UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

VOZ SOBRE IP EN INTERNET 2
CASO: INTERCONEXIÓN ENTRE LOS NODOS UNAM-DGSCA Y LA UNIVERSIDAD A&M DE TEXAS (TAMU).

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

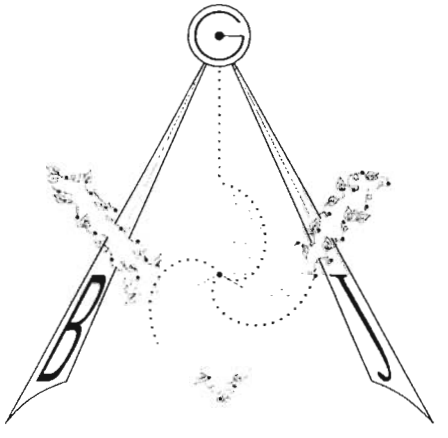
SÁNCHEZ SÁNCHEZ LUZ ESTELA

DIRECTOR: ING. NOÉ CRUZ MARÍN.

MÉXICO, D.F. 2005

DEDICATORIA

Esta tesis fué realizada en su totalidad
gracias al AMOR, ya que gracias a él
pude realizar un sueño más.



AGRADECIMIENTOS:

Al Gran Arquitecto Del Universo por darme la oportunidad de encontrar nuevamente la luz y la fortaleza para seguir adelante. Gracias.

A mi Madre, a mi Padre y a mi Hermano por su constante lucha y enseñanza a lo largo de mi vida, así como su incondicional apoyo y tolerancia. Gracias, recuerden que siempre estarán en mi corazón. Los Quiero Mucho.

A Semreh por guiarme hacia el camino de la verdad, así como tu gran Amor y Paciencia. ¡Ten'oio Amin Meluva Lle!
"This kind of certain, only comes just ones in lifetime"

A Hugo, Marco, Tomas, a mis amigos del Kung Fu por que gracias a ustedes aprendí a crecer, en especial a Eduardo, a los del Equipo de Triatlón por enseñarme a creer en mí y a los de DGSCA por compartir su conocimiento, a todos ellos por regalarme su hermosa amistad y apoyo incondicional.

A todo el Movimiento Buena Voluntad y en especial a Margarita por su constante lucha a mi lado. Sin ti no lo hubiera logrado, gracias. Te quiero Mucho.

:. Finalmente a Azul, gracias por existir :.

ÍNDICE

PREFACIO

La evolución en las formas de comunicación, por las cuales el hombre se comunicaba en primera instancia fueron sus manos, dibujos, su voz, etc., y conforme avanzó la tecnología, se fueron modificando éstas por medios más complejos. Comenzando el siglo XX el cambio fué mucho más rápido, se aplicaban nuevos tipos de tecnologías, desde las simples ondas de radio que rebotan en la atmósfera pasando por el telégrafo, el teléfono etc., hasta las actuales en las que en el hombre acorta distancias, desapareciendo éstas cada día más por medio de las redes de datos en la cual se pueden tener transferencias masivas de datos, charlas en tiempo real, así como videoconferencias. Donde las instituciones educativas buscan el contacto con estudiantes e investigadores a nivel nacional e internacional de forma inmediata, éste se hace mucho más cotidiano, por lo que, tratan de incrementar su productividad a través de la mejora en los medios de comunicación, ya sean por medios hablados o escritos en tiempo real, por lo que las instituciones invierten en la adquisición de tecnología e implementación de sistemas de comunicación en la cual intervienen los sistemas de Voz sobre IP.

Las instituciones de educación superior como la UNAM no son ajenas a esta evolución, ya que para lograr una formación óptima de sus alumnos, docentes e investigadores no solo nacionales si no también extranjeros, es necesario una comunicación continua y económicamente viable. Es por ello que las instituciones educativas requieren de este tipo de sistemas de comunicación de voz, para que los procesos de cooperación y generación de conocimiento se agilicen a medida que vayan avanzando a la par de tecnologías y redes enfocadas a la investigación como lo es Internet 2.

Debido a que las tecnologías de comunicaciones avanzan rápidamente, es común que cada día sea más necesario el interactuar de manera mucho más directa y de manera que se mantenga un flujo continuo de comunicación y así evitar confusiones ó incluso obtener respuestas mucho más claras y concisas por medio de sistemas de voz en tiempo real.

El desarrollo de esta tesis tiene como objetivo principal lograr la conexión de los nodos UNAM-DGSCA y la Universidad A&M de Texas (TAMU) por medio de un enlace de VoIP que mantenga en constante comunicación a ambas universidades de manera confiable a través de los medios de comunicación ya desarrollados en las redes de alto rendimiento de índole educativo y de investigación desarrolladas a nivel mundial. Utilizando "Internet 2".

La situación es la de desarrollar e implantar un sistema de voz por IP el cual sirva para organizar y actualizar de manera eficiente los sistemas de voz en las redes de datos manteniendo un rendimiento idóneo en la realización de llamadas por medio del IP ya sean a números telefónicos IP o a números telefónicos analógicos pertenecientes a ambas universidades aprovechando las capacidades del sistema o sistemas para entablar comunicación con otras universidades a través de la Voz sobre IP.

La tesis esta compuesta de seis capítulos, un anexo y un glosario que se describen de manera breve a continuación:

En el capítulo uno se observa de cerca la Telefonía tradicional, su organización, elementos que la conforman, nivel jerárquico, señalización y avance hasta nuestros días que fueron punto de partida para algunas de las tecnologías de datos de hoy en día.

El capítulo dos explora de manera básica las redes de datos, sus estándares, medios de acceso, tecnologías y diseño, idóneos para que en cualquier momento puedan viajar a través de ella cualquier tipo de aplicaciones sin que afecte su desempeño.

El capítulo tres proporciona una panorámica de los protocolos de comunicación, con los que se obtendrá una idea clara del comportamiento de las redes con la gama de protocolos TCP/IP y su relación con el capítulo quinto.

En el capítulo cuatro se describe el objetivo de Internet 2 a nivel mundial, observado un poco más de cerca la organización que rige los designios y avances de Internet 2 en México.

En el capítulo cinco se explica el funcionamiento de la Voz sobre IP, describiendo ampliamente su relación con la familia de protocolos TCP/IP y de manera más cercana con el protocolo IP, observando algunos de los protocolos de voz más detenidamente, de igual manera se abordan los diferentes protocolos y manejos del H.323, así como su posible sucesor SIP.

En el capítulo seis y último se observa la subred de telefonía IP que sirvió como antecedente a la voz sobre IP en la UNAM así como un análisis de las particularidades de RedUNAM y su la Red Telefónica Universitaria valorando la factibilidad de hacer posible la Interconexión entre los Nodos UNAM-DGSCA y la Universidad A&M de Texas (TAMU) a través de un enlace de voz sobre IP por medio del enlace a Internet 2 de la UNAM integrando así una solución robusta y con un crecimiento factible a futuro.

Además, se incluye un glosario, documentación que se desarrollo en la elaboración de la tesis como apoyo para la comprensión de la misma.

CAPÍTULO UNO

TELEFONÍA TRADICIONAL

1.1 Antecedentes históricos.

Una de las principales necesidades del hombre ha sido la comunicación oral, por lo que desde hace casi 127 años el hombre ha buscado la manera de lograr una comunicación a distancia, eficiente y rápida.

Gracias a las investigaciones en el campo de la física, electricidad y magnetismo se pudo lograr la transmisión de impulsos eléctricos llamada código Morse por medio de cables de cobre y con el surgimiento del telégrafo eléctrico, se realizaron las primeras comunicaciones a distancia. Sin embargo, no eran lo suficientemente rápidas y precisaban de un código adicional para poder lograr la comunicación. Utilizando el mismo principio se intentó transmitir la voz, pero debido a las muy variadas frecuencias y tonos en la voz humana hacia imposible su envío. Por lo que en 1876 después de años de investigación Alexander Graham Bell patentó su primer sistema telefónico, logrando la transmisión y recepción de la voz humana a distancia.

A partir de ese momento los servicios telefónicos empezaron a desarrollarse rápidamente, cientos de usuarios comenzaron a conectarse a la red. En un inicio las conexiones entre usuarios eran realizadas a través de centrales, las cuales eran operadas por personal que realizaba las interconexiones de manera manual, las líneas eran aéreas (sobre postes), poco a poco las líneas fueron sustituidas por cables subterráneos y centrales automáticas permitiendo el discado directo.

En los años 90's con la inserción de centrales computarizadas y teléfonos de discado por tonos cambio el aspecto del servicio. Éste se convirtió en algo dinámico, ágil y adaptado a las necesidades del nuevo mundo de actividades de fines del siglo XX. Así, con el desarrollo de las tecnologías afines a la electrónica y las telecomunicaciones, fue desarrollándose también el campo de la telefonía móvil.

Con la modulación digital, en la actualidad se utiliza la codificación de la voz mediante la presencia o ausencia de impulsos eléctricos, dando mayor confiabilidad, eficiencia y sobre todo flexibilidad a la transmisión de la voz. Sin embargo, hasta nuestros días la telefonía sigue una constante evolución.

1.2 Elementos de la Red Pública de Telefonía Conmutada (PSTN).

La Red Pública de Telefonía Conmutada (PSTN) ha evolucionado en todo el mundo desde que Alexander Graham Bell hizo la primera transmisión de voz sobre cableado en 1876. Pero antes de ver el estado actual de la PSTN y de qué depara para el futuro es importante comprender algunos aspectos básicos de ésta.

Actualmente la telefonía es mucho más completa, teniendo más elementos, dentro de los cuales destacan:

- ✓ Línea del abonado.
- ✓ Línea troncal.
- ✓ Central telefónica.
- ✓ Centrales de larga distancia.
- ✓ Centrales tandem.
- ✓ Plan de numeración.

Línea del abonado

La línea del abonado es el par de cobre en el cual fluye la información que corre desde la ubicación del abonado (usuario) hasta la central telefónica, constituyen un circuito o línea y las estaciones telefónicas se conocen como abonados (Fig. 1.1).

El abonado se identifica por un número. Este número esta compuesto por dos partes, la primera se identifica la central telefónica a la cual se encuentra conectado; en la segunda parte identifica el número del abonado dentro de esta central, así se pueden tener hasta 10,000 usuarios por oficina central.

Fig. 1.1 Diagrama Lógico de Conexión para una línea de abonado.

Línea troncal

Las troncales son aquellas líneas que se utilizan para conectar dos centrales (Fig. 1.2), la troncal tiene un ancho de banda mayor que la de una línea de abonado; la cantidad de líneas troncales entre centrales, está en función de la cantidad de comunicaciones efectivas entre centrales.

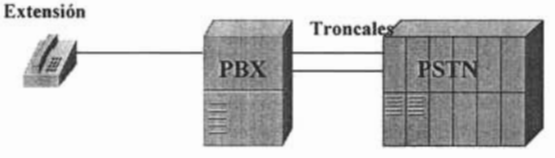


Fig. 1.2 Ejemplo de Diagrama de Conexión para líneas troncales.

Central telefónica

La existencia de las centrales telefónicas, es la de ahorrar el número de conexiones que deben efectuar desde los aparatos del abonado. La central telefónica es donde se dispone la organización de los abonados, así como la comunicación entre ellos, así mismo es conectada con otras centrales telefónicas teniendo una cobertura en una área determinada cada una de éstas. Si las centrales telefónicas no estuvieran conectadas entre sí, solamente los abonados pertenecientes a la misma área local se podrían comunicar.

Antes de continuar cabe mencionar que debe existir una jerarquía, debido a la cantidad de centrales existentes en una nación y su conexión con otras centrales a nivel mundial. Cabe destacar que éstas deben estar conectadas a una central telefónica primaria (tandem) que conecte a las centrales de nivel local. Cada central local depende de una y sólo una central primaria. Sin embargo de una central primaria dependen varias centrales locales. La misión primordial de la central primaria es la de conectar centrales

entre sí, cursando llamadas de tránsito, es decir, llamadas correspondientes de abonados que le son ajenas.

Al igual que con las centrales locales, sucede lo mismo con las primarias las cuales se conectan a una central de índole mayor. Esta central se denomina central secundaria. La función central de ésta es la de conectar centrales primarias entre sí, cursando llamadas de transito. Cabe mencionar que hay una tercer nivel llamado central nodal el cual tiene la misma función que la secundaria, solamente que ésta conecta centrales de índole secundario y cursa las llamadas entre ellas.

Centrales de larga distancia

Es el centro de conmutación que maneja la primera etapa de larga distancia. Siendo ésta la que empieza a comunicarse con otra central y así sucesivamente hasta alcanzar el número deseado. También en ésta se manejan las llamadas asistidas por la operadora.

Centrales Tandem

Las centrales Tandem son centrales de tránsito, es decir, sin abonados, a las que se le conectan otras centrales. Esto quiere decir que tiene la tarea de ser como un conmutador a nivel central. Se utilizan en áreas multicentrales para enrutar el tráfico de desbordamiento en las rutas directas entre las centrales locales del área multicentral; así también los tránsitos de Larga Distancia y la de llamadas locales en áreas extendidas. Una de las características de las centrales tandem es que no están jerarquizadas.

Plan de numeración

El objetivo del plan de numeración es asignar a cada abonado un número ID que determina su posición dentro de la red. El código de selección permite establecer la comunicación de un abonado con cualquier otro, sin importar su localización, incluso puede pertenecer a países diferentes.

1.2.1 Jerarquía de la red telefónica.

El gran número de usuarios y el alto tráfico que una red telefónica ha de soportar, hace que sea necesario el agruparlos por áreas geográficas y hacerlos depender de varias centrales de conmutación que tengan acceso entre sí o a través de otras. Aparece el concepto de jerarquía y dado que el número máximo de usuarios que una central admite es limitado, siendo mayor o menor, dependiendo de su categoría, es necesario una vez que ésta supera el concurso de más centrales de conmutación para atenderlos, y cuando el límite de estas centrales es alto, se necesita a su vez otras centrales de mayor nivel para gobernar la comunicación entre ellas.

En una red jerárquica se pueden dar varios niveles, pero cada central de un nivel depende solamente de otra de nivel superior, aunque la tendencia es conectar a más de una central por razones de seguridad (redundancia), asegurándose así el establecimiento de rutas entre usuarios del servicio telefónico.

Guiado por la distribución geográfica tenemos tres tipos de redes: las llamadas "urbanas", las "interurbanas" o de "larga distancia" y las "internacionales".

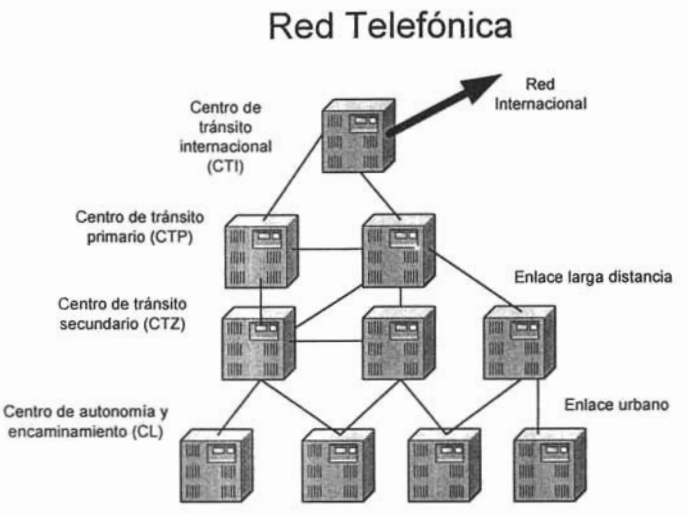


Fig. 1.3 Tipos y niveles de una red jerárquica.

1.3 Central de conmutación.

Éste se define como el conjunto de órganos de transmisión de tráfico, etapas de conmutación, medios de control y señalización en un nodo de la red que permite la interconexión de líneas de abonado y/u otros circuitos de telecomunicaciones, conforme requieran los usuarios. Este centro de conmutación pude ser público cuando los abonados son conectados directamente con la Red Telefónica Pública Conmutada (PSTN), o de índole privado (PBX) cuando la conexión se realiza por medio de una central con características similares pero de menor capacidad.

En términos generales el centro de conmutación está constituido por elementos que prestan las funciones de señalización, control y conmutación.

Una central se compone de dos subsistemas:

- ✓ Sistemas de Conmutación .
- ✓ Sistemas de Control.

El objetivo básico de la central telefónica es establecer el enlace entre los abonados (emisor y receptor) que desean establecer una comunicación; para ello debe disponer de los medios físicos, funciones y señalización necesarios para alcanzarlo con efectividad.

El sistema de conmutación es precisamente el conjunto de unidades y circuitos que constituyen el soporte físico de la conmutación. Cada vez que hay una petición de comunicación se debe seleccionar una ruta a través del conmutador. Este recorrido está formado por módulos y conmutadores, conocido como "vía de comunicación", ver Fig. 1.4.

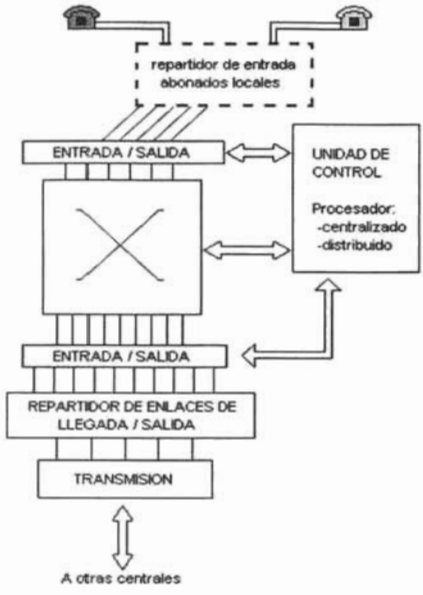


Fig. 1.4 Selección de la vía de comunicación.

Para realizar la constitución de esta vía, pueden hacer falta varios procesos de conmutación. Todas las operaciones necesarias para establecer la vía se realizan gracias al sistema de control, que es el responsable de la asignación de dispositivos libres y de la gestión del sistema de conexión entre módulos.

1.3.1 Fundamentos de los sistemas de conmutación.

En una red se distinguen los enlaces de entrada y salida de otras centrales, así como enlaces internos. Para conseguir mayor eficacia, el número de enlaces debe ser inferior al de abonados ya que no todos los abonados los utilizan simultáneamente. Por eso es necesario considerar en estos sistemas las llamadas etapas de "concentración" y "expansión", así como otras de distribución de los órganos de la central.

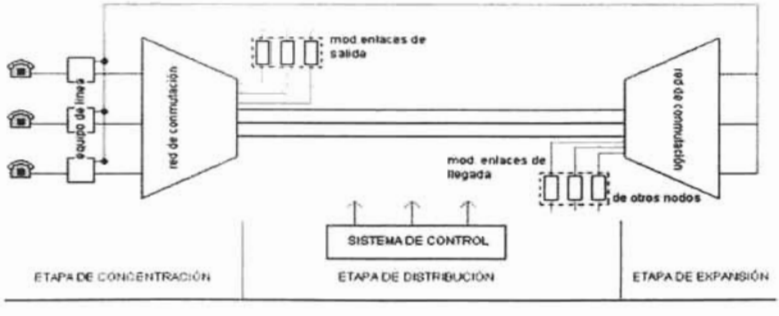


Fig. 1.5 Etapas de un sistema de conmutación.

Las etapas de concentración y expansión son muy similares, aunque hay algunas diferencias:

- ✓En las etapas de concentración el abonado que llama puede concertarse a cualquiera de los enlaces de salida.
- ✓En las etapas de expansión en cambio, el enlace de llegada se conecta sólo con el abonado receptor.

En las etapas de concentración se realiza la operación de búsqueda: cuando un abonado quiere afectar una llamada hay que buscar un enlace que se encuentre disponible. El número de entradas viene determinado por el de abonados, mientras que el de salidas lo está en función del tráfico que se origine hacia el exterior.

En las etapas de expansión, en cambio, se realiza una operación de selección: cuando una llamada entra en la central hay que seleccionar el abonado llamado entre todos los de la central.

En el módulo de usuario existen tantos equipos de línea como de usuario.

1.3.2 Multilíneas.

Estos son sistemas de conmutación sencillos, siendo sistemas multilíneas o KTS (Key Telephone System). Un sistema KTS permite conectar una serie de líneas telefónicas con un conjunto de extensiones telefónicas existentes en una pequeña empresa como se muestra en la Fig. 1.6, pero con la particularidad de permitir la captura de un enlace por cualquiera de las terminales (extensiones) conectadas, es decir, que las llamadas entrantes (de la PSTN) pueden ser atendidas en cualquier terminal, ya que en todos los equipos presentan una indicación acústica (timbre de llamada) y/o luminosa. De la misma manera, cualquier extensión puede tomar uno de los enlaces libres para realizar una llamada al exterior. No requiere operadora, y el número de extensiones es inferior a 50, además este tipo de sistemas tiene funciones muy reducidas.

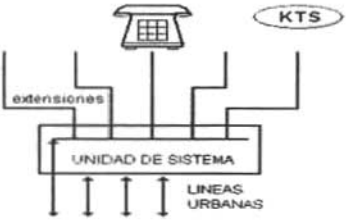


Fig. 1.6 Conexión de un sistema multilínea o KTS.

1.3.3 Central Privada de Conmutación (PBX).

Una central telefónica privada en realidad son PABX (Private Automatic Branch Exchange) actualmente a todos estos se les hace llamar PBX, los cuales realiza conmutación de circuitos, mantenimiento y métodos básicos de conmutación para brindar el servicio de telefonía a pequeñas áreas, con la posibilidad de prestar una gran cantidad de servicios y facilidades adicionales. Así mismo, estos sistemas integran comunicaciones de área amplia con equipos e interfases locales (T1, E1, ISDN, troncales análogas, teléfonos, teléfonos fijos inalámbricos). El desarrollo de las nuevas técnicas de

comunicación, tiende a integrar la transmisión y conmutación de voz y datos utilizando las mismas redes (redes multiservicios).

Son muy similares a las centrales públicas, excepto por que no incluyen algunas de sus funciones, al igual constan de sistemas de control y conmutación; evolucionado y ofreciendo servicios de tipo analógico y digital.

El PBX es un conjunto de elementos hardware, como por ejemplo procesadores, selectores, puertos de diversos tipos, etc. y elementos software.

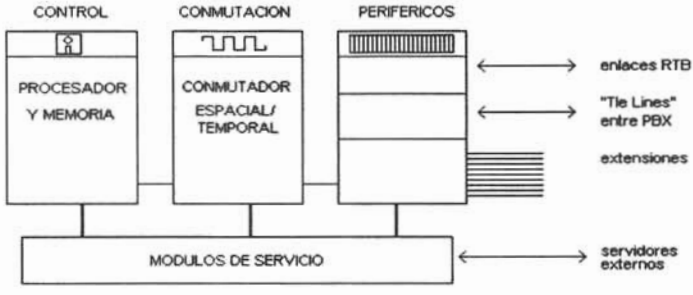


Fig. 1.7 Vista general del Hardware y procesos de un PBX.

Algunas de las funciones del PBX son:

- ✓ Transferencia de llamadas.
- ✓ Sistema para conocer el estado de las extensiones.
- ✓ Sistema de espera: Hace que si alguien llama a una extensión ocupada, el sistema haga esperar al llamante hasta que la extensión quede libre.
- ✓ Conferencias, que permite que llamadas del exterior logren comunicarse con varias extensiones a la vez.
- ✓ Mantener un archivo con información sobre las comunicaciones.
- ✓ Sistema de contraseñas.
- ✓ Desviar llamadas a petición de los usuarios, por si se van a mover de su puesto.

1.3.3.1 Distribuidor Automático de Llamadas (ACD).

Estos se emplean cuando se desea comunicar a los clientes con un servicio o con un grupo de soporte. Es decir, el tipo de central empleada en los Call Centers. Estos son utilizados en conjunto con los PBX, estos cuentan con un programa de gestión que permite que las llamadas a un mismo número sean atendidas por grupos de llamadas. Por lo que se permiten establecer:

- ✓ Colas de llamadas,
- ✓ Supervisiones de grupos,
- ✓ Prioridades en la atención de llamadas,
- ✓ Estadísticas de ocupación y desbordamiento, etc.

1.3.4 Central Office Exchange Service (CENTREX).

El servicio de CENTREX (Central Office Exchange Service) se puede definir como una central virtual sobre una central pública, ésta es proporcionada por los operadores públicos a través de la estructura telefónica básica que permite a sus abonados la utilización parcial de una central pública como si fuese un PABX, con el que se puede dar un servicio de comunicaciones a pequeñas oficinas de grandes empresas, integrándolas dentro de la red corporativa sin necesidad de hacer costosas inversiones.

No se necesitan de equipos de conmutación en sitio ya que son las propias extensiones de la central pública las que se tienden hasta el sitio de la empresa en cuestión, pero se hace necesario un tendido mayor de cables.

La función de emulación de una PABX se consigue mediante una función software en la central pública, con la que se pueden tener las facilidades propias de un PABX cualquiera.

1.3.5 Sistemas procesadores de voz.

La tecnología actual permite a los centros de llamadas tener sistemas que procesan la voz, estos elementos ayudan a mejorar la calidad de servicio a los clientes a la vez que reducen el tiempo humano necesario para la atención telefónica. A continuación se describirán algunos de estos servicios que se brindan:

IVR. Los equipos IVR (Interactive Voice Response) permiten automatizar gran parte de las llamadas de consulta. Estos equipos, basados en computadoras personales dedicadas, disponen de interfases telefónicas e informáticas Un ejemplo son los bancos que utilizan el sistemas de banco por teléfono en el cual piden el número de cuenta y PIN que son reconocidos por DTMF (Dual Tone Multi Frecuency) esto a través del teclado telefónico. Puede disponer de varios tipos de funcionalidades como componer frases, reconocimientos de tonos, pulsos y voz texto a voz, etc.

CTI. Las facilidades de CTI (Computer Telephony Integration) permiten integrar los sistemas telefónicos e informáticos, a través de los vínculos de datos entre los servidores informáticos. A través de vínculos de datos entre los servidores y las centrales telefónicas es posible disponer de "teléfonos virtuales" o de "sofá phones". Estos "teléfonos virtuales" son aplicaciones de PC que emulan las funciones de los teléfonos de escritorio, presentando en una pantalla las teclas de funciones más habituales en los agentes de Call Center (Atender, cortar, login, logout, no disponible, etc.). Así mismo las funciones de CTI permiten "sincronizar" la recuperación de datos en las aplicaciones de las PC´s de los agentes con el ingreso de cada llamada.

Correo de Voz. El correo de voz de los Call Centers brinda la posibilidad de dejar mensajes, en caso de demoras largas o fuera del horario de atención. Los mensajes son escuchados por los agentes, quienes los contestan en momentos de bajo tráfico telefónico entrante.

Los servicios pueden darse de alta para todos o sólo para algunos usuarios dependiendo de las políticas del administrador telefónico y de las características que se deseen tener.

1.3.6 Señalización telefónica.

Por señalización se entiende el conjunto de informaciones intercambiadas entre dos puntos de la red (usuario-central o central-central) que permiten la supervisión de estados o condiciones, el direccionamiento (establecimiento de llamada) y explotación de los recursos (gestión y mantenimiento de la red). En resumen la señalización es el lenguaje que las centrales telefónicas utilizan para hablarse entre sí y para hablar con los equipos terminales de los abonados. Como existen múltiples fabricantes de equipo telefónico es necesario que los equipos sigan "protocolos" de señalización", estas señales corresponden a las distintas fases de la conmutación.

1.3.6.1 Tipos de señalización.

Señalización multifrecuencia.

Utiliza la técnica de secuencia obligada, consiste en el envío de una señal (hacia delante) y recepción de una confirmación (hacia atrás), con objeto de una total seguridad. Por ejemplo, el sistema de señalización entre registradores y dentro de banda R2 del ITU-T utiliza 6 frecuencias en cada dirección, lo que hace un total de 12, que empleadas en un código de "dos entre seis" consigue 15 señales diferentes para cada dirección.

La aparición de los microprocesadores como unidades de control de las centrales, ha dado lugar a la progresiva sustitución de los mecanismos de la señalización convencionales por métodos más avanzados que se inspiran en las técnicas de diálogo entre procesadores, usuales en las redes de computadoras. Esto provocó una nueva tipificación de la señalización: por canal común y por canal asociado.

Señalización por canal asociado.

La señalización está directamente asociada al canal que transporta la información. Este tipo de señalización está clasificada por estado de bucle (corriente continua), frecuencia (dentro y fuera de banda) y digital (R2-CAS).

La **señalización por estado de bucle** se realiza mediante los hilos E&M (Exchange & Multiplex). Se denomina hilo M al hilo de transmisión (salida de central) y E al hilo de recepción (entrada a central). Las señales se representan aplicando y desconectando potenciales o mediante la apertura y cierre de un bucle.

La **señalización puede ser del tipo de señales de impulsos o por niveles indicativos de estados**; mientras el primero permite un plan complejo de señalización, el segundo garantiza una supervisión sencilla de la línea. Prácticamente este método sólo se usa en líneas bifilares y se pueden distinguir dos tipos: el procedimiento de señalización en bucle (mientras un extremo maneja los potenciales el otro lo hace con el bucle cerrado o abierto) y la señalización por un sólo hilo (potencial positivo o negativo en cada sentido).

Señalización en tramos de onda portadora. La señalización fuera de banda se trata de la portadora 3825±4 Hz. Se distinguen los procedimientos **Tone-off idle** con corriente de trabajo y **Tone-on idle** con corriente de reposo. El tone-off con emisión de portadora tiene mayor inmunidad frente al ruido pero el tone-on con supresión de portadora permite una mejor supervisión del servicio.

Señalización multifrecuente. Se trata de una codificación consistente en transmitir un juego de 2 entre 6 frecuencias, dentro de la banda del canal telefónico en

ambos sentidos: hacia adelante (1380, 500, 1620, 1740, 1860, 1980 Hz) y hacia atrás (1140, 1020, 900, 780, 660, 540 Hz).

Características	Tipo de señalización	
	R2-digital	SS no.7
Denominación	Asociada al canal	Canal común
Sigla identificación	CAS	SS7
Capacidad de señalización	64 kb/s	64 kb/s
Equivalencia en canales	30	1300
Red de señalización	rígida	Flexible
Tipos de servicio	telefonía	Cualquiera
Complejidad modelo OSI	Capa 1	Capa 1 a 4

Tabla. 1.1 Cuadro comparativo entre señalización R2 y señalización SS7.

Señalización por canal común

Cuando se trabaja con procesadores la señalización se transforma totalmente traduciéndose en un diálogo entre extremos. No se distingue una correspondencia entre el canal de señalización; es más, la vía de transmisión puede ser distinta. Así, el canal de señalización pasa a ser un canal de datos dentro de una red de señalización. La señalización de todos los canales se hace por un canal específico, dentro de los disponibles. Varios canales de información se combinan junto con los de señalización dentro de un medio de transmisión común, para lo cual las distintas señales se codifican y mezclan en el extremo emisor, realizándose el proceso contrario en el receptor, para recuperar la señal digital original.

Este tipo de señalización se denomina Señalización por Canal Común CCS (La nomenclatura SS7 corresponde al ITU-T y CCS7 a ANSI). Las principales características que identifican a la señalización CCS frente a CAS son:

- Tiempo de conexión menor.
- Número de mensajes prácticamente ilimitados.
- Flexibilidad para nuevos servicios.
- Encaminamiento alternativo.
- Corrección de errores mediante retransmisión de tramas.
- Es una arquitectura de protocolos estructurada en cuatro niveles.
- La capa 2 utiliza un protocolo de corrección de error ARQ tipo *go-back-N*.
- La capa 3 está prevista para mensajes en tiempo real de la red telefónica y es del tipo orientado sin-conexión.

Existen dos tipos de señalización por canal común en las redes analógicas; el SS6 iniciado en 1976 en Europa y CCIS (Common-channel Interoffice Signaling) en USA. Para las redes digitales, el ITU-T desarrolló desde 1980 sólo el sistema SS7. El sistema de señalización por canal común (CCS 7) fué adoptado en el año 1988 y es destinado a convertirse en estándar para las redes públicas de conmutación de circuitos. El ITU-T ha fijado y diseñado el SS7 con el propósito de ser el único compatible con la red digital futura y con los servicios integrados ISDN. La estructura lógica del SS7, se fundamenta en el modelo de 7 capas de Interconexión de Sistemas Abiertos (OSI), como se muestra en la Fig. 1.8.

El Sistema de Señalización nº 7 (SS7) es un arquitectura de protocolos de señalización completa en el que las unidades de señal son mensajes de las aplicaciones de señalización transportados en paquetes. Las características esenciales de este sistema son:

- Los enlaces y nodos de señalización constituyen una red de conmutación de paquetes lógicamente independiente de la de conmutación de circuitos, con un plan de direccionamiento distinto y definido a nivel internacional por ITU-T.
- Es un sistema de señalización por canal común. Existe un conjunto predefinido de canales entre centrales (y puntos de transferencia de señalización sin capacidad de conmutación de circuitos) dedicados a transportar mensajes de señalización relativa al establecimiento, liberación y supervisión de cualquier canal de 64 Kb/s de voz o datos. En los sistemas de señalización previos, por canal asociado, la señalización asociada a cada circuito de voz se transportaba por un canal de transmisión dedicado exclusivamente a él.

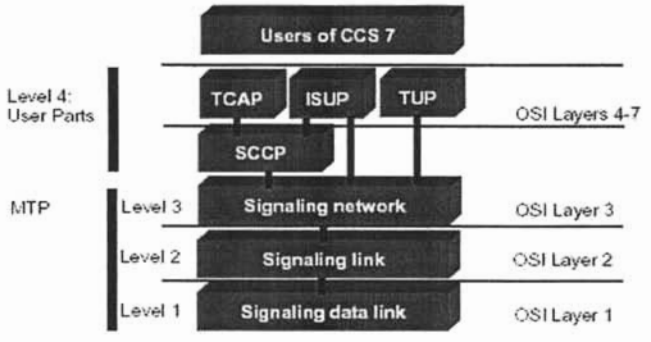


Fig. 1.8 Estructura lógica del SS7 con el modelo OSI.

1.3.7 Evolución de los protocolos de señalización para el transporte de Voz sobre redes IP.

La señalización en las redes telefónicas clásicas ha experimentado una intensa evolución a lo largo del siglo XX, al ritmo marcado por el propio desarrollo de las tecnologías de conmutación de circuitos en las que estas redes se fundamentan. Tras la conmutación manual de finales del siglo XIX y principios del XX, 1910 trajo la conmutación electromecánica. En esta etapa tecnológica, que duró hasta los años 60, la señalización se transportaba "en banda" (cambios de nivel y tonos dentro del propio canal telefónico) y era interpretada por elementos electromecánicos (relés) y electrónicos (filtros) en su tránsito por la red. A mediados de los 60, el proceso de digitalización de la red alcanzó la propia tecnología de conmutación - red digital integrada de transmisión más conmutación- con la llegada de las centrales digitales y el control de la conmutación por CPU (control por programa almacenado). De este modo, los canales síncronos de 64 Kb/s son conmutados octeto a octeto, espacial y temporalmente. Estos conmutadores ya están controlados íntegramente por procesadores que hablan un protocolo de señalización con procesadores de otras centrales.

Los primeros protocolos de señalización instalados en estos sistemas tenían una expresividad muy limitada y se basaban en el estado de ciertos bits de la trama TDM permanentemente asociados a cada canal de voz, como meras representaciones binarias de las señales analógicas de los sistemas precedentes. El salto cuántico se consiguió realmente cuando se aplicó totalmente la tecnología de redes de computadoras y las señales se convirtieron en mensajes intercambiados por aplicaciones sobre una red de conmutación de paquetes independiente y dedicada a este fin.

Si bien en la actualidad la red telefónica utiliza internamente esta forma de funcionamiento prácticamente en su totalidad, el último segmento por digitalizar, la red de acceso del abonado, permanece masivamente analógica, con una penetración discreta de accesos íntegramente digitales (ISDN). Consecuentemente, la señalización de abonado del servicio de telefonía tradicional ha evolucionado muy poco y es dentro de la red donde se realizó una revolución muy importante, transparente al usuario, que ha permitido la introducción de servicios suplementarios, de telefonía móvil, de red inteligente, B-ISDN interfuncionamiento con sistemas de telefonía sobre IP (VoIP) entre otros.

El sistema de señalización de red que ha soportado esta evolución con gran flexibilidad es el Sistema de Señalización nº 7. La primera norma del CCITT definiendo este sistema data desde 1981 (Libro Amarillo), y ha sido refinada y extendida en ediciones sucesivas en 1985 (Libro Rojo), 1989 (Libro Azul) y subsiguientes de ITU-T.

La red de paquetes para señalización en telefonía está diseñada específicamente para funcionar sobre canales de 64 Kb/s y a gestionar dichos enlaces. Por consiguiente no parece improbable una tendencia no sólo al desarrollo de formas de interfuncionamiento de arquitecturas basadas en SS7 con arquitecturas basadas en IP, sino a que IP influya poderosamente en la siguiente evolución de la infraestructura de red de señalización y gestión. Revisada aquí brevemente la historia de los sistemas de señalización, resulta curioso observar cómo la conmutación de paquetes, introducida en las redes tradicionales para ofrecer flexibilidad y fiabilidad a las labores de señalización en el plano de control de las torres de protocolos, se amplia en la actualidad al plano de usuario para el transporte de voz paquetizada, integrándose de nuevo voz y señalización.

1.4 Telefonía digital.

La Evolución hacia una Red Telefónica Integrada.

Existen diversas razones para convertir las facilidades de la red analógicas a digitales, pero la principal es la económica. Las facilidades digitales y los dispositivos son menos caros de diseñar, construir y mantener que los dispositivos analógicos. Ciertamente, la revolución del microprocesador en los últimos veinticinco años a producido la propagación de dispositivos digitales en todas las facetas de la vida y una baja sorprendente en los precios. Un motivo de esta conversión es que los equipos digitales introducen menos ruido, que se transmite junto con la señal de información. Esto significa que un medio digital proporciona un canal más limpio en las comunicaciones.

Las centrales telefónicas (CO) digitales son más fáciles de diseñar debido a que la computadora es el conmutador. Puesto que la mayoría de las CO digitales usan formato Multiplexación por división de tiempo (TDM), la velocidad de un conmutador digital puede incrementarse definiendo más intervalos de tiempo. El factor límite es la velocidad a la que las señales conmutan dentro de los dispositivos digitales. Como los procesadores se hacen más rápidos y relativamente menos caros, llegan a ser más fácil construir centrales digitales más rápidas y de mayor capacidad.

1.4.1 Modulación de Pulso Codificado (PCM).

Conversión analógica a digital.

La voz humana es una señal continua (analógica) en el rango de frecuencias de 0-4 Khz dentro del canal telefónico. Adicionalmente la comunicación digital, se basa en la

transmisión y recepción de bits discretos (0 y 1). Por consiguiente, para transmitir tanto la voz humana como otras señales analógicas es totalmente necesario convertir las señales analógicas en una corriente de bits, y para recibirlos en su estado inicial, realizar el proceso inverso. La conversión analógica a digital se hace por muestreo de las señales analógicas, caracterizando su nivel por una o más cifras, las cuales se transmiten por la vía digital. El proceso inverso se realiza regenerando las señales analógicas de acuerdo con las cifras que se reciban. A este proceso se le denomina **Modulación por pulsos codificados (PCM).**

Puede ser descrita como un método de conversión de analógico a digital. Esta conversión está basada en tres principios: Muestreo, Cuantificación y Codificación (ver Fig. 1.9).

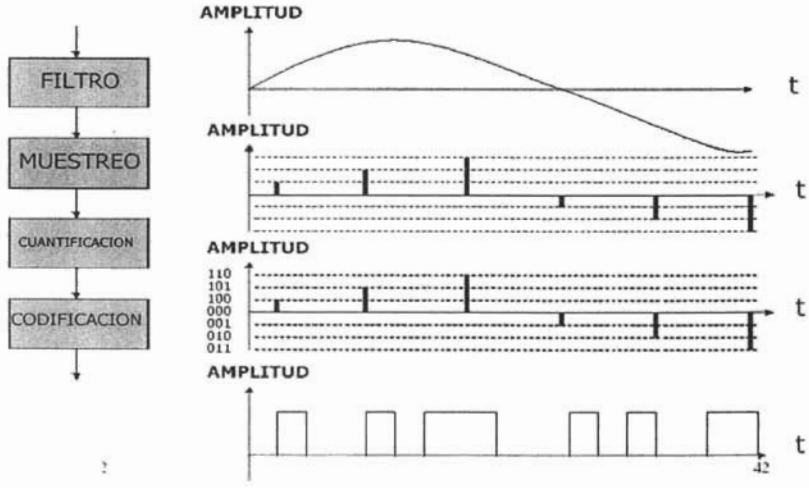


Fig. 1.9 Método de conversión analógica-digital.

La modulación tipo PCM se usa extensivamente en la telefonía digital (en los SPC (Storage Program Control)) que usa la multiplexación por división de tiempo (TDM). Se nombra a un canal de 64 Kbps como un Clear Channel o un Toll Quality. Sin embargo se suele usar velocidades de 32, 16, 8 y hasta 4 Kbps para meter dos, cuatro, ocho y hasta 16 conversaciones telefónicas en un sólo canal de 64 Kbps.

Con este método se varía la cadena de figuras transmitidas para representar las variaciones de el patrón de 0's y 1's introducidos al sistema. Esta técnica se emplea bastante en sistemas de transmisión de voz, y se le puede incorporar compresión, con la técnica denominada PCM. De acuerdo a los principios generalmente aceptados de diseño de sistemas telefónicos, se considera que el ancho de banda de la voz es de 4 Khz.

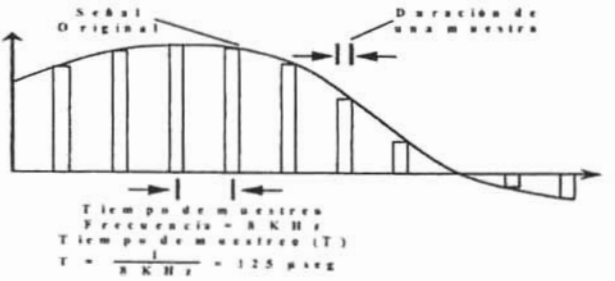


Fig. 1.10 Muestreo de la señal digital.

Para transportar la voz en forma digital, la señal de voz se muestrea 8,000 veces por segundo. Esta velocidad de muestreo está basado en el "Teorema de Muestreo" de Harry Nyquist, el cual expone que para ser capaz de reproducir adecuadamente una señal analógica desde una serie de muestras, el muestreo debe ser realizado al doble de la frecuencia mayor de la señal. La banda de paso del ciclo local se encuentra entre 0 y 4,000 Hz (el ancho de banda total de un canal de voz **FDM**, incluyendo la señal de voz y las bandas de guarda). La frecuencia máxima, 4 kHz, requiere una velocidad de muestreo de 8,000 ciclos por segundo, que corresponde a un intervalo de muestreo de 125 microsegundos.

Cada muestra de la señal de voz es convertida en una cadena de bits digitales. El proceso de convertir la muestra en una cadena de bits es la modulación de pulsos codificado (PCM) y se realiza por un dispositivo llamado **CODEC** (Codificador-Decodificador). El CODEC puede estar situado en el teléfono, en cuyo caso el ciclo local transporta señales digitales.

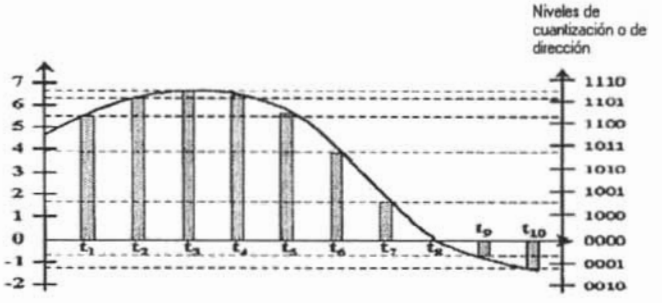


Fig.1.11 Conversión a cadenas de bits.

La señal de voz se muestrea cada 125 microsegundos, una vez cada 1/8,000 seg. Este muestreo, llamado **modulación por amplitud de pulso** (**PAM**), representa un nivel analógico que corresponde a la señal en ese momento. La amplitud de la muestra PAM se hace corresponder con un valor discreto sobre el eje de amplitud. Esta codificación digital es el escalón **PCM**.

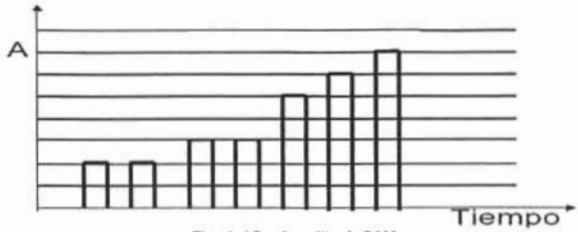


Fig. 1.12 Amplitud PAM.

Ahora bien, para lograr una buen calidad de la señal muestreada se requiere adicionalmente tomar muestras suficientes de su amplitud. Mientras más muestras se tomen de su amplitud, más calidad se obtendrá de la voz digitalizada, mayor fidelidad respecto a la señal original. PCM sigue el procedimiento general de digitalización ya mencionado. En este caso, en vez de generar pulsos de amplitud variable, se transmiten pulsos de magnitud constantes, que agrupados generan un código representativo de la amplitud de la señal analógica original.

Los niveles de amplitud se definen más juntos en los volúmenes bajos y más separados en los volúmenes altos, esto se denomina *compansión* (compresión-expansión). Hay dos algoritmos principales de compansión usados en la telefonía digital, la ley u, que es usada principalmente en los Estados Unidos, Canadá y Japón, y la ley A, que se usa en la mayor parte del mundo.

Las reglas de compansión definen 255 (ley-μ) ó 256 (ley-A) niveles de amplitud, por lo que cada muestra de voz es codificada con una palabra de 8 bits. Puesto que se toman 8,000 muestras cada segundo, el ancho de banda de un único canal de voz es de 64,000 bps. Esto se denomina algunas veces señalización digital de nivel 0, ó DS0.

Debería observarse que la señal de voz analógica no puede ser mapeada exactamente dentro de una escala de amplitud digital. Es decir, la señal digitalizada no es una replica exacta de la señal original; la diferencia se denomina **error de cuantificación**. El error de cuantificación tiene un efecto aditivo, de tal forma que el error es mayor cada vez que la señal experimenta una conversión de analógica a digital (A/D) o de digital a analógica (D/A) (que es lo que sucede cuando los conmutadores son analógicos y los enlaces son digitales). Debido al gran número de niveles de amplitud y al uso de la compansión se minimiza al error de cuantificación, y el resto se compensa fácilmente por el que se escucha.

La compansión reduce el efecto del error de cuantificación ya que utilizan una escala no lineal en el eje de amplitud. Concentrando los valores en las señales. El **PCM** es capaz de alcanzar 9 bits (512 niveles) de precisión, mientras que actualmente sólo se emplea un código de 8 bits. Para el confort de la mayoría de las personas, PCM se diseña para captar las sutilizas y los matices de la voz cuando se está hablando bajo, más que cuando se está gritando. El PCM con compansión (ley-A o ley-μ) tiene los estándares de calidad de redes de telefonía analógica y se considera *toll quality*.

1.4.2 Multiplexión por División de Tiempo (TDM).

La Multiplexión por División de Tiempo (**Time Division Multiplexing**) fué desarrollada para eliminar el problema del filtrado **FDM** (**Frecuency Division Multiplexing**) en las redes telefónicas públicas. Los multiplexores **TDM** permiten a múltiples usuarios compartir un canal digital usando ranuras de tiempo preasignadas. En **TDM** se reserva una ranura de tiempo, donde se colocan los marcos de usuario de cada

canal de baja velocidad que comparte un canal de alta velocidad y que se enlaza con otro multiplexor remoto.

TDM es un medio por el cual se transmite dos o más canales de información en el mismo circuito de comunicación utilizando la técnica de tiempo compartido. Se adapta bien a las señales binarias que consisten en impulsos que representan un dígito binario 1 ó 0. Estos impulsos pueden ser de muy corta duración y sin embargo, son capaces de transportar la información deseada; por tanto, muchos de ellos pueden comprimirse en el tiempo disponible de un canal digital. La señal original puede ser una onda analógica que se convierte en forma binaria para su transmisión, como las señales de voz de una red telefónica, o puede estar ya en forma digital, como los de un equipo de datos o un ordenador. Es un sistema sincronizado que normalmente implica PCM.

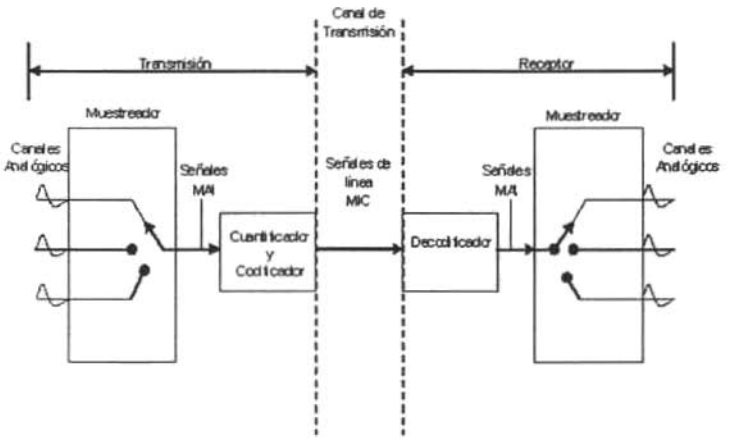


Fig. 1.13 Diagrama de un sistema TDM.

En la Fig. 1.13 puede verse un diagrama simplificado del sistema **TDM** con tres canales de información simultáneos. Las señales analógicas se muestrean y la MAI los transforma en impulsos, después la **PCM** codifica los muestreos. Posteriormente los muestreos se transmiten en serie en el mismo canal de comunicación, uno cada vez. En el receptor, el proceso de desmodulación se sincroniza de manera que cada muestreo de cada canal se dirige a su canal adecuado. Este proceso de denomina múltiplex o transmisión simultánea, porque se utiliza el mismo sistema de transmisión para más de un canal de información, y se llama **TDM** porque los canales de información comparten el tiempo disponible.

La parte de preparación de la señal y modulación del sistema se denomina multiplexor (MUX), y la parte de desmodulación se llama des-multiplexor (DE-MUX). En el MUX, como se ve en la fig. 1.13, un conmutador sincronizado (interruptor electromecánico) conecta secuencialmente un impulso de sincronización, seguido por cada canal de información, con la salida. El impulso de sincronización se utiliza para mantener al transmisor y receptor sincronizados, es decir, para mantener en fase el sincronizador del receptor con el del transmisor. El DEMUX dirige impulsos de sincronización hacia el sincronizador del receptor, y el muestreo de información envía los impulsos hasta sus canales correctos para su posterior análisis.

Una ventaja de la TDM es que puede utilizarse cualquier tipo de modulación por impulsos. Muchas compañías telefónicas emplean este método en sus sistemas PCM/TDM.

1.4.2.1 Jerarquía TDM Digital.

Para construir una trama TDM para telefonía se intercalan muestras de varios canales telefónicos junto con bits que sirven para la identificación y sincronización. Existen dos estándares o patrones: uno para USA (T1) y uno para Europa (E1).

T1

Las líneas T1 fueron las primeras portadoras digitales empleadas en los Estado Unidos. Una portadora T1 multiplexa 24 canales de voz sobre una única línea de transmisión usando **TDM**. La unidad básica de transmisión es una trama que contiene una muestra **PCM** en cada uno de los 24 canales (ver fig. 1.14). Ya que una muestra se representa con 8 bits, una trama única contiene 192 bits de datos de usuario. Cada trama está precedida por un bit de alineación de trama único, por lo que una trama T1 contiene 193 bits. Debido a que cada trama contiene una muestra de cada canal de voz, debe haber 8,000 tramas por segundo en un canal T1. Éste produce un ancho de banda de 1,544 Mbps., que también se conocen como señalización digital de nivel 1 (DS-1). Puesto que 8,000 bps son para la alineación de trama, la velocidad de datos de usuario es de 1,536 Mbps.

