UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN

"ESTÁNDAR H.323 PARA COMUNICACIONES MULTIMEDIA A TRAVÉZ DE REDES IP"

T E S I S

QUE PARA OBTENER EL GRADO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A :
ESTRADA HERNÁNDEZ YOLANDA

DIRECTOR DE TESIS:
ING. MANUEL QUINTERO CERVANTES

MÉXICO 2003

A G R A D E C I M I E T O S

A Dios

Ya que me ha dado la oportunidad de alcanzar uno de mis sueños.

A mis Padres

Leonor Hernández Cano y Jesús Estrada Quintanilla
A quienes dedico este trabajo de Tesis, por que son las dos personas que más admiro en este mundo y también por que gracias a los valores que me inculcaron, a su amor, comprensión y ejemplo he logrado una de mis metas.
Los amo.

A mis Hermanos

Eduardo, Rosa María y Jesús
Por que han sido para mi los mejores hermanos y sobre todo mis mejores amigos ya que me han ayudado a concretar muchos de mis anhelos.
Gracias por su apoyo y sus consejos

A mis Amigos

Hugol, Rosa Isabel, Oscar, Alfredo, Rocío, Felipe, Hugo, Edgar, Gregorio, Hans, a todos mis compañeros del TAC, NOC, NIC y de Tecmarketing
A todos los que me apoyaron en este trabajo de Tesis les agradezco infinitamente pero les agradezco más por brindarme su confianza y amistad.

A mi asesor

Ing. Manuel Quintero Cervantes
Gracias por todos sus consejos y por el apoyo que me brindo durante todo este tiempo ya que fue parte importante en esta trabajo de Tesis.

A la UNAM y a la DGSCA

Les agradezco por permitirme realizar mis estudios y sobre todo la formación academica que me brindarón.

ÍNDICE

CONTENIDO **PÁGINA**

INTRODUCCIÓN

En este trabajo de Tesis se presenta un tema que en estos días es muy importante ya que por medio de este podemos hacer crecer muchas áreas como es la educación, la medicina, los negocios, etc. ya que por su bajo costo y su sencillo manejo e implementación nos permite llegar a muchos lugares e incluso con el crecimiento y desarrollo de las redes de datos este ira creciendo de la mano, el hablar del estándar H.323 es hablar del surgimiento de una nueva era, una nueva era en la cual el tráfico de voz, datos y video pueden viajar juntos por la misma infraestructura de red y de esta manera hacer utilizables al 100% todos los recursos con los que contemos.
En este proyecto principalmente se hablará del estándar H.323 el cual es un estándar que fue aprobado en 1996 por la Unión Internacional de Telecomunicaciones (ITU), para promover la compatibilidad en las transmisiones de videoconferencia sobre redes IP. H.323 describe como se realizan las comunicaciones multimedia entre terminales, equipos y servicio de red, es parte del grupo mas grande de recomendaciones de la ITU, llamado H.3x, para la interoperabilidad de los multi-medios de comunicación. Por lo tanto, el estándar H.323 actualmente es el estándar de las próximas generaciones tecnológicas de teléfonos de Internet, terminales de audio y videoconferencia.

El objetivo principal de esta tesis es conocer la Arquitectura del estándar H.323 e implementar este estándar realizando algunas pruebas y demostrar la interoperabilidad que existe entre equipos de diferente proveedor y así mismo observar como se comporta la videoconferencia al variar el ancho de banda.
Esta tesis esta estructurada de manera tal, que se estime importante tanto los antecedentes y conceptos generales de las Redes de comunicaciones, así como el tema principal que es el Estándar H.323 y su implementación.

En el Primer Capítulo "Redes de Comunicaciones", se presentan antecedentes y conceptos de manera general, se presentará los procesos básicos de telecomunicaciones involucrados en la operación y funcionamiento de las redes de comunicaciones utilizadas en la actualidad. Se abarcaran los aspectos referentes a las redes de computadoras, la videoconferencia, así como la descripción de los elementos que componen a cada una de estas.

En el Segundo Capítulo " Protocolo TCP/IP", se abarca el esquema del funcionamiento del protocolo TCP/IP, el cual es el mas utilizado hasta nuestros días en lo referente a las redes de computadoras, así como los demás protocolos que lo componen, el aprovechamiento de estos en las comunicaciones entre computadoras no solamente en redes de área local, sino también al nivel de área amplia.

El Tercer Capítulo "H.323", presenta una breve reseña histórica del estándar, así como una descripción mas a detalle de su arquitectura, se hablará del estándar H.320 y del T.120 ya que son parte muy importante para el estándar H.323, de igual manera se presenta los elementos que integran este estándar así como la descripción de la forma en que trabaja H.323.

En el Cuarto y último Capítulo "Implementación de H.323", se muestra un área en donde se puede aplicar el estándar H.323 que es Videoconferencia Interactiva dentro de lo que es la Educación a Distancia, si bien es sabido esta área se encuentra en pleno crecimiento dentro de nuestro país, y con estas nuevas tecnologías podemos hacer que crezca a un paso gigantesco y que pueda llegar a muchos lugares ya que es un estándar para Videoconferencia de muy buena calidad y a un bajo costo.

CAPÍTULO I
REDES DE COMUNICACIONES

1.1 SISTEMAS ABIERTOS

En el campo tecnológico un sistema cerrado significa que una vez que una empresa adquiera computadoras de un determinado fabricante, se ve obligada a continuar adquiriendo ese fabricante, por la imposibilidad de conectar su equipo a aparatos diseñados por otros fabricantes. Esto está cambiando, ahora la tendencia son los *sistemas abiertos*, es decir, a equipos que se pueden conectar e intercambiar información con cualquier otro, sin importar la empresa y el país de que procedan. Para lograr esto, las compañías fabricantes deben ajustarse a los estándares que fijan organismos internacionales y nacionales, para hacer posible la comunicación de unos equipos con otros.

El objetivo de un sistema abierto es que un proceso corriendo en una computadora se puede comunicar con un proceso corriendo en otra computadora.

El establecimiento de normas o estándares internacionales, es muy importante para la relación de los ciudadanos de una nación con otra y para la interconexión de los sistemas de un país con los de otro. Enseguida se citan algunos sistemas para los cuales es vital el establecimiento de normas:

a) Sistema vehicular:
   En los semáforos el color verde es para "SIGA" y rojo para "ESPERE", tienen el mismo significado en todo el mundo.
b) El sistema ferroviario:

Las vías del ferr ocarril deben tener la misma forma y ancho entre rieles.

c) Sistema telefónico:

El código de colores de los pares de hilos debe de respetarse.

d) Sistema de transmisión de datos:

En base al estándar RS-232, es posible conectar una computadora aun equipo de comunicación de datos de cualquier fabricante que respete esa norma.

Organizaciones que establecen estándares:

ORGANIZACIÓN	AFILIACIÓN	INFLUENCIA
CCITT: Comité Consultivo Internacional de Telefonía y Telegrafía.	Es parte de la Unión Internacional de Telecomunicaciones (UIT).	Emite recomendaciones que son ley en los países en donde las comunicaciones son controladas por el estado.
ISO: International Standard Organization.	Relacionada con UIT.	Responsable del modelo OSI (Open System Interconnection).
ANSI: American National Standards Institute.	Organización de los EEUU.	Es la voz de los EEUU en ISO
EIA: Electronic Industries Association	Organización de los EEUU.	Es conocida por su estándar RS-232-C
IEEE: Institute of Electronic Engineers.	Sociedad Profesional.	Conocido por sus estándares para redes locales.
NBS: National Bureau of Standards.	Agencia del gobierno de los EEUU.	Emite estándares de procesamiento de datos

1.2 MODELO OSI

Para conseguir comunicación independiente de las características de las estaciones (arquitectura, sistemas operativos, etc.) se han definido arquitecturas de comunicación y familias de protocolos estándares que permiten la interconexión de sistemas abiertos.

Existen dos arquitecturas de protocolos que han servido como base para el desarrollo de comunicaciones interoperables:

- El Modelo OSI (Modelo de interconexión de sistemas abiertos) creado por ISO y la familia de protocolos ISO/OSI.
- El Modelo del DoD (Departamento de Defensa de Estados Unidos) y su familia de protocolos TCP/IP.

Otras familias de protocolos son:

- Xerox Network Systems (Xerox NS o XNS)
- Systems Network Architecture de IBM (SNA)
- NetBIOS de IBM
- UUCP (Unix to Unix Copy), etc.

El modelo de interconexión de sistemas abiertos se desarrolló en 1984, provee un marco en el que se especifican los demás estándares para los servicios y los protocolos de cada capa.*

* Fred Halsall, "Comunicación de datos, redes de computadores y sistemas abiertos", 4ta. Edición, Addison-Wesley, Iberoamericana, E.U. 1998.

OSI es una estructura o arquitectura que especifica las funciones de comunicación que deben desarrollarse con el fin de enlazar computadoras de diversos fabricantes y establecer las bases para la definición de estándares. El propósito es proveer una base común para coordinar el desarrollo de normas que hagan posible la interconexión de sistemas y proporcionar una arquitectura funcional y conceptual que permita que la información fluya a través de las redes. Además, describe la forma en que la información o los datos se trasladan desde programas de aplicación a través de un medio de red hasta otro programa de aplicación ubicado en otro equipo de una red.

El modelo OSI (ver Fig.1.2a) fue diseñado siguiendo la filosofía de la programación estructurada, en la cual el diseño de un sistema de información se hace dividiendo el trabajo global a realizar en funciones, módulos o capas más pequeñas que son más simples de diseñar y más fáciles de controlar. Cada capa o módulo tiene una función específica y cuando necesita llevar a cabo una función, utiliza los servicios de la capa o módulo inferior. Cuando este módulo termina su función, pasa el control y los datos a la capa superior.

El modelo OSI, divide las funciones de una red de computadoras en siete capas; cada capa se comunica con su igual en otro sistema remoto por medio de un protocolo. Sin embargo, la comunicación tiene realmente lugar usando los servicios de la capa inferior. La comunicación entre la capa n y la capa n-1 se conoce como *interface*. Así, cada capa presta servicios a la capa inmediatamente superior y usa los servicios de la capa inmediatamente inferior. La información fluye en forma lógica, horizontalmente usando protocolos y en forma real, verticalmente sobre interfaces. Un *protocolo* siempre conecta dos entidades al mismo nivel, es decir, la capa n de una entidad es la capa n de otra, mientras que una interfaz acopla capas de una misma entidad, por ejemplo, la capa n con la capa n-1.

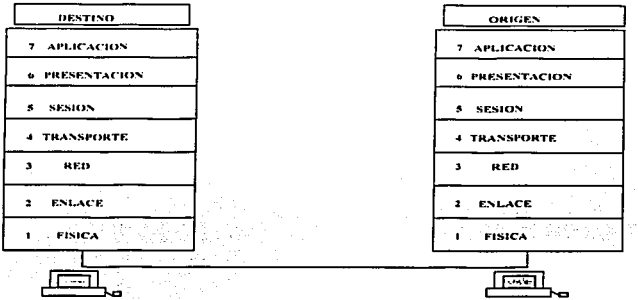


Fig. 1.2a. *Estructura en capas del Modelo OSI*

En realidad los datos no son transmitidos horizontalmente de máquina a máquina en una determinada capa, sino que son pasados verticalmente hacia abajo en la máquina transmisora y verticalmente hacia arriba en la máquina receptora. Sólo en la capa 1 ocurre comunicación real entre máquinas.

1.2.1 ENCAPSULAMIENTO

El encapsulamiento permite que las computadoras comuniquen datos. Cuando se desea enviar datos a otro host, en primer término los *datos* deben empaquetarse a través de un proceso denominado *encapsulamiento*. Luego, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, pies y otra información

El siguiente ejemplo de encapsulamiento, ilustra los cinco pasos de conversión que deben ejecutar las redes.

1. Crear los datos. Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en *datos* que pueden recorrer la red.

2. Empaquetar los datos para ser transportados de extremo a extremo. Los datos se empaquetan para ser transportados en la red. Al utilizar *segmentos*, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. Anexar (agregar) la dirección de red al encabezado. Los datos se colocan en un *paquete o datagrama* que contiene el encabezado de red con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

4. Anexar (agregar) la dirección local al encabezado de enlace de datos. Cada dispositivo de la red debe poner el paquete dentro de una *trama*. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. Realizar la conversión a *bits* para su transmisión. La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio.

1.2.2 FUNCIONES DE LAS CAPAS DEL MODELO OSI

Enseguida se resumen las funciones realizadas en cada una de las siete capas del modelo OSI:

1.- *CAPA FÍSICA:* Se especifican los requerimientos eléctricos, mecánicos y de procedimiento para activar, mantener y desactivar el enlace físico por medio de un canal de comunicación y trasmitir los datos a través de este medio. La unidad de transmisión es el bit.

Estos son:

Requerimientos Eléctricos:

- Niveles de voltaje para representar los bits.
- Base de tiempo para las señales.
- Duración de cada pulso
- Impedancia.

Requerimientos Mecánicos:

- Tipos de conectores (RS232-C RS449, RJ-45, etc.)
- Forma de los conectores
- Conexión mecánica al medio (fibra óptica, cable coaxial, par de hilos)

Requerimientos de procedimiento:

- Transmisión síncrona o asíncrona.
- Transmisión Full dúplex o half dúplex.
- Uso de cada pin en un conector.
- Código de línea.

2.- *CAPA DE ENLACE DE DATOS:* Provee a la capa de red una conexión confiable entre nodos adyacentes aún cuando el canal físico sea ruidoso. Funciones:

- Organiza los datos (paquetes) que recibe de la capa de red en tramas.
- Agrega información redundante a la trama, para permitir al receptor detectar si hubo error.
- Regula el tráfico usando búferes, para que un transmisor rápido no sature a un receptor lento.
- Agrega banderas que indican el comienzo y fin de una trama.
- Provee métodos para que las estaciones conectadas accedan al canal de comunicación.
- Empaqueta los bits que recibe de la capa física en tramas.
- Asegura la sincronía entre las computadoras que se comunican.
- Provee esquemas de direccionamiento entre múltiples nodos.

3.- *CAPA DE RED:* Establece una trayectoria física y lógica entre dos nodos que se comunican, enlaza los mensajes a través de nodos intermedios a su destino y controla el flujo de mensajes entre nodos.

Funciones:

- Establece rutas de un nodo fuente a un nodo destino, para la transmisión de paquetes.
- Direcciona los nodos intermedios en la ruta que siguen los paquetes.
- Ensambla los mensajes que recibe de la capa de transporte en paquetes y los desensambla en el otro extremo.
- Realiza el control de flujo y error.
- Reconoce prioridad en los mensajes
- Ofrece servicios de interconexión para redes por medio de routers.

4.- *CAPA DE TRANSPORTE*: Actúa como interfase entre las tres capas inferiores orientadas a comunicaciones (capas de interconexión) y las tres capas superiores están orientadas a computación (principalmente software) (capas de interoperabilidad). Provee los siguientes servicios:

- Asegura integridad de los mensajes.
- Control de flujo y control de error.
- Poleo o sondeo de los mensajes.
- Mapea direcciones a nombres, de modo que un usuario mantenga el mismo nombre en toda la red.
- Multiplexa conexiones de transporte a conexiones de red.

5.- *CAPA DE SESIÓN*: Ofrece a la capa de transporte, el servicio de establecimiento, mantenimiento y terminación de una sesión entre un proceso corriendo en una computadora y un proceso corriendo en otra.

Funciones:

- Controla el dialogo entre procesos, quién transmite, cuándo, qué tanto tiempo, etc.
- Sincronización. Restablece la comunicación si ocurre una ruptura del enlace sin perder datos.
- Transmite la información del usuario en forma ordenada.

6.- *CAPA DE PRESENTACIÓN:* Proporciona a la de aplicación mecanismos para traducir los formatos de datos del transmisor de modo que sean adecuados para el receptor. De este modo asegura al proceso de aplicación la solución de cualquier problema de sintaxis.
Sus funciones:

- Compresión de datos
- Encriptación de datos (para proporcionar seguridad en la transmisión)
- Transformación sintáctica del conjunto de caracteres (conversión de código EBCDIC a ASCII).

7.- *CAPA DE APLICACIÓN*: Provee servicios al usuario, es decir, al programa de aplicación:

- Transferencia, administración y acceso de archivos.
- Correo electrónico.
- Emulación de terminales de computadoras.
- Servicios de directorio.

Debido a que las capas inferiores (de la 1 a la 3) del modelo OSI controlan la transmisión física de mensajes a través de la red, se les denominan *capas de medios*. Por otro lado, las capas superiores (de la 4 a la 7) del modelo de referencia OSI se encargan de la transmisión precisa de datos entre equipos de la red, por lo cual se denominan *capas de host*.

1.3 REDES DE ÁREA LOCAL (LAN)

Las Redes de Área Local (LAN) permiten la interconexión de estaciones ubicadas en un área reducida y sirven a una entidad particular. Las velocidades de transmisión de datos actualmente se sitúan en el rango de 10 a 1000 Mbps. Inicialmente la instalación de una red se realiza para compartir algunos dispositivos periféricos, pero a medida que va creciendo la red, el compartir dichos dispositivos pierde relevancia en comparación con el resto de las ventajas.

Las redes enlazan también a las personas proporcionando una herramienta efectiva para la comunicación a través del Correo Electrónico, Videoconferencia y Telefonía IP. Los mensajes que pueden ser voz, datos y vídeo se envían instantáneamente a través de la red, los planes de trabajo pueden actualizarse tan pronto como ocurran cambios y se pueden planificar las reuniones en una videoconferencia sin necesidades de llamadas telefónicas tradicionales. Algunas de sus principales características son:

- Posibilidad de compartir periféricos como: impresoras, módem, fax, etc.
- Posibilidad de compartir grandes cantidades de información a través de distintos programas (bases de datos), de tal manera que sea más fácil su uso y actualización.
- Permite utilizar el correo electrónico para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de diferentes redes.
- Establecer enlaces con servidores haciendo que los recursos disponibles estén accesibles para cada una de las computadoras personales conectadas.
- Permite mejorar la seguridad y control de la información que se utiliza permitiendo la entrada de determinados usuarios, accediendo únicamente a determinada información o impidiendo la modificación de diversos datos.
- Permite alta velocidad en el envío de datos.
- Baja probabilidad de error.
- El medio de interconexión –par trenzado, cable coaxial y fibra óptica- es compartido por las estaciones.
- Se utilizan protocolos de contención para que los terminales accedan al medio y reducir las colisiones.

- El retardo de propagación depende del número de estaciones y longitud del medio.
- El ancho de banda se asigna dinámicamente.
- Los mensajes se conforman en paquetes con cabecera.

Una red está formada, principalmente por computadoras, un sistema operativo de red, los elementos de conexión y los estándares para redes definidos en las normas IEEE802. Las computadoras pueden desarrollar funciones de servidores o estaciones de trabajo y desde ellos se facilita a los usuarios el acceso a los dispositivos de red. Según el sistema operativo de red que se utilice y las necesidades de los usuarios, puede ocurrir que los distintos tipos de servidores residan en la misma computadora o se encuentren distribuidos en la red. Entre los sistemas operativos que podemos encontrar están Windows (XP, 2000, Milenium, NT, 98,95 y 3.11), Unix, Linux, entre otros. Los elementos de conexión son los cables, tarjetas de red, Repetidores, Hubs, Bridges, Switchs.

1.3.1 CONCEPTOS BÁSICOS DE REDES

1.3.1.1 TOPOLOGÍA DE REDES

En la actualidad existen estándares para redes de área local, definidas en las normas IEEE802. Cada una de ellas se diferencia por los distintos Controles de Acceso al Medio (MAC) que implementan y por su topología: bus, anillo, estrella.

La palabra topología literalmente significa "estudio de los mapas". La topología es objeto de estudio en las matemáticas, donde los "mapas" de nodos (puntos) y los enlaces (líneas) a menudo forman patrones. Examinando las

diversas topologías de una red, la *topología física* describe el esquema para el cableado de los dispositivos físicos y una *topología lógica* describe cómo fluyen los datos a través de una red para determinar el lugar donde se pueden producir colisiones.*

Una red puede tener un tipo de topología física y un tipo de topología lógica completamente distinto. 10Base-T de Ethernet usa una topología física en estrella extendida, pero actúa como si utilizara una topología de bus lógica. Token ring usa una topología física en estrella y un anillo lógico. FDDI usa un anillo físico y lógico.

Existen tres topologías fundamentales (bus, anillo y estrella) que están determinadas por el tipo de cable utilizado: el cable coaxial permite las tres topologías, mientras que el par trenzado y la fibra óptica aceptan topología en estrella. En redes más complejas se presentan topologías mixtas o híbridas que combinan varias de las formas básicas.

Existen dos tipos de conexión a una red: la conexión punto a punto y la conexión multipunto. La conexión punto a punto es una conexión entre dos dispositivos únicamente. Por ejemplo, cuando se conectan dos computadoras a través de una fibra óptica o un par trenzado.

En la conexión multipunto se utiliza un sólo cable para conectar más de dos dispositivos. Por ejemplo, cuando se utiliza un cable coaxial para unir varias computadoras.

Topología de bus. Esta es una topología de red multipunto (Fig. 1.3.1.1.a), que consiste en un cable lineal del cual cuelgan todas las computadoras de la red. En este tipo de topología, todos los dispositivos comparten el mismo medio físico de transmisión. Por ello, los mensajes que se transmiten son recibidos por los demás dispositivos de la red. En cada punto donde existe una computadora es necesario

* Robledo Sosa Cornelio, "Redes de Computadoras ". Editores e Impresos FOC 1998.

utilizar un conector en forma de T y en los extremos del cable de la red hay que poner un terminador. Los conectores T tiene dos extremos que permiten enlazar el cable de la red y la salida de la T se conecta a la computadora. La topología de bus sólo puede emplear cable coaxial, por lo que T tiene conectores BNC. Las redes con esta topología pueden ir hasta 185 m o hasta 500 m (cable coaxial grueso o delgado). El número máximo de computadoras que pueden ser conectadas bajo este esquema es de 30 a 100. Las características reales se establecen al momento de diseñar la red.

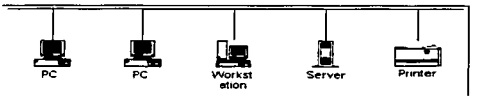


Fig. 1.3.1.1.a Topología de Bus

Topología de Anillo. La topología de anillo (Fig. 1.3.1.1.b) se caracteriza por un camino unidireccional cerrado que conecta todos los nodos. Dependiendo del control de acceso al medio, se dan nombres distintos a esta topología: **Bucle**; se utiliza para designar aquellos anillos en los que el control de acceso está centralizado (una de las estaciones se encarga de controlar el acceso a la red). **Anillo**: se utiliza cuando el control de acceso está distribuido por toda la red. Como las características de uno y otro tipo de la red son prácticamente las mismas, utilizamos el término anillo para las dos. En cuanto a fiabilidad, presenta características similares al **Bus**: la avería de una estación puede aislarse fácilmente, pero una avería en el cable inutiliza la red. Sin embargo, un problema de este tipo es más fácil de localizar, ya que el cable se encuentra físicamente dividido por las estaciones. Las redes de éste tipo, a menudo, se conectan formando topologías físicas distintas al anillo, pero conservando la estructura lógica (camino lógico unidireccional) de éste. Un ejemplo de esto es la topología en anillo / estrella, la cual presenta un tipo de conexión, donde todas las computadoras se conectan en círculo alrededor de un concentrador, que es el

encargado de formar eléctricamente el anillo a medida que se insertan más computadoras. En esta topología los mensajes viajan en una sola dirección y son leídos por cada computadora en forma individual y retransmitidos al anillo en caso de no ser el destinatario de un determinado mensaje. No existe un número máximo de computadoras conectados debido a que no se comparte un medio único.

Fig. 1.3.1.1.b Topología de anillo

Topología en estrella. Ésta también (Fig. 1.3.1.1.c) es una topología de red punto a punto, cada computadora está conectada a un concentrador. También se le denomina topología de concentradores. En esta topología el concentrador se encarga de distribuir adecuadamente los paquetes de datos desde la computadora que los envía hasta la que los recibe. La topología de estrella ofrece un mejor rendimiento, ya que los datos no van pasando de una computadora a otra hasta llegar al destinatario tal como ocurre en las redes con topología bus o anillo, sino que directamente van desde la computadora de origen al de destino. Si desea utilizar una red con cable par trenzado o fibra óptica, es obligatorio utilizar una topología en estrella.

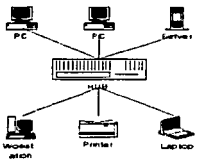


Fig. 1.3.1.1.c Topología en Estrella

1.3.1.2 ADAPTADORES DE RED

Una red de datos está formada por adaptadores o tarjetas de red que habiliten a la PC para conectarse a la red; un cable entre los adaptadores a través del cual viajan los datos y, finalmente una determinada topología o estructura de la red.

Lo primero que se requiere para conectar una computadora con otra es un adaptador o tarjeta de red. Algunas computadoras incorporan un adaptador de red integrado en la placa madre, pero habitualmente se instala una tarjeta de red en una de las ranuras de expansión; existen tarjetas de red para bus ISA y para bus PCI con soporte Plug and Play. Los adaptadores de red se clasifican según el método de acceso al cable de red (más exactamente, la manera en que señalizan el uso del cable), distinguiendo entre ARCNet, Token-Ring, ATM y Ethernet.

- *Adaptadores ARCNet.* Prácticamente en desuso. Los adaptadores ARCNet pueden trabajar con cable coaxial o líneas de fibra óptica y alcanzar una velocidad máxima de 2.5 Mbps.
- *Adaptadores Token Ring.* Utilizados principalmente en entornos de computadoras IBM. Los adaptadores Token Ring trabajan con cable

coaxial y las más comunes ofrecen una velocidad de 4 Mbps y 16 Mbps, aunque existen redes Token Ring a mayor velocidad.

- *Adaptadores ATM.* Los adaptadores de red ATM (Asynchronous Transfer Mode; Modo de Transferencia Asíncrona) son los más modernos y el futuro estándar en redes ofreciendo velocidades hasta de 10 Gbps (gigabits por segundo) en computadoras conectados por cables de fibra óptica. La principal caracteristica de los adaptadores ATM es que al transmitir datos entre dos computadoras de la red se crea una conexión directa entre ellos, mucho más rápida, pero tiene el inconveniente de que resultan muy caros y lejos del alcance de la mayoria de las empresas.
- *Adaptadores Ethernet.* Estos adaptadores ofrecen velocidades desde 10 Mbps (Ethernet original), 100 Mbps (FastEthernet) hasta 1000 Mbps (Gigabit Ethernet). Estos pueden utilizan los tres tipos de cables principales: coaxial, par trenzado y fibra óptica (dependiendo de la norma a utilizar).

Todos los adaptadores de red poseen en sus propios chips un número de 6 bytes impresos de fábrica, que les identifican de forma exclusiva y que pueden proporcionar a las aplicaciones que lo soliciten. La mayoría de los protocolos de red (excepto TCP/IP) utilizan ese número del adaptador de red, para identificar de forma univoca a cada miembro de una red.

1.3.1.3 MEDIOS DE TRANSMISION

Antes de ser instalado un adaptador de red, es necesario decidir el medio que lo va a unir y por el cual viajarán los datos. Se entiende por medio de transmisión a cualquier medio fisico que pueda transportar información en forma de señales electromagnéticas. Para efectuar la transmisión de la información se utilizan las técnicas de transmisión que pueden ser de banda base o banda ancha.

Las redes de banda ancha se caracterizan por operar con tecnología analógica: utilizando un módem para inyectar en el medio de transmisión señales portadoras, que son después modificadas por una señal digital. Debido a su naturaleza analógica, suelen estar multiplexadas por división de frecuencia (FDM), lo cual permite transportar múltiples portadoras y subcanales por un mismo camino. La denominación de banda ancha se debe a que se trabajan en una banda de frecuencia de radio de alta frecuencia (entre 10 y 400 MHz). Los elementos de conexión que pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

Las redes de banda base utilizan tecnología digital. Un controlador de la línea introduce en el canal variaciones de tensión. El canal se comporta como un mecanismo de transporte a través del cual se propagan estos pulsos digitales. Las redes de este tipo no consiguen el acceso múltiple al medio empleando portadoras analógicas, ni técnicas FDM, sino mediante multiplexado por división en el tiempo (TDM) o diversos protocolos. Los elementos de conexión que se pueden utilizar son: el cable de par trenzado y el cable coaxial de banda base.

Los tres tipos de cables más utilizados son coaxial, par trenzado y fibra óptica, pero existen otros medios como son Microondas, Radio UHF y Láser.

- *Cable coaxial y conector BNC.* El cable coaxial contiene un hilo de cobre en la parte central que es rodeada por un cilindro de plástico y después, por una maya. Soporta comunicaciones en banda base y en banda ancha; además ofrece mayor protección que el par trenzado frente a las interferencias externas. El cable coaxial de banda base, se usa para datos y para los sistemas de antenas colectivas de televisión. En función de sus características se clasifican en dos categorías: cable coaxial grueso (Utilizado en el estándar 10Base5) y cable coaxial delgado (Estándar 10Base2).

- *El cable coaxial grueso (Empleado en la norma 10base5)*, tiene un grosor que varia de 1 cm. a 0.5 pulgadas, lleva un conector tipo N, alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 500mts de segmento de red. También se denomina Thick Ethernet.
- *El cable coaxial delgado (Empleado en la norma 10base2)*, tiene un grosor de 0.25 pulgadas lleva un conector tipo BNC, alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 200 metros de segmento de red.
- El cable coaxial de banda ancha, está construido muy similar al coaxial de banda base aunque puede tener mayores diámetros y con diversos grosores de aislamiento. Su impedancia es de 75 ohms. Alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 1,800 metros de segmento de red. Puede transportar miles de canales de datos a baja velocidad.

- *Cable par trenzado*
  - El cable par trenzado, denominado UTP (Unshielded Twisted Pair; par trenzado sin apantallar) es similar al utilizado como cable telefónico, pero con algunas diferencias. El cable telefónico tiene 2 hilos y utiliza conectores RJ11 donde se enchufan teléfonos, módems, etc. Por el contrario, el par trenzado tiene dos pares de cable (4 hilos), al adquirir un cable par trenzado es fundamental conocer la categoría del cable, que define la velocidad máxima de transmisión de datos. Los cables UTP con categoría 3 (velocidad máxima de 16 Mbps) y categoría 4 (velocidad máxima de 20 Mbps) son suficientes para las redes Ethernet a 10 Mbps o Token Ring desde 4 a 16 Mbps. Pero si se trabajara con Ethernet a 100 Mbps (FastEthernet), se requiere un cable con categoría 5

(velocidad máxima 100 Mbps.). La categoría 6 es para transmisiones de 1000 Mbps y se utiliza en el Gigabit Ethernet

- STP (Shielded Twisted Pair; par trenzado apantallado) Cable en el cual los conductores van trenzados por parejas, y cada pareja de estas es cubierta por una capa metálica que hace de pantalla, es más caro que el UTP, pero supera los 100 Mbps.
- FTP(Foiled Twisted Pair), Es un cable de pares trenzados envuelto por una lámina, esta reduce las emisiones al exterior del propio cable y le protege de las interferencias que le pudiera inducir por las radiaciones.
- S-UTP Combina las ventajas del STP con el UTP. Es un cable UTP recubierto con una malla y una lámina, con lo cual presenta una mejor protección frente a radiaciones de alta y baja frecuencia.

- *Cables y conectores de fibra óptica.* La tecnología de fibra óptica transmite la información como pulsos de luz a través de un cable de fibra de vidrio. Ofrece una velocidad muy superior a la de los cables coaxial y par trenzado, pero es mucho más cara y su instalación y mantenimiento exige cuidados profesionales. Los cables de fibra óptica transportan los datos transmitidos en forma de un haz de luz fluctuante dentro de una fibra de vidrio y no como una señal eléctrica, las ondas de luz tienen un ancho de banda muy superior al de las ondas eléctricas lo que le permite al cable de fibra óptica alcanzar tazas de transmisión de cientos de mega bits por segundo, además las ondas de luz son inmunes a la interferencia electromagnética y a la diafonía. Un cable de fibra óptica utiliza fibra de vidrio individual para cada señal que se va a transmitir encerrada por el recubrimiento protector del cable que también protege a la fibra de cualquier fuente de luz externa. La fibra consta de 2 partes: el núcleo de vidrio y un revestimiento de vidrio con un índice de

refracción menor, la luz se propaga a lo largo del núcleo de fibra óptica.*

Los componentes que lo forman son:

- *Transmisor de energía óptica.* Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica en una señal óptica que se emite a través de la fibra óptica.
- *Fibra óptica.* Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica.
- *Detector de energía óptica.* Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal).

