**Tema 3: Xarxes d’àrea local**

L’objectiu d’aquest tema és l’estudi de les xarxes d’àrea local (Local Area Networks, LAN). El desenvolupament d’aquest tipus de xarxes s’origina els anys 70 amb l’objectiu d’interconnectar de forma econòmica un nombre reduït de computadors, impressores i altres dispositius, en una àrea geogràfica petita, com és un edifici o un campus. Tot i que hi ha hagut moltes propostes i productes comercials per LANs, avui en dia la tecnologia dominant és ethernet. En aquest tema s’estudien alguns conceptes bàsics relacionats amb les LANs, fent èmfasi en l’estudi de les xarxes ethernet.

**4.1 Introducció a les LANs**

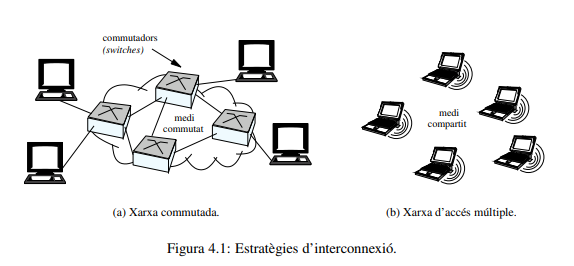
En els temes anteriors hem estudiat els protocols IP i TCP. Aquests protocols permeten la interconnexió heterogènia de xarxes: és a dir, permeten la connexió de hosts independentment de la xarxa física on estat connectats. L’única cosa que necessiten els protocols TCP/IP és disposar de xarxes físiques que siguin capaces de transportar datagrames. En aquest tema ens fixarem en les xarxes físiques.

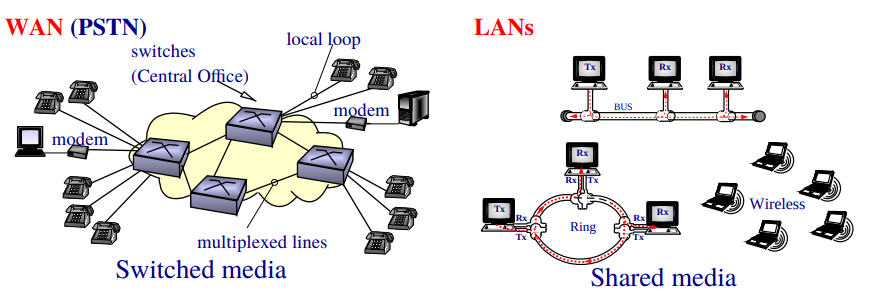
Si les classifiquem segons l’abast tenim:

* Wide Area Network, WAN (xarxes de gran abast): tenen com a condició de disseny poder cobrir una àrea geogràfica extensa (per exemple un país) i amb un número il·limitat (o molt gran) d’estacions. L’exemple més clar és la xarxa telefònica. Així doncs, la condició de disseny més important per a aquestes xarxes és l’escalabilitat.
* Local Area Network, LAN (xarxes d’àrea local): tenen com a condició de disseny la interconnexió d’un nombre limitat d’estacions en un àrea geogràfica petita, per exemple, un edifici. En aquest cas, l’escalabilitat no és tan important.

Segons les estratègies d’interconnexió, podem classificar les xarxes en:

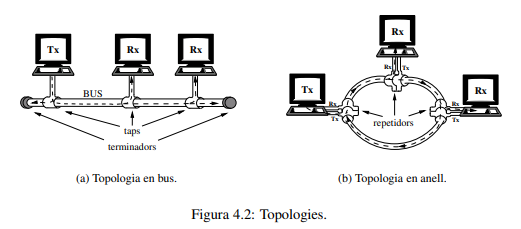
* Switched network (xarxa commutada): està formada per una interconnexió de “commutadors” que tenen com a objectiu encaminar la informació entre els dos nodes que es comuniquen (vegeu la figura 4.1(a)). El seu objectiu és, doncs, semblant a la dels routers. Ara, però, ens estem referint a dispositius dissenyats per a una xarxa física en concret, i el seu funcionament és típicament a nivell 2. L’avantatge més important d’aquest tipus de xarxa és la seva escalabilitat: a mesura que volem expandir la xarxa, simplement hi hem d’afegir més commutadors. Per aquest motiu, les WANs són sempre xarxes commutades. Un exemple és la xarxa telefònica.
* Multiaccess network (xarxa d’accés múltiple): l’inconvenient d’una xarxa commutada és que els commutadors poden encarir bastant la xarxa. Per això, típicament, les tecnologies LAN que s’han desenvolupat s’han basat en una aproximació més econòmica: l’accés múltiple. En una xarxa d’aquest tipus hi ha un medi compartit, com pot ser una transmissió ràdio (vegeu la figura 4.1(b)), un bus o un anell (com veurem més endavant). D’aquesta manera, quan l’estació transmissora envia un missatge, el reben tots els possibles destinataris, però només l’estació on va dirigida se’l queda i les altres el descarten. Amb aquesta aproximació ens estalviem els commutadors, però necessitem un protocol de “control d’accés al medi” (Medium Access Control, MAC) perquè les estacions que volen transmetre ho facin de forma ordenada.





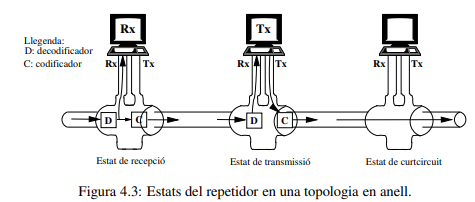
**4.2 Topologies**

Tal com s’ha explicat en la introducció, les tecnologies LAN que s’han desenvolupat en la pràctica es basen típicament en un medi compartit. Una possibilitat és fer servir l’espai lliure i una transmissió via ràdio, com es mostra en la figura 4.1(b). Aquesta possibilitat fins fa poc era massa cara i tradicionalment les LANs han fet servir medis cablejats. Una característica importat en el disseny de la LAN és la connexió o topologia de les estacions. Tot i que hi ha diverses topologies possibles (arbre, malla, estrella, bus i anell), les LANs que s’han desenvolupat en la pràctica s’han dissenyat normalment amb una topologia en bus o anell. Aquestes dues topologies s’expliquen a continuació.

****

**4.2.1 LAN en bus**

La figura 4.2(a) nostra una LAN amb topologia en bus. El bus pot consistir en un cable coaxial. Les estacions estan connectades al bus per uns taps que intercepten el bus. Quan una estació transmet, el senyal es propaga pel bus i el reben totes les estacions. En els extrems del bus hi ha unes resistències anomenades terminadors. Els terminadors eviten que el senyal es reflecteixi i provoqui echos que produirien interferències. L’exemple més rellevant de LAN en bus és Ethernet, que estudiarem en detall en la secció 4.6.

****

**4.2.2 LAN en anell**

La figura 4.2(b) nostra una LAN amb topologia en anell. Cada estació es connecta a l’anell amb un repetidor que intercepta l’anell. Els repetidors poden estar en tres estats (vegeu la figura 4.3):

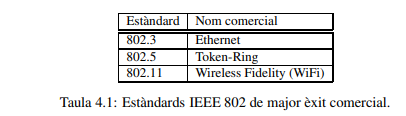
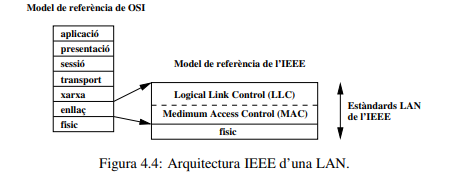
* Recepció: el repetidor decodifica el senyal i al cap d’un cert retard T = bits de retard / vt lliura els bits decodificats a l’estació que té connectada, i torna a codificar el senyal per enviar-lo anell avall.
* Transmissió: el repetidor decodifica el senyal i al cap d’un cert retard T = bits de retard / vt lliura els bits decodificats a l’estació que té connectada. Ara, però, transmet anell avall els bits que rep de l’estació.
* Curtcircuit: si no hi ha cap estació connectada (o si té alguna falla) el repetidor pot passar a un estat de curtcircuit. És com si el repetidor no hi fos.

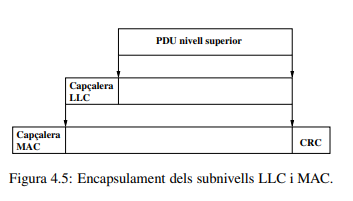
Exemples de xarxes LAN en anell són Token-Ring, desenvolupat per IBM i FDDI. Token-Ring ha estat la segona tecnologia amb èxit comercial després d’Ethernet. Actualment, però, ha quedat pràcticament substituïda per Ethernet. FDDI es va desenvolupar per poder cobrir una àrea geogràfica relativament extensa i a elevada velocitat. Està format per un anell dual de fibra òptica de fins a 100 km i 100 Mbps. Un dels dos anells serveix de tolerància a falles. Típicament FDDI s’ha fet servir com a backbone. Actualment també ha perdut mercat davant d’Ethernet, que, com veurem, ha desenvolupat estàndards a 100 Mbps i fins i tot a 1 Gbps.

**4.3 Arquitectura IEEE d’una LAN**

L’organisme capdavanter en l’estandardització de LANs ha estat l’IEEE. Els estàndards LAN desenvolupats per l’IEEE tenen el prefix 802. La taula 4.1 mostra els estàndards que han tingut un major èxit comercial.

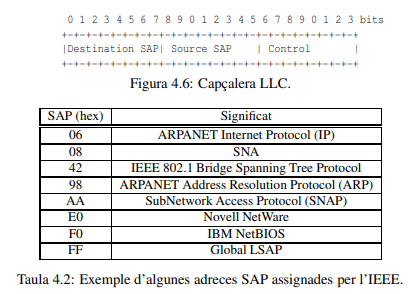
IEEE va decidir definir una interfície comú amb els nivells superiors per tots els seus estàndards LAN: IEEE 802.2 Logical Link Control (LLC) [12] 1 . D’aquesta manera, l’IEEE va definir el model de referència que mostra la figura 4.4. En aquest model de referència, el nivell d’enllaç¸ del model de referencia OSI es divideix en dos subnivells: **Logical Link Control (LLC)** i **Medium Access Control (MAC)**. La figura 4.5 mostra l’encapsulament d’aquest dos nivells i en les pròximes subseccions s’expliquen alguns detalls. L’acrònim PDU vol dir Protocol Data Unit. Aquest nom es va introduir en el model de referència OSI per referir-se a les estructures de dades que fa servir cada nivell. El CRC que afegeix el MAC serveix per al control d’errors.

****



**4.3.1 Logical Link Control (LLC)**

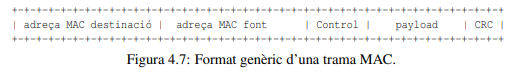
El subnivell Logical Link Control (LLC) defineix la interfície amb el nivell superior. L’estàndard defineix tres tipus de serveis: (i) No orientats a la connexió, (ii) orientat a la connexió i (iii) confirmats i no orientat a la connexió. La figura 4.6 mostra la capçalera LLC. L’estàndard es refereix als camps **Destination SAP (DSAP) i Source SAP (SSAP)** com a “adreces LLC”, tot i que tenen poc a veure amb el concepte d’adreça que hem vist fins ara. L’acrònim SAP vol dir Service Access Point. Aquest nom es va introduir en el model de referència OSI per referir-se al “punt de comunicació” entre nivells. En el cas concret de l’estàndard LLC, el SAP té un significat anàleg al camp de protocol de la capçalera IP: identifica el nivell superior on ha de lliurar-se el contingut de la trama. La taula 4.2 mostra algunes de les adreces assignades en aquest camp. El camp de control identifica el tipus de comanda. Segons el tipus, pot tenir un o dos bytes.