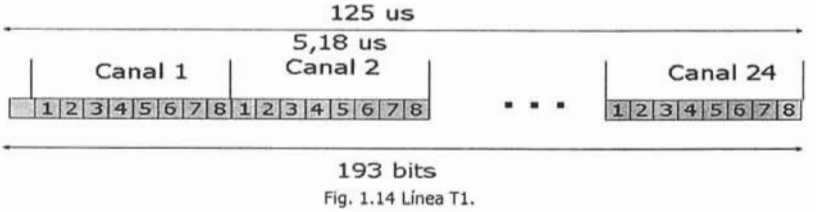


Fig. 1.14 Línea T1.

La multiplexación por división en el tiempo permite que sean multiplexadas varias portadoras T1 en portadoras de orden más alto. Cuatro canales T1 a 1.544 Mbps deberían generar 6.176 Mbps, pero T2 es en realidad de 6.312 Mbps. Los bits extra sirven para enmarcar y para recuperación en caso de que la portadora pierda sincronía. En el siguiente nivel se combinan seis corrientes T2 bit por bit para formar una corriente T3. A continuación se unen seis corrientes T3 para formar una corriente T4. En cada paso se añade una pequeña cantidad de bits extra para enmarcado y recuperación.

E1

La otra jerarquía TDM ampliamente usada está basada en el estándar de la Confederación Europea de Correos y Telecomunicaciones (CEPT). El primer nivel de la jerarquía digital CEPT multiplexa 32 intervalos de tiempo (cada uno con 8 bits, produciendo canales de 64 Kbps), estableciendo una trama de 256 bits y un ancho de banda de 2,048. Mbps. Uno de los 32 intervalos de tiempo se usa para señalizar, otro para alineación (sincronía) de trama y el resto para datos del usuario, resultando una velocidad de datos de 1,920 Mbps. Se parte de señales de voz de 4 KHz muestreadas a 8 KHz y cuantificadas usando 8 bits por muestra. Esto produce 64Kbits por seg. En el estándar europeo se multiplexan, en el primer nivel, 30 entradas de 64 Kb/seg. usándose 2 canales para señalización y sincronía.

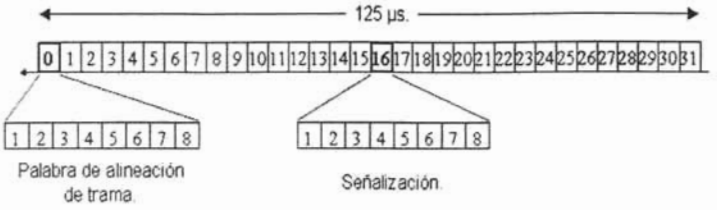


Fig. 1.15 Trama del estandar E1 .

En total 32 señales de 64Kbits/seg multiplexadas uniformemente producen una nueva trama de 2.048 Mbits/seg. En un segundo nivel se multiplexan 4 tramas de 2.048 Mbits/seg; esto produce una nueva trama de 8.448 Mbits/seg. En el tercero, cuarto y quinto nivel se agrupan cada vez cuatro tramas. Al final se obtiene una trama de alta velocidad: 565.148 Mbits/seg que contienen 7680 canales de voz.

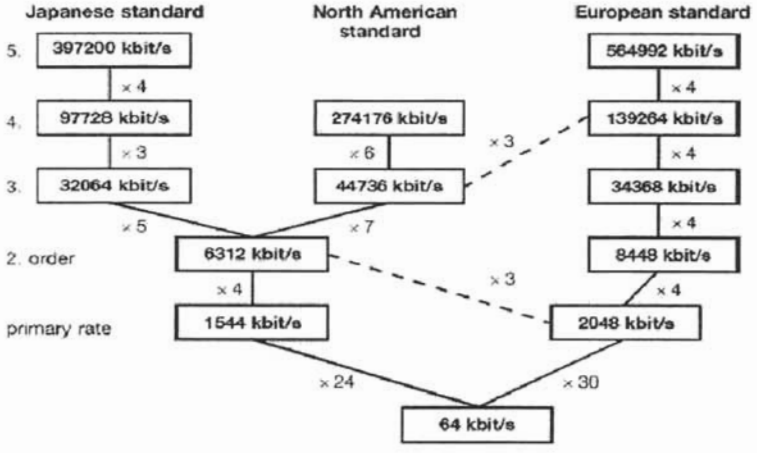


Fig. 1.16 Niveles de Multiplexación.

1.5 Red de Servicios Digitales Integrados (ISDN).

La red digital de servicios integrados (ISDN) es una extensión de la red pública telefónica, diseñada para transmitir llamadas de voz o datos digitalizados, desde un abonado a otro. Sus principales ventajas sobre la red de telefónica convencional son una mayor calidad de voz, mayores velocidades, menor tasa de error, mayor rapidez en el establecimiento de llamadas y mayor flexibilidad. Los costos de ISDN son similares a una llamada de teléfono convencional lo que, combinado con la velocidad disponible, hacen de la ISDN una buena elección para la interconexión de LAN´s, sobre todo cuando las comunicaciones entre ellas son muy intermitentes.

Los objetivos de la ISDN son, fundamentalmente, proporcionar una capacidad de interoperatividad en red que permita a los usuarios acceder fácilmente, integrar compartir información de todo tipo: datos, audio, texto, imagen y video, con independencia de las fronteras geográficas, organizativas y tecnológicas. La ISDN, así pues, es una consecuencia evidente de la convergencia de la informática y las telecomunicaciones.

La ITU (cuando se denominaba CCITT) define la ISDN como una red evolucionada de la red de telefonía integrada digital, que proporciona una conectividad digital extremo a extremo para dar soporte a una amplia gama de servicios, a los cuales los usuarios tienen acceso a través de un conjunto limitado de interfaces estándar multipropósito.

El concepto extremo a extremo significa que ISDN es una tecnología diseñada para digitalizar hasta el último metro, es decir, llevar la red digital hasta el abonado, fábrica u oficina.

Al provenir la ISDN de la RDI, las primeras instalaciones ofrecen conexiones a 64Kbps, llegando hasta el propio terminal de abonado. Los canales en la ISDN se dividen en canales B y canal D. Los primeros tienen una tasa de 64Kbps y el canal D tendrá una tasa de 16Kbps o de 64Kbps según se trate de un acceso básico (2B+ D) o un acceso primario (30B+ D) respectivamente. Estos canales están multiplexados en el tiempo. Debe tener modos de interconexión con redes no digitalizadas (con el fin de integrar la mayor cantidad de otras redes). A diferencia de la RDI que sólo soporta conmutación de circuitos, la ISDN incorpora centros de conmutación de paquetes, en ISDN deberá aparecer el tipo de servicio solicitado.

La ISDN utiliza las centrales digitales existentes (de la RDI) con canales de 64Kbps y cuando haga falta la interconexión con un servicio de conmutación de paquetes lo hará a través de la red pública que exista. Posteriormente, se integrará el servicio de conmutación de paquetes en la propia red (ISDN). El siguiente paso, podría ser la incorporación de anchos de banda superiores para servicios tales como videoconferencia, sonido Hi-FI, etc., mediante la utilización simultánea de varios canales. Ya para anchos de banda (ISDN Banda Ancha) que excedan las posibilidades de simultaneidad de canales (videotelefonía, TV, etc.), la vía hacia la integración vendría por la incorporación de nuevos elementos tecnológicos:

- Conmutadores de banda ancha.
- Acceso digital del usuario a la red por sistemas de fibra óptica.

Grupos Funcionales

Terminación de red 1 (TR1). Incluye funciones que pueden considerarse pertenecientes al nivel 1 del marco de referencia OSI, es decir, funciones asociadas con la terminación eléctrica y física de la red.

Terminación de red 1 (TR2). Realiza funciones de usuario a nivel 2 y 3 del Modelo de Referencia OSI, como conmutación, concentración o encaminamiento.

El **equipo terminal** se refiere al equipo del abonado que hace uso de la red ISDN. Se definen dos tipos:

- **Equipo terminal tipo 1 (ET1).** Son terminales diseñadas para conectarse directamente a la ISDN.

- **Equipo terminal tipo 2 (ET2).** Abarca los dispositivos no compatibles con ISDN: teléfonos analógicos, ordenadores personales, etc.

Adaptador de terminales (AT). Proporciona compatibilidad ISDN a los equipos no ISDN (Fig. 1.17).

Donde:

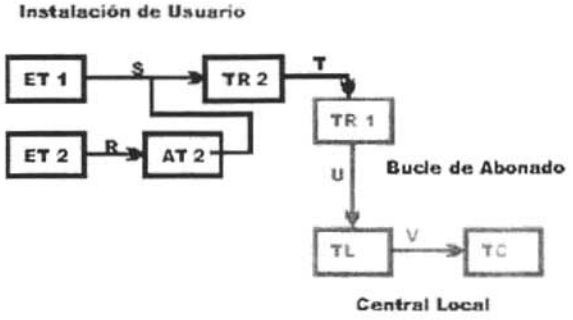


Fig. 1.17 Adaptador de terminal.

- ET1: Equipo terminal con conexión directa al punto S, esto es, directamente a la ISDN.
- ET2: Equipo terminal que precisa de un adaptador (AT) para conectarse al punto S.
- AT: Adaptador de equipo terminal. Adapta el punto R a la conexión de ISDN (punto S).
- TR2: Terminal de red. Centra digital que adapta los ET's a la Terminal de red (TR1). Sólo para accesos primarios donde existe una conexión física única entre cada ET y la TR2.
- TR1: Terminal de red. Conecta la instalación del usuario con la central digital local a través del bucle de abonado. Para accesos básicos el punto T y S son el mismo y los ETs están conectados a un bus pasivo.
- TL: Terminal de línea. Conecta la central local con el bucle de abonado.
- TC: Terminal de central. Conecta el TL con las etapas de conmutación internas de la central. Además, lleva a cabo el tratamiento de la señalización del acceso de usuario.

El punto S está constituido por 4 hilos (2 de transmisión y 2 de recepción), aunque opcionalmente puede llevar incorporados 2 pares de hilos para alimentar los ETs desde la TR.

CANALES ISDN

En comunicación de datos, un canal es un conducto unidireccional a través del cual fluye la información. Un canal puede transportar señales digitales o analógicas conteniendo datos de usuario o información de señalización de red. En entorno **ISDN** u otros entornos **TDM** digitales, un canal generalmente se refiere a un intervalo de tiempo en una línea de transmisión, y es full-duplex (bidireccional).

En canales ISDN, el ciclo local transporta señales sólo digitales y contiene varios canales usados para la señalización y datos de usuario. Los diferentes canales coexisten en el ciclo local usando **TDM**, hay tres tipos básicos de canales definidos para las comunicaciones de usuario en ISDN, distinguidos por su función y ancho de banda.

- **Canal D**. Transporta información de señalización entre usuario y red; también puede transportar paquetes de datos de usuario. La función principal del canal D es la señalización usuario-red, en el intercambio de estos mensajes de señalización es improbable usar todo el ancho de banda disponible. El canal sobrante se estima que sea lo bastante grande para permitir a los proveedores

de servicio ofrecer al usuario servicio de datos a velocidades de hasta 9,6 Kbps sobre el canal D. El canal D opera a 16 o 64 Kbps y depende de la interfaz de acceso al usuario.

- **Canal B**. Transporta información para servicios de usuario, incluyendo **voz, audio y datos** digitales; opera a la velocidad DS0 (64 Kbps). Ninguna petición de servicio es enviada sobre el canal B. Los canales B siempre operan a 64 Kbps, puesto que es la velocidad para las aplicaciones de voz. El canal puede usarse en modo circuito y en modo paquete. Hay una relación entre el canal B y D en la cual el canal D se usa para intercambiar los mensajes de señalización necesarios para solicitar servicios sobre el canal B.
- **Canal H**. Realiza la misma función que el canal B pero opera a velocidad superiores a DS0.

Los canales tipos B y D se agrupan, a su vez, en diferentes tipos o grupos (tabla 1.2), según el siguiente esquema:

Tipo	Función	Velocidad
B	Servicios básicos	64 Kbps.
D	Señalización	16 Kbps. (BRI) 64 Kbps. (PRI)
H_0	6 canales B	384 Kbps. (PRI)
H_1	todos los canales H0 H_{11} (24B) H_{12} (30B)	 1.536 Kbps. (PRI) 1.920 Kbps. (PRI)
H_2	ISDN de banda ancha H_{21} H_{22}	(propuesta actual) 32.768 Kbps. 43-45 Mbps.
H_4	ISDN de banda ancha	132-138,240 Mbps.

Tabla 1.2 Tipos de canales B y D.

Por tanto, las interfaces BRI y PRI tienen la siguiente estructura, ver tabla 1.3:

Interfaz	Estructura	Velocidad total	Velocidad disponible
BRI	2B + D16	192 Kbps.	144 Kbps.
PRI	23B + D64 30B + D64	1.544 Kbps. 2.048 Kbps.	1.536 Kbps. 1.984 Kbps.

Tabla 1.3 Características de las interfaces PRI y BRI.

Interfaz de Acceso al Usuario

Los canales de comunicación mencionados anteriormente pueden ser combinados de diferentes maneras para dar lugar a diferentes estructuras de acceso disponibles por los usuarios según sus necesidades. Las recomendaciones ISDN definen actualmente a dos interfaces de acceso diferentes, denominadas **Interfaz a Velocidad Básica (BRI)** e

Interfaz a Velocidad Primaria (PRI). Estas interfases operan al nivel del medio físico y el número de canales B, D y H disponibles.

BRI Interfaz a Velocidad Básica

El acceso básico o BRI (Basic Rate Interface) está constituido por dos canales de comunicación B a 64Kbps para la transmisión de información, y un canal D (a 16 Kbit/s.) para la señalización de usuario. La señalización, a través del Canal D, es por canal común, Cada controlador de interfaces "S" (TR1) puede soportar hasta 8 terminales conectados simultáneamente, que acceden al mismo canal D a través del Bus, mediante una técnica de disputa del mismo por colisión, que se vera más adelante. Sólo se pueden usar 2 terminales a la vez.

Este acceso básico es suficiente para las necesidades de la mayoría de los usuarios. Se emplea principalmente para instalaciones de abonado con un número reducido de terminales. A veces se utilizan varios accesos básicos como líneas de central ISDN de baja capacidad que funcionan a modo de TR2.

El Canal D de 16Kbps. se puede emplear en este acceso para Transmisión de Datos a 9600Kbps en forma de paquete y mientras no se este empleando para Señalización.

La configuración de este tipo de acceso permite el establecimiento de dos comunicaciones simultáneas a 64Kbps cada una de forma transparente por los canales B, y un número indeterminado de comunicaciones de datos en forma de paquetes hasta un máximo total de 9600Kbps por el canal D.

Actualmente se permite la conmutación de paquetes a 9600Kbps, por un sólo terminal en este tipo de acceso y por canal D, ya que por los canales B se puede transmitir lo que se quiera de forma transparente.

En el lado de instalaciones de usuario, (interfaz S/T), está soportado físicamente por una configuración a cuatro hilos (dos para transmisión y dos para recepción) en configuración de bus de datos (llamado bus pasivo). La velocidad de transmisión total es de 192Kbps distribuidos de la siguiente manera: canales B, canal D, y la información adicional necesaria para el mantenimiento del sincronismo, el mantenimiento de la estructura multitramas, que actualmente no se utiliza, y el control de acceso al canal de señalización.

En el lado red, (interfaz U), se utiliza como soporte para la transmisión el mismo ciclo de abonado analógico existente, la transmisión y recepción es a 2 Hilos y la transmisión es Full-Duplex con técnicas de cancelación de eco. La velocidad en línea es de 160 Kb/s. Es la TR 1 la que hace de interface S/T y la conversión de 4 a 2 Hilos y viceversa.

Interfaz a Velocidad Primaria (PRI).

El PRI dispone de varias configuraciones posibles. La configuración en Norteamérica y Japón se denomina 23B+ D, y significa que el interfaz comprende 23 canales B más un único canal D operando a 64Kbps; en Europa y la mayor parte del mundo, por lo que me enfocaré más a ésta, la configuración está constituida por 30 canales B a 64Kbps y un canal D a 64Kbps, con una velocidad operacional total de 2048Mbps.

La interfaz a 2048Mbps de PRI multiplexa 32 intervalos de tiempo de 6Kbps en una trama, numerados de 0 a 31. El intervalo de tiempo 0 se reserva para la alineación, sincronización y señalización de la capa física. Los intervalos de tiempo 1 a 15 y de 17 a

31 se usan para los canales B, mientras el intervalo de tiempo 16 se reserva para el canal D. El canal D no se emplea más que para señalización del tipo canal común, no se contempla la posibilidad de transmisión de datos a baja velocidad por el canal D como ocurría en el acceso básico.

En el lado de las instalaciones de usuario (interfaz T) se dispone de una trama de 2048Mbps que, a través de una agrupación funcional TR2 normalmente una central digital cuyas extensiones pueden ser líneas de interfaz S o equipo equivalente, puede estructurarse en otras combinaciones de canales de entre las ya mencionadas. (30B + D, 5H0 + D, H12 + D, etc.)

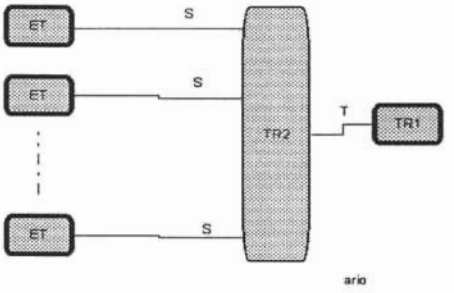


Fig. 1.18 Conexión de ET's a un acceso primario.

Arquitectura del Protocolo ISDN.

La ISDN se integra en el esquema de capas OSI (Open Systems Interconnection), en el que cada nivel realiza un subconjunto de las funciones requeridas para la comunicación.

La arquitectura del protocolo ISDN, respecto de los niveles OSI, se define como se muestra en la tabla 1.4:

Aplicación Presentación Sesión Transporte	Señalización de usuario extremo a extremo	Protocolos OSI				
Red	Control de llamada I.451	X.25 Paquetes				X.25 Paquetes
Enlace	LAP-D (I.441)					X.25 LAP-B
Físico	Nivel 1 (I.430, I.431)					
	Señalización	Conmutación de paquetes	Telemetría	Conmutación de circuitos	Circuitos punto a punto	Conmutación de paquetes
	Canal D			Canal B		

Tabla 1.4 Comparación de los protocolos ISDN con respecto al modelo OSI.

Las funciones del nivel físico incluyen:

- Codificación de los datos a ser transmitidos.
- Transmisión de datos en modo full duplex, a través del canal B.
- Transmisión de datos en modo full duplex, a través del canal D.
- Multiplexado de los canales para formar la estructura BRI o PRI.
- Activación y desactivación de los circuitos físicos.
- Alimentación del terminador de la red al dispositivo terminal.
- Identificación del terminal.
- Aislamiento de terminales defectuosos.
- Gestión de accesos al canal D.

El enlace de los canales se produce a través del procedimiento LAP-B (Link Access Procedure Balanced).

El protocolo LAP-B es un subconjunto del protocolo HDLC (High-level Data Link Control), que puede proporciona la conexión entre el usuario y la red a través de un enlace simple, por ejemplo en un canal B.

Asimismo, el protocolo LAP-D, derivado del anterior, proporciona una o más conexiones sobre un mismo canal (D), y por tanto permite cumplir con los requerimientos de señalización para múltiples canales B, asociados a un único canal D. La funcionalidad del protocolo LAP-D permite:

- Mensajes a un único o múltiples (broadcast) destinatarios.
- En caso de un único destinatario, se garantiza que no hay pérdida de ningún mensaje, así como su transmisión libre de errores, en la secuencia en que son originados.
- En caso de mensajes tipo "broadcast", LAP-D garantiza la transmisión libre de errores en la secuencia original, pero si hay errores durante la transmisión, los mensajes se pierden.

LAP-D proporciona direccionamiento y chequeo de errores en la capa 2, mediante una secuencia de verificación de tramas (FCS o Frame Check Sequence).

El SAPI o identificador de punto de acceso al servicio (Service Access Point Indentifier), mantiene aparte la información de las diferentes formas del canal D. SAPI 0 es para indicar información de señalización; SAPI 1 es para conexiones de paquetes de datos, empleando el protocolo ISDN Q.931; SAPI 16 es para paquetes de datos según las recomendaciones X.25 (nivel 3), y SAPI 63 se emplea para la información de gestión de LAP-D. Las otras posibilidades están reservadas para usos futuros.

El TEI identificador de terminal (Terminal Endpoint Identifier), es la segunda parte de la dirección LAP-D, y permite que sean identificados diferentes dispositivos en un determinado grupo. Esta dirección es empleada sólo en el canal D, y no debe de ser confundida con ninguna dirección de la capa 3, que corresponden a la red (por ejemplo, una dirección X.25, fig.1.19).

Bits:	8	1	1	6	1	7	1-2	8-1.024	2	8
Contenido:	Flag	C/R	EA0	SAPI	EA1	ETI	Control	Información	FCS	Flag

(Flag = 01111110)

Fig. 1.19 Contenido de una dirección X.25

Los modos de operación de LAP-D permiten realizar el reconocimiento de la correcta recepción (acknoledge mode) de tramas múltiples en el caso de un único destinatario, o bien no realizarlo (unacknowledge mode) en caso de mensajes tipo broadcast.

Se pueden establecer 3 tipos básico de conexiones ISDN:

- Llamadas de conmutación de circuitos a través del canal B: en las que la preparación se realiza a través del canal D.
- Llamadas de conmutación de paquetes a través del canal B: en las que la preparación se realiza a través del canal D, para la conexión de conmutación de circuitos a un nodo de conmutación de paquetes (de la operadora o privado).
- Llamadas de conmutación de paquetes a través del canal D: en las que el tráfico de paquetes es multiplexado con las señales de control en la capa de enlace (internetworking con canales B).

La señalización del canal D (Q.931), realiza las siguientes funciones:

- Verificación de compatibilidad: asegura que sólo reaccionen a una llamada aquellos equipos compatibles en una línea ISDN.
- Subdireccionamiento.
- Presentación de números.
- Establecimiento de la llamada.
- Selección del tipo de conexión (conmutación de paquetes o de circuitos).
- Generación de corrientes y tonos de llamada.
- Señalización usuario a usuario (de forma transparente a la red).
- Soporte de facilidades y servicios adicionales.

Los mensajes empleados para la señalización son:

- SETUP: para iniciar una llamada.
- ALERTING: para indicar el inicio de la fase de generación del tono.
- CONNECT: para señalizar el comienzo de la conexión.
- CONNECT ACKNOWLEDGE: reconocimiento local del mensaje de conexión.
- DISCONNECT: enviado por el terminal cuando va a colgar.
- RELEASE: respuesta a un mensaje de desconexión, iniciando la misma.
- RELEASE COMPLETE: reconocimiento local del mensaje de desconexión, confirmando la liberación correcta de la llamada.
- CALL PROCEEDING: enviada por la central a un terminal intentando establecer una llamada una vez que ha sido analizado el número llamado.
- SETUP ACKNOWLEDGEMENT: confirmación por la central, de la recepción del mensaje de SETUP, en caso de precisarse de información adicional para completar la llamada.
- USER INFORMATION: para la señalización usuario a usuario.
- INFORMATION: empleado por el terminal para enviar información adicional a la central en cualquier momento, durante una llamada.
- NOTIFY: usado por la central para enviar información a un terminal, en cualquier momento, durante una llamada.

Los elementos importantes, durante el envío de los mensajes de señalización, son:

- Número llamado, incluido en SETUP.
- Subdirección llamada, usada durante la llamada para seleccionar un equipo determinado.
- Número y subdirección del iniciador de la llamada, empleados en SETUP para identificar el origen de la llamada.
- BC (Bearer Capability): empleado durante SETUP, para seleccionar el tipo de conexión.

- HLC (High Layer Compatibility): empleado en SETUP por el equipo originario de la llamada, para identificar el servicio requerido y verificado por el equipo llamado para comprobar su compatibilidad.
- LLC (Low Layer Compatibility): empleado en SETUP por el equipo originario para especificar como ha sido codificada la información para el servicio.
- Número y subdirección conectadas, enviado al originario de la llamada para identificar al equipo con el que realmente se ha establecido la conexión.
- Indicador de situación: empleado para describir el estado de la conexión o para indicar el acceso al canal B, aún no habiendo sido completada la llamada.
- Visualización: utilizado en NOTIFY para proporcionar un mensaje en la pantalla de un terminal ISDN.
- Facilidades de teclado: empleados para introducir información adicional desde un teclado del terminal, una vez que han sido introducidos los datos relativos al número y subdirección del terminal llamado.
- Información usuario a usuario.

CAPÍTULO DOS

REDES DE DATOS

2.1 Concepto de red.

Una red es un sistema esencialmente conectado por objetos o personas. Las redes nos rodean por todas partes, incluso dentro de nuestro cuerpo. El sistema nervioso y cardiovascular sería un ejemplo de redes. Podemos pensar en redes al observar los sistemas de comunicación, transporte, social, biológico, etc.

2.2 Funcionamiento de una red.

El funcionamiento de una red de comunicaciones de datos es muy sencillo, para tener una idea clara del funcionamiento de una red se tomará el ejemplo de una empresa de mensajería en la cual los paquetes que son encomendados a ésta serán llevados de un lugar a otro. El paquete es clasificado, numerado, fechado y enviado a través de un medio que puede ser un medio de transporte ya sea por aire, tierra ó mar. El objetivo primordial es llevar el paquete a su destino final. En el caso de la redes de computadoras ó de datos, el modo de comunicarse es similar siendo estas apoyados por estándares, y protocolos internacionales tomando, por ejemplo, el TCP / IP o el modelo OSI, los cuales se tratarán más adelante en el presente capítulo.

Básicamente una red de comunicaciones es un conjunto de dispositivos de comunicaciones conectados a través de un medio de transmisión, de tal manera que se interconecten y organicen de tal manera que puedan ser operados y administrados con la finalidad de compartir recursos y servicios. En pocas palabras una red es un conjunto de equipos interconectados con el fin de intercambiar información y compartir recursos.

2.3 Redes de computadoras.

Como preámbulo las redes surgen de la necesidad de compartir recursos de alto costo entre varias personas. En los inicios de las computadoras, los recursos eran de un costo altísimo, el poder del cómputo era uno de los mas valiosos y mas costosos. En los centros de investigación se hacia necesario que todos los investigadores tuvieran acceso a estos tipos de recursos y que estos fueran distribuidos en forma tal que no se tuviese un desperdicio de tiempo de procesamiento.

En los años 40, las computadoras eran dispositivos electromecánicos grandes y propensos a los errores. En 1947, la invención de un transmisor semiconductor abrió muchas posibilidades a la creación de computadoras mucho más pequeñas y más fiables. Durante los años 50, las computadoras de grandes sistemas informáticos, que se ejecutaban con tarjetas perforadas, las comienzan a utilizar normalmente las grandes instituciones. A finales de los 50, se inventó el circuito integrado, que combinaba varios, y más tarde millones de transistores en una pequeña pieza de semiconductor. Durante los 60, las primeras redes de computadoras que se crearon, eran del tipo centralizado (Mainframe), es decir, un procesador central, el cual tenía el poder de cómputo y las terminales que le enviaban al procesador las tareas a realizar, con ello los circuitos integrados se comenzaron a usar mundialmente.

A finales de los 60 y comienzos de los 70, empezaron a surgir computadoras más pequeñas, llamadas microcomputadoras (aunque son más grandes que las estándares de hoy). En 1978, la compañía Apple Computer presentó la computadora personal. En 1981, IBM presentó la computadora personal de arquitectura abierta. El Mac amigo del usuario, el PC de arquitectura abierta de IBM, y la posterior micro-miniaturización de los circuitos integrados llevaron al uso extendido de las computadoras personales en las casas y en los negocios. A finales de los 80, los usuarios, con sus computadoras autosuficientes, comenzaron a compartir datos (archivos) y recursos (impresoras).

A principios de los 70, y continuando en los 90, el departamento de defensa de E.U.A. desarrolló redes de área amplia (WAN), grandes y fiables. Se ha usado algo de su tecnología para el desarrollo de las LAN, pero lo más importante es que las WAN del Departamento de defensa se convirtieron en lo que hoy conocemos como Internet.

A mediados de los 80, se desarrollaron las computadoras de propósito general conocidas como gateways (después routers). Estos dispositivos permitían la interconexión de LAN separadas, creando así las internetworks. El departamento de defensa ya tenía una internetwork extensa, pero la disponibilidad comercial de los routers, que llevaban a cabo las mejores selecciones de ruta, y conmutación de datos para muchos protocolos, permitieron la expansión de la red que hoy conocemos.

El desarrollo de la tecnología permitió tener redes que comunicaban computadoras en sitios distantes, este avance obligó a crear protocolos de comunicación entre las computadoras. Estos protocolos eran propiedad de los fabricantes de las máquinas. Aquí es donde se comienza a ver la necesidad de crear protocolos estándares para comunicar máquinas y redes de diferentes fabricantes y de diferentes tipos.

Con la llegada del nuevo siglo, el siguiente paso es la convergencia de las computadoras y la tecnología de las comunicaciones, especialmente la convergencia de ***voz***, *video y datos*, que han viajado tradicionalmente a través de sistemas diferentes; en un sólo flujo de información.

2.4 Clasificación de redes.

Los distintos tipos de redes son clasificados según la distancia en cuatro categorías, redes de área local (LAN), redes de área metropolitana (MAN) y redes de área amplia (WAN) y la red Internet. A medida que el uso de las computadoras crecía, pronto fue obvio que las redes LAN no eran suficientes. En un sistema LAN, cada área es una especie de isla electrónica. Era necesaria una forma de que la información se moviera eficientemente y rápidamente, no sólo dentro de un área o lugar, sino de un área a otra. Entonces, la solución fué la conexión de las LAN mediante redes de área metropolitana (MAN) y redes de área amplia (WAN). Debido a que las WAN permiten la conexión de usuarios de la red en zonas geográficas extensas, hicieron posible que diversas instituciones se comunicaran con el resto a larga distancia.

2.4.1 Redes de Área Local (LAN).

La red de área local (LAN) es una red de datos de alta velocidad, tolerante a fallas, que cubre un área geográficamente pequeña. Por lo general conecta estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. Las LAN´s tienen muchas ventajas para los usuarios de computadoras, como el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos entre los usuarios conectados y la comunicación entre usuarios vía correo electrónico y otras aplicaciones.

Las LAN están principalmente diseñadas para lo siguiente:

- ✓ Operar dentro de una zona geográficamente limitada.
- ✓ Permitir a muchos usuarios acceder a medios de alto ancho de banda.
- ✓ Proporcionar conectividad de tiempo completo a los servicios locales.
- ✓ Conectar físicamente dispositivos adyacentes.

2.4.1.1 Protocolos LAN.

Estos protocolos operan en las dos capas mas bajas del modelo de referencia OSI, entre la capa física y la capa de enlace de datos. En la Fig. 2.1 se comparan algunos protocolos LAN contra el modelo de referencia OSI.

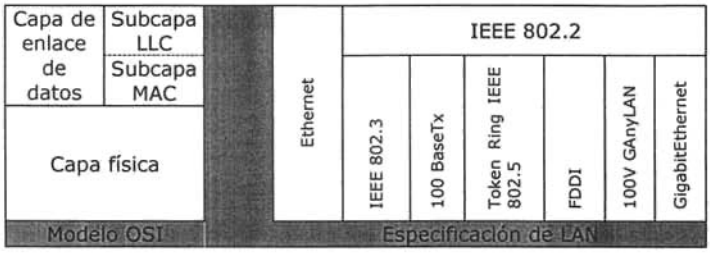


Fig. 2.1 Protocolos LAN contra el modelo de referencia OSI.

2.4.1.2 Métodos de acceso a medios LAN.

En la actualidad los protocolos LAN suelen utilizar uno de dos métodos para acceder al medio físico de la red: CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones) y estafeta circulante.

En el esquema de acceso a medios CSMA/CD, los dispositivos de la red compiten por el uso del medio de transmisión físico de la red. Por esta razón, al CSMA/CD a veces se le llama acceso por contención. Ejemplo de LAN´s que utilizan el esquema de acceso a medios CSMA/CD son las redes Ethernet/IEEE 802.3.

2.4.1.3 Dispositivos LAN.

Las LAN conectan dispositivos directamente a un segmento de red, entre estos dispositivos cabe incluir los siguientes:

- *NIC* (Tarjetas de interfaz de red): tarjeta de red conectada a la motherboard de la PC para poder conectarse a un segmento de red.
- *Repetidor*: limpia la señal, la regenera y la repite. Utilizado cuando la longitud del cable se extiende por encima del máximo permitido.
- *Hub*: es simplemente un repetidor multi-puertos, utilizado para conectar varios dispositivos a un mismo segmento de red.
- *Puente o Bridge*: Interconecta dos segmentos de red.
- *Switch:* Interconecta a varios segmentos de red y provee ancho de banda a cada puerto.

A los dispositivos que se conectan directamente a un segmento de red se les suele llamar hosts.

2.4.1.4 Tecnologías LAN.

Las tecnologías Ethernet son un protocolo de enlace de datos utilizado por la mayor parte de las redes de área local que operan en la actualidad. En el transcurso de más de 20 años en el cual se ha revisado y actualizado los estándares de Ethernet se han obtenido mejoras en las tecnologías, como FastEthernet y Gigabit Ethernet. Logrando de

esta forma proporcionar suficiente ancho de banda para las necesidades de prácticamente cualquier aplicación de red.

Antes de pasar más allá de otro punto cabe mencionar que Ethernet fué conocido como DIX Ethernet II en sus inicios siendo una creación de DEC, Intel y Xerox en 1980, después la IEEE (Institute of Electrical and Electronics Engineers) con el objetivo de desarrollar un estándar similar a Ethernet, en 1985 publicó el estándar IEEE 802.3 utilizándose el nombre de Ethernet para los productos que cumplen con el estándar 802.3 del IEEE.

Ethernet.

Ethernet proporciona una interfaz unificada al medio de red que permite la transmisión y recepción de varios protocolos de nivel de red de forma simultánea. Al igual que en la mayor parte de los protocolos de nivel de enlace que se utilizan en LAN. Ethernet realiza todo lo posible para transmitir datos al destino especificado, pero no hay ningún mecanismo que garantice una entrega correcta. La responsabilidad de correcta entrega recae en los protocolos que operan en los niveles del modelo OSI. Después del lanzamiento de IEEE 802.3 se publicó una serie de suplementos, siendo los siguientes:

IEEE 802.3a	Ethernet delgada 10Base2.
IEEE 802.3c	Especificaciones de repetidor a 10 Mbps.
IEEE 802.3d	Enlace entre repetidores por fibra óptica.
IEEE 802.3i	Ethernet de par trenzado 10Base-T.
IEEE 802.3j	Ethernet de fibra óptica 10Base-F.
IEEE 802.3u	Fast Ethernet 100Base-T y autonegociación.
IEEE 802.3x	Ethernet Full Duplex.
IEEE 802.3z	Gigabit Ethernet 1000Base-X.
IEEE 802.3ab	Gigabit Ethernet 1000Base-T (Par trenzado).
IEEE 802.3ac	Extensión del tamaño de trama a 1522 bytes para VLAN Tag.
IEEE 802.3ad	Agregación de enlaces para enlaces paralelos.

Variedades de red 802.3

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 3	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m en full duplex	Estrella	Bus
1000Base-T	UTP Cat5e	1000 Mbps	100 m	Estrella	Bus

Tabla 2.1 Variedades de red 802.3

Trama Ethernet.

La información transmitida a través de una red Ethernet, tiene el aspecto de tramas o paquetes de información (Fig. 2.2). La trama ethernet es de longitud variable, pero no es menor de 64 Bytes ni mayor de 1518 Bytes. La razón para que no sea menor de 64 Bytes, es para cumplir con las especificaciones de Round Trip Time, del estándar Ethernet. Si alguna trama de información es menor de 64 Bytes, debe ser completada con ceros para alcanzar los 64 Bytes. Existen tres especificaciones de trama sobre Ethernet, Ethernet II ó DIX, IEEE 802.3 y SNAP. La más común es el estándar de la IEEE 802.3.

Preamble (7-bytes)	Start Frame Delimiter (1-byte)	Dest. MAC Address (6-bytes)	Source MAC Address (6-bytes)	Length / Type (2-bytes)	MAC Client Data (0-n bytes)	Pad (0-p bytes)	Frame Check Sequence (4-bytes)

Fig. 2.2 Trama Ethernet IEEE 802.3

Preamble (Preámbulo): Secuencia de 56 bits con valores alternado 1 y 0 usados para la sincronización. Esto sirve para que los componentes en la red puedan detectar la presencia de señal y puedan leer la señal antes de que llegue la trama de datos.

Start Frame Delimiter (Delimitador de comienzo de trama): Secuencia de 8 bits configurados a 10101011 que indica el inicio de la trama.

Destination & Source MAC Addresses (Dirección destino y dirección origen la MAC): El campo de la dirección MAC destino identifica la estación que debe recibir la trama. La dirección MAC origen identifica la estación origen de la trama. El estándar 802.3 permite que estos campos de dirección sean de 2 ó 6 bytes de longitud pero virtualmente todas las implementaciones Ethernet en existencia usan direcciones de 6 bytes. La dirección destino puede especificar una "dirección individual" dirigido a una estación única o una "dirección multicast" destinada a un grupo de estaciones. Una dirección destino con todos los bits en 1 se refiere a todas las estaciones en la LAN y es denominada "dirección broadcast" (o difusión).

Lenght/Type (Longitud): Si el valor de este campo es menor o igual que 1500, entonces el campo Length/Type indica el número de bytes en el subsiguiente campo MAC Client Data. Si el valor de este campo es mayo o igual que 1563, entonces el campo Length/Type indica la naturaleza del protocolo MAC del tiempo cliente (tipo protocolo).

MAC Client Data: Este campo contiene los datos transferidos desde la estación origen hasta la estación destino. El tamaño máximo de este campo es de 1500 bytes. Si el tamaño de este campo es menor de 46 bytes, entonces es necesario el uso del campo subsiguiente "Pad" para hacer que el tamaño de la trama alcance el tamaño mínimo.

Pad: Si es necesario, bytes adicionales son agregados en este campo para hacer que la longitud de la trama alcance su valor mínimo. El mínimo tamaño de trama Ethernet es de 64 bytes desde el campo Destination MAC Address hasta el campo Frame Check Sequence.

Frame Check Sequence: Este campo contiene un valor de chequeo de redundancia de 4 bytes (CRC) para verificación de errores. Cuando una estación origen ensambla una trama MAC, realiza un calculo CRC sobre todos los bits desde el campo Destination MAC Addreess hasta el campo Pad (todo los campos excepto el preámbulo, el delimitado de

trama y la secuencia de chequeo de trama). La estación origen almacena este valor y lo transmite como parte de la trama. Cuando la trama es recibida por la estación destino, ésta realiza un chequeo idéntico. Si el valor calculado no coincide con el valor en el campo, la estación destino asume que ha ocurrido un error durante la transmisión y entonces descarta la trama completa.

Fast Ethernet y Gigabit Ethernet.

La especificación 802.3u del IEEE, define lo que se conoce habitualmente como Fast Ethernet, un protocolo del nivel de enlace de datos a 100Mbps. Fast Ethernet no modifica dos de los tres elementos que definen una red Ethernet. El nuevo protocolo utiliza el mismo formato de trama que el 802.3 del IEEE y el mismo mecanismo de control de acceso al medio CSMA/CD. Las modificaciones que permiten el incremento de velocidad se encuentra en varios elementos de la configuración del nivel físico, incluyendo el tipo de cable utilizado, la longitud de los segmentos de cable y el número de concentradores permitidos.

Gigabit Ethernet es definido por el 802.3z y se desarrolló para constituir la siguiente generación de red Ethernet, funcionando a 1Gbps, 10 veces la velocidad de Fast Ethernet. Utiliza el mismo formato de trama, tamaño de trama y método de control de acceso al medio, éste último es fundamentalmente el mismo pero con pocas modificaciones en su implementación, la mayor ventaja es que es posible expandir una red que soporte Fast Ethernet a Gigabit Ethernet sin tener que sustituir por completo los concentradores, conmutadores y cables. Sin embargo se deben hacer algunas actualizaciones de hardware.

2.4.2 Red de Área Extensa (WAN).

Una red de área extensa (WAN) es una red de comunicación de datos que tiene una cobertura geográficamente grande y suele utilizar las instalaciones de transmisión que ofrecen compañías de servicios como las telefónicas.

Las principales características de las WAN son:

- ✓ Funcionan más allá del ámbito geográfico de una LAN local. Utilizan los servicios de portadora, o carriers, tales como las operadoras locales en EE.UU (RBOC) y Sprint and MCI, en México existen como tales TELMEX, Avantel y ATT.
- ✓ Utilizan varios tipos de conexiones en serie para acceder al ancho de banda de la Red.

2.4.2.1 WAN y Modelo OSI.

Una WAN opera en la capa física, en la capa de enlace de datos y red del modelo de referencia OSI (ver fig. 2.3). Éste interconecta redes de área local (LAN). Las WAN proporcionan el intercambio de paquetes/trama de datos entre routers/puentes y las LAN que soportan.

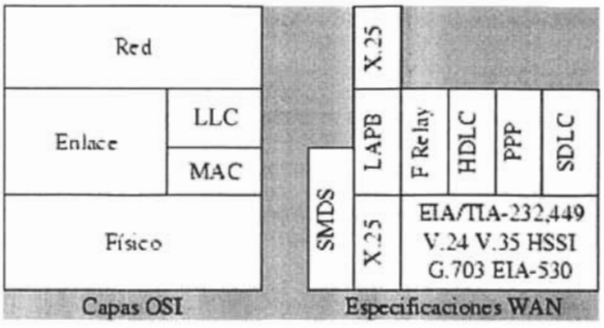


Fig. 2.3 Comparación de protocolos WAN en modelo de referencia OSI.

2.4.2.2 Protocolos y Estándares WAN.

Los protocolos de la capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios WAN. Los protocolos de enlace de datos WAN describen cómo se transportan las tramas entre sistemas en un único enlace de datos. Las tramas más comunes en la capa de enlace de datos, asociadas con las líneas seriales síncronas son las siguientes:

Protocolos WAN:

- ✓ HDLC (Control de enlace de datos de alto nivel) es un estándar IEEE que puede no ser compatible con diferentes fabricantes debido a la forma en que el fabricante haya elegido implementarlo. HDLC soporta configuraciones punto a punto y multipunto.
- ✓ Frame Relay. Utiliza servicios digitales de alta calidad e implica un entramado simplificado sin mecanismos de corrección de errores; esto significa que puede enviar información de la capa 2 mucho más rápido que otros protocolos WAN.
- ✓ PPP (Protocolo punto a punto) es muy parecido a HDLC, con un campo añadido para especificar el protocolo de capa superior. PPP contiene un campo de protocolo para identificar el protocolo de la capa de Red. PPP también se puede utilizar para transmisiones asíncronas.
- ✓ SDLC (Protocolo de control de enlace de datos síncrono) Es un protocolo de enlace de datos WAN diseñado por IBM para entornos SNA (Arquitectura de redes de sistema). El SDLC define un ambiente WAN multipunto permitiendo que varias estaciones se conecten a un recurso dedicado, en el cual define una estación primaria y una o más estaciones secundarias.
- ✓ LAPB (Procedimiento de acceso al enlace equilibrado). Es un protocolo de enlace de datos utilizado por X.25 que es tanto orientado a la conexión como fiable por sus capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retransmisión y reconocimiento de marcos.
- ✓ LAPD (Procedimiento de acceso al enlace en el canal D). El protocolo WAN de enlace de datos utilizado para la señalización y establecimiento de llamadas en un canal D de RDSI. Las transmisiones de datos tienen lugar en los canales B de RDSI.

Los estándares WAN están definidos por un número de autoridades reconocidas, incluidas las siguientes agencias:

- ✓ Unión internacional de telecomunicaciones-Sector de estandarización de las telecomunicaciones (ITU-T).
- ✓ Organización internacional para la estandarización (ISO).
- ✓ Grupo de trabajo de Internet (IETF).
- ✓ Asociación de industrias electrónicas (EIA).

Los estándares WAN normalmente describen los requisitos tanto en la capa física como de la capa de enlace de datos. La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuitos (DCE). Normalmente, un dispositivo DCE es un equipo que provee servicio a un dispositivo DTE, quien a su vez es un cliente conectado DTE.

Estándares WAN:

- ✓ EIA/TIA-232.
- ✓ EIA/TIA-449.
- ✓ V.24.
- ✓ V.35.
- ✓ X.21.
- ✓ G.703.
- ✓ EIA-530.
- ✓ HSSI.

2.4.2.3 Dispositivos WAN.

Por definición, las WAN conectan dispositivos separados por áreas geográficas amplias. Utilizan un gran número de tipos de dispositivos específicos para los ambientes WAN, entre estos dispositivos cabe incluir los siguientes:

- Routers
- Switches
- Modems
- Servidor de Comunicaciones

Una WAN contiene una colección de equipos dedicadas a ciertas tareas, estos equipos se llaman hosts. Los Hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de host a otro.

2.4.2.4 Tecnologías WAN.

Las tecnologías WAN son agrupadas en categorías de servicios de circuito conmutado, servicios de paquete conmutado, servicios de celda conmutada, servicios digitales dedicados y servicios analógicos.

Servicios de circuito conmutado.

La conmutación de circuitos se establece, mantiene y termina en un circuito físico dedicado a través de una red de transporte para cada sesión de comunicación. La comunicación de circuitos maneja dos tipos de transmisiones: transmisiones de datagramas, que están compuestas de tramas direccionadas de manera individual, y transmisiones en ráfagas de datos, que están compuestas de una ráfaga de datos para que la verificación de direcciones sólo se presente una vez. Existen dos servicios de circuito conmutado: POTS y RDSI de banda estrecha.

- POTS (Servicio telefónico analógico convencional). No es un servicio de datos de computadora. No se incluye por dos razones: muchas de sus tecnologías son parte de la creciente infraestructura de datos, y es un modelo de una red de comunicaciones de área amplia increíblemente fácil de utilizar. El medio típico son los cables de cobre de par trenzado. Es el servicio utilizado con una conexión telefónica estándar y aún es la forma más común de que un usuario de PC doméstico se conecte a Internet.
- RDSI de banda estrecha (Red digital de servicios integrados de banda estrecha). Fue el primer servicio de conexión telefónica completamente digital.

Servicios de paquete conmutado.

Éste es un método de comunicación en el que los dispositivos de la red comparten un sólo enlace punto a punto para transferir los datos formateados en forma de paquetes desde un origen hasta un destino a través de una red de transporte, cada paquete es dinámicamente conmutado (enrutado) al siguiente enlace, es decir, los protocolos son sin conexión.

- **X.25**. Aunque se trata de una antigua tecnología aún se utiliza. Tiene capacidades extensivas de comprobación de errores desde los días en que los enlaces WAN eran más propensos a ellos, lo que lo hace fiable pero limita su ancho de banda.
- **Frame Relay**. Una tecnología WAN extremadamente popular por derecho propio, Frame Relay es más eficiente que X.25, ofrece servicios similares. El ancho de banda máximo es de 44,736 Mbps.

Servicios de celda conmutada.

Una celda conmutada es lo mismo que un paquete. La verdadera diferencia es que un paquete es de tamaño variable y una celda es de tamaño fijo. Los servicios de celda conmutada incluyen los siguientes:

- **ATM** (Modo de transferencia asíncrona). ATM utiliza pequeñas tramas de longitud fija (53 bytes) para transportar los datos. El ancho de banda máximo es actualmente de 622 Mbps, aunque se está desarrollando soporte para velocidades más altas.
- **SMDS** (Servicios de datos multimegabits conmutado). Relacionado muy cerca con ATM, SMDS se utiliza normalmente en MAN (redes de área metropolitana). El ancho de banda es de 44,736 Mbps.

Servicios digitales dedicados.

Los servicios digitales dedicados también son de circuito conmutado, pero la conexión es una conexión "siempre activa":

- **T1, T3, E1, E3**. La serie T de servicios en EEUU y la serie E de servicios de Europa son tecnologías WAN extremadamente importantes. Al igual que el servicio de marcación, utilizan multiplexión por división de tiempo para "sectorizar" y asignar franjas de tiempo a la transmisión de datos; a continuación se muestra los anchos de banda de estos servicios (hay disponibilidad de otros anchos de banda):

- **T1: 1,544 Mbps**
- **T3: 44,736 Mbps**
- **E1: 2,048 Mbps**
- **E3: 34, 368 Mbps**

- **xDLS**. DSL significa línea digital de abonado, y la "x" indica una familia de tecnologías. Esta tecnología WAN es relativamente nueva y en desarrollo, propuesta para el uso doméstico, tiene un ancho de banda que disminuye cuando aumenta la distancia desde el equipo de la compañía telefónica. La "x" indica la familia completa de tecnologías DSL, incluidas las siguientes:

  - **HDSL** de alta velocidad de bits.
  - **SDSL** de línea única.
  - **ADSL** asimétrica.
  - **VDSL** de muy alta velocidad de bits.
  - **RADSL** de velocidad adaptable.

- **SONET** (Red óptica síncrona). Una familia de tecnologías de capa física de alta velocidad. SONET se diseñó para fibra óptica, pero también se puede implementar sobre canales de cobre. Se implementa a diferentes tipos de portadora óptica (OC), que van desde 51,84 Mbps (OC-1) hasta 9952 Mbps (OC-192).

2.4.3 Redes Virtuales.

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la necesidad de la gestión del administrador de la red cuando se producen cambios en los miembros del grupo. Más importante aún, es el hecho de la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma contínua, por su conexión al mismo segmento de la red o concentrador.

La definición de VLAN (Virtual LAN o red virtual), proporciona los medios adecuados para solucionar esta situación, por medio de la agrupación realizada de una forma lógica en lugar de una manera física.

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs o concentradores, de tal manera que ésto permite un control más inteligente del tráfico de la red, ya que éste dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

Finalmente se debe mencionar que existe un inconveniente con ésta tecnología, y es que al no tener un estándar definido (aunque la IEEE ha trabajado en el estándar 802.1q) se ha dejado libertad a los proveedores de equipos de redes, para que ellos mismos implementen sus propios protocolos, arquitectura y encapsulado de tramas.

2.4.3.1 VLAN's (LAN's Virtuales).

Las LAN Virtuales o mejor conocidas como VLAN (Virtual Local Area Network), consiste en una red de varios sistemas de orilla o cualquier host o equipo de red

(switches y routers), del cual todos son miembros de un dominio lógico de difusión (broadcast) único. Una VLAN no tiende a ser amplia físicamente por su cercanía al dominio de broadcast. La VLAN se apoya de varios aspectos en los equipos de red (ejemplo LAN Switches) estos soportan el enlace que hacen entre los protocolos de la VLAN. Cada una de las VLAN's se apoya por Spanning Tree (IEEE 802.1q), de este modo dividen a las VLAN's de tal forma que trabajen de manera independiente.

Tipos de VLAN.

- VLAN de puerto central: VLAN en la que todos los nodos en la misma VLAN se conectan al mismo puerto de switch.
- VLAN dinámica: VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos.
- VLAN estática: VLAN en la que los puertos de un switch se asignan estáticamente.

La utilidad de las VLAN radica en que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN o WAN, incluso situándose en distintos equipos de la misma red, de esta manera los usuarios pertenecientes a un grupo pueden mantener su pertenecía a un grupo lógico de trabajo, como se muestra en la Fig. 2.4 .

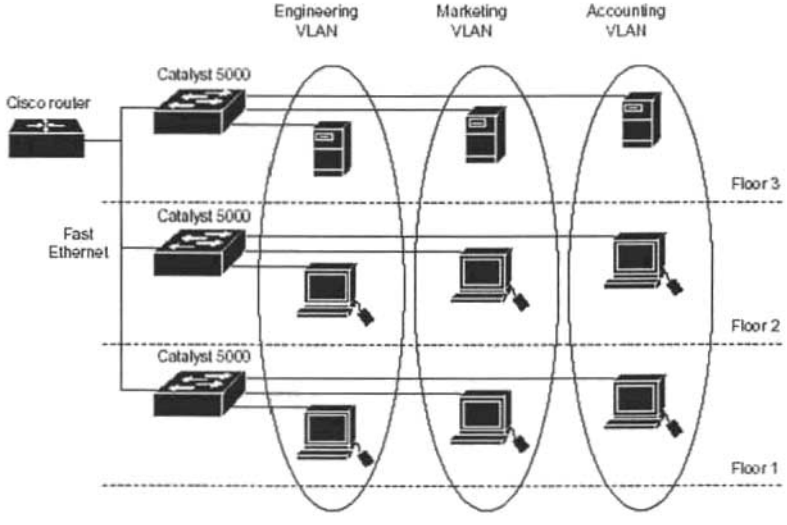


Fig. 2.4 VLAN's como redes definidas logicamente.

