El nivell de xarxa

PID_00218426

Ramon Musach Pi

Universitat Oberta de Catalunya

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

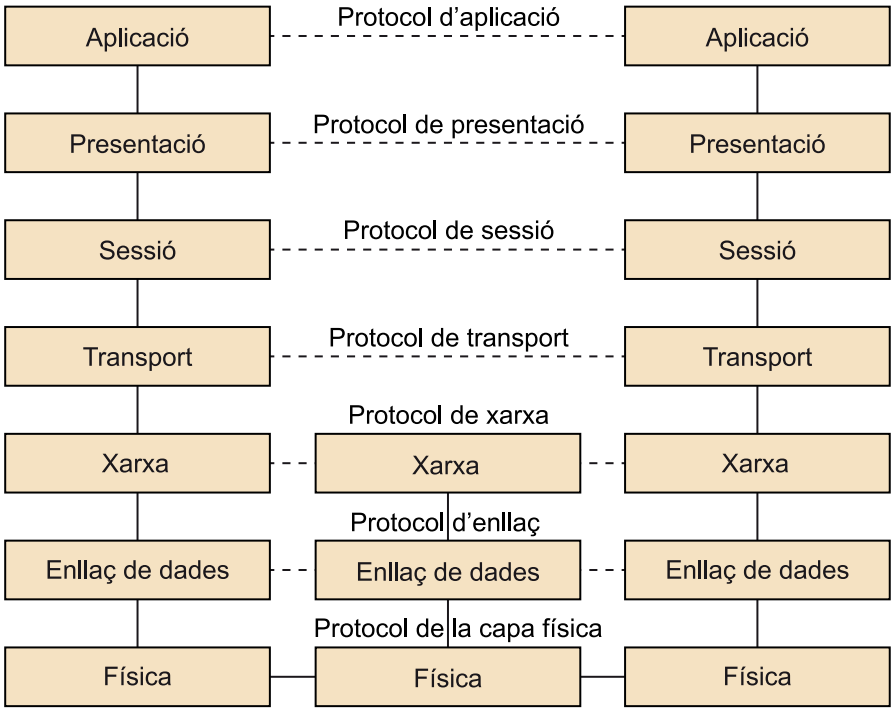
Introducció

El nivell de xarxa s'encarrega de transferir informació entre sistemes finals mitjançant alguna xarxa de comunicació. Proporciona connectivitat i ofereix mecanismes per a la selecció del millor camí entre dos nodes de la xarxa, independentment que els nodes estiguin en xarxes diferents, fins i tot, molt separades geogràficament.

Allibera a les capes superiors, que tractarem en els dos propers mòduls, de com es realitza la transmissió de dades i de les tecnologies de commutació emprades en les capes inferiors (física i d'enllaç).

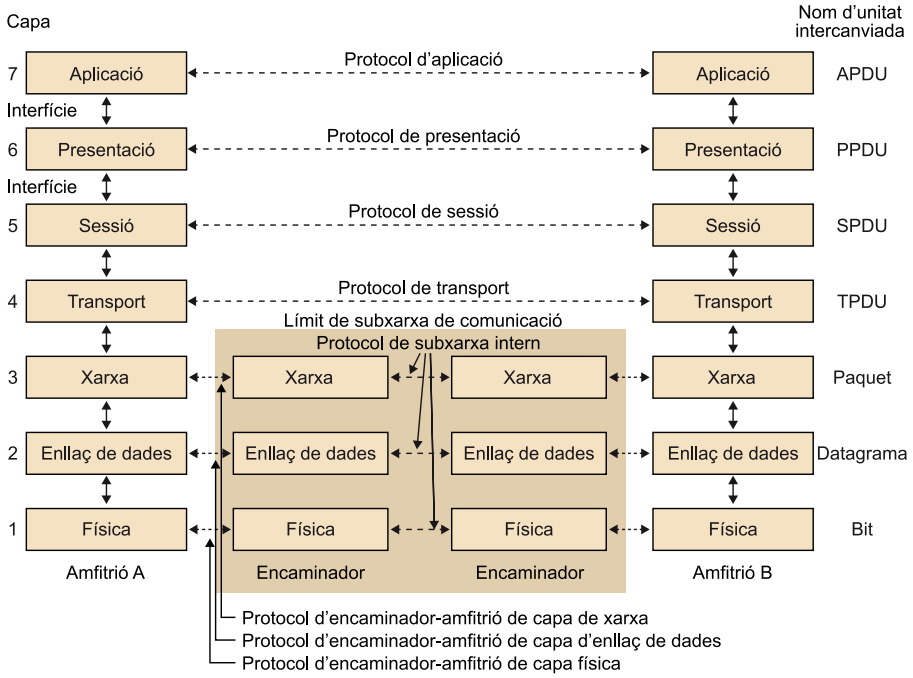
En el següent esquema, veiem com les tres capes inferiors estan relacionades amb la connexió i la comunicació amb la xarxa. Els paquets transmesos, creats per l'emissor, passen a través d'un o més nodes de la xarxa, que actuen com a retransmissors, fins arribar al node destí.

Figura 1



Esquema que relaciona els diferents protocols de l'emissor, del receptor i d'un node intermedi. Podem apreciar que en el node intermedi només s'implementa fins el nivell de xarxa.

Figura 2



En aquest esquema s'entra en més detall del procés de comunicació que es pot establir entre un node emissor i un receptor, amb un node intermedi. Podem apreciar que en el node intermedi, les capes física, d'enllaç i de xarxa donen suport a les dues tipologies de xarxa que uneix i, per tant, implementa els protocols necessaris per a una xarxa i per l'altre.

La capa de xarxa no és una capa d'extrem a extrem, en canvi sí que ho serà la capa de transport que tractarem en el proper mòdul. La **capa de transport** és la primera capa d'extrem a extrem entre sistemes finals (emissor i receptor). Per tant, són els nodes finals els que arriben a implementar tots els nivells, a diferència dels nodes intermedis (routers), que es queden en el tercer nivell (i.e. capa de xarxa).

Nota

Pel que fa al model d'Internet, aquest és un model **TCP/IP**, on per sobre del nivell de xarxa física, està el nivell **IP** o nivell Internet (nivell de *internetworking*).

Quan dos equips no estan connectats a la mateixa xarxa, cal emprar nodes intermedis anomenats **routers** (en català, encaminadors). Aquests nodes són els encarregats de connectar dues xarxes o més, amb la finalitat que les dades d'una xarxa arribin a la destinació de l'altra. Per a poder conèixer cap on es poden dirigir els paquets que van arribant, els routers disposen d'unes taules, anomenades **taules d'encaminament**. Per a poder portar a terme aquestes funcions cal que tant els routers com els equips finals disposin d'un identificador únic que permeti localitzar-los unívocament per tal que se'ls pugui enviar la informació. En particular, a la xarxa Internet, aquests identificadors es coneixen com a **adreces IP**.

Nota

A Internet, els routers només implementen fins el nivell IP (nivell de xarxa), mentre que TCP (nivell de transport) només s'implementa en els extrems, és a dir, en els ordinadors o equips finals.

Les funcions de la capa de xarxa van relacionades amb l'adreçament, encaminament i la definició de les rutes. En concret, es disposa de:

- Protocols que descriuen la manera d'enviar la informació.
- Protocols d'encaminament que decideixen per on han de passar els paquets fins arribar a la destinació.

- Mecanismes per informar d'errors que es produeixin en l'enviament d'aquests paquets.

Dins d'aquest nivell IP (o nivell de xarxa) tenim diferents protocols com l'**IP** (*Internet Protocol*), **ICMP** (*Internet control message protocol*) i **ARP** (*Adress resolution protocol*). Aquests tres protocols els tractarem en aquest mòdul.

1. *Internet Protocol* (IP)

IP (*Internet protocol*) és un protocol de la capa de xarxa utilitzat per a identificar els nodes de la xarxa. Les identificacions de cadascun dels nodes es fan amb el que s'anomena **adreçament IP**. L'IP és un protocol de xarxa que actualment té dues versions, que analitzarem amb més detall: el **protocol IPv4** (llegit com "IP versió 4") i la seva extensió **IPv6** (llegit com "IP versió 6").

L'IP és un protocol **no orientat a connexió** i, per tant, no implementa mecanismes per a garantir la integritat de les dades que s'envien per la xarxa. Això vol dir que no té mecanismes que permetin detectar pèrdues de paquets de dades (anomenats datagrames) o garantir que es reben en el mateix ordre que han estat emesos, ja que d'això se n'encarrega la capa de transport que tractarem en el proper mòdul. Només verifica que no hi hagi errors en el contingut de la capçalera de cada paquet (o datagrama).

1.1. IPv4

Defineix el format que s'ha d'utilitzar per a enviar informació entre dos punts de la xarxa. Va ser proposat el 1981 en el document RFC-791.

Document RFC

Un **document RFC** o document de demanda de comentaris, en anglès *Request for Comments* és un recull de propostes sobre noves investigacions i metodologies relacionades amb les tecnologies d'Internet. Els documents arriben a tenir vigència quan són aprovats per **l'Internet Engineering Task Force** (**IETF**).

Figura 3

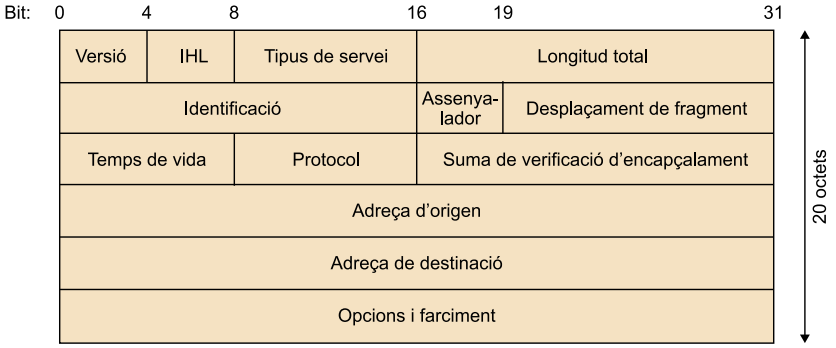
Network Working Group — Steve Crocker
Request for Comments: 1 — UCLA
7 April 1969

Title: Host Software
Author: Steve Crocker
Installation: UCLA
Date: 7 April 1969
Network Working Group Request for Comment: 1

Capçalera del primer document RFC (RFC-1) publicat el 7 d'abril de 1969.

Perquè la informació que es vol transmetre arribi a la destinació, aquesta no es pot enviar de qualsevol manera, sinó que cal empaquetar-la mitjançant el protocol IP. Cada paquet que es crea s'anomena datagrama, que serà la unitat mínima que es transmetrà per la xarxa. **Cada datagrama està format per una capçalera (o encapçalament IP) i les dades en sí que es volen enviar**. La capçalera IP conté una sèrie de camps de control, com per exemple: tota la informació de les màquines d'origen i de destí.

Figura 4



Capçalera d'IPv4.

A continuació, detallem el significat de cadascun dels camps que conformen la capçalera IPv4:

a) Versió: és un camp de quatre bits que indica la versió del protocol. En el cas de IPv4 pren el valor binari 0100 (4 en decimal), i per IPv6 el valor és 0110 (6 en decimal).

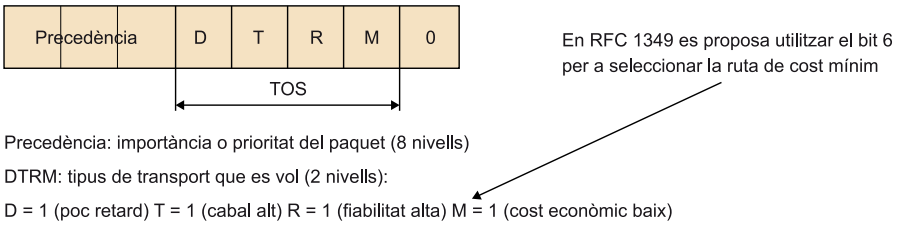
b) IHL: longitud de la capçalera. Atenent que la capçalera pot ser variable, ja que pot haver-hi o no opcions, cal explicitar la seva mida. S'expressa en paraules de 32 bits. Per tant, el nombre de bytes de la capçalera ha de ser múltiple de 4 i atenent que aquest camp té només 4 bits, la capçalera màxima que podem arribar a construir és de 60 bytes. Si no hi ha opcions, la capçalera IP ocupa com a mínim 20 bytes i el valor d'aquest camp és 5.

