# Administració de la xarxa

PID_00275594

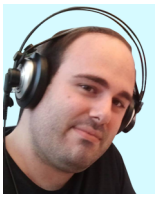
Miguel Martín Mateo
Javier Panadero Martínez
Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

**Miguel Martín Mateo**

Llicenciat en Matemàtiques per la Universitat de Barcelona (UB). Màster en Programari Lliure per la Universitat Oberta de Catalunya (UOC). Des de 2006, col·labora amb la UOC en assignatures del màster de Programari Lliure i el seu TFM, i en l'assignatura Administració de xarxes i sistemes operatius i el seu TFG. Més de vint anys d'experiència professional. Actualment, és consultor sobre l'administració de sistemes en aspectes relacionats amb l'automatització de processos i en el compliment i auditoria en entorns Windows i Unix a la multinacional Accenture. També té una àmplia experiència en el desenvolupament d'aplicacions relacionades amb caixers automàtics.

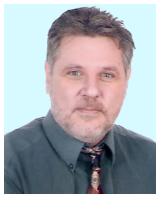


**Javier Panadero Martínez**

Enginyer informàtic i doctor en Computació d'Altes Prestacions per la Universitat Autònoma de Barcelona (UAB). Des de 2019, és professor dels Estudis d'Informàtica, Multimèdia i Telecomunicació de la Universitat Oberta de Catalunya (UOC). Director del màster universitari en Enginyeria Computacional i Matemàtica. Ha elaborat diversos materials sobre administració de sistemes i programació. Els seus interessos de recerca inclouen la computació paral·lela i distribuïda, l'optimització i simulació de sistemes complexos i els algorismes intel·ligents.

**Jordi Serra Ruiz**

Doctor en Informàtica per la Universitat Oberta de Catalunya (UOC). Enginyer superior en Informàtica per la Universitat Autònoma de Barcelona (UAB). Màster en Informàtica Industrial. Actualment, és professor de la UOC i és el director acadèmic del màster de Seguretat Informàtica de la UOC. Pertany al Grup de Recerca de Seguretat de la Informació KISON i és membre de l'IEEE.



**Miquel Colobran Huguet**

Doctor en Informàtica per la Universitat Autònoma de Barcelona (UAB). Consultor a la Universitat Oberta de Catalunya (UOC) d'assignatures sobre administració de sistemes i seguretat, i també d'informàtica i legislació en el grau i màster d'Informàtica i Multimèdia. Ha elaborat diversos materials i llibres sobre administració de sistemes, seguretat, informàtica forense i legislació aplicada a les tecnologies de la informació. La seva recerca s'emmarca dins de la seguretat, la influència de les TIC a la societat i l'enginyeria del coneixement.

**Josep Maria Arqués Soldevila**

Llicenciat en Informàtica per la Universitat Autònoma de Barcelona (UAB). Va fer el treball de recerca al Departament d'Enginyeria de la Informació i de les Comunicacions (DEIC) de l'esmentada universitat. Ha treballat com a professor ajudant i associat al DEIC, i ha exercit de consultor de diverses assignatures de la Universitat Oberta de Catalunya (UOC). Actualment, exerceix d'analista en informàtica forense.

**Eduard Marco Galindo**

Enginyer superior informàtic per la Universitat Politècnica de Catalunya (UPC). Des de 2003, col·labora amb la Universitat Oberta de Catalunya (UOC) com a tutor i professor col·laborador en el grau d'Informàtica i en el màster de Seguretat. Especialitzat en l'àmbit de l'Administració de Sistemes, ha format part de l'equip de redacció del temari de l'assignatura Administració de xarxes i sistemes operatius (AXSO) i ha exercit de consultor i tribunal en el seu TFG. En l'àmbit professional, treballa des de fa més de vint anys en el món dels sistemes informàtics, especialment en la capa *middleware* d'empreses i governs. Especialitzat en l'arquitectura de sistemes en l'àmbit empresarial, i també en la gestió d'equips de projecte i de serveis gestionats. Darrerament, iniciant una nova etapa professional i de recerca en projectes d'intel·ligència artificial en l'àmbit empresarial, forma part de l'equip tècnic de disseny i implementació de solucions.


Primera edició: setembre 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Miguel Martín Mateo, Javier Panadero Martínez, Jordi Serra Ruiz, Miquel Colobran Huguet, Josep Maria Arqués Soldevila, Eduard Marco Galindo
Producció: FUOC

# Índex

# Introducció

A l'hora de dissenyar i implementar una xarxa, s'han de tenir en compte els sis passos bàsics següents:

**1)** Selecció del disseny del cablejat i del maquinari.
**2)** Instal·lació del maquinari i del sistema operatiu de la xarxa.
**3)** Configuració del sistema operatiu i càrrega de les aplicacions.
**4)** Creació de l'entorn d'usuari.
**5)** Inicialització de l'administració de la xarxa.
**6)** Manteniment i monitorització de l'activitat de la xarxa.

**Vegeu també**

Vegeu el mòdul «Administració d'usuaris».

En aquest mòdul es pretén abastar, breument, diversos aspectes del disseny i el desenvolupament posterior d'una xarxa d'ordinadors. Així doncs, el mòdul comença amb la descripció dels elements que la integren i acaba definint, a grans trets, els passos que cal seguir per connectar una estació de treball a la xarxa. No es pretén fer un recull exhaustiu d'una matèria tan densa i heterogènia, sinó solament dotar l'administrador d'alguns criteris generals que el puguin ajudar a l'hora de començar (i mantenir) una tasca tan complexa com la que hem descrit.

# Objectius

Els materials didàctics d'aquest mòdul contenen les eines necessàries perquè l'estudiant assoleixi els objectius següents:

**1.** Poder descriure bàsicament els elements físics d'una xarxa d'ordinadors i conèixer la manera com interconnectar aquests elements entre si. A partir d'aquesta descripció podem veure que, segons les necessitats, trobarem dispositius i topologies adients als serveis que ha d'oferir la xarxa.

**2.** Conèixer els protocols de comunicació que han d'utilitzar els ordinadors de la xarxa i també la manera com es configuren les estacions i alguns serveis. En general, veurem que les accions que s'han de dur a terme són similars, amb independència de l'arquitectura i del sistema operatiu de la xarxa.

**3.** Descriure les tasques que ha de dur a terme l'administrador una vegada la xarxa ja està en funcionament (tasques de manteniment, supervisió i seguretat).

# 1. Introducció a l'administració de la xarxa

Els ordinadors personals permeten als usuaris individuals gestionar les seves pròpies dades per cobrir les necessitats particulars. Malgrat tot, els ordinadors aïllats no poden oferir un accés directe a les diferents dades d'una organització, ni poden compartir d'una manera fàcil la informació o els programes de què disposen. En aquest sentit, les xarxes proporcionen una bona solució de compromís entre els dos extrems: el processament individual i el processament centralitzat.

Entre els molts beneficis que comporta la implementació d'una xarxa, podem trobar els següents:

- **Compartició de dispositius perifèrics**: els usuaris de l'organització han de poder tenir accés als recursos compartits com ara discs durs de gran capacitat, dispositius de sortida de cost elevat (com, per exemple, impressores làser o traçadors –*plotters*–, etc.), o qualsevol altre dispositiu.

- **Comunicació entre els usuaris de l'organització**: els usuaris de l'organització s'han de poder comunicar entre ells, sigui per correu electrònic, videotrucades, xats corporatius, o qualsevol altre eina, per poder desenvolupar correctament la seva feina.

- **Facilitat de manteniment del programari**: sovint una bona part del programari es comparteix des de la xarxa, en lloc d'instal·lar-se individualment a cada estació de treball.

- **Gestió centralitzada dels recursos compartits**: és molt importat per al bon funcionament de l'organització poder compartir els seus recursos (eines, dades, servidors, etc.), independentment del grau de dispersió geogràfica que pugui tenir l'organització. Moltes vegades una organització té seus a diferents ciutats o, fins i tot, països. Tot i així, els recursos han de ser accessibles a totes les seus de l'organització.

Segons aquesta dispersió geogràfica, les xarxes es poden classificar de la manera següent:

- **LAN (*local area network* o xarxes d'àrea local)**: és una xarxa que connecta els ordinadors d'un àrea relativament petita i predeterminada amb unes dimensions de 10 a 1.000 m (per exemple, una sala de l'organització, un campus, etc.).

- **MAN (*metropolitan area network*)**: és aquella àrea que, mitjançant una connexió d'alta velocitat, ofereix cobertura en una zona geogràfica extensa d'1 a 10 km (per exemple, una ciutat).

- **WAN (*wide area network*)**: són les que permeten la interconnexió entre ciutats, països i continents i són les que donen connexions entre localitzacions a més de 10 km (per exemple, un país).

Tenint en compte la importància que té una xarxa en l'activitat diària de qualsevol organització, es fa evident la necessitat d'una figura que s'encarregui de dissenyar-la, implementar-la, mantenir-la i actualitzar-la sempre que calgui. Aquesta figura és l'administrador de la xarxa, el qual ha de conèixer els elements físics que la componen, els protocols de comunicació entre els diferents ordinadors (i els seus sistemes operatius), i també els requeriments mínims de seguretat que ha de satisfer la xarxa.

# 2. Elements i disseny físic d'una xarxa

A l'hora de dissenyar la nostra pròpia xarxa cal que, abans de començar, tinguem en compte una sèrie d'aspectes bàsics que podem veure reflectits tot seguit en les preguntes següents:

- Quants ordinadors (estacions de treball) hem de connectar a la xarxa?
- Quants ordinadors caldrà afegir en futures ampliacions?
- On i com es disposen els ordinadors? (Cal fer un croquis de la disposició de les màquines).
- Necessitem un servidor?
- Quina velocitat de transmissió es requereix?
- Quins recursos cal compartir?
- Quin programari voldrem instal·lar? En tenim les versions per funcionar en xarxa?

Abans de començar a contestar aquestes preguntes, ens caldrà fer un breu repàs de diversos conceptes que han aparegut en altres assignatures de xarxes d'ordinadors.

## 2.1. Elements d'una xarxa

Els elements bàsics d'una xarxa són el cablejat, els elements de connexió i els elements d'interconnexió de les xarxes.

