

Pràctica 1: Videoconferència i vídeo streaming en unicast

(Versió setembre 2011)

Autor: Rogelio Montañana

1.- Introducció i objectius

En aquesta pràctica es realitzen proves amb diverses ferramentes de videoconferència i vídeo streaming en mode unicast, amb l'objecte que l'alumne es familiaritze amb el seu funcionament.

Per al desenvolupament de la pràctica s'utilitzen ordinadors amb sistema operatiu MS Windows XP que han de tenir instal·lats els següents paquets de software:

- El programa **WireShark** que s'utilitza com a analitzador de trànsit. Aquest software és de domini públic i es pot obtenir de www.wireshark.org.
- El programa **Netmeeting** de Microsoft. És un software de videoconferència H.323 (unicast) que ve inclòs amb el sistema operatiu MS Windows en les seues diverses variants.
- El programa **VideoLAN**, que serveix per enviar i rebre emissions de vídeo en IP. És un software de lliure distribució que pot funcionar en unicast i en multicast i que es pot obtenir de www.videolan.org

Alguns ordinadors estan dotats de càmera de vídeo (Webcam), micròfon i auriculars, altres sols tenen micròfon i auriculars.

2.- Preparació

En primer lloc els alumnes han d'organitzar-se per treballar en equips de dos o tres persones. Cada equip utilitzarà una maqueta formada per dos ordinadors, al menys un dels quals ha de tenir càmera, auriculars i micròfon. L'altre ordinador pot tenir sols auriculars i micròfon.

Després arrencaran els ordinadors en el sistema operatiu Windows XP i entraran amb l'usuari i el password que indique el professor.

A continuació connectaran la càmera de vídeo a una de les connexions USB de l'ordinador, i de la mateixa manera també el micròfon i els auriculars a les diferents clavilles. Cal connectar els dispositius aprofitant les connexions de la part posterior de la caixa de l'ordinador. Els ordinadors que no disposen de càmera no podran realitzar l'emissió de vídeo, però sí la recepció. Els que no disposen de micròfon no podran realitzar l'emissió d'àudio.

Ara els alumnes hauran d'esbrinar les següents dades dels seus ordinadors:

Dada	Ordinador 1	Ordinador 2
Nom		
Adreça MAC		
Adreça IP		
Màscara		
Router per defecte		

Per a això seleccionaran amb el ratolí l'icona '**Inici**' en la part inferior esquerra de la pantalla i en el menú desplegable seleccionaran '**Executar...**'. En el camp '**Obrir**' teclejaran '**cmd**' i en la finestra que apareix teclejaran el comandament '**ipconfig /all**'. De la resposta a eixe comandament obtindran totes les dades requerides excepte el nom. Per esbrinar el nom utilitzaran el comandament '**nslookup adreça_IP**' on '**adreça_IP**' serà l'adreça IP que han esbrinat prèviament.

Per últim desactivaran el tallafocs (de Windows) què hi haja a l'ordinador.

Nota: Si en algun moment de la pràctica es produeixen comportaments estranys en algun equip, o els resultats d'alguna prova no són els esperats, s'ha de revisar detingudament totes les opcions i passos realitzats. Si a pesar d'això la prova segueix sense funcionar pot ser convenient reiniciar l'equip i repetir el procés a partir d'eixe punt.

3.- Proves de videoconferència amb Microsoft Netmeeting

El programa Netmeeting de Microsoft és un software de videoconferència que funciona en els sistemes operatius Windows que compleix amb els estàndards H.323 de la ITU-T. Per ficar-lo en marxa simplement farem doble clic sobre la icona corresponent, que ha d'estar en l'escriptori. En cas que no trobem la icona seleccionarem amb el ratolí la icona '**Inici**' en la part inferior esquerra de la pantalla, en el menú desplegable seleccionarem '**Executar...**' i en el camp '**Obrir**' teclejarem '**conf**', abreviatura de 'conference', que és el nom que rep l'executable del programa Netmeeting. D'aquesta forma executem el procés de configuració del Netmeeting, com a resultat del qual apareix una icona en l'escriptori.

Configuració de l'ample de banda

Abans d'establir una conferència anem a explorar les possibilitats que ens brinda el Netmeeting. Per a això seleccionem en la finestra del programa el menú desplegable '**Ferramentes**' i d'ell elegirem l'última opció anomenada '**Opcions**', amb la qual cosa ens apareix una finestra amb diverses pestanyes. D'aquestes seleccionarem la pestanya '**General**'; en ella podem veure i modificar les dades identificatives del conferenciant. Per poder utilitzar el Netmeeting han d'aparèixer com a mínim el Nom, Cognom i l'adreça de correu electrònic. En la part inferior de la finestra trobem un botó que fica '**Configuració de l'ample de banda**'. Si el polsem apareixerà una nova finestra que ens permetrà indicar la velocitat de la connexió a la xarxa, d'entre quatre possibilitats:

- Mòdem de 14,4 Kb/s
- Mòdem de 28,8 Kb/s
- Cable, xDSL ó RDSI
- Xarxa d'àrea local

Aquesta dada la utilitza el Netmeeting per fixar el cabdal màxim que ha de generar durant la conferència, el cabal pot ser menor si les característiques del vídeo i àudio ho permeten. Nosaltres elegirem l'opció '**Xarxa d'àrea local**' que és la que ens permet utilitzar major ample de banda (uns 450 Kb/s) i per tant ens ofereix major qualitat.

