Nivell d'enllaç i xarxes d'àrea local

Eduard Lara Ochoa
Xavier Vilajosana Guillén
René Serral i Gracià
Miquel Font Rosselló

PID_00171177

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

El nivell d'enllaç ha tingut un paper destacat al llarg de la història de les xarxes de computadors. És un nivell que, a diferència d'altres nivells de la torre OSI, ha estat tingut en compte en totes les arquitectures de xarxes de propietat creades durant els anys seixanta i setanta, i s'han fet nombrosos dissenys dels seus protocols. A més, a causa de la seva posició estratègica, està implementat en tots i cada un dels nodes d'una xarxa, de la mateixa manera que el nivell de xarxa.

Segons l'orientació clàssica, el nivell d'enllaç permet establir una connexió directa entre dues entitats amb l'objectiu de transmetre informació: són els anomenats *enllaços punt a punt*. No obstant això, veurem que el nivell d'enllaç també permet establir connexions en medis de difusió, en què participen més de dues entitats, cosa que ocorre generalment en les xarxes d'àrea local.

Per tant, trobarem el nivell d'enllaç implicat en diferents contextos:

- En les connexions locals d'un ordinador amb un perifèric (p. ex., una impressora).
- En les xarxes d'àrea local.
- En les xarxes d'accés a WAN.
- En les xarxes de transport WAN.

Aquest mòdul sobre el nivell d'enllaç s'ha estructurat de la manera següent:

1) En un primer gran apartat s'aborden les característiques generals del nivell d'enllaç. S'analitzen les funcionalitats del nivell d'enllaç agrupades en cinc grans blocs:

a) Gestió de les trames, que engloba funcions com ara: entramat de la trama, sincronització, transparència, numeració, multiplexació i adreçament.

b) Gestió de l'enllaç, en què es diferenciarà entre els serveis de la capa d'enllaç orientats a connexió i els no orientats a connexió.

c) Control de flux, en què s'estudien diferents algorismes desenvolupats per a compatibilitzar la velocitat de recepció de les trames amb la velocitat de processament en el receptor, entre els quals podem destacar: els mecanismes XON/XOFF i RTS/CTS, el protocol Stop & Wait i la finestra lliscant.

d) Control d'errors. Veurem que el nivell d'enllaç és l'encarregat d'intentar resoldre els errors de transmissió que introdueix la utilització de canals físics no perfectes. Les tècniques de control d'errors es presentaran dividides en 3 categories: la detecció d'errors, la correcció d'errors i la retransmissió de trames rebudes erròniament.

e) Control d'accés al medi. Aquesta funcionalitat es troba ubicada dins del gran apartat següent, ja que pren rellevància en les xarxes d'àrea local.

Veurem que totes aquestes funcionalitats normalment es troben implementades en els dispositius de nivell d'enllaç, també anomenats *targetes de xarxa* o *NIC*.

2) El segon gran apartat d'aquest mòdul se centrarà en l'estudi del nivell d'enllaç aplicat al context de les xarxes d'àrea local. Històricament les xarxes d'àrea local s'han basat en medis compartits (medis de difusió). Per a assegurar un accés equitatiu entre tots els terminals que comparteixen el medi, s'han dissenyat una sèrie de tècniques o protocols d'accés al medi, entre els quals tractarem: Aloha, Aloha ranurat, CSMA, CSMA/CD i CSMA/CA. També s'estudiaran les tecnologies més utilitzades en les xarxes d'àrea local tant en medis cablats, en què la tecnologia dominant és Ethernet IEEE 802.3, com en medis sense fils, en què Wireless LAN IEEE 802.11 és l'estàndard triat. Finalment s'establirà la classificació de les tecnologies sense fils segons la seva extensió i s'inclourà l'estudi de WiMAX (IEEE 802.16).

1. Característiques generals del nivell d'enllaç

Hem vist que la capa de xarxa proporciona un servei de comunicació entre dues màquines, i estableix diferents rutes o camins entre aquestes. Cada ruta de comunicació està formada per una sèrie d'enllaços, que connecten la màquina origen amb la de destinació utilitzant uns dispositius encaminadors intermedis. Quan un datagrama del nivell de xarxa surt de la màquina origen cap a la màquina destinació, va travessant cada un d'aquests enllaços individuals que conformen el recorregut d'extrem a extrem.

Es fa necessària una capa lògica addicional situada immediatament sota de la capa de xarxa, que s'encarregui de gestionar cada enllaç individual. Aquesta nova entitat ha d'oferir a la capa de xarxa un transport d'informació fiable entre els diferents enllaços que travessa al llarg d'un recorregut. La capa física no és capaç d'aportar cap dels elements necessaris per a la transmissió efectiva d'informació en un enllaç. La capa que fa aquesta funció rep el nom de *nivell d'enllaç*, i se situa entre els nivells físic i de xarxa.

El nivell d'enllaç consisteix en dos programes o processos que s'executen en tots dos costats d'un enllaç i es comuniquen entre si. Perquè aquests dos processos es puguin comunicar és necessari establir un format per a la informació que s'intercanvien i un conjunt de regles de comportament o protocols necessaris per a la transmissió de dades.

La principal comesa de la capa d'enllaç és la d'aconseguir que la comunicació de dades en un enllaç es faci correctament a través d'un medi físic de transmissió no perfecte, el qual pot introduir errors. D'una manera gràfica podem dir que el nivell d'enllaç s'encarrega d'establir i mantenir un pont de comunicació el més fiable possible entre dos nodes veïns, perquè per sobre puguin circular els datagrames de nivell superior, tal com podem observar en la figura 1.

De l'observació d'aquesta figura podem destacar dues característiques molt importants del nivell d'enllaç:

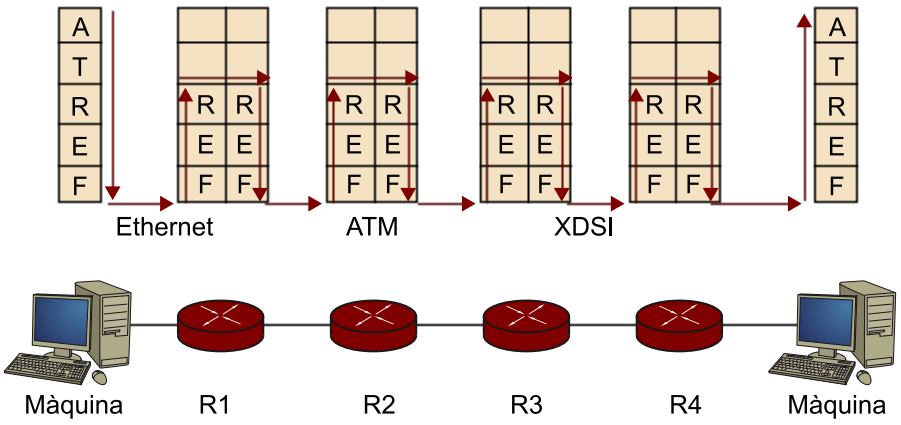
1) Els enllaços, al llarg d'un recorregut de comunicació, poden utilitzar diferents protocols i estar constituïts per tecnologies de base totalment diferents. Un encaminador pot disposar de diferents enllaços i cada un pot utilitzar un protocol de nivell d'enllaç diferent. En la figura 1 podem observar com un datagrama enviat des de la màquina origen és manejat per Ethernet en el primer enllaç, pel protocol ATM[1] en el segon enllaç, i va canviant de tecnologia successivament en cada nou enllaç.

(1) *ATM* és la sigla d'*asynchronous transfer mode*.

2) Una de les funcionalitats bàsiques del nivell d'enllaç consisteix a encapsular/desencapsular els datagrames de la capa de xarxa en unitats d'informació (PDU[2]) de la capa d'enllaç, anomenades *trames*. Les fletxes de la figura 1 indiquen el flux que segueix la informació al llarg del recorregut. Quan una trama arriba a un encaminador des d'un enllaç d'entrada, la capa d'enllaç desencapsula/extreu el datagrama de la trama rebuda i el lliura a la capa de xarxa. Una vegada la capa de xarxa determina per on ha d'encaminar el datagrama, l'envia a l'enllaç de sortida. Aquí el datagrama és encapsulat segons les normes del protocol de l'enllaç i és preparat per a ser enviat a través d'aquest.

(2)*PDU* és la sigla de *protocol data unit*.

Figura 1. Ruta de comunicació entre dues màquines finals

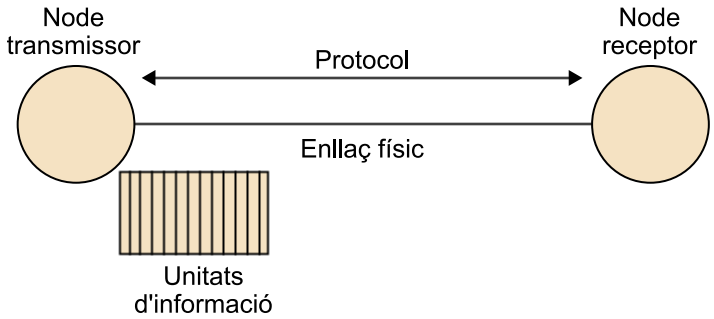


Ruta de comunicació creada entre dues màquines finals, formada per cinc enllaços: dos enllaços comuniquen les màquines finals amb els encaminadors de la xarxa i tres enllaços interns intercomuniquen només encaminadors de la xarxa

1.1. Terminologia i definicions

En el nivell d'enllaç identifiquem els elements següents:

Figura 2



- **Node**: és una màquina, que pot ser un terminal o un encaminador[3]. En la terminologia clàssica hi ha dos tipus nodes en un enllaç: el node transmissor o primari i el node receptor o secundari. No obstant això, i depenent del medi, tots dos poden fer funcions de transmissió i recepció.

- **Enllaç**: és el canal físic que connecta dos nodes adjacents en el recorregut de la comunicació.

(3)En anglès, *router*.

- **Protocol de la capa d'enllaç**: és la manera de comunicar-se entre els nodes, per a moure un datagrama sobre l'enllaç individual. Defineix el format de la informació intercanviada entre els nodes i també les accions preses per aquests nodes quan envien i reben aquestes unitats d'informació.

- **Trama**: són les unitats de dades (PDU) intercanviades per un protocol de la capa d'enllaç. El node transmissor encapsula el datagrama de la capa de xarxa en una trama de la capa d'enllaç i la transmet per l'enllaç. El node receptor rep la trama i n'extreu el datagrama de nivell de xarxa.

1.2. Tipus d'enllaços

Bàsicament podem destacar dos tipus d'enllaços:

1) Enllaços de comunicació punt a punt: només participen dues entitats o punts. Són enllaços 1 a 1, compostos per un únic node emissor en un extrem de l'enllaç i un únic node receptor en l'altre. Tots dos nodes utilitzen en exclusiva l'enllaç, sense compartir el canal. Són considerats enllaços punt a punt:

- El bucle d'abonat local, un cable de dos fils telefònic per a accés a Internet.

- Les xarxes d'àrea local Fast Ethernet.

- Les xarxes d'àrea local Gigabit Ethernet.

- PPP[4], HDLC[5] (en l'àmbit d'enllaç), X.25 en l'àmbit de xarxa i TCP[6] en l'àmbit de transport (en aquest cas és a més d'extrem a extrem).

2) Enllaços de difusió[7] o canals de multidifusió: són enllaços 1 a *N*, en què una sèrie de nodes estan connectats al mateix canal físic de comunicació. La transmissió feta per un node la reben tots els nodes connectats a l'enllaç. Es fan necessàries unes polítiques de coordinació (o protocols d'accés al medi) que permetin la compartició de l'únic medi de manera eficient, tractant d'evitar al màxim les col·lisions entre trames. Són enllaços de difusió:

- Les xarxes d'àrea local Ethernet (semidúplex).
- Les xarxes d'àrea local sense fils (Wi-Fi).
- Els enllaços amb satèl·lits.
- Les xarxes d'accés híbrid fibra-cable (HFC[8]).
- Les xarxes d'àrea local d'enllaç de testimoni.
- Les xarxes d'àrea local FDDI[9].
- Les xarxes metropolitanes (MAN[10]).

(4) *PPP* és la sigla de *point to point protocol*.

(5) *HDLC* és la sigla de *high level data link control*.

(6) *TCP* és la sigla de *transmission control protocol*.

(7) En anglès, *broadcast*.

(8) *HFC* és la sigla d'*hybrid fibre coaxal*.

(9) *FDDI* és la sigla de *fiber distributed data interface*.

(10) *MAN* és la sigla de *metropolitan area networks*.

1.3. Serveis proporcionats per la capa d'enllaç

El servei bàsic del nivell d'enllaç consisteix a moure correctament un datagrama de nivell de xarxa, des d'un node fins a un altre d'adjacent sobre un enllaç de comunicació fix al recorregut.

Els possibles serveis que pot oferir un protocol de la capa d'enllaç són:

1) Gestió de les trames: el nivell d'enllaç s'encarrega de l'organització i gestió de les trames. Entre les diverses funcionals que engloba la gestió de trames podem destacar:

- Entramat o composició de la trama.
- Sincronització en l'àmbit de trama.
- Transparència de trama.
- Numeració i seqüenciació.
- Multiplexació de trames de nivells superiors.
- Adreçament.

2) Gestió de l'enllaç: coordinació i gestió dels processos d'inicialització, manteniment i acabament de l'enllaç. Varia en funció del tipus de servei que subministra la capa d'enllaç a la capa de xarxa.

3) Control d'errors: es tracta d'una de les funcions bàsiques del nivell d'enllaç. S'assumeix que el medi de transmissió físic que hi ha "per sota" no és perfecte i introdueix errors de transmissió. És necessari destinar una part dels bits que s'intercanvien a la detecció i a la gestió posterior dels errors, per a controlar que no es produeixin errors de transmissió. El control d'errors distingeix tres categories de tècniques:

- Detecció d'errors (utilització de codis detectors d'errors).
- Correcció d'errors (utilització de codis correctors d'errors).
- Retransmissió de trames (implementació del lliurament fiable).

4) Control de flux: funcionalitat que permet que l'estació emissora i la receptora es posin d'acord en el ritme de transmissió de dades. Si l'estació receptora rep les trames més ràpidament del que és capaç de processar-les, el nivell d'enllaç remot les ha de "frenar" per a evitar que se saturi la memòria intermèdia o temporal que emmagatzema les trames pendents de processar.

5) Control d'accés al medi: aquesta funcionalitat pren rellevància en els enllaços d'accés múltiple o enllaços de difusió en què un nombre determinat de nodes comparteixen el mateix medi físic.

L'IEEE divideix la capa d'enllaç en dos subnivells:

- LLC[11]
- MAC[12]

[11] *LLC* és la sigla de *logical link layer*.

[12] *MAC* és la sigla de *medium access control*.

El subnivell MAC és l'encarregat d'especificar les regles amb què es transmet una trama sobre l'enllaç. La seva funció és la de garantir que els usuaris accedeixin correctament al medi de transmissió en condicions d'igual prioritat, i vetlla perquè l'accés no sigui simultani. Quan els accessos siguin simultanis, intentarà solucionar el conflicte entre els nodes. En els enllaços punt a punt els protocols d'accés al medi deixen de tenir sentit.

1.4. Adaptadors i dispositius de xarxa

Els nodes o encaminadors es connecten als enllaços per mitjà d'un adaptador, conegut com a *targeta d'interfície de xarxa* o *NIC*[13].

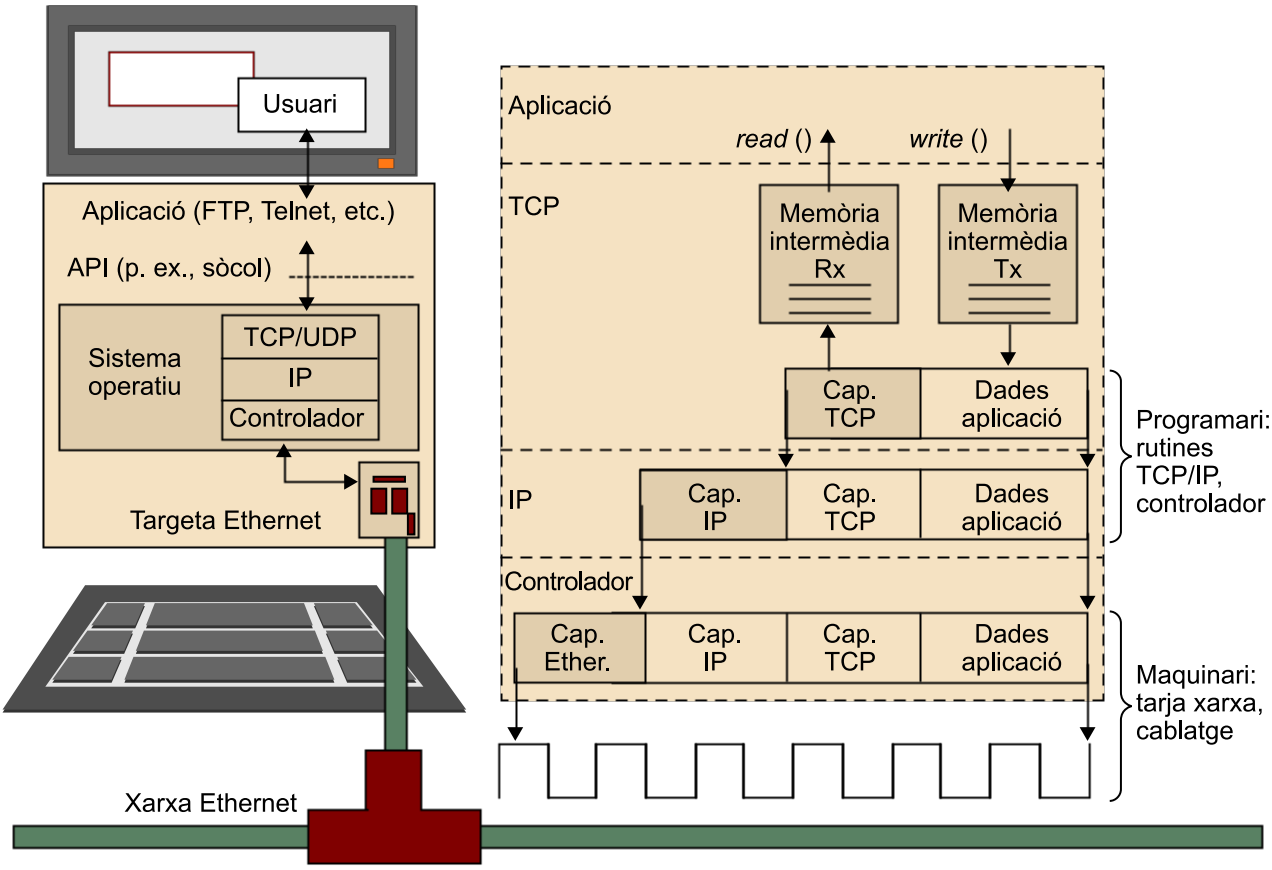
[13] *NIC* és la sigla de *network interface card*.

La importància d'una targeta de xarxa consisteix a tenir implementades majorment les funcionalitats del protocol de la capa d'enllaç. Si un protocol de la capa d'enllaç proporciona detecció d'errors, lliurament fiable (numeració i reconeixements) o accés aleatori, aquestes funcionalitats estan implementades completament en els adaptadors.

Físicament un adaptador és una placa de maquinari (o una targeta PCMCIA) que conté tots els elements d'un petit computador: memòria RAM, xip DSP, una interfície de bus amb la màquina, i una altra interfície per a connectar amb l'enllaç. Normalment es troba allotjat a la mateixa caixa física que la resta del node, i comparteix l'alimentació i els busos.

Els components principals d'un adaptador són la interfície del bus i la de l'enllaç. La interfície del bus és responsable de comunicar amb el node pare de l'adaptador. Transfereix dades i informació de control entre l'adaptador i el node pare. La interfície de l'enllaç és responsable d'implementar el protocol de la capa d'enllaç. També inclou els circuits de transmissió i recepció.

Figura 3



Un adaptador té un cert grau d'autonomia:

- En recepció: quan rep una trama, determina si la trama té errors. Si és així la rebutja sense notificar-ho al seu node pare. Si és correcta, desencapsularà el datagrama de la capa de xarxa i interromprà el seu node pare per a passar-lo cap amunt en la pila de protocols.

- En transmissió: quan un node passa un datagrama cap avall en la pila de protocols a un adaptador, delega totalment a l'adaptador la tasca de transmetre el datagrama sobre l'enllaç. L'adaptador encapsula el datagrama en una trama i transmet la trama en l'enllaç de comunicació.

Exercicis

1. Segons el que hem vist, creieu que tots els protocols de nivell d'enllaç ofereixen tots els serveis de la capa d'enllaç descrits?

Solució de l'exercici 1

No tots els serveis estan implementats en tots els protocols. Cada protocol específic de la capa d'enllaç defineix una sèrie de serveis i en rebutja d'altres.

2. Indiqueu quins possibles serveis de la capa d'enllaç també són oferts per les capes de xarxa o transport en els seus nivells superiors respectius.

Solució de l'exercici 2

- **Lliurament fiable**: tant la capa d'enllaç com la de transport poden proporcionar lliurament fiable. La capa de transport proporciona lliurament fiable entre dos processos d'extrem a extrem; en canvi, la capa d'enllaç proporciona lliurament fiable entre dos nodes connectats per un únic enllaç.

- **Control de flux**: la capa de transport també pot proporcionar control de flux. En aquest cas proporciona control de flux d'extrem a extrem, mentre que en un protocol de la capa d'enllaç es proporciona en una base de node a node adjacent.

- **Detecció d'errors**: són oferts també en la capa de transport i en la capa de xarxa.

3. Indiqueu si les tecnologies següents de nivell d'enllaç implementen els serveis de nivell d'enllaç.

	Entramat	**Accés al medi**	**Detecció errors**	**Correcció errors**	**Retransmissió trames**
PPP					
ATM					
Ethernet					
Retransmissió de trama					

4. Per què entre les funcionalitats del nivell d'enllaç no hi ha la de control de congestió?

Solució de l'exercici 4

Si el control de flux tracta de no saturar la memòria intermèdia (*buffer*) del node receptor, l'objectiu del control de congestió és no saturar les memòries intermèdies. És evident que en un enllaç no hi ha nodes intermedis. Tracta la comunicació directament amb el veí i, per tant, el control de congestió no té sentit.

5. Indiqueu els avantatges i desavantatges que hi pot haver en la correcció d'errors respecte a la retransmissió de trames errònies. En quines situacions és preferible la correcció d'errors?

Solució de l'exercici 5

La correcció d'errors evita el retard que implica sol·licitar la retransmissió de les trames. Al contrari, els codis correctors d'errors necessiten afegir molta redundància (bits extra) i, per tant, la transmissió és més ineficient i s'augmenta el sobrecost (la relació entre els bits d'informació i de control disminueix).

Un cas típic en què és preferible un codi corrector d'errors abans que un codi detector acompanyat de retransmissions és en comunicacions via satèl·lit. Convé més pagar en ineficiència per l'increment de bits redundants que en temps de retransmissions, perquè la distància que cal recórrer és molt gran.

2. Gestió de trames

2.1. Entramat

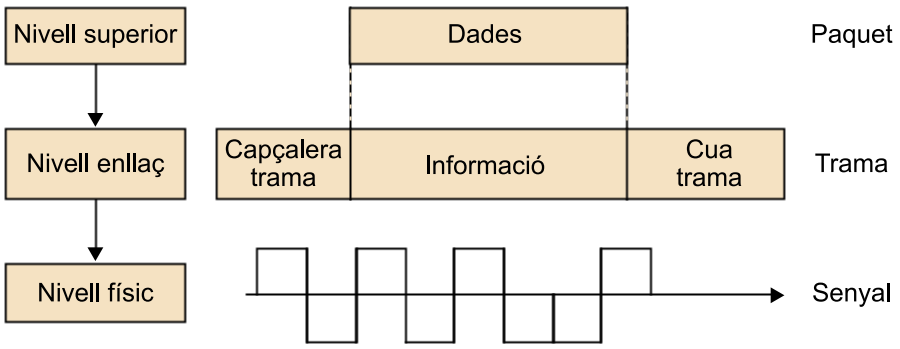
En el nivell d'enllaç, el control de la transmissió de dades entre nodes veïns es vertebra sobre el procés de creació i tramesa de la trama.

En la capa física la tramesa d'informació es fa en forma de bits solts de manera no fiable; la capa d'enllaç actua de manera diferent: construeix amb els bits estructures ordenades denominades *trames*[14], que són les que s'envien per l'enllaç.

[14]En anglès, *frames*.

La gran majoria de protocols de la capa d'enllaç encapsulen els datagrames de la capa de xarxa dins d'una trama abans de viatjar per l'enllaç. Una bona part de les tasques de la capa d'enllaç té a veure amb la construcció i identificació de les trames. Per exemple, un avantatge de la utilització de trames és que permet simplificar el procés de detecció i correcció d'errors.

Figura 4



Les trames s'organitzen en camps, de manera que hi ha camps amb bits d'informació i camps amb bits de control. Encara que l'estructura d'una trama depèn de cada protocol específic del nivell d'enllaç, generalment la podem dividir en les parts següents:

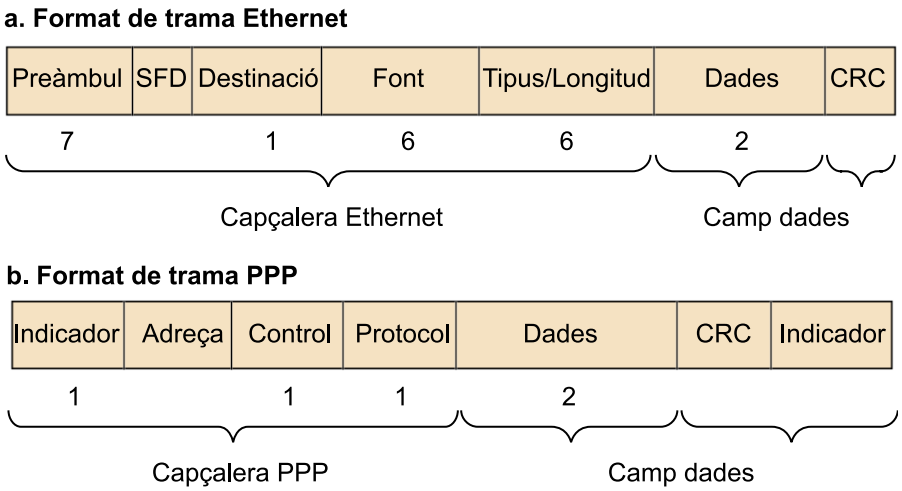
- Una capçalera, composta per camps de bits de control de la trama: adreça física, longitud de la trama, tipus de dades que transporta, etc.

- Un camp de dades, en què hi ha els bits d'informació corresponents a datagrames de la capa de xarxa.

- Una cua que tanca la trama; es tracta d'un camp de control necessari per a fer el control d'errors.

Podem comprovar aquesta divisió observant l'estructura de trama dels dos protocols més importants de nivell 2: Ethernet i PPP.

Figura 5. Formats de trama Ethernet i PPP



2.2. Sincronització en l'àmbit de trama

El sincronisme de trama[15] és el mecanisme que utilitza el nivell d'enllaç per a determinar l'inici i el final d'una trama dins del flux de bits o caràcters que arriba del nivell físic.

(15) En anglès, *framing*.

Fins ara hem parlat sempre del nivell físic com un medi capaç de transportar un flux de bits. Hi ha, tanmateix, alguns medis físics que tenen com a unitat de transmissió el caràcter, que es defineix com un bloc fix de bits. Aquest cas es coneix amb el nom de *transmissió orientada a caràcter*.

De fet, es parla de dos tipus de protocols, un per a cada un dels tipus de transmissió esmentats:

- **Protocols orientats a bit**: protocols de nivell d'enllaç dissenyats per a anar sobre una transmissió orientada a bit. En aquest cas el nivell físic té com a unitat de transmissió el bit. Un exemple típic és el protocol HDLC.

- **Protocols orientats a caràcter**: protocols de nivell d'enllaç dissenyats per a anar sobre una transmissió orientada a caràcter. El medi físic té com a unitat de transmissió el caràcter. Un exemple típic és el protocol BSC[16] d'IBM.

(16) *BSC* és la sigla de *binary synchronous control*.

Per a descriure els mecanismes de sincronització del nivell de trama, posarem com a exemples els que utilitzen els protocols HDLC i BSC, perquè són molt representatius.

2.2.1. Detecció de l'inici de trama

Depèn del tipus de transmissió:

- En transmissió orientada a caràcter, l'inici de trama s'indica amb un caràcter especial denominat *caràcter d'inici de trama*, com per exemple STX. STX[17] està definit en ASCII i en EBCDIC (IBM). S'utilitza en terminals IBM que utilitzen el protocol BSC.

(17)*STX* és la sigla de *start of text*.

- En transmissió orientada a bit, s'indica l'inici de trama amb una combinació especial de bits denominada *indicador*[18] *d'inici de trama*. En HDLC el patró de bits que identifica l'inici de trama és 01111110.

(18)En anglès, *flag*.

2.2.2. Detecció de final de trama

Es pot implementar utilitzant dos mètodes:

- Utilitzant un caràcter especial anomenat *caràcter de final de trama* (en transmissió orientada a caràcter) o una combinació especial de bits anomenada *indicador de final de trama* (en transmissió orientada a bit).

- Utilitzant un camp de longitud que indica la mida de la trama.

Alguns protocols utilitzen les dues tècniques conjuntament per a dur a terme el control d'errors. D'aquesta manera, si el caràcter de final de trama o l'indicador, segons el cas, no arriba al final de la trama indicat pel camp de longitud, es detecta un error de delimitació de trama, o error de *framing* (per exemple, Ethernet).

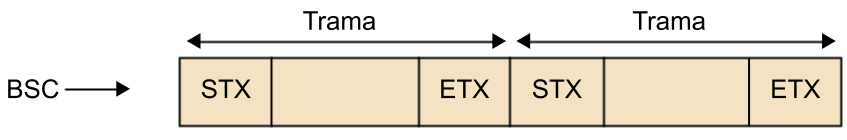
Exemples de sincronització de trama

(19)*ETX* és la sigla d'*end of text*.

1) Sincronització de trama en una transmissió orientada a caràcter:

Tant el codi ASCII com el codi EBCDIC tenen els caràcters de control STX i ETX[19]. Alguns dels protocols orientats a caràcter més estesos utilitzen aquests caràcters en el sincronisme de trama. La figura 6 mostra com seria el sincronisme de trama amb aquests dos caràcters:

Figura 6

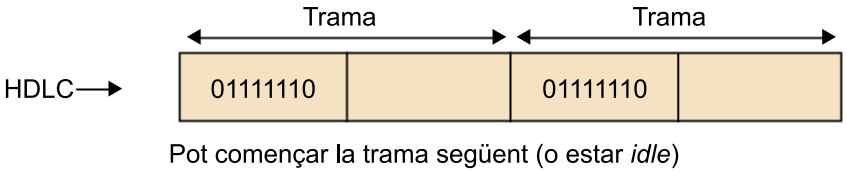


Un dels protocols orientats a caràcter més coneguts, BSC, utilitza els caràcters STX i ETX en la sincronització de les trames.

2) Sincronització de trama en una transmissió orientada a bit:

Com a exemple de sincronització de trama, considerarem la figura 7, que mostra els indicadors que utilitza el protocol HDLC:

Figura 7



En el protocol HDLC es defineix l'indicador de final de trama amb el mateix conjunt de bits que el d'inici de trama. El protocol permet que, si hi ha dues trames consecutives, l'indicador de final de trama sigui també el d'inici de trama de la següent, i així s'estalvia la transmissió d'aquest indicador.

2.3. Mecanisme de transparència

Les dades d'informació que transporta la trama són totalment arbitràries. Si no s'utilitza el camp de longitud, es pot donar el cas que en la detecció de final de trama, tant en transmissions orientades a caràcter com en les orientades a bit, un caràcter o un conjunt de bits de dades es pugui confondre amb l'indicador de final de trama. Això pot provocar situacions errònies, en què s'interpretarien erròniament finals de trama que no ho són. Per a evitar-ho s'utilitza un mecanisme de transparència, perquè la utilització del protocol no afecti en cap manera el missatge transmès.

Exemples de mecanismes de transparència

1) Mecanisme de transparència en una transmissió orientada a caràcter:

Per a aconseguir la transparència, el protocol BSC utilitza un tercer caràcter, el DLE[20]. Permet fer transparents ("escapar") caràcters de control que poden aparèixer fortuïtament dins del missatge (ja que aquest podria estar compost per qualsevol caràcter de l'alfabet del codi), i que en cas d'interpretar-se afectaria molt negativament el procés de la transmissió.

La tècnica per a aconseguir la transparència es coneix amb el nom de *farciment de caracters*[21]. El funcionament és el següent:

a) En transmissió:

- Els caràcters de control STX i ETX d'inici i final de trama van precedits d'un DLE.
- Quan troba un DLE entre les dades d'informació, insereix un altre DLE independentment del caràcter que segueixi. Per exemple, si els caràcters DLE-STX o DLE-ETX es troben barrejats en les dades, la capa d'enllaç insereix un DLE just abans de cada caràcter DEL, i envia finalment DLE-DLE-ETX o DLE-DLE-STX.

b) En recepció:

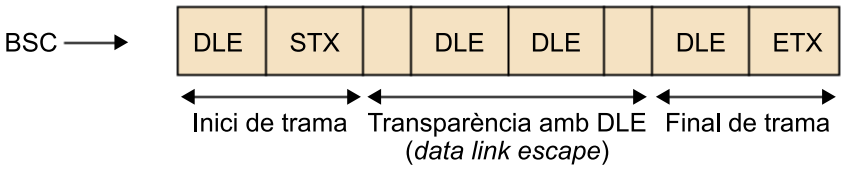
- Si rep els caràcters DLE-STX detecta inici de trama.
- Si rep els caràcters DLE-DLE, elimina un dels caràcters DLE i no s'interpreta el caràcter següent com a caràcter de control.
- Si rep DLE-ETX, ho interpreta com a final de trama.

(20) *DLE* és la sigla de *data link escape*.

(21) En anglès, *character stuffing*.

(22) En anglès, *bit stuffing*.

Figura 8



2) Mecanisme de transparència en una transmissió orientada a bit:

Hem vist que en el protocol HDLC l'indicador de delimitació de trama és 01111110. S'ha d'evitar que aquesta seqüència de bits es trobi dins del missatge de dades, perquè portaria a interpretacions errònies. El mecanisme de transparència que evita això rep el nom de *farciment de bit*[22] en protocols orientats a bit.