SNAP: utilitzat en TCP/IP.

**4.3.2 Medium Access Control (MAC)**

A diferència del subnivell LLC, el subnivell Medium Access Control (MAC) és diferent per a cada tecnologia LAN. El seu objectiu és regular l’accés al medi compartit. En la secció 4.6 estudiarem en detall el MAC d’Ethernet. L’estructura de dades (PDU) de nivell MAC s’anomena “trama” i és el que finalment es transmetrà per la xarxa física. La figura 4.7 mostra el format general d’una trama MAC. Les adreces MAC font i destinació identifiquen respectivament l’estació que transmet i l’estació a qui va dirigida la trama. El camp de control porta informació addicional pel funcionament del protocol. El payload porta la PDU de nivell superior (és un camp de mida variable). Finalment, el camp CRC porta un control d’errors de tota la trama (de forma anàloga al checksum d’un segment TCP).



**4.4 Tipus de MAC**

Tal com s’ha introduït en la secció 4.3.2, l’objectiu del MAC és regular l’accés de les estacions al medi compartit. A més, és desitjable que el protocol estigui distribuït: és a dir, que no faci falta un “àrbitre regulador” per controlar l’accés. El protocol MAC també ha de ser eficient i equitatiu (no hi ha d’haver estacions privilegiades que puguin aconseguir velocitats de transmissió majors que les altres). En la pràctica s’han fet servir dues estratègies per al disseny de protocols MAC:

* Pas de testimoni (MAC per pas de testimoni): en aquest tipus de MAC l’accés està regulat per un “testimoni” (**token**). L’estació que té el testimoni és la que pot transmetre i les altres han de restar en silenci. El testimoni es va passant entre les estacions, típicament després de la transmissió d’una trama l’estació passa el testimoni. Una analogia seria un grup de persones que es van passant el torn de paraula per poder xerrar.
* Accés al medi aleatori (MAC aleatoris): en aquest tipus de MAC no existeix testimoni. En canvi, les estacions proven de transmetre, i si es dona la mala sort que dues ho fan simultàniament (quan això passa es parla d’una **“col·lisió”**), aleshores s’esperen un temps aleatori (anomenat “**temps de backoff**”) i ho tornen a intentar. Perquè el MAC sigui equitatiu, totes les estacions han de tenir el mateix generador pel temps de backoff. Així doncs, en un MAC aleatori hi ha una probabilitat no nul·la que dues estacions col·lisionin. Les col·lisions, però, no són un mal funcionament de la xarxa, sinó que tenen una funció semblant a la del token en una xarxa per pas de testimoni.

MACs per pas de testimoni: LANS amb topologia en anell, exemples: FDDI i Token-Ring.

MACs aleatoris: LANs amb topologia en bus, exemples: Ethernet.

Tot i això, la topologia i el MAC no estan lligats. Per exemple, l’estàndard IEEE-802.4 (Token-Bus) especifica un MAC per pas de testimoni per una xarxa amb topologia en bus. Aquest estàndard, però, no ha arribat a tenir èxit comercial. A causa de la importància d’Ethernet (avui en dia acapara el mercat de LANs) la resta del tema el dedicarem a estudiar els MACs aleatoris i en particular Ethernet.

**4.4.1 Carrier Sense Multiple Access (CSMA)**

La baixa eficiència d’Aloha es pot millorar en alguns casos. Suposem que els retards de propagació són petits en comparació amb el temps de transmissió de la trama. Si una estació vol transmetre, i ho fa immediatament (com faria Aloha) provocarà amb molta probabilitat una col·lisió si el medi estava ocupat. CSMA consisteix a escoltar el medi abans de transmetre. Si el medi està lliure, l’estació transmet immediatament; si està ocupat, aleshores l’estació s’espera que el medi quedi lliure abans de transmetre. Igual que en Aloha, en CSMA també hi ha confirmacions, i la seva absència s’identifica amb una col·lisió. En aquest cas, la trama s’intenta retransmetre després d’un temps de backoff. En cas que el medi estigui ocupat, hi ha dues estratègies:

* CSMA 1 persistent: quan l’estació que vol transmetre veu que el medi s’allibera, aleshores transmet immediatament. Es diu “1 persistent” perquè l’estació transmet amb probabilitat 1 quan veu el medi lliure. Aquest mecanisme té l’inconvenient que si hi ha diverses estacions que estan esperant (o l’estació que transmet té més trames per transmetre), aleshores es produirà una col·lisió amb probabilitat 1 quan acabi la transmissió que hi ha en curs.
* CSMA no persistent: en aquest cas, l’estació que vol transmetre no transmet amb probabilitat 1. En canvi, quan el medi s’allibera s’espera un temps aleatori (diferent del backoff que hi ha després d’una col·lisió) i repeteix l’algorisme CSMA no persistent.

**4.5 Ethernet**

A mitjans dels anys 1970, Bob Metcalfe va dissenyar un protocol per interconnectar els computadors de l’empresa Xerox on treballava. Metcalfe es va basar en el protocol Aloha per al seu disseny. Al protocol que va dissenyar li va posar el nom de “Ethernet”, en referència a la idea que es tenia antigament que hi havia una substància (l’ether) que omplia l’espai i per on es propagaven les ones electromagnètiques. Actualment Ethernet s’ha convertit amb la tecnologia LAN que més es fa servir. A causa de la seva importància, en la resta d’aquest tema l’explicarem en detall.

**4.6.1 Trames Ethernet**

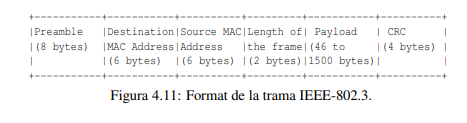
En la pràctica es fan servir dos formats de trames Ethernet: el format **Ethernet II o DIX** i el format **IEEE802.3**. Els dos formats són compatibles i es poden fer servir simultàniament. L’explicació de l’existència dels dos formats és la següent: després del disseny de Metcalfe, un consorci format per les empreses Digital, Intel i Xerox (DIX) va comercialitzar les primeres targes Ethernet amb el format de les trames que es coneix com Ethernet II o DIX. Més tard, l’IEEE va publicar l’estàndard 802.3 amb el mateix protocol, però un petit canvi en el format de les trames per fer-ho coherent amb l’estàndard 802.2, que en l’IEEE és comú a tots els MACs.

La figura 4.10 mostra el format de les trames Ethernet II o DIX. En el cas de fer servir el format DIX, no es fa servir el subnivell LLC (vegeu la secció 4.3). El significat dels camps és el següent:

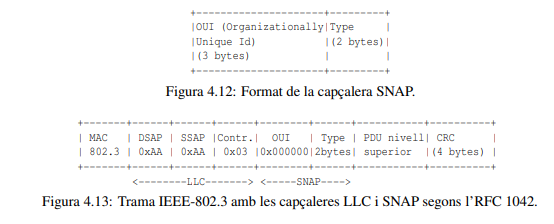
* Preàmbul: serveix per sincronitzar les targes en la recepció de la trama.
* Adreces destinació i font: identifiquen l’estació transmissora i receptora. Tenen 6 bytes (48 bits) i són úniques per cada tarja: l’organisme d’estandardització IEEE subministra blocs d’adreces a les empreses que en fabriquen per garantir la seva unicitat.
* Tipus: identifica el protocol de nivell superior (IP, ARP, etc.). En l’RFC 1700 [36, secció “ETHER TYPES”], hi ha el valor que ha assignat l’IETF a aquest camp per a cada tipus de protocol. Per exemple, per un datagrama IP es fa servir el valor 0x0800.
* Payload: camp d’informació. Pot tenir entre 46 i 1500 bytes. El motiu que hi hagi una mida mínima s’explica en la secció 4.6.3. Si el nombre de bytes d’informació és inferior a 46, Ethernet afegeix bytes addicionals fins a 46. En aquest cas, hi ha d’haver algun mecanisme que permeti descobrir els bytes que s’han afegit. Per exemple, en el cas de portar un datagrama IP, això es pot deduir a partir del camp header length de la capçalera IP.
* CRC: Serveix per a la detecció d’errors.

La figura 4.11 mostra el format de les trames IEEE-802.3. Comparant les figures 4.10 i 4.11 podem veure que l’única diferència és el camp de tipus, que en les trames 802.3 és un camp amb la mida del payload de la trama (length). A causa d’aquest camp, amb 802.3 no cal cap mecanisme addicional per poder descobrir els bytes que pot haver afegit el MAC per arribar al mínim de 46 (el camp de length no els compta). Per exemple, si la PDU de nivell superior té només 30 bytes, aleshores el camp de length té el valor de 30, mentre que el camp de payload tindrà 46 bytes. Per poder fer compatibles els dos formats, els valors del camp de tipus que es fa servir en les trames DIX és sempre major de 1500. D’aquesta manera, quan el driver d’una estació rep una trama amb un valor del camp de tipus menor o igual a 1500, aleshores interpreta que la trama rebuda té el format 802.3; altrament, identifica que té el format DIX.

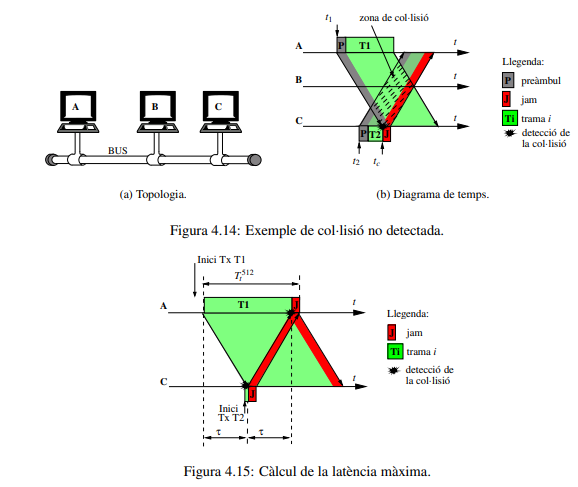




Cal recordar que tots els estàndards LAN de l’IEEE fan servir el subnivell LLC (vegeu la secció 4.3). Per tant, quan es fa servir 802.3, el protocol de nivell superior hauria de venir identificat pels camps DSAP i SSAP del nivell LLC (vegeu la secció 4.3). Això representa un problema addicional de cara a fer compatibles 802.3 amb DIX: els camps SAP del LLC tenen només 1 byte, mentre el camp de tipus de DIX en té 2. De manera que hi ha protocols que tenen un valor assignat per al camp tipus en les trames DIX que no tenen una adreça SAP assignada (perquè no hi ha tantes adreces SAP disponibles). Per solventar alguns problemes d’interoperabilitat entre protocols (com l’explicat anteriorment), l’IEEE va definir una extensió del LLC anomenada Sub-Network Access Protocol [14] (SNAP). L’adreça SAP d’aquest protocol és 0xAA (vegeu la taula 4.2). Quan es fa servir el protocol SNAP, després de la capçalera LLC s’afegeix la capçalera que mostra la figura 4.12. El camp Organizationally Unique Identifier (OUI) de la trama SNAP representa l’organisme que defineix els protocols i el camp Type identifica un protocol específic.



