Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Escuela de Ingeniería Mecánica Eléctrica

IMPLEMENTACIÓN Y TRANSMISIÓN DE VOZ SOBRE PROTOCOLO DE INTERNET A TRAVÉS DE UNA RED LAN/WAN

Alvaro Castillo Castillo

Asesorada por Ing. Jacobo Estuardo Ponce Chavarría

Guatemala, octubre de 2004

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Ancho de banda Es una medición de la capacidad de información de un enlace de comunicación. Es la diferencia entre la frecuencia más alta y la frecuencia más baja de un enlace de comunicación, y se mide en Hertz.

ARP Protocolo de resolución de dirección (de sus siglas en inglés).

Atenuación Reducción de la potencia de la señal, a medida que viaja por el cable, se expresa en términos de dB/100m por metro. A menor gama de dB, el cable es mejor.

ATM Modo de Transferencia Asíncrono (de sus siglas en inglés). Modo de transmisión en el que la información se organiza en celdas. Las celdas tienen 53 *bytes* de longitud y acceden a la red a través de conexiones virtuales.

Codec Dispositivo que realiza funciones de codificación, decodificación y compresión mediante algoritmos y circuitos que conducen la conversión de la señal analógica a digital y viceversa.

Dirección MAC Dirección de control de acceso medio (de sus siglas en inglés). Conocido como dirección de *hardware* o dirección física. Es una dirección asociada con un dispositivo de red en particular.

FTP Protocolo de transferencia de archivos (de sus siglas en inglés). Procedimiento que se utiliza para descargar archivos públicos de una computadora remota a una local.

Internet Es una red de cómputo a nivel mundial que agrupa a distintos tipos de redes usando un mismo protocolo de comunicación. Los usuarios en Internet pueden compartir datos, recursos y servicios. Internet se apoya en el conjunto de protocolos TCP/IP. De forma más específica, Internet es la WAN más grande que hay en el planeta.

Intranet Una red privada dentro de una compañía u organización que utiliza el mismo *software* que se encuentra en Internet, pero que es sólo para uso interno en una empresa.

E1 Conexión por medio de la línea telefónica que puede transportar datos con una velocidad de hasta 1,920 Mbps. Según el estándar europeo, 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).

Latancia Es el tiempo que toma una señal digital en atravesar el sistema desde la fuente hasta la aplicación final correspondiente. Es una característica propia del sistema. Es un retardo fijo.

T1 Un circuito digital punto a punto dedicado a 1,544 Mbps proporcionado por las compañías telefónicas en Norteamérica. 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.

RESUMEN

Con el desarrollo de las telecomunicaciones y en particular de Internet, una de las propuestas a nivel mundial que se ha venido desarrollando, es la de poder manejar voz sobre una red de datos.

Los problemas generados por la diversidad del gran número de redes de telecomunicaciones existentes, están motivando el estudio de mecanismos que favorezcan el homogenizar los medios de transporte de voz y datos utilizando redes LAN y WAN ya existentes. En el capítulo 1 del presente trabajo se establecen todas las definiciones teóricas y conceptos fundamentales de redes estructuradas por donde viaja la información.

La tecnología de Voz sobre IP (VoIP) pretende hacer convivir en la misma línea la voz y los datos utilizando los protocolos de transmisión existentes, protocolos que se estudian en el capítulo 2.

La VoIP se trata de una tecnología que permite comprimir la voz, empaquetarla y transmitirla, para que sea recibida del otro lado por algún tipo de equipo que convierta los paquetes de nuevo en voz. Este trabajo presenta la implementación de VoIP (*voice over internet protocol*) como una posible solución a este problema y se desarrolla también una primera aproximación al concepto de la terminología de la convergencia de redes. Todos estos temas son desarrollados en los capítulos 3 y 4.

Finalmente en el capítulo 5, se aporta un sencillo análisis de la situación actual de VoIP en el ámbito legal.

OBJETIVOS

- **General**

Realizar un estudio de la tecnología VoIP y su aplicación para transmitir voz a través de las redes de datos para su futura implementación.

- **Específicos**

1. Aprovechar la actual red de datos estructurada para transmitir datos y voz canalizados con protocolo IP. De tal forma que todo se unifique en una sola estructura simple, en una LAN *ethernet*.
2. Determinar las ventajas y desventajas de la tecnología VoIP.
3. Establecer los estándares que se utilizan en la transmisión de VoIP.
4. Analizar la regulación de VoIP y sus implicaciones en la interconexión de redes.

INTRODUCCIÓN

El crecimiento de las redes IP, tanto en área local como en área geográficamente lejana, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir voz sobre IP.

Si a todo lo anterior, se le suma el fenómeno de Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar consigo, la transmisión de voz sobre Internet es algo que resulta estratégico para las empresas modernas. Ya que la posibilidad de estar comunicados a costos más bajos dentro de las empresas y fuera de ellas, es la puerta de entrada de nuevos servicios. Lentamente la telefonía sobre IP está ganando terreno y todos quieren implementarla sobre la red LAN que la mayoría de empresas utiliza para la transmisión de datos.

El concepto original es relativamente simple: se trata de transformar la voz en “paquetes de información” manejables por una red LAN que utilice el protocolo internet (IP), materia que también incluye a las intranets y extranets. Gracias a otros protocolos de comunicación como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

La voz puede ser obtenida desde un micrófono conectado a una computadora, o bien desde un teléfono común. Para todo esto existen *gateways* (dispositivos de interconexión) que permiten intercomunicar las redes de datos.

De hecho, este sistema telefónico digital, una vez alcanzado el servidor más próximo al destino de la llamada telefónica, es capaz de traducir como información analógica y transmitirla hacia un teléfono común por la red telefónica tradicional. Vale decir que se puede mantener conversaciones teléfono a teléfono.

Ciertamente, existen objeciones de importancia que tienen que ver con la calidad del sistema y con el tiempo entre fallas de las redes LAN en comparación con las de telefonía. Sin embargo, la versatilidad y los costos del nuevo sistema hacen que los proveedores de servicios de Internet estén considerando la posibilidad de dar servicios sobre IP.

Sin lugar a dudas, los primeros que van a aprovechar las ventajas de voz sobre IP serán las grandes compañías que, en general, se encuentran geográficamente distribuidas y que tienen la posibilidad inmediata de explotar sus redes de datos LAN y WAN corporativas ya existentes.

1. DEFINICIONES TEÓRICAS Y COMPONENTES DE UNA RED DE DATOS

Una manera de pensar en redes es imaginársela como un equipo. Un equipo en el que se comparte tiempo, información y recursos para alcanzar una meta u objetivo. En su nivel más elemental, una red consiste en computadoras conectadas entre sí con un cable que les permite compartir datos. Todas las redes de computadoras, independientemente de su nivel de sofisticación, surgen de ese sistema tan simple que nace de la necesidad de compartir datos de forma rápida.

Las computadoras en forma personal pueden procesar y manipular rápidamente grandes cantidades de datos, pero no permiten que los usuarios compartan los datos de forma eficiente, lo que en el pasado les obligaba a imprimir los documentos o bien copiar los archivos en discos magnéticos para que otras personas pudieran editarlos y utilizarlos. En otras palabras, las computadoras trabajaban en un entorno totalmente independiente.

Con la disponibilidad y la gran capacidad de las computadoras personales, al utilizar redes de datos se traduce en un gran aumento de eficiencia y en la reducción de costos, objetivos que se alcanzan de tres formas diferentes: compartiendo información (datos), compartiendo *hardware* y *software* y finalmente, centralizando la administración y el soporte.

1.1 Definición de una red de área local (LAN)

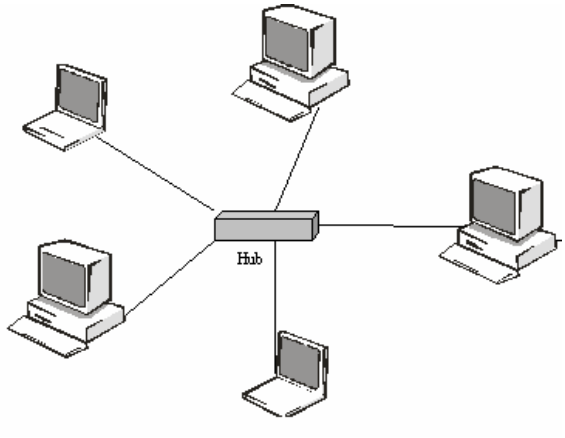
Una red de área local (LAN – *local area network*) consiste en un sistema de interconexiones de servidores o computadoras a través de un medio físico restringido a un área determinada, que puede ser una sola oficina, varias oficinas e incluso una interconexión entre edificios. Incluso una LAN puede ser tan simple y conformar 2 computadoras, o tan compleja que conecte a cientos de computadoras y periféricos.

Una LAN es un sistema eficiente de cableado para permitir el movimiento de información entre usuarios y compartir, no sólo esa información, sino también los recursos de *hardware* como lo son: impresoras, *módems*, discos duros de otra computadora, etc.

Algunos de los componentes universales que involucra una red LAN son los dispositivos de *interfaces* en cada computadora, los protocolos de transmisión de datos y el *software* de interpretación y administración de la red. El nivel de la administración de la red depende del tipo, configuración y número de usuarios involucrados que, en algunos casos puede ser considerable.

Alguna definición de LAN indica que una red de este tipo es toda aquella que conecta usuarios y sistemas dentro de un radio de 10 kilómetros. En la Figura 1 se muestra el esquema de una red LAN sencilla.

Figura 1. Red de área local - LAN



1.1.1 Tipos de cables

El sistema de cableado es el nivel físico de una red y está determinado por el tipo de cable y la topología que utiliza. En la actualidad se dispone de 4 tipos básicos de cable mismos que se detallan a continuación:

a) **Par trenzado sin apantallar** (UTP- *unshielded twisted pair*). Consiste en una manguera flexible en el interior de la cual se ubican 8 cables 22/24 AWG, repartidos en pares (4 pares) cada uno de los cuales va entrelazado entre sí. Es el más barato en cuanto a precio de compra e instalación. Permite velocidades de transmisión 100 Mhz sobre distancias de 100 metros.

b) **Par trenzado apantallado** (STP – *shielded twisted pair*). Al igual que el UTP consta de 4 pares de cables 22 AWG trenzados pero cubiertos con una pantalla o malla protectora alrededor. Años atrás tenía la ventaja, sobre el UTP, de poder superar los 100 Mhz. Hoy, con las nuevas tecnologías de cableado, esto ya no es así.

c) **Cable coaxial**. Este tipo de cable está disponible en varios diámetros. A mayor diámetro mayor capacidad de transmisión de datos, pero con el inconveniente de que es caro tanto el cable como los conectores. El cable coaxial se desestima debido a su alto costo de instalación y su baja adaptabilidad, pues básicamente permite utilizar topología de bus o sus derivados, sobre lo cual se ampliará más adelante.

d) **Fibra óptica**. Aunque la fibra óptica necesita dispositivos especiales (transreceptores) que conviertan las señales eléctricas en luz y viceversa es, entre todos los tipos de cable, el que permite mayor capacidad de transferencia de datos y a mayor distancias, con pérdidas mínimas en comparación al resto de tipos de cable. La fibra óptica constituye el medio ideal, dado que permite un ancho de banda más que suficiente para velocidades requeridas, incluso en los sistemas más avanzados (por encima de los 600 Mhz). Pero como inconveniente tiene el elevado costo de los transductores de señal.

Existen otros métodos de transmisión sin cable como las redes inalámbricas (infra-rojos y radiofrecuencia).

1.1.2 Cable UTP en cableado de redes

El cableado estructurado, como se le llama actualmente a una red física de cable para transporte de datos, cuenta con una tecnología que actualmente lo coloca a la par de los demás integrantes de la red (equipos, protocolos, *software*, etc.), por lo que es un componente fundamental en una infraestructura de comunicaciones; a tal punto que los servicios que utilizan los usuarios pueden estar delimitados por dicho componente.

Una red estructurada debe ser un sistema transparente al servicio de las comunicaciones permitiendo el paso de voz, datos o video por un mismo cable, y además debe prever las futuras ampliaciones o modificaciones de dicha infraestructura.

Entre el cable coaxial, la fibra y el cable de pares, está claro que el cable de pares además de ofrecer un ancho de banda muy elevado, ofrece bajo costo en su instalación y el tipo de conector que utiliza, siendo éste el conocido como RJ-45.

El cable a utilizar por excelencia es el par trenzado sin blindaje, conocido simplemente como UTP de cuatro pares.

1.1.2.1 Evolución del cable UTP

A lo largo de la historia de los cables UTP ha existido una evolución debido a una progresiva disminución en la atenuación de la diafonía (ruido eléctrico inducido entre pares adyacentes y que es eliminado por el entrelazado con un número de diferentes vueltas de los pares), así como un progresivo aumento en banda de frecuencias para su utilización. Por lo que se conocen las siguientes categoría de cable UTP:

- Anteriores a la categoría 3. Utilizados para la transmisión de voz análoga y transmisión de datos a baja velocidad.
- Categoría 3. Utilizados para voz análoga y digital, así como transmisión de datos hasta los 10 Mhz.
- Categoría 4. Utilizados para voz análoga y digital, así como transmisión de datos hasta los 20 Mhz.

- Categoría 5 y 5e. Indicados para voz análoga y digital, así como transmisión de datos hasta los 100 Mhz.
- Categoría 6. Esta categoría recién empieza a utilizarse y es ideal para voz análoga y digital, así como transmisión de datos de muy alta velocidad hasta los 200 Mhz

1.1.2.2 Factores de transmisión

Los factores de transmisión son los factores que limitan la transmisión de una señal a través del UTP. A continuación se definen los más importantes:

a. **Atenuación**. Mide la pérdida de la señal con la distancia. La atenuación aumenta con la frecuencia (a mayor frecuencia, mayor atenuación).
   Se mide en decibelios (dB) y es aconsejable que sea lo más baja posible. Cuanto menor sea, más fuerte será la señal.
b. **Diafonía de extremo cercano** (*NEXT*). Se produce cuando la señal de un par se acopla o filtra a otro par. El *NEXT* es ruido, se mide en decibelios y su valor refleja lo que se atenúa esa señal indeseada por lo que cuanto mayor sea el valor *NEXT*, tanto mejor.
c. **Relación entre atenuación y diafonía** (ACR). Es una forma sencilla de medir el ancho de banda disponible, cuanto mayor sea la diferencia entre uno y otro, mayor es el ancho de banda del que se dispone.

1.2 Topologías de una red LAN

Topología es la forma en que se estructura físicamente una red, cómo se distribuye la señal a las computadoras o equipos y de qué forma se interconectan entre sí. La topología de una red afecta a sus capacidades y la selección de una topología tendrá impacto sobre:

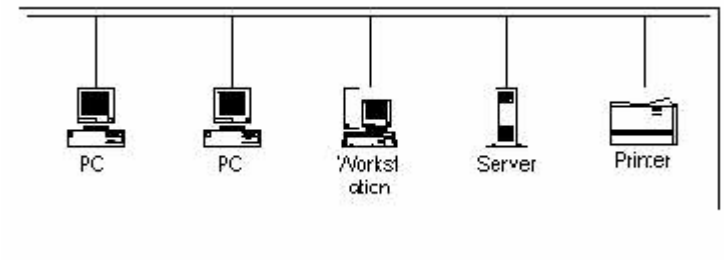
- El tipo de equipo que necesita la red, ya que difieren los métodos de comunicación.
- El crecimiento de la red.
- Las formas de gestionar la red.

1.2.1 Topología en bus

La topología bus consta de dispositivos conectados a un cable común compartido y también conocida como bus lineal porque los equipos se conectan en línea recta. Este método es el más simple en las redes de equipos y consta de un único cable llamado segmento central o *backbone* (columna vertebral) que conecta todos los equipos de la red en una única línea. En la figura 2 se muestra una red con topología de bus.

Tiene la ventaja de ser un sistema fácil de implementar. Si un equipo falla no se ve afectada. Sin embargo, existe restricción de longitud y para poder prolongarla es necesario utilizar equipo. No existe una administración centralizada. En la actualidad se está dejando de usar.

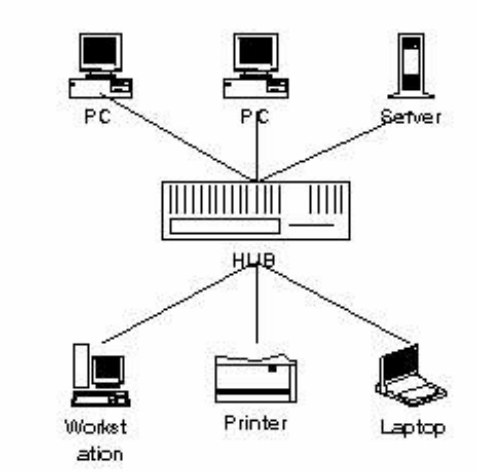
Figura 2. Red con topología en bus



1.2.2 Topología en estrella

En esta topología, los segmentos de cable de cada equipo están conectados a un componente centralizado llamado *hub*. Las señales son transmitidas desde el equipo emisor a través del *hub* a todos los equipos de la red. La figura 3 muestra un ejemplo de este tipo de topología.

Figura 3. Red con topología en estrella



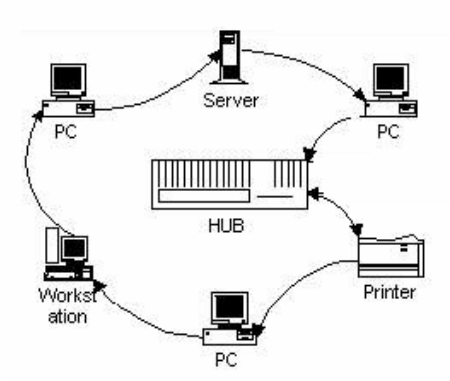
La ventaja que ofrece es que centraliza los recursos y la gestión. Sí un equipo falla (o el cable que lo conecta al *hub*), el resto de la red continuará funcionando normalmente. Por otro lado, la principal desventaja es que sí el *hub* falla la red falla. En algunas ocasiones el costo inicial es alto.

1.2.3 Topología de anillo

La topología en anillo conecta equipos en un único círculo de cable. La señal viaja a través del bucle en una dirección y pasa a través de cada equipo que puede actuar como amplificador de la señal y enviarla al siguiente equipo. La figura 4 muestra una red de topología en anillo.

