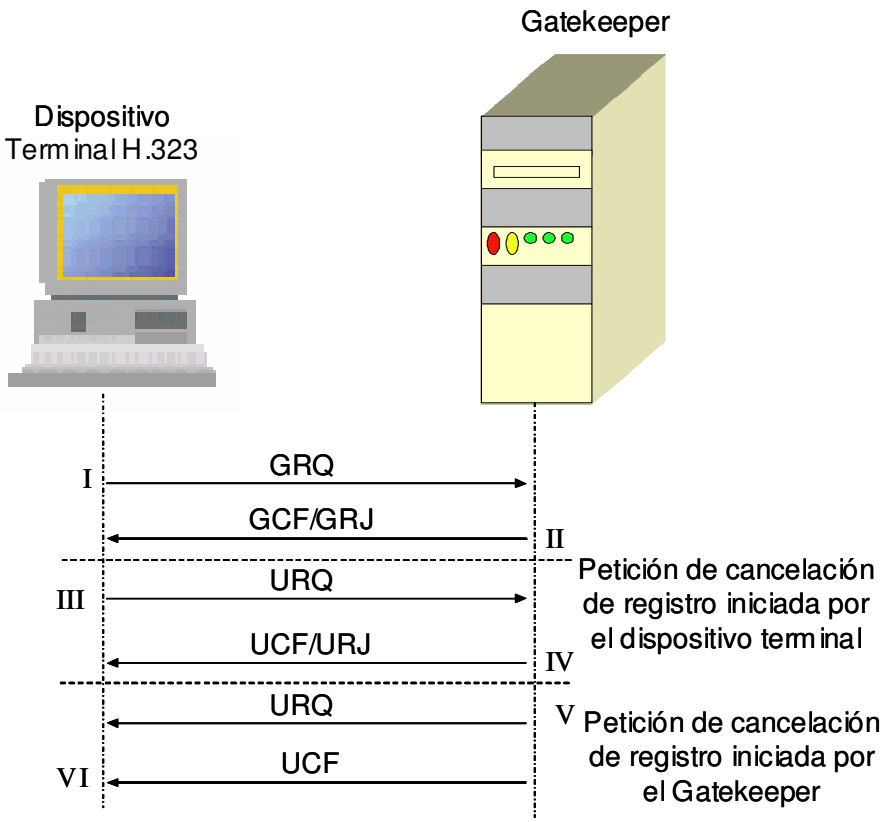



**Figura 7.** Procedimiento para Registro /Cancelación de Registro en el *Gatekeeper*

**4.1.5 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.

### 4.1.6 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.

## 4.2 VERSIONES H.323

El estándar H.323 es especificado por el grupo de estudio de UIT -T 16.

### 4.2.1 La versión 1

de la recomendación H.323 -- los sistemas y el equipo de teléfono visual para LANs que proporcionan la calidad del servicio (QOS) -- fue aceptada en octubre de 1996. Era, como el nombre sugiere, cargado pesadamente hacia comunicaciones de los multimedia en un ambiente del LAN. La versión 1 del estándar H.323 no proporciona QOS garantizado.

La aparición de los usos voz-sobre-IP (VOIP) y de la telefonía del IP ha pavimentado la manera para una revisión de la especificación H.323. La ausencia de un estándar para el IP excesivo de la voz dio lugar a los productos que eran incompatibles. Con el desarrollo de VOIP, los nuevos requisitos emergieron, por ejemplo el abastecimiento de la comunicación entre un teléfono PC-basado y un teléfono en una red cambiada tradicional del circuito (SCN). Tales requisitos forzaron la necesidad de un estándar para la telefonía del IP.

### 4.2.2 La versión 2

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:

#### 4.2.2.1 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.

#### 4.2.2.2 *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.

#### 4.2.2.3 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.

### 4.2.3 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:

#### 4.2.3.1 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.

#### 4.2.3.2 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.

#### 4.2.3.3 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*).

## 4.3 COMPONENTES BÁSICOS H.323

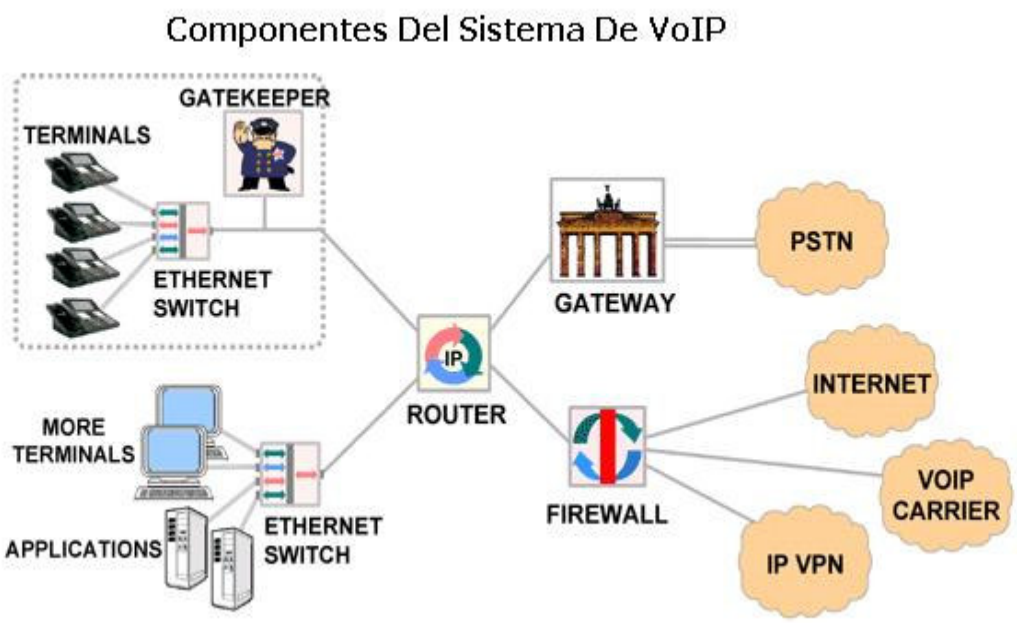



**Figura 8** Componentes del sistema VOIP

El estándar H.323 especifica cuatro clases de componentes, que, cuando es networked junto, proporcione el punto al punto y a los servicios punto-a-de múltiples puntos de la multimedia-comunicación:

- terminales.
- entradas.
- porteros .

- unidades de control de múltiples puntos (MCUs).

### 4.3.1 TERMINALES

Utilizado para las comunicaciones bidireccionales en tiempo real de los multimedia, un terminal H.323 puede ser un ordenador personal (PC) o un dispositivo independiente, funcionando un H.323 y los usos de los multimedia. Apoya comunicaciones audio y puede apoyar opcionalmente comunicaciones del vídeo o de datos. Porque el servicio básico proporcionado por un terminal H.323 es comunicaciones audio, un terminal H.323 desempeña un papel dominante en servicios de la telefonía del IP. Un terminal H.323 puede ser una PC o un dispositivo independiente, funcionando un apilado H.323 y usos de los multimedia. La meta fundamental de H.323 es intertrabajar con otros terminales de los multimedia. Los terminales H.323 son compatibles con los terminales H.324 en SCN y las redes, los terminales sin hilos H.310 en el B-b-isdn, los terminales H.320 en el ISDN, los terminales H.321 en el B-b-isdn, y los terminales H.322 en QoS garantizado LANs. Los terminales H.323 se pueden utilizar en conferencias de múltiples puntos.

**Figura 9.** teléfono IP

**4.3.1.1. 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).

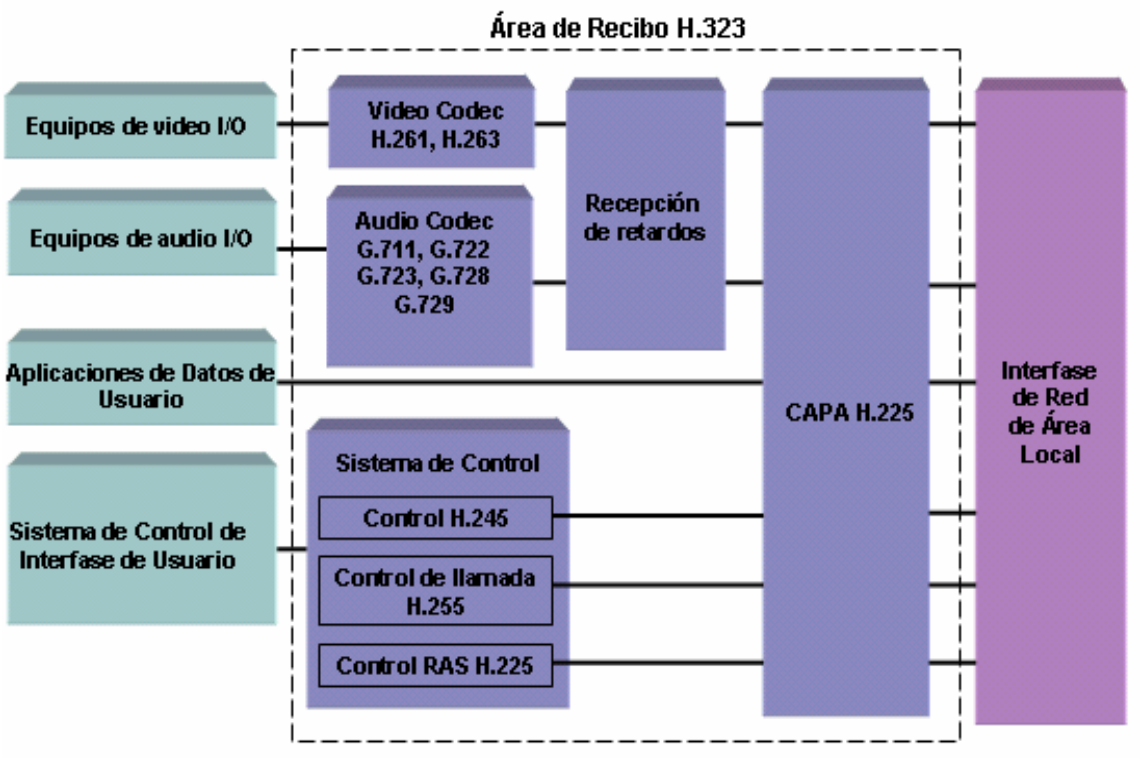



**Figura 10.** Arquitectura del Terminal H.323

### 4.3.2 **ENTRADAS**

Una entrada conecta dos redes disímiles. Una entrada H.323 proporciona conectividad entre una red H.323 y una red non-H.323. Por ejemplo, una entrada puede conectar y proporcionar la comunicación entre un terminal H.323 y las redes de SCN (las redes de SCN incluyen todas las redes cambiadas de la telefonía, e.g., la red de teléfono cambiada público [ PSTN ]). Esta conectividad de redes disímiles es alcanzada traduciendo los protocolos para la disposición y el lanzamiento de llamada, convirtiendo formatos de los medios

entre diversas redes, y transfiriendo la información entre las redes conectadas por la entrada. Una entrada no se requiere, sin embargo, para la comunicación entre dos terminales en una red H.323.

**Figura 11.** Arquitectura del Terminal H.323

#### 4.3.2.1 Características de las entradas.

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.

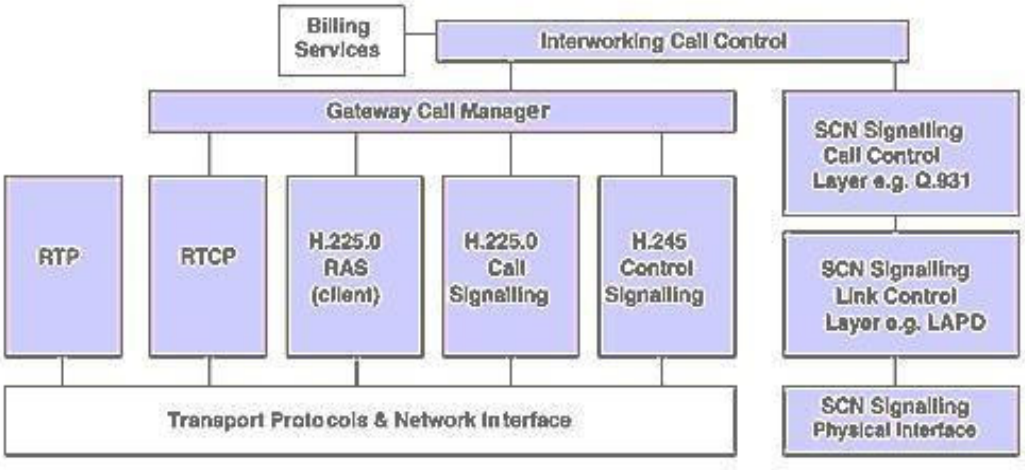



**Figura 12.** Gateway protocol stack

### 4.3.3 PORTEROS

Un portero puede ser considerado el cerebro de la red H.323. Es el punto focal para todas las llamadas dentro de la red H.323. Aunque no se requieren, los porteros proporcionan servicios importantes tales como dirección, autorización y autentificación de terminales y de entradas; gerencia de la anchura de banda; contabilidad; facturación; y carga. Los porteros pueden también proporcionar servicios de la llamar-encaminamiento.

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.

#### 4.3.3.1 CARACTERISTICAS 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*.

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.

