8

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

"VOZ SOBRE IP (VoIP)"

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A :

EMMA MERCEDES FRONTANA URIBE

DIRECTOR DE TESIS: ING JESUS REYES GARCIA

MEXICO, D. F. 2001

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

DEDICATORIAS Y AGRADECIMIENTOS

Dedico esta tesis especialmente a mi madre, Emma Uribe Jiménez y mi padre Bernardo Frontana de la Cruz, quienes han trabajado toda su vida por la superación de sus hijos. Gracias por todo su cariño, regaños, apoyo y atinados consejos.

A mis hermanos Ber, Beto, Mando y Saris por su ejemplo de superación y perseverancia.

A Silver , por su apoyo, cariño y compañía.

A mis amigas Erika García, Claudia Ayala, Miriam Reyes, Rita Saloma, Hilda Solís y Mónica García, con quienes he compartido alegrías y tristezas, y de quienes he aprendido mucho.

A todos mis compañeros y amigos de generación por el apoyo recibido durante la carrera.

Agradezco al Ingeniero Jesús Reyes García por las enseñanzas compartidas y por la confianza recibida en la elaboración de la presente tesis.

Al Dr. David Covarrubias y a todo el grupo de comunicaciones inalámbricas del Centro de Investigación y de Estudios Superiores de Ensenada, B.C. Por su confianza.

Al Centro de Instrumentación y Registro Sísmico, en especial al Ing Juan Manuel Espinoza, por las atenciones recibidas durante mi estancia en el centro.

A la Universidad Nacional Autónoma de México, en especial a la Facultad de Ingeniería: a todos mis profesores por su enseñanza y dedicación, a los administrativos, investigadores y trabajadores quienes día a día ponen su mayor esfuerzo para que la UNAM continúe siendo la máxima casa de estudios de nuestro país.

INTRODUCCIÓN

La transmisión y la conmutación de voz en forma de paquetes sobre redes de datos ha suscitado, en los últimos años, un interés considerable, principalmente como resultado de la aparición de los DSPs (Procesador Digital de Señal) potentes y de bajo costo.

Aunque la técnica VoFR (Voz sobre Frame Relay) no tuvo el éxito esperado, con la excepción quizás de Estados Unidos, introdujo varios mecanismos fundamentales para el transporte de voz en forma de paquetes, en especial la normalización de los algoritmos de codificación y de compresión de voz.
Además, la explosión de Internet, con el resultado de la adopción del protocolo IP (Protocolo de Internet) como protocolo universal de la red, ha conducido a una normalización activa de la señalización y del transporte de voz sobre la red IP. La combinación de las redes de voz y datos que permite la tecnología VoIP (Voz sobre IP) presenta un considerable interés para los proveedores de servicios de Internet porque les permite competir con los operadores convencionales de telefonía, sin tener que desplegar nuevas redes.

Por lo que respecta a las empresas, la convergencia de las redes de voz y de datos presenta igualmente varias ventajas; único cableado hasta la oficina, una única infraestructura de red, una única gestión de red, una mejor de integración de las aplicaciones de voz y de datos, la creación de nuevas aplicaciones, etc.

Para asegurar estas convergencias, los suministradores de productos de red han tenido que reunir sus capacidades provocando una ola de fusiones y adquisiciones sin precedentes en el sector de las telecomunicaciones.

Dada la gran penetración que tiene actualmente en nuestras vidas el teléfono y a que todavía no existe otra tecnología de telecomunicaciones más usada, resulta de gran importancia el estudio de nuevos métodos no tradicionales, como es el caso de Voz sobre IP (VoIP) para ofrecer servicios telefónicos, lo que motivó la elaboración de la presente tesis.

El presente trabajo de tiene como objetivo exponer los conceptos básicos y características de las redes IP, para comprender el funcionamiento de la tecnología VoIP, así como estudiar las diferentes aplicaciones que permite la implementación de VoIP. Básicamente consistió en un trabajo de investigación, el cual esta dividido en seis capítulos. A continuación se describe brevemente el contenido de cada uno.

El primer capítulo se estudia el origen de la telefonía y de la suite de protocolos TCP/IP, que dieron origen a la mundialmente famosa Internet, particularmente al Protocolo de Internet (IP), pieza fundamental en el surgimiento de la tecnología VoIP (Voz sobre IP).

En el segundo capítulo se analiza las diferentes funciones que realizan las diferentes capas que componen la suite de protocolos TCP/IP: capa física, capa de enlace de datos, capa de red, capa de transporte y capa de aplicación, las cuales desempeñan funciones específicas, que complementan a las demás.

En el tercer capítulo, se estudia la red IP, iniciando con la infraestructura que conforma este tipo de redes. En la primer sección se estudia las diferentes tecnologías de redes de área local (tecnologías LAN); ethernet, token ring y FDDI, después se estudia las tecnologías de redes de área amplia (tecnologías WAN); X.25, Frame Relay, ISDN y ATM. Posteriormente se habla de los dispositivos de interconexión necesarios para interconectar redes que se encuentran separadas físicamente como son los repetidores, los puentes, los enrutadores y los gateways. En la tercer sección se estudia el enrutamiento IP. Posteriormente se mencionan algunas técnicas que pueden ser implementadas para implementar la seguridad en una red IP. Finalmente se estudia la multidifusión, y la calidad de servicio (QoS) en redes IP, este último tema de suma importancia en la actualidad debido a que las aplicaciones de hoy en día como es el caso de VoIP requieren un aseguramiento de la calidad de servicio, para poder funcionar en forma adecuada, más allá del best-efford (mejor esfuerzo), el cual caracteriza a las redes IP más antiguas.

En el cuarto capítulo se estudian los aspectos fundamentales de la tecnología VoIP, desde cómo sé paquetiza la voz y los aspectos involucrados en este proceso, pasando por los codificadores de voz estandarizados para VoIP. También se estudian los estándares para VoIP, de los cuales se estudia con mayor profundidad el estándar de la ITU, H.323 ya que es el que más aceptación ha conseguido. En la penúltima sección se estudia la calidad de voz en redes IP, la cual debe tomarse en cuenta para el futuro exitoso de VoIP, se mencionan los principales elementos que afectan la calidad de voz y que deben ser tomados en consideración. Finalmente se habla de los aspectos de seguridad y su importancia en las aplicaciones VoIP.

En el quinto capítulo se estudian los factores que influirán para que VoIP tenga el éxito esperado, entre los cuales destaca el adecuado aseguramiento de la QoS como a la que estamos acostumbrado utilizando la red telefónica pública conmutada. Se presentan las principales aplicaciones y servicios que son posibles gracias a VoIP. Finalizando con las ventajas y desventajas que tienen los servicios IP.

En el sexto capítulo, se mencionan las principales operadoras que prestan servicios IP en México, así como las principales soluciones que existen en el mercado para implementar VoIP a nivel empresarial.

Finalmente se presentan las conclusiones del trabajo elaborado.

1. ANTECEDENTES

1 ANTECEDENTES

1.1 ORIGENES DE LA TELEFONIA.

El descubrimiento y aplicación de la electricidad representó un enorme avance social y económico. Pronto las comunicaciones tuvieron que adaptarse a ese nuevo estilo y, entre 1830 y 1844, se inventó el telégrafo eléctrico pero, por desgracia, no ofrecía un contacto personal ni directo.

Años más tarde, el sacerdote francés Gauthey propuso un sistema de transmisión de voz mediante tubos acústicos. Posteriormente varios científicos, como Robert Hooke, Joseph Henry, Michael Faraday y muchos otros, realizaron importantes avances pero sin éxito. Hasta que, en 1860, el alemán Philipp Reis inventó un aparato al que llamó teléfono, del griego "hablar a lo lejos", que transmitía sonidos en breves intervalos de tiempo.

Sin embargo sería Alexander Graham Bell, quien realizaría el invento del siglo. En 1871 inició sus investigaciones. Cuatro años más tarde, fabricó un sistema muy elemental que patentó bajo el título "Mejoramiento de transmisores y receptores para telégrafos eléctricos" y, en 1876, patentó otro avance: "Mejoras a la telegrafía". Al mismo tiempo Bell profundizó sus investigaciones para perfeccionar la transmisión de la voz humana. Sus ensayos culminaron aquel 10 de marzo de 1876, al probar su nuevo aparato que funcionaba con una pila eléctrica. Con ese aparato su ayudante sólo recibía señales audibles muy débiles por lo que, para reforzarlas, se le ocurrió aumentar la densidad de la pila eléctrica y le agregó ácido sulfúrico, parte del líquido se derramó y le quemó la pierna: "*Mr. Watson, come here, I want you* [Señor Watson, venga aquí, lo necesito]". Watson escuchó el llamado con insólita claridad... El teléfono había nacido.

El 10 de mayo de 1876, en la Academia de Artes y Ciencias de Boston, Bell presentó y demostró su sistema y sus fundamentos científicos, ganándose la admiración de todos. Tiempo después, ya con la patente, el 12 de febrero de 1877, Bell llevó a cabo la primera comunicación de larga distancia y habló por teléfono desde Boston, a través de una línea telegráfica, con un periodista que estaba en Salem, a 25 kilómetros de allí. Un año después se inició la comercialización del teléfono, cuando George W. Coy construyó, en New Haven, la primera central telefónica, con una veintena de clientes. Así surgió la Bell Telephone System Co., la cual posteriormente se convertiría en la National Bell Telephone Company. Pronto ingresó a la compañía Francis Blake, quien inventó un nuevo tipo de transmisor que permitía una comunicación bastante más clara. Este fue el detonador para que el teléfono adquiriera gran popularidad en las grandes ciudades de Estados Unidos y algunas de América Latina. En Europa el impacto fue inmediato. En Gran Bretaña se instaló una central telefónica y luego el servicio pasó a ser monopolio gubernamental, situación similar a la que se produjo en Francia y Alemania. A partir de entonces el avance no cesó, la vida del ser humano había cambiado, al fin lograba rebasar con su voz las distancias [21].

1.2 ORIGENES DE LA SUITE DE PROTOCOLOS TCP/IP.

Entre finales de los sesenta y principios de los setenta, la Internet comenzó a tomar la forma de una red de área extendida llamada ARPANET. La ARPANET fue creada en 1969 por la Agencia de Proyectos de Investigación Avanzados, del Departamento de Defensa de los Estados Unidos (Defense Advanced Research Proyects Agency, DARPA). Consistió de computadoras interconectadas usado un sistema experimental de conmutación de paquetes. Para 1972 se realizaron demostraciones en las cuales muchas terminales se conectaron a una variedad de servidores utilizando enlaces de telecomunicaciones. Conforme el experimento continuó, existió una creciente necesidad de simplificar el proceso de interconectar diferentes tipos de computadoras. Cada fabricante de computadoras usaba diferentes técnicas tanto en hardware como en software para enlazar sus sistemas. El objetivo era desarrollar un método de interconexión que pudiera soportar muchos tipos de computadoras diferentes sobre diferentes métodos de transmisión, incluyendo velocidades bajas, altas y conexiones inalámbricas.

El desarrollo del conjunto de protocolos TCP (Transmission Control Protocol, Protocolo de Control de Transmisión) se inició en 1973 por Bob Kahn, de DARPA y Vinton Cerf de la Universidad de Standford. Para 1978 estaba casi totalmente terminado y desde entonces se ha llamado TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet) debido a los requerimientos de dividir el protocolo TCP en un protocolo orientado a conexión (TCP), y un protocolo extremo a extremo no orientado a conexión (IP). DARPA (Defense Advanced Research Proyects Agency) financió a la Universidad de California en Berckeley para integrar TCP/IP a su versión UNIX. El producto integrado se convirtió en un éxito comercial y ayudó a marcar a TCP/IP como el estándar de funcionamiento entre redes a escoger en los Estados Unidos.

En 1975, la ARPANET se convirtió en una entidad de operación más que de experimentación, por lo que su funcionamiento fue transferido a la Agencia de Comunicaciones del Departamento de Defensa de los Estados Unidos (DCA, Defense Communications Agency). Así la DCA comenzó a administrar la red. En 1985, NSF (National Science Foundation, Fundación Nacional de Ciencia) inició el financiamiento de la creación de una dorsal (backbone) que pudiera enlazar muchas universidades e institutos de investigación. Esta fue llamada NSFnet, remplazando la ARPANET y convirtiéndose en la dorsal de Internet. En la figura 1.1 se ilustra la dorsal NSFNET.

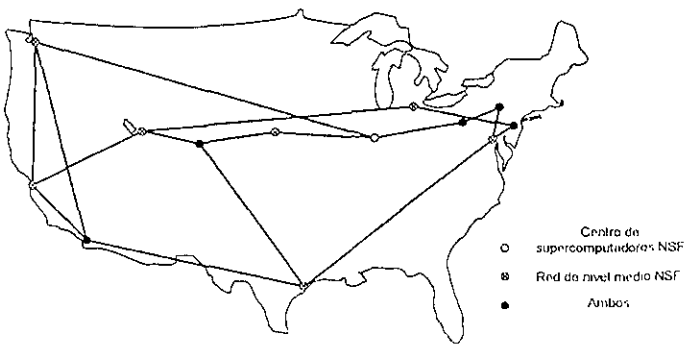

FIG 1.1 La dorsal (backbone) de NSFNET en 1988.

Desde entonces, el conjunto de protocolos TCP/IP ha continuado evolucionando. Uno de los aspectos más importantes del desarrollo de TCP/IP fue el programa de prueba y certificación llevado a cabo por el gobierno para asegurar que los desarrolladores conocieran los estándares TCP/IP publicados. Los estándares fueron divulgados y puestos a disposición del público, libres de licencia, para asegurar que los desarrolladores no adaptarán el estándar a sus necesidades, y llegarán a causar confusión con el resto de la comunidad TCP/IP.

1.3 ORIGENES DE VoIP o TELEFONIA EN INTERNET

Aproximadamente, cada diez años, el servicio de telecomunicaciones más básico, el teléfono sufre cambios dramáticos. En los años cincuentas; la introducción del cable coaxial trasatlántico permitió realizar llamadas internacionales sin hacer uso de las operadoras. En la década de los sesenta; la conmutación digital y la transmisión digital mejoraron drásticamente la calidad del audio. En 1970 con la entrada de los conmutadores programables se hizo posible la marcación por tonos así como la activación de servicios locales como la llamada en espera. Durante los años ochentas la implementación de sistemas para Señalización Por Canal Común como la Señalización Número Siete (SS7) hicieron posible servicios como los números 800. Estos cambios definen un salto de la transmisión y la señalización analógica, a la transmisión y señalización digitales, la transmisión utilizando circuitos conmutados y señalización basada en paquetes. En la década de los noventas, la telefonía en Internet marcó el último gran paso en esta lenta evolución hacia una infraestructura totalmente basada en paquetes. Realmente la historia de la Telefonía en Internet o VoIP comenzó hace veinte años aproximadamente. Los primeros artículos acerca de cómo transmitir voz fueron publicados a los inicios de los años setentas y el primer experimento en transmisión de paquetes de audio se realizó en agosto de 1974, cuando fue demostrada la transmisión de paquetes de voz en tiempo real entre el Instituto De Ciencias de la Información de la Universidad de Carolina del Sur y el Laboratorio Lincoln del Instituto Tecnológico de Massachussets. El primer RFC(Request for comments) acerca de paquetes de voz, el RFC 741 se publicó en 1977 [23].

En 1995, Vocaltec introdujo una de las primeras aplicaciones de telefonía en Internet para PC. Posteriormente fueron lanzados al mercado los Gateways para el Sistema Telefónico Público Conmutado (PSTN, Public Switched Telephone System) limitados únicamente a algunos puertos analógicos.

Cabe mencionar el impresionante desarrollo a nivel mundial de la telefonía móvil celular con más de 250 millones de abonados en la actualidad.

Hoy en día, la telefonía es la tecnología de mayor penetración en nuestras vidas. No existe otra tan utilizada como la de un aparato telefónico. Pero si la telefonía es una herramienta fundamental en el desarrollo de los negocios, también es uno de los rubros de mayor gasto en las empresas. Por eso, no es casual que se consideren varios métodos no tradicionales para la reducción de los costos telefónicos La

convergencia de las redes de voz y datos posibilita esa necesidad de disminuir costos, además de un mejor aprovechamiento de nuevos recursos y tecnologías disponibles en la actualidad.

Voz sobre IP es una tecnología que posibilita la integración de Voz y Datos con una capa de transporte ***común*** para estos dos mundos. Por ahora, las aplicaciones que utilizan la tecnología de Voz sobre IP apuntan al reemplazo de la red telefónica tradicional en comunicaciones de larga distancia. No sólo las empresas privadas pueden hacer uso de esta tecnología. También las telefónicas pueden beneficiarse con el desarrollo de redes y/o servicios en nuevas áreas con un costo de inicio varias veces inferior.

2. LA SUITE DE PROTOCOLOS TCP/IP.

2 LA SUITE DE PROTOCOLOS TCP/IP

2.1 LA SUITE DE PROTOCOLOS TCP/IP.

Aunque poca gente sabe lo que es TCP/IP (Transmisión Control Protocol/ Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet) todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca y es el más importante el protocolo IP(Internet Protocol, Protocolo de Internet). El nombre TCP/IP proviene de los dos protocolos más importantes de la familia: el TCP y el IP. Todos juntos llegan a ser más de 100 protocolos diferentes definidos en esta suite de protocolos [24].

El conjunto de protocolos TCP / IP es la base de la Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PCs, minicomputadoras y computadoras centrales sobre redes de área local y área extendida. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos ejecutándose en la ARPANET, una red de área extensa del departamento de defensa [25]. Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en máquinas de cualquier tamaño
- Estándar de EEUU desde 1983

La arquitectura de un sistema utilizando TCP/IP presenta las siguientes ventajas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimiento de extremo a extremo
- Protocolos estandarizados

2.2 ESTRUCTURA INTERNA DE LA SUITE TCP/IP.

El modelo básico en Internet y por tanto de TCP/IP es el modelo Cliente / servidor. La arquitectura de Internet está basada en capas. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (*International Standard Organization*) para la interconexión de sistemas abiertos (OSI) (ver Fig. 2.1) [25]. No

existe un modelo oficial de protocolos TCP/IP, al contrario del modelo OSI. Los protocolos se han ido definiendo anárquicamente, y a posteriori han sido englobados en capas.

<table>
<tr><td>Aplicación
Presentación
Sesión</td><td colspan="2">TELNET</td><td>FTP</td><td>SNMP</td><td>SMTP</td><td>DNS</td><td>HTTP</td></tr>
<tr><td>Transporte</td><td colspan="7">TCP</td></tr>
<tr><td>Red</td><td colspan="7">IP</td></tr>
<tr><td rowspan="2">Liga de Datos</td><td colspan="5">802.2</td><td>X.25</td><td>LLC/SNAP</td></tr>
<tr><td>802.3</td><td colspan="3">802.5</td><td colspan="2">LAPB</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td colspan="2">Token Ring</td><td>FDDI</td><td colspan="2">Línea Síncrona WAN</td><td>SONET</td></tr>
</table>

FIG 2.1 Relación entre la suite de protocolos TCP/IP con el modelo OSI.

La suite de protocolos TCP/IP esta organizada en las siguientes capas:

- Capa Física
- Capa de Enlace de datos
- Capa de Red
- Capa de Transporte
- Capa de Aplicación

2.2.1. LA CAPA FISICA

La capa física es la base de todas las redes. La capa física se encarga de la transmisión de bits a través del medio físico. El medio físico no se apoya en los servicios de ningún otro nivel, tampoco añade ningún encabezado a la información proveniente del nivel superior. Las características más importantes de esta capa son las siguientes:

- *Mecánicas*. Relacionadas con el tipo de conectores que se utilizan.
- *Eléctricas*. Relacionadas con la forma de representación de los bits.
- *Funcionales*. Relacionadas con las funciones que van a desarrollar los circuitos individuales que hay entre el sistema y el medio físico.
- *Procedimentales*. Especifican la secuencia de eventos por los cuales las cadenas de bits son transmitidas.

Los servicios que proporciona el nivel físico son los siguientes:

- Conexiones físicas
- Puntos extremos de conexión física secuenciamiento.
- Notificación de condición de fallo.
- Parámetros de calidad de servicio

2.2.2 LA CAPA DE ENLACE DE DATOS

El principal servicio de la capa de enlace de datos es ofrecer una comunicación eficiente y confiable entre dos sistemas que estén directamente conectados, para esto emplea funciones de control de flujo, detección y corrección de errores, las cuales serán estudiadas con mayor detalle en la siguiente sección. Las redes de difusión (generalmente redes LAN (Local Area Network, Red de Area Local)) tienen una consideración adicional en la capa de enlace de datos: controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos se encarga de este problema; la subcapa de acceso al medio ó subcapa MAC, la cuál será estudiada más adelante.

2.2.2.1 FUNCIONES DE LA CAPA DE ENLACE

Las principales funciones de la capa de enlace son:

- Creación de la trama de datos (enmarcado)
- Establecimiento y liberación de la conexión de enlace.
- Partición de la conexión de enlace de datos.
- Delimitación y sincronización de las tramas.
- Control de secuencia de los datos.
- Detección y corrección de errores.
- Control de flujo de los datos.
- Intercambio de identificaciones y parámetros.

La unidad básica de transmisión de datos en la capa de enlace es la trama. A continuación se hablará un poco más de las funciones de enmarcado, control de flujo, y control de errores, las cuales son las más importantes a nivel de enlace de datos.

ENMARCADO

A fin de proporcionar servicios a la capa de red, la capa de enlace de datos debe usar los servicios proporcionados a ella por la capa física. Lo que hace la capa física es aceptar un flujo de bits en bruto e intentar entregarlo al destino. No se garantiza que este flujo de bits esté libre de errores. El número de bits recibidos puede ser menor, igual o mayor que el número de bits transmitidos, y pueden tener diferentes valores. Es responsabilidad de la capa de enlace de datos detectar y, de ser necesario corregir los errores.

El enfoque común es que la capa de enlace de datos divida el flujo de bits en tramas discretas y que calcule la suma de comprobación para cada trama. Cuando una trama llega a su destino, se recalcula la suma de comprobación. Si la nueva suma de comprobación calculada es distinta de la contenida en la trama, la capa de enlace de datos sabe que ha ocurrido un error y toma medidas para manejarlo

Una forma de lograr esta división en tramas es introducir intervalos de tiempo entre las tramas, sin embargo, las redes pocas veces ofrecen garantías sobre la temporización, por lo que es posible que estos intervalos sean eliminados o que puedan introducirse otros intervalos durante la transmisión.

Dado que es demasiado riesgoso depender de la temporización para marcar el inicio y el fin de cada trama, se han diseñado otros métodos [1]. En esta sección veremos cuatro métodos.

1. Conteo de caracteres.
2. Caracteres de inicio y fin, con relleno de caracteres.
3. Indicadores de inicio y fin, con relleno de bits.
4. Violaciones de codificación de la capa física.

El primer método de enmarcado se vale de un campo del encabezado para especificar el número de caracteres en la trama. Cuando la capa de enlace de datos del destino ve la cuenta de caracteres, sabe cuántos siguen, y por tanto dónde está el fin la trama. Esta técnica se muestra en la figura 2.2 para cuatro tramas de 5,5,8 y 8 caracteres de longitud, respectivamente. El problema con este algoritmo es que la cuenta puede alterarse por un error de transmisión. Por ejemplo, si la cuenta de caracteres de 5 en el segundo trama de la figura 2.2 (b) se vuelve un 7, el destino perderá la sincronía y será incapaz de localizar el inicio la siguiente trama.

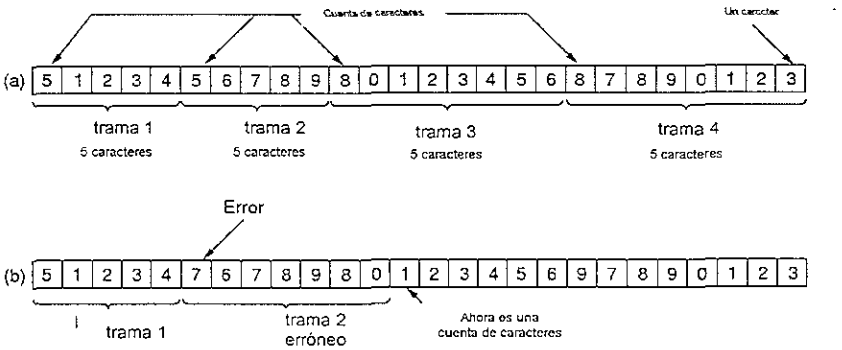

FIG. 2.2 Una corriente de caracteres. (a) Sin errores. (b) Con un error.

El segundo método de enmarcado supera el problema de resincronización tras un error, al hacer que cada trama comience con la secuencia de caracteres ASCII *DLE STX (Data Link Escape Start of Text, Escape de enlace de datos, Inicio de Texto)*, y termine con la secuencia *DEL ETX* (Data Link Escape End of Text, Escape de enlace de datos, Fin de Texto). De esta manera, si el destino llega a perder la pista de los límites de la trama, todo lo que tiene que hacer es buscar la secuencia de caracteres antes mencionada. Hay un problema importante con este método, cuando se transmiten datos binarios, ya que puede ocurrir fácilmente que los caracteres correspondientes a *DLE STX* o a *DLE ETX* ocurran en los datos, lo que interferirá el enmarcado. Una forma de resolver este problema es hacer que la capa de enlace de datos inserte un caracter ASCII *DLE* justo antes de cada caracter *DLE* "accidental" de los datos. La capa de enlace de datos del lado receptor quita

DETECCION Y CORRECCION DE ERRORES

La manera de asegurar la entrega confiable de datos es proporcionar al transmisor realimentación sobre lo que está ocurriendo en el otro lado de la línea. Un protocolo de nivel de enlace que quiere enviar tramas eficientemente debe de alguna manera ser capaz de recuperar las tramas perdidas o descartadas. Esto se consigue normalmente usando una combinación de dos mecanismos fundamentales: *acuses de recibo* (*acknowledgments*) y *temporizadores* (*timeouts*). Un acuse de recibo, comúnmente referido como *ACK*, es una pequeña trama de control con que el receptor informa al emisor de que ha recibido la transmisión. Si el emisor no recibe un ACK en un tiempo razonable la retransmite; este tiempo está medido por un temporizador. Normalmente, la trama se recibirá correctamente y el acuse llegará antes de que el temporizador termine, en cuyo caso se cancelará el temporizador. Sin embargo, si la trama o el acuse se pierde, el temporizador terminará, alertando al transmisor sobre un problema potencial. La solución obvia es simplemente transmitir de nuevo la trama. Sin embargo, aún cuando las tramas pueden transmitirse muchas veces, hay el peligro de que el receptor acepte la misma trama dos o más veces y que la pase a la capa de red más de una vez. Para evitar que ocurra esto, generalmente es necesario asignar números de secuencia a las tramas de salida, para que el receptor pueda distinguir las retransmisiones de los originales.

Se han desarrollado dos estrategias básicas para manejar los errores. Una es incluir suficiente información redundante en cada bloque de datos transmitido para que el receptor pueda deducir lo que debió ser el carácter transmitido. Otra estrategia es incluir sólo suficiente redundancia para que el receptor sepa que ha ocurrido un error (pero no qué error) y entonces solicite una retransmisión. La primera estrategia usa *códigos de corrección de errores*; la segunda usa *códigos de detección de errores*.

CONTROL DE FLUJO

Un problema que se presenta en la capa de enlace es qué hacer con un transmisor que sistemáticamente quiere enviar tramas a una velocidad mayor que aquella con que puede aceptarlos el receptor. Aún si la transmisión está libre de errores, en cierto punto el receptor simplemente no será capaz de manejar las tramas según van llegando y comenzará a perder algunos. La solución común es introducir un control de flujo para controlar la velocidad del transmisor de modo que no envíe a mayor velocidad que la que puede manejar el receptor. Este control de velocidad generalmente requiere algún mecanismo de realimentación, para que el transmisor pueda enterarse si el receptor es capaz de mantener el ritmo o no.

2.2.2.2 LA SUBCAPA DE ACCESO AL MEDIO

Cuando únicamente hay un medio común de transmisión, como ocurre en algunos sistemas de comunicaciones, el cuál necesita ser utilizado por varios usuarios, independientes entre ellos, surge la necesidad de establecer una estrategia de gestión o protocolo de acceso al medio a fin de gestionar y asignar el medio común de transmisión. Si no se considerase ningún tipo de protocolo, podrían ocurrir conflictos si más de un usuario quisiera acceder al recurso al mismo tiempo.

El protocolo de acceso al medio, en inglés Medium Access Control Protocol o simplemente MAC, es el encargado de gestionar cómo y cuándo cada uno de los usuarios de un sistema pueden utilizar el medio común de transmisión para enviar su información, este protocolo pertenece a la subcapa de control de acceso al medio (MAC). La subcapa MAC tiene especial importancia en las LAN (Local Area Network, Red de Area Local) casi todas éstas usan un canal multiacceso como base de su comunicación.

En la literatura existe un gran número de protocolos de acceso múltiple definidos y, fundamentalmente, todos ellos juegan con el grado de aleatoriedad del acceso, de modo que existe una clasificación que va desde el acceso puramente aleatorio de protocolos como S-ALOHA (Slotted ALOHA, ALOHA Ranurado) que reducen la aleatoriedad al máximo, donde se englobarían por ejemplo, las técnicas de sondeo o *polling*. En función de este grado de aleatoriedad, a continuación se detalla una primera clasificación que se podría efectuar de los protocolos de acceso múltiple.

- ***Asignación fija.*** La capacidad del canal (ancho de banda, ranura temporal o código) se reparte estáticamente entre los diferentes usuarios, que disponen el recurso de forma continua independientemente de sí hay o no hay información a transmitir. Propiamente aquí no existe ningún tipo de protocolo, puesto que no se establecen reglas específicas para regular el acceso al recurso. Los ejemplos más conocidos de estos protocolos son: FDMA (Frequency Division Multiple Access, Acceso Múltiple por División de Frecuencia), TDMA (Time División Múltiple Access, Acceso Múltiple por División de Tiempo) o DS/CDMA (Direct-Sequence Code Division Multiple Access, Acceso Múltiple por División de Código de Secuencia Directa).
- ***Asignación bajo demanda.*** La capacidad del canal se reparte ordenadamente entre los usuarios que disponen de información para transmitir. Este tipo de estrategias engloba las técnicas de sondeo o *polling*, en las cuales de forma centralizada la estación central periódicamente pregunta a los usuarios si disponen de información para transmitir y en caso afirmativo les asignaría el recurso en cuestión. La gran ventaja de estas técnicas es que garantizan que cada usuario disponga del recurso en propiedad sin verse afectado por el resto pero, en contrapartida, si hay muchos usuarios involucrados, el retardo consumido para preguntar a los usuarios, es muy grande y puede ocasionar retrasos en quienes verdaderamente sí necesitan del recurso.
- ***Acceso aleatorio repetitivo.*** Los usuarios acceden al recurso de forma aleatoria, lo que origina que puedan producirse colisiones en el caso de que dos o más de ellos quieran acceder a un mismo recurso simultáneamente. En este caso, deben implementarse mecanismos para resolver estas colisiones. El ejemplo más clásico de este tipo de protocolos lo constituye el protocolo ALOHA o su versión ranurada, S-ALOHA.
- ***Acceso aleatorio con reserva.*** Unicamente existe la posibilidad de colisionar en el acceso inicial al recurso, debido a que se efectúa sin tener ningún conocimiento acerca de lo que va hacer el resto de los usuarios. Una vez que se ha conseguido el acceso al canal se reserva el recurso de tal forma que los demás usuarios no intentarán acceder al mismo hasta que se haya completado la transmisión en curso. Dentro de este conjunto de protocolos se pueden destacar, entre otros los protocolos PRMA (Packet

Reservation Multiple Access, Acceso Múltiple por Reservación de Paquetes) y PRMA ++, en los que se habilita dentro de una estructura de trama un conjunto de ranuras temporales para enviar peticiones de acceso y otras ranuras temporales para la transmisión de información. En principio este protocolo fue diseñado para ser usado con la técnica de acceso TDMA, aunque también han aparecido versiones que permiten el uso de CDMA (Code Division Múltiple Access, Acceso Múltiple por División de Código).

2.2.3 LA CAPA DE RED

Esta capa se estudiará a profundidad en el próximo capítulo por lo que únicamente se mencionarán sus características generales, así como el formato del encabezado de trama IP.

El objetivo de la capa de red es proporcionar la ruta para una comunicación extremo a extremo a las entidades de transporte, independientemente de la forma en que se encuentren interconectados los sistemas que se quieren comunicar. Este nivel permite la transferencia de datos entre sistemas finales a través de uno o varios tipos de redes de datos, por lo que los niveles superiores no necesitan saber nada sobre como se realiza la transmisión en los niveles inferiores ni de la tecnología de conmutación utilizada para conectar los sistemas. Para lograr su cometido, la capa de red debe conocer la topología de la subred de comunicaciones (es decir, el grupo de enrutadores) y escoger las trayectorias adecuadas a través de ella; también debe tener cuidado de escoger las rutas a modo de evitar la carga extra de algunas de las líneas de comunicación y de los enrutadores mientras deja a otros sin trabajo. Por último, cuando el origen y el destino están en redes diferentes, es responsabilidad de la capa de red el manejo de estas diferencias y la resolución de los problemas que causan. La unidad básica de la capa de red es el datagrama[1].

EL DATAGRAMA IP.

El datagrama tiene dos partes: cabecera y texto; la cabecera tiene una parte fija de 20 bytes y una opcional de entre 0 y 40 bytes. La estructura de la cabecera es la que se muestra en la siguiente figura 2.4 [1].

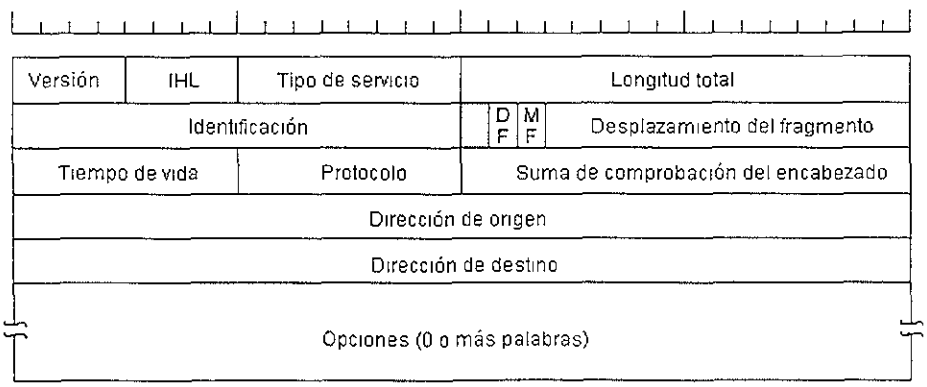

FIG. 2.4 La cabecera IP

A continuación analizaremos la cabecera campo por campo:

- **Campo Versión (Version).** Lleva el registro de la versión del protocolo al que pertenece el datagrama. Actualmente, es la 4 aunque se empieza a extender el uso de una nueva versión (la 6) con una estructura de datagrama diferente.

- **Longitud de cabecera (Internet Header Lenght).** Este campo es utilizado dado que la longitud de la cabecera no es constante. Se utiliza para saber donde empieza y donde acaba la cabecera, en palabras de 32 bits.

- **Tipo de Servicio (Type of service).** Permite seleccionar distintos tratamientos del datagrama mientras atraviesa la red (Prestaciones y Servicio de red). Son posibles varias combinaciones de confiabilidad y velocidad.

- **Longitud Total (Total Lenght).** Especifica la longitud del datagrama completo (cabecera incluida) en bytes. La longitud máxima es de 65,535 bytes.

- **Identificación (Identification).** Es necesario para que el destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

A continuación viene un bit sin uso y luego dos campos de 1 bit. *DF* significa no fragmentar (Don't fragment); es una orden para los enrutadores de que no fragmenten el datagrama, porque el destino es incapaz de juntar las piezas de nuevo. *MF* significa más fragmentos. Todos los fragmentos excepto el último tienen establecido este bit, que es necesario para saber cuándo han llegado todos los fragmentos de un datagrama.

- **Desplazamiento del fragmento (Fragment offset).** Indica en qué parte del datagrama actual va este fragmento. Todos los fragmentos excepto el último del datagrama deben tener un múltiplo de 8 bytes, que es la unidad de fragmento elemental. Dado que se proporcionan 13 bits, puede haber un máximo de 8192 fragmentos por datagrama, dando una longitud máxima de datagrama de 65,526 bytes, uno más que el campo de longitud total.

