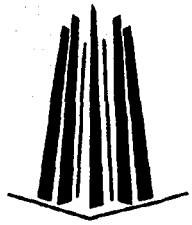


UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

"VoIP EN LA UNAM"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECÁNICO ELECTRICISTA
(ÁREA ELÉCTRICA Y ELECTRÓNICA)

P R E S E N T A :

GREGORIO GARCÍA TOSCANO

ASESOR: ING. JUAN GASTALDI PÉREZ

MÉXICO **2002**

PAGINACION DISCONTINUA

Con cariño y gratitud a mis padres Virginia y Gregorio, y a mi hermana Nora Angélica.

OBJETIVOS

- Evaluar la viabilidad de las tecnologías de VoIP (Voz sobre IP) como una alternativa para los nuevos proyectos de redes de voz que surjan en la UNAM.

- Exponer las experiencias y proyectos que han tenido lugar en la UNAM en cuanto a tecnologías de VoIP.

INTRODUCCIÓN

La *DGSCA* (*Dirección General de Servicios de Cómputo Académico*) en la UNAM, tiene como una de sus funciones básicas la investigación y evaluación de las nuevas tecnologías que están emergiendo en el campo de las redes de datos y voz, con el fin de aportar soluciones a los retos actuales y futuros que la Universidad tendrá que afrontar en estos rubros, derivados de la actividad académica, docente y de investigación que en ella tienen lugar.

En este sentido, la DGSCA, a través de su *Departamento de Redes*, ha formado *grupos de trabajo* internos para el estudio y desarrollo de distintos temas relevantes en el área de la tecnología de redes de datos tales como *H323*, *QoS*, *VoIP*, *IP-Multicast*, *MPLS*, *IPv6*, *Network Security*, *Wireless*, entre otros. El propósito de cada uno de estos grupos de trabajo va encaminado a generar la mayor cantidad posible de experiencia, con vistas a su posible implementación en la UNAM y como solución a problemas específicos o globales que tienen o tendrán lugar dentro de la misma. Aun y cuando alguna de ellas jamás logre una aplicación concreta dentro de la red, la experiencia y los resultados obtenidos servirán como detonante para todas las demás y para el todo en su conjunto, debido a la interconexión tan estrecha de los temas.

La experiencia que están obteniendo estos grupos de trabajo se esta volviendo cada vez más importante, toda vez que la UNAM se encuentra inmersa en el *proceso de reestructuración del backbone de su red de datos*. El camino que haya de tomar dicha reestructuración vendrá dictado por las necesidades actuales y futuras de sus usuarios, que en general demandan cada vez más *aplicaciones multimedia en tiempo real*, como son las *aplicaciones de voz y videoconferencia*. La apuesta de la UNAM en este sentido está sobre una "*Red Multiservicios de Alta Velocidad GigabitEthernet*" capaz de integrar todo tipo de información (*voz, video y datos*).

Otro factor que ha servido sin lugar a dudas como detonante para el estudio de todas estas tecnologías emergentes, es la integración de la UNAM a la *Internet2* desde hace ya algunos años. A este respecto, uno de sus principales objetivos es integrar a las Facultades e Institutos de la Universidad al movimiento vanguardista de la Internet2, alentando y facilitando la consecución de sus proyectos en materia de intercambio de información multimedia con sus homólogos en otras partes del país o del mundo.

En cuanto a VoIP (Voz sobre IP) se refiere, han sido varios los esfuerzos que se han realizado a fin de comprender y desarrollar esta tecnología. De hecho, hoy se cuenta ya con la primera red de VoIP sobre el campus universitario, y se está trabajando para llevarla hacia la WAN (*Proyecto de reestructuración de las Preparatorias*), así como a la Internet2 (*Proyecto Red Nacional e Internacional de VoIP sobre la Internet2*).

La tecnología de VoIP nos permite implementar redes de voz sobre las redes de datos LAN y/o WAN ya establecidas en nuestra empresa o institución. Esta tecnología ofrece prácticamente todas las funcionalidades y facilidades de un sistema telefónico tradicional a base de PBX's, pero con la ventaja adicional de ofrecer un ahorro en su implementación debido a su capacidad para hacer uso de la red de datos ya establecida, salvándose con ello los costos que implican la instalación de la red de cableado e infraestructura telefónicas necesarias (rosetas, cableado, registros, patches de concentración, obra negra, etc).

Aunado a lo anterior, está la facilidad en su mantenimiento y administración, así como la posibilidad de proporcionar mayor seguridad en las comunicaciones mediante la encriptación de la información. Así mismo, se puede mencionar su capacidad para ahorrar costos derivados de las llamadas de larga distancia debido a la posibilidad de hacer uso de la red WAN corporativa o la Internet como medio de conexión. Por último, ofrece una plataforma mucho más poderosa para el desarrollo de la próxima generación de servicios y aplicaciones CTI (*Computer Telephony Integration*).

El objetivo de esta tesis es presentar las experiencias que se han tenido en la UNAM en cuanto a tecnologías de VoIP, así como los proyectos que se han realizado o aquellos en los que actualmente se está trabajando. Por otra parte, esta tesis habla de la necesidad de contar con *Redes Multiservicios de Alta Velocidad bien diseñadas y dimensionadas*, a fin de que VoIP sea viable en la empresa. Aún quedan algunos retos y dificultades que resolver a fin de que VoIP sea una realidad en la Internet Comercial, y de manera que pueda competir de igual a igual con la Telefonía Tradicional por Conmutación de Circuitos. A la cabeza de esta lista está sin lugar a dudas la necesidad de contar con *mecanismos de QoS* (*Calidad de Servicio*) sobre las redes IP, de manera que las aplicaciones multimedia en tiempo real tengan un *servicio de entrega predecible en el tiempo.*

ÍNDICE

CAPÍTULO 1: LA PSTN Y EL SURGIMIENTO DE VoIP

CAPÍTULO 2: FUNDAMENTOS DE VoIP

CAPÍTULO 3: PROTOCOLOS DE SEÑALIZACIÓN H.323 Y SIP

CAPÍTULO 4: CALIDAD DE SERVICIO (QoS)

CAPÍTULO 5: RED DE DATOS DE LA UNAM E INTERNET2

CAPÍTULO 6: PROYECTOS DE VoIP EN LA UNAM E INTERNET2

CAPITULO 7: PRUEBAS REALIZADAS Y PROYECTOS A FUTURO

CAPÍTULO 1

LA PSTN Y EL SURGIMIENTO DE VoIP

"La bellota no es todavía roble cuando germina; debe realizarse a través de largos veranos y crueles inviernos; ha de aguantar los hielos, las nieves y los embates del viento antes de convertirse en un roble completamente desarrollado".

Si bien son los fundamentos los que hacen fuerte a una tecnología, son esos mismos fundamentos los que pudieran limitarla e impedirle alcanzar nuevas posibilidades de desarrollo. La PSTN (Red Telefónica Pública Conmutada) es una red que ha estado evolucionando desde hace más de 125 años. Durante ese tiempo, ha logrado ofrecer un nivel de servicio y confiabilidad como pocas redes mundiales. Sin embargo, debido a su carácter cerrado a la innovación y a las prácticas monopólicas de quienes la manejan, la PSTN no ha sido capaz de ofrecer las aplicaciones y los servicios que se requieren en el mundo moderno, ni aun menos los costos que se esperarian de ella.

En este capítulo se cubren las bases de la PSTN, sus componentes y sus servicios a fin de dar una breve introducción a la forma en la que opera actualmente, para luego pasar a discutir en dónde y por qué la PSTN puede ser mejorada. Finalmente, se anuncia el surgimiento de la Telefonía-IP que promete reducir los costos y ofrecer toda una nueva generación de servicios y aplicaciones en donde las bondades de la Telefonía y la Computación queden fusionadas. Así mismo, se enuncian las dificultades y los retos que la Telefonía-IP junto con la Internet Comercial deberán enfrentar a fin de hacer viable la telefonía sobre las redes de datos IP.

1.1 Los Comienzos de la PSTN

Los comienzos de la telefonía se remontan al año de 1876 cuando Alexander Graham Bell realizó la primera llamada en lo que se llamó *circuito ring-down*. Bajo este esquema, el establecimiento de una llamada no requería la marcación de un número ni había un timbrado involucrado. En su lugar, un cable físico conectaba directamente a los dispositivos extremos. Cuando una persona levantaba el teléfono su interlocutor también podía hacerlo con la certeza de que la llamada se establecería inmediatamente.

Con el tiempo, este simple diseño evolucionó desde una transmisión en un solo sentido, por la cual un único usuario podía hablar a la vez, a una transmisión bidireccional, en la que ambos usuarios podían hablar al mismo tiempo.

Este tipo de comunicación tenía la desventaja de requerir un cable físico hacia cada lugar al que un usuario deseara llamar. De manera que si hubiera **N** usuarios en una red y se requiriera interconectarlos totalmente, se necesitarían **Nx(N-1)/2** conexiones, lo cual por supuesto ni es costeable ni físicamente viable (ver Figura 1-1).

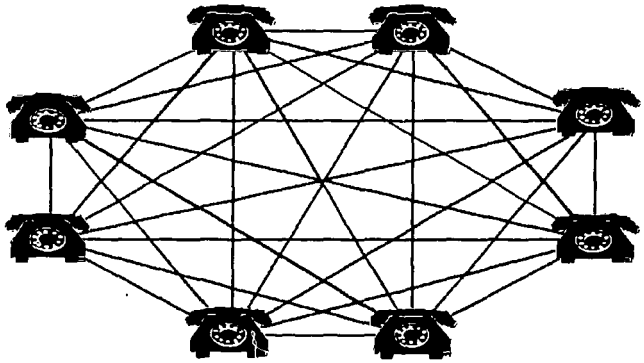


Figura 1-1:Conexión de todos contra todos (o Full-mesh).

Así pues, el siguiente desarrollo que vino al mundo de la telefonía fue la centralización de las conexiones de usuario en un punto de convergencia común, llamado CO (Central Office). Las CO's también tenían como una de sus funciones primarias el switcheo (conmutación) de las llamadas. En un principio el switcheo era realizado manualmente por un operador, mas con el paso del tiempo y con el advenimiento de los nuevos desarrollos en el campo de la electrónica (como el transistor y el circuito integrado), el switcheo pasó a ser realizado de manera automática por equipos especialmente diseñados llamados switches (ver Figura 1-2).

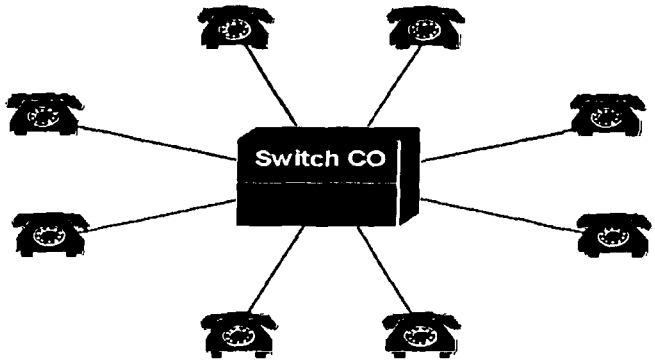


Figura 1-2:Esquema telefónico centralizado y switchado por la CO.

1.2 Señales Analógicas y Digitales

Puesto que todo cuanto escuchamos, incluyendo el habla humana, está en una forma analógica; no es de extrañar entonces que las redes telefónicas estuviesen basadas en un inicio sobre una infraestructura totalmente analógica. Sin embargo, aunque la comunicación analógica es ideal para la interacción humana, no es robusta ni lo suficientemente efectiva para recobrarse del ruido siempre presente en las líneas telefónicas. En los principios de las redes telefónicas, la transmisión analógica de la voz era pasada a través de amplificadores que reavivaban la señal. Empero, esta práctica no solo amplificaba la voz, sino también el ruido de la línea, lo que con frecuencia llevaba a conexiones defectuosas. Así pues, se requería de un método especial de amplificación que limpiase a la señal (ya no necesariamente analógica) del ruido externo al mismo tiempo que la iba amplificando.

Es en este momento de la historia cuando entran a la escena las redes telefónicas digitales, en las que el ruido de la línea no representa un problema tan grave, pues los repetidores no solo amplifican la señal, sino que también la llevan a su condición original. Esto es posible en las comunicaciones digitales gracias a que están basadas en la transmisión de sólo 1´s y 0´s, de manera que un repetidor digital sólo tiene que decidir si regenerar un 1 o un 0.

Cuando los beneficios de la representación digital se hicieron evidentes, las redes telefónicas emigraron hacia un esquema digital basado en las técnicas de ***codificación y multiplexación PCM-TDM***, como veremos más adelante.

1.3 Digitalización de las Señales de Voz

PCM (Pulse Code Modulation / Modulación por Pulsos Codificados) es el método más común para codificar las señales de voz en un flujo digital de 1's y 0's. Al igual que cualquier otra técnica de muestreo, PCM utiliza el teorema de Nyquist para obtener la versión digital de una señal analógica. El teorema de Nyquist establece básicamente que "*si una señal de voz es muestreada a intervalos de tiempo regulares y a la velocidad de por lo menos dos veces la frecuencia más alta, entonces las muestras obtenidas retienen toda la información original de la señal*".

El proceso PCM completo (ver Figura 1-3) para obtener la versión digital de una señal, y aprovechar de esta manera los beneficios asociados a la transmisión digital (como son su recuperación ante el ruido de la línea mediante el uso de repetidos "regeneradores"), es como sigue:

- ***Filtrado*** → Las señales analógicas primeramente son pasadas a través de un filtro (pasa-bajas) que filtra todo por arriba de los 4000 Hz. Esto entre otras cosas, tiene el efecto de limitar la cantidad de crosstalk en la transmisión, y deja pasar el rango de frecuencias donde prácticamente se encuentra concentrada la inteligencia de la señal.
- ***Muestreo de Nyquist*** → La señal analógica filtrada es entonces muestreada a una velocidad de 8000 (= 2 x 4000) veces por segundo, de acuerdo al Teorema de Nyquist.
- ***Cuantificación*** → Después de que la señal ha sido muestreada, es convertida a su forma digital discreta. Para tal efecto, las amplitudes de las muestras analógicas logradas son correlacionadas primeramente con una serie discreta y limitada de amplitudes digitales llamadas *niveles de cuantización*.
- ***Codificación y compresión*** → Cada muestra analógica es entonces ligada a la palabra o código binario asociado al nivel de cuantización determinado en el paso anterior. Por lo general, el esquema de digitalización PCM usa palabras de 8 bits ($2^8 = 256$ niveles de cuantización) para el proceso de codificación, así como un logaritmo de compresión para asignar más bits a las partes de la señal con menor amplitud.

Nota: *Dos variaciones de PCM son comúnmente usadas en la actualidad: la Ley-μ y la Ley-A, estándares usados en Norte América y Europa, respectivamente. Estos métodos son similares en cuanto que ambos usan compresión logarítmica para lograr de 12 a 13 bits de calidad linear PCM en palabras de solo 8 bits, pero difieren en detalles menores (por ejemplo, la ley-μ tiene una ligera ventaja sobre la ley-A en términos de una mayor razón o nivel de señal a ruido S/N).*

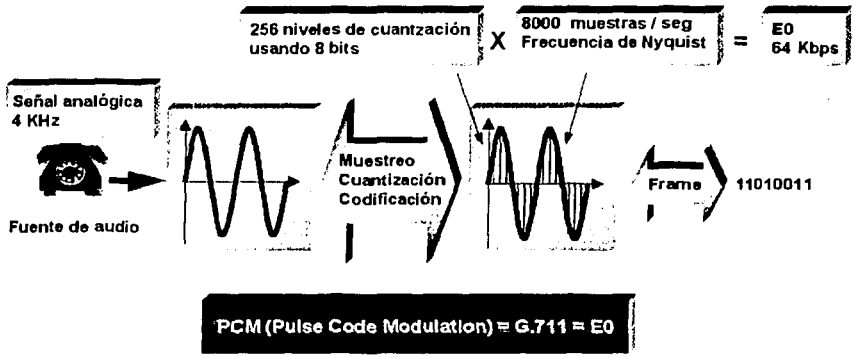


Figura 1-3: Proceso PCM para la digitalización de una señal analógica.

La cantidad de información transportada por una señal digital PCM es de 64 Kbps (= 8 bits x 8000 muestras/segundo). Este número representa la base para las llamadas "***Jerarquías Digitales PCM/TDM***" actuales en la Telefonía:

- ***Norma Europea*** → E0 (canal de 64 Kbps).
- ***Norma Americana*** → T0 (canal de 64 Kbps).

1.4 Estructura de la Red Telefónica

La infraestructura de la red telefónica comienza con un simple par de cobre que va desde la CO hasta el hogar. Este cableado físico es conocido comúnmente como *bucle local* y su función es conectar los teléfonos de abonado al switch de la CO (también conocido como switch Clase 5 o switch CO). La trayectoria lógica de comunicación entre la CO y el hogar es conocido como *línea telefónica*, y normalmente corre sobre un bucle local. Por otra parte, la trayectoria de comunicación entre dos switches CO es conocido como *troncal*.

En la Figura 1-4 se presentan los componentes básicos de toda red telefónica actual, es decir: los bucles locales, las líneas telefónicas, las troncales CO y las troncales privadas entre PBX'S (mejor conocidas como *tie lines* en el argot telefónico). Una explicación más detallada sobre estos componentes se presenta a continuación.

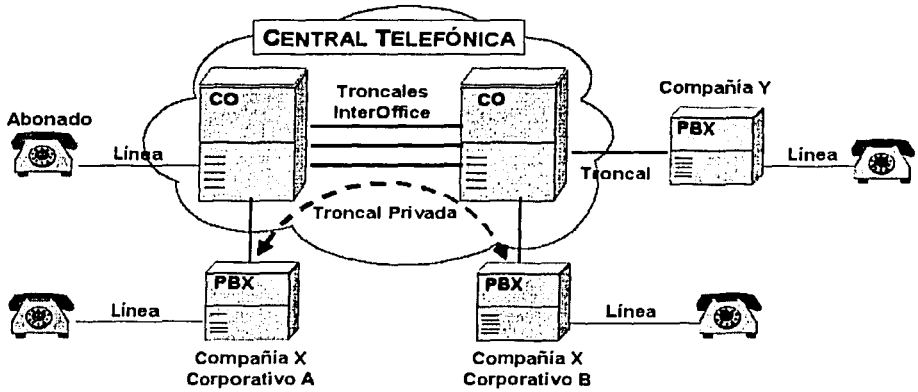


Figura 1-4: Bucle local, líneas y troncales telefónicas.

1.4.1 Bucle Local

Un bucle local es literalmente el par de cobre que conecta directamente un teléfono al switch CO de la compañía telefónica o al PBX de una empresa. Éste consiste de dos o hasta cuatro hilos, que son por lo general trenzados para minimizar los efectos de la inducción magnética creada al fluir la corriente por los cables (efecto mejor conocido como *crosstalk*).

1.4.2 Líneas

Los términos línea y bucle son frecuentemente confundidos. Aunque una línea está típicamente basada en un bucle físico, no es necesariamente una conexión física. Una línea es más bien la trayectoria lógica de comunicación entre un teléfono de usuario y un switch, o entre un PBX y un switch CO. Una línea rentada (o *tie line*) es una línea dedicada contratada a un *carrier* (proveedor de servicios de transporte) para el uso privado y exclusivo de un cliente arrendante que desea mantener una conexión directa entre dos sus PBX's corporativos.

1.4.3 Troncales

Mientras que un bucle es el medio a través del cual un teléfono se conecta a un switch, una troncal es un canal de comunicaciones mediante el cual se conectan dos switches, sean estos PBX's y/o switches CO. Por lo general, una troncal es un recurso compartido por todos los usuarios asociados a un sistema telefónico privado conformado por uno o más switches.

Los tipos de troncales más comunes en la Telefonía son las siguientes:

- ***Troncal Privada (Tie Line)*** → troncal usada para conectar a dos PBX's remotos (generalmente de una misma empresa) haciendo uso de la infraestructura de un carrier.
- ***Troncal CO*** → troncal usada para conectar directamente un PBX o un switch CO o para conectar dos switches CO.
- ***Troncal Foreing Exchange*** → troncal usada para conectar directamente un teléfono remoto a un PBX.
- ***Troncal DID/DOD (Direct Inward Dial/Direct Outward Dial)*** → troncal de un solo sentido que permite a un usuario marcar remotamente sobre un PBX (DID) o sobre un switch CO (DOD) sin la intervención de una operadora.

1.4.4 Esquema de Switcheo Jerarquizado

Así como no es efectivo ni costeable poner una línea telefónica entre un teléfono y cualquier otro teléfono al que se quiera llamar, tampoco es efectivo ni costeable poner una troncal entre cada par de switches CO. De esta manera, los switches CO de la red telefónica pública son desplegados por cuestiones de escalabilidad y costos bajo un esquema jerárquico. Los switches CO (o switches Clase 5) se interconectan a través de troncales hacia *switches tandem* (o switches Clase 4). Por último, existen switches tandem de mayor jerarquía que conectan a los switches tandem locales. En la Figura 1-5 se muestra un modelo simplificado del estructura jerárquica de la red telefónica pública, aunque de hecho casi todas las PSTN's actuales usan hasta 5 niveles en su estructura.

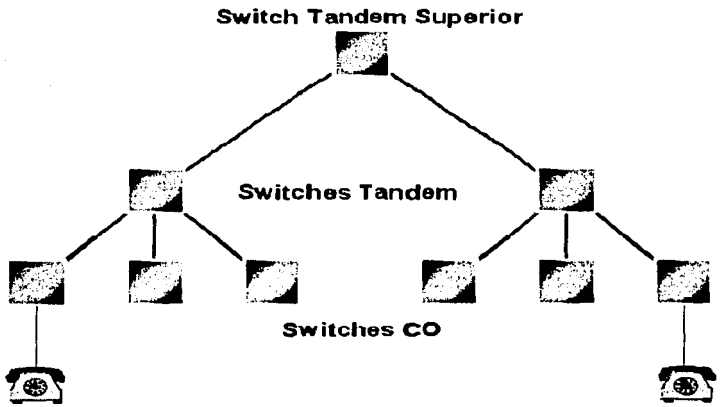


Figura 1-5: Esquema de Switcheo Jerarquizado

Hay veces en las que los switches CO se conectan unos a otros directamente. El que dos switches CO se conecten o no directamente, depende del flujo de llamadas entre ellos. Si bastante tráfico ocurre entre dos switches CO, un circuito dedicado es puesto entre ellos, con lo cual se logra liberar a toda una cadena de switches tandem superiores de esta carga innecesaria de llamadas.

1.5 Señalización en la PSTN

Ahora que se conoce cómo y por qué la PSTN se divide en jerarquías, es menester comprender cómo logran interactúan entre sí dos switches (sean estos PBX's o switches CO). Para tal efecto es importante profundizar en los conceptos de señalización, direccionamiento y ruteo, términos comunes tanto a las redes de voz como a las redes de datos.

El propósito de la señalización en una red de voz es el establecimiento y control de una conexión o llamada. Generalmente, los tipos de señalización usados sobre una red telefónica pueden agruparse dentro de una de las siguientes categorías:

- ***Señalización Usuario-a-Red*** → describe la forma en la que el teléfono del usuario se comunica con el switch de la CO o el PBX de la empresa.
- ***Señalización Red-a-Red*** → describe la forma en la que dos switches CO o PBX's se intercomunican.

1.5.1 Señalización Usuario-a-Red

Generalmente cuando un usuario se conecta hacia la PSTN lo hace a través de líneas analógicas o líneas digitales RDSI. El método de señalización más común usado para el caso de las comunicaciones analógicas usuario-a-red es la señalización DTMF (Dual Tone Multi-Frecuency). DTMF es conocida como una *señalización en banda* porque los tonos son transportados a través del canal de voz. La Figura 1-6 muestra la matriz de frecuencias usada para derivar los tonos asociados a cada dígito o tecla de un teléfono. Cuando se levanta el mango de un teléfono y se pulsan dígitos, los tonos que pasan desde el teléfono al switch CO al cual se conecta, le dicen a éste a que número se desea llamar.

Nota: la señalización en banda sufre de algunos problemas, el más notorio de los cuales se refiere a la posibilidad de la pérdida de los tonos. Esto ocurre cuando la señalización es transportada a través del canal de voz, y es la razón común por la que algunas veces se experimenta problemas cuando se accesa remotamente al correo de voz.

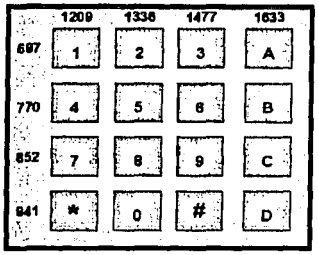


Figura 1-6: DTMF (Dual Tone Multi-Frecuency).

RDSI usa un método de señalización diferente conocida como *señalización fuera de banda*, ya que la señalización es transportada sobre un canal separado al de la voz. El canal sobre la cual es transportada la voz es llamado canal B y es de 64 kbps. Por otra parte, el canal sobre el cual la señalización es transportada es llamado canal D (o canal delta) y es de 16 kbps. La Figura 1-7 muestra una interface BRI (Basic Rate Interface), la cual consiste de dos canales B y un canal D.

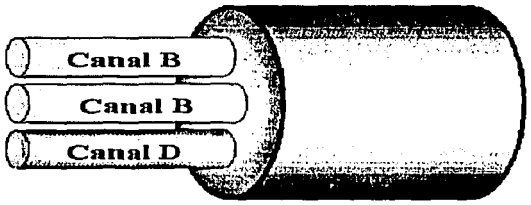


Figura 1-7: Interface BRI = 2B + D = 144 Kbps.

La señalización fuera de banda ofrece varios beneficios, incluyendo los siguientes:

- La señalización está multiplexada sobre un canal común.
- El efecto de *glare* se reduce significativamente (este efecto se da cuando dos personas sobre un mismo circuito amarran el extremo opuesto del circuito al mismo tiempo).
- Menor retardo de posmarcación.
- Facilidades adicionales son mejoradas al contar con un mayor ancho de banda.
- Puesto que los mensajes de establecimiento de llamada son enviados por un canal diferente, el establecimiento satisfactorio de una llamada es significativamente incrementado.

1.5.2 Señalización Red-a-Red

La señalización red-a-red (o de switch a switch) es normalmente usada sobre los siguientes medios de transmisión:

- T1/E1 sobre par trenzado o coaxial.
- T3/E3 o T4 sobre cable coaxial.
- T3/E3, T4/E4 sobre un enlace de microondas.
- SONET (Synchronous Optical Network) sobre fibra óptica.

Entre los tipos de señalización red-a-red están los métodos de señalización en banda tales como MFS (Multi-Frecuency Signaling) y RBS (Robbed Bit Signaling). Estos tipos de señalización pueden también ser usados como métodos de señalización usuario-a-red.

Los sistemas de transporte digital (T1 o T3) usan los bits A y B para indicar la señalización de supervisión (on/off hook). Los bits A/B emulan los tonos SF (Single Frecuency) que típicamente usa la presencia o ausencia de una señal para señalizar las transiciones de los bits A/B. Estos bits pueden ser robados del canal de voz o ser multiplexados sobre un canal común (esto último ocurre principalmente con los E1's en Europa).

MFS es similar a DTMF, pero utiliza un conjunto diferente de frecuencias. Como con DTMF, los tonos MFS son enviados en banda, pero en lugar de ser usados para señalizar entre un teléfono y un switch, los tonos MFS son usados para la señalización entre switches (sean de CO o PBX's).

La señalización red-a-red también usa el método de señalización fuera de banda conocido como SS7 (Signaling System 7) o C7 en los países europeos. SS7 es poderoso porque es un método de señalización fuera de banda y se interconecta a la Red Inteligente (RI). La conexión a la Red Inteligente permite a la PSTN ofrecer servicios CLASS (Custom Local Area Signaling Services).

SS7 es un método de envío de mensajes entre dos switches para un control básico de las llamadas y para hacer posible los servicios CLASS (que descansan sobre los switches CO y sobre la red SS7). La señalización SS7 es también usada para interconectar switches y bases de datos para ofrecer servicios de red especiales, tales como los servicios de 01-800 y los LNP's (Local Number Portability).

Algunos de los beneficios de moverse hacia una red SS7 son los siguientes:

- Reducción del retardo de posmarcación.
- Mejoramiento en el establecimiento satisfactorio de la llamada.
- Conexión a la red inteligente → esta conexión provee nuevas aplicaciones y servicios transparentes a lo largo de toda la red, así como la capacidad para crear nuevos servicios y aplicaciones más rápidamente.

1.6 Servicios y Aplicaciones en la PSTN

Numerosos servicios que no estaban disponibles hace solamente unos años atrás están ahora al alcance y servicio de los usuarios de la PSTN. Estos servicios vienen comúnmente en una de las siguientes dos formas:

- ***Facilidades del cliente llamante.***
- ***Facilidades CLASS (Custom Local Area Signaling Services).***

Las facilidades del cliente llamante dependen de los switches CO (y no de la PSTN entera) para transportar información entre switch y switch. Las facilidades CLASS, por otra parte, requieren de la señalización SS7 para transportar estas facilidades entre dos extremos cualesquiera sobre la PSTN.

Las siguientes son algunas de las facilidades del cliente llamante comúnmente encontradas en las PSTN's de hoy:

- ***Call waiting*** → notifica el arribo de una nueva llamada a un usuario que ya está enrolado en otra llamada.
- ***Call forwarding*** → permite que un usuario enrute sus llamadas entrantes hacia un destino diferente.
- ***Three-way calling*** → permite las conferencias tripartitas.

Con el despliegue de la señalización SS7 y de la Red Inteligente (RI), facilidades avanzadas pueden ahora ser transportadas extremo a extremo. En la siguiente lista se mencionan algunas de las facilidades CLASS actuales:

- ***Display*** → desplegado en pantalla del número de teléfono del llamante o ANI (Automatic Number Identification).
- ***Call blocking*** → bloqueo de llamada a números de teléfono específicos.
- ***Calling line ID blocking*** → bloqueo de que el número de teléfono sea mostrado en el display de algún otro teléfono (esto no procede con números 800 y otros números).
- ***Automatic callback*** → permite poner en espera al último número marcado y del cual se obtuvo una señal de ocupado, de manera de que cuando aquél se desocupe se pueda concretar de manera automática la llamada.
- ***Calling cards*** → son tarjetas de llamadas prepagadas; uno marca el número deseado, ingresa su password, y después habla con el destino.
- ***Números 01-800*** → el costo de la realización de una llamada no es cargado al llamante sino el llamado (aunque normalmente bajo una tasa premium).
- ***Líneas privadas o contratadas.***

1.7 Planes de Numeración en la PSTN

Una característica de la PSTN que poco ha cambiado con el tiempo es el plan de numeración o direccionamiento. Esencialmente dos planes de numeración son usados actualmente en la PSTN dependiendo del país en cuestión: el Plan de Numeración Norteamericano (NANP) y el Plan de Numeración Internacional E.164 de la ITU-T (International Telecommunication Union).

1.7.1 Plan de Numeración NANP

NANP es un plan de numeración de 11 dígitos compuesto de tres partes:

- ***Código de área o NPA (Numbering Plan Area).***
- ***Código de la CO (NXX).***
- ***Número de estación (XXXX).***

Este plan de numeración es frecuentemente referido como ***NPA-NXX-XXXX*** (donde NXX representa el código de área, con N tomando un valor entre 2 y 9 y X con un valor entre 0 y 9).

NANP es también referido como 1+10. Esto significa que cuando un 1 es el primer dígito marcado, éste será seguido por un número NPA-NXX-XXXX de 10 dígitos. Esto permite a una CO determinar cuando debe esperar un número telefónico de 7 o 10 dígitos.

1.7.2 Plan de Numeración E.164 de la ITU-T

La recomendación E.164 de la ITU-T especifica que para encaminar una llamada hacia un teléfono subscriptor específico será usada la siguiente información:

- ***Código de País o CC (Country Code).***
- ***Código Nacional de Destino o NDC (National Destination Code).***
- ***Número de Subscriptor o SN (Subscriber Number).***

El CC consiste de uno, dos o tres dígitos. El primer dígito (1-9) define la zona de numeración mundial (una lista de todas las CC's es encontrada en la Recomendación E.164 de la ITU-T). El NDC y el SC varían en longitud en base a las necesidades de un país, aunque ninguno de ellos contiene más de 15 dígitos.

Aunque los planes de numeración puedan no parecer importantes en este momento, son cruciales para el despliegue e implementación de toda red telefónica por conmutación de circuitos o aún de una red por conmutación de paquetes de VoIP.

1.8 Surgimiento de la Telefonía-IP

La convergencia de las redes de voz, video y datos ha sido un sueño largamente acariciado por todos. Las ventajas detrás de esta convergencia son innumerables: reducción en los costos de instalación, operación y mantenimiento, así como toda una nueva gama de servicios y aplicaciones que aprovechan la integración. Sin embargo, lo más que se había logrado hasta hace poco era pasar información de voz, video y datos sobre una misma infraestructura de transmisión (basada en switches ATM o multiplexores TDM) aunque sin lograr una verdadera integración.

Hoy con el crecimiento explosivo de la Internet y su capacidad para sortear toda clase de retos, es evidente que si alguna tecnología será capaz de integrar todo ésa será IP, haciendo de las redes de datos IP el punto de convergencia para todo tipo de aplicaciones y tráfico. El éxito de IP y en general de la suite de protocolos TCP/IP es tal que a lo largo de su desarrollo y evolución se han confeccionado algunas frases que hacen gala de su fortaleza:

- ***IP over everything*** → es decir, IP es capaz de correr sobre todo tipo de tecnología de enlace de datos LAN o WAN: Ethernet, FDDI, Token Ring, HDLC, ATM, FrameRelay, SONET, etc.
- ***Everything over IP*** → es decir, todo tipo de aplicación con algún componente de red es capaz de correr sobre IP.

La Internet junto con la Web han revolucionado el estilo de vida de las personas así como la forma de hacer negocios a lo largo de todo el mundo. Han dado paso a todo un nuevo paradigma en el mundo de los negocios en la forma del *e-commerce* (*e-business*), portales, *e-tailers* y aplicaciones colaborativas, etc. La Web a permitido a los usuarios encontrar productos y servicios, y a las empresas encontrar clientes o empresas aliadas con un solo click del mouse.

Tan solo en los últimos años la Internet y la Web han generado más innovaciones de lo que la Telefonía Tradicional ha producido en toda su historia (de alrededor de 125 años). Así pues, no es de extrañar que una de las próximas fronteras de la Internet y la Web sea aplicar el mismo grado de innovación a la Telefonía.

Para todos es evidente que las facilidades y los servicios de la Telefonía actual deben cambiar radicalmente para convertirse en un miembro funcional de la revolución en el mundo de los negocios. Sin embargo, dada sus limitaciones, es virtualmente imposible para Telefonía actual responder a estos requerimientos emergentes. Es precisamente en este punto de la historia que surge la necesidad de contar con algo como la Telefonía-IP. La Telefonía-IP hace de las comunicaciones de voz una aplicación más que corre sobre las redes de datos IP, y aprovecha toda la experiencia adquirida por la Internet y la Web para el desarrollo de la próxima generación de servicios y aplicaciones telefónicas.

En cuanto a servicios telefónicos se refiere, hay una clara imagen de lo que los usuarios y empresas requieren en el contexto de las nuevas necesidades del mundo actual. Por una parte, los usuarios quisieran seguir usando el teléfono para hacer y recibir llamadas así como para desplegar sus mensajes de voz. Pero por otra parte, quisieran también tener integrado su aparato telefónico a la PC y sacar provecho de todo tipo de aplicaciones CTI (Computer Telephony Integration), tales como manejo de Directorios Telefónicos, Mensajería Unificada, Centros de Llamadas, etc. En otras palabras, realizar las tareas más aconsejables para la PC, sobre la PC; y aquellas más aconsejables para el teléfono usando el teléfono y tener ambos dispositivos integrados.

1.9 Motivos detrás de la Convergencia

Aunque la Telefonía Tradicional (basada en los PBX's empresariales, los switches CO y la red conmutada o PSTN) es efectiva, y de hecho hace un buen trabajo en aquello para lo que fue diseñada, hay varias razones técnicas y de mercado que están promoviendo su transformación hacia una nueva red en donde la voz sea una aplicación más que corra sobre las redes de datos IP. Esto está ocurriendo por varias razones como hemos visto anteriormente:

- Dado que el tráfico de datos está creciendo mucho más rápido que el tráfico telefónico, hay un considerable interés en transportar voz sobre las redes de datos (en contraposición a la tradicional forma en donde se transportaban datos sobre las redes de voz).
- Con el incremento de la competencia debido a la desregulación de muchos de los mercados de las telecomunicaciones, varios carriers están buscando nuevas formas de mantener a la clientela existente. Su método por excelencia es la seducción mediante nuevos servicios y aplicaciones.
- La Telefonía Tradicional no es lo suficientemente rápida para crear y desplegar los nuevos servicios y aplicaciones que se necesitan para los negocios de hoy en la era del e-commerce, debido a estar cerrado su desarrollo a solo unos cuantos proveedores. Una infraestructura más abierta, por la cual muchos desarrolladores de software independientes pudieran proveer las aplicaciones, posibilitaría que más soluciones y aplicaciones creativas fueran desarrolladas.
- Las soluciones telefónicas tradicionales son complicadas tanto para los administradores como para los usuarios. A causa de la desalentadora complejidad para interoperar con los PBX's, los usuarios solo utilizan una fracción del conjunto total de las facilidades disponibles en el sistema.
- Ley de Moore: establece que la capacidad de procesamiento de los sistemas de cómputo se duplica cada 18 meses aproximadamente.
- El tráfico de voz, video y datos (o V/V/D) no pueden converger de manera total sobre la red telefónica tal y como está actualmente.

- Desperdicio del ancho de banda: las llamadas por redes de conmutación de circuitos requieren un circuito permanente de 64 Kbps por cada llamada telefónica. Ya sea que los participantes de la llamada hablen o no, los 64 Kbps de la conexión establecida no podrán ser usados por ningún otro usuario. Esto significa entre otras cosas, que la compañía telefónica o carrier no pueda usar este ancho de banda para ningún otro propósito y deba cobrar a sus usuarios en base al consumo de los recursos. Las redes de datos por otra parte, tienen la capacidad de usar el ancho de banda solamente cuando es requerido. Esta diferencia, aunque parezca pequeña, es el mayor beneficio de una red de voz corriendo bajo un régimen de switcheo de paquetes.

1.10 Desregularización de los Mercados

En la sección anterior se vieron algunos de los inconvenientes que están impulsando la convergencia de las redes de voz sobre las redes de datos. Una razón más para esta convergencia es más bien política que técnica. Varios países a lo largo de todo el mundo están abriendo sus mercados de telecomunicaciones a la competencia, y en algunos casos, se están vendiendo las telefónicas gubernamentales a las empresas privadas al darse cuenta de que las Telecomunicaciones serán importantes para sobrevivir en el presente siglo por el conocimiento y la prosperidad que generan.

Muchos nuevos carriers están considerando aprovechar esta oportunidad en la desregularización de los mercados. Impulsados por el influjo de la nueva competencia los esquemas de precios están cambiando, y tanto los nuevos como los viejos carriers están considerando desplegar lo último en tecnología al menor costo a fin de mantenerse en el mercado. La ventaja adicional de desplegar nueva tecnología es la habilidad para ofrecer servicios de valor agregado y desplegar estos nuevos servicios en poco tiempo.

1.11 Modelo Arquitectónico de la PSTN

La Telefonía Tradicional por Conmutación de Circuitos (así como la primera generación de soluciones en la Telefonía-IP) están basados sobre un modelo de procesamiento centralizado. Esto quiere decir que toda la inteligencia del sistema se encuentra concentrada en los PBX's o switches CO, y que deban por tanto realizar todas las funciones telefónicas, tales como el establecimiento de la llamada, el desvío de las llamadas, las conferencias, etc. Todas las peticiones, respuestas y cambios de estado deben ser procesados por el switch central, con la estación final (el teléfono) siendo una terminal tonta.

Las siguientes son algunas de las características de la Telefonía Tradicional:

- ***Modelo de procesamiento centralizado*** → la inteligencia del sistema está centralizada sobre los PBX's o switches CO.
- ***Terminales tontas*** → la manera en la que los usuarios acceden a las facilidades o servicios del sistema telefónico es a través del uso de códigos o del botón de flash.
- ***Software fuertemente dependiente del Hardware*** → las facilidades y servicios de voz están residentes en software, el cual por lo general es fuertemente dependiente del hardware propietario al fabricante o desarrollador.

1.12 Modelo de la Telefonía-IP

La Telefonía-IP, y en especial la segunda generación de soluciones de Telefonía-IP basadas en el protocolo SIP, siguen una arquitectura distribuida cliente/servidor, la cual a través de la Web ha demostrado ser una de las arquitecturas más exitosas de la historia.

La Web ha posibilitado que muchos servidores inteligentes ubicados en cualquier parte de la red interactúen con dispositivos clientes inteligentes basados en browsers. Son los dispositivos cliente (y no el servidor), los que inician y controlan la comunicación con el servidor. Cuando un usuario accesa a algún sitio, es su browser el que hace la petición, abre las aplicaciones (JAVA, Java script, Flash, Active X, etc) necesarias y reensambla la información enviada por el servidor. Además hay una completa desagregación de los servicios en el modelo de la Web; no solamente los servicios provienen de diferentes servidores sino que estos pueden ser provistos por diferentes y múltiples *service providers*. La características del modelo de procesamiento distribuido cliente/servidor de la Telefonía-IP son:

- ***Dispositivos de usuario inteligentes (clientes del sistema).***
- ***Servidores inteligentes y variados distribuidos a lo largo de la red.***
- ***Modelo abierto a la innovación y al rápido desarrollo de aplicaciones a bajos costos.***

1.13 Telefonía-IP

En la Figura 1-8 se ilustra el modelo por capas de la Telefonía-IP por el cual estándares abiertos existen en todas sus capas: la ***Capa de Infraestructura por Paquetes*** que transporta los paquetes de voz a nivel físico, la ***Capa de Control*** que es independiente de la capa de infraestructura, y la ***Capa de Aplicaciones*** que opera a través de API's (Aplication Programming Interfaces) abiertas que permiten que *Desarrolladores de Software Independientes (DSI)* creen aplicaciones de usuario interesantes.

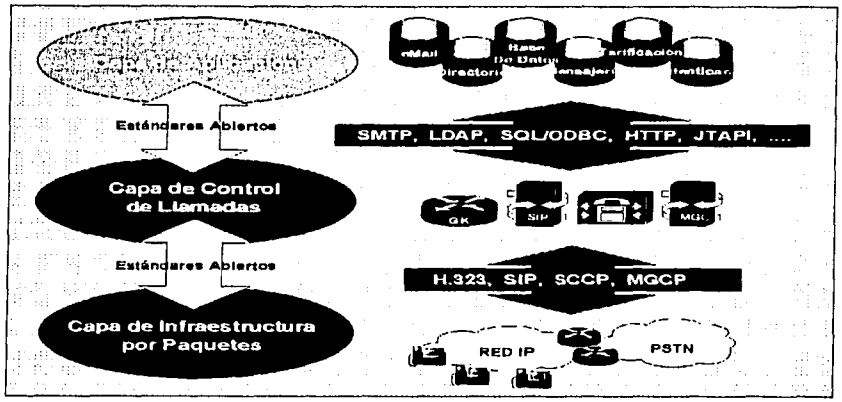


Figura 1-8: Modelo por capas de la Telefonía-IP.

El modelo por capas de la Telefonía-IP al igual que el modelo por capas OSI ofrece las siguientes ventajas:

- ***Reduce la complejidad*** → rompe el proceso de comunicación en partes más pequeñas y por ende más fáciles de manejar.
- ***Estandariza las interfaces*** → estandariza las interfaces de los diferentes componentes del sistema abriendo la puerta a múltiples empresas de desarrollo o soporte.
- ***Asegura la interoperabilidad de la tecnología*** → permite que diferentes tipos hardware y software interoperen entre sí.
- ***Facilita la ingeniería modular y la rápida evolución*** → evita que los cambios sobre una capa afecten a otras capas, acelerando de esta forma el desarrollo.
- ***Hace más fácil su enseñanza y aprendizaje*** → romper el proceso de comunicación en partes más pequeñas hace que el proceso de enseñanza y aprendizaje sean más fáciles.

1.13.1 Capa de Infraestructura por Paquetes

En este nuevo modelo la infraestructura por conmutación de circuitos es reemplazada por la infraestructura por paquetes. La infraestructura por paquetes está basada enteramente en los protocolos IP y UDP, y es independiente de la tecnología de la capa de enlaces de datos usada. La razón de usar IP como infraestructura de paquetes es de que resulta tan atractivo debido a su naturaleza omnipresente (IP over everything) y al hecho de ser la interfaz de facto para casi cualquier aplicación (Everything over IP).

Sin embargo, puesto que en las redes de paquetes IP es común y normal que se produzcan retardos, pérdida de paquetes y jitter (que es la variación en el tiempo de arribo de los paquetes de un flujo de tráfico continuo) como producto de la congestión de las redes, se requiere de un mecanismo adicional que proteja a la Telefonía-IP de estos problemas.

Nota: *TCP/IP fue construido para utilizar la pérdida de paquetes como medio para controlar el flujo de los paquetes; si algún paquete se pierde, éste simplemente será retransmitido).*

Nota: *La ITU-T recomienda un retardo unidireccional de no más de 150 ms en las comunicaciones telefónicas. Si una terminal receptora pidiera que un paquete fuese retransmitido, el retardo sería muy largo, y largos vacíos o rompimientos ocurrirían en la conversación. Por lo tanto, en la mayoría de las aplicaciones en tiempo real, la retransmisión de paquetes es peor que no recibir un paquete debido a la naturaleza sensitiva a los retrasos en el tiempo de arribo de la información.*

El mecanismo adicional que protege a las aplicaciones en tiempo real de los efectos perniciosos del retardo, jitter y pérdida de paquetes comunes a las redes IP, es el protocolo de transporte RTP (Real-time Transport Protocol). RTP corre por encima de los protocolos UDP e IP y es denotado comúnmente como RTP/UDP/IP. RTP es en realidad la piedra angular para el transporte en tiempo real del tráfico a través de las redes IP (Microsoft Netmeeting, por ejemplo, utiliza RTP para transportar comunicaciones de audio y video) al proveer el *timestamping* (estampado del tiempo de emisión). Para precisar, todos los protocolos de señalización de VoIP utilizan RTP/UDP/IP como mecanismo de transporte para el tráfico de voz. Frecuentemente, el flujo de paquetes RTP es conocido como *streams RTP*.

El encabezado de RTP cuenta con un campo en el que se estampa el tiempo exacto en el que el paquete fue enviado (en relación con el stream RTP completo). Esta información es conocida como *RTP Timestamping*, y es usada por el dispositivo terminal que recibe el flujo de audio para determinar si un paquete fue recibido en el orden y tiempo en que se le esperaba, de manera que pueda hacer las previsiones y cambios adecuados a fin de sobreponerse a cualquier problema potencial de congestión en la red y ofrecer una transmisión de calidad.

Aun cuando RTP es suficiente sin más para lograr una transmisión de calidad sobre redes IP bien diseñadas y dimensionadas, en la mayoría de los casos se requiere de mecanismos adicionales que permitan aislar al flujo de tráfico asociado a las aplicaciones en tiempo real de los problemas de congestión de la red. Tales mecanismos son conocidos globalmente como QoS (Calidad de Servicio) y su función es asegurar una entrega de paquetes a tiempo para un cierto flujo de datos independientemente de cualquier otro tráfico o congestión en la red.

Nota : *Como veremos más adelante, el problema de la pobre QoS presente actualmente en la mayoría de las redes de datos IP (y sobre todo de la Internet) está obstaculizando que aplicaciones como la Telefonía-IP se expandan al ritmo que uno desearía.*

1.13.2 Capa de Control de Llamadas

Un elemento clave de la Telefonía-IP es contar con estándares abiertos sobre su capa de control de llamadas. Refiriéndonos a la Figura 1-7 estos estándares abiertos son provistos por protocolos tales como H.323, SGCP, MGCP, SIP, etc. Tal como veremos en el Capítulo 3, son varias las funciones propias de un protocolo de control de llamadas, sin embargo puede decirse por el momento que sus funciones principales son: el manejo de la señalización para el registro de los dispositivos terminales; el establecimiento de los canales y recursos necesarios para una llamada; el manejo de la señalización para el establecimiento, mantenimiento y liberación de una llamada; y el mapeo o traducción entre los números telefónicos y las direcciones IP asociadas. Estas funciones son parecidas a las que la señalización SS7 y otras ofrecen en las redes telefónicas por conmutación de circuitos.

Si bien todos los protocolos de control de llamadas de VoIP resuelven un problema similar (la señalización y control de llamadas), cada protocolo fue desarrollado para resolver cierto tipo de problemas y servir para ciertos propósitos particulares. Por ejemplo, aunque H.323 es el protocolo de control de llamadas de VoIP más ampliamente diseminado, no es visto como un protocolo lo suficientemente robusto y escalable; para estos propósitos, protocolos tales como MGCP y SIP están siendo desarrollados. Aun cuando en un futuro se espera que alguno de estos protocolos quede como líder, por ahora varios protocolos serán usados simultáneamente y no hay necesidad de contar con un único protocolo de control de llamadas.

1.13.2.1 Protocolos de Control de Llamadas de VoIP

Al tiempo en que se escribe esto, los principales protocolos de control de llamadas de VoIP son H.323, SGCP, MGCP, SIP y IPDC. Estos se definen a continuación:

- ***H.323*** → constituye la recomendación de la ITU-U y cuenta con la mayor base instalada debido en parte a que antes de él no existía nada. En el Capítulo 3 se discute este protocolo en mayor detalle.
- ***SIP (Session Initiation Protocol)*** → éste protocolo está siendo actualmente desarrollado y permitirá que los dispositivos finales (*endpoints y gateways*) sean más inteligentes, posibilitando además servicios ampliados en la capa de control de llamadas. Aparte de sus buenas características de escalabilidad, este protocolo cuenta también con el menor *overhead* (carga) de señalización de los protocolos de control de llamadas de VoIP. En el Capítulo 3 se discute este protocolo con más detalle.
- ***SGCP (Simple Gateway Control Protocol)*** → fue desarrollado a principios de 1998 para reducir el costo de los Gateways haciendo que el control de las llamadas tuviera lugar en una plataforma centralizada.
- ***IPDC (Internet Protocol Device Control)*** → es muy parecido a SGCP, empero cuenta con muchos otros mecanismos de operación, administración, administración y aprovisionamiento.

- ***MGCP (Media Gateway Control Protocol)*** → a finales de 1998 la IETF fusiona a IPDC y SGCP en uno y lo llama MGCP. MGCP es básicamente SGCP con pocas adiciones para las funciones de aprovisionamiento.

1.13.3 Capa de Aplicación de Servicios

La capa de mayor interés para cualquier sistema de red es la capa de aplicación. Sin buenas aplicaciones, la infraestructura de red desplegada sería para nada. El contar con interfaces abiertas entre la capa de infraestructura y la capa de control de llamadas y entre la capa de control de llamadas y la capa de aplicación, permite a los desarrolladores de tecnología de VoIP simplemente escribir las API's (Application Programming Interface) estándar y dejar a los Desarrolladores de Software Independientes (DSI) la tarea de crear las aplicaciones de usuario. Cuando un sistema es diseñado conscientemente para ser abierto y flexible, toda una gama de posibilidades se hacen posibles en cuanto al desarrollo de nuevas aplicaciones.

Cuando se pasa hacia un nuevo modelo o infraestructura, no es necesario transportar todas las facilidades y servicios del viejo modelo o infraestructura. Tan solo es suficiente mantener las facilidades y servicios que los usuarios realmente requieren. Por otra parte, aplicaciones legadas tales como los *Call Centers* para redes empresariales, y las facilidades estándar de la PSTN tales como *call-waiting* y *call-forwarding*, deben ser portadas sobre la nueva infraestructura sin que el usuario note el cambio. Después de que estas aplicaciones y facilidades legadas sean portadas, literalmente cientos de nuevas aplicaciones podrán ser específicamente desarrolladas para la nueva infraestructura. Esto incluye (pero no está limitado a) la Mensajería Unificada, la Llamada de Internet en Espera, el presionar sobre una liga en alguna página Web para hablar con un ejecutivo de cuenta, el hablar hacia el establecimiento de pizzas más cercano marcando el mismo número independientemente de mi ubicación, etc.

Ejemplo de Call Centres: Supongamos que estamos navegando en la Web desde el D.F., y vemos algún producto o servicio que nos interesa de alguna empresa que se encuentra en Tijuana. Entonces, aunque queremos comprar ese producto tenemos una pregunta antes de estar dispuestos a adquirirlo, pero tal pregunta no viene contestada en la página Web. Puesto que se trata de una empresa pequeña no cuenta con números 01-800, y uno no desea cerrar su conexión dial-up hacia la Internet. Que pasaría entonces si con solo oprimir una liga en la página Web de la empresa se abriera el NetMeeting de nuestra PC y nos conectáramos mediante VoIP hacia un ejecutivo de cuenta de tal empresa? El representante aclararía nuestra duda y tomaría nuestra orden. Todos estaríamos felices: la empresa salvaría gastos por llamadas 01-800 y nosotros salvaríamos dinero no llamando hasta Tijuana y seguiríamos conectados a la Internet.

1.14 La Promesa de la Telefonía-IP

Las razones básicas por la que un carrier pudiera elegir desarrollar una red telefónica basada en paquetes IP en lugar de una red telefónica tradicional por conmutación de circuitos, depende de si sus costos de operación se reducen y si se hace más competitivo al ser capaz de ofrecer nuevos servicios y aplicaciones a sus usuarios. Como casi todo en la industria, es usualmente mejor y más fácil hacer negocios adicionales a partir de los clientes actuales que salir en busca de nuevos clientes. La Telefonía no es la excepción, los carriers han estado incrementando últimamente las facilidades y servicios que ofrecen a sus usuarios para crear un flujo de ingresos más alto. En cuanto a las empresas y organizaciones se refiere, la Telefonía-IP promete ya hacerlas más productivas y eficientes:

- Salvando costos de implementación, operación, mantenimiento y administración (un solo staff de administración, una sola infraestructura de red, etc).
- Salvando costos en llamadas de larga distancia hacia corporativos remotos.
- Ofreciendo todo un nuevo abanico de servicios y aplicaciones CTI (Mensajería Unificada, Call Centers de segunda generación, etc) más acordes a la nueva forma de operar y de hacer negocios de las empresas.

1.15 Retos a Vencer por la Telefonía-IP

La Telefonía-IP es una tecnología que ha teniendo un desarrollo importante durante los últimos años. Los conocedores auguran que dentro de muy poco llegará a madurar lo suficiente como para competir de igual a igual con la Telefonía Tradicional por conmutación de circuitos en todos los frentes. Mientras tanto, hay varios retos y dificultades que la Telefonía-IP junto con la Internet deben vencer antes de volverse en una solución viable:

- ***Estandarización de los diferentes protocolos involucrados*** → se han observado problemas de interoperabilidad entre varias de las soluciones de Telefonía-IP actuales.
- ***Mayores anchos de banda a nivel core, distribución y acceso sobre la Internet.***
- ***Desarrollo de redes que aseguren una entrega con QoS a nivel carrier y empresa*** → los problemas de congestión e incapacidad de las redes actuales para diferenciar y prioritizar el tráfico en función a sus necesidades particular de entrega (aplicaciones en tiempo real) obstaculizan que la Telefonía-IP logre el nivel de servicio deseado.
- ***Desarrollo de mejores técnicas de codificación de la voz*** → hay necesidad aun de contar con mejores técnicas de codificación a fin de lograr una voz de calidad con bajos anchos de banda de transmisión.
- ***Desarrollo de mejores protocolos de señalización y control de llamadas*** → la mayoría de los protocolos de señalización y control de llamadas producen grandes overheads de señalización. Además aun tiene problemas de escalabilidad.

- ***Desarrollo de mejores esquemas de seguridad*** → deben desarrollarse mejores esquemas de seguridad a fin de que los problemas de seguridad comunes a la Internet no la afecten (virus, jackers, etc).
- ***Establecimiento de requerimientos estrictos de operación y calidad*** → si la Telefonía-IP alguna vez competirá de igual a igual con la Telefonía Tradicional, entonces debe de ofrecer el nivel de calidad y confiabilidad que los reglamentos y disposiciones internacionales exigen a ésta última.

1.15.1 Tecnologías detrás de la Convergencia y Triunfo de VoIP

Hay varias tecnologías que actualmente están siendo desarrolladas o que están siendo implementadas a nivel empresa o carrier, y que serán decisivas para el éxito o viabilidad de la convergencia VVD, y por ende también de la Telefonía-IP.

A nivel carrier o ISP's:
- QoS (Quality of Service), MPLS (Multiprotocol Level Switching) e Ingeniería de Tráfico.
- Nuevos esquema de contabilización y tarificación en base al servicio ofrecido.

A nivel empresas u organizaciones:
- Red switchada de alta velocidad.
- Esquemas de QoS.
- Esquemas de seguridad.

En general, las tecnologías de enlace de datos que están siendo usadas actualmente para incrementar el ancho de banda de la Internet así como el de las redes empresariales a nivel core, distribución y acceso son:

- SONET [Synchronous Optical Network].
- ATM [Asynchronous Transfer Mode].
- DWDM [Dense Wave Division Multiplexing].
- GigabitEthernet.
- DSL [Digital Subscriber Line].

Junto con lo anterior, la Ley de Moore (duplicación de la capacidad de procesamiento cada 18 meses) posibilita que las PC's y los equipos de comunicaciones (router, switches, etc) estén mejor preparados para la convergencia.

La Telefonía-IP es una tecnología que ha teniendo un desarrollo importante en los últimos 5 años y que ya está siendo usada en las empresas en la forma de ***Telefonía-LAN***. Sin embargo, a nivel carrier aún le falta un gran trecho por recorrer (por ejemplo, aún no se cuenta con algo tan inteligente y desarrollado como la señalización SS7 y aún se tienen problemas de escalabilidad).

Pese a lo anterior, el movimiento hacia una red por paquetes IP en la que haya una convergencia de la voz, video y datos es inminente (IP será finalmente la tecnología que integre todo). La pregunta es mas bien, cuánto tiempo hace falta para que las técnicas de QoS y la Telefonía-IP maduren lo suficiente como para que las empresas y los carriers se vean seducidos por ella.