Este cable no capta ninguna interferencia electromagnética; la instalación es muy cara debido al alto costo del cable y al equipo que se necesita para realizarlo. Entre los tipos de conectores que existen esta el SC y ST.

- *Radio UHF.* Un radio en UHF necesita para su instalación la obtención de una licencia administrativa. No se ve interrumpida por cuerpos opacos gracias a su cualidad de difracción.
- *Microondas.* Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las super-altas frecuencias, utilizándose para las redes inalámbricas la banda de los 18-19 Ghz.

* Fred Halsall, "Comunicación de datos, redes de computadores y sistemas abiertos", 4ta. Edición, Addison-Wesley, Iberoamericana, E.U. 1998.

- *Láser.* Esta tecnología para redes inalámbricas es útil para conexiones punto a punto con visibilidad directa y se utiliza, para interconectar segmentos distantes de redes locales convencionales Ethernet, Token Ring, llegando a cubrir distancias de hasta 1,000 metros.

1.3.2 TIPOS DE REDES LAN

Los tipos comunes de redes LAN de media velocidad (2.5 a 16 Mbps) son los siguientes:
Ethernet (10 Mbps)
Token Ring (4 y 16 Mbps)
Arcnet (2.5 Mbps)

Y las redes LAN de alta velocidad (100 – 1000 Mbps) son:
FDDI
FastEthernet
100VG-AnyLan
Gigabit Ethernet
Fiber Channel

1.3.2.1 RED ETHERNET

Ethernet originalmente fue desarrollado como un experimento de red con cable coaxial en los años de 1970 por Xerox para operar con un rango de datos de 3Mbps usando (CSMA/CD Carrier Sense Múltiple Access/Colisión Detection). Satisfactoriamente aquel proyecto atrajo la atención y permitió que en 1980 la compañía Xerox junto con Digital Equipment Corporation, Intel Corporation comenzaran a desarrollar la versión 1.0 de Ethernet.

El estándar IEEE 802.3 es muy similar a la versión 1.0 de Ethernet el estándar fue aprobado en 1983 y subsecuentemente fue publicado como un estándar oficial en 1985(ANSI/IEEE Std 802.3-1985).

Esta red LAN usa el método de acceso (CSMA/CD) en el cual la Pc's compiten por el uso del medio de comunicación. En este método, cuando una PC desea transmitir un paquete de datos, sensa el canal para ver si hay señal portadora. Si la hay, significa que el canal está ocupado y la PC espera antes de sensarlo otra vez. Si la PC no detecta una portadora, significa que el canal está libre y procede a enviar su paquete.

Por la forma de sensar la portadora el método se llama *Carrier Sense (sesor de portadora)* y como el medio puede ser accesado por múltiples PCs, se le agrega *Múltiple Access (Accesso múltiple)*. Así el nombre del método es *Carrier Sense Múltiple Access (CSMA)*.

Con esta técnica hay el problema de que cuando dos PCs desean trasmitir un paquete, sensan el canal y no detectan portadora, ambas transmiten su paquete al mismo tiempo, por lo que provoca colisión de un paquete con otro. Para solucionar este problema Ethernet usa la técnica de detección de la colisión *(Collision Detection: CD)*, mediante la cual una PC trasmite su paquete tan pronto como ve el canal libre luego monitorea la transmisión. Si detecta colisión, trasmite una señal de alarma alertando a todas las PCs para que eviten la transmisión de paquetes porque ha ocurrido una colisión.

Después de un tiempo aleatorio, la PC intenta otra vez la transmisión, detectando primero si hay portadora y procede a trasmitir una trama si no la detecta. Con este método el acceso a la red es aleatorio, lo cual significa que una PC tiene una probabilidad de acceder la red en un momento dado, pero ese acceso no está garantizado.

El formato de la trama Ethernet (Fig. 1.3.2.1a) es el siguiente:

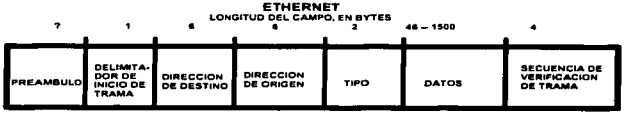


Fig. 1.3.2.1a. Trama Ethernet

Donde:

- *Preámbulo* : permite al receptor sincronizarse con el transmisor, contiene una secuencia de 7 octetos, cada octeto tiene el formato 10101010.
- *Inicio de trama (SOF)*: El byte delimitador de IEEE 802.3 finaliza con dos bits 1 consecutivos(10101011), que sirven para sincronizar las porciones de recepción de trama de todas las estaciones de la LAN. SOF se especifica explícitamente en Ethernet.
- *Direcciones de destino y de origen*: Los primeros 3 bytes de las direcciones son especificados por IEEE según el proveedor o fabricante. El proveedor de Ethernet o IEEE 802.3 especifica los últimos 3 bytes. La dirección de origen siempre es una dirección de unicast (de nodo único). La dirección de destino puede ser de unicast, de multicast (grupo) o de broadcast (todos los nodos).
- *Tipo (Ethernet)*: El tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.
- *Datos (Ethernet)*: Una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos contenidos en la trama se envían a un protocolo de capa superior, que se identifica en el campo tipo. Aunque la versión 2 de Ethernet no especifica ningún relleno, al contrario

de lo que sucede con IEEE 802.3, Ethernet espera por lo menos 46 bytes de datos.

- *Secuencia de verificación de trama (FCS)*: Esta secuencia contiene un valor de verificación por redundancia cíclica de 4 bytes (CRC), creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

1.3.2.1.1 TOPOLOGÍA DE LA RED ETHERNET

La topología lógica de la red Ethernet es de tipo bus lineal con una longitud máxima de 2.5 Kms y una velocidad de transmisión de *10* Mbps sobre un cable de banda base (coaxial grueso 10base5) y un máximo de 1024 estaciones de trabajo o PCs conectadas.

Tipos de redes Ethernet: básicamente hay 3 tipos de redes Ethernet 10BASE-5 en bus, 10BASE-2 bus, 10BASE-T en estrella bus.

La red Ethernet 10BASE-T. El cable usado por 10BASE-T es un par de hilos trenzados y la topología es físicamente una estrella aunque lógicamente sigue siendo un bus lineal.

1.3.2.2 TOKEN RING

La recomendación 802.5 del IEEE define una red basada en la tecnología la red Token Ring dentro de la topología de anillo. En esta configuración el medio lo constituyen enlaces punto a punto entre las estaciones; cada una recibe los datos y los retransmite si no son para ella. Mientras no haya nadie que transmita

circulará un pequeño paquete de bits llamado *Token* (testigo) que será continuamente retransmitido por las estaciones sin mensajes por enviar. Cuando una lo reciba y desee transmitir, lo toma retirándolo de la circulación y colocando en el enlace el paquete de datos que desea enviar; al concluir la transmisión retira los datos del medio, repone el token y lo envía hacia la siguiente estación.

En el caso de las redes Token Ring la red no necesariamente tiene que conformar un anillo físico, ya que existe un dispositivo denominado MAU (Multi-station Access Unit) que actúa como el centro de una estrella situada en la red, soportando hasta 7 terminales o utilizando una de sus salidas para conectar otra MAU. En caso de alguna incidencia en los terminales conectados a la MAU, ésta lo detecta y elimina de la red para evitar un corte en el flujo.

Como generalidades podemos mencionar que puede utilizarse fibra óptica para los enlaces, así como par trenzado y cable coaxial; las velocidades están comprendidas entre 1 y 16 Mbps, la máxima distancia entre estaciones es de 100 metros; El retardo de propagación está limitado y condicionado por las lecturas que haga cada estación del token y por la longitud del enlace. Un anillo soporta hasta 33 MAU y 260 estaciones, aunque la red puede extenderse más allá de estos límites mediante el empleo de puentes (bridges) y encaminadores (routers).

Con tráfico relativamente intenso es como más eficientemente opera esta técnica, en comparación con la CSMA/CD, ya que en caso de alta carga la degradación es lineal, al contrario de lo que sucede con CSMA/CD. Se recomienda cuando el tráfico generado por las estaciones es prácticamente continuo; en el caso en que el tráfico generado sea a ráfagas se recomienda el empleo de una red CSMA/CD.

1.3.2.3 FDDI (INTERFASE DE DATOS DISTRIBUIDA POR FIBRA)

Como se detalla en 1.3.2.1, las redes locales han operado desde la década de los ochenta a velocidades de 2.5Mbps (Arcnet), 4-16Mbps(Token Ring) y 10Mbps(Ethernet). Con el desarrollo de nuevas implementaciones se han agregado aplicaciones como videoconferencia y transferencia de archivos por mencionar algunas, que necesitan ser satisfechas con velocidades más altas de las proporcionadas por redes típicas.

La técnica FDDI –interface de datos distribuida sobre fibra óptica-, empleada para la construcción de redes MAN, es del tipo de paso de testigo en anillo con alto rendimiento, operando a 100 Mbps. Cubre superficies de hasta 100 km de radio, pudiendo tener hasta un máximo de 1000 estaciones conectadas.

Aunque funciona a velocidades más altas, la FDDI es similar al token ring. Las dos redes comparten muchas características, incluyendo la topología (anillo), la técnica de acceso al medio (transmisión de tokens), las características de confiabilidad (anillos redundantes) y otras características.

Una de las características de FDDI es el uso de la fibra óptica como medio de transmisión. La fibra óptica ofrece varias ventajas con respecto al cableado de cobre tradicional, como, por ejemplo:

- Seguridad: La fibra no emite señales eléctricas a las que se pueda acceder sin permiso.
- Confiabilidad: La fibra es inmune a la interferencia eléctrica.
- Velocidad: La fibra óptica tiene un potencial de rendimiento mucho mayor que el del cable de cobre.

FDDI define los dos tipos especificados de fibras: *monomodo*, y *multimodo*. Los modos se pueden representar como haces de rayos luminosos que entran a la

fibra a un ángulo particular. La fibra monomodo permite que sólo un modo de luz se propague a través de la fibra, mientras que la fibra multimodo permite que múltiples modos de luz se propaguen a través de la fibra. Como los diferentes modos de luz que se propagan a través de la fibra pueden recorrer distintas distancias (según los ángulos de entrada), y de esta manera llegan a su destino en distintos momentos (un fenómeno que se denomina dispersión modal). La fibra monomodo permite un ancho de banda mayor y distancias de tendido de cable más extensas que la fibra multimodo. Debido a estas características, la fibra monomodo se usa a menudo para la conectividad *entre* edificios mientras que la fibra multimodo se usa a menudo para la conectividad *dentro* de un edificio. La fibra multimodo usa los LED como dispositivos generadores de luz, mientras que la fibra monomodo generalmente usa láser.

FDDI especifica el uso de anillos dobles para las conexiones físicas. El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Uno de los dos anillos FDDI se denomina anillo primario, y el otro, anillo secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.

Las estaciones Clase B, o estaciones de una conexión *(SAS)*, se conectan a un anillo, mientras que las Clase A o estaciones con doble conexión *(DAS)*, se conectan a ambos anillos. Las SAS se conectan al anillo primario a través de un *concentrador*, que suministra conexiones para múltiples SAS. El concentrador garantiza que si se produce un fallo, o una interrupción en el suministro de alimentación, en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando los PC, o los dispositivos similares que frecuentemente se encienden y se apagan, se conectan al anillo.

En el gráfico (Fig. 1.3.2.3a) aparece una configuración FDDI típica con DAS y SAS.

Cada DAS de FDDI tiene dos puertos, que se designan A y B. Estos puertos conectan a la estación con el anillo doble FDDI; por lo tanto, cada puerto proporciona una conexión para el anillo primario y el anillo secundario.

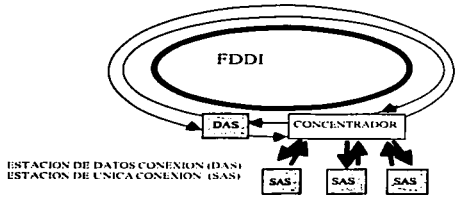


Fig. 1.3.2.3a. FDDI: Nodos DAS, SAS

1.3.2.4 FAST ETHERNET

Las redes Fast Ethernet usan la subcapa MAC original de Ethernet principalmente el mecanismo de control de acceso al medio CSMA/CD y se rigen por el estándar IEEE 802.3u. Esta moderna arquitectura de red permite transmitir a una velocidad de 100 Mbps e incluye también tres modelos de capas físicas dependiendo del tipo de medio que se esté usando: UTP cat.5 ó 3 y cable de Fibra óptica. Algunas características de las redes Fast Ethernet son:

- Están construidas con equipos (hubs, switches) 100BaseTX ó 100BaseFX distribuidos que utilizan líneas dedicadas para cada computadora.
- Las normas existentes son: 100BaseTX, 100BaseFX y 100BaseT4. 100BaseTX usa dos de los cuatro pares de hilos, que debe ser de categoría 5 o 6.

- La distancia del cable 100BaseTX al concentrador o switch no debe exceder los 100 metros.
- Emplea el método de codificación 4B/5B en el cual, secuencias de 4 bits son codificados en secuencia de 5 bits, por lo que el reloj de transmisión debe de ser de 125 Mhz para que la transferencia de datos sea de 100Mbps
- El protocolo puede operar tanto a 100 Mbps como a los 10 Mbps de la Ethernet clásica. Para ellos los adaptadores pueden identificar el tipo de equipo al que están conectados y seleccionar dinámicamente el modo de operación.
- Necesita tarjetas de red específicas para la velocidad de transmisión de 100Mbps.
- Al igual que la arquitectura de red Ethernet, utiliza el protocolo CSMA/CD y su costo de instalación es similar.

1.4 REDES DE AREA AMPLIA (WAN)

Las WAN operan más allá del alcance geográfico de una LAN, ya que utilizan conexiones en serie de distintos tipos para acceder al ancho de banda en áreas geográficas amplias. Al utilizar estos servicios para acceder al ancho de banda, brindan conectividad ya sea continua o parcial y permiten acceder a interfaces en serie que funcionan a distintas velocidades.

De acuerdo a su definición, una WAN conecta dispositivos que están separados por áreas extensas. Entre los dispositivos de WAN incluyen:

- Router: filtra y determina la ruta hacia su destino; se utiliza tanto en redes de área local como en redes de área externa.
- Switches, que se conectan al ancho de banda WAN para la comunicación de voz, datos y video.
- Módems, que realizan interfaz entre servicios de grado de voz, unidades de servicios de canal - unidades de servicio de datos (CSU-DSU) que realizan interfaz con los servicios T1-E1; dispositivos de adaptador de terminales de red, que realizan interfaz con los servicios de Red digital de servicios integrados (ISDN).
- Servidores de comunicación, que concentran la comunicación telefónica entrante y saliente del usuario.

Los estándares de la WAN son definidos y administrados, por autoridades incluyendo las siguientes entidades:

- El sector de normalización de las telecomunicaciones de la Unión de Telecomunicaciones Internacional (ITU-T), antiguamente (CCITT).
- Organización Internacional para la Normalización (ISO).
- Asociación de Industrias Electrónicas (EIA).

Los estándares WAN típicamente describen los requisitos de la capa física y de la capa de enlace de datos. Los protocolos de la capa física describen como realizar las conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios WAN. Estos servicios a menudo se obtienen de los proveedores de servicios de WAN, como ejemplo, las empresas que operan a nivel regional y entidades de correo, telefónicas y telegráficas.

La capa física de la WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de transmisión de datos (DCE). El DTE es un dispositivo ubicado en el extremo del usuario de una interfaz de red de usuario que sirve como origen de los datos, destino de los datos o ambas cosas. El DCE ofrece una

conexión física con la red, envía tráfico y proporciona una señal de temporización que se utiliza para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Normalmente DCE es el proveedor de servicios y el DTE es el dispositivo adjunto. En este ejemplo los servicios que se ofrecen al DTE están disponibles a través de un módem o CSU-DSU.

Varios estándares de la capa física especifican esta interfaz:

- EIA-TIA 232, estándar de interfaz común que soporta circuitos sin equilibrar a velocidades de señales de hasta 64 kbps.
- V.24, Un estándar ITU-T para una interfaz de la capa física entre DTE y DCE.
- V.35, describe un protocolo de capa física síncrona que se utiliza para la comunicación entre dispositivos de acceso a la red. Se recomienda para velocidades de hasta 48 kbps.

1.4.1 WAN Y LA CAPA DE ENLACE DE DATOS

Varias encapsulaciones de enlace de datos comunes, están asociadas con las líneas síncronas en serie:

- HDLC (Control de Enlace de Datos de Alta Capa), es un protocolo de enlace de datos síncrono orientado a bit desarrollado por la ISO. Especifica un método de encapsulamiento de datos para enlaces síncronos en serie que utilizan caracteres de trama y suma de comprobación. HDLC soporta tanto la configuración punto a punto como las configuraciones multipunto.
- Frame Relay (Transmisión de Tramas), utiliza instalaciones digitales de alta calidad. Al utilizar una trama simplificada sin mecanismos de

corrección de errores, además puede enviar información de la capa 2 muy rápidamente, en comparación con otros protocolos WAN.

- PPP (Protocolo punto a punto), suministra conexiones router –a- router y host a red a través de circuitos síncronos y asíncronos. PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- ISDN, es un conjunto de servicios digitales que transmite voz y datos. Además, es un protocolo de comunicación ofrecido por las empresas telefónicas, que permiten que las redes telefónicas transporten datos, voz y otro tráfico de origen.

1.4.2 FRAME RELAY

Es un protocolo de conmutación de paquetes que se fragmentan en unidades de transmisión llamadas "tramas" y se envían en ráfagas de alta velocidad de 64 kbps hasta 2048 Mbps a través de una red digital. Establece una conexión exclusiva durante el periodo de transmisión denominado "conexión virtual".

Utiliza una tecnología denominada de paquete rápido en la cual el chequeo de errores no se produce en ningún nodo intermedio de la transmisión si no que se hace en los extremos (estaciones no conectadas al sistema Frame Relay). Esto hace que sea más eficiente que X.25 y pueda transmitir por encima de 2.044 Mbps.

Otras de las ventajas son que necesita centros de conmutación (nodos) menos potentes y con menos capacidad de memoria que lo necesitado por X.25. Si el tráfico es muy intenso, con una gran cantidad de paquetes de pequeña longitud, su rendimiento es superior a X.25. Si se transfieren grandes archivos a altas velocidades, la relación precio/rendimiento es superior en X.25.

Las aplicaciones que corran en redes con tecnología Frame Relay deben de ser tolerantes a retardos variables. En este caso cae la transmisión de datos pero no aplicaciones del tipo de transmisiones de voz o video digital.*

El protocolo usado por Frame Relay en la capa de enlace de datos es el LAP-D que es un subconjunto del protocolo DIC. El formato de la trama LAP-D de Frame Relay es el siguiente:

- Flag, que es la secuencia de bits 01111110 que indica inicio y fin de la trama.
- CRC, el campo CRC es una secuencia de bits generados de los campos de encabezado y datos en base al algoritmo CRC y su función es permitir al receptor detectar si ha habido error en la comunicación.
- Datos, en este campo se ubica el paquete de transmisión que Frame Relay recibe de las capas superiores y puede variar de 262 a 8000 bytes, dependiendo de la longitud del paquete de datos que recibe de la aplicación.
- El encabezado de una trama frame Relay tiene los siguientes campos:
    - DLCI (Data Link Connection Identifier) este campo identifica el circuito virtual por donde se transmitirá esta trama. La primera parte del DLCI (MSB: most significant bit) es de 6 bits y la segunda DLCI (lsb:less significant bit) es de 4 bits. Así que en total se tienen 10 bits para el campo DLCI con lo que se pueden tener hasta 1024 circuitos virtuales.
    - CR (1 bit) no se usa actualmente.

* Robledo Sosa Cornelio, "Redes de Computadoras ". Editores e Impresos FOC 1998.

- FN (1 bit) y BN (1bit), se emplean para señalizar que existe congestión de la red.
- DE (1 bit) (Discard Elegibility) se usa para indicar tramas que pueden ser descartadas en condiciones de congestión de la red.

Características importantes son:

1. Soporta velocidades de 64 kbps a 2048Mbps
2. El tamaño de datos de la trama va de 262 a 8000 bytes
3. No hace funciones de control de flujo ni de control de errores como x.25, sino que deja esas funciones a protocolos de capa superior como TCP.
4. Es apropiado para operar bajo medios de comunicación poco ruidosos con un régimen de error 10^{-9} como fibra óptica.
5. Descarta las tramas que son detectadas con error sin avisar al emisor.
6. Opera a velocidades mayores que X.25 en virtud de que no hace las funciones correspondientes a la capa de red como control de flujo y de error.
7. Opera bajo los estándares Q.922 y Q.923 de la ITU.

1.4.3 ATM (Asynchronous Transfer Mode)

En 1988, CCITT (actualmente ITU) designó a ATM como el mecanismo de transporte planeado para el uso de futuros servicios de banda ancha. ATM es un circuito de transmisión de datos digitales de alta velocidad que en condiciones experimentales ha llegado a transferir datos hasta 2. 448 Gbps. La IEEE Spectrum asegura que esta velocidad se podrá incrementar en un futuro a los 10 Gbps.

ATM organiza los datos en celdas de tamaño de 53 bytes. Es asíncrono porque transmite a través de la red sin tener que ocupar fragmentos específicos de tiempo en alineación de paquetes. Individualmente, cada celda está formada por 48 bytes de datos precedidos de 5 bytes de información que se colocan en la cola de salida a la espera de ser multiplexada. Además, es una tecnología orientada a conexión, una vez que se establece la conexión, las celdas se distribuyen porque cada una de ellas contiene una cabecera que identifica la conexión de la celda a la cual pertenece.

ATM define dos interfaces que son: UNI (User Network Interface) y NNI (Network-Network Interface). UNI une un dispositivo de usuario a la red ATM y NNI describe una conexión entre dos nodos ATM. Dentro de UNI hay desarrolladas dos interfaces públicas: una de 45 Mbps y otra de 155 Mbps y tres privadas: una de 100 Mbps y dos de 155 Mbps (la interfaz estándar internacional SDH/SONET de 155 Mbps que permiten interoperabilidad entre públicas y privadas).

Como ATM es una red orientada a conexión, un enlace entre dos puntos empieza cuando uno transmite una solicitud a través de la UNI a la red. Un dispositivo responsable de la señalización pasa la señal a través de la red a su destino. Si el sistema indica que se acepta la conexión. Un circuito virtual se establece a través de la red ATM entre los dos puntos. Ambas interfaces contienen mapas para que las celdas puedan ser transferidas correctamente.

Cada celda contiene los siguientes campos:

- Un campo de bit reservado para uso futuro.
- Un campo de 8 bits denominado HEC (Header Error Control) que se utiliza para detectar errores.
- Un campo de 4 bits denominado Generic Flow Control que en un futuro servirá para permitir al usuario crear una conexión a uno o varios terminales.

- Un campo de 2 bits denominado Maintenance Payload Type que indica a un nodo ATM si la celda se está usando para mantenimiento de la red o es para uso normal.

- Un campo de 1 bit denominado Priority Type Identifier (PTI) que se utiliza para distinguir entre celdas con diferentes prioridades.

- Un campo de 8 bits formado por un identificador de ruta virtual denominado VPI (Virtual Path Identifier) que se utiliza para indicar la ruta de transmisión (este campo tiene una longitud de 12 bits en una interfaz NNI).

- Un campo de 16 bits formado por un identificador de circuito virtual VCI que se utiliza para indicar la ruta de transmisión.

ATM es totalmente transparente a cualquier protocolo. La carga de cada celda es pasar por el nodo ATM sin ser leída a nivel binario. ATM utiliza el concepto de control de error y flujo entre puntos finales, en contraste a una red convencional de paquetes conmutado que utiliza un control de error y flujo interno.

Algunos rasgos importantes de ATM son:

- Aunque es una tecnología orientada a conexión, también provee el servicio de tráfico sin conexión a través del uso de capas de adaptación.

- Maneja el concepto de circuitos virtuales proporcionando servicios de circuitos virtuales permanentes (PVC) y circuitos virtuales switcheados (SVC).

- Una conexión virtual de ATM permite la transmisión de señales de voz, video y datos, es decir, el rango de servicios prestados cubre:

voz, paquetes de datos (IP, Frame Relay), video, imagen y emulación de circuitos.

- ATM ofrece el potencial para estandarizar una arquitectura de red con técnicas de multiplexaje y switcheo que permiten usar SONET como base de transmisión física para velocidades muy altas (155 y 622 Mbps).

- Las normas o estándares para la tecnología ATM son fijados por ITU-T y el forum ATM.

1.5 VIDEOCONFERENCIA

La videoconferencia permite a un grupo de personas ubicadas en lugares distantes llevar a cabo reuniones como si estuvieran todas en una misma sala.

Un sistema de videoconferencia es una herramienta, como un teléfono o un fax. Pero además representa un arma estratégica en un mercado de información de alta competitividad. El compartir información de manera eficaz y económica es un requisito para sobrevivir en todas las áreas de la industria, negocios, gobierno, educación y entretenimiento.

La videoconferencia es un método de comunicación que permite el intercambio bidireccional, interactivo y en tiempo real, de vídeo, audio, gráficos y datos entre zonas o puntos diferentes. Con esto, se evitan los gastos y pérdida de tiempo que implican el traslado físico de la persona, todo esto a costos cada vez más bajos y con señales de mejor calidad. *

Facilidad de transmisión de información: la videoconferencia permite transmitir información desde un pizarrón hasta archivos de computadora; pues el sistema de videoconferencia acomoda virtualmente todas las cosas que podrían requerirse

* James R. Wilcox, "Videoconferencing, The Whole Picture", Telecom books, CMP Media, U.S.A, Canada

para llevar acabo una reunión exitosa, se pueden hacer uso de proyectores, transparencias, videograbadoras, pizarrones, etc.

Estas ventajas hacen a la videoconferencia el segmento de mayor crecimiento en el mundo real de las telecomunicaciones.

Existen dos posibles formas que se utilizan para llevar a cabo una videoconferencia que son: Sala de videoconferencia y Sistemas de videoconferencia de escritorio. Los parámetros que diferencian uno del otro son la interacción, participación y control.

Salas de conferencia, las cuales permiten la conexión a través de satélites a otros equipos con calidad de estudio, ofreciendo resultados altamente satisfactorios pero con un coste muy elevado. Y ésta se lleva a cabo mediante un CODEC (Codificador/Decodificador) dedicado.

El CODEC es un dispositivo electrónico que transmite y recibe señales de video que verán los participantes de la videoconferencia. Puede ser mas fácil pensar en el codec como un MODEM sumamente sofisticado, un MODEM toma datos digitales y los transmite a través de las líneas de teléfono regulares. El codec toma las señales analógicas, las comprime y digitaliza transmitiendo las señales a través de las líneas de teléfono digital.
En éstas uno de los participantes puede interactuar de forma independiente y selectiva con el resto, mediante el control de un operador que puede ser el mismo usuario.

Los sistemas de videoconferencia de escritorio que combina las computadoras personales y el hardware instalado en ellas para lograr las comunicaciones a través de Internet. Con un costo mucho más bajo, pero con menores prestaciones. En éstos la interacción se realiza entre todos de forma simultánea con el mismo nivel de participación.

La videoconferencia interactiva es el intercambio de imágenes y voces procedentes de otro sitio, cuya porción de vídeo se captura en una cámara y se presenta en un monitor, y el audio se captura en un micrófono y se reproduce en una bocina, así los participantes pueden escucharse entre sí y compartir las imágenes de vídeo con movimientos, unos de otros.

1.5.1 TIPOS DE VIDEOCONFERENCIA

En cuanto a la conexión existen básicamente 2 modelos:

- Videoconferencia Punto a Punto.

Es cuando la videoconferencia se va a realizar entre 2 únicos terminales de videoconferencia. En cada extremo, el audio es captado por los micrófonos, el video es captado por la cámara. Estas dos señales analógicas (audio y video) son enviadas al CODEC (COdificador DECodificador) para ser digitalizadas, comprimidas, combinadas en una sola secuencia de datos y enviadas al procesador. El procesador agrega señales de control e información a la secuencia de datos. La secuencia de datos (audio, video, control e información) es transmitida a la interfase de red para ser electrónicamente convertida al tipo de señalización empleada (ISDN, V.35, RS-449, E1, etc.). Ésta interfase pone la señal digital en la red para que ésta sea transmitida y pueda ser recibida sin variaciones por el equipo remoto. A la señal recibida se le extraen las señales de control e información para ser procesadas. A la secuencia de datos que queda es transferida al CODEC (codificador DECodificador) para separarlas, descomprimirlas y convertidas en señales análogas y ser enviadas al monitor y bocinas.

- Videoconferencia Multipunto.

En este modelo la videoconferencia va a ser entre más de 2 terminales. El equipo que enlaza tres o más sitios en una sola conferencia es llamado una unidad de control multipunto (MCU). Este equipo, a partir de ahora funciona como un puente de videoconferencia, se encargará de recibir la señal de todos los equipos de videoconferencia y de distribuir todas estas señales a todos los equipos, con el fin de que todos puedan participar al mismo tiempo en dicho evento. Este puente de videoconferencia se suele contratar a empresas de telecomunicaciones, dado su alto coste.

Hasta hace unos pocos años enviar Vídeo con Audio a través de una línea utilizando computadora, sólo era posible con costosos y sofisticados Hardware, y estaba reservado para grandes compañías. Afortunadamente, debido al avance producido en el Vídeo Digital es posible enviar dichas señales desde una computadora doméstica a través de líneas cómo: Líneas telefónicas, Redes y Redes Digitales.

Dos hechos están provocando un aumento considerable del interés sobre la videoconferencia:

Por un lado, la fama y expandibilidad de Internet es tan grande que, a pesar de las posibles limitaciones tecnológicas, se están instalando los primeros sistemas de videoconferencia con un resultado más que aceptable. Sin incurrir en un costo prohibitivo, es posible que desde nuestra computadora podamos transmitir o realizar videoconferencia con envío de señales digitales de Audio y Vídeo en tiempo real a través de la línea telefónica. Esto es posible utilizando una buena Tarjeta de Vídeo, un determinado Software y una Cámara que en principio puede ser la propia doméstica.

1.5.2 ELEMENTOS QUE COMPONEN LA VIDEOCONFERENCIA

Los sistemas de videoconferencia están compuestos por monitores, cámaras, micrófonos, altavoces y por el Codec.El terminal de Videoconferencia más común lleva todos los elementos integrados en un mueble: cámara de vídeo, el monitor y el codec con el compresor.

Otros sistemas tienen como plataforma una computadora personal, (PC, MAC,...) al cual se le instala un Kit que consta de: cámara, micrófono, altavoz, tarjetas codificadora de vídeo y audio, terminal de comunicación (RDSI) y software de funcionamiento.

Monitor.- Los equipos más completos llevan dos monitores. En cada monitor se puede ver una ventana, por la que se monitoriza la imagen local que se está transmitiendo. Estos monitores pueden ser de formato PAL o VGA y dependiendo de las necesidades del usuario pueden tener medidas de 15",17",27",29", y 35".

Cámara.- Son las utilizadas para llevar a cabo la videoconferencia, es decir, las que van a captar la imagen de los participantes para transmitirla al otro extremo. Estas cámaras pueden ser fijas o motorizadas, y suelen estar situadas, bien encima del monitor, bien debajo de éste, cuando se trata de sistemas compactos.

También se utilizan cámaras de documentos para la visualización de documentos escritos, gráficos, diapositivas, elementos sólidos, etc.

La mayoría de equipos admiten cámaras auxiliares, de modo que la videoconferencia pueda ser más flexible. La salida de vídeo puede ser conectada a un cañón de proyección y/o a un magnetoscopio, pudiéndose grabar la videoconferencia.

Casi todos los modelos admiten la conexión de proyectores de transparencias, cámaras de documentos, fax, y computadoras personales.

Micrófono.- Pueden ser de sobremesa, de mano, sin hilos, etc. Los más utilizados son omnidireccionales.

