UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

VOZ SOBRE EL PROTOCOLO DE INTERNET (VoIPv4).

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

MARCOS ISRAEL MARTINEZ SOTO

ASESOR: ING. JOSE JUAN CONTRERAS ESPINOSA

CO-ASESOR: ING. JOSE LUZ HERNANDEZ CASTILLO

CUAUTITLAN IZCALLI, EDO. DE MEX. 2004

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO.

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN.

VOZ SOBRE EL PROTOCOLO DE INTERNET (VoIPv4).

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECÁNICO ELECTRICISTA.

PRESENTA

MARCOS ISRAEL MARTÍNEZ SOTO.

ASESOR: ING. JOSÉ JUAN CONTRERAS ESPINOSA.

CO-ASESOR: ING. JOSÉ LUZ HERNÁNDEZ CASTILLO.

CUAUTITLAN IZCALLI, EDO. DE MÉXICO 2004.

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:

Voz sobre el Protocolo de Internet

que presenta el pasante: Marcos Israel Martinez Soto
con número de cuenta: 9105046-8 para obtener el titulo de :
Ingeniero Mecanico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 30 de Enero de 2004

PRESIDENTE	Ing. Jose Juan Contreras Espinosa	
VOCAL	Ing. Jorge de la Cruz Trejo	
SECRETARIO	M.C. Ramon Fuentes Villaseñor	
PRIMER SUPLENTE	Ing. Roberto Reyes Arce	
SEGUNDO SUPLENTE	Ing. Marcelo Bastida Tapia	

DEDICATORIAS.

Agradezco a Dios y a mis Padres que me ayudaron en la vida a llegar hasta esta etapa de mi carrera profesional, a mi Madre que se desvelo tanto años y me apoyo a continuar con la escuela con sus consejos y regaños. A mi hermana por ayudarme durante toda la carrera profesional y en la vida.

A Irma por darme su apoyo y comprensión en la escuela y en las situaciones difíciles que pasamos juntos.

A mis profesores y demás personas que me ayudaron y animaron a seguir adelante.

GRACIAS

ÍNDICE.

Capitulo 3- H.323.

Capítulo 4- Aplicaciones de VoIPv4.

INTRODUCCIÓN.

La Voz es el medio de comunicación en todo el mundo por el cual se han comunicado entre sí la humanidad a lo largo de la historia y ha servido para el adelanto en las comunicaciones de hoy en día, todo esto lleva a que en la actualidad con todos los sistemas de comunicación como son teléfonos, computadoras y sus aplicaciones como Internet se quieran integrar todas ellas en una sola tecnología, todo esto con el fin de un fácil acceso para cada persona, en cualquier parte del mundo que se requiera hacer uso ella.

Todo esto es aplicado a una nueva tecnología existente llamada "Voz sobre el protocolo de Internet", la cual consiste en que la voz es tratada como un paquete de información y es transportada sobre los cables de cobre de las redes telefónicas y de computadoras existentes en las ciudades de todo el mundo para que lleguen a su destino, todo esto en una de sus muchas aplicaciones llamada "Telefonía sobre el Protocolo de Internet" con la cual se podrán hacer llamadas telefónicas locales e internacionales sobre la red mundial de computadoras llamada Internet, a un precio muy bajo y con un teléfono especial, además se podrán realizar cosas como revisar el correo electrónico, acceder a paginas de Internet.

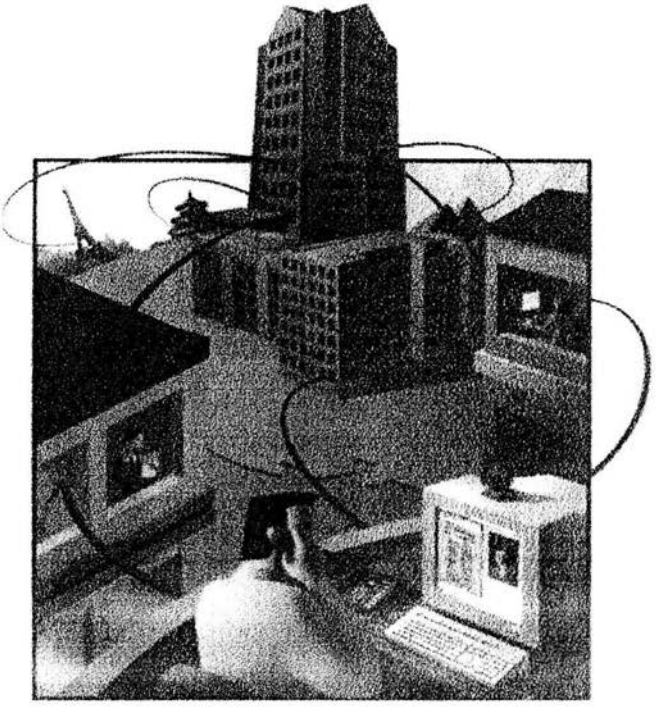
Entre otra de sus aplicaciones, la "Videoconferencia" es mas utilizada dentro de las empresas, universidades y hospitales, ya que se puede hablar y ver a cualquier persona de cualquier parte del mundo desde el hogar o la empresa, a un costo muy bajo y en cualquier momento. En los hospitales su usada en la "Telemedicina", ya que su funcionamiento es aplicado en los pacientes que ya no son translados a las ciudades grandes para una consulta menor y para las preguntas que tengan los médicos en los tratamientos requeridos para los pacientes, además de que sirve para conferencias entre médicos de diferentes lugares y de que ya no se tendrán que trasladarse hasta el lugar de la conferencia, ahorrándose todo esto en transporte y hospedaje de las personas involucradas.

Asimismo la Voz sobre IP tiene como ventaja la disminución de costos en el precio de las llamadas telefónicas nacionales e internacionales, en el cableado de redes con la integración de un solo cable para la voz y los datos, así como la implementación de algunas reglas o protocolos para asegurar su buen funcionamiento en las empresas y hogares del todo el mundo, además de la integración de las compañías telefónicas para su uso y funcionamiento de esta tecnología nueva.

Dentro de las desventajas se necesitan medidas tecnológicas, y de reglamentos por parte del gobierno y empresas para su buena aplicación y uso dentro la vida diaria, así como los diferentes fabricantes de todas estas aplicaciones deben ser compatibles sus tecnologías entre sí para que se puedan usar por todas empresas y hogares del mundo.

VOZ SOBRE EL PROTOCOLO DE INTERNET

(VoIPv4)



CAPITULO 1
VOZ Y PROTOCOLO DE INTERNET (IPv4).

1.1.- Voz.

Es el sonido producido por las cuerdas vocales humanas para transmitir información a través de algún medio (físico o no físico), el cual consiste en ondas de presión que causan vibraciones audibles e inaudibles en el aire para el oído humano y para que se produzca un sonido deben de existir 3 elementos:

- Fuente sonora (un cuerpo que vibre).
- Medio elástico de transmisión (aire).
- Receptor (oído humano).

1.1.2.- Características.

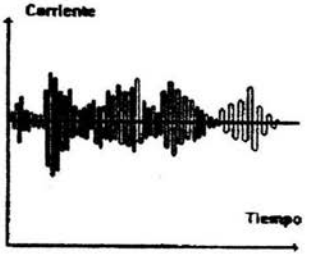
Tiene las siguientes que son:

a- Amplitud o Intensidad (energía que pose el sonido).
b- Frecuencia o Tono (no. de vibraciones por segundo).
c- Forma o Timbre (característica que distingue a 2 fuentes sonoras distintas de igual intensidad y frecuencia).

De las características del sonido hay 2 que son medibles:
1- Intensidad o Potencia- Es su fuerza relativa y su unidad de medida es el decibel (dB).
2- Frecuencia- Es el no. de veces ó ciclos que se repite una señal por segundo en un periodo de 2 Π rad. o 360° grados, y se mide en ciclos por segundo (hz.).

Debido a que el sonido como tal no puede ser transmitido a grandes distancias, es necesario convertir la señal de voz o sonora en una señal eléctrica, ya que en un sistema telefónico la voz se convierte en señal eléctrica para ser transmitida a través de la red. Por ejemplo como en la fig. 1 que muestra la forma de onda de una señal eléctrica de voz, es decir que una señal de voz se ha convertido en una señal eléctrica para su transmisión.

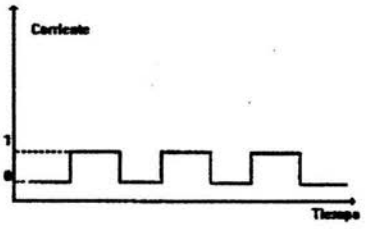
fig. 1
Señal analógica.



A esta señal se le conoce como señal analógica y sus características son amplitud, frecuencia y fase; pudiendo observar que la señal de voz de la fig. 1 tiene cambios muy repentinos en amplitud y frecuencia, debido a esto y a otros factores para realizar una transmisión más eficiente de la información contenida en esa señal eléctrica es necesario modificar en otra que permita realizar esto, la cual se le conoce como señal digital.

Una señal digital consiste en serie de pulsos, el cual se representa por una onda cuadrada en la fig. 2 y tiene como características amplitud, fase y frecuencia, y solo tiene 2 valores 0 y 1.

fig. 2.
Señal digital.

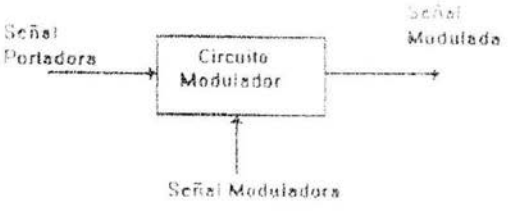


Debido a que la señal eléctrica de voz analógica como la digital son señales de baja frecuencia que no pueden ser transmitidas a grandes distancias, es necesario trasladar la información que contiene estas señales de baja frecuencia a señales de alta frecuencia que tiene la fuerza necesaria para viajar grandes distancias. Al proceso de modificar las características de una señal (amplitud, fase y frecuencia) de alta frecuencia a partir de otra de baja frecuencia se conoce como Modulación.

Este proceso consta de 3 etapas como en la fig. 3, las cuales son:

1- Señal Portadora- Es la señal de alta potencia que tiene la fuerza necesaria para recorrer grandes distancias.
2- Señal Moduladora- Es la señal de baja potencia que tiene la información a ser transmitida.
3- Señal Modulada- Es la señal resultante del proceso de modulación.

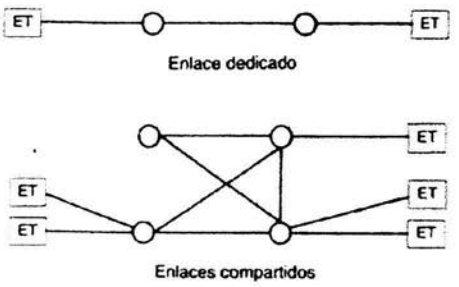
fig. 3
Modulación.



1.2.- Tipos de Conmutación.

La Redes conmutadas consisten en una sucesión alternante de nodos y canales de comunicación, es decir, después de ser transmitida la información a través de un canal, llega a un nodo, éste a su vez, la procesa lo necesario para poder transmitirla por el siguiente canal para llegar al siguiente nodo, y así sucesivamente de la fig. 4. Existen 2 tipos de conmutación en este tipo de redes: Conmutación de paquetes y Conmutación de circuitos.

Figura 4
Red conmutada.

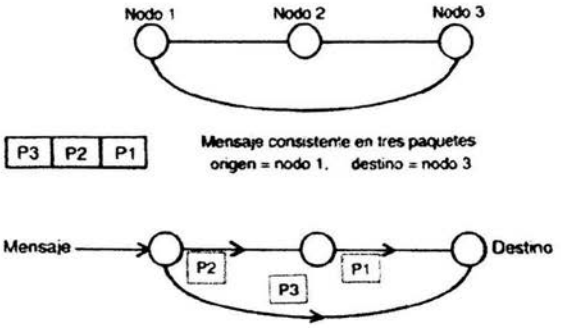


1.2.1.- Conmutación de paquetes.

Esta técnica se creo con la finalidad de utilizar mas eficientemente los medios de transmisión en sistemas multiusuario con trafico de ráfaga, aquí los datos de diferentes usuarios o aplicaciones pueden compartir una misma trayectoria fisica.

El mensaje se divide en pequeños paquetes independientes, a cada uno se le agrega información de control (por ejemplo, las direcciones del origen y del destino), y los paquetes circulan de nodo en nodo, posiblemente siguiendo diferentes rutas. Al llegar al nodo al que está conectado el usuario destino, se reensambla el mensaje y se le entrega en la fig. 5.

Figura 5
Conmutación de paquetes.



Los paquetes de datos es una secuencia de bits de un determinado tamaño que es enviada de una red como unidad individual, los paquetes son ensamblados en el nodo destino para obtener la información o mensaje transmitido, cada paquete que es enviado contiene bits de encabezado donde se puede encontrar información de la dirección del nodo fuente y destino.

El numero de secuencia del paquete y bits de verificación de errores para control, un sistema de conmutación de paquetes acepta paquetes de un nodo fuente, los almacena en el buffer de memoria de un conmutador y luego las retransmite a otro conmutador del sistema donde la misma operación de almacenaje-retransmisión ocurre.

Un sistema de este tipo no necesita que una trayectoria física dedicada sea establecida de antemano entre el emisor y receptor, para llevar acabo la conmutación de paquetes se utilizan 2 tipos de conexión.

- Orientada a conexión.
- No orientada a conexión.

1.2.1.1.- Orientada a conexión.

Este tipo de conexión trabaja como el sistema telefónico, la conexión es como un tubo y los mensajes llegan en el orden en que fueron enviados, es decir una conexión debe establecerse antes de que el servidor intercambie datos, la confiabilidad es lograda asignando un numero de secuencia a cada segmento transmitido y se utiliza una confirmación para verificar que los datos fueron recibidos por el otro servidor.

Para cada segmento enviado el servido que recibe debe regresar una confirmación (ACK) dentro de un periodo especifico de bytes recibidos, si un ACK no es recibido los datos son retransmitidos.

1.2.1.2.- No orientada a conexión.

Este tipo de servicio trabaja como el sistema de correo, cada mensaje trae la dirección completa del destino por lo que se lleva a cabo enrutamiento del paquete para hacer hacia donde se debe dirigir, la conmutación de paquetes se puede realizar de 2 formas: Circuitos virtuales y Datagramas.

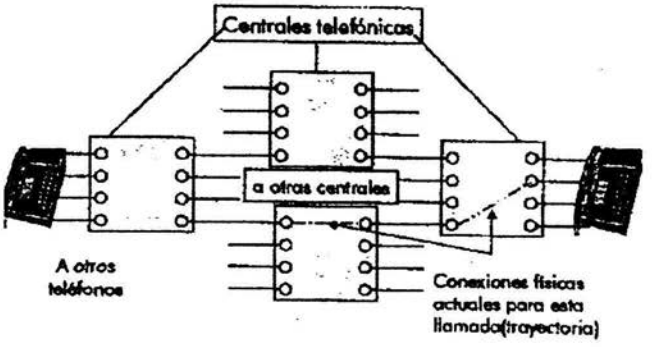
1.2.2.- Conmutación de circuitos.

En la conmutación de circuitos una trayectoria o circuito físico de la fig. 6 entre el equipo emisor y el receptor debe ser establecido antes de que los datos puedan ser transmitidas, después de que la conexión es establecida el uso del circuito es exclusivo y continuo durante el intercambio de información, cuando este intercambio es completado el circuito es desconectado y los enlaces físicos entre los nodos están listos para ser usados en otras conexiones.

El principal uso de esta técnica es en la red telefónica publica y sus características son:

- Tiempo de establecimiento elevado (segundos).
- Utilización de recursos ineficiente (transmisión de datos por ráfaga).
- Retardos pequeños y constantes.
- Comunicación en tiempo real y sin congestión.

Fig. 6
Conmutación de circuitos.



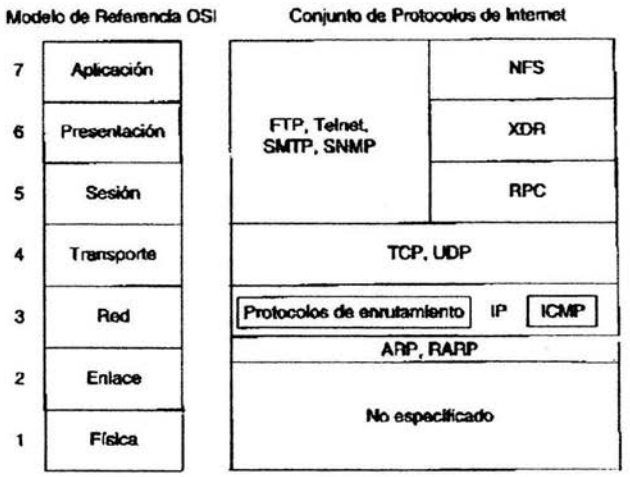
1.3.- Modelo referencia OSI.

La Organización internacional para la normalización (ISO) desarrollo el modelo de referencia OSI a principios de los 80's, el cual se ha convertido en el estándar para desarrollar protocolos que permiten que las computadoras se comuniquen, el modelo de referencia OSI (Interconexión de sistemas abiertos) fragmenta el problema de la comunicación entre computadoras en 7 capas.

Cada capa se ocupa solo de hablar con su correspondiente capa situada en la siguiente computadora de la fig. 7, además cada capa del modelo de referencia OSI proporciona servicios a la capa que esta por encima de ella (capa 5 a la capa 6, capa 6 a la capa 7) y solicita determinados servicios de la capa

directamente por debajo (5 a 4, 4 a 3). Esta propuesta por capas permite que cada una de ellas maneje una pequeña pieza de información, realice cualquier cambio que sea necesario a los datos y agregue las funciones necesarias para esa capa antes de hacer pasar los datos.

Fig. 7
Modelo de referencia OSI.



Los datos dejan de parecerse a datos humanos para parecerse mas a datos de computadora conforme van recorriendo el modelo de referencia OSI hasta convertirse en 1's y 0's (impulsos eléctricos),

1.3.1.- Características de las Capas.

Entender las capas del modelo OSI (aplicación, presentación, sesión, transporte, red, enlace y física) como ayudan que funcione el enrutamiento IP (Protocolo de Internet) y como es transportado a través de las capas 1 y 2, además de la comunicación entre datos comprende de 2 aspectos principales:

- El transporte. Involucra todas las funciones relacionadas con la transferencia de datos entre 2 usuarios finales.
- La manipulación de datos. Los datos deben ser liberados en una forma comprensible, en algunos casos los datos deben ser convertidos.

1.3.2.- Capa de aplicación.

Contiene una variedad de protocolos que hacen posible ofrecer una serie de aplicaciones al usuario final como: correo electrónico (e-mail), transferencia de archivos (ftp), terminal virtual (telnet), directorio telefónico, navegador de Internet (WWW) de la fig. 8.

Fig. 8
Capa de aplicación.

1.3.3.- Capa de presentación.

Garantiza que la información enviada por la capa de aplicación de un sistema es legible por la capa de aplicación del otro sistema, si fuera necesario la capa de presentación traduce entre múltiples formatos de datos utilizando un formato de representación de datos comunes, como en la fig. 9.

Fig. 9
Capa de presentación.

La capa de presentación se ocupa no solo del formato y representación de los datos de usuario, sino también de las estructuras de datos utilizadas por los programas.

1.3.4.- Capa de sesión.

Establece, administra y termina sesiones entre aplicaciones, las sesiones consisten en él dialogo entre 2 o más entidades de presentación; la capa de sesión sincroniza los diálogos entre las entidades de la capa de presentación y administra su intercambio de datos como en la fig. 10.

Fig. 10
Capa de sesión.

Además de la regulación básica de las conversiones (sesiones), la capa de sesión ofrece provisiones para la expedición de datos, clase de servicio y registro de los problemas de la capa de sesión, de presentación y la capa de aplicación.

1.3.5.- Capa de transporte.

Es responsable de asegurar un transporte de datos fiable en una interworking (redes interconectadas), esto se lleva a cabo mediante el control del flujo, la verificación de errores (suma de comprobación), la confirmación de extremo a extremo, la retransmisión y la secuencia de datos de la fig. 11. Algunas capas de transporte como TCP (Protocolo de control de transmisión) tienen mecanismos para manejar la congestión.

Fig. 11
Capa de transporte.

1.3.6.- Capa de red.

Proporciona la dirección lógica que permite que 2 sistemas distintos que se encuentra en redes lógicas diferentes determinen una posible ruta para comunicarse, en esta capa residen los protocolos de enrutamiento, entre las funciones de la capa de red se incluye las siguientes:

- Formateo de paquetes, direccionamiento de redes y host, resolución de direcciones y enrutamiento.
- Creación y mantenimiento de tablas de enrutamiento.

Fig. 12
Capa de red.

También participa en el control de congestión de la red, además los routers enrutan los paquetes IP sobre la base de su dirección de la capa de red.

1.3.7.- Capa de datos.

Proporciona un transporte fiable a través de un enlace físico, la capa de enlace tiene su propio esquema de direcciones como en la fig. 13. Este esquema se ocupa de la conectividad física y puede transportar tramas sobre la base de la dirección de la capa de enlace, los switches de ethernet conmutan él trafico de red sobre la base de la dirección de la capa de enlace (capa 2).

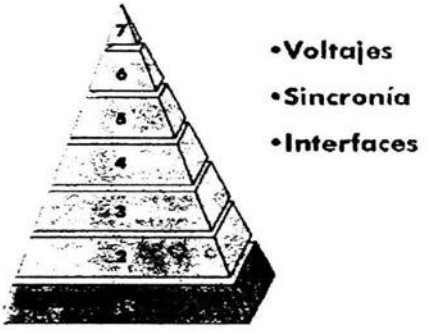
Fig. 13
Capa de enlace.

Además resuelve los problemas de daño, perdida o duplicidad de datos y participa en la regulación del flujo (evita que un transmisor muy rápido sature con datos a un receptor muy lento).

1.3.8.- Capa de física.

Se ocupa de crear 1's y 0's en el medio físico con cambios de impulsos/voltajes eléctricos, define tiempos de duración de los pulsos, él numero de pines que tiene el conector de la interfaz y sus funciones, la forma de establecer la conexión inicial y de interrumpirla de la fig. 14.

Fig. 14
Capa física.



Entre las especificaciones de comunicación de la capa física se encuentran las siguientes:

- EIA/TIA-232: Especificación de la asociación de industrias electrónicas/asociación de la industria de las telecomunicaciones, utilizada para comunicar dispositivos de computadoras.
- V.35: Mecanismo del sector de la normalización de las telecomunicaciones de la ITU-T (Unión Internacional de Telecomunicaciones) que define la velocidad de señalización desde 19,2 Kbps a 1,544 Mbps.

1.4.- Protocolo de Internet (IPv4).

Los Protocolos de Internet pueden usarse para establecer una comunicación a través de cualquier conjunto de interredes, están adaptados para las comunicaciones en LAN's (redes de área local) y en WAN (redes de área amplia), el conjunto de Protocolos de Internet incluye no solo especificaciones de las capas mas bajas como TCP e IP, sino también especificaciones para aplicaciones como el correo, la emulación de terminales y la transferencia de archivos.

El IP en sí mismo es un protocolo sin conexión que reside en la capa 3 (capa de red), lo que significa que no hay ningún mecanismo de fiabilidad, control de flujo, secuenciación o reconocimiento, otros protocolos como TCP se pueden alojar en la parte superior IP (capa 4) y pueden agregar control de flujo, secuenciación y otras características.

Dada la posición de IP en el modelo OSI no tiene que tratar con problemas de enlace de datos comunes como Ethernet, ATM (modo de transferencia de asíncrona), Frame relay y Token ring o cuestiones físicas como SONET (red óptica sincrona), el cobre y la fibra óptica, esto hace que IP sea virtualmente universal.

Se puede ejecutar IP en una casa u oficina a través de cualquier medio necesario (inalámbrico, banda base o ancha), IP esta considerado un protocolo de ráfagas (bursty) lo que significa que las aplicaciones que residen por encima de IP experimentan largos periodos de silencio, seguidos de la necesidad de una gran porción de ancho de banda.

Una de las mayores ventajas de IP es la posibilidad de escribir una aplicación una vez y tenerla para todo un conjunto de tipos de medios en cualquier sitio, independientemente de si esto ocurre a través de una conexión de DSL (línea de abonado digital) en casa o una línea T1 en el trabajo. Se puede dirigir un paquete IP de 3 maneras generales: a través de mecanismos de unidifusion, multidifusion y difusión, estos mecanismos proporcionan los medios para que cada paquete IP sea etiquetado con una dirección de destino, siéndolo cada una de ellas de una manera única:

- La unidifusion es muy simple porque solo identifica una dirección especifica y únicamente ese nodo envía el paquete a las capas superiores del modelo OSI.
- Los paquetes de difusión son enviados a todos los usuarios en una subred local, las difusiones pueden atravesar puentes y switches, pero no pasadas a través de routers.
- Los paquetes de multidifusion utilizan una gama especial de direcciones que permiten a un grupo de usuarios que se encuentren en subredes diferentes recibir el mismo flujo.

Independientemente del tipo de paquete IP que se utilice siempre se necesita direccionar la capa de enlace de datos.

1.4.1.- Direcciones de la capa de enlace.

Los 2 tipos de direcciones son la dirección de la capa de enlace y la dirección de la capa de red, la primera también conocida como MAC (control de acceso al medio) y las direcciones de la capa física son únicas para cada dispositivo, cuando él tráfico es enrutado sobre la base de la dirección de la capa MAC se dice que ha sido conmutado o puenteado.

1.4.2.- Formato de paquete IPv4.

La capa de red del IPv4 ofrece la fragmentación y reensamble de datagramas así como el informe de errores, junto con TCP representa el corazón del conjunto de IPv4.

Fig. 15
Formato del paquete IPv4.

Los campos del paquete IPv4 de la fig. 15 son:

- Versión: Indica la versión de IP usada actualmente.
- Longitud del encabezado IP (IHL): Indica la longitud del encabezado del datagrama en palabras de 32 bits.
- Tipo de servicio: Especifica la manera en que un protocolo de capa superior determinado requeriría que se manejara el datagrama actual, a través de este campo se pueden asignar varios niveles de importancia a los datagramas.
- Longitud total: Especificas en bytes la longitud de todo el paquete IP, incluyendo datos y encabezado.
- Identificación: Contiene un entero que identifica al datagrama actual, este campo se usa para ayudar a unir los fragmentos de datagramas.
- Banderas: Un campo de 3 bits los cuales los 2 bits menos significativos controlan la fragmentación, el primer bit especifica si puede fragmentarse el paquete y el segundo indica si el paquete es él ultimo de una serie de paquetes fragmentados.

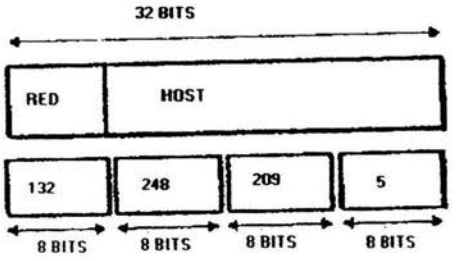
- Tiempo de vida: Lleva un contador que se disminuye en forma gradual hasta cero, punto en el cual el datagrama se descarta, esto evita que los paquetes se quedan indefinidamente en un ciclo.
- Protocolo: Indica cual de los protocolos de capa superior recibe los paquetes entrantes después de que termina el procesamiento del IP.
- Suma de verificación del encabezado: Ayuda a asegurar la integridad del encabezado IP.
- Dirección de origen: Especifica el nodo que envía.
- Dirección de destino: Especifica el modo que recibe.
- Opciones: Permite que el IP soporte varias opciones.
- Datos: Contiene información de las capas superiores.

1.4.3.- Dirección IPv4.

Es un número único de 32 bits de la fig. 16 para una PC con TCP/IP concreta en Internet escrita normalmente en decimal (por ejemplo: 128.122.40.227), sirve para identificar a un equipo o dispositivo que esta trabajando con TCP/IP, la cual debe ser única y no puede estar repetida. Por lo cual el significado de esta numeración es la siguiente: los primeros (128) significan el dominio, los segundos (122) el tipo de red, los terceros (40) el grupo de trabajo y los últimos (227) los nodos.

Todos los nodos de una red TCP/IP requieren una dirección numérica de 4 bytes (32 bits) que identifique una red y un host o nodo local de la red, esta dirección se escribe mediante 4 números separados por puntos, por ejemplo: 192.100.10.5. En la mayoría de los casos, el administrador de la red establece estas direcciones cuando instala nuevas estaciones sin embargo, existe software que permite a las estaciones consultar en un servidor las direcciones asignadas dinámicamente.

fig. 16
Dirección IPv4.



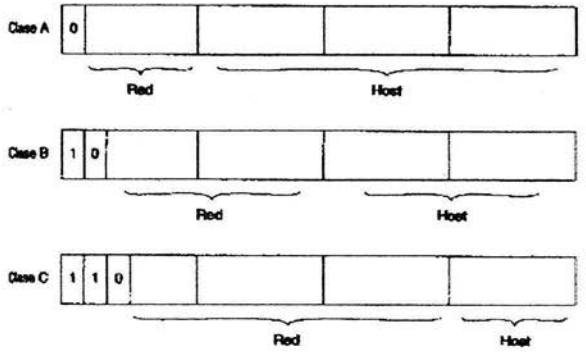
1.4.3.1. - Direccionamiento.

El proceso de enrutamiento de datagrama IPv4 a través de una interred depende del esquema de direccionamiento, una dirección IPv4 tiene una longitud de 32 bits dividida en 2 o 3 partes. La primera parte designa la dirección de red, la segunda parte (si la hay) indica la dirección de subred y la ultima parte designa la dirección del host, las direcciones de subred solo se presentan si el administrador de la red decidió que esta debía dividirse en subredes, la longitud de los campos de red, subred y host es variable.

El Direccionamiento IPv4 soporta 5 diferentes tipos de clases de red de la fig. 17 y los bits mas hacia la izquierda indican la clase de red, las cuales son las Clases asignadas de direcciones de Internet.

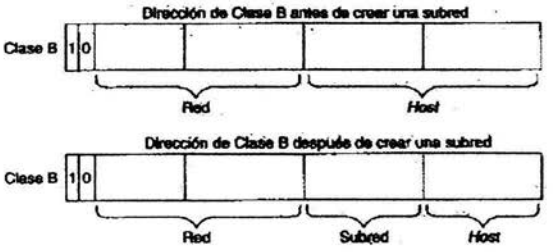
- Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (cada par de direcciones de red y de host, 2 tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red tener hasta 16,777,214 host.
- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16382 redes de hasta 65534 host cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2,097,150 redes de hasta 254 host cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de host en un área limitada. (Multicasting).
- Las direcciones de clase E se reservan para usos en el futuro

Fig. 17
Formatos de dirección de las clases A, B y C.



Las redes IPv4 también pueden dividirse en unidades más pequeñas denominadas subredes de la fig. 18, las cuales proporcionan flexibilidad adicional a los administradores de redes.

Fig. 18
Dirección de una subred.



1.5.- Protocolos de enrutamiento.

El IPv4 es un protocolo enrutado, lo cual es un paquete que transporta datos y su diferencia de un protocolo de enrutamiento en que este actualiza los routers para permitirles saber que ruta deberá recorrer un paquete, las redes IPv4 actualmente utilizan 2 tipos de protocolos de enrutamiento como:

- Enrutamiento por vector de distancia.
- Enrutamiento por estado de enlace.

Dentro de estos 2 protocolos de enrutamiento se hallan protocolos exteriores e interiores, el enrutamiento por vector de distancia se preocupa por él numero de saltos (routers) mientras que el enrutamiento por estado de enlace se preocupa del estado de las interfaces que el router soporta. Los protocolos de enrutamiento interiores se utilizan para actualizar los routers bajo el control de una autoridad de administrativa (sistema autónomo), los protocolos de enrutamiento exteriores se utilizan para permitir que redes que se encuentren en diferentes sistemas autónomos pasen actualizaciones de enrutamiento.

1.5.1.- Enrutamiento por vector de distancia.

Es un algoritmo que los routers utilizan para poder elegir la mejor ruta, este algoritmo utiliza el menor números de salto (cada router es un salto) para determinar la mejor ruta hasta el destino, las difusiones se envían periódicamente para actualizar routers adyacentes. Cuando el router empieza a difundir actualizaciones incluye todas las redes alcanzables que están directamente conectadas, las rutas que son recibidas por un router se guardan en una tabla de enrutamiento que es utilizada para transmitir paquetes.