Capçalera mínima: 5 paraules x 32 bits/paraula = 160 bits x 1 byte/8 bits = 20 bytes.

Capçalera màxima: 15 paraules x 32 bits/paraula = 480 bits x 1 byte/8 bits = 60 bytes.

c) Tipus de servei (*type of service*): especifica amb 8 bits la qualitat de servei desitjada per aquest paquet (o datagrama).

Figura 5



Bits del tipus de servei.

Exemples concrets de bits del tipus de servei els podem trobar en aquesta taula:

	D	T	R	M
TELNET	1	0	0	0
FTP control	1	0	0	0
FTP dades	0	1	0	0
SNMP	0	0	1	0
NNTP	0	0	0	1

Exemple de l'ús dels bits del tipus de servei

d) Longitud total (*length*): és la longitud total del paquet, incloent-hi les dades i l'encapçalament.

e) Identificador del datagrama: és el número de seqüència del datagrama. Per tant, és el nombre únic amb el que s'identifica cada datagrama que es genera.

En el cas que la informació no càpiga en un únic datagrama, la informació es divideix en diversos datagrames, convertint-se en fragments de l'hipotètic datagrama original. En aquest cas, l'identificador identifica el número de fragment per tal que es pugui reconstruir la informació original (i.e. el datagrama hipotètic) a l'arribar a la destinació.

f) Assenyalador (*flags*): en aquest camp de 3 bits, els dos bits de menys pes controlen la fragmentació dels paquets. Un bit identifica si el paquet es pot fragmentar o si és l'últim fragment del paquet o no.

g) Desplaçament de fragment (fragment *offset*): indica la posició que ocupa el fragment actual en el paquet original mitjançant 13 bits.

h) Temps de vida (també conegut com a **TTL**, *Time To Live*): aquest camp és necessari perquè no quedin datagrames voltant indefinidament per la xarxa sense trobar la destinació. Determina el temps de vida del datagrama, és a dir, els salts (passos per routers) que pot fer un datagrama. Cada vegada que travessa un router, el valor que hi ha en aquest camp es decrementa en una unitat, i quan arriba a 0, el datragrama es descarta i s'envia un paquet especial de notificació a l'ordinador que l'ha generat per tal que sàpiga que s'ha descartat aquest datagrama i no ha arribat al seu destí.

i) Protocol: indica el tipus de paquet (anomenat segment) que transporta, per tant, quin protocol de capa superior (capa de transport) ha generat el paquet.

j) Suma de verificació d'encapçalament (*header checksum*): aquest camp serveix per a detectar errors en la capçalera (no errors en la informació que s'envia fora de la capçalera, és a dir, les dades en sí, ja que aquesta tasca correspon a nivells superiors). Són 16 bits de control per saber si existeix algun error de transmissió en l'encapçalament del paquet IP.

k) Adreça d'origen (*source address*): especifica l'adreça IP de la màquina que ha generat el paquet.

l) Adreça de destinació (*destination address*): especifica l'adreça IP de la màquina on ha d'arribar el paquet.

m) Opcions i farciment (*options and padding*): les opcions, si n'hi ha, permeten que admeti seguretat, o longitud variable. En el farciment s'hi afegeix zeros perquè l'encapçalament sigui múltiple de 32 bits.

1.1.1. Adreçament IP

Els nodes d'una xarxa s'identifiquen de forma única mitjançant una adreça. En l'adreçament IP, en concret **IPv4**, aquesta adreça és un nombre de 32 bits que identifica cadascun dels nodes i també la xarxa a la que estan connectats.

Nota

InterNIC va ser el primer organisme encarregat de les adreces IP i noms de domini. Actualment, és l'**ICANN** (acrònim d'***Internet Corporation for Assigned Names and Numbers,*** Corporació d'Internet per a l'Assignació de Noms i Nombres) qui té assignades aquestes tasques.

Per a simplificar l'escriptura d'aquestes adreces, els 32 bits es divideixen en 4 blocs de 8 bits cadascun d'ells (octets), emprant-se sovint notació decimal enlloc de notació binària. Així cada bloc serà un nombre entre 0 i 255 ($2^8 - 1$).

Exemple

La notació de l'adreça IP són quatre xifres entre 0 i 255 separades per punts. Per a poder calcular l'adreça de xarxa en binari caldrà passar les quatre xifres de forma independent a notació binària. Per exemple, l'adreça 192.168.0.185 en binari seria:

192.168.0.185 = 11000000.10101000.00000000.10111001.

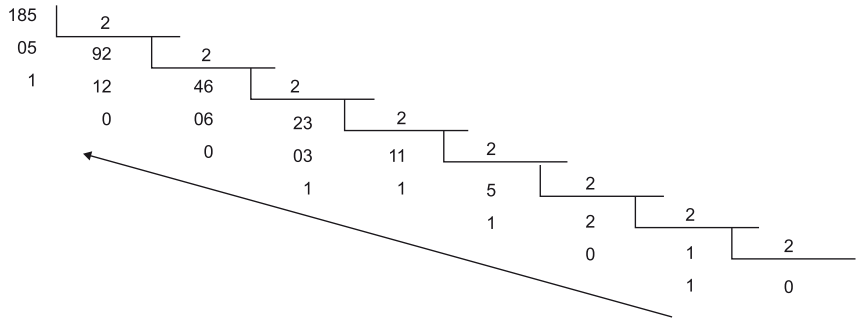
Sovint ens cal transformar nombres de decimal a binari i al revés. Expliquem com es pot portar a terme aquest procés, facilitant alguna calculadora que realitza aquesta conversió.

a) Conversió de decimal a binari

Per fer la conversió de decimal a binari cal començar a dividir el nombre entre 2 tantes vegades com faci falta. El valor binari del número decimal és la combinació del quocient de l'última divisió més tots els residus de totes les divisions en ordre invers (des de l'últim residu fins al primer).

Exemple: el nombre 185 es pot transformar en el seu valor binari 010111001, mitjançant el procés que es detalla en aquest gràfic:

Figura 6



b) Conversió de binari a decimal

Només cal anar multiplicant cada valor binari per la potència de 2 que correspongui atenent la seva posició.

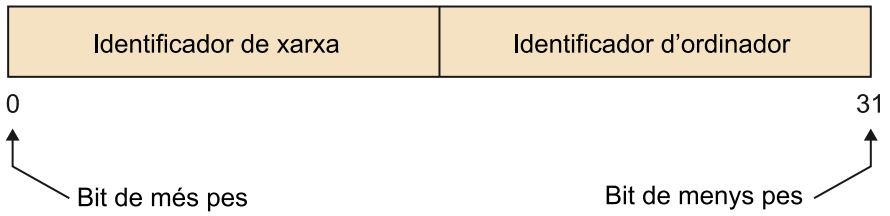
Exemple: Comprovem a quin valor decimal correspon el nombre binari 010111001

$1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 = 185$.

Com es pot veure, aquest format permet generar un gran volum d'adreces. La gestió d'aquest gran volum d'adreces pot ser complicat i, per tant, es va proposar que l'assignació d'adreces fos jeràrquica. Podem pensar per un moment com s'arribaria a gestionar l'adreçament si s'adjudiquessin les adreces de forma seqüencial tan bon punt ens connectem a la xarxa? Només pensem quants ordinadors hi ha al món que es connecten de forma simultània, al mateix temps. Només amb aquest fet ja tenim la resposta. Seria impossible!

Podem afirmar que una de les claus de l'expansió d'Internet és pel sistema d'adreçament jeràrquic que incorpora el protocol IP que utilitza. Així, a Internet, **les adreces IP estan compostes per dues parts**. Una part de l'adreça IP serveix per identificar la xarxa i el tros restant d'aquesta adreça IP és la que identifica l'equip o ordinador. Així doncs, les adreces es poden classificar i organitzar depenent de la xarxa a la que pertanyen.

Figura 7



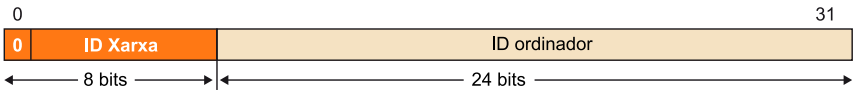
Els 32 bits (del 0 al 31) es reparteixen entre l'identificador de la xarxa i l'identificador de l'ordinador.

Els bits superiors de l'adreça IP són la part de xarxa, que ens indica la xarxa a la que pertanyen un conjunt d'equips; en definitiva, el router (encaminador) al que estan connectats aquests equips. En canvi, els bits inferiors de l'adreça IP identifiquen individualment cada equip dins la xarxa.

Inicialment, les xarxes es van dividir en 5 classes: A, B, C, D i E.

1) Xarxes de classe A. En les seves adreces, el primer bloc de 8 bit (octet) és el que identifica la xarxa, on el bit superior sempre és un **0** i els altres 3 blocs de 8 bits (24 bits) són els que identifiquen els equips de cadascuna d'aquestes xarxes. Com que el primer bit sempre és un 0, els 7 bits restants del primer bloc identifiquen la xarxa i la resta de bits -és a dir, 24- identifiquen els seus equips.

Figura 8

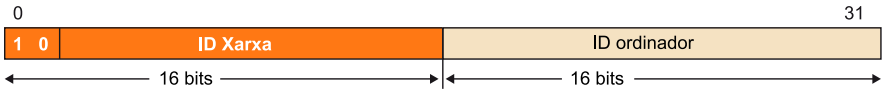


Aquestes adreces estan destinades a empreses molt grans i el fet de reservar tantes adreces per aquest tipus de xarxes ha donat lloc a la mancança actual d'adreces.

2) Xarxes de classe B. En una adreça de classe B els dos primers octets codifiquen les xarxes i del nombre total d'octets els dos bits que pesen més sempre valen **10**. Els 14 bits següents d'aquests dos primers octets s'utilitzen per a identificar les xarxes.

Els dos darrers octets (per tant, 16 bits) són els que identifiquen els equips connectats.

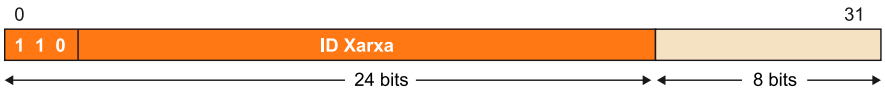
Figura 9



Adonem-nos que hi haurà més xarxes de classe B que de classe A, però cada xarxa de classe B accepta menys equips que una de classe A.

3) Xarxes de classe C. En les seves adreces, s'utilitzen els tres primers octets per a identificar les xarxes i es dedica l'últim a la identificació de cada equip. Els tres bits que pesen més de l'identificador de xarxa sempre tindran per valor el 110. I, en aquest cas, es disposa de 2^8 (256) adreces per a identificar equips en cadascuna d'aquestes xarxes.

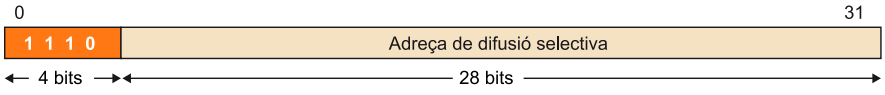
Figura 10



4) Xarxes de classe D. Es considera un tipus de xarxa especial que s'anomena xarxes de classes de multidestinació (en anglès, *multicast*). Es van crear per a permetre difusió selectiva o multicast en una adreça IP. Una adreça de difusió selectiva és una adreça exclusiva de xarxa que permet identificar el grup de computadores al que el missatge del multicast està dirigit. Per tant, una única estació pot transmetre simultàniament un sol corrent de dades a múltiples receptors. D'aquí que aquest tipus de trànsit se l'anomeni punt multipunt.

En les seves adreces, els quatre bits de més pes sempre valen 1110 i utilitza els 28 bits restants com a adreça de difusió selectiva.