1.16 Nichos de Mercado Actuales

Actualmente la Telefonía-IP está librando batallas sobre diferentes frentes que posibilitarán que en un futuro sea usada a nivel global. Por hoy sin embargo, los nichos de mercado donde más promete la Telefonía-IP, y en general la tecnología de Redes Multimedia (VVD), son:

- ***Transporte masivo de voz vía IP a nivel carrier*** → por ejemplo para el envío de Faxes los estudios han mostrado que aproximadamente el 60 % de las llamadas de larga distancias hacia el Japón son faxes.
- ***Redes Toll Bypass*** → está es la forma más común que las corporaciones buscarán para desplegar redes de VoIP. Este esquema permite a las corporaciones reemplazar sus líneas dedicadas usadas para la conexión entre PBX's remotos y rutear sus llamadas a través de la infraestructura de datos existente.
- ***Telefonía LAN*** → en la pequeña y mediana empresa, caracterizadas por contar con redes switcheadas de alta velocidad con un nivel de QoS asegurado, se está comenzando a usar la llamada Telefonía-LAN que actualmente cuenta con varios proveedores disponibles para la misma.

Del éxito que se tenga sobre cada uno de estos campos dependerá que la Telefonía-IP siga incursionando sobre otros campos. Al igual que la Telefonía de Celulares logró su aceptación de manera casi inmediata gracias a su capacidad para comunicar a sus usuarios independientemente de su ubicación, y pese a los problemas de conexión aun comunes y a sus elevados costos, la industria de la Telefonía-IP debe de mostrar a los clientes que una red de datos bien diseñada y dimensionada puede ofrecer un servicio de calidad y a bajos precios.

Conclusiones

La Telefonía Tradicional por conmutación de circuitos tiene una historia de más de 125 años de desarrollo y evolución. Con todo ese tiempo no es de extrañar que el nivel de confiabilidad logrado por aquélla sea difícil que alguna otra red global (incluyendo la Internet) pueda superarlos por ahora. Sin embargo, hay ciertas motivaciones tanto técnicas como de mercado que han abierto la puerta para el surgimiento de la Telefonía-IP y hacen pensar en la convergencia VVD sobre las redes de datos IP.

Por ahora el nicho de mercado para la Telefonía-IP está limitado a solo unas cuantas áreas (Telefonía LAN, transporte masivo de datos de voz vía IP, etc). Aún hace falta que se resuelvan ciertas cuestiones importantes para que la Telefonía-IP pretenda estar a la par de la Telefonía Tradicional. A la cabeza de esta lista está el problema de la incierta QoS de la Internet y de las redes empresariales.

La Telefonía-IP es una de las tecnologías en tiempo real que como ninguna otra ha puesto en evidencia las deficiencias y limitaciones actuales de la Internet. Los esfuerzos que se hagan por enmendar estas cuestiones serán importantes para que finalmente se logre la convergencia VVD sobre las redes de datos IP, con sus consiguientes beneficios en cuanto a nuevas y mejores aplicaciones y servicios que sacan ventaja de la integración CTI y que conlleven a una reducción en los costos de operación, servicio y mantenimiento. Del éxito de la Telefonía-IP dependerá en parte que la Internet alcance un estado más alto de desarrollo y evolución. Al final, serán los usuarios los ganadores, pues tendrán acceso a una tecnología con mayores posibilidades y una relación costo/beneficio más atractiva.

CAPÍTULO 2

FUNDAMENTOS DE VoIP

"La fortaleza o debilidad de una tecnología reside en su propia naturaleza".

Hay varias cuestiones y detalles que hay que tener en cuenta a la hora de diseñar e implementar redes de VoIP seguras y funcionales. Con este fin, es importante profundizar sobre los fundamentos alrededor de los cuales está construida esta tecnología, así como conocer los problemas a los que se enfrenta y como logra resolverlos.

Al igual que la Telefonía Tradicional por conmutación de circuitos TDM, la tecnología de VoIP debe responder a una serie de preguntas típicas a las redes de voz (Plan de señalización, Plan de numeración y marcación, Plan de sincronía, evitar el eco, etc), pero a su vez debe resolver todo un bagaje entero de nuevos retos y adversidades privativos a su naturaleza (evitar el retardo, el jitter o la pérdida de paquetes, uso de mejores esquemas de codificación y compresión, etc). En este capítulo se detalla algunas de estas cuestiones y se explica en qué forma afectan a las redes de voz basadas en paquetes IP. Algunas cuestiones más específicas, tales como son la calidad de servicio (QoS) y los protocolos de señalización y control usados en las redes de VoIP, serán abordados en capítulos posteriores.

2.1 Retardo / Latencia

El retardo o latencia en una red de voz se define como la cantidad de tiempo que le toma al habla salir de la boca del emisor y llegar al oído del receptor. El retardo es el primer aspecto importante a tener en cuenta en el diseño de toda red de VoIP, porque afecta de manera directa la percepción que los usuarios tienen sobre la calidad de las llamadas y del sistema de VoIP entero. Llamadas con excesivo retardo son difíciles para los participantes porque crean efectos de eco y alarga en general el espacio de tiempo entre las respuestas, haciendo difícil mantener una conversación fluida.

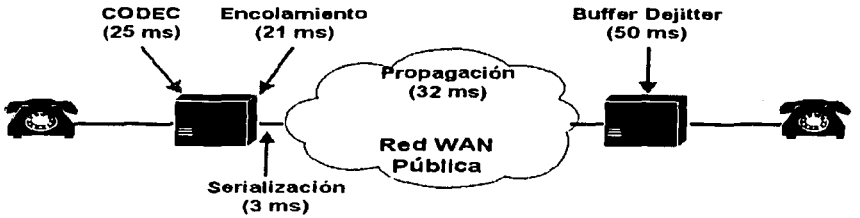
Existen básicamente tres tipos diferentes de retardo inherentes a las redes telefónicas de hoy: retardo de propagación, retardo de manejo y retardo de señalización:

- ***Retardo de Propagación*** → es causado por en retardo en la propagación de la señal (eléctrica o luminosa) sobre el medio de transporte usado (cobre o fibra). Aunque imperceptible para el oído humano, este retardo en conjunción con otros pueden causar una degradación significativa del habla.
- ***Retardo de Manejo*** → también conocido como retardo de procesamiento, es producido por el retardo asociado a procesos en el manejo de los paquetes (tales como el muestreo, la codificación-compresión, el empaquetamiento, el switcheo o el encolamiento) sobre los diferentes dispositivos por los que cruzan en su paso por la red
- ***Retardo de Señalización*** → es la cantidad de tiempo real que toma poner un bit o byte sobre la interface de salida de un equipo. La influencia del retardo de señalización sobre el retardo total es relativamente mínima.

Cuando los paquetes de voz son retenidos en una cola de espera (o buffer) debido a la congestión repentina sobre una interface de salida, el resultado es lo que se llama *Retardo de Encolamiento* (un tipo especial de retardo de manejo propio de las redes de datos). En redes congestionadas, el retardo de encolamiento puede producir hasta dos segundos de retardo (o incluso tirar el paquete). Este periodo largo de retardo es inaceptable para casi cualquier red de voz. De hecho, debe procurarse mantener este retardo a menos de 10 ms siempre que sea posible. Para tal efecto, puede rediseñarse la red para trabajar sobre un ambiente switchado y de alta velocidad (FastEthernet, GigabitEthetnet, etc) sobre la LAN, y usar cualquier combinación de los métodos de encolamiento del Capítulo 4 "QoS (Calidad de Servicio)" para la red LAN y WAN.

> ***Nota:*** *la Recomendación G.114 de la ITU-T especifica que para una obtener una buena calidad de voz, no más de 150 ms de retardo debe producirse en la transmisión de la misma de un extremo a extremo.*

La Figura 2-1 ilustra como puede calcularse el retardo extremo a extremo en una red que está usando a G.729 como CODEC:



PARÁMETRO DE RETARDO	RETARDO FIJO	RETARDO VARIABLE
Retardo del CODEC G.729 (5 ms inicial)	5 ms	--
Retardo del CODEC G.729 (10 ms por frame)	20 ms	--
Retardo de encapsulación	Ínfimo	
Retardo de encolamiento máximo	--	21 ms
Retardo de serialización	3 ms	--
Retardo de propagación	32 ms	--
Reatrdo de la red (red WAN pública)	--	variable
Buffer dejitter	50 ms	--
TOTAL	110 ms	> 21 ms

Figura 2-1: Retardo extremo a extremo en una red con G.729

Nota: el retardo del CODEC incluye 5 ms para la activación del VAD (Voice Activity Detection) así como el tiempo de procesamiento requerido para la cancelación del eco.

Tal como se muestra en la Figura 2-2, algunas formas de retardo, aunque más grandes que otras, son aceptadas porque ninguna otra alternativa existe. En las transmisiones satelitales por ejemplo, le toma a la señal aproximadamente 250 ms para alcanzar el satélite, y otros 250 ms para regresar devuelta hacia la tierra. Esto resulta en un retardo total de 500 ms. Aunque la recomendación de la ITU-U la califica como fuera del rango aceptable de calidad de voz, muchas conversaciones tienen lugar cada día sobre enlaces satelitales. De modo que la calidad de la voz está definida en base a lo que los usuarios aceptan y usan, y no solo en función del retardo permitido.

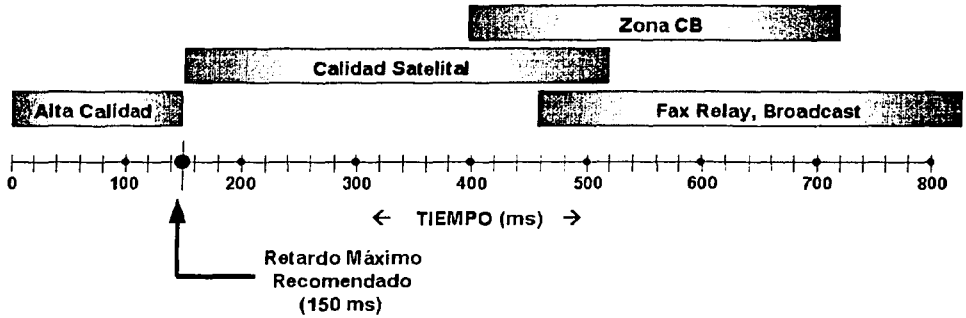


Figura 2-2: Retardo extremo-a-extremo.

2.2 Jitter

El Jitter es la variación en el tiempo de arribo de los paquetes y es un problema asociado sólo a las redes voz basadas en paquetes (o comunicación por ráfagas). Después de que un emisor envía paquetes sobre una red de datos a una rapidez constante (digamos un paquete cada 10 ms) , estos paquetes pueden retardarse en su paso por la red (debido a la congestión repentina de la misma) y arribar a intervalos irregulares en el receptor. El Jitter es pues la diferencia en tiempo entre cuándo era esperado un paquete y cuándo fue realmente recibido.

En la Figura 2-3, se puede ver que la cantidad de tiempo que le toma a un transmisor enviar los paquetes A, B, C y D, es el mismo ($T_A = T_B = T_C = T_D$). Sin embargo los paquetes C y D en su paso por la red encuentran cierta congestión y son recibidos después de lo esperado ($D_C \neq D_A$, $D_D \neq D_A$). Una forma de compensar este problema es usando *Buffers de Dejitter* sobre los extremos, que cancelen esta variación en el tiempo de arribo de los paquetes.

El Jitter y el retardo total no son la misma cosa. Sin embargo, tener demasiado Jitter en la red se traduce invariablemente en un incremento en la cantidad de retardo total, porque a mayor Jitter, más tiempo les llevará a los Buffers Dejitter compensar la naturaleza impredecible en la red.

Los Buffers Dejitter (anuladores del Jitter) hacen uso del mecanismo de *timestamping* (estampado del tiempo de emisión sobre los paquetes) del protocolo RTP, y puede ser de dos tipos:

- ***Estáticos*** → son más económicos pero la calidad del audio podría sufrir en redes muy impredecibles, debido a la pérdida de paquetes o al excesivo retardo introducidos al elegir tiempos para el Buffer de Dejitter muy cortos o largos, respectivamente.
- ***Dinámicos*** → aunque más caros, son el mejor mecanismo para cancelar el Jitter pues adaptan de manera dinámica el tiempo de latencia de un paquete sobre el Buffer en base a la variación en el retardo de los últimos paquetes.

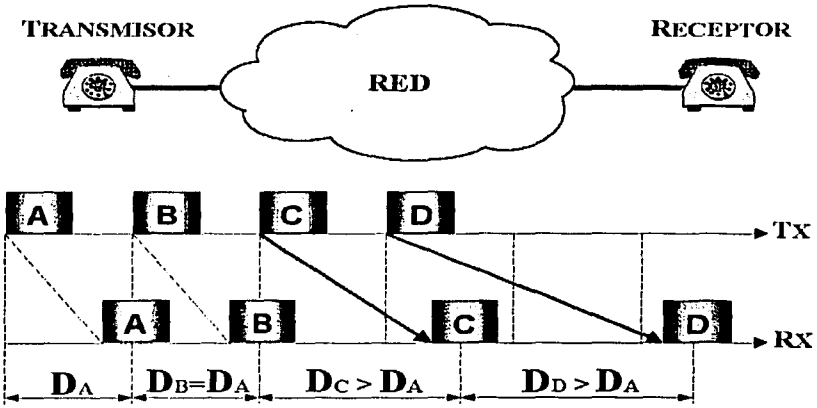


Figura 2-3: Variación en el tiempo de arribo de los paquetes (Jitter).

2.3 Pérdida de Paquetes

La pérdida de paquetes es algo común y aún esperado sobre las redes de datos. De hecho, muchos protocolos de datos usan la pérdida de paquetes para conocer las condiciones de la red y reducir de esta manera el número de paquetes que enviarán. Un ejemplo de esto último es el *mecanismo de ventaneo de TCP*).

Cuando hay tráfico crítico sobre la red es importante controlar la cantidad de pérdida de paquetes. Aplicaciones que no toleran la pérdida de paquetes exigen contar con un buen diseño de red, así como con mecanismos por los cuales se prioritice a los datos sensitivos al retardo o a la pérdida sobre aquellos que lo pueden tolerar.

Hay varios métodos de QoS desarrollados que permiten a los administradores clasificar y prioritizar los datos en función de su importancia. Si una red de datos está bien diseñada la pérdida de paquetes puede mantenerse al mínimo.

Algunas implementaciones de VoIP permiten a los equipos terminales sobreponerse a la pérdida periódica de paquetes: si un paquete de voz no es recibido cuando era esperado, se asume su pérdida y el último paquete recibido será repetido, como se muestra en la Figura 2-4.

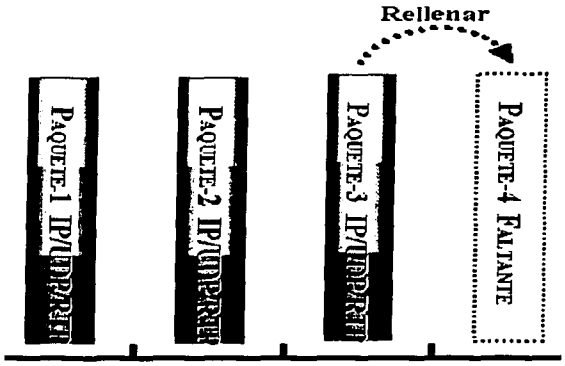


Figura 2-4: Estrategia de Encubrimiento para la pérdida de paquetes con G.729

En la Figura 2-4 cada línea representa un paquete. Los paquetes 1, 2 y 3 alcanzan satisfactoriamente el destino, pero el paquete 4 se pierde en algún punto de la transmisión. El equipo receptor espera por un periodo de tiempo y entonces corre una *Estrategia de Encubrimiento.* Esta estrategia de encubrimiento repite el último paquete recibido (en este caso, el paquete 3), de manera que el receptor no escuche silencios. Puesto que los paquetes son de tan solo 20 ms con G.729, el receptor en la mayoría de los casos no apreciara la diferencia. La estrategia de encubrimiento puede usarse solamente para pérdida de un sólo paquete. Si múltiples paquetes consecutivos se pierden, la estrategia no funcionará.

2.4 PCM (Pulse Code Modulation)

Aunque las comunicaciones analógicas son ideales para la comunicación humana, la transmisión analógica no es robusta ni lo suficientemente eficiente para recobrarse del ruido sobre las líneas de transmisión. En los inicios de las redes telefónicas, cuando una señal analógica era pasaba a través de amplificadores para recuperarla de la atenuación sufrida en su paso por la red, no solo se amplificaba la señal sino también el ruido de la línea. Este ruido en la línea derivaba frecuentemente en conexiones defectuosas.

Era mucho más eficiente digitalizar la voz en muestras digitales codificadas (compuestas de solo 1's y 0's) a fin de cancelar el ruido del medio y regenerar la señal. Cuando los beneficios de la representación digital se hizo evidente, la mayoría de las redes telefónicas migraron hacia un esquema digital PCM/TDM.

PCM es el método basado en el Teorema de Nyquist que permite llevar una señal analógica a su forma digital. Se basa en el filtrado y el muestreo de la señal analógica a la razón de 8000 veces por segundo, así como en la codificación de estas muestras usando un código numérico (ver Capítulo 1).

2.5 Compresión de la Voz

Si bien PCM logra una transmisión de calidad de la voz al aislarla del efecto del ruido sobre la línea, tiene el inconveniente de usar mayor ancho de banda que su representación analógica. Con el propósito de hacer un uso más eficiente del caro y escaso ancho de banda de los enlaces digitales WAN, varios esquemas de compresión han sido desarrollados a lo largo del tiempo. Algunos explotan la naturaleza redundante de la señal, mientras que otros están basados en el conocimiento de las características de la fuente emisora.

Son dos las variantes de PCM comúnmente usadas para comprimir: la Ley-μ y la Ley-A. Estos métodos son similares en cuanto que usan un esquema de compresión logarítmico para alcanzar de 12 a 13 bits de calidad PCM linear sobre palabras de 8 bits, y diferentes solo en detalles menores (la ley-μ tiene una ligera ventaja con un a menor razón de señal a ruido). El uso de alguno de ellos es histórico y privativo de cada región: en Norteamérica por ejemplo se usa la ley-μ, mientras que en Europa se usa la Ley-A.

Otro método de compresión frecuentemente usado es ADPCM (Adaptive Differential Pulse Code Modulation). PCM y ADPCM son ejemplos de técnicas de compresión bien conocidas que explotan las características redundantes de la señal misma. Sin embargo, durante los pasados 10 a 15 años han sido desarrolladas nuevas técnicas de compresión que explotan el conocimiento de las características de la fuente generadora del habla. Estas técnicas emplean procedimientos para el procesamiento de la señal que comprimen el habla mandando solamente información simplificada de los parámetros sobre la fuente emisora del habla y de la forma de la región vocal, requiriendo menor ancho de banda para transmitir la información.

Estas técnicas pueden denominarse como *Codificadores Fuente* e incluyen variaciones tales como LPC (Linear Predictive Coding) CELP (Code Excited Prediction Compresión) y MP-MLQ (Multipulse, Multilevel Quantization).

2.5.1 Estándares de Codificación de la Voz

Los esquemas de codificación CELP, MP-MLQ, PCM y ADPCM están estandarizados bajo las recomendaciones de la serie-G de la ITU-T. Los estándares de codificación de voz más populares para la Telefonía-IP incluyen a los siguientes:

- ***G.711*** → describe la técnica de codificación de voz PCM a 64 Kbps antes descrita, la voz codificada con G.711 está ya en el formato correcto para la entrega de voz digital en la red telefónica pública o entre PBX's.
- ***G.726*** → describe la codificación ADPCM a 40, 32, 24 y 16 Kbps; la voz ADPCM puede ser intercambiada directamente entre redes telefónicas públicas y basadas en paquetes.
- ***G.728*** → describe la variante a 16 Kbps y con bajo retardo de la compresión de voz CELP; la voz codificada con CELP debe ser transcodificada entre redes telefónicas públicas y basadas en paquetes que interactúan.
- ***G.729*** → describe a la compresión CELP que permite que la voz sea codificada en flujos de 8 Kbps; la calidad de voz que ofrece es parecida a ADPCM a 32 Kbps.
- ***G.723.1*** → describe la técnica de compresión que puede ser usada para comprimir voz u otras señales de audio con una tasa de bits muy baja; este codificador tiene dos velocidades asociadas: 5.3 Kbps (basado en CELP, flexible y con muy buena calidad) y 6.3 Kbps (basado MP-MLQ y con alta calidad).

2.5.2 MOS (Mean Opinion Score)

La calidad de la voz ofrecida por un sistema de codificación puede ser evaluada de dos maneras: subjetiva y objetivamente. Las personas realizan la evaluación subjetiva, mientras que las computadoras e instrumentos, que son más difíciles de engañar que el oído humano a ciertos trucos, realizan la evaluación objetiva de la calidad de la voz.

Los CODEC's de hoy descansan cada vez más sobre técnicas de evaluación subjetivas, pues las medidas objetivas de la calidad, tales como la distorsión armónica total o la relación señal a ruido S/N, no siempre se correlacionan con la percepción humana de lo que es la calidad, que en último término es una de las metas más importantes para la mayoría de las técnicas de compresión.

Una forma común de cuantificar de manera subjetiva la calidad de un CODEC de voz es el MOS (Mean Opinion Score). Puesto que la calidad de la voz es generalmente subjetiva al que escucha, es importante obtener un amplio rango de escuchas que la aprueben. Las pruebas MOS son aplicadas a un grupo de escuchas quienes dan una evaluación del material en un rango del 1 (malo) al 5 (excelente). Estos puntajes son promediados para obtener un Puntaje de Opinión Promedio o puntaje MOS. La pruebas MOS son también usadas para comparar que tan bien trabaja un CODEC bajo circunstancias diversas, incluyendo diferentes niveles de ruido de fondo, múltiples codificaciones y decodificaciones, etc. Esta información puede ser entonces usada para comparar a su vez otros CODEC's.

Los puntajes MOS para varios CODEC's ITU-T son ilustrados en la siguiente Tabla 2-1:

MÉTODO DE COMPRESIÓN	Bit Rate (kbps)	Procesamiento (mips)	Tamaño del Frame	Retardo (ms)	Puntaje MOS
G.711 PCM	64	.34	0.125	0.75	4.1
G.726 ADPCM	32	14	0.125	1	3.85
G.728 LD-CELP	16	33	0.625	3-5	3.61
G.729 CS-ACELP	8	20	10	10	3.92
G.729 por 2 codificaciones	8	20	10	20	3.27
G.729 por 3 codificaciones	8	20	10	20	2.68
G.729a CS-ACELP	8	10.5	10	10	3.7
G.723.1 MPMLQ	6.3	16	30	30	3.9
G.723.1 ACELP	5.3	16	30	30	3.65

Tabla 2-1: Métodos de compresión y sus respectivos puntajes MOS.

La Figura 2-5 provee un visión global sobre la calidad de voz para varias tecnologías de codificación de voz.

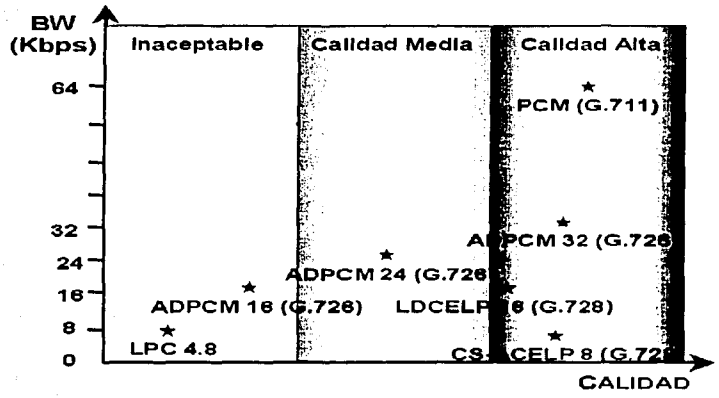


Figura 2-5: Tecnologías de codificación de voz.

Con el costo que implica mantener y crear la infraestructura necesaria para sostener las redes de alta calidad de hoy, podría parecer fácil y barato convertir todas las llamadas hacia una voz codificada con baja tasa de bits y salvar costos por concepto de ancho de banda. Hay sin embargo, algunas desventajas de comprimir la voz. Tal como se muestra en la Tabla 2-1, una de las principales desventajas es la distorsión de la señal debido a múltiples codificaciones y decodificaciones (también conocido como *codificación tandem*). Cuando una señal de voz G.729 es comprimida muchas veces, la señal puede degradarse desde un MOS de 3.92 (muy bueno) a 2.68 (normalmente inaceptable) después de tres codificaciones en tandem.

Para comprender como un alto MOS es alcanzado con un CODEC con baja tasa de bits tal como G.726, es importante comprender cómo trabajan estos codificadores. Estudios sobre los patrones del habla han mostrado que un porcentaje significativo de las llamadas de voz son silencios, con ráfagas de habla restantes repetitivas y correlacionales. Comprender este estudio hace posible tomar ventaja de los patrones del habla al usar modelos matemáticos para predecir el próximo sonido que se producirá, basándose tan solo en las muestras previas. Usando el mismo modelo de predicción tanto en el lado del codificador como del decodificador, la única información que necesita ser transmitida es la diferencia entre lo que se espera y lo que realmente ocurre en el habla. G.726 (ADPCM) usando 32 Kbps es frecuentemente catalogado como PCM a 64 Kbps (la máxima calidad). Con este tipo de codificador, cualquier señal que caiga dentro de los 4 KHz del ancho de banda de la voz puede ser digitalizado y transportado. Desafortunadamente, usando una menor tasa de bits para ADPCM (24 o 16 Kbps) causa caídas importantes en el puntaje MOS.

Para alcanzar CODEC's con aún menor tasa de bits, tal como G.729 y G.723.1 (conocidos como CODEC's con muy baja tasa de bits), y mantener una calidad de voz PCM aceptable, la codificación debe ser abandonada. Con el avance en la potencia de procesamiento [DSP – Digital Signal Processor] y costos [MIPS – Millions of Instructions per Second], así como con los avances en la tecnología de voz, se ha vuelto realidad usar la compresión de la voz a gran escala. Uno de los más interesantes hechos de LPC y otros CODEC's híbridos es que el habla real no es transmitida a través de la red. Los LPC's sintetizan el tracto vocal (cuerdas vocales, pulmones) y un filtro sintetiza otros componentes (boca, lengua, labios, etc). Los sonidos o excitaciones son enviados al filtro, y sale la voz sintetizada. Este nuevo esquema de codificación representa una mejora muy importante sobre PCM. Por ejemplo, los LPC's muestrean una vez cada 20 ms, a diferencia de PCM que muestrea 160 veces en los mismos 20 ms. Así en el mismo periodo de tiempo un LPC deberá transmitir 40 bits por segundo mientras que PCM debería enviar 1280 por segundo.

Los codificadores híbridos tales como CELP están construidos alrededor de la tecnología LPC y las mejoras adicionales sobre las técnicas de análisis y síntesis que remueven mucha de la naturaleza robótica de la primera generación de CODEC's de voz LPC. Los CODEC's híbridos requieren sintetizadores más complejos. Estos sintetizadores tiene 8 o 10 parámetros, los cuales son típicamente actualizados cada 20 ms. En la optimización de la calidad de la voz, CELP ha demostrado una transmisión significativamente baja para señales no de voz tales, como la música en espera. En la siguiente Figura 2-6 se muestra cómo estos nuevos codificadores híbridos trabajan.

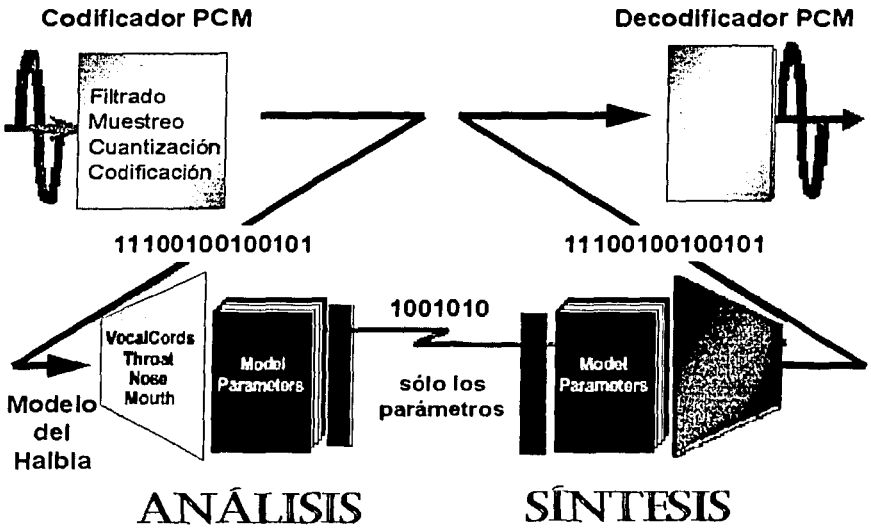


Figura 2-6: Codificadores Híbridos.

Estos nuevos codificadores traen consigo nuevos acuerdos de compromiso en el diseño. La codificación tandem ya ha sido discutida, pero es también importante abordar otras cuestiones que rondan alrededor de los codificadores con baja tasa de bits, tales como el retardo del codificador, el acuerdo de compromiso entre el ancho de banda y la calidad, el eco y el retardo total extremo a extremo.

2.6 Eco

En una red telefónica tradicional, el eco (o reflexión de la señal hacia el punto que la originó) es normalmente producido por discrepancias en la impedancia de los sistemas por los que pasa una señal. El caso más claro es aquel cuando una señal pasa de un sistema de dos a un sistema de cuatro hilos (ver Figura 2-7). Escuchar la propia voz mientras se está hablando es común y necesario para el que habla. Sin embargo, escuchar la propia voz después de ~25 ms puede causar interrupciones y romper la cadencia de la comunicación.

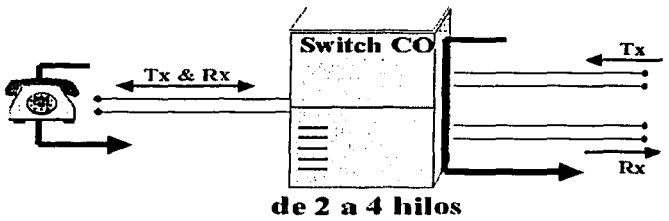


Figura 2-7: Eco causado por discrepancias en la impendancia.

El eco en la PSTN es controlado mediante canceladores de eco y un control estricto de las discrepancias en la impedancia sobre puntos de reflexión comunes. En las redes de voz basadas en paquetes, los canceladores de eco se construyen sobre los CODEC's que operan sobre cada DSP (Digital Signal Processor).

Para comprender cómo trabajan los canceladores de eco, antes se debe comprender de dónde proviene el eco. Por ejemplo, si el usuario A está hablando con el usuario B. El habla del usuario A hacia el usuario B es llamada G. Cuando G llega a un punto de discrepancia en las impedancias, es rebotada de regreso hacia el usuario A. El usuario A puede entonces escuchar el retardo varios milisegundos después de que el usuario A estaba realmente hablando.

Para remover el eco de la línea, el dispositivo del usuario A mantiene una imagen inversa del habla de A, llamada habla inversa (–G), por un cierto periodo de tiempo. Este cancelador de eco escucha el sonido proveniente del usuario B y substrae el habla inversa –G a fin de remover cualquier eco.

El diseño de los canceladores de eco está en función de la cantidad de tiempo total en la que la señal reflejada se espera ser recibida, fenómeno conocido como *Eco-Trail*. El eco-trail es normalmente de 32 ms.

2.7 VAD

En las redes tradicionales de voz una llamada consume un ancho de banda de 64 Kbps, sin importar si se habla o no. Por otra parte, en una conversación de voz normal una persona habla mientras que la otra escucha, lo cual significa que por lo menos el 50 por ciento del ancho de banda total es desperdiciado.

Cuando VAD (Detección Activa de la Voz) se habilita para trabajar sobre una red de VoIP, el ancho de banda antes malgastado puede ser ahora utilizado para otros propósitos.

Como se ilustra en la Figura 2-8, VAD trabaja detectando una caída en la amplitud del habla (en decibeles, dB), y deteniendo la transmisión de paquetes de voz durante esos momentos. VAD tiene ciertos problemas inherentes para determinar cuándo el habla termina o cuándo vuelve a comenzar, así como para distinguir entre el habla y el ruido de fondo. Típicamente, cuando VAD detecta una caída en la amplitud del habla, espera una cantidad fija de tiempo (típicamente de 200 ms) antes de detener la transmisión de paquetes.

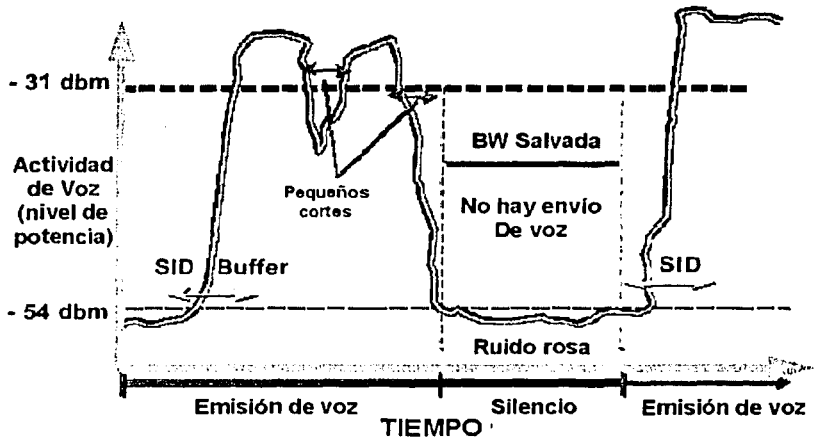


Figura 2-8: VAD (Voice Activity Detection).

2.8 Protocolo de Transporte

En el mundo TCP/IP, el servicio de transporte para el tráfico de paquetes IP puede ser ofrecido tanto por TCP (Transport Control Protocol) como por UDP (User Datagram Protocol). El uso de uno u otro depende de las necesidades de la aplicación. En general, TCP es usado cuando se desea una conexión confiable y UDP cuando se requiere poco *overhead* y la confiabilidad no es la preocupación principal.

Debido a la naturaleza sensitiva al tiempo del tráfico de voz, la elección lógica para el transporte de la voz es la combinación IP/UDP, si bien más información es necesaria a la

ofrecida por UDP para asegurar un tráfico en tiempo real sobre las redes de paquetes. Así pues, la IETF adoptó a RTP para tal prepósito, quedando entonces la cabecera para todo paquete de VoIP en la forma IP/UDP/RTP.

2.8.1 RTP (RFC-1889)

RTP (Real-time Transport Protocol) es el estándar para la transmisión de tráfico sensitivo al retardo sobre redes basadas en paquetes IP. El protocolo RTP corre sobre UDP e IP. Tal como se ve en la Figura 2-9, dos importantes bits de información en su encabezado son la información de secuenciación y las etiquetas de tiempo (o timestamping). RTP usa la información de secuenciación para determinar si los paquetes arriban en orden, y usa la información de timestamping para sincronizar el intervalo de arribo de los paquete de voz (y evitar efectos como el jitter).

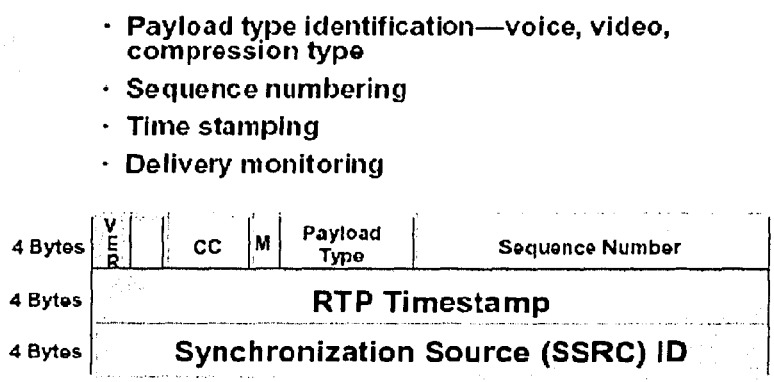


Figura 2-9: Encabezado de RTP (Real-time Transport Protocol).

RTP consiste de una parte de datos y de una parte de control llamada RTCP (o Protocolo de Control de RTP). La parte de datos de RTP es un protocolo ligero que permite soportar aplicaciones en tiempo real. Por otra parte, RTCP (RFC-1890) permite soportar conferencias tiempo real dentro de la Internet. Esto incluye la identificación de la fuente y el soporte sobre gateways. Ofrece también una retroalimentación de la QoS desde los receptores hacia el grupo multicast, así como la sincronización de diferentes flujos de medios (voz, video y datos).

RTP es importante para el tráfico en tiempo real, sin embargo tiene una desventaja. Las cabeceras IP/UDP/RTP tienen un tamaño de 20, 8 y 12 bytes, respectivamente. Esto genera una cabecera de paquete de 40 bytes, lo cual es dos veces más grande que el contenido real de de la información enviada usando G.729 con dos muestras de habla (cada 20 ms). Se puede usar CRTP (Compressed Real-time Protocol) para comprimir este header compuesto a tan sólo 2 o 4 bytes y eficientar el uso del ancho de banda (ver Figura 2-10).

CRTP (Compressed Real-time Protocol)
- Información real
  - (20 ms)x(8 kbps) = 20 bytes por payload
- Información de control
  - IP header = 20;
  - UDP header = 8;
  - RTP header = 12
  - 2x payload = 40 bytes
- Aplicando compresión de Header:
  - De 40 bytes a solo 2 o 4 bytes

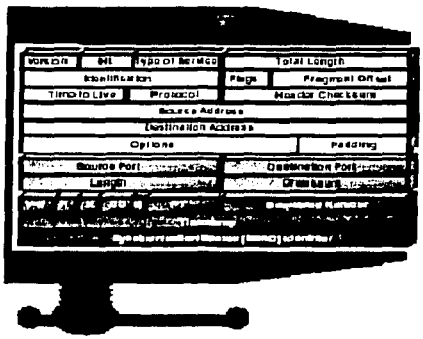


Figura 2-10: Compresión mediante CRTP (Compressed Real-time Protocol).

2.9 Flujo de una llamada en VoIP

El flujo de una llamada se refiere a los pasos generales que tienen lugar para el establecimiento de una llamada sobre una red de VoIP. El ejemplo que se presenta a continuación no pretende dar una descripción detallada sobre el flujo de una llamada, mas bien intenta dar una vista panorámica sobre los eventos que tienen lugar cuando se hace una llamada sobre una red que trabaja con VoIP. Una descripción detallada sobre el flujo de una llamada en VoIP es vista en el Capítulo 3, donde se abordan los diferentes protocolos de señalización y control de llamadas.

Dicho lo anterior, el flujo general de una llamada de voz uno-a-uno sigue los siguientes pasos:

1. El usuario levanta el mango del teléfono, señalizando una condición de descolgado.
2. la sesión de aplicación manda un tono de marcado y espera a que el usuario marque el número telefónico al que quiere llamar.
3. El usuario marca el número, el cual es acumulado por la sesión de aplicación.

4. El número es mapeado a su dirección IP vía un servidor de traslación de direcciones. La dirección IP devuelta puede ser la del host con el que se quiere hablar o la de un gateway intermedio que ayudará a completar la llamada.
5. La sesión de aplicación corre un protocolo de sesión (H.323) para establecer un canal de transmisión y recepción.
6. Si se está usando RSVP (Resource Reservation Protocol), la reservación RSVP tiene lugar para alcanzar la nivel de QoS deseado sobre la red IP.
7. Se activan los CODEC's en ambos extremos de la llamada y se establece la conversación usando IP/UDP/RTP.
8. Cualquier indicación sobre el progreso de la llamada (timbrado, ocupado, etc) que es transportada en banda es retirada tan pronto se establece el canal de audio. La señalización que sea detectada durante la llamada (digamos tonos DTMF para acceder al correo de voz) es encapsulada con RTCP y recibida por la sesión de aplicación para su procesamiento.
9. Cuando cualquiera de los participantes cuelga, se libera la reservación de RSVP y la sesión termina.

Una sesión puede utilizar cualquier protocolo de señalización y control de llamada. La Figura 2-11 muestra una sesión que ha sido establecida usando H.323 como protocolo de señalización.

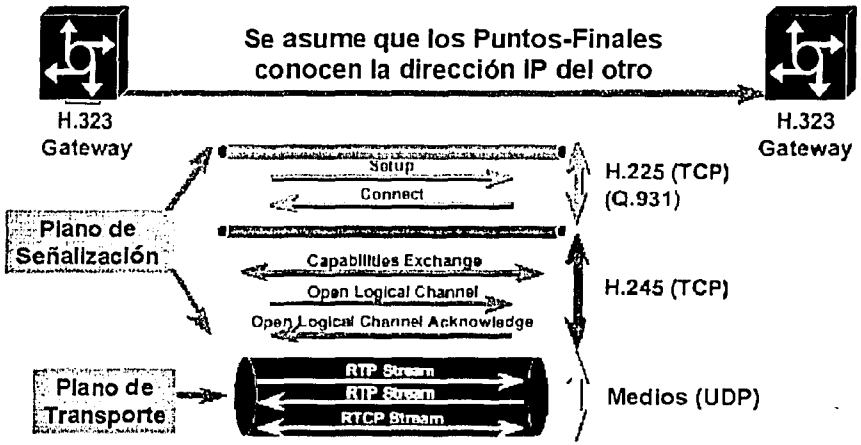


Figura 2-11: Flujo de una llamada mediante H.323

2.10 Alimentación de los IP-Phones

Un aspecto importante, aunque algunas veces olvidado es como proporcionar la alimentación a los IP-Phones (Teléfonos-IP). Existen básicamente tres formas diferentes de proporcionar la alimentación o potencia a los IP-Phones:

- *Alimentación a través de la misma línea de conexión a la red (Inline Power).*
- *Alimentación a través de un panel externo.*
- *Alimentación a través de un eliminador de pared.*

2.10.1 Inline Power

La ventaja de la alimentación a través de la línea es de que no se requiere un contacto de potencia local, permitiendo la centralización de la alimentación para los IP-Phones sobre los mismos switches que les dan la conexión a la red de datos IP.

Con el método de la alimentación en línea, los pares 2 y 3 (pins 1,2,3 y 6) de los cuatro pares del cable UTP Categoría 5 son usados para transmitir la potencia (6.3 W) desde el switch. Este método de proporcionar la alimentación es algunas veces conocido alimentación fantasma, porque la potencia viaja sobre los mismos dos pares usados para transmitir las señales de Ethernet sin interferir con su operación. Sin embargo, todavía no hay un estándar plenamente establecido.

2.10.2 External Patch Panel Power

Si el switch FastEthernet que proporciona la conexión a la red no posee las capacidades Inline Power, entonces se puede usar un patch panel de alimentación (ver Figura 2-12). El patch panel de alimentación puede ser insertado en el closet de cableado entre el switch y los IP-Phones.

Como se muestra en la Figura 2-12, el patch panel tiene dos puertos por conexión: un puerto sobre el lado del switch y un puerto sobre el lado del IP-Phone.

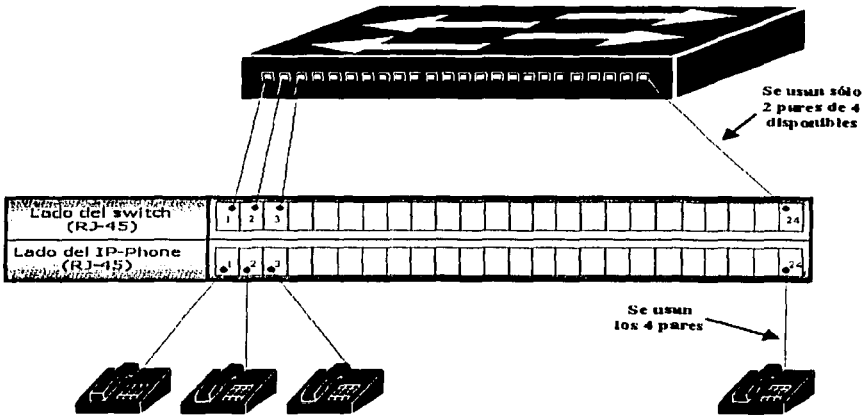


Figura 2-12: Alimentación de un IP-Phone a través de un Pach Panel.

A diferencia del método Inline Power, los pares Ethernet no transportan la potencia. En su lugar los pares restantes (1 y 4) son usados para entregar la potencia desde el patch panel (ver Figura 2-13).

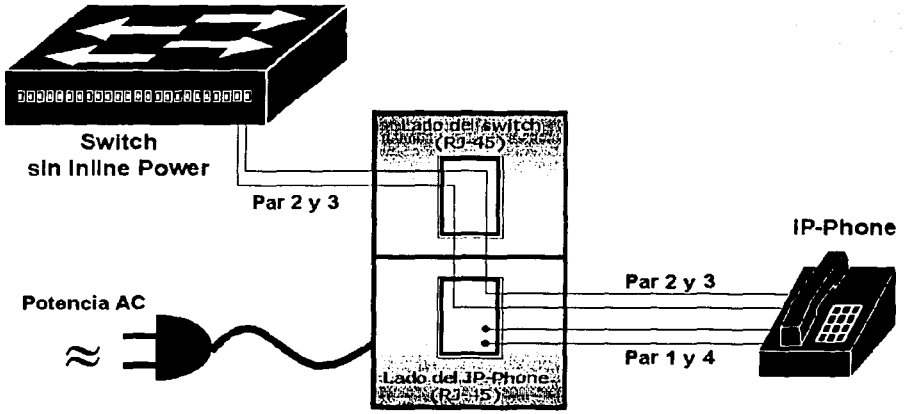


Figura 2-13: Conexión del switch y el IP-Phone sobre el Pach Panel.

2.10.3 Eliminador de Pared

La última opción para alimentar un IP-Phone es usando un eliminador local como se muestra en la Figura 2-14.

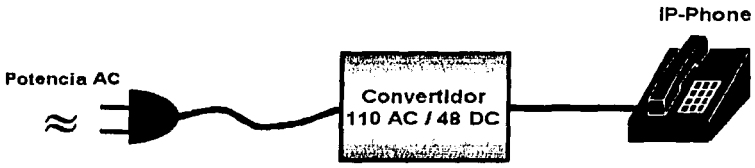


Figura 2-14: Alimentación a través de un eliminador de pared.

2.11 Conexión de los IP-Phones a la Red

Tal como se ilustra en la Figura 2-15, existen varias formas en las cuales un IP-Phone y la PC de usuario asociada pueden conectarse a la red de datos:

- ***Usando un único cable*** → este arreglo constituye la forma más común pues solo se requiere de un puerto de switch para proveer de conectividad a ambos dispositivos (el IP-Phone debe contar con el puerto para la conexión de la PC). Entre su ventajas están la facilidad de instalación, el ahorro en nueva infraestructura de cableado y puertos de switch. Su desventaja es de que si el IP-Phone queda fuera de servicio por alguna razón, la PC pierde conectividad.
- ***Usando múltiples cables*** → aunque esta opción dobla la cantidad de puertos de switch por cada usuario, provee un nivel de redundancia. Si el IP-Phone queda fuera de servicio, la PC no se ve afectada y viceversa.
- ***Usando una aplicación de SoftPhone corriendo sobre la PC*** → la conexión es la de la PC pues en este caso el IP-Phone es una aplicación JTAPI corriendo sobre la PC (comúnmente conocido como SotfPhone).

Cada uno de estos métodos de conexión tiene algunas cuestiones que resolver a fin de proveer una calidad de voz garantizada. Estas cuestiones pueden resumirse a los siguientes:

- Qué parámetros de velocidad o modo duplex deben ser usados para conectar un IP-Phone en cada caso.
- Qué esquema de direccionamiento IP o VLAN debe ser usado.
- Cómo clasificar y manejar el encolamiento para los flujos de VoIP provenientes de los IP-Phones.

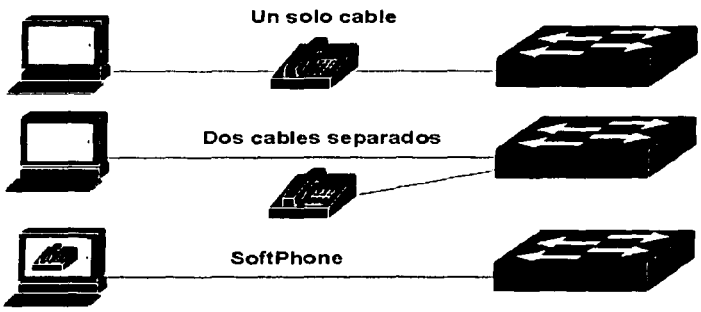


Figura 2-15: Conexión del IP-Phone y la PC asociada a la red.

2.12 Direccionamiento IP

Cada IP-Phone dentro de la red requiere de una dirección IP (junto con información relacionada como máscara de subred, default gateway, etc) para poder operar. Esto esencialmente significa que una organización requiere asignar una dirección IP adicional por cada usuario con IP-Phone. La información de direccionamiento IP puede ser configurada de manera estática sobre el IP-Phone, o puede ser provista de manera dinámica por un servidor DHCP (Dynamic Host Configuration Protocol).

En general, se cuenta con varias formas con las que se puede cumplir con este requerimiento de direccionamiento IP para los IP-Phones:

- Asignar direcciones IP usando la misma subred utilizada para las PC's.
- Modificar el plan de direccionamiento.
- Utilizar una subred (pública o privada) para el uso exclusivo de los IP-Phones. En caso de usarse direcciones no homologadas puede usarse NAT en los equipos de frontera (routers) para la comunicación con otras redes telefónicas IP compatibles a lo largo de la Internet.

En la Figura 2-16 muestra algunos ejemplos utilizados para direccionar los IP-Phones, PC's y SoftPhones.

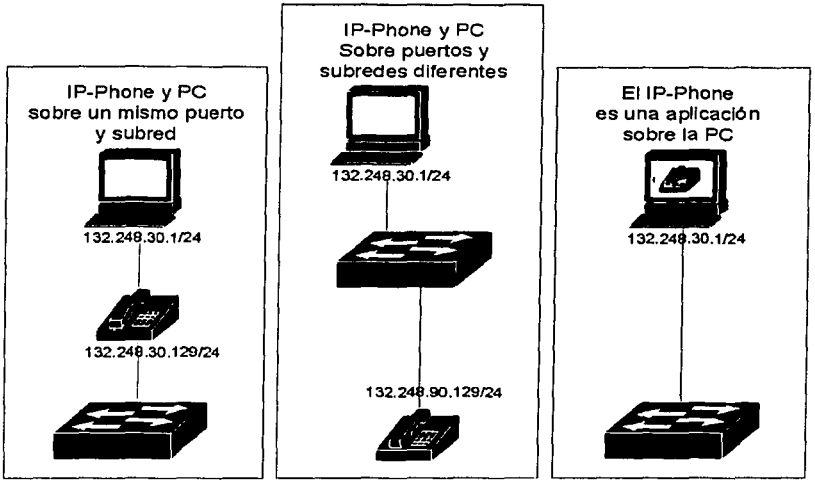


Figura 2-16: Direccionamiento IP usado para varias situaciones.

2.13 Plan de Marcación

Una de las áreas que con frecuencia causa la mayor cantidad de dolores de cabeza cuando se diseña una red telefónica es el plan de marcación. La causa de esto podría deberse por ejemplo a las dificultades que conlleva integrar redes dispares, pues muchas de estas redes no fueron diseñadas para una integración ulterior.

Un buen ejemplo de juntar redes dispares se da cuando dos compañías se fusionan. En tal escenario, las redes de datos (así como el direccionamiento IP, las aplicaciones y las bases de datos) de las compañías deben unirse. Es poco probable que ambas compañías usaran la misma metodología cuando implementaron sus redes de datos, así que algunos problemas podrían surgir. Los mismos problemas podrían presentarse para el caso de las redes telefónicas. Es muy probable que sus sistemas telefónicos (correo de voz, tarificación, facilidades de usuario y plan de marcación) pudieran no ser compatibles el uno con el otro.

Problemas con el plan de marcación podrían ocurrir también cuando una compañía decide instituir un plan de marcación global en todos sus corporativos. Considérese por ejemplo el caso de la compañía X en México. La compañía X ha crecido drásticamente durante los últimos tres años y ahora cuenta con 30 sitios a lo largo de todo el país, con su matriz en el D.F. La compañía X actualmente marca hacia la PSTN desde sus 29 sitios remotos. La

compañía quiere simplificar el plan de marcación en todos sus sitios remotos para lograr una mejor comunicación y facilidad de uso.

La compañía X cuenta actualmente con un gran PBX en su matriz y pequeños PBX en sus corporativos remotos. Varias alternativas de solución están disponibles para esta compañía:

- Contratar líneas dedicadas entre su matriz y cada uno de sus corporativos remotos.
- Contratar una VPN telefónica a algún carrier y marcar un código de acceso para acceder a la VPN desde cualquier lugar.
- Aprovechar la infraestructura de datos ya existente e implementar la red telefónica sobre la red de datos.

Sin importar que opción elija la compañía X, deben enfrentarse las siguientes cuestiones: diseño del plan de numeración y marcación, administración de la red y costos. Sin entrar en mucho detalle, la mayor parte de las cuestiones en las que se centra el diseño de un plan de marcación son:

- Crecimiento a futuro.
- Costo de las líneas dedicadas o VPN.
- Costo del equipo adicional para la red de voz basada en paquetes.
- Traslapamiento de los números telefónicos en los diferentes corporativos.
- Patrón de llamadas en cada sitio
- Horas pico (periodo del día cuando hay mayor carga de llamadas).

Como resultado del estudio de los puntos anteriores, la compañía X planea sustentar de un 20 a un 30 por ciento de crecimiento y usar un plan de marcación de 5 dígitos basado en sus patrones de crecimiento (pues no hay más de 1000 usuarios por corporativo y no habrá más de 100 corporativos), donde 2 dígitos serán usados para indicar el corporativo y 3 dígitos para indicar el subscriptor.

Por último, supongamos que la compañía X decidió emigrar su red telefónica hacia una plataforma totalmente de VoIP, haciendo de este forma que sus redes de voz y datos converjan sobre una única infraestructura de red basada en IP. Algunas de las cuestiones que deberían tenerse en cuenta antes y durante la emigración son las siguientes:

- Red de datos bien diseñada y dimensionada a nivel LAN y WAN.
  - LAN's corporativas → redes switchadas de alta velocidad.
  - WAN → anchos de banda adecuados a la demanda actual.
  - Topología centralizada hacia la matriz pero con trayectorias redundantes entre algunos corporativos.
- Contratación de líneas conmutadas (troncales digitales o analógicas) para la conexión hacia la PSTN en todos y cada uno de los diferentes corporativos de la empresa.
- Considerar los Gateways e interfaces que permitirán interconectar la red de datos hacia la PSTN en sus diferentes puntos.

- Contratación de líneas privadas para el intercambio de paquetes de voz, video y datos entre los diferentes corporativos de la compañía.
- Contratación de enlaces de datos en la matriz, para la conexión hacia la Internet de ésta y todos sus corporativos.
- Diseño del plan de direccionamiento IP global.
- Diseño del plan de ruteo de datos a nivel WAN.
- Diseño del plan de numeración y marcación telefónica global.
    - Marcar el número de extensión para alcanzar cualquier teléfono de usuario sobre la red corporativa.
    - Marcar 9 como dígito líder para realizar llamadas externas hacia la PSTN.
- Diseño del plan de ruteo telefónico local y global para la definición y optimización de rutas alternas en la realización de llamadas telefónicas.
- Asignación de DID's.
- Funcionamiento en red para la transparencia de las facilidades telefónicas de usuario a lo largo y ancho de toda la red (call-forward, call-back, call-pickup, transferencia de llamadas, conferencias, etc).
- Correo de voz corporativo (Mensajería Unificada), Aplicaciones IVR, Call Center.
- Operadora automática.
- Alimentación de los IP-Phones.
- PC's multimedia adecuadas para funcionar como SoftPhones.
- Uso de esquemas de QoS a nivel LAN y WAN.
- Limitación del número de llamadas.
- Esquemas de seguridad.

Lo que puede observarse como resultado de la integración o convergencia de la redes de voz, video y datos de una empresa son las siguientes:

- Convergencia de los medios de transporte (compartición del cableado en cobre/fibra).
- Convergencia de las herramientas de administración y monitoreo.
- Convergencia de las herramientas de seguridad.
- Convergencia de operaciones.
- Convergencia de las herramientas de tarificación y facturación.

Conclusiones

En este capítulo se han explorado algunos de los fundamentos alrededor de los cuales está construido VoIP, así como algunos consejos y reglas para el diseño e implementación de una red de voz basada en paquetes IP. En general, en el diseño de red de VoIP se deben cuidar aspectos tales como:

- Implementación sobre una red LAN/WAN bien diseñada y dimensionada.
- Elección del esquema de codificación a usar a lo largo de toda la red.
- Reducción del retardo total de una llamada sobre la WAN a no más de 150 ms.
- Uso de mecanismos de QoS para prioritizar el tráfico de paquetes de voz y reservarle el ancho de banda adecuado en su paso por los enlaces WAN.
- Diseño del plan numeración y marcación.
- Diseño del plan de direccionamiento IP.
- Conexión y alimentación de los IP-Phones.
- Protocolo de señalización y control de las llamadas a usar (H.323, SIP, etc).

CAPÍTULO 3

PROTOCOLOS DE SEÑALIZACIÓN H.323 Y SIP

"Detrás de toda comunicación potente y eficiente, está el respaldo de un lenguaje y unas reglas de comunicación simples y flexibles"

VoIP es una tecnología de reciente desarrollo en el mundo de las telecomunicaciones, por lo cual cabe esperar la llagada y desaparición de varias propuestas de VoIP en los próximos años. La propuesta que al final acabe imponiéndose será aquella que se capaz de ofrecer la siguiente generación de servicios y aplicaciones telefónicos, y mantenga un nivel de servicio y confiabilidad parecido o mejor que el del sistema telefónico tradicional. En todo caso, la relación costo/beneficio que ofrezca VoIP debe ser muy clara si es que pretende triunfar.

En este capítulo se hace una exploración de los modelos o arquitecturas de VoIP, así como de las diferentes propuestas que han surgido durante los últimos 5 años, haciendo hincapié en las ventajas y desventajas de cada una de ellas. Hablamos más específicamente sobre la primera generación de arquitecturas en la Telefonía-IP (tales como MGCP, Megaco u otros protocolos propietarios como SCCP de Cisco), caracterizados por su procesamiento centralizado. Así como de la segunda generación de arquitecturas de Telefonía-IP (como H.323 y SIP), caracterizadas por usar un modelo distribuido cliente-servidor e inteligencia sobre los teléfonos.