L’RFC 1042 [28] va especificar l’ús del protocol SNAP per a la integració de TCP/IP en una xarxa Ethernet 802.3. En aquest cas el camp de control LLC porta el valor 0x03 (Unnumbered Information), el camp OUI de la capçalera SNAP es posa tot a zeros i el camp Type de la capçalera SNAP porta el valor que s’especifica en l’RFC 1700 [36] (igual que el camp “tipus” de les trames DIX). La figura 4.13 mostra com queda una trama 802.3 amb les capçaleres LLC i SNAP segons les indicacions d’aquest RFC. Aquestes dues capçaleres ocupen 8 bytes, per tant, la PDU de nivell superior pot tenir fins un màxim de 1492 bytes. Així doncs, l’opció MSS que proposarà el protocol TCP durant el three-way-handshaking en una xarxa Ethernet amb un driver que transmet trames 802.3 serà de 1452 bytes. En canvi, si el driver transmet trames DIX, l’opció MSS serà de 1460 bytes.



**4.6.2 Protocol MAC Ethernet**

Al protocol que fa servir Ethernet se’l coneix com **CSMA with Collision Detection (CSMA/CD)**. La idea és la mateixa que el CSMA, però ara l’estació continua escoltant el medi mentre transmet la trama i deixa de transmetre immediatament si detecta una col·lisió. Si no es detecta col·lisió durant la transmissió de la trama, aleshores s’assumeix que no hi ha hagut col·lisió. Per tant, no cal que l’estació receptora enviï una confirmació. L’organisme d’estandardització IEEE ha estandarditzat Ethernet amb l’estàndard IEEE-802.3 [15]. Els detalls del protocol són els següents:

1. Transmissió: CSMA/CD 1 persistent. Entre trames, però, el medi ha d’estar sense senyal durant un temps major o igual a l’anomenat Inter Packet Gap (IPG), que l’estàndard fixa en 12 bytes (96 bits). Per tant, si una estació vol transmetre diverses trames consecutives, s’espera un IPG després de cada transmissió. Igualment, abans de començar una transmissió una estació espera (si cal) que hagi passat al menys un IPG des de l’últim bit rebut.
2. Col·lisió: quan hi ha una col·lisió, es deixa de transmetre la trama immediatament i es transmet un “senyal de jam” (jam en anglès vol dir “embús”). Aquest senyal té una mida de 32 bits i ha de ser tal que els bits enviats no puguin ser mai una trama vàlida. Després l’estació espera un temps de backoff i torna al punt 1.
3. El temps de backoff (tbackoff) és igual a [15, secció 4.2.3.2.5]:



On:

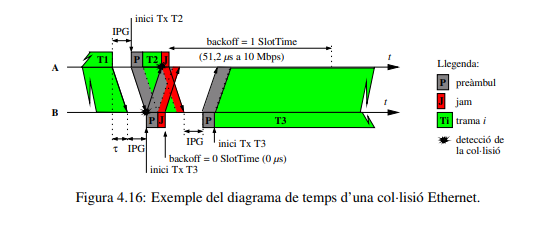
* (512) t és el temps de transmissió de 512 bits (per exemple: 51,2 µs a 10 Mbps). L’estàndard anomena aquest temps slot time (temps de ranura).
* n és un número enter aleatori uniformement distribuït en {0, 2min {N,10} - 1}. N ≥ 1 és el nombre de retransmissions de la trama.

Per exemple, a 10 Mbps, si hi ha una col·lisió es tria un backoff que pot valer 0 o 51,2 µs. Si torna a haver-hi col·lisió, es tria un backoff que pot valer: 0; 51,2; 102,4 o 153,6 µs i així successivament. Això es repeteix un màxim de 16 vegades. Si la retransmissió número 16 torna a col·lisionar, la trama es descarta.

Observacions:

* l’IPG serveix per donar temps a les estacions o detectar el medi lliure. Serveix també per fer el sincronisme de trama (quan el medi queda sense senyal, les targes interpreten que hi ha el final de recepció de la trama).
* Si una estació té una trama llesta per transmetre, quan s’allibera el medi espera un IPG i inicia la transmissió de la trama, independentment que en l’instant d’iniciar la transmissió el medi estigui ocupat o no [15, secció 4.2.3.2.1]. D’aquesta manera, dues estacions que esperen que s’alliberi el medi per transmetre, col·lisionaran i activaran el mecanisme de backoff. Si no es fes així, una estació que tingués un IPG lleugerament més petit bloquejaria les altres estacions i l’accés no seria equitatiu.
* El jam serveix perquè cap estació pugui detectar una trama que ha col·lisionat com a una trama correcte. El jam simplement són uns bits que fan que el control d’errors de la trama doni una trama sempre errònia i, per tant, totes les targes descartaran la trama.
* Si la col·lisió es detecta durant la transmissió del preàmbul de la trama (vegeu la secció 4.6.1), el senyal de jam es comença a transmetre immediatament després del preàmbul (és a dir, el preàmbul no s’interromp per començar a transmetre el jam.
* L’algorisme de backoff genera un número aleatori amb mitjana que es multiplica per dos cada vegada que es retransmet la mateixa trama. D’aquesta manera s’intenta eliminar el problema d’inestabilitat que hi pot haver en els MACs aleatoris.
* Si dues estacions volen transmetre simultàniament de forma sostinguda, després de cada transmissió hi haurà sempre una col·lisió: perquè l’estació que ha acabat espera un IPG i transmet de nou i l’altra fa una espera 1-persistent. La primera estació que triï un backoff més petit serà la que aconseguirà transmetre després de la col·lisió. Això passarà de mitjana un 50% de vegades per a cada estació, perquè l’algorisme de backoff és el mateix per a totes les estacions. Així doncs, les dues estacions es repartiran el medi de forma equitativa.

La figura 4.16 mostra el diagrama de temps explicatiu del que passa en una col·lisió Ethernet. En el diagrama, l’estació A està transmetent una trama (T1) i l’estació B té una trama llesta per transmetre (T3). Cada bit transmès per l’estació A arriba a B després del retard o latència τ entre les dues estacions. Suposem que l’estació A té més trames per transmetre (T2). Quan A acaba la transmissió, les dues estacions fan una transmissió 1-persistent, és a dir, quan veuen el medi lliure s’esperen un IPG i comencen a transmetre. Això provocarà una col·lisió. L’estació B detectarà la col·lisió mentre transmet el preàmbul de la trama T3. Així doncs, immediatament després de transmetre el preàmbul, l’estació B envia el senyal de jam. Igualment, l’estació A detectarà una col·lisió quan comenci a rebre el preàmbul de l’estació B. És possible que l’estació A ja hagi començat a transmetre T2 (com mostra la figura). En aquest cas, l’estació A deixa de transmetre immediatament i transmet el senyal de jam. Després de detectar la col·lisió, cada estació calcularà un temps de backoff, triant aleatòriament entre {0, 1} slot times. Suposem que l’estació B tria 0 i l’estació A tria 1. Si les dues estacions triessin el mateix número, aleshores tornaria a haver-hi una col·lisió i les estacions tornarien a provar triant entre {0, 1, 2, 3} slot times. Després de transmetre el senyal de jam, les dues estacions esperen el temps de backoff que han calculat i tornen a escoltar el medi. L’estació B el trobarà lliure, per tant, iniciarà la transmissió de T3 després d’un IPG. Quan l’estació A escolti el medi, el trobarà ocupat amb T3. Per tant, s’esperarà acabar de rebre la trama i farà la transmissió 1-persistent de T2 tot seguit.



**4.6.3 Mida mínima d’una trama Ethernet**

Tal com s’ha explicat en la secció 4.6.2, en CSMA/CD s’espera que l’estació que transmet la trama detecti si ha col·lisionat o no. Per això, l’estació receptora no envia confirmació. Aquesta condició introdueix una restricció en la mida mínima que poden tenir les trames, com veurem a continuació. Suposem que en la topologia de la figura 4.14(a), les estacions A i C comencen a transmetre una trama gairebé de forma simultània (en els instants t1 i t2) cap a l’estació B. Tal com hem vist en la secció 4.6.2, aquesta simultaneïtat passarà sovint en la xarxa: cada vegada que dues estacions esperen que s’alliberi el medi per transmetre. La figura 4.14(b) mostra el diagrama de temps de la transmissió de les dues trames. Tal com mostra la figura 4.14(b), al propagar-se les dues trames es produeix una “zona de col·lisió”. Qualsevol estació que escolta en aquesta zona (com són les estacions B i C) detecten una col·lisió. Quan l’estació C detecta la col·lisió, atura la transmissió de la seva trama i envia el senyal de jam. L’estació A, en canvi, queda fora de la zona de col·lisió perquè envia una trama massa petita i ja ha acabat la transmissió de la seva trama abans de començar a rebre la trama enviada per l’estació C. Això farà que l’estació C retransmeti la trama que ha col·lisionat, però no l’estació A. Així doncs, cal assegurar que la mida de les trames enviades permeti detectar sempre les col·lisions. Del raonament anterior podem deduir que hi ha una relació entre la trama mínima que es pot transmetre i la latència màxima de la xarxa.

És a dir, com més gran sigui la trama mínima que es pugui transmetre, més gran podrà ser la latència màxima que hi podrà haver en la xarxa perquè no hi hagi col·lisions no detectades. L’estàndard Ethernet fixa la mida mínima de la trama (sense el preàmbul) a 64 bytes (512 bits). L’estàndard 802.3 [15] anomena aquest temps slot time (temps de ranura). D’aquí que descomptant les adreces (2×6 bytes), camp type/leght (2 bytes) i CRC (4 bytes) queden els 46 bytes que ha de tenir com a mínim el camp de payload. La xarxa ha de dissenyar-se perquè sempre es pugui detectar una col·lisió al transmetre una trama de mida mínima. En concret, l’estàndard 802.3 [15, secció 4.2.3.2.3] diu literalment: the slot time shall be larger than the sum of the Physical Layer round-trip propagation time and the Media Access Layer maximum jam time. És a dir, si el round-trip és de 2τ segons, aleshores ha de complir-se: Tt(512) > 2τ+Tjam.

On Tjam és el temps de transmissió del jam (3,2 µs a 10 Mbps). A continuació intentarem justificar la relació anterior. En la justificació no tindrem en compte el preàmbul de les trames. Si el tinguéssim en compte la condició no seria tan restrictiva. És possible que no tenir en compte el preàmbul sigui una marge de seguretat introduït per l’estàndard. En la deducció també tindrem en compte que l’estàndard diu que la trama de mida mínima ha de ser un límit superior del fragment generat per una trama que ha col·lisionat [15, secció 4.2.3.2.3]. És a dir, en cas de col·lisió, abans del temps de transmissió d’una trama de mida mínima, l’estació ha d’haver tingut temps de transmetre el jam.