Posee la ventaja de tener un bajo costo de instalación y diseño sencillo. Y su desventaja es que sí un nodo o equipo se cae, toda la red se cae y no hay comunicación.

Figura 4. Red con topología en anillo

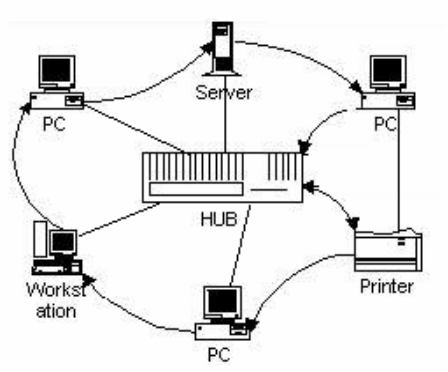


1.2.4 Topología de malla

Esta topología ofrece una redundancia y fiabilidad superiores porque cada equipo está conectado a todos los demás mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red, de modo que sí falla un cable, otro se hará cargo del tráfico.

Esto viene a ser una ventaja porque brinda una gran facilidad para la solución de problemas y una alta confiabilidad. La desventaja de esta topología es su elevado costo de instalación, ya que utilizan mucho cableado. En la figura 5 se muestra una red de malla.

Figura 5. Red con topología en malla



1.3 Componentes de una red LAN

Un sistema de cableado estructurado es la base de una red LAN moderna y consiste en una instalación de red, con puestos de trabajo cuya función irá determinada según la asignación que se dé a cada uno de estos puestos de trabajo desde un centro de cableado. Es decir, consiste en un sistema modular, en el que un punto por ejemplo, RJ45, puede ser de voz, de datos, etc., dependiendo del servicio asignado en el centro de cableado.

El cableado estructurado permite que un usuario que disponga, por ejemplo de una toma doble, pueda tener un puesto de datos y otro de voz, o dos de voz o dos de datos, dependiendo de sus necesidades en cada momento.

Para entender cómo funciona el sistema de cableado estructurado, hay que decir que consiste básicamente en un armario repartidor, donde se ubica toda la electrónica de red (*hub* y *switch*) y los paneles de puestos de trabajo.

Desde ese armario parten los cables que van a cada uno de los puestos de trabajo, pero en vez de partir el cableado a los puestos de datos directamente desde el *hub* o los de voz directamente desde la central telefónica,

lo que se hace es parcharlos. Normalmente se instalan en la parte posterior del armario repartidor, unos paneles para determinado número de usuarios desde los que parten los cables a cada uno de los puestos de trabajo.

Desde la parte de atrás de este panel se poncha el cable (normalmente UTP) y va a parar en el otro extremo al módulo que está en el interior de la roseta o caja, junto al puesto de trabajo determinado. Sí esta roseta ha de ser de datos o de voz, lo decidirá el usuario mediante un cable de parcheo, que conectará por un lado a la parte frontal del panel que está en el armario y por otro al *hub* (para dar suministro de datos) o al panel de la central telefónica (para dar suministro de voz).

Una red LAN puede que ocupe una ha*bit*ación pequeña, una sala grande, una oficina completa, varios niveles de un edificio, o incluso varios edificios separados entre sí. Sí este fuera el caso, normalmente en cada nivel de un edificio suele haber un armario repartidor que da servicio a sus correspondientes puestos de trabajo.

Para definir como interconectar los puestos entre sí en un mismo nivel, y entre los distintos armarios de distintos niveles, y entre distintos edificios, el sistema de cableado estructurado se divide en una serie de subsistemas.

Cada subsistema tiene una variedad de cables y elementos diseñados específicamente para dar una solución lo más económica posible para esa área determinada.

1.3.1 Subsistema de usuarios

El puesto del usuario, que va desde la toma de la tarjeta de red de la computadora hasta la toma de la pared. Sí se habla de cableado estructurado con cable UTP, se encontrará una tarjeta de red con adaptador RJ45 o bien modernos equipos con tomas para fibra óptica. En la figura 6 se muestra una toma de red conjuntamente con el cableado horizontal de la red.

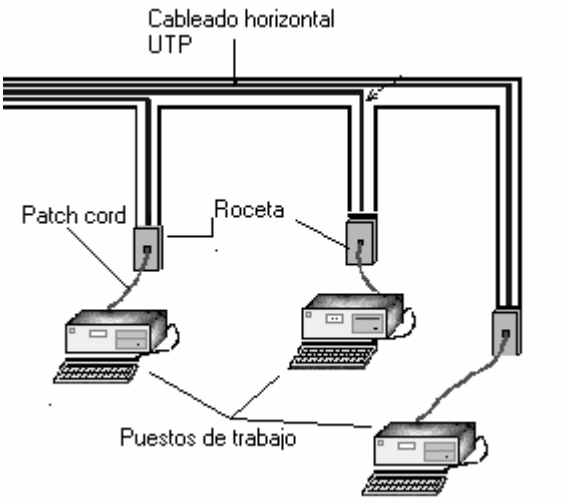
1.3.2 Subsistema horizontal

Es la conexión entre la toma del usuario y el panel del armario repartidor. Normalmente, sí no hay una distancia mayor a 90 metros, se utiliza cable de par trenzado (UTP o STP) que por un lado está ponchado a la toma de la roseta del puesto de trabajo y por el otro al panel del armario. Sí la distancia es mayor a los 90 metros, se puede encontrar cable coaxial RG58 hasta un máximo de 185 metros, o incluso con fibra óptica para distancias mayores.

Esta es una parte delicada de la red. La canalización del cableado siempre debe incluir tubería dedicado únicamente a llevar cableado de datos. Debe estar lo más separado posible de tomas de alta tensión, calor y maquinarias que emitan algún tipo de radiación. La radiación induce ruido que a su vez genera errores en la información que se transmite a través de la red.

El subsistema horizontal, como el que se muestra en la figura 6, es la parte de una red que exige siempre ser certificada puesto a puesto, pasando unas normas especificadas y estandarizadas para cable categoría 5, 5e o 6.

Figura 6. Subsistema horizontal



1.3.3 Subsistema de administración

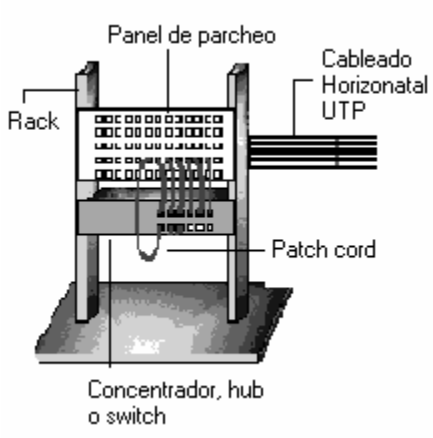
El subsistema de administración son todos los cables que se encuentran en el armario repartidor o *rack* y las asignaciones y/o interconexiones entre paneles, electrónica de red, centrales telefónicas, *módems*, etc., que hay efectuadas en ese armario.

La ubicación de los elementos de un subsistema de administración suele ser la siguiente: en la parte superior de un armario, de arriba abajo y con espacio para crecimiento, se instalan los paneles de puestos de usuario y los paneles de enlace con otros armarios. Después la electrónica de red, según la importancia de cada uno de los elementos que se instalen (primero un *switch*, luego un *hub*, etc.).

Los paneles de usuario son los que permiten asignar un servicio u otro, indistintamente a un puesto de trabajo. Mediante los cables de interconexión, de parcheo o *patch cords*, que en sus extremos cuentan con conectores RJ45, se

puede dar servicio desde un *hub*, desde un *switch*, desde una planta telefónica, etc. La figura 7 muestra el esquema de una armario.

Figura 7. Subsistema de administración



1.3.4 Subsistema vertical

El subsistema vertical también es conocido como *backbone* o troncal. Es el enlace entre los distintos subsistemas administrativos, o para decirlo de otra manera, el enlace entre los diferentes armarios de cada una de los niveles, que normalmente son enlazados con un armario repartidor principal, al cual están conectados directamente los servidores. Aunque comúnmente se utiliza cable de cobre UTP/STP, la tendencia es la utilización de fibra óptica.

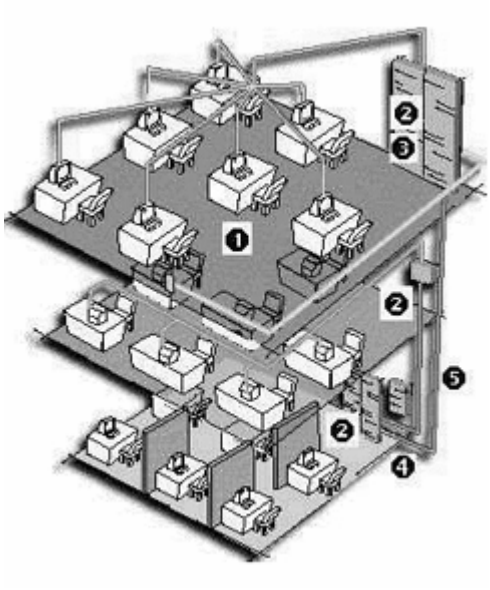
El hecho de que se utilice cada vez más la fibra óptica para enlazar armarios entre sí, viene dado por una serie de ventajas frente a la “teórica” desventaja de su precio.

La fibra óptica es inmune a las interferencias magnéticas, lo que no puede decirse del cable de cobre, cualquiera que sea el tipo. La fibra tiene un elevado ancho de banda y un diámetro menor al cable de par trenzado. Una fibra normal (de 62 a 90 micrómetros) puede transportar perfectamente 500

veces la información de un par de hilos de cobre. No tiene problemas de distancias, ya que las pérdidas de la fibra óptica se pueden notar en kilómetros, no en metros, y aún así son mínimas.

En cuanto a la velocidad y al ancho de banda, la fibra óptica es la solución ideal. En la figura 8 se muestra un subsistema vertical de un edificio.

Figura 8. Subsistema vertical



1.3.5 Subsistema campus

Finalmente el subsistema campus interconecta distintos edificios en una zona geográfica determinada. El enlace se hace, normalmente, uniendo entre sí los armarios principales de cada uno de los edificios. Se crea una red corporativa de área extensa. El medio físico por definición es la fibra óptica.

1.4 Electrónica de una red LAN

Para interconectar las redes locales existen diversos elementos, dependiendo del tipo de conexión que se quiera efectuar, del protocolo que utilicen unas y otras, etc. Se emplean dispositivos como *hub*s, *routers*, *gateway*s, tarjetas de red, etc. Dentro de cada uno de los elementos citados existe una gran variedad, que permite definir la finalidad y prestaciones de la red que monta.

Hoy en día, debido a las prestaciones y servicios tan elevados que se les exigen a las redes, se hace necesaria la instalación de dispositivos que permitan desde segmentar una red (*bridges*), hasta ampliar la distancia entre distintos servidores de la red (repetidores o *hub*s).

1.4.1 *Hub*

El *hub* también conocido como concentrador, ofrece un punto de conexión central, es decir, que centraliza las conexiones de red, eliminando de esta forma la problemática principal que ofrecen las topologías de bus y anillo, y utilizando por tanto las ventajas de una topología en estrella.

Técnicamente, un *hub* ofrece un enlace de comunicación para una determinada cifra de dispositivos. A cada una de las entradas se les llaman puertos. En este sentido, los *hub*s suelen tener puertos por lo general entre 8, 12 y 24 puertos.

El concentrador se usa como un lugar central donde conectar a los usuarios y los nodos de la red para gestionarla más fácilmente.

Además, los *hub*s pueden conectarse a otros concentradores, de forma que podamos crear una ramificación que nos proporciona flexibilidad para crecer de acuerdo a las necesidades de la instalación.

Existen algunos concentradores activos los cuales realizan funciones de amplificación y repetición de la señal; existen también concentradores pasivos que se limitan a efectuar el concentrado de cableado. Normalmente, estos dispositivos constan de puertos RJ45 que deberían soportar tanto 10 como 100 Mbps. Cada puerto detecta automáticamente la velocidad a la que opera el dispositivo conectado. Actualmente los concentradores son perfectamente administrables mediante una navegador *web* o una conexión serial.

1.4.2 *Switch*

El *switch* o conmutador realiza una función similar a la de un *hub*, conectando las computadoras a la red. Pero un *switch* es mucho más inteligente que un *hub* pasivo. En vez de dejar pasar el tráfico de red sin examinarlo, como hace un *hub*, un *switch* crea un circuito virtual entre el cliente y su destino, asegurando un porcentaje determinado del ancho de banda disponible.

En el medio compartido de un segmento *ethernet* conectado con un *hub*, todos sus vecinos compiten por la misma cantidad limitada de ancho de banda. Aunque un *switch* es más caro que un *hub*, puede aliviar la congestión en redes de alto tráfico.

Un *switch* por lo general, dispone de puertos auto-sensores 10/100 Mbps para mayor flexibilidad al migrar de *ethernet* 10 Mbps a *Fast ethernet* 100 Mbps. Para ser realmente flexible, el *switch* debería soportar 1024 direcciones

de control de acceso al medio (MAC). Como cada puerto soporta múltiples direcciones MAC, el *switch* ofrece a los administradores la posibilidad de conectar un *hub* (con varias computadoras) a un puerto dedicado del *switch*.

Para incrementar la densidad de puertos, el *switch* le permite apilar unidades adicionales mediante un conector de bus de alta velocidad. Tres puertos de alta velocidad facilitan al *switch* conectarse a otros dos segmentos y un servidor local, usando *Fast ethernet*, ATM, *Gigabit ethernet* o FDDI.

1.4.3 *Router*

Un *router* o enrutador es un conmutador de paquetes que opera a nivel de red y que permite interconectar tanto redes de área local como redes de área extensa. Así mismo, un *router* proporciona un control del tráfico y funciones de filtrado a nivel de red, es decir, trabaja con direcciones de nivel de red, como por ejemplo, con direcciones IP.

El *router* es capaz de encaminar dinámicamente, es decir, es capaz de seleccionar el camino que debe seguir un paquete en el momento en el que le llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

El *router* incluso es más inteligente que un *switch*, ya que además de leer direcciones MAC, analiza la información contenida en un paquete de red. El *router* lee cada paquete y lo envía a través del camino más eficiente posible al destino apropiado, según una serie de reglas recogidas en sus tablas.

Estos equipos se utilizan a menudo para conectar redes geográficamente separadas usando tecnologías como T1, E1, etc.

Un *router* ubicado en una sucursal es la conexión vital con las oficinas centrales y utiliza cualquier tipo de compresión para minimizar el ancho de banda de la red de área extensa. A la vez tiene la capacidad de saber cuándo mantener el tráfico de la red local dentro de ésta o conectarlo a la oficina central.

Uno de los mejores *routers* es el que soporta cualquier conexión de red de área extensa, usando los protocolos de red más comunes, IPX/SPX y TCP/IP, para una fácil integración con casi cualquier red. El *router* es capaz de soportar gestión remota.

1.4.4 Repetidor

Es un dispositivo que se interpone entre tramos de segmentos de cable muy largos para amplificar la señal que se transmite por el medio, para que así no se debilite y logre llegar hasta el siguiente nodo o repetidor.

1.4.5 Tarjeta de red

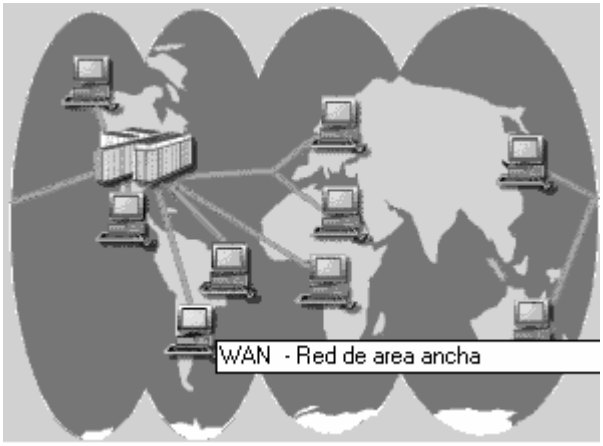
Es la tarjeta que tiene cada computadora para que ésta sea capaz de establecerse en la red. Es muy importante que a la hora de seleccionar la tarjeta de red se tenga en cuenta la velocidad a la que va a funcionar la red y el tipo de conector que utiliza.

1.5 Definición de una red de área extensa (WAN)

La red de área extensa (*wide area network*) es la que conecta un mayor número de equipos y computadoras y ocupa una extensión geográfica más extensa que las LAN. No existe un criterio objetivo para definir cuando una red pertenece a un tipo u otro, aunque generalmente una red WAN está formada por varias LAN interconectadas entre sí.

Una red WAN se utiliza para transmitir datos a larga distancia, interconectando facilidades de comunicación y servidores entre diferentes localidades o ciudades de un país completo. En estas redes por lo general se ven implicadas las compañías telefónicas y la velocidad de transmisión suele ser inferior que en las redes locales. La figura 9 da una idea clara de este concepto.

Figura 9. Red de área ancha - WAN



Varias redes de los tipos LAN y WAN pueden interconectarse entre sí formando una red lógica de área mayor y para que la transmisión entre todas ellas sea posible, se emplean los *routers* antes descritos.

1.5.1 Canales físicos de comunicación

El canal físico es el medio para conectar un punto con otro, con el propósito de transmitir y recibir datos.

Cuando la comunicación es telefónica se utiliza con frecuencia el término “pares” para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico. La clasificación de las líneas de comunicación es la siguiente:

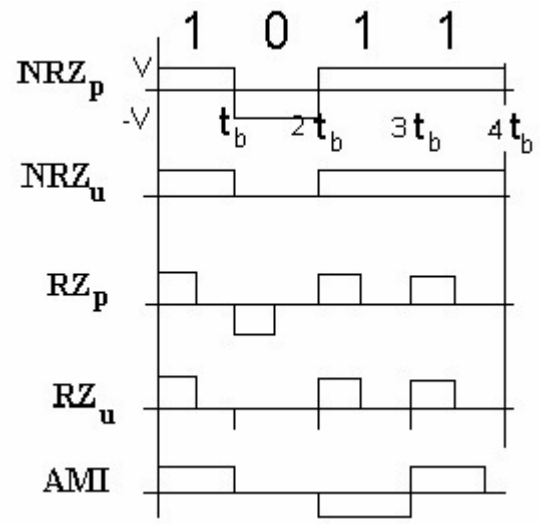
a) **Líneas conmutadas**: son las líneas que requieren marcar un código para establecer la comunicación con el otro extremo de la conexión. En teoría, los datos transmitidos a través de una línea telefónica puede alcanzar una velocidad de 53.3 kbps. Debido al ruido en la línea, propiedades del cable y al ruido eléctrico, este tipo de conexión es limitada a 33 kbps o menos.
b) **Líneas dedicadas**: son las líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.
c) **Líneas digitales**: en este tipo de línea, los *bits* son transmitidos en forma de señales digitales. Cada *bit* se representa por una variación de voltaje y esta se realiza mediante codificación digital en la cual los códigos más empleados son:

- ***NRZ (no return to zero) Polar***. Este código desplaza el nivel de referencia de la señal al punto medio de la amplitud de la señal. De este modo se reduce a la mitad la potencia requerida para transmitir la señal en comparación con el unipolar.