3.1 Modelos Arquitectónicos

La Telefonía Tradicional así como la primera generación de arquitecturas de la Telefonía-IP (tales como MGCP, Megaco u otros protocolos propietarios como SCCP de Cisco), están basadas sobre un modelo de procesamiento centralizado, por el cual toda la inteligencia y procesamiento del sistema se concentra sobre el switch CO o el servidor de comunicaciones, dejando muy poco a los dispositivos de usuario (teléfonos), que se comportan como terminales tontas.

El resultado de seguir este esquema no es necesariamente negativo, de hecho, la red telefónica tradicional sigue siendo por hoy una de las redes más grandes del mundo y con seguridad, la más confiable en cuanto al nivel de servicio ofrecido. Sin embargo, hay ciertos inconvenientes y problemas detrás de este esquema (como se vio en el Capítulo 1) que están llevando a hacer una apuesta cada vez más grande en la Telefonía-IP, basada en un diseño de procesamiento distribuido tipo cliente-servidor rico en prestaciones y aplicaciones.

A la cabeza de esta nueva ola en la Telefonía-IP están H.323 y SIP, protocolos de señalización y control de llamadas *peer-to-peer* (diseño cliente-servidor). Sus principales ventajas sobre la Telefonía Tradicional son:

- ***Innovación*** → hará posible la siguientes generación de servicios y aplicaciones telefónicas al permitir no sólo a los carriers, sino a todas las empresas desarrolladoras de software, participar en el proceso de creación de nuevas y mejores aplicaciones.
- ***Fácil uso*** → los usuarios podrán hacer uso de manera más fácil de todo un abanico de servicios y facilidades.
- ***Reducción de costos*** → habrá un ahorro de costos en llamadas de larga distancia, así como en gastos por concepto de administración y mantenimiento.

3.2 H.323

H.323 es una Recomendación de la ITU-T (International Telecomunication Union) para las comunicaciones multimedia (voz, video y datos) en tiempo real sobre redes de datos basadas en paquetes (incluyendo IP, IPX, etc) que pudieran no ofrecer un nivel de QoS garantizado. H.323 puede ser aplicado en una variedad de situaciones: solo audio (Telefonía-IP); audio y video (Videotelefonía); audio y datos; y audio, video y datos. H.323 puede también ser aplicado a comunicaciones multimedia multipunto. H.323 provee un centenar de servicios y, por lo tanto, puede ser aplicado a una amplia variedad de áreas: consumo, negocios y entretenimiento.

El estándar H.323 está dirigido a la señalización y control de llamadas, al control y transporte multimedia y al control del ancho de banda para conexiones punto-a-punto, punto-a-multipunto y de broadcast (difusión).

Este protocolo ha estado evolucionando a través del tiempo para adaptarse a los nuevos requerimientos y necesidades de las comunicaciones multimedia actuales, según lo muestra las diferentes versiones que sobre este protocolo han aparecido:

- ***Versión 1 de H.323 (Octubre de 1996).***
- ***Versión 2 de H.323 (Enero de 1998).***
- ***Versión 3 de H.323 (1999).***
- ***Versión 4 de H.323 (2000).***

H.323 es parte de la familia de las recomendaciones H.32x de la ITU-T. Las otras recomendaciones de la familia especifican servicios de comunicación multimedia sobre diferentes tipos de redes:

- H.310 sobre B-ISDN
- H.320 sobre ISDN
- H.321 sobre ATM
- H.322 sobre LAN's con QoS
- H.324 sobre PSTN/Wireless

Un los objetivos primarios en el desarrollo del estándar H.323 fue su interoperabilidad con estas otras redes de servicios multimedia ITU-T. Como se verá más adelante, esta interoperabilidad es lograda a través del uso de Gateways, encargados de realizar cualquier traslado de señalización o de formatos.

3.2.1 Componentes H.323

En la Figura 3-1 se ilustran los componentes o entidades H.323 básicas en una red multiservicios típica. Estos son:

- *Terminales*
- *Gateways*
- *Gatekeepers*
- *MCU's*
- *Proxy Servers*

Las Terminales, Gateways y MCU's son colectivamente conocidos como *puntos-finales*. Aún cuando una red H.323 pueda estar conformada solo por Terminales, los otros componentes son esenciales por los servicios que ofrecen.

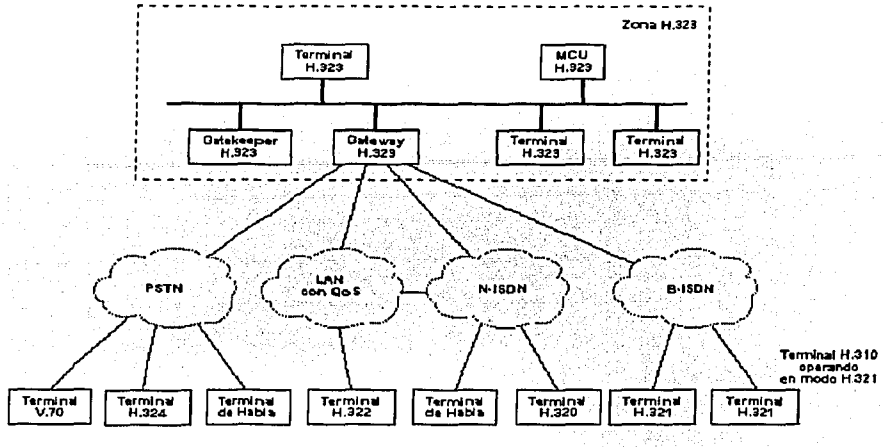


Figure 3-1: Interoperabilidad de H.323 con otras redes H.32x

3.2.2 Terminales H.323

Una Terminal H.323 es un punto-final sobre una red de datos capaz establecer comunicaciones en tiempo real punto-a-punto o punto-multipunto con otra Terminal H.323, Gateway o MCU. Como mínimo toda Terminal H.323 debe soportar comunicaciones de voz y opcionalmente, comunicaciones de video y/o datos. Puesto que el servicio básico provisto por la Terminales H.323 son comunicaciones de audio, estas juegan un papel importante en la Telefonía-IP.

Una Terminal H.323 puede ser ya sea una PC multimedia (SoftPhone) o un dispositivo stand-alone (Telefonos IP, Terminales de videoconferencia), corriendo H.323 y aplicaciones multimedia.

En la Figura 3-2 se ilustra una Terminal H.323 con sus componentes funcionales básicos. En general una Terminal H.323 está constituida por una unidad de control de sistema, la capa de señalización H.225, una unidad de codec de audio y una interface de red LAN. Las unidades de codec de video y de aplicaciones de datos de usuario son opcionales.

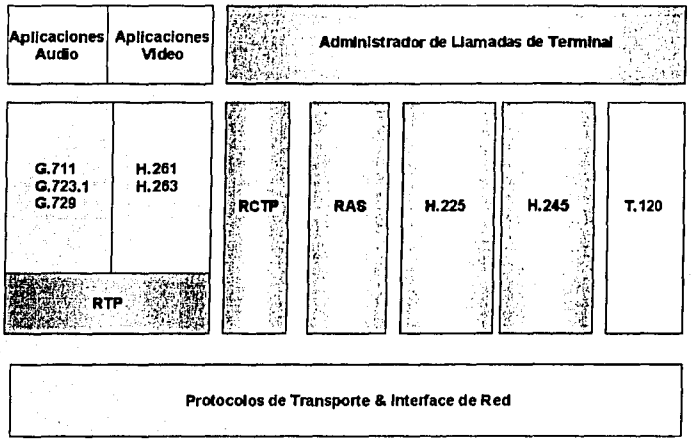


Figura 3-2: Stack de protocolos propios de las Terminales H.323

Las Terminales H.323 deben soportar las siguientes funcionalidades o capacidades:

- ***Señalización de Control H.245*** → para el intercambio de las capacidades de las Terminales y la creación de canales de medios.
- ***Señalización de Llamadas H.225*** → para la señalización de llamadas (establecimiento, mantenimiento y liberación).
- ***Señalización RAS H.225*** → para el registro y otros controles de admisión con un Gatekeeper.
- ***RTP/RTCP*** → para la secuenciación de los paquetes de audio y video.
- ***CODEC de Audio*** → realiza la codificación-decodificación del habla siguiendo alguno de los estándares de codificación (G.711, G.722, G.723.1, G.728 y G.729) y compresión de audio (Ley-A y Ley-μ).
- ***Interface de Red LAN*** → proporciona la interfaz de conexión hacia la red LAN.

Las Terminales H.323 pueden también soportar CODEC's de video y T.120 para conferencias de datos y capacidades de MCU.

3.2.3 Gateway (GW)

Un Gateway es un elemento opcional sobre un red de datos H.323, requerido solo cuando se desea que ésta interopere con una red no-H.323. La interoperabilidad entre redes de diferente naturaleza es lograda mediante la apropiada conversión entre formatos de medios (audio, video y datos); procedimientos y protocolos de comunicación (por ejemplo, de H.225 a H.221, o de H.245 a H.242); y transferencia de información entre las redes conectadas al Gateway. En general, el propósito de un Gateway es reflejar de manera transparente las características y facilidades de una red datos H.323 basada en paquetes sobre una red no-H.323 basada en conmutación de circuitos (PSTN, ISDN, ATM, etc), y viceversa.

El stack de protocolos propios de un Gateway se ilustra en la siguiente Figura 3-3, en donde se destacan sus elementos funcionales principales.

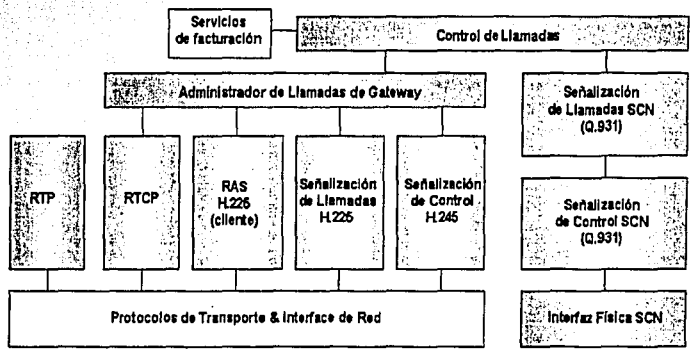


Figura 3-3: Stack de Protocolos propios de los Gateways.

Los Gatekeepers están al tanto de cuales puntos-finales son Gateways, porque esto les es indicado cuando las Terminales y los Gateways se registran ante un Gatekeeper. Un Gateway es un componente lógico de H.323 que puede ser implementado sólo o como parte de un Gatekeeper o MCU.

La Figura 3-4 muestra a un Gateway sirviendo de interfaz entre una terminal H.323 y una terminal no H.323.

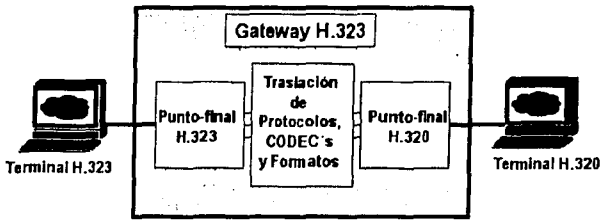


Figura 3-4: Gateway H.323-H.320

3.2.4 Gatekeeper (GK)

Los Gatekeepers proveen servicios de control de llamadas a los puntos-finales H.323, tales como la traslación de direcciones, la gestión del ancho de banda y control de acceso tal como se establece dentro de la señalización RAS. Un Gatekeeper es igualmente un elemento opcional sobre una red H.323; sin embargo, si está presente en la red las Terminales y los Gateways deben de usar sus servicios. El estándar H.323 define servicios obligatorios que el Gatekeeper debe proveer y especifica otras funcionalidades opcionales que puede proveer.

Una funcionalidad opcional de un Gatekeeper es el ruteo de la señalización de llamada. Los puntos-finales envían los mensajes de señalización de llamada al Gatekeeper, el cual los rutea hacia los puntos-finales destino. Alternativamente, los puntos finales pueden enviar sus mensajes de señalización de llamadas directamente a los puntos-finales par. Esta funcionalidad del Gatekeeper es valiosa, puesto que el monitoreo de las llamadas por el Gatekeeper provee un mejor control de las llamadas en la red. El ruteo de llamadas a través de Gatekeepers provee un mejor rendimiento en la red, puesto que el Gatekeeper puede hacer decisiones de ruteo basado sobre una variedad de factores, por ejemplo, el balanceo de carga entre Gateways.

Los servicios ofrecidos por un Gatekeeper son definidos por la señalización RAS e incluyen la traslación de direcciones, la admisión de control, el control del ancho de banda y la gestión de zona de dominio (ver Figura 3-5). Las redes H.323 que no tienen Gatekeepers no poseen estas capacidades; sin embargo, cuando sobre una red H.323 existen Gateways, es aconsejable que también exista un Gatekeeper que realice las funciones de traslado entre los números telefónicos E.164 entrantes y las direcciones IP asociadas. Un Gatekeeper es un componente lógico de H.323 que puede ser implementado sólo o como parte de un Gateway o MCU.

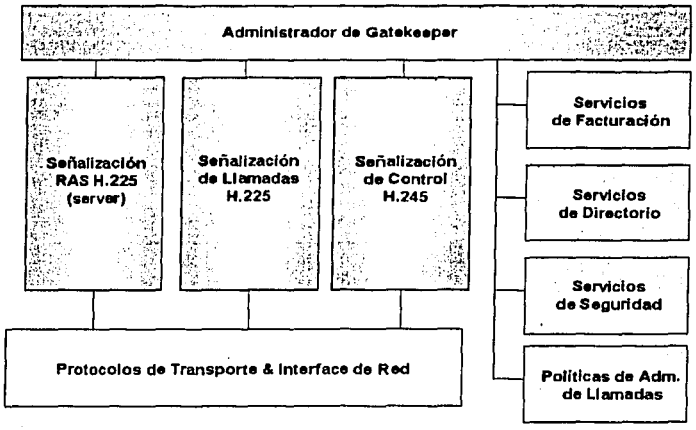


Figura 3-5: Elementos funcionales (obligatorios y opcionales) de un Gatekeeper.

Un Gatekeeper también puede proveer otros servicios, tales como la contabilidad, la tarificación, el ruteo de las llamadas, la gestión del ancho de banda, la gestión de la zona de dominio y la localización de Gateways, entre otros.

Un Gatekeeper es frecuentemente referido como el cerebro de una red H.323 por los servicios de control y administración centralizados que ofrece. Aunque los puntos-finales pueden conectarse directamente sin la intervención de un Gatekeeper, este tipo de funcionamiento es muy limitado. Los Gatekeepers son necesarios para asegurar una comunicación confiable y comercialmente factible.

En una red H.323 con administración y control centralizados todos los puntos-finales intentan registrarse con un Gatekeeper en el arranque usando el protocolo RAS. Cuando un punto-final desea comunicarse con otro, pide la aceptación de la llamada al Gatekeeper, usando un alias simbólico para el nombre del punto-final tal como una dirección E.164 o una dirección de e-mail. Si éste decide que la llamada procede, regresa la dirección IP destino al punto-final origen. Esta dirección IP puede ser la dirección real del punto-final deseado o la dirección de un punto intermedio (tal como un Proxy). Establecida la comunicación entre las Terminales, el Gatekeeper ya no necesita intervenir, con lo que la carga del sistema se reparte entre las Terminales. Finalmente, un Gatekeeper y sus puntos-finales registrados intercambian información de estado

Es responsabilidad del Gatekeeper mantener un control de todo el tráfico generado por las diversas comunicaciones H.323, a fin de no saturar la red de datos. El control de ancho de banda permite al administrador fijar un límite de utilización, por encima del cual se rechazan las llamadas bien sean internas o externas.

Otro aspecto importante que debe manejar el Gatekeeper es el enrutamiento de las llamadas. De esta forma, el propio Gatekeeper puede redireccionar las llamadas al Gateway mas indicado o elegir un nuevo destino sí el original no esta disponible. Es en este punto donde una solución por software puede dotar al administrador del sistema de herramientas potentes de control y definición de reglas.

Cuando un Gatekeeper está presente en una red H.323 provee varios servicios obligatorios a los puntos-finales dentro de su zona de administración. Estos servicios incluyen:

- ***Traslación de Direcciones*** → provee a los puntos-finales generadores de una llamada la traslación entre la dirección E.164 (número telefónico estándar) o los alias (gregorio@noc.unam.mx) del punto-final llamado y su dirección IP de transporte correspondiente. Esto es logrado mediante una tabla de traslación en el Gatekeeper que es generada y actualizada mediante los mensajes de Registro RAS.
- ***Control de Acceso*** → permite a un Gatekeeper la posibilidad restringir el acceso a la red a ciertas Terminales y Gateways. Son usados para tal efecto los mensajes RAS ARQ/ACF/ARJ (Admission Request / Admission Confirm / Admission Reject).
- ***Gestión del Ancho de Banda*** → permite a un Gatekeeper la posibilidad restringir la admisión de llamadas en base a la disponibilidad del ancho de banda. Son usados para tal efecto los mensajes RAS BRQ/BCF/BRJ (Bandwidth Request / Bandwitdth Confirm / Bandwidth Reject). Los administradores pueden gestionar el ancho de banda especificando un límite en el número máximo de llamadas simultáneas o denegando la autorización a llamar a ciertas Terminales durante momentos congestionados. El resultado es limitar el total del ancho de banda asignado a una fracción del total disponible, dejando el restante para las aplicaciones de datos normales.
- ***Gestión de Zona*** → permite a un Gatekeeper proveer las funciones de gestión y control antes expuestas a los puntos-finales que se han registrado con él.

Servicios opcionales que puede prestar un Gatekeeper, son:

- ***Señalización de Control de Llamadas*** → rutea los mensajes de señalización de llamada entre los puntos-finales cuando se está usado el esquema GKRCS (Gatekeeper Routed Call Signalling) para establecer el Canal de Señalización de Llamada entre los puntos-finales. Bajo el esquema DECS (Direct Endpoint Call Signalling), el Gatekeeper permite a los puntos-finales enviar los mensajes de señalización de llamada directamente entre ellos.

- ***Autorización de Llamada*** → permite que un Gatekeeper acepte o rechace la petición de llamada de un punto-final. Las razones para el rechazo pueden estar basadas en limitaciones sobre el número máximo de llamadas activas o en los privilegios/restricciones de los puntos-finales.
- ***Ruteo de Llamadas*** → Un Gatekeeper puede enrutar las llamadas originadas o entrantes a su zona. Esta capacidad ofrece muchas ventajas. Primeramente, información de contabilización de llamadas puede ser mantenida para procesos de facturación y seguridad. Segundo, un Gatekeeper puede enrutar una llamada hacia un Gateway apropiado basado en la disponibilidad del ancho de banda. Tercero, el enrutamiento puede ser usado para desarrollar servicios más avanzados tales como el direccionamiento móvil, el call-fordwarding y el desvió hacia el correo de voz.
- ***Servicios de Directorio y Contabilidad CDR (Call Detail Recording)***

3.2.5 Zonas Gatekeeper

Por razones de administración y escalabilidad los puntos-finales H.323 son agrupados en zonas o dominios. Cada zona tiene asociado un único Gatekeeper que proporciona servicios de Registro, Admisión y Estatus (RAS) a todos los puntos-finales miembro. El concepto de zonas es similar al de los dominios DNS, solo que en este caso hablamos de dominios RAS. Una zona es independiente de la topología de la red de datos. En general, una zona normalmente se hace corresponder con una zona geográfica.

Hay uno y solamente un Gatekeeper asociado a una zona en un momento dado, aunque si bien varios dispositivos podrían asumir su función para esa zona en caso de falla. Los dispositivos que podrían proveen las funciones de señalización RAS del Gatekeeper primario son referidos como Gatekeepers Alternos.

3.2.6 MCU y sus Elementos (MC y MP´s)

Un MCU (Unidad de Control Multipunto) es un punto-final sobre una red H.323 que proporciona soporte a conferencias multipunto entre tres o más puntos-finales y, como mínimo, consiste de un MC (Controlador Multipunto) y cero o más MP's (Procesadores Multipunto). Un MCU típico que soporta conferencias multipunto centralizadas consiste de un MC y un MP de audio, video y datos. Los MCU's gestionan los recursos de la conferencia, negocian entre las Terminales con el propósito de determinar que codec de audio/video usar. Aunque los Gatekeepers, Gateways y MCU's son elementos lógicamente separados, pueden estar implementados en sobre el mismo equipo físico.

Un ***MC (Multipoint Controller)*** provee las funciones de control para soportar conferencias entre tres o más puntos-finales en una conferencia multipunto. La señalización de llamada y de control es dirigida a través del MC de modo que las capacidades de los puntos-finales pueden ser determinados y los parámetros de comunicación ser negociados a fin de que los puntos-finales lleguen a un consenso sobre el modo de operación (¿transmisión de video o sólo audio?, ¿qué codec de audio/video usar?, etc). Además, un MC puede revisar el conjunto de capacidades que envía a las Terminales como resultado de la unión o separación de Terminales a la conferencia. Otra tarea útil del MC es enviar por unicast o multicast los streams de audio y video dependiendo de las capacidades de la red.

Cuando dos o más puntos-finales están en una conferencia, los puntos-finales deben usar el procedimiento de resolución Maestro-Esclavo de la Recomendación H.245 para determinar el MC que controlará la conferencia. El MP (Multipoint Processor) mezcla los streams de audio, video o datos recibidos y los distribuye a los puntos-finales participantes en una conferencia multipunto.

3.2.7 Servidor Proxy H.323

Un servidor Proxy H.323 es un proxy específicamente diseñado para las redes H.323. El Proxy opera en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los Proxys pueden determinar el destino de una llamada y establecer la conexión si se desea. Un servidor Proxy soporta las siguientes funciones claves:

- Mecanismos de QoS tales como IP-Precedence y RSVP: Terminales que no soportan RSVP (Resource Reservation Protocol) pueden conectarse hacia un Proxy cercano y delegarles esta función. Los Proxys pueden gestionar la QoS a través de RSVP o IP precedence.
- Un Proxy es compatible con NAT (Network Address Translation), posibilitando a los nodos H.323 estar desplegados en redes con espacios de direcciones IP no homologadas.
- Un Proxy desplegado sin un firewall o independiente de un firewall provee seguridad de modo que solo el tráfico H.323 pase a través de él. Un Proxy desplegado en conjunción con un firewall permite que el firewall sea configurado simplemente para pasar todo tráfico H.323 tratando al Proxy como un nodo confiable. Esto permite que el firewall provea seguridad en la red de datos y el Proxy provea de seguridad H.323.
- Comunicaciones seguras sobre las extranets.

Como las aplicaciones H.323 son dinámicamente alojadas en sockets para canales de audio, vídeo y datos, un firewall debe ser capaz de permitir trafico H.323 a través de él con una base inteligente. El firewall debe tener un Proxy H.323 o un canal de control capaz de determinar cual socket dinámico esta en uso por la sesión H.323, y permitir el tráfico cuando el canal de control está activo.

3.2.8 Suite de Protocolos H.323

H.323 está basado en varios protocolos, tal como se ilustra en la Figura 3-6. La familia de protocolos soporta la admisión de llamadas, setup, status, teardown, media streams y mensajes en el sistema H.323. Estos protocolos son soportados para mecanismos de entrega de paquetes confiables y no confiables sobre redes de datos.

Los protocolos especificados por H.323 están listados abajo. H.323 es independiente de los protocolos de red y transporte sobre los que corre y no los especifica.

La Recomendación H.323 es un conjunto de protocolos para conferencias voz, video y datos sobre redes basadas en paquetes tales como Internet. El stack de protocolos de H.323 está diseñado para operar con independencia de los protocolos de red y transporte usados. Como tal, H.323 puede ser usado arriba de cualquier red de transporte basada en paquetes (como Ethernet, TCP/UDP/IP, ATM, Frame Relay, etc) para proveer comunicaciones multimedia en tiempo real.

H.323, al igual que TCP/IP, es en realidad una familia de protocolos:

FUNCIÓN	PROTOCOLO
Señalización de Llamadas	H.225
Señalización H.225 de Registro, Admisión y Estatus	RAS - H.225
Señalización de Control	H.245
CODEC's de Audio	G.711, G.722, G.723, G.723.1, G.728 y G.729
CODEC's de Video	H.261 y H.263
Conferencias y compartición de datos	T.120
Medios de transporte	RTP/RTCP

El stack de protocolos H.323 corre encima de las capas de transporte y de red del modelo OSI. Si la red de paquetes usada es IP (que es la red más común) entonces el audio, video y señalización RAS H.225 usan el servicio de transporte no confiable de UDP, mientras que los paquetes de datos y control (H.245 y señalización de llamada H.225) son transportados usando los servicios de transporte confiable de TCP.

Aunque la mayoría de las implementaciones H.323 de hoy utilizan a TCP como mecanismo de transporte para señalización, la versión 2 de H.323 posibilita el transporte UDP.

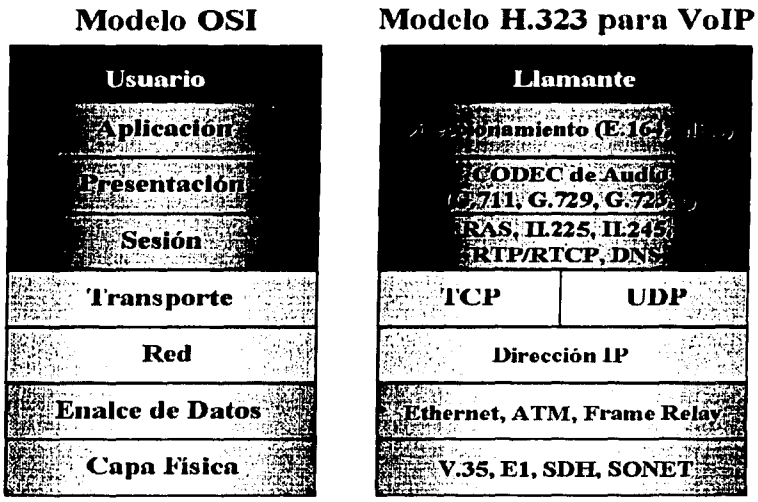


Figura 3-6: Comparación del Modelo OSI y el Modelo H.323 para VoIP.

3.2.9 Mecanismos de Señalización y Control

El flujo de información en una red H.323 consiste de una mezcla de *streams* (flujos) de mensajes de audio, video, datos y de control. La información de control es esencial para el establecimiento y liberación una llamada, para el intercambio y negociación de capacidades, y para propósitos de administración. H.323 usa tres protocolos de control :

- ***Señalización de Registro, Admisión y Estatus (RAS H.225)*** → provee un control de llamada en redes H.323 basadas en Gatekeepers.
- ***Señalización de Llamadas (H.225/Q.931)*** → usada para conectar, mantener y desconectar llamadas entre puntos finales.
- ***Señalización de Control de Medios y Transporte (H.245)*** → provee el canal H.245 confiable que transporta mensajes de control de medios. El transporte ocurre con un stream no confiable UDP.

Los mensajes de control y de procedimientos definen cómo los componentes H.323 se comunican. Los componentes H.323 se comunican a través de la transmisión de Flujos de Información, los cuales pueden ser clasificados como de video, audio, datos, control de comunicaciones y de llamada, etc. Las señales de control de llamada son usadas para el establecimiento y desconexión, y otras funciones de control. Los flujos de información

descritos arriba son formateados y enviados por las interfaces de red como se describe en la Recomendación H.225.

3.2.10 Señalización RAS H.225

La señalización RAS (Registro, Admisión y Estatus) provee servicios de control de acceso y admisión de llamadas sobre redes H.323 donde existen Gatekeepers y zonas. Con este objeto un canal RAS es establecido entre los puntos-finales y el Gatekeeper de zona. El canal RAS es abierto antes de que cualquier otro canal sea establecido y es independiente de la Señalización de Llamadas H.225 y de los canales de transporte de medios H.245. El canal RAS es una conexión UDP no confiable usada para las siguientes funciones:

- Descubrimiento de Gatekeeper
- Registro de un Punto-Final
- Localización de un Punto-Final
- Control del Ancho de Banda
- Autorización de Llamada
- Información sobre el Estatus

3.2.10.1 Descubrimiento del Gatekeeper

El Descubrimiento del Gatekeeper es un procedimiento estático o dinámico que los puntos-finales H.323 usan para determinar con cuál Gatekeeper quedarán registrados. En el método estático, los puntos-finales saben a priori la dirección de transporte IP del Gatekeeper y, por lo tanto, pueden intentar registrarse inmediatamente, aunque solo con él. El método dinámico requiere un mecanismo conocido como Autodescubrimiento, por el cual un punto-final manda un mensaje GRQ de multicast a la dirección de multicast descubrimiento de Gatekeeper (224.0.0.41 puerto 1718): "¿Quién es mi Gatekeeper?" Uno o más Gatekeepers pueden responderle con un mensaje GCF: "Yo puedo ser tu Gatekeeper". Los siguientes tres mensajes RAS son usados para el Autodescubrimiento del Gatekeeper:

- ***GRQ (Gatekeeper Request)*** → mensaje multicast enviado por un punto-final en busca de su Gatekeeper.
- ***GCF (Gatekeeper Confirm)*** → respuesta a una indicación GRQ de punto-final indicando la dirección de transporte del canal RAS del Gatekeeper.
- ***GRJ (Gatekeeper Reject)*** → anuncio que un Gatekeeper envía hacia un punto-final cuando no ha aceptado su registro. Esto es debido usualmente a una configuración sobre el Gateway o Gatekeeper.

La Figura 3-7 ilustra los procesos de mensajería y secuenciación del proceso del autodescubrimiento del Gatekeeper.

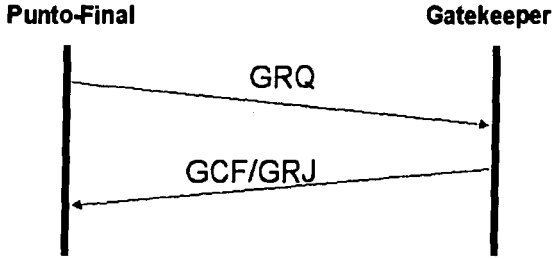


Figure 3-7: Autodescubrimiento del Gatekeeper.

Para proveer redundancia sobre una red H.323 basada en Gatekeepers, el Gatekeeper de registro puede indicar Gatekeepers alternativos que pueden ser usados en caso de que el Gatekeeper primario falle. La lista de Gatekeepers alternativos es proporcionada en el campo alternateGatekeeper de los mensajes GCF y RCF.

3.2.10.2 Registro de un Punto-Final

El registro es el proceso que permite a los puntos-finales adherirse a una zona e informar al Gatekeeper asociado sobre su dirección de transporte IP y su dirección de alias. El registro ocurre después del proceso de Descubrimiento de Gatekeeper, mas antes de que pueda intentarse realizar cualquier llamada. Se usan los siguiente seis mensajes RAS para permitir a un punto-final registrarse o cancelar su registro:

- ***RRQ (Registration Request)*** → enviado desde el punto-final a la dirección del canal RAS del Gatekeeper.
- ***RCF (Registration Confirm)*** → enviado por el Gatekeeper para confirmarle al punto-final sobre su registro.
- ***RRJ (Registration Reject)*** → enviado por Gatekeeper para rechazar el registro a un punto-final.
- ***URQ (Unregister Request)*** → mensaje enviado por un punto-final hacia el Gatekeeper o viceversa para cancelar el registro del punto-final.
- ***UCF (Unregister Confirm)*** → mensaje enviado por el Gatekeeper hacia el punto-final o viceversa para confirmar la cancelación del registro del punto-final.
- ***URJ (Unregister Reject)*** → mensaje usado para indicar que el punto-final en cuestión no se había registrado previamente con el Gatekeeper.

La Figura 3-8 ilustra los procesos de mensajería y secuenciación en el registro de un punto-final así como el desregistro de un punto-final o Gatekeeper.

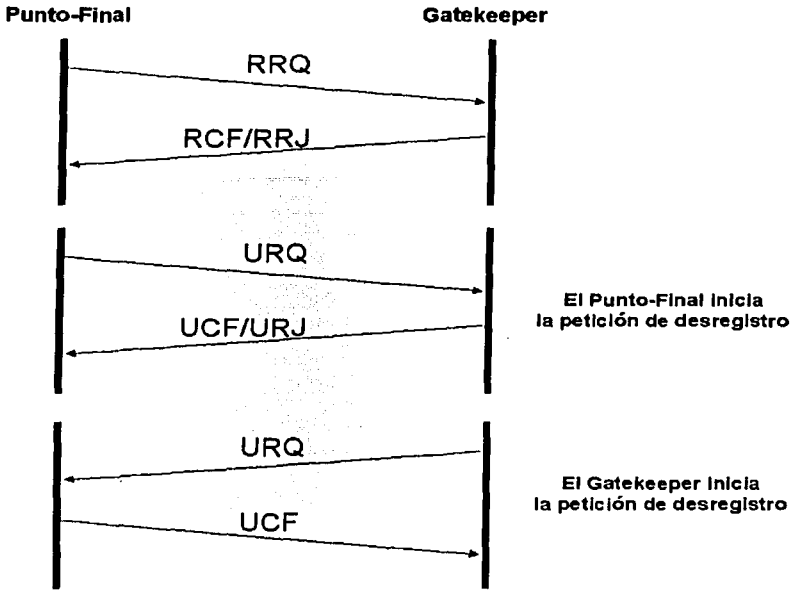


Figura 3-8: Registro/Desregistro RAS

3.2.10.3 Localización de un Punto-Final

Los puntos-finales y los Gatekeepers usan el proceso de "Localización de un punto-final" para obtener la dirección de transporte IP de un punto-final llamado cuando solo disponen de su dirección de alias. Los mensajes de localización son enviados a la dirección del canal RAS del Gatekeeper o a la dirección multicast de descubrimiento del Gatekeeper. El Gatekeeper responsable de la administración de esa zona le contesta al punto-final con un mensaje LCF (Location Confirmation) indicándole su propia dirección de transporte IP, así como la del punto-final requerido.

El punto-final o Gatekeeper puede incluir en la petición una o más direcciones E.164 fuera de la zona. Se usan los siguientes tres mensajes en la localización de un punto-final:

- ***LRQ (Location Request)*** → enviado para pedir la información de contacto de un punto-final o Gatekeeper para una o más direcciones E.164.

- ***LCF (Location Confirm)*** → enviado por el Gatekeeper y contiene la dirección del canal de señalización de llamada o del canal RAS de sí mismo o del punto-final requerido. Se usa la propia dirección cuando el GKRCS es usado y la dirección del punto-final requerido cuando la Señalización de Llamada de Punto-final Directa es usada.
- ***LRJ (Location Reject)*** → enviado por el Gatekeeper que recibe un LRQ para el cual el punto-final requerido no está registrado o no tiene recursos disponibles.

3.2.10.4 Control del Ancho de Banda

El control de ancho de banda es inicialmente gestionado a través de los intercambios de admisión entre un punto-final y el Gatekeeper con la secuencia ARQ/ACF/ARJ. El ancho de banda puede cambiarse durante una llamada. Se usan los siguientes mensajes para el cambio del ancho de banda:

- ***BRQ (BandWidth Request)*** → enviado por el punto-final hacia el Gatekeeper para pedir un incremento o decremento en el ancho de banda de una llamada.
- ***BCF (BandWidth Confirm)*** → enviado por el Gatekeeper al punto-final aceptando la petición para e cambio en el ancho de banda.
- ***BRJ (BandWidth Reject)*** → enviado por el Gatekeeper al punto-final rechazando la petición para el cambio en el ancho de banda (posiblemente por no haber ancho de banda disponible).

Nota: el control del ancho de banda está limitado por solo el Gateway o Gatekeeper y no toma en cuenta el estado de la red en sí. El Gatekeeper actual mira solo a su tabla estática de ancho de banda para determinar si una petición de ancho de banda es rechazada o aceptada.

3.2.10.5 Autorización de Llamada

El canal RAS es usado también para autorizar o denegar la petición de realización de llamada de un punto-final en base a cuestiones de disponibilidad de ancho de banda. Los siguientes mensajes proveen control de admisión en redes H.323:

- ***ARQ (Admission Request)*** → intento de un punto-final de iniciar una llamada.
- ***ACF (Admission Confirm)*** → autorización del Gatekeeper para la realización de la llamada.
- ***ARJ (Admisión Reject)*** → denegación a la petición del punto-final para la realización de la llamada.

3.2.10.6 Información sobre el Estatus

El Gatekeeper puede usar el canal RAS para obtener información sobre el estatus de algún punto-final. Este mensaje puede usarse para monitorear si un punto-final está en línea o fuera de línea debido a una condición de falla. El periodo de poleo típico para el mensaje de estatus es de 10 segundos. Durante el ACF, el Gatekeeper también puede pedir que el punto-final envíe mensajes de estatus periódicos durante la llamada. Se pueden usar los siguientes tres mensajes para proveer el estatus sobre un canal RAS:

- ***IRQ (Information Request)*** → enviado desde el Gatekeeper al punto-final pidiendo su estatus.
- ***IRR (Information Request Response)*** → enviado por el punto-final hacia el Gatekeeper en respuesta a un IRQ. Este mensaje también es enviado periódicamente si el Gatekeeper lo solicitara.
- ***SE (Status Enquery)*** → enviado fuera del canal RAS sobre el canal de sañalización de llamada. Un punto-final o Gatekeeper puede enviar un mensaje SE a otro punto-final para verificar el estado de una llamada. Los Gatekeepers típicamente usan estos mensajes para verificar si una llamada aun está activa.

3.2.11 Señalización de Llamadas H.225

El protocolo de Señalización de Llamadas H.225 es un derivado del protocolo de señalización de llamadas Q.931 de ISDN, y proporciona los mecanismos básico para el establecimiento, mantenimiento y liberación de llamadas entre dos puntos-finales H.323. Para tal efecto, un canal de señalización de llamadas confiable (puerto TCP 1720) es abierto entre los puntos-finales H.323 o entre un punto-final y su Gatekeeper, según el esquema de ruteo seguido, y por el cual se pasan los mensajes de señalización de llamada H.225.

Ruteo de los Mensajes de Señalización de Llamada: los mensajes de señalización de llamada H.225 pueden intercambiarse de manera directa entre los puntos-finales o ser ruteados a través de un Gatekeeper. El primero es el método DECS (Direct Endpoint Call Signalling), ver Figura 3-9. El segundo es el método GKRCS (Gatekeeper Routed Call Signalling), ver la Figura 3-10. El método elegido es decidido por el Gatekeeper durante el proceso inicial de registro RAS de los puntos-finales.

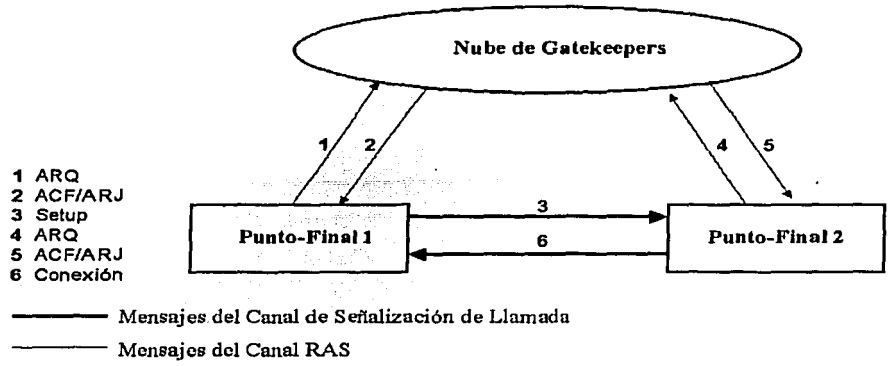


Figura 3-9: Señalización de Llamada Directa entre Puntos-Finales (DECS).

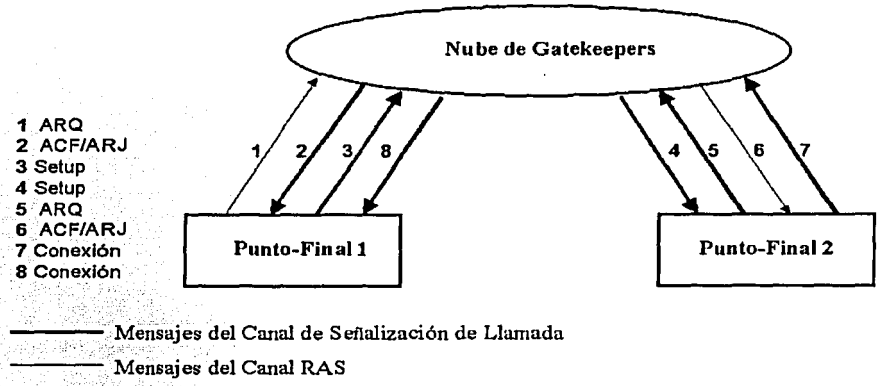


Figura 3-10: Señalización de Llamada Ruteada por Gatekeeper (GKRCS).

Los siguientes mensajes H.225 son los más comúnmente usados en redes H.323:

- ***Setup*** → un mensaje forward es enviado por la entidad H.323 llamante como un intento de establecer una conexión con la entidad H.323 llamada. Este mensaje es enviado sobre el puerto web-known TCP 1720.

- ***Call Proceeding*** → un mensaje retorno es enviado por la entidad llamada hacia la entidad llamante para anunciar que los procedimientos para el establecimiento de la llamada fueron iniciados.
- ***Alerting*** → un mensaje retorno es enviado desde la entidad llamada para avisar que el ring sobre la entidad llamada fue iniciado.
- ***Connect*** → un mensaje de retorno enviado desde la entidad llamada indicando a la entidad llamante que la parte llamada a contestado la llamada. El mensaje de conexión puede contener la dirección de transporte UDP/IP para la señalización de control H.245.
- ***Release Complete*** → enviado por el punto-final indicando la desconexión, lo cual indica que la llamada está siendo liberada. Este mensaje solo se envía si el canal de señalización está abierto o activo.
- ***Facility*** → mensaje Q.932 usado para pedir o confirmar servicios suplementarios. Es también usado para indicar si una llamada debe ser directa o debe pasar a través de un Gatekeeper.

3.2.12 Señalización de Control de Medios (H.245)

La señalización de control H.245 es usada para intercambiar mensajes de control extremo a extremo entre dos puntos-finales H.323 que quieren establecer una llamada. Los mensajes de control H.245, que son transportados sobre canales de control confiables H.245 (puerto TCP dinámico), proveen el medio para el intercambio de capacidades, modos de preferencias, indicaciones y la apertura/cierre de canales lógicos para la transmisión de audio, video, datos e información de control.

H.245 provee las siguientes funcionalidades de control de medios:

- ***Intercambio de Capacidades*** → H.245 permite a un punto-final dar a conocer sus capacidades a otro punto-final H.323 (tipo de medios audio-video-datos, CODEC's, bit-rates, etc) con el cual quiere establecer una llamada. Debe recordarse que este escenario no es una negociación, y que los parámetros anunciados en su lista de capacidades no necesariamente serán usados.
- ***Apertura y Cierre de Canales Lógicos*** → canales lógicos separados necesitan ser abiertos para que se de la comunicación de audio, video, datos. Es a través del canal lógico 0 que se envían mensajes de control necesarios para la apertura o cierre de tales canales de medios.
- ***Mensajes de Control de Flujo*** → estos mensajes proveen información de retroalimentación a los puntos-finales cuando se presentan problemas de comunicación.
- ***Otros Comandos y Mensajes*** → varios otros comandos y mensajes pueden ser usados durante una llamada para informar e instruir un cambio al punto-final par (como el cambio de CODEC).

Ruteo del Canal de Control: cuando es usada la señalización de llamada GKRCS, existen dos métodos para rutear el Canal de Control H.245. En el primer método, el Canal de Control H.245 es establecido directamente entre los puntos-finales. Ver Figura 3-11. En el segundo método, el Canal de Control H.245 es ruteado entre los puntos-finales a través del Getekeeper. Ver Figura 3-12. Este método permite al Gatekeeper redireccionar el Canal de Control H.245 hacia un MC cuando una conferencia multipunto ad hoc es switchada a partir de una conferencia punto-a-punto. Cuando la señalización de llamada DECS es usada, el Canal de Control H.245 solo puede ser conectado directamente entre los puntos-finales.

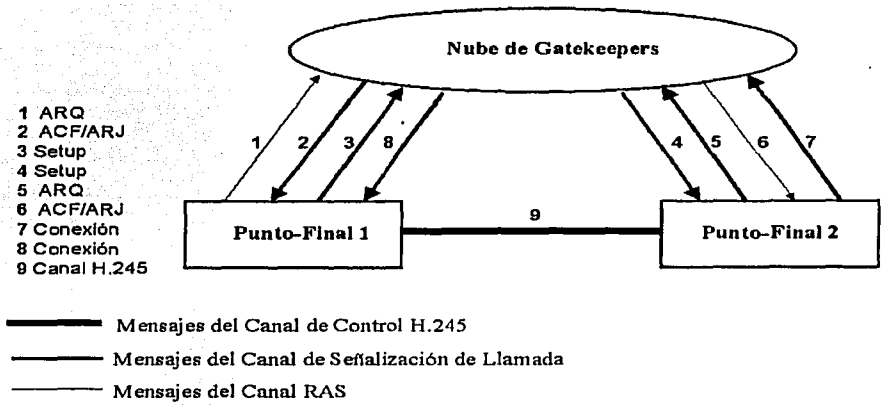


Figura 3-11: Conexión de Canal de Control H.245 Directo entre Puntos-Finales.

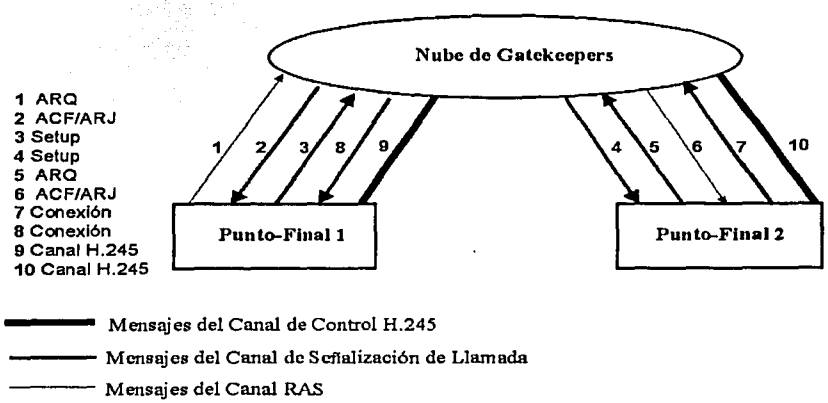


Figura 3-12: El Gatekeeper Rutea al Canal de Control H.245.

3.2.13 Transporte de Medios (RTP/RTCP)

RTP (Real-time Transport Protocol), junto con su protocolo de control asociado RTCP (Real-time Transport Control Protocol), provee el servicio de transporte en tiempo real de los streams de audio y video sobre una red de datos IP. Más específicamente, RTP/RTCP ofrece los servicios de entrega extremo a extremo en tiempo real y es empleado para lograr una sincronía y entrega ordenada de los streams de audio y video. RTP/RTCP es una recomendación de la IETF (Internet Engineering Task Force) que provee:

- ***Framing Lógico*** → define cómo el protocolo empaqueta los datos de audio y video para su transporte sobre un canal de comunicación seleccionado.
- ***Secuencia de Numeración*** → determina el orden de los paquetes de datos transportados sobre un canal de comunicaciones.
- ***Distinción del tipo de datos (payload)*** → permite diferenciación entre la voz y el video.
- ***Time-stamping*** → información sobre el tiempo de referencia asociado a un paquete.
- ***Monitoreo de Entrega***

Una vez que los procesos de control y establecimiento de llamada han sido completados, los paquetes de audio y video empiezan a ser enviados vía UDP (ver Tabla 3-2), aunque no sin antes habérseles adicionado el encabezado RTP/RTCP que provee el time-satmping y la secuencia de numeración. Con esta información el nodo receptor logra dar la cadencia y el orden apropiado a los paquetes recibidos, permitiendo que el usuario escuche y vea la información correctamente (ver Figura 3-13). RTP/RTCP hace uso de buffers para minimizar el jitter y la latencia, logrando un flujo continuo de audio y video.

Tabla 3-2: Puertos UDP

del	al	Aplicación	Prioridad
0	16383	No especificada	Baja
16384	32767	Audio	Alta
32768	49151	Whiteboard	Media
49152	65535	Video	Baja

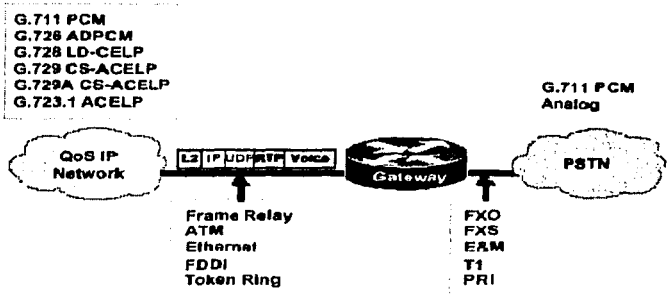


Figura 3-13: Gateway H.323 transportando los paquetes UDP con el encabezado RTP/RTCP (Notar que la capa RTP está arriba de la capa de transporte del modelo OSI).

3.2.14 Seguridad en H.323

La recomendación H.235 especifica los requerimientos de seguridad para las comunicaciones H.323. Cuatro servicios de seguridad son provistos: autenticación, integridad, privacidad y no rechazo.

La autenticación es provista por el control de admisión de los puntos-finales. Esto es manejado por el Gatekeeper que administra la zona. La integridad de los datos y la privacidad es provista por la encriptación. El no rechazo asegura que un punto-final no deniegue la participación de otro en una llamada. Esto es también provisto por los servicios del Gatekeeper.

Para implementar estos servicios de seguridad, H.235 puede hacerse uso de estándares tales como IPSec (IP Security) y TLS (Transport Layer Security).

3.2.15 Flujo de Llamadas H.323

Los flujos de llamada descritos en esta sección ilustran la forma en la que se establece una llamada entre dos puntos-finales H.323. Se asume que estas son llamadas de voz y que los puntos finales ya han completado su registrado ante el Gatekeeper apropiado. Los ejemplos de establecimiento de llamada incluyen dos implementaciones diferentes de Gatekeeper así como dos métodos diferentes de señalización de llamada.

Los ejemplos ilustrados en las Figuras 3-14 y 3-15 detallan los procedimientos de establecimiento de llamada para una implementación única de Gatekeeper. La Figura 3-14 ilustra el flujo de la llamada usando el esquema de señalización de llamada DECS entre dos puntos-finales compartiendo el Gatekeeper.

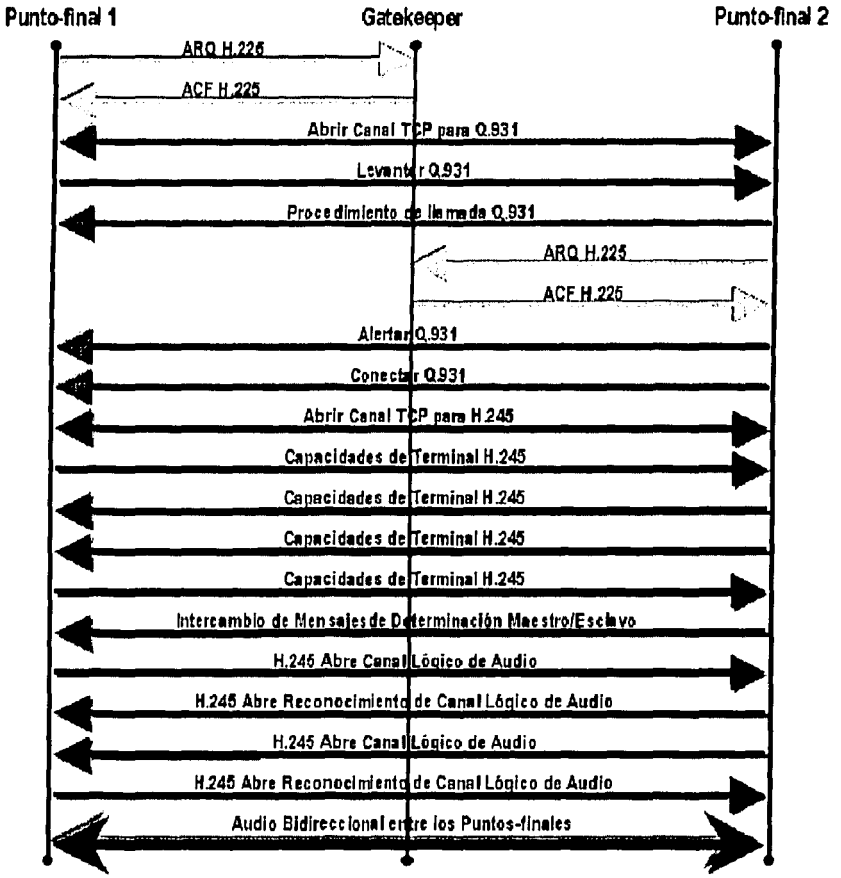


Figura 3-14: Señalización de Llamada DECS (mismo Gatekeeper).

La Figura 3-15 ilustra el flujo de la llamada usando el esquema de señalización de llamada GKRCS entre dos puntos-finales compartiendo el Gatekeeper. Notar que el procedimiento H.245 es manejado directamente entre los puntos finales y que no es ruteado por el Gatekeeper.

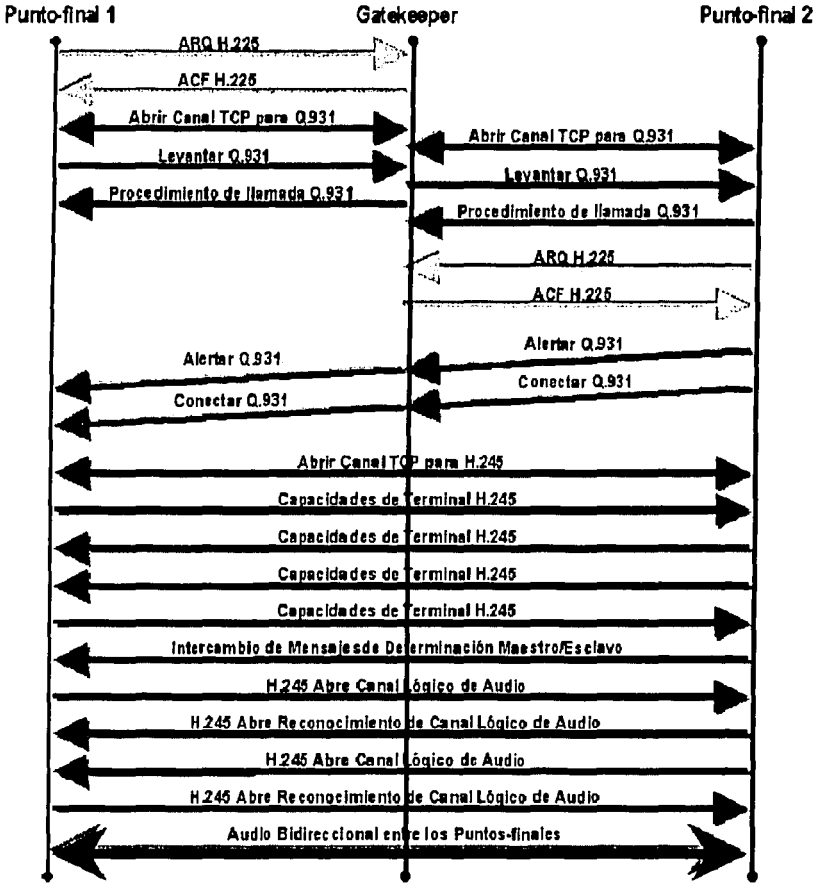


Figura 3-15: Señalización de Llamada GKRCS (mismo Gatekeeper).

Los ejemplos de la Figuras 3-16 y 3-17 ilustran los procedimientos de establecimiento de llamada para implementaciones duales de Gatekeeper. Específicamente, la Figura 3-16 ilustra el flujo de la llamada usando el esquema de señalización de llamada DECS entre los puntos-finales que tienen Gatekeepers diferentes. La principal diferencia entre GKRCS y DECS es que en el primero el mensaje de establecimiento es dirigido al Gatekeeper, mientras que en el segundo es dirigido hacia el punto-final Terminal.

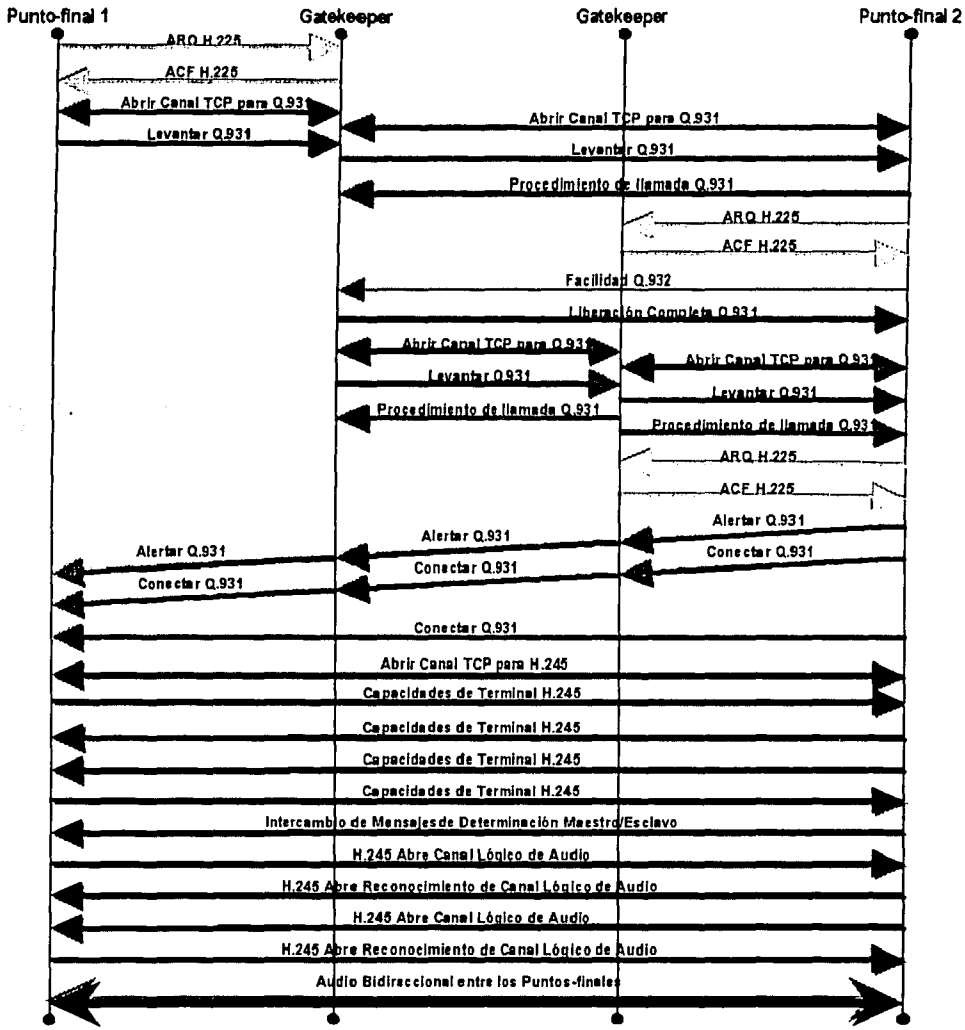


Figura 3-16: Señalización de Llamada DECS (dos Gatekeepers).