Modem.- El módem es un dispositivo que permite conectar dos computadoras remotas utilizando la línea telefónica de forma que puedan intercambiar información entre si. El módem es uno de los métodos más extendidos para la interconexión de computadoras por su sencillez y bajo costo. La gran cobertura de la red telefónica convencional posibilita la casi inmediata conexión de dos computadoras utilizando un módem. El módem es un dispositivo que convierte las señales digitales de la computadora en señales análogas que pueden ser transmitidas por el canal telefónico.

Codec.- Este dispositivo convierte las señales de vídeo y audio en señales digitales, es considerado el corazón del sistema de videoconferencias ya que se encarga de controlar todo el proceso de comunicaciones entre los sitios participantes, llamados sitio emisor y sitios remotos. Es el dispositivo que contiene las entradas para recibir la señal de los micrófonos, cámaras de vídeo y demás periféricos ubicados en las aulas.

El otro factor determinante es el avance en las técnicas de compresión de Vídeo por Software ("Codecs") que permiten rebajar la cantidad de datos a transmitir hasta niveles suficientemente bajos sin perder una calidad excesiva.

La mayoría de los equipos de videoconferencia también pueden compartir aplicaciones, tales como, Hojas de cálculo, Procesadores de texto, etc. Esto quiere decir que a la vez que compartimos audio y vídeo, podemos estar trabajando con un mismo documento, hacer anotaciones sobre él, modificar campos, tomar notas, etc.

El rendimiento obtenido al realizar videoconferencia depende mucho de la calidad de la Tarjeta de Vídeo, de su configuración y sobre todo del Módem, de los

protocolos y del tipo de línea que se utilice para la transmisión. Básicamente, los entornos son los siguientes:

- Transmisión entre terminales de computadora a través de una Red LAN. (Proporciona una calidad excelente a tamaños incluso de pantalla completa y con una velocidad de transmisión de tiempo real (24 Planos/seg)). Este tipo de conexión es típico de pequeñas y medianas empresas en su relación laboral diaria.

- Transmisión a través de línea telefónica normal e Internet. Está limitada al ancho de banda de la línea telefónica, la velocidad del Módem y la franja horaria. (Si se utiliza una buena Tarjeta de Vídeo, puede alcanzarse hasta 20 Planos/seg con un Pentium II 400Mhz y en una ventana de tamaño 176x144. No está nada mal para la inversión necesaria). Este tipo de conexión le está popularizando de forma explosiva los usuarios en general que disponen de una conexión a Internet.

- Transmisión a través de la red RDSI. Este caso es similar al anterior con la ventaja de que la RDSI puede alcanzar una velocidad de transferencia de 64 y 128 Kps, es decir hasta más de dos veces la de un Módem de última generación.

- Transmisión por alguna de las líneas anteriores pero utilizando Tarjetas de Vídeo con Compresión por Hardware.

FORMATOS DE VIDEO

Quick Time, es un sistema de vídeo de Apple Computer para Windows. Admite las mismas capacidades que AVI. Lleva la extensión MOV. Es un organizador de datos de tiempos en varias formas. Las cintas de video cuentan con una pista para video y dos para audio. Quick Times es una grabadora de multipista en la cual se puede tener un rango ilimitado de pistas. El formato Quick Times soporta videos y sonido digitalizados, animaciones de computadora, datos MIDI de señalización o

el potencial para órdenes interactivas. La extensión del software de Quick Times consiste en tres partes:

- Conjunto de Herramienta de Movie Toolbox. Es un conjunto de servicios del software del sistema de alto nivel.
- El MCI separa las aplicaciones de las complejidades de compresión y descompresión. Con las capacidades de degradado de Quick Times puede crear una película de 24 bits y reproducirla en 1,8, 16 ó 24 bits.
- El administrador de componentes: permite a los recursos externos registrar sus capacidades en el sistema durante el tiempo de ejecución.

Microsoft video para Windows, Audio Video Inteleaved (AVI). Sistema de video de Microsoft para Windows. Admite de 8 a 24 bits de imagen y de 8 a 16 bits de sonido. Lleva la extensión AVI. Es un software desarrollado por Microsoft que reproduce video interfoleado de movimiento a tiempo real y secuencias de audio Windows, sin equipo especializado. Con un equipo de aceleración se pueden ejecutar secuencias de video AVI a 30 cuadros por segundo. Los datos de videos están interfoleados con los de audio dentro del archivo que contienen las secuencias de movimiento.

Las características de AVI son:

- Reproducción desde el disco duro o del CD-ROM.
- Reproducción en computador con memoria limitada; los datos son enviados desde el disco duro o un CD-ROM sin utilizar grandes cantidades de memoria.
- La compresión de video mejora la calidad de secuencias de video y reduce el tamaño. AVI incluye dos herramientas para capturar, editar y reproducir secuencias de video: VIDCAD y VIDEDIT. AVI también incluye herramientas de preparación de datos, Bitedit, Paledit y WaveEdit, MCIAVI.DRV (controla MCI para Avi)

Con los reproductores de QuickTimes y con el Media Player de Windows con AVI instalado se pueden ver y editar películas. Se puede reproducir una película hacia

adelante o atrás y redimencionarla. Adicionalmente puede contar y copiar cuadros de una película y pegarlos en otra. Con Media Player de Windows puede ejecutar como una aplicación independiente o como un objeto incrustado en otras aplicaciones y documentos utilizando OLE.

FORMATOS DE IMÁGENES

CALIDAD DE LAS IMAGENES

Las imágenes de bitmap pueden guardarse en varias calidades: desde blanco y negro y escala de grises hasta 8 bits (256 colores), 16 bits (32,000 colores), y 24 bits (color real, 16,7 millones de colores), ocupando mayor memoria cuanto más alta sea su calidad. La resolución, medida en puntos por pulgada (dpi), influye en el tamaño final del documento, aunque en multimedia lo usual es usar 72 puntos por pulgada, que es la resolución de la pantalla.

IMAGEN FIJA

Generalmente la imagen fija en multimedia esta en formato mapa de bits o bitmap. Un bitmap se compone de los puntos de color en pantalla que pueblan su extensión formando así una imagen Los formatos de archivos de imágenes de bitmap más comunes son Windows Bitmap (BMP), TIFF (Taffed Information File Format) o GIF.

Existen otros formatos de imagen como Targa (TGA) o PCX actualmente en desuso en el campo multimedia, pero no así en el terreno profesional. (30)

CIF

Common Intermediate Format. Formato de video utilizado en sistemas de videoconferencia, fácilmente compatible con señales NTSC y PAL. Especifica una velocidad de transferencia de datos de 30 cuadros por seg., Con 288 líneas y 352 pixeles por línea en cada cuadro. CIF también suele denominarse Full Cif (FCIF) para distinguirlo de QCIF.

Cuadros por segundo

Medida utilizada para expresar la cantidad de información de almacenamiento y presentación de vídeo en movimiento. Se aplica tanto a vídeo digital como a vídeo de película. Cada cuadro es una imagen fija y la sensación de movimiento se consigue mediante la presentación de cuadros de rápida sucesión. Cuantos más cuadros se ejecuten por segundo, más fluido resulta el movimiento percibido. Por lo general se necesita una velocidad mínima de 30 cuadros por segundo para evitar que el movimiento sea entrecortado.

JPEG

Joint Photographic Experts Group. Formato de gráficos estandarizado. Las extensiones de archivos habituales son: jpg y jpeg. JPEG permite manipular niveles de compresión y descompresión, mediante la configuración de opciones de calidad.

PCX

Formato de archivo específico de Paintbrush para imágenes de mapa de bits. PCX comprime los archivos para ahorrar espacio en disco.

PIXEL

Las computadoras almacenan imágenes en forma de pequeños puntos de color rectangulares (o cuadros) denominados píxeles. El color de un píxel representa los valores medios de matiz, brillo y saturación del área que ocupa en la imagen original. El número de píxeles utilizados para describir una imagen es directamente proporcional al grado de detalle de la imagen electrónica. Véase también "Resolución".

PNG

Portable Network Graphics. Tipo de archivo gráfico optimizado para el uso de Internet y servicios en línea. Está destinado a sustituir el formato de archivo GIF.

PSD

Formato de archivo de Photoshop, programa que permite crear y trabajar con capas y canales.

QCIF

Quarter Common Intermidiate Format. Formato de videoconferencia que especifica una velocidad de transferencia de datos de 30 cuadros por seg., Con 144 líneas y 176 pixeles por línea en cada cuadro. Esto representa una cuarta parte de la resolución CIF y es adecuado para sistemas de videoconferencia que utilizan líneas telefónicas.

Resolución.

El número de pixeles de una pantalla de monitor, indicado por el número de pixeles existentes en los ejes horizontal y vertical. La nitidez de la imagen visualizada depende de la resolución y del tamaño del monitor. Una misma resolución de pixel ofrecerá mayor nitidez en un monitor pequeño que en uno grande ya que, en este último caso, el mismo número de pixeles se distribuye en un espacio mayor.

TGA

Uno de los formatos de archivo de mapa de bits más utilizados para el almacenamiento de imágenes de color verdadero de 24 a 32 bits.

TIFF

Tagged Image File Format. Formato inicialmente pensado para imágenes digitalizadas; ofrece gráficos de alta calidad. Era un formato de escala de grises, antes de la aparición de monitores y programas en color. Pude comprimirse mediante diversos métodos. No está pensado para Internet.

VGA

Vide Graphics Array. Sistema de presentación de gráficos para PC desarrollado por IBM. VGA se ha convertido en uno de los estándares típicos de PC. En modo de gráficos, los sistemas VGA ofrecen una resolución de 640x480 (con 16 colores) o 320x200 (con 256 colores). La paleta total se compone de 262.144 colores.

Actualmente, todos los PC son compatibles con VGA.

FORMATOS DE AUDIO

Windows WAVE (wav)

WAV es el formato de sonido propio de Windows, que puede ser reproducido en otros sistemas operativos. Un minuto de sonido con calidad CD (44.1 Khz/16 bits stereo) pesa 10 megas, y aún comprimido sigue pesando demasiado, por lo que la única opción que queda es bajar la resolución y cantidad de canales.

MPEG audio layer III (.mp3)

Es un estándar desarrollado bajo la dirección de la ISO (International Organization for Standardization) pensado para comprimir audio de alta calidad. Funciona con la filosofía de codificar sólo lo que el oído humano es capaz de percibir, descartando todo lo demás. Es ideal para grabar 10 discos en un sólo CD, aunque para audio en tiempo real por internéstor sigue siendo mucho. En compresiones muy altas, la pérdida de calidad es notoria.

A medida que fueron popularizándose conexiones más rápidas, se estandarizó el uso de MP3 a 128Kbps (dos o tres megas por tema).

QuickTime (.mov) - para escuchar en tiempo real

Por su ductilidad, este formato fue adoptado por la ISO como base del MPEG-4. El "revolucionario" Windows Media Player es una simple implementación del

MPEG-4 estándar, de un formato propietario de Microsoft, sin poseer la integración que ofrece QuickTime de audio, video, MIDI, texto, animación Flash, sprites, fotos panorámicas y objetos 3D. Esta integración nos permite presentar una gran diversidad de contenidos en el sitio, sin que tengan que bajarse un nuevo plugin a cada rato.

En el caso del audio, el codec QDesign del QT3 parte de la misma filosofía que el MP3, pero con una serie de optimizaciones acústicas que permiten trabajar a Bit-rates mucho más bajos, y obtener archivos que pesan entre 3 y 10 veces menos.

1.6 CALIDAD DE SERVICIO (QoS)

Aunque el ancho de banda continúa ampliándose en el Internet, el tráfico continúa ampliándose en una tarifa similar o mayor. La calidad de servicio (QoS), es la habilidad de una aplicación para recibir, de punta a punta, un predeterminado nivel de desempeño de una red. Así pues, es la capacidad de una red de proveer el mejor servicio, controlando sus tipos de tráficos, engloba una colección de tecnologías que permiten que las aplicaciones que transitan por la red, soliciten y reciban porcentajes de disponibilidad fiables en términos de capacidad del rendimiento de procesamiento de datos (anchura de banda).*

Antes de que los servicios de voz o video sean incluidos dentro del tráfico de la red, es necesario estar seguros de que existe un ancho de banda adecuado para todas las aplicaciones que estén dentro de la misma. Para empezar, se deberán sumar los requerimientos mínimos de ancho de banda para cada una de las aplicaciones (voz, datos o video) que estarán corriendo dentro de la red; esta suma representa los requerimientos mínimos de ancho de banda en cualquiera de los enlaces de la red y no deberá exceder el 75% del total del ancho de banda

* Srinivas Vegesna, "IP Quality of Service". Cisco Press. Indianapolis USA December 2000

disponible en dicho enlace. Esta regla del 75% asume que el restante ancho de banda es utilizado por tráfico como ruteo y tráfico de capa 2 generado por los switches así como aplicaciones adicionales como correo electrónico y http.

1.6.1 CLASIFCACIÓN DEL TRÁFICO

Antes de que el tráfico sea manipulado de acuerdo a los requerimientos del usuario éste será previamente identificado o etiquetado de alguna manera para poder ser diferenciado o señalado uno de otro, para hacer esto existen varias técnicas y estándares dentro de la industria. Dentro de estos destacan: Esquemas de capa 3 como lo son la precedencia de IP o la diferenciación de servicios. Esquemas de capa 2 encontramos técnicas como lo es el estándar 802.1P y las características de los datos por sí mismos.

Existiendo varias formas de clasificar el tráfico dentro de la red, debemos tener cuidado en separar las funciones que se realizarán dentro de los dispositivos de borde de red y los de backbone con el objetivo de lograr una Calidad de Servicio lo mejor posible.

Prioritización en capa 2

Dentro de ésta se encuentra 802.1p, es utilizada para agregar más información dentro de los encabezados de los paquetes de Ethernet y Token Ring (tecnologías de LAN) para permitir el soporte a redes virtuales (VLAN's) y la priorización de tráfico. Este estándar agrega 16 bits al encabezado, de los cuales 3 son utilizados como una etiqueta de diferenciación, lo cual permite 8 niveles de prioridad, del 0-7, y soportar capacidades de envio rápido de tráfico de características críticas y

sensitivas al retardo dentro de un ambiente LAN switcheado de capa 2. Puesto que el estándar opera en capa 2 soporta las tecnologías Ethernet y Token Ring.

El estándar, como ya hemos dicho, permite a los switches diferenciar el tráfico dentro de la red, y propone la siguiente relación de valores y tipo de tráfico, el cual puede ser manipulado dependiendo de los requerimientos del usuario.

Decimal	Binario	Tipo de tráfico
7	111	Reservado
6	110	Voz en tiempo real
5	101	Multimedia en tiempo real
4	100	Video en demanda
3	011	Crítico
2	010	Estándar
1	001	Background
0	000	Default

Prioritización en capa3

Dentro de la capa 3 y del protocolo IP, existe un campo llamado Tipo de Servicio (ToS) que va dentro del encabezado de dicho protocolo y que permite que las Clases de Servicio puedan existir, ya que este campo ToS utiliza 3 bits y por lo tanto nos permite tener hasta 8 posibles combinaciones(0-7) y por lo tanto 8 diferentes grupos de flujo de tráfico, es decir podemos diferenciar hasta 8 servicios dentro de la red.

Mientras que la capa 2 utiliza la etiqueta del 802.1p para diferenciar el tráfico dentro de la LAN, la capa 3 usa el campo de ToS, dentro de IP, para diferenciar tráfico en un ambiente ruteado y de enlaces WAN. En 1981 la IETF definió los tres bits de precedencia en el campo de ToS para representar o definir 8 niveles de prioridad o diferenciación. Cabe hacer la aclaración de que los bits de precedencia

van dentro del encabezado de IP, así que sólo puede utilizarse para diferenciar tráfico nativo IP o tráfico que sea transportado a través de túneles de IP.

Actualmente, y en lugar de usar solamente 3 bits, se utilizan los 6 bits más significativos del campo de ToS y el cual se refiere como DSCP, estos 6 bits son utilizados cuando el tráfico requiere salir de la red del campus a hacia la WAN través de los enrutadores de borde, ya que la clasificación de capa 2 es removida es necesaria una clasificación a nivel de capa 3 para proporcionar una calidad de servicio.

Decimal	Binario	Tipo de tráfico
7	111	Reservado control de red
6	110	Reservado control de internet
5	101	Crítico
4	100	Transmisión anulada
3	011	Transmisión
2	010	Inmediata
1	001	Prioridad
0	000	Default

Desde que en 1981 se definió este campo no había sido utilizado hasta ahora, y la primera pregunta que se hizo todo el mundo era: Qué dispositivo dentro de la red debería manejar la prioridad con el campo de ToS. Existen dos posibilidades: desde el cliente o el equipo de capa 3, ya sea enrutador o switch. La ventaja de que el cliente sea quien defina el campo de ToS es que la carga de procesamiento del enrutador será menor, además el cliente también tiene la capacidad de etiquetar a través del estándar 802.1p.

Una vez etiquetado el tráfico dentro de la red los dispositivos, dentro de la misma, pueden manejar o diferenciar los diferentes flujos de tráfico que existen y podrán manipularlos a través de mecanismos de encolamiento, políticas de enrutamiento, etc.

Hasta aquí hemos visto las dos posibilidades de diferenciar el flujo del tráfico dentro de la red, pero no hemos dicho para que lo necesitamos, básicamente el propósito es el de proteger el tráfico de voz que será transportado a través de una red de datos y el cual será clasificado como de mayor prioridad a diferencia del de datos o video o cualquier otra aplicación que esté dentro de la red, puesto que en momentos de saturación del tráfico en la red los paquetes de menor prioridad serán los primeros que dejarán de enviarse y sucesivamente hasta que la red regrese a un porcentaje de utilización bajo.

CARACTERÍSTICAS DE QoS

- Control sobre recursos
- Mayor eficiencia en el uso de los recursos de la red
- Servicios diferenciados
- Coexistencia de aplicaciones
- Integración de tráficos

ARQUITECTURA BÁSICA

Tres piezas fundamentales:

- QoS con un sólo elemento de red
- QoS bajo técnicas de señalización para la implementación de la calidad del servicio entre diversos elementos de red
- Procedimientos y funciones QoS de administración, manejo y control del tráfico a través de la red.

BASES DE IMPLEMENTACIÓN

- Calidad de servicio punta a punta
- Herramientas para el manejo de congestión
- Herramientas para evitar congestiones
- Mecanismos de eficiencia

NIVELES DE SERVICIO PUNTA A PUNTA

El tráfico en la red es originado por una variedad de aplicaciones en las estaciones terminales, estas aplicaciones difieren en sus servicios y requerimientos.

Hay 3 niveles básicos que pueden proveerse a través de la red:

- Servicio del Mejor Esfuerzo: Conectividad básica sin garantías.
- Servicio Diferenciado: Es algún tipo de tráfico que es tratado mejor que otro.
- Servicio Garantizado: Es el servicio garantizado, una absoluta reservación de recursos de la red para algún tráfico especifico

HERRAMIENTAS DE CONTROL DE CONGESTIÓN

Cuando se presentan sobre flujos de tráfico, uno de los caminos que siguen los equipos de red es el uso de algoritmos de encolamiento y la aplicación de mecanismos de prioritización.

HERRAMIENTAS PARA EVITAR LA CONGESTIÓN

Utiliza técnicas de monitoreo del tráfico de la red en un esfuerzo para anticiparse y evitar la generación de congestionamientos (comúnmente los denominados cuellos de botella).

MECANISMOS DE EFICIENCIA

Trabajan en conjunto con las otras herramientas para proveer niveles de eficiencia a las aplicaciones. Por ejemplo:

-Fragmentación

-Compresión de encabezados de los paquetes.

CAPÍTULO II
PROTOCOLO TCP/IP

2.1 INTRODUCCIÓN A INTERNET

Internet la red de redes, es una forma abreviada de la palabra "Internetwork", usa protocolos de redes abiertas (estándares que no son propietarios o controlados por alguna organización y que pueden ser usados gratuitamente por alguien para implementarlos en productos de software o hardware).

La Internet global es la que enlaza negocios, Instituciones Educativas y otras Organizaciones de todo tipo. Surge en septiembre de 1969, cuando la DARPA (Defense Advanced Research Project Agency) desarrolló un sistema de transmisión de mensajes eficaz ante un posible ataque nuclear que pudiese destruir una parte de la red de comunicaciones utilizada por el ejército. La idea era garantizar la recepción del mensaje a pesar de una destrucción parcial de la red. De este modo se unieron cuatro computadoras mediante un protocolo llamado NCP (Network Communications Protocol) formando la red llamada ARPANet. En poco tiempo este protocolo evolucionó hasta el que existe actualmente en Internet, el popular *TCP/IP* (Transmisión Control Protocol/ Internet Protocol) y de una aplicación puramente militar se pasó a otra más pacífica, ya que a dicha red se unieron con el propósito de mantenerse en contacto: científicos, Universidades y Centros de Investigación de EEUU, con el propósito de poner en común información y hacer partícipes de sus descubrimientos al resto del mundo.

En poco tiempo la DARPA y su red, basada ya en el protocolo TCP/IP, consiguió llegar al 90% de los departamentos de Ingeniería y computadoras de universidades americanas.*

El crecimiento tan espectacular que se ha producido en Internet, ha sido en gran medida a la creación de un sistema capaz de incorporar imágenes, gráficos y sonidos en las transmisiones (y no sólo caracteres como hasta entonces): el World Wide Web (Telaraña de cobertura mundial). La incorporación de este método, así como la apertura que se dió a mediados de los 90's autorizando la entrada de aplicaciones y servidores más comerciales en Internet y por lo tanto un crecimiento en el número de usuarios domésticos de todo el mundo.

Internet nos permite visitar los museos más conocidos del mundo; acceder a una completa biografía de los personajes más relevantes de la historia, conocer los productos que comercializa una determinada marca; Comprar los más diversos productos y servicios; Visitar la Casa Blanca en Washinton; Escuchar la música de un determinado cantante; Ver los nuevos proyectos de la NASA; Consultar en tiempo real, los resultados de unas elecciones generales; Realizar una videoconferencia con cualquier persona del mundo; Oír la voz de alguien que se encuentra en otro Continente; enviar y recibir archivos informáticos.

En la actualidad, todos los datos transmitidos a través de Internet usan el protocolo TCP/IP cuyo nombre proviene de sus dos protocolos principales (TCP e IP), pero que sólo son una parte de la *Suite de Protocolos TCP/IP*, los cuales permiten que millones de equipos informáticos de todo el mundo puedan comunicarse.

La Suite de Protocolos TCP/IP de Internet pueden utilizarse para la comunicación a través de cualquier conjunto de redes interconectadas. Además,

* Jose A. Carballar, "Internet: el mundo en sus manos", RA-MA, Madrid

son apropiados tanto para la WAN como para la LAN. El conjunto de protocolos Internet incluye no sólo las especificaciones de la Capa 3 y 4 (tales como IP y TCP), sino también la especificación para aplicaciones comunes tales como el correo electrónico, la conexión remota, la emulación de terminales y la transferencia de archivos.

Algunos de los motivos de su popularidad son:

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

Las principales características de la arquitectura de un sistema en TCP/IP son:

- *Independencia de la tecnología de red,* el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican como transmitir los datagramas en una red.
- *Conectividad Universal a través de la red,* la red de redes TCP/IP permite que se comuniquen cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de su fuente y su destino. Las computadoras intermedias de conmutación utilizan la dirección de destino para tomar decisiones de ruteo.
- *Acuses de recibo punto a punto*, los protocolos de TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.

A continuación, se resumen las cuatro capas de la Suite de Protocolos de TCP/IP:

- Capa de Aplicación: al igual que en el modelo OSI, en esta capa el usuario interactúa con las aplicaciones de red.
- Capa de Transporte: esta capa maneja el flujo de datos entre los host de dos redes interconectadas. TCP y UDP implementan la capa de transporte. TCP proporciona el transporte de datos orientado a la conexión, mientras que UDP es sin conexión.
- La capa de Internet: En esta capa los datos son movidos alrededor de las redes interconectadas. El protocolo de Internet (IP), opera en esta capa para rutear paquetes a través de redes independientes del medio.
- La Red: En esta capa los datos de la capa de red, que fueron ruteados apropiadamente, son trasmitidos a su destino.

2.2 ESTRATIFICACIÓN POR CAPAS DE TCP/IP

Los protocolos estratificados por capas están diseñados de modo que una capa n en el receptor de destino reciba exactamente el mismo objeto enviado por la correspondiente capa n de la fuente.

El principio de estratificación por capas explica por qué la estratificación es una idea poderosa. Esta permite que el diseñador de protocolos enfoque su atención hacia una capa a la vez, sin preocuparse acerca del desempeño de las capas inferiores. Las capas de aplicación y transporte cumplen con las condiciones de punto a punto y están diseñados de modo que el software en la fuente se comunique con su par en el destino final. Así, el principio de estratificación por capas establece que el paquete recibido por la capa de transporte en el destino final es idéntico al paquete enviado por la capa de transporte en la fuente original. Es fácil entender, que en las capas superiores, el principio de estratificación por capas se aplica a través de la transferencia punto a punto y que en las capas inferiores se aplica en una sóla transferencia de máquina.

En la estratificación por capas, en la capa de Internet, los anfitriones conectados a una red de redes debe considerarse como una gran red virtual, con los datagramas IP que hacen las veces de unas tramas de redes. Los datagramas viajan desde una fuente original hacia un destino final y el principio de la estratificación por capas garantiza que el destino final reciba exactamente el datagrama que envió la fuente. Además sabemos que el encabezado o "datagram" contiene campos, como "time to live", que cambia cada vez que el datagrama pasa a través de un ruteador. Así el destino final no recibirá exactamente el mismo diagrama que envió la fuente. Se concluye que, a pesar de que la mayor parte de los datagramas permanecen intactos cuando pasan a través de una red de redes, el principio de estratificación por capas sólo se aplica a los datagramas que realizan transferencia de una sóla máquina; por lo tanto se considera que la capa de Internet no proporciona un servicio punto a punto.

El modelo TCP/IP tiene cuatro capas (ver fig.2.2.a), en las cuales existen muchos protocolos:

MODELO TCP/IP

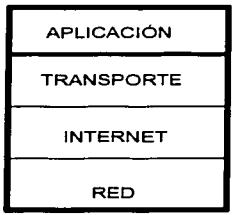


Fig. 2.2.a Modelo DoD (TCP/IP)

4. ***Capa de Aplicación:*** Es el nivel más alto, los usuarios llaman a una aplicación que accesan servicios disponibles a través de la red. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar y recibir datos, el cual puede ser una secuencia de mensajes o un flujo continuo de octetos. Además, está basada en el modelo Cliente-Servidor, los protocolos de aplicación incluyen FTP para transferencia de archivos, Telnet para sesiones con terminales remotas, SMTP para correo electrónico y SNMP para la administración de la red.
3. ***Capa de Transporte:*** La principal tarea es proporcionar la comunicación entre un programa de aplicación y otro (comunicación punto a punto). La capa de transporte maneja el flujo de datos y la corrección de errores. Tiene 2 protocolos de transporte muy diferentes: TCP y UDP, cada uno soporta aplicaciones con diferentes requerimientos en el desempeño y rehabilitación de la transmisión de datos.
2. ***Capa de Internet (Network):*** Esta capa maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. Encapsula el paquete en un datagrama IP, llena el encabezado del datagrama, utiliza un algoritmo de ruteo para determinar si puede entregar el datagrama directamente o si debe enviarlo a un ruteador y pasar el datagrama hacia la interfaz de red apropiada para su transmisión. IP es el protocolo dominante usado para el ruteo de los datos entre las redes, el cual determina la mejor ruta que seguirán los paquetes. ICMP (Internet Control Message Protocol) es una clase de protocolo que trabaja con IP, para pasar mensajes de error e información entre los host y los ruteadores. IGMP (Internet Group Management Protocol), ayuda al ruteador a pasar los datos a múltiples host por Multicast.
1. ***Capa de Red:*** También conocido como interface de red (network interface layer), los datos son transmitidos a través de una simple red. ARP y RARP son usados en algunas redes que necesitan convertir direcciones de red a direcciones físicas, operando en paralelo con el protocolo de Internet (IP).

Las comparaciones entre el modelo OSI y el modelo TCP/IP, son:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito).
- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola.
- TCP/IP soporta todos los protocolos físicos y de enlace de datos estándar.
- La información de TCP/IP se transfiere en una secuencia de datagramas.
- TCP/IP parece ser más simple porque tiene cuatro capas.

2.3 LA CAPA DE APLICACIÓN

En esta capa, los usuarios ejecutan programas de aplicación para acceder a los servicios disponibles a través de la Internet TCP/IP. Los programas de aplicación eligen la clase de transporte que necesitan, la cual puede ser cualquier mensaje o cadena de bytes para ser pasados a la capa de transporte.

Los protocolos de la capa de aplicación (fig. 2.3.a) están disponibles para la transferencia de archivos, el correo electrónico y la conexión remota. En la capa de aplicación también se brinda soporte para la administración de redes.

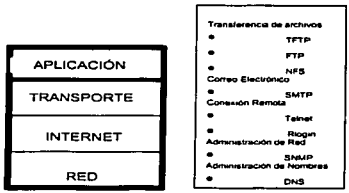


Fig. 2.3.a Capa de Aplicación

2.3.1 SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

Este protocolo especifica cómo interactúan dos sistemas de correo y el formato de los mensajes de control que intercambian para transferir el correo.

E-mail es ahora la herramienta de negocios tan común como el teléfono, la máquina de fax, el papel, etc. Algunas funciones básicas de correo para los clientes de Internet son:

- Recibir y Leer mensajes de correo.
- Enviar y Reenviar mensajes de correo
- Adjuntar archivos a los envíos de correo

Existen cuatro protocolos básicos que definen el correo. El protocolo de Transferencia de correo simple (*SMTP*), el cual define cómo los mensajes son enviados a través de Internet desde su fuente a su destino. El Post Office Protocol (POP) define como el cliente recupera sus mensajes del servidor de correo. El Internet Mail Access Protocol (IMAP) provee las herramientas para manejar cuentas en el servidor de correo a través de los sistemas de clientes. El Multipurpose Internet Mail Extensions (MIME) define métodos para encapsulación de varios tipos de archivos de datos en un formato que pueda ser transmitido a

través de Internet. Los Estándares para el formato de Mensajes de texto de Internet ARPA, están definidos en el RFC822.

E-mail es la aplicación base de Internet y es el responsable de su excesivo crecimiento. El correo electrónico funciona siguiendo el esquema general Cliente/Servidor, a saber: un equipo cliente conectándose a un servidor para obtener información. El equipo cliente utiliza un programa de correo y se conecta a un servidor de correo para enviar/recibir los mensajes. Existen dos conceptos del correo electrónico: El *servidor de correo* y la *cuenta de correo*.

- Servidor de correo (Mail server): Es una computadora que está conectada de forma directa y permanentemente a Internet y que funciona como lugar de almacenamiento donde se depositan los mensajes que envía y recibe el usuario. Los servidores de correo cuando envían un mensaje con un *programa de correo*, realizan tres pasos: primero se conecta al servidor SMTP, luego envía el mensaje desde su computadora al servidor de correo y finalmente se desconecta del servidor, es análogo a una oficina postal.
- Cuenta de correo: una cuenta de correo es simplemente un buzón

2.3.2 TELNET

Telnet permite al usuario de una localidad establecer una conexión TCP con un servidor de acceso a otro. Telnet transfiere después las pulsaciones de teclado directamente desde el teclado del usuario a la computadora remota como si hubiesen sido hechos en un teclado unido a la máquina remota. Telnet también transporta la salida de la máquina remota de regreso a la pantalla del usuario. El servicio se llama transparent (transparente) porque da la impresión de que el teclado y el monitor del usuario están conectados de manera directa a la máquina remota.