- ***NRZ Unipolar***. La forma de onda binaria que utilizan normalmente las computadoras se llama Unipolar, es decir, que el voltaje que representa los *bits* varía entre 0 voltios y +5 voltios. Se denomina NRZ porque el voltaje no vuelve a cero entre *bits* consecutivos de valor uno lógico. Este tipo de código es inadecuado para largas distancias.
- ***RZ (return to zero) Polar***. Esta codificación se caracteriza porque a la mitad del intervalo de *bit* el nivel de uno o del cero va a cero de ahí su nombre RZ. Es polar porque el uno se representa con un voltaje V positivo y el cero con –V negativo.
- ***RZ Unipolar***. La variación del voltaje que representa los *bits* varía entre 0 voltios y +5 voltios. El concepto explicado en c.3 se conserva respecto al tipo de codificación.
- ***Transmisión Bipolar o AMI*** (*Alternate Marks Inverted*). Es uno de los códigos más empleados en la transmisión digital a través de redes WAN. Este formato no tiene componente de corriente continua y su potencia a frecuencia cero es nula.

Se transmiten pulsos invirtiendo alternativamente la polaridad de los *bits* 1 y dos valores positivos sin alternancia entre ellos, serán interpretados como un error en la línea. Los 0´s lógicos con espacios sin presencia de voltaje. En la figura 10 se muestra un ejemplo de los tres tipos de códigos de transmisión descritos.

Figura 10. Códigos de transmisión más utilizados



1.5.2 *Interfaces*

Las *interfaces* son los que realizan la conexión eléctrica entre un equipo terminal de datos, conocido en general como DTE *(data terminal equipment)*, que puede ser un *router* por ejemplo, y un equipo que se encarga de enviar la información codificada, como por ejemplo un *módem*. Las *interfaces* comúnmente utilizadas son:

- RS-232 en DB25 y DB9. Para ambos tipos de conectores existe una configuración estándar para la conexión de los pines físicos. En este tipo de interfaz que emplea un intercambio en serie de datos binarios a velocidades de transmisión superiores a los 20 Kbps. El RS-232 es utilizado para transmitir síncronos así como también asíncronos, tales como SDLC, HDLC, *freme Relay* y X25. Sin embargo está limitado por una longitud de cable de aproximadamente 50 pies.

1.6 Componentes de una red WAN

Los componentes que se encuentran en una red WAN y que son vitales para lograr la comunicación entre equipos y otros dispositivos, tienen la misión de posibilitar la transmisión de mensajes y datos entre las redes geográficamente separadas. Los más importantes se describen a continuación.

1.6.1 *Módems*

Un *módem* es un dispositivo que convierte la señal digital en señal analógica y viceversa para que la información pueda llegar de una red a otra, a través de líneas análogas. Es decir que, un *módem* permite conectar dos redes remotas utilizando la línea telefónica.

Debido a que la computadora genera datos digitales, el *módem* se encarga de modular dichos datos para convertirlos en una señal análoga para ser enviados por una línea telefónica. El *módem* tiene que unir el espacio entre estos dos tipos de dispositivos. En la práctica se encuentran en el mercado dos grupos de *módems*, uno de ellos son los *módems* empleados en centros de transmisión con una permanente o casi permanente actividad, los cuales cuentan con mecanismos sofisticados de diagnóstico, control y administración centralizados y remotos.

El otro grupo de *módems* son los de escritorio cuyo principal uso es la conexión a través de la red pública telefónica, con cierta regularidad pero nunca con carácter permanente ni con uso exhaustivo. Los *módems* se pueden seleccionar de acuerdo a:

- La velocidad de transmisión.
- El tipo de línea que utiliza: dedicada, conmutada o ambas.
- La modulación que emplea: FSK, PSK, DPSK, QAM, TCM.
- Las posibilidades de compresión de datos para transmisión.
- La modalidad de trabajo: punto a punto o multipunto.
- Sí se instala interno o externo al equipo que envía y recibe los mensajes o información.

1.6.1.1 Tipos de modulación

La modulación de una señal digital generada por un equipo de procesamiento de datos, consiste en alterar una onda portadora senoidal generada por un oscilador, de acuerdo a la información que se transmite. De acuerdo a ello la modulación puede ser:

1. **Modulación de frecuencia FSK** *(frecuency shift keying)*. Electrónicamente consiste en un procedimiento de dos osciladores con frecuencias diferentes para dígitos 0 y 1. Normalmente esta modulación se utiliza para transmisión de datos en bajas velocidades y puede ser: Coherente: Donde no ocurre variación de fase de la portadora para dígitos del mismo valor. No Coherente: Donde puede ocurrir variación de fase en la portadora para dígitos del mismo valor.

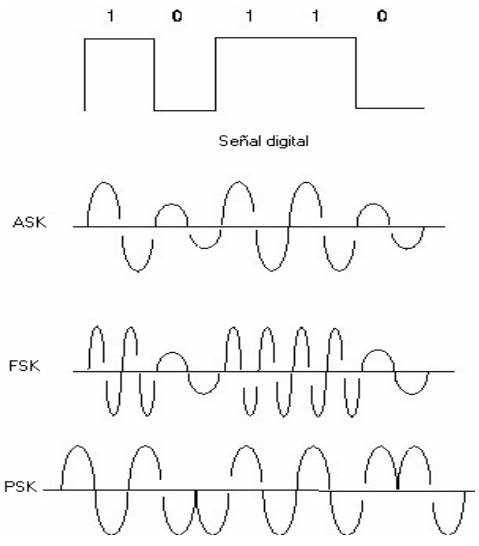
2. **Modulación ASK** *(amplitud shift keying*). No se utiliza en solitario para la transmisión de datos porque es muy sensible a interferencias de ruido eléctrico que pueden provocar errores en los datos recibidos. Esto se debe a que la amplitud de la onda es alterada de acuerdo con la variación de la señal de información, por lo que exige un medio en que la respuesta de amplitud sea estable.

3. **Modulación de fase PSK** *(phase shift keying).* En esta modulación se codifican los valores binarios como cambios de fase de la señal portadora. El ángulo de desfase entre la señal para un 0 y la señal para un 1 está asociado con los datos al ser transmitidos.

4. **Modulación diferencial de fase DPSK** *(diferential phase shift keying).* Consiste en una variación de PSK donde se toma el ángulo de fase del intervalo anterior como referencia para medir la fase de cualquier intervalo de señal.

5. **Modulación de amplitud de cuadratura QAM** *(quadrature amplitude modulation)*. Se emplea en los *módems* más rápidos. Consiste en una combinación de PSK y ASK, es decir, se van a combinar las variaciones de amplitud en referencia al momento de fase en que ocurren, con lo cual, se podrá incluir más *bits* en los mismos *hertz*. Las dos portadoras se superponen en cuadratura modulada en amplitud. La figura 11 muestra la forma de onda de las modulaciones digitales más conocidas.

Figura 11. Modulaciones ASK, FSK y PSK



1.6.1.2 Compresión de datos y control de errores

La compresión de datos previamente a ser transmitidos por el *módem* es algo esencial para optimizar el ancho de banda y enviar la máxima cantidad de información con los menores errores posibles. Los algoritmos de compresión más utilizados son:

a. **Codificación *huffman***. La cual crea una tabla que codifica a los caracteres con longitud de *bits* variables, los más empleados en 4 *bits* y los menos empleados empiezan con 5 llegando hasta 11 *bits*.

b. **Codificación *run-lenght***. Se identifican secuencias repetitivas de al menos tres caracteres, enviándose al carácter seguido del número que indica la cantidad de veces que debe ser repetido ese carácter.

MNP *(microcom network protocol)*, bajo estas siglas se agrupan un conjunto de protocolos que soportan interacción con aplicaciones de transferencia de datos. Está dividido en las clases siguientes:

1. Clase 2: Provee un mecanismo de control de errores para transmisión asincrónica a 2400 bps con protocolos orientados a *byte*, la eficiencia es de aproximadamente del 84%.

2. Clase 3. Permite al *módem* aceptar datos en formato asincrónico y transmitirlos en modalidad sincrónica. La ventaja de este servicio es que limitan los *bits* de *start* y *stop* consiguiendo así un rendimiento del 108%.

3. Clase 4. Este servicio provee un ensamblaje de paquetes adaptables. Posee un rendimiento de un 120%.

4. Clase 5. Este servicio provee compresión de datos, negociación y conversión duplex, técnica que consiste en que los *módems* se conectan a la menor velocidad, para luego comenzar a negociar el uso de velocidades superiores.

Finalmente, algo importante en la transmisión con *módems*, es la supresión de eco, ya que posibilita la transmisión en ambos sentidos. Esta técnica sólo es posible sí el diseño de los *módems* incorpora microprocesadores. La supresión de eco permite el uso de todo el ancho de banda de la línea para la transmisión simultanea en ambos sentidos del enlace.

1.6.2 Concentradores

Los concentradores con dispositivos que permiten la comunicación entre *módem*, conectado a un puerto de una computadora y varios *módems* conectados a un equipo terminal de datos en aplicaciones que usan protocolos. Este tipo de concentrador se conoce como análogo o Bridge. Un concentrador análogo es el encargado de crear un equilibrio eléctrico entre los distintos enlaces.

Existen otros concentradores digitales, también llamados *port-sharing* d*evices*, que permiten que varios equipos terminales de datos compartan un *módem* o un puerto de computadora en aplicaciones que usan protocolos.

1.6.3 Multiplexores

Los multiplexores son dispositivos que permiten la combinación de varios canales de datos en un circuito físico. Los tipos de multiplexores que existen son los siguientes:

a) **Multiplexor por división de frecuencia**: divide el ancho de banda de una línea entre varios canales donde cada canal ocupa una parte del ancho de banda de frecuencia total. Cada canal tiene una frecuencia central asignada.

b) **Multiplexor por división de tiempo**: aquí cada canal tiene asignado un período o lapso de tiempo en el canal principal y los distintos lapsos están repartidos por igual en todos los canales. Tiene la desventaja de que en caso de que un canal no sea utilizado, ese lapso de tiempo no se aprovecha por los otros canales, enviándose en vez de datos *bits* de relleno.

c) **Multiplexor por división de tiempo estadísticos:** estos dispositivos no le asignan lapsos de tiempo a los canales inactivos y además se puede asignar prioridades a los canales de acuerdo al tipo de información que se transmita.

1.7 Tipos de redes WAN

Los tipos de redes WAN varían de acuerdo al método para lograr la transmisión de datos de un punto a otro distante. Existen redes conmutadas, redes de canal virtual, redes llamadas datagramas y la PSTN o red pública de conmutación telefónica.

1.7.1 Redes conmutadas

Un ejemplo de este tipo de redes es aquella en la cual, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red. A este tipo de red se conoce como red conmutada por circuitos.

Otro tipo de red conmutada, la conmutada por mensaje, es aquella en la que una computadora suele ser el conmutador que se encarga de aceptar tráfico de las computadoras y terminales conectadas a ella.

La computadora examina la dirección que aparece en la cabecera del mensaje hacia el equipo terminal que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje en forma automática.

Finalmente, la red conmutada por paquetes, se caracteriza porque los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, están insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

1.7.2 Redes orientada a conexión

En las redes orientadas a conexión, existe el concepto de multiplexación de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas o paquetes de tráfico de distintos usuarios.

1.7.3 Redes no orientada a conexión

Este tipo de red llamada también datagrama, pasa directamente del estado libre al modo de transferencia de datos. Esta red no ofrece confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es *internet*.

1.7.4 Red pública de conmutación telefónica (PSTN)

Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

2. TRANSMISIÓN DE INFORMACIÓN

2.1 Definición de protocolo

El protocolo es un conjunto de normas que define cómo ha de realizarse una comunicación entre dos equipos, cómo ha de codificarse la información, cómo ha de transmitirse y todo lo que ambos equipos deben conocer para que efectivamente haya una comunicación. En términos informáticos, un protocolo es una normativa necesaria para que los datos enviados se reciban de forma adecuada. Los elementos que definen un protocolo son:

a) **Sintaxis :** formato, codificación y niveles de señal de datos.

b) **Semántica :** información de control y gestión de errores.

c) **Temporización :** coordinación entre la velocidad y orden secuencial de las señales.

Hay protocolos de muy diversos tipos. Unos se ocupan de aspectos bastantes primarios como por ejemplo, el de asegurar que el orden de los paquetes recibidos concuerda con el de emisión. A un nivel algo superior hay protocolos para garantizar que los datos enviados por una computadora se visualicen correctamente en el equipo receptor.

La informática moderna utiliza muchos protocolos distintos. La norma publicada por la *International Standards Organization* (OSI) y conocida como "modelo de 7 niveles" la cual reduce la complejidad de la comunicación de datos agrupando lógicamente ciertas funciones en cada uno de los niveles.

La totalidad de los aspectos contemplados en la comunicación entre ordenadores o servidores queda clasificada en siete niveles. La idea es que los protocolos concretos desarrollados en cada uno de los niveles puedan entenderse para conseguir una comunicación eficaz. De forma resumida, la función de cada uno de los niveles es la siguiente:

- Nivel 1: **Físico.** Se refiere a la forma de transmitir cada 0 y 1 que conforman toda información digital que viaja de un punto a otro. Esto incluye la definición de un 1 y un 0 en cuanto a señales eléctricas de la interfaz al medio de transmisión. A su vez esta encargado de aportar la señal empleada para la transmisión de los datos generados por los niveles superiores. Un ejemplo de protocolo es el RS-232, que define la utilización de los puertos serie de los ordenadores o servidores. En este nivel se define la forma de conectarse el cable a las tarjetas de red, cuantos pines debe tener cada conector y el uso funcional de cada uno de ellos.

  Define también la técnica de transmisión a emplear para el envío de los datos sobre el medio empleado. Se encarga de activar, mantener y desactivar un circuito físico. Este nivel trata la codificación y sincronización de los *bits* y es el responsable de hacer llegar los *bits* desde una computadora a otra.

- Nivel 2: **Enlace.** Este nivel se encarga, en el equipo o computadora origen, de alojar en una estructura lógica de agrupación de *bits*, llamada trama (*frame*), los datos provenientes de los niveles superiores. En el equipo o computadora destino, se encarga de agrupar los *bits* provenientes del nivel físico en tramas de datos (*freme*) que serán entregadas al nivel de red. Este nivel es el responsable de garantizar la

transferencia de tramas libres de errores de una computadora a otra a través del nivel físico. Además del concepto de trama, define conceptos tales como detección y corrección de errores y control de flujo. En redes de conmutación, además del control de flujo, controla el establecimiento mantenimiento y liberación de la conexión en cada uno de los enlaces. Asegura que el *bit* transmitido llegue de un nodo a otro, o del nodo al terminal (o viceversa). Es decir, garantiza un salto sin errores.

- Nivel 3: **Red.** Se centra en el establecimiento de una conexión punto a punto entre cliente y servidor. Es el nivel en el que se trata, por ejemplo, el direccionamiento y encauzamiento de mensajes y de la conversión de las direcciones lógicas y nombres, en direcciones físicas. Se encarga de determinar la ruta adecuada para el trayecto de los datos, basándose en condiciones de la red, prioridad del servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red. En un sistema intermedio, aquel que no procesa información sino que retransmite lo que los sistemas finales generan, sólo están presentes los niveles 1, 2 y en algunas ocasiones el 3. Son los que llamamos niveles bajos de la torre OSI. El resto, claro, son los niveles altos. Ejemplos de protocolos son: X25, *Frame Relay* y ATM para redes de conmutación, e IP para redes interconectadas.

- Nivel 4: **Transporte.** Es el primero de los niveles encargados del funcionamiento punto a punto. Se ocupa del formato y su misión es asegurar que una secuencia recibida de *bits* se transforme en datos significativos. Este nivel supone la existencia previa de una conexión fiable. Su función es parecida a la del nivel 2, salvo que garantiza la transmisión sin errores extremo a extremo, realizando una detección de los mismos, independientemente del tipo de red. Al otro extremo los

datos llegan sin errores, ordenados, sin pérdidas ni duplicados. En las redes de conmutación de paquetes, este nivel se encarga de fragmentar el mensaje en el origen y de recomponerlo en el destino. Así mismo informa a los niveles superiores del estado de la red. Ejemplos de protocolos ISO son: TP0, TP1, TP2, TP3 y TP4. Y ejemplos de protocolos para *internet* son: TCP y UDP.

- Nivel 5: **Sesión.** Es el encargado de que dos aplicaciones residentes en computadoras diferentes establezcan, usen y terminen una conexión llamada sesión. En el caso de la mayoría de las modernas aplicaciones informáticas (que se hallan divididas en componentes cliente y servidor), este nivel constituye un elemento inherente del propio diseño. Este nivel realiza reconocimientos de nombres y las funciones necesarias para que dos aplicaciones se comuniquen a través de la red.

- Nivel 6: **Presentación.** Determina el formato a utilizar (conocidos como sintaxis de transferencia) para el intercambio de datos en la red. Puede ser considerado un traductor de la red. Este nivel también maneja la seguridad de emisión pues, provee a la red servicios como el de encriptación de datos. Este nivel elimina los problemas que puedan surgir al comunicar distintas arquitecturas, pues cada arquitectura estructura los datos de una forma específica, que no tienen por que ser compatibles. En el nivel de transporte se traducen los datos a un formato común, que se define en este mismo nivel.

- Nivel 7: **Aplicación.** Recoge el resto de las funciones necesarias dependiendo de la aplicación. En la práctica hay otras formas de estructurar y llevar a cabo las comprobaciones necesarias para que una computadora pueda dialogar con otra. El modelo de siete niveles constituye sin embargo un modelo útil y se utiliza con carácter general, especialmente en los niveles inferiores, cuyos protocolos son de normas más estables.