Suposem que en la topologia de la figura 4.14(a), la latència màxima és de τ segons. És a dir, el retard entre les dues estacions més allunyades (A i C) és de τ segons (el round-trip serà 2τ). Suposem que aquestes dues estacions transmeten una trama (vegeu la figura 4.15). El cas més desfavorable és que l’estació C comenci a transmetre just abans de començar a rebre la transmissió de A: és a dir, τ segons més tard (això és juntament el que passa en l’exemple de la secció 4.6.2). Perquè l’estació A detecti la col·lisió, ha de continuar transmetent fins que arriba la transmissió de C: és a dir, τ segons més. D’aquí deduïm que si el temps de transmissió d’una trama de mida mínima és Tt(512), aleshores perquè no hi pugui haver col·lisions no detectades ha complir-se que: Tt(512) > 2τ. Si en aquest temps, a més, volem que l’estació A tingui temps de transmetre el jam (com diu l’estàndard), aleshores obtenim la desigualtat (4.6).

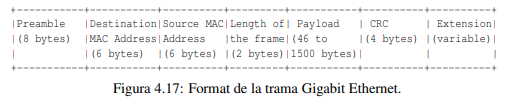
El temps Tt(512) es coneix amb el nom de “finestra de col·lisió” i mesurat en bits val 512 bits (en segons és 512/vt). El nom és degut al següent motiu. Suposem que una estació envia una trama de mida major a 64 bytes. Una conseqüència de l’equació (4.6) és que després d’un temps igual a Tt(512) t no és possible que l’estació detecti una col·lisió. Altrament, voldria dir que l’equació (4.6) no es compleix. La col·lisió d’una trama després d’haver passat la finestra de col·lisió és una indicació de retards excessius en la xarxa. Quan això es produeix es parla d’una late collision i algunes targes ho registren. Per exemple, en un router cisco la comanda show interface d’una interfície Ethernet dona entre altres la següent informació: 0 babbles, 0 late collision, 143 deferred. El significat és el següent: babbles (balbucejar) es refereix al nombre de cops que el temporitzador de la funció de jabber (parlotejar) ha expirat (vegeu la secció 4.6.5); late collision es refereix al nombre de cops que la tarja ha mesurat aquesta condició; deferred (posposat) es refereix al nombre de cops que el primer intent de transmissió d’una trama s’ha posposat perquè el medi estava ocupat.

El fet de fixar la mida mínima de les trames en 512 bits implica que la recepció d’una trama vàlida de mida inferior és una condició d’error: voldria dir que la tarja que l’ha enviat no controla correctament la transmissió de trames de mida mínima. Aquest tipus d’error s’anomena runt (en anglès vol dir animal de mida anormalment petita). En la pràctica, és normal que en una xarxa Ethernet hi hagi trames inferiors a 512 bits: les que resulten d’una col·lisió. Les trames que col·lisionen, però, tindran el CRC incorrecte i es descartaran. Podem veure que el slot time que es fa servir en el càlcul de temps de backoff (equació (4.5) és justament la finestra de col·lisió (Tt(512)). El motiu és assegurar que dues estacions que triïn números aleatoris diferents pel càlcul del backoff no col·lisionin.

Observació: tal com s’explica en la secció 4.6.5, hi ha nombrosos estàndards de nivell físic Ethernet amb diferents velocitats de transmissió. La restricció explicada anteriorment és valida només per als estàndards a 10 i 100 Mbps (coneguts comercialment com Ethernet i Fast Ethernet). Hi ha estàndards Ethernet a 1 Gbps (coneguts com a Gigabit Ethernet) on l’equació 4.6 introdueix una limitació massa restrictiva per la latència. Per exemple, per una velocitat de propagació de 2 · 108 m/s i suposant que la latència només depèn de la propagació en el medi, per complir l’equació 4.6 la distància màxima D d’un segment Gigabit Ethernet seria de:

(512−32)bits/109 bps > 2D/(2 · 108m/s)

És a dir: D < 48 m. Com que es desitja tenir segments d’almenys 100 m, en els estàndards Gigabit Ethernet la mida mínima de la trama canvia. Per exemple, en l’estàndard 1000BaseT la mida mínima (sense incloure el preàmbul) és de 512 bytes (en comptes dels 512 bits d’Ethernet). Per mantenir la compatibilitat amb els estàndards anteriors, en 1000BaseT s’ha definit el format de trama que mostra la figura 4.17. Podem veure que l’única diferència amb el format Ethernet (vegeu la figura 4.11), és que s’ha afegit el camp Extension. En aquest camp s’afegeixen (si és necessari) els bytes addicionals que permeten arribar a la mida mínima de 512 bytes. Aquests bytes es transmeten amb una codificació especial (carrier extension symbols) que permet distingir-los en la NIC que rep la trama. En mode full duplex no hi ha col·lisions (vegeu la secció 4.6.4). Per tant, no és necessari introduir la restricció de la trama mínima explicada en aquest apartat. Per exemple, en mode full duplex, Gigabit Ethernet no fa servir els extension symbols.

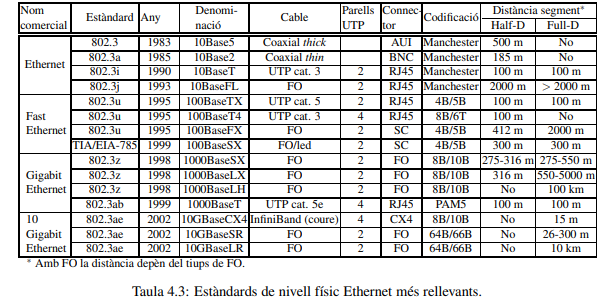


**4.6.4 Funcionament full duplex**

Tal com s’explica en la pròxima secció, els estàndards Ethernet que es fan servir en l’actualitat són amb cable UTP o fibra òptica. Amb fibra òptica i en la majoria dels casos on es fa servir UTP, es fan servir línies diferents per a la transmissió i recepció. En aquest casos, la col·lisió es detecta perquè es rep senyal per la línia de recepció mentre s’està transmetent per la línia de transmissió. En els estàndards Ethernet que fan servir línies diferents per a la transmissió i recepció, si es connecten dues targes (per exemple, dues estacions amb un cable creuat o una estació directament a un switch), aleshores és possible la transmissió i recepció simultànies. Per aquest motiu, hi ha targes Ethernet que suporten el mode de funcionament full duplex. Amb aquest mode de funcionament es desactiva el mecanisme d’accés CSMA/CD, ja que es possible transmetre i rebre simultàniament. Per tant, amb mode de funcionament full duplex, una línia 10BaseT, per exemple, podrà transmetre i rebre simultàniament aproximadament a 10 Mbps. Les targes que no estan en mode full duplex es diu que estan en mode half duplex. Les targes que suporten el mode de funcionament full duplex tenen un mecanisme d’autonegociació, de tal manera que si es connecten a una tarja que no ho suporti, passaran al mode de funcionament half duplex. Un altre avantatge del mode full duplex és que al no produir-se col·lisions, deixa d’haver-hi el problema de la trama mínima. Per tant, l’equació (4.6) ja no és necessari que es compleixi. Per aquest motiu, en mode full duplex i fibra òptica es poden fer servir segments de longitud de l’ordre de kilòmetres (l’atenuació és el factor que limita la distància màxima). Com que hi ha d’haver línies separades per transmetre i rebre, no tots els estàndards Ethernet poden funcionar en mode full duplex. La taula 4.3 indica quins ho permeten. Un hub tampoc pot tenir aquest mode de funcionament. Això és perquè el senyal que rep per la línia d’entrada un port ha d’enviar-lo per les línies de sortida de tots els altres ports. Per tant, si rep senyal per més d’una línia d’entrada, no podrà enviar simultàniament aquests senyals per les línies de sortida de tots els altres ports.

**4.6.5 Nivell físic Ethernet**

Hi ha nombrosos estàndards Ethernet de nivell físic. La taula 4.3 mostra els més rellevants. La revisió [15] de l’estàndard 802.3 inclou (entre altres) l’especificació de tots els estàndards de la taula 4.3. També hi ha estàndards Ethernet amb fibra òptica, que permeten cobrir distàncies majors per la seva baixa atenuació (vegeu el tema 5). La denominació “XBaseY” té el següent significat: “X” fa referència a la velocitat de transmissió en Mbps. La paraula “Base” fa referència a que la codificació és en “banda base” (vegeu el tema 5). Finalment, “Y” pot tenir diversos significats: si és un número fa referència a la distància màxima (aproximada) del segment en centenar de metres, altrament fa referència al tipus de medi de transmissió (“T”: Parell Trenat, “F”: Fibra òptica) i pot ser alguna altra característica (“4”: Fa servir els 4 parelles trenats, “X”: Full duplex).



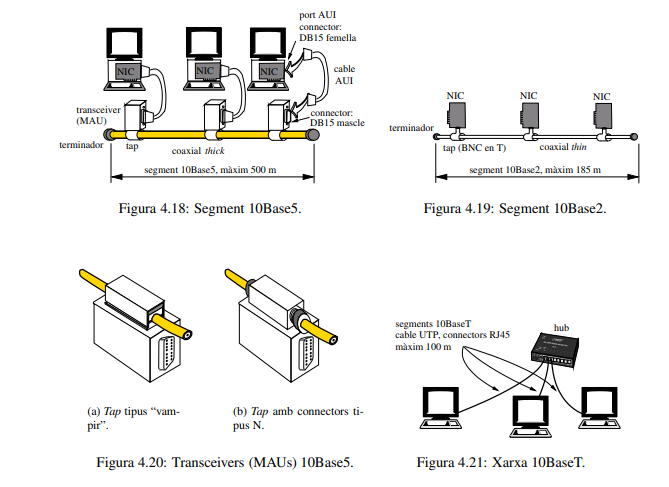
10Base5 va ser el primer estàndard Ethernet de l’IEEE. La figura 4.18 mostra els ingredients d’una xarxa 10Base5. El medi de transmissió és un cable coaxial anomenat thick (gruixut). Aquest cable té dos apantallaments, 0,5” de diàmetre i normalment és de color groc. Amb aquest cable es fan servir connectors anomenats de tipus “N” (vegeu la figura 4.22(a)). Amb 10Base5 les estacions es connecten al cable coaxial mitjançant un dispositiu actiu anomenat transceiver (de transmitter/receiver) o MAU (Media Access Unit). La MAU es connecta al cable coaxial mitjançant un tap (en aquest context, tap vol dir “punxar una línia de comunicacions”). Hi ha dos tipus de taps per 10Base5: un anomenat vampire (vampir), que punxa el coaxial per fer contacte amb els conductors (vegeu la figura 4.20(a)); i l’altre que fa servir connectors de tipus N (vegeu la figura 4.20(b)). La MAU es connecta amb la NIC amb un cable AUI (Attachment Unit Interface) amb connectors DB15, vegeu la figura 4.22(b).

