UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE PROTOCOLO H.323

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:
JOSÉ MANUEL FERNÁNDEZ ANAYA

PROMOCIÓN 1999 – I

LIMA – PERÚ

2002

A mis Padres y Hermanos por el apoyo
que me han brindado.

ESTUDIO DEL PROTOCOLO ESTANDAR H.323

SUMARIO

En este informe se examina la suite de protocolos H.323 que describe un sistema de comunicaciones multimedia en redes de paquetes. Se mencionan los protocolos y las entidades funcionales que se definen en la recomendación y se explican los mecanismos de señalización. También, se tratan temas sobre la actualidad de la recomendación: sus aplicaciones, productos y los desafíos a los que se enfrenta la norma. También se estudia, analiza e implementa un Guardián Gestor de Terminales H.323, basado en software de licencia libre, como una contribución a la difusión de esta tecnología.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

PRÓLOGO

El aumento de las prestaciones previsto en el ámbito Internet y la difusión de soluciones Intranet, las que son un ejemplo de la convergencia de las tecnologías de la comunicación y de la información, constituyen las premisas por la disponibilidad de ambientes en los cuales se puede transmitir de manera integrada voz, vídeo y datos, abasteciendo una vasta gama de servicios de telecomunicaciones, que esta revolucionando las actividades de muchos sectores. La suite de protocolos H.323 es un estándar que define los componentes y dá los lineamientos para la implementación de un ambiente multimedia.

H.323 es un estándar de comunicaciones desarrollado por la Unión Internacional de Telecomunicaciones (ITU), que especifica los componentes, protocolos y procedimientos que proveen servicios de comunicación multimedia (comunicaciones de audio, vídeo y datos en tiempo real), sobre redes de paquetes, incluyendo redes basadas en el protocolo Internet (IP). H323 es parte de la familia de recomendaciones ITU-T llamada H.32x que provee servicios de comunicación multimedia sobre una variedad de redes.

En el capítulo I se desarrolla brevemente y a manera de introducción, la teoría básica de redes de datos, protocolos de comunicación y diversos conceptos afines. En el capítulo II se hace una introducción a la suite de protocolos H.323, describiendo sus componentes principales, formas de señalización y control,

actualidad de la norma, así como de los desafíos y obstáculos a los que se enfrenta. En el capítulo III, ahondamos en el estudio del guardián H.323, por ser éste un componente fundamental en una red multimedia H.323, se estudia sus características obligatorias y opcionales, y sus aplicaciones. En el capítulo IV se hace una breve introducción al software de código abierto OpenH.323, el cual implementa la suite de protocolos H.323; se describe sus diferentes módulos, y se da los lineamientos para la implementación de un Guardián H.323 y de una Unidad de Control multipunto H.323.

CAPÍTULO I

INTRODUCCIÓN

1.1. Las redes de datos.

Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, lectoras de discos compactos o impresoras y que son capaces de realizar comunicaciones electrónicas. Las redes están unidas por cable, líneas de teléfono, ondas de radio, satélite, etc.

1.1.1. Objetivos.

Su objetivo principal es lograr que todos los programas y equipos estén disponible para cualquiera de la red que lo solicite, sin importar la localización física del recurso y del usuario.

Otro de sus objetivos consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, es decir que todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Igualmente la presencia de varios CPU(Central Processing Unit) significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque su rendimiento en general sea menor.

El ahorro económico debido a que los ordenadores pequeños tiene una mejor relación costo / rendimiento, en comparación con la que ofrece las máquinas grandes.

Proporciona un poderoso medio de comunicación entre personas que se encuentran en lugares distantes entre sí.

1.1.2. Clasificación básica de redes.

Red de Área Local (LAN: Local Area Network)

Es una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos ordenadores que disten entre si más de un kilómetro.

Una configuración típica en una red de área local es tener una computadora llamada servidor de ficheros en la que se almacena todo el software de control de la red así como el software que se comparte con los demás ordenadores de la red. Los ordenadores que no son servidores de ficheros reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y tienen software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

Red de Área Metropolitana (MAN: Metropolitan Area Network)

Las redes de área metropolitana cubren extensiones mayores como pueden ser una ciudad o un distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

Redes de Área Extensa (WAN: Wide Area Network)

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Se utilizan cables transoceánicos o satélites para enlazar puntos que están a grandes distancias entre si.

Con el uso de una WAN se puede conectar desde Perú con Japón sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada.

Se utilizan multiplexores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características pueden comunicarse sin problema. El mejor ejemplo de una red de área extensa es Internet.

1.1.3. Cableado de la red.

El Cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN.

Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Tipos de cable más utilizados en redes LAN:

a. Cable de par trenzado sin apantallar (UTP: Unshielded Twisted Pair).
b. Cable de par trenzado apantallado (STP: Shieles Twisted)
c. Cable Coaxial
d. Cable de fibra óptica
e. LAN sin cableado.

a. Cable de par trenzado sin apantallar (UTP)

Este tipo de cable es el más utilizado. La calidad del cable y por ende la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable (ver Tabla 1). Las graduaciones van desde el cable de teléfono, que solo transmite la voz humana a el cable de categoría 5 capaz de transferir 100 Mega bites por segundo.

TIPO	**USO**
Categoría 1	Voz (cable de teléfono)
Categoría 2	Datos a 4 Mbps (Local Talk)
Categoría 3	Datos a 10 Mbps (Ethernet)
Categoría 4	Datos a 20/16 Mbps (Token Ring)
Categoría 5	Datos a 100 Mbps (Fast Ethernet)
Categoría 6	Datos a 1000 Mbps (Gigabit Ethernet)

Tabla 1. Categorías UTP

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos.

Se recomienda el uso de cables de categoría 3 a 5 para la implementación de redes en PYMES (Pequeñas y Medianas Empresas).

El conector estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. La sigla RJ se refiere al Estándar Registered Jack, creado por la industria telefónica. Este estándar se encarga de definir la colocación de los cables en su pin correspondiente.

b. Cable de par trenzado apantallado (STP)

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este tipo de problemas existe un tipo de cable UTP que lleva apantallamiento, esto significa protección contra interferencias eléctricas. Este tipo de cable es usado por lo general en redes de topología Token Ring.

c. Cable Coaxial

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.

Aunque la instalación de cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias, también es posible conectar distancias mayores que con los cables de par trenzado (ver Tabla 2).

Existen dos tipos de cable coaxial:

- Cable coaxial fino (thin coaxial).
- Cable coaxial grueso (thick coaxial).

Es posible escuchar referencias sobre el cable coaxial fino como thinnet o 10Base2. Estos hacen referencia a una red de tipo Ethernet con un cable coaxial fino. Donde el 2 significa que el mayor segmento es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología BUS.

También se referencia el Cable Coaxial grueso como thicknet o 10Base5. Este hace referencia a una red de tipo Ethernet con un cableado coaxial grueso, donde el 5 significa que el mayor segmento posible es de 500 metros (ver Tabla 2). El cable coaxial es muy popular en las redes con topología de BUS. El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar. El conector más usado para el cable coaxial es el conector BNC(Bayone-Neill-Concelman).

d. Cable de Fibra Óptica

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar.

Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado (ver Tabla 2). Además la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencias o servicios interactivos. El costo es similar al cable coaxial o al cable UTP pero las dificultades de instalación y modificación son mayores. En algunas ocasiones escucharemos 10BaseF como referencia a este tipo de cableado; estas siglas hablan de una red Ethernet con cableado de fibra óptica.

Las principales características son:

- El aislante exterior está echo de teflón o PVC (Policloruro de vinilo).
- Fibras Kevlar (Tecnología de protección) ayudan a dar fuerza al cable y hace más difícil su ruptura.
- Se utiliza un recubrimiento de plástico para albergar a la fibra central.
- El centro del cable está echo de cristal o de fibras plásticas.

ESPECIFICACION	TIPO DE CABLE	LONGITUD MÁXIMA
10 base t	UTP	100 metros
10 BASE 2	Thin Coaxial	185 metros
10 BASE 5	Thick Coaxial	500 metros
10 Base F	Fibra Óptica	2000 metros

Tabla 2. Resumen de cables

e. LAN sin cableado

No todas las redes se implementan sobre un cableado, algunas utilizan señales de radio de alta frecuencia o haces infrarrojos para comunicarse. Cada punto de la red posee una antena desde la que emite y recibe. Para largas distancias se pueden utilizar teléfonos móviles o satélites.

Este tipo de conexión está especialmente indicada para su uso con portátiles o para edificios viejos en los que es imposible instalar un cableado.

Las desventajas de este tipo de redes son su alto costo, su susceptibilidad a las interferencias electromagnéticas y la baja seguridad que ofrecen. Además son más lentas que las redes que utilizan cableado.

1.2. Protocolos de comunicaciones.

Los protocolos son como reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma.

En esta sección describiremos dos tipos de protocolos:

- Protocolos de bajo nivel, y
- Protocolos de red.

1.2.1. Protocolos de bajo nivel

El protocolo de bajo nivel es, en cierto modo, la forma en que las señales se transmiten por el cable, transportando tanto datos como información y los procedimientos de control de uso del medio por los diferentes nodos.

Los protocolos de bajo nivel controlan el acceso al medio físico, lo que se conoce como MAC(Media Access Control) y, además, parte del nivel de transmisión de datos, ya que se encargan también de las señales de temporización de la transmisión.

Sobre todos los protocolos de bajo nivel MAC, se asientan en los protocolos de control lógico del enlace o LLC(Logical Link Control), definidos en el estándar IEEE 802.2.

Los protocolos de bajo nivel más utilizados son:

a. Ethernet.
f. Token Ring.
g. Token Bus.
h. FDDI.
i. CDDI.
j. HDLC.
k. Frame Relay.
l. ATM.

a. ETHERNET.

El protocolo de red Ethernet fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente, IEEE ha definido el estándar Ethernet 802.3. La forma de codificación difiere ligeramente en ambas definiciones. Es el método de conexión más extendido en la actualidad. La velocidad de transmisión de datos en Ethernet es de 10Mbits/s.

En el caso del protocolo Ethernet/IEEE 802.3, el acceso al medio se controla con un sistema conocido como 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 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 no escogerán el mismo tiempo de espera.

Existen cuatro tipos de Ethernet:

10base5: Es la Ethernet original. Utiliza cable coaxial grueso y transceptores insertados en él. La longitud máxima del bus es de 500 m con 100 estaciones por segmento, a una distancia mínima de 2.5 m entre puntos de inserción de los transceptores.

10base2: El costo de instalación del coaxial y los transceptores de las redes 10base5 las hacía prohibitivas para muchas empresas, lo cual indujo la utilización de un cable más fino y, por tanto más barato, que además no necesitaba transceptores insertados en él. Por esto, también se le conoce Ethernet fino o cheaper-net(red barata). La longitud máxima es de 185 metros y un máximo de 30 estaciones por segmento.

10baseT: El costo del cable coaxial fino sigue siendo mayor que el del cable telefónico de pares trenzados. Como en la mayoría de los edificios el tendido de la líneas de teléfono estaba hecho con cables de cuatro pares y el teléfono solo utiliza uno, se diseñó un modo de transmitir las señales Ethernet de 10 Mbits/s sobre dos pares trenzados en segmentos de hasta 100 metros. Esta facilidad de aprovechar los tendidos existentes ha dado gran popularidad a este tipo de Ethernet, siendo el más utilizado en la actualidad. Este tipo de Ethernet tiene una topología de estrella.

10baseF: Es la especificación Ethernet sobre fibra óptica. Los cables de cobre presentan el problema de ser susceptibles tanto de producir como de recibir interferencias. Por ello, en entornos industriales o donde existen equipos sensibles a las interferencias, es muy útil poder utilizar la fibra. Normalmente, las redes Ethernet de fibra suelen tener una topología en estrella.

En la actualidad han surgido nuevas especificaciones basadas en Ethernet que permiten transmitir datos a mayor velocidad como son:

Switched Ethernet: Esta especificación utiliza concentradores de red con canales de comunicación de alta velocidad en su interior, con una arquitectura similar a las centrales de teléfonos, que conmutan(switch) el tráfico entre las estaciones conectados a ellos. Esto permite que cada estación disponga de un canal de

10Mbits/s, en lugar de un único canal para todas ellas. La ventaja de esta especificación es que utiliza los mismos cables y tarjetas de red que el 10baseT, sustituyéndose sólo los concentradores.

Fast Ethernet/IEEE 802.3u (Ethernet de 100 Mbits/s): Esta especificación permite velocidades de transferencia de 100 Mbits/s sobre cables de pares trenzados, directamente desde cada estación. Requiere la sustitución de los concentradores y las tarjetas de red de las estaciones. El estándar 802.3u describe la especificación Fast Ethernet 100BASE-X.

Gigabit Ethernet/IEEE 802.3z/802.3ab (Ethernet de 1000 Mbits/s): Esta especificación permite velocidades de transferencia de 1000 Mbits/s sobre fibra óptica o cables de pares trenzados. El estándar 802.3z describe la especificación el sistema Gigabit Ethernet de fibra óptica 1000BASE-X y el estándar 802.3ab describe la especificación el sistema Gigabit Ethernet de par trenzado 1000BASE-T.

10GigabitEthernet/IEEE 802.3ae (Ethernet de 10 Gbits/s): Esta especificación permite velocidades de transferencia de 10 Gbits/s sobre fibra óptica.

b. TOKEN RING.

Las redes basadas en protocolos de paso de testigo(token passing), basan el control de acceso al medio en la posesión de un testigo. Este es un paquete con un contenido especial que permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el testigo va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el testigo a la siguiente.

Las redes de tipo token ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbits/s.

Existen redes token ring de 16 Mbits/s, pero no están definidas en ninguna especificación de IEEE.

c. TOKEN BUS.

Es una especificación de red basada en control de acceso al medio por paso de testigo con topología de bus.

d. FDI (Fiber Distributed Data Interface).

. Es una especificación de red sobre fibra óptica con topología de doble anillo, control de acceso al medio por paso de testigo y una velocidad de transmisión de 100 Mbits/s. Esta especificación estaba destinada a sustituir a la Ethernet pero el retraso en terminar las especificaciones por parte de los comités y los avances en otras tecnologías, principalmente Ethernet, la han relegado a unas pocas aplicaciones como interconexión de edificios.

e. CDDI (Copper Distributed Data Interface).

Es una modificación de la especificación FDDI para permitir el uso de cables de cobre de la llamada categoría cinco, cables de alta calidad específicos para transmisión de datos, en lugar de fibra óptica.

f. HDLC (High Level Data Link Control).

Es la especificación de red utilizada principalmente en las transmisiones por líneas telefónicas para comunicaciones de datos, como pueden ser las líneas punto a punto y las redes públicas de conmutación de paquetes.

g. FRAME RELAY .

Frame Relay (Paso de tramas) puede ser tanto un servicio prestado por una compañía telefónica como una especificación de red privada. Este sistema de transmisión permite velocidades de 56 kbits/s, n x 64 kbits/s o 2 Mbits/s. El servicio se puede establecer con líneas punto a punto entre ruteadores o por medio de una conexión con una red pública.

Un parámetro básico del servicio Frame Relay es el CIR (Commited Information Rate, Tasa de información asegurada), el cual se utiliza para facturar las conexiones a redes públicas. Este valor se basa en la naturaleza aleatoria de la transmisión de datos, ya que no todas las estaciones transmiten al mismo tiempo, con lo cual, la suma de la capacidad, en bits/s, de los canales de cada una de ellas, puede ser superior a la capacidad de los canales de interconexión. Cada estación puede transmitir toda la información que permita el canal, pero, en caso de que la red se congestione, sólo podrá transmitir, en principio, la cantidad permitida por el CIR.

h. ATM (Asynchronous Transfer Mode).