El software de cliente TELNET suele permitir que el usuario especifique una máquina remota, ya sea dando su nombre de dominio o su dirección IP. Como acepta direcciones IP, Telnet se puede usar con anfitriones aunque no se pueda establecer el enlace de un nombre con una dirección. Telnet ofrece tres servicios básicos. El primero, define una terminal virtual de red (network virtual terminal) que proporciona una interfaz estándar para los sistemas remotos. Los programas clientes no tienen que comprender los detalles de todos los sistemas remotos, se construyen para utilizarse con la interfaz estándar. En el segundo, Telnet incluye un mecanismo que permite al cliente y al servidor negociar opciones, asimismo proporciona un conjunto de opciones estándar. Por último, Telnet trata con ambos extremos de la conexión de manera simétrica. En particular, Telnet no fuerza la entrada de cliente para que ésta provenga de un teclado, ni al cliente para que muestre su salida en una pantalla. De esta manera, Telnet permite que cualquier programa se convierta en cliente, además cualquier extremo puede negociar las opciones. Cuando un usuario invoca a Telnet, un programa de aplicación en la máquina del usuario se convierte en el cliente. El cliente establece una conexión TCP con el servidor por medio de la cual se comunicarán: Una vez establecida la conexión, el cliente acepta los pulsos de teclado del usuario y los manda al servidor, al tiempo que acepta caracteres de manera concurrente que el servidor regresa y despliega en la pantalla del usuario. El servidor debe aceptar una conexión TCP del cliente y después transmitir los datos entre la conexión TCP y el sistema operativo local.

2.3.3 FTP (PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)

Dado un protocolo de transporte confiable de extremo a extremo como el TCP, la transferencia de archivos podría ser trivial, por lo que FTP ofrece facilidades de las funciones de transferencia de archivos proporcionando acceso interactivo,

especificaciones de formato y control de autentificación, aunque es posible conectarse como el usuario anonymous que no necesita contraseña.
TFTP es un protocolo de transferencia de archivos, no permite tanta interacción entre cliente y servidor como la que existe en FTP. TFTP utiliza UDP.

2.4 LA CAPA DE TRANSPORTE

Existen dos protocolos en la capa de transporte: TCP y UDP.

- TCP, es un protocolo confiable orientado a conexión. Se encarga de dividir los mensajes en segmentos, reagruparlos en la estación destino, reenviar todo lo que no se reciba y reagrupar los mensajes a partir de los segmentos. TCP brinda un circuito virtual entre aplicaciones de usuarios finales.
  La capa de transporte ejecuta dos funciones:
  - Control de Flujo, que se realiza mediante ventanas deslizantes.
  - Confiabilidad, proporcionada por números de secuencia y acuse de recibo.

- UDP, es un protocolo de Datagrama de Usuarios, no posee conexión y no es confiable. Aunque UDP es responsable por la transmisión de mensajes, no se provee ninguna verificación de software para la entrega de segmentos en esta capa; es por ello denominado "no confiable".

2.4.1 UDP (PROTOCOLO DE DATAGRAMA DE USUARIO)

UDP es un protocolo mucho más fácil que TCP y es útil en situaciones en las que no son necesarios los mecanismos de confiabilidad de TCP. UDP es usado en *VoIP (Voice over IP)* para transportar el actual tráfico de voz. TCP no es usado, porque el control de flujo y las retransmisiones de los paquetes de voz, no son necesarios. UDP es continuo para transmitir las cadenas de audio. A continuación estudiaremos los conceptos importantes de UDP, necesarios para la comprensión de esta tesis:

UDP proporciona el mecanismo primario que utilizan los protocolos de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir a los diferentes programas que se ejecutan al mismo tiempo en la misma máquina. Además de los datos, cada *mensaje UDP* o *datagrama de usuario* contiene tanto el número de puerto destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta. UDP utiliza el Protocolo de Internet subyacente para transportar un mensaje de una máquina a otra y proporcionar la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que los mensajes llegan, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las máquinas. Por lo tanto los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar, se puede resumir que:

El protocolo de Datagrama de usuario (UDP), proporciona un servicio de entrega sin conexión y no confiable, utilizando IP para transportar mensajes entre máquinas, agregando la capacidad para distinguir entre varios destinos dentro de una computadora anfitrión.

UDP no utiliza operaciones en ventana ni acuses de recibo. Los protocolos de la capa de aplicación pueden proporcionar confiabilidad. UDP ha sido diseñado

para aplicaciones que no necesitan agrupar secuencias de segmentos. Entre los protocolos que utiliza UDP se incluyen TFTP, SNMP, sistemas de archivo de red (NFS) y sistema de nombres de dominio (DNS).

2.4.1.1 FORMATO DE MENSAJES UDP

Cada mensaje UDP se conoce como *datagrama de usuario*, el cual consiste de dos partes: un encabezado UDP (8 Bytes) y un área de datos UDP. En la Fig. 2.4.1.1.a, se muestra cómo el encabezado se divide en cuatro campos de 2 Bytes (16 bits) cada uno, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP (checksum).

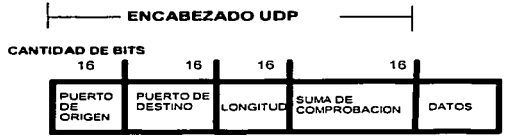


Fig. 2.4.1.1.a El encabezado UDP

Los campos PUERTO DE ORIGEN y PUERTO DESTINO contienen los números de puerto del protocolo UDP utilizados para el demultiplexado de datagramas entre los procesos que los esperan recibir. El PUERTO DE ORIGEN es opcional. Cuando se utiliza, especifica la parte a la que se deben enviar las respuestas, de lo contrario, puede tener valor de cero. El campo de LONGITUD contiene un conteo de los octetos en el datagrama UDP, incluyendo el encabezado y los datos de usuario UDP. Por lo tanto el valor mínimo para el campo de LONGITUD es de ocho octetos, que es la longitud del encabezado.

La suma de VERIFICACIÓN (CHECKSUM) es opcional y no es necesario utilizarla; un valor cero en el campo significa que la suma no se computó. Ésta incluye un pseudo-encabezado que tiene campos para las direcciones IP de origen y de destino. La dirección IP de destino debe ser conocida, cuando se envía un datagrama UDP y que éste la debe pasar a la capa UDP. Por tanto la capa UDP, puede obtener la dirección IP destino sin interactuar con la capa IP. Sin embargo la dirección IP de origen depende de la ruta que el IP seleccione para el datagrama, debido a que esta dirección identifica la interfaz de red sobre la que se transmite el datagrama. Por lo tanto, el UDP no puede conocer una dirección IP de origen a menos que interactúe con la capa IP.

UDP pide a la capa IP que compute la dirección IP de origen y destino, utilizándolas para construir un pseudo-encabezado, computa la suma de verificación, descarta el pseudo-encabezado y transfiere a la capa IP el datagrama UDP para su transmisión.

2.4.1.2 MULTIPLEXADO, DEMULTIPLEXADO Y PUERTOS UDP

UDP acepta datagramas de muchos programas de aplicación y los pasa a IP para su transmisión, también acepta datagramas UDP entrantes del IP y los transfiere al programa de aplicación apropiado. Conceptualmente, todo el multiplexado y el demultiplexado entre el software UDP y los programas de aplicación ocurren a través del mecanismo de puerto. Cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto del protocolo y un número de puerto asociado, antes de poder enviar un datagrama UDP. Una vez que se asigna el puerto, cualquier datagrama que envíe el

programa de aplicación a través de él, tendrá el número de puerto en el campo PUERTO DE ORIGEN UDP.

La forma más fácil de pensar en un puerto UDP es en una cola de espera. En la mayor parte de las implantaciones, cuando un programa de aplicación negocia con el sistema operativo la utilización de cierto puerto, el sistema operativo crea una cola de espera interna que puede almacenar los mensajes que lleguen. A menudo, la aplicación puede especificar o modificar el tamaño de la cola de espera. Cuando el UDP recibe un datagrama, verifica si el número de puerto destino corresponde a uno de los puertos que está en uso. Si no, envía mensajes de error ICMP de puerto no accesible y descarta el datagrama. Si encuentra un correspondiente, el UDP pone en cola de espera el nuevo datagrama, en el puerto en que lo pueda acceder un programa de aplicación.

¿Cómo se deben asignar el número de puertos de protocolo?, Esta pregunta es importante ya que dos computadoras necesitan estar de acuerdo en los números de puerto antes de que puedan interoperar. Existen dos enfoques fundamentales para la asignación de puertos. El primero se vale de una autoridad central. Todos se ponen de acuerdo en permitir que una autoridad central asigne los números de puerto conforme se necesiten y que publique la lista de todas las asignaciones. Entonces, todo el software se diseña de acuerdo con la lista. Este enfoque, se conoce como enfoque universal. El segundo enfoque para la asignación de puertos emplea la transformación dinámica, en este enfoque los puertos no se conocen de manera global. Siempre que un programa necesita un puerto, el software de red le asigna uno. Para conocer la asignación actual de puerto en otra computadora, es necesario enviar una solicitud que pregunte algo así como, ¿qué puerto está utilizando el servicio de transferencia de archivo?, La máquina objetivo responde al proporcionar el número de puerto correcto a utilizar. Algunos puertos son:

DECIMAL	*PALABRA CLAVE*	*DESCRIPCIÓN*
0	*ECHO*	*RESERVADO*
7	*DISCARD*	*ECO*
15	*NETSTAT*	*QUIÉN ESTÁ AHÍ O NETSTAT*
19	*CHARGER*	*GENERADOR DE CARACTERES*
42	*NAMESERVER*	*SERVIDOR DE NOMBRE DE ANFITRIONES*
43	*NICNAME*	*QUIÉN ES?*
53	*DNS*	*SERVIDOR DE NOMBRE DE DOMINIOS*
67	*BOOTPS*	*SERVIDOR DE PROTOCOLOS BOOTSTRAP*
69	*TFTF*	*TRANSFERENCIA TRIVIAL DE ARCHIVOS*
123	*NTP*	*PROTOCOLO DE TIEMPO DE RED*
161	*SNMP*	*MONITOREO DE RED SNMP*

2.4.2 TCP (PROTOCOLO DE CONTROL DE TRANSPORTE)

Al igual que UDP, TCP es un protocolo de la capa de Transporte. Sin embargo, mientras que UDP ofrece pocas formas de confiabilidad o garantías, TCP conecta hosts a través de una internetwork de forma confiable.

TCP, es un protocolo confiable orientado a conexión. Se encarga de dividir los mensajes en segmentos, reagruparlos en la estación destino, reenviar todo lo que no se reciba y reagrupar los mensajes a partir de los segmentos. TCP brinda un circuito virtual entre aplicaciones de usuarios finales.

TCP usa técnicas variadas para sincronizar el desempeño en la conexión. UDP interactúa en una sóla dirección y permite broadcast y multicast, transmisiones de datos de un host a muchos. La interacción de TCP es de forma dúplex,

permitiendo que la información viaje de ambos sentidos en cada segmento TCP y sólo soporta comunicación de host a host, circuitos punto a punto porque cada petición debe tener un acuse de recibo.

2.4.2.1 NECESIDAD DE LA ENTREGA DE FLUJO

En el nivel más bajo, las redes de comunicación por computadora proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir cuando los errores de transmisión interfieren en los datos, cuando falla el hardware de red o cuando las redes se sobrecargan demasiado. Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. Además, las tecnologías subyacentes de red pueden dictar un tamaño óptimo de paquete o formular otras obligaciones necesarias para lograr velocidades eficientes de transmisión.

En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega sin conexión y no confiable para las transferencias de gran volúmenes se vuelve tedioso, molesto y requiere que los programadores incorporen, en cada programa de aplicación, la detección y solución de errores. Por tal motivo, ha sido necesario encontrar soluciones de propósito general para el problema de proporcionar una entrega de flujo confiable.

La interfaz entre los programas de aplicación y los servicios de entrega confiable, se pueden caracterizar por cinco funciones:

- *Orientación de flujo:* cuando dos programas de aplicación transfieren grandes volúmenes de datos, pensamos en los datos como un flujo de bits. El servicio de entrega de flujo en la máquina de destino pasa

al receptor exactamente la misma secuencia de octetos que le pasa el transmisor en la máquina de origen.

- *Conexión de circuito virtual:* La transferencia de flujo es análoga a realizar una llamada telefónica. Antes de poder empezar la transferencia, los programas de aplicación, transmisor y receptor interactúan con sus respectivos sistemas operativos, informándose de la necesidad de realizar una transferencia de flujo. Una vez que se establecen todos los detalles, los módulos de protocolo informan a los programas de aplicación que se estableció una conexión y que la transferencia puede comenzar. Durante la transferencia, el software de protocolo en las dos máquinas continúan comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo, ambas máquinas detectarán la falla y la reportarán a los programas apropiados de aplicación. Se utiliza el término de circuitos virtuales para describir dichas conexiones porque aunque los programas de aplicación visualizan la conexión como un circuito dedicado de hardware, la confiabilidad que se proporciona depende del servicio de entrega de flujo.
- *Transferencia con memoria intermedia:* los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente octetos de datos. Cuando transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado. En el extremo receptor, el software de protocolo entrega octetos del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor. Para aplicaciones en la que los datos se deben entregar aunque no se llene una memoria intermedia, el servicio de flujo proporciona un mecanismo de empuje (push) que las aplicaciones utilizan para forzar una transferencia. En el extremo receptor, el empuje hace que el TCP ponga los datos a disposición de la aplicación sin demora.

- *Conexión Full Duplex:* Las conexiones proporcionadas por el servicio de flujo permiten la transferencia concurrente en ambas direcciones, la cual consiste en dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción. El servicio de flujo permite que un proceso de aplicación termine el flujo en una dirección mientras los datos continúan moviéndose en la otra dirección, haciendo que la conexión sea full duplex.

2.4.2.2 FORMATO DEL SEGMENTO TCP

La unidad de transferencia entre el software TCP de dos máquinas se conoce como *segmento (Fig. 2.4.2.2.a)*. Los segmentos se intercambian para establecer conexiones, transferir datos, enviar acuses de recibo, anunciar los tamaños de ventana y para cerrar conexiones. Debido a que el TCP utiliza acuses de recibo incorporados, un acuse que viaja de la máquina A a la máquina B puede viajar en el mismo segmento en el que viajan los datos de la máquina A a la máquina B, aun cuando el acuse de recibo se refiera a los datos enviados de B hacia A.

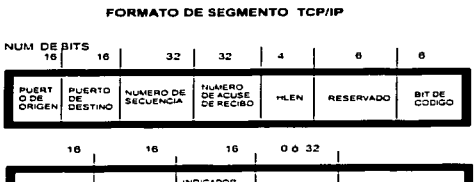


Fig. 2.4.2.2.a Formato de Segmento

Los campos de un segmento TCP, se definen de la siguiente manera:

- Puerto de origen: número del puerto que realiza la llamada.
- Puerto de destino: número del puerto que recibe la llamada.
- Número de secuencia: número que se utiliza para garantizar la secuencia correcta de los datos entrantes.
- Número de acuse de recibo: octeto siguiente TCP esperado
- HLEN: cantidad de palabras de 32 bits en el encabezado
- Reservado: se establece en cero
- Bits de código: funciones de control, tales como configuración y finalización de una sesión.
- Ventana: número de octetos que el emisor desea aceptar
- Suma de comprobación: suma de comprobación calculada de los campos de encabezado de datos.
- Señal de urgencia: indica el final de los datos urgentes.
- Opción: la definida actualmente; tamaño máximo del segmento TCP
- Datos: datos del protocolo de la capa superior.

2.4.2.3 NÚMERO DE PUERTO

Tanto el TCP como el UDP usan número de puertos para pasar información a las capas superiores. Los números de puerto se utilizan para realizar un seguimiento de las distintas conversaciones que atraviesan la red simultáneamente. Los puertos conocidos se definen en RFC1700.* Por ejemplo, cualquier conversación que se enlace con la aplicación FTP usará el número de puerto estándar 21.

* Un RFC(Request for Comments) es una serie de notas en las cuales se describen los estandares o recomendaciones, y se les asigna un numero RFC, el cual una vez publicado no podra ser cambiado y en caso de que se quieran hacer modificaciones estas se haran en un nuevo RFC y se le asignara otro numero RFC.

A las conversaciones en las que no se relaciona una aplicación con un número de puerto conocido, se le asigna un número de puerto seleccionados al azar dentro de un intervalo específico. Como se mencionó, estos números de puerto se usan como direcciones de origen y de destino en el segmento TCP. Algunos puertos están reservados tanto en TCP como en UDP, pero es posible que no se desarrollen aplicaciones que los utilicen. Los números de puerto tienen los siguientes intervalos asignados:

- Los números menores que 255 están designados para aplicaciones públicas.
- Los números del 255 al 1.023 se asignan a empresas para aplicaciones comerciales.
- Los números mayores que 1.023 no están regulados.

Un sistema final usa un número de puerto para seleccionar la aplicación adecuada. Un puerto de origen es asignado dinámicamente por el host de origen.

2.4.2.4 INTERCAMBIO DE SEÑALES DE TRES VÍAS CONEXIÓN ABIERTA TCP

Para que se establezca o inicie una conexión, los dos TCP utilizan procesos o estaciones finales en lugar de los TCP y deben sincronizarse en los números de secuencia inicial (ISN) de cada uno. Los números de secuencia se utilizan para controlar el orden de la comunicación y para garantizar que no existan datos faltantes que requieran varios paquetes. El número de secuencia inicial es el número de inicio que se utiliza cuando se establece una conexión TCP. El intercambio de los números de secuencia inicial durante la secuencia de conexión garantiza que se puedan recuperar datos perdidos si se producen problemas más tarde.

La sincronización se logra intercambiando los segmentos que transportan los ISN y un bit de control denominado SYN, que significa sincronizar (los segmentos que transportan el bit SYN también se denominan SYN). Para que la conexión se realice con éxito, se requiere un mecanismo adecuado para seleccionar una secuencia inicial y un intercambio de señales levemente complicado para intercambiar los ISN.

La sincronización requiere que cada parte, envíe su propio ISN y que reciba una confirmación (acuse de recibo) y un ISN desde la otra parte. Cada parte debe recibir el ISN de la otra parte y enviar un acuse de recibo (ACK) en un orden específico (Fig. 2.4.2.4.a).

2.4.2.5 ACUSE DE RECIBO SIMPLE Y OPERACIONES EN VENTANA TCP

El tamaño de ventana se refiere a segmentos de mensajes que se pueden transmitir mientras se espera un acuse de recibo. Una vez que un host trasmite la cantidad de bytes correspondientes al tamaño de ventana, debe recibir un acuse de recibo antes de que se pueda enviar más mensajes.

El tamaño de ventana determina la cantidad de datos que la estación receptora puede aceptar a la vez. Con un tamaño de ventana de 1, se debe confirmar la recepción de cada segmento antes de que se transmita otro segmento. Esto da como resultado un uso ineficaz del ancho de banda por parte del host.

El propósito de las operaciones en ventana es mejorar el control de flujo y la confiabilidad. Lamentablemente, con un tamaño de ventana de 1, lo que se obtiene es un uso poco eficiente del ancho de banda.

Para regular el flujo de datos entre dispositivos, el TCP utiliza un mecanismo de control de flujo. El TCP receptor envía una ventana al TCP emisor. Esta ventana especifica la cantidad de bytes, comenzando por el número de acuse de recibo, que el TCP receptor está preparado para recibir.

El TCP utiliza acuses de recibo que incorporan una expectativa, lo que significa que el número de acuse de recibo hace referencia al siguiente octeto esperado. Cuando decimos deslizante en la expresión ventana deslizante, nos referimos a que el tamaño de la ventana se negocia dinámicamente durante la sesión TCP. Una ventana deslizante da como resultado un uso más eficiente del ancho de banda por parte del host debido a que un tamaño mayor de ventana permite la transmisión de datos mientras se espera el acuse de recibo.

TCP transmite los segmentos por orden secuencial con un acuse de recibo que incorpora una referencia anticipada. Cada datagrama es numerado antes de la transmisión. En la estación receptora, TCP vuelve a unir los segmentos para formar un mensaje completo. Si falta algún número de secuencia en la serie, ese segmento se retransmite. Si no se confirma la recepción de un segmento dentro de un periodo determinado, éste se trasmite de nuevo.

Los números de secuencia y de acuse de recibo son direccionales, lo que significa que la comunicación se produce en ambas direcciones. La secuencia y los acuses de recibo tienen lugar con el emisor ubicado a la izquierda. Además, el TCP proporciona una comunicación totalmente full-dúplex y como resultado, los acuses de recibo proporcionan confiabilidad.

2.5 LA CAPA DE INTERNET

La capa de Internet del stack de TCP/IP corresponde a la capa de red del modelo OSI. Cada capa tiene la responsabilidad de portar paquetes a través de una internetwork utilizando direccionamiento basado en software.

- IP proporciona un enrutamiento para la entrega de datagramas de "mejor esfuerzo", sin conexiones. No tiene en cuenta el contenido de los datagramas. Simplemente, busca un modo para desplazar los datagramas a su destino.
- El protocolo de mensajes de control de Internet (ICMP) suministra capacidades de control y de envío de mensajes.
- El protocolo de resolución de direcciones (ARP) determina la dirección de la capa de enlace de datos para las direcciones IP conocidas.
- El protocolo de resolución de direcciones inversas (RARP) determina las direcciones de red cuando se conocen las direcciones de la capa de enlace de datos.

2.5.1. DATAGRAMA IP

Un datagrama IP contiene un encabezado IP y datos. Definición de los campos:

- VERS: número de versión.
- HLEN: longitud de encabezado, en palabras de 32 bits.
- Tipo de servicio: có mo se debe manejar el datagrama.

- Longitud total: longitud total (encabezado más datos).
- Identificación, señaladores y compensación de fragmentos: proporciona fragmentación de datagramas para permitir distintas MTU en la Internet.
- TTL: Campo de cuenta regresiva de tiempo de existencia. Cada estación debe disminuir este número en incrementos de uno o de la cantidad de segundos durante la cual requiere el paquete. Cuando el controlador llega a cero, el TTL se vence y el paquete se libera. TTL retiene los paquetes para evitar que viajen eternamente por la Internet en busca de destinos inexistentes.
- Protocolo: Protocolo de la capa superior (capa 4) que envía el datagrama. El campo de Protocolo determina el protocolo de la capa 4 que se transporta dentro de un datagrama IP. Aunque la mayoría del tráfico IP usa TCP, otros protocolos pueden usar IP. Cada encabezado IP debe identificar el protocolo de la capa 4 de destino para el datagrama. A los protocolos de la capa de transporte se les asigna números, de manera similar a la que se utiliza para los números de puerto. IP incluye el número de protocolo en el campo de protocolo.
- Suma de comprobación del encabezado: verificación de integridad del encabezado.
- Dirección IP de origen y dirección IP de destino: Dirección IP de 32 bits que identifican los dispositivos finales que participan en la comunicación.
- Opciones IP: verificación, depuración, seguridad y otras cuestiones de la red.

2.5.2. DIRECCIONAMIENTO IP

En redes existen dos esquemas de direccionamiento. El esquema de direccionamiento MAC y el esquema de direccionamiento IP.

Tal como se indica una dirección IP se basa en el protocolo de Internet. Cada LAN debe tener su propio direccionamiento IP, ya que la IP es fundamental para que se produzca el intercambio en las WAN. Las direcciones IP existen en la capa 3, la capa de red del modelo de referencia OSI. A diferencia de lo que ocurre con las direcciones MAC, que existen en un espacio de direccionamiento plano, las direcciones IP son jerárquicas. Una dirección IP incluye la dirección del dispositivo, así como la dirección de la red en la que ésta se ubica. Por lo tanto si un dispositivo se traslada de una red a otra, se debe cambiar la dirección IP del dispositivo para indicar que se ha realizado dicho cambio. El direccionamiento IP hace posible que los datos que pasan por los medios de red de la Internet llegue a su destino. La razón por la cual las direcciones IP se escriben en forma de bits es que de este modo los equipos informáticos pueden comprender la información que contienen. Para que los datos se transmitan a través de los medios, primero deben transformarse en impulsos eléctricos. Cuando un equipo recibe estos impulsos eléctricos, reconocen dos elementos: la presencia o ausencia de tensión en el cable. Como un equipo puede reconocer sólo dos elementos, se utiliza un esquema de números binarios.

2.5.2.1. SISTEMA DE NUMERACIÓN BINARIA

Una dirección IP es un valor de 32 bits escritos en forma de 4 octetos. Esto significa que existen cuatro grupos, cada uno de los cuales contiene ocho números binarios compuestos por 1 y 0. Como resulta difícil acordarse de una dirección de 32 bits de largo, se desarrolló una forma más sencilla de direcciones IP mediante el uso de número decimales. Denominado dirección de punto decimal.

2.5.2.2. CLASES DE DIRECCIONES IP

Para garantizar que cada número de red en la Internet sea único y distinto de cualquier otro número, una organización denominada Centro Internacional de Información de la Red (NIC), asigna bloques de direcciones IP a las empresas basándose en los tamaños de sus redes.

Cada dirección IP consta de dos partes: el número de red y el número de host. El número de red identifica la red de la que forma parte el dispositivo. El número de host identifica la conexión del dispositivo a esa red. NIC asigna 3 clases de direcciones IP. Reserva las direcciones IP de clase A para entidades gubernamentales, las direcciones IP de clase B para empresas medianas y las direcciones de clase C para todos los demás.

Cuando las direcciones IP de clase A se escriben en formato binario, el primer bit siempre es 0. Cuando las direcciones de clase B se escriben en formato binario, los primeros dos bits siempre son 1 y 0. Cuando las direcciones IP de clase C se escriben en formato binario, los 3 primeros bits siempre son 1, 1 y 0.

2.5.2.3 MÁSCARAS DE SUBRED

Las subredes se ocultan de las redes exteriores mediante el uso de máscaras denominadas máscaras de subred. Una máscara de subred tiene como propósito indicar a los dispositivos la parte de una dirección que corresponde al número de subred y la parte que corresponde al host.

Las máscaras de subred utilizan el mismo formato que el direccionamiento IP, también tienen una longitud de 32 bits y están divididas en 4 octetos. En las máscaras, la parte que corresponde a la red y a la subred contiene una serie ininterrumpida de números uno y la parte que corresponde al host contiene ceros.

Ejemplos:

Clase A	Red	Máscara
	25.0.0.0	255.0.0.0
	08.0.0.0	255.0.0.0
Clase B	132.248.0.0	255.255.0.0
	137.25.0.0	255.255.0.0
Clase C	221.240.56.0	255.255.255.0
	210.220.85.0	255.255.255.0

2.5.3. PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET (ICMP)

El ICMP es implementado por todos los host TCP/IP. Los mensajes ICMP se transmiten en datagramas IP y se utilizan para enviar mensajes de error y de control. ICMP utiliza los siguientes tipos de mensajes definidos:

- Destino inalcanzable
- Tiempo agotado
- Problema de parámetro
- Suprimir un origen
- Redireccionar
- Eco
- Respuesta en eco
- Timestamp (indicador de hora)
- Respuesta timestramp (indicador de hora)
- Solicitud de información
- Respuesta de información
- Solicitud de dirección
- Respuesta de dirección

Prueba de ICMP: Si un router recibe un paquete que no puede entregar a su destino final, el router le envía un mensaje ICMP de "host inalcanzable" al origen.

Una solicitud de eco es la que el router origen envía al router destino. Es posible que el mensaje no se pueda entregar por que no existe ninguna ruta conocida hacia el destino; una respuesta en eco es una respuesta exitosa a un comando **ping**.

2.5.4. PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES (ARP) Y PROTOCOLO DE RESOLUCIÓN INVERSA DE DIRECCIONES (RARP)

Para que dos máquinas de una determinada red se puedan comunicar, cada una debe de conocer la dirección física (MAC) de la otra. Por medio de la difusión de los ARPs (Protocolos de Resolución de Direcciones), un host puede de manera dinámica, descubrir la dirección de la capa MAC correspondiente a una dirección de la capa de red Particular. Por lo tanto ARP se utiliza para resolver o asignar una dirección IP conocida a una dirección de subcapa MAC. Para determinar la dirección de destino para un datagrama, se consulta la tabla de memoria caché ARP. Si la dirección no figura en la tabla, ARP envía una difusión (broadcast) que busca la estación de destino. Cada estación en la red recibe el broadcast, y solo la máquina que la tiene contesta enviando su dirección MAC que es colocada en la tabla de ARP del equipo origen.

RARP (Protocolo de Resolución Inversa de Direcciones) se utiliza para mapear direcciones de la capa MAC con direcciones IP, RARP que es la lógica inversa de ARP, puede ser utilizado por estaciones de trabajo sin disco que no conozcan sus direcciones IP cuando se inicializan. RARP se basa en la presencia de un servidor RARP que cuente con una entrada en la tabla, o en otro medio para responder a las solicitudes RARP. En el segmento local, se puede utilizar RARP para iniciar una secuencia de carga de sistema operativo a distancia.

CAPÍTULO III
H.323

3.1 DEFINICIÓN DEL ESTÁNDAR H.323

El estándar H.323, se define como una especificación que describe los protocolos para las comunicaciones en tiempo real de las redes basadas en el intercambio de paquetes IP, esto ha sido ratificado por la organización que coordina las normas internacionales para las redes y servicios de telecomunicación global *ITU (Unión Internacional de Telecomunicaciones)* como el estándar que permite la integración de audio, video, y datos para su intercambio en comunicaciones de redes de área local (LAN) como Ethernet o Token Ring, redes con modo de transmisión asíncrona (ATM), líneas arrendadas, o redes Frame Relay; así como a través de redes de área amplia (WAN).*

El H.323 es un estándar bastante flexible, ya que es independiente del hardware y del sistema operativo; además su diseño permite la compatibilidad de la red independientemente de su topología y su interacción en cualquier ambiente basado en el protocolo de Internet (IP).

H.323 no incluye estándares directos para garantizar una calidad de servicio. Contiene descripciones de modelos de llamadas, procedimientos de señalización y la descripción de equipos y componentes para conferencia en redes que se comunican por paquetes.

El estándar define una amplia gama de características y funciones, algunas de estas son requeridas, otras son opcionales. H.323 define cuatro componentes y la forma en que estos actúan recíprocamente entre si.

Estos son:

- Terminales
- Gateways
- Gatekeepers
- Unidad de Control Multipunto (MCU)

Entre las características más importantes del estándar H.323 tenemos:

- H.323 establece los estándares para audio y vídeo, asegurando que los equipos de distintos fabricantes se entiendan.
- H.323 contempla la gestión del ancho de banda disponible para evitar que la LAN se colapse con la comunicación de audio y vídeo, por ejemplo, limitando el número de conexiones simultáneas.
- H.323 se apoya en la norma T.120 para la colaboración y el manejo de datos que pueden ocurrir con el audio y vídeo juntos o separados.
- H.323 utiliza los mismos algoritmos de compresión para el vídeo y el audio que la norma H.320, e introduce algunos nuevos.
- H.323 utiliza los procedimientos de señalización de los canales lógicos del estándar H.245, los cuales se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y cómo se codifica y decodifica.
- Debido a que la comunicación H.323 es independiente de la topología de red, la red donde se comunican los puntos terminales H.323, pueden tener un sólo segmento o anillo, o bien puede ser más compleja, hasta requerir el paso por diversos concentradores, puentes, gateways o módems.

El H.323 también define videoconferencia punto a punto, donde los sitios participantes se están viendo uno al otro y pueden interactuar totalmente; así

* ITU –T Recomendation H.323 Version 4 (2000)

como multipunto, en la que un sitio establece comunicación con varios puntos remotos.

Dado que la videoconferencia tiene como objetivo fundamental establecer comunicación interactiva, simultánea y simétrica; por medio del intercambio de imágenes, audio y prácticamente cualquier tipo de información audiovisual; el estándar H.323 incluye funciones de videoconferencia que permiten controlar el ancho de banda del canal de comunicaciones requerido para transmitir señales de audio y vídeo que contienen gran cantidad información:

3.1.1 PERSPECTIVA HISTÓRICA DE H.323

La Unión Internacional de Telecomunicaciones (ITU), define una familia de estándares con los cuales proporciona las normas para las comunicaciones multimedia uno de estos estándares lo constituye el H.323. En el pasado los diseñadores y fabricantes de productos de computación estaban poco influenciados por la industria de las telecomunicaciones. La especificación del diseño de las telecomunicaciones ha evolucionado gradualmente en el transcurso de aproximadamente 100 años y en los últimos tiempos han tenido el soporte y dirección de las regulaciones gubernamentales. Los clientes de los productos en telecomunicación requieren de un 99.9% de confiabilidad e interoperatividad de los equipos en el extremo final del usuario. En contraste, la industria de la computación tiene la característica de sacar al mercado nuevos productos bajo condiciones de prueba, en los cuales los clientes toleran un bajo nivel de confiabilidad e interoperatividad. Solamente en algunos casos los clientes exigen un estándar cuando ello es indispensable.