2.2 Protocolos de la capa de acceso al medio

Los protocolos de la capa de acceso al medio, son los tipos de soperte físico de una LAN y entre estos encontramos los más utilizados que son el *token ring* y el *ethernet*, éste último con una amplia aceptación en el mercado informático, entre otras cosas, por la habilidad para soportar virtualmente todos los protocolos populares de red.

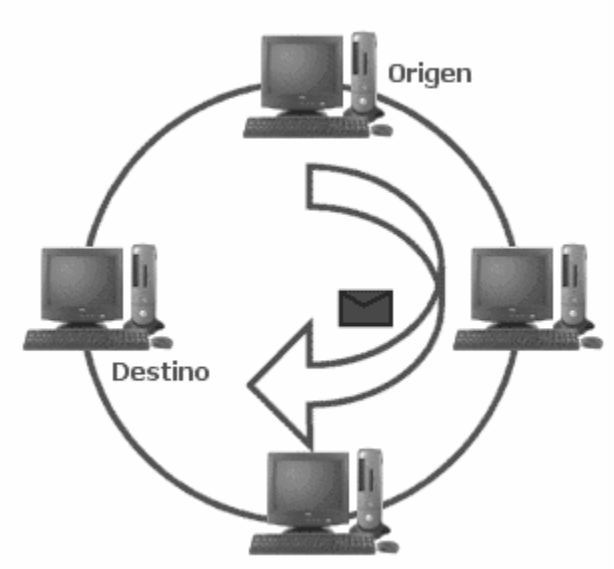
2.2.1 *Token ring*

Las redes *token ring* originalmente fueron desarrolladas por IBM en los años 1970s. Este fue el primer tipo de red de área local de la tecnología IBM (LAN). Este tipo de redes basan el control de acceso al medio en la posesión de un *token*, que es un paquete con un contenido especial que le permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el *token* va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el *token* a la siguiente. Cada estación puede mantener el *token* por un período limitado de tiempo.

Las redes de tipo *token ring* tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbits/s. Existen redes *token ring* de 16 Mbits/s, pero no están definidas en ninguna especificación de IEEE.

Los dispositivos en una red *token ring* se conectan a través de una unidad de interfaz de acceso múltiple llamada MAU. La MAU contiene un pequeño transformador de aislamiento para cada dispositivo conectado, el cual brinda protección similar a la de *local talk*. La figura 12 muestra el esquema de una figura red *token ring*.

Figura 12. Red Token Ring



2.2.1.1 Funcionamiento de la red *token ring*

Si una estación posee el *token* y tiene información por transmitir, esta divide el *token*, alterando un *bit* de éste que abre la información que se desea transmitir y finalmente manda la información hacia la siguiente estación en el anillo. Mientras la información del *freme* es circulada alrededor del anillo, no existe otro *token* en la red (a menos que el anillo soporte uno nuevo), por lo tanto otras estaciones que deseen transmitir deberán esperar. Por ello, es difícil que se presenten colisiones.

La información del *freme* circula en el anillo hasta que localiza la estación destino, en la que se copia la información para poderla procesar. La información del *freme* continúa circulando en el anillo y finalmente es borrada cuando regresa a la estación desde la cual se envió.

El instituto de Ingenieros Eléctricos y Electrónicos -IEEE - creó la norma 802.5 IEEE en la cual se establecen los estándares internacionales para una red *token ring*.

2.2.2 *Ethernet*

Las redes *ethernet* pertenecen a la categoría de redes LAN por lo que es muy frecuente encontrarlas en oficinas, fábricas, universidades, etc.

Ethernet es popular porque logra un buen balance entre velocidad, costo y facilidad de instalación.

Estos puntos fuertes, combinados con una amplia aceptación en el mercado informático y la habilidad para soportar virtualmente todos los protocolos populares de red, hacen de *ethernet* una tecnología de red ideal para la mayoría de los usuarios de computadoras hoy en día.

2.2.2.1 Topologías

Existen dos opciones para implementar una red *ethernet*. La primera consiste en conectar todas las computadoras sobre el cable de la red directamente. Esta opción se conoce como topología tipo bus. La segunda consiste en utilizar un dispositivo llamado *hub* o concentrador, en el cual se conecta cada uno de los cables de red de las computadoras. Esta topología se conoce como *Hub*. Un ejemplo de estos dos tipos de redes pueden apreciarse en las figuras 2 y 3.

Una red configurada como tipo *hub* puede conectarse a un bus o cable principal de red, ya que el concentrador además de las conexiones para las computadoras, tiene la posibilidad de conectarse al cable principal de un edificio. Un caso típico sería un edificio en el cual los usuarios de cada piso están conectados a un *hub* o concentrador. Los *hub* de todos los pisos están unidos entre sí por un bus o cable principal de la red (*backbone*).

2.2.2.2 Tarjeta de red *ethernet*

Cada computadora debe tener instalada una tarjeta de red, la cual incorpora los conectores necesarios para que el usuario pueda conectarse a la red. Esta tarjeta se debe introducir en el interior de la computadora.

Posee un microprocesador que se encarga de controlar todos los aspectos relacionados con la comunicación y otros como el empaquetamiento y desempaquetamiento de la información que se transmite y recibe, la codificación y decodificación, detección de errores.

En general se encarga de todas las tareas necesarias para que la computadora solamente se preocupe por entregarle la información que se desea transmitir y viceversa. Las tarjetas de red *ethernet* en las que se utiliza el cable UTP como medio físico, pueden transmitir la información entre computadoras a velocidades entre 10 y 100 millones de *bits* por segundo.

2.2.2.3 Transmisión de información en la red

Para garantizar que las computadoras conectadas en la red puedan comunicarse sin problemas, deben cumplir una serie de normas que se conocen generalmente con el nombre de protocolo. La red *ethernet* utiliza un protocolo llamado CSMA/CD (*carrier sense multiple access / carrier detect*), que quiere decir: Acceso múltiple por detección de portadora con detección de colisión.

Como todas las computadoras están conectadas sobre el mismo bus, se dice que el cable opera en acceso múltiple. Esto significa que cuando una computadora enviará información hacia otra computadora, debe colocar en el cable todo el paquete de información a ser transmitido. Dicho paquete incluye los datos sobre qué usuario los envía y qué usuario los recibe, además de la información en sí.

Antes de iniciar, el equipo que va a transmitir debe "escuchar" el canal para saber que está libre (CS, detección de portadora). En caso de estar ocupado, debe esperar un tiempo y volver a intentarlo nuevamente. En caso de estar libre, puede empezar a transmitir los datos correspondientes. Como se puede deducir, si dos computadoras "escuchan" el canal al mismo tiempo y éste se encuentra desocupado, empezarán a transmitir sus datos sobre el cable, lo que generará lo que se conoce con el nombre de colisión de información.

En este caso, las computadoras se retiran por un tiempo y luego cada una intenta nuevamente hacer su transmisión. Además, las computadoras que colisionaron colocan una señal en el cable de red que indica que se presentó un choque de datos o información.

Esta es una característica muy importante de este tipo de red, ya que cada computadora se retira del canal y no intenta por el contrario, seguir con su transmisión, lo que contribuye notablemente a reducir el tiempo de fallas en la línea. Las tarjetas de red tienen un circuito electrónico que se encarga de realizar las funciones que permiten “escuchan” el canal y detectar las colisiones.

Ethernet es conocida como la norma 803.2 IEEE ya que fue el Instituto de Ingenieros Eléctricos y Electrónicos - IEEE - quien especificó los estándares internacionales tanto del *hardware* como del formato de los mensajes relacionado con las redes *ethernet*. Las diferentes variantes de esta norma son la 10 Mbps *ethernet* y la 100 Mbps *ethernet*, basadas en el cable que se utiliza para la transmisión de información y sus longitudes máximas.

2.2.2.4 10 Mbps *ethernet*

Originalmente la 10 Mbps *ethernet* era una LAN de banda base que operaba a 10 Mbps utilizando el protocolo de acceso múltiple al medio conocido como CSMA/CD, sobre un cable coaxial.

En la actualidad, el estándar IEEE 803.2 provee una variedad de opciones de cableado, a través de los cuales se puede transmitir a esa misma velocidad. Esas opciones se diferencian una de otra por los identificadores asignados por la IEEE que incluyen tres tipos de información. En la tabla I se muestran los estándares ya establecidos:

Tabla I. Estándares establecidos por la IEEE sobre 10 Mbps *ethernet*

Características	**Valor *ethernet***	**Valores IEEE 802.3**					
		10Base5	**10Base2**	**1Base5**	**10BaseT**	**100BaseTX**	**100BaseT 4**
Velocidad de los datos (Mbps)	10	10	10	1	10	100	10
Método de señalización	Banda de base	Banda de base	Banda de base	Banda de base	Banda de base	Banda de base	Banda ancha
Longitud máxima del segmento (m)	500	500	185	250	100 con pares trenzados no blindados	100 UTP o STP	1800
Soporte	Coaxial de 50-ohmios (grueso)	Coaxial de 50-ohmios (grueso)	Coaxial de 50-ohmios (fino)	Pares trenzados sin blindaje	Pares trenzados sin blindaje	Categoría 5 Pares trenzados blindados o sin blindaje	Coaxial de 75-ohmios
Topología	Bus	Bus	Bus	Estrella	Estrella	Estrella	Bus

- El número “10”, representa la velocidad media de 10 Mbps.
- La palabra “BASE” indica que es una señal *ethernet* transportada sobre el medio.
- La tercera parte del identificador proporciona información del tipo y longitud del segmento físico por donde se transmite. Por ejemplo, el “5” indica que se utiliza en cable coaxial grueso y recuerda los 500 metros como longitud máxima permitida para un segmento individual. El “2” indica que se utiliza en cable coaxial delgado y redondea los 185 metros máximos de longitud l. Las letras “T” y “F” representan al par trenzado (*twisted-pair*) y fibra óptica (fiber optic), respectivamente y simplemente indican el tipo de cable utilizado.

2.2.2.5 100 Mbps *ethernet*

También conocida como *fast ethernet* que fue establecida para redes que requieren altas velocidades de transmisión, por lo que fue establecido el estándar IEEE 802.3u. Este estándar eleva el límite de velocidad de transmisión de 10 *megabits* por segundo a 100 *megabits* por segundo con sólo mínimos cambios en los cableados existentes.

Hay tres tipos de redes *fast ethernet* que han sido especificadas para la transmisión de información, estas son: 100BASE-T4, 100BASE-TX, 100BASE-FX. La IEEE ha identificado estos tres medios utilizando tres identificadores que son:

- El primero es el “100” que representa la velocidad media de 100 Mbps.
- La palabra “BASE” significa “banda base” la cual es un tipo de señalización. Esta señalización de banda base simplemente significa que lo que se transmite por el medio son señales de *ethernet*.

- La tercera parte del identificador representa el tipo de segmento. El tipo de segmento “T4” es un segmento de par trenzado que utiliza cuatro pares de cable telefónico trenzado. El segmento tipo “TX” es un segmento de par trenzado que utiliza dos pares de cables trenzados utilizados para datos desarrollados por el ANSI. El tipo de segmento “FX” es un enlace de fibra óptica que cumple con los estándares desarrollados por el ANSI y que utiliza dos tramos de fibra. Los estádares para TX y FX con conocidos conjuntamente como 100BASE-X.

2.2.2.6 *Gigabit ethernet*

Gigabit ethernet establecido por la norma IEEE 802.3z, es un estándar de escala superior que es compatible completamente con las instalaciones existentes de redes *ethernet*. Conserva el mismo método de acceso CSMA / CD y soporta modos de operación como *full-duplex y half-duplex*.

Al inicio, *Gigabit ethernet* soportó únicamente fibra óptica mono-modo y multi-modo y era empleado como *backbone* en redes existentes. En la actualidad ya puede ser utilizado para interconectar estaciones de trabajo, granjas de servidores, *switch*es, etc.

La capa física de *Gigabit ethernet* acepta 4 tipos de medios físicos los cuales son definidos en las normas 802.3z (1000Base-X) y 802.ab (1000 Base-T).

En el estándar 1000 Base-X la capa física es el canal de fibra óptica, la cual es una tecnología de interconexión entre estaciones de trabajo, servidores, dispositivos de almacenamiento y periféricos. Hay tres tipos de medios de transmisión que son incluidos en el estándar 1000 Base-X:

- 1000Base-SX : Utiliza una fibra multimodo de 850 nm.
- 1000Base-LX : Puede ser usada tanto con monomodo y multimodo de 1300nm.
- 1000BaseCX : Usa un cable de par trenzado de cobre blindado – STP -.

El estándar 1000Base-T emplea como medio de transmisión un cable UTP, utilizando 4 pares de líneas de categoría 5 o categoría 5e.

La capa MAC de *Gigabit ethernet* usa el mismo protocolo de *ethernet* CSMA/CD por lo que la máxima longitud de cable usado para interconectar las estaciones está limitado por ese protocolo. Si dos computadoras detectan el medio desocupado y comienzan la transmisión ocurrirá una colisión. La longitud máxima de un cable en *ethernet* es de 2.5 Km con un máximo de 4 repetidores. Como en *Gigabit* la tasa de *bit* se incrementa, al igual que la velocidad de transmisión, como resultado, si la misma longitud de cable se mantiene, entonces la computadora, servidor o equipo periférico puede transmitir a gran velocidad y no detectar una colisión al final del cable.

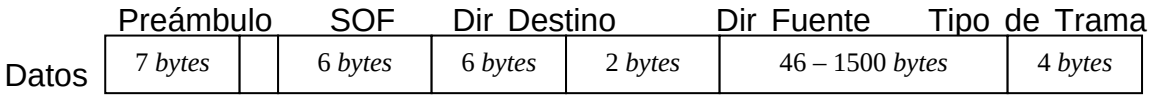
2.2.2.7 Formato de transmisión de *ethernet*

Los paquetes de información (también conocidos como tramas) que envía cada computadora por la red deben tener un formato específico y cumplir unas normas establecidas, para que sean comprendidas por todos los usuarios de la red. Esas normas cobijan aspectos como la longitud de los paquetes, polaridad o voltaje de los *bits*, códigos para detección de errores, etc.

La trama *ethernet* empieza con un preámbulo de 7 *bytes* iguales (10101010). Esto genera una onda cuadrada de 10 Mhz, durante un tiempo de 5.6 micro segundos, con el objeto de que el receptor se sincronice con el reloj

del transmisor. Después viene un *byte* llamado Inicio de trama SOF (*start of freme* 10101011), con el fin de marcar el comienzo de la información propiamente dicha. La figura 13 muestra el formato de la trama para una red *ethernet*.

Figura 13. Trama de una red



Los *bytes* correspondientes a la dirección de destino y de origen se utilizan para saber a quién va el mensaje y quién lo envía. Además, existe un carácter especial que puede indicar que el mensaje va dirigido a un grupo de usuarios o a todos los usuarios. El *byte* que indica la longitud del campo de datos indica al receptor cuantos *bytes* de información útil o verdadera debe esperar a continuación. Los datos corresponden al archivo en particular que se está enviando.

Los *bytes* de relleno se emplean para garantizar que la trama total tenga una longitud mínima de 64 *bytes* (sin contar el preámbulo ni el inicio de trama), en caso de que el archivo de datos sea muy corto. Esto se hace con el fin de desechar las tramas muy cortas (menores de 64 *bytes*) que puedan aparecer en el cable de la red, como consecuencia de transmisiones abortadas por colisiones.

El código de redundancia sirve para hacer detección de errores. Si algunos *bits* de datos llegan al receptor erróneamente (por causa del ruido), es casi seguro que el código de redundancia será incorrecto y, por lo tanto, el error será detectado.

En la computadora transmisora se da una codificación de los *bits*. Aunque los *bits* de información que entrega la tarjeta de red al cable se podrían entregar en forma directa (por ejemplo: 1 Voltio para un 1 lógico y 0 Voltios para un 0 lógico), esto no le permitiría al receptor saber en qué momento empieza cada uno. Además, la potencia que se pierde en el cable sería muy elevada. Por esto, la red utiliza una técnica denominada codificación Manchester, que consiste en asignar dos intervalos de tiempo iguales para cada *bit*.

2.3 Protocolo TCP/IP de red y transporte

Cuando un usuario desde su computadora se conecta a *internet* a través de una línea telefónica o una red local, visita alguna página de *web* o envía un mensaje de correo electrónico, se realizan un sinnúmero de pequeños procesos que tienen como objetivo conjunto transferir la información deseada y asegurar que dicha transmisión se realice libre de errores.

Durante tal transmisión se utilizan varios protocolos. Al conjunto de estos protocolos se les conoce como conjunto de protocolos TCP/IP (donde TCP e IP significan, respectivamente, *transmission control protocol e Internet protocol*) o sea protocolo de control para la transmisión y protocolo de internet.

TCP/IP agrupa docenas de protocolos, que implementan funciones a todos los niveles de las capas OSI excepto el físico. El modelo de comunicaciones de OSI define 7 capas. En cambio, TCP/IP utiliza 4, dichas capas son: aplicación, transporte, red y enlace.

La correspondencia entre las capas de TCP/IP y el modelo OSI es la siguiente:

La capa de aplicación de TCP/IP corresponde a las capas de aplicación, presentación y sesión de las capas OSI. Aunque se incluyen protocolos destinados a proporcionar servicios tales como correo electrónico (SMTP), trasferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo http (*hypertext transfer protocol*).

La capa de transporte de TCP/IP corresponde a la capa de transporte de OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

La capa de red TCP/IP corresponde a la capa de red y también se intersecta con la capa de enlace de OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Y por último, la capa enlace de TCP/IP corresponde a las capas de enlace y física de OSI. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada servidor, como puede ser una línea punto a punto o una red *ethernet*.