Características de las VLAN's:

- Control del Broadcast. Tal como los switches aíslan los dominios de colisión para adjuntar hosts y únicamente reenviar el tráfico de salida destinado a un puerto particular, las VLAN's afinan este concepto más allá y proporcionan completamente un asilamiento entre las VLAN's.
- Seguridad. Si no se incluye en un router una VLAN, ningún usuario fuera de esta VLAN podrá comunicarse con los usuarios dentro de la VLAN y viceversa.
- Rendimiento. Asignación a los usuarios de las VLAN's de un alto rendimiento de red que así lo requieran

- Administración de red. Utilización de software con el cual se permitiría la asignación de VLAN's a los usuarios y después la reasignación a otra VLAN, con ello la reconfiguración lógica de la LAN en segundos.

2.4.3.2 VPN's (Virtual Private Networks).

Una VPN (Virtual Private Network) es un sistema de simulación de una red privada sobre una red pública, en la cual los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están en redes públicas; por medio de la creación de túneles. Además agregan encriptación de manera que el tráfico que cruce por la red no pueda ser espiado, interceptado, leído o modificado, y autentificar positivamente cualquier extremo del enlace de comunicación de manera que no puedan acceder a los recursos del sistema.

Tunneling.

Esto es realizado por un proceso de "tuneleo" (Tunneling), por el cual un router encapsula un protocolo de la capa 3 dentro de otro protocolo (típicamente IP) para transportarlo a través de una red a otro router. El router desencapsula el paquete al momento de recibirlo. Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel. Este proceso se puede apreciar mejor en la fig. 2.5 (Vista lógica).

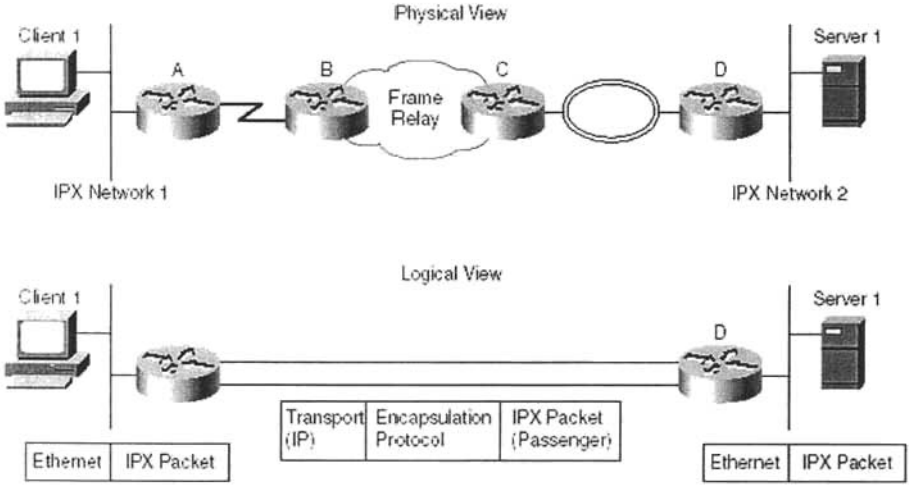


Fig. 2.5 Vista física y logica del proceso de "tuneleo".

Protocolos de tunneling.

El túnel requiere de tres diferentes protocolos:

- **Passenger protocol.:** El origen de la transportación de datos (IPX, NetBeui, IP).

- **Protocolo de encapsulación.**: Es el protocolo que se envuelve alrededor del dato original (GRE, IPSec, L2F, PPTP, L2TP)
- **Carrier protocol.:** Es el protocolo usado por la red sobre el cual la información está viajando.

La tecnología de túnel se puede basar en el protocolo de túnel de Nivel 2 o de Nivel 3; estos niveles corresponden al modelo referencia de interconexión de sistemas abiertos (OSI).

- **Protocolo de Nivel Dos:** Los protocolos de nivel 2 corresponden al nivel de enlace de datos, utilizando tramas (frames) como unidad de intercambio. PPTP y L2TP, en el envío de nivel 2 son los protocolos de túnel de nivel 2(L2F), ambos encapsulan el paquete útil en una trama de protocolo de punto a punto (PPP) que se enviará a través de la red.
- **Protocolo de Nivel Tres.**: Correspondiente al nivel de red, con el cual utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP (IP Sec) es un ejemplo de los protocolos de túnel de nivel 3; estos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

Tipos de redes virtuales privadas.

- **VPN de Acceso Remoto.**: Usado por usuarios remotos que usan conexiones de Internet. Cada usuario utiliza un túnel para comunicarse a la LAN principal.
- **VPN de Intranet.**: Permite a oficinas y/o usuarios acceder de forma segura a aplicaciones TCP/IP y/o datos que se ejecutan en los servidores de la LAN accediendo sólo los usuarios u oficinas autorizadas dentro de la red interna.
- **VPN de Extranet**: Las VPN's permiten un acceso seguro a las extranet en las cuales conectan redes IP privadas con acceso de mayor calidad para los involucrados.

2.5 Métodos de transmisión en redes.

La transmisión de datos en las LAN cae dentro de tres clasificaciones: unidifusión (unicast), multidifusión (multicast) y difusión (broadcast). En cada tipo de transmisión, se envía un sólo paquete a uno o más nodos.

En las transmisiones de unidifusión, se envía un sólo paquete desde el origen a un destino de la red. Primero, el nodo origen direcciona el paquete utilizando la dirección del nodo destino. Luego el paquete es enviado a la red y, finalmente, la red transfiere el paquete a su destino.

Las transmisiones de multidifusión constan de un sólo paquete de datos que se copia y envía a un subconjunto específico de nodos en la red. Primero, el nodo origen direcciona el paquete utilizando una dirección de multidifusión. Luego el paquete es enviado a través de la red, la cual genera copias del paquete y envía estas copias a cada uno de los nodos que se indica en la dirección de multidifusión.

Las transmisiones de difusión constan de un solo paquete de datos que se copian y envía a todos los nodos de la red. En este tipo de transmisiones, el nodo origen dirige el paquete utilizando la dirección de difusión. El paquete después es enviado a través de la red, la cual hace copias del paquete y las envía a cada uno de los nodos de la red.

2.6 Topologías de red.

La topología define la estructura de una red, su definición contiene dos partes: la topología física, que es el diseño real del cableado "el medio", y la topología lógica, que define cómo los hosts accede a los medios. La topología física (ver fig. 2.6) que se usa normalmente es en bus, en anillo, en estrella extendida, jerárquica y en malla.

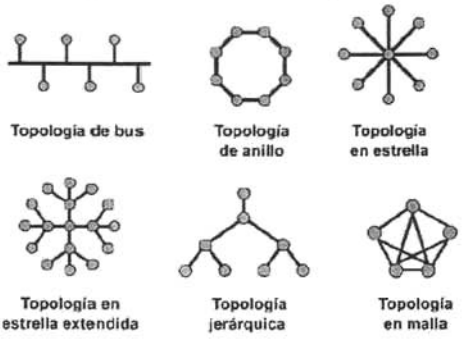


Fig. 2.6 Topologías físicas de red.

- **Topología en bus**. Emplea un único segmento de medio físico al que todos los hosts se conectan de forma directa.
- **Topología en anillo**. Conecta un host con el siguiente y al último hosts con el primero. Esto crea un anillo físico de cable.
- **Topología en estrella**. Conecta todos los cables a un punto central de concentración. Este punto normalmente es un hub o un switch.
- **Topología en estrella extendida**. Emplea la topología en estrella. Enlaza estrellas individuales enlazando sus hubs/switch.
- **Topología jerárquica**. Similar a la topología en estrella extendida, pero en lugar de enlazar hubs y switches, cada sistema secundario (subordinado) se enlaza a una computadora principal que controla el tráfico de la topología.
- **Topología en malla**. Se emplea cuando no puede hacer ninguna ruptura en la comunicación.

2.7 Medios de transmisión.

Para propagarse, una señal debe viajar a través de un medio, llamado medio de transmisión (fig. 2.7). Para su estudio, generalmente se clasifican en físicos (alámbricos) y No Físicos (inalámbricos).

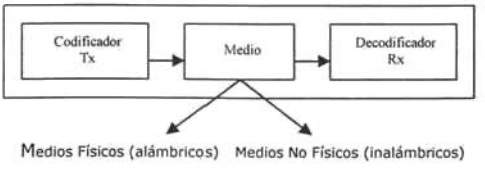


Fig. 2.7 Sistema de comunicación.

2.7.1 Alámbricos.

El cableado de cobre es el medio más común de unión entre hosts y dispositivos en redes locales. Existen varios tipos de cableado de cobre como son el coaxial, par trenzado y la fibra óptica. Sin embargo, sólo se mencionarán el par trenzado y la fibra óptica, debido a que el cable coaxial actualmente ya está en desuso.

Dentro del par trenzado existen dos tipos de cable que son: el par trenzado blindado (STP) y el par trenzado no blindado (UTP).

Par trenzado blindado (STP).

En la fig. 2.8 se puede observar que el cable STP está formado por una capa exterior plástica aislante y una capa interior de papel metálico, dentro de la cual se sitúan normalmente cuatro pares de cables, trenzados par a par, con revestimientos plásticos de diferentes colores para su identificación. Combina las técnicas de blindaje, cancelación y trenzado de cables. Según las especificaciones de uso de las instalaciones de red Ethernet, STP proporciona resistencia contra la interferencia electromagnética y de la radiofrecuencia sin aumentar significativamente el peso o tamaño del cable. El cable de par trenzado blindado tiene las mismas ventajas y desventajas que el cable de par trenzado no blindado. STP brinda mayor protección contra todos los tipos de interferencia externa, pero es más caro que el cable de par trenzado no blindado.

Fig. 2.8 Estructura interna del par trenzado blindado (STP).

A diferencia del cable coaxial, el blindaje en el STP no forma parte del circuito de datos y, por lo tanto, el cable debe estar conectado a tierra en ambos extremos. Normalmente, los instaladores conectan STP a tierra en el armario para el cableado y el hub, aunque esto no siempre es fácil de hacer, especialmente si los instaladores intentan usar paneles de conexión antiguos que no fueron diseñados para cable STP. Si la conexión a tierra no está bien realizada, el STP puede transformarse en una fuente de problemas, ya que permite que el blindaje actúe como si fuera una antena, absorbiendo las señales eléctricas de los demás hilos del cable y de las fuentes de ruido eléctrico que provienen del exterior del cable.

No es posible realizar tendidos de cable STP tan largos como con otros medios de networking (como por ejemplo, cable coaxial) sin repetir la señal, siendo la longitud máxima de cable recomendada de unos 100 metros.

Se especifica otro tipo de STP para instalaciones Token Ring. En este tipo de cable, conocido como STP de 150 ohmios, el cable no sólo está totalmente blindado para reducir la interferencia electromagnética y de radiofrecuencia, sino que a su vez cada par de hilos trenzados se encuentra blindado con respecto a los demás para reducir la diafonía. Si bien el blindaje empleado en el cable de par trenzado blindado de 150 ohmios no forma parte del circuito, como sucede con el cable coaxial, aún así debe estar conectado a tierra

en ambos extremos. Este tipo de cable STP requiere una cantidad mayor de aislamiento y de blindaje. Estos factores se combinan para aumentar de manera considerable el tamaño, peso y costo del cable. También requiere la instalación de grandes armarios o racks y conductos para el cableado, lujos que en muchos edificios antiguos no pueden permitirse.

Para la conexión de los cables STP a los diferentes dispositivos de red se usan unos conectores específicos, denominados conectores STP, similares a los RJ-45 descritos más abajo.

Par trenzado no blindado (UTP).

Compuesto por cuatro pares de hilos, trenzados par a par, y revestidos de un aislante plástico de colores para la identificación de los pares (Fig. 2.9). Cada par de hilos se encuentra aislado de los demás. Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuanto trenzado se permite por unidad de longitud del cable.

Fig. 2.9 Estructura interna del par trenzado no blindado (UTP).

Cuando se usa como medio de networking, el cable UTP tiene cuatro pares de hilos de cobre de calibre 22 ó 24. El UTP que se usa como medio de networking tiene una impedancia de 100 ohmios. Esto lo diferencia de los otros tipos de cables de par trenzado, como, por ejemplo, los que se utilizan para los teléfonos. Como el UTP tiene un diámetro externo de aproximadamente 0.43 cm., el hecho de que su tamaño sea pequeño puede ser ventajoso durante la instalación. Como el UTP se puede usar con la mayoría de las arquitecturas de networking principales, su popularidad va en aumento.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios de networking. De hecho, el cable UTP cuesta menos por metro que cualquier otro tipo de cableado de LAN, sin embargo, la ventaja real es su tamaño. Como su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Este puede ser un factor sumamente importante para tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ-45, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad.

Sin embargo, el cableado de par trenzado también tiene una serie de desventajas. El cable UTP es más sensible al ruido eléctrico y la interferencia que otros tipos de medios

de networking. Además, en una época el cable UTP era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable UTP es el más rápido entre los medios basados en cobre.

La distancia máxima recomendada entre repetidores es de 100 metros, y su rendimiento es de 10-100 Mbps.

Cable de fibra óptica.

Puede conducir transmisiones de luz moduladas. Una guía cilíndrica de diámetro muy pequeño (de 8 a 100µm), recubierta por un aislante, transporta la señal luminosa (ver fig. 2.10). El haz de luz se propaga, por el núcleo de la fibra. El diámetro exterior varía entre 100 y 500 µm. Si se compara con otros medios de networking, es más caro, sin embargo, no es susceptible a la interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera de los demás tipos de medios de networking descritos aquí. El cable de fibra óptica no transporta impulsos eléctricos, como lo hacen otros tipos de medios de networking que usan cables de cobre. En cambio, las señales que representan a los bits se convierten en haces de luz.

El cable de fibra óptica (fig. 2.11) está compuesto por dos fibras envueltas en revestimientos separados. Si se observa una sección transversal de este cable, veremos que cada fibra óptica se encuentra rodeada por capas de material amortiguador protector, normalmente un material plástico como Kevlar, y un revestimiento externo. El revestimiento exterior protege a todo el cable. Generalmente es de plástico y cumple con los códigos aplicables de incendio y construcción. El propósito del Kevlar es brindar una mayor amortiguación y protección para las frágiles fibras de vidrio que tienen el diámetro de un cabello. Siempre que los códigos requieran que los cables de fibra óptica deban estar bajo tierra, a veces se incluye un alambre de acero inoxidable como refuerzo.

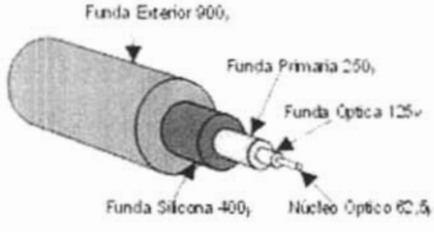


Fig. 2.10 Dimensiones de los revestimientos de una fibra óptica.

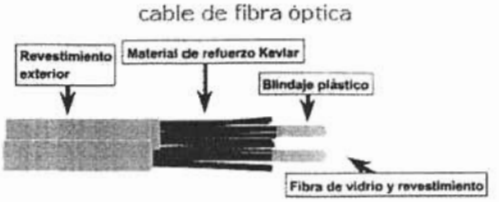


Fig. 2.11 Revestimientos del un cable de fibra óptica.

Las partes que guían la luz en una fibra óptica se denominan núcleo y revestimiento. El núcleo es generalmente un vidrio de alta pureza con un alto índice de refracción. Cuando el vidrio del núcleo está recubierto por una capa de revestimiento de vidrio o de plástico con un índice de refracción bajo, la luz se captura en el núcleo de la fibra. Este proceso se denomina reflexión interna total y permite que la fibra óptica actúe como un "tubo de luz", guiando la luz a través de enormes distancias, incluso dando vuelta en codos.

La longitud máxima de cable recomendada entre nodos es de 2.000 metros, y su rendimiento es alto, de 100 o más Mbps.

Principales Características:

- Alta velocidad de propagación.
- Atenuación débil, transporte a largas distancias.
- Sin problemas de toma de tierra.
- Inmunidad contra las perturbaciones electromagnéticas.
- Sin diafonía.
- Instalación en medio explosivo.
- Discreción e inviolabilidad de la conexión.
- Resistencia a la corrosión.

Existen dos tipos de fibra que son:

- Fibra monomodo.
- Fibra Multimodo: de gradiente gradual y de índice escalonado.

Fibra Monomodo.

Potencialmente, ésta es la fibra que ofrece la mayor capacidad de transporte de información. Tiene una banda de paso del orden de los 100 GHz/km. Los mayores flujos se consiguen con esta fibra, pero también es la más compleja de implantar. La fig. 2.12 muestra que sólo pueden ser transmitidos los rayos que tienen una trayectoria que sigue el eje de la fibra, por lo que se ha ganado el nombre de "monomodo" (modo de propagación, o camino del haz luminoso, único). Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten, es decir, de unos 5 a 8 μm. Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Los elevados flujos que se pueden alcanzar constituyen la principal ventaja de las fibras monomodo, ya que sus pequeñas dimensiones implican un manejo delicado y entrañan dificultades de conexión que aún no se dominan.

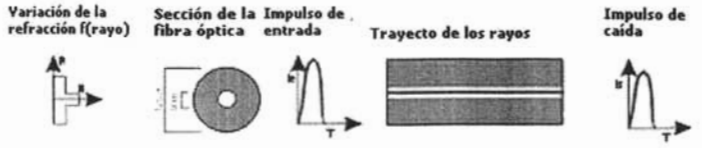


Fig. 2.12 Trayectoria del haz luminoso en la fibra monomodo.

Fibra multimodo de gradiente gradual.

Las fibras multimodo de índice de gradiente gradual tienen una banda de paso que llega hasta los 500MHz por kilómetro. Su principio se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra, como se puede ver en la fig. 2.13. Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra.

La fibra multimodo de índice de gradiente gradual de tamaño 62,5/125 µm (diámetro del núcleo/diámetro de la cubierta) está normalizado, pero se pueden encontrar otros tipos de fibra:

- Multimodo de índice escalonado 100/140 µm;
- Multimodo de índice de gradiente gradual 50/125 µm

Fig. 2.13 Trayectoria del haz luminoso en la fibra multimodo de gradiente gradual.

Fibra óptica de índice escalonado.

Las fibras multimodo de índice escalonado están fabricadas a base de vidrio, con una atenuación de 30 dB/km, o plástico, con una atenuación de 100 dB/km. Tienen una banda de paso que llega hasta los 40 MHz por kilómetro. En estas fibras, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea (fig. 2.14). El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice, de ahí su nombre de índice escalonado.

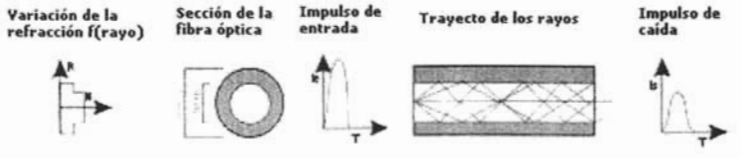


Fig. 2.14 Trayectoria del haz luminoso en la fibra óptica de índice escalonado.

En la tabla 2.2 se muestra unas de las principales especificaciones técnicas de los diferentes tipos de fibras ópticas:

Características	Fibras Multimodo		Fibras monomodo
	Índice escalonado	índice de gradiante gradual	
Diámetro del núcleo	100µm<Ø<600µm	50µm<Ø<100µm	8µm<Ø<10µm
Diámetro de cubierta	140µm<Ø<1000µm	25µm<Ø<150µm	125µm
Índice del núcleo	constante	carece del centro a la periferia	creciente o decreciente
Apertura numérica	0.30	0.20 a 0.27	muy pequeña I=0
Banda de Paso	20 a 10 Mhz/Km	200 a 1200 Mhz/km	>10Ghz/Km, no significativa
Atenuación según las ventanas			
0,85µm	8 a 20 dB/Km		
1,3µm		2,5 a 4 dB/Km	0,3 a 0,5 dB/Km
1,55µm		0,6 a 1,5 dB/Km	0,150 a 0,3dB/KM

Tabla 2.2 Especificaciones técnicas de las fibras ópticas.

2.7.2 Inalámbricos.

Se basan en la transmisión de ondas electromagnéticas, que pueden recorrer el vacío del espacio exterior y medios como el aire, por lo que no es necesario un medio físico para las señales inalámbricas, lo que hace que sean un medio muy versátil para el desarrollo de redes.

Conforme al espectro electromagnético (fig. 2.15) podemos dividir las ondas electromagnéticas de acuerdo a sus rangos de frecuencia y son:

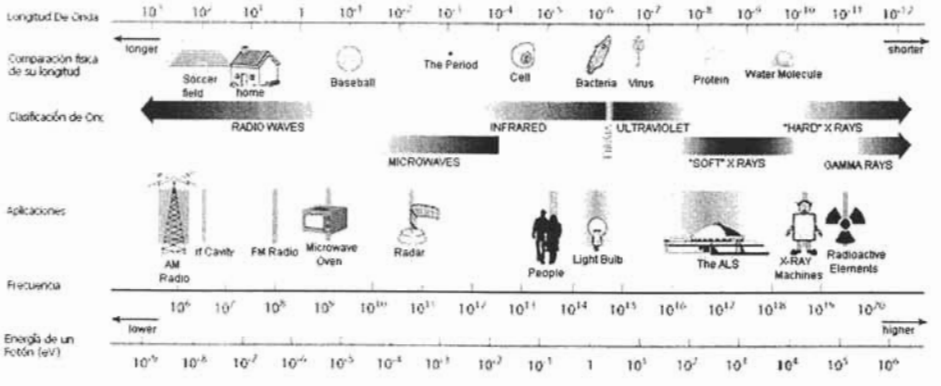


Fig. 2.15 Espectro electromagnético de las diferentes ondas electromagnéticas.

Señales de radio.

Consiste en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesario la visión directa de emisor y receptor. El rango de frecuencias en que oscila es de 10^2 a 10^6 hertz.

La velocidad de transmisión suele ser baja: 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Microondas.

Los enlaces de microondas se utilizan mucho como enlaces en lugares donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de SHF, de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.

Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2,4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionar hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.

Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

Las microondas se utilizan principalmente para transmisiones de televisión o telefonía a través de satélites estacionarios.

Infrarrojo.

Permite la transmisión de información a velocidades muy altas: 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida. Los rayos infrarrojos oscilan en los rangos de frecuencias entre 300 GHz – 430 THz hertz.

Enlaces ópticos al aire libre.

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire.

El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la línea de visión. Las aplicaciones típicas para estos enlaces se encuentran en los campus de las universidades, donde las carreteras no permiten tender cables, o entre los edificios de una compañía en una ciudad en la que resulte caro utilizar los cables telefónicos.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las prestaciones de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s. El límite para comunicaciones fiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Existen dos efectos atmosféricos importantes a tener en cuenta con los enlaces ópticos al aire libre:

- La dispersión de la luz que atenúa la señal óptica en proporción al número y al tamaño de las partículas en suspensión en la atmósfera. Las partículas pequeñas, como la niebla, polvo o humo, tienen un efecto que es función de su densidad y de la relación existente entre su tamaño y de la longitud de onda de la radiación infrarroja utilizada. La niebla, con una elevada densidad de partículas, de 1 a 10 mm de diámetro, tienen un efecto más acusado sobre el haz de luz. Las partículas de humo, más grandes, tienen menor densidad y, por tanto, menor efecto.
- Las brisas ascensionales (originadas por movimientos del aire como consecuencia de las variaciones en la temperatura) provocan variaciones en la densidad del aire y, por tanto, variaciones en el índice de refracción a lo largo del haz. Esto da lugar a la dispersión de parte de la luz a lo largo del haz. Este efecto puede reducirse elevando el haz de luz lo bastante con respecto a cualquier superficie caliente o utilizando emisores múltiples. La luz de cada emisor se ve afectada de diferente forma por las brisas, y los haces se promedian en el receptor.

Estos sistemas suelen emplearse para transmisiones digitales de alta velocidad en banda base. En EE.UU, todos los fabricantes de productos láser deben tener una certificación que garantiza la seguridad de sus productos.

En la tabla 2.3 se muestra las principales ventajas y desventajas de los medios inalámbricos.

Microondas (Microwave)	Ventajas:	Velocidad de la luz Usa poco lugar	
	Desventaja:	Se propagan solamente en la línea visual	
Satélite	Ventajas:	Siempre a la vista	
	Desventaja:	Posicionamiento y descenso muy caros	
Sin cable (infrarrojo, luz, radio)	Ventajas:	Flexible, Portátil	
	Desventaja:	Más lento Sujeto a interferencias	

Tabla 2.3 Ventajas y desventajas de los medios inálambricos.

2.8 Elementos de interconexión.

Los requisitos de longitud de cable no son limitantes para la mayor parte de las redes pequeñas. Sin embargo, si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada.

La ventaja es que se dispone de varios dispositivos que extienden la longitud de la red. Cada uno de lo dispositivos y los métodos usados para expandir la red tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otros tipos de dispositivos para aumentar la flexibilidad y el valor.

En la actualidad existen diferentes arquitecturas de red, sin embargo, pese a que son compatibles en cierta forma con el Modelo OSI no especifican el mismo tipo de capas y los protocolos que utilizan son diferentes.

A continuación en la fig. 2.16 se representa en que capa del Modelo OSI, trabaja cada dispositivo de interconexión.

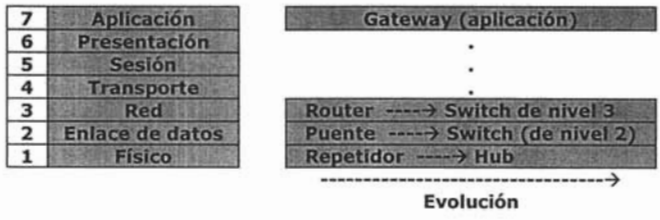


Fig. 2.16 Comparación de elementos de interconexión con el modelo OSI.

2.8.1 Repetidores.

Es un dispositivo que trabaja en la Capa Física del Modelo OSI. La finalidad de este dispositivo es incrementar el tamaño físico de la red, regenerando las señales para superar los efectos de la atenuación e interferencia del medio de transmisión, es decir, su función es incrementar la potencia de la señal de transmisión y limpiar la misma del ruido externo. Con un repetidor, la longitud del cable puede ser incrementado, así como el número de estaciones. Es necesario verificar el número máximo de repetidores que pueden ser conectados en un mismo segmento en las especificaciones del mismo. Los repetidores no son inteligentes. No aíslan el tráfico ni segmentan la red.

2.8.2 Concentradores (Hubs).

Son dispositivos que también trabajan en la Capa Física del modelo OSI. Un hub es un repetidor multipuertos. El repetidor únicamente regenera la señal, el hub además monitorea el segmento para verificar problemas de los equipos. En el caso de que el hub detecte un problema en alguno de sus puertos, puede desconectar a éste de la red; de esta forma el hub ayuda a tener una administración sencilla de la red. Además un hub permite la centralización de las topologías de red, actuando como punto de dispersión o centro de alambrado.

Las conexiones a hubs se denominan "conexiones de medios compartidos", ya que se comparte el total disponible de ancho de banda.

Tanto los repetidores como los hubs no pueden separar los dominios de colisión (fig.2.17).

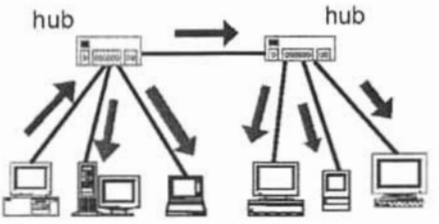


Fig. 2.17 Conexión entre hubs.

2.8.3 Puentes (Bridges).

Los puentes o bridges son dispositivos que trabajan en la Capa de Enlace de Datos del Modelo OSI. Ejecutan funciones de retraso siguiendo el protocolo MAC para conectar redes homogéneas. Su modo de funcionamiento es similar al de un filtro de direcciones, capturando las tramas que tienen como destino otro segmento y dejando el resto. Utilizan algoritmos de retransmisión muy simples, además separan los dominios de colisión pero no separa los dominios de difusión.

Funcionamiento:

- En Ethernet y 802.3 se usan puentes transparentes.
- En las retransmisiones se comporta como cualquier otra estación conectada a la LAN. Sigue el protocolo MAC (detección de colisiones, exponential back-off, etc.).
- Si el puerto de salida está ocupado se produce un retardo en la retransmisión.
  - Hay una cola de salida por cada puerto.
  - En caso de congestión podría descartar tramas.
- Cuando el puerto retransmite una trama usa la dirección origen de la trama original. No la dirección del puerto por el que se retransmite.
- Las estaciones finales no conocen la presencia del puente.

2.8.4 Conmutadores (Switches).

Este dispositivo opera en la capa de enlace de datos del Modelo OSI. Un conmutador tiene la característica de que cada nodo de la red dispone del ancho de banda completo de la LAN. El propósito del conmutador es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Básicamente un conmutador es un administrador inteligente del ancho de banda, aunque también existen switches capaces de trabajar en capa de red del modelo OSI, los cuales poseen algunas capacidades de un ruteador.

Otras de las características que presentan son:

- Diseñados para solucionar problemas de rendimiento de LAN (escasez de ancho de banda, cuellos de botella en la red).
- Alto rendimiento en el envío de paquetes y bajo tiempo de latencia.
- Segmentan un dominio de colisión en otros más pequeños como se muestra en la fig. 2.18.

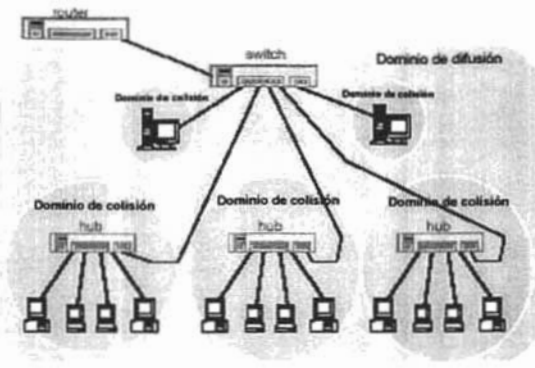


Fig. 2.18 Segmentación de dominios de colisión por medio de un switch.

2.8.5 Ruteadores (Routers).

Un ruteador es un dispositivo de *propósito general* diseñado para segmentar la red, con la idea de limitar el tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso a una WAN (ver fig. 2.19).

El ruteador opera en la capa de red del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes. El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente.
De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

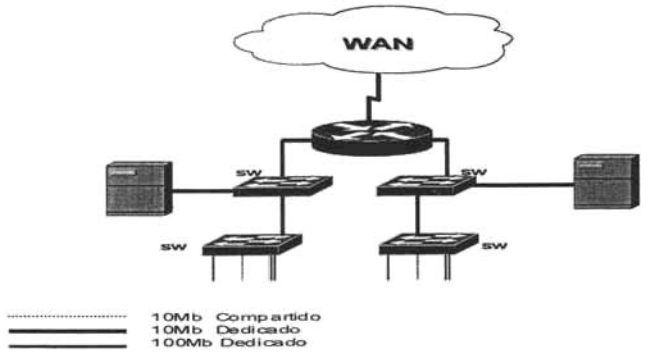


Fig. 2.19 Segmentación de la red por medio de un router.

Bases del enrutamiento.

Un host origen para enviar un paquete de información a un host destino, determina que debe direccionarlo diseccionado hacia una dirección física MAC de un ruteador, así como la dirección del protocolo a usar en el host destino.

El ruteador obtiene la información de la dirección destino del paquete, determinando si le es posible enviarlo al siguiente punto de conmutación o salto (hop) o no, mediante una comparación de la dirección destino con sus tablas de ruteo; si ésta se encuentra dentro de sus tablas de ruteo cambia la dirección física del paquete por la del siguiente punto de hop y reenvía el paquete, así consecutivamente hasta lograr llegar a su destino. Si el ruteador no contiene la dirección física dentro de sus tablas simplemente desecha el paquete.

Para comprender las bases del ruteo es importante la definición de los términos siguientes:

Ruteo: es el movimiento de la información a través de redes interconectadas, determinando la mejor ruta.

Mecanismo de enrutamiento: es el proceso que realiza un nodo o host para determinar de que manera manejará un paquete en base a una dirección destino.

Protocolos de ruteo: es el lenguaje con el que se comunican los ruteadores, para poder compartir información de la red y tomar decisiones, así como mantener y actualizar sus tablas. Los protocolos de ruteo utilizan un protocolo ruteable en la selección de la mejor ruta. Entre los protocolos de ruteo más usados son: RIP (Routing Information Protocol), IGRP/EIGRP (Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).

Protocolo ruteable: es cualquier protocolo que proporciona la suficiente información en su dirección de la capa de red para permitir el correcto envío de los paquetes de un host a otro. Los más utilizados son: IP (Internet Protocol), IPX (Internetwork Packet Exchange) y Apple Talk.

Tabla de ruteo: es la tabla que contiene información acerca de los posibles destinos en base a direcciones de red específicas. Estas tablas pueden ser configuradas de dos modos diferentes: estáticamente, que es la definida a la hora de su instalación y puede ser manipulada por los administradores de la red; dinámicamente, en el que son

utilizados algoritmos automáticos. Ambos sufren de desventajas, ya que el primero obliga a un procedimiento de configuración largo y tedioso; el segundo puede llegar a causar sobresaturación de la red por el constante intercambio de información de control entre los ruteadores instalados.

2.8.6 Puertas de enlace (Gateways).

Los gateways son ruteadores que implementados con software tienen la función de interconexión entre redes de varios fabricantes y tecnologías, así también, es un convertidor de protocolos ya que cumple como interfaz entre redes que manejan diferentes protocolos.

La funcionalidad de un gateway es desde la Capa de Transporte hasta la Capa de aplicación del Modelo OSI y la información que pasa a través de éstos es par a par que viene de las interfaces y programas o aplicaciones del usuario final.

En algunas ocasiones, se les divide en gateways de transporte, que sólo intervienen en los mecanismos de transporte, como por ejemplo el establecimiento de conexión y la traducción de direcciones; y gateways de aplicación que se encargan exclusivamente de analizar el contenido de los paquetes de datos.

La principal aplicación de los gateways en una red WAN es la de dar Servicios Proxy, como Compuertas de Acceso, Traducción de direcciones y Seguridad.

2.9 Transmisión de datos.

2.9.1 Modos de transmisión.

Transmisión simplex.

La transmisión simplex (sx) o *unidireccional* es aquella que ocurre en una dirección solamente, como se muestra en la fig. 2.20, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio, el paging unidireccional, etc.

Fig. 2.20 Transmisión simplex.

Transmisión half-duplex.

La transmisión half-duplex (hdx) permite transmitir en ambas direcciones (ver fig. 2.21); sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil (CB) donde el operador puede transmitir o recibir, pero no puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el

operador ha completado la transmisión, la otra parte debe ser avisada que puede empezar a transmitir (e.j. diciendo "cambio").

Fig. 2.21 Transmisión half duplex.

Transmisión full-duplex.

La transmisión full-duplex (fdx) permite transmitir en ambas direcciones y simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. Ejemplos de este tipo abundan en el terreno de las telecomunicaciones, el caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias.

Fig. 2.22 Transmisión full duplex.

2.9.2 Técnicas de transmisión

Transmisión asíncrona.

La transmisión asíncrona es aquella en la que se transmite o se recibe un caracter, bit por bit añadiéndole *bits de inicio*, y bits que indican el término de un paquete de datos, para separar así los paquetes que se van enviando/recibiendo para sincronizar al receptor con el transmisor. El bit de inicio le indica al dispositivo receptor que sigue un carácter de datos; igualmente el bit de término indica que el carácter o paquete ha sido completado.

Transmisión síncrona.

Este tipo de transmisión realiza el envío de un grupo de caracteres en un flujo continuo de bits. Para lograr la sincronización de ambos dispositivos (receptor y transmisor) ambos dispositivos proveen una señal de reloj que se usa para establecer la velocidad de transmisión de datos y para habilitar los dispositivos conectados a los módems para identificar los caracteres apropiados mientras estos son transmitidos o recibidos. Antes de iniciar la comunicación ambos dispositivos deben de establecer una sincronización entre ellos. Para esto, antes de enviar los datos se envían un grupo de caracteres especiales de sincronía. Una vez que se logra la sincronía, se pueden empezar a transmitir datos.

Por lo general los dispositivos que transmiten en forma síncrona son más caros que los asíncronos. Debido a que son más sofisticados en el hardware. A nivel mundial son más empleados los dispositivos asíncronos ya que facilitan mejor la comunicación.

2.10 Modelo de Referencia OSI.

2.10.1 Propósitos del Modelo de Referencia OSI.

En sus inicios los fabricantes tenían como objetivo el desarrollo de diferentes técnicas de transmisión o protocolos como respuesta a las necesidades de comunicación entre redes, para el aprovechamiento de las máximas velocidades disponibles de transmisión y para implementar grados de control mas sofisticados. Sin embargo, se tuvo una desventaja, ya que los fabricantes se desarrollaban de manera independiente, lo cual dió lugar a la incompatibilidad entre equipos de diferentes fabricantes y mayor fue el problema cuando distintos departamentos de diferentes organizaciones adquirían equipos de diferentes fabricantes y la necesidad de la comunicación era indispensable , la comunicación no era posible.

Las necesidades llevaron al desarrollo de un sistema que permitiera lograr la independencia del hardware y software, portabilidad de la aplicación y el cumplimiento de los estándares. Dando origen más tarde al Modelo de Referencia OSI (Open Systems Interconnection, Interconexión de sistemas abiertos) que permitía la interconexión entre sistemas heterogéneos.

En 1979, la Organización Internacional de Normalización (ISO) definió su modelo de arquitectura de red OSI. Este modelo fue adoptado en 1980 por el Comité Consultivo Internacional de Telefonía y Telegrafía (CCITT) en su recomendación X.200.

Para la transmisión de datos se tienen dos aspectos importantes, que son el transporte y la manipulación de datos. Estos, se dividieron a su vez en subfunciones denominadas "capas". Por lo que, el Modelo de Referencia OSI está integrado por 7 capas.

2.10.2 Capas del Modelo de Referencia OSI.

El modelo OSI realiza 7 funciones vistas en forma general, las cuales se representan específicamente en 7 capas o niveles en la arquitectura de la red. Cada capa al realizar sus funciones específicas (ver fig. 2.23), asume que las capas inferiores o superiores, según se esté dando el flujo de la información, han cumplido correctamente con sus funciones.

Fig. 2.23 Funciones de las capas del Modelo OSI.

Capa 7: La capa de aplicación.

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales. Es el medio por el cual los procesos de aplicación de usuario acceden al entorno OSI.

Su función principal es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.

Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, estando éstas controladas por protocolos de aplicación, y utilizando los servicios del nivel de presentación.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Algunos ejemplos de procesos de aplicación son:

- programas de hojas de cálculo.
- programas de procesamiento de texto.
- transferencia de archivos (ftp).
- login remoto (rlogin, telnet).
- correo electrónico (mail - smtp).
- páginas web (http).

Capa 6: La capa de presentación.

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo. Es también la responsable de la obtención y liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

Por ello, de ser necesario, la capa de presentación realiza las siguientes operaciones:

- traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de la red y viceversa.
- definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, define el orden de transmisión y la estructura de los registros.
- definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).
- dar formato a la información para visualizarla o imprimirla.
- comprimir los datos si es necesario.
- aplicar a los datos procesos criptográficos.

Capa 5: La capa de sesión.

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos.

Sus principales funciones son:

- establece, administra y finaliza las sesiones entre dos hosts que se están comunicando.
- si por algún motivo una sesión falla por cualquier causa ajena al usuario, esta capa restaura la sesión a partir de un punto seguro y sin pérdida de datos o si esto no es posible termina la sesión de una manera ordenada, revisando y recuperando todas sus funciones, evitando problemas en sistemas transaccionales.
- sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos, estableciendo las reglas o protocolos para el diálogo entre máquinas y así poder regular quien habla y por cuanto tiempo o si hablan en forma alterna, es decir, las reglas del diálogo que son acordadas.
- ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- manejar **tokens**. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación.
- hacer **checkpoints**, que son puntos de recuerdo en la transferencia de datos.

Capa 4: La capa de transporte.

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. Para ello segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor.

El límite entre la capa de sesión y la capa de transporte puede imaginarse como el límite entre los protocolos de capa de medios y los protocolos de capa de host. Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones, las tres capas inferiores se encargan del transporte de datos. Además, esta capa es la primera que se comunica directamente con su par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte, liberándolas de luchar por conseguir una transferencia de datos segura y económica. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Se conocen con el nombre de **circuitos virtuales** a las conexiones que se establecen dentro de una subred, y en ellos no hay la necesidad de elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico posterior.

Podemos resumir las funciones de la capa de transporte en los siguientes puntos:

- controla la interacción entre procesos usuarios.
- incluye controles de integración entre usuarios de la red para prevenir pérdidas o doble procesamiento de transmisiones.
- controla el flujo de transacciones y direccionamiento de máquinas a procesos de usuario.
- asegura que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- acepta los datos del nivel de sesión fragmentándolos en unidades más pequeñas llamadas **segmentos** en caso necesario y los pasa al nivel de red.
- realiza funciones de control y numeración de unidades de información, fragmentación y reensamblaje de mensajes.
- se encarga de garantizar la transferencia de información a través de la sub-red.

Capa 3: La capa de red.

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. También se ocupa de aspectos de contabilidad de paquetes.

Es la responsable de las funciones de conmutación y encaminamiento de la información, proporcionando los procedimientos precisos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.

Podemos resumir las funciones de la capa de red en los siguientes puntos:

- divide los mensajes de la capa de transporte en unidades más complejas, denominadas **paquetes**, y los ensambla al final.
- debe conocer la topología de la subred y manejar el caso en que la fuente y el destino están en redes distintas.
- para ello, se encarga de encaminar la información a través de la sub-red, mirando las direcciones del paquete para determinar los métodos de conmutación y enrutamiento, además rutea los paquetes de la fuente al destino a través de ruteadores intermedios.
- envía los paquetes de nodo a nodo usando, ya sea un circuito virtual, o datagramas.
- debe controlar la congestión de la subred.

En esta capa es donde trabajan los routers.

Capa 2: La capa de enlace de datos.

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, formación y entrega ordenada de tramas y control de flujo. Por lo tanto, su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo.

Sus principales funciones son:

- establece los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- agrega una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato predefinido llamado **trama o marco**. Suelen ser de unos cientos de bytes.
- sincroniza el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, para evitar tramas repetidas se usan números de secuencia en ellas.
- envía los paquetes de nodo a nodo usando ya sea como un circuito virtual o como datagramas.
- controla la congestión de la red.
- regula la velocidad de tráfico de datos.
- controla el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- se encarga de la secuencia de enlace lógico y de acceso al medio (soportes físicos de la red).

Capa 1: La capa física.

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son movidos.

Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, topología física de red, técnicas de conversión análoga/digital, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física.

Sus principales funciones las podemos resumir en:

- definir las características físicas (componentes y conectores mecánicos) y eléctricas (niveles de tensión).
- definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- transmitir el flujo de bits a través del medio. No existe estructura alguna.
- maneja voltajes y pulsos eléctricos (0's o 1's).
- especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- garantizar la conexión, pero no la fiabilidad de ésta.

Esta capa solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter.

En la siguiente tabla 2.4 se muestra a grandes rasgos algunos de los principales dispositivos de red, así como algunos de los protocolos que trabajan en las capas del modelo OSI.

Nivel	Capa	Dispositivos y protocolos
1	Físico	Cables, tarjetas y repetidores (hub).
2	Enlace	Puentes (bridges). HDLC y LLC.
3	Red	Encaminador(router). IP, IPX
4	Transporte	Pasarela (gateway). UDP, TCP,SPP.
5	Sesión	Pasarela. Bula Data Transfer Protocol
6	Presentación	Pasarela. Compresión, encriptado.
7	Aplicación	X.400

Tabla 2.4 Comparación de dispositivos y protocolos con las capas del modelo OSI.

CAPÍTULO TRES

TCP / IP

3.1 Arquitectura TCP / IP.

Desde los años 70 el grupo de protocolos TCP/IP (Transmission Control Protocol / Internet Protocol) se ha convertido en el estándar de la industria. El conjunto de protocolos TCP/IP se desarrolló como parte de la investigación efectuada por la agencia de proyectos e investigación avanzada para la defensa (DARPA). Originalmente se desarrolló para proporcionar comunicación dentro de la DARPA. Posteriormente TCP/IP se incluyó con la distribución Berkeley de UNIX. Ahora TCP/IP es el estándar factor para las comunicaciones entre redes y sirve como pilar de los protocolos de transporte para Internet, permitiendo la comunicación a nivel global de computadoras.

Dentro de la pila de protocolos TCP/IP destacan: TCP e IP. IP es el protocolo de capa 3, según el modelo de referencia OSI. Un servicio sin conexión que proporciona un máximo esfuerzo de entrega (no fiable) por toda la red. TCP es un protocolo de capa 4 según el modelo de referencia OSI. Un servicio orientado a la conexión que proporciona control de flujo y fiabilidad. La unión de estos protocolos permite un mayor rango de servicios.

La arquitectura de TCP/IP está basada en capas, haciendo más fácil la implementación de nuevos protocolos. El modelo de capas del TCP/IP es diferente al modelo de referencia OSI (ver fig. 3.1).

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- ✓ Independencia tecnológica en la conexión de bajo nivel y la arquitectura.
- ✓ Conectividad a través de la Red.
- ✓ Reconocimiento de extremo a extremo.
- ✓ Protocolos estandarizados.

OSI	TCP/IP
Aplicación Presentación Sesión	Aplicación
Transporte	Transporte
Red	Internet
Enlace Físico	Interfaz de red (no definida por TCP/IP)

Fig. 3.1 Relación del Modelo TCP/IP con el Modelo OSI

Capas del Modelo TCP/IP.

El modelo TCP/IP tiene cuatro capas: la capa de Aplicación, la capa de Transporte, la capa de Internet y la Interfaz de red.

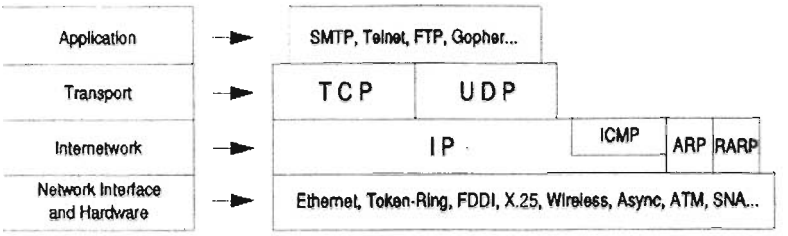


Fig. 3.2 Modelo de Capas de TCP/IP

3.2 Capa de acceso a la red.

Este nivel corresponde al hardware, estándares de la IEEE 802.3 entre otros. Además hay que hacer notar que esta capa no está definida por TCP/IP.

3.3 Capa de red.

Esta controla la comunicación entre un equipo y otro, conformado por protocolo IP, que proporcionan enrutamiento de datagramas sin conexión, con el máximo esfuerzo de entrega, no interesado por el contenido de los datagramas; por tanto no fiable. Busca la forma de llevar los datagramas a su destino.

3.3.1 RARP.

RARP (Reverse Address Resolution Protocol), es utilizado sólo en el caso en que el dispositivo o terminal no tenga una memoria o dispositivo de almacenamiento en el cual dar cabida a su dirección IP, en este caso se envía una petición RARP a un Servidor RARP el cual tiene almacenada la IP del dispositivo que así lo solicite. Esto es logrado al mandar un broadcast (difusión), y al encontrar el servidor RARP se le es enviada la dirección IP correspondiente.

3.3.2 ARP.

Para que los dispositivos se comuniquen, los dispositivos emisores necesitan las direcciones IP y MAC de los dispositivos de destino. Cuando intentan comunicarse con dispositivos cuyas direcciones IP ya conocen, deben determinar las direcciones MAC. El conjunto de protocolos TCP/IP tiene un protocolo, llamado ARP (Protocolo de Resolución Direcciones), y puede obtener automáticamente las direcciones MAC. ARP permite que una computadora encuentre la dirección MAC de la computadora que está asociada con una dirección IP

Las tablas del protocolo de resolución de direcciones (ARP) asignan las direcciones IP a sus correspondientes direcciones MAC. Las tablas ARP son secciones de la memoria RAM en las que la memoria caché se mantiene automáticamente en cada uno de los dispositivos. Cada computadora en la red mantiene una tabla ARP propia que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Siempre que un dispositivo de red desea enviar un paquete a través de la red, utiliza la información que le proporciona su tabla ARP.

Funcionamiento de ARP en una subred.

Si un host quiere enviar datos a otro host, debe saber las direcciones IP y MAC de destino. Si no puede localizar una dirección MAC para la dirección IP de destino en su tabla ARP, el host inicia un proceso que se llama petición ARP. Una petición ARP le permitirá descubrir la dirección MAC destino.

Un host construye un paquete de petición ARP y los envía a todos los dispositivos de la red, este paquete de petición ARP se divide en dos partes: la cabecera de la trama y el mensaje ARP.

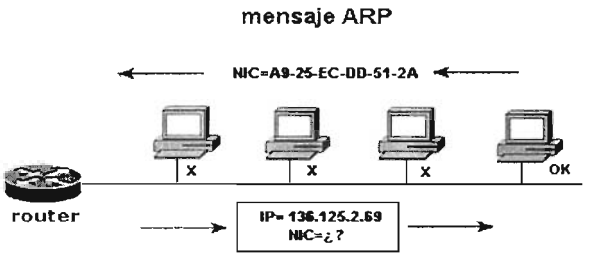


Fig. 3.3 Mensaje ARP en una subred.

Para asegurarse de que todos los dispositivos ven la petición ARP, el origen emplea una dirección MAC de difusión, como se muestra en la fig. 3.3. La dirección de difusión en el esquema de direccionamiento MAC tiene todas sus posiciones establecidas al valor hexadecimal F. Así, una dirección MAC de difusión tendría la forma FF-FF-FF-FF-FF-FF.

Debido a que los paquetes de peticiones ARP viajan en modo difusión, todos los dispositivos de la red local reciben los paquetes y los pasan a la capa de red para un examen más profundo. Si las direcciones IP de un dispositivo coinciden con las direcciones IP de destino de la petición ARP, el dispositivo responde enviando su dirección MAC de destino. A esto se le conoce como respuesta ARP.

Cuando el dispositivo de origen recibe la respuesta ARP, extrae la dirección MAC del campo de dirección hardware del remitente y actualiza su tabla ARP. El dispositivo de origen puede entonces dirigir adecuadamente sus datos con las direcciones IP y MAC de destino. También utiliza esta información para efectuar las encapsulaciones de las capas 2 y 3 de los datos, antes de enviarlos a la red.

Concepto avanzado ARP.

Uno de los problemas de las redes es el cómo comunicarse entre dispositivos de diferentes segmentos. El problema se divide en dos, primero obtener la dirección MAC del host de destino, o la de un router que puede enviar el paquete hasta el host de destino. Segundo transferir los paquetes de datos desde un segmento de red a otro, hasta llegar al host de destino. Para poder enviar un paquete a otro segmento de red se necesita de una puerta de enlace (Gateway) que es la dirección IP de la interfaz del gateway o router al cual se conecta el host de origen. El Gateway determina cual es el siguiente salto si a otro gateway o al equipo final.

Hay dos maneras más para poder hacer este tipo de comunicaciones la segunda es cuando los dispositivos escuchan los anuncios del router y guardan esta información, con

esta información los paquetes destinados a una red diferente se envían a la dirección MAC apropiada del router. La tercera es un proxy ARP en la cual un dispositivo envía una petición ARP sin importarle el destino, y el router responde con su dirección MAC contestando a la petición ARP. Si no existiese ningún gateway predeterminado, ni anuncios del router, ni respuesta a una petición ARP, no se puede enviar el paquete.

3.3.3 ICMP.

El protocolo ICMP (Internet Control Message Protocol), proporciona el medio para que el hosts y gateways se comuniquen. Los mensajes ICMP se transportan en los datagramas IP y se utilizan para enviar mensajes de error y control.

