Práctica 1: Vídeoconferencia y vídeo streaming en unicast

(Versión Septiembre de 2011)

Autor: Rogelio Montañana

1.- Introducción y objetivos

En esta práctica se realizan pruebas con diversas herramientas de videoconferencia y vídeo streaming en modo unicast, con el objeto de que el alumno se familiarice con su funcionamiento.

Para el desarrollo de la práctica se utilizan ordenadores con sistema operativo MS Windows XP que deben tener instalados los siguientes paquetes de software:

- El programa **Wireshark** que se utiliza como analizador de tráfico. Este software es de dominio público y se puede obtener de www.wireshark.org.
- El programa **Netmeeting** de Microsoft. Es un software de videoconferencia H.323 (unicast) que viene incluido con el sistema operativo MS Windows en sus diversas variantes.
- El programa **VideoLAN**, que sirve para enviar y recibir emisiones de vídeo en IP. Es un software de libre distribución que puede funcionar en unicast y en multicast y que se puede obtener de www.videolan.org

Algunos ordenadores están dotados de cámara de vídeo (Webcam), micrófono y auriculares, otros solo tienen micrófono y auriculares.

2.- Preparación

En primer lugar los alumnos deben organizarse para trabajar en equipos de dos o tres personas. Cada equipo utilizará una maqueta formada por dos ordenadores, al menos uno de los cuales debe tener cámara, auriculares y micrófono. El otro ordenador puede tener solo auriculares y micrófono.

Después arrancarán los ordenadores en el sistema operativo Windows XP y entrarán con el usuario y la password que indique el profesor.

A continuación conectarán la cámara de vídeo a una de las tomas USB del ordenador. Del mismo modo conectaremos el micrófono y los auriculares en sus respectivas entradas. Deben utilizarse las tomas traseras de la caja del ordenador tanto para conectar la cámara de vídeo como los auriculares y micrófono. Los ordenadores que no dispongan de cámara no podrán realizar la emisión de vídeo, pero sí la recepción. Los que no dispongan de micrófono no podrán realizar la emisión de audio.

Ahora los alumnos deben averiguar los siguientes datos de sus ordenadores:

Dato	**Ordenador 1**	**Ordenador 2**
Nombre		
Dirección MAC		
Dirección IP		
Máscara		
Router por defecto		

Pare ello seleccionarán con el ratón el icono **'Inicio'** en la parte inferior izquierda de la pantalla y en el menú desplegable seleccionarán **'Ejecutar…'**. En el campo **'Abrir'** teclearán **`'cmd'`** y en la ventana que aparece teclearán el comando **`'ipconfig/all'`**. De la respuesta a dicho comando obtendrán todos los datos requeridos excepto el nombre. Para averiguar el nombre utilizarán el comando '**`nslookup`** ***`dirección_IP`***' donde '***`dirección_IP`***' será la dirección IP que han averiguado previamente.

Por último desactivarán el cortafuegos (de Windows) que esté instalado en el ordenador.

Nota: si en algún momento de la práctica se producen comportamientos extraños en algún equipo, o los resultados de alguna prueba no son los esperados, se deben revisar detenidamente todas las opciones y pasos realizados. Si a pesar de eso la prueba sigue sin funcionar puede ser conveniente reiniciar el equipo y repetir el proceso a partir de ese punto.

3.- Pruebas de videoconferencia con Microsoft Netmeeting

El programa Netmeeting de Microsoft es un software de videoconferencia que funciona en los sistemas operativos Windows que cumple con los estándares H.323 de la ITU-T. Para ponerlo en marcha simplemente haremos doble clic sobre el icono correspondiente, que debe estar en el escritorio. En caso de que no encontremos el icono seleccionaremos con el ratón el icono **'Inicio'** en la parte inferior izquierda de la pantalla, en el menú desplegable seleccionaremos **'Ejecutar…'** y en .el campo **'Abrir'** teclearemos **`'conf'`**, abreviatura de 'conference', que es el nombre que recibe el ejecutable del programa Netmeeting. De esta forma ejecutamos el proceso de configuración del Netmeeting, como resultado del cual aparece un icono en el escritorio.

Configuración del ancho de banda

Antes de establecer una conferencia vamos a explorar las posibilidades que nos brinda el Netmeeting. Para ello seleccionamos en la ventana del programa el menú desplegable **'Herramientas'** y de él elegiremos la última opción llamada **'Opciones'**, con lo que nos aparece una ventana con varias pestañas. De éstas seleccionaremos la pestaña **'General'**; en ella podemos ver y modificar los datos identificativos del conferenciante. Para poder utilizar el Netmeeting deben aparecer como mínimo el Nombre, Apellido y la dirección de correo electrónico. En la parte inferior de la ventana encontramos un botón que pone **'Configuración del ancho de banda'**. Si lo pulsamos aparecerá una nueva ventana que nos permitirá indicar la velocidad de la conexión a la red, de entre cuatro posibilidades:

- Módem de 14,4 Kb/s
- Modem de 28,8 Kb/s
- Cable, xDSL ó RDSI
- Red de área local

Este dato lo utiliza el Netmeeting para fijar el caudal máximo que debe generar durante la conferencia, el caudal puede ser menor si las características del vídeo y audio lo permiten. Nosotros elegiremos la opción **'Red de área local'** que es la que nos permite utilizar mayor ancho de banda (unos 450 Kb/s) y por tanto nos ofrece mayor calidad.

