UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"SISTEMA DE TELEFONIA IP"

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JESÚS MARCOS FERNÁNDEZ SOLÓRZANO

PROMOCIÓN 1987-1

LIMA-PERÚ
2003

Dedico este trabajo a mis Padres quienes en todo momento me apoyaron durante mi vida universitaria así como en la conclusión del presente informe.

A mis hermanos por su constante aliento.

Y a mi esposa e hijo, quienes son la razón de mi existencia.

SISTEMA DE TELEFONÍA IP

SUMARIO

Actualmente el sector Telecomunicaciones viene presentando un impresionante dinamismo, que es impulsado por los efectos de la globalización, así como, las innovaciones tecnológicas, por lo que emerge como una estrategia competitiva la implantación de redes públicas que brinden los servicios de voz y datos sobre el protocolo Internet (IP).

En el Perú, las redes de conmutación interconectadas entre sí, representan una gran inversión de equipamiento, facilidades y sistemas de soporte. Es muy probable que en los próximos años, el tráfico de voz sea transportado sobre redes híbridas (Conmutación de circuitos y de paquetes).

En este entorno, Telefónica del Perú (TDP) viene desarrollando estudios para la implementación de Redes de Nueva Generación (NGN) a fin de reforzar su posición como uno de los principales protagonistas en el mercado de las Telecomunicaciones.

El presente informe explica los conceptos sobre la integración del tráfico de voz en las redes de datos, así como, la descripción detallada del funcionamiento y equipamiento de 4 nodos instalados en los locales de TDP: Miraflores, Washington, Arequipa y Trujillo, los cuales están basados en redes de Nueva Generación de 3Com y estuvieron en calidad de prueba durante los meses de abril y marzo del 2001.

INDICE

CAPITULO III

PROLOGO

La convergencia de los servicios telefónicos en las redes de datos está marcando el inicio de la unificación de los principales servicios en una sola red, además de la facilidad para el Operador de gestionar todos sus recursos desde una sola Plataforma. Por lo que transmitir voz sobre una red de paquetes IP unificada es la clave para la convergencia de datos y telefonía.

Esta nueva tecnología, cuyo origen se remonta muchos años atrás, ha cobrado gran importancia en los últimos años, dando lugar a grandes esfuerzos e inversiones que, sin duda, van a revolucionar las redes telefónicas y sobre todo, los servicios y aplicaciones que éstas nos ofrecen.

Tradicionalmente los servicios de telefonía y de datos han estado soportados por redes distintas basadas en tecnologías diferentes. Para el transporte del tráfico de voz se han utilizado hasta ahora redes telefónicas clásicas, basadas en las técnicas de conmutación de circuitos, las cuales están adaptadas a las características del tráfico de voz, en el que se asignan recursos de manera dedicada para cada comunicación en curso, tales como la capacidad o ancho de banda en los enlaces y capacidad de proceso en los nodos de la red.

Por el contrario, el tráfico de datos generado por las aplicaciones telemáticas, se caracteriza en general por su falta de continuidad «tráfico a

ráfagas». Es por ello que en las técnicas de conmutación de paquetes, la información a transmitir se divide en paquetes ó datagramas, los cuales se transmiten generalmente sin que exista una reserva previa de recursos.

Las ventajas que ofrece la convergencia de redes han sido desde un principio de índole económica. Debido a que las tecnologías como VoIP utilizan eficientemente el ancho de banda de las redes, permitiendo reducir los 64 kbits/s utilizados en cada conversación telefónica en las redes clásicas, además del importante ahorro en los costes de gestión y operación que se consigue por el hecho de utilizar una sola red para ambos servicios.

Sin embargo, no solo son las razones económicas las que justifican el interés e inversiones para converger las redes de voz y datos. Según coinciden los expertos, la principal razón de esta tendencia son las Aplicaciones, como la Mensajería Unificada, que permitirá englobar bajo un único interfaz de usuario siendo accesible desde cualquier parte de la red, a todos los servicios a través de los cuales recibimos mensajes (correo electrónico, fax, teléfonos, contestadores, etc).

Como se observa son muchos los retos que plantea la introducción de la tecnología VoIP, sobre todo si tenemos en cuenta que va a sustituir a otra tecnología que ha alcanzado un nivel de madurez y fiabilidad muy alto.

Entre estos retos podemos citar:

Calidad de Servicio (QoS). Es conocido el problema que presentan las redes IP a la hora de garantizar un cierto nivel de calidad de servicio a una determinada comunicación, a diferencia de las redes telefónicas, que reservan y garantizan los recursos a cada llamada. No obstante los

grandes esfuerzos que se invierten en la definición de modelos de QoS, todavía no se ha alcanzado una solución global que permita crear una Internet con QoS. Mientras este modelo no exista, VoIP estará acotada a las redes IP privadas o a las redes sobredimensionadas.

Fiabilidad. Las tecnologías empleadas en las redes telefónicas actuales presentan una fiabilidad muy alta: a menudo se hace referencia a los «cinco nueves» al hablar de ella (esto es, al 99,999%, lo que significa unos pocos segundos de mal funcionamiento al año). Las tecnologías utilizadas en Internet y, en particular, las creadas alrededor de VoIP, están todavía lejos de alcanzar esas cifras.

Seguridad. Como es conocido, la seguridad que ofrecen las redes IP y, en particular, la Internet es deficiente en algunos aspectos. Ataques del tipo «denegación de servicio» o posibles violaciones de la confidencialidad de las conversaciones son, entre otros, aspectos a mejorar si se quiere hacer un uso global de VoIP. Este aspecto es clave, sobre todo, si se piensa que el principal escenario de aplicación de VoIP son las redes corporativas.

Tarificación. Los operadores de telefonía tradicional basan sus ingresos en la contabilidad de llamadas realizadas por cada usuario y la tarificación que realizan de las mismas. Los esquemas de costes utilizados en Internet son radicalmente distintos; de hecho, el término «coste plano» o «tarifa plana» se ha popularizado sin duda gracias a ella. Por lo que se hace necesario armonizar ambos esquemas para adaptarlos a los nuevos escenarios.

Recursos Humanos. La universalidad y calidad del servicio telefónico actual descansa sobre un equipo de técnicos formados en las tecnologías de conmutación de circuitos. La transición hacia VoIP exigirá prestar atención a la formación y reconversión de este personal.

Para la elaboración del presente trabajo se han considerado los siguientes capítulos:

Capítulo I : En este capítulo se hace una introducción teórica al mundo de IP, así mismo, se explica el modelo de referencia OSI y los elementos de diseño de una red VoIP.

Capítulo II : En este capítulo se explica los protocolos de señalización H.323 y SIP utilizado en redes IP.

Capítulo III : En este capítulo se realiza una descripción detallada del funcionamiento y equipamiento de 4 nodos instalados en los locales de Telefónica del Perú: Miraflores, Washington, Arequipa y Trujillo, los cuales están basados en redes de Nueva Generación de 3Com.

CAPITULO I
CONCEPTOS BASICOS - VoIP

1.1. Introducción

Muchas de las ventajas de la Voz sobre IP (VoIP) vienen del uso Protocolo Internet (IP) como mecanismo de transporte. Para entender realmente esos beneficios, se debe entender en primer lugar qué significa realmente IP.

Antes de que se entienda que puede hacer IP y de qué manera se pueden ejecutar aplicaciones a través del IP, es necesario familiarizarse con el modelo de referencia de *Internetworking* de sistemas abiertos. (OSI, *Open Systems Interconnection*) y cómo se aplica a IP.

1. 2 Modelo de referencia OSI

La Organización internacional para la normalización (ISO, *Internacional Organization for Standardization*) desarrolló el modelo de referencia OSI a principios de los años ochenta, el cual se ha convertido en el estándar para desarrollar protocolos que permiten que las computadoras se comuniquen. Aunque no todos los protocolos siguen este modelo, mucha gente lo utiliza para desarrollar y enseñar nuevos protocolos.

El modelo de referencia OSI fragmenta el problema de la comunicación entre máquinas en siete capas. Cada capa se ocupa sólo de hablar con su correspondiente capa situada en la siguiente máquina (véase la Figura 1.1). Esto significa que la Capa 5 sólo se tiene que preocupar de hablar con la capa 5 de la máquina receptora y no sobre cuál puede ser el medio físico real.

Además, cada capa del modelo de referencia OSI proporciona servicios a la capa que está por encima de ella (Capa 5 a la Capa 6, Capa 6 a la Capa 7, etc.) y solicita determinados servicios de la capa directamente por debajo (5 a 4, 4 a 3, etc.).

Esta propuesta por capas permite que cada una de ellas maneje una pequeña pieza de información, realice cualquier cambio que sea necesario a los datos y agregue las funciones necesarias para esa capa antes de hacer pasar los datos. Los datos dejan de parecerse a datos humanos para parecerse más a datos de máquinas conforme van recorriendo el modelo de referencia OSI hasta convertirse en 1 y 0 (Impulsos eléctricos) en la capa física. La Figura 1.1 muestra el modelo de referencia OSI.

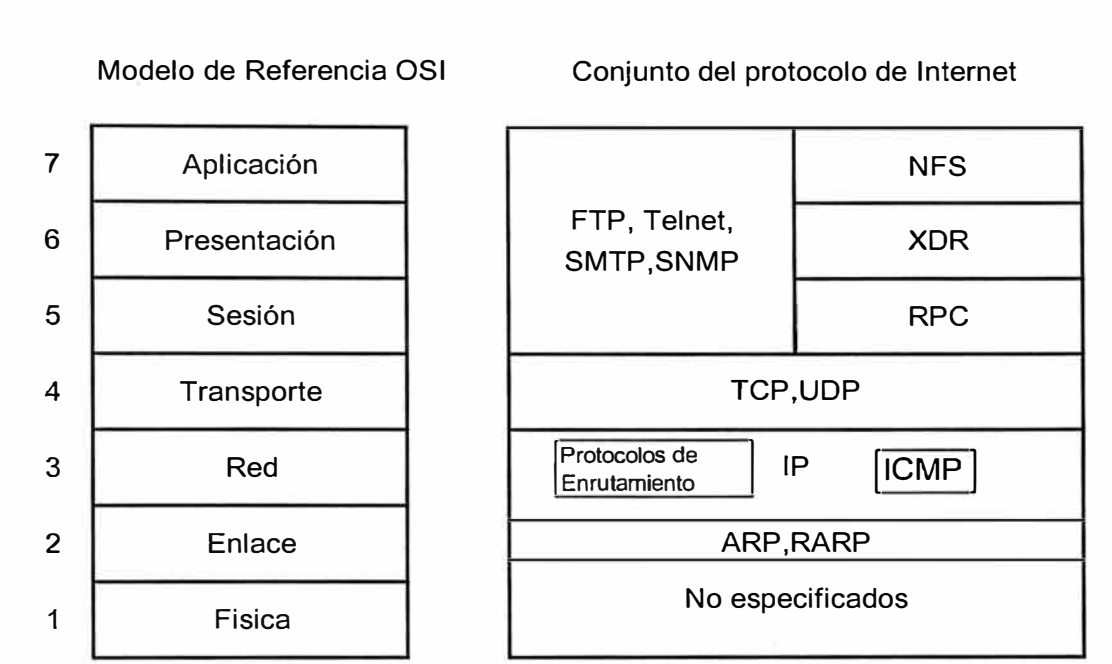


Figura 1.1 Modelo de referencia OSI.

A continuación explicaremos el funcionamiento de las capas de aplicación, presentación, sesión, transporte, red, enlace de datos y física.

1.2.1 La capa de Aplicación

La mayoría de los usuarios están familiarizados con la capa de aplicación. Algunas aplicaciones bien conocidas incluyen.

- Correo electrónico
- Navegador web.
- Procesador de textos.

1.2.2 La capa de Presentación

La capa de presentación garantiza que la información enviada por la capa de aplicación de un sistema es legible por la capa de aplicación del otro sistema.

La capa de presentación se ocupa no sólo del formato y representación de los datos de usuario, sino también de las estructuras de datos utilizadas por los programas. Por tanto, además de la transformación de formatos de datos (si fuera necesaria), la capa de presentación negocia la sintaxis de transferencia de datos para la capa de aplicación.

1.2.3 La capa de Sesión

Como su nombre implica, la capa de sesión establece, administra y termina sesiones entre aplicaciones. Las sesiones consisten en el diálogo entre dos o más entidades de presentación.

La capa de sesión sincroniza los diálogos entre las entidades de la capa de presentación y administra su intercambio de datos. Además de la regulación básica de las conversaciones (sesiones), la capa de sesión ofrece provisiones para la expedición de datos, clase de servicio (a través del uso de los bits de tipo de servicio [Tos]) y registro de los problemas de la capa de sesión, la capa de presentación y la capa de aplicación.

1.2.4 La capa de Transporte

La capa de transporte es responsable de asegurar un transporte de datos fiable en un *internetworking*. Esto se lleva a cabo mediante el control del flujo, la verificación de errores (suma de comprobación), la confirmación de extremo, la retransmisión y la secuenciación de datos.

Algunas capas de transporte, como el Protocolo para el control de la transmisión (TCP, *Transmisión Control Protocol*), tiene mecanismos para manejar la congestión. El TCP ajusta su temporizador de retransmisión cuando hay congestión o se pierden paquetes dentro de una red. TCP rebaja la cantidad de tráfico que envía cuando hay congestión. La congestión viene determinada porque no se reciben acuses de recibo desde el nodo de destino.

1.2.5. La capa de Red

La capa de red proporciona la dirección lógica que permite que dos sistemas dispares que se encuentran en redes lógicas diferentes determinen una posible ruta para comunicarse. La capa de red es la capa en la que residen los protocolos de enrutamiento.

En Internet, la dirección IP es de lejos el esquema de dirección más utilizado. Los protocolos de enrutamiento, como el Protocolo EIGRP (*Enhanced Interior Gateway Routing Protocol*, o IGRP mejorado), Primero la ruta libre más corta (OSPF, *Open Shortest Path First*), Protocolo de *gateway* fronterizo (BGP, *Border Gateway Protocol*), Sistema intermedio-sistema intermedio (IS-IS, *Intermediary System to Intermediary System*), y otros muchos, se utilizan para determinar las rutas entre dos subredes lógicas.

Los *routers* tradicionales enrutan los paquetes IP sobre la base de su dirección de la capa de red.

Entre las funciones claves de la capa de red se encuentran las siguientes.

- Formateo de paquetes, direccionamiento de redes y *hosts*, resolución de direcciones y enrutamiento.
- Creación y mantenimiento de tablas de enrutamiento.

1.2.6. La capa de enlace de datos

La capa de enlace de datos proporciona un transporte fiable a través de un enlace físico. La capa de enlace tiene su propio esquema de direcciones. Este esquema se ocupa de la conectividad física y puede transportar tramas sobre la base de la dirección de la capa de enlace.

Los *switches* tradicionales Ethernet conmutan el tráfico de red sobre la base de la dirección de la capa de enlace (Capa 2). Conmutar tráfico sobre la base de la dirección de la Capa 2 se conoce como *bridging* (puentear). De hecho, un *switch* Ethernet no es más que un puente de alta velocidad con múltiples interfaces.

1.2.7. La capa Física

La capa física se ocupa de crear “unos” y “ceros” en el medio físico con cambios de impulsos/voltaje eléctrico. Entre las especificaciones de comunicación comunes de la capa física se encuentran las siguientes:

- EIA/TIA-232. Especificación de la Asociación de industrias electrónicas/ Asociación de la industria de las telecomunicaciones (*Electrical Industries Association /*

Telecommunications Industry Asociation) utilizada para comunicar dispositivos de computadora. Se pueden utilizar diferentes conectores; esta interfaz se usa a menudo para conectar computadoras a módems.

- V.35. Mecanismo del sector de la normalización de las telecomunicaciones de la Unión internacional de las telecomunicaciones (ITU-T, *Internacional Telecommunication Union Telecommunication Standardization Sector*) que define la velocidad de señalización desde 19,2 Kbps a 1,544 Mbps. Esta interfaz física tiene un conector de 34 pines y es también conocido como un *Winchester Block*.
- RS-449, Utiliza 37 pines y es capaz de ir más allá que el RS-232.

1.3. Protocolo Internet

El Protocolo Internet (IP) es un protocolo no orientado a la conexión que reside en la Capa 3 (la capa de red), lo que significa que no hay ningún mecanismo de habilidad, control de flujo, secuenciación o reconocimiento. Otros protocolos, como el TCP, se pueden alojar en la parte superior del IP (Capa 4, sesión) y pueden agregar control del flujo, secuenciación y otras características.

Dada la posición de IP en el modelo de referencia OSI, no tiene que tratar con problemas de enlace de datos comunes como Ethernet, el Modo de transferencia asíncrona (ATM), Frame Relay

y Token Ring, o con cuestiones físicas como la Red óptica síncrona (SONET, *Synchronous Optical Network*), el cobre y la fibra óptica. Esto permite la difusión de IP.

Se puede ejecutar IP en una casa u oficina a través de cualquier medio necesario (por ejemplo, inalámbrico, banda amplia o banda base) esto no significa que cuando se diseña una red se puedan ignorar las dos capas inferiores. Únicamente significa que son independientes de las aplicaciones que se trabajen con IP.

IP está considerado como un protocolo *bursty* (ráfagas), lo que significa que las aplicaciones que residen por encima de IP experimentan largos periodos de silencio, seguidos de la necesidad de una gran porción de ancho de banda. Un buen ejemplo de esto es el correo electrónico. Si se configura el paquete de correo para descargar correo electrónico cada 20 minutos, existen unos 20 minutos de silencio durante los cuales no se necesita el ancho de banda.

Una de las mayores ventajas de IP es la posibilidad de escribir una aplicación una vez y tenerla para todo un conjunto de tipos de medios en cualquier sitio, independientemente de si esto ocurre a través de una conexión de línea de abonado digital (DSL) en casa, o una línea T1 en el trabajo.

Se puede transmitir un paquete IP de tres maneras generales a través de mecanismos de unidifusión, multidifusión o difusión. Explicados brevemente, estos mecanismos proporcionan los

medios para que cada paquete IP sea etiquetado con una dirección de destino, siéndolo cada una de ellas de una manera única:

- La unidifusión es muy simple porque solo identifica una dirección específica y únicamente ese nodo envía el paquete a las capas superiores del modelo de referencia OSI.
- Los paquetes de difusión son enviados a todos los usuarios en una subred local. Las difusiones pueden atravesar puentes y *switches*, pero no son pasadas a través de *routers* (a menos que estén configurados para hacerlos)
- Los paquetes de multidifusión utilizan una gama especial de direcciones que permite a un grupo de usuarios que se encuentran en subredes diferentes recibir el mismo flujo. Esto permite que el remitente envíe sólo un paquete que podrán recibir distintos *host* dispares.

Los paquetes de unidifusión, difusión y multidifusión tienen cada uno un propósito significativo. Los paquetes de difusión permiten que dos estaciones se comuniquen con independencia de su ubicación física. Los paquetes de difusión se utilizan para comunicarse con todo aquél que se encuentre en una subred simultáneamente. Los paquetes de multidifusión permiten aplicaciones, como la videoconferencia, que tienen un transmisor y múltiples receptores.

Independientemente del tipo de paquete IP que se utilice, siempre se necesita direccionar la capa de enlaces de datos.

1.4. Direcciones de la capa de enlace

Los dos tipos de direcciones son la dirección de la capa de enlace y la dirección de la capa red. Las direcciones de la capa de enlace de datos, también conocidas como Control de acceso al medio (MAC, *Media Access Control*), y las direcciones de la capa física son únicas para cada dispositivo. Por ejemplo, en una red de una área local (LAN), cada dispositivo tiene una dirección MAC que se identifica a sí misma en la LAN. Esto permite que las computadoras sepan quién está enviando el mensaje. Si se mira atentamente una trama Ethernet, los 12 primeros bytes son las direcciones MAC de origen y destino.

Si se utiliza un *switch* Ethernet LAN, el tráfico es enrutado a través del *switch* sobre la base de la dirección de la capa de enlace de enlace de datos (la dirección MAC). Si se utiliza un repetidor o *hub*, para conectar los dispositivos a la LAN, el paquete es transmitido a todos los puertos, con independencia de la dirección MAC. Esto es así porque el envío a través de un *hub* se hace sobre la base de una capa física y no sobre la capa de enlace de datos.

Cuando el tráfico es enrutado sobre la base de la dirección de capa MAC, se dice que ha sido **conmutado** o **puenteado**. Antes de que el enrutamiento se hiciera prominente a finales de los años ochenta, muchas compañías desarrollaron puentes para conectar dos redes dispares. Esto permitía conectar dos redes en la capa

de enlaces de datos con un método simple y barato. Sin embargo, como esos puentes no miraban la dirección de capa de red, también se podía transmitir por ese puente tráfico no deseado como difusiones o multidifusiones, lo que consumía una gran cantidad de ancho de banda.

La mayoría de las LAN en los años ochenta y principios de los noventa utilizaban un *hub* para conectar su estaciones de trabajo Ethernet. Este dispositivo se conocía como **repetidor** y solo duplicaba la información de la Capa 1. Por tanto, si una corporación tenía un *hub* de ocho puertos y uno de los puertos recibía un paquete, ese paquete sería repetido (los errores y todo) hacia los otros siete puertos.

A principios de los años noventa, las compañías empezaron a desarrollar *switches* de LAN, que eran básicamente una combinación de un *hub* y un puente. En estas circunstancias, el *switch* de LAN aprendió que direcciones de la Capa 2 eran enlazadas con cada uno de sus interfaces físicas y el tráfico transmitido sobre la base de la dirección de la Capa 2. Si el *switch* no tenía una lista de una dirección de la Capa 2 de destino en su tabla de switching, o si el paquete era un paquete de difusión, el paquete era repetido en todas las demás interfaces del *switch*.

Esta transición a los *switches* de red permitió que las redes hicieran un mejor uso de ancho de banda disponible. Este ahorro en el ancho de banda se realizaba impidiendo que paquetes IP

innecesarios fueran transmitidos en un puerto físico donde no residía el dispositivo receptor.

1.5. Direcciones IP

De todos los esquemas de direcciones, la dirección IP es la más importante de entender porque se debe comprender conceptualmente cómo se comunican esos dispositivos para construir redes de manera efectiva en la parte superior de una infraestructura de IP.

Existen muchos protocolos y cada uno de ellos tiene un esquema de direcciones diferentes.

La dirección de la capa de red normalmente es jerárquica. Mirando la Red pública de telefonía conmutada (PSTN, *Public Switched Telephone Network*) en la North American Numbering Plan Associaton (NANPA), cada área de plan de numeración (NPA, *Numbering Plan Area*) incluye una región, con un prefijo (Nxx) que denota una subregión y un identificador (xxxx) de estación que denota el teléfono real.

La dirección de capa de red descansa en la Capa 3 del modelo OSI. Esto permite que un grupo de computadoras reciba direcciones lógicas similares. El direccionamiento lógico es similar a determinar la dirección de una persona mirando su dirección de país, estado, código postal, ciudad y calle.

Los *routers* transmiten el tráfico sobre la base de la Capa 3, o dirección de la capa de red. La dirección IP soporta cinco clases

de red. Los bits que se encuentran más a la izquierda indican la clase de red, de la siguiente manera:

- Las redes de Clase A están principalmente destinadas con una pocas redes grandes ya que proporcionan sólo siete bits para el campo de dirección de red.
- Las redes de Clase B alojan 14 bits para el campo de dirección de red y 16 bits para el campo de dirección de *host*. Esta clase de direcciones ofrece un buen equilibrio entre el espacio de direcciones de red y de *host*.
- Las redes de Clase C. alojan 21 bits para el campo de dirección de red. Sin embargo, sólo proporcionan 8 bits para el campo de *host*, por lo que el número de *host* por red puede ser un factor de limitación.
- Las direcciones de Clase D están reservadas para grupos de difusión, como se describe en la petición de comentarios (RFC) 1112. En las direcciones de Clase D, los cuatro bits más altos definidos por 1,1,1 y 0.
- Las direcciones de Clase E también están definidas por IP, están reservadas para su utilización futura. En las direcciones de Clase E los cuatro bits superiores están definidos por 1 y el quinto bit es siempre 0.

Las direcciones IP están escritas en un formato llamado decimal, por ejemplo, 121.10.3.116. La Figura 1.2 muestra los formatos de dirección para redes IP A, B y C. Una manera fácil de

pensar en las clases de direcciones es que cuantas más redes se tengan menos *hosts* puede haber en esa red.

Las redes IP también se pueden dividir en pequeñas unidades llamadas **subredes.** Las subredes proporcionan una flexibilidad adicional a los administradores de la red.

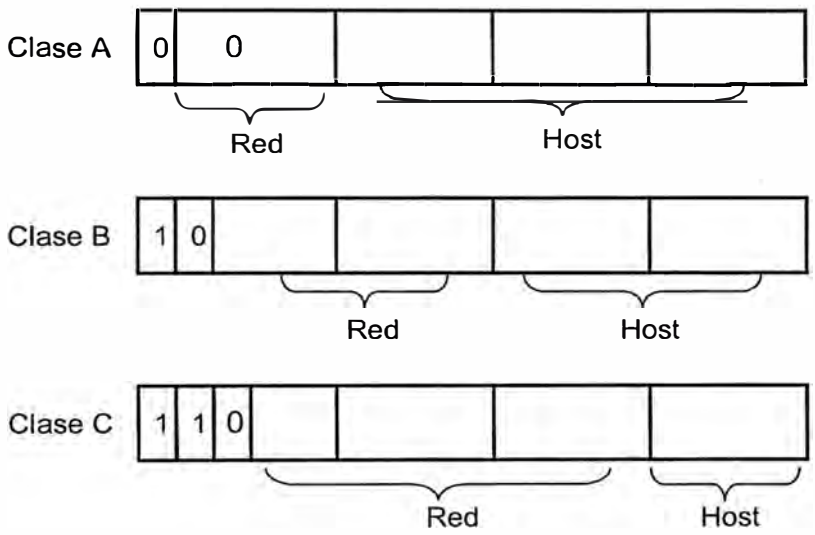


Figura 1.2. Formatos de dirección de Clase A, B y C.

El lugar de cambiar todas las direcciones a algún otro número de red básico, el administrador puede subdividir la red utilizando las subredes. Puede tomar bits de la parte de *host* de la dirección y utilizarlos como un campo de subred, como muestra la Figura 1.3.

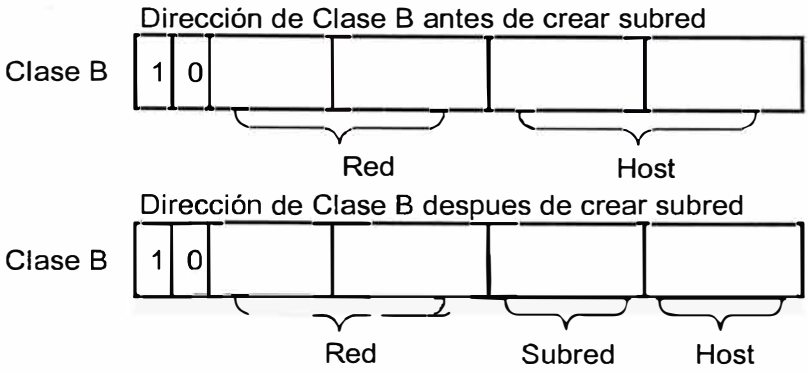


Figura 1.3. Subred de una dirección de clase A.

1.6. Protocolos de Enrutamiento

IP es un protocolo enrutado. Un protocolo enrutado es un paquete que transporta datos. Se diferencia de un protocolo de enrutamiento en que éste actualiza los *routers* para permitirles saber qué ruta deberá recorrer un paquete.

Actualmente, las redes IP utilizan dos tipos de protocolos de enrutamiento principales: el enrutamiento por vector de distancia y el enrutamiento por estado de enlace. Dentro de estos dos protocolos de enrutamiento se hallan protocolos de enrutamiento exteriores e interiores. El enrutamiento por **vector de distancia** se preocupa por el número de saltos (*routers*), mientras que el enrutamiento por estado de enlace se preocupa principalmente del estado de las interfaces que el *router* soporta (de ahí su nombre **estado de enlace**).

Los protocolos de enrutamiento interiores se utilizan para actualizar los *routers* bajo el control de una autoridad administrativa (sistema autónomo). Los protocolos de enrutamiento

exteriores se utilizan para permitir que redes que se encuentran en diferentes sistemas autónomos pasen actualizaciones de enrutamiento. Un buen ejemplo de un protocolo de enrutamiento exterior es el uso de BGP en Internet.

1.6.1. Enrutamiento por Vector distancia

El enrutamiento por vector de distancia es un algoritmo que los *routers* utilizan para poder elegir la mejor ruta. Este algoritmo utiliza el menor número de saltos (cada *router* es un salto) para determinar la mejor ruta hasta el destino.

Las difusiones se envían periódicamente para actualizar *routers* adyacentes. Cuando el *router* empieza a difundir actualizaciones, incluye todas las redes alcanzables que están directamente conectadas. Las rutas que son recibidas por un *router* se guardan en una tabla de enrutamiento, que es utilizada para transmitir paquetes.

Este método consume mucho ancho de banda porque la totalidad de la actualización del enrutamiento es enviada periódicamente (normalmente, cada 30 segundos).

1.6.2. Enrutamiento por estado de enlace

El enrutamiento por estado de enlace se distingue del enrutamiento por vector de distancia en que el primero transmite actualizaciones del enrutamiento sólo cuando cambia el estado de una interfaz. Esto significa que únicamente se envía tráfico y se consume ancho de banda cuando cambia una interfaz.

1.6.3. BGP

BGP (Protocolo de *Gateway* fronterizo) realiza enrutamiento entre dominios en las redes de Protocolo para el control de la transmisión/Protocolo Internet (TCP/IP, *Transmisión Control Protocol/Internet Protocol*). BGP es un protocolo de gateway exterior (EGP, *Exterior Gateway Protocolo*), lo que significa que realiza el enrutamiento entre múltiples sistemas autónomos e intercambia información sobre alcanzabilidad y enrutamiento con otros sistemas BGP.

