REAL TIME PROTOCOL
RTP

TAIRON EDUARDO FERRER MEJIA
MARCO ANTONIO SAENZ CABARCAS

Monografía de grado presentada como requisito para optar el titulo de Ingeniero Electrónico

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
MINOR DE TELECOMUNICACIONES
PROGRAMA DE INGENIERIA ELECTRONICA
CARTAGENA
2006

REAL TIME PROTOCOL
RTP

TAIRON EDUARDO FERRER MEJIA
MARCO ANTONIO SAENZ CABARCAS

MONOGRAFIA
DIRECTOR
MARGARITA ROSA UPEGUI FERRER M.Sc.

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
MINOR DE TELECOMUNICACIONES
PROGRAMA DE INGENIERIA ELECTRONICA
CARTAGENA
2006

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cartagena de Indias, Octubre de 2006

DEDICATORIA

A DIOS, Por entregarme la Fuerza necesaria para salir adelante y lograr una de mis metas.

A mis padres, Wilfredo y Maribel, que me brindaron su comprensión y apoyo en cada una de las fases de mi vida.

A mis hermanos, por su paciencia y apoyo a lo largo de mi carrera.

A mi sobrino, Santiago, por ser un motivo más de lucha.

A la vida, por darme una segunda oportunidad.

TAIRON

A Dios, Por siempre sentir su presencia en mí y llenarme de Fuerzas para luchar cada día más.

A Mis padres por ser soporte y brindarme la oportunidad de estudiar.

A mi esposa Vicky por su apoyo incondicional.

A mis Hijas Valentina y Angie por ser motivo constante de lucha.

MARCO

AGRADECIMIENTOS

A la Universidad Tecnológica de Bolívar por Abrirnos sus puertas y hacernos sentir como si fuese nuestro segundo hogar.

A los profesores por ser parte importante de nuestro proceso de aprendizaje.

A Nuestra directora de Monografía, Margarita Rosa Upegui Ferrer M.S.C. Por su paciencia y comprensión en todo momento.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

AH: Authentication Header. Cabecera de autenticación.

ARP: Address Resolution Protocol. Protocolo de resolución de direcciones.

ATM: Asynchronous Transfer Mode. Modo de transferencia asíncrono.

BGP: Border Gateway Protocol. Protocolo de encaminamiento utilizado en la periferia de las redes (externo).

CBR: Constant Bit Rate. Tasa de bits constante.

CBT: Core Based Tree. Protocolo de "*multicas*t" de tipo disperso *(sparse mod*e).

CIP: Classical IP Over ATM. Modo de encapsular el protocolo IP en ATM (RFC 1577).

CM: Controlador Multipunto. En inglés, MC.

CS: Control Site. En la aplicación Isabel, el CS es el sitio encargado de controlar remotamente todas las operaciones de la conferencia.

DCCP: Datagram Congestion Control Protocol. Protocolo de control de congestión de datagramas.

DVMRP: Distance Vector Multicast Routing Protocol. Protocolo de encaminamiento para multidifusión (multicast).

FRAME RELAY: Relevo de Tramas. Interfaz de Redes.

IETF: Internet Engineering Task Force. Grupo de trabajo dedicado a la estandarización y revisión de textos y recomendaciones sobre Internet.

IGMP: Internet Group Management Protocol. Protocolo que gestiona los grupos que se unen o abandonan una aplicación multicast.

ILS: Internet Locator Service.

IP: Internet Protocol. Protocolo de nivel 3, de uso generalizado para el encaminamiento en Internet.

IS: Interactive Site. Sitios o lugares desde los que se puede interactuar en la aplicación Isabel, con el resto de participantes de la Conferencia.

ITU: International Telecommunications Union.

IVS: INRIA Videoconferencing System. Permite transmitir audio y vídeo sobre Internet a partir de workstations.

JITTER: Fluctuación de retardo

LAN: Local Area Network. Red de Área Local

LANE: Local Area Network Emulation. Modo de funcionamiento que simula los servicios de una red de área local sobre una red de tecnología ATM.

MCS: Modo de comunicación seleccionado. En inglés, SCM

MInT: Multimedia Internet Terminal. Conjunto de herramientas que permite establecer y controlar sesiones multimedia en Internet.

MS: Main Site. Tipo especial de sitio en Isabel, donde hay audiencia y donde los ponentes realizan sus exposiciones.

MULTICAST: Es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios. El **multicast** es dirigido para aplicaciones del tipo

uno-para-varios y varios-para-varios, ofreciendo ventajas principalmente en aplicaciones multimedia compartidas.

MVoD: Mbone Video Conference Recording on Demand. Aplicación que permite la grabación y reproducción interactiva remota de videoconferencias multicast.

Nt: NetText. Editor de texto compartido diseñado para funcionar sobre Mbone.

NV: Network Video. Aplicación de videoconferencia que permite transmitir y recibir vídeo de baja velocidad en Internet.

PM: Procesador multipunto. En inglés, MP.

QoS: Quality of Service. Calidad de servicio.

RAT: Robust-Audio Tool. Herramienta que proporciona audio para teleconferencias en Internet.

RCC: Red de conmutación de circuitos.

RSVP: Resource Reservation Protocol. Protocolo de Reserva de recursos en Red.

RTCP: Real Time Control Protocol. Protocolo de control de tiempo real.

RTP: Real Time Protocol. Protocolo de tiempo real.

SDAP: Session Directory Announcement Protocol. Protocolo que anuncia las sesiones en la aplicación SDR.

SDP: Session Description Protocol. Protocolo que describe las sesiones en la aplicación SDR.

SDR: Session Directory. Aplicación directorio de sesiones diseñada para anunciar y planificar conferencias multimedia sobre Mbone.

TCP: Transport Control Protocol. Protocolo de control de transporte orientado a conexión, por lo que proporciona reensamblado y secuenciamiento de paquetes.

UCM: Unidad de Control Multipunto. En inglés, MCU.

UDP: User Datagram Protocol. Protocolo de intercambio de unidades de datos en Internet, de nivel 4, no orientado a conexión.

VIC: Video Conferencing Tool. Aplicación multimedia a tiempo real para conferencias de vídeo sobre Internet.

VLAN: Lan Virtual.

VoIP: Voz Sobre IP.

WAN: Wide Area Network. Red de área extensa, que conecta nodos situados en un área geográfica amplia.

WB: White Board. Pizarra electrónica compartida.

WP: Watch Point. Sitios que sólo reciben datos en la aplicación Isabel

INTRODUCCION

La red Internet se convirtió en una herramienta importante y fundamental dentro del desarrollo tecnológico, la necesidad de transmisión de información multimedia (audio y vídeo) tendrá un gran impacto en los sistemas de comunicación. Esta transmisión requerirá no sólo el soporte de las redes, sino también de los protocolos que ayuden a que esto se realice.

En este sentido se trabaja tanto en redes locales (LAN) como en *internetworks*. Podemos hablar de transmisión de información en tiempo real cuando se puede asegurar que la información llegue a su destino con unos parámetros determinados (retraso, rendimiento, fiabilidad, etc.). En este sentido se puede asumir que la transmisión multimedia tiene unos requerimientos temporales que necesitan del uso de esta transmisión en tiempo real.

En general las aplicaciones multimedia requieren una calidad de servicio (*QoS*) por parte de los servicios de red. De las nuevas redes se exige poder especificar esta calidad de servicio y asegurar su cumplimiento.

Dentro de lo anterior encontramos el protocolo RTP, quien provee transporte entre sistemas finales para datos en tiempo real sobre una red y es una base para la comunicación de información multimedia.

RESUMEN

El protocolo RTP tiene como función el transporte de extremo a extremo para aplicaciones que requieren transmisión de datos en tiempo real (ya sea o no en régimen interactivo), como pueden ser sonido, imágenes o datos de simulación. RTP se ha diseñado junto con su perfil de sonido y vídeo como protocolo de transporte para conferencias multimedia con múltiples participantes, siendo Así mismo válido para otras aplicaciones, como simulación interactiva, almacenamiento de flujos continuos de datos o aplicaciones de control de procesos.

Aunque generalmente se habla de RTP como un protocolo de transporte de nivel de aplicación, sería más riguroso definirlo como un modelo de protocolos, puesto que su especificación es deliberadamente incompleta y flexible, proporcionando una estructura y un conjunto de mecanismos comunes, en lugar de algoritmos concretos. El diseño de RTP atiende a dos principios de gran importancia en sistemas de tiempo real: integración del procesamiento de los diferentes niveles de la arquitectura de la pila de protocolos y de las aplicaciones, y segmentación de unidades de datos de transporte en el nivel de aplicación. Por ello, el desarrollo de una aplicación basada en RTP requiere Seguir la especificación general conjuntamente con un perfil que la complete, de los que el único desplegado actualmente es el perfil general para transporte de sonido y vídeo. Así mismo, para aquellos formatos multimedia no cubiertos

por el perfil general, es necesario especificar reglas de empaquetado específicas para el formato de datos.

Como nota general acerca de RTP, su diseño le hace ser aplicable tanto en entornos unicast como multicast, lo que en la práctica requiere que todos los mecanismos contemplados por el protocolo sean escalables. RTP proporciona, entre otras, funciones de identificación de tipos de contenido y de fuentes de sincronización, reordenación de la secuencia de unidades de datos, detección de pérdidas, seguridad e identificación de participantes y contenidos.

RTCP aporta funciones de identificación de participantes entre diferentes sesiones y sincronización entre distintos flujos RTP, realimentación acerca de la calidad de recepción, estimación del número de participantes en sesiones multimedia y transporte de información de monitorización y control. La definición de RTCP como componente adicional permite que aplicaciones que requieran un mayor nivel de control que el proporcionado por RTCP lo reemplacen con otros protocolos de control de A corto plazo, la alternativa más sólida como protocolo de transporte base para SIP es SCTP Arquitectura de los sistemas multimedia de Internet.

El diseño de RTP prevé la existencia de sistemas intermedios de nivel RTP, además de los sistemas terminales o aplicaciones de usuario. Los experimentos realizados en redes multicast durante el desarrollo de RTP han

demostrado la utilidad de estos elementos para hacer posible la comunicación multimedia en tiempo real de varios usuarios pertenecientes a diferentes organizaciones, en particular para solucionar los problemas derivados de conexiones con anchos de banda diversos y de la presencia de cortafuegos entre zonas administrativas.

Así, en aquellos casos en que los participantes en una sesión RTP pueden utilizar diferentes formatos multimedia, en lugar de establecer la configuración más restrictiva, se puede introducir elementos repetidores de nivel RTP (mezcladores RTP), en el punto de enlace con las zonas de ancho de banda limitado. Estos mezcladores combinan múltiples flujos de entrada en uno solo, pudiendo además traducir entre diferentes formatos multimedia. Así mismo, algunos participantes pueden no tener acceso multicast por encontrarse tras unos cortafuegos. Para estos casos, un repetidor de nivel RTP, un traductor RTP, puede hacer de intermediario. Estas situaciones requieren la instalación de dos Traductores (o un traductor bidireccional), uno a cada lado del cortafuegos; el primero introduce los flujos procedentes de la red multicast en la red unicast y el segundo realiza la operación inversa.

CAPITULO 1

CALIDAD Y SERVICIO EN REDES IP

Este capitulo trata un poco sobre los problemas de calidad de servicio en la redes IP, los umbrales de *QoS* definidos, las herramientas disponibles para hacerlo posible y protocolos necesarios para servicios de tiempo-real.

1.0 CALIDAD DE SERVICIO EN REDES IP

La calidad de servicio (QoS) es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los parámetros de QoS son: [1]el retardo, la variación del retardo y la pérdida de paquetes. Una red debe garantizar un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros.

La implementación de Políticas de Calidad de Servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

- Asignar ancho de banda en forma diferenciada
- Evitar y/o administrar la congestión en la red
- Manejar prioridades de acuerdo al tipo de tráfico
- Modelar el tráfico de la red

[1] GARCIA TOMAS, Jesús, RAYA, Víctor Rodrigo. Alta Velocidad y Calidad de Servicios en Redes IP.

Calidad de Servicio: el retardo, sus variaciones y pérdidas de paquetes.

1.1 CALIDAD DE SERVICIO *QoS (Quality of Service)*

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. En las redes [2] Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de ***CIR*** *(Commitated Information Rate)* con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como son los protocolos de tiempo-real **RTP** y de reserva **RSVP**. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (***VoIP***) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado ***LFI***. Mediante ***QoS (Quality os Service)*** se tiende a preservar los datos con estas características.

Los servicios tradicionales de la red Internet (***SMTP o FTP***) disponen de una calidad denominada "***best effort***"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como la web. Para servicios del tipo "***real-time***" (voz y vídeo) se requiere una latencia mínima.

[2] UILESS, Black. Tecnologías Emergentes para redes de Computadoras. Editorial Pearson Educación. Segunda Edición. 1997.

Frame Relay, ATM.

1.2. LATENCIA-JITTER.

Se denomina **latencia** a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "*store-andforward*" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc). Un tiempo de latencia variable se define como *jitter* sobre los datos de recepción. La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor.

Se han implementado diversas formas de buffer garantizados mediante software:

-Cola prioritaria: donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.

-Cola definida: donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.

-Cola ponderada: mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

1.3. VARIANTES DE SERVICIOS.

Los servicios de datos y de multimedia tienen distintos requerimientos de calidad referido a latencia y jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

TABLA 1
VARIANTES EN CAPA 2,3 y 4

CoS -(Class of Service).	***CoS*** se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada ***Tag o Label***) dentro del protocolo ***MAC***. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del switch ***LAN*** para la descarga de paquetes.
IEEE 802.1p	Determina el uso de un Tag en el encabezado de MAC con 3 bits de precedencia. Se define el protocolo para registración de ***CoS GARP*** (***Generic Attribute Registration Protocol***). Las aplicaciones específicas del GARP son la registración de direcciones multicast ***GMRP (Multicast GARP)*** y de usuarios ***VLAN*** con protocolo ***GVRP (LAN GARP)***
IEEE 802.1Q	Servicio ***VLAN*** para realizar enlaces troncales punto-a-punto en una red de switch.
IEEE 802.3x	Este standard examina el control de flujo en enlaces ***Etherne***t del tipo full-dúplex. Se aplica en enlaces punto-a-punto (***Fast y Gigabit Ethernet).*** Si existe congestión se emite hacia atrás un paquete llamado "***pause frame***" que detiene la emisión por un período de tiempo determinado. Una trama denominada "***time-to-wait zero***" permite reiniciar la emisión de paquetes.
IEEE 802.1D	-Define el protocolo ***STP (Spanning-Tree Protocol)***. Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. De esta forma se crean puertas redundantes en el cableado, el protocolo ***STP*** deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra.
ToS -(*Type of Service*).	Es sinónimo de ***CoS*** en la capa 3. Sobre el protocolo IP se define el ***ToS*** con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.
QoS -(*Quality of Service*)	En redes IP se define la tasa de acceso contratada **CAR** (*Committed Access Rate*) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación **RSVP** y de tiempo real **RTP**.

TABLA 2
CLASIFICACION DE LA QoS

Guaranteed	El servicio garantizado es utilizado para requerir un retardo máximo extremo-a-extremo. Se trata de un servicio análogo al **CBR** (*Constant Bit Rate*) en ATM. Se puede aplicar un concepto de reservación de tasa de bit (utiliza **RSVP**) o el método *Leaky-bucket*. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como *Hard QoS*.
Differentiared	El servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades
ToS (*Type of Service*)	Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un *Soft QoS*. El control de aplicación es del tipo *leaky-bucket*. ***Best-effort*.** -Este es un servicio por *default* que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo **FIFO**. Por ejemplo, el software Microsoft NetMeeting para aplicaciones multimediales utiliza la norma **H.323 (E.164)**; trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio **QoS**

1.4 HERRAMIENTAS PARA QoS.

Dentro de las herramientas para la calidad y servicio Se relacionan los distintos tipos de herramientas que se disponen para asegurar una QoS dentro de una red IP, por ejemplo el manejo de congestión y tráfico,

1.4.1 MANEJO DE CONGESTION Y TRÁFICO

Trata de conseguir mecanismos que prevengan o manejen una congestión, distribuyen el tráfico o incrementan la eficiencia de la red. Los protocolos involucrados en asegurar la calidad de servicio son los indicados en las Tablas Siguientes; A los mismos se refiere como mecanismos de señalización.

TABLA 3

HERRAMIENTAS DISPONIBLES PARA ASEGURAR LA QOS.

FIFO -(*First In, First Out*)	El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *Default* en las redes IP. Es válido solo en redes con mínima congestión. No provee protección, no analiza el ancho de banda ni la posición en la cola de espera.
PQ -(*Priority Queuing*).	Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles que puede aportar el encabezado del datagrama IP (**ToS** *Type of Service*). Se trata de 3 bits disponibles en el Byte 2 del encabezado de IPv4 (bits de precedencia).
CQ -(*Custom Queuing*)	Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. El operador reserva un espacio de buffer y una asignación temporal a cada tipo de servicio. Es una reservación estática
WFQ -(*Weighted Fair Queuing*).	Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket* –port de **TCP/UDP**-) y por el **ToS** en el protocolo IP. En este esquema la menor ponderación es servida primero. Con igual ponderación es transferido con prioridad el servicio de menor ancho de banda. El protocolo de reservación **RSVP** utiliza a **WFQ** para localizar espacios de buffer y garantizar el ancho de banda.

TABLA 4

CONTROL DE TRÁFICO

-WRED -(*Weighted Random Early Detection*)	Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta. Está diseñada para aplicaciones **TCP** debido a la posibilidad de retransmisión. Esta pérdida en la red obliga a **TCP** a un control de flujo reduciendo la ventana e incrementándola luego en forma paulatina. Un proceso de descarte generalizado, en cambio, produce la retransmisión en "olas" y reduce la eficiencia de la red
GTS -(*Generic Traffic Shaping*).	Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera.