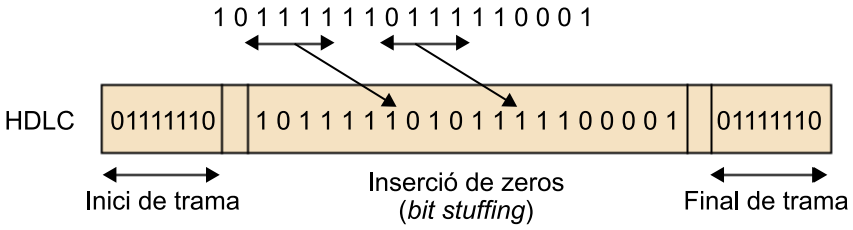
a) En TX:

Si hi ha cinc 1 seguits en el camp del missatge, s'insereix un 0 independentment del bit que segueixi a continuació. Si es produeix la coincidència que dins dels bits d'informació hi hagués l'indicador 01111110, la inserció del bit 0 faria que el receptor no ho interpretés com el final de trama. D'aquesta manera la seqüència de delimitació de trama (sis 1 seguits) és transmesa de manera única pel canal.

b) En RX:

El receptor elimina tots els 0 "extra" inserits pel transmissor. Si arriben cinc 1 seguits d'un 0, s'elimina el 0 i no s'interpreta la seqüència com un possible indicador.

Figura 9



2.4. Numeració i seqüenciació

Hem vist com els protocols de retransmissió ARQ[23] necessitaven numerar tant les trames d'informació com les trames de confirmació, per a poder relacionar unes amb altres i garantir d'aquesta manera el funcionament correcte de la retransmissions. Aquestes trames inclouen un número de seqüència en un dels camps de la capçalera que afegeix el protocol de nivell d'enllaç, juntament amb el camp de control, que serveix per a detectar possibles errors.

[23] *ARQ* és la sigla d'*automatic repeat request*.

Vegeu també

Vegeu la numeració de les trames en el mòdul "La capa de transport de dades" d'aquesta assignatura.

Veiem que la numeració de trames és conseqüència directa d'un protocol que fa recuperació automàtica d'errors (retransmissions); en la resta de casos no seria estrictament necessari fer una numeració de trames.

En el punt "Gestió de l'enllaç", veurem que normalment les trames de senyalització i control de l'enllaç (les que no són d'informació) no solen portar número de seqüència. Aquestes trames reben el nom de *trames no numerades*[24].

[24] En anglès, *unnumbered frames*.

2.5. Multiplexació en el nivell d'enllaç

El concepte de multiplexació ja s'ha introduït en altres mòduls de l'assignatura. Aquesta tècnica es pot utilitzar en qualsevol nivell de l'arquitectura de comunicacions. Veurem que també es pot trobar en un protocol de nivell d'enllaç.

La idea de la multiplexació consisteix a utilitzar un únic medi per a la transmissió de diferents fluxos d'informació.

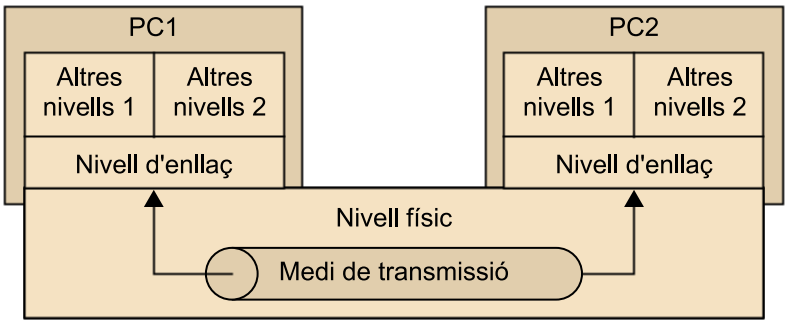
Òbviament, cal definir un mecanisme que permeti separar els diferents fluxos respecte a la recepció.

Vegem dos exemples en què pot ser útil tenir multiplexació en el nivell d'enllaç:

- Per exemple, en un enllaç multipunt. El fet de tenir el medi compartit es pot interpretar com si hi hagués un únic enllaç on es multiplexen les trames de les diferents estacions. El mecanisme de distinció de les diferents estacions es pot interpretar com un mecanisme de multiplexació. En aquest cas la multiplexació s'aconseguiria utilitzant una adreça de nivell d'enllaç, dins d'un dels camps de control de la trama, que identifica cada estació.

- Un altre exemple de multiplexació en el nivell d'enllaç és el que mostra la figura 10. En aquest exemple hi ha un nivell físic i d'enllaç comú i, per sobre, dues arquitectures de comunicacions (conjunt de protocols) diferents. En aquest cas el nivell d'enllaç porta les unitats d'informació de l'arquitectura 1 o 2 a la seva arquitectura parella 1 o 2, respectivament.

Figura 10. Exemple de multiplexació en el nivell d'enllaç



Aquest cas no és estrany en la pràctica, ja que hi ha nombrosos protocols de comunicacions que pot interessar que convisquin dins d'un mateix entorn i que comparteixin el mateix enllaç; per exemple, en una xarxa d'àrea local.

Per a poder distingir l'arquitectura que transmet les trames i, per tant, l'arquitectura a la qual cal lliurar-les, també s'utilitzen adreces de nivell d'enllaç.

2.6. Adreçament

L'adreçament en el nivell d'enllaç depèn del tipus d'enllaç existent:

- En els enllaços de comunicació punt a punt, el camp d'adreçament deixa de tenir sentit en haver-hi dues entitats participants en l'enllaç, i per tant és de sobres conegut l'altre extrem de l'enllaç. Per exemple, el camp *adreça* d'una trama PPP normalment porta sempre la mateixa adreça.

- En els enllaços de difusió, sí que es fa necessari el camp *adreça* de la capçalera de la trama, en haver-hi més d'un possible destinatari del missatge. Per exemple, Ethernet utilitza els camps d'adreça MAC destinació i origen amb tal finalitat.

3. Gestió de l'enllaç

Per *gestió de l'enllaç* entenem la manera com els nodes administren i estableixen l'enllaç, és a dir, si estructuren la transmissió per fases (com inicialització, manteniment i acabament), o bé fan transmissions sense establir una connexió prèvia.

El nivell d'enllaç reconeix dues maneres d'establir un enllaç entre dues entitats:

1) Protocols orientats a la connexió[25], com per exemple el protocol PPP.

[25]En anglès, *connection oriented*.

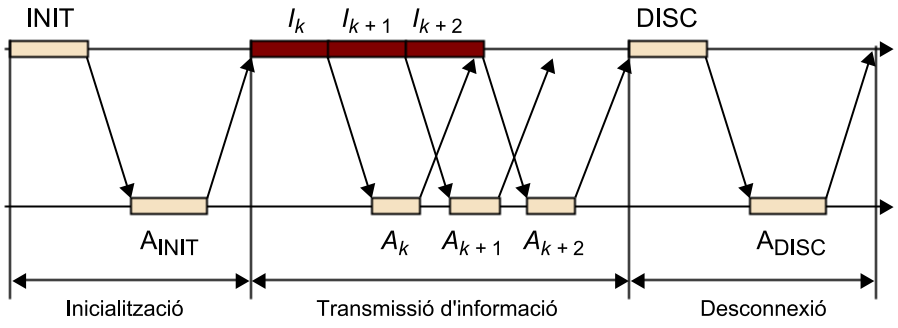
2) Protocols no orientats a la connexió[26], com per exemple el protocol Ethernet.

[26]En anglès, *connectionless*.

Un protocol orientat a la connexió és aquell que necessita una fase d'inicialització prèvia a la fase de transmissió de trames d'informació, en què normalment es negocien paràmetres necessaris per a la transmissió. També necessita una fase de desconnexió, en la qual s'acorda l'acabament de l'enllaç. Aquesta fase permet alliberar els recursos que s'hi dediquen, com les memòries intermèdies per a emmagatzemar les llistes de transmissió i recepció.

La figura 11 mostra les diferents fases que hi pot haver en una comunicació orientada a connexió:

Figura 11. Fases d'inicialització i desconnexió en un protocol orientat a la connexió



La trama INIT sol·licita la inicialització, que és confirmada per la trama AINIT. Les trames DISC i ADISC funcionen de manera anàloga per a la desconnexió. Aquestes trames són de control, necessàries per a l'establiment de l'enllaç, però no porten informació útil de nivells superiors. En les trames hi ha un camp de control que indica el tipus de trama, i que les permet diferenciar.

Les trames de control no solen estar numerades. La numeració de trames d'informació és necessària en protocols de recuperació automàtica d'errors, els quals generalment són orientats a la connexió.

En canvi, en un protocol d'enllaç no orientat a la connexió les entitats es comencen a intercanviar trames d'informació sense previ avís per l'enllaç. Habitualment són protocols que no utilitzen recuperació d'errors en el nivell d'enllaç i que, per tant, no necessiten numeració. En aquest cas tindríem un nivell d'enllaç no orientat a la connexió que podria fer detecció d'errors (descartant les trames errònies) però demanar la retransmissió de trames rebudes incorrectament.

Hi ha motius que poden justificar un nivell d'enllaç no orientat a la connexió: en aplicacions en temps real en les quals es transmet veu o vídeo, per exemple, és possible que el retard que es necessiti per a poder fer la recuperació d'errors no sigui acceptable.

De manera més concreta, la capa d'enllaç pot subministrar un dels tipus següents de servei a la capa de xarxa (són els tipus de servei que subministra el protocol HDLC):

1) Servei no orientat a connexió i sense justificant de recepció

La tramesa es fa sense esperar cap indicació del receptor sobre l'èxit o fracàs de l'operació. Tampoc no s'estableix o allibera una connexió. Aquest tipus de servei és apropiat quan la taxa d'error és molt baixa (xarxes locals o fibra òptica) i es deixa la missió de comprovar la correcció de la transmissió a les capes superiors (nivell de xarxa o de transport). També s'usa el servei no confirmat quan es vol transmetre informació en temps real (típicament, veu o dades) i no es vol sofrir el retard que imposaria un servei més sofisticat en la capa d'enllaç (se suposa que aquest tipus d'informació pot sofrir una petita taxa d'error sense efecte apreciable).

2) Servei no orientat a connexió amb justificant de recepció

Es produeix un justificant de recepció per a cada trama enviada encara que no hi hagi encara establiment de connexió. D'aquesta manera l'emissor pot estar segur que ha arribat.

3) Servei orientat a connexió amb justificant de recepció

És el més segur i sofisticat. L'emissor i el receptor estableixen una connexió explícita per endavant, les trames per enviar s'enumeren, i s'asseguren que són rebudes totes correctament en destinació i han estat transmeses a la capa de xarxa.

En el servei orientat a connexió es poden distingir tres fases: establiment de la connexió, tramesa de les dades i acabament de la connexió. En la primera es disposen els comptadors i memòries temporals necessaris per a la transmissió, en la segona s'envien les dades, i en la tercera s'allibera la memòria ocupada amb dades temporals i variables.

4. Control d'errors

En cas que es rebi una trama amb errors, el nivell d'enllaç pot adoptar una de les solucions següents:

1) Detecció d'errors i descart de la trama

Es tracta d'un servei molt comú en els protocols de la capa d'enllaç, que generalment s'implementa en maquinari. És un mecanisme que permet detectar si algun bit de la trama original ha canviat a causa d'efectes indesitjables del canal (atenuació, soroll, etc.). En cas que la comprovació doni positiva, es rebutjaria la trama o es prendrien altres accions. Les capes de transport i de xarxa també proporcionen una forma limitada de detecció d'errors. La detecció només és factible en aplicacions que tolerin un cert grau d'error en la informació rebuda.

2) Correcció d'errors (si s'utilitza un codi corrector adequat)

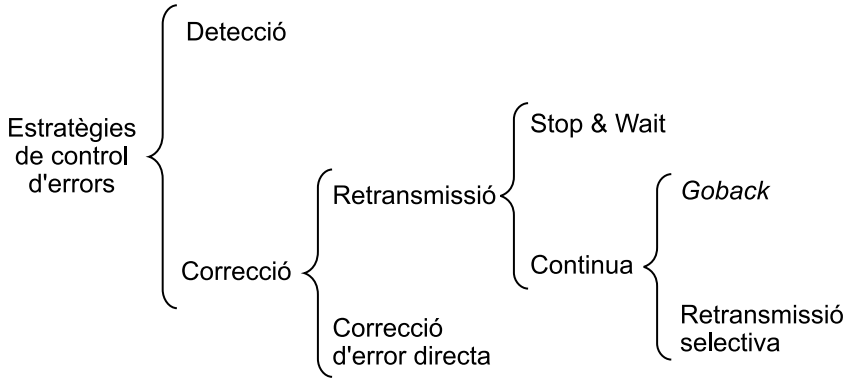
La correcció d'errors és similar a la detecció, però ara el receptor no solament es limita a detectar errors en els bits de la trama, sinó que intenta determinar on s'han produït aquests errors (i, per tant, corregir-los). Alguns protocols (com per exemple ATM) proporcionen correcció d'errors només per a la capçalera del paquet, però no és un servei gaire comú.

3) Sol·licitar la retransmissió per a un lliurament fiable

El servei de lliurament fiable de la capa d'enllaç es fa mitjançant reconeixements i retransmissions. Es tracta d'un servei poc comú en els protocols de nivell d'enllaç, ja que tradicionalment aquesta funcionalitat la fa el nivell de transport de la torre TCP/IP. Normalment aquesta utilització pren sentit en enllaços propensos a taxes d'error altes, com els enllaços sense fils, amb l'objectiu de corregir un error localment (en l'enllaç quan ocorre l'error) en lloc de forçar una retransmissió d'extrem a extrem de les dades per un protocol de nivell superior. Tanmateix, el lliurament fiable de la capa d'enllaç es pot considerar com una despesa innecessària per a enllaços d'errors en pocs bits, com els de fibra òptica, els de cable coaxial, i molts parells trenats de coure. Per aquesta raó, molts protocols de la capa d'enllaç no proporcionen un servei de lliurament fiable.

Aquestes estratègies en la lluita contra els errors estan resumides en la figura 12.

Figura 12



4.1. Estratègies de detecció d'errors

Suposem que el nivell d'enllaç és capaç de delimitar perfectament les trames del flux de bits que rep del nivell físic. Ara ens queda el problema de detectar quines d'aquestes trames tenen un o més bits erronis. En aquest apartat veurem majoritàriament alguns conceptes bàsics de la detecció d'errors i també alguns de la correcció d'errors.

Les tècniques de detecció i correcció d'errors són dues tècniques de control d'errors que garanteixen la integritat de les trames enviades a través d'un canal amb errors, i combaten els efectes indesitjables que introdueix, com l'atenuació, les interferències, el soroll, etc.

4.1.1. El soroll i els seus efectes

El soroll és el component que s'incorpora al missatge en algun moment de la transmissió i que no solament no eleva el nivell d'informació sinó que fins i tot el pot fer disminuir per sota de l'inicial. Es classifica en extrínsec, o aliè al circuit de dades, i intrínsec, que té el seu origen en algun element d'aquest circuit. Seria ideal que les transmissions es duguessin a terme sense soroll, però això no és possible.

El soroll en els sistemes de transmissió produeix errors. Denominem *taxa d'error en els bits* la relació existent entre el nombre de bits rebuts erròniament en un interval de temps i el nombre de bits enviats en aquell temps. La mesura d'aquesta magnitud s'ha d'efectuar en un interval prou llarg per a proporcionar una mitjana. L'ITU-T recomana un mínim de 15 min. En els sistemes comercials més usuals, aquesta taxa d'error sol fluctuar entre 10-4 i 10-12 en funció de les línies, la velocitat de transmissió, etc.

$$t_{Error} = \frac{Bits\ erronis}{Total\ bits}$$

Definim com a *taxa d'error residual* la relació entre el nombre de bits rebuts erròniament i no detectats o corregits en un període de temps pel sistema de protecció antierror que s'està aplicant (si és que se n'aplica algun) i el nombre total de bits enviats. Aquesta taxa és la que permet apreciar la seguretat d'un sistema teleinformàtic.

$$t_{Error\ residual} = \frac{Bits\ erronis\ no\ detectats}{Total\ bits}$$

4.1.2. Mètodes de lluita passiva

Un primer nivell de disminució d'errors s'aconsegueix disminuint les causes que els produeixen. Es tracta d'aplicar mètodes de lluita passiva, tal com podem veure en la taula següent:

Diferents sorolls i mètodes de lluita passiva aplicats		
Tipus de soroll	**Causa**	**Sistema de lluita passiva**
Eco	Males connexions. Mal estat de les línies.	Supressor d'eco.
Soroll blanc	Agitació tèrmica de la matèria a temperatura per sobre del zero absolut. D'altres.	Filtratge i ampliació. Utilització de bons conductors (superconductors) o fibra òptica.
Soroll impulsiu	Interferències electromagnètiques i descàrregues de qualsevol tipus sobre la línia o el seu entorn.	Blindatge de la línia. Utilització de línies de fibra òptica
Distorsió de fase	Característiques físiques de la línia utilitzada.	Equalitzador (amplificador selectiu).
Distorsió d'atenuació	Característiques físiques de la línia utilitzada.	Equalitzador (amplificador selectiu).
Diafonia	Inducció electromagnètica en conductors adjacents.	Trenat de parells. Blindatge dels parells. Ús de coaxial o fibra òptica.
Dispersió intermodal	Contrafases als feixos multimode d'índex escalonat en fibra òptica.	Ús de fibra monomode o multimode d'índex gradual.
Errors en connexions, equips i d'altres	Equips de transmissió defectuosos o amb tecnologia obsoleta.	Instal·lació i manteniment adequats. Millores tècniques.

No obstant això, el soroll no pot ser eliminat totalment del sistema, i per això en el cent per cent dels supòsits la probabilitat d'error és gran i s'ha de tenir en compte.

4.1.3. Aspectes bàsics de la detecció d'errors: codificació per a la protecció

Davant de la impossibilitat d'eliminar els errors, i si volem evitar les seves desagradables conseqüències en la transmissió de dades, sorgeix la necessitat de detectar-los una vegada generats per a aconseguir que el missatge emès es pugui reconstruir en l'extrem receptor amb la màxima fidelitat.

Tota trama pot tenir una combinació de bits arbitrària. Si hi ha error en un bit de la trama o més, la nova combinació és una altra possible trama. D'aquesta manera, només mirant els bits de la trama no és possible esbrinar si n'hi ha algun d'erroni.

En gairebé tots els casos, els sistemes utilitzats per a la protecció passen per la codificació. Aquesta tècnica consisteix a afegir bits extra a la trama realment enviada, de manera que en recepció permeti la detecció d'errors. Aquests bits extra es calculen a partir dels bits que cal protegir.

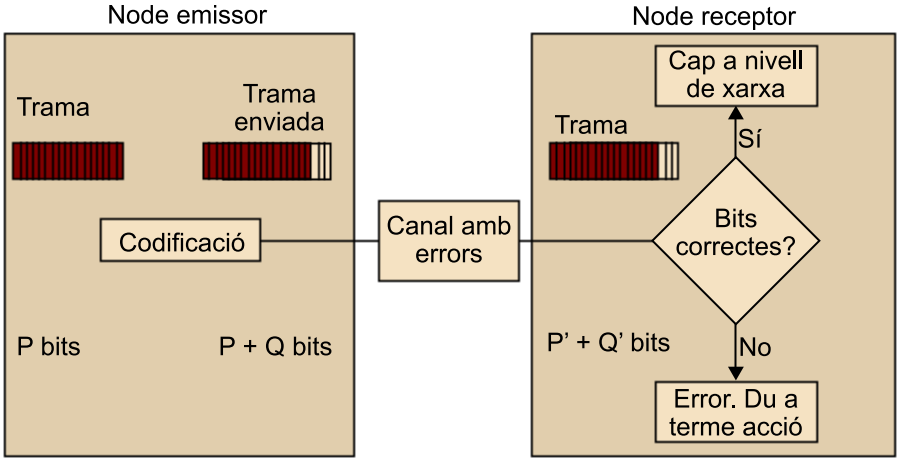
En afegir aquests bits estem utilitzant més bits dels estrictament necessaris per a transmetre la trama. Per aquest motiu es diu que els codis detectors d'errors afegeixen redundància als bits de dades que es volen protegir. Es defineix el concepte de redundància d'un codi com la diferència entre la informació màxima que podria proporcionar aquest codi utilitzant el seu alfabet i la que proporciona realment:

$$\%_{Redund} = \frac{Bits\ de\ control}{Bits\ totals} \times 100$$

Procés de la codificació

En la figura 13 podem observar el funcionament de l'operació de codificació d'una trama de *P* bits:

Figura 13



Suposem que la mida de la trama d'informació és de *P* bits, i que afegim *Q* bits per a la detecció i correcció d'errors dels *P* bits anteriors. Per tant, veiem que transformem el conjunt dels *P* bits que volem protegir en una nova combinació de *P* + *Q* bits. Ens referirem a aquesta nova combinació com a *paraula codi* del nou codi creat. Aquesta transformació és biunívoca, és a dir, a cada combinació determinada dels *P* bits que cal protegir correspon una sola combinació de *P* + *Q* bits, i viceversa.

Paraula codi

En aquest apartat ens referirem a les trames com a *paraules codi*, que és el terme que s'utilitza en el context de la detecció d'errors.

Es pot protegir tant el datagrama encapsulat dins de la trama com la seva capçalera, en què hi ha la informació d'adreçament en l'àmbit d'enllaç, els números de seqüència, etc.

Pel canal són enviats al node receptor tots els bits junts en una trama de nivell d'enllaç. El node receptor rep la nova trama de $P' + Q'$ bits, cosa que vol dir que pot ser diferent de la seqüència original tant en el missatge com en els bits de control d'error. El repte del receptor és determinar si la seqüència P' és igual o no que l'original P, ja que només ha rebut P' i Q'.

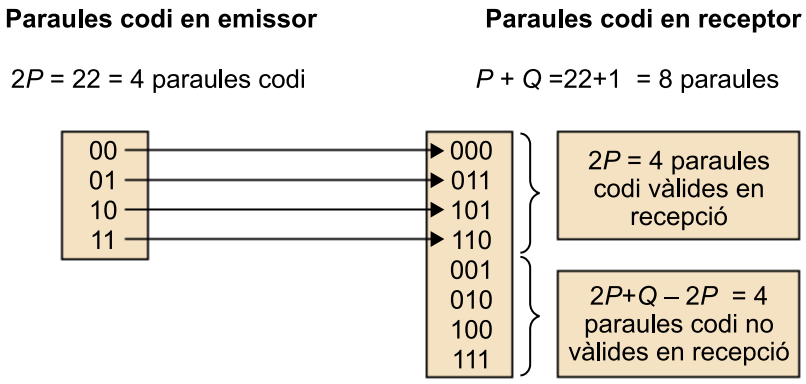
Aquesta qüestió es resol en termes deterministes, però veurem que hi haurà certes probabilitats de no detectar seqüències errònies. En efecte, observem que el nombre de paraules codi vàlides és igual al nombre de combinacions possibles dels bits de les dades que volem protegir ($2P$). En canvi, el nombre possible de paraules codi en recepció és de $2P + Q$. Les $2P + Q – 2Q$ combinacions restants són paraules codi no vàlides i no s'utilitzaran mai en transmissió (perquè no poden resultar mai de la transformació que aplica el codi als P bits que s'han de protegir).

Detectem que hi ha un error quan els bits erronis transformen una paraula codi vàlida en una de no vàlida. Si com a conseqüència dels bits erronis resulta una altra paraula codi vàlida, no detectarem l'error.

Exemple de detecció d'errors

Observem l'exemple següent en què cada paraula codi original de $P = 2$ bits s'ha protegit amb $Q = 1$ bit de redundància. La protecció utilitzada per a confeccionar la lògica del bit redundant ha estat l'OR exclusiva dels bits originals:

Figura 14



Podem obtenir les situacions següents en la transmissió de la seqüència "11":

Paraula codi rebuda	Acció	Decisió correcta
110	Paraula vàlida	SÍ
111	Paraula no vàlida	SÍ
101	Paraula vàlida	NO : situació per evitar

Havíem d'haver rebut "110", però en l'últim cas s'ha rebut la seqüència "101", en produir-se dos errors durant la transmissió. Mirem la taula de correspondència de paraules codi, i de manera determinista deduïm que la transmissió ha estat correcta. Però en realitat ha ocorregut un error no detectat.

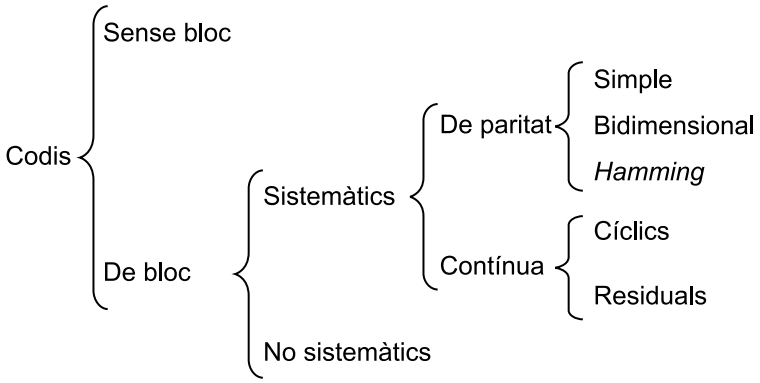
De manera implícita observem que hi ha un límit en la detecció d'errors per a una determinada codificació. En concret, la codificació anterior només permet detectar en un bit. Falla quan hi ha errors en més d'un bit.

4.1.4. Classificació dels codis detectors / correctors d'errors

L'estructura dels codis varia segons el tipus d'error que ha de detectar o corregir. Normalment, els codificadors i descodificadors s'implementen en autòmats lineals. Sorgeix, doncs, la necessitat d'aconseguir un equilibri entre la capacitat de tractament del codi, la velocitat de codificació i descodificació i la complexitat i el cost dels circuits associats.

A la figura 15 es proposa una classificació dels codis de transmissió de dades.

Figura 15



- Els **codis de bloc** es caracteritzen perquè el nombre d'elements que componen les paraules és constant. En aquests resulta de gran importància el concepte de distància de Hamming que veurem més endavant.

- Els **codis no sistemàtics** són aquells que formen les seves paraules aleatòriament a partir d'un conjunt de dues possibles paraules. Aquest conjunt ha d'existir també en la memòria de treball del receptor, perquè aquest pugui buscar la paraula rebuda i així comprovar que la transmissió és correcta. Per exemple, si s'estableix un codi per a transmetre dates en el qual els mesos se substitueixen per un signe del Zodíac, serà necessari que emissor i receptor tinguin la taula de signes en memòria juntament amb la correspondència mesos-signes.

- Els **codis sistemàtics** utilitzen un algorisme reversible que permet al receptor recuperar o comprovar la paraula original aplicant aquest algorisme en sentit invers a l'emissor. Per exemple, el mateix codi per a transmetre dates, però ara el mes es codifica utilitzant l'algorisme següent: nouMes = (13 – mes) + (anydeTraspas?1:0).

Ara ja no és necessari que emissor i receptor desin una taula de símbols, sinó que siguin capaços d'invertir l'algorisme anterior: mes = 13 + (anydeTraspas?1:0) – nouMes.

En aquest mòdul estudiarem els codis de paritat simple, bidimensional i de Hamming i els codis continus cíclics (CRC[27]) i les sumes de comprovació[28]. Tots són codis detectors d'errors i alguns, sota determinades circumstàncies, també permeten la correcció d'errors.

[27] *CRC* és la sigla de *cyclic redundancy check*.

[28] En anglès, *checksum*.

Veurem que:

- Les comprovacions de paritat s'utilitzen molt poc en la pràctica.
- Les sumes de comprovació són utilitzades en les capes de xarxa i de transport.
- Les comprovacions de redundància cíclica són utilitzades en la capa d'enllaç.

4.1.5. Robustesa d'un codi detector d'errors

No sempre s'aconsegueixen detectar tots els errors de bits que provoca el canal de transmissió. Hem vist que hi ha la possibilitat que el nivell d'enllaç no detecti seqüències de bits que contenen errors, de manera que el receptor pot lliurar un datagrama adulterat a la capa de xarxa.

Una mesura ideal per a comparar els diferents codis detectors d'error seria determinar la probabilitat que es produís un error no detectat en la transmissió d'una trama. Desafortunadament, aquesta probabilitat depèn de les característiques del medi de transmissió i del codi detector d'errors, i per això resulta difícil de determinar.

Per a mesurar empíricament la probabilitat d'una trama errònia no detectada hauríem de comptabilitzar totes les trames errònies no detectades i totes les trames errònies que es produeixen en l'enllaç. La relació entre aquests dos valors seria la probabilitat buscada.

A causa de les dificultats que comporta determinar la probabilitat d'una trama errònia no detectada, considerarem els tres paràmetres per a mesurar la **robustesa d'un codi detector d'errors**, que s'expliquen a continuació:

1) La distància mínima del codi (distància de Hamming del codi).

2) La capacitat de detecció de ràfegues d'error[29].

(29)En anglès, *burst detecting capability*.

3) La probabilitat que una combinació arbitrària de bits sigui acceptada com a paraula vàlida.

Com veurem a continuació, per a prendre aquestes mesures no hem de tenir en compte el tipus d'errors que introdueix el medi de transmissió. És a dir, aquestes mesures donen idea de la facilitat que té un codi per a determinar certs tipus d'errors. A l'hora de triar un codi o un altre caldrà tenir en compte quin tipus d'error introdueix el medi de transmissió per a triar el codi més adequat, és a dir, el que minimitzi la probabilitat de tenir una trama errònia no detectada.

Volem, per tant, triar un esquema de detecció d'errors en el qual la probabilitat d'aquestes ocurrències sigui petita. Generalment, les tècniques de detecció i correcció d'errors més sofisticades (és a dir, aquelles que tenen una probabilitat menor de permetre errors de bits no detectats) incorren en un cost major (es necessita més computació per a computar i transmetre un grau major de detecció i correcció d'errors de bits).

Probabilitats

És important no confondre la probabilitat d'error en una trama amb la probabilitat d'una trama errònia no detectada. La probabilitat d'error en una trama depèn exclusivament del medi. La probabilitat d'una trama errònia no detectada és molt més difícil de calcular perquè depèn, a més, del codi detector d'errors. El codi detector ideal detectaria totes les trames errònies.

Distància de Hamming

Per a definir la distància de Hamming d'un codi, primer és necessari introduir el concepte de distància de Hamming entre dues paraules codi.

La distància de Hamming entre dues paraules codi es defineix com el nombre de bits diferents que hi ha entre aquestes paraules. La distància mínima d'un codi, o distància de Hamming d'un codi, es defineix com la menor distància que hi ha entre dues paraules vàlides qualssevol del codi.

Exercici

6. Calculeu la distància de Hamming entre aquestes dues paraules codi: 100100101 i 000100001.

Solució de l'exercici 6

Entre les paraules codi següents, hi ha 2 bits de diferència; per tant, la seva distància val 2:

100100**1**01
000100**0**01

De la definició de la distància de Hamming d'un codi deduïm també que un mètode exhaustiu per a calcular-la seria considerar totes les parelles possibles de paraules vàlides, observar quants bits diferents hi ha i prendre el mínim. En la pràctica, generalment no s'aplica aquest mètode, sinó que el càlcul es fa a partir de les propietats del codi.

Com més gran és la distància de Hamming, més bits erronis hi ha d'haver perquè es produeixi un error no detectat i, per tant, el codi detector d'errors serà millor.

D'aquesta definició es dedueix que si la distància de Hamming d'un codi val *DH*, qualsevol combinació de *n* bits erronis es detectarà amb probabilitat 1, si compleix que:

$$N < D_H$$

Capacitat de detecció d'una ràfega d'error

Moltes vegades els errors no es produeixen en bits aïllats, sinó que són originats per espurnes (interferències) que afecten diferents bits consecutius. Normalment, tanmateix, una espurna no introdueix errors en tots els bits que coincideixen amb la seva durada. Segons les variacions elèctriques de la intensitat de l'espurna, alguns bits canvien, amb la qual cosa es produeix un error, i d'altres no canvien.

En una trama es defineix la ràfega d'error com el nombre de bits que hi ha entre el primer bit erroni i l'últim, tots dos inclosos.

La capacitat de detecció d'una ràfega d'error es defineix com l'enter major, anomenat *B*, tal que el codi és capaç de detectar totes les ràfegues d'error menors o iguals que *B*.

Exemple de ràfega d'error

En la trama següent, els bits erronis són els que estan marcats. Ja que entre el primer bit erroni i l'últim (tots dos inclosos) hi ha 7 bits, diem que la ràfega d'error val 7:

```
101000000000000
```

Evidentment, com més gran sigui la capacitat de detecció de ràfegues d'error, millor serà el codi detector d'errors.

La capacitat de detecció de ràfegues d'error és especialment important quan el medi de transmissió té tendència a introduir els errors en forma de ràfegues. En aquest cas, com més gran sigui la capacitat de detecció de ràfegues, menor serà la probabilitat de tenir una trama errònia no detectada.

Probabilitat que una combinació arbitrària de bits sigui acceptada com a paraula vàlida

Hem vist que si el nombre de bits erronis d'una trama no excedeix la distància de Hamming ni la capacitat de detecció de ràfegues, la trama errònia es detectarà amb probabilitat 1. En cas contrari, hi ha dues possibilitats:

a) La paraula codi corresponent a la trama errònia coincideix amb una altra paraula codi vàlida i, per tant, no es detecta l'error.

b) La paraula codi resultant és una paraula no vàlida i es detecta l'error.

El càlcul exacte de la probabilitat que la trama errònia no sigui detectada no és obvi. No obstant això, podem deduir de manera intuïtiva un valor aproximat, fent la suposició següent: que la paraula codi corresponent a la trama errònia passa a ser, amb la mateixa probabilitat, qualsevol altra paraula codi. Això equival a suposar que es tria una combinació arbitrària de bits. Si aquesta combinació és una paraula codi vàlida, no es detectarà l'error; si no ho és, l'error es detectarà.

Com que una paraula codi té una mesura de $P + Q$ bits, cada una de les combinacions arbitràries possibles es pot rebre amb una probabilitat d'$1/2^{P+Q}$. Com que hi ha 2^P paraules codi vàlides, la probabilitat que una combinació arbitrària de bits sigui acceptada com una paraula vàlida serà $2^P / 2^{P+Q} = 2^{-Q}$.

La probabilitat que una combinació arbitrària de bits sigui acceptada com una paraula vàlida és 2^{-Q}, en què Q és el nombre de bits que afegeix el codi detector d'errors.