BGP fue desarrollado para sustituir a su predecesor, el ahora obsoleto Protocolo de *gateway* exterior (EGP), como el protocolo de enrutamiento de *gateway* exterior estándar utilizado de manera global en Internet. BGP resuelve serios problemas que había con el Protocolo de *gateway* exterior y se adapta al crecimiento de Internet de manera más eficaz.

1.6.4. IS – IS

IS-IS es un protocolo de enrutamiento jerárquico por estado de enlace OSI. Circula por la red con información sobre el estado de enlace para construir una imagen completa y coherente de la topología de la red.

Para simplificar el diseño y operación del *router*, el IS-IS distingue entre los servicios de información (IS) de Capa 1 y de Capa 2:

- El servicio de información (IS) de Capa 1 se comunica con otros IS's de Capa 1 en la misma área.
- El servicio de información de Capa 2 enruta entre las áreas de Capa 1 y forma una *backbone* de enrutamiento entre dominios.

El enrutamiento jerárquico simplifica el diseño de la *backbone*, porque los servicios de información de Capa 1 sólo necesitan saber cómo llegar al servicio de información de Capa 2 más próximo. El protocolo de enrutamiento de *backbone* puede también cambiar sin tener ningún impacto en el protocolo de enrutamiento de área lógica.

1.6.5. OSPF

OSPF (Primero la ruta libre más corta) es un protocolo IGRP de estado de enlace. Fue diseñado para operar en las redes TCP/IP y subsanar los puntos débiles del Protocolo de información de enrutamiento (RIP, *Router Information Protocol*).

OSPF se derivó de una serie de fuentes, incluido el algoritmo Primero la ruta más corta (SPF, *shortest path first*) desarrollado por Bolt, Beranek and Newman, Inc. (BBN), una versión inicial del Protocolo de enrutamiento OSI IS-IS y otros esfuerzos de investigación.

1.6.6. IGRP

IGRP es un protocolo robusto para enrutamiento dentro de un sistema autónomo que tiene una topología arbitrariamente

compleja y que consiste en medios de diversos ancho de banda y características de retraso.

Cisco Systems desarrolló IGRP a mediados de los años ochenta. Es un protocolo de *gateway* interior por vector de distancia que utiliza una combinación de métricas para tomar decisiones de enrutamiento.

1.6.7. EIGRP

EIGRP (IGRP mejorado) es una versión mejorada del IGRP desarrollado por Cisco Systems, asimismo utiliza el mismo algoritmo por vector de distancia e información de distancia que IGRP. Las propiedades de convergencia y la eficacia operativa de EIGRP son significativamente mejores que las de IGRP.

EIGRP es protocolo IGP por vector de distancia que tiene las siguientes características:

- Utiliza una combinación de métricas para tomar decisiones de enrutamiento.
- Utiliza el Algoritmo de actualización de difusión(DUAL,*Diffusing Update Algorithm*) para permitir que las rutas converjan rápidamente.
- Envía actualizaciones parciales de las tablas de enrutamiento.
- Implementa un mecanismo de descubrimiento del router vecino.

1.6.8. RIP

RIP (Protocolo de información de enrutamiento) es un protocolo por vector de distancia que utiliza el número de saltos

como métrica. RIP es un IGP; realiza enrutamiento en el interior de un único sistema autónomo.

1.7. Mecanismos de transporte IP.

TCP y el Protocolo de datagrama de usuario (UDP, *User Datagram Protocol*) tienen funciones que pueden utilizar varias aplicaciones. Por ejemplo, si la fiabilidad es más importante que el retraso, se puede utilizar TCP/IP para garantizar la entrega de paquetes. Sin embargo, UDP/IP no utiliza la retransmisión de paquetes. Esto puede disminuir la fiabilidad, pero en algunos casos una última retransmisión no es de utilidad.

Para comparar varios protocolos de capa de transporte es necesario entender primero qué hace un paquete IP. La Figura 1.4. muestra los campos de un paquete IP.

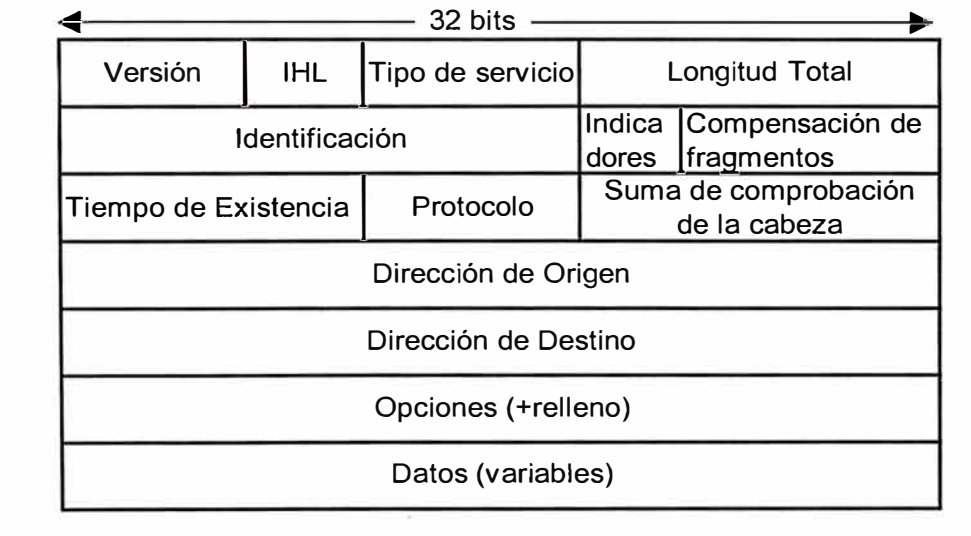


Figura 1.4. Campos de un paquete IP.

Los campos del paquete IP se definen de la siguiente manera:

- Versión. Indica si se está utilizando la versión 4 ó 6 de IP.

- Longitud de la cabecera IP (IHL). Indica la longitud del datagrama de la cabecera en palabras de 32 bits.
- Tipo de servicio. Especifica como un protocolo de capa superior determinado quiere que se maneje el datagrama actual. Se puede asignar a los paquetes varios niveles de calidad de servicio (QoS) dependiendo de este campo.
- Longitud total. Especifica la longitud de todo el paquete IP, incluidos los datos y la cabecera en bytes.
- Identificación. Contiene un número entero que identifica al datagrama actual. Este campo se utiliza para ayudar a unir diferentes fragmentos de un datagrama.
- Indicadores. Un campo de 3 bits en el que los 2 bits más bajos controlan la fragmentación. El bit de orden superior no se utiliza en este campo. El primer bit especifica si se puede fragmentar el paquete, el segundo bit especifica si el paquete es el último fragmento de una serie de paquetes fragmentados.
- Tiempo de existencia. Mantiene un contador que disminuye gradualmente hasta cero, en cuyo punto se descarta el datagrama. Esto impide que los paquetes entren en un bucle sin fin.
- Protocolo. Indica qué protocolo de capa superior está recibiendo los paquetes entrantes después de que haya completado el proceso IP.

- Suma de comprobación. Verifica que la cabecera no está corrompida.
- Dirección de origen. La dirección que envía.
- Dirección de destino. La dirección que recibe el datagrama.
- Opciones. Permite que IP soporte varias opciones, como la seguridad.
- Datos. Contiene datos de aplicación, así como información del protocolo de capa superior.

1.7.1. TCP

TCP proporciona un servicio de dúplex completo, reconocido y de flujo controlado a los protocolos de capa superior. Mueve los datos en una corriente de bytes continua no estructurada donde los bytes se identifican mediante números de secuencia.

Para maximizar el rendimiento o tasa de transferencia, TCP permite que cada estación envíe múltiples paquetes antes de que llegue un acuse de recibo. Cuando el remitente ha recibido un acuse de recibo para un paquete saliente, el remitente desliza la ventana de paquetes por la corriente de bytes y envía otro paquete. Este mecanismo de control del flujo se conoce como *sliding window* (ventana deslizante).

TCP puede soportar numerosas conversaciones de capa superior simultáneas. Los números de puerto de una cabecera TCP identifican una conversación de capa superior. Muchos puertos TCP bien conocidos están reservados para el Protocolo de

transferencia de archivos (FTP, *File Transfer Protocol*), World Wide Web (WWW), Telnet, etc.

Dentro de la porción de señalización de VoIP, TCP se utiliza para asegurar la fiabilidad de la configuración de una llamada. Debido a la manera de operar de TCP, actualmente no es posible utilizar TCP como el mecanismo para transportar la voz en una llamada VoIP. Con VoIP, la pérdida de paquetes es menos importante que la latencia.

Los campos de un paquete TCP son los siguientes:

- Puerto de origen y puerto de destino. Identifican los puntos en los que los procesos de origen y destino de la capa superior reciben los servicios TCP.
- Número de secuencia. Especifica el número asignado al primer byte de datos en el mensaje actual. En determinadas circunstancias, también se puede utilizar para identificar un número de secuencia inicial que hay que utilizar en la transmisión entrante.
- Número de acuse de recibo. Contiene el número de secuencia del siguiente byte de datos que el remitente del paquete espera recibir.
- Compensación de datos. Indica el número de palabras de 32 bits que hay en la cabecera TCP.
- Reservado. Reservado para utilización futura.
- Indicadores. Transportan información de control variada.

- Ventana. Especifica el tamaño de la ventana de recepción del remitente (es decir, el espacio de *buffer* disponible para datos entrantes).
- Suma de comprobación. Indica si la cabecera o datos se han modificado en el transporte.
- Señal de urgencia. Apunta al primer byte de datos urgentes en el paquete.
- Opciones. Especifica varias opciones TCP.
- Datos. Contiene información de la capa superior.

1.7.2. UDP

El UDP (Protocolo de datagrama de usuario) es un protocolo más sencillo que TCP y resulta útil en situaciones en las que los mecanismos de fiabilidad de TCP son innecesarios. UDP es un protocolo sin conexión y tiene una cabecera más pequeña, lo que conlleva un coste adicional mínimo.

La cabecera UDP sólo tiene cuatro campos: puerto de origen, puerto de destino, longitud y suma de comprobación UDP. Los campos de puerto de origen y destino realizan la misma función que en la cabecera TCP. El campo de longitud especifica la longitud de la cabecera y los datos de UDP, y el campo de suma de verificación permite la comprobación de la integridad del paquete. La suma de verificación UDP es opcional.

UDP se utiliza en VoIP para transportar el tráfico de voz real (los canales portadores). TCP no se utiliza porque no se necesitan

ni el control del flujo ni la retransmisión de paquetes de audio de voz. Como se utiliza UDP para transportar la corriente de audio, éste continúa transmitiendo, con independencia si se está sufriendo un 5 o un 50 por ciento de pérdida de paquete.

Si se utiliza TCP para VoIP, la latencia en la que se caería a la espera de los acuses de recibo y retransmisiones haría que la calidad de la voz fuera inaceptable. Con VoIP y otras aplicaciones de tiempo de real, controlar la latencia es más importante que asegurar la entrega fiable de cada paquete.

TCP se utiliza, por otra parte, para configurar llamadas en la mayoría de los protocolos de señalización VoIP.

1.8. Elementos de diseño de una red VoIP

Para crear un diseño de red apropiado, es importante conocer todas las interioridades y fundamentos de la tecnología de networking, así como los problemas a los que se enfrenta la voz sobre IP (VoIP), los cuales se explican a continuación:

- Retraso/ latencia.
- Fluctuación de fase.
- Compresión de voz.
- Eco.
- Pérdida de paquetes.
- Detección de actividades de voz
- Conversión digital a analógico.

1.8.1. Retraso/ latencia

El retraso o latencia en VoIP se caracteriza por el tiempo que tarda la voz en salir de la boca del que está hablando y en llegar al oído del que escuchando.

Existen tres tipos de retraso que son inherentes a las redes de telefonía actuales: retraso de propagación, retraso de serialización y retraso de manejo. El retraso de propagación es causado por la velocidad de la luz en la fibra óptica o en las redes basadas en cobre. El retraso de manejo, también llamado retraso de procesamiento , define muchas causas diferentes de retraso (empaquetado, compresión y *switching* de paquetes), y está causado por dispositivos que transmiten la trama a través de la red.

El retraso de serialización es la cantidad de tiempo que se tarda en colocar un bit o byte en una interfaz. Su influencia en el retraso es relativamente pequeña.

1.8.1.1 Retraso de propagación

La luz viaja a través del vacío a una velocidad de 300,000 kilómetros por segundo y los electrones viajan a través del cobre o de la fibra óptica a unos 200,000 kilómetros por segundo. Una red de fibra óptica alrededor del mundo (21,000 kilómetros) induce un retraso de sentido único de unos 70 milisegundos (70 ms). Aunque este retraso es casi imperceptible al oído humano, el retraso de

propagación, junto con los retrasos de manejo, puede provocar una degradación apreciable de la voz.

1.8.1.2 Retraso de manejo

Como se ha mencionado anteriormente, los dispositivos que envían la trama a través de la red provocan un retraso de manejo. Los retrasos de manejo pueden tener impacto en las redes telefónicas tradicionales, pero esos retrasos son un problema mayor en los entornos de paquetes.

1.8.1.3. Retraso en la gestión de colas

Una red basada en paquetes sufre retrasos por otras razones. Dos de estas razones son el tiempo que se necesita para mover un paquete hasta la cola de salida (*switching* de paquetes) y el retraso de la gestión de colas.

Cuando los paquetes se guardan en una cola debido a la congestión en una interfaz *outbound* (de salida), el resultado es un retraso en la gestión de colas. Este tipo de retrasos ocurre cuando se envían más paquetes que los que la interfaz puede manejar en un intervalo de tiempo dado.

El retraso en la gestión de colas de la cola de salida es otra causa de retraso. Este retraso debe estar por debajo de 10 ms. Siempre que se pueda utilizando cualquier método de gestión de colas que sea óptimo para la red.

La recomendación G.114 de la ITU-T especifica que para una buena calidad de voz no debe darse un retraso mayor de 150 ms

de una vía, de extremo a extremo. Con la implementación VoIP de Cisco, dos *routers* con un mínimo retraso de red utilizan sólo unos 60 ms de retraso de extremo a extremo. Esto deja 90 ms de retraso de red para mover el paquete IP desde el origen hasta el destino.

Existen algunas formas de retraso que son más largas, las cuales son aceptadas, porque no hay alternativa. En la transmisión por satélite, por ejemplo, se tarda aproximadamente 250 ms para que la transmisión alcance el satélite y otros 250 ms para volver a la tierra. Esto provoca un retraso total de 500 ms. A pesar de que la recomendación de la ITU-T afirma que esto está fuera de lo aceptable para la calidad de voz, muchas conversaciones tienen lugar cada día sobre enlaces de satélite. De esta manera, la calidad de voz viene a menudo definida como lo que los usuarios aceptan y utilizan.

En una red no administrada y congestionada, el retraso en la gestión de colas puede agregar más de dos segundos de retraso (o provocar que el paquete se caiga). Este largo periodo de retraso es inaceptable en casi todas las redes de voz. El retraso en la gestión de colas es sólo un componente del retraso de extremo a extremo. El retraso de extremo a extremo también se ve afectado por la fluctuación de fase.

1.8.2. Fluctuación de fase

Dicho de manera sencilla, la fluctuación de fase (*jitter*) es la variación del tiempo de llegada de un paquete. La fluctuación de fase es un problema que existe sólo en las redes basadas en paquetes. Cuando está en un entorno de voz por paquetes, el remitente espera transmitir de forma fiable paquetes de voz en un intervalo regular (por ejemplo, enviar una trama cada 20 ms). Esos paquetes de voz se pueden retrasar por toda la red de paquetes y no llegar con el mismo intervalo de tiempo regular a la estación receptora (por ejemplo, puede que no sean recibidos cada 20 ms, véase la Figura 1.5). La diferencia entre cuándo se esperaba recibir el paquete y cuándo se recibe en realidad es lo que se llama la fluctuación de fase.

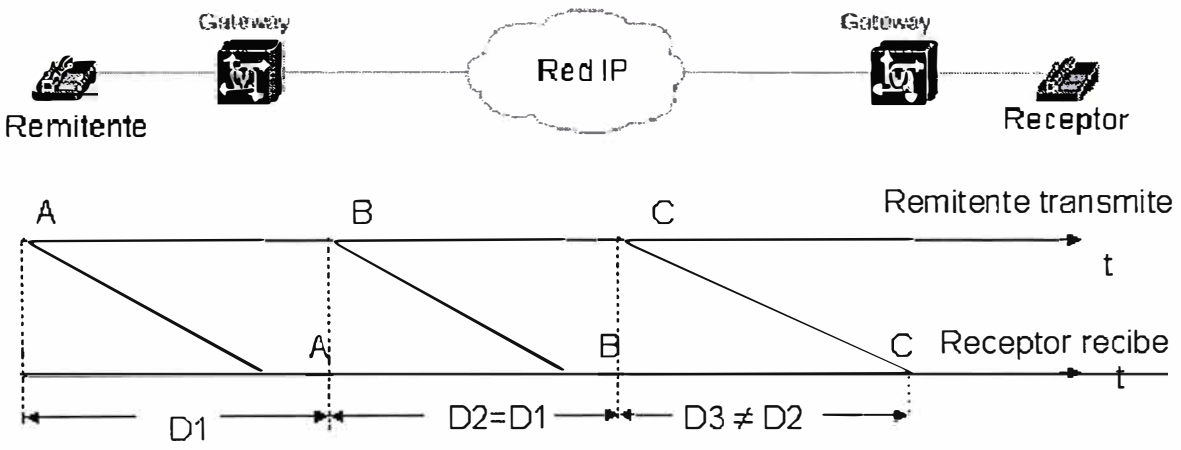


Figura 1.5. Variación de tiempo de llegada de un paquete (Fluctuación de fase)

En la Figura 1.5 se puede ver que el tiempo que se tarda en enviar y recibir los paquetes A y B es el mismo (D1 = D2). El paquete C tiene un retraso en la red y se recibe después de la hora a la que se le esperaba. Es por lo que es necesario un *buffer* de fluctuación de fase que oculta el retraso.

Es importante resaltar que la fluctuación de fase y el retraso total no es la misma cosa, a pesar de que tener mucha fluctuación de fase en una red de paquetes puede incrementar el retraso total de la red. Esto se debe a que cuanta más fluctuación de fase haya, más necesitará ser compensado el *buffer* de fluctuación de fase por la impredecible naturaleza de la red de paquetes.

Si la red de datos está bien construida y se toman las precauciones apropiadas, la fluctuación de fase es normalmente un problema menor y el *buffer* de fluctuación de fase no contribuye significativamente al retraso total de extremo a extremo.

1.8.3. Compresión de voz

Se utilizan dos variaciones básicas de PCM de 64 Kbps: La ley u y la ley a. Los métodos se parecen en que ambos utilizan compresión logarítmica para alcanzar de 12 a 13 bits de calidad PCM lineal en 8 bits, pero se diferencian en detalles de compresión relativamente menores (la ley u tiene una ligera ventaja en la capa baja, rendimiento en relación señal a ruido). Su utilización esta limitada históricamente a países y regiones fronterizos. En América del Norte se utiliza la ley u y en Europa la

ley a. Es importante tomar nota de que cuando se realiza una llamada de larga distancia, cualquier conversación que requiere un cambio de ley u a ley a es responsabilidad del país de la ley u.

Otro método de compresión utilizado a menudo es la modulación por impulsos codificados diferencial y adaptable (ADPCM, *Adaptive Differential Pulse Code Modulation*). Un ejemplo de utilización común de la ADPCM es la ITU-TG.726, que codifica utilizando muestras de 4 bits, lo que da una velocidad de transmisión de 32 Kbps. A diferencia de la PCM, los 4 bits no codifican directamente la amplitud de la voz, sino que codifican las diferencias de la amplitud, así como la velocidad de cambio de esa amplitud, empleando alguna predicción lineal rudimentaria.

PCM y ADPCM son ejemplos de codificación por forma de ondas, técnicas de compresión que explotan las características redundantes de la forma de ondas. En los últimos 10 ó 15 años se han desarrollado nuevas técnicas que llevan más allá el conocimiento de las características de la generación de la voz.

Estas técnicas emplean procedimientos de procesamiento de señales que comprimen la voz enviando sólo información paramétrica simplificada sobre la vibración y modulación de la voz original, necesitando menos ancho de banda para transmitir esa información.

Estas técnicas se puedan agrupar generalmente como codecs de origen e incluyen variaciones como la codificación con

predicción lineal (LPC, *Linear Predictive Coding*) la compresión de predicción lineal con excitación por código (CELP, *Code Excited Linear Prediction Compression*) y la MP-MLQ (*Multipulse, Multilevel Quantization*).

1.8.3.1. Normas de codificación de voz

La ITU-T normaliza los esquemas de codificación CELP, MP-MLQ PCM y ADPCM en sus recomendaciones de la serie G. Entre los estándares de codificación más populares para telefonía y voz por paquetes se encuentran:

- G.711 Describe la técnica de codificación de voz de PCM de 64 Kbps subrayada anteriormente; la voz codificada con G.711 está en un formato correcto para la entrega de voz digital en la red telefónica pública o a través de intercambio privado de ramas (PBX) .
- G.726. Describe la codificación de ADPCM a 40,32,24 y 16 Kbps; también se puede intercambiar voz ADPCM entre voz por paquetes y telefonía pública o redes PBX, suponiendo que estas últimas tiene la capacidad ADPCM.
- G.728. Describe una variación de bajo retraso de 16 Kbps de una compresión de voz CELP.
- G.729. Describe la compresión CELP que permite que la voz sea codificada en flujos de 8 Kbps; dos variaciones de este estándar (G.729 y G.729, anexo A) difieren ampliamente en cuanto a complejidad de computación y ambas proporcionan

generalmente una calidad de voz tan buena como la ADPCM de 32Kbps.

- G.723.1. Describe una técnica de compresión que se puede utilizar para comprimir voz u otros componentes de señales de audio de servicios multimedia a una baja velocidad de bit, como parte de la familia de estándares H.324. Dos velocidades de bits están asociadas con este codificador: 5,3 y 6,3 Kbps. La velocidad de bit más alta se basa en la tecnología MP-MLQ y proporciona una mayor calidad. La velocidad de bit más baja se basa en CELP y proporciona buena calidad, y permite que los diseñadores del sistema tengan flexibilidad adicional.

1.8.3.2. Mean Opinion Score

Hay dos formas de probar la calidad de la voz: subjetiva y objetivamente. Los humanos realizan pruebas de calidad de voz subjetivas mientras que las computadoras realizan pruebas de voz objetivas.

Los codecs se han desarrollado y armonizado sobre la base de medidas subjetivas de calidad de voz. Las medidas estándar de calidad objetiva, como una total distorsión armónica y relaciones señal a ruido no se corresponden muy bien con una percepción de calidad de voz humana, lo que al final es la meta de la mayoría de las técnicas de compresión de voz.

Una referencia subjetiva común para cuantificar el rendimiento de codec (codificador- decodificador) de voz es lo que

se llama la nota media de opinión (MOS, *Mean Opinion Score*). Las pruebas MOS se dan a un grupo de oyentes. Como la calidad de voz y sonido es subjetiva para los oyentes en general, es importante obtener una amplia gama de oyentes y material de prueba cuando se realiza una prueba MOS. Los oyentes otorgan a cada muestra de material de voz una puntuación entre 1 (malo) y 5 (excelente). Se extrae luego una media para obtener la puntuación media de la opinión.

La comprobación MOS se utiliza también para comparar como funciona un codec determinado bajo circunstancias distintas, incluidos diferentes niveles de ruidos de fondo, múltiples codificaciones y decodificaciones, etc. Se pueden luego utilizar estos datos para comparar con otros codecs. La puntuación MOS para varios codecs ITU-T aparece en la Tabla 1.1. Esta tabla muestra la relación entre codificadores de baja velocidad de bit y estándares PCM.

Método de Compresión	Velocidad de bit (Kbps)	Tamaño de muestra (ms)	Puntuación MOS
G.711 PCM	64	0,125	4,1
G.726 ADPCM	32	0,125	3,85
G.728 Predicción lineal con excitación por código de bajo retraso (LD-CELP)	15	0,625	3,61
G.729 Predicción lineal con excitación por código algebraico de estructura conjugada (CS-ACELP)	8	10	3,92
G.729ª CS-ACELP	8	10	3,7
G.723.1 MP-MLQ	6,3	30	3,9
G.723.1 ACELP	6,3	30	3,65

Fuente : Laboratorios Cisco

Tabla 1.1 Puntuación MOS de los codecs ITU-T

1.8.3.3. Medición de la calidad de voz según la percepción

Aunque la puntuación MOS es un método subjetivo para determinar la calidad de la voz, no es el único método para hacerlo. Existe la recomendación P. 861 de la ITU-T, que cubre las maneras con las que se puede determinar objetivamente la calidad de voz utilizando la Medición de calidad de voz según la percepción (PSQM, *Perceptual Speech Quality Measurement*).

PSQM tiene muchos inconvenientes cuando se utiliza con codecs de voz (vocoders) uno de estos inconvenientes es que lo que la "máquina" o PSQM oye no es lo que percibe el oído humano. En otros términos, una persona puede engañar al oído humano al percibir una voz de mayor calidad, pero una computadora no puede. PSQM fue desarrollado para "oír" deterioros provocados por la compresión y descompresión y no por la pérdida de paquetes o la fluctuación de fase.

1.8.4. Eco

En una conversación el eco es un fenómeno que puede ir desde lo ligeramente molesto hasta lo insoportable, provocando que la conversación sea ininteligible.

Oír la propia voz en el auricular mientras se está hablando es común y tranquilizador para la persona que está hablando. Oír la propia voz después de un retraso de unos 25ms puede provocar interrupciones y romper la cadencia de conversación.

En una red *toll* tradicional, el eco está normalmente provocado por un desajuste en la impedancia de la conversación del *switch* de red de cuatro cables al bucle local de dos cables (como muestra la Figura 1.6). En la Red Pública de Telefonía Conmutada (PSTN), el eco está regulado con canceladores de eco y un firme control sobre los desajustes de la impedancia en los puntos de reflexión común, como muestra la Figura 1.6

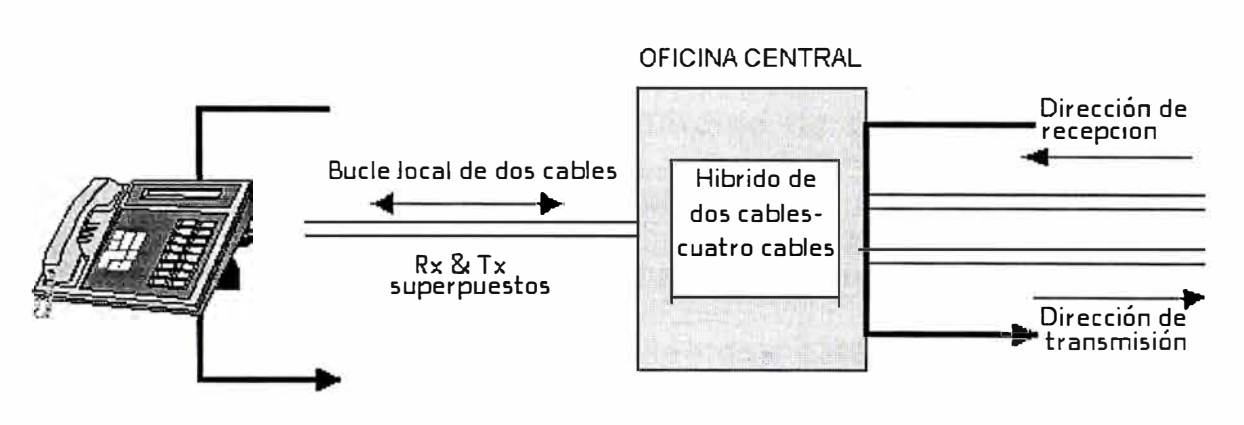


Fig. 1.6 Eco provocado por desajuste de la impedancia

El eco tiene dos inconvenientes: Puede ser alto y puede ser largo. Cuando más alto y largo es el eco, más incómodo resultará.

Las redes telefónicas en aquellas partes del mundo donde se utiliza principalmente la voz analógica emplean supresores de eco, que eliminan el eco ajustado la impedancia en un circuito. Este no es el mejor mecanismo que se puede utilizar para eliminar el eco y, de hecho, provoca otros problemas, Por ejemplo, no se puede utilizar la Red Digital de Servicios Integrados (RDSI) en una línea que tiene un supresor de eco, porque éste corta el radio de acción en la frecuencia que utiliza esa RDSI.

En las actuales redes basadas en paquetes, se pueden construir canceladores de eco en codecs de velocidad de transmisión baja y hacerlos funcionar en cada DSP. En las implementaciones de algunos fabricantes, la cancelación del eco se hace en el software; esta práctica reduce drásticamente los beneficios de la cancelación del eco. Sin embargo, VoIP de Cisco realiza toda su cancelación de eco en su DSP.

1.8.5. Pérdida de paquetes

En las redes de datos, la pérdida de paquetes es común y esperada. De hecho, muchos protocolos de datos utilizan la pérdida de paquetes para conocer las condiciones de la red y poder reducir el número de paquetes que están enviando.

Cuando se genera un tráfico muy intenso de las redes de datos, es importante controlar la cantidad de pérdida de paquetes que hay en esa red.

Cuando se genera voz en redes de datos, es importante construir una red que transporte con éxito la voz de manera fiable y oportuna. Resulta de gran ayuda poder utilizar un mecanismo para hacer que la voz sea resistente a la pérdida periódica de paquetes.

La implementación VoIP de Cisco Systems permite al *router* de voz responder a la pérdida de paquetes. Si un paquete de voz no es recibido cuando se esperaba (el tiempo esperado es

variable), se da por hecho que se ha perdido y se vuelve a repetir el último paquete recibido, como muestra la Figura 1.7.
Como el paquete perdido tiene sólo 20ms de voz, el oyente medio no aprecia la diferencia de la calidad de voz.

