Les capes superiors del model OSI: sessió, presentació i aplicació

PID_00218428

Ramon Musach Pi

Universitat Oberta de Catalunya

Índex

Introducció..... 5

1. El nivell d'aplicació..... 7
1.1. Model client-servidor 7
1.2. Model d'igual a igual (*peer-to-peer*, P2P) 8

2. Protocols de la capa d'aplicació..... 10
2.1. DNS: servei de noms a Internet 10
2.1.1. Què és? 10
2.1.2. Tipus i ubicació dels servidors DNS 12
2.1.3. Funcionament del servei DNS 13
2.2. El web i l'HTTP 14
2.2.1. Els llenguatges de marques HTML i XHTML 15
2.2.2. HTTP (*Hypertext Transfer Protocol*) 16
2.2.3. HTTPS (*hypertext transfer protocol secure*) 17
2.3. FTP (*File Transfer Protocol*) 17
2.3.1. TFTP (*Trivial File Transfer Protocol*) 19
2.4. Correu electrònic a Internet 19
2.4.1. SMTP (*Simple Mail Transfer Protocol*) 20
2.4.2. POP3 (*Post Office Protocol* o protocol d'accés simple a les bústies de correu) 21
2.4.3. IMAP (*Internet Message Access Protocol* o protocol d'accés a missatges d'Internet) 22
2.5. Servei de notícies NNTP (*Network News Transfer Protocol*) 23
2.6. Missatgeria instantània 24
2.7. Accés a ordinadors remots 24

3. Utilitats TCP/IP dels sistemes operatius..... 26

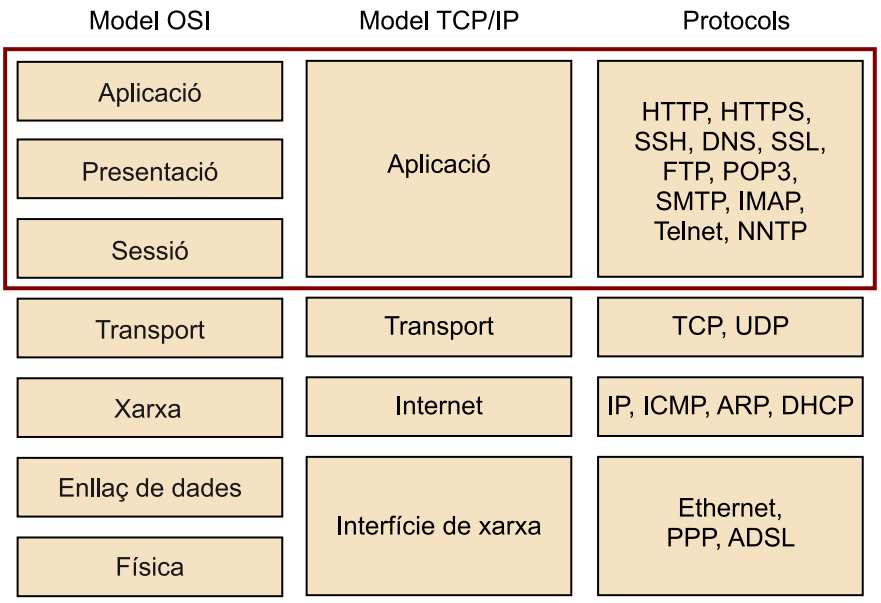
4. Aplicacions multimèdia i els seus protocols..... 28
4.1. Exemples d'aplicacions multimèdia 29
4.1.1. *Streaming* d'àudio i vídeo emmagatzemats 29
4.1.2. *Streaming* en directe d'àudio i vídeo 29
4.1.3. Àudio i vídeo en temps real interactiu 30
4.2. Compressió d'àudio i vídeo 30
4.2.1. Compressió d'àudio 30
4.2.2. Compressió de vídeo 31
4.2.3. Formats d'àudio i vídeo 31
4.3. Protocols per a aplicacions interactives en temps real 33
4.3.1. RTSP. *Real Time Streaming Protocol*..... 34
4.3.2. RTP. *Real Time Transport Protocol*..... 35

4.3.3. RTCP. *Real Time Control Protocol*..... 35
4.3.4. SIP. *Session Initiation Protocol*..... 36
4.3.5. H.323 37
4.3.6. Skype. 37

Introducció

Les capes del model TCP/IP no es corresponen exactament amb les capes del model OSI. **La capa d'aplicació de TCP/IP** és l'equivalent a les **capes de sessió**, **presentació** i **aplicació del model OSI**.

Figura 1



En aquesta taula disposem de les equivalències entre els dos models (OSI i TCP/IP) i els protocols associats a cada nivell.

Abans d'entrar en detalls en la capa d'aplicació, descriurem les capes de sessió i presentació del model OSI, amb funcionalitats que, en el model TCP/IP, ja venen integrades dins la capa d'aplicació.

El nivell de sessió en el model OSI

Aquesta capa del model OSI respon a peticions de servei de la capa de presentació i obté els serveis de la capa de transport. Organitza les funcions que permeten que dos usuaris es comuniquin mitjançant la xarxa. Dins d'aquestes funcions s'inclouen tasques de seguretat, contrasenyes d'usuaris i administració del sistema.

En aquest nivell es realitza **l'establiment, gestió (o utilització) i finalització (o alliberament) de les sessions de comunicació entre entitats del mateix nivell**. La gestió inclou la sincronització del flux de dades i el manteniment de les sessions establertes.

Per a la sincronització de l'intercanvi de dades utilitza uns punts de verificació, anomenats *check points*, per tal que davant d'una interrupció de la transmissió per qualsevol causa, aquesta es pugui reprendre des de l'últim punt de verificació en lloc de repetir-la des del principi.

Exemples de protocols de nivell de sessió són: ***Session Control Protocol*** (SCP) i ***Remote Procedure Call*** (RPC).

El nivell de presentació en el model OSI

El nivell de presentació respon a peticions de servei de la capa d'aplicació i obté els serveis de la capa de sessió.

La capa de presentació s'encarrega de traduir la informació del format del computador a un format comprensible pels usuaris. Inclou el control de les impressores, l'emulació de terminal i els sistemes de codificació. Per tant, podem afirmar que la capa de presentació s'encarrega dels aspectes relacionats amb la **sintaxi** i **semàntica de la informació** que es transmet, realitzant les conversions de representació necessàries per a la correcta interpretació de les estructures de dades i s'encarrega del significat de la informació transportada.

Per tant, incorpora tot un conjunt de **funcions de conversió, compressió i xifrat (o codificació) de les dades del nivell d'aplicació**.

Per exemple, la compressió de les dades s'utilitza per a reduir el nombre de bits a transmetre i el xifrat, emprant tècniques criptogràfiques com les que veurem en el proper mòdul, es fa servir per assegurar la privacitat i l'autenticació de les mateixes.

Les implementacions de la capa de presentació no acostumen a associar-se a una pila de protocols, sinó que utilitza estàndards de format de dades que siguin apropiats per a l'aplicació, com per exemple els formats de vídeo MPEG, Quicktime, etc; o els d'imatges com GIF, JPEG, TIFF, etc.

Tal com hem comentat, les funcionalitats de les capes de sessió i presentació, en el model TCP/IP venen integrades dins la capa d'aplicació i, per tant, en moltes aplicacions i protocols no es fa cap distinció entre les capes de presentació i aplicació. Un exemple el tenim amb HTTP, generalment considerat com a protocol de capa d'aplicació, tot i que també implementa funcionalitats pròpies de la capa de presentació.

1. El nivell d'aplicació

A partir d'aquest apartat tractarem el nivell d'aplicació, tal i com ho fa el model TCP/IP, integrant funcionalitats de les capes de sessió i de presentació del model OSI.

Els serveis de la capa d'aplicació faciliten la comunicació entre les aplicacions de programari (programes) que corren sobre aquesta capa i els serveis que ofereixen les capes inferiors. Així, els protocols del nivell de la capa de transport, ofereixen serveis a l'aplicació i, al mateix temps, l'aplicació requereix d'unes capacitats que aquesta capa inferior li ha d'oferir. Entre aquestes capacitats tenim: **transferència fiable**, per a no perdre informació per exemple en transferències de fitxers, **amplada de banda**, per exemple en transmissions d'imatges en temps real i **temporització** per a comunicacions en temps real.

Al tractar aquest nivell, procedirem a descriure tota una sèrie d'aplicacions, anomenades distribuïdes i protocols de comunicació associats.

Una **aplicació distribuïda** està formada per una col·lecció d'ordinadors autònoms enllaçats per una xarxa d'ordinadors i suportats per un programari que fa que els ordinadors autònoms actuïn com un servei integrat.

Les dues arquitectures distribuïdes més emprades actualment són:

Client-servidor (*client/server* en anglès) i **d'igual a igual** (*peer-to-peer* o P2P).

1.1. Model client-servidor

La majoria de les aplicacions de programari que funcionen en un entorn de xarxa segueixen un model client-servidor.

En aquest model, hi ha dos tipus de components que permeten comunicar-se entre elles: clients i servidors.

Els **clients** són els que fan les peticions de servei, iniciant sovint la comunicació amb el servidor.

Així podem parlar d'un programa client, iniciat per un usuari o per un altre programa que s'està executant en un *host* i que sol·licita un servei determinat a un altre *host* de la xarxa (habitualment un *host* remot). El procés finalitza quan aquest programa rep el servei sol·licitat.

Els **servidors** són els *hosts* que proveeixen serveis. Sovint són els que reben les peticions que realitzen els clients, les resolen i retornen les respostes als clients.

Un programa servidor és el que s'està executant en un *host*, sovint remot, que proporciona determinats serveis a múltiples programes clients. Quan el programa servidor s'inicia, comença a oferir els seus serveis, de manera ininterrompuda i continuada, a aquells clients que li sol·licitin.

Per exemple, quan un usuari utilitza un navegador (aplicació de programari del client) per a obrir una pàgina web, el protocol anomenat HTTP és el que dóna forma a la sol·licitud i l'envia des del client fins al servidor. Aquest mateix protocol és el que també donarà format i enviarà la resposta del servidor web al navegador del client.

1.2. Model d'igual a igual (*peer-to-peer*, P2P)

Un sistema d'igual a igual es caracteritza per ser un sistema distribuït en el que tots els nodes tenen les mateixes capacitats i, per tant, en el que la comunicació és simètrica.

Les xarxes *peer-to-peer* (xarxes punt a punt o més conegudes com a xarxes P2P) són aquelles xarxes que no contenen nodes clients i servidors fixes, sinó un nombre de nodes "iguals" (anomenats *peers*, parells) que funcionen a la vegada com a clients i servidors d'altres nodes de la xarxa. Aquests sistemes ofereixen i utilitzen una sèrie de recursos distribuïts per a portar a terme determinades funcions de forma descentralitzada. Aquests recursos poden ser molt diversos, tals com dades, amplada de banda o capacitat de càlcul.

