

Interconnexió de la xarxa

Josep Ferrer Tura, Àngel Alejandro Juan Pérez, Immaculada Salas
Díaz i Oriol Torres Carrió

Xarxes d'àrea local

Índex

Introducció	5
Resultats d'aprenentatge	7
1 Adreçament físic i lògic de la xarxa	9
1.1 Adreçament físic	9
1.2 Adreçament lògic	12
1.2.1 De decimal a binari	13
1.2.2 De binari a decimal	16
2 Protocols de nivell d'enllaç	19
2.1 Serveis de la capa d'enllaç	19
2.1.1 Control d'enllaç lògic	19
2.1.2 Control d'accés al medi	20
2.2 IEEE 802	22
2.2.1 L'Ethernet 802.3	23
2.2.2 Anell de testimoni (l'IEEE 802.5)	24
2.2.3 El DQDB (l'IEEE 802.6)	25
2.2.4 Les col·lisions	25
3 Protocols de xarxa	29
3.1 Funcions dels protocols de xarxa	29
3.2 IP (Internet protocol)	30
3.3 L'ICMP	32
3.3.1 L'ordre ping	32
3.3.2 L'ordre traceroute	32
3.4 ARP	33
3.4.1 Assignació estàtica	34
3.4.2 Assignació dinàmica	34
3.4.3 Protocol de resolució d'adreces invers (RARP)	35
3.5 IPX	36
3.5.1 Adreçament IPX	36
4 Adreçament IP	39
4.1 Encapçalament IP	39
4.2 Classes d'adreça IPv4	42
4.2.1 Adreça de classe A	44
4.2.2 Adreça de classe B	45
4.2.3 Adreça de classe C	47
4.2.4 Adreça de classe D	49
4.2.5 Adreça de classe E	49
4.2.6 CIDR (encaminament sense classe)	50
4.2.7 Espai d'adreces reservades	51
4.2.8 Esgotament de les adreces IPv4	52

4.3	Creació de subxarxes o subneeting	53
4.3.1	Màscara de subxarxa: part de xarxa i part de host	54
4.3.2	Manipulació de la màscara de subxarxa	55
4.3.3	Exemple de creació de subxarxes	56
4.4	Adreçament públic i privat: NAT	58
4.5	El protocol IPv6	59
4.5.1	Adreces IPv6	59
4.5.2	Característiques de la nova versió	60
4.5.3	Estructura de la IPv6	61
5	Protocols de la capa de transport	65
5.1	Funcions de la capa de transport	65
5.1.1	Transmissió de missatges d'extrem a extrem (end-to-end delivery)	66
5.1.2	Punts d'accés al servei	66
5.1.3	Fiabilitat de les transmissions	67
5.1.4	Control del flux: finestres "lliscants"	68
5.1.5	Multiplexació a la capa de transport	70
5.2	Serveis orientats a connexió: intercanvi de senyals a tres passes	70
5.3	Protocols de capa de transport i ports	72
5.3.1	UDP (user datagrama protocol)	72
5.3.2	TCP (Transmission Control Protocol)	73
5.3.3	Sòcols i ports	75
6	Protocols de la capa d'aplicació	79
6.1	Model client-servidor	79
6.2	Assignació automàtica d'adreces IP: BOOTP i DHCP	80
6.2.1	BOOTP	80
6.2.2	DHCP	81
6.3	Noms de hosts i DNS	82
6.3.1	Noms de domini	82
6.3.2	Fitxers hosts	83
6.3.3	DNS (domain name system)	84
6.3.4	DDNS (dynamic DNS)	85
6.3.5	Servidors d'impressió i zeroconf	85
6.4	Altres protocols i serveis: SMTP, POP, Telnet, FTP, HTTP, NTP, etc	86
6.5	Servidors intermediaris	89
6.6	Utilitats TCP/IP	90

Introducció

Aquesta unitat ofereix una visió més profunda de la capa de xarxa i presenta els conceptes més importants associats a les capes superiors del model TCP/IP, la capa de transport i la capa d'aplicació. Aquests conceptes poden resultar una mica teòrics al principi, però són fonamentals per comprendre bé la comunicació entre els ordinadors. Es recomana reforçar la comprensió dels conceptes teòrics mitjançant les activitats pràctiques que els acompanyen.

Es revisen alguns conceptes bàsics de la capa de xarxa i es presenten conceptes avançats d'adreçament IP, creació de subxarxes i protocols TCP/IP encaminats i d'encaminament. Aquesta capa de xarxa és fonamental per a la comunicació entre ordinadors de xarxes diferents. En aquest sentit, tant els encaminadors com el protocol IP tenen un paper fonamental que cal comprendre bé. A més a més, la creació de subxarxes constitueix una peça bàsica per poder ampliar l'interval disponible d'adreces IP en qualsevol xarxa local, per la qual cosa és una pràctica molt habitual en un gran nombre d'empreses.

En l'apartat "Protocols de la capa de transport" es treballa la capa de transport, que és la responsable de segmentar les dades que envia l'ordinador emissor i de tornar-les a ordenar un cop han arribat a l'ordinador de destinació. A més, aquesta capa s'encarrega de donar fiabilitat a la transmissió de les dades, per la qual cosa fa ús de mecanismes de control i de recuperació d'errors de transmissió. A aquest efecte, es presenten conceptes com ara el control del flux mitjançant l'ús de finestres lliscants, l'intercanvi de senyals per tres passes i els protocols TCP i UDP.

En l'apartat "Protocols de la capa d'aplicació" s'introdueix la capa d'aplicació i conceptes fonamentals d'aquesta capa, com són els serveis DNS i DHCP, i es revisen els principals protocols i serveis d'aquesta capa. La capa d'aplicació és la més propera a l'usuari final i proporciona serveis de xarxa com ara la transferència d'arxius mitjançant el protocol FTP, l'accés a pàgines web mitjançant el protocol HTTP o l'enviament de correus electrònics mitjançant protocols com ara POP3, SMTP o IMAP.

Per treballar els continguts d'aquesta unitat, és convenient fer les activitats i els exercicis d'autoavaluació, i llegir els annexos del material web.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Enumera i explica les característiques dels protocols que es configuren en una xarxa local, tenint en compte la tecnologia i els estàndards utilitzats.
 - Explica el sistema d'adreçament dels nodes que es fa servir en la xarxa local considerant les tecnologies de xarxa emprades.
 - Enumera i explica les característiques dels protocols que es configuren en una xarxa local, tenint en compte la tecnologia i els estàndards usats.

1. Adreçament físic i lògic de la xarxa

Com ja sabeu, podeu utilitzar un ordinador per connectar-vos a Internet. Aquesta connexió és possible, entre moltes més raons, perquè l'ordinador disposa d'una adreça IP i una adreça MAC (adreça física) única per poder ser identificat a la xarxa; l'adreça IP fa que la vostra màquina sigui l'única que rebi la informació que heu demanat.

1.1 Adreçament físic

Per poder connectar un ordinador a una xarxa és necessari que aquest disposi d'una targeta de xarxa, la qual s'identifica amb l'adreça MAC, que és única per a cada targeta de xarxa existent al món.

Si coneixeu l'adreça MAC i la utilitzeu és possible transmetre dades. D'aquesta manera, la informació arribarà únicament a la màquina que voleu, ja que és l'única que té el mateix nombre que heu fet servir.

Per poder comprovar l'adreça MAC de la vostra targeta de xarxa el que heu de fer varia depenent del sistema operatiu que utilitzeu:

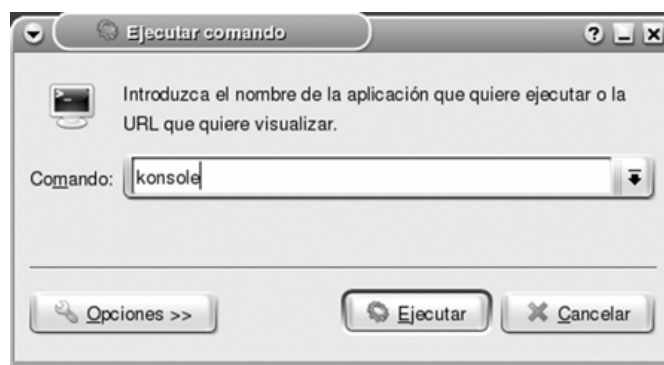
1. Sistema operatiu amb nucli Linux.

Si es tracta d'un **sistema operatiu amb nucli Linux**, heu d'obrir una consola de text i executar l'ordre *ifconfig*. Per canviar a una consola de text, el més comú és utilitzar la combinació de tecles de control, alternativa i funció 1 (Ctrl + Alt + F1). Per tornar a l'entorn gràfic habitualment cal prémer la combinació control, alternativa i funció 7 (Ctrl + Alt + F7). En algunes instal·lacions canvien els números de les tecles de funció.

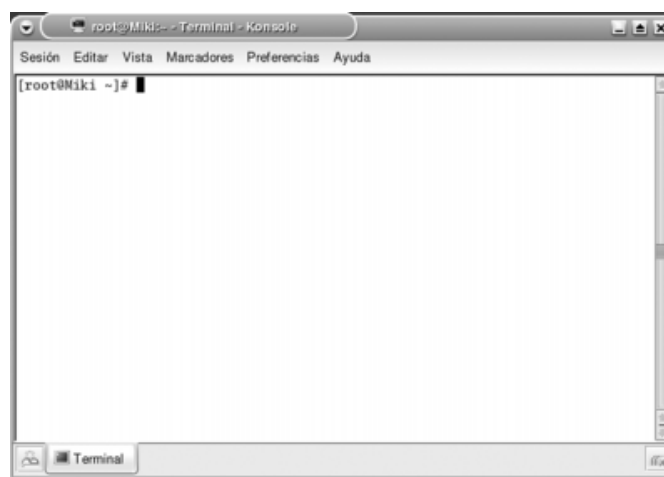
També es pot canviar a una consola de text utilitzant el terminal de text de l'entorn gràfic. Hi ha diferents maneres de fer-ho, en funció de la distribució que utilitzem:

- Fer clic a la icona opció de menú corresponent (pot anomenar-se *terminal* o *consola*).
- Per entorns d'escriptori de l'estil d'*Unity*: buscar la paraula terminal (és el nom de l'aplicació corresponent).
- Anar a *Executar ordre* i executar l'ordre *konsole* o la comanda corresponent de la vostra distribució (vegeu la figura 1.1).

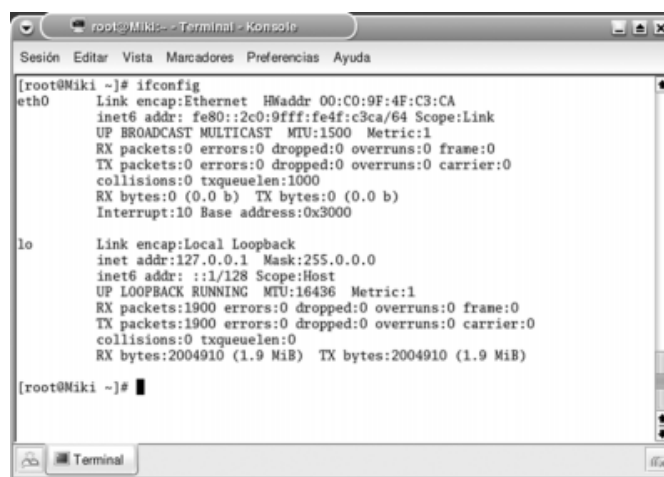


FIGURA 1.1. Pantalla d'execució en Linux

Una cop executada aquesta ordre, s'obrirà una finestra (vegeu la figura 1.2) de mode de text on podreu executar l'ordre *ifconfig*.

FIGURA 1.2. Consola en mode de text de Linux

Una vegada executada ja l'ordre *ifconfig*, veieu una finestra (figura 1.3) que mostra tota la informació sobre les connexions de xarxa. Com podeu comprovar, teniu molta informació i només cal que seleccioneu la que us interessa.

FIGURA 1.3. Informació proporcionada en executar *ifconfig*

En aquest cas, heu de buscar la informació sobre l'adreça MAC en l'entrada Hwaddr (adreça de maquinari o *hardware address*). Com s'ha comentat, el resultat ha de ser un nombre de 12 caràcters en format hexadecimal.

En aquest cas es tracta de la targeta de xarxa Ethernet, que en GNU/Linux és la interfície eth0; també es podria trobar un altra interfície Ethernet, que seria la eth1.

2. Sistema operatiu del tipus Windows XP o Windows 2000.

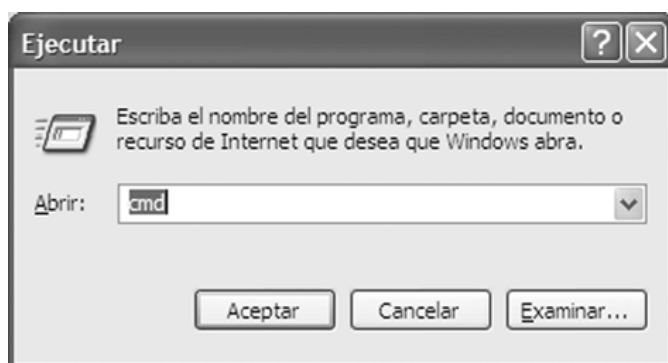
Si es tracta d'un **sistema operatiu del tipus Windows XP o Windows 2000**, heu d'obrir una consola de text i executar `ipconfig/all`. D'aquesta manera, hi trobareu tota la informació necessària.

Per iniciar una consola de text, heu d'anar a Inici/Executar i utilitzar l'ordre `cmd` (vegeu la figura 1.4).



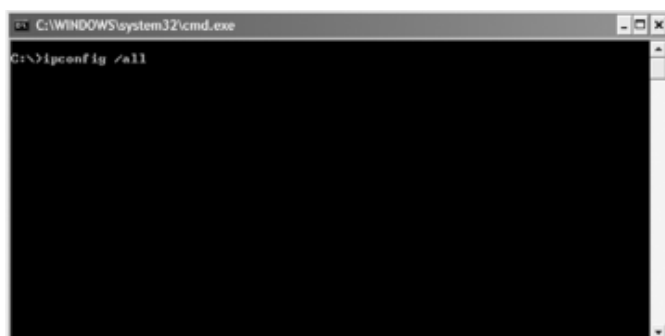
Logotip de Windows

FIGURA 1.4. Pantalla d'execució en Windows XP

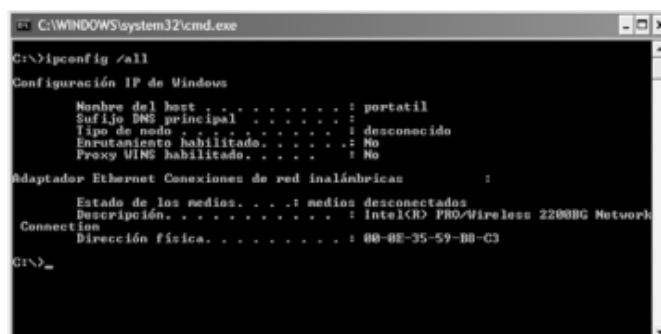


Un cop s'ha obert la finestra de text, si executeu l'ordre `ipconfig /all` us mostra tota la informació (vegeu la figura 1.5). Si executeu només `ipconfig`, veureu l'adreça IP de la vostra màquina i la màscara de subxarxa.

FIGURA 1.5. Pantalla de mode de text en Windows XP



Un cop executada aquesta ordre, podeu veure que apareix molta informació (vegeu la figura 1.6); només cal trobar la que us interessa en aquest moment.

FIGURA 1.6. Informació completa d'ipconfig

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : portatil
Sufijo DNS principal . . . . . : principal
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexiones de red inalámbricas :

Estado de los medios. . . . . : medios desconectados
Descripción. . . . . : Intel(R) PRO/Wireless 2200BG Network
Connection
Dirección física. . . . . : 00-0E-35-59-B0-C3