Configuració d'àudio

A continuació tornarem a la finestra d'opcions i polsarem la pestanya '**Àudio**' on podrem seleccionar diverses característiques, tals com l'ajust automàtic de volum del micròfon o la detecció automàtica de silenci. L' '**Ajust d'àudio**' serveix per ajustar el volum d'àudio a un nivell adequat, mitjançant una prova de nivell. Polsant el botó '**Avançat...**' accedim a la finestra '**Configuració de compressió avançada**' en la que marcarem la casella '**Establir manualment la configuració de compressió**' per poder explorar els còdecs que ens ofereix el Netmeeting, que són els següents:

- El G.723.1 amb els seus dos possibles cabals, 6.4 o 5.3 Kb/s
- Un còdec ADPCM propietari de Microsoft amb mostres de 4 bits i un cabdal de 32 Kb/s
- Els dos còdecs G.711 que existeixen, amb l'escala segons la llei 'mu' i segons la llei 'A'. Ambdós corresponen a un cabal de 64 Kb/s, per tant se tracta d'àudio no comprimit. Aquestos apareixen descrits com '**Llei u de CCITT**' i '**Llei A de CCITT**' (encara que la CCITT passà a anomenar-se ITU-T en 1993 Microsoft ha decidit utilitzar en aquest cas la denominació antiga).

Una vegada explorats els còdecs haurem de desmarcar la casella '**Establir manualment la configuració de compressió**'. La selecció automàtica és més còmoda ja que la manual requereix que ambdós participants trien el mateix còdec per a que la comunicació per àudio siga possible. Una vegada desmarcada aquesta casella tornarem a la finestra 'Àudio', on deixarem tots els paràmetres d'àudio amb els seus valors per defecte.

Configuració de vídeo

Ara polsarem la pestanya **‘Vídeo’**. En aquesta podem indicar si volem que sempre que s'estableix una comunicació s'envie vídeo, i si estem interessats en rebre vídeo automàticament a l'inici de cada cridada. Devem marcar ambdues caselles. El vídeo requereix amplitud de banda elevats i per eixe motiu el seu ús es considera opcional; en canvi l'àudio sempre s'envia, si el terminal ho suporta ja que és obligatori en H.323. A continuació tenim uns botons tipus 'radi' que ens permeten fixar el **‘Tamany d'imatge d'enviament’**; açò és senzillament la resolució de la imatge de vídeo que anem a transmetre (la que rebem la controla l'altre participant). Existeixen tres possibilitats anomenades **‘Petit’**, **‘Mig’** i **‘Gran’** que corresponen als formats SQCIF (128x96), QCIF (176x144) i CIF (352x288), respectivament. Nosaltres seleccionarem tamany Gran. El programa ens permet elegir qualsevol resolució independentment de l'ample de banda que tinguem, per exemple podríem seleccionar el format CIF amb mòdem de 14.4 Kb/s, encara que en eixe cas cada fotograma tardaria diversos segons en transmetre's amb la qual cosa el vídeo seria poc àgil. En la finestra de vídeo també podem indicar si volem enviar un vídeo **‘De millor qualitat’** o un **‘Més ràpid’**; ací el que fa el programa és intentar ajustar el número de fotogrames per segon que s'envien, de forma que en el primer cas sacrifica agilitat de moviment (fotogrames per segon) a favor de la qualitat d'imatge i en el segon procedeix al contrari, tractant de no superar en cap cas el cabal corresponent a l'ample de banda elegit. Per exemple en el cas d'estar transmetent les diapositives d'una presentació seria recomanable elegir el vídeo de millor qualitat ja que la imatge tindrà poc moviment. Nosaltres deixarem el valor per defecte.

Establiment de la conferència

Ara seleccionarem la pestanya **‘General’** i a continuació polsarem el botó **‘Cridada avançada...’** amb el que ens apareix la finestra d' **‘Opcions avançades de cridada’**. En aquesta finestra devem assegurar-nos que estiguen desmarcades les caselles **‘Usar un equip selector...’** i **‘Usar una porta d'enllaç...’**. Si aquestes caselles estan marcades no és possible establir conferències amb altres ordenadores.

Ara els alumnes provaran a realitzar una cridada i establir una videoconferència entre els dos ordinadors del seu equip. La cridada la faran des d'un dels ordinadors ficant en la finestra de cridada l'adreça IP o el nom de l'altre ordinador. L'altre ordinador rebirà la petició de cridada entrant que haurà d'acceptar, moment en el qual s'estableix la comunicació. Si tot funciona correctament en uns pocs segons hi haurà entre ambdós comunicació d'àudio i de vídeo (limitat per la disponibilitat de càmeres i micròfons/auriculars dels ordinadors). Si no apareix el vídeo segurament serà perquè no estan marcades les opcions corresponents en la finestra **‘Ferramentes’** -> **‘Opcions’** -> **‘Vídeo’**. Açò pot resoldre's polsant el botó Iniciar/Detindre vídeo, que es troba en la part esquerra de la finestra de Netmeeting (just dalt de la paraula 'Nom' de la llista de participants). Amb aquest botó cada conferenciant controla l'emissió del seu vídeo i la recepció del remot.

El Netmeeting pot configurar-se per a que accepte cridades automàticament. Per a això desplegarem el menú **‘Cridar’** i elegirem l'opció **‘Acceptar cridades automàticament’**. D'aquesta manera el Netmeeting accepta de forma immediata qualsevulla cridada entrant.

Alguns paràmetres de Netmeeting, per exemple la resolució de vídeo, es poden canviar en qualsevol moment durant una conferència. Altres, com per exemple el Ample de banda, poden canviar-se durant la conferència però la modificació sols té efecte a partir de la següent cridada. Per últim alguns paràmetres, com el còdec d'àudio (en el cas que s'haja configurat per a selecció manual), sols poden canviar-se quan no hi haja una cridada en curs. Observem per últim que el Netmeeting no permet una comunicació en grup, és una ferramenta de comunicació entre dos participants exclusivament.