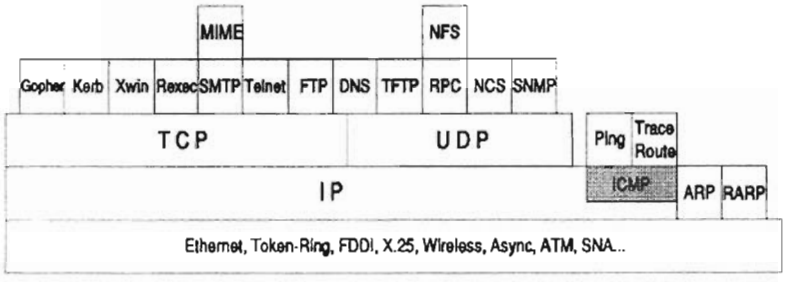


Fig. 3.4 Protocolo ICMP en el Modelo de capas TCP/IP.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión; esto será responsabilidad de los protocolos de las capas superiores, por ejemplo TCP (ver fig. 3.4).

Los mensajes ICMP viajan en el campo de datos de un datagrama IP, puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más ni más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla 3.1. El resto de los campos son distintos para cada tipo de mensaje ICMP.

Tipo	Mensaje
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Origen Extinguido (Sourch Quench)
5	Redireccionar (Redirect)
8	Solicitud de Eco (Echo)
11	Tiempo excedido (Time Exceded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Replay)
15	Solicitud de información (Information Request)
16	Respuesta de información (Information Replay)
17	Solicitud de máscara (Addressmask)
18	Respuesta de máscara (Addressmask Replay)

Tabla 3.1 Mensajes ICMP.

El formato y significado de cada mensaje de ICMP está documentado en el RFC 792.

3.3.4 IP (Internet Protocol).

El protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

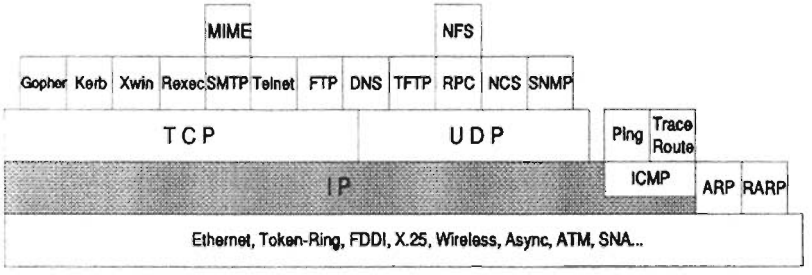


Fig. 3.5 Protocolo IP en el Modelo de capas TCP/IP.

Datagrama IP.

Un datagrama IP es la unidad de transferencia en el IP, contiene una cabecera y datos IP, y está rodeado por la cabecera de la capa del control de acceso al medio (MAC). Una trama se puede transmitir como una serie de datagramas que se reensamblan para dar lugar de nuevo a la trama en el equipo receptor. Los campos del datagrama son los siguientes (ver fig. 3.6):

- ✓ **Vers**. Número de versión
- ✓ **Longitud de la cabecera (Hlen)**. Longitud de la cabecera, palabras de 32 bits.
- ✓ **Tipo de servicio (TOS)**. Cómo se debería manipular el datagrama.
- ✓ **Longitud total**. Longitud total (cabecera + datos).
- ✓ **Identificación, flags, compensación de fragmentos**. Proporciona fragmentación de datagramas que permiten MTU (Maximum Transmission Unit) diferidas en la red.
- ✓ **TTL**. Tiempo de existencia
- ✓ **Protocolo**. El protocolo de capa superior (Capa 4) que envía y recibe el datagrama.
- ✓ **Suma de comprobación de la cabecera (checksum)**. Direcciones IP de 32 bits.
- ✓ **Opciones IP**. Pruebas, filtrado, seguridad y otras opciones de red.
- ✓ **Relleno.**

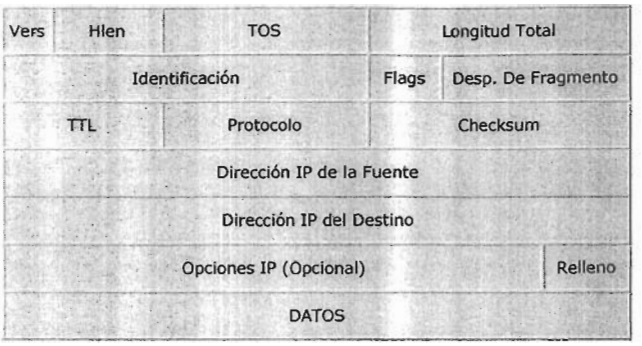


Fig. 3.6 Campos de un datagrama IP.

El campo Protocolo determina el protocolo de la Capa 4 portado dentro de un datagrama IP. Aunque la mayor parte del tráfico IP es TCP, otros protocolos también pueden utilizar IP. Cada cabecera IP debe identificar el protocolo de la Capa 4 de destino para el datagrama. Los protocolos de la capa de transporte se numeran, de forma similar a los números de puerto. IP incluye el número de protocolo en el campo Protocolo.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentada intencionalmente para permitir que el nodo con un buffer limitado pueda tomar todo el datagrama. Es responsabilidad del protocolo IP reensamblar los fragmentos del datagrama al orden correcto.

3.3.5 Direccionamiento IP.

El Protocolo IP identifica a cada host que se encuentra conectado a la red mediante su correspondiente dirección. Las direcciones IP se suelen expresar como números decimales separados por puntos. Los 32 bits de la dirección se dividen en cuatro octetos, el valor decimal máximo de cada octeto es de 255. El mayor número binario de 8 bits es 11111111 o en valor decimal 255.

Clases de direcciones.

La dirección de Internet (IP Address) se utiliza para identificar tanto al hosts en concreto como a la red a la que pertenece, de manera que sea posible distinguir a los hosts que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos. Una organización puede recibir tres clases de direcciones IP por parte del ARIN, RIPE, NCC, APNIC, o el ISP, que son los organismos encargados de asignar las direcciones IP según sea la región correspondiente.

Clase A.

Son las que en su primer byte tiene un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red (ver fig. 3.7). Esto significa que podrán existir 16, 777,214 millones de hosts en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, son pocas organizaciones que tiene una dirección de Clase A.

Clase B.

Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. Ver fig. 3.7. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del hosts permitiendo, por consiguiente, un número máximo de 64, 516 hosts en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de hosts que se necesitan conectar fuese mayor, sería posible obtener más de una dirección de Clase B, evitando de esta forma el uso de una Clase A.

Clase C.

En este caso, como se muestra en la fig. 3.7, el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 hosts en cada red. Estas direcciones permiten un menor número de hosts que las anteriores, aunque son las más numerosas pudiendo existir un gran número de redes de este tipo (más de dos millones).

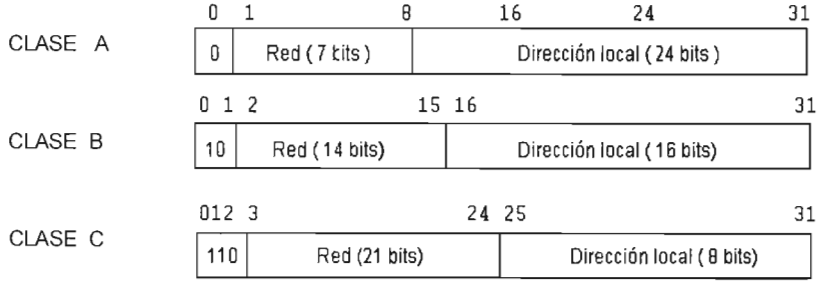


Fig. 3.7 Clases de direcciones IP.

Clase	Intervalo decimal del 1er octeto	Bits de orden superior del 1er octeto	ID de Red/Host (N=Red, H=Host)	Máscara de subred por defecto	Cantidad de Redes	Host por Red (Direcciones Utilizables)
A	1 - 126	0	N.H.H.H	255.0.0.0	126	16,777.214
B	128 - 191	1 0	N.N.H.H	255.255.0.0	16.382	65.534
C	192 - 223	1 1 0	N.N.N.H	255.255.255.0	2,097.150	254
D	224 - 239	1 1 1 0	Reservado para Multicast			
E	240 – 254	1 1 1 1 0	Experimental, se utiliza para investigación			

Tabla. 3.2 Clasificación de las direcciones IP.

En la clasificación de direcciones anteriores (tabla 3.2) se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D reservado para Multicast y E para uso experimental), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 del equipo está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, como en la identificación de host para máquinas que aún no saben su número de host dentro de la red, o en ambos casos.

El numero 255 del equipo tiene también un significado especial, puesto que se reserva para el broadcast (difusión) es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno.

3.3.6 IPv6 (Internet Protocol versión 6).

Esta es una nueva versión del protocolo IP, llamada IPv6, aunque también es conocida como IPng (Internet Protocol Next Generation). Es la versión 6, debido a que la número 5 no pasó de la fase experimental. La compatibilidad con la versión 4 es prácticamente total, ya que se han incluido características de compatibilidad. Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existía en la versión 4.

Esta cabecera ocupa el doble que la anterior versión, pero se ha simplificado omitiendo algunos campos y haciendo que otros sean opcionales. De esta manera, los routers no tienen que procesar tanta información. Los campos son los siguientes (ver fig.3.8):

- ✓ **Versión**: Este campo ocupa 4 bits, y contiene el número de versión del IP, en este caso 6.
- ✓ **Prioridad**: Ocupa 4 bits, e indica la importancia del paquete que se está enviando.
- ✓ **Etiqueta** de Flujo: Ocupa 24 bits. Indica que el paquete requiere un tratamiento especial por parte de los routers que lo soporten.
- ✓ **Longitud**: Ocupa 16 bits. Indica la longitud en bytes de los datos del mensaje
- ✓ **Siguiente Cabecera**: Ocupa 8 bits e indica a que protocolo corresponde la cabecera que está a continuación de la actual.
- ✓ **Tiempo de vida**: Ocupa 8 bits y tiene la misma función que la versión 4.
- ✓ **Dirección de origen**: Ocupa 128 bits (16 octetos), y es el número de dirección del origen.
- ✓ **Dirección de Destino**: Ocupa 128 bits (16 octetos). Es el número de dirección del destino.

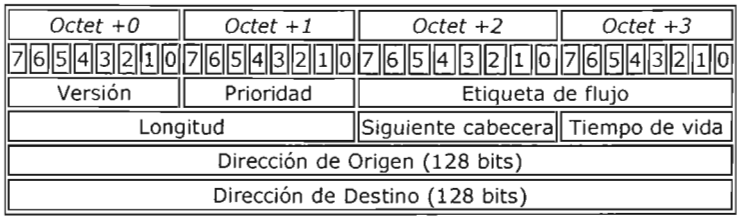


Fig. 3.8 Campos del datagrama Ipve6.

Direcciones IP Versión 6.

El cambio más significativo en las direcciones ha sido, que ahora, se refieren a un interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos mediante su interfaz.

El número de direcciones diferentes se ha multiplicado de una manera exagerada. Teóricamente, es posible tener 2128 direcciones diferentes. Este número quiere decir que se podrían llegar a tener más de 665.000 trillones de direcciones por metro cuadrado, aunque si siguieran una jerarquía, este número decrece hasta 1564 direcciones por metro cuadrado en el peor caso o tres trillones siendo optimistas.

En el IPv6 existen tres tipos básicos de direcciones:

- ✓ Direcciones unicast: Están dirigidas a un único interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.
- ✓ Direcciones anycast: Identifican a un conjunto de interfaces de red. El paquete se enviará a cualquier interfaz que forme parte del conjunto. En realidad son direcciones unicast que se encuentran asignadas a varios interfaces.
- ✓ Direcciones multicast: Identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente.

3.4 Capa de transporte.

En esta capa se encuentran dos protocolos: el protocolo de datagramas de usuario (UDP) y el protocolo de control de transmisión (TCP).

3.4.1 TCP (Transmission Control Protocol).

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

La cabecera de un datagrama contiene al menos 160 bits que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede ser que algunos no lleguen a su destino o lleguen con información errónea. Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, como se muestra en la fig. 3.9, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.

El campo final de la cabecera puede contener información opcional. En cualquier caso el tamaño de la cabecera debe ser múltiplo de 32 bits, por lo que puede ser necesario añadir un campo variable y que contenga ceros al final para conseguir este objetivo cuando se incluyen algunas opciones. El campo de HLEN contiene la longitud total de la cabecera TCP expresada en números de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

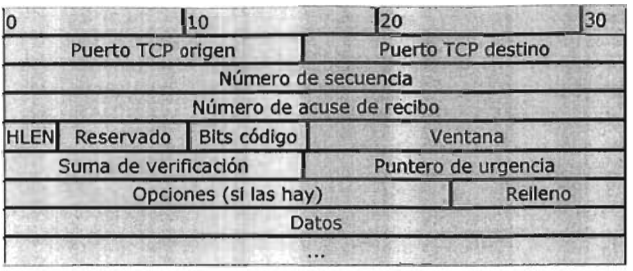


Fig. 3.9 Formato del segmento TCP.

- ✓ **Puerto de Origen.** Número del puerto que llama. Identifica el proceso de la capa superior en el extremo del origen de ese segmento, que puede ser o no el extremo que inicio la conexión.
- ✓ **Puerto de destino.** Número del puerto al que se llama. Del mismo modo, éste es el puerto asignado al final del destino para este segmento.
- ✓ **Número de Secuencia.** Número que se usa para asegurar la secuencia correcta en la llegada de los datos. Es el número de secuencia para el primer octeto en el campo de datos.
- ✓ **Número de acuse de recibo.** Apunta al número de secuencia del primer byte del próximo segmento que se espera recibir del otro lado. El siguiente octeto TCP que se espera.
- ✓ **Longitud de la cabecera (HLEN).** Número de palabras de 32 bits de la cabecera. El término HLEN no se emplea para nombrar a este campo de la cabecera TCP, aunque se aplica para un campo similar en la cabecera IP. El término que se emplea normalmente es "compensación de datos".
- ✓ **Reservado.** Establecido a cero.
- ✓ **Bits de código.** Funciones de control (como inicio y fin de una sesión). Este conjunto de bits se documenta normalmente como flags, "bits de código".
- ✓ **Ventana.** Número de octetos que aceptará el dispositivo. Es el tamaño del buffer disponible que tiene el emisor para recibir los datos.
- ✓ **Suma de Verificación.** Suma de comprobación calculada de los campos de datos y de cabecera.
- ✓ **Puntero de urgencia.** Indicador para el final de los datos urgentes, ya que el segmento podría contener datos no urgentes. TCP no marca el principio de los datos urgentes, es responsabilidad de la aplicación averiguarlo.
- ✓ **Opciones.** Tamaño máximo del segmento, diversas opciones como TCP.
- ✓ **Datos.** Datos del protocolo de capa superior.

Dos campos incluidos en la cabecera y que son de especial importancia son los números de puerto de origen y destino. Los puertos proporcionan una manera de distinguir las distintas transferencias, ya que un mismo host puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede ser que por medio de usuarios distintos. El puerto de origen contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado.

Los identificadores para cada extremo de la conexión se llaman sockets. El socket local se forma uniendo la dirección IP de origen y el número de puerto de origen. El socket remoto se obtiene al igual que el socket local uniendo la dirección IP destino y el número de puerto destino.

Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor debe tener asignado un número estándar para que pueda ser utilizado por el

cliente (ejemplo FTP por el puerto 21). Cuando es el servidor el que envía los datos, los números de puerto de origen se intercambian.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez que se ha recibido y comprobado la información satisfactoriamente. Estas señales se incluyen en el campo apropiado de la cabecera del datagrama (Número de acuse de recibo), que tiene un tamaño de 32 bits. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un periodo de tiempo razonable, el datagrama completo se volverá a enviar. Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del datagrama llegue con errores a su destino. Para poder detectar cuando sucede esto se incluye en la cabecera un campo de 16 bits, el cual contiene un valor calculado a partir de la información del datagrama completo (Suma de Verificación). En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera. Si el valor es distinto significaría que el datagrama es incorrecto, ya que en la cabecera o en la parte de datos del mismo hay algún error.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente. De esta manera el primero empezará por cero, el segundo contendrá un número que será igual al tamaño en bytes de la parte de datos del datagrama anterior, el tercero con la suma de los dos anteriores, y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor más a tener en cuenta durante la transmisión de información; es la potencia y velocidad con que cada uno de los ordenadores puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el ordenador de más potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla; dicho inconveniente se soluciona mediante un campo de 16 bits (Ventana) en la cabecera TCP, en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar. Si el valor llega a cero será necesario que el emisor se detenga. A medida que la información es procesada este valor aumenta indicando disponibilidad para continuar la recepción de datos.

3.4.2 UDP (User Data Protocol).

El protocolo de datagramas de usuario (UDP) puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. UDP es un protocolo mucho más simple. Puesto que UDP no admite numeración de los datagramas, este protocolo se utiliza principalmente cuando el orden en que se recibe los mismos, no es un factor único.

UDP no utiliza windowing ni acuses de recibo, por lo que la fiabilidad la proporcionan los protocolos de la capa de aplicación: UDP se diseñó para que no necesite reunir secuencias de segmentos. Cuando se utiliza el UDP la garantía de que un paquete llegue a su destino es mucho menor que con TCP debido a que no se utilizan las señales de confirmación. Por todas estas características la cabecera del UDP es mucho menor en

comparación con la del TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones.

Los protocolos que utilizan UDP son (ver fig.3.10):

- ✓ Protocolo TFTP
- ✓ Protocolo Simple de administración de redes (SNMP).
- ✓ Protocolo de configuración dinámica del host (DHCP)
- ✓ Sistema de denominación de dominio (DNS).
- ✓ Protocolo BOOTP.

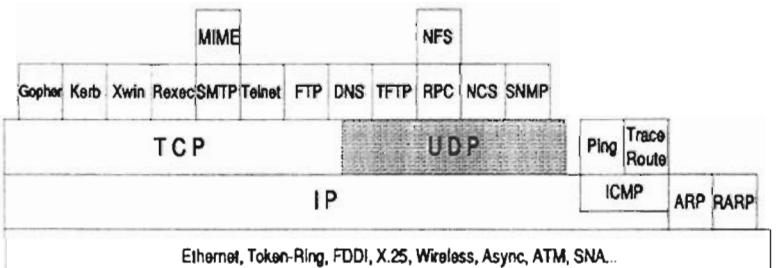


Fig. 3.10 Protocolo UDP en el Modelo de capas TCP/IP.

UDP es utilizado para transportar voz sobre IP, ya que si utilizamos TCP en el control de flujo y en la retransmisión para los paquetes de voz, serían innecesarios, por lo que la latencia implementada por los mensajes de reconocimiento y retransmisiones pueden traducirse en una calidad de voz inaceptable. En las aplicaciones como voz sobre IP, el control de la latencia es mucho más importante que asegurar la entrega de cada paquete.

3.5 Capa de aplicación.

Los protocolos de máximo nivel se denominan protocolos de aplicación. Se comunican con aplicaciones en otros hosts de Internet y constituyen la interfaz de usuario con la pila de protocolos TCP/IP.

Los números de puerto de las aplicaciones cliente, son asignados dinámicamente y generalmente son superiores al 1024. Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada host. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Todos los protocolos de alto nivel tienen algunas características en común. Pueden ser aplicaciones escritas por el usuario o aplicaciones estandarizadas y distribuidas con un producto TCP/IP. De hecho, la pila TCP/IP incluye protocolos de aplicación tales como:

- ✓ TELNET para el acceso interactivo de una terminal a un host remoto.
- ✓ FTP (File Transfer Protocol) para transferencias de alta velocidad de un disco a otro.
- ✓ SMTP (Simple Mail Transfer Protocol) como sistema de correo de Internet.
- ✓ TFTP (Trivial File Transfer Protocol) lee y escribe un fichero de o en un servidor.

- ✓ DNS (Domain Name Service) Tiene la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP.

Estas son las aplicaciones implementadas más ampliamente, pero existen muchas otras. Cada aplicación TCP/IP particular incluye un conjunto más o menos restringido de protocolos de aplicación.

Usan UDP o TCP como mecanismo de transporte. Hay que recordar que UDP no es fiable ni ofrece control de flujo, por lo que en este caso la aplicación ha de proporcionar sus propias rutinas de recuperación de errores y de control de flujo. Suele ser más fácil desarrollar aplicaciones sobre TCP, un protocolo fiable orientado a conexión. La mayoría de los protocolos de aplicación utilizan TCP, pero algunas aplicaciones se construyen sobre UDP para proporcionar un mejor rendimiento reduciendo la carga del sistema que genera el protocolo. La mayoría de ellas usa el modelo de interacción cliente/servidor.

Los números de puerto de las aplicaciones clientes son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puertos prefijados: son los llamados puertos well-known. Estos puertos están definidos en el RFC 1700.

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

CAPÍTULO CUATRO

INTERNET 2

4.1 Antecedentes.

Internet fué el resultado de varios proyectos de investigación y consecuencia final de un proceso que comenzó en el Pentágono Norteamericano por los años sesenta, con la red ARPAnet, en la que participaron investigadores civiles. Estos proyectos tuvieron un fuerte apoyo económico de empresas y entidades gubernamentales de los Estados Unidos. Así, Internet posteriormente se convirtió en una red académica orientada a la colaboración e investigación entre las distintas Universidades que conformaban dicha red. Con el tiempo esta red académica evolucionó hasta lo que hoy es Internet, el medio de comunicación informática más utilizado del planeta.

La red central de Internet (en sus comienzos ARPAnet) pasó a ser NSFnet y hasta hoy es el backbone de Internet. Sin embargo, debido a su privatización, se deterioró el servicio teniendo un impacto negativo para el cual inicialmente fue creada, a la colaboración e investigación académica, convirtiéndose en una red que involucra, en gran parte, intereses comerciales y particulares.

4.1.1 Limitantes de Internet.

Como consecuencia de la privatización, surgieron varias limitantes para la investigación y estudio de herramientas a gran escala.

Una de las principales limitantes es la confiabilidad de la red. En Internet es totalmente permitido tanto acceder como publicar cualquier clase de información, es decir, no existe restricción alguna para hacerlo. Por esto mismo se debe considerar, qué tan confiable es la información que de ella obtenemos, ya que muchas veces no es posible saber quién o qué es lo que se está transmitiendo por este medio. Debido a estas características la seguridad de la Internet no cumple con los requisitos necesarios para la investigación e intercambio de información académica.

Además los proveedores de servicios sobre Internet "sobrevenden" el ancho de banda del que disponen, haciendo imposible garantizar un servicio mínimo en horas pico de uso de la red. Esto es crítico cuando se piensa en aplicaciones que necesiten calidad de servicio garantizada, ya que los protocolos utilizados en la Internet actual no permiten esta funcionalidad.

Por otro lado, los enlaces de alta velocidad son aún demasiado costosos para poder realizar su comercialización masiva.

Todo esto, entonces, nos lleva a la conclusión que Internet no es un medio apto para dar el salto tecnológico que se necesita.

4.2 Orígenes de Internet 2.

Se emprendió un proyecto similar al de los años 60's, una red de cómputo con capacidades avanzadas separada de la Internet comercial actual; llamada "Internet 2". Su origen se basa en el espíritu de colaboración entre alrededor de 200 universidades del todo el mundo y su objetivo principal es desarrollar la próxima generación de aplicaciones telemáticas para la colaboración e investigación entre sus distintos miembros y permitir el desarrollo de aplicaciones y protocolos que luego puedan aplicarse a la Internet de todos.

Algunas de las aplicaciones en desarrollo dentro del proyecto de Internet 2 a nivel internacional son: telemedicina, bibliotecas digitales, laboratorios virtuales, manipulación a distancia y visualización de modelos 3D; aplicaciones todas ellas que no serían posibles de desarrollar con la tecnología del Internet de hoy.

De la misma forma en que la Internet de hoy surgió de las redes académicas en las décadas de 1980 y 1990, llevando al área comercial productos como el TCP/IP, el correo electrónico y la World Wide Web; Internet 2 dejará un legado de tecnologías y aplicaciones a ser adoptadas por las redes de comunicación comerciales del futuro, como el IPv6, el multicast y la calidad de servicio (QoS).

Se debe estar consciente de que este proyecto no planea reemplazar al Internet, al contrario, las nuevas aplicaciones que se desarrollen serán compartidas con otras redes como la de Internet. Internet 2 utilizará y continuará desplegando el servicio de muy alta velocidad de backbone de red (very high-speed Backbone Network Service, vBNS) creado por la Fundación Nacional para la Ciencia (National Science Foundation). Además de que se seguirán empleando servicios ya existentes como el correo electrónico, la conexión personal a la red y los grupos de noticias.

4.2.1 Ventajas.

Las redes usadas por Internet 2 son más rápidas, las aplicaciones desarrolladas utilizarán un completo conjunto de herramientas que se están desarrollando en la actualidad. En nuestros días, toda información en Internet viene dada con la misma prioridad como si ésta pasara a través de toda la red de un ordenador a otro. La "Calidad de servicio" permitirá a las aplicaciones requerir de una específica cantidad de ancho de banda o prioridad para ella. Esto permitirá a dos ordenadores hacer funcionar una aplicación y comunicarse a las altas velocidades necesarias para una interacción en tiempo real.

Es importante resaltar la diferencia en velocidad que tendrá, mucho más rápida que la WWW. Se piensa que una red de 100 a 1000 veces más veloz, permitirá a las aplicaciones cambiar el modo de trabajar e interactuar con los ordenadores. Aplicaciones como la tele-inmersión y las bibliotecas digitales cambiarán el modo que tiene la gente de usar los ordenadores para aprender, comunicarse y colaborar. Quizás las más excitantes posibilidades son aquellas que todavía no se han imaginado y serán desarrolladas junto con Internet2.

La participación en la Internet 2 está abierta para cualquier universidad que se comprometa a proveer facilidades para el desarrollo de aplicaciones avanzadas en su campus. La inversión financiera requerida para cumplir con estas obligaciones pueden ser más de lo que muchas instituciones puedan permitirse por ahora. Sin embargo, Internet 2 tiene la intención de acelerar la transmisión de nuevas posibilidades a la comunidad mayor del sistema de redes. El costo de la tecnología usada y desarrollada por Internet 2 descenderá a un nivel alcanzable para cualquier institución que actualmente tenga una conexión básica a la Internet.

	INTERNET	INTERNET2
Origen	Consecuencia final de un proceso que comenzó el Pentágono norteamericano en los años 60's con la Red Arpanet, en la que participaban investigadores civiles.	Proyecto desarrollado por una colaboración de más de 200 Universidades de Estados Unidos para crear aplicaciones avanzadas que beneficien a la educación y a la investigación.
Canales de comunicación	entre los NAPs: OC-3 (optical carrier)	entre dorsales vBNS (Very High Backbone Network Service) y Gigapops: OC-12
Velocidad	155 Mbps	hasta 622 Mbps.
Manejo de Información	La información viene dada con la misma prioridad.	Con "Calidad de Servicio", cada aplicación tendrá el específico ancho de banda que requiera. Resultados: dos ordenadores podrán hacer funcionar una aplicación a altas velocidades necesarias para una interacción en tiempo real.
Red y Servicios	No fueron diseñados de tal forma que no impidieran el desarrollo de nuevas aplicaciones.	Deberán ser capaces de responder a las exigencias de nuevas aplicaciones bajo ciertas formas más específicas o a través de arreglos especiales.
Utilización de Protocolos	Protocolo IPv4 (Internet Protocol versión 4)	Nueva versión IPv6.

Tabla 4.1 Cuadro comparativo entre Internet e Internet 2.

4.3 Internet 2 en México.

En México a partir de la iniciativa de 7 de las universidades más grandes de México (ITESM, IPN, UAM, UANL, UAT, UAG, UNAM), interesadas en trabajar en proyectos de investigación conjunta (tanto a nivel nacional como internacional), surge la necesidad de integrar y dar coherencia a los esfuerzos que venían realizando cada una de ellas, a través de un organismo que tuviera personalidad jurídica semejante a la de organismos internacionales dedicados a coordinar los trabajos de Internet 2 a nivel internacional.

Siguiendo el desarrollo mundial de redes de datos de mayor capacidad y velocidad, para utilizarlas en aplicaciones de alta tecnología, se toma la iniciativa de desarrollar una red de alta velocidad y unirse a la red internacional denominada Internet 2, con el fin de dotar a la Comunidad Científica y Universitaria de México de una red de telecomunicaciones que le permita crear una nueva generación de investigadores, dotándolos de mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología a nivel mundial.

De esta forma, el 12 de mayo de 1999 quedó constituida la Corporación Universitaria para el Desarrollo de Internet A.C. (CUDI).

El 20 de mayo de 1999, en la ciudad de San Diego, California, representantes de CUDI firman dos importantes memorándums de entendimiento con dos de las más importantes corporaciones universitarias que promueven y coordinan la disponibilidad de redes avanzadas para aplicaciones de investigación y educación en la Unión Americana, las cuales colaborarán conjuntamente con CUDI en el desarrollo de tecnologías y aplicaciones de la nueva generación de Internet. En esa misma fecha, se firmó un convenio con Telmex participando como Asociado Institucional.

El 6 de Octubre de 1999, en la ciudad de Ottawa Canadá, se firmó un memorándum de entendimiento entre CUDI y CANARIE, esta organización canadiense es la encargada del desarrollo de la red Internet avanzada en aquel país y con dicho acuerdo se podrán establecer programas de investigación, educación y colaboración entre ambos países.

El 10 de octubre de 2001, el Director General de CUDI y el Director de la Red Universitaria Nacional de Chile (REUNA), firmaron un Convenio de Colaboración entre ambas Instituciones, iniciando con esto la participación formal entre México y Chile en el Desarrollo de Aplicaciones en Internet 2.

En septiembre del 2000, se estableció la primera conexión entre las redes de Internet2 de México y Estados Unidos usando IPv4, que opera también en el Internet tradicional. Desde entonces se han establecido y realizado varios proyectos de educación e investigación entre las distintas instituciones participantes de CUDI.

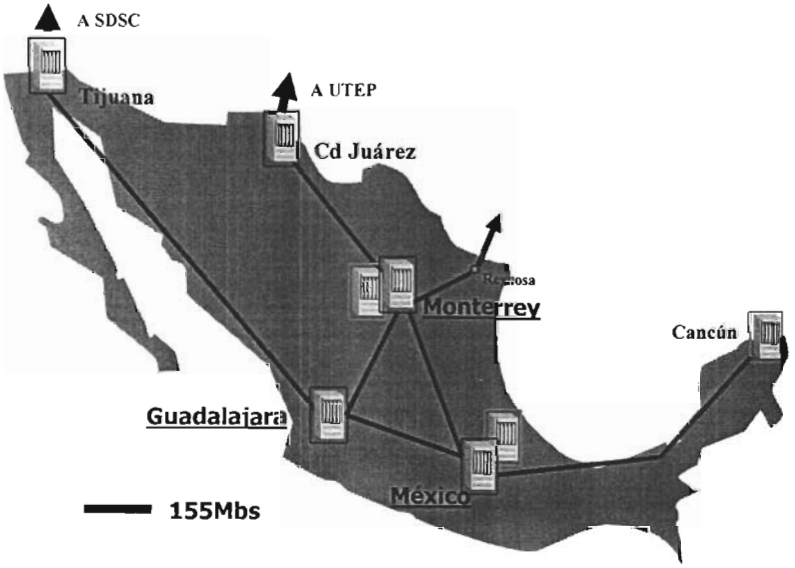


Fig. 4.1 Backbone de la red CUDI.

La Corporación Universitaria para el Desarrollo de Internet es una Asociación Civil que tiene por objeto promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México.

CUDI es el organismo que representa jurídicamente los intereses de las Universidades e Instituciones que conforman el proyecto de Internet 2 en México. Su labor consiste en coordinar las labores encaminadas al desarrollo de la red de cómputo avanzado en el país, brindar asesoría en cuanto a las aplicaciones que utilizarán esta red y fomentar la colaboración entre sus miembros.

El proyecto de Internet 2 en México propone apoyar al sistema de educación superior utilizando telecomunicaciones para:

- Incrementar la capacidad y calidad de los procesos educativos.
- Apoyar la investigación mediante herramientas compartidas y colaboraciones inter-institucionales.

- Permitir el desarrollo de aplicaciones para impulsar la nueva generación de Internet.

La Red CUDI esta patrocinada por Telmex y Avantel que proveen los enlaces en las distintas sedes para así lograr una robustez en el Backbone; como se observa en la fig. 4.1 y la fig. 4.2. Con enlaces de 155Mb/s de 8,000 km, cabe decir que la red es sólo para aplicaciones de educación e investigación.

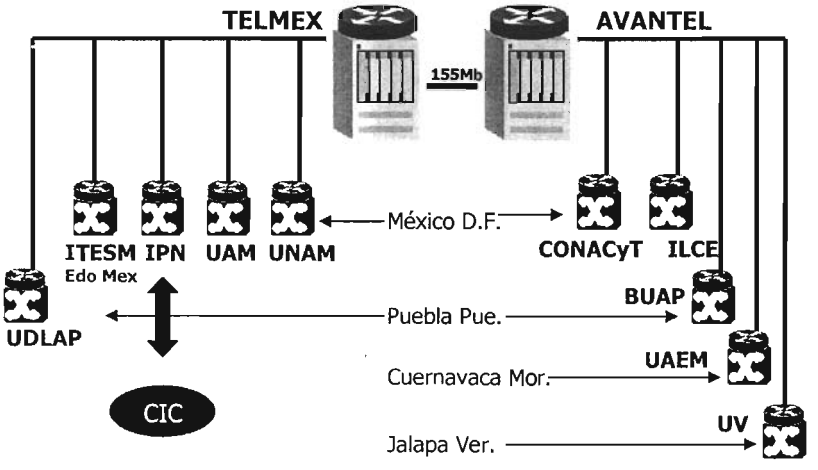


Fig. 4.2 Nodos de Acceso Principales.

4.3.1 Administración.

Actualmente CUDI esta conformada por cuatro categorías con un total de 51 miembros: 17 asociados académicos, 5 asociados institucionales, 31 afiliados académicos y 3 afiliados empresariales.

- **Asociados académicos** (17): Universidades que adquieren el compromiso financiero de absorber en proporción el costo de mantener la red operando. Forman parte del Consejo Directivo.

  - BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
  - CENTRO DE INVESTIGACIÓN CIENTÍFICA Y EDUCACIÓN SUPERIOR DE ENSENADA
  - CENTROS PÚBLICOS DE INVESTIGACIÓN CONACYT
  - INSTITUTO LATINOAMERICANO DE LA COMUNICACIÓN EDUCATIVA
  - INSTITUTO POLITÉCNICO NACIONAL
  - INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
  - UNIVERSIDAD AUTÓNOMA DE CIUDAD JUÁREZ
  - UNIVERSIDAD AUTÓNOMA DE LA LAGUNA
  - UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
  - UNIVERSIDAD AUTÓNOMA DE TAMAULIPAS
  - UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
  - UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS
  - UNIVERSIDAD AUTÓNOMA METROPOLITANA
  - UNIVERSIDAD DE GUADALAJARA
  - UNIVERSIDAD DE LAS AMÉRICAS – PUEBLA
  - UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
  - UNIVERSIDAD VERACRUZANA

- **Asociados institucionales** (5): Instituciones no universitarias que realizan una aportación mayor a la asociación. Forman parte del Consejo Directivo.
  - AVANTEL
  - CISCO
  - CONACYT
  - ENTERASYS
  - TELÉFONOS DE MÉXICO

- **Afiliados académicos** (31): Universidades que únicamente desean conectarse a la red.

  - CENTRO NACIONAL DE LAS ARTES
  - CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL IPN
  - COLEGIO DE POSTGRADUADOS
  - COLEGIO NACIONAL
  - INSTITUTO DE INVESTIGACIONES ELÉCTRICAS
  - INSTITUTO MEXICANO DEL PETRÓLEO
  - INSTITUTO NACIONAL DE SALUD PÚBLICA
  - INSTITUTO TECNOLÓGICO AUTÓNOMO DE MÉXICO
  - LABORATORIO NACIONAL DE INFORMÁTICA AVANZADA
  - TEXAS A&M MÉXICO, TAMU-MEX
  - UNIVERSIDAD ANÁHUAC DEL SUR
  - UNIVERSIDAD AUTÓNOMA AGUASCALIENTES
  - UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
  - UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA
  - UNIVERSIDAD AUTÓNOMA DE COAHUILA
  - UNIVERSIDAD AUTÓNOMA DE SAN LUIS POTOSÍ
  - UNIVERSIDAD AUTÓNOMA DE SINALOA
  - UNIVERSIDAD AUTÓNOMA DE TLAXCALA
  - UNIVERSIDAD AUTÓNOMA DE TABASCO
  - UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
  - UNIVERSIDAD POPULAR DEL ESTADO DE PUEBLA
  - UNIVERSIDAD DE COLIMA
  - UNIVERSIDAD DE SONORA
  - UNIVERSIDAD DEL VALLE DE MÉXICO
  - UNIVERSIDAD IBEROAMERICANA
  - UNIVERSIDAD LA SALLE
  - UNIVERSIDAD PANAMERICANA
  - UNIVERSIDAD PEDAGÓGICA NACIONAL
  - UNIVERSIDAD TECNOLÓGICA DE JALISCO
  - UNIVERSIDAD TECNOLÓGICA DE MÉXICO
  - UNIVERSIDAD TECNOLÓGICA DE PUEBLA

- **Afiliados institucionales** (3): Instituciones no universitarias que realizan una aportación menor a la asociación

  - SITARA NETWORKS
  - VCON
  - MARCONI

La conexión de los asociados y afiliados se puede observar en la fig. 4.2., la cual describe el modo de conexión de los afiliados y asociados de forma jerárquica al Backbone de la Red CUDI.

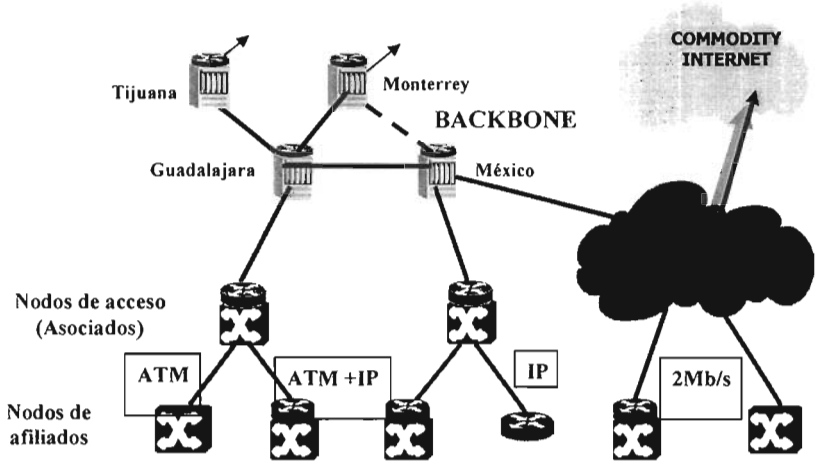


Fig. 4.2 Acceso de Afiliados y Asociados.

4.3.2 Organizaciones relacionadas con Internet 2.

El objetivo de transferir la tecnología de Internet 2 a las redes generales está conseguido, y para utilizar la enorme experiencia que existe fuera de la universidad, Internet 2 está trabajando con el gobierno federal, agencias, empresas privadas y organizaciones sin animo de lucro que tienen experiencia en como desarrollar redes telemáticas. Estas organizaciones proporcionan a los miembros de Internet 2 recursos y experiencia en adición a lo que tienen en sus propios campus. Por otra parte, proporcionan un canal al proyecto para el tipo de consideraciones que tendrán que ser tomadas en cuenta y así la tecnología de Internet 2 pueda migrar a otras redes más generales y comerciales.

En Latinoamérica existen organismos semejantes a CUDI como son:

- ✓ UCAID (University Corporation for Advanced Internet Development) de EUA. http://www.internet2.edu (ver fig. 4.3 y 4.4).
- ✓ CENIC (Corporation for Education Network Initiatives in California) de EUA. http://www.cenic.edu (ver fig. 4.5).
- ✓ CANARIE (Canadian Network for Advanced Research Industrie and Education) de Canadá. http://www.canarie.edu.ca .
- ✓ REUNA (Red Universitaria Nacional) de Chile. http://www.reuna.cl (ver fig. 4.7).
- ✓ RETINA (Red Teleinformática Académica) de Argentina. http://www.retina.ar (ver fig. 4.8).
- ✓ RNP (Rede Nationale de Ensino e Pesquisa) de Brasil. http://www.rnp.br(ver fig. 4.9).

En las figuras siguientes observamos los diferentes backbones que dan vida a la Red Internet 2 a nivel Internacional.

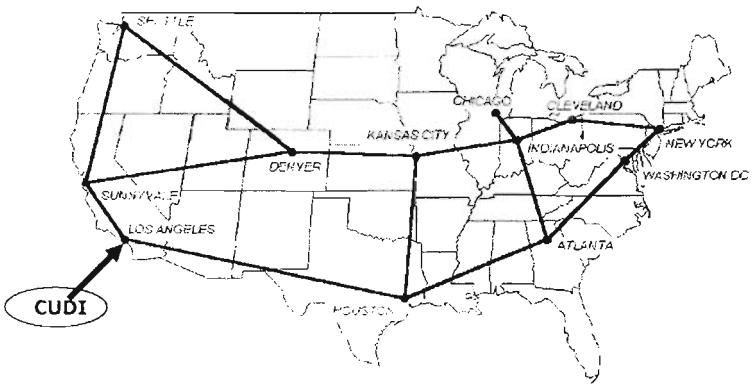


Fig. 4.3 Backbone ABELINE.

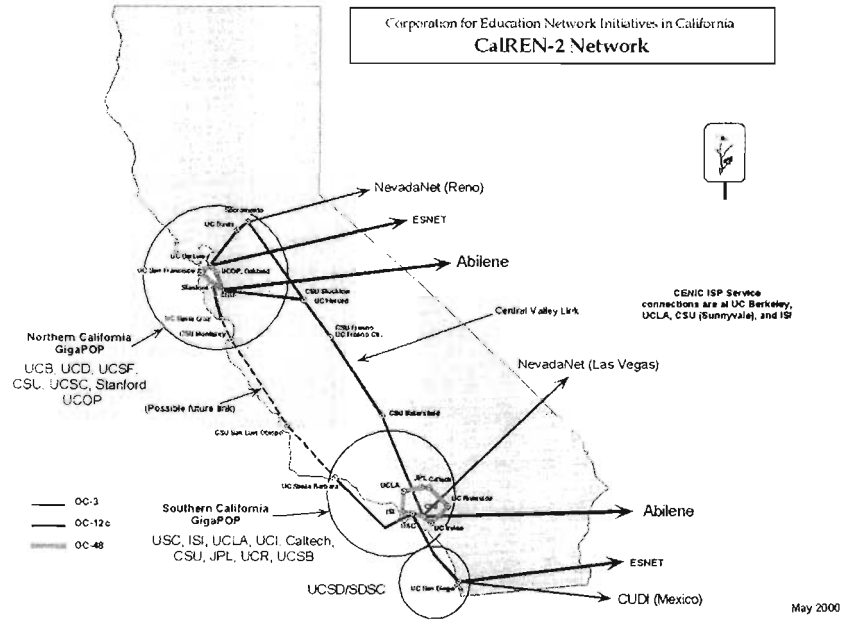


Fig. 4.5 CENIC (Corporation for Education Network Initiatives In California).

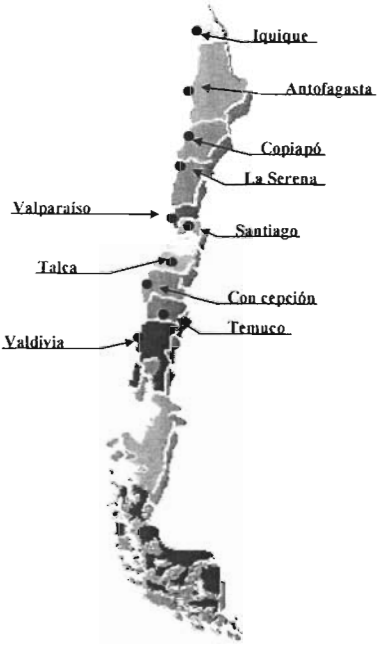


Fig. 4.7 REUNA (Red Universitaria Nacional de Chile).

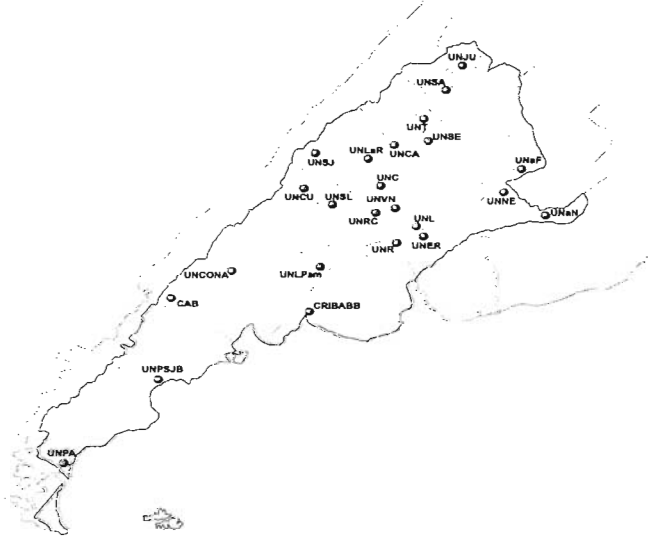


Fig. 4.8 RETINA (Red Teleinformática Académica de Argentina).

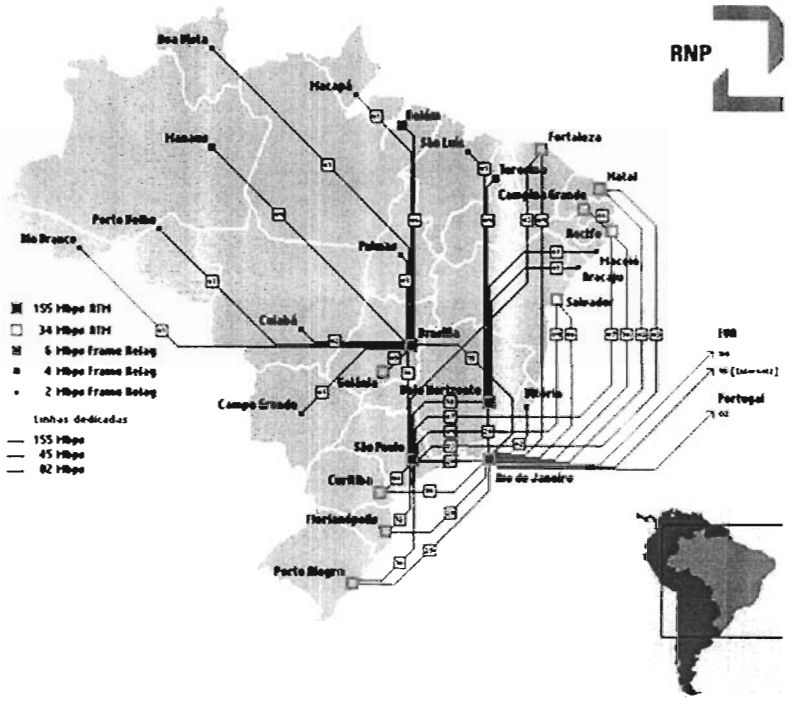


Fig. 4.9 Red RNP de Brasil.

La red mundial está integrada por 42 National Research and Education Networks (NREN´s) con acceso a más de 3,500 universidades (ver tabla 4.2).

Americas	Europe and the Middle East
CANARIE (Canada)	ARNES (Slovenia)
CEDIA (Ecuador)	BELNET (Belgium)
CNTI (Venezuela)	CARNET (Croatia)
CR2Net (Costa Rica)	CESnet (Czech Republic)
Abilene (EUA)	DANTE (Europe)
REUNA (Chile)	DFN-Verein (Germany)
RETINA (Argentina)	GIP-RENATER (France)
RNP [FAPESP / ANSP] (Brazil)	GRNET (Greece)
SENACYT (Panama)	HEAnet (Ireland)
	HUNGARNET (Hungary)
Asia-Pacific	GARR (Italy)
AAIREP (Australia)	Israel-IUCC (Israel)
APAN (Asia-Pacific)	NORDUnet (Nordic Countries)
APAN-KR (Korea)	POL-34 (Poland)
APRU (Asia-Pacific)	RCTS (Portugal)
CERNET, CSTNET, NSFCNET (China)	RedIris (Spain)
JAIRC (Japan)	RESTENA (Luxemburg)
JUCC (Hong Kong)	RIPN (Russia)
SingAREN (Singapore)	SANET (Slovakia)
NECTEC / UNINET (Thailand)	Stichting SURF (Netherlands)
Tanet2 (Taiwán)	SWITCH (Switzerland)
	TERENA (Europe)
	JISC, UKERNA (United Kingdom)

Tabla 4.2 Integrantes de la Red Internet 2

4.4 El backbone de Internet 2.

La red de Internet 2 está compuesta por redes principales o backbones en USA, a los cuales se conectan los llamados gigaPoPs y backbones internacionales a los que a su vez se conectan gigaPoPs o nodos en particular tales como Universidades. Un gigaPoP es una red regional (con ancho de banda del orden de los gigabits por segundo) conectada a Internet 2. Por ejemplo en USA el MIT, la Universidad de Boston y la Universidad de Harvard conforman el gigaPoP llamado BOS.

A continuación en la fig. 4.10 se muestra de manera general un esquema de Internet 2 :

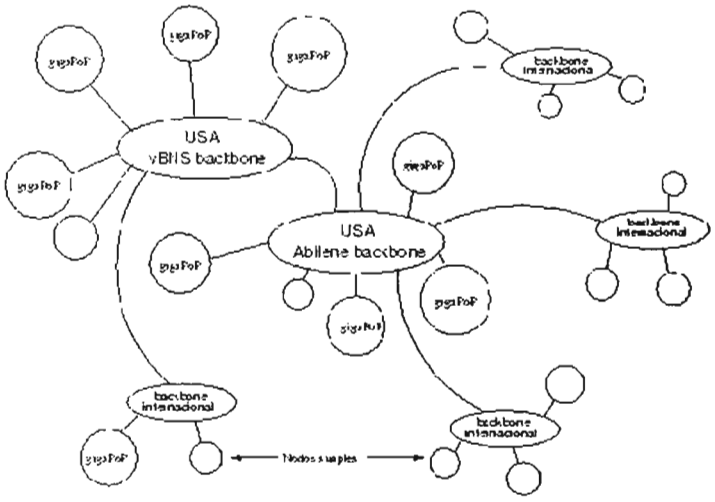


Fig. 4.10 Esquema de la red Internet 2.

En la Fig. 4.10 se puede visualizar que actualmente existen dos grandes backbones en USA (aunque hoy en día el backbone Abilene es mucho mayor en ancho de banda, 2.4 Gbps), de los cuales se distribuyen enlaces hacia backbones en otros países. Uno de estos backbones internacionales es REUNA (Red Universitaria Nacional).

Para la conexión a Internet 2 no es necesario un nuevo equipamiento, ni nuevas conexiones, por el lado de los usuarios de las respectivas Universidades conectadas a Internet 2. Los backbones son los responsables de encaminar el flujo de datos por Internet 2 o Internet comercial según corresponda.

El backbone de Internet 2 (la red Abilene y la red vBNS) tiene velocidades que superan los 2 Gbps, y las conexiones de las universidades a este backbone varían entre 45 Mbps y 622 Mbps.

4.5 Aplicaciones y servicios de Internet 2.

Los objetivos mencionados anteriormente son llevados a cabo mediante actividades de desarrollo y prueba de nuevos protocolos y aplicaciones para Internet 2. Estos desarrollos son hechos en comités llamados Grupos de Trabajo (Working Groups, WG). Cada WG pertenece a alguna área técnica de desarrollo de Internet 2: Ingeniería, Middleware (interfaces software que proveen funcionalidades rutinarias en una conexión típica Internet. Entre estas, como ejemplo se pueden mencionar la autenticación de usuarios) y Aplicaciones. Cada una de estas áreas posee un Director que es el responsable de las actividades de su área respectiva. Los miembros de estos grupos de trabajo pueden ser tanto miembros de Internet 2 como empresas de apoyo externo (las empresas de apoyo económico por ejemplo).