Com més gran sigui Q, menor serà aquesta probabilitat i millor serà el codi. Això demostra que, com més bits afegeix el codi detector d'errors, més difícil és que es produeixi un error no detectat.

4.1.6. Comprovacions de paritat

S'utilitzen poc en la pràctica perquè són poc robustos. No obstant això, són útils per a proporcionar comprensió de les tècniques de correcció d'errors.

Paritat simple (bit de paritat)

És el codi detector d'errors més senzill que hi ha. El control de paritat consisteix a afegir un sol bit (denominat *bit de paritat*) al bloc de bits que es vol protegir. Si la informació per enviar té P bits, l'emissor simplement inclou un bit addicional de paritat, i transmet $P + 1$ bits.

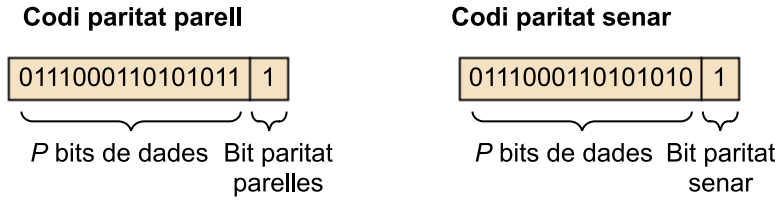
El valor del bit de paritat codifica el nombre total d'uns de la seqüència de P + 1 bits (la informació original més el bit de paritat). Hi ha dos esquemes segons com es codifiqui el bit de paritat:

- Esquema de paritat parell: bit de paritat a 1, si el nombre d'uns de la seqüència P + 1 és parell.

- Esquema de paritat senar: bit de paritat a 1, si el nombre d'uns de la seqüència P + 1 és senar.

La figura 16 mostra un esquema de paritat parella i un altre de senar, amb el bit de paritat simple emmagatzemat en un camp separat:

Figura 16



L'operació del receptor és també senzilla amb un bit de paritat simple. El receptor només necessita comptar el nombre d'uns en els P + 1 bits rebuts.

Si en la transmissió de la paraula codi es produeix un sol error (un 1 passa a valer 0 o un 0 passa a valer 1), la paritat de la paraula codi canviarà i no coincidirà amb la del bit de paritat. Per tant, es detectarà l'error. Però si es produeix un nombre parell d'errors de bits, la paritat serà la mateixa i l'error no es detectarà. Deduïm, doncs, que amb el bit de paritat el codi es permet detectar un nombre senar de bits erronis.

Càlcul del bit de paritat

Per a la generació del bit de paritat, els sistemes informàtics utilitzen el càlcul de l'operació binària XOR dels bits que es volen protegir:

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

- Per a la paritat parella, el bit de paritat es calcula:

$$P = b1 \oplus b2 \oplus ... \oplus bn$$

- Per a la paritat senar, el bit de paritat es calcula:

$$P = NOT(b1 \bigoplus b2 \bigoplus \ldots \bigoplus bn)$$

Utilització de la tècnica de bit de paritat

Quan s'utilitza la paritat com a codi detector d'errors, no hem d'imaginar que tota la trama està protegida amb un sol bit de paritat. La paritat únicament s'utilitza en transmissions orientades a caràcter asíncrones de baix rendiment, en què les trames d'aquestes transmissions estan formades per més d'un caràcter, cada un amb el seu bit de paritat.

La paritat simple és el codi detector d'errors que més s'utilitza en transmissions orientades a caràcter. Per exemple, la transmissió pel port sèrie d'un PC és orientada a caràcter. El dispositiu que controla el port sèrie (denominat *UART*[30]) afegeix automàticament un bit de paritat a cada caràcter transmès. Respecte a la recepció, l'UART també controla automàticament que el bit de paritat sigui correcte; en cas contrari, es produeix una condició d'error.

[30] *UART* és la sigla d'*universal asynchronous receiver transmitter*.

Robustesa del codi de paritat simple

Deduirem el valor dels tres paràmetres, introduïts anteriorment, que defineixen la robustesa del codi de paritat simple.

a) Per a qualsevol paraula vàlida, si es canvia un bit s'obté una paraula no vàlida, i si se'n canvien dos s'obté una altra paraula vàlida. Deduïm, doncs, que la diferència mínima entre dues paraules codi vàlides és de dos bits i, per tant, que la distància de Hamming val 2. En conseqüència, el codi és capaç de detectar amb probabilitat 1 totes les combinacions de bits erronis inferiors a 2 (és a dir, el codi detecta un bit erroni, com havíem vist anteriorment).

b) Ja que el codi no detecta una ràfega d'error igual a 2 (dos bits consecutius erronis), la capacitat de detecció de ràfegues val 1. És incapaç de detectar un nombre parell d'errors i tampoc no permet determinar la posició del bit erroni.

c) Finalment, la probabilitat que una combinació arbitrària de bits sigui acceptada com a paraula vàlida és $2^{-Q} = 2^{-1} = 0{,}5$, és a dir, dels caràcters que tinguin molts bits erronis, només se'n detectaran la meitat.

Veiem, per tant, que en condicions d'error ratxat, la probabilitat d'errors no detectats en una trama protegida per una paritat de bit simple és molt alta (es pot aproximar al 50%).

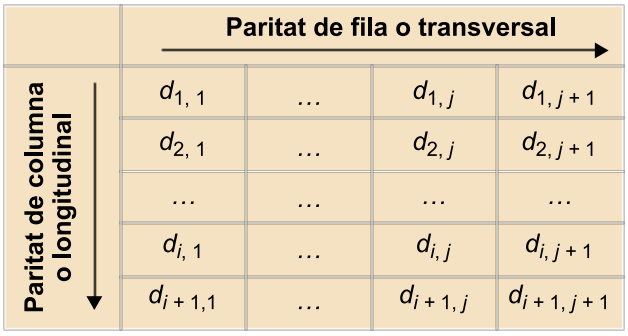
Codis de paritat bidimensional

Una manera de millorar la robustesa del codi detector d'errors per mitjà del bit de paritat consisteix a organitzar els *P* bits que cal protegir en una matriu de *i* files i *j* columnes. Es calcula un valor de paritat per a cada fila i per a cada columna.

La paritat de les files es denomina **paritat transversal** (o horitzontal), i la de les columnes, **paritat longitudinal** (o vertical). Els $i + j + 1$ bits de paritat resultants comprenen els bits de detecció d'error de la trama d'enllaç de dades.

Així doncs, la informació es transmet organitzada en blocs amb la seva paritat longitudinal i transversal respectiva. La transmissió del bloc es fa per files, de manera que els últims bits transmesos són els bits de la paritat longitudinal. La figura 17 mostra una generalització de dues dimensions de l'esquema de paritat de bit únic.

Figura 17



En la figura:

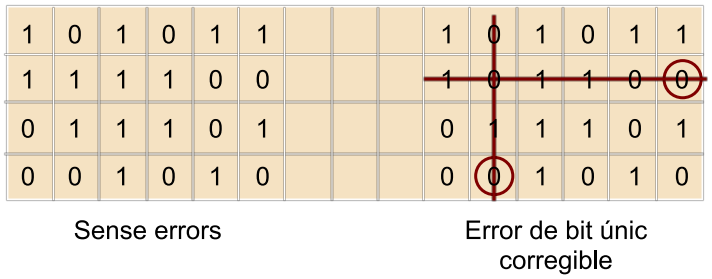
- $d_{i+1,x}$ per a $x \in [1,j]$ són paritats longitudinals.
- $d_{x,j+1}$ per a $x \in [1,i]$ són paritats transversals.
- $d_{i+1,j+1}$ és la paritat de les paritats transversals resultants, que coincideix amb la paritat de les paritats longitudinals. Es denomina *bit de quadrament*.

Funcionament en presència d'errors

Suposem ara que ocorre un error de bit únic en els *P* bits originals d'informació. Amb aquest esquema de paritat de dues dimensions, la paritat de la fila i la columna que contenen el bit canviat donarà un error. El receptor no solament podrà detectar l'error d'un bit simple sinó que es poden utilitzar els índexs de la fila i de la columna amb errors de paritats per a identificar de fet el bit que s'ha modificat i corregir aquest error.

La figura 18 mostra un exemple d'un bit amb valor 1 en la posició (2, 2) que s'ha modificat i ha canviat a 0.

Figura 18

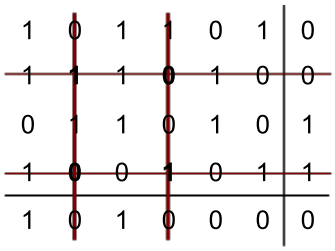


Una vegada comprovat que el bit de les paritats transversals coincideix amb les paritats longitudinals i transversals de la matriu, es pot aïllar el valor de la matriu (*i*, *j*) erroni per mitjà de les paritats de les files i columnes que resultin errònies. No solament detectarem l'error en les dades originals, sinó que també el podrem corregir.

De la mateixa manera, no solament es pot detectar i corregir un error en els bits originals d'informació, sinó també en els bits de paritat mateixos. No obstant això, una combinació de dos errors en un paquet pot ser detectada, però ja no corregida.

A continuació investigarem els casos en els quals una combinació d'errors no seria detectada. De la definició de paritat deduïm que aquest codi detectarà totes les combinacions de bits erronis que tinguin un nombre senar d'errors en alguna fila o columna. És a dir, no es detectaran les combinacions de bits erronis que tinguin un nombre parell d'errors en totes les files i columnes simultàniament. El cas més senzill és el que mostra la figura 19.

Figura 19. Combinació d'errors que no seria detectada



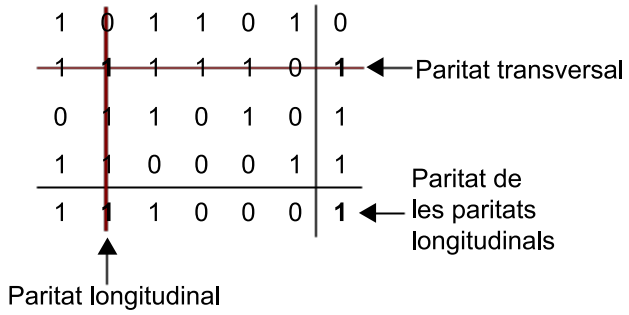
En aquest cas el sistema de codificació fallarà, i es prendrà com a vàlida una seqüència de dades amb errors.

Robustesa del codi de paritat bidimensional

Deduirem el valor dels paràmetres que mesuren la robustesa del codi de paritat bidimensional:

a) Si en un bloc canvia un dels bits que cal protegir, canviaran, a més, les paritats transversal, longitudinal i la paritat de les longitudinals: canvien 4 bits, i per tant $D_H = 4$.

Figura 20. Bits que canvien entre dues paraules codi vàlides consecutives



b) Per a determinar la capacitat de detecció de ràfegues hem de trobar la ràfega mínima no detectada. A partir de la figura 19 és fàcil deduir que la ràfega mínima no detectada es produeix quan els quatre bits erronis són adjacents, i la seva mida és igual a la longitud d'una fila més dos. Així doncs, la capacitat de detecció de ràfegues és la longitud d'una fila més u.

c) La probabilitat que una combinació arbitrària de bits sigui acceptada com a paraula vàlida és $1/2^{\text{Longitud fila + Longitud columna – 1}}$

Utilització del codi de paritat bidimensional

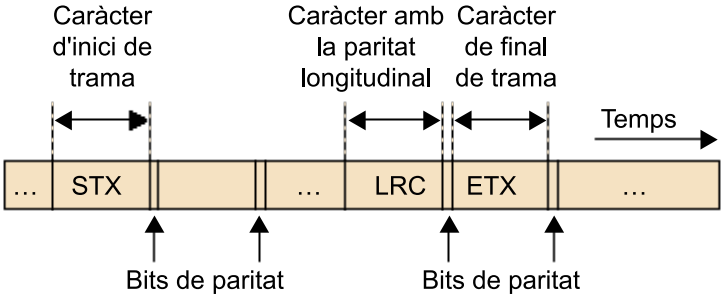
El codi de paritat longitudinal i transversal s'acostuma a utilitzar en transmissions asíncrones orientades a caràcter. El dispositiu transmissor afegeix automàticament un bit de paritat a cada caràcter, i d'aquesta manera la trama queda formada per un conjunt de caràcters als quals s'afegeix un caràcter amb la paritat longitudinal.

La figura 21 ens mostra la disposició que acabem d'explicar dels bits de paritat dins de la trama. A causa d'aquest caràcter extra, aquest codi detector d'errors es coneix també com a LRC[31] o BCC[32].

(31) *LRC* és la sigla de *longitudinal redundancy check*.

(32) *BCC* és la sigla de *block check character*.

Figura 21. Transmissió d'una trama amb els bits de paritat i el caràcter de paritat longitudinal LRC



El caràcter LRC se sol calcular fent l'operació XOR (paritat parella) dels caràcters que es volen protegir

És molt menys habitual que l'anterior, a causa, entre d'altres raons, de la gran ocupació de canal, que en el cas de blocs de 8 × 8 representa una redundància del 22,2% si no comptem el bit de quadrament, i del 23,4% incloent-lo.

Mètodes de comprovació de sumes

En la tècnica de comprovació de sumes, els *P* bits de la seqüència enviada són tractats com una seqüència d'enters de *k* bits. Un mètode senzill de comprovació de sumes consisteix simplement a sumar aquests enters de *k* bits, i utilitzar la suma resultant com a bits de detecció d'errors.

L'RFC 1071 discuteix l'algorisme de comprovació de suma d'Internet en detall. S'implementa per a comprovar la integritat i detectar errors en el datagrama d'Internet. Però en el seu càlcul només té en compte els octets[33] de la capçalera IP (només protegeix els camps de la capçalera, com l'adreça IP origen i destinació).

(33)En anglès, *bytes*.

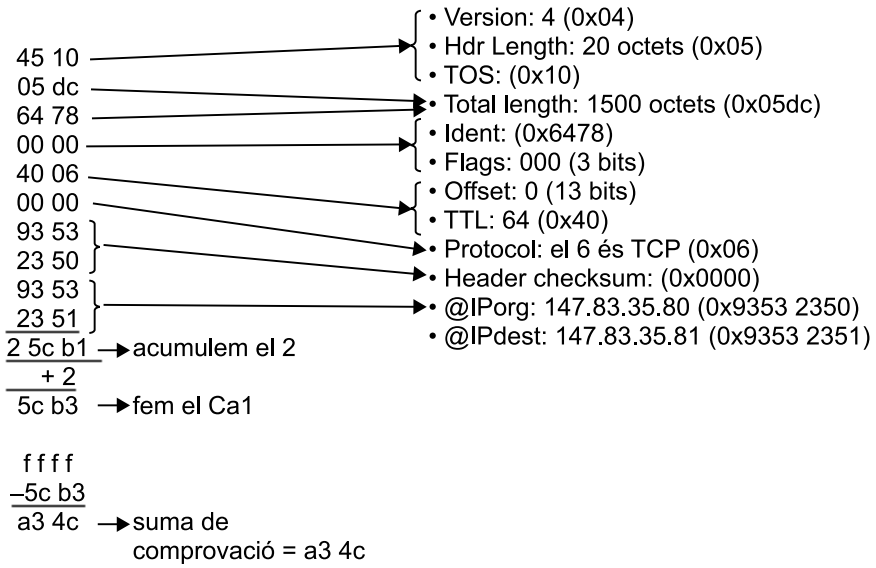
Procés de càlcul de la suma de comprovació

- Els octets de la capçalera del datagrama són alineats com a paraules de 16 bits.
- S'inicialitza la suma de comprovació (resultat de la suma) a 0.
- Se sumen les paraules de la capçalera amb transport.
- S'acumula el transport final juntament amb el resultat de la suma.
- Es calcula el complement a 1 del resultat final (amb el transport acumulat). El complement a 1 consisteix a canviar els 1 pels 0 i viceversa.

En emissió, s'omple el camp de suma de comprovació de la capçalera del datagrama amb el valor obtingut de la suma. El valor de la suma de comprovació s'ha de recalcular cada vegada que es travessa un encaminador (ja que hi ha camps de la capçalera que són mutables, com per exemple el camp TTL).

En recepció, es fa la suma tenint en compte el camp de comprovació de suma generat en l'emissor. Si el resultat de la suma té tots els bits a 1, significa que el datagrama és correcte. Si algun dels bits està a zero, indica que hi ha hagut un error.

Figura 22. Exemple de càlcul de la suma de comprovació



Codis de redundància cíclica

Com hem comentat, els codis detectors amb bit de paritat estan indicats per a transmissions orientades a caràcter. Per a transmissions orientades a bit no són útils, perquè les tires de bits en què es podria aplicar la paritat són molt més llargues i perdrien efectivitat. En lloc del bit de paritat s'utilitzen els denominats *codis CRC*. És una tècnica de detecció d'errors àmpliament utilitzada en les xarxes de computadors actuals.

Els codis CRC són coneguts com a codis polinòmics, ja que possibiliten veure la seqüència de bits enviats com un polinomi, els coeficients del qual són els valors 0 i 1 a la cadena de bits.

Sigui una S una seqüència de P bits s_{K-1}, s_{K-2}, ..., s_0; definim la representació polinòmica S(x) de la seqüència S de la manera següent:

$$S(x) = s_{p-1}x^{p-1} + s_{p-2}x^{p-2} + s_1x + s_0$$

L'objectiu de les potències x^j és distingir el pes del bit s_j dins de la seqüència. Per exemple, la representació polinòmica de la seqüència 1001001 és: $x^6 + x^3 + 1$.

Els codis detectors d'errors polinòmics es basen en el càlcul d'un nombre binari, conegut com a CRC, resultat d'una certa operació matemàtica efectuada amb els bits que s'han de protegir. Aquest nombre es posa en el camp de control d'errors de la trama. En recepció es repeteix el càlcul i s'interpreta que hi ha o no hi ha error, en funció de si coincideix o no amb el CRC rebut.

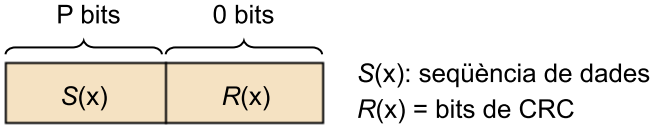
Codificació en emissió

Considerem que la seqüència inicial S és la formada pels P bits de la trama que volem protegir, que anomenarem $S(x)$ en la seva expressió polinòmica. Inicialment l'emissor i el receptor s'han de posar d'acord primer en un patró de $Q + 1$ bits, conegut com a *polinomi generador*, representat com a $G(x)$. Als P bits de la trama original l'emissor afegeix una seqüència de Q bits coneguda com a *CRC de la trama* i representada com a $R(x)$. Aquests bits són obtinguts com el residu de la divisió polinòmica següent en mòdul 2:

$$R(x) = reste\left(\frac{S(x)\cdot x^{Q}}{G(x)}\right)$$

En mòdul 2, la resta és igual que la suma, que alhora és l'operació XOR binària. La trama transmesa estarà formada pels bits P inicials i el CRC de Q bits.

Figura 23



L'expressió polinòmica de la trama transmesa serà:

$$S'(x) = S(x) \times x^{Q} + R(x)$$

Exemple de càlcul del CRC

Suposem que la seqüència de bits que cal protegir és 11001, amb un CRC de tres bits, i que el polinomi generador és $G(x) = x^3 + 1$. Tenim que $S(x) = x^4 + x^3 + 1$, i per tant, $S(x) \cdot x^3 = x^7 + x^6 + x^3$, i la divisió en mòdul 2 de $S(x) \cdot x^Q$ / $G(x)$ és:

$$\begin{array}{l|l} x^7 + x^6 + x^3 & x^3 + 1 \\ \hline x^7 + x^4 & x^4 + x^3 + x \\ \hline x^6 + x^4 + x^3 & \\ x^6 + x^3 & \\ \hline x^4 & \\ x^4 + x & \\ \hline x & \end{array}$$

S'obté que $R(x) = x$, i per tant el CRC que caldria afegir seria 010.

Comprovació en recepció

El patró de bits resultant $P + Q$ (interpretat com un nombre binari) és exactament divisible per G utilitzant aritmètica de mòdul 2 (considerant que les sumes i les restes que es fan són sense ports ni deutes). Això s'utilitzarà en recepció per a comprovar la integritat de les dades.

El receptor només ha de dividir els $P' + Q'$ bits rebuts entre G(x). Si el residu no és zero, el receptor sap que ha ocorregut un error; en el cas contrari s'accepta que és correcte.

Robustesa dels codis detectors CRC

Les propietats del codi CRC depenen del polinomi generador. En general, tanmateix, es pot demostrar que si triem un polinomi generador adequat de grau Q (és a dir, amb un CRC de Q bits):

a) La distància de Hamming del codi és major o igual que 4.

b) La capacitat de detecció de ràfegues d'error és menor o igual que Q (és a dir, que es poden detectar tots els bits d'error consecutius de Q bits o menys).

c) La probabilitat que una combinació arbitrària de bits sigui acceptada com a paraula vàlida val 2^{-Q}. També, cada un dels estàndards de CRC pot detectar qualsevol nombre senar d'errors en bits.

Polinomis generadors estandarditzats

El grau del polinomi generador $G(x)$ no és arbitrari, sinó que és determinat pel nombre de bits que volem que tingui el CRC. El residu de la divisió per a un polinomi de grau P és un polinomi de grau menor o igual que $P - 1$. Si volem que el CRC tingui Q bits, és a dir, que la seva representació polinòmica tingui un grau menor o igual que $Q - 1$, haurem de triar un polinomi generador de grau Q. En altres paraules, el grau del generador ha de ser igual al nombre de bits del CRC.

L'eficàcia del sistema depèn del polinomi generador triat. Hi ha polinomis generadors molt utilitzats que han estat estandarditzats internacionalment, de 8, 12, 16 i 32 bits. Per exemple, s'utilitza un CRC de 8 bits per a protegir la capçalera de 5 octets a les cel·les ATM. A continuació podem veure alguns polinomis generadors CRC estandarditzats:

- $CRC-12 = x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$
- $CRC-16 = x^{16} + x^{15} + x^2 + 1$
- $V41-ITU-T = x^{16} + x^{12} + x^5 + 1$

- $CRC-32 = x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$

L'estàndard de 32 bits, CRC-32, que s'ha adoptat en un cert nombre de protocols IEEE[34] de nivell d'enllaç, utilitza el generador de G(CRC-32) = 100000100110000010001110110110111.

(34) *IEEE* és la sigla d'*Institute of Electrical and Electronic Engineers*.

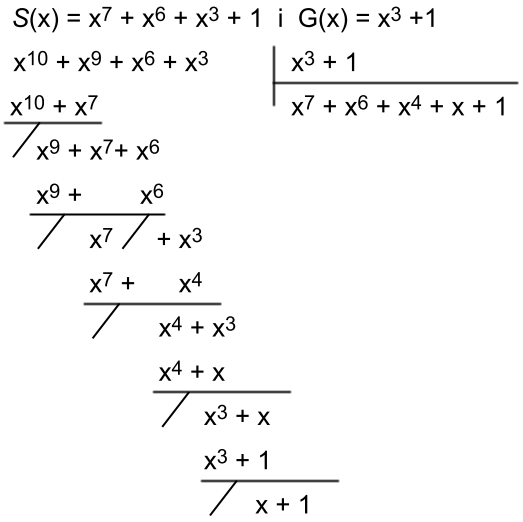
Els codis de 16 bits capturen tots els errors simples i dobles, tots els errors en els quals el nombre de bits afectats és senar, tots els errors en ràfega amb mida de ràfega menor o igual que 16, el 99,997% dels errors de ràfega de 17 bits i el 99,998% dels de 18 bits o majors.

Exemple d'ús de polinomi

Volem transmetre el missatge 11001001 protegint-lo d'errors utilitzant el polinomi CRC: x^3+1.

a) Determineu el missatge que ha de transmetre el node emissor.

Fem la divisió polinòmica següent: $S(x)\cdot x^3$ / $G(x)$, en què:



La divisió $S(x)\cdot x^3$ / $G(x)$ dóna com a quocient $C(x) = x^7 + x^6 + x^4 + x + 1$, i el residu, $R(x) = x + 1$.

Per tant, s'enviarà la seqüència: 11001001 + 011 (s'afegiran 3 bits de CRC).

Podem comprovar que la seqüència $S(x) \cdot x^3 + R(x)$ és divisible entre $G(x)$.

b) Si es rep el missatge 01001001, a causa que s'inverteix el bit més significatiu, quin seria el resultat del càlcul de CRC en recepció? Com se sap en recepció que ha ocorregut un error?

S'ha de fer la divisió del polinomi representat per la cadena de bits rebuda (01001001 + 011 = $x^9 + x^6 + x^3 + x + 1$) entre el polinomi generador. Hauria de sortir un residu 0 per a detectar que tot és correcte. $x^9 + x^6 + x^3 + x + 1 : x^3 + 1$ dóna de residu x, i això vol dir que ha ocorregut un error.

Exercici

7. Per què s'utilitza CRC en el nivell d'enllaç i la suma de comprovació en els nivells de xarxa i transport?

Solució de l'exercici 7

La detecció d'errors en la capa d'enllaç està implementada en el maquinari dedicat dels adaptadors, que poden fer ràpidament les operacions de CRC més complexes.

La capa de xarxa i de transport està implementada en programari en un equip final (*host*) com a part del sistema operatiu de l'equip final. La suma de comprovació és fàcil d'implementar en programari, ja que és un esquema de detecció d'errors simple i ràpid. Tanmateix, proporcionen una protecció relativament feble contra els errors si es compara amb CRC.

4.2. Estratègies de correcció d'errors

Hi ha la possibilitat d'instaurar un tipus de codi amb redundància suficient que, a més de detectar errors, permeti corregir alguns bits erronis en el receptor sense necessitat de sol·licitar una repetició de la transmissió. Aquest tipus de codis es denominen *autocorrectors*, i són eficaços sempre que els errors no es presentin en ràfegues de mida superior a un màxim admissible.

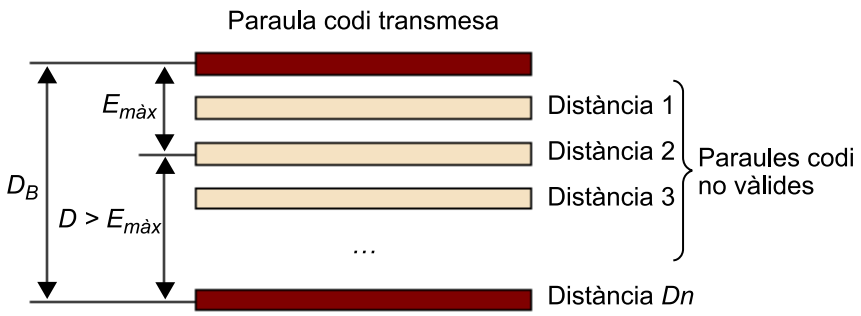
La tècnica d'utilitzar en el receptor un codi corrector d'errors per a detectar i recuperar errors (en lloc de sol·licitar la retransmissió de la trama) es coneix com a *tècnica de correcció d'errors cap endavant* (FEC[35]).

[35] *FEC* és la sigla de *forward error correction*.

Aquesta tècnica s'utilitza habitualment en l'emmagatzemament d'àudio i en dispositius de reproducció com els CD d'àudio. En la inicialització de la xarxa, es poden utilitzar tècniques FEC per si soles o al costat de les tècniques ARQ que hem examinat en el mòdul 3. Les tècniques FEC són valuoses, perquè poden disminuir el nombre de retransmissions de l'emissor requerides. I el que és potser més important, permeten la correcció immediata d'errors en el receptor. Això evita haver d'esperar el retard de propagació d'anada i tornada necessari perquè l'emissor rebi un paquet NAK i per a propagar cap enrere el paquet retransmès cap al receptor (un avantatge potencialment important per a aplicacions de temps real).

Amb la finalitat de fer una anàlisi més formal dels codis correctors s'utilitza el concepte de distància de Hamming, que ja hem introduït. En cas d'error, la correcció consisteix a suposar que la paraula codi transmesa és la paraula codi vàlida més pròxima a la paraula rebuda, segons el concepte de distància (criteri de la distància mínima). Per tant, serà la que tingui menys bits de diferència.

Figura 24. Codi corrector segons el criteri de la distància mínima



La figura 24 és una representació gràfica de la idea que tot just acabem d'exposar. En aquesta figura podem veure una possible paraula codi transmesa, i després trobem agrupades totes les paraules amb el nombre de bits de diferència (és a dir, que disten): 1, 2... fins a les paraules vàlides més pròximes a D_H bits de distància. Si es rep una de les trames que es troba a una distància 1, 2 ..., $E_{màx}$, és a dir, una de les paraules que no tenen cap altra paraula vàlida més pròxima que la transmesa, el codi corregirà l'error.

Per a saber quants bits és capaç de corregir el codi amb probabilitat 1, suposem que, en la figura, D_H és la distància mínima entre dues paraules vàlides (la distància de Hamming del codi).

Sigui $E_{màx}$ el nombre de bits erronis; de la figura deduïm que el criteri de distància mínima corregirà l'error si $E_{màx} < D$, en què $D = D_H - E_{màx}$.

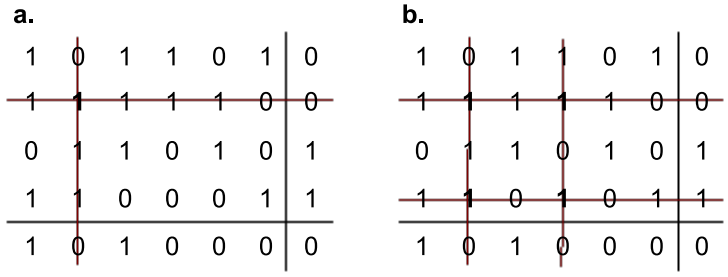
En definitiva, si la distància de Hamming d'un codi és D_H, utilitzant el **criteri de la distància mínima** es pot corregir qualsevol combinació de $E_{màx}$ bits erronis que compleixi:

$$E_{màx} < D_H / 2$$

4.2.1. Correcció d'errors en codis de paritat bidimensional

Hem vist que els codis de paritat bidimensional permeten corregir qualsevol error d'un sol bit buscant la fila i la columna amb la paritat canviada (tal com mostra l'esquema *a* de la figura 25). Tanmateix, si l'error es produeix en dos bits (esquema *b* de la figura) el codi ja no és capaç de corregir l'error.

Figura 25. Correcció de bits amb un codi amb paritat transversal i longitudinal



En aquesta figura els bits erronis estan marcats en negre. Si l'error es produís en els bits marcats en blanc, es tindria el mateix error longitudinal i transversal. Així doncs, el codi de paritat longitudinal i transversal no és capaç d'esbrinar quina de les dues possibilitats s'hauria de corregir.

La distància de Hamming dels codis amb paritat transversal i longitudinal és igual a 4. Per tant, es poden corregir $E_{màx} < 2$, és a dir, 1 bit, tal com havíem deduït anteriorment. Un codi amb $D_H = 5$ pot corregir $E_{màx} < 2{,}5$; és a dir, 2 bits.

4.2.2. Codis de Hamming

Són un tipus de codis de control de paritat en el qual els dígits de paritat s'intercalen en la paraula, de manera que poden identificar els possibles bits erronis. Normalment presenten distància mínima 3 (corregeixen un error) i poden utilitzar la paritat parella o senar. A continuació, s'estudiaran les regles de composició per a paraules de codi Hamming de distància 3 i paritat parella:

- Si la paraula original de dades té m bits es necessitaran h bits de paritat, ja que s'ha de complir que $2^h \geq m + h + 1$.

- Els bits es numeraran d'esquerra a dreta començant per 1.

- En les posicions que són potències de 2 (1, 2, 4, ..., $2P$) s'intercalaran els bits de paritat i es deixarà la resta per a bits de dades.

- Cada bit de paritat parella es calcula a partir d'una sèrie de bits de dades però no a partir de cap altre de paritat.

- Com a norma general, un bit de dades bn és comprovat pels bits de paritat b_i, b_j, ..., b_k, de manera que $n = i + j + ... + k$. Dit d'una altra manera, un bit de dades és comprovat per aquells bits de paritat les posicions dels quals són la descomposició en potències de dues diferents de la posició del bit de dades.

Per exemple:

- b_{18} serà comprovat per b_{16} i b_2, ja que $18 = 16 + 2 = 2^4 + 2^1$
- b_{22} serà comprovat per b_{16}, b_4 i b_2, ja que $22 = 16 + 4 + 2 = 2^4 + 2^2 + 2^1$
- b_{32} és bit de paritat, ja que la seva posició és una potència de 2, $32 = 2^5$

L'emissor envia la paraula codi al receptor (composta de dades i paritat), aquest comprova les equacions de paritat sobre les dades rebudes i, en l'hipotètic cas que un bit hagi sofert un canvi, pot detectar la seva posició restaurant-la al valor inicial.

A continuació, es desenvoluparan les equacions de paritat per a 4 bits de dades i 3 de paritat ($2^3 = 8 = 4 + 3 + 1$); en cada equació apareix un únic bit de paritat juntament amb els bits de dades que controla.

Equacions de paritat per a 4 bits de dades

a) $0 = b_1 \bigoplus b_3 \bigoplus b_6 \bigoplus b_7$

b) $0 = b_2 \bigoplus b_3 \bigoplus b_6 \bigoplus b_7$

c) $0 = b_4 \bigoplus b_5 \bigoplus b_6 \bigoplus b_7$

Per a comprendre el funcionament del mètode s'utilitzarà un exemple.

Exemple

Genereu la paraula codi per a transmetre les dades 1001: cal intercalar els bits de paritat en les posicions 1, 2 i 4 i que resulti $b_1\ b_2\ 1\ b_4\ 0\ 0\ 1$; perquè compleixin les equacions els bits de paritat seran $b_1 = 0$, $b_2 = 0$, $b_4 = 1$ i la paraula completa 0011001.

En el cas de 3 bits de paritat i 4 de dades, la redundància serà:

$$R = (3/7) \times 100 = 42{,}86\%$$

Aquesta és una redundància alta, però que se sol admetre en certs casos en canvi del poder corrector dels codis Hamming.

Suposem ara que l'emissor envia la paraula calculada al receptor i que a aquest li arriba 0011000. Com es pot apreciar, s'ha produït un error en un bit. Ara bé, és possible conèixer on s'ha generat aquest error a partir de la dada rebuda? Per a això el receptor ha de comprovar les equacions amb els valors rebuts:

$0 \oplus 1 \oplus 0 \oplus 0 = 1$: no es compleix a
$0 \oplus 1 \oplus 0 \oplus 0 = 1$: no es compleix b
$1 \oplus 0 \oplus 0 \oplus 0 = 1$: no es compleix c

Llavors l'error estarà en el bit que apareix en a, b i c, és a dir, el 7è.