Des dels seus inicis, els sistemes i aplicacions d'igual a igual s'han anat popularitzant a Internet amb aplicacions relacionades amb la compartició de fitxers, però també n'hi ha d'altres de molt populars com Skype, que proporciona videotrucades per la xarxa Internet, sistemes de missatgeria instantània, sistemes de processament distribuït, jocs,...

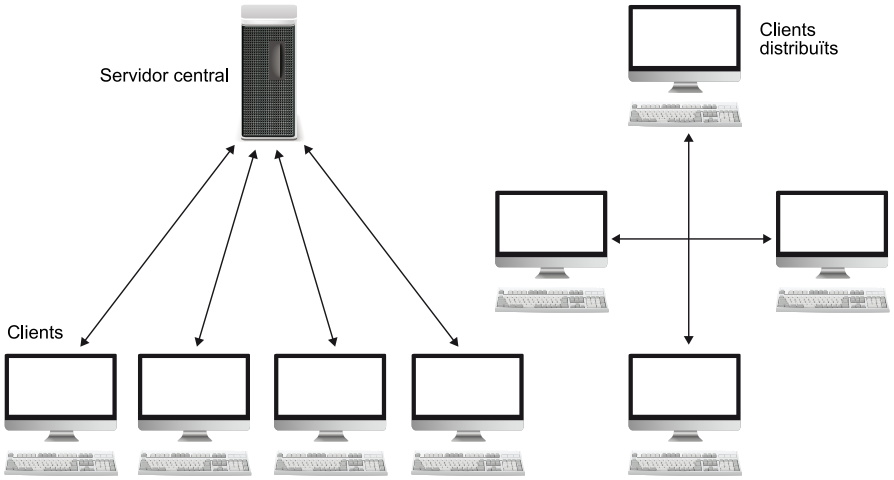
Les aplicacions d'igual a igual es van començar a popularitzar amb les aplicacions de compartició de fitxers. Concretament, Napster es va popularitzar prop de l'any 2000. Creat per Shawn Fanning, va ser pioner de les xarxes P2P d'intercanvi amb un servei de distribució d'arxius de música en format MP3.

Els nodes que formen un sistema o aplicació d'igual a igual s'organitzen amb el que es coneix com a **xarxa superposada** (*overlay network*, en anglès), que funciona sobre la xarxa física que connecta els nodes.

Exemple

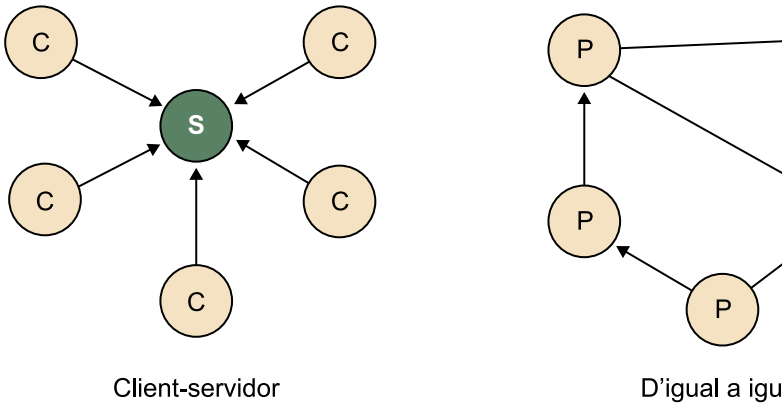
Alguns exemples de sistemes P2P són: Gnutella, FastTrack/KaZaA, BitTorrent, Overnet/eDonkey2000.

Figura 2



El primer esquema correspon a un model client-servidor i el segon a un sistema distribuït.

Figura 3



De forma més esquematitzada, el primer esquema correspon a un model client-servidor i el segon a un sistema *peer-to-peer*.

Els dos models descrits són, de fet, dues formes d'arribar a plantejar el disseny d'una aplicació, però hem de tenir en compte que sovint les aplicacions estan plantejades com a models híbrids entre diferents models, per a satisfer les necessitats dels usuaris d'aquestes aplicacions.

2. Protocols de la capa d'aplicació

En aquest apartat, descriurem tota una sèrie de protocols de comunicacions, associats directament a aplicacions que utilitzen Internet com a mitjà de comunicació. Aquestes aplicacions es coneixen com a aplicacions distribuïdes, ja que estan formades per diferents parts i cadascuna es troba en màquines diferents.

2.1. DNS: servei de noms a Internet

2.1.1. Què és?

Cadascun dels ordinadors que es connecten a Internet ho fan amb una adreça IP única. Atenent la dificultat que comporta recordar aquestes adreces, es va crear un **sistema de noms de domini**, en anglès *Domain Name System* (DNS), que permet traduir adreces IP amb noms que es poden recordar de forma més senzilla.

Un servei DNS rep les peticions que li arriben i realitza ràpidament aquesta traducció. Per exemple, quan escrivim una adreça web en el navegador, aquest fa la consulta al DNS per a conèixer l'adreça IP que li correspon.

Un **domini** és un grup de nodes que pertanyen a una mateixa organització i que tenen en comú una part de la seva adreça IP. Un domini està identificat per un nom de domini, que habitualment està associat a una organització. El nom complet d'un *host* està format pel nom del *host* més el nom del domini al qual pertany.

Un nom de domini es representa mitjançant una sèrie d'etiquetes separades per punts. Cada etiqueta representa un nivell diferent en la jerarquia de noms de domini.

Exemple

Per exemple, en el nom de domini www.uoc.edu, "edu" és el **domini de nivell superior** (*top-level domain*, TLD), "uoc" és el domini de segon nivell, i "www" és el domini de tercer nivell.

Així doncs, quan escrivim www.uoc.edu, el servei DNS li dirà al navegador que l'adreça IP de www.uoc.edu és 213.73.40.242. Per tant, el DNS funciona com un llistat telefònic, però en comptes de relacions de noms de persones i telèfons, té relacions de dominis i adreces IP.

Nota

Els noms de domini han d'estar enregistrats per *l'Internet Corporation for Assigned Names and Numbers*, **ICANN**, https://www.icann.org, o, en el seu defecte, per una empresa autoritzada a aquest efecte per aquesta entitat. L'ICANN es va crear el 1998 amb l'objectiu

d'encarregar-se de certes tasques que fins llavors estaven en mans de la IANA, entre les quals es troba l'aprovació i control dels dominis d'Internet.

Tot seguit mostrem alguns dels dominis de nivell superior aprovats per l'ICANN:

1) D'àmbit genèric:

.cat – Per a la llengua i cultura catalana

.com - Organitzacions comercials

.net - Estructures de la xarxa Internet

.org - Organitzacions d'una altra mena (sovint sense ànim de lucre o religioses)

.edu - Educació

.info - Agències d'informació

.int - Organitzacions internacionals (i.e. ONU)

.biz - Negocis

.mil – Militar

2) D'àmbit territorial:

.ad - Andorra

.au - Austràlia

.de - Alemanya

.es - Espanya

.fr - França

.it - Itàlia

.jp - Japó

.lu - Luxemburg

.nl - Països Baixos

.tr - Turquia

Per a més informació sobre els noms de dominis i el seu registre es pot consultar la següent guia publicada per ICANN:

"Guía para principiantes para NOMBRES DE DOMINIO"

https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-es.pdf

Altres serveis importants que proporciona el DNS són:

- **Traducció d'àlies** (noms addicionals que poden arribar a tenir els *hosts*; per exemple: www.uoc.edu és un àlies de www-org.uoc.edu). Al nom original se l'anomena canònic.

- **Traducció d'àlies del servidor de correu**. Tinguem en compte que una mateixa organització pot arribar a tenir diferents noms (àlies) per al seu domini de correu electrònic i per al servidor web.

- **Distribució de càrrega**. Redirigint, si és el cas, el tràfic a servidors web que disposen d'informació o serveis replicats, per a millorar-ne l'accés. Tinguem en compte que llocs webs amb molts accessos poden estar replicats en molts servidors, cadascun en un ordinador diferent i amb una adreça IP diferent.

2.1.2. Tipus i ubicació dels servidors DNS

Seria senzill que la xarxa Internet disposés d'un únic servidor per a portar a terme les equivalències entre les adreces IP i els noms de domini. Però, tal i com podem intuir, no seria efectiu, pel col·lapse que es podria produir en les peticions i respostes, a més del gran volum que hauria de tenir la base de dades d'aquest servidor.

El DNS és, realment, una base de dades de servidors, organitzats de forma jeràrquica i distribuïts per tot el món. Per tant, cap servidor DNS disposa de totes les equivalències entre noms i adreces IP.

Existeixen tres tipus de servidors DNS:

1) Servidors DNS arrel. Hi ha pocs servidors DNS arrel. Cadascun d'ells és, en realitat, un clúster de servidors reproduïts, per seguretat i fiabilitat.

Podem trobar la ubicació dels servidors arrel a: http://www.root-servers.org.

2) Servidors DNS de nivell de domini superior (*top-level domain*), TLD). Són els responsables dels dominis de primer nivell com .org, .com, .net, .edu, .us, .cat, .es…

3) Servidors DNS autoritzats. Cada organització que disposi d'ordinadors accessibles a Internet ha de disposar d'un registre públic que permeti fer la traducció de noms i adreces IP. Aquest llistat es troba en el que s'anomena un DNS autoritzat que pot ser un servidor proveït per la mateixa organització o bé per algun proveïdor de serveis.

4) Servidors DNS locals. Tot i que estrictament no pertanyen a la jerarquia de servidors de DNS, són fonamentals, ja que quan un node es connecta al seu ISP (proveïdor d'accés a Internet), aquest li proporciona l'adreça IP d'un o més servidors DNS locals. Aquest actua com a **proxy** (o servidor intermediari) i l'envia a la jerarquia de servidors DNS perquè resolgui la petició.

Proxy

Un proxy o servidor intermediari és un programa o dispositiu que realitza una acció en representació d'un altre. Fa d'intermediari entre el client i el servidor, filtrant el trànsit depenent de les polítiques que s'estableixin. Pot respondre peticions del client sempre que disposi de la resposta en la seva memòria cau, així s'estalvia de sol·licitar-ho al servidor.

Podem trobar els DNS de les principals operadores a: http://www.adslayuda.com/dns.html.

Figura 4

Mapa del món amb les ubicacions dels servidors de DNS. Extret de http://www.root-servers.org/.