### 2.1.1. Cablejat d'una xarxa

Podem distingir els tipus de cables següents:

**1) Parell trenat**: aquest tipus de cablejat està format per diversos fils conductors que es trenen entre si amb la finalitat de protegir-los del soroll ambiental. És el cablejat més econòmic i fàcil d'instal·lar. Poden arribar a distàncies de fins a 100 m (sense patir esmorteïments del senyal) i a velocitats que poden variar entre els 10 i els 100 MBps.

Hi ha diverses categories de cable parell trenat:

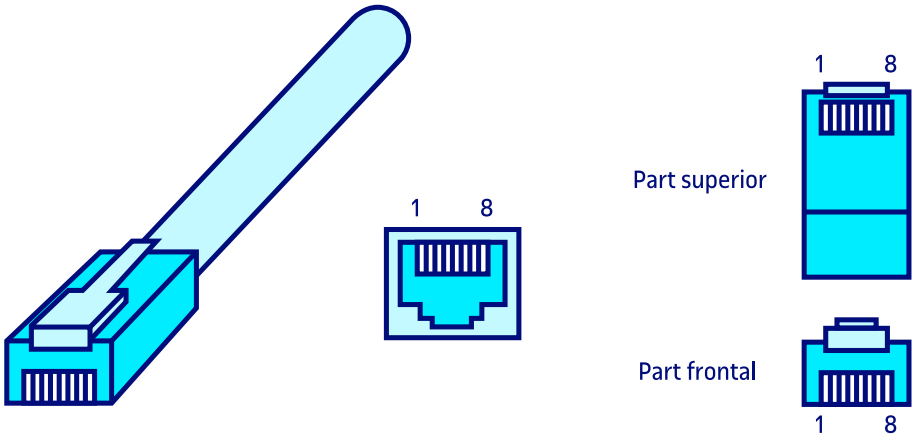
- **STP (*shielded twisted pair*)**: cable apantallat, format per dos parells de fils conductors recoberts per una malla.

- **UTP (*unshielded twisted pair*)**: cable sense apantallar, format per quatre parells de fils conductors. La figura 1 mostra l'aspecte d'un parell trenat UTP (el connector femella i el connector mascle, respectivament). Al mateix temps, els cables UTP es poden subdividir en diverses categories segons la seva velocitat de transmissió:
  - **Categoria 3**: poden arribar a velocitats de transmissió de 30 MBps.
  - **Categoria 5**: és el tipus de cable que s'utilitza més sovint. Pot arribar a velocitats de 100 MBps (xarxes Fast Ethernet). La categoria 5a (també anomenada 5+ o 5e) representa una millora de la categoria 5 i pot arribar fins a 1.000 MBps (xarxes Gigabit Ethernet).
  - **Categoria 6**: pot arribar a velocitats de 1.000 MBps.

**Categories UTP**

També hi ha les categories 6e i 7 i s'usaran en el futur per a xarxes de 10 Gigabit Ethernet (10.000 MBps).

Figura 1. Aspecte d'un cable UTP




Per exemple, connectant tots els ordinadors a un concentrador mitjançant un parell trenat i sense necessitat d'utilitzar un servidor dedicat, podem dissenyar una xarxa molt senzilla, perfectament vàlida per compartir recursos, i que es pot ampliar fàcilment fins a ocupar tots els ports del concentrador.

**Punt a punt**

S'anomenen punt a punt (*peer-to-peer*) les xarxes en què no hi ha un servidor dedicat. Totes les estacions de treball tenen el mateix estatus i comparteixen els recursos.

***Crossover***

Quan s'utilitza un concentrador, els dos extrems del cable (el que es connecta al concentrador i el que es connecta a la targeta de xarxa de l'ordinador) s'insereixen en el connector RJ45 de la mateixa manera, però quan els dos extrems es connecten directament entre dos ordinadors, cal fer el que s'anomena un cable creuat (*crossover*) i intercanviar l'ordre dels cables que transmeten les dades.

**2) Cable coaxial**: el cable coaxial disposa d'un únic conductor intern i diverses capes de protecció. N'hi ha de gruixut i de prim (RG-58A/U), i en distàncies no superiors als 2 km, pot permetre velocitats de transmissió de 20 MBps, mentre que en distàncies curtes (no superiors als 100 m) pot arribar als 100 MBps. El cable coaxial, si es compara amb el parell trenat, redueix els problemes d'esmorteïment del senyal a llargues distàncies i el percentatge de potèn-

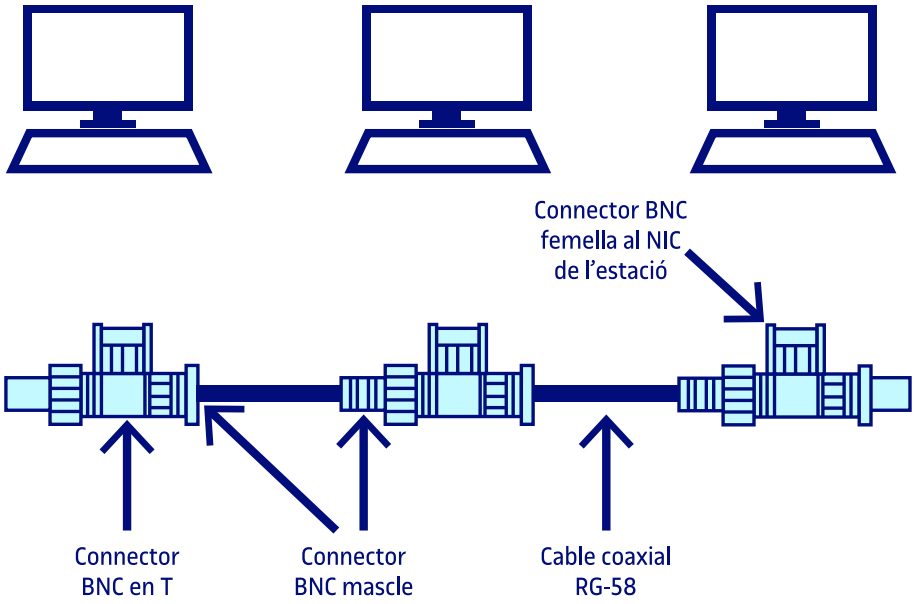
**Vegeu també**

Vegeu el mòdul «Administració de la seguretat».

cia que es perd en forma de radiació. És molt sensible a les accions de possibles espies i és susceptible al soroll produït pels aparells elèctrics (per exemple, un motor).

Per connectar diferents segments de cable coaxial s'utilitzen connectors BNC, mentre que per connectar un ordinador a la xarxa s'utilitzen connectors BNC en forma de T, com es pot veure a la figura 2.

Figura 2. Connexió d'un ordinador a la xarxa amb cable coaxial




**3) Fibra òptica**: la transmissió de la informació es duu a terme per un feix de llum que circula per un nucli fotoconductor. Permet una gran amplada de banda i pot arribar a velocitats de transmissió de l'ordre de centenars d'MBps o, fins i tot, GBps. La fibra òptica pateix un esmorteïment mínim del senyal, és immune a les interferències electromagnètiques i resulta difícil d'interceptar i espiar, ja que no emet cap senyal que pugui ser monitoritzat. Normalment s'utilitza conjuntament amb altres tipus de cablejat. Hi ha dos tipus diferents de fibra òptica, les monomode i les multimode. Les primeres es caracteritzen perquè només admeten un únic mode de transport (només poden transmetre els feixos de llum que segueixen l'eix de la fibra). Tenen una amplada de banda que pot arribar als 100 GHz/km. Pel que fa a les fibres multimode, amb un diàmetre de nucli més gran que les monomode, transporten múltiples modes de forma simultània. Són més fàcils d'implantar i tenen una amplada de banda que pot arribar fins als 500 MHz/km (menor que les monomode). Per exemple, poden ser especialment adequades per a sistemes de videovigilància o LAN.

### 2.1.2. Elements de connexió de xarxes

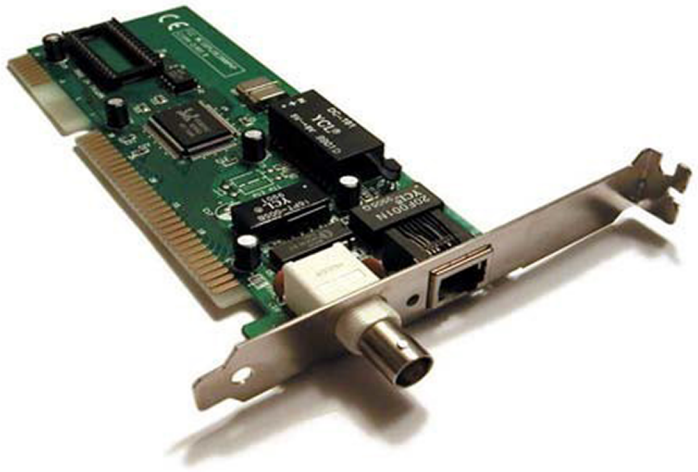
Entre els elements de connexió de xarxes podem distingir els següents:

**1) Targetes d'interfície de xarxa** (NIC, ***network interface card***): la connexió dels ordinadors a la xarxa es fa mitjançant les targetes d'interfície de xarxa. Podem veure a la figura 3 l'aspecte d'un NIC.

**Targetes d'interfície de xarxa**

Normalment, trobem aquestes targetes en format PCI o PCMCIA, en el cas d'ordinadors portàtils. Cada vegada hi ha més equips portàtils i de sobretaula amb una targeta integrada a la placa base. Alguns PDA disposen d'un NIC per connectar-se a una xarxa local sense fil.