TABLA 5

INCREMENTO DE LA EFICIENCIA - SEÑALIZACIÓN.

LFI (*Link Fragmentation and Interleaving*).	El tráfico interactivo como **Telnet** y **VoIP** es susceptible de sufrir latencia y jitter con grandes paquetes en la red o largas colas en enlaces de baja velocidad. Se basa en la fragmentación de datagramas y el intercalado de los paquetes de tráfico
RSVP -(*Resource Reservation Protocol*).	Se trata de implementar el concepto de Señalización. Se dispone de dos tipos de señalización: en-banda (por ejemplo los bits de precedencia para **ToS**) y fuera-de-banda (mediante un protocolo de comunicación como el RSVP). Este protocolo permite que un host o un router asegure la reservación de ancho de banda a lo

	largo de la red IP.
RTP-HC(*Real-Time Protocol-Header Compression*)	La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de **RTP/UDP/IP** a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas.

No todas las herramientas disponibles son usadas en los mismos router. Por ejemplo, la clasificación de paquetes, el control de admisión y el manejo de la configuración se usan en los router de borde (*eage*), en tanto que en los centrales (*backbone*) se gestiona la congestión. El tratamiento de la congestión se fundamenta en el manejo de las colas en buffer mediante diferentes técnicas. El buffer es la primera línea de defensa frente a la congestión. El manejo correcto (mediante **políticas de calidad** de servicio) del mismo permite determinar la calidad de servicio. Una segunda defensa es el control de flujo. El problema del control de flujo en **TCP** es que se da de extremo-a-extremo y no considera pasos intermedios. En **TCP** cada paquete de reconocimiento lleva un crédito con el tamaño del buffer disponible por el receptor. Un sobreflujo de datos en los routers de la red se reporta mediante el mensaje *Source Quench* en el protocolo [3] **ICMP**. Estos mecanismos son ineficientes y causan severos retardos en la conexión.

[3] http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html
Protocolo ICMP

CAPITULO 2

PROTOCOLO DE TIEMPO REAL

“RTP”

En este capitulo definiremos el protocolo de Tiempo Real RTP, junto con sus características y formato.

2.0 PROTOCOLO DE TIEMPO-REAL (RTP)

Debido a que el protocolo TCP no podía realizar ciertas funciones como el envío de información en tiempo real y el protocolo UDP es no orientado a la conexión y por lo tanto no proporciona ningún tipo de control de errores ni de flujo, aunque utiliza mecanismos de detección de errores. Cuando detecta un error en un datagrama en lugar de entregarlo a la aplicación se descarta, además no existe el concepto de calidad de servicio (**QoS**), debido a lo anterior surge el **Protocolo de Tiempo-Real** (RTP**)**. El cual fue desarrollado por **la IETF**, define realmente dos protocolos:

- RTP (Real Time Transport Protocol)
- RTCP (Real Time Transport Control Protocol)

El objetivo de este protocolo es el de proporcionar el transporte de extremo a extremo para aplicaciones con requisitos de tiempo real en [4] redes unicast o multicast:

- Videoconferencia.
- Difusión de audio/video.
- Simulaciones.

Sobre un servicio de red *unicast*, se copian por separado los datos, son enviados de la fuente para cada destino.

[4] UILESS, Black. Tecnologías Emergentes para redes de Computadoras. Editorial Pearson Educación. Segunda Edición. 1997.

Redes Unicast – Redes Multicast

Sobre un servicio de red *multicast*, los datos son enviados de la fuente sólo una vez y la red es responsable de transmitir los datos para las localizaciones múltiples. La multicast es más eficiente para muchas aplicaciones de multimedia como videoconferencias.

EL Protocolo en Tiempo Real (**RTP)**, provee transporte entre sistemas finales para datos en tiempo real sobre una red de datagramas. Generalmente opera sobre UDP por varios motivos:

- Aprovecha las funciones de control de error y de múltiplexación.
- Por ser un protocolo de transporte no orientado a la conexión, no ofrece confiabilidad, por lo que no generará retransmisiones que puedan congestionar la red (para datos en tiempo real, la confiabilidad no es tan importante como la entrega rápida).
- RTP soporta una amplia variedad de aplicaciones multimedia y está diseñado para adicionarle más aplicaciones sin cambiar el protocolo. Para cada clase de aplicación (por ejemplo, audio), RTP define un perfil y uno o más formatos . El *perfil* proporciona información para asegurar el entendimiento de los campos de la cebecera (header) de RTP para la aplicación. El formato especifica cómo los datos que siguen al *header* deben ser interpretados.

2.1 CARACTERISTICAS PRINCIPALES DE RTP

Las siguientes son características importantes de **RTP:**

- Los servicios que incluye **RTP** suministran toda la información necesaria para que una aplicación en tiempo real trabaje de manera interactiva y eficaz. Estos servicios suministran información como:
  - El formato de datos a transmitir
  - Números de secuencia en los paquetes para la reconstrucción de los datos.
  - Marcas de tiempo para su posterior uso.
  - Control del transporte.
- RTP puede funcionar sobre cualquier protocolo de transporte, aunque lo más habitual es usarlo sobre UDP.
- Soporta la transmisión mediante multienvío, si ésta es soportada por los protocolos de nivel inferior.
- No proporciona medios para la gestión de errores en la transmisión. Éste se deja en manos de los protocolos de niveles inferiores.
- Es un protocolo extensible, es decir, proporciona mecanismos para añadir nuevos servicios.
- Proporciona un mecanismo de confidencialidad, para lograr que únicamente los receptores sean capaces de decodificar los paquetes.
- Permite la negociación del medio de transporte y de los parámetros que se utilizarán para transmitir los distintos flujos.

2.2 FORMATO DE LOS PAQUETES RTP

La siguiente figura muestra la cabecera utilizada por el protocolo RTP

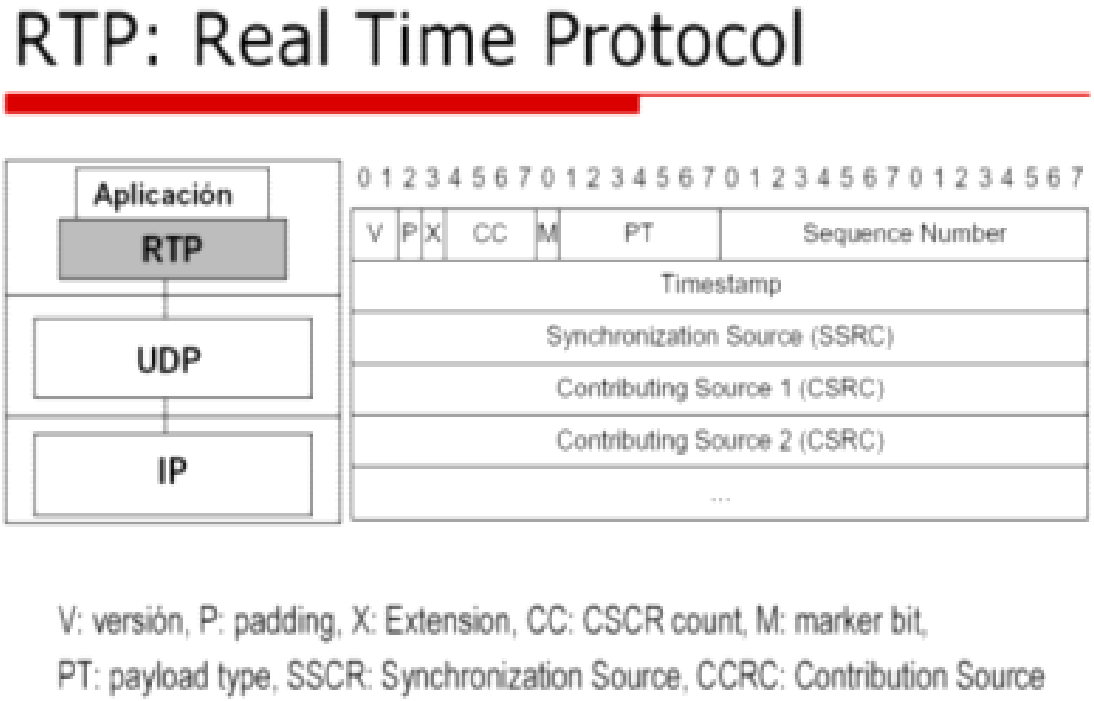


FIGURA 1. FORMATO DE LOS PAQUETES RTP

Los primeros 12 octetos (es decir, los campos V, P, X, CC, M, PT, sequence number, timestamp y SSRC) siempre están presentes, en tanto que los identificadores de "fuentes contribuyentes" (nodos que generan información al mismo tiempo supongamos, una para videoconferencia) son utilizados sólo en ciertas circunstancias. Después del *header* "básico" puede tenerse extensiones opcionales para el *header* (Extension header).

Finalmente el header es seguido por los datos (payload) que transporta RTP y su formato es definido por la aplicación.

El diseño del *header* de RTP busca llevar sólo aquellos campos que son necesarios para diversos tipos de aplicaciones.

- V: **Versión, (2 Bits):** los dos primeros bit, indica la versión del protocolo.
- P: **Padding, (1 Bits):** El siguiente bit identifica el *padding (Relleno)*. Indica si el campo de datos contiene información adicional, que no pertenece a la parte de datos. Para completar un bloque de cierto tamaño. El último byte en el mensaje UDP dice de qué tamaño es el *padding.*

Con esto se cumple el objetivo de tener un *header* RTP pequeño. La longitud de los datos se calcula a partir de la información del *header* del protocolo de la capa inferior (UDP en este caso).

- X **(Extensión), 1 bit:** El bit de extensión es utilizado para indicar la presencia de un *header* de extensión que puede ser definido para una aplicación específica y sigue al *header* principal. Ese tipo de *headers* son utilizados en raras ocasiones ya que es posible definir un *header* dentro de los datos (*payload*), como parte de la definición del formato de los datos para una aplicación en particular.

- CC **(CSRC count), 4 bits:** El bit X es seguido por 4 bits (CC) que cuentan el número de "fuentes contribuyentes" incluidas en el *header* de RTP (en caso de que existan dichas fuentes).
- **M (Marker), 1 bit:** Este bit es utilizado para indicar (Marcar) el *frame*. Por ejemplo, puede indicar el inicio de una conversación en RTP: el primer frame.
- **PT (payload type), 7 bits:** Los siguientes 7 bits indican qué tipo de dato multimedial se está transportando (*payload type*). En base a este valor, el receptor sabe cómo ha de reproducir los datos del paquete RTP. Los documentos de especificación de perfil registrados establecen una relación estática entre tipos de datos y formatos de datos. Este campo no debe utilizarse para la multiplexación de flujos de diferentes medios. Para ello se han de utilizar sesiones diferentes. El uso exacto del bit "marker" (M) y del "payload type" (PT) dependen del perfil (*profile*) de la aplicación. El *payload type* NO se usa como llave de demultiplexamiento para dirigir los datos a una aplicación diferente; ese demultiplexamiento lo realiza el protocolo de la capa inferior: UDP. Dos *streams* de datos multimediales diferentes utilizan números de puerto diferente.

- **Sequence number, 16 bits:** El número de secuencia es utilizado para permitir al receptor de un *stream* RTP detectar paquetes perdidos o que lleguen en desorden. Observe que RTP no indica qué hacer cuando se pierde un paquete (muy diferente a TCP que corrige la perdida por retransmisión e interpreta la perdida como un indicador de congestión que puede llevar a reducir el tamaño de la ventana en TCP). Por el contrario, RTP deja que la aplicación decida qué es lo mejor que puede hacer cuando el paquete se pierde. El campo **número de secuencia** se incrementa en uno en cada paquete RTP transmitido por una fuente en una sesión. Esto le permite al receptor detectar la pérdida de paquetes, y recomponer la secuencia original trasmitida por el origen.

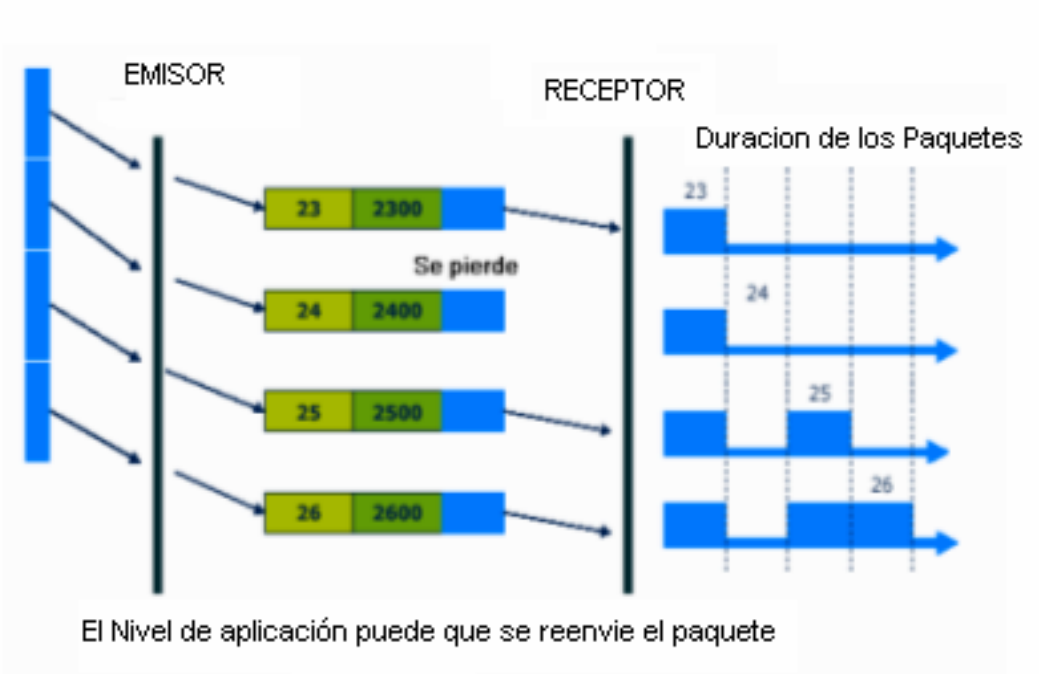


FIGURA 2. DETECCION DE PERDIDAS DE PAQUETES

- **Timestamp, 32 bits:** El campo de *timestamp* almacena el instante en el que el primer octeto del paquete RTP fue muestreado. El receptor utiliza este valor para reconstruir las referencias temporales de la señal original, y poder reproducirla a la velocidad adecuada. El *Timestamp* también puede ser utilizado para sincronizar flujos correspondientes a medios diferentes, por ejemplo, voz y vídeo, pero esta tarea no corresponde a RTP, sino a la aplicación. RTP no específica en que unidades se debe enviar este *timestamp,* las aplicaciones y sus formatos requieren diferentes estados de tiempo. El *timestamp* viene a ser un contador de "ticks" donde el tiempo entre "ticks" depende del formato de codificación de la aplicación (el estado del reloj es uno de los detalles que se especifica en el *profile* de RTP o en los datos *payload* de la aplicación).

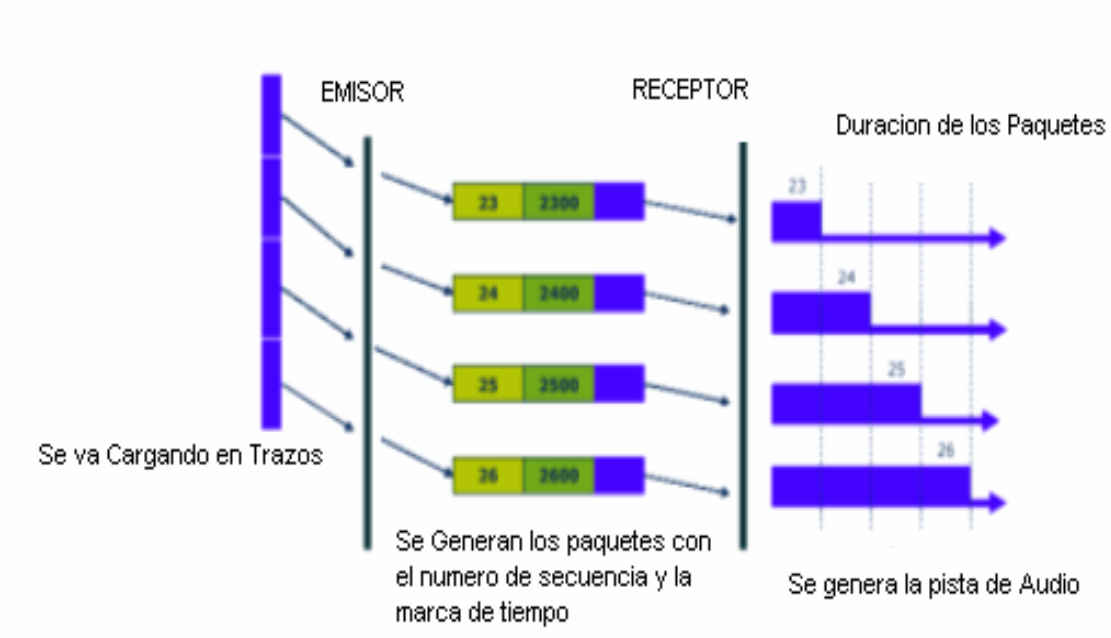


FIGURA 3. SEGMENTACION DE PAQUETES

- **SSRC, 32 bits:** El identificador de *fuente de sincronización* (SSRC) es un número de 32 bits que identifica de manera única una sola fuente en un *stream* RTP. En una conferencia multimedial, cada emisor escoge un SSRC aleatorio. El identificador de fuente es diferente de la dirección IP o del número de puerto, que permite, por ejemplo, que un nodo con múltiples fuentes (un equipo con varias cámaras) distinga cada una de las fuentes. Cuando un solo nodo genera diferentes *media streams* (por ejemplo, audio y video al mismo tiempo), no es necesario que utilice el mismo SSRC en cada *stream* ya que RTCP tiene un mecanismo para hacer sincronización intermedia. Este campo es utilizado por los **mezcladores** que son elementos que combinan los flujos procedentes de diferentes fuentes y reenvían el flujo combinado, marcándolo con su identificador SSRC. Los SSRC de las fuentes originales son adjuntados en la lista de identificadores CSRC (*Contributing Source*). Los mezcladores se utilizan para adaptar el flujo de grupos de usuarios que disponen de poco ancho de banda. De esta forma el resto de usuarios puede seguir haciendo uso de un ancho de banda más elevado.