Modo de transferencia asíncrono, es la especificación más reciente y con mayor futuro. Permite velocidades de a partir de 156 Mbits/s llegando a superar los 560 Mbits/s. Se basa en la transmisión de pequeños paquetes de datos de 56 bytes,

con una mínima cabecera de dirección que son conmutados por equipos de muy alta velocidad. La gran ventaja de esta especificación es la capacidad que tiene para transmitir información sensible a los retardos como pueden ser voz o imágenes digitalizadas combinada con datos, gracias a la capacidad de marcar los paquetes como eliminables, para que los equipos de conmutación puedan decidir que paquetes transmitir en caso de congestión de la red.

1.2.2. Protocolos de red

El protocolo de red determina el modo y organización de la información (tanto datos como controles) para su transmisión por el medio físico con el protocolo de bajo nivel. Los protocolos de red mas comunes son:

a. IPX/SPX.
b. DECnet.
c. X.25.
d. TCP/IP.
e. AppleTalk.
f. NetBEUI.

a. IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange).

Es el conjunto de protocolos utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

b. DECnet (Digital Equipement Corporation net).

Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles. Está muy extendido en el mundo académico.

Uno de sus componentes, LAT (Local Area Transport), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

c. X.25.

Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

d. TCP/IP (Transmision Control Protocol/ Internet Protocol).

Este no es un protocolo, si no un conjunto de protocolos, que toma su nombre de los dos más conocidos: TCP (Transmision Control Protocol) e IP (Internet Protocol). Esta familia de protocolos es la base de la red Internet, la mayor red de ordenadores del mundo. Por lo cual, se ha convertido en el más extendido.

e. AppleTalk.

Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con

gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

LocalTalk: Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida pero es adecuada para los servicios que en principio se requerían de ella, principalmente compartir impresoras.

Ethertalk: Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicaciones como la transferencia de ficheros.

Tokentalk: Es la versión de Appletalk para redes Token Ring.

f. NetBEUI (NetBIOS Extended User Interface).

Interfaz de usuario extendido para NetBIOS, es la versión de Microsoft del NetBIOS (Network Basic Input/Output System), que es el sistema de enlazar el software y el hardware de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.

1.3. Revisión breve de TCP/IP.

TCP/IP más que un protocolo es un conjunto de protocolos. Se ha convertido en el estándar de intercomunicación de redes de área extensa y es el único protocolo de enlace y transporte permitido en Internet.

La idea general de conectar una red con ordenadores diferentes partió de las investigaciones llevadas a cabo en la Defense Advanced Research Projects Agency

(DARPA). En el ámbito de esta investigación, DARPA desarrollo el conjunto de protocolos TCP/IP para establecer comunicaciones entre redes e implantó una red que recibió el nombre de ARPAnet, que más tarde se convirtió en Internet. El conjunto de protocolos TCP/IP define los formatos y normas utilizados en la transmisión y recepción de información con independencia de cualquier tipo de hardware determinado u organización de red. A pesar de los protocolos se desarrollaron para la Internet, TCP/IP se ha convertido en el estándar de hecho ya que muchas organizaciones publicas y privadas lo utilizan para su conectividad.

El éxito inicial de TCP/IP fue debido a su inclusión en las diferentes variedades del sistema operativo UNIX y fue impulsado porque su implantación resulta más cómoda y económica que los protocolos equivalentes. TCP/IP emplea un modelo de enrutamiento basado en "datagramas" (paquetes) en lugar de circuitos virtuales. TCP/IP brinda a los arquitectos de sistemas e ingenieros de comunicaciones una independencia del hardware utilizado.

1.3.1. Conjunto de protocolos TCP/IP

En líneas generales, el conjunto de protocolos TCP/IP se corresponde con el modelo de comunicaciones de red definido por la International Organization for Standardization (ISO). Este modelo se denomina modelo de referencia Interconexión de sistemas abiertos (OSI). El modelo OSI describe un sistema de redes ideal que permite establecer una comunicación entre procesos de capas distintas y fáciles de identificar. En el host, las capas prestan servicios a capas superiores y reciben servicios de capas inferiores. La Figura 1 muestra las siete capas del modelo de

referencia OSI y su correspondencia general con las capas del conjunto de protocolos TCP/IP.

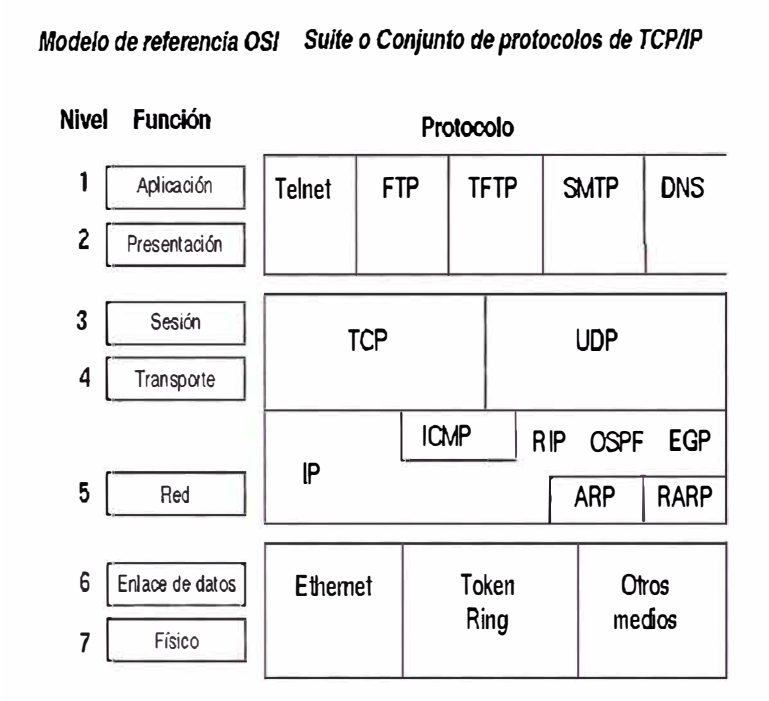

Figura 1. Modelo de referencia OSI

El sistema al determinar capas permite a los programadores concentrar sus esfuerzos en las funciones de una capa determinada. No es necesario que creen todo los mecanismos para enviar información a lo largo de la red. Sólo tienen que saber los servicios que el software debe proporcionar a la capa superior, los servicios que las capas inferiores pueden proporcionar al software y qué protocolos del conjunto proporcionan estos servicios.

En la Tabla 3 se enumeran los protocolos más comunes del conjunto de protocolos TCP/IP, los servicios que proporcionan.

Protocolos TCP/IP	Servicio
Protocolo Internet (IP)	Proporciona servicios para la entrega de paquetes (encaminamiento) entre nodos.
Protocolo de control de mensaje Internet (ICMP)	Regula la transmisión de mensajes de error y control entre los host y las Pasarelas.
Protocolo de resolución de direcciones (ARP)	Asigna direcciones Internet a direcciones físicas.
Protocolo de resolución de direcciones invertidas (RARP)	Asigna direcciones físicas a direcciones Internet.
Protocolo de control de transmisión (TCP)	Proporciona servicios de envío de flujos fiables entre los clientes.
Protocolo de datagrama de usuario (UDP)	Proporciona servicio de entrega de datagramas no fiable entre clientes.
Protocolo de transferencia de archivos (FTP)	Proporciona servicios de nivel de aplicación para la transferencia de archivos.
TELNET	Proporciona un método de emulación de terminal.
Protocolo de información de encaminamiento (RIP)	Permite el intercambio de información de encamina-miento de vectores de distancia entre ruteadores.
Protocolo Abrir la vía más corta primero (OPSF)	Permite el intercambio de información de encamina-miento de estado del enlace entre ruteadores.
Protocolo de Pasarela externa (EGP)	Permite el intercambio de información de encamina-miento entre ruteadores externos

Tabla 3. Protocolos TCP más comunes

1.3.2. Descripción general del uso de TCP/IP

Las aplicaciones que se desarrollan con TCP/IP, normalmente, usan varios protocolos del conjunto. La suma de las capas del conjunto de protocolos se conoce también como la pila (stack) de protocolo. Las aplicaciones definidas por el usuario se comunican con la capa superior del conjunto de protocolos. La capa de nivel superior del protocolo del computador de origen traspasa la información a las capas inferiores de la pila, que a su vez la pasan a la red física. La red física traspasa la información al ordenador de destino. Las capas inferiores de la pila de protocolo del ordenador de destino pasan la información a las capas superiores, que a su vez la pasan a la aplicación de destino.

Cada capa del conjunto de protocolos TCP/IP tiene varias funciones; estas funciones son independientes de las otras capas. No obstante, cada capa espera recibir determinados servicios de la capa inferior y cada capa proporciona ciertos servicios a la capa superior.

La Figura 2 muestra las diferentes capas del conjunto TCP/IP. Cada capa de la pila de protocolo del ordenador de origen se comunica con la misma capa del ordenador de destino. Las capas que se encuentran al mismo nivel en el ordenador de origen y de destino son pares. Asimismo, la aplicación del ordenador de origen y la del de destino también son pares. Desde el punto de vista del usuario o programador, la transferencia de paquetes se efectúa directamente de una capa par a otra.

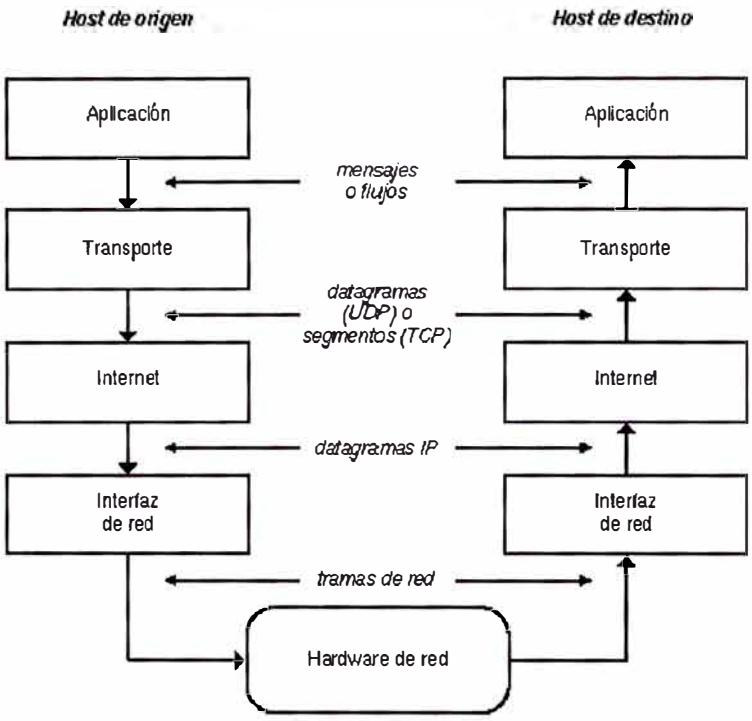

Figura 2. Capas de los protocolos TCP/IP

El proceso que utiliza una aplicación para transferir el contenido de un archivo es el siguiente:

a. La capa de la aplicación envía un flujo de bytes a la capa de transporte del ordenador de origen.

b. La capa de transporte divide el flujo en segmentos TCP, asigna un encabezado con un número de secuencia al segmento en cuestión y transmite este segmento a la capa de Internet (IP). Se calcula la suma de comprobación.

c. La capa de IP crea un paquete con parte de los datos que contiene el segmento TCP. La capa de IP añade al paquete un encabezado que indica las direcciones IP de origen y de destino. Esta capa también determina la dirección física del ordenador de destino o los ordenadores que actúan como intermediarios hasta el host de destino. Entonces, envía el paquete y la dirección física a la capa de enlace de datos. Se vuelve a calcular la suma de comprobación.

d. La capa de enlace de datos transmite el paquete IP en la sección de datos de una trama de enlace de datos al ordenador de destino. Si el ordenador de destino actúa como intermediario, el paso 3 volverá a repetirse hasta que se alcance el destino final.

e. Cuando se alcanza el ordenador de destino, la capa de enlace de datos descarta el encabezado del enlace y envía el paquete IP a la capa de IP.

f. La capa de IP verifica el encabezado del paquete. Si la suma de comprobación del encabezado no coincide con la calculada por dicha capa, el paquete se ignora.

g. Si las sumas coinciden, la capa IP descarta el encabezado y envía el segmento TCP a la capa TCP correspondiente. Esta capa comprueba el número de secuencia para determinar si el segmento, es el segmento correcto de la secuencia.

h. La capa TCP calcula una suma de comprobación para los datos y el encabezado TCP. Si la suma no coincide con la suma transmitida con el encabezado, la capa TCP descarta el segmento. Si la suma coincide y el segmento está en la secuencia correcta, la capa TCP envía un reconocimiento al ordenador de destino.

i. La capa TCP descarta el encabezado TCP y transfiere los bytes del segmento que acaba de recibir a la aplicación.

j. La aplicación que se encuentra en el ordenador de destino recibe un flujo de bytes como si estuviera conectado directamente a la aplicación del ordenador de origen.

1.3.3. Direccionamiento IP

TCP/IP lleva asociado una serie de conceptos a aclarar:

Hosts: son cada uno de los dispositivos conectados a la red. Un host puede ser un servidor, un puesto de la red, un servidor de impresoras, un ruteador, etc.

Dirección: es un código que identifica a cada dispositivo dentro de la red.

Red: Conjunto de hosts agrupados bajo una misma dirección de red.

Subred: conjunto de hosts dentro de una red.

El protocolo IP establece un sistema de direcciones que identifica a cada host de forma única. Todos los equipos y dispositivos de comunicaciones en una red TCP/IP han de tener una dirección IP única para poder establecerse la comunicación.

Cada vez que se envía un paquete a la red ésta determina el camino seguirá hasta su destino.

La dirección IP es un número de 4 bytes (32bits) que se representa como 4 enteros entre 0 y 255.

Cada dirección IP de 4 bytes se divide en dos partes:

- Una porción de la red, que identifica la red
- Una porción del Host, que identifica el nodo

Las direcciones IP se dividen en tres clases según los dos bits más importantes de los cuatro primeros bytes. Esto se hace para que los ruteadores puedan extraer la porción de la red de la dirección de manera eficiente.

A pesar de la clase de dirección, todos los nodos de una red única comparten la misma porción de la red; cada nodo tiene una porción única.

Dirección IP de un host 194.224.78.16

Para facilitar el encaminamiento de los datagramas, las direcciones IP se agrupan en redes. Una red es un grupo de direcciones IP que tienen en común una parte de su dirección. La dirección IP anterior hace referencia al host número 16 de la red 194.224.78.0

Dirección IP de una red 194.224.78.0

Por convenio la dirección de una red se obtiene a partir de los bits que tiene en común todas las direcciones de ella, con los demás bits puestos a cero. Dado que cada dirección IP se compone de 4 números enteros entre 0 y 255, la red comprende todas las direcciones desde 194.224.78.1 hasta 194.224.78.254. El número 0 se reserva para el número de la red y el número 255 es la dirección de difusión de la red, cualquier datagrama enviado a la dirección de difusión será recibido y procesado por todos los hosts de la red.

Existen unas clases de redes predeterminadas, cada dirección tiene una máscara que se determina en función de la dirección de la red. Para conocer, con exactitud, que parte de la dirección corresponde a la dirección de la red y que parte pertenece a la dirección del host, es necesario ver la máscara (ver Tabla 4).