Este método consume mucho ancho de banda porque la totalidad de la actualización del enrutamiento es enviada periódicamente (cada 30 seg.).

1.5.2.- Enrutamiento por estado de enlace.

Se distingue del enrutamiento por vector de distancia que el primero transmite actualizaciones del enrutamiento solo cuando cambia el estado de una interfaz, esto significa que únicamente se envía trafico y se consume ancho de banda cuando cambia una interfaz.

1.6.- Mecanismo de transporte IP.

El TCP y UDP (Protocolo de datagrama de usuario) implementan la capa de transporte de Internet, TCP proporciona el transporte de datos orientados a la conexión, mientras que la operación de UDP es sin conexión. Por ejemplo si la fiabilidad es más importante que el retraso se puede utilizar TCP/IP para garantizar la entrega de paquetes, UDP/IP no utiliza la retransmisión de paquetes, esto puede disminuir la fiabilidad.

1.6.1.- Protocolo de control de transmisión (TCP).

El Protocolo de control de transmisión (TCP) proporciona a los protocolos de capas superiores un servicio dúplex total, con confirmación de envío y control de flujo, los datos son transportados en un flujo de bytes continuo no estructurado en el que los bytes se identifican mediante no. de secuencia.

Para maximizar el rendimiento o tasa de trasferencia TCP permite que cada estación envíe múltiples paquetes antes de que llegue un acuse de recibo, cuando el remitente ha recibido un acuse de recibo para un paquete saliente el remitente desliza la ventana de paquetes por la corriente de bytes y envía otro paquete.

TCP soporta diversas conversaciones de capa superior a la vez, además de proveer comunicación entre 2 host mediante la capa de transporte y dentro de esta capa de encuentran 2 protocolos que son:

- El Protocolo de control de transmisión (TCP):
- El Protocolo de datagrama de usuario (UDP).

Dentro de la porción de señalización de VoIP, TCP se utiliza para asegurar la fiabilidad de la configuración de una llamada, debido a la manera de operar de TCP, actualmente no es posible utilizar TCP como el mecanismo para transportar la voz en una llamada VoIP. Con la VoIP la perdida es menos importante que la latencia (retraso).

El TCP tiene como características las siguientes:

- Es orientado a conexión, lo que significa que primero establece una sesión entre los 2 host y después inicia el intercambio de información.
- TCP asegura una confiabilidad en la correcta entrega de los mensajes mediante no. de secuencia y reconocimientos de mensajes recibidos, los no. de secuencia permiten que un mensaje muy grande pueda ser segmentado y reensamblado en el origen y el destino, el reconocimiento verifica que la información haya sido recibida.
- TCP usa comunicaciones en flujos de byte, lo que significa que la información es tratada como una secuencia de bytes sin limites en los mensajes.

Fig. 19
Formato del paquete TCP.

Los campos del paquete TCP de la fig. 19 son los siguientes:

- Puertos de origen y destino: Identifican los puntos en los cuales los procesos de las capas superiores de origen y destino reciben servicios TCP.
- Numero de secuencia: Especifica el no. asignado al primer byte de datos en el mensaje actual, también puede usarse para identificar un no. de secuencia inicial que se utilizara en al transmisión futura.
- Numero de confirmación de recepción: Contiene el no. de secuencia del siguiente byte de datos que se espera recibir por parte de la otra entidad remota emisora de paquetes.
- Control de datos: Indica el no. de palabras de 32 bits del encabezado TCP.
- Reservado: Para uso futuro.
- Banderas: Llevan diversa información de control.
- Ventana de transmisión: Especifica el tamaño de la ventana de recepción del emisor.
- Suma de verificación: Indica si se daño el encabezado en él transito.
- Apuntador urgente: Apunta al primer byte de datos urgentes en el paquete.
- Opciones: Especifica las diversas opciones de TCP.
- Datos: Contiene información de la capa superior.

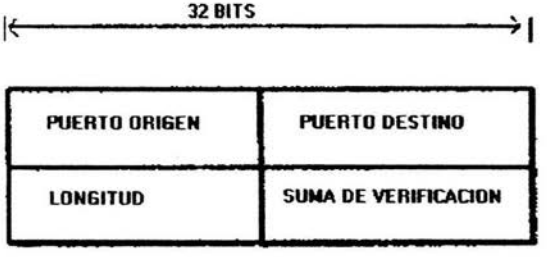
1.6.2.- Protocolo de datagrama de usuario (UDP).

El Protocolo de datagrama de usuario (UDP) es un protocolo más sencillo que TCP y es útil en situaciones en las que no son necesarios los mecanismos de confiabilidad de TCP, el encabezado UDP solo tiene 4 campos como en la fig. 20.

- Puerto de origen.
- Puerto de destino.
- Longitud.
- Suma de verificación UDP.

Los campos de puertos de origen y destino sirven para las mismas funciones que en el encabezado TCP, el campo de longitud especifica la longitud del encabezado UDP y de los datos y el campo de suma de verificación permite la revisión de la integridad del paquete, la suma de verificación UDP es opcional.

Fig. 20
Formato del paquete UDP.



Sus características del UDP son:

- Es orientado a no conexión, lo que significa que no establece una sesión entre los 2 host antes de intercambiar la información, los mensajes UDP pueden ser difundidos de tal manera que varios host reciben el mismo mensaje.
- UDP no garantiza la entrega de los menajes por lo que los paquetes pueden llegar en desorden duplicados, la confiabilidad de la entrega depende de las aplicaciones en los extremos.

UDP se utiliza en VoIP para transportar él trafico de voz real (canales portadores), TCP no se utiliza porque no se necesitan ni el control de flujo ni la retransmisión de paquetes de audio de voz, como se utiliza UDP para transportar la corriente de audio este continua transmitiendo con independencia de sí esta sufriendo un 5 o un 50 % de perdida de paquete.

Si se utiliza TCP para VoIP la latencia en la que se caería a la espera de los acuses de recibo y retransmisiones haría que la calidad de la voz fuera inaceptable, con VoIP y otras aplicaciones de tiempo real controlar la latencia es más importante que asegurar la entrega fiable de cada paquete, con TCP se utiliza para configurar las llamadas en la mayoría de los protocolos de señalización VoIP.

CAPITULO 2
CARACTERISTICAS Y FUNCIONAMIENTO DE LA VOZ SOBRE EL PROTOCOLO DE INTERNET (VoIPv4).

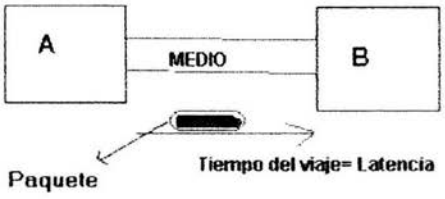
La Voz sobre IP (VoIP) es una tecnología que permite la transmisión de la voz a través de redes IPv4 en forma de paquetes de datos, el Protocolo de Internet (IPv4) es el protocolo utilizado en las redes de datos, como Internet para transmitir la información de un punto a otro. La información se segmenta en paquetes, y cada uno tiene escrita la dirección a la que se envía y de la que procede.

Para la creación de una red apropiada es importante conocer sus características y funcionamiento de la tecnología a usarse, así como los problemas que se va a enfrentar y sus consecuencias en la red de paquetes VoIP.

2.1.- Retraso (latencia).

La latencia es el tiempo que una unidad de trabajo tarda en recorrer el sistema, en una red local (LAN) se refiere al tiempo (ms.) que tardaría un paquete de datos en llegar de un extremo a otro, la latencia en el medio (o retardo de transmisión) es el tiempo mínimo que tardaría en llegar un paquete del extremo A al B como en la fig. 21.

Fig. 21
Latencia en el medio.



Otra definición es el tiempo que tarda la voz en salir del emisor al receptor cuando las personas están hablando vía telefónica, los cuales están relacionados a las redes de telefonía actuales y existen 3 diferentes tipos de retrasos: retraso de propagación, retraso de serialización y retraso de manejo.

2.1.1.- Retraso de propagación.

Es causado por la velocidad de la luz en la fibra óptica o en el cobre (200,000 km./s.) que difiere de la del vacío (300,000 km./s), este retraso junto con los retrasos de manejo puede provocar una degradación notable de la voz.

2.1.2.- Retraso de manejo.

Es también llamado retraso de procesamiento define las diferentes causas de retraso (empaquetado, compresión y conmutación de paquetes) y es causado por los dispositivos que transmiten la trama a través de la red, esto puede ser un problema en las redes telefónicas pero en las redes de computadoras son mayores los problemas.

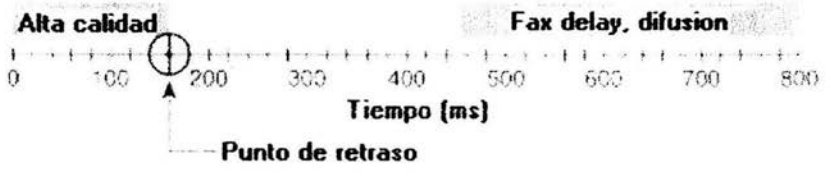
Todo esto afecta la calidad de la voz, los fabricantes pueden decidir cuantas muestras de voz quieren enviar en un paquete, el G.729 utiliza muestras de voz de 10 ms. cada incremento en las muestras por trama aumenta el retraso en 10 ms.,

2.1.3.- Retraso de gestión de colas.

La red basada en paquetes sufre retrasos por el tiempo que se necesita para mover un paquete hasta la cola de salida y el retraso de la gestión de colas, cuando los paquetes se guardan en una cola debido a la congestión en una interfaz de salida el resultado es un retraso de gestión de cola, esto ocurre cuando se envían mas paquetes que los que la interfaz puede manejar en un intervalo de tiempo dado.

Este retraso debe estar debajo de 10 ms. siempre que se pueda utilizar cualquier método de gestión de colas que se optimo para la red, la recomendación G.114 de ITU-T (Unión Internacional de Telecomunicaciones) especifica que para una buena calidad de voz no debe darse un retraso mayor de 150 ms. de una vía, de extremo a extremo como en la fig. 22.

Fig. 22
Retraso de extremo a extremo.



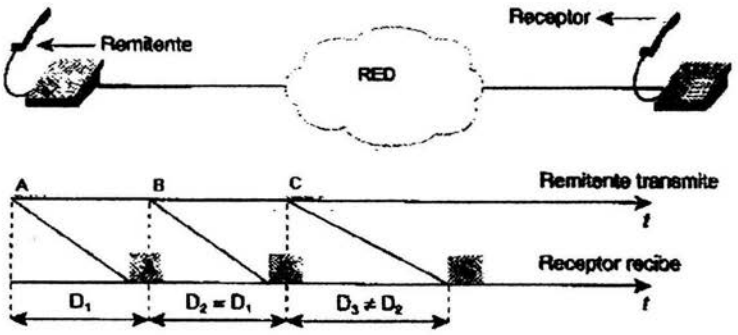
En una red no administrada y congestionada, el retraso en la gestión de colas puede agregar mas de 2 seg. de retraso (o provocar que el paquete se caiga), el retraso en la gestión de colas es solo un componente del retraso de extremo a extremo, este retraso se ve afectado por la fluctuación de fase.

2.2.- Fluctuación de fase (jitter).

Es la variación del tiempo de llegada de un paquete y solo existe en las redes de paquetes, esto pasa cuando el emisor transmite paquetes de voz en un intervalo regular (trama cada 20 ms) y este paquete se retrasa por toda la red de paquetes no llegando con el mismo intervalo al receptor, esto es la diferencia entre cuando se esperaba recibir el paquete y cuando se recibe en realidad.

Se ve que el tiempo que tarda en enviar y recibir los paquetes A y B es el mismo como en la fig. 23, el paquete C tiene un retraso en la red y se recibe después de la hora a la que se esperaba, es por lo que es necesario un bufer de fluctuación de fase que oculta el retraso.

Fig. 23
Variación del tiempo de llegada de un paquete.



2.3.- Modulación de códigos de pulsos (PCM).

El estándar para la representación digital de las señales de voz en las redes de telefonía esta dado por el formato PCM, en la cual la señal se filtra para obtener una versión baja limitada a W= 8 khz. La señal resultante se muestrea a la frecuencia de muestreo de Nysquist de 2W= 8 khz, cada muestra se aplica a un cuantizador con m=8 bits .

El numero de niveles en el cuantizador es de 256, los cuantizadores utilizados en telefonía son no uniformes, la técnica denominada compading se utiliza de tal forma que el tamaño de los intervalos aumente el tamaño de la señal x, la formula de la SNR es:

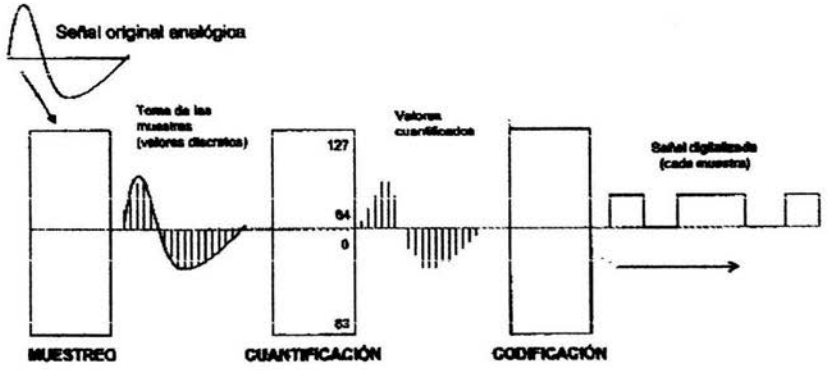
SNR db= 6m – 10 para voz en PCM.

El PCM aplica el concepto de la multiplexación por división de tiempo (TDM), el cual consiste en asignar una ranura o intervalo de tiempo distinto a cada canal y dentro de esto tipo de multiplexación esta la técnica de PCM, el cual es un método de conversión de la información de forma analógica a forma digital y viceversa; multiplexando varias señales del canal telefónico en tiempo compartido (TDM) a través de 3 etapas principales.

La transformación de una señal analógica en digital por modulación de pulsos codificados (PCM) se realiza como en la fig. 24 mediante los siguientes 3 pasos:

A. Muestreo.
B. Cuantizacion.
C. Codificación.

Fig. 24
Proceso de muestro, cuantificación y codificación de una señal analógica para su transmisión por un medio digital (PCM).



A- Muestreo.

Consiste en el proceso en el cual se obtienen pulsos periódicos cuyas amplitudes son las muestras de una onda continua, el periodo o intervalo de repetición de dichos pulsos esta regido por el teorema de Nysquist.

En los sistemas de transmisión de audio, la frecuencia de audio es transportada en forma continua a lo largo de la portadora, sin embargo esto es realmente necesario para transmitir la señal completa o si la transmisión del valor de la señal en intervalos regulares pudiera ser suficiente.

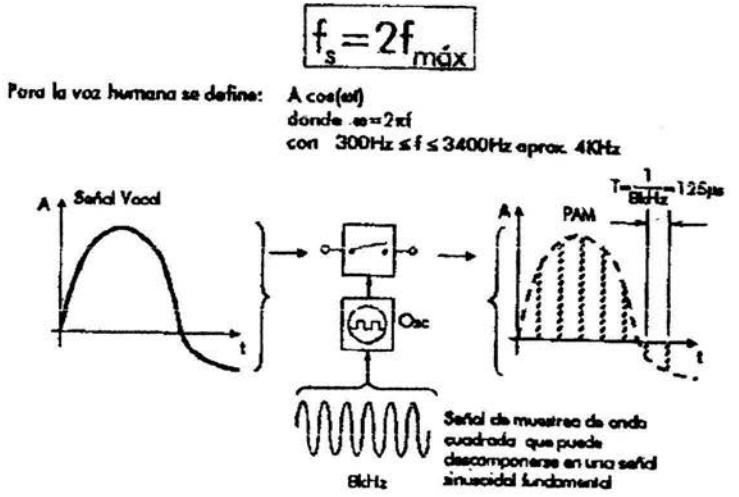
Aunque la comunicación analógica es la ideal para la comunicación humana, la transmisión analógica no es ni robusta ni eficaz para recuperarse del ruido de línea, es mas fácil separar las muestras digitales que son 0 y 1 bits del ruido de linea.

Por lo tanto cuando se genera las señales analógicas como muestras digitales se mantiene un sonido limpio, esto represento para la red telefónica una mejora y por esto se migro a la modulación de códigos de pulsos (PCM). La cual convierte el sonido analógico en forma digital muestreando el sonido analógico 8,000 veces por segundo y convirtiendo cada muestra en un código numérico.

Los científicos Nysquist y Shanon examinaron el problema y concluyeron que muestras tomadas en intervalos regulares pueden ser usados para transmitir una señal de audio; el teorema de Nyquist trata sobre que si se muestrea una señal analógica a una velocidad 2 veces superior a la frecuencia de interés mas alta, lo cual se puede reconstruir de nuevo de manera exacta esa señal en su forma analógica, esto da que el contenido de voz esta por debajo de los 4 Khz. y se requiere una velocidad de muestreo de 8,000 veces por segundo (125 ms entre muestras).

Es decir que una señal continua que no contenga señales mayores a ω hz. esta completamente determinada por muestras de la señal tomadas a intervalos $\frac{1}{2}\ \omega$ seg., este teorema expresado en terminos de frecuencia establece que la frecuencia de muestreo (fs) debe ser mayor o igual al doble de la frecuencia máxima de la señal muestreada como en la fig. 25.

Fig. 25
Frecuencia de muestreo.



Esto es fs: 2 ω, por lo tanto el ancho de banda de un canal telefónico de 300 a 3,400 hz con un margen de seguridad, se considera un ancho de banda B= 4,000 hz. será la frecuencia de muestreo:

fs= 2 * 4,000 hz= 8,000 hz= 8 Khz.

B- Cuantización.

Es el proceso donde se aproximan los valores de las señales PAM (Modulación por amplitud de pulsos) originales a un numero finito de niveles discretos de amplitud definida previamente, el no. de niveles de cuantificación M esta estrechamente relacionado con el no. de bits que son necesarios para codificar una señal, se usan 8 bits para codificar cada muestra y la relación es la siguiente:

$$M= 2^n$$

donde: $M= 2^8 = 256$ niveles.

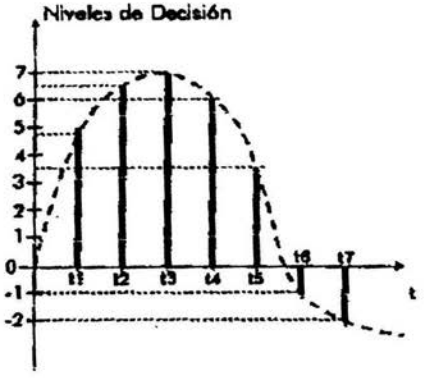
Sin embargo no es recomendable que todos esos niveles de voltaje o escalones tengan el mismo tamaño.

Representa la amplitud de una muestra por la amplitud del nivel discreto más cercano, para poder usar la transmisión digital cada valor de la muestra tendrá que ser representado por un código, dado que él numero de códigos es limitado, los valores de la amplitud serán redondeados al valor más cercano, el cual puede representarse por un código.

El no. de niveles de Cuantización M esta relacionado con el no. de bits *n* que son necesarios para decodificar una señal como en la fig. 26, hay 2 métodos para Cuantización de una señal:

- b.1- Cuantización lineal.
- b.2- Cuantización no lineal.

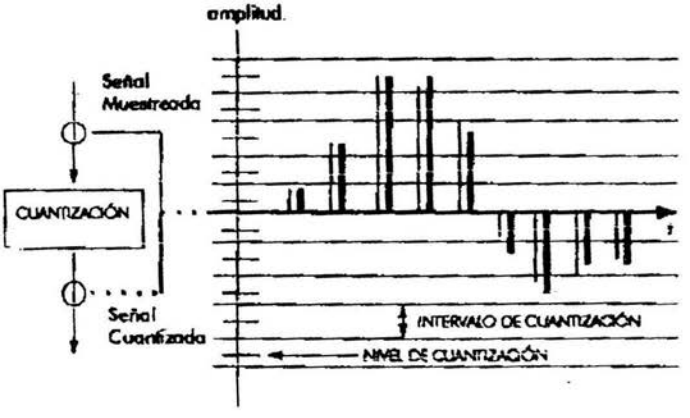
Fig. 26
Cuantización.



b.1- Cuantización lineal.

Este método el rango total de valores de voltaje que puede ser manejados es subdividido en un no. de subrangos de voltajes iguales, cada subrango corresponde a una combinación de código, la codificación de cualquier voltaje situado entre los limites bajo y alto de un subrango es codificado con el mismo código como en la fig. 27.

Fig. 27
Cuantizacion lineal.

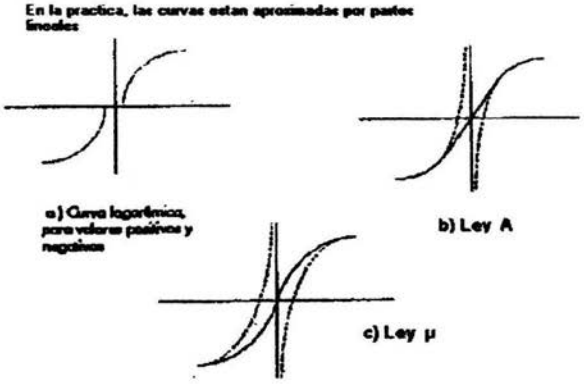


En el momento de decoficicar un código es representado por un voltaje correspondiente a la mitad del subrango (nivel de Cuantización o quantum), el resultado es que cierta cantidad de ruido es adicionada a la señal original esto es llamado ruido de Cuantización.

b.2- Cuantización no lineal.

Como la Cuantización lineal de señales resulta con una mala relación "señal a ruido" (SNR), la otra clase de Cuantización ha sido encontrada para obtener una SNR de un valor cte. para cualquier nivel de la señal, los niveles de Cuantización tienen que ser seleccionados de un modo logarítmico, esto significa que se usara una Cuantización no lineal como en la fig. 28.

Fig. 28
Cuantizacion no lineal.

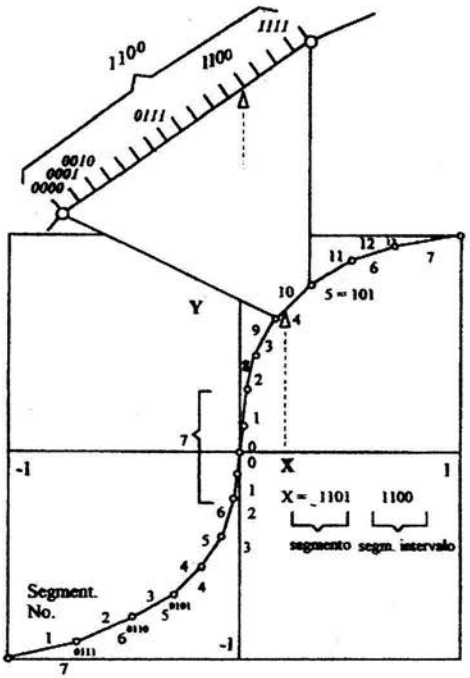


Los niveles de ruido altos pueden ser permitidos para señales muestreadas con un nivel alto pero no para señales con nivel pequeño, las curvas logarítmicas tienen la desventaja de que no pasan a través del origen, para resolver este problema hay 2 leyes compansion, las cuales consisten en la contracción y expansión.

En forma practica esto se hace aplicando la compresión de la señal en la transmisión y la expansión en la recepción aplicando las siguientes leyes de compansion:

1- Curva de la ley A: Estandarizado por ITU-T (Unión Internacional de Telecomunicaciones) usado en Europa (curva b), también conocida como de 13 segmentos, se utiliza la línea tangente a la curva desde el origen hasta los puntos de tangencial de la fig. 29.
2- Curva de la ley μ: Sistema estandarizado por la North American Bell y ITU-T, obtiene una curva a través del origen al desplazar toda la curva al origen (curva c).

Fig. 29
Ley A.



C- Codificación.

Es asignar un código binario (palabra de 8 bits) a cada una de las muestras PAM cuantizadas dependiendo de a cual de los 256 niveles se halla aproximado la muestra como en la fig. 29.

Después de ser cuantizada la muestra de entrada esta limitada a 256 valores discretos, la mitad de estas son muestras codificadas positivas y la otra mitad son muestras codificadas negativas, hay 256 niveles así que son necesarios 8 bits para codificar todos los niveles. Cada combinación de 8 bits corresponde a un nivel, para seleccionar cual combinación correspondería con cual nivel existen diferentes posibilidades.

2.4.- Compresión de voz.

Se utilizan 2 variaciones básicas de PCM de 64 Kps.: la ley μ y la ley a, los métodos se parecen en que ambos utilizan compresión logarítmica para alcanzar de 12 a 13 bits de calidad PCM lineal en 8 bits, pero se diferencian en detalles de compresión menores (la ley μ tiene una ligera ventaja en la capa baja, rendimiento en relación señal a ruido).

Otro método de compresión utilizado es la modulación por impulsos codificados diferencial y adaptable (ADPCM), que se usa en la ITU-T (Unión Internacional de Telecomunicaciones) G.726 que

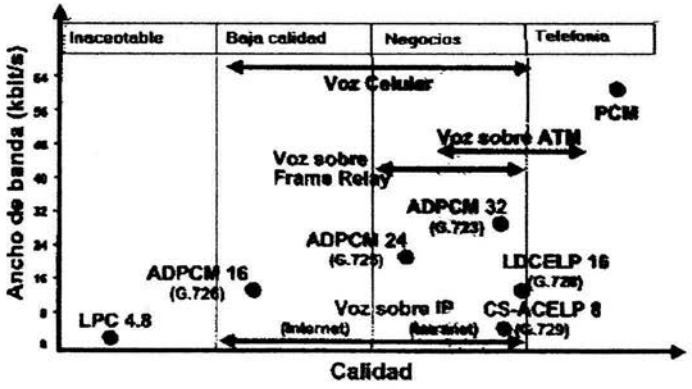
codifica utilizando muestras de 4 bits, lo que dan una velocidad de transmisión de 32 Kbps y codifican las diferencias de la amplitud, así como la velocidad de cambio de esa amplitud empleando algunas predicción lineal rudimentaria.

2.4.1.- Estándares.

La ITU-T normaliza los esquemas de codificación CELP (Predicción lineal de código estimulado), MP-MLQ (Cuantificación de probabilidad máxima de multiimpulso), PCM y ADPCM en sus recomendaciones de la serie G de la fig. 30, entre los estándares de codificación mas conocidas para la telefonía y voz por paquetes que incluyen:

- G.711. Describe la técnica de codificación de voz PCM de 64 Kbps, la voz codificada con G.711 esta en un formato correcto para la entrega de voz digital en la red telefónica publica o a través de intercambio privado de ramas (PBX).
- G.726. Describe la codificación de ADPCM a 40, 32, 24 y 16 Kbps, también puede intercambiar voz ADPCM entre voz por paquetes y telefonía publica o redes PBX.
- G.728. Describe una variación de bajo retraso de 16 Kbps de una compresión de voz CELP.
- G.729. Describe la compresión CELP que permite que la voz sea codificada en corrientes de 8 Kbps.
- G.723. Describe una técnica de compresión que se puede utilizar para comprimir voz u otros componentes de señales de audio de servicios multimedias a una baja velocidad de bit, como parte de los estándares H.324.

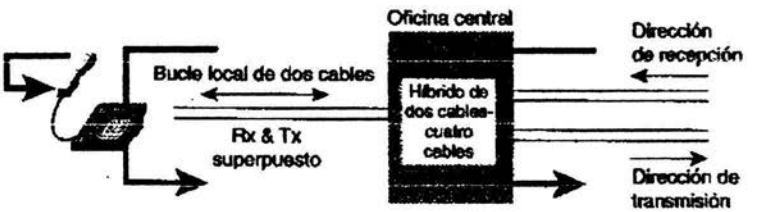
Fig. 30
Estándares para la compresión de voz.



2.5.- Eco.

Oír la propia voz después de un retraso de 25 ms. puede provocar interrupciones y romper la cadencia de la conversación, en una red tradicional el eco esta provocado por un desajuste en la impedancia de la conversación del switch de red de 4 cables al bucle local de 2 cables como en la fig. 31. En la red publica conmutada (PSTN) el eco esta regulado con canceladores de eco y un control sobre los desajustes de la impedancia en los puntos de reflexión común.

Fig. 31
Eco provocado por el desajuste de la impedancia.



El eco tiene 2 inconvenientes: puede ser alto y largo, cuando más alto y largo es el eco mas incomodo resulta, en las redes telefónicas donde se utiliza principalmente la voz analógica emplean supresores de eco que eliminan el eco tapando la impedancia en un circuito; en las actuales redes basadas en paquetes se puede construir canceladores de eco en codecs (Compresión/Descompresión) de velocidad de transmisión baja y hacerlos funcionar en cada DSP (Procesador de señal digital).

Los canceladores de eco están limitados por la cantidad total de tiempo que esperan a que llegue la palabra reflejada (echo tail), es importante configurar la cantidad apropiada de cancelación de eco cuando se instala inicialmente el equipamiento de VoIP, si no se configura suficiente cancelación de eco los que llaman oirán un eco durante la llamada telefónica, si se configura demasiada cancelación de eco el cancelador de eco tardar más tiempo en converger y eliminarlo.

2.6.- Pérdida de paquetes.

En las redes de datos la pérdida de paquetes es común y esperada, además de cuando se genera un tráfico muy intenso es importante controlar la cantidad de pérdida de paquetes que hay en esa red, con protocolos como la arquitectura de redes de sistemas (SNA) que no tolera la pérdida de paquetes es necesario construir bien una red que pueda priorizar los datos sensibles al tiempo por delante de los datos que pueden manejar el retraso y la pérdida de paquetes.

Cuando se genera voz en redes de datos es importante construir una red que transporte con éxito la voz de manera fiable y oportuna, resulta de gran ayuda poder utilizar un mecanismo para hacer que la voz sea resistente a la pérdida periódica de paquetes, como la calidad de servicio (QoS).

2.7.- Detección de la activación de voz.

En conversaciones de voz normales alguien habla y alguien escucha, en las redes actuales contienen canales bidereccionales de 64,000 bps. con independencia de si alguien esta hablando o no, esto significa que una conversación normal se pierde al menos el 50 % del total del ancho de banda, en realidad la cantidad de ancho de banda que se pierde puede ser mayor si se toma un muestreo estadístico de las interrupciones y pausas de los patrones normales de voz de una persona.

Al utilizar VoIP se puede utilizar en ancho de banda perdido para otros propósitos cuando esta habilitada la detección de la actividad de voz (VAD).

2.8.- Conversión digital a analógica.

Cada vez que una conversión pasa de lo digital a lo analógico y viceversa la voz o forma de onda es menos original, aunque las redes actuales pueden manejar por lo menos 7 conversiones D/A antes de que la calidad de voz se vea afectada, la compresión es menos robusta debido a estas conversiones.

Es importante tomar que la conversión D/A debe estar estrictamente administrada en un entorno de voz comprimido, a pesar de que las conversiones D/A afectan a todas las redes de voz, las redes VoIP que utilizan un codec PCM (G.711) son tan resistentes a los problemas causados por las conversiones D/A como las redes telefónicas actuales.

2.9.- Protocolo de transporte.

Por el protocolo de Internet (IPv4) se desplazan 2 tipos de tráfico: el protocolo de datagrama de usuario (UDP) y el protocolo para el control de la transmisión (TCP), se utiliza TCP cuando se necesita una conexión fiable y UDP cuando se necesita simplicidad y la fiabilidad no es la principal preocupación.

Debido a la naturaleza sensible al tiempo del tráfico de voz UDP/IP fue la elección lógica para transportar la voz, sin embargo se necesita mas información en una base paquete a paquete de lo que ofrece UDP, por lo tanto para él tráfico en tiempo real o sensible al retraso el IETF adopto el RTP (Protocolo de transporte para tiempo real). La VoIP circula en la parte superior de RTP que circula a su vez en la parte superior del UDP, por tanto VoIP es transportado con una cabecera de paquetes RTP/UDP/IP.

2.9.1.- Protocolo de transporte para tiempo real (RTP).

Proporciona el transporte extremo a extremo entre aplicaciones que requieran transmisión en tiempo real como servicios de audio o vídeo a través de redes de paquetes unidestino o multidestino; RTP proporciona los siguientes servicios:

- Identificación del tipo de información transportada (carga útil).
- Numeración secuencial.
- Inclusión de marcas de tiempo.
- Monitorizacion de la entrega.