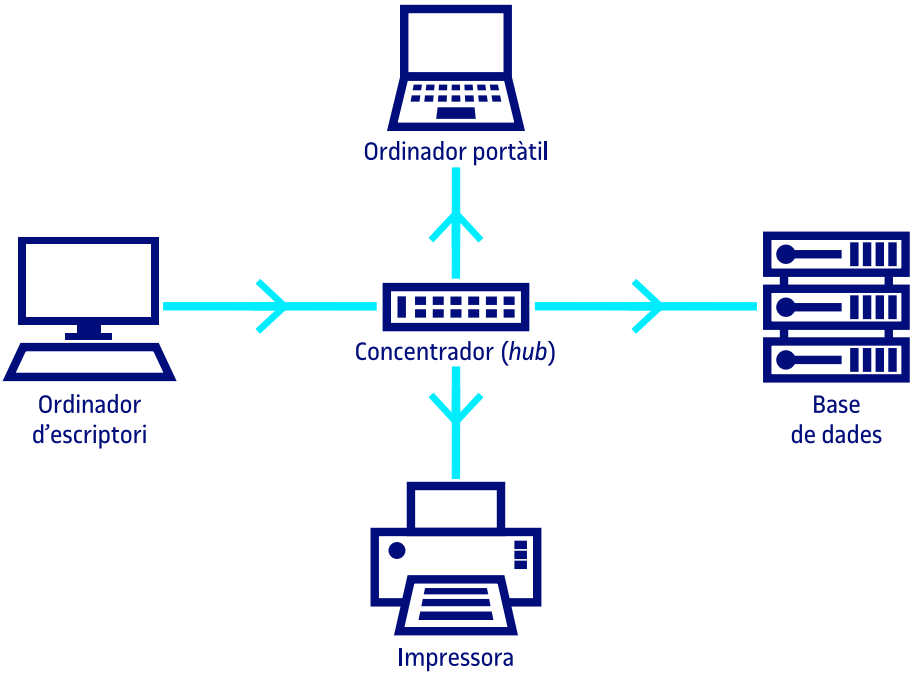
Figura 3. Targeta d'interfície de xarxa



**2) Tallafoc (*firewall*)**: qualsevol dispositiu (maquinari o programari) que permeti evitar que els usuaris no autoritzats accedeixin a una màquina determinada.

**3) Concentrador (*hub*)**: tal com es mostra a la figura 4, són dispositius que permeten compartir una línia de comunicació entre diversos ordinadors. Distribueixen tota la informació que reben de manera que la puguin rebre tots els dispositius connectats als seus ports.

Figura 4. Exemple de configuració d'un concentrador



**Amplada de banda**

Totes les estacions connectades al mateix concentrador o *stack* de concentradors competeixen per l'amplada de banda del canal.

**4) Commutador (*switch*)**: gestiona el flux del trànsit de la xarxa segons l'adreça de destinació de cada paquet. En altres paraules, els commutadors poden esbrinar quins dispositius estan connectats als seus ports i redirigeixen la informació únicament al port de destinació, en lloc de fer-ho indiscriminadament com els concentradors.

**5) Xarxa troncal (*backbone*)**: s'anomenen d'aquesta manera els cables principals que connecten entre si els segments d'una xarxa local. Habitualment són enllaços d'alta velocitat (per exemple, la fibra òptica).

**6) Armaris de connexió**: generalment la xarxa es divideix en diferents armaris de connexió que abasten tot el servei de la xarxa en un entorn determinat com, per exemple, tota la planta d'un edifici. Tots aquests armaris tenen una connexió a un armari central en què, normalment, hi ha agrupades totes les comunicacions i hi ha instal·lats els diferents servidors. Acostuma a ser una sala amb condicionament atmosfèric adequat, tant pel que fa a la temperatura com a la humitat, i normalment disposa d'alimentació elèctrica ininterrompuda.

**7) Servidor**: és l'ordinador que permet compartir els seus perifèrics amb altres estacions de la xarxa. N'hi ha de molts tipus diferents i es poden agrupar en tres categories generals: servidors d'impressió, de comunicacions i de fitxers. Dins d'una xarxa, poden estar dedicats exclusivament a donar aquests serveis, o també poden no ser exclusius i utilitzar-se com a estacions de treball.

**8) Estació de treball**: cada estació de treball executa el seu sistema operatiu propi (Unix, Linux, Windows 2000, etc.) i en aquest sistema operatiu s'executa un programari de xarxa que li permet comunicar-se amb els servidors i els altres dispositius de la xarxa, de manera que és tan senzill gestionar els recursos locals com els del servidor.

### 2.1.3. Elements d'interconnexió de les xarxes

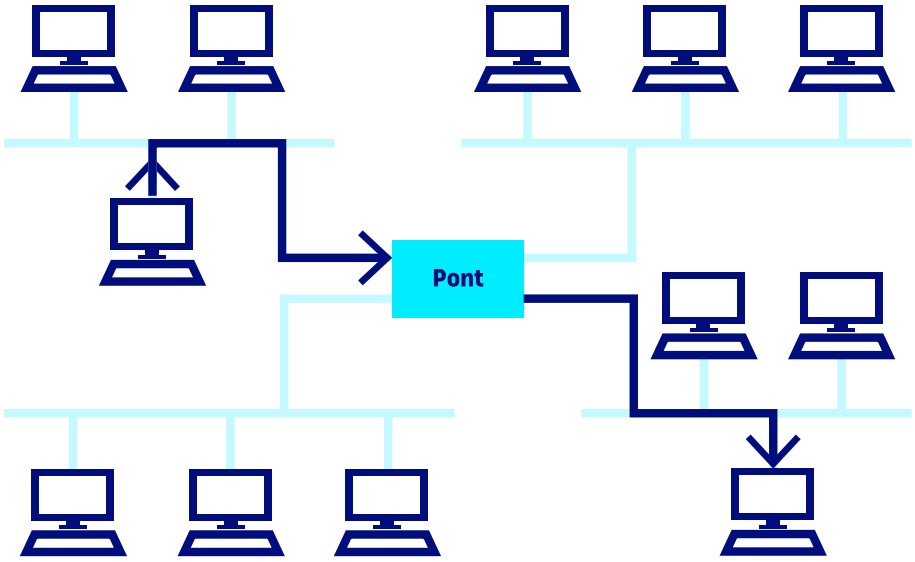
Podem distinguir quatre tipus diferents d'elements d'interconnexió:

**1) Repetidors**: són dispositius «no intel·ligents» que amplifiquen el senyal i eviten els problemes d'esmorteïment que es produeixen quan el cable arriba a una certa distància (recordem que, segons el cablejat que es faci servir, aquestes distàncies varien). Actuen en el que s'anomena capa física.

**2) Pont (*bridge*)**: connecten entre si dos segments de la xarxa (que poden ser diferents –vegeu l'exemple de la figura 5–) i actuen en la capa d'enllaç de les dades. A diferència del repetidor, el pont és prou «intel·ligent» per filtrar el trànsit d'informació entre els segments, té capacitat d'autoaprenentatge, fil-

tració i reenviament de la informació que passa a través d'ell. Amb la incorporació d'un pont, cada segment té una adreça IP diferent, de manera que la informació sempre s'encamina cap a la seva destinació i s'eviten els colls d'ampolla que es produeixen quan totes les estacions de treball es connecten al mateix segment.

Figura 5. Interconnexió de xarxes mitjançant un pont




**3) Encaminador (*router*)**: són dispositius que gestionen el trànsit de paquets que prové de l'exterior de la xarxa cap a l'interior (i a l'inrevés). Poden ser dispositius molt sofisticats i tenen capacitat d'actuar com a tallafoc. Són similars als ponts, però en canvi ofereixen serveis d'encaminament de les dades que es transmeten; és a dir, no solament poden filtrar la informació, sinó que, a més, també poden trobar la ruta de destinació més eficient per als paquets d'informació que es transmeten.

**4) Passarel·la (*gateway*)**: actuen en els nivells superiors de la jerarquia de protocols OSI. Permeten la interconnexió de xarxes que fan servir protocols incompatibles.

## 2.2. Topologia i tipus de xarxes

La topologia de la xarxa es refereix al camí físic que segueixen les dades per la xarxa, és a dir, la manera lògica com es connecten els diferents dispositius que la formen. Sovint, cal diferenciar entre la **topologia lògica** i la **topografia** o **disseny físic** (la manera com es «tiren» els cables).

Bàsicament, hi ha tres topologies que cal tenir en compte en una xarxa LAN:

**Topologia lògica**

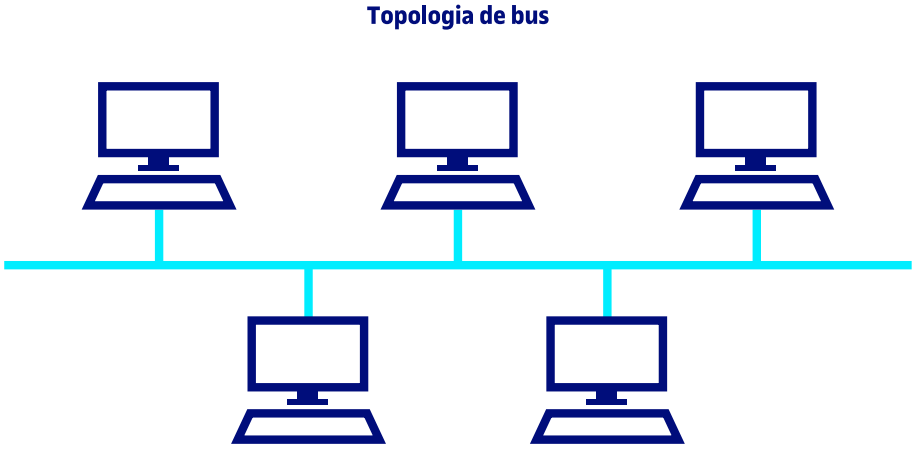
La topologia lògica pot ser diferent de la topografia, com veurem en els exemples que s'estudiaran més endavant.

**1) Topologia de bus**: en una xarxa en bus, tots els nodes (els servidors i les estacions de treball) es connecten a un cable comú (bus), com es pot veure a la figura 6. Els trets més característics d'aquesta topologia són els següents:

- Els nodes no retransmeten ni amplifiquen la informació.
- El temps de retenció de la informació als nodes és nul.
- Tots els missatges arriben a tots els nodes.
- No cal cap encaminament de la informació.
- La fiabilitat de la comunicació depèn únicament del bus (punt crític).
- La configuració és flexible i modular.
- És una tecnologia de baix cost que encara es fa servir freqüentment.
- Ofereix facilitat per interceptar la informació circulant.