Figura 11



5) Xarxes de classe E. Les seves adreces s'han reservat per a usos futurs. Normalment l'**IETF** (Comitè d'Experts en Enginyeria d'Internet o *Internet Engineering Task Force*) les fa servir per investigar i, per tant, no s'ha donat cap adreça de classe E per poder-la utilitzar a Internet.

S'identifiquen de la mateixa manera que les altres, mitjançant els bits de més pes. En aquest cas, els cinc primers bits tenen un valor fix: 11110.

Figura 12

Adreces de propòsit específic

Apart de l'anterior classificació de les adreces, també s'han reservat tota una sèrie d'adreces per a propòsits específics:

a) Adreces d'amfitrió. Indiquen un equip concret de la xarxa en la que ens trobem. Així la part de l'adreça de xarxa serà tot 0 i es mantindrà la part de l'adreça d'equip que correspongui.

b) Adreces de xarxa. Fan referència a la xarxa però no als equips de dins d'aquesta xarxa. Al revés que l'anterior, la part de l'adreça de xarxa es manté i la part de l'adreça que correspon a l'equip serà tot 0.

L'adreça 0.0.0.0 és un cas especial, que sovint no s'implementa en els sistemes operatius actuals, correspondria a "aquest amfitrió" "d'aquesta xarxa".

c) Adreces de difusió (***broadcast***). Es tracta d'una adreça especial que serveix per comunicar-se alhora amb tots els equips d'una determina xarxa. Els primers octets de l'adreça es mantenen i identifiquen la xarxa (depenent del tipus que sigui serà de més o menys octets), i cadascun dels octets restants que corresponen als equips, prenen el valor 255 cadascun d'ells. És a dir, es manté la part de l'adreça de xarxa i la resta d'octets serà igual per a tots de 255.

Sempre que s'enviï un missatge a l'adreça de difusió, tots els equips han de respondre.

Fixem-nos que si s'enviés un datagrama a l'adreça 255.255.255.255, s'estaria enviant a tots els equips de la xarxa Internet. Per a evitar-ho, els routers només poden reenviar trànsit de difusió (o també anomenat "missatges de *broadcast*") dins la xarxa que l'ha emès.

Xarxa	Adreça IP	Classe	Adreça de xarxa	Número màxim d'ordinadors que pot tenir aquesta xarxa	Adreça del *host*	Adreça de broadcast
1	74.13.24.67	A	74.0.0.0	2^{24}	0.12.24.67	74.255.255.255
2	88.126.102.103	A	88.0.0.0	2^{24}	0.126.102.103	88.255.255.255
3	195.180.160.140	C	195.180.160.0	256	0.0.0.140	195.180.160.255

En aquesta taula observem algunes adreces IP, havent numerat les xarxes a les que pertanyen (de manera que si dues adreces IP són d'ordinadors de la mateixa xarxa, tenen el mateix número assignat), la classe de cadascuna d'aquestes xarxes (A, B, C...), la corresponent adreça de xarxa i el detall de quants ordinadors pot tenir com a màxim cada xarxa (dependrà del tipus de xarxa). I per a cada adreça IP de la taula, l'adreça del *host* i l'adreça de broadcast de la xarxa.

Xarxa	Adreça IP	Classe	Adreça de xarxa	Número màxim d'ordinadors que pot tenir aquesta xarxa	Adreça del *host*	Adreça de broadcast
3	195.180.160.142	C	195.180.160.0	256	0.0.0.142	195.180.160.255
4	222.125.222.21	C	222.125.222.0	256	0.0.0.21	222.125.222.255
5	156.11.75.15	B	156.11.0.0	2^{16}	0.0.75.15	156.11.255.255

En aquesta taula observem algunes adreces IP, havent numerat les xarxes a les que pertanyen (de manera que si dues adreces IP són d'ordinadors de la mateixa xarxa, tenen el mateix número assignat), la classe de cadascuna d'aquestes xarxes (A, B, C...), la corresponent adreça de xarxa i el detall de quants ordinadors pot tenir com a màxim cada xarxa (dependrà del tipus de xarxa). I per a cada adreça IP de la taula, l'adreça del *host* i l'adreça de broadcast de la xarxa.

d) Adreces de *loopback*. Són adreces utilitzades internament pels equips. Van des de la 127.0.0.0 fins a la 127.0.0.255. Sovint a l'arrencar l'equip, el sistema operatiu crea una interfície virtual, anomenada de *loopback*, amb l'adreça 127.0.0.1 que permet enviar datagrames des de l'equip en el que estem a ell mateix. Això serveix, per exemple, per si volem tenir un servidor instal·lat al nostre ordinador i ens volem connectar, des del mateix ordinador, al servidor. El servidor estarà a l'adreça 127.0.0.1, també coneguda com *localhost*.

e) Adreces privades. Són utilitzades per les xarxes locals internes que no surten a Internet. A cada estació de treball se li pot assignar una adreça dins del rang de les adreces privades. S'utilitzen habitualment en xarxes d'àrea local (LAN), on no hi ha la necessitat de disposar d'una adreça IP global per a cada estació de treball o altres dispositius com impressores connectades a la xarxa.

El seu ús generalitzat també va ser provocat per l'escassetat d'adreces IP en aquest protocol IPv4.

Els routers es configuren de manera que descarten qualsevol tipus de trànsit dirigit a adreces privades. Aquest aïllament facilita generalment que des de fora de la xarxa privada no sigui possible connectar amb una màquina mitjançant aquestes adreces. Per tant, com que no és possible realitzar connexions externes entre diferents xarxes privades a través d'Internet, dues xarxes privades de diferents entorns (p.ex. empreses) poden emprar els mateixos rangs d'adreces sense que hi hagi cap conflicte. Com que dues xarxes privades de diferents entorns no es poden comunicar entre sí utilitzant adreces privades, no hi haurà col·lisions entre les diferents xarxes privades.

En el cas de voler establir comunicacions amb l'exterior, fora de la xarxa privada, el router de la xarxa disposa del que s'anomena una porta d'enllaç amb una adreça IP pública. Des de fora de la xarxa es pot arribar també a aquesta adreça IP pública del router i serà aquest dispositiu el que s'encarregarà d'enviar els paquets rebuts a l'equip que correspongui de la xarxa privada.

Si volem utilitzar una adreça privada, caldrà fer servir un rang concret. En aquesta taula presentem els rangs que defineixen adreces privades:

Classe	Rang xarxa	Descripció	Definit a
A	10.0.0.0 – 10.255.255.255	1 xarxa simple de classe A	RFC 1918 RFC 1597 (aquesta és l'especificació original però actualment està obsoleta)
B	172.16.0.0 – 172.31.255.255	16 xarxes de classe B	
C	192.168.0.0 – 192.168.255.255	256 xarxes de classe C	
B	169.254.0.0 – 169.254.255.255	1 xarxa simple de classe B	RFC 3300 i RFC 3927

Tal com hem comentat, el problema de les adreces privades és que no poden accedir directament a Internet. Els router mai no enviarà a Internet el trànsit originat en equips amb adreces privades o amb destinació a aquestes, ja que no sabrien com encaminar-lo. Per evitar aquesta limitació, els routers inclouen una tècnica anomenada **NAT**, *Network Address Translation*.

1.1.2. NAT (*Network Adress Translation*)

Tinguem en compte que cada equip d'una xarxa IPv4 ha de disposar d'una adreça pública per a poder accedir a la xarxa Internet. Però sovint les xarxes tenen més equips que IP assignades per les operadores. Per exemple, un usuari que té contractada una connexió ADSL amb una operadora només rep una IP pública, mentre que aquest mateix usuari disposa de múltiples dispositius (ordinadors, *smartphones*, tauletes...) que s'han de poder connectar a Internet emprant la mateixa connexió. Per tant, aquest usuari només té dues opcions, demanar més adreces IP a la seva operadora o bé utilitzar adreces IP privades, de manera que sigui el router qui faci la conversió des de l'adreça IP privada a la IP pública. Aquest segona opció, és un procés que és coneix com a NAT. La majoria dels sistemes que utilitzen NAT ho fan per permetre que múltiples ordinadors d'una xarxa privada accedeixin a Internet amb una única adreça IP pública.

Des de mitjans dels anys 1990, el NAT ha estat una eina molt popular per alleujar els problemes provocats per l'esgotament de l'espai d'adreces IPv4. A més, s'ha convertit en una funció estàndard i indispensable en tots els routers per a connexions domèstiques i d'oficina petita.

NAT és el procés mitjançant el qual es modifica la informació sobre les adreces a la capçalera del paquet IPv4, mentre aquest paquet està en trànsit per un router.

NAT està definit amb detall en els documents anomenats RFC-2663 i RFC-3022.

Depenent del tractament que es fa de les adreces, hi ha diferents formes de NAT: **1)** NAT estàtica, **2)** NAT dinàmica, **3)** NAT amb sobrecàrrega del TCP (també coneguda com a PAT, *Port Adress Translation*) i **4)** LSNAT (*Load Sharing NAT*, o NAT amb balanceig de càrrega). Tot seguit expliquem breument cadascuna d'elles:

1) NAT estàtica. És el cas més senzill i també es coneix amb el nom de NAT bàsic o NAT d'un a un. En aquest cas, cada adreça privada té la seva adreça pública equivalent. Serà l'administrador de la xarxa qui haurà de construir aquesta taula d'equivalències dins el router (en la part de configuració de NAT), amb les dificultats de gestió que pot comportar si hi ha un nombre elevat de traduccions a realitzar. Fixem-nos, també, que aquest tipus de NAT tampoc comporta cap estalvi d'adreces públiques, però si que pot interessar assignar una adreça pública concreta a alguns servidors que contínuament puguin estar publicant a Internet.

2) NAT dinàmica. Amb aquest mode, el router assigna, de forma dinàmica, cada adreça privada amb una adreça púbica. Al contrari que la NAT estàtica, l'objectiu de la NAT dinàmica és tenir menys adreces publiques que privades. Perquè això sigui viable, cal assumir que totes les màquines de la xarxa privada no estaran connectades al mateix temps a Internet. **En aquest cas, l'administrador de la xarxa haurà de fixar els rangs d'adreces privades i públiques utilitzades**.

3) PAT (***Port Adress Translation***). És un tipus de NAT dinàmica que permet reduir al màxim (fins a una) el nombre d'adreces IP públiques utilitzades dinàmicament. Ho porta a terme emprant el port TCP/UDP amb l'objectiu d'identificar l'equip origen de la comunicació dins la xarxa interna/privada. Per tant, és molt similar a la NAT dinàmica però afegint el rang dels ports que s'han d'emprar. Aquest rang estarà dins el rang de ports assignats per IANA per les aplicacions clients (del 1024 al 5000).

Exemple

Tipus de NAT	Adreça privada	Adreça pública
Estàtica	172.26.0.35	201.5.4.3
Estàtica	172.26.0.43	201.5.4.15
Dinàmica	Rang: 172.26.0.50 a 172.26.0.80	Rang: 201.5.4.100 a 201.5.4.110
PAT	Rangs 172.26.1.101 a 172.26.1.254 172.26.2.101 a 172.26.2.254	201.5.4.18 Ports del 1024 al 5000

En aquesta taula podem comprovar les equivalències entre adreces privades i publiques, apreciant-se les diferències esmentades entre els diferents tipus de NAT.

4) LSNAT (***Load Sharing NAT***). És un tipus de NAT concebut per a solucionar el problema de servidors d'aplicacions sobresaturats com portals o cercadors. Per exemple, és el que s'aplica en portals com el de la UOC.

Si hi ha més sol·licituds de les que el servidor pot atendre, podem o canviar el servidor per un de més potent (amb el risc associat que si falla, deixem de donar aquests serveis), o bé replicar el servidor existent amb altres màquines amb les mateixes prestacions que l'inicial. En aquest segon cas, que és el que fa referència a LSNAT, el que es fa és aplicar un sistema que publiqui tots els servidors a Internet, com si fos un únic servidor i el balanceja la càrrega repartint la càrrega entre tots, de manera que si un falla, es puguin redirigir les peticions cap a la resta de servidors, sense que l'usuari se n'assabenti. Serà un router o commutador d'altes prestacions qui s'encarregui del redireccionament, i per tant, de balancejar la càrrega de peticions dels servidors.