	Dirección Red	**Máscara**	**Hosts**
Red de Clase A	10.0.0.0	255.0.0.0	16.777.214 Hosts
Red de Clase B	144.102.0.0	255.255.0.0	65.534 Hosts
Red de Clase C	194.224.78.0	255.255.255.0	254 Hosts

Tabla 4. Ejemplos de redes

Direcciones de Clase A

Una dirección IP de la clase A consiste en una porción de la red de un byte seguido por una porción del Host de 3 bytes. El bit de mayor orden del byte de la porción de red se define siempre a 0. Por lo tanto se dispondrán de un total de 126 redes de la Clase A (1 a 126) y con más de 16 millones de nodos por red, (las redes entre 0 y 127 están reservadas)

Por ejemplo,

n = dirección de red (en bits) y h = dirección de host (en bits)

Clase A 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Direcciones de Clase B

Una dirección IP de la clase B consiste en una porción de la red de dos bytes seguido por una porción del Host de 2 bytes. Los dos bits de orden superior de la porción de red se definen siempre a 10. Por lo tanto se dispondrán de aproximadamente 16.000 redes de la Clase B (desde 128.x a 191.x) y con más de 65.000 nodos por red.

Por ejemplo,

n = dirección de red (en bits) y h = dirección de host (en bits)

Clase A 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Direcciones de Clase C

Una dirección IP de la clase C consiste en una porción de la red de tres bytes seguido por una porción del Host de 1 bytes. Los tres bits de orden superior de la porción de red se definen siempre a 110. Por lo tanto se dispondrán de aproximadamente 2 millones de redes de la Clase C (desde 192.x.x a 223.x.x) y con 254 nodos por red.

Por ejemplo,

n = dirección de red (en bits) y h = dirección de host (en bits)

Clase A 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Existen empresas y grupos de usuarios cuyas necesidades no llegan a los 254 hosts. Para atender las necesidades de estos grupos mas reducidos se crean subredes que segmentan las clases A, B o C (ver Tabla 5).

Dirección Red	**Máscara**	**1er Host**	**Ultimo Host**
194.224.78.0	255.255.255.0	194.224.78.1	194.224.78.254
194.224.78.128	255.255.255.128	194.224.78.129	194.224.78.254
194.224.78.240	255.255.255.254	194.224.78.241	194.224.78.242

Tabla 5. Ejemplos de subredes

Direcciones IP Reservadas

Las reglas de direccionamiento IP reservan los siguientes tipos de direcciones IP para propósitos especiales:

Direcciones de la red. Estas son las direcciones IP en las que la porción del Host está definida por ceros. Por ejemplo la dirección 129.47.0.0 es la dirección o numero de red correspondiente a una red Clase B.

Direcciones de difusión general. Son direcciones en las que la porción del Host está definida en todos(255). Un paquete con una dirección de difusión general se destina a todos los nodos de la red. Por norma general, ningún nodo tiene asignado una porción del Host formada sólo por unos.

Direcciones de retorno de bucle. La dirección de la red 127.0.0.0, y todas las direcciones del Host en la red, por ejemplo, 127.0.0.1, son reservadas.

Direcciones reservadas. Son direcciones en las que la porción de red está formada por ceros o todos(255)

Creación de subredes

Una red Internet (en una dirección de la red Internet única) puede dividirse en una o más redes más pequeñas. En la parte inferior están listadas algunas de las razones para dividir la red:

Usar varios medios. Puede ser imposible, inconveniente o demasiado caro conectar todos los nodos en un medio de la red única cuando estos nodos están demasiado lejos o conectados a un medio diferente.

Reducir la congestión. El tráfico entre nodos en una red única usa un ancho de banda de la red. Como resultado, se requieren más anchos de banda cuando el usuario tiene más nodos. La división de los nodos en varias redes reduce el número de nodos de la red. Si los nodos de una red de tamaño pequeño se comunican principalmente con otros nodos de la misma red, el nivel de congestión se reduce.

Reducir el uso del CPU. La reducción del uso de CPU los nodos conectados es similar a la reducción de la congestión. Más nodos en la red causan más difusiones generales en la red. Incluso si una difusión general no se envía a un nodo en particular, cada nodo de una red debe reaccionar ante la misma antes de decidir si debe aceptar o descartarse.

Aislar una red. La división de una red de mayor tamaño en redes más pequeñas, limita el impacto de uno de los problemas de la red sobre otra. Entre estos problemas se pueden incluir el error de hardware de la red, como una interconexión Ethernet abierta, o errores de software, como una operación de emisión confusa.

Mejorar el nivel de seguridad. En un medio de red de difusión general como es Ethernet, cada nodo de una red tiene acceso a todos los paquetes enviados a la misma. Si se permite sólo un tráfico de red sensitivo en una red, otros monitores de red pueden evitar el acceso a éste tipo de tráfico.

Hacer uso eficiente del espacio de la dirección IP. Si está asignando un número de red Clase A o B y tiene varias redes físicas pequeñas, puede dividir el espacio de dirección IP en varias subredes IP y asignarles redes físicas individuales. Con el uso de este método, no necesita conseguir más números de redes IP por cada red física.

Máscaras y direcciones de subredes

Cada subred funciona como si fuera una red independiente. Para redes remotas, sin embargo, las subredes aparecen colectivamente como redes discretas y únicas. Esto significa que la red local sólo necesita una dirección de red IP y estas redes remotas no necesitan poner atención en la ubicación de un nodo en una subred particular.

La comunicación entre un nodo en una subred local y un nodo en una subred diferente es parecida a la comunicación entre nodos de dos redes diferentes. Para un usuario, el encaminamiento entre subredes es transparente. Internamente, el software IP reconoce cualquier dirección IP que esté destinada a una subred y envía estos paquetes al ruteador de la misma.

Al igual que en la comunicación entre redes, la información del encaminamiento para la comunicación de la subred entre subredes se mantiene en la tabla de encaminamiento (por IP) para cada nodo o ruteador. Sin embargo, en el caso de las subredes, dicha información está formada por la dirección de la red y la dirección de la subred.

Cuando una red se distribuye en varias subredes, la porción del Host de la dirección IP se divide en dos partes, al igual que la dirección IP se divide en dos partes (4 bytes en total). La porción de la dirección del Host especifica la subred de la red IP y el nodo de dicha subred.

Por ejemplo, si una red tiene la porción de la dirección de la red Clase B 129.47, el resto de dicha dirección se puede dividir en direcciones de subred y del Host. Esta división está controlada por la red local a fin de obtener una mayor

flexibilidad en el funcionamiento de la red a nivel local. Por ejemplo, la dirección de subred puede contener cuatro bits de los dos bytes restantes. Esto permite 15 subredes, cada una con 4094 nodos. En otro ejemplo, la dirección de la subred puede contener ocho bits, lo que permite usar 254 subredes (una dirección de subred de todos los unos no es válida), cada una con 254 nodos.

Una máscara de subredes indica cómo se divide la porción del Host de una dirección IP en direcciones de subredes y porciones de dirección del Host local. La máscara de la red está representada por un número de 32 bits en el que las porciones de dirección de red y subred están formadas por una dirección IP completa y todas las del Host por ceros. Por ejemplo, con una porción de la dirección de la red IP de Clase B de 129.47 y una dirección de la subred de 4 bits, la máscara de subred constará de 20 unos y 12 ceros. En resumen, una máscara de subred amplía la porción de la dirección de la red de una dirección IP local. La siguiente figura muestra ejemplos de direcciones de redes IP, la relación con la máscara de subred y con la correspondiente subred.

El DNS

El servicio de nombres de dominios es un servicio de directorios basado en una base de datos distribuida. La función básica del servicio de nombres de dominios es la de facilitar el acceso a los recursos y servicios de Internet a través de nombres fácilmente recordables, en lugar de direcciones numéricas. Establece además un nivel de indirección que permite cambiar servicios de una máquina a otra o distribuir la carga de acceso a varios servidores sin necesidad de redistribuir o cambiar la dirección numérica.

1.3.4. UDP y TCP

UDP (User Datagram Protocol)

El protocolo IP proporciona tres definiciones muy importantes:

- Define la unidad básica para la transferencia de datos utilizada a través de una red TCP/IP

- Realiza la función de ruteo, indicando por donde deben ser enviados los datos.

- Incluye un conjunto de reglas que define cuando los paquetes enviados por la red deben ser descartados. Define las condiciones de error en el envío y recepción de paquetes.

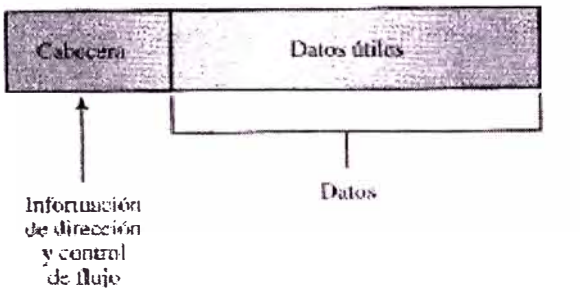

Figura 3. Estructura básica de un paquete

La unidad de datos en TCP/IP se denomina datagrama (ver Figura 3) y consta de un encabezado y de un área de datos. La cabecera del datagrama lleva una serie de datos como son las direcciones IP del emisor como del receptor, así como unos indicadores de tipo de servicio, protocolo y tiempo de vida. La red física trata al datagrama como si fuera un dato incluyendo la cabecera dentro de la parte de datos de la trama.

TCP/IP por lo tanto es capaz de transmitir datagramas IP entre hosts, donde cada datagrama es enviado a través de la red, basándose en la dirección IP del

destino. En el Protocolo Internet, una dirección hace referencia a un host, pero no hace ninguna distinción respecto a que usuario o que aplicación recibirá el datagrama. El protocolo UDP es el que se encarga de distinguir entre los diferentes destinos que un datagrama puede tener en un mismo host, permitiendo a varias aplicaciones que se ejecutan en una misma computadora envíen y reciban datagramas de forma independientes. El UDP proporciona puertos de protocolos utilizados para distinguir a que aplicación se dirige un datagrama.

TCP (Transmision Control Protocol)

El protocolo de control de transmisión especifica el formato de los datos y los acuse de recibo que intercambian dos computadoras para lograr una transferencia confiable, así como los procedimientos que la computadora utiliza para asegurarse que los datos llegan de una manera correcta. Al mismo tiempo especifica como el software distingue el destino correcto dentro de los posibles destinos dentro de una misma máquina. También especifica cómo dos computadoras inician una transferencia de flujo TCP y como se ponen de acuerdo cuando se completa.

1.3.5. Aplicaciones TCP/IP, servicios en Internet

Puertos

Cada host en Internet tiene una dirección única, esto significa, que todos los usuarios que desean conectar con un determinado ordenador han de dirigirse a la misma dirección. Dado el gran número de usuarios conectados a Internet, es probable que cualquier host con un servicio popular sea accedido por múltiples usuarios de forma simultánea. También es frecuente encontrar que un solo ordenador con una dirección IP se hace responsable de diversas tareas o servicios como Correo Electrónico, Servicio de Páginas Web, Servicio de transferencia de Ficheros, etc. Necesitamos un método para distinguir los flujos de información de cada tarea, usuario y servicio. Para este fin se ha definido el puerto en la especificación del protocolo TCP.

Cada servicio como Web, Correo, FTP, o DNS, tiene un puerto asignado. Cada comunicación con una dirección IP de dirige al puerto predeterminado en función de la aplicación (ver Tabla 6).

Protocolo	**Puerto Por Defecto**
FTP	21
SMTP	25
HTTP	80
POP	110

Tabla 6. Servicios más conocidos

Si deseamos establecer una sesión de transferencia de ficheros, a través de protocolo FTP nuestro programa ha de dirigirse al puerto 21.

Correo Electrónico

El correo electrónico, es un sistema que permite la transmisión e intercambio de mensajes en un formato informatizado.

Cada receptor de correo tiene una dirección única que le identifica en la red. Conociendo su dirección cualquier usuario de Internet en cualquier parte del mundo puede enviar un mensaje con la misma facilidad que envía un mensaje a otro usuario en su red local. Las direcciones de correo electrónico están divididas en dos partes separadas por el carácter arroba "@" (ver Tabla 7).

Identificación de usuario	**dominio**	**Dirección de correo electrónico**
eya	swin.net	eya@swin.net

Tabla 7. Composición de la dirección de correo electrónico

SMTP

EL protocolo SMTP es el estándar para la distribución de correo electrónico en Internet. Es un protocolo orientado a texto que utiliza los servicios de TCP/IP para recibir correo desde un cliente y para transferir mensajes desde un servidor a otro de forma fiable.

POP

El Protocolo de Oficina Postal define el diálogo entre un servidor de correo y la aplicación de correo electrónico. Al recibir los mensajes el servidor de correo los almacena en buzones privados para cada usuario. POP permite que un Agente de

Usuario (UA) acceda al buzón, descargue todos los mensajes pendientes y después borrarlos.

HTTP

El protocolo de transferencia de HyperTexto es el pegamento que une el World Wide Web. El servicio HTTP en un host permite que usuarios a distancia puedan acceder a los ficheros que almacena si éstos conocen su dirección exacta. El protocolo HTTP define un sistema de direcciones basado en Localizadores Uniformes de Recursos (URL). El URL de un recurso indica el protocolo o servicio que se emplea para ser accedido, la dirección del host donde se encuentra el recurso, y la ubicación del recurso dentro del host.

La información hypertexto se almacena en formato HTML. Se refiere a cada fichero como "página". El "Browser" es el programa de usuario que conecta con el servidor mediante HTTP e interpreta la página HTML antes de mostrarla al usuario.

FTP

FTP es el protocolo de transferencia de fichero de TCP/IP, permite tanto enviar como recibir ficheros desde o hacia un servidor FTP.

TELNET

El conjunto de protocolos TCP/IP incluye un protocolo de terminal remoto sencillo, llamado TELNET, el cual permite a un usuario establecer una conexión TCP con un servidor de acceso a otro. TELNET transfiere después las pulsaciones de teclado directamente desde el teclado del usuario a la computadora remota como si hubieran sido hechos en un teclado unido a la máquina remota.

1.4. Codificación de la voz.

Lo mas importante en una videoconferencia es la calidad de la voz. Ya que si la voz llega con retardo, ruido o entrecortado, la comunicación será defectuosa.

Los estudios demuestran que 100ms de retardo son detectables por el oido humano, pero es tolerable; 250ms de retardo ya molestan; y las demoras mayores son inaceptables. Obviamente que no solo tiene que ver la codificación, sino también el estado de la red, recursos de los equipos implicados, etc.

La industria de videotelefonía, así como el mercado de telefonía IP, se ha decidido por el uso de los algoritmos de compresión de audio G.7xx, los que se muestran en la Tabla 8. Un algoritmo ideal consume el menor ancho de banda y transmite el mayor espectro de frecuencias de audio. En videotelefonía, el ancho de banda no usado por el audio, puede ser utilizado para mejorar la calidad del vídeo.

Audio	**Rango(Hz)**	**BW consumido**	**Calidad**	**Complejidad**	**Usado por**
G.711	50-3600	48-64 Kbps	Alta	Baja	H.320 (R) H.323 (R)
G.722	50-6000	48-64 Kbps	Alta	Media	H.320 (O)
G.723	50-8000	6.3 ó 5.3 Kbps	Media	Media	H.323 (O H.324 (R)
G.728	50-3600	16 Kbps	Alta	Muy alta	H.320 (O) H.323 (O)
G.729	50-3600	8 Kbps	Alta	Media	Europeo
R = Requerido por este algoritmo de compresión; O = Opcional					

Tabla 8. Algoritmos G.7xx

1.5. Codificación del vídeo.

La compresión de vídeo ha funcionado gracias a que imagen capturada contiene más información de color y luminosidad que la que el ojo humano pude discriminar. Uno de los procesos empleados por los codificadores de vídeo es promediando la información de color de dos pixels adyacentes y descartar la mitad de ellos si la diferencia es pequeña; un observador no podrá distinguir esto en la imagen reconstruida.