Captura de trànsit amb WireShark

Ara els alumnes ficaran en marxa en ambdós ordinadors el programa WireShark i realitzaran captures de trànsit establint un filtre per poder analitzar més còmodament el trànsit de la conferència. Per a això han d'arrancar-lo fent doble clic sobre la icona 'WireShark', que està en el escriptori. En cas que no trobem la icona seleccionarem amb el ratolí la icona **‘Inici’** en la part inferior esquerra de la pantalla, en el menú desplegable seleccionarem **‘Executar...’** i en el camp **‘Obrir’** teclejarem **‘Wireshark’**. Si d'aquesta forma tampoc s'executa el programa consultarem amb el professor. Una vegada apareix la finestra

WireShark per configurar el filtre seleccionarem en la part superior el menú '**Capture**' i l'opció '**Interfaces...**'.

En aquesta opció apareixeran totes les interfícies instal·lades en el PC. Per exemple normalment apareixerà una interfície anomenada '**Adapter for Generic Dialup ...**' que correspon a la interfície sèrie del host (COM1) i la interfície Ethernet (el nom variarà depenent de la targeta de xarxa), que és sobre la que discorre el nostre trànsit (podria haver més d'una si l'ordinador té diverses targetes de xarxa). De totes les interfícies que apareixen haurem d'utilitzar la que té assignada l'adreça IP del nostre ordinador, que com podem comprovar pel comptador de paquets és la que està rebent el trànsit de la xarxa. En aquesta mateixa finestra, si pressionem el botó **options** associat a la nostra interfície o mitjançant el menú **capture i després options** (si haguéssim tancat la finestra d'interfícies inicial) anirem al camp '**Capture Filter:**' i teclejarem el filtre '**host adreça_IP**' on '**adreça_IP**' és l'adreça IP del host remot amb el que hem establert la conferència, per exemple '**host 147.156.103.32**'. Aquest filtre provoca que el WireShark sols capture i ens mostre els paquets que tenen com a origen o destinació l'ordinador amb el que estem establint la conferència. Hem d'activar la captura abans d'efectuar la cridada per veure tots els paquets intercanviats entre els hosts durant l'establiment de la comunicació. Entre ells es troben els corresponents al protocol de senyalització de H.323, que és reconegut pel WireShark.

- **A la vista de la captura obtinguda els alumnes han d'indicar quin és el protocol de senyalització utilitzat en H.323 (pista: el seu nom comença per Q).**

Una vegada establerta la comunicació el majoria del trànsit és UDP, que és la forma com s'envia la informació d'àudio i vídeo. Seleccionant un d'eixos paquets UDP podem amb l'ajuda del WireShark analitzar-lo amb més detall. Malgrat tot, WireShark no interpreta la capçalera RTP que està situada després de la capçalera UDP, ja que el protocol RTP no té un número de port reservat, com ocorre amb altres com HTTP i SMTP. Per a que WireShark analitzi el contingut d'un paquet RTP li ho haurem d'indicar. Açò ho podem fer seleccionant un d'eixos paquets, després despleguem el menú '**Analyze**' i elegim l'opció '**Decode As...**' la qual ens mostrarà una llarga llista de protocols possibles; elegirem de tots ells RTP i a partir d'eixe moment WireShark interpretarà les capçaleres RTP, no sols del paquet que hem seleccionat sinó les de tots els paquets que corresponen al mateix fluxe, és a dir que tinguen la mateixa adreça IP d'origen i destinació i el mateix port d'origen i destinació, ja que se suposa que tots eixos paquets són també RTP. Així podem veure algunes característiques de la comunicació.

Els alumnes ara hauran d'analitzar un paquet RTP amb informació de vídeo i utilitzar-lo per respondre a les següents preguntes:

- **¿Quina resolució s'està utilitzant per transmetre i per rebre vídeo? (pot no ser la mateixa en ambdós sentits)**
- **¿Quin còdec s'està utilitzant per a vídeo?**
- **¿Quin còdec s'està utilitzant per a àudio? ¿Amb quin cabal?**

Si se transmet àudio i vídeo la quantitat de paquets de vídeo es considerablement major que la d'àudio, per la qual cosa si volem capturar paquets d'àudio és convenient establir una conferència sense vídeo. També devem tenir en compte que la supressió de silencis fa que sols es transmeten paquets quan es parla, per la qual cosa en capturar àudio cal suprimir-la o assegurar-nos de parlar durant la conferència.

Monitorització del trànsit generat

Una altra experiència interessant és monitoritzar el trànsit que estem generant en la xarxa durant la conferència. Per a això utilitzarem l' '**Administrador de Tasques**' de Windows (pulsar Alt-Ctrl-Supr) i seleccionarem la pestanya '**Funcions de xarxa**' que ens mostra de manera gràfica i en escala percentual el grau d'ocupació de la targeta de xarxa (per interpretar correctament el significat dels valors que apareixen hem de recordar que els ordinadors estan connectats a un switch de 100 Mb/s). Utilitzant aquesta ferramenta els alumnes ara han de fer una estimació del cabal que envia el Netmeeting quan es configura per a 'Xarxa d'àrea local' i com canvia eixe cabal que envia el Netmeeting quan es configura per a 'Xarxa d'àrea local' i com canvia cabal en modificar l'ample de banda en la configuració (per a que el canvi faci efecte és precis establir de nou la conferència). La millor forma de fer aquestes proves es configurar un