2.1.3. Funcionament del servei DNS

La traducció dels noms la realitzen els anomenats servidors DNS, a petició de les aplicacions del client (navegadors, clients de correu o altres aplicacions) i de forma transparent a l'usuari.

Els usuaris sovint utilitzen com a servidor DNS el que proporciona el seu proveïdor de serveis d'Internet. L'adreça d'aquests servidors pot arribar a ser configurada de forma manual o automàtica mitjançant **DHCP** (***Dynamic Host Configuration Protocol***). En altres casos, els administradors de xarxa poden tenir configurats els seus propis servidors DNS.

Considerant que l'equivalència entre *hosts* i adreces IP no és permanent, els servidors DNS descarten la informació "caché" (cau) després d'un cert temps (que pot ser d'uns dos dies).

El protocol DNS generalment transporta les peticions i respostes per un port UDP, ja que per estructura i nivell de seguretat implementat és més ràpid. Però hi ha casos que s'utilitza el port TCP, sobretot quan cal transportar respostes més grans de 512 bytes de longitud i per raons de necessitat de fiabilitat.

Pel que fa a aspectes de seguretat relacionats amb els DNS, cal comentar que quan el servei DNS es va implementar no es van considerar aquests aspectes de seguretat. Una vulnerabilitat que es pot donar és la de fer creure a un ser-

vidor DNS una determinada traducció incorrecte. És el que s'anomena contaminació de la memòria cau del DNS, que consisteix en proporcionar, de forma maliciosa o intencionada, dades no originades per un servidor DNS autoritzat.

El servei ***Domain Name System Security Extensions*** (DNSSEC) modifica el DNS per a afegir respostes signades digitalment, de manera que així s'autentica l'origen de les dades del DNS. A partir del 10 de juliol de 2010, tots els **servidors arrels** haurien d'emprar aquest protocol DNSSEC: http://www.root-servers.org/.

Servidor arrel

Un **servidor arrel** és un servidor de noms de domini (DNS) que coneix on estan els servidors de domini per a cadascuna de les zones de més alt nivell a Internet. Els servidors arrel són fonamentals per al funcionament del DNS, ja que són els que coneixen tots els dominis de primer nivell, per tant són el primer pas en la traducció dels noms de *hosts* a adreces IP. Admeten un gran volum de consultes. A l'any 2006, n'hi havia tretze repartits per tot el món, amb rèpliques dels mateixos en diversos continents.

2.2. El web i l'HTTP

El servei web o WWW (*World Wide Web*, "teranyina d'abast mundial") és el que dóna accés a informació multimèdia, per tant amb continguts de diferents tipus: text, imatges, àudio, vídeo, etc. També inclou referències a altres elements d'informació tenint en compte el model dels sistemes hipertext. En la terminologia WWW, a tots aquest elements se'ls anomena **recursos**.

Un **sistema hipertext** permet recórrer un document de manera no necessàriament lineal o seqüencial, sinó seguint les referències o enllaços que l'usuari seleccioni, saltant a la part referenciada. Aquesta manera d'accedir a la informació es coneix, popularment amb el nom de "navegar". Quan aquesta navegació, a més a més de fer-se a partir del text, es fa a partir d'elements multimèdia i no només text, se l'anomena **sistemes hipermedia**.

El servei web és un sistema basat en el model client/servidor, El servidor emmagatzema la informació multimèdia i el client la sol·licita, mitjançant un navegador i la presenta a l'usuari.

El protocol que s'utilitza per al diàleg entre el client i el servidor és **HTTP** (***Hypertext Transfer Protocol***, protocol de transferència d'hipertext), que descriurem en un proper apartat.

Atenent que l'ordinador client, mitjançant el navegador, ha de mostrar la informació tal i com es desitja, cal que les especificacions de les característiques d'aquesta visualització quedin ben clares. És aquí on intervenen el que s'anomenen els llenguatges de marques (com HTML i XHTML).

El mètode general utilitzat en el servei WWW per a identificar la informació a la que es vol accedir es coneix amb el nom d'**identificadors uniformes de recursos** (URl). La definició de l'estàndard URl es dóna l'any 1998 amb la publicació RFC 2396.

Des d'un document es poden referenciar recursos especificant-ne les adreces, que es representen mitjançant la següent terminologia:esquema: identificador.

On:

- **Esquema** pot ser http, ftp, mailto,... estenent així la funcionalitat del servei web amb l'accés a servidors ftp o servidors de correu, des d'un client web.

- **Identificador** que conté el nom del recurs i el servidor on es troba.

Quan l'esquema és http o ftp, el servidor comença amb els caràcters "//", i el servidor i el nom del recurs se separa amb un caràcter "/"

Exemple

http://www.uoc.es/index.html.

2.2.1. Els llenguatges de marques HTML i XHTML

El llenguatge de marques és una forma de codificar un document emprant etiquetes (o marques) que contenen informació addicional sobre l'estructura, la presentació,... Aquests llenguatges estan dissenyats per a especificar documents hipermèdia.

Un dels llenguatges de marques més emprats és el llenguatge **HTML** (***HyperText Markup Language***), que es troba dins la família de llenguatges (X)HTML. Els fonaments del llenguatge HTML els va establir Tim Berners-Lee, l'any 1992, des del **CERN** (***European Organization for Nuclear Research***). Tim Berners-Lee va crear l'HTML seguint les normes del llenguatge **SGML** (*Standard Generalized Markup Language*).

SGML (*Standard Generalized Markup Language*) és un conjunt de normes que es publiquen el 1986 amb l'objectiu d'establir la sintaxi d'un document. Es basa en un sistema d'etiquetes que permet organitzar la informació del document.

Tot i que inicialment no va prosperar com a estàndard, sí que a partir del 1996, l'IETF tanca el desenvolupament de l'estàndard HTML i alhora és adoptat pel W3C (*World Wide Web Consortium*).

Nota

Un dels punts d'inflexió de la *World Wide Web* està amb la introducció del navegador web Mosaic, el 1993. Un navegador gràfic desenvolupat per un equip del **NCSA** (*National Center for Supercomputing Applications*, Centre Nacional d'Aplicacions de Supercomputació) a la Universitat d'Illinois.

Nota

El **W3C** (***World Wide Web Consortium***) i l'**IETF** (***Internet Engineering Task Force***) s'encarreguen de definir els estàndards web, és a dir, les normatives relatives a aspectes del Word Wide Web.

A partir de la versió HTML 4.01 es genera un altre llenguatge, l'anomenat **XHTML** (***eXtensible Hypertext Markup Language***). Un llenguatge de marques molt semblant a l'HTML però que enlloc de seguir les regles sintàctiques de l'SGML, segueix les d'un altre llenguatge de marques, l'**XML** (***eXtensible Markup Language***).

Pel que fa a l'actualitat del món web, hem de parlar de l'**HTML5** (o la seva variant XML, l'XHTML5). Correspon a la cinquena gran revisió del llenguatge bàsic de la World Wide Web, l'HTML. En aquesta versió es dóna la circumstància que, per primera vegada, HTML i XHTML s'han desenvolupat en paral·lel sota la regulació del Consorci **W3C**. Incorpora moltes funcionalitats que en els inicis no es van tenir en compte com: suport a continguts multimèdia (àudio, vídeo) amb etiquetes que contenen còdecs per a poder mostrar aquests continguts, suport a grans conjunts de dades, millores en formularis, nous visors, possibilitat d'arrossegar objectes com ara imatges, etc.

Des d'aquesta pàgina, http://html5test.com/, podem arribar a comprovar fins a quin punt els navegadors més populars actualment, com Google Chrome, Mozilla Firefox, Internet Explore, etc, estan implementant les noves funcionalitats d'HTML5.

Pel que fa a un altre concepte relacionat amb els documents hipermèdia, tenim el CSS, que s'utilitza per donar estil a documents XHTML i, d'aquesta forma, poder separar el contingut de la presentació.

El **CSS** (***Cascading Style Sheets***) és un llenguatge de fulls d'estil que permet descriure l'aspecte i format que tindrà un document escrit en un llenguatge de marques quan es mostri per pantalla o quan s'imprimeixi o, fins i tot, com es pronunciarà la informació present en el document a través d'un dispositiu de lectura. Tot i que s'aplica a HTML i XHTML, també pot ser aplicat a qualsevol tipus de document XML. Les seves especificacions també són mantingudes pel W3C.

2.2.2. HTTP (*Hypertext Transfer Protocol*)

HTTP és un protocol del nivell d'aplicació per a sistemes hipermèdia col·laboratius i distribuïts, que és la base del Web. Es troba definit en l'RFC 1945 i RFC 2616.

Aquest protocol s'encarrega de gestionar la major part del trànsit que circula per Internet, ja que està associat a la sol·licitud de recursos web.

Segueix el model general de peticions i respostes entre un client i un servidor, basant-se en un servei de transport fiable. HTTP utilitza primordialment el protocol TCP, i per defecte, el port 80.

Quan en un navegador s'escriu l'adreça http://www.uoc.edu es fa una crida al servei DNS perquè associï el nom de domini amb una adreça IP. Quan ja es coneix, s'envia una sol·licitud ***get*** al servidor web, el qual respon amb una resposta ***send*** (*get* i *send* són dues operacions del protocol HTTP). Dins una mateixa sessió es va produint aquest diàleg.

2.2.3. HTTPS (*hypertext transfer protocol secure*)

Per fer transaccions de dades segures mitjançant el web, s'utilitza el protocol **HTTPS** (***hypertext transfer protocol secure***). En aquest protocol, s'utilitza una tecnologia basada en certificats digitals amb la finalitat de garantir l'autenticació entre els extrems de la transacció. A més, HTTPS garanteix la confidencialitat de les dades, ja que xifra tots els paquets de dades enviats durant la sessió. Per a poder emprar HTTPS, el servidor web ha d'adquirir un certificat digital a un proveïdor d'aquest tipus de serveis. També utilitza TCP, però amb el port 443.