En el ejemplo final muestra el procedimiento de establecimiento de llamada para el método GKRCS, por el cual cada punto-final tiene un Gatekeeper diferente. Esto posibilita que mensajes LRQ's y LCF's sean enviados entre los dos Gatekeepers, lo que permite el control de los registros de tarificación en el Gatekeeper mientras los mensajes de establecimiento y control pasan a través del Gatekeeper.

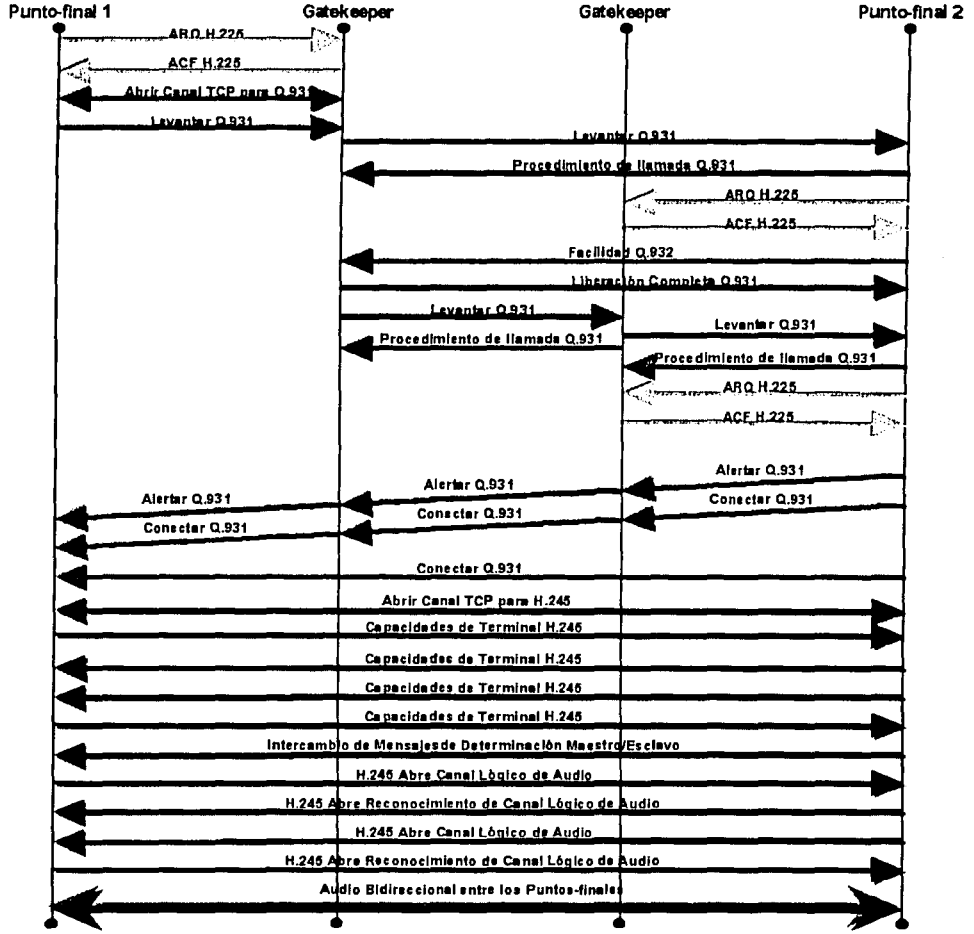


Figura 3-17: Señalización de Llamada GKRCS (dos Gatekeepers).

3.3 SIP (Session Initiation Protocol)

SIP es un estándar de la IETF para las comunicaciones multimedia (voz, video y datos) en tiempo real sobre redes IP. Al igual que otros protocolos de VoIP, SIP está diseñado para cumplir las funciones de señalización y administración de las sesiones multimedia entre dos o más Puntos-finales. Está definido bajo el RFC 2543 de la IETF, y algunas de sus aplicaciones más conocidas son la Telefonía-IP, la Video Conferencia y el Video Streaming.

En la terminología de TCP/IP, SIP es un protocolo sobre la capa de aplicación que usa los servicios de transporte de UDP, aunque también correr sobre TCP. SIP está basado sobre los protocolos existentes y bien conocidos de Internet y los extiende para soportar a la Telefonía-IP. La flexibilidad de los mensajes SIP permite la construcción de servicios telefónicos avanzados, incluyendo los servicios de movilidad.

SIP soporta sesiones unicast y multicast así como llamadas punto-a-punto o punto-a-multipunto. El establecimiento y término de una llamada pasa por las siguientes cinco etapas SIP: localización de usuario, capacidad de usuario, disponibilidad del usuario, levantamiento de la llamada y manejo de la llamada. A continuación se ofrece una descripción más detallada de cada una de estas etapas:

- ***Determinar la ubicación de un punto-final deseado*** → SIP soporta la resolución de direcciones, mapeo de nombres y redirección de llamada.
- ***Determinar las capacidades de medios del punto-final deseado*** → Vía SDP (Session Description Protocol), SIP determina el nivel más bajo de los servicios comunes entre los puntos-finales. Las conferencias son establecidas usando solamente las capacidades de medios que pueden ser soportados por todos los puntos-finales.
- ***Determinar la disponibilidad del punto-final deseado*** → Si una llamada no puede ser completada porque el punto-final deseado no está disponible, SIP determina si la parte llamada estaba ya en una llamada o si no contestó en un número determinado de timbrados. Entonces devuelve un mensaje indicando por qué el punto-final deseado estaba no disponible.
- ***Establecer una sesión entre el punto-final originante y deseado*** → Si la llamada puede ser completada, SIP establece una sesión entre los puntos-finales. SIP también soporta cambios sobre una llamada en curso, tales como la adición de otro punto-final a la conferencia o el cambio de las características de los medios o CODEC.
- ***Manejar la transferencia y terminación de las llamadas*** → SIP soporta la transferencia de llamadas desde un punto-final a otro. Durante la transferencia de una llamada, SIP simplemente establece una sesión entre el transferido y un nuevo punto-final (especificado por la parte que transfiere) y termina la sesión entre el transferido y la parte que transfiere. Al final de la llamada, SIP termina las sesiones entre todas las partes.

3.3.1 Componentes de SIP

SIP es un protocolo *peer-to-peer* basado en la arquitectura cliente-servidor. Como tal, los componentes de una red SIP pueden ser agrupados en dos categorías: Clientes o UA's (User Agents) y los Servidores de Red. La Figura 3-18 ilustra los componentes típicos de una red SIP.

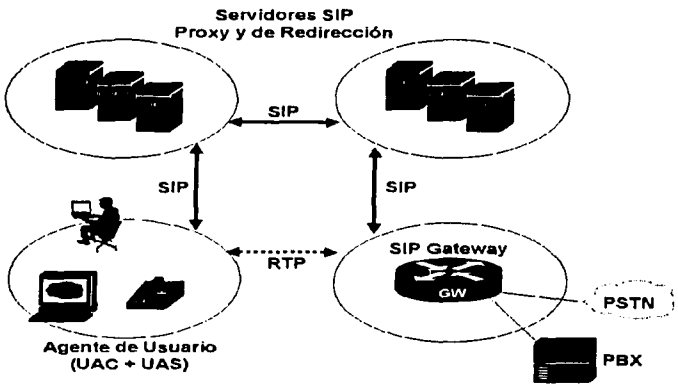


Figura 3-18: Componentes de una red SIP

3.3.1.1 Clientes SIP User Agent

Los peers o puntos-finales en una sesión SIP son generalmente llamados UA's (User Agents). Un Agente de Usuario tiene la capacidad para desempeñar tanto el rol de cliente como de servidor:

- ***UAC (User Agent Client)*** → aplicación de cliente que inicia peticiones SIP (tal como iniciar una llamada) actuando como el agente de usuario llamante.
- ***UAS (User Agent Server)*** → aplicación de servidor que recibe peticiones SIP (tales como una llamada entrante) y responde a ellas en nombre del usuario, actuando como el agente del usuario llamado.

Ejemplos de clientes SIP incluyen:

- Teléfonos SIP y Softphones (PC's que tienen las capacidades de teléfono instaladas).
- Gateways SIP (proveen muchos servicios a los Puntos-finales SIP en su comunicación con otro tipo de terminales, siendo los más comunes la traslación transparente entre formatos, procedimientos de comunicación y protocolos de señalización).

3.3.1.2 Servidores SIP

Existen básicamente tres tipos de servidores SIP:

- ***Servidor de Registro y Localización*** → en su función de registro, recibe y acepta las peticiones de registro (mensajes REGISTER) de los clientes. Conforme un usuario se mueve de posición dentro de la red, éste registra su nueva ubicación ante el Servidor de Registro local. Por otro lado, en su función de localización, devuelve a los Servidores Proxy o de Redirección la(s) dirección(es) IP donde posiblemente podría localizársele a un Punto-final llamado. Para localizar a un usuario, el Servidor Proxy o de Redirección envía el nombre del Punto-final llamado al Servidor de Localización, el cual devuelve cero o múltiples ubicaciones donde puede ser encontrado. Si el usuario llamante conoce de antemano la dirección IP del destino, puede entonces contactar directamente al UAS del usuario llamado. Los Servidores de Registro y Localización están frecuentemente implementados sobre los Servidores Proxy o de Redirección.
- ***Servidor Proxy*** → dispositivo intermedio que recibe las peticiones SIP de un cliente, sirviéndolas o reenviándolas a nombre del cliente al siguiente servidor SIP en la red. Un Servidor Proxy interpreta y, si es necesario, rescribe los mensajes de petición antes de reenviarlos. Los Servidores Proxy pueden proveer de funciones tales como la autenticación, autorización, control de acceso a la red, ruteo, retransmisión confiable de peticiones y seguridad.
- ***Servidor de Redirección*** → devuelve al cliente la dirección IP del Servidor SIP del próximo salto en la red, al que se podrá recurrir en busca de la dirección IP de algún otro punto-final con el cual se desea establecer una llamada. Los Servidores de Redirección no aceptan llamadas (a diferencia de los UAS), ni generan sus propias peticiones SIP (a diferencia de los Servidores Proxy), tan sólo se limitan a procesar y desviar las peticiones SIP recibidas.

Para complementar la información obtenida a través de los registros de usuario, el Servidor de Registro/Localización puede también usar uno o más protocolos TCP/IP (tales como finger, rwhois, LDAP, protocolos basados en multicast o mecanismos dependientes de los sistemas operativos) para determinar activamente el lugar donde un usuario puede ser encontrado.

Los Servidores SIP pueden interactuar con otros servidores de aplicación, tales como servidores LDAP (Lightweight Directory Access Protocol), bases de datos, servidores RADIUS o aplicaciones XML (Extensible Markup Language). Estos servicios de aplicación proveen servicios como directorio, autenticación, autorización y facturación.

3.3.2 Direccionamiento SIP

Los usuarios dentro de una red SIP son identificados por direcciones SIP únicas, también conocidas como URL's SIP. Una dirección SIP no es sino una dirección de e-mail tradicional a la que se le ha añadido una indicación sobre el protocolo con que deberá ser procesada (**SIP: user@host**). Esto es importante, pues significa que el direccionamiento y los servicios de nombres y de ruteo de la Internet pueden usarse para procesar las direcciones SIP sin modificación alguna. Los siguientes son algunos ejemplos de URL's en SIP:

SIP: gregorio@noc.unam.mx
SIP: gregorio@200.15.3.10
SIP: 5622-8509@redes.unam.mx

La porción de usuario de la dirección SIP puede ser ya sea un nombre o una dirección E.164, mientras que la porción de host puede ser un nombre de dominio o una dirección IP.

3.3.3 Encapsulación de Mensajes SIP -- MIME

MIME (Multipurpose Internet Mail Extensions) es el estándar de la Internet para describir los diferentes tipos de contenido sobre la Internet, incluyendo video e imágenes. Es usado ya por HTTP para componer páginas Web, y por los sistemas e-mail para codificar los mensajes e-mail. SIP usa este estándar bien conocido para codificar información, eliminando la necesidad de inventar una nueva técnica para codificar voz y multimedia sobre la Internet.

3.3.4 Mensajes SIP

Existen básicamente dos tipos de mensajes SIP: las peticiones provenientes desde un UAC o Servidor SIP, y las respuestas a una petición. SIP es un protocolo basado en texto en el que la sintaxis y campos de encabezados de sus mensajes son idénticos a los de HTTP. En las Tablas 3-3 y 3-4 se muestran las peticiones y códigos de respuesta usados por SIP:

Tabla 3-3: Mensajes de Petición en SIP	
INVITE	Usado para invitar a un Punto-final a participar en una llamada.
ACK	Aceptación a la petición INVITE enviada por un cliente.
BYE	Permite terminar una llamada y puede ser enviado tanto por el llamante como por el llamado.
CANCEL	Permite a una entidad SIP cancelar cualquier petición en curso, pero no termina una llamada que ya había sido aceptada.
OPTIONS	Permite indagar las capacidades de los UA y servidores.
REGISTER	Permite a los clientes registrar su información de localización ante un Servidor Proxy o de Redirección.

Tabla 3-4: Códigos de Mensajes de Respuesta en SIP	
SIP 1xx	Respuesta Informativa: petición recibida, continuando a procesar la petición
SIP 2xx	Respuesta de Éxito: acción satisfactoriamente recibida, comprendida y aceptada
SIP 3xx	Respuesta de Redirección: acción adicional necesaria para completar la petición
SIP 4xx	Respuesta de Falla de Cliente: la petición no tiene la sintaxis correcta o no puede ser ejecutada en un servidor
SIP 5xx	Respuesta de Falla de Servidor: falla en un servidor en el procesamiento de una petición aparentemente válida
SIP 6xx	Respuesta de Falla Global: petición que no puede ser procesada en ningún servidor

3.3.5 Proceso de Registro

El proceso de registro ocurre en el arranque cuando un cliente informa a un Servidor de Registro sobre su localización. Durante este proceso, el cliente manda una petición REGISTER al Servidor de Registro (generalmente albergado ya sea en el Servidor Proxy o el Servidor de Redirección) e incluye la dirección (o direcciones) en los cuales puede ser encontrado.

3.3.6 Establecimiento de Llamadas SIP

SIP es un protocolo que depende de los mensajes INVITE y ACK para el establecimiento satisfactorio de una llamada entre dos Puntos-finales. En su forma más básica, el Punto-final llamante envía una petición de INVITE a la dirección IP (puerto UDP 5060) del Punto-final llamado solicitándole unirse a una conferencia en particular o establecer una llamada punto-a-punto con él. En su petición el Punto-final incluye también información acerca de los tipos de medios y formatos que desea para la llamada. Si el Punto-final llamado desea aceptar la llamada, envía una respuesta afirmativa (SIP 2xx), retornando a su vez una lista sobre los medios y formatos que serán usados. De otra forma, envía una respuesta negativa (SIP 4xx). Una vez recibida la respuesta de aceptación, el Punto-final llamante manda un acuse de recibo o ACK y una sesión RTP es establecida para transportar los paquetes de voz entre los dos Puntos-finales. SDP (Session Description Protocol) provee la lógica de servicios, incluyendo el ruteo , rechazo, redirección, logeo y notificación. Si alguno de los Puntos-finales desea terminar la llamada envía un mensaje BYE.

El esquema de llamada antes descrito será usado siempre que el Punto-final conozca con precisión la dirección(es) IP del Punto-final llamado, pues en caso contrario requerirá de los servicios ofrecidos por algún Servidor SIP. En las siguientes secciones se proporcionan ejemplos de llamadas punto-a-punto establecidas usando ya sea un Servidor Proxy o un Servidor de Redirección. En estos escenarios, el establecimiento de una llamada es ilustrado para cuando el llamante conoce el nombre pero no la dirección IP del llamado, requiriendo los servicios de un Servidor SIP

Es común que de tiempo en tiempo un usuario final SIP se mueva de lugar y cambie su posición sobre la red. Para estos casos SIP cuenta con los Servidores de Registro/Localización, encargados de recibir los mensajes de registro de los Puntos-finales, así como de proporcionar esta información a los Servidores SIP que lo soliciten. El Servidor de Registro/Localización puede usar uno o más protocolos (incluyendo finger, rwhois y LDAP) para localizar a un usuario final. Puesto que el usuario final puede estar logeado en más de una estación, este deberá retornar más de una dirección IP.

3.3.6.1 Usando un Servidor Proxy

Cuando un Servidor Proxy es usado por un Punto-final para establecer una llamada SIP con otro Punto-final en la red, la siguiente cadena de eventos tiene lugar:

1. El UAC del **Punto-final1@Site1** llamante envía su petición de llamada INVITE hacia el Servidor Proxy (cuya dirección IP es conocida, pues ha sido previamente configurada sobre la estación del usuario llamante), y cuyo destino llamado es el **Punto-final2@Site2**.
2. El Servidor Proxy consulta al Servidor de Localización en busca de la información de ubicación del punto-final llamado.
3. El Servidor de Localización manda al Servidor Proxy información precisa sobre la ubicación del Punto-final2 (como se muestra en la Figura 3-19).
4. El Servidor Proxy desvía la petición INVITE hacia la(s) dirección(es) IP proporcionadas por el Servidor de Localización sobre la estación llamada (después de recibir la petición INVITE, el UAS del Punto-final llamado alerta al usuario generando un timbrado de teléfono).
5. El UAS del Punto-final llamado responde al Servidor Proxy con un mensaje de respuesta 100 TRYING indicándole que se está procesando la petición INVITE. El Servidor Proxy a su vez retransmite este mensaje hacia el Punto-final llamante.
6. El UAS del punto-final llamado retorna un mensaje de respuesta 200 OK para indicar la aceptación de la petición INVITE (como se muestra en la Figura 3-20).

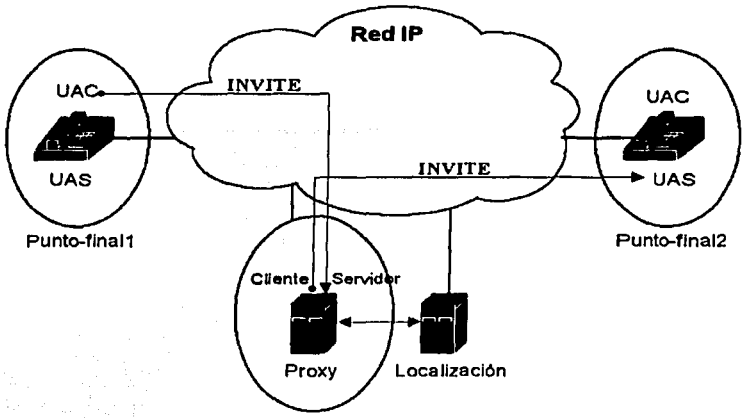


Figura 3-19: Petición de establecimiento de llamada a través de un Servidor Proxy.

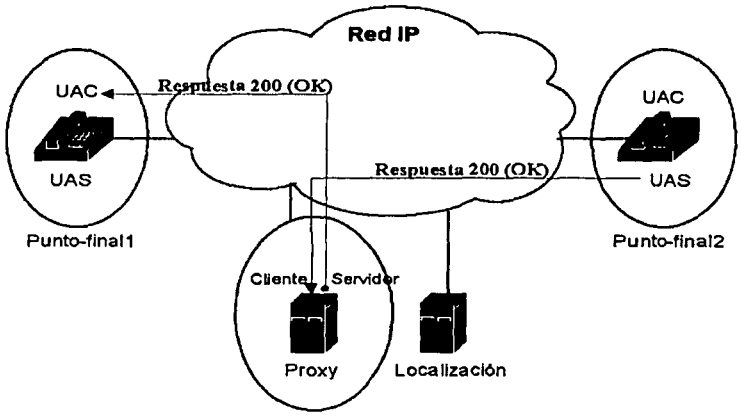


Figura 3-20: Respuesta 200 (OK) de aceptación de llamada.

7. El UAC del Punto-final1 llamante envía un mensaje de ACK hacia el Proxy Server, y éste a su vez hacia el Punto-final2 para completar el Handshake y pueda comenzar la llamada entre los Puntos-finales con apoyo de los servicios proporcionados por RTP (como se muestra en la Figura 3-21).

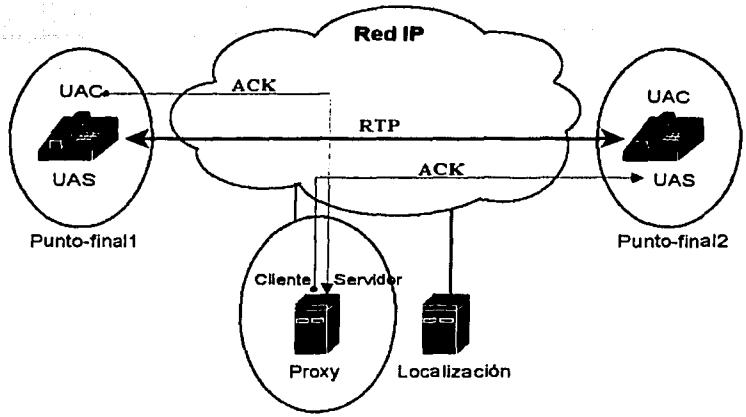


Figura 3-21: Establecimiento de llamada a través de un Servidor Proxy.

Los puntos anteriores son esquematizados convenientemente en el diagrama de flujo de la Figura 3-22:

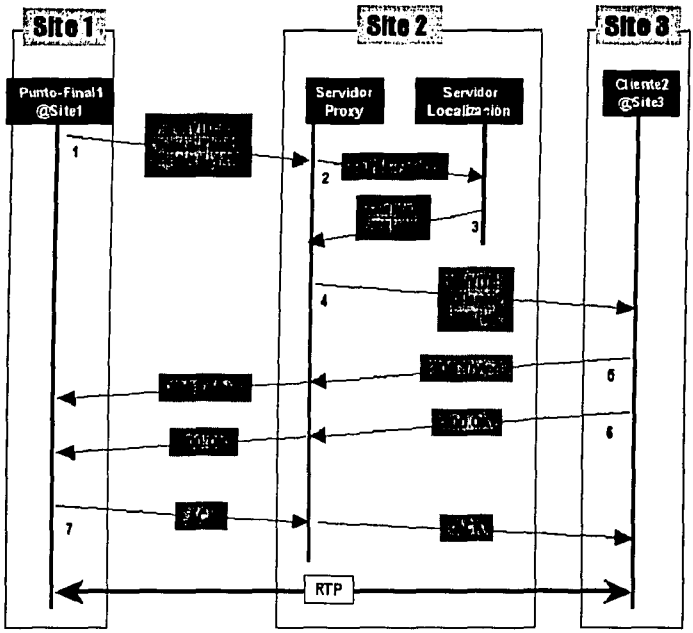


Figura 5: Diagrama de Flujo (llamada a través de un Servidor Proxy).

3.3.6.2 Usando un Servidor de Redirección

Cuando un Servidor de Redirección es usado por un Punto-final para establecer una llamada SIP con otro Punto-final en la red, la siguiente cadena de eventos tiene lugar (como se muestra en el diagrama de flujo de la Figura 6):

1. El UAC del **Punto-final1@Site1** llamante envía su petición de llamada INVITE hacia el Servidor de Redirección, y cuyo destino llamado es el **Punto-final2@Site2**.
2. El Servidor de Redirección consulta al Servidor de Localización en busca de la información de ubicación del punto-final llamado.
3. El Servidor de Localización manda al Servidor de Redirección información precisa sobre la ubicación del Punto-final2 (en este caso mediante un mensaje 302 MOVED TEMPORARILY, y con **Cliente2@Site2** como dirección de respuesta).

4. El Servidor de Redirección desvía este mensaje de ubicación hacia el UAC del Punto-final1.
5. El UAC del Punto-final llamante responde al Servidor de Redirección con un ACK.

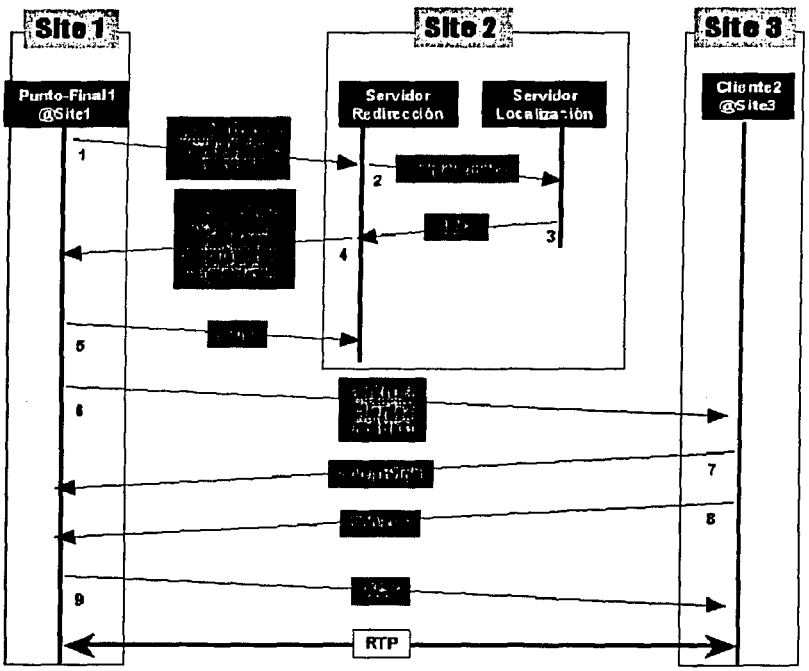


Figura 6: Diagrama de Flujo (llamada a través de un Servidor Proxy).

6. El UAC del Punto-final llamante manda una la petición de llamada INVITE directamente hacia la(s) dirección(es) IP del Punto-final llamado proporcionada(s) en el paso anterior.
7. El UAS del Punto-final2 llamado responde al UAC del Punto-final1 llamante con un mensaje de respuesta 100 TRYING indicándole que se está procesando su petición INVITE.
8. El UAS del Punto-final2 llamado responde al UAC del Punto-final1 llamante con un mensaje de respuesta 200 OK para indicarle la aceptación de la petición INVITE.

9. El UAC del Punto-final1 llamante envía un mensaje de ACK hacia el Punto-final2 para completar el Handshake y pueda comenzar la llamada entre los Puntos-finales mediante los auspicios de RTP.

3.3.7 SIP Versus H.323

SIP y H.323 fueron diseñados para realizar las funciones de señalización y control de llamadas sobre una arquitectura distribuida. Aunque SIP y H.323 también pueden ser usados para comunicar Puntos-finales con inteligencia limitada, ellos están especialmente provistos para la comunicación de Puntos-finales inteligentes.

Tabla 3-5: Provee una breve comparación entre SIP y H.323

ASPECTO	SIP	H.323
Clientes	Inteligentes	Inteligentes
Inteligencia de la red y servicios	Provista por los servidores (Proxy, Redirector, Registro)	Provista por los Gatekeepers
Modelo usado	Internet/WWW	Telefonía/QSIG
Protocolo de señalización	UDP o TCP	TCP (UDP es opcional enla versión 3)
Protocolos de medios	RTP	RTP
Código base	ASCII	Binario (ANSI)
Otros protocolos usados	SDP, http y MIME	H.225, H.245 y H.450
Interoperabilidad entre vendedores	Amplio	limitado

Aunque los mensajes de SIP no son directamente compatibles con H.323, ambos protocolos pueden coexistir sobre una misma red telefónica de paquetes si un dispositivo que soporte la interoperabilidad está disponible. Por ejemplo, un agente de llamada puede usar H.323 para comunicarse con Gateways y usar SIP para la señalización de agente de interllamada. Entonces, después de que la conexión ha sido establecida, la información fluye entre los diferentes Gateways en la forma de un stream RTP.

SIP tiene algunas ventajas sobre H.323, tales como un menor tiempo de establecimiento de llamada y menor complejidad. El diseño e implementación de SIP es parecida al de la Web, con una arquitectura modular y con funciones residentes sobre protocolos separados. Además en SIP los servidores no necesitan mantener el estado de la llamada. He aquí unas cuantas razones que hacen que SIP sea un protocolo superior a H.323:

- SIP desde su concepción fue diseñado para seguir el modelo de la Web basada en el protocolo HTTP. Como todos sabemos, son significativamente pocas las barreras y obstáculos para el desarrollo y despliegue de servicios innovativos cuando el control de la aplicaciones está ubicado en los Puntos-finales (esto está contraposición directa con el control de servicios del modelo tradicional del mundo de la telefonía, en donde los puntos finales carecen de capacidades de control y todos los servicios son controlados por un elemento de switcheo central).
- SIP es un protocolo abierto y escalable. Fue diseñado para ser un protocolo de propósito general. Entre las facilidades básicas de SIP, el protocolo también permite la movilidad personal proveyendo la capacidad para alcanzar a la parte llamada con una dirección única e independiente de su ubicación.
- Los proveedores de servicios de comunicaciones han visto en VoIP la forma de fusionar sus redes separadas de voz y de datos en una sola. SIP les ofrece un nuevo grado de escalabilidad, interoperabilidad y la facilidad para construir nuevos servicios y aplicaciones que se carecían antes con protocolos de VoIP más centralizados

Conclusiones

H.323 fue el primer estándar para el control y señalización de llamadas para VoIP. H.323 es un sistema híbrido que incorpora múltiples protocolos incluyendo Q.931 para la señalización, H.245 para negociación y RAS para el control de registro, admisión y estatus de la sesión. Está construido alrededor de Gatekeepers inteligentes centralizados, MCU's y Puntos-finales no tan inteligentes. Aunque el estándar H.323 se ha ido mejorando con el paso de sus diferentes versiones, problemas han aparecido, tales como tiempos de establecimiento de llamada muy largos, sobrecarga del protocolo ante conferencias, muchas funciones se requieren sobre cada Gatekeeper y problemas de escalabilidad en implementaciones donde los Gatekeepers realizan el ruteo de las llamadas.

Como respuesta a muchas de estas deficiencias y dificultades, protocolos como SIP está siendo actualmente desarrollados, y prometen ofrecer comunicaciones escalables y aplicaciones ricas y variadas. SIP es el protocolo de señalización de llamadas de la IETF para el establecimiento y administración de llamadas y conferencias multimedia en tiempo real sobre redes IP. Como protocolo IP basado en texto, se parece HTTP (Hypertext Transfer Protocol) y a SMTP (Simple Mail Transfer Protocol). SIP usa SDP (Session Description Protocol) para la descripción de los medios.

CAPÍTULO 4

CALIDAD DE SERVICIO

Si el servicio tradicional de entrega de paquetes "Best Efford" de las redes IP ha trabajado tan bien, por qué ahora deberíamos cambiarlo?

*La Internet ha recibido varias etiquetas a lo largo del tiempo, desde las más optimistas, como "**Supercarretera de la Información**", hasta las más pesimistas, como "**World Wide Wait**". Siendo la Internet una colección tan impresionante de redes interconectadas a lo largo de todo el mundo y transportando una vasta cantidad de información hacia todas partes, quizá merezca el epiteto de supercarretera. Sin embargo, la mayoría de nosotros en algún momento dado ha sufrido de la **impredecibilidad** del servicio ofrecido por la Internet y es difícil negar que la segunda etiqueta también le sea bien merecida. Esta supercarretera de la información aparece a veces más bien como una calle congestionada que decide retardar o perder por igual los diferentes flujos de tráfico sin tomar en consideración las necesidades específicas de los mismos. La **Calidad de Servicio (QoS)** es un esfuerzo por minimizar este tipo de problemas.*

*La QoS se ha convertido en un factor crítico para el éxito en la transición hacia redes corporativas multiservicios. Sobre todo ahora después de la aparición de aplicaciones multimedia en tiempo-real (tales como la Telefonía-IP, la Videoconfencia-IP y las VPN's) que requieren un servicio de red predecible y seguro para poder operar satisfactoriamente. En este sentido, varios mecanismos han sido desarrollados a fin de proveer QoS sobre una red IP. Los más importantes son **Intserv** y **Diffserv**, aunque actualmente **MPLS** y otros desarrollos parecen estar tomando auge.*

4.1 Por qué Requerimos QoS

La Internet es una de las redes más grandes y exitosas en el mundo. Su éxito es evidente a la luz del crecimiento exponencial que ha tenido durante las últimas décadas. No es de extrañar entonces, que mientras la Internet y las intranets corporativas continúan creciendo, aplicaciones provenientes de otras redes de comunicación (tales como la PSTN) están incursionando en el mundo de la Internet y haciendo de las redes IP el punto de convergencia para todo tipo de aplicaciones (voz, video y datos). Podría decirse hoy más que nunca que la Internet se está convirtiendo en más de un sentido en la red de redes.

4.1.1 No es Suficiente con Aumentar el Ancho de Banda

Es de esperar que con la expansión constante de la Internet, derivada del incremento diario en cuanto al número de usuarios y aplicaciones, también su tráfico se esté incrementando constantemente. Ante esta circunstancia, cabría preguntar si es suficiente como antes con aumentar el ancho de banda de la Internet para satisfacer las demandas crecientes. Y con sorpresa encontramos que no, ya no es suficiente. El problema actual de la Internet está más allá de una simple cuestión de capacidad. La presencia cada vez más grande en la Internet en cuanto a aplicaciones multimedia en tiempo-real (que requieren de servicios de red específicos para poder operar satisfactoriamente), hace que su tráfico no solamente se haya incrementado en volumen, sino que también haya cambiado de naturaleza. Así pues, la Internet debe reformarse.

4.1.2 Necesidades Cambiantes de las Aplicaciones de Internet

Las nuevas aplicaciones multimedia (tales como la Telefonía-IP y la Videoconferencia-IP), caracterizadas en la mayoría de los casos por trabajar en tiempo-real, están exigiendo una mayor predecibilidad de la red en cuanto al tiempo de entrega de sus flujos paquetes a fin de poder operar satisfactoriamente. Hoy sin embargo, la Internet y las redes IP en general, sólo pueden ofrecer un servicio de entrega de paquetes tipo *"**Best Efford**"*, por el cual no hay garantía de que un flujo de paquetes sea entregado a su destino, ni predecibilidad alguna sobre el tiempo de entrega del mismo. Un servicio de entrega de paquetes tipo "***Mejor Esfuezo***" solo garantiza (o más bien promete) que una vez se conozca el destino último de un paquete, la red encontrará, si le es posible, un camino que le permita la entrega del paquete. El tiempo que le pudiese tomar lograr la entrega (retardo de transmisión) es en el mejor de los casos una cuestión secundaria; y si ningún camino estuviera disponible, el paquete podría ser descartado (un caso extremo de retardo).

Nota: si se requiriera de una entrega de paquetes garantizada contra la pérdida, los hosts fuente y destino (y no la red) pueden utilizar un mecanismo extremo-a-extremo adicional (por ejemplo, TCP) para determinar si los paquetes están siendo entregados satisfactoriamente y retransmitirlos en caso de pérdida.

Así pues, la Internet no garantiza una entrega expedita de paquetes, ni la preservación de su orden temporal de emisión. Su interés está por hoy dirigido a encontrar un camino ***hacia dónde*** enviar los paquetes (protocolos de ruteo) y no en ***cuándo*** enviarlos o ***cuánto*** le llevará entregarlos. Durante los primeros días esta era una práctica aceptable, ya que la totalidad de las aplicaciones no estaban diseñadas para trabajar en tiempo-real, y por lo tanto no eran sensibles al retardo o al jitter. Cuando las cosas empezaban a alentarse demasiado en una red había una regla de oro que lo resolvía todo: "***adicionar más ancho de banda cuando las cosas se empiecen a congestionar***", ... y dejar a las leyes aleatorias del multiplexado estadístico la compartición del ancho de banda disponible. Tan pronto como el ancho de banda a lo largo de cualquiera de los enlaces con problemas eran significativamente más grande que la carga de tráfico promedio, todos quedaban generalmente contentos.

Sin embargo, los tiempos han cambiado. Las Intranets corporativas y los backbones IP comerciales de los ISP están haciendo frente a las demandas por una mayor predecibilidad en el comportamiento extremo-a-extremo de sus redes. Estas demandas están motivadas como vimos por un amplio rango de factores, desde el crecimiento explosivo de las PC's que corren aplicaciones multimedia hasta corporaciones que intentan migrar sus aplicaciones de misión crítica (de voz, video y datos) hacia redes propietarias basadas en paquetes IP. Los ISP's grandes y medianos están sintiendo la presión de proveer niveles de servicio predecibles y garantizados sobre sus redes. Tan pronto como el e-commerce se convierta en una de las formas de compra privilegiadas de sus usuarios, los ISP estarán bajo una presión significativa para mejorar continuamente la calidad de servicio de sus propias redes (ya sea para ganar nuevos clientes o para mantener los clientes que ya se tienen).

4.2 Entendiendo Mejor a la QoS

Como con la mayoría de las cosas en la vida, es menester conocer o fondo la esencia y las diferentes aristas de un problema a fin de poder ofrecer una solución satisfactoria. Por otra parte, del enfoque de que se parta dependerá el alcance de la solución lograda. Así pues, vayamos hacia lo que realmente importa ... las aplicaciones.

4.2.1 Las Aplicaciones y su Poder de Movimiento

Al igual que ante la pregunta sobre qué PC se debe adquirir (cuánta RAM, qué poder de procesamiento, etc), son las aplicaciones de red a ser usadas las que determinan la red que necesitamos. Como resultado, son las aplicaciones las que en última instancia estimulan los avances en las redes. La Internet no es la excepción. Su naturaleza, capacidades y servicios están en función de lo que por ella fluye.

En las siguientes tablas se agrupan en varias categorías las diferentes aplicaciones que hoy corren en la Internet. Como veremos, varias cosas útiles pueden sacarse de esta información en relación a lo que necesitamos cambiar, variar o modificar en la red.

TABLA 4-1: Clasificación de los flujos de tráfico en términos de su predecibilidad.

TIPO DE TRÁFICO	DESCRIPCIÓN
Stream (corriente)	Muestran una entrega de paquetes predecible con una tasa de bits constante (CBR). Por ejemplo, aunque sus tasas frecuentemente fluctúan, los streams de audio y video son considerados CBR pues tienen un límite superior cuantificable.
Burst (ráfaga)	Muestran una entrega de paquetes impredecible por "bloques" con una tasa de bits variable (VBR). Aplicaciones como FTP mueven sus datos en bultos que pueden incrementar la tasa de datos hasta usar todo el ancho de banda disponible en la red (no teniendo un límite superior).

TABLA 4-2: Clasificación de las aplicaciones en cuanto a su sensibilidad al retardo.

TOLERANCIA AL RETARDO	TIPO DE ENTREGA	DESCRIPCIÓN
↑ Alta	**Asíncrona**	No tienen restricciones sobre el tiempo de entrega.
	Síncrona	Sensitivas al retardo en el tiempo, pero flexibles.
	Interactiva	Aun cuando los retardos pueden ser notados por los usuarios, no afectan adversamente la funcionalidad.
Baja ↓	**Isócrona**	Sensitivas al retardo en el tiempo al punto de que se afecta adversamente la funcionalidad.
	Misión Crítica	Retardos en la entrega impiden toda funcionalidad

TABLA 4-3: Sensibilidad de varios tipos de tráfico al retardo, jitter y pérdida de paquetes.

TIPO DE TRÁFICO	ANCHO DE BANDA	ESTILO TÍPICO	SENSIBILIDAD AL RETARDO	SENSIBILIDAD AL JITTER	SENSIBILIDAD A LA PÉRDIDA
Transferencia de grandes volúmenes	10-100 Mbps	Periódica, 2 partes	Baja	Ninguna	Baja
Transferencia de datos	< 1 Mbps	A ráfagas, 2 partes	Moderada	Ninguna	Ninguna
Voz y facsímil	8-64 Kbps	Variable, 2 o más partes	Alta	Alta	Baja
Multimedia (voz más imágenes)	> 384 para video	Variable, 2 o más partes	Alta	Moderada	Baja
Video en demanda	28.8 Kbps a 1.5 Mbps	Variable, 2 o más partes	Baja	Baja	Baja

Con mucho la Telefonía-IP es por hoy la aplicación clave. La presión que el mercado está haciendo por introducir la Telefonía-IP, no hace sino poner en evidencia las deficiencias de la Internet y acelerar la definición de estándares para un control dirigido del ancho de banda sobre las redes IP. Aunque es una aplicación multimedia, sus requerimientos de ancho de banda son relativamente modestos (cerca de 8 Kbps en cada dirección), así que el ancho de banda no es un problema. Son la latencia y el jitter lo que trae problemas a esta aplicación. Para la Telefonía-IP (así como para otras ***aplicaciones en tiempo-real y bidireccionales***) son los requerimientos de tiempo mucho más importantes que los de ancho de banda.

4.2.2 Parámetros de Performance

Cuando solamente el servicio Best Efford es requerido o esperado en la red, no se necesita tener mucho cuidado siempre y cuando la red enrute los paquetes adecuadamente. Sin embargo, cuando se requiere ofrecer QoS extremo-a-extremo, es menester conocer más acerca del comportamiento dinámico de la red. Como se desprende de las tablas anteriores, hay ciertos parámetros que pueden ser usados para caracterizar el performance dentro de una red.

- ***Ancho de banda*** → una aplicación que requiere de un servicio garantizado generalmente tiene ciertos requerimientos de ancho de banda, necesitando que la red le asigne un ancho de banda mínimo específicamente dedicado a ella.
- ***Latencia y Jitter*** → son manifestaciones de la respuesta temporal impredecible de la red (debidos a los retardos de serialización, propagación, procesamiento y encolamiento) y están en función a los cambios en los patrones de congestión.
- ***Pérdida de paquetes*** → podrían deberse a problemas de corrupción o de enrutamiento, mas casi siempre se deben a la saturación de los enlaces de salida y al agotamiento de los buffers de encolamiento.

4.2.3 Congestiones Transitorias

El problema en la impredecibilidad del servicio de entrega de paquetes "Best Efford" se manifiesta para las aplicaciones multimedia en tiempo-real y bidireccionales en la forma de latencia y jitter. La causa más significativa detrás de estas manifestaciones adversas son las "***congestiones transitorias***" que tienen lugar en los equipos de comunicaciones de la red (routers y switches) por los que va pasando un paquete hasta alcanzar a su destino.

Por lo general, el flujo de tráfico asociado a la Internet es a través de ráfagas. Luego, si varias de estas ráfagas convergen de manera simultánea sobre un mismo router (o switch) para ser enviadas a través de un mismo enlace de salida que no fue dimensionado para soportar tal carga, el router experimentará una congestión. Dicho de otra manera, cuando a un router arriban de manera simultánea más paquetes de los que inmediatamente puede entregar sobre un enlace de salida, todos los paquetes que intentan pasar experimentarán retardos adicionales (puesto que serán puestos en colas temporales para después ser enviados cuando haya oportunidad). Cuando la congestión es muy severa o prolongada algunos paquetes podrían

empezar incluso a ser descartados (pues podría no haber espacio ya en las colas o buffers de espera).

Considérese por ejemplo el escenario de la Figura 4-1. Los paquetes arriban desde cada puerto de entrada a una velocidad máxima de Y1 a Yn paquetes por segundo (pps). Llevando a una entrada total de Y = Y1 + Y2 + ... + Yn. El enlace de salida extrae los paquetes a una velocidad de X pps. Cuando Y es menor que X, los paquetes no necesitan ser retenidos en la cola. Sin embargo, es frecuente que por la naturaleza a ráfagas del tráfico Y sea más grande por momento que X. En tales casos, el número de paquetes P sobre la cola para un intervalo T puede expresarse como P = T(Y –X). Un paquete que arribe en este periodo T experimenta una latencia adicional de P/X segundos (puesto que el paquete debe esperar a que la cola drene los P paquetes ya en ella a una velocidad de X pps). Si el paquete arriba cuando la cola está completamente llena, el paquete no tiene a dónde ir y es descartado o tirado por el router. El jitter proviene del hecho de que las componentes de Y exhiben un comportamiento aleatorio debido a su llegada por ráfagas.

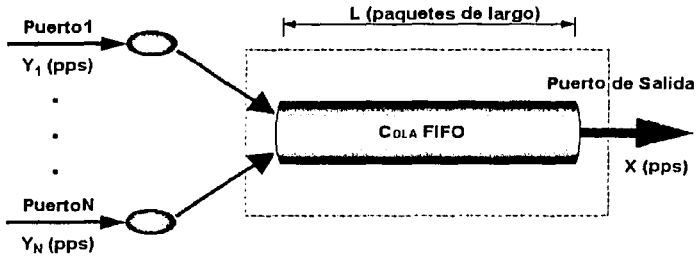


Figura 4-1: Encolamiento FIFO (First-in, Firdt-out) sobre un router Best Efford.

Hay varios factores a parte de los inherentes a la naturaleza propia de las redes IP, que podrían llevar a una congestión transitoria constante en una red:

- Excesivo uso.
- Horas pico.
- Ancho de banda insuficiente.
- Recursos de red insuficientes (memoria y procesamiento de los routers y switches).
- Mal diseño de red.
- Interferencia entre los diferentes flujos de tráfico (monopolización del ancho de banda).
- Uso inapropiado e indebido de los recursos de la red.

4.2.4 En Busca de una Solución

Puesto que no siempre es posible aumentar los recursos de la red a fin de resolver los problemas de tráfico de la misma, es necesario buscar otras soluciones. A este respecto, hay algunas observaciones que podrían dar luz en vísperas a encontrar una solución:

- ¿El efecto que sobreviene como consecuencia de la respuesta temporal impredecible de los routers ante congestión transitoria en la red, es el mismo para todas las aplicaciones?
- ¿Cómo tratan los routers a los diferentes flujos de tráfico de aplicación durante periodos de congestión transitoria ?

La idea detrás de estas preguntas es la necesidad de contar con routers capaces de diferenciar los diferentes flujos de tráfico de aplicación y servirlos de acuerdo a su prioridad relativa y/o a sus requerimientos de transmisión específicos (nivel de latencia, jitter, pérdida de paquetes, ancho de banda). Por supuesto que una de las premisas bajo esta nueva concepción es la de contar con mecanismos de encolamiento más sofisticados y eficientes que el sistema FIFO del servicio Best Efford. El procedimiento de registro en las aerolíneas para un vuelo es una analogía útil de lo que requieren hacer los routers a fin de proveer calidad de servicio a las aplicaciones en tiempo-real o ***"premium":***

> *En una aerolínea hay por lo general varios agentes que procesan los pasajeros tan rápido como les es posible, aunque a veces algunas aerolíneas podrían tener un número de clases de pasajeros para los que deben proveer un servicio de registro expedito. Para lograr esta meta, la aerolínea puede establecer múltiples colas, o líneas (una por cada clase de servicio del avión). La segregación de los pasajeros en distintas líneas (colas) permite a los agentes expedir un registro rápido a los clientes premium. El efecto neto es que los clientes premium experimentan un servicio de registro más rápido (es decir con menor latencia) y más predecible (menor jitter) que los clientes de una clase más económica.*

O expresado en términos de las redes de datos IP:

> *Para crear una Internet con capacidades de QoS, los diseñadores de red necesitan desarrollar routers capaces de clasificar los paquetes dentro de diferentes clases, encolar cada clase separadamente durante periodos de congestión y asignar niveles únicos de prioridad de procesamiento para cada clase. Con estas herramientas en mano, los diseñadores de red pueden empezar a controlar la latencia y jitter extremo-a-extremo experimentado por los clientes de clase premium.*

Sin embargo, proveer meramente una capacidad de diferenciación en el manejo de los paquetes dentro de los routers no es suficiente. Dos desarrollos adicionales se requieren antes de que una Internet con QoS se vuelva una realidad: ***la señalización y la contabilización***. En un sentido amplio, la señalización se refiere al establecimiento de mecanismos para la clasificación de los diferentes flujos de tráfico de aplicación, como de las reglas de servicio para los mismos a través trayectorias de red extremo-a-extremo. Adicionalmente, debe haber una contabilización sobre el uso de los recursos que cada quién hace, ya que ni la capacidad de los routers ni el ancho de banda de los enlaces son libres o ilimitados. El establecimiento de prioridades en el servicio para algunas clases de tráfico implica que otras clases serán penalizadas en forma conmensurable. Sin mecanismos para contabilizar y controlar el uso de los clientes para las diferentes clases de tráfico, cualquiera pediría el servicio premium, llevándonos de regreso al punto de donde partimos.

La contabilización de los recursos tiene dos componentes. Primero, las solicitudes para obtener los recursos de red requeridos deben ser autenticadas (a fin atender a las solicitudes legitimas y proteger al sistema contra intentos maliciosos por enajenar el proceso de asignación de recursos). Segundo, la utilización real de los recursos por parte de los usuarios deben ser monitoreados, seguidos y posiblemente autenticados (para asegurar que un paquete que está usando los recursos solicitados por un usuario específico provenga efectivamente de tal usuario). Finalmente, los proveedores de servicio utilizan la información de contabilización para generar los recibos de cobro para sus clientes de acuerdo a lo consumido.

4.2.5 Qué Debemos Superar

Las debilidades que las redes IP deben superar antes de que se pueda ofrecer QoS, pueden resumir en los siguientes puntos:

- *Los routers proveen una respuesta temporal impredecible ante congestiones transitorias en la red.*
- *Inhabilidad para proveer una prioridad en el servicio ante diferentes clases de tráfico.*
- *Inhabilidad para solicitar o modificar dinámicamente la calidad de servicio extremo-a-extremo.*
- *Mecanismos limitados para auditar el uso de los recursos de la red.*

Los siguientes son algunos de los beneficios y oportunidades que vienen de la mano con la introducción de QoS en una red IP:

- *Permite a las redes proporcionar los requerimientos de QoS adecuados a las aplicaciones existentes y emergentes (tales como la Telefonía-IP).*
- *Da el control sobre el uso de los recursos de una red al operador de la misma.*
- *Provee un servicio de entrega garantizado y diferenciado a través de una red. Lo cual es necesario para que se de la convergencia de la voz, video y datos en las redes IP.*

- *Permite a los ISP's proveer servicios premium junto con el servicio normal. Un proveedor podría entonces ofrecer toda una nueva gama de niveles de servicio al cliente (tales como Platinium, Gold, Silver y Bronze), y configurar su red para diferenciar el tráfico de acuerdo a las diferentes clases.*
- *Juega un rol esencial en los nuevos servicios de ISP ofertados, tales como las VPN's (Virtual Private Networks).*

4.3 Servicio Predecible Por-Salto

La habilidad para caracterizar el comportamiento QoS borde-a-borde depende de la habilidad para caracterizar y controlar el comportamiento de los enlaces y nodos a nivel de red. La meta de un ambiente con QoS habilitada es permitir un servicio de entrega predecible para ciertas clases o tipos de tráfico sin importar que otro tráfico está fluyendo a través de la red en cualquier tiempo. Una expresión alternativa de esta meta es la creación de una red IP multiservicios donde el tráfico a ráfagas tradicional pueda compartir la misma infraestructura (routers, switches y enlaces) junto con un tráfico con requerimientos más rigurosos de latencia, jitter, ancho de banda y/o pérdida de paquetes. Sin importar si el interés está en una red ISP, red de acceso o red corporativa (o alguna combinación de todas ellas), el camino extremo-a-extremo seguido por un paquete de usuario es meramente una secuencia de enlaces y routers. Así, la atención debe estar inicialmente dirigida hacia la dinámica del comportamiento de desvío de paquetes de un router. Aunque un router tradicional está enfocado principalmente hacia dónde enviará los paquetes (haciendo decisiones de ruteo basado en la dirección destino de cada paquete y en la tabla de ruteo local), los routers para redes con QoS habilitada deben permitir controlar el cuándo enviar los paquetes.

4.4 Herramientas de QoS

Sin importar el tamaño y alcance de una red IP, la calidad de voz extremo-a-extremo lograda sobre una red de datos IP es tan buena como la calidad ofrecida por su enlace más débil. La QoS extremo-a-extremo en una red depende en último término de las características de QoS de los saltos individuales a lo largo de una trayectoria ruta dada. Por ejemplo, en la Figura 4-2 la QoS experimentada por una aplicación telefónica intra-LAN depende única y exclusivamente de la LAN, mientras que la QoS de una aplicación telefónica sobre la WAN depende de las LAN en cada extremo, de los ISP's y del backbone entre los ISP's.

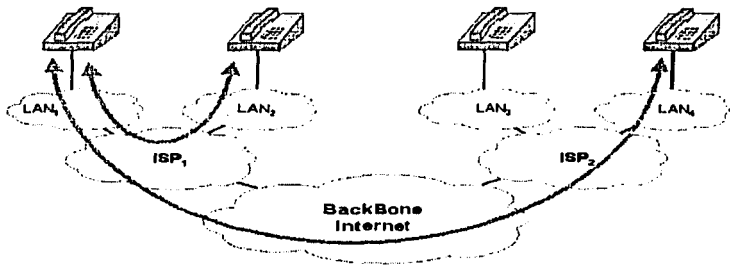


Figura 4-2: La QoS extremo-a-extremo depende de cada salto (LAN's, ISP's y Backbone).

La demanda por una protección relativa o absoluta de otro tráfico sobre cualquier segmento de red en particular. Estas demandas llevan directamente hacia tres requerimientos técnicos:

- ***QoS por-salto*** → los elementos QoS de control más pequeños sobre una red son el router y el switch. Estos nodos deben estar basados en una arquitectura que permita un encolamiento diferenciado y calendarización (scheduling) a ser aplicados en cada salto y sean capaces de utilizar apropiadamente las características de QoS de los enlaces intermedios (ATM, Frame Relay, Ethernet, etc).
- ***Ruteo e Ingeniería de Tráfico*** → cuando múltiples caminos existen a través de la red, distribuir el tráfico a través de estos caminos puede reducir la carga promedio y la rafagacidad a lo largo de cualquier camino. Esta práctica mejora la calidad de servicio aparente de una red porque cada router es menos propenso a tirar paquetes o introducir jitter. Mecanismos para descubrir e imponer un ruteo *no-shortest-path* son requeridos.
- ***Señalización y Aprovisionamiento*** → QoS por salto controlable y ruteo no-shortest-path son de poca utilidad si no son fácilmente manejables. Una solución práctica requiere algún grado de distribución automática de los parámetros de QoS y/o restricciones de Ingeniería de Tráfico hacia todos los nodos (switches y routers) en la red. La nueva información es distribuida siempre que un cliente imponga o cambie los requerimientos de QoS extremo-a-extremo (o borde-a-borde).

4.5 Esquema de Encolamiento CQS

La latencia, el jitter y la pérdida de paquetes sobre cualquier tipo de red llevan finalmente hacia mecanismos de QoS sobre los enlaces, hacia la utilización dinámica de colas y hacia el manejo de esquemas de encolamiento dentro de cada router.

Si la carga de la red excede la tasa de servicio, una sola cola como punto de congestión interna no es suficiente. En su lugar, se requiere una cola por cada clase de tráfico identificable con características de latencia, jitter y pérdida de paquetes independientes y únicas.

Cada una de estas colas debe tener sus propias políticas de descarte de paquetes (por ejemplo, diferentes umbrales más allá de los cuales los paquetes son aleatoriamente o definitivamente descartados). Por supuesto, las múltiples colas por interface de salida son inútiles sin un mecanismo para asignar los paquetes hacia las colas correctas. Es necesario contar con un método de ***clasificación*** que opere sobre y a la par del esquema de ruteo tradicional del próximo salto. Finalmente, las colas deben compartir la capacidad finita del enlace de salida al cual alimentan. Este requerimiento implica la adición de un mecanismo de ***scheduling*** (***calendarización***) para intercalar paquetes desde cada cola y, entonces, mediar el acceso al enlace de manera controlable y predecible.

Los requerimientos anteriores pueden resumirse diciendo que las redes con QoS habilitada requieren routers que puedan ***Clasificar, Encolar y Calendarizar*** (***CQS***) todo tipo de tráfico (ver Figura 4-3). Todo router con tales características se dice que sigue la arquitectura CQS.

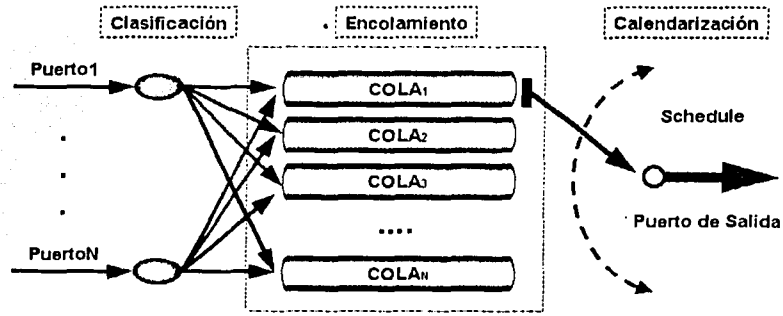


Figura 4-3: CQS permite un encolamiento y calendarización independientes.

En secciones posteriores de este capítulo se verán los diferentes métodos disponibles para clasificar tráfico, comparando sus complejidades relativas y la granularidad inherente con el cual cada esquema aísla diferentes clases de tráfico dentro de un flujo de paquetes. También se

evaluará los esquemas de encolamiento (la parte más importante de los cuales es la política de descarte de paquetes sobre la cola) estas políticas pueden ir desde el simple descarte de los paquetes que recién arriban cuando la cola ha alcanzado su límite (por ejemplo, cuando se ha quedado sin espacio) hasta es descarte aleatorio de paquetes recién llegados (basado en cuán cerca está la cola de cumplir ciertos atributos transportados por el paquete mismo). Finalmente, se considera los efectos temporales de los diferentes algoritmos de scheduling sobre la capacidad de la red para aislar diferentes clases de tráfico de otros.