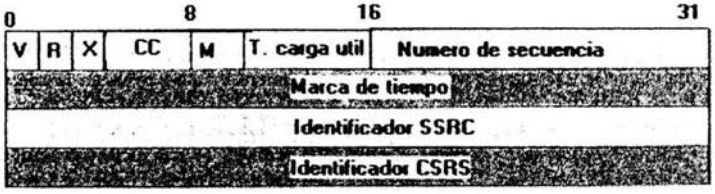
El RTP es el protocolo estándar para transmitir tráfico sensible al retraso por las redes basadas en paquetes, RTP recorre la parte superior del UDP e IPv4, RTP da a las conexiones receptoras información que no esta en las corrientes UDP/IP sin conexión. Dos bits de información importantes son la secuencia y la marca de temporizacion de la fig. 32, RTP utiliza la información de secuencia para determinar si los paquetes están llegando en orden y utiliza la información de marca de temporizacion para determinar el tiempo de llegada entre paquetes (fluctuación de fase).

2.9.1.1.- Formato del paquete RTP.

Las 3 primeras filas (12 bytes) están presentes en todos los paquetes, la cuarta fila (CSRC) se utiliza solo si un mezclador ha alterado la información del campo de carga útil como en la fig. 32, los campos que constituyen son los siguientes:

- Versión (V): este campo de 2 bits identifica la versión del RTP (actual 2).
- Relleno (R): este campo de 1 bit indica que el paquete contiene uno o más bytes de relleno que no son parte de la carga útil, este ultimo byte de este campo contiene el no. de bytes de relleno que tienen que ser ignorados, incluyendo a el mismo.
- Extensión (X): cuando se habilita este bit, se esta indicando que la cabecera debe estar seguida de una extensión de la cabecera.
- Cuenta CSRC (CC): este contador de 4 bits especifica que la cabecera debe estar seguida de una extensión de la cabecera.
- Marcador (M): este campo de 1 bit se define en el perfil y se usa para marcar eventos significativos, como los limites de una trama en una secuencia de paquetes.
- Tipo de carga útil (TC): este campo de 7 bits identifica el formato de la carga útil del paquete RTP y determina como las aplicaciones deben interpretarla.
- Numero de secuencia: este campo de 16 bits se incrementa en una unidad cada vez que se envía un paquete RTP, este no. se puede utilizar en el decodificador para detectar perdidas de paquetes y para recuperar secuencias de paquetes, el valor inicial se elige de forma aleatoria.
- SSRC: este no. aleatorio se utiliza para identificar las fuentes de sincronización dentro de la misma sesión RTP, indica donde se combinan los datos o bien la fuente de los mismos.
- Lista CSRC: esta lista contiene de 0 a 15 items de 32 bits, cada uno de los cuales especifica la fuente que ha contribuido a la carga útil contenida en el paquete.

Fig. 32
Cabecera de RTP.



Se puede utilizar RTP para servicios interactivos como la telefonía por Internet, RTP consta de una parte de datos y una de control esta ultima llamada Protocolo de control RTP (RTCP). La parte de datos de RTP es un protocolo limitado que proporciona soporte para aplicaciones con propiedades de tiempo real, como medios continuos (audio y vídeo) incluyendo la reconstrucción de la temporizacion, la detección de perdidas y la identificación de contenidos.

El protocolo de control RTP implica la transmisión periódica de paquetes de control a todos los participantes de una sesión, la función del RTCP es proporcionar un mecanismo de realimentacion para informar sobre la calidad en la distribución de los datos, esta que se puede utilizar para controlar a los codificadores que sean adaptables o para diagnosticar fallos en la distribución.

El RTCP define varios tipos de paquetes para transportar los distintos tipos de información de control, los cuales son:

- Informe del emisor (IE): el IE distribuye las estadísticas de emisión y recepción de los emisores activos.
- Informe del receptor (IR): el IR distribuye las estadísticas de recepción de los participantes que no sean emisores activos.
- Descripción de la fuente (DESF): el DESF proporciona información para describir la fuente.
- BYE: este mensaje indica el final de la participación de un emisor.
- APP: este paquete proporciona funciones especificas de la aplicación.

RTCP proporciona soporte para conferencias en tiempo real de grupos de cualquier tamaño dentro de Internet, esto incluye la identificación de la fuente y el soporte para Gateways como puentes de audio y vídeo, así como traductores de multidifusion a unidifusion. También ofrece un reaprovechamiento de la calidad de servicio desde los receptores hasta el grupo de multidifusion, y el soporte para la sincronización de diferentes corrientes de medios.

La utilización de RTP es importante para el tráfico en tiempo real pero existen algunos inconvenientes, las cabeceras IP/RTP/UDP tienen 20, 8 y 12 bytes, esto se agrega a una cabecera de 40 bytes es 2 veces más grande que la carga útil cuando se utiliza G.729 con 2 muestras de voz (20 ms). Se puede comprimir esta gran cabecera a 2 o 4 bytes utilizando la Compresión de cabecera RTP (CRTP).

El protocolo de control RTP (RTCP) se diseño para proveer la funcionalidad mínima de control, en particular RCTP no proporciona explícitamente ningún procedimiento para controlar la pertenencia y/o establecimiento de la sesión, la intención fue que un protocolo aparte se encargara del control de la sesión como el protocolo de inicio de sesión (SIP).

2.9.2.- Protocolo de datos de usuario fiable (RUDP).

El Protocolo de datos de usuario fiable (RUDP) incorpora fiabilidad a UDP, RUDP permite la fiabilidad sin la necesidad de tener un protocolo basado en la conexión como TCP, el método de RUDP es enviar múltiples del mismo paquete y permitir que la estación receptora descarte los paquetes innecesarios o redundantes. Además es un protocolo asociado que sirve para monitorizar la calidad del servicio observado por el receptor, así como para informar al emisor de esto mismo y de otras cuestiones relativas a los participantes.

Esta funcionalidad es especialmente útil en aquellas situaciones en las que el emisor pueda adaptar su algoritmo a las condiciones imperantes de la red, como el ancho de banda disponible, el retardo o la dispersión temporal en la red.

Con este mecanismo es mas probable que uno de los paquetes haga el viaje desde el remitente hasta el receptor, esto se conoce como Corrección de errores hacia delante (FEC) y existen pocas implementaciones de FEC debido a consideraciones del ancho de banda (utiliza una doble o triple cantidad mayor de ancho de banda).

2.10.- Calidad del Servicio (QoS).

En todo el proceso de la comunicación intervienen diversos factores que determinarán la calidad del servicio ofrecido. En este caso existen principalmente 2 elementos que la determina, el algoritmo de compresión utilizado y el retraso en la propagación de la señal.

La comunicación sobre la propia red de datos, obliga a compartir ancho de banda con todo el conjunto de aplicaciones que se ejecutan en la red. Por ello es necesario disminuir en lo posible la saturación de la red y de esta forma asegurar de no producir un colapso de las comunicaciones.

La calidad de servicio (QoS) es un termino que hace referencia a la clase de servicio (CoS) y al tipo de servicios (ToS), una CoS permite al administrador de la red agrupar diferentes flujos de paquetes teniendo cada uno requisitos de latencia y ancho de banda diferentes. Un ToS es un campo en una cabecera de IPv4 que permite que tenga lugar una clase de servicio, actualmente un campo ToS utiliza 3 bits lo que permite agrupar 8 flujos de paquetes o CoS (0-7).

Es importante anotar que las herramientas utilizadas para implementar estos servicios no son tan importantes como el resultado final conseguido, no hay que centrarse en una herramienta QoS para resolver todos los problemas QoS, en su lugar se debe mirar la red como un todo para determinar que herramientas si las hubiera, pertenecen a que partes de la red.

La QoS puede ayudar a resolver algunos de los problemas de la VoIP como son: la perdida de paquetes, la fluctuación de fase y el retraso de manejo; algunos de los problemas que la QoS no puede resolver son el retraso de propagación, el retraso de codec (Compresión/Descompresión), el retraso de muestreo y el retraso de digitalización.

Para ello se utilizan algoritmos de compresión, que, sin disminuir la calidad del sonido notablemente, si reduzcan drásticamente el ancho de banda utilizado. En una codificación normal, por ejemplo PCM, el muestreo de la señal con una resolución y frecuencia determinada se inyecta en la corriente de datos, con ello la calidad obtenida puede ser de un nueve sobre diez, ciertamente alta pero a costa de necesitar 64 Kbits por segundo para la transmisión.

Con los actuales algoritmos de compresión de predicción lineal, podemos alcanzar niveles de calidad de 7 u 8 sobre 10 y rebajar el ancho de banda necesario a 5,3 Kbits por segundo. En cuanto a la propagación, en todo el sistema se acumulan diversos retrasos producidos por diversos motivos, primero interviene la necesidad de comprimir paquetes de un tamaño concreto, realmente se produce un retraso por acumulación de la señal en este orden hablamos de retrasos del orden de 30 ms.

Posteriormente se producen retrasos en el tratamiento de la señal, aunque estos no deben sobrepasar el propio retraso de acumulación, por último nos encontramos con el retraso propio de la red aquí interviene la propagación propia de la red, routers, etc. Como norma general el retraso total introducido en una comunicación puede oscilar sobre los 200 ms, siendo una medida dependiente de la red y bastante oscilante. Como resumen se puede decir que la calidad total del servicio es algo inferior a la obtenida por la telefonía tradicional, pero dentro de unos márgenes totalmente aceptables.

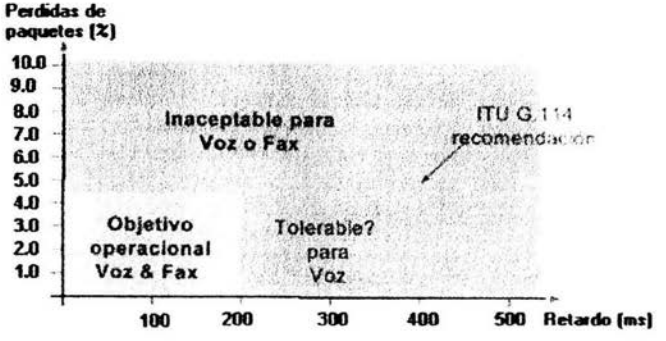
Una llamada telefónica VoIP puede ser equivalente a cualquier otro gran gasto que se planeara, por tanto es importante conocer que partes del limite no se puede cambiar y cuales se pueden controlar de

la tabla 1 y la fig. 33, la recomendación G.114 de la ITU-T sugiere que no haya mas de 150 ms. de retraso de extremo a extremo para mantener una buena calidad de voz.

Tabla 1
Retraso previsto de extremo a extremo.

	RETRASO FIJO	***RETRASO VARIABLE***
Retraso de codificador G.729 (5 ms look-ahead)	5 ms	
Retraso de codificador G.729 (10 ms por trama)	20 ms	
Retraso de empaquetamiento, incluido retraso de decodificador		
Retraso de gestión de cola 64 kbps troncal.		6 ms
Retraso de serialización (líneas privadas)	3 ms	
Retraso de red.	32 ms	
Bufer de fluctuación de fase		2-200 ms
Total – asumiendo un bufer de fluctuación de fase de 50 ms	**110 ms**	

Fig. 33
Estándares de compresión utilizados en Internet y grado de calidad de la voz que se obtiene.



2.10.1.- Limitaciones del ancho de banda.

Dependiendo de que codec sé este utilizando y de cuantas muestras de voz se quiera por paquete, la cantidad de ancho de banda por llamada puede incrementase drásticamente como en la tabla 2, para una explicación sobre los tamaños de los paquetes y el ancho de banda consumido son los siguientes:

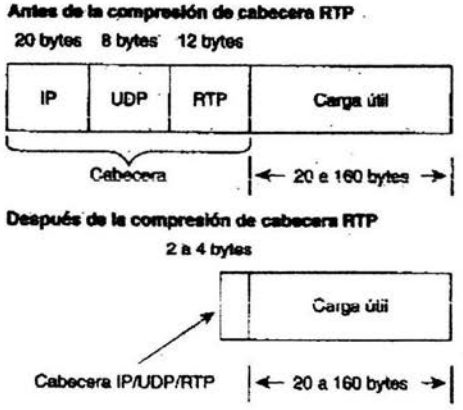
Tabla 2
Efectos del tipo de codec.

CODEC	*ANCHO DE BANDA CONSUMIDO*	*ANCHO DE BANDA CONSUMIDO CON cRTP.*	*LATENCIA DE MUESTRA.*
G.729 w/una 10 ms muestra / trama	40 kbps	9.6 kbps	10 ms
G.729 w/cuatro 10 ms muestra / trama	16 Kbps	8.4 Kbps	40 ms
G.729 w/dos 10 ms muestra / trama	24 Kbps	11.2 Kbps	20 ms
G.711 w/una 10 ms muestra / trama	112 Kbps	81.6 Kbps	10 ms
G.711 w/dos 10 ms muestra / trama	96 Kbps	80.8 Kbps	20 ms

2.10.2.- Protocolo de transporte en tiempo real comprimido (cRTP).

Para reducir el gran porcentaje de ancho de banda consumido por una llamada de voz G.729 se puede utilizar cRTP, la mayoría de las veces permite comprimir la cabecera de 40 bytes IP/RTP/UDP a 2 o 4 bytes de la fig. 34, con cRTP la cantidad de tráfico por llamada VoIP se reduce de 24 kbps. a 11.2 kbps., este es un gran aumento para enlaces de ancho de banda bajo.

Fig. 34
Compresión de cabecera RTP.



Por ejemplo para un enlace de 56 kbps. puede ahora transportar 4 llamadas G.729 VoIP a 11.2 kbps. cada una, sin cRTP solo se puede utilizar 2 llamadas VoIP G.729 a 26 kbps. Para evitar el consumo innecesario de ancho de banda disponible se utiliza cRTP en una base de enlace a enlace, este esquema de compresión reduce la cabecera IP/RTP/UDP a 2 bytes cuando las sumas de verificación de UDP no se utiliza o a 4 bytes cuando se utilizan las sumas de verificación de UDP.

cRTP utiliza algunas de las mismas técnicas que la compresión de cabecera del TCP, en la compresión de cabecera TCP la reducción del primer factor de dos en la velocidad de los datos ocurre porque la mitad de los bytes de las cabeceras IPv4 y TCP permanecen constantes a lo largo de la vida de la conexión.

2.10.2.1.- Desventajas sobre cRTP.

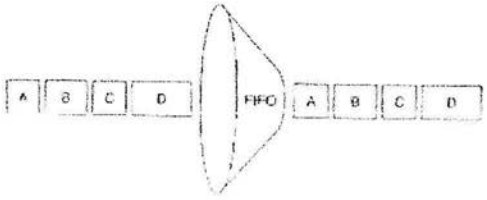
No se debe utilizar cRTP en interfaces de alta velocidad, ya que los inconvenientes de hacerlo son mayores que las ventajas, esto es que todo lo que supere la velocidad de T1 o E1 no necesita cRTP, al igual que ocurre con la compresión la CPU (unidad central de procesamiento) realiza trabajos de procesamientos adicionales para comprimir el paquete.

Esto incrementa la cantidad de utilización de la CPU en el router, por tanto se deben calcular las ventajas (requisito de ancho de banda más bajo) frente a los inconvenientes (mayor utilización del CPU).

2.10.3.- Gestión de colas.

Existe el concepto de Primero en entrar Primero en salir (FIFO) de la fig. 35, que significa que si somos los primeros en llegar seremos los primeros en salir, las redes actuales con su variedad de aplicaciones, protocolos y usuarios requieren una manera diferente para clasificar él tráfico. Cisco tiene varias herramientas de gestión de colas que permite al administrador de la red especificar que tipo de tráfico es especial o importante, y organizar la cola del tráfico sobre la base de esa información en lugar de hacerlo conforme al orden de llegada de los paquetes, la más popular de las herramientas para gestionar las colas se conoce como WFQ (gestión de colas apropiada ponderada).

Fig. 35
Cola FIFO no cambia el orden de los paquetes en la cola.



2.10.3.1.- Gestión de colas apropiada ponderada (WFQ).

La gestión de colas FIFO coloca todos los paquetes que recibe en una cola y los transmite conforme va haciendo ancho de banda disponible, la WFQ utiliza múltiples colas para separar los flujos y concede a cada flujo la misma cantidad de ancho de banda, esto evita que una aplicación como el protocolo de transferencia de archivos (FTP) consuma todo el ancho de banda.

WFQ asegura que las colas no carecen de ancho de banda y que él tráfico tiene un servicio previsible, los flujos de datos de bajo volumen reciben un servicio preferente, transmitiendo la totalidad de su carga ofrecida de manera oportuna.

Las corrientes de gran volumen de tráfico comparten la capacidad restante obteniendo un ancho de banda igual o proporcional, WFQ es similar a TDM (multiplexacion por división de tiempo) ya que divide el ancho de banda de igual manera entre los diferentes flujos de tal manera que no le falte a ninguna aplicación; sin embargo WFQ es superior a TDM porque cuando un flujo ya no esta presente WFQ se ajusta dinámicamente para utilizar el ancho de banda que queda libre para los flujos que todavía están transmitiendo.

La gestión de colas equitativa identifica las corrientes o flujos de datos sobre la base de varios factores, estos flujos de datos tienen prioridad dependiendo de la cantidad de ancho de banda que el flujo consuma, este algoritmo permite que el ancho de banda sea compartido equitativamente sin la utilización de listas de acceso u otras tareas administrativas que consuman tiempo; WFQ determina un flujo utilizando la dirección de origen y destino, el tipo de protocolo, la toma o numero de puerto y los valores QoS/ToS.

La gestión de colas equitativa permite que aplicaciones de ancho de banda bajo que constituyen la mayoría del tráfico, tengan todo el ancho de banda que necesitan relegando él tráfico de ancho de banda alto a compartir que resta de manera equitativa, también ofrece una fluctuación de fase reducida y permite que el ancho de banda disponible sea compartido entre todas las aplicaciones.

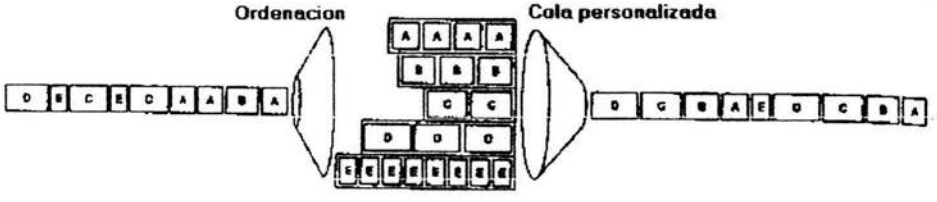
2.10.3.1.1.- Desventajas sobre WFQ.

El administrador de la red debe asegurara que las clases en WFQ son invocadas adecuadamente, con esto se evita que alguna aplicación solicite o utilice una prioridad mayor de la que le corresponde, WFQ no esta destinado a ejecutarse en interfaces que están registradas a mas de 2.048 Mbps.

2.10.3.2.- Gestión de colas personalizada (CQ).

Permite que los usuarios especifiquen un porcentaje de ancho de banda disponible para un protocolo determinado, se pueden definir hasta 16 colas de salida como la fig. 36, así como cola adicional para mensajes del sistema (mensajes de actividad); cada cola es atendida secuencialmente de manera cíclica, transmitiendo un porcentaje de tráfico antes de pasar a la siguiente cola.

Fig. 36
Estructura de cola personalizada.



El router determina cuantos bytes de cada cola deben ser transmitidos sobre la base de la velocidad de la interfaz y del porcentaje de tráfico configurado, esto es que otro tipo de tráfico puede utilizar el ancho de banda que no se utiliza de una cola A hasta que esa cola A requiera su porcentaje total.

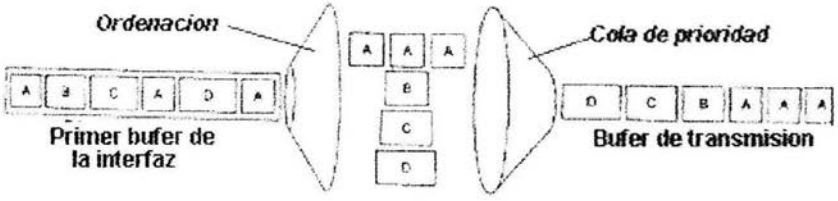
2.10.3.2.1.- Desventajas sobre CQ.

CQ requiere que se conozcan los tipos de puerto y de tráfico, esto equivale a una gran cantidad de sobrecarga administrativa, pero una vez que se ha completado esa sobrecarga administrativa CQ ofrece una propuesta mayor para la gestión de colas, que es lo que prefieren algunos clientes.

2.10.3.3.- Gestión de colas por prioridad (PQ).

Permite que el administrador de la red configure 4 prioridades de tráfico: alta, normal, media y baja; él tráfico de entrada es asignado a una de las 4 colas de salida de la fig. 37. El tráfico de la cola de prioridad alta es hasta que la cola este vacia, luego se transmite los paquetes que se encuentran en la cola de prioridad siguiente.

Fig. 37
Cuatro niveles de tráfico con prioridad.



Este orden en la gestión de colas asegura que el tráfico critico recibe siempre todo el ancho de banda que necesita, sin embargo impide que otras aplicaciones lo tengan, por tanto es importante entender los flujos del tráfico cuando se utiliza este mecanismo de gestión de colas para que las aplicaciones no carezcan del ancho de banda necesario, PQ se utiliza mejor cuando el tráfico de prioridad mas alta consume la menor cantidad de ancho de banda de la línea.

2.10.3.3.1- Desventaja sobre PQ.

Puede generar que el administrador de la red no atienda bien a las aplicaciones, una PQ inadecuadamente configurada puede atender a una cola y desatender completamente todas las demás, esto puede provocar que algunas aplicaciones dejen de funcionar.

2.10.3.4.- Políticas de enrutamiento.

Se pueden configurar una norma definida para los flujos de tráfico y no tener que depender completamente de los protocolos de enrutamiento para determinar el envío del tráfico y el enrutamiento, el enrutamiento con normas permite también definir el campo de precedencia IPv4 de tal manera que la red pueda utilizar diferentes clases de servicios.

Se pueden basar las normas en las direcciones IPv4, los números de puerto, los protocolos o el tamaño de los paquetes, se puede utilizar uno de estos descriptores para crear una simple norma o se pueden utilizar todos ellos para crear una norma complicada. Todos los paquetes recibidos en una interfaz que permita políticas de enrutamiento pasadas a través de filtros mejorados se conocen como mapas de ruta, estos dictan donde se transmiten los paquetes; las políticas de enrutamiento son especificas en la interfaz que recibe el paquete, no en la interfaz que envía los paquetes,

2.10.3.4.1.- Desventajas sobre las políticas de enrutamiento.

Hay que ser muy cuidadoso cuando se elige el tipo de normas o políticas que se enrutan ya que se pueden configurar determinadas normas para obligar a los routers Cisco a utilizar la ruta de switching de proceso (método mas lento de enviar paquetes), si se tiene cuidado se puede evitar que ocurra esto.

2.10.4.- Protocolo de configuración de reserva de recursos (RSVP).

Permite que los usuarios finales (puntos) señalen la red con el tipo de QoS necesario para una aplicación determinada, RSVP es un protocolo de señalización de extremo a extremo fuera de banda que solicita una determinada cantidad de ancho de banda y latencia con cada salto de red que soporta, sin un nodo de la red no soporta RSVP este protocolo se mueve hasta el siguiente salto.

Un nodo de la red tiene la opción de aprobar o denegar la reserva sobre la base de la carga de la interfaz para la que se solicita el servicio, las aplicaciones reciben una retroalimentacion dependiendo de si su petición de QoS ha sido aprobada o rechazada, algunas aplicaciones transmiten sus datos a todos sin preocuparse de la QoS.

Sin embargo otras aplicaciones inteligentes eligen no transmitir o tomar otra ruta, en el caso de VoIP esa ruta será la PSTN (Red telefónica publica conmutada); quien solicita los niveles de servicio en RSVP es la estación receptora y no la estación que transmite, esto permite que RSVP escale cuando se utiliza la tecnología de multidifusion IPv4 (un transmisor envía a múltiples receptores).

RSVP no es un protocolo de enrutamiento y no modifica la tabla de enrutamiento IPv4 basada en los flujos de tráfico o congestión, RSVP recorre simplemente IPv4 y permite que los protocolos de enrutamiento IPv4 elijan la ruta optima, esta ruta puede resultar no ser la ruta ideal de QoS.

2.10.4.1.- Desventajas sobre RSVP.

A pesar que RSVP es una herramienta de QoS no resuelve todos los problemas relacionados con QoS, tiene 3 inconvenientes: la escalabilidad, el control de admisión y el tiempo que tarda en preparar una reserva de extremo a extremo. RSVP tiene que ser desplegado en un entorno de gran escala, los

problemas de escalabilidad desconocidos que rodean a RSVP lo relegan hacia los límites de la red y lo obligan a utilizar otras herramientas QoS para el backbone de la red.

2.10.5.- Medición del tráfico.

Algunas veces es necesario regular o limitar la cantidad de tráfico que una aplicación puede enviar a través de varias interfaces o redes, Cisco tiene herramientas que permiten que el administrador de la red defina cuando ancho de banda puede utilizar una aplicación o incluso un usuario, estas funciones vienen de 2 maneras: herramientas de limite de tasa (CAR) y las herramientas de formación (GTS o FRTS).

La principal diferencia entre ambas herramientas de regulación del tráfico es que las de limite de tasa derivan el tráfico sobre la base de la medición, y la de formación generalmente almacenan temporalmente en un bufer el exceso de tráfico mientras esperan el siguiente intervalo abierto para transmitir los datos. CAR (Tasa de acceso comprometido) y las herramientas de formación del tráfico son similares en que ambas identifican cuando el tráfico excede el umbral definido por el administrador de la red.

A menudo estas 2 herramientas se utilizan juntas, la formación del tráfico se utiliza en él limite de la red (terminal del abonado) para asegurar que el cliente esta utilizado el ancho de banda necesario para la empresa, CAR se utiliza también en las redes de proveedores de servicios para asegurar que un abonado no excede de la cantidad de ancho de banda definida por su contrato con el proveedor de servicios.

2.10.5.1.- Tasa de acceso comprometido (CAR).

Es un mecanismo de medición que permite que el administrador de la red defina acciones de cumplimiento o de exceso, se puede utilizar una acción de cumplimiento para transmitir él tráfico y una acción de exceso para interrumpir el paquete o marcarlo con un valor de precedencia IPv4 mas bajo.

Los mecanismos de limitación de tasa de CAR permiten que el usuario:

- Controle la velocidad máxima del tráfico transmitido o recibido en una interfaz.
- Otorgue un control granular a la capa 3, lo que permite que una red IPv4 exhiba cualidades de red TDM.

Se puede limitar la tasa del tráfico por precedencia, dirección de control de acceso al medio (MAC), direcciones IPv4 u otros parámetros, los administradores de la red también pueden configurar listas de acceso para crear normas de límite de tasa mas granulares.

2.10.5.2.- Formación del tráfico(GTS-FRTS).

Ambos métodos de formación del tráfico son similares en cuanto a su implementación aunque sus interfaces de línea de comandos difieren algo y utilizan diferentes tipos de colas para contener y formar él tráfico que es aplazado, si un paquete es aplazado GTS utiliza WFQ para retener él tráfico diferido, FRTS utiliza CQ o PQ para retener él tráfico aplazado, dependiendo de lo que se haya configurado.

La formación del tráfico permite controlar él tráfico saliente de una interfaz para hacer coincidir su flujo con la velocidad de la interfaz de destino remota y asegurar que él tráfico se ajusta a las normas que se han contratado para el mismo, así se puede formar él tráfico adhiriéndose a un perfil determinado para reunir los requisitos de flujo y, eliminar los cuellos de botella en aquellas topologías que tengan desajustes de datos-tasa.

La formación del tráfico se utiliza principalmente para:

- Controlar la utilización del ancho de banda disponible.
- Establecer mediciones de tráfico.
- Regular el flujo del tráfico para evitar la congestión.

Se puede utilizar la formación del tráfico en las siguientes situaciones:

- Configurar la formación del tráfico en una interfaz con diferentes velocidades de acceso.
- Configurar la formación del tráfico si se ofrece un servicio de subtasa.

La formación de tráfico evita la perdida de paquetes, resulta de importancia para VoIP que se controle la latencia, al eliminar la cantidad de tráfico y perdida de tráfico en la red se pueden suavizar los patrones de tráfico y dar prioridad al tráfico en tiempo real.

GTS y FRTS son similares en la implementacion ya que comparten las mismas estructuras de código y datos, pero son diferentes con relación a sus interfaces de línea de comandos y los tipos de colas que utilizan.

GTS y FRTS son diferentes en estos 2 sentidos:

- FRTS soporta una formación basada en cada identificador de conexión de enlace de datos (DLCI), GTS es configurable por interfaz o subinterfaz.
- GTS soporta una cola de formación WFQ.

Se puede configurar GTS para que se comporte de la misma manera que FRTS asignando un DCLI (identificador de conexión de enlace de datos), por subinterfaz y utilizando soporte GTS más BECN. La formación de tráfico suaviza él tráfico almacenado que esta por encima de la tasa configurada en una cola, cuando llega un paquete a la interfaz para su transmisión ocurre lo siguiente:

- Si la cola esta vacía, el formador de tráfico procesa el paquete que llega, si el posible lo envía.
- Si los paquetes están en la cola, el formador de tráfico envía otro paquete nuevo a la cola.

Cuando los paquetes están en la cola, el formador de tráfico suprime él numero de paquetes que puede transmitir desde la cola en cada intervalo de tiempo.

CAPITULO 3
H.323.

3.1.- Historia de H.323.

Anteriormente al H.323, el ITU (Unión Internacional de Telecomunicaciones) se enfocó exclusivamente en la estandarización de las redes globales de telecomunicaciones, la ratificación de la norma (H.320) fue aprobada por el CCITT (Comité consultivo internacional para la telefonía y telegrafía) en Diciembre de 1990, sólo 3 años después se dispuso de equipos que cumplieran con la norma y que permitieran la interoperabilidad entre sí.

En Enero de 1996, un grupo de fabricantes de soluciones de redes y de pc's propuso la creación de un nuevo estándar ITU-T para incorporar voz y vídeo sobre una LAN (redes de área local). Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo hubo de contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

El H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local (LAN), metropolitana (MAN), regional o de área extensa (WAN), soporta así mismo Internet e Intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para "los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

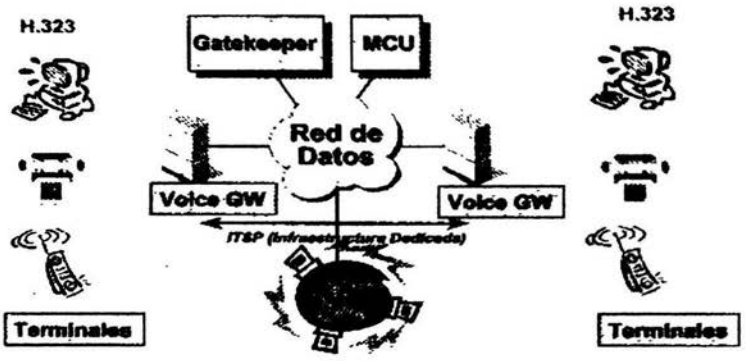
El H.323 también soporta videoconferencia sobre conexiones punto a punto, telefónicas y RDSI (Red Digital de Servicios Integrados); en estos casos se debe disponer un protocolo de transporte de paquetes tal como PPP (Protocolo de punto a punto). El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN, está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS), la tecnología de red más común en la que se están implementando H.323 es IP (Protocolo de Internet).

Este estándar define un amplio conjunto de características y funciones, algunas son necesarias y otras opcionales, el H.323 define mucho más que los terminales y el estándar definen los siguientes componente de la fig. 37 más relevantes:

- **Terminal**
- **Gateway.**
- **Gatekeeper.**
- **Unidad de Control Multipunto (MCU).**

El H.323 utiliza los mismos algoritmos de compresión para el vídeo y el audio que la norma H.320, aunque introduce algunos nuevos. Se utiliza T.120 para la colaboración de datos.

Fig. 38
Elementos para una comunicación en Internet.



3.2.- Introducción.

El H.323 es una especificación de la ITU-T para transmitir vídeo, audio y datos a través de una red IP (Protocolo de Internet) incluida la Internet, cuando son compatibles son H.323 los productos y aplicaciones de los fabricantes pueden comunicarse e interoperar unos con otros.