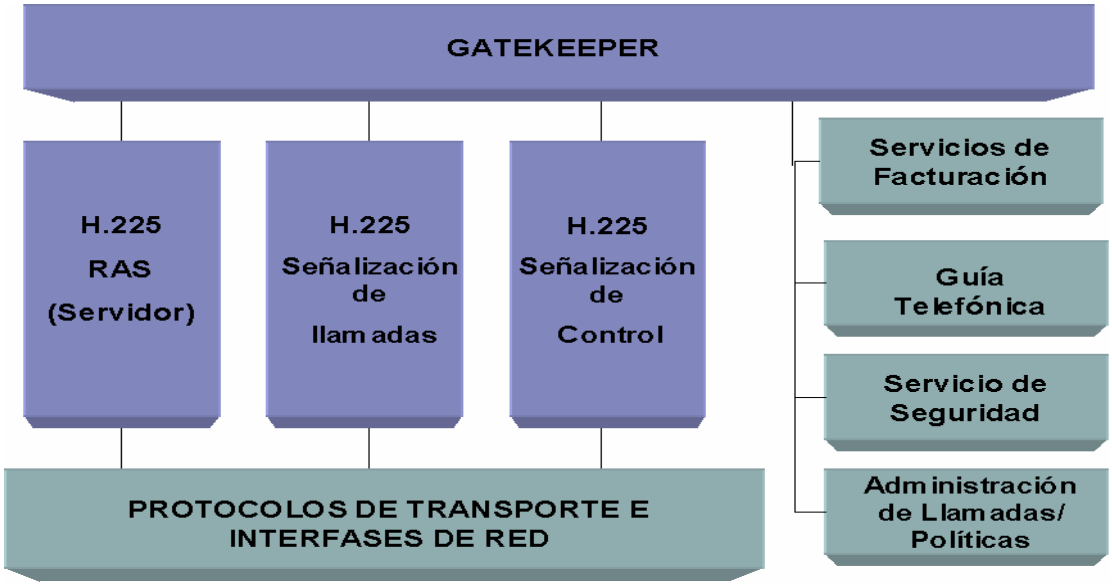



**Figura 13.** Componentes del *Gatekeeper*

#### 4.3.3.2 FUNCIONES OBLIGATORIAS DEL PORTERO

##### 4.3.3.2.1 CONVERSIÓN DE DIRECCIÓN

Las llamadas que originan dentro de una red H.323 pueden utilizar un alias para tratar el terminal de destinación. Las llamadas que originan fuera de la red H.323 y recibidas por una entrada pueden utilizar un número de teléfono E.164 (e.g., 310-442-9222) para tratar el terminal de destinación. El portero traduce

este número de teléfono E.164 o el alias a la dirección de red (e.g., 204.252.32:456 para una red IP-basada) para el terminal de destinación. La punto final de la destinación se puede alcanzar usando la dirección de red en la red H.323.

#### 4.3.3.2.2 CONTROL DE LA ADMISIÓN

El portero puede controlar la admisión de las puntos finales en la red H.323. Utiliza los mensajes de RAS, petición de la admisión (ARQ), confirma (ACF), y rechaza (ARJ) para alcanzar esto. Las admisiones controlan pueden ser una función nula que admite todas las puntos finales a la red H.323.

#### 4.3.3.2.3 CONTROL DE LA ANCHURA DE BANDA

El portero proporciona la ayuda para el control de la anchura de banda usando los mensajes de RAS, petición de la anchura de banda (BRQ), confirma (BCF), y rechaza (BRJ). Por ejemplo, si un encargado de red ha especificado un umbral para el número de conexiones simultáneas en la red H.323, el portero puede rechazar hacer más conexiones una vez que se alcance el umbral. El resultado es limitar la anchura de banda asignada total a alguna fracción del disponible total, saliendo de la anchura de banda restante para los usos de los

datos. El control de la anchura de banda puede también ser una función nula que acepta todos los pedidos cambios de la anchura de banda.

#### 4.3.3.2.4 GERENCIA DE LA ZONA

El portero proporciona las funciones antedichas -- conversión de dirección, control de las admisiones, y control de la anchura de banda -- para los terminales, las entradas, y MCUs situado dentro de su zona del control. Una zona H.323 se define en el asunto 3 .

### 4.3.3.3 FUNCIONES OPCIONALES DEL PORTERO

#### 4.3.3.3.1 EL SEÑALAR DEL LLAMAR-CONTROL

El portero puede encaminar llamar-señalar mensajes entre las puntos finales H.323. En un punto para señalar conferencia, el portero puede procesar los mensajes llamar-que señalan H.225. Alternativomente, el portero puede permitir que las puntos finales envíen los mensajes llamar-que señalan H.225 directamente el uno al otro.

#### 4.3.3.3.2 AUTORIZACIÓN DE LA LLAMADA

Cuando una punto final envía llamar-señalar mensajes al portero, el portero puede aceptar o rechazar la llamada, según la especificación H.225. Las razones del rechazamiento pueden incluir restricciones acceso-basadas o tiempo-basadas, a y desde los terminales o las entradas particulares.

#### 4.3.3.3.3 GERENCIA DE LLAMADA

El portero puede mantener la información sobre todas las llamadas activas H.323 de modo que pueda controlar su zona proporcionando la información mantenida a la función de la anchura de banda-gerencia o reencaminando las llamadas a diversas puntos finales para alcanzar balancear de la carga.

### 4.3.4 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.

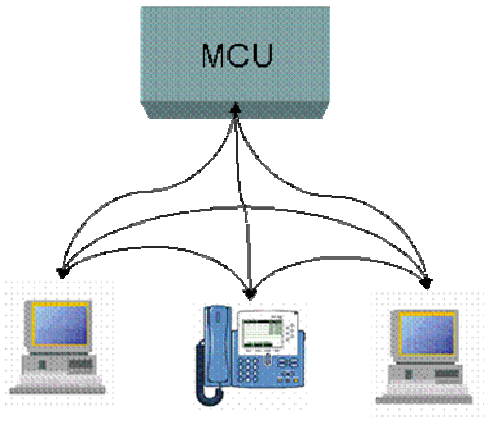



**Figura 15.** Conferencia Multipunto Descentralizada

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.

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.

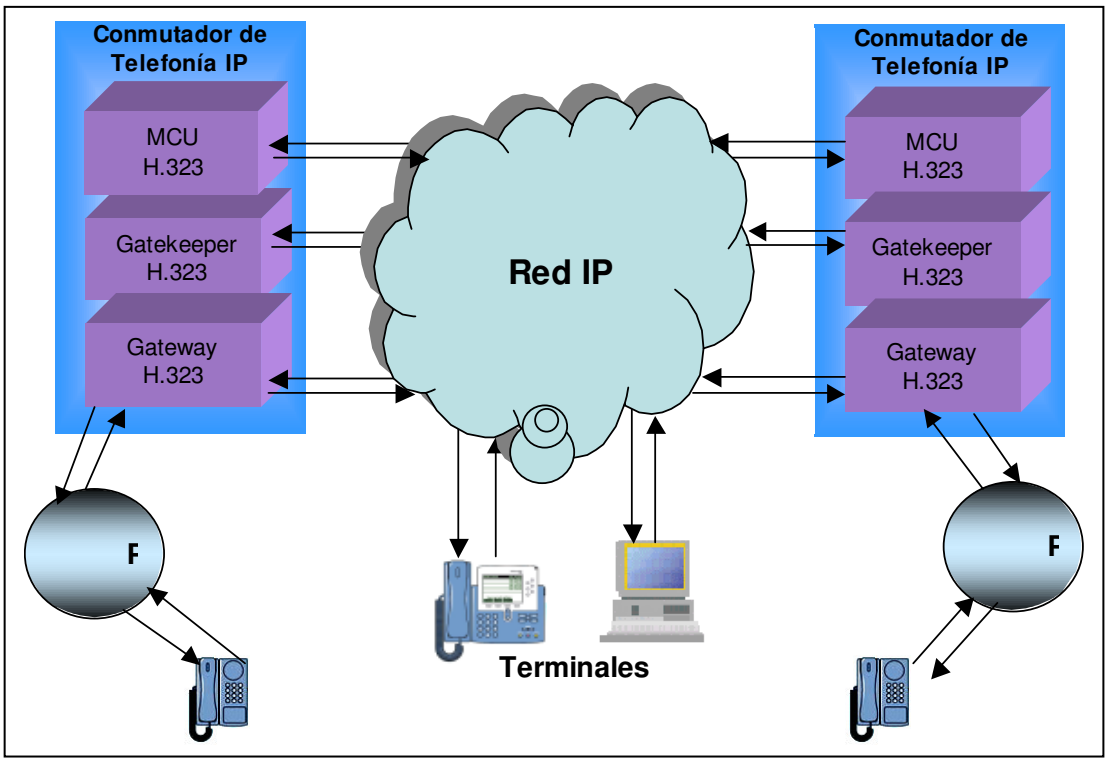



**Figura 16.** Distribución Lógica de los Componentes de una Red H.323

Durante una Llamada VoIP

# 5. 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).

## 5.1 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).

## 5.2 CAPACIDADES DE SIP

SIP soporta cinco facetas en el establecimiento y terminación de comunicaciones multimedia:

### 5.2.1 **Locación de usuario**:

determinación del dispositivo a utilizar por la comunicación

### 5.2.2 **Disponibilidad del usuario**:

determinación de la voluntad del receptor de la llamada de participar en las comunicaciones

### 5.2.3 **Capacidad del usuario:**

determinación del medio y de los parametros del medio a utilizar

### **5.2.4 Establecimiento de sesión:**

"ringing", establecimiento de los parámetros de las sesión en ambos extremos

### **5.2.5 Gestión de sesión:**

incluyendo transferencia y terminación de las sesiones, modificación de parámetros de la sesión y la invocación de servicios.

## 5.3 FRAMEWORK DE DISEÑO DE SIP

### 5.3.1 Integración con Protocolos IETF

SIP no es un protocolo integrado verticalmente.

SIP puede utilizar otros protocolos estándares para construir las sesiones de una aplicación basada en SIP. Por ejemplo:

- TCP/UDP - para transportar la información de señalización.
- TLS - para establecer sesiones seguras.
- DNS - para resolver nombres de servidores de acuerdo a la dirección de destino.
- RSVP, DiffServ - para asegurar la calidad de servicio de la sesión.
- RTP Real Time Protocol -para transportar las comunicaciones interactivas de voz, datos y video.
- RTSP Real Time Streaming Protocol - para controlar el envio de streaming media.
- SAP Session Advertisement Protocol - para publicar sesiones multimedia via multicast.
- SDP Session Description Protocol - para describir sesiones multimedia.
- MIME - Multipurpose Internet Mail Extension - estándar para describir contenido en Internet.

- HTTP - Hypertext Transfer Protocol - toma parte de la sintaxis y semantica, los mecanismos de autenticación, etc.
- SMTP - Simple Mail Transport Protocol - reutiliza headers, mecanismos de enrutamiento, modo de direccionamiento, etc.
- COPS - Common Open Policy Service - para establecer políticas de calidad y seguridad
- OSP - Open Settlement Protocol. - para automatizar el provissioning de los usuarios.
- XML - eXtensible Markup Language - para crear servicios y transmitir información de eventos.

### 5.3.2 Escalabilidad

La arquitectura SIP es escalable, flexible y distribuida.

- La funcionalidades tales como proxy, redirección, locación y registro puede residir en un único servidor o en varios servidores distribuidos.
- La funcionalidad distribuida permite incorporar nuevas funciones o procesos sin afectar los demás componentes.

- El protocolo conserva información de estado en los extremos, permitiendo recuperarse de fallas de alguno de los componentes.
- La escalabilidad y redundancia se logra bajo el paradigma de N+1
- No es necesario un control centralizado

### 5.3.3 Simplicidad

SIP está diseñado:

- "Rápido y simple en el centro."
- "Inteligente y con menor volumen en el borde."
- Basado en texto para una implementación y depuración simple.
- Utilización de "primitivas" (métodos y respuestas) para el establecimiento de sesiones. No define servicios o funciones…

### 5.3.4 Movilidad

- SIP permite implementar dos tipos de movilidad diferentes:

1. La movilidad personal, que permite que el usuario pueda ser alcanzado en un dispositivo cualquiera, mediante los servicios de

proxy y redirección

2. La movilidad intrínseca provista por la ubicuidad del protocolo IP.

- El registro permite mantener las locaciones actuales del usuario de manera dinámica.
- Basado en la locación actual el proxy server enrutará las llamadas a la locación actual del usuario.
- Ejemplos de aplicaciones de movilidad incluyen presencia y forking de llamadas.

### 5.3.5 Servicios de Valor Agregado

SIP puede soportar, entre otras, las siguientes funciones:

- Facilidades básicas (call waiting, call forwarding, call blocking etc.).
- Videoconferencias.
- Picture ID.
- Mensajería Unificada.
- Call forking.
- Click to talk.
- Presencia.

- Mensajes Instantáneos.
- Find me / Follow me.
- Conferencias ad-hoc y programadas.
- Control por aplicaciones externas (CTI)
- Colaboración Web

## 5.4 ARQUITECTURA

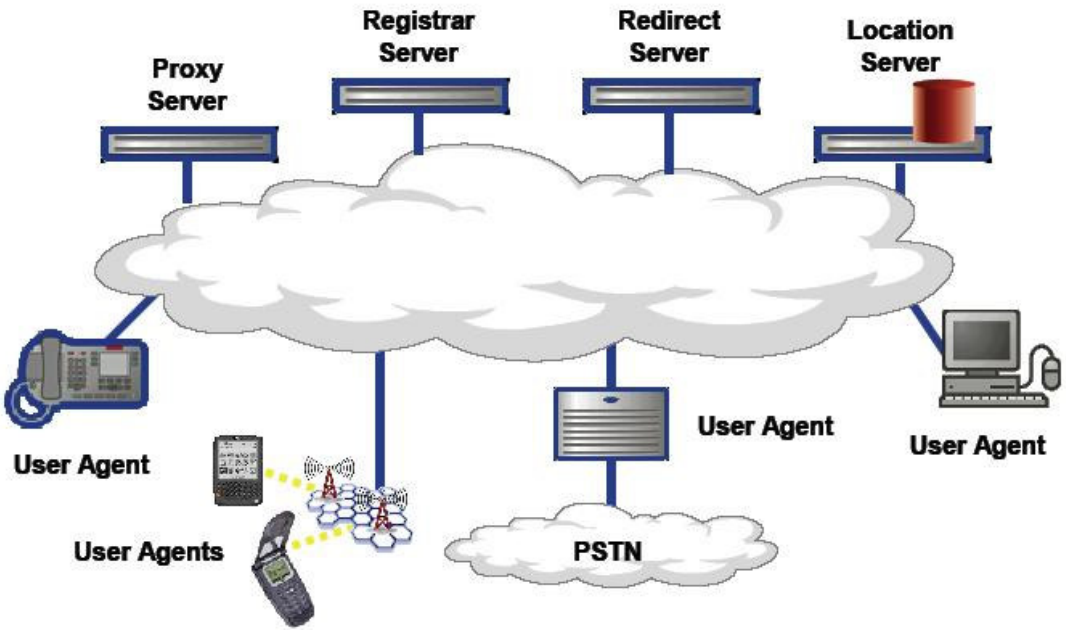



**Figura 15.** Arquitectura Distribuida en SIP

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.