Netmeeting per a que no emeta vídeo i per a que accepti automàticament les cridades entrants, de forma que tots els canvis i proves els farem des de l'altre ordinador únicament, contràriament seria necessari fer tots els canvis cada vegada en ambdós ordinadors de forma sincronitzada. Una vegada fetes les proves amb diferents amplituds de banda tornarem a ficar el Netmeeting en el valor inicial ('Xarxa d'àrea local') i amb la gràfica de **'Funcions de xarxa'** en pantalla farem el següent experiment: deixarem la càmera enfocada a una imatge estàtica durant uns segons fins que el cabal transmès s'estabilitzi clarament, segons podrem apreciar per la gràfica, segons podrem apreciar per la gràfica, aleshores provocarem un moviment en la imatge, per exemple passant alguna cosa per davant de la càmera i veurem com es modifica el cabal per aquest motiu. Haurem d'apreciar clarament en la gràfica els moments en que es produeix moviment davant de la càmera. Açò és un clar exemple de l'eficiència dels algorismes de compressió de vídeo, que permeten reduir el cabal de forma apreciable quan la imatge a transmetre és pràcticament la mateixa tot el temps (en realitat la imatge estàtica canvia més del que pareix ja que la il·luminació amb tubs fluorescents provoca 50 flaixos per segon i açò afecta als algorismes de compressió de vídeo).

En l'Administrador de Tasques també podem observar el consum de CPU que produeix la codificació/descodificació del vídeo, amb els ordinadors actuals aquesta càrrega no és important, però fa uns pocs anys es convertia en el factor limitant de la qualitat quan s'utilitzaven cabals elevats.

Configuració d'un Gateway (porta d'enllaç)

Ara anem a fer una prova de configurar el nostre Netmeeting per a que utilitzi un Gateway, anomenat 'porta d'enllaç' en la versió en castellà del software. Quan se té configurada una porta d'enllaç l'usuari pot cridar no sols a adreces IP sinó també a adreces E.164, és a dir a números de telèfon (les adreces E.164 són simples seqüències d'entre 1 i 15 dígits decimals). Se suposa que el terminal H.323 dirigirà totes les cridades que fem a adreces E.164 cap a la porta d'enllaç, que serà la encarregada de transferir-les a la xarxa telefònica. Com no disposem d'una vertadera porta d'enllaç anem a configurar-li com a porta d'enllaç a cada ordinador del laboratori l'altre ordinador amb el que fa les proves. D'aquesta forma quan cridem a una adreça E.164 la cridada l'enviarem a l'ordinador del nostre company, qualsevol que siga el número al que cridem.

Abans de configurar la porta d'enllaç provarem a efectuar una cridada a una adreça E.164 qualsevol, per exemple '12345'. Veurem que Netmeeting ens torna un missatge indicant que no ha pogut trobar eixe nom de persona en el servidor de directori. En no tindre configurada porta d'enllaç Netmeeting interpreta qualsevol seqüència de caràcters que no siga una adreça IP vàlida com a un nom que ha de buscar en el directori.

Ara configurarem la porta d'enllaç. Per a això desplegarem novament el menú **'Ferramentes'**, elegirem l'opció **'Opcions'** i en la finestra corresponent polsarem el botó de **'Cridada avançada'**. Veurem aparèixer una finestra en la part inferior de la qual podem donar la configuració de la porta d'enllaç. Seleccionarem primer la casella **'Usar una porta d'enllaç...'** i després teclejem en el camp **'Porta d'Enllaç'** l'adreça IP de l'altre ordinador de la nostra maqueta, amb el que estem realitzant les proves de Netmeeting.

A continuació repetirem la cridada a la mateixa adreça E.164 d'abans ('12345' o la que siga). Ara l'ordinador redirigirà la cridada a l'adreça IP de l'altre ordinador, que és la que té configurada com a porta d'enllaç. Però com que eixe ordinador rep una cridada H.323, que no pot transferir realment a la xarxa telefònica, la respon ell directament. Podem comprovar que, qualsevol que siga l'adreça E.164 que fiquem, la cridada sempre la rep l'ordinador que tenim configurat com a porta d'enllaç.

Configuració d'un Gatekeeper (equip selector)

Ara anem a fer una prova consistent en configurar el nostre Netmeeting per a que faci ús d'un Gatekeeper, anomenat 'equip selector' en la versió en castellà. De nou com no disposem d'un Gatekeeper real utilitzarem com Gatekeeper imaginari l'altre ordinador de la nostra maqueta. Però per poder analitzar els missatges que enviem ficarem abans en marxa una captura amb el WireShark definint el filtre **'dst host adreça_IP'** on **'adreça_IP'** és la de l'altre ordinador de la nostra maqueta. Açò ens permetrà analitzar tots els paquets que enviem a eixe ordinador; les respostes no ens interessen ja que en no tindre l'ordinador realment funcions de Gatekeeper no va a respondre als nostres missatges i els que ens envie seran únicament les proves que realitzi el nostre company en sentit contrari, que ens podrien confondre.

Una vegada tenim en marxa la captura configurem el Gatekeeper de la següent forma: entrem en **‘Ferramentes’** -> **‘Opcions’** -> **‘Cridada avançada’** i una vegada allí seleccionem la casella de la part superior que diu **‘Usar un equip selector...’**. En seleccionar aquesta opció automàticament es desactiva la corresponent a la **‘Porta d’Enllaç’** ja que ambdues són incompatibles i la d’Equip Selector té precedència. Com equip selector ficarem l’adreça de l’altre ordinador de la nostra maqueta (la mateixa que hem ficat en el filtre del WireShark). A continuació seleccionarem la casella **‘Iniciar la sessió usant el meu nom de compte’** i teclejarem en el camp **‘Nom de compte’** una combinació d’usuari i password separats pel caràcter **‘#’** (per exemple **‘pepito#secreta’**); aquest seria el codi que utilitzaríem per identifiquem com a usuari autoritzat davant el Gatekeeper, el qual normalment accediria en eixe moment a un servidor d’autenticació per comprovar que l’usuari és legítim i està autoritzat a utilitzar el servei¹. Una vegada configurat l’anterior pulsarem el botó **‘Acceptar’** i observarem que just en eixe moment el WireShark comença a capturar paquets; després de diversos intents i passats uns segons rebem el missatge **‘Temps de connexió de l’equip selector esgotat’** i el WireShark deixa de capturar paquets. En rebre eixe missatge pararem la captura i analitzarem el trànsit capturat pel WireShark. Per mig d’eixe anàlisi respondrem a les següents preguntes:

- **¿A quin protocol pertanyen els missatges que s’envien al Gatekeeper?**
- **¿Quants intents de connexió realitza el nostre equip?**
- **¿Quant de temps s’espera entre intents consecutius?**
- **¿Quina informació viatja en els paquets que s’envien al Gatekeeper?**
- **¿Què ocurreria si hi hagués un NAT entre el nostre ordinador i el Gatekeeper?**
- **¿Com s’envia la informació d’usuari#password que hem teclejat? ¿Pot eixa informació ser capturada per gent estranya?**

4.- Realitzar emissions de vídeo streaming amb VideoLAN

El VideoLAN és un programa que permet realitzar emissions de vídeo unicast o multicast. No és una ferramenta de videoconferència com el Netmeeting. Anem ara a explorar les possibilitats d’aquest software per establir un servidor de vídeo streaming en una xarxa.

El vídeo streaming pot servir-se des de múltiples fonts, per exemple:

- Fitxers del disc dur
- DVDs muntats en el lector de l’ordinador
- Càmeres de vídeo connectades a l’ordinador
- Targetes sintonitzadores de televisió terrestre o via satèl·lit

En el cas d’imatges en disc dur o DVD el vídeo i l’àudio tenen ja un format comprimit en origen, per la qual cosa la tasca de VideoLAN es limita a generar els fluxes i enviar-los per la xarxa. En el cas de càmeres de vídeo o targetes sintonitzadores el vídeo s’ha de comprimir en temps real mentre se captura, per poder emetre’l en el format elegit. VideoLAN disposa de diversos còdecs de vídeo. En el cas d’una emissió de vídeo prèviament comprimit (disc dur o DVD) és possible fer transcodificació en temps real, per adaptar l’emissió a l’ample de banda disponible en la xarxa. Anem a veure totes aquestes possibilitats per ordre.

Preparació

Per a aquestes proves els alumnes han de treballar també per parelles d’ordinadors, un dels quals actuarà como a servidor de vídeo i l’altre com a client. Els únics requisits són que el servidor ha de tenir càmera i el client auriculars.

Les proves les farem emetent des del servidor al client.

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.

En primer lloc anem a ficar 'a l'escolta' al client. Com totes les proves d'emissió les farem des del servidor no necessitarem tocar res en el client una vegada l'hem ficat a escoltar. De fet el client queda a servei del servidor, que pot enviar-li el vídeo que vulga, sense que el client pugui seleccionar res excepte decodificar o no el fluxe que rep.

El procediment per arrancar el client VideoLAN és el següent:

- 1- Arrancar el programa '**VLC media player**' mitjançant doble clic en la icona corresponent.
- 2- Seleccionar en la finestra que apareix el menú '**Archivo:F**'
- 3- Elegir de la llista l'opció '**Obrir Aparell de Captura...**'
- 4- En la finestra '**Obrir...**' seleccionar la pestanya '**Xarxa**'
- 5- En la llista de botons radio seleccionar '**UDP/RTP**'. El número de port ha de coincidir amb l'utilitzat pel servidor; utilitzarem el valor per defecte de '**1234**'.
- 6- Pulsar el botó '**OK**'
- 7- El client està llest per rebre qualsevol emissió que li arribi al port 1234, vinga d'on vingui.

En realitat no seria necessari utilitzar dos ordinadors per provar el VideoLAN, ja que en el propi servidor podem executar simultàniament una instància de VideoLAN configurat com a client. Anem doncs, seguint el procediment anterior, a arrancar un altre client en l'ordinador que actua de servidor. Açò és interessant perquè ens permetrà seguir localment, a mode de monitor, l'emissió que estem realitzant. La reproducció que realitza aquest client és realment obtinguda de la xarxa, no subministrada internament per l'ordinador, pel que permet detectar problemes en l'emissió, inclús a nivell físic; per exemple si se desconnecta el cable de xarxa del servidor la reproducció d'aquest client es para com la de qualsevol altre.

Emissió de vídeo streaming

La primera prova que farem consistirà en emetre des del servidor un vídeo que es troba en el disc dur, concretament en l'escriptori. El fitxer s'anomena 'Ethernet.mpg' i es tracta d'un vídeo de 10 minuts de duració amb les següents característiques:

- vídeo: MPEG-1, resolució 352x288 (SIF), 25 fps (fotogrames per segon), 1500 Kb/s
- àudio: MPEG-1 capa II, freq. mostreig 44,1 KHz, 2 canals (estèreo), 224 Kb/s

El fluxe total és per tant de 1,7 Mb/s aproximadament.

El procediment per ficar en marxa l'emissió en el servidor VideoLAN és el següent:

- 1- Arrancar el programa '**VLC media player**' mitjançant doble clic en la icona corresponent.
- 2- Seleccionar el menú '**Arxiu :F**'
- 3- Elegir de la llista l'opció '**Obrir Volcat de Xarxa.... N**'
- 4- En la finestra '**Obrir...**' seleccionar la pestanya '**Arxiu**'
- 5- Pulsar el botó '**Explorar**' i seleccionar el fitxer corresponent ('Ethernet.mpg')
- 6- Marcar la casella '**Volcat/Salvar**' i pulsar el botó '**Opcions**'.
- 7- En la finestra '**Volcat de sortida**' marcar la casella '**RTP**'. En eixe moment s'habiliten els camps '**Adreça**' i '**Port**'.
- 8- En el camp '**Adreça**' ficar l'adreça del client que ha de rebre el vídeo streaming. El camp '**Port**' ha de quedar amb el seu valor per defecte (1234).
- 9- Pulsar el botó '**OK**' en la finestra '**Volcat de sortida**'
- 10- Pulsar el botó '**OK**' en la finestra '**Obrir...**'.
- 11- Comença l'emissió de vídeo streaming.