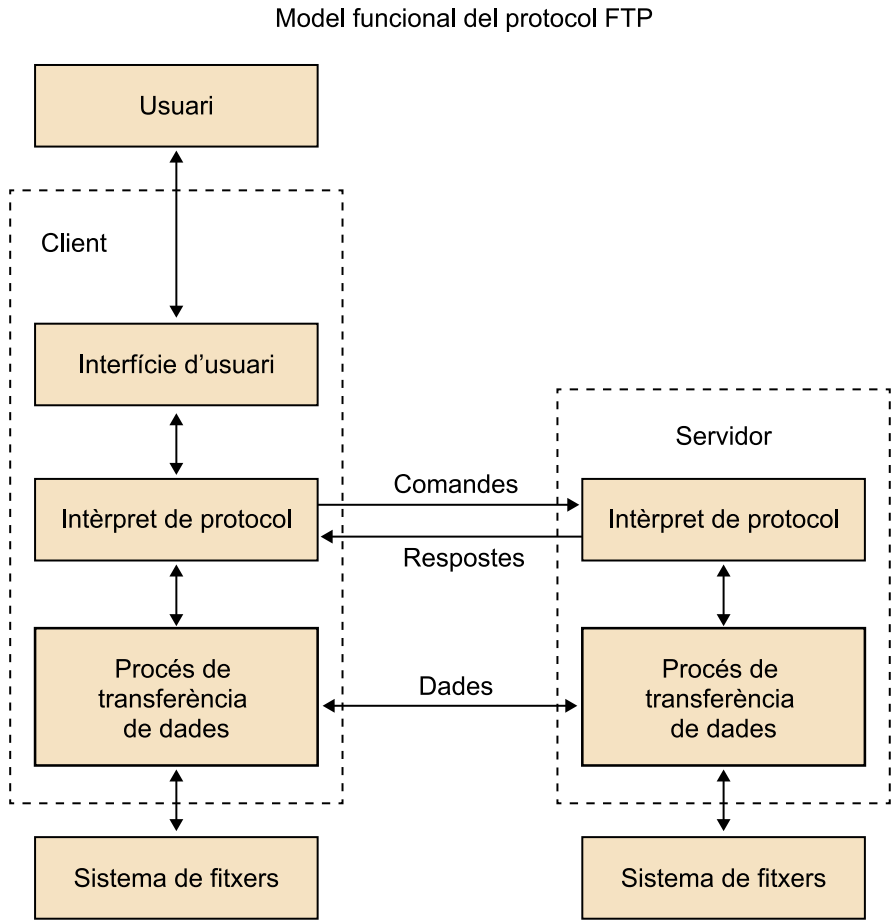
2.3. FTP (*File Transfer Protocol*)

Aquesta va ser una de les primeres aplicacions desenvolupades per a l'entorn d'Internet. L'especificació oficial d'aquest protocol, FTP (*File Transfer Protocol*, protocol de transferència de fitxers), es va publicar l'any 1985 en el document RFC 959.

Aquest protocol es basa en el model client/servidor i **permet la transferència de fitxers en els dos sentits, amb funcionalitats afegides com les de manipular el sistema de fitxers del servidor: modificar-los, esborrar-los, crear i esborrar directoris, llistar continguts, etc**. Actua de forma transparent a l'usuari, permetent la interoperabilitat entre sistemes de fitxers molt diferents.

En el model FTP existeixen dues entitats, tant en el servidor com en el client, que intervenen en la transferència de fitxers: **l'intèrpret de protocol i el procés de transferència de dades**. El primer s'encarrega de l'intercanvi de comandes de protocol i, el segon, sota el control del primer, s'encarrega d'intercanviar les dades, és a dir, els continguts dels fitxers que s'han de transmetre.

Figura 5



Model funcional del protocol FTP.

L'FTP es basa en connexions TCP i té assignats els ports 21 i 20. De fet, el port 21 s'utilitza per a l'intercanvi d'ordres i respostes i el 20 per a la transferència de dades. L'intèrpret de protocol del servidor ha d'estar preparat per a rebre peticions de connexió en un port TCP que, tal i com hem dit, és el número 21 per defecte.

Les peticions FTP són cadenes de caràcters ASCII que contenen la petició, paràmetres opcionals depenent de la petició i un caràcter de "final de línia" (caràcter <CRLF>).

Quan s'accedeix a un servidor FTP, en la majoria de casos, cal estar registrat prèviament per tal que accepti les peticions. Si el servidor permet connexions anònimes, l'accés serà més restringit i només es permetrà unes funcionalitats concretes, com per exemple l'accés a determinats fitxers. Tot i així, cal anar en compte a l'hora obrir el servidor a accessos anònims, ja que una errada en el programa servidor FTP, pot permetre intrusions no desitjades en el sistema.

2.3.1. TFTP (*Trivial File Transfer Protocol*)

Per la seva complexitat, el protocol FTP pot no ser el més apropiat per algunes situacions concretes en les que cal transferir fitxers d'un ordinador a un altre. Un exemple pot ser el d'una estació de treball sense disc que carrega el sistema operatiu per mitjà de la xarxa, des d'un ordinador que actua com a "servidor d'arrencada" de l'estació, proporcionant-li els fitxers que necessita. Una petita aplicació de la memòria ROM de l'estació controla aquesta transferència de fitxers.

En casos com aquest que acabem d'esmentar, de transmissions simples, s'ha definit el TFTP, *Trivial File Transfer Protocol*, especificat en l'estàndard RFC 1350. Aquest protocol es basa en datagrames, no requereix implementar el protocol TCP, ja que sovint utilitza UDP, proporcionant només dues operacions (llegir i escriure fitxers en el servidor), sense cap tipus d'identificació ni autenticació d'usuari.

2.4. Correu electrònic a Internet

El correu electrònic és l'aplicació distribuïda que permet l'enviament de missatges electrònics mitjançant sistemes informàtics. Quan es va especificar aquesta aplicació es va tenir molt en compte els elements i funcionalitats existents en el correu postal.

La funcionalitat està basada en la filosofia d'emmagatzematge i reenviament.

Hi ha hagut una gran evolució des dels primers sistemes que podien intercanviar únicament missatges de text ASCII fins als correus electrònics amb continguts multimèdia actuals.

Els protocols associats a aquesta aplicació són:

1) SMTP (***Simple Mail Transfer Protocol***), per a la transferència de missatges. És independent del format i el contingut del missatge.

2) POP3 (***Post Office protocol***), per a l'accés simple a bústies de correu.

3) IMAP4rev1 (***Internet Message Access Protocol***), per a l'accés complex a bústies de correu.

També va ser necessari definir un format de missatge, l'RFC 822, que posteriorment es va ampliar i va donar lloc al format MIME.

El **format dels missatges RFC 822** es basa en el format típic de les cartes postals amb informació del destinatari, del remitent i el contingut del missatge.

Aquest estàndard especifica les parts d'aquests missatges: capçalera, amb tota una sèrie de camps, i cos del missatge amb el contingut (opcional).

Com a camps obligatoris de la capçalera tenim: data (Date), origen (From), i destinatari (To) o destinatari de còpia cega (Bcc).

La norma RFC 822 defineix un format de missatge i un contingut amb una única part de text en ASCII de 7 bits. Es va considerar que aquest format era massa simple i que calia algun mètode per a superar-ne les limitacions.

En aquest context, el format **MIME**, ***Multipurpose Internet Mail Extensions***, (RFC 2045 a 2049) redefineix el format del missatge per a permetre, sense perdre la compatibilitat amb el format definit per l'RFC 822, les característiques següents:

- Contingut de text no només ASCII de 7 bits.
- Contingut no textual.
- Contingut amb múltiples parts (per permetre adjuntar fitxers).
- Capçaleres amb text no només ASCII de 7 bits.

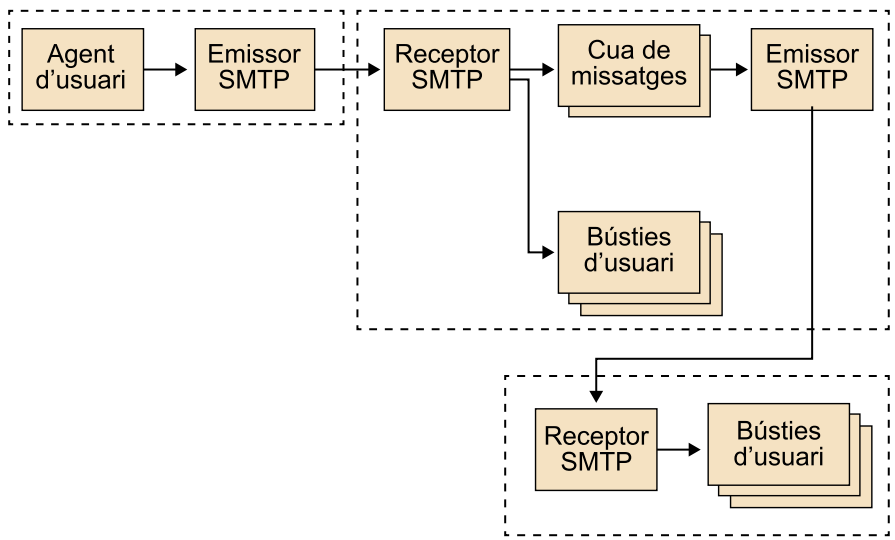
2.4.1. SMTP (*Simple Mail Transfer Protocol*)

És el protocol més utilitzat a Internet per a transferir missatges de correu electrònic. Ofereix una transferència fiable i eficient de missatges de correu.

La figura següent ens mostra el model d'un sistema SMTP:

Inici Figura 6 mòdul 5: esquema

Figura 6



Aquest estàndard també segueix el model client/servidor, en les especificacions del qual el terme *usuari* es diu *agent d'usuari*, *client* es diu *emissor SMTP* i *servidor* equival a *receptor SMTP*.

2.4.2. POP3 (*Post Office Protocol* o protocol d'accés simple a les bústies de correu)

Aquest protocol (descrit al RFC 1939) de la capa d'aplicació es va definir per a donar resposta a sistemes petits, on no necessàriament els sistemes clients estan sempre connectats i disposats a rebre missatges en qualsevol moment. Permet la recuperació de missatges de bústies de correu remots. A diferència d'IMAP (que veurem després), en l'esquema de POP3 l'emmagatzemament de correu es porta a terme a l'ordinador de l'usuari.

Associat al port 110 en comunicacions TCP, el POP3 no especifica cap mètode per a la tramesa de correu; altres protocols de transferència de correu, com l'SMTP que acabem de veure, proporcionen aquesta funcionalitat.

El model del POP3 consta dels següents elements: agent d'usuari, client POP3, servidor POP3. Quan el client POP3 necessita accedir a la bústia, es connecta amb el servidor POP3, recupera la informació que li interessa i tanca la connexió.

Els tres estats definits en la norma són:

1) Una vegada s'ha obert la connexió, la sessió entra en l'estat d'autorització, moment en el que el client s'ha d'identificar davant del servidor POP3.

2) Una vegada autoritzat, la sessió passa a l'estat de transacció. En ell, el client demana accions al servidor POP3 amb les comandes necessàries i aquest les atén.

3) Quan el client crida la comanda QUIT i la rep el servidor, la sessió entra en estat d'actualització. El servidor allibera els recursos, s'acomiada i tanca la connexió TCP.

