Práctica 3: Manejo de herramientas de videoconferencia y vídeo streaming en transmisión unicast y multicast

Autores: Santiago Felici
Rogelio Montañana

En esta práctica se realizan pruebas con diversas herramientas de videoconferencia, vídeo streaming y vídeo bajo demanda, tanto en modo unicast como en modo multicast. También se llevan a cabo diversos experimentos de transmisión multicast 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 dotados de cámara de vídeo, auriculares y micrófono. Además los ordenadores deben tener instalados los siguientes paquetes de software:

- El programa **Ethereal** que se utiliza como analizador de tráfico. Este software es de dominio público y se puede obtener de www.ethereal.com.
- El programa **Netmeeting** de Microsoft. Es un software de videoconferencia H.323 (unicast) que viene incluído 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
- Tres herramientas del paquete MBone llamadas **SDR, RAT y VIC**. Es un software de videoconferencia con capacidad multicast, de libre distribución que puede obtenerse de http://www-mice.cs.ucl.ac.uk/multimedia/software/

1.- Preparación

En primer lugar los alumnos deben arrancar los ordenadores en el sistema operativo Windows (MS Windows 2000) y entrar con el usuario administrador y la password que indique el profesor.

A continuación conectarán la cámara de vídeo a una de las tomas USB que hay en la parte trasera de la caja del ordenador. No debe utilizarse la toma USB frontal del ordenador ya que las cámara no es reconocida correctamente por el hardware y no funciona. El micrófono (conector rojo) se debe conectar a la clavija que hay a la derecha del conector USB frontal y los auriculares (conector blanco) a la que hay a la izquierda del USB frontal. Los ordenadores que no dispongan de cámara no podrán realizar la emisión de vídeo, pero sí la recepción. Los que no dispongan de micrófono y auriculares no podrán realizar la emisión y recepción de audio.

Ahora los alumnos deben averiguar los siguientes datos de su ordenador:

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 seleccionar **'Ejecutar…'**. En el campo **'Abrir'** teclearán **`'cmd'`** y en la ventana que aparece teclearán el comando **`'ipconfig/all'`**.

Por último desactivarán el cortafuegos del software Office Scan. Para ello deben proceder de la siguiente forma:

A) Seleccionar '**Inicio'** -> '**Todos los programas**'
B) Seleccionar **'Trend Micro Office Client'**

C) Seleccionar **'OfficeScan Client'**
D) En la ventana que aparece seleccionar la pestaña **'Cortafuegos de cliente empresarial'**
E) Desmarcar la casilla **'Activar el cortafuegos'** y pulsar **'Aceptar'**
F) Responder **'Sí'** a la pregunta **'¿Está seguro …?'**
G) Pulsar **'Salir'**

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 si sigue sin funcionar debemos reiniciar el equipo y repetir el proceso a partir de ese punto.

2.- Pruebas de videoconferencia con Microsoft Netmeeting

El programa Netmeeting de Microsoft es un software de videoconferencia que funciona en los sistemas operativos Windows de dicho fabricante y que cumple 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.

Configuración del ancho de banda

Antes de establecer una conferencia vamos a explorar las posibilidades que nos brinda este software. 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 las cuales seleccionaremos la pestaña **'General'**; en ella podemos ver y modificar los datos identificativos del conferenciante. Para poder utilizar el Netmeeting debe aparecer como mínimo el Nombre, Apellido y 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 permite 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 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 regular 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. Pulsando el botón **'Avanzado'** accedemos a una ventana desde la cual se puede fijar manualmente el códec de audio utilizado. Los códecs entre los que se puede elegir en el Netmeeting 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).

<u>En todos los parámetros de audio dejaremos los valores por defecto.</u>

Configuración de vídeo

En la pestaña de **'Vídeo'** 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. 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. Nosotros seleccionaremos tamaño Grande. 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. En este caso dejaremos el valor por defecto.

Establecimiento de la conferencia

Una vez arrancado el programa Netmeeting y ajustados los parámetros cada alumno deberá ponerse de acuerdo con un compañero para establecer una videoconferencia entre ambos. Uno de ellos llamará al otro poniendo en la ventana de llamada la dirección IP o el nombre del otro ordenador. El otro recibirá una petición de llamada entrante que deberá aceptar, momento en el cual se establece la comunicación. Si todo funciona correctamente en unos pocos segundos ambos tendrán comunicación de audio y de vídeo. Si no aparece el vídeo seguramente será porque alguno de ellos no marcó 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 aceptará 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, solo pueden cambiarse cuando no hay una llamada en curso.

Captura de tráfico con Ethereal

Ahora los alumnos pondrán en marcha el programa Ethereal y realizarán capturas de tráfico estableciendo un filtro para poder analizar más cómodamente el tráfico de la conferencia. Para ello deben arrancar el programa Ethereal haciendo 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 **'ethereal'**. Si de esta forma tampoco se encuentra el programa consultaremos con el profesor. Una vez aparece la ventana Ethereal para configurar el filtro seleccionaremos en la parte superior el menú '**Capture**' y la opción **'Interfaces…'**; al aparecer la ventana '**Capture Interfaces'** debemos pulsar el botón **'Prepare'** en la interfaz que corresponde a la tarjeta Ethernet (en caso de que haya varias interfaces esta se reconoce fácilmente por ser la que tiene asociada la dirección IP del ordenador). A continuación aparece la ventana **'Capture options'**; en esta 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 establecemos la conferencia, por ejemplo **'host 147.156.123.32'**. Este filtro provoca que el Ethereal solo nos muestre los paquetes que tienen como origen o destino el ordenador con el que estamos estableciendo la conferencia. Si activamos la captura antes de efectuar la llamada podemos ver todos los paquetes intercambiados entre los hosts para el establecimiento de la comunicación. Entre los paquetes TCP intercambiados para el establecimiento de la comunicación se encuentran los correspondientes al protocolo de señalización de H.323, que es reconocido por el Ethereal. A la vista de la captura obtenida **los alumnos deben indicar cual es dicho protocolo**.