Otra importante estrategia es transmitir únicamente las partes de un cuadro que varían de frame a frame. Los frames básicos (imágenes completas) son transmitidos pocas veces cada segundo. Los frames intermedios sólo contienen redefiniciones de este grupo de pixels que necesitan ser actualizados. Un proceso suplementario es la predicción de movimiento, éste usa un algoritmo de reconocimiento de patrones en el codificador para identificar los cuadros repetitivos (la mano de una persona, por ejemplo) y luego busca en frame el patrón, en el camino de movimiento probable.

Este algoritmo, DCT (Discrete Cosine Transform), esta incorporado en muchos esquemas de compresión de vídeo, incluyendo el H.261, H.263 y la serie MPEG (MPEG-1, MPEG-2 y MPEG-4). Estos esquemas difieren en la manera como manipulan los frames intermedios y las tazas de compresión alcanzados.

Otro truco en la compresión de vídeo es gaı.ar uniformidad en el movimiento enturbiando el retrato levemente. La reducción de la resolución no es notada en las ventanas pequeñas usadas por sistemas de videoteléfono ni el Netmeeting. Mientras se evalúan sistemas de videoteléfono para uso comercial, el costo cierra la atención

en un parámetro llamado CIF (Formato Intermedio Común). La Tabla 9 muestra las resoluciones en pixels para varios CIF múltiples.

Formato de vídeo H.32x	**Resolución**	**Usado por**
Sub-QCIF	128x196	H.263 (R)
QCIF (Quarter Commom Intermediate Format)	176x144	H.261 (R) H.263 (R)
CIF (Commom Intermediate Format)	352x288	H.261 (O) H.263 (O)
4CIF	704x576	
16CIF	1408x1152	
Otros formatos de vídeo		
MPEG-1 (VideoCD, VCR)	320x240	
HDTV (High Definition TV)	1440x1280	
R = Requerido por este algoritmo de compresión; O = Opcional		

Tabla 9. Tabla de resoluciones para varios CIF

CAPÍTULO II

ARQUITECTURA H.323"

2.1. Introducción

El estándar H323, es la tecnología base para la transmisión en tiempo real de comunicaciones de audio, vídeo y datos sobre redes basadas en paquetes. Especifica los componentes, protocolos y procedimientos que proveen comunicaciones multimedia en redes basadas en paquetes. El H323 puede ser usado para transmitir sólo audio (Telefonía IP); audio y vídeo (Videotelefonía); audio y datos; y audio, vídeo y datos (ver Figura 4).

La recomendación H.323 de la ITU-T, "Sistemas de Comunicaciones Multimedia Basados en Paquetes", trata de los requisitos técnicos para las comunicaciones multimedia en donde el transporte se realiza en redes de paquetes que no proveen calidad de servicio (QoS) garantizada. Es decir, la H.323 es un conjunto de protocolos para la comunicación punto a punto y punto a multipunto de voz, vídeo y datos en tiempo real sobre redes basadas en paquetes tales como IP, Ethernet y otros. La recomendación está diseñada para permitir que los clientes de las redes H.323 se puedan comunicar con clientes de otras redes.

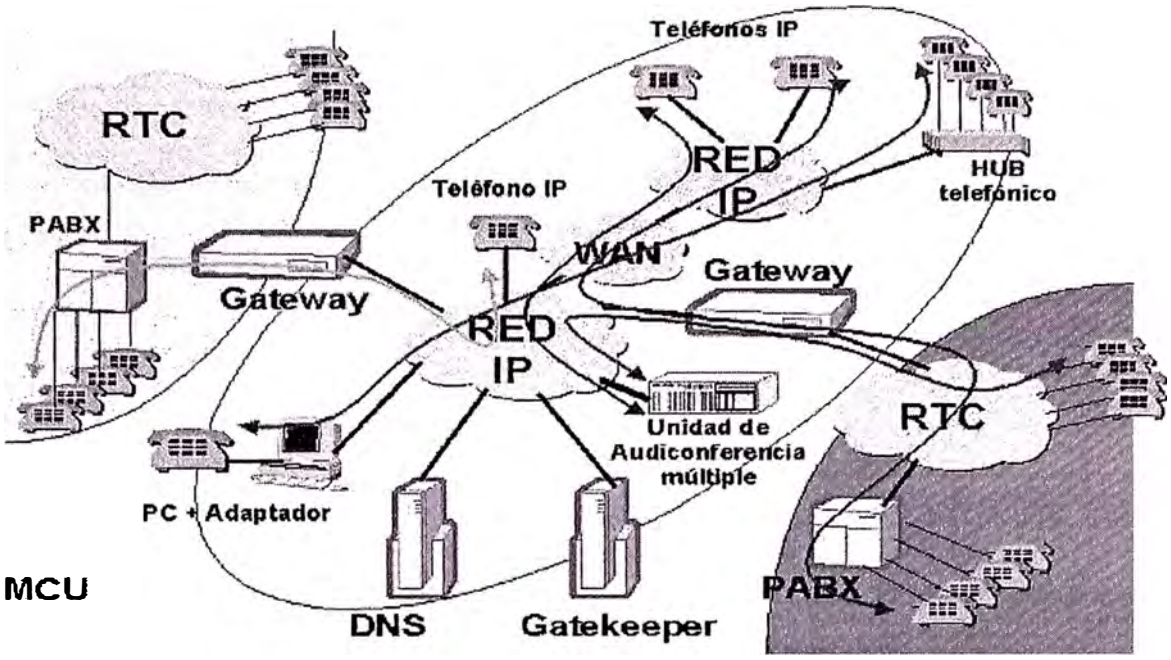

Figura 4. Elementos de una red de H.323.

La estandarización de los protocolos y procedimientos para las videoconferencias en redes de paquetes se inició debido al éxito creciente que experimentaron las redes de área local IP, IPX y AppleTalk en la década de los 90. La primera versión del H.323 ("Sistemas y Equipos de Telefonía Visual para Redes de Área Local que no proveen una Calidad de Servicio Garantizada") recayó en el grupo de estudio 15 de la ITU que ya había adquirido experiencia durante el desarrollo de la recomendación H.320 ("Conferencia Multimedia en RDSI"). Esta versión fue iniciada en mayo de 1995 y fue aprobada en junio de 1996.

No tuvo mucho éxito, puesto que no atrajo el interés del mercado hasta que Cisco y VocalTec fundaron un foro para el desarrollo de estándares de productos para Voz sobre IP (VoIP). El foro se incorporó al Consorcio Internacional de Teleconferencias Multimedia (IMTC) con el crecimiento del número de sus miembros. Fue el grupo de actividades de VoIP del consorcio el que adoptó el H.323

para el desarrollo Telefonía por Internet. El interés surgido por la normas motivó al grupo de estudio 16 de la ITU-T a ampliar la recomendación en su segunda versión ("Sistemas de Telecomunicaciones Multimedia basadas en Paquetes") publicada en febrero de 1998 añadiendo varios anexos. En la actualidad está en vigencia la versión 3 de la norma, publicada en septiembre de 1999, mientras que en el grupo de estudio 16 de la ITU-T se discute nueva versión.

El propósito de este trabajo es presentar una breve descripción sobre la arquitectura de la recomendación H.323 en cuanto a los protocolos, los procedimientos y los componentes que la forman. Una descripción más detallada se realiza con respecto a los procedimientos de la Señalización de Llamada importantes en el establecimiento de las conferencias explicando como se logran éstas en algunos escenarios interesantes. Al final se mencionan las aplicaciones de la recomendación y los productos que se ofrecen en el mercado, los obstáculos y los desafíos que afectan la adopción y desarrollo de la norma.

2.2. Componentes H.323

El H.323 especifica 4 tipos de componentes, los cuales, cuando se interconectan proveen servicios de comunicación multimedia punto a punto y punto a multipunto:

- Terminales (Terminals)
- Pasarelas (Gateways)
- Guardianes (Gatekeepers)
- Unidad de Control Multipunto (MCU: Multipoint Control Units)

La Figura 5 muestra un escenario general en el que participan los distintos componentes lógicos descritos en la recomendación. Éstos son los terminales, las pasarelas, las unidades de control multipunto (MCU) y el guardián. Una red con capacidades de comunicaciones multimedia puede ser implementada sólo con terminales H.323, pero con la adición de los demás componentes se puede lograr ampliar las facilidades brindadas por sus servicios. Los terminales, las pasarelas y MCUs se denominan colectivamente como extremos finales ya que en ellos se originan y terminan flujos de datos y de señalización.

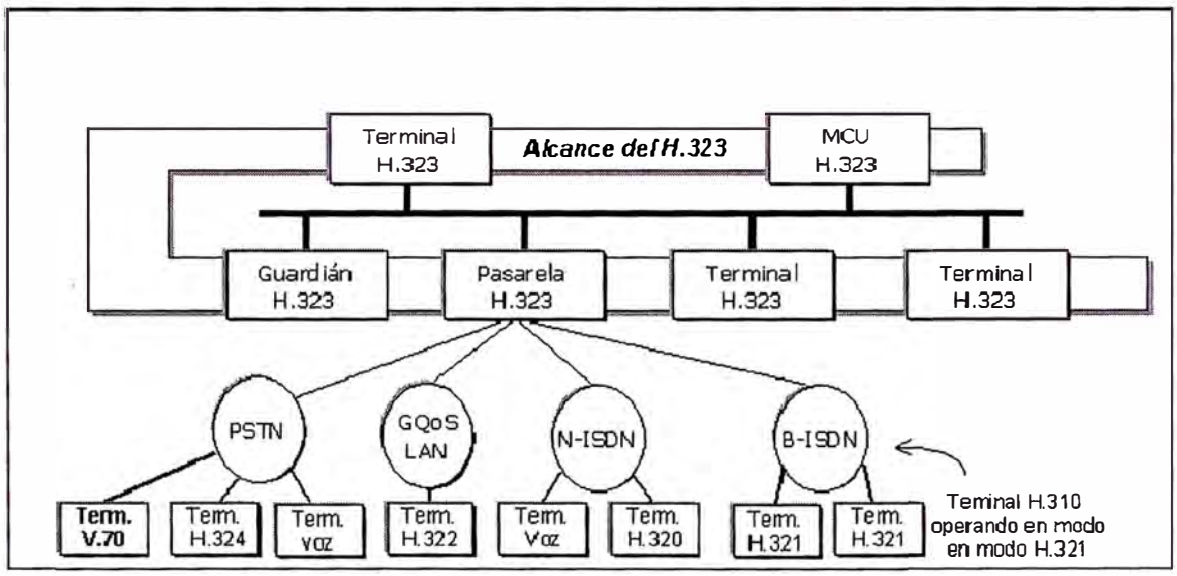

Figura 5. Interoperabilidad de la terminal H.323 (Adaptada de H.323 ITU-T)

2.3. Terminal H.323

El terminal, o cliente, es un extremo final que debe soportar, como requisito mínimo, la comunicación de audio.

En la Figura 6 se muestra un esquema de equipo terminal H.323 y los diversos bloques funcionales que lo componen.

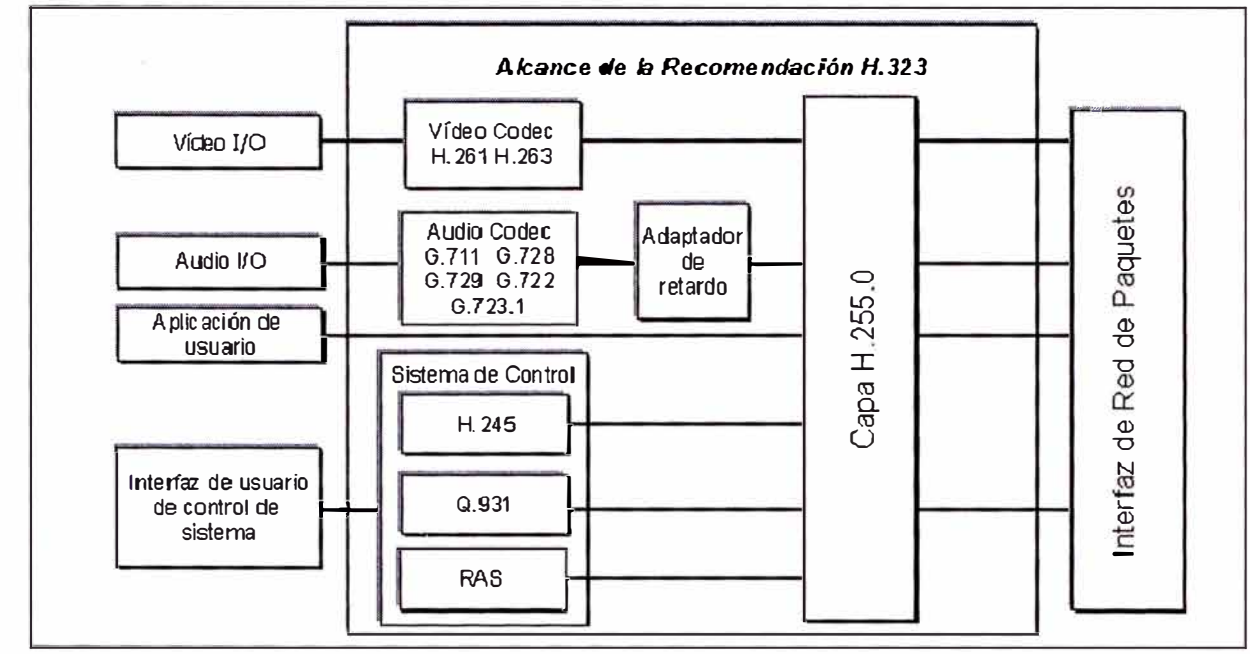

Figura 6. Equipo terminal H.323.(Adaptada de H.323 ITU-T)

2.4. Guardián H.323

El guardián es un elemento opcional que provee de servicios de control de llamada y de administración de recursos de la red. El área de la red administrado por un guardián se conoce como zona y ésta comprende a los extremos finales (terminales, pasarelas y MCUs) que se encuentran registrados en el guardián sometiéndose a su control. El guardián no puede ser destinatario final de una llamada.

- **Traducción de direcciones:** mantiene una base de datos para la traducción de aliases, por ejemplo, números telefónicos internacionales y direcciones de red.

- **Control de acceso y admisión de los extremos finales:** Control basado en la disponibilidad del ancho de banda, la limitación del número de llamadas H.323 simultáneas o por el registro de privilegios de las

terminales. Se realiza mediante mensajes de Solicitud, Admisión y Estado (RAS) definidos en H.225.0.

- **Administración del Ancho de Banda:** facilidad que le permite a los administradores de red la configuración del número de llamadas H.323 simultáneas o el condicionamiento de la autorización de ciertas terminales a horario determinado.

- **Capacidades de encaminamiento:** encaminamiento de todas las llamadas que se inician o terminan en su zona. Tiene varias ventajas, entre éstas, la estadística para propósitos de facturación y seguridad, el desarrollo de servicios de movilidad, reenvió de llamada y correo de voz.