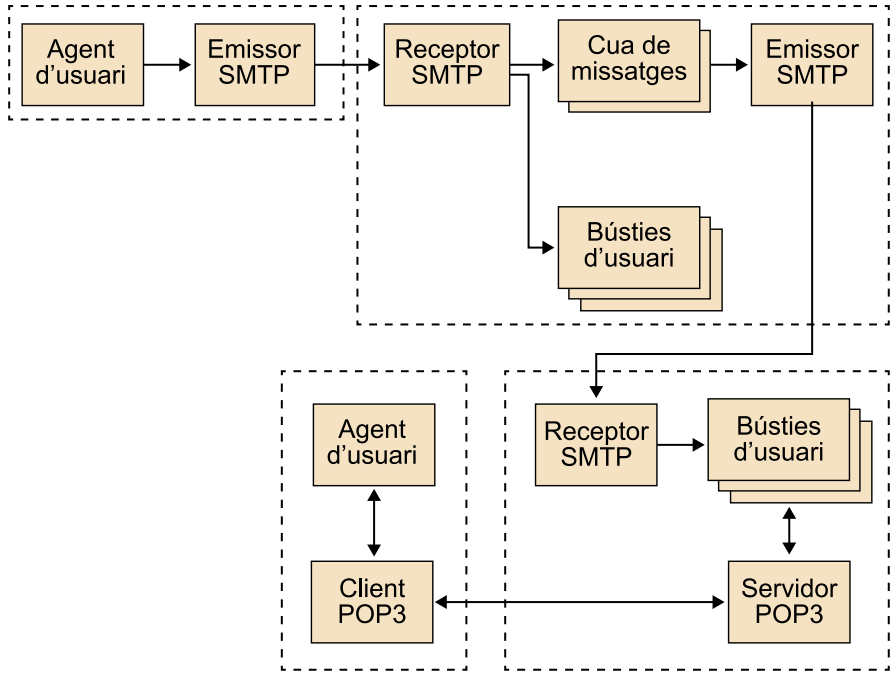
En aquest procés, client i servidor s'intercanvien ordres i respostes seguint el model de diàleg de **Telnet**:

- **Ordres**: ordres de text de quatre caràcters seguides d'espais i els arguments que requereixin. Finalitzen amb un <CRLF>.

- **Respostes**: una cadena de caràcters que comença per +OK o -ERR més una descripció.

En aquesta figura es presenten els elements del model funcional del POP3 integrats en un sistema en el que s'utilitza l'SMTP per a enviar el correu i el POP 3 per a accedir a les bústies:

Figura 7



2.4.3. IMAP (*Internet Message Access Protocol* o protocol d'accés a missatges d'Internet)

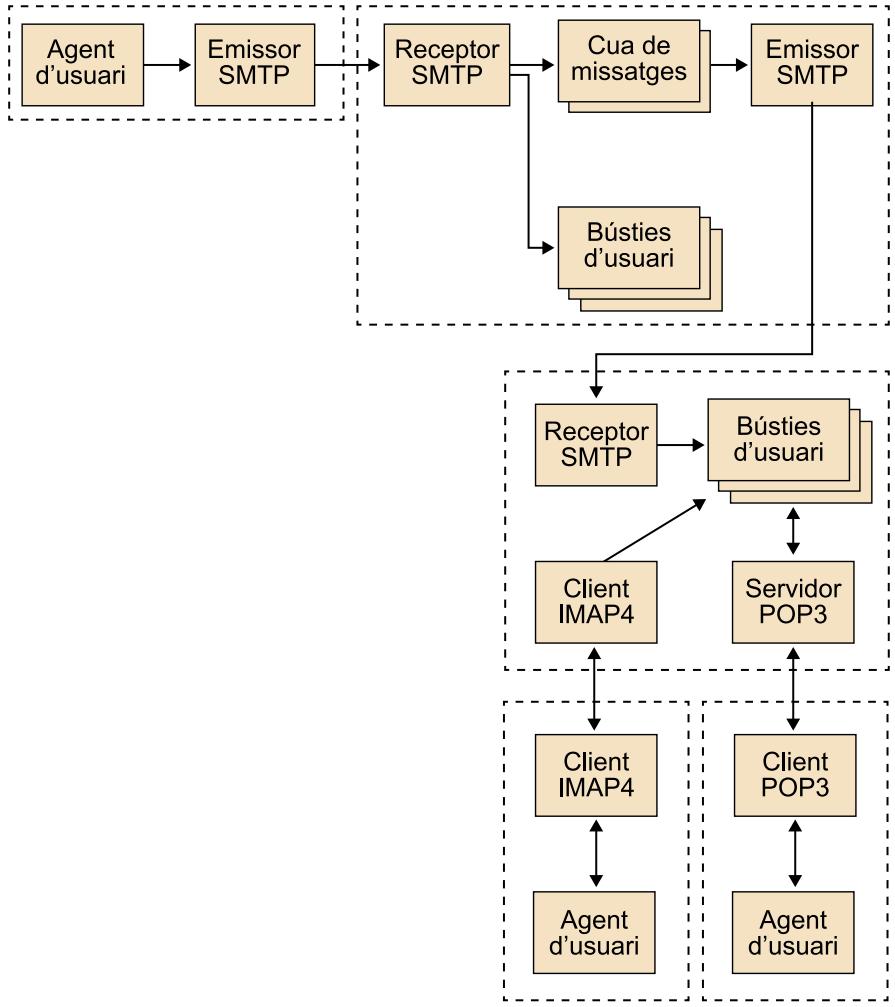
Aquest protocol proporciona a l'usuari accés remot a la bústia de correu. A diferència del POP3, els missatges de correu es dipositen en el servidor, on s'emmagatzemen estructurats en carpetes i on es manipulen. Per tant, és un protocol més complex que l'anterior.

El protocol d'accés a missatges Internet, en la seva versió actual 4 rev 1, s'anomena **IMAP4rev1** i està especificat en l'RFC 3501. L'IMAP4rev1 (a partir d'ara l'anomenarem IMAP4) permet a l'usuari disposar de diferents bústies estructurades de manera jeràrquica i, alhora, poder-les manipular de manera remota, tal com fa amb les bústies locals.

L'IMAP4 es pot utilitzar amb qualsevol protocol de transport fiable. Per norma general, s'utilitza el TCP i, en aquest cas, s'utilitza el port 143. Totes les interaccions entre client i servidor es porten a terme en forma de línies ASCII acabades amb un caràcter <CRLF>.

En aquesta figura es detallen els elements del model funcional de l'IMAP4 integrats en un sistema que utilitza SMTP per a enviar el correu i IMAP4 per a accedir a les bústies:

Figura 8



Nota

Degut a les característiques que hem explicat, el més habitual és que les aplicacions de correu electrònic, per exemple, **Outlook de Microsoft**, tinguin configurat un protocol SMTP (per enviar e-mails) i POP3 o IMAP4 (per rebre'ls i gestionar-los).

Una de les diferències més destacades entre POP3 i IMAP és que, si el programa de correu electrònic utilitza POP3, llavors aquest descarregarà tots els missatges a l'ordinador de l'usuari, sense deixar còpia en el servidor de missatgeria. Pel contrari, si fa servir IMAP, farà una còpia a l'ordinador de l'usuari i sempre mantindrà el missatge en el servidor. Per tant, en aquest segon cas, si s'esborra un missatge a l'ordinador de l'usuari, aquest no queda esborrat per sempre. A més a més, permet poder disposar de diferents dispositius clients sincronitzats.

2.5. Servei de notícies NNTP (*Network News Transfer Protocol*)

El servei de notícies (en anglès, *news*) permet la tramesa de missatges, al igual que fa el servei de correu electrònic, però amb la diferència que des de l'origen no s'especifica el destinatari o destinataris, sinó que qualsevol usuari amb accés al servei els pot llegir. Per tant, és comparable a la d'un tauler d'anuncis, on tothom pot llegir els missatges que hi ha penjats.

Els servidors de notícies es comuniquen entre si per a intercanviar-se articles per mitjà de l'NNTP (*Network News Transfer Protocol*), especificat en el document RFC 977. NNTP és un protocol per a la transferència d'informació entre clients mitjançant l'accés a grups de notícies o *newsgroups*, els quals contenen informació classificada per tòpics d'interès.

Per norma general, l'NNTP utilitza el protocol de transport TCP. El número de port assignat al servei de notícies és el 119.

2.6. Missatgeria instantània

L'evolució de les tecnologies, dels dispositius mòbils i la generalització d'Internet, propiciat per un abaratiment de costos, ha fet que molts usuaris arribin a comunicar-se per Internet mitjançant aquests tipus de dispositius. En aquest context s'ha popularitzat la comunicació entre usuaris mitjançant xats i missatgeria instantània (**IM**, *Instant Messaging*), amb una comunicació real, instantània, de text, àudio i vídeo.

XMPP, acrònim de *eXtensible Messaging Presence Protocol*, és un protocol lliure de missatgeria instantània basat en XML i estandarditzat per l'IETF. El port estàndard per a l'XMPP és el 5222. Utilitza una arquitectura client-servidor descentralitzada, on els clients no es comuniquen directament els uns amb els altres, sinó que ho fan a través dels servidors. Tot i així, altres sistemes de missatgeria instantània utilitzen arquitectures centralitzades.

Les funcionalitats principals que proporcionen els clients de missatgeria instantània són: comunicació de text, àudio i vídeo, transferència de fitxers, compartició d'escriptoris, ubicacions en els mapes, trucades telefòniques, etc.

Els principals clients de **missatgeria instantània mòbil** són: WhatsApp, Line i Telegram.

Altres clients de **missatgeria instantània** són: Hangouts, Pidgin (multixarxa), Skype, Trillian (multixarxa) o Viber.

2.7. Accés a ordinadors remots

Una de les aplicacions de l'accés remot a ordinadors és la de poder administrar un equip des d'un altre equip a través de la xarxa. També s'utilitza en les organitzacions per a permetre que els seus treballadors accedeixin als servidors de l'empresa, ja sigui des de l'oficina o des de les seves llars.

El protocol **Telnet** és el protocol que es va emprar a Internet o en xarxes d'àrea local per a proporcionar una comunicació bidireccional interactiva en l'accés a ordinadors remots. Es basa en el protocol de transport TCP, utilitzant el port 23. Normalment segueix el model client/servidor.

SSH (acrònim de *Secure Shell*) és un protocol que s'utilitza per a accedir a màquines remotes a través de la xarxa. Soluciona la falta de seguretat del protocol Telnet, al que se li afegeixen les següents funcionalitats: permet el xifratge per a evitar que es puguin interceptar les dades que s'envien i permet l'autenticació amb clau pública (que detallarem en el proper mòdul) per a assegurar que l'ordinador remot és qui diu ser.