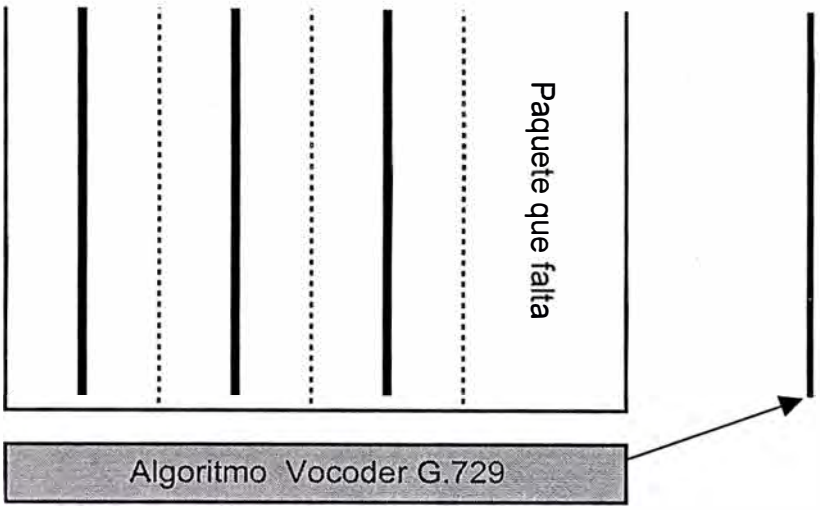


Figura. 1.7. Pérdida de paquete con G.729

Al utilizar la implementación G.729 de Cisco para VoIP se puede decir que cada línea de la Figura 1.7. representa un paquete. Los paquetes 1,2,3 alcanzan su destino, pero el paquete 4 se ha perdido en algún sitio durante la transmisión. La estación receptora espera durante un periodo de tiempo (por su *buffer* de fluctuación de fase) y luego ejecuta una **estrategia de ocultación**.

Esta estrategia de ocultación vuelve a repetir el último paquete recibido (en este caso, el paquete 3) por lo que el oyente no aprecia que hay lagunas de silencios. Como la voz perdida sólo es de 20 ms, el oyente no apreciará la diferencia. Se puede realizar esta estrategia de ocultación sólo si se pierde un único

paquete. Si se perdieran múltiples paquetes de forma consecutiva, la estrategia de ocultación se ejecuta sólo una vez hasta que se reciba otro paquete.

Debido a la estrategia de ocultación de G.729, de modo empírico se puede decir que G.729 tolera hasta un cinco por ciento de pérdida de paquetes como media a lo largo de toda una conversación.

1.8.6. Detección de la actividad de voz

En conversaciones de voz normales, alguien habla y alguien escucha. Las redes *toll* actuales contienen canales bidireccionales, de 64,000 bits por segundo (bps), con independencia de si alguien está hablando o no. Esto significa que en una conversación normal se pierde, por lo menos, el 50% del total del ancho de la banda. En la realidad, la cantidad de ancho de banda que se puede ser mayor si se toma un muestreo estadístico de las interrupciones y pausas de los patrones normales de voz de una persona.

Al utilizar VoIP, se puede utilizar este ancho de banda "perdido" para otros propósitos cuando está habilitada la detección de la actividad de voz (VAD, Voice Activity Detection). Como muestra la Figura 1.8, la VAD funciona detectando la magnitud de la voz en decibelios (dB) y decidiendo cuando debe dejar la voz de ser enpaquetada.

Normalmente, cuando la VAD detecta una disminución de la amplitud de la voz, espera un tiempo determinado antes de dejar

de poner tramas de voz en paquetes. Este tiempo determinado se conoce como ***hangover*** y suele ser de 200 ms.

Con todas las tecnologías se hacen concesiones. La VAD padece determinados problemas inherentes a la hora de determinar cuándo finaliza y empieza la voz y a la hora de distinguir la voz de un ruido de fondo. Esto significa que si se está en un espacio ruidoso, la VAD es incapaz de distinguir entre la voz y el ruido de fondo. Esto se conoce también como el **umbral de señal a ruido** (hace referencia a la voz y al ruido de fondo, véase la Figura 1.8). En determinadas situaciones, la VAD se inhabilita a sí misma al principio de la llamada.

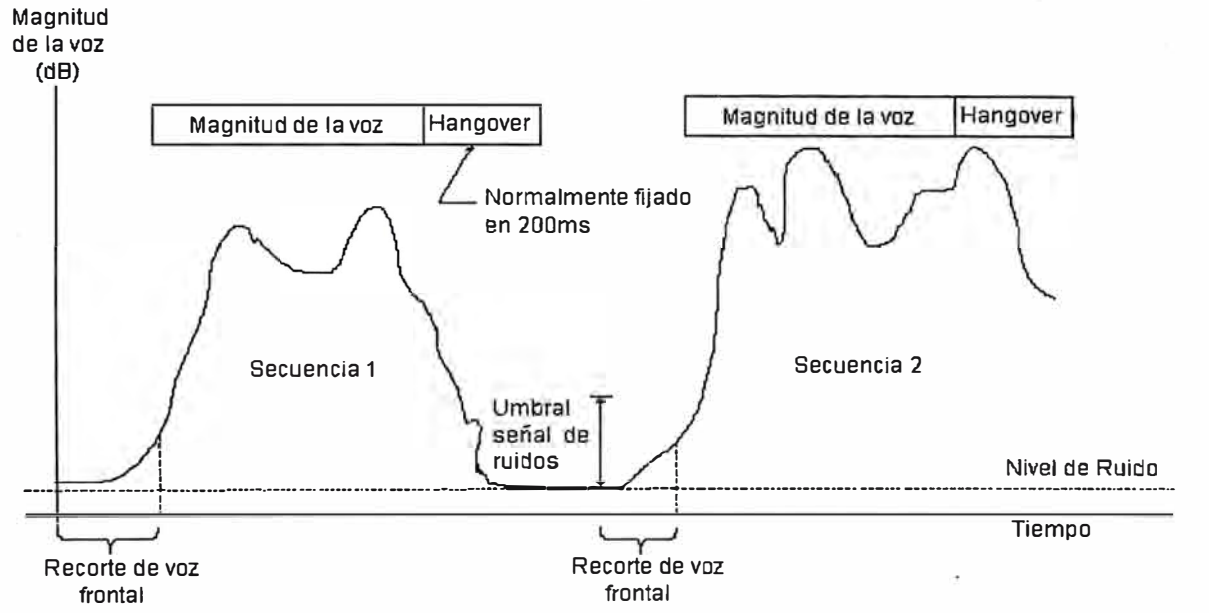


Figura 1.8 Detección de actividad de voz

Otro problema inherente con la VAD es detectar cuándo empieza la voz. Normalmente, el principio de una frase es cortada o recortada (véase la Figura 1.8). Este fenómeno se conoce como

recorte de voz frontal (*front-end speech clipping*). Normalmente, la persona que está oyendo la voz no se da cuenta del recorte de voz frontal.

1.8.7. Conversión digital a analógico

Los problemas de conversión digital y analógico (D/A) abundan también en las redes *toll*. A pesar de que todas las redes de *backbone* telefónico en los países del primer mundo son digitales, a veces ocurren conversiones D/A múltiples.

Cada vez que una conversión pasa de lo digital a lo analógico y viceversa, la voz o forma de onda es menos "verdadera". Aunque las redes *toll* actuales pueden manejar por lo menos siete conversiones D/A antes de que la calidad de voz se vea afectada, la palabra comprimida es menos robusta debido a esas conversiones.

Es importante tomar nota de que la conversión D/A debe estar estrictamente administrada en un entorno de voz comprimido. Cuando se utiliza G.729, sólo dos conversiones D/A hacen que la puntuación MOS disminuya rápidamente. La única manera de administrar la conversión D/A es tener los entornos VoIP de diseño que utilizó el diseñador de la red, con el menor número posible D/A.

A pesar de que las conversiones D/A afecta a todas las redes de voz, las redes VoIP que utilizan un codec PCM (G.711)

son tan resistentes a los problemas causados por las conversiones D/A como en las redes telefónicas actuales.

CAPITULO II
PROTOCOLOS DE SEÑALIZACION

2.1. Estándar H.323

2.1.1 Introducción

H.323 es una especificación de la ITU-T para transmitir audio, video y datos a través de una red de Protocolo Internet (IP), incluida la propia Internet. Cuando son compatibles con H.323, los productos y aplicaciones de los fabricantes pueden comunicarse e interoperar unos con otros. El H.323 estándar dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y multipunto. La serie H de las recomendaciones también especifica H.320 para la Red Digital de Servicios Integrados (RDSI) y H.324 para el Servicio telefónico analógico convencional (POTS, *Plain Old Telephone Service*) como mecanismos de transporte.

El H.323 estándar consta de los siguientes componentes y protocolos:

Función	**Protocolo**
Señalización de llamadas	H.225
Control de medios	H.245
Codecs de audio	G.711, G.722, G.723, G.728, G.729
Codecs de video	H.261, H.263

Función	Protocolo
Compartir datos	T.120
Transporte de medios	RTP/RTCP

2.1.2. Elementos H.323

La Figura 2.1 ilustra los elementos de un sistema H.323. Estos elementos son:

- Terminales
- *Gateways*
- *Gatekeepers*
- Unidades de control multipunto (MCU, *Multipoint Control Units*).

Los terminales, a los que a menudo se hace referencia como puntos finales, proporcionan conferencias punto a punto y multipunto para audio y de manera opcional, video y datos. Los *gateways* interconectan con la Red Pública de Telefonía Conmutada (PSTN) o la red ISDN (RDSI) para *interworking* el punto final de H.323. Los *gatekeepers* proporcionan el control de admisión y servicios de traducción de direcciones para terminales o *gateways*. Las MCU son dispositivos que permiten que dos o más terminales o *gateways* realicen conferencias con sesiones de audio y/o video.

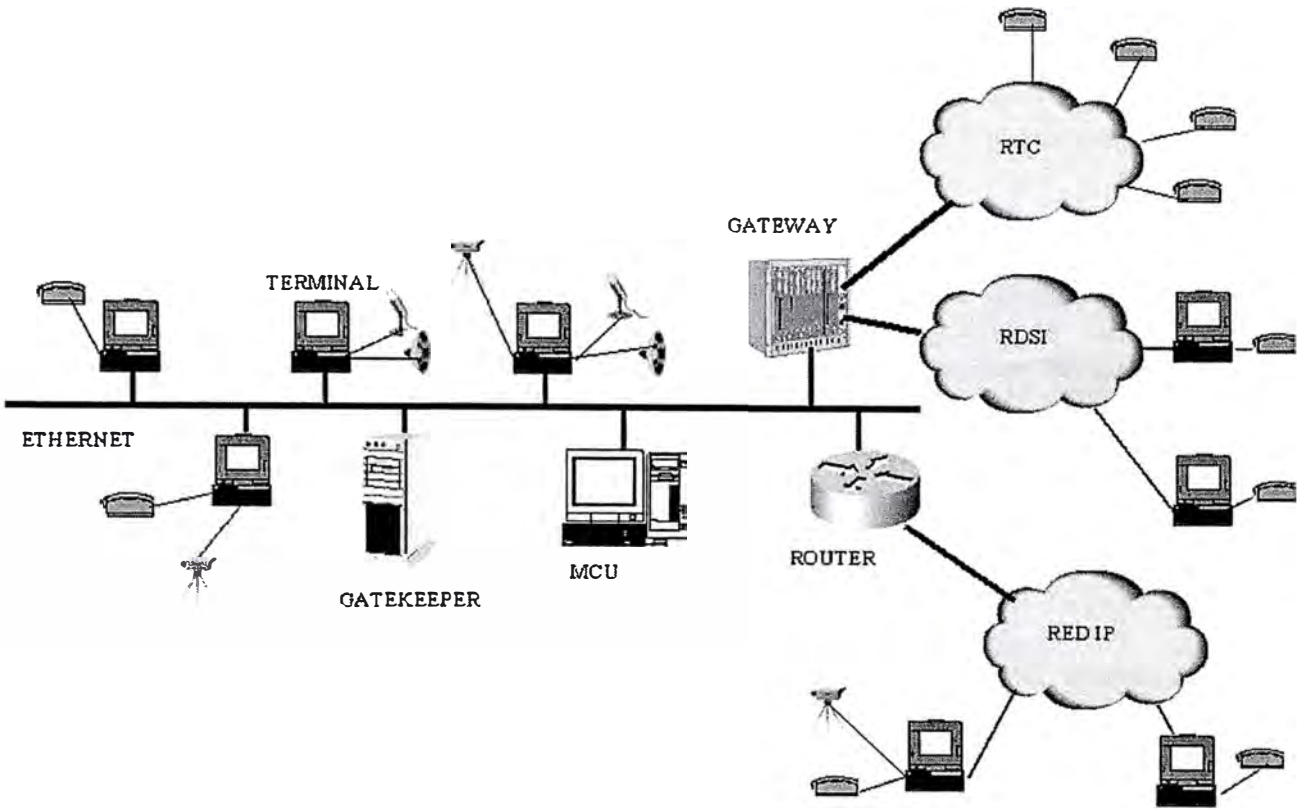


Figura 2.1. Elementos de *networking* H.323

2.1.2.1. Terminales

Los terminales H.323 deben tener una unidad de control de sistema, una transmisión de medios, codec de audio e interfaz de red basada en paquetes. Los requisitos opcionales incluyen un codec de video y aplicaciones de datos de usuario.

Las siguientes funciones y posibilidades se encuentran dentro del ámbito del terminal H.323:

- Unidad de Control de sistema. Proporciona a H.225 y H.245 el control de llamadas, intercambio de capacidad, mensajería y señalización de comandos para una actividad apropiada del terminal.

- Transmisión de medios. Formatea el audio, video, datos, flujos de control y mensajes transmitidos en la interfaz de red. La transmisión de medios recibe también el audio, video datos, flujos de control y mensajes desde la interfaz de red.
- Codec de audio. Codifica la señal desde el equipo de audio para su transmisión y decodifica el código de audio entrante. Las funciones que se requieren incluyen la codificación y decodificación de voz G.711 y recibir formatos de ley a y ley u. De manera opcional, se pueden soportar la codificación y decodificación G.722, G.723.1, G.728 y G.729.
- Interfaz de red. Una interfaz basada en paquetes que puede hacer servicios de unidifusión y multidifusión de extremo a extremo de Protocolo para el control de la transmisión (TCP) y el Protocolo de datagrama de usuario (UDP).
- Codec de video . Es opcional, debe ser capaz de codificar y decodificar video de acuerdo con el *Quarter Comment Intermediate Format* (QCIF) H.261.
- Canal de datos. Soporta aplicaciones como acceso a base de datos, transferencia de archivos y conferencias audio gráficas, como se especifica en la recomendación T.120.

2.1.2.2. *Gateway*

Un *gateway* es un punto final en una red de datos que proporciona una interfaz con otro tipo de red que oferta los mismos servicios multimedia. El *gateway* se encarga de realizar la conversión de protocolos entre las dos redes de manera que estas se puedan comunicar de forma transparente

para el usuario. Tal como se muestra en la Figura 2.2. Una aplicación del *gateway* H.323 es en telefonía IP, donde el *gateway* conecta una red IP con una red de circuito conmutado (SCN, *switched circuit network*).

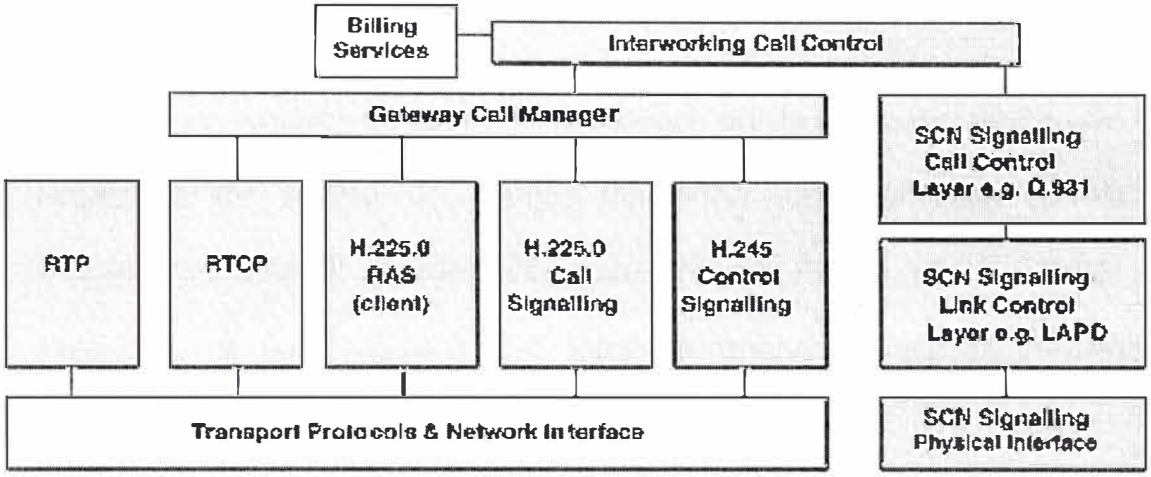


Figura 2.2. Pila de protocolos *del Gateway*

2.1.2.3. Gatekeeper

El *gatekeeper* es una función opcional que proporciona servicios de control de prellamada y nivel de llamada a los puntos finales H.323. En caso de ser instalado este elemento se convierte en el núcleo del sistema debido a que se encarga de gestionar todas las comunicaciones, por lo que todo punto final que quiera establecer una conexión debe remitirse a él.

Si un *gatekeeper* está presente en un sistema H.323 debe llevar a cabo lo siguiente:

- Conversión de direcciones. Las llamadas que se originan dentro de una red H.323 utilizan como direcciones de destino las direcciones IP. De igual manera, las llamadas que son originadas fuera de la red H.323 y

recepcionadas por el *gateway* son números telefónicos los cuales van a ser convertidos en direcciones IP para ser enrutados dentro de la red.

- Control de admisiones. Proporciona acceso autorizado a H.323 utilizando los mensajes *Admission Request/Admission Confirm/Admission Reject* (ARQ / ACF / ARJ).
- Control de ancho de banda. Consiste en la administración de los requisitos de ancho de banda utilizando los mensajes *Bandwidth Request/Bandwidth Confirm/Bandwidth Reject* (BRQ / BCF / BRJ). El resultado es la limitación del total de ancho de banda disponible, reservando lo necesario para aplicaciones de datos.
- Administración de zona.

Opcionalmente ,el *gatekeeper* puede aportar la siguiente funcionalidad:

- Señalización de control de llamadas. Utiliza el modelo de señalización de llamadas de *gatekeeper* enrutado (GKRCS, *Gatekeeper Routed Call Signalling*).
- Autorización de llamada. Permite que el *gatekeeper* restrinja el acceso a determinados terminales y *gateways*.
- Administración de ancho de banda. Permite que el *gatekeeper* rechace la admisión si el ancho de banda no está disponible.
- Administración de llamada. Los servicios incluyen el mantenimiento de una lista de llamadas activas que se puede utilizar para indicar que un punto final está ocupado.

En la Figura 2.3 observamos sus componentes.

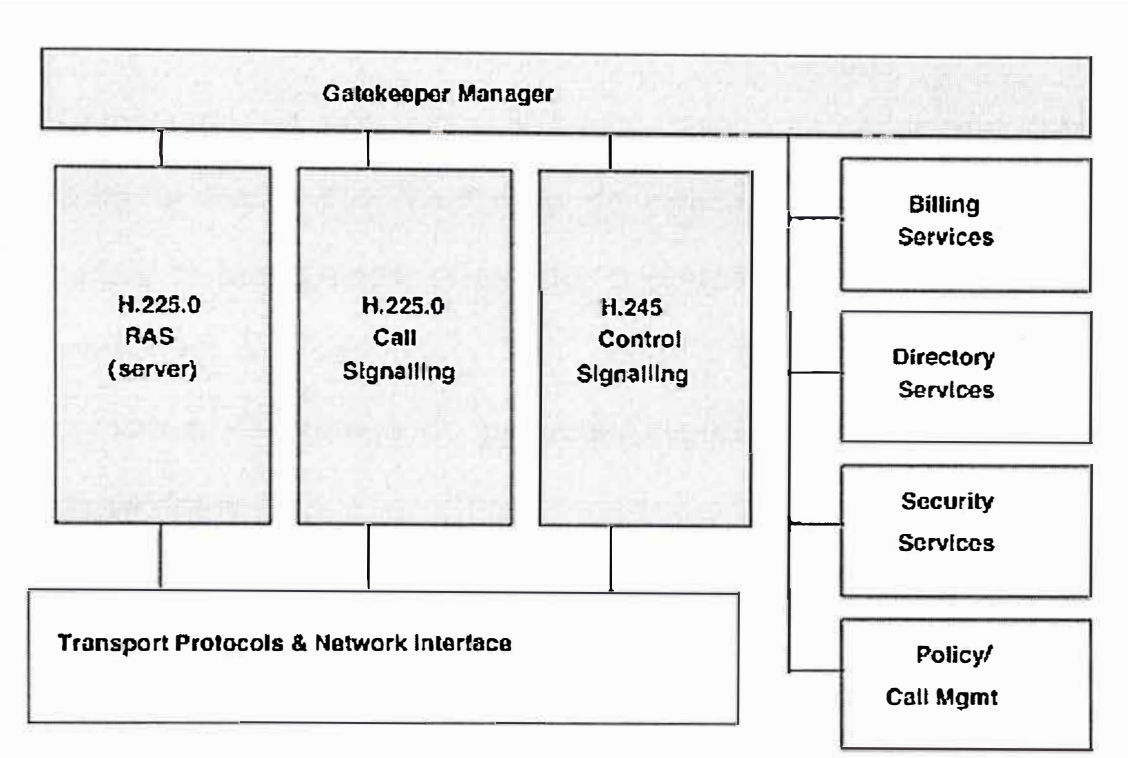


Figura 2.3 Componentes del *Gatekeeper*

2.1.2.4. Unidades de Control Multipunto (MCUs)

El MCU es la entidad que permite el establecimiento de comunicaciones multipunto, es decir, provee soporte para conferencia. Está integrado por un Controlador Multipunto (MC) y opcionalmente un Procesador Multipunto (MP).

El MC se encarga de gestionar la comunicación multipunto estableciendo las capacidades comunes de los terminales y el MP se encarga de la multiplexación de los canales de sonido, video y datos.

El *gatekeeper*, *gateway* y MCU's son componentes separados lógicamente en el estándar H.323 pero pueden estar implementados en un simple dispositivo físico.

2.1.3. Conjunto del protocolo H.323.

El conjunto del protocolo H.323 está basado en varios protocolos, como muestra la Figura 2.4. La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos de medios y los mensajes en los sistemas H.323. Estos protocolos son soportados por mecanismos de entrega de paquetes seguros y poco seguros sobre las redes de datos.

El conjunto del protocolo H.323 está dividido en tres áreas de control principales:

- Señalización de registro, admisiones y estado (RAS). Proporciona un control de prellamadas en las redes basadas en *gatekeeper* H.323.
- Señalización de control de llamadas. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales.
- Control y transporte de medios. Proporciona el canal H.245 seguro que transporta los mensajes de control de los medios. El transporte ocurre con un flujo UDP no seguro.

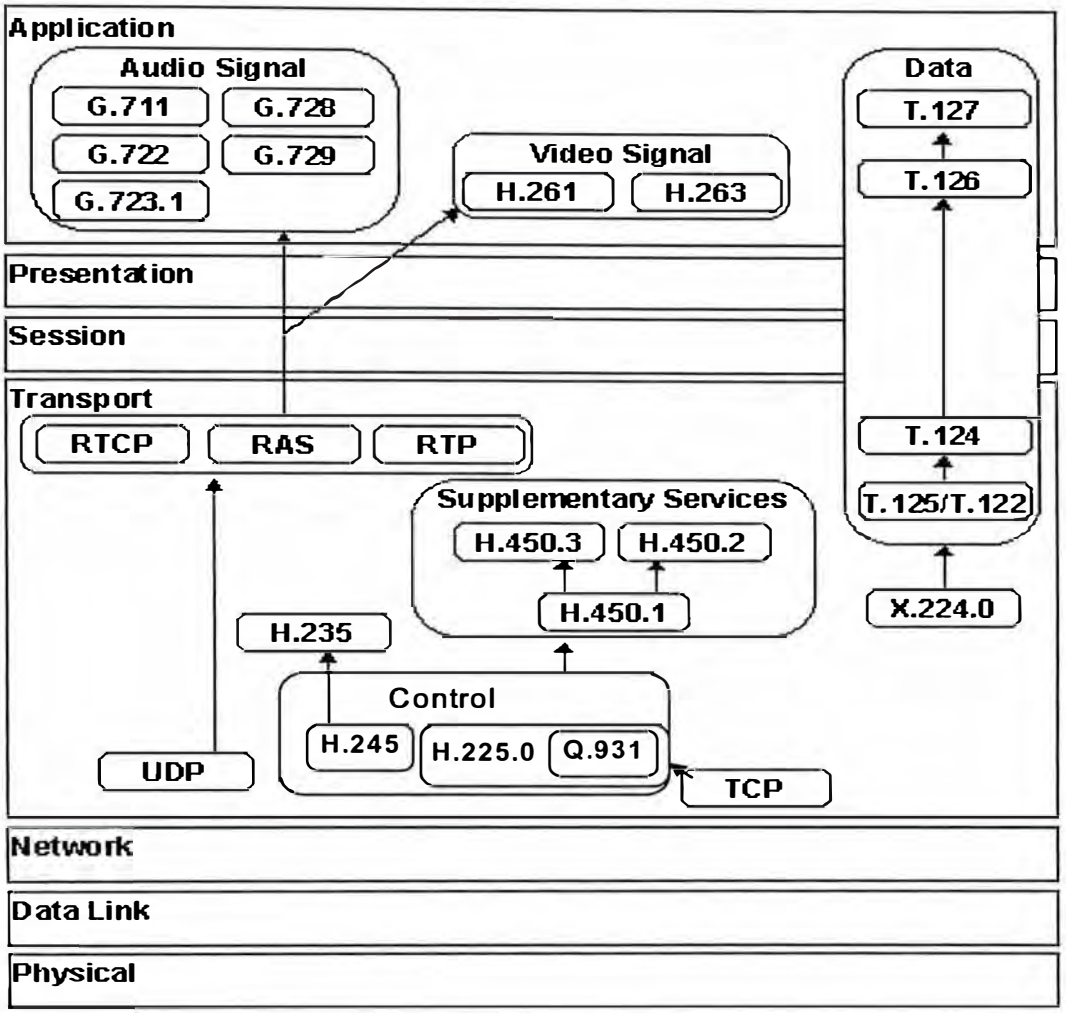


Figura 2.4 Pila de protocolos H.323

2.1.3.1 Señalización RAS

La señalización RAS proporciona un control de prellamadas en las redes H.323 donde existen *gatekeepers* y una zona. El canal RAS se establece entre puntos finales y *gatekeepers* a través de una red IP. El canal RAS está abierto antes de que ningún otro canal sea establecido y es independiente de la señalización de control de llamadas y de los canales de transporte de medios. Esta conexión UDP no segura transporta los mensajes RAS que realizan el registro, las admisiones, los cambios de ancho de banda, el estado y los procedimientos de liberación.

2.1.3.1.1 Descubrimiento del *gatekeeper*

El descubrimiento de *gatekeeper* es un proceso manual o automático que los puntos finales utilizan para identificar con que *gatekeeper* registrarse. En el método manual, los puntos finales están configurados con la dirección IP del *gatekeeper* predefinido. El método automático permite que la relación entre puntos finales y *gatekeepers* cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento (*autodiscovery*).

El autodescubrimiento permite que un punto final, que tal vez no conozca a su *gatekeeper* pueda descubrirlo a través de un mensaje de multidifusión. Como los puntos finales no tienen por que estar estáticamente configurados o reconfigurados para los *gatekeepers*, este método tiene menos cargas administrativas.

Existen tres mensajes RAS para el autodescubrimiento:

- *Gatekeepers Request* (GRQ).
- *Gatekeepers Confirm* (GCF).
- *Gatekeepers Reject* (GRJ).

2.1.3.1.2 Registro

El registro es el proceso que permite que los *gateways*, puntos finales y MCU alcancen una zona e informen al *gatekeeper* de sus direcciones IP y alias. El registro, que es un procedimiento necesario, ocurre después del proceso de descubrimiento, pero antes de que se intente realizar ninguna llamada. Se pueden utilizar los seis mensajes siguientes para permitir que un punto final registre y cancele registros:

- *Registration Request* (RRQ)

- *Registration Confirm* (RCF)
- *Registration Reject* (RRJ)
- *Unregister Request* (URQ)
- *Unregister Confirm* (UCF)
- *Unregister Reject* (URJ)

2.1.3.1.3 Admisiones

Los mensajes de admisión entre puntos finales y *gatekeepers* proporcionan las bases para la admisión de llamadas y control de ancho de banda. Los *gatekeepers* autorizan el acceso a las redes H.323 confirmando o rechazando una petición de admisión. Una petición de admisión incluye el ancho de banda solicitado, que puede ser reducida por el *gatekeeper* en la confirmación. Los siguientes mensajes proporcionan control de admisión en las redes H.323.

- ARQ. Un intento realizado por un punto final para iniciar la llamada.
- ACF. Una autorización dada por el *gatekeeper* para admitir la llamada.
- ARJ. Deniega la petición del punto final de tener acceso a la red para esta llamada determinada.

2.1.3.1.4 Información de estado

El *gatekeeper* puede utilizar el canal RAS para obtener información de estado desde un punto final. Podemos utilizar este mensaje para monitorizar si el punto final está en línea (*online*) o no (*offline*) debido a una condición de falla. El periodo típico de sondeo para los mensajes de estado es de 10 segundos. Se utilizan tres mensajes para proporcionar el estado en el canal RAS.