En aquest cas, tindrem *n* servidors amb diferents adreces privades, que estan identificats per una mateixa adreça pública (la que s'anomena *virtual IP address*). Sovint, el redireccionament cap a un dels servidors (i.e. passar de la *virtual IP address* a la IP privada d'un dels servidors), enlloc de portar-se a terme en el router, es fa en un commutador d'altes prestacions, ja que és necessària una gran capacitat de càrrega i processament.

Exemple

Un usuari que vulgui accedir a un servei web utilitzarà l'adreça virtual, però internament aquesta adreça pública estarà associada a un nombre determinat de servidors cadascun d'ells amb la corresponent adreça privada.

1.1.3. Subxarxes: CIDR (*Classless inter-domain routing*)

Una vegada definides totes les classes de xarxes, es va veure que el model tenia algunes mancances. Per exemple, en les xarxes de classe A i B, el nombre d'adreces és excessivament gran per a ser gestionades per un únic equip. Per a solventar-ho,es va proposar un mecanisme anomenat **CIDR**, ***Classless Inter-Domain Routing*** (encaminament entre dominis sense classe), que detallarem a continuació. EL CIDR és conegut normalment amb el sobrenom de "subxarxes".

CIDR permet dividir les adreces assignades a una xarxa en subxarxes més petites i manejables. Amb CIDR la separació entre l'equip i la xarxa es fa amb una màscara.

Per exemple, 147.44.2.11/24 ens indica que té 24 bits amb valor '1' que indiquen l'adreça de xarxa i 8 per a la dels equips. Per tant, ens diu que la màquina 147.44.2.11 pertany a la xarxa 147.44.2.0. La màscara que permet obtenir l'adreça de xarxa és 255.255.255.0 o, el que és el mateix, 24 bits amb valor '1'. També ens està dient que només hi haurà 255 màquines (des de 0 fins a 254, sent la 255 l'adreça de *broadcast*).

Un altre exemple podria ser l'adreça de classe B d'un equip: 172.24.100.45 i una màscara igual a 27, és a dir: 172.24.100.45/27. Atès que és una classe B i que la màscara té 27 bits a '1', això implica que tenim onze bits de subxarxa. Per tant, l'adreça de subxarxa a la qual pertany el dispositiu és 172.24.100.32/27. En aquest, hi hauria 32 adreces diferents, on l'adreça 31 seria la de *broadcast* (tot els bits d'adreça amb valor '1').

Detallem-ho gràficament amb aquesta taula en la que podem apreciar com a resultat final de l'operació binària AND realitzada la subxarxa a la que pertany el dispositiu:

	Adreça (en decimal)	**en binari**
Adreça del dispositiu	172.24.100.45	10101100. 00011000. 01100100. 00101101
Máscara (amb 27 bits a "1").	255.255.255.0	11111111. 11111111. 11111111. 11100000
Adreça de subxarxa resultant. Resulta de multiplicar (AND) l'adreça i la máscara bit a bit.	172.24.100.32	10101100. 00011000. 01100100. 00100000

Sovint, al treballar amb xarxes, aquesta divisió en subxarxes es fa atenent determinats criteris, per exemple, per separar una xarxa educativa d'una xarxa de gestió.

Amb la creació de subxarxes s'aconsegueix:

- Aïllar el trànsit de cada xarxa i, per tant, es millora la seguretat i el rendiment global de cadascuna d'elles.

- Es simplifica la resolució de problemes ja que al tenir-les segmentades és més senzill identificar l'origen dels mateixos.

Així, amb aquesta classificació en subxarxes es simplifica la feina dels routers, ja que per a decidir la ruta que ha de prendre el datagrama no han de comprovar tota l'adreça IP, sinó només la xarxa de destinació.

Creació de subxarxes

Cal dir que existeixen algunes aplicacions en línia que permeten automatitzar els càlculs per a la creació de subxarxes. Només cal fer una cerca a Internet amb els termes: ***network calculator*** o ***subnet calculator***. En concret trobarem:

http://www.subnet-calculator.com/

1.2. De l'adreçament IPv4 a IPv6

Quan es va dissenyar el protocol d'adreçament IPv4 es creia que hi hauria prou adreces per a donar resposta a un volum gran d'equips que es volguessin connectar a una xarxa com Internet. Però, amb el temps i l'increment exponencial de necessitat de connexió d'equips a la xarxa Internet (sobretot l'elevat increment d'assignacions a zones d'Àsia) propiciat també per l'increment de dispositius mòbils amb necessitats de connexió, ha fet que les adreces IPv4 es vagin quedant esgotades.

Per a minimitzar aquest problema es va dissenyar NAT, que tal i com hem comentat, permet utilitzar adreces privades per a accedir a la xarxa amb una sola IP pública. Però com que aquesta solució no és escalable, comportant moltes dificultats d'aplicació als proveïdors, es decideix incrementar els 32 bits de les adreces IPv4 a 128, donant pas a l'adreçament IPv6.

1.3. Adreçament IPv6

La mancança d'adreces IPv4 incentiva el disseny d'aquest nou protocol anomenat IPv6. Inicialment, es va plantejar de fer només una adaptació del protocol IPv4, però des d'un primer moment, ja es va veure que el volum de canvis aconsellaven la creació d'un nou protocol. A més, la solució NAT per si mateixa també podia arribar a representar un greu problema de rendiment en els routers, pel fet d'haver de mantenir taules de traducció d'adreces de milions de connexions a la vegada.

L'adreçament IPv6, pel fet que la longitud de l'adreça IP passa de 32 a 128 bits, fa que el rang d'adreces de la xarxa passi de 2^{32} a 2^{128} adreces possibles.

Nota

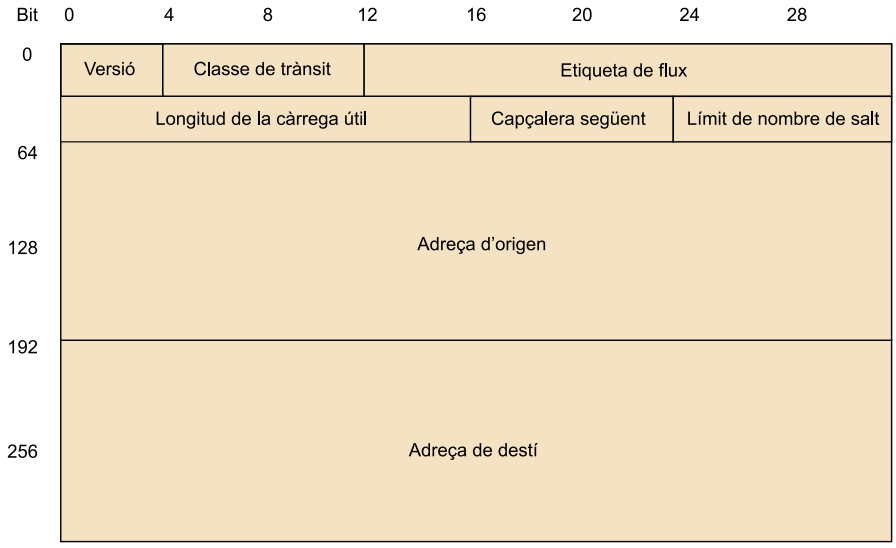
La diferència més rellevant entre **IPv4** i **IPv6** és la longitud de les adreces IP, passant de 32 bits a 128 bits.

1.3.1. Característiques d'IPv6

A continuació, passem a descriure les característiques del protocol IPv6.

Pel que fa a la capçalera de les adreces IPv6, aquesta té una longitud fixa de 40 bytes i consta dels camps que tot seguit descriurem.

Figura 13



Capçalera IPv6. En cada línia de l'esquema tenim 32 bits que per les 10 línies obtenim els 320 bits (40 bytes) que té la capçalera.

- **Versió** (*version*). De 4 bits. Conté la versió del protocol que conté el paquet. En el cas de IPv6 el valor és 0110 (6 en decimal).

- **Classe de trànsit** (*traffic class*). De 8 bits. És equivalent al camp tipus de servei d'IPv4. Classifica el paquet dins d'un trànsit determinat.

- **Etiqueta de flux** (*flow label*). De 20 bits. Per etiquetar un conjunt de paquets amb les mateixes característiques.

- **Longitud de la càrrega útil** (*payload length)*. De 16 bits. Longitud del paquet en bytes sense comptar la capçalera IP.

- **Capçalera següent** (*next header*). De 8 bits. Indica la posició en què es pot trobar la capçalera següent. És una novetat en IPv6 i facilita als routers el temps de procés, al no haver-hi opcions.

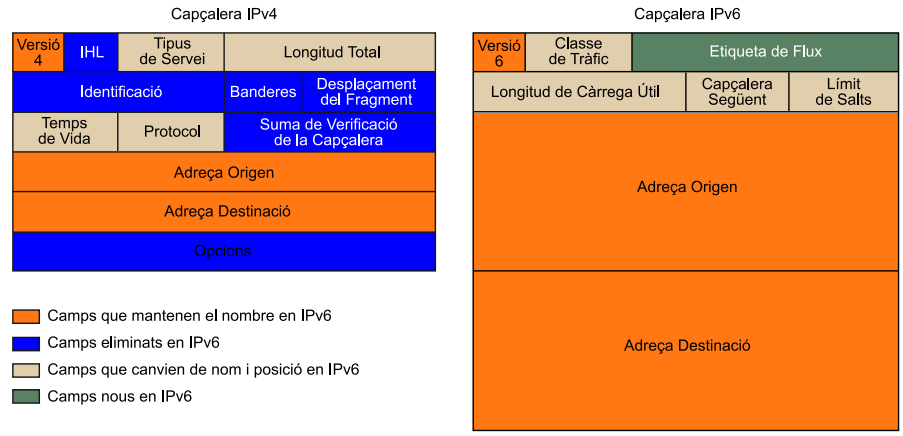
- **Nombre de salts** (*hop limit*). De 8 bits. Equivalent al camp TTL d'IPv4, però en aquest cas enlloc de comptar temps, compta nombre de salts.

- **Adreça d'origen** (*source address*). De 128 bits, especifica l'adreça IP de la màquina que ha generat el paquet.

- **Adreça de destinació** (*destination address*): De 128 bits, especifica l'adreça IP de la màquina on ha d'arribar el paquet.

En aquest esquema podem veure la comparativa entre les dues capçaleres, la de IPv4 i la de IPv6, amb el detall de les diferències:

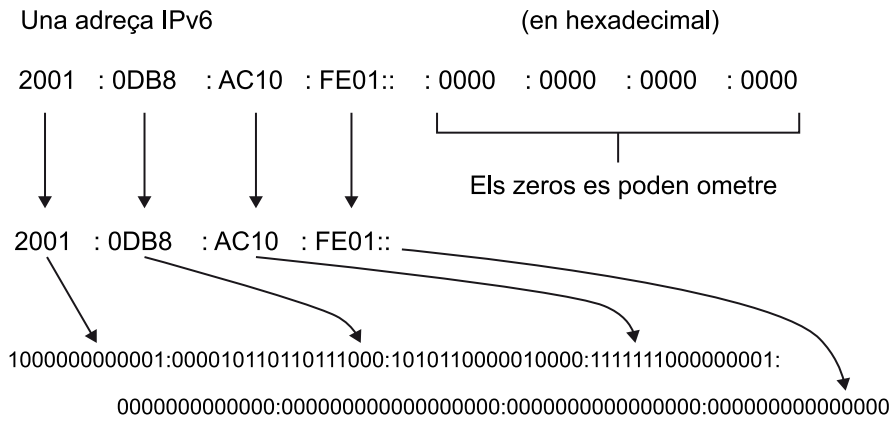
Figura 14



Comparativa capçalera IPv4 i IPv6.

Al tenir les adreces molts més bits, també canvia la forma d'especificar-les. En IPv6, les adreces s'indiquen en hexadecimal i s'utilitza com a notació els dos punts, en comptes del punt. Amb aquesta notació quan posem "::" estem indicant que en aquest punt de l'adreça s'ha de completar amb zeros.