Antes de la adopción, por parte de la industria, del estándar H.323 para comunicación multimedia, los fabricantes de sistemas de computación y periféricos habían tomado muy poco en consideración las especificaciones establecidas por el instituto de los estándares de las telecomunicaciones internacionales. *

Antes de H.323, la ITU se había enfocado exclusivamente en la estandarización de las redes globales de telecomunicaciones. Por ejemplo, en 1985 se comenzó el trabajo en la especificación que define el envío de imagen y voz sobre redes de circuitos conmutados, tales como RDSI. Posteriormente, 5 años después se lleva a cabo la ratificación de la norma H.320 por el CCITT en Diciembre de 1990, y fue hasta 3 años después que se dispuso que los equipos cumplieran con la norma y que permitieran la interoperabilidad entre sí. *

En Enero de 1996 un grupo de compañías de soluciones de redes y de computadoras propuso la creación de un nuevo estándar para incorporar videoconferencia en la LAN, en principio las investigaciones se centraron en las redes de área local, por ser estas más fáciles de controlar, pero después con la expansión de Internet, se tuvieron que tener en cuenta todas las redes IP dentro de una recomendación, marcando con esto el comienzo del estándar H.323.

En mayo de 1997, fue cuando formalmente el grupo de ingeniería de ITU redefinió el H.323 como la Recomendación para los sistemas de comunicaciones multimedia, la cual es una tecnología para la transmisión de audio en tiempo real, vídeo y comunicación de datos sobre Redes Basadas en Paquetes (PBN) (fig 3.1.1a) cual podría no proveer una garantía de calidad de servicio (QoS).**

* Bruce Kravitz. "H.323 Technology ", Vtel Corporation (1998)
** ITU –T Recomendation H.323 Version 4 (2000)

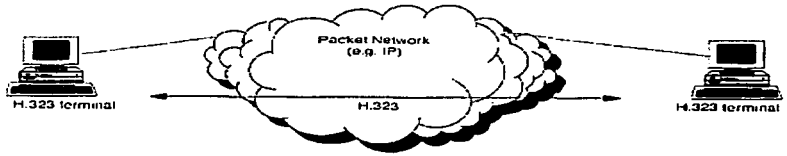


Fig. 3.1.1.a Redes Basadas en Paquetes

H.323 podría ser aplicado en una variedad de mecanismos como por ejemplo: videoconferencia, telefonía por Internet, audio y video (Videotelefonía), conferencia comercial, aprendizaje a distancia, equipos manejando voz, datos y video, en tiempo real, etc. H.323 puede ser aplicado a comunicaciones multimedia multipunto ya que contempla el control de la llamada, gestión de la información y el ancho de banda. Estas redes podrían consistir de un sólo segmento o tener una topología compleja la cual incorporara muchos segmentos de red, interconectados por otros enlaces de comunicaciones. Se hace notar que la operación de los terminales H.323 sobre segmentos múltiples de una red LAN (incluyendo Internet) puede resultar con un pobre performance. Los posibles recursos mediante los cuales la calidad del servicio puede ser garantizada en estos tipos de redes LAN y redes Internet, están más allá del alcance de esta recomendación, ya que es necesario de la ayuda de otros protocolos que no están contemplados en esta recomendación, y los cuales permitirán tener una calidad de servicio.

H.323 es comúnmente llamado un estándar, pero la ITU lo considera como una recomendación mas que un estándar, ya que las recomendaciones están abiertas a la interpretación de diferentes fabricantes y con esto deja libertad a los fabricantes para implementar capacidades que cumplan con los requerimientos de aplicaciones especiales. Las aplicaciones y productos interoperan, permitiendo la comunicación entre los usuarios sin necesidad de que éstos se preocupen por la

compatibilidad de sus sistemas. Durante el desarrollo de las especificaciones H.324 y H.323 para comunicación de multimedia, la colaboración entre la industria de la telecomunicación y la industria de la computación creció enormemente. El resultado de todo esto es que estas especificaciones han progresado más rápidamente que las precedentes y por otra parte las experiencias e innovaciones de ambas industrias convergen cada vez más hacia un objetivo común que es el usuario final.

3.1.2 H.323 UNA EXTENSIÓN DE H.320

H.320 es conocido como una sombrilla de recomendaciones individuales, cada una de las cuales cubre un diferente aspecto de comunicaciones. El H.320 describe normas para la videoconferencia punto a punto y multipunto en las Redes Digitales de Servicios Integrados (ISDN). Este estándar gobierna los conceptos básicos para el intercambio de audio y video en el proceso de comunicación.

La tecnología H.320 requiere típicamente redes separadas para el vídeo y los datos. Esto supone doble cableado e infraestructuras de red. Este modelo incrementó el costo de implantación por sistema. Por lo tanto como derivado de las anteriores recomendaciones, el H.323 presenta diversos estándares que permite a usuarios que han invertido cantidades considerables en sistemas H.320 en mejorar su operación con equipos personales de bajo costo.

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 al terminal no soporta servicios suplementarios tales como enrutado de llamadas, transferencia o retención. Son servicios a los que estamos acostumbrados por la tecnología de las centrales telefónicas.

En 1990 H.320 consistió de H.261 para video, G.711 para audio y otras tres recomendaciones para mezclar señales y control de llamada, otro componente

importante ha sido agregado en el transcurso de los años. La versión más reciente de H.320 se dio en el año 1996.*

H.323 se fundamenta en las especificaciones del H.320. Muchos de los componentes del H.320 se incluyen en el H.323.

H.323 se puede ver como una extensión del H.320. A diferencia de H.320 que requiere circuitos dedicados o conmutados, los sistemas H.323 dejan el control a las preexistentes redes IP para la comunicación bajo el T.120.

El estándar H.323 fue diseñado específicamente con las siguientes ideas en mente:

- 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.

H.323 se construye sobre muchos de los elementos del H.320 y a la vez amplia sus capacidades. Algunas de las capacidades añadidas resultan del comportamiento inherente al tráfico de paquetes y su forma de ser transmitidos. Otras capacidades resultan de las mejoras en las técnicas de compresión y señalización que han sido desarrolladas a lo largo del tiempo. Por ejemplo, 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., con resoluciones que van desde sub-QCIF hasta 4xFCIF(véase en el capítulo 3.2.1.2).

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 en

* ITU –T Recomendation H.320 (1998)

resolución QCIF. Además, una terminal puede soportar otros modos de vídeo con algoritmos propietarios o estándares.

Todas las terminales H.323 deben soportar audio. Y 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, una terminal debe ser capaz de codificar y decodificar la voz usando otros diferentes algoritmos.

El compartir datos es opcional en H.323, pero para estar presente, debe cumplir la norma T.120 (véase en el capítulo 3.2.3).

Algunas implantaciones de H.323 en videoconferencia, tendrán equipos de comunicación con vídeo, como un sistema interactivo, bidirecional y en tiempo real; pero no todas, pues algunas terminales H.323 son capaces de recibir y no de enviar secuencias de vídeo, para esto se utilizan tecnologías de *streaming vídeo* o envío de vídeo en una dirección. Por ejemplo, los proveedores de contenidos en Internet, recogen secuencias de vídeo para posteriormente difundirlas por enlaces IP, con este modelo de espectador se 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. H.320 está centrado en los puntos terminales y el H.323 se conforma con un modelo más orientado a la red; así que las características de una "solución" H.323 pueden encontrarse 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.

3.1.2.1 VENTAJAS DE LA TECNOLOGÍA H.323 CON RESPECTO A H.320

- Reducción de los costos de operación.

En H.323 se pueden utilizar los cableados de campus LAN, 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 separadas para el vídeo y los datos. Esto supone doble cableado e infraestructuras de red. Este modelo incrementa el costo de implantación por sistema.

- Más amplia difusión y mayor portabilidad.

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 salas o de las computadoras personales no podrán fácilmente soportar vídeo, lo cual limita también la accesibilidad y portabilidad de los sistemas.

- Un diseño Cliente / Servidor rico en prestaciones.

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. Un gatekeeper 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 al terminal no soporta servicios suplementarios tales como encaminado de llamadas, transferencia o retención.

3.2 ARQUITECTURA H.323

La Arquitectura de H.323 (fig.3.2.a) conecta usuarios vía a un sistema de redes heterogéneas con un esquema de direccionamiento universal y define un conjunto de funciones específicas para el framing y control de llamada, Codecs de audio y video, y comunicaciones de datos T.120, como se muestra en la figura 3.2.a también se muestran las interfaces para la red, y las interfaces de equipo de audio y video.
Esta arquitectura es la implementación más común de la especificación H.323. Esta misma arquitectura también puede implementarse para un MCU (Multipoint Control Unit) o Unidad de Control Multipunto H.323, gateway y gatekeeper.

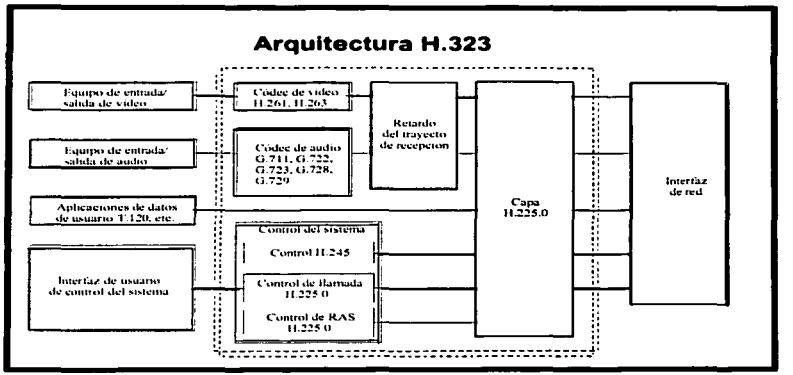


Fig. 3.2.a Arquitectura H.323

Como se mencionó anteriormente H.323 fue construido en base a algunos elementos de H.320 y al mismo tiempo H.323 extendió estas capacidades. Algunas de las adiciones a estas capacidades son resultado del comportamiento de las redes de paquetes, otros resultados se dieron de improvisaciones en compresión y técnicas de señalización.

Todos los componentes H.323 se describirán usando el stack H.323 para transmitir y recibir datos. La información es clasificada en video, audio, datos, control de comunicaciones y control de llamada.

3.2.1 CODECs

Los Codecs son equipos que codifican y decodifican una señal. En H.323 los codecs definen el formato de la información de audio y vídeo y representan la forma en que se comprime y transmite el audio y vídeo sobre la red. H.323 proporciona una variedad de opciones para codificar audio y vídeo. Dos Codecs, G.711 para audio y H.261 para el vídeo, son requeridos por la especificación de H.323. Las terminales H.323 deben ser capaces de enviar y recibir algoritmos de codificación A-law (A-law es el estándar para circuitos internacionales) y μ-law (véase en el capítulo 3.2.1.1), conocido como G.711, como determinado por ITU-T. Los Codecs de audio y vídeo adicionales proporcionan una variedad de rangos de bit estándar, retraso, y opciones de calidad que son convenientes para un rango de selecciones de la red. Usando H.323, los productos pueden negociar los Codecs de audio y vídeo no entendibles.

3.2.1.1 AUDIO CODEC

Como se mencionó todas las terminales H.323 deben soportar audio, de igual manera todas la terminales deben de soportar G.711 que es el algoritmo de audio.

G.711 es el mismo codec que es especificado para H.320.

Un audio CODEC codifica la señal de audio desde el micrófono para que sea transmitida por el terminal H.323 emisor y decodifica el código de audio recibido que es enviado al alta voz del terminal H.323 receptor. El audio es el servicio mínimo que provee el estándar H.323, todas las terminales deben tener al menos un audio CODEC soportado. Las señales de audio contienen sonidos comprimidos y digitalizados. H.323 soporta algoritmos, estándares de audio

CODEC ITU que incluyen G.711, el cual transmite voz a 56 ó 64 Kbps., audio CODECs adicionales como son el G.722 (64,56 y 48 Kbps), G.723.1 (5.3 y 6.3 Kbps), G.728(165Kbps) y G.729(8Kbps). El soporte a otros estándares de voz ITU es opcional ya que cada uno refleja calidad de voz, rango de bits y retardo de señal.

- G.711

G.711 es un estándar internacional para codificar audio sobre un canal que va de 48, 56, y 64 Kbps. Este es un esquema de modulación por codificación de pulsos (PCM) operando a 8kHz y con 8 bits por muestra. G.711 puede codificar frecuencias entre 0 y 4kHz usando modulación por pulsos. Cada uno de estos esquemas de codificación son diseñados de una manera logaritmica robusta. El valor menor de la señal es codificada usando mas bits, el valor alto de la señal requiere menos bits, esto asegura que la baja amplitud de la señal será bien representada, mientras mantenemos suficiente rango para codificar amplitudes altas.

El codec de un rango de bit alto es apropiado para audio sobre conexiones de alta velocidad.

Existen dos métodos de codificar audio : A-law (estándar Europeo) y μ-law (estándar en Japón y Norteamérica) son simétricos alrededor de cero μ-law usa 8 segmentos de 16 intervalos cada uno y en cada uno van de direcciones positivas a negativas, comenzando con un intervalo de tamaño de 2 en el segmento 1 e incrementándose a un intervalo de tamaño de 256 en el segmento 8. A-law usa 7 segmentos, el segmento menor usa un intervalo de 2, es dos veces el tamaño de los otros (32 segmentos). Los restante seis segmentos son "normal", con 16 intervalos cada uno incrementándose a un intervalo de tamaño de 128 en el segmento 7.

Asi, la A-law se sesga hacia la representación de señales más pequeñas con mayor fidelidad.

- G.723

Este codec especifica el formato y algoritmo utilizado para enviar y recibir comunicaciones de voz sobre la red. G.723 es un codec de alta velocidad que transmite audio a 5.3 y 6.3 Kbps que reducen el ancho de banda usado.

3.2.1.2 VIDEO CODEC

Un video CODEC codifica video desde la cámara para que sea transmitida por el terminal H.323 emisor y decodifica el código de video recibido el cual es enviado a la pantalla de video en el terminal receptor, H.323 especifica soporte opcional de video, sin embargo en la recomendación ITU H.261 menciona que las terminales deben de soportar codificación y decodificación de video

- H.261

Este codec de rango de bit alto es apropiado para el vídeo sobre conexiones de más alta velocidad.

El H.261 provee compatibilidad a través de muchas recomendaciones ITU y es usado con canales de comunicación superiores a 64 Kbps. Codifica completamente la trama inicial, luego codifica sólo las diferencias entre la inicial y las subsecuentes tramas para una mínima transmisión de paquetes. La compensación de movimiento otorga una calidad de imagen como una opción.

- H.263

Este codec especifica el formato y el algoritmo utilizado para enviar y recibir imágenes de vídeo sobre la red. Este codec soporta los formatos de imagen, CIF (common interchange format) o formato de intercambio común, el QCIF (quarter common interchange format) o cuarto de formato de intercambio común, el SQCIF (sub-quarter common interchange format) o sub-cuarto de formato de intercambio

común, (SQCIF) y es superior para transmisión de Internet sobre las conexiones de un rango de bit bajo, tales como un módem a 28.8 Kbps.
El estándar H.263 es una mejora del estándar H.261; mejora la calidad de la imagen usando una técnica de estimación de movimiento de medio pixel, predicción de tramas, y una tabla de codificación Huffman para un bajo rango de bits de transmisión y define cinco estándares de formato de imagen: subQCIF, QCIF, CIF, 4CIF y 16CIF.

3.2.2 CONTROL DE LA LLAMADA

Los siguientes estándares constituyen la Unidad del Sistema de Control, la cual proporciona las capacidades de control de llamada y framing:

3.2.2.1 H.225.0

Esta recomendación describe cómo audio, video, datos y control de la información sobre redes basadas en paquetes pueden ser administradas para proveer servicios en equipos H.323.
H.225 señalización de la llamada es usado para establecer conexiones entre terminales H.323, sobre los cuales los datos en tiempo real pueden ser transportados. La señalización de la llamada cubre el intercambio de mensajes del protocolo H.225 sobre un canal confiable de señalización de la llamada.
Este estándar define una capa que estructura el vídeo transmitido, audio, datos, y streams de control para la salida a la red, y recupera los correspondientes streams de la red. Como parte de transmisión de audio y vídeo, H.225.0 utiliza el formato de paquete especificado por IETF, RTP, y las especificaciones RTCP para las siguientes tareas:

- Framing lógico.
- Define cómo el protocolo empaqueta los datos de audio y vídeo en bits para él transportarlos sobre un canal de comunicación seleccionado.
- Secuencia de numeración.
- Determina el orden de los paquetes de datos transportados sobre un canal de comunicaciones.
- Detección de error.
- Después de comenzar una llamada, uno o más conexiones RTP o RTCP son establecidas. Múltiples streams permiten al H.225.0 enviar y recibir diferentes tipos de medios de comunicación simultáneamente, cada uno con su propia secuencia de numeración y opciones de calidad de servicio. Con soporte RTP y RTCP, el nodo receptor sincroniza los paquetes recibidos en el orden apropiado, para que el usuario escuche y vea la información correctamente.

3.2.2.2 H.225 RAS

La norma de H.225.0 también incluye el registro, admisión, y estado de control (RAS), el cual es utilizado para comunicar terminales con el gatekeeper. Un canal RAS es usado para el intercambio de mensajes de RAS, el canal de señalización RAS hace las conexiones entre el gatekeeper y los componentes H.323 disponibles. El gatekeeper controla la terminal H.323, gateway, y el acceso MCU a la red de área local concediendo o negando el permiso a las conexiones H.323.

3.2.2.2.1 Q.931

Este protocolo define cómo cada capa de H.323 interactúa con capas par, para que los participantes puedan interoperar con aceptación los formatos. El protocolo Q.931 reside dentro de H.225.0. Como parte del control de llamada de H.323, Q.931 es un protocolo de capa de eslabón para el establecimiento de las conexiones y datos framing. Q.931 proporciona un método para la definición de canales lógicos dentro de un canal más grande. Los mensajes de Q.931 contienen un protocolo discriminador que identifica cada mensaje único con un valor de referencia de llamada y un tipo del mensaje. La capa de H.225.0 especifica entonces como estos mensajes de Q.931 son recibidos y procesados.

3.2.2.3 H.245

Este estándar proporciona el mecanismo de control de llamada que permite a terminales H.323-compatibles conectarse a otros. H.245 proporciona un medio estándar para el establecimiento de las conexiones de audio y vídeo - las series de comandos y demandas que deben ser seguidas por un componente al conectarse y comunicarse con otro. Este estándar especifica la señalización, control de flujo y la canalización para los mensajes, demandas, y comandos.

La construcción en el framework de H.245 habilita selección del codec y la capacidad de negociación dentro de H.323. El rango de bit, el rango de frame, el formato de la imagen, y opciones del algoritmo son algunos de los elementos negociados por H.245.

3.2.3 COMUNICACIONES DE DATOS T.120

H.323 utiliza T.120 como el mecanismo para empaque y envío de datos. T.120 puede utilizar la capa de H.225.0 para enviar y recibir los paquetes de datos o simplemente crear una asociación con la sesión de H.323 y usar sus propias capacidades de transporte para transmitir los datos directamente a la red.

Con los streams de datos opcional que proporciona H.323 en conferencia, se apoya la colaboración en red, llevando a cabo transferencia de archivos y compartiendo programas y así soportar datos a través de las capacidades T.120 en clientes y MCUs que controlan y mezclan streams de datos. T.120 provee interoperabilidad punto a punto o multipunto de conferencias de datos en la aplicación, red y niveles de transporte.

3.2.3.1 SERIE T.120

La serie T.120 son los protocolos de transmisión para datos multimedia, el cual proporciona comunicaciones con audio y vídeo en tiempo real.

El estándar T.120 de ITU está formado por una colección de protocolos de comunicación y aplicación desarrollados y aprobados por las industrias de computadoras y telecomunicaciones internacionales. Usando estos protocolos, los desarrolladores pueden crear productos y servicios compatibles en tiempo real, conexiones de datos multipunto y conferencia. Con los programas basados en T.120, múltiples usuarios pueden participar en sesiones de conferencia sobre diferentes tipos de redes y conexiones.

Dependiendo del tipo de producto T.120, el programa puede hacer conexiones, transmitir y recibir datos, y colaborar usando características de conferencia de

datos compatible, como programa compartidos, conferencia de white board, y transferencia de archivo.

3.2.3.2 ARQUITECTURA DE T.120

Esta arquitectura sigue el modelo OSI de Interconexión de los Sistemas Abiertos que especifica una serie de capas, incluyendo los más bajos protocolos para conectar y transmitir datos, y la interacción con protocolos de más alto nivel de aplicación.

T.120 es un estándar que abarca los siguientes estándares y componentes de comunicación y aplicación:

- T.121

T.121 se describe cómo un protocolo de aplicación, como T.127 para la transferencia de archivo, desempeñando las siguientes funciones:

- Registros propios con la conferencia.
- Aplicar estas capacidades local y remotamente.
- Interoperar y negociar las capacidades con otras aplicaciones.

Asegurar la consistencia de la aplicación, T.121 es un estándar requerido para productos desarrollados bajo T.120. El ITU también recomienda que las aplicaciones incorporen T.121 para proporcionar interoperabilidad al producto.

- T.122

Esta norma define los servicios multipunto, los cuales permiten uno o más participantes para enviar datos como parte de una conferencia. Estos servicios multipunto son implementados por T.125, que proporciona el mecanismo para transportación de datos. Juntos, los estándares T.122 y T.125 constituyen los servicios de comunicación multipunto MCS de T.120. T.122 soporta varias tipologías de conferencia.

- T.123

Este estándar es el responsable de la transportación y secuencia de datos, y para controlar el flujo de datos por las redes, incluyendo las funciones conectar, desconectar, enviar, y recibir. Para el transporte de datos, T.123 define una serie de perfiles de interfaces de red. También, T.123 proporciona un mecanismo corrector de error que asegura la entrega de los datos exacta y fiable. El anexo B del T.123, se agrega al T.123 estándar para la conferencia de datos y también define el protocolo para conferencia de datos segura.

- T.124

Este estándar proporciona el control de conferencia genérico (GCC) para iniciar y administrar las conferencias de datos multipunto. El GCC desempeña las siguientes funciones:

- Servidores como el centro de información, dirigiendo usuarios y datos en y fuera de las conferencias y monitorean el progreso para que la última información de la conferencia siempre esté disponible.
- Manteniendo las listas de participantes de la conferencia y sus aplicaciones; el GCC identifica aplicaciones compatibles y rasgos para que los productos puedan interoperar.
- Tracks de los recursos MCS para que los conflictos no ocurran cuando los participantes de la conferencia usan los protocolos de aplicación múltiple, como el T.127 para transferencia de archivos y T.128 para compartir aplicaciones.

- T.125

Este estándar especifica cómo los datos son transmitidos dentro de una conferencia. T.125 define los canales privados y broadcast que transportan los datos, y asegura la comunicación exacta y eficaz entre los múltiples usuarios. T.125 también implementa los servicios multipunto definidos por T.122.

- T.126

Este estándar especifica como una aplicación envía y recibe la información whiteboard, en forma comprimida o expandida, para ver y actualizar la conferencia entre múltiples participantes. El papel de T.126 es manejar el workspace de los multiusuarios proporcionado por el whiteboard.

- T.127

Este estándar define como los archivos son transferidos simultáneamente entre los participantes de la conferencia. T.127 permite seleccionar uno o más archivos y transmitirlos en forma comprimida o expandida a todos o seleccionando a los participantes durante una conferencia.

- T.128

Este estándar fue propuesto por Microsoft como un agregado al estándar T.120 normal y es aceptado por la ITU, ITU-T. T.128 especifica el protocolo que comparte el programa, definiendo cómo los participantes en una conferencia de T.120 pueden compartir programas locales. Específicamente, T.128 permite a los múltiples participantes de la conferencia ver y colaborar en los programas compartidos.

3.2.3.3 BENEFICIOS DE T.120

Los productos y servicios T.120 ofrecen los siguientes beneficios a los usuarios:

- T.120 asegura que varios participantes puedan enviar y recibir datos en tiempo real sin cualquier error en la transmisión de los datos. Los usuarios pueden esperar esta fiabilidad sobre muchos tipos de conexiones soportadas, incluso el TCP/IP.
- Para la conferencia de datos multipunto, el estándar T.120 soporta una variedad de topologías comunes.

- Desarrolladores pueden crear aplicaciones con sólo T.120, o en la combinación con otros estándares de ITU, como el estándar H.323 para conferencia de audio y vídeo.

3.2.3.4 INTEROPERABILIDAD

Una de las características más importantes de la infraestructura T.120 es la interoperabilidad de productos y servicios que soportan el estándar.

La interoperabilidad de productos T.120 es medida en dos niveles: redes y aplicaciones. Los estándares T.122, T.123, T.124, y T.125 constituyen el nivel de gestión de redes de T.120. Los productos y servicios que se encuentran en estos estándares tienen la infraestructura necesaria para hacer lo siguiente:

- Establecer y mantener conferencias sin dependencia de cualquier plataforma.
- Manejar múltiples participantes y programas.
- Enviar y recibir datos con precisión y seguridad encima de una variedad de conexiones de red soportadas.

Los estándares T.126 y T.127 constituyen el nivel de las aplicaciones de T.120. Estos estándares aseguran que los whiteboard electrónicos y aplicaciones de transferencia de archivo desarrollados bajo T.120 pueden interoperar a través de las plataformas y redes, y dentro de las conferencias multiusuario.

3.2.4 PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP)

El RTP proporciona funciones de transporte adaptadas a aplicaciones que transmiten datos en tiempo real, como audio, video o dato de simulación, sobre servicios de red *multicast* o *unicast*.

RTP no hace la reservación de recursos de dirección y no garantiza calidad de servicios para servicios en tiempo real. El transporte de los datos es aumentado por un protocolo de control (RTCP) que permite monitorear la entrega de los datos en una manera escalable a grandes redes multicast, y proporcionar mínimo control y funcionalidad de identificación. El RTP y el RTCP son diseñados para ser independientes del transporte subyacente y las capas de la red. El protocolo soporta el uso de traductores y mezcladores a nivel RTP.

El RTP proporciona los servicios de entrega de extremo a extremo para datos con características de tiempo real, tales como: audio y video interactivos. Entre los servicios se encuentran el tipo de identificación de carga útil (payload), numeración de secuencia, timestamping y monitoreo de entrega.

Las aplicaciones típicamente ejecutan RTP encima de UDP para hacer uso de los servicios de multiplexación y checksum; ambos protocolos contribuyen funcionalmente con partes del protocolo de transporte. Sin embargo, el RTP puede ser usado con otra red subyacente conveniente o protocolos de transporte.

El RTP soporta transferencia de datos a múltiples destinos usando distribución multicast, si es proporcionada por la red subyacente.

El propio RTP no proporciona ningún mecanismo para asegurar oportuna entrega o proporciona otras garantías de calidad de servicio, pero cuenta con estos

servicios en las capas bajas para hacer esto. No garantiza la entrega o previene la entrega fuera de orden, ni asume que la red es fiable y entrega paquetes en secuencia. Los números de secuencia incluidos en el RTP permiten al receptor reconstruir la secuencia de paquetes enviados, pero los números de secuencia deben también ser usados para determinar la situación apropiada de un paquete, por ejemplo en la decodificación de vídeo, sin necesariamente decodificar los paquetes en la sucesión.

Mientras el RTP es diseñado para satisfacer las necesidades de conferencia de multiparticipantes multimedia, no se limita a eso la aplicación particular. El almacenamiento de datos continuos, la simulación distribuida interactiva, y el control y medida de las aplicaciones pueden también encontrar RTP aplicable.

El RTP consiste de dos partes estrechamente unidas:

- El protocolo de transporte en tiempo real (RTP), para llevar datos que tienen propiedades de tiempo real.

- El protocolo de control del RTP (RTCP), para supervisar la calidad de servicios y llevar la información sobre los participantes en una sesión continua.

El RTP representa un nuevo estilo de protocolo que sigue los principios a nivel de aplicación framing y procesamiento de capa integrada propuestos por Clark y Tennenhouse. Es decir, se piensa que RTP es maleable para proporcionar la información requerida por una aplicación particular y a menudo ser integrada en el procesamiento de aplicaciones que más tarde serán implementadas como una capa separada.

Varias aplicaciones de RTP, experimentales y comerciales, han sido ya implementadas de las especificaciones del proyecto. Éstas aplicaciones incluyen las herramientas de audio y vídeo junto con el diagnóstico de las herramientas como los monitores de tráfico. Los usuarios de estas herramientas son miles. Sin

embargo, el Internet actual no puede soportar la demanda potencial completa para servicios en tiempo real. Los servicios de alto ancho de banda que utilizan RTP, tales como vídeo, pueden potencialmente degradar la calidad de servicio de otros servicios de red. Es decir, los implementadores deben de tomar apropiadas precauciones para limitar el uso accidental de ancho de banda. La documentación de la aplicación debe especificar claramente las limitaciones y el posible impacto operacional de alto ancho de banda de los servicios en tiempo real en Internet y otros servicios de la red.

3.2.4.1 ORDEN DE BYTE, ALINEACIÓN Y TIPO DE FORMATO

Todos los campos de enteros son llevados en el orden de byte en la red, esto es, el primero el byte más significativo, a este byte se le conoce como big-endian.

Todos los datos de encabezados son alineados a una longitud natural, es decir, campos de 16 bits son alineados en offsets, campos de 32 bits son alineados en offsets divisibles por cuatro, etc. Octetos diseñados como forrados tienen el valor cero.

El tiempo Wallclock (tiempo absoluto) es representado usando el formato timestamp del protocolo de Tiempo de la Red (NTP), el cual es en segundo relativo a 0h UTC el 1 de enero de 1900. La resolución completa del timestamp NTP es 64 bits sin significado número de punto fijo con la parte entera en los primeros 32 bits y la parte fraccionaria en los últimos 32 bits. En algunos campos donde una representación más compacta es apropiada, solamente la mitad de los 32 bits son usados; esto es los 16 bits bajos de la parte entera y los 16 bits de la parte fraccionaria. Los 16 bits altos de la parte entera debe ser determinados independientemente.

3.2.4.1.1 CAMPOS DE LOS ENCABEZADOS FIJOS RTP

El encabezado RTP tiene el siguiente formato:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ver		P	X	CC				M	PT							Sequence Number															
Timestamp																															
SSRC																															
CSRC																														[0..15]	
:::																															

Los primeros 12 octetos son representados en cada paquete RTP, mientras la lista de identificadores CSRC son presentados solamente cuando es insertado por un mezclador. Los campos tienen el significado siguiente:

Campo	*Descripcion*	*Tamaño*
[illegible]	Version de RTP. Actualmente es la 2	2
[illegible]	Indica si existe informacion adicional al final del paquete. Esta informacion puede ser útil para los algoritmos de encriptación	1
[illegible]	Indica si a continuacion viene una cabecera de extension	1
[illegible]	Numero de identificadores CSRC que siguen a la cabecera fija.	4
[illegible]	Esta indicada para senalar eventos especiales como salirse de los límites.	1
[illegible]	Formato de la información que se transporta para que lo interprete la aplicacion	7
[illegible]	Se incrementa en uno por cada paquete envia, y sirve para que el receptor detecte perdidas de paquetes.	16
Timestamp	Tiempo en el que se muestra el primer octeto de los datos transmitidos en el paquete	32
[illegible]	Synchronization source identifier. Identifica la fuente del paquete	32
[illegible]	Contributing source identifiers. Esta informacion es introducida por los mezcladores para indicar que han contribuido ha modificar la información	32

Version (V): 2 bits. Este campo identifica la versión de RTP. (El valor 1 es usado por la primera versión de RTP y el valor 0 es usado por el protocolo inicial implementado en la herramienta "vat" de audio)

Padding (P): 1 bit. Si éste está activo, el paquete contiene uno o más octetos adicionales padding en el final, los cuales no son parte de la carga útil. El Padding puede ser necesario por algún algoritmo de cifrado con bloques de tamaño fijo o para llevar varios paquetes RTP en la capa de protocolo baja de la unidad de datos.

Extension (X): 1 bit. Si éste está activo, el encabezado fijo es permitido por exactamente una extensión del encabezado.

CSRC count (CC): 4 bits. Este contiene el número de identificadores CSRC que siguen al encabezado fijo.