Los actuales grupos de trabajo por área son:

- **Ingeniería:** IPv6, Measurement, Multicast, Network Management, Routing, Security, Topology.
- **Middleware:** MACE-Architecture, MACE-DIR (Directories), HEPKI-TAG (PKI Technical), HEPKI-PAG (PKI Policy).
- **Applications:** Arts and Humanities Initiative, Digital Imaging, Digital Video Initiative, Network Storage, Health Science Initiative, Research Channel, Video Conferencing (subcomité de Digital Video Initiative), Voice over IP.

Las dos primeras áreas tienen labores que son transparentes al usuario y que sólo sirven para ofrecer un mejor servicio a las aplicaciones de la tercera área, Applications. A partir de los nombres de los grupos de trabajo del área Applications uno puede deducir a grandes rasgos de qué se trata. En el grupo de trabajo de Network Storage, por ejemplo, se desarrolla la Infraestructura de Almacenamiento Distribuido en Internet 2 (o, en inglés, Internet 2 Distributed Storage Infrastructure), abreviado I2-DSI. El objetivo de esto es el almacenar datos replicados a través de la red y cuando un cliente intente acceder a los datos entonces el sistema le provea los datos que se encuentran en el servidor más cercano (en la red) a él, manteniendo así el tráfico lo más local posible.

Algunas de las aplicaciones avanzadas son:

- Tecnología de Redes de Telecomunicaciones.
- Educación a Distancia.
- Bibliotecas Digitales.
- Telemedicina y Salud.
- Ciencias de la Vida.
- Ciencias de la tierra.
- Astronomía.
- Visualización.
- Arte.
- Súper cómputo compartido.
- Laboratorios Remotos.

CAPÍTULO CINCO

VOZ SOBRE IP (VoIP)

5.1 Antecedentes VoIP.

Desde hace poco tiempo, se ha visto la posibilidad de utilizar la infraestructura de transporte de datos bajo el protocolo de comunicación TCP/IP para el transporte de tráfico de voz. Gracias a que se han desarrollado nuevos estándares y se ha mejorado notablemente las tecnologías de compresión de voz, mecanismos de control y prioridad de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un ambiente mucho más factible para llevar a cabo esta posibilidad. Este concepto es muy simple, básicamente es la transformación de la voz en paquetes de información que son transportados a través de una red de datos IP.

Con la aparición del manejo de voz sobre el protocolo de Internet (VoIP) junto con la fabricación de mejores **DSP** (Digital Signal Processor) los cuales son claves en la compresión y descompresión de la voz, hicieron posible la idea de realizar telefonía en una red de datos, además de otros factores, como la aparición de nuevas aplicaciones y la puesta definitiva de VoIP por fabricantes como Cisco System, Nortel Networks, entre otros.

A finales de 1997 el forum de VoIP del IMTC (International Multimedia Telecommunications Consortium) llegó a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP.

Debido a la existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP se debe considerarse como una clarificación del H.323, ya que H.323 recopila los protocolos necesarios de voz para lograr el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la interconexión con la infraestructura telefónica tradicional (PSTN). Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

5.2 Evolución.

Hoy las redes de datos no solamente integran en su funcionamiento la transmisión de datos exclusivamente, actualmente están convergiendo a la transmisión de voz y video, lo cual le da crecimiento y desarrollo a las tecnologías de voz sobre redes de datos, esto gracias al desarrollo e implantación de una infraestructura de conmutación (switching), siendo efectivo para las aplicaciones de software que se aplican dentro del IP, con lo cual no necesitan ser conocidas, dado que el IP transporta datos de extremo a extremo. Se debe de proporcionar una priorización adecuada en una red IP congestionada, que haga del conocimiento del tipo de aplicación que está ejecutándose, sea el caso de VoIP.

5.3 Funcionamiento.

En las redes IP es normal y habitual que se pierdan paquetes; de hecho, TCP/IP se construyó para utilizar la pérdida de paquetes como un medio para controlar el flujo de paquetes. En TCP/IP, si se pierde un paquete, éste es retransmitido. En la mayoría de las aplicaciones en tiempo real, la retransmisión de un paquete es peor que no recibir un paquete debido a la naturaleza de sensibilidad de tiempo de la información.

Por lo cual actualmente, todos los protocolos de señalización de voz sobre IP utilizan RTP/UDP/IP como mecanismo de transporte para el tráfico de voz. El protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol) se utiliza en conjunto con la cabecera del Protocolo de Datagrama de Usuario (UDP, User Datagram Protocol)/IP para proporcionar la marca de temporización. El RTP discurre por encima del UDP e IP y se anota normalmente como RTP/UDP/IP. El RTP es actualmente la piedra angular para transportar el tráfico en tiempo real para las redes IP.

El RTP tiene un campo que señala la hora exacta a la que se envió el paquete (en relación con la totalidad del flujo RTP). Esta información se conoce como **marca de temporización** (timestamp) de RTP y la utiliza el dispositivo finalizador/receptor del flujo de audio. El dispositivo receptor utiliza la marca de temporización RTP para determinar la hora a la que se espera un paquete, si el paquete era correcto, y si se recibió cuando se esperaba. Toda esta información ayuda a la estación receptora a determinar cómo adaptar sus propios parámetros para enmascarar cualquier problema de red potencial como, por ejemplo, el retraso, la fluctuación de fase y la pérdida de paquetes.

Es importante notar que las redes IP construidas adecuadamente son self-healing. Esto significa que utiliza protocolos de enrutamiento dinámico y que existen múltiples destinos posibles, es decir que funciona a la mejor ruta en un momento dado para transmitir los datos; lo que significa que es posible que la voz (que ha sido empaquetada en IP) tome múltiples rutas para el mismo destino. Cada paquete individual toma la mejor ruta entre el remitente y el destinatario.

Como es visto, en la red PSTN se lleva acabo un control de llamadas por medio de estándares; de manera similar en VoIP existen estándares que manejan y separan los flujos de RTP de los servicios, por lo que se desarrollan protocolos de control de llamada VoIP (H.323, MGCP, Media Gateway Control Protocol y SIP, Session Initiation Protocol). Todos ellos resuelven un problema similar: traducir una numeración telefónica en una dirección IP; sin embargo todos ellos pueden ser utilizados para propósitos diferentes.

El modo de funcionamiento que actualmente está implementado, variará un poco o nada, pero lo que si es posible observar, es que los protocolos de control de llamada de VoIP, aún tienen alguna limitación, pero el desarrollo alcanzado hasta el momento permite ofrecer servicios que antes no se hubieran imaginado.

5.4 Protocolos de voz.

Existen varios protocolos de llamadas de VoIP, los principales son H.323, el Protocolo de Control de Gateway Simple (SGCP, Simple Gateway Control Protocol), el Protocolo de Control de Dispositivo del Protocolo Internet (IPDC, Internet Protocol Device Control), el Protocolo MGCP y el SIP. Se definen de la siguiente manera:

- El H323 es la recomendación de la ITU-T que está más instalado, el cual se describirá mucho más a detalle en este capítulo.
- El SGCP fue desarrollado a principios de 1998 para reducir el costo de los puntos finales (gateways) al hacer que el control de llamadas inteligente tuviera lugar en una plataforma centralizada (o controlador de gateway).
- El IPDC es muy similar al SGCP, pero tiene otros muchos mecanismos para las operaciones, la administración, la gestión y las disposiciones que el SGCP.
- A finales de 1998, la IEFT detuvo el IPDC y el SGCP y lanzó el MGCP.
- El SIP se está desarrollando como un protocolo basado en los medios que permitirá que los dispositivos finales (el punto final o gateway) sean más

inteligentes, y admitirá servicios mejorados en la capa de control de llamadas.

5.4.1 Protocolo H.323 .

H.323 es una especificación de la ITU-T para transmitir audio, video y datos a través de una red IP, incluida la propia Internet. Cuando son compatibles con H.323, los productos y aplicaciones de los fabricantes pueden comunicarse e interoperar unos con otros. El estándar H.323 dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y multipunto.

El estándar H.323 consta de los siguientes componentes y protocolos (fig. 5.1):

Función	**Protocolo**
Señalización de llamadas	H.225
Control de medios	H.245
Códecs de audio	G.711, G.722, G.723, G.728, G.729
Códecs de video	H.261, H263
Compartir datos	T.120
Transporte de Medios	RTP/RTCP

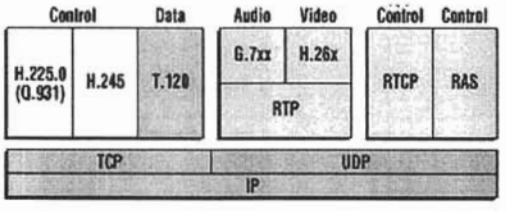


Fig. 5.1 Familia de protocolos H.323 .

5.4.1.1 Elementos H.323 .

Los elementos de un sistema H.323 incluyen terminales, gateways, gatekeepers y unidades de control multipunto (MCU, Multipoint Control Units), como se muestra en la fig. 5.2.

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

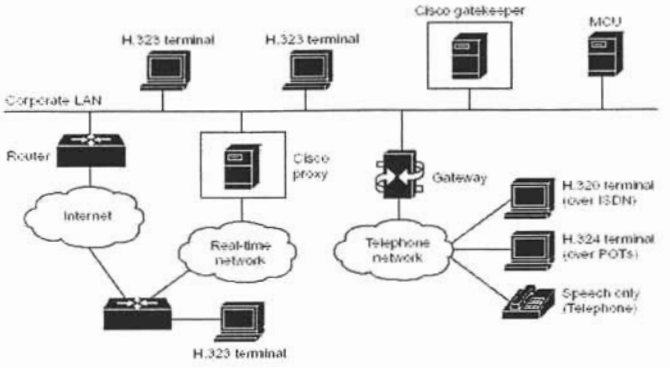


Fig. 5.2 Elementos de una red H.323 .

Terminal.

El elemento de red de H.323 definido como **terminal**, debe de tener una unidad de control de sistema, una transmisión de medios, códec de audio e interfaz de red basada en paquetes. Los requisitos opcionales incluyen un códec de video y aplicaciones de datos de usuario, como se ilustra en la fig. 5.3.

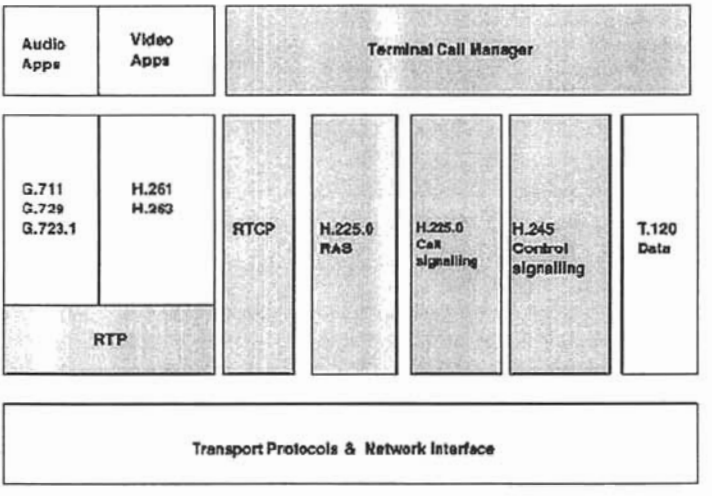


Fig. 5.3 Pila de protocolos de una terminal H.323 .

Las terminales H.323 tienen las siguientes funciones y posibilidades:

- Unidad de control de sistema. Proporciona a H.225 y H.245 el control de llamadas, intercambio de capacidad, mensajería y señalización de comandos para una actividad de la terminal.
- Transmisión de medios. Formatea el audio, video, datos, flujos de control y mensajes transmitidos en la interfaz de red. La transmisión de medios recibe también el audio, video, datos, flujos de control y mensajes desde la interfaz de red.

- Códec de audio. Codifica la señal desde el equipo de audio para su transmisión y descodifica el código de audio entrante. Las funciones que se requieren incluyendo la codificación y descodificación de voz G.711 para recibir y transmitir formatos de ley a y ley μ de manera opcional, se pueden soportar en la codificación y descodificación de G.722, G.723.1, G.278 y G.729.
- Interfaz de red. Una interfaz basada en paquetes que pueden hacer servicios de unidifusión y multidifusión de extremo a extremo de Protocolo para el Control de Transmisión (TCP) y el Protocolo de Datagrama de Usuario (UDP).
- Códec de video. Es opcional, pero si está proporcionado, debe ser capaz de codificar y descodificar video de acuerdo con el Querter Comment Intermediate Format (QCIF).
- Canal de datos. Soporta aplicaciones como el acceso de base de datos, transferencia de archivos y conferencia audiográficas (la posibilidad de modificar una imagen común sobre múltiples computadoras de usuarios de forma simultánea), como se especifica en la recomendación T.120.

Gateway.

El **gateway** H.323 refleja las características de un punto final de una red de circuito conmutado (SCN) y un punto final H.323. Traduce entre formatos de audio, video y transmisión de datos, así como en un sistema de comunicación y protocolos. Esto incluye la configuración y el borrado de la llamada en la red IP y en la red circuito conmutado (telefonía tradicional).

Los **gateways** no son necesarios a menos que se requiera una interconexión con la SCN. Por lo tanto, los puntos finales H.323 pueden comunicar directamente sobre la red de paquetes sin conectar con un gateway. El gateway actúa como un terminal H.323 o MCU en la red y una terminal SCN o MCU en la SCN, como se puede observar en la fig. 5.4 .

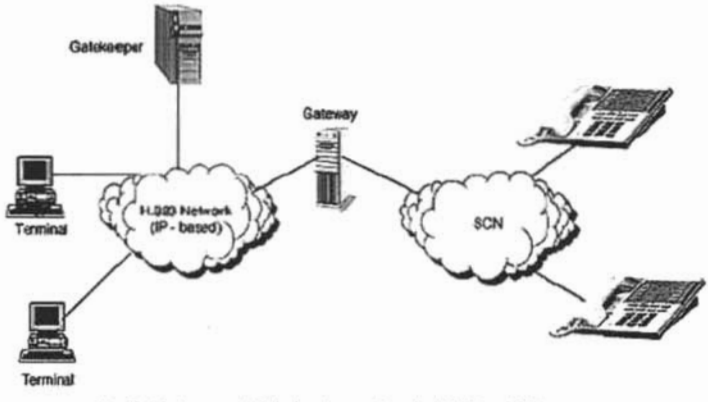


Fig. 5.4 Interoperabilidad entre protocolo H.323 y SCN.

Gatekeeper.

El **Gatekeeper** es una función opcional que proporciona servicios de control de prellamada y nivel de llamada a los puntos finales H.323. Los **gatekeepers** están lógicamente separados de los demás elementos de la red en los entornos H.323. El

gatekeeper presente en el sistema de H.323, cumple con las siguientes funciones (ver fig. 5.5):

- Conversión de direcciones. Proporciona direcciones IP de punto final desde los alias H.323 o direcciones E.164 (números de teléfono normales).
- Control de admisiones. Proporciona acceso autorizado a H323 utilizando los mensajes Admisión Request/Admision Confirm/Admision Reject (ARQ/ACF/ARJ).
- Control de ancho de banda. Consiste en la administración de los requisitos de ancho de banda utilizando los mensajes Bandwith Request/Bandwith Conform/Bandwith Reject (BRQ/BCF/BRJ).
- Administración de zona. Para los terminales, gateway y MCU registrados.
- Señalización de control de llamadas. Utiliza el modelo Señalización de llamadas de gatekeeper enrutado (GKRCS, Gatekeeper Routed Call Signaling).
- Autorización de llamada. Permite que el gatekeeper restrinja el acceso a determinados terminales y gateways o restrinja el acceso sobre la base de normas de la hora del día.
- Administración de ancho de banda. Permite que el gatekeeper rechace la admisión si el ancho de banda requerido no está disponible.
- Administración de llamada. Los servicios incluyen el mantenimiento de una lista de llamadas activas que se pueden utilizar para indicar que un punto final está ocupado.

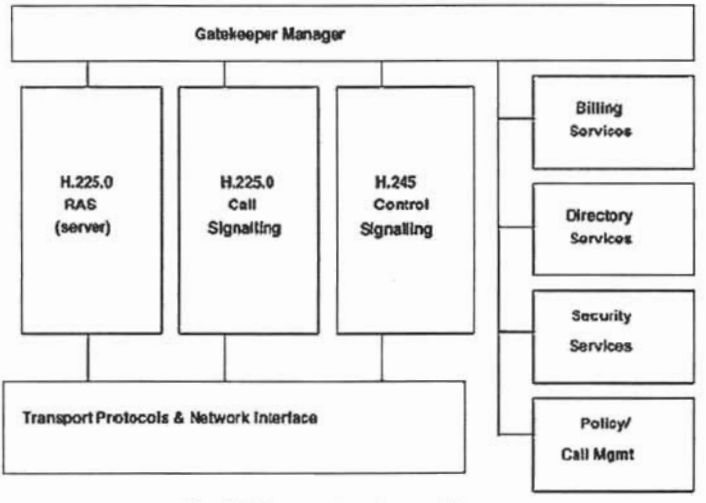


Fig. 5.5 Componentes de un gatekeeper.

MCU.

El MCU provee soporte para conferencias de tres o más terminales H.323, todas las terminales participantes en la conferencia establecen una conexión con el MCU. El MCU controla los recursos de la conferencia, negociando entre las terminales para determinar códec de audio ó video a usar, y los distribuye hacia los puntos finales que participan en la conferencia. El MCU, gatekeeper y gateway están lógicamente separados de los componentes estándar de H.323, pero pueden estar implementados como único dispositivo lógico.

Zona H.323

Una zona H.323 es una colección de todas las terminales, gateways y MCU manejados por un único gatekeeper (ver fig. 5.6). Una zona incluye como mínimo una terminal y puede incluir gateways o MCUs. Una zona contiene únicamente un gatekeeper. La zona H.323 puede estar de manera independiente en una topología de red, y estar comprendida por múltiples segmentos de red que están conectados por medio de un router u otros dispositivos.

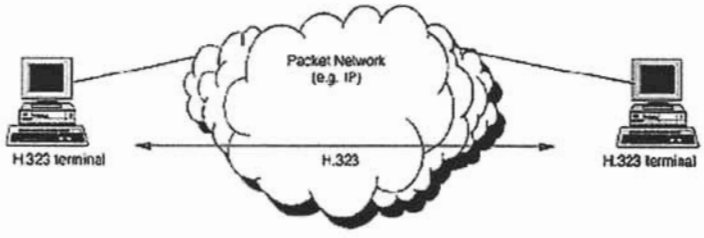


Fig. 5.6 Una zona H.323 .

5.4.1.2 Conjunto de Protocolos H.323 .

El conjunto de protocolos H.323 está basado en varios protocolos, como se muestra en la fig. 5.7 . La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos de medios y los mensajes en los sistemas H.323. Estos protocolos son soportados por mecanismos de entrega de paquetes seguros y poco seguros sobre las redes de datos.

A pesar de que la mayoría de las implementaciones H.323 utilizan actualmente el protocolo TCP como mecanismo de transporte para la señalización, la versión 2 de H.323 admite un transporte UDP básico. Así mismo, otras corporaciones estándar están investigando la utilización de mecanismos UDP más seguros para crear métodos de señalización más escalables.

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

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

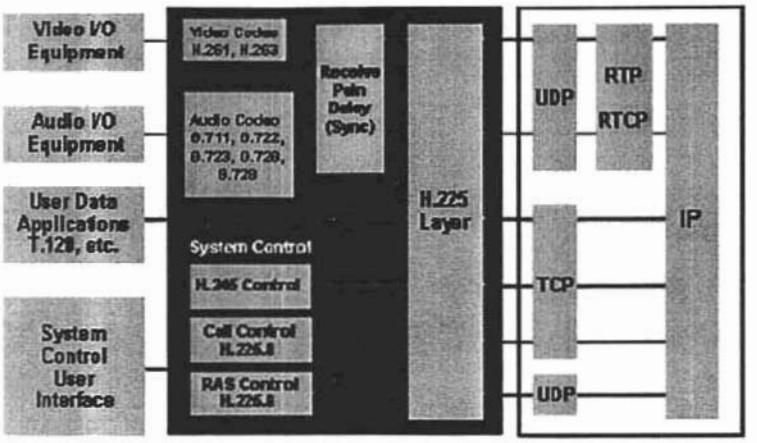


Fig. 5.7 Funciones de los protocolos H.323 .

5.4.1.2.1 Sistemas de control y señalización (H.245, H.225, RAS).

A continuación se explica el tipo de señalización RAS (Register Access and Status) y 0el uso de los protocolo de señalización y control de llamadas H.245 y H.225.

RAS.

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

Descubrimiento de Gatekeeper.

El descubrimiento de gatekeeper es un proceso manual o automático que los puntos finales utilizan para identificar con que gatekeeper registrarse. En el método manual (unicast), los puntos finales están configurados con la dirección IP del Gatekeeper y, por tanto, puede intentar el registro inmediatamente, pero únicamente con el gatekeeper predefinido. El método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento (auto discovery).

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

La dirección de difusión del descubrimiento de gatekeeper es 224.0.1.41, el puerto de descubrimiento UDP del gatekeeper es 1718, y el puerto de estado y registro UDP del

gatekeeper es 1719. Se utiliza estos tres mensajes RAS para autodescubrimiento del gatekeeper H.323:

- Gatekeeper Request (GRQ). Mensaje de multidifusión enviado por un punto final que está buscando al gatekeeper.
- Gatekeeper Confirm (GCF). Respuesta a un GRQ de punto final que indica la dirección de transporte del canal RAS del gatekeeper.
- Gatekeeper Reject (GRJ). Avisa al punto final de que el gatekeeper no quiere aceptar su registro. Normalmente se debe a una configuración en el gateway o gatekeeper.

En la fig. 5.8 se puede observar de manera clara el proceso de mensajes y secuencias para el autodescubrimiento.

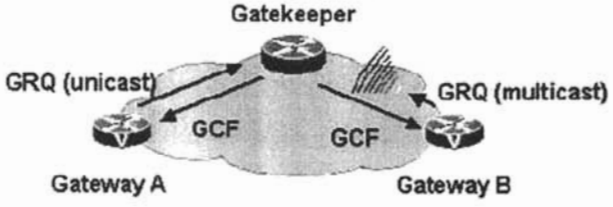


Fig. 5.8 Autodescubrimiento del gatekeeper.

Para propósitos de redundancia, el gatekeeper puede identificar gatekeepers alternativos en los mensajes GCF. Se pueden utilizar gatekeepers alternativos cuando falla el gatekeeper principal.

Registro.

El registro es el proceso que permite que los gateways, puntos finales y MCU alcancen una zona e informen al gatekeeper de sus direcciones IP y alias. El registro que es un proceso necesario, ocurre después del proceso de descubrimiento, pero antes de que se intente realizar alguna llamada. Se puede utilizar los seis mensajes siguientes para permitir que un punto final registre y cancele registros (ver fig. 5.9):

- Registration Request (RRQ). Enviado desde un punto final a la dirección del canal RAS del gatekeeper.
- Registration Confirm (RCF). Enviado por el gatekeeper, confirma un registro de punto final.
- Registration Reject (RRJ). Enviado por el gatekeeper, rechaza un registro de punto final.
- Unregister Request (URQ). Enviado desde un punto final o gatekeeper para cancelar un registro.
- Unregister Confirm (UCF). Enviado desde el punto final o gatekeeper para confirmar la cancelación de un registro.
- Unregister Reject (URJ). Indica que el punto final no estaba prerregistrado con el gatekeeper.

En la fig. 5.9 se ilustran los procesos de mensaje y secuencia para el registro de punto final y la cancelación de un registro de punto final y gatekeeper.

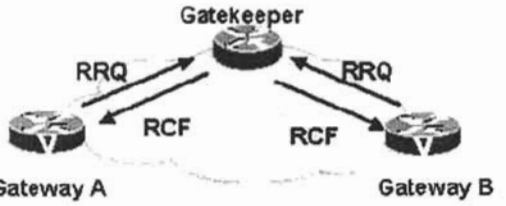


Fig. 5.9 registro de punto final y la cancelación de un registro de punto final y gatekeeper.

Localización de punto final.

Los puntos finales y gatekeepers utilizan la localización de punto final (endpoint) para obtener información de contacto cuando sólo está disponible la información de alias. Los mensajes locate (localizar) son enviados a la dirección del canal RAS del Gatekeeper o son multidifundidos a la dirección de difusión de descubrimiento del gatekeeper. El gatekeeper responsable del punto final solicitado responde indicando su propia información de contacto o la del punto final.

El punto final o gatekeeper puede incluir una o más direcciones E.164 fuera de la zona de petición. Se pueden utilizar los siguientes tres mensajes para localizar puntos finales:

- LRQ. Se envía para solicitar información de contacto del punto final o gatekeeper para una o más direcciones E.164.
- LCF. Se envía por el gatekeeper y contiene el canal de señalización de llamadas o dirección del canal RAS de sí mismo del punto final solicitado. Utiliza su propia dirección cuando se utiliza GKRCS y la dirección del punto final solicitado cuando se utiliza la Señalización de Llamada Directa de Punto Final (Direct Endpoint Call Signaling).
- Location Reject (LRJ). Es enviado a través de los gatekeepers que reciben un LRQ hacia los puntos finales que no están registrados o que no tienen recursos disponibles en éstos.

Admisiones.

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

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

El mensaje ACF contiene la dirección IP del gateway o gatekeeper de terminación y permite que el gateway origen inicie inmediatamente posprocedimientos de señalización de control de llamadas.

Información de Estado.

El gatekeeper puede utilizar el canal RAS para obtener información de estado desde un punto final. Podemos utilizar este mensaje para monitorizar si el punto final está en línea (online) o no (offline) debido a una condición de fallo. El periodo típico de sondeo para los mensajes de estado es de 10 segundos. Durante la ACF, el gatekeeper puede también solicitar que el punto final envíe mensajes de estado periódicos durante una llamada. Podemos utilizar los tres mensajes siguientes para proporcionar el estado en el canal RAS:

- Information Request (IRQ). Se envía desde el gatekeeper al punto final que solicita el estado.
- Information Request Response (IRR). Se envía desde el punto final al gatekeeper en respuesta a una petición de información IRQ. Este mesaje es también enviado desde un punto final si el gatekeeper solicita actualizaciones periódicas del estado.
- Status Enquiry. Se envía fuera del canal RAS en el canal de señalización de llamadas. Un punto final o gatekeeper puede enviar mensajes de Status Enquiry a otro punto final para verificar el estado de la llamada. Los gatekeepers suelen utilizar estos mensajes para verificar si las llamadas siguen activas.

Control de ancho de banda.

El control del ancho de banda se administra inicialmente a través del intercambio de admisiones entre un punto final y el gatekeeper en una secuencia ARQ/ACF/ARJ. Sin embargo, el ancho de banda puede cambiar durante una llamada. Podemos utilizar los siguientes mensajes para cambiar el ancho de banda:

- BRQ. Es enviado por un punto final al gatekeeper pidiendo un incremento o disminución en el ancho de banda de la llamada.
- BCF. Es enviado por el gatekeeper para confirmar la aceptación de la petición de cambio de ancho de banda.
- BRJ. Es enviado por el gatekeeper para rechazar la petición de cambio de ancho de banda (enviada si el ancho de banda solicitado no está disponible).

5.4.1.2.2 Señalización de control de llamadas (H.225).

En las redes H.323, los procedimientos de control de llamadas se basan en la recomendación de la ITU-T, que especifica la utilización y soporte de los mensajes de señalización Q.931. Un canal de control de llamadas seguro se crea en una red IP en el puerto 1720 del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre dos puntos finales para el propósito de conectar, mantener y desconectar las llamadas.

El control de llamadas real y los mensajes de actividad se mueven a puertos efímeros después de configurar la llamada inicial. Pero 1720 es el puerto que se conoce para las llamadas H.323. H.225 también especifica la utilización de los mensajes Q.932 para servicios suplementarios. Los siguientes mensajes Q.931 y Q.932 son los mensajes de señalización más utilizados en las redes H.323:

- Setup. Un mensaje hacia adelante enviado por la entidad H.323 que llama en un intento de establecer conexión con la entidad H.323 llamada. Este mensaje se envía en puerto TCP 1720 de H.225.

- Call Proceeding. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad que llama para avisar que los procedimientos de establecimiento de llamada se han iniciado.
- Alerting. Un mensaje hacia atrás enviado desde la entidad llamada para avisar a la parte que llama que el sonido de llamada se ha iniciado.
- Connect. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad llamante indicando que la parte llamada ha respondido la llamada. El mensaje de conexión puede contener la dirección de transporte UDP/IP para la señalización de control de H.225.
- Release Complete. Enviado por el punto final que inicia la desconexión, e indica que la llamada ha sido liberada. Se puede enviar este mensaje únicamente si el canal de señalización de la llamada está abierto o activo.
- Facility. Un mensaje Q.932 utilizado para solicitar o confirmar servicios suplementarios. También se utiliza para indicar si una llamada debe ser dirigida o debe ir a través de un gatekeeper.

La fig. 5.10 muestra los mensajes de señalización para la configuración de las llamadas H.323. La interacción con el gatekeeper se limita a los mensajes de RAS para los mensajes de estado de permiso y posibilidad de llamada.

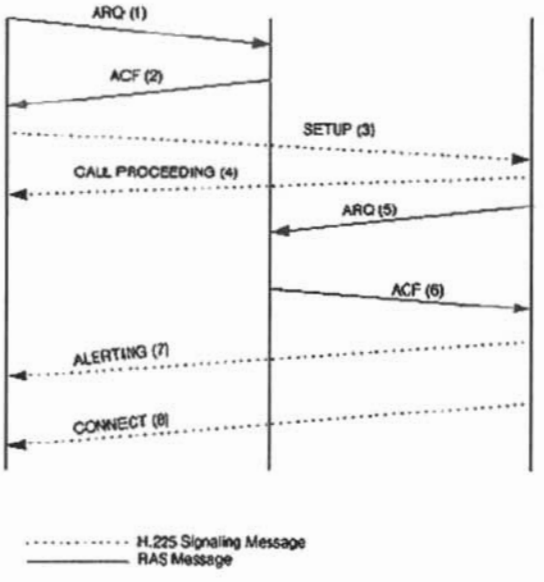


Fig. 5.10 Establecimiento de una llamada H.323 .

Se puede enrutar el canal de señalización de la llamada en una red H.323 de dos maneras: a través de Señalización de Llamada Directa de Punto Final (DECS, Direct Endpoint Call Signaling) y de Señalización de Llamada de Gatekeeper enrutado (GKRCS, Gatekeeper routed Call Signaling). En el método de DECS, los mensajes de señalización se envían directamente entre los dos puntos finales. En el método GKRCS, los mensajes de las llamadas entre los puntos finales son a través del gatekeeper. Estos dos métodos los podemos observar en la fig. 5.11 que a continuación se muestra:

Fig. 5.11 Enrutamiento de las llamadas por medio de DECS y GKRS.

Se puede ofrecer servicios suplementarios a través del método GKRCS si el canal de señalización de la llamada permanece abierto durante la misma. Los gatekeepers también pueden cerrar el canal de señalización de la llamada después de que se haya completado su configuración.

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

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

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

Si utilizamos la señalización de llamadas de gatekeeper enrutado, podemos controlar el enrutamiento del canal de dos maneras: utilizar Direct H.245 Control, que tiene lugar directamente entre dos puntos finales participantes, o bien utilizar Gatekeeper Touted H.245 Control, que tiene lugar entre cada punto final y su gatekeeper.

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

- Capabillity exchange. Consiste en mensajes que intercambian de manera segura las capacidades entre puntos finales, también llamados terminales. Estos mensajes indican capacidades del terminal para transmitir y recibir audio, video y datos al terminal que está participando. Para audio , el intercambio de capacidades incluye códec de transcodificación de voz de la serie G, como G.729 a 8Kbps, G.728 a 16Kbps, G.711 a 64Kbps, G.723 a 5.3 ó 6.3Kbps, G.722 a 48, 56 y 64Kbps. También incluye velocidades de muestreo de las series ISO, así como los códec de audio de voz de tasa completa, tasa media y tasa mejorada de GSM.
- Master-Slave Termination. Procedimientos utilizados para determinar qué punto final es el principal (maestro) y qué punto final es el secundario (esclavo) para una llamada determinada. La relación se mantiene durante la duración de la llamada y se utiliza para resolver conflictos entre puntos finales. Las reglas maestro-esclavo (master-slave) se utilizan cuando ambos puntos finales solicitan acciones similares a la vez.

- Round-Trip Delay. (retraso de ida y vuelta). Procedimientos utilizados para determinar el retraso entre los puntos finales de origen y de terminación. El mensaje RoundTripDelayRequest mide y verifica si la entidad remota del protocolo H.245 está activa.
- Logical Channel Signaling. Abre y cierra el canal lógico que transporta la información de audio, video y datos. El canal se prepara antes de la transmisión real para asegurar que los terminales están listos y son capaces de recibir y decodificar información. Los mismos mensajes de señalización establecen los canales unidireccionales y bidireccionales. Cuando se ha establecido la señalización del canal lógico con éxito, el puerto UDP para el canal de medios RTP es pasado desde el punto final de terminación hasta el punto final de origen. Así mismo, cuando se utiliza el modelo Gatekeeper Call Routed, es en este punto donde el gatekeeper puede desviar los flujos RTP proporcionando la dirección UDP/IP real del punto final de terminación.

Procedimientos de conexión rápida.

Los dos procedimientos disponibles para establecer canales de medios entre los puntos finales son H.245 y Fast Connect. Fast Connect permite que se establezca la conexión de medios para llamadas básicas punto a punto con mensaje de intercambio de ida y vuelta. Estos procedimientos dictan que el punto final llamante incluya el elemento faststart (inicio rápido) en el mensaje de configuración inicial.

La parte faststart contiene una secuencia de la estructuras codificadas del canal lógico, que dan capacidades al canal de medios y los parámetros necesarios para abrir e iniciar la transmisión de medios, en respuesta, el punto final llamado devuelve un mensaje H.225 (call proceeding, progress, alerting o connect) que contiene un elemento faststart que selecciona las capacidades de terminal aceptadas. En ese momento, tanto los puntos finales llamantes como los llamados pueden transmitir medios si las secuencias de configuración basadas en H.225 han alcanzado el estado conectado.

Tunneling H.245 .

Se puede encapsular o "tunelear" mensajes H.245 dentro del canal de señalización de llamadas H.225 en lugar de crear un canal de control H.245 separado. Este método mejora el tiempo de conexión de llamada y la asignación de recursos, y proporciona una sincronización entre la señalización y el control de llamadas. Se puede encapsular múltiples mensajes H.245 en un mensaje H.225. Asimismo, en cualquier momento un punto final puede conmutar una conexión H.245 separada.

Terminación de llamada.

Cualquier punto final que participe en una llamada puede iniciar el procedimiento de terminación de llamada. En primer lugar, deben cesar las transmisiones de medios (como audio, video o datos) y cerrarse todos los canales lógicos. A continuación, debe finalizarse la sesión H.245 y enviarse un mensaje de liberación completa (release complete message) en el canal de señalización de llamada, si sigue estando abierto o activo. En ese momento, si ningún gatekeeper está presente, se termina la llamada. Cuando un gatekeeper está presente, se utilizan los siguientes mensajes en el canal RAS para completar la terminación de llamada:

- Disengage Request (DRQ). Se envía por un punto final o gatekeeper para terminar una llamada.

- Disengage Confirm (DCF). Se envía por un punto final o gateekeper para confirmar la desconexión de la llamada.
- Disengage Reject. (DRJ). Se envía por un punto final o gatekeeper para rechazar la desconexión de llamada.

Transporte de medios (RTP/RTCP).

RTP proporciona transporte de medios en H.323 de manera más específica, RTP permite la entrega de extremo a extremo en tiempo real de audio, video y datos Inter. Activos sobre redes de unidifusión (unicast) o multidifusión (multicast). Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporización y monitorización.

RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y los QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP, donde los flujos RTP actúan en un número de puerto par y el flujo RTCP correspondiente actúa en el siguiente número de puerto más alto (impar).

5.4.1.2.4 Flujos de llamada H.323.

Los flujos de llamadas descritos en esta sección muestran cómo la familia de protocolos H.323 proporciona una configuración de llamada entre dos puntos finales. Imaginemos que son llamadas de voz en que todos los puntos finales han completado el registro con el gatekeeper apropiado. Los ejemplos de configuración de llamada incluyen dos implementaciones de gatekeeper diferentes, así como dos métodos de señalización de llamada diferentes.

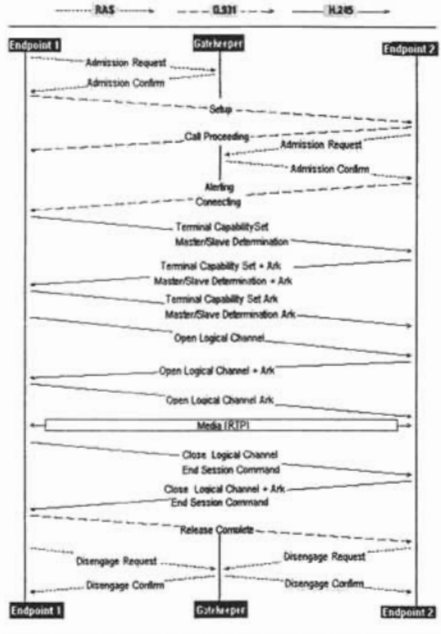


Fig. 5.12 Señalización directa de punto final. Mismo gatekeeper.

En la fig. 5.12 se muestran los flujos de llamada que utilizan la señalización directa de punto final entre dos puntos finales que comparten el gatekeeper.

En la siguiente fig. 5.13 se observan los procedimientos de llamada de gatekeeper doble. De manera específica los flujos de llamada utilizan una señalización de punto final directa entre dos puntos finales que tienen diferentes gatekeepers. La principal diferencia entre la GKRCS y la señalización de llamada directa es que en el primer caso el mensaje de configuración es diseccionada hacia el gatekeeper y en la señalización de llamada directa es direccionado hacia el punto final de terminación.

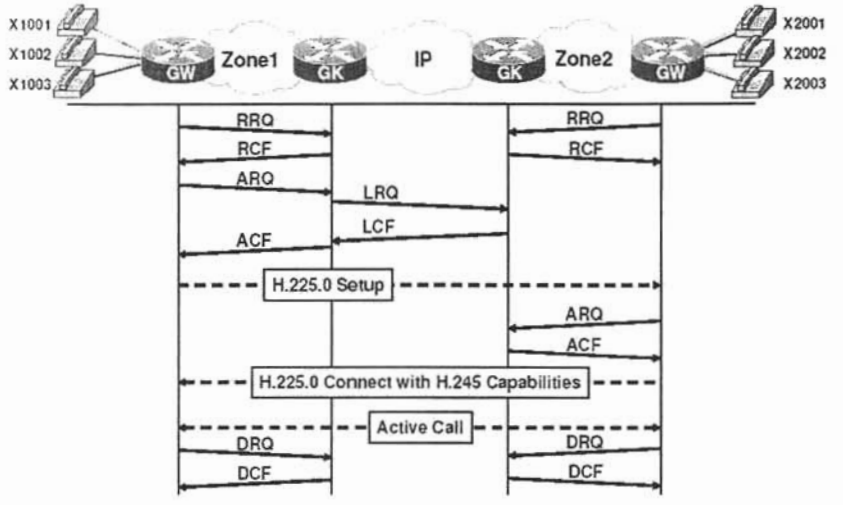


Fig. 5.13 Señalización directa de punto final. Dos gatekeepers.

5.4.2 Protocolo SIP .

El protocolo de inicio de sesión (**SIP**) es un protocolo de control de señalización de la capa de aplicación que se utiliza para establecer, mantener y terminar sesiones multimedia. Las sesiones multimedia incluyen telefonía Internet, las conferencias y otras aplicaciones similares que proporcionan medios como audio, video y datos.

El SIP se describe mejor como RFC 2543 desarrollado por el grupo IETF (Internet Engineering Task Force), indica que es un protocolo de control de capa de la aplicación (señalización) para crear, modificar y terminar sesiones con uno o más conjuntos participantes.

Estas sesiones multimedia incluyen audio, video y datos y pueden incluir múltiples participantes. El SIP permite que los participantes sean invitados a una conferencia improvisada. Esas sesiones multimedia pueden comunicarse a través de multidifusión o unidifusión, o bien por una combinación de ambos mecanismos de entrega.

La telefonía del IP se sigue desarrollando y en el futuro se requerirán posibilidades adicionales de señalización. La extensibilidad de SIP permite dichos desarrollos de funcionalidad incremental. Las cabeceras de los mensajes SIP son versátiles y se pueden registrar funciones adicionales con la Agencia de asignación de números Internet. La

flexibilidad de mensaje SIP también permite que los elementos construyan servicios telefónicos avanzados, incluidos los servicios de tipo de movilidad.

Actualmente están funcionando muy pocas implementaciones del protocolo SIP, a pesar de que muchos fabricantes y clientes están interesados en utilizarlo para desarrollar servicios mejorados. Principalmente por su operación en conjunto con otros protocolos de señalización, como **H.323,** por lo que su futuro es muy prometedor en la nueva telefonía de Internet y sea una nueva punta de lanza como lo es ahora **H.323**.

5.4.2.1 Origen del protocolo SIP.

El protocolo SIP se ha desarrollado dentro del grupo de trabajo MMUSIC (Multiparty Multimedia Session Control) del IETF, que es el responsable del desarrollo de protocolos para el soporte de conferencias multimedia sobre internet. Entre los protocolos desarrollados en este grupo destacan el SIP (Session Initiation Protocol) y el SDP (Session Description Protocol).

La primera red definida por MMUSIC fue la red MBONE (Multicast Backbone) que es una red virtual superpuesta sobre internet, que permite el desarrollo de conferencias multimedia con dos o más participantes. Ha sido ampliamente utilizada, sobre todo dentro del mundo académico, para tele-conferencias y tele-educación. En 1999, dentro del IETF, se creo un grupo de trabajo específico para SIP.

5.4.2.2 Modelo SIP.

Según se ha expuesto antes, las ventajas del protocolo SIP se derivan en primer lugar del modelo que utiliza: un modelo cliente/servidor. En una sesión SIP el extremo que inicia la comunicación es el cliente y el que responde es el servidor.

Dentro de la arquitectura SIP existen dos tipos de sistemas:

- ✓ Agentes de usuario: son los sistemas finales, capaces de iniciar o terminar una sesión SIP. Para realizar estas dos funciones, tiene dos partes: agente de usuario cliente (UAC) y agente de usuario servidor (UAS) que realizan las funciones necesarias para iniciar o terminar una sesión, respectivamente.
  Como ejemplos, se pueden citar: una terminal de usuario basada en SIP (PC multimedia o teléfono, fig. 5.14), que incluye UAC y UAS porque el usuario desea recibir y realizar llamadas, o un contestador, que sólo requiere UAS.

Fig. 5.14 Ejemplo de una terminal comercial.

- ✓ Servidores: son elementos opcionales que pueden actuar como sistemas intermedios en una sesión SIP entre dos o más agentes de usuario. Su función principal es facilitar el encaminamiento hacia el destino solicitado.

5.4.2.3 Mensajes SIP.

Según se ha indicado anteriormente, el protocolo SIP se basa en el intercambio de mensajes textuales, que pueden ser de dos tipos: peticiones o respuestas.

Peticiones incluidas en la primera versión del protocolo:

- ✓ INVITE: Mensaje inicial de invitación enviado por el extremo llamante.
- ✓ ACK: respuesta del agente llamante ante el mensaje de aceptación de la llamada por parte del destino.
- ✓ CANCEL: Cancela una petición en curso (ejemplo: el llamante cuelga antes de que el llamado acepte la invitación).
- ✓ BYE: Indicación de abandono de un participante en una sesión múltiple.
- ✓ OPTIONS: Consulta a un agente de usuario acerca de sus capacidades (ejemplo: códec)
- ✓ REGISTER: empleado por los usuarios para registrar su dirección de contacto actual.

Como norma general, el protocolo establece que toda petición ha de ser confirmada mediante la respuesta del extremo remoto, excepto el mensaje ACK que no requiere respuesta.

Existen propuestas para ampliar los mensajes SIP, pero los originales son los seis expuestos.

Las respuestas se basan en el empleo de códigos numéricos organizados en seis rangos que se identifican por el primer dígito:

- ✓ Provisionales (no terminan la transacción).
  - 1XX, INFORMATIVAS: son respuestas que indican que la petición está siendo procesada pero no se ha completado (e.j. 180= "ringing" indica que suena el timbre del terminal llamado pero no ha sido descolgado).
- ✓ Finales (terminan la transacción).
  - 2XX, ÉXITO: la petición ha sido completada con éxito en el extremo remoto (e.j.: 200 = "OK", el extremo remoto acepta la comunicación).
  - 3XX, REDIRECCIÓN: indica al llamante que su petición debe ser redirigida hacia otra ubicación (ej 302 ="moved temporarily").
  - 4XX, FALLO DE PETICIÓN: la petición tal como se ha recibido no puede cursarse. Se sugiere la posibilidad de reintentarla una vez modificada adecuadamente (e.j.: 400 ="bad request" indica error de sintaxis).
  - 5XX, ERROR DEL SERVIDOR: error en el servidor al procesar la información. Posiblemente subsanable si se reintenta la petición.
  - 6XX, FALLO GLOBAL: la petición no puede ser cursada, sin que proceda su reintento.

5.4.2.4 Ejemplo SIP .

En la siguiente fig. 5.15 se presenta, a modo de ejemplo, la secuencia de mensajes SIP intercambiados en una sesión establecida directamente entre dos usuarios, sin la intervención de servidores intermedios.

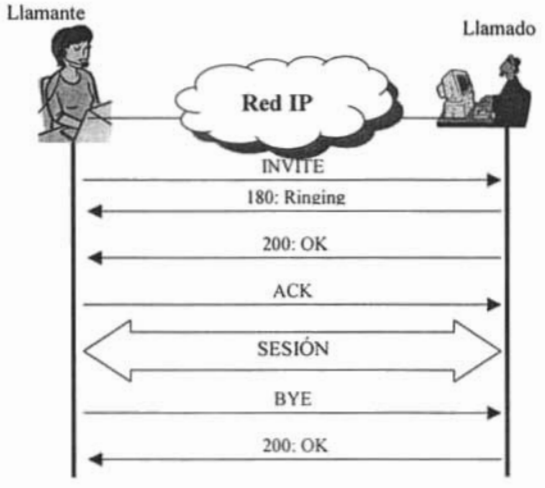


Fig. 5.15 Ejemplo de sesión con SIP.

El procedimiento que se refleja en el ejemplo anterior empieza con el mensaje INVITE del usuario llamante (UAC) al usuario llamado (UAS). En este mensaje se incluye información como: dirección origen, dirección destino y Call-ID (referencia local de la sesión) El cuero del mensaje incluye información sobre el tipo de sesión que se desea establecer en forma de mensaje SDP.

Si el llamado acepta la invitación, lo indica devolviendo el mensaje OK (200) hacia el origen. En este mensaje se incluyen, al menos, los parámetros: dirección origen, destino y call-ID y en el cuerpo del mensaje, el tipo de sesión que se acepta.

El establecimiento de la sesión, termina con el envío del mensaje ACK desde el llamante al llamado. En este punto la sesión está establecida y se realiza el intercambio de paquetes de video y voz sobre la sesión RTP.

Para liberar la sesión, cualquiera de los interlocutores envía un mensaje BYE hacia el extremo remoto y el extremo responde con OK (200).
Los mensajes SIP se transportan utilizando UDP (opción más habitual), sobre TCP o sobre STCP (Stream Control Transport) que es un protocolo desarrollado por el grupo de trabajo SIGTRAN del IETF diseñado para transporte fiable de señalización sobre IP.

5.4.2.5 Protocolo de Descripción de Sesión (SDP).

SDP (Session Description Protocol) es otro estándar de internet originado en el grupo de trabajo MMUSIC del IETF. Está especificado en la RFC2327 de abril de 1998.

SDP más que un protocolo es una norma que describe el formato de los mensajes en una sesión multimedia. Los mensajes SDP pueden contener información muy variada sobre las características de una sesión (nombre de la sesión, motivo, instante de inicio y final, tipo de medios involucrado, códecs a emplear, direcciones IP y puertos UDP para el flujo RTP, etc.).

A través del intercambio de mensajes SDP los extremos acuerdan las características particulares de una sesión concreta, durante la negociación de capacidades. Este proceso es fundamental en entornos abiertos, porque las terminales que participan tienen características heterogéneas.

El uso de SDP no es exclusivo del protocolo SIP, sino que se emplea en otros ámbitos, por ejemplo en el protocolo MEGACO/H.248, que se cita más adelante.

5.4.2.6 Servidores SIP .

Permiten completar el establecimiento de sesiones en situaciones en las que el interlocutor llamante desconoce la ubicación exacta del llamado (o su dirección IP exacta). Esta situación se producen cuando el llamado está tras una red privada o no posee una localización fija. Los servidores dan soporte a la movilidad de usuarios SIP. Existen varios tipos de servidores:

- *Servidor de registro*: acepta peticiones de registro de las UAC, actualizando la información relativa a cada uno de ellos en una base de datos de localización.
- *Servidor procurador*: recibe peticiones de inicio de sesión, encargándose de reenviarla hacia el siguiente sistema SIP (servidor o UAC).
- *Servidor de redirección:* similar a un servidor procurador pero no cursa directamente la invitación hacia el siguiente sistema SIP, sino que informa al llamante de la nueva dirección del destino (código 3XX).
- *Servidor de agente de usuario (UAS):* es el cuarto tipo de servidor.

5.4.2.7 Servicios sobre SIP .

Uno de los principales alicientes de SIP es la gran flexibilidad para soportar servicios. Algunos de estos servicios son similares a los servicios suplementarios que ofrece la red telefónica en un entorno IP, pero otros son completamente nuevos (ej. el servicio "*click to call*" ligado a una página web).

Para facilitar la creación y desarrollo de nuevos servicios sobre SIP, en terminales y servidores, existen varios mecanismos parecidos a los que se utilizan en servicios de páginas web:

- ✓ *SIP CGI (Common Gateway Interface)*: El concepto CGI fue desarrollado para permitir la integración de servicios sobre servidores web. El interfaz SIP CGI, (RFC 3050) permite invocar la ejecución de un programa (ejecutable, script en Perl...) al satisfacer una condición determinada (e.j. recibir un mensaje INVITE dirigido a un determinado usuario, la hora del día, si el usuario está libre, ocupado o no contesta, la prioridad de la llamada, el nombre del llamante, la empresa a la que pertenece).
- ✓ *SIP Applets/Servlets*: Es otro de los mecanismos utilizados en el soporte de las páginas web. Programas en Java que pueden ejecutarse en los clientes (applets) o en los servidores (servlets) y pueden interactuar con éstos a través de una interfaz normalizado. Por tanto, un servicio SIP puede darse a través de la

descarga de un applet en el terminal o asociando al usuario a un servlet en el servidor SIP.

- ✓ *Sripts CPL (Call Processing Language)*: Lenguaje textual de marcas, similar al HTML, definido por el IETF que permite especificar servicios a ejecutar en el servidor SIP proxy (reenvío, redireccionamiento o rechazo, búsquedas en bases de datos, envío de e-mail,...), ligados a condiciones.

Aprovechando todas estas funcionalidades es posible desarrollar servicios muy variados: redirección de llamada, prohibición de llamadas salientes a ciertos números, dirigir automáticamente la llamada a una persona u otra en función del idioma, encaminar según la prioridad, avisar por correo electrónico de las llamadas fallidas, etc.

5.4.3 Comparación H.323 Vs SIP .

En la siguiente tabla 5.1 se incluye la comparación de las principales características de los protocolos H.323 y SIP.

	H.323	**SIP**
Origen	ITU-T	IETF
Codificación	Binaria (ASN.1)	Texto plano
Transporte de señalización	TCP/UDP	UDP
Tiempo de establecimiento	~5 x tiempo ida/vuelta ~ 13 mensajes (TDP)	1.5 x tiempo ida/vuelta 3 mensajes
Disponibilidad comercial	Alta	En auge
Flexibilidad y extensibilidad	Baja	Alta (facilita extensión e integración con otros protocolos IP)
Complejidad	Alta	Baja

Tabla 5.1 Tasa de envío nominal y real de los códecs normalizados.