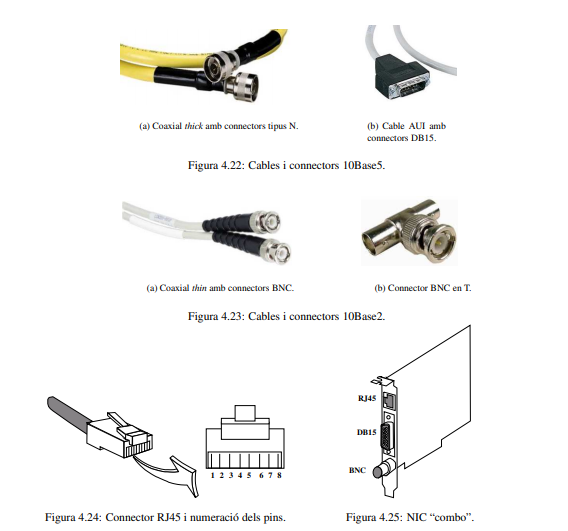
L’estàndard especifica que la MAU ha de tenir la següent funció de “tolerància a falles”: Una tarja Ethernet ha de transmetre un IPG després de cada trama per donar oportunitats de transmissió a les altres estacions. Si una tarja té un malfuncionament i transmet contínuament a la xarxa, aleshores la xarxa es quedaria bloquejada. Per evitar-ho, si una tarja transmet de forma sostinguda durant un temps major a un temps de seguretat, aleshores la MAU desconnecta l’estació de la xarxa. Aquesta condició d’error s’anomena jabber (parlotejar) i el sistema de protecció s’anomena “funció de jabber”. El temps de transmissió d’una trama de mida màxima a 10 Mbps és aproximadament de: 1500 · 8/107 = 1,2 ms. L’estàndard diu que la funció de jabber ha d’activar-se si hi ha un intent de transmissió major de 150 ms (és a dir, major de 10 vegades el temps de transmissió d’una trama de mida màxima).

Com és fàcil d’endevinar, el cablatge d’una xarxa 10Base5 és bastant car, per això ben aviat es varen estandarditzar solucions més econòmiques. Primer es va especificar l’estàndard 10Base2, que fa servir un coaxial amb un sol apantallament de 0,25”, anomenat thin (fi) i connectors BNC (vegeu la figura 4.23(a)). El cable i els connectors són sensiblement més econòmics que els que es fan servir amb 10Base5. A més, típicament no es fa servir MAU (està integrada en la NIC) i el coaxial es connecta a la NIC amb un connector BNC en T (vegeu les figures 4.19 i 4.23(b)). També hi ha MAUs amb un connector BNC que permet cablejar NICs amb port AUI fent servir coaxial thin.

Finalment es va estandarditzar el que s’ha convertit amb el cablatge més econòmic: 10BaseT (figura 4.21). Tant és així, que 10Base5 i 10Base2 han quedat obsolets. En 10BaseT les estacions es connecten a un repetidor (hub). El hub decodifica el senyal que rep per un port i el transmet, amb un retard de pocs bits, per tots els altres ports. 10BaseT fa servir cable UTP i connectors RJ45 en la NIC i el repetidor (vegeu la figura 4.24). També hi ha MAUs amb un connector RJ45 que permet cablejar NICs amb port AUI fent servir cable UTP. El cable UTP està estandarditzat per l’organisme d’estandardització EIA/TIA i te´ 4 parells trenats identificats amb colors com s’indica en la taula 4.4(a). Hi ha dos connexionats: L’EIA/TIA-568A (taula 4.4(b)) i l’EIA/TIA-568B (taula 4.4(c)). Per fer cables directes (connexió DCEDTE) es fa el mateix connexionat en els dos extrems del cable UTP. En l’apèndix 4.B s’explica com fer un cable creuat (per poder connectar DCE amb DCE o DTE amb DTE).

A causa d’aquesta barreja d’estàndards i connectors, durant un temps varen ser populars les NIC “combo” (vegeu la figura 4.25). Aquestes NICs porten un port AUI, per connectar a una MAU 10Base5; un port BNC, per connectar a una xarxa 10Base2; i un port RJ45 per connectar a una xarxa 10BaseT. Evidentment, només hi pot haver un dels ports connectat. També era freqüent barrejar Ethernets de nivell físic amb diferents cablatges en una mateixa xarxa: per exemple, fent servir 10Base5 com a backbone (per cobrir distàncies majors), d’on pengen segments 10Base2 o 10BaseT. Hi ha convertidors que permeten aquestes barreges. En l’actualitat, però, els cablatges amb coaxial (10Base5 i 10Base2) han quedat obsolets en favor del cablatge amb UTP. Si es necessita cobrir distàncies majors de les que permet UTP, aleshores es fa servir fibra òptica.

A 10BaseT han seguit els estàndards coneguts comercialment com Fast Ethernet a 100 Mbps i Gigabit Ethernet a 1 Gbps (vegeu la taula 4.3). Fins i tot, el juny de 2002 es va completar l’estàndard 10GBase Ethernet a 10 Gbps. 10GBase opera nomes´ en mode full-duplex.



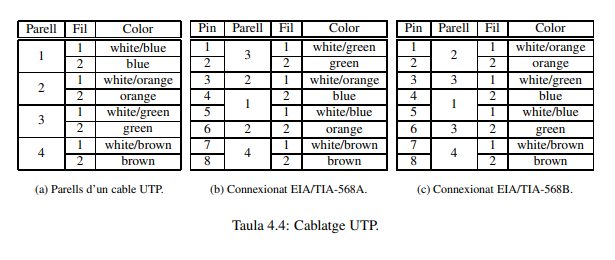
**4.7 Switches Ethernet**

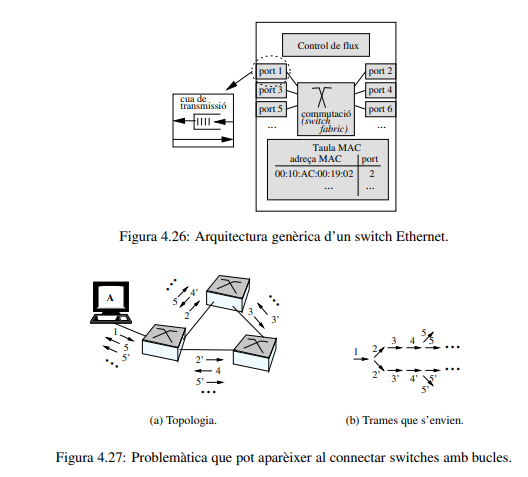
Tal com s’ha vist en la secció 4.5.1, un elevat nombre de col·lisions pot reduir considerablement l’eficiència d’una LAN amb accés al medi aleatori. Per aquest motiu, quan el nombre d’estacions d’una xarxa Ethernet comença a créixer, apareix la necessitat de segmentar o dividir el “domini de col·lisions”. Amb aquest nom es coneix el conjunt d’estacions que comparteixen el mateix medi de transmissió i que poden col·lisionar directament entre elles. Per exemple, un conjunt d’estacions connectades a un segment 10Base5, 10Base2 o a un hub formen un “domini de col·lisions”. Un router, en canvi, segmenta el domini de col·lisions. Això és perquè quan rep una trama per un port, no la transmet simultàniament per cap altra port (com faria un hub), sinó que: (i) Captura la trama completament; (ii) processa el datagrama IP i decideix per quin port s’ha de transmetre; (iii) s’emmagatzema en la cua de transmissió del port que toca; (iv) es transmet la trama accedint al medi com ho faria qualsevol altra estació. Aquest tipus de processat s’anomena store & forward (emmagatzemar i encaminar cap endavant). Del raonament anterior deduïm que cada port del router és un “domini de col·lisions” diferent.

Amb l’objectiu de segmentar el domini de col·lisions d’una xarxa Ethernet, però de forma més econòmica que amb un router, es varen introduir els dispositius anomenats bridges. Un bridge és un dispositiu amb un nombre reduït de ports (per exemple 2) que, igual que un router, també fa un processat store & forward de les trames, però a nivell 2. Un bridge té una NIC diferent en cada port. El funcionament és el següent: el bridge disposa d’una “taula MAC” on hi ha les tuples {adreça MAC, # port}. És a dir, en la “taula MAC” hi ha apuntat el port d’on “penja” cada adreça MAC. Quan arriba una trama per un port, el bridge: (i) La captura completament; (ii) mira la taula MAC per saber per quin port s’ha de transmetre; (iii) s’emmagatzema en la cua de transmissió del port que toca; (iv) es transmet la trama accedint al medi com ho faria qualsevol altra estació. Del raonament anterior deduïm que cada port del bridge és un “domini de col·lisions” diferent.

La “taula MAC” no ha d’inicialitzar-se manualment, sinó que la construeix el bridge de forma automàtica (es parla de learning bridges). Per fer-ho, cada vegada que arriba una trama, el bridge mira l’adreça font. Si l’adreça no es troba en la taula MAC, aleshores hi apunta que aquella adreça “penja” del port d’on ha arribat. Després mira l’adreça destinació. Si l’adreça no es troba en la taula MAC (o si és una adreça broadcast), aleshores es fa una còpia de la trama en les cues de transmissió de tots els ports (excepte del que ha arribat). Així, la trama es transmetrà per tots els ports per assegurar que arriba a la destinació. Si l’adreça destinació es troba en la taula, aleshores es posa la trama només en la cua de transmissió del port que diu la taula. De forma anàloga a les cache ARP (vegeu la secció d’ARP del tema 2), per mantenir les taules petites i actualitzades les entrades tenen un time-out. Cada vegada que una entrada es fa servir, el time-out es refresca. Si salta el time-out, l’entrada s’esborra de la taula.

Després dels bridges es varen introduir els switches (commutadors). Un switch té la mateixa funcionalitat que un bridge, però amb més ports i major capacitat de commutació de trames entre els ports (d’aquí el seu nom). La figura 4.26 mostra l’arquitectura genèrica d’un commutador Ethernet. L’element de commutació switch fabric és capaç¸ de commutar trames simultàniament entre ports diferents. Per exemple, una estació A connectada al port 1 que transmet cap a una estació B connectada al port 2 ho pot fer simultàniament a una estació C connectada al port 3 que transmet cap a una estació D connectada al port 4. Això vol dir que si els ports són a 10 Mbps, per exemple, aleshores les estacions A i B podran transmetre de forma simultània aproximadament a 10 Mbps cap a les destinacions (suposant que les destinacions no transmeten). En la secció 4.7.4 es donen més exemples de com els switches reparteixen el medi de transmissió.





**4.7.1 Spanning Tree Protocol**

De la descripció anterior podem veure que un switch també té funcions d’encaminament, que a primera vista poden semblar similars a les d’un router: en una xarxa formada per switches Ethernet, quan les taules MAC estan inicialitzades, les trames “salten” de switch a switch des de l’origen fins a la destinació. Hi ha, però, una diferència important: els routers es poden connectar amb una topologia arbitrària (l’algorisme d’encaminament s’encarregarà d’actualitzar les taules adequadament). Els switches, en canvi, no admeten una topologia arbitrària. Suposem, per exemple, la topologia de la figura 4.27(a). Si l’estació A envia una trama broadcast, cada switch transmetrà la trama per tots els ports, excepte per on arriba la trama. Així doncs, es generarà la seqüencia de transmissions que detalla la figura 4.27(b): és a dir, si no es pren cap mesura, hi haurà trames que es quedaran donant voltes indefinidament en el bucle. Això pot fer que fàcilment la xarxa es saturi i deixi de funcionar correctament.

La conclusió del exemple anterior és que en una xarxa amb switches no hi pot haver bucles. Per altra banda, en la pràctica és desitjable que n’hi pugui haver. Un motiu és evitar que la connexió accidental d’un bucle pugui provocar un mal funcionament de la xarxa. Si la xarxa és gran, és fàcil que això passi. Un altre motiu és que en la pràctica pot ser desitjable que hi hagi bucles per tenir tolerància a falles: és a dir, tenir diversos camins alternatius perquè si un d’ells deixa de funcionar, l’altre el pugui substituir.