Tal como se verá en las siguientes secciones, las arquitecturas de router CQS pueden implementarse en una variedad de combinaciones, cada una con sus características de QoS específicas sobre una red IP. La tarea de cada router bajo un esquema CQS es ahora:

- ***Saber dónde enviar un paquete (ruteo convencional).***
- ***Saber cuándo enviar un paquete (requerimiento de QoS adicional).***
- ***Completar las tareas anteriores independientemente de otros paquetes o tráfico sobre el router.***

4.5.1 Analogía (aerolíneas)

Un ejemplo del mundo real del esquema de encolamiento CQS está disponible desde la industria de las líneas aéreas:

Las áreas de registro (check-in) de un aeropuerto utilizan una arquitectura CQS para proveer diferentes niveles de servicio a diferentes clases de pasajeros. El punto de congestión es representado por un conjunto de agentes de registro quienes procesan los pasajeros tan rápido como les es posible y a una velocidad moderadamente constante. La velocidad del enlace de salida del punto de congestión es representada por la velocidad de atención de pasajeros de los agentes de registro (la aerolínea puede agregar o remover agentes para variar esta velocidad).

El arribo de los pasajeros que registran su salida para un vuelo dado es un proceso que tiene un carácter más bien aleatorio y por chorros (o ráfagas), alcanzando un pico típicamente durante la última hora antes del vuelo. La mayoría está familiarizado con las colas que se construyen durante el arribo repentino y simultáneo de un grupo de pasajeros.

Las líneas aéreas típicamente gustan de dar un servicio de registro expedito a sus clientes premium (por ejemplo, pasajeros de primera clase o aquellos que vuelan frecuentemente con ellos). Para hacer esto, varias líneas separadas (colas) son establecidas ante los agentes de registro. La clasificación de los pasajeros dentro de la cola apropiada puede hacerse de diferentes formas. Algunas veces las aerolíneas dejan que los mismos pasajeros vayan a la cola apropiada, mas en algunas otras ocasiones un representante dirige a la gente a la cola apropiada según la clase de sus tickets.

La acción de poner un pasajero en una de estas colas de registro representa una decisión de scheduling. Tipicamente, los agentes de registro están dedicados a cada cola (o clase de pasajeros) proporcionando una tasa mínima de atención a cada cola sin importar del bloqueo de cualquier otra cola. Para lograr un uso eficiente de los agentes, cuando una cola de alta prioridad se vacía, los agentes asociados usualmente empiezan a atender temporalmente pasajeros de colas de menor prioridad. Con la apropiada distribución de los agentes de registro, los pasajeros de clase premium experimentan un registro más rápido (menor latencia) y más predecible (menor jitter) que los pasajeros de clases más bajas.

4.6 QoS a Nivel de Enlace

Los mecanismos para ofrecer QoS sobre una red están disponibles también en algunas tecnologías de capa 2, tales como Frame Relay, Ethernet (802.1Q/p IEEE) y ATM. Siendo una tecnología orientada a la conexión, ATM ofrece un soporte fuerte de QoS y puede proveer una QoS garantizada por conexión, de hecho ATM es un ejemplo de arquitectura CQS.

Sin embargo, las tecnologías de capa 2 ofrecen una solución de QoS con alcances limitados y no pueden proveer QoS extremo-a-extremo, simplemente porque la Internet y las redes IP en general están hechas por una gran diversidad de tecnologías de capa 2. En una red, la QoS extremo-a-extremo es una tarea de la capa 3 y, por lo tanto, solamente el protocolo de red IP puede ofrecer una QoS extremo-a-extremo. No obstante, debe haber mecanismos a nivel de red que aprovechen las facilidades de QoS ofrecidas a nivel de capa de enlace.

4.7 Protocolos de QoS

Para soportar tráfico de aplicaciones de voz, video y datos con requerimientos de servicio variados, los sistemas en el core de la red IP necesitan diferenciar y servir los diferentes tipos de tráfico basado en sus necesidades. Las funciones de la QoS están destinadas a entregar servicios garantizados y diferenciados dando el control sobre el uso de los recursos de la red al operador. La QoS es un conjunto de requerimientos de servicio a ser cumplidos por la red a fin de transportar un flujo de tráfico.

Hay más de una forma de caracterizar a la QoS. Generalmente hablando, la QoS es la habilidad de una red (aplicación, host, switch o router) para proveer algún nivel de garantía sobre su servicio de entrega. Algunas aplicaciones son más estrictas que otras en cuanto a sus requerimientos de QoS (esto es, el ancho de banda, retardo/jitter, pérdida), por esta razón hay tres tipos de QoS disponibles en una red:

- ***Servicio Best Efford*** → proporciona una conectividad básica sin garantía sobre cuándo un paquete será entregado a su destino, aunque frecuentemente un paquete es descartado (tirado) solamente cuando la entrada de un router o el buffer de la cola de salida está sobresaturado. El servicio best efford realmente no es parte de la QoS porque ninguna servicio o garantía de entrega es hecha en el envío del tráfico. Este es el único servicio que la Internet ofrece actualmente.
- ***Servicio Diferenciado (Diffserv = Soft QoS)*** → en un servicio diferenciado el tráfico es agrupado en clases de acuerdo a sus requerimientos de servicio. Cada clase de tráfico es diferenciada por la red y servida de acuerdo a los mecanismos de QoS configurados para la clase. Este esquema de QoS es frecuentemente referido como ***suave*** (***soft***) porque, aun cuando haya mecanismos de QoS implementados, no garantiza por sí solo el servicio. Solamente diferencia el tráfico y permite un tratamiento preferencial de una clase de tráfico sobre otras sobre un dominio específico, pero quizá no sobre toda la trayectoria hacia un destino.
- ***Servicio Garantizado (Intserv = Hard QoS)*** → servicio que requiere que la red reserve los recursos necesarios para asegurar que cumplirá con los requerimientos de servicio para un flujo de tráfico específico. Este esquema de QoS es frecuentemente referido como ***duro*** (***hard***) porque requiere garantías rígidas de la red.

Estos tipos de QoS pueden ser aplicados a ***flujos de aplicación individuales*** o a ***flujos agregados***, entonces hay otra forma de categorizar a la QoS:

- ***Por Flujo*** → un "flujo" es definido como una corriente de datos individual y unidireccional entre dos aplicaciones (transmisor y receptor), identificada de manera única por la quintupla: dirección IP fuente y destino, puerto fuente y destino y protocolo de transporte.
- ***Por Agregación*** → una agregación es simplemente dos o más flujos. Típicamente los flujos tienen algo en común (por ejemplo, cualquiera de los parámetros de una quintupla, una etiqueta o prioridad, o información de autenticación).

4.8 Mecanismos y Funciones de QoS

A continuación se discuten algunos de los mecanismos o funciones usados para proveer QoS en una red IP. No hace falta decir que esta es un área donde la innovación es la norma:

- ***Clasificación y Marcación de Paquetes*** → *los routers sobre los bordes de una red con QoS habilitada, usan la de clasificación para identificar la clase respectiva para los diferentes flujos de tráfico basándose en uno o más campos del encabezado de TCP/IP. Entonces, la función de marcado es usada para colorear el tráfico clasificado estableciendo ya sea el campo IP-Precedence o el campo DSCP (Differentiated Services Code Point). Un ejemplo de una mecanismo con tal función es* ***CAR*** *(Commited Access Rate).*

- ***Administración de la Tasa de Tráfico*** → *los ISP's usan esta función para checar el cumplimientos del perfil de tráfico de un cliente, para lo cual miden (mediante un Token bucket) el tráfico proveniente del cliente y lo contrastan contra el perfil de tráfico asignado al cliente. El resultado de tal proceso es entonces pasado a la función de Traffic Shaping o Traffic Policing:*
  - ***Traffic Shaping*** → *permite a un cliente enviar su flujo de tráfico al ISP con una tasa salida constante de manera que su tráfico cumpla con las políticas de gestión de tráfico del ISP y éste pueda asegurar una entrega predecible. Esta función (de suavizar la emisión del tráfico para evitar situaciones de sobrecarga) está íntimamente relacionada con el esquema de encolamiento usado. Un ejemplo de una mecanismo con tal función es* ***GTS*** *(Generic Traffic Shaping).*
  - ***Traffic Policing*** → *permite tirar o descartar todos los paquetes que no cumplen con el perfil de tráfico. No pone en buffers el tráfico excedente, tirando de esta manera los paquetes que lleguen cuando la capacidad de emisión permitida es excedida. Un ejemplo de una mecanismo con tal función es* ***CAR*** *(Commited Access Rate).*
- ***Gestionar la Congestión*** → *se refiere a los diferentes esquemas de encolamiento CQS usados para manejar el envío de los flujos de tráfico sobre un enlace de salida (que pudiera empezar a congestionarse). Ejemplos son :* ***PQ*** *(Priority Queuing),* ***CQ*** *(Custom Queuing) y* ***WFQ*** *(Weighted Fair Queuing).*
- ***Asignación de Recursos*** → *una vez los diferentes flujos de tráfico han sido clasificados en clases, el* ***algoritmo de scheduling*** *determina que paquete es el siguiente en una cola. Cuán frecuentemente un flujo de tráfico es servido determina el ancho de banda o asignación de recursos para tal flujo. Esta función depende del esquema de encolamiento CQS usado.*
- ***Evitar la Congestión y Políticas de Descarte de Paquetes*** → *esta función permite a los routers detectar y evitar cualquier signo de congestión sobre un enlace, evitando de esta manera que las colas empiecen a saturarse y halla descarte de paquetes.* ***RED*** *(Random Early Detection) y* ***WRED*** *(Weighted Random Early Detection) son dos de los mecanismos frecuentemente usados para tal función.*
- ***Protocolo de Señalización de QoS*** → *permite que las aplicaciones señalicen a la red sus requerimientos de QoS por-flujo. El protocolo de reservación de recursos* ***RSVP*** *(Resource ReserVation Protocol) es un ejemplo de señalización de QoS en la red.*
- ***Policing routing*** → *es una función de QoS que permite al usuario cambiar el esquema de ruteo basado en el destino para rutear basándose en varios parámetros configurables de los paquetes. El ruteo QoS es un mecanismo de ruteo que toma en cuenta los requerimientos de QoS de los flujos a fin de seleccionar una ruta, para lo cual cuenta con algún conocimiento sobre la disponibilidad de los recursos en la red.*

- ***Control de Admisión*** → *permite prevenir el acceso no autorizado a los recursos de la red a flujos de tráfico sin los permisos o privilegios necesarios.*

4.9 Arquitecturas de QoS

Como hemos visto, el propósito de la QoS es proporcionar ***servicios de entrega garantizados y/o diferenciados*** a lo largo de la Internet o cualquier otra red IP. Los servicios garantizados y diferenciados proveen diferentes niveles de QoS, y cada uno de ellos representa un modelo o arquitectura para entregar QoS, como será visto en las siguientes secciones en las que se describen los modelos:

- ***Servicios Diferenciados (Diffserv).***
- ***Servicios Integrados o Garantizados (Intserv).***

4.10 Arquitectura Intserv: RSVP

Ante las deficiencias del viejo modelo servicio "Best Efford", la IETF establece en 1994 el "***Grupo de Trabajo Intserv***" cuyo propósito era desarrollar un modelo de servicio que estuviera a la altura con las necesidades de servicio de las nuevas aplicaciones emergentes de voz y video. Este modelo de servicios ampliados para la Internet pretendía proveer los medios para que las aplicaciones solicitaran a la red los recursos extremo-a-extremo que necesitaban para operar satisfactoriamente. Su propósito era dotar a la red de la inteligencia necesaria que asegurara un servicio de entrega garantizado extremo-a-extremo para las aplicaciones de usuario que lo solicitaran.

Como primer paso, el Grupo de Trabajo Intserv comienza su labor definiendo dos tipos diferentes de servicios en base a los requerimientos de las aplicaciones; y después pasa a diseñar el protocolo de red que soportará esos servicios. Los servicios que definió fueron:

- ***Servicio Garantizado*** → provee a las aplicaciones sensitivas al retardo y al jitter (tal como VoIP) un servicio de entrega predecible en el tiempo.
- ***Servicio de Carga Controlada*** → provee a las aplicaciones sensitivas a la pérdida de paquetes (tal como FTP) en la red un servicio de entrega con ancho de banda garantizado.

RSVP (Resource ReserVation Protocol) es el protocolo de señalización desarrollado por la IEFT para la arquitectura Intserv. RSVP permite a las aplicaciones de usuario solicitar a la red la reservación de los recursos necesarios por cada flujo (sesión). Tal como cualquier otro tráfico, RSVP depende del protocolo de ruteo en operación para enviar sus mensajes de control y establecer su conexión con recursos de red garantizados.

4.10.1 Operación de RSVP

RSVP reserva una porción del enlace de salida en cada router a lo largo del path de un flujo. El transmisor envía periódicamente mensajes PATH, los cuales describen el tipo de tráfico a ser enviado y los requerimientos de recursos necesarios para soportar el flujo de tráfico. Un receptor que recibe el mensaje PATH responde enviando un mensaje de reservación RESV hacia el Tx, yendo de regreso a través del mismo conjunto de routers por los que atravesó el mensaje PATH original. En cada router a lo largo del path, el mensaje RESV es procesado y la reservación es incorporada dentro del router (asumiendo que los recursos están disponibles para atender a la petición). Cuando el mensaje RESV alcanza al Tx, una reservación extremo-a-extremo es establecida. Los router pueden reducir los parámetros de QoS del mensaje RESV si la reservación no puede ser atendida.

4.10.2 Problemas de Escalabilidad de RSVP

RSVP al hacer reservación de recursos por cada flujo de tráfico de aplicación, sufre de ciertos problemas de escalabilidad en redes grandes, especialmente sobre la Internet, donde el número de flujos de tráfico pueden ser del orden de decenas o centenares de miles. He aquí unas de las desventajas que hacen a RSVP un protocolo devorador de recursos:

- Requiere muchos recursos de procesamiento y memoria en los routers.
- Requiere una cantidad substancial de información de estado para mantener una reservación sobre cada router a lo largo de la trayectoria de conexión.
- Es impráctico sobre una red grande donde la mayoría del tráfico tiene tiempos de vida cortos.

4.11 Arquitectura Diffserv

Como consecuencia de los problemas de escalabilidad de Intserv para ser desplegado sobre la Internet, en 1998 la IETF forma el ***Grupo de Trabajo Diffserv***, cuyo propósito era proveer una modelo de QoS escalable basado en la diferenciación del los flujos de tráfico mediante su clasificación en unas cuantas clases, con prioridades de servicio relativas entre las diferentes clases.

Diffserv es una arquitectura que provee el marco dentro del cual una red puede ofrecer a sus diferentes flujos de tráfico de aplicación un amplio rango de servicios de red, cada uno diferenciado con base al performance específico de transmisión (ancho de banda, latencia, jitter y pérdida de paquetes). Adicionalmente, se puede caracterizar un servicio en términos de la prioridad relativa de un flojo para acceder a los recursos de una red. Un flujo de tráfico de aplicación puede elegir el nivel de performance o prioridad que requiere simplemente marcando el ***campo DSCP*** del encabezado de sus paquetes con un valor específico. Este valor especifica el ***PHB*** (***Per-Hop Behavior***) que será dado al flujo de tráfico a lo largo de todo un ***Dominio Diffserv***.

La arquitectura de Diffserv es ilustrada en la Figura 4-4 y los dos principales bloques o mecanismos funcionales de Diffserv son mostrados en la Tabla 4-4. Aparte de estos dos bloques funcionales, la política de asignación de recursos juega un papel importante en la definición de las políticas de control de admisión, tasa de sobrereservación de recursos, etc.

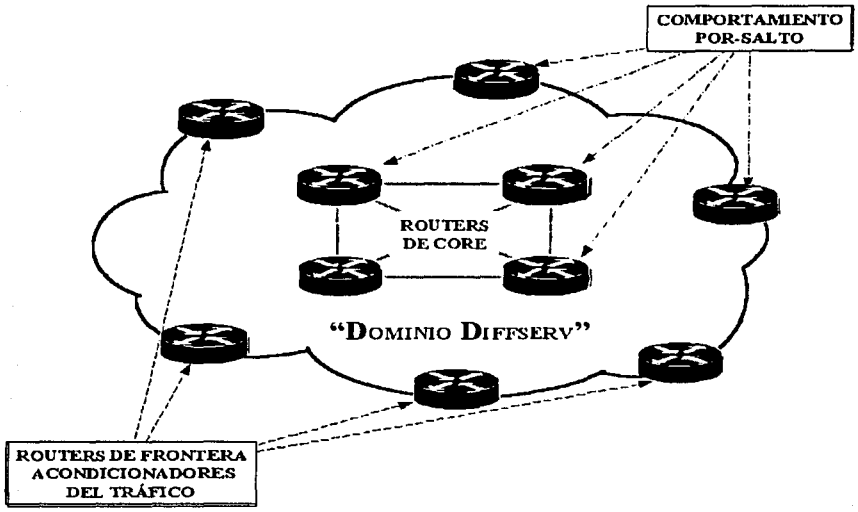


Figura 4-4: Arquitectura de Diffserv (router de frontera y de core).

Tabla 4-4: Bloques funcionales en la Arquitectura de Diffserv.

BLOQUE FUNCIONAL	UBICACIÓN EN LA RED	FUNCIONES	ACCIONES
Acondicionadores de Tráfico	*Sobre las interfaces de entrada al Domino Diffserv en los routers de frontera.*	• *Clasificación y marcación.* • *Traffic Shaping.* • *Traffic Policing.*	*Marcación de los paquetes con el DSCP correspondiente al perfil.* *Políticas y moldeado del tráfico entrada.*
PHB (Per-Hop Behavior)	*Sobre todos los routers en el Domino Diffserv.*	• *Asignación de recursos.* • *Esquemas de encolamiento CQS.* • *Política de descarte de paquetes.*	*Tratamiento o PHB aplicado a los paquetes basado en las características de servicio definidas por DSCP.*

El modelo operacional general de QoS es mostrado en la Figura 4-5.

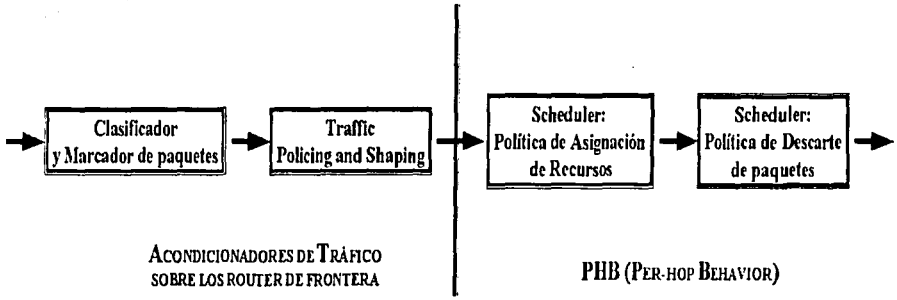


Figura 4-5: Modelo operacional general de QoS.

4.11.1 Servicios y PHB

Los nodos de red (routers, switches o host) que Diffserv habilitado usan el campo ***DSCP*** (***Differentiated Services Code Point***) del encabezado IP para seleccionar un PHB específico para un paquete. Un PHB es el tratamiento o servicio de envío externamente observable que cada nodo de un Domino Diffserv da a todos los paquetes que transportan un mismo valor DSCP.

Un flujo de tráfico que requiere un nivel de servicio específico transporta un valor DSCP apropiado en cada uno de sus paquetes. Se puede definir un PHB en términos de su prioridad relativa con respecto a otros PHB, o con relación a algunas características de servicio de tráfico observables, tales como la latencia, el jitter o la pérdida de paquetes. Los PHB's son aplicados por los acondicionadores de tráfico sobre los puntos de ingreso de la red (bordes de entrada) de acuerdo a políticas de tráfico predeterminadas. En las siguientes figuras se ilustra los campos DSCP y IP-Precedence de un paquete IP utilizados para clasificar los diferentes flujos de tráfico de aplicación:

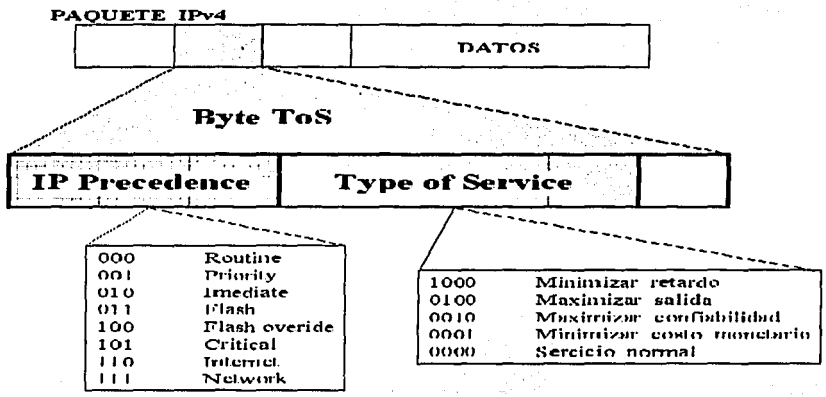


Figura 4-6: Campo Type of Service del encabezado de un paquete IP (RFC's 1812 y 1349).

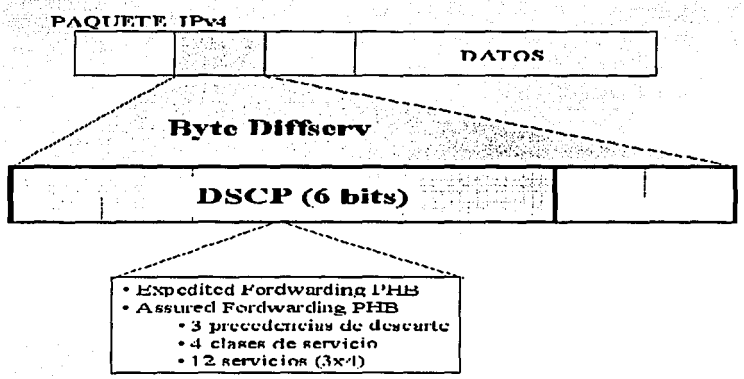


Figura 4-7: Campo Diffserv del encabezado de un paquete IP (RFC 2474).

Aunque Diffserv recomienda valores específicos de DSCP para cada PHB, el operador de una red pude elegir usar valores DSCP a los recomendados. El valor DSCP recomendado para el servicio Best Efford es 000000. Hay sin embargo, dos PHB's que están actualmente estandarizados:

- ***EF (Expedited Forwarding)*** → está destinado a aplicaciones en tiempo-real, tales como la Telefonía-IP
- ***AF (Assured Forwarding)*** → provee diferentes niveles de aseguramiento de envío a los paquetes basados en sus campos DSCP (tiene 4 clases y 3 precedencias de descarte por clase, para un total de 12 niveles de servicio, como se en la siguiente tabla).

PRECEDENCIA DE TIRADO	*CLASE #1*	*CLASE #2*	*CLASE #3*	*CLASE #4*
BAJA	*(AF11) 001010*	*(AF21) 010010*	*(AF31) 011010*	*(AF41) 100010*
MEDIA	*(AF12) 001100*	*(AF22) 010100*	*(AF32) 011100*	*(AF42) 100100*
ALTA	*(AF13) 001110*	*(AF23) 010110*	*(AF33) 011110*	*(AF43) 100110*

4.11.2 Acondicionadores de Tráfico sobre los Bordes de la Red

Los Acondicionadores de Tráfico juegan un papel crucial en la Ingeniería de Tráfico que tiene lugar en un dominio diffserv, de manera que la red pueda observar el PHB para todo el tráfico que entra a la red.

Son los routers ubicados sobre los bordes de una red con Diffserv habilitado los encargados de llevar a cabo la importante función de acondicionar el tráfico que entra al dominio Diffserv. Los bordes funcionan clasificando/marcando los diferentes flujos de tráfico ***coloreando el campo DSCP*** de acuerdo al PHB deseado, así como monitoreando que el tráfico entrante en la red cumpla con ciertos perfiles y políticas.

DSCP es el campo en el encabezado IP de un paquete que indica el PHB o tratamiento recibirá el paquete dentro de un dominio Diffserv. Las funciones principales de un Acondicionador de Tráfico pueden resumirse en los siguientes puntos (ver Figura 4-8):

- ***Clasificación*** → selecciona un paquete en base al contenido de alguna porción de su encabezado. Las formas más comunes de clasificar tráfico están basadas sobre el campo DSCP, pero pueden usarse otros campos (tales como la dirección fuente o destino; el puerto fuente o destino; o el campo de protocolo IP).
- ***Marcación*** → ayuda a escribir (rescribir) el campo DSCP de un paquete en base a su clase de tráfico.
- ***Medidor*** → checa el cumplimiento de un perfil de tráfico, basado sobre un descriptor de tráfico tal como un *token bucket*, y pasa el resultado a la función de marcación o al shaper o función de descarte para disparar una acción particular para los paquetes que cumplen o no con el perfil.
- ***Traffic Shaping*** → su función es retardar el tráfico en buffers para algunos paquetes de manera que se cumpla con cierto perfil de ingreso o egreso de tráfico a la red.
- ***Traffic Policing (políticas de descarte)*** → su función es tirar todo el tráfico que no cumpla con cierto perfil.

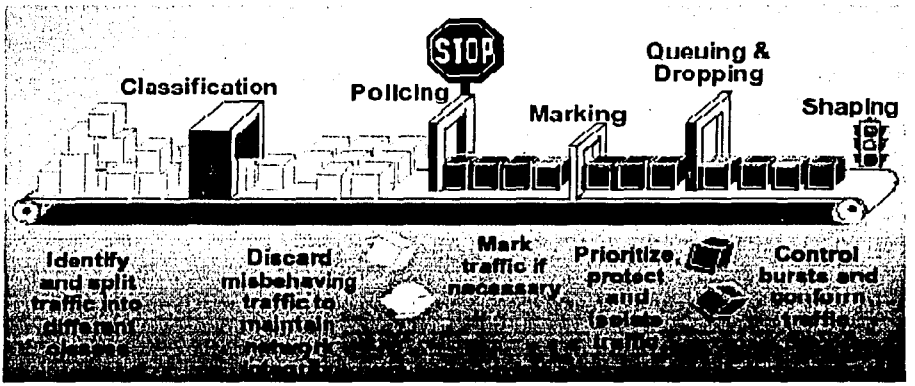


Figura 4-8: Funciones principales de un Acondicionador de Tráfico.

Conclusiones

El servicio tradicional de entrega de paquetes "***Best Efford***", que hasta hace poco había suficiente como inteligencia de red para los procesos de entrega que tenían lugar en la Internet, tiene que ser reformado ante el surgimiento de aplicaciones multimedia en tiempo-real (tales como la Telefonía-IP y la Videoconferencia-IP). Se requiere contar sobre las redes IP de un nuevo tipo de inteligencia (llamada ***QoS***) que les permita ofrecer ***predecibilidad en la entrega*** a los flujos de paquetes de las aplicaciones en tiempo-real y aislarlas de esta manera de los problemas de ***congestión en la red*** y efectos colaterales (***pérdida de paquetes, retardos y jitter***). En este sentido, hay varios esfuerzos que se están realizando a fin de proporcionar QoS a las redes IP. Los mecanismos de QoS más importantes con los que se cuenta actualmente son ***Intserv*** y ***Diffserv***, aunque algunos otros como ***MPLS*** están recién arribando y prometen ofrecer aún más, o colaborar con los anteriores en la búsqueda de una solución global.

CAPÍTULO 5

RED DE DATOS DE LA UNAM E INTERNET2

"Los problemas que enfrentamos hoy no pueden ser resueltos con el mismo nivel de pensamiento con que fueron creados"

Albert Einstein

El siglo pasado representó una enorme evolución en cuanto a las formas de ser y hacer de las sociedades en su conjunto a lo largo de todo el mundo, siendo la tecnología y su enorme progreso experimentado uno de los motores que estuvo detrás de todos estos cambios. El presente siglo promete cambios tan espectaculares como su predecesor, y sin lugar a dudas tanto la Teleinformática (entendida como la integración entre la Informática y las Telecomunicaciones) como la Biotecnología serán dos de las tecnologías que estarán detrás de este nuevo reto y con las que contarán las sociedades para competir en este mundo globalizado.

Es en este sentido que la UNAM (Universidad Nacional Autónoma de México), entendiendo el importante papel que representa la Informática y las Telecomunicaciones para encarar el presente siglo, se ha preocupado y ocupado en adecuar y renovar continuamente su infraestructura de Teleinformática a fin de estar a la altura de las exigencias cambiantes de su comunidad universitaria. Es por eso que hoy, en cuanto a Telecomunicaciones se refiere, la Universidad ofrece a usuarios una ***"Red Multiservicios de Alta Velocidad GigabitEthernet"*** *capaz de integrar todo tipo de información (voz, video y datos). Siendo su objetivo último, el establecer canales de comunicación que acerquen a la comunidad universitaria consigo misma y con otras instituciones, tanto a nivel nacional como internacional, permitiéndole el mejor desarrollo de su función educativa y de investigación.*

5.1 Red-UNAM

La ***Red de Telecomunicaciones de la UNAM*** (***Red-UNAM***) es una de las redes más grandes e importantes en América Latina. Esta red ha estado evolucionando a través del tiempo a fin de estar a la altura de las necesidades cambiantes de sus usuarios y cumplir con la función educativa de la Institución de mantener comunicados a sus investigadores, académicos y estudiantes dentro y fuera de la propia Universidad.

Es evidente y hasta esperado, que la evolución que ha experimentado la Red-UNAM a lo largo de los años haya ido de la mano con el desarrollo tecnológico observado en la Informática y las tecnologías de red y medios de transmisión. De hecho como veremos más a delante, la red de la UNAM tiende a integrar todo tipo de tráfico sobre una misma infraestructura de red, haciendo que la convergencia sobre una misma red multiservicios IP sea cada vez más evidente.

La evolución que ha tenido la Red-UNAM desde el año de 1986 a la fecha la podemos dividir en 4 etapas, según el backbone que la red del Campus de Cd. Universitaria ha tenido en cada momento:

- *Red de datos con un backbone basado en la tecnología Token Ring (1986).*
- *Red de datos con un backbone basado en la tecnología FDDI (1992).*
- *Red Integral de Telecomunicaciones con un backbone basado en la tecnología ATM (1997).*
- *Red Integral de Telecomunicaciones (o Red Multiservicios) con un backbone basado en la tecnología GigabitEthernet (2002).*

5.2 Backbone con Token Ring

Las principales características de esta red eran las siguientes (ver Figura 5-1):

- ***Backbone compartido*** constituido por un ***anillo Token Ring***.
- Presencia de *Bridges* (puentes) para segmentar la red a nivel capa 2 (dominio de colisiones) y no saturar al backbone.
- Redes locales Token Ring conectadas al backbone.
- Acceso de las estaciones de usuario a la red a través de MAU's (Multi-Access Units).
- No existían equipos que se encargaran del redireccionamiento interno de los paquetes (routers), puesto que el número de redes locales conectadas no lo ameritaba.
- No había aún una integración de las diferentes dependencias externas de la UNAM al Campus de Cd. Universitaria.

- La conexión hacia la Internet era hecha a través de enlaces satelitales hacia redes externas importantes en los EUA (como la red BitNet), ya que en nuestro país aún no había carriers con la infraestructura necesaria para soportar el servicio.
- Dadas las características de la red, era común que se presentaran fallas que afectaban el desempeño general de la red. Debido a esto, se vio la necesidad de migrar este esquema de red hacia otro que fuera mucho más confiable e incrementase el ancho de banda tanto en el backbone como en las redes locales.

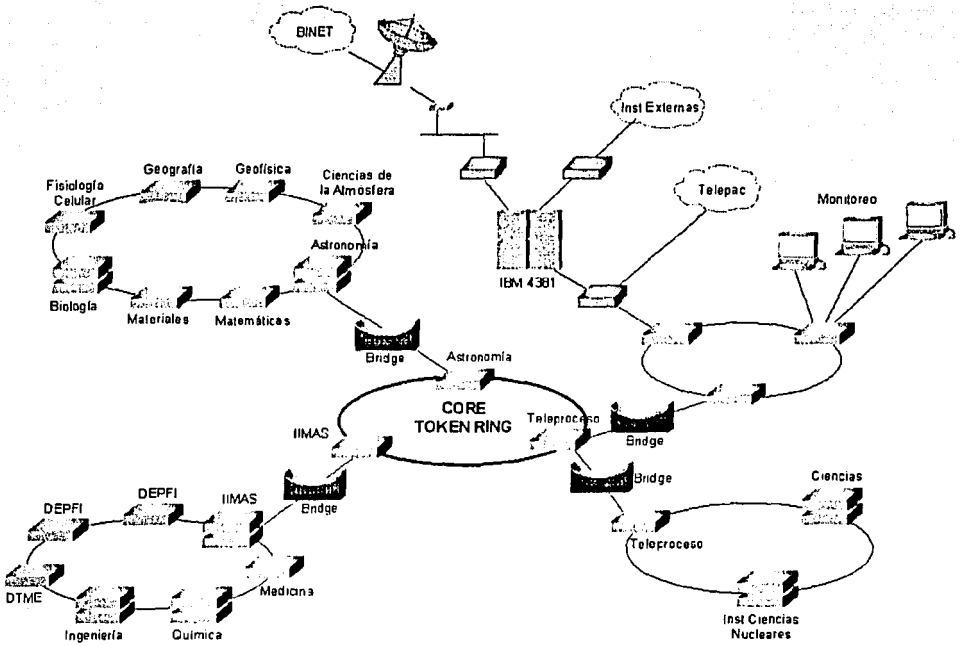


Figura 5-1: Red-UNAM con Token Ring como backbone.

5.3 Backbone con FDDI

Las principales características de esta red eran las siguientes (ver Figura 5-2):

- ***Backbone ruteado*** constituido por un ***anillo FDDI*** (*Fiber Distributed Data Interface*).
- El anillo FDDI estaba conformado por equipos de ruteo (Cisco AGS+) con alta densidad de puertos y mediante los cuales se lograba conectar a la mayoría de las redes locales de la Universidad (además de que segmentaba el *dominio de broadcast* de la red). La presencia de un switch (3com LANplex 2500) sobre el backbone brindaba una mayor velocidad de acceso a una de las redes locales más importantes por albergar a los nodos que proporcionaban los servicios de Internet más importantes para la comunidad universitaria e instituciones externas (servidor DNS, servidor de correo, servidores WWW de la UNAM, servidores FTP y Gopher, etc).
- En caso de que el backbone de FDDI llegase a presentar algún tipo de falla que impidiera la comunicación entre varios de sus nodos de core, existía un segmento Ethernet de respaldo. Con esta configuración se aseguraba la redundancia en la red a nivel global. En este segmento se encontraban siete ruteadores, cinco de los cuales también estaban conectados al backbone principal (de FDDI). Los dos restantes contaban con puertos que conectaban a las redes locales de la UNAM y a otras instituciones ajenas a la Universidad.
- Presencia de bridges y switches ubicados estratégicamente para segmentar el dominio de colisiones de algunas redes locales.
- El acceso de los usuarios a la red era generalmente a través de concentradores Ethernet (con coaxial grueso/delgado como medio de transmisión).
- Presencia de un anillo FDDI conectado al de backbone y que daba servicio a las computadoras de alto rendimiento del Depto. de Visualización y sobre las que investigadores de todo el campus podían realizar complejas simulaciones numéricas (mediante la Supercomputadora CRAY y varias estaciones de trabajo Silicon Graphics).
- Integración de todas las Dependencias de la UNAM externas al Campus de Cd. Universitaria (para recibir el servicio de datos y voz en algunos casos) mediante conexiones seriales punto a punto vía RDI, Microondas, Satélite o RadioMódems (Prepas, CCH's, ENEP's, Institutos de Investigación, etc)
- Conexión de Instituciones externas a la UNAM a través de enlaces seriales (con dos tipos posibles de conexión).
- Uso de routers con baja densidad de puertos (1 pto. Ethernet y 2 Seriales) (Telecom1 y Telecom3) destinados a la interconexión con Instituciones externas o carriers que proporcionaban acceso a la Internet.
- Esta red pretendía ofrecer una ***"Red Integral de Telecomunicaciones de la UNAM"***, sin embargo no logró serlo realmente.

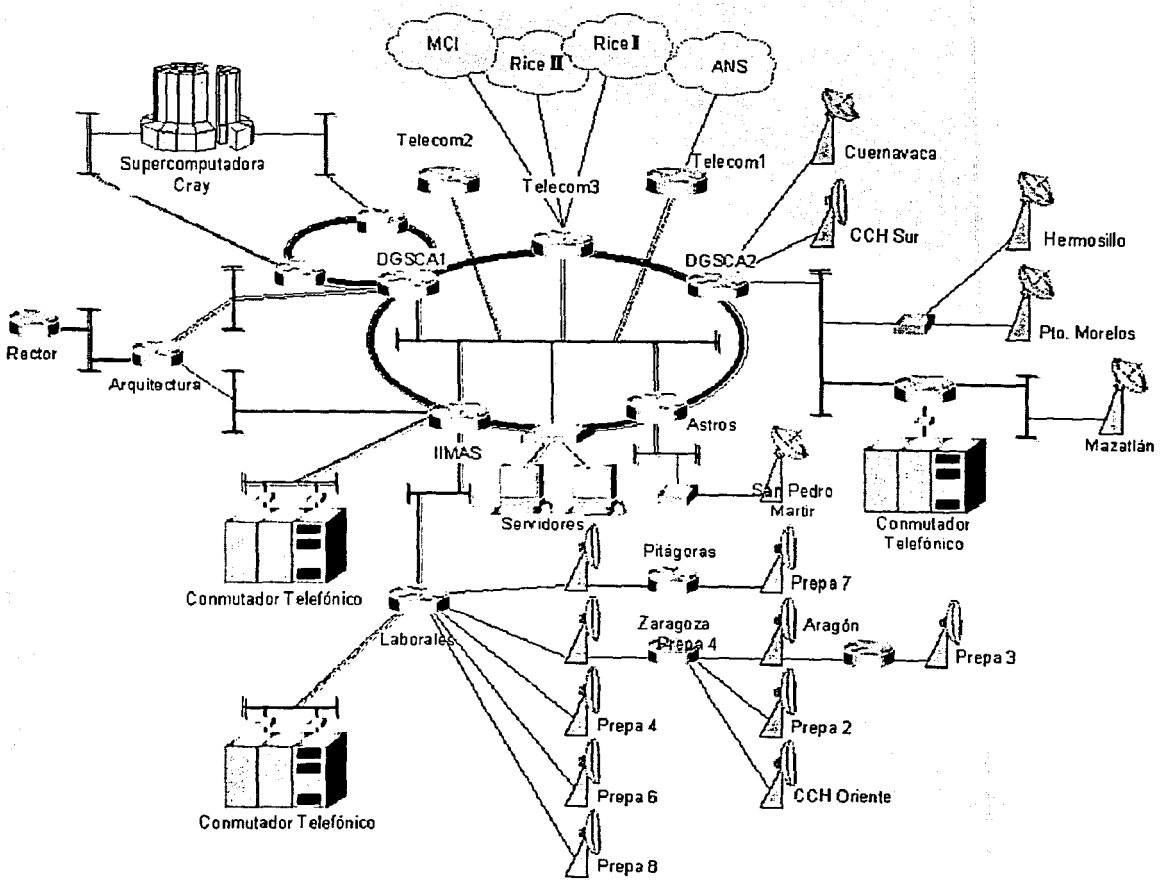


Figura 5-2: Red-UNAM con FDDI como backbone.

5.4 Backbone con ATM

Las principales características de esta red fueron las siguientes (ver Figura 5-4):

- Esta red fue diseña de manera tal que por primera vez fue posible transportar tráfico de voz, video y datos sobre una misma red dando lugar a lo que se dio por llamar "***Red Integral de Telecomunicaciones de la UNAM***".
- En paralelo a la creación de esta red, estaba el objetivo de integrar a todas las dependencias externas de la UNAM a través de su conexión a la red del Campus de Cd. Universitaria (que les ofrecía diferentes servicios de red, tales como la salida hacia la Internet y la conexión a la red telefónica universitaria).
- La red fue construida siguiendo un apago estricto a los cánones del buen diseño del ***modelo de arquitectura de red jerárquica***, es decir:

    - ***Core*** → Red ATM de alta velocidad (tecnología OC3 – 155 Mbps).
    - ***Distribución*** → Red FastEthernet (tecnología 100 Base-FX).
    - ***Acceso*** → Red FastEthernet o Ethernet (tecnologías 10 Base-FL / 10 Base-T).

- A diferencia del backbone anterior, éste era un ***backbone switcheado*** basado en la tecnología de ATM y *LAN-Emulation*.
- Al utilizar ATM como tecnología base en el backbone, se garantiza la calidad del servicio (QoS) de las aplicaciones de usuario final, al mismo tiempo que se permitía el transporte del tráfico de voz y video.
- A fin de lograr la integración, la red de backbone constaba en realidad de 2 cores, uno montado sobre el otro:

    - El primer core estaba conformado por una delta de switches ATM puros (Passports de la serie Magellan de Nortel) que se encargaban de transportar voz, video y datos. Los principales PBX's de la red telefónica se conectaban a esta red.
    - El segundo core estaba montado en paralelo sobre el primero y estaba constituido por 4 switches ATM (ubicados en DGSCA, Zona Cultural, IIMAS y Arquitectura respectivamente y conectados entre sí mediante enlaces en fibra OC-3 a 155 Mbps). Una característica de estos switches (Cellplex 7000 de 3Com) era el uso de LAN-Emulation para su interconexión con las redes de distribución y de acceso basadas en la tecnología Ethernet (100 Base-FX, 10 Base-TX). La función principal de este core era el transporte exclusivo del tráfico de datos. Ver Figura 5-3.

- La red de distribución estaba conformada por ***switches de capa 3*** (Lanplex 2500 o 3500 de 3Com) que se conectaban a la red de core mediante enlaces en fibra 100 Base-FX. Una de las habilidades de estos switches era su capacidad para segmentar la red mediante el concepto innovativo de las ***VLAN's*** (*LAN's Virtuales*). De hecho, los routers y switches de capa 3 estaban configurados para trabajar sobre una misma VLAN o segmento lógico, llamado ***VLAN de Administración*** (***red 132.248.254.0/24***).
- La red de acceso estaba compuesta por ***switches de capa 2*** (SuperStack 3300 o 1100 de 3com) que se conectaban a la red de distribución mediante enlaces en fibra 10 Base-FL o enlaces por cable UTP 10 Base-T.
- A fin de lograr una red de core y distribución de alta velocidad fue menester desplegar toda una red de fibra óptica a lo largo del campus universitario (fibra multimodo y monomodo).
- La Red-UNAM es una red heterogénea, ya que cuenta con equipos de diversos fabricantes, permitiendo la interoperabilidad entre los diversos proveedores de diferentes marcas; es escalable pues tiene la capacidad de crecer sin la necesidad de sustituir los equipos existentes; y es modular, ya que se puede actualizar hacia nuevas tecnologías con los mismos dispositivos.

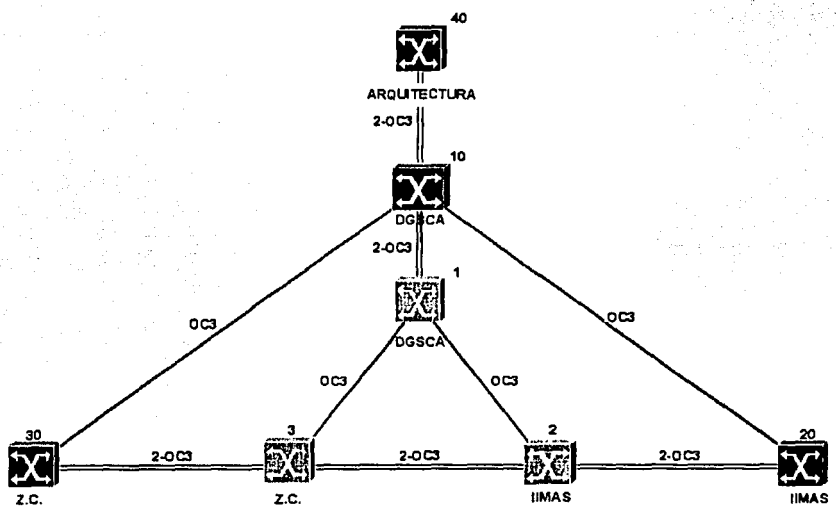


Figura 5-3: Backbone de la Red-UNAM mediante 2 cores ATM en paralelo.

- Los medios que hacen posible la comunicación hacia los lugares remotos son provistos mediante enlaces RDI (Red Digital Integrada), satelitales o de microondas.
- Para la comunicación con el exterior se contaba con una serie de routers distribuidos alrededor de la red que permiten que la información fuese transportada por el mejor camino hacia su destino, al igual que hacían posible la salida hacia la Internet mediante enlaces WAN externos E1's (2.048Mbps), o incluso por enlaces E3's (34.4 Mbps) ya hacia el final de sus existencia.
- Para la conexión hacia las diferentes dependencias externas de la UNAM, así como hacia empresas o instituciones privadas, era usual la utilización de enlaces digitales RDI a 64 Kbps (DS0) o 128 Kbps (2DS0), y en algunos casos se contaba con enlaces a 2.048 Mbps (E1) para las dependencias que requerían un mayor ancho de banda.
- IGRP y RIP son los protocolos de ruteo interno utilizados para comunicarse entre los routers del sistema autónomo; mientras que BGP es usado para la comunicación con los routers de otros sistemas autónomos (pertenecientes a otras Instituciones o a los carriers de la UNAM).
- La infraestructura de routers y switches de capa 3 de la red son multiprotocolos, es decir soportan: TCP/IP, IPX, NetBIOS y Apple Talk.
- En ese entonces la Red-UNAM abarcaba un número de 57 dependencias en Ciudad Universitaria y más de 80 instituciones externas en el D.F. o en el interior de la República, y con 6 enlaces satelitales. Ver Figura 5-4.
- Departamentos especialmente diseñados para mantener el funcionamiento de la Red-UNAM (NOC / TAC / NIC / Servidores / RAS).

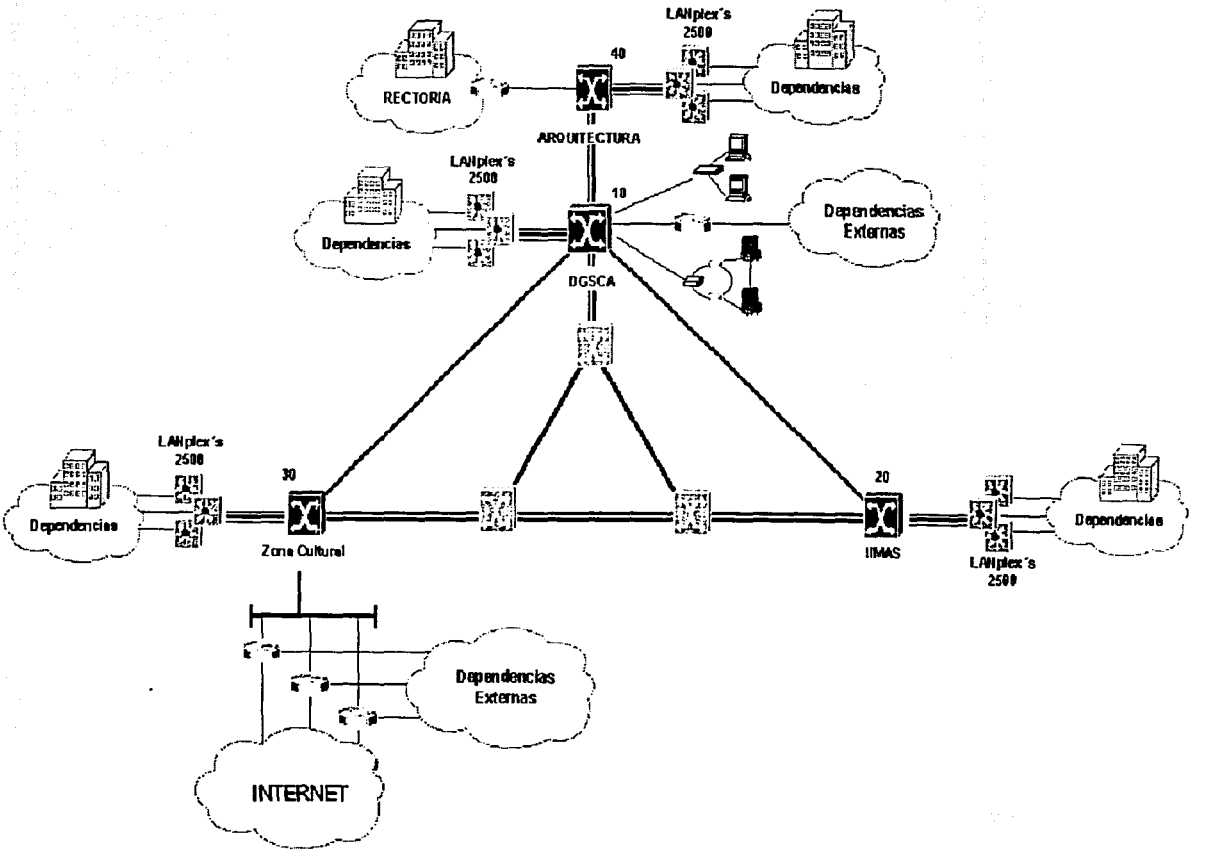


Figura 5-4: Red Core/Distribución/Acceso y Red WAN de la Red-UNAM

5.5 Backbone con GigabitEthernet

La estructura de la Red-UNAM bajo el backbone con GigabitEthernet está basada enteramente de acuerdo al esquema anterior con ATM, solo que los equipos de core tipo ATM-LANE así como la mayoría de los equipos de distribución fueron sustituidos por *SwitchRouters* con tecnología GigabitEthernet (1000 Mbps).

Las ventajas de esta nueva red son:

- ***Esquema de red jerárquico*** (core/distribución/acceso).
- ***Backbone Ruteado*** (los SwitchRouters de core realizan el ruteo del tráfico interno).
- ***Backbone full-mesh*** (malla total entre los SwitchRouters para mayor redundancia).
- Tecnologías de transporte:
  - GigabitEthernet sobre los equipos de core.
  - GigabitEthernet y FastEthernet sobre los equipos de distribución.
  - GigabitEthernet, FastEthernet y Ethernet sobre los equipos de acceso.
- Posibilidad de ampliar el ancho de banda de los enlaces de core o distribución mediante el uso de ***Trunkings en GigabitEthernet*** (o agrupación de enlaces) o usando la tecnología ***10-GigabitEthernet.***
- Uso de ***OSPF*** como protocolo de ruteo interno con las siguientes ventajas:
  - Menor tiempo de reconvergencia de la red ante un cambio en la topología de la misma.
  - Mejor uso del direccionamiento disponible mediante VLSM, CIDR y la Sumarización
  - ***Esquema de ruteo jerárquico*** (mediante el uso de áreas).
- Uso de ruteo estático hacia las dependencias externas.
- Uso de BGP como esquema de ruteo hacia los carriers (enlaces E3's – 34.36 Mbps) o hacia otros sistemas autónomos.
- Posibilidad para manejar Multicast sobre toda la red.
- Posibilidad de usar MPLS y otras tecnologías de QoS.
- Posibilidad de usar IPv6.
- Posibilidad para crear una red multiservicios (voz, video y datos).
- 3 enlaces hacia la Internet con más de 100 Mbps (3 x 34.36 Mbps)
  - E3 hacia UNINET (salida nacional).
  - E3 hacia AVANTEL (salida nacional).
  - E3 hacia TELEGLOBE (salida internacional).
- Red Multiprotocolo (TCP/IP, SPX/IPX, Apple Talk).

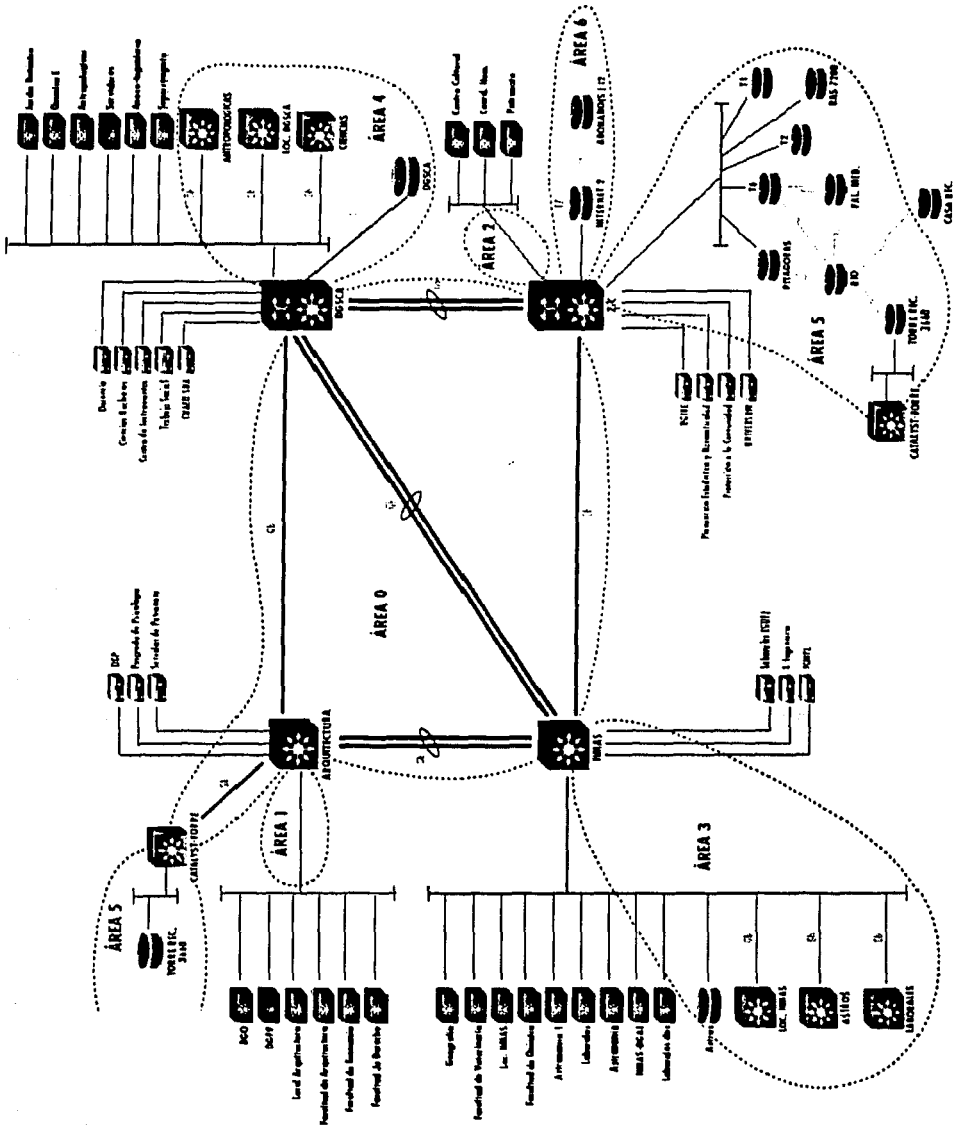


Figura 5-5: Red Core/Distribución/Acceso y Red WAN de la Red-UNAM actual.

5.6 Internet-2 México

La UNAM junto con varias Universidades e Instituciones más a lo largo y ancho de todo el territorio mexicano, han estado trabajando desde 1999 en la implementación de una red multiservicios de alta velocidad en México que forme parte de la red internacional denominada ***Internet-2***. El objetivo de esta red es dotar a la Comunidad Científica y Universitaria de México de una red de telecomunicaciones que les permita crear toda una nueva generación de investigadores, dotándoles de mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología a nivel mundial.

Para tal efecto, se procedió en 1999 a formar un organismo que promoviera y coordinara el desarrollo de la Internet-2 Mexicana, el CUDI:

> *El 8 de abril de 1999 se oficializó en Los Pinos la constitución de la* ***Corporación Universitaria para el Desarrollo de Internet (CUDI),*** *con la presencia como testigos de honor, del presidente de la República, Dr. Ernesto Zedillo Ponce de León, y de los Secretarios de Educación Pública, Lic. Miguel Limón Rojas y de Comunicaciones y Transportes Lic. Carlos Ruiz Sacristán.*

Para el cumplimiento de su misión, el CUDI persigue los siguientes objetivos específicos:

- Promover la creación de una red de telecomunicaciones con capacidades avanzadas.
- Fomentar y coordinar proyectos de investigación para el desarrollo de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo enfocadas al desarrollo científico y educativo de la sociedad mexicana.
- Promover el desarrollo de acciones encaminadas a la formación de recursos humanos capacitados en el uso de aplicaciones educativas y de tecnología avanzada de redes de telecomunicaciones y cómputo.
- Promover la interconexión e interoperabilidad de las redes de los Asociados Académicos y de los Afiliados.
- Promover el desarrollo de nuevas aplicaciones que realice.
- Difundir entre sus miembros los desarrollos que realice.

Según los estatutos establecidos por el CUDI, las Instituciones o Universidades miembro podrán tener uno de los siguientes niveles de asociación según su función específica dentro de la asociación: **Asociados Académicos, Asociados Institucionales** o bien **Afiliados**. Los actuales miembros del CUDI en sus tres categorías son:

TABLA 5-1: Tipos de Membresías en el CUDI.