Según se ha mencionado anteriormente, la ventaja fundamental del SIP frente al H.323 es la mayor simplicidad y flexibilidad. Las razones que justifican esta afirmación se apoyan en el hecho de que el establecimiento de H.323 requiere varios flujos de señalización (RAS, Q.931 y H.245) y la codificación de los mensajes es binaria. En cambio, en SIP existe un flujo único de señalización que se apoya sobre un número reducido de mensajes codificados de manera textual.

En la tabla 5.1 de comparación se aprecia que el protocolo SIP es más ágil que H.323 porque requiere menos mensajes en el establecimiento de una sesión y esto se traduce en un retardo y tiempo de establecimiento menor. En H.323, sin tener en cuenta los mensajes RAS intercambiados con el guardián, son necesarios: 3 mensajes Q.931, 4 mensajes H.245 y dos establecimientos de conexión TCP con tres mensajes cada uno; haciendo un total de 13 mensajes para establecer una sesión. Esto se ha reducido en las últimas versiones de H.323 al sustituir TCP por UDP y encapsular los mensajes H.245. Por otra parte en SIP son necesarios únicamente 3 mensajes para el establecimiento de una sesión. Estas diferencias en el número de mensajes se reflejan en el tiempo de establecimiento. En H.323 se emplea un tiempo 5 veces superior al retardo de ida y vuelta mientras que en SIP el tiempo es 1.5 veces el retardo de ida y vuelta.

Comparando la disponibilidad de equipos y aplicaciones en H.323 y SIP, se observa que hasta hace un par de años existían muy pocos para SIP. Sin embargo, últimamente

se han desarrollado múltiples aplicaciones SIP que avalan la apuesta por esta tecnología realizada por fabricantes y diseñadores.

5.5 Factores de VoIP .

Para crear un diseño de red apropiado, es importante conocer algunos de los fundamentos de la tecnología VoIP. Por lo tanto, es necesario tomar en cuenta muchos de los problemas a los que se enfrenta la Voz sobre IP y saber cómo pueden afectar a las redes de paquetes.

En la fig. 5.16 se ilustra las funciones básicas necesarias para el transporte de voz sobre una red de conmutación de paquetes.

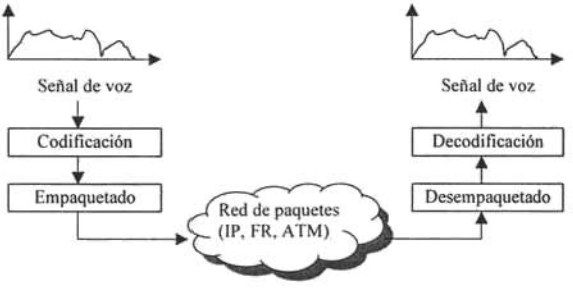


Fig. 5.16 Transporte de voz sobre red IP

El primer paso del proceso es el muestreo y digitalización de la señal vocal en el origen. A continuación se codifica la información en bloques obtenidos con una ventana temporal (el número de bits por bloque depende del codificador). El tercer paso es el empaquetamiento, en el que se encapsulan uno o más bloques de datos en un paquete (el empaquetamiento se produce en uno o varios pasos, dependiendo de la pila de protocolos que se utilice).

El proceso en el extremo de recepción es inverso al realizado en el origen: desempaquetado, decodificación y reconstrucción de la señal a partir de la señal digitalizada.

En apariencia es un proceso sencillo pero está determinado por los problemas derivados del transporte del flujo de información a través de la red. Según la carga de tráfico de los diferentes nodos, los paquetes sufren esperas variables dando lugar a fluctuaciones en el retardo (*jitter*) y en algunos casos a pérdidas de paquetes. Esto da lugar a un flujo de paquetes que no mantiene el espaciamiento constante y que es posiblemente incompleto. Desde el punto de vista del usuario estos problemas se traducen en la degradación de la voz.

En la definición de redes ATM se tuvo en cuenta la voz como servicio importante y se aseguraron diferentes calidades de servicio. Sin embargo las redes IP y *Frame Relay*, pensadas originalmente para datos, no incluyen requisitos estrictos de retardo y es necesario incluir una serie de mecanismos para obtener calidad de servicio adecuada para voz.

Los mecanismos complementarios que reducen los efectos indeseados (pérdida de paquetes y fluctuaciones de retardo) se orientan en dos sentidos:

- ✓ Eficiencia y calidad de servicio:
  - Codecs compresores que reducen el ancho de banda necesario.
  - *Buffers* en recepción que regeneran el espaciado entre paquetes y amortiguan las fluctuaciones del retardo.
  - Mecanismos de calidad de servicio en la red (e.j.: priorización de los paquetes de voz).

- ✓ Señalización:
  - Establecimiento y liberación dinámica de las llamadas VoIP.
  - Información para el usuario del progreso de la llamada.
  - Acuerdo en los códecs a emplear.
  - Movilidad de usuarios.
  - Control de acceso.
  - Tarificación.
  - Servicios suplementarios (ej. desvío de llamadas).
  - Interfuncionamiento con la red telefónica.
  - Tratamiento de señales no vocales (ej. MODEM o fax).

5.5.1 Códecs de voz.

Existen tres bloques de codificadores de voz, según las técnicas de codificación que emplean:

- *De forma de onda*: representan cada muestra del conversor analógico-digital por un valor binario. Un ejemplo representativo es el G.711 utilizado en la red telefónica conmutada.
- *Adaptativo diferencial*: es muy parecido al códec de forma de onda, pero no codifica el valor de la muestra, sino la diferencia entre cada muestra y la anterior. La ventaja fundamental que presenta es que necesita tasas de bits menores porque el rango de valores que tiene que codificar es mucho más reducido.
- *Predictivo lineal*: Son codificadores de bloques que trabajan con conjuntos de muestras, en vez de utilizar muestras aisladas. Seleccionan el conjunto a través de ventanas de muestreo, extraen una serie de características y las representan de manera parametrizada. Una de sus principales virtudes es la baja tasa binaria que generan. Al comparar la tasa binaria con la del G.711 se observan reducciones significativas por lo que se denominan códecs compresores. Estos codificadores se utilizan en ocasiones en las que el ancho de banda es un recurso escaso. Un ejemplo es el acceso vía MODEM telefónico a la telefonía IP a través de internet. Otro caso es el de un operador que ofrece tránsito de llamadas de larga distancia sobre una red IP.

En la tabla 5.2 se presentan las características más relevantes de los principales códecs de voz normalizados en recomendaciones de la serie G del ITU-T y el códec utilizado en GSM "*Full Rate*" (GSM 06.10) .

	G.711	G.721	G.726	G.727	G.728	G.729	G.723.1	GSM FR
Tipo de codificación	PCM	ADPCM	ADPCM	ADPCM	LD-CELP	CS-ACELP	MP-MLQ/ ACELP	RPE-LTP
Tasa binaria (Kbits/s)	64	32	16/24/ 32/40	16/24/ 32/40	16	8	6,4/5,3	13
Complejidad (MIPS)	0,1	10	12	12	33	22	16/18	2,5
Retardo codificador (ms)	0,125	0,125	0,625	0,125	0,125	15	37,5	20
Calidad (MOS)	4,2	4,0	4,0	4,0	4,0	4,0	3,7-3,9	3,6-3,8

Tabla 5.2 Códecs normalizados.

Las principales características que convienen destacar son:

- ✓ En conjunto, el tipo de codificación y la tasa binaria, dan *el factor de compresión,* indica la reducción de ancho de banda que proporciona. Se compara con los 64 Kbits/s habituales en la RTC.
- ✓ *La complejidad del algoritmo de codificación,* es directamente proporcional a la capacidad de proceso necesaria (influye en aspectos de implementación: si puede implementarse en software o requiere *hardware* específico) Normalmente el algoritmo es más complejo al aumentar el factor de compresión del códec..
- ✓ *Retardo de codificación,* depende del tipo de proceso que se realiza sobre las muestras. En los códecs LPC es superior a los demás porque es necesario esperar a obtener el grupo de muestras antes de codificar. El retardo puede ser despreciable en comparación con el resto de retardos pero si existen problemas de retardo es necesario optar por un codificador más sencillo.
- ✓ *Calidad,* evaluada mediante el parámetro MOS (*Mean Opinion Score*) que se obtienen a partir de la valoración subjetiva de un conjunto de personas. Se están proponiendo nuevos modelos como el E-model (modelo matemático que incluye parámetros como S/N, interferencias simultáneas a la señal de voz, interferencias retrasadas) y el de ETSI (Instituto Europeo de Normas de Telecomunicación) porque es un método que no tiene en cuenta las pérdidas o los errores.

5.5.2 Supresión de silencios.

Es un mecanismo complementario al empleo de códecs compresores para reducir el ancho da banda. Se pretende detectar períodos de silencio durante la conversación (mecanismos VAD, *Voice Activity Detection*) suprimiendo el envío de paquetes de voz mientras dure la situación. Como en la conversación telefónica cada interlocutor sólo habla la mitad del tiempo y realiza pausas entre frases, se pueden obtener reducciones de hasta el 60% en el flujo de paquetes.

Para evitar que el interlocutor piense que se ha cortado la comunicación durante los intervalos de silencio se envían periódicamente paquetes de silencio (SID, *Silence Insertion Description*) durante la pausa. Estos paquetes proporcionan una indicación del nivel de ruido que existe en el origen para que el receptor lo simule en el terminal remoto mediante un generador de ruido (Recomendación UIT-T I.366.2).

5.5.3 Retraso (Latencia).

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

Existen tres tipos de retraso que son inherentes a las redes de telefonía actuales: retraso de propagación, retraso de señalización y retraso de manejo.

- retraso de propagación es causado por la velocidad de la luz en la fibra óptica o en las redes basadas en cobre.
- retraso de manejo, también llamado retraso de procesamiento, define muchas causas diferentes de retraso (empaquetado, compresión y switching de paquetes), y está causado por dispositivos que transmiten la trama a través de la red.
- retrazo de señalización es la cantidad de tiempo que se tarda en colocar un bit o byte en una interfaz y es relativamente pequeña.

Retraso de propagación.

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

Retraso de Manejo.

Como se mencionó anteriormente, los dispositivos que envían la trama a través de la red provocan un retraso de manejo. Los retrasos de manejo pueden tener impacto en las redes telefónicas tradicionales, pero esos retrasos son un problema mayor en los entornos de paquetes. A continuación se explicará los diferentes retrasos de manejo y sus efectos en la calidad de voz.

5.5.4 Retardo extremo a extremo.

Existen muchos factores que contribuyen al retardo extremo a extremo: retardo del algoritmo de codificación, tiempo de empaquetado, tiempo de propagación (despreciable salvo en distancias muy grandes), tiempo de transmisión, tiempos de espera en los nodos de conmutación (dependiente del tráfico en la red) y tiempo de descompresión.

El retardo total extremo a extremo en una conversación telefónica, ha de mantenerse por debajo de un cierto nivel para minimizar dos efectos indeseables: la pérdida de interactividad y el eco.

A partir de 150 ms de retardo en un sentido, la comunicación se vuelve molesta por la pérdida de interactividad: la persona que habla al percibir que su interlocutor tarda en contestar, repite sus palabras y a la vez que recibe la respuesta procedente del otro extremo.

El segundo efecto, el eco, es más molesto cuanto mayor es el retardo ida y vuelta. Los motivos por los que se produce eco en la telefonía IP son los mismos de las redes telefónicas convencionales. Sin embargo, el retardo que introduce el transporte de voz por redes de paquetes (codificación, empaquetado, transporte y espera en los nodos) hace que los efectos sean más perjudiciales.

- *Eco eléctrico*: el bucle telefónico convencional consta de un par de hilos sobre los que se transmite de manera bidireccional. En el teléfono y en las centrales telefónicas se separan los dos sentidos de transmisión mediante bobinas híbridas. Como estos dispositivos no son perfectos, la separación de señales no es

completa y aparecen reflejos indeseados de las señales hacia los focos emisores. De todas las posibles reflexiones, la más molesta es la que presenta mayor desfase temporal con respecto a la señal original. Si el retardo ida y vuelta de la señal es elevado, **superior a 50 ms** el usuario percibe el eco. En la telefonía convencional este retardo sólo se produce en llamadas internacionales. Sin embargo, en las pasarelas VoIP este límite se supera con bastante frecuencia. Al superar 50 ms de retardo, es necesario utilizar mecanismos de supresión o cancelación de ecos.

- *Eco acústico*: es el que se produce por acoplo entre el altavoz y el micrófono. Suele ser despreciable en terminales telefónicas convencionales y sin embargo tiene entidad suficiente en equipos a manos libres o en teléfonos móviles que incluyen sus propios mecanismos de cancelación. En un entorno de telefonía IP con PC, que integran altavoz y micrófono en el equipo es necesario tener en cuenta el eco acústico.

En la teoría se plantea que el punto óptimo de cancelación de eco es en el punto más próximo a la reflexión. Sin embargo, en la práctica hay que tener en cuenta que el eco ha de ser cancelado por el operador que lo introduce. En la fig. 5.17, por ejemplo, el eco se percibe como consecuencia del retardo que introduce la red de tránsito VoIP, por lo que la cancelación del eco es responsabilidad del operador de tránsito y ha de llevarse a cabo en las pasarelas.

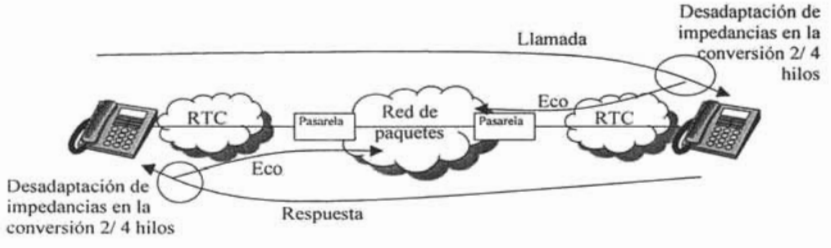


Fig. 5.17 Generación de eco eléctrico.

5.5.5 Fluctuación de retardo (jitter).

El transporte de voz empaquetada no es sensible sólo al retardo extremo a extremo (latencia) sino también a las fluctuaciones o variaciones de ese tiempo de retardo (*jitter*). Estas variaciones son debidas a la fluctuación en los tiempos de espera de los nodos de conmutación de la red que dependen del tráfico concreto del momento.

Estas variaciones en el tiempo de retardo se traducen en flujos de paquetes espaciados de manera irregular en el tiempo. Como la regeneración de la señal de voz en el receptor es un proceso síncrono, necesita disponer de un bloque de voz de manera periódica (con periodo dependiente de la ventana de muestreo del codificador) Sin embargo, por las variaciones del retardo, el flujo de paquetes recibido carece de la sincronía necesaria. Para evitarlo se utiliza un buffer amortiguador en el receptor que almacena los paquetes por orden de llegada extrayéndolos de manera síncrona. En la fig. 5.18 se observa cómo se reduce la incertidumbre del retardo sufrido por un paquete al incluir un buffer amortiguador.

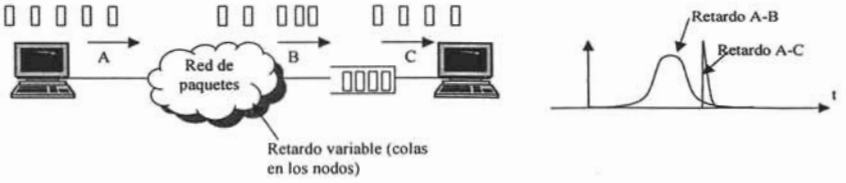


Fig. 5.18 Efecto del buffer amortiguador en el retardo.

El tamaño del buffer refleja el compromiso entre el filtrado de las variaciones de retardo (mejor cuanto mayor sea el buffer) y el retardo extra que se añade (menor cuanto menor sea el buffer). En la sigueinte fig. 5.19 se ilustra este compromiso.

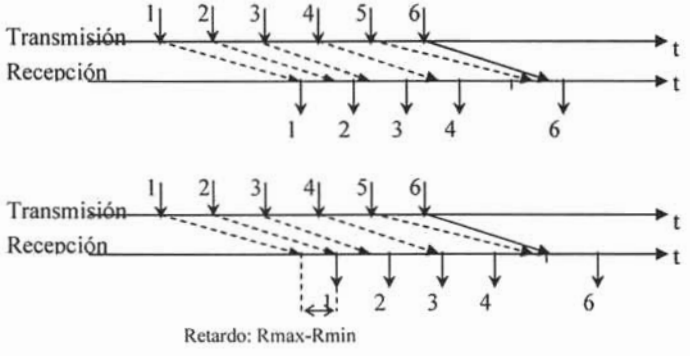


Fig. 5.19 Efecto del buffer amortiguador en la pérdida de paquetes

En la parte superior de la fig. 5.19 se representa un receptor que no utiliza buffer y por tanto un paquete que sufra un retardo grande (paquete 5 de la figura), se pierde. Si el retardo varía entre los límites conocidos (entre Rmax y Rmin), un buffer que introduzca un retardo adicional Rmax-Rmin en el paquete recibido, asegura que no se produzca nunca la pérdida de un paquete.

En el caso de voz sobre ATM la red puede ofrecer conexiones con retardo máximo (Rmax) y con variación máxima (Rmax-Rmin) garantizados por lo que el empleo de un buffer amortiguador solucionaría el problema de *jitter*.

En las redes IP actuales no hay garantía de retardo máximo por lo que existe una cierta probabilidad de pérdida de paquetes. En este caso es necesario ajustar el buffer en función de las pérdidas admisibles y el retardo adicional tolerable. En la práctica muchos equipos de VoIP suelen ajustar el buffer de manera automática en función de las características actuales del tráfico.

5.5.6 Pérdida de paquetes.

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

Cuando se genera un tráfico muy intenso en las redes de datos, es importante controlar la cantidad de pérdida de paquetes que hay en esa red. Con protocolos como SNA (System Network Arquitecture), que no toleran la pérdida de paquetes, se necesita construir adecuadamente una red que sea capaz de priorizar los datos sensibles al tiempo por delante de los datos que pueden manejar el retraso y la pérdida de paquetes.

Las pérdidas de paquetes se producen por errores de transmisión y por congestión de la red. Como el tráfico es impredecible en las redes de paquetes no orientadas a conexión, el número de paquetes que esperan salir por un enlace en un momento determinado supere la capacidad de la cola de salida. En este caso, el conmutador debe descartar los paquetes que no caben en la cola y se pierden. En algunos casos se descartan paquetes antes de que se produzca la congestión para que los emisores de flujo perciban las pérdidas como aviso de congestión inminente y reduzcan el tráfico.

En los emisores de voz, que tienen flujo de tasa fija, el aviso de congestión es inútil porque no pueden reducir la tasa de envío aunque se detecten las pérdidas. En este caso tampoco se pueden aplicar técnicas de retransmisión porque los paquetes serían descartados en el destino por llegar con retardo excesivo. Por este motivo en el caso de VoIP se utiliza el protocolo de transporte UDP en vez de TCP.

5.6 Elementos de una red VoIP .

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audioconferencia múltiple. (MCU Voz)
- Servicios de Directorio.

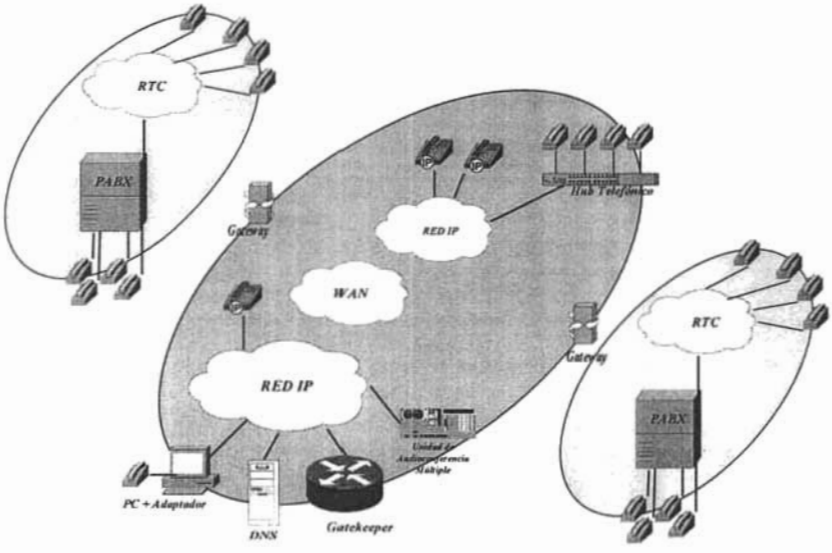


Fig. 5.20 Elementos de una red VoIP

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior (fig. 5.20), si bien merece la pena recalcar algunas ideas.

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de éste. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Podemos considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varios de los siguientes interfaces:

- FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
- FXS. Para conexión a enlaces de centralitas ó a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D)
- PRI. Acceso primario RDSI (30B+D)
- G703/G.704. (E&M digital) Conexión específica a centralitas a 2 Mbps.

Los distintos elementos pueden residir en plataformas físicas separadas, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos un Gatekeeper y Gateway. También podemos ver en la fig. 5.21 cómo Cisco ha implementado las funciones de Gateway en el router.

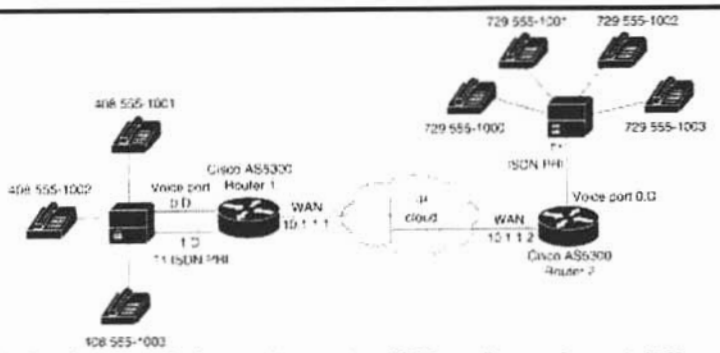


Fig. 5.21 Ejemplo de red con conexión de centralitas a routers CISCO que disponen de soporte VoIP.

Un aspecto importante a reseñar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es de más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP, cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un router. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar.

5.7 Calidad de Servicio QoS (Quality of Service).

En el mundo de las telecomunicaciones el recurso más caro es sin lugar a dudas el propio tráfico de datos. Según estudios recientes, los costos fijos destinados al alquiler de líneas de datos a los carriers suponen más del 75% de los costos en comunicaciones, por encima de los necesarios en personal y hardware.

En este escenario, el control del tipo de tráfico que se transmite y se recibe a través de la red de datos, se convierte en un problema económico muy importante.

En los últimos tiempos se ha dedicado gran esfuerzo a la diferenciación y priorización del tráfico de datos en función de su contenido, y al control del ancho de banda consumido por cada usuario o aplicación.

5.7.1 Calidad de servicio en aplicaciones.

Para poder brindar calidad de servicio en las aplicaciones, es necesario ofrecer soluciones que proporcionen un nivel de servicio óptimo para las necesidades del tráfico de su red:

Disponibilidad. Tener aplicaciones funcionando las 24 horas del día los 7 días a la semana es una necesidad cada vez más solicitada.
Respuesta. El usuario no sólo quiere disponibilidad. También es sensible al tiempo de espera en obtener respuesta a sus peticiones.

Además de estas dos características existen niveles de servicio (ver fig. 5.22) para referirse a las capacidades de punto a punto para proporcionar Calidad de Servicio o lo que significa la habilidad de la red para entregar los servicios requeridos a través de la red desde un punto a otro. Estos servicios se diferencían en sus niveles de calidad por como se pueden configurar diferentes características como ancho de banda, retardo, jitter y pérdida de paquetes, etc. .

Dentro de los tres niveles básicos de Calidad de Servicio de punta a punta y que pueden proporcionarse dentro de una red existen los siguientes:

- ***Servicio de Mejor Esfuerzo:*** también conocido sin Calidad de Servicio, ya que no garantiza la entrega de los paquetes hasta su destino.
- ***Servicios Diferenciados:*** también llamado como Calidad de Servicio suave, aquí uno de los tráficos es tratado mejor que los demás, entrega rápida, mayor ancho de banda en promedio, una tasa de pérdida menos, etc.
- ***Servicios Garantizados:*** también llamado Calidad de Servicio dura, en donde existe una absoluta reservación de recursos de la red para un tráfico en específico.

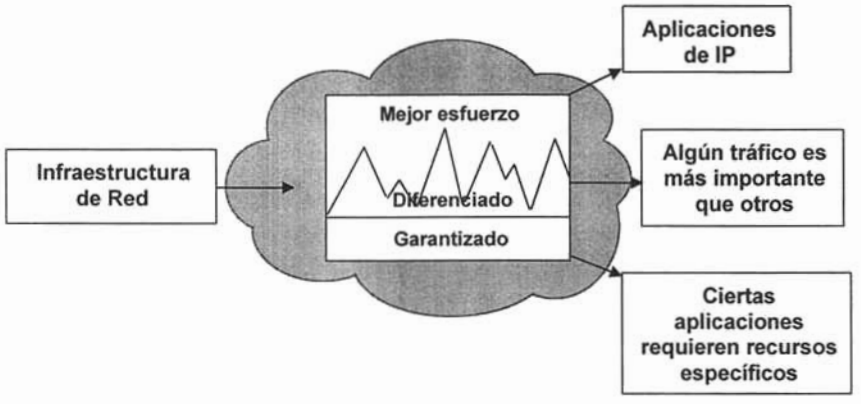


Fig. 5.22 Niveles de QoS.

En un ambiente de convergencia se integran voz, datos y video, y decimos integran porque dichos tipos de tráfico viajan a través de una misma infraestructura de transporte o de red, a pesar de que son procesados por la misma infraestructura, cada uno de ellos tienen diferentes características y por lo tanto requieren de diferentes recursos que proporciona la red para su correcto envío y entrega.

Se pueden mencionar algunas características y requerimientos básicos del tráfico de voz para su transporte dentro de la infraestructura de red multiservicios, como lo es su intolerancia a la pérdida de paquetes y a los retardos, dado que la presencia de ambos degrada la calidad de la transmisión y la entrega del servicio a los usuarios finales dando como resultado un mal servicio. En lo referente al retardo, éste debe ser constante y de extremo a extremo desde el punto donde se origina la llamada hasta el punto final de la misma, no debe de sobrepasar los 200 milisegundos (ms) para que sea satisfactoria para los usuarios.

Ahora se mencionará los requerimientos que la red debe proporcionar a los servicios de tráfico de voz:

- Proporcionar una política estricta de tráfico.
- El ancho de banda para la voz deberá ser reservado, lo mínimo.
- El tráfico de voz requiere de prioridad sobre los paquetes de datos.

5.7.2 Herramientas para QoS.

Para proporcionar un servicio de voz sobre la red de paquetes ya hemos mencionado los requerimientos de Calidad de Servicio para mantener los elementos de retardo y de latencia lo menor posible dentro de la red para mantener una calidad aceptable del servicio, pero no se ha hablado de las técnicas, salvo la de diferenciación de los paquetes dentro de la red, por lo que se hablará de las diferentes formas de manejar esta diferenciación dentro de los dispositivos.

5.7.2.1 Clasificación de tráfico.

Antes de que el tráfico sea manejado de acuerdo a sus requerimientos deberá ser etiquetado o identificado de alguna manera, por lo que existen varias formas de realizar esto incluyendo esquemas de capa 3 (Precedencia en IP o Servicios Diferenciados) y esquemas de capa 2 (protocolo 802.1P).

CAR (Commited Access Rate).

Una de las técnicas utilizadas por los enrutadores para la clasificación de paquetes es la tarifa comprometida de acceso (CAR), es una vieja técnica que implica un límite en la tasa de transferencia o el mantener el orden del tráfico en ciertos criterios. Esta técnica soporta la mayoría de los mecanismos de comparación y permite la clasificación de capa3.

En general, CAR es mayormente utilizado para paquetes de datos que para paquetes de voz. Por ejemplo, todo el tráfico de entrada de una interfaz ethernet o al menos 1 Mbs puede ser colocado dentro de una clase 3 dentro del esquema de precedencia de IP, y cualquier tráfico que exceda este Megabite puede clasificarse como 1 o ser tirado por el router. Otros nodos dentro de la red pueden entonces tratar de exceder o no conformarse con el tráfico marcado con una precedencia diferente. Todo el tráfico de voz podría conformar una tasa específica si ésta ha sido proporcionada correctamente

PBR (Policy-Based Routing).

Esta técnica también es utilizada para la clasificación del tráfico y permite al tráfico ser enrutado basado en el puerto origen o alguna lista de acceso, lo cual también puede ser usado para clasificar o marcar los paquetes.

5.7.2.2 Priorización de tráfico.

Dentro de los diferentes esquemas de priorización disponibles hoy día, los factores que se consideran, incluyen el tipo de tráfico que va a ser puesto dentro de la red y los enlaces WAN por los que vayan a atravesar. En lo referente al tráfico multiservicio sobre la WAN se recomiendan colas de baja latencia para enlaces de baja velocidad, lo cual permite especificar hasta 64 clases de tráfico, por ejemplo, colas de prioridad para voz y video interactivo, un mínimo de ancho de banda para SNA y colas de carga equitativa (WFQ weighted fair queuing) para otro tipo de tráfico. En la fig. 5.23 se señala un ejemplo:

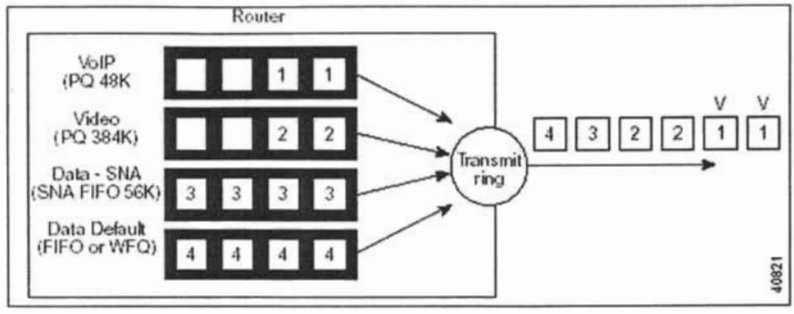


Fig. 5.23 Ejemplo de una preferencia de tráfico con valor 1 y que corresponden a paquetes de voz.

El tráfico de voz es puesto dentro una cola con prioridad de capacidades y es permitida en un ancho de banda de 48 kbps. El criterio de entrada a esta cola podría ser a través de la precedencia igual 5. El tráfico que exceda a 48 kbps debería ser tirado si la interfaz se congestiona. Más aún, un mecanismo de control de admisión deberá ser utilizado para asegurar que este valor no se exceda.

El video es puesto dentro de la cola de prioridad y es alojado con un ancho de banda 384 kbps, el criterio de entrada para esta cola podría ser la precedencia de IP con un valor de 4.

En tanto que el tráfico de SNA tiene un ancho de banda de 56 kbps. La operación de la cola dentro de esta clase de tráfico es del tipo donde el primero que entra es el primero que sale (FIFO) con un ancho de banda mínimo permitido de 56 kbps. El tráfico que exceda los 56 kbps será puesto en la cola de default.

Todo el tráfico restante puede ser puesto en la cola de default. La cual será despachada con un mecanismo FIFO a no ser que se especifique algún otro.

5.7.2.3 Técnicas de aprovechamiento del enlace.

Debido a que el ancho de banda es demasiado costoso, cuando se tiene un enlace WAN, solamente se cuenta con circuitos de baja velocidad cuando se necesitan conectarse sitios remotos y en estos casos es importante aprovechar al máximo el enlace tratando de enviar el máximo número de llamadas posible al mismo tiempo que se están transmitiendo datos de otro tipo sobre el mismo enlace.

CAPÍTULO SEIS

INTERCONEXIÓN ENTRE LOS NODOS UNAM-DGSCA Y LA UNIVERSIDAD A&M DE TEXAS (TAMU) A TRAVÉS DE INTERNET 2.

6.1 Introducción.

El proyecto de Voz sobre IP a través de Internet 2 apareció de manera formal en agosto del 2001 por medio de la invitación del workgroup de VoIP de Internet 2 a la UNAM, publicada en la página www.internet2.org/voip (ver Tabla 6.1) para la participación en la red internacional de pruebas de voz sobre IP, en conjunto con la Universidad A&M de Texas (TAMU), la cual es una de los principales universidades impulsoras del workgroup en conjunto con la Universidad de Indiana, éstas coordinan dicho grupo de trabajo. La motivación creció más ante el alcance y evolución del proyecto, manteniéndose vigente hasta el momento, tomándose de manera formal como tema de tesis por toda la gama de conocimientos que envuelve y por todo el futuro que se tiene dentro y fuera de la UNAM.

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 tested. 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.

Tabla 6.1 Invitación de participación en la Red de Pruebas VoIP.

6.1.1 Antecedente de VoIP en RedUNAM y problemática a resolver.

La implementación de tecnologías de VoIP en algunos de las diferentes institutos y facultades del campus universitario, comenzó en marzo del 2001 con la reestructuración de la Red en Rectoría, se implementó el primer sistema de voz sobre IP en RedUNAM, su principal objetivo es la de brindar comunicación en todo momento con los diferentes

colaboradores del Rector en turno de manera confiable, este proyecto se vió como una opción excelente para entablar de manera segura y privada las conversaciones de los distintos funcionarios, en base al recién terminado conflicto en la Universidad, y que dejó una palpable inseguridad en el sistema telefónico universitario, que daba pie a intervenciones telefónicas. Con la implementación de esta solución se creó una red privada alejada de la actual red telefónica y por lo tanto exclusiva, aunque en caso necesario, ésta es capaz de interactuar con la primera, así como inclusive hacer llamadas hacia la red telefónica de Teléfonos de México (TELMEX).

La solución de voz que se implantó y actualmente está en funcionamiento (ver fig. 6.1), es una solución de CISCO Systems llamada Media Convergens Server (MCS 7800) y en conjunto con software servidor de comunicaciones Cisco CallManager 3.0 instalado en MCS, dan pie a la realización de llamadas telefónicas IP.

6.1.1.1 Red Rectoría (Estructura de Telefonía IP).

Para la correcta implementación de la solución se tuvieron que seguir lineamientos para un correcto funcionamiento, estos puntos se siguen de manera similar en otras soluciones de voz diferentes a las de CISCO Systems, sólo varía la marca del sistema en esencia. En dicho proyecto se actualizaron diversos puntos que a continuación se observan:

- Actualización de los sistemas de acceso a red.
  - Switches Cisco Catalyst 6509 y 3524 (in-line power), que tiene la características de dar acceso a red y **alimentar** los diferente modelos de IP Phones, por medio del cable UTP que va del switch al IP Phone, sin la necesidad de un eliminador, estos siguen el estándar alimentación que permite la conexión de IP Phones y dispositivos que tengan esta ventaja.
- Actualización del hardaware de enrutamiento a Cisco Series 3600´s, 2600´s y 1700´s, para un mayor rendimiento, enrutamiento de los datos y dar redundancia a su enlace.
- Ampliación del ancho de banda en los enlaces WAN en la Red de Rectoría a enlaces E1 (2.048 Mbps).
- Ampliación del ancho de banda 1GB gracias a la conexión en Gigabit Ethernet con el backbone de RedUNAM, por medio de un enlace en fibra con uno de los switches Cisco con módulos en Gigabit Ethernet.
- Implementación de redundancia en su enlace.
- Cambio y reestructuración del cableado en Torre de Rectoría, en piso 6 y 12 respectivamente.
  - Instalación de cableado categoría 5e (100Base TX), para los distintos dispositivos.
  - Instalación de fibra óptica con módulos en Gigabit (1000 Base SX), que une los diferentes switches a la Red de Rectoría y que a su vez se une al backbone de RedUNAM.
- Instalación del sistema de VoIP para el grupo de funcionarios, tanto en Rectoría y dentro de todo el Campus de Ciudad Universitaria.

En la fig. 6.1 se presenta la red de datos y la red de VoIP instalada, en la cual se puede observar claramente la distribución de IP Phones sobre RedUNAM en el campus universitario de Ciudad Universitaria. Esta tecnología de telefonía IP está basada sobre la infraestructura de red AVVID (Architecture for Voice, Video and Integrated Data) de Cisco Systems.

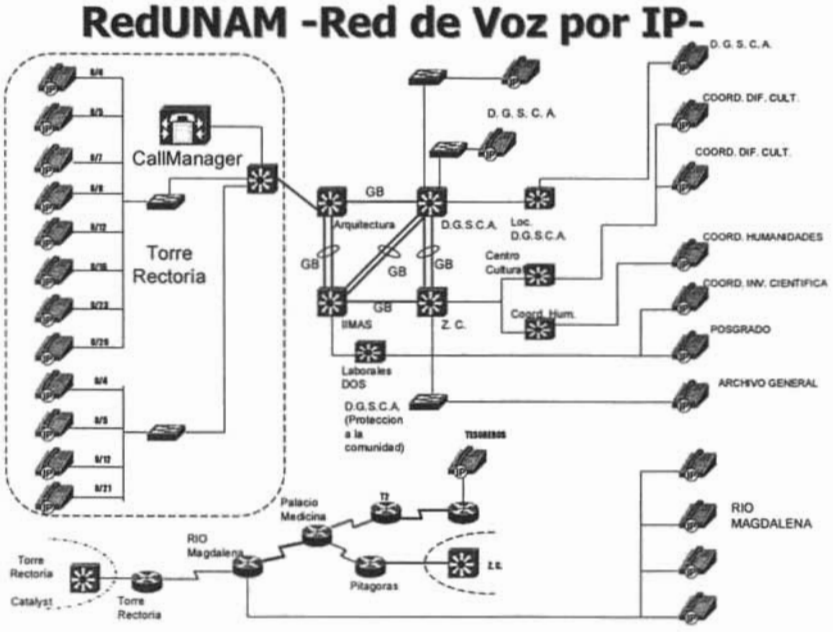


Fig. 6.1 Subred de Voz por IP para funcionarios.

El sistema de voz funciona gracias al servidor de comunicaciones de telefonía IP **Cisco CallManger** que se encuentra montado en el servidor MCS 7800, que da cabida a los diferentes servicios de señalización y control de las llamadas por medio del protocolo H.323, de ésta manera atendiendo a los diferentes Clientes de H.323 propios de CISCO y los llamados Terminales H.323 que son clientes de un tercero. El centro nervioso del sistema de telefonía IP es el Cisco CallManager, siendo éste un agente de llamadas, basado por un software. Cisco CallManager amplía los rasgos de telefonía en las empresas ofreciendo la capacidad para una red de dispositivos que pueden recibir y/o enviar datos hacia una red telefónica basada en paquetes, tales como IP phones, dispositivos multimedia, gateways de VoIP y aplicaciones multimedia. Servicios de datos, voz y video tales como mensajería unificada, conferencia multimedia, colaboración con centros de contacto, y respuesta con sistemas de respuesta interactiva con soluciones de telefonía IP a través de la telefonía con Cisco CallManager´s desarrollando programas de aplicación de interfase (API´s).

Los dispositivos para la solución de Telefonía IP de Cisco, abarcan tanto a teléfonos de escritorio (Cisco IP Phones 7960) y/o vía software, que es una aplicación que se monta dentro de la computadora (SoftPhones). Ambos tienen las mismas facilidades y funcionalidades que proveen la telefonía tradicional, y otros servicios que ofrece este tipo de solución, como lo es la habilidad para navegar en sitios WEB y servicio de directorio. Los teléfonos de escritorio tienen un switch integrado para su propia comunicación y otra para la interconectar a la PC (según el modelo), ésto para el caso de escasez de puntos de red.

Las aplicaciones de voz que están integradas dentro de la solución serían por ejemplo las aplicaciones de mensajería unificada, Contact Centers, IVRs (Interactive Voice Response), agregación automática conferencia, prioridad a emergencias, IP Phone

Messenger, Asistencia Personal, etc. Cada una de estas aplicaciones puede o no estar físicamente dentro de un equipo, la ubicación estaría lógicamente ubicada a través de la red, siendo de manera independiente al manejo y procesamiento de llamadas.

Es necesario mencionar la capacidad que hay en el sistema de Cisco en la interconexión del mismo con el sistema telefónico tradicional (TELMEX) y a su vez con los PBX´s que habilitaría la comunicación a las diferentes extensiones de la UNAM, para dicho propósito los routers Cisco series 3600, 2600 y 1700 tienen la capacidad de incorporar interfases digitales (E1s) y/o analógicas (FXS y FXO) que sirven de gateways; importante mencionar que la interconexión es factible y ha sido probada.

6.2 Análisis de Red UNAM para soporte de VoIP.

La Universidad Nacional Autónoma de México se ha caracterizado, a lo largo de toda su historia, por estar a la vanguardia en la investigación, enseñanza y sobre todo tecnología; por lo que la red de telecomunicaciones con que actualmente cuenta no escapa de esta perspectiva; al tomar en cuenta todos estos puntos, se expone el presente análisis para la viabilidad del presente proyecto.

La RedUNAM es un proyecto que se desarrolló para la transmisión de información entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la UNAM. Actualmente RedUNAM cuenta con más de 25,000 computadoras conectadas a la red de datos, más de 424 líneas del sistema telefónico digital que atienden a cerca de 12,000 cuentas de Dial-Up y 4 enlaces, sumando una capacidad de transmisión de más de 104 Mbps, para la conexión a Internet con diferentes proveedores de servicio.

La red ha ido evolucionando. Desde el año de 1987, la UNAM establece la primera conexión de la Red Académica de cómputo de aquel entonces con la Red BITNET mediante enlaces telefónicos desde Ciudad Universitaria hasta el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) y de ahí hasta San Antonio, Texas en los E.U.A. Dicha conexión consistía en una computadora IBM 4381 para manejo de correo electrónico.

Para 1989, a través del Instituto de Astronomía se establece un convenio para enlazar a la red académica de la UNAM con la red de la NFS en EUA. El enlace se realizó mediante el satélite mexicano Morelos II que conectaba al Instituto de Astronomía en la UNAM y al UCAR-NCAR con residencia en Boulder Colorado. La finalidad del proyecto estaba enfocada a la investigación de fenómenos astrales. A la par se llevó a cabo el primer enlace para conectar las redes de área local del Instituto de Astronomía y la Dirección General de Servicios de Cómputo Académico (DGSCA) utilizando enlaces de fibra óptica. A partir de ese momento se inició dentro de la UNAM una revolución en las comunicaciones.

Acciones como la adquisición masiva de computadoras personales, su conexión a red y la intercomunicación de redes de área local (principalmente en las dependencias de investigación científica) permitió desarrollar la infraestructura de comunicaciones de fibra óptica actual de RedUNAM, establecer más enlaces satelitales hacia Cuernavaca, Morelos, y San Pedro Mártir en Ensenada, Baja California Norte, también el primer enlace de microondas de alta velocidad sobre la Ciudad de México entre la Torre II de Humanidades y la Dirección General de Servicios de Cómputo Académico (DGSCA).

Para el año de 1990 la UNAM fue la primera institución en Latinoamérica que se incorpora a la red mundial Internet, que enlaza a millones de máquinas y decenas de millones de usuarios en todo el mundo. Su continuo desarrollo contempla como elemento

fundamental el diseño de una arquitectura que permita la comunicación de redes de diferentes arquitecturas trabajando bajo el protocolo TCP/IP mismo que se mantiene como estándar en la actualidad dada su funcionalidad y posibilidad de adaptación a los requerimientos que se van presentando.

La operación de la Red Integral de Telecomunicaciones con una plataforma de backbone basada en la tecnología ATM se inició en la primera semana del mes de agosto de 1997. En esa fecha solo se enviaba tráfico de datos. Para la segunda quincena del mes de octubre de 1999 se incorpora el tráfico de voz y videoconferencia. Este esquema, basado en ATM, funcionó hasta el mes de agosto del año 2002.

Desde finales del año 2001 se inició el proceso de revaloración de la tecnología que se estaba utilizando dentro del backbone, ya que si bien no era totalmente obsoleta, sí tenía limitantes en cuanto a proporcionar los nuevos servicios que los usuarios estaban demandando. Se determinó que la mejor tecnología de transporte para la RedUNAM es la de Gigabit Ethernet.

Se realizaron procesos de licitación, invitando a diversos fabricantes de equipo, de planeación de pruebas y de maquetas, finalmente se efectuó el proceso de migración que terminó en el mes de agosto del año 2002, cuando la totalidad de los switches ATM fueron apagados y retirados del backbone, quedando en funcionamiento un backbone con velocidades de 1Gbps mínimo dentro del Campus Universitario.

Con esta tecnología se tiene planeada la implementación de aplicaciones que requieren tanto ancho de banda, como una pérdida nula de paquetes, esto es aplicaciones en tiempo real:

- Voz sobre IP.
- Video por H.323 .
- Transmisiones Multicast.
- Telemedicina.
- Educación a distancia.
- Bibliotecas digitales.

Además de continuar con los servicios que actualmente se llevan a cabo y que históricamente han funcionado dentro de la red: correo electrónico, transferencia de archivos, páginas Web, etc.

Esto sólo es una muestra de las aplicaciones que poco a poco se estarán implementando a nivel de toda la RedUNAM, teniendo como premisa que ésta es una red multiservicio.

Descripción general de RedUNAM.

La RedUNAM es una red de computadoras LAN dentro de las dependencias e institutos; CAN entre las diversas Facultades e Institutos que se encuentran dentro de Ciudad Universitaria; MAN con las conexiones a las ENEPs, FESes, Preparatorias, CCHs y demás centros dentro del área metropolitana; WAN en las conexiones con instituciones externas (instituciones públicas y privadas) ubicados dentro de la República Mexicana y enlaces con otros ISP´s para proporcionar conectividad a nivel internacional.

Para lograr esta conectividad y extensión geográfica se utilizan diversas tecnologías para los diferentes tipos de conexiones que se tienen:

- LAN: Ethernet, Fast Ethernet.
- CAN: Fast Ethernet, Gigabit Ethernet.
- MAN: enlaces dedicados TDM, microondas.
- WAN: enlaces dedicados TDM, ATM, Frame Relay y satelitales.

Los cuales son la infraestructura tecnológica para proporcionar los servicios de conectividad y transporte, soportando los servicios proporcionados con la ayuda de la suite de protocolos TCP/IP.

Para entender cómo es que trabaja esta red multiservicio se describirán las diferentes capas con que cuenta y los elementos que cada una de estas capas utilizan para su funcionamiento, así como la relación que existe entre cada una de ellas para llevar a cabo una comunicación integral.

Descripción de la RedUNAM: Nivel de transporte.

La infraestructura con que cuenta la RedUNAM está dividida en forma jerárquica, en tres divisiones para su mejor administración y un mejor diseño; estas tres secciones son:

- *Capa de Backbone, core o espina dorsal;*
- *Capa de distribución y*
- *Capa de acceso.*

Que además de ayudar a tener un mejor desempeño de la propia red, sirve para poder detectar, aislar y resolver cualquier problema que se pueda presentar en ella teniendo un impacto menor a la mayor cantidad de usuarios posibles.

Capa de Backbone o Dorsal.

Se maneja un backbone o dorsal con tecnología Gigabit Ethernet entre los cuatro nodos principales: DGSCA, IIMAS, Arquitectura y Zona Cultural.

Las ventajas que obtenemos con esta tecnología dentro de la dorsal es un mayor ancho de banda que lo que se tenía con ATM, de sólo 155 Mbps ahora a 1Gbps; además, y muy importante, la sustitución del esquema de funcionamiento con LAN Emulation que se tenía con la anterior arquitectura de red y que contribuía a un mayor retardo en los tiempos de comunicación ya que el proceso de conversión de celdas a tramas aumentaba este retardo, que tal vez en datos no se observaba mucho, pero en las comunicaciones de voz y video a través de H.323 sí se apreciaban provocando pérdida de paquetes, retardo, cuadriculamiento de imágenes y pérdida de sonido.

Otro factor es que se elimina el dominio de broadcast tan grande que existía dentro de dicha dorsal ya que dentro de un mismo segmento lógico existían demasiados dispositivos lo que contribuía a mayor tráfico y, por lo tanto, congestión.

Dentro del diseño se ha pensado en la redundancia que pueda existir entre los nodos de la red (fig. 6.2). Se tiene un respaldo entre los dispositivos que manejarán Gigabit Ethernet, pero no sólo eso, sino también se mantendrá la conexión hacia los switches ATM como una doble redundancia y con esto mantener al 100% la disponibilidad de la RedUNAM.

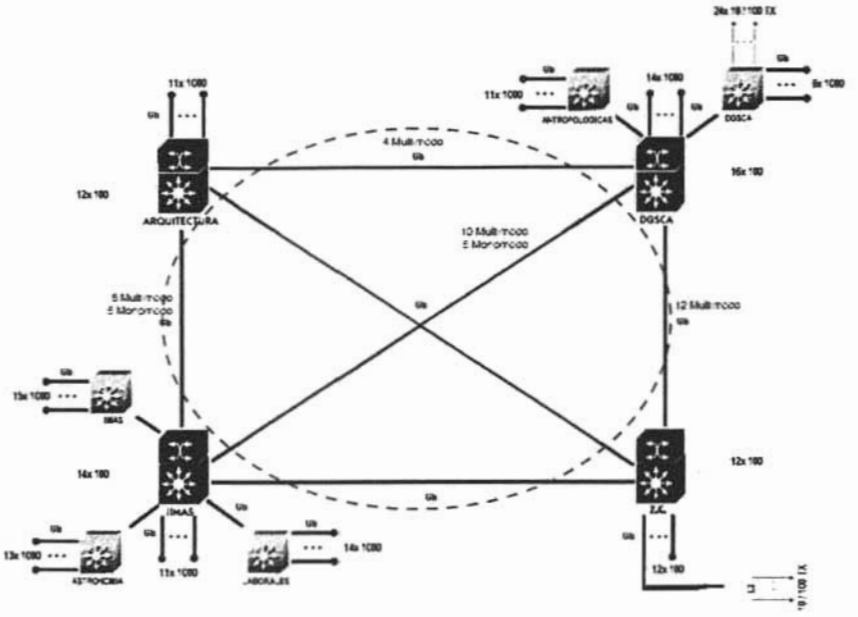


Fig. 6.2 Redundancia de Nodos.

Otra ventaja que tenemos con esta dorsal es que podemos realizar trunking, que es realizar conexiones en paralelo y balancear el tráfico entre estos enlaces, provocando que el ancho de banda se duplique o hasta se multiplique por 6, esto es que si se tuvieran instaladas las fibras ópticas se lograrían alcanzar velocidades de hasta 6Gbps entre cada uno de los 4 nodos principales.

Capa de Distribución.

Actualmente los costos en la adquisición de una tecnología Gigabit Ethernet no son tan altos, como al inicio de su desarrollo, por lo que en algunos casos se ha seleccionado esta tecnología para la conexión entre los dispositivos de backbone y los de distribución, que a su vez aglomeran las conexiones de la capa de acceso provenientes de los diferentes Institutos, Facultades, etc., existentes en el campus de Ciudad Universitaria. Estas conexiones hacia la capa de acceso varían en ancho de banda de 100 Mbps hasta 1 Gbps.

Esta capa de distribución se encargará de sustituir a los switches de capa 2 y 3 que se tienen actualmente funcionando (fig. 6.3), y que poco a poco están migrando, ya que lo que se diseñó es que las dependencias se conecten directamente a este switch de distribución para que él se encargue de comunicar a las dependencias que estén bajo su responsabilidad y que al backbone solamente pase el tráfico que tenga que llegar a algún nodo de dorsal e incluso que tenga que salir hacia la Internet, esto es fuera de la RedUNAM, vía los ISP´s con los que se tiene conexión.

El que una dependencia, dentro de Ciudad Universitaria, tenga una conexión en Gigabit Ethernet desde el nodo de distribución hasta el switch principal de dicha dependencia, depende del equipo que pueda adquirir, esto es que cambie el switch con que actualmente está conectándose, ya sea porque dicho dispositivo no soporte una tarjeta con puertos Gigabit Ethernet, o que el dispositivo no soporte características para

implementar diferenciación de tráfico utilizando el estándar 802.1q, o incluso capacidades de capa 3 como lo serían ruteo con protocolos estándar RIP, OSPF, IS-IS.