- **Tiempo de vida.** Es un contador que sirve para limitar la vida de un paquete. Se supone que este contador cuenta el tiempo en segundos, permitiendo una vida máxima de 255 seg; debe disminuirse en cada salto y se supone que disminuye muchas veces al encolarse durante un tiempo grande en un enrutador. En la práctica, simplemente cuenta los saltos. Cuando el contador llega a cero, el paquete

' *Los paquetes independientes de la organización de tipo sin conexion se llaman datagramas*

se descarta y se envía de regreso un paquete de aviso al servidor de origen. Esta característica evita que los datagramas vaguen eternamente, algo que de otra manera podría ocurrir si se llegan a corromper las tablas de enrutamiento.

Una vez que la capa de red ha ensamblado un datagrama completo, necesita saber qué hacer con él.

- **Protocolo.** Indica el protocolo de transporte al que debe entregarse el datagrama. TCP es una posibilidad, pero también está UDP y algunos más. La numeración de los protocolos es global en toda la Internet, y se define en el RFC 1700.

- **Suma de comprobación de la cabecera.** Verifica solamente la cabecera. Tal suma de comprobación es útil para la detección de errores generados por palabras de memoria erróneas en un enrutador. La suma de comprobación de la cabecera debe recalcularse en cada salto, pues cuando menos uno de los campos siempre cambia (el campo de tiempo de vida).

- **Dirección de origen (source address) y dirección de destino (destination address).** Corresponden a direcciones IP de origen y destino respectivamente.

- **Opciones.** No siempre están soportados en los enrutadores y se utilizan muy raramente; de estos podemos destacar las opciones mostradas en la tabla 2.1.

TABLA 2.1 Opciones del IP.

Opción	Descripción
Seguridad	Especifica qué tan secreto es el datagrama
Enrutamiento estricto desde el origen	Indica la trayectoria completa a seguir
Enrutamiento libre desde el origen	Da una lista de los enrutadores que no deben evitarse
Registrar ruta	Hace que cada enrutador agregue su dirección IP
Marca de tiempo	Hace que cada enrutador agregue su dirección y su marca de tiempo

2.2.4 LA CAPA DE TRANSPORTE

La capa de transporte no es sólo otra capa. Es el corazón de la jerarquía completa de los protocolos. La tarea de ésta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina de destino, independientemente de la red o redes físicas en uso. Sin la capa de transporte, el concepto total de los protocolos tendría poco sentido.

La capa de transporte ofrece dos tipos de servicios: *servicios orientados a conexión y servicios no orientados a conexión.* El servicio de transporte orientado a conexiones es parecido al servicio de red orientado a conexiones en muchos sentidos. En ambos casos, las conexiones tienen tres fases: establecimiento, transferencia de datos y liberación. El direccionamiento y el control de flujo también son

semejantes en ambas capas. Además, el servicio de transporte sin conexiones es muy parecido al servicio de red sin conexiones.

Para lograr un transporte de datos confiable la capa de transporte debe mejorar la QoS (Quality of Service, Calidad del Servicio)[2] proporcionada por la capa de red. El servicio de transporte puede permitir que el usuario especifique valores preferidos, aceptables y mínimos para varios parámetros de servicio en el momento de establecerse la conexión. Algunos parámetros también se aplican al transporte sin conexiones. Es responsabilidad de la capa de transporte examinar estos parámetros y, dependiendo de los tipos de servicio de red disponibles, determinar si puede proporcionar el servicio requerido. Algunos parámetros QoS, que se presentan resumidos en la tabla 2.2 Es importante aclarar que pocas redes y protocolos proporcionan todos estos parámetros. La gran mayoría simplemente hacen su mejor esfuerzo para reducir la tasa de errores.

Tabla 2.2 Parámetros de calidad de servicio típicos de la capa de transporte

Retardo de establecimiento de conexión
Probabilidad de falla de establecimiento de conexión
Rendimiento
Retardo de tránsito
Tasa de errores
Protección
Prioridad
Tenacidad

El servicio de transporte se implementa mediante un protocolo de transporte entre las dos entidades de transporte. En ciertos aspectos, los protocolos de transporte se parecen a los protocolos de enlace de datos, ambos se encargan del control de errores, la secuencia y el control de flujo. Sin embargo, existen diferencias significativas entre los dos. Estas diferencias se deben a diferencias importantes entre los entornos en que operan ambos protocolos, como se muestra en la figura 2.4. En la capa de enlace de datos, dos enrutadores se comunican directamente mediante un canal físico mientras que, en la capa de transporte, este canal físico es reemplazado por la subred completa

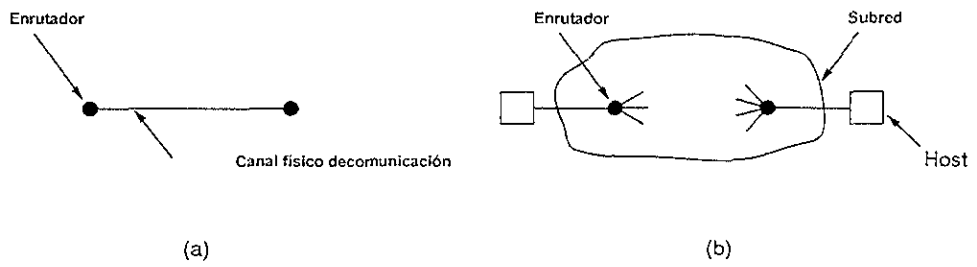

FIG. 2.4 (a) Entorno de la capa de enlace de datos. (b) Entorno de la capa de transporte.

[2] *La Calidad de Servicio se define como el tratamiento que se le da a cada paquete de un flujo de datos en los diferentes nodos por los*

El modelo TCP/IP tiene dos protocolos principales en la capa de transporte, un protocolo orientado a conexiones, el TCP, y uno sin conexiones, el UDP. En la siguiente sección estudiaremos ambos.

2.2.4.1 PROTOCOLOS DE LA CAPA DE TRANSPORTE

La capa de transporte es donde operan los protocolos TCP (Transmission Control Protocol, Protocolo de Control de Transmisión) y UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario). El TCP es un protocolo orientado a conexión y es responsable de la transferencia confiable de los datos entre dos computadoras. UDP es un protocolo no orientado a conexión. Es utilizado en lugar del protocolo TCP en situaciones donde no se necesiten utilizar todos los servicios de TCP. Algunas de las aplicaciones que utilizan UDP son: tráfico telefónico, el protocolo trivial de transferencia de archivos (TFTP, Trivial File Transfer Procotocol) y el procedimiento de llamada remoto (RPC, Remote Procedure Call).

EL PROTOCOLO TCP.

En esta parte daremos un repaso general del protocolo TCP, en la siguiente sección veremos la cabecera del protocolo, campo por campo.

El TCP se diseñó específicamente para proporcionar una corriente de bytes fiable a través de una interred[3] no confiable. Una interred es diferente a una sola red porque las distintas partes pueden tener topologías, anchos de banda, retardos, tamaño de paquete y otros parámetros con grandes diferencias. TCP fue diseñado para adaptarse dinámicamente a las propiedades de la interred y para ser robusto ante muchos tipos de fallas.

Cada byte en una conexión TCP tiene su propio número de secuencia de 32 bits. Se usan los números de secuencia tanto para acuses de recibo como para el mecanismo de ventana, que utilizan campos de cabecera de 32 bits distintos.

La entidad TCP transmisora y la receptora intercambian datos en forma de segmentos. Un segmento consiste en una cabecera TCP fija de 20 bytes (más una parte opcional)seguida de cero o más bytes de datos. El software de TCP decide el tamaño de los segmentos; puede acumular datos de varias escrituras para forma un segmento, o dividir los datos de una escritura en varios segmentos. Hay dos límites que restringen el tamaño del segmento. Primero, cada segmento, incluida la cabecera TCP, debe caber en la carga útil de 65,535 bytes del IP. Segundo, cada red tiene una unidad máxima de transferencia o MTU (Maximum Transfer Unit), y cada segmento debe caber en la MTU.

Un segmento demasiado grande para transitar por una red puede dividirse en varios segmentos mediante un enrutador. Cada segmento nuevo recibe sus propias cabeceras TCP e IP, por lo que la fragmentación en los enrutadores aumenta la carga extra total (puesto que cada segmento adicional agrega 40 bytes de información de cabecera).

El protocolo básico usado por las entidades TCP es el protocolo de ventana corrediza. Cuando un transmisor envía un segmento, también inicia un temporizador. Cuando llega el segmento al destino, la

[3] *Se define interred como un conjunto de redes interconectadas*

entidad TCP receptora devuelve un segmento (con datos, si existen de otro modo sin ellos) que contiene un número de acuse de recibo igual al siguiente número de secuencia que espera recibir. Si el temporizador del transmisor expira antes de la recepción del acuse de recibo, el transmisor envía de nuevo el segmento.

Aunque este protocolo se ve sencillo, tiene muchos vericuetos como veremos a continuación. Por ejemplo, dado que los segmentos pueden fragmentarse, es posible que llegue una parte del segmento transmitido y que la entidad TCP receptora envíe un acuse de recibo, pero la otra parte se pierda. También pueden llegar segmentos fuera de orden. Además pueden retardarse segmentos en tránsito durante tanto tiempo que el transmisor termina de temporizar y retransmite nuevamente. Si un segmento retransmitido toma una ruta distinta a la del original y se fragmenta de manera diferente, pueden llegar esporádicamente partes tanto del original como del duplicado, requiriéndose una administración cuidadosa para lograr una corriente de bits confiable. Por último siendo tantas las posibles redes que pueden conformar la interred, es posible que un segmento pueda toparse ocasionalmente con una red congestionada (o rota) en alguna parte de su trayectoria. El TCP debe estar preparado para manejar y resolver estos problemas de una manera eficiente.

Cuando la carga ofrecida a cualquier red es mayor que la que puede manejar, se genera un congestionamiento. TCP para evitar que ocurra el congestionamiento al establecer una conexión, tiene que seleccionar un tamaño de ventana adecuado. El receptor puede especificar una ventana con base en su tamaño de buffer. Si el transmisor se ajusta a su tamaño de ventana, no ocurrirán problemas por desbordamiento de buffers en la terminal receptora, pero aún pueden ocurrir debido a congestionamientos internos en la red.

El TCP usa varios temporizadores (al menos conceptualmente) para hacer su trabajo. El más importante de éstos es el temporizador de retransmisión. Al enviarse un segmento, se inicia un temporizador de retransmisiones. Si el acuse de recibo del segmento llega antes de expirar el temporizador, éste se detiene. Si, por otra parte, el temporizador termina antes de llegar el acuse de recibo, se retransmite el segmento (y se inicia nuevamente el temporizador

LA CABECERA DEL SEGMENTO TCP

En la figura 2.5 se muestra la distribución de un segmento TCP. Cada segmento comienza con una cabecera de formato fijo de 20 bytes. La cabecera fija puede ir seguida de opciones de cabecera. Tras las opciones, si las hay, pueden continuar hasta 65535-20-20=65515 bytes de datos, donde los primeros 20 se refieren a la cabecera IP y los segundos a la cabecera TCP.

Los segmentos sin datos son legales y se usan por lo común para acuses de recibo y mensajes de control.

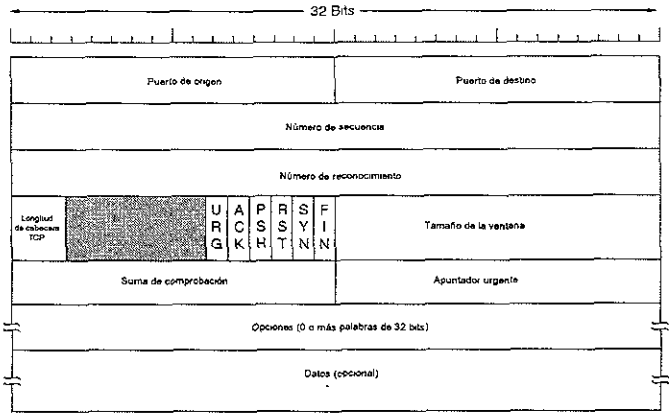

FIG. 2.5 Cabecera TCP

A continuación analizaremos la cabecera campo por campo:

- **Campos Puerto de origen y puerto de destino(Source/Destination Port Numbers).** Identifican los puntos terminales locales de las conexiones. Cada máquina puede decidir por sí mismo la manera de asignar sus propios puertos comenzando por el 256. La dirección de un puerto más la dirección IP de su host forman un TSAP único de 48 bits. Los números de socket de origen y de destino en conjunto identifican la conexión. Este campo tiene una longitud de 32 bits.

- **Campo número de secuencia (sequence number).** Indica el número de secuencia del primer byte de datos en este segmento. El campo tiene una longitud de 32 bits.

- **Campo número de acuse de recibo (también llamado número de reconocimiento).** Si el bit de control ACK esta activado, el campo contendrá el valor del siguiente byte que el receptor espera recibir. El campo tiene una longitud de 32 bits.

- **Campo Longitud de cabecera TCP (TCP Header Lenght).** Indica la cantidad de palabras de 32 bits contenidas en la cabecera TCP. Esta información es necesaria porque el campo de opciones es de longitud variable, por lo que la cabecera también. Técnicamente, este campo en realidad indica el comienzo de los datos en el segmento, medido en palabras de 32 bits, pero ese número es simplemente la longitud de la cabecera en palabras, por lo que el efecto es el mismo.

A continuación viene un campo de 6 bits que no se usan. Este conjunto de bits está reservado para uso futuro. Posteriormente vienen seis banderas de 1 bit.

- *URG.*

El apuntador urgente sirve para indicar un desplazamiento en bytes a partir del número actual de secuencia en el que se encuentran datos urgentes. Este recurso sustituye los mensajes de interrupción. Se establece en 1 si está en el apuntador urgente.

- *ACK.*

Se establece en 1 para indicar que el número de acuse de recibo es válido. Si el ACK es 0, el segmento no contiene un acuse de recibo, por lo que se ignora el campo de número de acuse de recibo.

- **PSH.**

El bit PSH indica datos empujados (con PUSH). Por este medio se solicita atentamente al receptor entregar los datos a la aplicación a su llegada y no ponerlos en buffer hasta la recepción del buffer completo.

- **RST.**

Se usa el bit RST para restablecer una conexión que se ha perdido debido a una caída de servidor u otra razón; también sirve para rechazar un segmento no válido o un intento de abrir una conexión.

- **SYN.**

El bit SYN se usa para establecer conexiones. La solicitud de conexión tiene SYN=1 y ACK=0 para indicar que el campo de acuse de recibo incorporado no está en uso. La respuesta de conexión sí lleva un reconocimiento, por lo que tiene SYN=1 y ACK=1. En esencia, el bit SYN se usa par denotar CONNECTION REQUEST Y CONNECTION ACCEPTED, usándose el bit ACK para distinguir entre ambas posibilidades.

- **FIN.**

Se usa para liberar una conexión; especifica que el transmisor no tiene más datos que transmitir. Sin embargo, tras cerrar una conexión un proceso puede continuar recibiendo datos indefinidamente. Ambos segmentos SYN y FIN, tienen números de secuencia y por tanto tienen garantía de procesarse en el orden correcto.

- **Campo Ventana.** El control de flujo en el TCP se maneja usando una ventana corrediza de tamaño variable. El campo de ventana indica la cantidad de bytes que pueden enviarse comenzando por el byte que ya se ha enviado de acuse de recibo. Este campo contiene un entero de 32 bits.

- **Campo Suma de Comprobación.** Este campo es usado para fiabilidad extrema. Es una suma de comprobación de la cabecera, los datos y la pseudocabecera conceptual mostrada en la figura 2.6. Al realizar este cálculo, se establece el campo de suma de comprobación del TCP en cero, y se rellena el campo de datos con un byte cero adicional si la longitud es un número impar. El algoritmo de suma de

comprobación simplemente suma todas las palabras de 16 bits en complemento a 1 y luego obtiene el complemento a 1 de la suma.

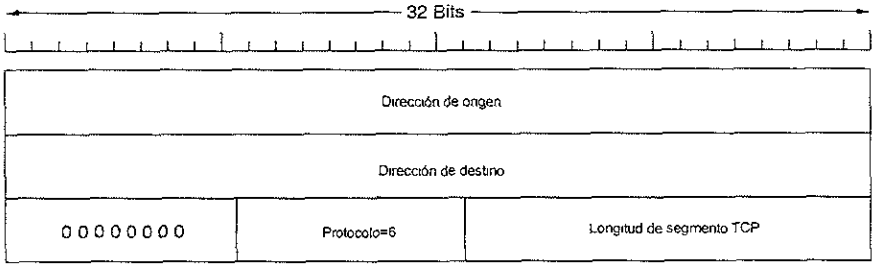

FIG. 2.6 Pseudocabecera incluida en la suma de comprobación del TCP.

La pseudocabecera contiene las direcciones IP de 32 bits de las máquinas de origen y de destino, el número de protocolo de TCP, y la cuenta de bytes de segmento TCP (incluida la cabecera). La inclusión de la pseudocabecera en el cálculo de la suma de comprobación TCP ayuda a detectar paquetes mal entregados.

- **Campo Apuntador urgente.** Apunta al primer octeto de datos para indicar que los datos que le siguen son urgentes. Este bit es significativo únicamente cuando esta establecido en 1.

- **Campo de Opciones.** El campo Opciones se diseñó para contar con una manera de agregar características extra no cubiertas por la cabecera normal. La opción más importante es la que permite que cada host especifique la carga útil TCP máxima que está dispuesto a aceptar. El uso de segmentos grandes es más eficiente que el de segmentos pequeños. Durante el establecimiento de la conexión, cada lado puede anunciar su máximo y ver el de su compañero. El más pequeño de los dos es el que se utilizará. Si un host no usa esta opción, predetermina una carga útil de 536 bytes. Si este campo tiene el primer octeto a cero, esto indica que no hay opciones.

EL PROTOCOLO UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario).

El protocolo UDP ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto encapsulados sin tener que establecer una conexión. Muchas aplicaciones cliente-servidor que tienen una solicitud y una respuesta usan el UDP en lugar de tomarse la molestia de establecer y luego liberar una conexión. Una dirección IP sirve para dirigir el datagrama hacia una máquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso específico localizado en la cabecera IP. La cabecera UDP también contiene un número de puerto de origen que permite al proceso recibido conocer como responder al datagrama. A continuación se analizará la cabecera UDP.

LA CABECERA DEL SEGMENTO UDP

Un segmento UDP consiste de una cabecera de 8 bytes seguida de los datos. En la figura 2.7 se ilustra la cabecera UDP. Los dos puertos sirven para lo mismo que en el TCP: para identificar los puntos terminales

de las máquinas de origen y destino. El campo de longitud UDP incluye la cabecera de 8 bytes y los datos. La suma de comprobación UDP incluye la misma pseudocabecera de formato mostrada en la figura 2.6, la cabecera UDP y los datos UDP, rellenados a una cantidad par de bytes de ser necesario. Esta suma es opcional y se almacena como 0 si no se calcula, e inutilizarla resulta absurdo, a menos que la calidad de los datos no importe.

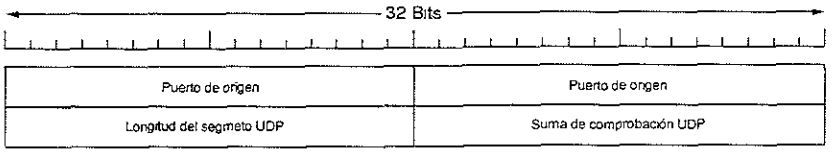

FIG. 2.7 La cabecera UDP.

2.2.5 LA CAPA DE APLICACIÓN.

Finalmente llegamos a la capa de aplicación. La capa de aplicación es el nivel más alto de la arquitectura TCP/IP. Esta capa provee un conjunto de interfaces para que las aplicaciones puedan acceder a los servicios de red así como los servicios necesarios para soportar las aplicaciones. Estos servicios pueden ser transferencia de archivos, accesos a las bases de datos, manejo de mensajes, etc.

En la tabla 2.3 se muestran algunas de las principales aplicaciones que se tienen en la capa de aplicación del conjunto de protocolos TCP/IP.

Tabla 2.3 Aplicaciones de la capa de transporte.

Arquitectura TCP/IP	**Acrónimo**	**Función**
Transferencia de archivos	FTP	Proceso que sirve para enviar o recibir archivos del proceso FTP del servidor al proceso TFP del cliente.
Protocolo sencillo de transferencia de correo	SMTP	Proceso que permite que un usuario pueda componer memorandos y los envíe a individuos o grupos.
Telnet	Telnet	Proceso que permite establecer una conexión a una máquina remota y se establezca una sesión interactiva.
Sistema de Nombres de Dominio	DNS	Proceso que permite obtener la dirección IP a partir del nombre de domnio.
Administración Sencilla de Redes	SNMP	Permite obtener estadísticos de los dispositivos de la red.

3. REDES IP

3 REDES IP

3. LA RED IP.

Uno de los principales requisitos en telecomunicaciones de empresas y particulares es una conexión de alta velocidad. En anteriores décadas, las redes de datos de alta velocidad se expandieron y empezaron a ofrecer su conexión a alta velocidad en los niveles altos de la red (entre conmutadores) y en pequeñas redes de área local (LANs). El protocolo IP (Internet Protocol, Protocolo de Internet) es utilizado hoy en la mayoría de estas redes. El principal beneficio del IP es que convierte a redes físicamente distintas en una red aparentemente homogénea [27]. A esto se le llama internetworking (interconexión de redes), y la resultante "meta-red"[1] se denomina *internet*[1]. Aunque existen otros protocolos disponibles, como ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono), estos no han alcanzado el nivel de madurez necesario.

En la actualidad, la mayor parte de la telefonía se efectúa en la PSTN[2]. Esto significa que una llamada reserva una conexión entre dos usuarios y nadie más puede hacer uso de ésta: cuando la llamada finaliza, la línea se libera para que pueda ser utilizada por otros usuarios.

La transmisión de voz paquetizada mediante el protocolo IP logra un mejor aprovechamiento del ancho de banda disponible que la telefonía tradicional por conmutación de circuitos; esta tecnología, denominada VoIP o Telefonía IP, hace posible el envío de paquetes entre dos o más suscriptores sin reservar la conexión y solo utiliza ancho de banda si tiene datos para transmitir. Esto se logra a través de la digitalización de las señales de audio encapsuladas en paquetes mediante el Protocolo de Transporte de Tiempo Real (RTP, Real-Time transport Protocol) y enviándolas en redes que emplean el protocolo IP, que al llegar a su destino se desencapsulan y reproducen [5].

En este capítulo se estudiarán a detalle las características de las redes IP, ya que es necesario su buen entendimiento para más adelante poder estudiar la tecnología VoIP.

3.1 INFRAESTRUCTURA DE LA RED

Construir la infraestructura de una red es una tarea compleja, requiere mucho trabajo de búsqueda de información, planeación, diseño y modelado.

La implementación de IP sobre diferentes protocolos depende del mecanismo usado para convertir las direcciones IP con las direcciones de hardware (direcciones MAC) en la capa de enlace de datos del modelo OSI. Es importante considerar los siguientes aspectos cuando se implementa IP sobre algún protocolo de enlace de datos:

[1] *Observe aquí la sutil diferencia entre una internet y La Internet. El último es el nombre oficial de una internet global particular*
[2] *PSTN (Public Switched Telephone Network - red telefónica pública conmutada)*

- *Conversión de direcciones*

Diferentes protocolos de la capa de enlace de datos tienen diferentes formas de convertir las direcciones IP en direcciones de hardware. En la suite TCP/IP, el protocolo utilizado para este propósito es el Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol).

- *Encapsulado y encabezados*

El encapsulamiento de los paquetes IP en la capa de enlace de datos y los encabezados que se generan deben ser evaluados.

- *Enrutamiento*

El enrutamiento es el proceso mediante el cual tratamos de encontrar un camino entre dos puntos de la red: el nodo origen y el nodo destino. Es un componente muy importante en las redes IP.

- *Unidad de transmisión máxima (Maximum Transmisión Unit, MTU)*

La unidad de transmisión máxima es el tamaño máximo de la trama de datos (en bytes) que tiene que ser transmitido al destino a través de la red.

3.1.1 TECNOLOGIA

Es importante entender el funcionamiento de cómo son transmitidos los datos en una red IP. En esta sección se estudiarán los fundamentos de las tecnologías de redes de área local (LAN) y redes de área amplia (WAN, Wide Area Network) más importantes.

3.1.1.1 TECNOLOGIAS DE REDES DE AREA LOCAL (LAN).

Cada estación de trabajo se conecta a la red por medio de una tarjeta de red (NIC, Network Interface Card, Tarjeta de Interfaz de Red). Cada tarjeta de red tiene una dirección de hardware que es única en todo el mundo. En la capa física cada estación de trabajo se comunica con otras estaciones de trabajo por medio de esa dirección de hardware. El protocolo IP al ser un protocolo de un nivel superior en el modelo OSI, se comunica utilizando una dirección lógica que en el caso de las redes IP es la dirección IP. Existen varias tecnologías LAN que son implementadas ampliamente hoy en día. A continuación se analizarán las tecnologías de área local Ethernet, Token Ring y FDDI (Fiber Distributed Data Interface, Interfaz de datos distribuidos por fibra).

- **ETHERNET/IEEE 802.3**[3]

Es la tecnología de red de área local más extendida en la actualidad Fue diseñada originalmente por Digital, Intel y Xerox. Posteriormente en 1983, fue formalizada por el IEEE como el estándar Ethernet 802.3. La velocidad de transmisión de datos en Ethernet es de 10Mbits/s en las configuraciones habituales, pudiendo

[3] *Aunque las especificaciones para Ethernet IEEE 802.3, Ethernet Rapido y Gigabit Ethernet son diferentes, todas serán consideradas como Redes de Area Local Ethernet*

llegar a ser de 100Mbits/s en las especificaciones Fast Ethernet. Al principio, sólo se usaba cable coaxial con una topología en BUS, sin embargo esto ha cambiado y ahora se utilizan nuevas tecnologías como el cable de par trenzado (10 Base-T), fibra óptica (10 Base-FL) y las conexiones a 100 Mbits/s (100 Base-X o Fast Ethernet).

Ethernet/IEEE 802.3, está diseñada de tal forma que no puede transmitir más de un usuario a la vez. El acceso al medio compartido es controlado utilizando el protocolo *CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones)*, cuyo principio de funcionamiento consiste en que una estación, para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza a transmitir. Si dos estaciones empiezan a transmitir al mismo tiempo, se produce una colisión, como se muestra en la figura 3.1, y ambas deben repetir la transmisión, para lo cual esperan un tiempo aleatorio antes de repetir, evitando de este modo una nueva colisión, ya que ambas escogerán un tiempo de espera distinto. Este proceso se repite hasta que se reciba confirmación de que la información ha llegado a su destino. Ethernet es una buena tecnología para una red de bajo tráfico o para aplicaciones que no demandan un gran ancho de banda.

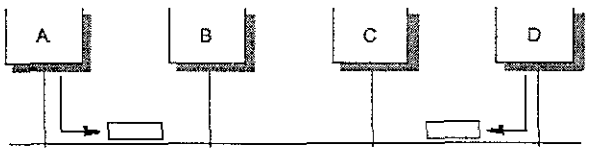

FIG 3.1 Colisión en una red Ethernet.

- **TOKEN RING/IEEE802.5**

La red Token-Ring es una implementación del estándar IEEE 802.5, en el cual se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras. El primer diseño de una red de Token-Ring es atribuido a E.E Newhall en 1969. IBM publicó por primera vez su topología de Token-Ring en marzo de 1982, cuando esta compañía presentó los papeles para el proyecto 802 del IEEE. IBM anunció el producto Token-Ring en 1984, y en 1985 éste llegó a ser un estándar de ANSI (*American National Standards Institute,* Instituto nacional estadounidense de estándares).

A diferencia de la tecnología Ethernet, el método de acceso a la red es conocido como Paso de Testigo (Token Passing) en donde, un Token (Ficha Virtual) es pasado de computadora a computadora, como se muestra en la figura 3.2. Cuando una computadora desea mandar información debe esperar a que le llegue el Token vacío, cuando le llega utiliza el Token para mandar la información a otra computadora, entonces cuando la otra computadora recibe la información regresa el Token a la computadora que envió, con el mensaje de que fue recibida la información. Así se libera el Token para volver a ser usado por cualquier otra computadora. Aquí debido a que una computadora requiere el Token para enviar información no hay colisiones, el problema reside en el tiempo que debe esperar una computadora para obtener el Token vacío. En una red Token-Ring los datos se transmiten a una velocidad de 4 ó 16Mbps. Todas las estaciones deben estar configuradas a la misma velocidad para que funcione apropiadamente la red. Cada computadora se

conecta a través de cable par trenzado ya sea blindado ó a un concentrador llamado MAU(Media Access Unit), y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por el cual da vueltas el Token. En realidad es el MAU que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.

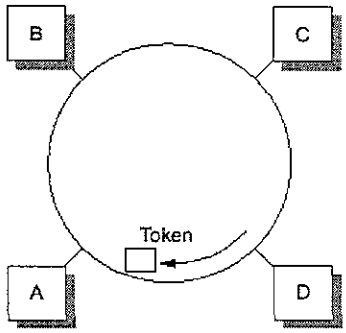

FIG 3.2 Token Passing en una red de área local Token-Ring.

En redes pequeñas a medianas con tráfico de datos pesado es más eficiente utilizar la tecnología Token Ring en lugar que Ethernet. Sin embargo, el enrutamiento directo de datos en Ethernet tiende a ser un poco mejor en redes que incluyen un gran número de computadoras con tráfico bajo o moderado.

- **FDDI (Fiber Distributed Data Interface, Interfaz de datos Distribuidos por fibra)**

Es una tecnología más de MAN que de LAN, utiliza topología lógica de anillo, el método de acceso es el llamado Paso de Token (Token Passing), el mismo utilizado en redes Token-Ring, pero permite transmisión de datos a 100 Mps y su medio de transmisión es la fibra óptica, por lo que permite mayores distancias de operación. El cableado de una red FDDI consiste de dos anillos de fibra. Si uno de ellos se rompe, el otro puede seguir operando y si los dos lo hacen, se pueden unir para formar un anillo del doble de tamaño. No está estandarizado por la IEEE sino por el Instituto Nacional de Estándares Americanos (ANSI) como X3T9.5 Esta red puede usarse de la misma manera que cualquiera de las LAN 802 pero, con su gran ancho de banda, otro uso común es como dorsal para conectar varias LAN de cobre.

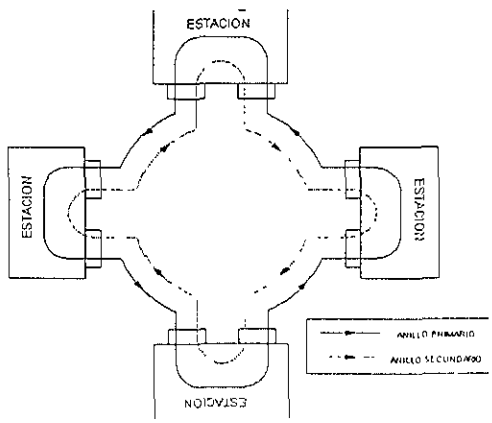

FIG 3.3 Anillo dual FDDI

La tabla 3.1 resume las características principales de las tecnologías estudiadas en este apartado [2][3].

TABLA 3.1 Características de las principales redes de área local.

	Ethernet	Token-Ring	FDDI
Topología	Bus[4]	Anillo	Anillo dual
Método de acceso	CSMA/CD	Paso de token	Paso de token
Velocidad(en Mbps)	10/100/1000	1/4/16/100	100
Difusión / Punto-punto	Difusión	Difusión	Difusión
Tamaño de la trama de información (bytes)	64-1516	32-16K	32-4400
Auto recuperación	No	Sí	Sí
Canal redundante	No	No	Sí
Admisión de clases prioritarias	No	Sí	Sí
Costo de la implementación (respecto a las otras)	Barato	Moderado	Caro
Ambiente de típico de implementación	Pequeñas oficinas, Institutos, Oficinas corporativas, comercio electrónico	Aerolíneas, bancos, sistemas de manufactura, redes con aplicaciones críticas.	Como dorsal para redes medianas y grandes.

3.1.1.2 TECNOLOGIAS DE REDES DE AREA AMPLIA (WAN)

Las tecnologías WAN son usadas principalmente para conectar redes que están separadas geográficamente. Usualmente se usan enrutadores en las conexiones WAN aunque también pueden usarse conmutadores.

Los requerimientos y la selección de tecnologías WAN son diferentes a las usadas en las LANs. La principal razón es que las tecnologías WAN son servicios que ofrecen las telefónicas, y resultan ser muy costosos. Las velocidades de transmisión entre las WAN y las LAN también son diferentes, mientras que en una red LAN se trabaja a velocidades de megabits por segundo en las redes WAN usualmente las velocidades de transmisión son del orden de kilobits por segundo. Estas y otras diferencias entre estos dos tipos de redes se presentan en la tabla 3.2 [2][3].

TABLA 3.2 Diferencias entre las redes LAN y WAN.

	LAN	WAN
Servicio por suscripción	No	Sí
Velocidades de transmisión	4,10,16,100,155,622 Mbps. 1 Gbps.	9.6, 14.4, 28.8, 56, 64, 128,256,512 Kbps 1.5,2,45,155,622 Mbps
Costo por Kbps (relativo con respecto al otro)	Barato	Muy caro
Costo por redundancia	Puede ser caro	Muy caro
Requerimiento de personal especializado	No es necesario	Sí

[4] (esto es cable lineal)

A continuación se estudiarán las principales tecnologías de área amplia.

- **LINEAS ARRENDADAS.**

Es la forma más común de conectar oficinas remotas con alguna oficina central. Básicamente una línea arrendada es un circuito permanente, entre las entidades que se desean comunicar. Las velocidades de conexión van desde los 64Kbps hasta los 45Mbps. Debido al costo y a la introducción de otras tecnologías WAN, los administradores de redes comenzaron a reemplazar las líneas dedicadas por otras tecnologías [2].

- **REDES X.25.**

Es un estándar internacional, desarrollado en los años setenta por el CCITT[5], y aceptado para conectar terminales y computadoras centrales a redes de conmutación de paquetes. Muchas redes públicas antiguas, en especial fuera de Estados Unidos siguen el estándar X.25.

Conmutación de paquetes es una tecnología de redes en la cual la información de muchos usuarios es combinada y enviada en un canal de transmisión en forma de unidades discretas llamadas paquetes; cada paquete lleva información del usuario aparte de la de enrutamiento lo cual asegura transmisiones confiables y exactas [6]. Existen dos tipos de redes de conmutación de paquetes:

- Redes Públicas (Telepac, Tymnet, Tlenet, etc)
- Redes Privadas.

El estándar X.25 describe la interfaz entre el equipo terminal de datos *(DTE, Data Terminal Equipment)* y el equipo terminal de comunicaciones de datos *(DCE, Data Communications Equipment)* para terminales operando en modo de paquete en una red de datos (pública o privada). En la figura 3.4 se ilustra la red X.25 con los diferentes elementos que la conforman. El estándar X.25 define el procedimiento para el intercambio de datos entre un dispositivo de usuario (DTE) y un nodo de red (DCE) estableciendo una sesión e intercambio de datos. El procedimiento incluye identificación de paquetes, direccionamiento (fuente y destino), número de canal lógico para reconocimiento o rechazo de paquetes, control de error y control de flujo.

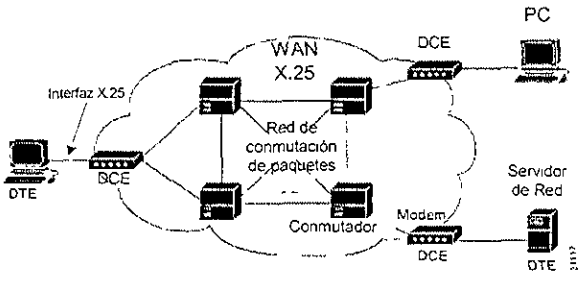

FIG 3.4 La red X.25

[5] CCITT (Comite Consultatif International Telegraphique et Telephonique, Comite consultivo internacional telefonico y telegrafico)

X.25 proporciona un número de secuencia de los paquetes para permitir al DTE y al DCE mantener los paquetes en un orden adecuado y para proporcionar una manera para el reconocimiento de ellos y de su recepción exitosa. La recomendación X.25 no se involucra en absoluto en los protocolos internos y algoritmos necesarios para operar en sí la red de conmutación de paquetes. En el sentido estricto el modelo OSI X.25 no es un protocolo de comunicación de datos, sino una especificación para una interfaz de red que utiliza protocolos individuales en cada uno de sus tres niveles [6]. En la figura 3.5 se ilustran los tres niveles del modelo OSI X.25.