Com pot comprovar-se fàcilment, durant l'emissió els botons de control de vídeo del client no funcionen, excepte el de parada/arranc del vídeo. Malgrat tot, el servidor pot controlar el vídeo amb els botons pause, play, retrocedir, etc.

Un mateix servidor podria distribuir simultàniament diversos fluxes de vídeo al mateix o a diferents clients. Per a això seria prou amb executar diferents instàncies del programa. En el cas de realitzar

diferents emissions cap al mateix client haurien d'utilitzar-se números de port diferents ja que sinó els fluxes arribaran mesclats i no serà possible veure correctament el vídeo.

Emissió de vídeo streaming amb transcodificació

Anem a provar ara les facilitats de transcodificació que ens ofereix el VideoLAN. La transcodificació ens permet convertir un fluxe o fitxer multimèdia canviant el còdec utilitzat, la resolució, el cabal, ... Suposem que necessitem difondre el vídeo de l'exemple cap a un client la connexió del qual fos de sols 256 Kb/s. Caldria reduir dràsticament el cabal, possiblement canviant a un còdec més eficient, baixant la resolució del vídeo o passant l'àudio d'estèreo a monoaural. En el nostre cas anem a emetre ara el vídeo amb els següents paràmetres:

- Còdec de vídeo: H.263
- Taxa de bits (kb/s): 128
- Resolució: SIF (352x288) (la mateixa que el vídeo original)
- Còdec d'àudio: MPEG-1 capa III
- Taxa de bits (kb/s): 64
- Canals: 1 (monoaural)

En el client no serà necessari realitzar cap canvi, sempre i quan es mantinga el mateix número de port, ja que la transcodificació es realitza exclusivament en el servidor. El client es limitarà a reproduir els fluxes d'àudio i vídeo que li arriben, fent ús dels còdecs i resolució elegits en el servidor (recordem que cada paquet d'informació multimèdia du escrita en la capçalera RTP la informació relativa al tipus de còdec utilitzat).

El procediment per realitzar una emissió amb transcodificació és molt semblant al d'una emissió normal. Tant sols cal emplenar a més en la finestra 'Volcat d'eixida' les opcions de transcodificació que es volen aplicar. Anem a descriure'l en detall:

- 1- Arrencar el programa '**VLC media player**'.
- 2- Seleccionar el menú '**Arxiu:F**'
- 3- Elegir de la llista l'opció '**Obrir Volcat de Xarxa...: N**'
- 4- En la finestra '**Obrir...**' seleccionar la pestanya '**Arxiu**'
- 5- Pulsar el botó '**Explorar**' i seleccionar el fitxer corresponent ('Ethernet.mpg')
- 6- Marcar la casella '**Volcat/Salvar**' i pulsar el botó '**Opcions**'.
- 7- En la finestra '**Volcat de sortida**' marcar la casella '**RTP**'.
- 8- En el camp '**Adreça**' ficar com abans l'adreça de l'altre ordinador. Deixar el camp '**Port**' amb el seu valor per defecte (1234).
- 9- Marcar la casella '**Còdec de vídeo**'. Seleccionar '**h263**'. En 'Taxa de bits (kb/s)' seleccionar '**128**'. En '**Escala**' deixar el valor per defecte (1).
- 10- Marcar la casella '**Còdec d'àudio**'. Seleccionar '**mp3**'. En 'Taxa de bits (kb/s)' seleccionar '**64**'. En '**Canals**' seleccionar '**1**'.
- 11- Pulsar el botó '**OK**' en la finestra '**Volcat de sortida**'
- 12- Pulsar el botó '**OK**' en la finestra '**Obrir...**'.
- 13- Comença l'emissió multicast.

La degradació de la qualitat, sobretot en el vídeo, és evident.

Realment pretén enviar una resolució SIF amb 128 Kb/s és excessiu. Amb aquest cabal s'hauria aconseguit millor qualitat baixant la resolució a QSIF (176x144). La resolució de vídeo la podem canviar en la transcodificació mitjançant el paràmetre '**Escala**'. Anem ara a repetir el procediment anterior mantenint tots els paràmetres igual excepte la '**Escala**' per a la que seleccionarem ara '**0.5**', que vol dir la meitat de resolució en cada dimensió, és a dir QSIF en aquest cas. Ara veurem el mateix vídeo en format més petit, però amb major qualitat.

Ara anem a fer una segona prova de transcodificació, però aquesta vegada utilitzarem el fitxer 'Carmen.mpg' que es troba en l'escriptori. Aquest vídeo, de tres minuts de durada té les següents característiques:

- vídeo: MPEG-2, resolució 720x576, 25 fps, 4500 Kb/s
- àudio: MPEG-1 capa II, freq. mostreig 48 KHz, 2 canals (estèreo), 192 Kb/s

Primer anem a emetre aquest vídeo sense modificacions. Com el vídeo suposa un cabal d'uns 4.7 Mb/s en quant hi haja tres emissions simultànies hi haurà saturació de la xarxa i la qualitat es degradarà. A continuació farem una emissió transcodificada, però abans de ficar en marxa l'emissió arrencarem l' 'Administrador de tasques' de Windows per monitoritzar l'ús de la CPU i observar així la càrrega que suposa la tasca de transcodificació en temps real.