- *Information Request* (IRQ). Se envía desde el *gatekeeper* al punto final que solicita el estado.
- *Information Request Response* (IRR). Se envía desde el punto final al *gatekeeper* en respuesta a una petición de información IRQ.
- *Status Enquiry*. Se envía fuera del canal RAS en el canal de señalización de llamadas. Los *gatekeepers* suelen utilizar estos mensajes para verificar si las llamadas siguen activas.

2.1.3.2 Señalización del control de llamadas (H.225)

El protocolo H.225 es utilizado para habilitar conexiones entre puntos finales H.323 (terminales y *gateway*) sobre el cual la información en tiempo real puede ser transportado. La señalización de llamadas involucra el intercambio de mensajes H.225 sobre un canal de señalización confiable. Por ejemplo los mensajes del protocolo H.225 son transportados sobre TCP en una red IP basada en H.323.

Los mensajes H.225 son intercambiados entre los puntos finales si no existe un *gatekeeper* en la red, en caso contrario los mensajes son intercambiados ya sea directamente entre los puntos terminales o enrutados a través de un *gatekeeper*. El método apropiado se decide en el *gatekeeper* durante el intercambio de mensajes de admisión RAS.

En la Figura 2.5 observamos el método de señalización de llamada directa de punto final.

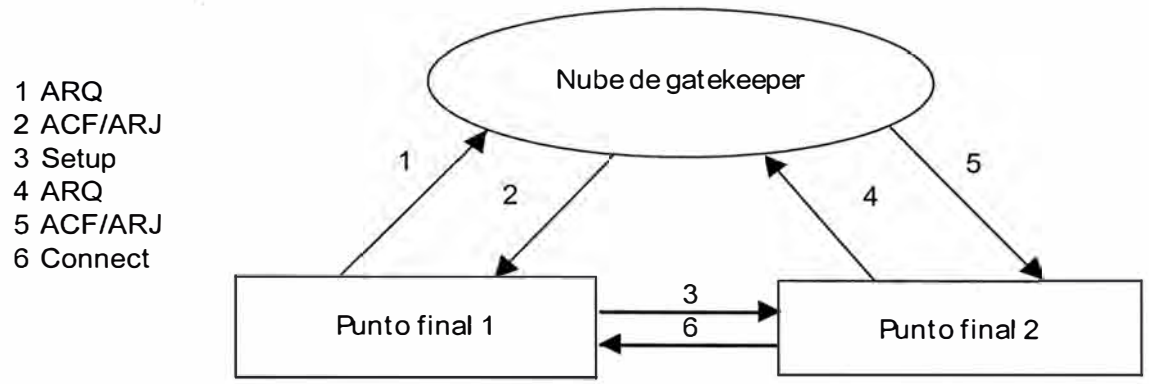


Figura 2.5. Señalización de llamada directa de punto final.

En la Figura 2.6 observamos los mensajes de señalización de las llamadas entre los puntos finales los cuales son enrutados a través del *gatekeeper*. Método GKRCS (*Gatekeeper Routed Call Signalling*).

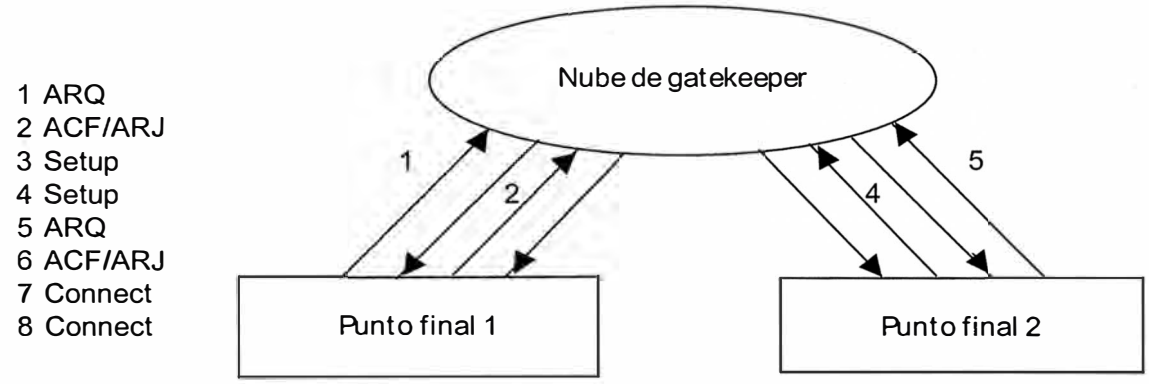


Figura 2.6 Señalización de llamada de *gatekeeper* enrutado

2.1.3.3 Control y transporte de los medios (H.245 y RTP/RTCP)

H.245 maneja mensajes de control de extremo a extremo entre entidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, video, datos y canal de control. Un punto final establece un canal H.245 para cada llamada con el punto final que está participando. El canal de control seguro se crea sobre IP utilizando

el puerto TCP dinámicamente asignado en el último mensaje de señalización de llamada.

El intercambio de capacidades, la apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes ocurren sobre este canal de control. H.245 también permite intercambio de capacidades separadas para la transmisión y recepción, así como la negociación de las funciones, como determinar que codec se debe utilizar.

Podemos hacer uso de los siguientes procedimientos y mensajes para permitir la operación de control H.245:

- *Capability Exchange*. Consiste en mensajes que intercambian de manera segura las capacidades entre dos puntos finales, también llamados terminales. Estos mensajes indican capacidades del terminal para transmitir y recibir audio, video y datos al terminal que está participando.
- *Master-Slave Termination*. Procedimientos utilizados para determinar que punto final es el principal (maestro) y que punto final es el secundario (esclavo) para una llamada determinada.
- *Round-Trip Delay*. (retraso de ida y vuelta) Procedimientos utilizados para determinar el retraso entre los puntos finales de origen y de terminación.
- *Logical Channel Signalling*. Abre y cierra el canal lógico que transporta la información de audio, video y datos. El canal se prepara antes de la transmisión real para asegurar que los terminales estén preparados y sean capaces de recibir y decodificar información.

2.1.3.3.1 *Real Time Transport Protocol* (RTP)

El RTP (*Real-Time Transport Protocol*, RFC 1889) es un protocolo que proporciona transporte de datos extremo a extremo para aplicaciones en tiempo real, como pueden ser la transmisión de sonido o video. Para ello proporciona identificación del flujo de datos transportado, secuenciación de los paquetes, marcas de tiempo y monitorización de la comunicación.

El RTP se sitúa en el nivel de sesión y generalmente se apoya sobre un protocolo de nivel de transporte no fiable como es UDP. Se implementa junto con la aplicación en lugar de hacerlo como una capa aislada y funciona junto con un protocolo de control denominado RTCP (*Real-Time Control Protocol*). En la Figura 2.7 se puede observar la pila de protocolos utilizada por una aplicación que hace uso de RTP.

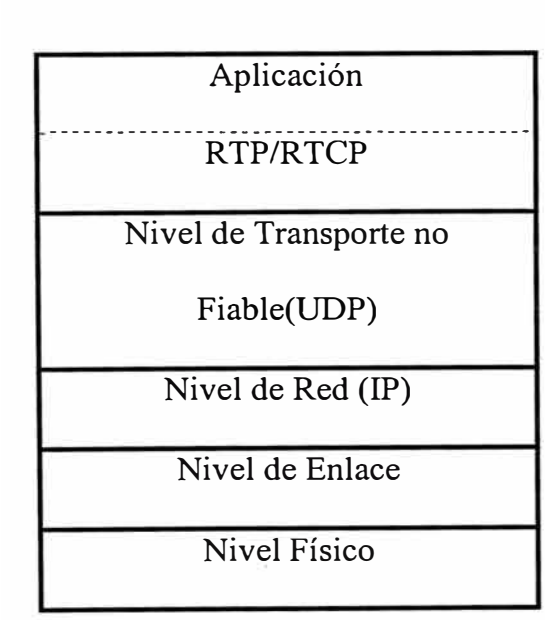


Figura 2.7- Pila de protocolos sobre la que se apoya el RTP.

2.1.3.3.2 *Real Time Transport Control Protocol* (RTCP)

El RTCP (*Real-Time Control Protocol*) trabaja conjuntamente con el RTP y se encarga de monitorizar la comunicación en tiempo real. Su función es propagar información acerca de la calidad con la que el usuario está recibiendo el flujo de información, de modo que la aplicación que hace uso del RTP puede actuar en consecuencia, adaptándose a las variaciones en el entorno de transmisión. En el caso que la comunicación sea multicast los mensajes RTCP deben llegar a cada uno de los usuarios conectados al grupo, de modo que todos tengan información de la calidad con la que está llegando la información al resto de usuarios.

Por tanto las funciones que lleva a cabo el RTCP son básicamente:

- Proporcionar información sobre la calidad con la que se están recibiendo los datos.
- Dar a conocer el número de usuarios conectados a una sesión en cada momento (en el caso de sesiones *multicast*).
- Temporizar la velocidad de transmisión de paquetes RTCP. Estos paquetes se envían periódicamente, pero lógicamente cuantos más clientes participen en una sesión menos frecuentemente se deberán enviar.

2.1.4. Flujos de llamada H.323

Los flujos de llamada bajo el estándar H.323, nos describen los pasos para la creación, establecimiento y liberación de una llamada.

En el ejemplo la red contiene 2 terminales H.323 denominados T1 y T2, los cuales están conectados al *gatekeeper*. Se asume una llamada

directa, así mismo que para el intercambio de datos multimedia (*media stream*) se usa la encapsulación RTP.

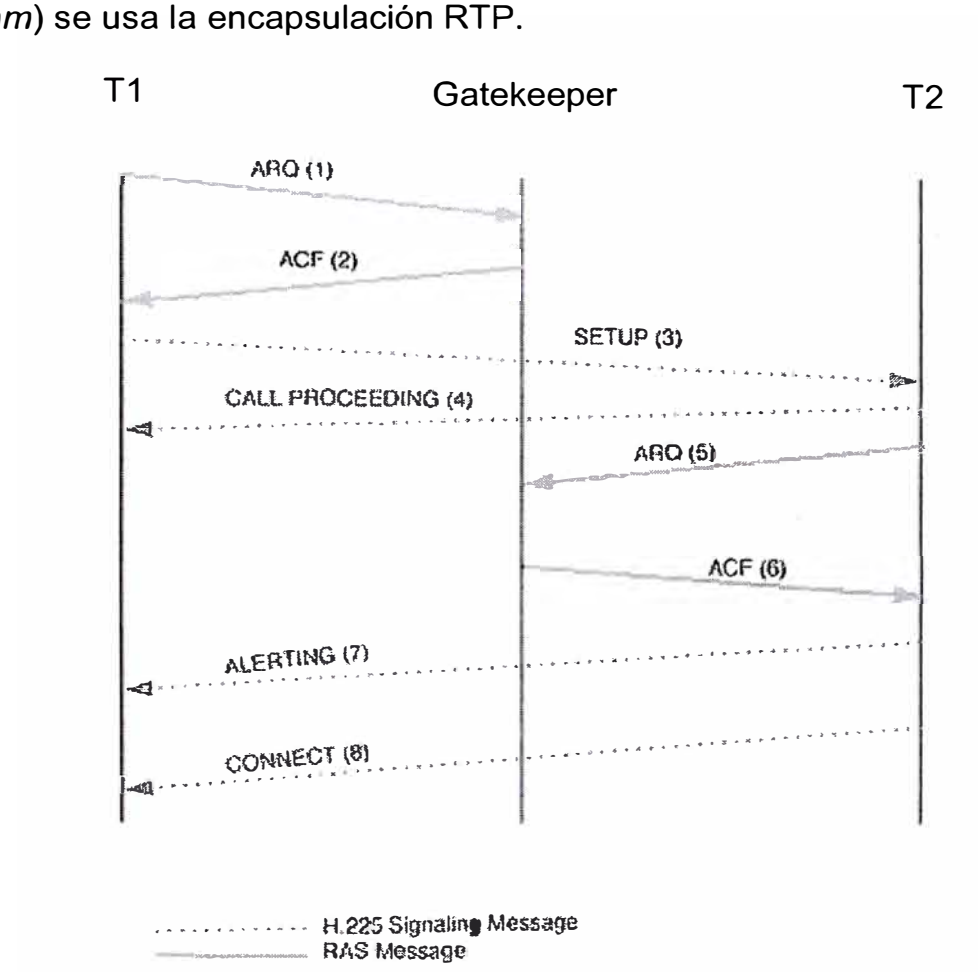


Figura 2.8 Establecimiento de llamada H.323

1. El terminal T1 envía el mensaje de registro mediante el RAS ARQ por intermedio del canal asignado con *el gatekeeper*. El T1 requiere el uso de una señalización directa de llamada.
2. El *gatekeeper* confirma la admisión del terminal T1 y envía el mensaje: ACF hacia el terminal T1, indicando que utilice una señalización directa.
3. El terminal T1 envía vía el protocolo H.225 un mensaje de establecimiento de la llamada al terminal T2, solicitando una conexión.
4. El terminal T2 con un mensaje H.225 indicando que prosiga la llamada.

5. El terminal T2 tiene que registrarse con el *gatekeepe*r, para el cual envía un mensaje ARQ al *gatekeeper* mediante el canal del RAS.
6. El *gatekeeper* confirma el registro enviando un mensaje RAS ACF.
7. El terminal 2 alerta al terminal 1 que la conexión se ha establecido mediante un mensaje RAS de alerting.
8. El terminal T2 confirma el establecimiento de los mensajes mediante mensajes connect hacia T1 estableciendo la llamada.

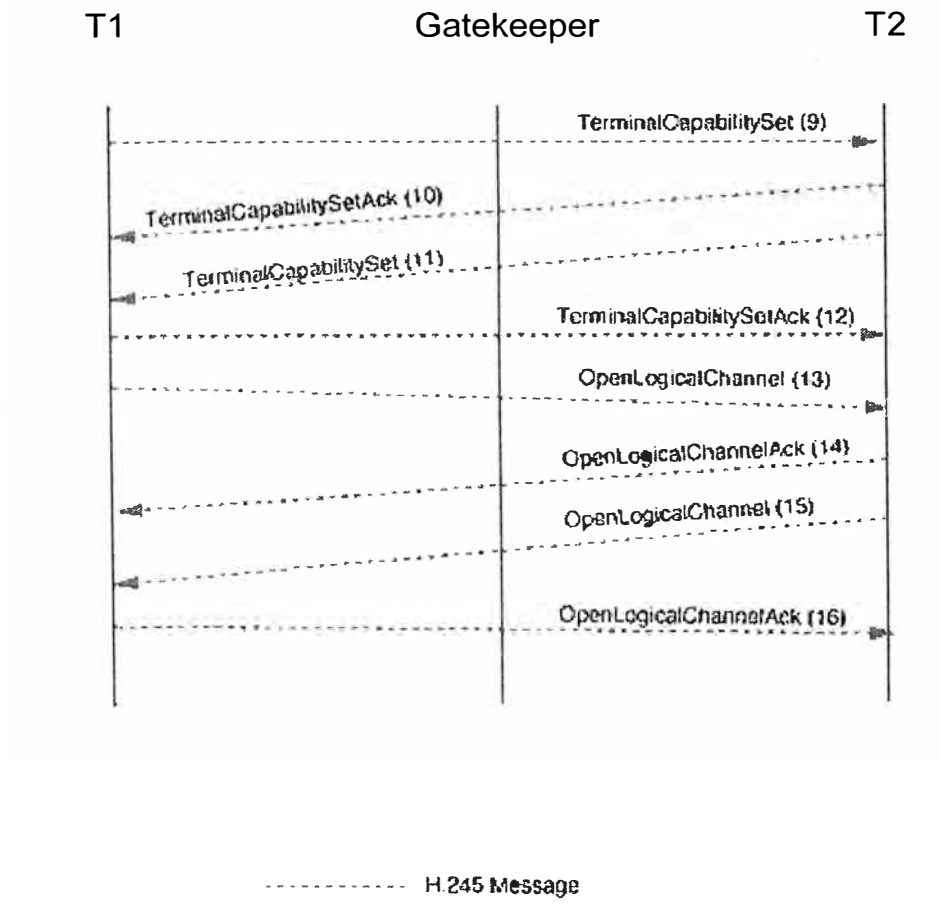


Figura 2.9 Flujo de control de señalización H.323

9. Un canal de control del H245 se establece entre T1 y T2. T1 envía el mensaje *TerminalCapabilitySet* solicitando la capacidad del terminalT2,

de igual manera el terminal T2 realiza lo mismo para intercambiar sus capacidades.

10. El T2 reconoce la capacidad de T1 enviando el mensaje *TerminalCapabilitySetACk*.
11. El T2 intercambia esta capacidad con T1 enviando un mensaje *TerminalCapacibilitySet*.
12. El T1 reconoce la capacidad de T2 enviando el mensaje *TerminalCapacibilitySetAck*.
13. T1 abre un canal multimedia con T2 enviando el mensaje *OpenLogicalChannel*.
14. T2 reconoce el establecimiento de un canal lógico unidireccional enviando el mensaje *OpenLogicalChannelAck*, el cual incluye la dirección de transporte RTP para ser utilizado en el envío de paquetes media stream y la dirección del canal RTCP desde donde va a recepcionar los mensajes desde T1.
15. T2 abre un canal media con T1 enviando el mensaje *OpenLogicalChannel*. La dirección de transporte del canal RTCP es incluida en el mensaje.
16. T1 reconoce el establecimiento de un canal lógico unidireccional desde T2 a T1 enviando el mensaje *OpenLogicalChannelAck*; también se incluye el reconocimiento de la dirección de transporte RTP localizado en T1, el cual va a ser utilizado por T2 para enviar RTP *media stream*. Se ha establecido una comunicación bidireccional media stream entre los 2

terminales. Se ilustra en la Figura 2.10 el flujo de control de H.323 para establecer el *media stream*.

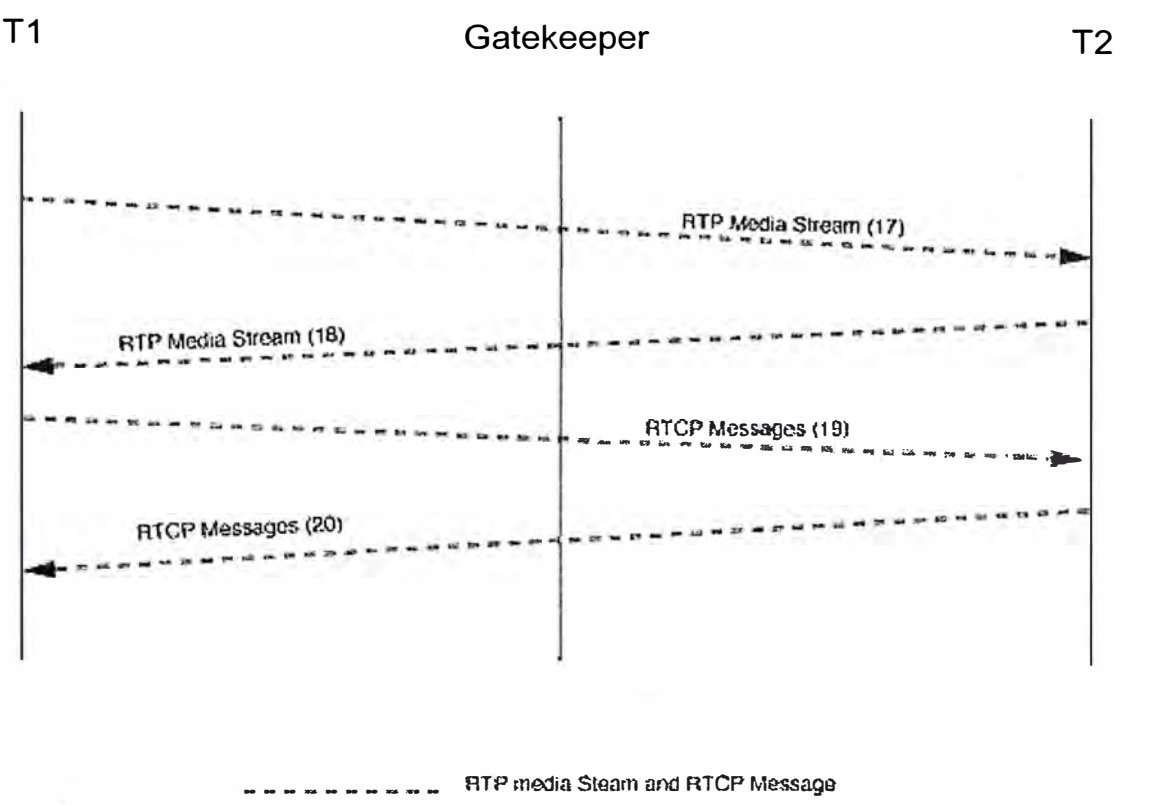


Figura 2.10 Flujo de control de H323

17. T1 envía los media stream mediante RTP encapsulado hacia T2
18. T2 envía los media stream mediante RTP encapsulado hacia T1
19. T1 envía mensajes RTCP hacia T2.
20. T2 envía RTCP mensajes hacia T1.

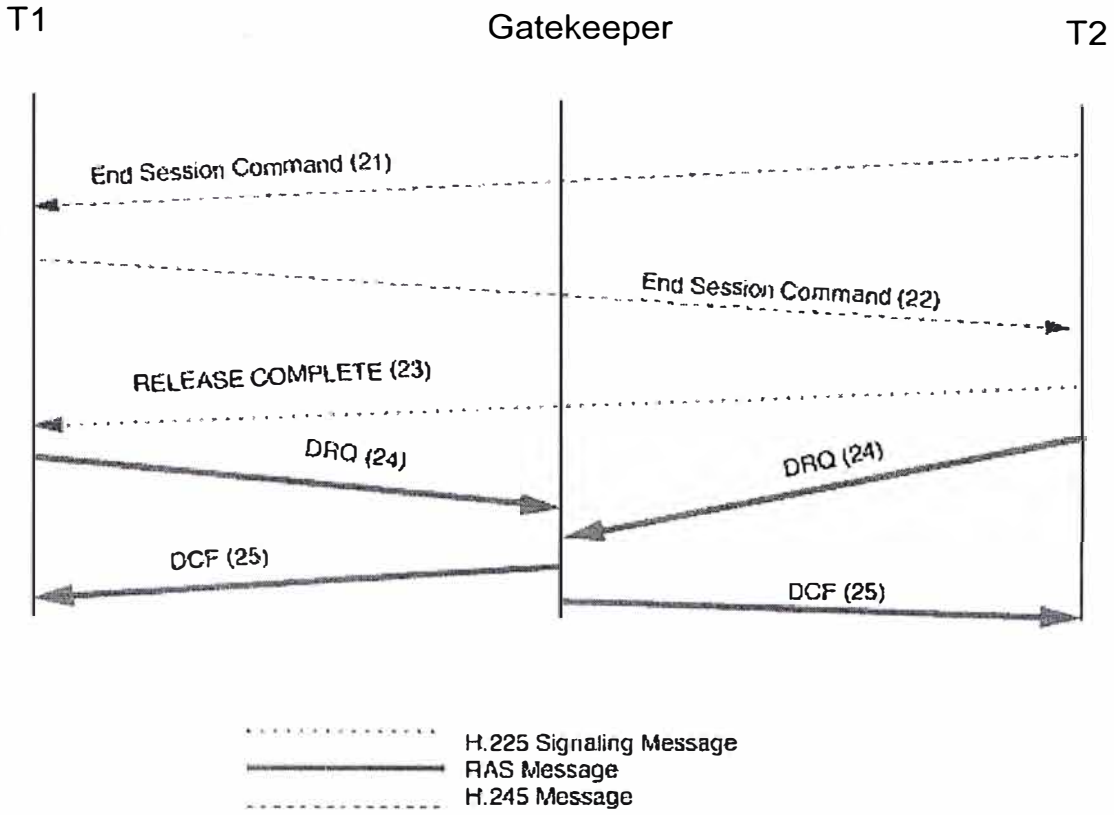


Figura 2.11. Liberación de la llamada H.323

21. T2 inicializa la liberación de la llamada, por lo que se envía el mensaje H.245 *EndSessionCommand* hacia T1.
22. T1 libera la llamada y confirma la liberación enviando el mensaje *EndSessionComand* hacia T2.
23. T2 completa la liberación de la llamada enviando un mensaje de liberación completada hacia T1.
24. T1 y T2 se liberan del *gatekeeper* enviando el mensaje RAS DRQ hacia el *gatekeeper*.
25. El *gatekeeper* libera los terminales confirmando mediante el mensaje DCF hacia T1 y T2.

2.2 Señalización SIP

2.2.1. Introducción

El protocolo SIP (*Session Initiation Protocol*) es un nuevo protocolo de control de señalización de la capa de aplicación que se utiliza para establecer, modificar y liberar sesiones multimedia. Fue desarrollado por el IETF (*Internet Engineering Task Force*) como parte de la Arquitectura de Conferencias Multimedia en Internet y fue diseñado para trabajar con otros protocolos de Internet tales como TCP/IP, UDP, DNS y otros.

Como su nombre lo indica es un protocolo que permite a dos puntos extremos establecer sesiones que pueden incluir diferentes tipos de datos tales como audio, video aunque actualmente se usa más para comunicaciones de audio (voz).

SIP incorpora elementos de dos Protocolos de Internet ampliamente usados: HTTP (*Hyper Text Transport Protocol*) usado en los navegadores web, y el SMTP (*Simple Mail Transport Protocol*) usado para el correo electrónico. Del HTTP recoge el diseño Cliente / Servidor y el uso de los URL (*Uniform Resource Locator*). El formato de un URL es: http://www.telefonica.com/5ess/). Del SMTP recoge el esquema de codificación de texto así como el uso de los *headers* que usamos cuando enviamos un correo electrónico: TO, FROM, DATE, SUBJECT.

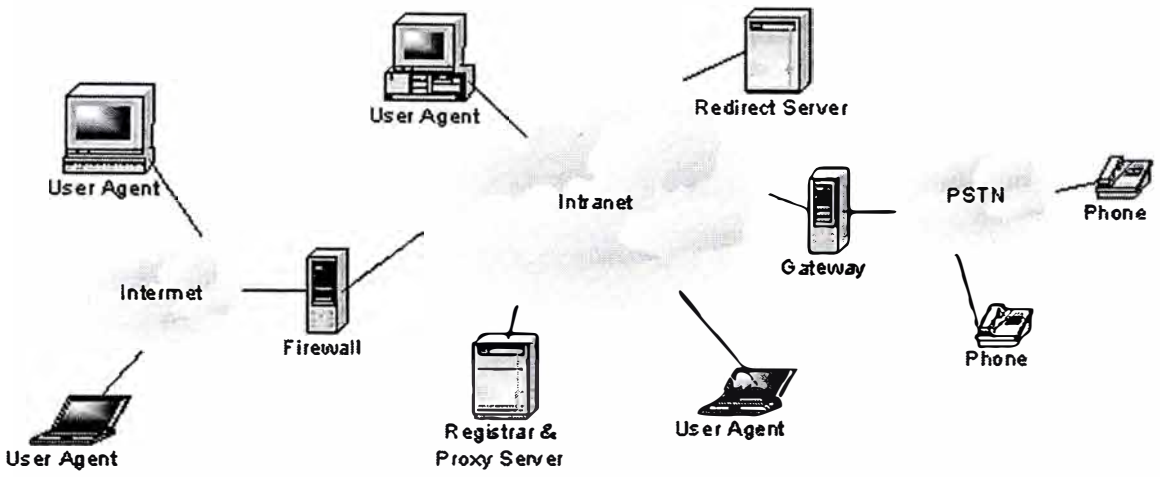


Figura 2.12 Red SIP

2.2.2. Componentes SIP

Los dos componentes de un sistema SIP son los agentes de usuario y los servidores de red.

2.2.2.1. Agentes de usuario

Los agentes de usuario son aplicaciones cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como cliente y servidor, respectivamente.

- Cliente. Inicia las peticiones SIP y actúa como el agente usuario del llamante.
- Servidor. Recibe las peticiones y devuelve las respuestas en nombre del usuario; actúa como el agente de usuario llamado.

2.2.2.2. Servidores de red

Se encuentran los siguientes:

- Servidor *Proxy*. Dispositivo intermedio que es capaz de responder y/o redireccionar mensajes de solicitud del agente usuario hacia el próximo

servidor SIP o a otro agente usuario dentro de la red, asimismo puede retener información para propósitos de facturación/contabilidad.

- Servidor de redirección (*Redirect Server*). Acepta las peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor. Numerosos saltos se pueden dar para alcanzar el destino final. La flexibilidad de SIP permite a los servidores contactar con externos *Location Servers* para determinar el usuario destino o las políticas de enrutamiento. Los servidores de redirección no aceptan llamadas ni tampoco procesan o reenvían peticiones SIP.