Figura 15



Exemple d'adreça IPv6 en hexadecimal i en binari. Fixem-nos que en la part final de l'adreça s'està emprant la forma abreujada ("::") per indicar els zeros consecutius.

Conversió d'hexadecimal a binari i al revés

Com podem comprovar, en molts casos, les adreces en IPv6 s'expressen en notació hexadecimal.

El **sistema hexadecimal** (abreujat hex) és un sistema numèric amb base 16. Es representa normalment utilitzant els símbols 0–9 i A–F o a–f. Aquest sistema numèric va ser introduït per primera vegada en informàtica el 1963 per IBM.

Per a **convertir un nombre hexadecimal a binari**, cadascun dels dígits hexadecimals han de convertir-se per separat a binari como si es tractés d'un nombre decimal (veure la conversió decimal a binari). Cada xifra sempre haurà de tenir 4 dígits binaris, per tant, si el resultat té menys de 4 dígits, es completarà amb zeros a l'esquerra fins arribar a 4.

Observem que cada xifra hexadecimal representada per una lletra (A, B, C, D, E o F) en els càlculs, es substituirà pel seu valor decimal (10, 11, 12, 13, 14 o 15 respectivament).

Així, per exemple, B en hexadecimal correspon a 11 en decimal, que convertit a binari amb el procediment indicat és 1011.

Per a **convertir de binari a hexadecimal**, es divideix el nombre binari en grups de 4 xifres començant per la dreta. Si el darrer bloc de 4 no és complert es completa amb zeros a l'esquerra. Cada bloc es passa a decimal (veure procés de conversió de binari a decimal), obtenint nombres entre 0 i 15. Els valors que es trobin entre 10 i 15 són substituïts per les lletres corresponents, la resta es prenen directament. La seqüència obtinguda correspon al nombre hexadecimal corresponent.

Per a fer la **conversió d'un nombre decimal a hexadecimal**, de forma manual, s'opera igual que en la conversió decimal a binari amb la diferència que ara es divideix entre 16 enlloc d'entre 2. Es van fent divisions successives amb els quocients obtinguts fins a que el quocient sigui inferior a 16. Els residus de les diferents divisions estaran entre 0 i 15, enlloc d'entre 0 i 1. El nombre hexadecimal s'obtindrà prenent el darrer quocient i tots els residus en ordre invers a com s'han obtingut (primer el darrer residu, després el penúltim, fins a prendre el residu de la primera divisió. Per a cadascun d'ells, si el valor està entre 0 i 9 es pren aquest valor directament, i si està entre 10 i 15 es posa el nombre en l'hexadecimal corresponent seguint la següent correspondència: 10=A; 11=B; 12=C; 13=D; 14=E; 15=F.

Adreces d'aplicacions en línia

Existeixen aplicacions en línia que permeten fer ràpidament aquestes conversions, com les que podem trobar a:

http://www.mathsisfun.com/binary-decimal-hexadecimal-converter.html

http://calc.50x.eu/

http://es.ncalculators.com/digital-computation/binary-hex-converter.htm

Exemple 1

En aquest exemple es converteix el nombre hexadecimal 61B9430E a binari, emprant el procediment indicat, fent les conversions dígit a dígit.

65B9432E = 0110 0101 1011 1001 0100 0011 0010 1110.

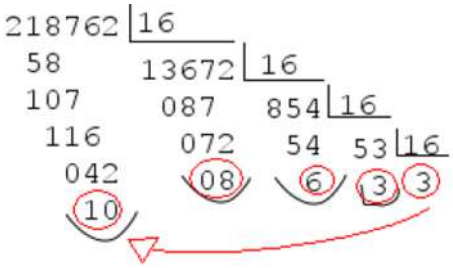
Exemple 2

Donat el nombre binari 101 1010 0100 1101 1011 0101 1110 1010, amb el procediment indicat obtindrem el nombre hexadecimal 5A4DB5EA.

Exemple 3

Donat el nombre decimal 218762, trobem el corresponent valor hexadecimal:

Figura 16



Aplicant el procediment indicat, trobem que serà 3368A.

En el cas de voler fer la **conversió d'hexadecimal a decimal**, només caldrà anar multiplicant cada dígit de dreta a esquerra per una potència de 16, començant per 160 i seguint per 161, 162, ... Recordem que les lletres es prenen com a valors numèrics seguint la correspondència indicada (A=10, B=11,...).

Exemple 4

Convertim el nombre 4A89D1 a nombre decimal:

4A89D1 = 1 · 160 + 13 · 161 + 9 · 162 + 8 · 163 + 10 · 164 + 4 · 165 = 4884945

Exemple 5

El nombre decimal 93, la representació del qual en sistema binari és 01011101, es pot escriure com 5D en hexadecimal (5 = 0101, D = 1101).

IPv6 representa, tal i com hem comentat, una gran evolució d'IPv4. Tot i que manté les principals funcions, les noves característiques més rellevants són:

- L'augment ja assenyalat de la mida de l'adreça IP que passa de 32 a 128 bits.
- Format de capçalera més simplificat, per a millorar el seu tractament en els routers.
- Possibilitat d'extensió de les capçaleres i de les opcions. Aquestes opcions es posen en capçaleres suplementàries IPv6 contingudes entre la capçalera IPv6 i la capçalera del paquet de transport. Així les opcions d'aquestes capçaleres IPv6, que aquí poden ser de longitud variable, no són tractades pels routers intermedis.
- Defineix extensions que permeten l'autenticació d'usuaris i la integritat de les dades mitjançant eines criptogràfiques.

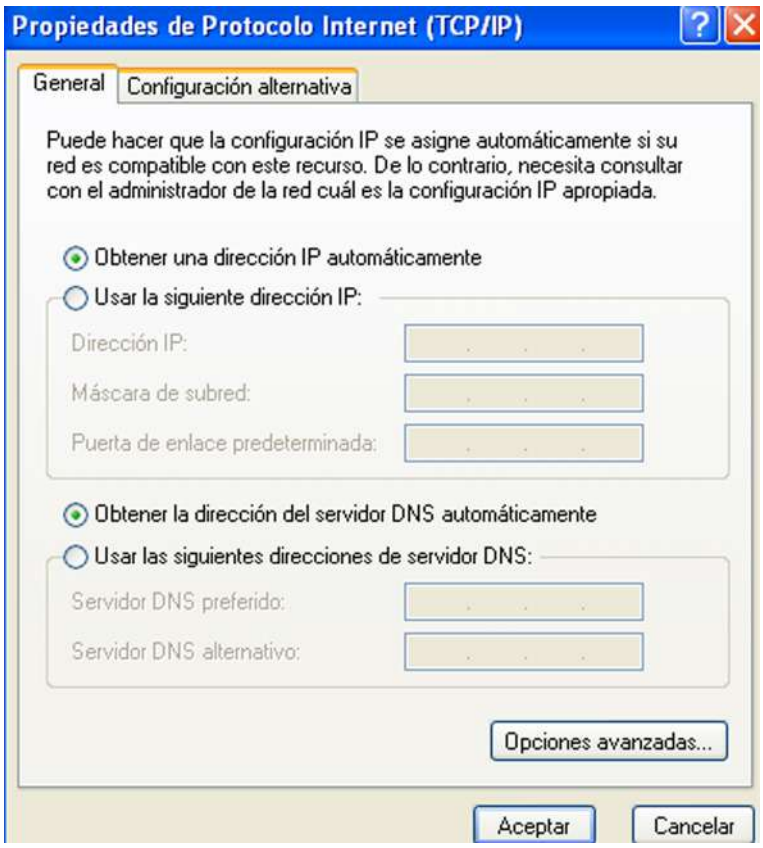
- Conté formes d'autoconfiguració com la configuració *Plug and Play* d'adreces de nodes sobre una xarxa aïllada, emprant DHCP.

- Permet un transició senzilla d'IPv4 a IPv6.

1.4. Configuració TCP/IP estàtica per un equip

En el cas de que s'hagi d'assignar una adreça IP fixa en un ordinador o qualsevol altre dispositiu, cal anar a les opcions de **connexions de xarxa** del sistema operatiu corresponent. Anant a les seves propietats, trobarem ***Protocol Internet*** **(TCP/IP)** o ***Protocol Internet versió 4*** **(TCP/IPv4)**, de manera que accedint a les seves propietats, arribarem a una pantalla com la que mostrem:

Figura 17

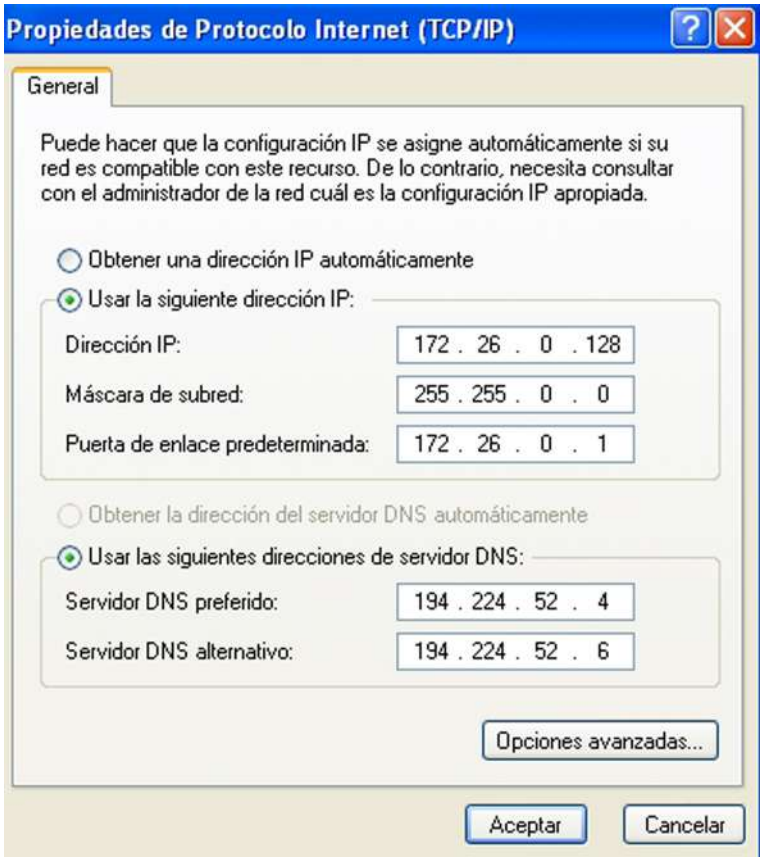


Pantalla de configuració del protocol TCP/IP configurat amb les opcions d'assignació automàtica d'IP i DNS (**adreçament dinàmic**).

En la imatge anterior, apareix el concepte de **DNS**. Tot i que hi aprofundirem quan tractem el nivell d'aplicació, ara fem una breu descripció d'aquest concepte. Un **sistema de noms de domini**, en anglès *Domain Name System* (DNS), 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 servidor DNS per a conèixer l'adreça IP que li correspon.

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***) o, en altres casos, els administradors de xarxa poden tenir configurats els seus propis servidors DNS.

Figura 18



Pantalla de configuració del protocol TCP/IP amb IP i DNS fixes (**adreçament estàtic**).

Les opcions són les que apareixen: opció que l'adreça IP s'assigni automàticament o bé que quedi determinada de forma fixa (en aquest cas, l'haurem d'introduir amb la corresponent màscara i adreça del router o porta d'enllaç predeterminada). El mateixa passa amb els anomenats camps DNS, depenent de si el servidor DHCP li indicarà aquests valors o s'utilitzaran una o dues adreces IP fixes de servidors DNS. Acceptant aquestes opcions ja es tindrà configurat el protocol.

Cal destacar que la IP assignada ha d'estar dins el rang de les adreces de la xarxa en la que es troba el router. Així si el router té una IP **192.168.0.1** un dels equips podria tenir, per exemple, una IP fixa **192.168.0.45**.

El fet que la IP es pugui assignar directament o bé l'haguem de fixar, dependrà de com tinguem configurat el router (amb DHCP activat o no).

En el cas de voler configurar TCP/IPv6, el procés serà semblant.