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 observarlo en más detalle. Sin embargo Ethereal no interpreta la cabecera RTP que viene a continuación, ya que al no tener reservado un número de puerto concreto Ethereal no puede determinar que es un paquete RTP. Para averiguarlo habría que analizar el flujo, cosa que Ethereal no intenta pues se limita a analizar los paquetes de forma individual. Pero si le decimos a Ethereal que un determinado paquete es RTP lo analizará y nos mostrará la estructura de su cabecera; además aplicará dicho análisis automáticamente a todos los paquetes que pertenezcan al mismo flujo, es decir que tengan la misma dirección IP de origen y destino y el mismo puerto de origen y destino. Para ello debemos proceder de la siguiente forma: en primer lugar elegiremos un paquete UDP que sepamos o supongamos que es RTP, después desplegaremos el menú **'Analyze'** y elegiremos la opción **'Decode As…'** la cual nos mostrará una larga lista de protocolos posibles; elegiremos RTP y a partir de ese momento Ethereal interpretará las cabeceras RTP. Así podremos ver algunas características de la comunicación.

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

- **¿Qué resolución se está utilizado 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?**

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'**[1] que nos muestra de manera gráfica y en escala porcentual el grado de ocupación de la tarjeta de red (recordemos que los ordenadores están conectados a un hub de 10 Mb/s). Utilizando esta herramienta los alumnos deben ahora hacer una estimación del caudal que envía el Netmeeting cuando se configura para 'Red de area local' y como cambia dicho caudal al cambiar 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, de forma que todos los cambios y pruebas los haremos desde el otro ordenador únicamente; de lo contrario sería preciso hacer todos los cambios en ambos ordenadores de forma sincronizada. Una vez hechas las pruebas con diferentes anchos de banda volveremos a poner el Netmeeting el valor inicial ('Red de area 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

[1] Esta pestaña sólo está disponible en Windows XP, no en Windows 2000.

cuando la imagen a transmitir es prácticamente la misma todo el tiempo (en realidad la imagen cambia más de lo que parece puesto que la iluminación con tubos fluorescentes provoca 50 destellos por segundo y esto afecta negativamente 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; aunque con los ordenadores actuales esta carga no es importante hace unos años resultaba ser a menudo 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. Para ello desplegaremos una vez más 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 ordenador del compañero con el que hemos realizado anteriormente las pruebas de Netmeeting. Esto provocará que nuestro Netmeeting enviará a esa dirección cualquier llamada que hagamos a direcciones E.164[2]. Como ya sabemos dicho ordenador no es un Gateway sino un simple terminal H.323, pero puesto que carecemos de un Gateway lo vamos a utilizar como sustituto. La consecuencia es que cuando dicho terminal recibe nuestra llamada la responde como si fuera dirigida a él. Esto lo podemos comprobar fácilmente, ya que si llamamos a cualquier dirección E.164 la llamada siempre irá a parar al Netmeeting de nuestro compañero.

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 aquí utilizaremos como sustituto de Gatekeeper el ordenador de nuestro compañero, ya que no disponemos de un Gatekeeper en el laboratorio. En primer lugar pondremos en marcha una captura con el Ehtereal definiendo el filtro '**dst host *dirección_IP***' donde ***'dirección_IP'*** es la de nuestro compañero; 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 lleguen de él (que serán las pruebas que realice nuestro compañero) 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 de nuestro compañero de pruebas (la misma que hemos puesto en el filtro del Ethereal). 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 de usuario que utilizaríamos para identificarnos como usuario autorizado ante el Gatekeeper, ya que el Gatekeeper normalmente tendrá acceso a un servidor de autenticación por medio del cual comprobará si el usuario es legítimo y si está autorizado a utilizar el servicio[3]. Una vez configurado todo lo anterior pulsaremos el botón '**Aceptar**' y observaremos que justo en ese momento el Ethereal empieza a capturar paquetes; pasados unos segundos recibimos el mensaje 'Tiempo de conexión del equipo selector agotado' y el Ethereal deja de capturar paquetes. Al recibir este mensaje pararemos la captura y analizaremos el tráfico capturado por el Ethereal. 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?**

[2] Las direcciones E.164 corresponden a los números de teléfono habituales. Están formadas por hasta 15 dígitos decimales sin ningún signo de puntuación.

[3] Obsérvese que con esta interfaz no es posible ocultar la password, que la password se conserva no encriptada y que cualquiera que tenga acceso al ordenador en un momento dado tiene acceso a la password.

- **¿Cuanto 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?**

3.- Pruebas básicas de multicast

En esta parte de la práctica vamos a realizar diversas pruebas y experimentos de transmisión multicast con el objetivo de familiarizarnos con su funcionamiento y mostrar algunas características interesantes. Para ello utilizaremos el comando ping y el analizador Ethereal.

Comprobación de la ruta para direcciones clase D

Antes de lanzar los ping vamos a comprobar que nuestro ordenador tiene soporte muticast. Dicha prueba consistirá en comprobar que existe una ruta defindа para las direcciones clase D. Esto lo haremos mediante el comando **`'route print'`** que ejecutaremos en una ventana de comandos que abriremos seleccionando 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'** tecleamos **`'cmd'`**. Veremos que en la lista de rutas que muestra aparece una a la red 224.0.0.0 con máscara 240.0.0.0. Esta 'red' corresponde precisamente a todo el rango de direcciones clase D. Veremos también que la puerta de acceso a dicha red es la dirección IP de nuestra interfaz Ethernet, lo cual significa que cuando nuestro host quiera enviar algún paquete a una dirección multicast lo hará directamente a través de dicha interfaz. También podemos ver que hay definida una ruta host (máscara de 32 bits) para la dirección broadcast (255.255.255.255) lo cual indica que los paquetes enviados a dicha dirección serán enviados también a la interfaz Ethernet. En una situación normal esto no tiene mucho interés, pero en el caso de que nuestro ordenador tuviera varias interfaces ethernet la configuración de estas rutas nos permitiría fijar por que interfaz (o interfaces) se enviarían los paquetes con direcciones de destino multicast o broadcast.