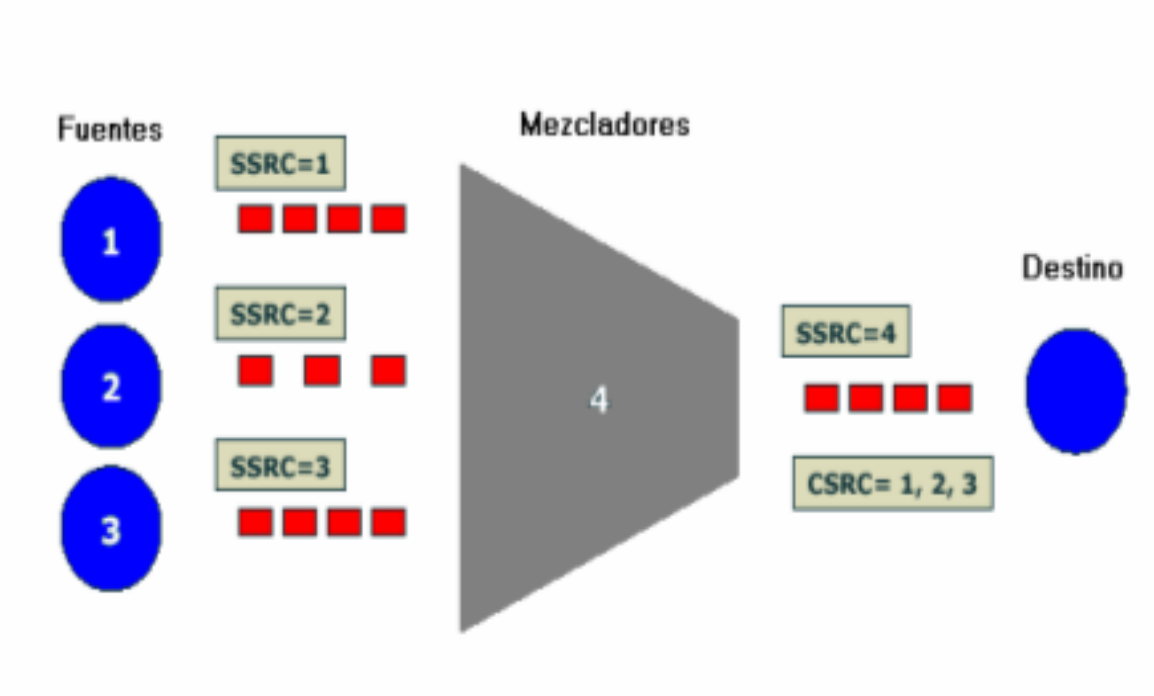


FIGURA 4. MEZCLADORES

Otro elemento definido en la arquitectura del protocolo RTP, son los **traductores**. Estos reenvían paquetes con su identificador **SSRC** intacto, aunque pueden modificar la codificación de los datos. Otro uso importante de los traductores consiste en la adaptación de paquetes **RTP** entre redes con protocolos de transporte y red subyacentes diferentes, como es el caso de redes con **IP/UDP** y para atravesar *firewalls*, que impiden la propagación de tráfico *multicast*. En este último caso es necesario el uso de dos traductores, uno a cada lado del *firewalls*, que conviertan el tráfico *multicast* a *unicast* y en el sentido contrario.

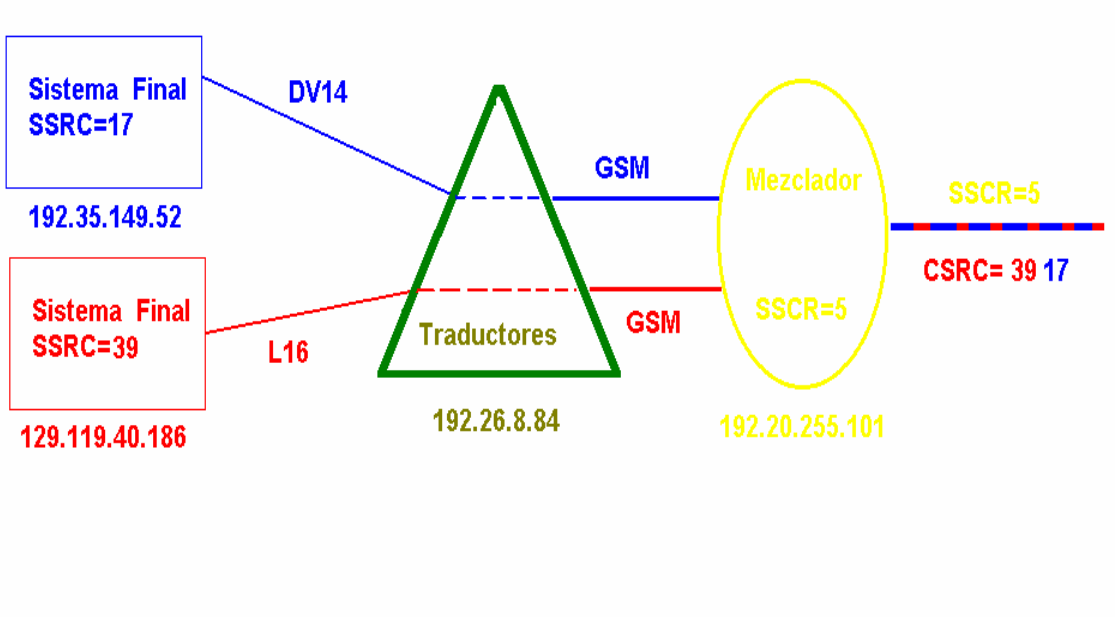


FIGURA 5. TRADUCTORES

Lista CSRC, de 0 a 15 elementos, cada uno de 32 bits: El identificador de *fuente contribuyente* (CSRC) es utilizado *sólo* cuando varios *streams* RTP pasan a través de un mezclador (*mixer*). Un mezclador puede ser utilizado para reducir los requerimientos de ancho de banda para una conferencia recibiendo datos de muchas fuentes y enviando estas como un sólo *stream*. El número de identificadores incluidos en el *header* RTP viene colocado en el campo CC (CSRC count). Si hay más de 15 fuentes contribuyentes, sólo 15 pueden ser identificadas.

- EJEMPLO DE RTP CON MEZCLADORES Y TRADUCTORES

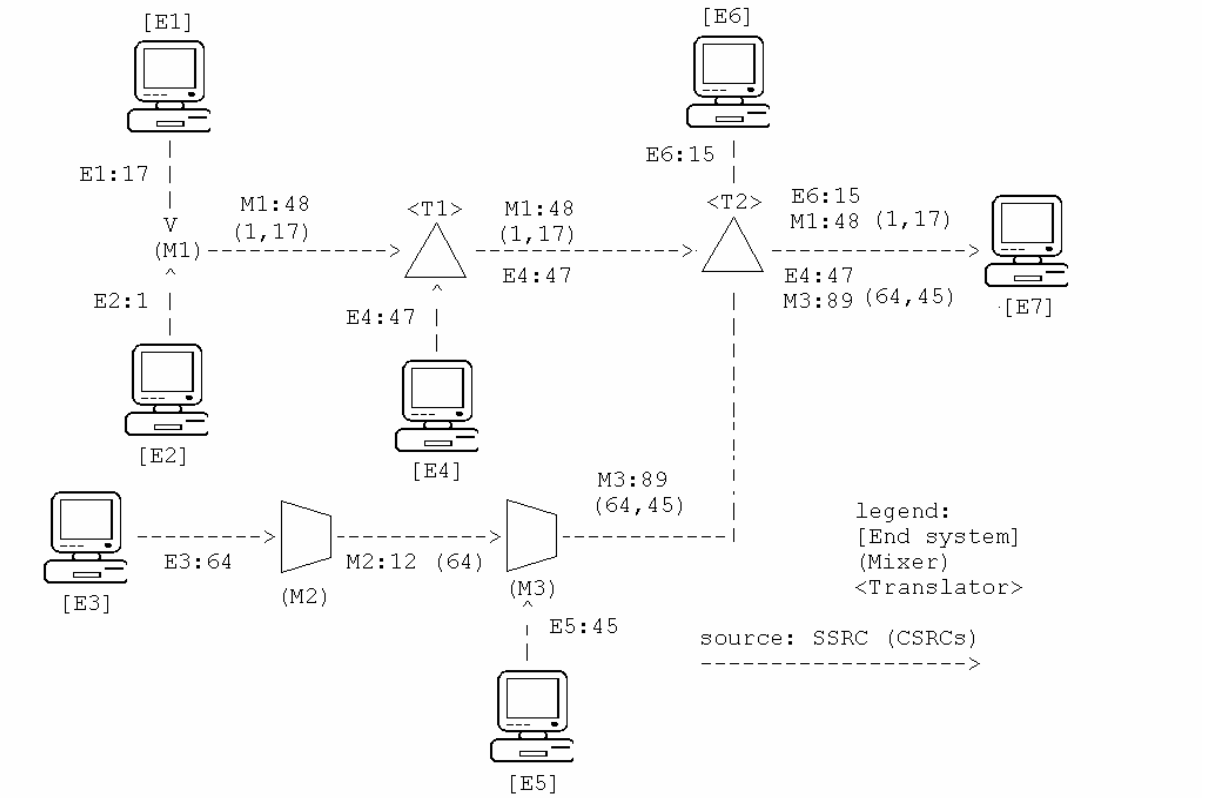


FIGURA 6. EJEMPLO DE RTP CON MEZCLADORES Y TRADUCTORES

Una colección de mezcladores y traductores se muestra en Fig. 6 ilustra su efecto en SSRC y identificador CSRC. En la figura, se muestran unos sistemas de extremo (E), traductores como triángulos (T) y mezcladores como ovalado (M). La anotación "M1:48(1,17)" designa un paquete que origina un mezclador M1, identificado por, M1 SSRC valoran de 48 y dos identifiers de CSRC, 1 y 17, copiado del identificador de SSRC de paquetes de E1 y E2.

2.3 SESIÓN RTP

Una sesión RTP, es una asociación entre un set de aplicaciones comunicandose con RTP. Una sesión es identificada por una dirección de la red y un par de puertos, (Un puerto Par para los datos RTP, el cual sirve para los datos de Multimedia y el siguiente puerto impar superior para RTCP para los datos de control.

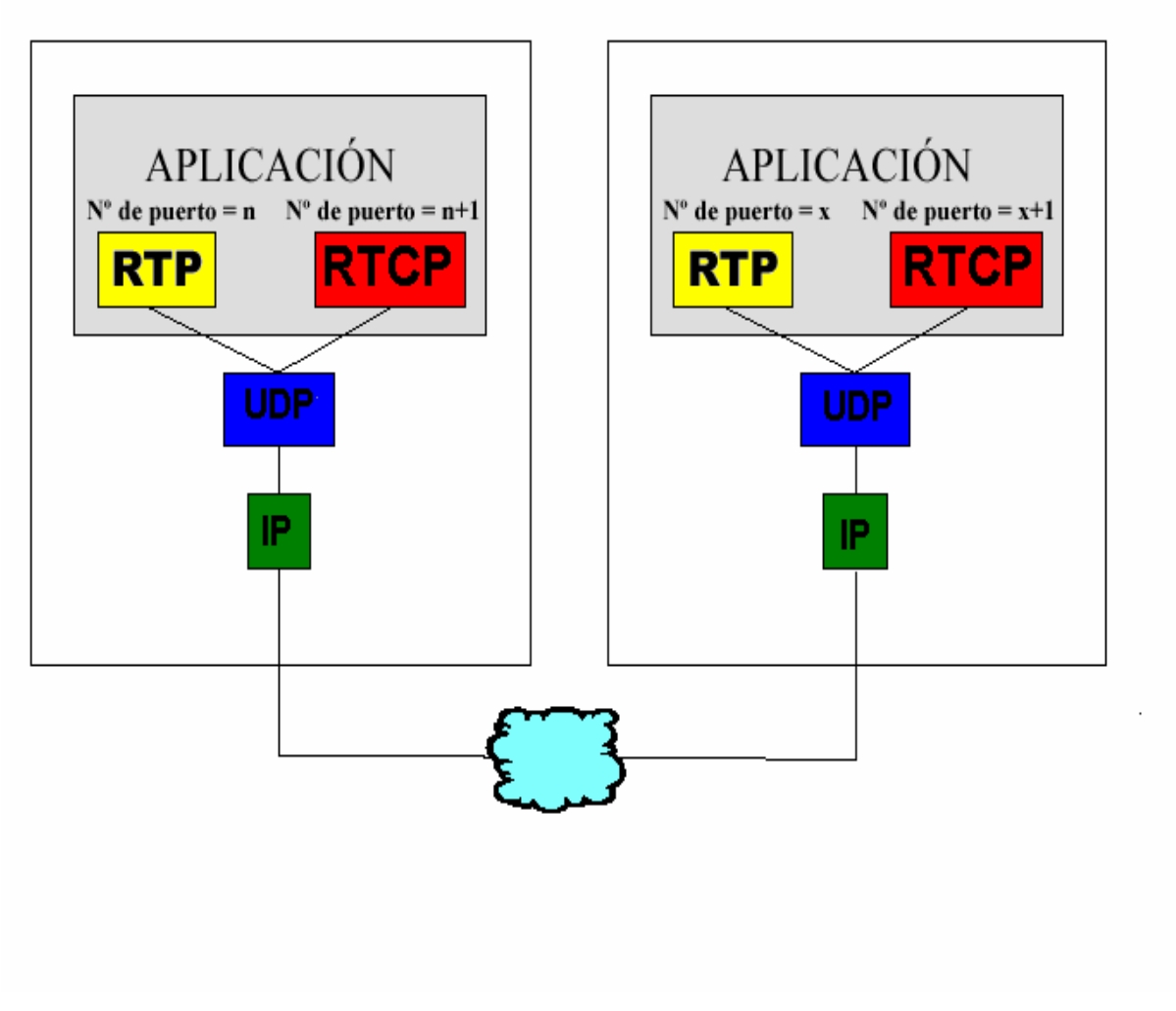


FIGURA 7 ENVÍO DE PAQUETES RTP/RTCP

Un participante es una sola máquina, *host*, o el usuario participando en la sesión. La participación en una sesión puede constar de recepción pasiva de datos (receptor), transmisión activa de datos (emisor), o ambos.

Cada tipo de multimedia es transmitido en una sesión diferente. Por ejemplo, si audio y el video son usados en una conferencia, entonces una sesión se usa para transmitir los datos de audio y una sesión separada se usa para transmitir los datos del video. Esto ayuda a los participantes a escoger cuál los tipos de datos (multimedia) quieren recibir por ejemplo, alguien que tiene una conexión de red con ancho de banda bajo sólo podría querer recibir la porción de audio de un congreso.

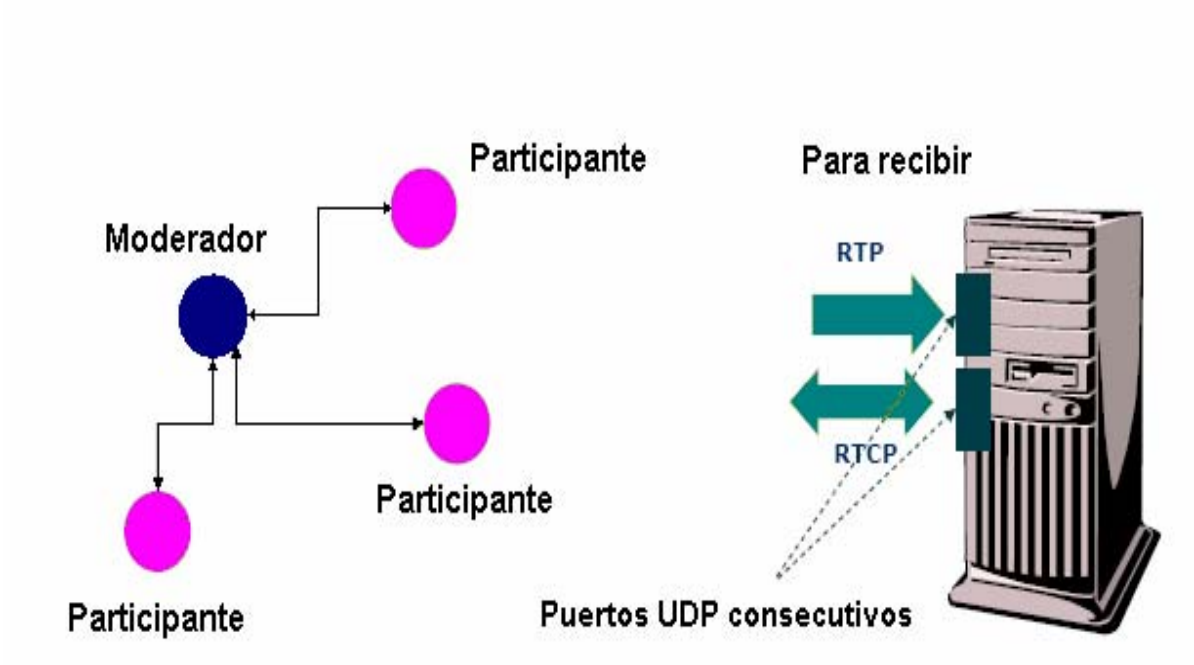


FIGURA 8 SESIÓN RTP

Dentro de la Sesión RTP tenemos en cuenta lo siguientes elementos:

- Una vez se ha establecido la sesión cada participante podrá transmitir bloques de información con una duración establecida (tiempo) en el campo de carga útil del protocolo RTP.