El H.323 dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y multipunto, la serie H de las recomendaciones también especifica H.320 para la Red digital de servicios integrados (RDSI) y H.324 para el Servicio telefónico analógico convencional (POTS) como mecanismos de transporte.

Las recomendaciones ITU-T que soporta las funciones de señalización H.323 y los medios apoyados de la fig. 39, son las siguientes:

Tabla 3
Funciones de señalización H.323.

FUNCIÓN	*PROTOCOLO*
Señalización de llamadas y empaquetado de flujos de medios para los sistemas de comunicación multimedia.	H.225
Protocolo de control de comunicación multimedia.	H.245
Codecs de audio	G.711, G.722, G.723, G728, G.729
Codecs de vídeo	H.261, H263
Protocolos de datos para conferencias multimedia	Series T.120
Transporte de medios	RTP/RTCP
Seguridad y cifrado de los terminales multimedia de la serie H.	H.235
Servicios complementarios de H.323	H.450.x

MEDIO	FORMATOS
Audio.	G.711, G.722, G.723, G.728, G.729, GSM.
Video.	H.261, H.262, H.263.
Protocolos de datos	Series T.120

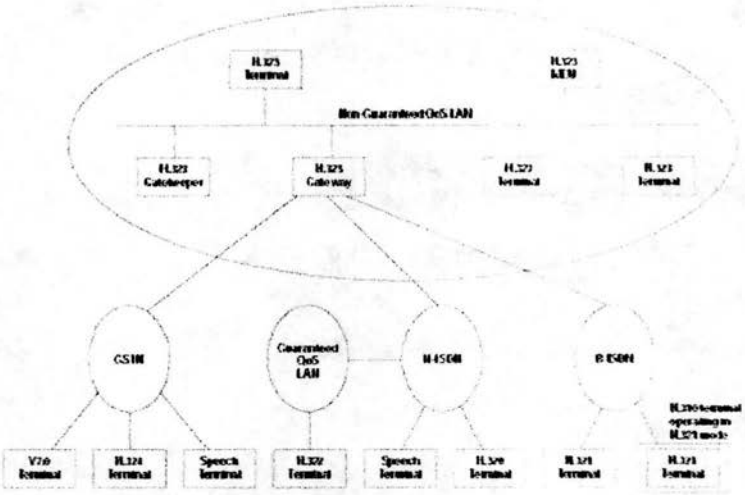
Fig. 39
Componentes principales de una red multimedia.

3.3.- Elementos .

En un sistema de H.323 incluyen como en la fig. 40 terminales, gateways, gatekeepers y unidades de control multipunto (MCU), los terminales (puntos finales) proporcionan conferencias punto a punto y multipunto para audio y de manera opcional vídeo y datos, los gateways interconectan con la PSTN o la red ISDN (RDSI) para interworking (redes interconectadas) en el punto final H.323.

Los gatekeepers proporcionan el control de admisión y servicios de traducción de direcciones para terminales o gateways, las MCU (unidades de control multipunto) son dispositivos que permiten que 2 o más terminales o gateways realicen conferencias con sesiones de audio y/o vídeo.

Fig. 40
Elementos de red H.323.

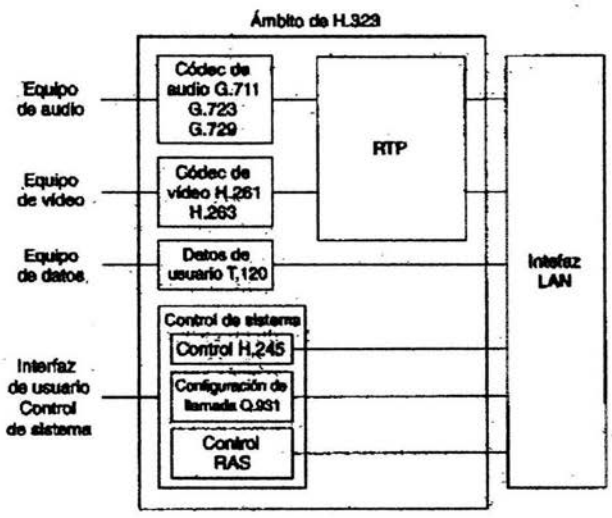


3.3.1.- Terminal.

Los terminales H.323 deben tener una unidad de control de sistema, una transmisión de medios, codec de audio e interfaz de red basada en paquetes de la fig. 41, los requisitos opcionales incluyen un codec de vídeo y aplicaciones de datos de usuario, las siguientes funciones y posibilidades se encuentran dentro del ámbito del terminal H.323:

- Unidad de control de sistema: proporciona a H.225 y H.245 el control de llamadas, intercambio de capacidad, mensajería y señalización de comandos para una actividad apropiada del terminal.
- Transmisión de medios: formatea el audio, vídeo, datos, flujos de control y mensajes transmitidos en la interfaz de red, la transmisión de medios recibe también el audio, vídeo, datos, flujos de control y mensajes desde la interfaz de red.
- Codec de audio. Codifica la señal desde el equipo de audio para su transmisión y decodifica el código de audio entrante, las funciones que se requieren incluyen la codificación y descodificación de voz G7.11 y recibir formatos de la ley μ, opcionalmente puede soporta la codificación y descodificación G7.22, G7.23.1, G.728 y G.729.
- Interfaz de red. Basada en paquetes que pueden hacer servicios de unidifusión y multidifusión de extremo a extremo del TCP y el UDP.
- Codec de vídeo. Es opcional pero si esta proporcionado debe ser capaz de codificar y descodificar vídeo de acuerdo con el QCIF H.261.
- Canal de datos. Soporta aplicaciones como acceso a base de datos, transferencia de archivos y conferencias como se especifica en la recomendación T.120.

Fig. 41
Relación entre los componentes de H.323.



3.3.2.- Gateway.

Se trata de un dispositivo repetidor electrónico que intercepta y adecua señales eléctricas de una red a otra, en Telefonía IP es un dispositivo que actúa de pasarela entre la red telefónica y una red IP como el de la fig. 42. Es capaz de convertir las llamadas de voz y fax en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet.

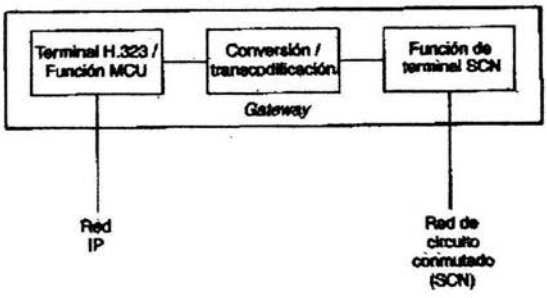
Fig. 42
Gateway.

Originalmente sólo trataban llamadas de voz, realizando la compresión/descompresión (codec), paquetización, enrutado de la llamada y el control de la señalización. Hoy en día muchos son capaces de manejar fax e incluir interfaces con controladores externos, como gatekeepers, soft-switches o sistemas de facturación.

Refleja las características de un punto final de una red de circuito conmutado (SCN) y un punto final H.323, traduce formatos de audio, vídeo y transmisión de datos, así como en sistemas de comunicación y protocolos. Esto incluye la configuración y el borrado de la llamada en la red IP y en la red SCN, los gateways no son necesarios a menos que se requiera la interconexión con la SCN.

Los puntos finales H.323 pueden comunicar directamente sobre la red de paquetes sin conectar con un Gateway, el Gateway actúa como una terminal H.323 o MCU en la red y un terminal SCN o MCU en al SCN de la fig. 43.

Fig. 43
Elemento del gateway H.323.



3.3.3.- Gatekeeper.

Es un componente del estándar ITU H.323, es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia. Los Gatekeepers proporcionan la inteligencia de la red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de los detalles de las llamadas para tarifar y comunicación con el sistema de gestión de la red.

También monitorizan la red para permitir su gestión en tiempo real, el balanceo de carga y el control del ancho de banda utilizado. Elemento básico a considerar a la hora de introducir servicios suplementarios.

Es una función opcional que proporciona servicios de control de prellamada y nivel de llamada a los puntos finales H.323, los gatekeepers están lógicamente separados de los demás elementos de la red en los entornos H.323, si se implementa mas de un Gatekeeper se lleva a cabo la intercomunicación de una manera no especifica.

La versión 3 de H.323 intenta recomendar una especificación de intercomunicación de Gatekeeper, este puede utilizar una simple secuencia consulta/respuesta (LRQ/FCF) para localizar a los usuarios remotos, para intercambiar alguna información la versión 3 utiliza el anexo G para la consulta de base de datos o intercambio.

El protocolo de OSP (Abrir primero la vía mas corta) se utiliza mucho para interacciones entre dominios tanto desde el gateway como desde el Gatekeeper, si un Gatekeeper esta presente en un sistema H.323 debe llevar a cabo lo siguiente:

- Conversión de direcciones. Proporciona acceso autorizado a H.323 utilizando los mensajes (ARQ/ACF/ARJ).
- Control de ancho de banda. Consiste en al administración de los requisitos de ancho de banda utilizando los mensajes (BRQ/BCF/BRJ).
- Administración de zona. Para los terminales, gateways y MCU registrados.

Opcionalmente el Gatekeeper puede aportar la siguiente funcionalidad:

- Señalización de control de llamadas. Utiliza el modelos de llamadas de Gatekeeper enrutado (GKRCS).
- Autorización de llamada. Permite que el Gatekeeper restrinja el acceso a determinados terminales y gateways o restrinja el acceso sobre la base de normas de la hora del día.
- Administración de llamada. Los servicios incluyen el mantenimiento de una lista de llamadas activas que se pueden utilizar para indicar que un punto final esta ocupado.

3.3.4.- Unidades de control multipunto (MCU).

El controlador multipunto (MC) soporta conferencias entre 3 o más puntos finales en una conferencia multipunto, los MC transmiten el conjunto de capacidades para cada punto final en la conferencia multipunto y pueden revisar las capacidades durante la conferencia, la función MC puede residir en un terminal, gateways, Gatekeeper o MCU.

El procesador multipunto (MP) recibe audio, vídeo y/o flujos de datos y los distribuye a los puntos finales que participan en una conferencia multipunto (multiconferencia), la MCU es un punto final que soporta conferencias multipunto y por lo menos consta de un MC y uno o mas MP. Si soporta conferencias multipunto centralizadas la MCU típica consta de un MC, un MP de audio, vídeo o datos.

3.3.5.- Servidor proxy H.323.

Actúa en la capa de aplicación y puede examinar los paquetes entre 2 aplicaciones que se comunican, los proxies pueden determinar el destino de una llamada y realizar la conexión si se desea, el proxy soporta las siguientes funciones:

- Las terminales que no soportan el protocolo de reserva de recursos (RSVP) se pueden conectar a través de un acceso o redes de área local (LAN), con una calidad de servicio (QoS) relativamente buena con el proxy.
- Los proxies soportan el enrutamiento del trafico H.323 separado del trafico de datos a través de un enrutamiento de aplicación especifico (ASR).
- Un proxy es compatible con la conversión de dirección de red, permitiendo que los nodos H.323 sean desplegados en las redes con un espacio de dirección privado.
- Un proxy desplegado sin un firewall o independientemente de un firewall proporciona seguridad, por lo que únicamente él tráfico H.323 pasa por el mismo. Un proxy desplegado junto con firewall permite que el firewall sea configurado para pasar todo él trafico H.323 tratando al proxy como si fuera un nodo de confianza.

3.4. Protocolos H.323.

La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos de medios y los mensajes en los sistemas H.323, estos protocolos son soportados por mecanismos de entrega de paquetes seguros y poco seguros sobre las redes de datos.

A pesar de que la mayoría de las implementaciones H.323 utilizan actualmente el protocolo TCP como el mecanismo de transporte para la señalización, la versión 2 de H.323 admite un transporte UDP básico, el conjunto del protocolo H.323 esta dividido en 3 áreas de control principales:

- Señalización de registro, admisiones y estado (RAS). Proporcionan un control de prellamadas en las redes basadas en gatekeepers H.323.
- Señalización de control de llamadas. Se utiliza para conecta, mantener y desconectar llamadas entre puntos finales.
- Control y transporte de medios. Proporciona el canal H.245 seguro que transporta los mensajes de control de los medios.

Fig. 44
Capas del conjunto del protocolo H.323

3.4.1.- Señalización RAS.

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

3.4.1.1.- Descubrimiento del gatekeeper.

El descubrimiento de Gatekeeper es un proceso manual o automático que los puntos finales utilizan para identifica con que Gatekeeper registrarse, en el método manual los puntos finales están configurados con la dirección IP del Gatekeeper y por tanto puede intentar el registro inmediatamente, pero únicamente con el Gatekeeper predefinido.

El método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento, este mecanismo permite que un punto final que tal vez no conozca a su Gatekeeper pueda descubrirlo a través de un mensaje multidifusión.

3.4.1.2.- Registro.

El registro es el proceso que permite que los gateways, puntos finales y MCU alcancen una zona e informen al Gatekeeper de sus direcciones IP y alias, el registro que un proceso necesario ocurre después del proceso de enrutamiento , pero antes de que se intente realizar ninguna llamada.

3.4.1.3.- Localización del punto final.

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

3.4.1.4.- Admisiones.

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

3.4.1.5.- Información de estado.

El gatekeeper puede utilizar el canal RAS para obtener información de estado desde un punto final, podemos utilizar este mensaje para monitorizar si el punto final esta en línea (online) o no (offline) debido a una condición de fallo, el periodo típico de sondeo para los mensajes de estado es de 10 seg.

3.4.1.6.- Control de ancho de banda.

Se administra inicialmente a través del intercambio de admisiones entre un punto final y el gatekeeper en una secuencia ARQ/ACF/ARJ, sin embargo el ancho de banda durante una llamada puede cambiar. El control de ancho de banda esta limitado en cuanto al ámbito al gatekeeper y a los gateways, y no tiene en cuenta el estado de la propia red, el gatekeeper solo mira en su ancho de banda estático para determinar si acepta o rechaza el ancho de banda solicitado.

3.4.2.- Señalización de control de llamada (H.225).

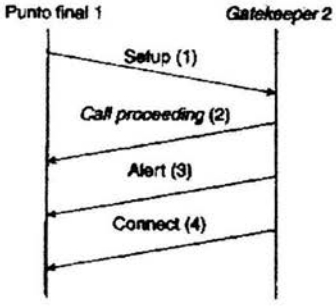
En las redes H.323 los procedimientos de control de llamadas se basan en la recomendación H.225 da la ITU-T, que especifica la utilización y soporte de los mensajes de señalización Q.931, un canal de control de llamadas seguro se crea en una red IP en el puerto del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre 2 puntos finales para el propósito de conectar, mantener y desconectar las llamadas.

El control de llamadas real y los mensajes de actividad se mueven a puertos breves después de configurar la llamada inicial, H.225 también especifica la utilización de los mensajes Q.932 para servicios suplementarios, los mensajes siguientes Q.931 y Q.932 son los mensajes de señalización mas utilizados en las redes H.323:

- Setup. Un mensaje hacia delante enviado por la entidad H.323 que llama en un intento de establecer conexión con la entidad H.323 llamada.
- Call proceeding. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad que llama para avisar que los procedimientos de establecimiento de llamada se han iniciado.
- Alerting. Un mensaje hacia atrás enviado desde la entidad llamada para avisar a la parte llamada que el sonido de llamada se a iniciado.
- Connect. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad llamante indicando que la parte llamada ha respondido a la llamada, el mensaje de conexión puede contener la dirección de transporte UDP/IP para la señalización de control H.245.
- Release complete. Enviado por el punto final que inicia la desconexión que indica que la llamada ha sido liberada, se puede enviar este mensaje únicamente si el canal de señalización de la llamada esta abierto o activo.
- Facility. Un mensaje Q.932 utilizado para solicitar o confirmar servicios suplementarios, también se utiliza para indicar su una llamada debe ser dirigida o debe ir a través de un gatekeeper.

Los mensajes de señalización para la configuración de llamada de la fig. 45, la interacción con el gatekeeper se limita a los mensajes RAS para los mensajes de estado de permiso y posibilidad de llamada.

Fig. 45
Mensaje de señalización de configuración de llamada.



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

H.245 maneja mensajes de control de extremo a extremo entre entidades H.323, los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, vídeo, datos y canal de control.

Un punto final estable un canal H.245 para cada llamada con el punto final que esta participando, el canal de control seguro se crea sobre IP utilizando el puerto TCP dinámicamente asignado en el último mensaje de señalización de llamada; el intercambio de capacidades, la apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes ocurren sobre este canal de control. H.245 también permite intercambio de capacidades separadas para la transmisión y recepción, así como la negociación de las funciones (determinación del codec).

3.4.3.1.- Procedimientos de conexión rápida.

Los 2 procedimientos disponibles para establecer canales de medios entre puntos finales son H.245 y Fast connect, Fast connect permite que se establezca la conexión de medios para llamadas básicas punto a punto con un mensaje de intercambio de ida y vuelta, estos procedimientos dictan que el punto final llamante incluye el elemento faststart (inicio rápido) en el mensaje de configuración inicial.

3.4.3.2.- Encapsular (Tunneling) H.245.

Se puede encapsular o tunelar mensajes H.245 dentro del canal de señalización de llamada H.225 en el lugar de crear un canal de control H.245 separado, este método mejora el tiempo de conexión de llamada y la asignación de recursos y proporciona una sincronización entre la señalización y el control de llamada, se puede encapsular múltiples mensajes H.245 en un mensaje H.225.

3.4.3.3.- Terminación de llamada.

Cualquier punto final que participe en una llamada puede iniciar el procedimiento de terminación de llamada, en primer lugar deben cesar las transmisiones de medios (audio, vídeo o datos) y cerrarse todos los canales lógicos, a continuación debe finalizar la sesión H.245 y enviarse un mensaje de liberación completa (release complete message) en el canal de señalización de llamada, si sigue estando abierto o activo.

En ese momento si ningún gatekeeper esta presente se termina la llamada, cuando un gatekeeper esta presente se utilizan los siguientes mensajes en el canal RAS para completar la terminación de llamada,

- Disengage request (DRQ). Se envía por un punto final o gatekeeper para terminar una llamada.
- Disengage confirm (DCF). Se envía por un punto final o gatekeeper para confirmar la desconexión de la llamada.
- Disengage reject (DRJ). Se envía por el punto final o gatekeeper para rechazar la desconexión de la llamada.

3.4.3.4.- Transporte de medios (RTP/RCTP).

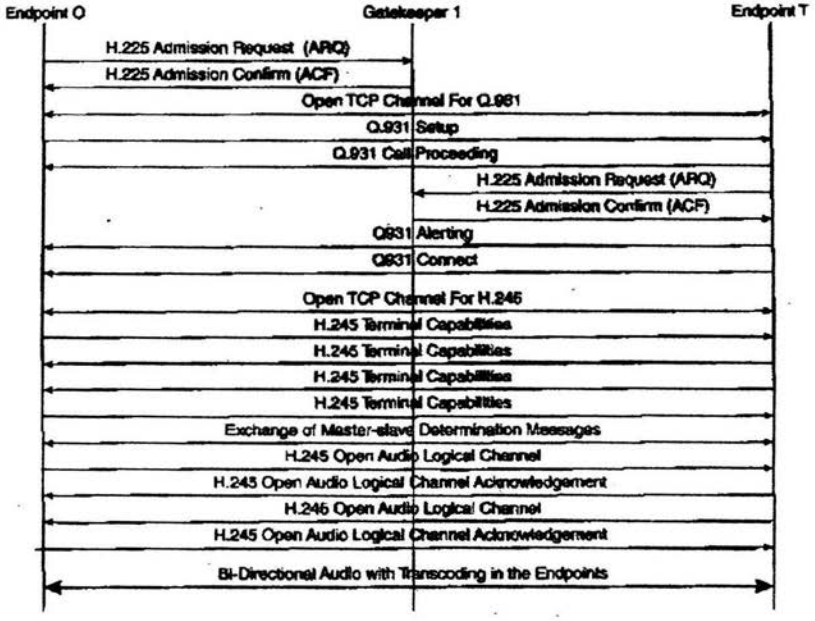
RTP (Protocolo de transporte para tiempo real) proporciona transporte de medios en H.323 y permite la entrega de extremo a extremo en tiempo real de audio, vídeo y datos interactivos sobre redes de unidifusión o multidifusión; los servicios de empaquetamiento y transmisión incluye la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización.

RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y las QoS, RTP monitoriza la entrega de datos y controla e identifica los servicios, el canal de medios se crea utilizando UDP donde los flujos RTP actúan en un no. de puerto par y el flujo RCTP correspondiente actúan en el siguiente de puerto mas alto (impar).

3.5.- Flujos de llamada H.323.

Los protocolos de H.323 proporcionan una configuración de llamada entre 2 puntos finales, suponiendo que son llamadas de voz y que todos los puntos finales han completado el registro con el gatekeeper apropiado, los procedimientos mostrados de las figs. 46-47 de configuración de llamada para las implementaciones de un único gatekeeper.

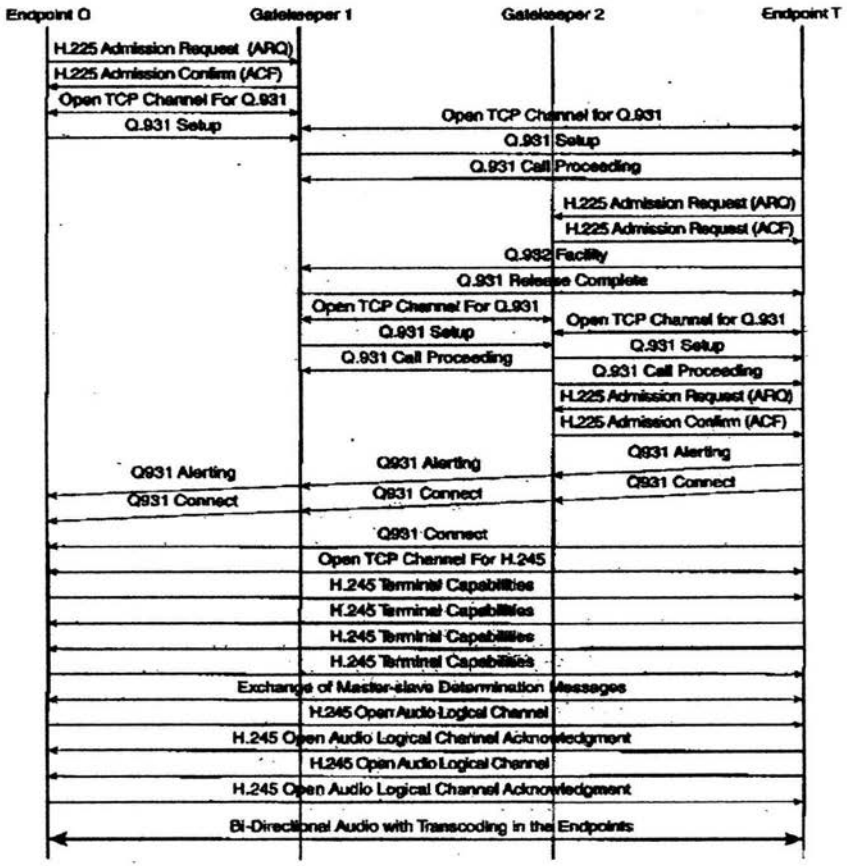
Fig. 46
Señalización directa de un punto final (mismo gatekeeper).



Los flujos de llamada de la fig. 46 que utilizan la señalización directa de un punto final entre 2 puntos finales que comparten el gatekeeper, los flujos de la fig. 47 de llamada que utilizan la señalización de

llamada en cuenta que el procedimiento H.245 esta manejando directamente entre los puntos finales y esta enrutado por el gatekeeper.

Fig. 47
Señalización de llamada de gatekeeper enrutado (mismo gatekeeper).



3.6.- H.323, una extensión del H.320.

El H.323 se fundamenta en las especificaciones del H.320, muchos de los componentes del H.320 se incluyen en el H.323. A esto el H.323 se puede ver como una extensión del H.320, el nuevo estándar fue diseñado específicamente con las siguientes ideas:

- Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931.
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

3.6.1.- Audio, Vídeo y Datos en H.323.

El H.323 se construye sobre muchos de los elementos del H.320 y a la vez amplía sus capacidades, algunas de las capacidades añadidas resultan del comportamiento inherente al tráfico de paquetes y su forma de ser transmitidos. Otras resultan de las mejoras en las técnicas de compresión y señalización que han sido desarrolladas a lo largo del tiempo. Un ejemplo de estas últimas es el nuevo algoritmo de compresión de vídeo H.263, que se basa en el H.261 y se ha optimizado para anchos de banda pequeños. A una determinada velocidad de transferencia, el H.263 ofrecerá una calidad de imagen considerablemente superior al H.261.

Todos las terminales H.323 deben soportar audio, concretamente deben ser capaces de codificar y decodificar audio en el algoritmo G.711, ya especificado en H.320. Para adaptarse a las necesidades de las diferentes redes, especialmente en conexiones con poco ancho de banda, un terminal debe ser capaz de codificar y decodificar la voz usando otros diferentes algoritmos.

Las capacidades de vídeo son opcionales, una terminal puede soportar o no la codificación de vídeo. Si se soporta el único modo exigido es el H.261, más allá de este punto una terminal puede soportar otros modos de vídeo con algoritmos propietarios o estándares.

La compartición de datos es opcional en H.323 y debe cumplir la norma T.120, los productos H.323 tienen nuevas capacidades debido a la añadida flexibilidad de las redes de datos tomando ventaja de los entornos IP y como resultado, los usuarios se benefician de las mismas.

3.6.2.- Ventajas de la tecnología H.323.

Reducción de los costos de operación.

H.323	H.320
Se pueden utilizar los cableados de los campus, las conexiones WAN basadas en routers IP y los servicios WAN para enviar vídeo. Esto es una fuente potencial de importantes ahorros de explotación. Los costos de soporte de las infraestructuras (por ejemplo SNMP) pueden combinarse.	La tecnología H.320 requiere típicamente redes separas para el vídeo y los datos. Esto supone doble cableado e infraestructuras de red. Este modelo incremento el costo de implantación por sistema.

Más amplia difusión y mayor portabilidad.

H.323	H.320
Con H.323, cada puerto con soporte IP puede potencialmente soportar vídeo. Esto hace la tecnología accesible a una más amplia variedad de usuarios. Además, es más fácil mover un equipo en nuestro entorno, lo que hará que un mismo equipo pueda ser usado para más aplicaciones.	Con H.320, se debe dedicar una línea por cada localización. La mayor parte de las PC's no podrán fácilmente soportar vídeo, lo cual limita también la accesibilidad y portabilidad de los sistemas.

Un diseño Cliente / Servidor con prestaciones.

H.323	H.320
El diseño del H.323 descansa fuertemente en los componentes de la red. Sus capacidades están distribuidas a través de la red. Un ejemplo es el gatekeeper este puede residir en un servidor, en un gateway o en una MCU. Se encarga de registrar los usuarios o clientes (sistemas de videoconferencia) y puede potencialmente ofrecerles un conjunto de funciones de comunicación.	Como norma, un equipo H.320 no se conecta a un servidor. Las características del sistema residen en la plataforma de videoconferencia misma. Este enfoque de comunicación orientado a la terminal no soporta servicios suplementarios tales como enrutado de llamadas, transferencia o retención. Son servicios que están por la tecnología de las centrales telefónicas.

3.7.- PROTOCOLO DE INICIO DE SESIÓN (SIP).

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

Los participantes en la sesión pueden ser personas o dispositivos como los servidores de los medios, el SIP proporciona funcionalidad para dar soporte a usuarios móviles operando como proxies, solicitando la redirección a la localización actual del usuario. El protocolo SIP se ha diseñado para ser independiente de los protocolos de las capas inferiores de transporte, el SIP es un protocolo cliente/servidor orientado a texto.

Una transacción consiste en una solicitud de un cliente junto con la correspondiente respuesta de uno o más servidores, las funciones de señalización básica se implementan mediante una o más transacciones.

Se puede utilizar invitaciones SIP para establecer sesiones y transportar descripciones de la sesión, SIP soporta sesiones unidifusión y multidusión, así como llamadas punto a punto y multipunto. Las comunicaciones se pueden establecer y terminar utilizando estas 5 facetas de SIP:

- Localización de usuario.
- Capacidad de usuario.
- Disponibilidad de usuario.
- Configuración de la llamada.
- Manejo de la llamada.

El SIP puede operar en conjunto con otros protocolos de señalización como el H.323, la telefonía IP se sigue desarrollando y en el futuro requerirá posibilidades adicionales de señalización y la extensibilidad de SIP permitara dichos desarrollos de funcionalidad. Las cabeceras de los mensajes SIP son versátiles y se pueden registrar funciones adicionales con la agencia de asignación de números Internet (IANA), la flexibilidad del mensaje SIP también permite que los elementos construyan servicios telefónicos avanzados, incluidos los servicios de tipo movilidad.

3.7.1.- Elementos.

Los 2 componentes de un sistema SIP son los agentes de usuario (UA) y los servidores de red (proxy), las partes que llaman y son llamadas se identifican con direcciones SIP, las partes necesitan localizar servidores y usuarios, las transacciones SIP.

3.7.2.- Agentes de usuario.

Son aplicaciones (SW) cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como cliente y servidor.

- Cliente. Inicia las peticiones SIP y actúa como el agente usuario del llamante.
- Servidor. Recibe y devuelve las respuestas en nombre del usuario, actúa como el agente de usuario llamado.

3.7.3.- Servidores de red.

Su función es la de llevar a cabo el encaminamiento de la llamada en la fase de establecimiento, es decir encontrar al usuario deseado en la red, existen 2 tipos de servidores de red SIP: los proxy y los redirect (redireccion):

- Servidor proxy. Actúa en nombre de otros clientes y contiene funciones de cliente y de servidor, un servidor proxy interpreta y puede rescribir cabezas de peticiones antes de pasarlas a los demás servidores.
- Servidor de redireccion. Acepta las peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor, estos servidores no aceptan llamadas ni tampoco procesan peticiones SIP.

3.7.4.- Direccionamiento.

Las direcciones SIP también llamadas localizadores universales de recursos (URL) SIP, existen en la forma de usuario @ host, un URL SIP se identifica por usuario@host; la parte de usuario de la dirección puede ser un nombre de usuario o un numero de teléfono y la parte de host puede ser un nombre de dominio o una dirección de red. Se puede identificar a un URL SIP de un usuario por su dirección de correo electrónico.

3.7.5.- Localización de un servidor.

Un cliente puede enviar una petición SIP directamente a un servidor proxy configurado localmente o en la dirección IP y el puerto del correspondiente URL SIP, enviar una petición SIP es relativamente fácil ya que la aplicación de sistema final conoce al servidor proxy, enviar una petición SIP de la segunda manera es algo mas complicado por las siguientes razones:

1- El cliente debe determinar la dirección IP y él numero de puerto del servidor al que va destinado la petición.

2- Si él numero de puerto no esta enumerado en el URL SIP, el puerto predeterminado es 5060.
3- Si el tipo de protocolo no esta enumerado en el URL SIP pedido, el cliente debe primero internar conectar utilizando el UDP o el TCP.
4- El cliente consulta el servidor de sistema de denominación de dominio (DNS) para buscar la dirección IP del host, si no encuentra ningún registro de dirección el cliente es incapaz de localizar al servidor y no puede continuar con la petición.

3.7.6.- Transacciones SIP.

Cuando se ha resuelto la dirección, el cliente envía uno o más peticiones SIP y recibe una o más respuestas desde el servidor especificado, todas las peticiones y respuestas asociadas con esa actividad están consideradas como parte de una transacción SIP.

Para mayor simplicidad y coherencia, los campos de cabecera en todos los mensajes de petición coinciden con los campo de cabecera en todos los mensajes de respuesta, se pueden transmitir transacciones SIP en los protocolos UDP y TCP.

Con TCP se pueden transportar todos los mensajes de petición y respuesta relacionados con una única transacción SIP sobre la misma conexión TCP, también se pueden transportar transacciones UDP la respuesta se envía a la dirección identificada en el campo de cabecera de la petición.

3.7.7.- Localización de un usuario.

La parte llamada puede desplazarse desde uno o varios sistemas finales a lo largo del tiempo, puede moverse desde una LAN corporativa a una oficina en casa conectada a través de su proveedor de servicios de Internet (ISP) o una conexión publica de Internet mientras atiende a una conferencia.

Para los servicios de localización SIP necesita acomodar la flexibilidad y la movilidad de los sistemas finales IP, las localizaciones de estos sistemas finales pueden estar registrados con el servidor SIP o con otros servidores de localización fuera del ámbito de SIP, la acción y resultado de localizar a un usuario depende del tipo de servidor SIP que se este utilizando.