2.5. Pasarela H.323

La pasarela provee de una comunicación bidireccional en tiempo real entre terminales H.323 de la red de paquetes y otras terminales definidas por la ITU ubicados en redes de conmutación de circuitos. La pasarela efectúa la traducción entre los formatos de transmisión y procedimientos de comunicación. Un ejemplo del primer caso sería: la traducción del formato de H.225.0 de una terminal H.323 al formato de H.221 de un terminal H.320. Esta traducción está especificada en la recomendación H.246.

La pasarela también realiza el establecimiento y la finalización de las llamadas en las redes que interconecta. También, puede realizar la traducción de formatos de datos, audio y vídeo. En general, el propósito de una pasarela es completar la llamada entre los extremos finales de las redes de paquetes y circuitos de manera transparente y en ambas direcciones. Se contempla que las terminales

H.323 se puedan comunicar con las terminales ITU listadas en la Tabla 10 a través de una pasarela.

Recomendación	**Tipo de red**
H.310	Red Digital de servicios Integrados de Banda Ancha (RDSI-BA)
H.320	Red Digital de servicios Integrados (RDSI)
H.321	Modo de Transferencia Asíncrono (ATM)
H.322	Red de Área Local con Calidad de Servicio Garantizado (GQoS-LAN)
H.324	Red Telefónica Conmutada General (GSTN)
H.324M	Terminal Móvil
-----	Servicio Telefónico Tradicional (POTS)

Tabla 10. Terminales que Inter-operan con H.323 mediante pasarelas.

2.6. Unidad de control multipunto (MCU)

La unidad de control multipunto (MCU) provee de la capacidad de que tres o más terminales, incluyendo pasarelas, puedan participar en una conferencia multipunto. También puede conectar a dos terminales en una comunicación punto a punto de la que posteriormente se convertirá en multipunto con la incorporación de otros participantes. El MCU está compuesto de dos partes: el Controlador Multipunto (MC) y el Procesador Multipunto (MP). La participación del MC es obligatoria y facilita la negociación entre las terminales para alcanzar un nivel común de comunicación por medio de la señalización de control. El MP es opcional y permite la mezcla, la conmutación y otros procesamientos de los flujos de media bajo el control del MC.

2.7. Mecanismo de control y señalización

El mecanismo de control y de señalización en H.323 es esencial para el establecimiento de los canales de flujo multimedia, su liberación, anuncio de las capacidades soportadas por las terminales y la negociación del uso de estas capacidades, y para propósitos de gestión de los recursos de la red. H.323 define tres protocolos para realizar las funciones de establecimiento, control y administración de usuarios y recursos de la red.

2.8. H.225 - Establecimiento, liberación y gestión de llamadas.

2.8.1. Señalización de la Llamada (H.225.0)

Para el establecimiento y la liberación de las llamadas entre dos extremos finales es necesario el intercambio de información sobre el propósito del mensaje de petición de establecimiento, indicación de alerta al llamado, conexión lista, la liberación lista, etc. También se intercambian elementos de información como la identificación del llamante, la identificación y dirección del llamado basada en un plan de numeración, la naturaleza del equipo que inicia la comunicación (guardián, pasarela, terminal,...), un número identificador de la conferencia, el propósito de la conferencia, los puntos de acceso al servicio de transporte (TSAPs) para el control de los flujos de media y otros datos relevantes.

La señalización de la llamada H.225.0 se basa en el protocolo de señalización Q.931 desarrollado para la Red Digital de Servicios Integrados. La señalización de la llamada puede ser intercambiada entre las terminales directamente en ausencia de un guardián.

2.8.2. Registro, Admisión y Estado (H.255.0 RAS)

Las funciones de registro, admisión y determinación del estado se realizan mediante el intercambio de mensajes entre el guardián responsable de una zona y sus extremos finales H.323, o con otros Guardianes (H.323 versión 3). El H.225.0 RAS utiliza un medio de transporte no fiable a diferencia del H.225.0 para la señalización de la llamada y entre sus objetivos se encuentran:

- **Descubrimiento del guardián:** cuando el extremo final necesita localizar la dirección del guardián en la red, envía un mensaje "Solicitud del Guardián, GRQ" a una dirección multipunto (224.0.1.41:1718 en redes IP) incrementando el alcance del mensaje en cada intento. Uno o más Guardianes responderán con la dirección solicitada mediante un mensaje de confirmación (GCF).

- **Registro del extremo final:** Todos los extremos finales deben registrarse con el guardián de la zona (RRQ y RCF/RRJ) . Esto permite que el guardián conozca la dirección y los aliases de los extremos finales de su zona para encaminar las llamadas o limitar la cantidad de usuarios activos de la red.

- **Localización del extremo final:** en ocasiones el guardián necesita actualizar su base de datos de aliases y direcciones de red. Para esto usa mensajes de localización del terminal periódicamente.

- **Otras funciones:** El guardián usa mensajes H.225.0 adicionales para desarrollar otras tareas de administración y control como la admisión de las llamadas solicitadas (ARQ y ACF), la determinación del estado de las llamadas (IRR), la liberación de las llamadas (DRQ y DCF) , la administración de la capacidad de la red (BRQ y BCF).

2.9. H.245 - Control de señalización

Antes de que se pueda establecer un enlace de comunicaciones multimedia consistente en uno o varios flujos mezclados se requiere del intercambio de información sobre las capacidades soportadas en cada terminal y la negociación de las capacidades que se usarán. Entre las funcionalidades del H.245 se pueden mencionar:

- **Intercambio de Capacidades:** Cada extremo final que participa de una comunicación multimedia anuncia sus capacidades de recepción y transmisión como codificadores y decodificadores, velocidad de transmisión, etc. El anuncio y el registro de las capacidades de los participantes se realiza con el intercambio de mensajes H.245 termCapSet y termCapAck.

- **Apertura y cierre de Canales Lógicos:** Los canales lógicos de audio y vídeo en H.323 son unidireccionales, de extremo a extremo e individuales. El canal lógico de datos es bidireccional. Se usa un canal lógico 0, que se mantiene abierto durante la conferencia, para el intercambio de mensajes de apertura y cierre de canales de media OpenLogicalChannel/OpenLogicalChannelAck y otros.

- **Mensajes de Control de Flujo:** Se intercambian mensajes de retroalimentación entre los extremos finales cuando se detectan problemas en la comunicación. Además se cuenta con la posibilidad de cambiar, durante la conferencia, las capacidades negociadas al inicio, por ejemplo solicitar un cambio de codificador.

2.10. Procedimientos de conexión

La descripción de los procedimientos de la señalización de la llamada se muestran a continuación en el contexto de algunos escenarios interesantes que se desarrollan en una red IP.

2.10.1. Llamada directa entre dos terminales H.323.

El escenario más sencillo descrito en H.323 es la conferencia entre dos terminales H.323 de la misma zona sin la mediación del guardián. Se explican con detalle las fases que intervienen.

Establecimiento de la Llamada: La terminal llamante debe enviar un mensaje H.225.0 Setup a través de una conexión fiable a un punto de acceso al servicio del nivel de transporte (TSAP) conocido de la terminal llamada. En TCP/IP la dirección TSAP definida por la IANA es el número de puerto 1720.

Supongamos que la conferencia se realizará en una red de paquetes IP. En el mensaje Setup se envían los datos enumerados anteriormente y que se describen a continuación:

- Un campo discriminador de protocolo puesto a 08H.
- Un valor de referencia de llamada CRV escogido en la terminal llamante que será el mismo para cada mensaje posterior concerniente a la llamada.
- El tipo de mensaje (05H para Setup).
- La capacidad de la portadora que indica si la conferencia será de audio sólo, audio y vídeo, etc.

- El número del llamado. Se puede usar un plan de numeración E.164 o un número particular.
- El número del llamante.
- La unidad de datos de protocolo PDU H.323 que encapsula información extensa y necesaria para la conferencia:
    - Un identificador de protocolo.
    - Un campo de dirección de origen con los aliases del llamante.
    - El tipo de equipo que solicita el establecimiento (MCU, pasarela,...).
- Identificadores: número telefónico E.164, URL-ID, dirección de transporte IP (dirección de red IP : 1720), e-mail, etc.
- Un identificador de llamante Call-ID establecido por el mismo llamante.
- Un identificador universal de la conferencia (CID). Éste hará referencia a la conferencia actual. Todos los participantes de la conferencia usarán el mismo CID. Si un participante entra y sale de la misma conferencia utilizará el mismo CID, pero distintos CRV y Call-ID.
- Un objetivo de la conferencia que puede ser: crear una conferencia, invitar al llamado a una conferencia existente o incorporarse a una.

El receptor del Setup(configuración) debe contestar inmediatamente con los mensajes H.225.0 Alerting(alerta), Call proceeding(procediendo a llamar) y Connect(conectar) (los dos primeros son opcionales) antes de que expire un temporizador en el origen puesto a 4 seg. Si recibe un mensaje Alerting indicando que la terminal llamada esta en espera de que el usuario conteste, entonces se puede

extender la espera hasta 3 min. Cuando el usuario contesta, se envían el mensaje Connect que incluye los siguientes elementos de información:

- Un discriminador de protocolo, el tipo de mensaje y CRV.
- La dirección de puerto TCP que el llamado usará para abrir el canal de control H.245.
- El tipo de terminal a través del cual se conectan (pasarela o no).
- El mismo CID y el Call-ID (identificador de llamada).

2.11. Actualidad del H.323

2.11.1. Estandarización

La H.323 es un estándar que ha sido ampliamente aceptado. A mediados de los 90s se desarrollaron varios productos propietarios para la telefonía en Internet. Los servicios prestados por estos productos estaban basados en protocolos incompatibles que de ninguna manera facilitaban la interoperabilidad. En contraste, ahora existen organizaciones que promueven la compatibilidad de productos basados en H.323 como el Consorcio Internacional de Teleconferencia Multimedia (IMTC) (organización sin fines de lucro con una membresía de más de 150 firmas) que emite certificaciones de interoperabilidad y compatibilidad.

2.11.2. Interconexión

El desarrollo y la estandarización de las pasarelas permite que los usuarios de terminales H.323 puedan comunicarse con clientes de diversas redes basadas en conmutación de circuitos (RTCP, ATM, RDSI,...).

2.11.3. Servicios Integrados y de valor añadido

Con la H.323 se hace posible el desarrollo de varios servicios adicionales como el correo electrónico, el correo de voz, funcionalidades de centros de atención al cliente (Call Centers) y videoconferencias, todos integrados en la misma red. También se han normalizado varios servicios de valor añadido como la transferencia de llamada, la transferencia de llamada y otros (H.450.X).

2.11.4. Aplicaciones y propuestas

Es extensa la lista de aplicaciones que se pueden realizar con el apoyo de la recomendación H.323 o con un subconjunto de ésta. A continuación se mencionan algunas de las aplicaciones, propuestas y estándares mas recientes y relevantes.

Servicios Multimedia:

Se pueden establecer todo tipo de servicios multimedia con el uso del H.323 que facilitan la interacción a distancia: tele-educación, tele-trabajo, tele-medicina,... Una de las aplicaciones más obvias proporcionadas por H.323 es la videoconferencia entre varios usuarios de la red. Existen muchas soluciones basadas en H.323 a nivel de Intranets (comunicaciones corporativas) en las que se puede proporcionar un grado de Calidad de Servicio mayor que en la Internet.

Telefonía en Internet:

La Telefonía en Internet, o Voz sobre IP (VoIP), es uno de los mercados de mayor crecimiento de las comunicaciones en la actualidad. Éste puede definirse como el suministro de los servicios telefónicos sobre Internet. Facilita el tráfico de voz en forma de paquetes de datos sobre una red de paquetes conmutados.

Beneficios:

a. Comunicaciones multimedia través del PC: En la actualidad existen algunos cientos de millones de equipos informáticos que están equipados, o pueden equiparse, con sistemas de reproducción multimedia (sintetizadores de sonido, micrófonos, altavoces, puertos,...) que lo habilitan como terminal de comunicaciones en redes de paquetes y circuitos.

b. Reducción del costo de las llamadas: El costo de acceso plano en Internet oscila entre las 2.500 a 5.000 pesetas (15 a 30 euros) dependiendo del portador de RTCP o el ISP. Incluso existen ISPs que no cobran por el acceso a Internet a cambio de disponer de los datos del subscriptor para realizar negocios. Realizando las llamadas de larga distancia con la Telefonía IP, el usuario puede transformar ese gasto a un monto constante mensual.

c. Reducción del número de redes: Las grandes y medianas empresas deben realizar un gasto periódico por el uso y el mantenimiento de sus redes telefónicas y de datos, además de que se deben sufragar los gastos de llamadas de larga distancia. Con VoIP estas empresas pueden usar sus redes LAN para el tráfico interno de voz y facsímil. Igualmente pueden usar VoIP para realizar las llamadas externas, aunque con distintos grados de dificultad dependiendo de la extensión del VoIP y los proveedores. La integración de la red telefónica con la red de datos tiene un costo relativo reducido que puede ser amortizado rápidamente. Las consultoras estiman que los gastos por mantenimiento se reducirían un 40%. A los beneficios de esta integración, se le pueden añadir los servicios de valor añadido del H.323 mencionados antes: e-mail, correo de voz, localización,...

d. Eficiencia de las transacciones: Las compañías orientadas a servicios pueden incorporar una solución de atención al cliente en sus páginas de Web. Presionando un botón de la página, el cliente podría iniciar una comunicación vocal con el centro de atención al cliente (Call Center) de la empresa desde el navegador. Esto facilita la rapidez de las transacciones e incrementa la satisfacción del cliente.

e. Mejoramiento del desempeño de las redes telefónicas: Los canales de voz que se establecen en las redes de circuitos conmutados de las empresas telefónicas consumen 64 Kbps de la capacidad de los enlaces entre sus centrales. Los codificadores de voz recomendados en la H.323 logran tasas de transferencia menores a los 8kbps lo que incrementaría la posibilidad de cursar más tráfico por la red telefónica.

RMOA (Real-Time Multimedia over ATM)

Es un nuevo estándar del "ATM Forum" para el transporte del tráfico de voz sobre redes de Internet basadas en ATM. En el estándar se define una nueva pasarela H.323 para transportar los flujos de media H.323 en tiempo real tomando ventaja de las características de Calidad de Servicio que ofrece ATM y reduciéndose la sobrecarga del transporte ATM.

iGSM:

Es una propuesta en estudio de servicio de valor añadido para redes móviles. Permite que un usuario de GSM pueda acceder al servicio de VoIP cuando éste se traslada a la red IP. El iGSM rastrea la localización del subscriptor iGSM al encender o apagar el terminal móvil o IP cuando accede o se retira de la red IP. El sistema experimental utiliza un mecanismo de traducción de los protocolos de señalización de GSM y H.323 para el registro, dado de baja y el procedimiento de reenvío de la llamada. Se implementa con el uso de pasarelas y Guardianes H.323. Aunque el iGSM se puede apoyar de otros sistemas de comunicaciones mutimedia de redes de paquetes, se ha utilizado el H.323 para demostrar su viabilidad.

2.11.5. Productos

Es considerable la oferta de productos H.323 en cuanto a componentes y software para desarrolladores. Existe una lista extensa en http://www.iptelephony.org. En la Tabla 11 se realiza una breve descripción de alguno de éstos componentes.