- Las tramas RTP se encapsulan en datagramas UDP.

- La cabecera RTP especificará el tipo de codificación de audio utilizada.

- Se incluirá un número de secuencia y marcas de tiempo.

CAPITULO 3

PROTOCOLO DE CONTROL DE TRANSPORTE DE TIEMPO REAL "RTCP"

Este capitulo nos muestra el protocolo de control de Transporte de Tiempo Real "RTCP", que es un protocolo diseñado para trabajar conjuntamente con RTP.

3.0 PROTOCOLO DE CONTROL DE TRANSPORTE DE TIEMPO REAL "RTCP"

RTCP (Real – Time Transport Control Portocol) nos proporciona un control en el flujo, que está asociado con datos para una aplicación de multimedia. Además de los datos de multimedia para una sesión, los datos de control son enviados periódicamente para todos los participantes en la sesión**.** Los paquetes **RTCP** pueden contener información acerca de la calidad de servicio (**QoS**) para los participantes de sesión, información acerca de la fuente transmitida en el puerto de datos, y las estadísticas relacionadas con los datos que les han sido transmitidas hasta en el momento.

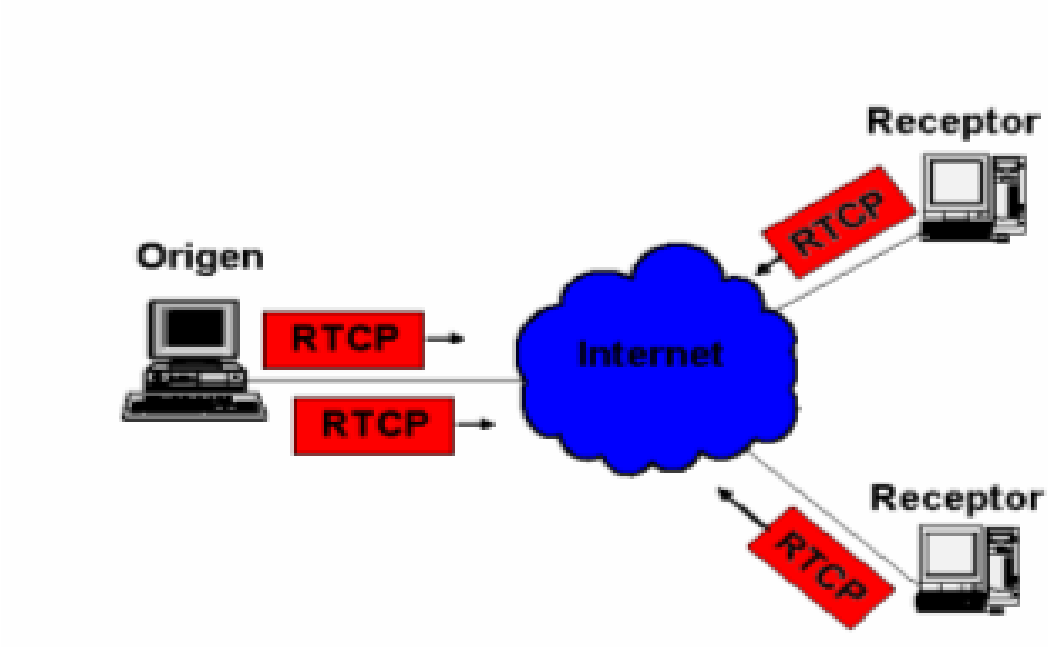


FIGURA 9 ENVÍO DE PAQUETES RTCP

Este *stream* de control tiene tres funciones principales:

1. Retroalimenta la información sobre el desempeño de la aplicación y de la red.
2. Ofrece una forma de correlacionar y sincronizar diferentes *media streams* que provienen del mismo emisor.
3. Proporciona una forma de transferir la identidad de un emisor para ser mostrada en la *interfase* de un usuario

La primera función es muy útil para aplicaciones de velocidad adaptadas y le permitiría, por ejemplo, utilizar un esquema de compresión más agresivo para reducir la congestión o enviar un *stream* de más alta calidad ya que hay poca congestión. Esta característica puede ser útil también para diagnosticar problemas de la red.

La segunda función parece estar ya cubierta con el identificador de fuente de sincronización de RTP (SSRC), pero en realidad no es así. Como se dijo antes, un nodo con varias cámaras pueden tener un SSRC diferente para cada cámara. Adicionalmente, no se requiere que un *stream* de audio y otro de video provenientes del mismo nodo utilicen el mismo SSRC. Ya que pueden darse colisiones de identificadores de SSRC es posible que se requiera cambiar el valor SSRC de un *stream*. Para poder manejar este problema, RTCP utiliza el concepto de nombre canónico (CNAME) que es asignado al emisor, este

nombre canónico es luego asociado a varios valores SSRC que pueden ser utilizados por dicho emisor utilizando RTCP.

La correlación simple de dos *streams* es sólo parte del problema de sincronización intermedia. Como, además, diferentes *streams* pueden tener también relojes diferentes (con diferentes estados de tiempo y aún diferentes grados de inexactitud) existe la necesidad de definir una forma de sincronizar *streams* exactamente entre ellos. RTCP maneja este problema

Hay 5 tipos de mensajes de control.

- *Sender Report* (Reporte del Emisor o remitente) es enviado por el emisor y además de contener información similar a los mensajes RR, incorpora datos sobre sincronización, paquetes acumulados y número de bytes enviados. La información extra en un reporte de emisor consta de:

  - Un *timestamp* que contiene el tiempo real del día, cuando el reporte fue generado.

  - Un *timestamp* RTP correspondiente al momento en que el reporte fue generado.

  - Un acumulado de los paquetes y bytes enviados por ese emisor desde que comenzó la transmisión.

- *Receiver Report* (Reporte del Receptor) Es enviado por los receptores y contiene información sobre la calidad de la entrega de datos, incluyendo último número de paquete recibido, número de paquetes perdidos y timestamps para calcular el retardo entre el emisor y el receptor.
- *Source Description* (Descripción de la fuente). contiene información que describe al emisor.
- *Bye*. Indica la finalización de la participación en una sesión.

- *Application-specific* (Aplicación en específico) Por ahora es experimental. Está reservado para aplicaciones futuras.

Los paquetes **RTCP** son enviados como un paquete compuesto que contiene al menos dos paquetes, un paquete de reporte y un paquete de descripción de la fuente. Todos los participantes en una sesión envían a **RTCP** los paquetes. Un participante que recientemente ha enviado paquetes de datos emite un reporte del remitente. El reporte del remitente (**SR**) contiene que el número total de paquetes y bytes enviados así como también la información que puede usarse para sincronizar media *streams* de sesiones diferentes.

Los participantes de sesión periódicamente emiten reportes de receptor para todo las fuentes de las cuales esta recibiendo paquetes de datos. Un reporte de receptor (**RR**) contiene información acerca del número de paquetes perdidos, el número de secuencia más alto que recibió, y un timestamp que puede usarse para estimar el retraso de ida y vuelta entre un emisor y el receptor.

El primero de los paquetes compuestos de **RTCP** tiene que ser de reporte, aun si ninguno de los datos ha sido enviado o recibido en cuyo caso, un reporte vacío de receptor es enviado. Todos los paquetes compuestos **RTCP** deben incluir un elemento de descripción de la fuente (**SDES**) que contiene el nombre canónico (**CNAME**) que identifica la fuente.

La información adicional podría ser incluida en la descripción de la fuente, algo como el nombre, la dirección de correo electrónico, el número de teléfono, localización geográfica, nombre de aplicación, o un mensaje describiendo el estado actual. Cuando una fuente ya no es activa, envía a un **RTCP** paquete BYE. El aviso BYE puede incluir la razón que la fuente deja la sesión.

Los paquetes de **RTCP** proveen un mecanismo para aplicaciones para definir y enviar documentación personalizada por el puerto de control **RTP**. A través de estos paquetes, **RTCP** proporciona los siguientes servicios:

- ***Monitorización de la Calidad de Servicio (QoS) y congestión de red***. La fusión Primaria de **RTCP** es proporcionar realimentación a una aplicación sobre la calidad de la distribución. Esta información le es útil a los Emisores, a los receptores y a otras terceras partes interesadas (monitoreo de aplicación). El Emisor puede ajustar su transmisión basándose en estos informes. El receptor puede determinar si la

congestión de la red local, regional o global. Los gestores de red pueden evaluar el rendimiento de la red para la distribución Multicast.

- ***Identificador de Fuentes***. Las fuentes de datos se identifican en los paquetes RTP con identificadores de 32 Bit generados aleatoriamente. Estos Identificadores no son apropiados para usuarios humanos. Los paquetes **RTCP SDES** (descripción de Fuente) contienen identificadores únicos globales (nombre Canónicos) e información textual, como el nombre de los participantes, el numero de teléfono, la dirección de e-mail, etc.

- ***Sincronización Intermedia***. **RTCP** envía informes con información de tiempo real que corresponde a una determinada marca temporal **RTC**. Esa información puede ser utilizada para la sincronización de fuentes de datos que procedan de distintas sesiones **RTP**.

- ***Escalonada de la información de control***. Los paquetes **RTCP** se envían periódicamente entre los participantes. Cuando el número de participantes aumenta, se hace necesario establecer un compromiso. Entre la obtención de la información actualizada y la sobrecarga por trafico de la red, Para escalar el trafico de grupos multicast grandes, **RTCP** a delimitado de control procedente de los recursos de la red a los que mas se accede. **RTP** limita el trafico de control al 5% del trafico total

de la sesión, esto se refuerza a justando el trafico **RTCP** a un régimen acorde al numero de Participantes.

- El protocolo **RSVP** (*Resourse Reservation Protocol*) es el protocolo de control de red que permite al receptor de datos solicitar una determinada calidad de servicio. Las aplicaciones en tiempo real usan el **RSVP** para reservar los recursos necesarios en los Routers a lo largo de los caminos de transmisión, de tal manera que el ancho de banda requerido este disponible cuando la transmisión tenga lugar. RSVP es el principal componente de los servicios integrados por Internet, puede proporcionar tantos servicios en tiempo real (garantiza una calidad) como servicios *Best - effort* (Se hace lo que se puede).

CAPITULO 4

ALTERNATIVA DE TRASNPORTE

En este capitulo se describen diferentes protocolos de transportes junto con sus características, entre los cuales encontramos el Protocolo de Control de Transmisión (TCP), UDP(User Datagram Protocol) , Protocolo de tiempo Real (RTP), SCTP (**S**imple **C**ontrol **T**ransmission **P**rotocol).

4.0 ALTERNATIVA DE TRANSPORTE

Se manejan diferentes protocolos TCP que es orientado a conexión, es fiable; UDP: Este protocolo es no orientado a la conexión, y por lo tanto no proporciona ningún tipo de control de errores ni de flujo; RTP: es un protocolo de transporte adaptadas a aplicaciones que transmitan datos en tiempo real, como audio, vídeo o dato de simulación, sobre servicios de red multicast o unicast; SCTP : es un protocolo de transporte fiable, diseñado para trabajar sobre redes de paquetes no orientadas a conexión, como IP

4.1 TCP: El protocolo TCP (Transmission Control Protocol, protocolo de control de transmisión) está basado en IP que es no fiable y no orientado a conexión, y sin embargo es orientado a conexión; Es necesario establecer una conexión previa entre los dos computadores antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

Es un protocolo fiable La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un [5] circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los puntos intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logré la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffer. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

[5] www.monografias.com.circuitosvirtules/#
Información sobre circuitos virtuales.

El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

4.2. UDP: Este protocolo es no orientado a la conexión, y por lo tanto no proporciona ningún tipo de control de errores ni de flujo, aunque si que utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama en lugar de entregarlo a la aplicación se descarta.

Este protocolo se ha definido teniendo en cuenta que el protocolo del nivel inferior (el protocolo IP) también es no orientado a la conexión y puede ser interesante tener un protocolo de transporte que explote estas características. Como el protocolo es no orientado a la conexión cada datagrama UDP existe independientemente del resto de datagramas UDP.

El protocolo UDP es muy sencillo y tiene utilidad para las aplicaciones que requieren pocos retardos o para ser utilizado en sistemas sencillos que no pueden implementar el protocolo TCP.

Las características del protocolo UDP son:

- ✓ No garantiza la fiabilidad. No podemos asegurar que cada datagrama UDP transmitido llegue a su destino. Es un protocolo del tipo best-effort porque hace lo que puede para transmitir los datagramas hacia la aplicación pero no puede garantizar que la aplicación los reciban.

- ✓ No preserva la secuencia de la información que proporciona la aplicación. La información se puede recibir desordenada (como ocurría en IP) y la aplicación debe estar preparada por si se pierden datagramas, llegan con retardo o llegan desordenados.

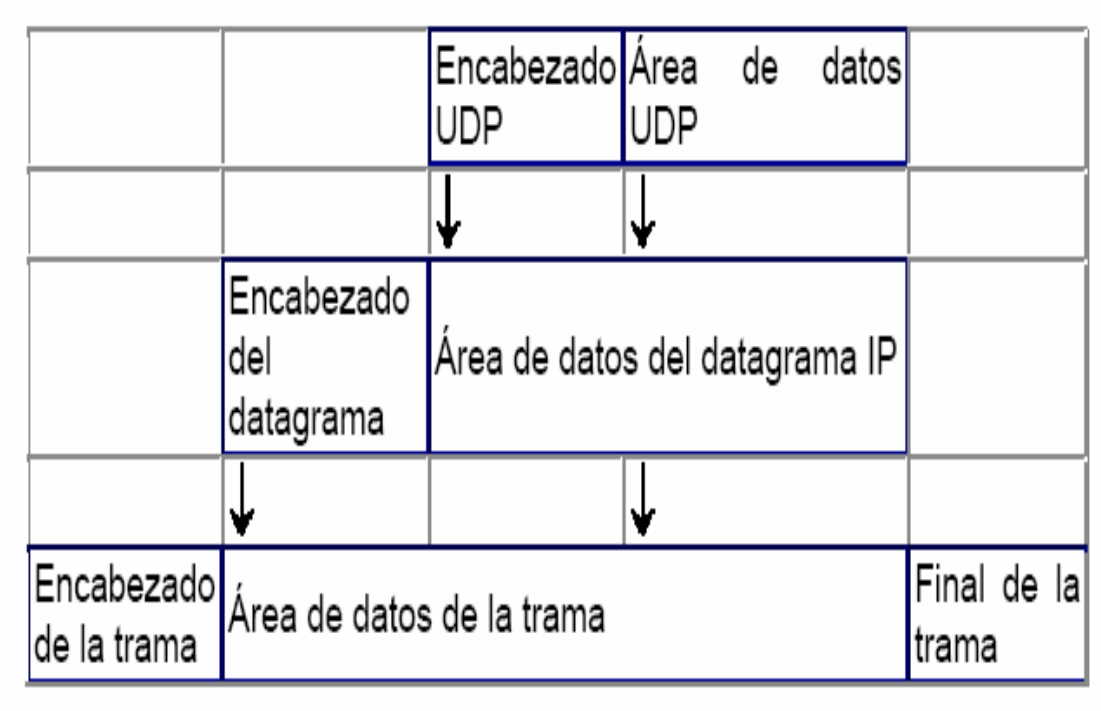


FIGURA 10. FORMATO DEL MENSAJE UDP

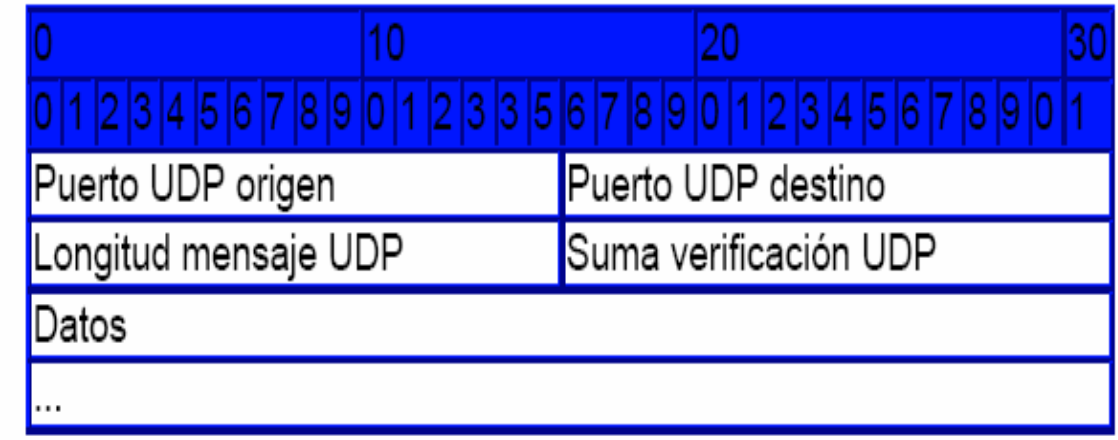


FIGURA 11. PUERTOS DE UDP

En la figura anterior se muestra los diferentes puertos de UDP Utilizados para el envío de mensaje.

Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.

Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.

Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.

Suma de verificación UDP (16 bits, opcional): Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.

Datos: Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

4.3. RTP: proporciona funciones de transporte adaptadas a aplicaciones que transmitan datos en tiempo real, como audio, vídeo o dato de simulación, sobre servicios de red *multicast* o *unicast*. RTP no implementa reserva de recursos ni servicio de garantía de control de calidad.

Las aplicaciones normalmente ejecutan RTP encima de UDP para hacer uso de su servicio de multiplexación y gestión de errores. RTP soporta la transferencia de datos a múltiples destinos usando la distribución *multicast* sólo si lo proporcionan los niveles inferiores.

RTP por si mismo no proporciona ningún mecanismo para asegurar el tiempo de entrega o proporcionar garantía de calidad de servicio. RTP como se ha indicado antes está formado por dos partes estrechamente relacionadas:

· El protocolo RTP que se encarga de transporta los datos con características en tiempo real.

El protocolo de control RTP (RTCP) que supervisa la calidad del servicio y gestiona la información acerca de los participantes en una sesión.

El objetivo de RTP es que sea maleable y proporcionar la información requerida por una aplicación particular y normalmente será integrada dentro de la aplicación en vez de constituir un nivel separado. La intención de RTP es que sea adaptado a través de las modificaciones y/o adiciones de las cabeceras necesarias.

4.4. SCTP *(**S**imple **C**ontrol **T**ransmission **P**rotocol*): es un protocolo de transporte fiable, diseñado para trabajar sobre redes de paquetes no orientadas a conexión, como IP. El Protocolo de transmisión de control de flujo (**SCTP**) es una nueva y robusta tecnología de transmisión de señales para las comunicaciones inalámbricas. Diseñado por el grupo de trabajo [6] **IETF SIGTRAN, el SCTP** es el sucesor del protocolo de señalización **SS7**. La robustez del SCTP nace de su capacidad de mantener varios flujos de datos en una misma conexión. Esto hace que el **SCTP** sea ideal para la conexión y monitoreo de teléfonos celulares y dispositivos de Internet inalámbricos. Con el **SCTP**, se pueden monitorear activamente las conexiones y rutas de señales, y pueden detectarse instantáneamente las interrupciones o pérdidas de las sesiones.

[6] www.ietf.com
Pagina Oficial IETF.

CAPITULO 5

APLICACIONES DE RTP

Encontramos diferentes aplicaciones de audio, video, audio – video, que se manejan con el protocolo RTP, entre otras que día tras días surgen y van tomando importancia dentro del mundo de la multimedia.

5.0 APLICACIONES RTP

Encontramos múltiples aplicaciones del Protocolo en Tiempo Real (RTP) como el MBONE, las aplicaciones de audio: (VAT, RAT, FREE PHONE), las aplicaciones de video: (*VIC*, NV, IVS), entre otras.

5.1. MBONE (IP MULTICAST BACKBONE)

MBone (*IP **M**ulticast Back**bone***) es una red virtual a nivel mundial que utiliza la técnica multicast y cuyo principal uso es la transmisión de vídeo y audio de forma óptima sobre Internet. La mayoría de las aplicaciones **MBone** están basadas en el protocolo **RTP**. Debido a que la comunicación es multicast permite el envío de uno a muchos paquetes de información, optimizando la carga que reciben las estaciones transmisora y receptoras así como el ancho de banda entre los enlaces que las unen. De esta manera son habituales las transmisiones de conferencias desde cualquier punto conectado al troncal y donde desde el equipo que se utiliza para recibir la transmisión se puede intervenir, si se desea, en el turno de preguntas, o bien mantener sesiones interactivas entre varios participantes.

Dentro del amplio banco de aplicaciones que han aparecido en estos últimos años (gran parte de ellas continúan en desarrollo), las que más éxito han tenido en **MBone** han sido las que permiten la realización de conferencias de audio y vídeo. Dentro de este grupo el **vat** y el **rat** son las más empleadas para la

transmisión / recepción de audio, y el **vic** para la transmisión / recepción de vídeo.

5.1.1. CARACTERÍSTICAS TÉCNICAS

Internet es una red en la que el intercambio de información entre estaciones locales o remotas se hace a través de datagramas IP. Un datagrama IP podríamos decir que es la unidad mínima de información en el lenguaje que hablan todos los equipos que forman parte de Internet. Estos datagramas IP están formados principalmente por una dirección origen y una dirección destino, y cada equipo de comunicaciones situado en la ruta entre ambos se encarga de enviar dicho datagrama por el camino adecuado. La base del MBone es IP multicast, Cuando un equipo envía un datagrama IP a una determinada dirección IP multicast, sólo es recibida por aquellos equipos que están a la escucha de esa dirección y, que por tanto, son capaces de entender las direcciones multicast. Aunque en los comienzos del MBone, pocas computadoras eran capaces de entender dichas direcciones, ya que se requerían ciertas modificaciones en el sistema operativo de los mismos, desde hace bastante tiempo prácticamente todos los computadores modernos pueden 'hablar' IP multicast.

Las direcciones IP multicast, que todo equipo conectado a MBone debe saber reconocer (a parte de otros detalles técnicos que están fuera de los objetivos de este artículo), son de la forma:

224.xxx.xxx.xxx

De todas las [6] direcciones IP multicast posibles con el formato anterior, algunas están reservadas para uso interno por equipos de comunicaciones que intercambian información sobre multicast, otras para uso local dentro de Intranet, y las comprendidas en el rango:

224.2.0.0.0 - 239.255.255.255

Son las que forman el conjunto de direcciones IP multicast usadas en el MBone para las conferencias multimedia. Dentro de este rango hay ciertas direcciones reservadas para los anuncios de sesiones MBone y ciertos rangos reservados para conferencias de ámbito local, institucional o parcialmente restringido.

Para que los Routers que interconectan las múltiples redes que forman el Internet puedan transmitir la información multicast es necesario que sepan distribuir los datagramas IP multicast con el mismo protocolo de encaminamiento multicast. Cuando un router esta cualificado para intercambiar datagramas IP multicast con otro u otros, decimos que es un router multicast, o abreviadamente un **mrouter** y que viene a ser la pieza elemental con la que se construye MBone.

[6] GARCIA TOMAS, Jesús, RAYA, Víctor Rodrigo. Alta Velocidad y Calidad de Servicios en Redes IP. Editorial Alfaomega. 2002. Direcciones IP

El primer protocolo de router multicast que ha sido implementado, y que ha dado lugar al surgimiento de MBone, ha sido el llamado [7] DVMRP (Distance Vector Routing Protocol). Los Routers multicast saben intercambiar información, siguiendo este protocolo, con otros Routers multicast similares a través de **túneles** definidos por los administradores de los mismos. Estos túneles encapsulan los datagramas IP multicast en otros datagramas IP unicast que son enviados por los caminos habituales y a través de Routers convencionales, desde el mrouter origen al destino. En el destino, se extraen los datagramas multicast y se inyectan en la red local. De esta forma se consigue distribuir el tráfico multicast a través del Internet. La interconexión de estos mrouters de fácil instalación ha ido incrementándose con el paso del tiempo, dando lugar al entramado de Routers multicast que forman el MBone.

Desde la aparición del primer protocolo de encaminamiento multicast, se han realizado grandes esfuerzos (coordinados por el IETF), para definir otros protocolos más sencillos, o de más fácil integración dentro de los protocolos de encaminamiento operativos en Internet. Uno de estos, el PIM (Protocol Independent Multicast), ha tenido bastante éxito dada su mayor simplicidad de funcionamiento y es por el que ha apostado uno de los fabricantes de routers con mayor presencia en Internet. Esto ha hecho que se haya ido implantando cada vez con mas fuerza frente a su antecesor (pero aún mayoritario) DVRMP.

En cuanto a las garantías de transmisión del tráfico multicast, se están desarrollando nuevas especificaciones que permiten garantizar la correcta

[7] http://www.ipinfusion.com/pdf/ZOS_DVMRP.pdf#search=%22dvmrp(distance%20vector%20routing%20protocol)%22
Protocolo DVMRP

difusión del mismo, y asegurar una calidad de servicio, detalle este fundamental para convertir lo que ha sido una red experimental en un servicio operativo totalmente integrado como una característica más de Internet. Estas especificaciones son por ejemplo el protocolo RTP (Real Time Protocol) que permite el intercambio de información en tiempo real, muy apropiado para el uso de MBone. Otras como el RSVP (Resource Reservation Protocol), permiten a los equipos implicados reservar temporalmente los recursos telemáticos necesarios requeridos por las aplicaciones durante el transcurso, por ejemplo, de una videoconferencia. Si todos los equipos intermedios entre el emisor y el(los) receptor(es) de una determinada transmisión multimedia hablan este protocolo RSVP, es posible que la estación emisora solicite unos recursos telemáticos necesarios durante la duración de dicho evento, de forma que, independientemente del estado de congestión de la red, exista una garantía de mantenimiento de estos recursos solicitados.

5.2 APLICACIONES DE AUDIO

Dentro de las aplicaciones de audio encontramos: VAT (Visual Audio Tool), RAT (Robust-Audio Tool), Free Phone,

5.2.1. VAT (Visual Audio Tool)

Es una herramienta de audio desarrollada por el *Network Research Group* del [8] **LBNL** (*Lawrence Berkeley National Laboratory*), es una aplicación multimedia a tiempo real para audioconferencias sobre Internet. El **VAT** está basado en el estándar de Internet **RTP**, desarrollado por el grupo de trabajo *Audio/Vídeo Transport* de la **IETF**. El **RTP** es un protocolo implementado completamente dentro del **VAT** (no se necesita mejorar el sistema para utilizar **RTP**).

El **VAT** puede funcionar en una comunicación punto a punto usando direcciones IP *unicast*, pero en un principio se diseñó para aprovechar las ventajas de IP *multicast*. Para usar multicast, el sistema ha de soportar *IP Multicast* y la red debe estar conectada a *Mbone*.

5.2.2. *RAT (Robust-Audio Tool)*

Es una herramienta que proporciona audio para telé conferencias en Internet. Está diseñado para ser robusto a la pérdida de paquetes y se adapta a las condiciones de la red. La señal de audio es tomada por el **RAT** y se codifica de manera comprimida. El flujo continuo de datos resultante se inserta en

[8] www.monografia.com./lbnl.pdf
Multimedia a tiempo Real LBNL

mente los paquetes son transmitidos secuencialmente hacia su destino utilizando *multicast*.

Los paquetes que son enviados a través de **Mbone** pueden no seguir siempre el mismo camino. Esto permite al sistema ajustarse a situaciones de congestión o errores en la red. Sin embargo, esto provoca que los paquetes no lleguen con una *rata* constante. Además los paquetes pueden perderse en la red o llegar fuera de secuencia. La aplicación **RAT** posee funcionalidades para solucionar la pérdida y la llegada desordenada de paquetes. Cuando se pierden paquetes en la red el receptor puede solucionar este problema, reemplazándolos antes de reproducir el audio utilizando alguna de las siguientes opciones:

- Silencio: **RAT** no hace nada y se mantiene en silencio cuando se pierden paquetes.
- Repetición: **RAT** reemplaza el paquete perdido con un duplicado del anterior.
- Cada paquete de audio contiene un poco de redundancia. Cuando un paquete es transmitido una representación muy comprimida de sus datos son colocados en la parte redundante del siguiente paquete. Por consiguiente, si se pierde un paquete hay bastantes probabilidades que el siguiente paquete contenga algo de los datos perdidos. De esta manera se puede reemplazar el paquete perdido. La representación

comprimida proporciona una calidad de audio más pobre que el paquete original.

A veces los paquetes desordenados pueden ser recuperados si el receptor retarda la reproducción del audio: la aplicación **RAT** permite la llegada de paquetes fuera de secuencia y entonces repara el flujo de audio. Incrementando el retardo en la reproducción se puede mejorar la calidad, pero esto sólo es factible en los casos en que el flujo de datos va en una sola dirección.

5.2.3. Free Phone

Es una aplicación de audio que maneja sesiones unicast múltiple y sesiones del multicast. Así no hay necesidad de tener varios casos de la herramienta que funciona simultáneamente.

Incluye la ayuda para las tarifas del muestreo que se extienden a partir del 8 a 48 Khz. Las altas tarifas del muestreo tales como 44 Khz y 48 Khz corresponden audio de la calidad del CD y de DAT, respectivamente.

Tiene como características más importantes:

1. Manipula múltiples sesiones unicast y multicast.
2. Implementa **RTP**.
3. Incluye un protocolo de señalización para contactar con participantes remotos.

4. Permite soportar una *rata* de 8 a 48 kHz.
5. Incluye un mecanismo de redundancia para la reconstrucción de paquetes.
6. Soporta el mecanismo de redundancia y la manipulación de los diferentes *ratas* usando los tipos especiales de *payload* RTP.
7. Incluye los codecs más utilizados: PCMU, GSM.
8. Es compatible con otras herramientas Mbone (RAT, VAT).

FIGURA 12. FREE PHONE

En la figura 11, se muestra un formato de la aplicación Free Phone., los diferentes iconos que aparecen son las funciones que este posee.

5.3 APLICACIONES DE VIDEO

Dentro de las aplicaciones de video encontramos el VIC (Video Conferencing Tool, NV (Network Video), IVS (INRIA Videoconferencing System),

5.3.1 *VIC* (Video Conferencing Tool)

Es una aplicación multimedia a tiempo real para conferencias de vídeo sobre Internet. El **VIC** ha sido diseñado con una arquitectura flexible y extensible para soportar diferentes entornos y configuraciones. Por ejemplo, en entornos de gran ancho de banda se puede originar un flujo **JPEG** usando compresión por hardware, mientras que en entornos de poco ancho de banda, como por ejemplo Internet, la codificación a baja velocidad se pueda hacer por software.
El **VIC** se basa en el estándar de Internet **RTP** (*Real-time Transport Protocol*) desarrollado por el grupo de trabajo *Audio/Video Transport* de la **IETF. El RTP** es un protocolo implementado completamente dentro del **VIC** (no se necesita mejorar el sistema para utilizar **RTP**). El **VIC** puede funcionar en una comunicación punto a punto usando direcciones IP *unicast*, pero en un principio se diseñó para aprovechar las ventajas de IP multicast. Para usar *multicast*, el sistema ha de soportar *IP Multicast* y la red debe estar conectada a **MBone**.

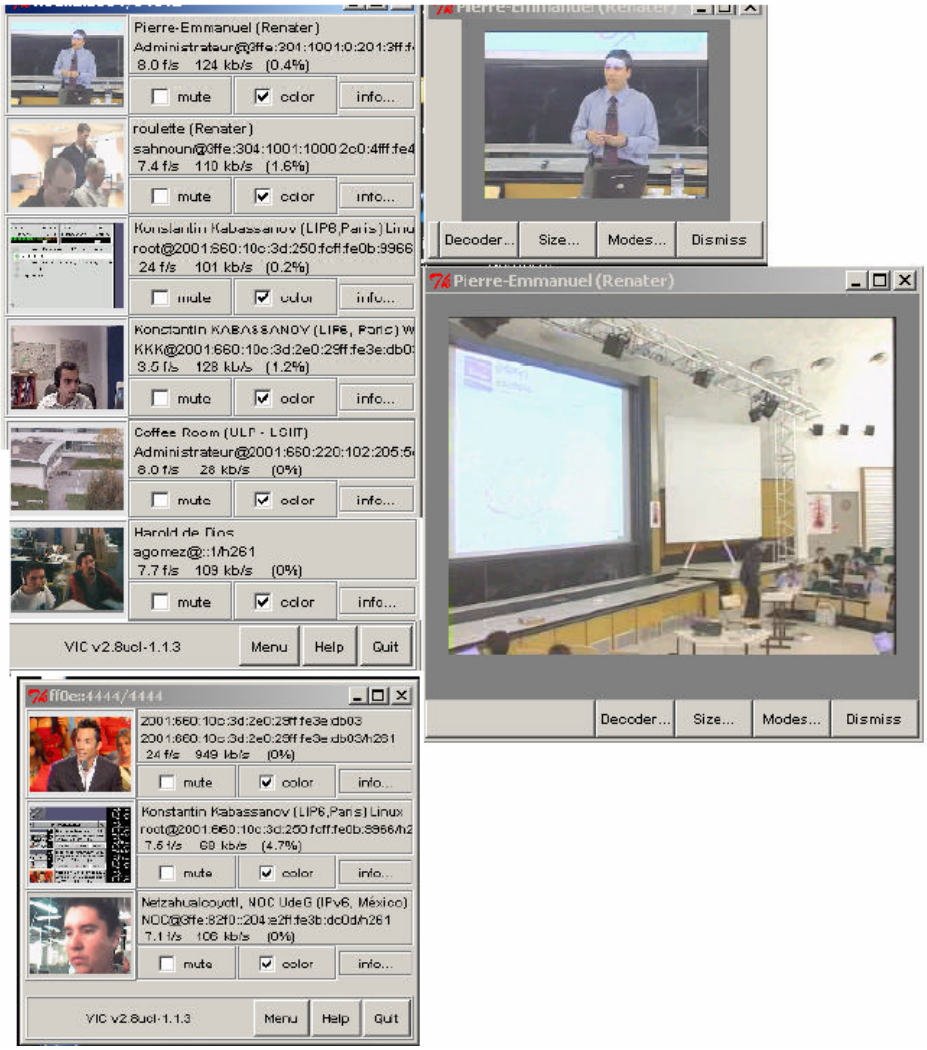


FIGURA 13. VIC (MULTIMEDIA VIDEO TOOL)

En la figura anterior se muestra la ventana de la aplicación VIC, la cual con sus diferentes iconos muestra las funciones que realiza.