TIPO DE MEMBRESÍA	MIEMBRO	OBSERVACIONES
ASOCIADOS ACADÉMICOS	❖ Benemérita Universidad Autónoma de Puebla (BUAP) ❖ Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) ❖ Instituto Politécnico Nacional (IPN) ❖ Instituto Tecnológico de Estudios Superiores Monterrey (ITESM) ❖ Laboratorio Nacional de Informática Avanzada ❖ Universidad Autónoma de Nuevo León (UANL) ❖ Universidad Autónoma de Tamaulipas (UAT) ❖ Universidad Autónoma Metropolitana (UAM) ❖ Universidad de Guadalajara (UDG) ❖ Universidad de Las Américas Puebla (UDLA-P) ❖ Universidad Nacional Autónoma de México (UNAM) ❖ Universidad La Salle (ULSA) ❖ Universidad Veracruzana (UV) ❖ Universidad Autónoma de Ciudad Juárez (UACJ) ❖ Universidad Autónoma del Estado de Hidalgo (UAE)	Universidades con proyectos avanzados de educación e investigación y redes de alta velocidad. Poseen los **Gigapops** (E3 – 155 Mbps)
ASOCIADOS INSTITUCIONALES	❖ Consejo Nacional de Ciencia y Tecnología (CONACYT) ❖ Teléfonos de México (TELMEX) ❖ Cabletron Systems S.A de C.V. ❖ Marconi Communications de México S.A. de C.V. ❖ Nortel Networks de México S.A. de C.V.	Patrocinadores oficiales
AFILIADOS	❖ Centro de Investigación Científico y de Educación Superior de Ensenada (CICESE) ❖ Instituto Tecnológico Autónomo de México (ITAM) ❖ Universidad Anáhuac del Sur (UAS) ❖ Universidad Autónoma de Chihuahua ❖ Universidad Autónoma de Coahuila ❖ Universidad Autónoma de Colima ❖ Universidad Autónoma de Tamaulipas ❖ Universidad Iberoamericana ❖ Universidad Tecnológica de México(UNITEC) ❖ Universidad del Valle de México (UVM) ❖ Colegio de la Frontera Sur ❖ Universidad Autónoma de la Laguna ❖ Instituto Latinoamericano de Comunicación Educativa ❖ Instituto Mexicano del Petróleo (IMP) ❖ Centro de Investigaciones en Geografía y Geomática (CENTRO GEO) ❖ Instituto de Investigaciones Eléctricas (IIE) ❖ Instituto Nacional de Astrofísica Óptica y Electrónica (INAOE) ❖ Sitara Networks, Inc ❖ Texas A&M University Center México ❖ Universidad Pedagógica Nacional (UPN) ❖ Universidad Autónoma de Sinaloa (UAS) ❖ Universidad Tecnológica de Puebla (UTP) ❖ Universidad Autónoma de Baja California (UABC)	Universidades interesadas en el avance tecnológico pero sin infraestructura de telecomunicaciones de alta velocidad. Poseen una acceso a la red mediante un E1

5.6.1 Topología y Descripción

El backbone de la red de Internet-2 Mexicana está formada por 4 SwitchesRouters ATM (Cisco BPX's) ubicados en la ciudades de México, Guadalajara, Monterrey y Tijuana conectados entre si por medio de enlaces SMT-1 (155 Mbps), como se muestra en la Figura 5-6 (se espera que en un futuro se agreguen 2 nodos más y que la malla entre ellos se cierre completamente).

Desde cada uno de estos nodos de core salen conexiones E3 (34.36 Mbps) hacia los diferentes nodos de distribución locales (mejor conocidos como ***GIGAPOP's***) y que dan servicio a los diferentes afiliados miembro mediante enlaces E1 (2.048 Mbps). La conexión hacia la red de Internet-2 internacional es lograda mediante enlaces que van hacia las redes Abilene y CalREN2 en EUA.

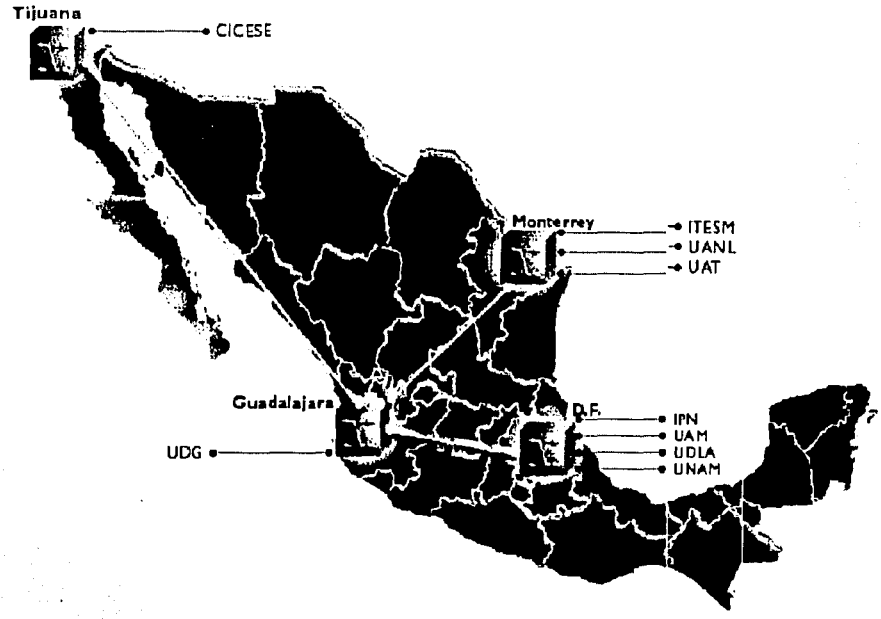


Figura 5-6: Backbone de la Red Internet-2 en México.

5.6.2 Aplicaciones y Grupos de Trabajo

Actualmente los diferentes asociados académicos de CUDI están trabajando en diferentes proyectos de investigación y desarrollo relevantes para la sustentabilidad de la red. Con este fin, se han formado grupos de trabajo que tienen que ver con algunos de los siguientes campos:

- IPv6.
- Multicast
- QoS.
- Seguridad en la red.
- Videoconferencia por H.323.
- VoIP mediante H.323 o SIP.
- Aplicaciones:
    - Educación a distancia
    - Bibliotecas digitales
    - Telemedicina
    - Supercómputo
    - Sistemas de información geográfica
    - Realidad virtual
    - Colaboratorios
    - Control a Distancia

En las Figuras 5-7 y 5-8 se muestra la estructura de la red a nivel core y distribución según el esquema de direccionamiento IPv4 o IPv6, respectivamente. Tan bien se muestra el esquema de ruteo BGP usado entre los diferentes sistemas autónomos.

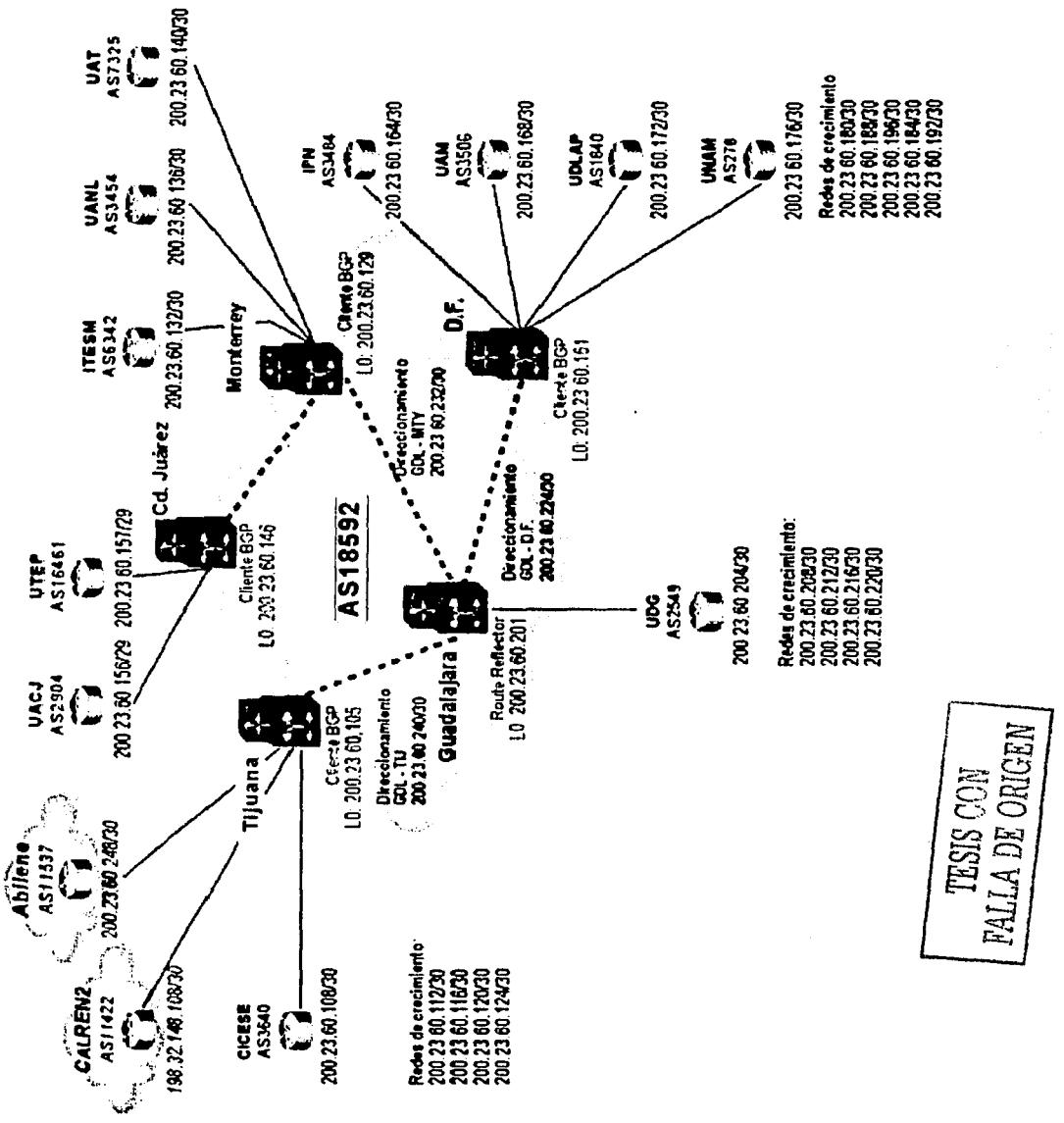


Figura 5-7: Nodos de Core y Distribución de la Red Internet-2 (direccionamiento IPv4).

Figura 5-8: Nodos de Core y Distribución de la Red Internet-2 (direccionamiento IPv6).

Conclusiones

En este capítulo se ha hecho un repaso breve a la evolución que ha experimentado la Red de Telecomunicaciones de la UNAM a través de los años. El objetivo es mostrar cómo la red a mejorado su servicio y desempeño conforme la tecnología en redes e informática ha mejorado, y entender por qué cada vez está más cerca el día en que las aplicaciones de voz, video y datos converjan sobre una misma red, la Red Multisevicios IP de Alta Velocidad. La Internet-2 representa en este sentido un esfuerzo internacional por recabar los elementos técnicos y tecnológicos necesarios para lograr esta meta, para después aplicar todo este bagaje de conocimientos en la Internet Comercial.

CAPÍTULO 6

PROYECTOS DE VoIP EN LA UNAM E INTERNET2

"Los retos de hoy no son sino la llave que abre la puerta hacia nuevas posibilidades"

*En el capítulo anterior hablábamos de la preocupación de la UNAM por adecuar y renovar continuamente su infraestructura de Teleinformática a fin de estar a la altura de las exigencias cambiantes de su comunidad universitaria. Es de esperar que hoy, después de que la Universidad ofrece a usuarios una "**Red Multiservicios de Alta Velocidad GigabitEthernet (Julio del 2002)**", haya algunos proyectos que intenten aprovechar las ventajas y capacidades de esta red para integrar todo tipo de información (voz, video y datos).*

*Uno de tales proyectos es la implementación de las tecnologías de VoIP sobre algunas de las redes LAN en algunos Institutos o Facultades del Campus universitario. Sin embargo, aún cuando las tecnologías de VoIP presentes actualmente en el mercado ofrecen soluciones atractivas para algunos entornos específicos de trabajo (**Telefonía LAN**), éstas aún se encuentran en desarrollo y evolución. En este sentido, proyectos tales como el de la Internet2 en donde se pretende implementar una red internacional de VoIP, proveen a la industria, a las empresas y a las universidades la retroalimentación necesaria para el desarrollo de mejores estándares de VoIP (en cuanto a su funcionalidad, escalabilidad y portabilidad), así como los elementos para que una empresa decida o no implementar alguna solución de VoIP sobre sus instalaciones, y en dado caso, bajo que condiciones.*

6.1 Red Telefónica para Funcionarios

En Marzo del 2001, a propósito de la reestructuración de la Red de Rectoría, se implementó el primer sistema telefónico de VoIP en la UNAM. Este sistema tenía como objetivo establecer una red de voz a través de la cual los diferentes funcionarios colaboradores del Sr. Rector pudieran mantenerse comunicados de manera segura y confiable.

Los requerimientos que por ese entonces se tomaron en cuenta para la elección de algún sistema de voz para tal proyecto fueron los siguientes:

- ***Red privada*** → *la red debería ser de uso privado y exclusivo, además debería estar separada de la infraestructura de la red telefónica normal de la UNAM, aunque dado el caso, debería ser capaz de interactuar con aquella e incluso usar sus recursos para hacer llamadas hacia Telmex.*
- ***Red segura*** → *la red debería ser ante todo segura (no más intervenciones telefónicas no autorizadas, o dicho de otra forma "**no más pájaros sobre el alambre**"), hay que recordar que por ese entonces estaba aun reciente el término de la huelga que habría llevado a la UNAM a estar paralizada por más de un año, y que la inseguridad había quedado más que nunca a flor de piel.*
- ***Movilidad*** → *las oficinas de los funcionarios podrían encontrarse sin problema alguno sobre cualquier parte de la UNAM (es decir, dentro o fuera del Campus de Cd. Universitaria) y aún así recibir el servicio de voz.*
- ***Costo reducido*** → *la inversión en la red de voz (cableado, equipos, instalación y mantenimiento) debería ser relativamente baja.*

Aunque hubo varias soluciones voz que se tomaron en consideración para este proyecto, la solución que finalmente se decidió apoyar fue el sistema de ***IP-Telephony de Cisco Systems*** debido al cumplimiento satisfactorio de cualquiera de los puntos antes expuestos.

6.2 Reestructuración de la Red de Rectoría

Antes de comenzar a describir el sistema de Telefonía-IP implementado, es conveniente describir los alcances del proyecto completo de la ***"Reestructuración de la Red de Datos de Rectoría (LAN y WAN)"***. En general este proyecto abarcó los siguientes puntos (y que a la postre serían significativos para el mejor funcionamiento de la red de voz implementada):

- *Actualización del hardware de ruteo y switcheo de las diferentes localidades de la Red*
  - *Routers → Cisco serie 3600's, 2600's y 1700's.*
  - *Switches → Cisco Catalyst 6509 y 3524 (in-line power).*

- *Ampliación del ancho de banda de la mayoría de los enlaces WAN de la Red de Rectoría hacia enlaces E1's (2.048 Mbps).*
- *Aprovisionamiento del nivel de redundancia apropiado para la Red de Rectoría.*
- *Reestructuración de la red de cableado de la Torre de Rectoría (pisos 6 y 12).*
  - *Tecnología 10/100 Base-TX (cobre) → red de acceso hacia las PC's de usuario.*
  - *Tecnología 1000 Base-SX (fibra) → red de distribución hacia los switches workgroup.*
- *Implementación del sistema telefónico de VoIP para el séquito de funcionarios colaboradores del Sr. Rector, ubicados ya sea sobre la Red de Datos de Rectoría o sobre la Red de Datos de la UNAM en general.*

En la Figura 6-1 se ilustra la Red de Datos de Rectoría (LAN/WAN) y la Red de VoIP implementada. Nótese la presencia de IP-Phones tanto sobre la Red de Datos de Rectoría como sobre la Red de Datos de la UNAM.

6.3 Descripción de la Solución de Cisco

Tal como se mencionó anteriormente, la solución que finalmente se decidió apoyar para este proyecto fue el sistema de ***Telefonía-IP de Cisco Systems,*** el cual está basado sobre la infraestructura de red ***AVVID (Architecture for Voice, Video and Integrated Data)*** de Cisco. No está de más entonces hacer una breve descripción de la misma.

De los capítulos anteriores sabemos que la Telefonía-IP se refiere a la tecnología para la transmisión de comunicaciones de voz sobre una red de datos IP. La solución de Telefonía-IP de Cisco promueve una infraestructura de red única e integrada para la transmisión de tráfico de voz, video y datos. Esta solución permite a las empresas obtener los beneficios de las redes convergentes (como son el incremento de la productividad, la flexibilidad y la reducción de los costos de operación). La solución de Telefonía-IP de Cisco consiste de los siguientes cuatro componentes primarios:

6.3.1 Infraestructura

Los elementos que componen la infraestructura para la solución de Telefonía-IP de Cisco incluyen a los siguientes:

- ***Gateways*** → para la interconexión del sistema con la PSTN o con los PBX's empresariales heredados se hace uso de Routers de la serie 1750, 2600, 3600, 7200 o Switches Catalyst de la serie 6000 que poseen tarjetas de troncales analógicas (FXO's) o digitales (E1's).

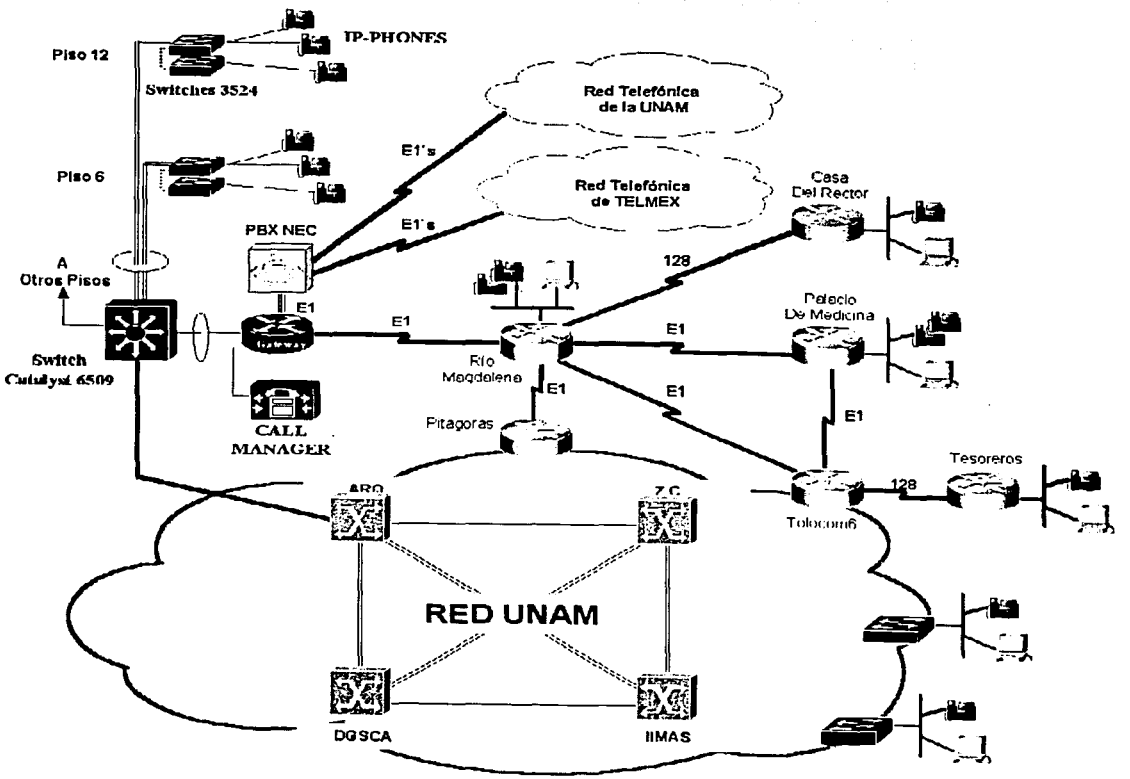


Figura 6-1: Red de Datos de Rectoria (LAN/WAN) y la Red de VoIP implementada.

- ***Switches In-Line Power*** → para proporcionar a los IP-Phones tanto la conexión a la red como la alimentación para su operación (aunque ésta también puede lograrse a través del uso de eliminadores de pared especiales). Ejemplos de Switches In-Line Power son los Switches de la serie 3500 o incluso los Switches Catalyst de la serie 6000 a través del uso de una tarjeta especial.
- ***Granjas de DSP's (Digital Signal Processors)*** → permiten el *transcoding* (es decir, la conversión entre diferentes códigos de compresión) y las switcheo de las conferencias de usuarios (*Conference bridging*). Ejemplos de equipos que brindan esta función son los Switches Catalyst de la serie 6000 a través del uso de una tarjeta espacial.

La infraestructura también incluye las interfaces y las facilidades necesarias para integrar PBX's heredados, correos de voz y sistemas de directorios.

6.3.2 Dispositivos Clientes

Los clientes para la solución de Telefonía-IP de Cisco son cualquiera de los dispositivos de usuario, ya sea un teléfono de escritorio (***IP-Phones***) o un teléfono simulado mediante un software aplicación que corre sobre una PC (***IP-SoftPhones***). Una característica de todos los teléfonos cliente es de que poseen una conexión Ethernet. Los IP-Phones proveen la mayoría de las funcionalidad y facilidades de un teléfono tradicional, así como facilidades más sofisticadas, tales como la habilidad para acceder a sitios Web.

6.3.3 Procesamiento de las Llamadas

El elemento central de la arquitectura distribuida del sistema Telefonía-IP de Cisco es el servidor de comunicaciones ***Cisco CallManager*** encargado de proveer los servicios de señalización y control de llamadas tanto a los clientes de Cisco como a clientes H.323 de terceros (este equipo según la nomenclatura de H.323 tiene las funciones de Gatekeeper.). El CallManager extiende las facilidades y capacidades telefónicas de una empresa hacia dispositivos telefónicos basados en paquetes tales como IP-Phones, SoftPhones, Gateways y aplicaciones multimedia. Servicios de datos, voz y video adicionales tales como Mensajería Unificada, Conferencia Multimedia, Contact Centres y Sistemas Multimedia de Respuesta Interactiva (IVR's) interactúan con la solución de Telefonía-IP a través API's (Application Programming Interfaces) sobre el CallManager. El CallManager es instalado sobre un ***Servidor MCS de la serie 7800*** (Media Convergence Server) o sobre un ***Sistema ICS 7750*** (Integrated Communication System).

6.3.4 Aplicaciones de Voz

Tal como las define AVVID, las aplicaciones de voz son físicamente independientes del procesamiento de llamadas o de la infraestructura de procesamiento de voz, y pueden residir en cualquier parte dentro de la red. Ejemplos de aplicaciones son la Mensajería Unificada, los Cantact Centres, los IVR's (Interactive Voice Response), la agregación automática a una conferencia, la respuesta ante una emergencia, el auto-attendant, etc.

6.4 Descripción de la Red Implementada

La Red de Telefonía-IP implementada para la Red de Funcionarios Colaboradores del Sr. Rector está constituida por un sistema de procesamiento de llamadas ***"Cisco CallManager (MCS 7850)"*** así como por la presencia de ***IP-Phones 7460*** y ***IP-SoftPhones*** distribuidos dentro y fuera de la Red de Datos de Rectoría.

Para la conexión del sistema hacia la Red de Telefonía de la UNAM (y por ende, también hacia Telmex) se usó un ***Gateway (Router Cisco 3640)*** con una ***interfaz E1 de voz***. Por otra parte, fue usado un ***Gateway (Router Cisco 1750)*** con ***interfaces FXS*** para conectar 2 teléfonos estándar remotos al sistema.

En las siguientes secciones se presentan algunos de los puntos involucrados en el diseño e implementación del sistema de Telefonía-IP instalado.

6.4.1 Componentes de la Red

Los elementos componentes de la Red de Telefonía-IP implementada para la Red telefónica de funcionarios, fueron:

- ***1 Cisco CallManager (MCS 7850) versión 3.0(11).***
- ***40 IP-Phones 7460.***
- ***Software y licencia*** *para el uso de IP SoftPhones sobre el sistema.*
- ***4 Switches Catalyst Cisco 3524 In-Line Power*** *para la conexión y alimentación de los IP-Phones ubicados sobre la Torre de Rectoría. Para el caso de los IP-Phones localizados externamente a la Torre de Rectoría se usaron eliminadores especiales para alimentar a los teléfonos.*
- ***1 Router Cisco 3640 con tarjeta E1 de voz*** *para la interconexión con el PBX NEC (NEAX-7400) perteneciente a la red telefónica de la UNAM.*
- ***1 Router Cisco 1750 con tarjeta FXS*** *para conectar dos teléfonos estándar ubicados en una localidad remota.*

6.4.2 Plan de Direccionamiento IP

El direccionamiento IP que se utilizó para numerar a los IP-Phones fue tomado del direccionamiento asociado a los segmentos de subred IP de la UNAM a donde se conectaban los IP-Phones. Aún cuando en algunos segmentos de subred se contaba con un servicio de DHCP, los IP-Phones se programaron para trabajar con direcciones estáticas.

6.4.3 Plan de Marcación

En el Plan de Marcación se define las extensiones asociadas al Sistema, los códigos para acceder a ciertas facilidades de usuario, así como la marcación que debe hacerse para interactuar entre el Sistema de Telefonía-IP y algún PBX de la UNAM o switch de Telmex:

- Extensiones de usuario → **100's**
- Extensiones para monitoreo y servicio → **300's**
- Marcación desde el Sistema de Telefonía-IP hacia la Red Telefónica de la UNAM usando la interfaz entre el Gateway H.323 (router 3640) y el PBX NEC (Neax 7400):
  - Extensiones del PBX → **20000's, 30000's y 40000's**
- Marcación desde el Sistema de Telefonía-IP hacia la Red Telefónica de Telmex usando la interfaz entre el Gateway H.323 (router 3640) y el PBX NEC Neax 7400:
  - Hacia Telmex → **9 + XXXX-XXXX, 9 + 01 + YY-XXXX-XXXX, etc**
- Marcación desde la Red Telefónica de la UNAM hacia el Sistema de Telefonía-IP usando la interfaz entre el Gateway H.323 (router 3640) y el PBX NEC Neax 7400:
  - Desde el PBX → ***8 + Extensión IP**
- Marcación desde la Red Telefónica de Telmex hacia el Sistema de Telefonía-IP usando la interfaz entre el Gateway H.323 (router 3640) y el PBX NEC Neax 7400:
  - Desde Telmex → **DID asociada a la Extensión IP (5622-85XX)**
- Códigos para ciertas facilidades:
  - Call-Pickup (tomar una llamada entrante desde otra extensión del grupo)→ **03**
  - Call-Parking (estacionar la llamada)→ **02**
  - Meet-me (agregarse a una conferencia preprogramada) → **01**

6.4.4 Transcoding y Conference Bridging

A fin de poder realizar las funciones de Transcoding (es decir, la conversión entre diferentes códigos de compresión) y las de switcheo para las conferencias de usuarios (Conference bridging), se instaló una tarjeta especial sobre el SwitchRouter 6509 la cual ofrece un Pull de DSP's.

6.4.5 Conexión y Alimentación de los IP-Phones

Para proporcionar a los IP-Phones tanto la conexión a la red como la alimentación para su operación, se usaron Switches Catalyst In-Line Power 3524 o eliminadores de pared para los casos en donde no se contara con tales switches. Se puso especial cuidado que las redes LAN a las cuales se conectaron los IP-Phones fueran en todos los casos switchadas y trabajaran con FastEthernet (100 Mbps). Por otro lado, se procuró usar el puerto FastEthetnet adicional presente sobre los IP-Phones para conectar la PC de usuario asociada.

6.4.6 Gateways en el Sistema

A fin de interconectar el Sistema de Telefonía-IP al la Red Telefónica de la UNAM se uso un Router Cisco 3640 (Gateway). El enlace que se utilizó para conectar el PBX NEC (NEAX 7400) al Router 3640 fue un E1 de voz (2.048 Mbps).

Se instaló también un Router Cisco 1750 con interfaces FXS para dar servicio a teléfonos estándar para una localidad remota de la Red de Rectoría.

6.4.7 QoS sobre los enlaces WAN

Sobre los enlace WAN de bajo ancho de banda se definió una estrategia de QoS mediante CQ (Custom Queing) a fin de prioritizar el tráfico de voz.

6.4.8 Seguridad

Se definieron algunas medidas de seguridad (tales como "Listas de Acceso" o filtros sobre algunos routers) para impedir que el CallManager fuera accesado por algún dispositivo de red ajeno a la Red de Telefonía-IP de Rectoría.

6.5 Configuraciones

A continuación se presentan las configuraciones hechas sobre los diferentes elementos perteneciente al sistema de Telefonía-IP, es decir:

- CallManager.
- SwitchRouter Catalyst 6509.
- Router-Gateways 3640 y 1750.
- PBX NEC (NEAX_7400).
- IP-Phones 7460.

6.5.1 Call Manager (MCS 7850)

La configuración más significativa realizada sobre el servidor de comunicaciones "Cisco Call Manager" se presenta en la siguiente serie de ilustraciones (obtenidas a través de la interface de administración http del sistema). Junto con cada ilustración acompaña una breve explicación del significado y función de cada una de ellas.

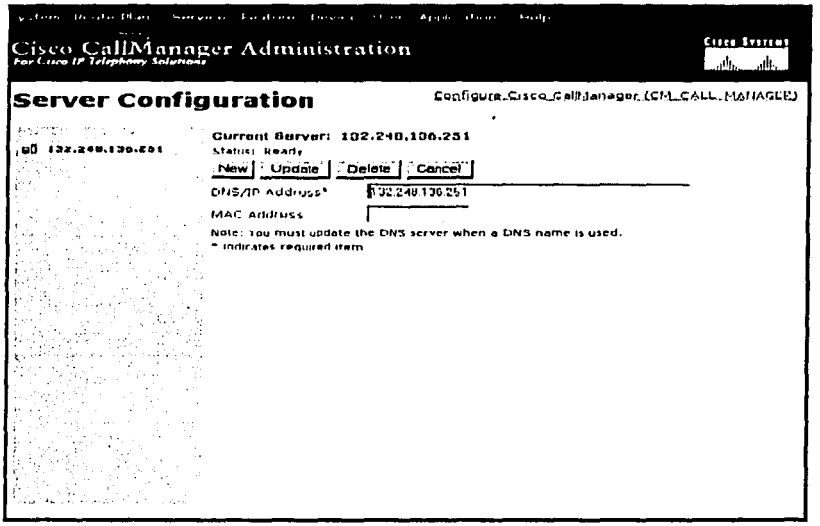


Figura 6-2: Define la dirección IP del servidor de comunicaciones CallManager. A tal dirección deberá recurrir un teléfono IP a fin de obtener la dirección IP de la extensión a la que desea llamar o la dirección IP de un router gateway.

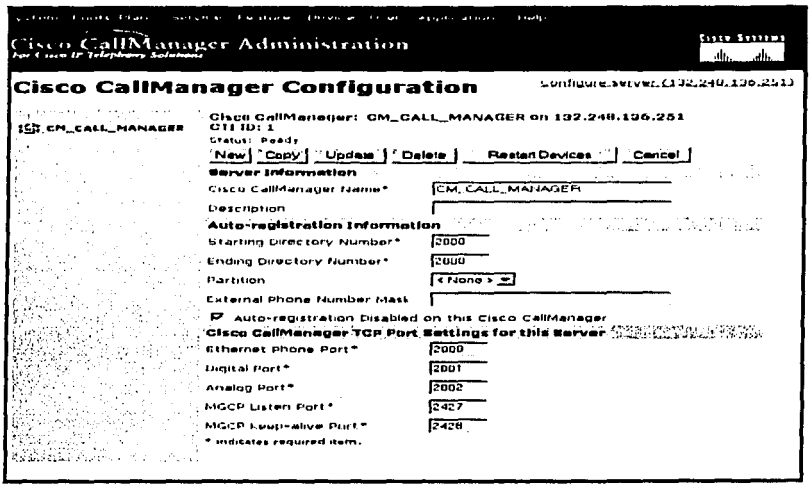


Figura 6-3: Define los puertos TCP que serán utilizados para la comunicación con el CallManager, así como el rango de números de extensión que un teléfono puede tomar en caso de que no se la haya asignado una extensión estática.

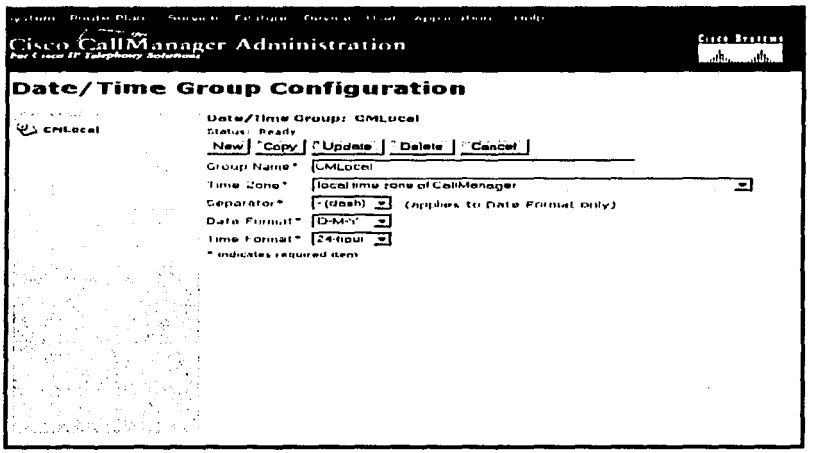


Figura 6-4: Define el formato de la hora y fecha que será vista en el display de los IP_Phones.

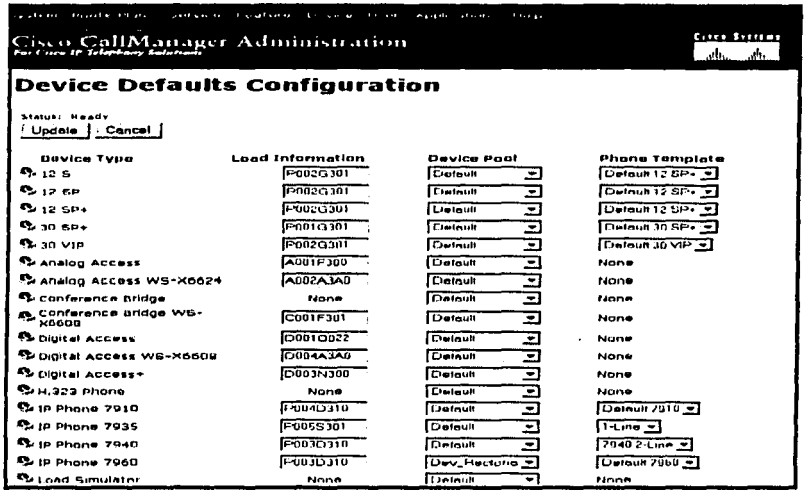


Figura 6-5: Define el software (o firmware) que por default estará operando sobre los diferentes dispositivos del sistema.

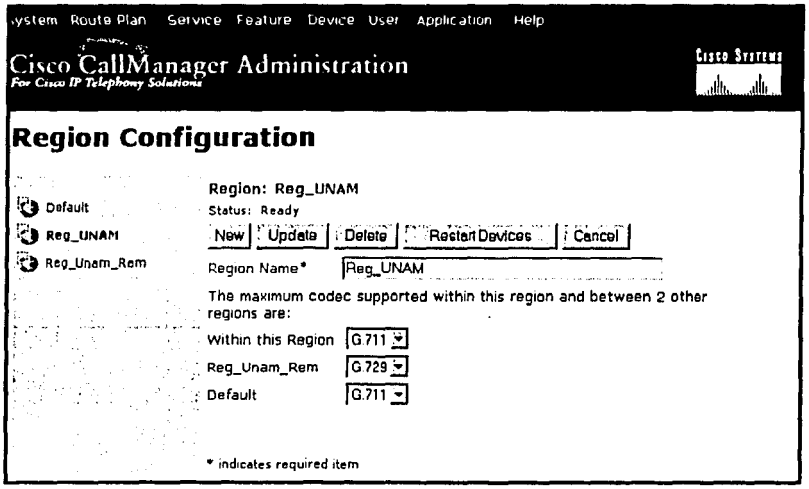


Figura 6-6: Define las diferentes regiones del sistema y los códigos de compresión que serán utilizados en la intercomunicación de una región con otra.

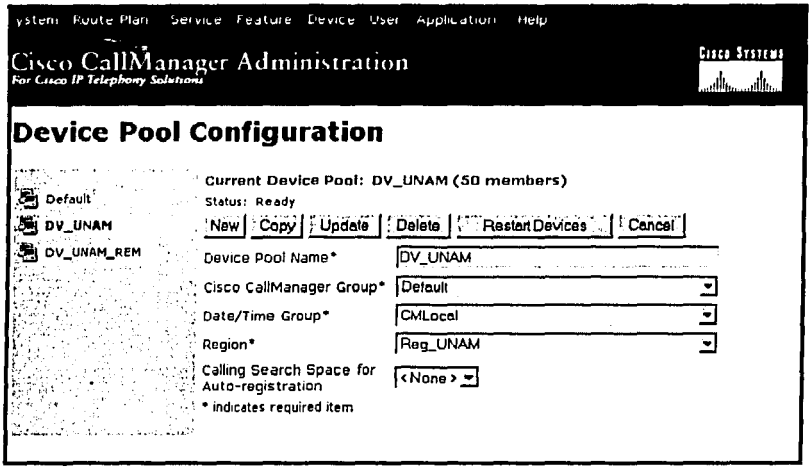


Figura 6-7: Define los diferentes pools de dispositivos posibles en el sistema y las características asociadas a cada uno de ellos. Todo dispositivo presente en el sistema tiene asociado un device-pool.

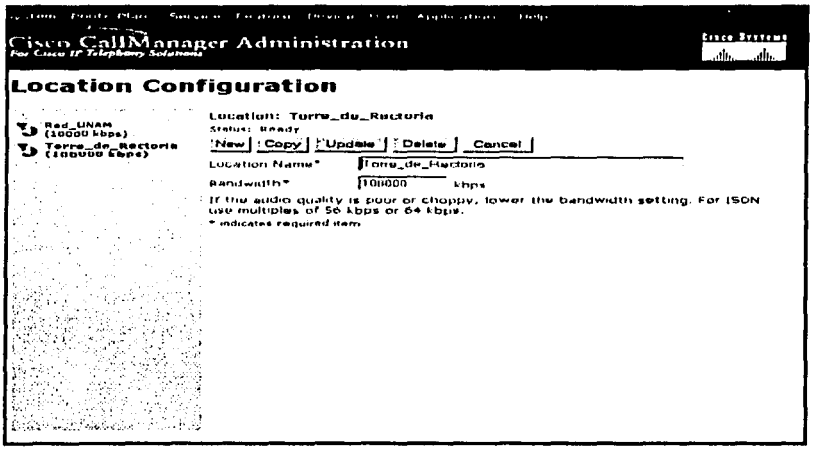


Figura 6-8: Define las diferentes localidades donde puede estar ubicado un IP-Phone o SoftPhone así como el ancho de banda asociado a cada una de estas localidades a fin de limitar el número de llamadas si fuese necesario.

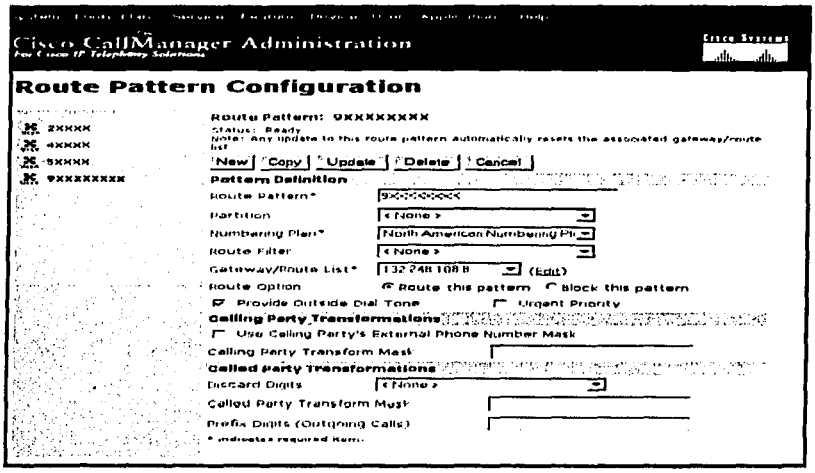


Figura 6-9: Define los patrones de marcación asociados a un sistema no-H.323 y que son accesados a través de un Gateway.

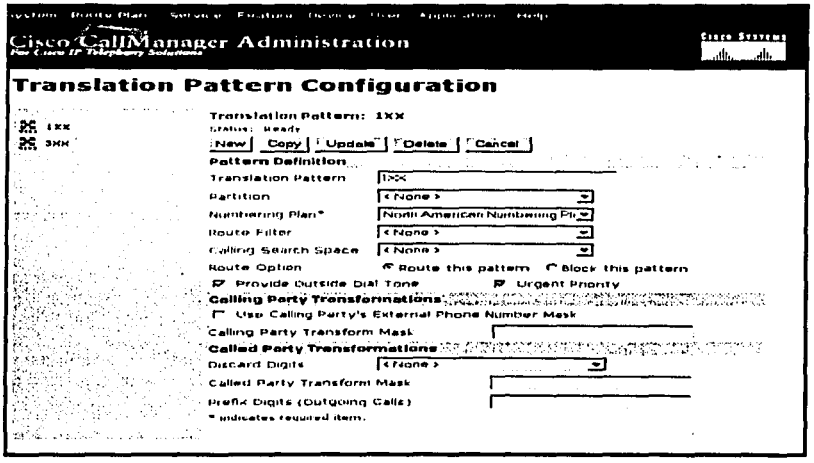


Figura 6-10: Define el rango de extensiones asociados al sistema y que pueden asignarse a los dispositivos H.323 presentes.

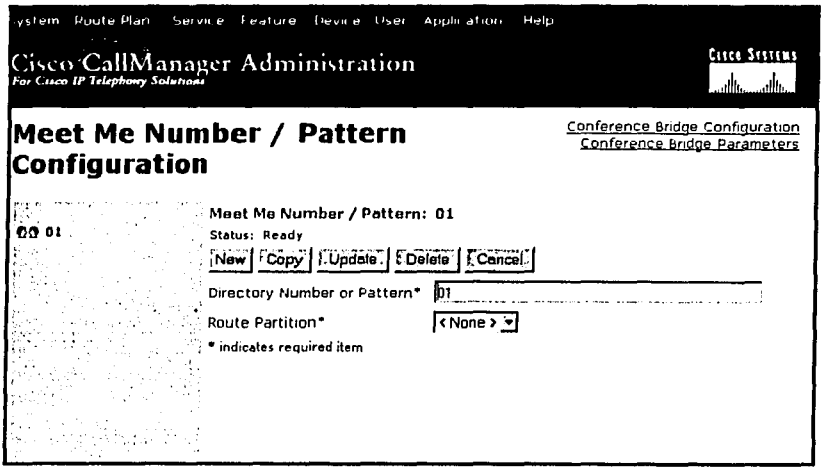


Figura 6-11: Define el código que los usuarios deberán marcar para agregarse a una conferencia programada.

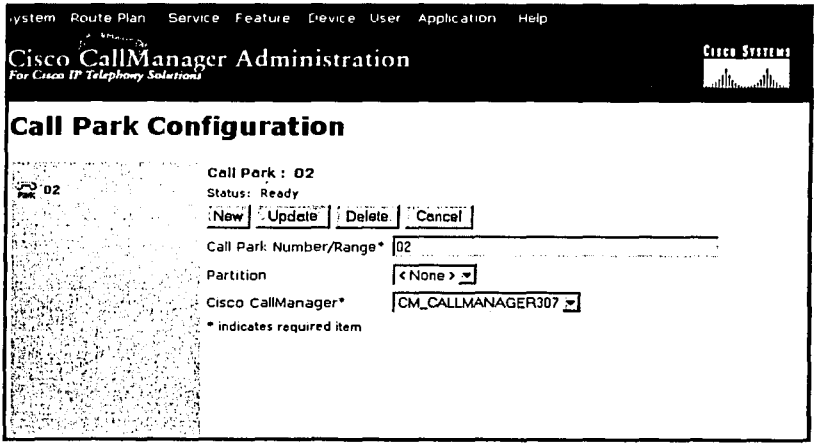


Figura 6-12: Define el código que los usuarios deberán marcar para parquear una llamada y retomarla en algún otro teléfono.

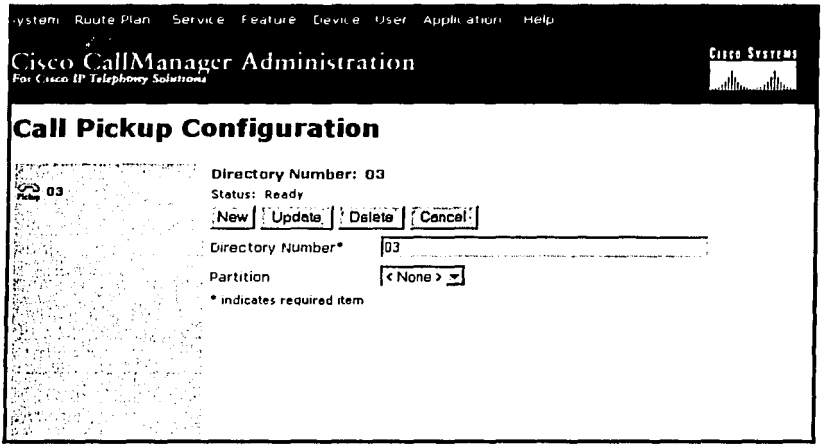


Figura 6-13: Define el código que los usuarios deberán marcar para jalar una llamada que está timbrando en algún otro teléfono de su grupo.

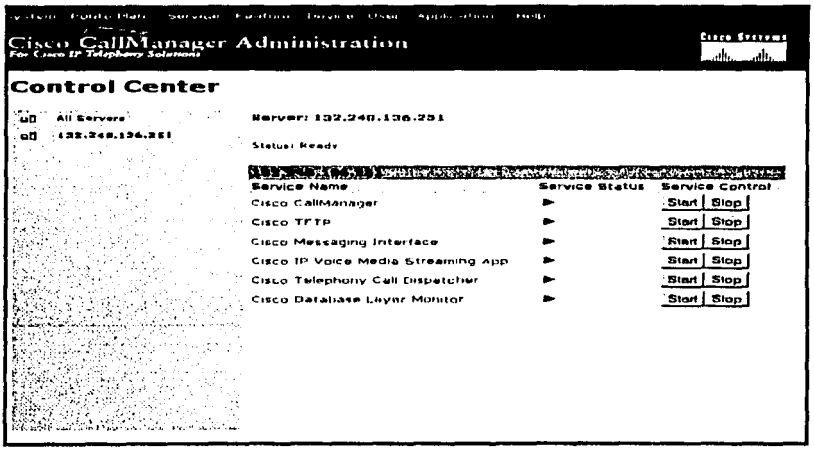


Figura 6-14: Muestra los servicios que presta el servidor de comunicaciones y permite iniciar o detener alguno de estos servicios para fines de mantenimiento o servicio.

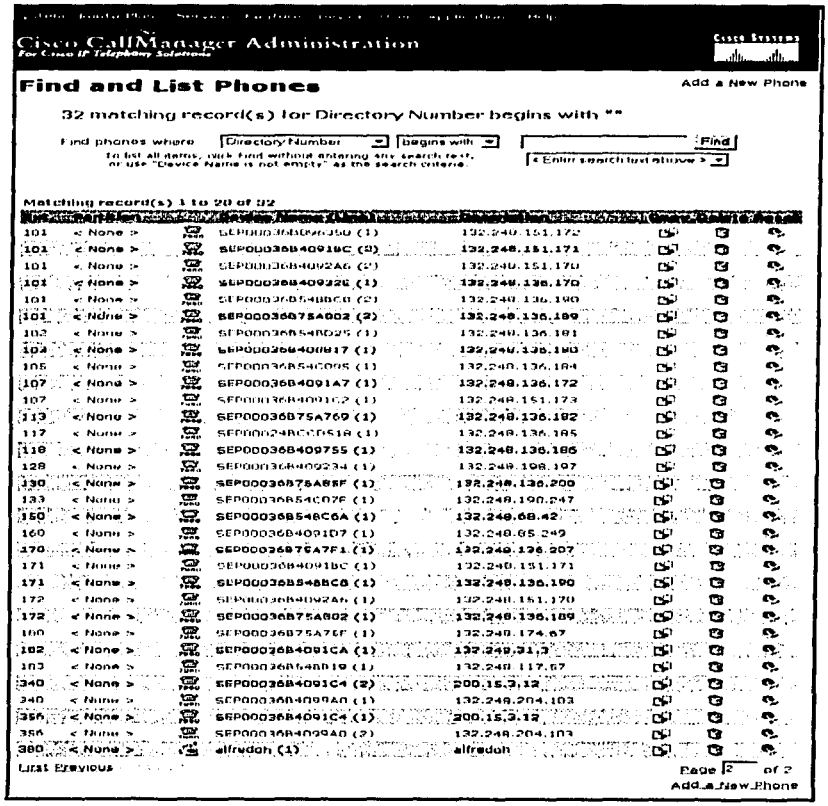


Figura 6-15: Muestra las extensiones definidas en el sistema (sean estas de IP-Phones o IP-SoftPhones), las direcciones MAC asociadas así como una descripción.

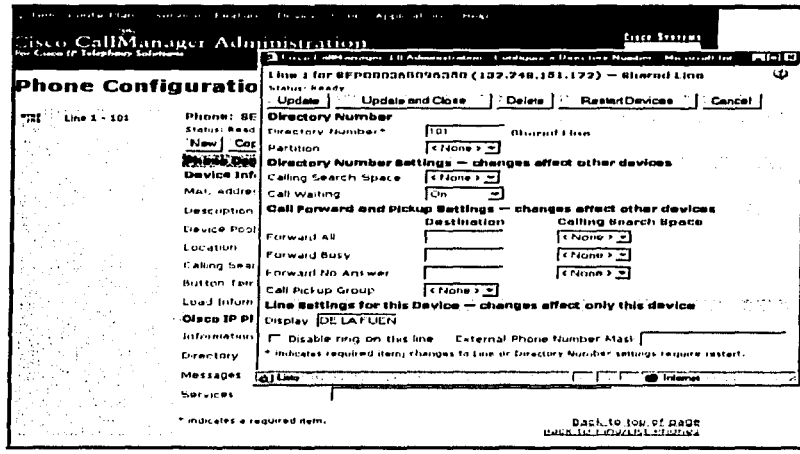


Figura 6-16: Define los parámetros de operación asociados a una extensión (como son el desvío de llamadas, el grupo call pickup, si es compartida la línea, el nombre que se desplegará cuando alguien llame, etc).

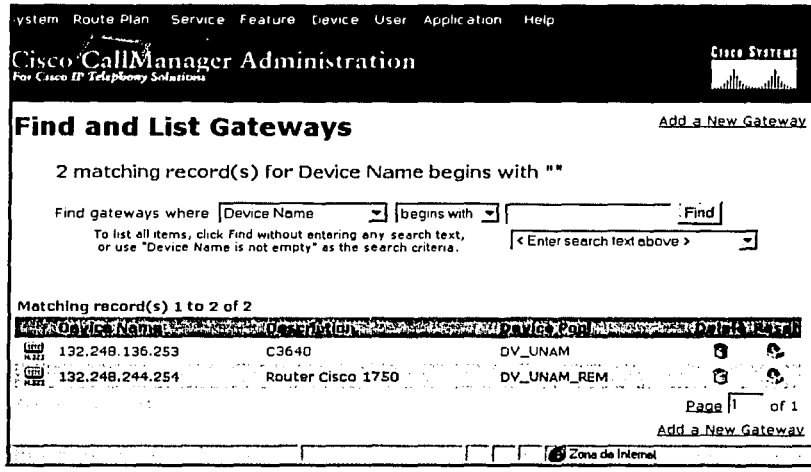


Figura 6-17: Muestra los Gateways H.323 definidos en el sistema para la intercomunicación con sistemas no-H.323 (tales como un PBX o la PSTN).

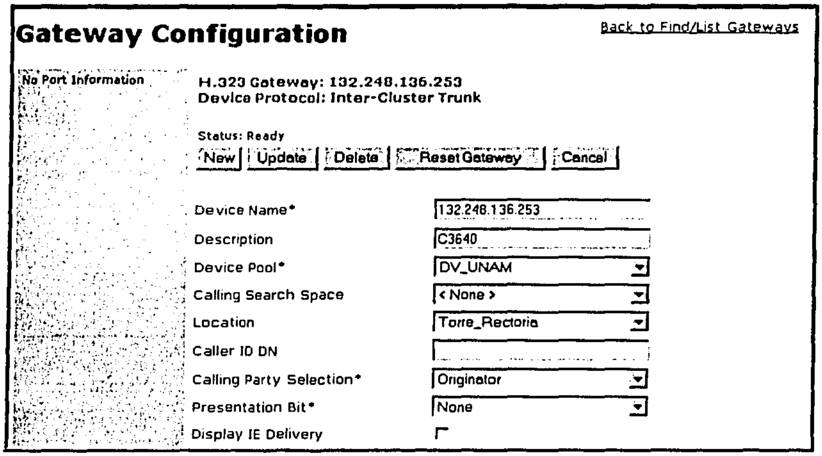


Figura 6-18: Muestra los parámetros de configuración asociados a un Gateway H.323 usado en este caso para la intercomunicación con el PBX NEC (NEAX_7400).

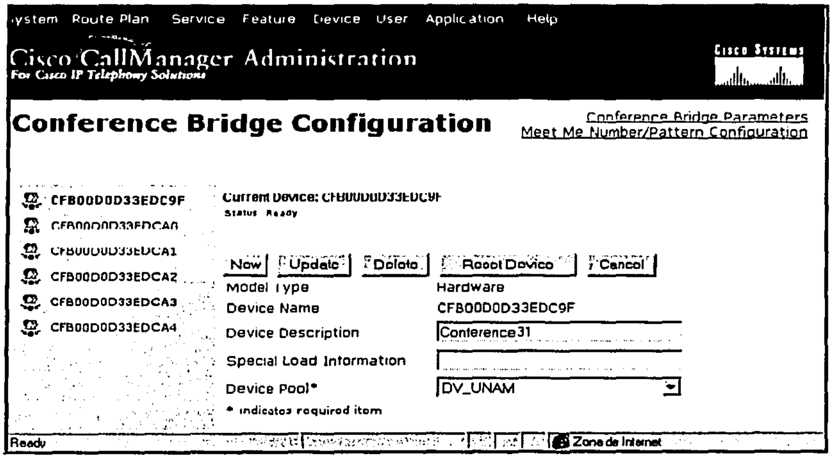


Figura 6-19: Muestra las direcciones MAC de los recursos del Switch Catalyst 6509 que serán usados para realizar la función de Conference Bridging.

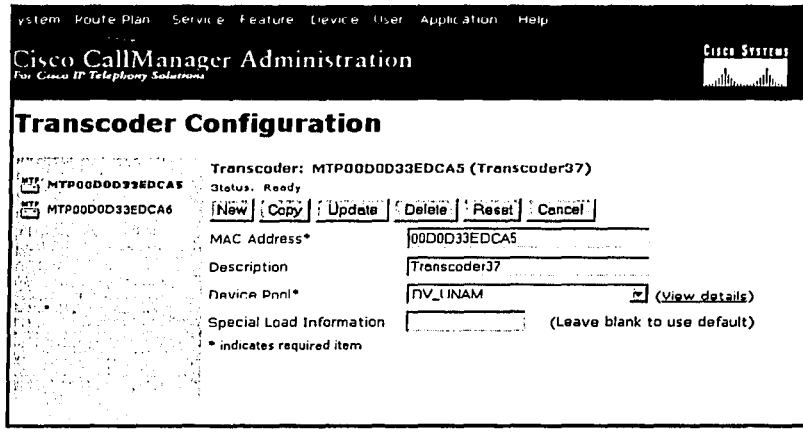


Figura 6-20: Muestra las direcciones MAC de los recursos del Switch Catalyst 6509 que serán usados para realizar la función de Transcodificación (conversión entre códigos de compresión).

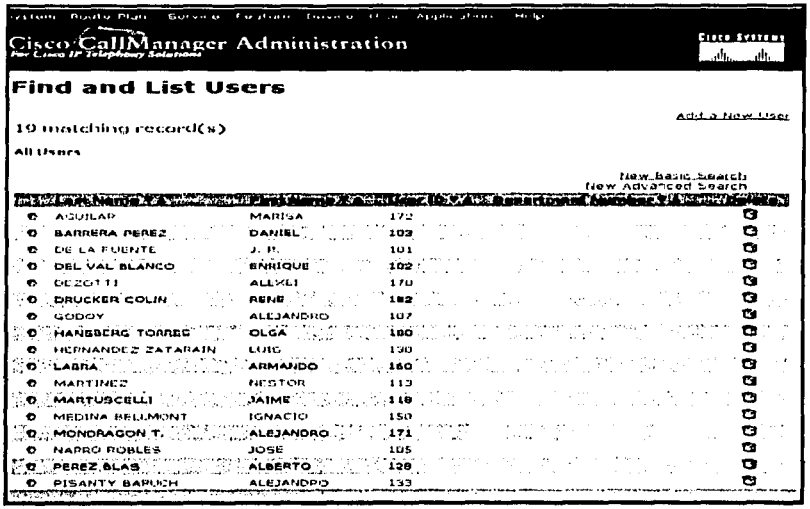


Figura 6-21: Muestra el Directorio Corporativo que será mostrado en los teléfonos y que puede ser usado para marcar por nombre a un usuario.

6.5.2 Router-Gateways 1750 y 3640 y PBX- NEC (NEAX_7400)

La configuración realizada sobre los Gateways presentes en el sistema de VoIP implementado, así como la del PBX NEC utilizado para la comunicación con la Red Telefónica de la UNAM o de Telmex, fueron:

Router Cisco 1750 (Gateway – Interface FXS)

```
GW-1750#sh run
!
hostname GW-1750
!
ip subnet-zero
!
interface Serial0
description Hacia-RedUNAM
ip unnumbered FastEthernet0
no ip directed-broadcast
!
interface FastEthernet0
description Red-LAN
ip address 132.248.244.254 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
speed auto
!
router igrp 278
network 132.248.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0 name Defaul_Route
no ip http server
!
voice-port 0/0
!
voice-port 0/1
!
dial-peer voice 1 voip
destination-pattern .T
session target ipv4:132.248.136.251
!
dial-peer voice 2 pots
destination-pattern 55555
port 0/0
!
dial-peer voice 3 pots
destination-pattern 55556
port 0/1
!
```

Router Cisco 3640 (Gateway – Interface E1 de voz)

```
GW-3640#sh run
!
hostname GW-3640
!
voice-card 1
!
call rsvp-sync
cns event-service server
!
ip subnet-zero
no ip domain-lookup
!
controller E1 1/0
 framing NO-CRC4
 clock source internal
 ds0-group 0 timeslots 1-2 type r2-digital r2-compelled
 cas-custom 0
  country telmex use-defaults
  category 2
  answer-signal group-b 1
!
interface FastEthernet0/0
 ip address 132.248.136.254 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 no ip mroute-cache
!
router igrp 278
 network 132.248.0.0
!
ip classless
no ip http server
ip route 0.0.0.0 0.0.0.0 FastEthernet0 name Default_Route
!
voice-port 1/0:0
 compand-type a-law
!
dial-peer voice 1 pots
 destination-pattern 2....
 port 1/0:0
 direct-inward-dial
 forward-digits all
!
dial-peer voice 2 pots
 destination-pattern 3....
 port 1/0:0
 direct-inward-dial
 forward-digits all
!
```

Continuación ...

```
!
dial-peer voice 3 pots
 destination-pattern 4....
 port 1/0:0
 direct-inward-dial
 forward-digits all
!
dial-peer voice 4 pots
 destination-pattern 9
 port 1/0:0
 direct-inward-dial
 forward-digits all
!
dial-peer voice 5 voip
 destination-pattern 1..
 session target ipv4:132.248.136.251
!
dial-peer voice 6 voip
 destination-pattern 3..
 session target ipv4:132.248.136.251
!
dial-peer voice 7 voip
 destination-pattern 5....
 session target ipv4:132.248.244.254
!
```

PBX NEC (NEAX 7400)

Assignment of Route Class Data
RT = 17 CDN = 4

CHANGE

FUNC : Route Class Parameters.