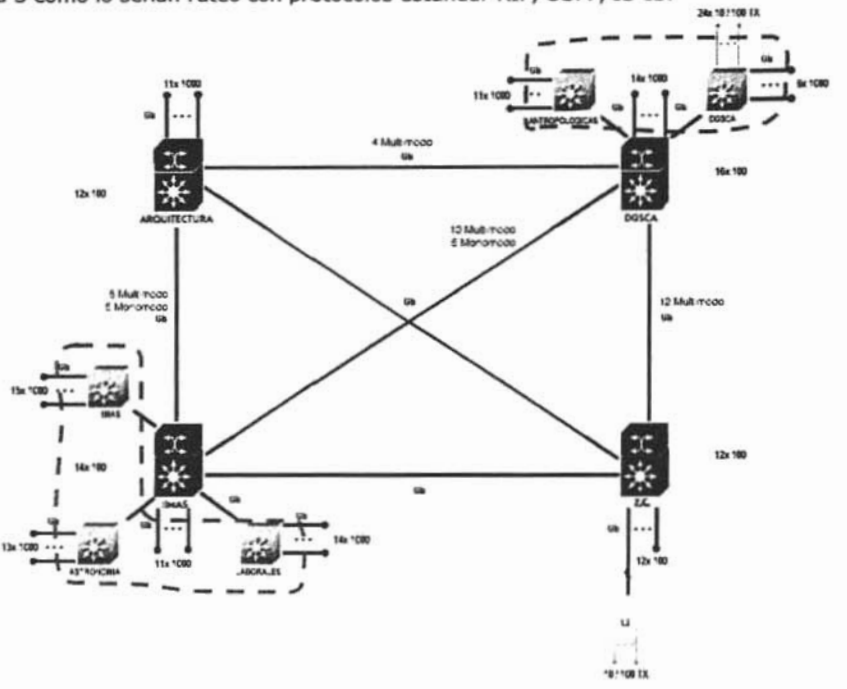


Fig. 6.3 Ejemplo de la capa de distribución en C.U.

Capa de Acceso.

En la capa de acceso se tiene definido que las dependencias, Institutos o Facultades que así lo deseen y justifiquen podrán tener una velocidad de acceso hasta de 1Gbps hacia los equipos de distribución (fig. 6.5).

Esta no es la única opción que se tiene hacia la capa de acceso sino también pueden continuar manejándose los anchos de banda que se habían manejando tradicionalmente de 10 y 100Mbps con tecnología Ethernet y FastEthernet respectivamente.

Los dispositivos de acceso deben ser switches capa 2, o incluso capa 3, esto dependerá del diseño que tenga cada una de las dependencias, así como del presupuesto que tengan a su disposición. Es recomendable que en esta capa se utilicen switches capa 2 o capa 3 para la mejor segmentación del tráfico y proporcionalmente un mejor funcionamiento de su red interna además que con ello dependerá la factibilidad o no de VoIP ya que es necesaria una red "switcheada" para su correcto funcionamiento.

Además de estos dispositivos de interconexión, casi todos los equipos de cómputo de las dependencias de la UNAM poseen tarjetas de red con tecnología Ethernet o FastEthernet, de modo que éstos al conectarse a RedUNAM hacen uso de esta tecnología (capa de acceso). La capa de acceso también se refiere a la interfaz final hacia el usuario.

Funcionamiento y Equipamiento.

Ahora que se ha dado la idea general de la estructura de transporte, se procede a describir el funcionamiento de RedUNAM de acuerdo a los equipos que la integran y a las funciones que realizan dentro de cada una de las capas (backbone, distribución, acceso). Los principales equipos son:

- *Switches Capa 2 y 3, BigIron y NetIron (backbone, distribución).*
- *LANplex (distribución y acceso).*
- *Ruteadores Capa 3 Cisco (equipos de orilla, conexión WAN y salidas a Internet).*
- *Passport 6400 (backbone).*

Switches capa 3, BigIron y NetIron 8000 (Dorsal y distribución).

Estos equipos son switches con capacidades de ruteo en capa 3 por lo que se utilizarán dentro de la dorsal dentro de la arquitectura de OSPF, lo que permitirá que todas las áreas se puedan comunicar entre sí y encaminar los paquetes de voz que provengan de RedUNAM o de otra entidad perteneciente a Internet 2.

Switches LAN LANplex 2500 (Capa de Acceso).

En la capa de acceso a RedUNAM, la mayor parte de los institutos, facultades y dependencias de la UNAM se conectan a través de uno o varios segmentos de red Ethernet, dependiendo del número de equipos terminales (PC's, impresoras, etc.) que posea dicha dependencia.

Estos segmentos de red se encuentran conectados a través de un switch LAN, algunos con capacidades de enrutamiento, modelo LANplex 2500 de la marca 3Com. Dicho equipo cuenta con una interfase de Fast Ethernet para llevar a cabo la capa de distribución de las dependencias y comunicarlas hacia el backbone.

Para dar un ejemplo de la capa de acceso, en la siguiente fig. 6.4 se observa que toda dependencia se conecta a través de un hub o switch a un puerto Ethernet en el LANplex 2500. Este puerto puede ser de fibra óptica o UTP dependiendo de la distancia geográfica entre el LANplex y la dependencia. Por otra parte, de la capa de acceso a la capa de distribución, o incluso el backbone, se realiza a través de un puerto Fast Ethernet, esto porque las capacidades de este equipo no soportan comunicaciones de 1Gbps. En este caso sería necesario switches para establecer llamadas por IP ya que el rendimiento baja demasiado en equipos Hub.

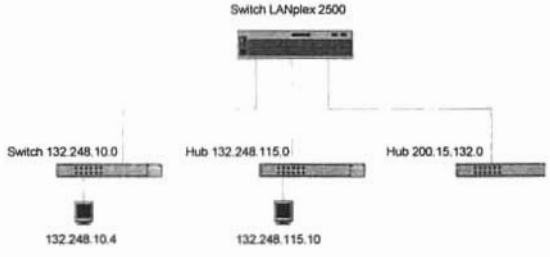


Fig. 6.4 Ejemplo de Capa de Acceso.

En conjunto, los 21 LANplex con que cuenta la Universidad (conectados a los equipos BigIRon y NetIron), cuentan en promedio con 5 segmentos de red Ethernet (5 dependencias) para dar servicio a un total de 99 dependencias. Estos equipos están

repartidos dentro de los cuatro nodos de telecomunicaciones de la UNAM (ver fig. 6.5) como sigue:

- Nodo DGSCA con 6 LANplex.
- Nodo Zona Cultural con 3 LANplex.
- Nodo IIMAS con 6 LANplex.
- Nodo Arquitectura con 6 LANplex.

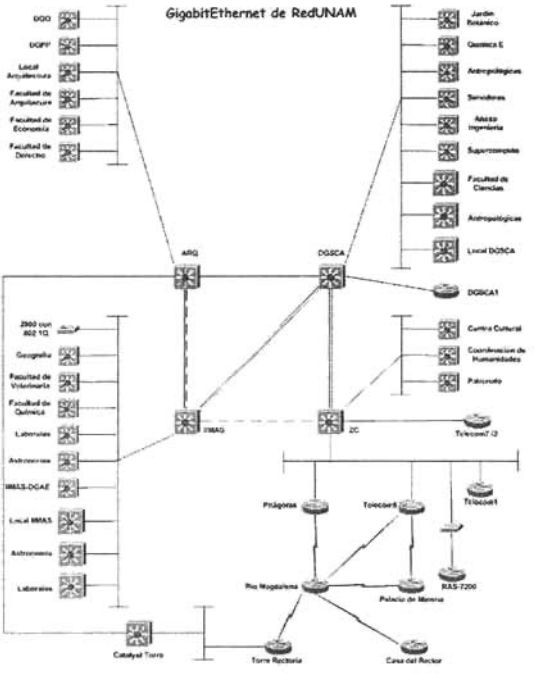


Fig. 6.5 Equipos de Core y Distribución de RedUNAM.

Las interfases de conexión entre los LANplex y los BigIron son a través de tecnología Fast Ethernet (Ver Fig. 6.5) con la finalidad de brindar una distribución de la información de todas las dependencias conectadas al LANplex con un ancho de banda adecuado. La interfase Fast Ethernet que conecta al LANplex 2500, con el BigIron se configura a la VLAN de administración por lo que todos los LANplex pertenecen a la misma red o lo que es lo mismo, la comunicación que establecen entre ellos es de punto a punto con la finalidad de establecer un óptimo enrutamiento de información entre las dependencias.

Con este esquema todas estas dependencias requieren establecer comunicación con las demás e inclusive con el resto de Internet, por lo que es necesario implantar servicios de enrutamiento de datos a través de TCP/IP desde el nivel de la capa de distribución y por supuesto en la dorsal.

Ruteadores.

Los dispositivos con que la RedUNAM dispone para llevar a cabo las conexiones WAN, ya sea con CCH's, ENP's, ENEP's, Institutos o cualquier otra dependencia UNAM, así

como a clientes externos, hospitales, escuelas, iniciativa privada; y por supuesto los enlaces con otros proveedores de servicio, en este caso Avantel, Uninet y Teleglobe, son los ruteadores.

Estos ruteadores son dispositivos multiprotocolo, de gran capacidad de procesamiento y memoria para soportar la gran carga de tráfico que por ellos pasa, ya que toda la información que se solicita de Internet y la que la propia UNAM genera, tiene forzosamente que pasar por alguno de los ruteadores de orilla con los que cuenta RedUNAM.

A pesar que existen solamente 3 ruteadores principales (ver fig. 6.6), éstos son lo suficientemente robustos para conectar cerca de 130 enlaces WAN de diversos anchos de banda, desde 64 kbps hasta 155Mbps.

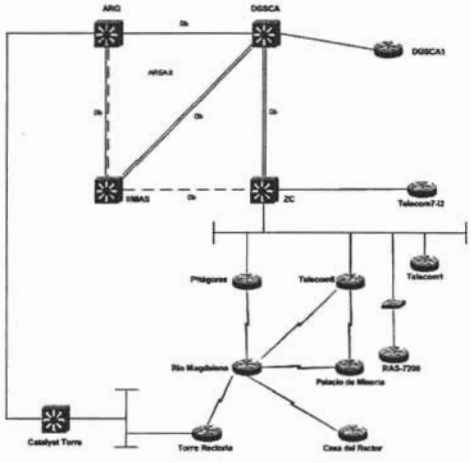


Fig. 6.6 Ruteadores WAN y de enlace a ISP's.

Estos equipos, no solamente cumplen con la funcionalidad de conectividad LAN-WAN, esto es, conectar a RedUNAM hacia el mundo (fig. 6.6) por medio de Internet e Internet 2, sino también cumplen una de las tareas más importantes dentro de las redes de datos que es buscar el mejor camino hacia un destino, consultando sus tablas de ruteo y con ellas comparan el destino de cada uno de los paquetes con los destinos que ellos pueden alcanzar habilitando el transporte de paquetes de voz a cualquier destino. A esta actividad lo llamamos enrutamiento.

Nivel de enrutamiento

En el ámbito de enrutamiento, la RedUNAM cuenta con un conjunto de redes de instituciones externas e internas, además de las conexiones a Internet. Actualmente la UNAM cuenta con 84 enlaces hacia instituciones externas, 71 enlaces a instituciones internas, además de 4 enlaces hacia otros proveedores de servicio (2 STM-1's) para brindar un ancho de banda de 180 Mbps aproximadamente de salida a Internet (ver fig. 6.6).

RedUNAM trabaja con protocolos de enrutamiento que hacen uso de la tecnología TCP/IP, y es necesario hablar acerca de la asignación de las subredes IP dentro de la RedUNAM.

Todas las conexiones entre dispositivos del backbone, distribución y acceso, además de las redes Ethernet de las diferentes dependencias tienen asignado un segmento de red para proveer el enrutamiento de información de TCP/IP entre ellas. Otra finalidad es la de reducir los dominios de broadcast dentro de la RedUNAM. Para llevar a cabo esta asignación, la RedUNAM cuenta actualmente con varios bloques de direcciones IP:

- 2 bloques de direcciones clase B: 132.248.0.0/16 y 132.247.0.0/16,
- 3 bloques de direcciones clase C: 200.15.1.0, 192.100.199.0 y 192.100.200.0.

La RedUNAM para fines de administración y enrutamiento, en la conexión entre los dispositivos de interconexión de backbone, distribución y acceso, tiene asignada toda la subred 132.248.255.0 con máscara de 255.255.255.252, con lo que podemos obtener 62 subredes para la interconexión entre dichos dispositivos, además que dentro de ella se encuentran todos los equipos encargados del enrutamiento.

La estructura general de enrutamiento de la RedUNAM es un sistema jerárquico dividido en diferentes áreas para su mejor funcionamiento y administración. Con esta división evitamos que la carga producida por los anuncios de las tablas de ruteo sature el procesamiento de los dispositivos de la dorsal y de los enrutadores de orilla.

En este enrutamiento todos los equipos con función de enrutamiento son peers o vecinos, es decir, se encuentran en un mismo dominio de broadcast.

Como se puede observar, las dependencias internas se encuentran conectadas en los puertos de los equipos LANplex 2500 o al BigIron o NetIron que cuenten con algún switch que soporte la conexión a velocidades de GigabitEthernet. El enrutamiento de información entre las diferentes dependencias puede ser de distintos tipos:

- Dependencias conectadas en un mismo LANplex.
- Dependencias conectadas en los Switches de dorsal o en distribución.
- Dependencias conectadas en los Cisco.

Existen 22 dependencias internas de RedUNAM que se encuentran directamente conectadas a los puertos Fast Ethernet de los equipos de la dorsal y distribución, BigIron y NetIron.

Para la conexión y comunicación hacia fuera de la RedUNAM se hace necesario contar con un equipo que brinde la capacidad de enrutamiento de paquetes a través de TCP/IP. Este mismo equipo funge como default gateway o puerta de default, para el switch de core ubicado en zona cultural, ya que este switch es el que tiene conexiones con los 3 enrutadores principales de RedUNAM y que fungen como enrutadores de borde hacia nuestros proveedores de servicio y consecuentemente hacia Internet.

Los enrutadores son de marca Cisco e integran el backbone de enrutamiento de RedUNAM como se muestra en la fig. 6.7.

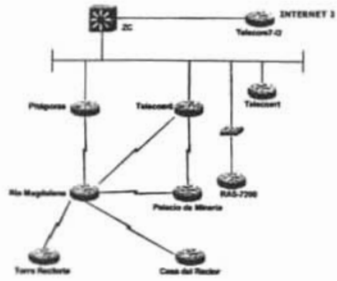


Fig. 6.7 Backbone de enrutamiento de RedUNAM.

Los encaminadores de RedUNAM permiten comunicar a los segmentos de diferentes Dependencias internas y externas e Institutos de la UNAM entre sí, es decir, segmentos que se encuentran conectados a los diferentes equipos BigIron, NEtIron, LANplex y Cisco, y a su vez con el resto del mundo con conexiones internacionales a Internet. La forma en que estos equipos llevan a cabo el enrutamiento de información es a través del intercambio de información de enrutamiento con el fin de que todos los enrutadores pertenecientes al Sistema Autónomo de la UNAM (AS278) tengan las rutas para poder llegar a cualquier otra red, sea dentro o fuera de la UNAM.

Los enrutadores Cisco tienen configurado dos tipos de enrutamiento: estático y dinámico. Esta configuración se debe a las diversas necesidades que se presentan en RedUNAM debido a la gran extensión geográfica, complejidad y diversidad de equipos que existen dentro de ésta trabajando con el protocolo interno OSPF y el protocolo externo BGP.

Protocolo OSPF.

Dentro de las características que envuelven al protocolo OSPF (Open Shortest Path First) están las siguientes:

- Protocolo de compuerta interna (IGP).
- Utiliza anuncio del estado de sus enlaces para construir su tabla de ruteo.
- Protocolo que es utilizado en redes diseñadas jerárquicamente (niveles de acceso, distribución y dorsal).
- Requiere de grandes cantidades de memoria para su procesamiento en cada uno de los enrutadores que lo utilicen.
- Poco tiempo para llevar a cabo la convergencia o conocimiento de la tabla de ruteo, lo que evita problemas de funcionamiento en la red.

A diferencia de un protocolo como RIP se tiene un menor tiempo de recuperación de anuncios de redes, esto es, un menor tiempo de convergencia, lo que da como resultado que el envío de la información sea mucho más rápido y que el tiempo de interrupciones sea mínimo o nulo.

También por la complejidad y extensión que tiene la RedUNAM requiere de un protocolo robusto y confiable para soportar la cantidad de mensajes de actualización de rutas, así como de control del mismo protocolo para proporcionar servicios multimedia y de tiempo real.

Ahora veamos cómo es que este protocolo está implementado dentro de los dispositivos de los switches y dispositivos de capa 3 con que cuenta la dorsal de la

RedUNAM, así como en los enrutadores de orilla que proporcionan la conexión de la UNAM con la Internet.

El backbone de RedUNAM está configurado por varias áreas de ruteo (ver fig. 6.8), seis áreas principales, además de dejar reservados dos identificadores de red para un futuro.

Esto es, la red está dividida en cuatro nodos principales, los cuales proporcionan el servicio de red a toda la UNAM, tanto dentro del campus de Ciudad Universitaria como los que se encuentran fuera de ella:

Nodo DGSCA:
- CUAED,
- Escuela Nacional de Trabajo Social,
- Facultad de Administración y Contaduría,
- Facultad de Ciencias,
- Anexo de Ingeniería.

Nodo Arquitectura:
- Rectoría,
- Facultad de Arquitectura,
- Proveeduría,
- Facultad de Psicología,
- Facultad de Filosofía,
- Facultad de Derecho.

Nodo IIMAS:
- Institutos de Investigación,
- Facultad de Química,
- Facultad de Veterinaria,
- Facultad de Economía,
- Facultad de Ingeniería.

Nodo Zona Cultural:
- Centro Cultural,
- Institutos de Investigación,
- Universum,
- Centro de Registro.

Las cuatro primeras áreas están destinadas para agrupar a los equipos que brindan servicio para redes LAN dentro del campus universitario y las dos restantes para los equipos que brinden servicio a dependencias fuera del campus así como instituciones externas, esto es en la WAN.

A continuación presentamos en la fig. 6.8 la distribución de los dispositivos de red conforme al área a la que pertenecen dentro del funcionamiento del protocolo OSPF:

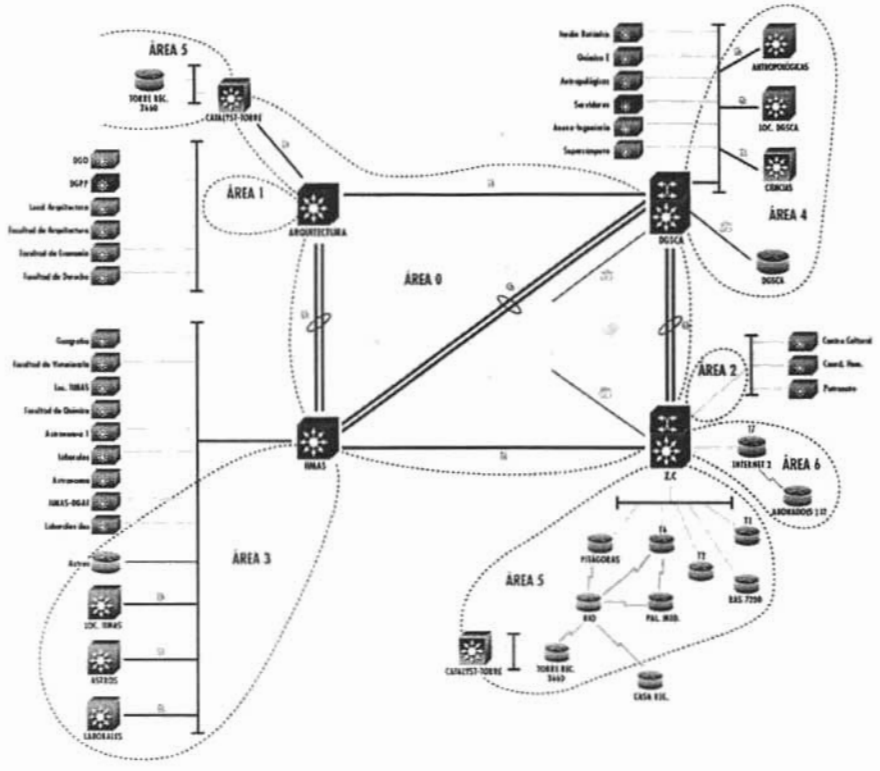


Fig. 6.8 Áreas OSPF.

Donde:

- El Área 0 está asignada para los equipos del Backbone en GigabitEthernet.
- El Área 1 está reservada para los equipos del nodo principal Arquitectura.
- El Área 2 está reservada para los equipos del nodo principal Zona Cultural.
- El Área 3 está asignada a los equipos del nodo principal IIMAS.
- El Área 4 está asignada a los equipos del nodo principal DGSCA.
- El Área 5 está asignada a los enrutadores con enlaces WAN hacia los ISP´s de la UNAM, dependencias fuera del campus, instituciones externas y la Red de Rectoría.
- El Área 6 está asignada a los enrutadores que conforman la red de Internet 2 de la UNAM así como de los que enrutadores se conectan a Internet 2 a través de la UNAM.

Los equipos de acceso, switches de la marca 3Com (Lanplex 2500 y CoreBuilder 3500), no son incluidos dentro de las áreas de OSPF, esto es, no tienen encendido el protocolo OSPF para el intercambio de tablas de ruteo con los equipos Foundry o Ciscos, ya que no son lo suficientemente robustos para ello. A pesar de esto los equipos están conectados a la RedUNAM, ya sea a un switch de la dorsal o a uno de distribución, ya que muchas de las dependencias que están recibiendo el servicio de red, lo hacen a través de estos dispositivos, y no están preparadas ni en diseño ni en infraestructura como para conectarse a un dispositivo de distribución o dorsal a una velocidad de 1Gbps. Poco a

poco estos dispositivos 3Com, estarán siendo migrados para que todas las dependencias estén recibiendo los beneficios de la nueva dorsal.

Para simplificar la administración y brindar mayor estabilidad al proceso de ruteo OSPF, en cada área se tomará la cantidad necesaria de direcciones comenzando por la IP más alta de la subred asignada, para configurarse en la primer interfase de loopback de cada equipo, con una máscara de 32 bits, forzando así a que dicha IP se tome como el RouterID.

Protocolo BGP.

Aunque tenemos configurado lo necesario para llegar a cualquier red conectada directamente a RedUNAM a través del enrutamiento estático y el protocolo OSPF, se hace necesario configurar en los enrutadores un protocolo de compuerta externa que permita comunicar el Sistema Autónomo de la UNAM con otros para que todas las redes de RedUNAM y las redes de las instituciones que dependen de ella sean anunciadas al resto del mundo. Este se hace a través del protocolo estándar BGP (Border Gateway Protocolo).

Existen dos modalidades en la implementación de BGP: iBGP y eBGP.

- Los enrutadores que pertenecen al mismo Sistema Autónomo de la UNAM e intercambian información de BGP, están hablando BGP interno (iBGP).

- Enrutadores que pertenecen a un diferente Sistema Autónomo de la UNAM e intercambian información de BGP, lo hacen a través de BGP externo (eBGP).

Antes de intercambiar información de enrutamiento con un Sistema Autónomo externo, BGP se asegura que todas las redes dentro de su Sistema Autónomo sean alcanzables, por lo que se hace necesario:

- Tener una configuración centralizada a través de un Router Reflector (conexión de uno contra todos) entre los enrutadores que hablan iBGP dentro del Sistema Autónomo a través de IGPs.

- Redistribuir rutas de IGP a BGP (y viceversa) del Sistema Autónomo, es decir, RIP e IGRP a BGP para el caso de RedUNAM.

Una vez que todas las redes internas de RedUNAM son conocidas por los enrutadores que tienen configurado el proceso de iBGP, se utiliza eBGP para anunciarlas a su(s) vecino(s) externo(s), equipos pertenecientes a otros ISP´s, ya que no es necesario que a todos los clientes de la RedUNAM se les propaguen estos anuncios. De esta forma todas las redes que dependen de RedUNAM son anunciadas al resto del mundo. Un proceso similar realizan los demás Sistemas Autónomos de toda Internet.

Es por lo anterior que BGP solamente está configurado en aquellos enrutadores que tienen enlaces con instituciones externas que pertenezcan a un Sistema Autónomo diferente al de la UNAM.

En la fig. 6.5 se puede observar que tres de los enrutadores de backbone tienen conexión hacia Internet, por lo tanto, cada uno de ellos tienen configurado eBGP para con sus vecinos de otros Sistemas Autónomos fuera de la UNAM e iBGP para con sus vecinos internos. En RedUNAM los enrutadores configurados con iBGP y eBGP son tres: dos enrutadores de ZC y uno más en Pitágoras.

Los encaminadores que tienen conectadas las salidas internacionales de RedUNAM mencionados en el párrafo anterior poseen una configuración más robusta, es por ello que éstos equipos necesitan ser de mayores capacidades de hardware con respecto a los otros enrutadores del backbone debido a que manejan información de enrutamiento tanto de protocolos IGPs y EGPs como de la redistribución que esto implica.

Este análisis de RedUNAM da como resultado la factibilidad de la implementación de tecnologías de Voz sobre IP a través del la red de datos en Ciudad Universitaria; para los campus y dependencias que se encuentran en el área metropolitana y en otras partes de la República sería necesario incrementar su ancho de banda y cambiar algunos de sus equipos de acceso para lograr este objetivo.

6.3 Análisis de la Red Telefónica de la UNAM.

Este análisis se lleva a acabo ya que el proyecto abarca la integración de los diferentes conmutadores telefónicos de la UNAM como parte del proyecto para una solución mucho más completa, comportándose como un todo, ya que no es factible la eliminación de los conmutadores telefónicos instalados en la UNAM y sustituirse por conmutadores IP, puesto que no se cuenta con los recursos necesarios y esta migración será gradual.

Actualmente la RedUNAM cuenta con una infraestructura de telecomunicaciones comprendida por las redes de datos, videoconferencia y telefonía.

De estas tres infraestructuras una de las que proporciona sus servicios a una mayor cobertura de universitarios es la de red de telefonía.

Esta red telefónica ha tenido un desarrollo con un crecimiento sostenido y constante durante los últimos 13 años, período en el cual se han probado, adquirido, configurado e instalado diversos conmutadores de grandes capacidades dentro del campus de Ciudad Universitaria, e incluso en los campus de la Cd. de México, Área Metropolitana e interior de la República.

En estos momentos la red telefónica está integrada por 40 conmutadores (PBX) de la marca NEC, distribuidos de la siguiente manera:

- **24 dentro de Ciudad Universitaria.**
    - Arquitectura
        - Facultad de Economía
        - Dirección General de Personal
        - Facultad de Ingeniería
        - Dirección General de Obras
        - Rectoría
    - IIMAS
        - Facultad de Medicina
        - Facultad de Veterinaria
        - Geografía
        - Instituto de Química
        - Química E

- Zona Cultural
  - Coordinación de Humanidades
  - Teatro Juan Ruiz Alarcón

- DGSCA
  - CUAED
  - Escuela Nacional de Trabajo Social
  - Antropológicas
  - Jardín Botánico

- Torre II
  - Instituto de Ingeniería
  - Radio UNAM

- **13 en área metropolitana.**

  - Centro Mascarones
  - Palacio de Minería
  - Unidad Médica Experimental (Hospital General de México)
  - ENEP Aragón
  - Fundación Roberto Medellín
  - FES Zaragoza Campus 1
  - FES Zaragoza Campus 2
  - Palacio de Medicina
  - ENEP Iztacala
  - FES Cuatitlán Campus 4
  - FES Cuatitlán Campus 1
  - ENEP Acatlán
  - Dirección General de Personal Pitágoras

- **4 al interior de la República.**

  - Instituto de Matemáticas Morelia
  - Campus Juriquilla
  - Temixco
  - Cuernavaca

Esto en cuanto a los PBX, pero a nivel más detallado estos 40 PBX´s proporcionan diversos servicios, que veremos más adelante, a través de toda una gama de infraestructura instalada y configurada en los mismos:

- 13,600 DID´s.
- 2120 troncales.
- 12,487 extensiones.
- Más de 15,000 aparatos telefónicos.
- Red de fibra óptica propia, necesaria para interconectar todo el campus de Cd. Universitaria.
- Enlaces de cable coaxial en las instalaciones de la UNAM.
- 37 locales de comunicaciones, 20 de ellos en Ciudad Universitaria.
- Protocolo SS7 propietario de NEC para interconectar los 40 conmutadores.
- 18 enlaces E1 rentados punto a punto para enlace entre dependencias del área metropolitana y a nivel nacional.

La infraestructura telefónica de la UNAM está soportada por dispositivos de la marca NEC, ver tabla 6.2, con los siguientes modelos:

Modelo	Cantidad
SDS	9
IVS	6
IMS	16
IMX	1
ICS	4
3COM	1
IPX y XP	3
Total	**40**

Tabla 6.2 Cantidad de PBX NEC.

Esta gama de diferentes modelos de conmutadores ofrecen diferentes servicios:

- Identificador de llamadas.
- Desvío de llamadas.
- Conferencias (de hasta 8 personas).
- Grupos de entrada.
- Jalar llamadas.
- Correo de voz.
- Retrollamadas.
- Intercomunicación para funciones de jefe-secretaria.
- Programación de hot-line.

Para controlar la funcionalidad de los servicios se tienen:

- Códigos personalizados para llamadas a celular, larga distancia nacional e internacional.
- Restricción por extensión para llamadas a celular, larga distancia nacional e internacional.
- Control de llamadas por plan de numeración y rutas.

La conformación de la red se presenta en la fig. 6.9 :

Nodo de Arquitectura.

1. Torre de Rectoría
2. Dir. Gral. de Obras
3. Facultad de Ingeniería
4. Dir. Gral. de Personal
5. Facultad de Economía

Nodo de Torre II.

6. Instituto de Ingeniería
7. Palacio de Minería
8. Unidad Médica Experimental
9. ENEP Aragón
10. Roberto Medellín
11. FES Zaragoza (campo 1)
12. FES Zaragoza (campo 2)

13. Palacio de Medicina
14. ENEP Iztacala
15. Morelia
16. FES Cuautitlán (campo 4)
17. FES Cuautitlán (campo 1)
18. Radio UNAM
19. ENEP Acatlán
20. Campus Juriquilla
21. Pitágoras
22. Facultad de Medicina

Nodo IIMAS.

23. Facultad de Veterinaria
24. Instituto de Geografía
25. Instituto de Química
26. Química E

Nodo Zona Cultural.

27. Cuernavaca
28. Coordinación de Humanidades
29. Teatro Juan Ruiz de Alarcón
30. Centro Mascarones

Nodo DGSCA.

31. Jardín Botánico
32. CUAED
33. Esc. Nal. de Trabajo Social
34. Temixco
35. Antropológicas

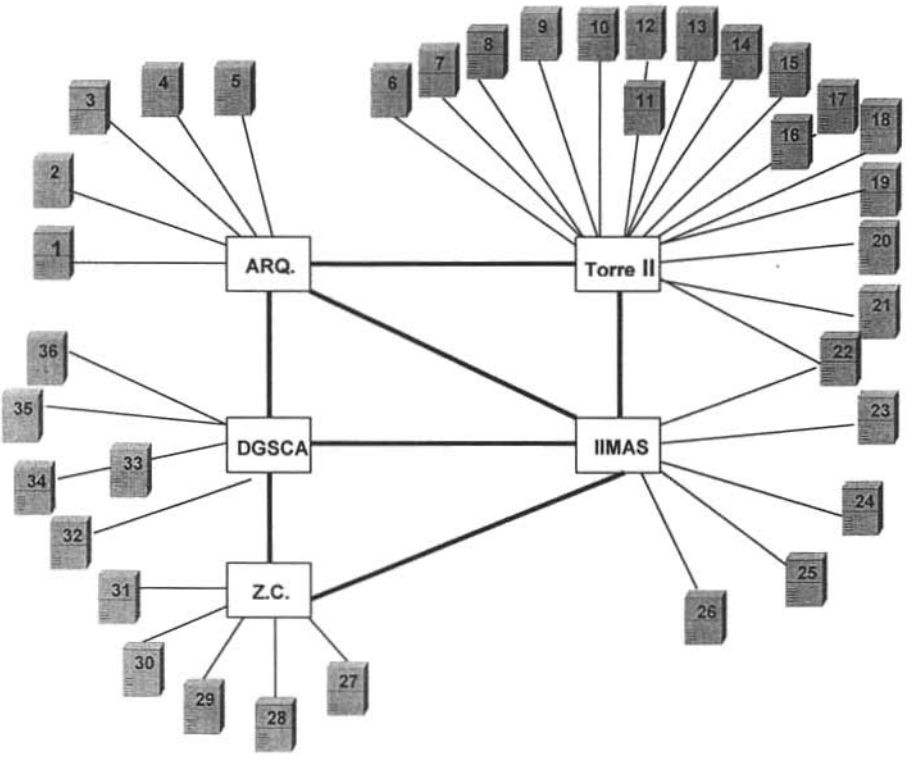


Fig. 6.9 BackBone Telefónico Universitario.

En cuanto al nivel de enrutamiento los conmutadores utilizan el protocolo SS7 (CCIT-7), para comunicarse entre todos los dispositivos que componen la red telefónica privada de la UNAM.

Para el intercambio de información con TELMEX y Avantel, quienes son los proveedores de servicios hacia la PSTN, utilizan una señalización R2 modificada, con lo que nos ayuda también a proporcionar los servicios anteriormente mencionados.

Dentro del backbone, conformado por los 5 nodos principales (Arquitectura, Torre II de Humanidades, IIMAS, Zona Cultural y la DGSCA), ubicados dentro de Ciudad Universitaria, los conmutadores pueden manejar y dirigir el tráfico entre ellos a través de un enrutamiento del tipo "estático", comparado con el de los enrutadores de datos, pero esta tabla de enrutamiento estática es llamada "tabla de códigos de punto". Estos códigos de punto tienen configurado qué circuito deben tomar para llegar a cierto número dentro del plan de numeración de la UNAM, teniendo en cuenta, claro está, el plan de numeración.

Además de estas rutas estáticas entre los conmutadores para llegar hacia un destino, se tienen configuradas rutas de desahogo o de respaldo, llamadas también de desborde, ya que si alguno de los circuitos está utilizándose al 100% de su capacidad, o si está fuera de servicio o por alguna razón falla, entonces se tiene la posibilidad de

tomar otra ruta para llegar a su destino, ya que dentro del diseño de la red se ha contemplado la redundancia física para llegar de un lugar a otro.

Cabe mencionar que esta redundancia, lógica y física, sólo existe dentro del nivel dorsal de la red, en casos muy especiales también se tiene una redundancia al nivel de los nodos de distribución ubicados en los nodos fuera de Ciudad Universitaria.

Dentro de la dorsal, que compone la red telefónica se encuentran enlaces troncales que conectan entre sí a los conmutadores centrales de la red, ver fig. 6.10. Al ser los que interconectan los dispositivos de diferentes nodos, estos enlaces deben de ser los suficientemente capaces de transportar la cantidad de llamadas generadas en cada uno de los nodos, que deseen comunicarse hacia algún otro, dentro de la misma Ciudad Universitaria.

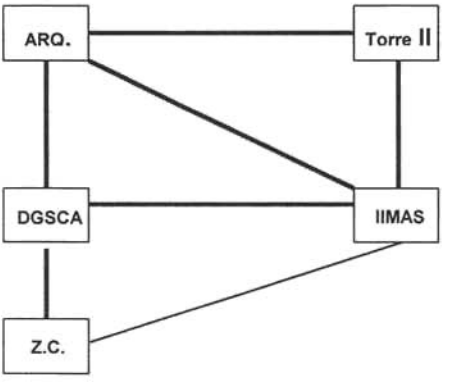


Fig. 6.10 Enlaces troncales.

Cada uno de estos enlaces está compuesto por 3 E1`s, es decir, son capaces de llevar a cabo hasta 90 conexiones simultáneas entre cada nodo, excepto de IIMAS a Z.C. (Zona Cultural) donde solamente hay 30 canales disponibles para llevar a cabo la transmisión de voz, fig. 6.11.

Otro nivel de redundancia se tiene a nivel de interconexión hacia la red pública conmutada (PSTN) ya que en la actualidad se tienen 56 enlaces E1´s para llevar a cabo esta comunicación. Estos E1´s son utilizados como "entradas" y "salidas" desde y hacia la PSTN.

Esta interconexión entre la RedUNAM y la PSTN, se lleva a cabo de forma distribuida dentro de los 5 nodos principales, teniendo en cuenta que estos enlaces tienen una capacidad finita y que podrán dar servicio, ya sea de entrada o salida, durante cierto tiempo antes de congestionarse con la cantidad de tráfico que es capaz de generar una red con 12,000 servicios.

Cada uno de los nodos principales tienen una cierta cantidad de enlaces E1 hacia la PSTN (observar tabla 6.3), algunos de ellos sólo se utilizan en un único sentido, ya sea para que salgan llamadas desde la UNAM hacia la PSTN o llamadas de la PSTN entren hacia la UNAM por algunos de estos enlaces. También hay circuitos, o enlaces, que son bidireccionales, esto es, que funcionan tanto para que entren y salgan llamadas UNAM-PSTN.

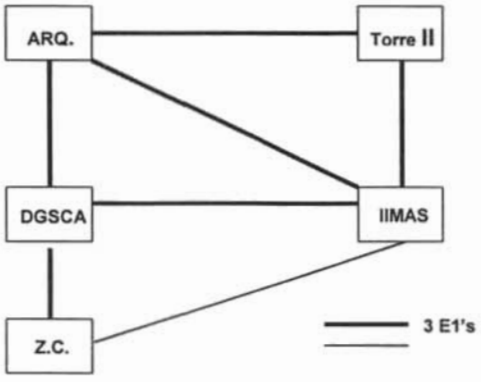


Fig. 6.11 Enlaces troncales E1's.

Nodo	Entrada	Salida
Arquitectura	6	10
Torre II	13.5	9.5
DGSCA	6	3
IIMAS	4	3
Zona Cultural	2	4

Tabla 6.3 Cantidad de enlaces por nodo hacia la PSTN.

6.4 Análisis de Internet 2 en la UNAM.

La UNAM ha jugado un papel primordial en el desarrollo e implantación de las telecomunicaciones e Internet en México. La participación en laboratorios tecnológicos para la implementación de tecnologías emergentes, con la colaboración de la UNAM en maquetas internacionales de pruebas para esquemas operacionales y reales, adecuados a las tecnologías y estándares que con esto conlleva, han marcado las pautas en los diseños y operación de las redes nacionales, gracias al trabajo que realiza. La UNAM en materia de redes permite establecer tendencias tecnológicas en las redes de telecomunicaciones pertenecientes a ésta, así como dar pautas nacionales.

Como se mencionó en el capítulo cuatro (Internet 2) la Universidad es miembro fundador de la implantación del modelo actual de lo que ahora es la red **CUDI** (Corporación Universitaria del Desarrollo Internet) creada en 1999 que lleva el desarrollo de la Red de Internet 2 en México. Como principales participantes están:

- CESESE
- ITESM
- IPN
- UAM
- UANL
- UAT
- UdeG
- UDLA
- UNAM

Resaltando como principal objetivo el dotar a la comunidad científica y universitaria de una red de telecomunicaciones que permita crear una nueva generación de investigadores, proporcionando a la UNAM de mejores herramientas que permitan desarrollar aplicaciones científicas y educativas de alta tecnología.

6.4.1 Proyección de la UNAM en Internet 2.

Como miembro fundador de CUDI, la UNAM ha alcanzado grandes metas gracias al esfuerzo de sus diferentes grupos de trabajo, obteniendo los siguientes logros:

- ✓ Centro de Operación de la Red I2 nacional (NOC I2).
- ✓ Centro de Operación de Videoconferencia I2 nacional (VNOC I2).
- ✓ Coordinador del Grupo de Enrutamiento.
- ✓ Coordinador del Grupo de IPv6.
- ✓ Coordinador del Grupo de Voz sobre IP.

Con lo cual, la UNAM marca los pasos a seguir en los diferentes rubros de las telecomunicaciones, gracias a la investigación y esfuerzo de sus universitarios.

6.4.2 Enlace de la UNAM a Internet 2.

Actualmente la UNAM cuenta con una conexión E3 (34.368 MB) permanente al Backbone de Internet 2 México. La distribución y enlaces son llevados a cabo por Telmex y Avantel, para obtener una idea mucho más clara de la actual conexión de la UNAM al Backbone a través de Telmex observe la fig. 6.12, en ésta se observa como es encaminado el tráfico de Internet 2 de la UNAM hacia el backbone de Internet 2 (CUDI) que comunica con los diferentes miembros, afiliados y asociados, a su vez a las redes de Abilene, UTEP y Houston, que proveen salida a Internet 2 a nivel mundial.

Fig. 6.12 Enlace UNAM a Internet 2.

6.4.3 Enrutamiento lógico de tráfico.

El enrutamiento de los datos en RedUNAM es diferenciado, ya que actualmente con el modelo actual de los datos que viajan por los diferentes medios lógicos y físicos, son claramente identificables los diferentes tipos de información que viajan a través de la misma, ya sean éstos datos, voz o video que van destinados a el Internet tradicional e Internet 2, dando el debido trato de enrutamiento a ambos y separando el tráfico como se observa en la fig. 6.13.

Esto se hace por medio del protocolo de enrutamiento en BGP y las políticas de enrutamiento que se están recibiendo desde los sistemas vecinos, delimitando por medio de este intercambio hasta donde serán propagados los anuncios, de ésta manera evitando los anuncios de Internet tradicional por medio del Founfry Networks NetIron 8000 que es un ASBR (Autonoumus System Border Router), que delimita el tráfico interno con el externo por medio de los anuncios de BGP en conjunto con las políticas de configuración y enrutamiento establecidas dentro de los Cisco Routers 7200 donde llega los ISP´s de la UNAM, y con el Cisco Router 7500 que recibe los anuncios del ISP de Internet 2 y su vez anuncia al ASBR por medio de BGP que maneja el tráfico de entrada y salida de Internet 2 generado por la UNAM y afiliados que se enlazan a éste por medio del enlace de TELMEX hacia el Backbone de CUDI, dirigiendo todo el tráfico correspondiente, por lo que si no se encuentran en las tablas de redes anunciadas por Internet 2 compartidas por los anuncios de BGP entre ambos (Founfry NetIron 8000 y

Cisco Router 7500) entonces son enviadas a los ISP´s de Internet tradicional, evitando el tráfico de datos no propios de Internet 2.

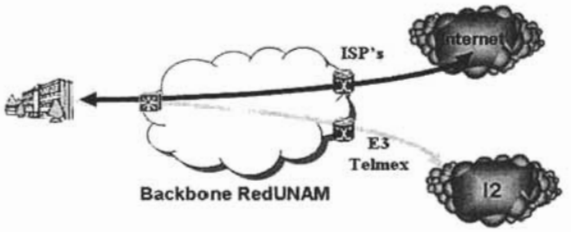


Fig. 6.13 Enrutamiento Lógico de Internet e Internet 2.

6.4.4 Resumen del Análisis de RedUNAM a través de Internet 2.

La integración de las diferentes dependencias pertenecientes a RedUNAM, que demanden las capacidades de Internet 2 ya se encuentran previstas desde el principio que se reestructuro ésta, esto se realiza gracias a los protocolos del enrutamiento en OSPF y BGP implementados, por lo que no se tiene que realizar cambios al momento que una dependencia universitaria así lo requiera, optimizando de esta manera los recursos, procesos de control y comportamiento del tráfico en los medios físicos y lógicos de la red. Proporcionado a su vez acceso a los distintos afiliados que tienen acceso a la misma, a través de RedUNAM.

Para que las diferentes aplicaciones de investigación y academia de la UNAM y por tanto hacia Internet 2, permitieran soportar un alto nivel de control, calidad y disponibilidad se buscó como fase inicial e inmediata el fortalecimiento de la infraestructura de backbone como se explicó anteriormente en este capítulo; que llevará a RedUNAM hacia una infraestructura robusta con tecnologías de vanguardia.

Se reestructuró y actualizó el antiguo backbone en ATM a Gigabit Ethernet, de esta forma RedUNAM es una de las redes académicas más robustas y de alta calidad de operación.

Obteniendo los siguientes beneficios:

- ✓ Soporte de tecnologías Emergentes
  - o Multicast a Nivel Backbone.
  - o Calidad de Servicio (QoS).
  - o IPv6.
  - o MPLS.
- ✓ Soporte de Aplicaciones Multimedia
  - o VoIP (Voz sobre IP).
  - o Video over IP.

Antes de la realización de este proyecto no existía alguna aplicación o solución para el transporte de paquetes IP de voz que hiciera uso del enlace de la UNAM a Internet 2.

El objetivo primordial es hacer uso de la red de Internet 2 para la investigación de tecnologías de Voz sobre IP, ayudando al desarrollo de mejores estándares, por ende

mejores soluciones de voz, y la puesta en escena de una red telefónica alterna internacional al nivel de Internet 2.

6.5 Propuesta de solución de VoIP.

La metodología que se ha seguido esta ahora esta basada en el procedimiento general para resolver un problema de ingeniería, planteado por Eduard Krick en el libro titulado "Introducción a la Ingeniería y al diseño en la Ingeniería".

Este método de solución de problemas esta compuesto por varias etapas representadas en el siguiente diagrama, fig. 6.14:

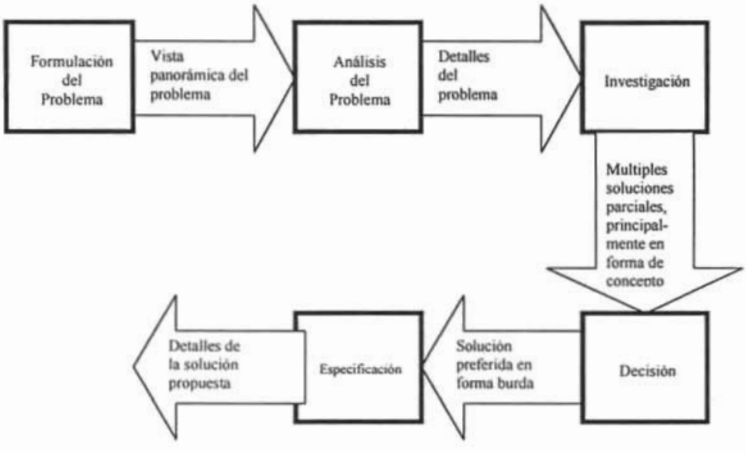


Fig. 6.14 Método de solución de problemas.

Por lo que del análisis anterior (puntos 6.2,6.3 y 6.4), se plantea en la fig. 6.15 la Propuesta de Operación de VoIP a través de Internet 2 en RedUNAM.

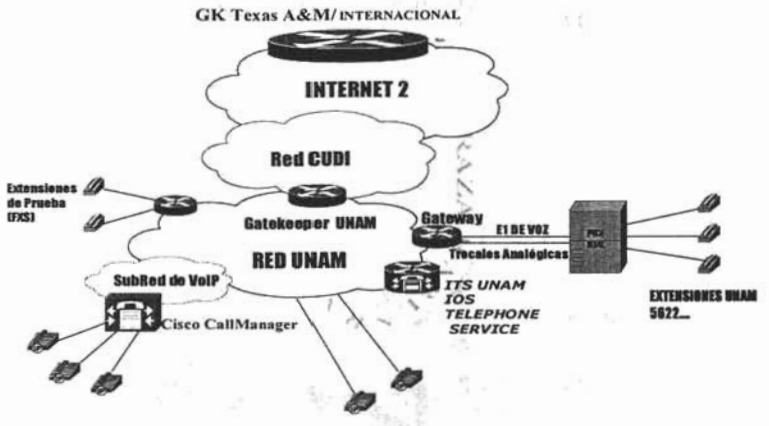


Fig. 6.15 Propuesta de funcionamiento de VoIP en la UNAM.

En este esquema se puede observar el ITS (IOS Telephone Service) siendo un equipo Cisco Router 1750 que brinda el servicio de agente de llamadas de los Teléfonos IP, este equipo además de brindar el servicio de Telefonía IP es uno de los H.323 Gateways VoIP registrado dentro del Gatekeeper UNAM realizando llamadas IP-IP a través de Internet 2, el equipo que realiza esta labor es un Cisco Router 3660. El Gatekeeper UNAM trabaja en conjunto con el Gatekeeper de la Universidad A&M de Texas y funcionan como medios de interconexión entre ambos nodos, las extensiones telefónicas universitarias realizan llamadas Analógico-IP por medio del Gateway ubicada dentro del mismo Cisco Router 3660 que tiene instalado un E1 de Voz el cual mantiene comunicación con el conmutador PBX NEC NEAX 2400, de igual manera por el E1 de Voz e ISDN PRI con señalización Q.SIG. Con este Gateway y su propio H.323 Gateway VoIP (Router 3660) que es registrado en el Gatekeeper universitario, son posibles las llamadas a los Teléfonos IP ubicados dentro del dominio del ITS y a su vez realizar y recibir llamadas de números telefónicos a través de Internet 2 pertenecientes al proyecto internacional de VoIP.

Si se cumplen con los requisitos mínimos de multimedia en una PC con plataforma Windows y soporte el software Microsoft Netmeeting pueden darse de alta terminales Microsoft NetMeeting que funcionan como SoftPhones las cuales puede realizar y recibir llamadas a extensiones telefónicas y números telefónicos de Internet 2. Es posible la anexión de la Subred de VoIP de Rectoría en caso de que se requiera.

6.5.1 Requisitos.

La infraestructura con la que cuenta actualmente la DGSCA-UNAM para la anexión a la red internacional de VoIP a través de Internet 2 es la siguiente:

- 1 Router Cisco 3660.
- 1 Router Cisco 1750.
- Software IOS correspondiente a los routers.
    - Software (C3660-JSX-M), Versión 12.1(3a)XI8 Tipo IP PLUS/H.323.

  - IOS (tm) C1700 Software (C1700-SV8Y7-M), Versión 12.2(11)YT2, Tipo IP PLUS.
- 1 Tarjeta E1 de voz 1 .
  - VWIC 1MFT-E1 Channelized E1/PRI port(s).
- 1 Tarjeta FXO.
  - 2 Voice FXO interfase(s).
- 1 Tarjetas FXS.
  - 2 Voice FXS interfase(s).
- 2 Troncales Telefónicas.
- 1 Cable Conversor Coaxial / RJ45.
- 2 Teléfonos Análogos.
- 6 Cisco IP Phone 7960.
- 1 Tarjeta de Enlace para troncales modelo 30CCTB en PBX NEC NEAX 2400.

Es importante mencionar que el equipo que da salida hacia la red Internet 2 (CUDI) es un Cisco router 7500 mencionado puntos atrás.

- ✓ Cisco Router 3660 con tarjeta E1 de voz, realiza las funciones de gateway entre la red Telefónica de la UNAM y la telefonía IP, por medio de un enlace digital E1 de voz compartido en el PBX NEAX 2400 a través de un cable BNC/RJ45. Maneja la capacidad de gatekeeper y VoIP Gateway.
- ✓ Cisco Router 1750 con tarjeta FXS, conecta a dos teléfonos estándar; además de tener el manejo de los teléfonos IP, por medio del ITS 2.01 y VoIP Gateway.

6.5.2 Etapas de desarrollo.

El funcionamiento del esquema se llevó a cabo en dos etapas, esto sucedió porque el Cisco CallManager no es de uso para pruebas, más importante aún, por seguridad ya que está en producción y su uso es para los funcionarios, por lo que se dio la tarea de encontrar una solución alterna en la cual se lograra la realización de pruebas, encontrado al IOS Telephone System (más información en www.cisco.com), como una opción viable y duradera.

En la primera etapa se puso en funcionamiento el esquema interno de convivencia del medio IP-Analógico e incorporación de los IP Phones al plan de marcación que lleva la UNAM para sus extensiones telefónicas. En una segunda etapa se puso en funcionamiento lo que fue la habilitación del Cisco Router 3660 como Gatekeeper para llevarlo al funcionamiento externo con el Gatekeeper de Texas A&M University e implantación del plan de marcación Internacional en la UNAM, y acceso de las extensiones universitarias a Internet2 y a la habilitación de H.323 VoIP Gateway en cada uno de los dispositivos finales para la realización de llamadas hacia Internet 2.