Com és fàcil comprovar, si es llegeixen els resultats de les equacions en ordre c, b, a i s'interpreta el valor resultant com un nombre codificat en binari, aquest ens indica la posició del bit erroni. En aquest cas de l'exemple: $c = 1$, $b = 1$, $a = 1$, i llavors $cba = 111 = 7_{10}$.

Amb freqüència els codis Hamming s'utilitzen sobre 7 bits de dades (1 caràcter ASCII). Per a això és necessària la utilització de 4 bits de paritat, i les equacions corresponents seran:

a) $0 = b_1 \oplus b_3 \oplus b_5 \oplus b_7 \oplus b_9 \oplus b_{11}$
b) $0 = b_2 \oplus b_3 \oplus b_6 \oplus b_7 \oplus b_{10} \oplus b_{11}$
c) $0 = b_4 \oplus b_5 \oplus b_6 \oplus b_7$
d) $0 = b_8 \oplus b_9 \oplus b_{10} \oplus b_{11}$

Càlcul de la mida dels codis Hamming

Quina és la raó perquè si la paraula original de dades té m bits es necessitin h bits de paritat, de manera que s'hagi de complir que $2^h \geq m + h + 1$?

La resposta és: per a codificar la posició d'1 bit erroni en $n = m + h$ bits de paraula de codi, caldrà que les equacions de control puguin detectar $n + 1$ resultats diferents. La suma d'una unitat correspon al resultat en absència d'error (no s'ha produït error en cap bit).

En codificar-se en base dos, el nombre de bits de paritat (equacions de paritat) necessaris serà el que compleixi que: $2^h = n + 1 = m + h + 1$.

Així doncs, aplicant la definició de logaritme a l'equació anterior es complirà que $h = \log_2(n+l)$ i, ja que els resultats decimals no tenen sentit (no és possible agafar mig bit de paritat), es prendrà sempre l'enter següent per excés. Això es podria representar com:

$$h = \lceil \log_2(n+l) \rceil$$

Els codis Hamming que compleixen la relació $2^h = n+1 = m+h+1$ es denominen *òptims*, en contrast d'aquells altres que utilitzen menys bits de dades dels que podrien usar amb els bits de control disponibles. Així, el codi que utilitza 7 bits de dades i 4 de paritat no és òptim, ja que amb 4 bits de paritat es podrien controlar $2^4 = 16$ resultats, corresponents a 15 bits diferents, és a dir, es podrien utilitzar fins a 15 – 4 = 11 bits de dades.

Exercicis

8. Quina mida mínima ha de tenir una paraula de codi Hamming amb 15 bits de dades capaç de corregir un error?

Solució de l'exercici 8

m = 15; per tant, es va provant fins a trobar el valor més petit de h que fa que $2^h \geq 15 + h + 1$: aquest valor és 5, i llavors $n = 15 + 5 = 20$.

9. És òptim el codi anterior? En cas que no ho sigui, indiqueu què caldria fer per a convertir-lo en òptim?

Solució de l'exercici 9

No és òptim. Perquè fos òptim hauria de complir:

$$2^h = n + 1 = m + h + 1: 2^5 = 32 \neq m + b + 1 = 15 + 5 + 1 = 21$$

Perquè fos òptim s'hauria de verificar que:

$32 = m + 5 + 1$
$M = 32 – 5 – 1 = 26$ bits de dades.

10. Expliqueu la configuració i les equacions de paritat d'un codi òptim amb 4 bits de paritat.

Solució de l'exercici 10

$b = 4$, $2^h = 2^4 = 16 = m + b + 1$

$m = 16 – h – 1 = 16 – 4 – 1 = 11$, és a dir, la configuració ha de ser 11 bits de dades i 4 de paritat, que fan un total de 15 bits. Les equacions de paritat seran:

a) $0 = b_1 \oplus b_3 \oplus b_5 \oplus b_7 \oplus b_9 \oplus b_{11} \oplus b_{13} \oplus b_{15}$
b) $0 = b_2 \oplus b_3 \oplus b_6 \oplus b_7 \oplus b_{10} \oplus b_{11} \oplus b_{13} \oplus b_{15}$
c) $0 = b_4 \oplus b_5 \oplus b_6 \oplus b_7 \oplus b_{12} \oplus b_{13} \oplus b_{14} \oplus b_{15}$
d) $0 = b_8 \oplus b_9 \oplus b_{10} \oplus b_{11} \oplus b_{12} \oplus b_{13} \oplus b_{14} \oplus b_{15}$

11. Quin és el nivell de redundància d'un codi Hamming amb 7 bits de dades i 4 de paritat?

Solució de l'exercici 11

$$\%_{Redund} = \frac{Bits\ de\ control}{Bits\ totals} \times 100 = \frac{4}{11} \times 100 = 36{,}36\%$$

Com veiem, el percentatge de redundància és bastant elevat. Aquest és un dels motius perquè aquests codis s'utilitzin únicament en circuits en què la implantació de sistemes de retramesa representaria un cost temps/canal molt elevat.

4.3. Estratègies de retransmissió de trames

El nivell d'enllaç pot implementar tècniques de retransmissió de trames basades en els protocols ARQ. De fet, aquestes tècniques es poden implementar tant en el nivell d'enllaç (per exemple, els protocols XMODEM, YMODEM i ZMODEM) com en el nivell de transport (protocol TCP).

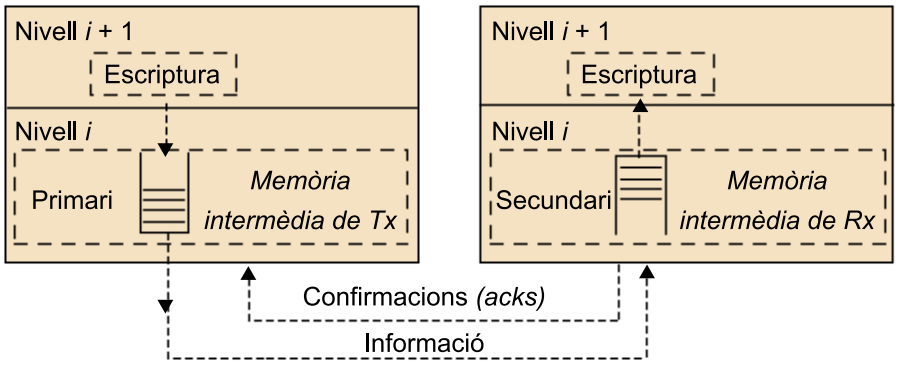
Vegeu també

Vegeu el funcionament dels protocols ARQ en el mòdul "La capa de transport de dades" d'aquesta assignatura.

Hem vist que el principal objectiu de les tècniques ARQ és que la informació transmesa arribi sense errors, sense duplicacions i en el mateix ordre en el qual s'envia. Bàsicament un protocol ARQ retransmet la informació que no arriba, o que arriba amb errors al node receptor. El receptor envia trames de confirmació a l'emissor per a informar-lo que ha rebut correctament les trames d'informació.

4.3.1. Elements d'un protocol ARQ

Figura 26



- Canal bidireccional. Per a un sistema de retransmissions és necessari que la comunicació sigui bidireccional (semidúplex o dúplex).

- Primari: entitat que transmet la informació (emissor).

- Secundari: entitat que rep/consumeix la informació (receptor). Envia els missatges de confirmació[36]. En la pràctica les dues entitats es poden comportar tant com a primari o com a secundari (*piggybacking*).

(36)En anglès, *acks*, abreviatura d'*acknowledgements*.

- Memòria intermèdia de transmissió: on es desa la informació que s'ha d'enviar o que s'ha enviat i que encara no ha estat confirmada pel secundari.

- Memòria intermèdia de recepció: memòria en el secundari en què es desa la informació rebuda fins que la llegeix el nivell superior.

4.3.2. Funcionament bàsic d'un protocol ARQ

- El primari o transmissor envia trames d'informació i les va desant en una memòria intermèdia de transmissió.

- Si la memòria de transmissió s'omple, el primari bloqueja l'escriptura del nivell superior fins que rebi confirmacions de trames d'informació.

- A mesura que arriben confirmacions del secundari, el primari esborra la informació confirmada de la memòria intermèdia de transmissió i deixa espai perquè el nivell superior pugui escriure més informació.

- En cas d'error, el primari pot retransmetre la informació, perquè la té emmagatzemada en la seva memòria intermèdia de transmissió.

4.3.3. Algorismes de retransmissió ARQ

Hi ha 3 tècniques ARQ:

1) Stop & Wait (tècnica *idle RQ,* s'usa en transmissions orientades a caràcter).

2) Go-Back-N

3) Retransmissió selectiva (aquestes dues últimes són tècniques Continuous Rq, i s'usen bàsicament en transmissions orientades a bit).

4.3.4. Eficiència dels protocols ARQ

Els protocols ARQ s'avaluen mitjançant el concepte d'eficiència:

$$E = \frac{V_{ef}}{V_t} = \frac{Duradadetransmissiód'informació}{Tempsdetransmissió} = \frac{T_{Trama}}{T_{Cicle}}$$

En la taula següent podem veure les fórmules d'eficiència dels protocols ARQ en presència i absència d'errors:

Eficiència	Sense errors	Amb errors
Stop & Wait	$\frac{1}{1+2a}$	$\frac{1}{N_t(1+2a)}$
Go-Back-N	100%	$\frac{1}{N_t(1+2a)-2a}$
Retransmissió selectiva	100%	$\frac{1}{N_t}$

N_t és el nombre mitjà de transmissions necessàries per a la transmissió amb èxit d'una trama, i *a* és la relació entre el temps de propagació i el temps de trama:

$$N_t = \frac{1}{(1-P_T)} = \frac{1}{P_{Trama\ sense\ errors}} = \frac{1}{(1-P_{Bit})^L} \qquad a = \frac{T_{Prop}}{T_{Trama}}$$

4.3.5. *Piggybacking*

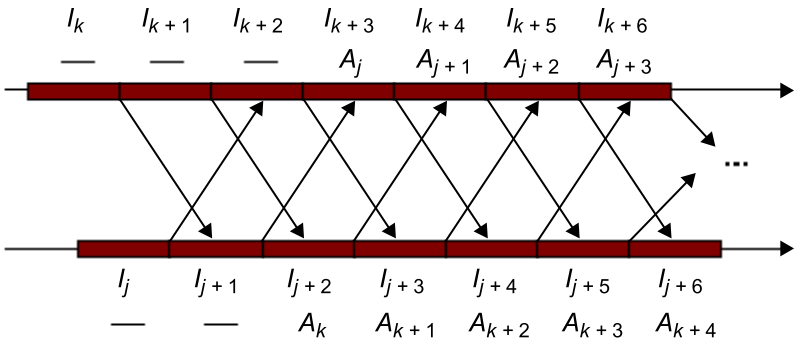
Es tracta d'una tècnica que podem trobar en un protocol de nivell d'enllaç. Fins aquest moment sempre hem considerat que hi havia una estació que transmetia trames d'informació (el primari) i una altra que les confirmava (el secundari). Ara bé, hi ha casos en els quals les dues estacions s'intercanvien trames d'informació recíprocament i, per tant, actuarien com a primari i secundari alhora i haurien d'alternar les trames d'informació amb les confirmacions.

Les trames de confirmació solen tenir una mida petita perquè l'única informació rellevant és la de l'identificador de la trama que confirmen. La major part dels bits d'aquestes trames l'ocupen els camps de control (indicadors de sincronització, CRC, etc.).

Si les dues estacions envien informació, ens interessarà aconseguir que l'eficiència en els dos sentits sigui tan alta com es pugui. Una manera d'augmentar l'eficiència en aquesta situació és incorporar les confirmacions a les trames d'informació (d'aquesta manera ens estalviem la transmissió dels altres camps de control de les confirmacions).

La manera de fer-ho consisteix a destinar un camp de la trama d'informació a l'identificador de la trama que es vol confirmar del primari contrari. Aquesta tècnica es coneix com a ***piggybacking***. La figura 27 mostra el diagrama de temps que s'obtindria utilitzant la tècnica del *piggybacking*.

Figura 27. Confirmació de les trames amb paritat *piggybacking* en un protocol de transmissió contínua



5. Control de flux

L'objectiu del control de flux és l'adaptació de la velocitat de transmissió eficaç entre el transmissor o primari i el receptor o secundari, de manera que sempre hi hagi recursos disponibles i no hi hagi pèrdua d'informació.

Generalment el receptor estableix una zona d'emmagatzemament temporal o memòria intermèdia, en què va acumulant les trames rebudes per l'enllaç, ja que necessita un cert temps per a processar-les (per a comprovar errors, ordenar per número de seqüència, desencapsular trames, enviar al nivell superior, que pot estar ocupat en aquell moment, etc.).

Si no hi hagués procediments per al control de flux, i un node rebés trames a una taxa superior a la que les pot processar, la memòria intermèdia temporal del receptor es desbordaria i es perdrien trames. Un protocol de la capa d'enllaç amb control del flux evita que el node emissor saturi la memòria intermèdia del node receptor i es perdi informació.

A continuació es tracten diferents mecanismes de control de flux implementats en el nivell d'enllaç.

5.1. Mecanisme de control de flux X-ON / X-OFF

S'utilitza en algunes transmissions entre dispositius informàtics (ordinadors, impressores) orientades a caràcter. Bàsicament aquest protocol utilitza dos caràcters per a controlar el flux:

- Caràcter XON, codi 17 ASCII
- Caràcter XOFF, codi 19 ASCII

Quan el receptor del missatge vol que l'emissor detingui el flux de dades, envia un caràcter XOFF (caràcter de pausa) a l'emissor, que li indica que la seva memòria intermèdia no admet més caràcters. Quan el transmissor rep un caràcter XOFF, es bloqueja i queda en espera de rebre el caràcter d'activació XON per a reprendre la transmissió. Aquest caràcter l'envia el receptor quan té suficient espai en la seva memòria intermèdia de recepció.

Aquest mecanisme funciona molt bé quan es tracta de transmetre fitxers de text, ja que els caràcters XON i XOFF no formen part dels caràcters usats normalment en aquest tipus de fitxers.

5.2. Mecanisme de control de flux entre un PC i un mòdem connectat al port sèrie

El port sèrie utilitza el protocol de nivell físic fora de banda RS232. Aquest protocol té dues línies que serveixen per a controlar de flux de dades: RTS[37] i CTS[38].

(37) *RTS* és la sigla de *request to send*.

(38) *CTS* és la sigla de *clear to send*.

Normalment el port sèrie es configura amb una velocitat de transmissió major de la que pot aconseguir el mòdem a través de la línia telefònica. El mòdem té una memòria intermèdia de transmissió en què es desa la informació que transmet a través de la línia telefònica.

Quan el PC té dades preparades per a transmetre el mòdem, activa la línia RTS. Si el mòdem activa la línia CTS, el PC li envia informació a una velocitat major de la que pot enviar el mòdem a la línia telefònica. Per tant, la memòria intermèdia de transmissió del mòdem s'omple. Quan arriba a un cert llindar, el mòdem desactiva la línia CTS, i la tornarà a activar quan la memòria intermèdia es buidi. D'aquesta manera el mòdem sempre té informació llesta per a transmetre a través de la línia telefònica, i podrà aprofitar al màxim la seva velocitat de transmissió.

5.3. Mecanisme de control del protocol ARQ Stop & Wait

És un mecanisme de control de flux inherent al seu funcionament. En l'enviament de cada trama hi ha una adaptació implícita de les velocitats de l'emissor i del receptor, que no es pot sobrepassar, per la manera de treballar del protocol.

El primari no pot enviar cap altra nova trama si no rep la confirmació de l'anterior. Per tant, per a aconseguir disminuir la velocitat de transmissió del primari, el secundari només ha de retardar la tramesa de les confirmacions. Cal recordar que aquest protocol només manté en vol una única trama sense confirmar.

5.4. Mecanisme de control dels protocols ARQ de transmissió contínua

Els protocols de transmissió contínua ARQ no solament s'utilitzen per a la recuperació d'errors, sinó també per al control de flux. Per a això utilitzen el concepte de *finestra lliscant*[39]. Els protocols que utilitzen aquest mecanisme reben el nom de *protocols de finestra*.

(39) En anglès, *sliding window*.

Vegeu també

Vegeu el funcionament dels protocols ARQ en el mòdul "La capa de transport de dades" d'aquesta assignatura.

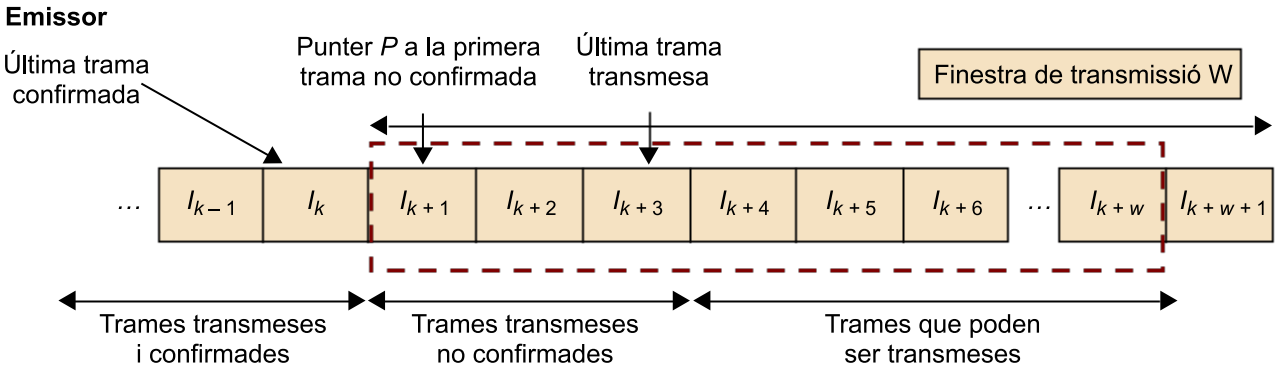
El concepte de finestra lliscant no s'ha de confondre amb el de memòria intermèdia de transmissió (o recepció), encara que s'utilitzi la finestra per a definir la mida d'aquesta memòria intermèdia. El mecanisme de la finestra lliscant es munta sobre la memòria intermèdia de transmissió i es desplaça sobre aquesta a mesura que arriben les confirmacions de les trames.

A continuació refresquem els conceptes de *finestra de transmissió* i *finestra de recepció*.

Finestra de transmissió

La finestra de transmissió marca el nombre de trames que es poden transmetre sense confirmar en el primari. La figura 28 il·lustra el funcionament d'un protocol de finestra de transmissió.

Figura 28. Funcionament d'un protocol de finestra en transmissió



En aquesta figura suposem que les confirmacions són acumulatives, és a dir, queden confirmades totes les trames amb número de seqüència menor o igual que l'última confirmada.

El primari pot enviar fins a W trames d'informació sense confirmar, les quals queden emmagatzemades en la memòria intermèdia de transmissió. El paràmetre W és la mida de la finestra de transmissió. Si I_k és l'última trama confirmada, l'emissor només pot transmetre fins a la trama I_{k+w}.

El primari bàsicament manté un punter P a la primera trama no confirmada. Abans de cada transmissió (sempre que ho permeti el nivell inferior) avalua la diferència següent:

- Si (*Número de seqüència de trama per transmetre – Número de seqüència de trama* P *no confirmada*) < W = TRANSMET.
- Si (*Número de seqüència de trama per transmetre – Número de seqüència de trama* P *no confirmada* ≥ W = ES PARA.

En aquesta situació, per a fer control de flux en un protocol de finestra, n'hi ha prou que el secundari deixi d'enviar confirmacions. En l'exemple anterior, si no arriben més confirmacions després de transmetre la trama I_{k+w}, el primari esgotarà la finestra i es pararà.

Quan arriben confirmacions de noves trames, l'índex P que apunta a la primera trama no confirmada (i per tant, la finestra de trames que es poden transmetre) s'actualitza i avança, i permet la transmissió de noves trames.

Finestra de recepció

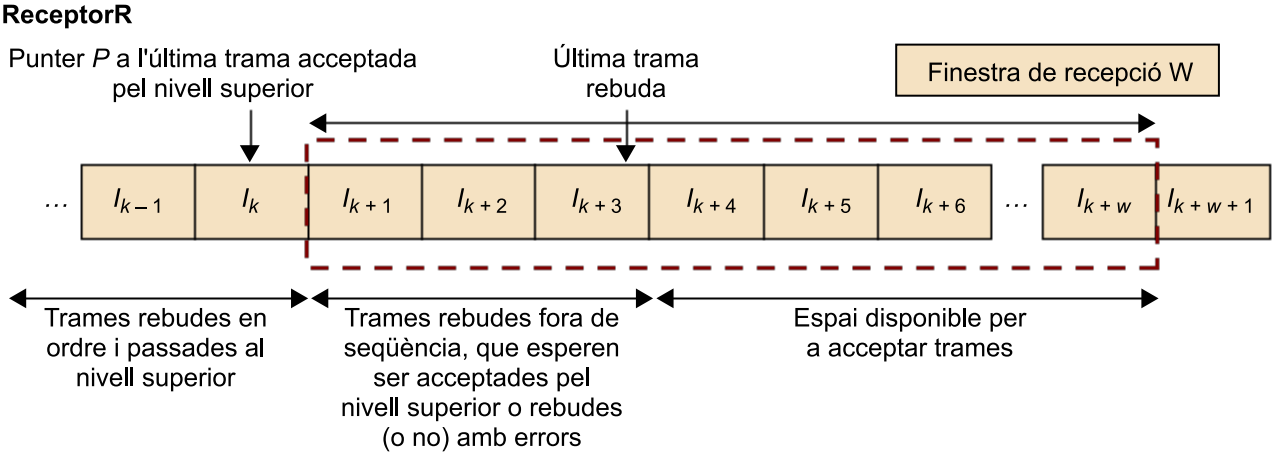
La finestra de transmissió no solament permet dimensionar la mida de la memòria intermèdia de transmissió, sinó també la memòria intermèdia de recepció.

Per analogia amb la finestra de transmissió, la finestra de recepció es defineix com el nombre màxim de trames que ha d'emmagatzemar el secundari. Assumint que el nivell d'enllaç treu de la finestra de recepció totes les trames amb número de seqüència anterior, que han estat rebudes correctament, en ordre i acceptades pel nivell superior, podem trobar els tipus següents de trames a la finestra de recepció:

- Trames rebudes sense errors i en ordre que no poden ser acceptades momentàniament pel nivell superior.
- Trames rebudes sense errors, però fora d'ordre, que s'han de reordenar.
- Trames rebudes amb errors i, per tant, descartades.
- Trames no rebudes perquè s'han perdut.

En la figura 29 podem veure un exemple de finestra de recepció.

Figura 29



La trama I_k i totes les trames anteriors han estat rebudes sense errors i en ordre pel secundari i han estat acceptades pel nivell superior. Per tant el nivell d'enllaç les ha esborrades de la finestra de recepció. Les úniques trames que pot haver de confirmar i ordenar el secundari són les trames que van des de la I_{k+1} fins a la I_{k+w}, les úniques que el primari ha estat autoritzat a transmetre.

Observem que el valor màxim de la finestra de recepció serà W. Aquesta és la mida de la finestra de recepció en un protocol ARQ amb retransmissió selectiva, que coincideix amb la mida de la finestra de la finestra de transmissió. El problema de la reordenació només té sentit en el cas del protocol ARQ de retransmissió selectiva. En els protocols Stop & Wait i Go back N n'hi ha prou que la finestra de recepció sigui igual a 1. En la taula següent podem veure un resum de la mida de les finestres en els tres protocols:

Mida de les finestres de transmissió i recepció		
Protocol	**Finestra de transmissió**	**Finestra de recepció**
Stop & Wait	1	1
Go back N	W	1
Retransmissió selectiva	W	W

5.5. Finestra òptima

Hem vist que, en absència d'errors, l'eficiència dels protocols de transmissió contínua és del 100%, gràcies al fet que el primari no roman mai aturat, i sempre està transmetent i esperant confirmacions. En un protocol de finestra, aquesta condició no es pot donar si la mida de la finestra no és prou gran, ja

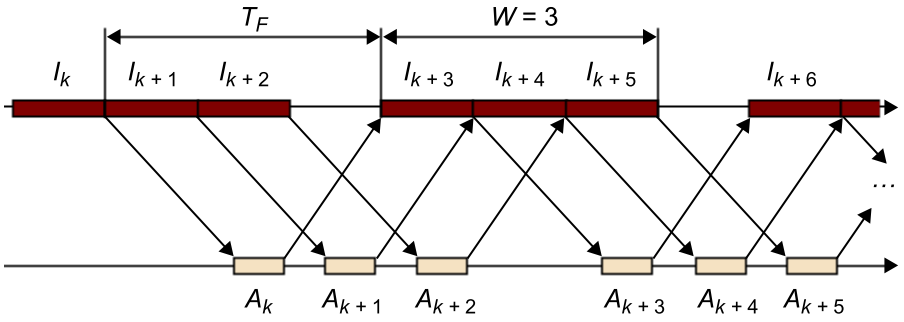
que el transmissor es pot arribar a bloquejar en espera de rebre les confirmacions que alliberin la seva finestra, cosa que es tradueix en una baixada del rendiment o l'eficiència del protocol.

D'altra banda, si la finestra del protocol és molt gran, pot ser un inconvenient, ja que les memòries intermèdies de transmissió i recepció s'han de dimensionar per a poder emmagatzemar un nombre de trames igual que la finestra. A més, no s'experimenta cap millora en el rendiment pel fet que sigui molt gran.

Es defineix la **finestra òptima** (W_{opt}) com la finestra lliscant mínima que permet aconseguir una eficiència del protocol del 100%.

Podem estudiar l'esquema de la figura 30.

Figura 30. Parada del primari en cas de finestra petita



Mostra un exemple en què la finestra de transmissió val $W = 3$; per tant, es poden transmetre tres trames sense confirmar. Com que $T_{cicle} > T_w$, el primari roman un cert temps bloquejat esperant l'arribada de confirmacions que permeti avançar la finestra de transmissió. Si tenim ocupat el primari transmetent un temps igual a T_{cicle}, obtenim la màxima eficiència de la transmissió. És a dir, quan $T_{cicle} < T_w$, el primari no es pararia mai i s'obtindria la màxima eficiència de transmissió al 100% en absència d'errors.

Definim la finestra òptima com:

$$E = \frac{T_w}{T_{Cicle}} = 1 \text{ en què } T_w = W_{Trama}$$

$$T_w = T_{Cicle} = W_{Trama} \rightarrow W = \frac{T_{Trama}}{T_{Cicle}}$$

- Si $W < W_{òptima}$ la velocitat efectiva serà inferior a la que podríem aconseguir amb una finestra més gran.

- Si $W > W_{òptima}$ no augmentarem la velocitat efectiva més enllà de l'aconseguida amb la finestra òptima.

6. Importància del nivell d'enllaç segons el context

Fins ara hem explicat les funcions que podem trobar en el nivell d'enllaç. No obstant això, és important entendre que el nivell d'enllaç no sempre efectua totes les funcions explicades. Depenent del context en què treballi un protocol de nivell d'enllaç, pot fer unes funcions i implementar-ne d'altres.

Per exemple, en Internet (torre TCP/IP), el nivell d'enllaç no du a terme cap funció de recuperació d'errors, simplement descarta les trames errònies. La recuperació d'errors la fan els nivells superiors, normalment el nivell de transport.

Podem trobar el nivell d'enllaç en les diferents situacions:

a) Comunicació punt a punt entre dos computadors locals: per exemple, la comunicació pel port sèrie entre dos PC per a poder fer una transferència de fitxers. A causa del reduït nombre d'elements que intervenen en aquest cas, normalment tota l'arquitectura de comunicacions estarà integrada en el mateix programa. Evidentment, aquí no hi haurà nivell de xarxa i el nivell d'enllaç serà responsable de la recuperació d'errors.

b) Entorn d'accés a WAN[40] (Internet). Actualment, és un dels més habituals. Milions d'usuaris l'utilitzen per a accedir a Internet. En aquest entorn el protocol de nivell d'enllaç s'estableix entre el computador de l'usuari i el computador del proveïdor d'Internet. Aquí l'usuari es connecta al proveïdor mitjançant un mòdem. El proveïdor disposa d'una bateria de mòdems perquè múltiples usuaris es puguin connectar simultàniament.

(40) *WAN* és la sigla de *wide area networks*.

c) Xarxa d'àrea local (LAN[41]). Una característica d'aquests tipus de xarxes és que està formada per una comunitat de computadors que comparteixen un únic medi de transmissió. Són xarxes multipunt o de difusió. En les xarxes d'àrea local podem distingir dues maneres d'organitzar la comunicació entre les computadores sense interferir entre si:

(41) *LAN* és la sigla de *local area networks*.

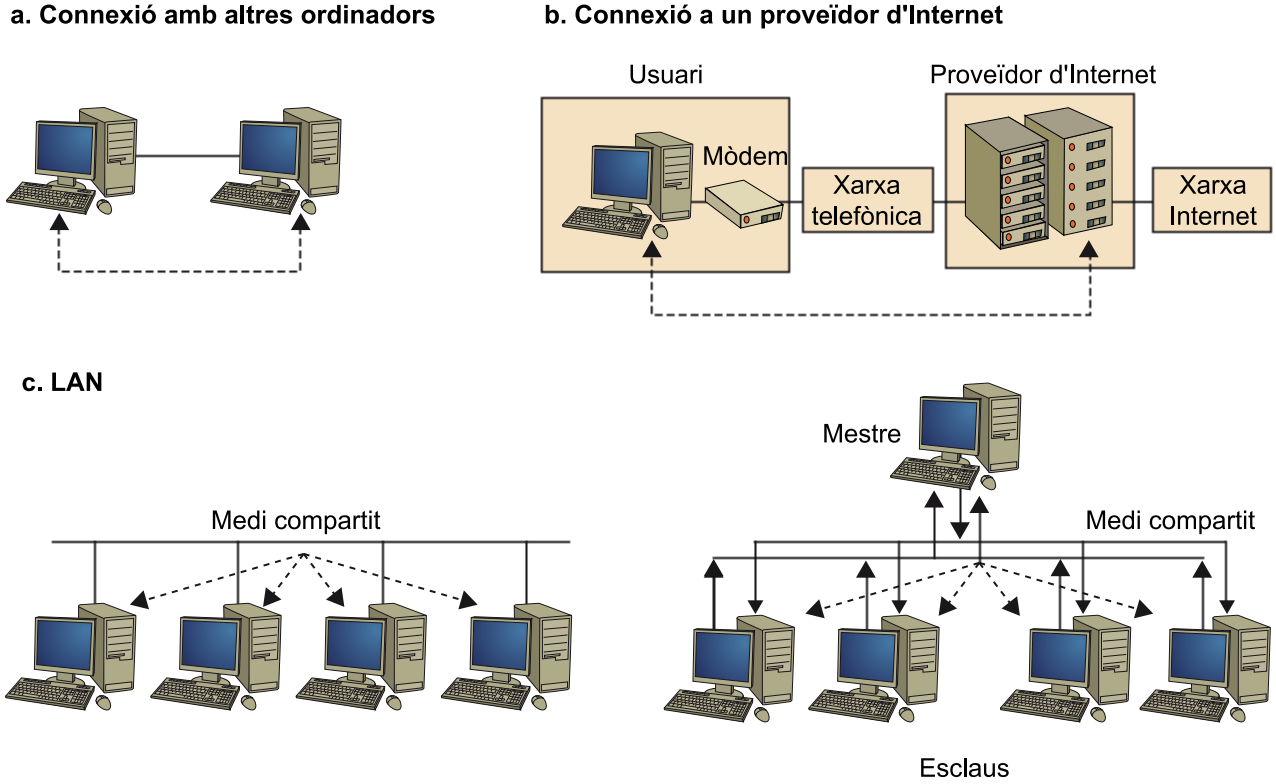
- Un computador **mestre** s'encarrega d'arbitrar totes les comunicacions. Les comunicacions són entre el mestre i un altre dels computadors (els **esclaus**), o viceversa. En aquest entorn podem interpretar que hi ha un enllaç punt a punt entre el mestre i cada un dels esclaus, i que el mestre selecciona alternativament un dels enllaços possibles segons algun algorisme d'arbitratge.

- No hi ha un àrbitre que seleccioni un dels enllaços possibles. L'algorisme d'accés està distribuït entre els computadors que accedeixen al medi.

d) Xarxes troncals d'àrea estesa (WAN[42]). Es corresponen amb el nivell d'enllaç existent a les xarxes troncals dels proveïdors d'accés a Internet o empreses de telecomunicacions. Aquestes tecnologies serveixen per a comunicar computadores separades per distàncies molt grans.

(42) *WAN* és la sigla de *wide area networks*.

Figura 31. Exemples de contextos en els quals es pot trobar el nivell d'enllaç



En aquesta figura, les línies discontínues connecten els dispositius entre els quals s'estableixen el protocol de nivell d'enllaç.

La classificació dels protocols de nivell d'enllaç envers el context d'utilització guiarà l'estructuració dels punts següents del mòdul d'enllaç:

- El nivell d'enllaç entre dos computadors locals: estudiarem protocols utilitzats en la comunicació entre ordinadors locals o un ordinador i un dispositiu d'entrada/sortida a través del port sèrie o el port paral·lel: RS232, BSC.

- El nivell d'enllaç a les xarxes d'àrea local (LAN), en què estudiarem el problema de les xarxes de difusió que s'han fet servir històricament en les xarxes d'àrea local. Centrarem l'estudi en les tecnologies més utilitzades en les xarxes d'àrea local tant en medis cablats (Ethernet) com en medis sense fils (Wi-FI 802.11). Aquí s'establirà la classificació de les tecnologies sense fils segons la seva extensió i s'inclourà l'estudi de WiMAX (802.16).

- El nivell d'enllaç a les xarxes d'acces a WAN. Estudiarem els protocols bàsics de nivell d'enllaç, HDLC i PPP, sobre els quals es fonamenten una bona

part de les tecnologies d'accés a les xarxes d'àrea estesa per mitjà d'un operador de telecomunicacions. Per a complementar aquest apartat veurem les principals tecnologies o sistemes d'accés a WAN que s'han fet servir en els darrers anys fins avui dia: RTC/RTB, RDSI (T1/E1), ADSL i HFC.

- El nivell d'enllaç en les xarxes de transport WAN. Veurem les tecnologies principals emprades per les operadores de telecomunicacions en el nivell d'enllaç en les xarxes de transport WAN: x.25, retransmissió de trama, ATM i MPLS.