C:\>
```

Un cop heu aconseguit arribar a aquesta pantalla, n'heu d'analitzar el contingut: com podeu comprovar, hi apareix el nom de la màquina, el seu número, el DNS principal, el model de targeta instal·lat –que és a *Descripció*; en aquest cas, veieu que es tracta d'una targeta sense fils o *wireless* fabricada per Intel– i, finalment, l'adreça MAC, que és un nombre de 12 xifres en format hexadecimal.

És molt important que tingueu en compte el sistema operatiu amb el qual trebal·leu, ja que a cada sistema s'utilitzen ordres diferents per poder accedir a la informació que ens interessa, en aquest cas l'adreça MAC.

Com podeu comprovar, l'adreça MAC i l'adreça IP no són les úniques informacions que hi apareixen. En aquests moments veieu molta informació que no sabeu què significa ni per què serveix, però no us preocupeu, ja que us serà molt familiar en acabar aquest mòdul.

1.2 Adreçament lògic

L'adreça IP és la responsable que la vostra màquina sigui trobada a la xarxa. Aquesta adreça ha de ser única per a cada ordinador, ja que si n'hi hagués més d'una màquina amb la mateixa adreça, entrarien en conflicte i cap d'elles no podria rebre informació. Aquest fet podria provocar un malfuncionament de tota la xarxa i això cal evitar-ho.

Un octet està format per l'agrupació de vuit bits.

L'adreça IP està composta per un nombre prou alt de bits perquè l'IP no es repeteixi en dues màquines diferents. En realitat, l'adreça està composta per 32 bits agrupats en grups de 8 bits que formen 4 octets. Quan llegiu una adreça IP, trobareu quatre grups de vuit bits cadascun.

La notació decimal

La notació decimal és aquella amb què tots esteu acostumats a treballar des de petits. Cal tenir en compte que, al contrari del que sempre s'ha dit, no es comença a comptar per l'1 sinó pel 0. Si no ho feu així, durant tot aquest mòdul tindreu moltes dificultats.

Com heu vist, el fet que una adreça IP estigui formada per bits genera un problema en les persones que no estan acostumades a treballar en sistema binari és a dir, utilitzant bits. Per aquesta raó, les adreces IP també s'expressen en notació decimal, que és la que esteu acostumats a utilitzar i fàcil de comprendre. Quan utilitzeu aquesta notació, comprovareu que una adreça IP està formada per quatre grups de nombres separats per un punt, com podeu veure a la taula 1.1.

Màxim valor binari:
11111111. Màxim valor
decimal: 255

Canvi de sistema

Per fer el canvi d'un sistema de numeració a l'altre, agafareu un octet i el transformareu, a continuació agafareu un altre octet i també el transformareu, i ho fareu així fins a tenir els quatre octets transformats. Un cop hàgiu acabat aquesta tasca, agafareu els nombres que heu calculat i els escriureu separats per un punt.

TAULA 1.1. Adreça IP en notació decimal i binària

Adreça IP en notació decimal	Adreça IP en notació binària
192.168.34.6	11000000.10101000.00100010.00000110

La separació per punts facilita la lectura i la comprensió de l'adreça IP, i també la conversió de notació binària a notació decimal. A més, utilitzant aquest sistema el nombre més gran que hi pot haver en cada octet és quan els vuit bits tenen el valor d'1. Així doncs, fent la conversió comprovareu que el valor màxim en notació decimal seria de 255. Aquesta transformació de binari a decimal serà molt important durant tot el mòdul. Per tant, val la pena que domineu el canvi d'una notació a l'altra.

1.2.1 De decimal a binari

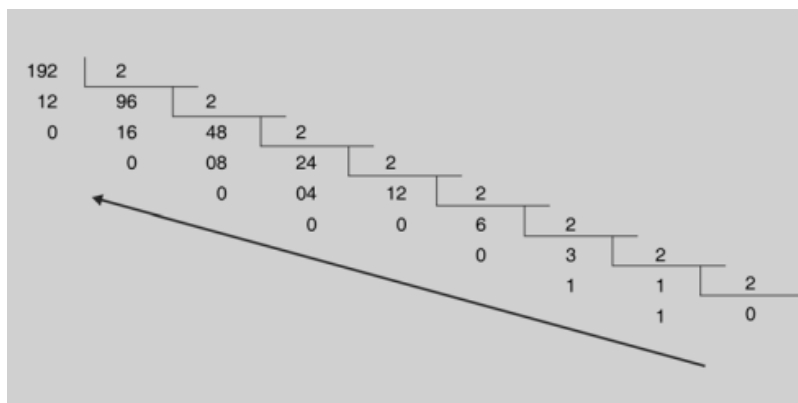
A continuació, veureu uns quants exemples de canvi de base perquè pugueu practicar la conversió de binari a decimal i de decimal a binari.

El primer exemple de transformació serà el corresponent a l'adreça IP 192.168.32.123.

Ús del sistema decimal

El canvi de base serà un dels més utilitzats a l'hora de crear xarxes, ja que les adreces IP es donen en notació decimal perquè les persones les comprenguin millor.

FIGURA 1.7. Transformació de decimal a binari del nombre 192



Prenem el 192 i, com que s'ha de passar a notació binària, comencem a dividir el nombre per la base a la qual volem arribar, és a dir, 2 (figura 1.7).

Un cop s'ha fet la divisió, agafarem les restes de cada divisió feta però en sentit contrari –tal com indica la fletxa–: si ho fem així, el nombre en notació binària que us queda és el següent: 11000000

Una adreça IP consta de quatre octets separats per punts. Com que s'ha pres un dels camps de l'adreça en notació decimal per transformar-la a notació binària, el resultat hauria de ser un octet –és a dir, 8 bits–, i com es pot comprovar el resultat ha estat un nombre de vuit bits.

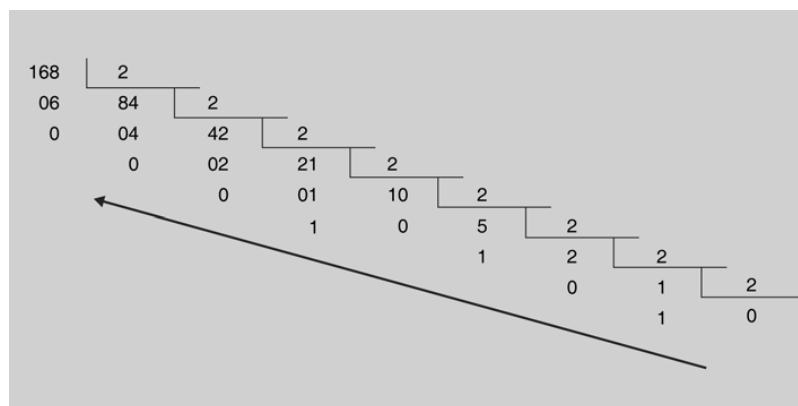
Per fer el canvi de base de decimal a binari, heu de dividir el nombre que voleu transformar entre la base a la qual voleu arribar tantes vegades com sigui possible fins a arribar a 0. Un cop heu arribat a 0, heu de prendre les restes de totes les divisions –des de l'última fins a la primera–, que només poden ser 0 o 1.

Un cop heu obtingut el primer octet, heu de transformar la resta de l'adreça IP. Per tant, ara heu d'agafar el segon octet, que és el nombre 168, i fer la transformació de base. S'ha d'anar fent la transformació de tota l'adreça octet a octet.

Per fer aquesta transformació, s'ha d'aplicar el mateix sistema que s'ha aplicat abans per transformar el 192 (figura 1.7); és a dir, agafem el 168 (figura 1.8) i el comencem a dividir entre 2 tantes vegades com faci falta. Aquesta divisió es realitzarà fins que s'hagi de multiplicar per 0.

Les restes en el sistema binari seran sempre i únicament o un 0 o un 1, perquè són els únics nombres permesos en aquest sistema.

FIGURA 1.8. Transformació de decimal a binari del nombre 168



És evident que, com en el cas anterior, el resultat ha de tenir 8 bits perquè és un camp d'una adreça IP. Recordeu, però, que per obtenir el nombre s'han d'agafar les restes des de l'última divisió fins a la primera: 10101000

Vegeu ara la transformació del tercer camp de l'adreça IP (figura 1.9): el procediment és el mateix, sempre dividir per la base a la qual volem arribar.

El nombre resultant tampoc no és de 8 bits, ja que per transformar-lo de decimal a binari només se'n necessiten 7. Per tant, com en el cas anterior, s'ha de posar un 0 al bit de més pes, és a dir, al bit de més a l'esquerra. El nombre resultant és: 01111011

Si uniu tots els nombres calculats, el resultat és el següent: 11000000.10101000.00100000.01111011

Aquí teniu l'adreça IP 192.168.32.123 en format binari.

Després d'haver vist la conversió de decimal a binari, us preguntareu per què és necessari separar l'adreça amb un punt cada vuit bits i què volen dir cada un dels nombres utilitzats. Aquestes dues qüestions tenen una explicació molt senzilla.

Per les persones, és molt més senzill recordar un nom que no pas un nombre perquè estem acostumats a treballar amb noms i no ho estem tant a fer-ho amb nombres, i per això es converteix aquest nombre en un nom.

A cada màquina connectada a Internet se li assigna un nom o, el que és el mateix, una adreça IP. Per intentar connectar amb una màquina determinada, es pot utilitzar el nom o l'adreça IP. A partir de l'equivalència entre noms i IP, l'adreça IP 213.123.121.21 podria correspondre a un servidor anomenat formació.informàtica.escola.es.

A l'hora de recordar una adreça d'una pàgina web a Internet, és més senzill de recordar un nom que no pas molts nombres. Per exemple, tothom recorda www.google.com, però ningú no en recorda l'equivalent en nombres; per aquest motiu, es fa una conversió del nom a l'adreça IP amb nombres, que en definitiva és el que entén la màquina.

El sistema que s'encarrega de traduir les adreces de noms a IP és el sistema de noms de domini (o *Domain Name System* o **DNS**)

Quan un usuari comença a navegar per Internet, indica al navegador el nom de la pàgina web a la qual vol accedir, per exemple, <http://www.google.com>. L'ordinador s'encarrega de convertir-lo a l'adreça IP –que seria 216.239.59.104– i, un cop es té aquesta dada, el navegador realitzarà la conversió d'aquest a un nombre binari –11011000.11101111.00111011.01101000–, que és el que la màquina és capaç d'entendre.

1.2.2 De binari a decimal

Per poder treballar correctament amb xarxes, no només cal saber fer el canvi de decimal a binari, sinó que també cal saber fer la conversió contrària és a dir, de binari a decimal. Heu de tenir en compte que, un cop heu entès la transformació de decimal a binari, la transformació contrària és molt més senzilla d'aprendre i de realitzar.

Utilitzarem la mateixa adreça IP que en el canvi de decimal a binari perquè veieu el funcionament d'aquesta conversió i pugueu comprovar ràpidament que el resultat ha estat correcte.

Partim de l'adreça IP en binari 11000000.10101000.00100000.01111011. En aquest cas, partiu amb avantatge, perquè ja sabeu el resultat que ha de sortir: 192.168.32.123.

El primer pas és separar el nombre en octets; en aquest cas, com que l'adreça IP ja la tenim separada en octets, començarem a treballar amb el primer nombre: 11000000.

S'ha d'agafar cada un dels bits i multiplicar-los per la base en què està el nombre que s'ha de transformar elevada a la posició que ocupa dins del nombre. Cal recordar que la primera posició –la de més a la dreta– sempre és 0, i s'hi han de sumar les multiplicacions.

$$\begin{aligned} 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 &= \\ = 1 \cdot 128 + 1 \cdot 64 + 0 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 &= \\ = 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 &= 192 \end{aligned}$$

Una vegada s'han fet les operacions (la multiplicació i la suma), ja es té el nombre del primer octet transformat a base 10. A continuació, s'ha de transformar el segon octet: 10101000.

$$\begin{aligned} 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 &= \\ = 1 \cdot 128 + 0 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 &= \\ = 128 + 0 + 32 + 0 + 8 + 0 + 0 + 0 &= 168 \end{aligned}$$

Ara és el moment de fer la transformació del tercer octet 00100000.

$$\begin{aligned} 0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 &= \\ = 0 \cdot 128 + 0 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 &= \\ = 0 + 0 + 32 + 0 + 0 + 0 + 0 + 0 &= 32 \end{aligned}$$

I per completar el canvi de base, només queda la transformació de l'últim octet, que en aquest cas és el 01111011:

$$\begin{aligned} 0 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 &= \\ = 0 \cdot 128 + 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 &= \\ = 0 + 64 + 32 + 16 + 8 + 0 + 2 + 1 &= 123 \end{aligned}$$

Un cop ha acabat la transformació del quart octet, només cal agafar tots els resultats i escriure'ls separats per un punt d'aquesta manera s'aconsegueix tenir l'adreça IP en format decimal.

Ús del canvi de binari a decimal

És molt important dominar aquesta transformació, perquè l'haureu de fer contínuament quan trebal·leu amb xarxes d'ordinadors.

Recordeu que per fer la transformació de binari a decimal sempre s'ha de multiplicar per la base de sortida.

Com podeu comprovar, el resultat obtingut és el que esperàveu, ja que coincideix amb el nombre en decimal que teníeu abans de començar.

Cal recordar que quan es fa la conversió de binari a decimal, la posició del bit de menys pes és 0.

2. Protocols de nivell d'enllaç

La capa d'enllaç és la responsable de la transferència fiable d'informació entre dos equips a través del medi de transmissió fent servir els serveis de la capa física. Aquests dos equips han d'estar connectats al mateix medi i aquesta capa s'encarrega de donar-los una adreça perquè es puguin comunicar entre ells. Per fer més fàcil la comunicació, s'agrupa la informació en trames i es controla que arribin a la destinació sense errors, controlant el flux de la comunicació perquè els equips puguin rebre la informació.

En el cas que dos equips intentin fer servir el medi al mateix temps, es produirien errors pels encavalcaments. Per tant, aquesta capa també ha de gestionar el moment en què un equip pot accedir al medi i així mitigar les col·lisions.

Generalment, l'accés al medi es gestiona des del microprogramari (*firmware*) de la targeta adaptadora i l'enllaç lògic mitjançant programari en el controlador del dispositiu.

2.1 Serveis de la capa d'enllaç

Dins de la capa d'enllaç es poden diferenciar dos conjunts de serveis complementaris. D'una banda, la gestió de la informació de la capa de xarxa, com pot ser la comprovació d'errors i la gestió del flux de dades entre equips amb velocitats diferents, s'anomena *control d'enllaç* (*logical link control*, LLC).

De l'altra, la gestió de l'adreçament físic dels equips, la distribució de les trames i la gestió de l'accés concurrent al medi compartit s'anomena *control d'accés al medi* (*medium access control*, MAC).

2.1.1 Control d'enllaç lògic

El control d'enllaç lògic gestiona la transmissió de trames entre dues estacions sense cap node intermedi i, en conseqüència, permet l'accés múltiple. A més, s'encarrega d'especificar l'equip origen i l'equip destinació. En el cas de l'Ethernet, aquesta adreça s'anomena *adreça MAC* (*medium access control address*).

Aquest protocol defineix mecanismes per controlar l'intercanvi de dades entre estacions. Hi ha tres serveis possibles:

1. **Servei no orientat a connexió sense confirmació:** Aquest mecanisme és el més senzill, ja que no inclou mecanismes de control de flux de dades ni

de control d'errors, per la qual cosa, amb aquest sistema no es garanteix el lliurament de les dades.

És útil quan els mecanismes de control de flux i d'integritat ja s'ofereixen en capes superiors. Un exemple d'això és el TCP, que ja ofereix prou mecanismes per assegurar la transmissió de la informació.

En alguns casos és preferible un servei no orientat a connexió i sense confirmació. Per exemple, pot ser preferible perdre alguns paquets abans que evitar el retard que comporta la retransmissió en una aplicació de videoconferència.

2. **Servei en mode connexió:** S'estableix una connexió lògica entre els equips prèvia a l'intercanvi de dades. En aquest cas, hi ha un sistema de control de flux i d'errors.

Sol ser útil en dispositius extremament simples les capes superiors dels quals disposen de poc programari.

3. **Servei no orientat a connexió amb confirmació:** És una barreja dels anteriors: els datagrames es confirmen quan es reben, però no hi ha connexió.

Una aplicació possible són els senyals d'alarma: cal confirmar que s'han rebut correctament.

2.1.2 Control d'accés al medi

El control d'accés al medi (MAC, *medium access control*) fa referència als protocols que decideixen a quin ordinador es permet transmetre dades.

A l'hora de parlar del control d'accés al medi és important esmentar les dues categories que hi ha: les deterministes (per torns) i les no deterministes (a grans trets, "el primer que arriba és el primer a ser servit").

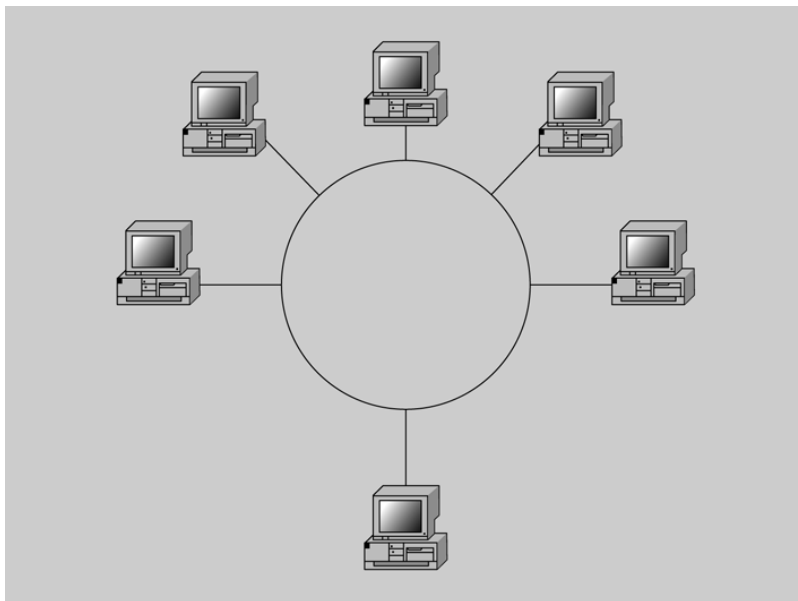
Protocols MAC deterministes

Els protocols MAC deterministes utilitzen una modalitat basada en la creació de torns. Un exemple d'aquests torns es fonamenta en la transmissió de testimonis (*tokens*).

La tècnica de la transmissió de testimonis es basa en un costum propi de les tribus d'indis nadius americans que, durant les reunions, es passaven el testimoni o "**bastó que parla**". De fet, la persona que tenia a les mans el "**bastó**" era escoltat per tothom fins que finalitzava el parlament, moment en què passava el testimoni a una altra persona.

Hi ha un protocol d'enllaç de dades, que rep el nom d'*anell de testimoni* (*token ring*), en què els ordinadors que estan connectats a la xarxa es distribueixen en forma d'anell (figura 2.1). Per aquest anell circula un testimoni (*token*) de dades especials que és pres temporalment per l'ordinador que vol transmetre dades. Un cop ha finalitzat la transmissió de dades, l'ordinador deixa lliure el testimoni perquè torni a circular per l'anell i pugui ser pres per un altre ordinador.

FIGURA 2.1. Anell de testimoni



Físicament sol substituir-se l'anella per un concentrador al qual hi estan connectats tots els ordinadors. Aquest concentrador, quan arriba una trama per la connexió número n l'envia per la connexió $n+1$; quan n'arriba una per la darrera connexió, l'envia per la primera. D'aquesta manera simula una anella. Això permet realitzar una instal·lació física més senzilla.

Avui en dia, Token Ring ha quedat obsolet. No obstant això, altres protocols posteriors, com ara FDDI, s'han implementat seguint aquesta mateixa filosofia. FDDI és un dels protocols que treballen amb fibra òptica (però, ni molt menys, l'únic).

Protocols MAC no deterministes

Els protocols MAC no deterministes utilitzen la premissa "el primer que arriba és el primer a ser servit" (FCFS, *first-come, first-served*) com, per exemple, l'accés múltiple amb detecció de portadora i detecció de col·lisions (CSMA/CD, *carrier sense multiple access / collision detect*).

Aquest tipus de protocol és el que fa servir Ethernet, atès que permet que els dispositius de xarxa esdevinguin els responsables d'administrar el seu dret a transmetre. De fet, la mecànica es fonamenta en el fet que les estacions d'una xarxa CSMA/CD escoltin quin és el millor moment per transmetre. Malgrat tot, en cas que dues estacions transmetin alhora es produeix una col·lisió i cap de les transmissions de les estacions no té èxit.

Col·lisió

A l'Ethernet, una col·lisió és el resultat de dos nodes que transmeten simultàniament. Les trames de cadascun dels dispositius col·lideixen i es fan malbé quan es troben en el medi físic.

En el moment en què les estacions de la xarxa senten que hi ha hagut una col·lisió, esperen en silenci; és a dir, a partir d'una ordre per torns, les estacions transmissores esperen un període de temps aleatori abans de transmetre. Aquesta espera per part de les estacions permet que no hi hagi una segona col·lisió.

Com heu pogut deduir, hi ha dos punts importants en tot protocol d'accés al medi:

- On es fa el control? Si el control es fa centralitzat o distribuït.
- Com es fa el control? És un compromís entre prestacions, cost i complexitat tenint en compte el tipus de medi que es comparteix.

En el cas sobre el lloc *on es fa el control*, si parlem d'un control centralitzat voldrà dir que es designa un equip que fa de controlador del medi. En el cas que sigui un control descentralitzat, tots els equips en conjunt decideixen qui accedeix en aquell moment al medi.

Podem classificar el cas sobre la manera *com es fa el control* en tres grans grups:

1. **Rotació circular.** Mitjançant la tècnica de rotació circular, es dona a cada estació l'oportunitat de transmetre en una seqüència determinada. Cada estació pot fer-ho dins d'uns límits establerts o bé declinar l'oportunitat.

En el cas que molts equips tinguin la necessitat de transmetre durant un llarg període de temps és molt eficient, ja que es reparteixen el medi equitativament. Al contrari, si hi ha pocs equips que tinguin la necessitat de transmetre informació durant un llarg període de temps, resulta poc eficient, atès que es perd el temps en què els equips que no volen transmetre es van passant el testimoni.

2. **Reserva.** Les tècniques amb què es fa una reserva del medi són adequades per al trànsit continu: es divideix el temps en porcions i els equips que volen transmetre fan reserves.

3. **Contenció.** En el cas de trànsit a ràfegues, són més adequades les tècniques de contenció, que consisteixen a no controlar el torn per transmetre, és a dir, que tots els equips poden transmetre en qualsevol moment. Per això cal determinar alguna manera de saber si el medi ja està en ús. Aquest sistema, per la naturalesa totalment distribuïda que té, és molt eficient quan la càrrega de la xarxa és de mitjana a alta. En cas que la càrrega sigui alta, tendeix a ser menys eficient per les col·lisions que s'hi produeixen.

Un exemple de protocol d'accés al medi per rotació circular és l'anell de testimoni (IEEE 802.5).

Un exemple de protocol d'accés al medi amb reserva és el DQDB (IEEE_802.6).

Un exemple de protocol d'accés al medi per contenció és l'Ethernet (IEEE 802.3).

2.2 IEEE 802

Dins del conjunt d'estàndards IEEE 802, podem trobar la definició del medi, la capa física i la capa d'enllaç de protocols com l'Ethernet, l'anell de testimoni, el Wi-Fi, el WiMAX o el Bluetooth.