5.3.2 NV (Network Video)

Permite al usuario transmitir y recibir vídeo de baja velocidad vía UDP/IP a través de Internet. El flujo de vídeo puede ser enviado usando una conexión punto a punto, o puede ser enviado a varios destinos a la vez a través de IP multicast. Los receptores no necesitan un hardware especial, sólo un X *display.*

Los emisores necesitan algún tipo de tarjeta de captura de Vídeo.

En la mayoría de los aspectos el VIC ha dejado obsoleto el NV, excepto en la posibilidad que tiene el NV de enviar vídeo de la pantalla de usuario, mientras que el VIC sólo puede enviar vídeo de un dispositivo externo (por ejemplo, una vídeo cámara).

5.3.3 IVS (INRIA Videoconferencing System)

IVS es una de las primeras herramientas de videoconferencia para Internet (la primera versión estuvo disponible en 1992). IVS permite transmitir audio y vídeo sobre Internet a partir de [9] workstations. Incluye los codecs de audio PCM y ADPCM, y el codec de vídeo H.261. Gracias a que son codecs de software pocas actualizaciones de hardware hacen falta en las maquinas implicadas, sólo una cámara de vídeo y una tarjeta capturadora de vídeo.

[9] Es una estación de trabajo en la cual se realiza el proceso de comunicación.

[10] Los codecs hardware H.261 requieren líneas dedicadas o circuitos conmutados para la transmisión de datos, mientras que los codecs software H.261 de IVS utiliza datagramas UDP. Son necesarios algunos cambios para utilizar esta última codificación sobre redes de conmutación de paquetes como por ejemplo Internet. El esquema de empaquetado del vídeo H.261 utiliza RTP.

IVS también incluye un control de errores para solucionar la pérdida de paquetes en Internet. Incluye una realimentación sobre la tasa (“ *rate*”) el cual adapta la imagen al proceso de codificación, así como el “*rate”* de salida del codificador, dependiendo de las condiciones de la red.

5.3.4 Rendez-Vous

Aplicación con RTP, que permite enviar vía multicast un archivo MPEG a todos los participantes; el MPEG se codifica a H.261 de manera que se puede recibir el vídeo utilizando Rendez-Vous o el VIC.

[10] TANENBAUM, Andrés. Redes de Computadoras. Editorial Prentice Hall.

Los Codecs

5.4 APLICACIONES DIRECTORIO DE SESIONES

Dentro de las aplicaciones de directorio de sesiones encontramos SDR, Multikit, Pizarra Electrónica.

5.4.1 SDR (*Session Directory Tool*)

Directorio de sesiones **MBone**, nos permite conocer las sesiones que están activas en todo momento, conectarnos a cualquiera de ellas, o definir nuestra propia sesión **MBone**. **SDR** es una aplicación Directorio de Sesiones diseñada para anunciar y planificar conferencias multimedia sobre **Mbone**. **SDR** fue implementado a partir de la aplicación **sd** (*Mbone Session Directory* de **LBL**). **SDR** es una extensión del modelo **sd**, añadiendo nuevas funcionalidades como por ejemplo más información sobre los recursos requeridos por una conferencia y, además, proporciona un interfaz más flexible para conocer las sesiones existentes.

La aplicación **SDR** dispone de un protocolo para anunciar las sesiones de llamado **SDAP** (*Session Directory Announcement Protocol*), Mediante este protocolo se utiliza *IP multicast* para enviar un paquete que describe una sesión. Los receptores simplemente escuchan una dirección multicast conocida y un puerto. Las sesiones se describen utilizando el protocolo **SDP** (*Session Description Protocol*). Cuando se recibe un paquete que anuncia una sesión éste simplemente es un mensaje SDP, y entonces la aplicación **SDR** puede mostrar la información de la sesión al usuario.

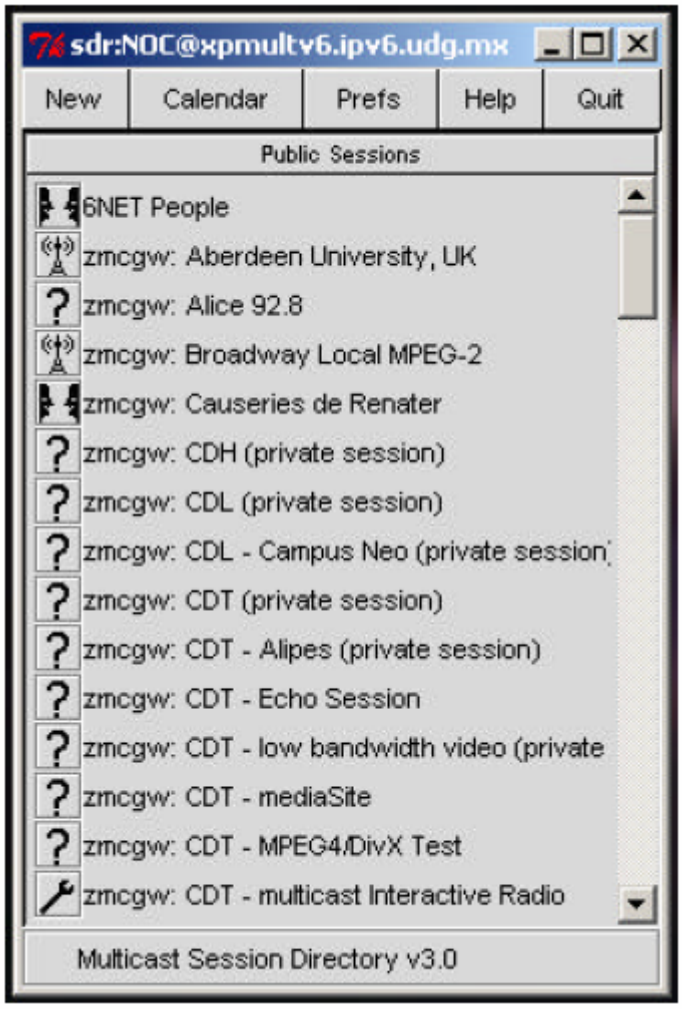


FIGURA 14. SDR (SESSION DIRECTORY TOOL)

Las principales funcionalidades se Muestran en la grafica y se explican a continuación:

- Crear nuevas sesiones o unirse a alguna de las existentes.
- Puede limitarse el alcance del tráfico que anuncia la sesión (*TTL scope* y *administrative scope*).

- Mostrar al usuario el ancho de banda total de la conferencia y el usado por cada Aplicación de la conferencia.
- Anunciar sesiones de manera segura, es decir, anunciar sesiones de manera Privada.
- Cuatro modos para ver las sesiones una vez recibidos los anuncios de éstas (*All Sessions, Prefered Sessions, Current Sessions, Future Sessions*). Opción calendario para ver las sesiones existentes.

5.4.2 Multikit

Multikit es un *browser*-directorio distribuido, que muestra uno o más “directorios multicast” que contienen anuncios que se reciben mediante IP multicast a través de Mbone. Estos anuncios describen eventos multimedia, como pueden ser conferencias, conciertos u otro tipo de datos. Para descifrar los anuncios que se reciben se usa, como en el caso del SDR, el protocolo SDP.

Usando multikit un usuario puede obtener información de eventos multimedia, como por ejemplo donde tienen o tendrán lugar. El usuario puede participar en los eventos. Si lo hace se ejecuta entonces la aplicación multimedia correspondiente (de audio, de vídeo,...). Multikit permite también al usuario crear sus propios anuncios, y crear u organizar sus propios directorios.

5.4.3 Pizarra Electrónica

Es una aplicación que nos proporciona el acceso a una pizarra en la que disponemos de una serie de utilidades tanto para escribir textos con varios tamaños y formas, así como para realizar dibujos a mano alzada y formas geométricas sencillas. Cualquier diseño que creemos en esta pizarra virtual, será automáticamente visto por todos los participantes en la sesión, y cualquiera podrá hacer modificaciones sobre dichas imágenes. También tenemos la posibilidad de incorporar archivos en formato PostScript en la pizarra.

5.4.3.1 Digital Lecture Borrad

Básicamente es una pizarra electrónica mejorada adaptada a las necesidades de la tele-enseñanza síncrona. Diferentes medios de comunicación se integran en un sencillo interfaz de usuario. La Digital Lecture Board proporciona flexibilidad para el uso de los medios de comunicación, da soporte al trabajo en grupo, y puede ser integrada en un entorno de enseñanza y soportar la mayoría de los requerimientos de tele-enseñanza síncronos (construcción, transmisión, grabación, reproducción, y preparación de conferencias y materiales de enseñanza).

5.5 EDITORES DE TEXTO

Dentro de los editores de texto encontramos: **NT (*Network Text*)** que es un editor de texto compartido diseñado para funcionar sobre Mbone. No es un procesador de texto (no está claro que compartir un procesador de texto sea una tarea útil) y tampoco una whiteboard. Mediante Nt puede haber mucha interactividad a menos que alguien intencionadamente bloquee una parte del texto; entonces nadie más en la sesión puede editarlo o borrarlo. Varias personas pueden, si lo desean, editar simultáneamente un documento. Varias personas pueden incluso editar el mismo bloque de texto simultáneamente, pero si más de una persona intenta editar la misma línea a la vez hay conflicto, y sólo se mantiene uno de los cambios que se puedan dar.

Nt intenta que no haya confusiones en el usuario por culpa de actuaciones inesperadas de otros participantes, pero muchas veces a causa de las condiciones de la red puede suceder que un cambio llegue con mucho retardo. Si esto sucede, Nt intentará dar un resultado consistente, pero puede que no sea el esperado. A causa de todo esto se recomienda el uso de la aplicación Nt como parte de una conferencia multimedia como herramienta de apoyo, y no usarla como único canal de comunicación.

5.6 GRABACIÓN - REPRODUCCIÓN DE SESIONES MBONE

La aplicación MVoD (Mbone Vídeo Conference Recording on Demand) ofrece una solución para la grabación y reproducción interactiva remota de videoconferencias multicast. MVoD ofrece un entorno para que un usuario pueda interactivamente grabar conferencias de audio/vídeo sobre un servidor remoto, todo esto controlado mediante una aplicación cliente local, y más tarde el mismo usuario o otros usuarios pueden reproducir la sesión bajo demanda utilizando IP unicast o multicast.

Por otra parte se esta implementando la red M6bone que es un servicio que esta para realizar implementaciones con Ipv6 Multicast a sitios y entidades que se muestren interesadas al respecto. Este servicio esta basado en el piloto de IPv6 de Renater (Reseau Nacional de Telecommunications pour la Technologie l'Enseignement et la Recherche) que en conjunto con la asociación Aristote se involucra en la difusión de nuevas tecnologías con G6 (Grupo de IPv6 testers, Francia). El principal objetivo es desarrollar avanzados servicios en IPv6, con el propósito de participar en la promoción del protocolo. Esto habilita el uso de herramientas de videoconferencia Multicast en la red como son las de mbone (sdr,vic,rat,nte,wbd).

5.7 M6bone

En la siguiente imagen se muestra como funciona la red de **M6bone**.

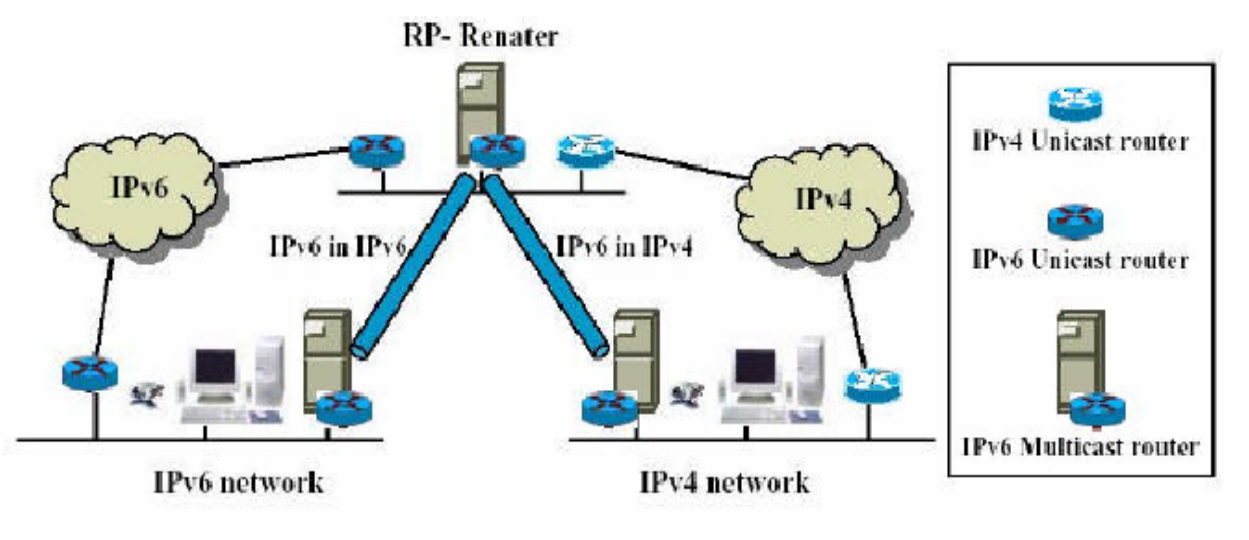


FIGURA 15. FUNCIONAMIENTO DE M6BONE

Aquí podemos apreciar que el RP (Rendevous-Point) funciona como equipo principal el cual hace la distribución de los anuncios por medio de RIPng, cada sitio que está conectado debe hacerlo a través de VPNs (Tuneles), estos túneles pueden ser establecidos por dos maneras, las cuales son:

- Para sitios en los cuales exista una conectividad IPv6, el túnel estaría establecido en IPv6 Multicast en un túnel IPv6 unicast.

Para sitios que solo cuentan con conexión IPv4, el túnel estaría establecido en IPv6 Multicast en un túnel IPv4.

5.8 INTEGRACIÓN HERRAMIENTAS MBONE: MINT, MASH

Habitualmente en Mbone los controladores de las conferencias sólo permiten la combinación de los diferentes medios de comunicación, Lo que hacen estos controladores (por ejemplo, el SDR) es simplemente arrancar el proceso y pasarle unos parámetros.

Cuando una conferencia ha empezado una comunicación funciona por si mismo ignorando el resto de medios de comunicaciones. Para ciertas aplicaciones sería deseable un control mayor:

1. Un *floor control* (aplicación que se utiliza para negociar quien utiliza la comunicación en una conferencia) ha de saber cuando una conferencia empieza, acaba, o cuando los participantes salen o entran.

2. Aplicaciones de playback y recorders han de detectar el speaker y así tener la posibilidad de sólo grabar ciertos emisores.

3. Ciertas aplicaciones quizá quieran comunicarse con otras sesiones y entonces, por ejemplo, reducir el tamaño de la imagen del vídeo cuando otra conferencia empieza.

De todo esto nace la idea de integrar diferentes aplicaciones de Mbone en una sola, creando una especie de proceso intermedio que comunique diversos medios de comunicaciones a diversas aplicaciones Mbone.

5.9. MInT (Multimedia Internet Terminal)

MInT es un conjunto de herramientas multimedia, flexible, que permite establecer y controlar sesiones multimedia en Internet. La arquitectura de esta aplicación es distribuida, sin ningún componente central. MInT ofrece las siguientes posibilidades:

1. Transmisión y recepción de audio con calidad [11] GSM hasta calidad CD a partir de las herramientas NEVOT y VAT.
2. Transmisión y recepción de vídeo basándose en el VIC.
3. Un controlador de conferencia integrado que oculta la complejidad individual de cada herramienta que integra el MInT.
4. *Floor Control*: Aplicación usada para negociar quien utiliza la comunicación en una conferencia. Las conferencias con grandes retardos y bajo *rate* en el vídeo, cuando un conferenciante acaba de hablar, la tendencia natural de todos los participantes es entrar a hablar todos a la vez, provocando un exceso de utilización del ancho de banda. Utilizando esta aplicación se evita este problema.
5. Sistema de “votación” basado en el MPOLL: Herramienta proporcionada por el CRC. MPoll es una aplicación para hacer polling (encuestas) a tiempo real y capta información sobre el rate de los participantes. Usa

[11] http://es.wikipedia.org/wiki/GSM, GSM

multicast para distribuir las preguntas y respuestas a todos los participantes.

6. Interfaz al SDR.
7. Posibilidades de usar RSVP para todas las aplicaciones.
8. Transmisión adaptativa de vídeo.
9. Poder ver colectivamente y remotamente documentos postcript.
10. Invitación a usuarios remotos a una conferencia basándose en el SIP (*Session Initiation Protocol*).

Para integrar las aplicaciones del MInT se ha implementado un protocolo de comunicaciones llamado PMM (*Pattern Matching Multicast*). Utilizando este protocolo varios medios pueden comunicarse entre ellos.

El PMM no es más que un bus o proceso intermedio que replica mensajes: le llega un mensaje y es reenviado a través de algún mecanismo IPC de UNIX. Concretamente, la función del PMM es escuchar un puerto TCP esperando conexiones.