Marker (M): 1 bit. La interpretación de esta marca está definida por un perfil. Esto permite eventos significantes tales como fronteras frame para ser marcadas en los stream de los paquetes. Un perfil puede definir adicionales bits marcados o especificar que no hay bits marcados por cambiar el número de bits en el tipo de campo de carga útil.

Payload type (PT): 7 bits. Este campo identifica el formato de la carga útil del RTP y determina su interpretación por la aplicación.

Sequence number: 16 bits. El número de secuencia incrementado por uno por cada paquete de datos RTP enviado, y puede ser usado por el receptor que detecta los paquetes perdidos y restaura la secuencia de paquetes. El valor inicial de la secuencia es aleatorio para hacer más difícil el conocimiento del texto en claro de la encriptación en un ataque.

Timestamp: 32 bits. Este refleja el muestreo instantáneo del primer octeto en el paquete de datos RTP. El muestreo instantáneo debe ser derivado de un reloj que se incrementa monotónica y linealmente en tiempo permitiendo la sincronización y los cálculos.

SSRC: 32 bits. Este campo identifica la fuente de sincronización. Este identificador es cambiado aleatoriamente, porque dos fuentes de sincronización con las misma sesión RTP deben tener el mismo identificador SSRC.

CSRC list: 0 a 15, cada 32 bits. La lista CSRC identifica las fuentes de contribución de la carga útil contenidas en el paquete.

3.2.5 PROTOCOLO DE CONTROL DEL RTP (RTCP)

El protocolo de control RTCP está basado en la transmisión periódica de paquetes de control a todos los participantes en la sesión, usando los mismos mecanismos de distribución como los paquetes de datos. El protocolo subyacente debe proporcionar multiplexación de los datos y paquetes de control, por ejemplo usando separados números de puerto con UDP. El RTCP realiza cuatro funciones:

1. La función primaria es proporcionar la regeneración en la calidad de la distribución de los datos. Ésta es una parte integra del papel de RTP como un protocolo de transporte y se relaciona al flujo y funciones de control de congestión de protocolos de transporte. La regeneración puede ser directamente utilizada para control de codificaciones adaptables, pero experimentos con IPmulticasting han mostrado que también es crítico conseguir la regeneración de los receptores para diagnosticar fallas en la distribución enviando recepción de regeneración se informa a todos los participantes permitiendo a uno que esté observando los problemas a evaluar si esos problemas son locales o globales. Con un mecanismo de distribución como el multicast de IP, también es posible para una entidad como

un proveedor de servicio de red quién no es involucrado por otra parte en la sesión para recibir la información de la regeneración y actuar como un monitor third party para diagnosticar problemas de red. Esta función de regeneración es realizada por el remitente RTCP y el receptor informa.

2. RTCP lleva un identificador persistente a nivel de transporte para una fuente RTP llamada el nombre canónico o CNAME. El identificador de SSRC puede cambiar si un conflicto se descubre o un programa se reinicia, los receptores requieren el CNAME para guardar la huella de cada participante. Los receptores también requieren el CNAME para asociar los streams de datos múltiples de participantes dados en un conjunto de sesiones RTP relacionadas, por ejemplo la sincronización de audio y vídeo.

3. Las primeras dos funciones requieren que todos los participantes envíen paquetes RTCP, por consiguiente, la proporción debe controlarse en orden por el RTP para número grande de participantes. Teniendo cada participante que enviar sus paquetes de control a todos los otros, cada uno puede independientemente observar el número de participantes. Este número se usa para calcular la proporción en la cual los paquetes se envían.

4. Una cuarta, la función optativa es llevar la sesión mínima de control de información, por ejemplo identificación de los participantes a ser desplegada en la interfaz de usuario. Esto es más probablemente útil en sesiones "flojamente controladas" dónde los participantes entran y salen sin el control de número de miembros o parámetros de negociación. RTCP sirve como un canal conveniente para localizar a todos los participantes, pero necesariamente no es esperado para apoyar todo el control de comunicación de requisitos de una aplicación.

Las funciones de 1 a 3 son mandatorias cuando el RTP es usado en el medioambiente IP multicast, y son recomendadas para todos los ambientes.

3.2.5.1 FORMATO DEL PAQUETE RTCP

RTCP tiene los siguientes paquetes:

Paquete	*Descripcion*
[illegible]	Sender Report. Sirve para la transmision y recepcion de las estadisiticas de los participantes que son emisores activos
[illegible]	Receiver report : Sirve para la recepcion de estadisticas de los participantes que no son emisores activos
[illegible]	Source description. Describe la fuente, incluye el CNAME
[illegible]	Indica un fin de la participacion en el grupo
[illegible]	Funciones especificas de aplicacion

SR: Sender report, Reporte del remitente, para transmisión y recepción de estadísticas de los participantes que son los remitentes activos.

RR: Receiver report, Reporte de los receptores, para la recepción de estadísticas de los participantes que no son los remitentes activos.

SDES: Source description items, artículos de descripción de las fuentes, incluyendo el CNAME

BYE: Indica fin de la participación.

APP: Especifica funciones de la aplicación.

Cada paquete RTCP empieza con una parte fija que es similar a los paquetes de datos RTP, seguido por elementos estructurados que pueden ser de longitud variable de acuerdo con el tipo de paquete.

Para cumplir las funciones de este protocolo se imponen las siguientes condiciones:

- Las estadísticas de recepción (en SR o RR) deben ser enviadas tan a menudo como lo permita el ancho de banda para maximizar la resolución de las estadísticas.
- Los nuevos receptores deben recibir el CNAME de una fuente tan pronto como sea posible para identificar la fuente.
- El número de tipos de paquetes deben aparecer en el primer paquete para determinar su tratamiento.
- El intervalo de transmisión de paquetes RTCP debe ser calculado de forma que se permita tener sesiones que vayan desde pocos participantes a miles. Para ello, en cada sesión se asume que el tráfico de datos está sujeto a un límite denominado "ancho de banda de sesión" que se divide entre los participantes. Este ancho de banda debe ser reservado y limitado por la red. El parámetro de ancho de banda de sesión debe ser proporcionado por la aplicación de control de sesión. A partir de este valor y en función del número de participantes se calcula el intervalo con una formula empírica.

El objetivo de este protocolo es la de transportar información de tiempo real. No se plantea como un nuevo nivel sino como una parte de otros niveles como el de aplicación o sesión. Su única utilidad es su utilización con otros protocolos de red que si que proporcione lo que le falte.

Resumen de las características más importantes:

- Si sólo proporciona los niveles de red

Características:

- Ligero: Implementación simple.
- Flexible: No indica algoritmos.
- Neutral frente transporte.
- Escalable: Unicast, multicast, broadcast.

- Separación de datos y control.
- Seguro: posibilidad de encriptación y autenticación.
- Datos: Temporización, detección de perdidas, etiquetados de contenidos.
- Control: Realimentación de QoS, estimación de miembros y detección de bucles.

Funcionalidad

- Segmentación realizada por UDP o IP.
- Resecuenciación de paquetes.
- Detección de pérdidas para estimación posterior.
- Sincronización entre media: sincronización y control de retrasos.
- Realimentación de QoS y velocidad.
- Identificación de la fuente.

3.3 COMPONENTES H.323

El H. 323 es considerado algunas veces como una especificación paraguas, dando a entender que hace referencia a otras recomendaciones. La serie H. 323 incluye otras recomendaciones tales como el H.225.0 Packet and Synchronization, el H. 245 Control, los H. 261 y H. 263 Video Codecs, los G. 711, G. 722, G. 728, G. 729 y G. 723 Audio Codecs y la serie T. 120 de protocolos de comunicaciones multimedia. Todas estas especificaciones juntas definen un número de nuevos componentes de redes

- H. 323 Terminal
- H. 323 MCU
- H. 323 Gatekeeper
- H. 323 Gateway

Los cuales, interoperan en el extremo final del usuario con otros estándares amigables y redes, mediante el H. 323 Gateway tal como está representado en la siguiente figura (Fig. 3.3.a).

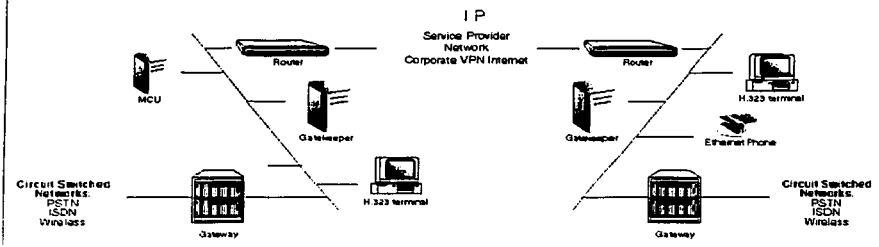


Fig. 3.3.a Componentes H.323

3.3.1 H. 323 TERMINAL

Los terminales H.323 son los clientes finales en la LAN, que proporcionan una comunicación multimedia bidireccional en tiempo real. Un terminal H.323 puede ser una simple PC corriendo aplicaciones multimedia. Todos los terminales deben soportar la comunicación de voz, mientras que la de video y datos son opcionales. Un ejemplo de una terminal H.323 es mostrada en la siguiente figura (fig.3.3.1.a).

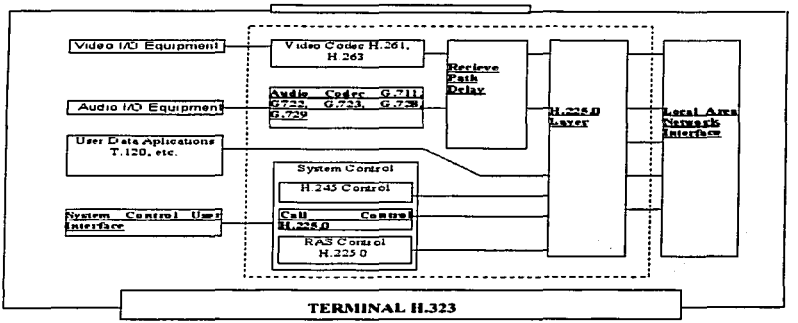


Fig 3.3.1.a Terminal H.323

El diagrama muestra las interfaces del equipo del usuario, video codec, audio codec, equipo telemático, capa H.225.0, sistemas de control de funciones y la interfase para la red basada en paquetes. Todos los terminales H.323 debe tener una unidad de control de sistema, interfaces de red y una unidad audio codec. La unidad de video codec y las aplicaciones de datos del usuario son opcionales.

El terminal H. 323 permite más de un canal para cada una de las modalidades de uso.

Los siguientes elementos están definidos dentro de la recomendación de H.323, en cuanto al Terminal se refiere:

- El video Codec (H.261, etc.) codifica el video desde la fuente de video (por ejemplo una cámara) para la transmisión y descodificación la recibe el video codec el cual lo despliega en un display de video.
- El audio codec (G.711,etc) codifica la señal de audio desde el micrófono para la transmisión y descodificación, lo recibe el audio codec el cual lo saca por el altavoz.
- El canal de datos soporta aplicaciones telemáticas como por ejemplo Whiteboards, still transferir imágenes, intercambio de archivos, acceso a base de datos conferencia audigrafica, etc.
- La unidad de control de sistema (H.245, H.225.0) provee señalización para una apropiada operación del Terminal H.323, mas que nada para el control de la llamada, capacidad de intercambio, señalización de comandos e indicaciones y mensajes que describen cuando está abierto y lleno el contenido de los canales lógicos.
- Capa H.225.0 le da formato al video, audio y los datos que son transmitidos, dentro de mensajes que son puestos en la interfase de la red y repara el video recibido, el audio, los datos y control streams desde mensajes que de igual manera han sido puestos en la interfase de red.

El video codec es opcional. La capacidad de video podría ser suministrada de acuerdo a los requerimientos de esta recomendación. Todos los terminales H.323 que proveen videocomunicaciones podrían ser capaces de codificar y decodificar video de acuerdo a H.261. Opcionalmente una terminal quizá también sería capaz de codificar y decodificar de acuerdo a H.261 o H.263

El terminal H.323 podría opcionalmente enviar más de un canal de video al mismo tiempo al igual que puede recibir más de un canal al mismo tiempo.

Modos de Trabajo.

H.323 soporta diferentes modos de trabajo en base a las capacidades de la red y de los clientes o terminales.

En el momento del establecimiento de la llamada, los terminales intercambian información acerca de ellos mismo entre sí. Este intercambio de información (CAPS) describe la capacidad de cada terminal para recibir y procesar la información recibida. Los terminales con capacidad de transmitir limitan el contenido de su transmisión a lo que el receptor ha indicado que es capaz de recibir. La ausencia de capacidad para recibir indica que el terminal es de solamente emisor. Como ya se ha mencionado anteriormente, ésta es una diferencia fundamental entre los terminales H.320 y H.323.

Además, los terminales pueden dinámicamente cambiar sus capacidades durante una comunicación o sesión, solicitando nuevos servicios y eliminándolos.

3.3.2 H.323 UNIDAD DE CONTROL MULTIPUNTO (MCU)

La unidad de control multipunto de H.323 (MCU), provee soporte para conferencias de tres o más terminales H.323. Todos los terminales que participan en la conferencia establecen una conexión con el MCU. El MCU administra los recursos de la conferencia negociables entre terminales, con el propósito de determinar el audio o video codificación/decodificación (CODEC) que se va a usar. El gatekeeper, gateway y el MCU son lógicamente componentes separados, pero pueden ser implementados como un simple equipo físico.

Una MCU se forma de dos partes: un Controlador Multipunto (MC) que es obligatorio y un procesador multipunto (MP) opcional. En el caso más simple, una MCU puede estar formada por un MC únicamente.

Los Controladores Multipunto, Procesos Multipunto y Unidad de Control Multipunto provee soporte para conferencia multipunto

Controlador Multipunto

Un controlador multipunto (MC) es una entidad H.323 que proporciona las capacidades de negociación entre todos los terminales para conseguir la comunicación. Puede controlar así mismo recursos de la conferencia tales como el vídeo multicast. El MC no realiza mezcla ni conmutación de audio, vídeo o datos.

Procesador Multipunto

Un procesador multipunto (MP) es la entidad H.323 cuyo hardware y software especializado mezclan, conmutan y procesan el audio, vídeo y/o los datos de los participantes en una conferencia multipunto. El MP puede procesar una única secuencia multimedia o varias simultáneamente, dependiente del tipo de conferencia soportada.

3.3.3 H.323 GATEKEEPER

El Gatekeeper (GK) puede ser considerado como el cerebro de la red H.323. Este es el punto principal para todas las llamadas dentro de la red H.323. El Gatekeeper provee importantes servicios como por ejemplo proporciona la traducción de direcciones, autorización y autentificación, es decir el control de acceso a la red de los terminales, gateways, MCUs.

Por lo tanto el Gatekeeper realiza el control de admisión y servicio de translación de direcciones y a la vez administra de ancho de banda. El Gatekeeper también puede proveer de servicios como el de ruteo de llamada y localización de Gateways.

3.3.3.1 CARACTERÍSTICAS DEL GATEKEEPER

El Gatekeeper provee servicio de control de la llamada para Terminales H.323, como por ejemplo traslación de direcciones y administración del ancho de banda como se define con el RAS. El Gatekeeper en redes H.323 es opcional. A pesar de esto, este componente está presente en una red y tanto los terminales como los gateway usan sus servicios. El estándar H.323 define obligatoriamente servicios que el gatekeeper debe proveer y especifica otras funciones que son opcionales las cuales también puede proveer el gatekeeper.

Una característica opcional del gatekeeper es el ruteo de la señalización de la llamada(call-signaling). Los terminales envían mensajes call-signaling a el gatekeeper, el cual va a rutear estos mensajes a los terminales destino, sin embargo esta acción la pueden realizar los terminales directamente ya que pueden mandar los mensajes de call-signaling a sus terminal semejante sin necesidad del gatekeeper. Esta característica del gatekeeper es valiosa, ya que puede monitorear las llamadas y así ofrecer un mejor control de las llamadas en la red.

El ruteo de las llamadas a través del gatekeeper provee mejor rendimiento en la red ya que el gatekeeper puede hacer ruteo basándose en decisiones sobre una variedad de factores como por ejemplo el balanceo de cargas entre gateways.

Un gatekeeper como hemos dicho es opcional en un sistema H.323. Los servicios ofrecidos por el gatekeeper son definidos por el RAS e incluye traslación de direcciones, control de admisión, control de ancho de banda y administración

de zona (figura 3.3.3.1.a). Un gatekeeper es lógicamente un componente de una red H.323 pero puede ser implementado como parte de un gateway o un MCU.

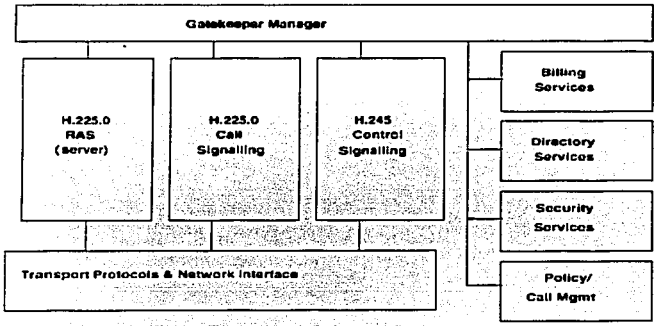


Fig. 3.3.3.1.a H.323 Gatekeeper

3.3.3.2 FUNCIONES DEL GATEKEEPER

Traslación de direcciones.

Las llamadas originadas dentro de una red H.323 pueden usar un alias que va a ser recibida en forma de dirección por la terminal destino. Las llamadas originadas salen de la red H.323 y son recibidas por un gateway que puede estar usando números telefónicos para direccionar hacia terminal destino. Los gatekeeper

trasladan estos números telefónicos o el alias a una dirección IP de la red, la cual de esta manera será recibida por el terminal destino. De esta manera el terminal destino será alcanzado dentro de la red H.323 por medio de la dirección IP.

Control de Admisión

El gatekeeper puede controlar la admisión de los terminales dentro de la red H.323. Éste usa mensajes RAS, solicitud de admisión (ARQ), confirmación (ACF) y rechazo (ARJ), para llevar a cabo esto. El control de admisión podría ser una función nula que admita todas las terminales de la red H.323.

Control de Ancho de Banda

El gatekeeper provee soporte para el control del ancho de banda, usando mensajes de RAS, solicitud de ancho de banda (BRQ), confirmación (BCF) y rechazo (BRJ). Por ejemplo si un administrador tiene especificado un umbral para el número de conexiones simultaneas sobre la red de H.323, el gatekeeper puede no aceptar otra conexión una vez que ha sido alcanzado este umbral. El resultado es limitar el total de ancho de banda destinado del total disponible, dejando así el restante para las aplicaciones de datos. El control del ancho de banda podría ser también una función nula que acepte todas solicitudes para cambios en el ancho de banda.

Administración de zona

El Gatekeeper provee sobre todo funciones de traslación de direcciones, control de admisión, y control de ancho de banda, para terminales, gateways y MCUs localizados dentro de esta zona de control.

Una zona es una colección de todos los terminales, gateways y MCUs manejados por un simple gatekeeper (figura 3.3.3.2.a). Una zona por lo menos incluye un terminal y podría incluir gateways o MCUs. Una zona tiene sólo un gatekeeper.

Una zona podría ser independiente de la topología de red y podría estar conformada de varios segmentos de red que estén conectados usando routers o otros equipos.

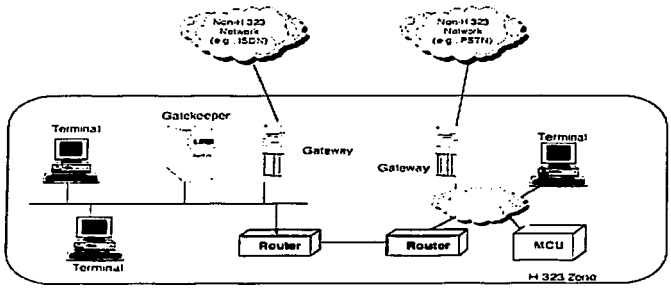


Fig. 3.3.3.2.a Zona Gatekeeper

3.3.3.3 FUNCIONES OPCIONALES DEL GATEKEEPER

Señalización de control-llamada (call-control)

El Gatekeeper puede rutear mensajes de control-llamada entre las terminales de H.323. En una conferencia punto a punto, el gatekeeper podría procesar H.225 mensajes de control-llamada. Alternativamente el gatekeeper podría permitirle a las terminales enviar H.225 mensajes de control-llamada directamente a cada una de las otras terminales.

Autorización de la llamada

Cuando una terminal envía mensajes de control-llamada a el gatekeeper, el gatekeeper podría aceptar o rechazar la llamada, de acuerdo a la especificación del H.225. La razón por la cual se podría rechazar podría ser basada en los accesos o basada en restricciones del tiempo, esto se puede hacer para un terminal o un gateway.

Administración de la llamada

El gatekeeper podría mantener información acerca de todas las llamadas H.323 activas, por lo tanto éste puede controlar esta zona y proveer el mantenimiento de la información para el funcionamiento de la administración del ancho de banda o para re-rutear las llamadas a diferentes terminales para llevar a cabo el balanceo de cargas.

3.3.4 H.323 GATEWAY

Un gateway H.323 (GW) es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es conectar redes diferentes y reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. En otras palabras, un H.323 Gateway nos servirá de pasarela entre el entorno de video sobre IP H.323 y el entorno vídeo sobre RDSI H.320.

3.3.4.1 CARACTERISTICAS DEL GATEWAY

Un gateway (Figura 3.3.4.1.a) provee la translación de protocolos para cuando se inicia la llamada hasta que se libera, la conversión de los formatos de medios entre diferentes redes y la transferencia de información entre redes H.323 y otras que no son redes H.323

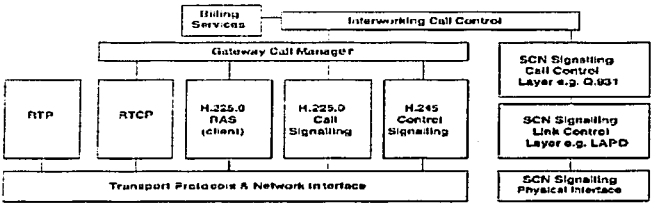


Fig. 3.3.4.1.a H.323 Gateway

Sobre el lado de H.323, un gateway corre H.245 control de la señalización para el intercambio de capacidades, H.225 señalización de la llamada para la inicialización y liberación de la llamada y H.225 registro, admisión y estado (RAS), para registrarse con el Gatekeeper.

Los terminales H.323 se comunican con el gateway usando el H.245 el protocolo de control-señalización y el H.225 protocolo de llamada-señalización. El gateway traslada estos protocolos en una forma transparente para las respectivas partes tanto como para la red H.323 como para la que no es H.323. Este gateway también tiene las características de ambas terminales, de la terminal de una red H.323 y de la otra terminal que este conectada y que pertenezca a una red diferente.

Un gateway es un componente lógico de H.323 y puede ser implementado como parte de un gatekeeper o un MCU.

3.3.4.2 CARACTERÍSTICAS DEL GATEKEEPER Y GATEWAY

El H.225 RAS es usado entre los terminales H.323 (terminales y gateways) y gatekeepers para lo siguiente:

- Descubrimiento del Gatekeeper (GRQ).
- Registro de terminal.
- Localización de terminal.
- Control de admisión.
- Sañales de acceso.

Los mensajes del RAS son llevados sobre un canal RAS que no es confiable. Por lo tanto, el intercambio de los mensajes RAS podrían ser asociados con interrupciones.

Descubrimiento del Gatekeeper

El proceso del descubrimiento del Gatekeeper es usado por los terminales H.323 para determinar el gatekeeper con el cual se van a registrar. El descubrimiento del gatekeeper puede hacerse estáticamente o dinámicamente. En el descubrimiento estático, la terminal conoce la dirección de transporte del Gatekeeper. En el método dinámico del descubrimiento del gatekeeper, las terminales multicast envian un mensaje GRQ, por medio de estas direcciones multicast se realiza el descubrimiento de los Gatekeepers.

Registro de terminales

El registro es un proceso usado por las terminales para unirse a una zona e informar al gatekeeper del transporte de la zona y direcciones de los alias. Todos los terminales se registran con un gatekeeper como parte de su configuración.

Localización de terminales
La localización de terminales es un proceso por el cual el transporte de la dirección de una terminal es determinado y dado ya sea por la dirección del alias.

Otro control
El canal RAS es usado para otro tipo de mecanismo de control, como por ejemplo control de admisión, para restringir la entrada de una terminal dentro de la zona, control de ancho de banda y el control de la liberación de la llamada, donde una terminal es desasociada de un gatekeeper y de la zona.

Con esto terminamos el tercer Capítulo y en cuanto al futuro del estándar H.323 veremos que es el protocolo de referencia dentro del mundo de la emisión de audio y video con anchos de banda reducidos.

Ante el desarrollo de las redes de datos, se ha planteado la posibilidad de utilizarlas para el envió de información multimedia como imágenes, voz e incluso música. Estas redes, basadas en el protocolo IP, han conseguido introducirse tanto en el mundo de los negocios como en el entorno residencial.

El desarrollo de las redes de la nueva generación no oculta el hecho de que se encuentren aun en sus albores, comenzando ahora el siguiente paso en su evolución y haciendo que se conviertan en vías de comunicación unificadas al servicio de millones de usuarios. Así surgen nuevas oportunidades de negocio para operadores y proveedores de red.

El estándar H.323 será una incorporación muy importante a la serie de Recomendaciones H.3x, adoptada ampliamente por la industria como normas para las comunicaciones de multimedios por Internet.

CAPÍTULO IV
IMPLEMENTACIÓN DE H.323

4.1 APLICACIÓN DE H.323

Como se ha mencionado en el capítulo anterior, el estándar H.323 forma parte del grupo de estándares de las comunicaciones multimedia; la videoconferencia se encuentra enmarcada en los servicios de comunicaciones multimedia, ya que es un servicio digital para el intercambio de información audiovisual entre dos o más grupos de personas, generalmente ubicadas geográficamente en sitios distantes.

Por otro lado, resulta innegable que los últimos años han impuesto la implantación de IP como protocolo universal de red, incluso para servicios en tiempo real, para los que no estaban en principio diseñado. En este sentido resulta de especial interés la aparición del estándar H.323 el cual ofrece un interesante marco de convergencia de los servicios de video, audio y datos sobre IP.

De esta manera, frente a las primeras soluciones propietarias para videoconferencia IP punto a punto o punto a multipunto, H.323 propone una solución global que abarca un amplio conjunto de estándares: H.261 o H.263 para la codificación de video, G.711, G.729 y G.723 para la codificación de audio, T.120 para el canal de datos, RTP y RTCP para la gestión de flujos en tiempo real y H.245 y H.225 para la señalización de control de llamada.

El relativo éxito de H.323 se ha visto reflejado en la aparición de la multitud de productos comerciales que se basan en él.

El estándar H.323 puede ser implementado en una variedad de aplicaciones, este trabajo esta enfocado a la videoconferencia, ya que es un claro ejemplo donde se puede ver al estándar H.323 aplicado y a su vez la videoconferencia como es bien sabido se puede implementar en varios sistemas como por ejemplo: Educación a Distancia, Teleasistencia, Comercio Electrónico, etc. Hay una infinidad de usos que se le puede dar a la videoconferencia pero nosotros nos enfocamos a la videoconferencia interactiva dentro del área de la educación a distancia.

4.1.1 EDUCACIÓN A DISTANCIA

La educación a distancia nació, en parte, para atender a una población que no podía ingresar al sistema regular. Era una manera de dar oportunidades de educación a nivel básico y a nivel universitario a personas que por razones de trabajo u otro tipo de problemas no se ajustaban a los requerimientos de la educación formal más cerrada en tiempos y espacios.

La educación a distancia es proveer un ambiente de aprendizaje a un alumno remoto. Cuenta con una estructura curricular, material de aprendizaje estructurado, estrategias y tácticas instruccionales, estrategias y tácticas de aprendizaje, diversas formas de apoyo fuentes externas y herramientas.

Es una modalidad donde la enseñanza y el aprendizaje ocurren en tiempo real y lugares interactivamente mediados por algún tipo de tecnología. Es una modalidad distinta tanto en teoria como en la practica a las formas

convencionales de impartir educación. Es aquella la cual promueve el aprendizaje a través de diferentes medios, es una estrategia educativa basada en la aplicación de la tecnología al aprendizaje, sin limitación de lugar, tiempo, ocupación o edad de los educandos. Son aquellas formas de estudio que no son guiadas y/o controladas directamente por la presencia del profesor en el aula, sino a través de un método de comunicación social que permite la interacción profesor-alumno. Así mismo es la transmisión de conocimientos a través de distintos medios, tanto de comunicación como informáticos, en sus diversas combinaciones para ofrecer modelos educativos mas flexibles en tiempo y espacio. El sello distintivo de la educación a distancia es la separación del profesor y el alumno , ya sea en el espacio y/o el tiempo.

La educación a distancia, también esta presente dentro de la UNAM y la CUAED (Coordinación de Universidad Abierta y Educación a Distancia) es la entidad universitaria encargada de fortalecer el desarrollo de la Educación Abierta, Continua y a Distancia. Su objetivo fundamental consiste en extender la educación dentro y fuera de la UNAM*.

Las modalidades educativas que desarrolla la CUAED son flexibles, dinámicas y basadas en la calidad académica y responden a las circunstancias personales de los estudiantes y a sus necesidades particulares de aprendizaje. La CUAED atiende a alumnos del sistema escolarizado, del Sistema Universidad Abierta, del Programa Universidad en Línea (PUE), a los profesores de la UNAM integrados a la enseñanza a distancia y al sector público y privado interesado en programas académicos de actualización y capacitación.

La CUAED está conformada por una Coordinación General y tres direcciones de área: Dirección de Sistema Universidad Abierta, Dirección de Educación Continua y Dirección de Educación a Distancia. Cada una de ellas cuenta con programas específicos que interactúan entre sí en la combinación de

* http:/ pompeya.cuaed.unam.mx

metodologías educativas y recursos tecnológicos para ofrecer diversas oportunidades de educación universitaria.

Las actividades fundamentales de la CUAED son la divulgación de las prácticas de Educación del Sistema Universidad Abierta, Continua y a Distancia más adecuadas, así como el impulso a los mejores usos educativos de la tecnología que resultan de su actividad de prospección y producción de materiales.

Su tarea también radica en difundir los métodos de evaluación, acreditación y certificación de conocimientos; colaborar con las entidades universitarias para su óptima integración en Educación Abierta, Continua y a Distancia y, responder a las necesidades de educación y capacitación de instituciones educativas, sociales, gubernamentales y empresas privadas a fin de llevar a la Universidad a las diferentes organizaciones que la requieran, sean éstas nacionales o internacionales.

En suma, la CUAED realiza actividades de docencia, investigación, divulgación, capacitación, intercambio académico y cooperación internacional, y sus programas estratégicos son:

- Uso de medios y tecnologías para la educación Abierta y a Distancia
- Fortalecimiento y expansión de la Educación Abierta y a Distancia
- Universidad en línea
- Educación Continua a Distancia
- Recursos humanos para la Educación a Distancia
- Calidad de la Educación

Los avances tecnológicos incorporados al proceso educativo, apuntalan hacia una formación profesional diferente a la tradicional, más integral, con un abonado camino hacia la excelencia académica. La educación a distancia es una esperanza para reestablecer la democracia educativa en el mundo ya que la potencialidad que tienen las nuevas tecnologías permitirá poner la educación al alcance de toda la población y, sobre todo, de las minorías. Este es un compromiso para quienes diseñan y desarrollan proyectos educativos.

La educación a distancia permitirá a la sociedad contemporánea generar condiciones de vida más equitativas. Al facilitar el acceso a la educación para la mayoría de los ciudadanos, constituye una esperanza genuina de igualdad social.

La educación a distancia es una estrategia que permitirá, paradójicamente, acortar distancias, eliminar viejas tradiciones falsamente homogenizadoras de los sistemas educativos al hacer realidad la igualdad de oportunidades. La igualdad de posibilidades para acceder a la educación es uno de los principales logros de este sistema, donde todos son instruidos.