Per solventar els problemes que representen els bucles en la interconnexió de switches, es va desenvolupar l’estàndard STP (Spanning Tree Protocol), que després ha estat substituït pel RSTP (Rapid Spanning Tree Protocol) [17, secció 17]. En poques paraules, els switches que fan servir RSTP s’intercanvien un conjunt de missatges per deixar una topologia “en arbre”, en què no hi hagi bucles. Perquè sempre quedi una topologia en arbre, RSTP pot deixar alguns ports en estat de “bloqueig”. Els ports que estan en aquest estat descarten totes les trames de dades que reben i, per tant, no participen en la inicialització de la taula MAC. Les úniques trames que capturen els ports en l’estat de “bloqueig” són els missatges RSTP. De manera que els ports poden passar a l’estat normal de funcionament si hi ha un canvi en la topologia que ho requereixi.

**4.7.2 Dominis broadcast**

Al segmentar el domini de col·lisions, els switches Ethernet permeten augmentar l’escalabilitat de la LAN. De fet, una LAN Ethernet amb switches és una barreja entre “medi compartit” i “medi commutat” (vegeu la secció 4.1): Una vegada que els switches tenen les taules MAC inicialitzades, encaminen les trames perquè travessin només els enllaços necessaris per arribar a la destinació.

Hi ha però, un factor que introdueix una limitació en l’escalabilitat d’una xarxa Ethernet i que els switches no resolen: les trames broadcast. En el tema 2 hem vist que hi ha nombrosos protocols que envien trames d’aquest tipus: ARP, DHCP, DNS, RIP, etc. Els broadcast tenen com a objectiu arribar a totes les estacions de la xarxa i a nivell Ethernet es transmeten amb adreça destinació FF:FF:FF:FF:FF:FF. Quan un switch rep una trama amb aquesta adreça destinació, l’envia pet tots els ports, excepte el port d’on ha arribat, perquè la trama es propagui per tota la xarxa. Per aquest motiu, totes les estacions Ethernet interconnectades amb dispositius de nivell 1-2 (coaxial, hubs i switches) es diu que formen un “domini broadcast” (broadcast domain).

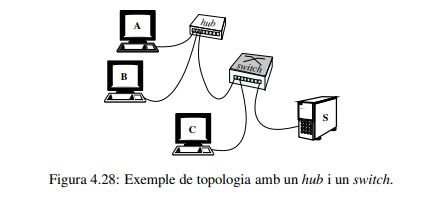
A diferència dels switches, els routers sí que segmenten el domini broadcast. És a dir, si un router rep una trama Ethernet broadcast, no la transmetrà pels altres ports. Si no fos així, Internet es col·lapsaria!

**4.7.3 Control de flux**

Tal com mostra la figura 4.26, un dels elements del switch és el “control de flux”. A continuació hi ha un exemple que explica la necessitat d’aquest element. Suposem un switch amb ports 10/100. Això vol dir que els ports poden transmetre a 10 o 100 Mbps, segons el dispositiu que hi hagi connectat. Aquests tipus de ports tenen un mecanisme d’autonegociació que permet detectar la velocitat de transmissió del dispositiu que s’hi connecta. Com que els ports transmeten de forma independent entre ells, en un switch és possible que hi hagi ports que transmeten a diferents velocitats. Suposem ara que en un dels ports hi ha una estació amb una tarja a 100 Mbps que transmet cap a una altra estació que té una tarja a 10 Mbps. En aquest cas hi haurà un port configurat a 100 Mbps que transmet cap a un port configurat a 10 Mbps. Evidentment, la cua de transmissió del port a 10 Mbps ràpidament s’omplirà i el switch començarà a perdre trames si no pren cap mesura. Quan passa això, s’activa el “control de flux” del switch, per aconseguir que la velocitat mitjana del port més ràpid s’ajusti a la del port més lent.

Per fer el control de flux, un switch “frena” els ports que envien trames cap al port congestionat. És a dir, cap al port on la cua de transmissió s’omple excessivament. L’algorisme de control de flux és específic de cada fabricant. Un switch que no tingui un control de flux eficient perdrà trames fàcilment. Per a “frenar” els ports hi ha dos mecanismes: (i) Amb un senyal de jabber (només es fa servir en mode half duplex); i (ii) amb trames de pausa [15, Annex 31B] (nomes´ es fa servir en mode full duplex).

El terme jabber ja l’hem introduït en la secció 4.6.5, pàgina 85, per referir-nos a la transmissió anormalment gran d’una tarja. En cas del control de flux, el senyal de jabber es refereix a un senyal que el switch envia pels ports que vol frenar, simulant la transmissió d’una trama. Les estacions que pengen del ports on el switch envia el jabber veuen el medi ocupat i deixen de transmetre (seguint el mecanisme CSMA/CD). Amb mode full duplex l’algorisme de CSMA/CD es desactiva, per tant, el senyal de jabber no serveix per fer el control de flux. En mode full duplex el control de flux s’ha de fer amb les “trames de pausa”. Les trames de pausa són unes trames especials que el switch envia pels ports full duplex que vol frenar. La trama de pausa porta un camp amb un enter indicant el nombre de slot times que l’estació que rep la trama ha de restar en silenci.



**4.7.4 Repartició del medi de transmissió**

Les importants diferències que hi ha entre el funcionament d’un hub i un switch fan que la repartició del medi de transmissió entre les estacions depengui en gran mesura dels dispositius que es facin servir i de com estan interconnectats. Considerem, per exemple, una xarxa 10BaseT amb la topologia de la figura 4.28: En la xarxa hi ha 3 estacions (A, B, C) idèntiques i un servidor (S) connectats amb un hub i un switch, tal com mostra la figura. Suposarem que: (i) Les estacions i el servidor són molt més ràpids que la xarxa; (ii) les transferències només es fan entre les estacions i el servidor; (iii) per simplicitat, suposarem que només es transmeten segments d’informació (no considerarem l’efecte de les confirmacions). Considerem els següents escenaris:

**Les estacions descarreguen simultàniament un fitxer del servidor.** En aquest cas el coll d’ampolla és el port que connecta S amb el switch. Les 3 connexions TCP enviaran la finestra de transmissió que quedarà emmagatzemada en la cua de transmissió del driver de la tarja d’S. Per tant, la tarja d’S tindrà sempre trames llestes per transmetre. Com que no hi ha pèrdues, les finestres de transmissió seran les advertides per les estacions, que seran iguals perquè suposem que les estacions són idèntiques. Així doncs, en mitjana, S enviarà successivament una finestra de cada estació. Per tant, la velocitat efectiva aconseguida per les tres estacions serà la mateixa: Aproximadament 10 Mbps/3.

**Les estacions transmeten simultàniament un fitxer cap el servidor.** En aquest cas, el coll d’ampolla també és el port que connecta S amb el switch, però ara el comportament és ben diferent: ara les finestres de transmissió de TCP estaran en les cues de transmissió dels drivers de les targes de les estacions (per tant, aquestes targes tindran sempre trames llestes per transmetre). En aquest cas tampoc hi haurà pèrdues i les finestres seran les advertides per S. Com que tots els ports són de 10 Mbps, al switch arribaran 20 Mbps destinats cap al port on hi ha el servidor. El port és de 10 Mbps, per tant, la cua de transmissió d’aquest port s’omplirà ràpidament i el switch haurà de fer un control de flux en els ports on pengen les estacions per no perdre trames. El control de flux el farà simultàniament pels dos ports on pengen les estacions: per exemple, enviant un senyal de jabber simultàniament per aquests dos ports cada vegada que la cua de transmissió del port congestionat assoleix un cert nivell. Això vol dir que el nombre de segments que aconseguiran entrar pels ports del switch on hi ha les estacions serà, en mitjana, el mateix. És a dir, la capacitat de l’enllaç¸ congestionat (10 Mbps) es repartirà al 50% entre aquests dos ports: aproximadament 5 Mbps per a cada un. Això vol dir que l’estació C quedarà afavorida: podrà transmetre aproximadament amb una velocitat efectiva de 5 Mbps; mentre que les estacions A i B es repartiran equitativament els altres 5 Mbps: és a dir, podran transmetre aproximadament amb una velocitat efectiva de 2,5 Mbps. Això vol dir que si el fitxer que transmeten les tres estacions té la mateixa mida, aleshores quan l’estació C hagi transmès el fitxer, les estacions A i B només hauran transmès la meitat del fitxer. A partir d’aquest moment (suposant que l’estació C no torna a transmetre), la velocitat efectiva de A i B augmentarà aproximadament a 5 Mbps.

4.7.5 LANs Virtuals

Tal com s’ha explicat en la secció 4.7.2, un switch Ethernet forma un domini broadcast. Normalment és convenient per motius d’eficiència i seguretat tenir els servidors i hosts relacionats en dominis broadcast diferents, cada un identificat per una subxarxa. La figura 4.29 en mostra un possible exemple. En la pràctica, però, el nombre de hosts i servidors pot ser desconegut quan es dissenya la xarxa. A més, la seva ubicació física pot no estar relacionada amb la subxarxa a què pertanyen. Per exemple, és possible que es desitgi tenir tots els servidors centralitzats en una habitació aïllada, per motius de seguretat i refrigerada. La tecnologia anomenada “LAN virtual” (Virtual LAN, VLAN) permet introduir aquesta flexibilitat. La figura 4.30 en mostra un exemple. La distribució lògica de la figura 4.30, correspon a la de la figura 4.29. És a dir, amb VLANs podem aconseguir que la distribució lògica dels dominis de broadcast no es correspongui amb la distribució i connexió física dels commutadors.

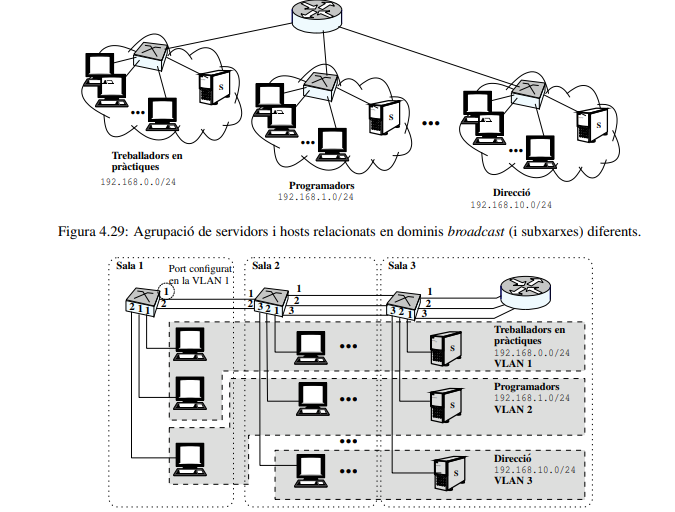


Figura 4.30: Exemple de VLANs: la ubicació física dels commutadors (Sala 1, Sala 2, Sala 3) no es correspon amb la distribució lògica dels dominis broadcast (subxarxes 192.168.x.0/24).