Configuración de audio

A continuación volveremos a la ventana de opciones y pulsaremos la pestaña **'Audio'** donde podremos seleccionar diversas características, tales como el ajuste automático de volumen del micrófono o la detección automática de silencios. El **'Ajuste de audio'** sirve para ajustar el volumen de audio a un nivel adecuado, mediante una prueba de nivel. Pulsando el botón **'Avanzado…'** accedemos a la ventana '**Configuración de compresión avanzada**' en la que se marcaremos la casilla '**Establecer manualmente la configuración de compresión**' para poder explorar los códecs que nos ofrece el Netmeeting, que son los siguientes:

- El G.723.1 con sus dos posibles caudales, 6,4 ó 5,3 Kb/s
- Un códec ADPCM propietario de Microsoft con muestras de 4 bits y un caudal de 32 Kb/s
- Los dos códecs G.711 que existen, con la escala según la ley 'mu' y según la ley 'A'. Ambos corresponden a un caudal de 64 Kb/s, por tanto se trata de audio no comprimido. Estos aparecen descritos como **'Ley u de CCITT'** y **'Ley A de CCITT'** (aunque la CCITT pasó a llamarse ITU-T en 1993 Microsoft ha decidido utilizar en este caso la denominación antigua).

Una vez explorados los códecs debemos desmarcar la casilla '**Establecer manualmente la configuración de compresión**'. La selección automática es más cómoda ya que la manual requiere que ambos participantes elijan el mismo códec para que la comunicación por audio sea posible. Una vez desmarcada

esta casilla volveremos a la ventana 'Audio', donde dejaremos todos los parámetros de audio con sus valores por defecto.

Configuración de vídeo

Ahora pulsaremos la pestaña **'Vídeo'**. En esta podemos indicar si queremos que siempre que se establezca una comunicación se envíe vídeo, y si estamos interesados en recibir vídeo automáticamente al inicio de cada llamada. Debemos marcar ambas casillas. El vídeo requiere anchos de banda elevados y por ese motivo su uso se considera opcional; en cambio el audio siempre se envía, si el terminal lo soporta ya que es obligatorio en H.323. A continuación tenemos unos botones tipo 'radio' que nos permiten fijar el **'Tamaño de imagen de envío'**; esto es sencillamente la resolución de la imagen de vídeo que vamos a transmitir (la que recibimos la controla el otro participante) Existen tres posibilidades denominadas **'Pequeño'**, **'Medio'** y **'Grande'** que corresponden a los formatos SQCIF (128x96), QCIF (176x144) y CIF (352x288), respectivamente. Nosotros seleccionaremos tamaño Grande. El programa nos permite elegir cualquier resolución independientemente del ancho de banda que tengamos, por ejemplo podríamos seleccionar el formato CIF con módem de 14,4 Kb/s, aunque en este caso cada fotograma tardaría varios segundos en transmitirse con lo que el vídeo sería poco ágil. En la ventana de vídeo también podemos indicar si queremos enviar un vídeo **'De mejor calidad'** o uno **'Más rápido'**; aquí lo que hace el programa es intentar ajustar el número de fotogramas por segundo que se envían, de forma que en el primer caso sacrifica agilidad de movimiento (fotogramas por segundo) en pro de la calidad de imagen y en el segundo procede al contrario, tratando de no superar en ningún caso el caudal correspondiente al Ancho de banda elegido. Por ejemplo en el caso de estar transmitiendo las diapositivas de una presentación sería recomendable elegir el vídeo de mejor calidad puesto que la imagen tendrá poco movimiento. Nosotros dejaremos el valor por defecto.

Establecimiento de la conferencia

Ahora seleccionaremos la pestaña **'General'** y a continuación pulsaremos el botón '**Llamada avanzada…**' con lo que nos aparece la ventana de **'Opciones avanzadas de llamada'**. En esta ventana debemos asegurarnos de que estén desmarcadas las casillas **'Usar un equipo selector…'** y '**Usar una puerta de enlace…'**. Si estas casillas están marcadas no es posible establecer conferencias con otros ordenadores.

Ahora los alumnos probarán a realizar una llamada y establecer una vídeoconferencia entre los dos ordenadores de su equipo. La llamada la harán desde uno de los ordenadores poniendo en la ventana de llamada la dirección IP o el nombre del otro ordenador. El otro ordenador recibirá la petición de llamada entrante que deberá aceptar, momento en el cual se establece la comunicación. Si todo funciona correctamente en unos pocos segundos habrá entre ambos comunicación de audio y de vídeo (limitado por la disponibilidad de cámaras y micrófonos/auriculares de los ordenadores). Si no aparece el vídeo seguramente será porque no están marcadas las opciones correspondientes en la ventana '**Herramientas**' -> '**Opciones**' -> '**Vídeo**'. Esto puede resolverse pulsando el botón Iniciar/Detener vídeo, que se encuentra en la parte izquierda de la ventana de Netmeeting (justo arriba de la palabra 'Nombre' de la lista de participantes). Con este botón cada conferenciante controla la emisión de su vídeo y la recepción del remoto.

El Netmeeting puede configurarse para que acepte llamadas automáticamente. Para esto desplegaremos el menú **'Llamar'** y elegiremos la opción **'Aceptar llamadas automáticamente'**. De este modo el Netmeeting acepta de forma inmediata cualquier llamada entrante.

Algunos parámetros de Netmeeting, por ejemplo la resolución de vídeo, se pueden cambiar en cualquier momento durante una conferencia, Otros, como por ejemplo el Ancho de banda, pueden cambiarse durante la conferencia pero la modificación solo tiene efecto a partir de la siguiente llamada. Por último algunos parámetros, como el códec de audio (en el caso de que se haya configurado para selección manual) , solo pueden cambiarse cuando no hay una llamada en curso. Obsérvese por último que el Netmeeting no permite una comunicación en grupo, es una herramienta de comunicación entre dos participantes exclusivamente.