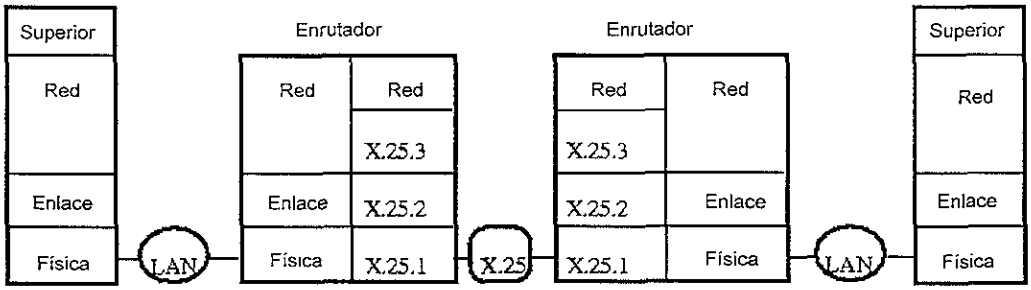

FIG 3.5 Relación del modelo X.25 como parte del modelo OSI.

El nivel físico y de enlace se encargan de mover los paquetes de datos, mientras que el nivel de red se encarga de la asignación de direcciones, empaquetamiento/desempaquetamiento, control de flujo, control de error y multicanalización de datos.

Básicamente este protocolo permite al usuario establecer circuitos virtuales[6] y después enviar paquetes de hasta 128 bytes a través de ellos. Estos paquetes se entregan en forma confiable y ordenada. X.25 esta orientado a la conexión y trabaja con circuitos virtuales tanto conmutados como permanentes[7]. La mayor parte de las redes X.25 trabajan a velocidades de hasta 64 Kbps, lo cual las hace obsoletas para muchos propósitos.

- **FRAME RELAY.**

Se ha definido como una conmutación de paquetes de alta velocidad y se perfiló fuertemente como una solución para la interconectividad de redes locales de datos en los noventa

Frame Relay define la interfaz DTE-DCE (con características de alta velocidad) para conexión a una red pública conmutada. Frame Relay combina la multiplexación estadística[8] y la administración de los puertos

---

[6] *Un circuito virtual, es un enlace de comunicación que aparece como un circuito dedicado punto a punto También se puede decir que es un sistema que entrega paquetes de datos en una secuencia de orden garantizada, tales que ellos pueden arribar por medio de un circuito punto a punto real*

[7] *Un circuito virtual permanente, es un arreglo permanente de circuito virtual entre usuarios en una red de conmutación de paquetes, es análogo a la línea dedicada ó permanente en una red telefónica*

[8] *La multiplexación estadística es una mejora de la multiplexación en tiempo (TDM, Time División Multiplexing) basada en un manejo adecuado del ancho de banda para lo cual se hace uso de herramientas de probabilidad.*

de la conmutación de paquetes X.25 con la alta velocidad y bajo retado de la conmutación de circuitos TDM. De una manera contraria a X.25, Frame Relay elimina por completo el procesamiento del nivel 3, nivel de red, y solo usa parte de las funciones del nivel 2, nivel de enlace, las cuales incluyen la verificación de error. Todas las demás funciones, tales como supervisión, reconocimientos (ACK), números de secuencia, rotación de ventana, son eliminados en esta tecnología, ganando con todo ello incrementar el caudal eficaz [9] de la red ya que las tramas no requieren mucho procesamiento.

Una de las características de Frame Relay es que la estructura de la trama es de longitud variable quedando con un intervalo dinámico que va desde muy pocos hasta miles de caracteres. Resulta conveniente enfatizar que Frame Relay opera excelentemente con redes locales de datos, las cuales requieren tramas de tamaño variable, esto significa que se tendrán retardos variables (siempre menores a los de X.25). Es por eso que Frame Relay no es apropiada para llevar información sensible al tiempo como voz o vídeo.

En resumen, el crecimiento de las aplicaciones de las computadoras requieren de comunicaciones rápidas, la proliferación de computadoras personales (PC, Personal Computer) y estaciones de trabajo, así como la mayor disponibilidad del uso de líneas libres de error, se han combinado para crear una nueva forma de red de conmutación de paquetes de cobertura amplia, lo anterior dio origen a Frame Relay. Esta tecnología presenta las siguientes características: alta velocidad, bajo retardo, comparición de puertos y compartición del ancho de banda, las cuales juntas son la solución ideal para el tráfico tipo ráfaga.

Se puede pensar en Frame Relay como una línea virtual rentada. El cliente renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas de hasta 1600 bytes entre ellos. La diferencia entre una línea rentada real y una virtual es que, con una real, el usuario puede enviar tráfico durante todo el día a máxima velocidad. Con una línea virtual se pueden enviar ráfagas de datos a toda velocidad, pero el uso promedio largo plazo deberá ser inferior a un nivel predeterminado. Además de competir con las líneas arrendadas, Frame Relay también compite con los circuitos virtuales permanentes de X.25, excepto que opera a altas velocidades, usualmente a 1.5 Mbps.

Frame Relay, proporciona un servicio mínimo que básicamente es una forma de determinar el inicio y el fin de cada marco y de detectar errores de transmisión. Si se recibe una trama Frame Relay simplemente lo descarta. Corresponde al usuario descubrir que se perdió un bloque y emprender la acción necesaria para recuperarlo. A diferencia de X.25, Frame Relay no proporciona acuses de recibo ni control de flujo normal. Sin embargo, tiene un bit en el encabezado que un extremo de la conexión puede habilitar para indicar al otro extremo que hay problemas. El uso de este bit es opción de los usuarios.

- **RED DIGITAL DE SERVICIOS INTEGRADOS (ISND).**

La Red Digital de Servicios Integrados (ISDN, Integrated Services Digital Network) es una red que ha evolucionado, en general, a partir de la Red Digital Integrada (RDI) para telefonía y que proporciona una conectividad digital de extremo a extremo para apoyar una amplia gama de servicios. El concepto de

[9] *El Caudal eficaz (Throughut) es un indicador de la capacidad de manejo de datos. Mide que tantos datos son procesados como salida de una computadora, dispositivo, enlace, red o sistema.*

"extremo a extremo" significa que ISDN es una tecnología diseñada para digitalizar hasta el último metro, es decir, llevar la red digital hasta el abonado, fábrica u oficina. La ISDN permite la integración de servicios de voz, datos, imagen, vídeo y texto en una sola red pública digital interconectada con la red telefónica actual, permitiendo alta velocidad de transmisión y garantizando una transferencia digital de la información, reduciendo así los errores casi a cero. La transmisión de información a través de la ISDN no es solo más rápida, sino también más segura y confiable.

El desarrollo y estandarización de la ISDN incluye el desarrollo de los protocolos, convenciones o reglas que permiten la comunicación entre los diferentes usuarios de ISDN y la red, y la interacción entre dichos usuarios.

- **ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono).**

En 1987, la ITU-T (International Telecommunications Union – Telecommunications, Unión Internacional de Telecomunicaciones - Telecomunicaciones) seleccionó a ATM como la respuesta adecuada para integrar las ventajas de la conmutación de paquetes y de la conmutación de circuitos. En 1990, la ITU-T añadía un conjunto de 13 recomendaciones a la serie I (ISDN) para especificar los aspectos más importantes de ATM.

Básicamente, es la tecnología que presenta las siguientes características: capacidad de integración de diversos tipos de tráfico, administración del ancho de banda asignado a cada una de las señales que circulan por la red, sean éstas voz, datos o imágenes, de manera que el usuario final la reciba en forma integrada y finalmente la capacidad de optimizar la relación entre la suma de las velocidades de pico de las fuentes y la velocidad del enlace. Por estas razones, la tecnología ATM, que fue propuesta originalmente por la Industria de las Telecomunicaciones, es recomendada en la actualidad como solución universal para redes de banda ancha por los más importantes organismos de las industrias de las Comunicaciones y Computadoras, como la mencionada ITU-T, el Foro ATM o el IETF (Internet Engineering Task Force, Fuerza de trabajo de Ingeniería en Internet) [27].

Los conceptos ATM son, en esencia muy simples:

- Operación por conmutación de paquetes. Los paquetes son de longitud fija (48 octetos de información y 5 octetos de control), denominados celdas. Esta opción de celdas de tamaño fijo permite el uso de nodos de conmutación a velocidades muy altas.
- Orientado a conexión[10] en el nivel más bajo. La información se transfiere por canales virtuales asignados durante la duración de la conexión.
- La asignación del ancho de banda se realiza en función de la demanda de envío de tráfico.
- No se realiza control de errores en el campo de datos, y el control de flujo se realiza fundamentalmente por los ETD[11] de usuario. Con ello maximizar la eficiencia.

[10] *Al ser ATM una técnica orientada a conexion, tiene que establecer una conexión virtual entre usuarios finales antes de que se comience a transmitir la información*
[11] *ETD, equipos terminales de datos.*

- Proporciona transparencia temporal, es decir, pequeñas variaciones de retardo entre las señales de la fuente y el destino.
- Las celdas se transmiten a intervalos regulares; si no hay información se transmiten celdas no asignadas.
- Se garantiza que las celdas lleguen a su destino en el mismo orden en el que fueron transmitidas.

La tecnología ATM comprende un tendido físico (cable de cobre, cable coaxial, enlace de microondas, enlace satelital o cable de fibra óptica), elementos de conmutación, concentradores de acceso (HUB), dispositivos de adaptación (Enrutadores, Codecs, etc.), y dispositivos de interfaz (tarjetas de comunicación, cámaras de vídeo, centrales telefónicas, etc.). ATM es una tecnología de conmutación y transmisión a muy alta velocidad que permite enviar voz, vídeo y datos sobre la misma red, a velocidades que varían de 25 Mbps (millones de bits por segundo) a 1 Gbps (mil millones de bits por segundo) lo cual permite reducir los costos de operación de las redes y ofrecer grandes anchos de banda a precios económicos.

Mediante el ATM se pueden consolidar varias redes diferentes al simplificar el manejo y mantenimiento de las mismas, al igual que reduce la necesidad de usar múltiples enlaces.

3.1.1.2 EQUIPO DE CONECTIVIDAD

Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor. Los elementos de interconectividad más importantes para redes LAN son: repetidores, puentes, enrutadores, gateways (pasarelas). Cada uno representa un nivel diferente de conectividad y funcionalidad tal como se define por el modelo OSI.

REPETIDORES

La forma más simple de un producto de interconectividad de LANs es el repetidor. Opera en el nivel más bajo, el nivel físico del modelo OSI, los repetidores extienden físicamente el alcance de LANs idénticas, al regenerar las señales desde un cable y transmitiéndolas hacia otro. Siendo conectores de la capa física, los repetidores no realizan ningún tipo del procesamiento de alto nivel requerido en redes más complejas, y como resultado de esto, tienen el más alto caudal eficaz, pues pasan directamente los datos de una LAN a la otra con muy poco retardo por procesamiento. Como dispositivo de interconectividad, los repetidores están limitados a distancias cortas (menos de dos kilómetros). Por esta razón no se pueden considerar como conectores remotos de LANs.

PUENTES

En el siguiente nivel de complejidad, están los puentes. Los puentes conectan LANs al nivel de la capa de enlace de datos y más específicamente en el subnivel de control de acceso al medio (MAC). Como tales los puentes "leen" las direcciones de origen y destino del paquete de datos y, si la dirección indica un nodo en una LAN remota, le envía paquetes a esa LAN (eso se llama direccionamiento). Si la dirección reside en la LAN conectada localmente, el puente descarta (o filtra) ese paquete. En efecto, los puentes crean redes lógicamente unificadas a partir de grupos de subredes dispares. Los puentes y los otros tipos de soluciones de interconectividad de alto nivel sirven para crear inter-redes de cobertura amplia capaces de expandirse miles de kilómetros.

Puesto que los puentes funcionan por debajo de la capa de red del modelo OSI, éstos son independientes del protocolo, permitiéndoles a los usuarios la interconexión de LANs con diferentes protocolos tales como TCP/IP, Novel Netware, SNA, etc.

ENRUTADORES

Enlazando LANs en la capa de red del modelo OSI, los enrutadores ofrecen el siguiente nivel de conectividad con un enrutamiento selectivo de paquetes individuales de datos a través de múltiples trayectorias de comunicación. Los enrutadores pueden enviar paquetes a través de diferentes trayectorias en la red dependiendo de prioridades del usuario. Con su habilidad de ir más profundamente dentro de los formatos de los paquetes, los enrutadores pueden proveer segmentación. Sin embargo el procesamiento extra (overhead) requerido para manipular los paquetes afecta negativamente su caudal eficaz. En la mayoría de los casos los enrutadores introducen retardos mayores al enviar paquetes de un nodo a otro, resultando en tiempos de respuesta más lentos. Como conectores de la capa de red, trabajan con protocolos específicos. Algunos enrutadores pueden conectar solamente LANs con protocolos de alto nivel idénticos, mientras que otros más sofisticados pueden interconectar varios protocolos. Los enrutadores son una pieza muy importante en los equipos que conforman una red IP ya que es el dispositivo de la conexión de los diferentes grupos de redes llamados subredes IP

GATEWAYS (PASARELAS).

Como se analizó anteriormente, los puentes y enrutadores son utilizados para resolver los problemas de interconexión, de subredes en un ambiente donde todos los dispositivos manejan protocolos compatibles con el modelo OSI. Se dan muchas situaciones en las que existen subredes de arquitectura propietaria, tales como la SNA (System Network Architecture) de la IBM , que requieren interconectarse con subredes del tipo OSI. Para interconectar subredes totalmente diferentes (OSI/SNA) se utiliza el gateway, el cual realiza la conversión de protocolos para todas las siete capas de la OSI, más todas las capas de la arquitectura propietaria. Por lo que la pasarela es por lo tanto un dispositivo que realiza una translación completa de protocolos y retransmisión de paquetes entre sistemas diferentes.

De acuerdo a lo anterior, mediante la pasarela es posible conectar cualquier tipo de red entre sí, proporcionando una completa funcionalidad, desde el manejo de bits en el nivel físico pasando por la formación de las tramas de un paquete, detección de error, enrutamiento, control de flujo, etc.

3.2 ADMINISTRACIÓN DE LAS DIRECCIONES, LOS NOMBRES Y LA RED.

Una red IP tiene dos muy importantes recursos, sus direcciones IP y la estructura de nombres correspondientes dentro de la red. Para poder ofrecer una comunicación efectiva entre las estaciones y los servidores en una red, cada estación debe mantener una identidad única. En una red IP esto se logra utilizando las direcciones IP. La distribución y administración de estas direcciones es una consideración muy importante en el diseño de una red IP.

Para los usuarios resulta difícil recordar las direcciones IP debido a su estructura, por lo que es más fácil recordar nombres y tener esos nombres relacionados a máquinas individuales conectadas a una red. Estos nombres deben ser traducidos a direcciones IP ya que las redes no utilizan identificadores basados en cadenas ASCII. La administración de estos nombres y los mecanismos de traducción utilizados serán estudiados en esta sección.

Después de que la red ha sido diseñada e implementada esta debe ser administrada, deben monitorearse parámetros como el control de flujo, cuellos de botella, seguridad, etc. Existen diferentes sistemas que pueden ser incorporados en las redes IP desde un inicio para ayudar a una adecuada administración de la red, los cuales serán estudiados en este apartado.

3.2.1 ADMINISTRACIÓN DE LAS DIRECCIONES

Como se mencionó con anterioridad la distribución y administración de las direcciones de la capa de red es una tarea muy importante. Las direcciones de las redes y las subredes deben estar muy bien planeadas, administradas y documentadas, ya que éstas direcciones no pueden ser asignadas dinámicamente. Los números de red los asigna el NIC (Network Information Center, centro de información de redes) para evitar conflictos. Las direcciones de red, que son números de 32 bits, generalmente se escriben en notación decimal con puntos. En este formato, cada uno de los 4 bytes se escribe en decimal, de 0 a 255.

Al contrario de lo que ocurre con la red misma, los dispositivos conectados a la red generalmente pueden ser configurados para tener direcciones asignadas en forma dinámica.

3.2.1.1 DIRECCIONAMIENTO IP.

Cada interfaz de red de cada nodo (servidor o enrutador) en una red IP se identifica mediante una dirección única, la dirección IP. Las direcciones IP tienen una estructura jerárquica [28]. Una parte de la dirección corresponde a la red, y la otra al nodo dentro de la red. Cuando un enrutador recibe un datagrama por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente sólo contienen direcciones de red, no de nodo) y envía el datagrama por la interfaz correspondiente. La combinación es única: no hay dos máquinas que tengan la misma dirección IP. Todas las direcciones IP son de 32 bits de longitud y se usan en los campos de dirección de origen y dirección de destino de los paquetes IP. Para dar flexibilidad a la asignación hay cinco tipos básicos de direcciones en función de la longitud de los campos, las cuales serán explicadas a continuación. Los diferentes formatos usados para las direcciones IP se muestran en la figura 3.6 [1]. Aquellas máquinas conectadas a varias redes tienen direcciones IP diferentes en cada red.

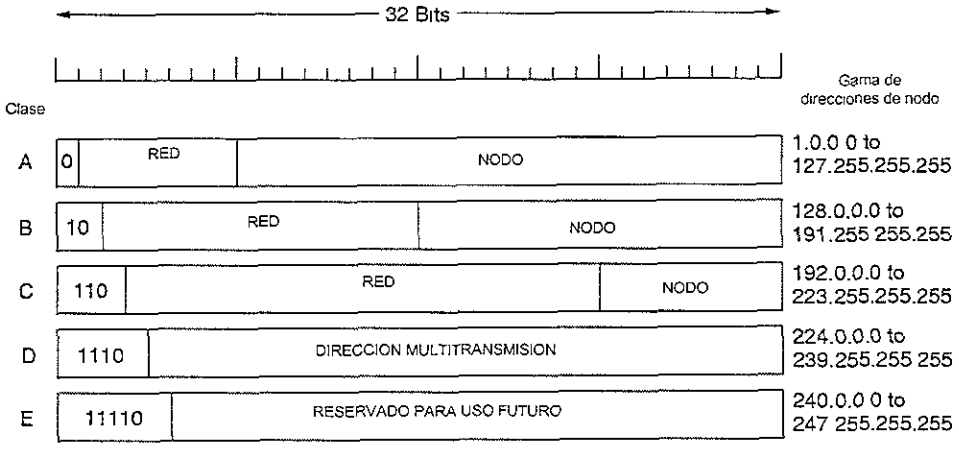

FIG 3.6. Formatos de dirección IP

- **DIRECCIONES CLASE "A".**

El primer bit, el más significativo, tiene el valor *0* indicando dirección de tipo A. Los siguientes siete bits son usados para el número de red, teniendo una posibilidad de 128 redes (2^7). Los 24 bits restantes son utilizados para indicar el número de nodo. Esta clase de direcciones permite tener muchos sistemas conectados en una única subred siendo idónea para grandes redes con muchos equipos.

- **DIRECCIONES CLASE "B".**

Los primeros dos bits de la dirección están definidos como *10*. Los siguientes 14 bits son utilizados para la dirección de la red y lo siguientes 14 bits son dedicados para los números de nodo. Este tipo de direcciones son más usadas para redes de tamaño mediano.

- **DIRECCIONES CLASE "C".**

Los primeros tres bits son *110*. Esta clase de direcciones está pensada para subredes pequeñas con pocos equipos.(Hasta 255 direcciones diferentes para una subred). Los siguientes 21 bits son utilizados para indicar el número de red.

- **DIRECCIONES CLASE "D".**

Las direcciones multidifusión o de clase D tienen definidos los primeros cuatro bits como *1110*. Esta clase está pensada para direcciones de **multidifusión o multidestino.** Con una dirección de este tipo se envía un mismo datagrama[12] a un grupo de equipos previamente definidos, evitando así, el tener que generar un datagrama para cada destinatario con cada dirección unicast o individual si el contenido del datagrama es el mismo para todos.

- **DIRECCIONES CLASE "E".**

Los primeros cinco bits están definidos como *11110*. La clase E está reservada para posibles usos futuros.

- **DIRECCIONES IP ESPECIALES**

Existen ciertas clases de direcciones que no pueden ser utilizadas para identificar a una subred o a un sistema, el formato de estas se muestra en la figura 3.7.

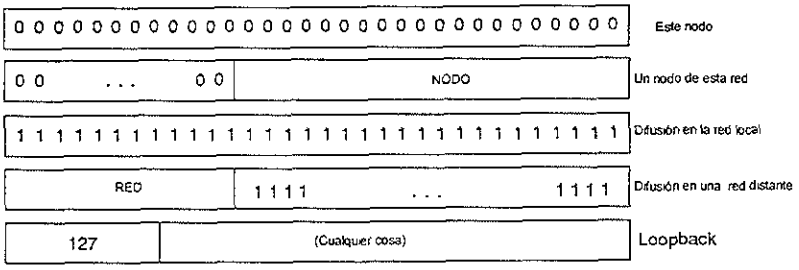

FIG 3.7 Direcciones IP especiales

La dirección IP *0.0.0.0* es usada por los nodos cuando están arrancando, pero no se usan después. Las direcciones de IP con *0* como número de red se refieren a la red actual. Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tienen que saber su clase para saber cuantos ceros hay que incluir) La dirección que consiste solamente en unos permite la difusión en la red local, por lo común una LAN. Las direcciones con un número de red propio y solamente unos en el campo de nodo permiten que las máquinas envíen paquetes de difusión a LANs distantes desde cualquier parte de la Internet. Por último, todas las dirección de la forma 127.xx.yy.zz se reservan para pruebas de realimentación (loopback). Los paquetes enviados a esa dirección no se colocan en el medio de transmisión; se procesan

[12] *Los paquetes de tipo no orientado a conexion se llaman datagramas*

localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número [1].

3.2.1.1.1 SUBREDES (SUBNETTING)

En 1985 el RFC 950 definió el estándar que soporta el *subnetting* ó división de redes clase A, B o C en redes más pequeñas. El subnetting fue implementado para solucionar algunos de los problemas que algunas partes de Internet comenzaban a presentar con la jerarquía de direccionamiento de dos niveles.

- Las tablas de enrutamiento de Internet comenzaron a crecer.
- Los administradores locales tenían que solicitar otro número de red para Internet antes de que una red local pudiera ser instalada.

Ambos problemas fueron solucionados agregando otro nivel a la jerarquía de la estructura de las direcciones IP. En lugar de una clasificación jerárquica de dos niveles, el subnetting soporta una jerarquía de tres niveles. La figura 3.8 ilustra la idea básica del subnetting que es, dividir el campo número de host en dos partes, el número de subred y número de nodo en la subred.

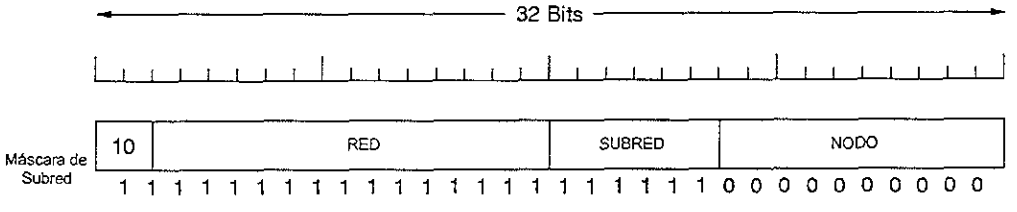

FIG 3.8 Una de las formas de generar una subred clase B.

Fuera de la red, la subred no es visible, por lo que la asignación de una subred nueva no requiere comunicación con el NIC ni la modificación de bases de datos externas. Cuantos bits se deberán asignar para la subred y cuantos para el nodo es decisión del administrador.

El número de bits que pueden ser utilizados para indicar la subred puede variar. Para especificar cuantos bits son usados y en que parte del campo *número de nodo* están localizados, se definió la máscara de subred. La máscara de subred usa el mismo formato y técnica de representación que presentan las direcciones IP. La máscara de subred tiene "1s" en todos los bits excepto aquellos que especifican el campo nodo. Por ejemplo la máscara de subred que define ocho bits para la subred en una red clase A con dirección 34.0.0.0 es 255.255.0.0. La máscara de subred que especifica 16 bits para una red clase A con la misma dirección que la del ejemplo es 255.255.255.0. Tradicionalmente todas las subredes pertenecientes a la misma red utilizan la misma máscara.

3.2.1.2 ASIGNACION DE DIRECCIONES

Las direcciones pueden ser asignadas a los nodos de dos formas: direccionamiento estático o direccionamiento dinámico.

- **ASIGNACION ESTATICA**

Las direcciones estáticas son asignadas por el administrador de la red de acuerdo a un plan de direccionamiento . Una dirección estática no cambia hasta que el administrador manualmente la modifica.

- **ASIGNACION DINAMICA**

Las direcciones dinámicas son asignadas a los dispositivos cuanto estos se conectan a la red utilizando protocolos especial. A los dispositivos que utilizan direccionamiento dinámico se les establecen diferentes direcciones IP cada vez que estos se conectan a la red. El direccionamiento dinámico utiliza el protocolo DHCP (Dynamic Host Configuration Protocol), el cual será estudiado más adelante.

3.2.1.3 PROTOCOLOS INVOLUCRADOS EN EL DIRECCIONAMIENTO IP

- **ARP (Address Resolution Protocol, Protocolo de resolución de direcciones)**

En redes punto a punto el nivel de red (los enrutadores) se ocupa de hacer llegar los datagramas a la red destino, de acuerdo con rutas perfectamente especificadas en las tablas. Sin embargo dentro de una red broadcast (normalmente una LAN) hace falta un mecanismo que permita descubrir a que dirección MAC corresponde la dirección IP del paquete que se quiere entregar. Esto no puede hacerse mediante una tabla estática, ya que en redes grandes sería muy difícil de mantener. Además, dicha correspondencia puede cambiar, por ejemplo si a un ordenador se le cambia la tarjeta LAN o si se cambia un servidor a otro ordenador. En estos casos cambia la dirección MAC pero se quiere mantener la dirección IP. Para permitir la configuración automática de correspondencias dirección MAC-dirección IP se creó el protocolo denominado ARP (Address Resolution Protocol).

El mecanismo ARP se utiliza en todas las redes broadcast para descubrir el destinatario de los paquetes.

- **RARP (Reverse address Resolution Protocol, Protocolo de resolución de direcciones en reversa)**

A veces se plantea el problema inverso a ARP, es decir hallar la dirección IP de una determinada dirección LAN. Por ejemplo, cuando se arranca una estación de trabajo 'diskless', es decir, que tiene su disco de arranque en otra estación, ésta desconoce todo lo relativo a su configuración de red (incluida la dirección IP) excepto la dirección MAC que está almacenada en su tarjeta de red local.

Para resolver este problema se creó el protocolo RARP, que consiste en que la estación emita una trama broadcast indicando su dirección LAN y solicitando que alguien le informe de cual es la dirección IP que le

corresponde. En este caso una máquina en la red local (el servidor RARP) atenderá la petición, consultará en sus tablas, y devolverá la dirección IP correspondiente.

- **BOOTP (Bootstrap Protocol, Protocolo alterno de arranque)**

Una desventaja de RARP es que usa dirección de destino que contiene únicamente unos (difusión limitada) para llegar al servidor RARP. Sin embargo, tales difusiones no son reenviadas por los enrutadores, por lo que se requiere un servidor RARP en cada red. Para superar este problema, se ha inventado un protocolo alterno de arranque llamado BOOTP. A diferencia del RARP, BOOTP usa mensajes UDP, los cuales se reenvían a través de los enrutadores. Este protocolo también proporciona información adicional a una estación de trabajo sin disco, incluida la dirección IP del servidor de archivos que contiene la imagen de memoria, la dirección IP del enrutador predeterminado y la máscara de subred a usar.

- **DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host)**

El IETF diseñó en 1993 el protocolo DHCP (Dynamic Host Configuration Protocol), que es muy similar al BOOTP pero permite una asignación dinámica de direcciones IP. En DHCP el cliente solicita al servidor una dirección IP en 'alquiler' para poder trabajar; el tiempo que dura el alquiler es negociado entre cliente y el servidor en el momento de establecer la conexión, y puede variar entre unos pocos minutos o duración indefinida. La mayor flexibilidad de DHCP le ha convertido en el protocolo preferido para la configuración remota de ordenadores en una red local. Con DHCP se mejora notablemente la seguridad y fiabilidad de una red; también se simplifican las labores de administración de la red.

Un inconveniente de DHCP frente a RARP o BOOTP es que, al no haber una asignación permanente de direcciones IP, si se desea rastrear un problema pasado cierto tiempo y sólo se dispone de la dirección IP resulta más difícil (a veces imposible) averiguar que ordenador o usuario ha sido el causante del problema.

3.2.2 ADMINISTRACION DE NOMBRES

Ya que las direcciones IP de los nodos conectados a Internet no son fáciles de recordar, en su lugar se emplean en paralelo a ellas los denominados Nombres de Dominio o DN (Domain Name) y la relación existente entre la dirección IP y el DN se gestiona mediante el DNS (Domain Name System, Sistema de Nombre de Domino). Los nombres de dominio son unos nombres conocidos, públicos, accesibles a través de diversos medios y fáciles de recordar asignados a los ordenadores conectados a la red Internet. (Por ejemplo: www.netscape.com) que se conectan con números exclusivos de IP (por ejemplo 123.45.123 45), que sirven como direcciones de ruta en Internet. Los servidores DNS, cada uno responsable de uno o más dominios, constituyen una red jerárquica distribuida, almacenan y traducen los nombres de Internet a los correspondientes números IP necesarios para la transmisión de información a través de la red.

El sistema de nombres de dominio está compuesto principalmente por tres elementos:

- *El espació de nombres de dominio y registro de recursos.* El espacio es una base de datos distribuida que guarda la información de la estructura jerárquica y los datos asociados con los recursos que están conectados a la red. El espacio de nombres se utiliza para resolver las direcciones IP a partir de los nombres de los ordenadores ó hosts. La estructura jerárquica del espacio es una estructura de árbol, con la raíz en la cima. El árbol del DNS tiene muchas ramas. Estas ramas se originan de un punto llamado nodo. Cada uno de estos nodos corresponde a un recurso de la red (un host o un gateway) a esta estructura se la llama el espacio de nombres de dominio. Un dominio es una parte de la estructura del espacio de nombres. El registro de recursos más común en un ordenador individual es la dirección IP.
- *Servidores de Nombres*. Son los repositorios de toda la información que conforma el espacio de nombres de dominio y de los recursos que pertenecen al espacio. La principal tarea del servidor de nombres es responder a las preguntas de los clientes.
- *Resolvedores*. Son programas que corren en los nodos y que se encargan de hacer las consultas a los servidores de nombres.

3.2.2.1. MANEJO DEL SISTEMA DE REGISTRO DE NOMBRE PARA USUARIO DE INTERNET.

Los Nombres de Dominio se estructuran como una jerarquía. Se dividen en dominios de primer nivel (TLDs: Top-Level Domains), y cada TLD en dominios de segundo nivel (SLDs: Second-Level Domains), etc. Existen más de 200 TLDs nacionales, es decir country-codes (ccTLDs), que son administrados por sus gobiernos correspondientes o por entidades privadas con el permiso adecuado del gobierno nacional y que hacen referencia al lugar donde han sido registrados (*es* para España, *se* para Suecia, *uk* para Gran Bretaña, *ch* para Suiza, etc). Un pequeño grupo de dominios de primer nivel genéricos (gTLDs) no llevan un identificador nacional pero denotan la función intencionada de aquella porción del espacio del dominio, no teniendo relación alguna con la localización física del solicitante. Estos son:

- com para organizaciones comerciales
- edu para instituciones educativas
- gov para agencias estatales
- int para organizaciones internacionales
- mil para agencias militares
- net para proveedores de servicios de red
- org para organizaciones sin ánimo de lucro

3.2.3 GESTION DE LA RED

Las redes corporativas, hoy en día, manejan cualquier tipo de información, sea voz, texto o imágenes, al tender las aplicaciones a ser multimedia, y se extienden para cubrir todos los entornos donde la empresa se desenvuelve: local, nacional e internacional, proporcionando la vía de comunicación interna, y a través de pasarelas externas, necesarios para el desarrollo de su actividad.

Cualquier red, de manera muy simple, se constituye con nodos de conmutación, a los que se conectan los usuarios, y enlaces de transmisión que sirven para interconectarlos, bien sean privados o a través de redes públicas. El correcto funcionamiento de la red, de cara a los usuarios, vendrá determinado por la disponibilidad del servicio conforme a lo planificado, lo que implica que cada uno de los elementos que intervienen en la comunicación ha de estar operativo y configurado de una determinada manera; cualquier cambio no esperado puede dar lugar a errores en la transmisión si no se detecta y corrigen sus efectos a tiempo, para lo que resulta esencial disponer de un sistema de gestión de red, adecuado a los requerimientos que demandan los usuarios.

El objetivo genérico de un sistema de gestión de red es proporcionar una plataforma de gestión distribuida para todo tipo de entornos de red, en nuestro caso redes IP, con las siguientes características:

- Monitorizar el estado actual de la red y su funcionamiento y responder a los comandos del ordenador que controla la red.
- Proporcionar un filtrado inteligente de las alarmas, que ayude a minimizar el tiempo requerido para localizar fallos.
- Aislar errores, de una manera automática, tanto de hardware como de software.
- Generar tráfico para simular condiciones reales en la red y realizar pruebas de funcionamiento.
- Adoptar acciones correctoras que ayuden al personal encargado de la red a solucionar problemas.
- Presentar información de la configuración, dando así una perspectiva más amplia de la red.
- Recoger y analizar datos de gestión muy valiosos, que permitan hacer una planificación de la red a corto y largo plazo.
- Almacenar estadísticas sobre el funcionamiento de la red.
- Formular aquellas recomendaciones útiles para el usuario.

La gestión de red se lleva a cabo mediante una aplicación software residente en el ordenador designado como Gestor de la red que, mediante una interfaz de operador, permite la gestión, y otras residentes en cada uno de los elementos que conforman la estructura de la red, es decir los nodos y medios de transmisión. El software de gestión responde a los comandos del operador de red, enviando información a los elementos de la red y/o recibiendo información de ellos. Es posible construir una gran red de gestores mediante el uso de varios servidores de datos, en la que cada uno de estos atienda un subconjunto concreto de nodos. Al iniciar una aplicación que actúe como cliente, elegirá uno de los gestores al que conectarse y entonces, dependiendo

del nivel de autoridad, administrar los nodos asociados. Esta arquitectura distribuida permite optimizar el tráfico y los tiempos de respuesta, lo que es especialmente importante en las grandes redes internacionales.

3.2.3.1 MECANISMOS PARA LA GESTION DE REDES IP

Los mecanismos para la gestión de la red que pueden ser utilizados en una red se limitan a unas cuantas tecnologías, las cuales son estándares que casi todos los fabricantes tienen que seguir y hacer disponibles utilizando sus productos.

Cuando la Internet comenzó a crecer, los administradores de red se percataron de que algunos procedimientos necesitaban ser introducidos para gestionar las redes que apenas estaban en desarrollo. El protocolo SNMP (*Simple Network Management Protocol*) fue introducido como una solución "temporal" ya que se esperaba mejorar el sistema. Posteriormente se introdujo el protocolo CMIP (*Common Management Information Protocol*) definido por la ISO. CMIP sirve para el intercambio de información de gestión entre las aplicaciones y los agentes (nodos), que acceden al servicio mediante la interfaz estándar CMIS (*Common Management Information Service*), que, en el caso de utilizar el protocolo TCP/IP recibe el nombre de CMOT. Sin embargo debido a su gran complejidad, éste protocolo, no tuvo la aceptación para la gestión de redes corporativas, es el SNMP, dada su sencillez, el que ha impuesto.

Dado que en la industria existen otros estándares de facto para redes, tal como es el caso del TCP/IP, una gran mayoría de fabricantes soportan un conjunto de estándares de gestión denominado SNMP (*Simple Network Management Protocol*), que incluye un protocolo, una especificación de estructura de base de datos y un conjunto de definiciones de objetos de datos.