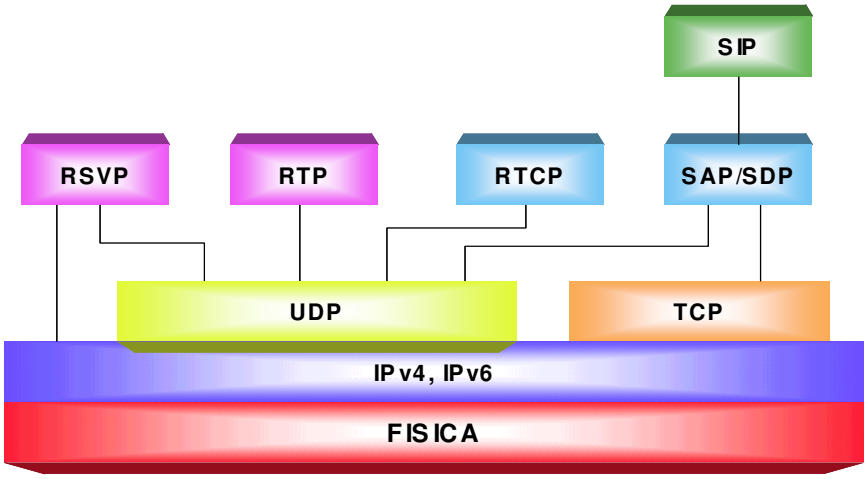



**Figura 16.** Pila de Protocolos SIP

### 5.4.1 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, así 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.

## 5.5 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.

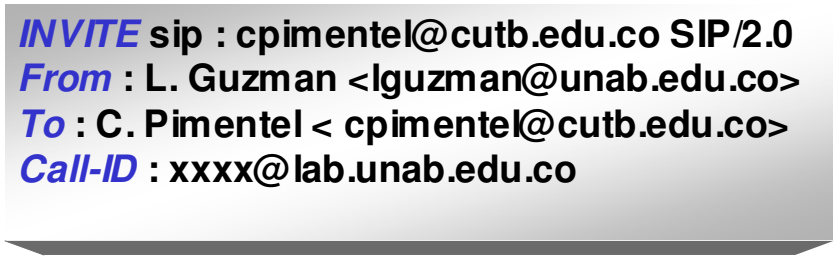



**Figura. 20** Mensaje de invitación SIP

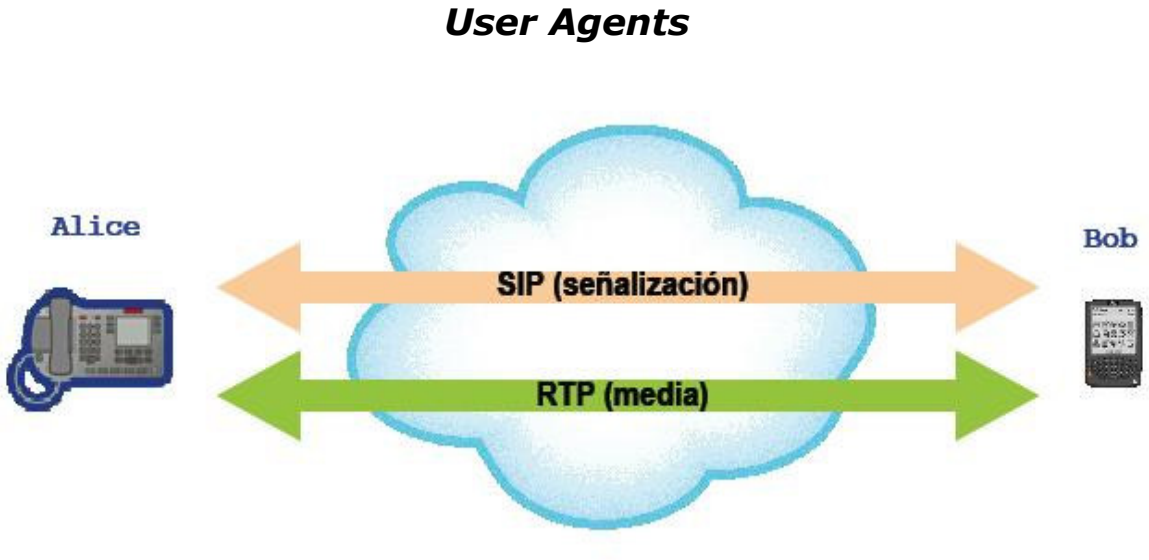



**FIGURA 21**. agentes de usuario

El protocolo SIP es "peer to peer": Dos User Agents pueden establecer una sesión entre sí

### 5.5.1 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 así como la información de control.

- Una aplicación que inicia, recibe y termina llamadas o sesiones.
    - User Agent Clients (UAC) - Una entidad que inicia una sesión.
    - User Agent Server (UAS) - Una entidad que recibe una sesión.
    - Las entidades se implementan de acuerdo a la función del User Agent, en general se implementan ambas.
- Los User Agents pueden tomar distintas formas de acuerdo a su función:
    - Teléfono
    - Softphone
    - Gateway PSTN
    - Servidor de conferencias
    - Servidor de voice mail
    - IVR
    - Discador

### 5.5.2 SERVIDOR PROXY

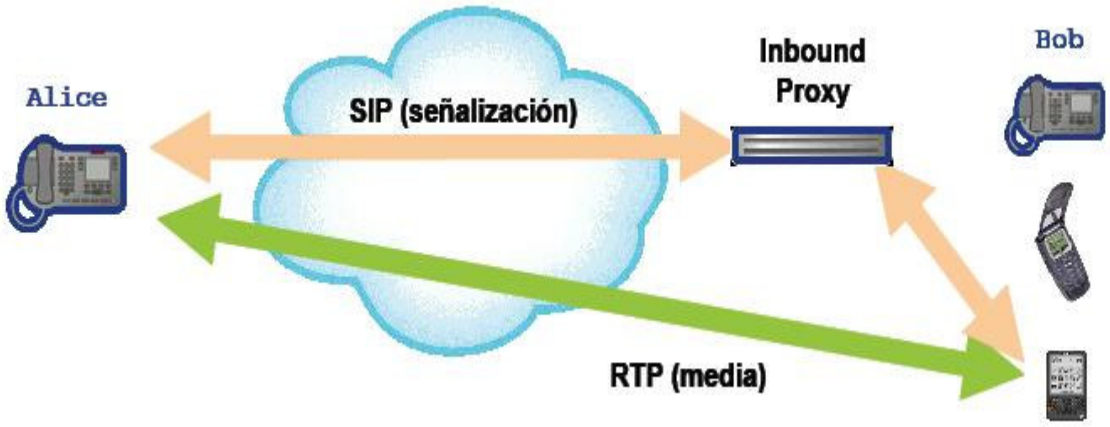



**FIGURA 22.** servidor proxy

Alice desea establecer una sesión con Bob

Si bien dos User Agents pueden establecer una sesión entre sí…

- Cómo se independiza al usuario del dispositivo que utiliza ?
- Como se resuelve la dirección IP de cada User Agent, si el dispositivo cambia ?
- Cómo se implementan servicios como Presencia, Voice Mail, Billing, etc para cada uno de los usuarios ?
- Cómo hace un usuario para definir reglas de preferencia o búsqueda para sus sesiones entrantes ?

Respuesta: Utilizando un servidor Proxy que reciba las sesiones entrantes e implemente estos servicios para los usuarios de un dominio

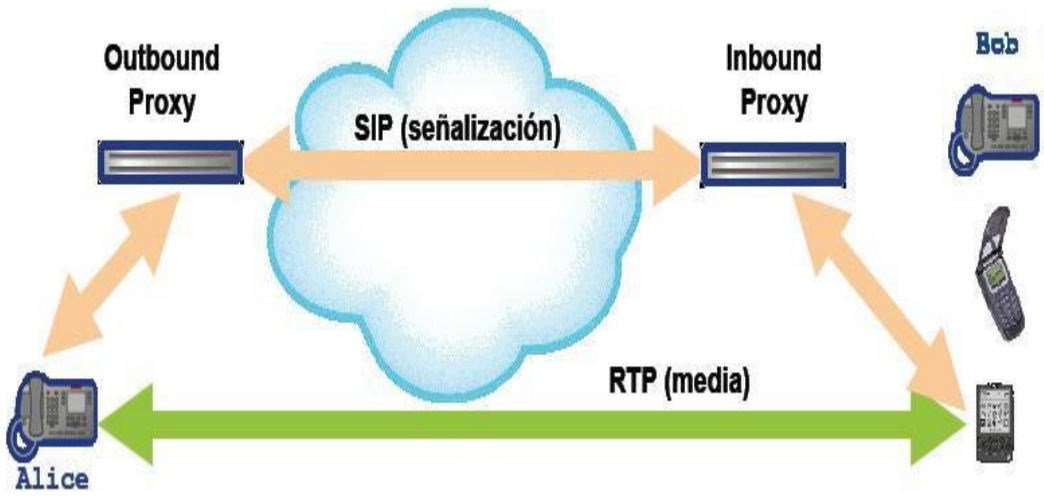



**FIGURA 23.** señalización SIP

De la misma manera, se suele utilizar un servidor Proxy saliente, para simplificar la administración de los usuarios de un dominio, y aplicar políticas, accounting, etc a las sesiones salientes de ese dominio.
Un mismo servidor puede funcionar como Proxy entrante y saliente de un dominio

Un aplicación intermedia que actúa tanto con servidor y cliente, generando mensajes SIP a nombre del cliente que generó el mensaje original. Los mensajes pueden ser respondidos internamente o pasandolos a otros servidores, posiblemente después de cierta traducción.

Interpreta, re-escribe o traduce un mensaje antes de enrutarlo.
El proxy puede enrutar mensajes SIP aun sin conocer ciertos métodos, permitiendo la interoperabilidad
Conceptualmente se dividen en dos tipos de Proxy Server:

- El outbound proxy recibe los request de los user agents de su dominio y define su enrutamiento basado en los datos de la URI de destino.
- El inbound proxy recibe los request para user agents de su dominio y define su localización utilizando los registros del location server.

La división entre Proxy, Registrar, Redirect y Location Servers no es física, sino conceptual, con lo cual dichas funciones pueden coresidir en un único server o estar separadas por motivos de escalabilidad, redundancia o rendimiento

### 5.5.3 REDIRECT SERVER

Un servidor que acepta un request SIP, mapea la dirección en cero o más nuevas direcciones y retorna estas direcciones al cliente.
Al contrario que un proxy server, el redirect server no inicia sus propios mensajes de SIP, sólo responde.
Al contrario de un user agent, el redirect server no acepta o termina llamadas.

Un servidor que acepta mensajes del tipo REGISTER. Este servidor permite popular el Location Server de manera dinámica. Un usuario puede estar registrado con múltiples dispositivos Un dispositivo puede tener registrado múltiples usuarios Cada usuario es responsable de registrar y mantener el registro en sus diferentes dispositivos

### 5.5.4 Location Server

Un servidor que es utilizado por un redirect o proxy server SIP para obtener información acerca de las posibles locaciones de un usuario llamado. Alimentado por el Registrar Server o por interfaces de provisionamiento de usuarios. Es un base de datos, No utiliza SIP para comunicarse con los otros servidores

### 5.5.5 Mensajes SIP - Métodos

INVITE - Inicia una llamada invitando a un usuario a participar en una sesión.

ACK - Confirma que el cliente ha recibido una respuesta final a un método INVITE.

BYE - Indica la terminación de la llamada.

CANCEL - Cancela un requerimiento pendiente.

REGISTER - Registra al user agent.

OPTIONS - Usado para consultar las capacidades de un servidor.

INFO - Usado para transportar información fuera de banda, como dígitos DTMF.

MESSAGE - Transporta mensajes de texto entre user agents.

REFER - Solicita generar una sesión desde una tercera parte

SUSCRIBE - Suscribe al user agent a ser notificado sobre eventos que ocurran en otro user agent

NOTIFY - Notifica los eventos suscriptos

UPDATE - Modifica elementos del diálogo activo

PRACK - Confirmación provisoria

PUBLISH - Publica la notificación de eventos

### 5.5.6 Direcciones SIP

Las direcciones SIP están identificadas por una URI (Uniform Resource Identifier) con la forma: user@host. Ejemplos de URIs SIP:

- sip:mstokle@nortelnetworks.com
- sip:bob@192.168.10.1
- sip:14083831088@gateway.nortel.com
- sips:mstokle@nortelnetworks.com

Los proxy server pueden resolver y transformar URIs del tipo tel, que contienen direcciones E.164

- tel:+541148277237

Dependiendo del tipo de user agent, estos también pueden utilizar otros tipos de URIs como http: o mailto:

- http://www.nortelnetworks.com
- mailto:mstokle@nortelnetworks.com

Las URIs se diferencian de las URLs en que estas últimas apuntan a una ubicación física específica (ejemplo: un archivo)

### 5.5.7 Proceso para Establecer una Comunicación

Establecer una comunicación usando SIP ocurre usualmente en 6 pasos:

1. Localización del usuario.
2. Determinación del medio a utilizar - Se efectúa por medio de un modelo de oferta/respuesta por intermedio de SDP (Session Description Protocol)
3. Determinación de la parte llamada de aceptar la llamada - aceptar o rechazar.