Hi ha diferents tipus de VLANs. El que més es fa servir és l’anomenat “per port” (port-based, portcentric). Cada port del commutador està associat a una VLAN. Tots els hosts que pengen del port pertanyen a la VLAN que té associada. La VLAN es pot associar al port estàticament o dinàmicament. Per exemple, amb el protocol VMPS (VLAN Management Policy Server) de CISCO, quan un port que té una assignació dinàmica rep una trama, mira quina és l’adreça MAC font de la trama. Després envia un missatge VMPS a un servidor per consultar a quina VLAN està associada la MAC i configura el port segons el missatge rebut del servidor.

En l’exemple de la figura 4.30 les VLANs estan configurades per port. Cada switch aïlla els ports que pertanyen a VLANs diferents. Per a cada VLAN el switch té una taula MAC diferent. De fet, és com si un mateix switch es substituís per tants switchs com VLANs si han definit. Si arriba una trama broadcast per un port, el switches només el reenvia pels altres ports que pertanyen a la mateixa VLAN. Per això, es diu que les VLANs segmenten el domini broadcast. D’aquesta manera, per anar d’una VLAN a una altra és necessari passar pel router.

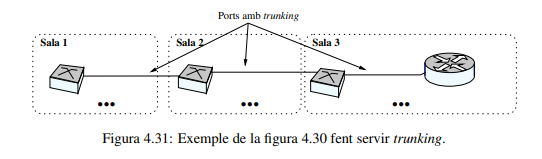
Fer servir la tècnica de VLANs per port explicada anteriorment porta a haver de connectar més d’un port entre dos commutadors o entre un router i un commutador (vegeu la figura 4.30). Per evitar-ho es fa servir un dels següents estàndards:

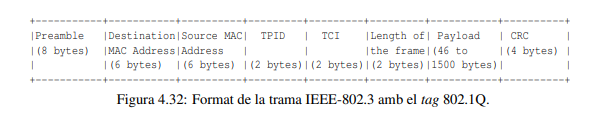
* Inter-Switch Link (ISL), que és un protocol propietari de CISCO.
* L’estàndard IEEE-802.1Q [16].

Els dos estàndards es basen a afegir un tag a les trames que s’envien entre els dos commutadors, o entre el commutador i el router perquè un mateix port pugui portar tràfic de més d’una VLAN. El tag identifica la VLAN a què pertany la trama. CISCO anomena els ports que fan servir un d’aquests estàndards com ports trunking. La figura 4.31 mostra com quedaria l’exemple de la figura 4.30 fent servir trunking. Quan la trama s’envia per un port que no té trunking, aleshores el tag s’elimina.

En l’estàndard IEEE-802.1Q el tag consisteix en la inserció de 4 bytes entre el camp source address i Type/Length de la trama Ethernet. La figura 4.32 mostra com queda una trama IEEE-802.3 amb el tag 802.1Q. El tag està format pels camps:

* Tag Protocol Identifier (TPID): Porta el valor 0x8100 quan el tag s’ha afegit a una trama Ethernet.
* Tag Control Information (TCI): camp que porta informació de control, entre la qual cal destacar l’identificador de la VLAN a la que pertany la trama (VLAN ID). Aquest identificador té 12 bits.





**4.8 LANs sense fils**

Les LANs sense fils, wireless LAN (WLAN), tenen diverses avantatges molt interessants respecte a les xarxes cablejades:

* Estalviar el cost del cablatge, que molt cops representa una part important del pressupost de la xarxa.
* Flexibilitat en el desplegament de la xarxa: la xarxa es pot instal·lar i desinstal·lar amb molta facilitat. Això és necessari en xarxes que només es necessiten de forma temporal, com ara una xarxa muntada durant una conferència, una situació d’emergència, etc.
* Mobilitat: les estacions es poden moure lliurement en la xarxa sense la limitació que introdueix la connexió a una roseta en una xarxa cablejada.

Per contra, la transmissió sense fils representa un repte tecnològic molt més difícil de superar que en el de la transmissió per cable:

* Per transmetre els senyals cal fer servir modulacions d’altra freqüència que faci possible la seva propagació per l’espai.
* Quan el senyal es propaga per l’espai s’atenua ràpidament, de forma que la potència útil del senyal rebut és molt feble.
* La presència d’obstacles i el canvi de les condicions del medi on es propaga el senyal (sobretot en cas d’haver-hi mobilitat) fan que la potència del senyal útil rebut variï constantment.
* La feblesa del senyal útil rebut fa que quedi emmascarat amb un gran nombre de factors que introdueixen soroll i interferències.

Per aquests motius, el desenvolupament de les WLANs no ha estat significatiu fins al final de la dècada dels 90. El desenvolupament ha estat, però, tan ràpid que en la actualitat gairebé tots els computadors portàtils que es venen porten una tarja WLAN integrada.

S’han estandarditzat diversos protocols per a WLANs. Els més representatius han estat HiperLan de l’organisme d’estandardització ETSI i 802.11 de l’IEEE. A hores d’ara, però, 802.11 és el protocol que s’ha imposat comercialment. El nom comercial de 802.11 és WiFi (Wireless fidelity). A causa de la dificultat que té la transmissió sense fils, 802.11 és un protocol molt més complex que Ethernet. En aquesta secció veurem només una introducció a alguns aspectes bàsics del protocol.

802.11 fa servir les anomenades bandes de freqüència Industrial, Scientific, and Medical (ISM). Aquestes freqüències es varen reservar internacionalment per a usos no comercials i no estan assignades a un operador de telecomunicacions. Hi ha diversos estàndards de nivell físic. La diferència més important és la velocitat de transmissió màxima i la banda de freqüències:

* 802.11: fins a 2 Mbps, banda de 2,4 GHz.
* 802.11b: fins a 11 Mbps, banda de 2,4 GHz.
* 802.11a: fins a 54 Mbps, banda de 5 GHz.
* 802.11g: fins a 54 Mbps, banda de 2,4 GHz.

802.11 té dos modes de funcionament:

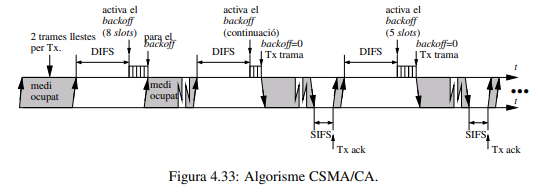
* Infraestructura: és un mode centralitzat on totes les transmissions han de passar per una estació especial anomenada Access Point (AP). L’AP envia trames especials de senyalització beacons per notificar la seva presència. Les estacions han de buscar i associar-se amb un AP per poder accedir a la WLAN. Després de la fase d’associació, sol haver-hi una fase d’autentificació.
* Ad–hoc: és un mode distribuït on totes les estacions accedeixen al medi de la mateixa manera (no hi ha APs).

En una WLAN l’estació que transmet no pot detectar una col·lisió mentre transmet una trama, a causa de l’enorme diferència de potència que hi ha entre el senyal transmès i el senyal rebut. Per això, en 802.11 s’han definit dos mecanismes d’accés al medi:

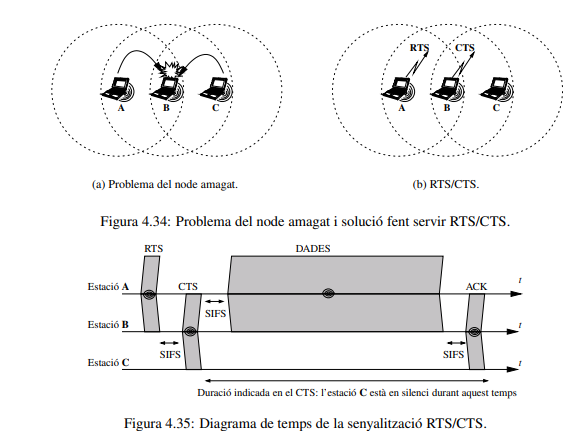
* Point Coordination Function (PCF): és un mode de funcionament opcional. Fa servir un MAC centralitzat. Només es pot fer servir en mode infraestructura. En PCF l’AP fa una enquesta (polling) a les estacions per veure si tenen alguna trama per transmetre. Les estacions només poden transmetre quan es fa l’enquesta, d’aquesta manera s’eviten les col·lisions. Quan es fa servir aquest mode, l’AP intercala el mode PCF (anomenat interval sense contenció) amb el mode DCF (anomenat interval amb contenció) que s’explica a continuació.
* Distributed Coordination Function (DCF): és un mode de funcionament obligatori (han d’implementar-lo totes les estacions). De fet, la major part de les targes que es comercialitzen en l’actualitat només implementen aquest mode (no implementen el mode opcional PCF). DCF fa servir un MAC distribuït anomenat Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). DCF es pot fer servir tant en mode infraestructura com en mode ad-hoc. El mecanisme CSMA/CA és bastant més complex que el senzill CSMA/CD d’ethernet. A continuació es fa una breu descripció.

**4.8.1 Mecanisme CSMA/CA**

Per reduir al màxim el nombre de col·lisions, a diferència de CSMA/CD, CSMA/CA fa un accés al medi no persistent (no s’envia la trama immediatament quan s’allibera el medi). A més, la detecció de les col·lisions en CSMA/CA és completament diferent al d’ethernet: tal com s’ha explicat abans, una diferència fonamental amb ethernet és que l’estació transmissora no pot detectar una col·lisió mentre fa la transmissió d’una trama. Per això, per a la transmissió de trames unicast 802.11 implementa una mena de mecanisme ARQ del tipus Stop and Wait: el destinatari de la trama envia una confirmació. Aquest mecanisme s’explica tot seguit. En el cas d’enviar-se una trama broadcast, com que no hi ha un destinatari únic, aquest mecanisme no es pot fer servir i en cas de col·lisió la trama es perd. Això amb ethernet no passa perquè el transmissor de la trama és el responsable de detectar la col·lisió, independentment de si la trama és broadcast o no. Així doncs, en 802.11 és fàcil que les trames broadcast es perdin. El diagrama de temps de la figura 4.33 i les següent regles sumaritzen el mecanisme CSMA/CA de 802.11:



1. Quan una estació (primari) vol transmetre una trama d’informació, escolta el medi. Si el medi està ocupat passa al punt 2. Si el medi està lliure, espera un Distributed InteFrame Space (DIFS) i si mentre s’espera no veu el medi ocupat, transmet la trama després del DIFS. Si mentre espera el DIFS veu el medi ocupat, passa al punt 2.

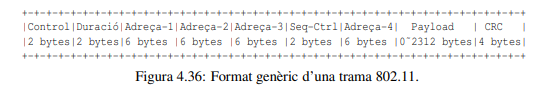


1. El primari inicialitza un backoff. Mentre el medi està ocupat, el backoff està parat i cada cop que el medi està lliure durant un DIFS, el backoff s’activa. Mentre el backoff està activat es decrementa després d’intervals fixos de temps anomenats slots. En la inicialització del backoff la tarja tria un número d’slots uniformement distribuït en l’interval [0..CW], on CW s’anomena Contention Window i val: CW = 2 n −1. Normalment s’agafa com a primer valor n = 5 (CW = 31). Quan el backoff arriba a 0, el primari transmet la trama immediatament.
2. Després de rebre una trama, el secundari espera un Short InteFrame Space (SIFS) i envia una confirmació immediatament. El SIFS és un temps menor que el DIFS. D’aquesta manera la transmissió d’una confirmació té prioritat sobre la transmissió d’una trama.
3. Si després d’enviar una trama el primari no rep la confirmació abans d’un DIFS, interpreta que hi ha hagut una col·lisió. En aquest cas incrementa el valor de n de la CW i torna al punt 2. És a dir, en cas d’haver de retransmetre successivament la trama, CW valdrà 31, 63, 127, .. Aquest increment exponencial de CW evita que la xarxa pugui tornar-se inestable (vegeu la secció 4.5.1). Si després de rebre la confirmació el primari té més trames per transmetre, torna al punt 2.

