

Unió Europea

Fons Social Europeu
L'FSE inverteix en el teu futur

Xarxes Locals

1r SMX

Paco Galera

Copyright © 2024 - P. Galera

Continguts

1. UD1. Caracterització de xarxes locals	6
1.1 Un model de comunicació	6
1.1.1 Components d'una comunicació telemàtica	6
1.2 Serveis i protocols	6
1.3 Topologia de xarxes	6
1.3.1 Topologia física	7
1.3.2 Topologia lògica	9
1.4 Classificació de xarxes	9
1.4.1 Extensió (localització geoogràfica)	9
1.4.2 Tecnologia de transmissió	10
1.4.3 Nivell d'accés o seguretat	10
1.5 Elements de la xarxa	10
1.5.1 Sistema de cablejat i radiolèctric	10
1.5.2 Els dispositius de xarxa	11
1.5.3 Nodes de la xarxa	11
1.5.4 Software de xarxa	11
1.6 Arquitectura de la xarxa	11
1.6.1 Adreçament	12
1.6.2 Encaminament	12
1.6.3 Accés al medi	12
1.6.4 Control de fluxe	12
1.6.5 Sincronització	12
1.6.6 Control d'errors	12
1.6.7 Format dels missatges	12
1.6.8 Multiplexació	12
1.6.9 Arquitectura per capes	12
2. UD2. Instal·lació física d'una xarxa (I). Medis de transmissió	17
2.1 Introducció	17
2.2 Tipus de cablejat de xarxa	17
2.2.1 Cable de parell trenat	17
2.2.2 Cable coaxial	20
2.2.3 Fibra òptica	21
2.3 Transmissions sense fil	23
2.3.1 Infrarrojos (IR)	24
2.3.2 Radiofreqüència (RF)	24

3. UD3. Instal·lació física d'una xarxa (II). Dispositius de connexió	27
3.1 Connectors per a xarxes	27
3.1.1 Connector RJ11	27
3.1.2 Connector RJ45	27
3.1.3 Connector BNC	27
3.1.4 Connector DB9	28
3.1.5 Connector DB25	28
3.1.6 Connector ST (Fibra)	29
3.1.7 Connector SC (Fibra)	29
3.2 Ferramentes	30
3.3 La targeta de xarxa	31
3.3.1 Configuració de l'adaptador de xarxa	32
3.4 Model TCP/IP	33
3.4.1 Protocol IP	33
3.4.2 Protocol TCP	34
3.5 Ethernet	34
3.5.1 Projecte 802	34
3.5.2 Comprovació d'errors al nivell d'enllaç LCC	36
3.5.3 Algorisme CSMA/CD	36
3.5.4 Tipus d'Ethernet	37
3.6 Cablejat de xarxa	37
3.6.1 Enrutament del cablejat	37
3.6.2 Muntatge de cables en canaletes	38
3.6.3 Suport de cablejat horitzontal	39
3.6.4 Muntatge d'armaris i <i>patch-pannels</i>	40
3.6.5 Personal	40
3.6.6 Termes	41
3.6.7 Organismes i normativa	41
4. UD4. Dispositius específics d'una xarxa local	43
4.1 Introducció	43
4.2 Repetidor	43
4.3 Hub	44
4.3.1 Tipus de Hubs	44
4.3.2 Tipus de connexions al Hub	44
4.3.3 Connexió entre Hubs	45
4.3.4 Topologia Hubs	45
4.4 Pont o Bridge	46
4.4.1 Domini de col·lisió	47

4.5 Switch o Commutador	47
4.6 Router o Encaminador	48
4.6.1 Característiques	49
4.6.2 Protocols d'encaminament	50
4.6.3 Temps de convergència	50
4.6.4 Passarel·les	51
5. UD5. Instal·lació i configuració d'equips de xarxa	52
5.1 El sistema operatiu en xarxa	52
5.1.1 Components del sistema	52
5.2 Families de protocols en Microsoft	52
5.3 Família de protocols TCP/IP	53
5.3.1 Protocol IP	53
5.3.2 Protocol TCP	56
5.4 Adreçament IP (Classful)	56
5.4.1 Classes de una adreça IP: classe A	56
5.4.2 Classes de una adreça IP: classe B	56
5.4.3 Classes de una adreça IP: classe C	57
5.4.4 Classes de una adreça IP: classe D	57
5.4.5 Classes de una adreça IP: classe E	57
5.5 Adreces públiques i privades	57
5.5.1 Adreces IP privades reservades	57
5.6 Adreces IP estàtiques i dinàmiques	57
5.7 Adreces IP especials	58
5.8 Càcul de l'adreça de <i>broadcast</i>	59
5.9 Adreçament <i>Classful</i>	59
5.9.1 <i>Subnetting</i>	60
5.10 Adreçament <i>Classless</i>	61
6. UD6. Escenaris de xarxes	63
6.1 Configuració de la xarxa	63
6.1.1 Nom de l'equip	63
6.1.2 Adreça IP, Màscara, MAC i Adreça de broadcast	63
6.1.3 Porta d'enllaç	64
6.1.4 Servidors DNS	64
6.1.5 Informació del driver i de la connexió	64
6.1.6 Connexions sense fils	64
6.2 Test de velocitat de la xarxa local	64
6.3 Adaptadors de xarxa en VirtualBox	65
6.3.1 NAT en VirtualBox	66

6.3.2 Xarxa NAT en VirtualBox	68
6.3.3 Adaptador pont en VirtualBox	70
6.3.4 Xarxa interna	70
6.3.5 Adaptador sols-amfitrió	72
6.4 Netplan	74
6.4.1 Configurar targeta de xarxa per DHCP	75
6.4.2 Configurar targeta de xarxa amb IP fixa	76
6.4.3 Aplicar les configuracions	76

1. UD1. Caracterització de xarxes locals

1.1 Un model de comunicació

A qualsevol comunicació poden distingir-se (mínim) 6 components:

- La **font** és l'orige del qual procedeix la informació
- L'**emissor** és l'element que s'encarrega de transformar la informació proporcionada per la font per a adaptar-la al canal-medi per el qual es transmetrà.
- El **canal o medi** és l'element per el qual es transmet la informació. Aquest pot ser algú tipus de cable o, en el cas de comunicacions sense fil, l'aire.
- El **soroll** és qualsevol perturbació sobre el medi que afecte a la informació. Açò fa que la informació arribe amb modificacions.
- El **receptor** és l'element que s'encarrega d'extraure la informació del canal i transformar-la per tal que puga ser interpretada correctament per el destí.
- El **destí** és el lloc o entitat que consumeix la informació. Normalment és una persona.