Para lanzar los pings que vienen a continuación podemos utilizar la misma ventana de comandos que hemos utilizado para el **`'route print'.`**

Prueba 1: ping a todos los hosts multicast (224.0.0.1)

La dirección 224.0.0.1 corresponde a todos los hosts multicast de una red (si tecleamos el comando 'nslookup 224.0.0.1' veremos que esa dirección se resuelve en el nombre 'ALL_SYSTEMS.MCAST.NET'). Por tanto si hacemos ping a dicha dirección debemos recibir tantas respuestas como hosts con soporte multicast hay en nuestra red, o mejor dicho en nuestra LAN ya que estos paquetes (como todos los dirigidos a direcciones 224.0.0.0/24) no son propagados por los routers. En este caso la LAN abarca todo el edificio donde se encuentra el laboratorio. Vamos a enviar un paquete de ping a dicha dirección mediante el comando **`'ping -n 1 224.0.0.1'`** (la opción **`'-n 1'`** indica que se envíe un solo paquete). Con este ping deberíamos recibir tantas respuestas como hosts con soporte multicast estén encendidos en estos momentos en nuestra LAN, pero como podremos comprobar recibimos una sola respuesta. Evidentemente hay más de un host con soporte multicast en nuestra red puesto que ya solo en el laboratorio donde nos encontramos hay más de una docena, todos con soporte multicast. Para averiguar lo que ocurre vamos a repetir el mismo ping, pero poniendo en marcha una captura en el Ethereal con el filtro **`'host`** ***`dirección_IP`*** **`and icmp'`** donde ***`'dirección_IP'`*** es la dirección IP de nuestro ordenador. Este filtro captura todo el tráfico ICMP con origen o destino nuestro ordenador, de forma que podremos ver con todo detalle el tráfico que realmente provoca nuestro ping. Así podremos ver que, en efecto, el ping genera múltiples respuestas, pero el programa ping de Windows solo reporta la primera e ignora el resto, probablemente para evitar 'confunidr' al usuario. Por el número de respuestas reflejadas en el Ethereal podremos saber, ahora sí, cuantos hosts con soporte multicast se encuentran encendidos y conectados en este momento en el edificio.

En el detalle mostrado por el Ethereal los alumnos deben ahora seleccionar el ping enviado por su ordenador (el primero que aparece en la ventana superior) y analizar dicho paquete. En particular deben observar la dirección MAC de destino, que debe ser 01:00:5E:00:00:01. Esta dirección corresponde al OUI

01-00-5E, que fue reservado para uso del IETF; el siguiente bit está a cero y los 23 restantes reproducen los 23 últimos bits de la dirección IP.

Prueba 2. ping a la dirección broadcast de nuestra red

Vamos a hacer ahora un ping a la dirección broadcast de la red en la que nos encontramos. Sería más fácil hacer ping a la dirección 255.255.255.255, pero Windows no lo permite. En cualquier caso el que vamos a hacer es completamente equivalente. Los alumnos deberán calcular dicha dirección a partir de la IP y máscara de su ordenador. Una vez obtenida la dirección broadcast deberán lanzarle un **'ping –n 1'**, poniendo previamente en marcha la captura del Ethereal con el filtro **'host *dirección_IP* and icmp'**. Tendremos el mismo comportamiento que antes, es decir el programa ping reporta una única respuesta, pero el Ethereal nos permite saber cuantas hay realmente. Ahora el número de respuestas recibidas corresponde al número de hosts con soporte del protocolo IP que están encendidos y conectados en este momento en el edificio. El número de respuestas debe ser ligeramente superior al de antes, ya que ahora deben contestar todos los hosts que tienen IP, con o sin soporte multicast; los que aparecen nuevos son los que no tienen soporte multicast[4]. Los alumnos deberán anotar los resultados obtenidos en ambos pings.

Normalmente los hosts sin soporte multicast corresponden a uno de los siguientes grupos:

- Impresoras con conexión LAN. Estos dispositivos se comportan como hosts en la red pero debido a su naturaleza no requieren soporte multicast.
- Equipos de red gestionables de nivel 1 (hubs) o de nivel 2 (conmutadores LAN). Tampoco requieren soporte multicast.
- Ordenadores cuyo sistema operativo no soporta multicast, por ejemplo MS Windows 95.

En la ventana del Ethereal los alumnos analizarán ahora el ping enviado por su ordenador (el primero de la lista) y observarán que la dirección MAC de destino es FF:FF:FF:FF:FF:FF, como sería de esperar; una consecuencia curiosa de esto es que, aunque el ping lo hemos enviado a la dirección broadcast de nuestra red IP, si existen en la LAN ordenadores de otra red IP también nos responderán. Lo mismo ocurría con el ping a la dirección 224.0.0.1, que también era respondido por todos los hosts multicast de la LAN, independientemente de la red a la que pertenecieran.

Prueba 3: ping broadcast a una red remota

Ahora vamos a realizar un envío a la dirección broadcast de otra red IP. Vamos a utilizar para ello la red 147.156.2.0/23, que corresponde a los ordenadores del Servicio de Informática. Como siempre primero pondremos en marcha el Ethereal con el filtro **'host *dirección_IP* and icmp'** y luego haremos **'ping –n 1 *direccion_IP*'** donde '***direccion_IP'*** será en este caso la dirección broadcast de la red 147.156.2.0/23. En esta red siempre hay al menos una docena de ordenadores encendidos, por lo que lo normal sería recibir varias respuestas. Sin embargo se recibe solo una respuesta, Esto se debe a que el router que tiene directamente conectada dicha red tiene configurado el comando **'no ip directed-broadcast'** para evitar ataques de ping broadcast desde el exterior. Por consiguiente cuando dicho router recibe un ping dirigido a esa red en vez de propagarlo a los hosts que están en ella responde el con un solo ping, actuando a modo de representante[5]. Se da circunstancia de que el router de esa red y el de la nuestra son el mismo router (es decir, ambas LANs están conectadas al mismo router), cosa que podemos descubrir si nos fijamos en la dirección IP del host que responde a nuestro ping. La configuración **'no ip directed-broadcast'** evita que se genere un tráfico en la red y una carga en los hosts que podrían provocar o facilitar la realización de ataques de denegación de servicio.

Prueba 4: ping a todos los routers multicast (224.0.0.2)y a otras direcciones reservadas

[4] Para que el cómputo fuera riguroso habría que haber hecho los dos pings al mismo tiempo, ya que entre uno y otro puede haberse encendido o apagado algún ordenador del edificio.

[5] Obsérvese que en le caso del ping de Windows el uso de **'no ip directed-broadcast'** pasa totalmente desapercibido para el usuario, ya que este recibe siempre una sola respuesta.