Las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

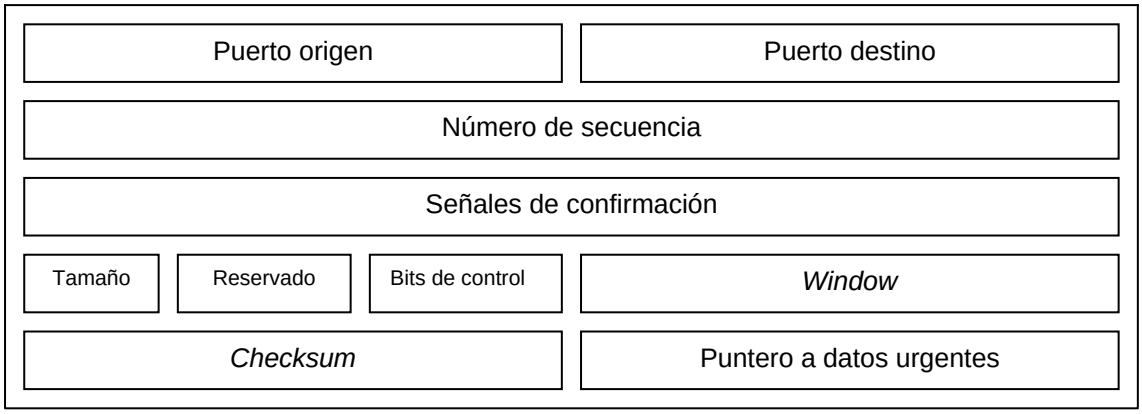
Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (*datagram*), y son conjuntos de datos que se envían como mensajes independientes.

2.3.1 Protocolo 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 cierta 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 figura 14 muestra el formato de la cabecera TCP.

Figura 14. Formato de cabecera TCP



La cabecera de un datagrama contiene al menos 160 *bit* 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 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 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.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante y 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 que tiene un tamaño de 32 *bit*.

Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período 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 *bit*, el cual contiene un valor calculado a partir de la

información del datagrama completo (*checksum*). 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.

2.3.1.1 Protocolos alternativos a TCP

TCP es el protocolo más utilizado para el nivel de transporte en *internet*, pero además de éste existen otros protocolos que pueden ser más convenientes en determinadas ocasiones. Tal es el caso de UDP y ICMP.

El protocolo UDP (*user datagram protocol*) o protocolo de datagramas de usuario puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP no admite numeración de los datagramas, este protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, o también cuando se quiere enviar información de poco tamaño que cabe en un único datagrama.

Cuando se utiliza 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 bastante menor en tamaño que la de TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones.

Un ejemplo típico de una situación en la que se utiliza el UDP es cuando se pretende conectar con un ordenador de la red, utilizando para ello el nombre del sistema. Este nombre tendrá que ser convertido a la dirección IP que le corresponde y, por tanto, tendrá que ser enviado a algún servidor que

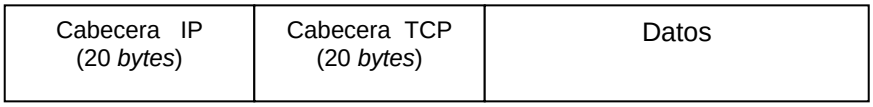
posea la base de datos necesaria para efectuar la conversión. En este caso es mucho más conveniente el uso de UDP.

El protocolo CMP (*internet control message protocol*) o protocolo de mensajes de control de *internet* (ICMP) es de características similares al UDP, pero con un formato aún más simple. Su utilidad no está en el transporte de datos "de usuario", sino en los mensajes de error y de control necesarios para los sistemas de la red.

2.3.2 Protocolo IP (*Internet protocol*)

El IP es un protocolo que pertenece al nivel de red, por lo tanto, es utilizado por los protocolos de nivel de transporte como TCP para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando. Suponiendo que el protocolo TCP ha sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructura del mensaje una vez tratado quedaría tal y como se muestra en la figura 15.

Figura 15. Estructura del mensaje utilizando protocolos TCP e IP



2.3.2.1 Protocolo IP versión 4

La versión del protocolo IP viene dada por la información de los campos que conforma la cabecera IP de la figura 15. Dicha cabecera tiene un tamaño de 160 *bits* o 20 *bytes* y está formada por los siguientes campos:

- **Versión:** número del protocolo IP utilizado. Y de acuerdo a la figura 15 debe tener el valor 4. Tamaño: 4 *bits*.

- **Longitud de la cabecera IHL** (*internet* h*eader lenght*): especifica la longitud de la cabecera expresada en el número de grupos de 32 *bit* que contiene. Tamaño 4 *bits*.

- **Tipo de servicio:** el tipo o la calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño 8 *bits*.

- **Longitud total:** es la longitud en *bytes* del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 *bits*, el tamaño máximo del datagrama no podrá superar los 65,535 *bytes*, aunque en la práctica este valor será mucho más pequeño. Tamaño 16 *bits*.

- **Identificación:** valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 *bits*.

- ***Flags* o banderas:** son indicadores utilizados en la fragmentación. Tamaño: 3 *bits*.

- **Fragmentación:** contiene un valor para poder ensamblar los datagramas que se hayan fragmentado. Esta expresado en grupos de 8 *bytes* (64 *bits*), comenzando por el valor cero para el primer fragmento. Tamaño: 16 *bit*.

- **Límite de existencia:** contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, aunque esto es bastante improbable que suceda no debe descuidarse. Tamaño: 8 *bit*.

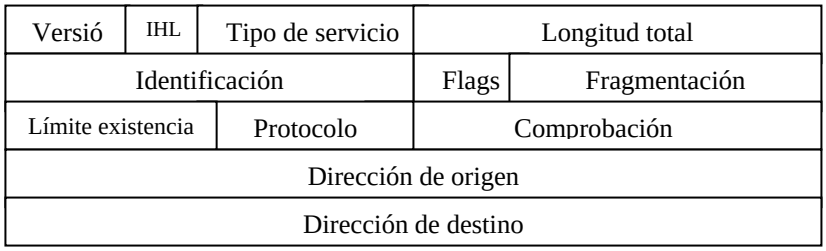
- **Protocolo:** utilizado en este campo para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 *bits*.

- **Comprobación o *checksum*:** es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Tamaño: 16 *bits*.

- **Dirección de origen:** contienen la dirección del *host* que envía el paquete. Tamaño: 32 *bits*.

- **Dirección de destino:** esta dirección es la del *host* que recibirá la información. Los *routers* o *gateways* intermedios deben conocerla para dirigir correctamente le paquete. Tamaño 32 *bits*. La figura 16 muestra la organización de la cabecara IP versión 4.

Figura 16. Organización de la cabecera IP versión 4



2.3.2.1.1 La dirección de internet

El protocolo IP identifica a cada computadora que se encuentre conectada a la red mediante su correspondiente dirección. Esta dirección es un número de 32 *bits* que debe ser único para cada *host* y normalmente suele representarse como cuatro cifras de 8 *bit* separadas por puntos.

La dirección de *internet* (IP *address*) se utiliza para identificar tanto a la computadora en concreto como la red a la que pertenece, de manera que sea posible distinguir a las computadoras 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, se establecieron cuatros clases diferentes de direcciones, las cuales se representan mediante cuatro rangos de valores:

- Clase A: son las que primer *byte* tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones usan solamente 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.

- Clase B: estas direcciones utilizan en su primer *byte* un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros *bytes* de la dirección, teniendo que ser un valor entre 128.1 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 *host* permitiendo, por consiguiente, un número máximo de 64516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.

- Clase C: en este caso 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 computadoras en cada red. Estas direcciones permiten un menor número de *host* que las anteriores, aunque son as más numerosas pudiendo existir un gran número de redes de este tipo (más de dos millones).

- ***Supernetting:*** el enrutamiento se basa en máscaras de red más cortas que la máscara de red natural de la dirección IP. Otra diferencia es que máscaras del *supernetting* son siempre contiguas, mientras que las de las clases A, B y C pueden tener una parte local no contigua. Este método es conocido como CIDR (*classless interdomain rotuing*). El CIDR no enruta de acuerdo a la clase del número de red (de ahí el término "*classless*": sin clase) sino sólo según los *bits* de orden superior de la dirección IP, que se denominan prefijo IP. Cada entrada de ruteo CIDR contiene una dirección IP de 32 *bits* y una máscara de red de 32 *bits*, que en conjunto dan la longitud y valor del prefijo IP.

El número 255 tiene un significado especial, ya que se reserva para el *broadcast*. El *broadcast* es necesario para 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 un mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de *broadcast* es cuando se quiere convertir el nombre por dominio de una computadora a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del *broadcast* se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo en unos en binario) en cada *byte* que identifique al *host*. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

2.3.2.2 Protocolo IP versión 6

La nueva versión del protocolo IP recibe el nombre de Ipv6, aunque es también conocido comúnmente como IPNG (internet protocol next generation). El número de versión de este protocolo es el 6 frente a la versión 4 utilizada hasta entonces, puesto que la versión 5 no pasó de la fase experimental.

Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión 4 no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPNG se ha diseñado para solucionar todos los problemas que

surgen con la versión anterior y además ofrecer soporte a las nuevas redes de alto rendimiento como la ATM, *Gigabit ethernet*, etc.

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 *bit*, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera, como se muestra a continuación, se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal. El formato es el siguiente:

- **Versión:** número de la versión del protocolo IP, que este caso contendrá el valor 6. Tamaño: 4 *bit*.

- **Prioridad:** contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 4 *bit*.

- **Etiqueta de Flujo:** indica cuando el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten. Tamaño: 24 *bit*.

- **Longitud:** es la longitud en *bytes* de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 *bit*.

- **Siguiente cabecera:** se usa para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 *bit*.

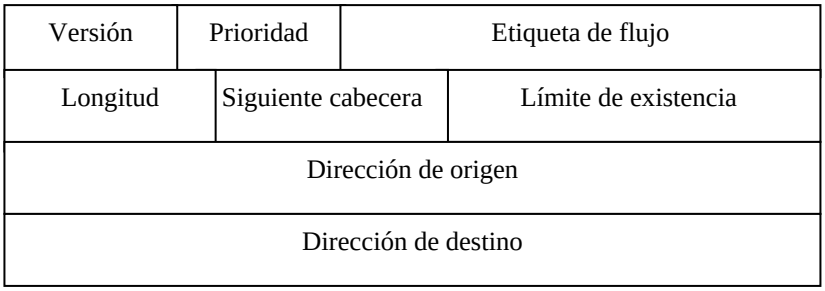
- **Límite de existencia:** tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño: 8 *bit*.

- **Dirección de origen:** el número de dirección del *host* que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 *bit*.

- **Dirección destino:** número de dirección de destino, aunque puede no coincidir con la dirección del *host* final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. Tamaño: 128 *bit*.

La figura 17 muestra la organización de la cabecara IP versión 6.

Figura 17. Organización de la cabecera IP versión 6



2.3.2.2.1 Direcciones en la versión 6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 *bit*, cuatro veces mayor.

Estas nuevas direcciones identifican a una interfaz o conjunto de *interfaces* y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos a través de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 *bits* es enorme. Teóricamente 2 elevado a las 128 direcciones posibles, siempre que no apliquemos algún formato u organización a estas direcciones.

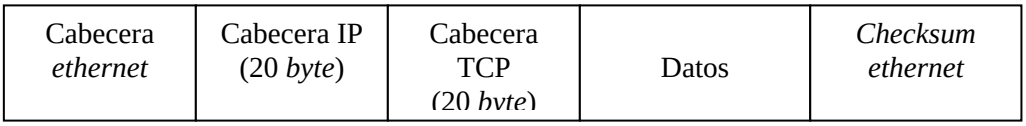
2.4 Ruteo en protocolo IP

El ruteo es el proceso que permite que la información llegue hasta su destino final, es decir, llevar los datos de una computadora a otra por medio de red. Las tareas del ruteo son implementadas por el protocolo IP sin que los protocolos de un nivel superior tales como TCP o UDP tengan constancia de ello.

Cuando se quiere enviar información por internet a una computadora, el protocolo IP comprueba sí la computadora de destino se encuentran en la misma red local que la computadora origen. Sí es así, se enviará el correspondiente datagrama de forma directa: la cabecera IP contendrá el valor de la dirección internet de la computadora destino, y la cabecera *ethernet* contendrá el valor de la dirección de la red *ethernet* que corresponde a este mismo ordenador.

En la figura 18 se muestra el formato de un mensaje IP cuyo protocolo de nivel de transporte es TCP y que es enviado a través de una red *ethernet*, tal y como se supone en lo descrito en el párrafo anterior.

Figura 18. Mensaje TCP/IP en una red *ethernet*



La cabecera *ethernet* consta de 14 *bytes* en los que se incluyen 3 campos: La dirección de origen (48 *bit*), la dirección de destino (48 *bit*) y el código de tipo (16 *bit*) que se utiliza para permitir el uso de diferentes protocolos en la misma red (TCP/IP es uno de ellos).

El *checksum* o campo de detección de errores (32 *bit*) no se incluye en la cabecera *ethernet*, sino que se sitúa al final del mensaje y se calcula a partir de todos los datos del paquete completo.

En una red *ethernet* los paquetes son transportados de una computadora a otra de manera que son visibles para todos, siendo necesario un procedimiento para identificar los paquetes que pertenecen a cada computadora.

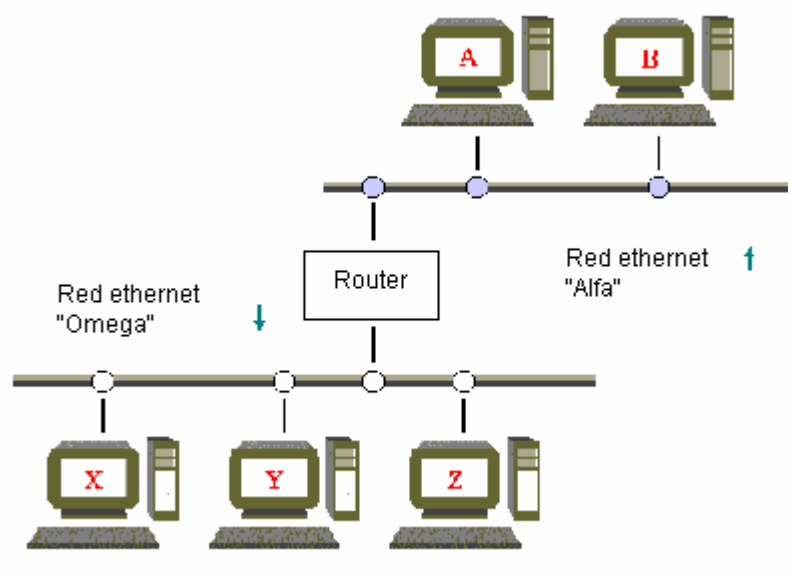
Cuando el paquete es recibido en el otro extremo, la cabecera y el *checksum* se retiran, se comprueba que los datos corresponden a un mensaje IP y este mensaje se pasa al protocolo IP para que sea procesado.

2.4.1 Ruteo indirecto

Cuando se pretende enviar información a una computadora remota que está situada en una red local diferente a la computadora de origen, el proceso resulta más complicado. Esto se conoce como ruteo indirecto, y es el caso que se presenta más frecuentemente cuando se envía información en *internet*.

La figura 19 muestra un caso en el que dos redes LAN que utilizan la tecnología de *internet* se enlazan para intercambiar información, creando una red lógica de mayor tamaño gracias a la funcionalidad del protocolo IP.

Figura 19. Interconexión de dos redes LAN.



Fuente: **http://www.geocities.com/red.html**

En internet existe un elevado número de redes independientes conectadas entre sí mediante el uso de los *routers*. El *router*, por su puesto, puede enviar y recibir información de los *host* de todas las redes a las que está conectando, y siempre será en forma directa.

De acuerdo a la figura 19, el *host* A puede comunicarse con el *host* B, así como los *host*s A y B pueden enviar o recibir información del *router*. En ambos casos se trata de ruteo directo.

Si sólo fuéramos a enviar información de manera directa dentro de una misma red no sería necesario el uso del protocolo TCP/IP, siendo el mismo especialmente indicado cuando se desea una comunicación con otras redes.

En el caso de la figura anterior, los datagramas tendrán que ser encaminados a través del *router* para llegar a su destino. La forma de hacer esto es a través del protocolo IP, el cual decide sí la información puede enviarse directamente o si por el contrario debe utilizarse el método indirecto a través de un *router*.

Si en la figura 19 se supone que el *host* B de la red 1 necesita comunicarse con el *host* X situado en la red 2, una vez que se ha determinado que el destino no se encuentra en la misma red, envía el datagrama IP hacia el *router* correspondiente. Como este *router* y la computadora que envía la información se encuentran conectados a la misma red, se trata por tanto de ruteo directo, y por lo tanto sólo será necesario determinar la dirección *ethernet* del *router* mediante un protocolo llamado ARP.

El paquete enviado incluirá la dirección del *router* como dirección *ethernet* de destino, pero sin embargo, la dirección de destino IP corresponderá a la computadora final a la que va dirigido el paquete, es decir, la computadora X.

El *router* recibe el paquete y a través del protocolo IP comprueba que la dirección de *internet* de destino no corresponde con ninguna de las asignadas como suyas, procediendo entonces a determinar la localización de la red 2, en la que se entrega el paquete a la computadora de destino.

Como lo más probable es que la red de *internet* cuente con múltiples enlaces con otras LAN, y por lo tanto más de un *router*, la manera en la que el protocolo IP determina la red correcta a dónde debe dirigirse, se logra mediante

el uso de una tabla donde se relaciona cada una de las redes existentes con el *router* que debe usarse para tener acceso. Esta tabla es utilizada por cada una de las computadoras.

Por esta razón, cuando un *router* recibe un paquete que debe ser encaminado, busca en su propia tabla de redes la entrada correspondiente a la red para, una vez encontrada, entregarlo a la computadora de destino. Como es posible que el *router* no tenga conexión directa a la misma red que la computadora destino, la búsqueda en su tabla de redes dará como resultado la dirección de un nuevo *router* al que cual dirigir el paquete, y así continuará el proceso sucesivamente hasta encontrar el destino final.

La creación y mantenimiento de la tabla de redes para el ruteo es un proceso complejo que debe ser realizado por el administrador de la red. Aquí hay que tener en cuanta que la enorme extensión de *internet* supone una gran dificultad para conseguir que sean correctas todas las entradas de la tabla, además de que esta tabla puede llegar a tener un tamaño considerable. El uso de *routers* por defecto mejora la situación al permitir que sean estos los que guarden el registro de la red sin que las computadoras individuales tengan que ocuparse en ello.

2.5 Protocolo de resolución de direcciones (ARP)

El protocolo de resolución de direcciones (ARP) es necesario debido a que las direcciones *ethernet* y las direcciones IP son dos números distintos y que no guardan ninguna relación. Así, cuando pretendemos dirigirnos a un *host* a través de su dirección de *internet* se necesita convertir ésta a la correspondiente dirección *ethernet*.