7. El nivell d'enllaç en les xarxes d'àrea local

La capa del nivell d'enllaç[43] pot gestionar dos tipus d'enllaços: els enllaços punt a punt[44] i els enllaços de difusió[45].

[43] En anglès, *link layer*.

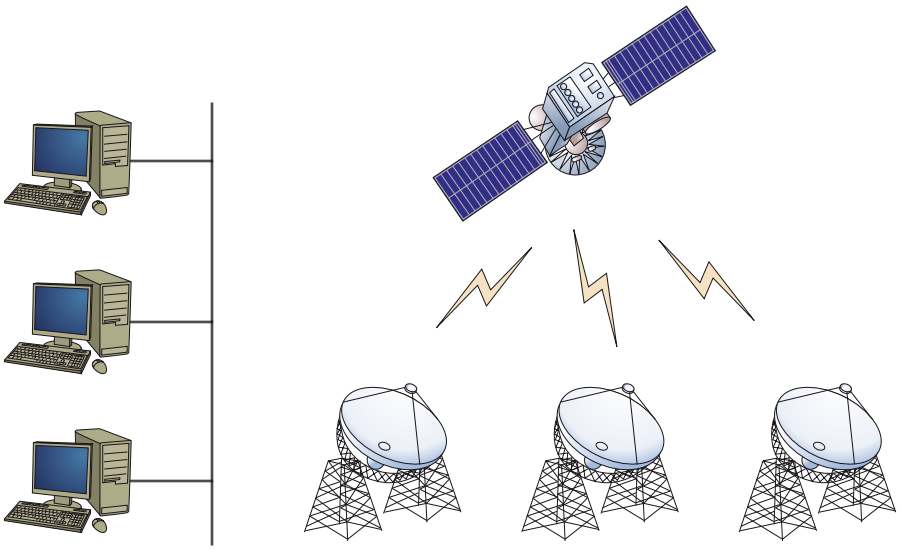
[44] En anglès, *point to point links*.

[45] En anglès, *broadcast links*.

Un enllaç punt a punt consisteix en un sol emissor i un sol receptor connectats per un sol cable. Hi ha determinats protocols de comunicacions que funcionen sobre enllaços punt a punt, com per exemple PPP o HDLC. Coordinar l'accés en aquests tipus d'enllaços és trivial.

En els enllaços per difusió hi ha múltiples nodes (o estacions) emissors i receptors connectats sobre el mateix cable (o canal); comparteixen el canal per a enviar i rebre informació. Es parla del concepte de difusió perquè quan un node transmet una trama d'informació, el canal difon una còpia de la trama a cada estació connectada al cable. La noció de difusió ens pot resultar familiar en el cas de la transmissió de senyals de televisió. La televisió consisteix en un node fix (antena o repetidor) que transmet a tots els nodes (aparells o receptors de televisió). Les xarxes d'àrea local Ethernet o les xarxes Wi-Fi són altres exemples de xarxes locals en què s'apliquen aquests conceptes.

Figura 32



7.1. MAC

Els protocols d'accés múltiple (MAC[46]) són molt més beneficiosos quan les comunicacions punt a punt es tornen ineficients: quan no és possible tenir una línia punt a punt entre cada parell d'estacions de la xarxa, quan la utilització

[46] *MAC* és la sigla de *media access control*.

de les línies punt a punt és molt baixa, per raons econòmiques, etc. També són molt útils en el cas en què hi hagi un nombre elevat de nodes transmetent informació d'una manera descoordinada, per exemple, quan cada estació decideix independentment de les altres el que vol transmetre, a qui ho vol enviar i en quin moment ho vol fer. En resum, la necessitat d'un protocol d'accés múltiple apareix quan hi ha la necessitat de comunicacions entre nodes independents en una xarxa interconnectada.

Les dues característiques importants d'aquests tipus de xarxes són:

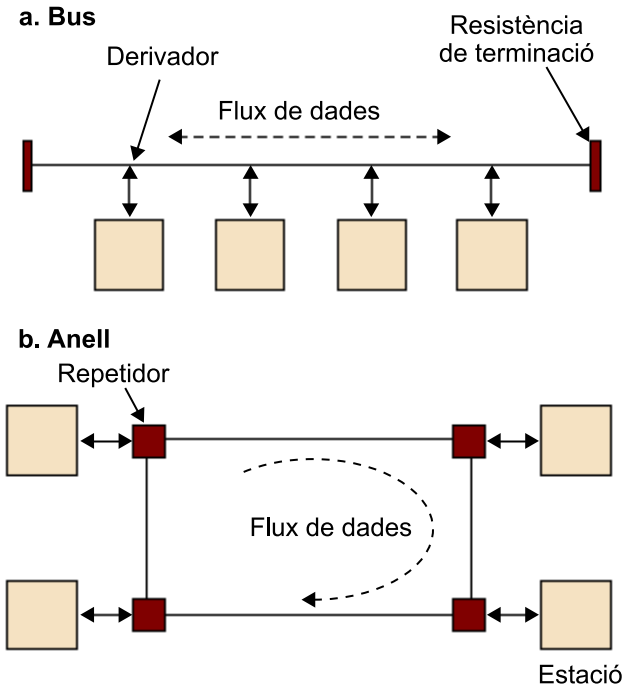
1) La xarxa conté nodes independents que s'intenten comunicar a través d'un únic canal de comunicació compartit. Un node que vol transmetre informació necessita revisar l'estat del canal per si està lliure o no abans de començar la transmissió.

2) En un instant de temps donat, el nombre d'estacions de la xarxa que volen transmetre informació és desconegut i canvia dinàmicament amb el temps.

Definir els protocols d'accés al medi consisteix en una sèrie de regles que cada node o estació de la xarxa ha de seguir per tal de compartir un recurs; en el nostre cas, un canal (o cable, o l'aire...) compartit. L'elecció dels protocols d'accés depèn molt de la naturalesa del tipus de trànsit i del rendiment que demandaran les estacions de la xarxa.

Suposem que tenim un conjunt d'estacions o nodes que estan interconnectats d'alguna manera entre si i que comparteixen el medi o canal de comunicació per a enviar i rebre informació. Una xarxa funciona en mode difusió quan la informació transmesa des d'una estació origen cap a una estació destinació la poden escoltar la resta d'estacions de la xarxa, malgrat que la informació no vagi destinada explícitament a aquestes.

Figura 33. Exemple de xarxa de difusió



Les estacions estan interconnectades en topologia en forma de bus i en forma d'anell.

Una estació estarà en estat actiu si té informació per transmetre. Hi pot haver estacions connectades en una xarxa que no estiguin en estat actiu.

Durant els darrers anys s'han desenvolupat molts protocols d'accés múltiple al medi; els podem classificar de la manera següent:

a) MAC estàtics (TDMA, FDMA, CDMA).

b) MAC dinàmics:

- Accés dinàmic per control centralitzat.
- Accés dinàmic per control distribuït (pas de testimoni)

c) MAC aleatoris (Aloha, Aloha segmentat, CSMA[47], CSMA/CD[48]).

[47] *CSMA* és la sigla de *carrier sense multiple access*.

[48] *CSMA/CD* és la sigla de *CSMA with collision detection*.

El principal avantatge dels protocols estàtics és que cada node té garantit una amplada de banda determinada, i que cada transmissió generalment no interfereix amb la d'un altre. El desavantatge principal és que l'amplada de banda del canal és assignada tant a les estacions o nodes que volen transmetre com als que no volen transmetre, i que l'amplada de banda desaprofitada (inutilitzada) no es pot traspassar d'un node a un altre. En general, els estàtics tenen un rendiment prou acceptable davant altes càrregues de trànsit, i els seus temps de resposta per a iniciar la transmissió solen ser baixos. Els protocols d'accés dinàmics són molt atractius, ja que ofereixen retards de resposta baixos davant un trànsit baix.

7.1.1. TDM

La tècnica de TDM[49] serveix per a repartir l'amplada de banda del canal entre tots els nodes que comparteixen el canal de comunicacions en el domini temporal.

(49) *TDM* és la sigla de *time division multiplexing*.

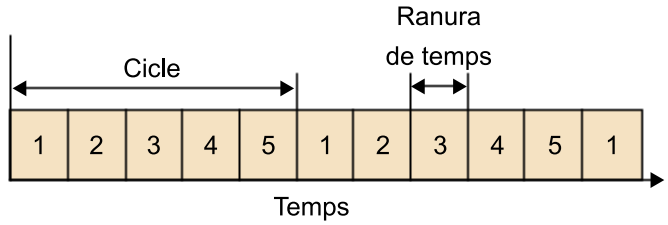
Si tenim un canal que vol suportar la transmissió de N nodes, TDM divideix la línia temporal en N particions temporals[50]. Cada partició temporal és assignada a un sol dels N nodes perquè durant aquesta partició el node pugui transmetre informació. Generalment la durada de la partició temporal es tria de tal manera que una trama sencera es pugui transmetre durant la durada de la partició. Per tant, cada estació o node té dret a transmetre durant un període fix de temps. Aquest dret passa de node en node correlativament, fins que tots els nodes han tingut el dret a transmetre. Una vegada s'arriba al darrer node, aquest cicle torna a començar de nou, i dóna de nou el dret de transmissió al primer node.

(50) En anglès, *time slots*.

Si tenim un canal compartit amb una amplada de banda de R bps, amb N nodes, un node disposa de mitjana d'una amplada de banda dedicada només per a ell de R/N bps.

Aquest sistema té dos inconvenients: el primer, que si dels N nodes només n'hi ha $M < N$ que volen transmetre informació, l'amplada de banda total del canal R no s'aprofita totalment, ja que cada node només aprofita una amplada de banda de R/N, i en conjunt només s'aprofita una amplada de banda de $R \cdot M/N < R$. El segon inconvenient és que quan un node vol transmetre dues trames seguides, després d'haver transmès la primera, ha d'esperar tot un torn complet perquè pugui tornar a transmetre el segon paquet.

Figura 34. Exemple d'un accés al canal en TDM



7.1.2. FDM

La tècnica FDM[51] divideix l'amplada de banda del canal entre diferents freqüències i assigna una amplada de banda (en freqüència) a cada un dels nodes.

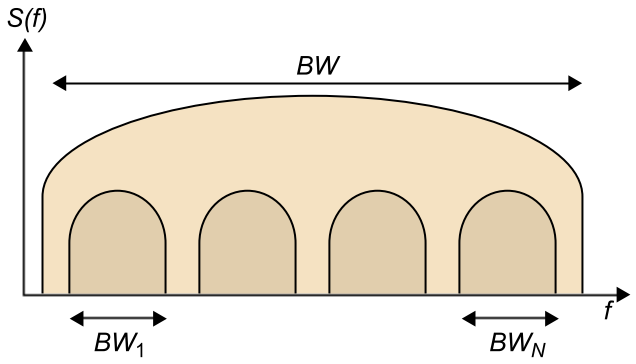
(51) *FDM* és la sigla de *frequency division multiplexing*.

FDM crea *N* petits subcanals, cada un a una freqüència diferent dels altres, amb la particularitat que tots els nodes poden transmetre a la vegada, però a diferent freqüència. Amb aquest sistema l'amplada de banda del canal *R* es divideix entre cadascun dels *N* nodes i dóna una amplada de banda de *R*/*N* per node.

Aquest sistema, per exemple, és utilitzat en la retransmissió de la TV convencional. Diferents cadenes de televisió transmeten els seus programes per ones de ràdio i de televisió per l'aire, totes al mateix temps, però cada cadena de televisió per un canal diferent (a una freqüència diferent), de tal manera que les emissions no se superposen en l'espai freqüencial. El receptor (en el nostre cas, l'aparell de televisió) per mitjà d'un filtre (selector del canal) decideix quines freqüències vol acceptar (i per tant, rebutjar les ones d'altres canals) per a veure un determinat canal de televisió.

Com a principal inconvenient, aquest sistema redueix l'amplada de banda d'un node a *R*/*N* bps malgrat que sigui l'únic node de la xarxa que vulgui transmetre informació.

Figura 35. Exemple de divisió de la freqüència del canal *BW* en subcanals BW_i



7.1.3. CDMA

CDMA[52] s'ha utilitzat en aplicacions militars, i actualment, en canals d'accés múltiple sense fils.

(52)*CDMA* és la sigla de *code division multiple access*.

CDMA permet que diversos nodes transmetin simultàniament. Aquest sistema assigna un codi d'unes característiques especials a cada node. Cada node utilitza el seu únic codi per a codificar els bits que transmet, i els respectius nodes receptors de la informació saben el codi de l'emissor.

Si no es produeixen interferències per diverses transmissions simultànies de diferents emissors, el receptor, a partir d'unes operacions matemàtiques i del codi de l'emissor, és capaç de recuperar el missatge original transmès. En canvi, quan diversos emissors transmeten a la vegada, el receptor rep un senyal

format per la suma de les diferents emissions, i per mitjà d'un procés de codificació/descodificació matemàtica amb el codi d'un emissor, detecta que la informació és incorrecta.

Per analogia real, CDMA seria com si tinguéssim un grup de persones que parlen en diverses llengües diferents: els humans som capaços de captar molt bé els missatges en la llengua que entenem, i no tenim en compte els missatges en les llengües que desconeixem.

7.1.4. Protocols d'accés dinàmics

Les dues característiques ideals que cal que tingui un protocol d'accés múltiple són les següents:

1) Quan només hi ha un sol node actiu, és a dir, que vol transmetre informació, l'amplada de banda del canal *R* ha d'estar disponible per a aquest node.

2) Quan hi ha *N* nodes que utilitzen el canal, l'amplada de banda disponible (o rendiment[53]) per a cada node ha de ser el més aproximat possible a *R*/*N*. Aquesta condició no la compleixen els protocols aleatoris o de contenció, que s'expliquen en un altre apartat.

[53] En anglès, *throughput*.

Vegeu també

Vegeu aquesta condició en l'apartat 8 d'aquest mòdul didàctic.

Per aquest motiu, els investigadors desenvoluparen una nova classe de protocols anomenats *protocols d'accés per rotació circular*[54]. El més important d'aquesta classe de protocols és el control centralitzat[55]: requereix que un dels nodes sigui el que s'anomena el *màster* (o central), i que sigui el controlador del canal. El node màster autoritza[56] el primer node per a transmetre diverses trames enviant-li un missatge. Una vegada aquest node ha acabat de transmetre, el node màster comunica al segon node l'autorització per a transmetre. I el procés es va repetint de manera cíclica[57]. El node màster, a més a més, controla quan un node ha acabat de transmetre les seves trames observant l'estat del senyal del canal. Aquest sistema elimina les particions buides, i augmenta l'eficiència global del sistema. El principal inconvenient és que introdueix el temps que es triga a comunicar a un node la indicació que pot començar a transmetre la informació (*delay polling*). El segon inconvenient és que si el node màster falla, la xarxa es torna inoperativa.

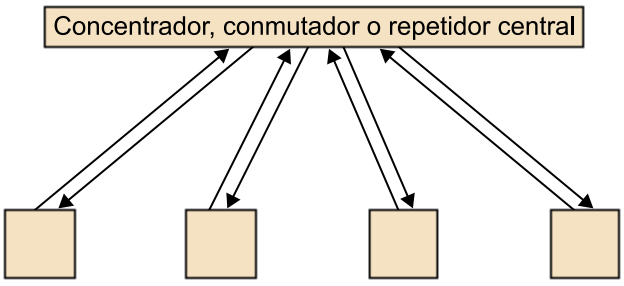
[54] En anglès, *taking turns protocols*.

[55] En anglès, *polling control*.

[56] En anglès, *poll*.

[57] En anglès, *round-robin*.

Figura 36. *Polling* amb topologia en estrella

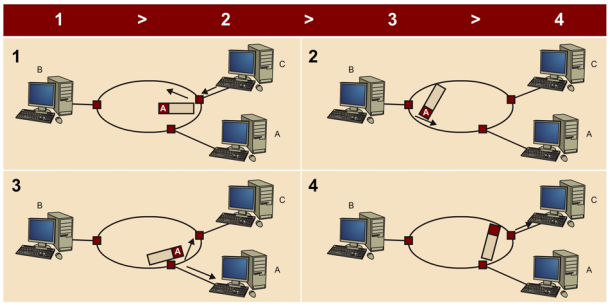


Uns altres protocols d'aquests tipus són els protocols basats en el control distribuït[58]. En aquest cas no hi ha cap node màster que reguli l'accés al canal. L'accés es basa en una petita trama, anomenada *testimoni*[59], de propòsit especial, que circula pels nodes disposats en una topologia en anell. El node 1 transmet el testimoni al node 2, el node 2 al node 3..., i finalment el node *N* al node 1, i es torna a començar el cicle rotatori. Quan una estació ha rebut el testimoni té el dret a transmetre una trama d'informació, que també circula per l'anell (d'estació en estació) fins que l'estació destinatària la captura. Si una estació rep el testimoni i no vol transmetre cap trama d'informació, envia el testimoni cap a l'estació següent. El pas del testimoni es fa d'una manera descentralitzada i augmenta molt el rendiment de la xarxa. L'inconvenient principal és que si un node falla pot fallar tot l'anell que formen els nodes.

(58)En anglès, *token passing protocol*.

(59)En anglès, *token*.

Figura 37. Control distribuït pel pas del testimoni



1. C transmet una trama cap a A.
2. La trama no va dirigida cap a B. L'estació B la ignora.
3. L'estació A recull la trama i la retransmet cap a C.
4. L'estació C absorbeix la trama.

7.1.5. Protocols d'accés aleatori o de contenció

Les tècniques de contenció (o aleatòries) ofereixen un accés fàcil al canal de la xarxa quan la càrrega global sobre la xarxa és baixa. En general s'utilitzen en les xarxes de difusió que comparteixen un mateix canal amb un gran nombre variable de nodes amb trànsit a ràfegues[60].

(60)En anglès, *bursty*.

Això significa que moltes estacions no tenen informació per transmetre la gran part del temps, i en un instant de temps, només una petita part d'aquestes estacions volen enviar informació, i ho fan a ràfegues.

En els protocols de contenció és possible tenir diverses transmissions superposades en el temps per diverses estacions. Una superposició en la transmissió d'una trama produeix una col·lisió, i provoca la destrucció de totes les trames involucrades en aquell moment. Si només transmet un sol node, la trama és rebuda pel destinatari sense cap problema. És important distingir la diferència entre un error de transmissió (errors provocats pel renou del canal) i una col·lisió de trames (provocada per la superposició de dues trames sobre el mateix canal de comunicació).

En els protocols d'accés aleatori quan un node transmet ho fa a la velocitat que li permet l'amplada de banda del canal *R*. Quan es produeix una col·lisió, els nodes involucrats en la col·lisió retransmeten les trames fins a aconseguir transmetre la trama sense col·lisió. Després de detectar una col·lisió, el node espera un temps aleatori per a tornar a intentar la retransmissió de la trama, i cada node involucrat en aquesta col·lisió tria un temps aleatori diferent i independent de l'altre node, i això provoca que la probabilitat que es torni a produir una col·lisió sigui més baixa.

Les col·lisions i les conseqüents retransmissions són el preu que s'ha de pagar per la descoordinació entre estacions i per l'accés aleatori sobre el mateix canal. Les col·lisions limiten la quantitat d'informació que es pot transmetre sobre el canal, proporcionen un ordre aleatori per a iniciar la transmissió, i introdueixen un retard variable[61] entre els paquets. El gran desavantatge que tenen és que grans fluctuacions estadístiques de les característiques del trànsit poden provocar que el canal tingui un rendiment pràcticament zero, ja que el canal s'inunda de col·lisions contínuament.

(61)En anglès, *delay jitter*.

Es defineix el temps de propagació d'un senyal (t_p) com el temps màxim que el senyal es propaga entre qualsevol parell de transmissors i receptors de la xarxa. En general, el període de detecció de la col·lisió es calcula aproximadament com el temps de propagació del senyal. Aquest valor afecta el rendiment dels protocols.

Es defineix el temps de vulnerabilitat (T_v) o finestra de col·lisions com el temps en què una trama és susceptible d'experimentar col·lisions.

Aloha pur

El primer protocol de la família Aloha, de l'any 1970, és un protocol descentralitzat anomenat *Aloha pur*: quan arriba una trama del nivell d'enllaç, el node immediatament la transmet sobre el canal. Si la trama transmesa experimenta un col·lisió amb una o més trames transmeses per altres nodes, el node, després d'acabar de transmetre la seva trama col·lidida, immediatament retransmetrà la trama amb probabilitat *p*. Si no, el node esperarà un temps, que és la durada de la transmissió d'una trama completa. Després d'aquesta espera, transmetrà la trama amb probabilitat *p* o esperarà un altre temps de transmissió de trama completa amb probabilitat 1 – *p*.

Exemple d'Ahola pur

Suposem que l'estació *A* transmet una trama en l'instant t_0. La transmissió d'una trama té una durada t_{Trama}. L'estació A no sap si alguna estació ha transmès una trama abans de t_0 o la transmetrà després de t_0. Això significa que si en l'interval $[t_0 - t_{Trama}, t_0]$ hi ha alguna estació que ha començat a transmetre una trama, o bé si alguna estació comença a transmetre una trama en l'interval $[t_0, t_0 + t_{Trama}]$, es produirà una col·lisió. Per tant, el temps de vulnerabilitat valdrà:

$$T_V = (t_0 + t_{Trama}) - (t_0 - t_{Trama}) = 2t_{Trama})$$

Per a calcular la durada d'una col·lisió, si una estació *A* transmet una trama en l'instant t_0:

- Si una estació *B* transmet la trama en l'instant t_0, la durada de la col·lisió serà $t_{col} = t_{Trama}$.
- Si l'estació *B* transmet en l'interval $[t_0 - t_{Trama}, t_0]$ o $[t_0, t_0 + t_{Trama}]$ la durada de la col·lisió serà:

$$t_{Trama} \leq t_{col}\ 2t_{Trama}$$

Per a analitzar el rendiment d'un protocol Aloha pur definim les variables següents:

- *S*: rendiment del canal; és el nombre mitjà de transmissions amb èxit per temps de transmissió de trama t_{Trama}.
- *G*: càrrega oferta; és el nombre mitjà d'intents de transmissions per temps de transmissió de trama t_{Trama}.
- *E*: nombre mitjà de retransmissions.
- P_0: probabilitat que durant el temps de vulnerabilitat $T_v = 2 \cdot t_{Trama}$ cap estació no generi cap trama per transmetre, i per tant, no es generin col·lisions.

Per a modelitzar matemàticament el comportament, considerem un conjunt d'infinits nodes, en què cada un genera trames de longitud fixa segons un procés de Poisson. Suposem que el procés d'arribades de noves trames i de trames retransmeses segueix un procés de Poisson. Això ens dóna que:

$$P_0 = e^{-\frac{G \cdot 2 \cdot T_{Trama}}{T_{Trama}}} = e^{-2G}$$
$$S = G \cdot P_0 = G \cdot e^{-2G}$$
$$\frac{dS}{dG} = e^{-2G} - 2 \cdot G \cdot e^{-2G}$$
$$\frac{dS}{dG} = 0 \Rightarrow G = 0{,}5$$
$$S_{\max} = \frac{1}{2e} = 0{,}184$$

Aloha segmentat

Cada trama té una longitud fixa de *L* bits. El temps és divideix en segments o *slots* de L/*R* segons (una partició té una durada igual al temps per a transmetre una trama), en què *R* és la velocitat de transmissió. En aquest cas el sistema passa de ser continu (Aloha) a discret.

Els nodes només poden transmetre les trames a l'inici de cada partició. Els nodes estan sincronitzats de tal manera que saben en quin instant de temps comença una partició. Quan dues o més trames col·lideixen en una partició, tots els nodes detecten la col·lisió abans que la partició temporal acabi.

D'una partició temporal en què només hi ha un sol node que transmet se'n diu que es tracta d'una partició satisfactòria: no es produeix col·lisió i la transmissió és satisfactòria.

Per a calcular el temps de col·lisió, en aquest cas dues estacions només poden transmetre al principi dels segments, de manera que:

$$t_{col} = t_{Trama}$$

Per a calcular el temps de vulnerabilitat, només es poden produir col·lisions en el temps del segment, de manera que la vulnerabilitat valdrà:

$$t_v = t_{Trama}$$

Així doncs, les equacions del rendiment d'Aloha segmentat, ja que $t_v = t_{Trama}$, són:

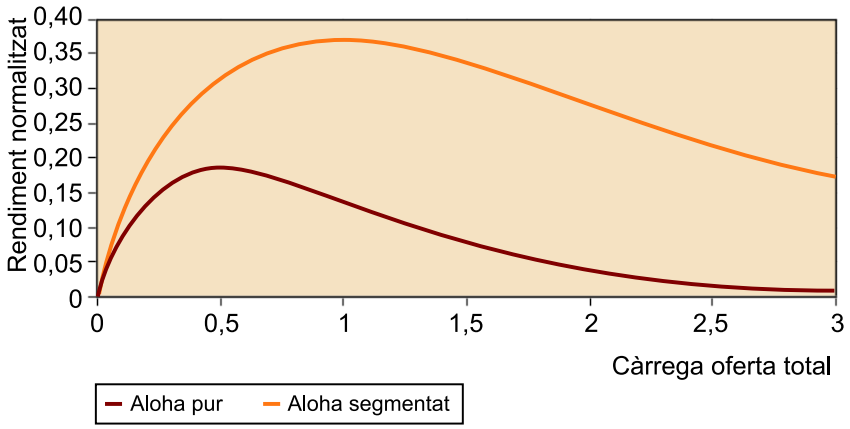
$$P_0 = e^{-\frac{G \cdot T_{Trama}}{T_{Trama}}} = e^{-G}$$
$$S = G \cdot P_0 = G \cdot e^{-G}$$
$$\frac{dS}{dG} = e^{-G} - \cdot G \cdot e^{-G}$$
$$\frac{dS}{dG} = 0 \Rightarrow G = 1$$
$$S_{\max} = \frac{1}{e} = 0{,}368$$

Comparació del rendiment entre Aloha pur i Aloha segmentat

La figura 38 ens mostra el rendiment de tots dos protocols. El rendiment d'Aloha segmentat és màxim quan la càrrega oferta (les trames noves més les trames retransmeses) és 1 (per exemple, una trama per temps de transmissió d'una trama). Com que el rendiment màxim d'Aloha segmentat és 1/*e*, això significa que, de mitjana, cada trama s'ha de transmetre *e* (2,718) vegades o aproximadament 3 vegades. Menys del 40% de les trames per temps de transmissió d'una trama es poden transmetre correctament en canals Aloha.

El rendiment màxim a què es pot arribar en un canal Aloha pur s'ha vist que ha de ser menor que $1/2e$, menor que en Aloha segmentat. Aloha segmentat té l'avantatge de tenir més eficiència en el rendiment, amb l'inconvenient de la necessitat de sincronització (per a saber l'inici de cada ranura) i de l'increment del sobrecost (relació entre el nombre de bits d'informació d'una trama i el nombre de bits total d'una trama) de les capçaleres quan les trames de mida gran són segmentades en trames més curtes per a fer-les cabre en la durada de les particions.

Figura 38. Rendiment per a Aloha pur i segmentat



Respecte al nombre mitjà de retransmissions, la ràtio G/S mesura el retard mitjà que transcorre, ja que representa el nombre de transmissions abans que una trama sigui transmesa amb èxit. Per a Aloha segmentat, la probabilitat de tenir $K-1$ intents seguits d'un intent amb èxit de transmissió d'una trama és:

$$P_K = e^{-G}(1-e^{-G})^{K-1}$$

I el nombre mitjà de transmissions és:

$$Q = \sum_{K=1}^{\infty} K \cdot P_K = \sum_{K=1}^{\infty} K \cdot e^{-G}(1-e^{-G})^{K-1} = e^{G}$$

$$S = \frac{G}{e^{G}} = \frac{\ln Q}{Q}$$

Finalment, el nombre mitjà de retransmissions és:

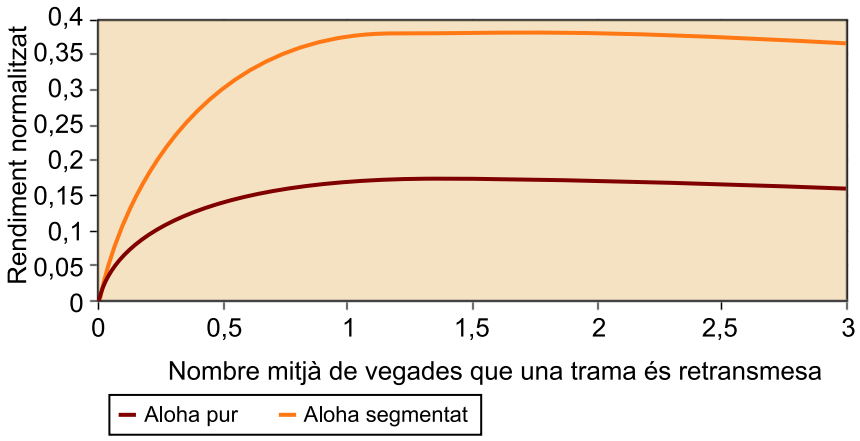
$$E = Q - 1 = e^{G-1}$$

Per a Aloha pur, tenim que:

$$E = e^{2 \cdot G-1}$$

A partir d'aquestes equacions es pot deduir la figura 39, que ens mostra el nombre de retransmissions en funció del rendiment del canal (S):

Figura 39. Nombre de retransmissions per a Aloha pur i segmentat



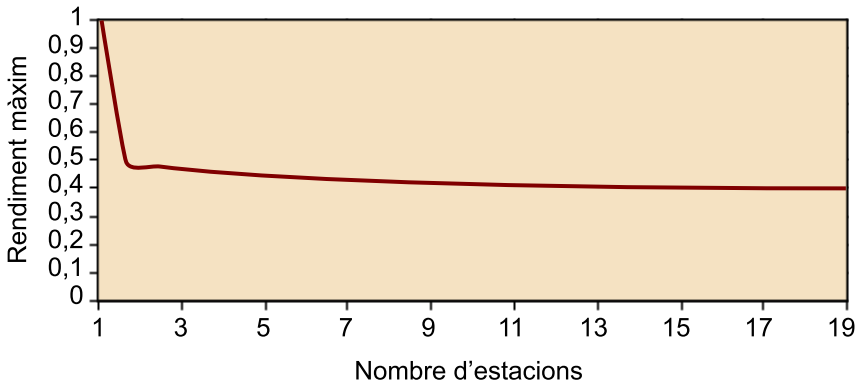
Rendiment d'Aloha segmentat en funció del nombre d'estacions

Ara suposem que tenim N nodes en una xarxa Aloha segmentat. Cada node transmet una trama amb una probabilitat p, i decideix no transmetre amb probabilitat $1 - p$:

$$S = \binom{N}{1} \cdot p \cdot (1-p)^{N-1} = N \cdot p \cdot (1-p)^{N-1}$$
$$\frac{dS}{dp} = N \cdot (1-p)^{N-1} - N \cdot (N-1) \Rightarrow p \cdot (1-p)^{N-2}$$
$$\frac{dS}{dp} = 0 \Rightarrow p = \frac{1}{N}$$
$$S_{max} = \left(1 - \frac{1}{N}\right)^{N-1} \rightarrow \frac{1}{e} \text{ quan } N \rightarrow \infty$$

La figura 40 ens mostra el rendiment màxim en funció del nombre d'usuaris o nodes reals. Per a un nombre de nodes baix, la probabilitat del succés és alta. Quan el nombre de nodes s'incrementa, el rendiment degenera assimptòticament a $1/e$, tal com havíem calculat en el model anterior.

Figura 40. Transmissió simètrica en Aloha pur

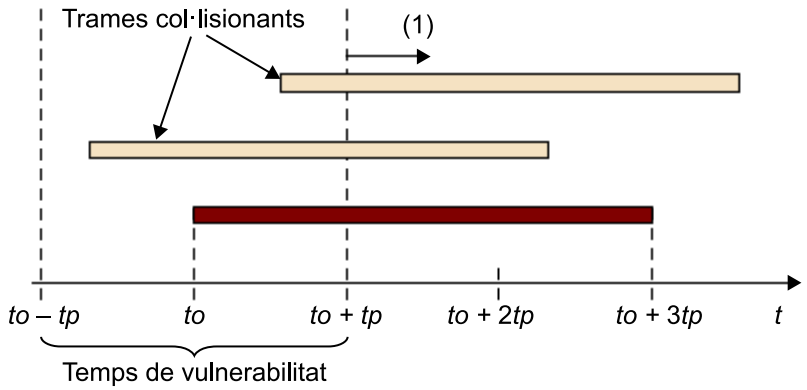


CSMA

En canals amb un temps de propagació baix en comparació del temps de transmissió d'una trama, les col·lisions es poden reduir significativament exigint que cada node actiu escolti el canal per si hi ha alguna trama transmetent-se pel canal abans d'iniciar la seva pròpia transmissió ("escoltar abans de parlar"). En aquest cas, quan una estació o node està transmetent un paquet, totes les altres estacions de la xarxa aturen la seva transmissió durant el temps en què es transmet la trama. En definitiva, durant la transmissió d'una trama, les altres estacions estan en silenci.

En CSMA el temps de vulnerabilitat es tria com el temps màxim de propagació $T_v = 2 \cdot t_p$, en què t_p = distància del bus / V_p. El temps es divideix en ranures de temps molt petites (de durada t_p), i és com si utilitzéssim Aloha segmentat amb particions molt curtes, amb la reducció del nombre de col·lisions.

Figura 41



En CSMA tenim diverses estratègies de funcionament:

- No persistent. L'estació activa escolta el canal i opera de la manera següent: 1) si l'estació detecta que el canal està lliure, la trama és transmesa immediatament, i 2) si l'estació detecta que el canal està ocupat, l'estació espera un temps aleatori abans de tornar a intentar testejar l'estat del canal.

- P-persistent. Només és utilitzat en els canals segmentats. En aquest cas l'estació opera de la manera següent: 1) si l'estació detecta que el canal està lliure, l'estació transmet amb probabilitat p (o difereix a la partició següent de temps amb probabilitat $1 - p$), i 2) si l'estació detecta que el canal està ocupat, l'estació continua escoltant fins que el canal es detecta lliure, i llavors, transmet la trama amb probabilitat p (o difereix a la partició següent de temps amb probabilitat $1 - p$).

Un cas especial del cas p-persistent és el cas 1-persistent, que permet transmetre una trama immediatament quan es detecta que el canal està lliure. El cas p-persistent està pensant per a utilitzar-lo quan tenim un canal en què totes les estacions sempre tenen trames per transmetre, i el canal difícilment està en un estat lliure, per tal d'obtenir un rendiment elevat.