Ahora probaremos a enviar un ping a la dirección 224.0.0.2, que corresponde a todos los routers multicast (ALL_ROUTERS.MCAST.NET en nslookup), Como siempre utilizaremos el Ethereal con el filtro habitual (**'host *dirección_IP* and icmp'**) para saber el número de respuestas realmente recibidas.

Otras direcciones multicast reservadas son las siguientes (el nombre entre paréntesis corresponde al que le asigna el DNS a esa dirección, consultable con nslookup):

224.0.0.5	Routers OSPF (OSPF-ALL.MCAST.NET)
224.0.0.9	Routers RIP v2 (RIP2-ROUTERS.MCAST.NET)
224.0.0.10	Router con IGRP/EIGRP (IGRP-ROUTERS.MCAST.NET)
224.0.0.13	Routers PIM v2 (PIM-ROUTERS.MCAST.NET)
224.0.0.22	Mensajes Membership Report de IGMP v3 (IGMP.MCAST.NET)
224.0.1.1	NTP (Network Time Protocol) (NTP.MCAST.NET)
224.0.1.41	Gatekeepers H.323 (GATEKEEPER.MCAST.NET)
224.2.127.254	Anuncio de sesiones SAP, Session Announcement Protocol (SAP.MCAST.NET)

Haciendo ping a cada una de estas direcciones y con la ayuda del Ethereal responde a las siguientes preguntas:

- ¿Cuantos routers OSPF, RIP v2, IGRP/EIGRP y PIM v2 hay en la LAN del edificio?
- ¿Cuantos hosts tienen soporte de IGMP v3 en la LAN del edificio?
- ¿Cuantos hosts estan en el grupo multicast de servidores de tiempo NTP en la red de la Universidad?
- ¿Cuántos Gatekeepers H.323 hay ahora mismo accesibles en la Internet?
- ¿Cuántos hosts estan en este momento participando del anuncio de sesiones de SAP en Internet?

Recuerda que las direcciones 224.0.0.0/24 siempre tienen restringido su ámbito a la red local (TTL=1). En cambio las direcciones 224.0.1.0/24 se propagan por toda la Internet. La dirección 224.0.1.1 es una excepción a esta regla, ya que está filtrada por el router de salida de la Universidad de Valencia.

Resulta interesante, en el caso del ping a las direcciones 224.0.1.41 y 224.2.127.254, activar antes de la captura la función de resolución de nombres de Ethereal. Para ello hay que seleccionar en el menú 'Capture' la opción 'Options' y marcar la casilla 'Enable network name resolution'. De esta forma podemos hacernos una idea de la ubicación fisica de los hosts que están respondiendo a nuestros pings.

La primera vez que se hace ping a las direcciones 224.0.1.41 y 224.2.127.254 el número de respuestas obtenidas puede ser muy pequeño. A partir del segundo ping el número de respuestas obtenidas es mucho mayor y constante. Probablemente esto se debe a que el primer ping no se difunda adecuadamente por no estar completamente establecido el árbol de distribución desde el emisor (nuestro host) a los miembros de ese grupo multicast en toda la Internet.

En realidad el grupo 224.2.127.254 tiene en la Internet muchos más participantes de los que han respondido a nuestro ping. Lo que ocurre es que la mayoría simplemente no responde a los mensajes ICMP enviados a dicho grupo multicast. Generalmente solo los routers responden a esos pings.

Prueba 5: Exploración del tráfico multicast no IP en la red

Ahora vamos a analizar con el Ethereal el tráfico multicast no IP que recibe nuestro ordenador. Si utilizamos el filtro **'multicast and not ip'** capturamos no solo el tráfico multicast sino tambien el broadcast que es abrumadoramente mayoritario por culpa del ARP. Para evitarlo usaremos en su lugar el filtro **'multicast and not broadcast and not ip'**. Al poner la captura en marcha observaremos que se obtienen paquetes de multitud de protocolos diferentes. Los alumnos deberán:

- **Identificar al menos tres de dichos protocolos. ¿Tienen algún significado especial las direcciones MAC utilizadas por esos protocolos?**

? **También deberán calcular el ratio aproximado de paquetes por segundo obtenidos[6].**

Una vez hecha esta prueba repetirán la captura con el mismo filtro, pero cuidando esta vez de desmarcar en la ventana '**Capture options**' la casilla **'Capture packets in promiscuous mode'**. Observarán los paquetes capturados en esta segunda prueba y estimarán el ratio en paquetes por segundo capturados. Deberán explicar los resultados obtenidos y las diferencias que hayan observado entre ambas capturas.

4.- Pruebas con las herramientas MBone (SDR, VIC, RAT)

Las herramientas MBone son un conjunto de programas que permiten realizar videoconferencias multicast a través de Internet. El software es de libre distribución y puede obtenerse de http://www-mice.cs.ucl.ac.uk/multimedia/software/. De la multitud de herramientas disponibles nosotros utilizaremos el SDR, el VIC y el RAT.

SDR (Session Directory) permite crear y anunciar sesiones multicast, así como unirnos a otras ya existentes. Es la aplicación principal ya que actúa como gestor de las demás herramientas y es la única que se invoca directamente, el resto son normalmente utilizadas a través del SDR. El VIC es la herramienta de video y el RAT la de audio

Recibir la lista de emisiones de Internet con SDR

Para ejecutar el SDR debemos hacer doble clic en el icono correspondiente, o bien seleccionar **'Inicio'** -> **'Todos los programas'**, de la lista seleccionar '**Mbone Tools**' y una vez allí '**sdr**'. A continuación aparece una ventana con la lista de sesiones. Para ver una sesión la seleccionamos mediante doble clic. Las sesiones que podemos ver son realmente una parte muy pequeña del total, ya que la mayoría están anunciadas pero no activas y de las que están activas la mayoría utiliza codecs que no tienen el VIC ni el RAT. Una de las sesiones que puede seguirse y casi siempre está activa es la 'UO Presents KWAX Classical Radio', una emisora de radio de la Universidad de Oregón. Si la seleccionamos el SDR arrancará el RAT y podremos recibirla (esta emisión es solo de audio).