L'existència d'un únic bus fa que l'excés de trànsit pugui provocar una disminució important del rendiment de la xarxa. Per controlar el trànsit de la xarxa, es poden fer servir commutadors que siguin capaços de discriminar el trànsit circulant.

Figura 6. Xarxa amb topologia de bus




**2) Topologia en anell**: en una xarxa en anell el cable va d'estació a estació (i al servidor) sense cap punt final. Cada node té connexions amb dues estacions més. Aquest tipus de xarxa es pot veure a la figura 7. Els trets més característics d'aquesta topologia són els següents:

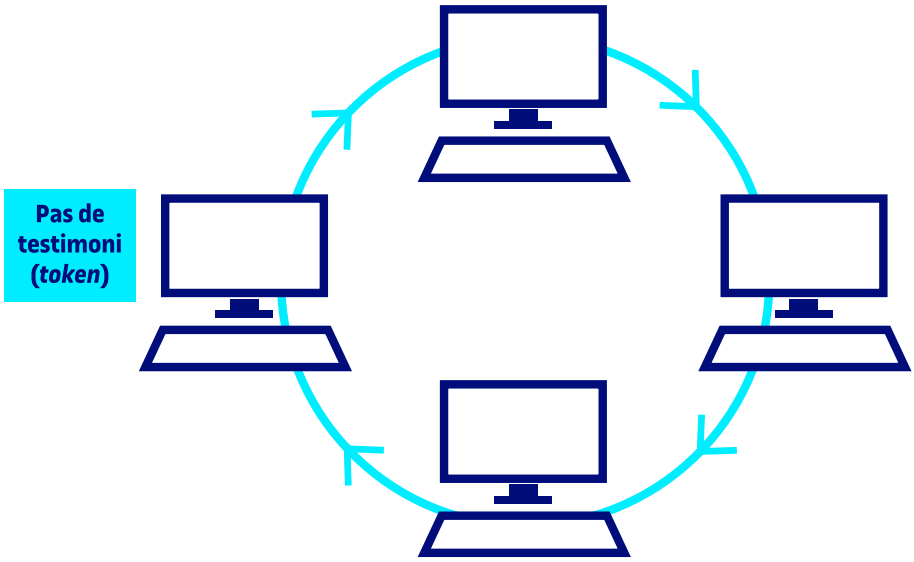
- Cada node amplifica i distribueix la informació que rep.

- Els missatges viatgen per l'anell node a node, de manera que totes les informacions passen per tots els mòduls de comunicació de les estacions (facilitat per interceptar la informació).

- No cal dirigir l'encaminament de la informació.

- La fiabilitat de l'anell depèn de cadascun dels nodes i de la via de comunicació que forma l'anell. La caiguda d'una sola estació podria provocar que la xarxa sencera deixés de funcionar.

Figura 7. Xarxa amb topologia d'anell



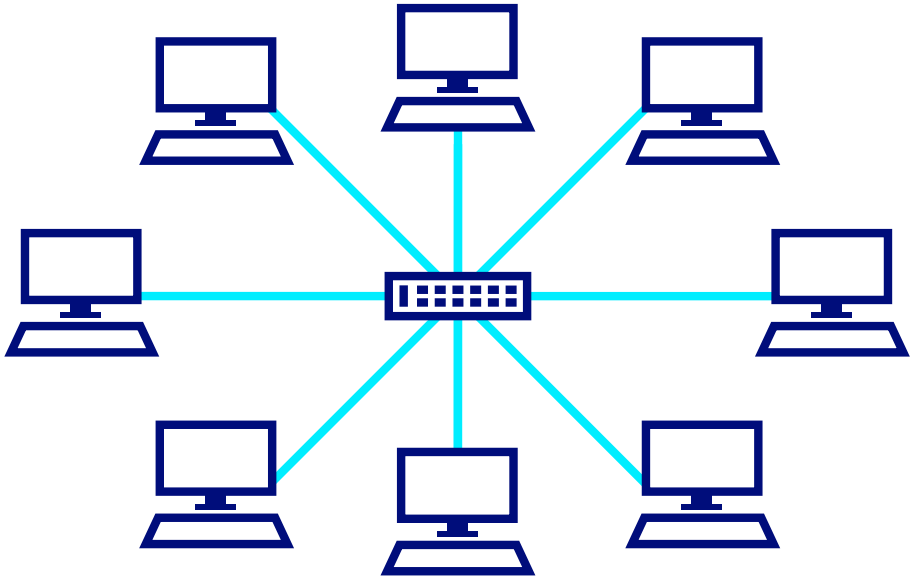

**3) Topologia en estrella**: en aquest cas, tal com mostra la figura 8, totes les estacions de treball i el servidor es connecten a un sol concentrador o commutador. Observem que l'element diferenciador més important respecte a les altres topologies és la centralització de les connexions. Aquest fet la converteix en una topologia especialment resistent a la caiguda de les estacions de treball, tot i que com a principal defecte ens ofereix un punt crític, l'element central, el qual si és atacat o cau per qualsevol motiu, pot provocar la caiguda de la xarxa sencera. Els trets més característics d'aquesta topologia són els següents:

- Totes les estacions es comuniquen entre si mitjançant un node central.
- El dispositiu central pot ser actiu o passiu.
- Les fallades tenen una repercussió molt diferent segons on es produeixen.

**Manteniment de la xarxa**

«Documentar» el disseny i els components que formen part de la xarxa ajuda a les futures tasques de manteniment.

Figura 8. Xarxa amb topologia d'estrella



A l'hora de triar una topologia de xarxa, s'han de tenir en compte els aspectes següents:

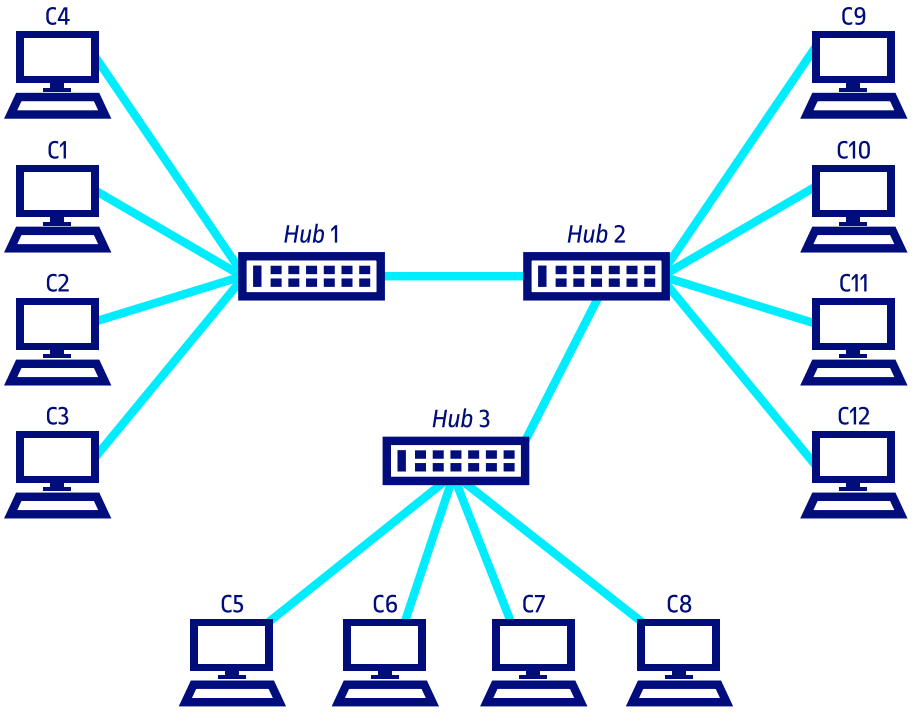
- Distància màxima que es pot obtenir.
- Nombre màxim d'estacions.
- Flexibilitat a l'hora d'afegir o eliminar estacions de treball.
- Tolerància a caigudes de les estacions.
- Retard dels missatges.
- Cost.
- Flux d'informació que pot circular per la xarxa.

**Col·locació dels cables**

Encara que físicament no es deixin connectats, és aconsellable tenir els cables tirats pels canals amb un 10 % més del que es preveu fer servir.

Les topologies de bus i d'anell són les més utilitzades en xarxes locals, tot i que per motius de flexibilitat, fiabilitat i seguretat, el disseny físic en estrella també ha esdevingut molt popular amb xarxes que, lògicament, poden funcionar en bus o anell, però que tenen una topologia física d'estrella.

Figura 9. Disseny físic basat en concentradors




Tal com es pot observar a la figura 9, en el concentrador es barregen tots els senyals de totes les estacions i es transmeten a totes com si es tractés d'una configuració en bus, malgrat que això genera un alt trànsit, característic de les xarxes tipus bus, els costos i la «dificultat» de manteniment són reduïts.

### 2.3. Tipus de xarxes locals

L'Institute of Electrical and Electronic Engineers (IEEE) és un organisme que data de l'any 1980 i que va elaborar les **normes IEEE 802.x**, les quals defineixen els estàndards pel que fa al funcionament de les xarxes d'àrea local.

Les normes IEEE 802.x defineixen els estàndards pel que fa al funcionament de les xarxes d'àrea local. A continuació, es descriuen els estàndards més utilitzats:

- **IEEE 802.3**: estàndard basat en la versió 2.0 de la xarxa Ethernet. Defineix una xarxa amb topologia de bus i mètode d'accés CSMA/CD (totes les estacions poden accedir simultàniament al medi i competeixen per la utilització del canal de comunicació). El seu camp d'aplicació és en entorns tècnics i oficines, universitats i hospitals.

- **IEEE 802.4**: defineix una xarxa amb topologia de bus i pas de testimoni (*token*). Solament pot accedir a la utilització del canal l'estació en possessió del testimoni. S'utilitza en entorns industrials i es coneix amb el nom de Token-bus.

- **IEEE 802.5**: estàndard basat en la xarxa Token Ring d'IBM. Defineix una xarxa amb topologia d'anell i pas de testimoni. Ha esdevingut popular en entorns d'oficines, amb un nivell d'implantació similar a les xarxes Ethernet.

- **IEEE 802.15**: defineix les xarxes d'àrea personal sense fill, utilitzades en la interconnexió de dispositius personals. És el que coneixem com a Bluetooth.