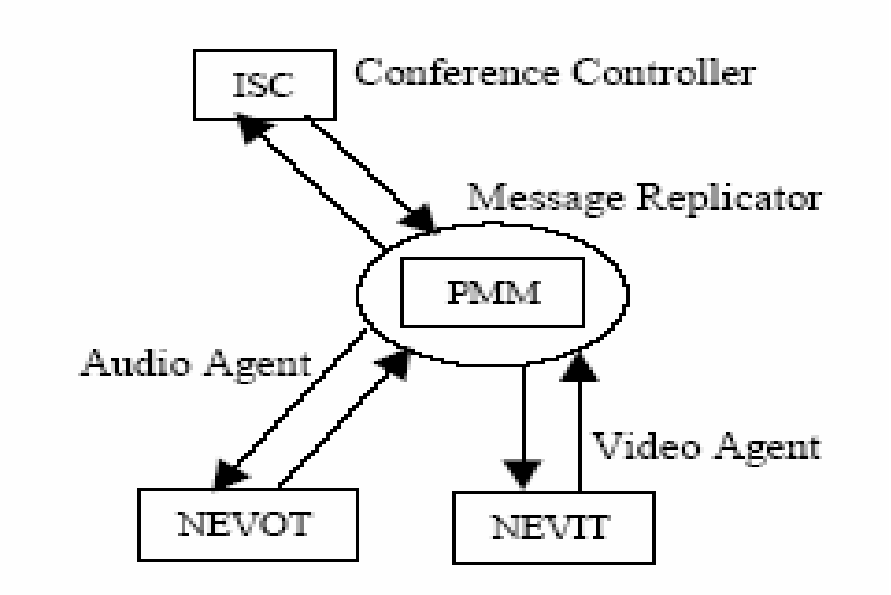


FIGURA 16 PARTE DEL MINT CON PMM.

La figura anterior muestra un esquema de cómo es el funcionamiento de PMM.

5.10 MASH

El proyecto MASH se ha centrado sobretodo en integrar un conjunto de aplicaciones dentro de lo que se llama el “MASH shell” o simplemente “mash”. Mash utiliza un *split programming model*, donde las complejas tareas de programación multimedia son descompuestas en simples objetos que son enlazados juntos y configurados por un lenguaje de script como es Tcl. Está formado por aplicaciones ya existentes (como el VAT y el VIC, pero ahora son un Tcl script que es interpretado por el mash, intérprete Tcl), y nuevas aplicaciones (como por ejemplo el MediaBoard).

Las aplicaciones que integra el Mash actualmente son las siguientes:

1. RSDR: Es el SDR de LBL/UCB modificado para permitir ser empezadas las grabaciones desde una lista SDR de sesiones.

2. VIC, VAT: Modificadas para funcionar integradas en el Mash.

3. MediaBoard: Pizarra electrónica. Es una aplicación distribuida, interactiva, que proporciona un espacio de trabajo compartido para participantes remotos. El MediaBoard permite, después de una sesión, que el contenido de la pizarra sea grabado. También soporta una reproducción síncrona de la secuencia de eventos dibujados, así los participantes podrán buscar cosas sobre la conferencia una vez esta haya terminado. Utiliza el protocolo SRM (no estándar), que le proporciona transporte seguro.

SRM (*Scalable, Reliable Multicast*): Algunas aplicaciones requieren el transporte multicast seguro. Tradicionalmente para hacer el transporte seguro se usaba un complejo y monolítico nivel entre la aplicación y la red: se tenía que aplicar un protocolo específico y esto era una limitación ya que existe un amplio rango de aplicaciones con diferentes requerimientos de seguridad. SRM tiene la posibilidad de especializarse a una aplicación de acuerdo con sus necesidades. MediaBoard ha sido la principal aplicación para la especialización de SRM.

1. Recorder: Aplicación para la grabación de sesiones. Toma como entrada direcciones de sesiones donde escuchar, y la localización y/o nombres de archivos accesibles vía NFS de los cuales pueden almacenar datos.

2. Player: Aplicación para reproducir sesiones grabadas. Toma como entradas la localización de los ficheros de datos y las direcciones de sesión sobre las cuales reproducir los datos. El interfaz del Player proporciona un acceso aleatorio por multi-sesiones.

Dentro del proyecto MASH también se desarrollan otras actividades, todas Relacionadas con lo anterior:

1. SCUBA (*Scalable, ConseUs-based Bandwidth Allocation*): Mecanismo para compartir ancho de banda en tiempo real en multimedia a partir del interés de los receptores. Se usa un algoritmo distribuido para establecer un consenso entre todos los participantes de una conferencia para el ancho de banda de una sesión; se usa un mecanismo de votación para establecer este consenso.

2. MeGa: Arquitectura para la transmisión multimedia en redes heterogéneas, para el despliegue de los llamados *media gateways*. Esta arquitectura confía a un protocolo "*soft state"* que facilite la robustez y

flexibilidad. El control del ancho de banda de los [12]gateways se realiza mediante el protocolo SCUBA.

Gran parte de las aplicaciones aquí enumeradas están disponibles para casi cualquier plataforma informática: desde un simple PC con Windows95, hasta una estación de trabajo con UNIX (en casi cualquiera de sus variantes), lo cual ha contribuido a la popularidad de las mismas. De este modo cualquier PC multimedia básico, es decir, que disponga de una tarjeta de audio y un micrófono, nos permitirá convertirnos en un nodo receptor de MBone y asistir a cualquiera de las videoconferencias que se emiten, o intervenir en aquellas en las que se permita la participación remota.

5.11 ORENETA

Oreneta es una plataforma para el análisis de red en tiempo real. El objetivo para el desarrollo de esta herramienta es la obtención de una utilidad capaz de visualizar en tiempo real medidas de calidad del servicio (QoS) de los flujos que circulan en una red, en concreto el retardo extremo a extremo y sus variaciones, que es especialmente importante en aplicaciones interactivas y en tiempo real. Se pretende facilitar a los administradores de la red la comparación de diferentes políticas de gestión para evaluarlas al instante y de forma visual, sin modificar el contenido de lo que se examina.

[12] TANENBAUM, Andrés. Redes de Computadoras. Editorial Prentice Hall.

Gateway

5.11.1 Arquitectura

ORENETA trabaja capturando el tráfico de la red en dos puntos distintos mediante dos sondas. Las sondas capturan el tráfico en modo pasivo, minimizando la interferencia con el tráfico analizado. Esto permite el análisis de tráfico 'real' aportando un valor agregado sobre las medidas de tráfico generado. Aun así es posible el análisis de tráfico generado mediante el uso de otras utilidades. Las capturas de tráfico son preprocesadas en las sondas y enviadas a un analizador. Éste es el elemento que hace los cálculos de las medidas con los datos obtenidos de las sondas y ofrece la interacción con el u

suario. El analizador desglosa las medidas obtenidas en flujos unidireccionales, lo que permite observar de forma clara los parámetros y comportamiento de cada uno de ellos. Esto a su vez permite la caracterización del tráfico. El control de las sondas se realiza desde el analizador. El sistema funciona según la arquitectura cliente/servidor, siendo el cliente el analizador y las sondas los servidores.

Esta herramienta hace especial énfasis en el cálculo de medidas en un sentido, como el "one-way delay", "ip delay variation" o "one-way packet loss" , propuestas por el grupo de trabajo IP Performance Metrics. Las medidas en un sentido no se pueden deducir de las medidas "round-trip", ya que la composición de las redes de comunicaciones, y sobretodo con QoS, puede hacer que tenga diferentes comportamientos en cada uno de los sentidos de la

comunicación. Mediante estos parámetros se puede saber con mayor precisión de qué forma se comporta la red y evaluar el impacto de diferentes políticas de QoS.

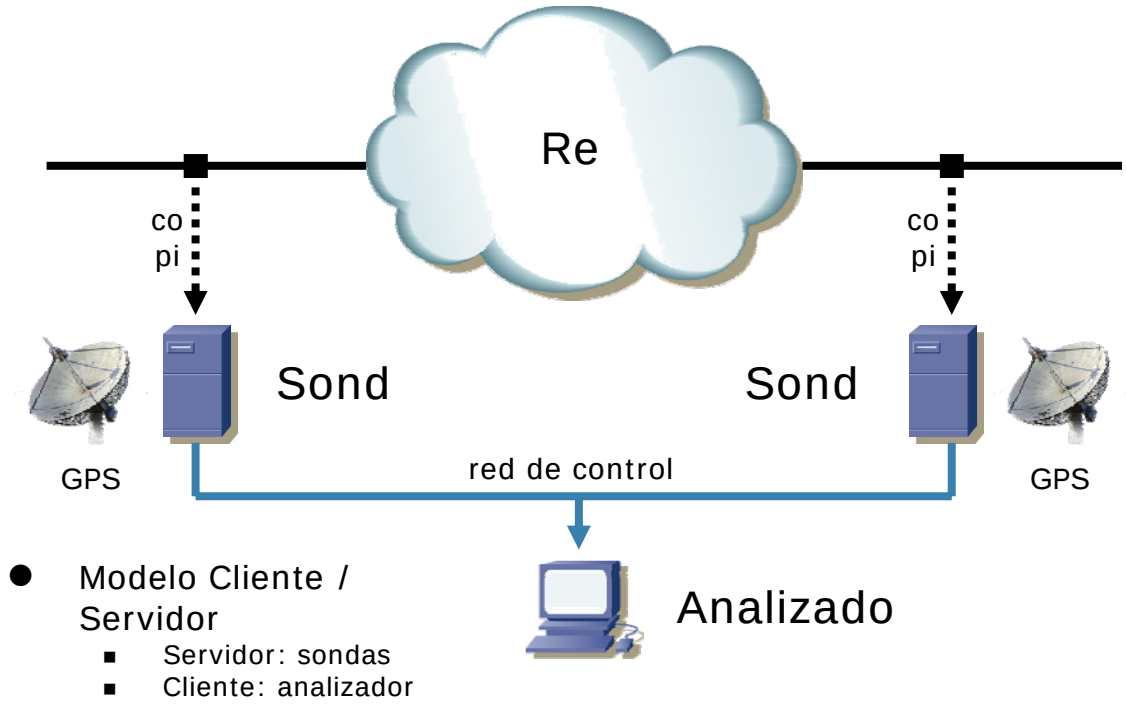


FIGURA 17. ONE-WAY DELAY

5.11.2 Sincronización de las sondas

Para el cálculo de los valores en un sentido se necesita que las sondas estén sincronizadas entre sí. ORENETA se basa en la utilización del protocolo NTP como método de sincronización. Este protocolo no es suficiente cuando las distancias, en tiempo, son cortas entre las sondas, dado que no obtiene una gran precisión. En estos casos se hace necesaria una fuente de sincronización externa, como GPS, para dotar a la plataforma de la máxima precisión. Aun así, la herramienta permite la comparación de otras medidas, como el rendimiento, sin que ambas sondas estén sincronizadas. Existen dos momentos donde se puede realizar la marca de tiempo en un paquete IP:

- *Wire - Time*. Se marcar el paquete en el momento que es visto por la tarjeta de red. Esto se consigue con hardware específico para realizar esta tarea a un costo muy elevado.
- *U s e r - T i m e. L*os paquetes se marcan en el *User- Time*, es decir, el sistema operativo subyacente es el que realiza la marca, introduciendo cierta variabilidad en las medidas, que en la práctica resulta prácticamente despreciable por ser varios órdenes de magnitud inferior a los valores de las medidas.

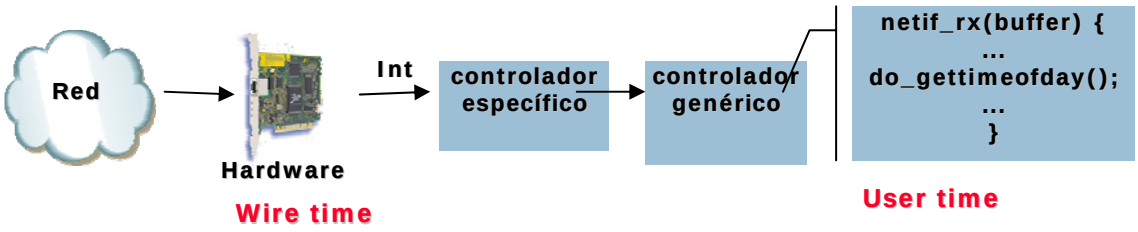


FIGURA 18. MARCA DE TIEMPO

5.11.3 Captura pasiva

El hecho de capturar el tráfico de forma pasiva dificulta la tarea de identificar los paquetes de un flujo. En un sistema de medidas activas cada paquete se marca con un identificador generado artificialmente, mientras que en uno de capturas pasiva este identificador no existe. No se puede depender del campo "identificador" de las cabeceras IPv4 por dos motivos: es susceptible de alteración por motivos de seguridad y además no aparece en el protocolo IPv6. ORENETA implementa un sistema para generar un identificador a partir de los campos invariables de las cabeceras IP así como 40 octetos de los datos. Este identificador es generado mediante la función CRC-32, creando un identificador de 4 octetos que junto a las direcciones, puertos y marcas de tiempo configuran toda la información que se envía al analizador por cada paquete. Así, por cada paquete IPv4 se envían al analizador 28 octetos de datos por paquete y 42 octetos en el caso de IPv6, siempre de forma independiente al tamaño del paquete IP. ORENETA es capaz de analizar flujos de datos IPv4 e IPv6, sin

observarse ninguna diferencia en el rendimiento obtenido entre las dos versiones. De forma automática, cuando un flujo es visto en cada una de las sondas se reconoce como un flujo común, visualizándose como tal y empezando a almacenar de forma automática los cálculos de tráfico asociados. Estos datos se almacenan durante 300 segundos

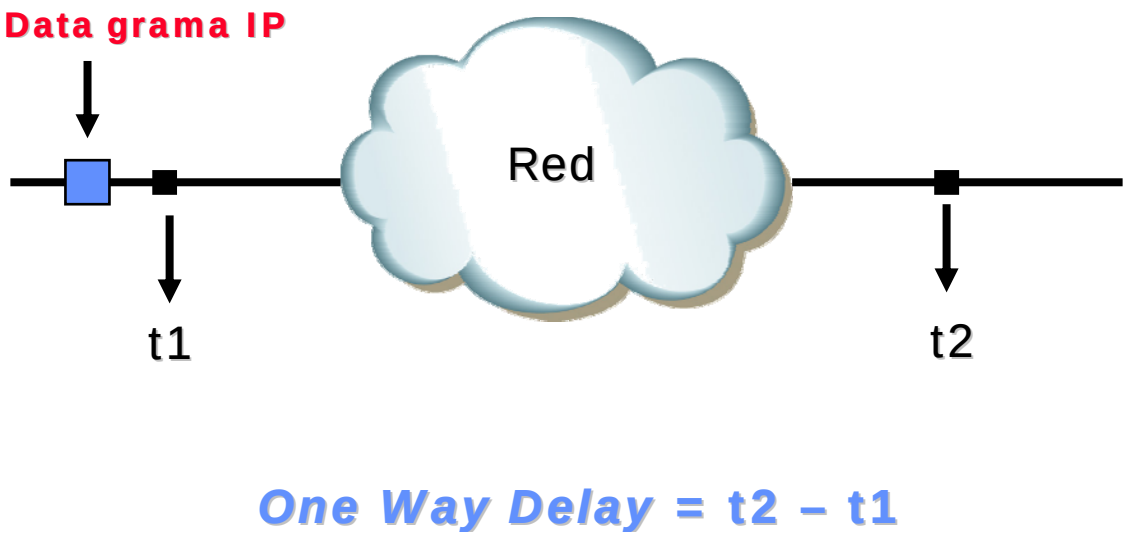


FIGURA 19. FLUJO DE DATOS

5.11.4 Filtrado

El tráfico que capturan las sondas puede ser de muy diversa índole. ORENETA permite el filtrado del tráfico no deseado. Dado que las sondas utilizan la librería libpcap, utilizan su sistema de filtros. Esto filtros se especifican mediante cadenas de texto que siguen la sintaxis de otros programas basados en esta librería, como **tcpdump o ethereal** y se aplican desde el analizador. La utilización de filtros permite no sólo una mejor claridad en la representación,

sino que además reduce el cálculo necesario y por lo tanto mejora su eficiencia.

5.11.5 REPRESENTACIÓN DE LOS FLUJOS

Toda esta información se presenta en tiempo real en el analizador. Mediante gráficas dinámicas auto escalables donde se pueden ver los cambios en un flujo, comparar flujos activos entre sí o incluso comparar flujos activos con otros que se hayan almacenado previamente. Se puede entonces comparar las posibles diferencias existentes entre flujos analizados en diferentes horarios o en otros escenarios.

5.11.6 HARDWARE/SOFTWARE

No se ha utilizado hardware específico para la captura del tráfico en las sondas, bastan unas simples tarjetas de red Ethernet, aunque ORENETA puede funcionar con otro tipo de tecnologías de red, como ATM y Wireless. De igual forma, los ordenadores utilizados no tienen ningún requerimiento especial. Para las pruebas se han utilizado Pentium III Celeron 600 en las sondas y un Pentium IV 2.4 para el analizador. Con estos equipos se puede conseguir una capacidad de análisis superior a los 25 Mbps. Teniendo en cuenta que un vídeo con calidad DVD-MPEG2 trabaja a 10 Mbps, queda patente su efectividad en el

análisis de flujos individuales de tráfico multimedia. Las sondas se han desarrollado en C bajo Linux, funcionando en la mayoría de distribuciones actuales. El analizador está implementado en Java y se ha probado en varias plataformas con éxito.

CONCLUSIONES

- Protocolo de Tiempo Real (RTP) ha sido incorporado en las aplicaciones sin necesidad de implementarse en un nivel separado y junto con el protocolo de control de tiempo real (RTCP) nos proporcionan envíos de paquete con monitoreo de Calidad de Servicio (QoS), para que el emisor pueda ajustar su transmisión. Los participantes se envían paquetes RTCP para informar fundamentalmente sobre la calidad de la recepción de paquete en una aplicación de multimedia.