Un servidor de redirección simplemente devuelve la lista completa de localizaciones y permite que el cliente directamente al usuario, un servidor proxy puede probar las direcciones en paralelo hasta que la llamada tenga éxito.

3.8.- Mensajes SIP.

Existen 2 tipos de mensajes SIP: peticiones iniciadas por los clientes y respuestas devueltas desde los servidores, cada mensaje contiene una cabecera que describe los detalles desde los servidores. SIP es un protocolo basado en texto con una sintaxis de mensajes y campos de cabecera idénticos al protocolo de transferencia de hipertexto (HTTP), los mensajes SIP se envían sobre los protocolos TCP o UDP con múltiples mensajes transportados en una única conexión TCP o datagrama UDP.

3.8.1.- Cabecera de mensaje.

Se utilizan para especificar la parte llamante, la ruta y el tipo de mensaje de una llamada, los 4 grupos de cabecera de mensaje son los siguientes:

- Cabeceras generales. Se aplica a las peticiones y a las respuestas.
- Cabeceras de entidad. Define información sobre el tipo de cuerpo del mensaje y longitud.
- Cabeceras de petición. Permite que el cliente incluya información de petición adicional.
- Cabeceras de respuestas. Permite que el servidor incluya información de respuesta adicional.

3.8.2.- Peticiones de mensaje.

La comunicación SIP presenta 6 tipos de peticiones de mensaje, estas peticiones a las que se hace referencia como métodos, permiten que los agentes de usuarios y servidores de red localicen, inviten y administren llamadas; las 6 peticiones SIP son las siguientes:

- INVITE. Este método indica que el usuario o servicios es invitado a participar en una sesión, incluye una descripción de sesión y para llamadas de 2 vías, la parte llamante indica el tipo de medio.
- ACK. Estas peticiones corresponden a una petición INVITE, representa la confirmación final por parte del sistema final y concluye la transacción iniciada por el comando INVITE.
- OPTIONS. Este método permite consultar y reunir posibilidades de agentes de usuarios y servidores de red, esta petición no se utiliza para establecer sesiones.
- BYE. Este método se utiliza por las partes que llaman y son llamadas para liberar una llamada, antes de liberar realmente la llamada el agente de usuario envía esta petición al servidor indicando el deseo de liberar la sesión.
- CANCEL. Esta petición permite que los agentes de usuario y servidores de red cancelen cualquier petición que este en progreso, esto no afecta a las peticiones terminadas en las que las respuestas finales ya fueron recibidas.
- REGISTER. Este método se utiliza por los clientes para registrar información de localización con los servidores SIP.

3.8.3- Respuestas de mensajes.

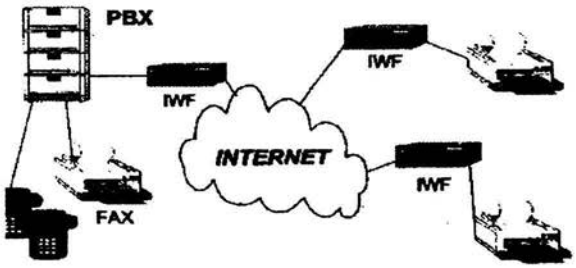
Están basadas en la recepción e interpretación de una petición correspondiente, se envían como respuesta a una petición e indican si la llamada ha tenido éxito o ha fallado, incluido el servidor.

CAPITULO 4
APLICACIONES DE VoIPv4.

4.1.- FAX SOBRE IP (FoIP).

Al utilizar fax sobre Internet (FoIP) la empresa reduce costos de llamadas de larga distancia entre un 20 y 30 %, se garantiza la seguridad (encriptar documento), proporcionar mayor rapidez en los envíos y se eleva el nivel de productividad de la empresa. El envío de faxes a través de la red mundial requiere la existencia de un marco legal y regulatorio que permita la operación de la voz sobre IP, la solución permite la conveniencia de que Internet sea un carrier (portador) para voz y para el fax.

Fig. 48
Fax a través de Internet.



Si lo anterior es posible y permitido, los beneficios repercutirán en todos los involucrados desde los proveedores hasta el usuario final que demanda servicios eficientes de calidad a bajo costo; el concepto y propósito fundamental del fax sobre Internet son simples: se utiliza la red publica que solo cuesta una llamada local.

La solución que ofrece FoIP a los 3 sectores principales: corporaciones, empresas medianas y pequeñas, y al hogar son las siguientes:

- Sector corporativo. Ofrece un beneficio complementario, generalmente estas empresas poseen la infraestructura necesaria para enviar documentos vía telefónica y el tener un ahorro de costos operativos en él tráfico de faxes al exterior.
- Sector de mediana y pequeña empresa. Este sector podría ser él mas beneficiado con esta solución, no cuenta con grandes redes y necesita medios de transmisión de documentos a la medida de sus responsabilidades en regiones o piases específicos.
- Sector final. Se convierte en una gran ventaja si se encuentra acompañado de voz sobre IP por la reducción de costos en las llamadas de larga distancia.

Los 2 retos antes los cuales se enfrenta esta solución para lograr una presencia fuerte en el mercado:

- La cobertura.
- El marco legal.
- La infraestructura de las telecomunicaciones.

En México corresponde a la Cofetel (Comisión federal de telecomunicaciones) establecer el marco regulatorio para proveer servicios no solo de envío de fax, sino de servicios de IP; México cuenta con la infraestructura necesaria para ofrecer este servicio.

4.1.2.- Funcionamiento.

El funcionamiento del envío de un fax común se realiza una llamada local al servidor local el cual a su vez la envía a través de la red mundial a otro servidor localizado en otra ciudad o país, para que se conecte a la red pública y así se entregue el documento otro fax o PC, en oposición al anterior sistema tradicional en donde una llamada generada en un fax es enviada a la red telefónica, enrutada, digitalizada y dirigida a otro fax.

El nuevo sistema de envío realiza 2 pasos adicionales, la llamada se va a un fax/server local y luego viaja por Internet a otro, de esta manera se ahorra la llamada de larga distancia puesto que antes, por medio de una llamada local se contacta al proveedor de servicio que se encargaría del resto.

El envío de fax a través de Internet existen 3 posibilidades: de fax a fax, de PC a fax y de PC a PC, en cualquiera de ellas el servidor de fax es de suma importancia pues una computadora con muchas líneas telefónicas y faxes individuales que posibilita el envío apropiado de los documentos; el cual consta del documento que es enviado por medio de una llamada local ya sea originada en un fax o PC aun fax/server para luego este intercomunicarse por medio de Internet con otro que puede encontrarse dentro o fuera del país, permitiendo un ahorro en el costo de la larga distancia, este segundo fax/server enruta la llamada a traces de la red pública o del operador local, para luego enviar el documento ya sea un fax común o a una PC:

4.2.- CONMUTADORES IP.

La mayoría de las empresas poseen una PBX (Central privada de comunicaciones telefónica) de tecnología propietaria para la red telefónica y una red LAN completamente separada para el transporte de datos, pero últimamente las redes de voz y datos se están relacionando cada vez mas, e integrando una sola red mas sofisticada que permite que las comunicaciones de voz viajen sobre las líneas de datos.

Esta integración es una de las tendencias tecnológicas más importantes en la actualidad, que permite notables mejoras y ahorros en las redes de comunicaciones de las empresas: simplificando la administración de los recursos de la red, expansión de la capacidad, soporte a nuevas aplicaciones y disminución de los costos por llamadas de larga distancia.

Las funciones manejadas por la red de circuito conmutado esta migrando a la red de datos IP, la calidad y confiabilidad de la infraestructura de la red IP y de la arquitectura PBX IP son aspectos claves en la convergencia de voz y datos.

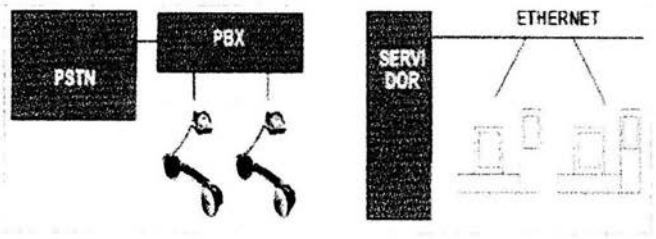
4.2.1.- Características.

Una PBX IP es un sistema capaz de proveer todas las capacidades de un conmutador tradicional sobre redes IP a nivel LAN y WAN, el sistema PBX IP se encuentra constituido principalmente por 3 componentes:

- El dispositivo de usuario.
- El centro de procesamiento de llamadas.
- Gateways IP/PSTN (protocolo de Internet/red publica telefónica conmutada).

Estos 3 subsistemas hacen uso de la infraestructura LAN/WAN existente para intercomunicarse entre sí de la fig. 49.

Fig. 49
Intercomunicación de los 3 sistemas.



4.2.2.- Funcionamiento.

El dispositivo de usuario presenta 2 opciones: un teléfono IP o una PC con software H.323, el teléfono IP es un dispositivo que ofrece una calidad de transmisión y un conjunto de servicios telefónicos similares a los PBX tradicionales, su definición en la red de datos se realiza mediante la asignación de una dirección IP dentro de la red y su operación satisface el estándar H.323.

Los teléfonos IP se conectan directamente a una computadora permitiendo tener la misma funcionalidad de una teléfono tradicional, pero ahora conectado a una LAN. El centro de procesamiento de llamadas provee la inteligencia de red necesaria para que las comunicaciones IP posean todas las funcionalidades de una PBX tradicional, sus funciones principales son la señalización (Q.931 para ISDN y H.225/H.245 para paquetes IP), control de llamadas y supervisión de la calidad de conexión mediante la administración de esquemas de compresión.

Una vez que la comunicación queda establecida entre 2 partes, el centro de procesamiento de llamadas libera la conexión hasta que se recibe una nueva solicitud, la principal ventaja del centro de

procesamiento de llamadas es que puede centralizar en un servidor las funciones PBX requeridas para varios sitios remotos, lo que reduce enormemente los costos de despliegue y gestión de la red.

Además puede ser administrado a través de un servidor web y ofrece la posibilidad de ejecutar administración remota, los Gateways IP/PSTN se encargan de interconectar el sistema PBX IP a la PSTN (Red publica de telefonía conmutada), esta conexión es esencial en este tipo de sistemas mientras la gran mayoría del trafico sea transportado por la PSTN.

La función principal del gateway es servir de interface entre una red IP y una red de circuitos, convirtiendo paquetes de voz IP en canales telefónicos tradicionales y viceversa, otras funcionalidades incluidas en los PBX IP son:

- Resistencia a cortes de abastecimiento de energía.
- Configuración redundante en el servidor para aumentar la confiabilidad en el control de llamada.
- Enrutamiento de llamada alternativo cuando los enlaces IP o los enlaces telefónicos no están disponibles.
- Dar prioridad al trafico de voz sobre grandes redes corporativas IP, garantizando de esta forma una calidad de servicio aceptable de extremo a extremo.

La tendencia más importante será la migración desde una estructura compuesta predominante por sistemas propietarios a una industria mas abierta y con sistemas compatibles sobre el formato IP, la nueva industria PBX IP incluirá 4 grandes áreas de negocio:

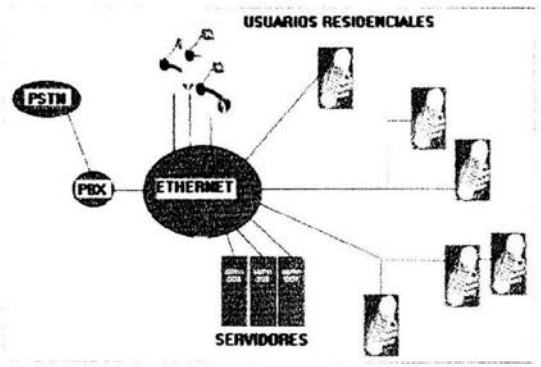
1. Infraestructura IP: compuesta por la conectividad IP provista principalmente por los proveedores de equipamiento LAN/WAN.
2. Control de llamada (sistemas operativos y servidores): sistemas operativos LAN con la capacidad de proveer servicios y funcionalidades telefónicas tradicionales, los servidores serán provistos por los principales proveedores actuales, agregando características de confiabilidad y disponibilidad.
3. Dispositivos de usuario: software y teléfonos IP capaces de ser conectadas a redes IP directamente con niveles de calidad similares a la red telefónica tradicional.
4. Aplicaciones avanzadas: aprovechando la natural integración de los sistemas telefónicos y datos, surgirán aplicaciones mas sofisticadas que los servicios telefónicos clásicos.

4.2.3.- Aplicaciones.

A- PBX IP detrás del sistemas PBX tradicional existente.

Esta configuración extiende la cobertura del sistema telefónico privado haciendo uso de la red IP como transporte, el PBX IP se conecta al PBX tradicional mediante un gateway y el centro de procesamiento de llamadas se instala en un servidor NT en el centro de datos de la empresa, bajo esta configuración se mantiene todas las funcionalidades telefónicas y el ambiente de operación es transparente para el usuario como en la fig. 50.

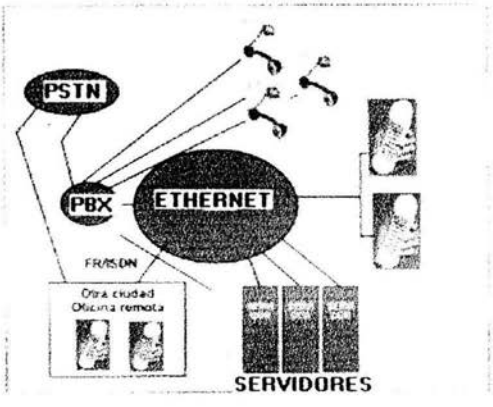
Fig. 50
PBX IP.



B- Oficinas remotas sobre la red IP.

Esta aplicación es similar a la anterior en cuanto a funcionalidades, con la diferencia que se incluye interfaces WAN IP para conectar en red determinados sitios remotos, el procesamiento de llamada puede permanecer centralizado o puede ser instalado en el sitio remoto como fuente secundaria de la fig. 51.

Fig. 51
Oficina remota.

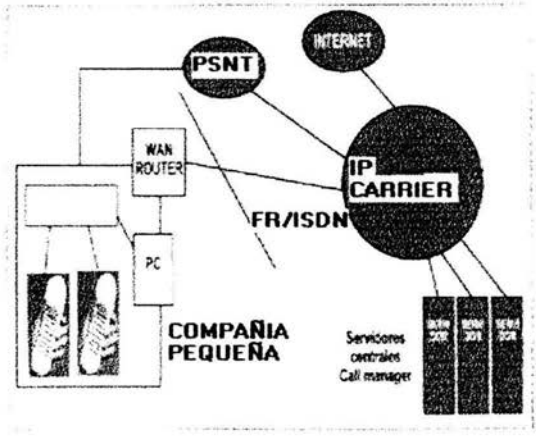


C- Servicios públicos.

La funcionalidad de la PBX IP pueden ser ofrecida como un servicio público por los carriers o ISPs (proveedor de servicios de Internet) a clientes corporativos o residenciales, aquí el centro de procesamiento de llamadas no pertenece a la red del cliente sino al carrier o al ISP que ofrece el servicio.

Cada cliente puede utilizar funcionalidades telefónicas avanzadas sin estar restringido a encargarse directamente del procesamiento de llamadas ni escalamientos de capacidades rígidos de la fig. 52, la tradicional central telefónica será paulatinamente sustituida por la red de conmutación de paquetes, esto generara importantes ahorros a las empresas quienes solo deberán preocuparse de robustecer su red IP. De esta forma solucionaran sus necesidades de voz y datos al mismo tiempo, él termino de la tecnología propietaria en telefonía redundara en grandes beneficios para los consumidores quienes ya no pagaran por distancia sino por conexión.

Fig. 52
Servicios públicos.



4.3.- TELEFONÍA IP.

La telefonía IP o VoIP (Voz transmitida sobre Protocolo Internet) permite a los usuarios establecer llamadas de voz sobre conexiones IP (redes de datos corporativos, Intranets, Extranet, Internet, etc.), y a la vez reducir considerablemente el presupuesto correspondiente al servicio telefónico, llegando inclusive a eliminarlo por completo en lo que se refiere a la comunicación interna entre sucursales de una empresa o de un grupo de empresas.

Si no desea tener un PC en su oficina o en casa, pero requiere tener accesar a Internet, consultar base de datos, comunicarse con sus clientes vía correo electrónico, agendar citas y accesar a paginas web, los teléfonos IP (protocolo de Internet) son la opción ideal. Además de contar con acceso a Internet los teléfonos IP como la fig. 53 permiten hacer llamadas de larga distancia nacional e internacional a bajo costo, debido a la utilización de Internet como medio de transporte de la voz, además se podrá tener al alcance otros servicios como identificador de llamada y marcaje rápido.

Fig. 53
Teléfono IP.

4.3.1.- Características.

La Voz sobre IP (VoIP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación de voz, fax, aplicaciones de mensajes de voz que son transportadas vía red IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

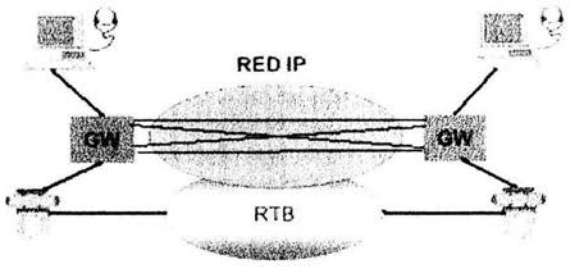
La telefonía IP convierte la computadora en un teléfono, es un servicio que permite realizar llamadas desde redes que utilizan el protocolo de comunicación IP (Internet Protocolo), es decir, el sistema que permite comunicar computadores de todo el mundo a través de las líneas telefónicas. Esta tecnología digitaliza la voz y la comprime en paquetes de datos que se reconvierten de nuevo en voz en el punto de destino, algunas formas de acceder a este servicio como en la fig. 54 son:

- Comunicación entre usuarios de PC conectados a Internet. Mediante el uso de computadoras multimedia y un programa adecuado se pueden entablar una conversación en tiempo real con otra computadora similar ubicada en cualquier parte del mundo.

- La segunda modalidad es la que posibilita la comunicación entre 2 usuarios, aunque uno de ellos no esté conectado a Internet. Una persona conectada a través de su PC con Internet puede llamar a un teléfono fijo.

- La tercera modalidad, y la más reciente, permitió ampliar las comunicaciones. 2 teléfonos fijos pueden comunicarse entre sí por medio del protocolo IP; uno de ellos llama a una central conectada a Internet y ésta lo comunica con el otro teléfono fijo de manera similar a la descrita anteriormente.

Fig. 54
Comunicación telefónica a través de Internet.



4.3.2.- Funcionamiento.

La conversión de la voz a datos requiere una sofisticada formulación matemática, que comprime la voz humana digitalizada en un conjunto de datos mucho más pequeños y manejables, una fórmula similar expande los datos comprimidos para devolver la voz a su estado original una vez que llega a su destino, minimizando el ancho de banda consumido, por lo que se optimizan los recursos disponibles. Por ejemplo, una conversación de telefonía IP ocupa aproximadamente la octava parte que una tradicional.

Uno de los principales logros de la telefonía IP consiste en realizar todo ese complicado proceso de compresión y descompresión de la voz en una pequeña fracción de segundo.

Debido a que las formulaciones matemáticas y los procesadores de señal para la compresión y descompresión de la voz en datos son cada vez más eficientes, y los anchos de banda disponibles para el traslado de la voz sobre IP cada vez son mayores, la calidad de las comunicaciones de voz sobre IP ha superado la de la telefonía celular, y prácticamente ha igualado a la de las llamadas telefónicas sobre sistemas de telefonía estándar.

El enrutamiento de una llamada es la operación encargada de encaminarla a través de la red hasta el punto final, seleccionando el gateway VoIP más adecuado. Este enrutamiento se lleva a cabo según unas tablas de condiciones que se programan en distintos gateways VoIP denominados Servidores de Directorio.

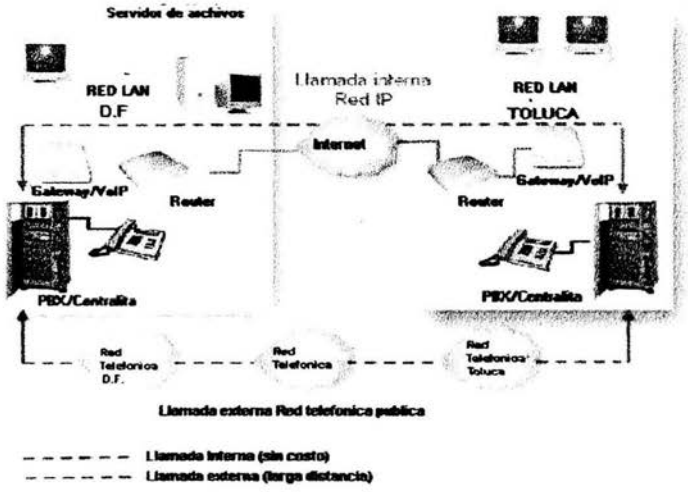
Un teléfono puede llamar a otro conectándose a un gateway VoIP (directamente, a través de central telefónica o con llamada exterior desde la calle) que digitalice y comprima la voz, estos gateways VoIP soportan varios teléfonos/conversaciones simultáneamente. En las instalaciones que necesiten más entradas y salidas simultáneas que las soportadas por un solo gateway VoIP, se puede instalar más gateways VoIP (se pueden implementar tantos como se necesiten).

La instalación de un sistema de telefonía IP requiere de un estudio personalizado de las necesidades propias de cada cliente. A continuación, se presenta ejemplos de la aplicación de esta tecnología.

4.3.2.1.- Solución para conexiones permanentes.

La empresa cuenta con 2 sucursales: una en D.F. y otra en Toluca como en la fig. 55, ambas están conectadas a Internet utilizando una línea dedicada en cada lugar. Esta conexión a Internet le permite a los usuarios de Toluca conectarse al servidor ubicado en el D.F. y hacer uso de los sistemas de gestión de la empresa. Sin embargo, la facturación telefónica correspondiente a las llamadas entre ambas sucursales es bastante alto, por lo que se plantea instalar un sistema de telefonía alternativo entre sus oficinas, para reducir dicha facturación.

Fig. 55
Conexión permanente.



Para lograr los objetivos planteados, se ha instalado en cada extremo un Gateway VoIP de 4 canales de Voz, los mismos que están conectados a la central telefónica y a la red local de cada sucursal. Con esta solución se pueden efectuar hasta 4 comunicaciones simultaneas de 2 tipos diferentes:

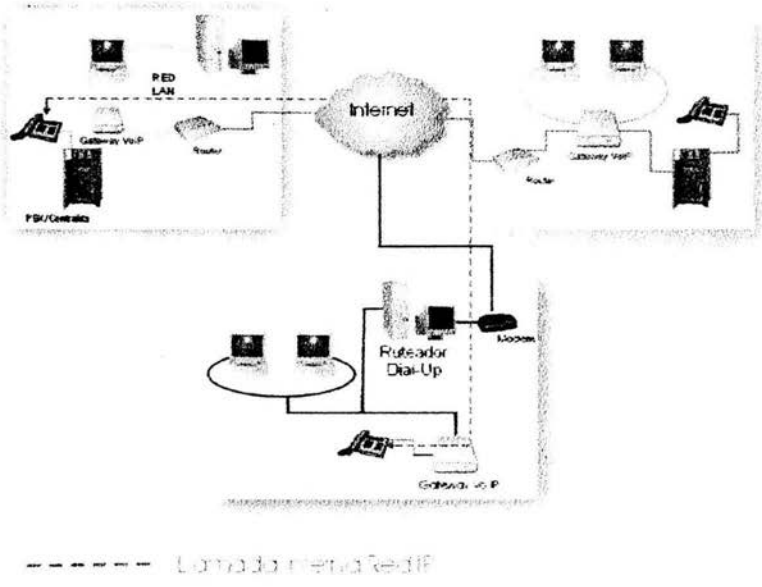
Comunicación Interna: Al estar conectadas las sucursales por redes de datos, las llamadas internas, de voz o fax, son totalmente gratuitas, excepto por el gasto fijo mensual del alquiler (que ya esta cubierto) del acceso a Internet. Por ejemplo, una llamada desde la oficina 15 del D.F. a la oficina 43 de Toluca tendría un costo nulo, independientemente de la duración de la misma.

Comunicación Externa: En este caso, la llamada irá a través de la línea de datos hasta la central de destino (costo nulo), y una vez allí saldrá a la Red Telefónica Conmutada, siendo su costo el de una llamada local. Por ejemplo, la extensión 42 en el D.F. quiere llamar al número 311564 de Toluca; la llamada pasa por la central de la sede en el D.F., luego por el gateway del D.F., llega al de Toluca y sale "a la calle" por la central de Toluca, siendo el costo total el de una llamada local y no la de una llamada de larga distancia.

4.3.2.2.- Solución para conexiones mixtas.

La empresa ha decidido abrir una nueva sucursales en Cuernavaca e integrarla a su red de telefonía IP de la fig. 56. No obstante, no requieren conectarse permanentemente a Internet hasta alcanzar un volumen de negocio que justifique ese costo.

Fig. 56
Conexión mixta.



Como la nueva sucursal de Cuernavaca cuenta con 5 estaciones de trabajo, se propone instalar un ruteador Dial-up (conexión telefónica) para conectar la red en Cuernavaca con la red en D.F. y a la vez un Gateway VoIP de un solo canal que ira conectado directamente a un teléfono. Con ello, los usuarios de Cuernavaca puedan realizar por telefonía IP llamadas "internas" a sus sucursales sin costo, y "externas" a D.F. y Toluca a costo de llamada local.

4.4.- VIDEOCONFERENCIA.

4.4.1- Introducción.

Desde la introducción del primer sistema de videoconferencia comercial en 1982 hasta nuestros días, muchas cosas han cambiado en el panorama de la videoconferencia desde el punto de vista tecnológico y de aplicación a las necesidades de los usuarios. Las primeras soluciones estaban basadas en tecnologías propietarias, y por lo tanto, que no permitían la comunicación entre sistemas de diferentes fabricantes. Por otro lado, desde aquel primer concepto de sala de videoconferencia de muy alto costo, se ha pasado a sistemas mucho más flexibles, económicos y que pueden adaptarse a las diferentes necesidades de los usuarios, según cuales sean sus aplicaciones y capacidad económica.

Actualmente se plantean continuas evoluciones y retos tecnológicos, el más importante del momento es la integración de la videoconferencia sobre las redes de datos, utilizando éstas para el transporte de la voz y del vídeo junto con los datos. Además hay que mantener la integración y comunicación con el mundo exterior a nuestra organización, que en la mayor parte de los casos será a través de RDSI.

Sólo con un diseño adecuado de las redes de videoconferencia, en función de la aplicación y de las infraestructuras de que dispongamos, se conseguirá beneficiar de inmediato de las inmensas posibilidades que brinda la videoconferencia para las empresas de hoy.

Con el objetivo de beneficiarse de la efectividad y fiabilidad del uso de la videoconferencia dentro de cualquier organización, el cliente debe considerar el sistema completo. Este incluye los equipos terminales y la red a la que se conectan dichos equipos, como un acueducto que suministra agua a una ciudad, la capacidad de una solución de videoconferencia será tan eficaz como lo sea su punto más débil. Una integración inteligente sobre diferentes medios de transporte es crucial para el éxito de la implantación de una red de videoconferencia.

Los clientes con una sensibilidad especial hacia sus redes de datos están buscando constantemente las formas de optimizar el uso de las redes existentes y de sus recursos. Esto significa a menudo la combinación de datos, vídeo y voz en una única red corporativa.

4.4.2.- Características.

Aquellos ya familiarizados con la videoconferencia tienden a pensar en los equipos de comunicación con vídeo como un sistema interactivo, bi-direccional y en tiempo real, así serán ciertamente muchas de las implantaciones H.323, pero no todas. Algunos terminales H.323 son capaces de recibir y no de enviar secuencias de vídeo, esto permite utilizar tecnologías de *streaming video* o envío de vídeo en una dirección como la fig. 57.

Fig. 57
Videoconferencia.

Los proveedores de contenidos un concepto familiar en el entorno Internet recogen secuencias de vídeo para posteriormente poder ser difundidas por enlaces IP, este modelo de espectador podría también reproducir secuencias enviadas por correo electrónico, sesiones de formación a distancia, etc.

El H.323 fue diseñado para proporcionar una solución de vídeo de calidad y a la vez mantener las capacidades de las redes públicas conmutadas. Como hemos mencionado anteriormente, muchas de las diferencias entre el H.323 y el H.320 tienen sus raíces en las diferencias inherentes entre las 2 clases de redes tratadas. Mientras muchas de las características del H.320 están centradas en los puntos terminales, el H.323 se conforma con un modelo más orientado a la red, muchas de las características de una "solución" H.323 pueden residir en servidores o en la propia red por ejemplo:

- **Multicast**
- **Servicio centralizado de directorio**
- **Funcionamiento asimétrico.**
- **Capacidades multipunto distribuidas**

Los productos H.323 tienen nuevas capacidades debido a la añadida flexibilidad de las redes de datos tomando ventaja de los entornos IP y como resultado, los usuarios se benefician de las mismas.

Con H.323, se alcanzara un crecimiento exponencial en el número de terminales empleados, el usuario va a necesitar un sistema centralizado para gestionar los equipos conectados en su red. Como los sistemas de videoconferencia forman para de la red de datos, se tendrá una enorme ventaja si se puede utilizar el mismo tipo de herramientas para gestionarlos que las que ya se utilizo con la red de datos y los equipos en ella instalados.

Una herramienta basada en el protocolo SNMP (Protocolo simple de administración de redes) es la solución ideal para gestionar una red de vídeo H.323 desde una localización centralizada, el H.323

permite utilizar la red de datos para transportar vídeo, una gestión SNMP permite utilizar la red de datos para gestionar los equipos de esa red.

Otro reto es el ancho de banda de las infraestructuras, muchas de las redes LAN están optimizadas y diseñadas para un tipo de aplicaciones: transacción de datos. Los usuarios comparten el ancho de banda dentro de una red para acceder a un servidor, a una impresora y a dispositivos de comunicaciones, los paquetes de datos se procesan de manera lineal conforme llegan.

En ocasiones el usuario experimente retardos debido a congestiones de la red, para aplicaciones de tipo transacción de datos, estos retardos introducidos por la red pueden incluso llegar a no ser perceptibles por el usuario. Y en ningún caso, dicho retardo daña irreparablemente la aplicación las aplicaciones de datos multimedia, especialmente las interactivas como la videoconferencia, no pueden aceptar dichos retardos. Por lo tanto, en estos casos será necesario adaptar las infraestructuras de LAN para soportar aplicaciones H.323.

En la parte de red de área extensa (WAN) el problema pudiera ser más importante, muchos de los enlaces WAN fueron ideados para transportar datos no en tiempo real, el H.323 demanda un incremento de la calidad de servicio (QoS) tanto en la LAN como en la WAN.

Los sistemas de videoconferencia H.323 son una de las herramientas de colaboración de más amplia difusión, permiten a los investigadores interactuar en tiempo real gracias a redes que aseguran transferencias efectivas de alta calidad. De esta forma, las videoconferencias permiten que la colaboración se realice en forma transparente entre distintos puntos del planeta

Mientras que IP es la solución elegida en la mayoría de los casos para las necesidades internas de videoconferencia, tales como comunicación entre sucursales, para establecer comunicaciones entre empresas que no tienen una relación patrimonial fuerte y para la realización de videoconferencias internacionales o en ciertas zonas específicas.

4.4.3.- Funcionamiento.

El problema central de la videoconferencia es garantizar la calidad de las imágenes y el audio que circula por la red, aunque pueden realizarse videoconferencia con señales analógicas como en los estudios de televisión, lo usual al servirse de redes de computadoras es enviar el vídeo digitalizado formando un paquete de datos.

Los paquetes deben apegarse a los protocolos como TCP/IP que garantizan la llegada, lo que produce un defase, conocido como latencia, la cual puede acarrear una perdida de sincronía entre el audio y vídeo. Para resolver este problema normalmente se trata de enviar la misma información a través de la red con menos datos, esto se logra mediante el uso de algoritmos de compresión y descompresión (Codec).