- **IEEE 802.16**: defineix les xarxes d'accés sense fil de banda ampla coneguda com a WiMAX, i que tenen com a objectiu l'accés a la xarxa des de casa sense fil.

De tots els estàndards que acabem d'esmentar, possiblement les **xarxes Ethernet** són les que han tingut més popularitat.

**Com fer un canvi tecnològic important**

Si s'ha de fer un canvi tecnològic important (per exemple, passar d'Ethernet de 10 MB a 100 MB 1 GB), s'hauria d'analitzar si és millor fer-ho d'una manera gradual o canviar de cop i interrompre tots els serveis durant el temps que faci falta.

La major part de les implementacions de xarxes Ethernet tenen velocitats de transmissió de 10 MBps. A continuació, es detallen els diferents **tipus segons el cablejat** que s'utilitzi (el primer nombre fa referència a la velocitat en MBps i el segon als metres que pot tenir el segment –multiplicat per cent–, sense que el senyal pateixi esmorteïments):

- **1Base-5**: cable de parell trenat amb una velocitat de transmissió d'1 MBps i una longitud màxima de segment de cinc-cents metres.

- **10Base-T**: cable de parell trenat UTP amb una longitud màxima de segment de cent metres en una topologia física d'estrella.

- **100Base-T**: semblant a l'anterior, però amb velocitats de transmissió de 100 MBps (anomenada també Fast Ethernet).

- **10Base-5 (*thick wire*)**: cable coaxial gruixut amb una velocitat de transmissió de 10 MBps. Accepta fins a cent llocs de treball en segments de longitud de com a molt cinc-cents metres.

- **10Base-2 (*thin wire*)**: cable coaxial prim amb una velocitat de transmissió de 10 MBps. Accepta fins a trenta llocs de treball en segments de longitud de com a molt cent vuitanta-cinc metres.

- **10Base-F**: fibra òptica amb velocitats de transmissió de 10 MBps.

### 2.3.1. Xarxes locals sense fil (WLAN: *wireless local area network*)

A l'hora de triar un tipus de xarxa, també val la pena considerar altres opcions diferents dels tipus que hem estudiat fins ara. Per exemple, en tots els tipus examinats hem pogut copsar els problemes següents:

- Dificultat, o fins i tot impossibilitat, per fer arribar el cablejat quan el lloc és físicament de difícil accés.

- Necessitat de fer una estimació de creixement de la xarxa i desenvolupar més infraestructura de la que es necessita en un principi per poder preveure aquest creixement en el futur.

- En tots els casos cal fer forats a les parets o al terra per tirar el cablejat necessari.

Per poder resoldre aquest tipus de problemes, han aparegut les anomenades WLAN (*wireless local area network*), és a dir, xarxes locals sense fil basades en ones de ràdio o infraroges. L'objectiu primordial en aquestes xarxes és la comoditat de l'usuari final (o sigui, la possibilitat de connectar-se a la xarxa des de qualsevol lloc de l'organització i en qualsevol moment), i la facilitat d'implementació i creixement de la xarxa (sense oblidar que aspectes com ara la fiabilitat i l'amplada de banda també són importants).

L'IEEE ha definit la norma 802.11 (i posteriors) per regular el funcionament de les xarxes sense fil. La més estesa és la norma 802.11b, amb velocitats de fins a 11 MBps. Emet dins la banda de 2.4 GHz ISM (*industrial, scientific and medical*).

Podem veure les característiques principals d'aquestes normes a la taula 1.

Taula 1. Normes de xarxes wifi

| Protocol | Data de normalització | Freqüències | Velocitat (típica) | Velocitat (màxima) | Abast interior | Abast exterior |
|---|---|---|---|---|---|---|
| **Norma inicial** | 1997 | 2,4-2,5 GHz | 1 MBit/s | 2 MBit/s | ? | ? |
| **802.11a** | 1999 | 5,15-5,35 GHz<br>5,47-5,725 GHz<br>5,725-5,875 GHz | 25 MBit/s | 54 MBit/s | ~25 m | ~75 m |
| **802.11b** | 1999 | 2,4-2,5 GHz | 6,5 MBit/s | 11 MBit/s | ~35 m | ~100 m |
| **802.11g** | 2003 | 2,4-2,5 GHz | 25 MBit/s | 54 MBit/s | ~25 m | ~75 m |
| **802.11n** | 2009 | 2,4 GHz i/o 5 GHz | 200 MBit/s | 450 MBit/s | ~50 m | ~125 m |
| **802.11ad** | 2012 | 3 GBit/s | 7 GBit/s | 450 MBit/s | ~10 m | ~30 m |
| **802.11ac** | Gener 2014 | 5,15-5,35 GHz<br>5,47-5,875 GHz | 433 MBit/s | 1.300 MBit/s | ~20 m | ~50 m |

| Protocol | Data de normalització | Freqüències | Velocitat (típica) | Velocitat (màxima) | Abast interior | Abast exterior |
|---|---|---|---|---|---|---|
| **801.22af** | Febrer 2014 | Bandes de tv entre 54-790 MHz | 568,9 MBit/s | 568,9 MBit/s | | ~1.000 m |
| **802.11ax** | 2019 | 2,4 GHz i/o 5 GHz | 1.300 MBit/s | 10 GBit/s | ~50 m | ~125 m |

### 2.3.2. *Wi-Fi protected access* (WPA)

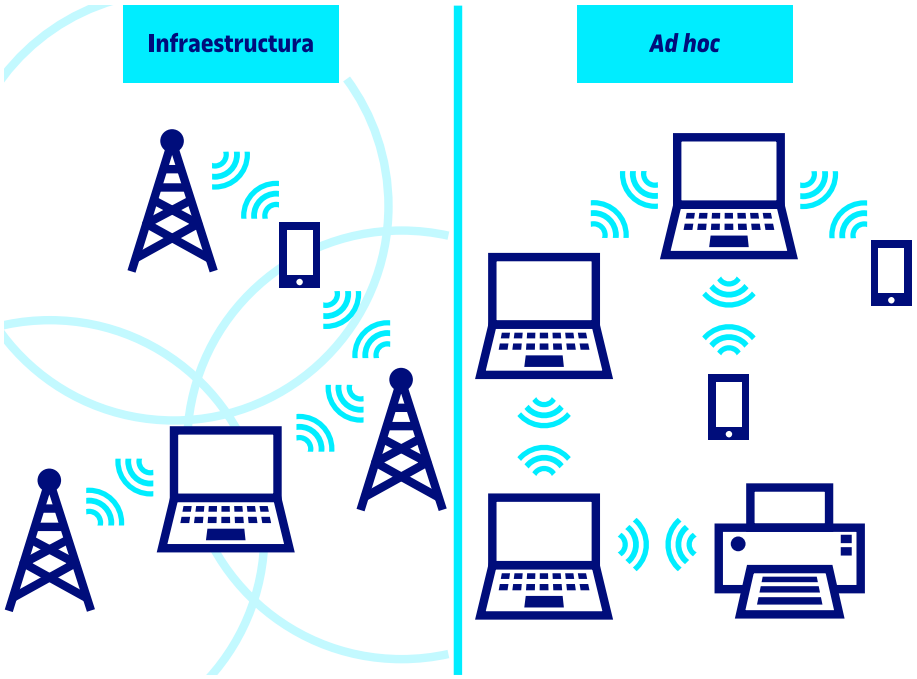
Com que la informació no necessita cap mitjà determinat per circular, aquestes xarxes presenten problemes de seguretat importants. Per exemple, en una configuració normal de xarxa, el tallafoc sol ser un element crític de la seguretat i reuneix bona part de les mesures de protecció que eviten els atacs exteriors. En una xarxa sense fils, els atacants ja no necessiten «passar» pel tallafoc i poden atacar directament altres dispositius de la xarxa. La norma 802.11 preveu la utilització del protocol WEP (*wired equivalent protocol*) per resoldre aquests problemes, però no és un mecanisme de protecció segur perquè actualment pot ser desxifrat sense gaires problemes.

Arran dels problemes de seguretat provocats pel protocol WEP, s'ha desenvolupat l'anomenat WPA (*wi-fi protected access*), el qual forma part de l'especificació 802.11i. Així doncs, en l'actualitat, ens trobarem amb **mecanismes de seguretat** com l'ús de xifrat AES, un millor protocol d'autenticació (ús del WPA) i control de la integritat del missatge (ús de la funció *hash* MIC, enlloc del CRC-32 emprat en el protocol WEP). Malgrat tot, cal tenir present que les xarxes WLAN requereixen, a causa de la seva naturalesa intrínseca, unes mesures de seguretat més grans que les que s'adoptarien en una xarxa «cablejada» normal.

### 2.3.3. Xarxes *ad hoc*

Les WLAN poden operar en mode *ad hoc* o en mode infraestructura:

Figura 10. Xarxes wifi en infraestructura i *ad hoc*




- **Mode *ad hoc* (client en front de client)**: totes les màquines que estan dins la mateixa zona d'abast es poden comunicar entre si directament. No és habitual, encara que és pràctic, per exemple, per intercanviar la informació entre dos ordinadors (seria similar a la connexió de dos ordinadors mitjançant un cable trenat). Es pot veure un exemple a la part dreta de la figura 10.

- **Mode infraestructura (client en front de punt d'accés)**: les estacions es comuniquen amb els anomenats punts d'accés, que actuen de repetidors i difonen la informació a la resta de la xarxa, com es mostra a la part esquerra de la figura 10.

Finalment, també cal tenir present la tecnologia WiMAX (*worldwide interoperability for microwave access*), estàndard (IEEE 802.16) de transmissió da dades sense fil, dissenyat per ésser utilitzat a l'àrea metropolitana, proporcionant accessos concurrents en àrees de com a molt 48 quilòmetres de radi i amb velocitats de transmissió de fins a 70 MBps. Com és evident, aquesta tecnologia permet connectar el nostre dispositiu mòbil (ordinador portàtil, PDA, etc.) a qualsevol indret i, entre altres avantatges, podria fer arribar internet a zones de difícil accés on no sigui possible instal·lar cap infraestructura. Emet dins la banda de 2 a 11 Ghz i de 10 a 60 GHz per a una comunicació entre antenes proveïdores de servei. L'algorisme de xifrat emprat és un triple DES, però es preveu l'adopció de l'algorisme AES quan comenci la seva comercialització.