Para el protocolo SNMP la red constituye un conjunto de elementos básicos: Administradores o Gestores (*Network Management Stations*) ubicados en el/los equipo/s de gestión de red y Agentes (elementos pasivos ubicados en los host, enrutadores, multiplexores, módems, etc. a ser gestionados), siendo los segundos los que envían información a los primeros, relativa a los elementos gestionados, bien al ser interrogados o de manera secuencial (ver figura 3.9). A través de la MIB (*Management Information Base)* se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo en cuestión. La MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos, que contiene información sobre variables/valores que se pueden adoptar [29].

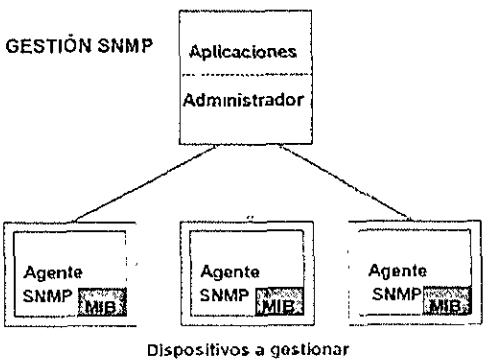

FIG 3.9 Gestión SNMP

En resumen, la gestión de red es una actividad compleja, en muchos casos, pero imprescindible para controlar los recursos de red y conseguir mantener la disponibilidad y grado de servicio que los usuarios demandan. La falta de estándares, la existencia de protocolos propietarios, la rápida evolución de la tecnología y la diversidad de entornos hace que a veces sea imposible mantener un único sistema y haya que mantener varios con distintas interfaces, pero la aplicación de inteligencia artificial, la utilización de interfaces amigables y la disponibilidad de terminales gráficos ayudarán en gran medida al gestor de red en el desempeño de su trabajo.

3.3 ENRUTAMIENTO IP

Una función fundamental de la capa de red es encaminar paquetes de la máquina de origen a la de destino. En la mayoría de las subredes, los paquetes requerirán varias escalas para completar el viaje. El enrutamiento se refiere al proceso de determinar la trayectoria que un datagrama debe seguir para alcanzar su destino. A los dispositivos que pueden elegir las trayectorias, entre el nodo fuente y el nodo destino, se les denomina enrutadores. Los algoritmos que escogen las rutas y las estructuras de datos que éstos usan son un área principal del diseño de la capa de red.

El algoritmo de enrutamiento es aquella parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada. Con datagramas esto se hace para cada paquete; con circuitos virtuales se hace sólo para cada nuevo circuito en el momento de efectuar la llamada. Los algoritmos de enrutamiento pueden agruparse en dos clases principales; *algoritmos no adaptables o enrutamiento estático* y *algoritmos adaptables o enrutamiento dinámico.* Los cuales serán descritos a continuación.

- **Enrutamiento estático.**

En el enrutamiento estático, las rutas están basadas en información de la topología no obtenida en tiempo real, sino previamente. Se fija cada posible ruta de antemano, según la capacidad de la línea, el tráfico esperado, u otros criterios. En cada enrutador se cargan sus tablas de rutas de forma estática, por lo que no necesita intercambiar ninguna información de enrutamiento con sus vecinos, y por tanto no requiere para su funcionamiento un protocolo de enrutamiento. Una de las desventajas del enrutamiento estático es que se vuelve imposible responder a situaciones cambiantes (p. ej. Saturación, exceso de tráfico o fallo de una línea).

- **Enrutamiento dinámico.**

En el enrutamiento dinámico, las rutas se fijan en cada momento en función de información en tiempo real que los enrutadores reciben del estado de la red. Se utilizan *algoritmos autoadaptativos* y es preciso utilizar un **protocolo de enrutamiento** que permita a los enrutadores intercambiar continuamente información sobre el estado de la red. Los algoritmos no pueden ser demasiado complejos pues han de implementarse en los enrutadores y ejecutarse cada poco tiempo.

En la siguiente sección se estudiarán algunos de los más importantes algoritmos de enrutamiento.

3.3.1. ALGORITMOS DE ENRUTAMIENTO

3.3.1.1 ENRUTAMIENTO POR LA TRAYECTORIA MÁS CORTA.

Esta técnica se utiliza tanto en enrutamiento estático como en enrutamiento dinámico. Para saber elegir el camino más corto primero debemos definir como medimos la distancia. La longitud de un trayecto se mide como la suma de las longitudes de cada uno de los tramos, o enlaces que se atraviesan [28]. Generalmente la 'longitud' de un enlace se mide como una combinación de diversos factores, por ejemplo:

- Velocidad del enlace (información estática)
- Tráfico medio (puede ser información estática o dinámica)
- Retardo (información dinámica medida enviando paquetes de prueba)
- Costo (información estática especificada por el usuario)

El peso relativo que se da a cada uno de los factores que intervienen en el cálculo del costo de un trayecto se denomina *métrica*. La métrica puede ser fijada o modificada al configurar el enrutador; cuando se utiliza un protocolo de enrutamiento la métrica suele estar muy relacionada con el algoritmo utilizado.

Si se utiliza información invariable (velocidad del enlace o costo) esta estrategia puede aplicarse a un enrutamiento estático. En un ordenador se carga toda la información sobre la topología de la red y se calculan las rutas óptimas en cada caso; una vez obtenidas se cargan en todos los enrutadores de la red.

Si se emplean además parámetros dinámicos (tráfico medio, retardo) obtenidos en tiempo real el algoritmo puede utilizarse para enrutamiento dinámico. En este caso la información se suele manejar de forma descentralizada y los cálculos también se hacen de manera descentralizada en todos los enrutadores.

3.3.1.2. ENRUTAMIENTO POR INUNDACION.

Es un algoritmo estático, en el que cada paquete de entrada se envía por cada una de las líneas de salida, excepto aquella por la que llegó. La inundación evidentemente genera grandes cantidades de paquetes duplicados; de hecho, una cantidad infinita a menos que se tomen algunas medidas para limitar el proceso. Para limitarlo se fija un número máximo de saltos para cada paquete igual al máximo de saltos que hay hasta llegar al punto más lejano de la red (decimos que ese número de saltos constituye el tamaño o *diámetro* de la red). Otra posibilidad es identificar todos los paquetes de manera no ambigua (por ejemplo numerándolos) para que cada enrutador mantenga una lista de los paquetes enviados; así puede evitar reenviarlos de nuevo. También puede usarse *inundación selectiva*: el paquete se envía sólo por las líneas que aproximadamente van en la dirección correcta. La inundación se utiliza en algunos algoritmos de enrutamiento multitransmisión.

3.3.1.3 ENRUTAMIENTO BASADO EN FLUJO.

Es un algoritmo estático, los dos algoritmos anteriores únicamente toman en cuenta la topología de la red; no consideran la carga. El enrutamiento basado en flujo considera tanto la topología como la cantidad de tráfico medio que soportan las líneas, y en base a esta información intenta optimizar el conjunto de las rutas para utilizar el camino menos congestionado en cada caso.

3.3.1.4 ENRUTAMIENTO POR VECTOR DISTANCIA.

Las computadoras modernas generalmente usan algoritmos de enrutamiento dinámico en lugar de los estáticos antes descritos. En particular, dos algoritmos dinámicos, el enrutamiento por vector distancia y el enrutamiento por estado de enlace, son los más comunes.

Los algoritmos de enrutamiento por vector distancia operan haciendo que cada enrutador mantenga una tabla de enrutamiento indexada por, y conteniendo un registro de, cada enrutador de la subred. Esta entrada comprende dos partes: la línea preferida de salida hacia ese destino y una estimación del tiempo o distancia a ese destino. Estas tablas se actualizan regularmente con información obtenida de los enrutadores vecinos. Cada enrutador manda la tabla completa de distancias a todos sus vecinos, y solo a estos. Con su información y la recibida de sus vecinos cada enrutador recalcula continuamente su tabla de distancias.

La métrica (es decir la medida de la distancia) puede ser número de saltos, retardo, paquetes encolados, etc., o una combinación de estos u otros parámetros. Para medir el retardo el enrutador envía un paquete de prueba que debe ser respondido por el enrutador remoto (por ejemplo en IP se utilizan paquetes especiales denominados ECHO).

3.3.1. 5 ENRUTAMIENTO POR ESTADO DE ENLACE.

El enrutamiento basado en el estado del enlace apareció como un intento de resolver los problemas que planteaba el enrutamiento por vector distancia. Se trata de un algoritmo más complejo y robusto, compuesto por cuatro fases:

1. Descubrir los enrutadores vecinos y averiguar sus direcciones.
2. Medir el retardo o costo de llegar a cada vecino.
3. Construir un paquete que resuma toda esta información, y enviarlo a **todos** los enrutadores.
4. Calcular el camino más corto a cada enrutador.

Veamos resumidamente que sucede en cada fase:

1. Para conocerse los enrutadores al activarse envían paquetes de presentación (HELLO) por todas sus interfaces; los paquetes HELLO son respondidos con mensajes identificativos por los enrutadores.
2. Para conocer el retardo los enrutadores envían paquetes de prueba (p. ej. ECHO) que son respondidos por el enrutador remoto, y miden el tiempo de ida y vuelta. En ocasiones se toma en cuenta el tiempo en cola, y en ocasiones no. Ambas opciones tienen sus ventajas e inconvenientes.
3. Con toda la información obtenida el enrutador debe construir un paquete y enviarlo a todos los otros enrutadores. Para esto utiliza *inundación*. Los paquetes se numeran para detectar (y descartar) duplicados, e ignorar paquetes obsoletos (si llega el paquete 26 después de haber recibido el 28 se descarta). Además cada paquete tiene una vida limitada, al cabo de la cual es descartado.
4. Con toda la información obtenida el enrutador conoce perfectamente la topología de la red, y puede calcular el camino óptimo mediante el algoritmo del camino más corto por ejemplo.

3.3.1.6 ENRUTAMIENTO JERARQUICO

A medida que crece en tamaño las redes, crecen proporcionalmente las tablas de enrutamiento. Las tablas que siempre crecen no sólo consumen memoria del enrutador, sino que también se necesita más tiempo CPU para examinarlas y más ancho de banda para enviar informes de estado entre enrutadores. En cierto momento, la red puede crecer hasta el punto en que ya no es factible que cada enrutador tenga una entrada para cada uno de los demás enrutadores, por lo que el enrutamiento tendrá que hacerse jerárquicamente, como ocurre en la red telefónica.

Al usarse el enrutamiento jerárquico, los enrutadores se dividen en regiones, donde cada enrutador conoce todos los detalles de la manera de enrutar paquetes a destinos dentro de su propia región, pero no sabe nada de la estructura interna de las otras regiones. Al interconectar diferentes redes, es natural considerar cada una como región independiente, a fin de liberar a los enrutadores de una red de la necesidad de conocer la estructura topológica de las demás. En la práctica se suelen dar dos o más niveles jerárquicos de enrutamiento.

3.3.1.7 ENRUTAMIENTO POR DIFUSION (BROADCAST)

En algunas aplicaciones, los hosts necesitan enviar un paquete a varios hosts o a todos los demás. El envío simultáneo de un paquete a todos los destinos se llama difusión; se han propuesto varios métodos para llevarla a cabo.

A veces esto se hace por inundación, ya que esta técnica es especialmente apropiada en este caso. Sin embargo se pueden producir bucles en la red. Otro método es el enrutamiento *multidestino*. Se manda un único paquete con todas las direcciones a las que debe enviarse, y en cada enrutador se replica en aquellas interfaces donde esta justificado, es decir, las que son parte de la mejor ruta para alguno de los destinos indicados. Otro algoritmo es construir el árbol de extensión (*spanning tree)* correspondiente al origen, y seguirlo, replicando el paquete allí donde haya una bifurcación. El árbol de extensión no tiene bucles. El sistema es óptimo, ya que se asegura que la distribución se hará generando el número mínimo de paquetes y sin duplicados. Pero esto requiere que cada enrutador conozca cuales de sus interfaces forman parte del árbol de extensión para el enrutador origen, y cuales no. Con enrutamiento del estado del enlace los enrutadores poseen esta información. Por último el algoritmo de *enrutamiento por el camino inverso* intenta emular al árbol de extensión cuando la información sobre la topología no está disponible. Consiste en lo siguiente: el enrutador examina la dirección origen del paquete recibido, y la interfaz por la que le ha llegado; si la interfaz es la vía habitual para esa dirección es bastante probable que el paquete no sea un duplicado, por lo que lo reenviará por todas las interfaces excepto por aquella por la que vino; si no es la interfaz habitual para esa dirección el paquete se descarta pues es muy probable que sea un duplicado. Esta técnica evita que se produzcan bucles y consigue una eficiencia bastante buena, aunque no tanto como el árbol de extensión ya que algunos paquetes no llegaran a su destino por la ruta óptima.

3.3.1.8 ENRUTAMIENTO POR MULTITRANSMISIÓN(MULTIDIFUSIÓN).

En algunas aplicaciones, procesos muy separados trabajan juntos en grupos; por ejemplo, un grupo de procesos que implementan una base de datos distribuida. Con frecuencia es necesario que un proceso envíe un mensaje a todos los demás miembros del grupo. Por tanto, necesitamos una manera de enviar mensajes a grupos bien definidos de tamaño numéricamente grande, pero pequeños en comparación con la totalidad de la red.

El envío de un mensaje a uno de tales grupos se llama multitransmisión, y su algoritmo de enrutamiento es el enrutamiento por multitransmisión. Para la multitransmisión se requiere administración de grupos. Se necesita alguna manera de crear y destruir grupos, y un mecanismo para que los procesos se unan a los grupos y salgan de ellos. La forma de realizar estas tareas no le concierne al algoritmo de enrutamiento. Lo que sí le concierne es que, cuando un proceso se una a un grupo, informe a su host del hecho. Es importante que los enrutadores sepan cuáles de sus hosts pertenecen a qué grupos. Los hosts deben informar a sus enrutadores de los cambios en los miembros del grupo, o los enrutadores deben enviar periódicamente la lista de sus hosts. De cualquier manera, los enrutadores aprenden qué hosts pertenecen a cuáles grupos. Los enrutadores les dicen a sus vecinos, de manera que la información se propaga a través de la red.

3.4 ACCESO REMOTO

A medida que las redes se vuelven más globales en sus metas, hay una necesidad creciente y constante de todas las partes de la organización, de estar conectadas. Esta demanda se extiende aún a aquellos usuarios que pueden solo muy raramente visitar físicamente las oficinas de la compañía.

Hoy, todos los usuarios remotos y oficinas remotas necesitan estar conectados y los productos para acceso remoto se han convertido en el puente entre estas islas remotas y la oficina central.

3.4.1 SERVIDORES DE ACCESO REMOTO

Mientras que Ethernet es "local" a un área geográfica, como un edificio, usuarios remotos, tales como personal de ventas que viaja, requieren acceso a recursos de la red. El acceso remoto a la LAN se está convirtiendo rápidamente en un modo usual de proveer este tipo de conectividad.

Las soluciones de acceso remoto utilizan servicios telefónicos para vincular usuarios remotos u oficinas a la red corporativa. Para aplicaciones exigentes, donde la velocidad y el acceso permanente son cruciales, una solución tipo línea dedicada debiera ser aplicada. Esto implica el comprar un "enrutador" y un servicio de línea especial el cual esencialmente consiste en una línea telefónica dedicada con un cierto ancho de banda – pudiendo este ir desde los 56 Kbps a varios Megabits por segundo. Esta solución está limitada a la conexión de dos oficinas y puede ser muy cara. Los accesos remotos por marcado ("Dial-Up Remote Access" y RAS Services "Remote Access Services") ofrecen tanto a la oficina remota como al usuario remoto la economía y flexibilidad de los servicios telefónicos al estilo "pague lo que usa".

Con acceso remoto asincrónico, líneas de telefonía común se combinan con módem y servidores de acceso remoto para permitir a los usuarios y a las redes, marcar a cualquier parte del mundo y tener acceso a los datos.

Servidores de acceso remoto proveen puntos de conexión de marcado entrante como saliente para aplicaciones de la red a la cual están unidos. Para usuarios de PC remotas o portátiles, existe la flexibilidad de conectarse desde cualquier parte con servicio de telefonía básica, incluidos hoteles, aeronaves, etc.

La tecnología Acceso Remoto está optimizada para un número de aplicaciones remotas. Las aplicaciones de nodos remotos y de control remoto son aquellas en las que un usuario en una PC marca dentro de una red y es capaz de funcionar tal y como lo haría si él o ella estuvieran conectados directamente a la red (con la salvedad de la velocidad de transmisión de los datos que dependerá obviamente de la velocidad del vínculo remoto).

Una conexión LAN-to-LAN es cuando una red remota completa es soportada a través de una conexión "dial-up". Servidores de Acceso Remoto en cada extremo de la conexión hacen las veces de "enrutadores" para generar automáticamente una conexión cuando se requieren recursos remotos.

La conexión "dial-up" es mantenida de acuerdo a parámetros establecidos por el encargado de redes, en cuanto a "time-outs", protocolos permitidos, duración de la conexión, etc.

Las aplicaciones de acceso a Internet involucran el uso de servidores de acceso remoto para protección ("firewall") de la red local frente a potenciales eventos de seguridad presentes en la Internet. El encargado de la red configura filtros para asegurarse que solamente tráfico autorizado puede pasar entre la red local e Internet.

"Modem sharing" o compartir modems es la habilidad de servidores de acceso remoto de proveer acceso, a usuarios de la red, a un banco de modems, tanto para aplicaciones "dial-in", cuanto para aplicaciones "dial-out". Software, corriendo sobre "hosts" conectados a la red, le permite a estos conectarse a modems unidos a servidores de acceso remoto, proveyendo así servicios de comunicación económicos desde el "sitio" centralizador y preservando la inversión económica en modems y demás hardware de comunicaciones.

La clave para el control de costos es la habilidad del servidor de acceso remoto para enrutar los protocolos deseados y para implementar decisiones basadas en políticas de cómo las conexiones marcadas entre sitios deben ser manejadas.

La demanda de aplicaciones de Acceso Remoto por marcado está ocasionando una gran evolución en la funcionalidad tanto de terminales como de servidores.

3.4.2 PROTOCOLOS DE AUTENTIFICACION DE ACCESO REMOTO

El acceso remoto a las intranets corporativas, así como a la Internet, ha hecho que los Servidores de Acceso Remoto (RAS) se vuelvan una parte vital de los servicios de internetworking de hoy en dia. A continuación se mencionarán algunos de los protocolos de acceso remoto que existen.

- **Protocolo PPTP (Point-to –Point Tunneling Protocol).**

PPTP se diseñó para proporcionar comunicaciones autenticadas y cifradas entre un cliente y una puerta de enlace o entre dos puertas de enlace (sin necesitar una infraestructura de clave pública) utilizando un Id. de usuario y una contraseña. Apareció por primera vez en 1996, implementado por Microsoft. El objetivo del diseño era la simplicidad, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP. Actualmente este protocolo, aunque muy popular en el mundo Microsoft, está siendo sustituido por el L2TP, ya que sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual.

- **Protocolo L2TP (Layer 2 Tunneling Protocol)**

El protocolo L2TP es una de las técnicas emergentes para ofrecer conexión remota a las intranets corporativas. Este protocolo ha emergido de dos protocolos diferentes: el PPTP y el L2F (Layer 2 Forwarding).

L2TP es un protocolo maduro en la senda de los estándares IETF que ha sido ampliamente implementado. L2TP encapsula las tramas del protocolo punto a punto (PPP, Point-to-Point Protocol) que van a enviarse a través de redes IP, X.25, frame Relay, o modo de transferencia asíncronica (ATM, Asynchronous Transfer Mode). Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN[13] en Internet. L2TP sobre IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de *control* L2TP para el mantenimiento del túnel. L2TP también utiliza UDP para enviar tramas PPP encapsuladas en L2TP como *datos* del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar mediante el modo de transporte IPSec para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad. L2TP se diseñó específicamente para conexiones cliente a servidores de acceso a redes, así como para conexiones puerta de enlace a puerta de enlace. Es una buena solución para conexiones seguras de acceso remoto y de puerta de enlace a puerta de enlace [30].

3.5 SEGURIDAD IP

El concepto de seguridad en la información es mucho más amplio que la simple protección de datos a nivel lógico. Para proporcionar una seguridad real debemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habría que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

[13] *Una VPN, Red Privada Virtual, es una forma de compartir y transmitir información entre un circulo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos*

1. ***Sistemas aislados.*** Son los que no están conectados a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.
2. ***Sistemas interconectados.*** Hoy por hoy casi cualquier computadora pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencia que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad podrían clasificarse de la siguiente forma:

1. ***Seguridad física.*** Engloba todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de respaldos, etc. También se suelen tener en cuanta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.
2. ***Seguridad de la información.*** Se refiere a la reservación de la información frente a observadores no autorizados(intrusos). Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, el tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.
3. ***Seguridad en el canal de comunicación.*** Los canales de comunicación rara vez se consideran seguros. Debido a que la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.
4. ***Problemas de autentificación.*** Debido a los problemas de canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen.
5. ***Problemas de suplantación.*** En las redes tenemos el problema añadido de que cualquier usuario no autorizado puede acceder al sistema desde fuera, por lo que debemos de confiar en sistemas fiables para garantizar que los usuarios son están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en password para corregir esto.

Especialmente con el crecimiento comercial de la Internet muchas empresas se enfrentan ante la necesidad de conectar sus redes al exterior; sin embargo esto plantea varios problemas de seguridad por diversos motivos, por ejemplo:

- Los ordenadores de la red local contienen información de carácter confidencial cuya salvaguardia resulta vital para la empresa.

- Del exterior pueden llegar virus u otro tipo de programas que perjudicarían seriamente los ordenadores de la empresa.
- Los empleados pueden utilizar la conexión a Internet para salir a lugares no autorizados (por ejemplo servidores de información no relacionados con la actividad profesional de la empresa).

3.5.1 TECNICAS UTILIZADAS PARA LA SEGURIDAD EN LAS REDES.

Las siguientes técnicas son usadas comúnmente para ofrecer varios grados de servicios de seguridad en una red de computadoras, algunas de las cuales serán estudiadas más adelante.

- Filtrado IP
- Traducción de direcciones de Red (Network Address Translation, NAT)
- SOCKS
- Capa de sockets segura (Secure Sockets Layer, SSL)
- Firewalls
- Servidores Proxy
- Protocolos de validación de identificación.
- Programas Antivirus.

3.5.1.1 FILTRADO DE PAQUETES IP

El nivel de red es el más importante en el filtrado de paquetes. El filtrado de paquetes es una técnica de cortafuegos (firewall)[14] aplicada normalmente en los enrutadores que permite, controlar la transferencia de información entre las redes que une el propio enrutador con base en:

- La dirección IP de origen
- La dirección IP de destino
- El tipo de protocolo de nivel superior que transporta el paquete: TCP, UDP o ICMP[15].
- El campo de opciones IP, que generalmente no se utiliza, pero que puede contener información como la ruta que debe seguir el paquete IP.

[14] *El firewall es un sistema que refuerza las políticas de control de acceso, con el objetivo de proteger a las redes internas del acceso no autorizado vía Internet o mediante otra red externa.*

[15] *ICMP (Protocolo de Control de Mensajes Internet), es un protocolo robusto encargado de generar mensajes de error en caso de fallas durante el transporte de los datos por el cable*

Una de las principales ventajas que se tiene con el filtrado de paquetes es la protección centralizada, ya que con un único enrutador, habilitado con ésta opción, situado estratégicamente puede protegerse toda una red, además de que el filtrado de paquetes puede realizarse de forma totalmente transparente a los servicios de los usuarios. A pesar de la gran variedad de sistemas que permiten el filtrado de paquetes, ésta técnica comparte una serie de limitaciones; las reglas de filtrado[16] son difíciles de configurar y probar, siempre existe algún agujero que puede escaparse al administrador de seguridad, los cuales permiten la entrada de ataques externos.

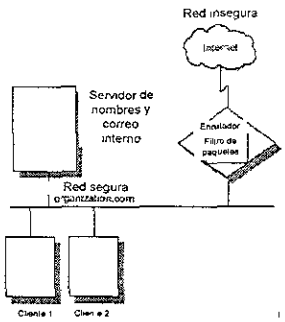

FIG 3.10 Enrutador habilitado para filtrado de paquetes

3.5.1.2 NAT (NETWORK ADDRESS TRANSLATION, TRADUCCION DE DIRECCIONES DE RED)

NAT, es el proceso de translación de una dirección IP interna y no registrada, en una dirección IP valida en Internet. Esta característica del servicio permite seguir utilizando las direcciones actuales que posee el cliente, sin necesidad de realizar un cambio de numeración. De esta forma y como ventaja adicional, se oculta la numeración IP interna de la red. Cuanta menos información se proporcione acerca de la red, menor será la probabilidad de un ataque [31].

Existe una restricción en cuanto a la numeración IP interna que es posible utilizar: Sólo se aceptan redes que se encuentren dentro de los rangos definidos en el RFC1918 (Address Allocation for Private Internets).

3.5.1.3 FIREWALLS

Un firewall es un conjunto de sistemas ubicado en el sitio central de conexión de una red. Usualmente es colocado como protección para la conexión de la red a la Internet. La función principal de un firewall es controlar el acceso desde y hacia la red protegida. Todas las conexiones externas son forzadas a pasar a través del firewall, donde son examinadas y evaluadas antes de determinar que conexiones son permitidas y cuales son rechazadas.

[16] *Con las reglas de filtrado puede controlarse el tráfico hacia/desde una máquina identificada por una dirección, pero no puede realizarse un control por usuario*

Un firewall puede ser un enrutador, una PC, un servidor o un conjunto de servidores, configurados específicamente para proteger una Red de protocolos y servicios que puedan ser mal utilizados desde fuera de la Red.

El firewall usualmente es colocado como el gateway de nivel mas alto de le red hacia la Internet, sin embargo el firewall también se puede colocar en el gateway más bajo de la red para proveer protección a pequeños grupos de servidores o subredes.

El funcionamiento de un firewall se basa en el manejo y administración de los protocolos de TCP/IP (Transfer Control Protocol / Internet Protocol) conocidos como la suite TCP, dentro de los cuales se pueden encontrar todos los servicios y protocolos usados en INTERNET.

La administración de estos servicios y protocolos la realiza básicamente a partir de 2 objetos conocidos como: Entidades y Reglas, donde las entidades son máquinas o grupos que pueden ser Redes, Subredes, servidores, etc., y las reglas determinan que tipo de permisos tienen cada una de estas entidades, es decir que protocolos y que servicios pueden utilizar a través del firewall ya sea de la Internet hacia la red protegida por este o de la red protegida hacia la Internet, un firewall ofrece otros servicios como limitar el acceso de los usuarios a Internet, filtrar la información a la que se tiene acceso en la Internet, es decir controlar el acceso a paginas consideradas ofensivas, etc.

El mayor problema de los firewalls es que restringen mucho el acceso a la Internet desde la red protegida. Básicamente, reducen el uso de la Internet al que se podría hacer desde un terminal. Tener que entrar en el firewall y desde allí realizar todo el acceso a Internet es una restricción muy seria. Programas como *Netscape*, que requieren una conexión directa con la Internet, no funcionan desde detrás de un firewall. La solución a todos estos problemas es un Servidor Proxy [32].

3.5.1.4 SERVIDORES PROXY

Los servidores proxy proporcionan el acceso a una red insegura para determinados protocolos de aplicación a través de un servidor con doble acceso. Un proxy es un servidor que recibe peticiones de archivos o páginas en Internet. El navegador hace la solicitud al proxy, quien se encarga de cargar los documentos de la red y enviarlos al navegador.

El proxy guarda en memoria la información que ha cargado de la red, de modo que si otro usuario intenta cargar la misma información, el proxy la tendrá en memoria, reduciendo el tiempo de acceso.

Como el Proxy conserva localmente la información, el acceso a páginas que se visitan frecuentemente es mucho más rápido. La carga de la red se reduce, ya que las páginas cargadas del Proxy no incurren en accesos externos a Internet. Adicionalmente, si el sitio al que se desea entrar tiene problemas, se carga la información existente en el proxy, de esta manera se puede tener acceso a la información

Es importante realizar las conexiones a través de un proxy junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un enrutador con filtrado de paquetes Si hay conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor proxy y producirse ataques desde el exterior.

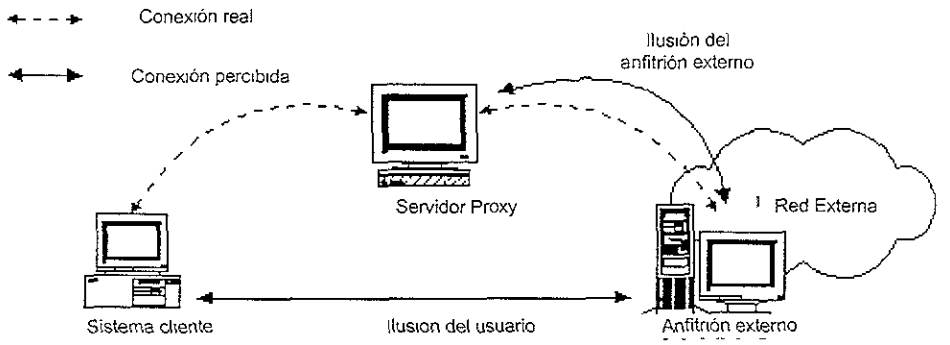

FIG 3.11 El servidor Proxy

3.5.1.5 IPSec (IP Security Architecture, Arquitectura de Seguridad IP).

El protocolo de Internet, IP, también conocido como IPv4, no provee por sí mismo ninguna protección a sus transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. IPSec intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos, pero IPSec ofrece soporte para ambos de un modo uniforme.

IPSec provee confidencialidad[17], integridad[18], autenticidad[19], y protección a la réplica[20] a través de dos nuevos protocolos. Estos protocolos se llaman «Cabecera de Autentificación» (AH, "Authentication Header") y «Cargo de Seguridad Encapsulado» (ESP, "Encapsulated Security Payload").

AH provee autentificación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH también asegura partes de la cabecera IP del paquete (como las direcciones de origen o destino).

ESP puede proveer autentificación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera en el paquete). La protección a la réplica requiere autentificación e integridad (éstas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autentificación y/o integridad. Del mismo modo, puede usar la autentificación y/o la integridad con o sin la confidencialidad.

---

[17] *La confidencialidad se define como el asegurarse de que sea difícil para todos comprender qué datos se han comunicado, excepto para el receptor.*

[18] *La Integridad garantiza que los datos no puedan ser cambiados en el camino.*

[19] *La Autenticidad permite que los usuarios firmen sus datos de modo que otros puedan verificar que realmente usted es quien los envió.*

[20] *La Protección a la réplica asegura que una transacción solo se pueda llevar a cabo una vez, a menos que se autorice que la repitan*

3.5.1.5 SOCKS

SOCKS es un protocolo de red para conexiones TCP/IP que nos permite dirigir el tráfico de una red de igual manera que un servidor proxy [33]. SOCKS se creo inicialmente para ser utilizado como firewall, actualmente es aplicado en soluciones VPN, Extranets, Servidores Proxy y por supuesto como firewall. Este protocolo permite verificar los paquetes entrantes y los que salen, "escondiendo" las direcciones IP de nuestra red interna. Existen dos versiones de SOCKS la V.4 la V.5 esta última agrega un método de autentificación para hacer más robusto el modelo de seguridad de nuestras aplicaciones.

Existen tres funciones generales tanto para V.4 como V.5: realizan la petición de la conexión desde el cliente pasando por el servidor SOCKS hasta la red exterior, habilitan un circuito de tipo proxy entre el cliente y el servidor SOCKS y reenvían los datos de la aplicación entre la red interior y la exterior.

El servidor SOCKS se implementa entre la red interna y la externa. Permitiendo a los usuarios internos acceder a recursos en la red externa, así mismo, bloquea todo intento de usuarios externos de acceder a la red interna sin autorización previa. Cuando un cliente de red necesita conectarse a un servidor externo se conecta primero al servidor que tiene implementado SOCKS, este último hace la petición a la máquina que el cliente desea y le manda la información de regreso al cliente. Para esto la máquina externa no conoce la dirección del cliente que generó la petición, solo conoce la dirección del servidor con SOCKS. El puerto que generalmente es usado en los servidores para ofrecer este servicio es el 1080 pero puede variar dependiendo de la configuración de este.

La ventaja principal de Socks es su popularidad. Debido a que se emplea ampliamente, la utilización del servidor y clientes tipo Socks (por ejemplo, versiones de programas como FTP y Telnet que ya han sido convertidos a Socks de usuario) están disponibles de forma común y es fácil encontrar ayuda. Esto puede ser un arma de dos filos; se han reportado casos en donde los intrusos a sitios con firewalls han instalado sus propios clientes con conocimientos de Socks.

Una desventaja de Socks es que funciona sólo para clientes basados en TCP; no funciona para clientes basados en UDP.

3.6 MULTIDIFUSION Y CALIDAD DE SERVICIO (QoS)

Las aplicaciones de hoy en día son muy diferentes a aquellas que fueron desarrolladas algunos años atrás. Anteriormente las aplicaciones estaban principalmente basadas en texto, con usuarios especialmente entrenados, sentados enfrente de un equipo terminal descifrando la información encriptada que era desplegada en la pantalla. Hoy en día las aplicaciones ofrecen ayudas gráficas, explicaciones habladas y en algunos casos hasta suplementos en vídeo. Estas aplicaciones son utilizadas por los usuarios en las oficinas y en los hogares quienes ya no requieren de un entrenamiento muy sofisticado.

Este desarrollo ha traído cambios significativos en muchas áreas desde nuevas expectativas por parte de los usuarios, en el diseño de las aplicaciones, la infraestructura de la red y la necesidad de más ancho de

banda. Estos cambios han resultado en la aparición de nuevas aplicaciones para lograr satisfacer los requerimientos, una de ellas es el concepto de multidifusión.

Además de la multidifusión, otras tecnologías, como el desarrollo de los protocolos RSVP (Resource Reservation Protocol) y el protocolo RTP (Real Time Protocol) para cubrir otras demandas. Por primera vez se ha tomado en serio la calidad de servicio (QoS)[21] por los administradores de red.

3.6.1 MULTIDIFUSIÓN.

Multidifusión es... una necesidad, cuando se tiene información (*mucha* información habitualmente) que debe ser transmitida a varios usuarios (pero no a *todos*) en una red, entonces la respuesta es Multidifusión. Una situación frecuente donde se utiliza es en la difusión de audio y vídeo en tiempo real a un conjunto de usuarios que se han unido a una conferencia distribuida [34].

Multidifusión es, en gran medida, como la televisión o la radio, es decir, sólo aquellos que han sintonizado sus receptores (al seleccionar una frecuencia particular que les interesa) reciben la información.

3.6.1.1 MULTIDIFUSIÓN IP.

Internet es una red en la que el intercambio de información entre equipos locales o remotos se hace a través de datagramas IP. Estos datagramas IP están formados principalmente por una dirección origen y una dirección destino, y cada equipo de comunicaciones situado en la ruta entre ambos se encarga de enviar dicho datagrama por el camino adecuado. Esto implica que cada estación conectada a Internet debe tener una dirección que la identifique, lo que se llama dirección IP, y constituye un sello de identidad global y único para cada equipo en Internet.

Pueden clasificarse en tres tipos en función de la dirección de destino:

- **IP unidifusión**: La dirección corresponde a un solo receptor y será éste el único que procese los datagramas IP con ese destino (conexión uno-a-uno).
- **IP difusión**: La dirección corresponde a todos los equipos conectados en un mismo tramo de red local y el datagrama IP es procesado por todos ellos (conexión uno-a-todos dentro de la misma subred).
- **IP multidifusión**: La dirección corresponde a un grupo de equipos, y sólo estos procesarán los datagramas IP con ese destino (conexión uno-a-muchos, o uno-a-varios).

Cuando un equipo envía un datagrama IP a una determinada dirección IP multidifusión, sólo es recibida por aquellos equipos que están a la escucha de esa dirección y, que por tanto, son capaces de entender las direcciones multidifusión [35]. Para ello es necesario que la PC permita, a las aplicaciones que hacen uso del multidifusión, configurar el dispositivo de red para recibir, no sólo los datagramas que van destinados a su dirección IP, como es habitual, sino también aquellos que van destinados a una determinada dirección multidifusión. Del mismo modo, se debe poder indicar al dispositivo de red, que deje de recibir los

[21] *Desde el punto de vista de red se define calidad de servicio QoS como el tratamiento que se le da a cada paquete de un flujo en los nodos, para que cumplan con una serie de políticas especificadas para cada flujo*

datagramas de una determina dirección multidifusión. Estas acciones de unirse (join) o abandonar (leave) una determinada dirección multidifusión, también son significativas para los dispositivos que enrutan los datagramas multidifusión entre varias subredes (mrouters) y son realizadas por medio de un protocolo sencillo llamado IGMP (Internet Group Management Protocol), del que hablaremos más adelante.