Captura de tráfico con WireShark

Ahora los alumnos pondrán en marcha en ambos ordenadores el programa Wireshark y realizarán capturas de tráfico estableciendo un filtro para poder analizar más cómodamente el tráfico de la conferencia. Para ello deben arrancarlo haciendo doble clic sobre el icono 'Wireshark', que debe estar en el escritorio. En caso de que no encontremos el icono seleccionaremos con el ratón el icono **'Inicio'** en la parte inferior izquierda de la pantalla, en el menú desplegable seleccionaremos **'Ejecutar…'** y en .el campo **'Abrir'** teclearemos **`'wireshark'`**. Si de esta forma tampoco se ejecuta el programa consultaremos con el profesor. Una vez aparece la ventana Wireshark para configurar el filtro seleccionaremos en la parte superior el menú '**Capture**' y la opción **'Interfaces…'.**

En esta opción aparecerán todas las interfaces instaladas en el PC. Por ejemplo normalmente aparecerá una interfaz llamada '**Adapter for Generic Dialup** …" que corresponde a la interfaz serie del host (COM1) y la interfaz cuyo nombre variará dependiendo de la tarjeta de red, que es la interfaz Ethernet sobre la que discurre nuestro tráfico (podría haber más de una si el ordenador tiene varias tarjetas de red). De todas las interfaces que aparecen deberemos utilizar la que tiene asignada la dirección IP de nuestro ordenador, que como podremos comprobar por el contador de paquetes es la que está recibiendo el tráfico de la red . En esa misma ventana, si presionamos el botón **options** asociado a nuestra interfaz o **mediante el menú capture y luego options (** si hubiéramos cerrado la venta de interfaces inicial**)** iremos al campo **'Capture Filter:'** y teclearemos el filtro **`'host`** ***`dirección_IP`*****`'`** donde **`'`*****`dirección_IP`*****`'`** es la dirección IP del host remoto con el que hemos establecido la conferencia, por ejemplo **`'host 147.156.103.32'`**. Este filtro provoca que el Wireshark solo capture y nos muestre los paquetes que tienen como origen o destino el ordenador con el que estamos estableciendo la conferencia. Debemos activar la captura antes de efectuar la llamada para ver todos los paquetes intercambiados entre los hosts durante el establecimiento de la comunicación. Entre ellos se encuentran los correspondientes al protocolo de señalización de H.323, que es reconocido por el Wireshark.

- **A la vista de la captura obtenida los alumnos deben indicar cual es el protocolo de señalización utilizado en H.323 (pista: su nombre empieza por Q).**

Una vez establecida la comunicación el grueso del tráfico es UDP, que es la forma como se envía la información de audio y vídeo. Seleccionando uno de esos paquetes UDP podemos con la ayuda del Wireshark analizarlo con más detalle. Sin embargo, algunas versiones del Wireshark no interpretan la cabecera RTP que está situada después de la cabecera UDP, ya que el protocolo RTP no tiene un número de puerto reservado, como ocurre con otros como HTTP y SMTP. Para que Wireshark analice el contenido del un paquete RTP se lo tenemos que indicar. Esto lo podemos hacer seleccionando uno de esos paquetes, después desplegamos el menú **'Analyze'** y elegimos la opción **'Decode As…'** la cual nos mostrará una larga lista de protocolos posibles; elegiremos de todos ellos RTP y a partir de ese momento Wireshark interpretará las cabeceras RTP, no solo del paquete que hemos seleccionado sino las de todos los paquetes que corresponden al mismo flujo, es decir que tengan la misma dirección IP de origen y destino y el mismo puerto de origen y destino, ya que se supone que todos esos paquetes son también RTP. Así podremos ver algunas características de la comunicación.

Los alumnos deberán ahora analizar un paquete RTP con información de vídeo y utilizarlo para responder a las siguientes preguntas:

- **¿Qué resolución se está utilizando para transmitir y para recibir vídeo? (puede no ser la misma en ambos sentidos)**
- **¿Qué códec se está utilizando para vídeo?**
- **¿Qué códec se está utilizando para audio? ¿Con que caudal?**

Si se transmite audio y vídeo la cantidad de paquetes de vídeo es considerablemente mayor que la de audio, por lo que si queremos capturar paquetes de audio es conveniente establecer una conferencia sin vídeo. También debemos tomar en cuenta que la supresión de silencios hace que solo se transmitan paquetes cuando se habla, por lo que al capturar audio hay que suprimirla o asegurarnos de hablar durante la conferencia.

Monitorización del tráfico generado

Otra experiencia interesante es monitorizar el tráfico que estamos generando en la red durante la conferencia. Para ello utilizaremos el **'Administrador de Tareas'** de Windows (pulsar Alt-Ctrl-Supr) y

seleccionaremos la pestaña **'Funciones de red'** que nos muestra de manera gráfica y en escala porcentual el grado de ocupación de la tarjeta de red (para interpretar correctamente el significado de los valores que aparecen debemos recordar que los ordenadores están **conectados a un switch de 100 Mb/s**). Utilizando esta herramienta los alumnos deben ahora hacer una estimación del caudal que envía el Netmeeting cuando se configura para 'Red de área local' y como cambia dicho caudal al modificar el ancho de banda en la configuración (para que el cambio surta efecto es preciso establecer de nuevo la conferencia). La mejor forma de hacer estas pruebas es configurar un Netmeeting para que no emita vídeo y para que acepte automáticamente las llamadas entrantes, de forma que todos los cambios y pruebas los haremos desde el otro ordenador únicamente; de lo contrario sería preciso hacer todos los cambios cada vez en ambos ordenadores de forma sincronizada. Una vez hechas las pruebas con diferentes anchos de banda volveremos a poner el Netmeeting en el valor inicial ('Red de área local') y con la gráfica de **'Funciones de red'** en pantalla haremos el siguiente experimento: dejaremos la cámara enfocada a una imagen estática durante unos segundos hasta que el caudal transmitido se estabilice claramente, según podremos apreciar por la gráfica; entonces provocaremos un movimiento en la imagen, por ejemplo pasando algo por delante de la cámara y veremos como se modifica el caudal por este motivo. Deberemos apreciar claramente en la gráfica los momentos en que se produce movimiento ante la cámara. Esto es un claro ejemplo de la eficiencia de los algoritmos de compresión de vídeo, que permiten reducir el caudal de forma apreciable cuando la imagen a transmitir es prácticamente la misma todo el tiempo (en realidad la imagen estática cambia más de lo que parece puesto que la iluminación con tubos fluorescentes provoca 50 destellos por segundo y esto afecta a los algoritmos de compresión de vídeo).