És possible que una estació detecti que el canal està lliure quan una altra estació justament hagi iniciat la transmissió de la seva trama, i això provoqui després una col·lisió.

Per a calcular el temps de col·lisió s'assumeix que l'estació *A* transmet una trama en l'instant t_0.

- Si l'estació *B* transmet la seva trama en l'instant t_o la durada de la col·lisió és $t_{col} = t_{Trama}$

- Si l'estació *B* transmet en l'instant $[t_0 - t_p, t_0]$ o $[t_0, t_0 + t_p]$:

$$t_{Trama} \leq t_{col} \leq + t_{Trama} \approx 2t_p$$

Per a calcular el rendiment del CSMA, suposem que t_p és el temps de propagació màxim del canal, T_{Trama} és el temps de transmissió del paquet, i definim $a = t_p/T_{Trama}$. El rendiment màxim del canal CSMA es pot obtenir en funció de l'amplada de banda d'Aloha segmentat S_{SA}:

$$S_{CSMA} = \frac{S_{SA}}{2a + S_{SA}(1+a)}$$

Per a entorns oberts (per exemple, xarxes sense fils, típicament a = 0,001 fins a 0,1), quan el canal està lleugerament carregat, el retard perquè una estació pugui accedir i transmetre al canal és relativament curt. Aquest retard és independent del nombre d'estacions. En particular, quan només hi ha una sola estació, aquest retard és zero. El rendiment del canal amb CSMA decau quan la càrrega introduïda en la xarxa creix, com en tots els algorismes de contenció.

Per resumir, la taula següent ens mostra el temps del vulnerabilitat i el temps de durada d'una col·lisió amb els tres algorismes esmentats:

	Temps de vulnerabilitat	**Durada d'una col·lisió**
Aloha pur	$2 \cdot t_{Trama}$	$t_{Trama} \leq t_{col} \leq 2 \cdot t_{Trama}$
Aloha segmentat	t_{Trama}	t_{Trama}
CSMA	$2 \cdot t_{prop}$	$t_{Trama} + t_{prop}$

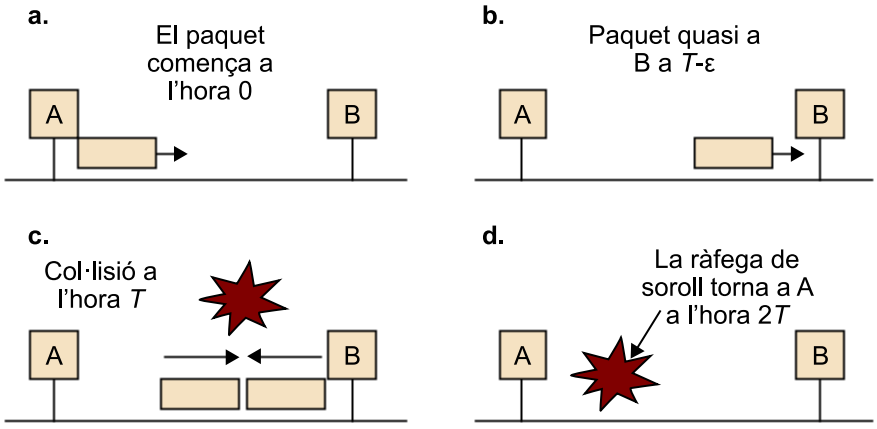
CSMA/CD

El rendiment de l'escolta de la portadora (escolta de l'estat del canal) pot ser millorat i permetre que les estacions involucrades en una col·lisió puguin avortar la seva transmissió una vegada hagin detectat la col·lisió, sense haver de finalitzar tota la transmissió de la trama. Les trames que han sofert una col·lisió són retransmeses després d'un retard aleatori i en cada col·lisió que afecti el mateix paquet es va duplicant el retard de la retransmissió. La raó d'això és que els períodes de col·lisió es fan més curts i les col·lisions no continuaran durant tota la transmissió de la trama. Els mecanismes típics per a detectar la col·lisió consisteixen a comparar el senyal emès i el senyal rebut pel canal.

Aquest mecanisme de funcionament ("si hi ha algú més que també parla al mateix temps, deixa de parlar") s'anomena *detecció de la col·lisió*[62]. (CD).

[62] En anglès, *colision detection*.

Figura 42. Temps màxim de detecció d'una col·lisió (t = temps de propagació)



7.1.6. Adreçament en el nivell MAC

Tal com s'ha explicat, les estacions en una xarxa d'àrea local envien trames a altres estacions sobre un canal compartit. Això significa que quan un node envia una trama, tots els altres nodes de la xarxa reben aquesta trama. Però concretament, un node de la LAN no vol transmetre la trama a totes les altres estacions, sinó que només la vol transmetre a una estació concreta. Per a

proveir aquesta funcionalitat, cada node o estació de la xarxa ha de disposar d'una adreça pròpia que li permeti adreçar una trama a una estació concreta. Per això, dins la trama que es transmet hi sol haver un camp que conté l'adreça a qui va destinada aquesta trama. D'aquesta manera, quan un node o estació rep una trama, pot determinar si aquesta va dirigida a ell o no.

Si l'adreça destinació de la trama coincideix amb l'adreça pròpia de l'estació, l'estació extreu el datagrama de nivell de xarxa de la trama del nivell d'enllaç, i passa el datagrama al nivell superior de la pila de protocols. Si l'adreça destinació no coincideix amb l'adreça de l'estació que l'escolta, l'estació descarta aquesta trama.

Adreçament en una LAN

Cada adreça de nivell LAN també s'anomena *adreça física*, *adreça MAC* o *adreça Ethernet* si s'utilitza la tecnologia Ethernet. Per a Ethernet (i per a altres tecnologies) les adreces estan constituïdes per 6 octets, que proporcionen 2^{48} possibles adreces diferents.

Habitualment les adreces s'expressen en format hexadecimal, separades pel símbol "-", com per exemple, 1A-23-F9-CD-06-9B. Els adaptadors de xarxa LAN porten dins d'una memòria ROM la seva adreça de fàbrica, i aquesta és permanent. Dos adaptadors de xarxa mai no tenen la mateixa adreça LAN. L'organisme IEEE gestiona l'espai d'adreces físiques de tot el món. L'IEEE fixa o determina els primers 24 bits de l'adreça per a cada fabricant, i dóna permís al fabricant dels adaptadors a crear una combinació única per als darrers 24 bits de l'adreça.

Les adreces LAN no tenen una estructura jeràrquica, ja que aquesta és fixada pel fabricant en el moment de la fabricació, al contrari de les adreces IP en Internet. Per exemple, quan un ordinador es desplaça o canvia d'una xarxa IP a una altra, cal canviar-ne l'adreça IP (i també la màscara i la passarel·la[63]), malgrat que l'adreça física sigui la mateixa.

(63) En anglès, *gateway*.

Els adaptadors LAN interpreten una adreça especial anomenada *adreça de difusió*[64]. Per a Ethernet és la FF-FF-FF-FF-FF-FF (48 bits amb 1 consecutius). Serveix per a enviar una trama de nivell LAN a totes les estacions, i es posa en el camp d'adreça destinació aquesta adreça de difusió. A diferència d'una adreça que no és de difusió, en què diverses estacions la poden rebre però no la processen si no va destinada a una estació en concret, amb una adreça de difusió enviem la trama perquè totes les estacions que la rebin la processin.

(64) En anglès, *broadcast address*.

Per a associar les adreces IP amb les adreces de nivell LAN, hi ha un protocol anomenat *ARP*[65] que manté dins una taula ARP les dades següents: adreça IP, adreça física, TTL[66]. El camp TTL serveix per a indicar si una entrada de la

(65) *ARP* és la sigla d'*address resolution protocol*.

taula s'ha d'esborrar o no, si ha expirat o no temporalment la seva validesa (habitualment és cada 20 min). Per això, quan una estació vol associar una adreça IP amb una adreça física desconeguda, envia una trama de nivell LAN de difusió (a totes les estacions de la xarxa local amb adreça FF-FF-FF-FF-FF-FF) en un paquet especial anomenat *paquet ARP*, emmarcat dins una trama MAC, que conté l'adreça IP per la qual es pregunta. L'estació que realment té assignada l'adreça IP preguntada respon al paquet ARP, i envia a l'estació que ha demanat la seva adreça MAC física una trama estàndard (no de difusió). Finalment l'estació que l'ha demanada pot actualitzar la seva taula ARP.

(66) *TTL* és la sigla de *time to live*.

7.2. Ethernet

Pels anys setanta, Bob Metcalfe va dissenyar un protocol per a connectar els ordinadors de l'empresa Xerox. Aquest protocol estava basat en el protocol Aloha, i li va posar el nom d'*Ethernet*.

Pels anys vuitanta, un grup format per les empreses Digital, Intel i Xerox, conegut com a DIX, va ser el primer a implementar Ethernet DIX, i es va crear i implementar la primera especificació de LAN Ethernet. A mitjan anys vuitanta, l'institut IEEE va utilitzar la base d'Ethernet DIX per a publicar l'especificació 802.3 Ethernet.

Entre els anys vuitanta i noranta hi havia en el mercat comercial dos tipus de xarxes d'àrea local: les basades en el protocol Ethernet (estandarditzades en IEEE 802.3) i les basades en protocols d'accés de torn rotatori (anell de testimoni IEEE 802.5 i FDDI).

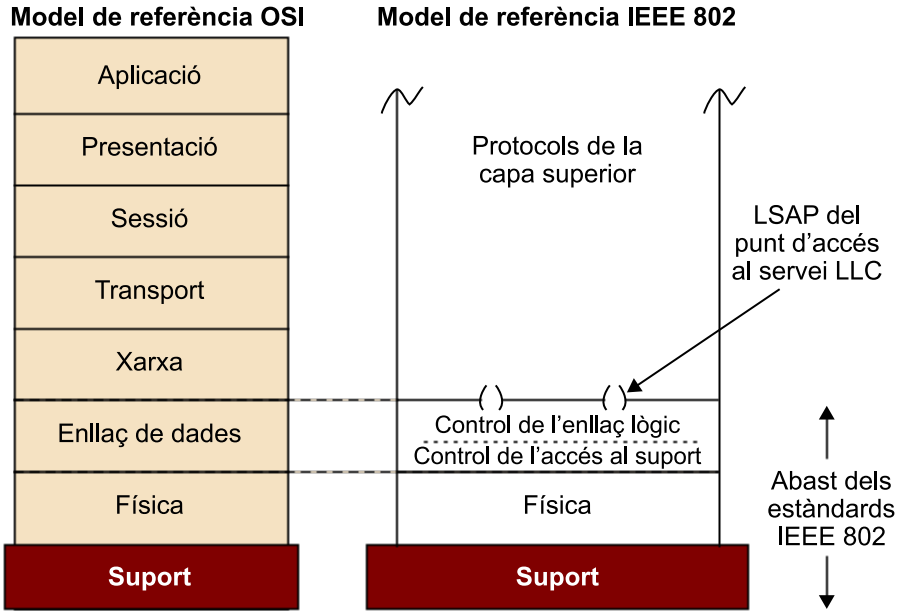
A poc a poc, malgrat que les prestacions de rendiment no eren òptimes, l'estàndard Ethernet va anant guanyant terreny als protocols basats en testimoni, i es van desenvolupar noves tecnologies basades en l'estàndard bàsic, que incrementaven la velocitat de transmissió i s'adaptaven a nous tipus de cablatge.

Actualment, Ethernet s'ha convertit en l'estàndard *de facto* de les xarxes d'àrea local i és la tecnologia LAN d'ús més freqüent actualment.

Quan es dissenya una LAN del comitè IEEE 802 s'han de definir els nivells més baixos del model OSI[67]. Hi ha dues subcapes, el nivell físic i el nivell d'enllaç, que se subdivideix en dos nivells: LLC i MAC. IEEE va definir el model de referència següent:

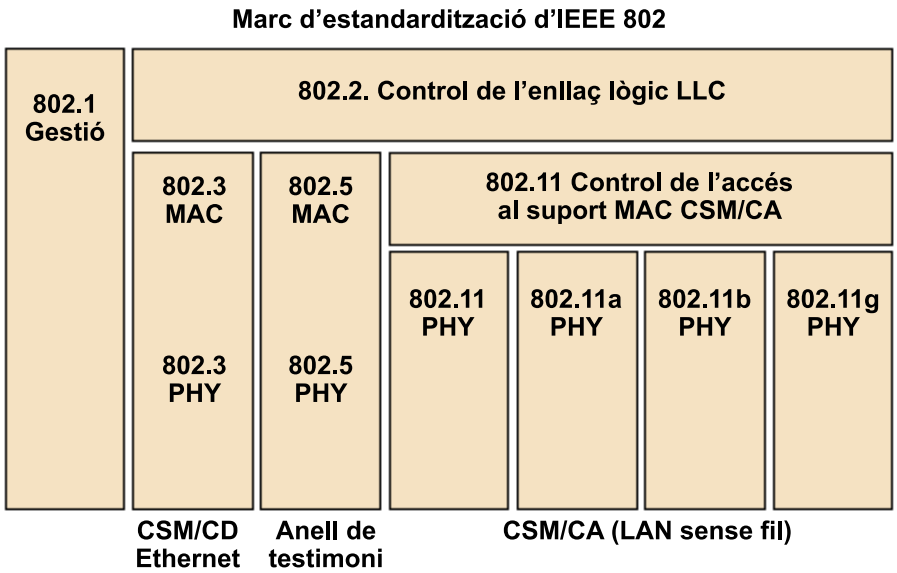
(67) *OSI* és la sigla d'*open systems interconnection*. En català, interconnexió de sistemes oberts.

Figura 43



El subnivell LLC (IEEE 802.2), basat en el protocol HDLC, es va definir com una interfície comuna amb els nivells superiors per a tots els seus estàndards de LAN (802.3 Ethernet, 802.4 Token-Bus, 802.5 Token-Ring, 802.11 Wi-Fi, etc.), i ocultava la complexitat dels diferents sistemes d'accés al medi i del format de les trames.

Figura 44. Esquema d'estandardització IEEE 802.2

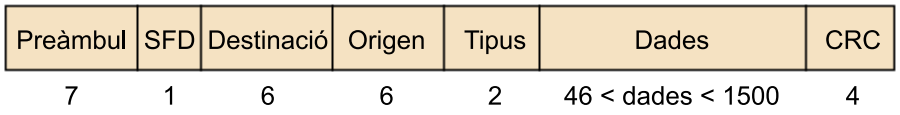


7.2.1. Format de les trames Ethernet

En la pràctica hi ha dues versions de trama Ethernet: el format Ethernet II o DIX i el format IEEE 802.3. Els dos formats són compatibles i es poden utilitzar simultàniament.

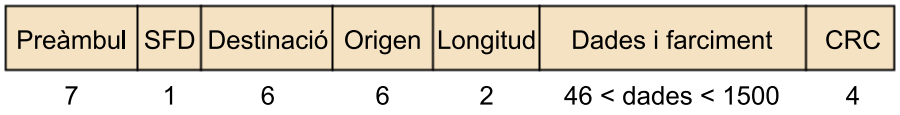
Inicialment el format Ethernet DIX va ser desenvolupat pel consorci Digital, Intel i Xerox (DIX) amb la particularitat que no utilitza la capa LLC.

Figura 45. Ethernet DIX versió II



Un temps més tard l'IEEE va publicar l'estàndard 802.3, amb el mateix protocol d'accés CSMA/CD, però amb un petit canvi en el format de les trames, per fer-lo coherent amb l'estàndard IEEE 802.2 (LLC) en l'RFC 1042.

Figura 46. IEEE 802.3



Format de la trama IEEE 802.3

La descripció dels camps és la següent:

- Preàmbul: serveix per a sincronitzar les targetes en la recepció de la trama. 7 octets de 0s i d'1s alternats.

- SFD[68]: responsable que les estacions receptores sincronitzin els seus rellotges amb el missatge entrant, amb la finalitat que no es produeixin errors en llegir-lo.

- **Adreces destinació i font**: identifiquen l'estació transmissora i receptora. Cada NIC té un número d'identificació de 6 octets, que és únic i està en el maquinari de la targeta. L'organisme d'estandardització IEEE subministra blocs d'adreces a les empreses que fabriquen targetes per a garantir que siguin úniques.

- **Tipus** (utilitzat en Ethernet DIX): indica el tipus de protocol de nivell superior (IP, ARP, etc.) que està ocupant el format de paquet Ethernet DIX versió II. Quan una trama arriba a un ordinador, es necessita saber el seu tipus per a identificar el mòdul del programari que s'ha d'utilitzar per a processar-la. Els valors assignats per l'IEEE en el RFC1700 que tenen valors superiors a 0x05DC (1.500 decimal) són:

[68] *SFD* és la sigla de *start frame delimiter*.

Ether type	Protocol
0800	Datagrama IP
0806	ARP Request/Reply
8053	RARP

Ether type	Protocol
8137	Netware IPX

- **Length** (Ethernet IEEE 802.3): defineix la longitud del camp de dades. No es tenen en compte els octets addicionals. Té els valors extrems de (46 ≤ *payload* ≤ 1.500 octets).

- **Payload**: camp d'informació. Pot tenir entre 46 i 1500 octets. Aquest camp ha de tenir una mida mínima per a poder detectar les col·lisions. Si el nombre d'octets d'informació és inferior a 46, Ethernet li afegeix octets addicionals fins a completar-ne 46. Hi ha d'haver un mecanisme que permeti descobrir els octets que s'han afegit. Per exemple, en el cas de portar un datagrama IP, es pot deduir a partir del camp *header length* de la capçalera IP. La mida de la trama mínima és: 6 + 6 + 2 + 46 + 4 = 64 octets (sense preàmbul). La mida de la trama màxima és: 6 + 6 + 2 + 1500 + 4 = 1.518 octets (sense preàmbul).

- **Condicions d'error**: *jabber* és quan la longitud de trama > 1.518 octets (trama llarga[69]); *runt* és quan la longitud de trama < 64 octets (trama curta[70]), i es produeix un error, malgrat el CRC sigui correcte. Són freqüents en una xarxa Ethernet a causa de les col·lisions. No obstant això, les trames que col·lideixen tindran el CRC incorrecte i es descartaran.

- CRC: serveix per a la detecció d'errors. El remitent fa un control CRC (*cyclical redundancy*) per a efectuar una revisió d'integritat.

[69] En anglès, *long frame.*

[70] En anglès, *short frame.*

L'única diferència entre la trama Ethernet DIX i la IEEE 802.3 és la substitució del camp *Type* pel camp *Length*. El camp *Length* no té en compte els octets addicionals per a arribar als 46, i per tant, no és necessari un mecanisme addicional per a poder descobrir els octets que ha afegit el MAC per a arribar a la trama mínima.

Els dos formats de trama es diferencien pel següent:

- *Type* (trames DIX) < 1.500 (0x05DC) (oficialment, però en la pràctica comença des de 0x0600 o 1536).

- *Length* (trames 802.3) > 1.514 màxim.

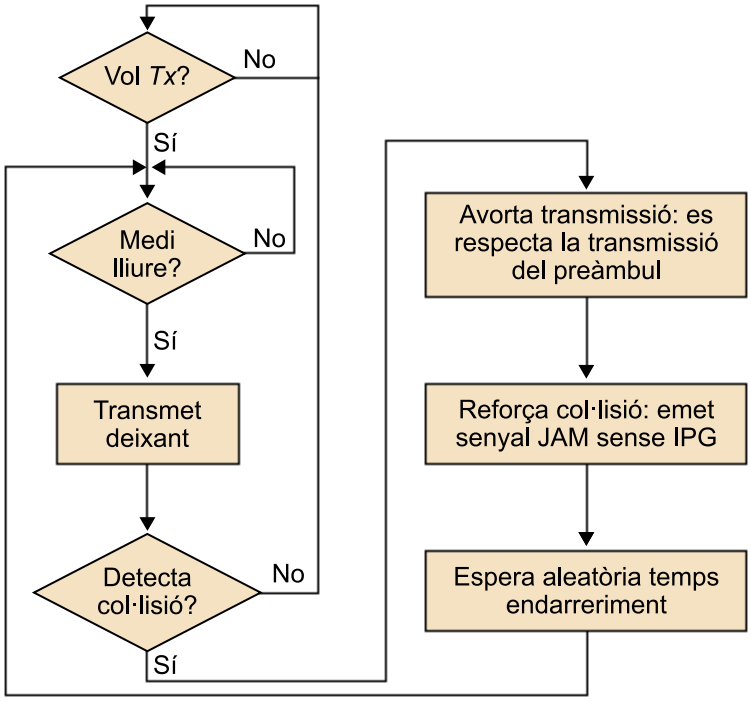
- Permet que les versions d'Ethernet no es confonguin i puguin ser utilitzades al mateix temps en la mateixa xarxa LAN.

7.2.2. Funcionament del protocol: CSMA/CD

El protocol utilitzat en Ethernet és el CSMA/CD, una variant del CSMA.

CSMA és més eficient que Aloha pur i Aloha segmentat, però quan les dues trames col·lideixen, el canal es torna inutilitzable mentre duri la transmissió de les trames que col·lideixen. Si la mida de les trames és elevada en comparació del temps de propagació, es desaprofita una gran quantitat de temps. CSMA/CD intenta reduir el temps de transmissió de les col·lisions.

Figura 47



CSMA/CD es comporta com CSMA 1-persistent. Abans de transmetre escolta el medi, i si està lliure, transmet la trama immediatament (amb probabilitat 1 si el canal està lliure).

Si el canal està ocupat, continua escoltant fins que quedi lliure, i llavors transmet la trama immediatament.

CSMA/CD abans de transmetre ha de deixar un temps, entre trama i trama, major o igual que l'IGP[71]. Té un valor de 96 bits. Serveix per a donar temps a les estacions a detectar si el medi està lliure i detectar el final de la recepció de la trama:

(71) *IGP* és la sigla d'*inter packet gap*.

- Temps d'espera entre trames consecutives enviades per una mateixa estació.

- Temps d'espera des de l'últim bit rebut.

Mentre es transmet la trama, l'estació contínua escoltant el canal. Si no es detecta col·lisió durant la transmissió de la trama, aleshores s'assumeix que no hi ha col·lisió. Per tant, no cal que l'estació receptora enviï una confirmació.

Si es detecta una col·lisió durant la transmissió:

- Es deixa de transmetre immediatament.

- Es transmet un petit senyal d'interferència anomenat *JAM* de 32 bits. Serveix perquè cap estació no pugui detectar una trama que ha col·lidit amb una trama correcta. D'aquesta manera totes les targetes Ethernet descarten la trama.

- Després de transmetre el senyal d'interferència JAM s'espera un temps aleatori anomenat *Back-Off*, i s'intenta transmetre de nou la trama.

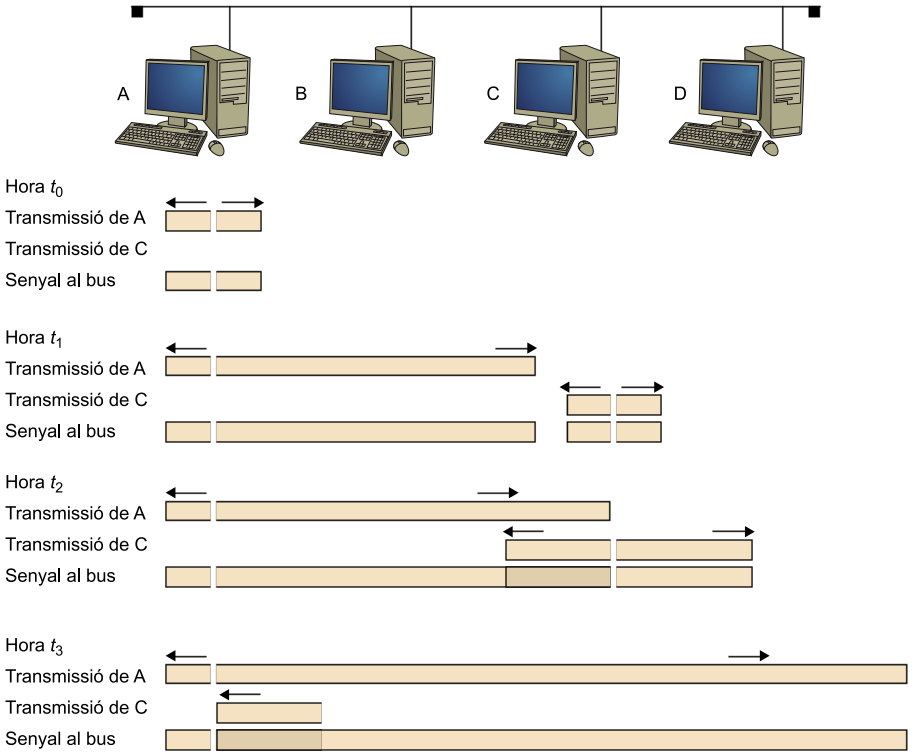
L'algorisme de Back-Off genera un nombre aleatori de mitjana que es multiplica per 2 cada vegada que es retransmet la mateixa trama. D'aquesta manera s'intenta eliminar el problema de la inestabilitat que hi pot haver en els MAC aleatoris:

$$T_{backoff} = n \cdot T_t(512)$$

en què $T_t(512)$ és el temps de transmissió de 512 bits (per exemple: 51,2 μs a 10 Mbps). Rep el nom de *temps de ranura*. n és un nombre enter aleatori uniformement distribuït en $\{0, 2^{min\{N, 10\}} - 1\}$. $N \geq 1$ és el nombre de retransmissions de la trama.

Per exemple, per a 10 Mbps: Back-Off per a $N = 1$ (1a. retransmissió) = {0, 51,2 μs}, Back-Off per a $N = 2$ (2a. retransmissió) = {0, 51,2, 102,4, 153,6 μs}. Aquest algorisme es repeteix un màxim de 16 vegades. Si en la retransmissió número 16 es torna a col·lidir, la trama es descarta.

Figura 48. Superposició de diverses senyals sobre el mateix canal



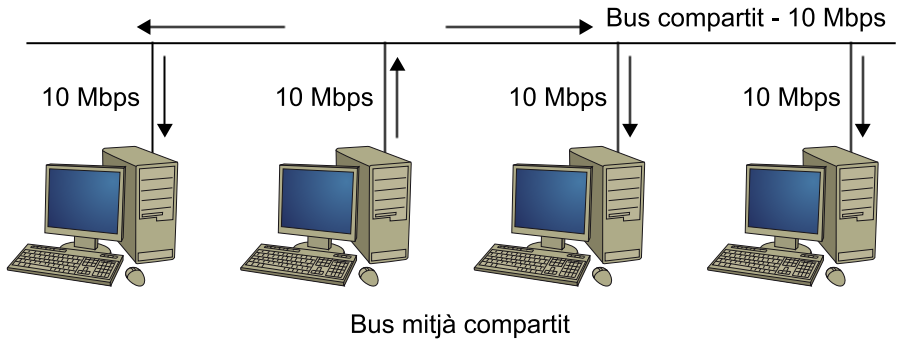
7.2.3. Dominis de col·lisió i domini de difusió

Un domini de col·lisió és el conjunt de segments en què les estacions connectades comparteixen el mateix medi de transmissió, i poden col·lidir directament entre elles. Les estacions Ethernet interconnectades amb dispositius de nivell 1 i 2 (coaxial, concentradors[72]) formen un únic domini de difusió.

[72]En anglès, *hubs*.

Un domini de difusió defineix un conjunt de segments pels quals s'envien trames de difusió. Les trames de difusió tenen como a objectiu arribar a totes les estacions de la xarxa, i a escala d'Ethernet es transmeten amb l'adreça MAC de destinació FF:FF:FF:FF:FF:FF. Hi ha nombrosos protocols que envien trames d'aquest tipus: ARP, DHCP, DNS, RIP, etc.

Figura 49

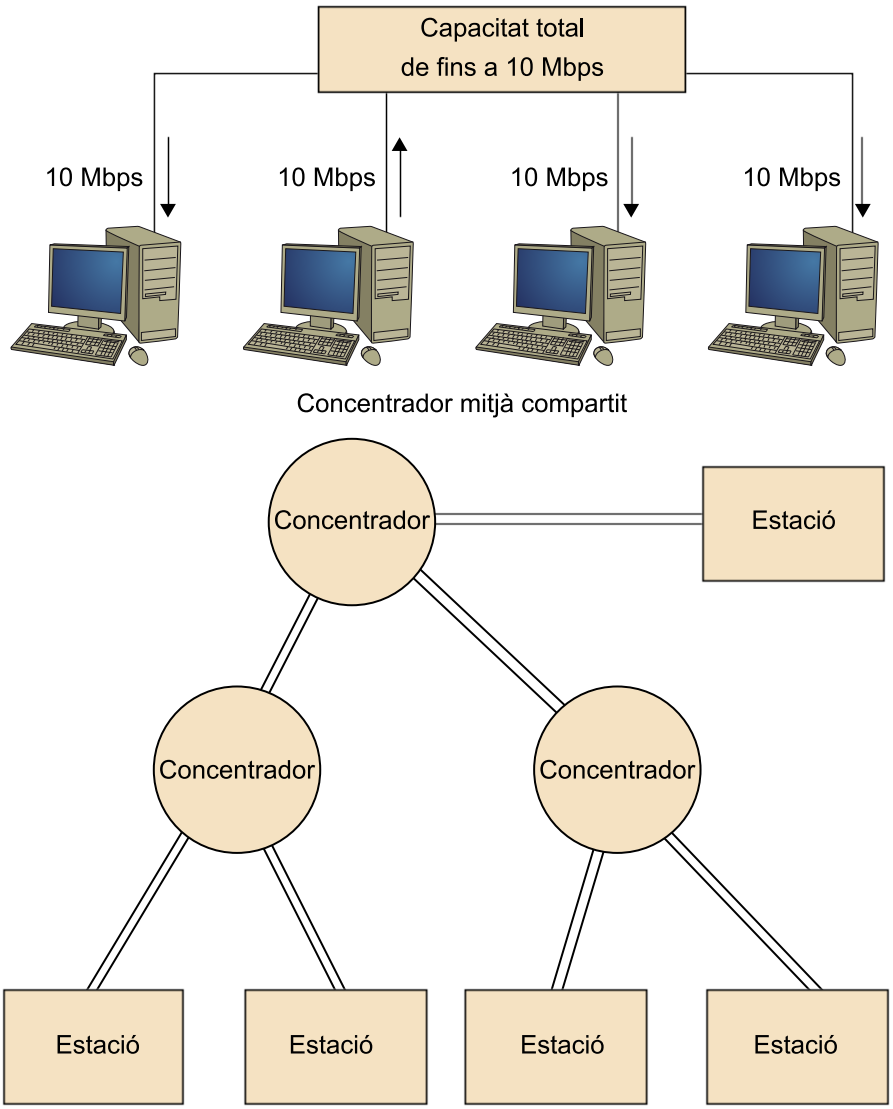


Un repetidor consta només de dos ports. Un concentrador és un repetidor multiport (més de dos ports).

Un concentrador és un dispositiu que opera a nivell 1 del model OSI (mouen bits entre dispositius). Regenera i sincronitza el senyal. Són dispositius de xarxa molt econòmics. No fa cap funció de commutació. No espera a tenir tota la trama per a començar a reenviar-la a la resta dels ports. No entén de trama, només de bits.

Un concentrador eixampla el domini de col·lisions: la xarxa a tots dos costats del repetidor és un mateix domini de col·lisió. Això provoca una degradació del rendiment de la xarxa que depèn del nombre de terminals connectats. Els terminals connectats a un concentrador comparteixen l'amplada de banda. Els concentradors, de manera inherent, són elements semidúplex i també incrementen la mida d'un domini de difusió.

Figura 50



Un pont[73] consta de 2 ports i té el funcionament basat principalment en programari. Cada port d'un pont és un domini de col·lisió diferent.

(73)En anglès, *bridge*.

Figura 51. Funcionament d'un pont

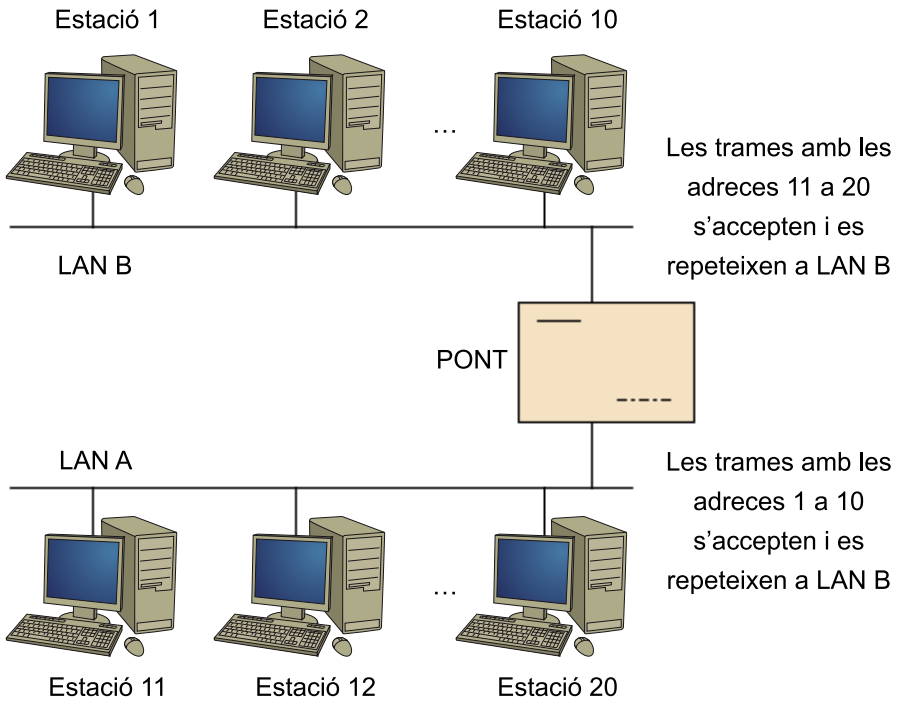
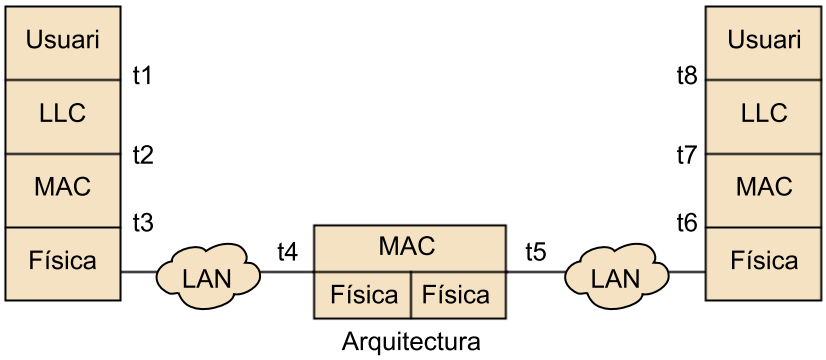


Figura 52. Arquitectura d'un pont



Un commutador[74] consta de més ports i de més capacitat de commutació que un pont. El funcionament d'un commutador està basat bàsicament en maquinari. Prenen decisions d'encaminament basades en adreces MAC. Operen a nivell 2 de la torre OSI. Tots dos disposen d'una taula MAC amb la taula (adreça MAC, número de port), que indica les adreces MAC conegudes que pengen de cada port. Les entrades en la taula MAC d'un commutador han de ser actualitzades dins un determinat temporitzador[75] (como en ARP):

(74)En anglès, *switch*.