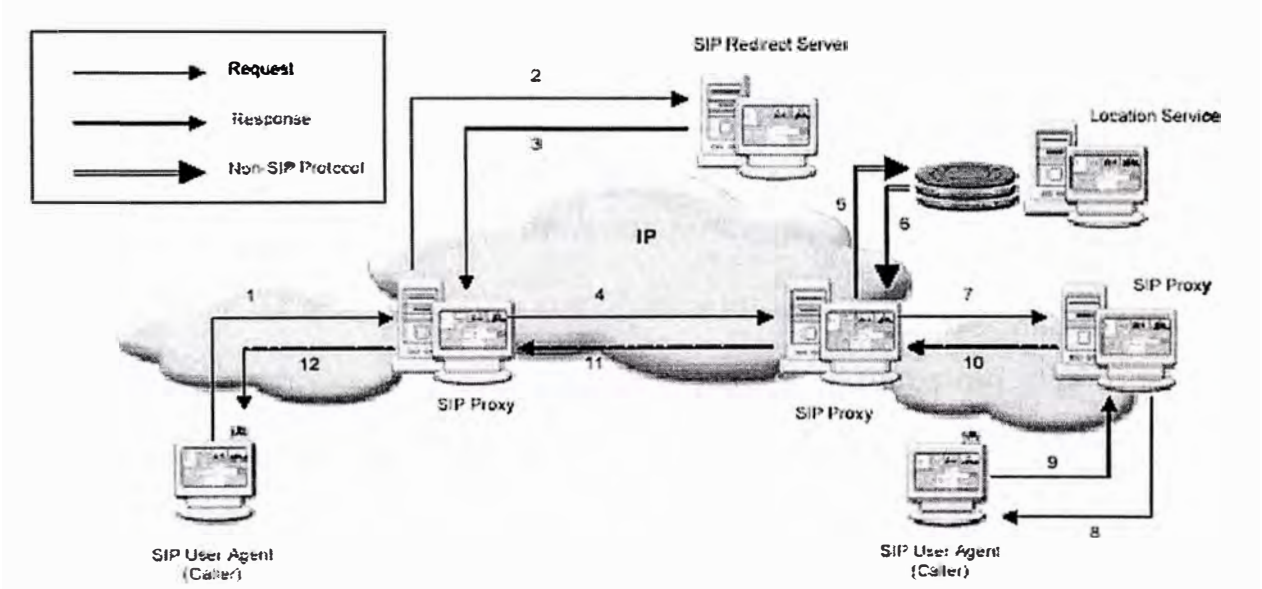


Figura 2.13 Inicio de una sesión

- *Registrar Server.* El Agente de usuario envía un mensaje de registro al SIP *Registrar Server* y el Servidor almacena la información de registro en un *Location Server* vía un protocolo no SIP. Una vez que la información es almacenada, el *Registrar Server* envía la respuesta apropiada de retorno al agente de usuario (*User Agent*).

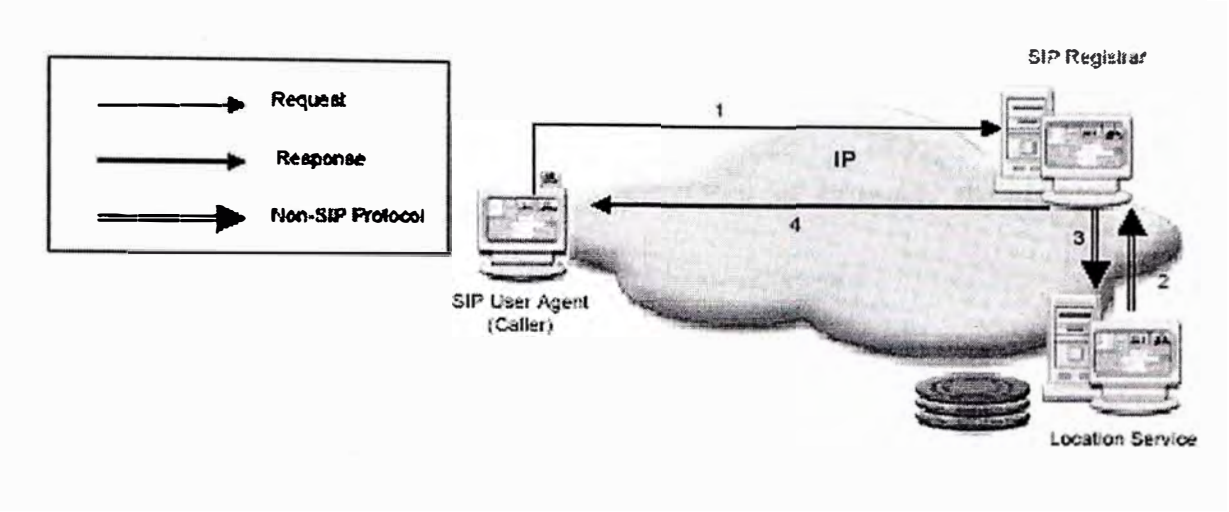


Figura 2.14. Registro SIP

2.2.3 Direccionamiento

Las direcciones SIP también llamadas localizadores universales de recursos (URL) SIP, existen en la forma de usuarios@hosts. Similar a una dirección de correo electrónico, un URL SIP se identifica por usuario@hosts. La parte de usuario de la dirección puede ser un nombre de usuario o un número de teléfono y la parte de *hosts* puede ser un nombre de dominio o una dirección de red. Se puede identificar a un URL SIP de un usuario por su dirección de correo electrónico. Estos ejemplos muestran dos posibles direcciones URL SIP:

Sip:ciscopress@cisco.com

Sip:4085262222@171.171.171.1

2.2.3.1 Localización de un servidor

Un cliente puede enviar una petición SIP directamente a un servidor *proxy* configurado localmente o bien a la dirección IP y puerto del correspondiente URL SIP. Enviar una petición SIP es relativamente fácil ya que la aplicación de sistema final conoce al servidor *proxy*. Enviar una

petición SIP de la segunda manera es algo mas complicado por las siguientes razones:

- El cliente debe determinar la dirección IP y el número de puerto del servidor al que va destinada la petición.
- Si el tipo de protocolo no está enumerado en el URL SIP pedido, el cliente debe primero intentar conectar utilizando el Protocolo de datagrama de usuario (UDP) o el protocolo para el control de transmisión (TCP).
- El cliente consulta el servidor de Sistema de denominación de dominio (DNS) para buscar la dirección IP del *hosts*. Si no encuentra ningún registro de dirección, el cliente es incapaz de localizar al servidor y no puede continuar con la petición.

2.2.3.1 Transacciones SIP

Cuando se ha resuelto el tema de la dirección, el cliente envía una o más peticiones SIP y recibe una o más respuestas desde el servidor especificado. Todas las peticiones y respuestas asociadas con esa actividad están consideradas como parte de una transacción SIP. Para una mayor simplicidad y coherencia, los campos de cabecera en todos los mensajes de petición coinciden con los campos de cabecera en todos los mensajes de respuesta.

Se pueden transmitir transacciones SIP en los protocolos UDP y TCP. En el caso de TCP, se pueden transportar todos los mensajes de petición y respuesta relacionados con una única transacción SIP sobre la misma conexión TCP. También se pueden transportar transacciones SIP separadas

entre las dos entidades sobre la misma conexión TCP. Si se utiliza UDP, la respuesta se envía a la dirección identificada en el campo de cabecera de la petición.

2.2.3.3. Localización de un usuario

La parte llamada puede desplazarse desde uno o varios sistemas finales a lo largo del tiempo. Puede moverse desde la red de área local (LAN) corporativa a una oficina en casa conectada a través de su proveedor de servicios de Internet (ISP) o a una conexión pública Internet mientras atiende a una conferencia. Por tanto, para los servicios de localización, SIP necesita acomodar la flexibilidad y la movilidad de los sistemas finales IP. Las localizaciones de estos sistemas finales pueden estar registradas con el servidor SIP o con otros servidores de localización fuera del ámbito de SIP. En este último caso el servidor SIP almacena la lista de localizaciones basadas en el servidor de localización exterior que está devolviendo múltiples posibilidades de *host*.

2.2.4. Mensajes SIP

Existen dos tipos de mensajes los cuales se dividen en mensajes de solicitud también llamados métodos, y mensajes de respuesta. Cada mensaje contiene una cabecera que describe los detalles de la comunicación. SIP es un protocolo basado en texto con una sintaxis de mensajes y campos de cabecera idénticos al Protocolo de transferencia de hipertexto (http). Los mensajes SIP se envían sobre los protocolos TCP ó UDP con múltiples mensajes transportados en una única conexión TCP o datagrama UDP.

2.2.4.1 Peticiones de mensajes

La comunicación SIP presenta seis tipos de peticiones de mensaje. Estas peticiones permiten que los agentes de usuarios y servidores de red localicen, inviten y administren llamadas. Los cuales se muestran en la Tabla 2.1.

Mensaje	Función
INVITE	Iniciar llamada
ACK	Confirmar respuesta final
BYE	Terminar y transferir llamada
CANCEL	Cancelar búsquedas y timbrado
OPTIONS	Facilidades soportadas por extremo remoto
REGISTER	Registrarse con el Servidor de Localización

Tabla 2.1 Peticiones de Mensaje

2.2.4.2 Respuestas de mensajes

Las respuestas a los mensajes SIP están basadas en la recepción y análisis de la petición correspondiente. Se envían como respuesta a una petición e indican si la llamada ha tenido éxito o ha fallado, incluido el estado del servidor. En la Tabla 2.2 se muestran las respuestas SIP.

Tabla 2.2 Respuestas SIP

Código	**Función**
1XX	PROVISIONAL
100	CONTINUE
180	RINGING
2XX	SUCCESS
200	OK
3XX	REDIRECT
300	MULTIPLE CHOICE
301	MOVED PERMANENTLY
302	MOVED TEMPORALY
4XX	CLIENT ERROR
400	BAD REQUEST
5XX	SERVER ERROR
500	SERVER INTERNAL ERROR
501	NOT IMPLEMENTED
502	BAD GATEWAY
503	SERVICE UNAVAILABLE
505	VERSION NOT SUPPORTED
6XX	GLOBAL FAILURE
600	BUSY
601	DECLINE
604	DOES NOT EXIST
606	NOT ACCEPTED

2.2.4.3. Estructura mensaje SIP

En la Figura 2.15 se muestra la sintaxis para un mensaje SIP.

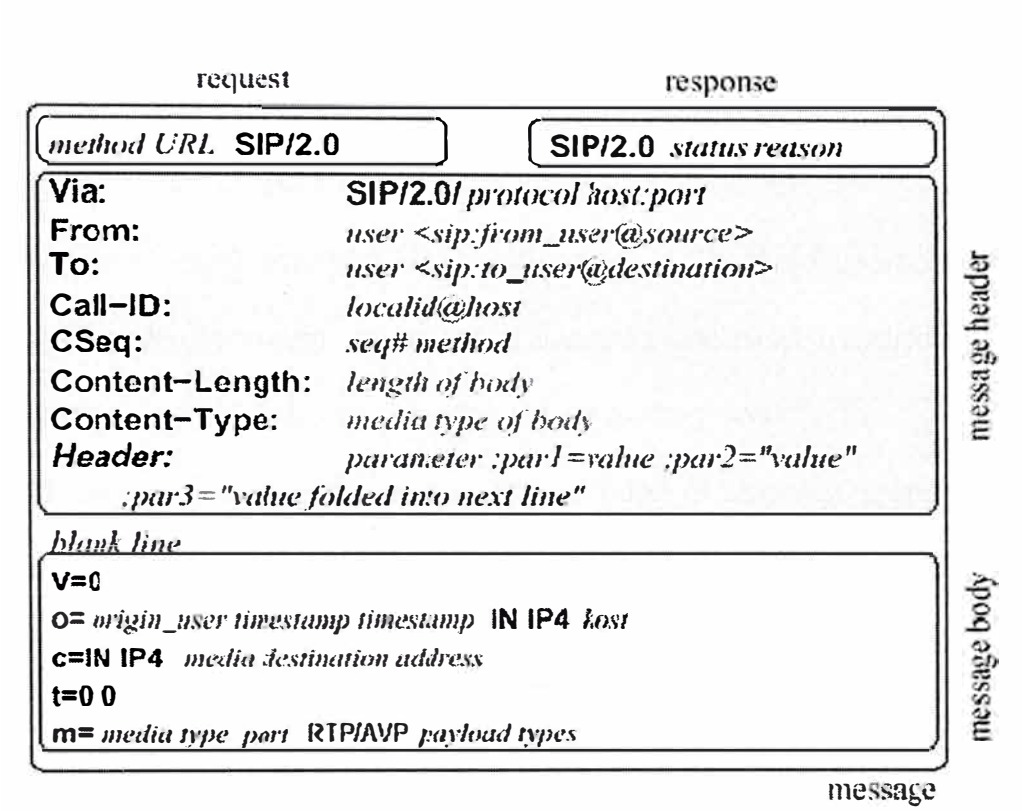


Figura 2.15 Sintaxis SIP

2.2.5. Operatividad básica de SIP

Los servidores SIP manejan las peticiones entrantes de dos maneras. Esta operatividad básica se fundamenta en invitar a un participante a una llamada. Los dos modos básicos de operar del servidor SIP son los siguientes:

- Servidores *proxy.*
- Servidores de redirección.

2.2.5.1 Ejemplo de servidor *proxy*

El intercambio de comunicación para el método INVITE utilizando el servidor *proxy* se ilustra en la Figura 2.16.

Los pasos operacionales en el modo *proxy* que se necesitan para que una llamada de doble vía tenga éxito son los siguientes:

1) El servidor *proxy* acepta la petición INVITE del cliente.
2) El servidor *proxy* identifica la localización utilizando las direcciones y los servicios de localización proporcionados.
3) Se emite una petición INVITE a la dirección de la localización devuelta.
4) El agente de llamadas de la parte llamada alerta al usuario y devuelve una indicación de éxito al servidor *proxy* peticionario
5) Una respuesta OK (200) es enviada desde el servidor *proxy* a la parte llamante.
6) La parte llamante confirma la recepción emitiendo una petición ACK, que es transmitida por el *proxy* o enviada directamente a la parte llamada.

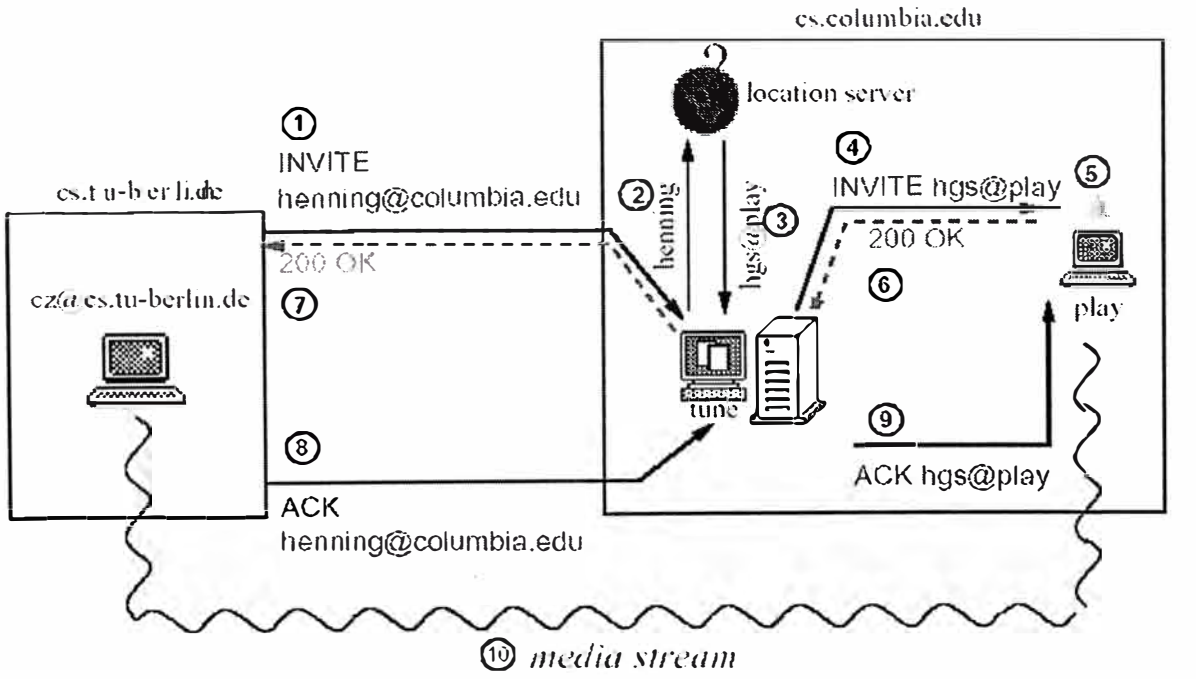


Figura 2.16 Modo de operación *proxy*

2.2.5.2 Ejemplo de servidor de redirección

El intercambio de protocolo para la petición INVITE que utiliza el servidor de redirección aparece en la Figura 2.17.

Los pasos operacionales en el modo de redirección (*redirect*) para que una llamada de doble vía tenga éxito son los siguientes:

1) El servidor de redirección acepta la petición INVITE desde la parte llamante y contacta los servicios de localización con la información facilitada.
2) Cuando se ha localizado al usuario, el servidor de redirección devuelve la dirección directamente a la parte llamante. A diferencia del servidor *proxy*, el servidor de redirección no emite ningún INVITE.
3) El agente de usuario envía un ACK al servidor de redirección confirmando que la transacción se ha completado.
4) El agente de usuario envía una petición INVITE directamente a la dirección devuelta por el servidor de redirección.
5) La parte llamada proporciona una indicación de éxito (200 OK) y la parte llamante devuelve un ACK.

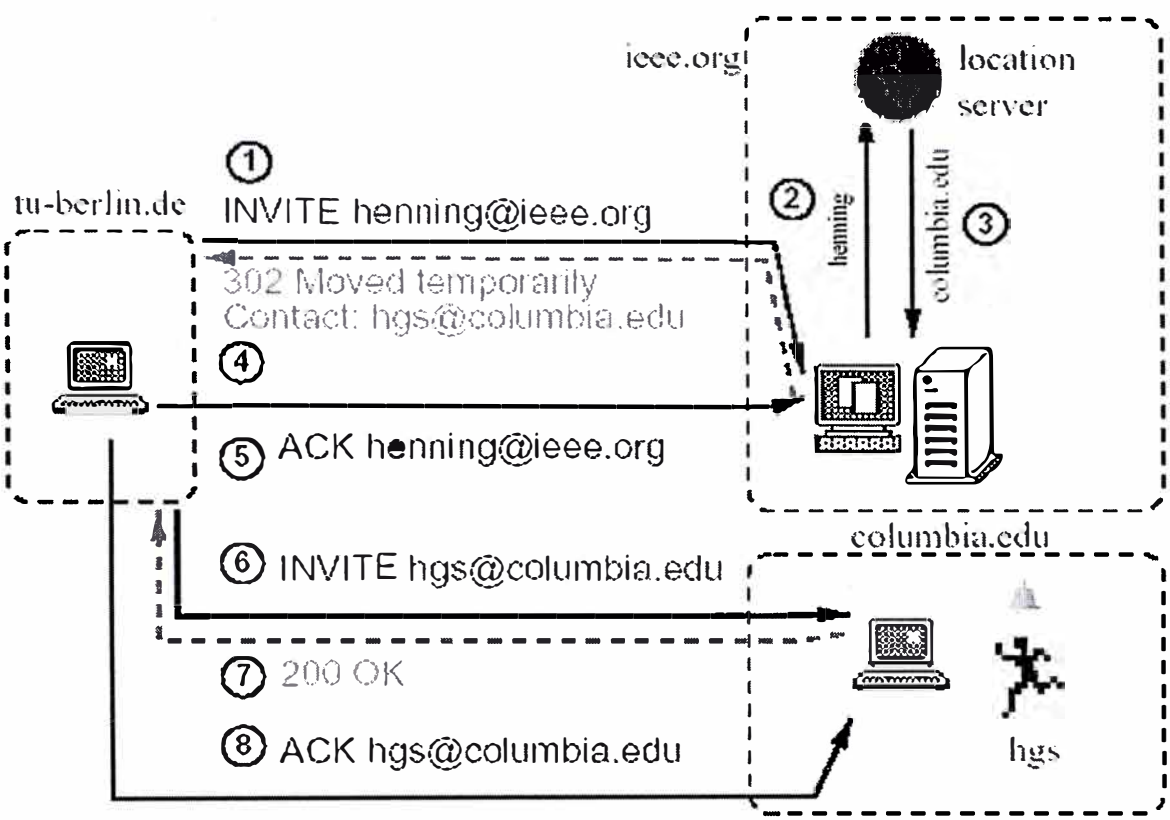


Figura 2.17. Modo de operación de redirección.

CAPITULO III
REDES DE NUEVA GENERACION – SOLUCION DE 3Com VoIP

3.1. Introducción

La telefonía IP se está convirtiendo en una tecnología muy utilizada para la transmisión de voz según lo evidenciado por el mercado en productos computarizados de telefonía. Esto es posible por los recientes avances en diversas tecnologías. En el campo de procesamiento de señales, los nuevos estándares de compresión permiten que las señales de voz sean codificadas a bajas tasas de bits, manteniendo una calidad aceptable para los servicios de telefonía. Por otra parte, el incremento de ancho de banda en las redes de acceso IP asociado con el incremento de la capacidad de enrutamiento en los "backbone" IP hacen posible alcanzar un nivel de interacción similar al ofrecido por las redes de conmutación de circuitos. Además, el crecimiento dramático de terminales IP con gran potencia de procesamiento, memoria, y capacidad de multimedia permiten que los servicios de voz basados en IP puedan desplegarse a gran escala.

Por otra parte, la PSTN ha hecho logros impresionantes en términos de cobertura, confiabilidad, y facilidad de empleo. La disponibilidad del servicio es tal que los usuarios están acostumbrados a recibir la señal de marcar, cada vez que levantan el teléfono, por lo que tratar de obtener éstas características en una red IP, es uno de los principales desafíos de la

ingeniería. Una parte de los servicios de voz que son ofrecidos por la PSTN emigrará a una tecnología basada en IP. Sin embargo, la telefonía IP y los servicios de la PSTN coexistirán por un tiempo considerable. Por lo que la interconexión entre los usuarios de telefonía del IP y los usuarios de la PSTN es esencial.

Asimismo, la red IP se ha convertido en una alternativa deseable para aquellos usuarios telefónicos que desean ahorrar dinero en sus facturas telefónicas de llamadas de larga distancia o para aquellos que están a la mitad de una sesión de servicio de acceso remoto y desean conversar telefónicamente o enviar / recibir una transmisión de fax sin interrupción. La telefonía IP permite a los Proveedores de Servicio ofrecer un mejor servicio en llamadas de Larga Distancia y a un menor costo, por medio de la utilización de las técnicas de compresión.

La Plataforma de Telefonía IP CommWorks es una red de Conmutación de Paquetes y no existe conexión fija entre dos puntos; la voz se convierte a datos y viaja a través de la red en pequeños paquetes que son reensamblados por el Media Gateway destino. Esta Plataforma CommWorks es más eficiente que los sistemas tradicionales debido a que un circuito no se mantiene conectado durante el tiempo que dura la llamada, los paquetes fluyen solo cuando hay información de voz que transmitir.

Como se observa en la Figura 3.1, la Plataforma CommWorks consiste de tres hileras o capas convergentes que dirigen la conectividad universal con la intervención de protocolo de señalización y un ambiente abierto de desarrollo, basado en normas para la creación de aplicaciones y

servicios. El uso de interfaces estándar de programación de aplicaciones (APIs) permite personalizar las aplicaciones de desarrollo de servicios.

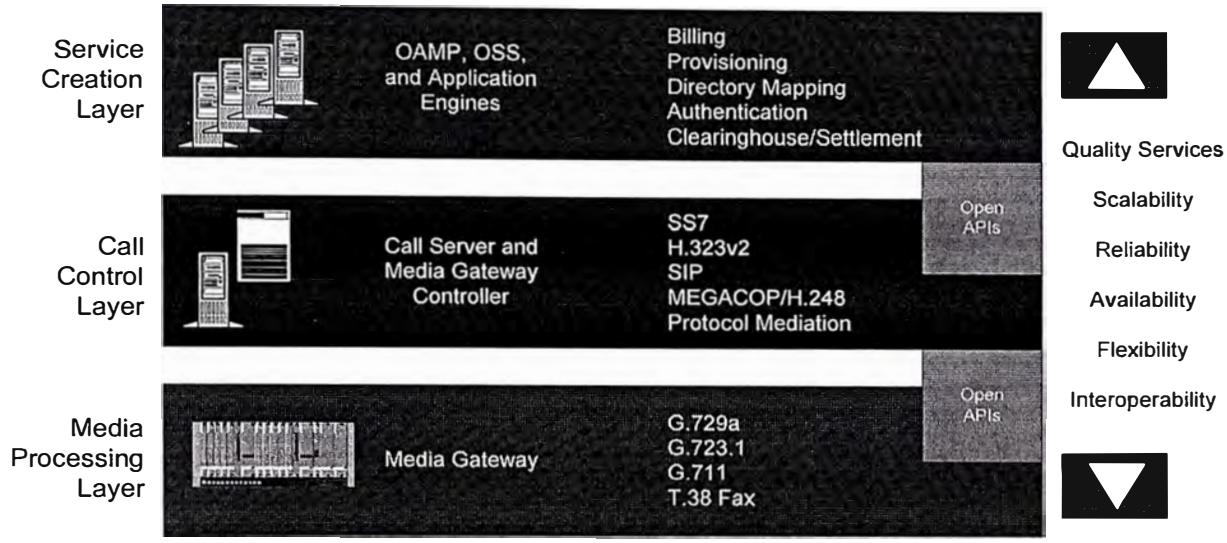


Figura 3.1. Arquitectura Modular de 3Com.

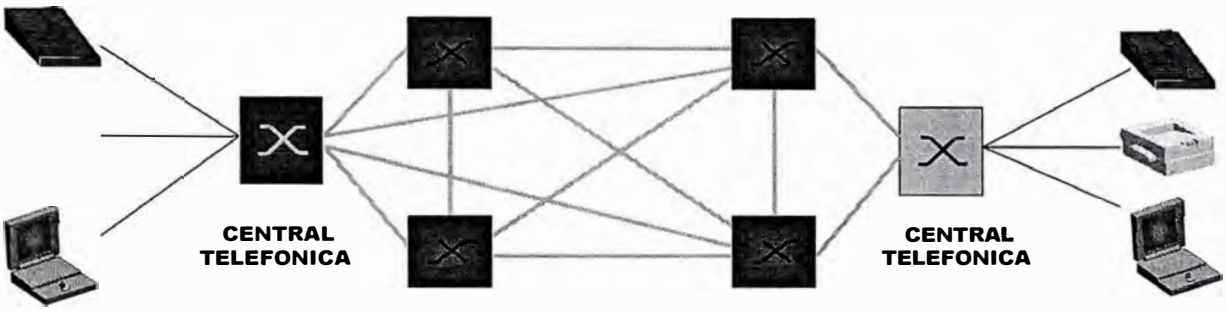
En la Capa 1 de procesamiento de medios, el Media Gateway (MG) Total Control 1000 brinda conectividad universal entre las redes IP y PSTN.

En la Capa 2 de Señalización y Control de Llamadas, se realizan en su conjunto un servicio de Softswitch de primera generación, basados en Gatekeepers, SIP Proxy Servers, SS7 Signaling Gateways y Softswitch (o Media Gateway Controller – MGC) de nueva generación, esta capa proporciona señalización universal y control de llamadas a través de la transmisión de protocolo.

En la capa 3 de creación de servicio, se provee la capacidad para desarrollar e implementar servicios, como por ejemplo la mensajería unificada.

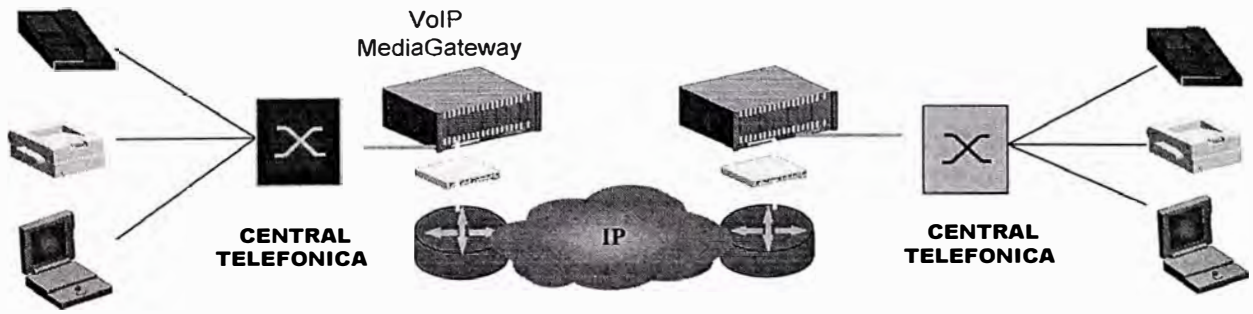
Una de las caracteríscas de esta Plataforma es que soporta la funcionalidad *Transparent Trunking*, como uno de los requerimientos de

convivencia e interfuncionalidad entre la red PSTN y la red de Nueva Generación. Esta funcionalidad permite que el sistema de 3Com provea al cliente, acceso directo al backbone de la IP, en este caso el usuario llamante, así como el llamado desconocen que la red de transporte es IP. Según los gráficos de las Figuras 3.2 y 3.3 observamos la integración y la convergencia de las redes de conmutación de paquetes y de circuitos.



Red del Operador

Figura 3.2 Red tradicional de conmutación de circuitos



Red IP Gestionada por el Operador

Figura 3.3 Red integrada de los servicios de voz

3.2. Solución de 3Com - Revisión del Sistema

3.2.1 Introducción

Este capítulo describe el equipamiento de la red y la infraestructura asociada. Así mismo muestra el funcionamiento general de la red, detallando sus componentes, haciendo énfasis en el esquema físico y bosquejo de la topología de cada Nodo.