ARP es el protocolo encargado de realizar las conversiones de dirección correspondientes a cada *host*. Para ello cada sistema cuenta con una tabla con la dirección IP y la dirección *ethernet* de algunos de los otros sistemas de la misma red. Sin embargo, también puede ocurrir que el ordenador de destino no se encuentre en la tabla de direcciones, teniendo entonces que obtenerla por otros medios.

Con la finalidad de obtener una dirección *ethernet* destino que no se encuentra en la tabla de conversiones se utiliza el mensaje ARP de petición. Este mensaje es enviado como *broadcast*, es decir, que estará disponible para que el resto de los sistemas de la red lo examinen, y el cual contiene una solicitud de la dirección final de un sistema a partir de su dirección IP. Cuando el ordenador con el que se quiere comunicar analiza este mensaje comprueba que la dirección IP corresponde a la suya y envía de regreso el mensaje ARP de respuesta, el cual contendrá la dirección *ethernet* que se estaba buscando.

La computadora que solicitó la información recibirá entonces el mensaje de respuesta y añadirá la dirección a su propia tabla de conversiones para futuras referencias. El mensaje de petición ARP contiene las direcciones IP y *ethernet* de la computadora que solicita la información, además de la dirección IP de la computadora de destino.

Estos mensajes con aprovechados en algunas ocasiones también por otros sistemas de la red para actualizar sus tablas, ya que el mensaje es enviado en forma de *broadcast*. El ordenador de destino, una vez que ha completado el mensaje inicial con su propia dirección *ethernet*, envía la respuesta directamente a la computadora que solicitó la información.

2.6 Servicios a nivel de red

Los servicios de red son tareas de tipo administrativo que deben realizarse al tener una red TCP/IP. El servicio más importante es crear un registro central de nombres y direcciones IP.

Existen organizaciones o empresas que realizan esta labor para toda la red *internet*. Es necesario mantener una base de datos que contenga la información de cada sistema de la red. Como mínimo, se necesita el nombre y la dirección IP de cada sistema y el administrador de red será el encargado de asignar direcciones IP. La base de datos debe ser capaz de verificar que no haya nombres duplicados en la red.

Lo más común es asignar las direcciones de la forma más simple, empezando por 1 y de manera correlativa. En cuanto a la asignación de nombres a las computadoras no es tan sistemática. Pueden ser cualquier expresión compuesta de letras, números y guiones. Desde el punto de vista de los usuarios, es recomendable que los nombres sean lo más cortos posibles. En algunos casos, los departamentos de una empresa eligen un tema o nombre relacionado con ellos.

Por lo anterior, el *software* TCP/IP necesita ser capaz de traducir nombres de computadoras en direcciones IP para poder abrir la conexión. La mayoría de *software* incluye dos vías para hacer esta traducción: una tabla

estática o un servidor de nombres. La tabla estática es indicada para pequeñas empresas u organizaciones, siempre y cuando no estén conectadas a otra red.

3. UNIÓN DE VOZ Y DATOS

3.1 Futuro de la unión de voz y datos

El desarrollo de las telecomunicaciones y de *internet* ha hecho que tecnologías enfocadas a la unión de voz y datos, comiencen a ser una realidad tanto en el mundo de los negocios, del ocio como de las investigaciones. En la actualidad se busca una homogeneidad de los medios de transporte de voz y datos.

La convergencia de las redes de telecomunicaciones actuales supone encontrar la tecnología que permita hacer convivir en la misma línea la voz y los datos. Esto obliga a establecer un modelo o sistema que permita empaquetar la voz para que pueda ser transmitida junto con los datos.

Existen una variedad de tecnologías que se están desarrollando actualmente en el uso simultáneo de voz y datos, es por ello que en este capítulo se habla de algunas de estas tecnologías: *voice*LAN, VoIP y *voicespan*.

3.2 Definición de *voice*LAN

*Voice*LAN describe un concepto que unifica todos los niveles funcionales y físicos de una red LAN y de las redes locales de voz. Permite ahorrar costos, tener una red con mayor flexibilidad, uniformidad y eficacia notable del servicio. Para los usuarios esto se traduce en una mayor facilidad de empleo y logra mayor familiaridad con las operaciones de sistema.

3.2.1 Red LAN extendida

Otro aspecto importante de la *voice*LAN es que permite trabajar con LAN extendidas o de área metropolitana, es decir que utilizan un acceso a distancia. En la actualidad un usuario no está fijo en un lugar, tiene la necesidad de estarse moviendo y ahora tiene acceso completo a la red de su empresa aún en la distancia.

Con la ayuda de las tecnologías de acceso distante, tales como *módems*, se han borrado las barreras de la distancia. Teniendo una red integrada, el mismo usuario distante con una sola conexión a la red corporativa, puede no solamente utilizar la red de datos, sino también a todas las aplicaciones de ella, tales como la voz.

Para el manejo de los medios de *voice*LAN en una red, se tiene dos opciones predominantes, ATM y *ethernet*, cada una de ellas tiene su ventaja; por ejemplo ATM es probablemente mejor en la manipulación de las necesidades en tiempo real en la voz, debido a su capacidad inherente de proporcionar una reservación de ancho de banda para un tipo específico de tráfico (voz). ATM aunque es una solución relativamente costosa para una LAN comparado con *fast* y *Gigabit ethernet*, *ethernet* es a menudo la mejor solución debido a su capacidad de utilizar tipos múltiples del tráfico.

3.2.2 Retardo de datos y voz

El retardo en el tráfico de los datos tiene cierto grado de tolerancia. Las aplicaciones interactivas, por ejemplo, pueden tolerar varios segundos de retardo mientras que esperan una respuesta a una petición.

Pero las aplicaciones de voz son intolerantes a los retardos, debido a la naturaleza del espectador. El retardo de la señal distorsiona el sonido de la voz, mientras que este serio retraso de la señal la hace inutilizable.

Dentro de una red LAN, desafortunadamente el retardo es un hecho real. Las redes de área local funcionan asumiendo que todo el tráfico en la red es igual, este principio esta basado en el diseño básico de *ethernet*. El protocolo de *ethernet*, en su modo original, no tiene ninguna capacidad para dar la prioridad a tipos de tráfico por clase y no proporciona una calidad garantizada en los estándares del servicio.

Para que los datos y la voz coexistan sin un estándar de calidad, los diseñadores de la red deben tener un cuidado extremo en el diseño del funcionamiento del tráfico. A menudo, esto se logra proporcionando un determinado ancho de banda como una posible solución de los retardos causados por el tráfico. La introducción de voz a la red de datos, establece un nuevo estándar de calidad y definitivamente tres soluciones son necesarias: la capacidad de dar una prioridad al tráfico; la capacidad de reservar un ancho de banda según sea el tipo de la aplicación; y la capacidad de proveer un mayor ancho de banda.

3.2.3 Ventajas de *voice*LAN

*Voice*LAN permite una integración profunda de la infraestructura de la red y de sus aplicaciones utilizadas. Esto es una realidad significativa para la industria de las telecomunicaciones en su totalidad y existen varias ventajas al poner en práctica esta tecnología. Estas ventajas incluyen:

- Ofrece una sola infraestructura que elimina los costos de los sistemas de voz.
- Permite a las empresas combinar muchas de las tareas tradicionalmente separadas de las redes de los datos y de la voz.
- Abre la puerta para la telefonía servidor/cliente, creando un lazo menos rígido y costoso.

3.3 Definición de voz sobre IP (VoIP)

La voz sobre IP (VoIP) es una de las soluciones propuestas y desarrolladas para encontrar un método que nos permita transmitir voz y datos sobre un protocolo de ám*bit*o mundial como lo es el protocolo IP, teniendo en cuenta que *internet* es una red de redes.

En la historia de la digitalización de la voz, fue hasta 1995 que la empresa *vocaltec* lanza al mercado su producto *Internet Phone* el cual permite el establecimiento de llamadas telefónicas de una computadora a otra y por medio de la transmisión *internet*.

VoIP se puede definir entonces como la capacidad de hacer llamadas telefónicas, haciendo todo lo que podemos hacer hoy con la red telefónica, incluso enviar fax, con redes de datos basadas en el protocolo IP con un estándar de calidad de servicio (QoS – *quality of service*), además con una relación de costo/beneficio superior.

3.3.1 Transmisión de paquetes

La transmisión de paquete de voz es similar a la transmisión de un correo electrónico desde el origen. hasta el destino. El problema es que en las transmisiones IP no está garantizado el éxito, por lo cual si el correo no es legible o se pierde un paquete, es necesario hacer la retransmisión del mismo y su recuperación es factible.

Pero en el caso de la transmisión de voz esto no es así, ya que la necesidad de recibir los paquetes en un determinado orden, así como la necesidad de asegurar que no haya pérdidas de información provoca que se implementen nuevas técnicas en la solución de este servicio.

El verdadero problema hoy en día es que la telefonía conmutada establece circuitos virtuales exclusivos entre el origen y el destino y ahí la calidad es innegable y segura. Por el contrario, la transmisión de voz sobre IP comparte el circuito y el ancho de banda con los datos y los paquetes pueden atravesar multitud de nodos antes de llegar a su destino, lo que supone deficiencias en la transmisión de paquetes de voz.

3.3.2 Calidad de transmisión de voz

Referente a la calidad de la transmisión de la voz, todos los fabricantes e investigaciones hacen referencia a tres factores determinantes:

- ✓ **Codificación de voz.** Influyen en la digitalización de la voz en paquetes de datos y que serán transmitidos por la red IP, también influyen por el retardo

necesario para la descompensación de esos paquetes de voz, lo que implica un mayor retardo en la comunicación.

- ✓ **Cancelación de eco.** Es un requerimiento necesario para una comunicación a través de VoIP que elimina de forma automática y en tiempo real posibles ecos, ya que si no lo hiciera haría inteligible la comunicación.
- ✓ **Latencia.** Es el tiempo necesario para que la voz viaje de un extremo a otro, incluyen los tiempos necesarios para la compresión, transmisión y descompresión.

Este tiempo tiende a minimizarse pero jamás podrá ser suprimido. Actualmente los tiempos que se están obteniendo de latencia giran alrededor de 120 ms en *internet*.

3.3.3 Aplicaciones de VoIP

VoIP se puede aplicar casi a cualquier necesidad de las comunicaciones de voz, extendiéndose desde un intercomunicador entre oficinas simple a los ambientes complejos de multiconferencia. La calidad de la reproducción de la voz que proporciona también se puede adaptar según la aplicación. Por ejemplo las llamadas de un cliente pueden necesitar una mayor calidad que las llamadas internas. Por lo tanto, el equipo de VoIP debe tener la flexibilidad de abastecer a una amplia gama de configuraciones, ambientes y la capacidad de mezclar la telefonía tradicional con VoIP.

Con lo anteriormente descrito, se pueden poner en marcha una serie de aplicaciones que son de gran demanda, las cuales producen de forma inmediata un ahorro significativo:

- Centros de llamadas (*call center*).

- Redes privadas virtuales de Voz (VPN).
- Centros de llamadas por la *WEB*.
- Aplicaciones de fax.
- Multiconferencia.

3.3.4 Ventajas en los servicios IP

Los servicios de VoIP presentan una multitud de ventajas en todos los aspectos. Su enumeración y explicación debe de realizarse de forma sencilla y transparente. Generalmente, las ventajas de la tecnología se pueden dividir en las cuatro categorías siguientes:

- **Reducción de costos.** Aunque la reducción de costos del servicio telefónico es siempre un asunto popular y proporciona una buena razón para introducir VoIP, los ahorros reales a largo plazo sigue siendo un tema de discusión en la industria. El compartir equipo y los costos de operación a través de datos y voz puede también mejorar la eficacia de la red, dado que el exceso de ancho de banda en una red se puede utilizar por la otra.

- **Simplificación.** Una infraestructura integrada que utiliza todas las formas de comunicación permite más estandarizaciones y reduce el complemento total del equipo. Esta infraestructura combinada puede utilizar la optimización dinámica del ancho de banda y un mejor diseño. Las diferencias entre los modelos de tráfico de voz y datos ofrecen otras oportunidades para las mejoras significativas de la eficacia.

- **Consolidación.** Una red IP permite combinar las operaciones comunes entre varios departamentos en una empresa y consolidar el uso de los recursos y servicios. Estos pueden ser, por ejemplo, directorios y bases de

datos que pueden fácilmente ser compartidos en forma segura y confidencial.

- **Aplicaciones avanzadas.** Aunque la telefonía básica y el fax son las aplicaciones iniciales para VoIP, se espera obtener mayores ventajas derivadas de los servicios multimedia y de aplicaciones de multiservicios.

3.4 Definición de *voicespan*

Voicespan es una tecnología de comunicación que pretende la transmisión simultánea de voz y datos de alta calidad en la red telefónica mundial, desarrollado por AT&T Pradyne.

VoiceSpan es una de las nuevas tecnologías la cual implemente "voz y datos simultáneos" (SVD – *simultaneous voice and data*).

3.4.1 Ventajas de la tecnología SVD

Por su alto nivel tecnológico, SVD ofrece un notable funcionamiento en:

- ✓ **Velocidad de datos muy altos.** Durante el silencio, es decir cuando la voz no está momentáneamente presente en el circuito, los datos se pueden enviar de 28.8 a 33.6 Kbps.
  Durante sonido, es decir cuando la voz está presente, los datos se transmiten de 16.8 a 24 Kbps. La velocidad eficaz media es en promedio de hasta 25.2 y 30.7 Kbps.

- ✓ **Alta calidad de audio.** Significa sonido de alta calidad, efectos sonoros, música y otros sonidos especiales.

- ✓ **Calidad de audio ajustable.** El usuario puede negociar la calidad del audio con respecto a la velocidad de datos que la aplicación le exige.
- ✓ **Los retardos más bajos.** El retardo de audio total transmitido al receptor, es a lo sumo de 60ms.

- ✓ **Funcionamiento confiable y robusto.** Incluso en llamadas internacionales y líneas telefónicas de mala calidad.

- ✓ **Protocolo de datos transparente.** SVD se acomoda a cualquier protocolo tanto síncrono como asíncrono.

Por su alta calidad, SVD proporciona un excelente funcionamiento en aplicaciones altamente interactivas, tales como juegos y aplicaciones de comunicación de audio y datos. Esta tecnología es compatible con las técnicas de compresión y almacenaje de audio comunes en *software*.

3.4.2 Aplicaciones de la SVD

La tecnología de SVD crea, permite y redefine principalmente nuevas aplicaciones individuales y cliente / servidor, incluyendo:

- ✓ **Cómputo en colaboración.** Se puede compartir y discutir los documentos con los compañeros de trabajo, al mismo tiempo que se corrigen.

- ✓ **Aprendizaje a distancia.** El usuario puede tomar las sesiones de la conferencia sin necesidad de estar presente en el mismo lugar. Al mismo tiempo puede interactuar recíprocamente y recibir retroalimentación.

- ✓ **Trabajo en casa.** Permite que el usuario tenga acceso remotamente a todas las funciones del servidor, y a las funciones del teléfono para proveer al usuario un aspecto del trabajo de oficina en su casa.
- ✓ ***Software* y soporte del sistema.** Permite diagnosticar mientras que se habla con el cliente. Ayuda experta en cualquier lugar.

- ✓ **Multiconferencia.** Se puede hacer multi-conferencias desde diferentes lugares y los usuarios interactúan entre sí.

- ✓ **Juegos interactivos.** Agrega una nueva dimensión a los juegos interactivos, desarrollando una estrategia contra opositor.

- ✓ **Compras vía telefónica.** Permite hacer las compras en línea más amigables, al interactuar con otra persona.

4. VOZ SOBRE IP (VoIP)

El crecimiento del uso de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y prioridad de tráfico, protocolos de transmisión, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP.

Si a lo anterior, se le suma el fenómeno *internet*, junto con el potencial ahorro económico que este tipo de tecnologías puede significar, la VoIP es un tema de actualidad para muchas empresas a nivel mundial.

El concepto original es relativamente simple: se trata de transformar la voz en paquetes de información manejables por una red IP. Gracias a otros protocolos de comunicación, como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

La voz puede ser obtenida desde un micrófono conectado a la placa de sonido de la computadora, o bien desde un teléfono común: existen *gateways* (que son positivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a *internet* para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información

analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Vale decir que es posible mantener conversaciones teléfono a teléfono.

Ciertamente, existen objeciones de importancia que tienen que ver con la calidad del sistema y con el tiempo entre fallas de las redes de datos, en comparación con las de telefonía. Sin embargo, la versatilidad y los costos del nuevo sistema hacen se esté comenzando a considerar la posibilidad de dar servicios sobre IP y, de hecho algunas están empezando a hacer pruebas.

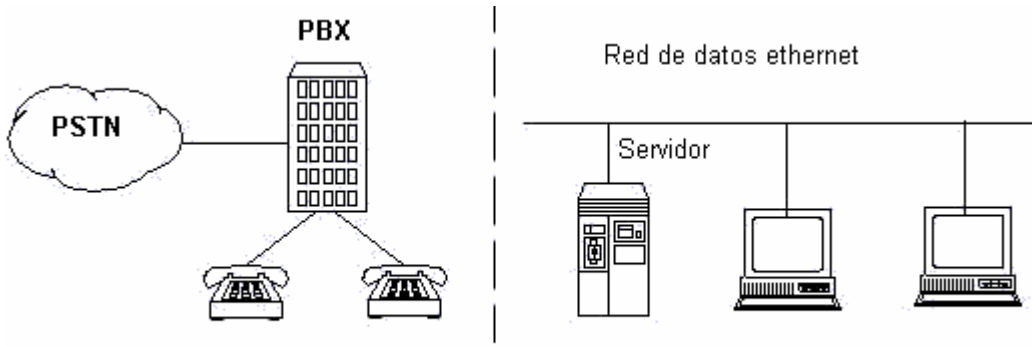
4.1 Arquitectura de una red de voz sobre IP

La convergencia de la voz a las redes de datos es un reto serio y complicado, si se toma en cuenta que esos dos tipos de información son esencialmente diferentes. Implementar una red convergente supone un estudio previo de las ventajas y desventajas que la red tradicional telefónica tiene respecto a la red de datos. Es por ello que es importante aclararlas.

4.1.1 Escenario tradicional de redes separadas

Tradicionalmente las áreas tecnológicas de redes de datos y telecomunicaciones (voz e imágenes) han estado separadas. Aun en la actualidad la mayoría de corporaciones y empresas poseen una central telefónica y una red LAN completamente separada para el transporte de datos. Ese esquema se muestra de una manera sencilla en la figura 20.