2. ICMP (*Internet control message protocol*)

L'ICMP correspon a un mecanisme bàsic que s'utilitza per a gestionar les incidències que es poden arribar a produir en una xarxa IP, independentment de la tecnologia utilitzada en nivells inferiors. Per tant, complementa el protocol IP per a tasques de control i notificació d'errors.

Els missatges ICMP són els que s'incorporen dins els paquets IP posant el valor del camp protocol de la capçalera IP a 1. Aquest valor 1 en aquest camp ens indica que el camp de dades conté el missatge ICMP.

Existeixen tretze tipus de missatges ICMP i una trentena de subtipus. Podem trobar la descripció detallada d'aquest protocol amb **tots els tipus de missatge ICMP** en el document **RFC-792**: http://www.rfc-es.org/rfc/rfc0792-es.txt.

Tot i que aquest protocol està concebut per aquesta capa de xarxa, hi ha algunes aplicacions que el fan servir directament com a eines de diagnòstic de xarxa. Entre elles tenim **ping** i **traceroute**.

2.1. Ping

Permet veure si un equip es troba connectat a la xarxa, utilitzant el protocol ICMP. Amb l'ordre *ping* es comprova la connectivitat entre un *host* i un *host* remot.

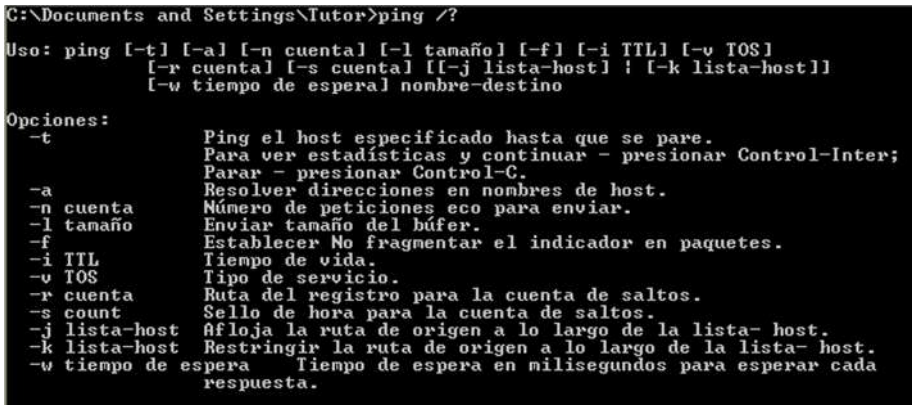
La majoria de sistemes operatius incorporen aquesta ordre ***ping***. Quan s'executa la comanda ***ping [adreça IP o nom d'un host remot]***, s'envien missatges ICMP de tipus 8. Si el missatge arriba al destí, el *host* remot respon amb un missatge ICMP de tipus 0, informant que està actiu i el temps que s'ha trigat en rebre la resposta. Si el *host* remot no està actiu o no existeix, transcorregut un temps sense rebre res, es rep per pantalla un missatge d'error, indicant que no s'ha trobat.

Aquesta comanda també permet comprovar si la targeta de xarxa del nostre propi ordinador està operativa i té configurat una adreça TCP/IP. Només cal fer ***ping 127.0.0.1*** o, equivalentment, ***ping localhost***.

Figura 19

S'ha executat l'ordre **ping 192.168.0.1**, que correspon a l'adreça del router de la xarxa. Aquest ha respost amb els paràmetres que es presenten a la captura de pantalla.

Figura 20



S'ha executat **ping /?** i se'ns mostren les diferents opcions amb les que es pot executar aquesta comanda.

2.2. Traceroute (tracert)

Permet descobrir els encaminadors intermedis entre l'origen i la destinació dels datagrames. Per tant, permet esbrinar quines rutes segueixen els paquets entre dos *hosts* és a dir, tot els encaminadors pels que han passat.

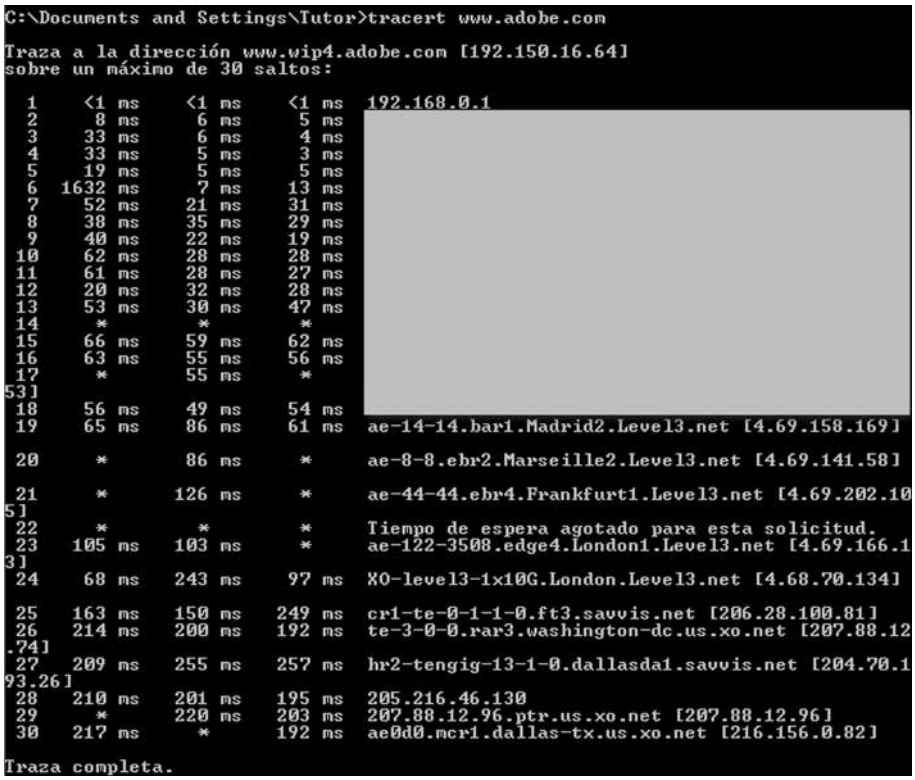
Mostra l'adreça de cadascuna de les interfícies dels encaminadors per les quals passa el paquet.

L'ordre és: ***traceroute [adreça IP o nom DNS del host destinació]*** (o **tracert** en el sistema operatiu Windows).

Amb traceroute (tracert) es pot detectar l'existència de colls d'ampolla en una xarxa, identificant l'origen del problema.

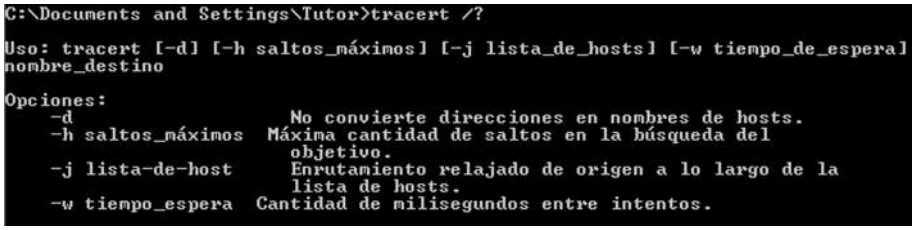
A l'executar per pantalla la comanda, una de les columnes indica el nombre de salts, el nom o l'adreça IP de l'encaminador corresponent i en les altres tres columnes els temps associats a tres intents d'arribar fins al proper encaminador.

Figura 21



S'ha executat en Windows **tracert** (www.adobe.com) i se'ns mostra, bona part de les dades de la ruta, amb el nombre de salt, els temps dels tres intents i les adreces dels routers intermedis pels quals han circulat els paquets.

Figura 22



S'ha executat en Windows **tracert /?** i se'ns mostren les diferents opcions amb les que es pot executar aquesta comanda.

El seu funcionament és el següent: s'envia un paquet al *host* destí amb el camp TTL=1. Així, el primer encaminador que el rep respon amb un missatge ICMP del tipus 11, el qual evidentment conté l'adreça origen d'aquest encaminador. Després es torna a enviar el mateix paquet però ara amb TTL=2. Així, el que el descartarà serà el segon encaminador pel que passi. I així anem enviant paquets incrementant el TTL i, per tant, rebent les respostes dels encaminadors. Quan el paquet arriba a la màquina destí, aquest paquet té un destinatari que és un servei d'aquella màquina que no espera cap petició. Per tant, respon amb un missatge ICMP del tipus 3 que vol dir "*host* inabastable". Així, ja sabem que s'ha arribat al destí i no cal seguir enviant paquets amb TTL més grans.

3. ARP (*Adress Resolution Protocol*)

El protocol ARP, *Adress Resolution Protocol*, s'encarrega de trobar l'adreça física d'un ordinador, emprada en les capes inferiors, a partir de la seva adreça de la capa de xarxa. Està definit en els RFC 826 fins el 1982.

Els routers (encaminadors) necessiten conèixer l'adreça física, l'adreça MAC d'una adreça IP. Qui s'encarrega d'aquest mapeig d'adreces és el protocol ARP.

Quan una estació ha d'enviar un paquet a una estació de la mateixa xarxa local, l'estació origen dedueix que l'estació destí està a la mateixa xarxa a partir de l'adreça IP de l'estació de destí. D'aquesta manera reconeix que no ha d'enviar el paquet a cap altre router.

Però per a poder enviar-li les trames Ethernet on aniran els paquets, cal que conegui l'adreça física, l'adreça MAC, del destinatari. Per a obtenir-la emet un paquet dins d'una trama Ethernet amb l'adreça de *broadcast* com a destí i amb l'adreça IP com a contingut.

Si el destí és de la mateixa subxarxa, llavors no passa pel router, sinó que és l'equip origen qui envia el datagrama a l'equip destí directament.

En canvi, si el destí pertany a una altra xarxa, llavors el router contesta amb l'adreça MAC del router i l'equip origen envia el datagrama al router, qui s'encarregarà de fer el procés cap a les altres xarxes a les que està connectat.

En definitiva, el funcionament és el següent: un *host* que vol conèixer l'adreça MAC que té una certa IP envia un paquet de tipus petició (ARP *request*) a l'adreça de *broadcast* de la capa d'enllaç i espera que la màquina que tingui aquella IP respongui (ARP *response*).

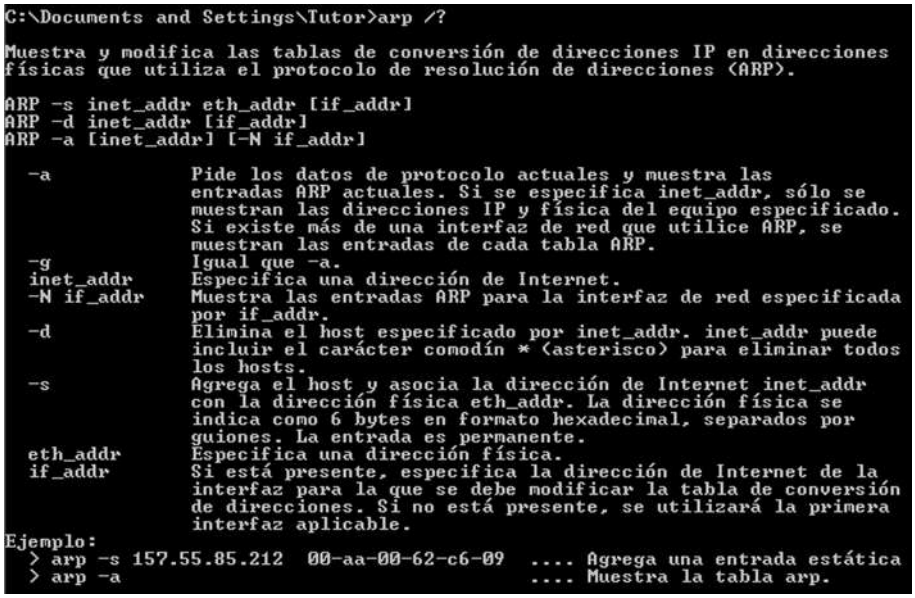
Quan s'obté la resposta, que conté l'adreça física, aquesta s'emmagatzema en local, en la que s'anomena **caché ARP** amb les **correspondències IP-MAC (adreça física- adreça IP)**. Per tant, abans de fer el procés anterior, es mira si ja té la resposta en la seva taula ARP. Aquesta taula s'esborra periòdicament per evitar que si una IP s'assigna a un altre equip, a l'equip antic li segueixin arribant paquets que ara ja no són seus.