En el Administrador de Tareas también podemos observar el consumo de CPU que produce la codificación/descodificación del vídeo; con los ordenadores actuales esta carga no es importante, pero hace unos pocos años se convertía en el factor limitante de la calidad cuando se utilizaban caudales elevados.

Configuración de un Gateway (puerta de enlace)

Ahora vamos a hacer una prueba de configurar nuestro Netmeeting para que utilice un Gateway, llamado 'puerta de enlace' en la versión en castellano del software. Cuando se tiene configurada una puerta de enlace el usuario puede llamar no solo a direcciones IP sino también a direcciones E.164, es decir a números de teléfono (las direcciones E.164 son simples secuencias de entre 1 y 15 dígitos decimales). Se supone que el terminal H.323 dirigirá todas las llamadas que hagamos a direcciones E.164 hacia la puerta de enlace, que será la encargada de transferirlas a la red telefónica. Como no disponemos de una verdadera puerta de enlace vamos a configurarle como puerta de enlace a cada ordenador del laboratorio el otro ordenador con el que hace las pruebas. De esta forma cuando llamemos a una dirección E.164 la llamada la enviaremos al ordenador de nuestro compañero, cualquiera que sea el número al que llamemos.

Antes de configurar la puerta de enlace probaremos a efectuar una llamada a una dirección E.164 cualquiera, por ejemplo '**12345**'. Veremos que Netmeeting nos devuelve un mensaje indicando que no ha podido encontrar ese nombre de persona en el servidor de directorio. Al no tener configurada puerta de enlace Netmeeting interpreta cualquier secuencia de caracteres que no sea una dirección IP válida como un nombre que debe buscar en el directorio.

Ahora configuraremos la puerta de enlace. Para ello desplegaremos nuevamente el menú **'Herramientas'**, elegiremos la opción **'Opciones'** y en la ventana correspondiente pulsaremos el botón de '**Llamada avanzada'**. Veremos aparecer una ventana en cuya parte inferior podemos dar la configuración de la puerta de enlace. Seleccionaremos primero la casilla '**Usar una puerta de enlace…'** y después teclearemos en el campo **'Puerta de Enlace'** la dirección IP del otro ordenador de nuestra maqueta, con el que estamos realizando las pruebas de Netmeeting.

A continuación repetiremos la llamada a la misma dirección E.164 de antes ('**12345**' o la que sea). Ahora el ordenador redirigirá la llamada a la dirección IP del otro ordenador, que es la que tiene configurada como puerta de enlace. Pero puesto que ese ordenador recibe una llamada H.323 que no puede realmente transferir a la red telefónica la responde él directamente. Podemos comprobar que, cualquiera que sea la dirección E.164 que pongamos, la llamada siempre la recibe el ordenador que tenemos configurado como puerta de enlace.

Configuración de un Gatekeeper (equipo selector)

Ahora vamos a hacer una prueba consistente en configurar nuestro Netmeeting para que haga uso de un Gatekeeper, llamado 'equipo selector' en la versión en castellano. De nuevo como no disponemos de un Gatekeeper real utilizaremos como Gatekeeper imaginario el otro ordenador de nuestra maqueta. Pero para poder analizar los mensajes que enviamos pondremos antes en marcha una captura con el Wireshark definiendo el filtro '**dst host *dirección_IP***' donde ***'dirección_IP'*** es la del otro ordenador de nuestra maqueta. Esto nos permitirá analizar todos los paquetes que enviamos a dicho ordenador; las respuestas no nos interesan ya que al no tener el ordenador realmente funciones de Gatekeeper no va a responder a nuestros mensajes y los que nos envíe serán únicamente las pruebas que realice nuestro compañero en sentido contrario, que nos podrían confundir.

Una vez tenemos en marcha la captura configuramos el Gatekeeper de la siguiente forma: entramos en **'Herramientas'** -> **'Opciones'** -> **'Llamada avanzada'** y una vez allí seleccionamos la casilla de la parte superior que dice **'Usar un equipo selector…'**. Al seleccionar esta opción automáticamente se desactiva la correspondiente a la **'Puerta de Enlace'** ya que ambas son incompatibles y la de Equipo Selector tiene precedencia. Como equipo selector pondremos la dirección del otro ordenador de nuestra maqueta (la misma que hemos puesto en el filtro del Wireshark). A continuación seleccionaremos la casilla **'Iniciar la sesión usando mi nombre de cuenta'** y teclearemos en el campo '**Nombre de cuenta**' una combinación de usuario y password separados por el carácter '#' (por ejemplo **'pepito#secreta'**); este sería el código que utilizaríamos para identificarnos como usuario autorizado ante el Gatekeeper, el cual normalmente accedería en ese momento a un servidor de autenticación para comprobar que el usuario es legítimo y está autorizado a utilizar el servicio[1]. Una vez configurado lo anterior pulsaremos el botón '**Aceptar**' y observaremos que justo en ese momento el Wireshark empieza a capturar paquetes; al cabo de varios intentos y pasados unos segundos recibimos el mensaje 'Tiempo de conexión del equipo selector agotado' y el Wireshark deja de capturar paquetes. Al recibir este mensaje pararemos la captura y analizaremos el tráfico capturado por el Wireshark. Por medio de dicho análisis responderemos a las siguientes preguntas:

- **¿A qué protocolo pertenecen los mensajes que se envían al Gatekeeper?**
- **¿Cuántos intentos de conexión realiza nuestro equipo?**
- **¿Cuánto tiempo se espera entre intentos consecutivos?**
- **¿Qué información viaja en los paquetes que se envían al Gatekeeper?**
- **¿Qué ocurriría si hubiera un NAT entre nuestro ordenador y el Gatekeeper?**
- **¿Cómo se envía la información de usuario#password que hemos tecleado? ¿Puede esa información ser capturada por extraños?**

4.- Realizar emisiones de vídeo streaming con VideoLAN

El VideoLAN es un programa que permite realizar emisiones de vídeo unicast o multicast. No es una herramienta de vídeoconferencia como el Netmeeting. Vamos ahora a explorar las posibilidades de este software para establecer un servidor de vídeo streaming en una red.

El vídeo streaming puede servirse desde múltiples fuentes, por ejemplo:

- Ficheros del disco duro
- DVDs montados en el lector del ordenador
- Cámaras de vídeo conectadas al ordenador
- Tarjetas sintonizadoras de televisión terrestre o vía satélite

En el caso de imágenes en disco duro o DVD el vídeo y el audio tienen ya un formato comprimido en origen, por lo que la labor de VideoLAN se limita a generar los flujos y enviarlos por la red. En el caso de

[1] Obsérvese que con esta interfaz la password es visible a los demás en el momento de teclearla, que la password se conserva no encriptada y que cualquiera que tenga acceso al ordenador en un momento dado tiene acceso a la password.

cámaras de vídeo o tarjetas sintonizadoras el vídeo se ha de comprimir en tiempo real mientras se captura, para poder emitirlo en el formato elegido. VideoLAN dispone de varios códecs de vídeo. En el caso de una emisión de vídeo previamente comprimido (disco duro o DVD) es posible hacer transcodificación en tiempo real, para adaptar la emisión al ancho de banda disponible en la red. Vamos a ver todas estas posibilidades por orden.

Preparación

Para estas pruebas los alumnos deben trabajar también por parejas de ordenadores, uno de los cuales actuará como servidor de vídeo y el otro como cliente. Los únicos requisitos son que el servidor debe tener cámara y el cliente auriculares.

Las pruebas las haremos emitiendo desde el servidor al cliente.

En primer lugar vamos a poner 'a la escucha' al cliente. Como todas las pruebas de emisión las haremos desde el servidor no necesitaremos tocar nada en el cliente una vez lo hayamos puesto 'a la escucha'. De hecho el cliente queda a merced del servidor, que puede enviarle el video que quiera, sin que el cliente pueda seleccionar nada excepto decodificar o no el flujo que recibe.

El procedimiento para arrancar el cliente VideoLAN es el siguiente:

1- Arrancar el programa '**VLC media player**' mediante doble clic en el icono correspondiente.
2- Seleccionar en la ventana que aparece el menú '**Archivo:F**'
3- Elegir de la lista la opción '**Abrir Aparato de Captura…**'
4- En la ventana '**Abrir…**' seleccionar la pestaña '**Red**'
5- En la lista de botones radio seleccionar '**UDP/RTP**'. El número de puerto debe coincidir con el utilizado por el servidor; utilizaremos el valor por defecto de **'1234'**.
6- Pulsar el botón '**OK**'
7- El cliente está listo para recibir cualquier emisión que le llegue al puerto 1234, venga de donde venga.

En realidad no sería necesario utilizar dos ordenadores para probar el VideoLAN, ya que en el propio servidor podemos ejecutar simultáneamente una instancia de VideoLAN configurado como cliente. Vamos pues, siguiendo el procedimiento anterior, a arrancar otro cliente en el ordenador que actúa de servidor. Esto es interesante porque nos permitirá seguir localmente, a modo de monitor, la emisión que estamos realizando. La reproducción que realiza este cliente es realmente obtenida de la red, no suministrada internamente por el ordenador, por lo que permite detectar problemas en la emisión, incluso a nivel físico; por ejemplo si se desconecta el cable de red del servidor la reproducción de este cliente se para como la de cualquier otro.

Emisión de vídeo streaming

La primera prueba que haremos consistirá en emitir desde el servidor un vídeo que se encuentra en el disco duro, concretamente en el escritorio. El fichero se denomina 'Ethernet.mpg' y se trata de un vídeo de 10 minutos de duración con las siguientes características:

- vídeo: MPEG-1, resolución 352x288 (SIF), 25 fps (fotogramas por segundo), 1500 Kb/s
- audio: MPEG-1 capa II, frec. muestreo 44,1 KHz, 2 canales (estéreo), 224 Kb/s

El flujo total es por tanto de 1,7 Mb/s aproximadamente.

El procedimiento para poner en marcha la emisión en el servidor VideoLAN es el siguiente:

1- Arrancar el programa '**VLC media player**' mediante doble clic en el icono correspondiente.
2- Seleccionar el menú '**Archivo:F**'
3- Elegir de la lista la opción '**Abrir Volcado de Red…: N**'
4- En la ventana '**Abrir…**' seleccionar la pestaña '**Archivo**'
5- Pulsar el botón '**Explorar**' y seleccionar el fichero correspondiente ('Ethernet.mpg')
6- Marcar la casilla **'Volcado/Salvar'** y pulsar el botón **'Opciones'**.