La Figura 3.4 muestra los componentes de la Plataforma de Telefonía IP y la interacción entre ellos :

Estos componentes son:

- El Media Gateway
- El Gateway SS7, si se usa SS7
- El Proxy Server (Aplicaciones SIP)
- El Gatekeeper (Aplicaciones no SIP)
- Los Back-End Servers: Directory Server, Billing Support y el Accounting Server.
- El Provisioning Server o el Web Configuration Server (La interface basada en la Web para el Directory Server)

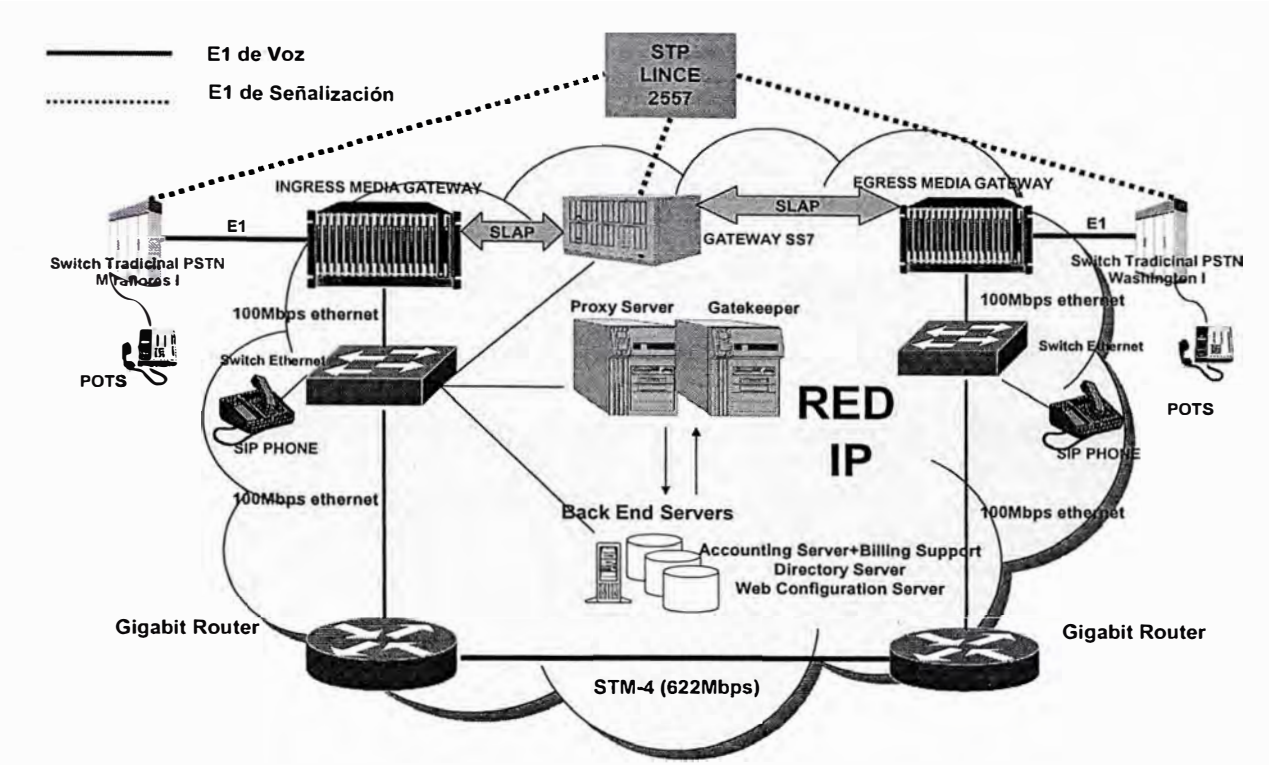


Figura 3.4 Componentes de la Plataforma de Telefonía IP

3.2.2 Flujo de Tráfico

Cuando una llamada se establece, el tráfico de voz, fax, ó módems fluye entre el Media Gateway de Ingreso y el de Egreso.

El tráfico de audio generado en el lado de ingreso fluye a través de un Switch Tradicional PSTN a través de un E1 canalizado hacia la Tarjeta Hiper Digital Signal Processor (DSP) del Media Gateway. La codificación del audio en el Hiper DSP está en el formato G.711 (64Kbps) ó G.723.1 (5.3Kpbs), y luego el audio es enviado a través de un Packet Bus en el Media Gateway hacia una Tarjeta EdgeServer Pro que corre bajo Windows NT. La tarjeta EdgeServer Pro envía el audio a través de su interface Ethernet de 100 Mbps sobre una red IP hacia el Media Gateway de Egreso.

Entre los Media Gateways, la data fluye encapsulada dentro de los protocolos RTP/UDP/IP.

En el Media Gateway de Egreso, la Tarjeta EdgeServer Pro recibe el audio a través de su puerto Ethernet de 100 Mbps y lo envía a través del Packet Bus interno hacia la Tarjeta Hiper DSP. La tarjeta Hiper DSP envía el audio en un canal de un E1 que está interconectado a un Switch Tradicional PSTN, para luego salir hacia su destino.

3.2.3 Flujo de Trafico con SS7 habilitado

EL diagrama de la Figura 3.4 también ilustra el flujo de una llamada en una red de Voz sobre IP con una red de SS7.

Como se observa en la Figura 3.4, una solicitud de servicio puede iniciarse a través de un teléfono análogo, referido a POTS (Plain Old Telephone Service), o un modem de datos/fax conectado a una línea POTS ó un telefono SIP. La solicitud de una línea POTS es recibida por un Switch PSTN. El Switch PSTN tiene troncales de señalización SS7 (mostrados con líneas punteadas) separadas de las troncales de canales de voz. El switch PSTN utiliza un mensaje de señalización sobre un *Link* hacia el *Signalling Transfer Point* (STP), el cual indica el intento de establecer una llamada.

El STP es un Switch de paquetes de datos que conmuta los mensajes de señalización hacia un destino apropiado. El mensaje de señalización del Switch PSTN especifica la dirección de destino del Gateway de señalización de la red de VoIP (conocido como Gateway SS7) y también especifica la troncal DS0 (CIC) de canal de voz, que el Switch PSTN ha reservado para la nueva llamada. El STP enruta el mensaje de señalización de la nueva

llamada hacia el Gateway de Señalización en la red de VoIP. Los mensajes de señalización usan el protocolo ISUP sobre un protocolo de red confiable.

El Gateway de señalización VoIP de recepción traduce el mensaje ISUP a un mensaje desarrollado por 3Com (protocolo propietario SLAP) y lo transporta sobre la red IP al Media Gateway apropiado (Media Gateway Ingress). El Media Gateway interpreta el mensaje de señalización SLAP y lo asocia con el canal reservado del E1 (DS0), posteriormente procesa la solicitud de establecimiento de la llamada como si fuera un mensaje de señalización del E1 ISDN PRI (Canal D).

Si el intento de la llamada se origina desde el Gateway de Señalización de la red VoIP hacia la red PSTN, el Gateway SS7 reserva una troncal de un E1 del Media Gateway elegido y convierte esa información en un mensaje de establecimiento de llamada (IAM) hacia el señalizador del Switch PSTN.

El Gateway SS7 usa el protocolo SLAP (Signaling LAN Application Protocol) para enlazar la Red SS7 con el Media Gateway (Ingress Media Gateway y Egress Media Gateway). SLAP es la interface entre el Media Gateway y el Gateway SS7. Según la Figura 3.4 el SLAP reemplaza el canal D de Señalización que normalmente existe en una interface ISDN PRI, asimismo define mensajes que facilitan el inicio del Sistema, shut down, y recuperación de errores. SLAP es un software propietario de 3Com.

En las Figuras 3.5 y 3.6 observamos el interfuncionamiento para SIP y H323 respectivamente, para el caso en que el abonado llamante inicia la desconexión.

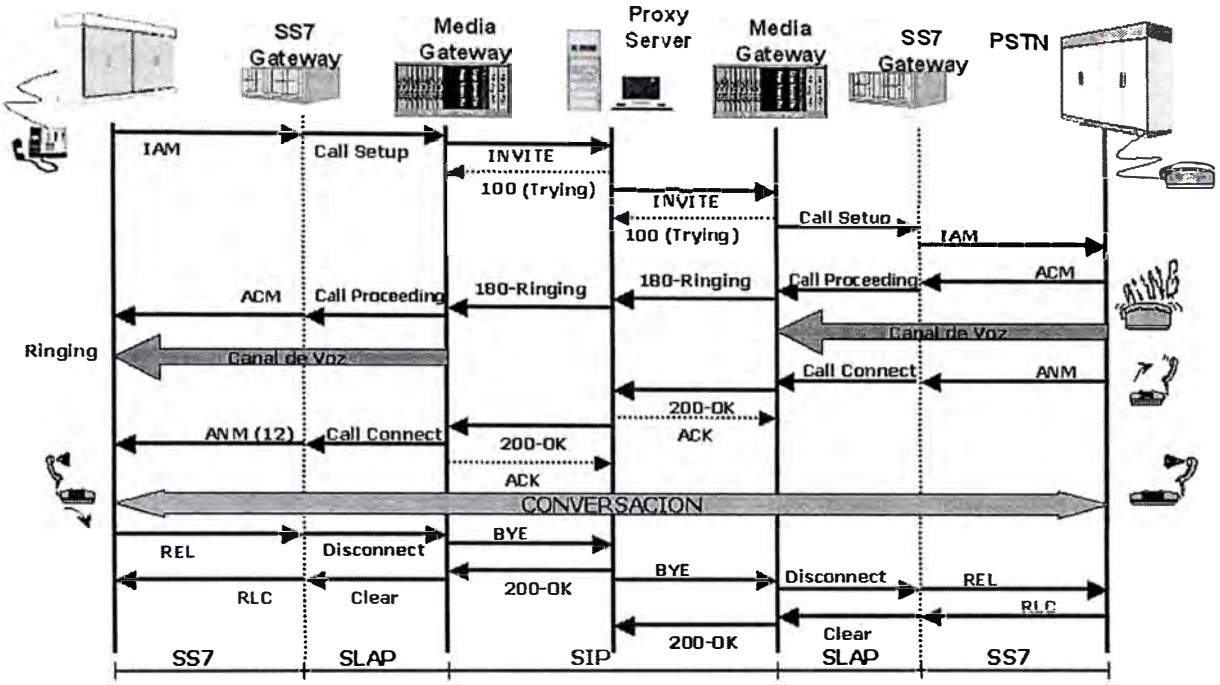


Figura 3.5 Interfuncionamiento SS7 – SIP

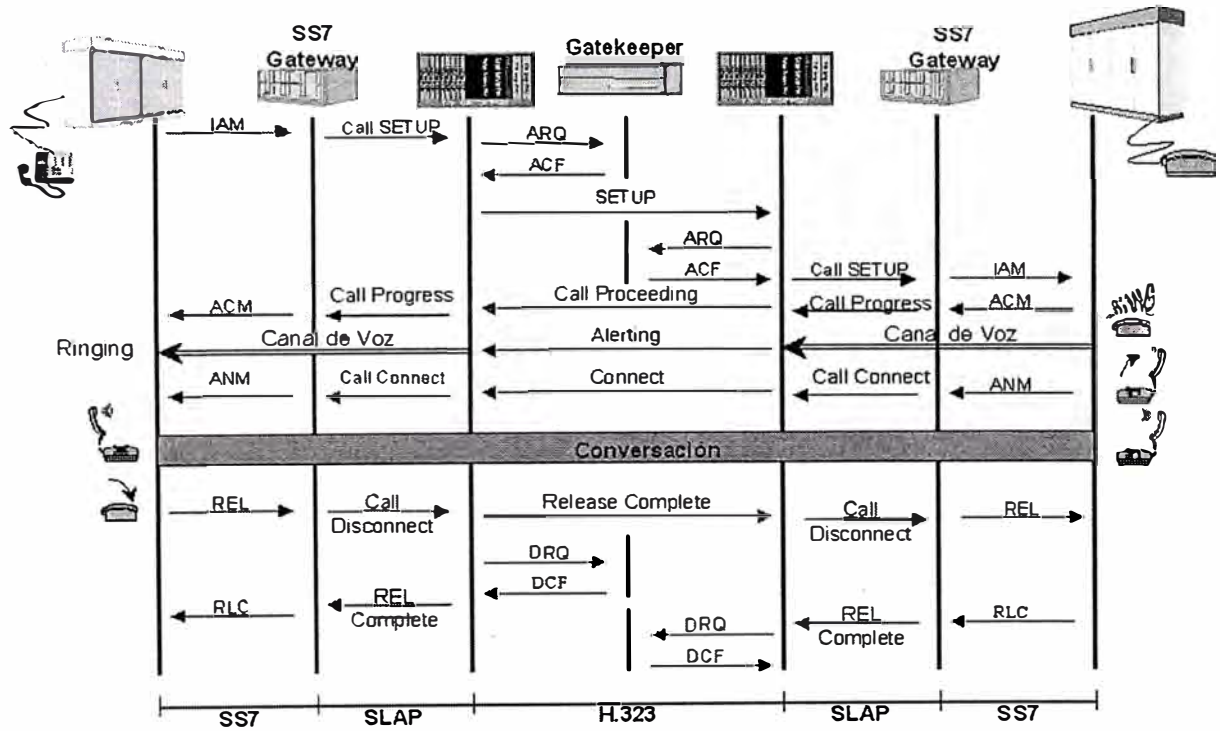


Figura 3.6 Interfuncionamiento SS7 – H323

3.3 Topología de la Red

A continuación mostramos la topología de nuestra red basada en equipos 3Com.

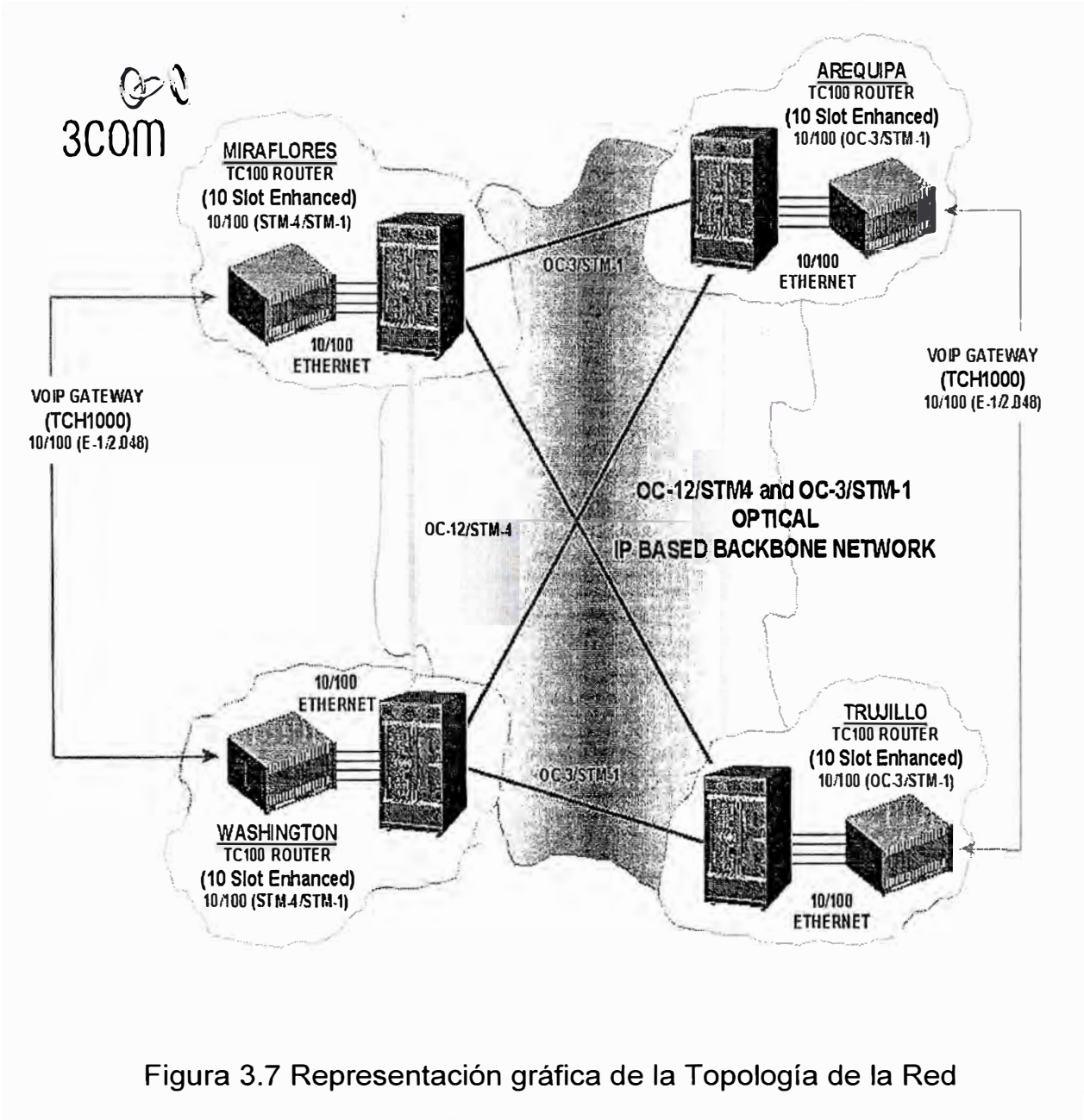


Figura 3.7 Representación gráfica de la Topología de la Red

Asimismo mostramos en la Figura 3.8 el escenario de pruebas y la interconexión con las centrales de conmutación.

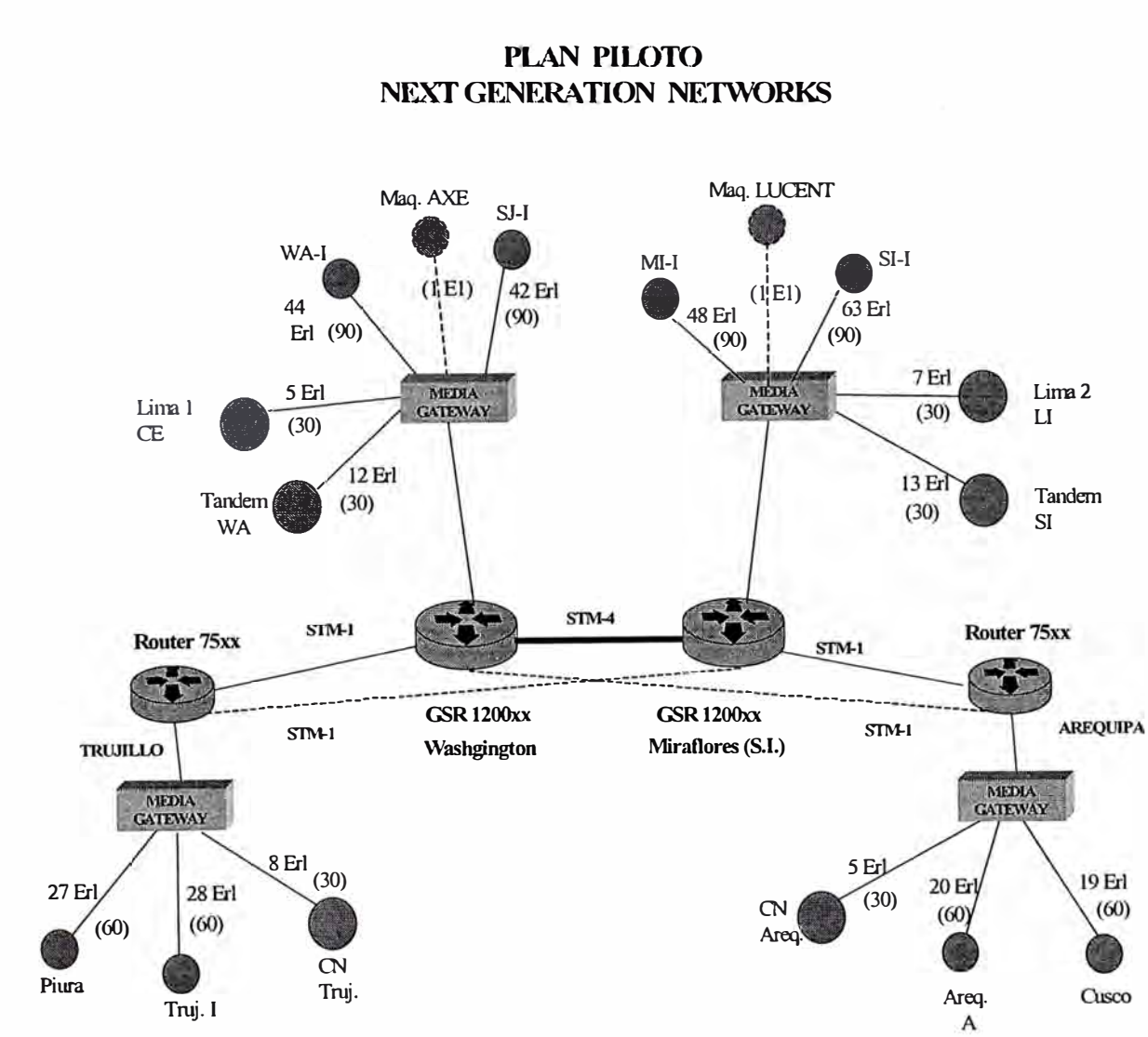


Figura 3.8 Interconexión de la Red IP con las centrales de Conmutación.

3.4 Hardware de la Red / Descripción de los equipos

3.4.1 Equipamiento – VoIP Gateways

En cada uno de los Nodos (Miraflores, Arequipa, Washington y Trujillo) se instaló el siguiente equipamiento.

- Un CommWorks Total Control 1000 Gateway.
- Un CommWorks Total Control 100-10 Router.
- Un 3Com 3900 10/100 Ethernet Switch
- Un E-1 120/75 ohm Patch Panel
- Un Cybex Video Switch

3.4.1.1 CommWorks Total Control 1000 Media Gateway.

El Media Gateway (MG) Total Control 1000 otorga a los usuarios la facilidad de mantener conversaciones telefónicas con una red IP como medio de transporte antes que la red telefónica pública conmutada (PSTN) suministrando la interfaz entre el circuito local conmutado y la red IP. Las llamadas de clientes telefónicos son transportadas al MG a través de Channelized/PRI T1/E1 o Inter-Machine Trunks (IMTs). Una vez establecida la llamada, el audio se transporta de los usuarios telefónicos al MG. Luego, la señal análoga de audio es procesada dentro del magazín con un CODificador – DECodificador (Codec) y transformada en una corriente comprimida digital de audio en forma de paquetes. Esta corriente comprimida de audio es encapsulada dentro del RTP/UDP/IP y transmitida en la red de paquete a un Gateway remoto ubicado en las inmediaciones del teléfono remoto. (La Figura 3.9 muestra la configuración del MG).

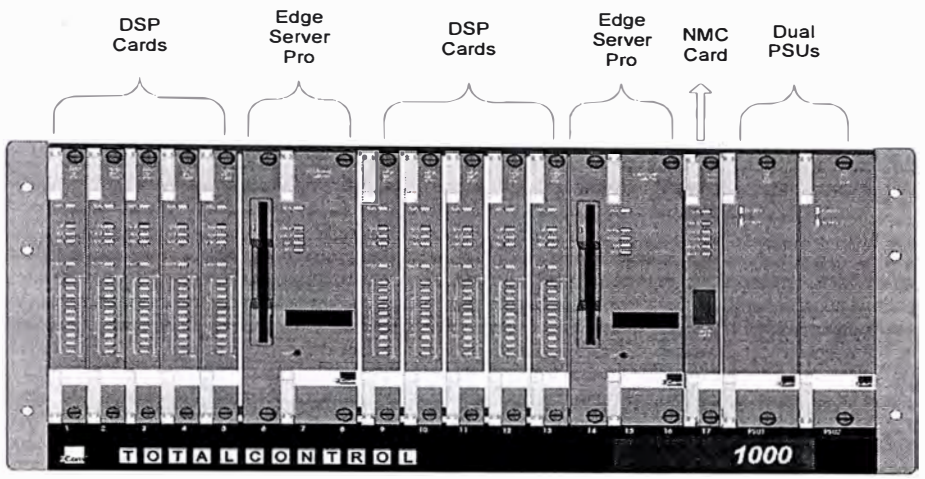


Figura 3.9 Media Gateway Total Control 1000 de 3Com.

El Media Gateway Total Control 1000 tiene las siguientes características:

- Chasis de alta densidad, compatible con NEBS (240/300 T1/E1 llamadas por 8.75" unidad con redundancia de Gateway – que escala hasta un máximo de 312/390 T1/E1 llamadas por Gateway).
- Fax sobre IP (FoIP) de Tiempo Real con T.38 y G3 fax.
- Relay de datos en banda vocal a través de G.711 Codec.
- Interfaces T1 y E1/PRI & E1/MFC R2 o IMT PSTN.
- Interfaces 10/100BaseT Ethernet LAN.
- Soporte de Codec G.723.1, G.729a y G.711 PCM .
- Detección DTMF.
- Módulo de Respuesta Vocal Interactivo (Interactive Voice Response - opcional).
- Generación (vía CDRs) y entrega de registros de facturación.
- SNMP administrable (incluye la gestión RTP).
- Generación de registros de eventos y estadísticas.
- Soporte API en una interfaz estándar.

- Capacidad de proveer servicios de VoIP y FoIP de tiempo real en el mismo chasis.
- Capacidad de soportar una combinación de servicios SIP o H.323 en el mismo chasis.

La Arquitectura del MG está diseñado con un software altamente modular con tres componentes principales, que se enumeran a continuación:

- El bloque funcional central.
- La interfaz programadora de aplicación (API).
- El software DSP.

3.4.1.1.1. Funciones Centrales de Telefonía IP

Estas funciones son básicas para la plataforma y proveen la estructura subyacente que permite al Gateway operar en forma adecuada. Esta capa contiene stacks de protocolo, media stream handlers, manipuladores de las solicitudes vocales y funciones de comando y control general del sistema. También contiene manipuladores de transporte de datos internos para mover las corrientes de medios y control entre los módulos dentro del Gateway. La Figura 3.10, muestra como están integradas las funciones Core IP Telephony al sistema.

3.4.1.1.2 Soporte de Application Programming Interface (API)

El MG soporta un API abierto, permitiendo a 3Com integrarse perfectamente con aplicaciones de terceros. Esta arquitectura abierta le permite desarrollar rápidamente e integrar aplicaciones personalizadas al sistema de Telefonía IP CommWorks IP.

Además de los ya conocidos Win32 APIs tales como TAPI, Winsock 2 y otros, los usuarios pueden aprovechar las ventajas de una gran variedad de herramientas de desarrollo de Windows NT para cambiar aplicaciones dentro de un ciclo muy corto. Las siguientes funcionalidades están disponibles para la implementación del servicio en el MG a través del API abierto y sólido:

- Procesamiento de llamadas (lado LAN y lado SCN)
- Control de conferencia.
- Respuesta Vocal Interactiva (IVR).
- Procesamiento de registros de facturación (realizado a través de la comunicación con el Gatekeeper o SIP Proxy)
- Gestión de autenticación del usuario (realizado a través de la comunicación con el Gatekeeper o SIP Proxy)
- Servicios de directorio (realizados a través de la comunicación con el Gatekeeper ó SIP Proxy)
- Inicialización y configuración del sistema
- Notificación y manejo de errores / fallas
- Monitorización y reinicio del procesamiento
- Recolección de estadísticas de llamadas

El objetivo del API es permitir que los proveedores de servicios tengan la opción de desarrollar sus propias aplicaciones de valor agregado para el Gateway y Gatekeeper/SIP Proxy.

La Figura 3.10 muestra la forma en que los API's pueden integrarse a las funciones Core IP Telephony para proveer una solución completa. Además del API, la solución CommWorks también soporta el control remoto de aplicación a través del Remote Procedure Calls (RPCs). El RPC permite a los clientes remotos controlar las actividades de la plataforma. Estos RPCs son adicionales al procedimiento estándar de llamadas remotas del Windows NT.

3.4.1.1.3 Software Total Control 1000 DSP

Algunas de sus principales características son

- El suministro de poder de procesamiento paralelo masivo distribuido (más de 1.200 MIPS por tarjeta) con la capacidad para co-procesar diferentes funciones tales como transmisión Codec/modem/fax, simultáneamente – brindándole la máxima flexibilidad.
- Capacidad de codificación / decodificación y carga Codec dinámica.
- La funcionalidad bit-intensive H.323 ha sido incorporada y distribuida en el área DSP.
- Codecs vocales de alta calidad.

El software DSP, además de manejar todas las funciones de procesamiento de Codec vocales también brinda:

- Cancelación de eco compatible con G.168
- Regulador de Jitter para compensar las discrepancias en las demoras por medio de un “mayor esfuerzo” realizado por la red IP.
- Supresión de silencio para detener la transmisión de paquetes durante períodos en los que no se habla.

- Comfort noise generation (CNG)

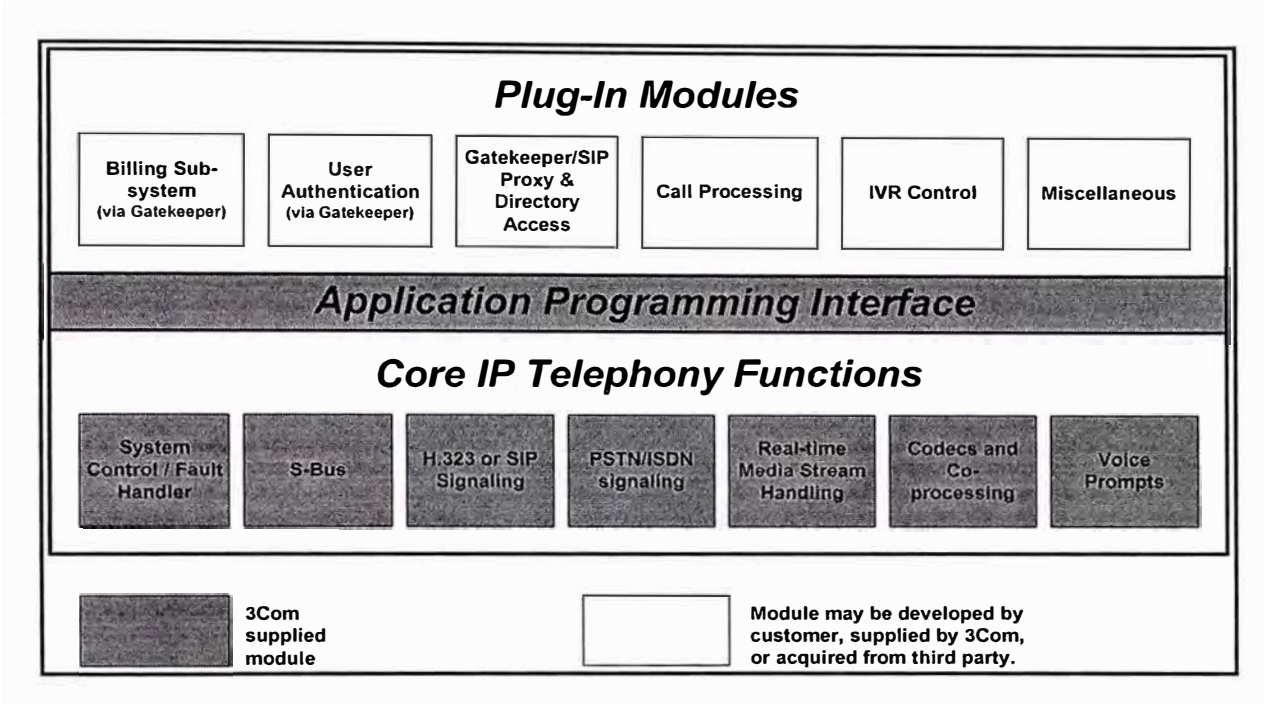


Figura 3.10. Módulos de Software del Total Control 1000 Media Gateway.