1.1.1 Components d'una comunicació telemàtica

- Els **terminals** són els equip que es comuniquen. Exemple: ordinadors, perifèrics d'ús en xarxa (impressores, escàners...) i altres dispositius (mòbils, tauletes...).
- Els **dispositius de xarxa** són el conjunt d'elements físics que fan possible la comunicació entre terminals font i destí. Aquests dispositius són:
- **Canal de comunicació:** és el medi per el qual circula la informació. Exemple: cable UTP de cat 5.
- **Elements d'interconnexió:** són els encarregats d'interconnectar tots els terminals de la xarxa i seleccionar el millor camí per el qual circularà la informació (si és que hi ha més d'un). Exemple: connector RJ45, antenes i equips intermedis.
- **Adaptadors de xarxa:** converteixen el format d'informació dels terminals en el format emprat per la xarxa de comunicació.
- Els **programes de xarxa** permeten controlar el funcionament de la xarxa, per a fer-la més fiable.

1.2 Serveis i protocols

Serveis són les funcionalitats que ofereix una xarxa. Per poder oferir estes funcionalitats deuen de seguir un protocol establert i estandarditzat. Exemple: en una xarxa telefònica són serveis: la transmissió de veu, la transmissió de dades, les trucades en espera...

Protocol són les normes o regles a seguir al moment de realitzar una comunicació/transmissió de dades. Exemple: en una xarxa de dades un protocol habitual és el protocol TCP.

Per tant, si una xarxa preten oferir un servei haurà de comprovar si compta amb un protocol adequat per poder oferir-lo.

1.3 Topologia de xarxes

Una **xarxa** és un conjunt d'ordinadors i/o dispositius connectats per enllaços d'un medi físic (medis guiatos) o sense fil (medis no guiatos) i que comparteixen informació (fitxers), recursos (CD, impressora...).

La **topologia** d'una xarxa és la configuració espacial en que es disposen les seues línies i nodes. Existeixen dos tipus de topologies:

- **Topologia física:** descriu com estan dispostos a la xarxa els media de transmissió.
- **Topologia lògica:** defineix com accedeixen els equips a la xarxa.

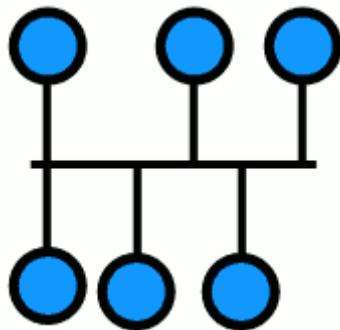
1.3.1 Topologia física

Les topologies físiques es poden classificar en:

- Bus
- Malla
- Estrela
- Arbre
- Anell
- Mixta o irregular

Bus

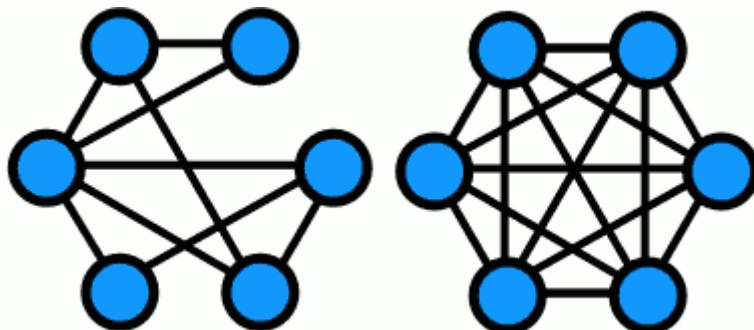
S'empra un únic cable per connectar els equips.



- **Avantatges:** baix cost per emprar poc cablejat.
- **Desavantatges:** controlar les col·lisions. Xifrat per tal de mantenir la privacitat. Si falla un enllaç la xarxa deixa de funcionar completament.

Malla

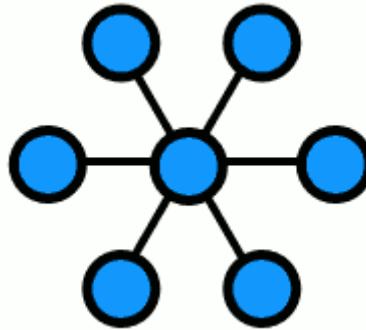
Interconnexió total de tots els nodes



- **Avantatges:** si una ruta falla es pot seleccionar altra alternativa.
- **Desavantatges:** més costós perquè fa falta més cablejat.

Estrela

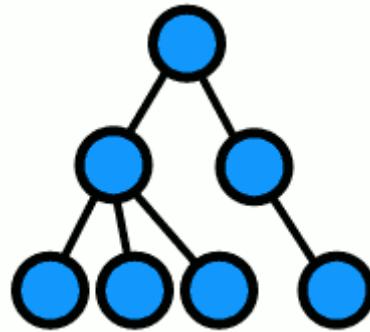
Connecta tots els cables amb un punt central de concentració. Per regla general es tracta d'un *Hub* o un *Switch*.



- **Avantatges:** el node central realitza les tasques de distribució, conmutació i control per evitar col·lisions.
- **Desavantatges:** si el node central falla es queda tota la xarxa inutilitzada.

Arbre

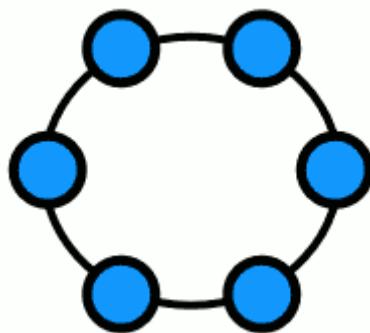
Es connecten tots els nodes de forma jerarquitzada. Molt emprat en xarxes de telefonia on els enllaços intermedis són centraletes locals i regionals.



- **Avantatges:** cost bastant optimitzat.
- **Desavantatges:** la fallada d'un node o enllaç deixa un conjunt de nodes incomunicats.