4. Establecimiento del medio.

5. Modificación de la llamada o manejo de la misma - ejemplo, transferencia.

6. Terminación de la llamada.

### 5.7.8 Flujos de Ejemplo: Registro

- Cada vez que el usuario enciende su dispositivo (Teléfono SIP, PC, u otro dispositivo SIP), el cliente se registra con el registrar server.
- La registración también ocurre cuando el usuario modifica su locación física o enciende un nuevo dispositivo.
- La información de registro se refresca periódicamente y cada usuario debe de registrarse con el registrar server.
- El registrar server actualiza la base de datos del location server
- La registración puede hacerse por otros medios (páginas web, scripts, admin, etc.).
- El location server enlaza la dirección de registro del tipo sip:mstokle@nortelnetworks.com con las direcciones físicas de los dispositivos, del tipo sip:mstokle@47.46.208.11 o sip:mstokle@pda.mstokle.cala.nortel.com

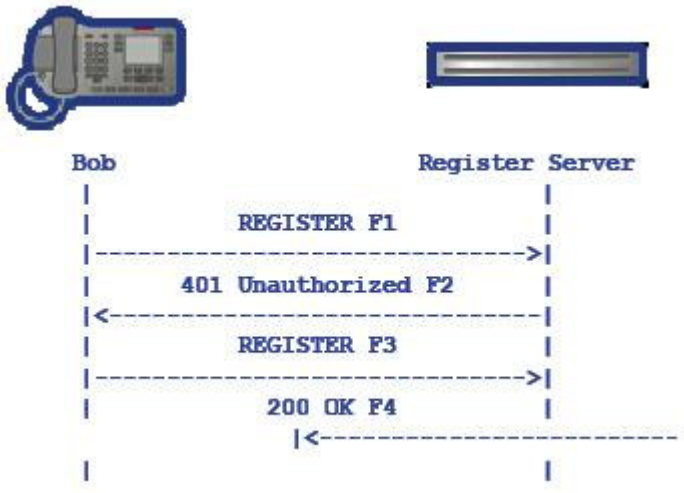



**FIGURA 24**. registro

### 5.5.9 Flujos de Ejemplo: Llamada básica

SIP es esencialmente un protocolo peer-to-peer

- En este caso, Alice y Bob conocen su locación actual y pueden contactarse directamente.
- Alice envía un INVITE a Bob. En el cuerpo del INVITE ofrece sus capacidades de media usando SDP (audio, video, juegos, etc).
- El user agent de Bob envía una respuesta provisional (180 Ringing).

- Una vez que el usuario contesta la llamada, el user agent envía la respuesta definitiva (200 OK) y en el cuerpo de esa respuesta se envía la respuesta sobre la media utilizar usando SDP.
- El user agent de Alice envia el ACK y se establece el path de media utilizando los protocolos apropiados (RTP en este caso).
- Bob corta la llamada, su user agent envia un BYE
- El user agent de Alice envía su respuesta exitosa (200 OK)


**figura 25** Llamada básica

## 5.6 FLUJO DE MEDIOS (AUDIO, VIDEOS, DATOS)

### 5.6.1 *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).

### 5.6.2 *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.

### 5.6.3 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.

# 6 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.

## 6.1 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.

### 6.1.1 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

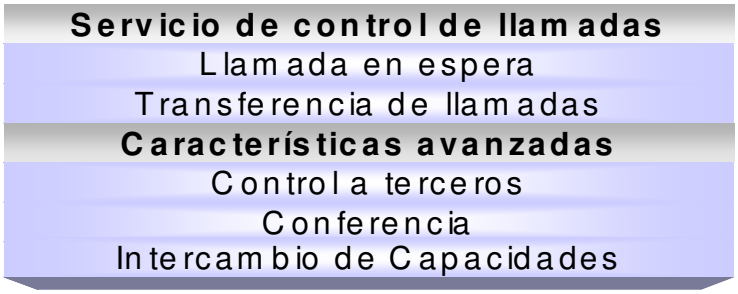



**Figura 26** Características de Funcionalidad en H.323 y SIP.

#### 6.1.1.1 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

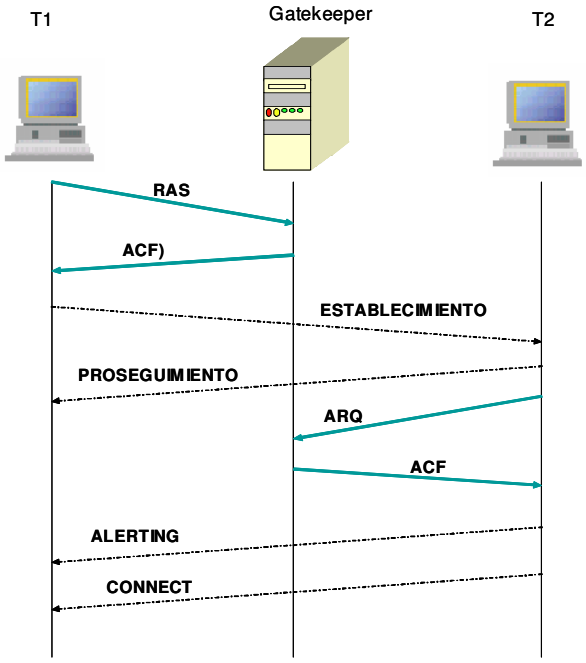



**Figura. 27** Establecimiento de llamada H.323

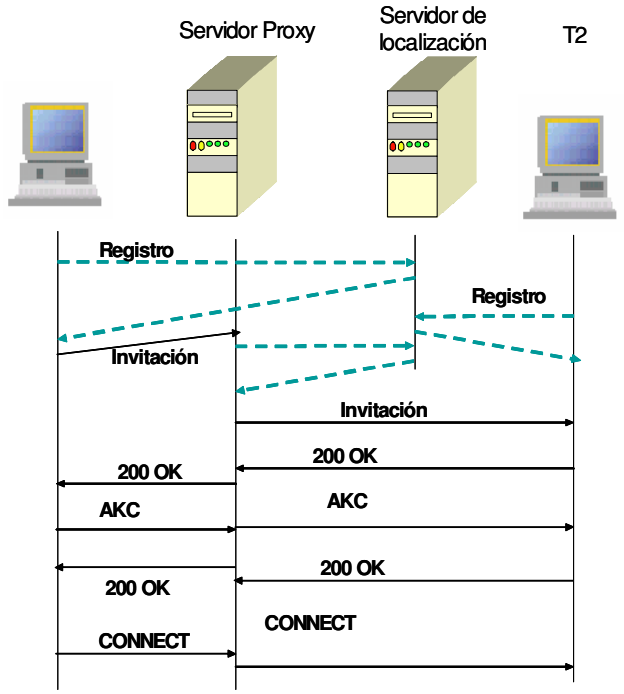



**Figura. 28** Establecimiento de llamada SIP

**6.1.1.2 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.

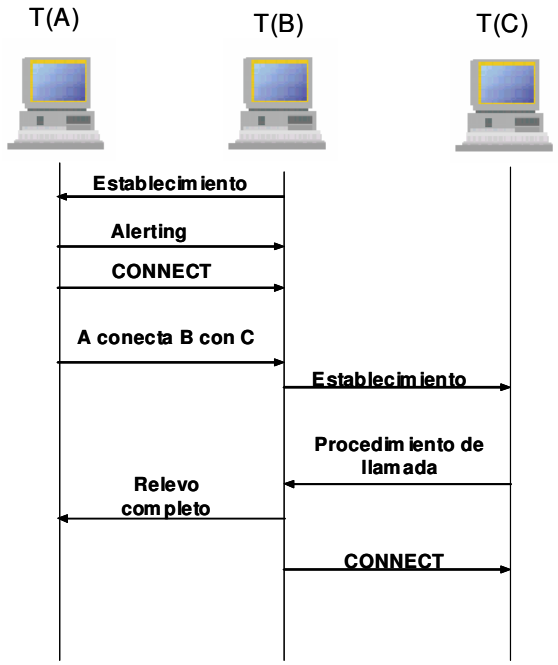



**Figura. 29** Transferencia ciega de llamada en H.323

# 7. CALIDAD DE SERVICIO (QOS) EN VOIP

En todo el proceso de la comunicación intervienen diversos factores que nos determinarán la calidad del servicio ofrecido.
En este caso, existen principalmente dos elementos que nos determinan esta calidad, el algoritmo de compresión utilizado y el retraso en la propagación de la señal.
La comunicación sobre la propia red de datos, nos obliga a compartir ancho de banda con todo el conjunto de aplicaciones que se ejecutan en nuestra red. Por ello es necesario disminuir en lo posible la saturación de la red y de esta forma asegurarnos de no producir un colapso de todas nuestras comunicaciones.
Para ello se utilizan algoritmos de compresión, que, sin disminuir la calidad del sonido notablemente, si reduzcan drásticamente el ancho de banda utilizado.
En una codificación normal, por ejemplo PCM, el muestreo de la señal con una resolución y frecuencia determinada se inyecta en la corriente de datos. Con ello la calidad obtenida puede ser de un nueve sobre diez, ciertamente alta pero a costa de necesitar 64 Kbits por segundo para la transmisión.
Con los actuales algoritmos de compresión de predicción lineal, podemos alcanzar niveles de calidad de siete u ocho sobre diez y rebajar el ancho de banda necesario a 5,3 Kbits por segundo.
En cuanto a la propagación, en todo el sistema se acumulan diversos retrasos producidos por diversos motivos.

Primero interviene la necesidad de comprimir paquetes de un tamaño concreto. Realmente se produce un retraso por acumulación de la señal. En este orden hablamos de retrasos del orden de 30 ms.
Posteriormente se producen retrasos en el tratamiento de la señal, aunque estos no deben sobrepasar el propio retraso de acumulación.
Por último se encuentra el retraso propio de la red. Aquí interviene la propagación propia de la red, routers, etc.
Como norma general el retraso total introducido en una comunicación puede oscilar sobre los 200 ms. Siendo una medida dependiente de la red y bastante oscilante.

Como resumen podemos decir que la calidad total del servicio es algo inferior a la obtenida por la telefonía tradicional, pero dentro de unos márgenes totalmente aceptables.

## 7.1 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.

### 7.1.1 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.

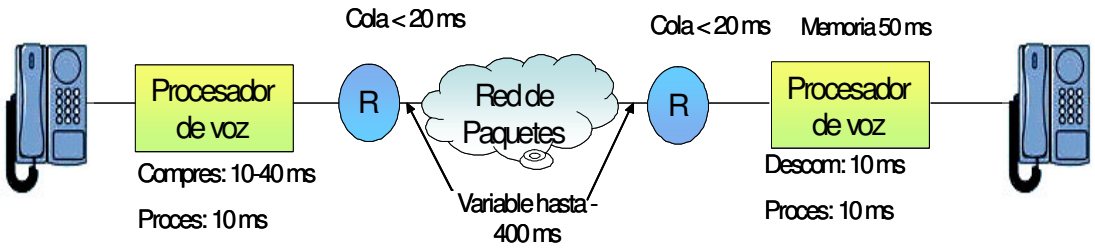



**Figura 30.** Contribuciones a la Latencia en VOIP

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.

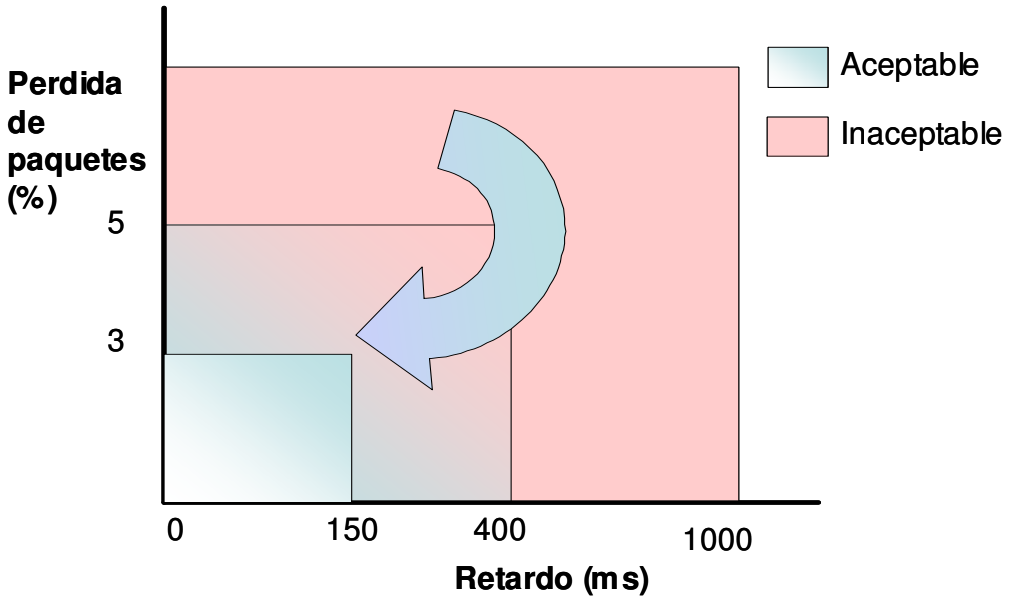



**Figura 31.** Áreas de Funcionamiento en Telefonía IP

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

### 7.1.2 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).

### 7.1.3 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 32).

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.