Cada un dels estàndards pertany a un grup de treball que s'identifica amb un punt i el número. Per exemple, el grup de treball de l'Ethernet s'anomena 802.3, el qual defineix tant la capa física com el control d'accés al medi. Amb la capa física també s'inclou l'especificació del medi de transmissió i la topologia de xarxa. El protocol de control d'enllaç lògic no el recull l'IEEE 802.3, sinó que es defineix en l'IEEE 802.2, depenent del tipus de medi (l'Ethernet, anell de testimoni, l'FDDI, 802.11, etc.).

2.2.1 L'Ethernet 802.3

La tècnica de control d'accés al medi més usada actualment en topologies en bus i estrella és la d'accés múltiple amb detecció de portadora i detecció d'errors o col·lisions (CSMA/CD, *carrier sense multiple access / collision detect*). Aquesta tècnica va ser desenvolupada per Xerox per a xarxes locals i va ser la base per a l'especificació posterior IEEE 802.3.

Aquesta tecnologia de difusió duu a terme tres funcions fonamentals:

1. Transmetre i rebre paquets de dades.
2. Descodificar paquets de dades i comprovar la validesa de les adreces abans de passar-los a les capes superiors del model de referència OSI.
3. Detectar els errors que hi pugui haver en la xarxa o en els mateixos paquets que es transmeten.

En el mètode d'accés múltiple amb detecció de portadora i detecció de col·lisions, els dispositius de la xarxa treballen "escoltant abans de transmetre" (CS, *carrier sense*); és a dir, quan un dispositiu vol enviar dades, en primer lloc comprova si el medi està ocupat. En cas que estigui lliure, el dispositiu comença a transmetre les dades, tot i que, mentrestant, el dispositiu continua escoltant per confirmar que no hi ha cap altra estació que també transmeti dades. Si s'esdevé aquesta situació, hi podria haver una col·lisió. En cas contrari, el dispositiu finalitza la transmissió i torna a la modalitat d'oïent (figura 2.2).

Quan col·lideixen dues trames perquè fan servir el medi concurrentment, el medi queda inutilitzat mentre dura la transmissió. Les regles que es defineixen per a l'ús del medi són les següents:

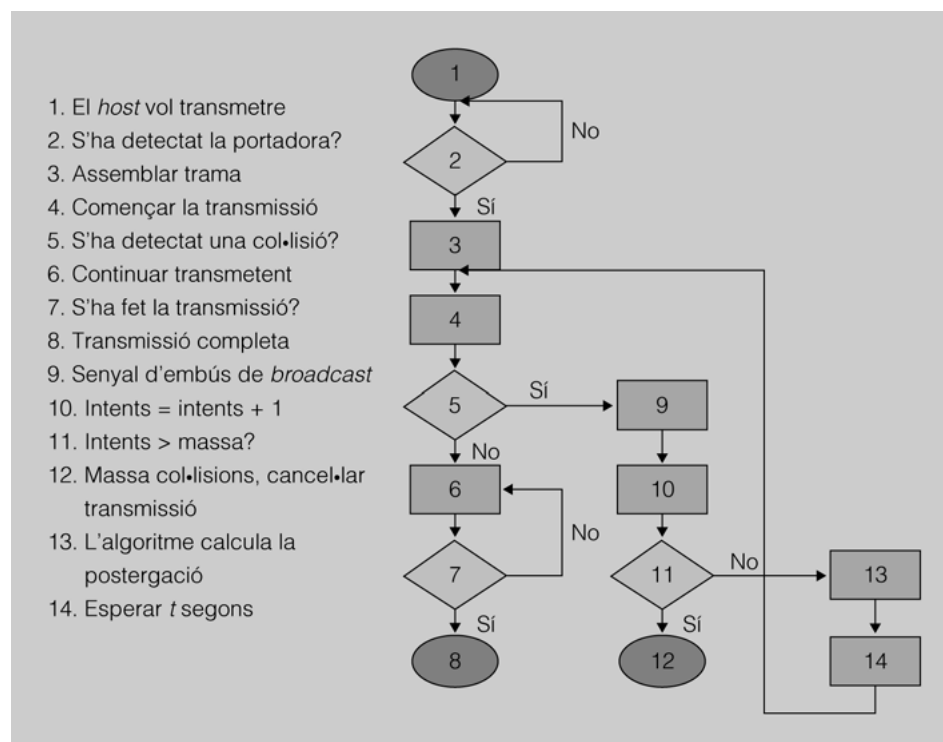
- L'equip transmet si el medi està lliure.
- Si el medi està ocupat, l'equip continua escoltant fins que quedi lliure.
- Si es detecta una col·lisió, l'equip transmet un senyal d'alerta perquè tots els equips s'adonin de la col·lisió.
- Espera un temps aleatori i ho torna a intentar.

Detecció de col·lisions

Els dispositius de xarxa tenen la capacitat de detectar quan s'ha produït una col·lisió, atès que augmenta l'amplitud del senyal (CD, *collision detect*). Quan hi ha una col·lisió, cadascun dels dispositius que transmet dades continua amb la transmissió durant un espai de temps breu per confirmar que tots els dispositius veuen la col·lisió i introdueixen un algoritme de retard; és a dir, esperen un espai de temps aleatori.

Per tant, es tracta d'un control d'accés al medi per contenció descentralitzat, ja que no hi ha cap equip encarregat de la gestió del medi, sinó que aplicant un conjunt de regles en tots els equips sorgeix un ordre del caos aparent.

FIGURA 2.2. Procés CSMA_CD



2.2.2 Anell de testimoni (l'IEEE 802.5)

La tècnica d'anell de testimoni per al control d'accés al medi es basa en una petita trama, anomenada *testimoni* (*token*), que va circulant per tots els equips.

En començar a transmetre, es canvia un dels bits del testimoni i comencen a circular les trames de dades. Evidentment, quan una estació transmet desapareix el testimoni i, per tant, totes les estacions s'han de mantenir escoltant.

La trama que s'ha emès fa una volta completa a l'anell i l'estació emissora la torna a llegir (per comprovar que no s'han alterat les dades) i l'elimina. El testimoni es torna a inserir quan l'equip ha acabat de transmetre o si li arriba de nou l'emissió abans d'haver acabat d'emetre. Un cop inserit de nou el testimoni, l'estació següent decideix si vol transmetre o passa el testimoni a la següent.

Es tracta d'un sistema poc eficaç si la càrrega del medi és baixa, ja que un equip ha d'esperar que li arribi el testimoni encara que la resta no vulgui transmetre. Tot i això, en cas de càrrega alta és un sistema per torns molt equitatiu que dona l'oportunitat de transmetre a tots els equips de la xarxa.

Els inconvenients principals de la xarxa en anell de testimoni són la definició de procediments per controlar els possibles errors en l'anell. Per exemple, si es perdés el testimoni, cap equip no podria transmetre.

En aquest estàndard també podem trobar certes característiques opcionals com uns bits per definir la prioritat d'una trama, l'opció d'alliberament ràpid del testimoni, o bé, una xarxa dedicada per al pas del testimoni.

Aquest protocol actualment es troba en desús per la popularització de l'Ethernet.

2.2.3 EI DQDB (l'IEEE 802.6)

DQDB significa 'bus dual de cua distribuïda' (*distributed-queue dual-bus network*) i ja no s'usa per l'expansió de les xarxes LAN i WAN. Al principi estava dissenyat per ser una xarxa MAN (xarxa d'àrea metropolitana), a mig camí entre una LAN (xarxa d'àrea local) i una WAN (xarxa d'àrea àmplia), que prometia velocitat per a xarxes que s'escapen de l'àrea local.

En el cas de l'estàndard IEEE 802.6, és format per dos busos unidireccionals paral·lels per a tota l'àrea que s'ha de cobrir. Quan un equip vol transmetre, de primer ha de confirmar l'adreça del receptor (dreta o esquerra) i després ha de fer servir el bus adequat. Un cop formada la xarxa, cada equip ha de comprovar les adreces dels altres equips, cosa que genera grans esperes, especialment quan la xarxa creix en nombre d'equips.

2.2.4 Les col·lisions

Les col·lisions acostumen a produir-se quan dos o més estacions Ethernet transmeten alhora dins d'un mateix domini de col·lisió. A grans trets, una col·lisió és detectada mentre s'estava transmetent una trama, tot i que, en intents posteriors, la trama s'hagi transmès correctament.

Una diferència important que hi ha entre col·lisió i transmissió diferida és que la primera es produeix quan ja s'ha començat a transmetre la trama, mentre que la segona es produeix abans de començar a transmetre la trama.

Aquesta situació és diferent en el cas de les trames amb transmissions diferides, atès que permeten la inexistència de col·lisions.

Les trames parcials o totalment fallides són les resultants de l'existència d'una col·lisió i s'anomenen fragments de la col·lisió.

Podeu trobar la definició de **domini de col·lisió** a l'apartat "Dominis de col·lisió i difusió (broadcast i segmentació)".

Transmissió diferida

La transmissió diferida és un procés de latència en què entra una estació amb intenció de transmetre si, prèviament, ha confirmat que el medi està ocupat. A grans trets, la transmissió es basa en una cadena de processos, com "esperar, escoltar i transmetre".

Tipus de col·lisions

Els principals tipus d'errors que hi poden haver amb trames Ethernet s'anomenen col·lisions locals, col·lisions remotes i, per últim, col·lisions endarrerides.

La **col·lisió local** és una situació que es produeix quan un senyal que viatja per un medi es troba amb un senyal d'una altra estació. És en aquest moment quan les ones se solapen, això és, es cancel·len algunes parts del senyal i unes altres es reforcen (és a dir, se'n dobla el valor). Quan es dobla una part del senyal, es produeix un augment del seu voltatge per sobre del nivell màxim permès. Totes les estacions presents en el segment de la xarxa on es produeix aquesta situació notaran aquest augment de la tensió i la identificaran com una col·lisió.

Col·lisions endarrerides

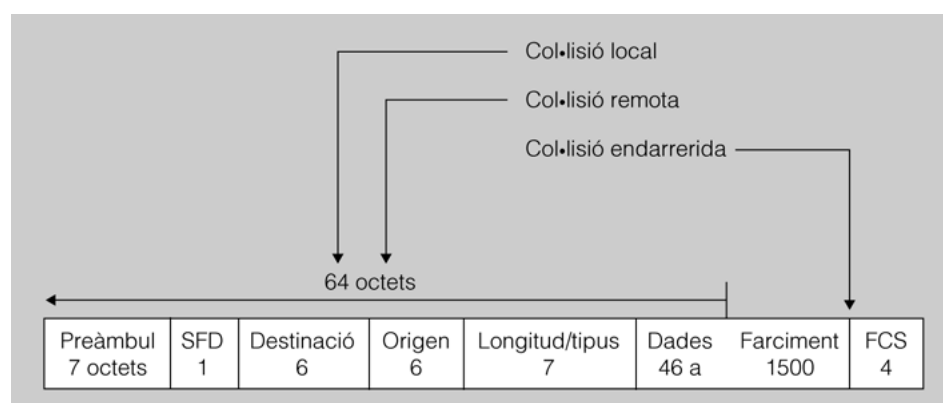
Es pot donar una col·lisió endarrerida si el temps que tarda una senyal a desplaçar-se des d'un extrem de la xarxa a l'altre excedeix, aproximadament, els 57,6 microsegons.

Una de les conseqüències d'una col·lisió és la presència de trossets de les trames que han col·lidit circulant per la xarxa. En aquest cas, quan el resultat que es deriva de la col·lisió són trames malmeses que no presenten la longitud mínima i que, a més, tenen una seqüència de verificació (FCS, *frame check sequence*) errònia s'anomena **col·lisió remota**.

Per altra banda, s'anomena **col·lisió endarrerida** la presència d'una trama amb la seqüència de verificació errònia provocada per una targeta d'interfície de xarxa (NIC, *network interface card*) defectuosa. Val a dir que també es considera col·lisió endarrerida la degradació de la trama d'informació per una longitud de cable de xarxa excessiu.

Un cop definits els diferents tipus de col·lisions que hi poden haver, és important situar la seva influència dins de l'estructura d'una trama Ethernet IEEE 802.3 tal com mostra la figura 2.3.

FIGURA 2.3. Tipus de col·lisions



Característiques de cada tipus (resum):

- Col·lisió local:
 - Es produeix quan coincideixen dues trames al mateix segment.
 - Es detecta per sobrevoltatge al senyal (per coincidència de dades amb voltatge alt —els voltatges es “sumen”—).

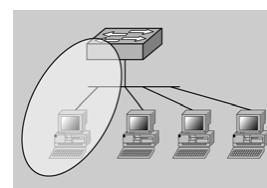
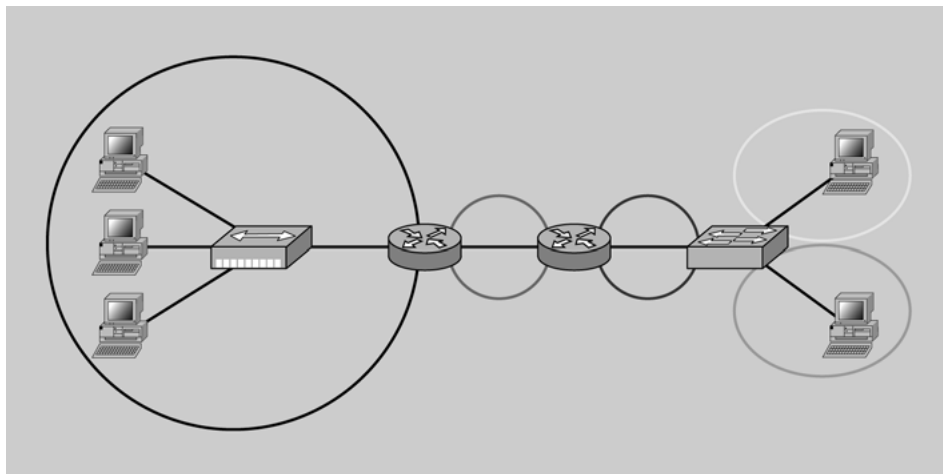
- Col·lisió remota:
 - Es detecta perquè hi ha fragments de trama circulant pel segment. Aquests fragments tenen una longitud inferior a la mínima i/o una FCS errònia.
 - Sol originar-se per una col·lisió local en un altre segment. Aquesta col·lisió genera senyals amb sobrevoltatge que no són reenviats pel dispositiu que uneix els segments.
- Col·lisió endarrerida:
 - Es detecta per una FCS errònia.
 - És originada habitualment per una targeta de xarxa defectuosa (NIC) o per la degradació del senyal causada per un cable de xarxa de longitud excessiva.

Dominis de col·lisió i difusió (broadcast i segmentació)

Un domini de col·lisió és, tal com mostra la figura 2.4, un segment físic d'una xarxa d'ordinadors on hi ha possibilitats que els paquets puguin xocar, això és, en el cas que dos ordinadors transmetin per un medi compartit.

Un segment de xarxa és qualsevol medi de xarxa compartit com, per exemple, un cable i un dispositiu, és a dir, un commutador o un concentrador.

FIGURA 2.4. Cinc dominis de col·lisió



Un segment de xarxa és qualsevol medi de xarxa compartit com, per exemple, un cable i un dispositiu, o sigui un commutador o un concentrador.

Símbols utilitzats

Un **commutador** (*switch*) es representa com un dispositiu rectangular amb 4 fletxes.

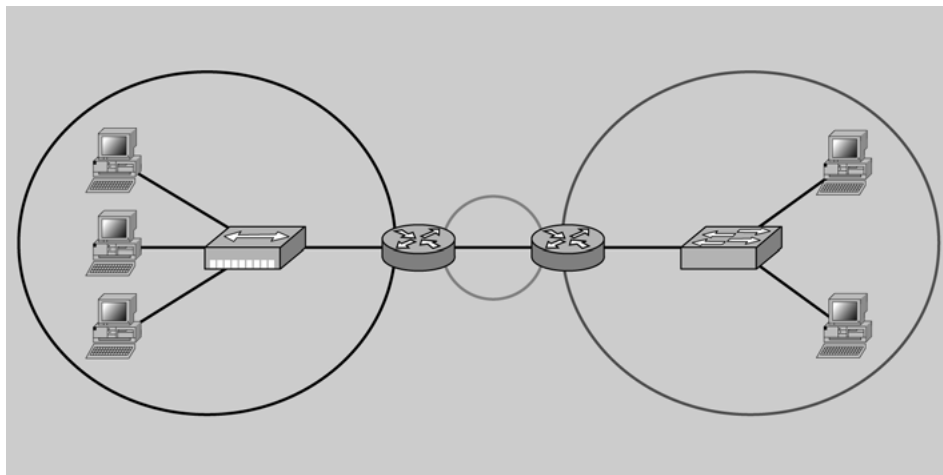
Un **concentrador** (*hub*) es representa com un dispositiu rectangular amb 2 fletxes.

Un **encaminador** (*router*) es representa com un dispositiu de forma circular.

Des del punt de vista dels dispositius que hi ha en una xarxa, cal destacar que els commutadors i els encaminadors segmenten dominis de col·lisió. En el cas dels concentradors, presenten un únic domini de col·lisió, és a dir, en el cas que dos equips provoquin una col·lisió en un segment associat a un port del concentrador, tots els altres dispositius es veuen afectats (encara que estiguin connectats a diferents ports).

Tal com es veu en la figura 2.5, un domini de difusió MAC (*media access control*) està constituït per tots els dispositius que estan connectats a una xarxa d'àrea local i que reben difusions de trames de dades enviades d'una màquina a totes les altres. A grans trets, podem dir que un domini de difusió MAC és un grup de dispositius de la xarxa que envien i reben missatges de difusió entre ells.

FIGURA 2.5. Tres dominis de difusió



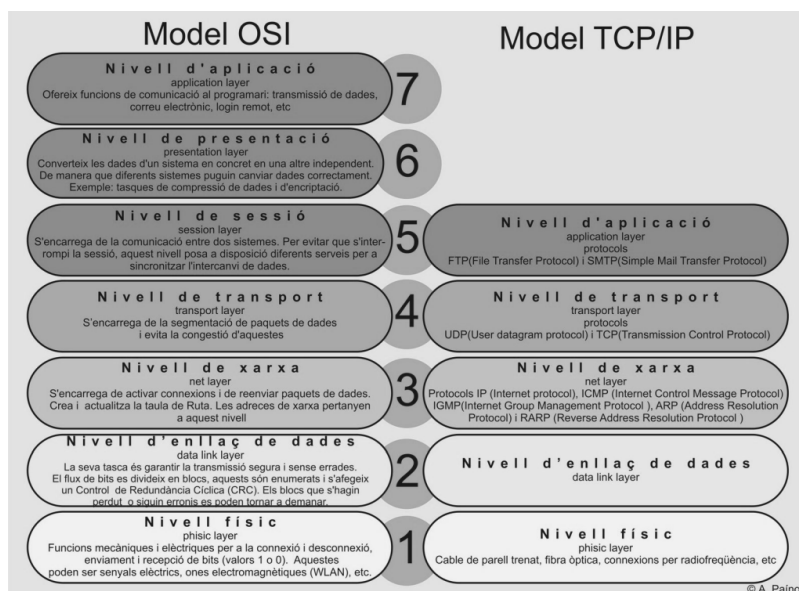
Des del punt de vista dels dispositius presents en una xarxa, cal destacar que els encaminadors segmenten els dominis de difusió.

3. Protocols de xarxa

El terme *protocol de xarxa* descriu tot el programari d'un ordinador que permet que les seves aplicacions utilitzin els recursos, però no són programes que es puguin instal·lar o esborrar. Aquests programes són diferents segons el sistema operatiu que es faci servir. Poden ser fitxers de suport, com les biblioteques de vincles dinàmics (DLL, *dynamic load library*) en els sistemes Windows, o poden estar integrats en el nucli o com un mòdul que es pot carregar en qualsevol moment, en el cas dels sistemes GNU/Linux.

Tot i això, en adaptadors de gamma alta, certes parts dels protocols de xarxa s'implementen mitjançant microprogramari o xips dedicats per treure la càrrega que comporta aquesta feina al sistema operatiu.

FIGURA 3.1. Models OSI i TCP-IP



Els protocols de xarxa, que se situen en la capa 3 del model OSI (figura 3.1), són els responsables de transmetre informació des d'un ordinador amfitrió (*host*) a un altre sense necessitat que aquests estiguin connectats directament: la informació viatja des de l'ordinador amfitrió origen fins al de destinació traspasant tants medis com calgui; per tant, també ha de ser capaç d'encaminar els paquets.

3.1 Funcions dels protocols de xarxa

En el cas que dos equips no estiguin connectats a la mateixa xarxa, cal definir un mecanisme perquè les dades es passin a uns nodes que fan d'intermediaris,

anomenats *encaminadors*. Aquests nodes connecten dues xarxes o més i la funció principal és retransmetre dades d'una xarxa a una altra d'acord amb una ruta perquè els paquets arribin a la destinació.

1. Adreçament

La capa de xarxa ha de mantenir l'adreçament dels ordinadors amfitrions; d'una banda, per enviar dades entre ordinadors amfitrions que no estan connectats directament i, de l'altra, perquè els encaminadors estableixin la millor ruta entre els dos punts.

Per tant, cal identificar d'una manera única els ordinadors amfitrions i cal definir un sistema d'agrupar-los per afavorir que, quan els encaminadors que hi ha al mig dels dos extrems es comuniquin, siguin capaços de dirigir el trànsit eficientment.

2. Encaminament

Per passar dades entre un ordinador amfitrió i un altre cal definir un mecanisme d'encaminament perquè, cada cop que es passin les dades a l'encaminador següent, estigui més a prop del node final.

Els encaminadors són equips la funció principal dels quals és moure els paquets entre les xarxes a les quals estan connectats tenint en compte factors com la proximitat del node final o la saturació d'algun enllaç.

3. Tipus de ruta

Una altra de les funcions dels protocols de xarxa és definir una ruta entre els dos ordinadors amfitrions que s'han de comunicar. Es poden seguir dues estratègies:

- **Sense connexió:** sense establir cap camí en concret, cada vegada que s'envii un datagrama es decidirà el camí que es recorrerà.
- **Circuit virtual:** s'estableix inicialment un camí entre els dos equips i es reserven recursos per a aquest camí. Equivaldria a passar un cable d'extrem a extrem dedicat per aquests dos ordinadors amfitrions.

3.2 IP (Internet protocol)

La versió més usada actualment del protocol IP és la IPv4, definida en l'RFC 791 del 1981. Actualment ja disposa d'un successor, la IPv6, l'ús de la qual es va estenent progressivament.

Totes les versions del protocol IP permeten l'enviament de paquets entre equips sense establir cap mena de connexió. Això vol dir que l'ordinador amfitrió origen envia dades al destinatari sense esperar cap mena de notificació que les dades s'han rebut correctament.

Avui dia, el TCP/IP és el conjunt de protocols escollit per a la immensa majoria de les xarxes actuals i, per descomptat, per a qualsevol sistema que es vulgui connectar a Internet.

Tot i que per enviar dades entre dos ordinadors amfitrions ja n'hi ha prou amb el protocol IP, no ofereix cap mena de garantia que s'enviïn correctament les dades o, ni tan sols, que arribin a la destinació. De fet, no ens garanteix que les dades, si arriben a la destinació, estiguin intactes, ja que el control d'errors només es fa sobre les capçaleres, no sobre les dades que transmet. Així doncs, tot i que es pot fer servir IP directament, per a aplicacions que requereixen fiabilitat fan servir al protocol de la capa de transport TCP.

1. Adreçament IP

Una de les funcions principals dels protocols de xarxa és proveir d'adreçament els elements perquè puguin enviar-se dades entre si. Entre el protocol IPv4 i el protocol IPv6 canvia la longitud i la representació de la direcció completament.

2. Tipus d'adreçament

En l'RFC 1918 del 1996 es defineixen els conjunts sobre el total d'adreces IPv4 que es destinen a la creació de xarxes privades, com pot ser la xarxa interna d'una empresa que no necessita que es pugui accedir als equips directament des d'Internet. Els rangs definits com a privats són els següents:

- El bloc que va de la IP 10.0.0.0 a la 10.255.255.255
- El bloc que va de la IP 172.16.0.0 a la 172.31.255.255
- El bloc que va de la IP 192.168.0.0 a la 192.168.255.255

En l'RFC 3330 del 2002 es va definir un altre rang que es pot considerar privat i que s'anomena *d'autoconfiguració* (o *d'enllaç local*). Aquest rang va de la IP 169.254.0.0 a la 169.254.255.255. S'anomena *d'autoconfiguració* perquè, en cas que un equip que es vulgui connectar a la xarxa sol·licitant una IP mitjançant el protocol DHCP no obtingui resposta, s'autoassigna una IP aleatòria dintre d'aquest rang per obtenir un accés mínim a la xarxa.

Les adreces privades només són visibles dins les xarxes locals on són definides. Per tant, a Internet pot haver-hi adreces privades que apareguin a més d'una xarxa local, ja que, en no veure's entre elles, no s'interfereixen. NAT permet que aquests ordinadors amb adreces privades puguin utilitzar l'adreça pública de l'encaminador per accedir a Internet.

Les adreces públiques, per contra, es veuen a tot Internet i no pot haver-hi dues màquines amb la mateixa adreça IP.

3. La necessitat de la IPv6

La IP v4 consta de quatre octets (és a dir, 32 bits) que es representen separats per punts en decimal; per exemple, una adreça vàlida pot ser 1.2.3.4.

Podeu consultar què és el **NAT** a l'apartat "Adreçament públic i privat: NAT".

Això dona un total de 2^{32} adreces vàlides, o el que és el mateix, 4.294.967.296 adreces possibles. Amb la gran expansió d'Internet ha esdevingut un problema, ja que el nombre d'adreces assignades respecte al total d'adreces possibles és cada vegada més alt. Per això s'han desenvolupat tècniques com el NAT, per permetre que sistemes amb adreçament privat es puguin comunicar amb sistemes amb adreçament públic.

Amb la idea de permetre que qualsevol dispositiu pugui tenir una adreça IP única, es va desenvolupar la IPv6: es va passar dels 32 bits de la IPv4 als 128 de la nova versió. Això dona un total de 2^{128} , és a dir, $3,4 \cdot 10^{38}$ adreces IP. Dit d'una manera més entenedora, cada persona del planeta pot tenir uns quants milions d'adreces IPv6.

La representació de les adreces IPv6 és sensiblement diferent: es representen en hexadecimal en conjunts de 16 bits separats per dos punts. Per exemple, una adreça IPv6 vàlida pot ser: 2001:0123:4567:89ab:cdef:dead:beef:0001

3.3 L'ICMP

L'ICMP és un protocol de la capa de xarxa que complementa el protocol IP per a tasques de control i notificació d'errors. Està definit en l'RFC 792 com a complement imprescindible del protocol IP.

Malgrat que aquest protocol no està concebut perquè hi hagi aplicacions que el facin servir, n'hi ha algunes com *ping* i *traceroute* que l'utilitzen, principalment com a eines de diagnostic de la xarxa.

3.3.1 L'ordre ping

Mitjançant l'ordre *ping* es pot comprovar si hi ha connectivitat entre dos equips diferents mitjançant paquets ICMP. L'ordinador amfitrió que executa l'ordre *ping* envia una petició d'eco (*echo request*) i l'equip que la rep ha de contestar amb una resposta d'eco (*echo reply*). Sovint s'utilitza el temps que es tarda des que s'envia la petició fins que es rep la resposta per mesurar latències de xarxa, per això algunes vegades el terme *ping* es pot referir a aquest retard.

3.3.2 L'ordre traceroute

L'ordre *traceroute* és una eina que ens permet, dintre d'unes certes limitacions, descobrir la ruta que segueix un paquet IP des de l'equip origen fins al de destinació. Per fer-ho s'utilitza el camp TTL dels paquets IP, el qual indica el nombre de salts que li resten abans que es descarti el paquet.

Si s'envia un paquet amb un TTL d'1, el primer encaminador descartarà el paquet i enviarà un paquet ICMP de tipus temps esgotat (*time exceeded*) a l'ordinador amfitrió que ha originat el primer paquet. Aquest paquet de temps esgotat conté l'adreça IP de l'encaminador que ha descartat el paquet inicial. Així s'obté l'adreça IP del primer encaminador. Si es repeteix l'operació amb un 2 obtindrem el següent, i així successivament.

A continuació podem veure la sortida de l'execució de l'ordre `tracert`:

```

1 # traceroute to systemadmin.es
2   traceroute to systemadmin.es (91.121.113.59), 30 hops max, 40 byte packets
3   1  82.98.141.253 (82.98.141.253)  1.935 ms  2.245 ms  2.491 ms
4   2  10.1.1.1 (10.1.1.1)  0.324 ms  0.367 ms  0.419 ms
5   3  193.149.1.81 (193.149.1.81)  4.406 ms  *  *
6   4  *  *  *
7   5  160g.rbx-2-6k.routers.choix.eu (213.186.32.222)  22.144 ms  *  *
8   6  rbx-36-m1.routers.choix.eu (213.251.191.231)  20.266 ms  20.257 ms  20.460
9   7  mail.systemadmin.es (91.121.113.59)  20.042 ms  19.878 ms  19.848 ms

```

Tot i això, alguns encaminadors poden no enviar aquest missatge ICMP i només descartar el paquet; per tant, si no s'ha rebut la resposta en un cert temps es marca l'encaminador amb un asterisc, com en el salt 4 de l'exemple anterior.

De totes maneres, és possible que hi hagi encaminadors que no puguem descobrir perquè no modifiquen el TTL del paquet i, per tant, les dades passen silenciosament a través seu.

3.4 ARP

El protocol ARP s'encarrega de resoldre l'adreça de la capa d'enllaç a partir de l'adreça de la capa de xarxa tal com està definit en l'RFC 826 del 1982. En el cas típic ens trobaríem amb una xarxa IP sobre una xarxa Ethernet i, per tant, el protocol ARP ens resoldria l'adreça MAC a partir de l'adreça IP.

Per fer això, la màquina que vol saber l'adreça MAC que té una certa IP envia un paquet de tipus petició ARP (*ARP request*) a l'adreça de difusió de la capa d'enllaç i espera que la màquina que té la IP o qualsevol altra li respongui mitjançant un paquet de resposta ARP (*ARP response*).

Un cop obtinguda la resposta, s'emmagatzema, durant un cert temps, en una taula local de cada sistema: això evita que cada vegada que es vulgui enviar un paquet s'hagi de tornar a demanar la mateixa informació. Aquesta taula ARP s'esborra periòdicament per evitar que si una IP s'assigna a un altre equip els paquets es continuïn enviant a l'equip antic.

Adreça MAC de difusió

Hi ha un tipus d'adreça MAC especial que tots els dispositius d'una xarxa LAN utilitzen per comunicar-se d'una manera simultània. Aquesta adreça s'anomena *adreça de difusió* i es representa FF-FF-FF-FF-FF-FF.

3.4.1 Assignació estàtica

Quan les adreces IP s'assignen estàticament, cadascun dels dispositius s'ha de configurar amb una única adreça IP. De fet, aquest mètode requereix guardar registres de les assignacions d'adreces, atès que podrien aparèixer problemes dins d'una xarxa en cas d'utilitzar adreces IP duplicades.

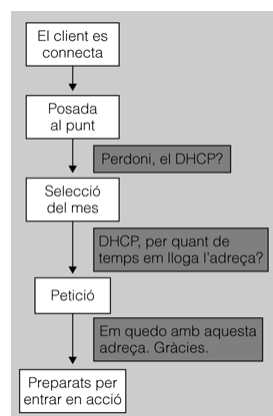
Des del punt de vista de la xarxa, hi ha diversos dispositius que han de tenir assignada d'una manera permanent (o estàtica) una adreça IP, ja que alguns dispositius hi han de fer referència. En cas que dispositius com impressores en xarxa, servidors d'aplicacions o encaminadors no disposin d'una adreça IP estàtica, la xarxa s'ha de configurar de nou en tot moment. En poques paraules, si es donés aquesta situació, la xarxa esdevindria inútil.

L'assignació estàtica d'adreces IP té l'inconvenient que pot comportar problemes de seguretat, ja que pot esdevenir una porta d'accés important per als pirates informàtics. Cal destacar que poden passar dies o setmanes fins que no es detecta que els pirates han accedit a les dades contingudes en l'ordinador.

Podeu consultar el referent a DDNS (DNS dinàmic) a l'apartat "DDNS (dynamic DNS)".

Per a un dispositiu de referència, una alternativa a l'ús d'una adreça estàtica és assignar dinàmicament un nom a la seva adreça. Així es pot accedir el dispositiu fent referència al nom que li hem assignat (que no varia), en lloc de fer-ho a l'adreça IP (que pot variar si és dinàmica). DDNS (DNS dinàmic) és un protocol que permet fer aquesta mena d'assignacions dinàmiques de noms a adreces IP.

3.4.2 Assignació dinàmica



Esquema d'assignació dinàmica d'adreces

Tenint en compte que dins d'una xarxa hi ha un ventall d'adreces que ja estan assignades, la resta s'han d'assignar, per exemple, a les màquines que s'hi connectin. Amb tot, depenent de les dimensions de la xarxa, el nombre d'adreces disponibles pot ser limitat. Per això es va trobar el mètode d'assignació dinàmica d'adreces IP, perquè es connectin intermitentment a la xarxa. Aquest servei d'atorgament de les adreces IP que, en el moment de la connexió, estiguin lliures permet evitar la feina de configuració a l'administrador de la xarxa.

Per a l'assignació dinàmica de les adreces IP es van crear serveis com el **DHCP** o el **BOOTP**.

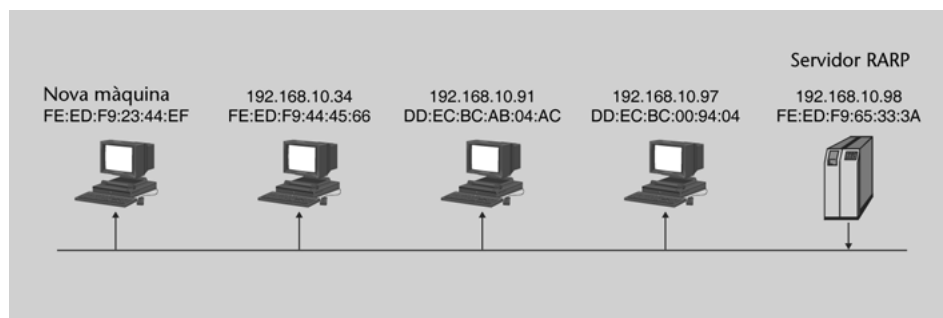
3.4.3 Protocol de resolució d'adreces invers (RARP)

El **protocol RARP** serveix perquè les màquines que no tenen una adreça IP la puguin obtenir.

El funcionament és el següent: quan una màquina es connecta a la xarxa i no té adreça, envia un missatge de difusió per demanar-ne una. Aquest missatge només és respost pel servidor RARP amb un nou paquet de difusió que conté l'adreça IP que caldrà assignar a la màquina sol·licitant.

Totes les màquines ignoraran el paquet excepte la màquina que hem connectat, que entendrà que el missatge és per a ella i se'l quedarà. En el moment en què la nova màquina accepti el paquet enviat pel servidor RARP, l'examinarà i n'extraurà l'adreça IP. En aquest moment, la nova màquina ja tindrà la seva pròpia adreça IP i, per tant, ja podrà començar a transmetre dades (figura 3.2).

FIGURA 3.2. Servidor i missatges RARP



Cal destacar que el missatge RARP que envia l'ordinador que acabem de connectar el rebran totes les màquines, atès que no sap quin és el servidor RARP, l'examinaran i, en veure que es tracta d'una petició d'adreça IP (és a dir, un paquet que no és per a ells), l'ignoraran. Solament el servidor RARP entendrà que el paquet està adreçat a ell.

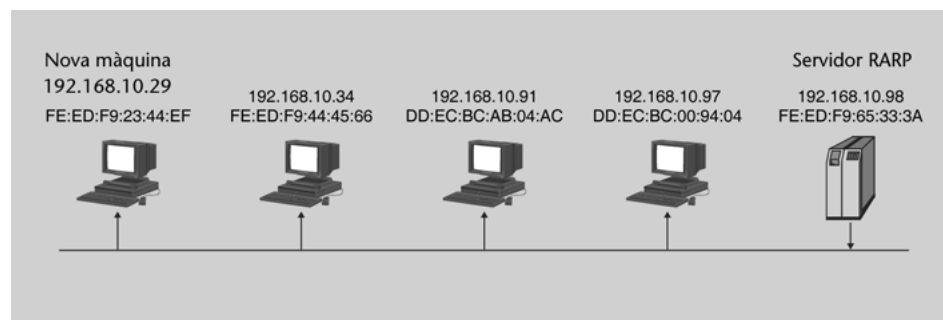
Un cop rebut el missatge RARP, el servidor enviarà un paquet en modalitat de difusió (*broadcast*) amb la informació necessària perquè la nova màquina pugui fer la transmissió corresponent. En aquest cas, el paquet arribarà novament a totes les màquines, que examinaran el paquet rebut, comprovaran que no és per a elles i l'ignoraran.

Com ja hem comentat, totes les màquines ignoraran el paquet excepte la màquina que hem connectat, que entendrà que el missatge és per a ella i se'l quedarà. Un cop la nostra màquina hagi acceptat el paquet enviat pel servidor RARP, l'examinarà i n'extraurà l'adreça IP. De fet, com que la nova màquina ja tindrà la seva pròpia adreça IP, ja podrà començar a transmetre dades (figura 3.3).

El servidor RARP té configurada una llista de parells d'adreça MAC-adreça IP a assignar. D'aquesta manera sempre assigna la mateixa adreça IP a la mateixa màquina.

Servei DHCP

Davant la limitació del nombre d'adreces presents dins una xarxa, i el creixement exponencial que presenta, es va optar per estalviar adreces en ordinadors que es connecten intermitentment. Per fer-ho, es va crear un servei que proporcionés adreces IP que, en el moment de la connexió, estiguessin lliures. Per tant, el servei DHCP es fonamenta en el servidor DHCP que dona adreces (a partir d'un interval d'adreces que té) als ordinadors que es connecten a la xarxa.

FIGURA 3.3. Obtenció d'adreça IP

els protocols BOOTP i DHCP es veuen a l'apartat "Assignació automàtica d'adreces IP: BOOTP i DHCP".

RARP ha deixat d'utilitzar-se. Ha estat substituït per BOOTP i, sobretot, per DHCP, que tenen més prestacions.

3.5 IPX

El protocol d'intercanvi de paquets entre xarxes (IPX, *Internetwork packet exchange*) és un protocol de datagrames ràpid no orientat a connexió que s'encarrega de transmetre dades per la xarxa posant a cada paquet l'adreça de la destinació.

És un protocol de datagrames que s'assembla (tot i que més simple i amb menys fiabilitat) al protocol IP pel que fa a les operacions bàsiques, però diferent quant al sistema d'adreçament, al format de paquets i a l'àmbit general. És un protocol que actualment ja no s'usa i que només es troba en jocs antics per jugar en xarxa.

Datagrama

És un fragment de paquet que s'envia amb prou informació perquè la xarxa pugui encaminar-lo cap a la destinació; no es garanteix que hi arribin tots i tampoc que hi arribin en l'ordre correcte.

3.5.1 Adreçament IPX

L'adreçament IPX utilitza adreces de 32 bits que s'assignen completament sobre una xarxa, en comptes de fer-ho sobre un equip individual. Per identificar cada equip, s'utilitza maquinari específic.

Cada adreça té tres components:

- **Adreça de xarxa**, valor de 32 bits assignat per un administrador i limitat a una xarxa determinada.
- **Número de node**, derivat d'una adreça MAC (48 bits) que s'obté de la targeta de xarxa.
- **Número de sòcol**, valor de 16 bits assignat pel sistema operatiu de xarxa (NetWare) a un procés concret dins d'un node.

Un node dins d'una xarxa es representarà de la manera següent:

Mentre que un procés dins de la xarxa es representarà d'aquesta manera:

1 Número de connexió + número de sòcol

Al model OSI, la gestió del procés i el número de sòcol correspon a la capa de transport.

Al conjunt de protocols TCP/IP, aquesta gestió la fan els protocols TCP i UDP.

Els protocols TCP i UDP es tracten a l'apartat "Protocols de capa de transport i ports".

4. Adreçament IP

L'adreçament IP es fa servir per poder identificar ordinadors i d'altres dispositius. Aquest es basa, per una banda, en la pròpia direcció del equip que l'identifica quan es comunica amb la resta d'equips i la màscara de xarxa que permet saber si un altre equip amb el que ens hem de comunicar està dins de la mateixa xarxa o bé cal fer ús d'algun encaminador per tal de d'establir-hi una comunicació.

En el cas que la direcció amb la qual ens haguem de comunicar no estigui directament connectat al equip, caldrà consultar la taula de rutes. En aquesta taula hi constaran les xarxes per les quals haguem de passar per algun encaminador en concret i finalment una entrada amb el nostre encaminador per defecte.

4.1 Encapçalament IP

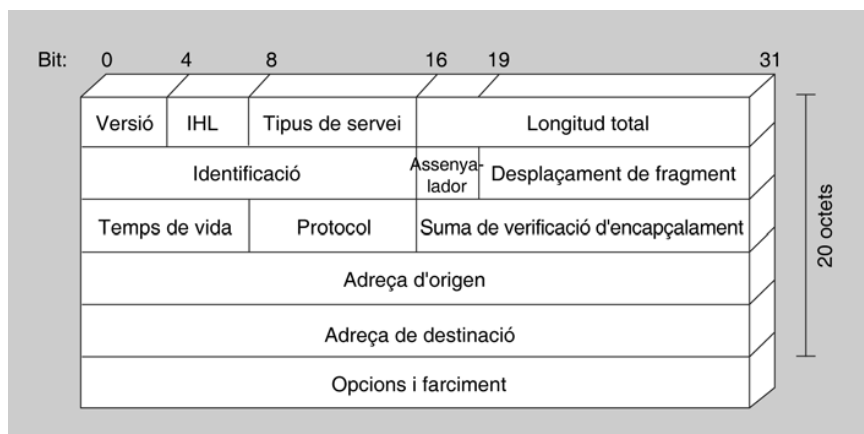
Tota la informació que es vol transmetre s'ha d'empaquetar en *datagrames*, unitats que es transmetran per la xarxa. Perquè arribin a la destinació, cal empaquetar la informació mitjançant el protocol IP, el qual hi afegeix uns camps de control anomenats *encapçalaments* que contenen tota la informació de la màquina d'origen i de destinació.

Un dels camps més importants a l'hora de transmetre la informació per Internet és l'**encapçalament IP**: el protocol hi afegeix una sèrie de dades importants perquè puguin circular per la xarxa i arribar a la destinació.

IPHL: *IP head length*.

Com veiem en la figura 4.1, l'encapçalament IP està format per diferents camps:

FIGURA 4.1. Encapçalament IP

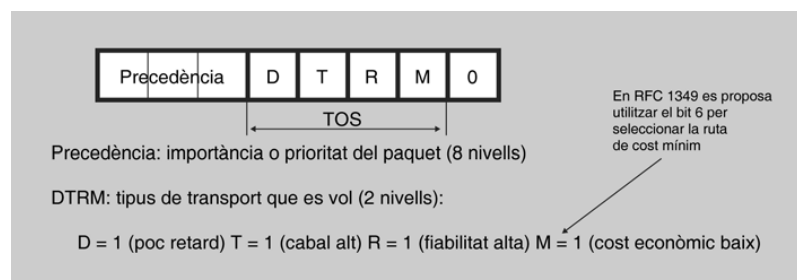


- **Versió:** és un camp de quatre bits que indica la versió del protocol. Per paquets IPv4 es faria servir el valor 4 i de la mateixa manera seria el 6 si el paquet és IPv6.
- **IHL:** indica la longitud de l'encapçalament IP. Serveix per saber en quin punt exacte comencen les dades que es volen transmetre.
- **Tipus de servei** (*type of service*): especifica la qualitat de servei desitjada per aquest paquet, utilitzant 8 bits (figura 4.2).

Significat dels bits

D = 1 Poc retard T = 1 Cabal alt
R = 1 Fiabilitat alta M = 1 Cost
econòmic baix

FIGURA 4.2. Tipus de servei



Els significats dels bits del tipus de servei i un exemple d'ús, els podeu veure a la taula 4.1 i taula 4.2, respectivament.

TAULA 4.1. Significat dels bits del tipus de servei

D	T	R	M	
0	0	0	0	Defecte
0	0	0	1	Minimitzar el cost monetari
0	0	1	0	Maximitzar la fiabilitat
0	1	0	0	Maximitzar el cabal
1	0	0	0	Minimitzar el retard
1	1	1	1	Maximitzar la seguretat

TAULA 4.2. Exemple de l'ús dels bits del tipus de servei

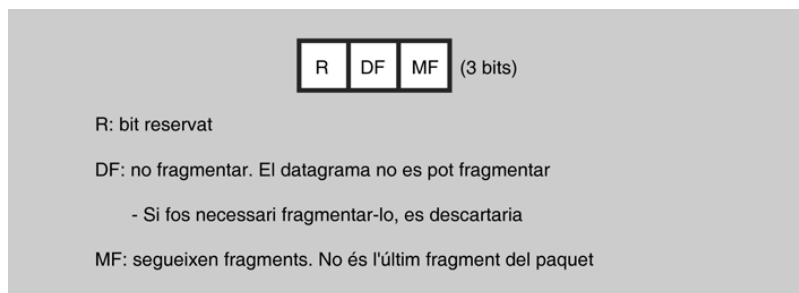
	D	T	R	M
TELNET	1	0	0	0
FTP control	1	0	0	0
FTP dades	0	1	0	0
SNMP	0	0	1	0
NNTP	0	0	0	1

- **Longitud total** (*total length*): especifica la longitud total del paquet incloent-hi les dades i l'encapçalament.
- **Identificació** (*identification*): identifica el número de seqüència del datagra-

ma. En el cas que el paquet es divideixi en fragments més petits per circular per una xarxa que tingui una unitat de transmissió més petita, identifica el número de fragment per tal de reconstruir el paquet original al arribar a la destinació.

- **Assenyalador** (*flags*): és un camp de tres bits (figura 4.3) en què els dos bits de menys pes controlen la fragmentació dels paquets. Un bit identifica si el paquet es pot fragmentar, i l'altre si és l'últim fragment de paquet o no.

FIGURA 4.3. Utilització dels assenyaladors



- **Desplaçament de fragment** (*fragment offset*): Indica la posició que ocupa el fragment actual en el paquet original mitjançant 13 bits.
- **Temps de vida** (*Time To Live*): aquest camp determina el temps de vida del paquet o, dit d'una altra manera, els salts (passos per encaminadors) que pot fer un paquet. Cada vegada que travessa un encaminador, el valor que hi ha en aquest camp es decrementa en una unitat. Aquest camp és necessari perquè no quedin paquets voltant per la xarxa sense trobar la destinació.
- **Protocol**: indica quin protocol de capa superior ha generat el paquet. Els protocols que pot utilitzar són els que es poden veure en la taula 4.3.

TAULA 4.3. Alguns codis dels protocols que pot encapsular el protocol IP

Decimal	Hexadecimal	Protocol	Descripció
1	01	ICMP	Protocol de missatges de control per Internet (<i>Internet control message protocol</i>)
2	02	IGMP	Protocol d'administració del grup Internet (<i>Internet group management protocol</i>)
3	03	GGP	Protocol de passarel·la a passarel·la (<i>gateway-to-gateway protocol</i>)
4	04	IP	Protocol d'Internet
6	06	TCP	Protocol de control de transmissió (<i>transmission control protocol</i>)
8	08	EGP	Protocol de passarel·la exterior (<i>exterior gateway protocol</i>)
.	.	.	.

TAULA 4.3 (continuació)

Decimal	Hexadecimal	Protocol	Descripció
9	09	IGP	Protocol de passarel·la interior (<i>interior gateway protocol</i>)
17	11	UDP	Protocol de datagrama d'usuari (<i>user datagram protocol</i>)
29	1D	ISO-TP4	ISO transport protocol 4
88	58	IGRP	Internet gateway routing protocol (Cisco)
89	59	OSPF	Open shortest path first protocol

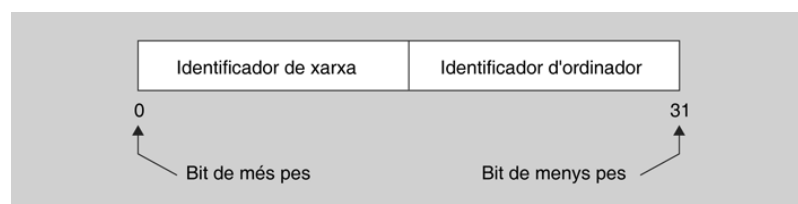
- **Suma de verificació d'encapçalament** (*header checksum*): bits de control per saber si existeix algun error de transmissió en l'encapçalament del paquet IP.
- **Adreça d'origen** (*source address*): especifica l'adreça de la màquina que ha generat el paquet.
- **Adreça de destinació** (*destination address*): especifica l'adreça de la màquina a la qual es volen enviar les dades.
- **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.

Després d'aquest encapçalament es troben les dades que es volen transmetre.

4.2 Classes d'adreça IPv4

L'adreça IP és un nombre de 32 bits que identifica cada una de les màquines que estan connectades a Internet o a qualsevol xarxa, i també la xarxa a la qual estan connectades. Una part de l'adreça IP, segons la seva màscara de xarxa, serveix per identificar la xarxa, sent el tros restant de la direcció IP la que identifica la màquina (figura 4.4).

FIGURA 4.4. IP dividida en xarxa i ordinador



Operació AND

Una operació lògica AND té com a resultat: 0 AND 0 = 0 0
AND 1 = 0 1 AND 0 = 0 1
AND 1 = 1

Per poder separar el camp que identifica la xarxa del camp que identifica la màquina, s'ha d'aplicar una màscara de xarxa. És a dir, al aplicar la operació lògica **AND** entre la màscara de xarxa i l'adreça IP s'obté la xarxa.

La notació de l'adreça IP són quatre xifres menors o iguals a 255 separades per punts. Per poder calcular l'adreça de xarxa caldrà passar les quatre xifres de forma independent a binari. Per exemple l'adreça 192.168.2.23 en binari seria:

1 192.168.2.23 = 11000000.10101000.00000010.00010111

La màscara de xarxa resulta molt més simple ja que sempre seran un conjunt de uns al principi i en algun punt canviaran a zeros:

1 255.255.0.0 = 11111111.11111111.00000000.00000000

Els valors possibles de la màscara de xarxa són els que es mostren a la taula 4.4.

TAULA 4.4. Valors possibles de la màscara de xarxa

Valor en decimal	Valor en binari
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Aplicant l'operació lògica AND, s'obté el següent resultat:

1 11000000.10101000.00000010.00010111 ^ 11111111.11111111.00000000.00000000 =
2 = 11000000.10101000.00000000.00000000

D'aquest resultat s'obté l'adreça de xarxa, en binari 11000000.10101000.00000000.00000000, és a dir, 192.168.0.0 en decimal. Per tant, el valor dels dos últims octets és l'identificador de l'equip.

Depenent de la quantitat de bits que s'utilitzin per identificar la xarxa, es classifica dintre d'un tipus o d'una altra.

Hi ha tres classes principals d'adreces IP:

- **Adreça de classe A:** el primer octet identifica la xarxa.
- **Adreça de classe B:** els dos primers octets identifiquen la xarxa.
- **Adreça de classe C:** els tres primers octets identifiquen la xarxa.

A més de dues classes addicionals que es tracten per separat:

- **Adreça de classe D:** Es tracta d'un conjunt d'adreces reservades per multidifusió.
- **Adreça de classe E:** Es tracta d'una classe reservada.

Una adreça de multidifusió té com a destinataris un subconjunt dels possibles destinataris de la xarxa. *Multidifusió* és el mateix que *multicast* o *difusió selectiva*, que es veu a l'apartat "Adreça de classe D".

4.2.1 Adreça de classe A

En una adreça de classe A el primer octet identifica la xarxa i el bit que pesa més sempre té el valor de 0. Els 7 bits següents identifiquen la xarxa, i la resta de bits —és a dir, 24— identifiquen les màquines connectades. Aquesta combinació fa que la primera xarxa sigui la 0.0.0.0 i l'última, la 127.255.255.255. Amb adreces de classe A es poden implementar poques xarxes, però cada xarxa pot incloure molts equips.

Adreça de classe A

Es poden implementar poques xarxes i molts equips per cada xarxa.

Xarxes < 128

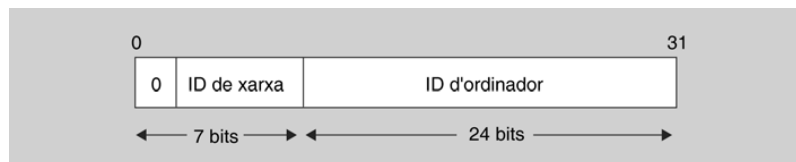
Dispositius > 65.535

Si s'utilitzen 7 bits per identificar les xarxes, podreu obtenir 2^7 xarxes (128 xarxes), a cada una de les quals es poden connectar 2^{24} -2 màquines (concretament, 16.777.214 màquines).

Amb una adreça de classe A, es poden implementar 128 xarxes i connectar-hi uns 16 milions d'ordinadors. Aquesta adreça utilitza el primer octet com a identificador de xarxa i el bit de més pes sempre és 0.

Si teniu l'adreça IP 68.127.23.4 i voleu comprovar de quin tipus d'adreça es tracta, només cal agafar el primer octet, en aquest cas el 68, i fer la conversió a binari (figura 4.5).

FIGURA 4.5. Adreça de classe A

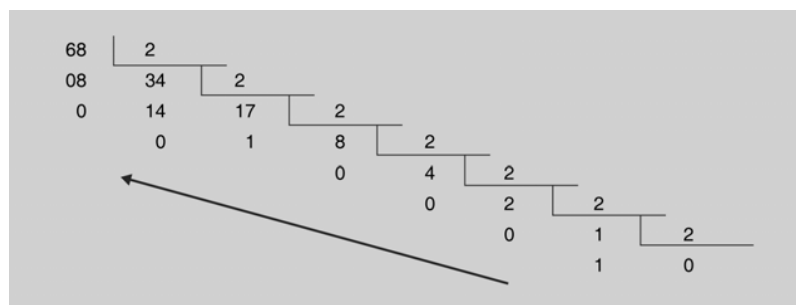


Recordeu

Recordeu que per fer la conversió de decimal a binari cal començar a dividir el nombre entre 2 tantes vegades com faci falta. I que a l'hora de fer la transformació, cal agafar els bits des de l'última divisió fins a la primera: és a dir, l'últim resultat obtingut és el bit de més pes i el primer resultat obtingut és el bit de menys pes.

Després de dividir 68 entre 2 ha quedat un nombre de 7 bits, tal com podeu veure a la figura 4.6. Com que les adreces IP es basen en octets, cal afegir un bit amb valor 0 al bit que pesa més. Per tant, el nombre transformat que queda és el següent: 01000100

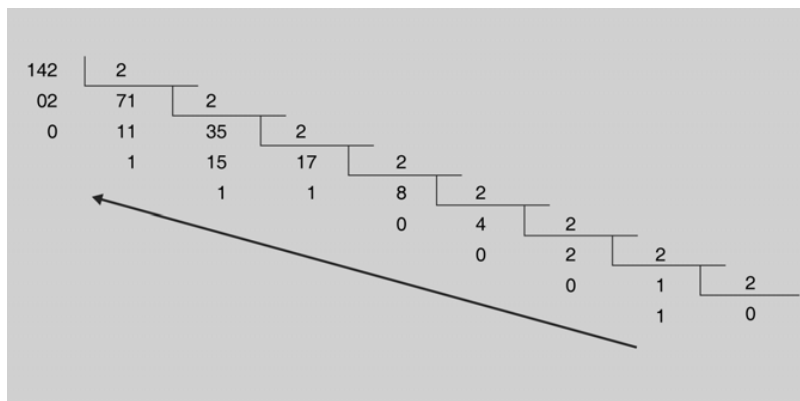
FIGURA 4.6. Transformació a binari del nombre 68



Com podeu comprovar, el bit que pesa més d'aquest octet té un valor de 0, que és precisament el que identifica que es tracta d'una adreça de classe A. Així doncs, la resta d'octets (.127.23.4 en valor decimal) identifiquen dins de la xarxa l'ordinador del qual comprova l'adreça IP.

Suposeu que teniu l'adreça 142.123.23.1 i voleu saber si es tracta d'una adreça de classe A. Heu de seguir el mateix procediment: agafar el primer camp de l'adreça IP i canviar-lo de base de decimal a binari (figura 4.7).

FIGURA 4.7. Transformació a binari del nombre 142



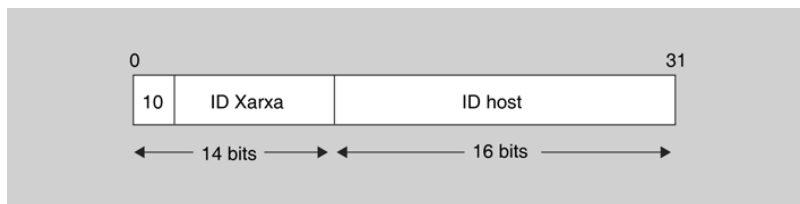
El nombre obtingut és el 10001110. Si observeu el bit que pesa més, comprovareu que té com a valor 1. Com que en les adreces de classe A el bit que pesa més ha de tenir un valor de 0, aquesta adreça no és de classe A.

Per saber de quin tipus d'adreça és aquesta IP, caldrà esperar i continuar llegint. Més endavant, sereu capaços de dir amb total seguretat de quin tipus d'adreça es tracta.

4.2.2 Adreça de classe B

En una adreça de classe B (figura 4.8) els dos primer octets codifiquen les xarxes i del nombre total d'octets els dos que pesen més sempre valen 10. Els 14 bits següents s'utilitzen per identificar les xarxes. En aquest tipus d'adreça es fan servir 16 bits per identificar les màquines connectades. Aquesta combinació fa que la primera xarxa de classe B tingui el valor 128.0.0.0 i l'última adreça de classe B tingui el valor de 191.255.255.255. El fet d'utilitzar adreces de classe B comporta que hi hagi més xarxes que amb una adreça de classe A, però per contra, cada adreça de classe B accepta menys màquines connectades.

FIGURA 4.8. Adreça de classe B



Si s'utilitzen 14 bits per identificar les xarxes, podreu obtenir 2^{14} xarxes, és a dir, 16.384 xarxes. A cadascuna d'aquestes xarxes s'hi poden connectar $2^{16}-2$ màquines, en concret, 65.534 màquines.

Adreça de classe B

Es pot implementar un nombre mitjà de xarxes i un nombre mitjà d'ordinadors a cada xarxa.

Xarxes < 17.000

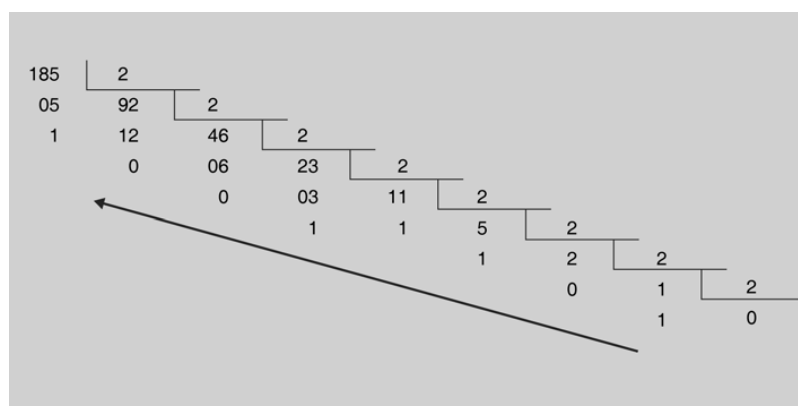
Dispositius < 65.535

Amb una adreça de classe B, es poden implementar 16.384 xarxes i connectar-hi uns 65.000 ordinadors. Aquesta adreça utilitza els dos primers octets com a identificadors de xarxa i els dos bits que pesen més valen sempre 10.

Un exemple d'adreça de classe B podria ser la IP 185.23.145.233. Si no esteu segurs que sigui una adreça de classe B, només cal que seguiu els mateixos passos que abans (figura 4.9): agafeu el primer camp i comenceu la transformació a binari.

El resultat de la transformació de decimal a binari és 10111001. Com en el cas de l'adreça de classe A, heu de buscar el bit que pesa més. Atès que en aquest cas és l'1, heu de buscar també el segon bit que pesa més, que com podeu comprovar, a la figura 4.9, és el 0. És a dir, aquesta adreça comença per 10. Si repasseu les característiques de les adreces de classe B, comprovareu que comencen amb els dos bits que pesen més i tenen un valor de 10.

FIGURA 4.9. Transformació a binari del nombre 185



Podeu concloure que es tracta d'una adreça de classe B, que l'adreça de xarxa és 185.23 i que la resta de nombres corresponen a la numeració de l'ordinador del qual comprova l'adreça IP.

Seguint l'exemple de l'adreça de classe A

Podeu comprovar si l'adreça anterior, aquella que no és de classe A, correspon a una adreça de classe B. Només cal que recordeu de quina adreça es tractava.

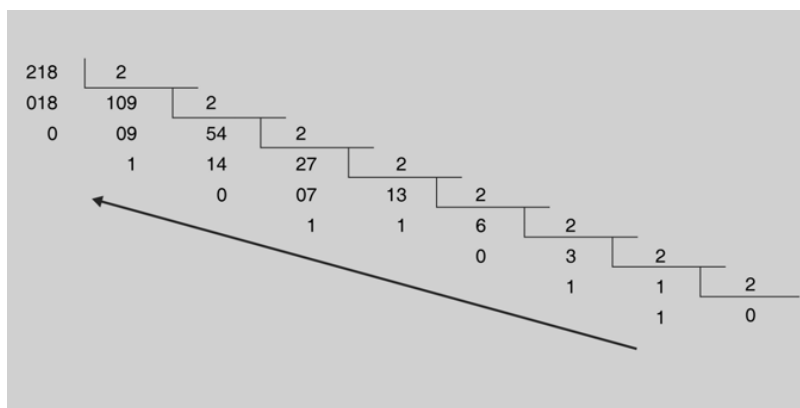
L'adreça era 142.123.23.1 i havíeu arribat a la conclusió que no es tractava d'una adreça de classe A. Recordeu que el valor del primer octet de l'adreça en format binari era: 10001110.

Si comproveu els dos bits que pesen més -ja que no es tractava d'una adreça de classe A-, comprovareu que el seu valor és 10. Aquesta dada s'ajusta a les característiques que havia de complir una adreça de classe B.