Anell

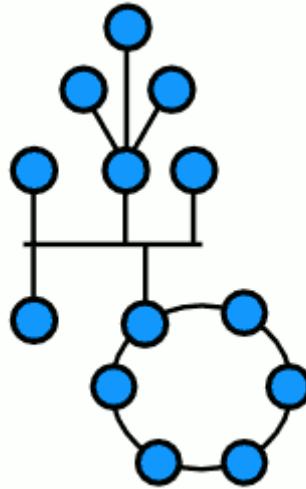
Tots els nodes estan connectats a una única via amb els seus dos extrems units.



- **Avantatges:** s'eviten col·lisions.
- **Desavantatges:** si falla un enllaç, la xarxa deixa de funcionar completament.

Mixta o irregular

És el que s'empra a la vida real quan la xarxa té certa envergadura. Es mesclen diverses topologies.



- **Avantatges:** cada tram s'adapta a les seues característiques.

- **Desavantatges:** major complexitat de gestió del trànsit.

1.3.2 Topologia lògica

La topologia lògica de la xarxa descriu la forma en que els equips es comuniquen dintre de la xarxa i pot ser:

- **Topologia de bus lògic:** cada equip envia les seues dades cap a tots els demés sense ningú tipus de filtre. Tots els nodes de la xarxa miren les dades que circulen per aquesta i decideixen si les dades són per a ells o no en funció de la adreça de destí.
- **Ús de testics (token):** el testic va passant entre els diferents equips de la xarxa. Si el dispositiu que té el testic en eixe moment vol transmetre dades a través de la xarxa pot fer-ho i en cas contrari passa el testic al següent node.

1.4 Classificació de xarxes

Les xarxes es poden classificar en funció de múltiples criteris:

- Extensió (localització geogràfica).
- La tecnologia de transmissió.
- El nivell d'accés o seguretat.

1.4.1 Extensió (localització geoogràfica)

- **Xarxes d'àrea local (LAN):**
 - Una xarxa d'àea local té una **reduïda extensió** limitada, la seu tecnologia de transmissió sol ser difusió. La velocitat està entre els 10 a 1000Mbps. Les xarxes d'àrea local més exteses són *Ethernet* i *Token Ring*.
 - Solen tenir un retard molt baix a les transmissions i una taxa d'errors molt baixa. Solen ser xarxes privades i administrades per els seus propietaris.
- **Xarxes d'àrea metropolitana (MAN):**
 - No superen una distància d'unes desenes de KM. En esència les MAN són una extensió de les LAN i com a tal empren tecnologies semblants. Les xarxes MAN de vegades s'empren per a interconnexió de xarxes LAN ubicades en diferents recintes geogràfics.
- **Xarxes d'àrea extesa (WAN):**
 - S'empren sobre grans espais geogràfics. Poden cobrir distàncies de fins a milers de KM. Solen ser pùbliques i administrades per organismes o empreses nacionals. Gestionen taxes d'error altes. Les variants tecnològiques de les WAN són nombroses encara que es poden destacar aquelles basades en RDSI, FDDI, ATM FRAMERELAY.

- **Xarxes d'àrea personal (PAN):**
- Són xarxes amb una extensió d'uns pocs metres i interconnecten uns pocs equips (habitualment una habitació). Presenten una **configuració senzilla o automàtica, baix cost i actualment solen ser sense fil.**

1.4.2 Tecnologia de transmissió

- Xarxes de difusió (broadcast o multipunt)
- Xarxes comutades (punt a punt)
- Comutació de circuits
- Comutació de paquets

Xarxes de difusió (broadcast o multipunt)

- El **canal de transmissió és compartit** per tots els equips de la xarxa. Normalment, cada missatge transmés té un únic destinatari, l'adreça del qual apareix al missatge, però per conèixer si l'escollit és ell, cada equip de la xarxa ha d'escutar cada missatge, analitzar l'adreça destí i comprovar si coincideix amb la pròpia, descartant-lo en cas contrari.
- Evidentment aquesta forma de treball provoca **problemes de privadesa**. L'única protecció efectiva a les xarxes de difusió és el xifrat de la informació. Aquest tipus de línies s'empren en xarxes menudes geogràficament localitzades. És important establir un mecanisme per evitar col·lisions.

Xarxes comutades (punt a punt)

- **Comutació de circuits:** consisteix en establir un **circuit físic diferenciat** de la resta entre emissor i receptor en cada procés de comunicació. Aquest tipus de comutació és el que es produeix quan dues persones parlen per telèfon.
- **Comutació de paquets:** es basa en l'**ús d'un conjunt de nodes** que s'encarreguen de l'emmagatzematge temporal i reenviament de la informació que reben d'altres nodes. L'usuari al transmetre, envia un bloc de dades denominat paquet. Aquest bloc té un format definit que recull, entre d'altres, qui és el destinatari de la informació. Una vegada dipositat a la xarxa, cada paquet és enviat d'un node a altre fins que aplega al seu punt de destí. La ruta per arribar al destí **no té perquè ser la mateixa per a tots els paquets**.

1.4.3 Nivell d'accés o seguretat

- **Internet:** mètode d'interconnexió descentralitzada de xarxes d'equips implementat en un conjunt de protocols denominat TCP/IP i garanteix que les xarxes físiques heterogènies funcionen com una xarxa lògica única, d'alçaç mundial.
- **Intranet:** és tracta d'una xarxa dintre d'altra xarxa local (LAN) privada, empresarial o educativa que proporciona Internet.
- **Extranet:** xarxa privada virtual (VPN) que empra protocols d'Internet, de comunicació i probablement infraestructura pública de comunicació per tal de compartir de manera segura part de la informació o operació pròpia d'una organització amb proveïdors, compradors, socis, clients o qualsevol altre negoci o organització.