Addicionalment, per resoldre el problema del “node amagat”, en la transmissió de trames unicast 802.11 permet fer servir el mecanisme Request To Send/Clear To Send (RTS/CTS). El problema del node amagat (hidden node) es dona en una situació com la que mostra la figura 4.34(a). En aquest cas l’estació C està “amagada” de l’estació A (no estan en cobertura). Si l’estació A vol transmetre a l’estació B, l’estació C no ho detectarà, de manera que si l’estació C comença a transmetre mentre ho fa l’estació A, les dues transmissions provocaran una col·lisió en l’estació B (que no podrà rebre la trama que li enviava A). Les figures 4.34(b) i 4.35 mostren la senyalització RTS/CTS. Quan l’estació B envia la trama CTS, l’estació C la rebrà, de manera que, tot i no rebre el senyal d’A, romandrà en silenci mentre transmet A. Aquest mecanisme s’anomena virtual sensing, fent referència a que l’estació C és capaç d’estar al corrent de la transmissió d’A, tot i no poder-la escoltar. A tots els efectes, l’estació C actua com si escoltés el medi ocupat durant el temps indicat en la trama CTS. Com que el mecanisme RTS/CTS només és eficient si es transmeten trames de mida gran, les targes disposen d’un llindar a partir del qual es fa servir aquest mecanisme. Per a la transmissió de trames més petites que aquest llindar, RTS/CTS no es fa servir. Típicament el llindar val 500 bytes.

**4.8.2 Trames 802.11**

A diferència d’ethernet, en 802.11 hi ha definides diferents tipus de trames. La figura 4.36 mostra el format genèric. Segons el tipus de trama, hi ha camps que poden o no ésser-hi.

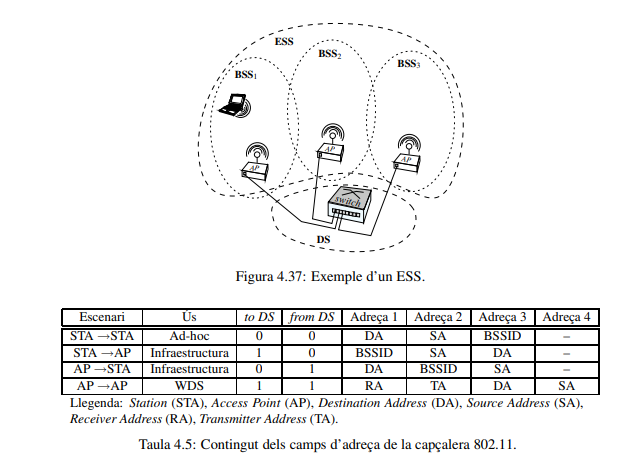


El significat dels camps és el següent:

* Control: indica el tipus de trama.
* Duració: indica la duració (tal com s’ha explicat en la secció 4.8.1).
* Adreça–1∼4: hi ha 4 camps d’adreça que s’expliquen en la pròxima secció. Les adreces tenen 6 bytes (48 bits) i el mateix format que les adreces ethernet. Igual que amb ethernet, l’adreça FF:FF:FF:FF:FF:FF és l’adreça broadcast.
* Seq-Crtl (Sequence Control): es fa servir en la fragmentació. En 802.11 hi ha definit un mecanisme de fragmentació per l’elevada tassa d’error que hi pot haver en el medi de transmissió. La tarja manté un llindar que s’ajusta segons la tassa d’error. Si la trama a transmetre és major que aquest llindar, la trama es fragmenta. Així, en cas d’error, només s’han de retransmetre els fragments erronis i no tota la trama.
* Payload: és el camp de dades. Pot portar fins a 2312 bytes (MTU màxim). A diferència d’ethernet, però, no solen fer-se servir trames de mida màxima. Això és perquè com més gran és la trama, més fàcil és que arribi amb errors i més ineficient serà el protocol si la trama s’ha de retransmetre. Els drives que hi ha en la pràctica solen fixar una MTU per defecte de 1500 bytes, per compatibilitat amb ethernet.
* CRC: Control d’errors (igual que en ethernet).

**4.8.3 Adreçament**

Una característica important d’una WLAN és que fa servir la banda de freqüències no regulada ISM. Això fa que hi pugui haver diverses WLANs independents que estiguin dintre del mateix radi de cobertura. Per exemple, actualment els operadors de telecomunicacions ofereixen línies ADSL amb un modem-router sense fils 802.11. Dos veïns d’un mateix edifici que disposin d’aquests equips podrien ser un exemple de WLANs 802.11 superposades. En aquest cas, no és desitjable que els equips d’una WLAN rebin les trames enviades en altres WLANs, és a dir, cal un mecanisme de filtratge. Amb l’objectiu de poder identificar estacions que formen part de xarxes diferents, 802.11 defineix l’anomenat Basic Service Set (BSS), identificat per un número de 48 bits anomenat BSS Identifier (BSSID).



Les trames que porten un BSSID diferent al que pertany la tarja es descarten. Quan una estació encara no ha accedit a la seva xarxa i desconeix el BSSID, pot accedir fent servir el broadcast BSSID, que coincideix amb l’adreça 802.11 broadcast: FF:FF:FF:FF:FF:FF.

Si una xarxa 802.11 està formada per un únic BSS, aleshores es diu que és un Independent BSS (IBSS). Un BSS pot ser en mode infraestructura (en aquest cas hi ha un AP), o mode ad-hoc. En mode infraestructura, cada AP forma un BSS diferent i el BSSID és l’adreça 802.11 de l’AP. Si una xarxa està formada per més d’un BSS, es parla d’un Extended Service Set (ESS) i la part de la xarxa que permet la interconnexió dels diferents BSS s’anomena Distribution System (DS).

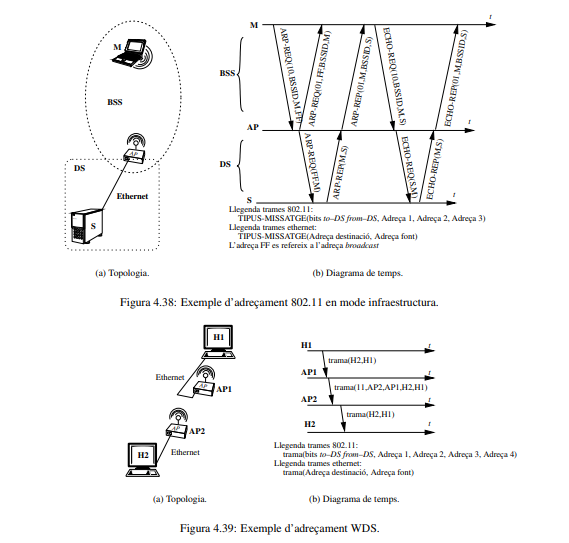
Els APs comercials solen tenir un port ethernet. Per aquest motiu es diu que actuen com bridges 802.11–ethernet. Un exemple d’un ESS podria ser una xarxa formada per diversos APs interconnectats per una xarxa ethernet (vegeu la figura 4.37). Cada AP formaria un BSS diferent i el DS estaria format per la xarxa ethernet. A continuació s’analitzen alguns detalls que fan possible la interoperabilitat entre 802.11 i ethernet.

802.11 ha estat dissenyat perquè es pugui integrar fàcilment amb una xarxa ethernet. De fet, IEEE assigna blocs d’adreces als fabricants de targes 802.11 que no se solapen amb les adreces assignades als fabricants de targes ethernet. D’aquesta manera, en una xarxa amb targes 802.11 i ethernet, la unicitat de les adreces està garantida. Això permet que una tarja 802.11 pugui comunicar-se amb una tarja ethernet de forma transparent per a la tarja ethernet. Per aconseguir-ho la capçalera 802.11 té 4 camps d’adreça. El significat d’aquests camp depèn de l’escenari on es transmet la trama. La taula 4.5 mostra els possibles significats. Els bits to DS i from DS formen part del camp de control que hi ha en la capçalera 802.11. La segona columna de la taula 4.5 (Ús) indica el mode de funcionament en que es fa servir cada tipus d’adreçament (els modes s’expliquen en l’apartat 4.8): en mode Ad–hoc només es fa servir l’adreçament STA →STA; en mode infraestructura es fan servir el adreçaments STA →AP i AP →STA; finalment, l’adreçament AP →AP només es fa servir quan el DS és també sense fils. Aquest escenari s’anomena Wireless Distribution System (WDS). Aquesta taula i els possibles escenaris s’expliquen a continuació.

El camp Adreça–1 porta sempre l’adreça del receptor de la trama. Tal com es veurà més endavant, el receptor, no és sempre la destinació de la trama. Per això, en la taula es distingeix entre Receiver Address (RA) i Destination Address (DA). Anàlogament, el camp Adreça–2 porta sempre l’adreça del transmissor de la trama, que no sempre és l’adreça font. D’aquí la distinció entre Transmitter Address (TA) i Source Address (SA).

Per explicar l’ús de les adreces en mode infraestructura farem servir l’exemple de la figura 4.38. La topologia (figura 4.38(a)) està formada per una estació 802.11 (M), un AP i un servidor (S). Suposem que les caches ARP estan buides i que es fa un ping de M a S. El diagrama de la figura 4.38(b) mostra els missatges que es generen i les adreces que portaran les trames 802.11. El diagrama de temps s’explica ell mateix.

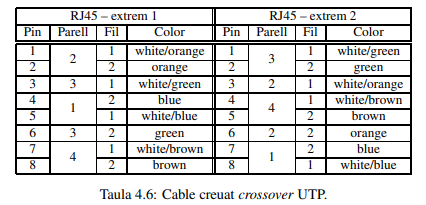
L’adreçament anomenat Wireless Distribution System (WDS) es fa servir en un escenari com el que mostra la figura 4.39. Aquest escenari s’anomena també wireless bridge i els APs fan d’enllaç entre dos segments ethernet.



**Apèndix:**

**Cable creuat crossover UTP**

Per fer un cable creuat (crossover) amb 10BaseT i 100BaseTX (connexió DCE-DCE o DTE-DTE) típicament es fa servir EIA/TIA-568A en un extrem i EIA/TIA-568B en l’altra. Aquest connexionat creua els dos parells que 10BaseT i 100BaseTX fan servir per a la recepció (pins 1, 2) i transmissió (pins 3, 6) (vegeu la taula 4.4).



Amb aquest connexionat, però, els pins 4, 5 i 7, 8 queden sense creuar. Els estàndards 100BaseT4 i 1000BaseT fan servir els 4 parells per això, un cable creuat d’aquesta manera no serveix: Cal creuar els 4 parells. Així doncs, per fer un cable creuat per 100BaseT4 o 1000BaseT cal creuar els pins 1, 2 i 3, 6 com abans i, a més, cal creuar el parell 1 amb el 4. És a dir, connectar els pins 4, 5 respectivament amb els pins 7, 8. Per exemple, si en un extrem fem servir EIA/TIA-568B, el creuament de la taula 4.6 serviria per a tots els estàndards amb cable UTP.