**WEP**

*Wired equivalent protocol* es basa en un xifrat RC4. Cal situar una clau WEP predeterminada a cada punt d'accés i a cada client. Només aquells clients amb la mateixa clau se'ls permetrà l'accés.

**Elements portables**

És important que, per aprofitar tots els avantatges de les xarxes sense fil, les estacions de treball també puguin ser elements portables, com ara un ordinador portàtil o un PDA.

### 2.3.4. Xarxes de fibra òptica

Les **xarxes de fibra òptica** consisteixen en un fil molt fi de material transparent, vidre o materials plàstics, pel qual s'envien polsos de llum que representen les dades a transmetre. El feix de llum queda completament confinat i es propaga per l'interior de la fibra amb un angle de reflexió. La font de llum pot provenir d'un làser o un díode led. L'ús d'aquest cable és molt ampli i, en comunicacions, aquest pot transmetre una gran quantitat d'informació en un temps curt i a gran distància. Suporta amplades de banda i velocitats extremadament altes. La gran quantitat d'informació que es pot transmetre per unitat de cable de fibra òptica és, indiscutiblement, el seu major avantatge. Quant al seu cost, es pot produir cable de fibra òptica a un cost més baix si es compara amb la mateixa quantitat de cable de coure.

Les xarxes de fibra òptica que han arribat als usuaris domèstics en els últims temps són àmpliament conegudes en els entorns professionals. Inicialment es van començar a emprar en la connexió de servidors a cabines de dades i en la interconnexió de servidors amb un alt flux de dades, primerament en entorns de supercomputació i posteriorment per la interconnexió d'equips orientats a l'alt rendiment i alta disponibilitat en què les diferents parts del servei (servidor web, servidor d'aplicacions, servidor de bases de dades) estan en diferents equips físics. Una altra de les aplicacions típiques de la fibra òptica ha estat la creació de línies dedicades d'interconnexió dels diferents centres de treball de les empreses.

D'altra banda, cada cop està més estès l'ús de la computació al núvol, no solament per a l'emmagatzematge de dades, sinó també per al seu processament (AWS, Azure, etc.). Aquests nous models de còmput fan imprescindible l'ús de xarxes de fibra òptica per transportar grans volums de dades a molt alta velocitat.

Fora de l'àmbit empresarial, l'alta demanda de serveis de videoconferència i distribució de continguts multimèdia sota demanda, fa que cada vegada siguin més populars els serveis d'*streaming* proporcionats tant per les operadores de comunicacions com per les companyies dedicades a aquest tipus de servei (Netflix, HBO, Disney, etc.). A causa del gran volum de dades que s'han d'enviar per la xarxa per poder visualitzar el contingut en temps real i l'alta velocitat de transmissió necessària per tenir una bona qualitat de servei (SoS), les xarxes de fibra òptica són molt apropiades per als usuaris que utilitzin aquest tipus de servei.

# 3. Protocols de comunicació

Una vegada instal·lat el maquinari, el cablejat i els diversos dispositius que formen la xarxa, cal instal·lar el programari de xarxa, que gestionarà tots els serveis. Aquests serveis s'articulen en un conjunt de protocols que permetran la comunicació entre els diferents ordinadors de la xarxa. Els protocols més comuns són els de la família TCP/IP (entre d'altres, com per exemple Apple Talk per a sistemes Apple Macintosh, en desús des de la publicació de Mac OS X v10.6 el 2009, IPX/SPX, etc.).

## 3.1. TCP/IP

TCP/IP està format per un conjunt de protocols que permeten compartir recursos als ordinadors d'una xarxa. El va desenvolupar l'any 1972 el Departament de Defensa dels Estats Units d'Amèrica amb la finalitat d'interconnectar els recursos de la coneguda xarxa ARPANET (una xarxa del Departament de Defensa) i, amb el pas del temps, s'ha convertit en l'estàndard utilitzat a internet. També està estretament vinculat al sistema operatiu Unix, tot i que actualment la gran majoria de sistemes operatius suporten TCP/IP. De fet, els protocols TCP/IP són extremadament flexibles, de manera que gairebé totes les tecnologies subjacents (Ethernet, Token Ring, etc.) es poden fer servir per transmetre trànsit TCP/IP.

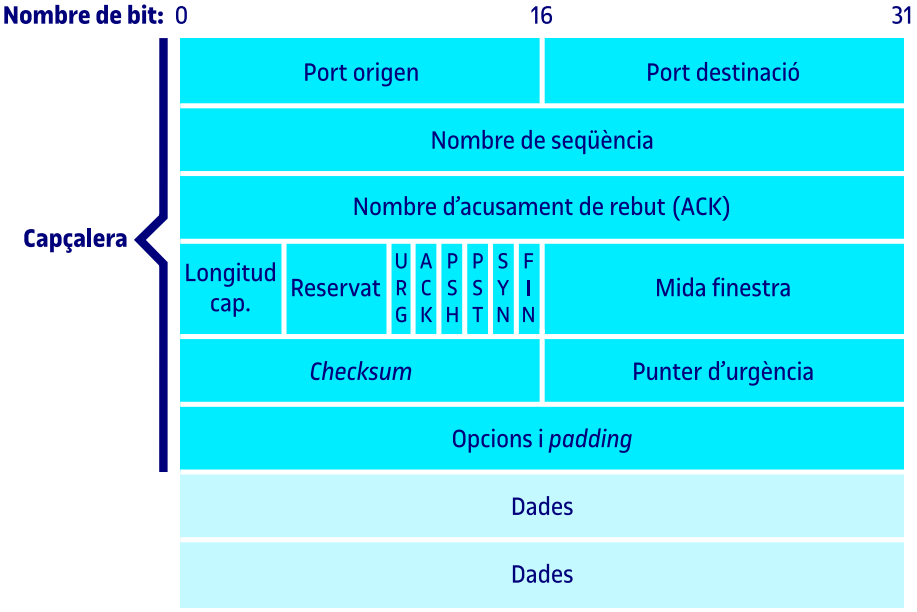
**Protocols**

**TCP** i **IP** només són dos dels protocols englobats dins el conjunt genèric TCP/IP, però són els més coneguts i, finalment, són els que donen el nom al conjunt sencer.

El protocol **UDP** (*user datagram protocol*) és un protocol no fiable i no orientat a connexió, situat a la capa de transport del model OSI (la mateixa que el protocol TCP).

**Altres protocols** TCP/IP: ARP (*address resolution protocol*), ICMP (*internet control message protocol*).

Figura 11. Segment TCP




Quan s'utilitza el protocol TCP/IP, la informació es transmet com una seqüència de **datagrames** que, amb l'estructura que es mostra a la figura 11, contenen les dades que cal transmetre i la informació de control. Cadascun d'aquests datagrames s'envia individualment a la xarxa, de manera que la informació

original pugui ser reconstruïda quan arriba a la màquina de destinació a partir del reagrupament dels datagrames enviats (val a dir que els datagrames no han d'arribar necessàriament amb el mateix ordre en què van ser lliurats). El protocol TCP (*transmission control protocol*) garanteix la recepció de les dades i que els datagrames siguin refets en l'ordre correcte (servei fiable de transmissió extrem a extrem). Al mateix temps, aquest servei descansa en el proporcionat pel protocol IP (*internet protocol*), que no és fiable i que fa funcions d'encaminament dels datagrames.

L'arquitectura del TCP/IP consta de quatre nivells o capes, en què s'agrupen els protocols, i que es relacionen amb els nivells OSI de la manera següent:

**1) Nivell d'aplicació**: es correspon amb els nivells OSI d'aplicació, presentació i sessió. El nivell d'aplicació és el nivell que els programes més habituals utilitzen per comunicar-se per mitjà d'una xarxa amb altres programes. Alguns programes específics s'executen en aquest nivell. Proporcionen serveis que treballen directament amb les aplicacions d'usuari. Aquests programes i els seus corresponents protocols inclouen **HTTP** (*hyper text transfer protocol*), **FTP** (*file transfer protocol*), **SMTP**, **SSH**, **DNS**, entre d'altres.

**OSI**

OSI és el protocol de referència d'Interconnexió de Sistemes Oberts (OSI), llançat el 1984, i va ser el model de xarxa descriptiu creat per l'ISO (Organització Internacional per a l'Estandardització).

**2) Nivell de transport**: coincideix amb el nivell de transport del model OSI. Els protocols del nivell de transport poden solucionar problemes com ara la fiabilitat i la seguretat que les dades arriben al destí i ho fan en l'ordre correcte. En el conjunt de protocols TCP/IP, els protocols de transport també determinen a quina aplicació van destinades les dades. **TCP** és un mecanisme de transport fiable i orientat a connexió, el qual proporciona un flux fiable de bytes, assegura que les dades arribin completes, sense danys i en ordre. **UDP** és un protocol de datagrames sense connexió. És un protocol no fiable, que no verifica que els paquets arribin al seu destí, ni tampoc dona garanties que arribin en ordre. UDP s'utilitza normalment per a aplicacions d'*streaming* en què l'arribada a temps dels paquets és més important que la fiabilitat, o per a aplicacions senzilles del tipus petició/resposta com el servei DNS, en què la sobrecàrrega de les capçaleres que aporten fiabilitat és desproporcionada per la mida dels paquets.

**3) Nivell d'interxarxa**: és el nivell de xarxa del model OSI. Tal com va ser definit originalment, el nivell de xarxa soluciona el problema de transportar paquets per mitjà d'una xarxa senzilla.

**4) Nivell d'enllaç**: la capa d'enllaç no forma part realment de la pila TCP/IP, però és el mètode utilitzat per passar paquets de la capa internet d'un dispositiu a la capa internet d'un altre dispositiu. Aquest procés pot ser controlat tant pel programari com pel maquinari.