1.5 Elements de la xarxa

A una xarxa podem distingir els següents elements:

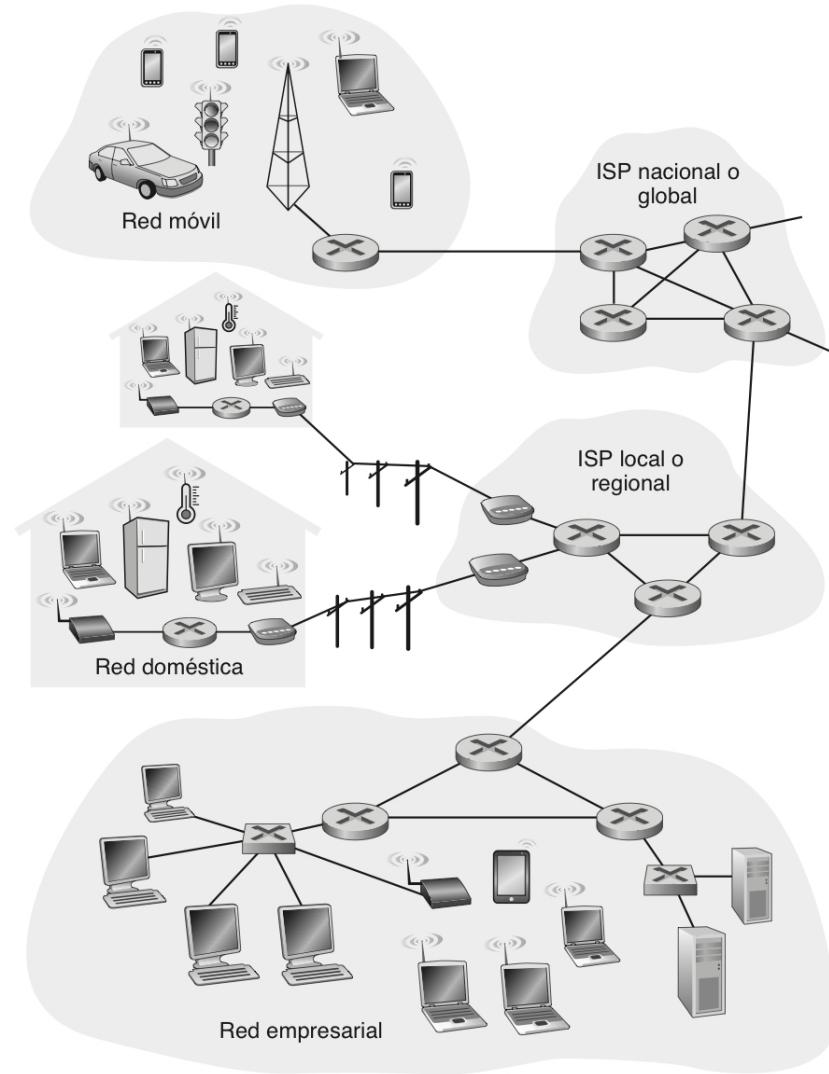
- El sistema de cablejat i radioelèctric.
- Dispositius de xarxa
- Nodes de xarxa
- Software de xarxa

1.5.1 Sistema de cablejat i radiolèctric

Condueixen la senyal per transportar la informació. El sistema de cablejat està format pel cable (normalment coure o fibra òptica) i els seus connectors. Cada tipus de cablejat porta el seu propi sistema de connectorització.

1.5.2 Els dispositius de xarxa

Interconnecten màquines i serveis. Poden ser mòdems, routers, proxies, repetidors...



1.5.3 Nodes de la xarxa

Els nodes poden estar connectats a la xarxa mitjançant cable o sense fil. Cada node requerirà al menys d'una interfície de xarxa per poder connectar-se al cable o antena.

1.5.4 Software de xarxa

- Aplicacions: gestors de xarxa (aplicacions que emprén els diferents nivells de xarxa), els recopiladors d'estadístiques, analitzadors de congestió.
- Sistemes operatius.

1.6 Arquitectura de la xarxa

De igual forma que els sistemes operatius s'encarreguen de gestionar eficientment els recursos d'un equip, el software de xarxa realitza la mateixa tasca de cara als recursos físics de la xarxa (hardware).

Les xarxes de comunicacions han de poder resoldre problemes d'adreçament, accés al medi, sincronització, format dels missatges, encaminament, control de fluxe, control d'errors i multiplexació.

1.6.1 Adreçament

Una xarxa té múltiples equips i és necessari que cada equip tinga una **adreça diferenciada** a la xarxa. Al mateix temps, cada equip pot tenir diversos processos en marxa... Es necessita un mecanisme per tal que un procés d'un equip es pugui区别 amb un altre procés (**port**) d'un altre equip vol connectar-se.

1.6.2 Encaminament

Si la xarxa permet arribar a un destí per diverses rutes, es necessita un mecanisme que determine quina és la millor ruta en un moment donat.

1.6.3 Accés al medi

Si existeix un mecanisme de comunicació de difusió, ha d'existir un mecanisme per controlar l'ordre de transmissió i evitar col·lisions.

1.6.4 Control de fluxe

Un emissor molt ràpid pot saturar/desbordar a un receptor. Hem de comptar amb un mecanisme per controlar aquest fluxe.

1.6.5 Sincronització

El receptor ha de poder determinar quan una senyal comença a arribar i quan acaba, així com la durada de cada element de la senyal. En algunes xarxes, les dades arriben desordenades. Hem de comptar amb un mecanisme que permeti ordenar les dades en el destí.

1.6.6 Control d'errors

A totes les xarxes de comunicacions quan transmetem hi ha un xicotet percentatge d'errors. Hem de comptar amb mecanismes que permeten la seua **detecció i correcció**.