El port estàndard per a contactar amb un servidor SSH és el port 22.

Telnet i SSH són protocols basats en text (i.e. no gràfics). Per això es van desenvolupar algunes aplicacions que permetessin una administració gràfica remota com: **VNC** (*Virtual Network Computing*) i **RDP** (*Remote Desktop Protocol*).

VNC és un desenvolupament multiplataforma que disposa d'implementacions lliures per a diferents sistemes operatius, de les que destacarem **TightVNC**. Permet controlar la pantalla d'un equip des d'un altre equip de forma remota. Per tant, hi ha una exportació de l'escriptori d'un equip (servidor VNC) que és importat a un altre equip remot (client) mitjançant un visor. El port TCP d'un servidor VNC és el 5900.

Una altra aplicació que també permet una gestió remota, molt utilitzada actualment, és **TeamViewer** (també disponible com a aplicació per a dispositius mòbils – apps-): http://www.teamviewer.com/es/

El protocol **RDP** (*Remote Desktop Protocol*) és un protocol propietat de Microsoft. És el que fa servir el servei anomenat *Terminal Services*. Aquest servei utilitza per defecte el port TCP 3389 en el servidor per a rebre les peticions.

Cal esmentar també en aquest apartat que una altra via per a l'administració remota és l'ús d'aplicacions locals, com navegadors web, que transmeten la interacció de l'usuari mitjançant algun protocol de xarxa cap a l'equip administrat. En el cas dels navegadors web, la interacció utilitzarà els protocols HTTP i HTTPS. Amb aquesta opció, el client no necessita disposar de cap aplicació addicional.

3. Utilitats TCP/IP dels sistemes operatius

En les xarxes en les que s'utilitza el protocol TCP/IP, els sistemes operatius disposen d'un conjunt d'**utilitats** o **petites aplicacions** que ens faciliten informació sobre la nostra configuració de xarxa o de les connexions i sobre el rendiment de la xarxa. Per tant, ens poden ser d'utilitat per esbrinar i solucionar problemes de funcionament i rendiment de la xarxa local.

Entre les utilitats més destacades en entorns **Windows** (moltes d'elles també disponibles en entorns **Unix/Linux**) trobem: Ipconfig/ifconfig, Ping, Tracert, hostname, Arp, Netstat, Nslookup, getmac... El **sistema operatiu d'Apple OS X** també incorpora eines amb aquestes funcionalitats: analitzador del Sistema, preferències del sistema, utilitat de xarxa (que inclou comandes com ping, traceroute, netstat, finger...), terminal...

Tot i que, per la seva funcionalitat en alguns casos, ja s'han tractat en mòduls anteriors, atenent que són realment aplicacions, en fem un recull també en aquest mòdul.

Passem a descriure breument algunes d'aquestes utilitats:

1) ipconfig: En concret, *ipconfig* ens pot ser d'utilitat per a solucionar un problema de xarxa TCP/IP, ja que ens permet comprovar la configuració de TCP/IP en l'equip que té el problema. Podem utilitzar la comanda ipconfig per obtenir informació de la configuració de l'equip, incloent l'adreça IP, la màscara de subxarxa i la porta d'enllaç predeterminada. A les primeres versions de Windows, aquesta comanda se l'anomenava *winipcfg* en lloc d'*ipconfig*.

Permet visualitzar els valors de configuració de xarxa del TCP/IP. Per a visualitzar els seus paràmetres principals podem executar ***ipconfig/all***, el qual permet visualitzar els paràmetres de la configuració.

2) ping: La comanda *ping* ajuda a comprovar la connectivitat en el nivell IP, és a dir, permet comprovar si un equip o dispositiu de la xarxa, amb una IP assignada, es troba actiu dins d'aquesta xarxa. Podem utilitzar *ping* per enviar una sol·licitud a un nom d'*host* o a una adreça IP de destinació. Així podrem comprovar si podem connectar-nos a altres equips o altres recursos de la xarxa.

Per tant, la comanda *ping* és una ordre que envia paquets a un ordinador remot i espera la seva resposta.

3) hostname: Permet visualitzar el nom de la màquina local.

4) netstat: Windows (i també Linux) ens ofereixen una eina que ens va mostrant quines connexions de xarxa tenim a cada moment. Per executar-la podem fer: **netstat –an**.

Per entendre millor quines connexions tenim obertes, el millor és que abans d'executar aquesta ordre tanquem tots els programes a excepció de MSDOS (el que tenim actiu amb Símbol del sistema), per així anar comprovant des del principi quines connexions tenim i quines es van obrint.

Si volem que s'actualitzi automàticament la informació, podem escriure **netstat -an 5** (on 5 pot ser qualsevol número i fa referència a l'interval d'actualització, que pot ser, el nombre de segons que han de passar perquè s'actualitzi la informació).

Per obtenir una petita ajuda en relació amb netstat executarem: **netstat /help**

5) tracert: El programa *tracert* de Windows (*traceroute en Unix)* permet veure per quins routers passa una connexió d'Internet. Proporciona també informació sobre el temps que triguen els paquets en anar i tornar a aquests *routers*.

Per emprar tracert amb Windows, només cal executar, per exemple: tracert www.google.com.

També podem trobar aquesta eina per Mac OS X, anant a Aplicacions/Utilitats i obrint l'aplicació "Utilitat de Xarxa", dins trobarem la pestanya traceroute on a l'escriure el domini o IP, es començarà a traçar la ruta.

6) nslookup: Amb aquesta aplicació ens estem connectant als nostres servidors DNS per poder arribar a conèixer la IP d'un *host* concret. Per exemple, si escrivim nslookup www.yahoo.com, obtindrem la IP d'aquest servidor.

7) getmac: Mostra les adreces MAC dels adaptadors de xarxa que tinguem instal·lats en el sistema. Aquest nombre identifica de manera única cada adaptador de xarxa.

8) Arp: Cadascun dels equips que utilitzen TCP/IP disposen d'una taula ARP amb la qual van enregistrant les adreces IP i les adreces MAC associades. Amb aquesta ordre es visualitza aquesta taula amb les adreces estàtiques i dinàmiques, permetent també incorporar-hi noves entrades (adreces estàtiques). Cadascuna de les entrades o registres d'aquesta taula tenen un temps de vida màxim, anomenat *time to live* o TTL, i quan aquest expira, l'entrada corresponent és esborrada de la taula.

4. Aplicacions multimèdia i els seus protocols

En aquest apartat descriurem tota una sèrie de tècniques i protocols per a treballar amb continguts multimèdia a la xarxa Internet, tot i que també són extensibles a altres tipus de xarxes, com per exemple xarxes de videovigilància.

En els darrers anys han aparegut moltes aplicacions que permeten transmetre àudio i vídeo a través d'Internet, com per exemple: *streaming* de vídeo, telefonia IP, àudio i vídeo conferències, radio i TV per Internet, etc.

Aquestes aplicacions tenen uns requisits molt diferents als de les aplicacions tradicionals com la transferència de fitxers, correu electrònic...

Les aplicacions multimèdia tenen una **alta tolerància a pèrdues de dades** en la transmissió i, en canvi, són **molt sensibles als retards temporals** que es puguin produir en aquesta comunicació. Que no es vegi uns quants bits d'un vídeo o siguin erronis pot ser no detectable per a l'ull humà, però, en canvi, un retard d'uns centenars de mil·lisegons, pot fer que el vídeo arribi entretallant-se.

Les **xarxes multimèdia** són aquelles que s'utilitzen primordialment per al tràfic de veu, àudio i vídeo. Atenent que han de treballar amb continguts multimèdia, cal que tinguin molt en compte els retards, el ***jitter*** i una mínima amplada de banda, a més a més dels paràmetres de qualitat que tota xarxa de dades ha de disposar.

Jitter

Un *jitter* en telecomunicacions és una variabilitat en el temps d'execució dels paquets. Pot tractar-se d'un retard o d'un avançament, que en aplicacions multimèdia provoca que no es puguin executar adequadament.

Per tant, en les aplicacions multimèdia, hi ha tolerància pel que fa a la pèrdua de dades, sempre i quan no hi hagi retards i les pèrdues siguin ocasionals.

Per a poder satisfer aquests requisits, s'utilitzen dos mecanismes clau:

- Mecanismes de compressió específics per a cada tipus de tràfic.
- Protocols de comunicació que optimitzin la transmissió de dades en base als requeriments esmentats.

Coneixem que el nivell de transport ofereix tota una sèrie de serveis al nivell d'aplicació, però cada aplicació té uns requisits diferents i, per tant, el nivell de transport els ha de satisfer. Els protocols originals d'Internet TCP i UDP es concentraven només amb transferències fiables, ja que les primeres aplicacions no eren en temps real. A mesura que s'han anat desenvolupat aquest tipus

d'aplicacions, s'han especificat nous protocols de transport que són els que tractarem en aquest tema per a oferir aquests nous serveis relacionats amb el multimèdia.

4.1. Exemples d'aplicacions multimèdia

Actualment a la xarxa Internet hi ha molts tipus d'aplicacions multimèdia. Podem classificar-les en tres grans tipus:

1) *Streaming* d'àudio/vídeo emmagatzemat.
2) *Streaming* en directe.
3) Àudio i vídeo en temps real interactiu.

Són situacions molt diferents al cas clàssic de descarregar un contingut multimèdia i després visualitzar-lo, el qual ja quedaria cobert amb una transferència de fitxers amb protocols HTTP i FTP.

4.1.1. *Streaming* d'àudio i vídeo emmagatzemats

Amb aquest tipus d'aplicacions, els clients demanen continguts d'àudio i vídeo comprimits que es troben emmagatzemats en servidors. Aquests continguts poden ser programes de televisió o de ràdio, vídeos, música, etc.

Aquestes aplicacions es caracteritzen perquè els continguts estan **emmagatzemats prèviament en un servidor**, així l'usuari pot aturar la reproducció, rebobinar... utilitzen la **tècnica de l'*streaming*** i una **reproducció continua**, per tant, sense gaires retards.

La reproducció en temps real (***streaming*** en anglès) és una tècnica que permet reproduir fitxers d'àudio i de vídeo. Amb l'*streaming*, l'usuari veu una part del contingut i la resta es va rebent a mesura que es reprodueix.

4.1.2. *Streaming* en directe d'àudio i vídeo

Aquest tipus d'aplicacions funcionen com el *broadcast* tradicional de ràdio i televisió, on un emissor transmet a molts receptors, però en aquest cas es porta a terme en una xarxa com Internet.

En aquest cas, el contingut multimèdia no es troba emmagatzemat, per tant, l'usuari no pot avançar en la seva reproducció.