Para lograr compatibilidad entre los codecs se han desarrollado estándares para los formatos y los protocolos de transmisión (H.320, H.323, H.324), H.320 es un estándar para la transmisión de audio y vídeo a través de redes de telefonía digital, para la compresión usa el estándar H.261 que contempla 2 tamaños de imagen uno de 352 por 258 llamado Common interchange format (CIF) y el Quarter CIF (QCIF) de 176 por 144.

El estándar para la transmisión a través de redes de paquetes digitalizados como Internet es el H.324 y su estándar de asociado es el H.225 encargado de la comunicación entre la red de área local (LAN) e Internet. El estándar para la transmisión a través de líneas telefónicas analógicas es el H.324 y su estándar de compresión asociado es el H.263.

En una Videoconferencia el vídeo, audio y datos son interactivamente compartidos entre los participantes que se encuentran en diferentes lugares, debido a que el vídeo es una señal que contiene una enorme cantidad de información requiere de un canal de comunicaciones con un ancho de banda muy grande para transmitirlo de un lugar a otro, para controlar el ancho de banda del canal de comunicaciones es necesario comprimir el vídeo para que utilice un ancho de banda menor.

Esta compresión de vídeo trae consigo una degradación en la calidad del mismo ya que a mayor compresión menor calidad de vídeo, el dispositivo que realiza la compresión y descompresión es llamado Codec, es un dispositivo que también actúa como interface entre todo el equipo en la sala y la red de comunicaciones.

4.4.4.- Aplicaciones.

El audio, vídeo y los datos entran al codec el cual se encarga de transmitir una sola señal digital hacia el equipo remoto, de los cuales existen varios tipos de sistemas de videoconferencia para varias aplicaciones como son:

A. Desktop (computadora).
B. Educación a distancia.
C. Telemedicina.
D. NetMeeting.

A- Desktop.

Se basan en computadoras personales (PC) con tarjetas de expansión, una cámara, un sistema de audio y software basado en Windows, durante una llamada se puede ver la imagen en movimiento de la persona que esta en el otro extremo de la línea, se pude oír su voz y se puede compartir archivos de la PC y aplicaciones.

La mayoría de los sistemas Desktop solo trabajan con una velocidad de 128 Kbps., y algunos a 384 Kbps., actualmente están surgiendo nuevos estándares que permiten realizar estas aplicaciones utilizando una línea telefónica conmutada y un módem; la compresión realizada en estos sistemas es muy severa y ello repercute en que para muchas aplicaciones no cubre los requisitos.

B- Educación a distancia y Telemedicina.

Estos sistemas especializados pueden ser fácilmente acomodados con el diseño propio y con periféricos adicionales como reproductores de 35 mm. , toda clase de gráficas basadas en computadora, cámaras adicionales, monitores, fuentes de vídeo, videograbadora y pizarrones electrónicos.

D- NetMeeting.

Permite utilizando un PC con conexión a una Intranet local o Internet, comunicarse con otras personas sin gastar demasiado, también chatear, compartir muchas aplicaciones en Windows, intercambiar información gráfica en una pizarra electrónica, transferir archivos y controlar remotamente otro PC de la fig. 58.

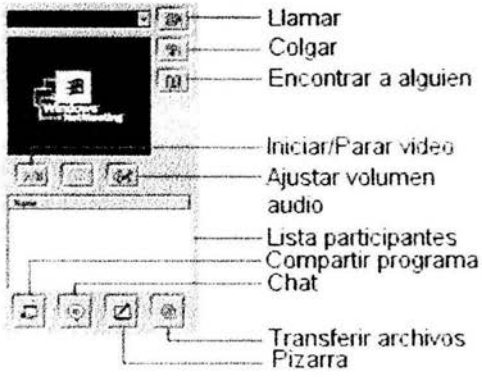
Con NetMeeting puede participar en conferencias, colaborar en el trabajo con un archivo mediante las características de NetMeeting y compartir información a través de Internet o de la intranet corporativa, permite realizar llamadas mediante servidores de directorio, servidores de conferencia y páginas Web. Facilita la realización de llamadas en Internet, la intranet de la organización y mediante teléfonos; al compartir programas, podrá trabajar fácilmente con otros participantes en la conferencia.

Con la característica conversación puede hablar con varias personas, además es posible codificar las llamadas de conversación, lo que garantiza la privacidad de las conferencias.

Entre las posibilidades destacan las siguientes:

- Conferencias de Audio y Vídeo: Se habla y se ve a cualquier persona en Internet.
- Pizarra: Permite intercambiar información gráfica con otras personas.
- Chat: Además de audio, se puede mantener conversaciones utilizando texto, opcionalmente cuando la calidad de la conexión no es buena y el audio/vídeo es deficiente.
- Directorio Internet: El Directorio Internet de Microsoft es un sitio Web mantenido por Microsoft en el se puede localizar a otras personas y llamarlas utilizando NetMeeting.
- Transferencia de Ficheros (FTP): Permite enviar ficheros mientras se realiza una conferencia de audio/vídeo.
- Compartir Aplicaciones: Se comparte múltiples aplicaciones mientras se realiza una conferencia, manteniendo siempre el control sobre el uso de dichas aplicaciones.
- Compartir Escritorio: Se controla remotamente otra PC.
- Seguridad: NetMeeting utiliza 3 tipos seguridad para proteger la privacidad.

Fig. 58
Ventana de netmeeting.



4.4.5.- Beneficios de transmitir una videoconferencia sobre IP.

La transmisión IP es más económica, debido a que se paga una renta plana independientemente del uso. Sin embargo, más importante es la consecuencia de este modelo de costos, ya que mediante este sistema de transmisión no hay frenos al uso intensivo de esta herramienta. Cuando cada minuto cuesta, como en el caso de ISDN, solamente los altos ejecutivos están autorizados para ocupar videoconferencia.

Por el contrario, la transmisión IP permite que ésta sea una herramienta cada vez más utilizada para nuevas actividades y aplicaciones, de esta manera, los enormes y comprobados beneficios de la videoconferencia se pueden aplicar a todas las áreas de la empresa, multiplicando la eficiencia y los ahorros. En conclusión, solamente la transmisión IP permite realmente considerar una masificación del uso de la videoconferencia.

Destacándose la posibilidad de integrar todas las aplicaciones de productividad de la empresa es otro de los beneficios directos de la videoconferencia sobre IP, en este sentido, cabe mencionar que la videoconferencia no es un fin en sí, sino una herramienta más dentro de todas las existentes en el mercado de las Tecnologías de Información y gracias a la transmisión IP, se puede combinar de manera eficiente con herramientas tales como e-mail, streaming, mensajería instantánea, bases de datos y sistemas de información, permitiendo la complementariedad y convergencia entre diferentes aplicaciones, con el propósito de lograr trabajar en forma colaborativa.

4.5.- IP MÓVIL.

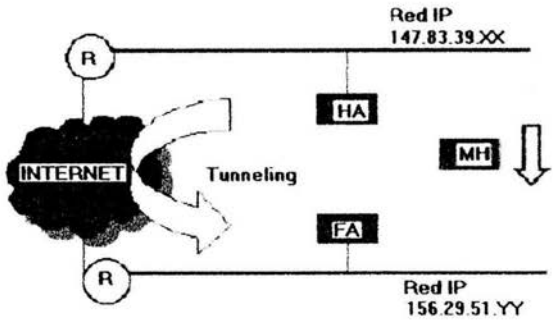
En los últimos años se han logrado números progresos en el campo de las tecnologías de comunicación, se concentran en 2 avances relevantes que son el creciente desarrollo de la informática portátil y la importante implantación de los sistemas de comunicación móviles.

Sin embargo, los protocolos actuales de internetworking (TCP/IP, IPX o AppleTalk) presentan serias complicaciones a la hora de tratar con nodos que presentan cierto grado de movilidad, la mayoría de las variantes del protocolo IP asumen de manera implícita que el punto al cual se esta conectando un nodo es fijo. Por otro lado la dirección IP de un nodo lo identifica de manera unívoca en la red en la que se encuentre conectado, luego cualquier paquete que vaya destinado hacia ese nodo es encaminado en función de la información contenida en la IP del mismo que identifica la red en que esta conectado.

4.5.1.- Características.

Un nodo móvil se desplaza de una red a otra manteniendo su dirección IP, no será localizable en su nueva situación ya que los paquetes dirigidos hacia ese nodo serán encaminados a su anterior punto de conexión. Mediante IP Móvil de la fig. 59 se pretende dotar al nodo de cierta libertad para moverse libremente a través de Internet, estando siempre accesible mediante una dirección IP.

Fig. 59
Arquitectura Móvil IP (IETF).



MH- Nodo móvil.
HA- Agente Local.
FA- Agente externo.

Existe un agente local y otro externo, los cuales colaboran para permitir que el nodo móvil pueda moverse conservando su IP. Muchos usuarios de Internet tienen pc's portátiles (laptops) y quieren mantenerse conectados al visitar una instalación lejana, e incluso de camino hacia ella.

El problema reside en el propio direccionamiento, cada dirección IP contiene 3 tipos de información: la clase, él numero de red y él numero de host. Por ejemplo, si consideramos la dirección IP 160.80.40.20. El 160.80 da la clase B, él numero de red es 8272 y él numero de host 10260 (40.20).

Los enrutadores tienen información en sus tablas que indican la línea que corresponde a la red 160.80., cuando llega un paquete con su dirección IP de destino de la forma 160.80.xxx.yyy, sale por esa línea. Si cambiamos esa maquina a un lugar lejano, los paquetes se continuaran enviando a su LAN (o enrutador) base, el propietario ya no podrá utilizar ciertas aplicaciones como puede ser simplemente su correo electrónico.

Dar otra dirección IP para asociarla a su nueva ubicación no parece muy interesante, ya que se tendría que informar a mucha gente, programas y base de datos sobre el cambio. Otro enfoque es hacer que los enrutadores usen por completo la dirección IP en lugar de solo la clase y la red. Esta estrategia es inviable, ya cada enrutador tendría millones de entradas, lo que produciría un gran costo.

El IETF (Grupo de trabajo en ingeniería de Internet) estableció un grupo de trabajo para llegar a la solución, concretando varias metas consideradas deseables.

Las principales metas son las siguientes:
1. Todo host móvil debe ser capaz de usar su dirección IP base en cualquier lugar.
2. No se permiten cambios software en los host fijos.
3. No se permiten cambios software del enrutador ni a sus tablas.
4. La mayoría de los paquetes para los host móviles no deben desviarse en el camino.
5. No se debe incidir en carga extra cuando un host móvil este en su base.

En síntesis, la solución escogida consiste en que cada instalación que quiera permitir movilidad a sus usuarios deben crear un agente base, cada instalación que permita visitantes debe crear un agente externo al llegar un host móvil a una instalación externa, se pone en contacto con el host externo y se registra. Entonces el host externo se comunica con el host base del usuario y le da la dirección de encargo (care-off address), normalmente la misma dirección IP que el agente externo.

Al llegar un paquete a la LAN base del usuario, llega a través del enrutador conectado a la LAN, el enrutador entonces trata de localizar el host de la manera normal difundiendo un paquete ARP (Protocolo de resolución de direcciones) que pregunte por ejemplo: ¿Cuál es la dirección Ethernet 160.80.40.20 ?, el agente base responde a esta solicitud dando su propia dirección Ethernet.

El enrutador entonces envía el paquete para 160.80.40.20 al agente base, este a su vez lo envía en túnel a la dirección de encargado, encapsulándolo en el campo de carga útil de un paquete IP dirigido a un agente externo. El agente externo lo desencapsula y lo entrega a la dirección de enlace de datos del host móvil, además el agente externo entrega la dirección de encargo al transmisor, para que los paquetes futuros puedan enviarse en túnel directamente al agente externo.

Hay que tener en cuenta un detalle, en el momento de moverse un host móvil, el enrutador tiene en cache sus direcciones Ethernet (que pronto dejaran de ser validas), para reemplazar esa dirección Ethernet por la dirección del agente base, se usa un truco llamado ARP gratuito. Este es un mensaje especial al enrutador, no solicitado, que causa que reemplace una entrada especifica de la cache, en este caso la del host móvil apunto de irse. Al regresar el host móvil después, se usa el mismo truco para actualizar la cache del enrutador.

El diseño no nos impide que un host móvil pueda ser su propio agente externo, pero este enfoque solo seria viable si el host móvil (en su función como agente externo) esta conectado lógicamente a Internet en su instalación actual. También debe adquirir una dirección IP de encargado (temporal) para usarla, esta dirección debe pertenecer a la LAN a la que esta conectado actualmente, la solución de IETF para host móviles resuelve otros problemas no mencionados anteriormente.

En este nuevo protocolo nos encontramos con 3 nuevas entidades:
- El nodo móvil.
- El agente local.
- El agente externo.

4.5.2.- Funcionamiento.

Como cualquier otro protocolo éste consta de una serie de operaciones o etapas que pasamos a enumerar a continuación y que posteriormente serán explicadas:

- En primer lugar tanto el agente local como el agente externo anuncian su presencia al nodo móvil a través de los *mensajes de anuncio*, que son generados de manera periódica por la red. En ocasiones es el propio nodo móvil el que puede solicitar estos mensajes mediante el envío de una solicitud de agente.
- En segundo lugar el nodo móvil una vez recibido el mensaje de anuncio determina su posición comprobando si se encuentra en su red local o si por el contrario se encuentra en una red externa. En el primero de los casos el nodo actuará sin necesidad de las funciones de apoyo a la movilidad. En el segundo de los casos el nodo debe obtener una dirección especial denominada *dirección de*

cuidado de la nueva red. La obtención de esta dirección de cuidado se puede realizar de dos maneras distintas:

- La dirección del agente externo.
- Si se encuentra fuera del alcance de un agente externo, debe obtener esta dirección como una dirección IP local por algún método. Una de las posibilidades seria a través del DHCP (Protocolo de configuración dinámica de direcciones). En este tipo de casos a esta dirección de cuidado se la denomina *dirección de cuidado colocada.*
- Una vez obtenida esta dirección de cuidado, el nodo móvil debe registrarla con su agente local. Para ello el nodo envía una solicitud de registro al agente local y éste le envía un mensaje de contestación.
- Cualquier paquete que le sea enviado al nodo móvil va a ser interceptado por el agente local, el cual lo enviará mediante un procedimiento denominado *tunneling* a la dirección de cuidado. En el otro extremo del túnel el agente externo será el que reciba el paquete y el encargado de enviárselo al nodo móvil. Si el nodo móvil posee una dirección de cuidado colocada el agente externo no interviene en la recepción del paquete.
- Para aquellos paquetes que sean originados en el nodo móvil no tienen que pasar necesariamente por el agente local sino que pueden ser transportados hasta la dirección IP.

4.5.2.2.- Procedimientos.

Descubrimiento del agente.

Es un procedimiento por el que el nodo móvil determina si se encuentra en su red local o si por el contrario y debido a su movimiento se encuentra en una red externa, asimismo se utiliza para obtener la dirección de cuidado necesaria para el nodo móvil. Este procedimiento es sencillo y utiliza dos tipos de mensajes mencionados anteriormente: el anuncio de agente y de solicitud de agente.

1. Anuncio de agente.

Se necesitara un anuncio por parte del agente local o bien por parte del agente externo de la disponibilidad para aceptar un nodo móvil en su red, el agente local deberá estar siempre dispuesto para servir a sus nodos móviles. Para evitar posible saturaciones que le impidan cumplir con su compromiso se permite una configuración de un agente local a una determinada población de agentes móviles.

Puede ocurrir que un agente externo no pueda servir a un nodo móvil que no pertenece a su red, a pesar de ello el agente externo no puede parar de emitir los mensajes para que el nodo móvil identifique que se encuentra dentro de su red de cobertura. Este mensaje de anuncio consiste en un mensaje ICMP (Protocolo de mensajes de control de Internet) el cual ha sido extendido para permitir abarcar esta nueva funcionalidad.

2. Solicitud de agente.

Estos mensajes son los que envía el nodo móvil bien cuando no recibe ningún mensaje de anuncio de agente o bien porque no puede esperar a su envío debido al cambio de enlace en un breve espacio de

tiempo. Este mensaje por lo tanto lo que hace es forzar un mensaje de anuncio para cualquier agente que se encuentre situado en su mismo enlace.

Registro.

Las razones por las cuales un nodo móvil debe registrarse son las siguientes:

- Su punto de conexión a Internet ha variado respecto al que tenia anteriormente.
- Su registro esta a punto de caducarse.
- Si se encuentra en una red extensa y detecta que su nodo externo se ha reiniciado.

Lo que se persigue con el registro es pedir al agente externo que nos proporcione sus servicios, una vez hecho esto el nodo móvil informa a su agente local de su dirección de cuidado en la red. Si el nodo regresa a su red local debe iniciar un proceso en el cual se debe des-registrar con su nodo local para que a partir de ahora y hasta un nuevo cambio pueda actuar como un nodo fijo.

El proceso de registro esta formado por 3 pasos:

- El nodo móvil envía una petición de registro.
- El agente recibe la petición de registro y envía al nodo móvil un mensaje de contestación para indicarle si su petición ha sido o no registrada.
- Si el nodo no recibe la contestación en un periodo más o menos corto de tiempo volverá a retransmitir la petición pero cada vez en intervalos más largos de tiempo hasta que consiga recibir la contestación. Para ello es necesario la cooperación ente los agentes locales y externos para que intercambien mensajes de petición de registro.

1. Petición de registro.

El nodo móvil se registra con su agente local mediante el envío de este mensaje, el agente local modificará o creará nuevas entradas a la lista que mantiene con todos los nodos con movilidad.

2. Respuesta del registro.

Es necesario que el nodo móvil reciba una respuesta del registro por parte del agente local, esta respuesta puede llegar de dos maneras diferentes:

- Si el servicio se solicita a través de un agente externo, será éste el que reciba la contestación de registro y a continuación se la envía al nodo móvil.
- Si por el contrario el nodo móvil utiliza una dirección de cuidado colocada será el mismo el que reciba dicha respuesta.

En este mensaje no solo se le informa al nodo móvil el resultado de su petición de registro sino que también se le informa del tiempo de vida de dicho registro, que puede tener una duración diferente de la pedida por el nodo móvil (igual o inferior), el agente externo no puede modificar este tiempo de vida.

Encaminamiento.

Se distinguen 2 opciones:
- El nodo se encuentra conectado a su red local.
- El nodo se encuentra en una red externa.

En el primero de los casos presentados el nodo se comportaría como si fuera un nodo fijo por lo que las normas para el encaminamiento son las mismas que se mencionan en el encaminamiento de paquetes IP hacia cualquier nodo convencional.

En el segundo de los casos se distinguen 2 situaciones:
- El destino es un nodo móvil
- El origen es un nodo móvil.

Nodo Móvil en destino.

El protocolo IP móvil necesita que los paquetes que se envían desde una red local hasta un nodo móvil sean encapsulados, lo que modifica en encaminamiento tradicional ya que se necesita un nodo intermedio antes de llegar al destino. Este nodo intermedio será el encargado de desencapsular el paquete y enviar el paquete original al destinatario final.

Para el envío de un paquete se necesitan una serie de operaciones o pasos que son a continuación:
- Un router de la red local (generalmente es el agente local) anuncia que existe conexión hasta el prefijo de red equivalente al de la dirección local del nodo móvil, es decir, todo paquete que vaya destinado al nodo móvil será encaminado hacia su red local y recibido por su agente local.
- El agente local toma el paquete y consulta su entrada en la lista que mantiene de movilidad para obtener las direcciones de cuidados que tiene registradas.
- El agente local envía una copia del paquete, encapsulándolo, hacia cada dirección de cuidado a través de túneles, mediante un proceso que se denomina tunneling.

En cada dirección de cuidado se extrae el paquete original y se le entrega al nodo móvil, si se trata de una dirección de cuidado de un agente externo, es éste el encargado de deshacer el encapsulamiento del paquete. Posteriormente consulta el campo de dirección IP de destino para comprobar si coincide con alguno de los nodos móviles a los que está prestando servicio, si hay coincidencia el agente envía el paquete al nodo.

Si la dirección de cuidado es una dirección de cuidado colocada, el nodo no recibe ningún servicio por parte de ningún agente externo y por lo tanto será él el que se encargue de llevar a cabo las tareas de desencapsulamiento.

Nodo Móvil en origen.

Tanto si el nodo móvil depende de un agente externo como si no existen 2 alternativas a la hora de determinar un router adecuado para dar salida a los paquetes, en el caso de dependencia de un agente externo puede ocurrir:
- El router puede ser el propio agente externo.

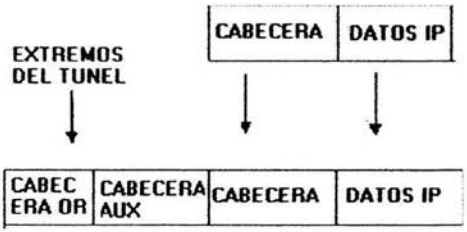
- El router puede ser cualquiera cuya dirección IP aparezca en los campos de Router Address del mensaje de anuncio, siempre y cuando el nodo móvil sea capaz de determinar la dirección de la capa de enlace del router deseado sin tener que enviar peticiones ARP.

En el caso de poseer una dirección de cuidado colocada se tiene:
- Elegir algún router que esté enviando mensajes de anuncio de router (no confundir con los mensajes de anuncio de agente).
- Obtener la dirección del router de la misma manera que se obtuvo la dirección de cuidado colocada, en nuestro caso a través del DHCP.

Tunneling (Encapsulamiento).

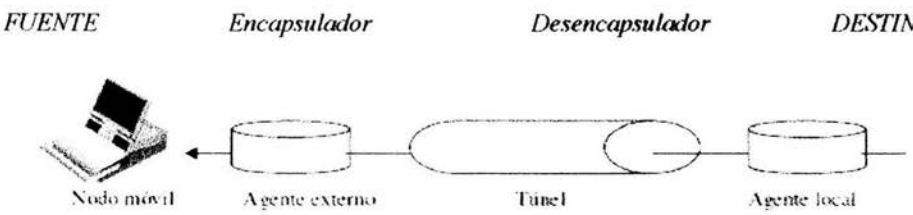
Los paquetes son encapsulados de manera que se modifica el enrutamiento habitual, siendo entregado a destinatarios intermedios distintos de los que vienen indicados en el campo de dirección de destino de la cabecera de original IP de la fig. 60.

Fig. 60
Encapsulamiento.



Una vez que el datagrama encapsulado llega a estos nodos intermedios se desencapsula lo que da lugar al datagrama original IP, este datagrama es el que será entregado al destino que viene indicado en el campo de la cabecera mencionado anteriormente. Es a este proceso de encapsular y desencapsular lo que se conoce como tunneling.

El esquema general de este proceso se puede resumir de la siguiente manera:



El punto de entrada al túnel seria el nodo encapsulador y el punto de salida del túnel seria el nodo desencapsulador, el mismo túnel puede ser utilizado por muchos pares fuente-destino. Actualmente las técnicas de encapsulado IP son útiles para realizar transmisiones multicast e incluso llevar a cabo operaciones de seguridad y privacidad en Internet.

Las desventajas que ofrece esta técnica son:
- Los datagramas encapsulados son generalmente más largos que los datagramas originarios.
- La encapsulación no se puede llevar a cabo a no ser que el nodo de la salida del túnel sea capaz de desencapsular el datagrama.

Existen distintas técnicas de encapsulado:
- Encapsulado IP-in-IP.
- Encapsulado IP-mínimo.
- Encapsulado GRE.

Seguridad.

Las redes y nodos móviles son particularmente propensos a recibir ataques que comprometan su seguridad, la mayor parte de las veces los nodos móviles se conectaran a Internet a través de redes inalámbricas. Este tipo de conexiones son particularmente vulnerables a escuchas silenciosas, ataques activos de respuesta y otros tipos de ataques activos es por esta razón por la cual hay que tener un especial cuidado en el tema de la seguridad.

Durante el proceso de registro de un nodo móvil, el agente local debe estar seguro de que la petición que está recibiendo es una petición de un nodo móvil verdadero y no de uno falso, el Protocolo IP móvil intenta solucionar este problema mediante la especificación de una asociación de seguridad entre el host local y el nodo móvil, cuya configuración es manual. Se utiliza un índice de seguridad que se incluye en todos los mensajes que el nodo móvil envía al agente local.

Este índice está formado por un numero que indica el algoritmo utilizado en la codificación del mensaje y un secreto que solo los dos conocen, este secreto puede ser o bien un acuerdo por ambas partes para el intercambio de una llave o bien el agente local manda al nodo móvil un dato que espera que le sea devuelto pasado un determinado periodo de tiempo.

Los usuarios que tengan datos privados que no desea que sean observados por nadie más deben usar mecanismo de seguridad (encriptación) ajenos al protocolo de IP Móvil y que, por lo tanto, no están especificados. En las peticiones de registro existe un campo que permite al agente local determinar si dicha petición se ha realizado recientemente y por lo tanto que no es una petición que ya ha sido escuchada y se produzca un duplicado. Para ello existen dos algoritmos:

- timestamp.
- nonces.

Todos los agentes locales deben implementar esta protección contra duplicados basados en marcas de tiempo.

Aplicaciones.

- Un avión con un router IP Móvil con la funcionalidad de las redes móviles, puede volar por todo el mundo con todos los pasajeros conectados continuamente a Internet. Los pasajeros conectan asistentes personales digitales (PDA) o sus teléfonos celulares al router en el avión utilizando las tecnologías tradicionales LAN, como Ethernet o 802.11b. No se requieren dispositivos especiales de movilidad en la medida en que la red es la que permite la movilidad.
- Ambulancias que necesitan viajar grandes distancias y que cuentan con una red móvil a bordo, podrán intercambiar información de diagnóstico y ofrecer tratamiento inmediato a pacientes.
- Naves guardacostas podrán mantener la conectividad con sus estaciones de tierra mientras patrullan los mares.

4.5.3.- SOLUCIONES PARA PROPORCIONAR MOVILIDAD A LAS ESTACIONES DE REDES IP.

Para dotar de movilidad a un nodo de la red, hay varias alternativas que se van a tratar: establecimiento de rutas especificas para terminales con movilidad, cambio de la dirección IP de los terminales y soluciones basadas en realizar cambios a nivel de la capa de enlace.

1. Creación de rutas especificas para nodos con movilidad.

La utilización de rutas especificas para los nodos a los cuales se quiere dotar de movilidad implica la reconfiguracion de las tablas de encaminamiento de los dispositivos de interconexión de red o enrutadores para permitir contactar con el host móvil en su nueva ubicación.

Esta solución es costosa ya que generaría un gran incremento de trafico en la red para soportar la movilidad de los nodos, ya que para ello seria necesario actualizar las tablas de encaminamiento como mínimo de todos los routers entre el enlace local y el nuevo punto de enlace. Si tenemos en cuenta él numero de posibles nodos móviles en una red y la velocidad con la que estos cambian de ubicación, estas actualizaciones de las tablas de encaminamiento podrían llegar a colapsar la red. De lo que se deduce que cuantas menos actualizaciones hagamos en los routers mejor pero en contra nos encontramos con que se limita las posibilidades de encaminamiento.

2. Cambio de direcciones IP.

Consiste en asignar al nodo móvil una nueva dirección IP acorde con su nuevo punto de conexión a la red, esta solución no es muy recomendable ya que requiere que a la entrada en una nueva ubicación cambie su dirección IP. Si esta operación no se realiza de manera instantánea, cualquier consulta de la dirección IP del nodo puede ser errónea.

La velocidad con la que un nodo móvil puede cambiar su ubicación y por lo tanto su IP, se hará necesario un mecanismo para verificar la actualidad de la dirección IP devuelta por el servidor de nombres de dominio (DNS). El resultado es un gran numero de consultas actualizaciones que generan un alto nivel de trafico en la red.

3. Soluciones a nivel de la capa de enlace.

Las 2 soluciones a nivel de la capa de enlace que pretenden permitir la movilidad de los nodos, la primera de ellas se basa en el CDPD (Cellular Digital Packet Data), que se trata de un estándar diseñado para transmitir paquetes IP a través de los canales de radio no utilizados por el servicio de voz en el sistema de telefonía celular norteamericano.

El CDPD asigna a cada nodo móvil una dirección fija dentro de su área de cobertura, la segunda solución se basa en el estándar de IEEE 802.11, realizado por el IEEE (Instituto de ingenieros eléctricos y electrónicos) para la comunicación de redes de área local inalámbricas.

Ambas soluciones presentan 2 inconvenientes. Por un lado las soluciones a nivel de capa de enlace proporcionan movilidad para un solo tipo de medio físico, por lo que habría que buscar una solución para cada de ellos. Y por otro lado la movilidad con estas soluciones se encuentra mas o menos limitada geográficamente. El protocolo IP móvil es el único capaz de proporcionar movilidad en cualquier tipo de medio y en una extensión geográfica.

4.6.- PROBLEMAS DE CONFIGURACION DE LA VOZ SOBRE IP.

Las cuestiones de señalización, calidad de servicios (QoS) y arquitectura son los fundamentos básicos del despliegue de Voz sobre IP (VoIP).

4.6.1.- Consideraciones del plan de marcación.

Un plan de marcación es el método por el cual se asigna un numero de teléfono individual o por bloques a las líneas o ctos. físicos, en las Redes publicas de telefonía conmutada (PSTN) los planes de marcación se crean partiendo bloques de números de manera jerárquica (10,000 números). Para crear un plan de marcación para una red de voz empresarial también se asignan números de teléfono individuales.

La PSTN utiliza una jerarquía especifica, la recomendación E164 de la ITU-T sanciona las especificaciones de las llamadas entre países, la North american numbering plan (NANP) construida sobre la recomendación ITU-T especifica cuantos dígitos se pueden utilizar y para que se pueden utilizar. También se pueden desplegar sistemas VoIP utilizando esta propuesta jerárquica, los gatekeepers H.323 pueden formar una malla jerárquica de zonas locales, regionales, nacionales e internacionales, estas zonas proporcionan una ruta determinista para la señalización de llamada aunque la voz real tome la mejor ruta.

4.6.2.- Problemas del plan de marcación.

Los administradores de las redes empresariales de voz privadas suelen tener problemas en el plan de marcación cuando lanzan uno para toda la empresa que abarca varios sitios remotos, esta topología los administradores de la red deben decidirse por un numero de dígitos utilizable en el plan de marcación y estar seguros de que los números no se superponen.

Para el administrador de la red la transparencia de las funciones o la posibilidad de utilizar las mismas funciones en múltiples intercambios privados de ramas (PBX) y en todas las ubicaciones; para algunas corporaciones con miles de sitios los primeros 3 o 4 dígitos representan él numero del almacén y el resto de los dígitos (1 o 2) representa cada extensión, las grandes corporaciones con miles de sitios remotos utilizan solo unas pocas extensiones.

En determinadas circunstancias las empresas con varias sucursales remotas deben asignar una gran cantidad de dígitos para satisfacer las necesidades de todos los posibles usuarios, dichas empresas simplifican su plan de marcación implementando un procedimiento de marcación de 2 fases.

Con la marcación de 2 fases el que llama puede marcar un código de acceso (similar a utilizar una tarjeta de llamada) que lo enruta hacia un lugar especifico en la red, la persona que recibe un segundo tono de marcado en cuyo momento puede marcar él numero real al que quiere llamar.

La marcación en 2 fases ofrece 2 ventajas principales: el plan de marcación del PBX remoto puede ser sencillo y la red no necesita tener un plan de marcación que englobe el plan de marcación de la totalidad de la red, en su lugar la red utiliza en grupo de códigos de acceso que se corresponden con puntos de switching remotos.

Las limitaciones de esta marcación es que los usuarios deben seguir un procedimiento de 2 fases y que deben esperar hasta que la red les pida de manera apropiada entradas adicionales, a pesar de estas limitaciones las redes empresariales privadas implementan la marcación en 2 fases por 3 razones:

1- Si han crecido rápidamente.
2- Si se han fusionado con otra corporación.
3- Si han adquirido otra corporación que utilizaba otro tipo de tecnología PBX.

Utilizar un plan de marcación de una única fase (plan de conversión) requiere generalmente que los usuarios no cambien sus hábitos de marcado, si la compañía no tenia una arquitectura de plan de marcación en el pasado imponer una arquitectura VoIP puede introducir algunos retos, como la posibilidad de superposición de numero o la carencia de funciones de enrutamiento de llamadas.