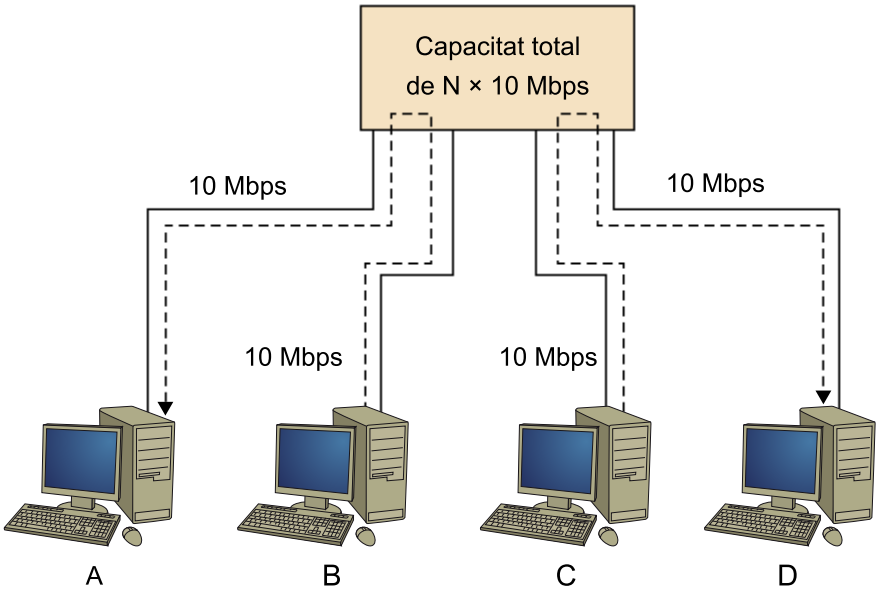
(75)En anglès, *time-out*.

- Cada vegada que una entrada s'utilitza, el temporitzador es refresca.
- Si salta el temporitzador, l'entrada s'esborra de la taula.

Com els commutadors, que són dispositius Store & Forward (commuten trames a nivell 2), no propaguen les col·lisions, segmenten el domini de col·lisions d'una xarxa Ethernet (disminueixen la mida dels dominis de col·lisió). Augmenten l'amplada de banda disponible per usuari, ja que minimitzen el trànsit de col·lisions. Creen un circuit virtual (camí dedicat) entre dos dispositius que es volen comunicar. En principi ni augmenten ni dismi-

nueixen el domini de difusió. Els commutadors amb VLAN sí que poden segmentar el domini de difusió. Els commutadors transmeten a més velocitat que els encaminadors (nivell 3), i a més a més, són més econòmics.

Figura 53. *Switching hub*



7.2.4. Ethernet commutada

Els commutadors són els dispositius que han permès fer evolucionar les antigues xarxes Ethernet compartides multiaccés (construïdes per mitjà d'un bus o per mitjà de concentradors) a les xarxes Ethernet commutades en què cada usuari té una amplada de banda del 100%.

Un commutador bàsicament està compost pels elements següents: processador, ports, detectors de col·lisió, memòria intermèdia, taules d'adreces MAC i la matriu de connexions.

S'utilitza un processador perquè es necessita una gran velocitat de processament de la informació (trames).

Els ports són les entrades i sortides dels ordinadors o altres xarxes, que poden tenir distintes velocitats (10, 100, 1.000, etc.) i de diferents tecnologies (Ethernet, anell de testimoni, etc.).

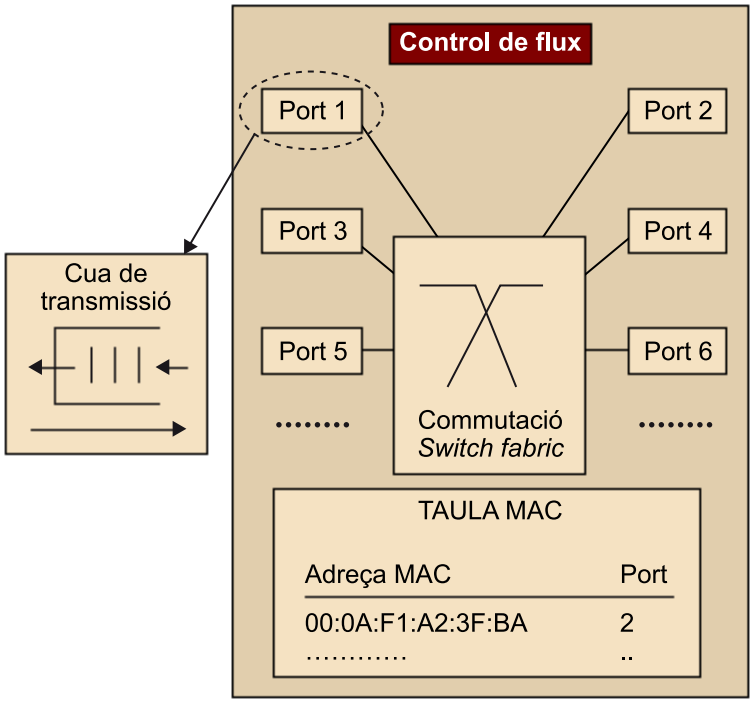
Els detectors de col·lisió són necessaris quan utilitzem una transmissió semidúplex en lloc de dúplex. Les memòries intermèdies les utilitzem per no haver d'obligar a efectuar repeticions des de les estacions. La taula d'adreces MAC és la que indica on està connectat un equip final o una xarxa. La matriu de connexions efectua físicament les connexions entre els ports.

El funcionament d'un commutador es basa en el procediment de Store & Forward: quan arriba una trama per un port, la desa per a estudiar per quin port l'ha de retransmetre:

- Es mira la seva adreça MAC origen: si l'adreça no es troba en la taula MAC o és en un port diferent, aleshores apunta aquesta adreça juntament amb el port pel qual ha arribat. La taula MAC es construeix de manera automàtica: aprèn les entrades en la taula MAC mirant les adreces font de les trames rebudes, juntament amb el port per on ha arribat.

- Mira la seva adreça MAC destinació i comprova que estigui en la taula MAC per a saber a quina cua de transmissió ha d'enviar la trama: si l'adreça no es troba en la taula MAC (o si és una adreça de difusió), aleshores envia la trama a les cues de transmissió de tots els ports (excepte el port pel qual ha arribat). Si l'adreça destinació es troba en la taula, aleshores posa la trama només en la cua de transmissió del port que diu la taula.

Figura 54. Arquitectura genèrica d'un commutador Ethernet



Quan un commutador rep una trama, el que fa en primer lloc és desar-la en una memòria intermèdia, per a enviar-la després als ports concrets de sortida. El commutador envia la trama des del port origen al port destinació i si es produeix una col·lisió es retransmet la trama des de la memòria intermèdia. Amb aquest procés s'evita que les estacions d'origen hagin de tornar a reenviar les trames en cas de col·lisió. No hi ha contenció, ja que s'envien les trames en el mateix ordre en què arriben, com una cua FIFO[76].

(76) *FIFO* és la sigla de *first in / first out*.

El commutador pot gestionar la memòria intermèdia de dues maneres diferents: una cua vinculada a cada port específic, o una memòria compartida per a tots els ports del commutador.

Hi ha dos tipus de commutació:

1) Store & Forward: el commutador desa tota la trama completa abans de retransmetre-la. Ofereix la màxima latència (retard) per a la comprovació d'errors. Amb aquest mètode es comproven tots els camps de la trama amb el CRC, i si aquest valor és correcte, la trama es reenvia. Sol ser el mètode predeterminat a la gran majoria de commutadors.

2) Cut-through: consisteix a enviar una trama tan enviat com es rebi la capçalera de la trama sense esperar que la trama s'hagi rebut completament. Si hi ha errors en la trama aquests errors s'envien amb la trama i es perjudica el rendiment de la xarxa per les retransmissions. També té una opció (*fragment free*) per a filtrar els fragments de col·lisió abans de fer la commutació.

7.2.5. STP / RSTP

Les topologies redundants ofereixen protecció davant la caiguda d'un determinat enllaç, port o dispositiu. Seria desitjable que hi hagués bucles per a tenir diversos camins alternatius, perquè si un deixés de funcionar, un altre camí fos l'alternatiu. Malgrat això, les topologies commutades ofereixen certs problemes, com en les tempestes de difusió, transmissions de múltiples còpies de trames, i inestabilitat en les taules MAC dels commutadors. L'algorisme STP[77] (IEEE 802.1d) o l'RSTP[78] permeten crear topologies lliures de llaços a partir de topologies físiques amb llaços redundants. Els commutadors que utilitzen STP/RSTP s'intercanvien un conjunt de missatges BPDU per a deixar una topologia lliure de bucles (topologia en arbre o estrella). Per a això, poden arribar a desconnectar o bloquejar un port si hi ha un altre camí en el mateix segment. Els ports bloquejats descarten totes les trames de dades que reben i només capturen els missatges RSTP. D'aquesta manera poden passar a l'estat normal de funcionament si hi ha un canvi en la topologia que ho requereixi.

(77) *STP* és la sigla de *spanning tree protocol.*

(78) *RSTP* és la sigla de *rapid spanning tree protocol.*

7.2.6. Ethernet semidúplex

Generalment les targetes dúplex tenen un mecanisme d'autonegociació que permet detectar si és possible activar-lo. En Ethernet hi ha dos tipus de comunicacions:

1) Semidúplex: només un únic dispositiu pot enviar i rebre informació a la vegada. Si diversos dispositius es volen comunicar a la vegada produiran col·lisions. Quan es produeix una col·lisió l'estació deixa de transmetre. Una connexió d'aquest tipus és la que es produeix quan diversos equips estan connectats a un concentrador; per la seva manera de funcionar, si el senyal es rep

per un port d'entrada l'ha d'enviar als altres ports, i si rep un altre senyal per un altre port, no podrà enviar simultàniament aquests senyals. El mode de funcionament semidúplex s'implementa amb el protocol CSMA/CD.

2) Dúplex: les comunicacions permeten que dos dispositius es comuniquin entre si de manera simultània. Quan es connecta una targeta semidúplex a un commutador amb UTP, s'activa el mode dúplex i es desactiva el mecanisme CSMA/CD. Quan la xarxa funciona en mode dúplex es duplica la capacitat de l'enllaç, i no es produeixen col·lisions, ja que els dos dispositius formen un únic domini de col·lisió. El cable UTP té quatre parells de cables, que donen moltes possibilitats; 10BaseT i 100BaseTX utilitzen dos parells: un per a la transmissió i l'altre per a la recepció de manera simultània. La col·lisió es detecta perquè es rep el senyal pel parell de recepció mentre s'està transmetent pel parell de transmissió. 100BaseT4 utilitza un parell per a transmetre, un per a rebre i els altres dos per a transmetre i rebre de manera simultània.

A més a més, generalment els ports 10/100 Mbps tenen un mecanisme d'autonegociació que permet detectar la velocitat de transmissió del dispositiu que es connecta. Ho fan per mitjà d'un control de flux per mitjà d'unes trames especials Jabber (mode semidúplex) o Pause (mode dúplex).

7.2.7. LAN virtuals

Una LAN virtual (VLAN) és un agrupament lògic de dispositius de xarxa o d'estacions que no estan subjectes a un agrupament físic. Permeten agrupar dispositius per funcions, equips, departaments o aplicacions en l'organització empresarial.

El commutador manté una taula MAC diferent per a cada VLAN. Cada commutador aïlla els ports que pertanyen a VLAN diferents. És per això que si arriba una trama de difusió per un port, el commutador només la reenvia als altres ports que pertanyen a la mateixa VLAN. Una VLAN és un únic domini de difusió creat per un o més commutadors, que no està subjecte a cap segment físic i és tractat com una subxarxa. La comunicació entre diferents VLAN es fa per mitjà d'un dispositiu de nivell 3 (per exemple, un encaminador).

La creació de les VLAN millora el rendiment i la seguretat de la xarxa commutada i serveix per a controlar la propagació de la difusió. Proporciona segmentació i flexibilitat organitzativa. Permet agrupar usuaris per funcions lògiques i no per ubicació física. Permet tenir servidors i ordinadors relacionats entre diferents dominis de difusió, cada un identificat amb una xarxa. Simplifica la tasca d'agregar i moure recursos per una subxarxa.

Hi ha dos tipus de VLAN:

1) VLAN estàtiques: basades en ports. Cada port d'un commutador s'associa estàticament a una VLAN. Totes les estacions que pengen d'aquest port pertanyen a la VLAN que té associada. És el mètode més utilitzat. Són segures i fàcils de configurar i controlar.

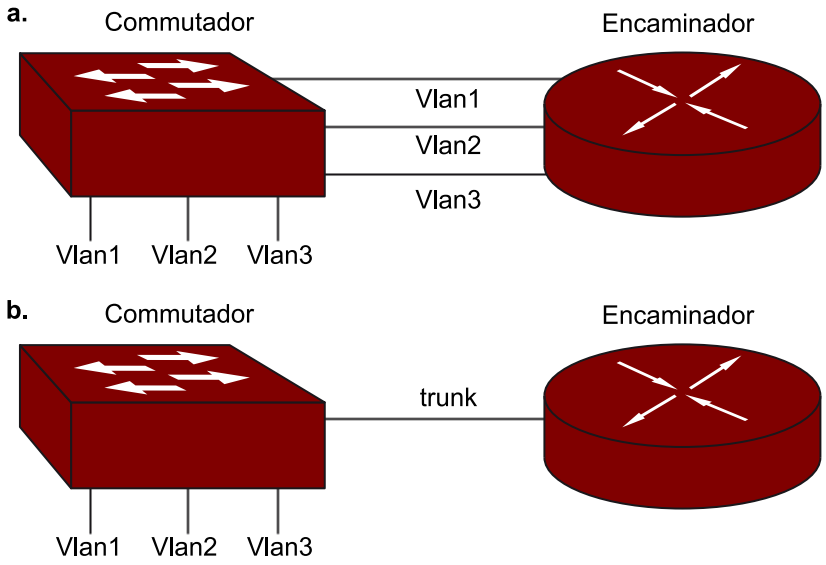
2) VLAN dinàmiques: basades en adreces lògiques (IP) o en adreces físiques (MAC). En un mateix port hi pot haver ordinadors de diferents VLAN. Cada commutador detecta que es connecta una nova estació a un port, i consulta una base de dades per a saber a quina VLAN pertany. En aquest cas la VLAN a la qual pertany l'ordinador s'identifica per l'adreça MAC de l'ordinador. Quan una estació es connecta, per mitjà de la seva adreça MAC es configura automàticament el port amb la configuració de la VLAN corresponent.

Es va desenvolupar el *VLAN trunking protocol* per a gestionar la transferència de trames de diferents VLAN a través d'una sola línia física[79]. Serveix per a evitar connectar o enllaçar un cable per cada VLAN entre dos commutadors o entre un encaminador i un commutador. Un enllaç de línia física agrupa múltiples enllaços virtuals sobre un únic enllaç físic, afegint unes etiquetes especials a les trames per a identificar a quina VLAN pertany la trama.

[79] En anglès, *trunk*.

En la figura 55 es mostren dues alternatives per a interconnectar VLAN entre elles per mitjà d'un encaminador: amb línia física o sense.

Figura 55. Interconnexió de VLAN mitjançant un encaminador: amb línia física o sense



a. Utilitza molts ports. No és escalable. **b.** Estalvia ports cablejats. Permet afegir VLAN sense cost. Requereix el protocol per a etiquetar les trames ISL o IEEE 802.1Q.

Els dos mètodes, ISL[80] i IEEE 802.1Q, es basen a afegir un identificador[81] a la capçalera de la trama quan és encaminada pel commutador. L'identificador identifica la VLAN a la qual pertany la trama. Quan la trama s'envia per un port que no té *trunking*, el commutador elimina l'identificador abans d'enviar-lo a l'estació destinació.

[80] *ISL* és la sigla d'*inter-switch link*.

[81] En anglès, *tag*.

7.2.8. Tecnologies Ethernet

El comitè IEEE ha definit diferents configuracions físiques alternatives que ha tingut aquesta tecnologia, i ha proporcionat una gran varietat d'opcions.

Nom comercial	Estàndard	Denominació	Cable	Parells UTP	Dúplex	Connector	Codificació	Distància segment
Ethernet	802.3	10Base5	Coaxial Thick		No	AUI	Manchester	500 m
	802.3a	10Base2	Coaxial Thin		No	BNC	Manchester	185 m
	802.3i	10BaseT	UTP cat.3	2	Sí	RJ-45	Manchester	100 m
Fast Ethernet	802.3u	100BaseTX	UTP cat.5	2	Sí	RJ-45	4B/5B	100m
	802.3u	100BaseT4	UTP cat.3	4	No	RJ-45	8B/6T	100 m
Gigabit Ethernet	802.3ab	100BaseT	UTP cat.5	4	Sí	RJ-45	8B/10B	100 m

La nomenclatura d'Ethernet utilitzada és **XBaseY**, en què:

- **X** és la velocitat de transmissió en Mbps.
- **Base** és la codificació en banda base.
- **Y** pot tenir diversos significats: si és un nombre fa referència a la distància màxima (aproximada) del segment en centenars de metres. Pot fer referència al tipus de medi de transmissió (T: parell trenat; F: fibra òptica) i pot ser alguna altra característica (4: utilitza els quatre parells trenats; X: dúplex).

1) Especificacions IEEE 802.3 10 Mbps (Ethernet)

a) 10BASE-T

- Utilitza el cablatge que s'ha convertit en el més econòmic: UTP (parell trenat no apantallat) amb els connectors RJ-45.
- Topologia en estrella. La senyalització és digital Manchester.
- La longitud màxima del cable és de 100 m.
- Utilitza cable UTP i connectors RJ-45 en la NIC i el repetidor.
- En 10BaseT les estacions es connecten a través d'un concentrador. El concentrador regenera i amplifica el senyal que rep per un port i el transmet a la resta de ports, amb un retard de pocs bits.

- Actualment, però, els cablatges amb coaxial (10Base5 i 10Base2) han quedat obsolets en favor del cablatge amb UTP. Si es necessiten cobrir distàncies majors de les que permet UTP, aleshores s'utilitza fibra òptica.

- El mode de funcionament pot ser semidúplex o dúplex, depenent del dispositiu connectat.

Especificacions 10BaseX				
	10BASE5	**10BASE2**	**10BASET**	**10BASE-FP**
Transmission Medium	Coaxial Cable (50 ohm)	Coaxial Cable (50 ohm)	Unshielded twister pair	850-nm optical fiber pair
Signaling Technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/On-Off
Topology	Bus	Bus	Star	Star
Maximum segment length (m)	500	185	100	500
Nodes per segment	100	30	----	33
Cable diamenter (mm)	10	5	0.4 to 0.6	62.5/125 µm

2) Especificacions IEEE 802.3 100 Mbps (Fast Ethernet)

És el conjunt d'especificacions desenvolupades pel comitè IEEE 802.3 per a proporcionar més velocitat a les LAN.

a) 100BASE-TX

- També conegut como a *100BASE-X*. Es permet la utilització tant de STP como d'UTP de cat5.

- Utilitza dos parells de cable de parell trenat: un parell per a transmissió i un altre per a recepció.

- La longitud màxima és de 100 m.

- Utilitza la senyalització 4B/5B - NRZI. Utilitza grups de 5 bits per a enviar 4 bits de dades.

b) 100BASE-FX

- Utilitza dues fibres òptiques, una per a transmissió i una altra per a recepció, en mode dúplex.

- És necessari un convertidor optoelectrònic que converteixi la seqüència de grups del codi 4B/5B-NRZI en senyals òptics.

- La longitud màxima és de 100 m.

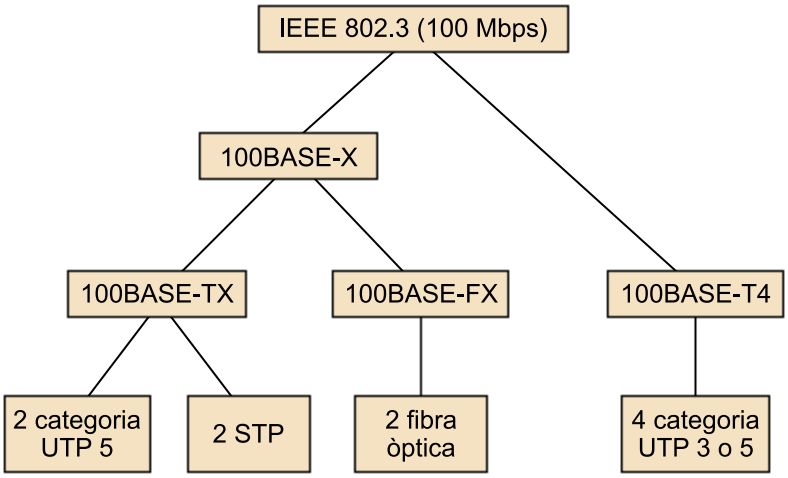
c) 100BASE-T4

- S'utilitzen els quatre parells trenats: tres s'utilitzen per a la transmissió amb una velocitat efectiva de 33,3 Mbps i l'altre, juntament amb dos dels utilitzats en la transmissió, s'utilitzen per a la recepció. Hi ha dos parells que s'han de configurar per a una transmissió bidireccional.

- La longitud màxima és de 100 m. Utilitza la senyalització 8B/6T.

- És utilitzat per xarxes que necessiten baixa qualitat de parells trenats en una xarxa 100 Mbps Ethernet.

Figura 56. Diagrama 100BaseX



3) Especificacions IEEE 802.3 1000 Mbps (Gigabit Ethernet)

a) 1000BASE-CX

Estàndard Gigabit Ethernet sobre cable de coure, que ha estat reemplaçat per 1000BASE-T.

b) Gigabit Ethernet 1000BASE-T (802.3z/802.3ab)

- Utilitza els quatre parells UTPcat5 per a enviar i rebre simultàniament.
- Codificació 8B/10B.
- Distància típica de 1.000 m.

c) 1000BASE-SX

- Estàndard Gigabit Ethernet sobre fibra òptica que opera sobre fibra multimode.

- Típica distància fins a 550 m.

d) 1000BASE-LX

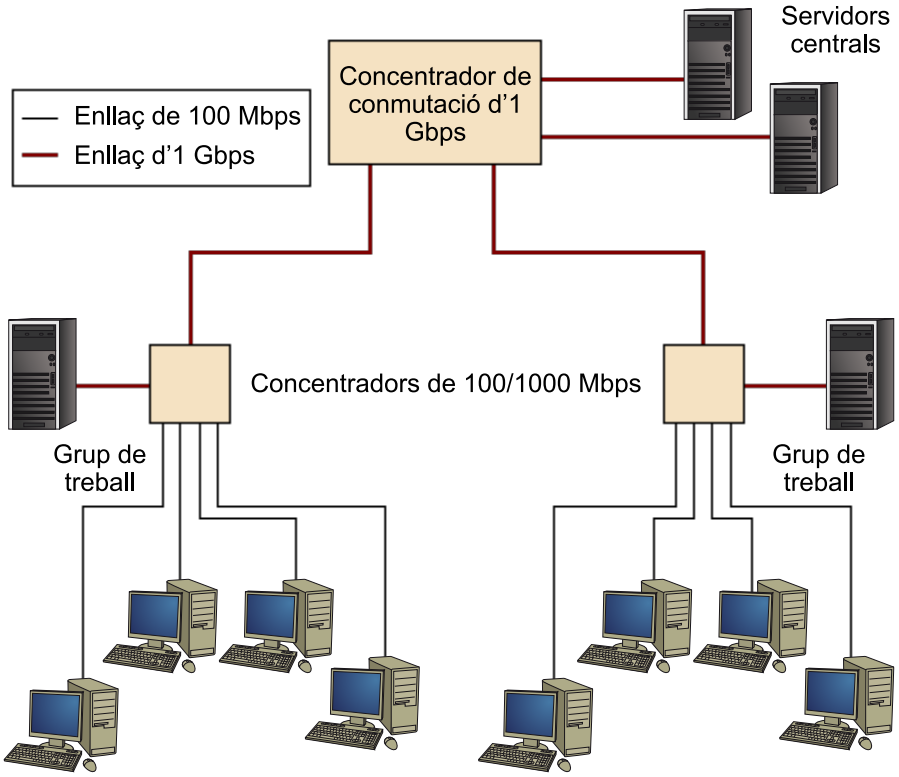
- Estàndard Gigabit Ethernet sobre fibra òptica que opera sobre fibra monomode.

- Típica distància de 550 m a 5 km.

e) 10 Gigabit Ethernet (802.3ae)

Opera només en mode dúplex i amb fibra òptica.

Figura 57. Els enllaços 1000BaseX es poden utilitzar per a interconnectar xarxes LAN de menys velocitat



Quadre resum de diverses especificacions 10xzBaseY									
	10BASE 2	10BASE 5	10BASE -T	100BASE -TX	1000BASE -FX	1000BASE -CX	1000BASE -T	1000BASE -SX	1000BASE -LX
Medis	Coaxial de 50 ohms (Thinnte)	Coaxial de 50 ohms (Thinteh)	UTP categoria 3,4,5 EIA/TIA, dos parells	UTP categoria 5 EIA/TIA dos parells	Fibra multimode 62.5/125	STP	UTP categoria 5 EIA/TIA quatre parells	Fibra micro multimode 62.5/50	Fibra micro multimode 62.5/50; fibra monomode de 9 micrones

Quadre resum de diverses especificacions 10xzBaseY									
	10BASE 2	**10BASE 5**	**10BASE -T**	**100BASE -TX**	**1000BASE -FX**	**1000BASE -CX**	**1000BASE -T**	**1000BASE -SX**	**1000BASE -LX**
Longitud de segment màxim	185 m	500 m	100 m	100 m	400 m	25 m	100 m	275 m per a microfibra 62.5;550 m per a microfibra de 50	440 m per microfibra 62.5;550 m per microfibra de 50; de 3 a 10 km per fibra monomode
Topologia	Bus	Bus	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Connector	BNC	AUI (interfície d'unitat de connexió)	RJ-45 ISO 8877	RJ-45 ISO 8877		RJ-45 ISO 8877	RJ-45 ISO 8877		

7.3. Xarxes sense fils

Els avantatges de les xarxes sense fils són la mobilitat i la seva flexibilitat, la facilitat d'instal·lació, l'escalabilitat, el dinamisme en els canvis de la topologia, i que poden arribar on no pot arribar el cable. Com a principals inconvenients tenim el seu elevat cost inicial i la seva seguretat.

El seu àmbit d'aplicació és molt ampli. Són de gran utilitat en edificis històrics, en entorns canviants, en què hi ha usuaris en moviment (hospitals, oficines, fàbriques...), en grups de treball eventuals, en ambients industrials en què les condicions mediambientals són problemàtiques, en usos domèstics, etc.

7.3.1. Característiques de les xarxes sense fils

Les diferents tecnologies sense fils se solen agrupar basant-se en el radi d'acció (l'abast) de cadascuna:

- Xarxes personals sense fils (WPAN[82]): aquest concepte s'aplica quan la distància que es vol cobrir és d'uns quants metres. La família d'estàndards més representatius són el 802.15.1 (Bluetooth), 802.15.3a (UWB) i el 802.15.4 (Zigbee).

(82) *WPAN* és la sigla de *wireless personal area network*.

- Xarxes locals sense fils (WLAN[83]): permeten donar serveis a distàncies d'un centenar de metres (un pis, una planta d'un edifici, una nau industrial, uns carrers...). L'estàndard més destacat en aquest camp és el 802.11 (Wi-Fi).

(83) *WLAN* és la sigla de *wireless local area network*.

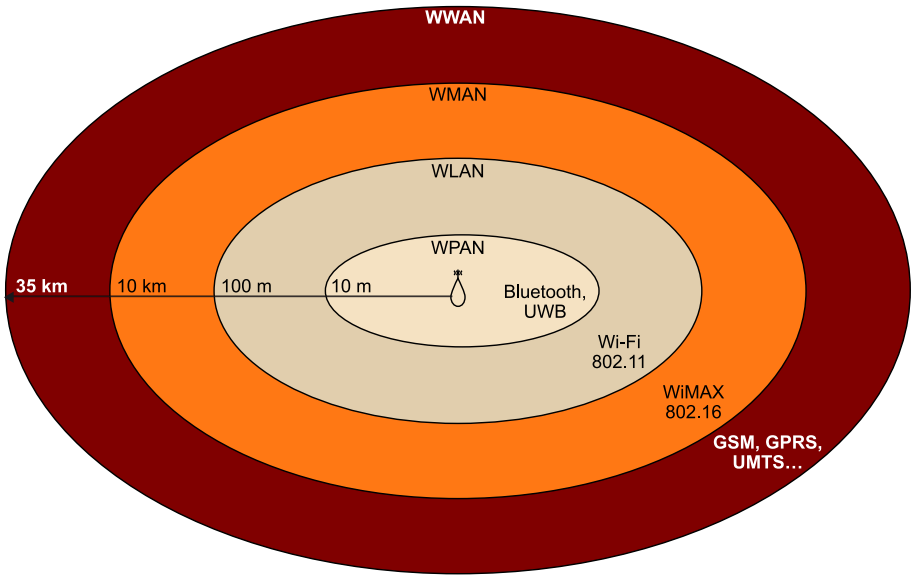
- Xarxes metropolitanes sense fils (WMAN[84]): permeten donar serveis a distàncies d'uns quants quilòmetres (un barri, un poble, una urbanització...). L'estàndard més destacat en aquest camp és el 802.16 (WiMAX).

(84) *WMAN* és la sigla de *wireless metropolitan area network*.

- Xarxes de gran abast sense fils (WWAN[85]): tenen una cobertura més àmplia. La família d'estàndards més representatius són el GSM, el GPRS i l'UMTS.

(85) *WWAN* és la sigla de *wireless wide area network*.

Figura 58. Classificació de les tecnologies sense fils



7.3.2. Wi-Fi (IEEE 802.11)

L'estàndard IEEE 802.11, també anomenat *Wireless Ethernet*, fou aprovat l'any 1997. Fou pensat per a desenvolupar LAN dins la banda de freqüències ISM: banda a 2,4 GHz, pensada per a usos industrials, científics, mèdics i no comercials sense autorització administrativa de cap govern. S'utilitza dins de zones geogràfiques molt limitades. Aquest estàndard especifica una interfície aèria entre un client sense fils i una estació base o entre dos clients sense fils.

El terme *Wi-Fi*[86] fa referència al conjunt d'estàndards per a xarxes sense fils basat en les especificacions IEEE 802.11x, i fou creat per la Wi-Fi Alliance. Tot producte que ha estat testejat i aprovat per la Wi-Fi Alliance duu el text "Wi-Fi Certified", cosa que en garanteix la interoperabilitat. Les principals característiques de les diferents especificacions IEEE 802.11x es detallen en el quadre següent:

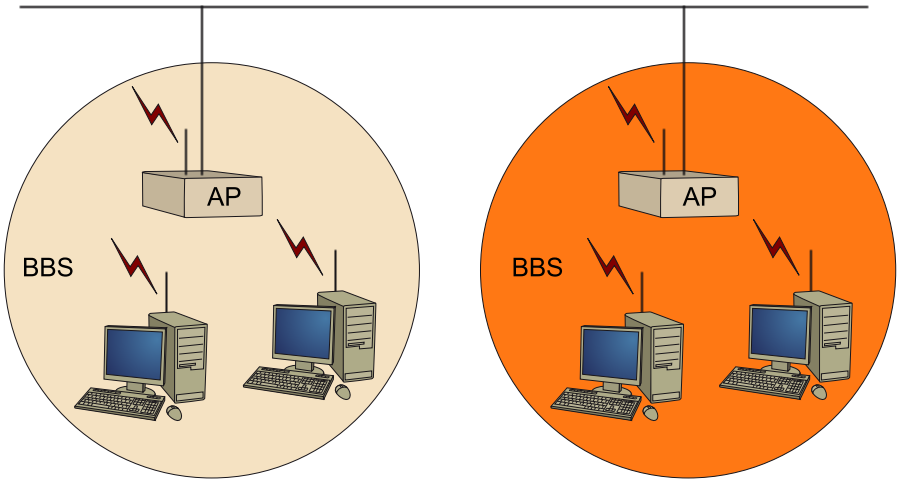
(86) En anglès, *wireless fidelity*.

Protocol	Any	Freqüència operació	Esquema de modulació	Velocitat màxima	Rendiment	Seguretat
802.11	1997	2,4-2,5 GHz	FHSS o DSSS	2 Mbps		WEP i WPA/WPA2
802.11a	1999	5,15-5,35/ 5,47-5,725/ 5,725-5,875 GHz	OFDM	54 Mbps	25 Mbps	WEP i WPA/WPA2
802.11b	1999	2,4-2,5 GHz	DSSS amb CKK	11 Mbps	6 Mbps	WEP i WPA/WPA2
802.11g	2003	2,4-2,5 GHz	OFDM sobre 20 Mpbs, DSSS amb CKK sobre 20 Mbps	54 Mbps	22 Mbps	WEP i WPA/WPA2
802.11n	2008	2,4 GHz o 5 GHz bandes		540 Mbps		WEP i WPA/WPA2

Arquitectura de xarxa

L'arquitectura bàsica d'una LAN sense fils és la següent:

Figura 59



S'anomena *BSS*[87], que normalment conté una o més estacions sense fils i una estació base central, coneguda com a *AP*[88]. Les estacions sense fils poden estar fixes o mòbils, i es comuniquen amb l'estació base central amb el protocol MAC IEEE 802.11. Es coneix com a mode d'infraestructura. Aquesta topologia utilitza el concepte de cel·la, que és l'àrea en què un senyal radioelèctric és efectiu.