- La aparición de equipos PC con capacidad suficiente para realizar todo el procesado multimedia, mediante software ha permitido que las aplicaciones, solo el hecho de incrementar la frecuencia y capacidades de los procesadores genéricos permiten realizar estas operaciones.

- El diseño de RTP le hace ser aplicable tanto en entornos unicast como multicast, lo que en la práctica requiere que todos los mecanismos contemplados por el protocolo sean escalables. RTP proporciona, entre otras, funciones de identificación de tipos de contenido y de fuentes de sincronización, reordenación de la secuencia de unidades de datos, detección de pérdidas, seguridad e identificación de participantes y contenidos.

- Recomendamos trabajar en la realización de la práctica del manejo de calidad de servicio en redes inalámbricas (Frottle), que se muestra como una experiencia muy importante dentro de las comunicaciones.

- Recomendamos trabajar sobre el protocolo UDP LITE, DCCP (Datagram Congestión Control Protocol), que son protocolos que están en vía de crecimiento y que son de transporte.

- Recomendamos investigar sobre el protocolo PPTP es un protocolo desarrollado para el acceso a redes privadas virtuales (**VPN**). Este protocolo se emplea en situaciones en las que los usuarios de una red privada corporativa precisan de un acceso a la red privada desde un lugar remoto.

BIBLIOGRAFIA

- GARCIA TOMAS, Jesús, RAYA, Víctor Rodrigo. Alta Velocidad y Calidad de Servicios en Redes IP. Editorial Alfaomega. 2002. Pagina 350 – 405.

  Conceptos generales de redes IP, calidad de servicio (QoS), Calidad de servicios redes IP.

- STALLING, William. Organización y Arquitectura de Computadores. Editorial Prentice Hall. Quinta Edición. 2000. Paginas 220 – 340.

Redes de computadores, protocolos de transporte.

- TANENBAUM, Andrés. Redes de Computadoras. Editorial Prentice Hall. Cuarta Edición. 2003.

  Los Codecs, Normas de comunicaciones.

- LEON GARCIA, Alberto, WIDJAJA, Indra. Redes de Comunicaciones. Editorial Mc Graw Hill. 2002

  Protocolo RTP, sistemas orientados y no a conexión.

- UILESS, Black. Tecnologías Emergentes para redes de Computadoras. Editorial Pearson Educación. Segunda Edición. 1997.

Encontramos información general acerca de todos los protocolos de Transporte, además de las tecnologías que estan surgiendo en el mundo de la multimedia.

- Audio-Video Transport Working Group. RTP: A Transport Protocol for Real-Time Applications. RFC 1889, 1997.

- Network Research Group. VAT – LBNL Audio Conferencing Tool. http://www-nrg.ee.lbl.gov/vat, 1998.

Sitios WEB

www.monografias.com

http://www.sunrisetelecom.com/espanol/frame

http://www.m6bone.net/

http://netweb.usc.edu/pim/

http://imasd.elmundo.es/imasd/ipv6/queesipv6.html

http://www.rediris.es/rediris/boletin/65/enfoque1.pdf

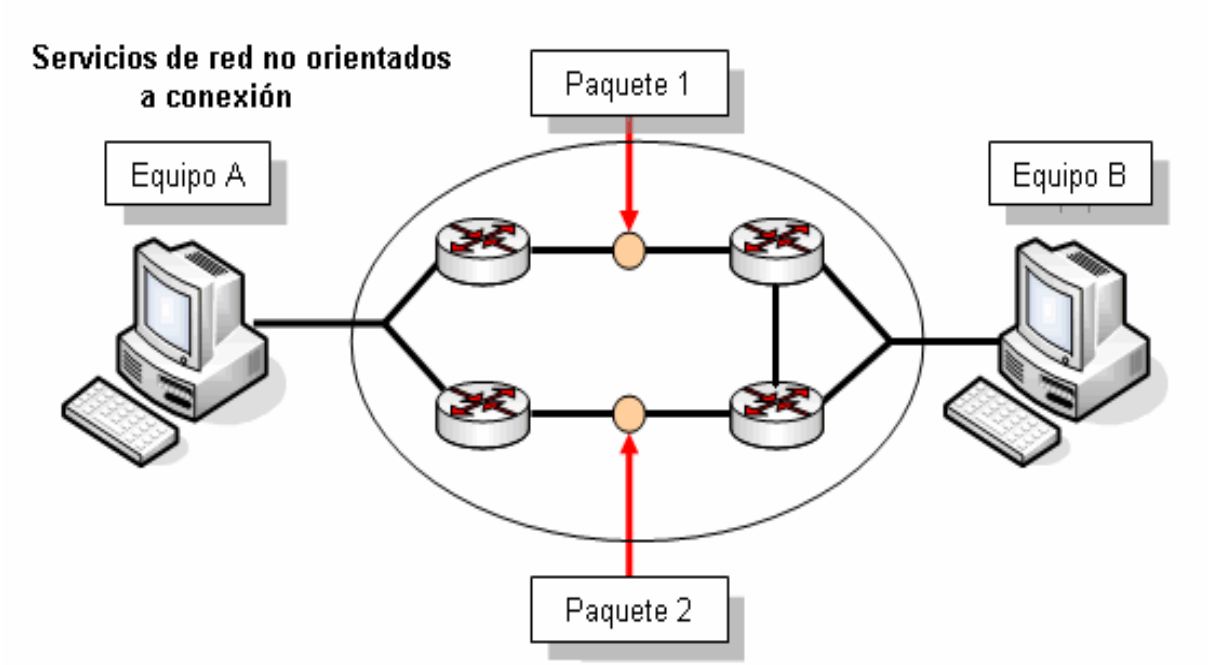
ANEXOS

En los anexos tenemos un concepto muy utilizado dentro de nuestro trabajo que es sistemas orientados o no a conexión, luego presentamos la arquitectura general de los sistemas multimedia del IETF y finalmente una tabla que compara diferentes protocolos.

ANEXO 1

SERVICIOS DE RED ORIENTADOS O NO A CONEXIÓN

La mayoría de los servicios de red usan un sistema de entrega no orientado a conexión. Estos servicios manejan cada paquete por separado y lo envían a través de la red. Los paquetes pueden tomar distintas rutas para atravesar la red, pero se vuelven a ensamblar cuando llegan a su destino. En un sistema no orientado a conexión, no se hace contacto con el destino antes de que se envíe el paquete. Una buena analogía para un sistema de entrega no orientado a conexión es el sistema de correos. No se hace contacto con el destinatario antes de que la carta se envíe desde un destino a otro. La carta se envía hacia su destino y el destinatario se entera de su existencia cuando la recibe. Suponemos (Correos mediante) que la carta llega a su destino.



Servicios de red orientados a conexión

En los sistemas orientados a conexión, se establece una conexión entre emisor y receptor antes de que se transfieran los datos. Un ejemplo de una red orientada a conexión es el sistema telefónico. Se hace una llamada, se establece una conexión y luego se produce la comunicación.

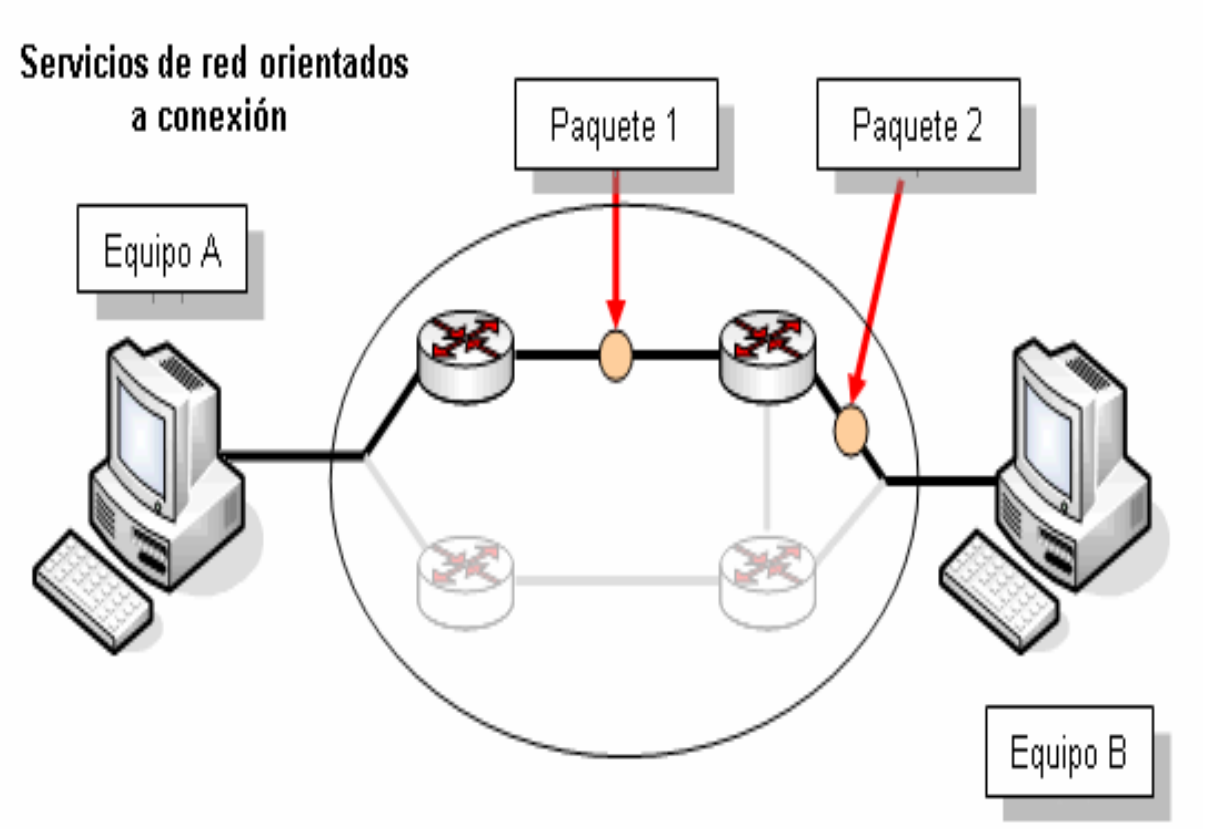
Comparación de los procesos de red no orientados a conexión y orientados a conexión

Los procesos de redes no orientados a conexión se definen como conmutados por paquetes. En estos procesos, a medida que los paquetes se transportan desde el origen hasta el destino, se pueden pasar a distintas rutas, así como también (posiblemente) llegar fuera del orden correcto. Los dispositivos

realizan la determinación de ruta para cada paquete basándose en diversos criterios. Algunos de los criterios como, por ejemplo, el ancho de banda disponible, puede variar de un paquete a otro.

Los procesos de red orientados a conexión a menudo se denominan conmutados por circuito. Estos procesos establecen en primer lugar una conexión con el receptor y luego comienza la transferencia de datos. Todos los paquetes se transportan de forma secuencial a través del mismo circuito físico, o más comúnmente, a través del mismo circuito virtual.

Internet es una enorme red no orientada a conexión en la cual la entrega de paquetes es manejada por IP. TCP (Capa 4) agrega servicios orientados a conexión en la parte superior de IP (Capa 3). Los segmentos TCP se encapsulan en paquetes IP para ser transportados a través de Internet. TCP proporciona servicios orientados a conexión para permitir una entrega fiable de los datos.


Servicios de red orientados a conexión
Paquete 1
Paquete 2
Equipo A
Equipo B

ANEXO 3

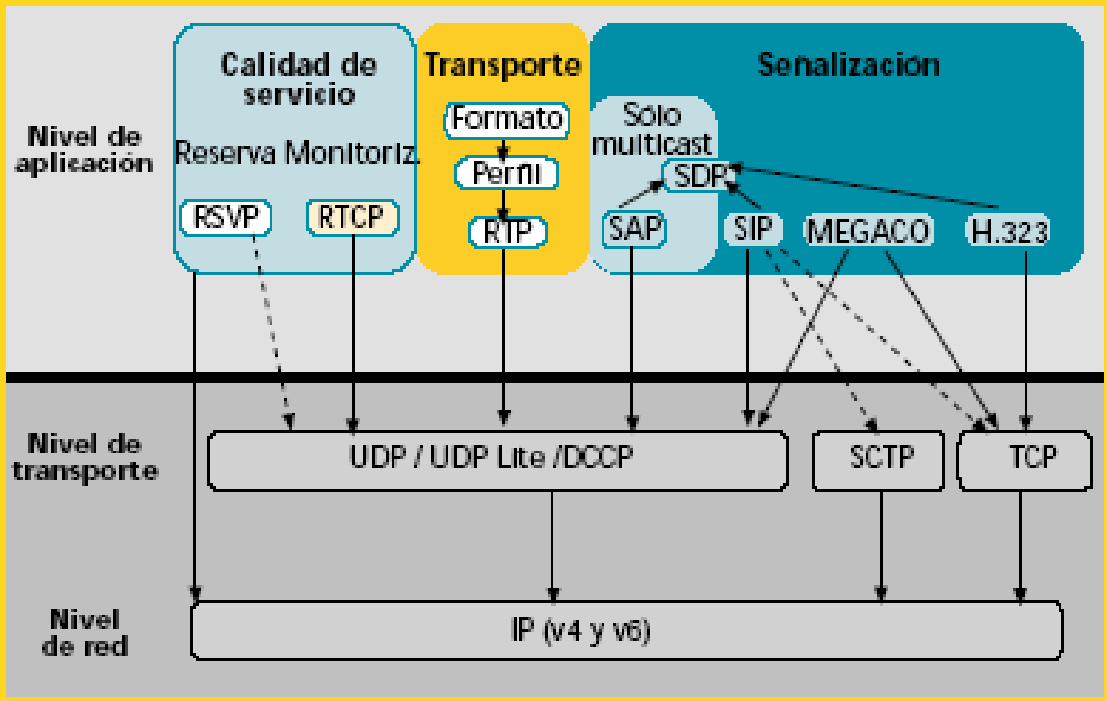
ARQUITECTURA GENERAL DE LOS SISTEMAS MULTIMEDIA DEL IETF

El modelo desarrollado por el IETF para los sistemas de comunicación multimedia en tiempo real se ha diseñado para sesiones multimedia con múltiples participantes en las que se utilizan diversos medios y formatos de datos intercambiados mediante redes y equipamiento heterogéneos. Se caracteriza por ser abierto, flexible, modular, escalable y adaptable a la diversidad de Internet.

Desde que comenzó su desarrollo, con los primeros protocolos y aplicaciones experimentales de conferencia multimedia en Internet (aplicaciones de Mbone), se ha ido formando un conjunto sólido de protocolos de transporte y señalización en tiempo real que ya permite la realización de aplicaciones
y dispositivos como los teléfonos IP basados en SIP. La arquitectura de sesiones multimedia del IETF [3,4, 14, 8], a diferencia de la arquitectura H.323, está constituida por un amplio conjunto de protocolos independientes e intercambiables, cada uno de los cuales cumple funciones complementarias.
En la figura se presentan los protocolos de mayor importancia en esta arquitectura, que engloba dos protocolos de *señalización de nivel de aplicación* definidos por el IETF: SIP [18, 7] y SAP [6]. SIP cumple las funciones de establecimiento de sesiones por invitación, así como de modificación y finalización. SAP es un protocolo de *anuncio de sesiones* desarrollado para

entornos multicast. El protocolo MEGACO, desarrollado por el IETF y estandarizado por la ITU-T en la recomendación H.248, especifica los procedimientos de control de las pasarelas o sistemas de interconexión de redes de diferentes tipos, en particular entre redes de conmutación de paquetes y redes de conmutación de circuitos. En general, el formato de descripción de sesiones multimedia utilizado es SDP.

FIGURA 1: ARQUITECTURA DE SISTEMAS MULTIMEDIA DEL IETF



En la figura aparece H.323 entre los protocolos de señalización, puesto que puede sustituir a SIP en las funciones de señalización, del mismo modo que es

posible interconectar zonas de la red que utilizan SIP con zonas que utilizan H.323.

Las funciones de *garantía de calidad de servicio*, ya sea mediante reserva de recursos o mediante servicios integrados o diferenciados, quedan delegadas en otros protocolos, preferentemente RSVP y Diff-Serv, y se pueden articular siguiendo arquitecturas como MPLS. Asimismo, el protocolo de *transporte en tiempo real* preferente es RTP, protocolo de nivel de aplicación que engloba al Protocolo de control de la transmisión RTCP. RTP, desarrollado por el IETF ha sido adoptado por la ITU-T para su recomendación H.323.

Todos los protocolos de nivel de aplicación comentados son independientes del protocolo de transporte subyacente. En la práctica, las aplicaciones basadas en RTP utilizan UDP como protocolo de nivel de transporte de datos. No obstante, se trata de una solución incompleta que no satisface los requisitos de control de congestión de flujos RTP, por lo que actualmente se desarrollan diversos Protocolos de transporte con los que se pretende superar ésta y otras limitaciones de UDP y TCP.

Algunos de estos nuevos protocolos se muestran en la figura, Asimismo, la experiencia ha puesto de manifiesto las limitaciones de UDP como protocolo de Transporte de los mensajes SIP, al tiempo que TCP no es una solución adecuada a sistemas de tiempo real. A corto plazo, la alternativa más sólida como protocolo de transporte base para SIP es SCTP.

A grandes rasgos, las funciones realizadas por los componentes expuestos quedan completadas con los siguientes servicios:

• *Servicios de directori*o, delegados en el protocolo LDAP [20].

• *Autenticación, autorización y contabilida*d, para los cuales las soluciones del IETF más consolidadas actualmente son los protocolos RADIUS [2] y DIAMETER.

• *Búsqueda de pasarelas* entre zonas con diferentes protocolos de señalización, proporcionados por el protocolo TRIP [9], válido para sistemas basados en SIP y H.323.