Per realitzar la transcodificació procedirem com abans, però aquesta vegada aplicarem els següents paràmetres:

- Còdec de vídeo: **mp4v** (MPEG-4)
 - Taxa de bits (kb/s): **384**
 - Escala: **0,75** (resolució 540x432)
- Còdec d'àudio: **mp3** (MPEG-1 capa III)
 - Taxa de bits (kb/s): **96**
 - Canals: **2**

Amb aquest cabal (480 Kb/s) hauria d'haver unes 17-18 emissions simultànies per a que hi hagués problemes en la xarxa.

No tots els còdecs que es poden seleccionar funcionaran, alguns no tenen el programa corresponent incorporat en el VideoLAN. En particular els còdec que no funcionen en l'emissió des de fitxer són 'DIV1 o 'theo' en vídeo i 'vorb', 'flac', 'spx' 's16l' i 'fl32' en àudio.

Emissió de vídeo en directe

Com dèiem abans, a més de poder emetre vídeo prèviament comprimit VideoLAN també pot utilitzar com a entrada qualsevol font de vídeo habitual, com càmeres o targetes sintonitzadores de televisió. Nosaltres farem ara una prova amb les càmeres de vídeo de les que disposem.

Com en els casos anterior controlarem tota l'emissió des del servidor, per la qual cosa no serà necessari realitzar cap modificació en el client, que es limitarà a reproduir el vídeo que li enviarem, independentment del seu origen, còdec, resolució, cabal, etc.

En el cas d'una emissió de vídeo en directe és obligatori utilitzar les opcions de transcodificació, ha que aquesta és la manera de indicar-li a VideoLAN el format d'àudio i vídeo que volem generar. Per a això anem a utilitzar el següent procediment:

- 1- Arrencar el programa '**VLC media player**'.
- 2- Seleccionar el menú '**Arxiu:F**'
- 3- Elegir de la llista l'opció '**Obrir Volcat de Xarxa.... N**'
- 4- En la finestra '**Obrir...**' seleccionar la pestanya '**DirectShow**'
- 5- En la línia on apareix '**Nom de l'aparell de vídeo**' pulsar el botó '**Refresh list**', desplegar la llista que apareix a l'esquerra i seleccionar l'opció que coincideix amb vostre tipus de càmera. Si no apareix aquesta opció hem de pulsar novament el botó '**Refresh list**' fins que aparega.
- 6- En la línia on apareix '**Nom de l'aparell d'àudio**' deixar l'opció que apareix ('**Per Defecte**').
- 7- Comprovar que no estiguen marcades las casellas '**Propietats de l'aparell**' i '**Propietats del sintonitzador**'.
- 8- Marcar la casella '**Volcat/Salvar**' i pulsar el botó '**Opcions**'.
- 9- En la finestra '**Volcat de sortida**' marcar la casella '**RTP**'.
- 10- En el camp '**Adreça**' ficar l'adreça del client. Deixar el camp '**Port**' amb el seu valor per defecte (1234).
- 11- Marca la casella '**Còdec de vídeo**'. Seleccionar '**mp1v**'. En 'Taxa de bits (kb/s)' seleccionar '**512**'. En '**Escala**' deixar el valor per defecte (1).
- 12- Marcar la casella '**Còdec d'àudio**'. Seleccionar '**mp3**'. En 'Taxa de bits (kb/s)' seleccionar '**64**'. En '**Canals**' seleccionar '**1**'.
- 13- Pulsar el botó '**OK**' en la finestra '**Volcat de sortida**'
- 14- Pulsar el botó '**OK**' en la finestra '**Obrir...**'.

15- Comença l'emissió.

Si tot ha funcionat correctament l'emissió inclou tant vídeo com àudio. Com podem comprovar fàcilment el retard introduït per la codificació és de diversos segons, encara que açò depèn de la complexitat del còdec utilitzat. La resolució de la càmera que estem utilitzant és de 320x240 i 30 fps. La resolució pot reduir-se en la transcodificació amb el paràmetre '**Escala**'.

Podem utilitzar qualsevol còdec de vídeo o àudio dels que apareixen en la llista desplegable, excepte els que no estan implementats, que són en aquest cas: 'DIV1', 'h263' i 'theo' en vídeo i 'vorb', 'flac' 'spx', 's161' i 'fl32' en àudio.

Si en lloc d'elegir el còdec MPEG-1 elegim el H.264 veurem com l'ús de CPU augmenta considerablement per tractar-se d'un còdec de gran complexitat. (Utilitzeu per veure'l l' 'Administrador de tasques').

Seria possible establir una comunicació per videoconferència bidireccional entre dos ordinadors mitjançant el VideoLAN, encara que aquest programa no està pensat per a això, com el Netmeeting. Observem que el VideoLAN ofereix un servei no orientat a connexió on el servidor envia el seu fluxe d'àudio/vídeo sense saber ni tant sols si el client l'està rebent. A més el retard introduït pel procés de codificació fa difícil mantenir una interacció entre els participants.

8.- Finalització

En acabar la pràctica els alumnes han de reactivar el tallafocs que desactivaren al principi.

ANNEX I: Filtres en WireShark.

En WireShark és possible construir filtres que determinen si un determinat tipus de paquets va a ser capturat o no. En cas de que no s'utilitze cap filtre, tots els paquets són capturats.