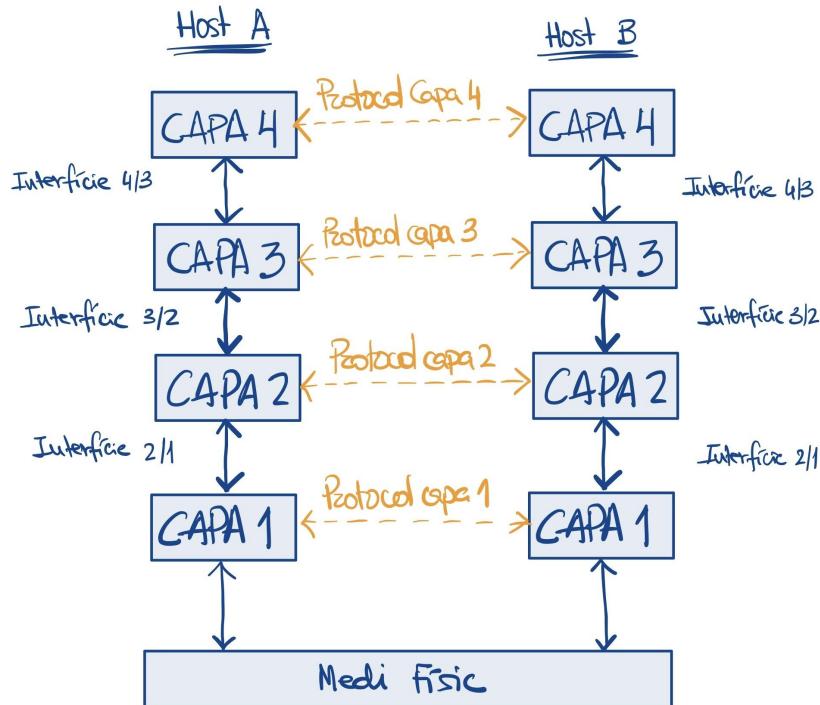
1.6.7 Format dels missatges

Ambdues parts han d'estar d'acord amb el format de les dades que es transmeten.

1.6.8 Multiplexació

Si compartim un medi de transmissió, hem d'assegurar que si hi han més d'una comunicació al mateix temps que no s'interferisquen.

1.6.9 Arquitectura per capes



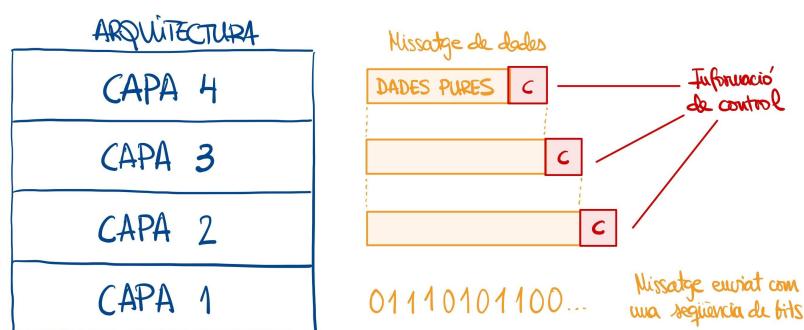
És molt més senzill descomposar els problemes de la xarxa si la organitzem en **capes o nivells** i que cada capa s'encarregue d'una funcionalitat.

Cada capa ofereix uns serveis a les capes superiors, alliberant-les de coneixement detallat de com es realitzen aqueixos serveis.

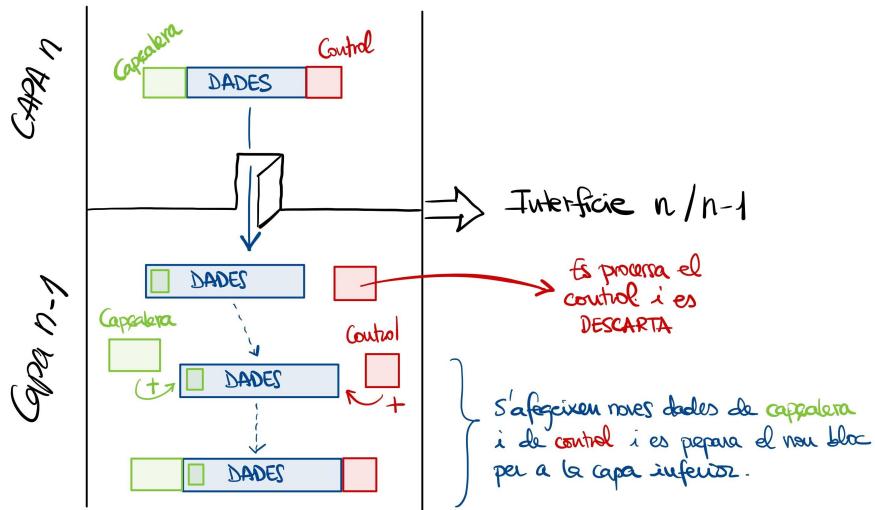
Al mateix temps, la capa n en una màquina conversa amb la capa n de l'altra màquina.

Les regles i convencions emprades en aquesta cnversació es coneixen conjuntament com **protocol de la capa n** .

Quan un sistema vol enviar un missatge a altre, la informació ha de "baixar" fins al medi físic i a través d'aquest arribar al sistema remot. Conforme va descendint es produeixen transformacions, per exemple, addició de camps de capçalera, fragmentació de paquets en altres més menuts... Totes aquestes transformacions són reversibles i en el sistema remot es realitzen en sentit invers fins que un missatge igual que l'original és depositat al nivell de destí.



Entre cada parell de capes adjacents hi ha una interfície, **que defineix els serveis i operacions primitives que la capa inferior ofereix a la superior**. El disseny clar i net d'una interfície, a més de minimitzar la quantitat d'informació que deu passar-se entre capes, fa més simple la substitució d'una capa per altra completament diferent.