Ahora cerraremos la ventana SDR y arrancaremos el Ethereal con un filtro para capturar únicamente los paquetes destinados a la dirección 224.2.127.254. Esta es la dirección del protocolo de anuncio de sesiones SAP (Session Announcement Protocol). De momento nuestro ordenador no recibe ningún paquete de ese tipo. A continuación arrancaremos el SDR como antes y veremos que empezamos a recibir gran cantidad de paquetes y que dicho flujo es constante. Parando la captura podremos analizar alguno de ellos y observaremos que contienen información detallada sobre las diferentes sesiones que aparecen anunciadas en la ventana del SDR. Estos mensajes se envían periódicamente con el fin de que si aparece un nuevo participante en la red reciba en unos pocos minutos la información de todas las sesiones anunciadas. El primer mensaje capturado no debería ser un anuncio SDR sino un IGMP Membership Report enviado por nuestro host al grupo multicast del SDR (224.2.127.254) para unirse a él.

Realizar emisiones propias con SDR

Nuestro mayor interés en relación con las herramientas Mbone no es ver las emisiones que llegan del exterior, sino realizar emisiones multicast propias.

Aunque es posible crear una sesión diferente en cada ordenador, resulta más interesante crear sesiones compartidas. Por tanto para esta parte de la práctica los alumnos se organizarán en grupos de tres o cuatro ordenadores, según lo indique el profesor, que compartirán una misma sesión. Un ordenador de cada grupo será el encargado de crear la sesión y el resto se unirá a ella.

Para crear la sesión seleccionaremos en la ventana de sesiones del SDR '**New**' y a continuación '**Create advertised session**'. Entramos entonces en un diálogo con varias etapas:

[6] Para esto podemos usar el tiempo relativo de captura qua aparece en la primera columna, que nos premite saber de forma trivial el tiempo que ha durado la captura que hemos efectuado.

0. En la etapa 0 asignaremos a cada sesión un nombre; utilizaremos como nombre de sesión el de nuestro ordenador (p. ej. Lab3inf012); además le asignaremos una descripción (es obligatorio asignar una).
1. En la etapa 1 elegiremos el valor por defecto (sesión tipo Test).
2. En la etapa 2 también elegiremos los valores por defecto (sesión de dos horas de duración a empezar de forma inmediata).
3. En la etapa 3, '**Select the Distribution Scope**', elegiremos 'IPv4 Local Scope' con lo que se nos asignará una dirección del rango 239.255.0.0/16 que tiene restringido el alcance al ámbito local.
4. En la etapa 4 elegiremos audio y vídeo. Si no nos permite seleccionar alguno de estos dos medios es que no ha reconocido el hardware correspondiente (tarjeta de sonido o cámara USB).
5. En la etapa 5 '**Provide Contact Details**' podemos dejar los valores por defecto.
6. En la etapa 6 '**Select security parameters for this session**' también podemos dejar los valores por defecto.

A continuación aparece una pantalla resumen ('**Review session details**') donde ya podemos ver las direcciones multicast que el SDR ha asignado al flujo de vídeo y de audio. Estas direcciones las elige el SDR de froma que sean únicas en toda la red, para evitar conflicto con otras sesiones anunciadas o activas. Como hemos elegido ámbito local el SDR nos asigna direcciones del rango 239.255.0.0/16, de lo contrario nos habría asignado direcciones del rango 224.2.0.0/16, reservado por el IANA para el SDR.

Una vez dados todos los datos pulsaremos el botón '**Aceptar**' y a partir de ese momento veremos aparecer nuestra sesión en la ventana SDR. La sesión aparecerá también en todos los ordenadores del laboratorio (no solo los de nuestro grupo) ya que periódicamente estamos enviando un mensaje multicast de anuncio de nuestra sesión a todo el ámbito donde tiene lugar la emisión (en nuestro caso la LAN).

Una vez creada la sesión cualquier ordenador puede unirse a ella simplemente seleccionándola de la lista que muestra la ventana de SDR. Aunque hemos acordado entre nosotros dividirnos en grupos de tres o cuatro ordenadores el SDR las sesiones no tienen asignado grupo a priori y cualquier ordenador puede unirse a cualquier sesión, no hay ningún mecanismo que impida a un participante recibir, o incluso emitir, en una sesión que no sea la suya.

Para unirnos a una sesión debemos hacer clic en ella y en la ventana que aparece hacer click en '**Join**'. Como SDR ha asignado una dirección multicast diferente al audio y al vídeo nos da opción de unirnos independientemente a cada uno de ambos medios. Si nos unimos al vídeo el SDR arrancará el programa VIC y si nos unimos al audio arrancará el RAT. También podemos unirnos a ambos.

Al arrancar el vídeo (VIC) veremos aparecer una pequeña ventana por cada emisión en curso (si es que ya hay alguna). Para generar nuestra propia emisión seleccionaremos el menú '**Transmit**' y en '**Device…**' el dispositivo '**USB camera**'. Después pulsaremos el botón '**Transmit**' y a partir de ese momento estaremos emitiendo vídeo. Podemos utilizar los mandos del '**Rate Control**' para regular el caudal (en Kb/s) y el número de fotogramas por segundo que generamos. En la parte del 'Encoder' podemos indicar el formato de compresión de vídeo de entre varias posibilidades, entre las que se encuentra el jpeg (M-JPEG) el H.261, el H.263 y el H.263+, con formato pequeño, normal o grande. Algunos de los codecs que aparecen (por ejemplo M-JPEG) no están disponibles pues requieren asistencia por hardware que nuestro ordenador no tiene. El control de calidad nos permitirá establecer un compromiso entre el número de fotogramas por segundo y la calidad de cada fotograma, intentando en todo momento no superar el caudal fijado en 'Rate Control'.

En la ventana VIC podemos ver en ventanas miniatura las emisiones de vídeo que se están realizando en nuestro grupo multicast. Cada emisión indica la dirección IP del emisor, el caudal que está generando en Kb/s, la tasa de pérdidas (en %) y el número de fotogramas por segundo. Podemos elegir una de dichas emisiones para verla en una ventana de mayor tamaño; esta ventana puede configurarse para que conmute automáticamente por voz, lo cual es especialmente interesante para conferencias multipunto. Desde el momento en que nos unimos a la sesión de vídeo nuestro ordenador está recibiendo todos los flujos de vídeo que se producen, independientemente de que ampliemos o no alguno de ellos, puesto que todos emiten en el mismo grupo multicast y por tanto no podemos seleccionar uno para recibirlo de forma aislada en nuestro ordenador. Para que esto fuera posible cada flujo de vídeo debería tener una dirección multicast diferente y para esto cada uno debería estar definido en una sesión SDR diferente.