Els filtres es construeixen mitjançant expressions que consisteixen en una o més primitives. Les primitives, usualment, consisteixen en un identificador (nom o número), precedides per un o més qualificadors. Existeixen tres tipus diferents de qualificadors:

- De tipus: Identifiquen un nom o adreça, els seus possibles valors són *host*, *net* i *port*. Per exemple, 'host glup.uv.es', 'net 147.156', 'port 20'. Si no existeix cap qualificador de tipus, s'assumeix que el tipus és host.
- D'adreça: Identifiquen una adreça particular de transferència, açò és, un origen o destinació. Els seus valors possibles són *src*, *dst*, *src or dst* i *src and dst*. Per exemple, 'src glup.uv.es', 'dst net 147.156', 'src or dst port ftp-data'. Si no s'indica cap qualificador d'adreça, es pren el qualificador d'adreça per defecte (src or dst).
- De protocol: Identifiquen un protocol particular. Els seus valors possibles són ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp i udp. Per exemple, 'ether src glup.uv.es', 'arp net 147.156', 'tcp port 21'. Si no s'especifica cap protocol, tots els protocols que siguin consistents amb la identificació de tipus són capturats.

Com pot veure's per l'explicació dels diferents tipus de qualificadors, sempre estan presents, encara que siga per defecte, els tres tipus de qualificadors. Així, l'expressió ip 147.156.222.65 és equivalent a ip src or dst host 147.156.222.65.

Poden construir-se filtres més complexos mitjançant la combinació de primitives mitjançant la utilització de parèntesis i/o les paraules *and*, *or* i *not*., sent la prioritat de *not* major que la de *and* i *or*, la prioritat de la qual entre sí és igual. Així, per exemple, 'ip multicast and (ip src 147.156.222.65)' indica que es capturen tots els paquets multicast l'origen del qual siga 147.156.222.65. Un altre exemple, 'host glup.uv.es and not port ftp' indica que es capturen tots els paquets l'origen o destinació dels quals és glup.uv.es excepte aquells el port d'origen o destinació del qual és el de ftp (port 21).

Un llistat de les primitives més utilitzades es troba en la següent taula:

Primitiva	Descripció
dst host <ordenador>	Veritat si el camp destinació del paquet és l' <ordenador>
src host <ordenador>	Veritat si el camp origen del paquet és l' <ordenador>
Host <ordenador>	Veritat si el camp origen o destinació del paquet és l' <ordenador>
ether dst <ordenador>	Veritat si l'adreça ethernet de destinació és l' <ordenador>
ether src <ordenador>	Veritat si l'adreça ethernet d'origen és l' <ordenador>
ether host <ordenador>	Veritat si l'adreça ethernet d'origen o destinació és l' <ordenador>
gateway <ordenador>	Veritat si el paquet utilitza com a passarel·la (gateway) l' <ordenador>
dst net <red>	Veritat si l'adreça de destinació del paquet correspon a una adreça de la <xarxa>
src net <red>	Veritat si l'adreça d'origen del paquet correspon a una adreça de la <xarxa>
net <red>	Veritat si les adreces d'origen o destinació del paquet corresponen a una adreça de la <xarxa>
dst net <red> mask < mascara>	Veritat si l'adreça de destinació del paquet correspon a una adreça de la <xarxa> de màscara < mascara>
src net <red> mask < mascara>	Veritat si l'adreça d'origen del paquet correspon a una adreça de la <xarxa> de màscara < mascara>
net <red> mask < mascara>	Veritat si les adreces d'origen o destinació del paquet corresponen a una adreça de la <xarxa> de màscara < mascara>

Primitiva	Descripció
dst net <red>/<longitud>	Veritat si l'adreça de destinació del paquet correspon a una adreça de la <xarxa> la màscara de la qual s'indica per <longitud>
src net <red>/<longitud>	Veritat si l'adreça d'origen del paquet correspon a una adreça de la <xarxa> la màscara de la qual s'indica per <longitud>
net <red>/<longitud>	Veritat si les adreces d'origen o destinació del paquet corresponen a una adreça de la <xarxa> la màscara de la qual s'indica per <longitud>
dst port <puerto> ²	Veritat si el paquet té com a destinació el port donat per <port>
src port <puerto>	Veritat si el paquet té com a origen el port donat per <port>
Port <puerto>	Veritat si el paquet té com a origen o destinació el port donat per <port>
Less <longitud>	Veritat si el paquet té una longitud menor o igual que <longitud>
greater <longitud>	Veritat si el paquet té una longitud major o igual que <longitud>
ether broadcast	Veritat si el paquet és un paquete ethernet broadcast.
ip broadcast	Veritat si el paquet és un paquet IP broadcast.
ether multicast	Veritat si el paquet és un paquet ethernet multicast.
ip multicast	Veritat si el paquet és un paquet IP multicast.

A més de les expressions anteriors, existeixen expressions del tipus <expressió 1> <operador> <expressió 2>, on <operador> és <, >, <=, >=, =, != i <expressió 1> i <expressió 2> són expressions aritmètiques compostes per constants enteres (expressades amb la sintaxi de C), els operadors +, -, *, /, &, |, i un accés especial a les dades del paquet.

Per accedir a les dades d'un paquet s'utilitza la sintaxis *protocol [desplaçament: tamany]*, on *protocol* és un dels protocols vàlids (*ether, fddi, tr, ip, arp, rarp, tcp, udp, icmp* o *ip6*), *desplaçament* és el desplaçament, en bytes, des del començament de les dades del protocol especificat, i *tamany* són els bytes a analitzar. Així, *ip[0] & 0x0F != 5* indica tots els paquets que contenen opcions IP (camp IHL de valor distint de 5), mentre que *ip[6 : 2] & 0x1FFF = 0* indica sols datagrames no fragmentats o l'últim fragment dels datagrames fragmentats.

Altres exemples sobre multicast:

--El filtre "ether multicast" és equivalent a "ether[0]&1!=0" per capturar trames multicast (analitza el bit I/G de l'adreça física)

--El filtre "ip multicast" és equivalent a "ip[16]&0xF0==0xE0", prenent el byte 16 de la capçalera IP i comprovar que coincideix amb els primers 4 bits d'una adreça 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.