Un altre exemple

Comproveu una altra adreça per veure el vostre domini en aquestes tasques. L'adreça que us proposem és la següent: IP 218.12.12.12

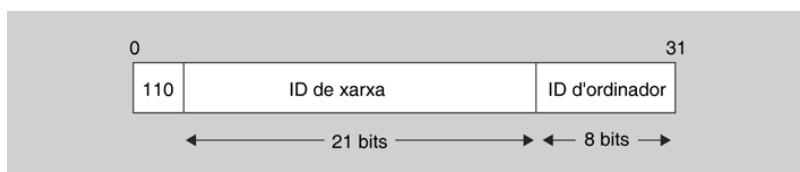
La comprovació sempre segueix els mateixos passos; primer heu de fer la transformació (figura 4.10):

FIGURA 4.10. Transformació a binari del nombre 218

Un cop teniu el nombre en binari -en aquest cas, el 11011010-, heu de comprovar quins són els bits que pesen més: com podeu veure, el bit que pesa més és l'1, però el segon no és el 0 i, en conseqüència, aquesta adreça IP no és de classe B. De quina classe és? Segur que ho descobrireu més endavant.

4.2.3 Adreça de classe C

En una adreça de classe C (figura 4.11) s'utilitzen els tres primers octets per identificar les xarxes i es dedica l'últim a la identificació d'ordinador. Els tres bits que pesen més de l'identificador de xarxa sempre tindran per valor 110: la primera xarxa de classe C que es pot implementar tindrà l'adreça IP 192.0.0.0 i l'última serà la 223.255.255.255. Aquest valor indica que es poden implementar moltes xarxes a les adreces de classe C, però també que es poden connectar poques màquines a cada xarxa.

FIGURA 4.11. Adreça de classe C

Si s'utilitzen 21 bits per identificar les xarxes, podreu obtenir 2^{21} xarxes, és a dir, 2.097.152 xarxes. A cada una d'aquestes xarxes s'hi poden connectar 2^8-2 màquines, és a dir, 254.

Adreça de classe C

Es poden implementar moltes xarxes i molt pocs ordinadors a cada xarxa.

Xarxes > 17.000

Dispositius < 256

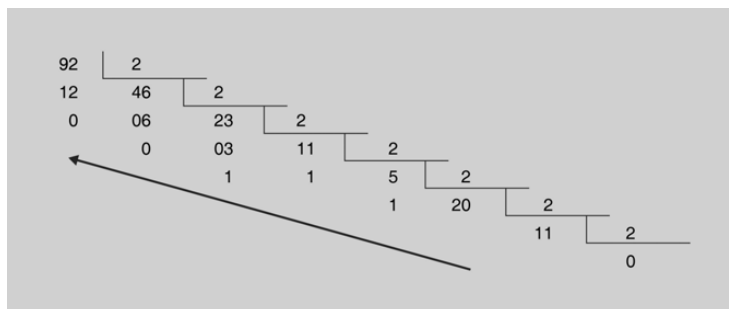
Amb una adreça de classe C, es poden implementar uns dos milions de xarxes i connectar-hi uns 256 ordinadors. Aquesta adreça emprà els tres primers octets com a identificadors de xarxa i els tres bits que pesen sempre són 110.

Exemples

Com en els casos anteriors, en aquest també es posaran exemples d'adreces de classe C, com la següent: 92.3.23.54.

Per comprovar si es tracta realment d'una adreça de classe C, els passos que heu de seguir són els mateixos que en els casos anteriors: transformar el primer camp de l'adreça IP a binari (veure figura 4.12).

FIGURA 4.12. Transformació a binari del nombre 92



El resultat obtingut de la transformació és 1011100. Com podeu comprovar, només són 7 bits i, per tant, heu afegir un 0 a la posició que pesa més i així tindreu el nombre 01011100. Per comprovar si es tracta d'una adreça de classe C, heu de mirar el bit que pesa més.

Després de comprovar que aquest bit és el 0 i de repassar les característiques de les adreces IP, veieu que una adreça de classe C sempre comença amb la combinació de bits 110. No és el cas de l'adreça IP que heu transformat, ja que comença per 0, i per tant, no és una adreça de classe C.

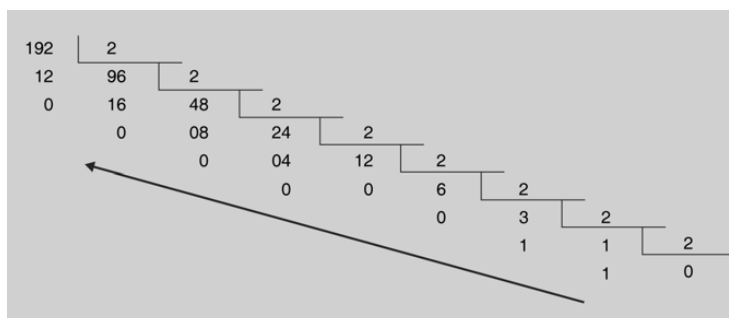
De quin tipus és, doncs? Si comproveu les característiques de les adreces IP vistes fins ara, comprovareu que les de classe A començaven amb un 0: per tant, aquesta adreça IP no és de classe C, sinó que és de classe A.

Comproveu l'adreça IP 192.3.23.54. Amb el que heu après, podeu indicar també quina és la part de l'adreça IP que identifica la xarxa i quina part identifica els ordinadors.

Per saber quina part de l'adreça IP identifica la xarxa, el primer que cal esbrinar és el tipus d'adreça. Coneixent el tipus, podreu dir sense por d'equivocar-vos quina part de l'adreça IP identifica la xarxa.

Per començar, doncs, cal fer la transformació de decimal a binari (figura 4.13), ja que aquesta és la manera més senzilla d'identificar el tipus d'adreça.

FIGURA 4.13. Transformació a binari del nombre 192



El primer camp de l'adreça IP en binari té el valor de 11000000 i, com podeu comprovar, l'inici de l'adreça IP en format binari és 110. Si consulteu les característiques dels diferents tipus d'adreces IP, veureu que les de classe A comencen per 0, les de classe B comencen per 10 i les de classe C, per 110; per tant, la que ens ocupa és una adreça de classe C.

Comproveu ara quina part de l'adreça IP determina la xarxa i quina part determina l'identificador d'ordinador.

Si consulteu les característiques de l'adreça de classe C, podeu comprovar que els 21 bits

que segueixen els tres primers identifiquen la xarxa i els últims 8 bits, l'ordinador. Per tant, a l'adreça teniu: Identificador de xarxa Identificador de l'estació de treball

En format binari seria de la manera següent: Identificador de xarxa Identificador de l'estació de treball. L'identificador de la xarxa és 192.3.23 i l'identificador de l'ordinador és .5.

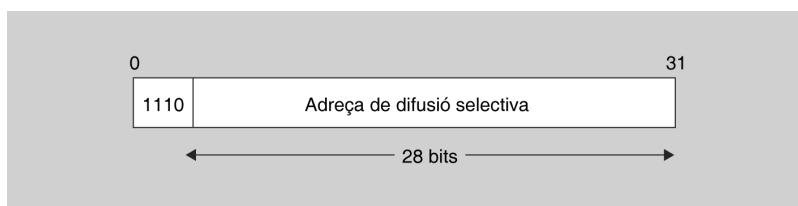
4.2.4 Adreça de classe D

L'adreça de classe D (figura 4.14) es va crear per permetre difusió selectiva o *multicast* en una adreça IP. Una **adreça de difusió selectiva** és una adreça exclusiva de xarxa que dirigeix els paquets amb aquesta direcció de destinació cap a grups predefinitos d'adreces IP. Per tant, una sola estació pot transmetre simultàniament un sol corrent de dades a múltiples receptors.

Multicast és una forma de transmissió.

L'adreça de classe D es pot diferenciar de les altres gràcies als quatre bits de més pes, que en una adreça d'aquesta classe valen sempre 1110 i, per tant, són adreces de xarxa que comencen en el nombre 224.0.0.0 i acaben en el nombre 239.255.255.255. Aquesta adreça utilitza els 28 bits restants com a adreça de difusió selectiva.

FIGURA 4.14. Adreça de classe D



Les adreces de classe D estan reservades per a adreces de difusió selectiva.

L'adreça de classe D no té cap octet dedicat a la xarxa ni cap de dedicat a l'identificador d'ordinador perquè és una adreça de difusió selectiva. S'ha de tenir en compte que es pot diferenciar una adreça de classe D de les altres mitjançant els quatre primers bits, que sempre tindran el valor de 1110.

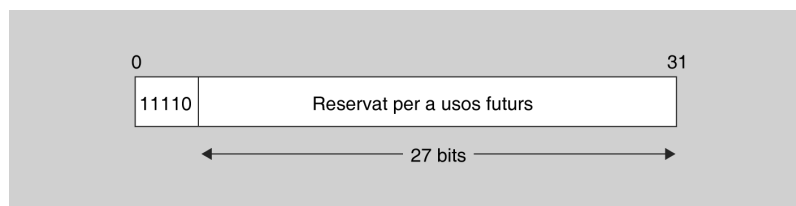
4.2.5 Adreça de classe E

Les adreces de classe E (figura 4.15) són adreces IP que s'han reservat per a usos futurs. Normalment l'IEFF (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.

De totes maneres, s'identificarà una adreça de classe E de la mateixa manera que s'identifiquen les altres: per mitjà dels bits que pesen més. En el cas de l'adreça de classe E, els cinc primers bits que pesen més tenen un valor fix: 11110. Tenint en compte que aquests bits no poden variar les adreces IP de classe E, van de

l'adreça 240.0.0.0 fins a l'adreça 247.255.255.255, i els 27 bits restants estan reservats.

FIGURA 4.15. Adreça de classe E



Les adreces de classe E estan reservades per a usos futurs i de moment només les fa servir l'IEFT per investigar. Els cinc bits que pesen més tenen el valor de 11110.

No és difícil adonar-se que una manera ràpida de conèixer la classe d'una adreça a partir de la seva notació decimal és mirar el primer octet i:

- Si es troba entre 0 i 127, és de classe A
- Si es troba entre 128 i 191, és de classe B
- Si es troba entre 192 i 223, és de classe C
- Si es troba entre 224 i 239, és de classe D
- Si es troba entre 240 i 247, és de classe E

4.2.6 CIDR (encaminament sense classe)

{Adreça IP} / {nombre de bits "1" en la màscara de subxarxa}

Amb la ràpida expansió d'Internet va quedar clar que l'encaminament basat en classes no era suficient, és per això que l'any 1993 es va proposar la CIDR (*classless inter-domain routing*) que vol dir encaminament entre dominis sense classe. Gràcies a aquest sistema es millora el mètode amb el que s'interpreten les adreces IP a més de com s'encaminen els paquets.

En lloc de parlar de classes es fa servir el nombre de bits a 1 de la màscara de xarxa per tal d'indicar la xarxa. Les classes A, B i C tindrien una màscara de xarxa amb 8, 16 i 24 bits a 1 respectivament. Per exemple, per tal de definir la xarxa que va del 192.168.0.0 a la 192.168.255.255 (seria una classe B) indiquem la IP i amb un barra els 16 bits a 1 de la màscara de xarxa. Per tant la notació seria: 192.168.0.0/16

Per poder fer ús de CIDR, els encaminadors de la xarxa han de ser capaços d'interpretar adreces IP que no pertanyen a cap de les classes convencionals (A, B o C). Per aquest motiu, els encaminadors que fan ús de protocols antics d'encaminament, com ara RIPv1 (la primera versió de RIP), no donen suport a CIDR. Cal dir que **RIPv2** —és a dir, la segona versió de RIP— sí que **suporta CIDR**.

4.2.7 Espai d'adreces reservades

Hi ha certs conjunts d'IP que estan reservats per usos especials:

- Quan l'identificador d'equip és 0, es fa referència a la xarxa a la qual està connectat.
- Quan l'identificador d'equip són tot 1 vol dir totes les màquines; això seria una adreça de difusió (*broadcast*).
- Quan tota l'adreça són 0 indica totes les IPs de la màquina.
- Adreça de *loopback*. La xarxa 127.0.0.0/8 indica que el paquet es que a la mateixa màquina i retorna internament, es refereix sempre al equip local.
- Adreces privades. Són adreces que només es poden utilitzar dins d'una organització privada no encaminables. Els blocs d'adreces privades són els següents:
 - 10.0.0.0/8: és una classe A que permet 2^{24} hosts a la xarxa. Per la grandària que té se sol dividir en subxarxes.
 - 172.16.0.0/12: és una xarxa que admet fins a 2^{20} equips connectats a la xarxa
 - 192.168.0.0/16: és una classe C que permet fins a 2^{16} equips. Encara que sigui la més petita de les tres és la més comuna.

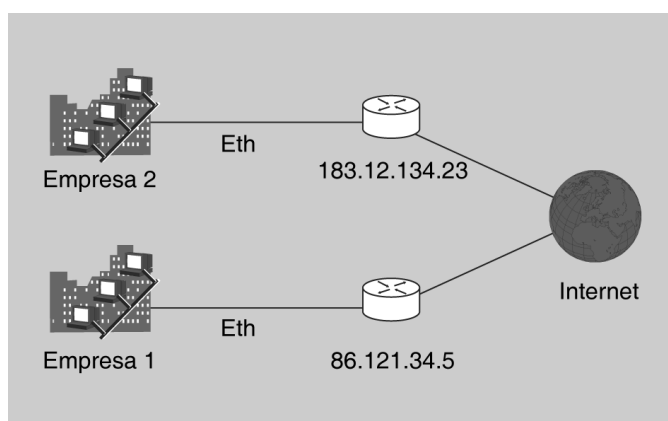
Gràcies a això, en diferents xarxes privades es poden repetir les mateixes adreces IP, sense que entrin en conflicte, ja que l'una no té visibilitat de l'altra.

Per tal de tenir accés a Internet caldrà, doncs, fer ús de NAT per traduir les IP internes a una IP pública perquè des de l'altre extrem sembli que la IP és pública.

Exemple d'espai d'adreces reservades

En la figura 4.16 podeu veure que hi ha dues empreses connectades a Internet per mitjà d'un servidor connectat a l'encaminador de sortida.

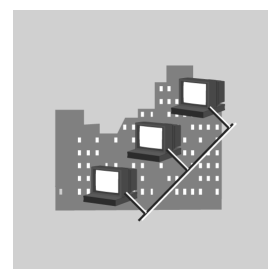
FIGURA 4.16. Xarxes privades



L'adreça 127.0.0.1 es refereix a la màquina mateixa.

Divisió en xarxes més petites

La utilització de les adreces privades permet la creació de xarxes empresarials que es poden dividir per formar xarxes més petites que són més fàcils de manipular i controlar.



Xarxa d'una empresa

Les dues empreses tenen adreces IP de sortida a Internet diferents, tal com podeu apreciar, però en canvi, a les xarxes internes poden utilitzar les mateixes adreces IP. Quan un empleat de l'empresa 1 envia un paquet a Internet té l'adreça IP de l'emissor: IP 86.121.34.5-, que és l'adreça IP amb què aquesta empresa surt a Internet.

4.2.8 Esgotament de les adreces IPv4

Totes les classes d'adreces vistes fins ara són adreces vàlides per navegar per Internet, però s'ha de tenir en compte que hi ha un grup d'adreces que tenen un valor especial perquè són adreces dedicades a usos especials o, dit amb altres paraules, són adreces reservades.

Les adreces IP de classe A, B, C, D i E utilitzen el protocol IPv4. Aquest protocol fa servir 32 bits per codificar cada adreça IP, cosa que significa que només hi pot haver uns quatre mil milions d'ordinadors connectats a Internet a tot el món suposant que s'empressin totes les adreces. Com ja hem dit, hi ha moltes adreces reservades i, per tant, a la pràctica aquesta quantitat es redueix exponencialment.

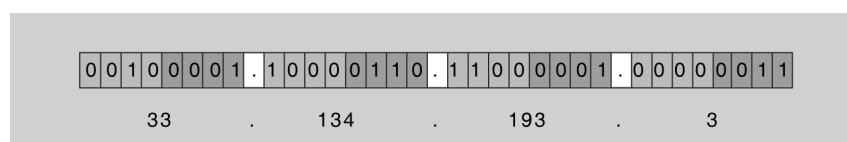
La realitat és que les adreces IP es van esgotant a mesura que el nombre de màquines connectades a Internet creix a un ritme exponencial: cada dia hi ha més gent que es vol connectar a Internet que abans no s'hi connectava. Això fa que les adreces IP actuals siguin insuficients per atendre totes les peticions.

Per solucionar aquest problema, apareix el protocol IPv6, que té l'avantatge que utilitza 128 bits per codificar les adreces IP. A diferència del protocol IPv4 -que escriu l'adreça en blocs de vuit bits separats per punts o en format decimal-, el protocol IPv6 l'escriu en blocs de 16 bits separats per dos punts o en format hexadecimal.

Adreça IPv4

Descompon els 32 bits de la figura 4.17 en blocs de vuit bits separats per punts i en format decimal.

FIGURA 4.17. Adreça IPv4

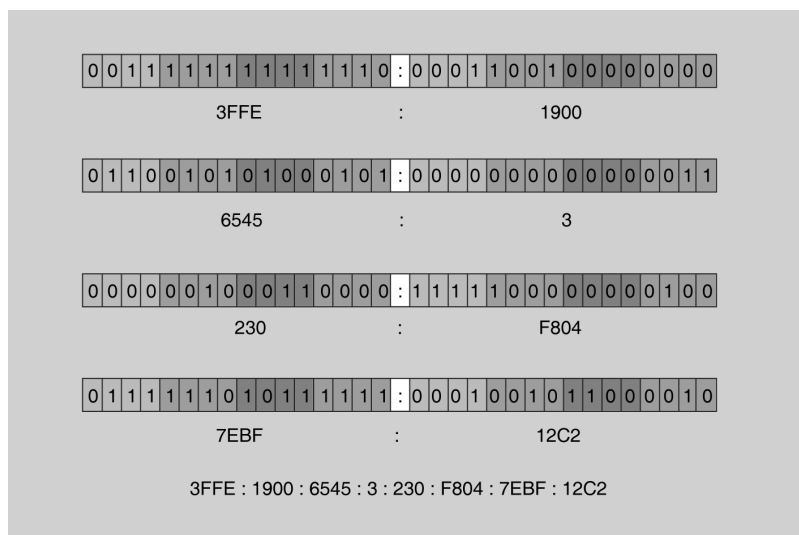


Format decimal 33.134.193.3

Format binari 00100001.10000110.11000001.00000011

Adreça IPv6

Descompon els 128 bits de la figura 4.18 en grups de 16 bits separats per dos punts o en format hexadecimal.

FIGURA 4.18. Adreça IPv6

Format hexadecimal 3FFE:1900:6545:3:230:F804:7EBF:12C2

Format binari 0011111111111100 : 0001100100000000 : 0110010101000101
 : 0000000000000011 : 000001000110000 : 1111100000000100 :
 011111010111111 : 0001001011000010

Recordatori

Per passar d'hexadecimal a binari, cada dígit hexadecimal es substitueix per 4 bits amb la seva representació binària (zeros a l'esquerra inclosos) tenint en compte que A equival a 10, B equival a 11, C equival a 12, D equival a 13, E equival a 14 i F equival a 15.

4.3 Creació de subxarxes o subneeting

La **creació de subxarxes** o *subnetting* consisteix a dividir una xarxa gran en múltiples segments de xarxa o subxarxes. És habitual dividir xarxes en subxarxes segons criteris d'ubicació geogràfica (per exemple, pisos d'un edifici connectats per una LAN o diferents edificis connectats per una WAN), criteris departamentals (per exemple, una subxarxa per al departament de màrqueting, una altra per al de comptabilitat, etc.), criteris tecnològics (per exemple, Ethernet, anell de testimoni, etc.) o per funcionalitat dels servidors (servidor d'aplicacions, servidor de bases de dades, servidor de còpies de seguretat).

La creació de subxarxes permet aïllar el trànsit de cada xarxa, la qual cosa té els avantatges següents:

- **Millora la seguretat i el rendiment global.** Les subxarxes s'han de connectar entre si mitjançant encaminadors o altres dispositius de la capa de xarxa. En la seva configuració habitual, aquests dispositius no deixen passar enviaments en difusió, la qual cosa permet un millor ús dels mitjans

de transmissió i un control més fàcil dels paquets que circulen per la xarxa (en filtrar tots els paquets que no van destinats a la mateixa xarxa).

- **Simplifica la resolució de problemes.** En tenir la xarxa segmentada en petites subxarxes, resulta més fàcil identificar l'origen de possibles problemes de comunicació, que, d'altra banda, només afecten un segment concret i no tota la xarxa.

4.3.1 Màscara de subxarxa: part de xarxa i part de host

La màscara de subxarxa indica quina part de l'adreça IP identifica la xarxa i quina part identifica el *host*. En concret, quan es considera una adreça IP en binari i la corresponent màscara de xarxa en binari, la part de l'adreça IP que identifica a la xarxa és la que correspon a la part de valors 1 en la màscara de subxarxa associada, mentre que la part de l'adreça IP que identifica el *host* és la que correspon a la part de valors 0 en la màscara de xarxa associada.

La taula 4.5 mostra un exemple de com la màscara de subxarxa permet determinar la part de l'adreça IP que correspon a la xarxa i la part que correspon al *host*. En l'exemple, es té que l'adreça IP inicial, 199.34.89.123 fa referència al *host* de la xarxa que té 199.34.89.0 per adreça IP.

TAULA 4.5. Exemple d'ús d'una màscara de subxarxa estàndard

	Binari	Decimal
Adreça IP de host	11000111 00100010 01011001 01111011	199.34.89.123
Màscara de subxarxa	11111111 11111111 11111111 00000000	255.255.255.0
Part de xarxa	11000111 00100010 01011001	199.34.89.
Part del host	01111011	.123
Adreça IP de xarxa	11000111 00100010 01011001 00000000	199.34.89.0
Adreça IP de difusió	11000111 00100010 01011001 11111111	199.34.89.255
Rang d'adreces IP assignables a hosts en aquesta xarxa	11000111 00100010 01011001 00000001 fins a 11000111 00100010 01011001 11111110	199.34.89.1 fins a 199.34.89.254

En l'exemple anterior s'ha fet servir la màscara de xarxa predeterminada per a una adreça IP de classe C (255.255.255.0), però el mateix seria vàlid si es fes ús d'una màscara de subxarxa no estàndard, tal com mostra la taula 4.6. En aquest cas, en què la màscara de subxarxa conté dos bits 1 més que els corresponents a una màscara de xarxa de classe C (és a dir, s'han agafat dos bits més per a identificar la part de l'adreça IP que correspon a la xarxa), l'adreça IP inicial 199.34.89.123 fa referència al *host* 59 de la xarxa que té per adreça IP 199.34.89.64.

TAULA 4.6. Exemple d'ús d'una màscara de subxarxa no estàndard

	Binari	Decimal
Adreça IP de host	11000111 00100010 01011001 01111011	199.34.89.123
Màscara de subxarxa	11111111 11111111 11111111 11000000	255.255.255.192
Part de xarxa	11000111 00100010 01011001	199.34.89.64
Part del host	01111011	.59
Adreça IP de xarxa	11000111 00100010 01011001 01000000	199.34.89.64
Adreça IP de difusió	11000111 00100010 01011001 01111111	199.34.89.127
Rang d'adreces IP assignables a hosts en aquesta xarxa	11000111 00100010 01011001 01000001 fins a 11000111 00100010 01011001 01111110	199.34.89.65 fins a 199.34.89.126

4.3.2 Manipulació de la màscara de subxarxa

El procés de creació de subxarxes (*subnetting*) es fa manipulant les màscares de subxarxa de manera que tinguin més bits 1 per designar la part de l'adreça IP que correspon a la xarxa. En tenir més bits disponibles a la part de xarxa, es poden assignar més adreces IP de xarxa.

Evidentment, com més bits s'agafin per formar la part de xarxa, menys bits quedaran per a la part del *host*, amb la qual cosa el nombre d'adreces IP disponibles per a *hosts* disminuirà. El nombre mínim de bits que es poden prendre de la part de *host* per assignar-los a la part de xarxa és de 2. D'altra banda, la part de *host* ha de tenir sempre un mínim de 2 bits assignats.

La taula 4.7 mostra el nombre de subxarxes (i el nombre de *hosts* per xarxa) que es poden crear manipulant la màscara de xarxa d'una adreça IP de classe B. Cal recordar que, de manera predeterminada, una adreça IP de classe B reserva 16 bits per a la part de *host* (màscara de subxarxa 255.255.0.0), per la qual cosa defineix una única xarxa amb $2^{16}-2 = 65.534$ nodes.

Agafar bits "en préstec"

Se sol fer ús de l'expressió *agafar bits en préstec* de la màscara de subxarxa per indicar que es dediquen a la part de *xarxa* bits que inicialment estaven dedicats a la part de *host*.

El nombre d'equips que caben en una xarxa són determinats per 2^N bits destinats als equips menys dues IP:

- La IP amb tots els bits que identifica l'equip estan a zero es fa servir per identificar la xarxa. Es pot configurar l'encaminador perquè sigui utilitzable, però és preferible no fer-ho.
- La IP amb tots els bits a 1 es fa servir per difusió.

TAULA 4.7. Creació de subxarxes a partir d'una adreça IP de classe B

Màscara de subxarxa (binari)	Màscara de subxarxa (decimal)	Nombre de subxarxes	Nombre de nodes per subxarxa
11111111 11111111 11000000 00000000	255.255.192.0	$2^2 = 4$	$2^{14} - 2 = 16.382$
11111111 11111111 11100000 00000000	255.255.224.0	$2^3 = 8$	$2^{13} - 2 = 8.190$
11111111 11111111 11110000 00000000	255.255.240.0	$2^4 = 16$	$2^{12} - 2 = 4.094$
11111111 11111111 11111000 00000000	255.255.248.0	$2^5 = 32$	$2^{11} - 2 = 2.046$
11111111 11111111 11111100 00000000	255.255.252.0	$2^6 = 64$	$2^{10} - 2 = 1.022$
11111111 11111111 11111110 00000000	255.255.254.0	$2^7 = 128$	$2^9 - 2 = 510$
11111111 11111111 11111111 00000000	255.255.255.0	$2^8 = 256$	$2^8 - 2 = 254$
11111111 11111111 11111111 10000000	255.255.255.128	$2^9 = 512$	$2^7 - 2 = 126$
11111111 11111111 11111111 11000000	255.255.255.192	$2^{10} = 1.024$	$2^6 - 2 = 62$
11111111 11111111 11111111 11100000	255.255.255.224	$2^{11} = 2.048$	$2^5 - 2 = 30$
11111111 11111111 11111111 11110000	255.255.255.240	$2^{12} = 4.096$	$2^4 - 2 = 14$
11111111 11111111 11111111 11111000	255.255.255.248	$2^{13} = 8.192$	$2^3 - 2 = 6$
11111111 11111111 11111111 11111100	255.255.255.252	$2^{14} = 16.384$	$2^2 - 2 = 2$

4.3.3 Exemple de creació de subxarxes

Es vol segmentar una xarxa de classe C amb IP 199.34.89.0 en sis subxarxes (una per cada departament de la institució o empresa on està instal·lada la xarxa).

Nombre de subxarxes

Per calcular el nombre de subxarxes (n) que es poden formar amb m bits ($m > 1$), s'aplica la fórmula següent: $n = 2^m$ on 2^m és el nombre d'adreces possibles que es poden formar amb m bits. En alguns dispositius antics (avui en dia molt pocs), a aquesta quantitat cal restar-hi 2, ja que no poden utilitzar les adreces de xarxa i difusió.

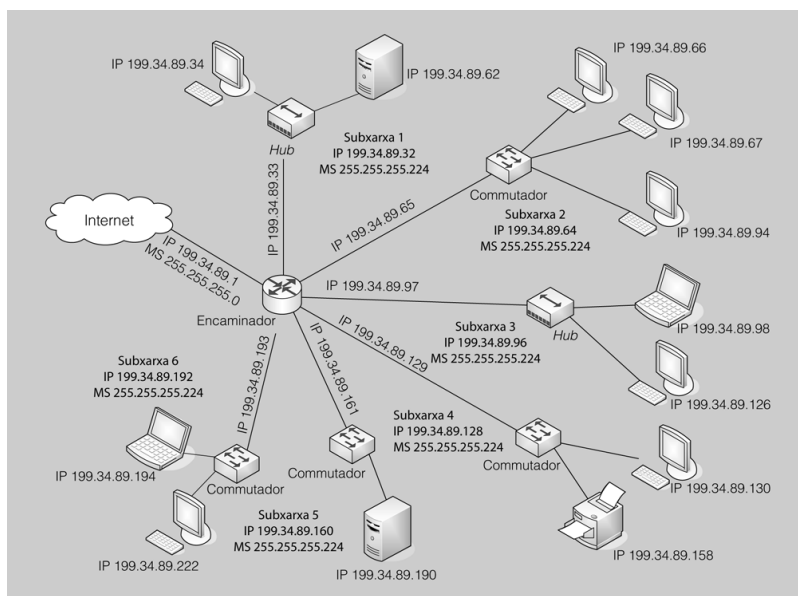
Una manera de fer-ho seria la següent: atès que es necessitaran sis subxarxes, caldrà “agafar en préstec” 3 bits de la part de *host* de la IP anterior i passar-los a la part de xarxa (ens cal agafar un mínim de 3 bits, ja que $2^3 = 8$ (i $8 \geq 6$)). Això vol dir que la nova màscara de subxarxa serà 11111111 11111111 11111111 11100000, és a dir, 255.255.255.224.

D'altra banda, com que només quedaran 5 bits disponibles per a la part de *host*, cadascuna de les sis subxarxes podrà tenir un màxim de $2^5 - 2 = 30$ nodes (és a dir, hi haurà 30 adreces IP disponibles per a *hosts* entre l'adreça IP de cada subxarxa i l'adreça IP de difusió de cada subxarxa). La taula 4.8 mostra la informació associada al procés de creació de subxarxes així com a cadascuna de les sis subxarxes creades.

TAULA 4.8. Creació de sis subxarxes a partir d'una xarxa de classe C

	Binari	Decimal
Adreça IP xarxa inicial	11000111 00100010 01011001 00000000	199.34.89.0
Màscara de subxarxa inicial	11111111 11111111 11111111 00000000	255.255.255.0
Nova màscara de subxarxa	11111111 11111111 11111111 11100000	255.255.255.224
Subxarxa 1: adreça IP de subxarxa	11000111 00100010 01011001 00100000	199.34.89.32
Subxarxa 1: adreça IP de difusió	11000111 00100010 01011001 00111111	199.34.89.63
Subxarxa 2: adreça IP de subxarxa	11000111 00100010 01011001 01000000	199.34.89.64
Subxarxa 2: adreça IP de difusió	11000111 00100010 01011001 01011111	199.34.89.95
Subxarxa 3: adreça IP de subxarxa	11000111 00100010 01011001 01100000	199.34.89.96
Subxarxa 3: adreça IP de difusió	11000111 00100010 01011001 01111111	199.34.89.127
Subxarxa 4: adreça IP de subxarxa	11000111 00100010 01011001 10000000	199.34.89.128
Subxarxa 4: adreça IP de difusió	11000111 00100010 01011001 10011111	199.34.89.159
Subxarxa 5: adreça IP de subxarxa	11000111 00100010 01011001 10100000	199.34.89.160
Subxarxa 5: adreça IP de difusió	11000111 00100010 01011001 10111111	199.34.89.191
Subxarxa 6: adreça IP de subxarxa	11000111 00100010 01011001 11000000	199.34.89.192
Subxarxa 6: adreça IP de difusió	11000111 00100010 01011001 11011111	199.34.89.223

La figura 4.19 mostra un esquema que il·lustra el resultat del procés de creació de subxarxes descrit.

FIGURA 4.19. Exemple de creació de subxarxes

Alguns llocs web proporcionen informació i eines per automatitzar els càlculs per la creació de subxarxes. Cercant a Internet per termes com ara *network calculator* o *subnet calculator*.

L'encaminador central connecta els diferents segments de xarxa mitjançant les seves interfícies (una per cada segment o subxarxa), cadascuna de les quals té la seva pròpia adreça IP. Així, per exemple, quan el *host* 199.34.89.34 vol enviar dades al *host* 199.34.89.126, l'encaminador utilitza l'adreça IP de destinació i de la màscara de subxarxa 255.255.255.224 per determinar l'adreça IP de la