Las direcciones IP multidifusión se suelen denominar "grupo multidifusión", ya que no están asignadas a un equipo en concreto de forma permanente, sino a un grupo de equipos determinado y de forma temporal. Por otro lado, no es necesario que un equipo pertenezca a un grupo concreto multidifusión para enviar datagramas al mismo.

Las direcciones IP multidifusión, que todo equipo conectado a la red multidifusión debe saber reconocer, forman una clase de direccionamiento llamada clase D, (ver capítulo 3, sección 3.2.1.1 DIRECCION IP).

Los datagramas multidifusión son enviados hacia los miembros del grupo destino usando la misma fiabilidad "best effort[22]" que los datagramas IP unidifusión. Esto quiere decir que no existe garantía de que los datagramas lleguen a su destino, ni de que lo hagan de forma ordenada. El protocolo de transporte empleado es el UDP que ofrece la ventaja de que al ser un protocolo ligero (ver capítulo 2, sección2.2.4.1 PROTOCOLOS DE LA CAPA DE TRANSPORTE), los datagramas sufren menos retrasos en alcanzar su destino. Sin embargo la demanda de aplicaciones en tiempo real, es son las conferencias de audio y vídeo, si bien son tolerantes a perdidas de paquetes, no lo son en cuanto a que estos lleguen de forma desordenada.

Hasta aquí hemos estudiado el funcionamiento de IP multidifusión dentro de un segmento de red. Sin embargo para que los datagramas IP puedan ser propagados a través de distintos tramos de red se requieren enrutadores multidifusión (mrouters). Cuando un enrutador esta cualificado para intercambiar datagramas IP multidifusión con otro u otros , decimos que es un enrutador multidifusión, o abreviadamente un mrouter. Un mrouter debe contar con un mecanismo para conocer en todo momento los equipos que pertenecen a un determinado grupo multidifusión en cada una de las redes que interconecta y para cada pareja {dirección IP origen (o fuente), grupo multidifusión} debe saber cómo encaminar los datagramas, originados en esa dirección IP, a los segmentos de red donde haya otros miembros de ese grupo multidifusión.

IGMP (INTERNET GROUP MANAGEMENT PROTOCOL).

Del mismo modo que el ICMP (Internet Control Message Protocol), el IGMP (Internet Group Management Protocol) es una parte integral del IP (ver figura 3.11). El Protocolo IGMP, es un protocolo que administra la membresía de los servidores en los grupos IP multidifusión.

[22] *Best-effort se define como el mejor esfuerzo.*

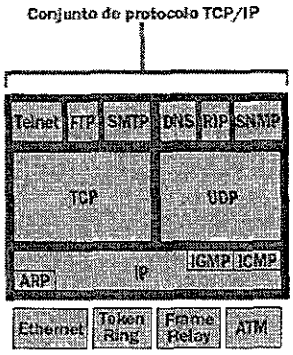

FIG 3.12 Suite de protocolos TCP/IP

El IGMP es requerido en todos los servidores que soportan el nivel 2 de la transmisión IP multidifusión. Los paquetes IGMP son enviados utilizando una cabecera IP.

Los mensajes IGMP toman dos formas:

1. Cuando un servidor se une a un grupo de servidores, envía un mensaje de Reporte de Membresía de Servidor (Host Membership Report) a la dirección IP multidifusión para todos los servidores o a la dirección multidifusión deseada declarando su membresía en un grupo de servidores específico haciendo referencia a la dirección IP multidifusión.
2. Cuando un enrutador revisa la red para asegurarse de que hay miembros de un grupo de servidores específico, envía un mensaje de Petición de Membresía de Servidor (Host Membership Query) a la dirección IP multidifusión para todos los servidores. Si no se reciben respuestas a la petición después de varios intentos, el enrutador supone que no hay membresías en ese grupo para esa red y deja de anunciar la información de red de ese grupo a los otros enrutadores.

Para que la transmisión de IP multidifusión incluya enrutadores a lo largo de una red los enrutadores utilizan protocolos de enrutamiento multidifusión para comunicar la información del grupo de servidores de tal manera que cada enrutador que soporte el redireccionamiento multidifusión sé de cuenta de qué redes contienen miembros para cuál grupo de servidores.

3.6.1.2 ENRUTAMIENTO MULTIDIFUSION

Las ventajas de la idea del IP multidifusión se hacen patentes cuando podemos extender el esquema de funcionamiento entre varias subredes, es decir, cuando los miembros de un determinado grupo multidifusión están distribuidos en varios segmentos de red distintos, interconectados a través de mrouters. Para que el concepto multidifusión funcione, no basta con que los enrutadores multidifusión conozcan, por medio del IGMP, qué equipos pertenecen a un determinado grupo multidifusión en los segmentos de red que éste conecta, sino que deben saber tomar las decisiones necesarias para enlutar los datagramas multidifusión entre dichas subredes, asegurando que los datagramas enviados por un determinado equipo lleguen a todos los miembros de cada grupo multidifusión, y procurar, por otro lado, que no se produzcan bucles, esto es, que

cada datagrama llegue a sus destinatarios sólo una vez (y, preferiblemente, por el camino más corto). Es decir, debe existir una determinada política de enrutamiento multidifusión, o dicho de otra forma, estos enrutadores deben implementar un protocolo de enrutamiento multidifusión. Un protocolo de enrutamiento multidifusión es el que se encarga de la construcción de los árboles de distribución (delivery trees) y habilitar la remisión (forwarding) de datagramas multidifusión. La característica diferencial entre el enrutamiento unicast y el multidifusión, es que los datagramas multidifusión deben ser remitidos acullá de su origen. Si un datagrama IP multidifusión es remitido hacia su origen, se podría producir un bucle de remisión, que podría dar lugar a una 'avalancha' multidifusión.

Todos los protocolos de enrutamiento multidifusión hacen uso del protocolo IGMP para conocer la filiación de los equipos finales a cada determinado grupo multidifusión, pero difieren en la forma de intercambiar dicha información entre mrouters vecinos, así como en las técnicas empleadas en la construcción de los árboles de distribución.

Los protocolos de enrutamiento multidifusión pueden ser agrupados en dos categorías: protocolos modo denso (dense mode) y protocolos modo esparcido (sparse mode) [2].

Los protocolos modo denso asumen una alta concentración de servidores participando en la multidifusión. Inicialmente los datos son difundidos por toda la red, después suprimen las trayectorias que no tienen receptores interesados. Los protocolos modo denso son apropiados para redes locales, pocas fuentes-muchos receptores interesados. Algunos ejemplos de este tipo de protocolos son: DVMRP (Distance Vector Multidifusión Routing Protocol,), MOSPF (Multidifusión Open Shortest Path First) y el protocolo PIM-DIM (Protocol Independent Multidifussion- Dense Mode).

Los protocolos modo esparcido asumen que nadie está interesado en recibir la información a menos que explícitamente pida transmisión. Estos protocolos están diseñados para situaciones donde los grupos multidifusión están dispersos en una región extensa. Los protocolos de modo esparcido pueden funcionar en entornos de redes LAN, pero son más eficaces en las redes de área extensa. En este caso no se difunde el tráfico por toda la red lo cual ocasiona un ahorro en el ancho de banda comparado con el consumo en ancho de banda de los protocolos en modo denso. Algunos ejemplos de este tipo de protocolos son: PIM-SM (Protocolo Independent Multidifusióning-Sparse Mode) y CBT (Core-Based Tree).

3.6.2 CALIDAD DE SERVICIO (QoS, QUALITY OF SERVICE)

Los últimos años han sido testigos del rápido crecimiento del tráfico de redes informáticas. Los administradores agregan continuamente nuevos recursos para tratar de responder al ritmo de la creciente demanda. Incluso los clientes de redes no están, a menudo, satisfechos con el rendimiento de la red. El uso creciente de un nuevo tipo de aplicaciones multimedia ávidas de recursos va a agudizar esta situación.

Estas aplicaciones emergentes generan tráfico a ritmos variables y requieren normalmente que la red pueda transportar tráfico al ritmo que las aplicaciones lo han generado. Asimismo, las aplicaciones son más o menos tolerantes a retrasos de tráfico en la red y a variaciones de los mismos. Algunas aplicaciones pueden

tolerar cierto grado de pérdida de tráfico, mientras que otras no. Si dispusiéramos de recursos de red infinitos, todo el tráfico de las aplicaciones podría transportarse al ritmo requerido, sin latencia y sin pérdida de paquete. Sin embargo, los recursos de red no son infinitos. Como consecuencia, hay partes de la red en las que los recursos no pueden responder a la demanda [36].

La QoS puede definirse desde dos puntos de vista:

- Desde el punto de vista del usuario
- Desde el punto de vista de la red

Desde el punto de vista del usuario podemos decir que QoS es el desempeño que el usuario observa sobre las aplicaciones en la red.

Desde el punto de vista de la red definimos la QoS como el tratamiento que se le da a cada paquete de un flujo en los nodos, para que cumplan con una serie de políticas especificadas para cada flujo.

3.6.2 CALIDAD DE SERVICIO EN REDES IP

La Redes IP actuales no ofrecen servicios de transporte con cierta QoS, las cuales están construidas mediante la unión de dispositivos de red, los enrutadores. Estos dispositivos se intercambian el tráfico entre ellos mediante interfaces. Si la velocidad en la que el tráfico llega a una interfaz es superior a la velocidad en la que la interfaz puede enviar tráfico al siguiente dispositivo, se produce una congestión. De esta forma, la capacidad de una interfaz para enviar tráfico constituye un recurso de red fundamental. Los mecanismos de QoS funcionan al establecer preferencias en la asignación de este recurso en favor de cierto tráfico.

Para poder realizar esta acción, es necesario, en primer lugar, identificar tráficos diferentes. El tráfico que llega a los dispositivos de red se separa en distintos *flujos* mediante el proceso de *clasificación de paquetes*. El tráfico de cada flujo se envía a una *cola* en la interfaz de reenvío. Las colas de cada interfaz se *gestionan* dé acuerdo con algunos algoritmos. El algoritmo de administración de cola determina la velocidad a la que se reenvía el tráfico de cada cola. De este modo, se determinan los recursos que se asignan a cada cola y a los flujos correspondientes. Para proporcionar QoS en redes, es necesario configurar y proporcionar a los dispositivos de red lo siguiente:

1. Información de clasificación por la que los dispositivos separan el tráfico en flujos.
2. Colas y algoritmos de administración de cola que controlan el tráfico de los diferentes flujos

Nos referiremos a ambos como *mecanismos de control de tráfico*. Los mecanismos de control del tráfico por separado no resultan útiles. Deben proporcionarse o configurarse a través de muchos recursos de una forma coordinada que proporcione *servicios* de un extremo a otro en una red. Para proporcionar servicios útiles, son necesarios tanto los mecanismos de control de tráfico como los mecanismos de provisión y configuración.

3.6.2.1 TECNOLOGÍAS DE QoS EN REDES IP

Las aplicaciones, la topología de la red y la política de QoS dictan qué tipo de QoS es más apropiado para un flujo individual o para varios. Para conseguir los diferentes tipos de QoS existen diversos protocolos y algoritmos.

RSVP (RESOURCE RESERVATION PROTOCOL, PROTOCOLO DE RESERVACION DE RECURSOS).

El Protocolo de Reserva es un protocolo de señalización que proporciona un control para la reserva y para habilitar los servicios integrados[23], estando orientado a redes IP. La reserva de recursos se realiza en los enrutadores intermedios situados a lo largo de toda la ruta de datos de la aplicación. Es, hasta el momento, la más compleja de todas las tecnologías de QoS para las aplicaciones (hosts) y para los distintos elementos de la red (enrutadores y puentes).

RSVP, define un modelo de asignación de QoS en el que cada receptor (para una sesión) fuese responsable de elegir su propio nivel de reserva de recursos, iniciando la reserva y manteniéndola activa tanto tiempo como desee. Consistiendo, pues, en una solución distribuida que permite a múltiples receptores heterogéneos efectuar reservas específicamente dimensionadas según sus propias necesidades. Además, para mantener el control el receptor puede enviar sus especificaciones a la fuente encargada de solicitar las reservas de la red. En definitiva, RSVP permite que las aplicaciones soliciten una calidad de servicio específica a la red. Su tarea consiste en establecer y mantener las reservas de recursos en un árbol de distribución, con independencia de cómo se hayan creado.

Diffserv (DIFFERENTIATED SERVICES, SERVICIOS DIFERENCIADOS)

Diffserv un protocolo de QoS propuesto por IETF que, permite especificar diferentes clases de servicio marcando los paquetes. Permite a los proveedores de servicios Internet y a usuarios de grandes redes IP corporativas desplegar rápidamente diferentes niveles QoS en la dorsal. Consiste en un método para marcar o etiquetar paquetes, permitiendo a los enrutadores modificar su comportamiento de envío. Cada tipo de etiqueta representa un determinado tipo de QoS y el tráfico con la misma etiqueta se trata de la misma forma.
Para proporcionar los diferentes niveles de servicio utiliza el campo *type of service* (TOS) o *Diffserv Codepoint* (DSCP) de la cabecera del estándar Ipv4 e Ipv6, este campo es llamado diffserv codepoint (DSCP). Los host o los enrutadores que envían tráfico a una red diffserv marcan cada paquete transmitido con el valor DSCP. Los enrutadores de una red diffserv utilizan DSCP para clasificar paquetes y para aplicar un comportamiento de cola específico basado en los resultados de la clasificación. El tráfico de varios flujos con requisitos de QoS parecidos se marca con el mismo DSCP, al agregar el flujo a una cola común o al programar el comportamiento.

[23] *Intserv es una estructura para definir servicios. Como tal, incluye un conjunto de mecanismos de control de tráfico subyacentes. Los servicios Intserv se suelen aplicar por conversación individual. Normalmente, aunque no de forma necesaria, Intserv se asocia con el protocolo de señalización RSVP.*

MPLS (MULTIPROTOCOL LABEL SWHITCHING).

El Multi-Protocol Label Switching (MPLS) es un protocolo propuesto por IETF que usa en esquema de etiquetado del tráfico hacia delante: el tráfico es marcado en su entrada a la red pero no en los puntos de salida. En el modelo de capas de OSI, MPLS se situaría entre la capa 2 (enlace) y la capa 3 (red).
MPLS reside únicamente en los enrutadores y es independiente del protocolo utilizado (de ahí lo de "multi-protocol"), lo que permite que pueda ser utilizado sobre otros protocolos distintos a IP, como IPX, ATME, PPP, Ethernet, Frame Relay, sobre SONET y Token ring.

Esta tecnología combina algunas de las prestaciones de las redes orientadas a la conexión con las de las redes sin conexión. Permite a un enrutador o a un conmutador asignar una etiqueta a cada una de las entradas de la tabla de enrutamiento y comunicar esa etiqueta a los enrutadores y conmutadores vecinos. Cuando uno de estos dispositivos pasa un paquete al más próximo, el enrutador o el conmutador añade a ese paquete una etiqueta asociada con la entrada de tabla de enrutamiento. La etiqueta permite al enrutador o conmutador identificar el próximo salto o saltos sin mirar la dirección. La idea es, por tanto, posibilitar que los paquetes etiquetados fluyan de extremo a extremo sin forzar a los enrutadores o conmutadores a mirar las direcciones.

Los mecanismos de QoS proporcionan un conjunto de herramientas que el administrador de redes puede utilizar para administrar el uso de recursos de red de una forma controlada y eficaz. Como resultado, se obtendrá un servicio mejor a las aplicaciones y a usuarios de misiones críticas, al mismo tiempo que se va frenando el ritmo al que es necesario aumentar la capacidad. En resumen, QoS ayuda a mejorar el servicio a los usuarios de la red, al mismo tiempo que reduce los costos de ofrecer dichos servicios.

4. VOZ SOBRE IP

4 VOZ SOBRE IP

Tradicionalmente, las comunicaciones de voz siempre se habían realizado por circuitos conmutados; en otras palabras, a través de canales temporales que se abren para transportar la llamada en cuestión y se reservan para uso exclusivo. Sin embargo, esta forma de comunicación tiene sus pros y contras: en primer término, está la alta calidad y confiabilidad que la tecnología ha alcanzado; por el otro, la ineficiencia en cuanto al aprovechamiento de los canales. En otras palabras, se desaprovecha la capacidad del sistema.

La contraparte a la forma de transmitir descrita anteriormente es la conmutación de paquetes. Comúnmente empleada para las comunicaciones de datos, esta propuesta tecnológica se caracteriza por usar medios compartidos. Los canales no se reservan para una sesión, al contrario: los paquetes que componen la información de todos los usuarios viajan intercalados entre sí, sobre un mismo canal. Algunas ventajas son la eficiencia (se aprovechan más los canales), así como el costo; recuérdese que la industria de los datos se ha desarrollado principalmente sobre estándares abiertos, lo cual equivale a menores precios. En cuanto a las desventajas, existe una principal: las redes de datos aún presentan ineficiencias para comunicaciones de voz, sobre todo en cuestión de retardo (paquetes que no llegan a tiempo) y caídas (las redes de datos suelen fallar). Asimismo, hay que recordar que los usuarios están acostumbrados a usar sus teléfonos sin contratiempo alguno [19][20].

Pese a todo, la tendencia actual es que el tráfico de voz se mude hacia las redes de datos. Los problemas técnicos descritos, paulatinamente se irán resolviendo al grado de que muchas empresas aprovecharán las ventajas que ofrece la voz sobre redes de datos en la actualidad [37].

En este capítulo se estudiarán las principales características de la tecnología VoIP. Iniciando con un estudio de la voz en paquetes, las técnicas empleadas para paquetizarla, posteriormente se hablará de los diferentes codificadores de voz para VoIP. Parte importante y fundamental de la tecnología VoIP son los estándares involucrados, los cuales serán revisados en la sección tres de este capítulo. Posteriormente se hablará del concepto de calidad de voz, es decir las cuestiones que deben tenerse en cuenta para poder ofrecer un servicio de voz aceptable a través de una red de paquetes. Finalmente se hablará del aspecto seguridad el cual debe ser tomado en cuanta en la implementación de la tecnología VoIP.

4.1 VOZ EN PAQUETES.

Las expectativas en las telecomunicaciones son la integración de servicios de voz y datos en una sola unidad fundamental llamada paquete. El tratamiento de los datos paquetizados ha sido ampliamente estudiado y desarrollado en las redes locales de datos. Por su parte, la voz requiere de un tratamiento especial, tal que le permita el tratamiento adecuado en ancho de banda para su manejo en paquetes por lo que, se recomienda utilizar técnicas adecuadas de compresión y codificación de voz.

La comunicación de voz ha sido históricamente manejada por redes analógicas con conmutación de circuitos tales como la Red Pública Telefónica Sin embargo, la conmutación de paquetes resulta atractiva tanto para voz como para datos, por un cierto número de razones, entre las cuales cabe mencionar, la maduración de la

tecnología de conmutación de paquetes como una tecnología promisoria de gran alcance para la integración de servicios.

Más aún la conmutación de paquetes ofrece muchas ventajas potenciales en términos de respuestas. Una ventaja es la utilización eficiente de la capacidad del canal, particularmente para el tráfico a ráfagas. Aunque no es tan a ráfagas como un dato interactivo, la voz muestra algunas ráfagas en la forma de talk-spurts (paquetes, estallidos, talk-spurts:arreglo de señales de voz ya paquetizados). La duración promedio de éstos estallidos (talk-spurts) depende de la sensibilidad del detector de voz, pero sí es bien conocido que los parlantes individuales están activos solamente entre el 35-45% en una típica conversación telefónica. Al enviar los paquetes de voz solamente durante tales estallidos, la conmutación de paquetes ofrece una manera natural para multicanalizar las llamadas de voz también como con voz y datos [7].

Sin embargo, la paquetización de voz no está exenta de dificultades. La voz continua de calidad aceptable debe ser reconstruida desde paquetes de voz que experimenten retardos variables a través de la red. El proceso de reconstrucción envuelve compensación para los componentes de retardo variable por imponer un retardo adicional. De aquí, que los paquetes deben ser enviados con un bajo promedio de retardo y una baja variabilidad en el retardo.

La etapa de paquetización para el caso de la señal de voz, requiere de un esquema de codificación/compresión que proporcione ciertas características específicas para su aplicación, la cuales se muestran en la figura 4.1.

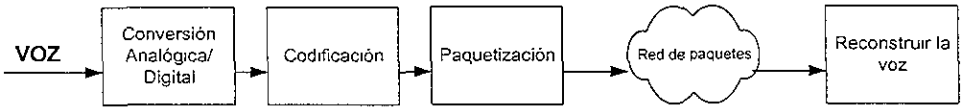

FIG 4.1 Etapas de procesamiento para el transporte de la voz en modo paquete.

4.1.1 CONVERSION ANALOGICA/DIGITAL

El proceso de conversión de la forma análoga a la forma digital está compuesto de tres conceptos lógicos básicos: el muestreo, la cuantización y la codificación [38].

El muestreo es el proceso de tomar medidas instantáneas de una señal análoga cambiante en el tiempo, tal como la amplitud de una forma de onda compleja. La información muestreada permite reconstituir más o menos una representación de la forma de onda original. Sin embargo, si las muestras son relativamente escasas (o infrecuentes), la información entre las muestras se perderá. El teorema de muestreo establece que es posible capturar toda la información de la forma de onda si se utiliza una frecuencia de muestreo del doble de la frecuencia más elevada contenida en la forma de onda. En los sistemas telefónicos la velocidad de muestreo ha sido establecida a 8000 muestras por segundo.

Una vez que la muestra y su valor han sido obtenidos, la cuantización es el siguiente proceso para la reducción de la señal análoga compleja; ésta permite aproximar la muestra a uno de los niveles de una escala

designada. Hay que notar que el proceso de cuantización puede introducir un ruido de cuantización; una diferencia entre el valor original de la amplitud muestreada y el valor aproximado correspondiente a la escala seleccionada, donde la magnitud de este error estará determinada por la fineza de la escala empleada.

El siguiente proceso se refiere a la codificación la cual será tratado ampliamente en la siguiente sección.

4.1.2 CODIFICACION/COMPRESION DE VOZ

El objetivo de la mayoría de las técnicas de codificación, ha sido reducir significativamente la velocidad de transmisión manteniendo la calidad y robustez de la misma, para optimizar el ancho de banda disponible.

Generalmente este objetivo se ha convertido en un compromiso entre estos dos factores. Las técnicas que alcanzan las menores tasas de transmisión, regularmente reducen la calidad de voz, tienden a ser altamente sensibles al ruido y representan retardos de codificación elevados.

Para el estudio de los nuevos esquemas de digitalización y compresión de voz es importante hacer una clasificación que enfatice la diferencia entre los esquemas que requieren de la sintetización de la voz humana y aquellos que directamente procesan la voz humana como señal de entrada del circuito de procesamiento [7]. Bajo estas consideraciones, los esquemas para la digitalización y la compresión de voz se pueden clasificar en tres categorías principales [4]:

- Codificación de forma de onda.
- Codificación de fuente.
- Codificación híbrida.

Las técnicas de codificación de forma de onda, son técnicas que pretenden imitar la forma de onda de la voz de la mejor manera posible mediante la transmisión en tiempo real de una muestra específica de magnitud.

Las técnicas de codificación fuente analizan la forma de onda original de la voz, para extraer de ésta parámetros perceptualmente importantes para el oído humano. La voz es reconstruida en el extremo receptor basándose en los parámetros transmitidos.

Finalmente, tenemos las técnicas de codificación híbrida, este tipo de técnicas se basan en la combinación de las dos técnicas descritas anteriormente.

La voz reproducida por las tres categorías anteriores puede ser clasificada genéricamente dentro de las siguientes clases:

- **Calidad comercial telefónica (toll quality):** calidad de voz similar a la empleada en los enlaces telefónicos comerciales. Calidad alta y gran naturalidad de voz.
- **Calidad de comunicación (communication quality):** calidad aceptable para aplicaciones de tipo militar, no profesionales y en ambiente móvil. Calidad buena pero con pérdidas en la naturalidad de la voz humana.

- **Calidad sintética (sinthetic quality):** calidad de voz generada artificialmente y de tipo computarizada. Carece de la naturalidad de la voz humana.

En la tabla 4.1 se resumen las características de los esquemas de codificación mencionados con anterioridad.

TABLA 4.1 Esquemas de codificación para voz.

Esquema	**Tipo**	**Velocidad de codificación**
Codificación de forma de onda	PCM	64 Kbps
	ADPCM	32 Kbps
	CVSD	12-32 Kbps
Codificación de fuente	LPC	2.4 – 4.8 Kbps
Codificación híbrida	**Dominio del Tiempo**	
	RELP	
	APC	4.8-16 Kbps
	Multipulse Coding	
	CELP	
	Dominio de la Frecuencia	8-24 kbps
	ATC	
	SBC	

PCM- Pulse Code Modulation
ADPCM- Adaptive Differential PCM
CVSD- Continuos Variable Slope Delta Modulation
LPC-Linear Predictive Coding
RELP- Residual Excited Linear Prediction
APC- Adaptive Predicting Coding
CELP- Code Excited Linear Prediction
ATC- Adaptive Transfer Coding
SBC – Subband Coding

4.1.2.1 CODIGOS DE FORMA DE ONDA [7]

PCM (PULSE CODE MODULATION)
Emplea una velocidad de digitalización de 64 Kbps. En un principio utilizaba un esquema de digitalización que asignaba códigos digitales a cada muestra de señales de voz para representar la amplitud de la señal (requerían muchos bits de resolución por muestra). De acuerdo a la forma de onda de la voz existen partes de la señal de voz con bajos niveles de energía y otras partes con altos niveles de energía. Por lo anterior se colocaron más bits de resolución a volúmenes bajos y pequeños de sonido, para así compensar y representar más adecuadamente de manera digital la complejidad de la forma de onda de la señal. Esta técnica de codificación tiene un nivel de calidad de 4, en la escala de 0 a 5 (Mean Option Score, MOS).

ADPCM (ADAPTIVE DIFFERENTIAL PCM).
Emplea una velocidad de digitalización de 32 Kbps. Esta técnica en lugar de tratar de disminuir el ancho de banda modelado de la voz humana, lo que hace es procesar y codificar la diferencia de las muestras como opuestas a la amplitud de las muestras mismas. El factor de calidad de la voz con ADPCM es de 4.2.

El inconveniente de esta técnica es que el esquema de 32Kbps no puede ser soportado por todos los módems analógicos de datos.

CVSD(CONTINUOS VARIABLE SLOPE DELTA MODULATION).
Esta técnica ha sido empleada con mucho éxito en Comunicaciones vía satélite y Radio Terrestres. Emplea velocidades de digitalización tan bajas como 12 y 16 Kbps. Tiene un nivel muy adecuado de calidad y de reconocimiento de voz.

Este esquema de codificación es sumamente económico de implementar, ya que se basa en una aproximación analógica, la cual se puede llevar a un solo circuito integrado.

4.1.1.2 CODIGOS DE FUENTE

El más conocido de estos códigos es el LPC en el cual se reduce drásticamente la velocidad de digitalización.

LPC (LINEAR PREDICTIVE CODING).
La técnica de codificación LPC produce voz ultra-comprimida con velocidades de datos de cientos a algunos miles de bits por segundo, para lo cual este esquema de codificación se basa en un conocimiento del proceso de generación de voz. El proceso es modelado por dos tipos de generadores de sonidos y por un filtro digital variante en el tiempo. Los generadores representan ya sea sonidos de voz (tales como vocales) con ciertas propiedades de tono, o sonidos de otro tipo (tales como el sonido de la mayoría de las consonantes) las cuales son mejor caracterizados por una fuente de ruido aleatoria.

En esta técnica de compresión de voz la señal de audio es descompuesta en bloques de tiempo (tramas), transmitiendo la fuente en cada trama un conjunto de parámetros al destino. Estos parámetros contienen la información necesaria concerniente al modelo del filtro digital, la decisión así como las

características de sí el sonido enviado corresponde o no a señales de voz. No obstante que este tipo de códigos desarrolla señales de voz a muy bajas velocidades, su principal desventaja es su baja calidad de la voz (2.9 en la escala de 5). Además de lo anterior LPC no es apropiada para aquellos sonidos que no sean de naturaleza humana, o bien de cierta naturaleza de complejidad (por ejemplo: múltiples personas hablando simultáneamente).

4.1.1.2 CODIGOS HIBRIDOS.

Los nuevos esquemas de codificación que son en general de características híbridas, usan como su nombre lo indica propiedades de la codificación fuente y la codificación de forma de onda, tomando las mejores características de los dos esquemas de codificación anteriores.

Los modelos de los esquemas híbridos de codificación de voz son usados para quitar la redundancia de la forma de onda del habla y producir una señal que puede ser codificada más eficientemente que la señal de voz misma de entrada. Estos modelos se clasifican en códigos híbridos en el dominio del tiempo y códigos híbridos en el dominio de la frecuencia.

4.1.1.2.1 CODIGOS HIBRIDOS EN EL DOMINIO DEL TIEMPO

Los códigos híbridos en el dominio del tiempo efectúan sus operaciones de procesamiento en muestras en el tiempo real de las señales de voz. Al igual que en los otros códigos emplean un modelo para el mecanismo de producción de la voz pero con una notable diferencia. Estos modelos son utilizados para remover la redundancia de la forma de onda de la señal de voz, y así producir una señal que puede ser codificada mucho más eficientemente que la misma señal de entrada original.

RELP (RESIDUAL EXCITED LINEAR PREDICTION).

Esta técnica utiliza una predicción lineal para modelar el comportamiento de la voz como un filtro variante con el tiempo, el cual es utilizado para filtrar inversamente la señal de voz de entrada. La señal remanente o residual filtrada fuertemente pasa bajos (0-8000 Hz) puede por lo tanto ser codificada, transmitida y después utilizada en el receptor para reconstruir las frecuencias remanentes. Este proceso introduce una degradación para ciertos sonidos y ciertos tonos de voz (especialmente aquellos con componentes de altas frecuencias).

APC (ADAPTIVE PREDICTING CODING).

Esta técnica lleva a cabo un cierto número de operaciones de procesamiento en el dominio del tiempo en el residuo, para de esta manera reducir la información contenida en la señal que va a ser codificada y transmitida.

MULTIPULSO.

Tanto la técnica de multipulso como APC utilizan algoritmos que lograr formar una representación compacta de la técnica residual de producción lineal. Esta técnica es caracterizada por un conjunto de pulsos no uniformemente esparcidos en tiempo y de diferentes tamaños.

CELP (CODE EXCITED LINERAR PREDICTION).

Es una nueva familia de códigos híbridos en el dominio del tiempo que ha tenido una fuerte aceptación y desarrollo en los tres últimos años. Estas técnicas de codificación producen una muy buena calidad de sonido a velocidades de datos de 4.8 a 8 Kbps. Sin embargo resulta ser por un lado muy compleja en su implementación y por otro lado, no es transparente a señales no de voz. La mayor área de aplicación de esta técnica es en la Telefonía Digital Celular.

La diferencia fundamental de la tecnología CELP con los otros esquemas híbridos se da en dos aspectos: PRIMERO, en lugar de excitar el modelo del comportamiento de la voz con muestras individuales o bien con simples generadores, CELP lo que emplea son vectores integrales (completos) de muestras almacenadas escogidas de un LIBRO DE CODIGOS.

SEGUNDO, CELP emplea una técnica conocida como Análisis por Síntesis para seleccionar el vector tomándolo de manera aleatoria del libro de códigos, empleándolo después para generar una señal sintética de voz que va a ser comparada a la salida con la señal original de entrada. Para llevar a cabo lo anterior, es necesario efectuar una búsqueda exhaustiva por todos los posibles vectores para encontrar aquél que produce la más cercana aproximación con la forma de onda de la señal de voz. Todo este procedimiento requiere de un procesador extremadamente complejo y costoso.

4.1.1.2.2 CODIGOS HÍBRIDOS EN EL DOMINIO DE LA FRECUENCIA

ATC (ADAPTIVE TRANSFER CODING).

Su principio se basa en la propiedad de que la voz producida por un parlante puede variar fuertemente en su contenido espectral, presentándose regiones de energía con bajas y altas componentes de frecuencia, dividiéndose estas regiones en señales correspondientes a voz (bajas frecuencias), y a cualquier otro tipo de sonido (altas frecuencias).

El algoritmo ATC está diseñado para asignar el mayor ancho de banda de transmisión a aquellos componentes que mayor representatividad presentan en el espectro de la señal (Asignación Ponderada del Ancho de Banda). El resultado anterior da lugar a una excelente fidelidad para señales tanto de bajas como de altas frecuencias, así como con señales de sonido no de voz limitadas en su contenido espectral.

SBC (SUBBAND CODING).

En conjunto con la técnica TDHS (Time Domain Harmonic Scaling) emplea el hecho de que ciertas regiones del espectro de voz contienen más energía que otras, dividiendo el espectro en varias bandas no traslapadas, las cuales son codificadas de manera independiente utilizando técnicas en el dominio del tiempo.

4.1.3 PAQUETIZACIÓN DE LA VOZ

Para cursar tráfico de voz a través de redes de paquetes, p.e. Internet, se requiere la "paquetización" de las muestras de voz previamente digitalizadas, por cuanto son los paquetes las unidades de datos que se transportan por la red IP. También, y dada las limitaciones de recursos de ésta, es necesario reducir el

consumo de ancho de banda mediante compresión de datos. En el extremo de destino se realizan estas funciones a la inversa.

Generalmente hablando, los protocolos de red desarrollados para conmutación de paquetes de datos no son apropiados para la voz debido a las diferentes naturalezas de la voz y los datos. A diferencia de los datos, la naturaleza de la voz es subjetiva y conversacional. La voz puede tolerar una cierta cantidad de distorsión (por ejemplo: compresión, recortes –amplitud, frecuencia-) pero es sensitiva al retardo de transmisor a receptor. Aunque la cantidad exacta del máximo retardo tolerable está sujeto a debate, es generalmente aceptado que esté entre los límites aproximados de 100-600 ms. (La Red Telefónica Pública, por ejemplo, tiene una especificación máxima de 600 ms).

A fin de minimizar los retardos por paquetización y almacenamiento, se ha propuesto que los paquetes de voz deban ser relativamente cortos, del orden de 200-700 bits, y generalmente contienen menos de 10-50 mseg. Los protocolos de red deben ser simplificados para acortar los encabezados de los paquetes de voz (por ejemplo: en el orden de 4-6 octetos), aunque se necesitan contadores de tiempo y número de secuencia [7].

4.2 CODIFICADORES DE VOZ PARA VoIP.

El proceso de codificación–decodificación, explicado anteriormente, introduce demora, que se suma a la demora que añade la red. Esta demora, no admisible por encima de cierto valor, es un serio impedimento al que se ve sometido el tráfico con requerimientos de tiempo real al ser cursado por redes de datagramas, como el caso de la voz.

Así, es conveniente una baja velocidad resultante de la codificación, por las implicaciones que tiene en el ancho de banda y en la compartición de recursos, pero esto se traduce en mayor complejidad de implementación de los codificadores de voz y una mayor demora en el desarrollo de su tarea, a lo que se adiciona inferior calidad en la reproducción de la voz.

Por otra parte, la combinación de otros medios con la voz sugiere tener en cuenta los "silencios" de la conversación, lo que en principio posibilita una mejor explotación del ancho de banda, así es común el empleo de "algoritmos de compresión del silencio" en la codificación de voz. Esto a su vez requiere la utilización de algoritmos de detección de la actividad de voz (VAD) y algoritmos de generación de ruido de confort (CNG), posibilitándose así que la señal de voz codificada resultante se transmita con una velocidad no uniforme en función del nivel de actividad que presente la fuente generadora.

El mecanismo de compresión del silencio es crítico en las prestaciones de la codificación de voz, ya que una implementación inadecuada conlleva a un deterioro significativo de la inteligibilidad de la voz.