3.4.1.2 CommWork Total Control 100-10 Gigabit Router

CommWork Total Control 100 Gigabit Routers proporciona una solución confiable, de alto rendimiento diseñada para resolver las demandas de los Proveedores de Servicios de la red IP.

Diseñado para ser usado en aplicaciones de gran ancho de banda, estos routers "backbone" son capaces de reenviar una alta densidad de paquetes a través de la estructura de la red IP, mientras aseguran la más alta confiabilidad posible y disponibilidad de la red.

La familia Total Control 100 Gigabit Router ofrece cinco modelos con capacidades de enrutamiento desde 0.5 a 40 millones de paquetes por segundo y una capacidad de switching desde 8 Gbps a 90 Gbps. Asimismo, ofrecen tarjetas de interfaz intercambiables y diseño escalable que permite a

los Proveedores de Servicio desarrollar su infraestructura para dar soporte al crecimiento exponencial de los clientes.

Total Control 100 Gigabit Router soporta interfaces múltiples, que permiten a los Proveedores de Servicio combinar una variedad de servicios, incluyendo servicios mejorados de datos, Telefonía IP, telefonía inalámbrica, cable, y línea digital del suscriptor, en una red integrada, y redes de multiservicios basados en paquetes.

Especificaciones:

- Capacidad de Switcheo

  50 Gbps

  Packet Forwarding

  20 Mpps

- Dimensiones y peso

  Ancho: 44 cm (17.3 in)

  Profundidad: 60 cm (23.6 in)

  Altura: 75 cm (29.5 in)

  Peso: 120 kg (264 lb)

- Eléctrico

  Requerimientos de potencia - 1500 VA

  Voltaje de entrada (AC) - 100–120 V, 200–240 V

  Frecuencia de entrada - 50/60 Hz

- Interface Card Slots (Half-size)

  10

- Procesador

  AMD K6-2 300 MHz

- Memoria

  64 MB to 256

  Maximum Route Entries 250,000

- Redundancia

  Route Manager - si

  Switching Fabric - si

  Power Supply - si

  Fan - si

- LAN Densidad del puerto

  Ethernet 10 Mbps – 80 ports

  Fast Ethernet 100 Mbps – 40 ports

  Gigabit Ethernet 1000 Mbps – 5 ports

- WAN Port Density

  V.24/X.21/V.35 (up to 6 Mbps) 40

  T1 Clear/Channelized - 40

  E1 Clear/Channelized - 40

  T3 Clear - 20

  E3 Clear - 20

  E3 Channelized - 5

  OC-3c POS (SMF/MMF) - 40

  OC-3c ATM (SMF/MMF) - 40

  OC-12c POS (SMF/MMF) - 20

OC-12c ATM (SMF/MMF) - 10

OC-48c POS - 5

- Rangos ambientales

  Temperatura de operación (5°–40°C, 41°–104°F)

  Humedad Relativa(20%–80%)

  Almacenamiento (8%–90%)

- Protocolos de ruteo

  RIPv1, RIPv2, OSPF, BGP4, IGMPv2, DVMRPv3, PIM-DM

- Protocolos de Interconectividad

  IP, IPX

- Calidad de servicio

  Diffserve, Monitoreo del BW entrante, control de prioridad del BW saliente, y control de las tramas descartadas.

- Management

  CLI, Web browser

3.4.1.3 3Com 3900 10/100 Ethernet Switch.

El 3Com 3900 10/100 es un Switch Ethernet de alta densidad para los Workgroups y Backbones. Este switch sensa el ancho de banda de trabajo (Ethernet/Fast Ethernet) en entornos de alta densidad.

Características

- Dos slots de extensión acomodan los módulos 1000BASE-SX o 1000BASE-LX para escalamiento.
- Soporta hasta 16.000 direcciones MAC.

- IEEE 802.3x controla el flujo en todos los puertos full-duplex, mejorando el funcionamiento y reduciendo al mínimo las pérdida del paquete.
- Full Soporte de implementación de VLAN.

Especificaciones

- Cantidad de Puertos: 24 10/100 Ethernet, Ethernet de 1 Gigabit, ranuras de extensión de Ethernet de 2 Gigabits.
- Media Interfaces: 10/100 Base-TX/RJ-45, 1000BASE-SX/SC; 1000BASE-LX-SC.
- Características del Switch Ethernet: Full switching en todos los puertos 10/100/1000 Mbps. auto-negociación de full-/half-duplex y control de flujo; soporta 802.1Q VLAN; priorización de tráfico 802.1p.

Este switch Fast Ethernet / Gigabit Ethernet permite que su red sea segmentada, tal que pueda contener el tráfico eficientemente, reduciendo la carga total sin afectar el acceso en los casos críticos.

Cuando una red de repetidores HUB's está en operación, cualquier información que sea enviada por los workstation se pasa a través de toda la red, (sin importar los destinos de la información). Esto da lugar a un tráfico innecesario que puede hacer lenta a la red o hacerla caer. El switch soluciona este problema porque él "escucha" a la red y aprende automáticamente qué Workstation pueden ser rechazados Por lo que puede filtrar cualquier información, transmitiendo el tráfico del acceso relevante solamente (en vez de todos los accesos como un repetidor HUBs).

Si se tiene una Workstation con alto rendimiento que requiere de gran ancho de banda, entonces se deberá conectar directamente a un Switch. Los puertos 10/100 pueden conectarse a una red de 10BASE-T o 100BASE-TX. Si se tiene ambos tipos de redes, se puede conectarlas usando el switch de modo que todos sus Workstation puedan comunicarse. Alternativamente, si se utiliza 10BASE-T y desea mejorar el funcionamiento introduciendo 100BASE-TX, el switch protege sus inversiones porque mantiene las conexiones 10BASE-T a su equipo original de la red.

3.4.2 Equipamiento - BES site (Ubicado en Miraflores)

El Nodo de Miraflores fue diseñado como BES site, en el que CommWorks ha desarrollado un paquete completo de aplicaciones BES (Back End Service). Estas aplicaciones proveen de una solución completa (Operational Support System) necesarias para cumplir con todas las necesidades en un esquema de telefonía IP. Todos los componentes de señalización, facturación y capacidades de creación de servicios residirán en este Nodo además de los componentes descritos anteriormente. Esta red está constituida de la siguiente red de Servidores :

- CommWorks 7210 Directory Server*
- CommWorks 7220 Accounting Server*
- CommWorks 7230 Billing Support Server*
- CommWorks 7240 Web Configuration Server*
- CommWorks 8010 Service Creation Engine*
- CommWorks 8210 Unified Messaging Server*
- CommWorks 4007 SCC7 Gateway*

- CommWorks 4200 H.323 Gatekeeper*
- CommWorks 4220 SIP Proxy*
- CommWorks 5210 IP Telephony Network Management*

3.4.2.1 CommWorks 7210 Directory Server

El CommWorks 7210 Directory Server provee información para traducir un número telefónico compatible con E.164 a una dirección IP (o nombre DNS) del Gateway de un área específica de llamadas. Para ello, el Directory Server actúa como el depósito de base de datos y provee información de mapeo entre un número telefónico de destino y la dirección IP del Gateway de "despegue" más cercano. Normalmente el Gateway llamante puede no tener la información de ruteo de la red IP dentro de su propia base de datos para poder enviar paquetes de audio comprimidos a la dirección de destino. En ese caso, el Gateway envía una pregunta al Gatekeeper, que luego se comunica con el Directory Server sobre la red IP para solicitar una dirección IP de destino que concuerde con el número telefónico llamado. El Directory Server realiza una búsqueda real en la base de datos y devuelve la dirección IP requerida.

El CommWorks 7210 Directory Server soporta las siguientes funcionalidades:

- Acceso Gatekeeper/Proxy Server a través del ODBC.
- Permite registrar actualizaciones / adiciones / supresiones / dudas a través del navegador de la Web (u otra interfaz definida).
- El almacenamiento de registros de la base de datos brinda mapeo entre Gatekeepers y Proxy Servers y las Direcciones E.164 correspondientes

(es decir, código de país y 4 o 7 dígitos del número (significativo nacional).

- Utiliza el modelo de Global Proximity para las tablas de ruteo.
- Código de País.
- NDC/NPA (es decir, código de área).
- Mapeo del plan nacional de discado del número del abonado

Este servidor proporciona información de encaminamiento a los GKs en el BES site. Hay un Directory Server (DS) localizado en el BES site de Miraflores señalado como primario. Desde que los GKs apuntan al BES site, el DS primario sería el responsable de la carga total de la red.

Los diferentes tipos de tráfico manejados por el Directory Server son los siguientes:

1) Consulta de la base de datos de encaminamiento desde el GK sobre la misma LAN. En caso de falla (local) de GKs, el GK secundario hará las consultas de encaminamiento al Directory Server. Para nuestro caso el GK secundario esta en la misma ubicación (Miraflores).
2) Tráfico de administración de la red tal como SNMP, mejoras etc.

3.4.2.2 CommWorks 7220 Accounting Server

El CommWorks 7220 Accounting Server almacena los registros de detalle de llamadas (Call Detail Records - CDRs) generados por el ingreso y egreso de Gateways para aquellas llamadas completadas con éxito y para los intentos de llamadas. El Accounting Server soporta las siguientes características:

- Acceso Gatekeeper/Proxy Server a través de ODBC.
- Permite el registro de dudas a través del navegador de la Web.
- Almacena CDRs llamada por llamada
- Soporta la función de transformación de datos para exportar al depósito de datos o a otras bases de datos externas

Una vez que se recibe la llamada, el Gateway crea un CDR para dicha llamada (se complete o no) y luego envía la información al Gatekeeper. El Gatekeeper envía los datos al Accounting Server en una función configurable de procesamiento de lotes.

3.4.2.2.1 Generación de Registro de Detalle de Llamadas

En la implementación de 3Com, el proceso de generación de CDR es llevado a cabo por cada uno de los CDRs individualmente marcando los registros de inicio y finalización creados por los Gateways de ingreso y egreso. Una vez creados, los CDRs son enviados al Gatekeeper y luego al Accounting Server. En el Accounting Server, los CDRs individuales se transforman en un único formato “super CDR” combinando la información dentro de los CDRs en un CDR combinado.

La Figura 3.11 muestra la forma en que se generan los CDRs por medio del CommWorks IP Telephony System.

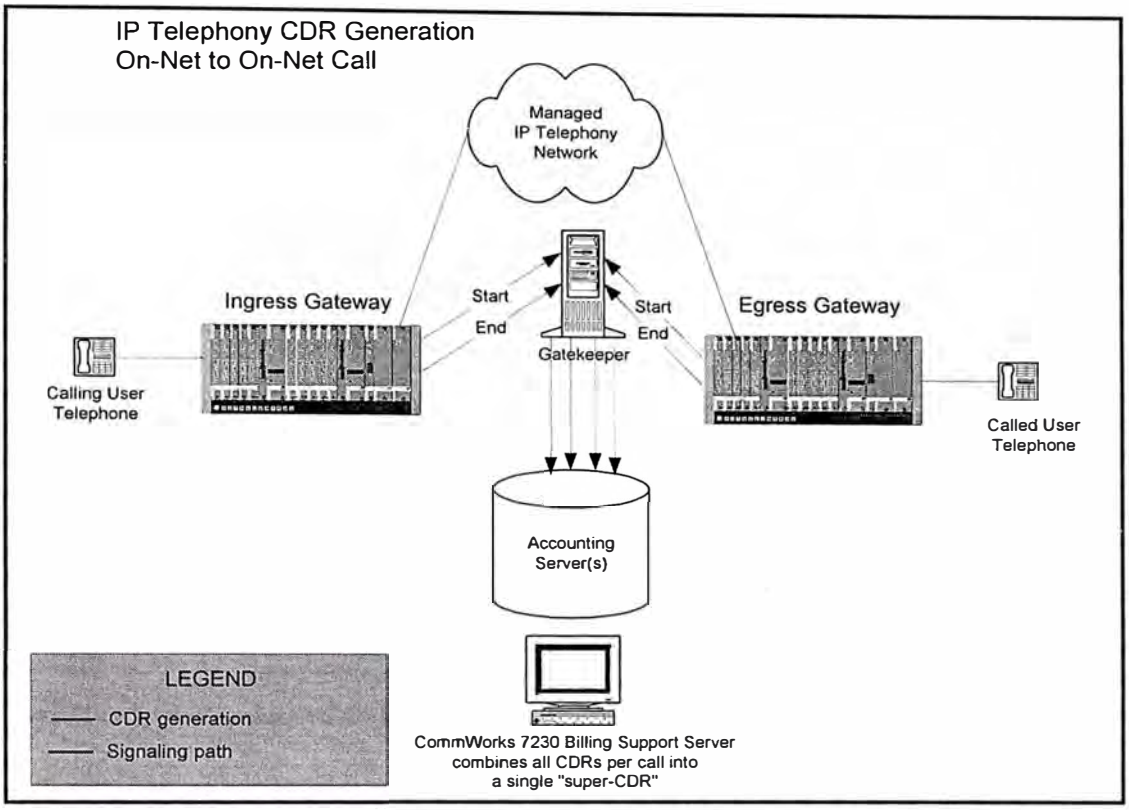


Figura 3.11 Generación del Registro de Detalle de Llamadas.

3.4.2.2.2 Formato de Registro del Detalle de Llamadas

Los registros que detallan las llamadas son diseñados para permitir la capacidad de facturación total y el análisis extenso y gestión del nivel de servicio:

- Version.
- CDR Source Identifier.
- Call ID.
- Call Type.
- Call Accessed Start Time.
- Call Established Start Time.
- Call Disconnect Start Time.
- Disconnect Reason.
- Audio Packets Sent.
- Audio Packets Received.
- Audio Packets Lost.
- RFP Frame Size.
- Frame Length.
- Voice Signal Frame Size.

Holding Time Duration.

Service Type.

Account Number/User ID.

Charge Amount.

Initial Balance.

Called Party Number/DNIS.

Account Identification Code.

Originating Line Information (OLI) Digits.

Calling Party Number/ANI.

Destination Number.

Ingress Gateway IP Address.

Egress Gateway IP Address.

Ingress SIP Proxy IP Address.

Egress SIP Proxy IP Address.

Codec Type.

Calling Party IP Address.

Called Party IP Address.

Rate Plan ID.

Account Type.

Session_ID.

PSTN Interface Number.

Sequence Call Number.

Session_End_ID.

Port_ID.

Slot_ID.

Number of PIN Failures.

Number of Call Attempts.

3.4.2.3 CommWorks 7230 Billing Support Server

El CommWorks 7230 Billing Support Server se usa para combinar el ingreso y egreso individual de CDRs almacenados en el Accounting Server en un formato “super CDR” (SCDR) y luego enviar esa información a una operación del Open Settlements Protocol (OSP) o del Centro de Intercambio de Información. La Figura 3.12 muestra como trabaja la aplicación del servidor de soporte de facturación.

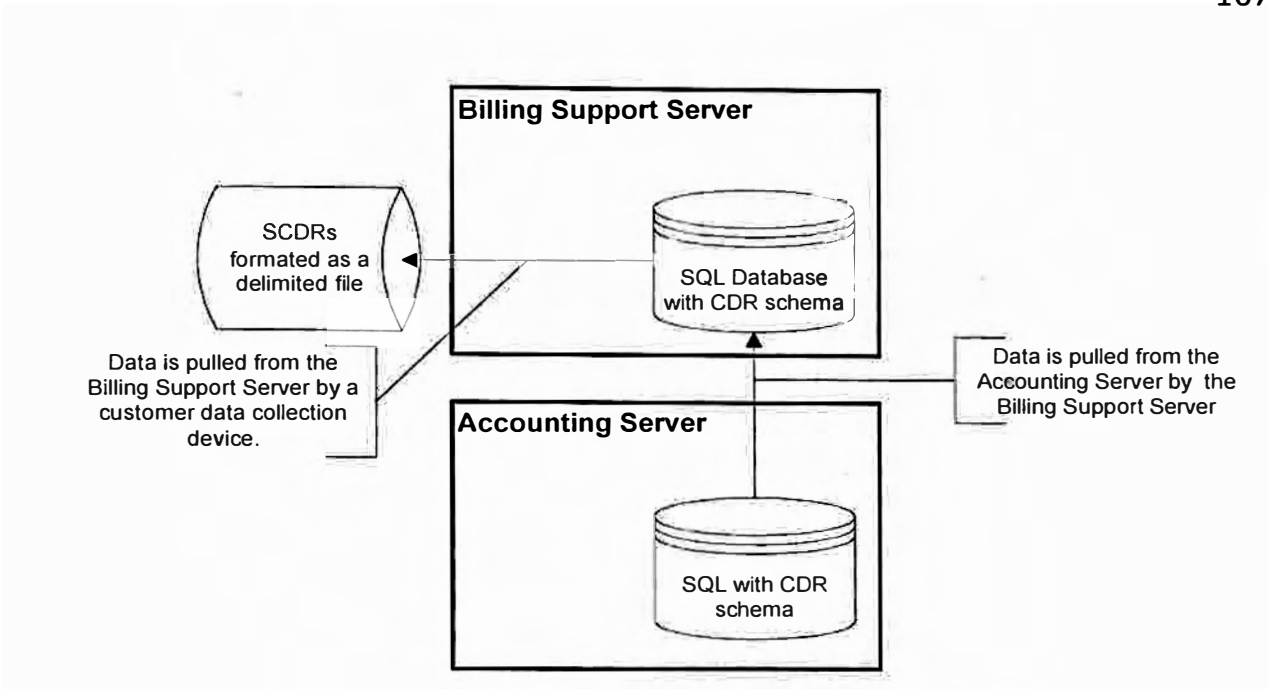


Figura 3.12 Servidor de Soporte de Facturación CommWorks 7230.

3.4.2.4 CommWorks 7240 Web Configuration Server

El CommWorks 7240 Web Configuration Server provee acceso por medio del navegador de la web a los Back End Servers, Gatekeeper y Servidor Proxy SIP CommWorks. El CommWorks 7240 está diseñado para gestionar las aplicaciones de Telefonía IP (software). Esta función es normalmente realizada por otros grupos dentro del grupo de operaciones de red del carrier. Se puede utilizar esta interfaz de la web para examinar, definir, cambiar y modificar:

- El Servidor de Directorio
  - Los datos de ruteo de llamada en el Servidor de Directorio.
  - Las asignaciones del Gateway (registro de MGs específicos a Gatekeepers o SIP Proxy Servers específicos).
  - Las asignaciones del Gatekeeper/Proxy Server (asignación de zonas, super zonas, autorización entre dominios y códigos locales).

  - Excepciones de discado (solo lectura), basadas en el nivel de tratamiento de ruteo de llamadas.
- Servidor de Autenticación / Tarificación
  - Tarjeta de llamada e información de la tarifa de la llamada del usuario en el Servidor de Autenticación / Tarificación.
  - Información del plan de llamadas.
  - Información del plan de tarifas.
- Gestión General de la Aplicación
  - Configuraciones Data Management System (DMS) que permiten conexiones a varias bases de datos utilizadas por las aplicaciones BES.

3.4.2.5 CommWorks 8010 Service Creation Engine

El CommWorks 8010 SCE, tiene la capacidad de despliegue para una amplia gama de servicios de voz, e-mail y de fax incluyendo:

- Mensajería unificada.
- Correo de voz.
- El mensaje o fax sobre demanda.
- Difusión del mensaje o del fax.
- Fax mail.
- Respuesta interactiva de la voz (IVR).
- Texto audio.
- Notificación Out-dial

Componentes del CommWorks SCE.

- Programa editor.- Programas convencionales similares a C y/o al BASIC.
- El interfaz del ordenador HOST.- Provee soporte de aplicación para CTI (computer telephony integration) y de IVR (respuesta interactiva de la voz) vía accesos seriales, Ethernet, Token Ring, los Gateways de la red, el Internet, TCP/IP, y SNA/SDLC.
- Interfaz de Red.
- Interfaz de Grabación directa .- Permite un control total de la edición de la grabación de mensaje, directamente del CommWorks SCE.
- Opciones del control documentario .- Proporciona una captura de documento completamente equipada y capacidad de manejo para la imagen escaneada, el fax, o los ficheros de datos.
- Control de visualización de video .- Permite a los desarrolladores crear simples ventanas administrativas para el usuario final, reportes en la pantalla, y las pantallas de la entrada de la base de datos. Todas las aplicaciones de la pantalla se pueden manejar por la consola o los X-terminales remotos.
- Tarjeta de voz
- Reconocimiento de voz .- Soporta reconocimiento discreto y continuo de la voz.
- Text-to-Speech .- Esta disponible para los que deseen agregar síntesis de dato-a-voz a sus aplicaciones de CommWorks SCE.

3.4.2.6 CommWorks 8210 Unified Messaging Server

El sistema de mensajería unificada CommWorks 8210 ofrece nuevos servicios de mensajería a sus clientes tanto residenciales como profesionales. Los usuarios pueden acceder a sus correos electrónicos, buzón de voz y mensajes de fax desde la red de teléfonos públicos, Internet, banda ancha o redes inalámbricas utilizando cualquier tipo de dispositivos como teléfonos, ordenadores personales y portátiles, correo electrónico, navegadores, teléfonos portátiles y PDAs (personal digital assisants).

Además de las funciones universales de mensajería unificada, CommWorks 8210 proporciona capacidades unificadas de buzón de correo por lo que los usuarios pueden recuperar mensajes desde múltiples cuentas POP3 e IMAP4 (Internet Messaging Access Protocol) a través de la misma interfaz. Esta función ofrece a los usuarios un mayor grado de flexibilidad y capacidad para las comunicaciones que otros servicios de mensajería unificada.

La solución CommWorks además incluye un servidor de correo Web que permite a los usuarios acceder a sus mensajes de voz, de fax y de correo electrónico desde cualquier conexión de Internet utilizando navegadores estándar.

El sistema de mensajería unificada CommWorks 8210 también permite a los usuarios de Palm la posibilidad de copiar el contenido del libro de direcciones de su Palm directamente en el libro de direcciones personal de su cuenta de mensaje unificada. Los clientes pueden, de esta manera, enviar correos electrónicos, mensajes de voz o de fax a cualquier dirección

de correo electrónico o número de teléfono que esté registrado en la libreta de direcciones directamente desde su cuenta de correo unificada. Esta mejora, además, incluye una función de agregación automática de direcciones de correo electrónico.

Si un usuario elige activar esta función, CommWorks 8210 capturará las nuevas direcciones de correo electrónico recibidas en la cuenta y automáticamente las incluirá en la libreta personal de direcciones. Para evitar que se añadan direcciones no deseadas, el sistema sólo captura las direcciones de correo electrónico de los mensajes que han sido abiertos por el destinatario.

3.4.2.7 CommWorks 4007 SCC7 Gateway

La integración del CommWorks 4007 en la red SS7 brinda los siguientes beneficios:

- Menor Costo Operativo.- Suprime la necesidad de un operador de alquilar servicios de enlace o expandir sus conmutadores de circuitos para agregar capacidades PRI a medida que se requieren más conexiones.
- Mayor Eficiencia de Puertos .- Permite a los puertos/ grupos de puertos actuar como un único grupo de enlaces, lo que resulta en un uso más intenso de los puertos y en una mayor eficiencia de recursos.
- Diseño de Servicio a Prueba del Futuro.- Utiliza SS7/ISUP para reemplazar los servicios PRI existentes, la migración hacia redes convergentes es posible sin costos significativos de nuevo hardware y prolongados ciclos de desarrollo.

En un entorno de SS7, la señalización de llamadas (por ejemplo, el establecimiento y la supresión de funciones) puede ser provista a través de enlaces A o F a partir de la conmutación intermedia al Gateway SS7 y luego en el chasis por medio de señalización de control de llamadas basada en IP. La información es luego entregada a los DS0s individuales a través del Packet Bus. Los datos de la llamada son enviados directamente a la tarjeta Total Control 1000 DSP por medio del uso de Inter-Machine Trunks (IMTs) del switch. La Figura 3.13 presenta la conectividad física necesaria para ello.

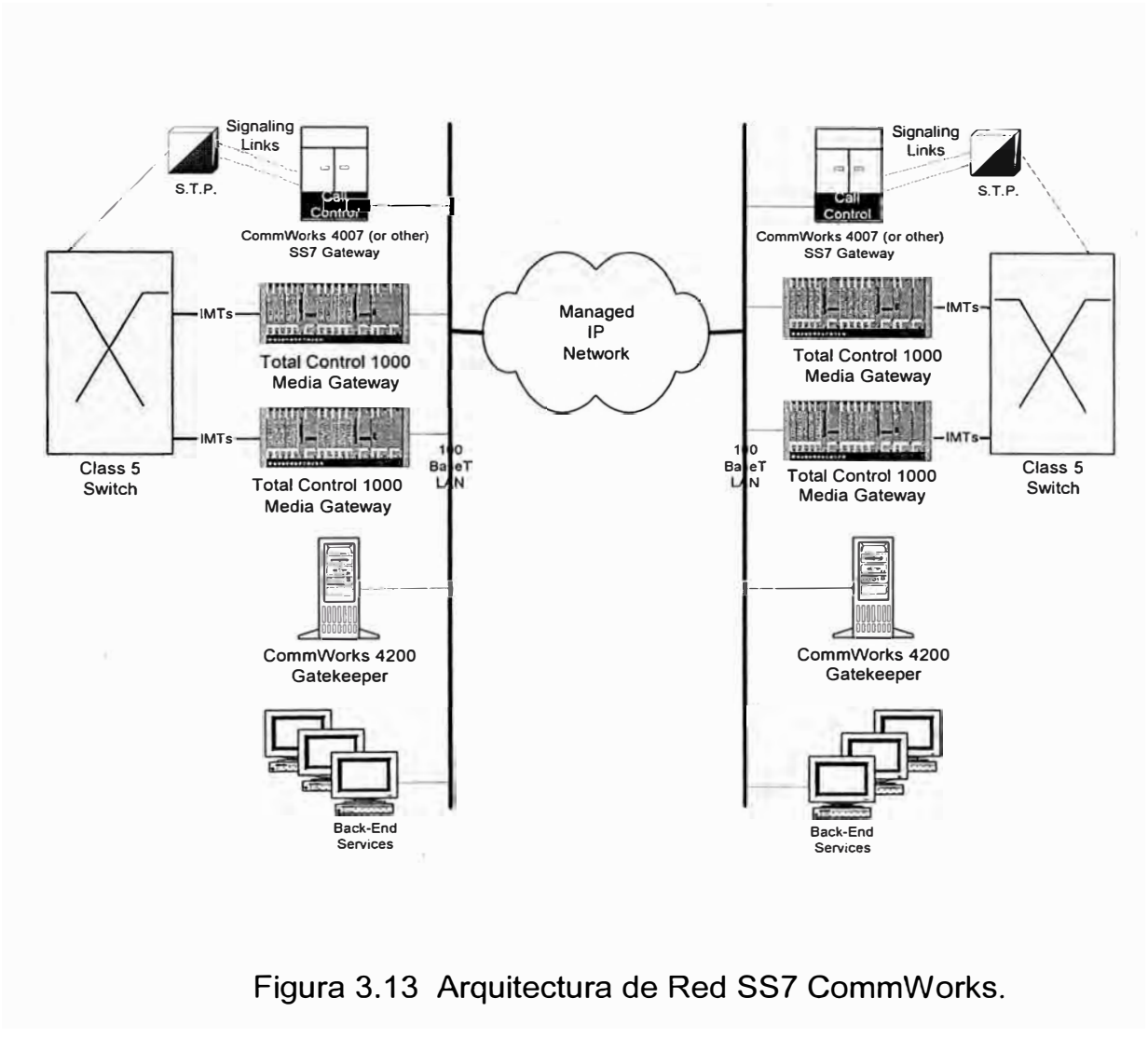


Figura 3.13 Arquitectura de Red SS7 CommWorks.

El Gateway de Señalización CommWorks 4007 está diseñado para trabajar en conjunto con los siguientes conmutadores de telecomunicaciones y Puntos de Transferencia de Señales (STPs):

Alcatel	Lucent
DSC Communications	Nortel
Ericsson	Siemens
Fujitsu	Tekelec
GPT	

3.4.2.8. CommWorks 4200 H.323 Gatekeeper

El CommWorks 4200 Gatekeeper de 3Com es una aplicación de software que provee control de llamadas, enrutamiento de llamadas, gestión de recursos y control de admisiones a la red IP Telephony basada en H.323. Sus responsabilidades incluyen la autorización del uso de la red, resolviendo los números telefónicos compatibles con E.164 en direcciones IP, cargando información de eventos y estadísticas llamada por llamada e identificando la tarifa a la cual se cobrará la llamada solicitada. El Gatekeeper provee éstos servicios con el soporte de recursos de back-end server (Back-End Services). El Gatekeeper también conoce la utilización de puertos y la carga de llamadas en todas las Gateways dentro de su zona definida y puede informarlo.

El diseño arquitectónico del CommWorks Gatekeeper asegura que las aplicaciones de terceros como por ejemplo las aplicaciones del Operation

Support System (OSS), por ejemplo : facturación, autenticación o provisión a clientes puedan ser fácilmente "enchufadas" a través del uso de los conjuntos API que habilitan los servicios extensivos provistos por 3Com. La Figura 3.14 presenta un diagrama de bloque del CommWorks 4200 Gatekeeper.