subxarxa de destinació i el *host* corresponent. Per contra, quan un encaminador situat a Internet intenta enviar dades al *host* 192.34.89.126, només ha de saber l'adreça IP pública de l'encaminador de la xarxa, que és 192.34.89.1 amb màscara de subxarxa 255.255.255.0 (és a dir, no fa ús de la màscara de subxarxa manipulada). És l'encaminador de la xarxa qui s'encarrega d'aplicar la màscara de subxarxa 255.255.255.224 per enviar les dades al node destinatari.

4.4 Adreçament públic i privat: NAT

Una de les tècniques per afrontar l'esgotament de les adreces IPv4 és el NAT (*network address translation*), però té un ús que va més enllà, ja que mitjançant NAT podem fer que xarxes amb direccionament en conflicte pugui establir una comunicació.

1. El NAT bàsic

El NAT més simple només té en compte la IP d'origen, que sempre es tradueix en una altra IP (NAT estàtic) o conjunt d'IP (NAT dinàmic) d'una altra xarxa. En aquest cas, els ports TCP (protocol de transport) no es tenen en compte i, per tant, el NAT bàsic només opera a la capa de xarxa.

2. El PAT

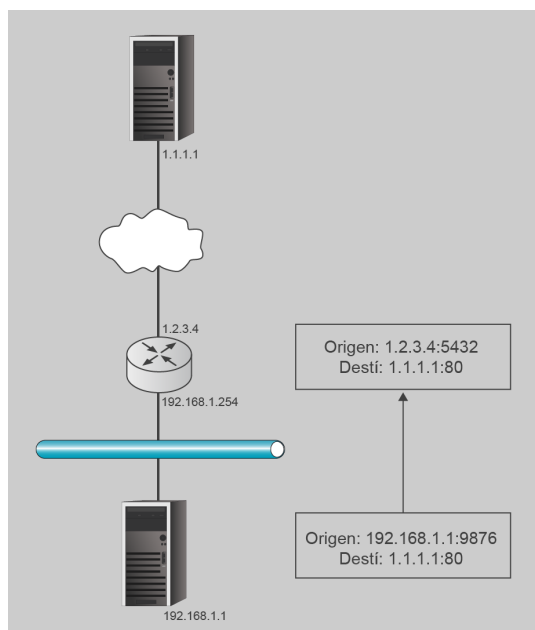
El PAT és el tipus més usat de NAT: no solament actua en la capa de xarxa, sinó també en la capa de transport traduint els ports TCP i UDP. Mitjançant aquesta tècnica, podem tenir un conjunt de màquines en una xarxa privada que surten a Internet amb una mateixa adreça IP, però amb un port diferent.

Cada paquet TCP i UDP conté tant l'adreça IP de l'equip d'origen com la del receptor, a més del port d'origen i del port de destinació. En el cas de l'extrem públic, és important mantenir el port de destinació, ja que els serveis escolten un port concret; per exemple, un servidor web normalment escolta el port 80 i, per tant, en el costat de la xarxa a la qual s'accedeix no es pot modificar el port, però el port d'origen no ha de ser necessàriament un port fix, sinó que pot variar.

Per tant, el dispositiu encarregat de fer el PAT ha de mantenir una taula amb el port que es fa servir per a la connexió en l'extrem de la xarxa a la qual es vol connectar i relacionar-lo amb la connexió que s'origina en la xarxa que emmascaren, i resoldre els possibles conflictes de ports que s'originin en la xarxa.

Per exemple, tal com podeu veure en la figura 4.20, suposem que la màquina 192.168.1.1 vol establir una connexió amb la IP pública 1.1.1.1 pel port 80. Aquest ordinador amfitrió triarà un port aleatori per establir-la; per exemple, el 9876. El dispositiu PAT escollirà un altre port; per exemple, el 5432, i enviarà un paquet amb la seva IP pública (1.2.3.4) al port de destinació 1.1.1.1:80. Quan al dispositiu PAT hi arriba un paquet amb destinació al port 5432, consultarà la taula i l'enviarà a la màquina de la xarxa privada 192.168.1.1 que ha iniciat la connexió.

La sigla *PAT* significa 'traducció d'adreces per port' (*port address translation*).

FIGURA 4.20. Exemple de PAT

4.5 El protocol IPv6

La definició del protocol IPv6 es pot trobar en l'RFC 2460 (1998). La característica més destacada és l'augment de les adreces IP de 2^{32} a 2^{128} . Aquest increment d'adreces permet que qualsevol dispositiu pugui disposar d'una IP fixa pròpia, ja que cada persona del planeta podria disposar de diversos milions d'adreces IPv6. L'espai d'adreces és tan gran que, per cada metre quadrat de la terra, hi pot haver $6 \cdot 10^{23}$ adreces IPv6, aproximadament.

4.5.1 Adreces IPv6

Les adreces IPv6 s'assignen a interfícies, no a nodes. Un mateix node pot tenir interfícies diferents i, per tant, diverses adreces úniques vàlides per identificar el node. Fins i tot, un únic adaptador de xarxa podria tenir interfícies virtuals diferents i, cadascuna, una adreça única. Això, combinat amb la gran quantitat d'adreces possibles per a una adreça de 128 bits, permet simplificar l'encaminament. Com que es poden agrupar les adreces per jerarquies, proveïdors, proximitat, etc., les taules d'encaminament es poden simplificar per fer-les més petites i, per tant, més ràpides.

Adreça IPv6

Format hexadecimal 3FFE : 1900 : 6545 : 3 : 230 : F804 : 7EBF : 12C2

Format binari 0011111111111110 : 0001100100000000 : 0110010101000101
: 0000000000000011 : 0000001000110000 : 1111100000000100 :
0111110101111111 : 0001001011000010

Hi ha tres tipus principals d'adreces IPv6:

- Distribució a una única destinació (*unicast*).
- Distribució a un única destinació d'un conjunt de destinacions possibles (*anycast*). Una petició dirigida a una IP *anycast* s'encamina al node més proper dintre de tots els nodes rèplica que existeixin.
- Distribució múltiple (*multicast*). Es lliura a totes les adreces dins d'aquest grup de multidistribució.

El prefix que tindrà sempre és `ff00::`.

Els termes *distribució múltiple*, *multicast*, *multidistribució* i *multidifusió* són equivalents.

Els dos punts dobles (::) signifiquen que entre : i : va un grup de tants zeros com dígit hi falten per a completar l'adreça.

Les adreces especials són les següents:

- L'adreça dels rangs privats en adreces IPv6 (enllaç local o *link local*) té el prefix `fe80::`.
- L'adreça de retrobucle (*loopback*) que en la IPv4 era `127.0.0.1` passa a ser `::1`.

4.5.2 Característiques de la nova versió

A part de l'augment d'adreces IP, també s'han introduït altres millores al protocol; les més destacades són:

- Autoconfiguració amb ICMPv6
- *Jumboframes*
- Desaparició de la difusió

Autoconfiguració amb ICMPv6

Mitjançant el protocol de xarxa ICMPv6 (RFC 2461), es pot enviar un paquet a l'adreça d'enllaç de fusió anomenat *sol·licitud d'encaminador* (*router solicitation*) per demanar els paràmetres de configuració. En cas que l'encaminador estigui configurat per respondre aquests paquets, enviarà una resposta anomenada *anunci d'encaminador* (*router advertisement*) amb els paràmetres de configuració de la capa de xarxa.

Per obtenir altres paràmetres addicionals es pot fer servir el protocol DHCPv6.

Jumboframes

En la versió 4 del protocol IP un paquet podia contenir fins a $2^{16}-1$ octets de càrrega, mentre que la IPv6, mitjançant una extensió del protocol, permet enviar fins a $2^{32}-1$ IPv6 octets. Els paquets IPv6 que passen de 65.535 octets de càrrega s'anomenen *jumboframes*.

Evidentment, per poder enviar aquests paquets tan grans la capa d'enllaç ha de permetre-ho. Per tant, la capacitat d'enviar paquets grans queda relegada a la capacitat de la xarxa.

Desaparició de la difusió

En la IPv6, l'adreça més alta d'una xarxa no té cap significat especial, desapareix l'adreça de difusió i se substitueix per adreces de multidifusió. Per tant, ja no és possible enviar un paquet a tots els equips connectats a una xarxa.

Es pot obtenir la mateixa funcionalitat que l'adreça de difusió de la IPv4 mitjançant un grup de multidifusió que contingui tots els equips de la xarxa. Aquest grup sempre té l'adreça FF01 : : 1.

4.5.3 Estructura de la IPv6

L'estructura de la IPv6 s'ha pensat per ser més flexible que la definida per la IPv4. Inclou una capçalera obligatòria amb les dades bàsiques de 40 octets i, a continuació, pot tenir diverses capçaleres d'expansió. Aquesta capçalera inicial s'anomena *de la IPv6*, per simplificar-ho. S'han definit les capçaleres d'extensió següents:

- **Capçalera d'opcions salt-a-salt:** conté opcions especials que cada salt ha d'examinar.
- **Capçalera d'encaminament:** conté informació per dirigir el paquet per un node intermedi, o més, abans d'arribar a la destinació.
- **Capçalera de fragmentació:** conté informació sobre la fragmentació.
- **Capçalera d'autenticació:** d'IPSec, s'integra a IPv6 i proporciona integritat i autenticació al paquet.
- **Capçalera d'encapsulament de la càrrega de seguretat:** d'IPSec, s'integra a IPv6 i proporciona seguretat a les dades enviades.
- **Capçalera d'opcions per a la destinació:** conté informació addicional perquè sigui examinada a la destinació.

L'estàndard IPv6 recomana un cert ordre en cas que es faci servir més d'una capçalera i prescriu que la IPv6 sempre ha d'anar primer:

1. Capçalera IPv6.
2. Capçalera d'opcions salt-a-salt.
3. Capçalera d'opcions per a la destinació: opcions que s'han de processar en la primera destinació que apareix en el camp d'adreces IPv6 i les destinacions següents indicades en la capçalera d'encaminament.
4. Capçalera d'encaminament.
5. Capçalera de fragmentació.
6. Capçalera d'autenticació.
7. Capçalera de d'encapsulament de la càrrega de seguretat.
8. Capçalera d'opcions per a la destinació: opcions que només ha de processar la destinació final del paquet.

Capçalera IPv6

La capçalera IPv6 té una longitud fixa de 40 octets, xifra que contrasta amb la capçalera IPv4, que només és de 20 octets. Els camps d'aquesta capçalera són: un total de 40 octets respecte als 20 octets de la capçalera IPv4.

- **Versió (4 bits):** el valor d'aquest camp sempre ha de ser 6.
- **Classe de trànsit(8 bits):** camp que es fa servir per classificar el trànsit. Els 6 primers bits serveixen per classificar el trànsit i els 2 restants per a la prioritat.
- **Etiqueta de flux (20 bits):** camp creat per donar un tracte especial a les aplicacions de temps real.
- **Longitud de la càrrega (16 bits):** indica la longitud de la resta del paquet IPv6 en octets, excloent-ne la capçalera.
- **Capçalera següent (8 bits):** indica el tipus de la capçalera següent.
- **Límit de salts (8 bits):** s'ha canviat el nom al TTL, ja que els encaminadors no solen calcular el temps que tarda un paquet a transmetre's, sinó el nombre de salts que fa.
- **Adreça d'origen (128 bits):** adreça de l'equip que origina el paquet.
- **Adreça de destinació (128 bits):** adreça de l'equip al qual va destinat el paquet.

La capçalera IPv6, tot i que és més gran, disposa de menys camps que la capçalera IPv4 i no té una suma de verificació (*checksum*). Això està fet així perquè si un encaminador ha de modificar la capçalera (per exemple per canviar el valor del camp de límit de salts, és a dir, l'antic TTL), no hagi de recalculer la suma de verificació i, per tant, s'agilitzi l'encaminament.

Capçalera d'opcions salt-a-salt

La capçalera d'opcions salt-a-salt, si hi és present, porta informació addicional que cal que sigui examinada per tots els dispositius d'encaminament al llarg del camí. Els camps d'aquesta capçalera són:

- **Capçalera següent (8 bits):** indica el tipus de la capçalera següent.
- **Longitud de la capçalera sense incloure els primers 64 bits (8 bits):** indica la mida d'aquesta capçalera, ja que és de longitud variable, en unitats de 64 bits, sense incloure-hi els primers 64 bits.
- **Opcions:** camp de longitud variable amb les definicions de les opcions. Cada definició d'opció consta de tres camps:
 - Tipus d'opció (8 bits) per identificar l'opció.
 - Longitud de l'opció (8 bits) en octets.
 - Dades de l'opció.

Capçalera de fragmentació

En el cas de la IPv6, només pot fragmentar el node d'origen, mentre que en el cas de la IPv4 se n'encarreguen els dispositius encaminadors. Per enviar el paquet de la mida adequada, el node que origina el paquet ha de descobrir l'MTU de totes les xarxes de la ruta fins a la destinació per fragmentar les dades com calgui. Si no s'executa l'algorisme per descobrir l'MTU de la ruta, el node originant haurà de limitar la mida dels paquets a 1.280 octets. Aquesta és la mida mínima d'MTU que ha de permetre la xarxa perquè hi puguin circular paquets IPv6.

Els camps d'aquesta capçalera són els següents:

- **Capçalera següent (8 bits):** indica el tipus de la capçalera que ve a continuació.
- **Reservat (8 bits):** octets reservats que s'han d'inicialitzar a zero.
- **Desplaçament del fragment (13 bits):** *offset* del fragment respecte al paquet original en unitats de 64 bits.
- **Reservat (2 bits):** octets reservats que s'han d'inicialitzar a zero.
- **Indicador de més fragments (1 bits):** indica que hi ha més fragments (bit a 1), o bé, si és l'últim fragment (bit a 0). És semblant al camp MF de la IPv4.
- **Identificació (32 bits):** es fa servir per identificar d'una manera única el paquet original del fragment.

Capçalera d'encaminament

La capçalera d'encaminament conté una llista d'un o més nodes intermedis per on es vol dirigir el paquet a la destinació. Aquesta capçalera comença amb 4 camps de 8 bits, seguits de les dades específiques del tipus d'encaminament. Els camps són:

- **Capçalera següent (8 bits):** indica el tipus de la capçalera que ve a continuació.
- **Longitud de la capçalera d'extensió** sense incloure-hi els primers 64 bits (8 bits).
- **Tipus d'encaminament (8 bits):** identifica el tipus particular de capçalera. Pot ser 0, 1 i 2:
 - El tipus 0 és susceptible d'atac de denegació de servei; per tant, es considera obsolet.
 - El tipus 1 es fa servir per a un projecte de l'agència americana DARPA.
 - El tipus 2 és una versió restringida del tipus 0.
- Segments que queden (8 bits) abans d'acabar aquesta capçalera.
- Dades del tipus d'encaminament: pot tenir una longitud variable.

Capçalera d'opcions per a la destinació

La capçalera d'opcions per a la destinació és igual que la d'opcions salt-a-salt, però només l'ha d'examinar el node de destinació del paquet. Els camps són iguals:

- **Capçalera següent (8 bits):** indica el tipus de la capçalera següent.
- **Longitud de la capçalera** sense incloure-hi els primers 64 bits (8 bits).
- **Opcions:** camp de longitud variable amb les definicions de les opcions.

5. Protocols de la capa de transport

Els protocols de la capa de transport supervisen la transmissió de les dades d'extrem a extrem, és a dir, des d'un programa que s'està executant en un *host* A d'una xarxa X fins a un altre programa que s'està executant en un *host* B d'una xarxa Y. La capa de transport actua com a lligam entre les capes superiors (sessió, presentació i aplicació) i les capes inferiors (xarxa, enllaç de dades i física). D'aquesta manera, les capes superiors poden utilitzar els serveis de la capa de transport per interactuar amb la xarxa sense haver d'interactuar directament amb les capes inferiors.

Les principals funcions de la capa de transport són dues:

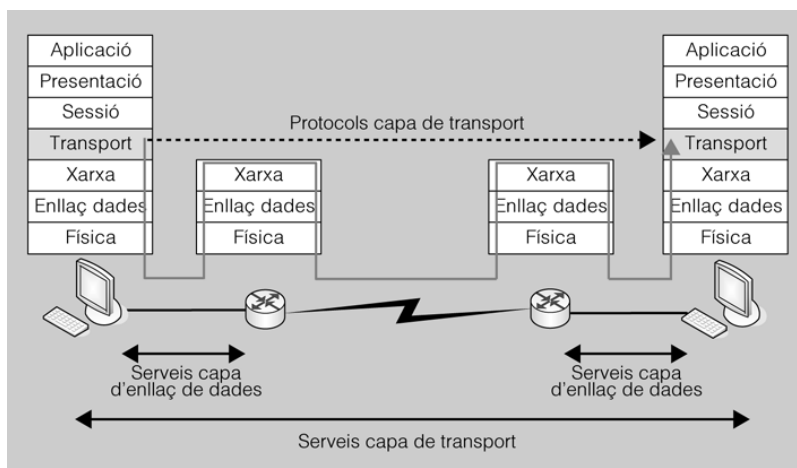
- el control del flux d'extrem a extrem, que ve proporcionat per les finestres "lliscants", i
- la fiabilitat de la transmissió, que és garantida pels paquets d'acusaments de rebut o ACK (*acknowledgment packets*) i pels nombres de seqüència.

Alguns exemples de protocols de la capa de transport són el protocol TCP (*transmission control protocol*) i el protocol UDP (*user datagram protocol*). De fet, són els dos protocols d'ús habitual a la capa de transport del conjunt TCP/IP.

5.1 Funcions de la capa de transport

Els serveis de la capa de transport són implementats per un protocol de la mateixa capa que és utilitzat per comunicar dos *hosts* (figura 5.1).

FIGURA 5.1. Serveis de la capa de transport



Encaminador i capes OSI

El *router* o encaminador és un dispositiu de capa 3 en el model OSI, és a dir, implementa la capa física, la capa d'enllaç de dades i la capa de xarxa.

Els serveis proporcionats per la capa de transport fan una funció semblant als serveis que proporciona la capa d'enllaç de dades. Els serveis de la capa d'enllaç de dades, però, actuen sobre una única xarxa, mentre que els de la capa de transport actuen sobre una *internetwork* formada per diverses xarxes.

Els serveis proporcionats pels protocols de la capa de transport es poden dividir en cinc grans categories: transmissió de missatges d'extrem a extrem, adreçament, fiabilitat de les transmissions, control del flux i multiplexació.

5.1.1 Transmissió de missatges d'extrem a extrem (end-to-end delivery)

La capa de xarxa supervisa la transmissió dels paquets individuals de dades d'extrem a extrem (entre el *host* emissor i el *host* receptor). A la capa de xarxa, però, no es tenen en compte les possibles relacions existents entre els diferents paquets, ni tan sols en el cas de paquets que pertanyen a un mateix missatge, és a dir: la capa de xarxa tracta cada paquet de manera independent. Per contra, la capa de transport s'assegura de la transmissió correcta de tot el missatge, que estarà format per diversos paquets individuals que caldrà ordenar en la destinació.

Fragmentació de missatges en paquets

Abans de ser enviats del *host* origen al *host* destinació, els missatges són fragmentats en paquets, els quals són enviats de forma individual per la xarxa. Aquests paquets solen incloure informació, com ara l'ordre del paquet dintre del missatge, que permet la reconstrucció del missatge original al *host* destinació.

Transmissions d'extrem a extrem

La transmissió d'extrem a extrem és un concepte que fa referència a les transmissions que es produeixen entre dos *hosts* situats en xarxes distintes.

5.1.2 Punts d'accés al servei

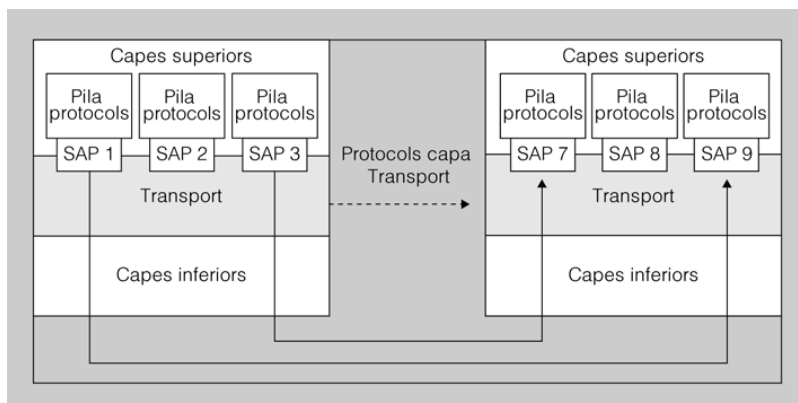
Algunes piles o *suites* de protocols combinen en un únic paquet diferents protocols de les capes superiors (sessió, presentació i aplicació). Això fa que sovint els serveis que presta la capa de transport a la capa de sessió siguin, en realitat, serveis al conjunt de capes superiors: les dades generades en la capa d'aplicació d'un *host* A s'hauran de lliurar a un programa determinat dels que s'estan executant en la capa d'aplicació d'un *host* B destinació, és a dir, hi poden haver múltiples comunicacions establertes entre ubicacions concretes del *host* A i ubicacions concretes del *host* B (figura 5.2).

Aquestes ubicacions es coneixen amb el nom de **punts d'accés al servei** (*service access point* o SAP).

Per tal de garantir la transmissió correcta de les dades entre els respectius punts d'accés al servei, ens caldrà un tercer nivell de direccionament (a més del físic i

del lògic): els protocols de la capa de transport han de saber quins protocols de capes superiors s'estan comunicant.

FIGURA 5.2. Punts d'accés al servei o SAP



5.1.3 Fiabilitat de les transmissions

En la capa de transport, la fiabilitat de les transmissions es fonamenta en quatre mecanismes de control bàsics:

1. **Control d'errors.** Els serveis de la capa d'enllaç de dades garanteixen la transmissió sense errors entre dos nodes de la mateixa xarxa. Això, però, no és garantia que no hi hagi errors entre el lliurament d'extrem a extrem en una *internetwork* (per exemple, errors produïts en els encaminadors no serien detectats per les funcions de la capa d'enllaç de dades). En la capa de transport es fa ús d'algoritmes implementats en programari, com ara la suma de verificació o *checksum*, per detectar errors en la transmissió d'extrem a extrem. Quan un error és detectat, es procedeix a la retransmissió dels paquets corresponents.
2. **Control de la seqüència.** Al *host* origen de la transmissió, la capa de transport és responsable de garantir que les dades rebudes des de les capes superiors són utilitzables per les capes inferiors: quan la unitat de dades rebuda de les capes superiors és més gran que la mida d'un datagrama o d'una trama, el protocol de transport la divideix en blocs més petits anomenats **segments** (procés de segmentació); si, per contra, la unitat de dades provinent de les capes superiors és més petita que la mida d'un datagrama o d'una trama, el protocol de transport pot concatenar diverses d'aquestes unitats per formar-ne una d'única (procés de concatenació). D'altra banda, en el *host* destinació de la transmissió, la capa de transport és responsable de garantir que els paquets rebuts són correctament assembleats per donar sentit al missatge: molts serveis de la capa de transport afegeixen un **nombre de seqüència** al final de cada segment; aquest nombre indica l'ordre en què els segments s'han d'assemblar (si s'ha produït segmentació) o dividir (si s'ha produït concatenació) en la destinació.
3. **Control de pèrdues.** Els nombres de seqüència permeten als protocols de capa de transport del *host* receptor identificar qualsevol segment perdut

Suma de verificació

Les tècniques de suma de verificació o *checksum* fan ús d'operacions algebraiques per detectar canvis no intencionats entre les dades emeses i les dades finalment rebudes.

i sol·licitar-ne el reenviament. D'aquesta manera, la capa de transport garanteix que tots els segments d'una transmissió arribin a la seva destinació final.

4. **Control de duplicitats.** Els nombres de seqüència permeten als protocols de capa de transport del *host* receptor identificar i descartar els segments que s'han rebut per duplicat. D'aquesta manera, la capa de transport garanteix la no-duplicat dels segments rebuts.

5.1.4 Control del flux: finestres "lliscants"

La capa de transport és també la responsable del control del flux en una transmissió d'extrem a extrem dins una *internetwork*.

Internetwork

Una internetwork o internet (no confondre amb Internet) és qualsevol xarxa formada per diverses xarxes connectades entre si mitjançant dispositius de capa 3 (encaminadors, per exemple).

El **control del flux** és un conjunt de procediments que permeten indicar al *host* emissor quina quantitat de dades (en nombre de paquets o en nombre de *bytes*) ha de transmetre abans de parar-se a esperar un **acusament de rebuda** o **ACK** per part del *host* receptor. El flux de dades no ha de saturar mai el *buffer* del *host* receptor.

Els dos mètodes més habituals per controlar el flux d'una transmissió són el mètode *stop-and-wait* i el de finestra lliscant:

- En el mètode ***stop-and-wait*** l'emissor espera l'acusament de rebuda per a cadascun dels paquets de dades que envia, de manera que no enviarà un nou paquet fins que no rebi l'ACK del paquet anterior. Òbviament, aquest mètode de transmissió no és gaire eficient, ja que cal esperar la confirmació de cada paquet enviat abans de poder-ne enviar un de nou.
- En el mètode de ***finestra lliscant*** (*sliding window*), l'emissor pot enviar un nombre acordat de paquets abans d'esperar un únic acusament de rebuda o ACK per a tots ells. El terme *finestra lliscant* fa referència a un rang o finestra imaginària que va desplaçant-se per sobre de la seqüència de paquets que conformen la transmissió (figura 5.3).

5.1.5 Multiplexació a la capa de transport

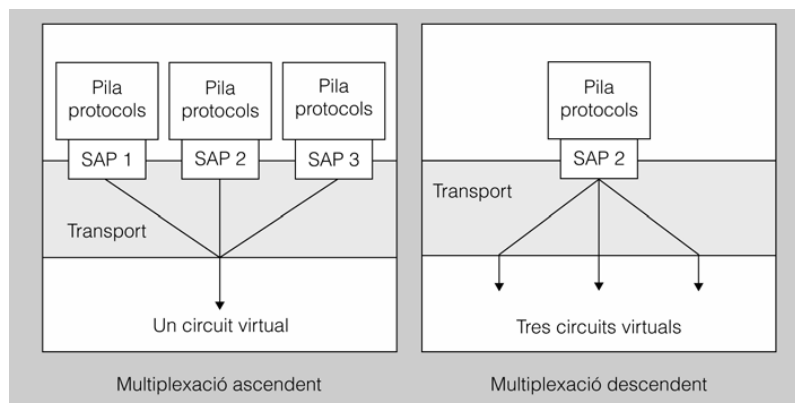
Per millorar l'eficiència de la transmissió, la capa de transport permet fer **multiplexació**. La multiplexació en aquesta capa pot ser de dos tipus (figura 5.5):

- **Múltiples connexions de capa de transport utilitzen la mateixa connexió de xarxa (multiplexació ascendent).** La capa de transport utilitza circuits virtuals basats en els serveis proporcionats per les capes inferiors. La capa de transport permet compartir l'ús d'un mateix circuit virtual per part de diverses transmissions. Així, gràcies a la multiplexació ascendent, diferents aplicacions (HTTP, FTP, etc.) o diferents usuaris poden estar compartint un mateix circuit virtual.
- **Una connexió de capa de transport utilitza múltiples connexions de xarxa (multiplexació descendent).** La capa de transport també permet dividir una única connexió en diferents circuits virtuals per tal de millorar la velocitat de transmissió.

Circuit virtual

Un circuit virtual és una connexió entre dos *hosts* que, tot i estar basada en múltiples connexions físiques que poden anar variant amb el temps, funciona -des del punt de vista lògic- com una única connexió directa.