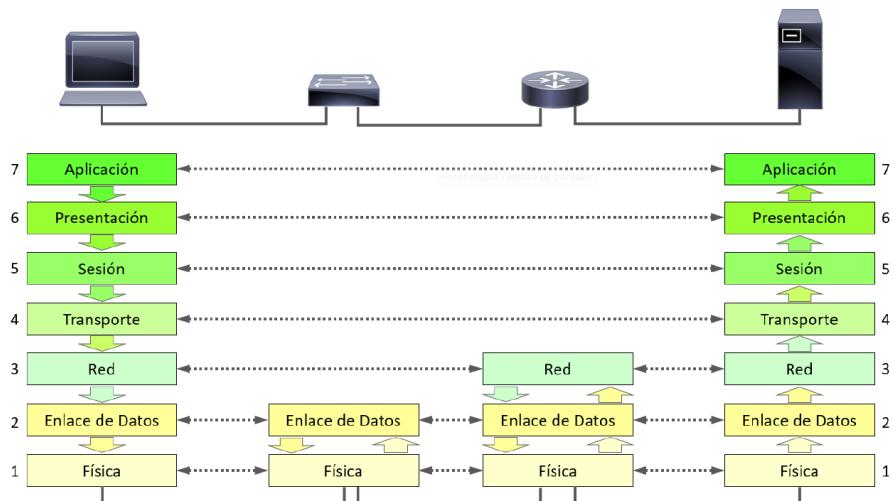
El model ISO-OSI

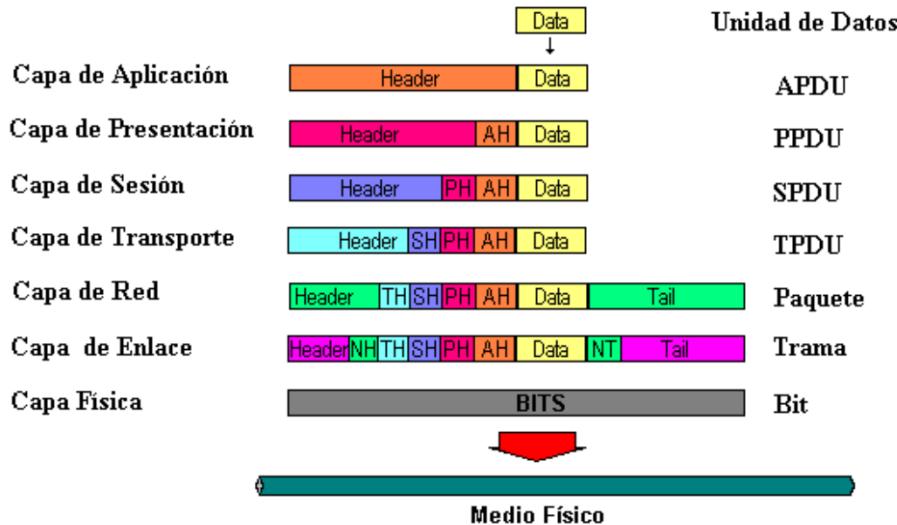
Un model de referència

Al 1977, la Organització Internacional de Normes (*ISO, International Standard Organization*) va crear un subcomitè per desenvolupar estàndards de comunicació de dades que permeten la interoperabilitat entre productes de distints fabricants. Després de diverses investigacions van elaborar un model de referència OSI (*Open System Interconnection*).

OSI no és realment una arquitectura de xarxa, sino un **model de referència**, és a dir, un model teòric que **cimenta les bases** del que hauria de ser la "arquitectura de xarxa ideal", però és massa purista i aparegué tard.

El model proposat per OSI està estructurat en **7 capes** o nivells, casaduc d'ells s'encarrega d'ofrir una sèrie de serveis a la capa superior i de tornar resultats a la capa inferior.



**NIVELL FÍSIC (I)**

La capa física s'encarrega de definir les característiques **mecàniques, elèctriques, funcionals i de procediment** per poder establir i alliberar connexions entre dos equips de xarxa.

És la capa de nivell més baix, s'encarrega de les **transmissions dels bits** i defineix paràmetres com: durada dels polsos elèctrics, nombre de Volts (V) de la senyal, la modulació, el tipus de cablejat...

NIVELL D'ENLLAÇ (II)

La tasca principal d'aquesta capa és **establir una línia de comunicació lliure d'errors** que puga ser emprada per la capa inmediatament superior (xarxa).

Hem vist que el nivell físic opera amb bits. La capa d'enllaç s'encarrega de **fraccionar el missatge** en blocs de dades de nivell 2 anomenats **trames o frames**.

L'emissor envia les trames en seqüència per la línia de transmissió i espera les trames de confirmació que generarà la capa d'enllaç del receptor.

Altra funció de la capa d'enllaç és **assegurar el flux de dades entre emissors ràpids i receptors lents** o al revés.

A més a més, també s'ocuparà dels **errors** que es produisquen (eliminar trames defectuosos, solicitar retransmissió, descartar duplicades...).

NIVELL DE XARXA (III)

La principal funció de la capa 3 és l'**encaminament**, és a dir, com escollir la ruta més adequada perquè el bloc de dades de nivell de xarxa, anomenat **paquet**, arribe al seu destí. Cada destí està identificat unequívocament a la subxarxa per una **adreça**.

Altra funció important és la del tractament de la **congestió**. Quan hi ha sobrecàrrega de paquets a la xarxa, s'obstreuixen uns a altres generant colls de botella als punts més sensibles. Un bon sistema de gestió de xarxa evitarà o paliarà aquests problemes de congestió desviant paquets cap a altres rutes inicialment no previstes.

NIVELL DE TRANSPORT (IV)

Capa de transició entre els nivells de xarxa i els nivells orientats a les aplicacions (5, 6 i 7).

Els paquets poden haver près rutes distintes i arribar als seus destins **desordenats**. És funció de la capa de transport del receptor **assegurar que les dades són les mateixes que envia la capa de transport de l'emissor**, és a dir, no s'han produït **errors i ordenar-los** en el cas que arriben desordenats.

NIVELL DE SESSIÓ (V)

Permet el **diàleg** entre emissor i receptor **establint una sessió** que portarà un transport de dades ordinari (capa de transport) però **amb possibilitat de restaurar-la** en cas que es produisquen errors a la transmissió.

Un exemple típic és la descàrrega d'un fitxer que es talla poc abans de finalitzar. Si a l'inici de la descàrrega s'establí una sessió, podrà ser resincronitzada, de tal manera que a la següent connexió es transmeten dades a partir de l'últim bloc transmés sense error.

NIVELL DE PRESENTACIÓ (VI)

Aquesta capa **s'ocupa de la sintaxi i de la semàntica** de la informació que es preten transmetre, és a dir, **investiga el contingut informatiu de les dades perquè emissor i receptor puguen "entendre's"**.