4.1.2 VIDEOCONFERENCIA INTERACTIVA

La inclusión de la videoconferencia, en los servicios de educación, es imprescindible para superar el modelo ya clásico de clase asíncrona. En dicho modelo la interacción entre alumno y profesor no se efectúa en tiempo real sino a través de lo que se ha dado en llamar, de una manera algo pomposa, tutoría virtual, la cual en muchos casos, no deja de ser sino una aplicación particular del correo electrónico. La videoconferencia define un paradigma educativo en donde se integran los servicios típicos del trabajo colaborativo con los mecanismos de comunicación audiovisual duplex en tiempo real.

La incorporación de la videoconferencia en aplicaciones de educación no es un aspecto trivial ya que añade al proceso educativo un componente tan importante como es el "sentido de presencia".

Efectivamente la existencia del elemento presencial resulta clave para el alumno tanto como una motivación como a la hora de resolver dudas, recibir propuestas de problemas o ser evaluado. La comunicación audiovisual directa permite, además, superar la ineficiencia de los procesos de comunicación

textuales asíncronos ya comentados (correo electrónico) evitando la desconfianza que estos todavía suscitan entre el alumnado, normalmente suspicaces ante la obligación de establecer sus dudas por escrito.

La Videoconferencia Interactiva es una herramienta eficaz que puede usarse en el ámbito de la Educación a Distancia. Este sistema puede integrarse en los programas de Educación a Distancia con una adaptación mínima al plan de estudios de los cursos y puede diseñarse para favorecer la comunicación por medio del video y audio bidireccional entre múltiples localidades.

La mayoría de los sistemas de Videoconferencia Interactiva utilizan el video digital comprimido para la transmisión de imágenes en movimiento por medio de las redes de transmisión de datos.

El proceso de condensación video imágenes reduce la cantidad de datos transmitidos, de esta manera se transmiten sólo los cambios producidos en los cuadros de imágenes. Al reducir el ancho de banda exigido para la transmisión de imágenes, la condensación de video imágenes redujo también los costos de transmisión.

Las Videoconferencias Interactivas, a menudo se transmiten por medio de líneas del teléfono especializadas de tipo T1. Estas líneas trabajan a altas velocidades y son muy eficaces para esta tecnología, pero se alquilan por medio de circuitos especiales y tienen un costo de mantenimiento mensual relativamente alto, los costos de comunicación se calculan en función de la distancia y en el tiempo de comunicación. Pero con el estándar H.323, podemos reducir costos, por que no es necesario alquilar ninguna línea ya que por medio de este estándar podemos utilizar nuestra propia infraestructura de red para transmitir la videoconferencia.

La Videoconferencia Interactiva normalmente es usada para conectar dos sitios remotos empleando sofisticada tecnología de computadoras. El centro de la Videoconferencia Interactiva es el codec (codificador/decodificador). Éste es el

dispositivo electrónico que transmite y recibe las señales de audio y video que los miembros de la clase escucharan y verán en sus monitores.

Además de monitores, otro tipo de equipamiento es necesario para hacer una Videoconferencia Interactiva exitosa. Pueden incorporarse varias de las tecnologías instruccionales de uso más corriente como ser: los videos, micrófonos, cámaras, y computadoras.

La videoconferencia interactiva (fig 4.1.1.a) también se puede hacer multipunto, es decir, conectar simultáneamente más de dos sitios a través del uso de una unidad de mando de multi-punto, o MCU.

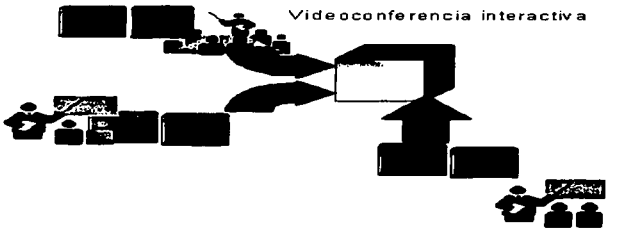


Fig. 4.1.1.a Videoconferencia Interactiva

La Videoconferencia Interactiva permite 'en tiempo real' establecer contacto visual entre los estudiantes y el instructor o entre estudiantes localizados en sitios remotos. También soporta el uso de diversos medios de comunicación: Las pizarras, documentos electrónicos, escritos a mano y videos pueden incorporarse a la transmisión. Permite la conexión con expertos de otras situaciones geográficas, pudiendo proporcionar acceso para los estudiantes de necesidades especiales y acceso adicional a los estudiantes de sitios remotos.

Hoy en día con estas nuevas tecnologías y estos estándares ya no existen limitaciones en este tipo de educación, ya que los costos iniciales del equipo no son elevados y ya no es necesario del arrendamiento de las líneas (cableado telefónico) para transmitir y realizar las videoconferencias.

Antes las compañías que producían los equipos desarrollaban sus propios métodos de condensación de imágenes, lo que generaba (a veces) un problema de incompatibilidad de equipos. Pero como el estándar H.323 esta abierto a la interpretación de diferentes fabricantes, lo cual deja libertad a los fabricantes para implementar capacidades que cumplan con los requerimientos de aplicaciones especiales, y por lo tanto las aplicaciones y productos interoperan, permitiendo la comunicación entre los usuarios sin necesidad de que éstos se preocupen por compatibilidad de equipos.

Según el equipamiento empleado, se pueden establecer los siguientes tipos de Videoconferencias Interactivas:

Videoconferencias de escritorio: Este sistema utiliza una computadora personal y un software especializado. Estos sistemas son menos caros, pero ofrecen una resolución limitada. Ellos son más efectivos para el uso individual o de grupos pequeños (hasta 4 alumnos). Hoy día, sin embargo, el mercado latinoamericano está dominado por las más básicas aplicaciones de videoconferencia de salas privadas y públicas, y no de escritorio.

Videoconferencias para pequeños auditorios: Este sistema se diseña principalmente para grupos pequeños (4-12 participantes) todos situados alrededor de una mesa de conferencias.

Videoconferencias de sala: Este tipo de sistema normalmente usa una alta calidad de componentes y equipos y una interfaz que permite que todos los participantes sean vistos en los monitores.

Las videoconferencias interactivas pueden ser una herramienta instruccional muy eficaz para el educador a distancia; como con otras tecnologías, su utilidad

está directamente relacionada a que el instructor entienda sus beneficios, limitaciones y las distintas estrategias de utilización. La Realidad Virtual se impone como una nueva forma de interacción entre el hombre y la computadora. Cuando se construyen aplicaciones para múltiples usuarios se puede crear un entorno para trabajo colaborativo.

Este tipo de aplicación parece especialmente aplicable a procesos educativos. Hoy en día se están probando procesos simulados de Educación a Distancia por Realidad Virtual y, en un futuro no muy lejano, con el avance de la tecnología, se podrá soportar fácilmente este tipo de Educación a Distancia en todo el país.

La Educación a Distancia no puede ni debe permanecer al margen de lo que hoy en día representa la revolución tecnológica con su herramienta más valiosa: INTERNET. Es evidente el poder de la videoconferencia como una herramienta de negocios y educativa que se demuestra en los centros de enseñanza que utilizan video para enlazar estudiantes y profesores alrededor del mundo.

4.1.3 H.323 Y CALIDAD DE SERVICIO

Ya se ha visto que la videoconferencia es una aplicación donde el estándar H.323 juega un papel muy importante, pero el objetivo principal en este trabajo de tesis no es nada mas el implementar el estándar H.323 realizando videoconferencia, si no que, lo principal es mostrar una de las bondades del estándar H.323, y en la cual nos vamos a centrar, y esta es que principalmente este estándar nos permite trabajar en conjunto con otros protocolos.

Como se mencionó en el Capítulo III, el estándar H.323 no proporciona una garantía de calidad de servicio por si solo, por lo cual en este capítulo aplicaremos en conjunto H.323 y Calidad de Servicio (QoS).

Actualmente en la base de desarrollo de las redes se encuentran los mecanismos de garantía de servicio, que a lo largo de la ultima década se han introducido en las redes basadas en IP. Mecanismos como la priorización del trafico o la reserva de recursos en routers y en otros dispositivos de red, permite reducir los retardos y jitters en las redes IP, hasta valores no apreciables por el ser humano, facilitando su uso para el trafico de voz.

Como se menciono en el Capitulo I, Calidad de servicio, es la capacidad de la red para proporcionar un mejor servicio al trafico seleccionado, así mismo, es una serie de técnicas para administrar: ancho de banda, retardo y perdida de paquetes

Algunas características de QoS son:

- Políticas y funciones de administración para el control y administración de tráfico de principio a fin a través de una red.
- Colas, calendarización y características del tráfico.
- Selección del tráfico
- Técnicas de señalización para coordinar QoS de principio a fin entre los elementos de la red.
- Administración y Control de congestión

El retardo es uno de los factores que se habrán de cuidar para proporcionar los servicios de voz sobre una red multiservicio. Algunas de las causas que provocan el retardo en los equipos de borde y entre el intercambio de trafico entre switches y rutadores son las siguientes:

- Congestión.
- Ausencia de políticas de trafico
- Grandes colas de paquetes en enlaces pequeños
- Tamaño de paquetes variables.

Existen dos tipos de retardo que afectan al tráfico de voz: retardo absoluto y retardo variable (o jitter). El retardo absoluto es el tiempo que toma a los paquetes de voz el viajar desde el origen hasta llegar a su destino final. En tanto que el retardo variable es un retardo que se presenta desde el origen hasta el destino final y que afecta a cada uno de los paquetes, este es diferente para cada uno de ellos, y se presenta en cada uno de los equipos intermedios (switches y routers) por donde va atravesando el paquete hasta llegar a su destino final.

Otro factor que contribuye al retardo es la latencia que se refiere al tiempo que pasa cuando un dispositivo solicita acceso a la red y esta solicitud es procesada y enviada. La latencia a través de toda la red de un punto a punto esta asociada a la red. La serializacion del retardo es un aspecto de latencia que corresponde al tiempo que se toma para enviar un paquete hacia una interfaz (esto es, el tiempo que toma el mover el paquete hacia una cola de salida) este tiempo depende del volumen de datos y la velocidad de la línea para procesar la cantidad de trafico que tiene que entregar.

Antes de que el tráfico sea manejado de acuerdo a sus requerimientos deberá ser etiquetado o identificado de alguna manera, por lo que existen varias formas de clasificar el trafico (Capitulo I, 1.6.1 Clasificación del tráfico), incluyendo esquemas de capa 3 (Precedencia en IP o Servicios Diferenciados) y esquemas de capa 2 (protocolo 802.1P).

CAR (Commited Access Rate): Una de las técnicas utilizadas por los enrutadores para la clasificación de paquetes es la tarifa comprometida de acceso (CAR) es una vieja técnica que implica un limite en la tasa de transferencia o el mantener el orden del tráfico de acuerdo a ciertos criterios. Esta técnica soporta la mayoría de los mecanismos de comparación y permiten la clasificación de capa 3.

En general, CAR es mayormente utilizado para paquetes de datos que para paquetes de voz. Por ejemplo, todo el tráfico de entrada de una interfaz ethernet o al menos 1 Mbs puede ser colocado dentro de una clase 3 dentro del esquema de

precedencia de IP, y cualquier tráfico que exceda este Megabite puede clasificarse como 1 o ser tirado por el router. Otros nodos dentro de la red pueden entonces tratar de exceder o no conformarse con el tráfico marcado con una precedencia diferente. Todo el tráfico de voz podría conformar una tasa especifica si esta ha sido proporcionada correctamente

PBR (Policy-Based Routing): Esta técnica también es utilizada para la clasificación del tráfico y permite al tráfico ser enrutado basandose en el puerto origen o alguna lista de acceso, lo cual también puede ser usado para clasificar o marcar los paquetes.

4.1.3.1 TÉCNICAS DE APROVECHAMIENTO DEL ENLACE

CRTP (Compresión RTP)

Además de los estándares de compresión de voz existen otros mecanismos que ayudan a incrementar el aprovechamiento del enlace comprimiendo los encabezados del paquete de Voz. CRTP es la compresión del Protocolo de Tiempo Real y comprime el encabezado correspondiente a los 40 bytes que nos proporciona la suma de los encabezados de IP + UDP + RTP hasta 4 u 8 bytes. (Figura 4.1.3.1.a). El protocolo RTP es un protocolo host-a-host utilizado para transportar tráfico de aplicaciones multimedia, incluyendo VoIP. La compresión del encabezado de RTP incrementa la eficiencia de la transmisión de paquetes multimedia sobre enlaces seriales de baja velocidad.

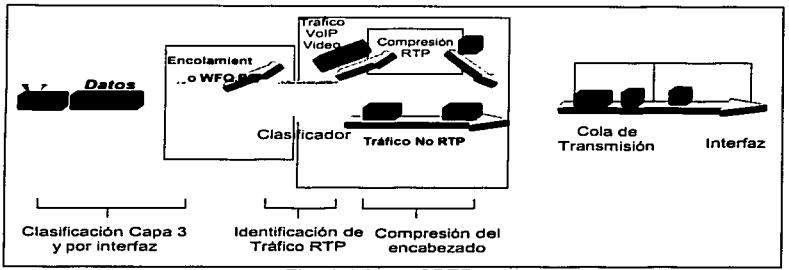


Fig. 4.1.3.1.a CRTP

Típicamente para aplicaciones de audio el encabezado de RTP tiene una longitud de 40 bytes y la parte de datos (voz o video) del paquete va de 20 a 150 bytes (son muy pequeños). Dada la combinación de los encabezados RTP/UDP/IP resulta, en muchas ocasiones, que el encabezado sea de mayor tamaño que la parte de datos que deseamos transportar, de ahí el utilizar la compresión del encabezado que de 40 bytes totales resulten solamente 2 o 5 bytes de encabezado(Fig. 4.1.3.1.b). Para enlaces de baja velocidad, debajo de los 384 bytes, resulta una herramienta que reduce la saturación del enlace por parte de tráfico multimedia.

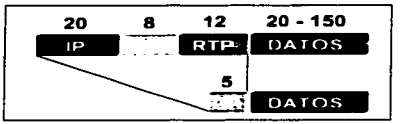
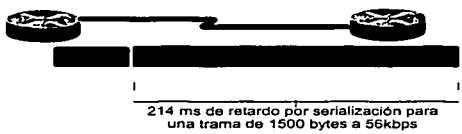


Figura 4.1.3.1.c CRTP

LFI (Fragmentación e Intercalamiento de Paquetes)

Para enlaces menores a 768 kbps se recomienda utilizar técnicas de fragmentación e intercalamiento de paquetes (Figura 4.1.3.1.d y Figura 4.1.3.1.e). Estas técnicas nos ayudan a prevenir y evitar tanto el delay como el jitter existentes en la transmisión de información ya que muchas veces existen paquetes demasiado grandes que harán que paquetes más pequeños estén en espera encolados para ser transmitidos hasta que el paquete de mayor tamaño sea despachado. Al mismo tiempo podemos intercalar paquetes de voz con paquetes de datos y así no esperar a que nuestro trafico de voz quede encolado en momentos de congestión.



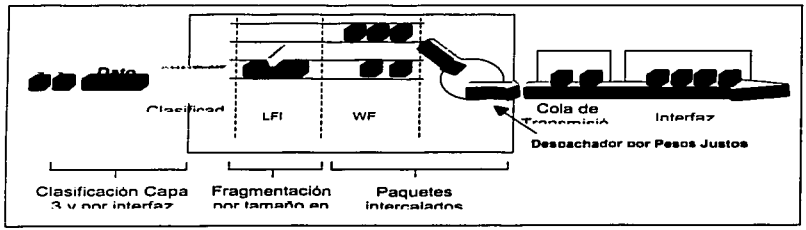


Figura 4.1.3.1.d y e LFI

4.1.3.2 HERRAMIENTAS DE ADMINISTRACIÓN DE CONGESTIÓN

Una vez que en un dispositivo de red se presenta un desbordamiento en el arribo de tráfico debe utilizar un algoritmo para ordenar el tráfico y de alguna forma prioritizarlo hacia un enlace de salida.

Existen diversas técnicas para realizar esta actividad y a continuación se mencionan algunas:

Encolamiento First-in, First-out (FIFO). No existen concepto de priorizar los paquetes, los paquetes salen en el orden que llegan.

- También es conocida como first-come, first served (FCFS) queuing.
- No conceptos de prioridades, no clasificación.
- Existe solamente una cola.
- Todos los paquetes son tratados igual.
- Cuando ninguna estrategia de encolamiento esta configurada FIFO es default (excepto interfaces seriales E1).

Encolamiento de peso justo (Weighted Fair Queuing (WFQ)). Divide el ancho de banda basándose en pesos. Asegura el tiempo de respuesta en aplicaciones criticas.

- WFQ da al tráfico de bajo volumen como telnet, prioridad sobre el tráfico de alto volumen como FTP.
- Cada cola corresponde a diferente flujo.

Encolamiento Personalizado (Custom Queuing (CQ). El ancho de banda es asignado para cada tipo de tráfico. Especificando el número de bytes o paquetes por cola.

- Se puede especificar el número de bytes a forwardear de la cola.
- Posibilidad para especificar el número máximo de paquetes en cada cola.
- El sistema mantiene 17 colas de salida para cada interface.
- La cola con número 0 es utilizada para paquetes de alta prioridad como keepalive y paquetes de señalización.

Encolamiento de Prioridad (Priority Queuing (PQ)). Paquetes con alta prioridad son trasmitidos primero que los de baja prioridad.

- 4 tipos de prioridades(alta, media, normal y baja).
- Se pueden definir una serie de filtros basados en las características de los paquetes que causan que el router distribuya el tráfico en estas 4 colas.
- La cola con más alta prioridad es atendida primero hasta que esta vacía.
- Paquetes que no han sido asignados a ninguna prioridad caen dentro de la cola de tipo normal

Encolamineto de peso justo basado en clases (Class-Based Weighted fair queuing (CBWFQ)): Extiende las funcionalidades de WFQ para proveer soporte para clases de trafico de usuarios definidos, CBWFQ define clases de trafico basadas en criterios marcados, protocolos, listas de control de acceso e interfaces de entrada. Una cola es reservada para cada clase y el tráfico perteneciente a una clase es enviado a la cola de dicha clase. Para caracterizar una clase se puede asignar ancho de banda, peso y el limite máximo de paquetes

Encolamiento de baja latencia (Low Latency Queuing (LLQ)). Es ahora el método preferido, este es un híbrido de los métodos de encolamiento anteriores, LLQ combina PQ, CQ, WFQ. LLQ provee encolamiento de prioridad a un CBWFQ, reduciendo jitter en el trafico de voz, habilita el uso de una simple cola de prioridad con CBWFQ permitiendo direccionar el trafico perteneciente a una clase para el CBWFQ. Uno de los beneficios es que tiene una configuración consistente a través de todos los tipos de medio. LLQ da una cola de prioridad y lo demás es dividido en pesos para dar preferencias.

4.2 PRUEBAS

4.2.1 OBJETIVO

El objetivo de estas pruebas es realizar videoconferencia con H.323 y probar la interoperabilidad y compatibilidad que existe entre los equipos y así mismo demostrar una de las bondades de H.323, que es el trabajar en conjunto con otros protocolos y en este caso vamos aplicar una de las técnicas de Calidad de Servicio que es la de Encolamiento de Prioridad y el objetivo de aplicar calidad de servicio es mas que nada darle prioridad a cierta clase de tráfico, y esto es un punto muy importante ya que si queremos que nuestra videoconferencia interactiva tenga prioridad sobre otro tipo de tráfico, a pesar de los factores que intervienen como por ejemplo la congestión en el ancho de banda lo cual puede provocar que exista retardos o variaciones, es recomendable aplicar alguna técnica de Calidad de Servicio.

4.2.2 IMPLEMENTACION DE PRUEBAS

Las pruebas realizadas se dividieron en dos fases: La primera de estas fases es en la cual se realizan pruebas que muestran el desempeño del equipo dentro de la red, interoperabilidad y compatibilidad y en la segunda fase sé checa ingeniería de tráfico y QoS.

Los aspectos a evaluar en estas pruebas son:

- Desempeño dentro de la Red.
- Pruebas de Interoperabilidad.
- Compatibilidad entre equipos.
- Comportamiento a máximas capacidades.
- Calidad de Servicio (QoS).
- Ingeniería de tráfico.

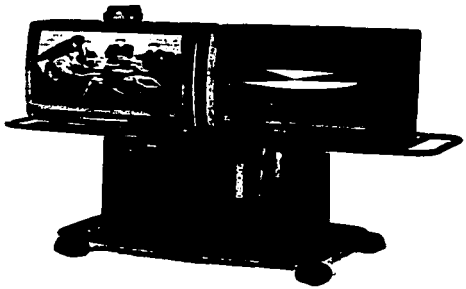
4.2.2.1 EQUIPO UTILIZADO

El chequeo de los equipos se realizó en la primera etapa con conexiones punto a punto y de acuerdo al progreso de las mismas, el nivel de complejidad se incrementó de acuerdo a la respuesta de los equipos.

Las marcas que se analizaron fueron las siguientes:

Equipo: TANDBERG Proveedor: DISITEM.

Este equipo esta ubicado en el aula de videoconferencia de DGSCA (Figura 4.2.2.1.a).



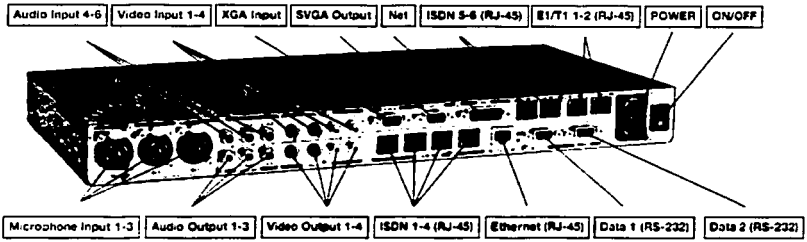
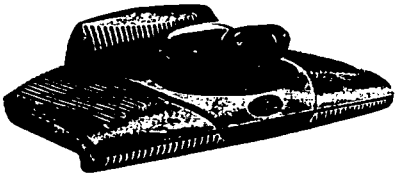


Figura 4.2.2.1.a Equipo TANDBERG

Características principales.

TANDBERG Modelo 6000		
Sobre ISDN, IP y enlaces E1 / T1 Características de la Red Auto marcado de H.320/H.323 Downspeeding TF Profiles de red programables Password Administrador de llamadas inteligente Características H.323 (IP) Precedencia de IP (QoS) Tipo de servicio IP (TOS) Auto gatekeeper discovery Dynamic playout and lipsync buffering Componentes del sistema 1 o 2 monitores, control remoto inalámbrico, W.A.V.E. cámara, microfono, Modulo de Audio Natural TM, cables integrados Estándar de video H. 261, H.263, H.263+, H.263++ (Natural VideoTF) Administrador de video inteligente Entradas de video (5 entradas) 1 x MiniDin, S-video: cámara principal 1 x MiniDin, S-video: auxiliary/document camera 1 x RCA/Phono, composite: document camera/aux 1 x RCA/Phono, composite: VCR 1 x XGA: PC Salidas de video (5 salidas) 1 x MiniDin, S-video: monitor principal 1 x MiniDin, S-video: dual monitor 1 x RCA/Phono, composite: monitor principal o VCR 1 x RCA/Phono, composite: dual monitor o VCR 1 x SVGA: monitor principal, dual monitor o VGA loop	audio bridge para mas de 5 sitios DuoVideo Formato de video NTSC o PAL Resolucion 4CIF (704 x 576 pixels), Digital Clarity TF Interlaced CIF (352 x 576 pixels), Natural Video CIF (352 x 288 pixels) QCIF (176 x 144 pixels) SQCIF (128 x 96 pixels) CIF, 4CIF, H.261 Annex D Estandar de Audio G.711, G.722, G.722.1, G.728 Características de Audio Teléfono add-on via MultiSite TF TANDBERG Natural Audio Modulo Four separate acoustic echo cancellers Audio mixer Automatic gain control Reducción automatica de ruido Audio level meters VCR ducking Entradas de Audio (6 entradas) 3 x microfono, 24V phantom powered, XLR conector 1 x RCA/Phono, nivel de línea: audiomixer 1 x RCA/Phono, nivel de línea: auxiliar 1 x RCA/Phono, nivel de línea: VCR Interfases de Red 6 x ISDN BRI (RJ-45), S-interfase 1 x E1/T1 G.703 (RJ-45) para ISDN PRI o enlaces E1/T1 1 x E1/T1 (RJ-45) para ISDN PRI cascadeado 1 x LAN / Ethernet (RJ-45) 10/100 Mbit Ethernet / Internet / Intranet Conectividad TCP/IP, SNMP, DHCP, ARP, FTP, Telnet, HTTP, servidor web interno Otros estándares ITU soportados H.320, H.323, H.281, BONDING (ISO 13871), H.231, H.243	W.A.V.E. (Wide Angle View) camara 12 x zoom 1/3" CCD +5°/-15° tilt +/-95° pan 76° vista vertical 270° vista horizontal 460 (NTSC) / 450 (PAL) horizontal TV líneas Min. iluminacion 7 Lux (F1.8) Auto o manual enfoque 15 near and far-end camera pre-sets Voice-activated camera positioning Up to 4 camera daisy chain supports VISCA cámara suporte Presentaciones y Colaboración (ISDN, IP y enlaces E1/T1) T.120 soporta Microsoft NetMeeting via RS-232 (9-pin D-sub) Streaming (compatible con Apple QuickTime y RealPlayer v8 etc.) Local System Management 1 x RS-232 usado para el control dela cámara principal 1 x RS-232 para actualizaciones de software, control local y diagnósticos Control remoto y sistema de menús Administración del sistema remotamente Administración Total via web browser, Telnet, FTP y SNMP Menu para seleccionar lenguaje Potencia Auto-sensing power supply 100 - 250V AC, 50 - 60 Hz 65 watts max. para codec y camara principal Monitor 32" NTSC monitor o 29/33" PAL soporte para atro tipo de monitor.

Equipo: POLYCOM, Proveedor: SIO (Soluciones Integrales para Oficina).
Este equipo se encontraba ubicado en CUAED (Figura 4.2.2.1.b).



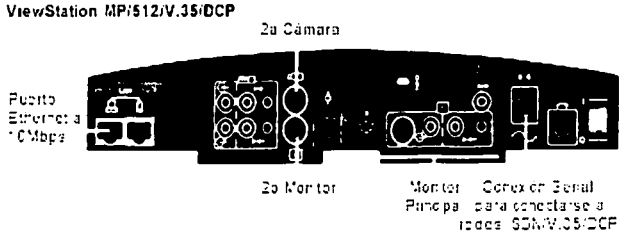


Figura 4.2.2.1.b Equipo Polycom

Caracteristicas principales.

POLYCOM		
Modelo View Station.		
ViewStation DCP 512 Especificaciones Técnicas Estándares soportados ITU-T H.320 (px64),H.323 Video H.261, Annex D H.263+, Annex: L,F,T,I,J,u Audio G.728, G.722, G.711 Polycom Acoustic Plus 716 Comunicaciones H.221 Pantalla Video Resolución H.261, H.263+ Modo: FCIF 352x288 Resolución de graficos H.261 Mode: 4 x FCIF/ Annex-D Graphic Image Capture JPEG via Web browser Velocidad de Transmisión H.320 rango de datos (kbps) 56 - 512 H.323 rango de datos (kbps) 64 - 768 Entradas de Video (NTSC o PAL) Camara Principal S-Video o composite Document Camera S-Video VCR In (para playback) Composite Salidas de Video (NTSC o PAL) Monitor principal S-Video o Composite 2nd Monitor S-Video VCR Out (recording) Composite	Monitor principal sistema Auto-PIP Auto-on, auto-swap, auto-off Main Voice Tracking Camera Image Sensor 1/3 in IT CCD Lens 12 x Zoom; f=5.4 to 64.8mm; F=1.8 to 2.7 mm: Auto Focus White Balance Automatico Presets 10 presets camara local 10 preset positiones far-end camara Tracking Technique Voice tracking or track to presets Full-Duplex Digital Audio Supresión automática de ruido Conector RCA 2 Monitores L&R audio-out RCA phono Microfono Digital Pod Coverage 360° Integrated Speakerphone Administración Remota Extensivos diagnosticos y software actualizaciones via PC, LAN	Ethernet/ Internet/ Intranet Conectividad Suportes TCP/IP, DNS, WINS, SNMP, DHCP, ARP, WWW, ftp, Telnet 10/100 Mbps Ethernet Hub T.120 • IP, WebStation • y NetMeeting • capacidad para videoconferencia via web Aplicationes Suportadas Microsoft PowerPoint y NetMeeting Interfaces de Network ViewStation DCP DCP Port RJ-45 conector Auto-IP detección y configuración 2-cables soportados Puertos programables como PDM (TN-2224 24 puerto y TN-2181 16 puerto) Especificaciones Electricas Auto-sense power supply Operating voltage/power 90-260 VAC, 47-63Hz/ 40 watts Especificaciones fisicas Tamaño de ViewStation 33cm X 20cm X 15cm Peso 2.7kg (6lbs) Languajes Suportados ingles, frances, aleman, español, Italiano, Chino y japones Garantia 1 año en todas las partes

Equipo: VCON, Proveedor: Integri

Equipo ubicado en el área de Redes de DGSCA(Figura 4.2.2.1.c).

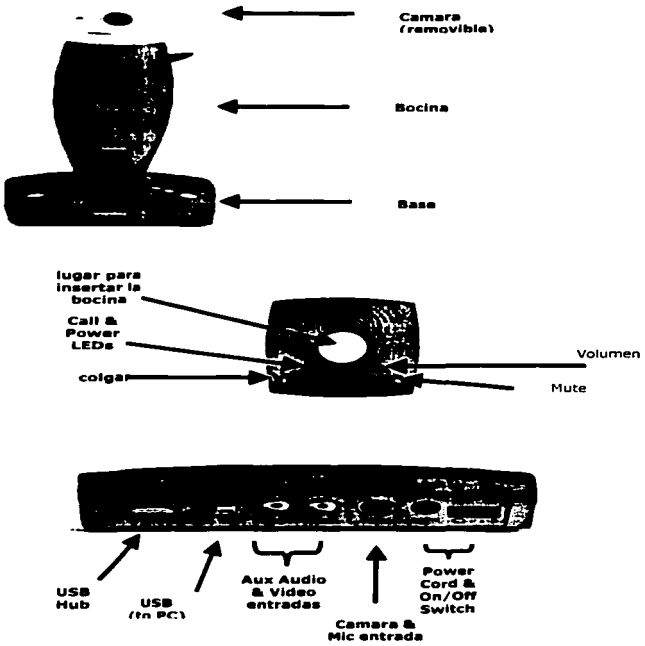


Figura 4.2.2.1.c Equipo VCON

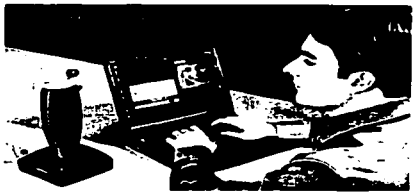


Figura 4.2.2.1.d VCON

Caracteristicas principales.

VCON.	
Vigo	
•"Hot-pluggable" USB conexiones para PC o laptop •IP conferencia a un rango de datos desde 1.5Mbps •bocina y cámara Removible •Envio de llamada, Transferencia y Ad-Hoc Conferencia via MXM •Botones sobre la base para funciones comunes •Suportado para Windows 98, 2000, ME, XP •USB hub para futuros perifericos •vClip – Personal Recording Software •Entradas auxiliares de audio y video •Wide-band, alta-calidad de audio •Suportado para VCON's Interactive Multicast •QoS via VCON PacketAssist™ Arquitectura •Dual CPU Support •Calidad Superior de video via H.263 •Small footprint (6" x 6"), peso 35 ounzas •Padded nylon carrying case	•El ViGO tiene un rango de datos desde 1.5Mbps, permitiendo a los usuarios escoger desde un amplio rango de velocidades de transmisión •Puede participar en seciones de multicast interactiva •ViGO tiene entradas alternativas de video y audio, haciendo que ViGO sea mas versátil y facil para incorporalo dentro de una red empresarial. •ViGO's USB hub significa que los usuarios no tienen que escoger entre ViGO y otro dispositivo USB. •ViGO incluye todo lo que un usuario necesita para participar en una videoconferencia. No hay necesidad de comprar bocinas adicionales u otro equipo.

4.2.2.2 PRUEBAS REALIZADAS. FASE UNO

Se examinó la parte de configuración del equipo, las velocidades a las que se pueden trabajar y los protocolos de audio y video que se usaron.

El esquema para las pruebas punto a punto para los equipos que se probaron, fue el siguiente Figura 4.2.2.2.a.