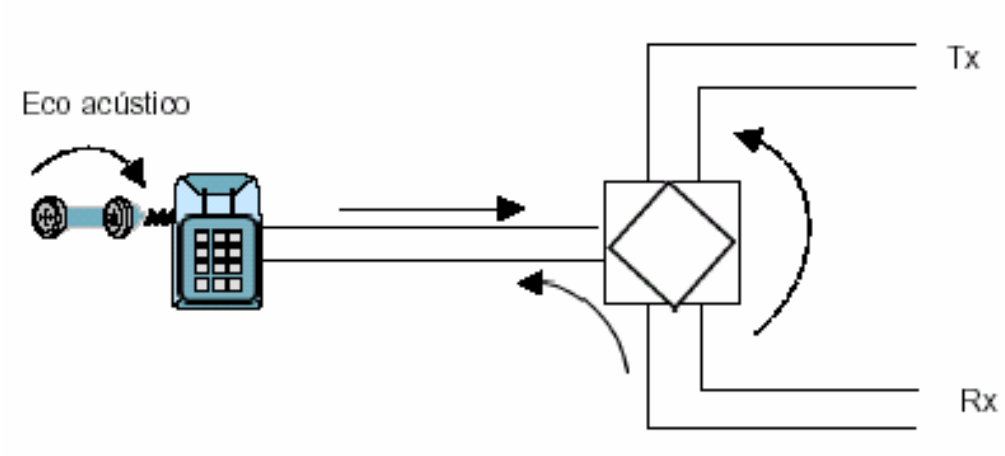



**Figura 32.** Fuentes de Eco

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.

### 7.1.4 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.

### 7.1.5 Packet Loss.

Es la tasa de perdida de paquetes. Representa el porcentaje de paquetes transmitidos que se descartan en la red. Estos descartes pueden ser producto de alta tasa de error en alguno de los medios de enlace o por sobrepasarse la capacidad de un buffer de una interfaz en momentos de congestión. Los paquetes perdidos son retransmitidos en aplicaciones que no son de Tiempo

Real; en cambio para telefonía, no pueden ser recuperados y se produce una distorsión vocal.

## 7.2 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 33.

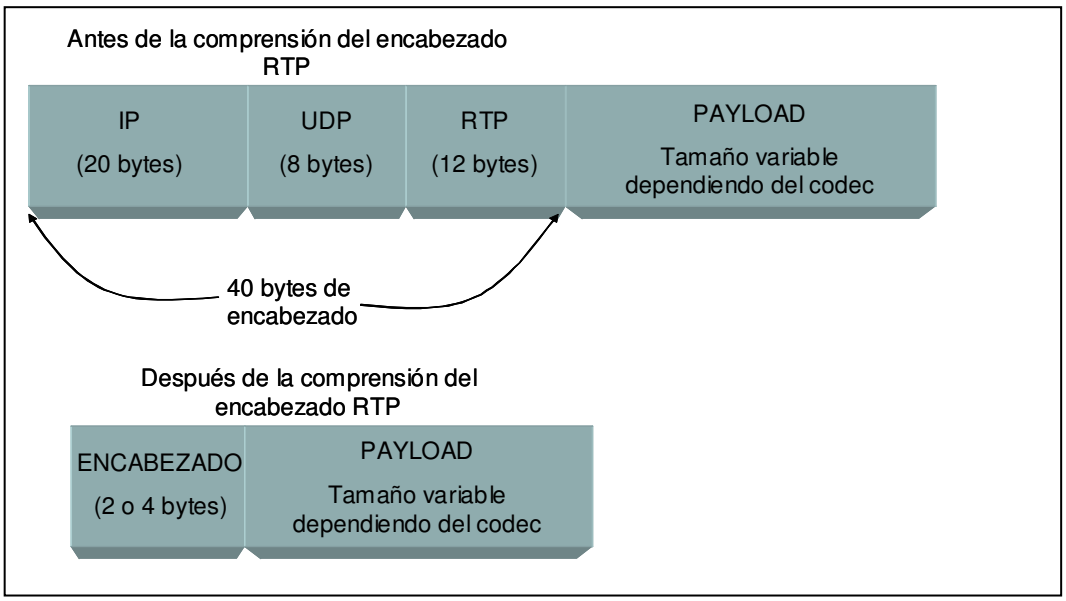



**Figura 33.** Comprensión del RTP

## 7.3 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.

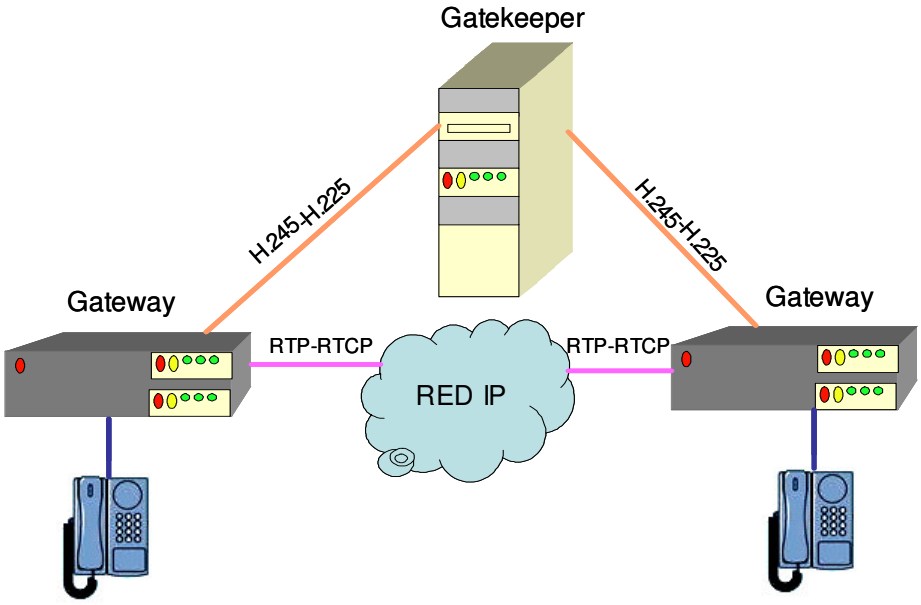



**Figura 34.** Proceso de una llamada

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.

# 8. VENTAJAS VOIP

La Telefonía IP permite que las organizaciones y los individuos disminuyan los costos de servicios existentes como voz y transmisión de video, ampliando al mismo tiempo sus medios de comunicación al incluir videoconferencias por módem, aplicaciones compartidas y herramientas de pizarrón.

En el pasado las organizaciones han instalado redes por separado para manejar el tráfico tradicional de voz, datos y video. Ya que cada una tenía diferentes requerimientos de transporte, estas redes eran costosas de instalar, mantener y reconfigurar. Además, ya que las mismas eran físicamente distintas, su integración era difícil, si no es que imposible, lo que limitaba su uso potencial.

La Telefonía IP combina voz, video y datos al especificar un transporte común, IP, para cada elemento, uniendo de manera efectiva tres redes en una. El resultado es una mayor capacidad de administración, menores costos de soporte, un nuevo tipo de herramientas de colaboración y mejor productividad.

Sus ventajas potenciales sobre la telefonía convencional son múltiples: es un servicio mucho más barato (a veces, incluso gratis), permite el nomadismo (es decir, el uso de un mismo número de teléfono independientemente de dónde se

encuentre físicamente el usuario) y tiene capacidad multimedia. Además, la calidad del servicio es cada vez mejor, similar a la del teléfono convencional, y permite la interconexión. Existe ya tecnología incluso para solucionar uno de sus grandes problemas, las llamadas a números de emergencia.

## 8.1 FLEXIBILIDAD

Con VOIP, usted puede hacer que una llamada dondequiera si usted tiene conectividad de banda ancha. Desde el IP los teléfonos o ATA´s difundieron su Información sobre el Internet, ellos se pueden administrar por el abastecedor dondequiera . Los viajeros del negocio pueden tomar tan sus teléfonos o ATA´s con ellos en viajes y siempre tener acceso a su teléfono casero. Otra alternativa es el softphone . Un softphone es el software del cliente que carga el servicio de VOIP sobre su tablero del escritorio o computadora portátil, tiene un interfaz en su pantalla que parezca un teléfono tradicional. Mientras usted tiene un headset/microphone, usted puede poner llamadas de su computadora portátil dondequiera en el mundo de banda ancha-conectado.
La mayoría de las compañías de VOIP proporcionan las características que las compañías normales del teléfono cargan extraordinariamente para cuando las agregan a su plan del servicio. VOIP incluye los siguientes servicios:

- Identificación Del Llamador.

- El esperar de llamada .
- Transferencia de la llamada .
- Repita el dial .
- Vuelva la llamada .
- El llamar de tres vías.

## 8.2 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

## 8.3 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.

## 8.4 DESVENTAJAS

- Transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación.
- El aspecto de seguridad es muy relevante como se explicará posteriormente.

- Se cambia confiabilidad por velocidad.

- Finalmente, tenemos que resaltar que así como PSTN, VOIP no puede prestar servicio a todos sus clientes (por ejemplo, una llamada GSM no pude manejar más de algunos cientos o un par de miles de clientes).

- Por ahora, el servicio está restringido a redes privadas (y en consecuencia a pocos usuarios), ya que en un ambiente como una red pública Internet, los niveles de calidad telefónica son bajos pues

tal red no puede proveer anchos de banda reservados ni controlar la dramática fluctuación de carga que se presenta.

- El control de congestión de TCP hace reducir la ventana de transmisión cuando detecta pérdida de paquetes, y el audio y el video son aplicaciones cuya rata de transferencia no permite disminuciones de este tipo en la ventana de transmisión.

# 9.ASPECTOS LEGALES

## 9.1 REGULACIÓN VIGENTE PARA PRESTAR SERVICIOS DE VOIP EN COLOMBIA

La política regulatória del sector de las telecomunicaciones en Colombia tiene por directriz regular por servicios mas no por tecnología. En este orden de ideas, y en la medida en que VOIP es una tecnología que permite la comunicación de voz a través de una red basada en protocolo IP, no existe en Colombia regulación alguna al respecto, y no se ha proyectado emitirla. El servicio de comunicación de voz, independientemente de la red que se emplee para su prestación, está regulado por las normas previstas para cada servicio, y por lo tanto los interesados en prestar un determinado servicio empleando tecnología IP deberán obtener la respectiva licencia por medio de la cual se autoriza la prestación del servicio. Finalmente, teniendo en cuenta lo anteriormente establecido, al no existir regulación específica para la prestación de VOIP, la prestación de este tipo de comunicaciones por redes IP deberá hacerse mediante la obtención de una licencia que habilite al operador para prestar servicios de telefonía a terceros, la cual la expide el Ministerio de Comunicaciones, de acuerdo con las normas vigentes (Ley 142 de 1994 y Res. CRT 087 de 1997). Diferente es el caso del

establecimiento de redes privadas de telecomunicaciones, para lo cual se deberá tener en cuenta lo previsto en el Decreto 930 de 2992, en la medida en que no se presta servicio a terceros a través de este tipo de redes.

## 9.2 FILOSOFÍA DE ASONET

La Asociación Nacional de Empresas de Internet- ASONET ASONET declara públicamente que bajo el principio de ofrecer al usuario colombiano el servicio de Internet de mejor calidad, al más bajo precio:

1. Rechaza categóricamente la prestación de cualquier servicio ilegal o fraudulento de telecomunicaciones o que viole derechos adquiridos y legítimos de terceros.

2. Expulsará de su agremiación a cualquier asociado al que se le compruebe que hace práctica de estas actividades ilegales o clandestinas.

3. Apoyará todas aquellas políticas, regulaciones y medidas que incentiven la masificación del Internet como medio de comunicación, información, investigación, esparcimiento, educación y negocios.

4. Considera que la Telefonía IP y la VOIP no violan la regulación vigente sobre TPBC.

5. Entiende que estos nuevas formas de telecomunicación afecta a los operadores establecidos quienes pagaron altos costos por la infraestructura por sus licencias de TPBCLD e invita a todos los actores para que bajo mecanismos de concertación busquemos soluciones prácticas que permitan la libre competencia en igualdad de condiciones.

6. Promoverá la libre y leal competencia en el mercado de servicios de Internet y denunciará las prácticas comerciales restrictivas, desleales y de posesión dominante.

7. Pugnará por que se garantice oportunamente y a costos razonables el acceso a la infraestructura de telecomunicaciones y las tecnologías de la información.

8. Con base en las consideraciones contenidas en éste documento ASONET reafirma su posición y la de sus miembros, en el sentido de que la VOIP es claramente de un servicio de valor agregado, y que los esfuerzos del ministerio deben estar encaminados a garantizar la eliminación de restricciones que

permitan a los demás operadores del sector, la posibilidad de tener acceso a la interconexión con otras redes, señalización y numeración.

## 9.3 SECTOR DE LAS TELECOMUNICACIONES EN COLOMBIA

El sector de las telecomunicaciones en Colombia ha tenido un proceso especial de transición del monopolio de empresas públicas a la libre competencia, que se inició con la apertura de la larga distancia (1987), y siguió con las subastas por los servicios celulares y de PCs. Su estructura competitiva actual tiene varias características. Predomina el monopolio y la posición dominante de las empresas públicas (TELCOS) sobre la red y los servicios de TPBC. Como las TELCOS compiten como ISPs con el sector privado por los mercados de usuarios del Internet, impiden a las ISPs privadas la desagregación del bucle local y no suministran infraestructura (Els) en términos de oportunidad y costos razonables.

El sector público domina la TPBCL con 7.2 millones de líneas fijas y altas tarifas locales. El sector público domina también el TPBCLD (ETB, TELECOM, ORBITEL-50% EPM) y el servicio de telefonía móvil de PCS (EPM-ETB). Realmente el único servicio con total inversión privada en Colombia es el TMC. El sector público ejerce monopolio sobre la RTPBC y sobre la infraestructura e

instalaciones esenciales con lo cual impide el acceso de nuevos operadores a la prestación de los servicios de valor agregado.