En línea con las limitaciones propias de las redes de datagramas para cursar tráfico con requerimientos de tiempo real, se ha hecho necesario el desarrollo de normas, o recomendaciones, que permitan enfrentar satisfactoriamente este problema [39]. En tal sentido ITU (International

Telecommunications Union, Unión Internacional de Telecomunicaciones) ha publicado tres normas de codificación: G.723.1, G.729 y G.729A:

- **G.723.1 :** establece un vocoder[1] para comunicaciones multimedia a 6,4 Kbps y 5,3 Kbps, con una demora de codificación de 37,5 mseg. G.723.1 requiere un índice de transmisión muy bajo ofreciendo una calidad de audio cercana a la tarificada. G.723.1 ha sido seleccionada por el VoIP Forum como el codec básico para aplicaciones de telefonía IP de bajo índice de bits.
- **G.729** : establece un vocoder a 8 kbps con una demora de codificación de 15 mseg. Originalmente pensada para entornos inalámbricos, pero es aplicable a entornos IP y comunicaciones multimedia. Presenta nivel de complejidad mayor que G.723.1
- **G.729A :** es una versión, versión A, de G.729, con menor grado de complejidad y prestaciones que ésta, diseñado para integración de voz y datos. La codificación se hace a una velocidad de 8 kbps con una demora de 15 mseg. Presenta menos requerimientos que G.729 en cuanto a capacidad de procesamiento y de almacenamiento.

Estas tres recomendaciones presentan, hasta ahora, las mejores características de cara a la Telefonía IP o VoIP, pues sus requerimientos de ancho de banda son considerablemente más modestos que los establecidos por otras normas anteriores, desde la "vieja" recomendación G.711 (1965) a 64 Kbps utilizada en los sistemas PCM, hasta la G.728 a 16 Kbps. En los tres casos la calidad de voz se cataloga de buena. En la tabla 4.2 se muestran las principales características de los codificadores mencionados.

TABLA 4.2. Principales características de los codificadores de voz para VoIP.

Designación ITU	Ancho de Banda de Audio	Velocidad de Transmisión	Algoritmo de Compresión	Comentarios
G.711	3.4 KHz	56K, 64Kbps	PCM	Compresión simple de amplitud; Ampliamente extendido en PSTN
G.728	3.4 KHz	16Kbps	LD-CELP	Misma calidad que G.711; Videoconferencia de bajo índice
G.723.1	3.4 KHz	48K, 56K, 64Kbps	LP-MLQ	Cercano a la calidad tarificada; Codec básico del VoIP Forum
G.729 and G.729A	3.4 Khz.	8Kbps	CS-ACELP	Baja latencia[2] y ligeramente mejor calidad que G.723.1; Aplicaciones más nuevas de telefonía IP

[1] *El termino VOCODER significa Codificador de Voz*

[2] *La latencia es el tiempo requerido para que una señal atraviese la red, es decir la suma de retardos ocasionados por el paso de los paquetes por los diferentes nodos que pertenecen a su trayectoria*

4.3 SEÑALIZACION PARA VoIP.

Llegados a este punto, conviene aclarar que es la señalización. Entendemos por señalización el conjunto de información que debe ser intercambiado entre los diferentes elementos de una red de telecomunicaciones para establecer, supervisar, mantener y liberar una conexión.

Existen dos protocolos estándar para la señalización VoIP: el marco H.323 definido por la ITU-T y el SIP (Session Initiation Protocolo, Protocolo de Inicio de Sesión) de la IETF (Internet Engineering Task Force, Fuerza de trabajo de Ingeniería de Internet).

Debido a la gran aceptación e importancia que actualmente tiene el estándar H.323, éste será estudiado con mayor profundidad, en la parte final de esta sección donde se hablará del estándar SIP.

4.3.1. El ESTANDAR H.323

El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes de área local (LAN). H.323 está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Por ejemplo TCP/IP sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol). El estándar incluye dispositivos punto a punto y punto-multipunto. H.323 controla el direccionamiento de llamadas, gestiona los servicios multimedia y el ancho de banda así como las interfaces entre redes LAN y otras redes.

4.3.1.1. LA ARQUITECTURA H.323

H.323 define cuatro componentes principales de un sistema de comunicación basada en H.323: Terminales, Gateways, Gatekeepers y Unidades de Control Multipunto(MCU, Multipoint Control Unit). Los cuales se representan en la figura 4.2.

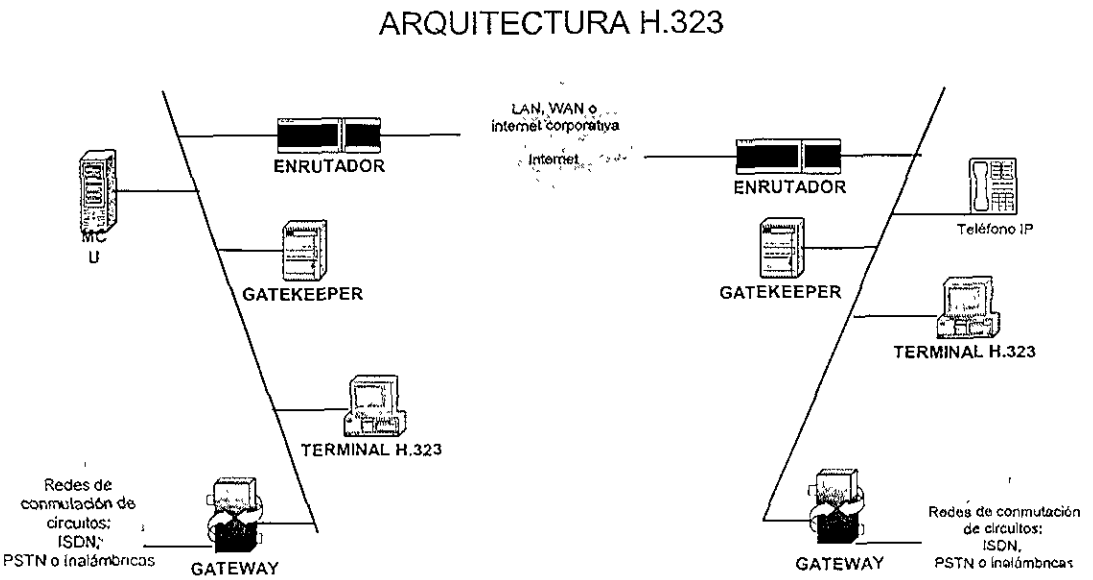

FIG 4.2 Arquitectura H.323

TERMINALES

Las *terminales* H.323 son los puntos finales en una LAN, proporciona comunicación bidireccional en tiempo real con otra terminal H.323, gateway o MCU. Esta comunicación consta de señales de control, indicaciones, audio, video y/o datos entre las dos terminales. El funcionamiento de toda *terminal* debe incluir el tratamiento necesario de la señal para su envío por la red de datos. Deben realizar la captación, digitalización, y compresión de la señal de forma que la carga a soportar por toda comunicación este repartida entre las diversas terminales. Conforme a la especificación, una terminal debe permitir comunicaciones de voz; la compatibilidad con datos y vídeo es opcional

Todas las *terminales* deben soportar la recomendación H.245 que especifica los protocolos de control para comunicaciones multimedia, mensajes para la apertura y cierre de canales para el flujo de la información (voz, vídeo o datos). Los otros tres componentes que se requieren son: el Q.931 (para el establecimiento de la llamada), RAS(para registro y control con el gatekeeper) y soporte para RTP y RTCP. Todos estas especificaciones serán explicadas más adelante. Los componentes opcionales en las terminales H.323 son el codec de video, la sección T.120 para intercambio de datos y las capacidades para el MCU. Los cuales se representan en la figura 4.3 [12].

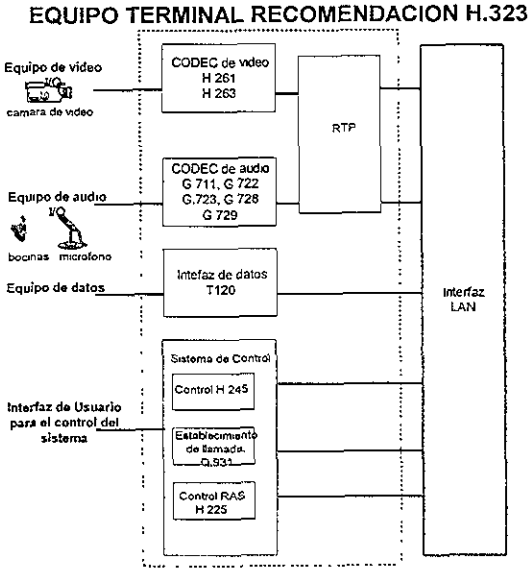

FIG 4.3 Estructura de las terminales de la especificación H.323

GATEWAY

Es un elemento opcional en una conferencia H.323. Proporciona comunicación bidireccional en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red de conmutación de circuitos (SCN, Switched Circuit Network). En general el propósito del gateway es reflejar transparentemente las características de los formatos de transmisión y los procedimientos de comunicación. de un extremo en la red IP a otro en una red de conmutación de circuitos(PSTN o ISDN) y viceversa.

En el lado H.323, el *gateway* utiliza el protocolo de señalización H.245 para intercambiar las capacidades, el protocolo H.225 para establecer y liberar las llamadas y el protocolo RAS para su registro en el gatekeeper. Del lado de la SCN, el *gateway* utiliza los protocolos específicos de la red (por ejemplo protocolos de ISDN y SS7).

Las terminales se comunican con el *gateway* usando el protocolo de señalización y control H.245 y el protocolo de señalización de llamada H.225. El *gateway* traduce estos protocolos a sus respectivas contrapartes en una red diferente a la H.323 y viceversa. La traducción entre los formatos de audio, video y datos pueden ser realizadas también por el *gateway*.

Los *gateways* no son necesarios si no se requieren conexiones a otras redes ya que los endpoints[3] pueden comunicarse directamente con otros endpoints que se encuentren dentro de la misma LAN.

GATEKEEPER

El *gatekeeper* Es el componente más importante dentro de un sistema H.323. El estándar H.323 esta implementado en las redes en secciones llamadas *zonas*. Las *zonas* son el conjunto de endpoints sobre los cuales un gatekeeper tiene jurisdicción. Los endpoints puenden ser terminales, gateways o MCUs; cualquier combinación de estas entidades puede ser registrada por el *gatekeeper*. Sin importar la localización física del código del *gatekeeper*, solamente debe haber uno activo por zona.

El *gatekeeper* es el punto central que ofrece los servicios de logística dentro del sistema H.323. Puede ser controlado y configurado en forma remota por alguna aplicación usando el protocolo HTTP (Hyper Text Transfer Protocol, Protocolo de Transferencia de Hipertexto) o el protocolo SNMP(Simple Network Management Protocol, Protocolo Sencillo de Administración de Redes).

Las funciones obligatorias, especificadas por el estándar H.323, que debe desempeñar un *gatekeeper* son las siguientes

- Traducción de direcciones
- Control de admisiones
- Administración del ancho de banda
- Administración de la zona

FUNCIONES OBLIGATORIAS DE LOS GATEKEEPERS.

TRADUCCION DE DIRECCIONES

El gatekeeper proporciona la resolución de direcciones entre el alias LAN y la dirección IP cuando el endpoint solicita el servicio. Típicamente los usuarios no saben las direcciones IP de las terminales a las que desean llamar y es tarea del gatekeeper interpretar las direcciones alias (identificadores H.323, URL, número telefónico o dirección de correo electrónico) en direcciones IP.

[3] *En la arquitectura H.323 el termino endpoint se refiere a los equipos terminales, gateways o MCU's (Unidades de control multipunto)*

CONTROL DE ADMISIONES

El gatekeeper puede controlar la admisión de los endpoints que deseen ingresar a la zona H.323, la cual se realiza utilizando los siguientes mensajes RAS:

- Solicitud de admisión, ARQ(Admission Request).
- Confirmación de admisión, ACF (Admission Confirm Message).
- Rechazo de Admisión, ARJ (Admission Reject Message).

Los criterios para admitir nuevos endpoints pueden ser diferentes como por ejemplo: ancho de banda disponible, autorización, etc.

CONTROL DEL ANCHO DE BANDA

El ancho de banda de la red puede ser monitoreado y controlado por el gatekeeper para asegurar que el tráfico de audio y/o vídeo no exceda el umbral permitido para establecer una adecuada eficiencia de las aplicaciones críticas de la red. El gatekeeper puede rechazar nuevas conexiones cuando se han alcanzado los límites establecidos por el administrador. Los mensajes de RAS utilizados para el control del ancho de banda son:

- Solicitud del ancho de banda, BRQ(Bandwidht Request Message)
- Confirmación del ancho de banda, BCF(Bandwidht Confirm Message)
- Rechazo del ancho de banda, BRJ(Bandwidht Reject Message)

ADMINISTRACION DE LA ZONA

Todas las funciones arriba mencionadas son realizadas por el gatekeeper (traducción de direcciones, control de admisiones, control del ancho de banda) en todos los endpoints (terminales, gateways y MCUs) que se encuentren dentro de la zona de control correspondiente de éste.

Además de las funciones obligatorias mencionadas anteriormente, el gatekeeper puede desempeñar otras funciones opcionales, las cuales son:

- Enrutamiento del control de llamadas
- Autorización de llamada
- Autentificación de llamada
- Administración del ancho de banda
- Servicios de administración de llamadas
- Servicios suplementarios
- Directorio de servicios

FUNCIONES OPCIONALES QUE PUEDEN DESEMPEÑAR DE LOS GATEKEEPERS.

ENRUTAMIENTO DEL CONTROL DE LAS LLAMADAS.

Existen dos modelos para el enrutamiento de las llamadas: modo directo y modo enrutado. El gatekeeper realiza la traducción de direcciones y provee a los endpoints con la dirección de transporte para la señalización de llamada del canal destino.

En el modo directo, el gatekeeper proporciona a los endpoints la dirección de los endpoints destino. La comunicación en este caso se realiza directamente entre los endpoints sin la necesidad de que participe el gatekeeper.

En el modo enrutado el gatekeeper da a los endpoints su propia dirección como dirección destino. El gatekeeper recibe todos los mensajes y él mismo se encarga de enrutarlos al endpoint destino, es decir el gatekeeper realiza tareas de intermediario entre los endpoints que han establecido una comunicación. El modelo de enrutamiento permite una completa administración de las llamadas, por lo que es el modelo más utilizado para asegurar una entrega eficiente de los mensajes, y una adecuada implementación de los servicios adicionales.

AUTENTIFICACION DE LLAMADA.

El gatekeeper tiene la capacidad de realizar funciones de autentificación de llamada para identificar al usuario.

AUTORIZACION Y ACCESO DE LLAMADA.

El gatekeeper autoriza una llamada con base en los derechos de acceso de cada uno de los usuarios. Puede rechazar llamadas de terminales cuya autorización haya fallado. Las políticas de acceso las determina el administrador basado en los criterios de seguridad de la red.

ADMINISTRACION DEL ANCHO DE BANDA.

El gatekeeper puede controlar y limitar el número de terminales H.323 permitidas para usar la red simultáneamente. A través de la señalización H.225, se habilita al gatekeeper para limitar el ancho de banda de alguna llamada otorgándole menor del que fue requerido por la terminal así como también se pueden rechazar algunas llamadas si se determina que no hay suficiente ancho de banda disponible en la red como para soportar las llamadas.

SERVICIOS DE ADMINISTRACION DE LLAMADAS.

El gatekeeper puede llevar una lista de todas las llamadas H.323 entrantes similarmente a los registros de los PBX. Esta información es necesaria para indicar si alguna terminal esta ocupada y proporciona información para el control del ancho de bada.

SERVICIOS SUPLEMENTARIOS

Los servicios suplementarios para el estándar H.450 tales como la transferencia de llamada o llamada en espera son críticos en la funciones telefónicas de los usuarios de las empresas. Los usuario esperan que la red le proporcione estos servicios transparentemente. Tanto el gatekeeper como las terminales pueden encargarse de las actividades involucradas para llevar a cabo estas tareas, pero el gatekeeper puede cumplir las tareas más eficientemente por la complejidad de estas.

DIRECTORIO DE SERVICIOS.

La base de datos del gatekeeper contiene la información de los usuarios necesaria para implementar el directorio de servicios. El directorio de servicios es utilizado para la búsqueda de otros usuarios de la red. Estos directorios son actualizados y configurados con la información necesaria para establecer eficientemente las conexiones entre los usuarios.

Aunque originalmente el gatekeeper fue considerado por la ITU como un componente opcional dentro de la red H.323, el gatekeeper se ha convertido en una herramienta esencial de ayuda a las organizaciones para lograr aprovechar al máximo todas las ventajas que ofrecen las aplicaciones de VoIP. Finalmente hablaremos de las Unidades de Control Multipunto.

UNIDAD DE CONTROL MULTIPUNTO (MCU, MULTIPOINT CONTROL UNIT)

Una MCU es un extremo que proporciona la capacidad para que tres o más endpoints participen en una conferencia multipunto. Todas las terminales que participan en la conferencia establecen una conexión con la MCU.

Una MCU se forma de dos partes:

- Controlador multipunto, MC (Multi-point controller) que es obligatorio
- Procesador multipunto, MP (Multi-point processor) que es opcional.

En el caso más simple, un MCU puede estar formado por un MC únicamente.

EL CONTROLADOR MULTIPUNTO.

Realiza las negociación H.245 entre todas las terminales para determinar las capacidades comunes de proceso de audio y vídeo Puede controlar así mismo los recurso de la conferencia tales como el vídeo multicast. El MC no realiza mezcla ni conmutación de audio, vídeo o datos.

EL PROCESADOR MULTIPUNTO.

Mezcla , procesa y enruta las secuencias de audio, vídeo y/o datos entre los participantes en una conferencia multipunto. El MP puede procesar una única secuencia multimedia o varias simultáneamente, dependiente del tipo de conferencia soportada.

Las capacidades MC y MP pueden incorporarse en un dispositivo dedicado o ser parte de otros dispositivos H.323.

4.3.1.2. LA SUITE DE PROTOCOLOS H.323

La suite H.323 es un conjunto de programas de software, los cuales se guían por la recomendación ITU H.323 y todas las recomendaciones asociadas, ésta realiza las funciones necesarias para establecer y mantener una sesión de conferencias en tiempo real de audio, video y datos sobre redes IP de datos. Los protocolos más importantes y obligatorios en la suite H.323 son: *el protocolo RAS, el protocolo de señalización Q.931, el protocolo H.245, los protocolos RTP (Real Time Protocol, Protocolo de tiempo real), el RTCP (Real Time Control Protocol, Protocolo de Control de tiempo real y el estándar G.711 para codificación de voz*, los cuales serán estudiados en la siguiente sección [11][12][19]. En la figura 4.5 se representa la suite de protocolos H.323.

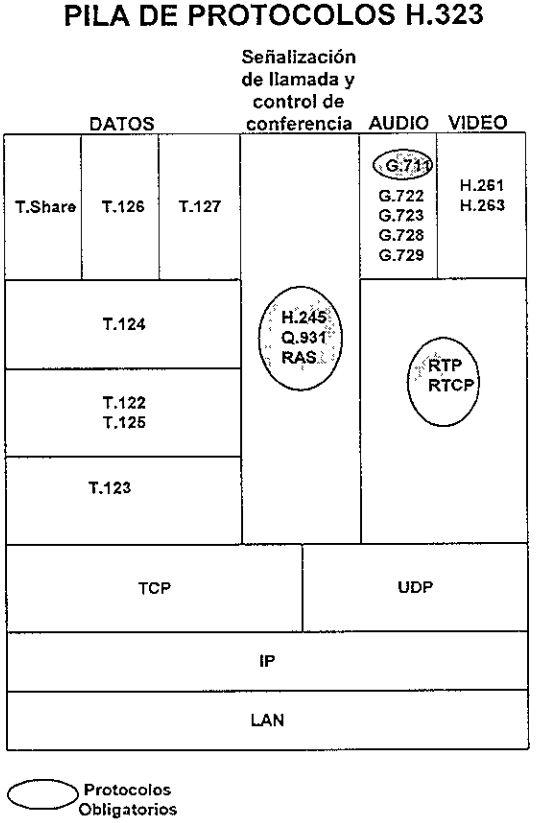

FIG 4.5 Suite de protocolos H.323.

4.3.1.2.1 RAS (REGISTRATION, ADMISSION, AND STATUS, REGISTRO, ADMISION Y ESTADO.

Es el protocolo de comunicación entre los endpoints (terminales, gateways y MCUs) y el gatekeeper. El RAS es usado para desempeñar las tareas de registro, control de admisiones, cambios en el ancho de banda, estado y liberación entre los endpoints y los gatekeepers. El intercambio de mensajes se realiza a través de los canales RAS. Este canal de señalización se abre entre los endpoints y el gatekeeper antes de establecer

cualquier otro canal. Los mensajes son transportados utilizando el protocolo confiable TCP. Finalmente es importante mencionar que la señalización RAS no es usada si no está presente el gatekeeper. La tabla 4.3 resume los mensajes RAS y sus funciones.

TABLA 4.3 Mensajes de señalización RAS.

Mensaje	Acrónimo	Función
Solicitud de registro	RRQ(Registration Request)	Solicitud de registro de una terminal o gateway al gatekeeper. El gateway puede confirmar (RCF, Registration Confirm Request) o rechazar la solicitud (RRJ, Registration Reject Message)
Solicitud de admisión	ARQ(Admission Request)	Solicitud de admisión a la red de paquetes por una terminal al gatekeeper. El gatekeeper puede confirmar (ACF, Admission Reject Message) o rechazar la solicitud (ARJ, Admisión Reject Message)
Solicitud de ancho de banda	BRQ(Bandwidth Request)	Solicitud para cambiar la asignación del ancho de banda por una terminal al gatekeeper. El gatekeeper puede confirmar (BCF, Bandwidth Confirm Message) o rechazar la solicitud (BRJ, Bandwidth Reject Message)
Solicitud de liberación	DRQ(Disengage Request)	Si la solicitad es hecha por el endpoint al gatekeeper, el mensaje informa al gatekeeper que el endpoint a abandonado la sesión; si el gatekeeper es quien hace la solicitud el mensaje obligará al endpoint a dejar la llamada. El gatekeeper puede confirmar (DCF, Disengage Confirm Message) o rechazar la solicitud (DRJ, Disengage Rejec Message).
Solicitud de información	IRQ(Info Request)	Solicitud de información de estado del gatekeeper a la terminal.
Respuesta a solicitud de información	IRR(Info Request Response)	Respuesta al mensaje IRQ. Puede ser enviada por la terminal al gatekeeper sin ser solicitada cada cierto tiempo.
Temporizadores y solicitudes RAS en progreso	RIP (RAS timers and Request in Progress)	Tiempos de espera predeterminados recomendados para la respuesta de los mensajes RAS y cuentas de reintento si la respuesta no es recibida.

4.3.1.2.2 Q.931.

Es utilizado en la señalización para el establecimiento de la llamada entre dos terminales. Los mensajes son transportados en paquetes TCP. La tabla 4.4 contiene la lista de los mensajes de señalización Q.931.

TABLA 4.4 Mensajes de señalización Q.931

Mensaje	Función
Alertamiento (Alerting)	Este mensaje es enviado por la terminal con la que se desea establecer la llamada para indicar al transmisor que el receptor a sido alertado de la llamada. "El teléfono esta sonando".
Procedimiento de llamada (Call Proceeding)	Este mensaje es enviado por la terminal con la que se desea establecer una llamada para indicar que el establecimiento de la llamada ha sido iniciado y ninguna otra solicitud de llamada será aceptada.
Conexión (Connect)	Este mensaje es enviado de la terminal con la que se desea establecer una llamada a la terminar que desea establecer la llamada para indicar la aceptación de la llamada.
Establecimiento de llamada (Setup)	Indica a la entidad H.323 llamada que otra entidad desea establecer una llamada con ella.
Consulta de estado (Status Inquiry)	Puede ser enviada por un endpoint o por el gatekeeper a otro endpoint para solicitar el estado de la llamada.
Estado (Status)	Respuesta a la solicitud de consulta del estado de la llamada

4.3.1.2.3. H.245.

El estándar H.245 especifica los protocolos de control para comunicaciones multimedia, mensajes para la apertura y cierre de canales lógicos para el flujo de los distintos medios, y otros comandos, peticiones e indicaciones. Tan pronto como se ha establecido la llamada por Q.931 las dos entidades intercambian la información de sus capacidades de terminal. El intercambio de las características de capacidad es una de las características fundamentales en la recomendación de la ITU y se lleva a cabo a través del canal H.245. Todos los mensajes H.245 son transportados utilizando el protocolo TCP. La tabla 4.5 contiene la lista de los mensajes de señalización H.245.

TABLA 4.5 Mensajes de señalización H.245.

Mensaje	Función
Determinación Maestro-Esclavo	Determina cual de las terminales funcionará como maestra y cual como esclava. Posibles contestaciones: confirmación, rechazo ó liberación (en caso de terminar el tiempo de temporización).
Establecimiento de las capacidades de la terminal	Contiene información referente a las capacidades de la terminal para transmitir y recibir los flujos multimedia. Posibles contestaciones: confirmación, rechazo ó liberación (en caso de terminar el tiempo de temporización).
Apertura del canal lógico	Abre un canal lógico par transportar la información audiovisual y de datos. Posibles contestaciones: confirmación o rechazo.
Cierre del canal lógico	Cierra el canal lógico que se ha establecido entre los endpoints. Posibles contestaciones: confirmación.
Modo de petición	Usado por la terminal receptora para realizar la petición de algún modo particular de transmisión a la terminal transmisora. En general los posibles modos de transmisión son: Modo video, Modo audio, Modo datos y Modo encriptado. Posibles contestaciones: confirmación, rechazo ó liberación (en caso de terminar el tiempo de temporización).
Envío de las capacidades de la terminal fijadas	Comandos para establecer las capacidades de las terminales transmisora y receptora. Se realiza enviando un conjunto de capacidades de terminal hasta que logran ponerse de acuerdo las terminales.
Comando de fin de sesión	Indica la finalización de una sesión H.245. Después de una transmisión, la terminal no enviará ningún otro mensaje H 245.

4.3.1.2.4. G.711.

Modulación por codificación de pulsos (PCM) de frecuencias vocales. Codec de Audio, con 3.1 Khz. de ancho de banda a 48,56 y 64 Kbps (telefonía convencional). (ver capítulo 4, sección 4.2. "CODIFICADORES DE VOZ PARA VoIP")

4.3.1.2.5 RTP (REAL TIME-PROTOCOL, PROTOCOLO DE TIEMPO REAL).

RTP (Real Time Protocol) es el estándar de Internet para transportar datos en tiempo real, tal como, audio y vídeo, sobre redes de paquetes. Proporciona funciones de transporte de fin a fin, para la transmisión de datos en tiempo real, sobre servicios *unicast* o *multicast,* donde la información es dirigida a varios destinos o a un solo destino.

El proceso de transporte incluye tomar el flujo de bits generados por el codificador, romper los flujos en paquetes y enviar los paquetes a través de la red para después realizar el proceso inverso del lado del receptor. El proceso es complejo ya que los paquetes pueden extraviarse, sufrir retardos variables y perder el orden en la red. RTP utiliza el protocolo UDP como protocolo de transporte para ofrecer una entrega oportuna de los datos. Para el monitoreo de la entrega de datos y para funciones de control usa el protocolo RTCP (Real Time Control Protocol, Protocolo de Control de Tiempo Real).

RTP incluye información sobre los orígenes del tráfico, por lo que se puede multiplexar en el camino, con marcas de tiempo específicas para cada medio transportado, el cual se utiliza para eliminar el jitter, esto es, la variación de los bits en el tiempo (adelantan y atrasan) y para dar sincronización entre flujos. De modo que, varios paquetes pueden llevar la misma marca de tiempo si pertenecen a la misma unidad de datos a nivel de aplicación, un ejemplo muy claro de esto es el mismo cuadro de vídeo. Para detectar pérdidas dentro del flujo asigna números de secuencia.

El número de secuencia incluida en RTP permite al receptor reconstruir la secuencia de paquetes enviados, además determina una localización más apropiada de un paquete y por lo tanto no tiene necesariamente que decodificar los paquetes en secuencia, tal como ocurre en la decodificación de vídeo.

RTP juega un papel clave en los sistemas de VoIP, ya que se encuentra en el corazón de la aplicación, moviendo los paquetes de voz entre los participantes. La relación entre los protocolos de señalización y el protocolo RTP es que los primeros se encargan de establecer los parámetros de la sesión y el segundo se encarga del transporte de los datos.

4.3.1.2.6. RTCP (Real-Time Control Protocol, Protocolo de Control de Tiempo Real)

El protocolo RTP usualmente es asociado con el protocolo RTCP. Mientras que RTP ofrece una forma de transportar los datos multimedia a través de la red, éste no tiene mecanismos de control para indicar al transmisor que está sucediendo en la red. El protocolo RTP se basa en el envío periódico de paquetes de control a todos los participantes de una sesión.

RTCP aumenta las funciones de RTP dando un mecanismo de retroalimentación de la calidad del tráfico RTP. El protocolo RTCP es responsable de ofrecer al transmisor y al receptor reportes que incluyen información como estadísticas y cuentas de los paquetes. Utiliza un puerto UDP diferente (usualmente uno mayor) del utilizado por el protocolo RTP.

4.3.1.1. EL PROCESO DE LLAMADAS EN H.323.

Las entidades H.323 establecen conexiones en diferentes fases. Si consideramos un escenario en el cual exista un gatekeeper, la conexión entre dos terminales de este gatekeeper sigue los siguientes pasos: establecimiento de llamada, intercambio de capacidades, intercambio de información audiovisual y la terminación de llamada, las cuales serán explicadas a continuación.

4.3.1.1. 1. ESTABLECIMIENTO DE LLAMADA

El establecimiento de llamada se muestra en la figura 4.6.

1. El Endpoint 1 (EP1) envía un *mensaje RAS de ARQ* en el canal RAS al gatekeeper (GK) para solicitar su ingreso a la red de paquetes. El EP1 solicita el uso de la señalización directa de llamada.
2. El GK confirma la admisión del EP1 enviando un *mensaje RAS de ACF* al EP1. El GK indica en el ACF que EP1 puede usar señalización directa.
3. El EP1 envía un *mensaje Q.931 de establecimiento de llamada* a Endpoint 2 (EP2) indicando que el EP1 desea establecer una sesión.
4. El EP2 responde al EP1 con un *mensaje Q.931 de procedimiento de llamada* indicando que el establecimiento de la llamada ha sido iniciado.
5. El EP2 envía un *mensaje RAS de ARQ* en el canal RAS al GK para solicitar su ingreso y registro a la red de paquetes.
6. El GK confirma la admisión del EP2 enviando un *mensaje RAS de ACF* al EP2.
7. El EP2 avisa al EP1 que ha sido avisado de la llamada enviando un mensaje *Q.931 de alertamiento.*
8. El EP2 confirma el establecimiento de la conexión enviando un *mensaje Q.931 de conexión* al EP1. La llamada ha quedado establecida [8].

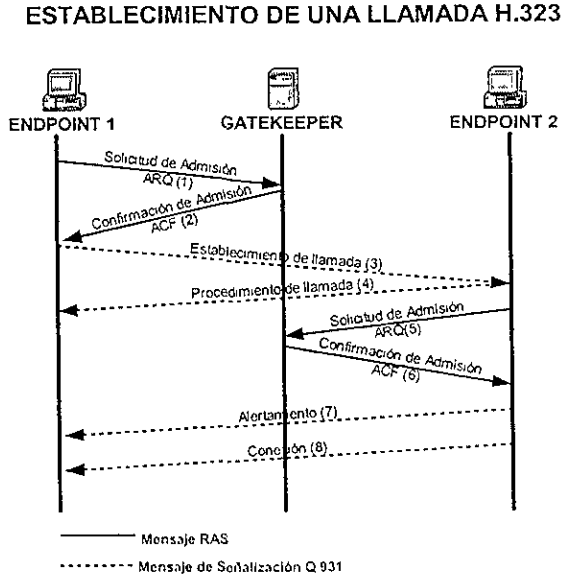

FIG 4.6 Establecimiento de llamada en H.323.

4.3.1.1.2. INTERCAMBIO DE CAPACIDADES.

Estableciendo el canal H.245 a través de una nueva conexión TCP, las entidades llamante y llamada determinarán los parámetros de la comunicación: codificadores a utilizar, número de conexiones y direcciones a utilizar, puertos, números de muestra por trama, función maestro-esclavo, etc., lo que les permite establecer canales para la transmisión de medios (audio, video y datos) [40]. El establecimiento de llamada se muestra en la figura 4.7. A continuación se describirán los pasos involucrados.

9. El canal de control H.245 es establecido entre el EP1 y el EP2. EP1 envía un *mensaje de establecimiento de las capacidades de terminal* para informar de sus capacidades para el envío y recepción de los flujos multimedia al EP2.
10. El EP2 envía *un mensaje de confirmación de las capacidades de la terminal* del EP1
11. El EP2 intercambia la información de sus capacidades enviando un *mensaje H.245 de establecimiento de capacidades.*
12. El EP1 envía un *mensaje de confirmación de las capacidades de la terminal* del EP2.
13. El EP1 abre un canal lógico con el EP2 enviando un *mensaje de apertura de canal lógico.* La dirección de transporte del canal RTCP es incluida en el mensaje.
14. El EP2 confirma el establecimiento del canal lógico unidireccional del EP1 al EP2 enviando el mensaje H.245 de confirmación de apertura del canal lógico. En el mensaje de reconocimiento se incluye la dirección de transporte RTP asignada por el EP2 para ser usada por el EP1 para enviar el flujo multimedia RTP. También se envía la dirección RTCP recibida por el EP2 anteriormente.
15. El EP2 envía un mensaje H.245 de apertura de canal lógico al EP1 para establecer su canal lógico. La dirección de transporte para el canal RTCP es incluida en el mensaje.
16. El EP1 confirma el establecimiento del canal lógico unidireccional del EP2 al EP1 con el mensaje H.245 de confirmación de apertura del canal lógico. En el mensaje de confirmación se incluye la dirección RTP de transporte asignada por el EP1 al EP2 para el envío del flujo multimedia. También se envía la dirección RTCP recibida por el EP1 anteriormente. La comunicación bidireccional entre las dos terminales ya esta establecida.

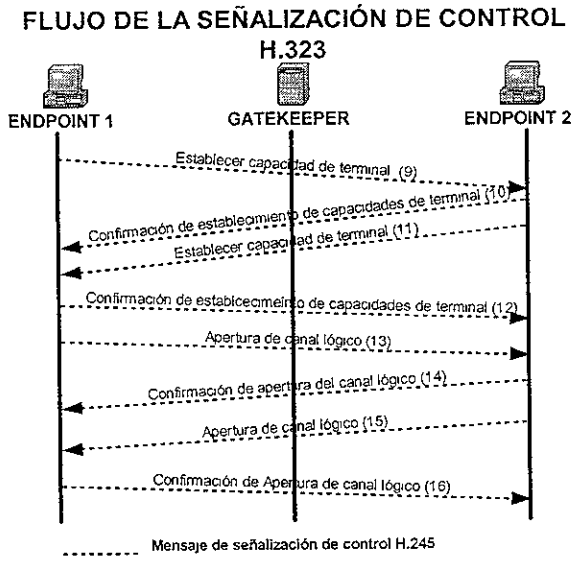

FIG 4.7 Intercambio de capacidades.

4.3.1.1. 3. INTERCAMBIO DE INFORMACION AUDIOVISUAL.

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

17. El EP1 envía el flujo multimedia RTP encapsulado al EP2.
18. El EP2 envía el flujo multimedia RTP encapsulado al EP1.
19. El EP1 envía mensajes RTCP al EP2.
20. El EP2 envía mensajes RTCP al EP1.

Lo anterior se muestra en la figura 4.8.

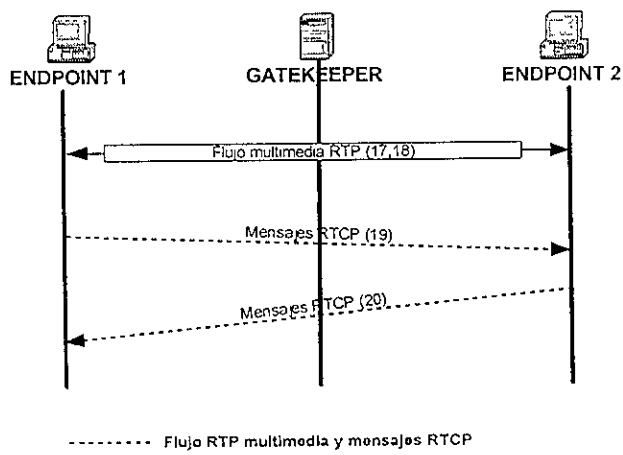

FIG 4.8 Intercambio de información audiovisual

4.3.1.1. 4. TERMINACION DE LLAMADA.