7- En la ventana '**Volcado de salida**' marcar la casilla '**RTP**'. . En ese momento se habilitan los campos '**Dirección**' y '**Puerto**'.
8- En el campo '**Dirección**' poner la dirección del cliente que debe recibir el video streaming. El campo '**Puerto**' debe quedar con su valor por defecto (1234).
9- Pulsar el botón '**OK**' en la ventana '**Volcado de salida**'
10- Pulsar el botón '**OK**' en la ventana '**Abrir…**'.
11- Empieza la emisión de video streaming.

Como puede comprobarse fácilmente, durante la emisión los botones de control de vídeo del cliente no funcionan, salvo el de parada/arranque del vídeo. Sin embargo el servidor puede controlar el vídeo con los botones pause, play, retroceder, etc.

Un mismo servidor podría distribuir simultáneamente varios flujos de video al mismo o diferentes clientes. Bastaría para ello con ejecutar diferentes instancias del programa. En el caso de realizar diferentes emisiones hacia el mismo cliente deberían utilizarse números de puerto diferentes pues de lo contrario los flujos llegarán mezclados y no será posible ver correctamente el vídeo.

Emisión de vídeo streaming con transcodificación

Vamos a probar ahora las facilidades de transcodificación que nos ofrece el VideoLAN. La transcodificación nos permite convertir un flujo o fichero multimedia cambiando el códec utilizado, la resolución, el caudal, etc. Supongamos que necesitáramos difundir el vídeo del ejemplo hacia un cliente cuya conexión fuera de solo 256 Kb/s. Habría que reducir drásticamente el caudal, posiblemente cambiando a un códec más eficiente, bajando la resolución del vídeo o pasando el audio de estéreo a monoaural. En nuestro caso vamos a emitir ahora el vídeo con los siguientes parámetros:

- Códec de vídeo: H.263
- Tasa de bits (kb/s): 128
- Resolución: SIF (352x288) (la misma que el vídeo original)
- Códec de audio: MPEG-1 capa III
- Tasa de bits (kb/s): 64
- Canales: 1 (monoaural)

En el cliente no será necesario realizar ningún cambio, siempre y cuando se mantenga el mismo número de puerto, ya que la transcodificación se realiza exclusivamente en el servidor. El cliente se limitará a reproducir los flujos de audio y vídeo que le lleguen, haciendo uso de los códecs y resolución elegidos en el servidor (recordemos que cada paquete de información multimedia lleva escrita en la cabecera RTP la información relativa al tipo de códec utilizado).

El procedimiento para realizar una emisión con transcodificación es muy similar al de una emisión normal. Tan solo hay que rellenar además en la ventana 'Volcado de salida' las opciones de transcodificación que se quieren aplicar. Vamos a describirlo en detalle:

1- Arrancar el programa '**VLC media player**'.
2- Seleccionar el menú '**Archivo:F**'
3- Elegir de la lista la opción '**Abrir Volcado de Red…: N**'
4- En la ventana '**Abrir…**' seleccionar la pestaña '**Archivo**'
5- Pulsar el botón '**Explorar**' y seleccionar el fichero correspondiente ('Ethernet.mpg')
6- Marcar la casilla **'Volcado/Salvar'** y pulsar el botón **'Opciones'**.
7- En la ventana '**Volcado de salida**' marcar la casilla '**RTP**'.
8- En el campo '**Dirección**' poner como antes la dirección del otro ordenador. Dejar el campo '**Puerto**' con su valor por defecto (1234).
9- Marca la casilla '**Códec de vídeo**'. Seleccionar '**h263**'. En 'Tasa de bits (kb/s)' seleccionar '**128**'. En '**Escala**' dejar el valor por defecto (1).
10- Marcar la casilla '**Códec de audio**'. Seleccionar '**mp3**'. En 'Tasa de bits (kb/s)' seleccionar '**64**'. En '**Canales**' seleccionar '**1**'.
11- Pulsar el botón '**OK**' en la ventana '**Volcado de salida**'
12- Pulsar el botón '**OK**' en la ventana '**Abrir…**'.
13- Empieza la emisión multicast.

La degradación de la calidad, sobre todo en el vídeo, es evidente.

Realmente pretender enviar una resolución SIF con 128 Kb/s es excesivo. Con este caudal se habría conseguido mejor calidad bajado la resolución a QSIF (176x144). La resolución de vídeo la podemos cambiar en la transcodificación mediante el parámetro '**Escala**'. Vamos ahora a repetir el procedimiento anterior manteniendo todos los parámetros igual salvo la '**Escala**' para la que seleccionaremos ahora '**0.5'**, que quiere decir la mitad de resolución en cada dimensión, es decir QSIF en este caso. Ahora veremos el mismo vídeo en formato más pequeño, pero con mayor calidad.

Ahora vamos a hacer una segunda prueba de transcodificación pero esta vez utilizaremos el fichero 'Carmen.mpg' que se encuentra en el escritorio. Este vídeo, de tres minutos de duración tiene las siguientes características:

- vídeo: MPEG-2, resolución 720x576, 25 fps, 4500 Kb/s
- audio: MPEG-1 capa II, frec. muestreo 48 KHz, 2 canales (estéreo), 192 Kb/s

Primero vamos a emitir este vídeo sin modificaciones. Como el vídeo supone un caudal de unos 4,7 Mb/s en cuanto haya tres emisiones simultáneas habrá saturación de la red y la calidad se degradará. A continuación haremos una emisión transcodificada, pero antes de poner en marcha la emisión arrancaremos el 'Administrador de tareas' de Windows para monitorizar el uso de la CPU y observar así la carga que supone la labor de transcodificación en tiempo real.