ASONET considera que el BY-PASS y demás métodos que eluden la TPBCLD son fraudulentos y clandestinos y atentan contra los derechos adquiridos de los beneficiarios de las licencias, las cuales vencerán a finales del 2007 y su prorroga tendrá que realizarse de conformidad con la regulación vigente en su momento. Los operadores de servicios de Internet no tienen acceso a las redes e infraestructura a costos razonables.

Defiende los principios constitucionales de la defensa de los usuarios libre competencia y enfatiza que el Internet es una herramienta para consolidar el proceso de apertura a la competencia en beneficio del usuario y del desarrollo social y económico del país.

ASONET ha ofrecido en todo momento al Gobierno y al sector su cooperación y esfuerzo para llegar a un acuerdo concertado con las TELCOS sobre los intereses, la interpretación y la aplicación del TLC en materia de servicios de telecomunicaciones, para lograr acuerdos mutuamente satisfactorios a favor de los intereses del sector y del país.

Fundamentados en los principios de gradualidad, equidad y oportunidad, de conformidad con los objetivos sociales de universalidad y solidaridad en el suministro de los servicios de telecomunicaciones, ASONET insta a las empresas públicas dominantes a participar en el mercado del Internet

competitivamente, con eficiencia y transparencia, alejadas de prácticas corruptas, burocráticas y politiqueras, asegurando al sector privado el uso de la infraestructura pública remunerada a costos razonables.

## 9.4 COMPETENCIA ABIERTA EN SERVICIOS DE INTERNET

Internet es un instrumento de entretenimiento, educación, investigación, comunicación e información. Para lograr su penetración en todas las capas sociales y lugares del país se requiere de banda ancha disponible, costos razonables para el usuario, disposición de las mejores tecnologías y bajos precios de PCs.

Consideramos que se debe evitar tanto el monopolio y posición dominante de las empresas americanas en el país, como de las públicas en los servicios básicos y de valor agregado de telecomunicaciones. Lamentablemente ésta premisa no está siendo considerada por los operadores públicos establecidos, a pesar de lo cual ASONET ofrece su cooperación y esfuerzo para llegar a un acuerdo concertado con el sector público sobre los intereses nacionales en materia de servicios de telecomunicaciones y lograr la masificación del servicio de Internet, favorecer a los usuarios, obtener un real servicio universal del Internet, aumentar el comercio electrónico y desarrollar rápidamente las tecnologías de VOIP/Telefonía IP.

## 9.5 VOIP ES UN SERVICIO DE VALOR AGREGADO O UNA TECNOLOGIA

En Colombia y otros países del mundo se discute actualmente la legalidad del origen y terminación de llamadas de voz sobre la red IP. De acuerdo con los intereses de las diferentes empresas del sector de telecomunicaciones, la Voz sobre IP se quiere encasillar regulatoriamente como un servicio de TPBC o de VALOR AGREGADO.

VOIP es un termino genérico para la prestación del servicio de voz, fax y otros relacionados, mediante conmutación de paquetes sobre redes basadas en IP- Internet Protocol (UIT-FMPT 2001).

Telefonía Internet- IP, es el transporte de voz entre terminales de una red IP identificados por una dirección IP y terminales de la red.

Así como la Voz sobre IP (VOIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP y a la dirección IP del destinatario en forma de paquetes de datos, el servicio de Telefonía IP es una aplicación inmediata de esta tecnología, que permite la realización de llamadas telefónicas en paquetes sobre redes IP u otras redes utilizando un PC, gateways, modems y teléfonos estándares.

En una llamada telefónica por IP, la voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de Internet a la persona con la que estamos hablando. Cuando alcanzan su destino éstos

paquetes son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original. Ello es totalmente diferente desde el punto de vista tecnológico, regulatorio y del servicio a la llamada telefónica mediante el servicio de TPBC que usa la RTPBC.

En resumen, los principios básicos que tienen lugar en una llamada a través de Internet son conversión de la señal de voz analógica a formato digital y compresión de señal a protocolo de Internet (IP) para su transmisión por la red de Internet. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

# 10. SEGURIDAD

Desafortunadamente existen numerosas amenazas que conciernen a las redes VOIP; muchas de las cuales no resultan obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables.

La información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en tu red, creando grabaciones completas de conversaciones y datos de usuario.

La conversación es en sí misma un riesgo y el objetivo más obvio de una red VOIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VOIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso, peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en tu red.

Las llamadas son también vulnerables al "secuestro". En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la

llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

La enorme disponibilidad de las redes VOIP es otro punto sensible. En el PSTN, la disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VOIP. Todos estamos familiarizados con los efectos demoledores de los ataques de denegación de servicio. Si se dirigen a puntos clave de tu red, podrían incluso destruir la posibilidad de comunicarte vía voz o datos.

Los teléfonos y servidores son blancos por sí mismos. Aunque sean de menor tamaño o nos sigan pareciendo simples teléfonos, son en base, ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de bugs o agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

## 10.1 COMO DEFENDERSE

Se ha hablado de la maravilla de la tecnología de voz sobre ip, y se han encontrado graves problemas de seguridad. Afortunadamente, la situación no es irremediable. En resumidas cuentas, los riesgos que comporta usar el protocolo VOIP no son muy diferentes de los que nos podemos encontrar en las redes habituales de IP. Desafortunadamente, en los "rollouts" iniciales y en diseños de hardware para voz, software y protocolos, la seguridad no es su punto fuerte. Esto es lo que siempre suele pasar cada vez que aparece una nueva tecnología.

Existen algunas pruebas que puedan aliviar las amenazas sobre esta tecnología.

Lo primero que se debe tener en mente a la hora de leer sobre VOIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, puede hacerse. Y encriptar es la única forma de prevenirse ante un ataque. Desafortunadamente, come ancho de banda. Por tanto... ¿Qué se puede hacer? Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual personal network), el protocolo Ipsec (IP segura) y otros protocolos como SRTP (secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación. Esto debería aliviar cualquier atisbo de amenaza. Otra opción podría ser QOS (Quality of Service); los requerimientos para QOS

asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad.

Lo próximo, como debería esperarse, podría ser el proceso de securizar todos los elementos que componen la red VOIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Necesitas configurar cada uno de esos dispositivos para asegurarte de que están en línea con tus demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches y actualizaciones. Se trata del mismo tipo de precauciones que podrías tomar cuando añades nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VOIP.

Tal como se ha mencionado, la disponibilidad de tu red VOIP es otra de nuestras preocupaciones. Una pérdida de potencia puede provocar que tu red se caiga y los ataques son difíciles de contrarrestar. Aparte de configurar con propiedad el router, recuerda que estos ataques no solo irán dirigidos a tus servicios de datos, sino también a los de voz.

Por último, se puede emplear un firewall y un IDS (Intrusion Detection System) para ayudar a proteger la red de voz. Los firewalls de VOIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están

constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el costo está lejos de verse oscurecido por la cantidad de beneficios, así que se aconceja que se perfeccionen los controles de acceso. Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores. Y recuerda: no hay mejor defensa que estar prevenido para el ataque.

## 10.2 VPN (VIRTUAL PERSONAL NETWORK)

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de e-mail, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un

medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services(RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

### 10.2.1 Estructura de las VPNs

Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

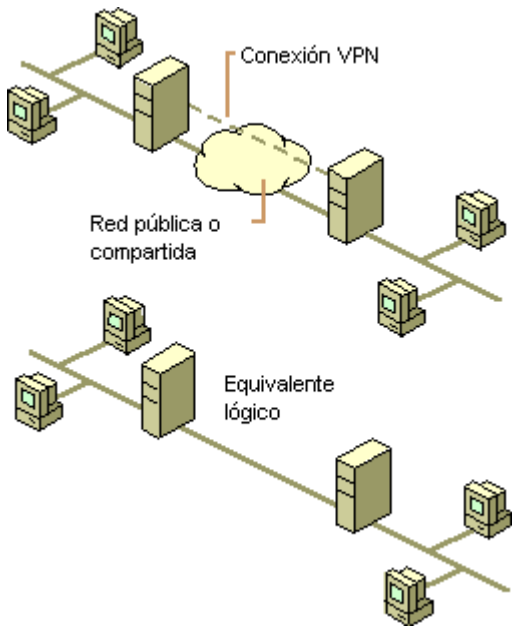



**Figura 34.** Estructura de las VPNs

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida

atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de túneles (“Tunneling”) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de proposals del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

### 10.2.2 Protocolos utilizados en las VPNs

PPTP

Point-to-Point Tunneling Protocol fue desarrollados por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete

IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego “llaman” al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego “llama” al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para

protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

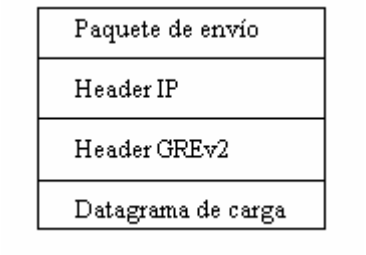



**Figura 36.** capas del encapsulamiento PPTP.

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el

que se intercambia un “secreto” y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

### 10.3 IPSEC (IP SEGURA)

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

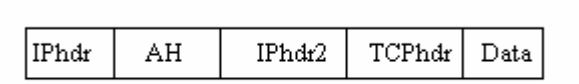
Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

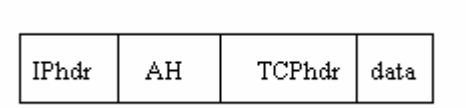
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel es:



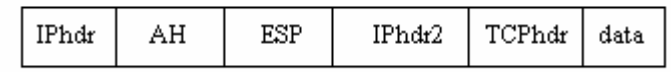

Un ejemplo de paquete AH en modo transporte es:




Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:


Este tipo de paquete se denomina Transport Adjacency.

La versión de entunelamiento sería:




Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

## 10.4 IDS (INTRUSION DETECTION SYSTEM)

El propósito de un sistema de detección de intrusos (IDS -Intrusion Detection System) es identificar los accesos no autorizados o el uso incorrecto de un sistema de computación. Estos sistemas son similares a las alarmas antirrobo. Hacen sonar una alarma y algunas veces toman acciones correctivas cuando un intruso es detectado. Estos, generalmente se dividen en dos categorías: identificación de anormalidades en el sistema o uso incorrecto de los mismos. Los detectores de anormalidades vigilan cualquier comportamiento que se desvíe del uso normal de los sistemas, mientras que los detectores de usos incorrectos hacen lo propio con cualquier comportamiento que coincida con un conocido escenario de ataque.

Como ejemplo de ello, algunos sistemas actúan como un programa de captura de paquetes de redes, interpretando actividad höstil reconociendo los patrones de tráfico en las redes que indiquen que se está produciendo un ataque. Una vez que la vulnerabilidad es identificada, el administrador es informado vía correo electrónico y una alarma es desplegada en la cónsola de administración. Adicionalmente, el ataque puede ser determinado automáticamente, al ser introducido a una base de datos o grabado para su posterior revisión.

# 11. PROGRAMAS PARA ESTABLECER COMUNICACION VOIP

## 11.1 SKYPE

Skype es una utilidad para hablar a través del PC con tus conocidos que promete una mayor calidad de sonido que el resto de programas de este tipo, incluso afirmando más que una llamada de teléfono ordinaria. ¿Lo conseguirá Skype? Skype es lo más parecido a realizar una llamada que existe, hasta suenan los típicos sonidos telefónicos. Realizas la llamada (con un simple clic), puedes descolgar cuando te llaman, colgar, incluso comunica si ya se está hablando con otra persona.

Skype posee lista de amigos, logs de llamadas, un buscador rápido y completo con el que encontrarás fácilmente personas con las que hablar en el idioma que desees, diferentes estados (disponible, invisible, ocupado, etc.), ¡hasta tiene llamadas perdidas!

Skype es muy fácil de usar, bastará con hacer doble clic sobre la persona a la que quieras llamar y listo. También permite enviar mensajes de texto.

A nivel técnico reseñar que Skype, de los creadores de KaZaA, no presenta ningún tipo de problemas por tipo de conexión, router o firewalls, además, no

incluye ningún tipo de publicidad ni spyware (comprobado con Ad-aware y Spybot Search & Destroy).

En resumen, Skype es una excelente forma de hablar totalmente gratis con tus amigos o conocer nuevas personas.

• Requisitos mínimos:

· Procesador: 400 MHz

· Memoria RAM: 128 MB

· Micrófono

· Conexión a Internet

• Cambios recientes:

Algunas nuevas opciones como, por ejemplo, la lista centralizada de contactos, chat, el editor de idioma para la interfaz (que incluye español) o los cambios en cuanto a los avisos y estilo del texto, además de numerosas correcciones de errores.


**Figura 37.** ventana principal SKYPE

## 11.2 NETMMETING

### 11.2.1 CONFIGURACION DEL NETMETING

Si nuestro Sistema Operativo es Windows XP o Windows 2000, no hace falta instalar Microsoft NetMeeting pues ya está instalado. Para lanzarlo basta con abrir el menú de Inicio, pulsar en ejecutar y escribir "conf.exe".

Antes de lanzar esta aplicación, es necesario que los dispositivos capturadores del audio y video( cámara y micrófono ) estén ya conectados a nuestro ordenador y encendidos.

Lanzamos la ejecución de NetMeeting y aparecerá la siguiente ventana:


**Figura 38.** Ventana Principal NETMEETING

Antes de poder realizar una llamada, hemos de registrarnos en el servidor. Para hacerlo pulsamos en la opción "Herramientas" ( "Tools" ) del menú superior y vamos a la subopción "Opciones" ( "Options" ).