En la ventana de RAT (audio) podemos pulsar en la ventana el botón '**Options**' con lo que aparece una nueva ventana; en ella el botón '**Category**' muestra un desplegable que tiene varias opciones; si elegimos la que pone '**Codecs**' podremos ver una lista completa de los codecs soportados y su descripción detallada. En RAT existen gran cantidad de codecs, desde el L16-48K-Stereo (16 bits por muestra, 48000 muestras por segundo, dos canales, sin comprimir), que ocupa 1536 Kb/s, hasta el LPC-8K-Mono (8000 muestras por segundo, un canal comprimido) que ocupa 5,6 Kb/s. Para cada codec el RAT asigna un tamaño por defecto de la carga útil del paquete RTP ('RTP payload'), que puede ser modificado por el usuario. El tamaño de la carga útil permite fijar un compromiso entre el overhead introducido por las cabeceras (que aconseja paquetes grandes) y el retardo de paquetización (que aconseja paquetes pequeños).

Ahora los alumnos deben identificar las direcciones IP utilizadas por cada una de las emisiones multicast que están teniendo lugar en el laboratorio. Con el Ethereal definirán un filtro de forma que capturen únicamente el tráfico correspondiente a la emisión que están realizando desde su ordenador. Deberán analizar los paquetes capturados, observar las direcciones MAC de origen y destino, las direcciones IP de origen y destino y las cabeceras RTP (utilizando como antes la función **'Decode As…'** del Ethereal).

Como es bien sabido un protocolo fundamental para el funcionamiento de IP multicast es el IGMP (Internet Group Management Protocol). Ahora los alumnos deben definir un filtro en el Ethereal para capturar únicamente los mensajes IGMP que se produzcan en la red. Con el filtro definido probarán a unirse y abandonar las emisiones en curso a fin de provocar el envío de mensajes IGMP y poder analizarlos con detalle. Mediante dicho análisis deberán responder a las siguientes preguntas:

- **¿Qué código se utiliza en el campo protocolo de la cabecera IP para indicar IGMP?**
- **¿Cómo se distingue si es IGMP v1, v2 ó v3? ¿Qué versión estamos utilizando?**
- **¿Va escrita en algún sitio del mensaje IGMP la dirección multicast sobre la que se aplica el comando?**

Como ya hemos visto SDR realiza el anuncio de sesiones mediante el protocolo SAP (Session Announcement Protocol) que utiliza la dirección 224.2.127.254.

- **¿Con que filtro podríamos saber si estamos enviando a la red mensajes de dicho protocolo, y con que frecuencia enviamos dichos mensajes?**
- **¿Qué hosts están enviando los mensajes SDR? ¿Todos? ¿Solo los que emiten audio o vídeo? ¿Solo el que anunció la sesión en primer lugar?**
- **Si paramos la emisión de audio y vídeo en nuestro ordenador, pero mantenemos la recepción ¿dejamos completamente de transmitir en ese grupo multicast? ¿Cómo podríamos comprobarlo?**

5.- Pruebas con VideoLAN

VideoLAN es un software de dominio público que permite realizar distribución de vídeo streaming por Internet. El software incorpora tanto las funciones de servidor como de cliente.

Recibir la lista de emisiones de Internet con VideoLAN

Antes de arrancar el VideoLAN pondremos en marcha con el Ethereal una captura de los paquetes dirigidos a 224.2.127.254 para poder observar como cambia la recepción de dichos paquetes cuando arranquemos VideoLAN.

Para ejecutarlo simplemente buscaremos el icono de nombre 'VLC media player' y haremos doble clic en él, o bien seleccionaremos **'Inicio' -> 'Todos los programas'** y de la lista elegiremos '**VideoLAN**' y una vez allí '**VLC media player'**. En la ventana de VLC media player que aparece elegiremos el menú desplegable '**Ver**' y en este la opción '**Lista de Reproducción'**. En la nueva ventana elegiremos el menú **'Administrar',** iremos a '**Servicios discovery'** y elegiremos '**Anuncios de SAP'** En ese momento veremos que el Ethereal empieza a capturar paquetes, y aparece una entrada desplegable 'SAP' en la lista. Si la abrimos veremos una lista de canales que va creciendo a medida que recibimos mensajes SAP. Ahora pararemos la captura

del Ethereal y veremos que, salvo el primer mensaje que corresponde al IGMP 'Membership Report' de nuestro host al grupo de SAP, todo lo demás son anuncios de sesiones como los que recibíamos con el SDR.

En la lista la mayoría de las entradas corresponden a canales de televisión, casi todos utilizando codecs MPEG. Hay también algunos canales de radio que utilizan MP3. La lista es similar al directorio de sesiones que veíamos con el SDR; la principal diferencia es que el VideoLAN está preparado para emisiones de vídeo streaming y que aquí algunas emisiones están agrupadas. Uno de los grupos que siempre suele estar activo es el BELNET (red de investigación belga).

Recibir una emisión de televisión multicast con VideoLAN

Ahora probaremos a 'sintonizar' uno de los canales y luego lo pararemos con los mandos que aparecen en la parte superior de la ventana. En una ventana pondremos en marcha antes el 'Administrador de Tareas' de Windows con la pestaña 'Funciones de red' para poder observar el tráfico en la red (solo Windows XP). Para evitar problemas debidos a un tráfico excesivo en la red todos los alumnos harán las pruebas con el mismo canal, que les indicará el profesor; un buen candidato es el canal BELNET-IAD-CRAPS del grupo BELNET que normalmente está siempre activo; se trata de un canal de dibujos animados que emite un caudal MPEG-2 de unos 3,5 Mb/s (calidad broadcast, 720x576 de resolución). Como se puede comprobar los únicos mandos de control del vídeo que funcionan son el de parar y reproducir, al tratarse de un vídeo multicast no es posible utilizar el avance o retroceso rápidos. Ahora pondremos en marcha un filtro con el Ethereal para capturar solo los paquetes IGMP que envía nuestro ordenador. Con la captura del Ethereal en marcha arrancaremos y pararemos varias veces el vídeo que estábamos viendo, a continuación pararemos la captura y analizaremos los resultados obtenidos para intentar responder a las siguientes preguntas:

- **¿Cuanto tarda la red en dejar de enviarnos el flujo multicast cuando paramos el vídeo?**
- **¿Cuánto tarda en enviárnoslo nuevamente cuando lo volvemos a solicitar?**
- **¿Qué mensaje envía nuestro ordenador cuando paramos el vídeo?**
- **¿Qué mensaje envía nuestro ordenador cuando arrancamos el vídeo?**
- **¿Que dirección multicast está utilizando la emisión de vídeo que estamos recibiendo?**
- **¿Sería posible recibir únicamente el audio de dicha emisión por multicast?**

Sabida la dirección que utiliza la emisión vamos a configurar ahora en el ethereal el filtro adecuado para que se capture solo ese tráfico multicast. Cuando hayamos conseguido capturar unos cuantos paquetes de dicho tráfico vamos a analizarlo para responder a las siguientes preguntas:

- **¿Quién es el emisor del vídeo?**
- **¿A que formato o codec pertenece la emisión?**
- **Analizando una secuencia de 20 paquetes ¿Se aprecia pérdida o cambio de orden de los paquetes en recepción?**

Provocar una situación de saturación y descarte de paquetes en la red con VideoLAN

Ahora todos los alumnos sintonizarán el canal 'BELNET-GEANT-MOVIE', también en el grupo BELNET. Este es un canal promocional de la red académica europea Geant que emite vídeo MPEG-2 con calidad HDTV (televisión de alta definición, resolución 1920x1152), que genera un caudal de unos 9 Mb/s. Como los ordenadores del laboratorio están todos conectados a un hub de 10 Mb/s, esto casi satura la red local, pero si no hay ninguna otra actividad funciona correctamente. Afortunadamente al ser una emisión multicast los paquetes solo se envían una vez independientemente del número de receptores. Resulta interesante monitorizar en tiempo real durante la recepción el tráfico con el Administrador de Tareas de Windows (pestaña 'Funciones de Red', solo disponible en Windows XP) para observar el caudal que está generando en la red la recepción de dicho flujo. También se puede monitorizar (XP o 2000) la carga de CPU que genera la decodificación del vídeo. Ahora uno de los alumnos a indicación del profesor recibirá un canal de los que emiten a 3,5 Mb/s (por ejemplo el BELNET-IAD-CRAPS). El caudal resultante superará ahora los 10 Mb/s, con lo que al cabo de unos segundos ambas emisiones empezarán a perder paquetes y la calidad del vídeo y el audio se degradará a niveles inaceptables.

6.- Realizar emisiones de vídeo streaming en multicast

Además de poder recibir emisiones el VideoLAN permite realizar emisiones de vídeo unicast o multicast. No es sin embargo una herramienta de vídeoconferencia como las de MBone que hemos probado anteriormente. 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 cámaras de vídeo o tarjetas sintonizadotas el vídeo se ha de comprimir en tiempo real mientras se captura, para poder emitirlo en el formato elegido. VideoLAN dispone de varios codecs 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 organizarse en grupos de dos 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 debe tener auriculares.

Las pruebas las haremos emitiendo desde cada servidor a una dirección IP multicast diferente. Suponiendo que nuestro servidor tiene la dirección IP **147.156.x.y** utilizaremos la dirección multicast **239.255.x.y**. De esta forma nos aseguramos de que no habrá duplicidad de direcciones. Por otro lado al utilizar direcciones 239.255.0.0/16 nos aseguramos de que nuestras pruebas no salen de la LAN (pues este rango de direcciones está siempre confinado a la LAN).

En primer lugar vamos a poner 'a la escucha' al cliente de la emisión mutlicast. Como todas las pruebas de emisión las hacemos con la misma dirección multicast, no necesitaremos tocar nada en el cliente una vez lo hayamos puesto 'a la escucha' en dicha dirección. Por supuesto en la práctica el cliente podría ir cambiando de dirección multicast y 'sintoniando' los diferentes 'canales' de las emisiones en curso.

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 Multiemisión**'. En ese momento se habilitan los campos '**Dirección**' y '**Puerto**'.
6- En el campo '**Dirección**' poner la dirección que utilizará el servidor para la emisión multicast (la 239.255.x.y donde x.y son los dos últimos bytes de la dirección IP del servidor). El campo '**Puerto**' debe quedar con su valor por defecto (1234).
7- Pulsar el botón '**OK**'
8- El cliente está listo para recibir cualquier emisión que se produzca en la dirección 239.255.x.y.

A partir de este momento el cliente ya está preparado para recibir cualquier emisión multicast que ocurra en esa dirección y la tarjeta de red está preparada para capturar cualquier trama ethernet cuya dirección MAC de destino coincida con la MAC de mapeo de la dirección IP que hemos seleccionado.

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 de salida'** y pulsar el botón **'Opciones'**.
7- En la ventana '**Volcado de salida**' marcar la casilla '**UDP**'. . En ese momento se habilitan los campos '**Dirección**' y '**Puerto**'.
8- En el campo '**Dirección**' poner la dirección que utilizará el servidor para la emisión multicast (la 239.255.x.y donde x.y son los dos últimos bytes de la dirección IP del servidor). 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 multicast.

Como puede comprobarse fácilmente, durante la emisión los botones de control de vídeo del cliente no funcionan, salvo el de parada/arranque del vídeo. El servidor tampoco puede utilizar dichos botones, pero dispone de un mando deslizante con el que puede controlar la posición del vídeo que se está emitiendo.

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 anterior a través de una red de enlaces de 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 constante la dirección IP de la emisión multicast, 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 trasncodificación 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 de salida'** y pulsar el botón **'Opciones'**.
7- En la ventana '**Volcado de salida**' marcar la casilla '**UDP**'.
8- En el campo '**Dirección**' poner la dirección (239.255.x.y). 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 si emitimos todo el tiempo en la misma dirección multicast (239.255.x.y) no es necesario realizar ninguna modificación en los clientes, pues estos se limitarán a reproducir el vídeo que les enviemos, independientemente de su origen, códec, resolución, caudal, etc.

Para poder efectuar una emisión de vídeo en directo es necesario hacer uso de las opciones de transcodificación, ya que esta es la manera de indicarle a VideoLAN el formato de audio y vídeo que queremos generar. Vamos a hacer ahora una prueba utilizando 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 '**Video Blaster WebCam 3 (WDM)**'. 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 de salida'** y pulsar el botón **'Opciones'**.
9- En la ventana '**Volcado de salida**' marcar la casilla '**UDP**'.
10- En el campo '**Dirección**' poner la dirección (239.255.x.y). 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 multicast.