(87) *BSS* és la sigla de *basic service set*.

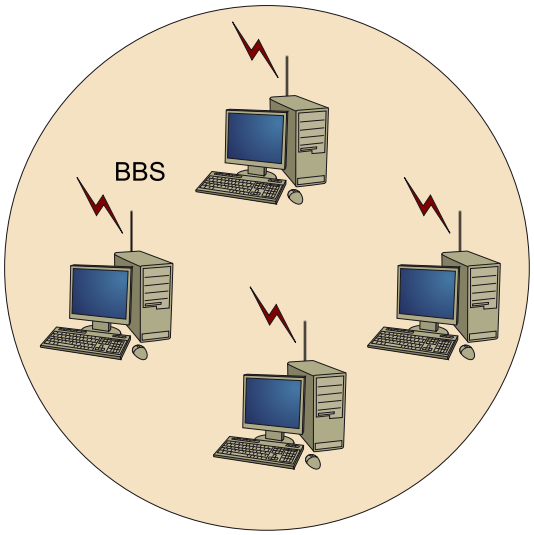
(88) *AP* és la sigla d'*access point*.

Diversos AP es poden connectar entre ells (per exemple, utilitzant una Ethernet cablada o un altre canal sense fils) formant el que s'anomena *sistema de distribució* (DS). En aquest cas, el sistema DS apareix en les capes superiors (per exemple, en el nivell IP) com una xarxa 802.

També les estacions poden formar una BSS o un grup d'estacions entre elles, d'igual a igual[89] sense control central, i es diu que funciona en forma de xarxa *ad hoc*. S'utilitza en general amb estacions que es troben casualment i es volen comunicar. Només calen dos equips amb el seu corresponent adaptador sense fils.

(89)En anglès, *peer to peer*.

Figura 60



Capa física

L'estàndard IEEE 802.11 defineix la capa física i la capa d'accés al medi (MAC). La capa MAC de l'IEEE 802.11 assumeix funcions que en general són assumides en altres protocols per les capes superiors, com són la fragmentació, la recuperació d'errors, el control de la mobilitat i la conservació de la potència.

La capa física utilitza un espectre estès per seqüència directa (DSSS[90]) que codifica cada bit en una cadena de bits, anomenat *codi*. Aquesta tècnica és molt similar a la utilitzada en CDMA, excepte que totes les estacions mòbils (o estacions base) utilitzen el mateix codi. A causa de la utilització del mateix codi per part de totes les estacions que formen la xarxa, DSSS no és un protocol d'accés múltiple: es tracta d'un mecanisme de la capa física que a partir d'un senyal emet una energia sobre un rang de freqüències concret, i provoca que el receptor pugui recuperar el senyal original.

(90)DSSS és la sigla de *direct sequence spread spectrum*.

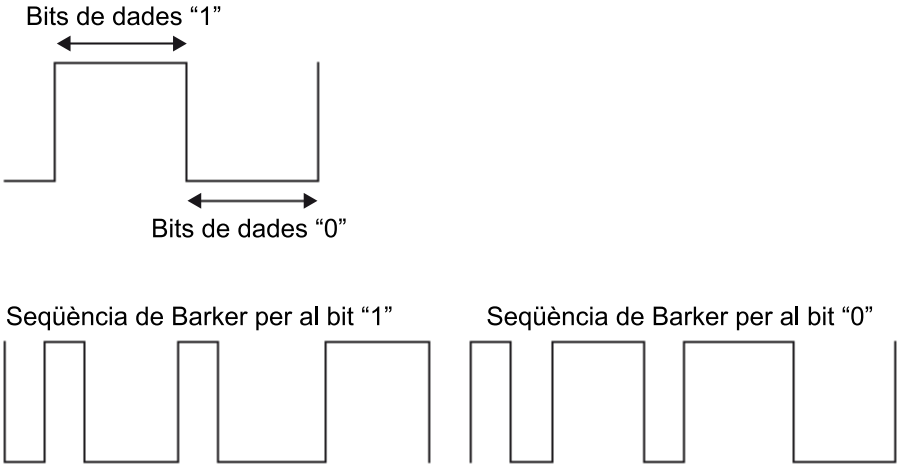
Hi ha dos tipus de medis per a la instal·lació de xarxes sense fils: per ones de radiofreqüència i per senyals òptics d'infrarojos.

La capa IEEE 802.11 defineix tres possibles esquemes de la capa física: DSSS, FHSS[91] (espectre estès per salt de freqüència) i llum infraroja en banda base (sense modular).

(91)*FHSS* és la sigla de *frequency hopping spread spectrum*.

La radiofreqüència utilitza les bandes de 2,4 GHz i de 5,7 GHz. No tenen problemes per a propagar-se a través dels obstacles. El DSSS genera un patró de bits pseudoaleatori (senyal de xip) per a cada un dels bits que formen el senyal. Com més gran sigui el patró més resistents són les dades a possibles interferències (de 10 a 100 bits). Aquesta seqüència és coneguda com a seqüència de Barker (o codi de dispersió). La seqüència és balancejada, és a dir, aproximadament hi ha la mateixa quantitat de zeros que d'uns. Totes les estacions coneixen la seqüència utilitzada. Aquesta seqüència proporciona un guany de processament (per a 10 bits, s'obté una G = 10 dB, per a 100 bits, G = 20 dB). El guany ha de ser major o igual que l'SNR (relació senyal/soroll).

Figura 61. Codificació de Barker



En DSSS, la modulació en la freqüència 2,4 GHz utilitza variacions en fase d'una sola portadora en amplitud constant: DBPSK[92] i DQPSK[93]. En la banda de 5,7 GHz, s'utilitzen variacions de freqüència de múltiples portadores: OFDM[94].

En els canals a Europa i els EUA, DSSS utilitza un rang de freqüències de 2,400 GHz - 2,4835 GHz. Això ens dóna una amplada de banda de 83,5 MHz. Se subdivideix en canals de 5 MHz cadascun, cosa que ens proporciona un total de 14 canals independents. Cada estat té autoritzat utilitzar un subconjunt d'aquests canals. A Espanya s'usen els canals 10 i 11, corresponents a freqüències centrals de 2,457 GHz i 2,462 GHz, respectivament. Els identificadors de canals, freqüències centrals, i dominis reguladors per a cada canal usat per IEEE 802.11b i IEEE 802.11g són els següents:

(92) *DBPSK* és la sigla de *differential binary phase shift keying*.

(93) *DQPSK* és la sigla de *differential quadrature phase shift keying*.

(94) *OFDM* és la sigla d'*ortogonal frecuency division multiplexing*.

Canal	Freqüència en MHz	Dominis reguladors				
		Amèrica (-A)	EMEA (-E)	Israel (-I)	Xina (-C)	Japó (-J)
1	2.412	X	X	–	X	X
2	2.417	X	X	–	X	X
3	2.422	X	X	X	X	X
4	2.427	X	X	X	X	X

Canal	Freqüència en MHz	Dominis reguladors				
		Amèrica (-A)	EMEA (-E)	Israel (-I)	Xina (-C)	Japó (-J)
5	2.432	X	X	X	X	X
6	2.437	X	X	X	X	X
7	2.442	X	X	X	X	X
8	2.447	X	X	X	X	X
9	2.452	X	X	X	X	X
10	2.457	X	X	–	X	X
11	2.462	X	X	–	X	X
12	2.467	–	X	–	–	X
13	2.472	–	X	–	–	X
14	2.484	–	-	–	–	X

En la capa física que utilitza FHSS, la modulació en la banda de 2,4 GHz utilitzada és l'FSK (modulació en freqüència) segons el quadre següent:

Rang freqüències centrals amb FHSS			
Límit inferior	Límit superior	Rang regulatori	Àrea geogràfica
2,402 GHz	2,480 GHz	2,400-2,4835 GHz	Amèrica del Nord
2,402 GHz	2,480 GHz	2,400-2,4835 GHz	Europa
2,473 GHz	2,495 GHz	2,471-2,497 GHz	Japó
2,447 GHz	2,473 GHz	2,445-2,475 GHz	Espanya
2,448 GHz	2,482 GHz	2,4465-2,4835 GHz	França

La banda de freqüències en FHSS assignada es divideix en subbandes de menor freqüència, anomenades *canals*, amb la mateixa amplada de banda. Cada tram d'informació es transmetrà a una freqüència distinta durant un interval de temps molt curt[95] (menor que 400 ms), i a continuació salta a una freqüència diferent. El patró d'ús del canal és pseudoaleatori. La seqüència de salt es desa en taules, que coneixen tant l'emissor com el receptor. Així, la banda de 2,4 GHz s'organitza en 79 canals amb una amplada de banda d'1 MHz cada un. El nombre de salts per segon es regula a cada país. Per exemple, als EUA és de 2,5 salts/segon.

(95) En anglès, anomenat *dwell*.

La capa física per infrarojos s'utilitza en entorns molt localitzats, en una sola àrea o habitació. Utilitza unes freqüències d'emissió entre $3{,}10 \cdot 10^{14}$ i $3{,}52 \cdot 10^{14}$ Hz. El comportament és semblant al de la llum. Els inconvenients d'aquest sistema són que no travessa els objectes sòlids, que té poca capacitat de difusió, i que és massa sensible a objectes mòbils, a la llum solar directa i a les làmpa-

des. Les restriccions de potència d'emissió limiten la cobertura a desenes de metres. Es produeix dispersió i rebots, que provoquen interferències i limiten la velocitat de transmissió.

7.3.3. CSMA/CA

El protocol utilitzat en IEEE 802.11 és el CSMA/CA[96]. El protocol CSMA és el primer que observa el canal per a determinar si el canal està ocupat o no per part d'una altra estació que estigui transmetent una trama. En una especificació sense fils, la capa física monitora el nivell d'energia de les ones de ràdio a una determinada freqüència per a determinar si una estació ocupa o no el canal (l'aire), i envia aquesta informació a la seva capa MAC. Si s'observa que el canal està lliure per un temps igual o superior al DIFS[97], l'estació està autoritzada a transmetre. Aquesta trama serà rebuda per l'estació receptora si cap estació no ha interferit amb la transmissió d'aquesta trama.

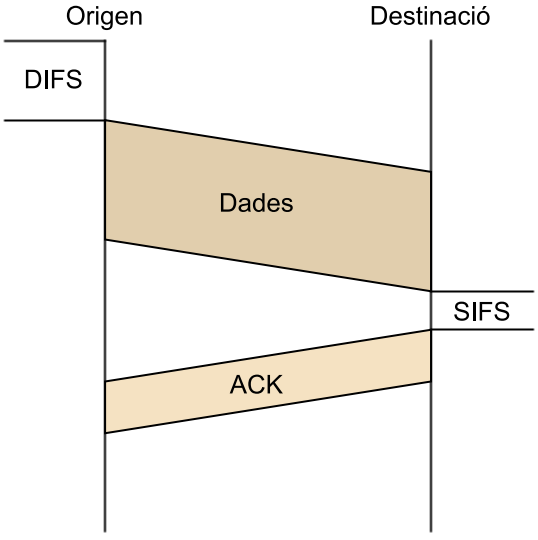
(96) *CSMA/CA* és la sigla de *CSMA with collision avoidance*.

(97) *DIFS* és la sigla de *distributed inter frame space*.

Quan l'estació ha rebut correctament i completament una trama, espera un espai curt de temps anomenat *SIFS*[98] i aleshores envia una confirmació explícita cap a l'emissor i li indica que ha rebut correctament la trama. S'ha d'enviar aquesta trama, ja que en un entorn obert com és l'aire l'emissor per ell sol no pot determinar si ha ocorregut una col·lisió o no.

(98) *SIFS* és la sigla de *short inter frame spacing*.

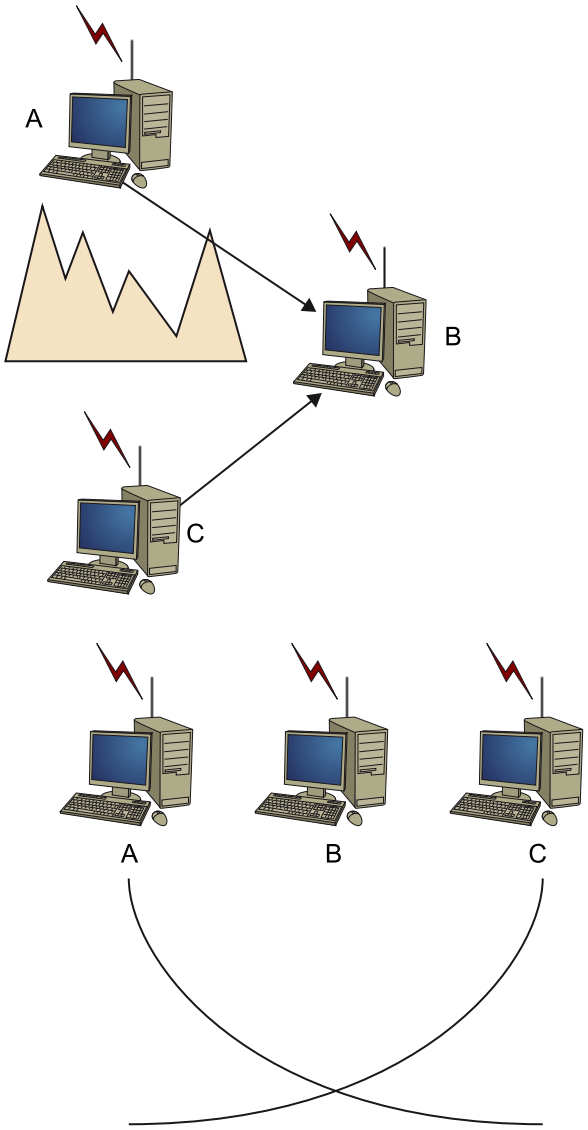
Figura 62



Quan l'emissor detecta que el canal està ocupat, executa un algorisme de *Back-Off* similar al que utilitza Ethernet; quan torna a detectar que el canal està lliure, aleshores espera un temps DIFS, i després l'estació calcula un temps addicional aleatori de *Back-Off* i el comença a comptar amb un comptador cap enrere mentre el canal estigui lliure. Quan el temporitzador del *back-off* aleatori arriba a zero, l'estació transmet la trama. L'interval de temps sobre el qual el temporitzador de *back-off* calcula el temps aleatori es va doblant cada vegada que una trama transmesa experimenta una col·lisió.

Una situació que pot ocórrer és el que s'anomena el *problema del terminal ocult*. Suposem que l'estació *A* transmet a l'estació B. Suposem que també l'estació C transmet cap a l'estació *B*. Les obstruccions físiques en l'entorn (una muntanya, per exemple) poden provocar que A i C no es puguin comunicar entre elles, ja que només les seves transmissions arriben a l'estació B. Un segon escenari resulta del fet que el receptor no pot detectar les col·lisions a causa al problema de fàding (pèrdua) del senyal quan es propaga pel medi sense fils. La figura 63 mostra el cas en què A i C estan col·locades de tal manera que els seus senyals no són prou potents perquè entre ells es detectin transmissions, i el senyal només és prou potent per a comunicar-se amb l'estació que està al mig, l'estació *B*.

Figura 63



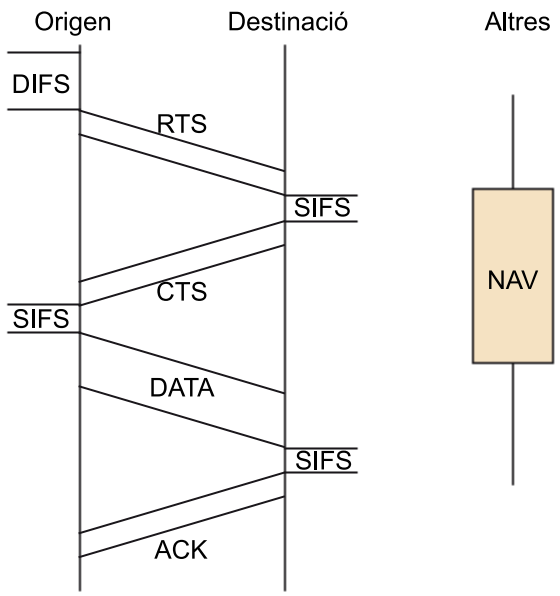
El protocol IEEE 802.11 no implementa el mecanisme de detecció de col·lisió (CD) com ho fa Ethernet (CSMA/CD). Això és perquè la capacitat de detectar col·lisions requereix la capacitat d'enviar i rebre al mateix temps. A causa de les dificultats per a detectar les col·lisions en un entorn sense fils, els enginyers d'IEEE 802.11 desenvoluparen aquest accés al medi amb la idea de prevenir les

(99) *NAV* és la sigla de *network allocation vector*.

col·lisions, en lloc de detectar i recuperar les col·lisions. En primer lloc, una trama IEEE 802.11 conté un camp de durada en el qual l'estació emissora indica explícitament la quantitat de temps en què la trama s'estarà transmetent. Aquest valor permet a les altres estacions determinar el temps mínim (NAV[99]) que han d'esperar per a accedir al medi.

El protocol també pot utilitzar una petita trama de control anomenada *RTS* i una altra anomenada *CTS* per a reservar l'accés al canal. Quan un emissor vol enviar una trama, primer envia una RTS al receptor, i li indica la durada de la trama de dades en el paquet RTS. El receptor, quan rep una trama RTS, li respon amb un paquet CTS, i dóna a l'emissor permís explícit per a començar a transmetre. Totes les altres estacions que escolten les trames RTS i CTS saben que han d'esperar per a les seves respectives transmissions per no interferir amb aquesta transmissió. Un emissor i un receptor poden operar d'aquesta manera, o sense utilitzar les trames RTS i CTS. L'ús de RTS i CTS ens proporciona dues ajudes. Primer, com que la trama CTS serà escoltada per totes les estacions dins el radi d'acció de l'estació receptora, la trama CTS ajuda a resoldre el problema dels terminals ocults. Segon, com que les trames RTS i CTS són curtes, una col·lisió només es produirà durant la comunicació d'RTS i CTS, és a dir, durant la transmissió d'RTS i de CTS (cal notar que quan les trames RTS i CTS són enviades correctament, no es produeix cap col·lisió durant la transmissió de la trama de dades i de la trama d'ACK).

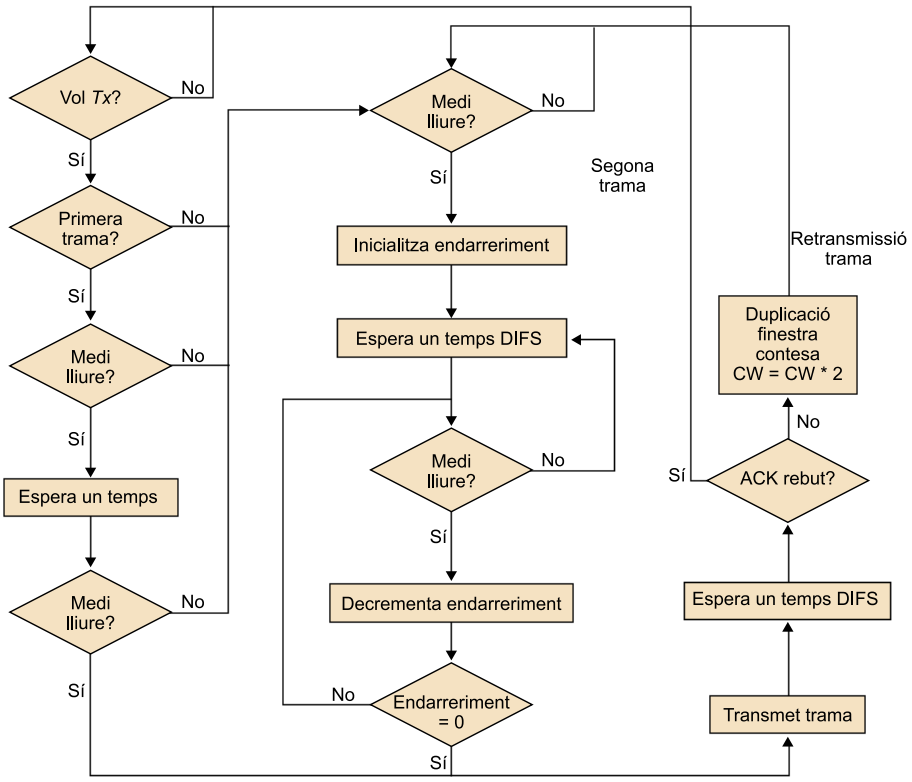
Figura 64



L'estàndard IEEE 802.11 també descriu altres característiques com la sincronització temporal, la gestió de la potència, la unió i desunió de les estacions a la xarxa, els mecanismes de seguretat, el xifratge, etc.

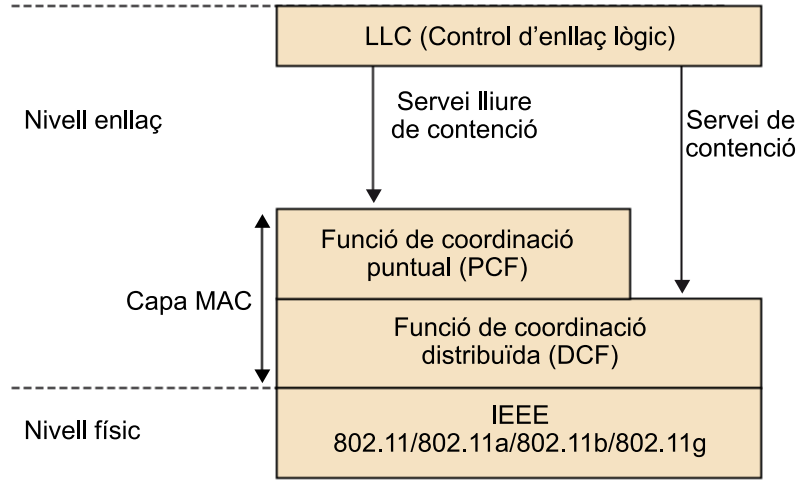
Resumint, l'algorisme de funcionament del CSMA/CA és el següent:

Figura 65



Definim la funció de coordinació com la funcionalitat que determina, dins un conjunt bàsic de serveis BSS, quan una estació pot transmetre o rebre unitats de dades de nivell MAC a través del medi sense fils. La capa MAC es compon de dues funcionalitats bàsiques: la funció de coordinació puntual (PCF) i la funció de coordinació distribuïda (DFC). La gran majoria de targetes comercials només implementen DCF, i no implementen el mode opcional PCF.

Figura 66



La DFC:

- Es pot utilitzar tant en mode d'infraestructura com en mode *ad hoc*.

- Permet la utilització de CSMA/CD amb RTS/CTS, que es coneix com a MA-CA.
- Permet el reconeixement d'ACK i provoca retransmissions si no es rep.
- Permet utilitzar el camp durada/ID, que conté el temps de reserva per a la transmissió i *ACK*.
- Implementa la fragmentació de dades.
- Concedeix prioritat a les trames amb l'ús de l'espaiat entre trames IFS.
- Suporta difusió i multidifusió sense ACK.

7.3.4. Trames IEEE 802.11

Les trames MAC contenen els components bàsics següents:

- Una capçalera MAC, que conté camps de control, durada, adreçament i control de seqüència.
- Un cos de trama de longitud variable, que conté informació específica del tipus de trama.
- Una seqüència de suma de comprovació (FCS) que conté un codi de redundància CRC de 32 bits.

Les trames MAC es poden classificar en tres tipus:

1) Trames de dades

2) Trames de control: ACK, RTC, CTS i trames lliures de contenda.

3) Trames de gestió: servei d'associació, trames de Beacon o portadora, trames TIM o de trànsit pendent en el punt d'accés.

El format d'una trama MC genèrica té l'estructura següent:

Figura 67

2 octets	2 octets	6 octets	6 octets	6 octets	2 octets	6 octets	0-2.312 octets	4 octets
Control de trama	Durada /ID	Adreça 1	Adreça 2	Adreça 3	Control de seqüència	Adreça 4	Cos de trama	FCS

Els camps que componen la trama són:

- **Durada**: en trames de Power Save per a dipositius amb limitacions de potència, conté l'identificador o AID d'estació. En la resta, s'utilitza per a indicar la durada del període que ha reservat una estació.

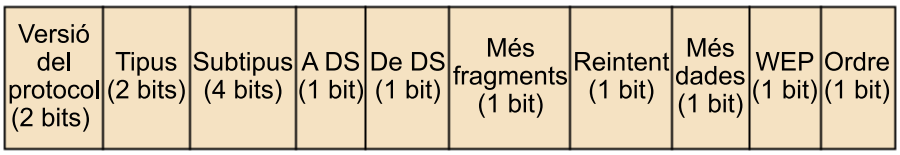
- **Address 1-4**: conté les adreces de 48 bits en què s'inclouran l'estació emissora, la que rep, la del punt d'accés origen i la del punt d'accés destinació.

- **Cos de la trama**: varia segons el tipus de trama que es vol enviar.

- **FCS**: conté la suma de comprovació.

Els camps de control tenen l'estructura següent:

Figura 68



- **Versió**

- **Type / Subtype**: Type indica si la trama és de dades, control o gestió; el camp Subtype ens identifica cada un dels tipus de trama de cada un d'aquests.

- **To DS / From DS**: identifica si la trama s'envia o es rep al sistema de distribució o des d'aquest. En xarxes *ad hoc*, To DS i From DS estan a zero. El cas més complex preveu l'enviament entre dues estacions per mitjà d'un sistema de distribució, i aquests dos bits estan a 1.

- **Més fragments**: s'activa si s'usa una fragmentació.

- **Retry**: s'activa si la trama és de retransmissió.

- **Power management**: s'activa si l'estació utilitza el mode d'economia de potència.

- **More data**: s'activa si l'estació té trames pendents en un punt d'accés.

- **WEP**: s'activa si s'utilitza el mecanisme d'autentificació i xifratge.

- **Order**: s'utilitza amb el servei d'ordenació estricta.

7.3.5. WiMAX (IEEE 802.16)

La tecnologia WiMAX[100] (interoperabilitat mundial per a l'accés per microones) representa una evolució pel que fa al Wi-Fi.

(100) *WiMAX* és la sigla de *worldwide interoperability microwave access*.

Està basada en els estàndards 802.16 (WMAN), desenvolupats per l'IEEE i per HiperMAN de l'ETSI. Permet la connectivitat entre punts fixos, nòmades i mòbils, i eventualment la connectivitat mòbil sense la necessitat de tenir una línia punt a punt amb una estació base.

La norma IEEE 802.16, publicada el desembre de 2001, va servir per a fomentar l'operativitat entre els sistemes LMDS[101]. Inicialment el rang de freqüències era entre 10 i 66 GHz amb necessitat de visió directa. Al començament de 2003, amb l'aparició del 802.16a, es va ampliar el rang de freqüències camp a les bandes de 2 a 11 GHz. L'any 2004 apareix l'estàndard 802.16-2004, també conegut com a WiMAX.

(101) *LMDS* és la sigla de *local multipoint distribution system*.

El WiMAX Forum és una agrupació de més de 350 companyies, i s'encarrega de promoure la interoperatibilitat de dispositius 802.16 i la unificació dels estàndards a tot el món.

	802.16	802.16a	802.16e
Espectre	10-66 GHz	< 11 GHz	< 6 GHz
Funcionament	Solament amb visió directa	Sense visió directa (NLOS)	Sense visió directa (NLOS)
Amplada de banda	32-134 Mbps amb canals de 28 MHz	Fins a 75 MHz amb canals de 20 MHz	Fins a 15 Mbps amb canals de 5 MHz
Modulació	QPSK, 16 QAM i 64 QAM	OFDM amb 256 subportadores QPSK, 16 QAM, 64 QAM	El mateix que 802.16a
Mobilitat	Sistema fix	Sistema fix	Mobilitat pedestre
Amplada de l'espectre	20, 25 i 28 MHz	Selecció entre 1,25 i 20 MHz	El mateix que 802.16a amb els canals de pujada per a estalviar potència
Distància	2-5 km aproximadament	5-50 km aproximadament	2-5 km aproximadament

Les seves principals característiques es resumeixen a continuació:

- Modulació adaptativa: es trien dinàmicament en funció de les condicions de l'enllaç; si aquest té un bon comportament (poques pèrdues), s'utilitza una modulació que porta més bits i, per tant, la velocitat augmenta.

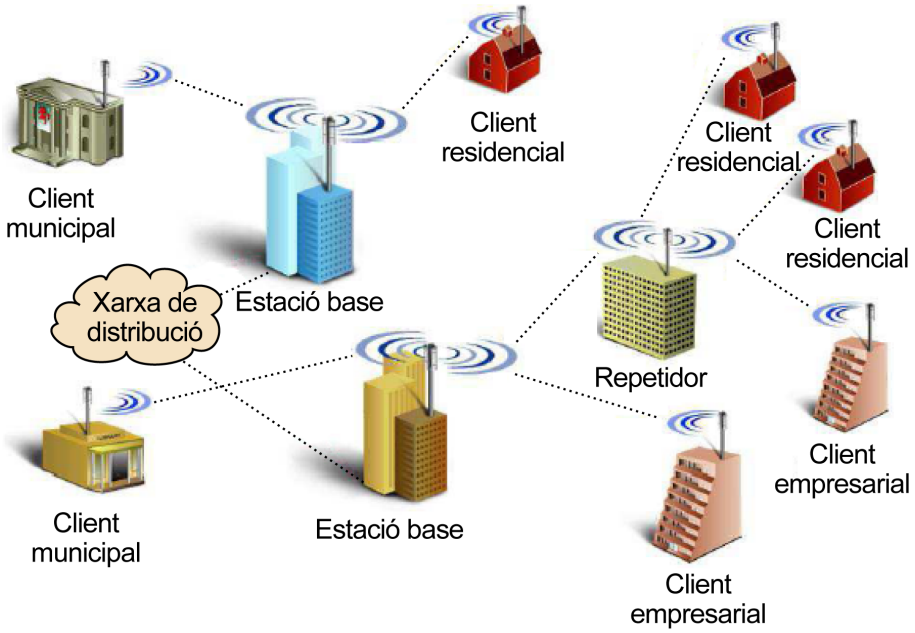
- Banda freqüencial: es pot treballar en banda lliure de 5,4 GHz, però amb poca potència i amb visió directa. També hi ha banda llicenciada a 3,5 GHz en què no és imprescindible la visió directa.

- Elements: hi ha dos tipus de components, l'estació base (unitats d'accés AU) i les unitats d'abonat (SU).

- Perfils: permeten enllaços punt a punt (amb visió directa) i punt multipunt (sense necessitat de visió directa).

- Permet qualitat de servei (QoS): gràcies al fet de que WiMAX està orientat a la connexió.

Figura 69. Topologia de la xarxa WiMAX



Pre-WiMAX

Cal fer esment de l'aparició d'equipament anomenat **pre-WiMAX**. Molts fabricants no van esperar a l'aprovació definitiva de l'estàndard 802.16, i van treure al mercat (i a hores d'ara encara n'hi ha) equips que implementen un protocol de propietat basat en els desenvolupaments fets per a la tecnologia WiMAX. Aquests dispositius, tot i proporcionar altes prestacions, no permeten interoperabilitat amb els altres fabricants. Per contra, aquests equips treballen en bandes de freqüència lliure (sense llicència), de manera que han acabat essent una bona opció (i força utilitzada) per a desplegaments en aquest tipus d'entorns.

Pel que fa a velocitats, cal diferenciar entre la velocitat de transmissió en l'aire i la velocitat real (coneguda com a *throughput*). En el cas concret de WiMAX i pre-WiMAX la velocitat dels equips és lleugerament diferent:

Velocitats pre-WiMAX / WiMAX		
Tecnologia	**Velocitat màxima aire**	**Velocitat màxima real**
pre-WiMAX	54 Mbps	~30 Mbps
WiMAX	70 Mbps	~40 Mbps

Resum

En aquest mòdul didàctic s'han abordat les característiques i funcionalitats principals del nivell d'enllaç, com la gestió de trames, la gestió de l'enllaç, el control de flux i el control d'errors. Són una sèrie de funcionalitats que transformen un medi físic no perfecte i amb errors en un medi que ofereix un servei fiable als protocols de nivell de xarxa. Hem vist que normalment aquestes funcionalitats són fetes per uns dispositius d'enllaç, anomenats *targetes de xarxa*.

També hem presentat els diferents contextos en què es podia trobar el nivell d'enllaç: comunicació punt a punt entre dos computadors locals, entorn d'accés a xarxes WAN, context de xarxa d'àrea local (LAN) i xarxes de transport d'àrea estesa (WAN).

Precisament en l'apartat següent s'ha descrit el context de xarxa d'àrea local associat al nivell d'enllaç: els àmbits en què s'instal·len i les característiques que en defineixen el funcionament, com ara els medis de transmissió que s'utilitzen, les topologies i els protocols d'accés al medi. Des del punt de vista del medi de transmissió, hem distingit entre LAN cablades, si el medi és guiat (cable o fibra òptica), i LAN sense fils, quan el medi és l'aire.

Hem vist que les topologies tenen un paper important en el disseny i instal·lació d'una LAN: l'estrella, el bus i l'anell són les més habituals. Darrerament han aparegut els busos i els anells en estrella, és a dir, xarxes que presenten una topologia física en estrella i es comporten com si fossin busos o anells (la topologia lògica).

Com que les LAN són un medi compartit, s'ha estudiat la necessitat d'establir protocols d'accés per a decidir quina estació pot transmetre trames d'informació a cada moment. Són mecanismes flexibles, justos i fàcils d'implementar. Dels molts que s'han proposat, CSMA/CD (en les xarxes Ethernet), el pas de testimoni (en els anells) i el CSMA/CA (en les xarxes sense fils) són els més utilitzats.

Finalment, s'han descrit els estàndards aprovats que descriuen les tecnologies més utilitzades en les xarxes d'àrea local:

- Ethernet IEEE 802.3, tecnologia dominant en medis cablats.
- Wireless LAN IEEE 802.11, estàndard en medis sense fils.
- WiMAX IEEE 802.16, tecnologia sense fils per a xarxes MAN.

Bibliografia

Bertsekas, D.; Gallager, R. (1992). *Data networks* (2a. ed.). Englewood Cliffs: Prentice Hall.

Halsall, F. (1998). *Comunicaciones de datos, redes de computadoras y sistemas abiertos* (4a. ed.). Addison-Wesley.

Kurose, J. F.; Ross, K. W. (2005). *Computer networking: a top-down approach featuring the Internet.* Addison-Wesley.

Stallings, W. (2000). *Comunicaciones de datos y redes de computadores 6*. Prentice-Hall.

Tanenbaum, A. S. (2003). *Redes de computadores* (4a. ed.). Pearson.