Veremos una ventana como la siguiente:

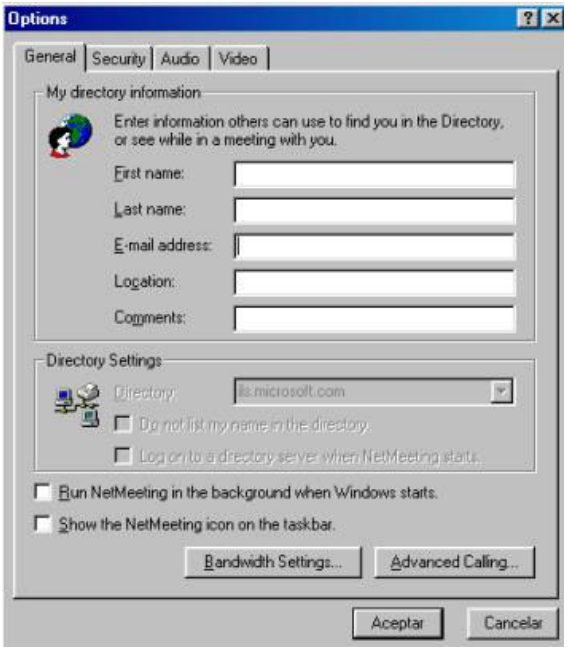



**Figura 39.** NETMEETING/Opciones

En esta ventana pulsamos sobre el botón "Llamada Avanzada..." ("Advanced Calling...") y llegamos a una ventana como la siguiente:

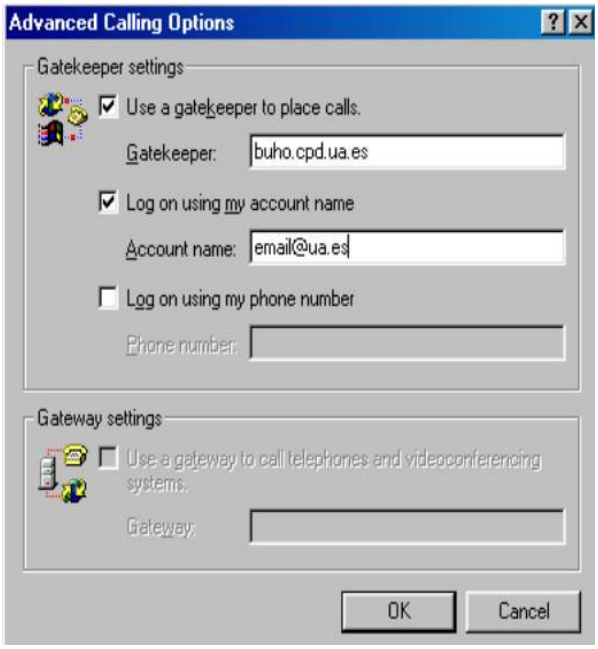



**Figura 40.** NETMEETING/Opciones /Herramientas/ Llamada Avanzada

Seleccionamos la opción "Usar un equipo selector para ubicar todas las llamadas." ("Use a Gatekeeper to place calls"). Al marcar esta opción se habilita un cuadro de texto titulado "Equipo Selector" ("Gatekeeper") en el que escribiremos "buho.cpd.ua.es".

Seleccionamos la opción "Iniciar la sesión usando mi nombre de cuenta" ("Log on using my account name"). Al marcar esta opción se habilita el cuadro de texto titulado "Nombre de cuenta" ("Account name") en el que escribiremos nuestra dirección de correo electrónico

Aceptamos 2 veces ( en esta ventana y en la anterior ) y comprobaremos que el registro en el servidor ha sido satisfactorio si en la esquina inferior derecha de la ventana principal se ilumina un icono en el que aparecen 2 ordenadores conectados. Si no se ha registrado con éxito, saldrá una ventana indicando que no ha podido registrarse en el servidor.

Una vez registrados ya podremos realizar llamadas al exterior desde la ventana principal escribiendo la IP de la persona con la que queremos realizar la videoconferencia:

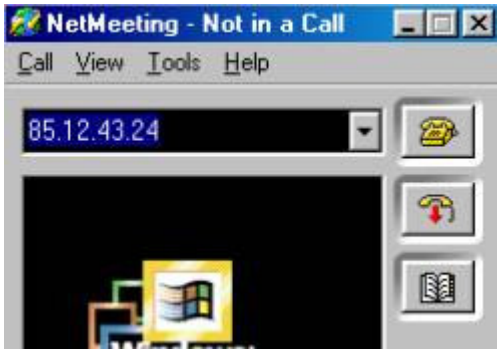



**Figura 38.** Ventana Principal NETMEETING

Debido a la programación de NetMeeting, la llamada la ha de iniciar siempre el cliente que esté dentro de la red de la Universidad.

Utilizando NetMeeting SÍ podremos establecer videoconferencias con:

Otros clientes internos de la red general que utilicen el software de videoconferencia H.323 OpenPhone y que este esté configurado como se indica en el apartado siguiente ( "Configuración OpenPhone" ). Para establecer esta llamada, el otro usuario también debe estar registrado en el servidor y deberemos llamarle utilizando su dirección de correo UA en vez de su IP. En esta situación debe iniciar la llamada el cliente que utilice NetMeeting.

Clientes externos a la red general que utilicen IPs de tipo publico ( las que no sean del tipo 10.xxx.xxx.xxx o 192.168.xxx.xxx o 172.16-31.xxx.xxx ) y que utilicen cualquier aplicación de videoconferencia H.323.

Clientes externos a la red general que utilicen cualquier aplicación de videoconferencia H.323 y que acceden a Internet a través de ADSL en modo Monopuesto.

Clientes externos a la red general que utilicen cualquier aplicación de videoconferencia H.323 y que acceden a Internet a través de ADSL en modo Multipuesto. Este router ADSL ha de ser compatible con H.323. y estar configurado para que las llamadas entrantes H.323 vayan a un ordenador de la red interna.

Clientes externos a la red general que acceden a Internet a través de cualquier otro dispositivo que haga NAT y/o tenga un Firewall habilitado. En este caso, este cliente externo puede optar por 2 soluciones:

1. Instalar otro servidor Gatekeeper en su red. Si opta por esta solución podrá utilizar cualquier aplicación de videoconferencia H.323. Para la selección y configuración del servidor Gatekeeper puede ponerse en contacto con nosotros.

2. Redireccionar y permitir la entrada de los puertos TCP 1731, 1720, 1721, 1722, 1723 y 1724 y UDP necesarios ( ver apartado siguiente ) al ordenador de la intranet que vaya a realizar la videoconferencia y utilizar OpenPhone configurado tal y como se explica en el apartado siguiente "Configuración OpenPhone".

Utilizando NetMeeting NO podremos establecer videoconferencias con:

Otro cliente interno de la red general que también utilice NetMeeting.

Clientes externos a la red general que acceden a Internet a través de ADSL en modo Multipuesto y que utilicen NetMeeting.

## 13. PREGUNTAS FRECUENTES

- **¿Puedo utilizar mi computadora mientras que hablo en el teléfono?**

  Sí

- **¿Puedo llevar mi adaptador del teléfono conmigo cuando viajo?**

  Usted puede poder utilizar su servicio de VOIP dondequiera que usted viaje mientras usted tiene una conexión de alta velocidad del Internet disponible. En ese caso trabajaría igual que su hogar o negocio de.

- **¿Cómo sé si tengo una llamada telefónica de VOIP?**

  Sonará como cualquier otra llamada.

- **¿Cuáles son algunas desventajas de la voz del Internet?**

  Si usted está considerando el sustituir de su servicio telefónico tradicional por VOIP, hay algunas diferencias posibles:
  · Algunos servicios de VOIP no trabajan durante interrupciones de la energía y el abastecedor de servicio puede no ofrecer energía de reserva.

· No todos los servicios de VOIP conectan directamente con los servicios de emergencia.

· Los abastecedores de VOIP pueden o pueden no ofrecer listados de la página del directorio assistance/white.

- **¿Qué clase de equipo necesito?**

Se requiere una conexión de banda ancha (del Internet de alta velocidad). Esto puede estar con un módem de cable, o servicios de alta velocidad tales como DSL o una red de área local. Usted puede enganchar encima de un micrófono barato a su computadora y enviar su voz a través de un módem de cable o conectar un teléfono directamente con un adaptador del teléfono.

- **¿Sustituye al sistema tradicional telefónico ?**

No en su totalidad. Por varios motivos, a veces es mas conveniente efectuar alguna llamada por la telefonía convencional como medio alternativo, dado que es algo mas crítica en cuanto a estabilidad a todos los puntos la telefonia IP. Podemos hablar de un 80% a un 95% del servicio.

- **¿Puedo enviar FAX usando las líneas de telefonía VOIP ?**

  Si. Conecte el equipo de FAX a dicha línea.

- **¿Puedo conectar un MODEM a las líneas de telefonía VOIP ?**

  No. El sistema ya dispone de una capa de datos, con lo cual no es posible efectuar sobre ella tunelizaciones. Además tenga en cuenta que el ancho de banda para cada canal de VOIP es inferior a 22kbps.

- **¿Se requiere conexión permanente a Internet ?**

  No. Puede conectar bajo demanda, pero es aconsejable disponer de conexión permanente. Tenga en cuenta que otros usuarios podrían llamarle.

- **¿Puedo instalar un contestador automático en la línea de VOIP ?**

  Si. Su comportamiento es como cualquier línea analógica proporcionada por cualquier operadora.

- **¿Existen servicios de redireccionamiento de la llamada a otros números** ?

  Si. Opcionalmente puede contratar que su teléfono de voIP al recibir una llamada, sea cursada a otro teléfono, tanto de voIP como de telefonía convencional móvil o fija.

- **¿Cómo funciona el servicio de teléfono tradicional?**

  La red telefónica tradicional se le conoce como PSTN acrónimo de Public Switched Telephone Network o Red Pública de Telefonía Conmutada y emplea la tecnología de conmutación de circuitos para transmitir las llamadas. Se crea una conexión dedicada o circuito que conecta a las dos partes involucradas en la comunicación. Cuando se marca un número telefónico se genera un camino dedicado desde el teléfono del que llama hasta el que recibe la llamada. La red telefónica proporciona transmisiones en tiempo real con garantía de calidad en el servicio asegurado por el circuito dedicado durante la llamada. El circuito no es empleado eficientemente porque esta dedicado durante el todo el tiempo que dure la llamada pero la mayoría de las conversaciones están compuestas principalmente por silencio, así que el circuito en uso, no esta transmitiendo nada realmente.

- **¿Por qué VOIP aprovecha mejor las nuevas tecnologías que la red telefónica convencional o PSTN?**

  Una limitación innata de la PSTN es que la inteligencia reside en las Oficinas Centrales (OC) de las telefónicas o en los conmutadores (o PBX's) de las compañías. La tecnología en esos sistemas es altamente confiable pero los cambios son caros y lentos de realizar. En contraste, la arquitectura IP emplea redes de servidores y ruteadores que son rápidamente escalables en potencia, y las frecuentes innovaciones en software ofrece nuevas características y funcionalidad, lo anterior da como resultado que por ejemplo los ruteadores de alta categoría puedan procesar más información a una fracción del costo y tamaño de un switch tradicional de las Oficinas Centrales (OC) de las telefónicas.

- **¿Requeriré ayuda o saber mucho de computación para usar el servicio?**

  No, para emplear el servicio no requieres ser un guru en comunicaciones o TCP/IP te enviaremos todas las instrucciones necesarias para que cualquier persona pueda instalar y usar cualquiera de las soluciones. En caso de que prefieras que un Ingeniero te visite con mucho gusto te podremos auxiliar con un cargo extra.

- **¿Qué es una cuenta? ¿Por qué una cuenta?**

  Es algo así como tu usuario y password (palabra clave) que se te asigna cuando adquieres el servicio, la misma cuenta puede ser empleada para los diferentes servicios como PC2P, D2P y puede ser empleada en cualquier lugar del mundo.

- **¿Cuales son los requerimientos mínimos para la solución de software o PC2P?**

  **Los requerimientos mínimos para PC2P son:**

  Pentium 266 MHz PC or higher

  32 MB RAM

  Windows 95/98/NT/2000/ME/XP

  Tarjeta de audio full duplex (la mayoría de las tarjetas son Full-Duplex)

  Micrófono y bocinas, o diadema.

  Conexión a Internet.

  Módem de 33.6 Kbps (para una mayor calidad de sonido recomendamos módem de 64 Kbps o superior)

  Descargar el software PC-to-Phone o Dialer.

- **¿VOIP es lo correcto para mi compañía?**

Todas las personas y empresas desde pequeñas hasta grandes corporativos que realicen llamadas de larga distancia frecuentemente, podrán ver ahorros reales de hasta el 80% a 90% en sus gastos telefónicos ya que típicamente cuentan con conexión a Internet y su volumen de llamadas puede ser enrutado utilizando el sistema VOIP.

- **¿Qué requiero para habilitar este servicio para mi Pequeña o Mediana empresa?**

  Si cuentas con un servicio de Internet de banda ancha (Por ejemplo Prodigy Infinitum, i-Go, Maxcom, conexión por cable, etc.) puedes adquirir un equipo Cisco ATA 186 con dos puertos para poder realizar dos llamadas simultaneas, adquirir una o dos cuentas y uno o dos teléfono(s) análogos y un nodo a tu red local Ethernet RJ-45, asignarle una dirección IP a tu dispositivo mediante DHCP o de forma manual y comenzar a ahorrar dinero.

  En resumen requieres de 5 elementos

  Conexión a Internet de banda ancha.

  Cuenta de usuario

  Nodo de red

  Dirección IP

Teléfono(s) análogo(s)

- **¿Qué condiciones de red afectan la calidad de la voz, o la calidad de las llamadas?**

  La calidad de VOIP esta sujeta a los siguientes condiciones de red durante las comunicaciones:

  Ancho de banda o Bandwidth – Cada llamada tiene su promedio y requerimientos mínimos de ancho de banda. Si el ancho de banda de la red IP no puede soportar los requerimientos mínimos, la calidad de la voz no será buena, o la voz se cortará. La red IP debe cumplir los requerimientos mínimos establecidos para mantener una llamada, para nuestro servicio 17kpbs por llamada es el mínimo requerido.