Para realizar la transcodificación procederemos como antes, pero esta vez aplicaremos los siguientes parámetros:

- Códec de vídeo: **mp4v** (MPEG-4)
  - Tasa de bits (kb/s): **384**
  - Escala: **0,75** (resolución 540x432)
- Códec de audio: **mp3** (MPEG-1 capa III)
  - Tasa de bits (kb/s): **96**
  - Canales: **2**

Con este caudal (480 Kb/s) tendría que haber unas 17-18 emisiones simultáneas para que hubiera problemas en la red.

No todos los códecs que se pueden seleccionar funcionan, algunos no tienen el programa correspondiente incorporado en el VideoLAN. En particular los códecs que no funcionan en la emisión desde fichero son 'DIV1' y 'theo' en vídeo y 'vorb', 'flac', 'spx', 's16l' y 'fl32' en audio.

Emisión de vídeo en directo

Como decíamos antes, además de poder emitir vídeo previamente comprimido videoLAN también puede utilizar como entrada cualquier fuente de vídeo habitual, como cámaras o tarjetas sintonizadoras de televisión. Nosotros haremos ahora una prueba con las cámaras de vídeo de que disponemos.

Como en los casos anteriores controlaremos toda la emisión desde el servidor, por lo que no será necesario realizar ninguna modificación en el cliente, que se limitará a reproducir el vídeo que le enviemos, independientemente de su origen, códec, resolución, caudal, etc.

En el caso de una emisión de vídeo en directo es obligatorio utilizar las opciones de transcodificación, ya que esta es la manera de indicarle a VideoLAN el formato de audio y vídeo que queremos generar. Para ello vamos a emplear el siguiente procedimiento:

1- Arrancar el programa '**VLC media player**'.
2- Seleccionar el menú '**Archivo:F**'
3- Elegir de la lista la opción '**Abrir Volcado de Red…: N**'
4- En la ventana '**Abrir…**' seleccionar la pestaña '**DirectShow**'

5- En la línea donde aparece '**Nombre del aparato de vídeo**' pulsar el botón '**Refresh list**', desplegar la lista que aparece a la izquierda y seleccionar la opción '**que corresponda con el tipo de cámara conectada**. Si no aparece esta opción debemos pulsar nuevamente el botón '**Refresh list**' hasta que aparezca.
6- En la línea donde aparece '**Nombre del aparato de audio**' dejar la opción que aparece ('**Por Defecto**').
7- Comprobar que no estén marcadas las casillas '**Propiedades del aparato**' y '**Propiedades del sintonizador**'.
8- Marcar la casilla **'Volcado/Salvar'** y pulsar el botón **'Opciones'**.
9- En la ventana '**Volcado de salida**' marcar la casilla '**RTP**'.
10- En el campo '**Dirección**' poner la dirección del cliente. Dejar el campo '**Puerto**' con su valor por defecto (1234).
11- Marca la casilla '**Códec de vídeo**'. Seleccionar '**mp1v**'. En 'Tasa de bits (kb/s)' seleccionar '**512**'. En '**Escala**' dejar el valor por defecto (1).
12- Marcar la casilla '**Códec de audio**'. Seleccionar '**mp3**'. En 'Tasa de bits (kb/s)' seleccionar '**64**'. En '**Canales**' seleccionar '**1**'.
13- Pulsar el botón '**OK**' en la ventana '**Volcado de salida**'
14- Pulsar el botón '**OK**' en la ventana '**Abrir…**'.
15- Empieza la emisión.

Si todo ha funcionado correctamente la emisión incluye tanto vídeo como audio. Como podemos comprobar fácilmente el retardo introducido por la codificación es de varios segundos, aunque esto depende de la complejidad del códec utilizado. La resolución de la cámara que estamos utilizando es de 320x240 y 30 fps. La resolución puede reducirse en la transcodificación con el parámetro '**Escala**'.

Podemos utilizar cualquier códec de vídeo o audio de los que aparecen en la lista desplegable, salvo los que no están implementados, que son en este caso: 'DIV1' 'h263' y 'theo' en vídeo y . 'vorb', 'flac', 'spx', 's16l' y 'fl32' en audio.

Si en vez de elegir el códec MPEG-1 elegimos el H.264 veremos como el uso de CPU aumenta considerablemente por tratarse de un códec de gran complejidad. (Utilizar para verlo el 'Administrador de tareas').

Sería posible establecer una comunicación por vídeoconferencia bidireccional entre dos ordenadores mediante el VideoLAN, aunque este programa no está pensado para ello, como el Netmeeting. Obsérvese que el VideoLAN ofrece un servicio no orientado a conexión donde el servidor envía su flujo de audio/vídeo sin saber siquiera si el cliente lo está recibiendo. Además el retardo introducido por el proceso de codificación hace difícil mantener una interacción entre los participantes.

8.- Finalización

Al terminar la práctica los alumnos deben reactivar el cortafuegos que desactivaron al principio.

ANEXO I: Filtros en wireshark.

En Wireshark es posible construir filtros que determinen si un determinado tipo de paquetes va a ser capturado o no. En caso de que no se utilice ningún filtro, todos los paquetes son capturados.

Los filtros se construyen mediante expresiones que consisten en una o más primitivas. Las primitivas, usualmente, consisten en un identificador (nombre o número), precedidas por uno o más calificadores. Existen tres tipos diferentes de calificadores:

- De tipo: Identifican un nombre o dirección, sus posibles valores son *host*, *net* y *port*. Por ejemplo, 'host glup.uv.es', 'net 147.156', 'port 20'. Si no existe ningún calificador de tipo, se asume que el tipo es host.

- De dirección: Identifican una dirección particular de transferencia, esto es, un origen o destino. Sus valores posibles son *src*, *dst*, *src or dst* y *src and dst*. Por ejemplo, 'src glup.uv.es', 'dst net 147.156', 'src or dst port ftp-data'. Si no se indica ningún calificador de dirección, se toma el calificador de dirección por defecto (src or dst).