FIGURA 5.5. Multiplexació a la capa de transport



5.2 Serveis orientats a connexió: intercanvi de senyals a tres passes

La transmissió de dades d'extrem a extrem es pot dur a terme en mode orientat a connexió o bé en mode no orientat a connexió.

Un protocol **orientat a connexió** estableix un circuit virtual a través de la *internetwork* entre el *host* emissor i el receptor. Tots els paquets d'un mateix missatge són enviats per aquest circuit virtual.

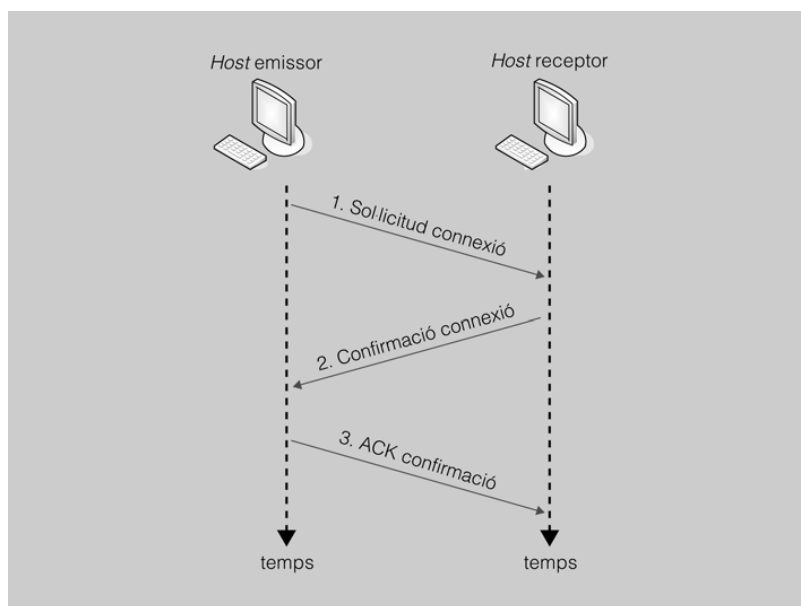
Utilitzar un únic circuit per enviar tots els paquets d'un mateix missatge facilita el procés d'enviament i recepció d'acusaments de rebuda i la retransmissió dels paquets perduts o defectuosos. Per tant, els serveis orientats a connexió són

considerats serveis altament fiables. La transmissió orientada a connexió té tres etapes:

1. Establiment de la connexió. Abans que un dispositiu pugui enviar dades a un altre, el dispositiu que inicia la comunicació ha de comprovar la disponibilitat de l'altre per rebre dades i s'ha d'establir un camí a través de la xarxa per on s'enviaran les dades. L'establiment de la connexió requereix tres accions concretes que configuren l'anomenat procés de **salutació a tres passes** (*three-way handshake*), tal com es mostra a la figura 5.6.

- El *host* que sol·licita la connexió envia un paquet de sol·licitud de connexió al *host* destinatari.
- El *host* destinatari retorna un paquet de confirmació al *host* sol·licitant.
- El *host* sol·licitant envia un paquet amb l'acusament de rebuda del paquet de confirmació.

FIGURA 5.6. Procés de salutació a tres passes



2. Transferència de dades.

3. Finalització de la connexió. Un cop totes les dades s'han transferit, cal finalitzar la connexió. Aquest procés de finalització també requereix una salutació a tres passes:

- El *host* que havia iniciat la transmissió envia un paquet al *host* receptor en què sol·licita la desconnexió.
- El *host* receptor confirma la sol·licitud de desconnexió.
- El *host* sol·licitant respon amb un paquet d'acusament de rebuda del paquet de confirmació.

Datagrama

Un paquet o datagrama és un conjunt de dades amb un format especial que en permet la transmissió per la xarxa. En alguns textos, el terme *paquet* es reserva per fer referència a qualsevol conjunt de dades llest per ser transmès, mentre que el terme *datagrama* es reserva per fer referència a paquets d'un servei no fiable, com ara el que proporciona UDP.

5.3 Protocols de capa de transport i ports

En la pila TCP/IP, hi ha dos protocols clau associats a la capa de transport: TCP i UDP. El protocol UDP es fa servir quan es vol prioritzar la velocitat de la transmissió sobre la fiabilitat de la transmissió (per exemple, serveis de videoconferència). La majoria d'aplicacions, però, fan ús del protocol TCP, ja que aquest protocol proporciona fiabilitat a les transmissions d'extrem a extrem.

En el seu ús més habitual, el concepte de *procés* fa referència a un programa en execució.

El protocol IP transmet un datagrama des del *host* origen fins al *host* destinació, i és, per tant, un protocol de *host* a *host*. Els sistemes operatius actuals, però, són multiusuari i multiprocés. Per tant, quan un datagrama arriba a un *host* que està executant diversos processos concurrents, cal determinar quin dels processos és el veritable destinatari de la transmissió. D'altra banda, la transmissió procedirà d'un procés concret dels múltiples processos concurrents en el *host* origen.

La interfície entre els processos i els seus ports corresponents la proporciona el sistema operatiu del host.

Els protocols de transport de la *suite* TCP/IP defineixen un conjunt de punts de connexió en processos individuals anomenats **ports**. Un port és un punt d'origen o de destinació de les dades, habitualment un *buffer*, que permet emmagatzemar dades que seran utilitzades per un procés concret.

Buffer

En el seu ús més habitual, es pot entendre el concepte de *buffer* com una àrea del host destinació en la qual s'emmagatzemen temporalment les dades transmeses fins que poden ser processades per l'aplicació destinació.

Els protocols de capa de transport de la pila TCP/IP són protocols port a port. Aquests protocols transmeten el datagrama des del port origen fins als serveis IP del *host* origen i des dels serveis IP del *host* de destinació fins al port de destinació. Cada port és identificat per un enter positiu entre 0 i 65.535 que s'inclou en la capçalera del datagrama que es transmet. Un exemple de port és el port 80, que s'utilitza habitualment per acceptar sol·licituds de pàgines web mitjançant el protocol HTTP.

5.3.1 UDP (user datagrama protocol)

UDP (*user datagrama protocol*) opera en la capa de transport del model OSI i proporciona serveis de transmissió ràpida de dades però sense fiabilitat.

UDP és un protocol no orientat a connexió, és a dir, UDP no comprova que el *host* destinació estigui disponible abans de començar la transmissió. Per aquest motiu, UDP no ofereix cap garantia que els paquets enviats seran rebuts en el *host* destinació. Com que tampoc no fa ús de nombres de seqüència, UDP no

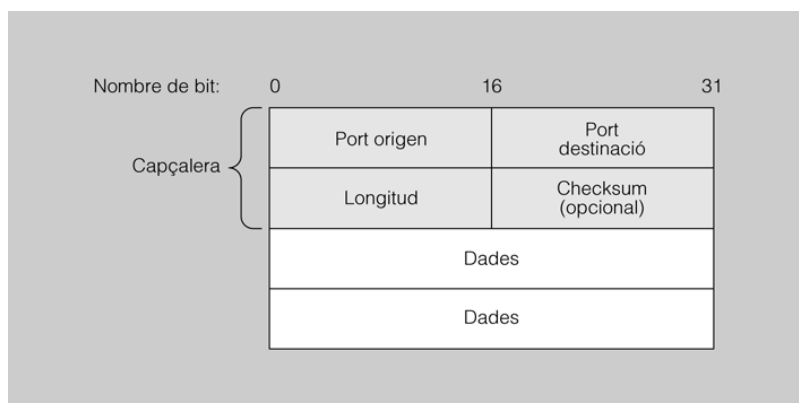
ofereix cap garantia que, en el cas que els paquets arribin a la destinació, aquests siguin rebuts en l'ordre correcte. A més, UDP tampoc no proporciona mètodes de detecció d'errors. Tot això fa que les transmissions UDP no es puguin considerar fiables.

Tot i no proporcionar transmissions fiables, en ser UDP un protocol molt senzill resulta força eficient des del punt de vista de la velocitat de transmissió, per la qual cosa UDP és molt útil en situacions en què cal transferir una gran quantitat de dades en poc temps. Aquest és el cas, per exemple, de transmissions de vídeo o àudio per Internet i en temps real.

La figura 5.7 mostra un segment UDP, els principals camps del qual es descriuen a continuació:

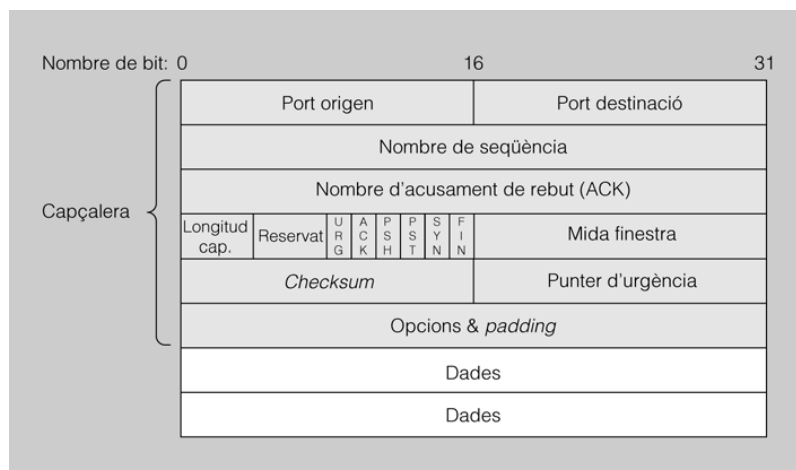
- **Port origen.** Indica el nombre de port que inicia la transmissió al *host* origen. Aquest camp té una longitud de 16 bits.
- **Port destinació.** Indica el nombre de port al *host* destinació. Aquest camp té una longitud de 16 bits.
- **Longitud.** Indica la longitud total del datagrama en *bytes*. La longitud d'aquest camp és de 16 bits.
- **Suma de verificació.** Aquest camp, opcional en UDP, permet al *host* destinació determinar si el segment s'ha corromput durant la transmissió. La seva longitud és de 16 bits.
- **Dades.** Conté les dades enviades pel *host* origen. La mida d'aquest camp és variable.

FIGURA 5.7. Camps d'un segment UDP



5.3.2 TCP (Transmission Control Protocol)

TCP (*Transmission Control Protocol*) opera en la capa de transport del model OSI i proporciona serveis de transmissió fiable de dades.

FIGURA 5.8. Camps d'un segment TCP

TCP és un protocol orientat a connexió. A més, TCP garanteix la fiabilitat de la transmissió mitjançant l'ús de nombres de seqüència i mètodes de suma de verificació o *checksum*. Sense totes aquestes mesures, les dades serien transmeses de manera indiscriminada, sense comprovar, per exemple, si el *host* destinació està o no disponible o si les dades s'han corromput durant la transmissió. Finalment, TCP proporciona també control del flux per garantir que un *host* no és col·lapsat amb més dades de les que el seu *buffer* pot emmagatzemar.

La figura 5.8 mostra el format d'un segment TCP, els principals camps del qual es descriuen a continuació:

Protocol orientat a connexió

Abans que el protocol comenci amb la transmissió de les dades, s'estableix una connexió entre els nodes o extrems de la comunicació.

- **Port origen.** Indica el nombre de port que inicia la transmissió al *host* origen. Aquest camp té una longitud de 16 bits.
- **Port destinació.** Indica el nombre de port al *host* destinació. Aquest camp té una longitud de 16 bits.
- **Nombre de seqüència.** Indica la posició que ocupa aquest segment en relació amb el conjunt de segments en què s'ha dividit un missatge. Aquest camp té 32 bits de longitud.
- **Nombre d'acusament de rebuda (*acknowledgment number*).** S'utilitza per enviar un acusament de rebuda. Quan el bit ACK és actiu (val "1"), aquest camp indica el nombre de seqüència del segment que s'espera rebre a continuació. La seva longitud és de 32 bits.
- **Longitud de la capçalera.** Indica la longitud total de la capçalera d'un segment TCP. Aquest camp té 4 bits de longitud.
- **Reservat.** Aquest és un camp de 6 bits reservat per a un ús futur.
- **Bits de control (URG, ACK, PSH, RST, SYN, FIN).** Cadascun d'aquests bits o indicadors (*flags*) és independent de la resta.
 - URG. Quan està actiu indica que el camp punter d'urgència conté informació per al *host* receptor.

- ACK. Quan està actiu indica que el camp nombre ACK conté informació per al *host* receptor.
 - PSH. Quan està actiu indica que el *host* receptor ha de passar les dades a les capes superiors de manera immediata.
 - RST. Quan està actiu indica que cal reiniciar la connexió pel fet que hi ha hagut alguna confusió en els nombres de seqüència.
 - SYN. Quan està actiu indica que cal sincronitzar els nombres de seqüència entre els dos *hosts*.
 - FIN. Quan està actiu indica que el segment actual és el darrer d'una seqüència i que cal finalitzar la connexió.
- **Mida de la finestra.** És un camp de 16 bits que indica la mida de la finestra lliscant.
 - **Suma de verificació.** Aquest camp permet al *host* destinació determinar si el segment s'ha corromput durant la transmissió. La seva longitud és de 16 bits.
 - **Punter d'urgència.** És el darrer camp obligatori d'un encapçalament TCP. Quan el bit URG és actiu, aquest camp de 16 bits indica que hi ha dades urgents en el camp dades i la seva localització.
 - **Opcions i caràcter de farciment (*padding*).** La mida d'aquest camp pot ser 0 o 32 bits, en funció de si el segment conté informació addicional (com ara la mida màxima de segment que pot suportar una xarxa) o no. Si es fan servir opcions, la part de caràcters de farciment (*padding*) conté bits d'emplenament per tal que la mida total del camp arribi fins als 32 bits.
 - **Dades.** Conté les dades enviades pel *host* origen. La mida d'aquest camp és variable.

5.3.3 Sòcols i ports

Cada procés que s'estigui executant en una màquina té assignat un **nombre de port**. S'anomena **sòcol** o **socket** **d'un procés** el parell format per el nombre de port del procés i l'adreça IP del *host* on el procés s'està executant.

Exemple de nombre de port

El nombre de port predeterminat per a un servei HTTP és el 80; si l'adreça IP d'un *host* on s'està executant un servei HTTP és 10.44.8.81, llavors el sòcol del servei HTTP en aquell *host* seria 10.44.8.81:80. És a dir, el *host* assumeix que qualsevol sol·licitud que arribi al port 80 serà de tipus HTTP.

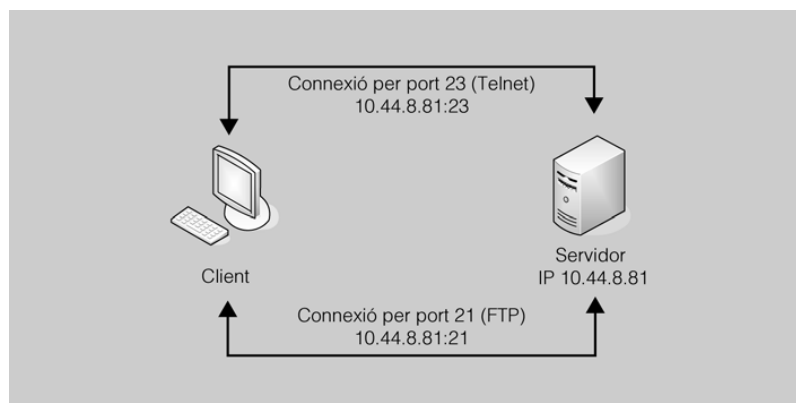
Els sòcols o *sockets* permeten crear connexions virtuals entre un procés en execució en un *host* A i el mateix procés en execució en un altre *host* B. L'ús de nombres de ports simplifica les comunicacions TCP/IP i garanteix que les dades són transmeses a les aplicacions correctes.

SAP i ports

Ethernet utilitza punts d'accés al servei per identificar cadascun dels diferents circuits de comunicació establerts entre dos *hosts* dins d'una mateixa subxarxa, amb la qual cosa es permet la multiplexació de la connexió. Per contra, TCP/IP utilitza ports per tal d'identificar les comunicacions entre dos *hosts* d'una *internet-work*.

L'ús de ports simplifica les comunicacions TCP/IP i garanteix que les dades són transmeses a l'aplicació correcta. Quan, per exemple, un client fa una sol·licitud de comunicació a un servidor pel port 23, el servidor immediatament sap que el client pretén iniciar una sessió Telnet. Llavors, el servidor connecta al port Telnet del client -el 23 per defecte- i estableix un circuit virtual (figura 5.9).

FIGURA 5.9. Camps d'un segment TCP



Els hosts clients sol·liciten serveis que ofereixen altres hosts, anomenats servidors.

Els nombres de port van des del 0 fins al 65535 i es poden dividir en tres grups:

- **Ports coneguts** (del 0 al 1023): són assignats a processos als quals només pot accedir el sistema operatiu o l'administrador del sistema. Aquests ports estan assignats a protocols oberts d'ús molt estès (per exemple, correu electrònic, DNS, HTTP...). Normalment només pot executar el procés que els implementa el propi sistema operatiu o un administrador del sistema.
- **Ports registrats** (del 1024 al 49151): són accessibles a processos i usuaris sense privilegis especials. Estan assignats a companyies amb aplicacions comercials.
- **Ports dinàmics o privats** (del 49152 al 65535): són ports lliures que l'usuari pot fer servir sense restriccions.

Telnet

Telnet és un servei que s'utilitza per connectar-se a un *host* remot mitjançant TCP/IP. El protocol corresponent, del mateix nom pertany a la capa d'aplicació.

La taula 5.1 conté una relació dels ports més habituals en TCP/IP i el seu servei associat. La major part dels servidors mantenen un fitxer de text amb el nombre de port associat a cada servei. Això permet canviar el nombre de port que per defecte té un determinat servei (per exemple, enlloc de fer servir el port 23, es pot configurar el port 2330 per al servei Telnet). Alguns administradors fan ús d'aquesta tècnica per tractar de dificultar l'accés dels pirates o *hackers* als seus servidors.

TAULA 5.1. Ports més habituals en TCP/IP

Nombre de port	Nom del procés	Protocol
7	ECHO	TCP i UDP
20	FTP-DATA	TCP
21	FTP	TCP
22	SSH	TCP
23	TELNET	TCP
.		

TAULA 5.1 (continuació)

Nombre de port	Nom del procés	Protocol
25	SMTP	TCP
53	DNS	TCP i UDP
69	TFTP	UDP
80	HTTP	TCP i UDP
110	POP3	TCP
119	NNTP	TCP
143	IMAP	TCP
443	HTTPS	TCP

Ports i seguretat

Per motius de seguretat, alguns administradors de xarxa acostumen a canviar els nombres de port assignats als serveis més habituals.

Podeu trobar informació complementària a www.ietf.org/rfc/rfc1700.txt (conté la normativa d'Internet RFC1700).

6. Protocols de la capa d'aplicació

Com que la *suite* TCP/IP es va desenvolupar abans que el model OSI, les capes del model TCP/IP no corresponen exactament a les capes del model OSI. La capa d'aplicació de TCP/IP ve a ser l'equivalent de combinar les capes de sessió, presentació i aplicació del model OSI.

Els serveis de la capa d'aplicació faciliten la comunicació entre les aplicacions de programari, que corren por sobre d'aquesta capa, i els serveis que presten les capes inferiors, de manera que la xarxa pugui interpretar les sol·licituds provinents d'una aplicació i, alhora, l'aplicació pugui interpretar les dades que li arriben de la xarxa. Mitjançant els protocols de la capa d'aplicació, les aplicacions de programari negocien amb la xarxa aspectes relacionats amb el format de les dades, polítiques de seguretat i sincronització, etc.

Així, per exemple, quan es fa ús d'un navegador per obrir una pàgina web, el protocol de la capa d'aplicació HTTP dona format a la sol·licitud i l'envia des del navegador del client (una aplicació de programari) fins al servidor. El mateix protocol s'encarrega també de donar format i enviar la resposta del servidor web al navegador del client.

6.1 Model client-servidor

La major part de les aplicacions de programari que funcionen en un entorn de xarxa segueixen un **model client-servidor**. Aquestes aplicacions -com ara FTP, navegadors web i programes de correu electrònic-, tenen dos components que els permeten comunicar-se entre elles: la part client i la part servidor.

Un **programa client** és un 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). Un programa client és iniciat per un usuari o per un altre programa, i finalitza quan el programa rep el servei sol·licitat.

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

6.2 Assignació automàtica d'adreces IP: BOOTP i DHCP

Cada *host* connectat a una xarxa TCP/IP ha de conèixer la informació bàsica següent:

- la seva adreça IP,
- la seva màscara de subxarxa,
- l'adreça IP del *gateway* predeterminat i
- l'adreça IP d'un servidor DNS.

Tota aquesta informació pot estar enregistrada de manera manual a un fitxer de configuració que és consultat quan el *host* s'engega o, alternativament, pot ser assignada de manera dinàmica durant el procés d'arrencada mitjançant protocols com ara BOOTP o DHCP.

6.2.1 BOOTP

BOOTP (*bootstrap protocol*) és un protocol de la capa d'aplicació que utilitza una llista centralitzada d'adreces IP per tal d'assignar, de manera dinàmica, adreces IP als nodes d'una xarxa.

Les adreces que assigna BOOTP són, per tant, **adreces IP dinàmiques**, en el sentit que són assignades de manera automàtica per un servidor en resposta a una sol·licitud del client o *host*, i que poden canviar en el futur també de manera automàtica.

En una xarxa on hi ha un servidor BOOTP, el procés d'assignació d'adreces és el següent: quan un dispositiu client o *host* es connecta a la xarxa, envia un missatge de difusió (*broadcast*) a la xarxa sol·licitant una adreça IP. En el missatge s'inclou l'adreça física (MAC) del sol·licitant. Llavors, el servidor BOOTP anota l'adreça MAC en la seva llista i li respon un missatge al client amb la informació següent: adreça IP que li assigna, la màscara de subxarxa associada, l'adreça IP i el nom del servidor BOOTP i l'adreça IP d'un encaminador o *gateway* predeterminat que dona sortida a l'exterior de la xarxa (a Internet, per exemple).

La principal diferència entre els protocols RARP i BOOTP és que el primer no és encaminat (*routable*), de manera que caldria tenir un servidor RARP per cada segment de xarxa o LAN. A més, el RARP només proporciona l'adreça IP, però no pot assignar màscares de subxarxa ni altra informació addicional, com ara l'adreça IP del servidor o la de l'encaminador.

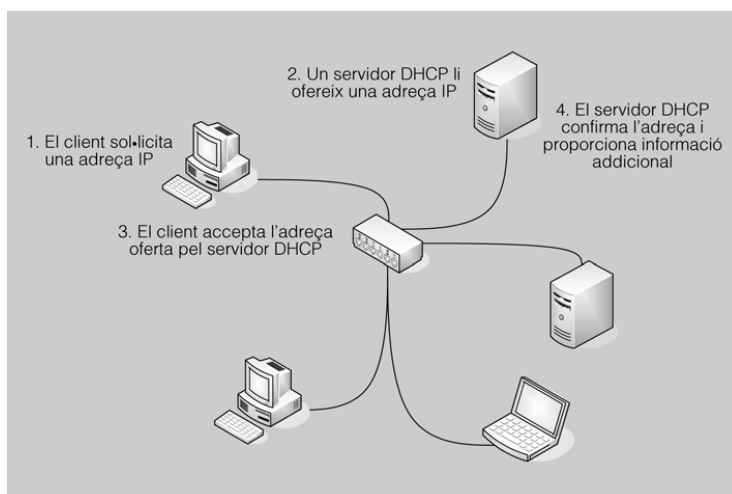
6.2.2 DHCP

DHCP (*dynamic host configuration protocol*) és un altre protocol de la capa d'aplicació que millora algunes de les funcions del protocol BOOTP. La major part de les xarxes actuals fan ús d'un servidor DHCP per assignar les adreces IP als *hosts* de manera dinàmica.

En les xarxes on es fa servir el protocol DHCP, el servidor DHCP assigna temporalment adreces IP als nodes que s'hi connectin. El temps d'aquesta assignació temporal o préstec està en funció de la configuració concreta del servidor i del client o *host*. Quan el termini de préstec finalitza, el client pot sol·licitar una renovació. En configurar un servei DHCP és necessari establir un rang d'adreces IP disponibles per a préstec i, si cal, una llista de les adreces reservades que quedaran excloses de préstec. A més, també caldrà configurar quina és la durada predeterminada del préstec.

El funcionament del procés d'assignació via DHCP és el següent (figura 6.1):

FIGURA 6.1. Assignació d'adreces IP mitjançant DHCP



1. Quan un client es connecta a una xarxa, envia un paquet de tipus *DHCP discover* per difusió (*broadcast*).
2. Cada servidor DHCP situat en la mateixa subxarxa que el client respon -també en difusió- oferint al client una adreça IP disponible (i d'altra informació addicional: màscara de subxarxa, adreça IP del servidor DHCP, duració del préstec, etc.); a més, el servidor DHCP retira provisionalment aquesta adreça de la llista d'adreces disponibles.
3. El client accepta la primera oferta d'adreça IP rebuda i envia un missatge d'acceptació en difusió, de manera que la resta de servidors DHCP sàpiguen que ja té una IP i que, per tant, poden tornar a la llista d'adreces disponibles aquelles adreces IP no utilitzades.

4. Quan el servidor DHCP seleccionat ha rebut el missatge d'acceptació del client, contesta amb un altre missatge de confirmació, el qual incorpora informació addicional (màscara de subxarxa, adreça dels servidors DNS, adreça del *gateway* o encaminador predeterminat, etc.).

Un procés semblant al descrit es produeix cada cop que el període de préstec de l'adreça IP finalitza i el client vol demanar la renovació. Des del mateix client -o des del servidor-, es pot forçar també la finalització del préstec d'una adreça IP assignada per DHCP i, fins i tot, forçar l'assignació d'una nova adreça IP.

Alliberament i renovació de l'adreça IP en Linux

Per alliberar la màquina de l'adreça IP actualment assignada es pot fer ús de l'ordre *dhclient -r*. Per demanar una nova adreça IP es pot fer ús de l'ordre *dhclient eth0* o *dhclient wlan0*, segons la interfície que vulguem renovar.

Alliberament i renovació de l'adreça IP en Windows

En Windows, per alliberar la màquina de l'adreça IP actualment assignada es pot fer ús de l'ordre *ipconfig / release*. Per demanar una nova adreça IP es pot fer ús de l'ordre *ipconfig /renew*.

6.3 Noms de hosts i DNS

El adreçament en TCP/IP es fa mitjançant l'ús de nombres (adreces IP, màscares de subxarxa, etc.). Com que per als humans és més fàcil recordar i treballar amb noms que no amb números llargs, les autoritats que gestionen Internet han establert un sistema de noms per a tots els nodes connectats a Internet, de manera que qualsevol *host* pugui ser fàcilment identificat amb un nom.

6.3.1 Noms de domini

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* (*fully qualified host name*) està format pel nom del *host* més el nom del domini al qual pertany.

Exclusivitat dels dominis

Un cop que una organització o individu ha enregistrat un nom de domini per a ús propi a Internet, cap altra organització ni individu pot fer ús del mateix nom de domini a Internet.

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. Per exemple, en el nom de domini www.ioc.cat, “cat” és el **domini de nivell superior** (*top-level domain*), “ioc” és el domini de segon nivell, i “www” és el domini de tercer nivell. Cada domini de segon nivell pot contenir múltiples dominis de tercer nivell, per exemple: ftp.ioc.cat, eines.ioc.cat, etc.

Els noms de domini han d'estar enregistrats per l'ICANN o, en el seu defecte, per una empresa autoritzada a aquest efecte per aquesta entitat. La taula 6.1 mostra alguns dels dominis de nivell superior aprovats per l'ICANN.

L'ICANN és l'*Internet Corporation for Assigned Names and Numbers* o, en català, la Corporació d'Internet per a l'Assignació de Noms i Números.

TAULA 6.1. Exemples de dominis de nivell superior (top-level domains)

Domini	Tipus d'organització
com	Comercial
edu	Educativa (universitats, etc.)
gov	Governamental
org	Organització sense ànim de lucre
net	Organització que ofereix serveis per a Internet (ISP, etc.)
museum	Museus
es	Espanya
cat	Catalunya
uk	Regne Unit
fr	França

Exemples de noms de domini i host

Alguns exemples de nom de domini són: ioc.cat, uoc.edu, ibm.com, mec.es. Com a exemple de nom de *host* tenim: host1.ioc.cat.

6.3.2 Fitxers hosts

En moltes organitzacions es fa ús d'uns fitxers de text anomenats **fitxers** hosts per tal de mantenir, només per a ús privat (no visible des d'Internet), una taula que associa noms de domini interns (un per cada *host* de la xarxa) amb les adreces IP corresponents. Cada nom de domini té un **àlies** que serveix de nom curt alternatiu per fer referència al *host*. A continuació un exemple de fitxer *hosts*:

```

1 GNU nano 2.0.9          Archivo: hosts
2
3     127.0.0.1      localhost
4     127.0.1.1      laptop
5
6     # The following lines are desirable for IPv6 capable hosts
7
8     ::1    localhost ip6-localhost ip6-loopback
9     fe00::0 ip6-localnet
10    ff00::0 ip6-mcastprefix
11    ff02::1 ip6-allnodes
12    ff02::2 ip6-allrouters
13    ff02::3 ip6-allhosts

```

6.3.3 DNS (domain name system)

DNS és un servei de la capa d'aplicació que s'encarrega d'associar noms de domini públics a adreces IP d'Internet. El servei DNS no està centralitzat en cap fitxer ni servidor concret, sinó que és proporcionat per un conjunt de servidors distribuïts per tot el món que segueixen una ordenació jeràrquica o piramidal, en el cim de la qual hi ha tretze **servidors arrel**.

DNS és un servei fiable

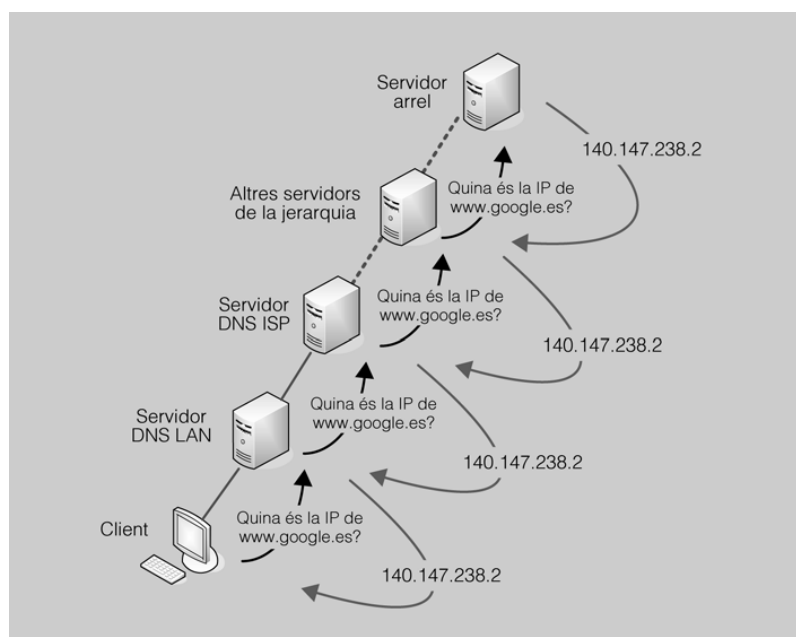
El fet que DNS sigui un servei distribuït entre servidors de tot el món permet garantir-ne el funcionament fins i tot quan alguns d'aquests servidors no estiguin disponibles per alguna raó.

Per tal de dirigir el trànsit de manera eficient, el servei DNS es divideix en tres components conceptuais:

1. Resolutors. Pertany a aquesta categoria qualsevol *host* d'Internet que necessiti esbrinar informació sobre noms de domini. El client resolutor o *resolver* està integrat en aplicacions TCP/IP, com ara HTTP. Quan s'introdueix en un navegador una adreça web, com ara <http://www.google.es>, el programari client HTTP inicia el servei resolutor per tractar d'esbrinar l'adreça IP associada a www.google.es. Si el *host* havia visitat aquesta pàgina recentment, és probable que l'adreça IP associada estigui encara enregistrada en la memòria del mateix *host*, per la qual cosa podrà ser recuperada ràpidament. Si no és així, el servei resolutor passarà la consulta al servidor de noms que el *host* tingui assignat.

2. Servidors de noms de domini (servidors DNS). Aquests servidors contenen bases de dades amb noms de domini i adreces IP associades, informació que proporcionen als resolutors (*resolvers*) quan reben una petició d'aquests. Si un servidor DNS no pot resoldre o esbrinar quina és l'adreça IP que correspon a un nom concret, li passa la consulta a un altre servidor DNS de nivell superior. Aquest procés continua fins a trobar un servidor DNS que conegui l'adreça IP associada al nom de domini especificat (figura 6.2).

FIGURA 6.2. Procés de resolució de noms de domini



3. Espai de noms de domini. Aquest concepte fa referència a la base de dades que conté totes les adreces IP d'Internet (adreces IP públiques) i els noms de domini corresponents. Cal notar que aquesta base de dades no està emmagatzemada en cap servidor concret, sinó que està distribuïda entre molts servidors diferents a Internet.

Qualsevol *host* que s'hagi de comunicar amb altres *hosts* via Internet ha de tenir un servidor DNS assignat. De fet, és freqüent trobar que un *host* té assignats dos servidors DNS, un DNS primari i un DNS secundari, de manera que si el servidor DNS primari falla el *host* pugui recórrer al secundari. Les adreces IP dels servidors DNS (primari i secundari) es poden configurar manualment o bé de manera automàtica mitjançant el servei DHCP.

6.3.4 DDNS (dynamic DNS)

DNS proporciona una manera ràpida i fiable de trobar l'adreça IP pública associada a un determinat nom de domini sempre que l'adreça IP d'aquest domini sigui estàtica, és a dir, no canviï de manera freqüent amb el temps. Actualment, però, molts usuaris d'Internet disposen d'adreces IP dinàmiques, és a dir, les adreces IP públiques que tenen assignades van canviant amb el temps de manera periòdica. Això no representa cap problema si l'usuari es limita a rebre i enviar missatges de correu electrònic o a navegar per Internet, però sí pot ser un problema si l'usuari vol instal·lar-se un servidor que sigui accessible des d'Internet (per exemple, un servidor HTTP de pàgines web o un servidor FTP).

Una possible solució a aquest problema és utilitzar **DDNS** (dynamic DNS), que consisteix a instal·lar al *host* de l'usuari un petit programa que detecta els canvis en l'adreça IP del *host* i els notifica automàticament a un proveïdor de serveis d'Internet prèviament escollit, el qual s'encarrega d'actualitzar la informació a tots els servidors DNS d'Internet en qüestió de minuts.

6.3.5 Servidors d'impressió i zeroconf

Els servidors d'impressió proporcionen la possibilitat de compartir impressores entre múltiples clients d'una xarxa.

Ja siguin servidors dedicats en exclusiva a oferir el servei d'impressió o bé estacions de treball que a més es fan servir per oferir l'accés a una impressora connectada a aquestes estacions, els servidors d'impressió solen tenir instal·lat un programari especial (o, si més no, un sistema operatiu de xarxa) que els permet gestionar les peticions d'ús dels serveis d'impressió per part dels diferents clients. Quan un servidor d'impressió rep una petició d'un client, passa la petició a la impressora si aquesta està lliure; si no ho està, o bé guarda la petició en un *buffer* o bé la guarda en un disc dur fins que la impressora queda lliure (aquest procés s'anomena gestió de cues o *spooling*).

Zeroconf (*zero configuration*) és un conjunt de protocols dissenyats per simplificar la configuració de nodes en una xarxa TCP/IP. Zeroconf assigna a cada node una adreça IP, és capaç de resoldre o esbrinar l'adreça IP associada a un nom de domini sense fer ús de servidors DNS, i permet descobrir serveis disponibles a la xarxa (serveis d'impressió, etc.).

Zeroconf davant NetBIOS

Abans de l'aparició de Zeroconf, la comunicació entre *hosts* directament connectats era possible quan totes dues eren màquines amb el mateix sistema operatiu (per exemple Windows amb protocol NetBIOS o Macintosh amb protocol AppleTalk), però no quan eren màquines amb diferents sistemes operatius.

Zeroconf permet la comunicació entre dos *hosts* directament connectats sense haver de configurar manualment les respectives adreces IP ni haver d'utilitzar servidors DHCP ni servidors DNS. Per fer això, Zeroconf fa ús del protocol **IPv4LL** (*IP version 4 link local*), que assigna de manera automàtica adreces IP privades en el rang 169.254.1.0 a 169.254.254.255.

IPv4LL és especialment útil amb impressores de xarxa: moltes impressores no disposen d'interfícies que permetin a l'administrador de la xarxa configurar fàcilment els seus paràmetres TCP/IP; per contra, si aquestes impressores suporten Zeroconf i IPv4LL, es poden connectar directament a la xarxa sense necessitat de fer cap mena de configuració addicional.

6.4 Altres protocols i serveis: SMTP, POP, Telnet, FTP, HTTP, NTP, etc

Els protocols de les capes superiors controlen el procés de donar format als paquets de dades d'acord amb les demandes dels usuaris. A continuació es presenten alguns d'aquests protocols:

- **FTP** (*file transfer protocol*). FTP permet als clients pujar i baixar fitxers a un servidor i d'un servidor que estigui executant un servei FTP. Aquest tipus de servei no depèn de cap sistema operatiu concret, motiu pel qual qualsevol client pot fer ús d'aquest protocol amb independència de quin sistema operatiu faci servir. Això converteix FTP en un servei que permet compartir fàcilment la informació entre clients de diferents plataformes. FTP fa ús de TCP per a les comunicacions entre clients i servidors, i utilitza paquets ACK (d'acusament de rebuda) durant la transferència.

La pila de protocols TCP/IP inclou una utilitat FTP que permet, sense necessitat d'instal·lar cap programa addicional, fer ús del servei FTP mitjançant la línia d'ordres. Per defecte, el servidor FTP utilitza el port 20 per a les connexions, mentre que els clients fan ús del port 21.

- **TFTP** (*trivial file transfer protocol*). TFTP s'utilitza quan la transferència d'un fitxer no requereix l'ús de paquets ACK. Aquest protocol es fa servir habitualment durant la configuració d'encaminadors. Pel que fa al seu funcionament, és semblant a FTP, i les diferències més importants entre tots dos són la velocitat (TFTP és més ràpid atès que no requereix paquets ACK)

i l'autenticació (TFTP no proporciona autenticació d'usuari). A més, TFTP només suporta transferència de dades unidireccional (a diferència d'FTP, que permet la transferència en les dues direccions alhora). Per defecte, el servei TFTP opera a través del port 69.

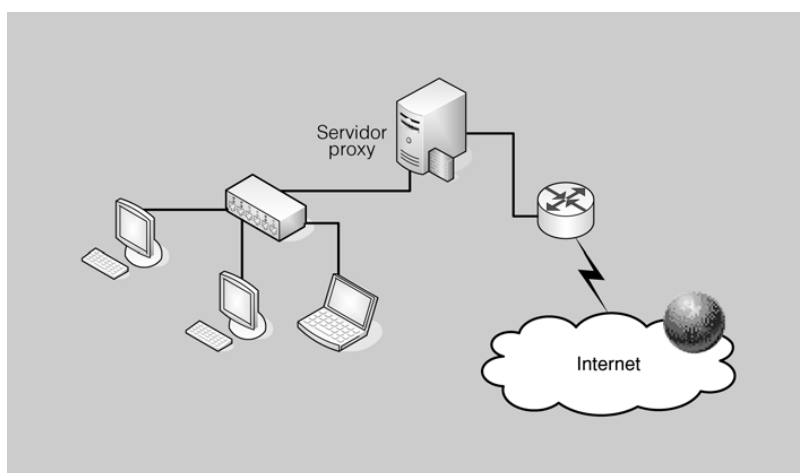
- **HTTP (*hypertext transfer protocol*)**. El protocol HTTP és el que gestiona la major part del trànsit que actualment circula per Internet. Quan un usuari sol·licita un recurs web, aquesta sol·licitud es fa mitjançant HTTP. Així, per exemple, quan s'escriu en un navegador l'adreça <http://www.ioc.cat>, es fa una crida al servei DNS perquè resolgui el nom de domini en una adreça IP. Quan aquesta adreça IP és resolta, s'envia una sol·licitud *get* al servidor web, el qual retorna una resposta *send* (totes dues són operacions del protocol HTTP). Aquest tipus de comunicació es produeix diversos cops durant una mateixa sessió en un lloc web. HTTP també fa ús del protocol TCP i opera, per defecte, en el port 80.
- **HTTPS (*hypertext transfer protocol secure*)**. HTTPS s'utilitza per fer transaccions (de dades) segures via web. HTTPS utilitza una tecnologia basada en certificats digitals amb la finalitat de garantir una autenticació mútua entre el client i el servidor que participen de la transacció. A més, HTTPS encripta tots els paquets de dades enviats durant la sessió, la qual cosa garanteix la confidencialitat de les dades. Per poder utilitzar HTTPS, un lloc web ha d'adquirir un certificat digital d'un proveïdor d'aquest tipus de serveis. HTTPS també utilitza TCP i, per defecte, opera en el port 443.
- **POP3 (*post office protocol v3*)**. POP3 és un servei de recepció de correu electrònic que proporciona a l'usuari accés a la seva carpeta *Inbox* d'entrada de missatges electrònics. POP3 s'encarrega de contactar amb el servidor de correu i de sol·licitar-li els nous missatges destinats al compte de l'usuari. Per tant, POP3 només presta serveis de recepció de missatges electrònics (no gestiona l'enviament de missatges). POP3 utilitza TCP i opera, per defecte, en el port 110.
- **SPOP3 (*secure post office protocol v3*)**. SPOP3 permet l'accés dels usuaris a la seva *Inbox* de correu electrònic mitjançant una connexió segura. SPOP3 es basa en l'ús de certificats digitals i en l'encriptació de les dades durant la sessió. SPOP3 fa ús del protocol TCP i, per defecte, opera en el port 995.
- **IMAP (*Internet message access protocol*)**. IMAP permet a un client de correu electrònic accedir a altres carpetes més enllà de la carpeta *Inbox* de correu entrant. Així, IMAP gestiona l'accés a les carpetes de missatges electrònics esborrats, missatges enviats, contactes, etc. Malgrat tot, tant IMAP com POP3 són serveis de recepció de correu electrònic (no gestionen enviament de correu electrònic). IMAP també utilitza TCP i, per defecte, fa ús del port 143.
- **SIMAP (*secure Internet message access protocol*)**. De manera anàloga a allò que passava amb SPOP3, SIMAP proporciona seguretat en la transmissió de missatges electrònics mitjançant l'ús de certificats digitals i de tècniques d'encriptació. SIMAP fa ús del protocol TCP i, per defecte, opera sobre el port 993.

- **SMTP (*simple mail transport protocol*)**. Els serveis POP3, SPOP3, IMAP i SIMAP només gestionen la recepció de correu electrònic. Per gestionar l'enviament de missatges es fa ús del protocol SMTP. Els missatges són enviats des d'un servidor SMTP a un altre servidor SMTP. Per poder fer aquesta operació, cada servidor SMTP fa ús del servei DNS. SMTP utilitza TCP i, per defecte, opera sobre el port 25.
- **TELNET (*terminal emulation*)**. Una aplicació Telnet fa ús del protocol TELNET per connectar un client a un servidor remot. El protocol TELNET proporciona comunicació bidireccional entre clients i servidors. Aquest protocol s'utilitza especialment en tasques d'administració remota d'un servidor mitjançant una consola d'ordres (aplicació Telnet) que s'està operant des del client. TELNET s'utilitza freqüentment per verificar el funcionament correcte de serveis remots (com ara SMTP, POP3 o IMAP) i per obrir ports en el servidor remot. Aquest protocol fa ús de TCP i, per defecte, opera sobre el port 23.
- **NNTP (*network news transfer protocol*)**. NNTP és un protocol que millora l'antic BBS (*bulletin board system*) per a la transferència d'informació entre clients mitjançant l'accés a grups de notícies o *newsgroups*, els quals contenen informació classificada per temes d'interès. NNTP utilitza el protocol TCP i, per defecte, opera sobre el port 119.
- **NTP (*network time protocol*)**. NTP s'utilitza per sincronitzar rellotges entre diferents ordinadors d'una xarxa. Aquest protocol, encara que molt simple, té la seva importància, ja que molts paquets tenen un temps de vida predeterminat que s'ha d'actualitzar constantment, per la qual cosa resulta fonamental que els diferents *hosts* per on el paquet passa estiguin sincronitzats. NTP fa ús del protocol UDP i, per defecte, opera sobre el port 123.
- **SNMP (*simple network management protocol*)**. SNMP és un protocol de gestió de xarxa que consisteix en dos components: l'agent SNMP (part client) i la consola de gestió SNMP (part servidor). La consola de gestió envia ordres get als agents SNMP per sol·licitar-los informació sobre la configuració de la xarxa, l'ús dels recursos, la configuració DHCP, la configuració DNS, la configuració WINS, la configuració de dispositius, els missatges d'error que s'han produït, etc. Per la seva banda, els agents SNMP responen a la petició mitjançant un missatge trap. Per motius de seguretat, els agents SNMP només contesten les peticions d'aquelles consoles de gestió que reconeixen com a membres de la mateixa xarxa. SNMP és un protocol que s'ha implementat en eines propietàries distintes. Així, per exemple, Hewlett Packard proporciona l'eina HP Open View, mentre que Microsoft proporciona l'eina SNMP Server. SNMP utilitza el protocol UDP per demanar la informació i, per defecte, opera sobre els ports 161 i 162.

6.5 Servidors intermediaris

Un **servidor intermediari** o *proxy* proporciona múltiples avantatges a l'hora de connectar una xarxa d'àrea local a Internet. D'una banda, l'intermediari pot fer les tasques d'un tallafocs (*firewall*), filtrant el trànsit que entra i surt de la xarxa local i augmentant, d'aquesta manera, la seguretat. D'altra banda, el servidor intermediari també pot proporcionar serveis de cau, la qual cosa permet incrementar el rendiment de la xarxa.

FIGURA 6.3. El servidor intermediari permet filtrar el trànsit des d'Internet i cap a Internet



En efecte, els servidors intermediaris poden inspeccionar tot el trànsit d'entrada i sortida de la xarxa (des d'Internet i cap a Internet) i determinar si alguna transmissió ha de ser filtrada o s'ha de restringir (figura 6.3). Atès que el servidor intermediari filtra les dades en els dos sentits (entrada i sortida), pot evitar l'accés des de la xarxa local a determinades pàgines web i també restringir l'accés no autoritzat d'usuaris externs a recursos o serveis de la xarxa local. Una funció addicional dels servidors intermediaris és la d'emascarar l'adreça IP dels *hosts* de la xarxa local, de manera que aquesta no sigui visible des d'Internet. Els servidors intermediaris poden ser servidors maquinari dedicats o simplement programari que s'està executant en una estació de treball.

Un dels servidors *proxy* més populars i més utilitzats és Squid.

Una altra aplicació habitual dels servidors intermediaris-cau és la seva capacitat per emmagatzemar la informació que és demanada amb més assiduitat. És freqüent que els diferents usuaris d'una mateixa xarxa local consultin les mateixes pàgines web. Quan una persona requereix una pàgina web concreta, l'intermediari connecta amb el lloc, descarrega la pàgina i la desa en memòria. Quan una segona persona torna a demanar la mateixa pàgina, l'intermediari li envia la que ha emmagatzemat en cau, i elimina així la necessitat de fer la sol·licitud a Internet, la qual cosa estalvia temps i trànsit de paquets a Internet. Algunes etiquetes *http* poden informar el servidor intermediari que certes pàgines o certs continguts són dinàmics (canvien sovint), informació que fa servir l'intermediari per incrementar

la freqüència en què actualitza la versió d'aquests continguts en la seva memòria cau.

6.6 Utilitats TCP/IP

En les xarxes on es fa servir el protocol TCP/IP, es pot fer ús d'un conjunt d'utilitats (petites aplicacions) que ajuden a identificar possibles problemes de funcionament o rendiment de la xarxa (dispositius de xarxa que no responen a les peticions, formació de colls d'ampolla en la xarxa, etc.). Entre les utilitats més destacades en entorns Windows (moltes d'elles també estan disponibles en entorns Unix/Linux), trobem les següents: Ping, Tracert, Arp, Netstat, Ipconfig/Ifconfig i Nslookup. A continuació es descriu breument cadascuna d'aquestes utilitats:

Opcions de Ping

Ping ofereix tota una sèrie d'opcions addicionals que permeten introduir algunes variants interessants. En la consola d'ordres de Linux, aquestes opcions es poden consultar fent un *man ping*. A Ms Windows es consulten amb *ping /?*.

- **Ping:** l'ordre *ping* es pot fer servir per comprovar la connectivitat entre el nostre *host* i un determinat *host* remot. En executar des d'un *host A* l'ordre *ping < adreça IP o nom d'un host B >* s'envien un conjunt de paquets de 32 bytes cadascun. Si els paquets arriben a la seva destinació (*host B*), llavors tots dos *hosts* es poden comunicar entre ells; en cas contrari (si els paquets enviats es perden pel camí), no hi ha connectivitat entre els *hosts*. Ping utilitza el protocol ICMP. Per comprovar si la targeta de xarxa del nostre propi *host* és operativa i té configurada la pila TCP/IP es pot fer un *ping 127.0.0.1* o, equivalentment, *ping localhost*.

```

1 ioc@ioc-laptop:/# ping -c 5 localhost
2
3 PING localhost (127.0.0.1) 56(84) bytes of data.
4 64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.068 ms
5 64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.057 ms
6 64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.062 ms
7 64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.060 ms
8 64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.066 ms
9
10 — localhost ping statistics —
11 5 packets transmitted, 5 received, 0% packet loss, time 4009ms
12 rtt min/avg/max/mdev = 0.057/0.062/0.068/0.009 ms

```

Opcions de Tracert/Traceroute

Tracert ofereix tota una sèrie d'opcions addicionals. En la consola d'ordres aquestes opcions es poden consultar fent un *man traceroute* a Linux o un *tracert /?* a Windows.

- **Traceroute (GNU/Linux) /Tracert (Windows):** aquesta utilitat permet veure la ruta que segueix un paquet fins a arribar a la seva destinació, és a dir: mostra l'adreça de cadascuna de les interfícies dels encaminadors pels quals passa el paquet TCP/IP. L'ordre que cal fer servir és *traceroute < adreça IP o nom DNS del host destinació >* (tracert en Windows). Aquesta ordre permet detectar l'existència de colls d'ampolla en una xarxa i identifica l'origen d'aquest problema. La primera columna de la sortida (*output*) resultant indica el nombre de salt, la segona mostra el nom o l'adreça IP del *host* corresponent i les tres columnes següents indiquen els temps associats a tres intents d'arribar fins al proper encaminador.

```

1 ioc@ioc-laptop:/# traceroute www.google.com
2
3 traceroute to www.google.com (74.125.230.82), 30 hops max, 60 byte packets
4  1 192.168.1.1 (192.168.1.1) 1.420 ms 5.337 ms 6.288 ms
5  2 192.168.153.1 (192.168.153.1) 45.247 ms 47.201 ms 49.165 ms
6  3 145.Red-80-58-117.staticIP.rima-tde.net (80.58.117.145) 51.126 ms
7 53.087 ms 55.045 ms
8  4 So2-0-0-0-grtbcntb1.red.telefonica-wholesale.net (84.16.6.65) 56.985 ms
9 58.918 ms 60.879 ms
10  5 Xe1-0-0-0-grtpartv2.red.telefonica-wholesale.net (84.16.13.134) 96.820
11 ms
12 So7-1-0-0-grtbcnes1.red.telefonica-wholesale.net (84.16.12.57) 64.800 ms
13 So4-0-0-0-grtbcnes1.red.telefonica-wholesale.net.12.16.84.in-addr.arpa
14 (84.16.12.201) 67.757 ms
15  6 Xe9-3-0-0-grtpartv1.red.telefonica-wholesale.net (213.140.49.153)
16 86.708 ms 58.744 ms Xe0-3-0-0-grtpartv1.red.telefonica-wholesale.net
17 (84.16.12.213) 66.798 ms
18  7 G00GLE-xe-9-0-0-0-grtpartv1.red.telefonica-wholesale.net (84.16.6.106)
19 84.733 ms G00GLE-xe-3-1-0-0-grtpartv1.red.telefonica-wholesale.net
20 (84.16.6.98)
21 86.714 ms G00GLE-xe-9-0-0-0-grtpartv1.red.telefonica-wholesale.net
22 (84.16.6.106)
23 84.633 ms
24  8 209.85.250.142 (209.85.250.142) 92.616 ms 98.570 ms 94.532 ms
25  9 64.233.175.115 (64.233.175.115) 86.546 ms 86.460 ms 86.456 ms
26 10 74.125.230.82 (74.125.230.82) 101.377 ms 98.354 ms 100.301 ms
27 ioc@ioc-laptop:/#

```

Opcions d'Arp

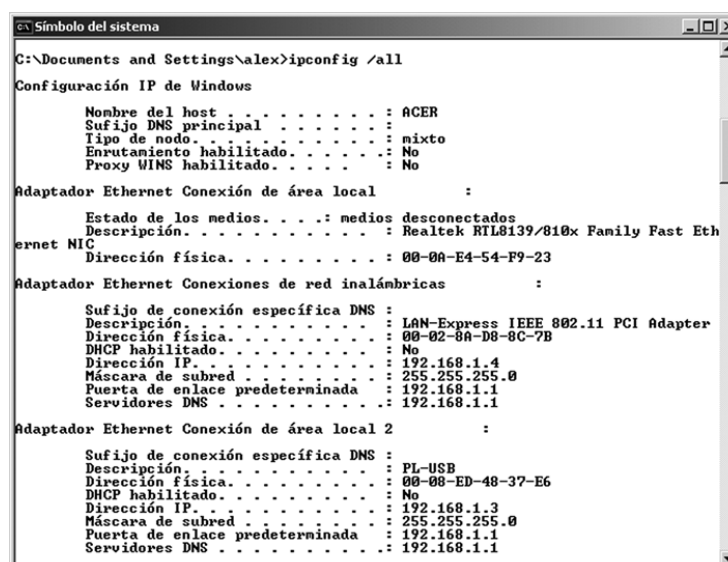
Arp ofereix tota una sèrie d'opcions addicionals. A la consola d'ordres aquestes opcions es poden consultar fent un *man arp* a Linux o *arp /?* a Windows.

- **Arp:** cada *host* que utilitza TCP/IP manté una taula ARP en la qual enregistra adreces IP i les corresponents adreces MAC associades. L'ordre *arp* permet visualitzar aquesta taula (adreces estàtiques i dinàmiques) i també afegir-hi entrades noves (adreces estàtiques). Els registres de la taula ARP tenen un temps de vida màxim (*time to live* o TTL) i, quan aquest expira, l'entrada corresponent és esborrada de la taula.

Les diferents opcions d'*Ipconfig* es poden consultar fent un *man ifconfig* o *ipconfig -?* en la consola de windows.

- **Ipconfig/Ifconfig:** aquesta utilitat permet veure la configuració TCP/IP (adreça IP del *host*, màscara de subxarxa, adreça IP del *gateway*, servidor DHCP, servidor DNS, etc.) associada a cadascuna de les targetes de la xarxa del *host*. L'ordre en sistemes Windows és *ipconfig*. En el cas de sistemes Unix/Linux, l'ordre és *ifconfig* (figura 6.4).

FIGURA 6.4. Ús de l'ordre ipconfig



Opcions de Netstat

Netstat ofereix tota una sèrie d'opcions addicionals. En la consola d'ordres aquestes opcions es poden consultar fent un *man netstat* a Linux o un *netstat /?* a Windows.

- **Netstat:** aquesta utilitat permet veure les connexions TCP/IP establertes i algunes estadístiques associades. L'ordre que s'ha de fer servir és *netstat*. La primera columna de la sortida (*protocol*) resultant indica el protocol utilitzat, la segona i tercera indiquen paquets enviat i rebuts, la quart columna indica el nom i port local, la cinquena columna indica el nom i port de destinació; finalment, la sisena columna indica l'estat de la connexió.

```

1 ioc@ioc-laptop:/# netstat
2   Conexiones activas de Internet (servidores w/o)
3
4   Protocolo Recv-Q Send-Q Dirección Local      Dirección Externa    Estado
5   tcp        38      0   ioc-laptop.lo:50551 www.dropbox.com:https CLOSE_WAIT
6   tcp        38      0   ioc-laptop.lo:51841 174.36.30.90-stat:https CLOSE_WAIT
7   tcp         0      0   ioc-laptop.lo:57128 wy-in-f17.1e100.n:https
8   ESTABLECIDO
9   tcp        38      0   ioc-laptop.lo:45816 75.126.115.38-sta:https CLOSE_WAIT
10  tcp         0      0   ioc-laptop.lo:60411 208.43.202.47-stati:www
11  ESTABLECIDO
12  udp        320     0   ioc-laptop.lo:39074 72.21.194.1:33486
13  ESTABLECIDO
14  udp        320     0   ioc-laptop.lo:49831 72.21.194.1:33488
15  ESTABLECIDO
16  udp         0      0   ioc-laptop.lo:52658 72.21.214.128:33491
17  ESTABLECIDO
18  udp         0      0   ioc-laptop.lo:56506 72.21.194.1:33491
19  ESTABLECIDO
20  udp         0      0   ioc-laptop.lo:33483 72.21.214.128:33492
21  ESTABLECIDO
22  udp        320     0   ioc-laptop.lo:46812 72.21.194.1:33487
23  ESTABLECIDO
24  udp        320     0   ioc-laptop.lo:57573 72.21.194.1:33490
25  ESTABLECIDO
26  udp        320     0   ioc-laptop.lo:45189 72.21.194.1:33489
27  ESTABLECIDO
28  udp        416     0   ioc-laptop.lo:52998 72.21.194.1:33484
29  ESTABLECIDO
30  udp        384     0   ioc-laptop.lo:35086 250.Red-80-58-61:domain
31  ESTABLECIDO
32  udp        320     0   ioc-laptop.lo:43278 72.21.194.1:33485
33  ESTABLECIDO

```

- **Nslookup:** aquesta utilitat permet demanar a un servidor DNS per l'adreça IP d'un *host* del qual es coneix el nom de domini, o bé a l'inrevés, demanar a un servidor DNS el nom de domini associat a una adreça IP coneguda.

```
1 ioc@ioc-laptop:/# nslookup www.google.com
2   Server:           80.58.61.250
3   Address:          80.58.61.250#53
4
5   Non-authoritative answer:
6   www.google.com canonical name = www.l.google.com.
7   Name:   www.l.google.com
8   Address: 74.125.230.83
9   Name:   www.l.google.com
10  Address: 74.125.230.82
11  Name:   www.l.google.com
12  Address: 74.125.230.81
13  Name:   www.l.google.com
14  Address: 74.125.230.80
15  Name:   www.l.google.com
16  Address: 74.125.230.84
17
18 ioc@ioc-laptop:/# nslookup www.muchomasdeporte.com
19   Server:           80.58.61.250
20   Address:          80.58.61.250#53
21
22   Non-authoritative answer:
23   Name:   www.muchomasdeporte.com
24   Address: 65.61.167.242
```