  Retraso o Delay – El retraso en la voz durante una llamada causará dificultad en la interacción entre las partes involucradas. Perdida de Paquetes o Packet Loss – Las redes IP separan grandes bloques de datos en bloques más pequeños llamados paquetes. Estos paquetes en cierto tiempo se perderán durante la transmisión, si hay retrasos en la red o su calidad es mala, la voz se distorsionará en el

destino debido a la perdida de dichos paquetes.

Fluctuaciones o Jitter – Si una red IP produce diferente latencia para distintos

- **¿Que tan seguras son las llamadas por este servicio ?**

  Incluso son más seguras que las llamadas telefónicas convencionales ya que la información viaja en forma de paquetes IP, y en ciertos casos la información viaja cifrada.

- **¿Puedo utilizar el servicio en otras plataformas como Mac OS, Linux, Unix, etc?**

  Puesto que es una tecnología independiente de PCs funciona sin importar que Sistema Operativo emplees actualmente.
  Para lo único que emplearías una PC es para ver tu saldo y/o registrarte y esto lo puedes realizar bajo cualquier plataforma ya que es a través de Internet.

# CONCLUSIONES

En cuanto a la implementación de esta solución sobre redes públicas tales como Internet, la solución es viable pero al no existir QOS el coste a asumir es muy elevado en cuanto a pérdidas de paquetes e inteligibilidad de las conversaciones. Por ello el mercado está situado en un compás de espera donde la urgencia mostrada por las organizaciones empresariales usuarias marcarán el ritmo de desarrollo e implantación de soluciones que garanticen QOS.

Según todas las fuentes consultadas, y las opiniones de especialistas en la materia, podemos concluir que VOIP se perfila como una de las tecnologías más prometedoras del momento. Probablemente el elevado costo que supondrá garantizar la calidad del servicio retrasará su implantación definitiva, pero en cuanto las diferencias políticas se eliminen y se implante IPv6, la telefonía tal y como la conocemos sufrirá un cambio radical. Solo habrá que esperar a los precios de las operadoras para utilizar sus gateways, y desear que no se excedan ya que esta situación podría retrasar la llegada al usuario de esta revolución tecnológica.

La competencia entre los ISP y operadores del mercado para la prestación de servicios de transmisión de voz significa un beneficio para el usuario final, quien a través de un servicio prestado en condiciones de mercado bajo la supervisión del Estado, podrá acceder a servicios cada vez más especializados, acorde con sus necesidades específicas y contratados a empresas colombianas y no exclusivamente o por lo menos en su gran mayoría a empresas extranjeras.

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).

En la actualidad VOIP soportada sobre Redes Privadas con un diseño adecuado es una solución totalmente viable y operativa. Las organizaciones empresariales muestran gran inquietud por su aplicación y su incorporación inmediata sobre Intranets es totalmente factible ya que se mejoran ostensiblemente los ratios establecidos por los parámetros Calidad/Precio. La solución actual implica diseño y optimización y combinación de las distintas herramientas y recursos disponibles en las propias organizaciones.

Cabe resaltar que existen dos aspectos muy relevantes que de momento constituyen la gran barrera para la llegada de la convergencia.: QOS aplicada a

VOIP y los aspectos legales a considerar. La implicación que estos aspectos tengan en el desarrollo de esta tecnología constituirán la base para la elaboración de próximos artículos que complementen al actual.

## RECOMENDACIONES

1. Empezar por la red WAN de la empresa (si la tiene), unificar en un mismo medio voz, datos y video por un mismo medio, nos da los beneficios de:

- Administrar un solo equipo (router)

- Aprovechar anchos de banda desperdiciados por la demanda de cada aplicación (voz, datos, video, etc.)

- Aprovechar anchos de banda por horarios, existen generalmente diferentes picos de demanda en cada aplicación (voz, datos, video, etc.)

- Eliminar costos de larga distancia y servicio medido

2. Adquisición de nueva infraestructura por crecimiento de nuevas necesidades se realiza ya en un ambiente de una red convergente, es decir, adquirir teléfonos IP, switches preparados para telefonía IP con calidad de servicio (QoS).

3. Sustitución tecnológica se va realizando en función de que el equipamiento está ya obsoleto o inservible.

4. Necesidades de seguridad en las conversaciones de voz, una llamada entre teléfonos IP, la voz está encriptada.

5. Reducción de pérdidas de información y conectividad que afectan los procesos productivos del negocio

6. Justificación basada en nuevas aplicaciones que aumentarán la productividad y rentabilidad del negocio.

Al final del proyecto, Usted tendrá una Red Convergente en el cual se justificó por los ahorros y beneficios que aportó a la empresa.

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).

# ANEXOS

**ANEXO A.** Laboratorio de conversación implementando una Red de datos con el Software Netmeeting.

## PRACTICA Nº1

### CONVERSACIÓN UTILIZANDO LA RED DE DATOS CON EL SOFTWARE NETMEETING (VoIP)

- Simular y experimentar una conversación de voz sobre IP utilizando como herramienta básica NetMeeting.

## EQUIPOS

- Micrófonos.
- Parlantes.
- Switches
- Routers
- Computadores para formar una red.

**CONCEPTOS PRELIMINARES**

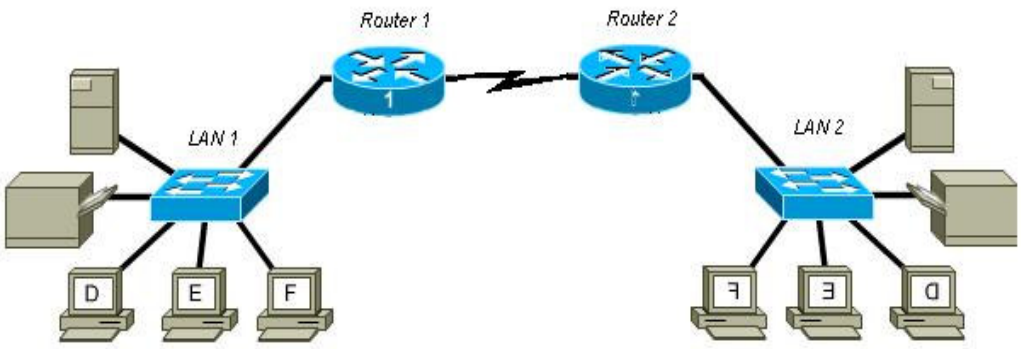
- Recursos VoIP, Disponible en internet como: www.recursosvoip.com

*PRELABORATORIO*

Utilizando el software de comunicación NetMeeting, desarrolle el procedimiento completo para utilizar las herramientas de comunicación que este nos ofrece.

**PROCEDIMIENTO**

1. **Crear la siguiente red o una parecida.**




- Se crean dos redes de área local para conectarlas cada una a un Router diferente emulando un enlace WAN.
- Se establece la configuración respectiva de la red y se verifica que existe conectividad en todos los puntos de la red.

- Se inicia una sesión con el NetMeeting en las redes de área local y se realizan las configuraciones pertinentes de audio (Altavoz y micrófono).
- Se realizan los ajustes correspondiente para establecer una llamada utilizando netmeeting.
- Se utiliza la dirección IP del host para establecer una llamada. Si no conoce la dirección IP del equipo utilice el comando Ipconfig en el símbolo del sistema.

NOTA: Se debe conocer la dirección IP del host destino para establecer la llamada.

- Comprobar que efectivamente se establece la llamada utilizando el micrófono multimedia y los altavoces

**ANÁLISIS E INTERPRETACIÓN DE RESULTADOS**

**CONCLUSIONES Y RECOMENDACIONES**

**ANEXO B.** Código 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 |

**ANEXO C.** auto evaluación VOIP

1. **La tecnología IP segmenta las transmisiones en**

1. celdas del mismo tamaño
2. paquetes del mismo número de bytes
3. celdas de distinto tamaño
4. paquetes de distinto tamaño

2. **Los componentes principales de una red de voz sobre paquetes son: la pasarela de medios y señalización, el controlador de pasarelas y ..**

1. servidor de aplicaciones
2. servidor de llamadas
3. enrutador de llamadas

3. **Para VOIP se utiliza el protocolo UDP porque**

    1. es seguro
    2. es fiable

3. está orientado a conexión

4. no retransmite los datos en caso de pérdida de paquetes

**4. La evolución de la VOIP tiende a**

1. suprimir la red telefónica convencional de conmutación de circuitos (RTPC)

2. suprimir la señalización (SS7)

3. proporcionar servicios IP de valor agregado

5. **El softswitch debe tener la capacidad de realizar las funciones de una central de conmutación**

1. solo de paquetes

2. solo de circuitos

3. ambas funciones

6. **En la arquitectura H.323, el servicio de control de llamadas lo proporciona**

1. el terminal

2. la pasarela

3. el gatekeeper

4. el MCU

7. **La negociación de capacidades y canales de audio/video se realiza por medio del protocolo**

   1. H.245correcto

   2. H.225

   3. Q.931

   4. RAS

8. **El gatekeeper realiza la función de**

   1. Conversión de medios

   2. Establecimiento y terminación de llamadas

   3. Encaminamiento mediante traducción de direccionescorrecto

9. **¿A partir de que retardo comienza a ser molesta la audición?**

   1. 100 ms

   2. 250 ms

   3. 350 ms

10. **Para una efectiva conversación en telefonía IP, la pérdida de paquetes no debería superar el**

    1. 5%
    2. 10%
    3. 15%

11. **Los codec de voz suponen un compromiso entre compresión-calidad percibida. ¿Cual cree que se oirá con mayor claridad?**

    1. G.711
    2. G.723.1
    3. G.728

12. **¿Cual de estos protocolos interviene en el establecimiento de una llamada H.323?**

    1. Q.931
    2. H.248
    3. G.722

13. **El pasado año, segun Telegeography el tráfico de VoIP entre EEUU e Iberoamérica**

    1. No fue significativo (<10% de penetración)
    2. Fue similar al tráfico de telefonía convencional.
    3. Fué bastante superior al tráfico de telefonía convencional.

14. **Una consideración para regular la VOIP es la QOS. ¿Que considera la rec. G.144 como calidad aceptable para la mayoría?**

    1. Eco menor de 200 ms
    2. Pérdida de paquetes <10%
    3. Retardo menor de 150 ms
    4. Pérdida de paquetes menor del 5%

15. **Las redes locales inalámbricas (WLAN) permitirían acceder a un nodo alrededor de**

    1. 10 usuarios de VOIP
    2. 20 usuarios de VOIP
    3. 40 usuarios de VOIP

16. **Las llamadas VOIP inalámbricas están limitadas por**

    1. Cobertura en el interior de un recinto
    2. En entornos cerrados (aeropuertos, hoteles...)
    3. El nº de usuarios simultáneos

**Responda falso o verdadero a las siguientes 7 preguntas**

17. **H.323 especifica que las puntos finales H.323 deben apoyar el vídeo?**

    1. verdad
    2. . falso

18. **Una zona H.323 es controlada por unos o más porteros.?**

    1. verdad
    2. falso

19. **La recomendación G.723.1 especifica la codificación audio en un índice de 16 kbps.?**

    1. verdad
    2. falso

**20. Un portero es un componente esencial de una red H.323.?**

1. verdad
2. falso

**21. Las puntos finales H.323 utilizan protocolo de RAS para descubrir a su portero.**

1. verdad
2. b. falso

**22. Las puntos finales H.323 utilizan H.225 para establecer los canales de los medios.?**

1. verdad
2. falso

**23. Todas las llamadas H.323 son señaladas encaminando a través de un portero.?**

1. verdad
2. falso

24. **Una zona H.323 puede atravesar a través de redes múltiples.?**

    1. verdad
    2. falso

**Escoja la respuesta que completa la frase en forma correcta**

17. **RAS se puede definir como** _____.

    a. control de la corriente de los medios

    b. controle señalar

    c. el señalar de llamada

    d. transporte de la corriente de los medios

    e. registro y admisión

26. **H.225 se puede definir como** _____.

    a. control de la corriente de los medios

    b. controle señalar

    c. el señalar de llamada

    d. transporte de la corriente de los medios

    e. registro y admisión

**27. H.245 se puede definir como _____.**

a. control de la corriente de los medios

b. controle señalar

c. el señalar de llamada

d. transporte de la corriente de los medios

e. registro y admisión

**29. H.323 se puede definir como _____.**

a. servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios de los multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

**30. H.320 se puede definir como _____.**

a. servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios d e los

multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

**30. H.321 se puede definir como _____.**

a. servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios de los multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

**31. H.322 se puede definir como _____.**

a. servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios de los multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

**33. H.324 se puede definir como _____.**

a. servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios de los multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

**34. H.310 se puede definir como _____.**

servicios B-b-isdn excesivo de los multimedia

b. redes garantizadas excedente de QoS de los servicios de los multimedia

c. redes excesivas del paquete de los servicios de los multimedia

d. servicios SCN excesivo de los multimedia

e. servicios ISDN excesivo de los multimedia

## REFEENCIAS BIBLIOGRAFICAS

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”

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".

DOUSKALIS, B. (2000). IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR

GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol Architecture and Requeriments. RFC 2805, Abril 2000.

HAMDI, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P. (Mayo, 1999).Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999, pags. 104-111.

**ENLACES A PAGINAS RELACIONADAS CON VOIP**

http://www.nortelnetworks.com

http://www.iec.org

( Consolidación internacional de ingeniería)

http://www.skype.com/intl/es

(comienza a realizar llamadas gratuitas a todo el mundo)

http://www.microsoft.com/catalog/display.asp

(pagina oficial netmmeting, te muestra que es , como funciona,

instalación, requisitos para el netmeeting)


http://www.cisco.com

( uno de los mas grandes provedores de hardware y software a nivel mundial)


www.alcatel.es

(fabricante de hardware y software para protocolos de comunicaciones)


http://www.sipcenter.org

(SIP Center)