Figura 20. Redes de voz y datos separadas



Las señalizaciones de las redes telefónicas clásicas como la mostrada en la figura 20, cuya cuna fue la señalización transportada en banda, es decir, con cambios de nivel y tonos dentro del propio canal telefónico, 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 desarrolló su propia tecnología de conmutación, que consistía en una red digital integrada de transmisión más conmutación, es decir, las centrales digitales con un CPU capaz de controlar adecuadamente las conmutaciones. En este punto, el control de todo se realizaba por medio de un procesador que utilizaba protocolos de señalización para comunicarse con procesadores de otras centrales.

En la actualidad la red telefónica utiliza internamente una tecnología de redes que trabaja mediante el intercambio de paquetes de voz, que son meras

representaciones binarias de las señales analógicas de los sistemas precedentes.

Las redes telefónicas de voz y fax conmutadas se caracterizan porque:

- ✓ Es preciso realizar el establecimiento de llamada para iniciar la conexión.
- ✓ Se reservan recursos de la red durante todo el tiempo que dura la conexión.
- ✓ Se utiliza un ancho de banda fijo, típicamente 64 kbps por canal de voz, el cual puede ser consumido o no en función del tráfico.
- ✓ Los precios generalmente se basan en el tiempo de uso.
- ✓ Los proveedores están sujetos a las normas del sector y regulados y controlados por las autoridades pertinentes de telecomunicaciones.
- ✓ El servicio debe ser universal para todo ámbito o región.

Por el contrario, las redes de datos basadas en la conmutación de paquetes, se identifican por las siguientes características:

- ✓ Para asegurar la entrega de los datos se requiere el direccionamiento por paquetes, sin que sea necesario el establecimiento de llamada.
- ✓ El consumo de los recursos de red se realiza en función de las necesidades, sin que, por lo general, sean reservados siguiendo un criterio de extremo a extremo.
- ✓ Los precios se forman exclusivamente en función de la competencia entre de la oferta y la demanda.
- ✓ Los servicios se prestan de acuerdo a los criterios impuestos por la demanda, las aplicaciones que utilizan y variando ampliamente en cuanto a cobertura geográfica y velocidad de la tecnología aplicada.

Las diferencias entre la operación de las redes de voz y datos requieren distintos enfoques de gestión. Tradicionalmente la industria de la telefonía trabaja con altas exigencias de fiabilidad conocidas como “los cinco nuevos” 99.999 por ciento.

Esto se traduce en unos objetivos de diseño de centrales públicas de conmutación que garantizan niveles de caída del servicio de sólo dos horas cada cuarenta años de operación.

4.1.2 Escenario de una red que migra a VoIP y sus componentes

La migración o convergencia de la transmisión voz sobre una red de datos es posible gracias a que la voz se puede digitalizar, es decir, transformar en *bit* que se pueden agrupar en paquetes susceptibles de ser transmitidos a través de una red LAN de datos. Una red de comunicaciones no sabe sí lo que está transmitiendo es un registro de una base de datos o parte de una conversación telefónica que ha sido digitalizada. Con ello se consigue usar el mismo medio (la red) para distintas funciones, reduciendo así el costo de inversión y explotación.

La voz digitalizada puede ser transmitida en cualquier red IP, tanto en su vertiente *internet* (comunicación pública o externa) como Intranet (comunicación privada). Esto permite gozar de unas tarifas mucho más bajas que las ofertadas por los operadores convencionales, y lo que es más importante, independiente de la distancia.

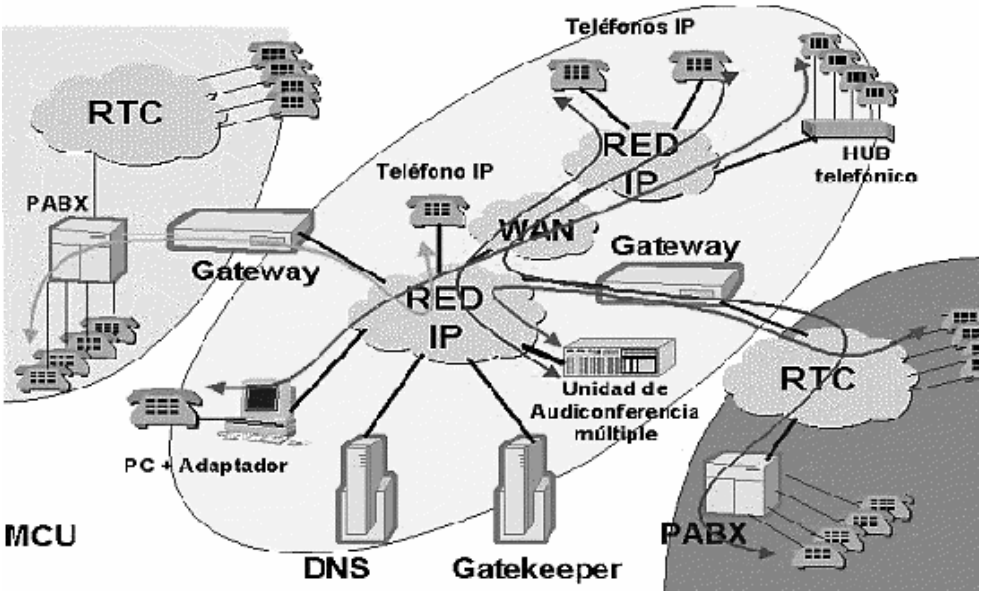
El hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, nos permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel

tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (*computer telephony integration*) tendrán una implantación muchos más simple.

Actualmente podemos partir de una serie de elemento ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son mostrados en la figura 21 y mencionados a continuación:

- Teléfonos IP.
- Adaptadores para PC.
- *Hub*s telefónicos.
- *Gateways* (pasarelas RTC/IP).
- *Gatekeeper* (no utilizado en todos los sistemas).
- Unidades de audioconferencia múltiple (MCU voz).
- Servicios de directorio.

Figura 21. Elementos de una red VoIP



Las funciones de los distintos elementos son fácilmente entendibles, sin embargo vale la pena recalcar algunas ideas.

4.1.2.1 *Gatekeeper* de VoIP

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 aquel.

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. Los *gatekeepers* de VoIP se conectan a los *gateways* o terminales mediante enlaces estándar H.323v2, utilizando el protocolo RAS H.225. Estos dispositivos intervienen también en la autenticación, enrutamiento, contabilidad de llamadas y determinación de tarifas.

4.1.2.2 *Gateway* de VoIP

El *gateway* es un elemento esencial en la mayoría de las redes pues su misión es la de proveer un acceso ininterrumpido a red VoIP y enlazarla con la red telefónica analógica o RDSI. La persona que realiza una llamada ingresa a un *gateway* por medio de un teléfono convencional discando un número de acceso. Una vez que la llamada fue autenticada, la persona disca el número deseado y oye los tonos de llamada habituales hasta que alguien responde del otro lado. Tanto quien llama como quien responde se sienten como una llamada telefónica típica.

Se puede considerar al *gateway* como una caja que por un lado tiene una *interface* LAN y por el otro dispone de uno o varios de las siguientes *interfaces*:

- FXO. Para conexión a extensiones de centralitas o a la red telefónica básica.
- FXF. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI.
- PRI. Acceso primario RDSI.
- G703/G704. (E&M *digital*) Conexión especifica a centralitas a 2 Mbps.

4.2 VoIP. Estándares de los distintos aspectos de la comunicación

La implementación de nuevos estándares viene a ser el anteproyecto necesario para diseñar, implementar y gestionar las comunicaciones de voz y datos. En su desarrollo trabajan diferentes entidades reconocidas como organizaciones de estándares internacionales, entre los que se encuentran:

ANSI (*American National Standars Institute*), IEEE (*Institute of Electrical and Electronics Engineers*), ISO (*Internacional Organization for Standardization*), UIT (*Unión Internacional de Telecomunicaciones*).

La interoperatividad multifabricante ya no es problema gracias a que el IMTC (*International Multimedia Teleconferencing Consortium*) avanza mucho en esta área crítica y son precisamente ellos, quienes en 1997 logran un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP.

Debido a que ya existe el estándar H.323 que se detallará más adelante, y que cubre la mayor parte de las necesidades para la integración de la voz, se decidió que éste fuera la base de la VoIP. De esto modo, la VoIP debe considerarse como una clarificación del H.323 de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se estableció que H.323 tendría prioridad sobre el VoIP.

La 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 establecimiento de nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional.

La VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación, éstos son:

4.2.1 Direccionamiento

El direccionamiento de una llamada consiste en localizar las estaciones o computadoras H.323 que desean comunicarse a través del *gatekeeper*. Los estándares utilizados para tal efecto son:

- RAS (***Registration, Admision and Status***). Protocolo de comunicación que permite a una terminal H.323 localizar a otra terminal H.323 a través del *gatekeeper*. Cabe mencionar que una terminal H.323, es una terminal que proporciona en tiempo real comunicación bidireccional con otro terminal H.323 o MCU. El intercambio de información incluye controles, indicaciones, audio, video y datos.

- DNS (***Domain Name Service***). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

4.2.2 Señalización

La señalización son los mensajes que se envían los terminales H.323 una vez realizado el direccionamiento mediante un mensaje RAS o DNS. El terminal llamante envía un mensaje al *gatekeeper* para que éste lo identifique. El *gatekeeper* puede aceptar o no la llamada y enviará al terminal llamante un mensaje de confirmación o negación. Los estándares de señalización son:

a) **Q.931. Señalización inicial de llamada:** define la interfaz y los mensajes de señalización entre el usuario y la red. El protocolo implementado a este nivel determina las rutas tomadas a través de la red para conectar a los usuarios entre sí.

b) **H.225. Control de llamada:** señalización, registro y admisión, paquetización y sincronización del flujo de voz. Cuando el llamante acepta la conexión, a través del canal H.225 se enviará la dirección IP donde establecer el canal H.245. El mensaje de "*setup*" contiene información del usuario necesaria para la sesión de conferencia, como el nombre identificador, localización geográfica, comentarios, etc. además de la dirección IP del usuario y el puerto TCP que usará para control en la fase de establecimiento.

c) **H.245. Protocolo de control:** especifica los mensajes de apertura y cierre de canales para los flujos de voz. Aquí se negocian los parámetros de la comunicación y después de obtenida toda esa información, la conexión TCP puede ser finalizada. Las entidades llamante y llamada determinan los codificadores a utilizar, número de conexiones y direcciones a utilizar, puertos y número de muestras por trama.

Esta comunicación debe permanecer mientras intercambien información los terminales y les permite modificar parámetros.

4.2.3 Compresión de voz

- **Requeridos:** G.711 y G.723. Estos protocolos de audio usan el sonido de entre 48 y 64 Kbps y dan una calidad de audio de teléfono. Especifican algoritmos para la comprensión del tráfico de la voz. El protocolo G.723 tiene la capacidad de realizar compresión de voz, datos y video.
- **Opcionales:** G.728, G.729 y G.722. Estos protocolos tienen también la capacidad de realizar compresión de voz y pueden ser soportados sin problema y son características principales son: G.722 (54, 56 y 48 Kbps), G.728 (16 Kbps) y G.729 (8 Kbps).

4.2.4 Transmisión de voz

En este punto, ambos terminales establecen canales de información a través de la arquitectura RTP/UDP/IP estandarizada para el intercambio de información. El estándar establecido es:

a) **UDP.** La transmisión se realiza sobre paquetes UDP, pues aunque no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

b) **RTP (*real time protocol*)**. Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en la recepción.

4.2.5 Control de la transmisión

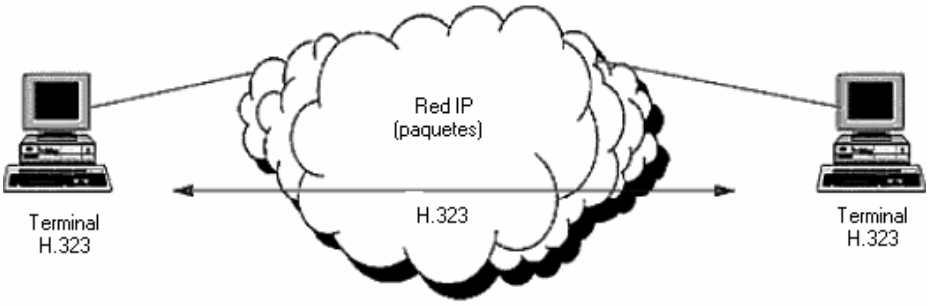
Mediante el control del flujo de información recibida, se logra obtener una buena calidad de comunicación mediante canales de realimentación. El protocolo RTCP es estándar y se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

4.3 Protocolo H.323. Arquitectura

H.323 es un estándar que especifica los componentes, protocolos y procedimientos que proporcionan servicios de comunicación multimedia (audio, vídeo y datos en tiempo real) sobre redes de paquetes (incluyendo las IP). H.323 es parte de la familia de las recomendaciones de la ITU-T llamadas H.32x que proporcionan servicios de comunicación multimedia sobre una gran variedad de redes.

Las redes de paquetes incluyen LANs, redes de empresas, MANs y WANs. H.323 puede ser aplicado en una gran variedad de modos: audio, audio + video, video + datos, datos + audio, y también puede ser aplicado sobre comunicaciones multipunto. En la figura 22 se muestra la comunicación de dos terminales H.323 en una red basada en paquetes como lo es una red IP.

Figura 22. Terminales H.323 en una red IP



4.3.1 Paquetización de la voz

La implementación de comunicaciones de voz sobre IP obliga a considerar el impacto que pueda tener sobre las actuales comunicaciones de datos. Es necesario saber que la voz sobre IP se puede desplegar al ritmo en que la red de datos esté preparada y que será el administrador quien decida este ritmo en función de la situación actual de su red de datos.

Siempre hay que recordar que las razones fundamentales de por qué implementar la voz sobre IP son:

- **Independencia de tecnología.** Las redes LAN y WAN pueden utilizar cualquier tecnología (*ethernet*, *token ring*, *ATM*, *frame relay*, etc.) y tipos de *hardware* y *software* en los *host*, las cuales son soportadas por numerosos fabricantes.

- **Flexibilidad.** Ofrece tolerancia a los errores con recuperación robusta ante fallos, posibilidad de enrutar datos entre diferentes redes o sub-redes.

- **Fácil de usar.** IP es un entorno abierto, probado en el mundo real durante muchos años y sus redes son las más económicas para instalar y mantener.

4.3.1.1 Muestreo

La señal de voz es continua en el tiempo y en amplitud. Para que pueda ser procesada por *hardware* y *software* digital es necesario convertirla a una señal que sea discreta tanto en el tiempo como en amplitud.

El muestreo consiste en el proceso de conversión de señales continuas a señales discretas en el tiempo. Este proceso se realiza midiendo la señal en momentos periódicos del tiempo. Sí se aumenta el número de muestras por unidad de tiempo, la señal muestreada se parecerá más a la señal continua.

La historia del muestreo de voz comienza con la codificación del canal vocal a 64 Kb/s, sin embargo, esta velocidad de muestreo no es la más apropiada para muchas aplicaciones debido a la elevada tasa de datos.

Esa velocidad ahora ha cambiado de acuerdo al tipo de codificadores y compresión que se utilizan. Los tipos de algoritmos de codificación vocal se codifican mediante los siguientes algoritmos:

- **Codificadores de forma de onda el dominio del tiempo:** PCM G.711, ADPCM G.726. Este tipo de codificadores intentan reproducir la forma de la onda de la señal de entrada sin tener en cuenta la naturaleza de la misma.

- **Codificadores de forma de onda en el dominio de la frecuencia:** ATC que utiliza la técnica de transformada discreta coseno DCT utilizada normalmente en codificadores de video.

- **Codificadores vocoder:** LPC en los que se codifican los parámetros relacionados con la percepción.

La codificación LPC (*linear predictive coders*) es útil para señales que pueden modelarse como un sistema lineal y se basa en la estimación lineal de la fuente. Además existen las codificaciones RPE, VSELP, CELP que son del tipo análisis y síntesis de la señal. La codificación VSELP (*vector sum excited linear predictive*) es usada en el sistema celular americano. Y la CELP (*code excited linear prediction*) se aplica en la norma G.729 para aplicaciones de voz sobre protocolo IP.

4.3.1.2 Ancho de banda

Hay que tener presente el ancho de banda de una comunicación de voz IP y el número de comunicaciones simultáneas que se requieran.

Habitualmente en el entorno LAN, donde se utiliza tecnología *switch* a 10 o 100 Mhz, se elige la compresión G711 con un ancho de banda de 84.7 Kb/s ya que se obtiene mayor calidad y se dispone de suficiente ancho de banda.

En cambio en el entorno WAN, donde el ancho de banda es más escaso y costoso, se elige la compresión G723 con un ancho de banda de 27.2 Kb/s. Afortunadamente el ancho de banda de las comunicaciones de voz no aumentará en el futuro y en cambio el ancho de banda en la WAN tiene a aumentar a la vez que los precios se reducen. Esto permitirá que cada vez sea más barato aumentar el número de comunicaciones de voz en la WAN.

Cuando se cambia la voz clásica (circuitos) a voz sobre IP (paquetes), hay que tener presente que los paquetes de datos de todas las aplicaciones (servidores de archivos, correo electrónico, Navegación por *internet*, video,

aplicaciones ERP, consultas a bases de datos, etc.) van a compartir las mismas “autopistas y carreteras” de datos.

Por esto habrá que tener presente el ancho de banda necesario de cada aplicación y su prioridad, con el fin de que la red de datos cumpla con los requisitos de cada tipo de aplicación.

4.3.1.3 Compresión

La parte final de la paquetización es la compresión. En este proceso se utiliza comúnmente el estándar internacional, el protocolo G.711, el cual es un esquema PCM que opera con una rata de muestreo de 8 Khz con 8 *bits* por muestra. Este protocolo es un estándar de audio telefónico que trabaja en un canal de 64 kbps.

De acuerdo al teorema de Nyquist, el cual establece que una señal debe ser muestreada al doble de su mayor componente de frecuencia, por lo que G.711 puede codificar frecuencias entre 0 y 4 Khz.

4.3.2 Uso del protocolo RTP/RTCP

RTP es un protocolo estándar para el transporte de datos (ya sea de audio o de video) en tiempo real sobre la *internet*, que hace funcional al protocolo H.323 para la aplicación de VoIP. El objetivo de este protocolo es el de conseguir independencia sobre el protocolo de transporte, de manera que pueda ser usado sobre otros protocolos.