Nombre	Vendedor	Configuración	H.323	Otras Características
Pasarelas				
Pasarela	World Connect	NT 4.0	1.0	Hasta 48 puertos, FAX
DM3 IP Link	Dialogic	Solaris, NT, Win	2.0	Hasta 120 puertos, FAX
Guardianes				
H.323 Guardián	Ericsson	NT 4.0, UNIS	2.0	Servicio de directorio, control de ancho banda
VocalTec Guardián	VocalTec	NT 4.0	2.0	Servicio de directorio, SMNP
MCUs				
Encounter 3000 NetServer	Ezenia	NT 4.0	1.0	H.261,H.263,G.711,G.722,G.723,G.728,T.1 hasta 2Mbps,32 usuarios simultáneos
MCU-323	Radvision	Hardware	2.0	H.261,G.711,G723,G.729,h.263, 10/1 BaseT, sin programación de conf., no mo mixto, 15 usuarios
Terminales				
Intel Vídeo Pone	Intel	Win 98	1.0	Audio, vídeo y data
Meeteing Point	CUSeeMe	Win,Solaris, Linux	1.0	Audio, vídeo y data

Tabla 11. Ejemplos de productos basados en H.323

2.12. Desafíos y obstáculos

2.12.1. Seguridad

Debido al costo de la implementación y la reducción en el tiempo de desarrollo, existen muchos productos H.323 que carecen de las facilidades de seguridad que se proponen en el estándar (versión 2), que se detallan en la recomendación H.235.

2.12.2. Calidad

La pobre garantía de calidad en las redes IP es un tema de estudio intensivo. H.323 puede aprovechar cualquiera de las soluciones propuestas para el resolver este problema a nivel de red y transporte (InterServ y Diffserv), además de utilizar métodos de codificación eficientes tanto para voz y vídeo. A pesar de ello, en un entorno tan heterogéneo como Internet la calidad de la voz es menor que en las redes RTCP.

2.12.3. Servicios de Valor Añadido

Los productos H.323 no sólo deben proporcionar operaciones de bajo costo, también deben incluir servicios de valor añadido para poderle ganar terreno a las comunicaciones de voz en las RTCPs. El conjunto limitado de servicios de valor añadido que se han implementado en los productos H.323, como los problemas de escalabilidad e incompatibilidad de los productos de diferentes fabricantes afectan negativamente la decisión en la instalación de los servicios H.323.

2.12.4. Nuevas Normas

En los últimos años han surgido otros sistemas de señalización, entre ellos el SIP, Protocolo de Iniciación de Sesión. Éste es el estándar propuesto por el IETF para el establecimiento de conexiones para VoIP. Es un protocolo de control a nivel de aplicación para la creación, modificación y finalización de sesiones con uno o varios participantes. SIP se fundamenta en el modelo cliente-servidor basado en HTTP y se distingue por el establecimiento de canales fiables independientemente de la capa de transporte. No necesita del TCP para lograr la fiabilidad. Los canales fiables se establecen mediante el intercambio de mensajes de invitación y asentimiento y sobre éstos se transfieren los mensajes de control. Todas las peticiones enviadas al servidor son respondidas por éste en un proceso denominado con el nombre de transacción. SIP depende del Protocolo de Descripción de Sesión (SDP) para llevar a cabo la negociación de los codificadores de cada una de los medios que se usarán durante la conferencia.

Los componentes del SIP son el agente usuario y servidores de red. El primero es un sistema final que actúa en representación del usuario y se compone de dos partes: el Cliente de Agente de Usuario (UAC), que envía las solicitudes de SIP, y el Servidor de Agente de Usuario (UAS), que recibe las solicitudes y retorna las respuestas por el usuario. Existen tres tipos de servidores de red. Un Servidor de Registro que actualiza la información sobre la localización de los usuarios, un Servidor Proxy que recibe peticiones y las reenvía al servidor del próximo salto que tiene información de la localización de los usuarios llamados, y un Servidor de Redirección que procesa las peticiones de los clientes respondiéndoles con la

dirección del servidor del próximo en lugar de reenviar la petición. Con estos componentes, el SIP provee de todas las funcionalidades necesarias para el establecimiento de conferencias: localización de los usuarios, establecimiento de la llamada, disponibilidad de los usuarios, determinación de las capacidades de los usuarios y manejo de las llamadas.

Tanto el H.323 como el SIP se proponen para la implementación de servicios como el de VoIP. Se puede realizar una comparación entre ambos por sus cualidades de complejidad, extensibilidad, escalabilidad y ofertas de servicios en la que, como resultado, se observa que SIP posee varias ventajas (ver Tabla 12).

H.323	**SIP**
Protocolos Complejos	Más Sencillo
Representación Binaria de los mensajes en ASN.1	Representación Textual
Poca modularidad	Muy Modular
Poco escalable	Altamente escalable
Señalización compleja	Señalización simple
Respaldado por ITU	Respaldado por IETF
Centenas de elementos	Sólo 37 cabeceras
Detección de lazos complicados, con estados	Detección de lazo sencillo, sin estados

Tabla 12. Comparación cualitativa entre H.323 y SIP.

CAPÍTULO III

GUARDIÁN H.323

8.1. Introducción

El Guardián es la herramienta más poderosa de administración disponible para una red multimedia H.323. Como el cerebro de una red H.323, esta aplicación realiza el control esencial, administrativo, y funciones directivas requeridas para mantener la integridad de las redes tanto de la empresa como del carrier.

Como un mecanismo estándar dominante en la industria, integrado en la red H.323, el Guardián provee las siguientes funciones:

- Autenticación
- Autorización
- Contabilidad
- Control y ruteo de llamadas
- Servicio de telefonía básica tal como servicios de directorio funciones de PBX (Private Branch Exchange)
- Control de ancho de banda H.323 usado para proveer calidad de servicio (QoS) y proteger otras aplicaciones de red criticas del tráfico H.323

- Control total del uso de la red
- Administración total del sistema y políticas de seguridad.

El objetivo de este capítulo es explicar los beneficios de integrar un Guardián cuando se diseña aplicaciones de telefonía IP basadas en una red H.323.

8.2. Entorno

El Guardián es el punto focal de una red multimedia H.323. El estándar H.323 en redes de producción se implementa a través de zonas. Las zonas son un conjunto de puntos terminales sobre los cuales uno y solamente un Guardián tiene jurisdicción. Ellas incluyen cualquier número de terminales, Pasarelas, y unidades de conferencia multipunto (MCUs); cualquier de estas entidades pueden registrarse en un Guardián.

A pesar de la localización física del código del programa del Guardián, debe haber únicamente un Guardián por zona. Las zonas pueden ser definidas de acuerdo a la localización geográfica (tal es como en las diferentes sucursales) o de acuerdo a superposiciones de conexiones de red (tal es como subredes en los pisos de un edificio con diferentes rangos de direcciones IP) o de acuerdo al paradigma funcional (organizacional).

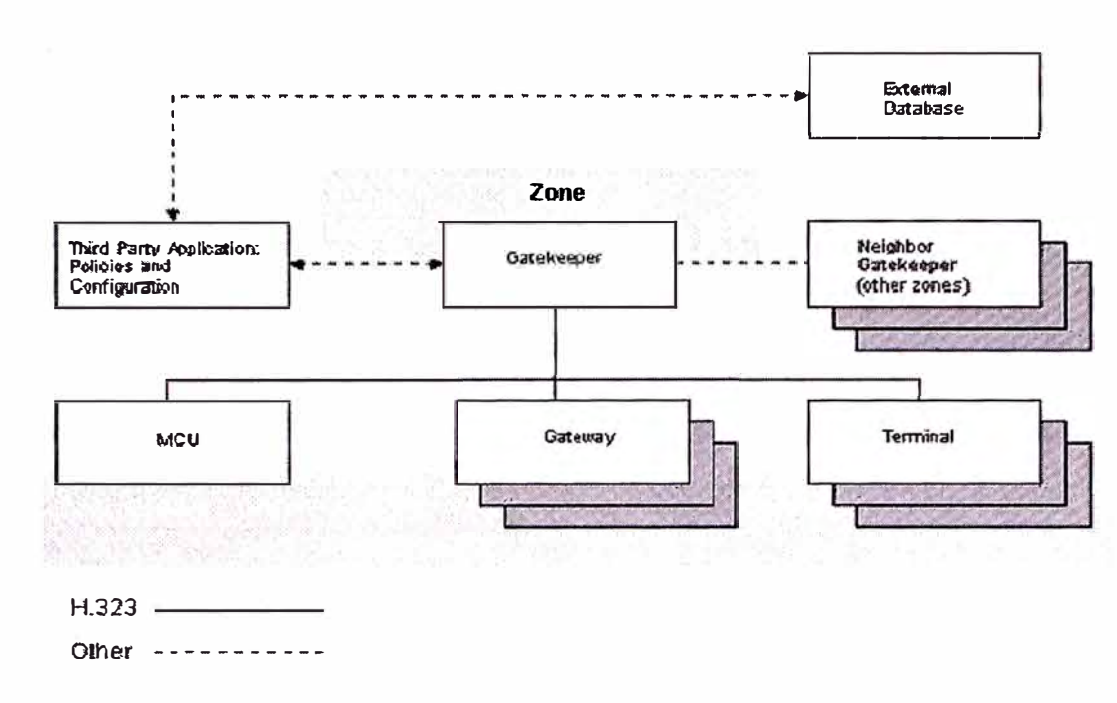

Figura 7. El entorno de un Guardián

Un Guardián administra todas las actividades de la zona. Cada vez que una entidad H.323 hace su presencia, esta enviará una interrogante a la red, preguntando cuales(si lo hay) Guardianes están presentes y aceptarán sus requerimientos de registro de esta entidad o envían un requerimiento de registro a un Guardián predeterminado. El descubrimiento del punto final y el proceso de registro es un prerrequisito para el Guardián administrador de zona.

Elegir un Guardián es crítico para la óptima operación de una solución H.323. El Guardián permite a los desarrolladores la capacidad de escalar el sistema a un gran número de usuarios mientras toman cuidado del ruteo de llamadas interzonales.

La identificación de puntos finales en una zona es hecha usando direcciones IP, alias (tales como identificadores H.323, direcciones de e-mail, y URLs) o número de teléfonos. El Guardián es el punto focal para la inserción de la lógica

dentro de una red H.323. Este puede ser configurado y controlado remotamente por aplicaciones de terceras partes usando HTTP o SNMP. Por ejemplo, un planificador de red puede configurar un Guardián para especificar un conjunto específico de puntos finales dentro de una zona y proveer a los usuarios políticas y procedimientos únicos, como se muestra en la Tabla 13.

Procedimientos de administración de requerimientos de zona	**Procedimientos y políticas opcionales**
Traslado de direcciones	Autorización de llamadas
Control de admisiones	Administración de ancho de banda
Control de ancho de banda	Servicios suplementarios
	Servicios de directorio
	Servicios de administración de llamadas
	Señalización de control de llamadas

Tabla 13. Políticas y procedimientos.

8.3. Características obligatorias

Las funciones obligatorias de un Guardián según la especificación de la Unión Internacional de Telecomunicaciones (ITU) son las siguientes:

- Traslado de direcciones
- Control de admisión
- Control de ancho de banda
- Administración de red

8.3.1. Traslado de direcciones

El Guardián provee traslado de direcciones entre un alias y la dirección de transporte hasta un requerimiento de un punto final por servicio. Un usuario típicamente no conoce la dirección IP de otros terminales (o entidades) a los cuales quiere llamar, el Guardián traslada una dirección alias (identificador H.323, URL, número de teléfono, o dirección de e-mail) a una dirección de transporte. Hay una serie de mecanismos disponibles que pueden ser implementados para actualizar la tabla de traslaciones, uno de los cuales es el uso del canal de registro, admisión y estado (RAS). Otros mecanismo pueden ser implementados para soportar puntos finales que no usan el canal RAS para ruteo de mensajes de comunicaciones.

8.3.2. Control de admisión

El Guardián autoriza el acceso a la red basado en guías H.323 y otros criterios usando los mensajes de requerimientos de admisión (ARQ), mensajes de confirmación de admisión (ACF), y mensajes de rechazo de admisión (ARJ). Como un resultado de los recursos compartidos limitados, no todos los usuarios serán capaces de acceder a la red al mismo tiempo. El Guardián también protege la integridad de la red para todos los usuarios de acuerdo a las políticas especificadas. Los Guardianes autorizarán los accesos a la red de acuerdo a las políticas guías que un administrador de la red ha seleccionado cuando configura un Guardián y / o una zona. El acceso a la red y servicios especiales (uso de una Pasarela, por ejemplo) pueden ser basados en autorizaciones de llamadas, uso de ancho de banda, u otro criterio.

8.3.3. Control de ancho de banda

El Guardián monitorea y controla el uso del ancho de banda en la red y asegura que el tráfico de audio y / o vídeo no exceda la carga máxima de la red definida por el administrador de red. El administrador de red tiene la capacidad de restringir el uso de tráfico H.323con la finalidad de ofrecer calidad de servicio (QoS) a otras aplicaciones más críticas. El Guardián también todos los requerimientos de cambio de anchos de banda donde no se han impuesto políticas.

8.3.4. Administración de red

El Guardián usa un modelo de ruteo llamada-señalización, para rutear llamadas señalizadas y controlar los canales para las entidades apropiadas en la red. Además, el Guardián puede implementar lógica para otorgar / denegar terminales, Pasarelas, y acceso a MCUs para elementos asociados a la red tales como ancho de banda, Pasarelas, MCU, servicios de directorio, etc. Este realiza este procedimiento monitoreando todas las llamadas concurrentes en una zona y aplicando políticas de administración de la red para cualquier nueva llamada(sesión) que el usuario puede inicializar.

8.4. Características opcionales

Para poder diferenciar entre los diversos productos del mercado, se pueden evaluar las siguientes características opcionales:

- Control de ruteo de llamadas.
- Autentificación de llamadas.
- Acceso / autorización de llamadas
- Contabilidad de llamadas
- Administración de ancho de banda
- Servicios de administración de llamadas
- Servicios suplementarios
- Servicios de directorio

8.4.1. Control de ruteo de llamadas.

Hay dos modelos para ruteo de llamadas: modo directo y modo ruteado. El modo ruteado es el modelo preferido ampliamente. Cuando el Guardián realiza el traslado de direcciones, Guardián provee puntos finales con la dirección de transporte destinados al canal de señalización de llamadas.

En el modo directo, el Guardián provee los puntos finales con la dirección del punto final destino y los direcciona al canal de señalización de llamada de modo que todos los mensajes sean intercambiados directamente entre los dos puntos sin la intervención del Guardián (ver Tabla 14).

Procedimientos de administración de requerimientos de zona	**Procedimientos y políticas opcionales**
Traslado de direcciones	Autorización de llamadas
Control de admisiones	Administración de ancho de banda
Control de ancho de banda	Servicios suplementarios
	Servicios de directorio
	Servicios de administración de llamadas
Procedimientos opcionales	
Señalización de control de llamadas	

Tabla 14. Señalización de llamada directa

Con el modo ruteado, el Guardián provee su propia dirección como la dirección de destino de modo que éste recibe todos los mensajes de señalización de llamadas y maneja el ruteo de señalización de llamada de él mismo y de todos los puntos durante la sesión. En este caso, el Guardián un canal de señalización abierto mientras hace el ruteo de llamada durante la duración de llamada. El modo ruteado es fundamental para la administración de la llamada, así se realiza la función de hunting de llamada, provee control separado sobre cada parte de la llamada conectando y desconectando cada parte separadamente, y provee servicios suplementarios y propietarios. El Guardián de modelo ruteado es el método preferido para asegurar la distribución eficiente de servicios suplementarios tan bien como mayor robustez en la administración de la red (ver Figura 8).