VoIP soporta la marcación en 2 fases, pero cuando se utilizan este plan se debe tener mucho cuidado por las siguientes razones:

- Se pueden perder los tonos de marcación multifrecuencia (DTMF) conforme recorren la red IP si se utiliza una codificación inapropiada, codificar un flujo de voz transportado sobre RTP (Protocolo de Tiempo Real) y a través de métodos alternativos, dentro de una ruta de señalización (H.245) permite el transporte de entrada DTMF en la red.
- Puede darse la codificación tandem (compresión dual) que reduce la calidad de la llamada, debido a una pobre planificación de la red.
- Pueden darse las conversiones múltiples digital a analógico (D/A), lo que también reduce la calidad de la llamada.

Es muy común la perdida de paquetes cuando se utiliza una red IP, sin embargo si el tono DTMF es transportado en flujo UDP (Protocolo de Datagrama de usuario) se puede perder el paquete o el tono, o ser estos ordenados inadecuadamente lo que causa que se marque una secuencia errónea de dígitos, si el proveedor VoIP utiliza un repetidor DTMF que permite que los tonos DTMF sean transportados en TCP, el transporte del DTMF es tan fiable como la PSTN.

Sin embargo, si ninguna entidad controla la red de datos y voz, es posible tener en la marcación de fase única o de 2 fases ciclos de compresión múltiple lo que afecta a la calidad de voz; la conversiones D/A múltiples también pueden afectar a la calidad de voz, donde las conversiones D/A levantan realmente la cabeza es cuando se manejan modems o alguna otra transmisión de datos sobre voz.

4.7.- Transparencia de la función.

Conmutar desde redes de voz de multiplexión por división de tiempo (TDM) a soluciones de voz basadas en paquetes requiere también que el cliente se mueva y soporte las aplicaciones y funcionalidad existentes de manera similar; muchos PBX tienen métodos de señalización registrados por lo que no pueden cambiar a IP, esto dificulta tener una red VoIP rentable que ofrezca funciones limitadas.

La razón por las que las redes VoIP son difíciles de debe a la naturaleza propietaria de los protocolos de señalización entre PBX, estos métodos de señalización propietarios no pueden ser transportados por una red VoIP; en un intento de proporcionar alguna interoperabilidad entre PBX y los fabricantes que utilizan la señalización digital se ha desarrollado el estándar Q.Sig de la ETSI (Instituto Europeo de normas de telecomunicación).

Este estándar se basa en la pila de señalización Q.931 pero contiene extensiones que permiten que la información de señalización adicional sea pasada entre los PBX, Q.Sig es un protocolo basado en estándares que permiten que diferentes tipos de PBX, así como diferentes redes puedan interactuar.

4.7.1.- Transparencia de las funciones en la PSTN.

Se basan principalmente en el sistema de señalización 7 (SS7) y las aplicaciones construidas sobre el mismo, para transportar y tunelear de manera transparente funciones por múltiples redes, es SS7 debe ser soportado como la interfaz de línea de base obligatoria. El conjunto del protocolo H.323 se desarrollo asumiendo las interfaces Q.931 (RDSI) en los gateways de voz.

El conjunto del protocolo no tiene un mecanismo transparente para transportar y tunelear mensajes SS7, incluidos los protocolos basados en la red inteligente (IN).

CONCLUSIONES.

Con esta nueva tecnología de la información (TI) de "Voz sobre IP" (VoIP), sé beneficiaria las telecomunicaciones en la vida diaria dentro del hogar, hospitales, universidades y empresas en cualquier parte del mundo por su uso, funcionamiento y bajos costos requeridos.

Ya que el Internet se tiene un acceso en la mayor parte del mundo y cada vez hay mas computadoras y teléfonos (fijos y móviles) para su uso, esta tecnología es cada vez más accesible para todos ya que cada una de las empresas, hospitales, hogares y universidades necesitan de una de red para estar comunicados con el mundo, así como la integración de las redes de voz y datos en una sola para que la información viaje sobre los cables de cobre o fibra óptica, o por medio del aire esto es inalambricamente, y cada empleado o persona tenga su teléfono IP o computadora para comunicarse a cualquier parte a un precio muy bajo por medio de la red mundial de Internet.

Por esto sea considerado un gran adelanto en las telecomunicaciones, esto se debe a que el Protocolo de Internet (IP) es la base de las redes tipo LAN y WAN usadas en todo el mundo, y la facilidad de uso de este tipo de protocolo que se puede usar en cualquier plataforma o red.

Además del uso de la conmutación de paquetes que se maneja para mandar y recibir la información que viaja de un lado a otro ahorrando con esto un gran ancho de banda y tiempo, y complementándose con el modelo OSI que divide la información que manda y recibe en 7 capas o procesos junto con los protocolos como IP/TCP; ya que con el estándar H.323 se beneficia esta tecnología de VoIP para el manejo de videoconferencias con el audio, datos y video. Integrándose con el H.323 y demás elementos relacionados como las terminales, Gateway, Gatekeeper, y unidades de control multipunto tiene la ventaja de los estándares que son compatibles con los elementos y los medios como el audio, video y datos que sean aplicables y de uso con las computadoras para las personas involucradas en una videoconferencia.

Esto se ayuda del Protocolo de inicio de sesión (SIP) para su uso en sesiones multimedia que incluyen audio, video y datos en Internet como conferencias y telefonía, ya que el SIP se establecen, se mantienen y terminan las sesiones en donde sean utilizadas. Ya que sus usos y aplicaciones de IP son muy diversos como la telefonía, la videoconferencia, la movilidad, el fax y los conmutadores todo esto beneficiara al usuario final para cualquier aplicación requerida hoy y en futuro, y que será aplicable en las telecomunicaciones en todo el mundo y en la vida diaria. Por lo tanto, el uso y las aplicaciones de Voz sobre IP pueden ser utilizadas en hogares, hospitales, universidades y empresas para la integración de datos, audio y video.

GLOSARIO.

A

- **ADPCM (Modulación por codificación de impulsos diferencial adaptativa):** Forma de codificar el sonido de forma que ocupe menos espacio, asociada con la comunicación de voz digitalizada.
- **Ancho de banda (bandwidth)**: Determina el volumen de información que puede circular por un medio físico de comunicación de datos, a mayor ancho de banda mejor velocidad de acceso y se mide en Hz. o bps (bits por seg.).
- **Atenuación**: Disminución en la magnitud de una señal.
- **Amplitud:** Se refiere al tamaño de una señal analógica.
- **ATM (Modo de transferencia asíncrona):** Estándar CCITT para retransmisión de celdas en la cual la información para diferentes tipos de servicios se transmite en pequeñas celdas de tamaño fijo.
- **ARP (Protocolo de resolución de direcciones):** Protocolo de Internet utilizado para asignar una dirección IP a una dirección MAC.
- **ACK (Acuse de recibo):** Notificación enviada por un dispositivo de red a otro para confirmar que se produjo un determinado evento.
- **Agente:** Software que procesa consultas y devuelve respuestas en nombre de una aplicación.
- **Algoritmo:** Proceso definido para obtener la solución de un problema.
- **ANSI (Instituto nacional americano de normalización):** Organización compuesta por empresas, organismos del gobierno y otros miembros que coordina las actividades relacionadas con los estándares.
- **Aplicación:** programa que realiza una función directamente para un usuario (los clientes FTP y telnet).
- **Analógica:** Cualquier dispositivo o señal física que varia continuamente en intensidad o cantidad sobre un intervalo infinito de voltajes o corrientes.

B

- **Bits**: Palabra que significa símbolos o dígitos binarios; proviene de ***binary digits***; es también una medida de la cantidad de información contenida en un mensaje, definida por C. E. Shannon.
- **Banda base:** Transmisión de la señal sin utilizar una señal de portadora, usando la banda de frecuencia original.
- **Baudio:** Unidad de velocidad de señalización igual al numero de elementos de señal discontinua que se transmite por segundo.
- **Byte:** Serie de dígitos binarios consecutivos sobre los cuales se opera como una unidad (byte de 8 bits).
- **Bridge (puente):** Elemento que permite enlazar redes de igual naturaleza y cuya función es gestionar el tráfico de mensajes entre ambas.
- **Banda ancha:** Técnica de transmisión de alta velocidad y capacidad que permite la transmisión.
- **Buffer**: Espacio de almacenaje temporal.
- **Backbone:** Parte de una red que actúa como una ruta primaria para el tráfico que se origina en y se destina a otras redes.
- **Binario:** Sistema de numeración caracterizado por 1´s y 0´s.
- **Bucle**: Ruta en la que los paquetes nunca alcanzan su destino, sino que recorren repetidamente una serie cte. de nodos de red.

C

- **Codec:** Algoritmos de Compresión/Descompresión, se utilizan para reducir el tamaño de los datos multimedia, tanto audio como vídeo, compactan (codifican) un flujo de datos multimedia cuando se envía y lo restituyen (decodifican) cuando se recibe. Un codec se usa para conversiones analógicas a digitales, algunos ejemplos de *codecs* típicos son G.711, G.723.1, G.729 o G.726.
- **Canal**: Se usa para identificar una trayectoria a través de la cual serán enviadas las señales; también se usa para describir una banda de frecuencias.
- **Codificación:** Proceso por el cual los bits son representadas por tensiones, técnicas eléctricas utilizadas para transportar señales binarias.
- **Compresión de datos:** Reducir la cantidad de bits asignados a la representación de un conjunto de datos.
- **Conmutación de paquetes:** Transmisión de información estructurada en unidades pequeñas llamadas paquetes, dando a cada paquete un tratamiento independiente de los demás a lo largo de la red.
- **Conmutación de circuitos:** Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación de circuitos más ubicua es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, «ranuras» de tiempo o frecuencias) dedicados para cada llamada telefónica.
- **Columna vertebral (backbone):** Conexión de alta velocidad que une computadoras encargadas de hacer circular grandes volúmenes de información.
- **Capa de aplicación**: Capa 7 del modelo OSI, esta capa provee servicios a procesos de aplicaciones (e-mail, FTP) que no pertenecen al modelo OSI. La capa identifica y establece la disponibilidad de las partes que se tiene pensado comunicar, sincroniza aplicaciones y aprueba los procedimientos para recuperación de errores y control de los datos.
- **Capa de presentación:** Capa 6 del modelo OSI, esta capa garantiza que la información enviada por la capa de aplicación de un sistema sea legible por la capa de aplicación de otro, esta capa también se encuentra involucrada con las estructuras de datos utilizadas por los programas.
- **Capa de sesión:** Capa 5 del modelo OSI, esta capa establece, gestiona y termina sesiones entre aplicaciones y gestiona el intercambio de datos entre entidades de la capa de presentación.
- **Capa de transporte:** Capa 4 del modelo OSI, esta capa es responsable de una comunicación de red confiable entre 2 nodos extremos, también provee mecanismos para el establecimiento, mantenimiento y terminación de ctos. virtuales, detección y recuperación de fallos en el transporte y control de flujo de información.
- **Capa de red:** Capa 3 del modelo OSI, esta capa provee conectividad y selección de rutas entre 2 sistemas terminales, aquí es donde tiene lugar el enrutamiento.
- **Capa de enlace**: Capa 2 del modelo OSI, esta capa brinda un transito confiable de datos a través de un enlace físico; además tiene correspondencia con el direccionamiento físico, topología de red, disciplina de línea, notificación de error, entrega solicitada de frames y control de flujo.
- **Capa física:** Capa 1 del modelo OSI, define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para la activación, mantenimiento y desactivaron de la capa física entre sistemas finales.
- **Circuito virtual:** Circuito lógico creado para garantizar una comunicación confiable entre 2 dispositivos de red.
- **Código de corrección de errores**: Código que tiene suficiente inteligencia e incorpora información de señalización como para permitir la detección y corrección de muchos errores en el receptor.
- **Código de detección de errores:** Código que puede detectar errores de transmisión mediante un análisis de los datos recibidos.
- **Colisión:** Es el resultado de 2 nodos transmitiendo en forma simultanea.

- **CSMA/CD (Acceso múltiple con detección e portadora y detección de colisiones):** Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos primero verifican el canal en busca de una portadora.
- **Concentrador (Hub):** Dispositivo que sirve como centro de una red de topología en estrella.
- **CRC (Verificación de redundancia cíclica):** Un método de detección de error que construye un polinomio cuyos coeficientes de los términos son los valores de cada uno de los bits de un bloque de datos.
- **Cabecera (header):** Parte inicial de un mensaje o paquete que contiene caracteres para su control y encaminamiento.
- **Calidad de servicio (QoS):** Es un parámetro de la apreciación que el usuario hace de un determinado servicio compuesto de varios factores.
- **Campo (field):** Cada uno de los datos individuales de un registro.
- **CCITT (Comité consultivo internacional para la telefonía y telegrafía):** Organismo internacional encargado de establecer recomendaciones referentes a las telecomunicaciones (teléfono, telegrafía y datos), actualmente se llama ITU-T.
- **CDPD** (Cellular Digital Packet Data). Estándar diseñado para transmitir paquetes IP a través de los canales de radio no utilizados por el servicio de voz en el sistema de telefonía celular norteamericano.
- **cRTP (Protocolo de transporte en tiempo real comprimido):** Esta basado en la compresión de la cabecera TCP, CRTP reduce los 40 bytes de las cabeceras IP/UDP/RTP a 4.
- **Circuito:** Ruta de comunicaciones entre 2 o más puntos.
- **Cliente:** Nodo o programa de sw que solicita servicios de un servidor.
- **Cola:** En enrutamiento, reserva acumulada de paquetes que esperan a ser enviados a través de una interfaz de router.
- **Control de flujo**. Técnica de control del flujo en al cual un receptor le permite al emisor transmitir datos hasta que la ventana este llena.
- **Celda:** Una unidad de datos que es transmitida a través de una red, similar a un bloque de datos.
- **Cos (Clase de servicio):** Un esquema de priorizacion de datos que etiqueta a los datos con un nivel de prioridad especifica.

D

- **Dirección IP**: Un número único de 32 bits para una computadora TCP/IP concreta en Internet, escrita normalmente por 4 números en decimal (por ejemplo, 128.122.40.227).
- **Datagrama:** Agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual.
- **Demodulacion:** Proceso de retornar una señal modulada a su forma original.
- **Dirección de red:** Dirección de capa de red que se refiere a un dispositivo de red lógico, en vez de físico (dirección de protocolo).
- **DHCP (Protocolo de configuración dinámica de direcciones IP):** Protocolo que proporciona un mecanismo para asignar direcciones IP dinámicamente para que esas direcciones se puedan volver a utilizar automáticamente cuando los hosts ya no lo necesiten.
- **DNS (Sistema de Nombres de Dominio).** Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.
- **DSL (Línea digital de suscriptor):** Tecnología que permite a un proveedor usar el exceso de ancho de banda de sus líneas de pares de cobre para proporcionar servicios de datos.
- **Dirección de destino:** Dirección de un dispositivo de red que recibe datos.
- **Direccionamiento:** Un concepto de redes que describe el proceso de asignar números de identificación únicos (direcciones) aun dispositivo de red.

- **DSP (Procesador de señal digital):** Un microprocesador digital especializado que realiza cálculos o digitaliza señales originalmente analógicas, su gran ventaja es que son programables. Entre sus principales usos está la compresión de señales de voz, son la pieza clave de los codec.

E

- **Encriptar:** Procedimiento para codificar información de manera que pueda transmitirse sin peligro de ser interceptada o alterada antes de que llegue a su destinatario.
- **Entidad:** La especificación H.323 lo define como cualquier componente que cumpla con el estándar.
- **Extremo:** Un *extremo* H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.
- **EIA (Asociación de industrias electrónicas):** Es un comité de ANSI responsable de algunos estándares a nivel físico, eléctrico y funcional.
- **Encaminamiento (routing):** Determinación del camino a tomar en la red por una comunicación o por un paquete de datos.
- **Ethernet:** Red de área local con topología de bus y velocidad de 10 Mbs sobre cable coaxial que sigue la norma IEEE 802.3.
- **Encapsulación.** Envoltura de datos en una cabecera de protocolo en particular.
- **Enlace:** Canal de comunicaciones de red que consiste en un cto. o ruta de transmisión y todo el equipo relacionado entre un emisor y receptor.
- **Enrutamiento:** Proceso de descubrimiento de una ruta hacia el hosts de destino.
- **EGP (Protocolo de gateway exterior):** Enruta datos entre sistemas autónomos (BGP).

F

- **Fax/server:** Envío local por medio de un teleproductor de imágenes.
- **Frecuencia:** Número de periodos por unidad de tiempo; si la unidad de tiempo es un segundo, la frecuencia se mide en Hertz.
- **Frame:** Agrupación lógica de información enviada como unidad de la capa de enlace de datos por medio de transmisión. Los términos Datagrama, mensaje, paquete de datos y segmento también se utilizan para describir agrupaciones lógicas de información en diversas capas del modelo OSI.
- **Fragmentación:** Proceso de dividir un paquete en unidades más pequeñas cuando se transmite por un medio de red que no puede soportar el tamaño original del paquete.
- **FTP (Protocolo de transferencia de archivos):** Permite a un usuario de un sistema acceder y transferir información a y desde otro sistema a través de una red.
- **Fast ethernet:** Una tecnología de redes con amplio ancho de banda y que se basa en el estándar 802.3 ethernet de 100 Mbps.
- **FoIP (Fax sobre IP):** Envió de documentos a través de Internet.
- **Frame relay**: Protocolo de capa de enlace de datos conmutado estándar que manipula múltiples ctos. virtuales utilizando una forma de encapsulacion HDLC.
- **FDDI (Interfaz de datos distribuidos por fibra)**: Estándar LAN que especifica una red de transmisión de testigo de 100 Mbps. que utiliza cable de fibra óptica.
- **Firewall**: Dispositivo que controla quien puede acceder a una red privada y que es por sí mismo inmune a al penetración.
- **Flujo**: Corriente de datos que viaja a través de 2 puntos extremos a través de una red (estación LAN a otra).

G

- **Gatekeeper:** Un componente del estándar ITU H.323, es la unidad central de control que gestiona las prestaciones en una red de Voz o Fax sobre IP, o de aplicaciones multimedia y de videoconferencia. Los Gatekeepers proporcionan la inteligencia de red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de los detalles de las llamadas para tarifar y comunicación con el sistema de gestión de la red.
- **Gateway:** En general se trata de una pasarela entre 2 redes, técnicamente se trata de un dispositivo repetidor electrónico que intercepta y adecua señales eléctricas de una red a otra. En Telefonía IP se entiende que estamos hablando de un dispositivo que actúa de pasarela entre la red telefónica y una red IP. Es capaz de convertir las llamadas de voz y fax, en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet.
- **Gb (Gigabit).** Aproximadamente 1,000,000,000 bits.

H

- **H.323:** Es la recomendación (incluye referencias a otros estándares, como H.225 y H.245) de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para las comunicaciones multimedia sobre redes basadas en paquetes que no proporcionan una Calidad de Servicio (QoS) garantizada. Define las diferentes entidades que hacen posible estas comunicaciones multimedia: endpoints, gateways, unidades de conferencia multipunto (MCU) y gatekeepers, así como sus interacciones.
- **Host:** Sistema de computadoras en una red que implica un sistema de computación.
- **Hub (concentrador):** Elemento multipuerta y multiacceso empleado para la interconexión de distintos tipos de arquitectura, pudiendo ser activo o pasivo.
- **HLDC (Control de enlace de datos de alto nivel).** Protocolo sincrono de la capa de red de datos orientado a bits desarrollado por la ISO.
- **HTTP (Protocolo de transferencia de hipertexto).** Protocolo utilizado por los navegadores web y los servidores web para transferir archivos.

I

- **IETF (Grupo de ingeniería de Internet):** Grupos de trabajo responsable de resolver las necesidades de ingeniería a corto plazo.
- **IP (Internet Protocolo):** La parte IP del protocolo de comunicaciones TCP/IP. Implementa el nivel de red (capa 3 de la pila de protocolos OSI), que contiene una dirección de red y se utiliza para enrutar un paquete hacia otra red o subred. IP acepta paquetes de la capa 4 de transporte (TCP o UDP), añade su propia cabecera y envía un datagrama a la capa 2 (enlace). Puede fragmentar el paquete para acomodarse a la máxima unidad de transmisión (MTU, Maximum Transmission Unit) de la red.
- **ITU-T (Unión Internacional de las Telecomunicaciones – Sector de normalización):** Antes conocida como CCITT (Comite Consultatif Internationale de Telegraphie et Telephonie). Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones: crea estándares, reparte frecuencias para varios servicios, etc.
  El grupo ITU-T recomienda estándares para telecomunicaciones y está en Génova (Suiza), también se encarga de elaborar recomendaciones sobre codecs (compresión/descompresión de audio) y módems.
- **Intranet:** Utilización de la tecnología de Internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una empresa.

- **IEEE (Instituto de ingenieros eléctricos y electrónicos):** Organismo americano responsable de determinados estándares en el campo de las telecomunicaciones.
- **ISO (Organización de estándares internacionales):** Organismo cuya función es la de coordinar los trabajos de normalización realizados por los diferentes organismos internacionales.
- **ISP (Proveedor de servicio de Internet):** Es una empresa que suministra a otras empresas o personas el acceso a Internet, además de otros servicios opcionales.
- **ICMP (Protocolo de mensajes de control a nivel de red en Internet)**: Protocolo de Internet de capa de red que informa de errores y ofrece otra información relativa al procesamiento de paquetes IP.
- **IPBX (Centralita Privada basada en IP):** PBX basada en IP.
- **IPSec (Protocolo de Seguridad IP):** Proporciona servicios de seguridad como autentificación, integridad, confidencialidad y control de acceso en al capa IP.
- **ITSP (Proveedor de Servicios de Telefonía Internet, PSTI):** Compañía telefónica que provee el servicio de Internet.
- **Impedancia.** Es la oposición al flujo de corriente eléctrica en un cto. de c.a.
- **IGP (Protocolo de gateway interior):** Protocolo de Internet utilizado para intercambiar información de enrutamiento dentro de un sistema autónomo.
- **Interfaz:** Conexión entre 2 sistemas o dispositivos.
- **Interworking:** Colección de redes interconectadas mediante routers y otros dispositivos que funcionan como una única red.

J

- **Jitter (variación de retardo):** Es un término que se refiere al nivel de variación de retado que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio o vídeo, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos inintelegibles.

K

- **kbit/s (kilobit por seg.):** Expresa una velocidad de transferencia binaria de 1,000 bits por segundo.

L

- **LAN (Red de área local):** Una red pequeña de datos que cubre un área limitada, como el interior de un edificio o un grupo reducido de edificios, que conecta estaciones de trabajo, periféricos, terminales y otro dispositivos en un solo edificio.
- **LOOP:** Arreglo de comunicaciones multipunto donde las estaciones se conectan en forma de anillo o loop.
- **LLC (Control de enlace lógico):** La mas alta de las 2 subcapas de la capa de enlace de datos, manipula el control de errores, control de flujo, entramado y direccionamiento de la subcapa MAC.
- **Latencia**: En tiempo de demora que un dispositivo de red introduce cuando bloques de datos pasan por ella.

M

- **Media Gateway:** Denominación genérica para referirse a varios productos agrupados bajo el protocolo MGCP (Media Gateway Control Protocol). La principal misión de un Media Gateway es la conversión IP/TDM bajo el control de un Softswitch.
- **MGCP (Protocolo Controlador de media Gateway):** Es un protocolo de control de dispositivos, donde un gateway esclavo (MG, Media Gateway) es controlado por un maestro (MGC, Media Gateway Controller).
- **Muestreo**: Proceso mediante el cual se representa una señal continua por medio de valores discretos de la misma, llamados muestras.
- **MAN (Red de área metropolitana):** Red que resulta de varias redes locales (LAN) interconectadas por un enlace de mayor velocidad o backbone.
- **Multimedia:** Combinación de varias tecnologías de presentación de información (imágenes, sonido, animación, vídeo, texto).
- **Modelo de referencia OSI:** Modelo de referencia de interconexión de sistemas abiertos, el cual consiste en 7 capas cada una de las cuales especifica funciones particulares de la red.
- **MAC (control de acceso al medio):** Un protocolo para acceder a un medio de comunicaciones especifico, que constituye una sub-capa en el nivel 2 del modelo OSI.
- **MAU (unidad de acceso al medio):** Dispositivo empleado en las LAN's para permitir el acceso de las terminales al medio de transmisión.
- **Modulación:** Variación en el tiempo de ciertas características (amplitud, frecuencia o fase) de una señal eléctrica, portadora, conforme a la señal que se desea transmitir.
- **MCU (Unidad de Control Multipunto):** Dispositivos que permiten que 2 o mas terminales o gateways realicen conferencias con sesiones de audio y/o video.
- **MEGACO (Media Gateway Control):** Es un protocolo de VoIP, combinación de los protocolos MGCP e IPDC. Es más sencillo que H.323
- **MPLS (Conmutación de Etiquetas Multiprotocolo):** Habilita él envió rápido de celdas a través de una red, lo cual proporciona una implementación HW de bajo costo, escalabilidad a una velocidad baja y flexibilidad en al gestión de flujos de tráfico.
- **Mensaje:** Agrupación lógica de información de la capa de aplicación, compuesta por un numero de agrupaciones lógicas de las capas inferiores.
- **Método de acceso**. Forma en que los dispositivos de red acceden al medio de red.
- **Multidifusion:** Paquetes únicos copiados por la red y enviados a un subconjunto especifico de direcciones de red.
- **Multiplexacion:** Esquema que permite que se transmita múltiples señales lógicas simultáneamente a través de un único canal físico.

N

- **Nodos**: Puntos en los cuales se ubican equipos de procesamiento en una red, y a los cuales están conectados los enlaces de la misma.
- **Números de saltos**: Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino.
- **Numero de red**: La parte de una dirección IP que especifica la red a la que pertenece el host.

O

- **OSI (interconexión de sistemas abiertos):** Esta es una recomendación de la ISO que describe una estructura de 7 capas para la partición de comunicación de datos.

- **OSP (Abrir primero la vía mas corta):** Es un protocolo de enrutamiento por estado de enlace basado en estándares libres.
- **Octeto de 8 bits:** Se utiliza con frecuencia (en lugar de byte) debido a que algunas arquitecturas de maquinas emplean bytes que no tiene 8 bits de longitud.
- **OSPF (Primero la ruta libre más corta):** Algoritmo de enrutamiento IGP jerárquico por estado de enlace propuesto como sucesor de RIP en Internet.

P

- **PBX (Intercambio de rama privada):** Central privada de comunicaciones telefónica, un sistema telefónico utilizado en compañías y organizaciones, privado por tanto, para manejar llamadas externas e internas. La ventaja es que la compañía no necesita una línea telefónica para cada uno de sus teléfonos. Además las llamadas internas no salen al exterior y por tanto no son facturadas.
- **PCM (Modulación por código de pulso):** Convierte una señal analógica (sonido, voz normalmente) en digital para que pueda ser procesada por un dispositivo digital, normalmente un ordenador. Si, como ocurre en Telefonía IP, nos interesa comprimir el resultado para transmitirlo ocupando el menor ancho de banda posible, necesitaremos usar además un codec. Método común de digitalizar la señal de la voz, se requiere un ancho de banda de 64 kb por segundo para un canal de voz digitalizada.
- **PSTN (Red publica de telefonía conmutada):** Red telefónica publica convencional de conmutación de circuitos.
- **Protocolo**: Conjunto de reglas para que pueda ser realizado un proceso de comunicaciones.
- **Puente (bridge):** Dispositivo que conecta y pasa paquetes entre 2 segmentos de red que utilicen el mismo protocolo de comunicaciones, este opera en la capa de enlace de datos (capa 2) del modelo OSI.
- **Paquete:** Agrupamiento lógico de información que incluye un encabezado que contiene información de control y datos del usuario, los paquetes utilizan frecuentemente para hacer referencia a las unidades de datos de las capas de red.
- **Par trenzado:** Medio de transmisión de velocidad relativamente baja que consiste en 2 cables aislados dispuestos en forma de espiral regular, los cables pueden ser blindados (FTP) o sin blindaje (UTP).
- **Petición de comentarios (RFC):** Serie de documentos empleada como medio de comunicación primarios para transmitir información acerca de Internet, además documentan especificaciones de protocolos.
- **Portadora:** Onda electromagnética o de corriente alterna de frecuencia única, apropiada para la modulación por otra señal que transporta datos.
- **POTS (servicio telefónico del viejo plan):** Se refiere al servicio telefónico (teléfonos analógicos) ofrecido por las redes publicas.
- **Proxy:** Elemento intermedio entre las la LAN y la WAN que realiza funciones de separación entre ambas y filtrado paquetes.
- **PAM (Modulación por amplitud de pulsos):** La señal analógica es filtrada y convertida en forma de onda digitalizada.
- **PPP (Protocolo de punto a punto):** Sucesor de SLIP que proporciona conexiones de red router a router y host a red a través de ctos. sincronos y asíncronos, se diseño para funcionar con varios protocolos de la capa de red (IP,IPX).
- **PDU (Unidad de datos del protocolo):** Termino OSI equivalente a paquete.
- **Protocolo de enrutamiento:** Protocolo que realiza enrutamiento a través de la implementacion de un algoritmo de enrutamiento .
- **Protocolo enrutado:** Protocolo que pude ser enrutado a través de un router.

- **Protocolo:** Es un conjunto de reglas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.
- **PVC (Circuito virtual permanente):** Los PVC ahorran el ancho de banda relacionado con el establecimiento y el desmantelamiento del cto. en situaciones en las que ciertos ctos. virtuales deben existir de forma permanente.

Q

- **QoS (Calidad de Servicio):** Parámetros asociados con la priorizacion de datos que especifican la cantidad de ancho de banda que requiere una prioridad de transmisión de datos, así como la cantidad máxima de latencia que la transmisión pueda tolerar para que la transmisión tenga sentido.

R

- **RTP (Protocolo de Tiempo Real):** El protocolo estándar en Internet para el transporte de datos en tiempo real, incluyendo audio y vídeo. Se utiliza prácticamente en todas las arquitecturas que hacen uso de VoIP, videoconferencia, multimedia bajo demanda y otras aplicaciones similares. Se trata de un protocolo *ligero* que soporta identificación del contenido, reconstrucción temporal de los datos enviados y también detecta la pérdida de paquetes de datos.
- **Redes conmutadas**: redes de telecomunicaciones que usan el principio de conmutación: compartir canales entre diferentes conversaciones.
- **Red (Network):** Dos o más computadoras conectadas para cumplir una función como compartir periféricos (impresoras), información (datos) o para comunicarse.
- **Ruteador (router):** Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta optima por la cual se enviara él trafico de red, los ruteadores envían paquetes de una red a otra en base a la información de capa de red.
- **RFC (Solicitud de comentarios):** Recomendaciones dadas por el comité para la estandarización de la familia de protocolos TCP/IP, además incluye documentos informáticos y propuestas de estándar para su discusión.
- **RIP (Protocolo de información de ruteo):** Protocolo de red que emplea el ruteo dinámico por vector distancia.
- **RAS (Registro, Autentificación y Estado):** Proporciona un control de prellamadas en las redes H.323 donde existen gatekeepers y una zona.
- **RSVP (Protocolo de Reserva de recursos):** Protocolo que soporta la reserva de recursos en una red IP.
- **RDSI (Red digital de servicios integrados):** Protocolo de comunicación ofrecido por las compañías telefónicas que permite que las redes telefónicas trasmitan datos, voz y trafico de otro origen.
- **Resolución de direcciones**: Método para resolver diferencias entre esquemas de direccionamiento de computadoras, la resolución de direcciones especifica un método de asignación de direcciones de la capa de red (capa 3) a direcciones de la capa de enlace de datos (capa 2).

S

- **SIP (Protocolo de iniciación de sesión):** Es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Un estándar de la IETF (Internet Engineering Task Force) definido en la RFC 2543. SIP se utiliza para iniciar, manejar y terminar sesiones interactivas entre uno o más usuarios en Internet. Inspirado en

los protocolos HTTP (web) y SMTP (email), proporciona escalabilidad, flexibilidad y facilita la creación de nuevos servicios.

Cada vez se utiliza más en VoIP, gateways, teléfonos IP, softswitches, aunque también se utiliza en aplicaciones de vídeo, notificación de eventos, mensajería instantánea, juegos interactivos, chat, etc.