- De protocolo: Identifican un protocolo particular. Sus valores posibles son ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp y udp. Por ejemplo, 'ether src glup.uv.es', 'arp net 147.156', 'tcp port 21'. Si no se especifica ningún protocolo, todos los protocolos que sean consistentes con la identificación de tipo son capturados.

Como puede verse por la explicación de los diferentes tipos de calificadores, siempre están presentes, aunque sea por defecto, los tres tipos de calificadores. Así, la expresión ip 147.156.222.65 es equivalente a ip src or dst host 147.156.222.65.

Pueden construirse filtros más complejos mediante la combinación de primitivas mediante la utilización de paréntesis y/o las palabras *and*, *or* y *not*., siendo la prioridad de *not* mayor que la de *and* y *or*, cuya prioridad entre si es igual. Así, por ejemplo, 'ip multicast and (ip src 147.156.222.65)' indica que se capturen todos los paquetes multicast cuyo origen sea 147.156.222.65. Otro ejemplo, 'host glup.uv.es and not port ftp' in indica que se capturen todos los paquetes cuyo origen o destino es glup.uv.es excepto aquellos cuyo puerto de origen o destino es el de ftp (puerto 21).

Un listado de las primitivas más utilizadas se encuentra en la siguiente tabla:

Primitiva	**Descripción**
dst host <ordenador>	Verdad si el campo destino del paquete es el <ordenador>
src host <ordenador>	Verdad si el campo origen del paquete es el <ordenador>
Host <ordenador>	Verdad si el campo origen o destino del paquete es el <ordenador>
ether dst <ordenador>	Verdad si la dirección ethernet de destino es el <ordenador>
ether src <ordenador>	Verdad si la dirección ethernet de origen es el <ordenador>
ether host <ordenador>	Verdad si la dirección ethernet de origen o destino es el <ordenador>
gateway <ordenador>	Verdad si el paquete utiliza como pasarela (gateway) el <ordenador>
dst net <red>	Verdad si la dirección de destino del paquete corresponde a una dirección de la <red>
src net <red>	Verdad si la dirección de origen del paquete corresponde a una dirección de la <red>
net <red>	Verdad si las dirección de origen o destino del paquete corresponde a una dirección de la <red>
dst net <red> mask <mascara>	Verdad si la dirección de destino del paquete corresponde a una dirección de la <red> de máscara <mascara>
src net <red> mask <mascara>	Verdad si la dirección de origen del paquete corresponde a una dirección de la <red> de máscara <mascara>
net <red> mask <mascara>	Verdad si las dirección de origen o destino del paquete corresponde a una dirección de la <red> de máscara <mascara>

Primitiva	**Descripción**
dst net <red>/<longitud>	Verdad si la dirección de destino del paquete corresponde a una dirección de la <red> cuya máscara se indica por <longitud>
src net <red>/<longitud>	Verdad si la dirección de origen del paquete corresponde a una dirección de la <red> cuya máscara se indica por <longitud>
net <red>/<longitud>	Verdad si las dirección de origen o destino del paquete corresponde a una dirección de la <red> cuya máscara se indica por <longitud>
dst port <puerto>[2]	Verdad si el paquete tiene como destino el puerto dado por <puerto>
src port <puerto>	Verdad si el paquete tiene como origen el puerto dado por <puerto>
Port <puerto>	Verdad si el paquete tiene como origen o destino el puerto dado por <puerto>
Less <longitud>	Verdad si el paquete tiene una longitud menor o igual que <longitud>
greater <longitud>	Verdad si el paquete tiene una longitud mayor o igual que <longitud>
ether broadcast	Verdad si el paquete es un paquete ethernet broadcast.
ip broadcast	Verdad si el paquete es un paquete IP broadcast.
ether multicast	Verdad si el paquete es un paquete ethernet multicast.
ip multicast	Verdad si el paquete es un paquete IP multicast.

Además de las expresiones anteriores, existen expresiones del tipo *<expresión 1> <operador> <expresión 2>*, donde *<operador>* es <, >, <=, >=, =, *!=* y *<expresión 1>* y *<expresión 2>* son expresiones aritméticas compuestas por constantes enteras (expresadas con la sintaxis de C), los operadores +, -, *, /, &, |, y un acceso especial a los datos del paquete.

Para acceder a los datos de un paquete se utiliza la sintaxis *protocolo [desplazamiento : tamaño]*, donde *protocolo* es uno de los protocolos validos (*ether*, *fddi*, *tr*, *ip*, *arp*, *rarp*, *tcp*, *udp*, *icmp* o *ip6*), *desplazamiento* es el desplazamiento, en bytes, desde el comienzo de los datos del protocolo especificado, y *tamaño* son los bytes a analizar. Así, ip[0] & 0x0F !=5 indica todos los paquetes que contienen opciones IP (campo IHL de valor distinto de 5), mientras que ip[6 : 2] & 0x1FFF = 0 indica solo datagramas no fragmentados o el último fragmento de los datagramas fragmentados.

Otros ejemplos sobre multicast:

--El filtro “ether multicast” es equivalente a “ether[0]&1!=0” para capturar tramas multicast (analiza el bit I/G de la dirección física)
--El filtro “ip multicast” es equivalente a “ip[16]&0xF0==0xE0”, tomando el byte 16 de la cabecera IP y comprobar que coincide con los primeros 4 bits de una dirección multicast “1110” o 0xE

[2] Esta expresión y las dos siguientes pueden ir precedidas de tcp o udp, para indicar que solo se desea el puerto correspondiente al protocolo tcp o udp.