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 con el parámetro '**Escala**' en la transcodificación).

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').

Ataque de denegación de servicio en una emisión multicast

A diferencia del SDR el VideoLAN no está preparado para recibir dos emisiones diferentes en la misma dirección multicast. Si lo hace intenta reproducirlas como si fueran una sola, con lo que no se recibe correctamente ninguna de ambas. Vamos a comprobarlo emitiendo simultáneamente desde dos servidores a la misma dirección multicast.

Para esta prueba se deben agrupar dos parejas servidor-cliente. Para el correcto funcionamiento de esta prueba es importante que los servidores no tenga abierto ningún cliente, por tanto los servidores deberán terminar el proceso VideoLAN cliente que tenían activo y mantener únicamente el servidor. Ambos servidores emitirán en la misma dirección multicast, que será la de uno de ellos elegida de mutuo acuerdo. Ambos clientes deben recibir esa dirección multicast, uno ya la tendrá por lo que solo será necesario cambiarla en el otro, con el procedimiento utilizado anteriormente:

1- Seleccionar el menú '**Archivo:F**'
2- Elegir la opción '**Abrir Aparato de Captura…**'
3- En la ventana '**Abrir…**' seleccionar la pestaña '**Red**'
4- En la lista de botones seleccionar '**UDP/RTP Multiemisión**'.
5- En el campo '**Dirección**' poner la dirección multicast (239.255.x.y)
6- Pulsar el botón '**OK**'
7- El cliente está listo para recibir cualquier emisión que se produzca en la dirección 239.255.x.y.

Una vez preparados los clientes pondremos en marcha las dos emisiones, una en cada servidor. Para una utilizaremos el vídeo 'Ethernet.mpg' que ya conocemos, y para la otra el vídeo 'Carmen-1m.mpg', que tiene las siguientes características:

? vídeo: MPEG-4, resolución 720x576, 25 fps, 1024 Kb/s
? audio: MPEG-1 capa II, frec. muestreo 48 KHz, 2 canales (estéreo), 192 Kb/s

(Este es el mismo vídeo que utilizábamos antes, pero con el caudal de vídeo reducido a 1024 Kb/s para que la red no presente problemas de saturación al emitir múltiples flujos en paralelo.)

Para emitir cada vídeo seguiremos el procedimiento ya conocido:

1- Seleccionar el menú '**Archivo:F**'
2- Elegir la opción '**Abrir Volcado de Red…: N**'
3- En la ventana '**Abrir…**' seleccionar la pestaña '**Archivo**'
4- Pulsar el botón '**Explorar**' y seleccionar el fichero correspondiente ('Ethernet.mpg' o 'Carmen.mpg')
5- Marcar la casilla **'Volcado de salida'** y pulsar el botón **'Opciones'**.
6- En la ventana '**Volcado de salida**' marcar la casilla '**UDP**'
7- En el campo '**Dirección**' poner la dirección multicast (239.255.x.y)
8- Asegurarse de desmarcar las casillas '**Códec de vídeo**' y '**Códec de audio**' (para estas pruebas no utilizaremos transcodificación)
9- Pulsar el botón '**OK**'
10- Empieza la emisión multicast.

Cuando empieza la primera emisión el cliente reproduce el vídeo correctamente. Al empezar la segunda el cliente intenta reproducir los paquetes de ambos vídeos según le llegan. Como cada uno tiene una resolución diferente la imagen cambia continuamente de tamaño, el sonido se pierde y solo se produce de vez en cuando un chasquido. Si tenemos en marcha el Administrador de Tareas de Windows veremos que el uso de la CPU aumenta considerablemente como consecuencia del intento por decodificar los paquetes de ambos vídeos entrelazados como si fueran uno solo. Si la situación se mantiene durante algún tiempo el programa VideoLAN puede caer en un error fatal que le hace terminar de manera abrupta (por este motivo hemos suprimido el VideoLAN cliente en los servidores).

Este sencillo experimento nos muestra con que facilidad es posible sabotear, intencionadamente o por accidente, una emisión multicast. Si el cliente de VideoLAN nos hubiera permitido especificar el emisor habríamos podido seleccionar uno de los dos vídeos y reproducirlo correctamente. Esto es lo que se conoce como SSM (Source Specific Multicast). Obsérvese que, aunque el SSM nos permitiría visualizar únicamente el vídeo que nos interesa la tarjeta de red nos estaría pasando ambos flujos a la CPU, pues su filtrado es por la dirección MAC de destino y esta es idéntica para ambas emisiones.

En todas las pruebas de emisión que hemos realizado mediante VideoLAN hemos asignado estáticamente las direcciones multicast. En este caso dicha labor era sencilla puesto que las emisiones estaban confinadas a la LAN, pero si quisiéramos realizar emisiones de duración limitada en toda la Internet lo lógico sería haber dejado que el protocolo SAP asignara dinámicamente las direcciones multicast, como hicimos en el caso del SDR. Ya hemos visto en el apartado anterior al recibir emisiones del exterior que VideoLAN también puede hacer uso de SAP, aunque nosotros no hemos utilizado esa funcionalidad en las pruebas de emisión que hemos realizado.

7.- Finalización

Al terminar la práctica los alumnos deben reactivar el cortafuegos que desactivaron al principio. Para ello deben proceder de la siguiente forma:

11- Seleccionar '**Inicio'** -> '**Todos los programas**'
12- Seleccionar **'Trend Micro Office Client'**
13- Seleccionar **'OfficeScan Client'**
14- En la ventana que aparece seleccionar la pestaña **'Cortafuegos de cliente empresarial'**
15- Marcar la casilla **'Activar el cortafuegos'** y pulsar **'Aceptar'**
16- Pulsar '**Salir**'

ANEXO I: Filtros en ethereal.

En Ethereal es posible construir filtros que determinen si un determinado paquetes van a ser o no capturado. 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>

Primitiva	Descripción
net <red> mask <mascara>	Verdad si las dirección de origen o destino del paquete corresponde a una dirección de la <red> de máscara <mascara>
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>[7]	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 cabecer IP y comprobar que coincide con los primeros 4 bits de una dirección multicast “1110” o 0xE

[7] 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.