### 3.2. IPv6 o IPng (*next generation internet protocol*)

És la nova versió del protocol d'internet (IP), destinada a substituir la que encara s'està utilitzant (coneguda com a **IPv4**). Fou dissenyat per Steve Deering i Craig Mudge, i adoptat per l'Institute Engineering Task Force (IETF) l'any 1994. A la nova versió es varen eliminar aquelles funcions del protocol IP que no s'empraven i se n'afegiren de noves. Vegem, tot seguit, quines són les prestacions més importants de l'IPv6:

- **Major capacitat d'adreçament**. Una de les principals deficiències del protocol IPv4 consistia en la seva poca capacitat d'adreçament (2ˆ32). Les noves adreces, formades per 16 octets, permeten una capacitat d'adreçament molt més elevada i suficient per evitar el col·lapse de l'assignació d'adreces: 2ˆ128, aproximadament, 3,4 × 10ˆ38. A més, pel mateix motiu, amb IPv4 no es poden assignar adreces públiques a tots els usuaris o dispositius, sense les quals els serveis d'extrem a extrem no poden funcionar (per exemple, veu i vídeo sobre IP).

- **Seguretat integrada mitjançant IPSec**. És un conjunt de protocols de xarxa segura que autentica i xifra els paquets de dades per proporcionar una comunicació xifrada segura entre dos equips per mitjà d'una xarxa de protocol d'internet. S'utilitza en xarxes privades virtuals (conegudes per les sigles VPN).

- **Mobilitat**. Possibilitat que un node mantingui la seva adreça IP, malgrat la seva mobilitat.

- **Autoconfiguració**. El nou protocol també inclou de base la possibilitat que el mateix *host* sigui capaç d'autoconfigurar les seves interfícies i connectar-se a la xarxa.

Altres propietats interessants inclouen un nou sistema de representació de noms de domini (DNS), fàcilment ampliable a noves prestacions, túnels IPv6 en IPv4 (permeten que màquines amb l'IPv6 instal·lat es puguin comunicar entre si per mitjà d'una xarxa IPv4), i nous tipus d'adreces:

- **Unicast**. Un paquet lliurat a una adreça d'aquest tipus solament arribarà a la interfície identificada amb aquesta adreça (és l'equivalent de les adreces IPv4 actuals).

- **Anycast**. En aquest cas, l'adreça arribarà a *alguna* (l'adreça més propera segons el protocol d'encaminament) de les interfícies identificades amb l'adreça del conjunt.

- **Multicast**. En aquest cas, l'adreça arribarà a *totes* les adreces de les interfícies del grup (equivalent a les adreces *broadcast* d'IPv4).

# 4. Configuració de la xarxa en els ordinadors (client/servidor)

Tot i que el concepte client/servidor abasta altres aspectes que aquí no exposarem, en el cas que ens ocupa entendrem que l'ordinador que actua com a servidor és aquell al qual arriben les sol·licituds d'altres ordinadors (els clients), normalment connectats a la mateixa xarxa.

Per poder treballar en un entorn client/servidor, cal que els clients executin el programari de xarxa en el sistema operatiu «normal» de l'estació de treball. D'altra banda, el servidor també executarà el seu programari a l'espera de rebre les sol·licituds de les estacions de treball que volen accedir als seus serveis. Aquest flux d'informació requereix que els servidors i els clients comparteixin el mateix protocol de comunicació.

## 4.1. Configuració de les estacions de treball

A continuació, parlarem molt breument dels passos que cal seguir per connectar una estació de treball a la xarxa. Aquesta operació depèn molt del sistema i del protocol que es triï, de manera que totes les indicacions que es donaran són de caràcter molt general.

**1) Instal·lació i configuració dels controladors de la targeta de xarxa**

El primer pas consisteix a instal·lar i configurar els controladors del NIC de la nostra estació de treball.

**Targeta *Plug and Play***

Si la targeta de xarxa és *Plug and Play* es configurarà automàticament.

En aquests casos, especialment quan les targetes són de fabricants diferents, la instal·lació i la configuració dels controladors pot ser una tasca complicada en què s'hagin de resoldre conflictes d'E/S (entrada/sortida) i d'interrupcions amb altres NIC o altres recursos del sistema.

**Observació**

Una estació de treball pot necessitar més d'un NIC!

**2) Selecció i configuració del protocol de comunicació**

En cas que necessitem connexió amb Novell, caldrà instal·lar el protocol SPX/IPX. Per fer-ho amb Macintosh, cal el protocol Apple Talk. Com ja s'ha indicat, però, el protocol més comú és TCP/IP, imprescindible si volem tenir accés a internet.

**3) Instal·lació i configuració de clients**

En aquest punt, és on s'instal·len les aplicacions que faran servir els recursos de la xarxa, com per exemple un servidor de fitxers que pot donar servei a clients tipus FTP o de compartició de fitxers per mitjà d'unitats de xarxa, o un servidor web o d'aplicacions.

**4) Altres aspectes configurables**

A partir d'aquest moment, es poden configurar altres aspectes, com els següents:

- Control d'accessos:
  - Per recursos: permet proporcionar una contrasenya per a cada recurs compartit.
  - Per usuaris: permet especificar els usuaris i grups que tenen accés a cadascun dels recursos compartits.

- Compartició de fitxers:
  - Permís de lectura.
  - Complet.
  - Permís de lectura o complet segons contrasenya.

- Compartició d'impressores.

- Identificació de la màquina (serà el nom amb què apareixerà a la xarxa).

- Grup de treball a què pertany la màquina.

**Controladors d'impressora**

La impressora ha d'estar instal·lada amb els controladors necessaris a l'ordinador on estigui connectada. Les estacions que l'hagin de fer servir també necessitaran tenir instal·lats els controladors.

## Resum

Les xarxes d'ordinadors permeten aprofitar millor els recursos del sistema. En aquest mòdul, s'han vist els elements que formen part de la xarxa i alguns criteris que poden ajudar els administradors a l'hora de triar aquests elements i connectar-los entre si. Una vegada es disposa de la xarxa, físicament parlant, cal fer que els ordinadors parlin el mateix «idioma», és a dir, tinguin definit el mateix protocol de comunicacions (el més utilitzat és el TCP/IP), la instal·lació del qual està íntimament lligada a la configuració de les estacions de treball. Tot i l'heterogeneïtat de les xarxes, els protocols i els sistemes operatius de xarxa, aquestes accions sempre s'han de fer d'una manera o altra, tot i que la manera com es fan pot variar molt.

Finalment, una vegada la xarxa ja estigui en funcionament, l'administrador no pot oblidar que les xarxes no es mantenen per si soles i que requereixen un gran esforç de manteniment: creació i administració de l'entorn de l'usuari, monitorització de la xarxa, actualització del programari, detecció d'atacs, etc.

# Activitats

**1.** En cas que tingueu accés a una xarxa d'ordinadors, responsgueu les qüestions següents:

**a)** Localitzeu i identifiqueu físicament tots els elements que formen part de la xarxa.
**b)** Quina topologia s'ha utilitzat en el seu disseny?
**c)** Quins protocols de comunicació es fan servir?
**d)** Com es configuren les estacions de treball?
**e)** Quins programaris de monitorització s'utilitzen?
**f)** Localitzeu i identifiqueu els elements de seguretat (programari i maquinari).

**2.** Si no disposeu d'accés a una xarxa d'ordinadors, enumereu i descriviu tots els elements que participen en una connexió a internet per la xarxa telefònica:

Casa ↔ proveïdor de serveis d'internet ↔ internet

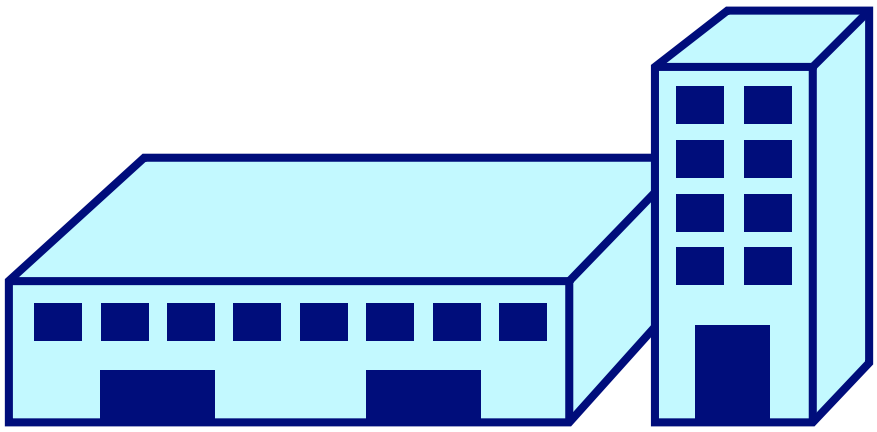
Un element que caldrà que tingueu en compte (i del qual també parlarem en el mòdul de seguretat de la xarxa) és que, per tal de respondre a possibles problemes legals (i a efectes de tarifació), un proveïdor d'internet hauria d'enregistrar les adreces IP que va proporcionant dinàmicament als usuaris, juntament amb el número de telèfon que s'ha fet servir per connectar-s'hi, i també l'interval de temps en què s'han utilitzat.

# Exercicis d'autoavaluació

**1.** Ompliu cadascuna de les caselles de la taula següent amb alguna d'aquestes opcions: *baix*/*moderat*/*alt*.

| | **Parell trenat** | **Coaxial** | **Fibra òptica** |
|---|---|---|---|
| **Cost** | | | |
| **Amplada de banda** | | | |
| **Longitud** | | | |
| **Interferències** | | | |
| **Fiabilitat** | | | |

**2.** Heu de dissenyar i implementar una xarxa per a un edifici d'oficines format per un bloc de quatre plantes i una nau industrial que treballa amb molts motors. Dissenyeu un traçat per al cablejat elèctric per tal d'alimentar els motors i després indiqueu els dispositius de comunicació que s'haurien d'instal·lar, tant a la nau industrial com a l'edifici, per tenir una xarxa local que comuniqui les oficines amb els punts de treball de la nau industrial.



**3.** Determineu quina de les característiques següents no es pot atribuir a qualsevol topologia en estrella:

**a)** Totes les estacions es connecten a un element central.
**b)** Quan una estació emet un missatge sempre arriba a totes les estacions de la xarxa.
**c)** És una topologia resistent a la caiguda de les estacions de treball.
**d)** El dispositiu central pot ser actiu o passiu.