CDN	FUNC	DT	CDN	FUNC	DT	CDN	FUNC	DT
1	OSGS	= 2	16	SMDR2	= 0	31	OGRL	= 0
2	ONSG	= 2	17	H/M	= 0	32	ICRL	= 0
3	ISGS	= 2	18	MC	= 0	33	HD	= 0
4	ANSG	= 2	19	ANI	= 0	34	GUARD	= 0
5	TF	= 3	20	D	= 0	35	WINK	= 0
6	TCL	= 4	21	MSB	= 0	36	VAD	= 0
7	LJT	= 1	22	MSW	= 0	37	CLD	= 0
8	RLP	= 2	23	TR	= 0	38	FA	= 0
9	TQ	= 0	24	OC	= 1	39	BC	= 0
10	SMDR	= 0	25	R/L	= 0	40	TCM	= 0
11	TD	= 0	26	RVSD	= 0	41	TDMQ	= 0
12	DR	= 0	27	TL	= 0	42	TRSC	= 0
13	AC	= 0	28	ANS	= 1	43	BT	= 0
14	TNT	= 0	29	TELP	= 0	44	PVR	= 0
15	LSG	= 1	30	PAD	= 7	45	A/D	= 1

INSG : Signal Selection for Incoming (0-15).
1: DP, 10 pps, 33% Make.
2. PB, 60 msec. Interruption or No.7 CCIS
3: DP/PB
4: MF
5. DP, 20 pps, 33% Make.
7: DP, 20 pps, 50% Make.
8: PB, 120 msec Interruption.
9: DP, 10 pps, 40% Make.
10: MFC

NOTE: ESC key is pressed at the End of entering Route Class Parameters for the next operation. While entering other parameters, this key works as a Black Tab key.

6.5.3 IP-Phones 7960

A cada uno de los IP-Phones presentes en el sistema se le configuraron los siguientes parámetros:

- Dirección IP y máscara de subred (correspondientes a la subred donde se encuentre el IP-Phone). No se usaron los servicios DHCP para este efecto, sino que los teléfono se numeraron de manera estática.
- Default gateway (correspondientes a la subred donde se encuentre el IP-Phone).
- Dirección IP del servidor de TFTP.
- Personalización de las Speed-Calls (teclas de marcación rápida).
- Conexión de la PC del usuario al puerto FastEthernet secundario del IP-Phone.
- Configuración de las VLAN's para separar el tráfico de PC's y IP-Phones en una red.

En la siguiente figura se ilustra los IP-Phones utilizados así como una breve descripción de sus facilidades:

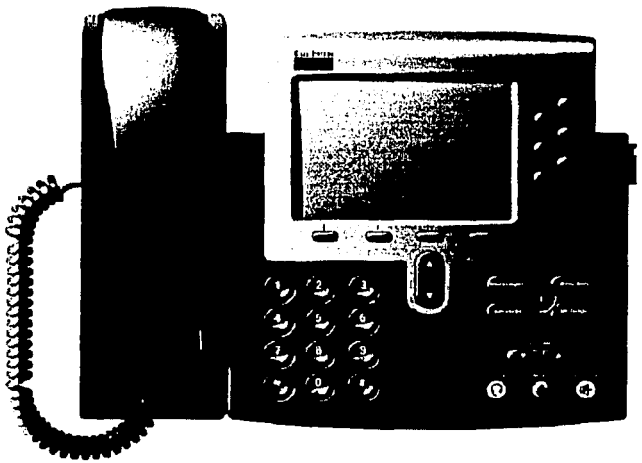


Figura 6-22: Cisco IP Phone 7960.

Cisco IP Phone 7960 features:

- Botones de línea configurables líneas o como speed dials.
- Display basado en pixeles.
- Cuatro Soft-keys con facilidades sensitivas al contexto.
- Cinco botones de funciones fijas (Mensajes, Servicios, Información, Directorio, Parámetros).
- Speaker full-duplex.
- Indicador de mensaje en espera.
- Dos conectores switchados 10/100 BaseT (RJ-45).
- Aprovisionamiento de alimentación ya sea de la línea o por un eliminador..

6.6 Lecciones que Dejó este Proyecto

Hay varias lecciones de primera mano que dejó este proyecto y que sin duda alguna serán de importancia para futuros desarrollos sobre la UNAM. Algunas de las reflexiones o cuestiones que deben cuidarse a futuro son las siguientes:

- Necesidad de contar con una red LAN bien diseñada y dimensionada.
  - Modelo de red jerárquico
    - Core → GigabitEthernet
    - Distribución → GigabitEthernet o FastEthernet
    - Acceso → GigabitEthernet, FatEthernet o Ethernet
  - Red switcheada
  - Uso de VLAN's.
- Necesidad de contar con el ancho de banda suficiente sobre los enlaces WAN y uso de esquemas de QoS para prioritizar el tráfico de voz en situaciones de congestión.
- Diseño de un plan de direccionamiento IP que tenga en cuenta las necesidades actuales y futuras de la base instalada de PC's y IP-Phones.
- Diseño de un plan de marcación telefónica que cumpla con las necesidades actuales y futuras.
- Definición de los puntos de conexión hacia la PSTN o hacia la red telefónica heredada.
- Necesidad de contar con un buen sistema de monitoreo y administración para los diferentes elementos del sistema.
- Contar con planes de seguridad que aíslen al sistema de problemas típicos de las redes de datos (virus, jackers, etc)
- Contar con un sistema de Telefonía-IP:
  - Apegado a los estándares.
  - Capaz de escalar sin problema alguno (hacia todo el campus de la red UNAM).
  - Capaz de rutear una llamada por una ruta alterna en caso de no estar disponible la primaria.
  - Escalable.
  - Capaz de trabajar en red con otros sistemas haciendo que las facilidades de usuario sean transparentes.
  - Que otorgue mayor inteligencia a los IP-Phones (arquitectura cliente/servidor).
  - Que ofrezca una forma conveniente de conectar y alimentar a los IP-Phones.
  - Que ofrezca aplicaciones y facilidades de usuario interesantes.
- Planes de seguridad.
- Etc.

6.7 Red Nacional-Internacional de VoIP

En el capítulo anterior hablábamos de la importancia de la Internet2, así como de los desarrollos que están teniendo lugar alrededor de ella, a fin de llevar a la Internet Comercial hacia su siguiente nivel de desarrollo y evolución, y cumplir de esta manera con las nuevas exigencias que sus usuarios demandan de ella. Con tal objetivo, actualmente están teniendo lugar en la Internet2 varios proyectos provenientes de diferentes áreas de interés que ayudarán significativamente a su desarrollo. Uno de tales proyectos es la implementación de una red internacional de VoIP basada en el protocolo de señalización H.323.

6.7.1 Objetivo de la Red Nacional-Internacional

Aun cuando algunas de las tecnologías de VoIP presentes actualmente en el mercado ofrecen soluciones atractivas para algunos entornos particulares de trabajo, éstas aun se encuentran en desarrollo y evolución. Por tal motivo, en Agosto del 2001 se lanzó una invitación a la comunidad internacional de la Internet2 para participar en un proyecto para la implementación de una red internacional de VoIP. El objetivo detrás de esta iniciativa (como puede verse en el siguiente cuadro, en donde se presenta el anuncio de la invitación original) es la de proveer a la industria de la retroalimentación necesaria para el desarrollo de mejores estándares de VoIP (en cuanto a su funcionalidad, escalabilidad, portabilidad, etc).

6.8 Red Nacional de VoIP

La decisión de la Internet2 Mexicana (y en especial de la UNAM) de propagar la tecnología de VoIP a lo largo y ancho de toda su red, así como participar en un proyecto de envergadura internacional estuvo apegada a las siguientes motivaciones:

- *Promover una mayor cercanía e intercomunicación entre los diferentes integrantes del CUDI (para efectos de troubleshooting, asesorías, reuniones, eventos, etc).*
- *Ahorrar gastos por concepto de llamadas de larga distancia nacionales e internacionales hacia las diferentes universidades pertenecientes a la Internet2.*
- *Hacer partícipes en este proyecto a todos los integrantes del CUDI que así lo deseen.*
- *Dar continuidad al espíritu innovador de CUDI.*
- *Promover un acercamiento con los proveedores de tecnologías de VoIP.*
- *Atesorar información de primera mano que ofrezca a los diferentes integrantes del CUDI los elementos para decidir si implementar esta tecnología en algún proyecto de telefonía futuro dentro de sus campus.*

INVITACIÓN ORIGINAL HECHA EN LA PÁGINA www.internet2.edu/voip EN AGOSTO DEL 2001 PARA PARTICIPAR EN EL PROYECTO DE VOIP SOBRE LA INTERNET2.

Internet2 Voice Over IP Testbed

The Internet2 VoIP Working Group is looking for Internet2 member universities and international partners to participate in a testbed for voice transmission over high-performance networks. This project will demonstrate the ability to successfully provide reliable long distance voice service over high bandwidth networks. We are looking for 20 sites initially to participate. Our goal is to have 10 sites connected by the Fall 2001 Internet2 Member Meeting and to have an additional 10 sites connected by the Spring 2002 Internet2 Member Meeting.

Assumptions

1. *The initial sites would connect circuit switched campus telephone systems over the Abilene network using ITU-T H.323 standards compliant gateways and gatekeepers.*
2. *The second round of sites would include sites with VoIP PBXs.*
3. *The third round of sites would include SIP compliant gateways.*
4. *All system components would be industry standards compliant.*
5. *All solutions recommended must be scalable and manageable.*
6. *The initial 20 sites will include international sites.*
7. *No through traffic would be allowed over this testbed. All voice traffic would be campus to campus.*

Goals

1. *To provide best practice documents that describe issues and recommendations that result from the testbed connections.*
2. *To coordinate H.323 issues with the Digital Video Working Group that deal with converged services on a single network.*
3. *To provide data that describes the call setup statistics, customer satisfaction, network latency and other pertinent information.*
4. *To assist in the development of troubleshooting tools that will assist network administrators and end users in isolating network faults.*
5. *To provide feedback to the industry that will further the development of VoIP standards.*

Timelines

1. *To have 10 sites connected by the Fall 2001 Internet2 Member Meeting.*
2. *To have an additional 10 sites and the first set of best practice documents online by the Spring 2002 Internet2 Member Meeting.*

Requirements for Participation

Any Internet2 institutions interested in participating in the VoIP Internet2 Testbed are encouraged to contact VoIP Working Group co-chair Walt Magnussen (w-magnussen@tamu.edu) no later than August 31. Requirements to participate include:

1. *Abilene network connection.*
2. *ITU-T H.323 compliant gateway and gatekeeper.*
3. *Multicast access to the Gatekeeper.*
4. *Access to technical resources on your campus.*
5. *Ability to provide utilization statistics and customer satisfaction surveys.*

6.8.1 Metas Técnicas y de Operación

Las metas técnicas y de operación que este proyecto pretende alcanzar dentro de la Internet2 mexicana (CUDI) se resumen a lo siguiente:

- *Desplegar una red de VoIP escalable mediante el protocolo de señalización H.323 que permita mantener en contacto a los diferentes integrantes del CUDI.*
- *Permitir el movimiento transparente de las terminales de usuario (SoftPhones) a lo largo y ancho de la red de CUDI.*
- *Permitir su interoperabilidad con las redes locales de Telefonía TDM o IP de las universidades.*
  - *Conexión hacia las redes telefónicas universitarias (mediante enlaces TDM hacia los PBX's locales).*
  - *Conexión hacia las redes de VoIP universitarias en caso de haberlas (mediante la conexión hacia el Gatekeeper, IP-PBX o Servidor de Comunicaciones locales).*
- *Permitir su prolongación temporal hacia aquellos lugares donde se realicen eventos especiales del CUDI (eventos de primavera).*
- *Aprovechar las características de Multicast y QoS presentes en la Internet2 mexicana.*

6.8.2 Topología y Descripción de la Red

La ***Red Nacional de VoIP*** está basada en el conocido protocolo de señalización y control de llamadas H.323. El core de la red está constituido básicamente por un Gatekeeper (GK) ubicado sobre uno de los routers de distribución de la UNAM, y de varios Gateways (GW's) desplegados a lo largo de los diferentes POP's asociados a las universidades presentes en la Internet2 mexicana. El GK de la UNAM (**GK_{UNAM}**) es usado para rutear las peticiones de llamada provenientes de los diferentes GW's presentes en la red (ver Figura 6-23). Además, el GK_{UNAM} tiene también la función de rutear las peticiones de llamada desde o hacia la ***Red Internacional de VoIP***, como se verá más adelante en la descripción de la Red Internacional de VoIP.

Las redes telefónicas universitarias tradicionales tienen acceso a la Red Nacional de VoIP mediante GW's locales. Estos GW's universitarios son generalmente routers Cisco de la serie 1700's, 2600's o 3600's. Las troncales (analógicas o digitales) usadas para interconectar los GW's y PBX's universitarios son interfaces FXO's, E1's o PRI's, donde la capacidad y elección de las mismas depende de las necesidades específicas de cada universidad. Generalmente los PBX's universitarios se han programan para que cuando reciban una cadena de dígitos de usuario, a la cual se le ha antepuesto el **dígito líder 8**, la llamada sea enrutada hacia la troncal que va hacia el GW local. Cuando un GW recibe una petición de llamada, éste determina si la llamada debe ser enviada el PBX local o hacia un punto de la Red Nacional de VoIP. Si la llamada debe ser enviada hacia la red de VoIP, entonces el GW pregunta al GK_{UNAM} (o al GK local en caso de existir) a fin de ubicar el mejor Punto-final (Terminal o GW) que pueda recibir y concretar la llamada. Para tal fin, el GK_{UNAM} checa su tabla de ruteo de números y proporciona al GW la dirección IP del Punto-final terminal deseado.

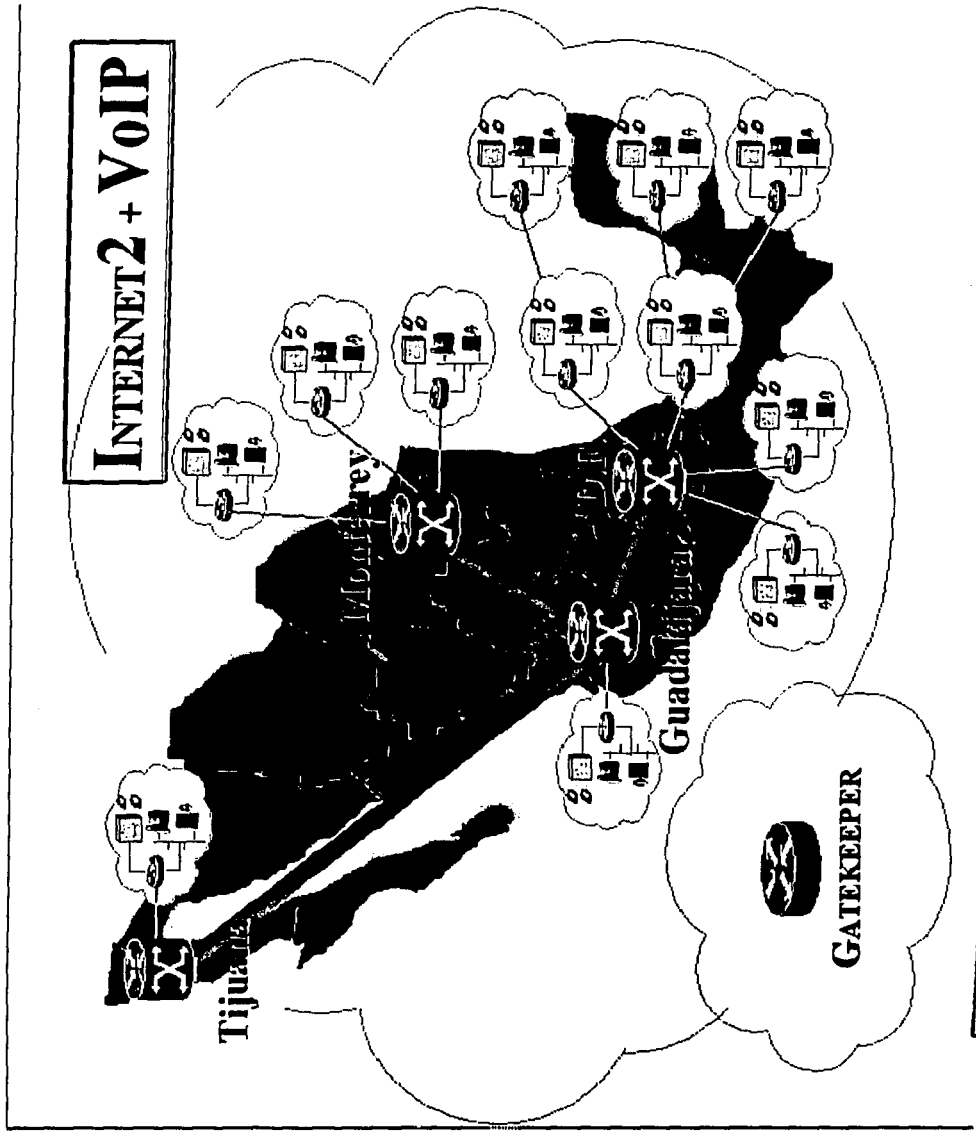


Figura 6-23: Red Nacional de VoIP mediante H.323

He aquí un resumen de la estructura y funcionamiento de la Red Nacional de VoIP:

- Uso del Gatekeeper de la UNAM (GK_{UNAM}) para resolver las peticiones de llamada a nivel nacional (e internacional como se verá más adelante).
- Gateways universitarios ubicados sobre los POP's locales e implementados sobre routers Cisco de la serie 1700's, 2600's o 3600's.
- Integración entre los PBX's y GW's universitarios mediante interfaces FXO's, E1's o PRI's , según las necesidades de cada universidad.
- Acceso a la red de VoIP desde la red telefónica universitaria marcando el dígito líder 8.
- Directorio telefónico global (mediante el uso de un servidor LDAP).
- Posibilidad de movilidad de los SoftPhones a lo largo y ancho de la red.
- Posibilidad de realizar conferencias haciendo uso de los recursos de los PBX's.

En la siguiente tabla se resumen las funciones de los diferentes componentes del core nacional basado en el GK_{UNAM} y varios GW's locales conectados a los PBX's universitarios:

COMPONENTE	FUNCIÓN
Gatekeeper UNAM (GK_{UNAM})	*Realiza el ruteo de las llamadas a nivel nacional (mediante el uso de códigos de área).*
	Distribuye los códigos de área hacia los GK's universitarios locales en caso de existir.
	Reenvía un mensaje LRQ hacia el GK universitario si la llamada pertenece a su área local de control.
	Provee la administración de su zona (pull de GW's).
Gatekeeper Local (GK) (en caso de existir)	*Realiza el ruteo de llamadas a nivel local (cuando hay varios GW's locales sobre una universidad).*
	Distribuye sus códigos de área locales hacia el GK_{UNAM}.
	Provee la gestión de los recursos del pull de GW's locales (mediante RAI, gw-priority u otra técnica).
	Provee la administración de su zona local (pull de GW's).
Gateway Local (GW)	*Actúa como interface entre la Red de Nacional de VoIP y el PBX universitario local.*
	Normaliza la cadena de dígitos provenientes de un PBX antes de que entren a la red de VoIP.
	Normaliza la cadena de dígitos provenientes de la red de VoIP antes que entren a un PBX universitario.
	Contiene la configuración de los dial peers.
	Se registra en el arranque ante el GK universitario local o ante el GK_{UNAM} en su defecto.

6.8.3 Plan de Marcación

Con respecto al plan de marcación, cada componente dentro la Red Nacional de VoIP es responsable de una porción del plan de marcación global. Los GW's son responsables de hacer las decisiones de ruteo sobre los bordes de la red, es decir entre los PBX's universitarios locales y la Red Nacional de VoIP. Mientras tanto, el GK_{UNAM} (o los GK's universitarios en caso de existir) maneja la lógica de ruteo para las llamadas entre cualesquiera dos dispositivos dentro de la Red Nacional de VoIP.

Hay dos reglas básicas asociadas al plan de marcación de la Red Nacional de VoIP que permiten una interoperabilidad transparente con las redes telefónicas universitarias (constituidas por PBX's). Estas son las siguientes:

- Apego irrestricto al plan nacional mexicano de numeración y marcación telefónicas (el cual a su vez está sustentado en el estándar mundial de marcación E.164), es decir:
  - Llamadas nacionales→ ***lada nacional + código de área + número local.***
  - Llamadas locales → ***número local.***
- Acceso a la Red Nacional de VoIP desde las redes telefónicas universitarias tradicionales (constituidas por PBX's) marcando el ***dígito líder 8.***

Nota: *referirse al Capítulo 2 donde se explican las reglas para el buen diseño del plan de marcación de una red de VoIP.*

La configuración que requiere hacerse sobre los diferentes equipos que componen la Red Nacional de VoIP a fin de implementar el plan de marcación a ser usado, depende en gran medida de las herramientas que proporciona la solución tecnológica de VoIP elegida. Para el caso de la solución de Cisco, la configuración se resume básicamente a los siguientes puntos:

- Definición de los Dial Peers en los GW's (POTS y VoIP).
- Normalización o traslación de números telefónicos en los GW's.
- Definición de los Prefijos de Tecnología en los GW's.
- Definición de las zonas locales y los prefijos de búsqueda en el GK_{UNAM}.

6.8.4 Configuración de los Diferentes Elementos

A fin de comprender la configuración presente en cada elemento componente de la Red Nacional de VoIP, usaremos el siguiente esquema simplificado compuesto por el GK_{UNAM} y dos GW's universitarios (ver Figura 6-24).

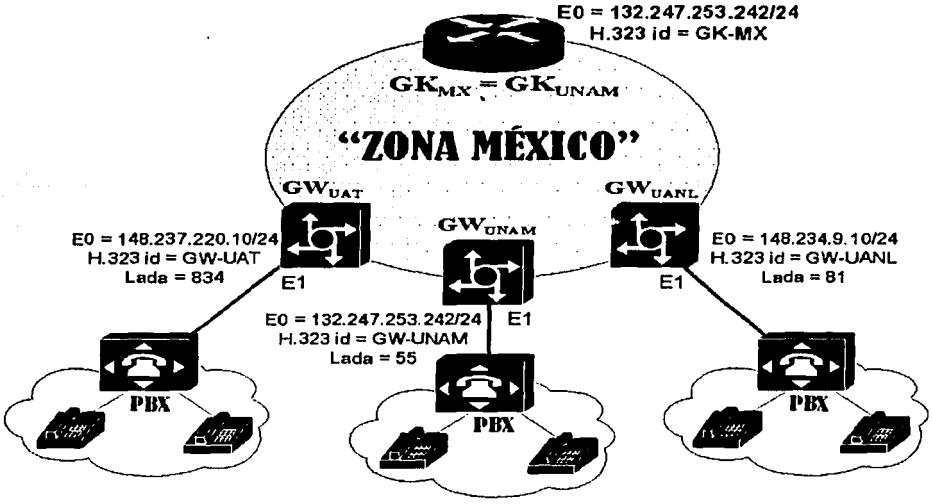


Figura 6-24: Esquema simplificado de la Red Nacional de VoIP.

Los requerimientos de configuración para cada uno de estos componentes de red son los siguientes.

1. ***Para los GW's:***

   1.1. *Configurar los enlaces de conexión TDM hacia los PBX's universitarios.*
   1.2. *Configurar los Dial Peers hacia la red TDM (POTS dial peers).*
   1.3. *Configurar los GW's para que se registren ante el GK_{UNAM}.*
   1.4. *Configurar los Dial Peers hacia la red de VoIP (VoIP dial peers).*
   1.5. *Configurar la normalización o traslación de números telefónicos (su propósito es reducir el número de dial-peers por cada GW).*

2. ***Para el GK_{UNAM}:***

   2.1. *Configurar el nombre y zona del GK_{UNAM}.*
   2.2. *Configurar los prefijos E.164 asociados a cada GW universitario.*

A continuación se presentan las configuraciones asociadas a cada uno de estos equipos, haciendo una referencia a los índices anteriores según la función que está siendo configurada. Hay que tomar en consideración que para que interoperen con la Red Internacional de VoIP, estas configuraciones deben modificarse un poco):

Gatekeeper de México y Gateway de la UNAM (sobre el mismo Router)

```
hostname GK-MEXICO
!
voice-card 3
!
translation-rule 1                                          ----------> 1.5
  Rule 0 ^011.% 1
  Rule 1 ^012.% 2
  Rule 2 ^013.% 3
  Rule 3 ^014.% 4
  Rule 4 ^015.% 5
  Rule 5 ^016.% 6
  Rule 6 ^017.% 7
  Rule 7 ^018.% 8
  Rule 8 ^019.% 9
!
controller E1 3/0                                           ----------> 1.1
  framing NO-CRC4
  clock source internal
  ds0-group 0 timeslots 1-31 type r2-digital r2-compelled
!
interface FastEthernet0
  ip address 132.248.108.10 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id GK-MEXICO ipaddr 132.247.253.242 1718  ----------> 1.3
  h323-gateway voip h323-id GW-UNAM
!
interface FastEthernet1
ip address 132.247.253.242 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet1 name Default-Route
no ip http server
!
voice-port 3/0:0
  timeouts interdigit 3
!
dial-peer cor custom
!
dial-peer voice 1 voip                                      ----------> 1.4
  destination-pattern 01T
  translate-outgoing called 1                               ----------> 1.5
  session target ras
!
dial-peer voice 2 pots                                      ----------> 1.2
  destination-pattern 562 . . . . .
  direct-inward-dial
  port 3/0:0
!
gateway
!
gatekeeper
  zone local GK-MEXICO unam.mx 132.247.253.242              ----------> 2.1
  zone prefix GK-MEXICO  834* gw-priority 10 GW-UAT         ----------> 2.2
  zone prefix GK-MEXICO  81* gw-priority 10 GW-UANL         ----------> 2.2
  zone prefix GK-MEXICO  55* gw-priority 10 GW-UNAM         ----------> 2.2
  no shutdown
```

Gateway de la UAT

```
Building configuration...
!
hostname GW-UAT
!
controller E1 1/0
  framing NO-CRC
  clock source internal
  ds0-group 0 timeslots 1-31 type r2-digital r2-compelled
!
translation-rule 1
  Rule 0 ^011.% 1
  Rule 1 ^012.% 2
  Rule 2 ^013.% 3
  Rule 3 ^014.% 4
  Rule 4 ^015.% 5
  Rule 5 ^016.% 6
  Rule 6 ^017.% 7
  Rule 7 ^018.% 8
  Rule 8 ^019.% 9
!
interface Ethernet0/0
  ip address 148.237.220.10 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id GK-MEXICO ipaddr 132.247.253.242 1719
  h323-gateway voip h323-id GW-UAT
  h323-gateway voip tech-prefix 834
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
voice-port 1/0:0
  timeouts interdigit 3
!
dial-peer cor custom
!
dial-peer voice 1 voip
  destination-pattern 01T
  translate-outgoing called 1
  session target ras
!
dial-peer voice 2 pots
  destination-pattern 834 . . . . . .
  port 1/0:0
!
gateway
!
```

Gateway de la UANL

```
Building configuration...
!
hostname GW-UANL
!
controller E1 1/0
  framing NO-CRC
  clock source internal
  ds0-group 0 timeslots 1-31 type r2-digital r2-compelled
!
translation-rule 1
  Rule 0 ^011.% 1
  Rule 1 ^012.% 2
  Rule 2 ^013.% 3
  Rule 3 ^014.% 4
  Rule 4 ^015.% 5
  Rule 5 ^016.% 6
  Rule 6 ^017.% 7
  Rule 7 ^018.% 8
  Rule 8 ^019.% 9
!
interface Ethernet0/0
  ip address 148.234.9.10 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id GK-MEXICO ipaddr 132.247.253.242 1719
  h323-gateway voip h323-id GW-UANL
  h323-gateway voip tech-prefix 81
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
voice-port 1/0:0
  timeouts interdigit 3
!
dial-peer cor custom
!
dial-peer voice 1 voip
  destination-pattern 01T
  translate-outgoing called 1
  session target ras
!
dial-peer voice 2 pots
  destination-pattern 81 . . . . . .
  port 1/0:0
!
gateway
!
```

6.9 Red Internacional de VoIP basada en un Core de Gatekeepers

Tal como para la Red Nacional de VoIP, el core de la ***Red Internacional de VoIP*** está constituido por una estructura jerárquica de Gateways (GW's) y Gatekeepers (GK's). Los GW's, típicamente desplegados a lo largo de los diferentes POP's presentes en la red de Internet2, requieren de los servicios de los GK's para realizar llamadas nacionales e internacionales. De esta manera, los GK's son usados para agrupar los diferentes GW's nacionales asociados dentro de zonas lógicas de control y realizar el ruteo de las llamadas entre tales zonas.

Sin embargo, para una red de VoIP como la descrita se requiere de un elemento adicional que haga al sistema escalable y simplifique la administración del plan de marcación de la red (compuesta de numerosos GK's nacionales). Este elemento adicional es el ***Directory Gatekeeper Global (DGK$_{GLOBAL}$)***, responsable del ruteo de llamadas en los GK's nacionales. Por supuesto que en una red de VoIP como ésta en la que existen varios niveles jerárquicos, los GK's nacionales podrían hacer las veces de DGK's hacia los niveles inferiores.

Con respecto al plan de marcación, cada componente dentro la red de VoIP es responsable de una porción del plan de marcación global. Los GW's son responsables de hacer decisiones de ruteo en los bordes de la red, es decir, entre las redes telefónicas universitarias y la red de VoIP. Por otra parte, son los GK's y los DGK's los que manejan la lógica de ruteo de las llamadas entre los diferentes dispositivos dentro de la Red Nacional/Internacional de VoIP.

La comunicación entre los GW's y GK's está basada sobre la ***señalización RAS*** (Registro, Admisión y Estatus) del ***protocolo H.323v2***. Es decir, los GW's preguntan a los GK's por la dirección IP destino de una llamada por medio de mensajes RAS tipo ARQ/ACF (Admission Request/Admisión Confirm). Los GK's y DGK's también se comunican por medio de mensajes de localización RAS tipo LRQ/LCF (Location Request/Location Confirm). En la Figura 6-25 se ilustra la secuencia de mensajes RAS que tiene lugar cuando un teléfono A llama a un teléfono B remoto sobre una red de VoIP cuyo core está basado en una estructura jerárquica de GK's.

Nota: referirse al Capítulo 3 donde se explica con mayor detalle los diferentes mensajes RAS que tienen lugar en la comunicación entre un GW y un GK, o entre dos GK's.

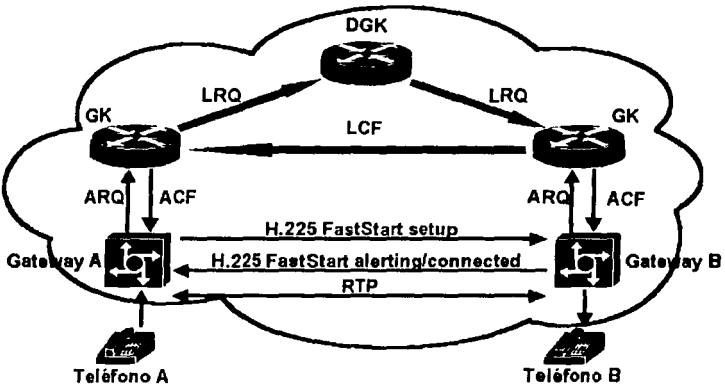


Figura 6-25: Diferentes tipos de mensajes RAS sobre una red basada en Gatekeepers.

La siguiente Tabla resume las funciones de los componentes de una red basada en GK's.

COMPONENTE	FUNCIÓN
Directory Gatekeeper (DGK)	*Realiza el ruteo de las llamadas a nivel país (ejemplo: código de país).*
	Distribuye los códigos de país con otros DGK's.
	Reenvía un mensaje LRQ a un DGK homólogo si la llamada no termina en su área local de control.
Gatekeeper (GK)	*Realiza el ruteo de las llamadas a nivel medio o ciudad (ejemplo: código de área).*
	Distribuye los códigos de área con otros GK's.
	Provee la gestión de los recursos de los GW's (mediante RAI, gw-priority u otro mecanismo).
	Provee la administración de su zona de control.
Gateway (GW)	*Actúa como interface entre la red telefónica tradicional con PBX's y la red de VoIP.*
	Normaliza la cadena de dígitos proveniente de la red telefónica tradicional antes de que entre a la red de VoIP.
	Normaliza la cadena de dígitos proveniente de la red de VoIP antes de que entre a la red telefónica tradicional local.
	Alberga la configuración de los dial peers.
	Se registra en el arranque ante un GK de zona.

La Figura 6-26 ilustra de manera global la relación entre los diferentes GW's, GK's y DGK's para algunas universidades sobre la Red Internacional de VoIP.

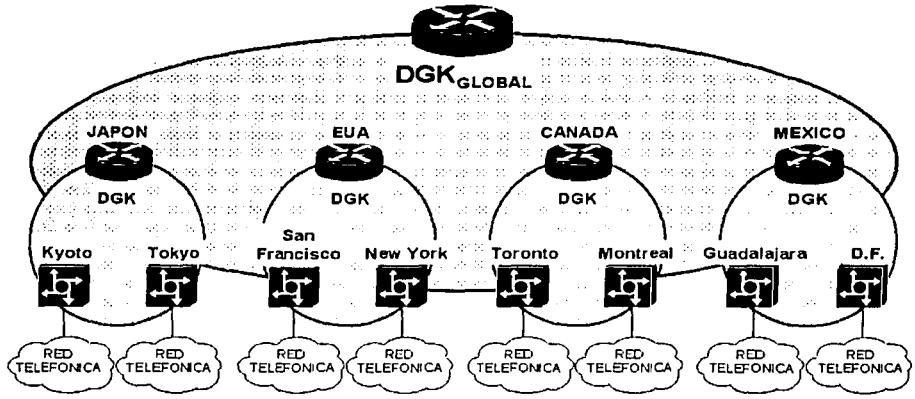


Figura 6-26: Relación entre Redes Telefónicas Universitarias, Gateways, Directory Gatekeepers y Global Directory Gatekeeper

6.9.1 Plan de Marcación

Tal como se mencionó anteriormente, cada componente dentro la red de VoIP es responsable de una porción del plan de marcación global: los GW's son responsables de hacer las decisiones de ruteo sobre los bordes de la red, es decir, deciden si mandan la llamada hacia los PBX's universitarios locales o hacia la Red Nacional/Internacional de VoIP. Mientras tanto, el DGK_{GLOBAL}, los DGK y los GK's universitarios manejan la lógica de ruteo para las llamadas para dos dispositivos cualesquiera dentro de la red de VoIP.

Hay dos principios básicos asociados al plan de marcación de la Red Internacional de VoIP que permiten una interoperabilidad transparente con las redes telefónicas universitarias (a base de PBX's) y que evitan tener problemas legales con las carriers de algún país. Estos son los siguientes:

- Apego irrestricto al plan internacional de numeración y marcación telefónica mundial:
  - Llamadas internacionales → ***lada internacional + código de país + código de área + número local.***
  - Llamadas nacionales → ***lada nacional + código de área + número local.***
  - Llamadas locales → ***número local (de 7 a 8 dígitos).***
- No se permite bajo ninguna circunstancia que una universidad en algún país acceda a la PSTN de otro país a través de la red internacional de VoIP.

Nota: referirse al Capítulo 2 donde se explican las reglas para el buen diseño del plan de marcación de una red de VoIP.

6.9.2 Configuración de los Diferentes Elementos

La configuración que se requiere hacer en los diferentes elementos que componen la Red Internacional de VoIP es parecida a la descrita para el caso de la Red Nacional de VoIP, excepto por el DGK_{GLOBAL} y los $DGK_{NACIONALES}$ que requiere una configuración específica y algunos cambios menores sobre los GW's. A fin de comprender la configuración presente en cada elemento componente de la Red Internacional de VoIP, usaremos el siguiente esquema simplificado compuesto por el GK_{GLOBAL}, dos DGK nacionales y un pull de GW's universitarios locales asociados (ver Figuras 6-27 y 6-28).

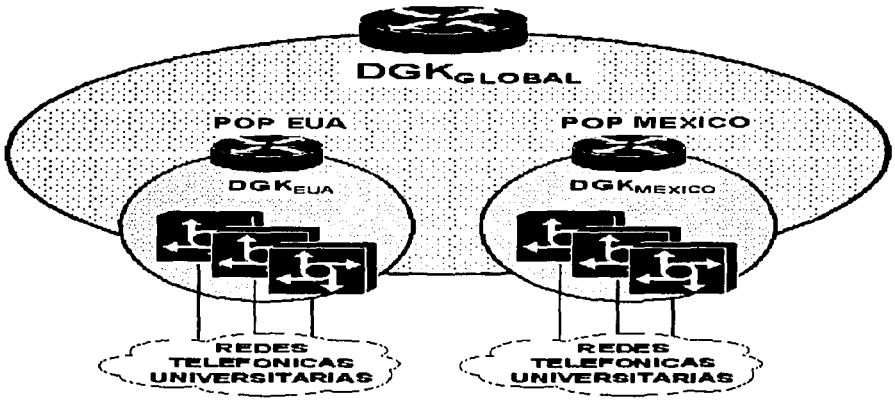


Figura 6-27: Ejemplo de configuración para la Red Internacional de VoIP.

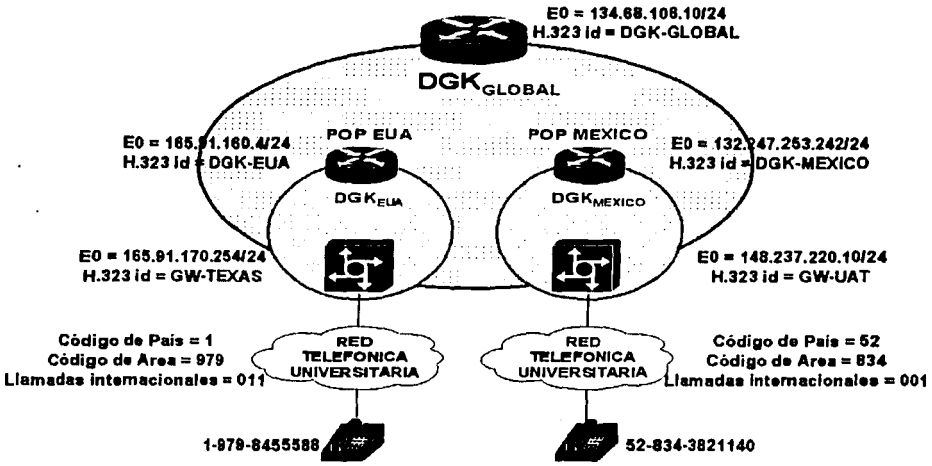


Figura 6-28: Topología detallada de la red (del Ejemplo).

Los requerimientos de configuración para cada uno de estos componentes de red son los siguientes.

Para la comunicación dentro de una misma zona (o país):

1. *Para los GW's*
- 1.1. *Configurar los enlaces de conexión TDM hacia los PBX's universitarios.*
- 1.2. *Configurar los Dial Peers hacia la red TDM (POTS dial peers).*
- 1.3. *Configurar los GW's para que se registren ante el $GK_{NACIONAL}$.*
- 1.4. *Configurar los Dial Peers hacia la red de VoIP (VoIP dial peers).*
- 1.5. *Configurar la normalización o traslación de números telefónicos.*

2. *Para el $GK_{NACIONAL}$*
- 2.1. *Configurar el nombre y zona del $GK_{NACIONAL}$.*
- 2.2. *Configurar los prefijos E.164 asociados a cada GW universitario.*

Para la comunicación con otras zonas (o países) declarar el DGK_{GLOBAL} en cada zona:

- 2.3. *Configurar el nombre, dirección IP y zona del DGK_{GLOBAL}.*

3. *Para el DGK_{GLOBAL}*
- 3.1. *Configurar la tabla maestra de prefijos de zona de los $DGK_{NACIONALES}$.*

Nota: como se había mencionado con anterioridad $DGK_{MEXICO} = GK_{UNAM}$.

A continuación se presentan las configuraciones asociadas a cada uno de estos equipos:

DGK-GLOBAL

```
Current configuration:
!
hostname DGK-GLOBAL
!
!
interface FastEthernet0/0
   ip address 172.19.49.178 255.255.255.192
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
no ip http server
!
gatekeeper
   zone local DGK-GLOBAL internet2.edu 134.68.106.10
   zone remote DGK-EUA tamu.edu 165.91.160.4 1719
   zone remote DGK-MEXICO unam.mx 132.247.253.242 1719
   zone prefix DGK-EUA 1*
   zone prefix DGK-MEXICO 52*
   lrq forward-queries
   no shutdown
!
```

DGK-MEXICO

```
Current configuration:
!
hostname DGK-MEXICO
!
!
interface Ethernet0/0
   ip address 132.247.253.242 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
!
gatekeeper
   zone local DGK-MEXICO unam.mx 132.247.253.242
   zone remote DGK-GLOBAL internet2.edu 172.19.50.100 1719
   zone prefix DGK-MEXICO 52834* gw-priority 10 GW-UAT
   zone prefix DGK-GLOBAL *
   no shutdown
!
```

GW-UAT (Gateway de una Universidad en México)

```
Building configuration...
!
hostname GW-UAT
!
controller E1 1/0
  framing NO-CRC
  clock source internal
  ds0-group 0 timeslots 1-31 type r2-digital r2-compelled
!
translation-rule 1
  Rule 0 ^001.% 1
  Rule 1 ^002.% 2
  Rule 2 ^003.% 3
  Rule 3 ^004.% 4
  Rule 4 ^005.% 5
  Rule 5 ^006.% 6
  Rule 6 ^007.% 7
  Rule 7 ^008.% 8
  Rule 8 ^009.% 9
!
translation-rule 2
  Rule 0 ^011.% 521
  Rule 1 ^012.% 522
  Rule 2 ^013.% 523
  Rule 3 ^014.% 524
  Rule 4 ^015.% 525
  Rule 5 ^016.% 526
  Rule 6 ^017.% 527
  Rule 7 ^018.% 528
  Rule 8 ^019.% 529
!
interface Ethernet0/0
  ip address 148.237.220.10 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id GK-MEXICO ipaddr 132.247.253.242 1719
  h323-gateway voip h323-id GW-UAT
  h323-gateway voip tech-prefix 52834
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
voice-port 1/0:0
  timeouts interdigit 3
!
dial-peer cor custom
!
dial-peer voice 1 voip
  destination-pattern 00T
  translate-outgoing called 1
  session target ras
!
```

Continuación ...

```
!
dial-peer voice 2 voip
  destination-pattern 01T
  translate-outgoing called 2
  session target ras
!
dial-peer voice 3 pots
  destination-pattern 834 . . . . . .
  direct-inward-dial
  port 1/0:0
!
gateway
!
```

DGK-EUA

```
Current configuration:
!
hostname DGK-EUA
!
!
interface Ethernet0/0
  ip address 165.91.160.4 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
!
gatekeeper
  zone local DGK-EUA tamu.edu 165.91.160.4
  zone remote DGK-GLOBAL internet2.edu 134.68.106.10 1719
  zone prefix DGK-EUA 1979* gw-priority 10 GW-TEXAS
  zone prefix DGK-GLOBAL *
  no shutdown
!
```

GW-TEXAS (Gateway de una Universidad en EUA)

```
Current configuration:
!
hostname GW-TEXAS
!
!
controller E1 1/0
  framing NO-CRC
  clock source internal
  ds0-group 0 timeslots 1-31 type r2-digital r2-compelled
!
```

Continuación ...

```
translation-rule 1
   Rule 0 ^0111.% 1
   Rule 1 ^0112.% 2
   Rule 2 ^0113.% 3
   Rule 3 ^0114.% 4
   Rule 4 ^0115.% 5
   Rule 5 ^0116.% 6
   Rule 6 ^0117.% 7
   Rule 7 ^0118.% 8
   Rule 8 ^0119.% 9
!
!
interface Ethernet0/0
  ip address 165.91.170.254 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id NA-GK ipaddr 165.91.160.4 1719
  h323-gateway voip h323-id GW-TEXAS
  h323-gateway voip tech-prefix 1979
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
!
voice-port 1/0:0
  timeouts interdigit 3
!
dial-peer cor custom
!
!
dial-peer voice 1 voip
  destination-pattern 011T
  translate-outgoing called 1
  session target ras
!
dial-peer voice 2 voip
  destination-pattern 1T
  session target ras
!
dial-peer voice 3 pots
  destination-pattern 1979 .......
  direct-inward-dial
  port 1/0:0
!
gateway
!
```

En la Figura 6-29 se ilustra la estructura real de la Red Internacional de VoIP mostrando la conexión de la UNAM a la misma. Por otra parte, en la figura 6-30 se muestra el desplegado sobre la página de Internet2 en los EUA donde se anuncia la incorporación de la UNAM a la Red Internacional de VoIP.

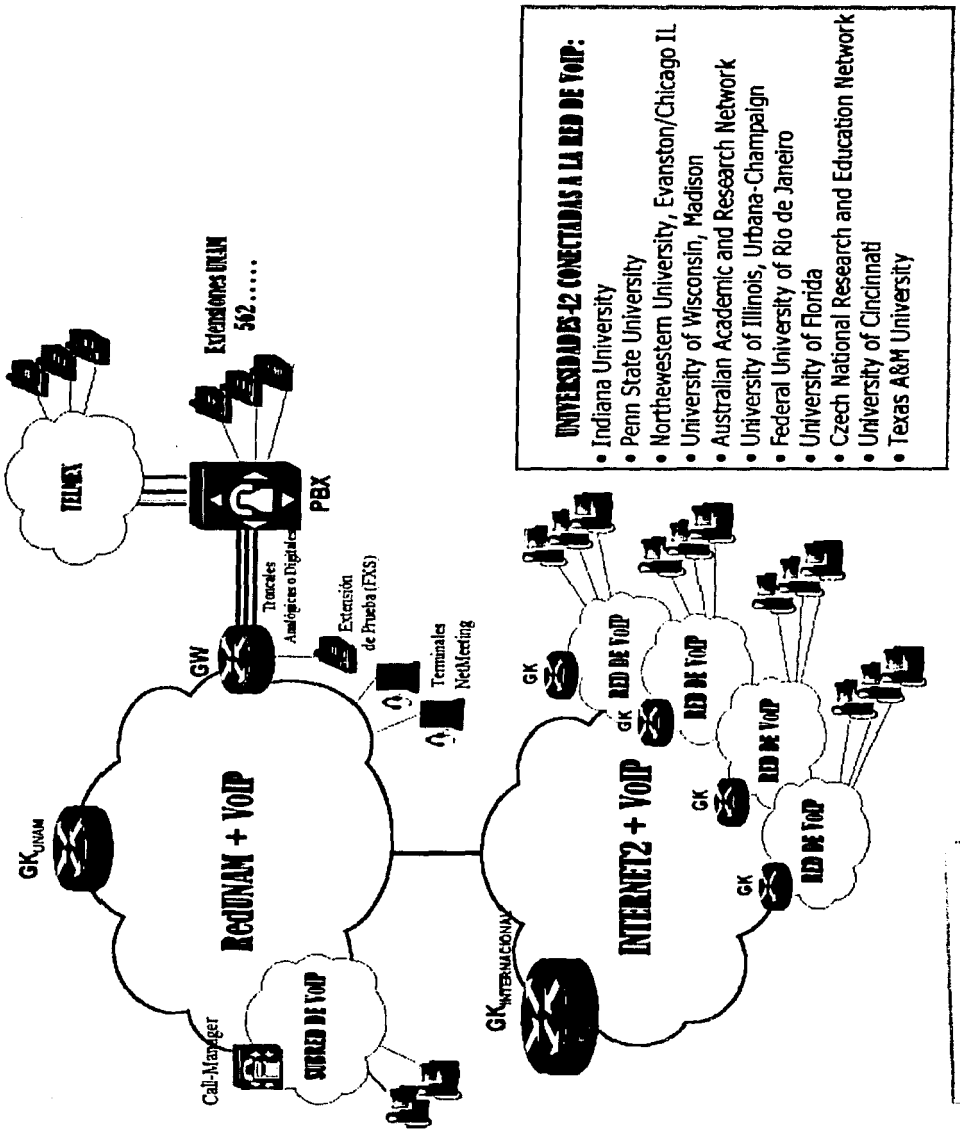


Figura 6-29: Topología real de la Red Internacional de VoIP.

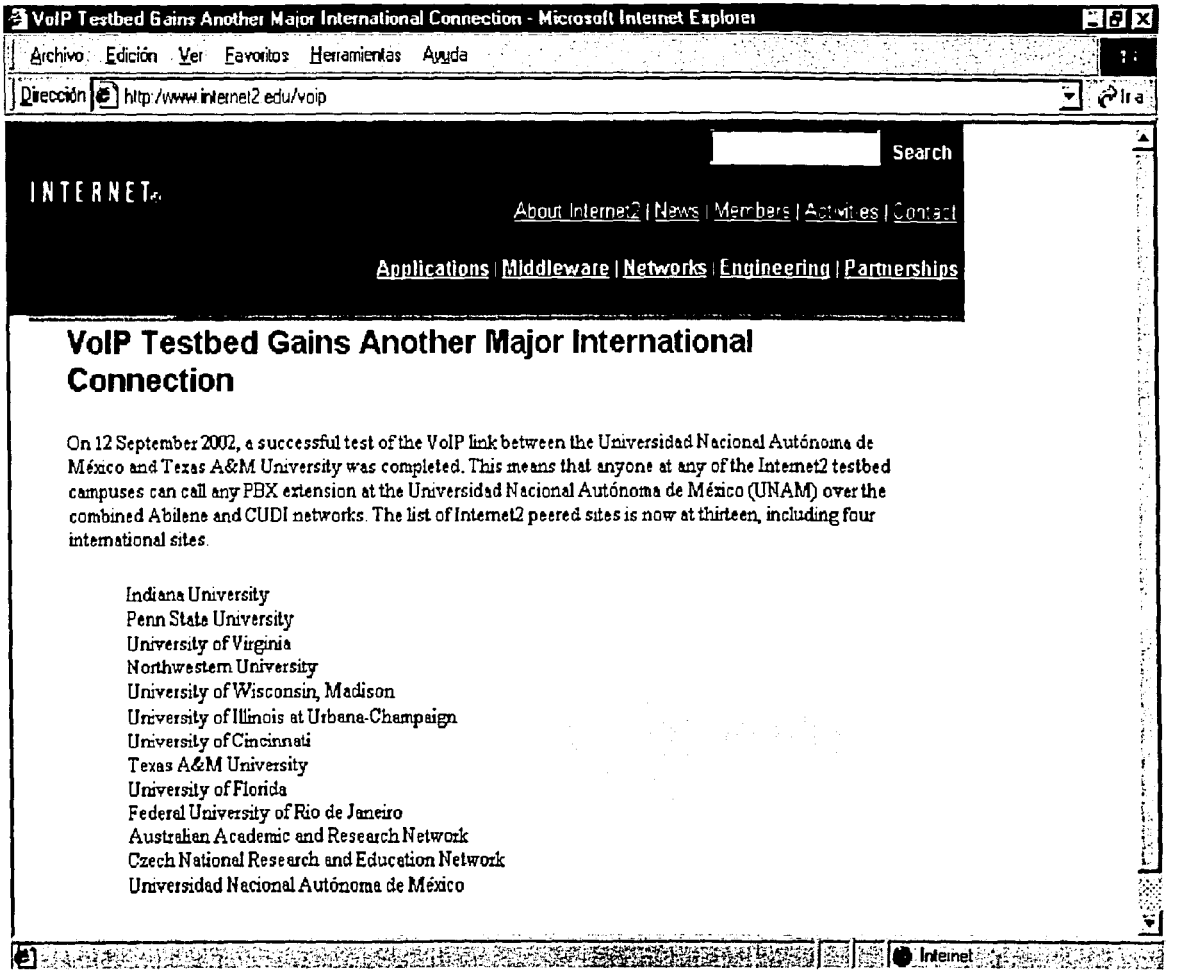


Figura 6-30: Incorporación de la UNAM a la Red Internacional de VoIP.

6.9.3 Configuración del Directory Gatekeeper Global

A continuación se muestra una parte de la configuración real del Directory Gatekeeper Global de la Red Internacional de VoIP. Esta información fue proporcionada directamente por sus administradores y corresponde a la configuración presente al día 03-Septiembre-2002.

DGK-GLOBAL (gk01.internet2.edu.edu = 134.68.106.10)

```
Current configuration:
!
gatekeeper
  zone local IUGK iu.edu 134.68.106.10
  zone local PSUGK psu.edu
  zone local UVIRGINIAGK virginia.edu
  zone local NWUGK nwu.edu
  zone local UWISC 134.68.106.10
  zone local TAMU tamu.edu
  zone remote AARNet edu.au 203.22.212.245 1719
  zone remote UIUCGK uiuc.edu 130.126.1.3 1719
  zone remote UFRJGK ufrj.br 146.164.247.202 1719
  zone remote UFLGK ufl.edu 128.227.75.68 1719
  zone remote CESNETGK cesnet.cz 195.113.144.84 1719
  zone remote UCGK uc.edu 129.137.0.2 1719
  zone remote TAMUI2 tamu.edu 165.91.160.4 1719
  zone remote UNAMGK unam.mx 132.247.253.242 1719
  zone remote AARNet edu.au 203.22.212.245 1719
  zone prefix UIUCGK 1217244 ....
  zone prefix UIUCGK 1217265 ....
  zone prefix UIUCGK 1217332 ....
  zone prefix UIUCGK 1217333 ....
  zone prefix IUGK 1317274 ....
  zone prefix IUGK 1317278 ....
  zone prefix UFLGK 135233478 ..
  zone prefix UVIRGINIAGK 1434243 ....
  zone prefix UVIRGINIAGK 1434924 ....
  zone prefix UVIRGINIAGK 14349820 ...
  zone prefix UVIRGINIAGK 14349821 ...
  zone prefix UVIRGINIAGK 14349822 ...
  zone prefix UVIRGINIAGK 14349823 ...
  zone prefix UVIRGINIAGK 14349824 ...
  zone prefix UVIRGINIAGK 14349825 ...
  zone prefix UVIRGINIAGK 14349826 ...
  zone prefix TAMUI2 1512425 ....
  zone prefix UCGK 1513556 ....
  zone prefix UCGK 1513558 ....
  zone prefix UWISC 1608001 ....
  zone prefix UWISC 1608262 ....
  zone prefix UWISC 1608263 ....
  zone prefix UWISC 1608264 ....
  zone prefix UWISC 1608265 ....
  zone prefix IUGK 1812855 ....
  zone prefix IUGK 1812856 ....
```

Continuación ...

```
zone prefix IUGK 1812857 . . . .
zone prefix PSUGK 1814863 . . . .
zone prefix NWUGK 184746770 . .
zone prefix TAMU 1979458 . . . .
zone prefix TAMUI2 1979458 . . . .
zone prefix TAMUI2 1979845 . . . .
zone prefix TAMUI2 1979847 . . . .
zone prefix TAMUI2 1979862 . . . .
zone prefix CESNETGK 420 . . . . . .
zone prefix UNAMGK 5255562 . . . . .
zone prefix UFRJGK 55212562 . . . .
zone prefix UFRJGK 55212598 . . . .
zone prefix AARNet 61 . . . . . .
gw-type-prefix 1#* default-technology
lrq fordward-queries
no shutdown
!
```

Conclusiones

La UNAM desde siempre se ha preocupado por estar a la vanguardia en cuanto a tecnologías de redes de datos, a fin de proveer un mejor servicio a su comunidad universitaria. En los últimos años con el surgimiento de las tecnologías de VoIP, se ha estado trabajando sobre algunos proyectos sobre Telefonía-IP. Lo aprendido en cada uno de estos proyectos será de importancia sin lugar a dudas para todo proyecto de telefonía venidero, y le proporcionará a la UNAM en su momento los elementos para hacer elecciones y decisión sabias.

En este capítulo hemos visto algunos de los proyectos más importantes sobre tecnologías de VoIP en los que la UNAM ha estado trabajando o participando, a saber: Implementación de la ***Red de Telefonía-IP para la Red de Funcionarios de Rectoría*** y la ***Red Nacional e Internacional de VoIP sobre la Internet2***. Como se mencionaba en alguna parte este capítulo, el sentido de proyectos como el de la Red Nacional e Internacional de VoIP es el de proveer a la industria, a las empresas y a las universidades la retroalimentación necesaria para el desarrollo de mejores estándares de VoIP (en cuanto a su funcionalidad, escalabilidad y portabilidad y que a la postre conlleven a mejores productos), así como de los elementos para que las empresas decidan o no implementar alguna solución de VoIP sobre sus instalaciones, y en dado caso, bajo que condiciones.