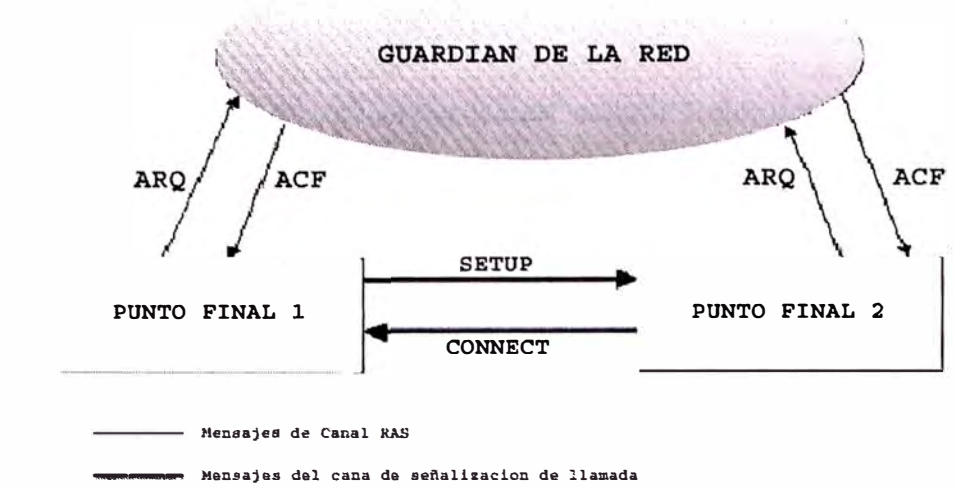

Figura 8. Señalización de ruteo llamadas

8.4.2. Autentificación de llamadas.

El Guardián tiene la capacidad para realizar funciones de autentificación de llamadas identificando el usuario o proveyendo un token dado o un certificado.

8.4.3. Acceso / autorización de llamadas

El Guardián autoriza una llamada basado en derechos de acceso de usuario. Este puede rechazar las llamadas de un terminal como resultado de una falla de autorización. La razón para rechazar puede incluir pero no estar limitados a restringir el acceso a o de un terminal particular o Pasarela y restringir el acceso durante ciertos periodos de tiempo. La administración de los sistemas de información de las corporaciones (MIS) y la administración de tecnologías de información (IT) tienen la flexibilidad para determinar los criterios de fallas y pases de autorización, basados en

razones de seguridad tales como acceso restringido a servicios o llamadas fuera de la zona.

El administrador de red puede elegir admitir todos los requerimientos bajo ciertas circunstancias de bajo uso. Es importante notar que el control de admisión es un camino para preservar la integridad de las llamadas y sesiones que están en progreso cuando un usuario requiere acceso. Las políticas también pueden ser implementadas para terminar una llamada saliente ante un requerimiento de alta prioridad.

8.4.4. Contabilidad de llamadas

Una vez que la llamada es terminada, el Guardián a la entidad de contabilidad los detalles de la llamada. El Guardián puede funcionar también en cooperación con los sistemas de back-Office para generar la facturación. La información generada puede incluir muchos detalles como la duración de la llamada, origen, destino, y QoS.

8.4.5. Administración de ancho de banda

El Guardián puede controlar y limitar el número de terminales H.323 permitidos para el uso simultáneo de la red. A través de la señalización H.225.o, el Guardián es capaz de limitar el ancho de banda de las llamadas así rechazará cuando no hay suficiente ancho de banda. El Guardián puede trabajar en conjunción con un servidor QoS mejorar el QoS de las llamadas. Esta función también opera durante una llamada activa cuando un terminal de usuario requiere mas ancho de banda.

8.4.6. Servicios de administración de llamadas

El Guardián es capaz de mantener una lista de llamadas salientes H.323 esto es similar a un log PBX. Esta información es necesaria para indicar que un terminal de llamadas está ocupado y para proveer información para la función de administración de ancho de banda.

8.4.7. Servicios suplementarios

Servicios suplementarios por el estándar H.450, tales como el reenvío y transferencia, estos son funciones criticas que los usuarios de telefonía en empresas esperan que su red provea. Ambos, el Guardián y el terminal puede proveer soporte para los servicios suplementarios; sin embargo, el Guardián realiza esta tarea con menos complejidad computacional y carga en el lado del cliente.

8.4.8. Servicios de directorio

La base de datos del Guardián contiene los perfiles del usuario que proveen la información necesaria para la implementación de los servicios de directorio para ayudar a un usuario a encontrar a otro. Este puede acceder a otro servicio de directorio (tales como a un ILS) que son actualizados o configurados con la información necesaria para la conexión de llamadas.

8.5. Aplicaciones, rol actual y futuro.

8.5.1. Aplicaciones prácticas

La función del Guardián es ser eficaz y adaptable a las necesidades de la red H.323 de un ISP o de un carrier. Cuando se le uso en su total funcionalidad, una organización puede maximizar su productividad y flujo de trabajo.

Algunos ejemplos prácticos de cómo el Guardián puede ayudar a las organizaciones, son:

- ISPs pueden cobrar por garantizar el ancho de banda y empaquetar servicios especiales.
- Los administradores de Intranet tienen pueden interoperar entre planes de discado PBX y terminales IP.
- Los administradores de red tienen interfaces rápidas y fácil de usar para modificar o actualizar configuraciones de zonas cuando un individuo en la red necesita servicios adicionales.
- Los call center multimedia para servicios de clientes, realizan ruteo de llamadas basados en la necesidad y una variedad de otras características automáticas de distribución de llamadas.

8.5.2. Rol actual

A pesar que el Guardián se consideró inicialmente como un componente opcional en una red H.323 por el ITU, éste se ha convertido en una herramienta esencial, ayudando a las organizaciones a mantener ventajas comparativas en un fuerte mercado competitivo. En el mercado empresarial basado en la productividad y en el retorno de inversión, el Guardián se ha convertido en el jugador clave en actualizar las estructuras de las intranets corporativas para soportar capacidades de centrales IP y comunicaciones multimedia en tiempo real. Incorporando el Guardián, las compañías son beneficiadas en el mejoramiento de su productividad y el incremento de sus rentas como resultado de una eficiente y efectiva colaboración entre sus trabajadores, clientes y cadena de vendedores de suministros. Además, las organizaciones se favorecen en el ahorro de costos por la telefonía IP, evitando algunas aplicaciones y simplificando la administración de la red.

Para proveedores de servicios, el Guardián genera nuevos flujos de rentas al puentear las redes de telefonía pública conmutada (PTSN) con redes IP, respondiendo a la urgente necesidad de interoperatividad a través de la red de telecomunicaciones global. Para satisfacer la demanda de alta calidad, redes de transporte de bajo costo, los ISPs deben tener Guardianes al igual que los carrier para transportar efectivamente las llamadas y así mejorar sus rentas.

8.5.3. Futuro

Desde que el protocolo ITU H.323 y el Guardián están comercialmente disponibles, la revolución de las comunicaciones IP han parado, y las

comunicaciones de voz y vídeo en tiempo real sobre redes están siendo desarrollados globalmente en empresas y en entornos de carriers. Ahora, cientos de miles de personas alrededor del mundo usando productos y servicios basados en Guardianes en telefonía IP. Como el número IP de los dispositivos conectados y personas crece y alcanza valores críticos, las comunicaciones IP serán un lugar común, y el Guardián continuará jugando un papel importante generando nuevas aplicaciones y nuevos servicios en la red.

CAPÍTULO IV

SOFTWARE OPENSOFT H.323

4.1. Introducción

El Internet es parte ya de nuestras comunicaciones. Muchos de nosotros gastamos mucho tiempo enviando correo electrónico a amigos y familiares, revisando los sitios de noticias, y navegando en la red por entretenimiento e investigación.

Gran parte de la empresas y monopolios en el mundo han dicho que H.323 será la manera en que nos comunicaremos en el futuro, ya sea por telefonía IP o videoconferencia o simplemente compartiendo datos. Todo eso es perfecto y bueno, pero el H.323 no es libre ni abierto. Esto es entrampado por las patentes y derechos intelectuales de propiedad, las especificaciones registradas en el registro de la propiedad literaria y grupos de estándares que no son basados en Internet. Los derechos que licencian algunos de los codificadores del H. 323 puede exceder los $100,000, y simplemente comprar todas las especificaciones pueden convertir a un hombre rico en pobre.

El objetivo del OpenH323 es desarrollar un estándar libre y abierto para el uso del Internet, y en el proceso, mejorarlo y trabajado para la comunidad del Internet. Este proceso ayudará el desarrollo de las características del H.323 a largo

plazo, así como las características innecesarias serán descartadas, hasta que se implemente una referencia limpia y funcional, de modo que el mercado y su uso crezcan lo que no es posible bajo las condiciones actuales.

El modelo de desarrollo "consenso áspero y código corriendo" de Internet, a la par con el código abierto y la fuerza intelectual mundial de centenares de desarrolladores y probadores, ha producido algunos de los más eficientes aplicativos y sistemas seguros. Tenemos como ejemplo el Apache, Sendmail, y Linux.

4.2. OpenH323

El proyecto OpenH323 se propone crear una implementación en código abierto del protocolo de teleconferencia H.323 de la ITU, con todas sus características y totalmente interoperable, que puede ser usado por desarrolladores personales y usuarios comerciales sin ningún costo.

El desarrollo del OpenH323 es coordinado por la compañía Australiana Equivalencia Pty Ltda, pero está abierto a cualquier interesado. Se fomenta el uso comercial y privado del código OpenH323, inclusive el uso en productos y reventa comerciales, a través del MPL (Mozilla Public License).

Este proyecto se inició en Septiembre de 1998.

OpenH323 es necesario porque las implementaciones comerciales de la pila de protocolos H.323 son costosas en licenciamiento y distribución. Ellas también contienen IP propietarias que no pueden ser usadas o distribuidas sin el permiso de los propietarios y no son código abierto. Si usuarios normales o compañías pequeñas están creando aplicaciones y servicios que requieren el uso del protocolo H.323, ellos

también deben tener la oportunidad de encontrarlas al igual que las grandes corporaciones.

4.2.1. Contribuciones

Las siguientes personas y compañías han aportado con recursos y espacios web a éste proyecto:

- Equivalence Pty Ltd: Iniciador del proyecto, y continúa siendo el mayor contribuyente de código fuente.
- Quicknet Technologies: Adquirida por la empresa anterior en marzo del 2000, ha continuado promoviendo el desarrollo del proyecto.
- Derek Smithies de la compañía Indranet, quien ha desarrollado el codec de vídeo para el proyecto, y continua apoyando en las listas de correo.
- Roger Hardiman , quien ha desarrollados los puertos xBSD para MAC.
- Los puertos WindowsCE de PwLib y OpenH323, y muchos de los puertos BeOS, han sido provistos por Yuri Kiryanov.
- Otros contribuyentes son: Graeme Reid & Frank Derks (H.450), Mark Cooke (conversores y videograbadores), Franz Furbass (H.235), Michele Piccini (H.261) y muchos otros.
- Vovida Networks ha provisto recursos y es parte de una alianza estratégica con Equivalence Pty Ltd para llevar al OpenH323 a un uso comercial.
- iFace.com ha provisto de material para el desarrollo del soporte del guardián.

4.2.2. Características implementadas

- Algoritmo de umbral dinámico, para detección de silencio.
- Cliente gráfico para Windows.
- Cliente en línea de comandos, para Linux, Windows y otros.
- MCU , pasarela PSTN y máquina contestadora para todas las plataformas.
- Codificadores de voz soportados en software: GSM full rate (06.10), LPC-10 y G.711 ley u y G.711 ley A.
- Codificadores de voz soportados con hardware adecuado: G.723.1, G.728 y G.729 .
- Soporte para Quicknet xJack (únicamente Linux y Win32)
- Soporte de tarjetas Voicetronics VPB4 (únicamente Win32)
- Supresión de silencio.
- Transmisión y recepción de vídeo H.261 (Linux, BSD y Win32)
- Soporte de cliente Guardián (RAS), con descubrimiento broadcast y multicast.
- Soporte del anexo D H.235 para acceso de Guardianes.
- Inicio rápido y tunnelling H.245.
- Mensajes de indicación al usuario.
- Soporte de algunos H.450
- Librería compartidas y DLL's

4.2.3. Características por implementar

- Tamaño de buffer ajustable dinámicamente, basado en estadísticas RTP.
- Servicio de directorio de guardianes (soporte LRQ).
- Soporte para más tarjetas telefónicas (Especialmente las de alta densidad).
- Soporte H.263 (si es posible por el tema de patentes ...)
- Más soporte H.450.
- Más soporte de seguridad y encriptamiento H.235.
- Transporte Multicast para RTP.
- Soporte para controlador multipunto (conferencia).
- Soporte para conferencias T.120.

4.2.4. Proyectos relacionados

Muchas personas están trabajando en otros proyectos basados en H.323:

- Yuri Kiryanov ha hecho grandes trabajos con OpenH323 sobre Windows CE y BeOS (http://www.dogsbone.com)
- Jan Willamowius está trabajando sobre un Guardián H.323 usando OpenH323 bajo GPL. (http://www.willamowius.de/openh323gk.html)
- Motonori Shindo ha escrito un decodificar PDU (http://www.mbuf.org/~moto/h323/h323decoder.html)
- Benny LP ha desarrollado un Generador de Llamadas para pruebas y análisis de performance. (http://callgen323.sourceforge.net/)

- Damian Slee ha creado un control OCX que permite acceder al OpenH323 desde Visual Basic. (http://www.geocities.com/rddamian/)

- Ashley Unitt ha desarrollado otro Guardián en código abierto, sin las restricciones de GPL. (http://www.opengatekeeper.org/)

- Marco Budde ha producido una Pasarela ISDN a H.323 (http://www.telos.de/linux/H323/default_e.htm)

- Carlos Sevilla ha desarrollado otra Pasarela ISDN a H.323 (http://www.openisdngw.org/)

- Damien Sandras ha escrito un cliente gráfico H.323 Client llamado GnomeMeeting para Linux (x86/sparc/ppc) y FreeBSD. (http://www.gnomemeeting.org/)

- Andreas Sikkema ha añadido decodificación H.323 a Ethereal (analizador de protocolos gratuito) (http://www.voice2sniff.org/).

4.3. Implementación de aplicativo con OpenH323

En esta sección se explica como realizar la implementación de una red básica H.323, usando el OpenH323. Los componentes ha implementar son los siguientes:

- **Guardián:** Se instalará en sistema operativo Linux, lo cual es recomendado para una mejor performance.

- **Terminal de voz:** Se instalará tanto en Windows como en Linux, con el fin de satisfacer las necesidades de los diferentes usuarios.

- **Unidad de control multipunto:** Se instalará en Linux, también por lograr una mejor performance.

4.3.1. Software necesario

Todo el software que se utilizará está disponible en la siguiente dirección: **http://www.openh323.org** , tanto en fuentes como compilado.

- **PWLib V1.3.8:** Es librería de código multiplataforma que puede ser usado para escribir aplicaciones que corren tanto en Windows, Linux y unas pocas variantes de Unix. Este ha sido desarrollado por Equivalence, y es también de código abierto.

- **OpenH323 V1.9.7:** (Requiere de PWLib). Es la implementación en código abierto de la pila de protocolos H.323, el cual puede ser usado tanto para aplicaciones privadas como comerciales. Ha sido desarrollado por el proyecto OpenH323.

- **OpenPhone V1.5.4:** (Requiere de PWLib, OpenH323). Es el terminal de voz (cliente H323) para ambiente Windows.