Els sistemes operatius incorporen una ordre anomenada **arp** amb la que podem conèixer, entre d'altres opcions, el contingut d'aquesta taula. En concret, amb la comanda de sistema **arp –a** podem conèixer aquets continguts.

Figura 23

S'ha executat en Windows, **arp -a** i se'ns mostren els continguts d'aquesta taula.

Figura 24



S'ha executat en Windows **arp /?** i se'ns mostren les diferents opcions amb les que es pot executar aquesta comanda.

4. Router (o encaminador)

És un dispositiu de xarxa que permet interconnectar xarxes (físiques i lògiques). La seva estructura interna és semblant a la d'un ordinador, ja que disposa de memòria, interfícies d'entrada i sortida, CPU (unitat central de processament) i un sistema operatiu.

Figura 25

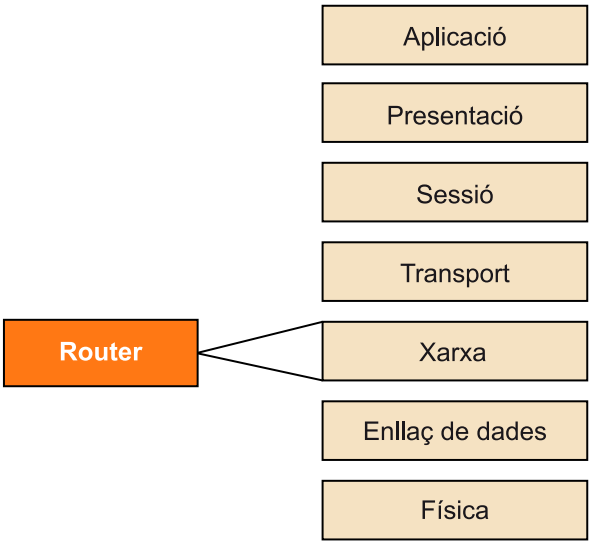
Dos models de routers, que també actuen com a punts d'accés Wi-Fi.

S'utilitza tant en xarxes locals com en xarxes de gran abast. Pren la informació en el **nivell de xarxa** per a prendre les decisions d'encaminament o ruta més adequada per a enviar les dades rebudes, de manera que aquestes puguin arribar al seu destí.

Permet la comunicació entre un únic ordinador o dispositiu i Internet, entre una xarxa e Internet, o entre dues o més xarxes.

La seva funcionalitat és la de proporcionar als paquets de dades (datagrames) que es transmeten una ruta segura i fiable des de l'origen fins a la destinació. Els routers treballen en la capa 3 del model OSI, és a dir, en la capa de xarxa i utilitzen adreces IP (*Internet Protocol*, protocol d'Internet) per encaminar i commutar els paquets de dades en les diferents interfícies.

Figura 26



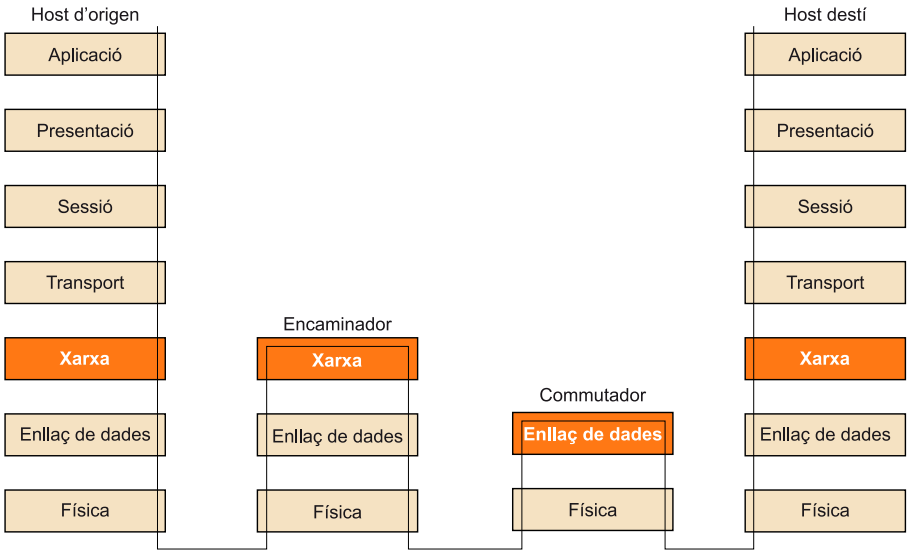
El router intervé a nivell de la capa de xarxa.

Per tant, són dispositius que tenen unes funcions claus per al bon funcionament de les xarxes. Per a dur-les a terme, s'han de configurar diferents paràmetres d'aquests dispositius.

Per a portar a terme aquestes funcionalitats incorpora alguns algoritmes com **RIP** (protocol d'informació de l'encaminament), que calcula la distància entre l'encaminador i l'estació receptora del paquet, tenint en compte paràmetres com el nombre de salts necessaris.

La diferència fonamental entre un ***switch*** (o commutador) i un ***router*** (o encaminador) és que el primer opera en la capa d'enllaç, enviant paquets emprant les adreces MAC, comentades en el mòdul anterior, i el router opera en la capa de xarxa, emprant adreces IP.

Figura 27



En aquest esquema podem veure el nivell en el que actuen un *switch* (commutador) i un router (encaminador). Per tant, queda justificat que els routers els presentem en aquest mòdul en el que estem aprofundint en la capa de xarxa.

Pel que fa a les funcions principals dels **routers**, aquestes estan directament associades amb funcionalitats pròpies de la capa de xarxa:

- **Segmentació**. Poden segmentar el trànsit d'una xarxa gran en diverses xarxes més petites. D'aquesta forma, els paquets de difusió o *broadcast* es poden canalitzar directament cap a la part de la xarxa que els pertoca.

- **Commutació**. Amb aquesta funcionalitat, els paquets de dades es van enviant per la interfície correcta. La decisió es pren en base a les taules d'encaminament.

- **Determinació de la ruta**. Els routers determinen la ruta en base a diferents paràmetres com l'amplada de banda de la línia, el nombre de salts que ha de fer un paquet de dades i els paràmetres de rendiment. Tinguem ben en compte, per tant, que dos paquets de dades amb un mateix origen i destí poden seguir rutes diferents.

Existeixen dues categories de routers: **1)** els més professionals i **2)** els d'un àmbit domèstic o de petites oficines. Els primers estan dissenyats per a crear xarxes corporatives de mida mitjana o gran, amb àmplies possibilitats de configuració i gestió. Els líders en aquests tipus d'equipaments són: Cisco, 3Com, Nokia… Pel que fa als segons, tenim fabricants com: Intel, 3Com, D-Link, NetGear, Linksys…

Cada router té les seves pròpies característiques externes, per exemple pel que fa a nombre i tipus de ports exteriors que ofereix.

4.1. Les taules d'encaminament

L'encaminament en el router es porta a terme mitjançant unes taules, anomenades taules d'encaminament que disposen de la informació necessària per a interconnectar totes les subxarxes que formen Internet.

El router és el que decideix la ruta que han de seguir els paquets consultant la seva taula d'encaminament. Tot dispositiu que tingui una adreça IP assignada haurà de disposar d'una taula d'encaminament, sigui una estació, router o qualsevol altre dispositiu.

Presentem una taula d'encaminament d'una estació, amb IP 172.26.0.27, amb un adaptador Wi-Fi instal·lat. Aquesta taula s'ha obtingut mitjançat la comanda de Windows: ***route print***.

Figura 28

```
C:\Documents and Settings\Tutor>route print
===========================================================================
ILista de interfaces
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 0c 43 ae f8 f2 ...... 802.11n USB Wireless LAN Card - Minipuerto
el administrador de paquetes
===========================================================================
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de acceso   Interfaz  Métrica
          0.0.0.0          0.0.0.0       172.26.0.1     172.26.0.27       25
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      169.254.0.0      255.255.0.0      172.26.0.27     172.26.0.27       20
       172.26.0.0    255.255.255.0      172.26.0.27     172.26.0.27       25
      172.26.0.27  255.255.255.255        127.0.0.1       127.0.0.1       25
   172.26.255.255  255.255.255.255      172.26.0.27     172.26.0.27       25
        224.0.0.0        240.0.0.0      172.26.0.27     172.26.0.27       25
  255.255.255.255  255.255.255.255      172.26.0.27     172.26.0.27       1
Puerta de enlace predeterminada:       172.26.0.1
===========================================================================
Rutas persistentes:
  ninguno
```

Taula d'encaminament obtinguda amb la comanda ***route print*** del sistema operatiu Windows.

Les files de la taula es consulten no en l'ordre en què apareixen sinó en l'ordre de màscara decreixent (en primer lloc les de 32 bits, etc).

Detallem alguns dels elements de la taula:

- La primera entrada (0.0.0.0) permet a l'estació comunicar-se amb estacions remotes. Notem que la màscara no té cap bit a 1. Aquesta és la ruta per defecte. L'encaminador establert per a accedir a estacions remotes queda identificat a la taula amb la IP: 172.26.0.1. Correspon a la porta d'enllaç.

- La tercera entrada: 169.254.0.0 correspon al que s'anomena *zeroconf route*, una adreça privada que s'activa per autoconfigurar-se la xarxa, abans d'activar-se el DHCP.

- L'adreça 172.26.0.27 correspon a l'adreça IP de l'estació, anomenant-se interfície de ***Loopback*** (adreça amb la que es coneix l'ordinador local des del mateix ordinador local).

- La vuitena entrada (255.255.255.255), només ens indica que els *broadcasts* IP es restringiran a la xarxa local.

4.2. Routers Wi-Fi

Actualment la majoria de routers incorporen la possibilitat addicional de connexió sense fils. Atenent que són dispositius fonamentals a l'hora de configurar una xarxa sense fils, en el següent apartat d'aquest tema tractarem el tema de la instal·lació d'una xarxa Wi-Fi, detallant l'equipament Wi-Fi necessari, el procés i els elements que ens poden portar a configurar-la i alguns programes que ens poden ser útils per a treballar amb xarxes sense fils.

Figura 29

5. Configuració d'un router

Abans d'endinsar-nos en el procés de configuració d'un router, detallarem els elements que el composen:

- Un programari intern per a gestió de les comunicacions.

- Ports per a connectar el punt d'accés a Internet o a la xarxa cablejada. Els punts d'accés poden disposar d'un o més ports 10/100Base-T (RJ-45). Per tant, porten integrat un hub o switch; i, en el cas de necessitar més ports, sempre es pot comprar un hub o switch independent i connectar-lo a un dels ports del router.

I en el cas que sigui un router Wi-Fi:

- Un equip de ràdio (de 2,4 Ghz en el cas de 802.11b i 802.11g, o de 5 Ghz en el cas de 802.11a).

- Una o dues antenes, que poden o no apreciar-se exteriorment.

Figura 30

Router ADSL de Movistar, Home Station ADB P.DG A4001N1, dissenyat per Telefónica I+D. Podem observar les antenes, enllaç a la línia ADSL, 4 ports d'enllaç Ethernet per a connectar-los a un ordinador, a un switch, a un hub..., botó de reset (per a restablir-lo a la configuració de fàbrica), botó per a connectar/desconnectar el Wi-Fi del router i el connector al corrent elèctric.

Pel que fa al tema dels ports, també podem trobar routers que en disposen d'altres com:

- ***Uplink port***, uns ports especials per a connectar un hub o switch d'una xarxa local Ethernet;
- Ports paral·lels o USB per a connectar-hi, per exemple, una impressora;
- Ports per a connectar una antena externa per a millorar l'abast.

Pel que fa a la **configuració i gestió del router**, sovint només cal connectar-se amb un navegador a l'adreça IP del router. Així, entrarem en una interfície basada en pàgines web des de la que podrem configurar els seus paràmetres.

Figura 31

Grups de paràmetres del router TP-LINK Wireless N Router WR841N que són accessibles i, bona part d'ells, configurables des d'aquesta interfície.