Figura 4.2.2.2.a Esquema de conexión

Para Polycom se comenzaron las pruebas con el modelo View Station realizando conexiones punto a punto dentro de la misma DGSCA. Desde el departamento de Redes hasta CUAED y el equipo respondió sin problemas, como estaba previsto, ya que solamente se conectaban por medio de un cable UTP y un switch 1100 3COM

Se hicieron pruebas a 64Kbps de ancho de banda y como era lógico solo se recibía y enviaba audio ya que el reducido BW era muy poco para que el video se transmitiera. Se aumentó el ancho de banda a 6 canales (384kbps) y ya se recibía imagen a muy buena calidad.

En el caso de Tandberg se probó el modelo 6000 que cuenta con un gran número de opciones para la realización de videoconferencia H.323

Este equipo fue uno de los que funcionaron correctamente en todas las pruebas que se le realizaron, ya que en la prueba de comportamiento, compatibilidad y desempeño, trabajó óptimamente, solo se observó que en las especificaciones se menciona que puede tener hasta 4 equipos conectados, pero no lo puede hacer a una velocidad de 768 kbps, solo permite 2 a esta velocidad y los demás los mantiene a un ancho de banda menor.

Para el caso de VCON se realizaron pruebas con el equipo de escritorio VIGO las pruebas fueron de la misma forma que en los casos anteriores. Estos equipos presentaron un excelente desempeño en la prueba de conectividad punto a punto a diferentes velocidades (arriba de 64 Kbps).

Para la videoconferencia se instaló un software de VCON llamado Meeting Point (Figura 4.2.2.2.b), este software se instalo en el departamento de Redes de DGSCA ya que en los demás puntos donde se realizaron las pruebas no se nos permitió entrar a la configuración de los equipos ya que toda la administración y configuración de dichos equipos fue realizada por los encargados de esas áreas, y solo al final de las pruebas ellos nos enviaron el reporte, por lo tanto la mayoría de los resultados los obtuvimos mediante el software instalado en el área de Redes.

Figura 4.2.2.2.b Meeting Point

En este software podemos observar las propiedades y parámetros configurados de la videoconferencia.

El programa se configura con los datos del usuario e IP de la máquina, para que este equipo sea reconocido dentro de la red de videoconferencia y en caso de que se este utilizando un software de administración como lo es el MXM (Media Xchange Manager), el equipo va ser fácilmente agregado a la base de datos del software, en seguida se muestran algunas de las imágenes del programa (figura 4.2.2.2.c,d y e):

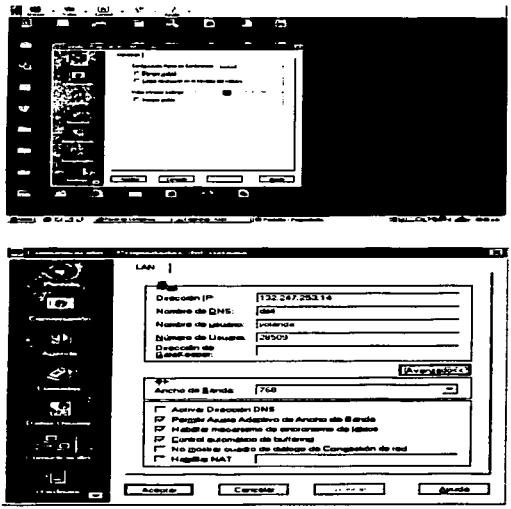


Figura 4.2.2.2.c y d Parametros de Meeting Point

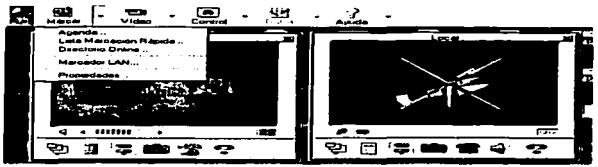


Figura 4.2.2.2.e Propiedades de Meeting Point

Estas son imágenes de las pruebas que se realizaron. Como ya se mencionó se probaron varias velocidades 64, 128, 256, 384, 512 y 768 kbps.

El Meeting Point nos muestra algunos datos de cómo sé esta llevando a cabo la videoconferencia cómo son los formatos, el ancho de banda y se observa que al variar la velocidad la calidad de la imagen es cada vez mejor (figuras 4.2.2.2.f y g).

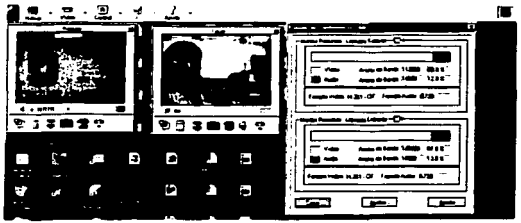


Figura 4.2.2.2.f imagen es a 128 kbps

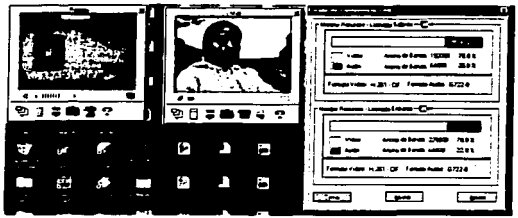


Figura 4.2.2.2.g Imagen a 256 kbps

En el recuadro de la derecha se muestra el comportamiento de la red, es decir cuanto ancho de banda es consumido por audio y video.Y también se muestra que tanto en llamada entrante como saliente están usando los mismos formatos, es decir que tanto el equipo que envía como el que recibe, hacen una negociación y aunque sean equipos de diferente fabricante existe compatibilidad y establecen el formato al cual van a transmitir, este formato es igual para ambos lados para evitar problemas de comunicación (ver figura 4.2.2.2.h, i y j).

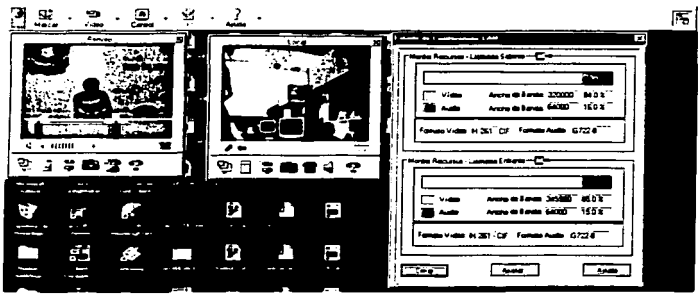


Figura 4.2.2.2.h Velocidad a 384kbps.

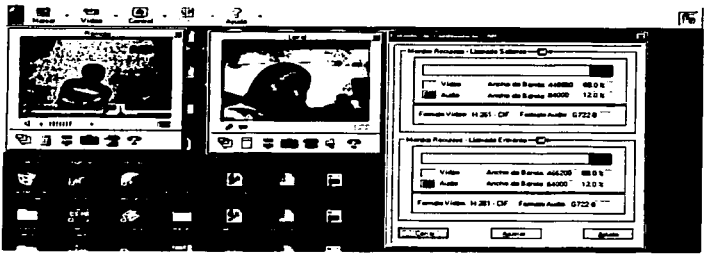


Figura 4.2.2.2.i Velocidad a 512kbps.

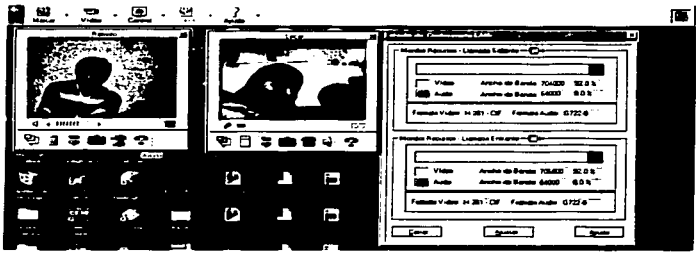


Figura 4.2.2.2.j Velocidad a 768kbps

Después de haber realizado estas pruebas se probó el desempeño de los equipos dentro de una videoconferencia H.323 controlada por un MCU de VCON en software, el cual se instaló en una máquina SUN Enterpise 250.

Se probó este MCU debido a que con un MCU de hardware se presentó el problema de que no aguantaba varias conexiones a 768 kbps.

El MCU de VCON ofrece una solución a esto ya que es capaz de aguantar alrededor de 20 equipos conectados a 768 kbps.

Se necesita de una máquina robusta que soporte esta aplicación. La administración es sencilla ya que se controla por medio de un web browser. La cantidad de equipos que puedas tener conectados depende de la memoria de la máquina en que se tenga instalado el MCU.

El MCU se instaló en el aula de videoconferencia y se estableció una sesión de videoconferencia a la cual se conectaron 3 sitios: el equipo de VIGO, el POLYCOM y el TAMBERG, el esquema fue el siguiente (figura 4.2.2.2.k):

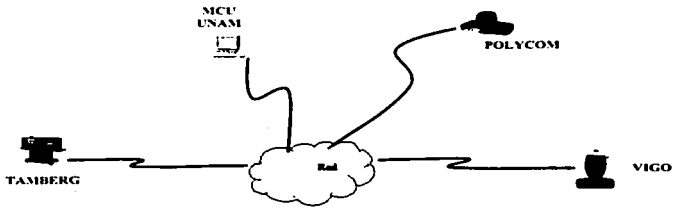


Figura 4.2.2.2.k Diagrama de Conexión

Las pruebas que se realizaron fueron de la misma manera que las anteriores, demostrar la compatibilidad e interoperabilidad entre equipos y así mismo observar como se comportaba la videoconferencia con las variaciones de velocidad. A continuación se muestran algunas imágenes de la videoconferencia multipunto (figura 4.2.2.2.k,l).

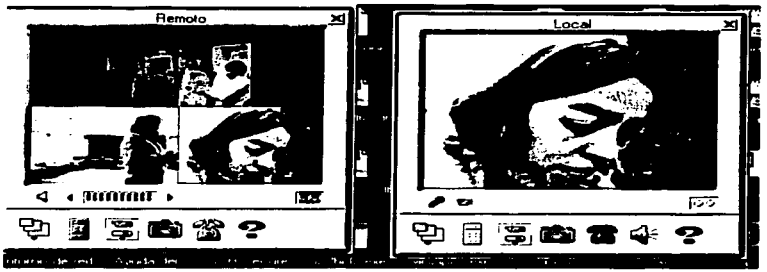


Figura 4.2.2.2.k Velocidad de 256kbps

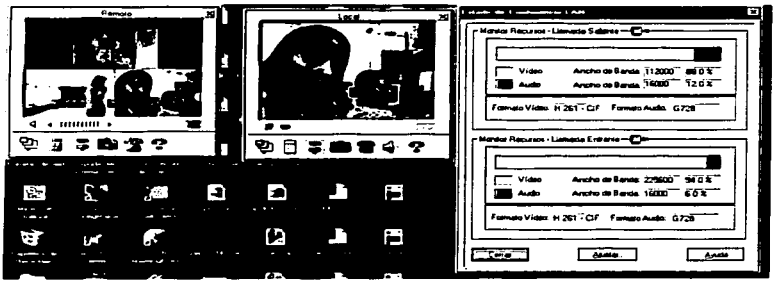


Figura 4.2.2.2.l Velocidad de 768kbps

Los equipos respondieron favorablemente y solo hubo algunos problemas para iniciarse dentro de la sesión de videoconferencia y se presentó cuadriculamiento de voz y video e incluso desconexiones periódicas, pero una vez dentro de sesión trabajaron sin problemas, en las pruebas de comportamiento a máximas capacidades trabajó excelentemente y permitió gran diversidad de accesorios extra para el auxilio y adaptación de la videoconferencia.

4.2.2.3 PRUEBAS REALIZADAS. FASE DOS

La segunda fase de las pruebas consistió en aplicar una técnica de Calidad de Servicio, como se mencionó en él capítulo 4.1.2, que algo que caracteriza al estándar H.323 es que nos permite trabajar en conjunto con otros protocolos en este caso lo que se realizó fueron pruebas aplicando una herramienta de administración de tráfico que es la de Encolamiento de Prioridad (Priority queuing), la configuración de esta herramienta se realizo en un router ya que este es el equipo capaz de direccionar el flujo de paquetes y el cual nos proporciona datos acerca del comportamiento de la red.

Las pruebas fueron las siguientes:

Se analizaron los paquetes generados por comunicaciones H.323 de Videoconferencia

Para generar trafico dentro de la red se generan grupos de tráfico:

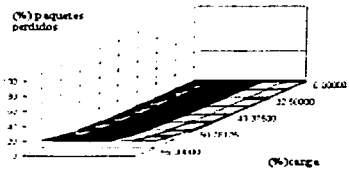
–Dos de videoconferencias H.323

–Uno de FTP y uno de http, 20 flujos FTP o HTTP por grupo

Metodología

•Primero:

–Sin prioridad en los puertos, se envía el tráfico por ambas conexiones

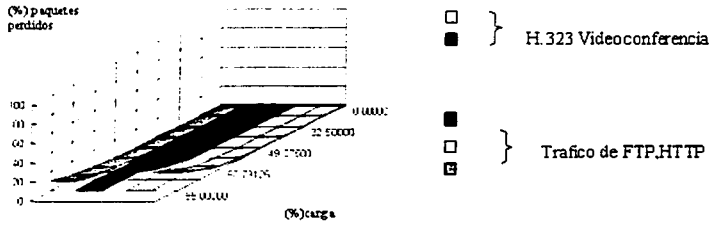


H.323 Videoconferencia

Trafico de FTP.HTTP

Se observa que sin prioridad cualquier tipo de trafico es indiferente y se transmite igual sin darle prioridad a ninguno de ellos.

•Segundo:
Se da prioridad para los paquetes de Videoconferencia H.323 (se le asigna una prioridad alta)
Queda sin prioridad él trafico restante (el cual toma una prioridad normal)
Después de esto se comienza a enviar el tráfico

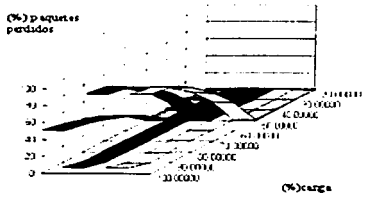


En esta prueba se observa que los paquetes que son de Videoconferencia H.323 ahora tienen prioridad con respecto al demás tráfico por lo cual la perdida de paquetes es mínima.

En las siguientes gráficas se observa: la latencia y su distribución, Pérdida de paquetes.

Pérdida de paquetes

Con prioridad, la perdida de paquetes Inicia en el 90% para el grupo 1(videoconferencia h.323) y en el 50% para grupo 2 (Trafico de FTP, HTTP)

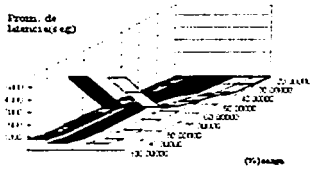


H.323 Videoconferencia

Trafico de FTP,HTTP

Latencia

Con prioridad, se observa que en el grupo 1(videoconferencia H.323) la latencia comienza a parecer aproximadamente cuando lleva el 90% de carga y en cuanto para el grupo 2 aproximadamente es en el 40% de carga.



H.323 Videoconferencia

Trafico de FTP,HTTP

Con esto se da por terminada la segunda fase de las pruebas, se observó que utilizar una herramienta de Calidad de Servicio es muy útil ya que estamos dando prioridad a los paquetes que para nosotros son más importantes en este caso se utilizó Encolamiento de Prioridad ya que esta técnica y la de CAR (rate limit), son las únicas que el router con el que se realizaron las pruebas soportaba y no se realizaron pruebas con Rate Limit ya que para nuestro caso (videoconferencia), es mas útil usar Encolamiento de Prioridad ya que cuando se configura esto dentro de un router lo que hace es que si en el momento existen paquetes de alta prioridad, estos se van a transmitir primero dejando hasta lo ultimo los de baja prioridad y con Rate Limit lo que se hace es asignar anchos de banda a cierto tipo de trafico y si en un momento dado no se esta transmitiendo nada por el ancho de banda asignado, ese ancho de banda es desperdiciado ya que no se puede transmitir nada mas que el tipo de datos que se configuraron para ese ancho de banda, por esta razón solo se realizaron pruebas con Encolamiento de Prioridad.

Es importante mencionar que el usar técnicas de calidad de servicio es algo sumamente útil dentro de nuestra red ya que vamos a tener un alto aprovechamiento de esta, pero hay que recalcar que no siempre va ser posible usar en conjunto H.323 con otros protocolos fuera de nuestra red ya que la mayoría de protocolos son configurados en el Router, y si es el caso de que uno no tenga la administración de dicho Router pues no nos será posible aplicar esto a menos que los administradores lo configuren.

4.3 PROPUESTA DE H.323

Con las pruebas realizadas tanto de Videoconferencia H.323 y Calidad de Servicio observamos que trabajar H.323 en conjunto con QoS se aprovechan mejor los recursos de la red, se revisó la posibilidad de realizar otras pruebas pero en esta ocasión realizar videoconferencia H.323 en alguna institución, empresa u escuela ya que en las pruebas que se realizaron el tráfico que se aplicó fue generado por algunas aplicaciones y siempre fue constante y en realidad el tráfico que circula en una red es muy variable por lo cual para ver realmente las ventajas y beneficios que se obtienen al utilizar H.323 dentro de la red se observarán al aplicar esta dentro de una red con tráfico real.

Lo que se propone es realizar videoconferencia H.323 y así mismo aplicar QoS dentro la red, en este caso se busca una institución que actualmente realice videoconferencia para que de esta manera al realizar las pruebas se observe la diferencia entre su estándar utilizado y H.323.

Por lo tanto se escogió a la ENEP de Aragón ya que es una escuela en donde algunas clases se imparten vía videoconferencia, aunque por el momento son muy pocas las clases que se imparten por este medio pero pensando en futuro puede ser que crezcan en cuanto a este aspecto.

Para poner en práctica esta propuesta es necesario saber el tipo de enlace y equipo tanto de videoconferencia como de comunicaciones con que cuenta dicha escuela ya que es necesario saber estos datos para poder llevar a cabo las pruebas.

Analizando el enlace que tiene asignado la ENEP de Aragón observamos que este enlace actualmente es un E1 el cual se encuentra descanalizado, es decir esta dividido: tienen asignado un ancho de banda de 384kb únicamente para videoconferencia ya que actualmente transmiten videoconferencia por H.320 y

para esto es necesario tener un enlace dedicado exclusivamente para la videoconferencia y 1600kb para datos los cuales están compartidos entre la ENEP de Aragón y la Escuela Nacional Preparatoria #3.

En cuanto al equipo de comunicaciones, en la ENEP de Aragón se cuenta con un Router Cisco series 4000 versión 9.21 (datos proporcionados por Ing. Víctor Velasco, Jefe del Departamento de Informática de la ENEP de Aragón) y el equipo de videoconferencia que tienen es un Tamberg 900 (datos proporcionados por los encargados del Departamento de Videoconferencia DGSCA).

Lo que se espera obtener con estas pruebas es que se observe la diferencia entre usar H.320 (es el estándar que se esta utilizando actualmente en Aragón) y H.323 para la videoconferencia, además una de las ventajas que nos ofrece utilizar H.323 es que podríamos liberar los 384kb que se tienen dedicados a la videoconferencia ya que H.323 no necesita que se dedique ancho de banda para transmitir videoconferencia, por que H.323 utiliza la misma infraestructura de la red, por lo tanto esos 384kb podrían ser utilizados para datos, junto con los 1600kb que están destinados para esto, así de esta manera se descongestionaría un poco la red ya que el porcentaje de utilización actualmente del enlace que se tiene en Aragón esta por arriba del 90% (este dato fue proporcionado por el departamento de Centro de operación de la Red en DGSCA), y este nivel de utilización se presenta por que no es suficiente el ancho de banda que se tienen destinado actualmente a los datos.

Como el objetivo de estas pruebas también es trabajar en conjunto H.323 con QoS, entonces aplicaríamos QoS en la red de la ENEP de Aragón ya que es muy útil por que a pesar de que con H.323 se liberarían los 384Kb que están dedicados actualmente a la videoconferencia, el ancho de banda seguiría siendo insuficiente y si no existiera QoS dentro de nuestra red quizá la videoconferencia no tendría una buena calidad, por lo mismo de la saturación que existe en el enlace, por lo tanto se sugiere aplicar alguna técnica de calidad de servicio.

Esto para que cuando se quiera transmitir videoconferencia a través de la red le de prioridad a todo los paquetes generados en la videoconferencia con esto uno de los beneficios es que ahora no se va a desperdiciar el ancho de banda como se hace actualmente, ya que al estar dedicados esos 384Kb para la videoconferencia se observa un desperdicio por que cuando no se transmite videoconferencia por el enlace pues no se esta ocupando ese ancho de banda, en cambio al utilizar H.323 y QoS se esta utilizando todo el E1 para datos y si se necesitara realizar una videoconferencia pues solo en ese momento el router, una vez configurada la técnica de calidad de servicio, va a detectar paquetes de videoconferencia y les va dar prioridad a estos sobre los demás y una vez terminada la videoconferencia el router va detectar que ya no hay paquetes de videoconferencia y nuevamente va dejar pasar el trafico de datos normalmente, de esta manera no se desperdicia ancho de banda al contrario va ser aprovechado durante el tiempo que no se esta transmitiendo videoconferencia.

Para llevar a cabo esta prueba lo que se tiene que hacer es lo siguiente:

1- Se debe tener el enlace completo para datos (es decir el E1 ya no debe de estar descanalizado).

2- Se debe de configurar H.323 en los equipos de videoconferencia.

3- Así mismo en el router de la ENEP de Aragón se tienen que agregar las líneas correspondientes de calidad de servicio, realmente esto es muy fácil de configurar ya que solo son 3 o 4 líneas de configuración que se tiene que agregar en la configuración general del router y esto nos lleva menos de 10 minutos.

En el siguiente esquema se observa como está diseñado el backbone de RedUNAM (figura 4.3.a) y como es que está conectada la ENEP de Aragón a este backbone y observamos que en el único router en el que tenemos que hacer modificaciones es en el que se encuentra en Aragón.

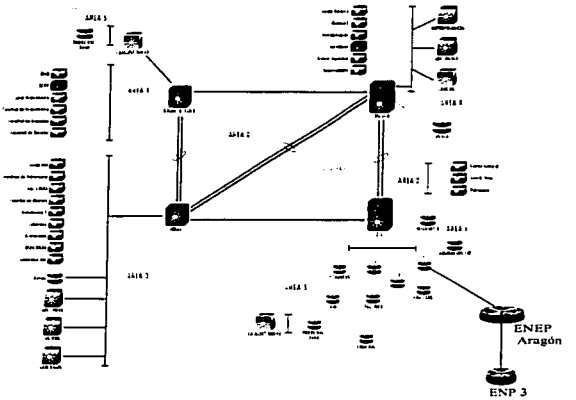


Figura 4.3.a Backbone de RedUNAM

Teniendo en cuenta los requerimientos para llevar a cabo estas pruebas, el siguiente paso es investigar con cada uno de los encargados tanto del enlace como de los equipos de videoconferencia y datos, si es posible llevar a cabo estas pruebas.

Los encargados de administrar el E1 que se tiene en Aragón, comentaron que actualmente se tiene dividido el enlace pero que esto no representa ningún problema, y si es posible tener el E1 solo para datos, después de esto se investigó si había algún problema en configurar H.323 en los equipos de videoconferencia que se tienen y el personal del Departamento de Videoconferencia de DGSCA mencionó que lo único que se debe de hacer es cambiar algunos parámetros en los equipos y que tampoco había problema alguno, pero cuando se investigó si

era posible configurar calidad de servicio en el router de Aragón, el personal del Departamento de Operación de la Red en DGSCA, mencionó que no es posible configurarle calidad de servicio a este router, ya que la versión que tiene no lo soporta.

Por lo tanto para llevar a cabo estas pruebas lo que se recomienda es cambiar el equipo de comunicaciones que se tiene, es decir cambiar el router por otro con una versión más actual (puede ser un equipo Cisco 2600 o en adelante, ya que con este tipo de equipo se puede configurar mas opciones), cambiar este equipo nos traería muchos beneficios, ya que no se trata de tan solo cambiar un equipo, sino que como se ha mencionado anteriormente las redes tienden a crecer, y cada día dentro del área de telecomunicaciones van saliendo nuevas tecnologías y el tener un equipo mas actual aparte de que nos permite tener un mejor desempeño en nuestra red, también nos permitirá aplicar esta gran variedad de tecnologías, protocolos, etc. Las cuales nos ayudan a administrar mejor la red.

Otra solución por el momento seria contratar quizá otro E1 así tendríamos más ancho de banda, lo cual por el momento nos permitiría llevar a cabo una videoconferencia con una calidad media ya que el enlace no se encontraría tan saturado y nos permitiría transmitir de alguna manera mejor la videoconferencia a comparación de solo tener un E1 como se tiene actualmente, pero esto a la larga no nos representaría una ventaja ya que como se menciono las redes a futuro van creciendo y este ancho de banda se seguiría saturando.

Así que si tuvieran que elegir por alguna de las dos opciones, la más recomendable es cambiar el router aunque lo ideal seria cambiar el router y contratar otro E1, pero si no se tiene presupuesto para ambos, pues solo seria el cambio del router ya que es la mejor opción.

Actualmente son muchas las instituciones que llevan acabo videoconferencia por medio de H.323, un ejemplo es la Universidad del Estado de México (dato proporcionado por los ingenieros de videoconferencia en DGSCA), esta universidad transmite videoconferencia H.323 dentro de la red de Internet, pero la

gran mayoría se encuentra transmitiendo videoconferencia H.323 dentro de Internet2, ya que aun es una red que no se encuentra saturada y por lo tanto pueden aprovechar mejor el ancho de banda con que disponen.

Internet2 es otra opción para poder implementar H.323 dentro de la ENEP de Aragón, y para poder estar dentro de esta red basta con que se solicite el acceso, pero también se debe de tener en cuenta algo muy importante, que es la infraestructura de red con que la cuenta la institución y en este caso lo que se mencionaba anteriormente (lo del cambio del router), nos ayudaría mucho para poder estar dentro de esta red.

La conclusión de estas pruebas desgraciadamente no se llevó acabo, pero este propuesta queda abierta por si alguien se interesa en retomarla y quizá podría dar la pauta para un nuevo trabajo de tesis.

CONCLUSIONES

En este trabajo de tesis se habló de la importancia que tiene en estos días el estándar H.323 ya que es una de las tecnologías mas importantes y atractivas de estos tiempos, debido a su implementación dentro de varias áreas, la mayoría de ellas relacionada con la educación, y también algo que es muy atractivo es su bajo costo de operación, porque como se mencionó, funciona sobre la misma infraestructura de red de datos, además de que ofrece una excelente calidad, actualmente las nuevas computadoras trabajan con plataformas que soportan mas el poder de multimedia, con procesadores veloces, con mas instrucciones y chips aceleradores de multimedia y esto hace que el estándar crezca cada vez mas y sea utilizado en muchas áreas.

Pero a pesar de esto, de esta aceptación que esta adquiriendo el estándar en lo que es la videoconferencia implementada en el área de la educación, en México el desarrollo de los sistemas de educación a distancia han sido difícil de implementar, y esto es por varias razones, una de ellas y la más importante es el presupuesto que se le otorga a la educación en general y no obstante este es repartido y lo cual nos lleva a que el presupuesto destinado a la implementación de la tecnología es muy escaso, aun sabiendo que el uso de la tecnología para facilitar la educación debería ser un punto importante para todas las escuelas que imparten una educación media superior, superior e incluso Posgrados en el país, sin embargo es todavía muy difícil de encontrar que en las escuela se aplique esto, y aún dentro la UNAM hay escuelas o facultades en las cuales no se aplica, o bien se aplica escasamente, y esto como se mencionó se debe al escaso presupuesto y también al rechazo del personal docente ya que existe un cierto paradigma hacia la implementación de la tecnología.

Y si queremos que en México la evolución de estos sistemas de educación sea mayor y más rápida, no se debe de rechazar la tecnología y mucho menos no darle importancia ya que la tecnología dentro de la educación nos ayuda a impulsar diversos modelos de educación, reducir distancias físicas, sociales y culturales aparte el alto intercambio de ideas y conocimientos y lo principal nos ayuda a expandir la educación impartida en las instituciones mas allá de su campus y con esto podríamos alcanzar la meta de superar todo el rezago educativo. La educación es uno de los indicadores de los avances y calidad de vida de cualquier país siendo en México un tema prioritario para elevar el nivel de vida de la población y de esta manera no quedarse atrás en el uso de estas tecnologías y poderlas aplicar donde se requiera

Con el estándar H.323 podremos hacer que un gran número de instituciones implementen videoconferencia interactiva a muy bajo costo y de esta manera hacer que la transmisión de voz, datos y video en tiempo real pueda llegar a ser algo cotidiano y se pueda emplear dentro de un gran número de instituciones, ya que con la tendencia de mejorar las redes de datos existentes se obtendrá que se utilice e implemente una gran cantidad de protocolos y tecnologías, y el uso del estándar H.323 aumentará a medida que lo haga el desarrollo y crecimiento de las redes de datos y con lo cual será posible que muchas instituciones educativas utilicen H.323 para poder transmitir educación a distancia vía videoconferencia interactiva y además se puede impartir cursos y seminarios de actualización al personal docente, para realizar juntas, etc. ya que la intención de utilizar este tipo de tecnología es que se aproveche al máximo todo lo que nos brinda.

Por otra parte, lo que realmente hace atractivo al estándar H.323 sobre otras tecnologías similares es que alrededor de él se encuentran otras tecnologías como son, QoS, Multicast, MPLS, etc., las cuales de la misma manera que H.323 trabajan sobre la red de datos para mejorar su desempeño con procedimientos especializados que hacen que el uso de estándares como H.323 sea más confiable y poderoso.

Y para utilizar cualquier sistema de H.323 a su potencial máximo, es esencial que los múltiples niveles de actividad estén bien planeados, saber qué es lo que queremos, hasta donde se quiere llegar y sobre todo saber con que contamos para poder realizarlo.

De esta manera se muestra que este trabajo de tesis cumplió con el objetivo principal que era la implementación de H.323 y se observó como este estándar nos permite utilizarlo en conjunto con otros protocolos, en este caso Calidad de Servicio y además comprobamos la interoperabilidad que existe entre equipos de videoconferencia de diferente proveedor y al mismo tiempo observamos como se comporto la videoconferencia al variar el ancho de banda por lo tanto el estándar H.323, resulta una solución muy interesante para los mercados de redes en el futuro, ya que es muy importante implementar este estándar dentro de la educación para su desarrollo y crecimiento.

BIBLIOGRAFÍA

IP QUALITY OF SERVICE, SRINIVAS VEGESNA
CISCO PRESS
INDIANAPOLIS USA DECEMBER 2000

VIDEOCONFERENCING, THE WHOLE PICTURE, JAMES R. WILCOX
TELECOM BOOKS, CMP MEDIA
US, CANADA

REDES LOCALES, JOSE LUIS RAYA, CRISTINA RAYA
RA-MA
MADRID

INTERNET EL MUNDO EN SUS MANOS, JOSE A. CARBALLAR
RA-MA
MADRID

"COMUNICACIÓN DE DATOS, REDES DE COMPUTADORES Y SISTEMAS ABIERTOS",
FRED HALSALL
4TA. EDICIÓN, ADDISON-WESLEY, IBEROAMERICANA, E.U. 1998.

REDES DE COMPUTADORAS, ROBLEDO SOSA CORNELIO
EDITORES E IMPRESOS FOC 1998.

TCP/IP ILUSTRATED, VOL. 1, STEVENS, W. RICHARD,
EDIT. ADDISON WESLEY, E.U. 1994.

CISCO SYSTEMS, *INTERNETWORKING TECHNOLOGY OVERVIEW*,
E.U. 1993

H.323 TECHNOLOGY VTEL CORPORATION (1998), BRUCE KRAVITZ.

ITU –T RECOMENDATION H.323 VERSION 5 (25 DE OCTUBRE DEL 2002)

DEPLOYING CISCO QOS FOR ENTERPRISE NETWORKS VERSIÓN 1.0

CISCO SYSTEMS , INC., 2001

SITIOS WEB CONSULTADOS
HTTP://WWW.CISCO.COM/
HTTP://WWW.OPENH323.ORG
HTTP://WWW.H323FORUM.ORG
HTTP://WWW.VCON.COM/
HTTP://WWW.TAMBERG.COM/
HTTP://WWW.POLYCOM.COM/HOME/