- **SS7 (Sistema de señalización N° 7):** Es un estándar global para telecomunicaciones definido por la ITU, define los procedimientos y protocolos mediante los cuales los elementos de la Red Telefónica Conmutada (RTC o PSTN, Public Switched Telephone Network) intercambian información sobre una red de señalización digital para establecer, enrutar, facturar y controlar llamadas, tanto a terminales fijos como móviles.
- **Señalizar**: Proceso mediante el cual se notifica algo (es decir, se envía una señal de control de un equipo de la red a otro).
- **Señal digital:** Lenguaje de computadoras que consta solamente de 2 estados, encendido y apagado, los cuales se indican mediante una serie de impulsos de tensión.
- **Señal**: Es la información que se transmite por una red pudiendo ser analógica o digital.
- **SAP (Protocolo de Anuncio de Servicios):** Permite la notificación de recursos.
- **SONET (Red óptica sincrona)**: Transmisión por fibra óptica y utiliza una señal de 51.85 Mbps.
- **SNMP (Protocolo simple de administración de redes):** Es un protocolo de administración de red que se usa para informar condiciones anómalas de la red y especificar valores de umbrales de red.

T

- **Telefonía IP:** Tecnología para la transmisión de llamadas telefónicas ordinarias sobre Internet u otras redes de paquetes utilizando un PC, gateways y teléfonos estándar. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional. Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.
- **TCP (Protocolo de control de transmisión):** Protocolo de comunicación que permite comunicarse a los ordenadores a través de Internet, asegura que un mensaje es enviado completo y de forma fiable. Se trata de un protocolo orientado a conexión.
- **Terminal:** Un *terminal* H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.
- **Tasas de transmisión**: número de símbolos digitales que se transmiten por un canal en cada segundo.
- **TDM (Multiplexacion por división de tiempo):** Técnica de multiplexacion por división en el tiempo que permite intercalar los datos procedentes de varios usuarios en un único canal.
- **Topología:** Disposición física de los distintos elementos que componen una red.
- **Trama (frame):** Procedimiento mediante el cual un protocolo añade a los datos originales un encabezado y una cola.
- **Token ring.** LAN de transmisión de testigos y funciona a 4 o 16 Mbps. a través de una topología en anillo.
- **Telnet**: Protocolo de emulación de terminal estándar de la pila del protocolo TCP/IP , se utiliza para la conexión de terminales remotos.

- **Testigo (Token):** Trama que contiene información de control, la posesión del testigo permite a un dispositivo de red transmitir datos en la red.
- **Transmisión asíncrona:** Señales digitales que se transmiten sin una sincronización precisa y tienen diferentes frecuencias y relaciones de fases.
- **Tunneling:** Arquitectura diseñada para proporcionar los servicios necesarios para implementar un esquema de encapsulacion punto a punto estándar.

U

- **UDP (Protocolo de Datagrama de usuario):** Protocolo sin conexión de transporte en el protocolo de TCP/IP, UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejadas por otro protocolo.
- **UTP (par trenzado sin apantallar):** Conductores trenzados entre si para minimizar el efecto de la inducción electromagnética entre ellos.
- **Unidifusion**: Capacidad de transmisión en una sola dirección entre una estación emisora y una receptora.

V

- **Voz sobre IP:** Permite la transmisión de la voz a través de redes IP en forma de paquetes de datos, el Protocolo de Internet (IP) es el protocolo utilizado en las redes de datos, como Internet para transmitir la información de un punto a otro. La información se segmenta en paquetes, y cada uno tiene escrita la dirección a la que se envía y de la que procede.
- **VPN (Red Privada Virtual):** Red que usa Internet o una red publica como backbone de transporte para conectarse en forma segura a un negocio con oficinas remotas.

W

- **WAN (Red de área amplia):** Una red de comunicaciones utilizada para conectar ordenadores y otros dispositivos a gran escala, las conexiones pueden ser privadas o públicas.

X.

- **X.25:** Estándar ITU-T que define como se mantiene las conexiones entre DTE y DCE para el acceso a terminales remotas y las comunicaciones entre computadoras en las PDN.

APÉNDICE.

Tecnología del Protocolo de Voz sobre IP (VoIPv4).

Estándares.

Señalización.	
	ITU-T ESTÁNDARES Y RECOMENDACIONES.
H.323 v.2	Sistemas de comunicaciones multimedia basados en paquetes.
H.225	Protocolos de señalización de llamada y medios de comunicación vierten la paquetización para la multimedia basada en paquetes (incluye Q.931 y RAS)
H.245.0 Anexo G.	Las comunicaciones de Gatekeeper a Gatekeeper (inter-dominio)
H.245	Protocolo de control para las comunicaciones multimedia.
H.235	Seguridad y encriptación para las series H de las terminales multimedia.
H.450.X	Los servicios suplementarios para la multimedia: 1. Protocolo funcional genérico para el apoyo de servicios suplementarios en H.323. 2. Transferencia de llamado. 3. Diversión. 4. Espera. 5. Descolgar y recepción. 6. Llamada en espera. 7. El mensaje de indicación de espera
H.323 ANEXO D	Fax de tiempo real que usa T.38
H.323 ANEXO E	Llamada de conexión sobre UDP
H.323 ANEXO F	Solo usa el dispositivo
T.38	Los procedimientos para el grupo 3 de tiempo real de comunicaciones de fax sobre las redes IP.
T.120 series.	Protocolos de datos para la conferencia multimedia.
IETF RFCs - Versión.	
RFC 2543	SIP: Protocolo de iniciación de Sesión
RFC 2327	SDP: Protocolo de descripción de Sesión
Versión de Internet.	SAP: Protocolo de anuncio de Sesión
Control de Gateway.	
ITU	
H.G.C.P.	Recomendación propuesta para el control de protocolo Gateway.
IETF	
Versión de Internet	MGCP: Protocolo de control de los medios del Gateway
Versión de Internet	MEGACO: Protocolo.
Versión.	SGCP: Protocolo Gateway de control simple.
Versión de Internet.	IPDC: Dispositivo de control IP.
Transporte de media	
IETF	
RFC 1889.	RTP: Protocolo de transporte de tiempo real
RFC 1889	RTCP: Protocolo de mando de transporte de tiempo real

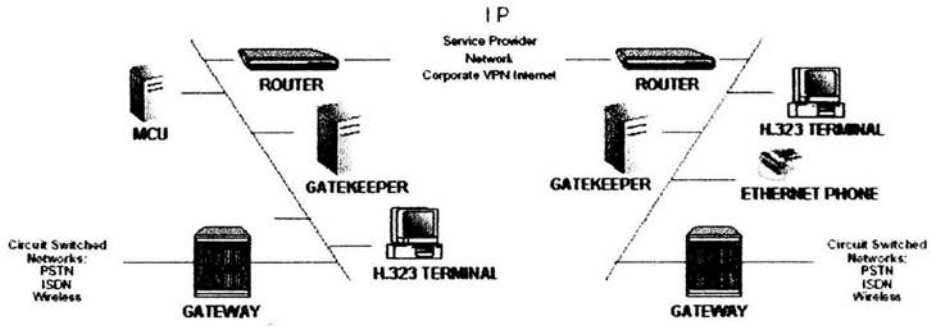
RFC 2324	RTSP: Protocolo de serialización de tiempo real.

Media Encoding				
ITU				
VOZ				
STANDAR	*ALGORITMO*	*BIT DE Proporción (Kbit/s)*	*TIPICA* Retraso de fin a fin típico (ms) (excluyendo el retraso del canal)	*RESULTADO DE CALIDAD DE VOZ*
G.711	PCM	48,.56,64	<< 1	EXCELENTE
G.723.1	MPE-ACELP	5.3, 6.3	67-97	BUENA
G.728	LD-CELP	16	<< 2	BUENA
G.729	CS-ACELP	8	25-35	BUENA
G.729 ANEXO A	CD-ACELP	8	25-35	BUENA
G.722	SUB-BANDA ADPCM	48,56,64	< 2	BUENA
G.726	ADPCM	16,24,32,40	60	BUENA
G.727	EADPCM	16,24,32,40	60	BUENA

VIDEO			
STANDAR	*ALGORITMO*	*BIT DE Proporción (Kbit/s)*	*CALIDAD DE IMAGEN*
H.261	El coseno discreto transforma (DCT) con la compensación del movimiento	p x 64 (p = # de ISDN B canales)	BAJA
H.263	Mejora de la versión H.261	Varios	MEDIA

Arquitectura H.323.

Gatekeeper	Maneja una zona (colección de dispositivos de H.323).
Funcionalidad requerida	Traduce la dirección, el control de admisión, el control del ancho de banda.
Funcionalidad optativa	Autorización la llamada, la dirección del ancho de banda, los servicios suplementarios, los servicios del directorio, los servicios de dirección de llamada.
Gateway.	Proporciona la interoperabilidad entre las diferentes de redes, convierte la señalización y la media, ejemplo: Gateway IP/PSTN.
Terminal H.323.	Endpoint o LAN. Soporta en tiempo real comunicaciones en 2 sentidos con otra entidad H.323. Debe apoyar la voz (codecs de audio) y señalización (Q.931, H.245, RAS). Opcionalmente soporta el vídeo y datos por ejemplo, teléfono de PC o videoteléfono, el teléfono de Ethernet.
MCU	Soporta conferencias entre 3 o más endpoints. Contiene el controlador multipoint MC para la señalización. Puede contener el procesador multi-punto (MP) par medio de una serie de procesos. Puede ser autosuficiente (PC) o integrada a una Gateway, Gatekeeper o terminal.

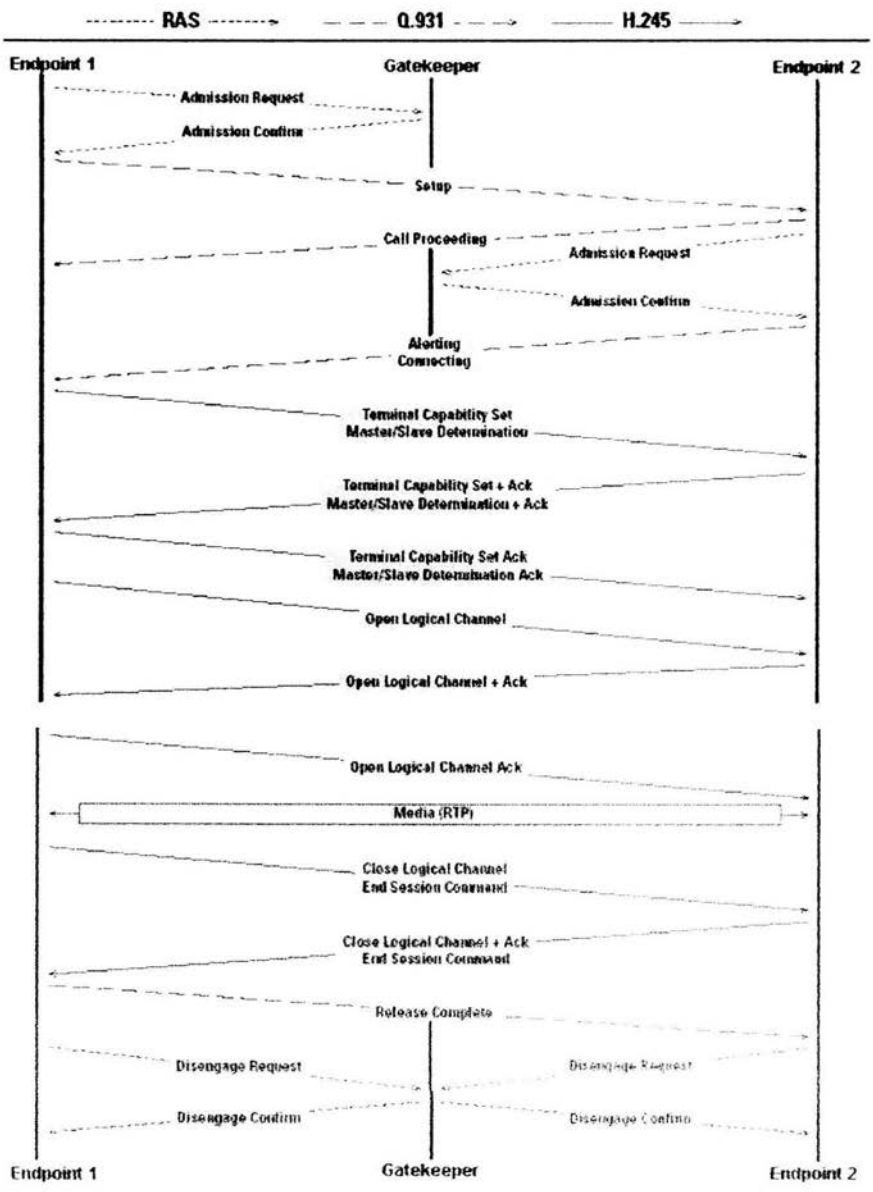


Comandos - H.323.

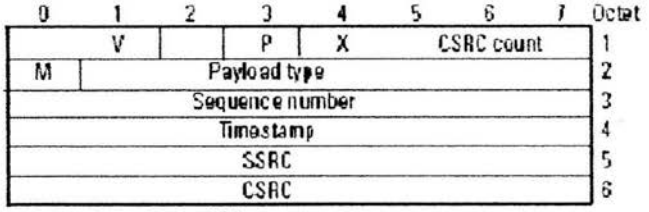
Mensajes importantes	**de H.323**
RAS.	
MENSAJE	***FUNCION***
RRQ – Petición de Registro.	Solicita a una terminal o Gateway para registrarse con un Gatekeeper. Ambos Gatekeeper confirman o rechazan (RCF o RRJ).
ARQ – Petición de Admisión.	Demanda el acceso a la red del paquete de la terminal al Gatekeeper. Ambos Gatekeeper confirman o rechazan (ACF o ARJ).
BRQ – Petición de Banda ancha.	Solicita la asignación del cambio del ancho de banda de la terminal al Gatekeeper. Ambos Gatekeeper confirman o rechazan (BCF o BRJ).
DRQ- Petición de desacoplamiento.	Envía del endpoint al Gatekeeper, DRQ informa Gatekeeper que el endpoint está lleno; si envió del Gatekeeper al endpoint, DRQ fuerza la llamada para ser dejado. El Gatekeeper confirma o rechaza (DCF o DRJ). Si DRQ enviara por el Gatekeeper, los endpoint deben contestar con DCF.
IRQ – Petición de Info.	La petición del estado de la información del Gatekeeper a la terminal.
IRR – Petición de Información.	La petición a IRQ. Puede enviarse a un no solicitado por la terminal al Gatekeeper a intervalos predeterminados.
RAS- Tiempos y peticiones en progreso de RIP.	Los valores de la interrupción predefinido recomendados para la contestación de los mensajes del RAS y las cuentas del reintento subsecuentes si la contestación no se recibe.
Q.931	
MENSAJE	***FUNCION***
Alerta.	El usuario llamado ha sido alertado "el teléfono está sonando." Enviando llamado por el usuario.
Procedimiento de la llamada	El establecimiento de la llamada pedida se ha comenzado y ninguna más información de establecimiento de llamada se aceptara. Enviado el llamado por el usuario.
Conexión.	Aceptando el llamado de la llamada entrante. Enviado de la entidad llamada a la entidad llamante.

Setup.	Indica un llamado de la entidad H.323, preparar una conexión a la entidad llamada.
Descarga Completa.	Indica la liberación de la llamada si H.225.0 (Q.931) la señalización de llamada del canal está abierta. Después, la llamada de referencia puede reusarse. Enviada por una terminal.
Estado	Solicita un mensaje de la señal de llamada desconocida o a un mensaje de pregunta de Estado. Proporciona la información del estado de la llamada.
Estado de investigación.	Solicita el estado de las llamadas. Puede enviarse por un endpoint o Gatekeeper a otro endpoint.
H.245	
MENSAJE	***FUNCION***
Determinación del maestro-esclavo.	Determinar cuando una terminal es el maestro y cuando esclavo. Las posibles respuestas: Reconocimientos, Rechazos, Liberación (en caso de un tiempo fuera).
Capacidad de la Terminal establecida.	Contiene información sobre la capacidad de una terminal para transmitir y recibir las series de multimedia. Las posibles contestaciones: Reconocimiento, Rechazo, Liberación.
Canal Lógico abierto.	Abierto el canal lógico para el transporte de audiovisual y datos de información. Las posibles contestaciones: Reconocimientos, Rechazos, Confirmaciones.
Canal Lógico cerrado.	El cierre del canal lógico entre 2 endpoints. Las posibles contestaciones: Reconocimiento.
Modo de respuesta.	Usado para recibir la terminal de los modos de respuestas particulares de transmisión de una terminal. Los tipos del modo generales incluyen Modo de Vídeo, Modo de Audio, Modo de Datos, y Modo de Encriptación. Las posibles contestaciones: Reconocimiento, Rechazo, Liberación.
Capacidad de envío de la Terminal establecida.	Los comandos de principio-fin de la terminal indica si transmite y recibe las capacidades enviadas a 1 o más terminales.
Sesión de comandos finales.	Indica el fin de la sesión de H.245. Después de la transmisión, la terminal no enviará más mensajes a H.245.

Llamada de H.323.



Encabezado RTP.



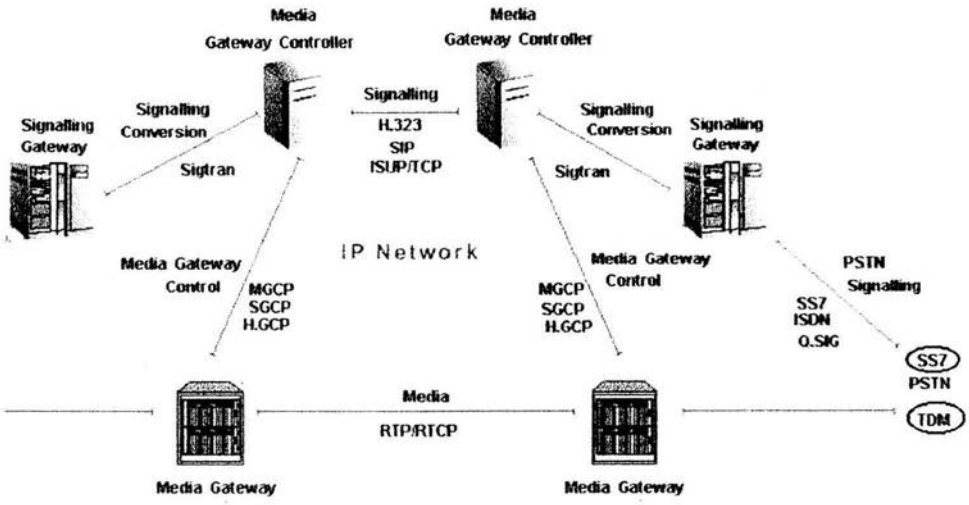
RTP structure

V	Versión. Identifica la versión de RTP.
P	Relleno. Cuando el contenido del paquete de uno o más rellenos adicionales al final de los octetos, que son parte del relleno.
X	Extensión del bit. Cuando el encabezado es fijo sigue exactamente una extensión del encabezado, con un formato definido.
CSR Contador.	Contiene el número de identificadores de CSRC que siguen al encabezado fijo.
M	Marcador. La interpretación del marcador está definida por un perfil. Se piensa que permite los eventos significantes como los límites del marco sean marcados por una serie de paquetes.
Tipo de la carga útil	Identifica el formato de la carga útil de RTP y determina su interpretación por la aplicación. Un perfil especifica que una cartografía estática predefinida de tipo de la carga útil codifica a los formatos de la carga útil. Pueden definirse los códigos de tipo de carga útil adicionales dinámicamente a través de los medios del non-RTP.
Número de secuencia.	Los incrementos por uno para cada RTP de datos del paquete enviado, y puede usarse por el receptor para descubrir la pérdida del paquete y restaurar la sucesión del paquete.
Tiempo del timbre.	Refleja el momento de la muestra del primer octeto en el RTP de los datos paquete. El momento de la muestra debe derivarse de un reloj que incrementa la monotonía y linealmente a tiempo para permitir sincronización y cálculos del jitter. La resolución del reloj debe ser suficiente para la exactitud de la sincronización deseada y por medir del jitter de llegada del paquete (un tictac por el marco vídeo es típicamente insuficiente).
SSRC	Identifica la fuente de la sincronización. Este identificador es escogido al azar, con el intento que ninguna de las 2 fuentes de la sincronización dentro de la misma sesión de RTP tendrá el mismo identificador de SSRC.
CSRC	Contribuye a la lista de identificadores de la fuente. Identifica las fuentes contribuyendo para la carga útil contenida en este paquete.

Convergencia en la arquitectura de red.

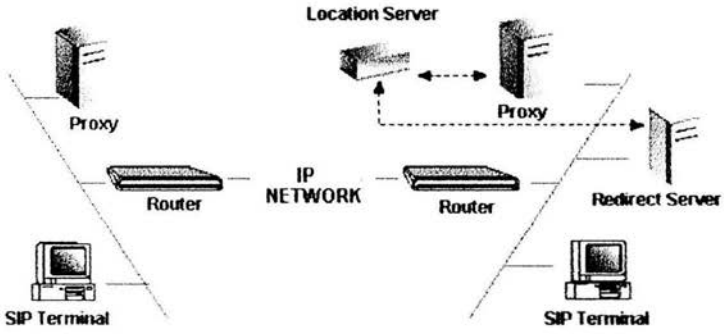
- **Controlador media del Gateway**: El arreglo de las Coordenadas, manejo y terminación de flujos de los medios del Gateway.
- **Señalización del Gateway**: la interfaz del SS7-IP, las coordenadas SS7 ven los elementos de IP y los elementos de IP de SS7.

- **Gateway media:** Terminal de línea PSTN y serie de medios de comunicación empaquetados para el transporte del IP.



Arquitectura SIP.

UAC (usuario agente cliente)	Aplicación de la llamada que comienza y envía las peticiones del SIP.
UAS (usuario agente servicio)	Recibe y responde para SIP las peticiones en nombre de los clientes; acepta, remite, o se niega las llamadas.
Terminal SIP	Soporta en tiempo real, comunicación en 2 sentidos con otra entidad del SIP. Soporta ambos la señalización y media, similar a la terminal de H.323. Contiene UAC.
Proxy.	Contacta uno o más clientes o servidores próximos y pasa la otra llamada de petición. Contiene UAC y UAS.
Servidor remitente.	Acepta las peticiones del SIP, mapas de dirección en cero o nuevas direcciones e ingresos en esas direcciones al cliente. No comienza las peticiones del SIP o acepte las peticiones de llamadas.
Servidor de locación.	Proporciona la información sobre las posibles llamadas de una locación para redirigirlos y a los servidores proxy. Puede co-localizarse con un servidor del SIP.



Métodos de SIP.

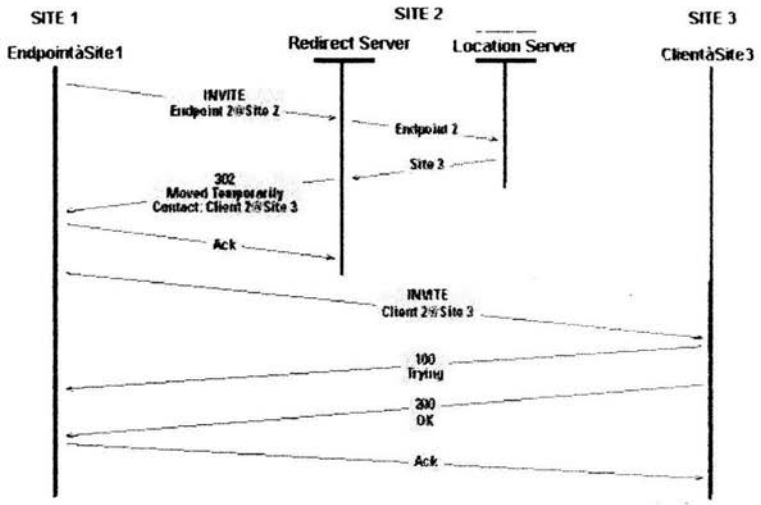
Comandos	Función.
Invitación	Inicializa la llamada.
ACK	Responde a la confirmación final.
BYE	Termina y transfiere la llamada.
Cancel	Cancela la búsqueda y el timbrado.
Opciones	Soporta otros lados en un futuro.
Registro.	Servicio que registra la localización.

Códigos de respuesta de SIP.

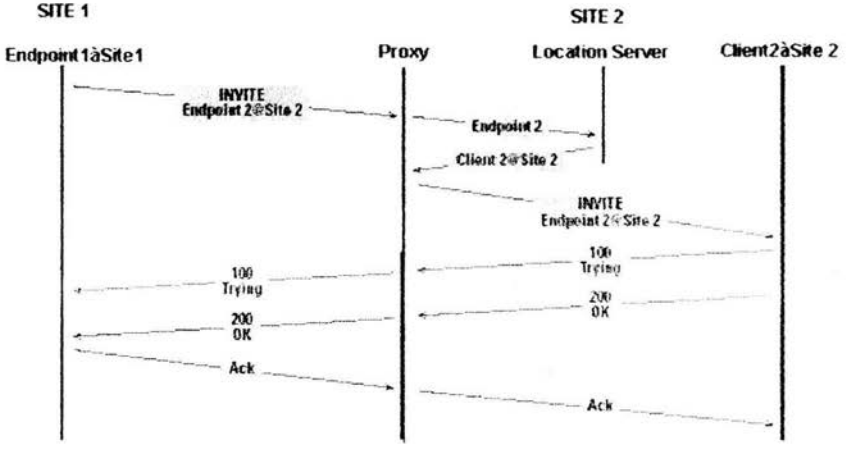
Código de respuesta prefijo.	Respuesta SIP	Función
1xx	Búsqueda, timbrado.	Proporciona el estado.
2xx	Exitoso.	La acción solicitada fue recibida, comprendida y aceptada.
3xx	Regreso.	El cliente debe realizar una acción adicional para completar la solicitud.
4xx	Fallas en peticiones.	La solicitud no es valida en este servidor.
5xx	Fallas en servidores.	La solicitud puede ser valida.
6xx	Fallas globales.	La solicitud fallara siempre.

Llamada de SIP.

Modo de operación remitente de SIP.



Modo de operación de Proxy con SIP.



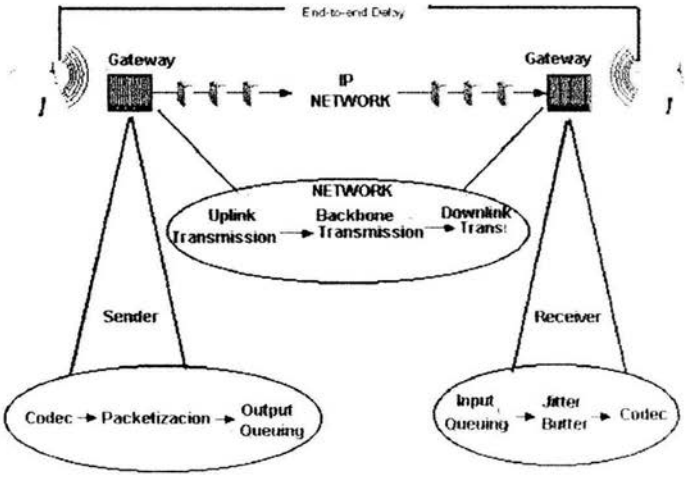
Factores que afectan la calidad de voz y como medirlos.

Retardo. El retraso excesivo de fin a fin hace la conversación inconveniente y antinatural. Cada componente en el camino de la transmisión, el envío, red, y el receptor agregan el retraso. El IRC-T G.114 (El tiempo de transmisión en un sentido) se recomienda 150 ms. como el máximo deseado del estado latente para lograr una calidad de voz superior.

Tabla de muestra de retraso.

Parámetro	Retraso fijo	Retraso variable.
CODEC (G.729)	25 ms.	
Paquetizacion	Incluido en CODEC	
Retraso de cola.		Depende de la transmisión de subida. En el orden de unos pocos ms.
Retraso de la red	50 ms.	
Jitter buffer	50 ms.	
Total	125 ms.	

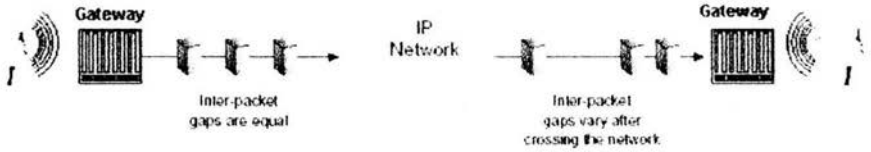
Retraso de fin a fin.



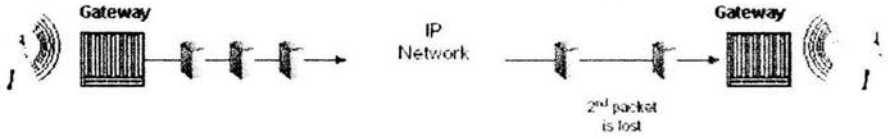
Jitter- Cuantifica los efectos de retrasos de la red en las llegadas del paquete al receptor. Los paquetes son transmitidos a los intervalos iguales de la entrada izquierda que llegan a la entrada correcta a los intervalos irregulares. El jitter excesivo hace el discurso agitado y dificil de entender. El jitter es calculado basado en el tiempo de llegada de los paquetes sucesivos.

Para la voz de calidad superior, el medio tiempo de llegada al receptor debe ser casi igual al paquete en el transmisor y la desviación estándar debe ser baja. Los buffers del jitter (los buffers del paquete que

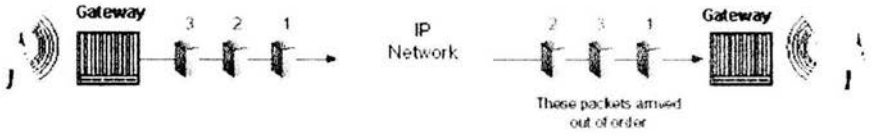
sostienen los paquetes entrantes para una cantidad especificada de tiempo) se usa neutralizar los efectos de fluctuaciones de la red y crear un flujo del paquete liso al fin receptor.



Paquetes perdidos- Típicamente ocurre en cada bursts o periódicamente debido a una red consistentemente congestionada. La pérdida periódica más de 5-10% de todos los paquetes de voz transmitidos pueden degradar la calidad de la voz significativamente. Ocasionalmente los bursts pierden el paquete además también pueden hacer difícil la conversación.



Secuencia de errores- La congestión de paquetes en las redes de conmutación puede causar que los paquetes puedan tomar rutas diferentes para alcanzar el mismo destino. Los paquetes pueden llegar fuera de orden resultando él dialogo alterado.



BIBLIOGRAFÍA.

1- UNIFIED IP INTERWORKING
DHIMAN D. CHOWDHURY
SPINGER.
2000.

2- REDES DE COMUNICACIONES.
CONCEPTOS FUNDAMENTALES Y ARQUITECTURAS BÁSICAS.
ALBERTO LEÓN-GARCÍA / INDRA WIDJAJA.
Mc GRAW HILL.
2002.

3- INTEGRACIÓN DE REDES DE VOZ Y DATOS
SCOTT KEAGY
CISCO SYSTEMS
PEARSON EDUCATION
2001.

4- PRINCIPIOS DE TRANSMISIÓN DE DATOS
A. ARTON.
RA-MA.
1999

5- TECNOLOGÍAS EMERGENTES PARA REDES DE COMPUTADORAS.
UYLESS BLACK
PEARSON EDUCATION.
2° Edic. 1999.

6- LOS SERVICIOS DE TELECOMUNICACIONES.
REDES, APLICACIONES Y COSTOS
JOSÉ A CARBALLAR F.
RA-MA.
1999

7- REDES LOCALES
J. L. RAYA / CRISTINA RAYA.
ALFAOMEGA.
2002.

8- TODO SOBRE COMUNICACIONES
JOSÉ MANUEL HUIDROBRO
PARANINFO.
3° Edic. 2000.

9- REDES DE COMPUTADORAS
MICHAEL J. PALMER
THOMSON LEARNING.
2001.

10- INTERCONECTIVIDAD
MANUAL PARA RESOLUCIÓN DE PROBLEMAS
CISCO SYSTEMS.
PRENTICE HALL
2000.

11- REDES Y SERVICIOS DE TELECOMUNICACIONES.
JOSE M. HUIDROBO MOYA.
PARANINFO.
2001.

12- RED
LA COMUNIDAD DE EXPERTOS EN REDES.
AÑO 1998, 1999, 2000, 2001.

13- TÉCNICA PCM DE 1 ORDEN / TELEFONIA PARA CONMUTACION.
INTTELMEX
1998.

Paginas de Internet.

1- http://www.dnet.com.pe.
2- http://www.comunicaciones.unitronics.es
3- http://www.recursosvoip.com.
4- http://www.red.com.mx.
5- http://www.juniper.net.
6- http://www.radcom.com
7- http://www.protocols.com
8- http://www.cisco.com.mx