Figura 32

Grups de paràmetres de configuració d'un router Zyxel.

Una vegada hem entrat a la part de **configuració del router**, procedirem a revisar i, si cal, a modificar la seva configuració.

Primer de tot, cal tenir que compte que cada router té una configuració pròpia i **sovint la configuració que ve predeterminada de fàbrica ja pot satisfer els nostres interessos**. Tot i així, es recomana variar els paràmetres de seguretat que venen per defecte, com per exemple claus WEP/WPA i nom d'usuari i clau d'accés (*password*) per accedir a la configuració, ja que aquests valors per defecte es poden obtenir fàcilment per Internet.

Nota

Tot i així, també hi ha alguns routers que no utilitzen una interfície web, sinó que requereixen la introducció directa d'una línia de comandes, el que es coneix amb el nom d'interfície de línia de comandes: **CLI**, *Command Life Interface*; o, fins i tot, que es requereixi un sistema operatiu particular com és el cas d'Airport Base Station d'Apple.

Destaquem que podem distingir dos conjunts de paràmetres en la configuració dels routers: **1)** els que permeten gestionar la connexió de la xarxa cablejada o Internet (***Internet setting, IP seting, network setting*** o similar) i **2)** els que gestionen la xarxa sense fils (***Wireless setting, AP setting*** o semblant).

En el cas de la **gestió de la xarxa cablejada**, els paràmetres que cal configurar en el router són els mateixos que els que es configuren en un ordinador o dispositiu més de la xarxa cablejada. Per tant, el router tindrà dues adreces IP (i màscares de subxarxa), una que l'identifica dins de la xarxa sense fils i l'altra per a identificar-lo dins la xarxa cablejada.

Abans de realitzar canvis en la configuració del router és recomanable disposar del manual d'usuari que posa a la nostra disposició el seu fabricant i, al realitzar qualsevol canvi, documentar-lo per a poder-lo revertir si és el cas. També hi ha la possibilitat de restablir els seus valors de configuració directament als valors de fàbrica. Els routers professionals disposen de més opcions que els domèstics.

Les opcions de configuració incideixen en aspectes de gestió de la xarxa com:

- **Habilitar** o **deshabilitar la xarxa sense fils (*Enable Wireless Networking*)**. Pot ser útil quan només volem el punt d'accés amb les funcions de router i per la xarxa cablejada.

- **Servidor DHCP**. Sovint els punts d'accés tenen habilitat el servidor DHCP per tal d'assignar de forma automàtica les adreces IP als equips que es connecten. Però amb aquesta opció el podem deshabilitar.

- **Potència de transmissió (*Transmit power*).** Aquesta opció està implementada en alguns punts d'accés i permet variar la potència de transmissió per a donar més cobertura.

- **Registre d'activitat (*Log File*).** Alguns punts d'accés ofereixen la possibilitat de desar un registre de l'activitat realitzada. Pot permetre comprovar l'activitat de la xarxa i detectar-ne possibles intrusions.

Pel que fa a **les xarxes sense fils**, el procés d'instal·lació és relativament senzill, considerant que els certificats Wi-Fi ens garanteixen la bona compatibilitat entre els diferents equips i dispositius.

Es poden establir dos tipus de xarxes sense fils: **modus ad hoc** o **modus infraestructura**.

Per a instal·lar una xarxa ad hoc, en primer lloc caldrà situar a poca distància els diferents equips que es vol interconnectar i en un dels equips es configurarà de forma manual els paràmetres Wi-Fi. Per a configurar-ho caldrà executar el programa d'utilitats Wi-Fi de la targeta Wi-Fi o emprar l'eina o aplicació Wi-Fi que incorpora el mateix sistema operatiu. En línies generals caldrà configurar:

- El tipus de xarxa, en modus ad hoc, BSS, equip a equip, o termes similars.

- Posar un nom a la xarxa, el que es coneix amb el nom de SSID (*Service Set Identifier*) o nom de xarxa (*Network Name*).

- Canal, escollint algun número concret de canal tipus de seguretat, pot ser WEP o WPA per exemple, amb una clau d'accés.

Així, qualsevol altre ordinador o dispositiu amb adaptador Wi-Fi que tingui configurats els mateixos paràmetres i dins el mateix radi de cobertura, podrà formar part de la xarxa i compartir recursos amb la resta d'ordinadors de la xarxa.

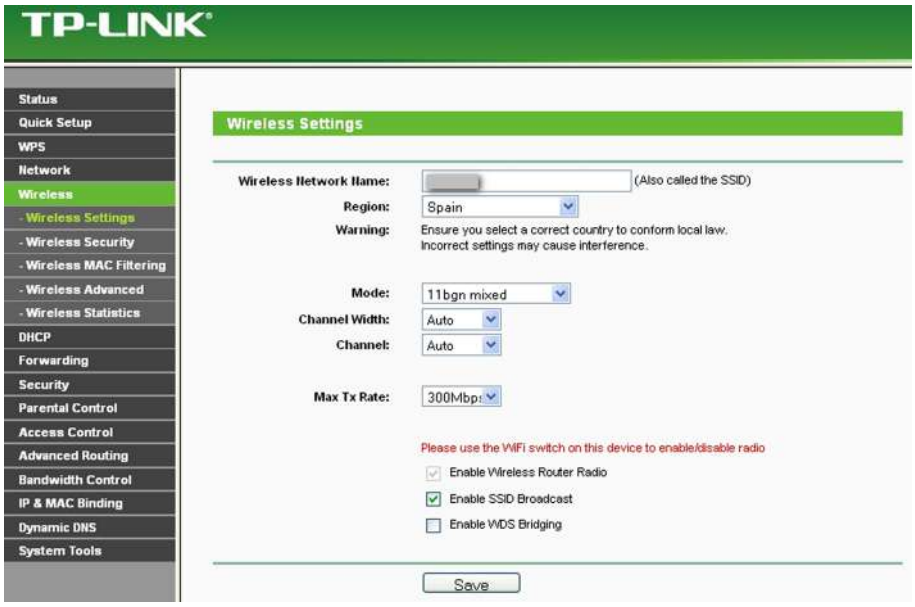
Per a configurar una xarxa Wi-Fi en **modus infraestructura**, caldrà configurar el router Wi-Fi. Pel que fa als **paràmetres dels routers Wi-Fi** que podem canviar destacarem:

- **SSID (*Service Set Identifier*)**, que és el nom de la xarxa (*Network name*), el que permet identificar el servei i és el que apareix quan fem una cerca de xarxes sense fils.

- **Canal (*Channel*)**, amb el qual s'emet el senyal d'ona portadora de ràdio. Sovint el sistema permet que l'assignació de canal sigui automàtica o manual. Abans d'escollir un nombre de canal, és convenient explorar les xarxes sense fils de la zona per a poder emprar un canal que no s'estigui utilitzant.

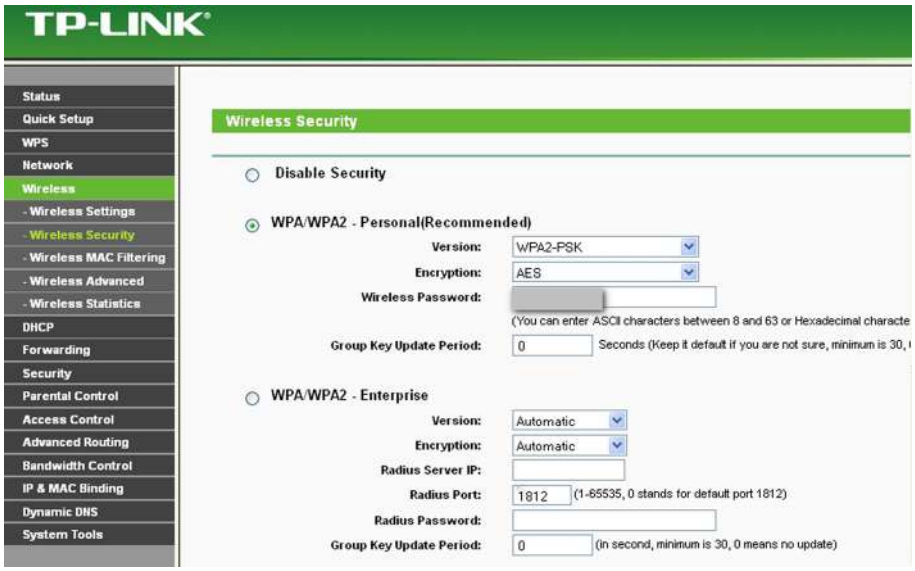
- **Seguretat (*security*)**, els paràmetres de configuració de seguretat en el router, permeten poder donar accés a la nostra xarxa sense fils als equips o usuaris que vulguem, i/o xifrar l'intercanvi d'informació que es produeixi. El tema de configuració de la seguretat, per la seva rellevància el tractarem en un proper apartat.

Figura 33



En aquesta captura de pantalla es presenten els **Wireless Settings** d'un router del fabricant **TP-LINK**. Es visualitzen, entre d'altres, els paràmetres: SSID i Channel.

Figura 34



En aquesta captura de pantalla es presenta ***Wireless Security*** d'un router del fabricant **TP-LINK**. Ens permet comprovar el protocol de seguretat emprat WPA2-PSK, amb xifrat AES, i el password configurat (en la figura està esborrat).

L'àrea de cobertura, o zona dins la qual un ordinador o dispositiu pot connectar-se amb el router, depèn de factors com la localització del router, les interferències radioelèctriques, els tipus d'antenes, els obstacles que puguin existir entre el punt d'accés i l'ordinador o dispositiu. En el cas de voler ampliar la zona de cobertura, hi ha la possibilitat d'anar situant diferents **punts d'accés** que complementin les cobertures del router.

Els punts d'accés es configuren de forma molt semblant als routers i permeten estendre el radi de cobertura de la xarxa sense fils.

Punts d'accés (AP, *acces point*)

Un **punt d'accés** és un dispositiu encarregat de connectar dispositius Wi-Fi, que tenen les seves corresponents targetes de xarxa, per a crear una xarxa sense fils. Els punts d'accés també són sovint el pont d'interconnexió entre la xarxa cablejada i Internet, per tant, molts d'ells també actuen com a routers.

Pel que fa a la configuració dels ordinadors o dispositius que vulguem connectar sense fils a una xarxa amb un router o un punt d'accés, cal que aquests disposin de l'adaptador o targeta de xarxa corresponent i que aquest quedi configurat per tal que pugui accedir al router o al punt d'accés de la xarxa desitjada. Sovint, només fent una exploració de les xarxes sense fils i acceptant l'opció de connectar, l'equip ja s'adaptarà automàticament a la configuració que li enviï el router. Només caldrà entrar la clau WEP/WPA per a establir-ne la connexió.

Si el router està configurat per a no admetre connexions automàtiques, caldrà configurar cada equip de forma manual amb els paràmetres de la xarxa com: tipus de xarxa, nom de la xarxa, canal i seguretat.

També en el cas que el router no tingui activada l'opció d'assignació automàtica de les adreces IP (DHCP activat), caldrà configurar l'ordinador de forma manual. Aquest procés dependrà del sistema operatiu que tinguem instal·lat, tot i que els paràmetres que haurem d'entrar seran:

- **Número IP de l'ordinador**. És important assenyalar que cal que estigui en el rang d'adreces acceptades pel router. Per exemple, si el router té l'adreça 172.26.0.1, aleshores als equips es podrien assignar als números 172.26.0.x on x tindrà valors entre 2 i 255.

- **Màscara de subxarxa**. Generalment serà el nombre 255.255.255.0, per a xarxes que disposin de menys de 255 terminals.

- **Porta d'enllaç**. Correspon l'adreça IP del router. En l'exemple anterior seria 172.26.0.1.

- **DNS**. En aquest cas, podem configurar-ho de manera que prengui de forma automàtica aquests valors del router o bé que l'usuari introdueixi manualment els DNS, amb els valors que li haurà facilitat el seu proveïdor de serveis.

Una vegada s'hagi instal·lat la xarxa, només caldrà comprovar que funciona correctament. En concret, es pot comprovar si hi ha connexió a Internet en els diferents equips, si es localitzen els recursos compartits amb altres equips...