Tras el intercambio de información audiovisual y con el objeto de finalizar la llamada, las entidades H.323 realizan los siguientes pasos:

21. El EP2 inicia la liberación de la llamada. Envía un comando H.245 de fin de sesión al EP1.
22. El EP1 libera la llamada y confirma la terminación de la sesión enviando un comando H.245 de fin de sesión al EP2.
23. El EP2 completa la liberación de la llamada enviando un mensaje H.225 de liberación completa al EP1.
24. El EP1 y el EP2 realizan una petición de liberación al gatekeeper enviando a este un mensaje RAS de solicitud de liberación.
25. El gatekeeper confirma la petición de liberación a los Endpoints enviando un mensaje RAS de confirmación de solicitud de liberación (DCF).

En la figura 4.9 se muestra el proceso de terminación de llamada.

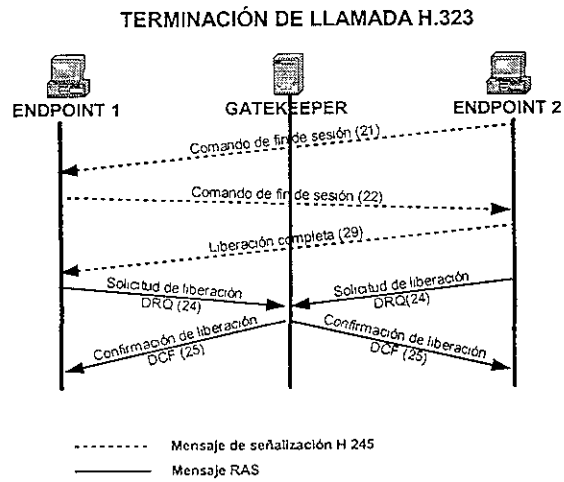

FIG 4.9 Terminación de llamada H.323.

4.3.2. El ESTANDAR SIP (SESSION INITIATION PROTOCOL, PROTOCOLO PARA INICIO DE SESION).

El protocolo de inicio de sesión (SIP) es un protocolo de aplicación desarrollado por el IETF dentro del grupo MMUSIC (Multiparty Multimedia Session Control) y especificado en el RFC2543 [13].

Como su nombre lo dice SIP, es usado para comenzar la sesión entre los usuarios. Proporciona los servicios de localización de usuario (de hecho es una de sus más importantes características), establecimiento de llamada, administración de los participantes de la sesión (usando una extensión de SIP) y limitadas características de invocación. Interesantemente, SIP no define el tipo de sesión que esta establecida SIP puede establecer fácilmente una conferencia de audio y video o una sesión de juego.

Cada solicitud SIP consiste de un junto de campos de cabecera que describen la llamada como un todo seguida de un cuerpo de mensaje que describe individualmente cada una de las sesiones que conforman la llamada.

SIP es un protocolo cliente-servidor, similar al protocolo http (Hypertext Transport Protocol, Protocolo de Transferencia de Hipertexto) tanto en sintaxis como en semántica. Las solicitudes son generadas por una entidad (el cliente) y enviadas a la entidad receptora (el servidor). El servidor procesa la petición y después envía una respuesta al cliente. Una solicitud y su respuesta son conocidas como una transacción. El software en un el equipo terminal que interacciona con el usuario es conocido como agente de usuario (UA, User Agent). El agente de usuario esta formado de dos componentes, un agente de usuario cliente (UAC, User Agent Client) y un agente de usuario de servidor (UAS, User Agent Server). El UAC es responsable de la iniciación de las llamadas (enviando las solicitudes) y el UAS es responsable de contestar las llamadas (enviando respuestas). Una aplicación típica de telefonía en Internet, contiene tanto el UAS y el UAC.

La versión actual de SIP (SIP 2.0) contiene seis tipos de peticiones, las cuales se conocen como métodos, brevemente descritas en la tabla 4.5 [5].

Tabla. 4.5 Tipos de peticiones en SIP.

Comando	Función
INVITE	Iniciación de llamada. Invita a un usuario a participar en una llamada.
ACK	Es usado para el intercambio confiable de mensajes para invitaciones. El usuario recibe una respuesta final de la invitación.
BYE	Terminación y Transferencia de llamada entre dos clientes.
CANCEL	Termina la búsqueda pendiente de algún usuario.
OPTIONS	Solicita información de las características de la otra terminal.
REGISTER	Transporta la información acerca de la localización del usuario a un servidor SIP de registro.

Además de las terminales H.323 que representan teléfonos IP o gateways, la arquitectura SIP define cuatro tipos de servidores:

- Servidor Proxy.
- Servidor de Redirección
- Servidor de Registro.
- Agente de llamada (Call Agent)

SERVIDOR PROXY.

Se encarga de enrutar peticiones/respuestas hacia el destino final. El enrutamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final. Para estos casos, existe un parámetro incluido en las peticiones/respuestas denominado *Via* que incluye los sistemas intermedios que han participado en el proceso

de enrutamiento. Esto afecta únicamente a la información de control pues el transporte de medios salvo en el caso de requerir codificación intermedia, se realiza directamente entre origen y destino.

SERVIDOR DE REDIRECCION.

También recibe las solicitudes y determina el siguiente servidor al cual llegarán los paquetes. En lugar de reenviar las solicitudes, regresa la dirección del siguiente servidor al cliente. Las funciones primarias de los servidores proxy y de redirección es el enrutamiento de la llamada (determinar el conjunto de servidores que utilizará para completar la llamada). Un servidor proxy o de redirección puede usar diferentes medios para determinar el siguiente servidor a utilizar como ejecutar programas y consultar bases de datos.

SERVIDOR DE REGISTRO.

Mantiene la localización actual de un usuario. Se utiliza para que las terminales registren la localización en la que se encuentran . Este servidor facilita la movilidad de usuarios, al actualizar dinámicamente la misma.

AGENTE DE LLAMADA (Call agent).

Realiza las funciones de los tres servidores anteriores, además de poder realizar las siguientes acciones:

- Localizar a un usuario mediante la redirección de la llamada a una o varias localizaciones.
- Implementar servicios de redirección como reenvío si esta ocupado, reenvío si no contesta, etc.
- Implementar filtrado de llamada en función del origen o del instante de la llamada.
- Almacenar información de administración de llamadas.
- Realizar cualquier otra función de gestión.

Las direcciones SIP son identificadas mediante los denominados URLs (Uniform Resource Locator, Localizador Uniforme de Recursos), que siguen la estructura *user@host*, donde *user* corresponde a un nombre, identificador o número telefónico y *host* es el dominio al que pertenece el usuario o dirección de red [40].

La principal característica de SIP frente a H.323 es su simplicidad. Mientras que H.323v1 necesita 5 o 6 intercambios de información entre los destinatarios antes de establecer una conexión, SIP requiere únicamente uno y puede ser transmitido por TCP o UDP.

4.4 CALIDAD DE VOZ (VQ, VOICE QUALITY) EN REDES IP.

Las redes telefónicas públicas conmutadas (PSTN) tradicionales han evolucionado para proveer un servicio óptimo para aplicaciones de voz sensibles al tiempo que requieren baja demora, jitter[4] reducido y un ancho de banda constante pero bajo, es decir la VQ de las PSTN es relativamente estándar y predecible.
Las redes IP actuales utilizan un enfoque de "el mejor esfuerzo" (best effort) para transportar los paquetes a sus destinos. Esto significa que los enrutadores reenvían los paquetes según el criterio "primero en entrar, primero en salir", y si se produce congestión, suprimen los paquetes que sobran sin tener en cuenta su importancia. Esto es claramente inaceptable para el transporte de voz.

Si esperamos que convergan las redes PSTN e IP, las redes IP (y los puntos de convergencia) deben ser mejorados con mecanismos que aseguren la calidad de servicio (QoS) requerida para transportar voz. Este punto es especialmente importante considerando que los usuarios de redes telefónicas tradicionales están acostumbrados a estándares elevados de VQ. Proveer una calidad de servicio comparable en redes IP motivará la aceptación y el éxito iniciales de los servicios VoIP, tales como voz sobre IP (VoIP). Este punto es especialmente importante considerando que los usuarios de las redes telefónicas tradicionales están acostumbrados a estándares elevados de VQ. Proveer una calidad de servicio comparable en redes IP motivará la aceptación y éxito iniciales de los servicios VoIP, tales como voz sobre IP (VoIP) [10][15].

4.4.1 CALIDAD DE VOZ (VQ, VOICE QUALITY)

Calidad de voz significa muchas cosas distintas, dependiendo de la perspectiva adoptada. Por un lado, es una forma de describir y evaluar la fidelidad e inteligibilidad de la voz y las características de la señal de voz analógica misma. Por otro lado, puede describir el desempeño de los mecanismos básicos de transporte. Sin embargo, *VQ se define como la medida cuantitativa y cualitativa de la calidad del sonido y la conversación de una llamada telefónica*

Son muchos los factores que pueden influir en la percepción que se tenga de la calidad de una llamada telefónica, y van desde la facilidad o dificultad para establecer la llamada a la calidad del sonido en el auricular. A un nivel muy elevado, la calidad de una llamada básica está integrada por tres componentes fundamentales:

- Calidad del servicio
- Calidad del sonido
- Calidad de la conversación

En la tabla 4.6 se describen estos tres componentes en mayor detalle.

[4] *Jitter-variabilidad en el retardo*

Tabla. 4.6 Detalles de la Calidad del servicio, calidad del sonido y calidad de la conversación.

Calidad de Servicio	Calidad del sonido	Calidad de la conversación
• Servicios ofrecidos- tales como tarjetas de llamada, servicios 1-800/900, sígueme y correo de voz. • Disponibilidad de usuarios en otros países o regiones. • Disponibilidad de la red – tiempo muerto, señales de ocupado. • Confiabilidad –tal como llamadas canceladas o número equivocado. • Precio	• Volumen • Distorsión • Ruido • Desvanecimiento • Cruce de llamadas	• Volumen, distorsión, ruido • Desvanecimiento • Cruce de llamadas • Eco • Demora extremo a extremo • Desempeño en supresión de silencios • Desempeño de cancelador de eco.

Los componentes de la tabla 4.6 impactan la calidad percibida sin importar si la llamada telefónica se realiza a través de líneas PSTN tradicionales, nuevas redes VoIP o un híbrido de ambas y con frecuencia dependen uno del otro cuando se trata del juicio final de un usuario respecto a la calidad de una llamada telefónica dada.

Considerando la definición anterior de VQ, surgen tres elementos como factores primarios que afectan la VQ, particularmente en el caso de redes que utilizan tecnologías VoIP.

- Claridad
- Latencia (retardo extremo a extremo)
- Eco

Una de las principales razones por las que la claridad, la latencia y el eco se agrupan juntas es que muchos usuarios reportan una VQ inaceptable si alguno de los aspectos de la VQ resulta inaceptable.

4.4.1.1 CLARIDAD

La claridad describe la fidelidad de la percepción, la limpieza y la naturaleza no distorsionada de una señal de voz en particular. Los factores que afectan la claridad de la voz en una red IP son: la pérdida de paquetes, él algoritmo de compresión utilizado, el ruido y el eco, y obviamente el retardo ocasionado por estas.

PERDIDA DE PAQUETES

La pérdida de paquetes no es rara en las redes IP. Cuando la red, o incluso algunos de sus enlaces, se congestionan, las memorias temporales (buffers) de los enrutadores se saturan y comienzan a perder paquetes. Otros motivos pueden ser los cambios de ruta como resultado de que algunos enlaces de la red no están funcionando.

Para las aplicaciones que no operan en tiempo real, tales como transferencias de archivos, la pérdida de paquetes no resulta crítica. Los protocolos de paquetes permiten la retransmisión para recuperar los paquetes cancelados. Sin embargo, en el caso de información de voz en tiempo real, los paquetes deben llegar dentro de una ventana de tiempo relativamente estrecha para ser útiles en la reconstrucción de la señal de voz. En el caso de la voz, las retransmisiones añadirían una demora excesiva a la reconstrucción y causarían la sobreposición del habla o que ésta resultara ininteligible.

Para evitar la pérdida de paquetes para aplicaciones en tiempo real, se requieren mecanismos en la red IP para asegurar un rendimiento mínimo para las aplicaciones seleccionadas. Pueden emplearse diversos mecanismos para lograr este objetivo, los cuales incluyen esquemas para asignación de prioridades, como las colas de espera con ponderación equitativa y mecanismos para control de flujo en el enrutador como los esquemas MPLS y RSV. (ver capítulo 3, sección 3.6.2 "CALIDAD DE SERVICIO").

ALGORITMO DE CODIFICACION UTILIZADO

Dependiendo del tipo de codec utilizado, la forma de onda real de la voz puede ser reproducida en el extremo receptor de una conversación VoIP. Los codecs como el G.711 pueden ser considerados como lineales debido a que se acercan mucho a reproducir la forma de onda. Sin embargo los codecs con baja velocidad de bits como el G.729 y el G.723.1 (ver capítulo 4, sección 4.2 "CODIFICADORES DE VOZ PARA VoIP) tratan de reproducir el sonido subjetivo de la señal en lugar de la forma de onda del habla, y por lo tanto, generalmente son considerados como lineales.

Esencialmente entre mayor sea la reducción del ancho de banda, mayor será el costo de computación asociado al codec para un nivel dado de claridad percibida. Adicionalmente mayores ahorros en el ancho de banda generalmente causan una mayor demora de procesamiento y, por tanto, un aumento significativamente mayor en retardo extremo- extremo. El efecto de un codec sobre la calidad de voz también es influenciado por el tamaño del paquete, la pérdida del paquete y cualquier mecanismo de corrección de error usado por el mismo codec.

RUIDO

Todo ruido, sin importar cuál sea su origen, tiene el potencial de reducir la claridad de una señal de voz. El ruido puede tener su origen en bits de error en las líneas para transmisión de datos.

ECO

El habla cuyo eco se regresa al auricular como el que se percibe durante conversaciones, puede tener un efecto significativo sobre la claridad percibida

4.4.1.2 LATENCIA. (RETARDO EXTREMO-EXTREMO).

La latencia es el tiempo requerido para que una señal atraviese la red. En el contexto de la telefonía, la latencia es el tiempo requerido para que una señal generada en la boca de la persona que llama, llegue al oído de la persona que escucha. La latencia es la suma de los retardos en los distintos dispositivos de la red y a través de los enlaces de la red por los cuales transita la voz. Son muchos los factores que contribuyen a la latencia entre los cuales se tienen: el retardo en la red IP, el retardo en la captura de paquetes, en el enrutamiento, los tiempos en la cola de espera, el retardo debido al algoritmo de codificación utilizado y, el retardo ocasionado por los dispositivos VoIP.

RETARDO EN LA RED IP.

El retardo en la red IP está determinado principalmente por las demoras de buffering[5], colas de espera y conmutación o enrutamiento de los enrutadores IP.

RETARDO EN LA CAPTURA DE PAQUETES.

El retardo en la captura de paquetes es el tiempo requerido para recibir todo el paquete completo antes de procesarlo y transferirlo a través del enrutador. Esta demora es determinada por la longitud del paquete y la velocidad de transmisión. El uso de paquetes cortos a través de troncales de alta velocidad puede reducir la demora pero también tiene el potencial de reducir la eficiencia de la red.

RETARDO EN EL ENRUTAMIENTO

La demora en el enrutador es el tiempo que el enrutador requiere para reenviar el paquete. Este tiempo es necesario para analizar el encabezado del paquete, revisar la tabla de enrutamiento y enrutar el paquete al puerto de salida.

TIEMPO EN LA COLA DE ESPERA.

Debido a la naturaleza de multiplexión estadística de las redes IP y a la naturaleza asíncrona de la llegada de los paquetes, se requiere una cola de espera (y por tanto de retraso) en los puertos de entrada y salida de un conmutador de paquetes. Este retraso está en función de la carga de tráfico a través de los puertos.

RETARDO EN LOS DISPOSITIVOS VoIP.

Los gateways VoIP y las terminales VoIP también contribuyen en forma significativa a la latencia como resultado del procesamiento de la señal tato en el lado transmisor como en el lado receptor del enlace.

En el lado de transmisión, el retardo por colocación en paquetes es otro factor, éste retardo es el tiempo requerido para llenar un paquete con datos de voz. Entre más largo sea el tamaño del paquete, mayor será el tiempo requerido.

[5] *El término buffering se refiere al almacenamiento temporal de datos en algún dispositivo*

En el lado de recepción, los paquetes de voz deben ser retrasados para compensar el jitter (variación en los tiempos entre llegadas de los paquetes). Incluso los paquetes generados con un espacio de tiempo constante llegarán al receptor con una distribución espaciada en forma aleatoria como resultado de las distintas acumulaciones de tiempos en colas de espera que experimentan los paquetes y las diversas rutas de transmisión en la red IP.

No importa qué tan bien se diseñen los dispositivos y redes VoIP, existe un retraso fundamental que simple y sencillamente no puede ser eliminado. Esto es, siempre se introducirá cierto retardo como resultado de los límites físicos de la colocación en paquetes, el tiempo de procesamiento y el tiempo de propagación.

El retardo no afecta directamente la calidad de voz sino que afecta el carácter de una conversación. Debajo de 100 ms, la mayoría de los usuarios no percibirán la demora. Entre 100 ms y 300 ms los usuarios percibirán un ligero retraso en la respuesta de la otra persona. Este retraso puede afectar en que el que escucha percibe el estado de ánimo de la conversación. En esta situación la conversación parecería fría. Las interrupciones son más frecuentes y la conversación se sale de ritmo. Después de 300 ms, el retraso es obvio para los usuarios. En cierto punto, la conversación es virtualmente imposible.

Un fenómeno interesante relacionado con el retardo tiene mucho que ver con el eco. Hablando en términos generales, existe un eco en muchas PSTN (Red telefónica pública conmutada), pero debido al lugar donde se origina el eco y la latencia muy baja, con frecuencia el eco pasa desapercibido. Sin embargo, cuando se introducen niveles de demora VoIP, el eco con frecuencia se hace notable.

4.4.1.3. ECO

Desde una perspectiva telefónica, el eco es el sonido de la voz de quien habla que regresa a sus oídos a través del auricular del teléfono.

Si el tiempo entre la fase dicha originalmente y el eco de regreso es corto (25 a 30 ms), o si el nivel de eco es muy bajo (aproximadamente –25 dB), es probable que no cause ninguna molestia ni alteración a las conversaciones de voz. Es cuando el eco es lo suficientemente audible como para ser escuchado cuando atraviesa por redes con niveles de retardo muy elevados (generalmente alrededor de 30 ms o más) que la calidad d voz se vuelve problemática.

En la mayoría de los casos, el eco es causado por una discordancia eléctrica entre dispositivos telefónicos analógicos y medios de transmisión en una parte de la red denominada circuito de cola. Un circuito de cola es todo aquello conectado entre el gateway de voz y el teléfono.

Para manejar este eco indeseable, componentes funcionales conocidos como canceladores de eco se instalan en el conmutador loca, el gateway VoIP o la terminal VoIP, generalmente tan cerca como sea posible del circuito de cola que causa el eco.

4.5 SEGURIDAD

Cuando la idea de transmitir voz sobre el Protocolo de Internet (VoIP), estaba todavía en su infancia, la seguridad era una de las preocupaciones primarias. Después se comenzó a hablar de la Calidad de Servicio (QoS), esta paso a ser la preocupación principal. Ahora que VoIP esta ganando mucho interés, las corporaciones de todos tamaños buscan la forma para mantener segura su información confidencial.
Actualmente el tema de la seguridad ha regresado a la escena. Algunas compañías están desarrollando medidas de seguridad de buscar-ir (get-go), otras prefieren esperar que los eruditos en seguridad den el paso. La mayoría de los desarrollos en seguridad se enfocan a soluciones WAN, ya que usar las redes LAN para voz y video es un territorio aún desprivilegiado.
La seguridad en comunicaciones de VoIP tiene cuatro principales componentes:

- Autentificación
- Integridad
- Confidencialidad
- No-repudiación

La autentificación determina el control de acceso y verifica los términos del servicio. La protección de Integridad asegura que los datos sean accesados por algún intruso antes de que lleguen a su destino. La protección de confidencialidad evita accesos a la información sin contar con la autorización, también es usado para protección de privacidad. No-repudiación asegura la contabilidad para facturación y propósitos legales.

4.5.1 IMPORTANCIA DE LA SEGURIDAD

La mayoría de las preocupaciones, en cuanto a seguridad se refiere, se originan de las experiencias de los usuarios con las redes existentes. Pero hay diferencias importantes entre las transmisiones comunes de datos y las transmisiones de aplicaciones en tiempo real, la forma en las que estas son procesadas en una red IP (diferencias que automáticamente disminuyen algunos de estos temores, es importante también entender las opciones disponibles en lo que a seguridad se refiere. Finalmente como en cualquier otro desarrollo tecnológico, la seguridad requiere ser evaluada en el contexto de infraestructura, mantenimiento y otros costos) así como en los requerimientos de QoS de ambas.

4.5.1.1 SEGURIDAD EN REDES DE AREA AMPLIA (WAN)

La Siguiente generación de compañías de telecomunicaciones y proveedores de servicios parecen no darse cuenta de los riesgos de VoIP, dada la naturaleza de la comunicación en tiempo real. Por ejemplo, es muy difícil reensamblar y darles un sentido a los paquetes de voz como ocurre en los paquetes únicamente de datos. También mientras resulta muy fácil analizar mensajes de texto usando sistemas automáticos, se

requiere una mayor sofisticación que usar sistemas automáticos para analizar y extraer información útil de una conversación de voz o vídeo.

Finalmente, es muy difícil impactar la integridad de los paquetes de voz, ya que la comunicación de voz y vídeo es en tiempo real, cualquier daño que ocasione una recepción confusa introduciendo una latencia más que la usual provocará que el usuario termine la llamada.

Todas estas razones pueden minimizar los cuestionamientos en seguridad pero, no eliminan la necesidad fundamental de la seguridad. A aumentado el acceso de los usuarios a los circuitos de voz y señalización de la RTPC con la llegada de VoIP. El acceso de los gateways a la red puede ser usado virtualmente en cualquier parte del mundo. La próxima generación de red consiste de una red central de paquetes limitada por una mezcla de agentes, gateways y puntos de acceso. Los ataques a la red pueden ser directamente desde cualquiera de estos elementos en la red, lo que hace esencial puntos de prueba de seguridad en la red.

De acuerdo con John Kimmins, director de seguridad de Telcordia Technologies. Inc :"Es especialmente importante verificar la integridad del establecimiento de la conexión", La manipulación de los datos o espiar las conversaciones telefónicas pueden ser motivadas por una variedad de razones desde la simple intención de causarle problemas alguien impactando la productividad de los individuos o los negocios"

Aunque la IETF esta desarrollando protocolos de seguridad como el IPSec, para mejorar la de seguridad en las redes, estos se enfocan al contexto de redes virtuales privadas (VPNs).

Solo nos queda ver que tan rápido podremos definir e implementar protocolos de seguridad que incorporen los cuatro componentes básicos mencionados al inicio en las redes públicas para voz y video sobre IP.

4.5.1.2. SEGURIDAD EN REDES DE AREA LOCAL (LANs)

La situación es un poco diferente para las soluciones LAN. Primero porque las comunicaciones de datos, voz y video comparten la misma red local, y ya se tienen implementados los firewalls que prevendrán llamadas de usuarios sin autorización que deseen dentro de la red corporativa.

En segundo lugar, una comunicación sobre la LAN es un riesgo por los hackers internos quienes tienen información de identidad de los individuos que participan en las conversaciones. Esto hace importante asegurar la conversación, no únicamente proteger la información confidencia sino también proteger la privacidad.

4.5.1.2.1. SOLUCIONES PARA MEJORAR LA SEGURIDAD EN REDES LAN.

DETECCION DE INTRUSOS.

Las intrusiones en las redes administradas y locales pueden ser detectas monitoreando la red mediante el uso de algún paquete de software. Los agentes de software analizan el tráfico, buscando amenazas de paquetes. Detectando algún mal uso, el agente puede responder inmediatamente terminando la conexión o notificando el

hecho al administrador enviando alertas e la pantalla, a través de un correo electrónico, enviando un pager o un mensaje SMNP.

AUTENTIFICACION Y ENCRIPTACION.

Otra opción para mejorar la seguridad es usar estándares de seguridad para la red y los datos como la autentificación y la encriptación. La autentificación se asegura de que el usuario cuente con los derechos de acceso. Ya que una llamada entrante puede ser originada desde cualquier parte del mundo, la autentificación puede ser aplicada solo mínimamente en la comunicación de voz y vídeo. Por otro lado, la encriptación ofrece una solución muy atractiva.

La encriptación[6] previene de accesos sin autorización y del posible daño de los datos tanto de intrusos tanto internos como externos. La mayor preocupación es el impacto que ocasionaría la encriptación en la latencia y en la QoS de comunicaciones en tiempo real. Este problema es aumentado por los algoritmos de compresión cuando los codificadores de velocidad de bit baja como el G.723.1 y el G.729 son usados (en oposición al G.711). La mayor parte de las empresas que han desarrollado soluciones para VoIP aconsejan la utilización del codificador G.711 como la solución más apropiada. El utilizar los codificadores de velocidad de bit baja puede crear latencia inaceptable sin embargo, esta restricción puede desaparecer cuando aumente la velocidad de encriptación con el desarrollo de la tecnología, pero no resuelve el problema de los accesos a través del firewall.

ACCESO DE FIREWALL.

Cisco Sistema, Truste Information Sistema, check Point Software e *Intel* han estado trabajando juntos en el desarrollo de productos para firewall que soporten el estándar de comunicación H.323. La intención es permitir llamadas de audio y video a través de los firewalls de las compañías y sobre INTERNET, mientras mantienen la seguridad de los datos de las redes corporativas.

La mayor parte de las preocupaciones viene de la experiencia con comunicaciones de datos y no aplican a las comunicaciones de VoIP. En el mercado existen soluciones en esta materia disponibles. La seguridad es una cuestión de equilibrar la sensibilidad de la empresa en lo que ha seguridad se refiere, aplicaciones y a los requerimientos de QoS, y el costo de establecer la infraestructura, el mantenimiento y el soporte.

Típicamente las compañías grandes son altamente sensibles a las cuestiones de seguridad por lo que cuentan con políticas de seguridad muy exigentes, estas también cuentan con una infraestructura de seguridad que puede ser aprovechada para ofrecer seguridad en VoIP.

Por otra parte, los negocios pequeños pueden escoger no implementar totalmente la encriptación, principalmente para evitar costos de infraestructura y soporte, para tomar ventaja de los grandes ahorros en el uso del ancho de banda con codificadores de velocidades de bajo bit. O estas pequeñas compañías pueden

[6] *Se define por encriptación al conjunto de técnicas que permiten codificar la información que circula en alguna red de manera que las personas no autorizadas no puedan leerla ni manipularla*

tener políticas que asignen una pequeña infraestructura para asegurar solamente las llamadas de los ejecutivos.

La Seguridad es una cuestión a tomar en cuenta en comunicaciones de VoIP pero, tomando medidas básicas de seguridad no debe presentarse como un problema.

5. TENDENCIAS DE VoIP Y APLICACIONES.

5 TENDENCIAS Y APLICACIONES DE VoIP

La posibilidad de que los futuros servicios de red puedan estar basados principalmente en IP ha provocado un tremendo interés por la tecnología de voz a través de IP (VoIP). Aunque ha menudo se considera una forma de realizar llamadas baratas a través de la red pública Internet, la tecnología VoIP tiene un mayor valor estratégico a largo plazo. Abre la puerta a la integración de voz, vídeo y datos en una misma red basada en el protocolo Internet y puede reducir potencialmente el coste de los equipos, las operaciones y la gestión de las redes. Incluso puede sentar la base de nuevos tipos de servicios de comunicaciones. Así la convergencia entre la voz y los datos no viene dada sólo por el ahorro, sino por los nuevos servicios que podrán ser ofrecidos en estas redes. Por ejemplo, con VoIP integrada en una red de datos, si una persona se encuentra ausente de su puesto y recibe una llamada, el sistema puede mirar su agenda, encontrar la sala en la que está reunido y pasar la llamada automáticamente [46]. En la figura 5.1 se muestran las diferentes redes que deben existir para prestar los servicios de voz, datos y vídeo sin implementar la tecnología de VoIP.

En este capítulo, se estudiarán los diferentes aspectos que deberán cumplirse para asegurar una aceptación con exitosa de la tecnología VoIP. Posteriormente se hablará de las diferentes aplicaciones que podrán ser implementadas con ésta tecnología. Finalmente se mencionarán las ventajas y desventajas que presenta la implementación de esta nueva tecnología.

5.1 FACTORES DE EXITO PARA VoIP.

La implantación satisfactoria de la tecnología VoIP exige una mejora significativa de las redes y los dispositivos IP con una funcionalidad de QoS (Calidad de servicio), fiabilidad, funcionamiento recíproco con las redes telefónicas ya existentes y una tarificación basada en el uso.

ASEGURAR LA CALIDAD DE SERVICIO (QoS).

El primer obstáculo importante, que ha recibido gran atención, es la necesidad de aportar una calidad de servicio garantizada. El protocolo Internet se diseñó principalmente para transportar tráfico de datos que no es sensible al retardo o a la variación del retardo (jitter). Antes de poder implantar la tecnología VoIP a gran escala, los enrutadores IP deben ser capaces de asignar los recursos de la red necesarios para ofrecer una calidad de voz aceptable.

Los fabricantes de equipos de red así como grupos de trabajo, tales como IETF están desarrollando varios mecanismos para hacer posible este aspecto *(ver capítulo 3, sección 3.6.2.1 "TECNOLOGÍAS DE QoS EN REDES IP" y capítulo 4, sección 4.4 "CALIDAD DE VOZ (VQ, VOICE QUALITY) EN REDES IP")*. Entre las soluciones incluyen; sistemas de asignación de prioridades. tales como, colas justas ponderadas y mecanismos de control de flujo en los enrutadores ("categoría de servicio"), así como la identificación de flujos

Aunque ya existe la tecnología que hace posible el transporte de paquetes mediante asignación de prioridades, los fabricantes de equipos todavía no han definido e implantado estándares para muchos de los mecanismos. Por consiguiente, los enrutadores preparados para VoIP siguen siendo la excepción en las redes IP.

Otro problema aún más difícil de resolver, es encontrar una manera de garantizar la QoS de extremo a extremo. Cuando un proveedor de servicios de Internet u otra compañía operadora comercial transporta el tráfico IP, los paquetes de datos pueden pasar por muchos recorridos a través de numerosas redes.

Actualmente es casi imposible asegurar que al tráfico de voz se le asigne siempre suficiente ancho de banda de la red. Serán necesarios acuerdos de nivel de servicio entre los proveedores de servicios, para establecer una QoS de extremo a extremo en un entorno de múltiples proveedores de servicios, y será preciso vigilar el tráfico para asegurar que se cumplan los acuerdos.

FIABILIDAD Y DISPONIBILIDAD.

Los usuarios de teléfonos esperar oír un tono de marcación cada vez que descuelgan el aparato, y esperan obtener siempre un alta de calidad de voz. Las empresas, los servicios de emergencias y otros usuarios dependen de la fiabilidad y disponibilidad casi absolutas que ofrece la red pública conmutada.

Aunque las redes IP son muy fiables para aplicaciones tales como correo electrónico y para transmitir paquetes fallidos, en las aplicaciones sensibles como voz, a través de IP, los procesos normales de corrección de errores pueden no aportar de manera fiable la QoS que desean los clientes.

Los proveedores de servicios pueden abordar este problema de varias maneras: instalando equipos de mayor capacidad y equipos con redundancia incorporada; sobreconfigurando los enlaces para que puedan hacer frente a sobrecargas de tráfico; o añadiendo sistemas de reserva en caso de fallo. Los fabricantes de equipos de red están presentando nuevos conmutadores y enrutadores IP con mayor capacidad y rendimiento, y con redundancia incorporada.

Aunque la mayoría de los grandes conmutadores preparados para la tecnología VoIP, sólo pueden hacer frente a una fracción de las llamadas que gestiona una central de conmutación totalmente cargada de una red conmutada, algunos fabricantes afirman que ofrecerán enrutadores de red con capacidades que llegan hasta varios terabits.

REQUISITOS DE FUNCIONAMIENTO RECIPROCO, CON LAS REDES TELEFÓNICAS ACTUALES.

El funcionamiento entre las redes basadas en el protocolo IP con la red Pública Conmutada, PSTN[1], es esencial para un servicio a nivel comercial. Sin embargo, las redes IP con conmutación de paquetes "carecen de conexiones", ofreciendo únicamente conexiones virtuales entre puntos extremos de la red y compartiendo ancho de banda entre todos los usuarios de la red. La red conmutada con conmutación de líneas, por otra parte establece conexiones dedicadas de extremo a extremo y asigna cierto ancho de banda mientras dura la llamada. El establecimiento y control de las llamadas se consigue mediante la señalización. Los gateways

[1] *PSTN (Public Switched Telephone Network, Red Telefónica Pública Conmutada)*

VoIP aportan la interface entre las redes basadas en IP y la PSTN(Public Switched Telephone Network, Red telefónica pública conmutada). Estos gateways convierten la transmisión de voz, así como la señalización IP, a los numerosos protocolos utilizados por las compañías operadoras de redes inalámbricas y de cable. Para poder funcionar recíprocamente y de manera correcta con las redes telefónicas existentes y sus servicios, es esencial asegurar el funcionamiento recíproco entre la señalización IP y la red SS7 (Signal System No.7, Sistema de señalización No. 7) La red SS7 controla el establecimiento y la gestión de las llamadas en la red conmutada WAN, además de aportar la implantación de servicios de red inteligentes y mejorados.

Los gateways y gatekeepers basados en H.323 ya proporcionan un funcionamiento recíproco básico para llamadas de voz entre redes basadas en IP y la red pública conmutada, y prometen admitir muy pronto el nivel de funcionamiento recíproco con SS7 necesario para ofrecer los mismos servicios de valor añadido que ofrece la red telefónica existente.

TARIFICACION: EL RESULTADO FINAL.

La tarificación es el resultado final para cualquier negocio. Si los proveedores de servicios pretenden prestar distintas clases de servicio, es esencial una tarificación basada en el uso. Proporciona la base para establecer los precios relacionados con el servicio y para controlar las cargas de tráfico de la red mediante contratos de tráfico.

En las redes IP, la generación de registros detallados de las llamadas para la tarificación basada en el uso de la misma, ya sea en tiempo o en volumen, es especialmente compleja, ya que no todos los paquetes de datos relacionados con una determinada llamada siguen necesariamente el mismo recorrido hasta llegar a su destino, y por ello pueden experimentar distintos niveles de QoS durante el trayecto. Para asegurar el cumplimiento de acuerdo de nivel de servicio, los gateways de acceso IP/PSTN deben monitorizar la calidad durante toda una llamada de VoIP.

Además, los datos de tarificación recopilados deben ser compatibles con los sistemas de tarificación de otras redes o de otros proveedores de servicio, con quienes deba intercambiarse información de tarificación

UNA PROPUESTA A LARGO PLAZO

Se espera que el valor a largo plazo de VoIP se concrete con la prestación de servicios de telefonía de calidad, comparable a la de los servicios prestados por las compañías operadoras, así como con aplicaciones multimedia a través de las redes principales IP de reciente desarrollo. A continuación se hablará de las diferentes aplicaciones para VoIP.

5.2 APLICACIONES Y SERVICIOS PARA LA TECNOLOGÍA VoIP.

La principal diferencia entre la PSTN convencional y la telefonía IP, es que esta última constituye un servicio de voz construido en la cima de una red de servicios de comunicaciones de datos. Como resultado, la tecnología VoIP tiene la posibilidad de ir más allá de los servicios ofrecidos por una simple comunicación de voz. Los servicios de datos fácilmente pueden ser combinados con servicios de voz para dar nacimiento a

nuevas aplicaciones y servicios que no son posibles ofrecer en las redes telefónicas tradicionales. En esta sección se describirán algunas de las nuevas aplicaciones que serán posibles gracias a la convergencia voz y datos, aunque hay que aclarar que estas aplicaciones no constituyen todo el mercado posible para VoIP, ya que con mucha frecuencia se crean nuevas aplicaciones [2] [41]. A continuación se enumeran algunas de las aplicaciones clave para VoIP:

TELEFONIA EN INTERNET/VOZ A TRAVÉS DE INTERNET.