CAPÍTULO 7

PRUEBAS REALIZADAS Y PROYECTOS A FUTURO

"Uno no puede beberse la palabra agua. La fórmula H_2O no puede mantener a un barco a flote. La palabra lluvia no puede mojarle a uno. Se debe experimentar el agua o la lluvia para saber lo que estas palabras significan verdaderamente. Lo único que realmente explica las cosas es vivirlas"

El camino que ha llevado hacia una mejor comprensión de las tecnologías de VoIP ha sido largo y ha pasado por la realización de una serie de pruebas interrelacionadas. Todas estas pruebas fueron previas a cualquier implementación real, y de hecho estuvieron pensadas para aportar algún grado de experiencia así como para resolver algunas cuestiones importantes en relación a algunos de los proyectos de Telefonía-IP que han tenido lugar en la UNAM (ver el Capítulo 6).

En las siguientes secciones se describe brevemente algunas de estas pruebas, intentando presentarlas en el orden en que fueron realizadas y dejando ver como se lograba avanzar un paso hacia adelante con la concreción de cada una de ellas. Cabe mencionar que en la mayoría de los casos estas pruebas fueron realizadas sobre equipos y soluciones de Cisco. Por último, se expone un nuevo proyecto que intenta implementar una red de VoIP basada en el protocolo de señalización y control de llamadas SIP (el cual promete superar todo lo logrado hasta el momento por H.323).

7.1 Comunicación Mediante Dial-Peers

El propósito de esta prueba era establecer una conexión telefónica sobre una red de datos IP usando dos teléfonos estándar conectados a routers de la serie 2600 mediante interfaces FXS. Ver la ilustración de la Figura 7-1 y las configuraciones correspondientes a tal prueba.

Figura 7-1: Comunicación telefónica sobre una red de datos IP (usando dial-peers).

ROUTER-A

```
Current configuration:
!
hostname Router-A
!
voice-port 1/0/0
!
voice-port 1/0/1
!
interface Ethernet0/0
 ip address 132.248.10.254 255.255.255.0
!
ip classless
no ip http server
ip route 0.0.0.0 0.0.0.0 Ethernet0/0 name Default_Route
!
dial-peer voice 1 pots
 destination-pattern 28509
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 46017
 session target ipv4:132.248.20.254
!
```

ROUTER-B

```
Current configuration:
!
hostname Router-B
!
voice-port 1/0/0
!
voice-port 1/0/1
!
interface Ethernet0/0
 ip address 132.248.20.254 255.255.255.0
!
ip classless
no ip http server
ip route 0.0.0.0 0.0.0.0 Ethernet0/0 name Default_Route
!
dial-peer voice 1 pots
 destination-pattern 46017
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 28509
 session target ipv4:132.248.10.254
!
```

Nota: *La llave para comprender las implementaciones de VoIP de Cisco es entender el uso de los* ***Dial-Peers****. Los dial-peers son comandos que son usados para asociar números telefónicos sobre ciertas interfaces especiales en un router (Gateway) y determinar la dirección IP del router hacia donde se debe enviar una llamada a fin de establecer una conexión con un teléfono asociado a ese otro router. Los dial-peers son usados para definir las características asociadas con cada tramo de la llamada e identificar el origen y destino de una llamada. Existen básicamente dos tipos de dial-peers:* ***POTS Dial-Peer*** *y los* ***VoIP Dial-Peer****.*

7.2 Comunicación PBX/Gateway

La idea detrás de esta prueba era permitir la interconexión entre un PBX de la UNAM (NEC NEAX-7400) y un Router (Gateway) a través de diferentes tipos de troncales: analógicas (FXO's) y digitales (E1's). Una vez lograda la conexión, los teléfonos sobre el router eran capaces de realizar llamadas no sólo a las extensiones del PBX, sino también hacia números telefónicos sobre Telmex. En la Figura 7-2 se ilustra el esquema de pruebas y la configuración realizada sobre el router.

Nota: *El router se configuró para enviar los dígitos del número marcado sobre la troncal analógica para el caso cuando se quisiera llamar a una extensión sobre el PBX, y enviar los dígitos por la troncal digital E1 en caso de querer llamar hacia Telmex. El PBX al recibir los dígitos de la extensión o número telefónico marcados desde un teléfono sobre el router, enrutaba la llamada por el camino más adecuado según su forma normal de operación. Por otra parte, cuando se quería realizar una llamada desde el PBX (sistema telefónico tradicional) hacia un teléfono sobre el router, se marcaba el número deseado pero antecedido el dígito líder *8 a fin de indicarle al PBX la troncal o ruta por donde debía enviar la llamada hacia el router (en este caso, se podía usar tanto la troncal analógica como la digital según la ocupación de las mismas). En caso de querer llamar desde Telmex, se marcaba a un número DID (Direct Inward Dial) asociado al PBX y éste se encargaba de enrutar la llamada hacia el lugar correcto. El sistema era capaz de realizar tanto transferencias como conferencias de llamadas, solo que usando los recursos del PBX.*

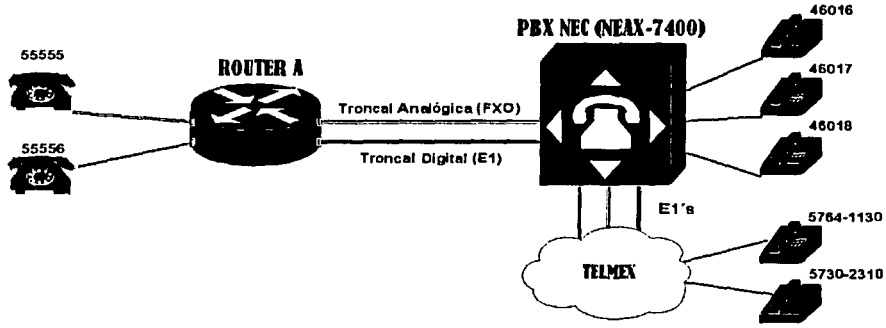


Figura 7-2: Comunicación PBX/Gateway a través de varios tipos de troncales.

ROUTER-A

```
Current configuration:
!
version 12.0
service password-encryption
!
hostname Router-A
!
enable password 7 0103140B4D1B140037
!
controller E1 2/0
 framing NO-CRC4
 clock source internal
 ds0-group 0 timeslots 1-30 type r2-digital r2-compelled
 cas-custom 0
   country telmex use-defaults
   category 2
   answer-signal group-b 1
!
voice-port 0/0
!
voice-port 0/1
!
voice-port 1/0
!
voice-port 1/1
!
interface Ethernet0/0
 ip address 132.248.10.254 255.255.255.0
!
ip classless
no ip http server
ip route 0.0.0.0 0.0.0.0 Ethernet0/0 name Default_Route
!
dial-peer voice 1 pots
 destination-pattern 55555
 port 0/0
!
dial-peer voice 2 pots
 destination-pattern 55556
 port 0/1
!
dial-peer voice 3 pots
 destination-pattern 4....
 port 1/0
 forward-digits all
!
dial-peer voice 4 pots
 destination-pattern 9........
 port 2/0:0
 forward-digits all
!
```

7.3 Comunicación PBX/PBX Usando la Red IP

En esta prueba se conectaron dos PBX's NEC ubicados sobre el mismo campus universitario a través de la red de datos IP (ver Figura 7-3). Aun cuando la prueba resultó exitosa fue un tanto limitada, pues no se logró una transparencia en las facilidades de usuario (call-forward, call.back, etc) debido a que no se contaba con tarjetas de voz E1/ISDN tanto sobre los routers como en los PBX's, que permitiera hacer uso de la señalización QSIG, básica para este tipo de cuestiones.

Los PBX's estaban configurados para rutear las llamadas a través de la red de datos IP para el caso de llamadas entre extensiones. Sin embargo, el plan de ruteo de los PBX's era tal que si alguno de ellos se quedaba momentáneamente sin conexión hacia Telmex, empezaba a usar los recursos del otro PBX (a través de la red IP) a fin de acceder hacia la red de Telmex.

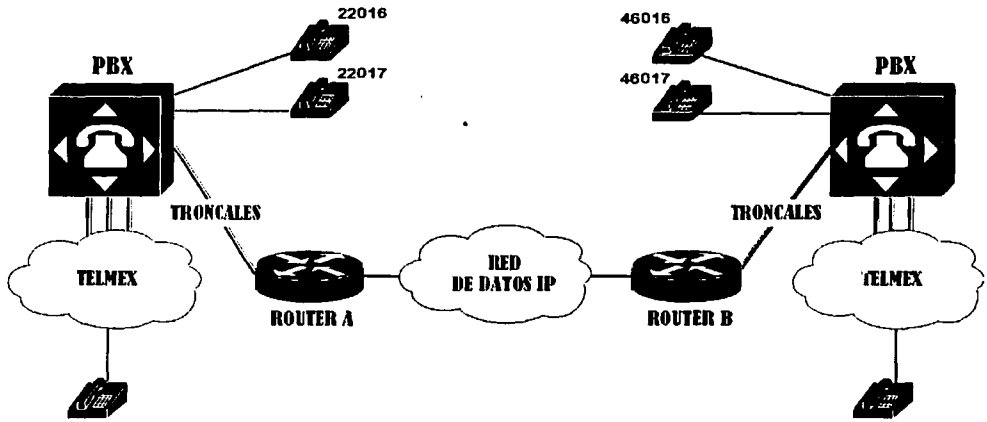


Figura 7-3: Comunicación PBX/PBX a través la red de datos IP.

7.4 Comunicación Telefonía-IP / PSTN

Esta prueba es prácticamente una réplica del sistema de Telefonía-IP que se instaló para la comunicación telefónica entre los colaboradores del Sr. Rector. Ver el Capítulo 6 donde se describe a detalle tal esquema.

7.5 Enlace entre Dos Sistemas de Telefonía-IP

En esta prueba se interconectaron dos sistemas de Telefonía-IP, a saber: el ***Sistema Telefónico NBX de 3com*** y el ***Sistema Call-Manager de Cisco*** (ver Figura 7-4). El propósito de esta conexión era saber hasta que grado podían interactuar estos dos sistemas (apego a los estándares) y conocer mejor las opciones de ruteo de llamadas de ambos. La siguiente lista presenta algunas característica del sistema implementado:

- Uso de un Gatekeeper para la intercomunicación de los sistemas a nivel H.323.
- Conexión de los sistemas a la red telefónica tradicional mediante el uso de troncales analógicas y/o digitales (constituyendo la segunda vía de intercomunicación posible entre los sistemas).
- Definición de planes de ruteo sobre cada sistema de Telefonía-IP a fin de usar rutas alternas para completar una llamada en caso de fallar la ruta principal de acceso.

Nota: Durante el desarrollo de la prueba se puso en evidencia la falta de interoperabilidad entre los sistemas dentro de varios renglones. Por una parte, los IPPhones y SoftPhones pertenecientes a uno de los sistemas no podían registrarse y operar sobre el otro sistema. Además, fue necesario usar un Gatekeeper externo para poder intercomunicarlos a nivel IP. Lo anterior nos habla de una falta de normalización de los estándares sobre las soluciones de Telefonía-IP en el mercado.

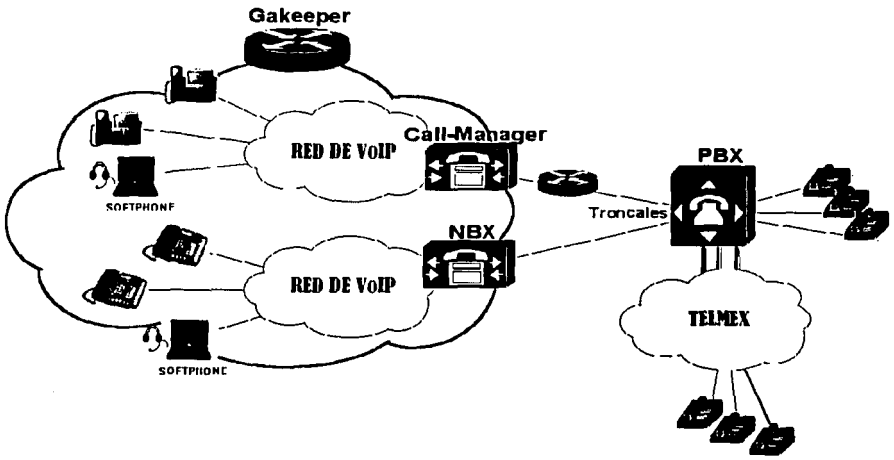


Figura 7-4: Comunicación entre dos sistemas de Telefonía-IP.

7.6 Red Local de VoIP Mediante H.323

El diseño y construcción de esta red local de VoIP fue la antesala para que la UNAM decidiera participar en el proyecto de la ***Red Nacional e Internacional de VoIP*** descrita en el capítulo 6. La filosofía que se siguió para el diseño e implementación esta red fue la misma que fue expuesta para la Red Nacional de VoIP, es decir:

- Uso de un Gatekeeper (GK_{UNAM}) para resolver las peticiones de llamadas de VoIP a nivel local.
- Integración de cualquier sistema de VoIP sublocal (presente en alguna Facultad o Instituto) mediante su conexión H.323 al GK_{UNAM}.
- Integración de la Red Telefónica Conmutada de la UNAM a la Red de VoIP mediante la conexión de un PBX NEC a un Gateway (Router 3660) a través de troncales analógicas y digitales.
- Acceso a la Red de VoIP desde la Red Telefónica Conmutada Universitaria marcando el dígito líder ✱8.
- Conexión de Terminales Netmeeting (de Microsoft) a la Red de VoIP, y de ésta a la Red Telefónica Conmutada de la UNAM
- Posibilidad de realizar conferencias haciendo uso de los recursos de los PBX's.

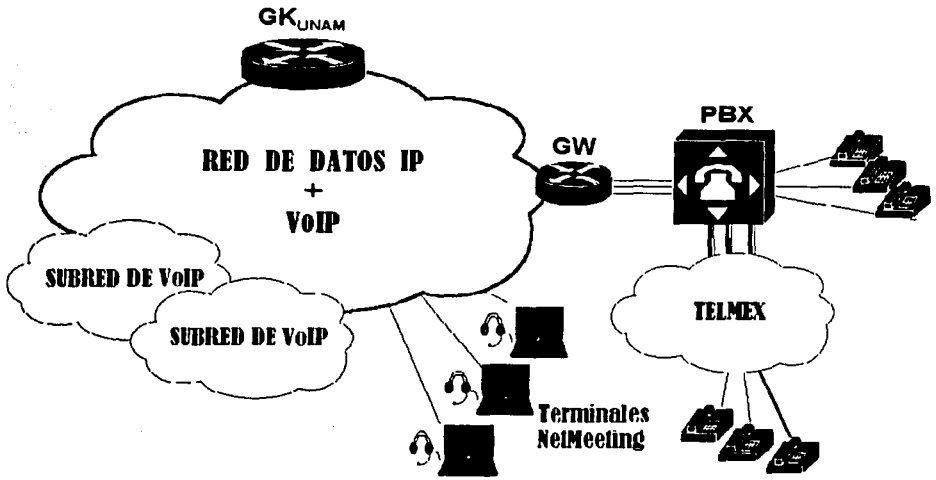


Figura 7-5: Red Local de VoIP mediante H.323 (mediante la conexión PBX's/Gateway's/Gatekeeper y la marcación con el dígito líder ✱8).

7.7 La Red Telefónica de la UNAM y sus Retos

De todos es conocido que la Red Telefónica de la UNAM tiene en puerta varios retos que enfrentar a mediano plazo. Por una parte, existe la necesidad de buscar una alternativa a la infraestructura actual de PBX's NEC debido a que las tarjetas de extensiones y troncales son muy caras y el proveedor de las mismas parece estarse quedando fuera del mercado.

Por otra parte, existe la necesidad de buscar una mejor alternativa para llevar el servicio de telefonía a dependencias de la UNAM externas al campus de Cd. Universitaria. Entre tales instituciones están las Preparatorias, las ENEP's y los CCH's. La forma actual de llevar el servicio de telefonía y datos a tales instituciones es contratar líneas dedicadas separadas a las de datos y recibirlas en un MUX para su descanalización. Sin embargo, se ha podido constatar que esta no es una buena solución debido a los costos que implica.

Aunado a lo anterior, está surgiendo un interés creciente de las Dependencias, Institutos y Facultades de la UNAM por implementar sus propias redes telefónicas. En varios casos están pensando implementar alguno de los nuevos sistemas de Telefonía-IP (ya sean IP-PBX's o Servidores de Comunicaciones Telefónicas), y unirse al resto de la red telefónica de la UNAM a la manera de células de VoIP.

Ante estas y otras circunstancias, hay la necesidad de investigar las soluciones tecnológicas actuales a fin de enfrentar los retos de un futuro cercano y permitir una red telefónica en la UNAM que siga siendo funcional y eficiente. En este sentido, la evaluación de las tecnologías de Telefonía-IP tiene una importancia innegable en estos momentos.

El objetivo es seguir contando con un Sistema Telefónico integrado (con capacidad de operar en red y donde las facilidades de usuario sean transparentes a lo largo de toda la red), a demás de ser escalable, funcional y eficiente.

7.8 Evaluación de Algunas Soluciones de Telefonía-IP en el Mercado

Como parte de los esfuerzos que se están haciendo actualmente para buscar soluciones a los problemas y retos en la comunicación telefónica, se están evaluando varias de las soluciones de Telefonía-IP existentes actualmente en el mercado y saber de una vez por todas si pueden ser de utilidad. En tal sentido, es menester contar con un esquema de pruebas para la evaluación de las mismas.

7.8.1 Soluciones de Telefonía-IP en el Mercado

Las tecnologías y soluciones de Telefonía-IP más importantes en el mercado (mejor conocidas con por el nombre de LAN-Telephony), y que ya han sido evaluadas (ver la Figura 7-6) son:

- ***Servidores de Comunicaciones:***
  - *Cisco (AVVID – Call Manager)*
  - *3com (NBX)*
- ***IP-PBX's:***
  - *Avaya (Definity)*
  - *Siemens (HiPath)*
  - *Mitel (MN-3300)*
  - *Alcatel*

Figura 7-6: Soluciones de Telefonía-IP ya evaluadas.

7.8.2 Esquema de Pruebas Propuesto (Solución de AVAYA)

A continuación se expone un conjunto de características y funcionalidades que se desearía probar o conocer más a fondo para la solución de VoIP de AVAYA:

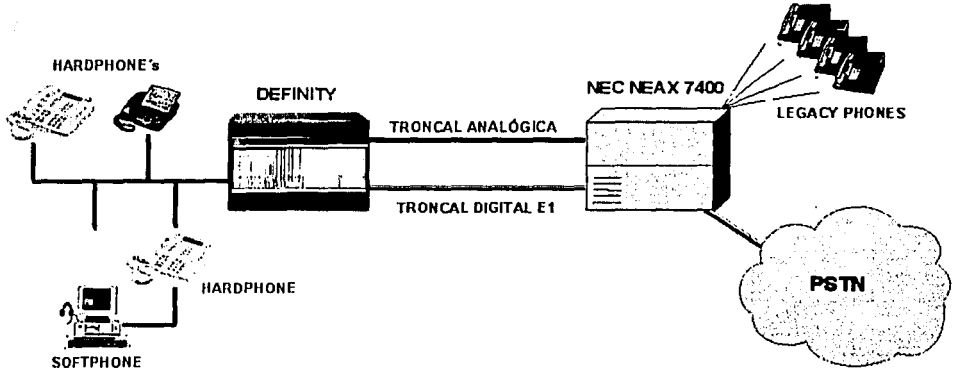
1) Gama de funcionalidades de los IP-Phones (Hardphones y Softphones):

- *Amigabilidad (facilidad en el uso de las teclas y/o softkeys para realizar diferentes funciones de usuario).*
- *Redial (Last Number Dialed).*
- *Call Forward (internal/external).*
- *Follow me.*
- *Call Park.*
- *Hold/Resume.*
- *Music on Hold.*
- *Speaker.*
- *PickUp.*
- *HuntGroups.*
- *Directorio telefónico integrado.*
- *Mostrar en el display el nombre del llamante.*
- *Transferencia de llamadas (internal/external restrictions?).*
- *Conferencia tripartita.*
- *Speed calls definidas por el usuario.*
- *Capacidad multilíneas.*
- *Múltiples líneas aparentes (hacia otras extensiones).*
- *Caller ID information (ANI/DNIS).*
- *Lámpara para correo de voz.*
- *¿Tipos de fuentes de alimentación usados por los Hardphones?*
- *Posibilidad de conectar una PC a la LAN a través del IPphone (presencia de un puerto para la PC).*
- *Definición de features de los IP-Phones por parte del usuario (speed calls, call forward, etc).*
- *Direccionamiento IP para IPphones a través de un servidor DHCP.*
- *Echo Cancellation.*
- *Control de volumen (timbrado/voz)*
- *Llamada por nombre o número.*
- *Firmware actualizable.*
- *Features adicionales.*

2) Features del sistema de VoIP

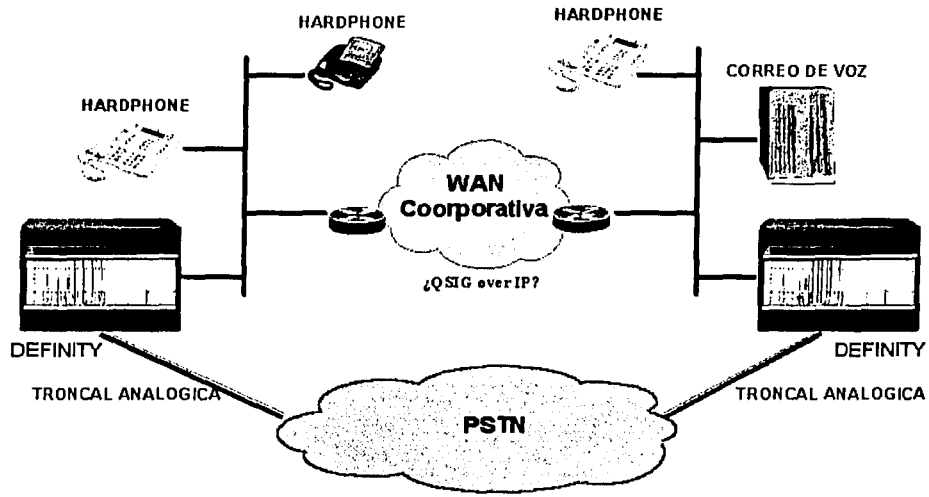
- *Interoperabilidad con PBX NEC (NEAX 7400) y/o PSTN a través de troncales digitales E1.*
- *Interoperabilidad con PBX NEC (NEAX 7400) y/o PSTN a través de troncales analógicas.*

INTEROPERABILIDAD CON EL PBX NEC



- *Escalabilidad y transparencia de funciones sobre una red de PBX's IP (funcionalidad Gatekeeper/Gateway, Redundancia, QSIG IP, cluster de sistemas de VoIP).*
- *Soporte a estaciones H.323 de terceros (cumplimiento con el estándar H.323).*
- *Capacidad para interoperar con Gatekeppers/Gateways de terceros.*
- *Definición del path (troncal) de salida de una llamada en base a la clase de servicio del usuario (COS) y/o restricciones del sistema (COR).*
- *Definición de VLAN's con objeto de aislar la red de VoIP de la red de datos normal (broadcast), en caso de que los IPphones cuenten con un puerto para PC.*
- *Definición de códigos de cuenta.*
- *Capacidad para recibir (mandar) el Caller ID.*
- *Conexión de teléfonos analógicos/digitales normales (incluso fax).*
- *Esquemas de compresión soportados (G.711, G.723.1, G.729 A/B).*
- *Marcaciones y conversaciones simultáneas (uso de recursos: DSP's y DTMF's).*
- *Densidad de puertos.*

TRANSPARENCIA DE SERVICIOS Y FEATURES SOBRE UN RED DE IP PBX´s



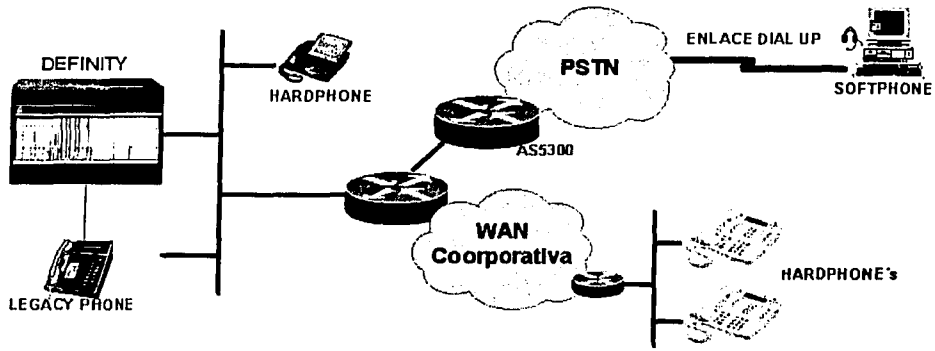
3) SoftPhones

- *Conexión de softphone's al sistema de VoIP a través de la WAN corporativa.*
- *Conexión de softphone's al sistema de VoIP a través de enlaces Dial Up.*

4) Esquemas de Compresión y QoS

- *Probar el sistema de VoIP a lo largo de la LAN y/o WAN, checando los diferentes esquemas de compresión (G711, G723, G729, etc) y la preservación de las features.*
- *Comportamiento del sistema de VoIP sobre una nube VPN.*
- *Probar la QoS ofrecida en caso de contar con switches relacionados.*
- *Probar la QoS sobre una red congestionada (inyección de tráfico a la red de datos a través del generador de tráfico Smart Bits).*

IPPHONES SOBRE LA WAN Y LA PSTN



5) Sistema de Correo de Voz

- *Centralized Voice Mail.*
- *Sistema de mensajeria unificada (voz, emails, fax y pagers)*

6) Administración y monitoreo del sistema de VoIP y sus componentes

- *Interfaz de administración (Http, telnet, puerto de consola RS232, etc).*
- *Capacidad para monitorear el estado de los IPphones (registrado, desocupado, en llamada, etc).*
- *Registro automático de los IPphones en el sistema de VoIP después de que éste último ha estado ausente durante algún tiempo en la red.*
- *Monitoreo del performance del sistema.*
- *Sistema de alarmas.*
- *Registro detallado de llamadas o CDR (tarificación de llamadas).*
- *Backups de la base de datos.*
- *Actualización de la versión del sistema de VoIP.*

7) Esquemas de seguridad usados

- *Encriptación de la información en su paso por la red (seguridad contra sniffers) ?*
- *Uso de http en la administración del sistema?*
- *Definición de código de bloqueo para la realización de llamadas desde el IPphone, según lo desee el usuario?*

7.8.3 Esquema de Pruebas Propuesto (Solución de MITEL)

A continuación se expone un conjunto de características y funcionalidades que se desearía probar o conocer más a fondo para la solución de VoIP de MITEL:

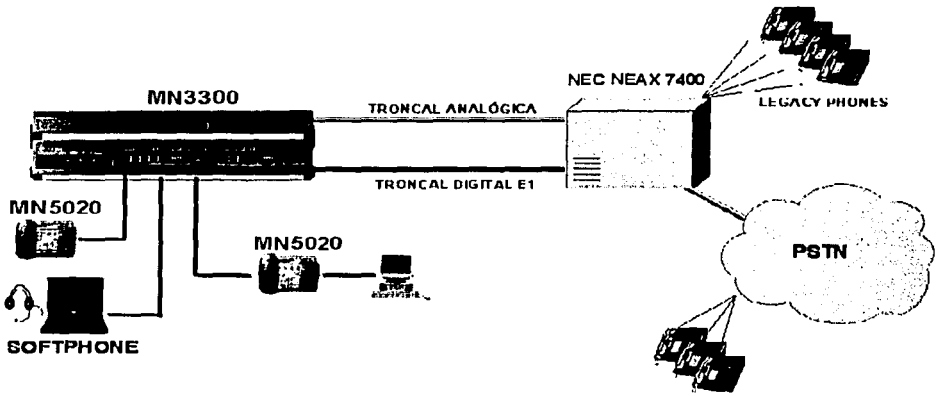
1) Gama de funcionalidades de los IPphones y Softphones:

- *Amigabilidad (facilidad en el uso de las teclas y/o softkeys para realizar diferentes funciones de usuario).*
- *Redial (Last Number Dialed).*
- *Call Forward (internal/external).*
- *Follow me.*
- *Call Park.*
- *Hold/Resume.*
- *Music on Hold.*
- *Speaker.*
- *PickUp.*
- *HuntGroups.*
- *Directorio telefónico integrado.*
- *Llamada por nombre o número.*
- *Mostrar en el display el nombre del llamante.*
- *Transferencia de llamadas.*
- *Conferencia tripartita.*
- *Speed calls.*
- *Capacidad multilíneas.*
- *Múltiples líneas aparentes (hacia otras extensiones).*
- *Caller ID information (ANI/DNIS).*
- *Lámpara para correo de voz.*
- *Tipos de fuentes de alimentación usados por los IPphones*
- *Posibilidad de conectar una PC a la LAN a través del IPphone (presencia de un puerto para la PC).*
- *Definición de features del IPphone por parte del usuario (speed calls, call forward, etc).*
- *Direccionamiento IP para IPphones a través de un servidor DHCP.*
- *Echo Cancellation.*
- *Control de volumen (timbrado/voz)*
- *Firmware actualizable.*
- *Features adicionales.*

2) Features del sistema de VoIP

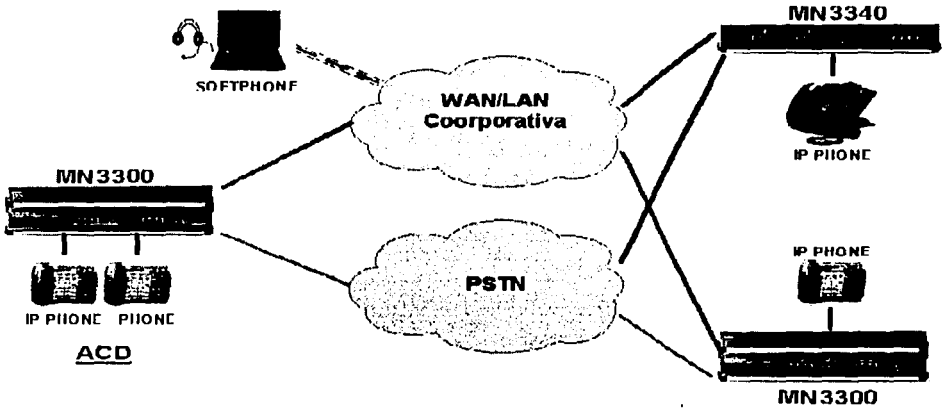
- *Interoperabilidad con PBX NEC (NEAX 7400) y/o PSTN a través de troncales digitales E1.*
- *Interoperabilidad con PBX NEC (NEAX 7400) y/o PSTN a través de troncales analógicas.*

INTEROPERABILIDAD CON EL PBX-NEC



- *Escalabilidad y transparencia de funciones y servicios sobre una red de PBX's MITEL (¿Redundancia, MSDN/DPNSS, QSIG IP, cluster de sistemas de VoIP?).*
- *Soporte a estaciones H.323 de terceros (cumplimiento con el estándar H.323).*
- *Capacidad para interoperar con Gatekeppers/Gateways de terceros.*
- *Flexibilidad en la definición y elección de la ruta de salida para una llamada externa al sistema (COS, COR, tenant, multipath).*
- *Definición de VLAN's con objeto de aislar la red de VoIP de la red de datos normal (broadcast), en caso de que los IPphones cuenten con un puerto para PC.*
- *Definición de códigos de cuenta.*
- *Capacidad para recibir (mandar) el Caller ID.*
- *Conexión de teléfonos analógicos/digitales normales (incluso fax).*
- *Esquemas de compresión soportados (G.711, G.723.1, G.729).*
- *Marcaciones y conversaciones simultáneas (uso de recursos: DSP's y DTMF's).*
- *Densidad de puertos.*

TRANSPARENCIA DE SERVICIOS Y FEATURES SOBRE UN RED DE ICP's (a nivel TDM e IP)



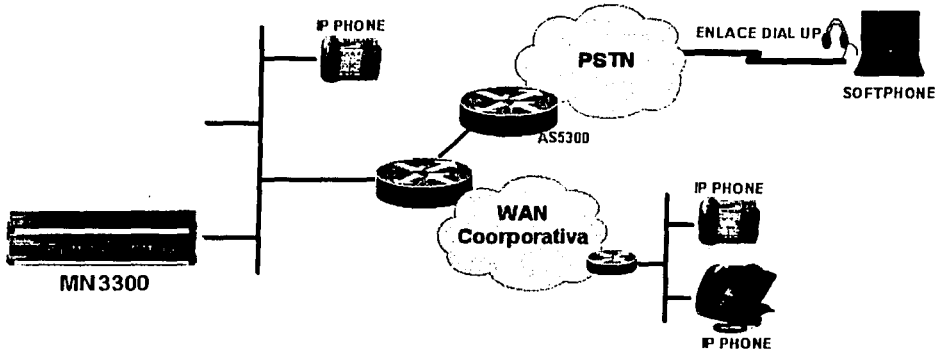
3) Softphones

- *Conexión de softphone's al sistema de VoIP a través de la WAN corporativa.*
- *Conexión de softphone's al sistema de VoIP a través de enlaces Dial Up.*

4) Esquemas de compresión y QoS

- *Probar el sistema de VoIP a lo largo de la LAN y/o WAN, checando los diferentes esquemas de compresión (G711, G723, G729, etc) y la preservación de las features.*
- *Comportamiento del sistema de VoIP sobre una nube VPN.*
- *Probar la QoS ofrecida en caso de contar con switches relacionados.*
- *Probar la QoS sobre una red congestionada (inyección de tráfico a la red de datos a través del generador de tráfico Smart Bits).*

IPPHONES SOBRE LA WAN Y LA PSTN



5) *Sistema de Correo de Voz*

- *Centralized Voice Mail.*
- *Sistema de mensajería unificada (voz, emails, fax y pagers)*

6) *Administración y monitoreo del sistema de VoIP y sus componentes*

- *Interfaz de administración (Http, telnet, puerto de consola RS232, etc).*
- *Capacidad para monitorear el estado de los IPphones (registrado, desocupado, en llamada, etc).*
- *Registro automático de los IPphones en el sistema de VoIP después de que éste último ha estado ausente durante algún tiempo en la red.*
- *Monitoreo del performance del sistema.*
- *Sistema de alarmas.*
- *Registro detallado de llamadas o CDR (tarificación de llamadas).*
- *Backups de la base de datos.*
- *Actualización de la versión del sistema de VoIP.*

7) *Esquemas de seguridad usados*

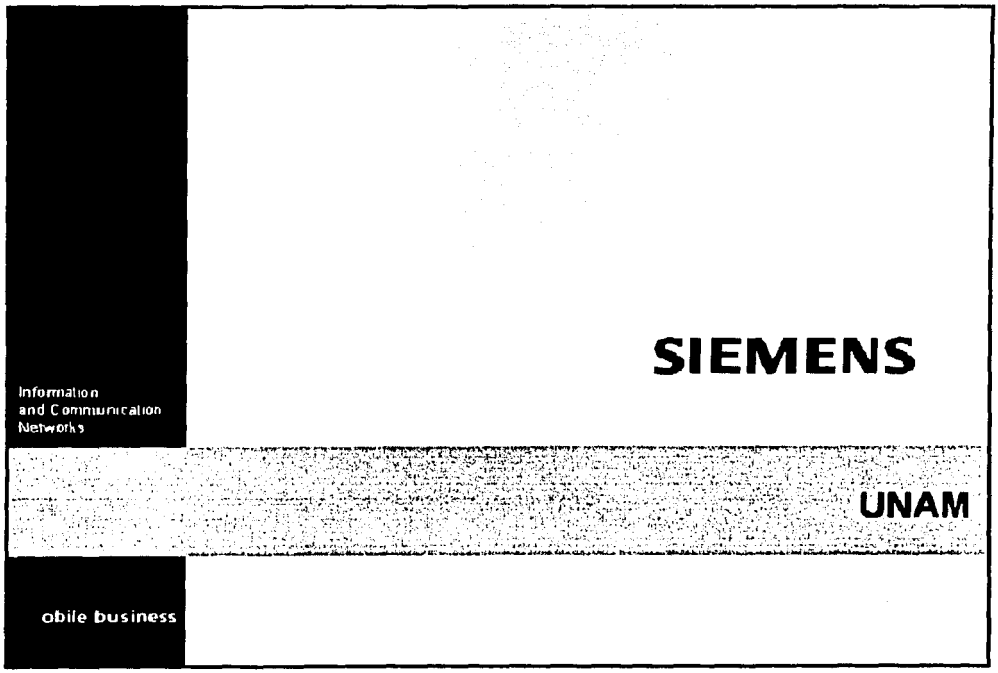
- *Encriptación de la información en su paso por la red (seguridad contra sniffers) ?*
- *Uso de http en la administración del sistema (¿Código rojo, Nimda?)*
- *Definición de código de bloqueo para la realización de llamadas desde el IPphone, según lo desee el usuario?*

8) Aplicaciones (Call Center, CTI, IVR, Mensajería Unificada, etc)

- *Integración de Aplicaciones CTI.*

7.8.4 Esquema de Pruebas Propuesto (Solución de SIEMENS)

A continuación se expone un conjunto de pruebas que SIEMENS propuso a la UNAM a fin de mostrar las características y funcionalidades de su solución, a propósito del interés del Instituto de Ingeniería por instalar un sistema de Telefonía-IP sobre sus instalaciones:



Integra

SIEMENS

Descripción del Proyecto

Red Corporativa "UNAM"

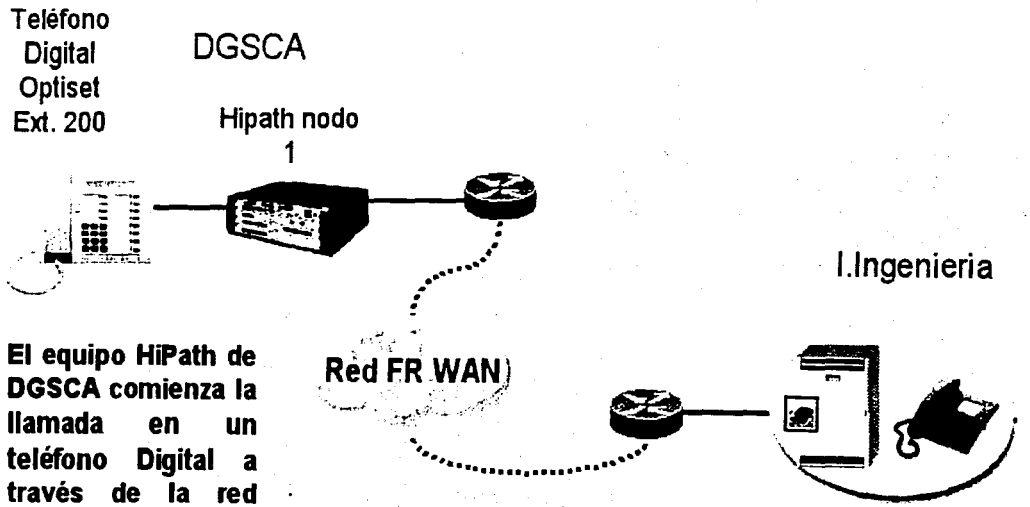
Siemens ha desarrollado una propuesta técnica integrando una red convergente de voz y datos basado en una plataforma Cisco e integrando su nueva solución de Voz a través de IP basado en sistemas HiPath.

- Infraestructura de datos.
- Infraestructura de Voz en localidades remotas.
- Interconexión de voz a través de IP Trunking.

Protocolo 1:

SIEMENS

Comunicación Teléfono Digital a Teléfono Analógico



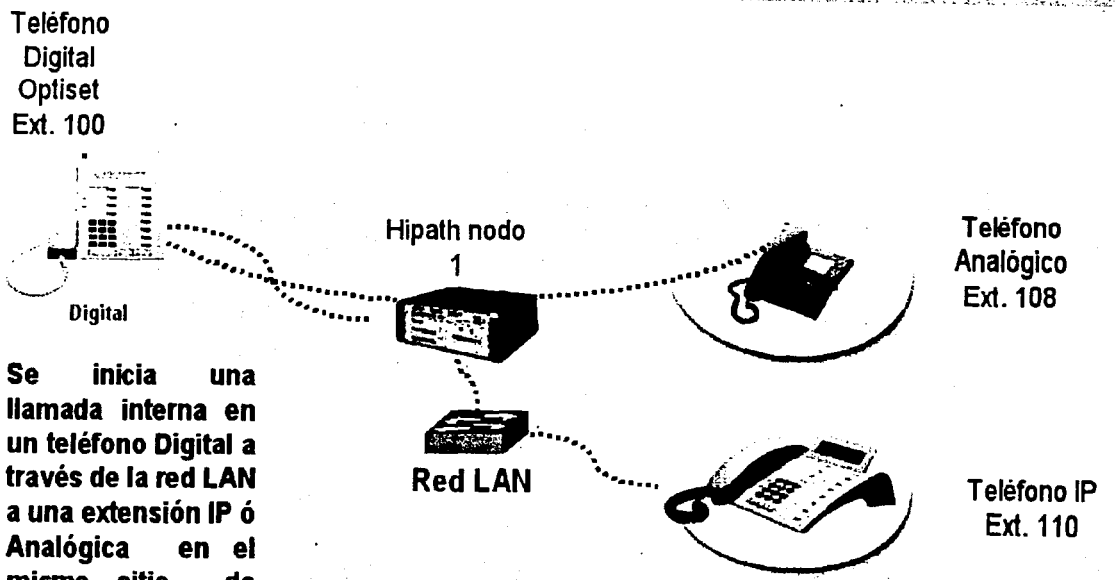
El equipo HiPath de DGSCA comienza la llamada en un teléfono Digital a través de la red WAN a nodo ingenieria en donde la recibe tambien un equipo HiPath y lo envia a un teléfono Analógico.

Integra

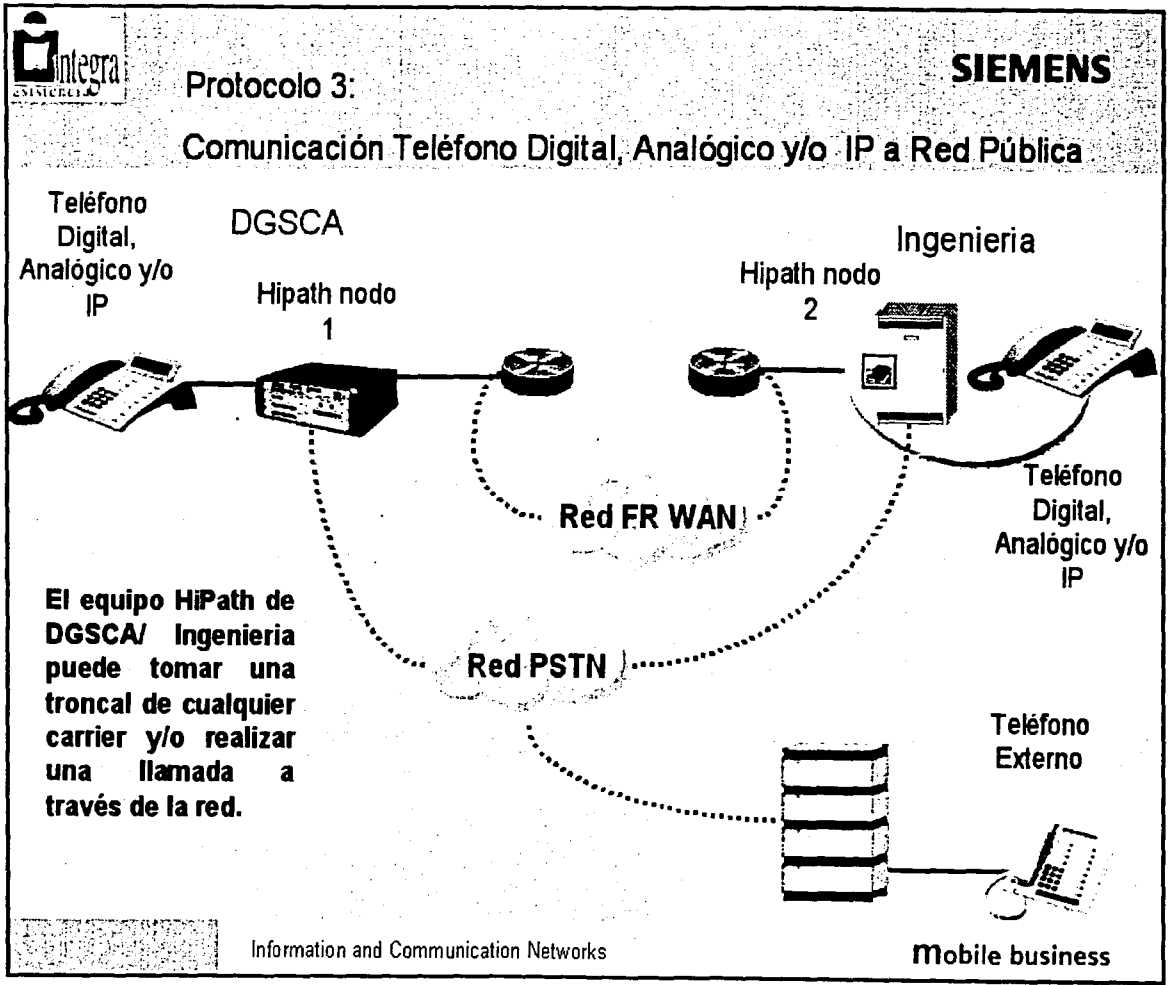
Protocolo 2:

SIEMENS

Comunicación Interna Teléfono Digital a Teléfono IP ó Analógico



Se inicia una llamada interna en un teléfono Digital a través de la red LAN a una extensión IP ó Analógica en el mismo sitio de Ingenieria
Ejemplo: Ext. 100 a Ext. 108 o 110

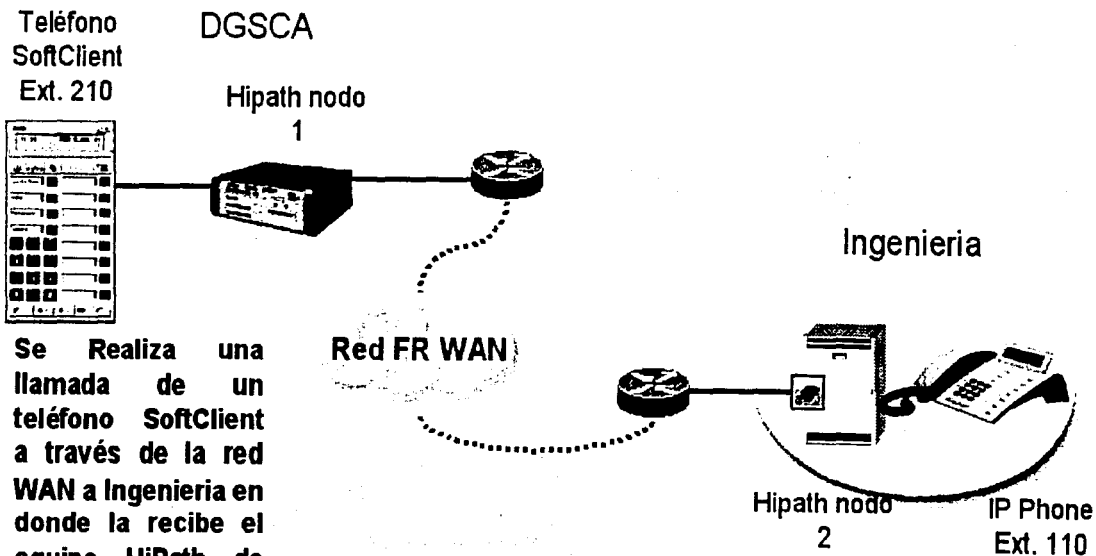

Protocolo 3:
SIEMENS
Comunicación Teléfono Digital, Analógico y/o IP a Red Pública
Teléfono Digital, Analógico y/o IP
DGSCA
Hipath nodo 1
Ingenieria
Hipath nodo 2
Red FR WAN
Teléfono Digital, Analógico y/o IP
El equipo HiPath de DGSCA/ Ingenieria puede tomar una troncal de cualquier carrier y/o realizar una llamada a través de la red.
Red PSTN
Teléfono Externo
Information and Communication Networks
Mobile business

Integra

SIEMENS

Protocolo 4:

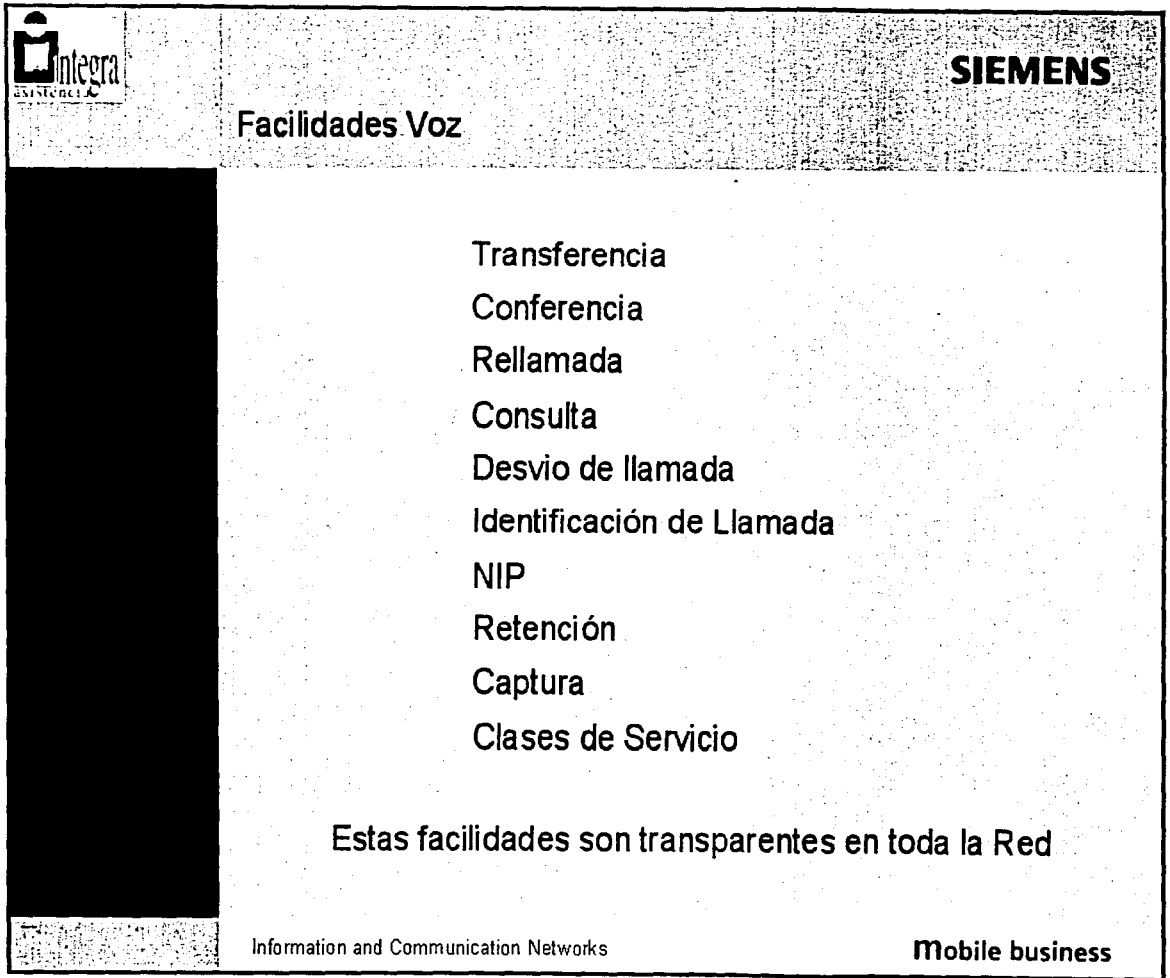
Comunicación Teléfono SoftClient a Teléfono IP



Se Realiza una llamada de un teléfono SoftClient a través de la red WAN a Ingenieria en donde la recibe el equipo HiPath de DGSCA y un teléfono OptiPoint IP

Information and Communication Networks

Mobile business



7.9 Proyecto: Red de VoIP Mediante SIP

La ***Red de VoIP Nacional e Internacional*** mediante el protocolo H.323, ha dejado ver ciertas debilidades en el uso de H.323 como protocolo de señalización y control de llamadas. Problemas de escalabilidad y altos retardos en la señalización de las llamadas son los problemas más comunes.

Como resultado de lo anterior, en la UNAM se están haciendo los preparativos para el diseño e implementación de una nueva red de VoIP basada en el protocolo de señalización y control de llamadas SIP (Session Initiation Protocol). Los objetivos, alcances, diseño e implementación son muy parecidos a los de la Red Nacional e Internacional de VoIP mediante H.323; solo que se obtendrán los beneficios y ventajas asociadas a este mejor protocolo de señalización basado enteramente en una arquitectura distribuida cliente/servidor con terminales inteligentes y adaptadas a la Web. En las Figuras 7-7 y 7-8 se ilustra un boceto de este proyecto.

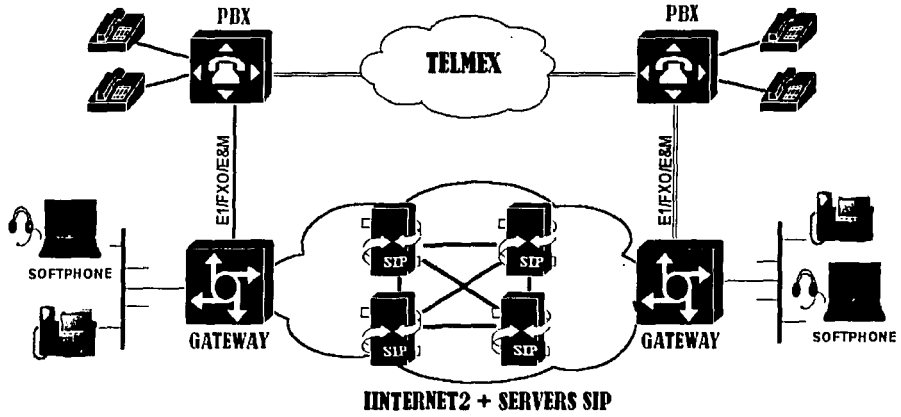


Figura 7-7: Dos usuarios sobre la propuesta de SIP (a base de ServersProxy SIP)

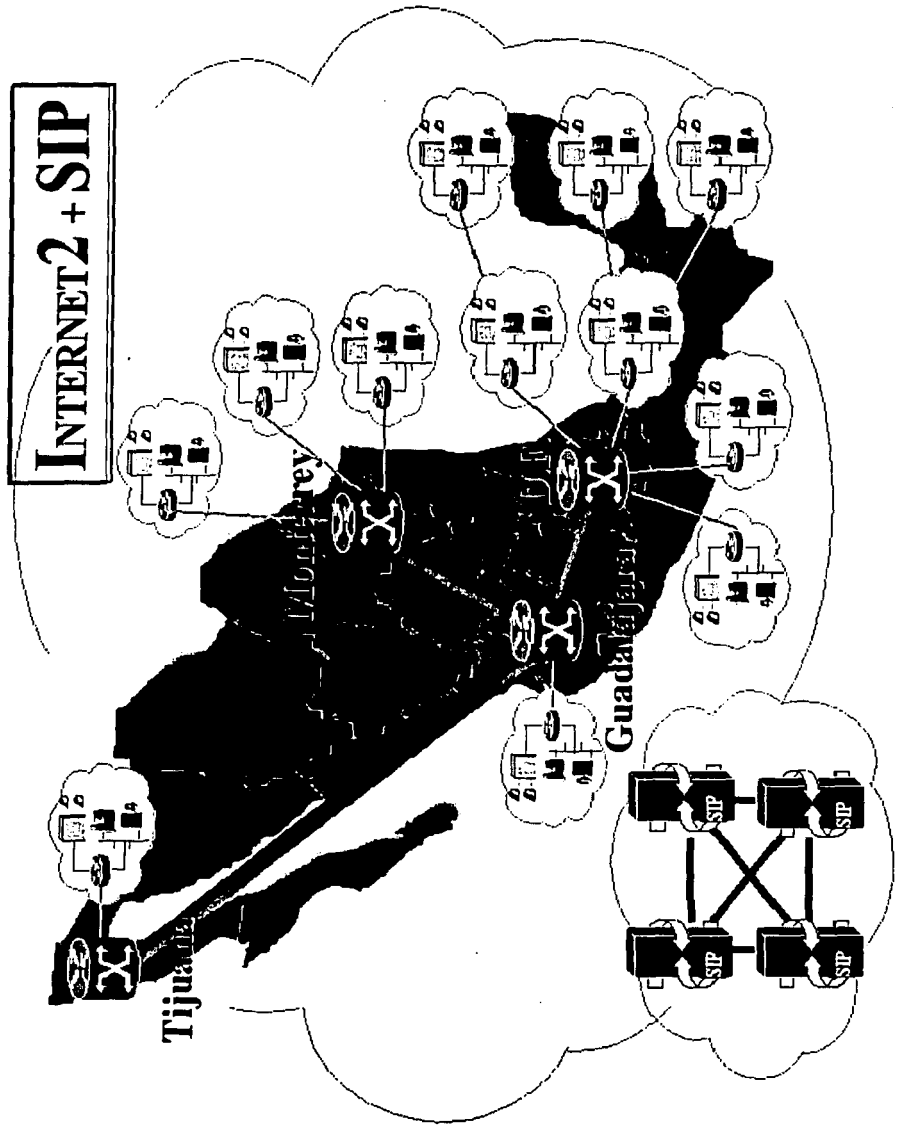


Figura 7-7: Red Nacional de VoIP mediante SIP (basada en Proxy Servers SIP).

Conclusiones:

En las secciones anteriores de este capítulo se han presentado algunas de las pruebas que se han realizado alrededor de las tecnologías de VoIP. La importancia de estas pruebas estriba en el bagaje de conocimientos que se logró atesorar y que en su momento fueron esenciales para la implementación de algunos proyectos. La decisión de probar y conocer las soluciones de Telefonía-IP actualmente presentes en el mercado proporcionará alguna de las bases en la búsqueda de soluciones a los problemas que la UNAM enfrenta actualmente en cuanto a comunicaciones telefónicas se refiere.

BIBLIOGRAFÍA

- "Voice over IP Fundamentals", Jonathan Davidson, Editorial Ciscopress
- "Packetized Voice and Data Integration", Robert Caputo, Editorial McGraw-Hill
- "IP Quality of Service", Srinivas Vegesna, Editorial Ciscopress
- "Data and Computer Communications", William Stallings, Editorial Macmillan
- "Redes de Computadores", Uyless Black, Editorial Rama
- "Redes de Alta Velocidad", Jesús García Tomás, Editorial Rama