RTP dispone de características comunes con protocolos de transporte. No obstante, difiere de ellos (por ejemplo TCP), en que no ofrece ninguna función de fiabilidad o de control de flujo y congestión.

Eso sí, siendo un protocolo abierto, dispone de la capacidad para que se le añadan estas funciones. Consta de una parte de control llamada RTCP (*real time control protocol*), aunque puede omitirse si se desea. El protocolo RTCP se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones que corrijan ese problema.

4.3.3 Arquitectura H.323

El estándar H.323 especifica 3 tipos de componentes, los cuales, trabajando juntos, proporcionan un servicio de comunicación multimedia punto-punto o punto-multipunto. Estos componente son los siguientes:

4.3.3.1 Terminal H.323

Utilizado para comunicación bidireccional multimedia, un terminal H.323 puede ser o bien un PC o un dispositivo, corriendo H.323 y las aplicaciones multimedia adecuadas. La comunicación que proporciona es en tiempo real con otro terminal, o con un MCU (*unidad de control multipunto*). Es importante recordar que un MCU también es un elemento funcional de la red H.323 que permite soportar comunicaciones multipunto, como lo es la conferencia entre varios terminales.

4.3.3.2 *Gatekeeper* H.323

Puede ser considerado el cerebro de la red H.323. Aunque no es obligatorio y es un elemento opcional de la arquitectura, los *gatekeepers* proporcionan importantes servicios tales como:

- El direccionamiento.
- La facturación.
- La autorización y autentificación de terminales y *gateways* H.323.
- La gestión del ancho de banda.
- Realizar enrutamientos de llamadas.

4.3.3.3 *Gateway* H.323

Un *gateway* conecta dos redes diferentes. Es decir, permite conectividad entre redes H.323 y redes que no sean H.323 (por ejemplo conectar una red H.323 con la RTC). Esta conectividad se consigue traduciendo los protocolos para establecimiento de llamada, convirtiendo el formato de la información, y transfiriendo información entre las dos redes conectadas por éste. Si un terminal H.323 quiere comunicarse con otro terminal en la misma red H.323 el *gateway* no es necesario.

4.3.4 Inicio, establecimiento y finalización de una llamada

Si se considera el escenario en el cual exista un *gatekeeper* el primer paso para la conexión entre dos terminales es el establecimiento de llamada. El protocolo H.225/RAS (*registration, admission and status*) es el protocolo entre extremos (terminales y *gateways*) y el *gatekeeper*.

La entidad llamante envía mensajes RAS solicitando la identificación del usuario llamante utilizando un mensaje llamada ARQ. El *gatekeeper* aceptará la llamada y enviará al terminal llamante un mensaje de confirmación llamado ACF, o bien rechazará la llamada mediante el mensaje ARJ.

4.3.4.1 Señalización de llamada H.225

Cuando el *gatekeeper* acepta la llamada, la entidad llamante establecerá una conexión TCP con el terminal llamado para establecer el canal de señalización H.225. Para ello, utilizará la información (dirección IP y puerto) recibidos del *gatekeeper* a través del mensaje ACF. La entidad llamante al recibir dicha conexión contactará con su *gatekeeper* a través del canal RAS solicitando permiso para poder contestar. En caso positivo (ACF), el llamante aceptara la conexión y a través de dicho canal H.225 enviará la dirección IP y el puerto, donde establecer ese canal para negociación de parámetros y control de comunicación.

Una vez obtenida esa información, la conexión puede ser finalizada, ya que no es necesario intercambiar mas parámetros a través de este canal.

4.3.4.2 Señalización de control de llamada H.245

Establecido el canal H.245 a través de una nueva conexión TCP, las entidades llamante y llamada determinaran los parámetros de la comunicación: Codificadores a utilizar, número de conexiones y direcciones a utilizar, puertos, número de muestras por trama, función maestro-esclavo, etc., lo que les permite establecer canales para la transmisión de medios (audio y datos).

Esta conexión debe permanecer mientras intercambien información los terminales H.323 y les permite modificar parámetros (*codecs*, muestras por trama, etc.).

4.3.4.3 Negociación y gestión de canales lógicos

En este punto, ambos terminales negocian y establecen canales de información a través de la arquitectura RTP/UDP/IP para el transporte de medios, así como canales de control a través de la arquitectura RTCP/UDP/IP para los canales de realimentación, al objeto de controlar la calidad de los flujos de información recibida por el otro extremo de la comunicación.

4.3.4.4 Finalización de llamada

Tras el intercambio de información las entidades H.323 deben informarse a través del canal H.245 y mediante el envío de las señales de finalización conocidas como *EndSessionCommand*, el fin de la llamada. Esta señal provocará el cierre del canal H.245. Además deberán informarle al *gatekeeper* mediante el envío del mensaje RAS DRQ (*disengage request*) que la llamada ha terminado. El *gatekeeper* inmediatamente puede liberar recursos y proporcionar información para la tarificación, entre otras.

4.4 Retardos de 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 inferior a 150 ms no es detectable. Si el retardo es mayor a 150 ms pero inferior a 300 ms es detectable pero no molesto.

Retardos mayores a 300 ms son molestos para mantener una conversación y resulta casi imposible llevarla de manera fluida.

Debido a que las redes LAN 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 ya mencionado anteriormente y 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.

4.4.1 Retardos fijos

El retardo fijo conocido como latencia es el que se produce a través del canal de comunicación. En otras palabras, es el tiempo que le toma a la señal digital atravesar el sistema desde la fuente hasta la aplicación correspondiente. La latencia es una característica propia del sistema, del equipo transmisión y tarjetas de red. La latencia incluye el tiempo que necesitan los equipos (*router*, servidor, tarjeta de red) en transformar o procesar la señal de datos y se manifiesta como un retardo corto entre la entrada y la salida de cada dispositivo.

4.4.2 Retardos variables

Otro tiempo de retardo es el conocido como *jitter*, que esta definido por el número de paquetes perdidos entre la entrada y la salida del sistema. Este retardo es la variación en la latencia, y mientras que la latancia se mide a nivel de señal, el *jitter* se mide en función de paquetes IP.

Idealmente el *jitter* debe ser cero para que el mensaje sea comprensible. Cuando la red tenga este tipo retardo, la voz deberá hacerse pasar por un sistema (*buffer*) que encole los paquetes de voz y entregue el mensaje retardado al oyente, pero sin paquetes perdidos.

4.5 Calidad de servicio QoS en VoIP

La calidad de servicio QoS en telefonía IP viene dada, entre otros aspectos, por la fiabilidad, el caudal y la seguridad. Para mejorar la calidad de la telefonía IP se debe dar soporte de calidad de servicio y aumentar el caudal o canal disponible.

La entrega de señales de voz y video desde un punto a otro no se puede considerar realizada con un éxito total a menos que la calidad de las señales transmitidas satisfaga al receptor. La calidad de la voz extremo a extremo, determinada por los sucesivos proceso de codificación–decodificación, y la pérdida de paquetes en la red es fundamental. Así mismo, la demora extremo a extremo, debido a procesos de codificación–decodificación, paquetización y compresión, afecta la interactividad en la conversación, y por tanto la QoS.

Las redes IP son redes del tipo *best-effort* y por tanto no ofrecen garantía QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, *jitter* y pérdidas de paquetes.

Por tanto, es necesario buscar QoS no sólo en la red, sino también en los terminales, y en los procesos que en los mismos se desarrollan, de ahí que sea necesario también decir que la sensibilidad a la pérdida de paquetes, a las demoras y sus fluctuaciones que experimentan los servicios de VoIP, dependen en buena medida de los mecanismos implementados en los terminales.

Los procesos como: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor, inciden directamente en la QoS. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita a la red poder manejar más conexiones simultáneas, pero se incrementa la demora y la distorsión de las señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

Otro aspecto a tener en cuenta es el compromiso entre la demora de paquetización y la utilización del canal (relación entre *bytes* de información y *bytes* de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de paquetización para cierto estándar de codificación. Claro está, según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50%, con un crecimiento de la demora en forma exponencial en el caso de los *codecs* de baja velocidad como el G.723.

Para resumir, entre los factores que afectan a la calidad se encuentran los siguientes:

- Requerimientos de ancho de banda. La velocidad de transmisión de la infraestructura de red y su topología física.

- Funciones de control. Incluye la reserva de recursos, provisión y monitoreo requeridos para establecer y mantener la conexión multimedia.

- Latencia y retardo. De la fuente al destino de la señal a través de la red.

- *Jitter*. Variación en los tiempos de llegada entre los paquetes.

- Pérdida de paquetes. Cuando un paquete de voz se pierde en la red es preciso disponer de algún tipo de compensación de la señal en el extremo receptor.

Para aumentar la QoS en una red de VoIP bien diseñada debe incluir los siguientes mecanismos:

- **RSVP:** *resource resServation protocol*, es un protocolo que permite la reserva del ancho de banda y definir el retardo máximo.

- **WFQ:** *weighted fair queuing* que permite dar prioridad a los paquetes de voz sobre otros menos críticos, como el correo por ejemplo.

- **WRED:** *weighted random early detect*, un algoritmo de control de congestión que permite monitorizar la carga, el descarte selectivo de paquetes y el control de flujo.

4.6 Fabricantes y componentes disponibles en el mercado para VoIP

Dos de las empresas pioneras en el desarrollo de VoIP y que estuvieron relacionadas con el estándar para VoIP, fueron 3COM *corporation* y *siemens public communications networks*. Trabajando conjuntamente, estas empresas integraron una vía de acceso a *internet* con el *switch* digital para producir el primer y único *switch* multi-servicio.

La plataforma *total control* de 3Com y el *switch* digital EWSD de Siemens permiten una nueva generación de funciones de llamadas personalizadas, incluyendo VoIP. Estas empresas poseen un acuerdo conjunto de desarrollo que combina un sistema de red de voz y datos para producir el primer y único *switch* multi-servicio *class* 5 EWSD que simplifica el acceso remoto a *internet*. El acuerdo logrado entre esas dos compañías los ubica en la vanguardia de la convergencia de redes.

Por su parte, Cisco desde 1999 ha venido optimizando su línea de productos y entre ellos, las mejoras en *software* y *hardware* para sus productos de acceso de múltiples servicios, lo que permite a los proveedores de servicio y a los clientes corporativos desarrollar infraestructuras de red a gran escala y de voz basadas en paquetes, a una fracción del precio de tecnologías tradicionales.

En *software* desarrollaron el Cisco IOS que ofrece la integración completa de la voz, video y datos. Adicionalmente, los *routers* de acceso de múltiples servicios de Cisco como los de las series 2600 y 3600, en combinación con su H.323 *Gatekeeper*, permite a los clientes construir redes muy grandes de VoIP. Y para ofrecer una solución ideal, los proveedores

pueden contar con el *Gateway* Cisco 5300 VoIP que facilita la administración de VoIP.

Otro fabricante de dispositivos para VoIP es Motorota ING y su objetivo es minimizar el costo de comunicaciones, un aspecto cada vez más crítico.

Esta reducción se está consiguiendo mediante el desarrollo de equipos flexibles, capaces de adaptarse a distintos entornos LAN (*ethernet*, *token ring*, SDLC) y WAN. Estos equipos tienen la capacidad además de manejar tráfico multimedia (voz y video), a fin de sacar el máximo rendimiento de las líneas de comunicaciones. Los equipos de Motorota ING son a la vez *router* y conmutador y pueden comunicarse utilizando redes WAN, públicas y privadas, de líneas punto a punto, RDSI, *frame relay* o IP. Además, dependiendo del modelo, los *routers* Motorota tienen *interfaces ethernet*, *token ring*, Serie y RDSI.

Uno de los productos que ofrece Motorota ING es el VOIP que permite utilizar la misma plataforma *hardware*, es decir, utilizar los mismos equipos y emplear tanto protocolos propietarios como protocolos estándar como el H.323.

5. REGULACIONES RESPECTO AL SERVICIO DE VoIP

5.1 Regulaciones internacionales

En lo que se refiere al marco legal, la legislación vigente desde 1998 de la Comisión Europea y de la española CMT (comisión del mercado de las telecomunicaciones) es clara: la transmisión de voz a través de *internet* utilizando teléfonos convencionales es un servicio de valor agregado y como tal, no tiene que cumplir regulaciones tradicionales de las operadoras tradicionales, ni contribuir al servicio universal, bastando una simple autorización administrativa para presentarlo.

A medida que se sale de un mercado regulado (telefonía tradicional) y se va hacia uno no regulado (datos), hay un ahorro significativo a causa de la competencia. Ya que sin restricciones legales los proveedores pueden implementar y ofrecer soluciones de todo tipo.

En los Estados Unidos, debido al rápido crecimiento de la VoIP la Comisión Federal de Comunicaciones (FCC por sus siglas en inglés), estudia desde el año 2003 imponer regulaciones a las compañías que ofrezcan VoIP, con las que tendrían que pagar varios de los mismos impuestos que pagan las compañías telefónicas tradicionales.

Según expertos para el sector empresarial en Latinoamérica, donde las tarifas telefónicas son muy altas, sobre todo en larga distancia, la opción de VoIP podría representar un gran respiro sobre sus costos de operación.

Ahora sólo falta esperar que harán las compañías telefónicas tradicionales con respecto a un servicio que podría convertirse en la nueva forma de comunicación.

5.2 Regulaciones para Guatemala

Actualmente en Guatemala existen diferentes posiciones en cuanto a las necesidades de introducir un marco regulatorio a los nuevos servicios relacionados con la telefonía IP. Por una parte, algunos son de la opinión de que es prematuro regular servicios que aún no cuentan con la madurez y presencia en el mercado como para poder sobrevivir a medidas reguladoras y de control.

Por otro lado, la experiencia dicta que la introducción de nuevos servicios en el mercado suele ser mucho más sencilla en aquellos países en los que existe un mercado estable, en lo que se refiere a leyes de competencia y medidas de protección al usuario, sin embargo, en aquellos otros en los que el mercado es dominado por un monopolio o por presencia de un operador que restringa el acceso a usuarios finales y la interconexión a redes internacionales, como antes lo era la empresa Guatemalteca de Telecomunicaciones; el marco regulatorio debe facilitar la entrada y supervivencia de los nuevos servicios y proveedores.

En cualquier caso, la necesidad o no, de introducir un marco regulatorio para los servicios de telefonía IP, vendrán condicionados a la realidad del mercado local en cada país.

En Guatemala, la Superintendencia de Telecomunicaciones tendrá que ser el ente regulador que determine, cuándo sea el momento, el marco legal que facultare y normare el desarrollo de VoIP.

Aunque como un comentario personal, considero que el Estado de Guatemala no tiene la capacidad económica ni tecnológica para regular redes tradicionales (datos), menos redes de VoIP. Si la realidad fuera otra y el Estado tuviera la capacidad, sería algo muy conveniente, principalmente para evitar competencia desleal entre los proveedores que ofrecen una solución de VoIP.

CONCLUSIONES

1. En la actualidad, un diseño adecuado de VoIP soportada sobre redes LAN privadas es una solución totalmente viable y operativa. Las empresas actualmente muestran gran inquietud por su aplicación, ya que su incorporación inmediata sobre Intranets es totalmente factible porque la calidad de la comunicación, el ahorro y el control de llamadas es evidente.

2. La instalación de una sola red dentro del ámbito de la empresa que maneja tanto datos como VoIP, brinda una ventaja importante a nivel de cableado e infraestructura. Y sí a esto le añadimos el bajo costo de mantenimiento, la gestión del administrador de red resulta más sencilla.

3. Un aspecto muy importante, que de momento constituye la gran barrera para implementar VoIP es la calidad de servicio QoS. Todas las soluciones de VoIP deberán garantizar esta calidad de servicio basándose en retardos no mayores a los 150 milisegundos y ancho de banda disponible en una red IP.

4. La ley de Guatemala y de muchos otros países en principio, no presentan inconvenientes para la implementación de la VoIP. Además, muchas consultoras internacionales presentan esta solución como una verdadera alternativa de negocios, razón por la cual VoIP ya ha empezado a utilizarse.

5. Se puede deducir que si el futuro es IP, debido sobre todo a su ám*bit*o de cobertura actual y su aceptación, VoIP puede abrir las puertas hacia la convergencia de redes. Esta convergencia supone en términos

económicos una auténtica revolución que afectará desde el entorno empresarial hasta el entorno doméstico y que se traduce en reducción de costos.

RECOMENDACIONES

1. Es conveniente considerar como parte de la implementación de VoIP, una solución de *software* que dote al administrador de la red de datos de herramientas potentes de control y definición de reglas. Ya que es preciso tener muy en cuenta que el dispositivo de control de tráfico (*gatekeeper*) debe mantener un nivel aceptable de saturación de la red. El control del ancho de banda permite, al administrador, fijar un límite de utilización, por encima del cual se rechazan las llamadas, bien sean internas o externas.

2. Es factible, en cuanto a otras capacidades añadidas a VoIP, asignar a cada dispositivo o terminal direcciones dinámicas mediante DHCP. De esta forma no se tiene ningún problema de movilidad o traslados de los diversos puestos de trabajo y usuarios. Este registro permite una localización física automática de cualquier usuario.

BIBLIOGRAFÍA

1. Caputo R. **Cisco packetized Voice & Data Integration**. McGraw Hill. june 1999.

2. Coulouris G.G., Jean Dollimore, Addison Wesley. **Distributed Systems, Concepts and Design**. 2a. ed. 1994.

3. Dufour I.G. **Network intelligence**. BT Telecomunications Series Chapman & Hall. 2000.

4. Goncalves M. **Voice over IP Networks**. Mc Graw Hill. october 1998.

5. Helg G. **Óbice Over Data Networks; Covering IP and *frame relay***. McGraw Hill. june 1998.

6. Hersen O., Gurle D., Petit J. **IP Telephony**. Addison Wesley. 1999.

7. Itu. **Tabla of Contents and Summary of Recommendation H.323, ITU**. august 1998.

8. Neves Adriano. **Voz sobre IP**. España: 2000

9. Prieto Alberto, Antonio Lloris, Juan Carlos Torres. **Introducción a la informática**. Impreso en España, 1989.

10. Tanembawm A. **Computer Networks**. Prentice – Hall. 1997.

11. Teixeira Manuel. **Voz sobre *frame relay*, IP y ATM**. España: 1999.

12. Vega B. **Señalización de redes digitales de telecomunicaciones**. Ahciet –ICT. 2a. ed. 2000.