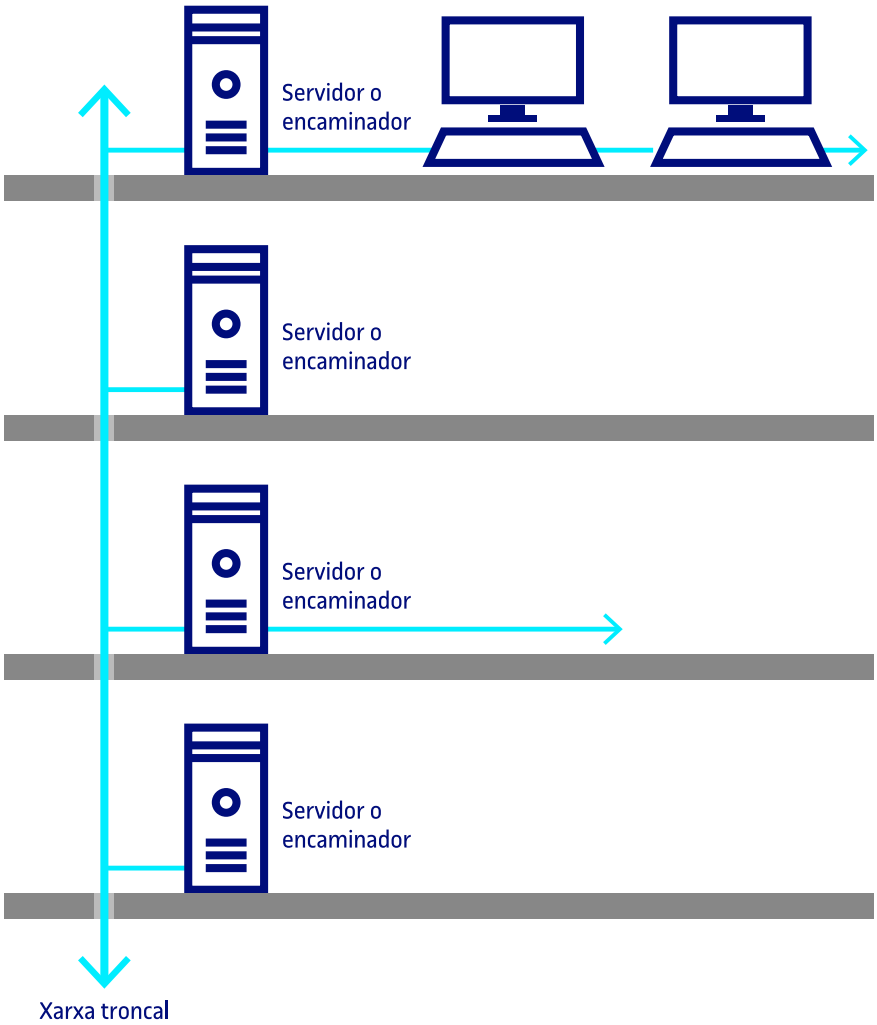
# Solucionari

## Exercicis d'autoavaluació

1.

| | Parell trenat | Coaxial | Fibra òptica |
|---|---|---|---|
| **Cost** | Baix | Moderat | Alt |
| **Amplada de banda** | Moderat | Alt | Molt alt |
| **Longitud** | 100 m | 1 km | Alguns km |
| **Interferències** | Baix | Molt baix | Cap |
| **Fiabilitat** | Alt | Alt | Molt alt |

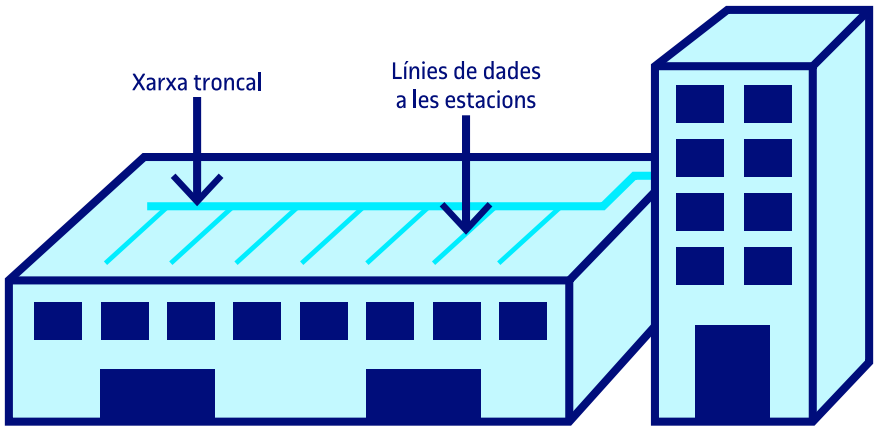
2.




A la planta, el cablejat també hauria de seguir un esquema de tipus xarxa troncal (*backbone*), amb branques als punts necessaris. Les qüestions bàsiques que cal tenir en compte en el seu disseny són les següents:

- Les distàncies del cablejat no han de ser superiors a les permeses. En cas contrari, cal posar regeneradors del senyal.
- S'ha de tenir molt en compte el problema de les interferències elèctriques i, per tant, l'electricitat i les dades no poden anar pels mateixos llocs.

- Si hi ha armaris de connexió, cal tenir en compte les qüestions de protecció de les vibracions i de l'alimentació elèctrica.




**3. b**

# Glossari

***backbone*** Vegeu **xarxa troncal**.

**10Base-T** *m* Cable de parell trenat UTP amb una longitud màxima de segment de cent metres en una topologia física d'estrella.

**100Base-T** *m* Cable de parell trenat UTP amb velocitats de transmissió de 100 MBps.
**sin.**: Fast Ethernet

**10Base-2** *m* Cable coaxial prim amb una velocitat de transmissió de 10 MBps. Accepta fins a trenta llocs de treball en segments de longitud de com a molt cent vuitanta-cinc metres.
**sin.**: *thin wire*

**10Base-5** *m* Cable coaxial gruixut amb una velocitat de transmissió de 10 MBps. Accepta fins a cent llocs de treball en segments de longitud de com a molt cinc-cents metres.
**sin.**: *thick wire*

**commutador** *m* Dispositiu que gestiona el flux del trànsit de la xarxa tenint en compte l'adreça de destinació de cada paquet. En altres paraules, els commutadors poden esbrinar quins dispositius estan connectats als seus ports i redirigeixen la informació únicament al port de destinació, en lloc de fer-ho indiscriminadament, com els concentradors.
**en.**: *switch*

**concentrador** *m* Dispositiu que permet compartir una línia de comunicació entre diversos ordinadors. Distribueix tota la informació que rep perquè pugui arribar a tots els dispositius connectats.
**en.**: *hub*

**DHCP** *m* Vegeu **protocol dinàmic de configuració de l'hoste**.

***dynamic host configuration protocol*** Vegeu **protocol dinàmic de configuració de l'hoste**.

**encaminador** *m* Dispositiu que gestiona el trànsit de paquets provinent de l'exterior de la xarxa cap a l'interior (i a l'inrevés). Pot tenir capacitat d'actuar com a tallafoc. Pot filtrar i trobar l'encaminament òptim dels paquets.
**en.**: *router*

***fast Ethernet*** Vegeu **100Base-T**.

***firewall*** Vegeu **tallafoc**.

***hub*** Vegeu **concentrador**.

**IEEE** *m* Vegeu **Institute of Electrical and Electronic Engineers**.

**Institute of Electrical and Electronic Engineers** *m* Organisme que data de l'any 1980 i que va elaborar les normes IEEE 802.x, les quals defineixen els estàndards pel que fa al funcionament de les xarxes d'àrea local.
**sigla**: IEEE

***network interface card*** Vegeu **targeta d'interfície de la xarxa**.

***NIC*** *f* Vegeu **targeta d'interfície de la xarxa**.

**protocol dinàmic de configuració de l'hoste** *m* Protocol TCP/IP que permet l'assignació dinàmica d'adreces IP.
**en.**: *dynamic host configuration protocol*
**sigla**: DHCP

***router*** Vegeu **encaminador**.

***switch*** Vegeu **commutador**.

**tallafoc** *m* Qualsevol dispositiu (maquinari o programari) que permet evitar que els usuaris no autoritzats accedeixin a una màquina determinada.
**en.**: *firewall*

**targeta d'interfície de la xarxa** *f* Targeta d'interfície que permet la connexió de l'estació de treball a la xarxa.
**en.**: *network interface card*

**sigla**: NIC

***thick wire*** Vegeu **10Base-5**.

***thin wire*** Vegeu **10Base-2**.

***wireless local area network*** Vegeu **xarxa d'àrea local sense fil**.

***WLAN*** *f* Vegeu **xarxa d'àrea local sense fil**.

**xarxa d'àrea local sense fil** *f* Xarxa de telecomunicacions local sense fil basada en ones de ràdio o infraroges.
**en.**: *wireless local area network*
**sigla**: WLAN

**xarxa troncal** *f* Conjunt de cables principals que connecten entre si els segments d'una xarxa local. Habitualment són enllaços d'alta velocitat (per exemple, la fibra òptica).
**en.**: *backbone*

# Bibliografia

**Anònim** (2000). *Linux Máxima Seguridad*. Nova Jersey: Prentice Hall.

**Arnedo Moreno, J.** (2002). «Xarxes locals sense fil». Article UOC.

**Colobrán Huguet, M.; Morón Lerma, E.** (2004). *Introducción a la Seguridad Informática*. Barcelona: Planeta UOC.

**Halsall, F.** (1996). *Data Communications, computer networks and open systems*. Nova York: McGraw-Hill.

**Jimeno García, M. T.; Míguez Pérez, C.; Matas García, A. M.; Pérez Agudín, J.** (2008). *Guía Práctica Hacker*. Madrid: Anaya Multimedia.

**Palet Martínez, J.** (2000). *Tutorial d'IPv6*. Madrid: Consulintel.

**Stallings, W.** (2000). *Comunicacions informàtiques i de dades* (6a. edició). Nova Jersey: Prentice Hall.

**Tanembaum, A. S.** (1991). *Redes de Ordenadores*. Mèxic: Prentice-Hall Hispanoamericana.