Es requereix una reproducció contínua i es poden donar retards rellevants a l'inici de la reproducció.

4.1.3. Àudio i vídeo en temps real interactiu

Aquest tipus d'aplicacions permeten que els usuaris interactuïn en temps real de forma síncrona. Corresponen a aplicacions que permeten establir connexions d'àudio i/o vídeo, trucades telefòniques i/o videoconferències, com per exemple Google Talk o Skype. Són aplicacions especialment sensibles als retards.

4.2. Compressió d'àudio i vídeo

Per a enviar dades multimèdia (àudio i vídeo) per Internet, primer cal digitalitzar i comprimir aquestes dades.

El perquè de digitalitzar el trobem en el fet que les xarxes de computadors transmeten bits; i el fet de comprimir ve donat perquè l'àudio i el vídeo sense comprimir ocupa molt espai i, per tant, la seva transmissió pot arribar a consumir molta amplada de banda.

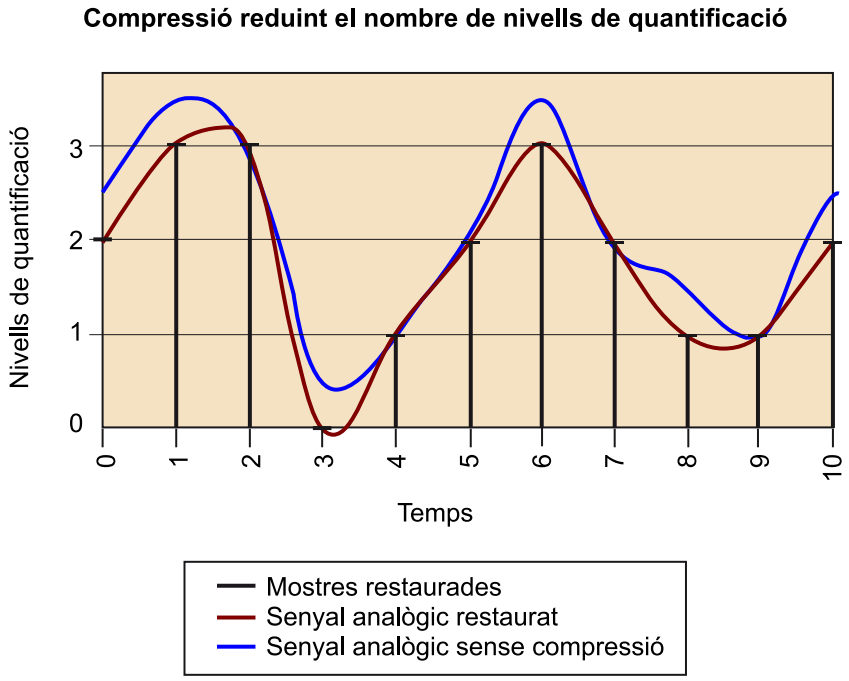
4.2.1. Compressió d'àudio

Una de les tècniques de compressió d'àudio és la de tipus **PCM** (*pulse code modulation*), que es basa en la recollida de mostres d'àudio a una freqüència determinada. El valor de cada mostra escollida s'arrodoneix a un valor discret i, per tant, es pot representar amb una nombre finit de bits que dependrà del nombre de valors que podem prendre de les mostres.

En definitiva, PCM és un procediment de modulació utilitzat per a transformar un senyal analògic en una seqüència de bits.

En el cas concret de PCM, utilitzat en la codificació de veu, es recullen 8.000 mostres per segon i cada mostra es representa amb 8 bits. Per tant, es tindrà un senyal digital amb una taxa de 64.000 bits per segon (64kbs). A partir del senyal digital obtingut es podrà recuperar el senyal analògic, tot i que lògicament, pel mostreig utilitzat, no serà exactament el mateix que l'original. En el cas de recollir més mostres, el senyal analògic descodificat serà més semblant a l'original.

Figura 9



En aquest gràfic apreciem com el senyal analògic continu (en color blau) es discretitza en les mostres (color negre). I com a partir d'aquestes mostres es reconstrueix un senyal analògic molt semblant a l'original (en color vermell).

Per a les compressions de so amb qualitat, una de les tècniques més emprades és l'estàndard **MPEG 1 Layer 3**, més conegut com **MP3**. Les seves taxes de compressió són de 96 kbps, 128 kbps i 160 kbps.

4.2.2. Compressió de vídeo

El vídeo és una successió d'imatges trameses a una taxa constant, que pot ser d'unes 24 o 30 imatges per segon. Una imatge sense comprimir presenta una successió de píxels, en la que cada píxel es representa amb un cert nombre de bits que indiquen el color i la lluminositat.

Les tècniques de compressió de vídeo estan basades en reduir la redundància que presenten les imatges consecutives del vídeo (redundància temporal), a més de la redundància pròpia dins de la mateixa imatge (redundància espacial). Reduint aquestes redundàncies s'aconsegueix la compressió del vídeo.

Un dels estàndards més emprats en compressió de vídeo és MPEG, en les seves diferents versions.

4.2.3. Formats d'àudio i vídeo

Els formats d'àudio més coneguts són:

- **WAV**: acrònim de ***Waveform Audio Format***, és un format d'àudio originari de Microsoft que permet enregistrar so en diferents qualitats, d'11.025 a 44.100 Hz. Ara bé, com que els arxius WAV tenen una qualitat de so molt alta solen ocupar molt espai (per exemple, un arxiu d'àudio amb una du-

rada de tres minuts pot ocupar de 20 a 30 MB al disc). Una de les principals avantatges del format WAV és la seva possibilitat de conversió a altres formats (per exemple, a MP3).

- **AIFF**: acrònim de ***Audio Interchange File Format***. Té unes característiques molt similars a les del format WAV. Va ser dissenyat per als sistemes operatius Apple.

Actualment, els formats WAV i AIFF ja no s'utilitzen tant a l'existir formats amb una compressió més alta i una qualitat semblant, com, per exemple, el format MP3. Ambdós formats no permeten realitzar *streaming*, però s'utilitzen com a base per a altres formats com RealAudio. Si es comprimeixen perden molta qualitat.

- **MP3**: és un format de compressió d'àudio creat pel grup Moving Picture Experts Group, sota la supervisió de la ISO. Els arxius d'aquest format s'identifiquen amb l'extensió **.mp3**. És un dels formats més populars a Internet, ja que ofereix una bona qualitat de so, amb una elevada compressió de dades. Es pot realitzar *streaming* amb aquest format i també es pot baixar amb HTTP o FTP.

- **MP4**: És un nou format d'àudio basat en l'estàndard de codificació avançada d'àudio. S'utilitza amb diferents extensions:
  - .mp4: Extensió oficial per a àudio, vídeo i continguts avançats.
  - .m4a: és l'extensió adoptada per Apple per a la distribució de música en iTunes i per ser reproduïda en els seus dispositius.

- **MIDI**: Prové de les sigles de *Musical Instrument Digital Interface*, la interfície digital per a instruments musicals. És un protocol de comunicació estàndard utilitzat per a comunicar instruments digitals electrònics i, per tant, dades entre sintetitzadors, programes, processadors d'efectes i altres dispositius. Es tracta d'un format utilitzat en l'àmbit de la composició musical i generalment té l'extensió **.mid**. Ocupen molt poc i per tant, són idonis per a connexions amb poca amplada de banda. Amb aquest format no es pot realitzar *streaming*.

- **Real Audio**: és un format utilitzat a Internet per a la reproducció en temps real, de manera que l'arxiu es reprodueix mentre es descarrega. La seva problemàtica va associada amb què al ser arxius excessivament grans, cal una gran capacitat d'emmagatzematge.

Entre la diversitat de formats de vídeo existents destacarem:

- **MPEG**: Estàndard desenvolupat per ***Moving Picture Experts Group*** (d'aquí les sigles MPEG), un grup de treball coordinat entre d'altres per la ISO. Suporta tres tipus d'informació: àudio, vídeo i *streaming*. Ofereix una al-

ta compressió amb poques pèrdues, per tant, és un dels formats més emprats. Des de l'any 1991 han anat apareixent diferents versions: MPEG-1, MPEG-2... Des de la web oficial de MPEG podem veure les característiques de les diferents versions: http://mpeg.chiariglione.org/.

- **QuickTime Movie**: és un format propietat d'Apple. La seva extensió és **.mov**. Es pot visualitzar amb el reproductor QuickTime, que permet realitzar vídeos del mateix format i disposa d'algunes opcions bàsiques per a editar-los. Inicialment estava pensat només com a format de vídeo, però actualment es pot emprar per a qualsevol tipus de medi (imatges, àudio, vídeo, Flash, etc). Amb un servidor de vídeo dedicat és possible realitzar *streaming* de vídeo d'aquest format.

- **Real Media**: És un dels formats més emprats per a realitzar *streaming*. És un format propietat de Real Networks.

- **Windows Media Video**: desenvolupat per Microsoft per al seu reproductor Windows Media Player. Els arxius d'aquest format tenen extensió **.wmv**, que correspon a l'arxiu que conté vídeo; **.wma**, que conté àudio, i **.asf** (*Advanced Streaming Format*) com a format per *streaming*.

- **AVI**, ***Audio/Video Interleaved***: és un format que va ser definit per Microsoft i que posteriorment va ser millorat i anomenat AVI 2.0. Aquest format permet emmagatzemar simultàniament un flux de dades de vídeo i diversos fluxos d'àudio (és a dir, que pot contenir bandes sonores en diversos idiomes). Ha estat substituït pel format Windows Media. Amb aquest format no és pot realitzar *streaming*, ja que s'ha de emmagatzemar primer el contingut i després reproduir-lo.

- **Flash video**. és un format de vídeo creat per Flash que permet realitzar *streaming*. L'extensió dels fitxers en aquest format és **.flv**. Funciona amb l'aplicació Flash Player. Permet les mateixes funcionalitats que les animacions efectuades amb Flash (fitxers **.swf**).

4.3. Protocols per a aplicacions interactives en temps real

El creixement exponencial d'Internet, amb un accés ràpid a la descàrrega de fitxers grans, fa que les tecnologies, en definitiva els protocols associats, vagin evolucionant.

Com a alternativa a la utilització dels serveis estàndards d'Internet FTP i HTTP per a la transferència de dades, sobretot amb informació multimèdia, es realitza una transferència que sigui processada com un flux regular i continu, sense

que calgui esperar que la informació multimèdia hagi arribat completament per a ser reproduïda. Això és el que s'anomena reproducció en temps real (o *streaming*).