Aunque existen numerosas interrogantes relativos a la telefonía a través de la red pública Internet –incluida la futura reglamentación, seguridad y fiabilidad- se espera que la telefonía IP a través de redes públicas, proveedores de servicios de Internet y redes empresariales alcance el éxito a largo plazo. Las primeras implantaciones tendrán lugar en redes empresariales, en las que la calidad del servicio es más fácil de gestionar y la integración de los servicios de datos y voz en una misma red puede traducirse en enormes ahorros potenciales.

INTEGRACIÓN DE DATOS, VOZ Y FAX.

Al igual que se hace con la voz, cabe la posibilidad de realizar transmisiones de FAX sobre redes de Telefonía IP, consiguiendo de esta manera reducir de forma significativa los costes de una empresa en transmisión de fax. En este caso no es necesario para el usuario que recibe el fax de disponer de equipos especiales ya que los faxes se seguirán recibiendo a través de una máquina de fax convencional. Una aplicación típica en este tema es el envío masivo de fax, ya que el usuario sólo enviará una copia del fax que desea enviar, así como la lista de números telefónicos de destino y el sistema se encargará de realizar todos los envíos enrutando los faxes al punto desde donde la llamada de destino es más económica. Así se contará con una única red para voz, datos y fax.

VIDEO TELEFONIA.

Ya que la telefonía IP también soporta transmisiones de vídeo, es fácil implementar aplicaciones de vídeo-telefonía. En la figura 5.3 se ilustra la aplicación de vídeo telefonía utilizando computadores personales.

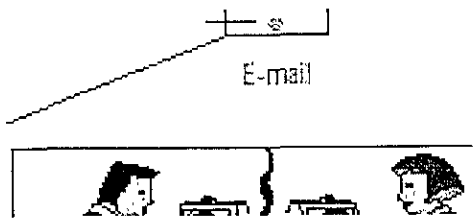

FIG 5.1. La aplicación de video telefonía utilizando computadoras personales.

CENTROS DE LLAMADAS (CALL CENTERS)[2].

Los centros de llamadas pueden usar la Telefonía IP, mejorando la calidad de la información intercambiada en cada sesión. Por ejemplo un usuario podría navegar por información conectado, antes de realizar la consulta a un operador. Una vez en comunicación con el operador, se podría trabajar con un documento compartido a través de la pantalla. De esta forma se consigue sistemas de una gran calidad en el servicio a ofrecer, además de reducir de forma considerable el coste de líneas telefónicas y de Distribuidores Automáticos de Llamadas (ACD).

REDES PRIVADAS VIRTUALES DE VOZ.

Esta aplicación consiste en la interconexión de las centralitas telefónicas a través de la red IP corporativa, de manera que se puede realizar una llamada desde una extensión de la oficina A otra extensión de la oficina B a través de la red de datos de la empresa, produciéndose esta llamada de forma gratuita ya que se aprovecha la infraestructura de datos ya existente. Un ejemplo claro de este servicio serían los bancos y su red de oficinas.

CENTROS DE LLAMADAS POR EL WEB.

Si una compañía tiene su información disponible en un sitio en Internet, los usuarios que visitan este sitio podrían no solo visualizar la información que esta compañía les ofrece, sino que podría establecer una comunicación con una persona del departamento de ventas sin necesidad de cortar la conexión. De esta manera el operador de ventas cuando atienda la llamada tendrá en su pantalla la misma información que esta viendo el usuario. Esta aplicación tiene las siguientes ventajas:

- Al ser la llamada a través de Internet, para el usuario no tiene coste adicional, aprovecha la llamada telefónica que tenía establecida para la comunicación de datos, para mantener también la comunicación de voz, esto permite tener a la empresa un servicio similar al de las líneas 900.
- El usuario puede mantenerse conectado mientras habla con un operador de ventas.
- El cliente trata con operadores humanos, que le podrán asesorar, esta característica mejorará sin lugar a duda el resultado de un sistema de comercio electrónico.
- El operador puede cerrar la venta de manera más fácil ya que el usuario es bastante reacio a dar los datos de su tarjeta de crédito en una pagina en Internet por temas de seguridad que todos conocen, sin embargo no tendrá ningún inconveniente de dar esos datos verbalmente al operador de ventas, teniendo el usuario plena garantía de que sus datos están a salvo.

[2] *Centro de llamadas es un término genérico que por lo general se refiere a centros de reservaciones, oficinas de ayuda, líneas de información o centros de servicio al cliente, independientemente de cómo están organizados o de que tipo de transacciones atienden*

MULTICONFERENCIA.

La telefonía IP permite la conexión de 3 o más usuarios simultáneamente compartiendo las conversaciones de voz o incluso documentos sobre el que todos los miembros de la multiconferencia pueden participar en la revisión, esto resulta de gran utilidad para empresas que realicen reuniones virtuales, con los consiguientes ahorro de gastos que supone el desplazamiento de personas.

MENSAJES UNIFICADOS.

La mayoría de los empleados cuentan con varios servicios de comunicaciones por medio de los cuales se encuentran en contacto con sus clientes o colegas durante el curso del cumplimiento de sus tareas. Entre estos servicios se tienen direcciones de correo electrónico, un número de teléfono celular, un número de teléfono convencional, y un número de fax en su oficina, además quizá cuenten con otro número telefónico y de fax para su casa. Esta variedad de puntos de contacto dan como resultado que el usuario no pueda ser contactado rápidamente si se encuentra fuera de su oficina.

Los servicios de mensajes ofrecidos por las compañías telefónicas tradicionales están restringidos únicamente a los mensajes de voz; no permiten que se accese a los faxes o direcciones de correo electrónico. Con el uso de los sistemas de conmutación de paquetes tales como redes IP, se harán realidad los sistemas de unificación de mensajes. Los cuales permitirán a los usuarios accesar a todos sus mensajes a su conveniencia desde un punto centralizado. El correo de voz de su casa o las llamadas de trabajo podrán se reenviadas a la misma localización de correo. Esta característica puede aún ser más extendida utilizando un único número telefónico para todos los servicios de telecomunicaciones. En la figura 5.4 se ilustra la unificación de mensajes.

5.3 VENTAJAS E INCONVENIENTES DE LOS SERVICIOS IP

En esta sección se analizan por separado tanto las ventajas como los inconvenientes del uso de los servicios IP en los ámbitos más comunes.

VENTAJAS

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 al objeto de hacer llegar a los posibles usuarios la bondad de su implantación en un futuro no muy lejano. Hay que evitar la confusión y prematuro rechazo ante algo que se plantea como la solución universal y que no se termina de entender . En esta línea destacan tres grandes bloques:

- **ENTORNO EMPRESARIAL**
    1. Amplia reducción en los costes de la factura telefónica. Los costes de todo tipo de llamadas se equipararán al de una llamada local de forma que la reducción en los costes del tráfico de voz será a todas luces muy importante.

2. Nuevas posibilidades de marketing directo y potenciación del servicio de atención al cliente. Podrán implantar la filosofía "Push 2 Talk" que consiste en un icono situado en una página en Internet a través del cual un navegante podrá dialogar con personal especializado de la compañía mientras continúa navegando por la red.
3. Potenciación del teletrabajo y de los teletrabajadores. Con una única conexión se podrá acceder a aplicaciones corporativas, al correo vocal, atender llamadas o buscar información sobre nuevos proyectos.

- USUARIOS FINALES
  1. En este momento el usuario final que ocupe su línea de teléfono doméstica para transmisión de datos no puede recibir comunicaciones de voz al estar la línea ocupada. Los nuevos servicios de VoIP no sólo le permitirán atender llamadas de forma simultánea sino que además podrá conocer quien le llama y de esa forma admitir y rechazar llamadas e incluso desviarlas.

- **PROVEEDORES DE SERVICIOS.**
  1. XoIP será su nuevo argumento comercial. X supone poder ofrecer voz, datos, fax o cualquier servicio susceptible de ser transmitido por una red IP. El ejemplo más claro es la nueva vertiente estadounidense denominada Internet Telephony Service Providers (ITSPs) quienes ya ofrecen todo tipo de servicios a través de redes IP.

DESVENTAJAS

Si todo está tan claro, si ya existe tecnología, si los estándares están validados por organismos internacionales (caso del H.323 definido por la ITU), si la ley en principio no presenta inconvenientes y si además las consultoras internacionales presentan esta solución como la verdadera alternativa de negocio en el año 2005, la lógica hace pensar que la implantación de XoIP se realizará de forma inmediata. Pero el verdadero caballo de batalla se resume con tres letras "QoS".

Quality of Service: garantizar calidad de servicio en base a retardos y ancho de banda disponible en una red IP no es realmente posible sobre una red IP. Distintos organismos y fabricantes empiezan a definir soluciones y estándares, pero su aplicación o implantación no se considera posible en un mínimo de 2 a 3 años. *(ver capítulo 3, sección 3 6 2.1 "TECNOLOGÍAS DE QoS EN REDES IP" y capítulo 4, sección 4 4 "CALIDAD DE VOZ (VQ, VOICE QUALITY) EN REDES IP").*

6. EQUIPO, SOFTWARE Y SUMINISTRADORES DE SERVICIO PARA VoIP.

6 EQUIPO, SOFTWARE Y SUMINISTRADORES DE SERVICIOS PARA VoIP.

6.1. OPERADORAS QUE OFRECEN SERVICIOS IP EN MEXICO.

En México tres operadores han decido apostar por el tan popular Protocolo de Internet. Avantel, Protel y Telmex a finales de 1999 anunciaron que ya estaban a disposición del mercado mexicano, los servicios de comunicaciones basados en IP [21].

6.1.1 PROTEL

La primera telefónica mexicana que libero una red completamente basada en el protocolo IP fue Protel. La infraestructura en cuestión está completamente basada en equipo de CISCO, y se enfoca a la provisión de servicios de valor agregado: redes privadas virtuales (VPN), VPN con acceso telefónico e Internet; estos servicios serán entregados en forma independiente a la larga distancia de voz, que seguirá sobre plataforma conmutada tradicional.

Esta red IP permite ofrecer no solo servicios de calidad, sino que también ofrece la posibilidad de generarlos en forma ágil, con la posibilidad de crear paquetes específicos a la medida del usuario. Esta red tendrá presencia en 35 ciudades del país, y con procesos para optimización del ancho de banda busca hacer a un lado problemas de congestión.

FIG 6.1 Componentes funcionales de la arquitectura AVVID.

6.1.2. AVANTEL.

Haciendo uso de la red IP que tienen, esta compañía lanzó dos nuevos servicios: Avantel IP Plus y Avantel IP Voz.

Avantel IP Plus, mediante un solo acceso, permite a los clientes tener servicio de voz, datos y vídeo sobre IP, lo cual resulta mucho más económico que tener múltiples accesos para distintos servicios. En esta red el cliente paga una renta fija por todas las llamadas que haga dentro de la red IP de Avantel, ya sea que tenga enlazadas varias localidades al servicio, o se comunique con otros clientes que hayan contratado el servicio, o se comunique con otros clientes que hayan contratado el servicio. Así mismo el servicio permite asignar a cada aplicación la prioridad y el ancho de banda necesario para su óptimo desempeño y la velocidad de acceso que el cliente puede solicitar va de 10 Kbps hasta 2.048 Mbps.

Por otro lado, Avantel IP Voz es un servicio de telefonía a través de una red IP. Este, puede tenerse haciendo uso de teléfonos convencionales y para la terminación de llamadas fuera de la red, se entrega a la red conmutada. Si las llamadas son dentro de la misma red, el cliente paga una renta fija; en cambio, por las llamadas que salen a la red pública conmutada, el cobro se realiza por minuto. La gente de Avantel asegura que con este servicio pueden lograrse ahorros hasta de 50% en llamadas internacionales y elimina los gastos por servicio medido.

La tecnología de transporte de la red es ATM (Asynchorous Transfer Mode, Modo de Transferencia Asíncrono) y su velocidad es de 622 Mbps. Ambos servicios llegan al cliente mediante un enlace dedicado que se conecta entre las instalaciones del usuario a la red de Avantel, y todos los servicios (voz, datos, vídeo) se integran en un solo equipo. IP Plus e IP Voz ya están disponibles en 34 ciudades de la República.

6.1.3 TELMEX.

De igual manera, Telmex, la principal empresa de telecomunicaciones de México, lanzó Red Universal Telmex, servicio dirigido a empresas multinacionales que reciben, por parte de sus corporativos, la recomendación de contratar este tipo de servicios. Para poder prestar este tipo de servicio, Telmex aumentó el número de canales de transporte de su red de fibra óptica, la cual mide 32,000 kilómetros y utiliza tecnología de transmisión ATM, cuyo principal proveedor de infraestructura es Cisco.

Red Universal integra los servicios de voz, datos y vídeo que Telmex provee actualmente por separado y ofrece la capacidad para soportar aplicaciones de banda ancha. Asimismo, puede tenerse acceso a la red mediante diversos medios como cobre, radio y fibra. La red incorpora protocolos de comunicaciones como IP, Frame-Relay, ISDN y ADSL. Esta red entró en funcionamiento desde el primero de diciembre de 1999 y se tiene la posibilidad de contratar servicios con un ancho de banda variable, el cual podrá ir desde 56 Kbps hasta 2 Mbps.

6.2 PRINCIPALES COMPAÑIAS QUE OFRECEN SOLUCIONES A NIVEL EMPRESARIA PARA VoIP.

La convergencia de voz y datos en un solo sistema que utilice una infraestructura LAN empresarial para soportar teléfonos IP/ethernet ha tardado mucho en hacerse realidad.

En un estudio realizado por Network Computing de México, entre los diferentes fabricantes, se evaluó la capacidad de las opciones de VoIP de diversos fabricantes para conectar a 10,000 ó más usuarios en una red telefónica privada, se encontró que las únicas compañías capaces de ofrecer soluciones de VoIP a nivel empresarial son: Alcatel, Lucent Technolgies, Cisco Systems y Nortel Networks [42].

6.2.1. CISCO SYSTEMS.

Cisco presenta una solución que permitiría maximizar su retorno de la inversión para una infraestructura convergente, minimizar el costo del cableado y reducir los costos asociados con adiciones y cambios en los teléfonos corporativos.

La solución de Cisco se llama AVVID (Architecture for Voice, Video and Integrated Data), la cual se basa en una arquitectura de tres bloques funcionales distintos: *infraestructura*, como conmutadores y enrutadores; *aplicaciones*, como control de llamadas y mensajería unificada; *y clientes*, como teléfonos IP fijos e inalámbricos, equipo de videoconferencia basado en H.323 y PC de escritorio. La figura 6.2 ilustra los componentes funcionales de la solución de cisco. AVVID es una solución corporativa para la integración de datos, voz y vídeo sobre una protocolo de transporte común, el IP [45].

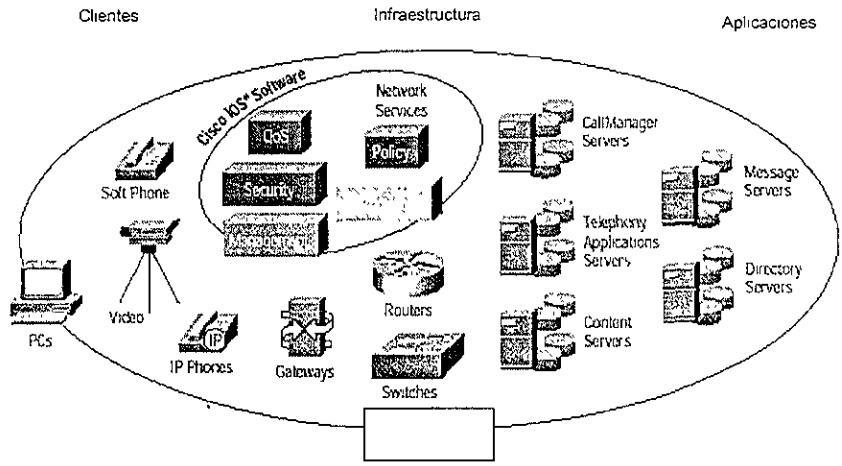

FIG 6.2 Componentes funcionales de la arquitectura AVVID

La versión más reciente del software *CallManager* de Cisco opera en una plataforma Microsoft Windows 2000. Cisco ataca el problema de la estabilidad controlando cuidadosamente el hardware; el software viene cargado en un servidor Compaq y Cisco sólo lo maneja en esa plataforma.

Los servidores Cisco *CallManager* que proporcionan la funcionalidad PBX[1], como se muestra en la figura 6.3, también pueden tener servidores redundantes para mejorar la disponibilidad. Aunque no es común encontrar PBX redundantes, un sistema telefónico que depende de Windows (aunque sea Windows 2000) es importante. El producto de Cisco puede configurarse de modo que un teléfono pueda tener un servidor primario y un secundario. Si uno se cae, el otro se hará cargo automáticamente.

Los teléfonos IP de Cisco tienen todas las funciones de una PBX empresarial, como reenvío de llamadas, timbre diferenciado y conferencias. En un año será posible usar números PIN para monitorear llamadas y controlar el acceso. Los teléfonos pueden recibir alimentación eléctrica a través de equipo de conmutación Cisco desde el gabinete, pero esto todavía no se estandariza. Dado que los teléfonos se pueden comunicar directamente, no se depende tanto de los recursos del servidor una vez establecida la llamada. El sistema de correo de voz que Cisco propuso para implementar transferencia integrada de mensajes tiene varias limitaciones, siendo la más notable la necesidad de usar Microsoft Exchange, además, se requiere un servidor por cada 500-1,000 usuarios de correo de voz.

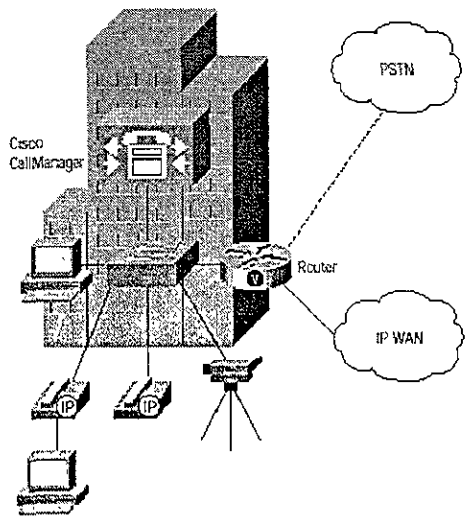

FIG 6.3 Telefonía IP al escritorio.

6.2.2 ALCATEL.

La plataforma Alcatel OmniPCX 4400 es una parte integral de las soluciones OmniSolutions de Alcatel dirigidas a las empresas.

La plataforma OmniPCX 4400 ofrece herramientas empresariales de voz integradas en PC, acceso móvil (Personal Wireless Telephony) a todas las aplicaciones de servidor de voz y datos, gestión basada en Internet de infraestructura de voz y datos, acceso a todos los servicios de red mediante IP, aplicaciones integradas de servidor/directorio, opciones de "navegar y hablar (surf and talk)" y seguridad.

[1] *PBX-Private Branch Exchange, Central privada de conmutación*

La plataforma OmniPCX 4400 está basada en la arquitectura abierta del UNIX, que en general es más estable que los servidores basados en Windows 2000 y NT que usan Cisco y Nortel. Utiliza productos y aplicaciones escalables para crecer con el desarrollo de las necesidades de las empresas, y permite una integración fácil con las tecnologías avanzadas de las adquisiciones de Alcatel, incluyendo los conmutadores de datos de Packet Engines y Xylan, y los centros de contactos de Genesys, así como tecnologías de red y aplicación de cualquier suministrador comprometido con los estándares abiertos.

La OmniPCX 4400 se compone de los siguientes módulos:

- OmniTouch: Call Center (centro de llamadas) integrado.
- OmniDesktop: aplicaciones CTI (Computer Telephony Interface); Teléfonos: Digitales (Reflexes) e IP, mostrado en la figura 6.4.
- OmniMessage: aplicaciones de mensajería de voz.
- OmniVista: gestión de red de voz y datos integrada.

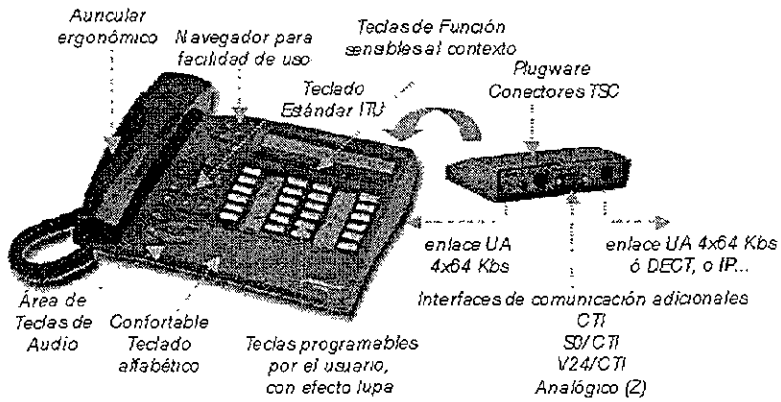

FIG 6.4 Teléfono Reflexes para telefonía IP de Alcatel.

6.2.3 LUCENT TECHNOLOGIES.

Lucent combina la velocidad y potencia de las redes de datos con la calidad y fiabilidad de las redes de voz para crear *MultiVoice,* la solución de Voz sobre IP (VoIP) para los proveedores de servicios. Esta solución ofrece una alternativa costeable a la PSTN, ofreciendo servicios de voz y fax sobre redes IP, tales como la Internet, redes privadas y extranets, para clientes que se encuentren prácticamente en cualquier parte del mundo.

MultiVoice ofrece una infraestructura compatible, escalable, de rápida implementación con arquitectura de clase portadora; funcionalidad para gateways, gatekeepers y clientes PC, calidad comercial telefónica, integración a la red pública conmutada y soporte para administración de red y calidad de servicio (QoS) [45].

MultiVoice VoIP es otro avance importante en el portafolio de soluciones Lucent diseñado, para ayudar a los clientes a construir la siguiente generación de redes.

El conjunto de productos completo, ofrecen soluciones VoIP para proveedores de servicio, las cuales consisten de los siguientes elementos:

1. Gateways MultiVoice, los cuales interconectan las redes de circuitos con las redes de paquetes.
2. Administrador de Acceso MultiVoICE (MVAM), el cual funciona como gatekeeper H.323 ofreciendo control de llamadas, autentificación de usuarios, enrutamiento, traducción de números, programación de flujos de llamadas y registro de los detalles de las llamadas.
3. API MVAM (Interface para programación de aplicaciones), la cual ofrece una interfaz en tiempo real para agregar aplicaciones de Lucent o de terceros al sistema. Las aplicaciones primarias ofrecen servicios de facturación y enrutamiento a bajo costo.
4. Navis Access, ofrece administración y monitoreo de los elementos de la red.
5. Lucent NetworkCare Services, ofrece soporte de primera clase para los clientes, con funciones de diseño, instalación y administración de la red.

6.2.4 NORTEL NETWORKS

El paquete *Succession Communication Server* es la solución que ofrece Nortel Networks a empresas que quieren implementar hoy un sistema de comunicación totalmente abierto, diseñado para enriquecer redes WAN y LAN con el uso de aplicaciones unificadas de voz y datos. La arquitectura distribuida de *Succession* significa que toda o una parte de la solución puede ser fácilmente integrada en la red corporativa existente: LAN, WAN o Intranet.

Succession ofrece la inteligencia que la red IP necesita para administrar conexiones entre puntos extremos, como gateways, terminales IP nativas y clientes IP. El servidor también realiza importantes servicios de control de llamadas, como traducción de direcciones, control de admisión y ancho de banda, autorización de llamadas de terminales y gateways, y administración de zonas.

La solución incluye a *CallPilot,* una aplicación para comunicaciones multimedia definidas por el cliente diseñada para ofrecer mensajería unificada y funcionalidad de comunicaciones a una organización. CallPilot integra múltiples funciones e integra un paquete de software modular que le permite al usuario agregar mensajería de escritorio, de fax y reconocimiento de voz, en cualquier combinación, a un buzón de voz estándar.

Al igual que la solución de Cisco, el producto Succession Communication Server, de Nortel, opera en la plataforma Windows. Sin embargo, ésta se basa en Windows NT 4.0 en lugar de Windows 2000 y requiere 20 servidores para soportar los 10,000 usuarios en la Fase 2. Cisco requiere sólo ocho servidores, y algunos de ellos se usan como respaldos redundantes. Nortel dice que incrementará el número de usuarios soportados por servidor en versiones futuras del software. La solución de transferencia integrada de mensajes y correo de voz de Nortel impresiona más que los productos de los otros fabricantes, pues soporta el mayor

número de productos de correo electrónico: Lotus Notes, Microsoft Exchange y Outlook, Netscape, Novell GroupWise y Qualcomm Eudora IMAP.

Para el acceso de trabajadores a distancia, Nortel propone su teléfono de software i2052. Además de permitir el paso al sistema telefónico desde el hogar, este teléfono ofrece capacidades de pizarrón, transferencia de archivos y compartir aplicaciones.

Hasta aquí se han estudiado las soluciones más importantes, existentes actualmente en el mercado para VoIP, la tecnología VoIP crece poco a poco. Los fabricantes junto con las telefónicas construyen redes que la soporten de manera masiva.

Existe un aspecto muy importante que debe desterrarse; la VoIP no es gratuita. Alguien tiene que pagar la tecnología. Conforme se estandariza el uso, el modelo de negocio también irá cambiando. Para los usuarios residenciales seguirá existiendo la renta mensual y para las empresas la renta de su red privada virtual (encriptada). Habrá, además, tarifas por terminación de llamadas provenientes de otros países y, al igual que internet, algunas compañías ofrecerán accesos de mejor calidad con otro precio.

Algunos corporativos ya tienen instalado su gateway para VoIP pero no lo dicen, quizás por estrategia o por desconocimiento de lo que la ley dicta. "La legislación en México está un poco arcaica y no contempla el tráfico IP", el tráfico internacional que llega a nuestro país paga una tarifa de liquidación (tan sólo de Estados Unidos llegan tres llamadas por una que sale), pero en VoIP esas tarifas no existen porque la frontera se atraviesa en calidad de datos. En otras palabras, es un área gris que no está regulada.

Montar el equipo, rentar el enlace privado, tener ancho de banda suficiente, cuidar que el proveedor ofrezca QoS, que prioritice el paquete de voz en cualquier cola de espera, tener un conmutador apropiado, no infringir la ley usando la red privada para otros fines; son sólo algunos de los puntos por cumplir para hacer realidad la telefonía IP.

CONCLUSIONES

El tráfico de datos tradicionalmente ha sido forzado ha ajustarse a la capacidad de ofrecen la redes telefónicas públicas conmutadas (por ejemplo, el uso de los módems). La Internet ha generado una opción para revertir esta situación, ahora la voz y el fax pueden ser transportados en redes de datos, como es el caso de las redes IP, con la posibilidad de integrar vídeo y otras aplicaciones multimedia como se expuso en el capítulo quinto de este trabajo.

Aunque inicialmente al telefonía IP puede ser vista como una forma de realizar llamadas telefónicas baratas, su verdadera importancia es que ha llegado para revolucionar la forma de ofrecer servicios telefónicos, las aplicaciones emergentes permiten ofrecen servicios multimedia de voz, los cuales no pueden ser proporcionados por las redes telefónicas tradicionales. Aunque en algunos momentos se ha llegado a especular en sí VoIP, podría llegar a reemplazar la telefonía tradicional, hay que aclarar que para que esto suceda primeramente se deberá tener la capacidad de ofrecer un servicio con la calidad ofrecida actualmente por las redes telefónicas públicas, las cuales han tardado más de cien años de desarrollo para llegar a ofrecer la calidad que hoy en día nos prestan.

Por lo que más que pensar en que le éxito de VoIP se tendrá cuando se logre el desplazamiento de las redes telefónicas tradicionales, debemos pensar en el éxito de la tecnología VoIP como una integración de las redes telefónicas con las redes de datos, es decir, que cuando un usuario desee hacer una llamada desde su PC a un teléfono tradicional no tenga que esperar mucho tiempo, y se haga en forma transparente y con la calidad de servicio acostumbrada. Que se tenga la posibilidad de hacer llamadas telefónicas entre PCs, o bien entre teléfonos tradicionales usando las redes IP. Todo esto en un ambiente multimedia.

Es decir la tendencia, es la convergencia entre las redes de voz y datos, en una sola red de paquetes, a través de la cual se podrán transportar voz, fax, datos y vídeo, la cuál se integrará con las redes telefónicas públicas conmutadas, que darán inicio a las denominadas *redes de siguiente generación*.

Las aplicaciones, equipo de conectividad y suministradores de servicios ya están disponibles, en el caso de México, desde 1999 existen redes públicas basadas completamente en el protocolo IP , las cuales ofrecen servicios para transportar voz, datos y vídeo como es el caso de las telefónicas Protel, Avantel y Telmex.

En cuanto a los fabricantes podemos decir que existen un sin fin de ellos, cada uno ofreciendo equipos ya sea para conectividad como es el caso de los enrutadores, gateways, gatekeepers, teléfonos IP, y aplicaciones para VoIP, estos pueden ser desde pequeñas compañías como ECI Telecom , Franklin Telecom., Inter. Tel, VocalTec, Micom, VipNet, Cheap Call, DigiEurope, las cuales se dedican a la fabricación de gateways para VoIP, o bien compañías como Multitud, Vox Pone, Cine Com, Box Top, las cuales se destacan por sus aplicaciones para VoIP, o bien compañías muy grandes que ofrecen soluciones completas, las cuales incluyen desde equipos de interconexión para las redes IP, hardware para VoIP y las aplicaciones

correspondientes, como es el caso de las compañías como Alcatel, Lucent, Nortel y Cisco cuyas soluciones fueron estudiadas en el capítulo sexto.

Esta tesis presenta un estudio los conceptos básicos y las características de las redes IP, los cuales permiten entender el funcionamiento de VoIP, en redes de datos cableadas, pero abre una oportunidad de continuar con un estudio de la características, y funcionamiento de esta tecnología en ambientes de comunicaciones inalámbricas como son: VoIP sobre satélites, o bien VoIP en sistemas de comunicaciones móviles en estudio.

BIBLIOGRAFIA

Y

REFERENCIAS

BIBLIOGRAFIA Y REFERENCIAS DE INTERNET

LIBROS

1. Tanenbaum, Andrew
   Redes de Computadoras
   3a. Edición
   México, Editorial Prentice Hall, 1997
   ISBN 968-880-958-6

2. Murhammer, Martin
   Leek, Kog-Keong,
   IP Network Design Guide
   1a. Edición
   EE.UU. IBM, 1999

3. Raleigh Center
   Local Area Netwok Concepts and Products: LAN Architecture
   1a Edición
   EE.UU. IBM, 1999

4. Black
   Voice over IP
   1a. Edición
   EE.UU. Editorial Prentice Hall, 1998

5. González, Isaura
   Análisis del Sistema de Señalización No. 7 para el transporte de voz mediante el protocolo IP".
   Tesis para obtener el grado de Maestro en Ciencias
   México, CICESE, 2000

6. Covarubias, David
   Conmutación de Paquetes X.25
   Notas para el curso de Redes Locales de Datos
   México, CICESE, 1992

7. Ramonet, María
   Covarrubias, David
   Compresión de Voz en servicios multimedia para redes de comunicaciones de Banda Amplia
   Notas para el curso de Comunicaciones Digitales
   México, CICESE, 1994

TUTORIALES EN LA INTERNET

8. H.323
   Web Proforum Tutorials
   http://www.iec.org

9. A primer on the H.323 series estandar
   DataBeam Corporation
   http://www.databeam.com

10. Calidad de Voz (VQ) en Redes Telelfónicas e IP Convergentes
Web Proforum Tutorials
http://www.iec.com

ARTICULOS

11. Rizzetto Daniele,
Catania Claudio
A voice over IP service architecture for integrated communications
IEEE Internet Computing Magazine
Junio, 1999.

12. Hong Liu,
Mouchtaris Petros
Voice over IP signaling: H.323 and Beyond
IEEE Communications Magazine
Octubre, 2000.

13. Schulzrine Henning,
Rosenberg Jonhan
The IETF Internet Telephony Architecture and Protocols
IEEE Network
Junio, 1999

14. Rizzetto Daniele,
Catania Claudio
Voice over IP Service Architecture for Integrated Communications
IEEE Network
Junio, 1999

15. Li Bo,
Hamdi Mounir
QoS- Enabled Voice Support in the Next Generation Internet: Issues, Existing Approaches and Challenges.
IEEE Communications Magazine
Abril, 2000

16. Hassan Mahbub,
Alfandika Nayandoro
Internet Telephony: Services, Technical Challenges, and Products.
IEEE Communications Magazine
Abril, 2000

17. Keepence Barry
Quality of Service for Voice over IP.
3COM

18. Quality of Service in Enterprise Networks
Extreme Networks
1999

19. Kostas Thomas,
Borella Michael
Real Time Voice Over Packet-Switched Networks

IEEE Networks
Febrero, 1998

20. Tsun-Chieh Chiang,
Janet Douglas
IN Services for Converged (Intenet Telephones)
IEEE Communications Magazine
Junio, 2000

21. G. Uriz e I. De la Torre,
"Las Telefónicas, de lleno sobre IP",
Revista NET @, Volumen 4, Número 89,
Noviembre, 999

PAGINAS DE AYUDA EN LA INTERNET

22. El desarrollo de la telefonía
http://www.telmex.net/mapa/mapa.htm

23. Internet Telephony
http://www.comsoc.org/ni/public/1999/may/

24. Protocolos de Red: Protocolos TCP/IP
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

25. Informática y Sociedad: Protocolos TCP/IP
http://www4.uji.es/~al019803/Tcpip.htm

26. El protocolo IP (Internet Protocolo)
http://es.conectiva.com/doc/libros/online/gar/node23.html

27. Los Principios de las Redes ATM
http://www.disc.ua.es/asignaturas/rc/trabajos/atm/Atm.html,

28. Curso de redes, capítulo 5: El nivel de Red"
h ttp://www.timagazine.net/magazine/0499/redescap5.cfm?tipo=I

29. La gestión de Redes
http://www.timagazine.net/magazine/versecciones.cfm?seccion=Redes%20y%20Comunicaciones&startrow=111

30 Acceso a redes protegidas con privacidad de Microsoft: seguridad en redes privadas virtuales e intranets "
http://www.microsoft.com/latam/technet/articulos/windows2k/msppna/

31. Managed Firewall Services
http://www.sedeco.com.ar/security0/sc0/managed0.htm

32. Inconvenientes de los firewalls
http://www.linux.cu/mirrors/books/conectiva/gs/node899.html

33. SOCKS
http://members.tripod.com/~rebeli0n/tec/socks.txt

34. Como hacer Multidifusión sobre TCP/IP
http://jungla.dit.upm.es/~jmseyas/linux/mcast.como/Multidifusión-Como-1.html#ss1.1

35. MBone: arquitectura y aplicaciones
http://www.timagazine.net/magazine/1198/mbone.cfm?tipo=I

36. Resumen de los mecanismos de QoS y cómo interoperan
http://www.microsoft.com/latam/technet/articulos/windows2k/qosmech/

37. ¿Cuál será la voz de la Red?.
http://www.netarroba.com.mx/informe/informea_128.htm

38. TELEFONIA MOVIL, Las técnicas digitales
http://obelix.umh.es/99-00/teleco_sist/mpcm/public_html/pcm.html#1).-%20Conversión%20A/D

39. Telefonía IP, estado del arte
http://www.ahciet.net/REVISTA/86/default.asp?IR=86&IC=21

40. Protocolos de señalización para el transporte de Voz sobre redes IP
http://www.it.uc3m.es/~jmoreno/articulos/protocolssenalizacion.pdf

41. VoIP: una puerta hacia la convergencia
http://www.cesga.es/ga/default.html?Recetga/Proxrecet.html&2

42. Una tecnología inmadura, voz, sobre IP
http://www.ncm.com.mx/web/articulo.php3?code=188

43. Sistema de comunicaciones NBX 100 de 3Com
http://www.3com.com

44. MultiVoice VoIP Solutions
http://www.lucent.com

45. Architecture for Voice, Video and Integrated Data
http://www.cisco.com

46. Telecomunications News
http://www.hp.com