- **GnomeMeeting V0.93:** (Requiere de PWLib, OpenH323). Es un terminal de vídeoconferencia para Gnome (interfaz gráfica para Linux).

- **OpenMCU V1.0.19:** (Requiere de PWLib, OpenH323). Es la Unidad de Control multipunto, que permite desarrollar multi conferencias.

- **OpenGK V2.0a:** (Requiere de PWLib). Es el Guardián H323, desarrollado usando el OpenH323 bajo licencia GPL (GNU General Public License).

4.3.2. Hardware necesario

- Excepto por las computadoras necesarias, no se necesita hardware adicional.

- El Guardián y el MCU pueden estar en una misma máquina, no menor de Pentium III con 256 MB de memoria (funciona en menos, pero es recomendable para obtener una óptima performance)

4.3.3. Instalación

Bajar el software desde la siguiente dirección: http://www.openh323.org :

Software	Sistema Operativo	Tipo de archivo
Pwlib 1.3.8	Linux	Código fuente
Openh323 1.9.7	Linux	Código fuente
Pwlib 1.3.8	Windows	DLL
Openh323 1.9.7	Windows	DLL
OpenGk 1.2.3	Linux	Código fuente
OpenMCU 1.0.19	Linux	Código fuente
OpenPhone	Windows	EXE
GnomeNetmeeting	Linux	RPM

- **Librerías:**

Windows: No es necesario compilar, tanto la librería OpenH323 como la Pwlib pueden bajarse compiladas como DLL.

Linux: A pesar que se puede bajar ya compiladas, es recomendable bajar el fuente y compilarlos, para lo cual se debe seguir los siguientes pasos:

Desempaquetar y descomprimir:

[Host]$ tar xvfz openh323_1.9.7.tar.gz

[Host]$ tar xvfz pwlib_1.3.8.tar.gz

Configurar variables de entorno:

[Host]$ export PWLIBDIR=$HOME/pwlib

[Host]$ export OPENH323DIR=$HOME/openh323

[Host]$ export LD_LIBRARY_PATH=$PWLIBDIR/lib:$OPENH323DIR/lib

- Compilar la librería PwLib: (necesario GNU make [=3.75], bision [>=1.25] y flex [>=2.5.4], la mayoría de los Linux's viene con estos paquetes)

  [Host]$ cd $PWLIBDIR

  [Host]$ make both

- Compilar la librería OpenH323:

  [Host]$ cd $OPENH323DIR

  [Host]$ make both

- **Guardián:**

Linux: Existen varios tipos de Guardianes desarrollados con OpenH323, nosotros experimentaremos con el Guardián ofrecido por el proyecto OpenH323:

- Desempaquetar y descomprimir:

  [Host]$ tar xvfz gk-2.0a.tgz

- Compilar:

  [Host]$ cd openh323gk

  [Host]$ NO_LDAP=1 make both

- **Terminal de voz:**

OpenPhone (Windows): Se debe seguir los siguientes pasos:

Descomprimir el archivo zip en una nueva carpeta.

Descomprimir las librerías PwLib y OpenH323 en el mismo directorio.

Ejecutar el comando openphone.exe, luego de cual aparecerá el terminal.

GnomeMeeting (Linux): Viene con el RedHat 8.0 (Distribución de Linux)

- **Unidad de control multipunto:**

Linux: Se debe seguir los siguientes pasos:

Desempaquetar y descomprimir:

[Host]$ tar xvfz openmcu_1.0.19.tar.gz

Compilar:

[Host]$ cd openmcu

[Host]$ make both

4.3.4. Funcionamiento

Se deberá seguir los siguientes pasos:

1. Iniciar el Guardían y el MCU, en Linux:

   [Host]$ cd $HOME/openh323gk/obj_linux_x86_r

   [Host]$ ./gnugk -r –b 10000000 &

   [Host]$ cd $HOME/openmcu/obj_linux_x86_r

   [Host]$ ./openmcu

2. Iniciar el terminal en un PC Windows: Se deberá ejecutar el archivo openphone.exe. Se configurará el codificador de audio G.711-Alaw, como primero en la lista de codificadores y la habilitar la opción de Guardián.

3. Iniciar el terminal el GnomeMeeting en Linux, y configurar el Guardián:

4. Con los componentes instalados se puede realizar comunicaciones de voz, vídeo y voz, así como videoconferencias.

RECOMENDACIONES Y CONCLUSIONES

1. La suite de protocolos H.323 es un estándar de comunicaciones desarrollado por la Unión Internacional de Telecomunicaciones (ITU), que especifica los componentes, protocolos y procedimientos que proveen servicios de comunicación multimedia (comunicaciones de audio, vídeo y datos en tiempo real).

2. Este estándar está teniendo gran aceptación en todo tipo de corporaciones, por ser simple y útil.

3. Se recomienda que en toda red multimedia H.323 debe configurarse al menos un Guardián H.323, para aprovechar al máximo de todas las bondades que este tipo de red ofrece, este componente actualmente se está convirtiendo en el corazón de esta red.

4. Se recomienda mayor investigación respecto al software OpenH323, que implementa la suite de protocolos H.323, y que además es de código abierto, pues permite a todos el hacer uso de este estándar sin tener que pagar sumas por patentes, derechos de propiedad, etc. Se recomienda su uso en universidades, las que también podrían colaborar en el desarrollo del mismo, como un aporte a todas aquellas personas que gustan del software libre, y que solo así podemos estar al tanto de la tecnología.

ANEXO A: GLOSARIO

POP	Protocolo para lectura de e-mails (Post Office Protocol)
ACF	Confirmación de admisión (admission confirmation)
ANSI	American National Standard Institute
Apache	Servidor web http de código abierto
AppleTalk.	Protocolo de bajo nivel
ARJ	Rechazo de admisión (admission reject)
ARP	Protocolo de resolución de Direcciones (Address Resolution Protocol)
ARQ	Petición de admisión (admission request)
ATM	Modo de transferencia asíncrono (asynchronous transfer mode)
Back-Office	Concepto referido a la infraestructura no visible
BCF	Confirmación de cambio de ancho de banda (bandwidth change confirmation)
BeOS	Sistema Operativo especializado en multimedia
BNC	Conector de cable coaxial (Bayone-Neill-Concelman)
BRQ	Petición de cambio de ancho de banda (bandwidth change request)
BSD	Distribución de Software (Berkeley Software Distribution)
BUS	Topología de red
BW	Ancho de Banda (Band Width)
Call Center	Centro donde se concentran todas las llamadas
Carrier	Empresa dedicada al transporte de información
CCITT	Comité Consultatif International Telégraphique et Teléphonique
CDDI	Protocolo de bajo nivel (Copper Distributed Data Interface)
CID	Identificador de conferencia (conference identifier)
CIR	Tasa de información asegurada(Commited Information Rate)

CPU	Unidad de procesamiento central (Central Processing Unit)
CRV	Valor de referencia de llamada (Call Reference Value)
CSMA/CD	Acceso múltiple por detección de portadora con detección de colisiones(Carrier Sense Multiple Access with Collision Detection)
DARPA	Defense Advanced Research Projects Agency
DCF	Confirmación de desligamiento (*disengage confirmation*)
DECnet.	Digital Equipement Corporation net
DLL's	Librería de enlace dinámico (Dinamic Link Library)
DNS	Sistema de nombres de dominio (domain name system)
DRQ	Petición de desligamiento (*disengage request*)
E.164	Plan de numeración para telefonía
EGP	Extern Gateway Protocol
Ethereal	Analizador de protocolos gratuito
Ethernet	Protocolo de bajo nivel
FDDI	Fiber Distributed Data Interface
Frame Relay	Protocolo de bajo nivel
FreeBSD	Sistema Operativo para PC (Operating System)
FTP	Protocolo para transferencia de archivos (File Transfer Protocol)
G.711	Estándar para codificación de voz
G.723.1	Estándar para codificación de voz (dual)
G.728	Estándar para codificación de voz (bajo retardo)
G.729	Estándar para codificación de voz (menor bit rate que el G.728)
Gatekeeper	Componente de una red H323 (Guardián)
Gateway	Pasarela
GCF	Confirmación de controlador de acceso (*gatekeeper confirmation*)
GQOS	Calidad de servicio garantizada (guaranteed quality of service)
GRQ	Petición de controlador de acceso (*gatekeeper request*)

GSM	Sistema de telefonía celular (Global System for Movile Comunications)
H.221	Estándar para servicios audiovisuales (teleconferencia)
H.225	Especifica la señalización de llamadas
H.245	Especifica el control de señalización
H.246	Estándar para pasarelas H.323
H.261	Estándar para codificación de video
H.320	Estándar para videoconferencia
H.450	Especificación suplementaria que define señalización y procedimientos para proveer tanto telefonía como servicios
H.323	Suite de protocolos para comunicaciones multimedia
HARDWARE	Se refiere a la parte física de un equipo
HDLC	Control de alto nivel del enlace de datos (high level data link control)
HOST	Máquina, servidor, PC
HTTP	Protocolo de transferencia de hipertexto (hypertext transfer protocol)
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identificador
IEEE	Institute of Electric and Electronic Engineers
IETF	Internet Engineering Task Force
iGSM	Sistema de telefonía celular orientado a Internet (Internet Global System for Movile Comunications)
ILS	Internet List Service
IMTC	International Multimedia Teleconferencing Consortium
Internet	Red de redes
Intranet	Red corporativa
IP	Protocolo Internet (Internet protocol)
IPX	Intercambio de protocolo de inter red (internetwork protocol exchange)
SPX.	Sequenced Packet eXchange

IRQ	Petición de información (information request)
IRR	Respuesta a petición de información (*information request response*)
ISO	International Organization for Standardization
ISP	Proveedor de servicio de Internet (Internet Service Provider)
IT	Tecnologías de la información (Information Technologies)
ITU	International Telecomunication Union
LAN	Red de área local (Local Area Network)
LINUX	Versión UNIX para Pcs, en código abierto.
LLC	Logical Link Control
LPC-10	Técnica de análisis de voz (Linear Predictive Coding)
LRQ	Petición de localización (*location request*)
MAC	Dirección física de una interfaz de red (Media Access Control)
MAC(PC)	Tecnología de microcomputadores (Macintosh)
MAN	Red de cobertura metropolitana (Metropolitan Area Network)
MC	Controlador multipunto (multipoint controller)
MCU	Unidad de control multipunto (multipoint control unit)
MIS	Administración de sistemas de información (Management Information System)
MP	Procesador multipunto (multipoint processor)
MPL	Licencia pública Mozilla (Mozilla Public License)
MTU	Unidad de transmisión máxima (maximum transmission unit)
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
OCX	Control de Windows
OPENSOFT	Software de código abierto
OPSF	Open Protocol Shortest Path First
OSI	Modelo de referencia Interconexión de sistemas abiertos

PBN	Red por paquetes (packet based network)
PBX	Private Branch Exchange
PC	Computador personal (Personal Computer)
PDU	Unidad de datos de paquetes (packet data unit)
PPP	Protocolo punto a punto (Point to Point Protocol)
PRI	Interfaz de velocidad primaria (primary rate interface)
PTSN	Red servicios de telefonía privada (Private Telephony Service Network)
PVC	Policloruro de vinilo
PwLib	Librería multiplataforma para lenguaje C
PYMES	Pequeñas y medianas empresas
Q.931	Protocolo de control de conexión ISDN
QOS	Calidad de servicio (quality of service)
RARP	Protocolo de resolución inversa de direcciones (Reverse Address Resolution Protocol)
RAS	Registro, admisión y situación
RCC	Red con conmutación de circuitos
RCF	Confirmación de registro (registration confirmation)
RCF	Confirmación de registro (*registration confirmation*)
RDSI	Red digital de servicios integrados
RDSI-BA	Red digital de servicios integrados de banda ancha
RDSI-BE	Red digital de servicios integrados de banda estrecha
RIP	Route Information Protocol
RJ-45	Conector de cable UTP
RMOA	Real-Time Multimedia over ATM
RRJ	Rechazo de registro (*registration reject*)
RRQ	Petición de registro (*registration request*)
RTCP	Protocolo de control en tiempo real (*real time control protocol*)

SDP	Protocolo de descripción de sesión (Session Description Protocol)
Sendmail	Agente de transferencia mensajes, en código abierto
SIP	Estándar para comunicaciones multimedia desarrollado por IETF (Session Initiation Protocol)
SMTP	Protocolo para transferencia de e-mails (Simple Mail Transfer Protocol)
SNMP	Protocolo para monitoreo y control de equipos (Simple Network Management Protocol)
SOFTWARE	Se refiere a la parte lógica de un equipo (programas)
SPARC/PPC	Tecnología de micropocesadores de la empresa Sun Microsystems
SPX	Intercambio de protocolo secuencial (sequential protocol exchange)
STACK	Pila
STP	Shieles Twisted
T.120	Estándar de teleconferencia multimedia
TCP	Protocolo de control de transporte (transport control protocol)
TELNET	Protocolo para acceso remoto a un computador
Token Ring	Protocolo de bajo nivel
Token Bus	Protocolo de bajo nivel
TSAP	Transport Service Access Point
UAC	User Agent Client
UAS	User Agent Server
UDP	Protocolo de datagrama de usuario (user datagram protocol)
UIT-T	Unión Internacional de Telecomunicaciones - Sector de Normalización de las Telecomunicaciones
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VoIP	Voz sobre IP
VPB4	Tarjeta para voz sobre IP de la empresa VoiceTronix

WAN	Red de área extensa (Wide Area Network)
Win32	Sistema operativo Windows de 32 bits
WindowsCE	Sistema operativo Windows para computadores de mano
X.25.	Protocolo de Red
x86	Computador compatible
XBSD	Sistema operativo

BIBLIOGRAFÍA

[1] ITU-T SG16. Recommendation H.323: Packet-based multimedia communications systems. International Telecommunication Union. Sept., 1999. http://etsi.org/tiphon

[2] Karim, Asim. H.323 and Associated Protocols. http://www.cis.ohio-state. edu/~jain/cis788-99/h323/index.html. Ohio State University. USA, febrero de 2000.

[3] Hersent, O., D. Gurle and Jean-Pierre Petit. IP Telephony, Packet-Based Multimedia Communications Systems. Addison-Wesley, 2000.

[4] Toga, J. and H. ElGebaly. Demystifying Multimedia Conferencing Over the Internet Using the H.323 Set of Standards. Intel Technology Journal. 1998 http://developer.intel.com/technology/itj/q21998/articles/art_4.htm

[5] Consorcio Internacional de Teleconferencia Multimedia. http://www.imtc.org

[6] Thomsen, Guy and Yashvant Jani. Internet Telephony: Going like crazy. IEEE Spectrum, Vol 37, N° 5. Institute of Electrical and Electronics Engineers, Inc. USA. May, 2000

[7] Carlos M. Pazos, Marek. R. Kotelba and Andrew G. Malis. Real-Time Multimedia over ATM. IEEE Communications, Vol 38, N° 4. Institute of Electrical and Electronics Engineers, Inc. USA. April, 2000.

[8] Herman C. H. Rao, Yi-Bing Lin and Sheng-Lin Cho. iGSM: Voice Service for Mobile Networks. IEEE Communications, Vol 38, N° 4. Institute of Electrical and Electronics Engineers, Inc. USA. April, 2000.

[9] IP x Stream market research. **http://www.iptelephony.org/GIP/vendors**

[10] Arora, Rakesh. Voice over IP: Protocols and Standards. http://www.cis.ohio-state.edu/~jain/cis788-99/voip_protocols/index.html. Ohio State University. USA, febrero de 2000.