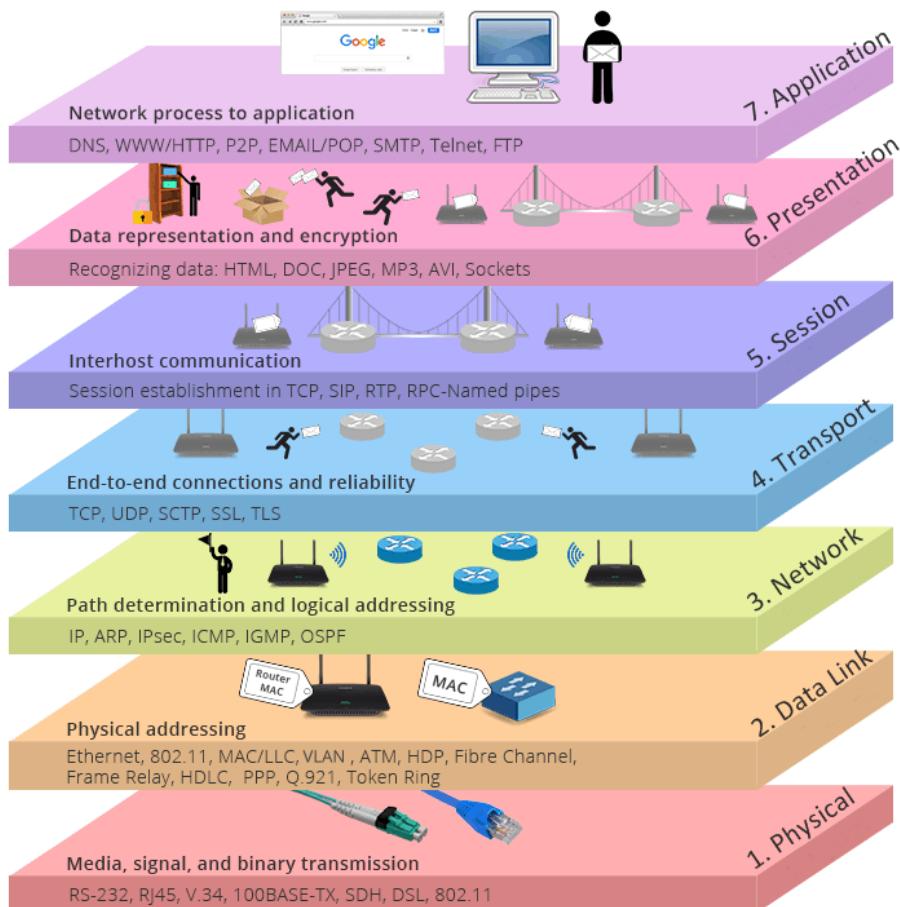
Per exemple: suposem una transmissió de text entre un emissor que empra codificació ASCII per a la representació d'informació alfanumèrica i un receptor que empra codificació EBCDIC. Si les dades son enviades i prou, el receptor no serà capaç d'interpretar-les perquè estan "parlant llengüetes distints". Necessiten un servei de conversió i interpretació que és el que fa la capa de presentació.

Altra funció de la capa de presentació pot ser la de **comprimir i/o encriptar les dades**.

NIVELL D'APLICACIÓ (VII)

És la capa superior de la jerarquia i és la capa amb la qual es comuniquen les aplicacions.

S'encarrega d'ofrir una **inferficie comú a través de la qual es comunicaran les aplicacions**, sense tenir en compte si l'aplicació origi i la aplicació destí estan a la mateixa màquina o en màquines diferents.



2. UD2. Instal·lació física d'una xarxa (I). Medis de transmissió

2.1 Introducció

El **medi de transmissió** és el suport físic que facilita el transport de la informació i suposa una part fonamental en la comunicació de les dades.

Normalment es realitza la transmissió emprant cablejat de xarxa, però també es pot fer sense fil, de manera inalàmbrica.

Atenir en compte...

- La **inversió estimada per a cables** en una instal·lació sol ser **inferior al 10%** de cost total.
- El **70% dels errors produïts** en una xarxa es deuen a defectes de **cablejat**.

Per tant, **no hem d'escatimar massa** les inversiona en cablejat estructurat.

La qualitat d'una transmissió depen de les propietats del material:

- **Propietats físiques**: son les propietats generals que permeten descriure un material. Per exemple: pes, color, temperatura de fusió, coeficient de dilatació...
- **Propietats mecàniques**: descriuen la resistència que presenta un material quan se'l somet a forces externes. Per exemple: elasticitat, plasticitat, duresa, fragilitat...
- **Propietats elèctriques**: son les que determinen el comportament d'un determinat material al passar per ell el corrent elèctric. Trobem materials aïllants, conductors i semiconductors.

Finalment, cal tenir el compte el fenòmen de l'**atenuació**, que és la pèrdua de potència sofrida per una senyal al transitar per qualsevol medi de transmissió.

2.2 Tipus de cablejat de xarxa

- **Cablejat metàlic**: transmeten la informació mitjançant **impulsos elèctrics**.
- **Parell trenat (TP = Twisted Pair)**
- **Coaxial**
- **Cables de fibra òptica**: transmeten la informació mitjançant **rajos de llum**.

2.2.1 Cable de parell trenat

Està compost per:

- Una o més parelles de filaments metàl·lics aïllats (normalment de coure).
- Parelles trenades entre si.
- Recobriment mitjançant funda protectora.



Constitueixen el mode més **simple i econòmic** de tots els medis de transmissió.

Es tracta d'un cable molt **susceptible a interferències electromagnètiques (EMI)** i per tal de reduir-les tenim dues actuacions:

- **Trenar els parells** de mode que les intensitats de transmissió i recepció anulen perturbacions electromagnètiques.
- **Apantallar** els cables, és a dir, emprar un protector que els aïlle de les interferències.

Efecte de Crosstalk

El **crosstalk**, o diafonía, és un fenomen en què els senyals elèctrics transmesos en un conductor afecten involuntàriament conductors adjacents. Això pot provocar interferències i distorsió en les comunicacions, especialment en cables o línies elèctriques pròximes.

El **crosstalk** pot ser causat per diversos factors, com ara la proximitat física dels conductors, la capacitat i inductància entre ells, o problemes d'apantallament inadequat. **En entorns de xarxa, el crosstalk pot conduir a errors de transmissió, pèrdua de senyal i reducció de la qualitat de la comunicació.**

Per mitigar els efectes del **crosstalk**, es poden prendre mesures com utilitzar cables **apantallats**, mantenir distàncies adequades entre conductors, o implementar tècniques de cancel·lació de diafonia.

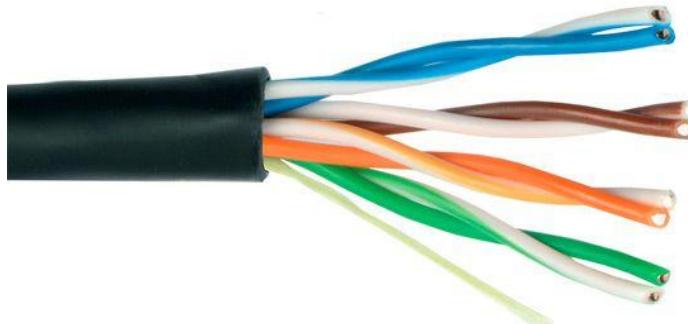
Cable UTP

UTP (Unshielded Twisted Pair) significa *parell trenat sense pantalla/escut*.