6.5.2.1 Primera etapa.

La red que se implementó en un principio para dicho propósito está basada en dos partes, la primera constituida por el agente de llamadas ITS 2.02 (IOS Telephone Service) que es un sistema de telefonía IP basado en hardware, esto quiere decir que es montado dentro de un router. En la tabla 6.4 puede verse los requisitos de memoria FLASH y memoria RAM así como la capacidad máxima de teléfonos IP. Se hicieron pruebas (Ver Punto 6.7) en diversos equipos para montar el ITS y se muestran sus características de funcionamiento en la tabla 6.4. Actualmente esta montado el ITS 2.02 en un Cisco router 1750 (ver siguiente inciso Configuración ITS), los IP Phones que están dentro del esquema son los Cisco IP Phones 7960 que están distribuidos dentro y fuera

de la Red de la DGSCA, la capacidad de IP Phones varía según el router en el cual se habilite éste.

Cisco Platform	Maximum Cisco IP Phones	Maximum DNs	Minimum DRAM Memory	Recommended DRAM Memory	Minimum Flash Memory	Recommended Flash Memory	Cisco IOS Release
Cisco 1750routers	24	120	64 MB	96 MB	32 MB	32 MB	12.2(13)T
Cisco 2600-XM[1] series	24	96	96 MB	96 MB	32 MB	32 MB	12.2(13)T
Cisco 3660 routers	48	288	96 MB	128 MB	32 MB	32 MB	12.2(13)T

Tabla 6.4 Requisitos mínimos para ITS.

En la anterior tabla sólo se mencionan algunos de los routers que soportan dicha tecnología, para más información consultar www.cisco.com.

Configuración ITS.

En el siguiente cuadro A.1, se puede observar la configuración del ITS (Router 1750), a ésta configuración se le hicieron algunas modificaciones por motivos de seguridad y así evitar un mal uso de la información.

```
tftp-server flash:P00303020209.bin
tftp-server flash:SEPDEFAULT.cnf
tftp-server flash:XMLDefault.cnf.xml

Telephony-service
 load 7960-7940 P00303020209
 max-ephones 12
 max-dn 48
 ip source-address 132.248.1.10 port 2000
 user-locale ES
 network-locale ES
 max-conferences 8
 transfer-pattern *
keepalive 10
 moh music-on-hold.au
 date-format dd-mm-yy
!
ephone-dn  10
 number 46990
 name Alfredo TAC
 no huntstop
 hold-alert 30 originator
!
ephone  1
 username "Alfredo"
 mac-address 0003.6B54.BBC8
 paging-dn 1
 button  1:10 2:20
dial-peer voice 1 voip
 description CONEXION-GK-UNAM
 destination-pattern .T
 session target ipv4:132.247.253.242
 no vad
!
dial-peer voice 2 voip
 description CONEXION-CUDI-CISCO
 destination-pattern 2....
 session target ipv4:158.97.84.131
!
dial-peer voice 3 voip
 destination-pattern .T
 session target ras
!
```

Cuadro A.1 Configuración del ITS (Router 1750).

Para habilitarlo fue necesario:

Software
- Cisco ITS V2.1 requires Cisco IOS Release 12.2(11)YT, Cisco IOS Release 12.2(15)T, or a later version.
- IP Plus.

Firmware de IP Phones
- Phone firmware files:
  - P00303020209.bin—for Cisco IP Phone 7940 and Cisco IP Phone 7960
  - P00403020209.bin—for Cisco IP Phone 7910
  - P00503010100.bin—for Cisco IP Conference Station 7935
  - S00103020002.bin—for Cisco IP Phone 7914
  - ata18x-v2-15-ms-020927a.zup—for Cisco ATA-186 and Cisco ATA-188

6.5.2.1.1 Conexión PBX NEC NEAX 2400.

A fin de Interconectar el sistema de telefonía IP a la Red telefónica de la UNAM se hizo uso de un Cisco Router 3660 como gateway (ver Fig. 6.16), esto gracias a la interfaz E1 de voz. El enlace utilizado para conectar el PBX NEC NEAX 2400 al Cisco Router 3660 fue el de un E1 (2.048 MB) de voz, modelo 1MFT-E1, contiene 1 módulo PVDM-12 este es un DSP (Digital Signal Processor) que permite el tráfico de voz en paquetes de datos, conectado a través de la tecnología ISDN con el protocolo de señalización Q.SIG, señalización que maneja el conmutador PBX NEC. Este enlace es necesario para que se incluyan los teléfonos tradicionales a la maqueta y con esto hacer mucho más completa la solución.

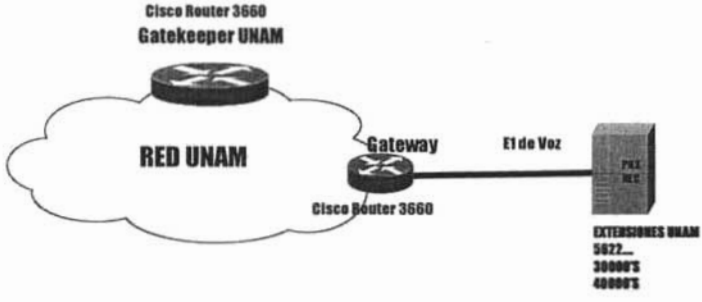


Fig. 6.16 Conexión de gateway y PBX.

6.5.2.1.2 Gateways en el sistema.

Para lograr la comunicación con los diferentes medios y modos de comunicación se observa que debe de haber un intermediario que interactúe entre el mundo digital y analógico, tanto en el medio IP-IP, Analógico-Digital/IP y IP-IPvoicePackets, el logro en estos se da por los elementos llamados gateways de voz y VoIP Gateways.

La segunda parte dentro de esta etapa es la conexión del sistema de la Red Telefónica de la UNAM para tener una solución más completa e incluir las extensiones y no excluirlas ya que disminuiría la cantidad de llamadas que se realizarían, esto es hecho (incluyendo con esto a TELMEX) por medio de un Gateway (Cisco Router 3660) con una interfase E1 de Voz.

Configuración Gateway (E1 de Voz).

Como se puede observar en el cuadro A.2, el E1 de voz esta configurado con señalización ISDN y canales tipo PRI con señalización Q.SIG. Así como un peer para comunicarse con teléfonos análogos puesto que hace recepción y envió de llamadas por el puerto del controlador E1.

Importante: la configuración se encuentra modificada por motivos de seguridad.

Para habilitarlo fue necesario:

Software

- ✓ Version de IOS Version 12.1(3a)XI8 IP PLUS H.323

Hardaware

- ✓ ICVM 12 E1 controller.

```
voice-card 3
!
isdn switch-type primary-qsig
call rsvp-sync
cns event-service server
!
controller E1 3/0
 framing NO-CRC4
 pri-group timeslots 1-10,16
!
interface Serial3/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 no cdp enable
!
voice-port 3/0:15
!
dial-peer voice 4 pots
 destination-pattern 4....
 no digit-strip
 direct-inward-dial
 port 3/0:15
 forward-digits all
```

Cuadro A.2 Configuración Gateway .

Configuración Gatekeeper.

Esta es la configuración del gatekeeper UNAM para lograr la conexión con otros gatekeepers (ver cuadro A.3). Importante: la configuración ha sido alterada por motivos de seguridad.

```
gatekeeper
 zone local UNAMGK unam.mx 200.15.2021
zone remote TAMUI2 tamu 201.36.4.2  1719
zone remote GK_UAEH reduaeh.mx 102.3.4.2 1719
 zone prefix GK_UAEH 8727....
zone prefix UNAMGK 5255562.....
 zone prefix I2GK *
 zone prefix TAMUI2 *
 gw-type-prefix 1#* default-technology
 lrq forward-queries
 no shutdown
```

Cuadro A.3 Configuración Gatekeeper de la UNAM.

Para habilitarlo fue necesario:

Software

- ✓ Version de IOS Version 12.1(3a)XI8 IP PLUS H.323

6.5.2.1.3 Direccionamiento IP para los Cisco IP Phones.

El direccionamiento IP que se utilizó para asignar a las direcciones IP´s correspondientes a los Cisco IP Phones, está tomado del direccionamiento asociado a los segmentos de subredes IP de la UNAM donde son conectados los IP Phones, en algunos segmentos se cuenta con el servicio de DHCP, aún con esto se consideró asignarles direcciones de tipo estático. Un punto notorio es que no es necesario que se tenga una dirección IP propia de la UNAM para hacer uso del sistema, ver cuadro A.3.

6.5.2.1.4 Plan de marcación.

El plan de marcación se definió con la asociación de extensiones del sistema ITS con el llevado por el plan de marcación de la red de telefonía de la UNAM, y siendo asignado extensiones sólo validas dentro de la UNAM y DID´s que son números telefónicos válidos tanto dentro y fuera de la UNAM, validados por una ruta dirigida a la tarjeta E1 ubicada dentro del PBX.

- ✓ Plan de marcación del sistema IP hacia la Red Telefónica de la UNAM usando la interfase de VoIP Gateway H.323 (router 3660 y 1750) y el PBX NEC NEAX 2400.
  - o Extensiones del PBX 20000´s, 30000´s y 40000´s.

- ✓ Plan de marcación del Sistema IP hacia Red Telefónica de TELMEX usando la interfase de VoIP Gateway H.323 (router 3660 y 1750) y el PBX NEC NEAX 2400.
  - o Marcación del dígito líder 9+XXXXXXXX, 9+01+ZZ+XXXXXXXX, etc.

- ✓ Plan de marcación de la Red Telefónica de la UNAM hacia el sistema IP, usando rutas hacia la interfase E1 de voz en el PBX y la interfase de VoIP Gateway H.323 (router 3660 y 1750) y el PBX NEC NEAX 2400.
  - o 4699X y 2889X

- ✓ Plan de marcación desde la Red Telefónica TELMEX hacia el sistema IP usando una interfase de VoIP Gateway H.323 (router 3660 y 1750) y el PBX NEC NEAX 2400.
  - o Desde TELMEX mediante la asociación de DID´s asociadas a las extensiones IP 5622889X.

6.6 Segunda etapa.

El funcionamiento del procesamiento de llamadas y encaminamiento de las mismas es realizado a través de la activación de la modalidad de Gatekeeper en el Cisco Router 3660, puede ser cualquier otro router que así lo soporte (para más información consultar la página www.cisco.com) la conexión al Gatekeeper de la Universidad A&M de Texas no sólo sirve para la realización de llamadas entre tales Universidades ya que el Gatekeeper es a su vez un Gatekeeper Internacional esto quiere decir a simples rasgos que es un conmutador internacional que comunica a otras instituciones, consiguiendo la capacidad de realizar llamadas Internacionales a diferentes instituciones albergadas alrededor del mundo principalmente hacia EU, siendo la UNAM la doceava universidad en integrarse a la red Internacional de VoIP a través de Internet 2 dentro de las que están:

- ✓ Czech National Research and Education Network.
- ✓ University of Illinois, Urbana-Champaign.
- ✓ Australian Academic and Research Network.

- ✓ Northwestern University, Evanston/Chicago ILL.
- ✓ University of Wisconsin, Madison.
- ✓ Federal University of Rio de Janeiro.
- ✓ University of Cincinnati.
- ✓ Texas A&M University.
- ✓ University of Virginia.
- ✓ Penn State University.
- ✓ Indiana University.
- ✓ University of México.

Constantemente se están integrando más universidades por lo que esta lista ha aumentado.

6.6.1 Plan de marcación en Internet 2 y acceso de extensiones UNAM a Internet 2.

Actualmente el plan de marcación está siguiendo el lineamiento de los estándares dados por ENUM (Telephone Number Mapping working group) que no es más que el llevado internacionalmente por los diferentes países para la marcación telefónica tradicional. Esto se lleva así hasta que no se encuentre un estándar de marcación para Internet 2.Un ejemplo sería el siguiente:

- ✓ Plan de Marcación:
  - o Llamadas Nacionales Lada Nacional + Código de Área + Número Local.
  - o Llamadas Internacionales: Lada Internacional + Código de Área + Número Local.

- ✓ Acceso a la red Internacional de VoIP desde las redes telefónicas universitarias tradicionales, mediante la marcación del dígito líder ***8**.

6.6.2 H.323 VoIP Gateway.

Para anexar los teléfonos de la Red Telefónica de la UNAM al esquema de operación de VoIP entre ambos nodos (UNAM-DGSCA y la Universidad A&M de Texas), se configuró por medio del Cisco Router 3660 un H.323 VoIP Gateway (ver cuadro A.4) que resuelve las llamadas provenientes de la Red Telefónica de la UNAM hacia Internet 2, por medio de la interfase E1 de Voz dentro del Gatekeeper de la UNAM y éste encamina las llamadas al Gatekeeper en la Universidad A&M de Texas, del mismo modo se dió de alta otro H.323 Gateway VoIP en el Cisco Router 1750 que administra los Cisco IP Phones.

Configuración Gateway VoIP H.323.

A continuación se puede describe la configuración del GW VoIP H.323, en el cuadro A.4 Importante: la configuración se encuentra modificada por motivos de seguridad.

```
interface FastEthernet0/1
 ip address 132.248.204.14 255.255.255.0
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id GK ipaddr 10.23.6.9 1719
 h323-gateway voip h323-id  GW
 h323-gateway voip tech-prefix 1#
```

Cuadro A.4 Configuración del Gateway VoIP H3.23.

Para habilitarlo fue necesario:
Software

- ✓ Version de IOS Version 12.1(3a)XI8 IP PLUS

6.7 Pruebas.

Las pruebas realizadas dentro del proyecto fueron amplias y variadas, aquí se presentan las más relevantes que fueron abriendo paso a un gama más amplia de pruebas.

Esquema de pruebas de evaluación de los sistemas de VoIP

Evaluación de funcionalidades de Teléfonos IP:

- ✓ Amigabilidad (Facilidad de uso de las teclas y/o softkeys para diversas funciones de usuario ejemplo: transferencia, retención, espera en línea, etc.).
- ✓ Redial.
- ✓ Call Forward.
- ✓ Follow me.
- ✓ Call Park.
- ✓ Hola/Resume.
- ✓ Speaker.
- ✓ PickUP.
- ✓ HuntGroups.
- ✓ Directorio Telefónico integrado.
- ✓ Identificador de llamadas (Nombre y Número).
- ✓ Transferencia de llamadas
- ✓ Conferencia tripartita
- ✓ Capacidad Multilíneas
- ✓ Lámpara para correo de voz.
- ✓ Tipos de alimentación para los IP Phones.
  - o Duración (en llamada, en espera)
- ✓ Plan de numeración
  - o Extensión de longitud variable.
  - o Número identificador para llamas externas.
- ✓ Puerto PC y Puerto SW en IP Phone.
- ✓ Definición de funcionalidades por parte del usuario.
- ✓ Funcionalidades Adicionales. (Convenidas por el Proveedor).
- ✓ Direccionamiento por servidor DHCP
- ✓ Configuración de los parámetros estáticos (Dirección IP, DNS, Gateway, Mascara)
- ✓ Interoperabilidad con otros fabricantes.
- ✓ Seguridad (VPN, Encriptación)

SoftPhones

- ✓ Igualar las mismas capacidades con los IP Phones, así como funcionalidades adicionales.
- ✓ Conexión de Softphones al sistema de VoIP a través de enlaces Dial Up.
- ✓ Seguridad (VPN, encriptación).

IP Phone Wireless.

- ✓ Amigabilidad (Facilidad de uso y rapidez en funciones de usuario, ejemplo: transferencia, retención, espera en línea, etc.).
- ✓ Igualar capacidades con IP Phones, así como funcionalidades adicionales.
- ✓ Seguridad (estándares de seguridad, WEP, WPA) y creación de VPN´s entre el equipo y el sistema.
- ✓ Interoperabilidad con diferentes fabricantes (Access Points, Bridges, Telefonos IP y Wireless).
- ✓ Estándares que soporta.
  - o Capacidad de Soporte del estándar 802.11i.
  - o Soporte de estándares al 802.11
- ✓ Interoperabilidad con otros sistemas de VoIP.

Funcionalidades del Sistema de Telefonía IP.

- ✓ Esquemas de señalización usados:
  - o Interoperabilidad con PBX (NEC) y/o PSTN a traves de troncales digitales E1 (R2 modificado,

ISDN, QSIG, PRI, etc.).
    - Uso de R2 y QSIG en un mismo sistema de VoIP.(Utilizando dos E1´s al mismo tiempo)
  - Interoperabilidad con PBX y/o PSTN a través de troncales analógicas.
  - Interoperabilidad con otros sistemas de VoIP, iguales o semejantes (uso y cumplimiento del estándar H.323, uso y cumplimiento del estándar SIP).
- ✓ Definición de clases de servicios (COS).
- ✓ Definición de clases de restricciones (COR).
- ✓ Definición de VLAN´s.
- ✓ Definición de códigos de cuenta.
- ✓ Capacidad de recibir y enviar el caller ID
- ✓ Estabilidad y redundancia.

Esquemas de Compresión y QoS.

- ✓ Compresión en diferentes niveles de compresión (G.711, G.723, G.729, etc) comprobando las funcionalidades y comportamiento de la calidad de la voz. A nivel LAN y/o WAN.
- ✓ Comportamiento del Sistema de VoIP en VPN´s , y creación de VPN´s por parte del equipo.
- ✓ Probar QoS y si los paquetes son etiquetados por el equipo.
- ✓ Probar QoS, inyectando tráfico de datos.

Capacidad para ofrecer servicios de FAX/MODEM

Administración y monitoreo de VoIP y sus Componentes.

- ✓ Registro detallado de llamadas o CDR (tarificación de llamadas).
- ✓ Monitoreo del Permormance del sistema.
- ✓ Interfaz de Administración (http, telnet, puerto de consola, etc.).
- ✓ Administración de los teléfonos IP
  - WEB
  - Telnet
  - Vía CLI
  - Sistema
- ✓ Estabilidad del sistema.
- ✓ Registro de nuevas funcionalidades y registro sin el registro de una caída del sistema (Reiniciar).

Dentro de la búsqueda de un equipo que reuniera las necesidades óptimas para la instalación del Gatekeeper se obtuvo a préstamo un Cisco Router 2600 obtenido como resultado en primera instancia el alta del Gatekeeper y configuración de líneas FXS y FXO, la primera provee el servicio de un teléfono básico, la segunda es usada como línea troncal telefónica conectándose en este caso a un PBX NEC NEAX 2400 por medio una línea analógica (ver fig. 6.17). En este tiempo aún no se entablaba comunicación hacia el nodo ubicado en Texas, ya que este no sería el Router que se utilizaría definitivamente.

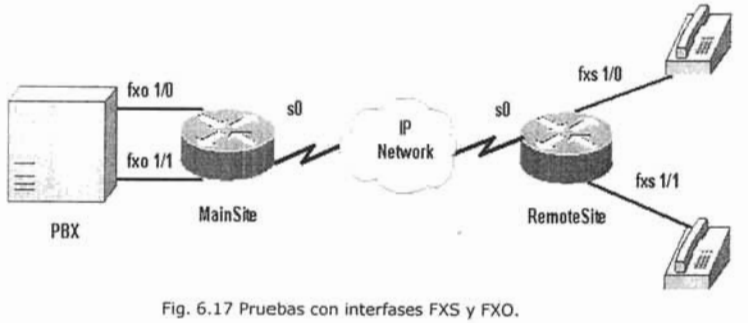


Fig. 6.17 Pruebas con interfases FXS y FXO.

El ITS como instrumento de agente de llamadas o procesador de comunicaciones de telefonía IP, se instauró primeramente en un Cisco Router 2620, éste actuando a manera de pruebas de la tecnología pero sólo estuvo un corto tiempo en la realización de pruebas logrando un nulo avance, como alternativa se tomó un Cisco Router 1750 que fue puesto en disposición del laboratorio de VoIP. Se lograron con éxito varias pruebas de las cuales

se dió de alta en el ITS teléfonos IP (Cisco IP Phone 7960) dentro de la DGSCA-UNAM y en Facultades dentro del Campus Universitario así como pruebas a Nivel WAN en la ENEP Acatlán y en la ciudad de Puebla con motivo de la Reunión de Otoño (2003) de la Red CUDI, obtenida una comunicación con éxito y sin pormenores. Se pensó poner el ITS dentro del Cisco Router 3660 pero sabiendo de la carga de trabajo que tendría como Gatekeeper se optó por no cargarlo dentro de éste.

Tiempo después se consiguió un Cisco Router 3660 el cual formaba parte del laboratorio ya que con éste se impartían laboratorios en cursos que imparte la propia DGSCA-UNAM y que se utiliza actualmente en este proyecto como Gatekeeper el cual tiene las siguientes características:

- 2 FastEthernet/IEEE 802.3.
- 19 Serial network interfases.
- 1 Puerto Channelized E1/PRI.
- 2 Interfases de Voz FXO.
- 2 Interfases de Voz FXS.
- 16MB de Memoria Flash.
- 16MB de Memoria RAM.

Con lo anterior se obtuvo comunicación con la Universidad A&M de Texas a través de las interfases FXS y FXO como se puede observar en la fig. 6.18.

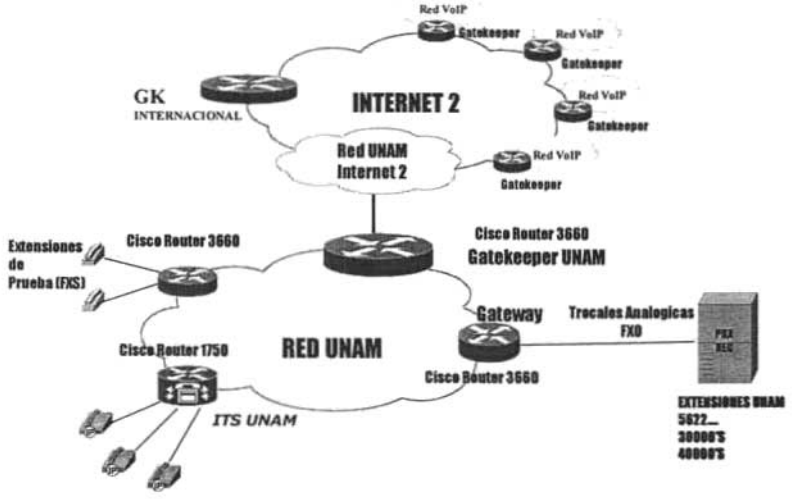


Fig. 6.18 Prueba de realización de llamadas con interfases FXS.

Tiempo después se obtuvo a una Tarjeta E1 30PRT propia para uso con el PBX NEC NEAX 2400 con señalización CAS R2, con ésta y la tarjeta controladora E1 de Voz se configuró dando lugar a la realización de llamadas de extensiones a Teléfonos IP y viceversa, y a TELMEX de igual manera como se puede ver en la fig. 6.19. Con esta tarjeta se obtuvo como consecuencia más líneas disponibles para la realización de llamadas a través de las extensiones analógicas y digitales de la Universidad. A su vez se integraron los Teléfonos IP a dicha conexión asignándoles números DID´s y extensiones mediante ARS (Access Routing Static) de esta manera se pueden marcar a estos desde cualquier lugar del mundo donde exista un teléfono y marcación directa dentro de la UNAM.

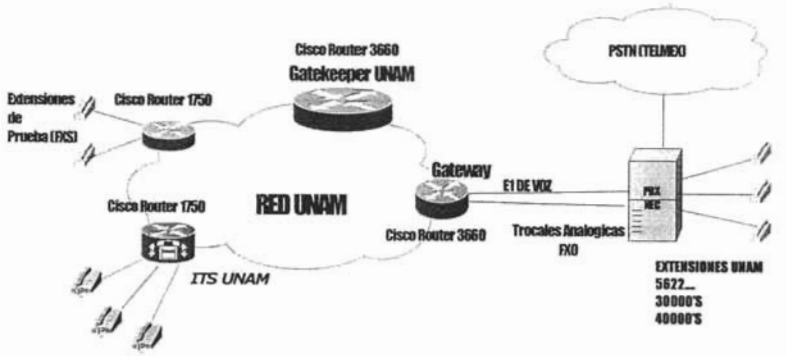


Fig. 6.19 Conexión de la maqueta hacia PSTN.

No obstante la conexión aportaba características mínimas (envío y recepción de llamadas) al tiempo de realizar llamadas de Teléfonos IP se experimentaron errores de sincronía al momento de realizar llamadas hacia la PSTN (TELMEX) ya que sólo en este caso ocurría errores de sincronía; es decir que cada determinado tiempo la llamada se degradaba y consecuentemente se perdía la comunicación telefónica, se llegó a la conclusión de que la señalización que utiliza TELMEX (CAS R2 modificado) entraba en desincronización al pasar de R2-SS7-R2 ya que los E1's de Voz que se reciben en la UNAM llegan en CAS R2 por medio de los PBX se convierten en SS7, ya que en las llamadas internas de extensión a extensión, en los teléfonos IP y en las llamadas a través de Internet 2 no ocurrió tal error.

Al surgir esta problemática el personal de Telefonía de la UNAM cambio la tarjeta tipo CAS R2 a una de ISDN con señalización Q.SIG modelo 30DTK, no sólo se eliminó el problema sino que se vió mejoría en los servicios de telefonía, como es identificación de llamada, transferencia, conferencia y envió de DID's. Fue necesario cambiar la configuración que se tenía programada con CAS R2 y cambiar la configuración de la tarjeta controladora E1 de voz ISDN PRI.

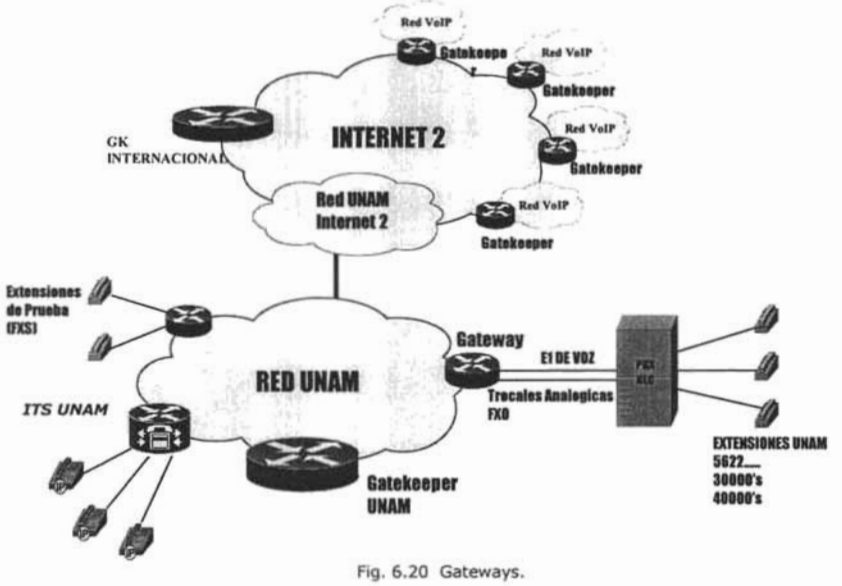


Fig. 6.20 Gateways.

En esta parte también se configuraron los Gateways VoIP H.323 que se registran con el Gatekeeper consiguiendo acceso al nodo de la Universidad A&M de Texas y con esto a la Red Internacional de Pruebas de VoIP en Internet 2. Existen actualmente dos, uno en el ITS (Cisco Router 1750) que dan acceso a los IP Phones, y un segundo ubicado en el Cisco Router 3660 que sirve de gateway con ayuda de la interfase E1 de voz, que brinda servicio a los Teléfonos Tradicionales de la UNAM.

6.8 Beneficios alcanzados.

Con este esquema final de operación (fig. 6.21) se pretendió alcanzar, metas técnicas y de operación dentro de Internet 2 alcanzando lo siguiente:

- Desplegar una red de VoIP escalable mediante el protocolo de señalización H.323 que permita mantener en contacto a los diferentes integrantes de la Universidad de Texas.
- Permitir el movimiento transparente de las terminales de usuario a lo largo y ancho de la red UNAM-DGSCA y Universidad A&M de Texas e Internacional de VoIP.
- 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 de Internet 2.

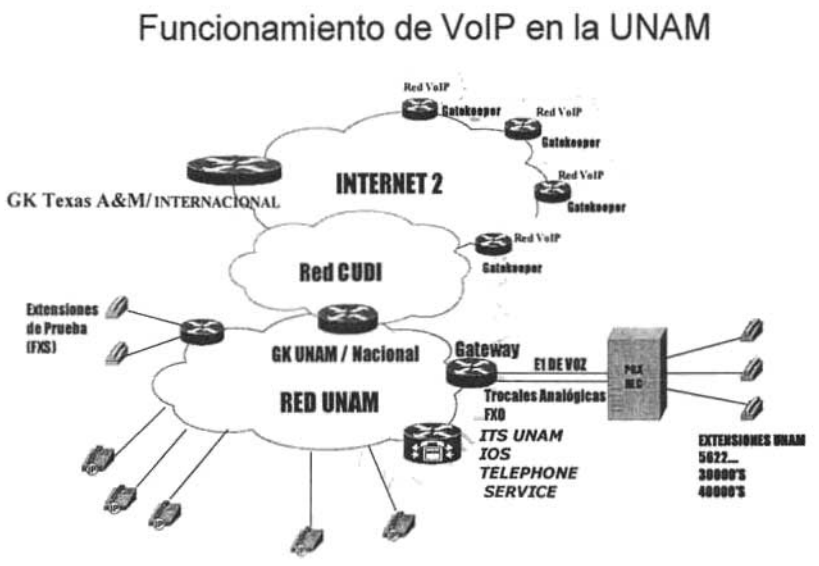


Fig. 6.21 Solución final al enlace entre nodos UNAM-DGSCA y la Universidad A&M de Texas.

CONCLUSIONES

Conclusiones y comentarios finales.

- ✓ Se cumplió el objetivo principal de interconectar los nodos UNAM-DGSCA y la Universidad A&M de Texas por medio de un enlace de Voz sobre IP a través de la red de Internet 2, con la ayuda de los equipos proporcionados por la DGSCA y asesoría del Departamento de Telecomunicaciones.

- ✓ El esfuerzo en conjunto de la UNAM con la Universidad A&M de Texas y el apoyo mútuo en las investigaciones de VoIP invita a trabajar mucho más fuerte, además de la disposición de la UNAM de estar a la vanguardia en lo que respecta a tecnología de redes y proveer a la comunidad universitaria principalmente, a sus investigadores y alumnos, servicios de calidad, como los de cualquier universidad a nivel mundial.

- ✓ Cierto es que la UNAM está cambiando a pasos agigantados y con esto también sus formas de comunicación, puesto que con este proyecto se proporciona un mejor enfoque en la selección de tecnologías de voz sobre redes de datos.

- ✓ No toda la infraestructura de la universidad soportaría VoIP, ya que muchas de las escuelas, facultades, CCH's y demás dependencias no cuentan con una infraestructura adecuada (Ancho de Banda y Switches).

- ✓ Muchas de las universidades e instituciones no cuentan con los recursos económicos suficientes y de conocimiento con respecto a este tipo de tecnologías o no existe un interés marcado.

- ✓ También he cierto que la implementación de VoIP en las redes universitarias representa un gran ahorro económico en llamadas nacionales como internacionales, ayudando a tener un mejor vínculo entre académicos, favoreciendo así a la realización de cualquier proyecto combatiendo una mas de sus múltiples limitantes.

- ✓ La implementación de la voz por IP es factible si y sólo si se tiene una buena estructura de red de datos y el instinto para detectar las grades expectativas que ésta arranca.

- ✓ Es necesario que se tenga muy en cuenta la tecnología llamada SIP ya que ésta es mucho más robusta y actualizable para innovar nuevos rumbos en las tecnologías y protocolos de VoIP siendo que fue elaborada exclusivamente para este propósito.

- ✓ Como conclusión final, la VoIP no vendrá a sustituir a la telefonía que actualmente usamos, aún hay mucho que indagar y probar para que se tenga mucho mejor desempeño en la actual red telefónica, un logro es que con esta clase de proyectos se forza a otras instituciones a tomar cartas en el asunto por el fuerte incremento de la utilización de la tecnologías de VoIP para mejorar sus servicios.

- ✓ Además de dejarme grandes satisfacciones personales, asi como un crecimiento profesional, gracias al proyecto alcancé un mayor entendimiento de las tecnologías de redes de datos y de voz, aprovechando los recursos que pude tener a mí alcance.

- ✓ Las conclusiones de esta tesis son satisfactorias ya que la viabilidad del proyecto satisfizo una amplia gama de posibilidades, con la presentación

de este proyecto se ha logrado el interés de muchas otras universidades a unirse a este proyecto, ya que el trabajo no termina solamente en la interconexión de ambas universidades (UNAM y la Universidad A&M de Texas), si no que ha crecido a otro proyecto que es la de hacer un gatekeeper Nacional que interconecte a otros gatekeeper de los miembros de CUDI, ya que no sólo impulsa a la UNAM sino la convierte en la iniciadora como coordinadora del grupo de Voz por IP a nivel CUDI.

BIBLIOGRAFÍA

GLOSARIO

BIBLIOGRAFÍA

Libros:

- **Anne Smith**
  Demystifying Convergence and VoIP
  Cisco Press http://www.ciscopress.com
  Primera Edición, 2001

- **Cisco Networking Academy Program**
  Cisco Networking Academy Program CCNA 1 and 2 Lab Companion
  Cisco Press http://www.ciscopress.com
  Tercera Edición, 2003
  SBN 1587131110

- **Craig Scanner**
  Manual de Referencia Redes
  MacGraw-Hill
  Primera Edición, 2002
  ISBN 8448136209

- **Gary Kessler,Peter Southwick**
  RDSI Conceptos, funcionalidad y servicios
  McGraw-Hill
  Primera Edición, 2001
  ISBN 8448128761

- **Jonathan Davidson, James Peters**
  Voice Over IP Fundamentals
  Cisco Press http://www.ciscopress.com
  Tercera Edición, 2000
  ISBN 1578701686

- **Scott Keagy**
  Integrating Voice and Data Networks
  Cisco Press http://www.ciscopress.com
  Primera Edición, 2000
  ISBN 1578701961

- **Steve McQuerry, Kelly McGrew, Stephen Foy**
  Cisco Voice over Frame Relay, ATM, and IP
  Cisco Press http://www.ciscopress.com
  Primera Edición, 2001
  ISBN 1578702275

Manuales y Tutoriales:

- **Understanding Cisco IOS Gatekeeper Call Routing**
  Cisco
  Cisco Web Site www.cisco.com

- **Understanding, Configuring and Troubleshooting Resource Allocation Indication**
  Cisco
  Cisco Web Site www.cisco.com

- **Required Cisco ITS Configuration**
  Cisco
  Cisco Web Site www.cisco.com

- **Tutorial H.323**
  IEC
  Web ProForum Tutorials www.iec.org/online/tutorials

- **Voice over Internet Protocol**
  IEC
  Web ProForum Tutorials www.iec.org/online/tutorials

Ligas de Internet:

Para capítulo uno:

- http://es.geocities.com/october_1975/telefon.htm
- http://www.alocybernet.com/tutoriales/inicio.htm
- http://www.mideplan.go.cr/PND-2002-2006/est-crec-gen-emp/Telecomunicaciones/Diagnostico-telecomunicaciones.htm

Para capítulo dos:

- http://enete.us.es/docu_enete/varios/redes/
- http://www.htmlweb.net/redes/osi/
- http://www.unet.edu.ve/materias/electronica/ing_redes/

Para capítulo tres:

- http://www.saulo.net/pub/tcpip/index.html
- www.protocols.com

Para capítulo cuatro:

- www.internet2.edu
- www.cudi.edu.mx

Para capítulo cinco:

- www.openh323.com
- www.iec.org
- www.cisco.com
- www.webnuevastecnologias.com/newtecnofr/docinteres/pdfmono5.pdf
- www.commlogik.com/programas/VOIP.pdf
- www.tmintl.agilent.com/upload/files/mx/Fund%20VoIP.pdf
- www.multiradio.com.ar/Soluciones/VoIP.htm
- www.comunicaciones.unitronics.es/Soluciones.htm
- www.recursosvoip.com/tutoria1/h323.php

GLOSARIO

Access Gateway Gateway de acceso. Un gateway es un elemento de la red que actúa como punto de entrada a otra red. Un access gateway es un gateway entre la red telefónica y otras redes como Internet.

ACD Automatic Call Distributor. Distribuidor automático de llamadas. Sistema telefónico especializado que puede manejar llamadas entrantes o realizar llamadas salientes. Puede reconocer y responder una llamada entrante, buscar en su base de datos instrucciones sobre qué hacer con la llamada, reproducir locuciones, grabar respuestas del usuario y enviar la llamada a un operador, cuando haya uno libre o cuando termine la locución.

ADPCM Adaptive Digital Pulse Code Modulation. Forma de codificar el sonido de forma que ocupe menos espacio.

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

ANI Automatic Number Identification. Detección del número que llama.

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

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

C7 Common Channel Signaling System No.7 Ver SS7.

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

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

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

Codec Codec. Algoritmos de Compresión/Descompresión. Se utilizan para reducir el tamaño de los datos multimedia, tanto audio como vídeo. Compactan (codifican) un flujo de datos multimedia cuando se envía y lo restituyen (decodifican) cuando se recibe. Entre los codec de audio más extendidos se encuentran: GSM (Global Standard for Mobile Communications), ADPCM, PCM, DSP TrueSpeech, CCITT y Lernout & Hauspie. Y entre los codec de vídeo tenemos a Cinepak, Indeo, Video 1 y RLE.

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

CT Computer Telephony. Añadir las posibilidades que ofrecen los ordenadores a la realización, recepción y manejo de las llamadas telefónicas.

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

DNIS Dialed Number Identification Service. Un servicio telefónico que permite al llamado saber el número marcado por el llamante. Es una prestación habitual en los números gratuitos (800 y 900), y permite identificar el número originalmente marcado cuando varios números 900 acaban en un mismo circuito. Funcionan pasando el número marcado al dispositivo destino de la llamada, que puede actuar en función de ese dato a la hora de enrutar, encolar o tratar la llamada en general. Un uso típico consiste en dar un tratamiento diferenciado a los usuarios llamantes en campañas de marketing o simplemente en las llamadas a un centro de llamadas (Call Center).

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

DSP Digital Signal Processor. Un microprocesador digital especializado que realiza cálculos o digitaliza señales originalmente analógicas. Su gran ventaja es que son programables. Entre sus principales usos está la

compresión de señales de voz. Son la pieza clave de los codec.

DTM Dynamic Synchronous Transfer Mode. Tecnología de conmutación de circuitos dinámica que proporciona transporte entre routers a través de canales, y permite el transporte óptico de información a altas velocidades. En DTM, un canal tiene un ancho de banda dedicado, y forma una ruta dinámica entre emisor y receptor, pasando a través de routers en su camino. Canales con cierta calidad de servicio (QoS) son establecidos 'al vuelo' y fijados de forma extremadamente rápida. Los routers utilizados a lo largo del camino pasan los datos de un enlace a otro, ya que no necesitan chequear las direcciones de los paquetes. Como no es necesario almacenar los paquetes en buffers, no los necesitan y no hay riesgo de sobrecarga de buffers, que podría causar pérdida de paquetes y congestión de red.

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

E1 Conexión por medio de la línea telefónica que puede transportar datos con una velocidad de hasta 1,920 Mbps. Según el estándar europeo (ITU), un E1 está formado por 30 canales de datos de 64 kbps más 2 canales de señalización. E1 es la versión europea de T1 (DS-1). Velocidades disponibles:
E1: 30 canales, 2,048 Mbps
E2: 120 canales, 8,448 Mbps
E3: 480 canales, 34,368 Mbps
E4: 1920 canales, 139,264 Mbps
E5: 7680 canales, 565,148 Mbps

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

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

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

Gateway En general se trata de una pasarela entre dos redes. Técnicamente se trata de un dispositivo repetidor electrónico que intercepta y adecua señales eléctricas de una red a otra. En Telefonía IP se entiende que estamos hablando de un dispositivo que actúa de pasarela entre la red telefónica y una red IP. Es capaz de convertir las llamadas de voz y fax, en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet. Originalmente sólo trataban llamadas de voz, realizando la compresión/descompresión, paquetización, enrutado de la llamada y el control de la señalización. Hoy en día muchos son capaces de manejar fax e incluir interfaces con controladores externos, como gatekeepers, soft-switches o sistemas de facturación.

GSM Global System for Mobile Communications. GSM es la tecnología telefónica móvil digital basada en TDMA predominante en Europa, aunque se usa en otras zonas del mundo. Se desarrolló en los años 80 y se desplegó en siete países europeos en 1992. Se utiliza en Europa, Asia, Australia, Norteamérica y Chile. Opera en las bandas de 900MHz y 1.8GHz en Europa y en la banda de 1.9GHz PCS en U.S.A. GSM define el sistema celular completo, no sólo el interface radio (TDMA, CDMA, etc.). En 2000 había más de 250 millones de usuarios GSM, lo que representa más de la mitad de la población mundial de usuarios de telefonía móvil. La codificación de audio del estándar GSM se utiliza en Telefonía IP y en la codificación de audio en ficheros WAV y AIFF.

H.323 H.323 es la recomendación global (incluye referencias a otros estándares, como H.225 y H.245) de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para las comunicaciones multimedia sobre redes basadas en paquetes que no proporcionan una Calidad de Servicio (QoS, Quality of Service) garantizada. Define las diferentes entidades que hacen posible estas comunicaciones multimedia: endpoints, gateways, unidades de conferencia multipunto (MCU) y gatekeepers, así como sus interacciones.

HDLC High Level Data Link Control. Protocolo desarrollado por ISO y basado en trabajos previos realizados por IBM sobre SDLC. Más información en http://www.protocols.com/pbook/

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

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

IETF Internet Engineering Task Force. Se reúne tres veces al año para fijar estándares técnicos sobre temas relacionados con Internet.

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

IP Internet Protocol. La parte IP del protocolo de comunicaciones TCP/IP. Implementa el nivel de red (capa 3 de la pila de protocolos OSI), que contiene una dirección de red y se utiliza para enrutar un paquete hacia otra red o subred. IP acepta paquetes de la capa 4 de transporte (TCP o UDP), añade su propia cabecera y envía un

	datagrama a la capa 2 (enlace). Puede fragmentar el paquete para acomodarse a la máxima unidad de transmisión (MTU, Maximum Transmission Unit) de la red. Dirección IP: un número único de 32 bits para una máquina TCP/IP concreta en Internet, escrita normalmente en decimal (por ejemplo, 128.122.40.227).
IP PBX	IP Private Branch eXchange. Centralita IP. Dispositivo de red IP que se encarga de conmutar tráfico telefónico de VoIP.
IP Telephony	Telefonía IP. Tecnología para la transmisión de llamadas telefónicas ordinarias sobre Internet u otras redes de paquetes utilizando un PC, gateways y teléfonos estándar. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional. Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.
ISDN	Integrated Services Digital Network (RDSI, Red Digital de Servicios Integrados). Red telefónica pensada para mejorar los servicios de telecomunicaciones a nivel mundial. Proporciona un estándar aceptado internacionalmente para voz, datos y señalización. Todas las transmisiones son digitales extremo a extremo, utiliza señalización fuera de banda, y proporciona más ancho de banda que la red telefónica tradicional. Más información en http://www.ralphb.net/ISDN/intro.html
ITU-T	International Telecommunications Union - Telecommunication. Antes conocida como CCITT (Comite Consultatif Internationale de Telegraphie et Telephonie). Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones: crea estándares, reparte frecuencias para varios servicios, etc. El grupo ITU-T recomienda estándares para telecomunicaciones y está en Génova (Suiza). También se encarga de elaborar recomendaciones sobre codecs (compresión/descompresión de audio) y modems.
IVR	Interactive Voice Response. IVR consiste en un conjunto de mensajes de voz y marcación de tonos desde un teléfono, de este modo se obtiene información del usuario llamante que en el destino sirve para la autenticación e identificación del mismo. También permite realizar transacciones totalmente automatizadas. Ultimamente las tecnologías de reconocimiento del habla están reemplazando a la detección de tonos DTMF, debido a la mejora en la fiabilidad que se ha conseguido.
J1	La versión japonesa del sistema E en Europa o T en Norteamérica. J1: 24 canales, 1.544 Mbps J2: 96 canales, 6.312 Mbps J3: 480 canales, 32.064 Mbps J4: 1440 canales, 97.728 Mbps J5: 5760 canales, 400.352 Mbps
LAN	Local Area Network. Red de área local. Una red pequeña de datos que cubre un área limitada, como el interior de un edificio o un grupo reducido de edificios.
LAPD	Link Access Protocol - Channel D. LAPD es un protocolo de nivel 2 definido en CCITT Q.920/921. LAPD funciona en Modo Asincrono Balanceado (ABM, Asynchronous Balanced Mode), siendo este modo totalmente balanceado, es decir, no hay relación maestro/esclavo.Más información en http://www.protocols.com/pbook/
LDAP	Lightweight Directory Access Protocol. Es un protocolo software que permite localizar a personas, organizaciones y otros recursos como ficheros o dispositivos en una red, bien en Internet o en una intranet. LDAP es una versión ligera del Protocolo de Acceso a Directorio (DAP), que a su vez es parte del protocolo X.500, un estándar para servicios de directorio en red. LDAP es más ligero porque es su versión inicial no incluía características de seguridad. Desarrollado originalmente en la Universidad de Michigan, actualmente lo utilizan más de 40 compañías en sus productos: Netscape lo incluye en la última versión del Comunnicator, Microsoft lo utiliza en su Directorio Activo y en Outlook Express. Novell en sus servicios de directorio NetWare y Cisco en sus equipos para redes. Un directorio LDAP está organizado en forma de árbol jerárquico y tiene los siguientes niveles: directorio raíz, países, organizaciones, departamentos y recursos individuales (personas, ficheros o recursos de red).
LEC	Local Exchange Carrier. Compañía que proporciona servicios telefónicos a nivel local.
Media Gateway	Denominación genérica para referirse a varios productos agrupados bajo el protocolo MGCP (Media Gateway Control Protocol). La principal misión de un Media Gateway es la conversión IP/TDM bajo el control de un Softswitch.
Media Server	Dispositivo que procesa aplicaciones multimedia como distribución de llamadas, fax bajo demanda y programas de respuesta a emails automática. Facilitan el mantenimiento y la administración, ofrecen menores costes y aportan mayor flexibilidad a la hora de desarrollar nuevas aplicaciones.
MEGACO	Media Gateway Control. MEGACO es un protocolo de VoIP, combinación de los protocolos MGCP e IPDC. Es más sencillo que H.323.
MGCP	Media Gateway Controller Protocol. MGCP es un protocolo de control de dispositivos, donde un gateway esclavo (MG, Media Gateway) es controlado por un maestro (MGC, Media Gateway Controller). Más información en http://www.cs.columbia.edu/~hgs/sip/
Module	Módulo. Una tarjeta que no puede trabajar sola, debe conectarse a otra tarjeta.
Multi-Service Access Switch	Punto de acceso de los usuarios a redes de banda ancha.
Multi-Service Router	Un tipo de router que examina las llamadas en la red telefónica antes de que sean enviadas a un destino concreto. Se basa en un enlace especial de señalización que llega de la centralita y permite que un sistema de

pre-enrutamiento reciba dicha señalización, examine el estado actual del call center y le devuelva una notificación a la centralita para que ésta envíe la llamada al destino elegido. La ventaja es que la llamada es enrutada o desviada antes de aceptarla. También es posible realizar un post-enrutamiento cuando no es posible tomar la decisión sobre el destino final de la llamada hasta que ésta alcance un destino concreto.

NAT Network Address Translation. Un estándar definido en la RFC 1631 que permite a una red de área local (LAN) utilizar un conjunto de direcciones IP internamente y un segundo conjunto de direcciones externamente. El dispositivo que hace NAT se sitúa en el punto de salida a Internet y realiza todas las traducciones de direcciones IP que sean necesarias. NAT se incluye normalmente en los routers y en algunos firewalls. NAT tiene básicamente tres propósitos:
1.-Proporcionar funcionalidad de firewall al ocultar las direcciones IP internas.
2.-Permitir a una compañía utilizar todas las direcciones IP internas que desee sin posibilidad de conflicto con otras compañías y un conjunto limitado de direcciones externas.
3.-Combinar varios tipos de conexiones (normalmente RDSI) en una única conexión a Internet.

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

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

PSTN Public Switched Telephone Network. Red telefónica convencional.

Router Un dispositivo físico, o a veces un programa corriendo en un ordenador, que reenvía paquetes de datos de una red LAN o WAN a otra. Basados en tablas o protocolos de enrutamiento, leen la dirección de red destino de cada paquete que les llega y deciden enviarlo por la ruta más adecuada (en base a la carga de tráfico, coste, velocidad u otros factores). Los routers trabajan en el nivel 3 de la pila de protocolos, mientras los bridges y conmutadores lo hacen en el nivel 2.

RTP Routing Table Protocol. Protocolo telefónico que hace uso de una lista de instrucciones o tabla que le indica cómo manejar llamadas telefónicas entrantes.

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

SCCP Signaling Connection Control Part. SCCP proporciona servicios de red, tanto orientados a conexión como no orientados a conexión, sobre el nivel 3 de MTP. Más información en http://www.pt.com/tutorials/ss7/

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

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

SCTP Simple Control Transmission Protocol. SCTP es un protocolo de transporte fiable, diseñado para trabajar sobre redes de paquetes no orientadas a conexión, como IP. Más información en http://www.ietf.org/ids.by.wg/sigtran.html

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

SDP Session Description Protocol. SDP lo utiliza SIP para describir las capacidades multimedia de los participantes en la llamada y negociar un conjunto común de capacidades multimedia a utilizar. Más información en http://www.cs.columbia.edu/~hgs/sip/

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

SGCP Simple Gateway Control Protocol. SGCP es un protocolo utilizado con SGCI para controlar Gateways VoIP desde elementos de control de llamada externos. Más información en http://www.argreenhouse.com/SGCP/sgcp-v1-0.html

SIP Session Initiation Protocol. SIP es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Un estándar de la IETF (Internet Engineering Task Force) definido en la RFC 2543. SIP se utiliza para iniciar, manejar y terminar sesiones interactivas entre uno o más usuarios en Internet. Inspirado en los protocolos HTTP (web) y SMTP (email), proporciona escalabilidad, flexibilidad y facilita la creación de nuevos servicios. Cada vez se utiliza más en VoIP,

gateways, teléfonos IP, softswitches, aunque también se utiliza en aplicaciones de vídeo, notificación de eventos, mensajería instantánea, juegos interactivos, chat, etc. Más información en http://www.cs.columbia.edu/~hgs/sip/

SS7 Common Channel Signaling System Nº 7. SS7 es un estándar global para telecomunicaciones definido por la Unión Internacional de Telecomunicaciones (Sector de Estandarización de Telecomunicaciones). Define los procedimientos y protocolos mediante los cuales los elementos de la Red Telefónica Conmutada (RTC o PSTN, Public Switched Telephone Network) intercambian información sobre una red de señalización digital para establecer, enrutar, facturar y controlar llamadas, tanto a terminales fijos como móviles. Más información en http://www.pt.com/tutorials/ss7/

T1 Un circuito digital punto a punto dedicado a 1,544 Mbps proporcionado por las compañías telefónicas en Norteamérica. Más información en Newton's Telecom Dictionary. Ver E1 y J1 para los equivalentes europeos y japonés, respectivamente. Permite la transmisión de voz y datos y en muchos casos se utilizan para proporcionar conexiones a Internet.
T1(DS1):24 canales, 1,544 Mbps
T2(DS2):96 canales, 6,312 Mbps
T3(DS3):672 canales, 44,736 Mbps
T4(DS4): 4032 canales, 274,176 Mbps

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

TDMA Time Division Multiple Access. Tecnología para la transmisión digital de señales de radio; por ejemplo, entre un teléfono móvil y una estación radiobase. En TDMA, la banda de frecuencia se divide en un número de canales que a la vez se agrupa en unidades de tiempo de modo que varias llamadas pueden compartir un canal único sin interferir una con otra. TDMA es también el nombre de una tecnología digital basada en la norma IS-136. TDMA es la designación actual para lo que anteriormente era conocido como D-AMPS.

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

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

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

VoIP Voice Over IP (Voz sobre IP). Tecnología que permite la transmisión de la voz a través de redes IP, Internet normalmente. La Telefonía IP es una aplicación inmediata de esta tecnología.

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

WAP Wireless Application Protocol. Un protocolo gratuito y abierto, sin licencia, para comunicaciones inalámbricas que hace posible crear servicios avanzados de telecomunicación y acceder a páginas de Internet desde dispositivos WAP. Ha tenido gran aceptación por parte de la industria. Más información en http://www.wapforum.org/what/index.htm

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

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

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