La **reproducció en temps real (*streaming*)** transmet informació multimèdia en temps real utilitzant el protocol **RTSP** (*Real Time Streaming Protocol*) junt amb altres protocols de transport en temps real com **RTP** (*Real-time Transport Protocol*) i el control de sessió dinàmic **RTCP** (RTP *Control Protocol*). L'*streaming*, i aquí està el seu avantatge, no utilitza la màxima amplada de banda de què disposa el client, sinó només l'amplada de banda necessària per anar reproduint els continguts en temps real. A més, no es realitza una descàrrega complerta dels continguts, sinó que a mesura que es reprodueixen els va descarregant.

Depenent de com s'obtingui la informació a difondre, la reproducció en temps real es pot dividir en dues categories:

- **Reproducció del temps real en directe**, es porta a terme la transmissió dels esdeveniments en el mateix moment que estan succeint. En aquest tipus de transmissió, s'utilitza el terme de *broadcast* (difusió), ja que s'està transmetent "en directe" la mateixa informació a tots els clients.

- **Reproducció en temps real multimèdia a la carta**, o **VoD**, *Vídeo on Demand* o **AVoD**, *Audio and Video on Demand*, són sistemes que permeten als usuaris la selecció i reproducció de continguts d'àudio i vídeo sota demanda.

4.3.1. RTSP. *Real Time Streaming Protocol*

Aquest protocol estableix i controla un o varis *streamings* sincronitzats de dades multimèdia (àudio i vídeo). Porta el control remot de l'enviament mitjançant una xarxa de servidors de dades multimèdia.

En RTSP no hi ha connexions, només sessions mantingudes pel servidor. I cada sessió té el seu identificador. Així una sessió RTSP no està lligada a una connexió a nivell de transport, per tant, es pot emprar tant TCP com UDP. També pot arribar a treballar juntament amb altres protocols de transport com RTP i RTCP.

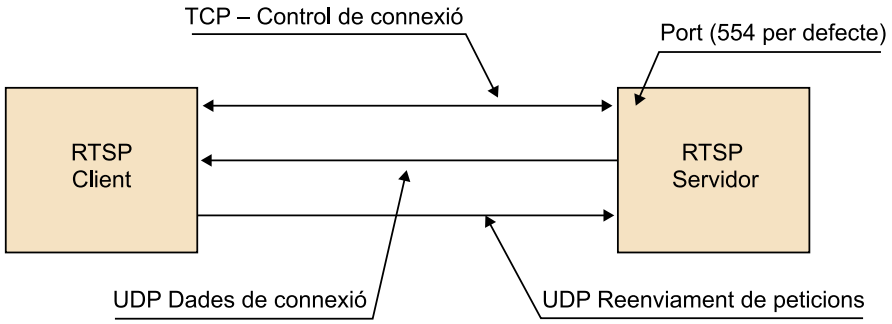
Aquest protocol està especificat en l'RFC 2326.

Les operacions que es porten a terme en aquest protocol són:

- Recuperació de dades del servidor de continguts multimèdia.

- Invitació d'un servidor de dades a una conferència.
- Afegir contingut a una presentació existent.

Figura 10



Esquema de funcionament del protocol RTSP.

4.3.2. RTP. *Real Time Transport Protocol*

És un protocol de nivell d'aplicació desenvolupat per l'*Audio-Video Transport Working Group* de la IETF (*Internet Engineering Task Force*) que s'utilitza per a enviar qualsevol tipus de format: PCM, MP3, etc. per a àudio o H.263 per a vídeo.

És un protocol complementari a altres protocols de temps real, com SIP o H.323, que descriurem posteriorment.

Funciona sobre el protocol de transport UDP. L'emissor encapsula un tros de dades dins del paquet RTP, que també s'encapsula dins d'un segment UDP, dins d'un paquet IP. El receptor extreu les dades RTP del segment UDP i les passa al reproductor per tal que aquest descodifiqui el contingut i el reprodueixi. Per tant, fixem-nos que es reconeix en els extrems, i els encaminadors no es preocupen del contingut dels paquets IP que hi circulen.

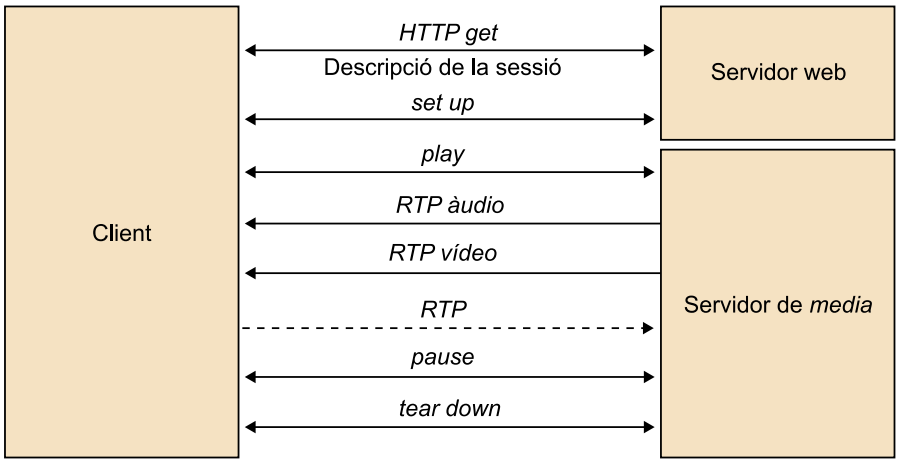
De fet, RTP el que fa es facilitar la interoperabilitat entre aplicacions multimèdia.

Aquest protocol no es preocupa que les dades arribin a destinació o tinguin la qualitat adequada, ni garanteix que els paquets arribin ordenadament.

4.3.3. RTCP. *Real Time Control Protocol*

Aquest protocol utilitza el mateix mecanisme de distribució que el protocol RTP i es basa en la transmissió periòdica de paquets de control a tots els participants en una sessió.

Figura 11



Funcionament del protocol RTP/RTCP.

RTCP realitza quatre funcions bàsiques:

1) Dóna informació sobre la qualitat de les dades distribuïdes.

2) Manté un identificador persistent que fa que si algun identificador canvia es puguin recuperar els participants de la sessió.

3) Controla la taxa d'enviament, per si hi hagués un nombre massa elevat de participants.

4) Aquesta funció és opcional. Correspon a la de comunicar un mínim d'informació de control de la sessió, com per exemple que es mostri la identificació d'un participant en la interfície d'usuari.

4.3.4. SIP. *Session Initiation Protocol*

SIP (*Session Initiation Protocol*) és un protocol del nivell d'aplicació que permet inicialitzar, modificar i finalitzar sessions interactives, que impliquin elements multimèdia com vídeo, veu, missatgeria instantània, jocs en línia, realitat virtual, etc. Una de les seves principals aplicacions és en les **conferències *multicast***, és a dir, aplicacions amb diferents usuaris alhora. Juntament amb el protocol H.323 també és un dels principals protocols emprats per **VoIP**.

Nota

Multicast, o difusió selectiva, és l'enviament de paquets d'informació a múltiples destinataris d'una xarxa de forma simultània.

Nota

VoIP (acrònim de *Voice over* IP), anomenada també telefonia IP, és una tecnologia que permet mantenir converses amb veu a Internet, o en qualsevol xarxa que utilitzi el protocol TCP/IP. Per tant, el senyal de veu s'envia en forma digital, en paquets, en lloc d'enviar-se en forma digital o analògica a través de circuits de telefonia convencionals.

Treballa en cooperació amb altres protocols com **RTP i RTCP**, per al transport i control d'enviament de dades, i **RTSP** per al control del *streaming* de dades multimèdia; i permet que aplicacions que utilitzen els usuaris per a comunicar-se puguin posar-se d'acord amb el tipus de sessió que volen compartir.

SIP no ofereix serveis, sinó primitives que es poden utilitzar per a oferir diferents tipus de serveis. Permet gestionar sessions de forma independent dels protocols de transport que hi hagi per sota. Els clients SIP habitualment usen el port TCP i UDP 5060 per a connectar-se als servidors SIP.

4.3.5. H.323

És un protocol alternatiu a SIP, molt emprat per transmetre àudio i vídeo en temps real. Està dedicat a la transmissió de veu sobre IP (VoIP). De forma opcional, també pot donar suport al vídeo.

Permet establir comunicació entre un equip connectat a Internet i un telèfon connectat a la xarxa telefònica.

Dins de les seves especificacions inclou com negociar les codificacions d'àudio i vídeo entre els extrems de la comunicació, com s'envien els trossos d'àudio i vídeo (utilitza RTP), com els equips es comuniquen amb els seus *gatekeepers* (commutadors virtuals opcionals que permeten la comunicació entre terminals H.323) i com els equips connectats a Internet es connecten amb els telèfons connectats a la xarxa telefònica.

Com a diferències entre els protocols SIP i H.323 tenim:

- H.323 és un servei integrat de protocols per a portar a terme conferències multimèdia, segons les especificacions esmentades, mentre que SIP només s'encarrega de l'inici i gestió de la sessió, sense cap tipus d'imposició en el transport o en els formats d'àudio i vídeo suportats.

- H.323 va ser definit per la ITU, per tant, des de la vessant de telefonia, mentre que SIP va ser definit per la IETF, per tant, des de la vesant d'estàndards d'Internet.

- H.323 és un estàndard més complex que SIP i, per tant, SIP és més senzill d'implementar.

4.3.6. Skype.

És un sistema de telefonia d'igual a igual (*peer-to-peer*, P2P) que funciona sobre la xarxa Internet. Va ser desenvolupat per l'equip que va fer KaZaA l'any 2003, fundat per Niklas Zennström i Janus Friis, basant-se en el mateix protocol que utilitzava aquest anomenat **FastTrack**. L'any 2011 va ser adquirit per Microsoft.

És la competència d'estàndards de transmissió de veu sobre IP com **SIP** o **H.323**.

Entre les seves funcionalitats, trobem l'àudio i videoconferències gratuïtes.

En aquesta pàgina podem trobar totes les seves funcionalitats:

http://www.skype.com/es/features/

L'arquitectura que implementa **Fastrack** és la d'una xarxa superposada (overlay network, en anglès), amb dos tipus de nodes: els nodes normals i els supernodes. Un node normal correspon a l'ordinador on l'usuari instal·la l'aplicació Skype i permet fer trucades i missatges de text. Entra a la xarxa amb el seu usuari i paraula de pas i així es connecta a un supernode que pot ser qualsevol altre node amb Ip pública i prous recursos. Un altre element, el servidor d'entrada és el que emmagatzema a tots els usuaris i paraules de pas de tota la xarxa Skype. Tot i així, a part d'aquesta validació, totes les altres operacions a la xarxa es fan de forma totalment descentralitzada.

Considerant que el seu codi és tancat i el protocol propietari, es dificulta la interoperabilitat amb altres sistemes.