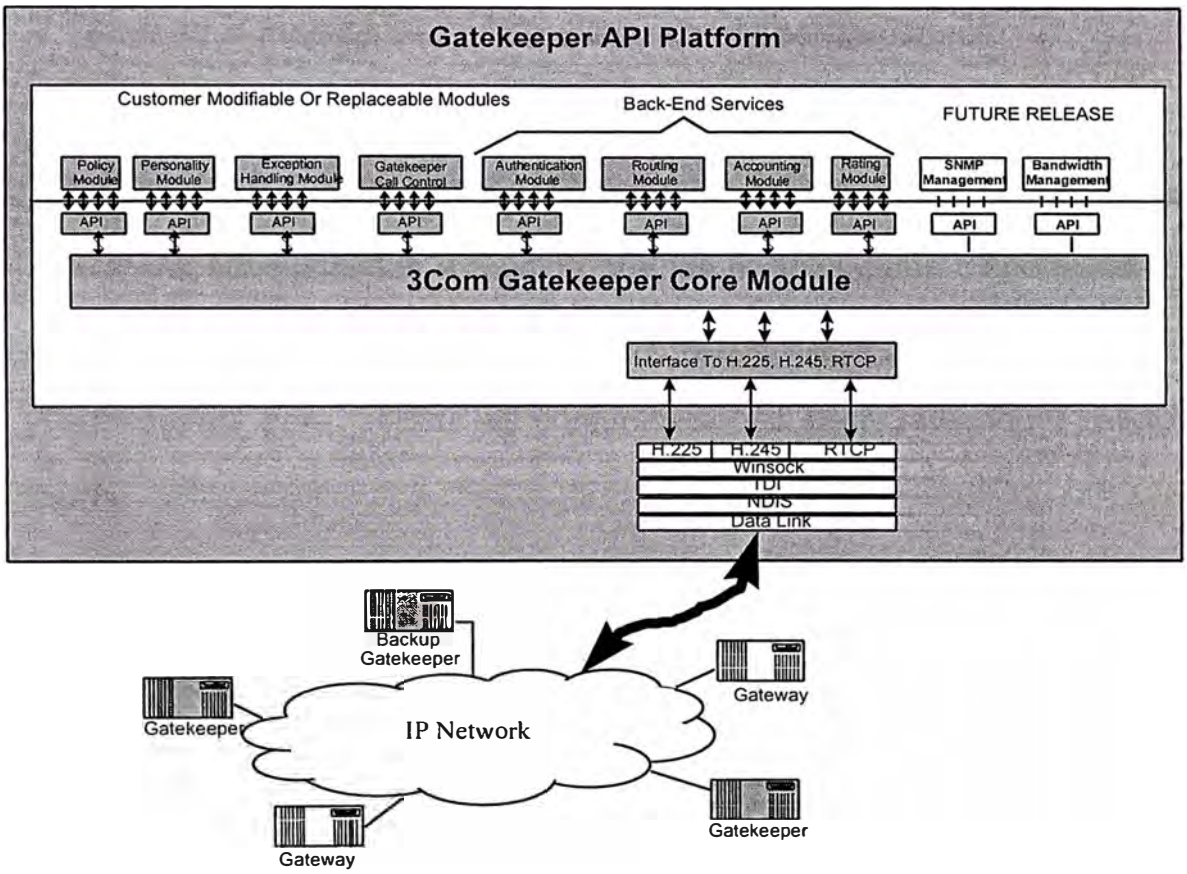


Figura 3.14. Diagrama de Bloque del CommWorks 4200 Gatekeeper.

3Com ha utilizado siempre las normas H.225 para proveer las comunicaciones Gatekeeper. Desafortunadamente, esta norma no está muy bien definida y no ha sido implementada por otros vendedores en una forma

similar. En la actualidad se soportan las comunicaciones Gatekeeper a Gatekeeper, usando un protocolo extendido H.225 RAS.

El CommWorks 4200 Gatekeeper soporta las siguientes características:

- Total compatibilidad con los aspectos obligatorios y los no obligatorios del H.323 versión 2; que incluye H.225.0v2, RASv2 y H.245v3
  - Soporta el modelo de Señalización Directa de Llamadas
  - Soporta el modelo de Señalización ruteada de Gatekeeper
  - Soporta Rápida Conexión
- La señalización inter-Gatekeeper a través del RAS será soportado en versiones subsiguientes a medida que las normas estén disponibles. La versión actual soporta los intercambios de mensajes LRQ/LCF/LRJ entre Gatekeepers para facilitar las comunicaciones inter-Gatekeeper o inter-zona.
- SNMP administrable.
- Autorización y autenticación de servicios.
- Identificación del usuario por medio de autenticación de PIN.
- Autenticación por medio de ANI.
- Resolución de dirección y módulo de ruteo.
- Registración Final.
- Enrutamiento a través de las comunicaciones con Directory BES.
- Archivo de Registro de Detalle de Llamadas en el Servidor de Base de Datos Contables.

- Tasación de cargos de llamadas a través del Servidor de Base de Datos de Tarificación.
- APIs abiertos para la interfaz con los servicios de autenticación, contabilidad, enrutamiento y tarificación de terceros.
- Registro manual de 'No-Registrado/Admisión/Estado' de Clientes (RAS) .
- Emisión de Llamadas H.450.2 .
- Control de seguridad por medio del registro de una lista de Gateways "de confianza" que se permite registrar.

3.4.2.9 CommWorks 4220 SIP Proxy Server

El CommWorks 4220 SIP Proxy Server es una aplicación de software que provee control de llamadas, enrutamiento de llamadas, gestión de recursos y control de admisiones a la red de Telefonía IP basada en SIP. Como proxy server de re-dirección, sus responsabilidades incluyen los servicios de registro para dispositivos terminales, autorizando el uso de la red, traduciendo números telefónicos compatibles con E.164- a direcciones IP, registrando información estadística y de eventos llamada por llamada e identificando la tarifa a la cual la llamada solicitada será facturada. El Proxy Server provee estos servicios con el soporte de recursos de back-en (Back-END Services). El CommWorks 4220 también conoce la utilización de puertos y la carga de llamadas en todas las Gateways dentro de su zona definida y puede informarlo. Además el Proxy Server SIP provee numerosos servicios IP Centrex tales como

- Varios mecanismos y disparadores de emisión de llamadas (no disponible, ocupado, incondicional, etc.)

- Soporte para llamada en espera.
- Soporte para servicios de seguimiento.

Las comunicaciones del Servidor Proxy SIP y la interoperabilidad con puntos de terminación están aseguradas por medio de la estricta observancia de las normas RFC 2354.

3.4.2.10 CommWork 5210 IP Telephony Network Management

El CommWorks 5210 IP Telephony Manager es un sistema de gestión de elementos basado en SNMP que reside en estaciones de trabajo Solaris o HP-UX. Provee una interfaz de usuario gráfica (GUI) para realizar las siguientes funciones generales para la monitorización y control del media Gateway (MG) Total Control 1000 media (MG).

- Gestión de fallas (traps y estado de los errores)
- Gestión de configuración (visualizar, modificar, guardar y restablecer)
- Gestión de contabilidad (inventario, hardware y versiones de software)
- Gestión de perfomance
- Gestión de seguridad (derechos de acceso y uso)

El administrador de telefonía IP CommWorks 5210 opcionalmente puede ser lanzado por medio de un nivel más alto de aplicaciones de sistema de gestión de red (NMS) tales como HP OpenView.

Usando la tarjeta de gestión de red (NMC) que aloja el SNMP del MG que provee un punto único de gestión para el chasis el CommWorks 5210 usa la versión 1 del protocolo Simple Network Management Protocol (SNMP) para comunicarse con el MG.

Además el CommWorks 5210 se comunica con los servidores basados en Microsoft Windows NT (H.323 Gatekeeper, Directory Server, etc.) a través de el Common Agent. El Common Agent de 3Com aloja los gestores SNMP de los servidores y provee un único punto de gestión remota a cada una de estas aplicaciones.

Específicamente, el administrador de telefonía IP CommWorks 5210 provee las siguientes funciones:

1) Gestión de Fallas

- Envía los traps y los eventos del SNMP hacia adelante a un nivel más alto del sistema de gestión de red. El CommWorks 5210 no registra directamente los eventos o informa las condiciones de falla / traps. La mayoría de los clientes prefiere usar una aplicación de gestión de mayor nivel (por ejemplo el HP OpenView) para la gestión de fallas.
- Permite a los usuarios especificar cuáles son los traps que están habilitados para cada componente. Para algunos parámetros operativos, se pueden fijar umbrales para especificar las condiciones bajo las cuales los traps deberían generarse (es decir, índice de pérdida de paquete, etc.)
- Pueden establecerse filtros de traps para Gatekeepers, Proxy Servers y Back-End Servers basados en el índice al cual cada trap es generado. Esto ayuda a impedir las avalanchas de traps en condiciones de error.
- Los comandos disponibles de mantenimiento en la consola incluyen
    - Sacar la tarjeta, el troncal o el DS0 del servicio

- Restaurar el servicio
- Resetear el hardware y el software
- Busy-out del puerto o troncal

- Las pruebas de las tarjetas Total Control 1000 incluyen :
  - 105/108 pruebas
  - Auto test
- Soporte al cliente NTP para asegurar el registro exacto de tiempo de los eventos

2) Gestión de Configuración
   - Configuraciones de parámetros DSP en el MG
   - Configuraciones de parámetros de tarjeta de enlace en el MG
   - Configuración de guardar y restablecer en el MG, Gatekeeper, SIP Proxy Server todas las aplicaciones Back-End Service (BES)
   - Configuraciones de traps SNMP (destinos, habilitación / inhabilitación de traps específicos por tarjeta, configuraciones de umbrales)
   - Actualización de software para todos los componentes del CommWorks ITS
3) Gestión de Contabilidad
   - Gestión de inventario (información detallada de todas las tarjetas en el chasis).
   - Visores virtuales de panel (visores de panel delanteros y traseros para cada tarjeta en el MG).

- El Virtual Front Panel Display (VFPD) provee visualización gráfica del chasis del MG y de cada NAC dentro del MG. Presenta los LEDs e indica los cambios en el estado de la tarjeta representados por el LED.
- El Virtual Rear Panel Display (VRPD) provee visualización gráfica y acceso a todas las interfaces ubicadas en los diversos NICs dentro del chasis del MG.

- Provee información de la versión del software y del hardware.
- Visualización de la Tabla de Registro que permite determinar cuáles MGs están registrados con una Gatekeeper o Proxy Server en particular.

4) Gestión de perfomance

- Presenta las estadísticas en planillas (no hay tablas gráficas dentro del CommWorks 5210).
- Presenta las estadísticas por grupo funcional (es decir, MG, Gatekeeper, estadísticas de llamadas y paquetes, eventos de modems, estadísticas DS0).
- Monitorización / Observación del servicio en tiempo real para las llamadas específicas en curso (se puede escribir texto dentro del CommWorks 5210 que permite que numerosos objetos MIB sean cuestionados en tiempo real, como por ejemplo, pérdida de paquetes, paquetes enviados, jitter, demora, etc. Nota: La demora de ida y vuelta no puede medirse en tiempo real).

- Capacidad para seleccionar uno o más parámetros de un grupo de presentaciones estadísticas personalizadas (es decir, intentos fallidos de conexión, longitud de la llamada, ANI). Se pueden seleccionar hasta diez parámetros por grupo.
- Monitorización de todos los MIBs de perfomance relacionados con el NT con respecto al Gateway (por ejemplo, utilización de la CPU, uso de memoria, etc.)

5) Seguridad

- Capacidad de establecer, modificar y visualizar los community strings para los componentes administrados. Nota: los community strings NMC solo pueden ser modificados por un usuario autorizado (es decir, se debe conocer el valor corriente lectura-escritura para realizar un cambio). Los valores corrientes solo pueden visualizarse de la interfaz del puerto de la Consola NMC local (o a través de un navegador MIB externo).
- Lista de estaciones de Provisión / Configuración autorizadas, hasta diez direcciones IP pueden ser definidas para autorizar el ingreso explícito al sistema a través del NMC

3.5 Topologías de los Nodos

3.5.1 Trujillo

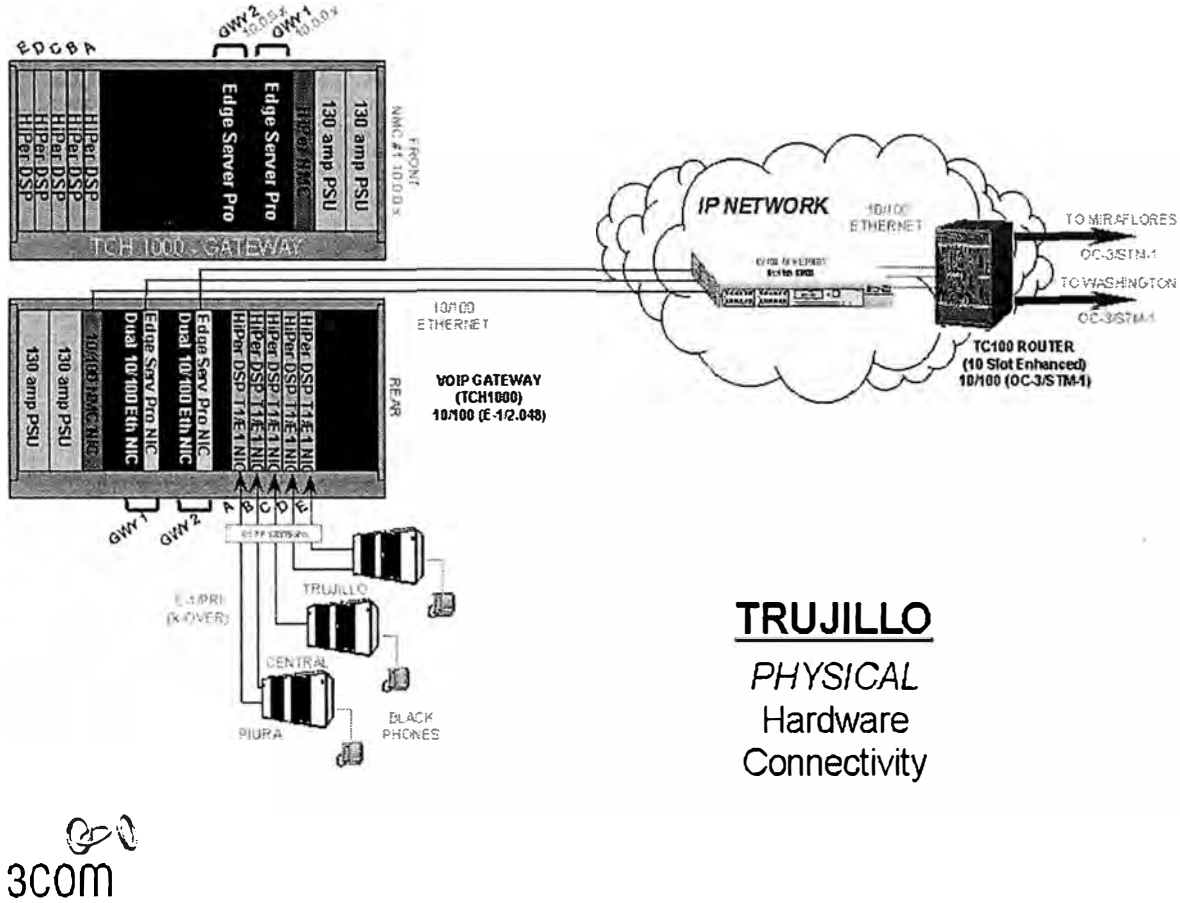


Figura 3.15 Configuración de los equipos en Nodo Trujillo

3.5.2 Arequipa

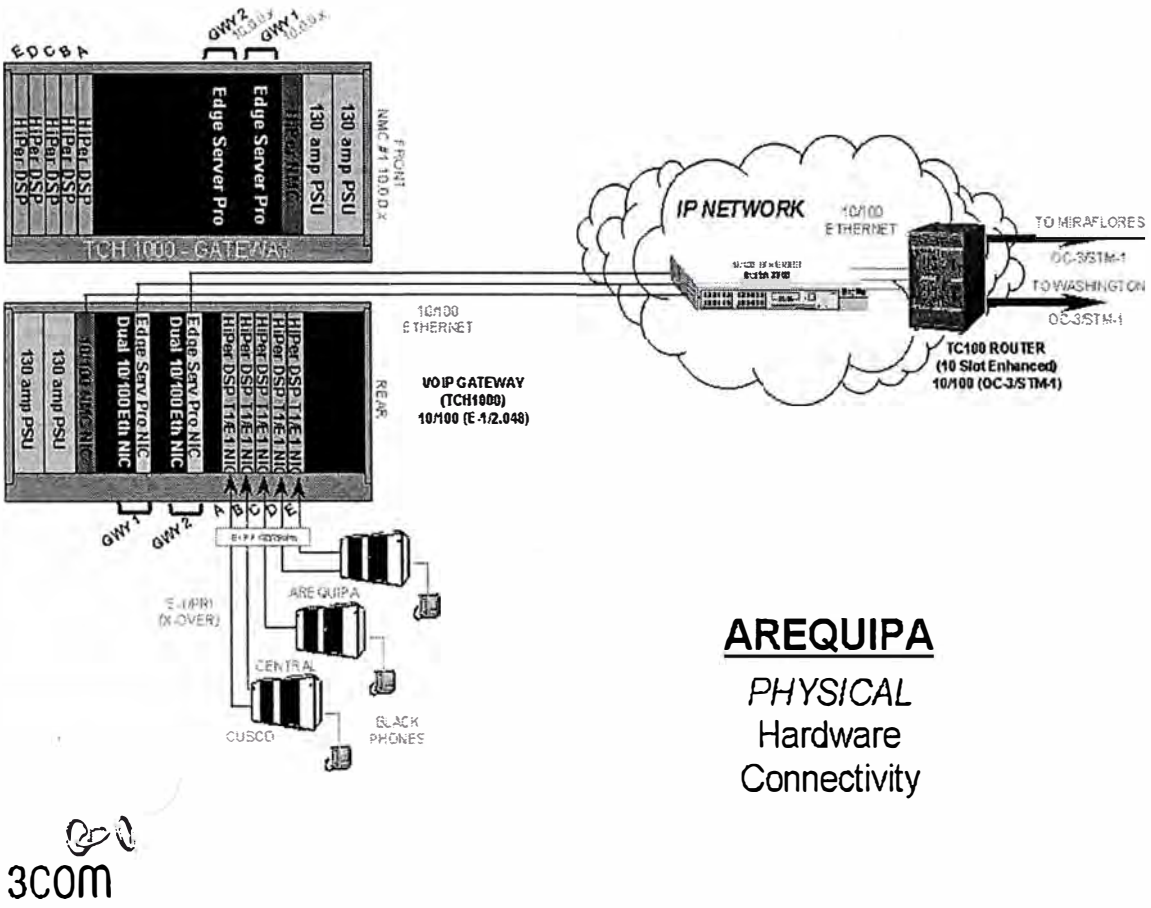


Figura 3.16 Configuración de los equipos en Nodo Arequipa

3.5.3 Washington

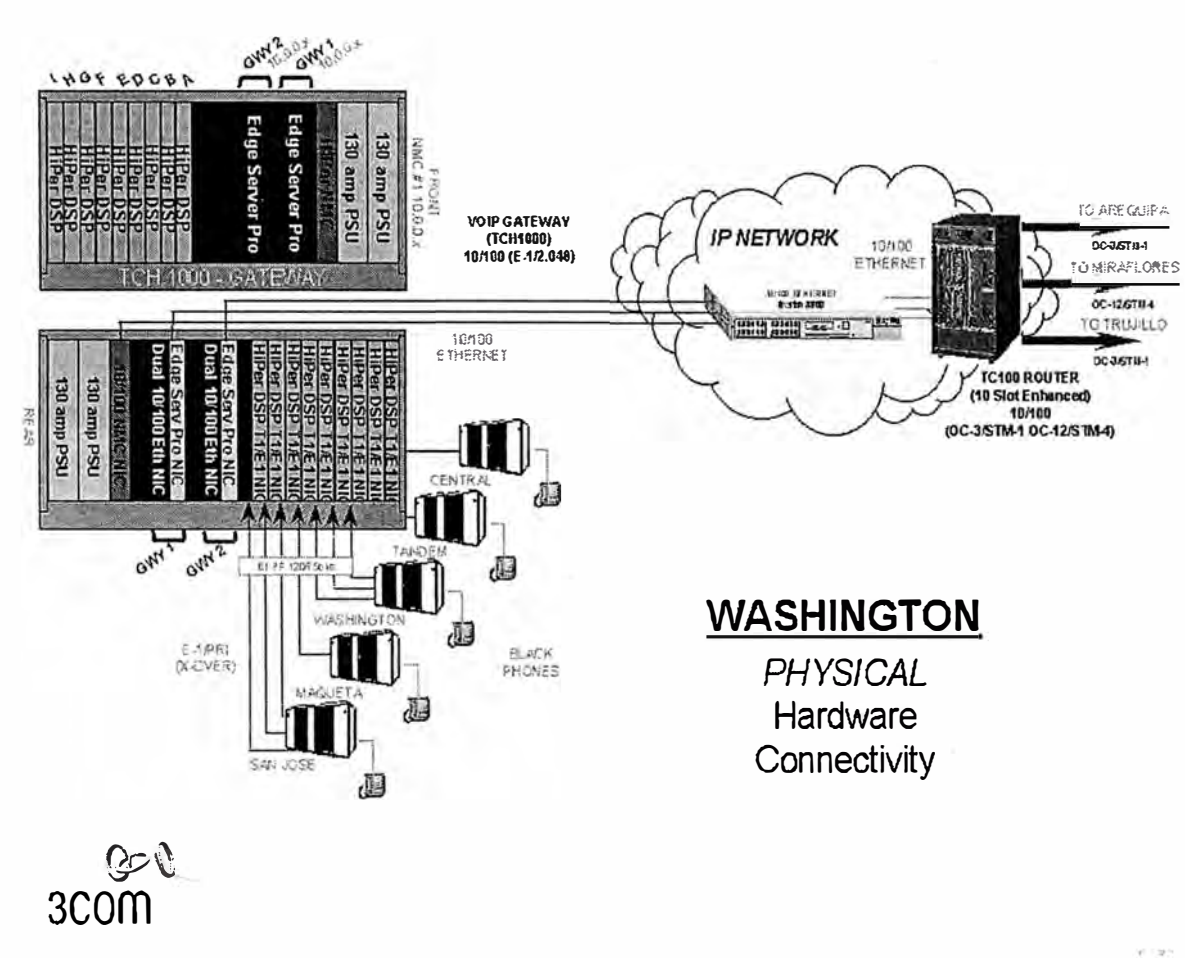


Figura 3.17 Configuración de los equipos en Nodo Washington

3.5.4 Miraflores BES Site

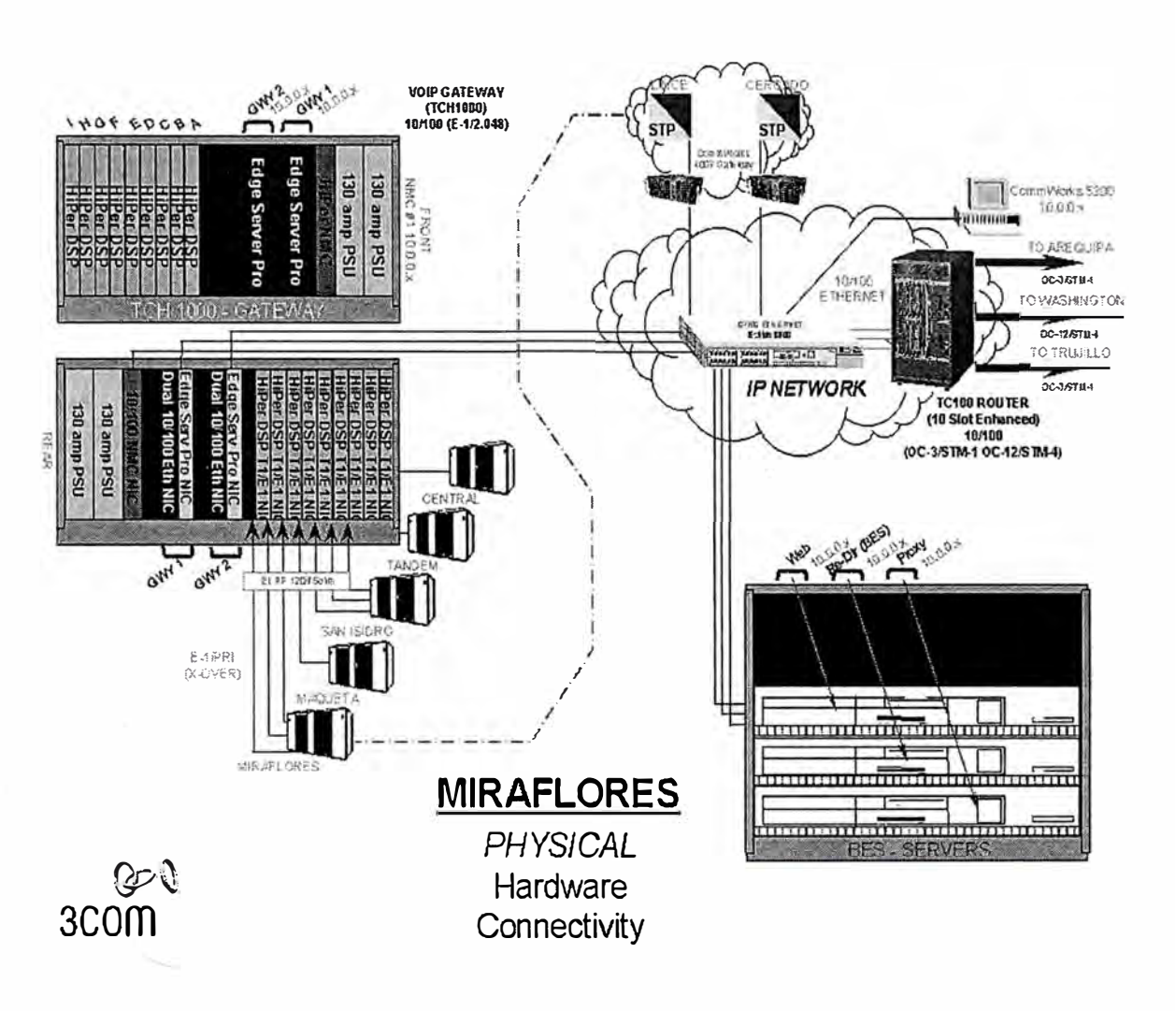


Figura 3.18 Configuración de los equipos en Nodo Miraflores.

CONCLUSIONES

1) Voz sobre IP es una tecnología. Telefonía IP, por otra parte, es una aplicación de la tecnología VoIP. La telefonía IP representa muy probablemente el siguiente paso en la evolución de las redes de conmutación de voz de hoy, a una verdadera infraestructura sobre multimedia.
2) El crecimiento y la fuerte implantación de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, los mecanismos de control y priorización de tráfico, los protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permiten la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP.
3) La convergencia plantea un serio reto: las redes de voz y datos son esencialmente diferentes. Por ejemplo las redes de voz, que emplean conmutación de circuitos, se caracterizan por requerir el establecimiento de llamada, reservar recursos de la red durante todo el tiempo que dura la conexión, utilizar ancho de banda fijo (típicamente 64 Kbps por canal de voz). En cambio, las redes de datos, basadas en conmutación de paquetes, se identifican por que no requieren del envío de datos para el

establecimiento de llamada, el consumo de los recursos de red se realizan en función de las necesidades. Por lo que implementar una red convergente supone estudiar las diferencias existentes entre las características de las redes de voz y de datos, comprendiendo los problemas técnicos que implican dichas diferencias sin perder de vista en ningún momento la perspectiva del usuario final.

4) Respecto a los Factores que afectan la calidad podemos indicar los siguientes:

- Requerimientos de ancho de banda: la velocidad de transmisión de la infraestructura de red y su topología física.
- Funciones de control: incluye la reserva de recursos, provisión y monitorización requeridos para establecer y mantener la conexión multimedia.
- Latencia o retardo: de la fuente al destino de la señal a través de la red.
- Jitter: variación en los tiempos de llegada entre los paquetes. Para minimizar este factor los paquetes entrantes han de ser introducidos en un buffer y, desde allí, enviados a intervalos estándar.
- Pérdida de paquetes: cuando un paquete de video o de voz se pierde en la red es preciso disponer de algún tipo de compensación de la señal en el extremo receptor.

5) Sobre el sistema de telefonía IP de 3Com, ésta se basa en una arquitectura abierta de tres niveles de gateways, gatekeepers y servidores backend interconectados mediante protocolos abiertos basados en normas. La arquitectura modular de 3Com presenta APIs estándar en cada nivel a fin de brindarle a los Operadores flexibilidad para personalizar el sistema, facilitando la diferenciación de servicios y la integración de las “mejores” aplicaciones de oficina back-to-back. Este sistema modular está basado en normas que soporta telefonía sobre IP de teléfono a teléfono y de PC a teléfono en redes conmutadas por paquetes.

BIBLIOGRAFIA

[1] “Redes de Computadoras” , Andrew S. Tanenbaum, Tercera edición.

[2] “Trial Plan for Telefónica del Perú VoIP Trial”, CommWorks Corporation.

[3] “Voice Over IP Fundamentals” , Jonathan Davidson / James Peters.

[4] “Tecnologías de Interconectividad de redes” PRENTICE-HALL México 1988.

[5] “Carrier Grade Voice over IP” Daniel Collins – McGraw-Hill.

[6] Pagina Web ProForum Tutorials “ http://www.iec.org

[7] Página Web http://www.3Com.com

[8] Página Web http://www.Commworks.com