Les seues principals característiques són:

- És sensible a interferències.
- Ofereix un gran ample de banda.
- És simple i barat.
- És flexible i fàcil d'instal·lar.
- Connecta habitualment estacions de treball, terminals i dispositius.

Tot açò fa que siga **el cable més emprat per a comunicar xarxes d'ordinadors**.

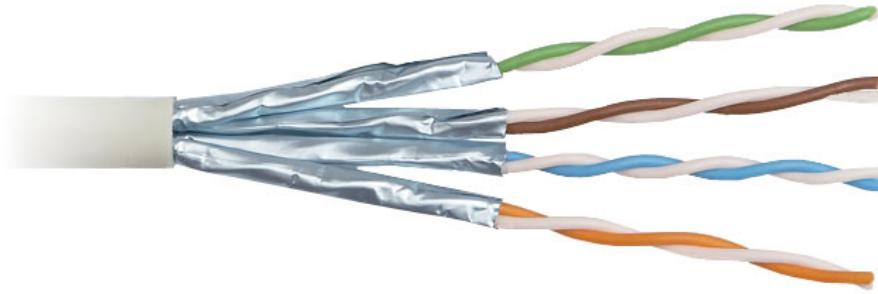


Cable STP

STP (Shielded Twisted Pair) significa *parell trenat apantallat*.

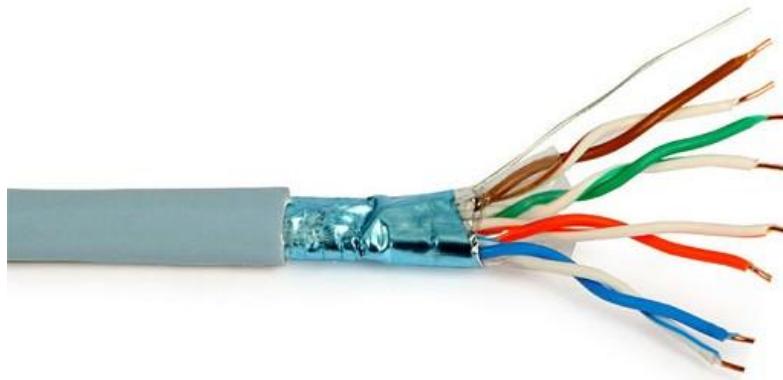
Es tracta d'un cable apantallat, molt similar a l'UTP però amb un recobriment per a cada parella de cables (normalment metàlic). El recobriment ha de conectar-se a la terra de la instal·lació per a les derivacions elèctriques.

L'esmentat recobriment **redueix el soroll** exterior del cable produït per interferències electromagnètiques (EMI) i de radiofreqüència (RFI). També redueix el soroll elèctric dins del cable. Al tractar-se d'un cable més protegit pot treballar amb distàncies i freqüències majors.



Cable FTP

FTP (Foiled Twisted Pair) significa *parell trenat amb pantalla global*. És semblant al STP, però el recobriment és exterior i global.



Les cables STP i FTP tenen alguns desavantatges

- Falta de flexibilitat
- Incòmodes d'instal·lar
- Més cars que el cable UTP

Per aquestes raons, normalment sols s'empren en línies troncals o en llocs molt exposats a interferències electromagnètiques.

Classificació de cables de parell trenat

Dintre dels **parells trenats** podem distingir **2 classificacions**:

- **Les categories:** cada categoria especifica unes característiques elèctriques per al cable: atenuació, capacitat de la línia, freqüència de treball màxima...
- **Les classes:** cada classe especifica les distàncies permeses, l'ample de banda aconseguit i les aplicacions per a les quals és útil en funció d'aquestes característiques.

Categoría	Freqüència màxima	Velocitat màxima	Ús
Cat.3	16 Mhz	10 Mbps	Obsolet
Cat.4	20 Mhz	20 Mbps	Obsolet
Cat.5	100 Mhz	100 Mbps	Xarxes Fast Ethernet
Cat.5e	[100-350] Mhz	1 Gbps	Xarxes Fast/Gigabit Ethernet
Cat.6	250 Mhz	1 Gbps	Xarxes Gigabit Ethernet
Cat.7	600 Mhz	10 Gbps	Xarxes Gigabit Ethernet i futures

2.2.2 Cable coaxial

Degut al seu tipus d'apantallament és menys susceptible a interferències (EMI) que el parell trenat.

Està compost per una malla de coure recobert d'una capa aïllant flexible. També pot estar fet d'alumini recobert d'estany (més econòmic).

Permet cobrir majors distàncies (entre 500 m i diversos km) i connectar un major nombre d'estacions en una línia compartida.

Degut a la seua duresa i poca flexibilitat ha deixat d'emprar-se en instal·lacions de cablejat estructurat, però continua utilitzant-se en la distribució de TV per cable.



• AVANTATGES:

- Arriba a majors distàncies que el cable UTP o STP (500m vs 100m).
- Més econòmic que la fibra òptica.
- Major blindatge que el cable UTP.

• DESAVANTATGES:

- Instal·lació més costosa.
- Major dimensió per la seua grossor.
- Més rígid.
- És necessària una connexió elèctrica sòlida en els extrems. En cas contrari, apareix soroll elèctric que interfereix en la transmissió de la senyal. Per eixa raó, no és suportat pels estàndards actuals.

	COAXIAL		PARELL TRENAT	
	GROS	FI	UTP	STP/FTP
Velocitat de transmissió	1 Gbps	10 Mbps	1 Gbps	1 Gbps
Longitud màxima del segment	1-2 km	200 m	100 m	100 m
Inmunitat front interferències	Màxima	Bona	Mínima	Bona
Connectors emprats	Transceptor	BNC	RJ45	RJ45
Flexibilitat física	Baixa	Mitjana	Màxima	Mitjana
Dificultat d'instal·lació	Alta	Baixa	Baixa	Alta
Cost	Alt	Baixa	Molt baix	Baix

2.2.3 Fibra òptica

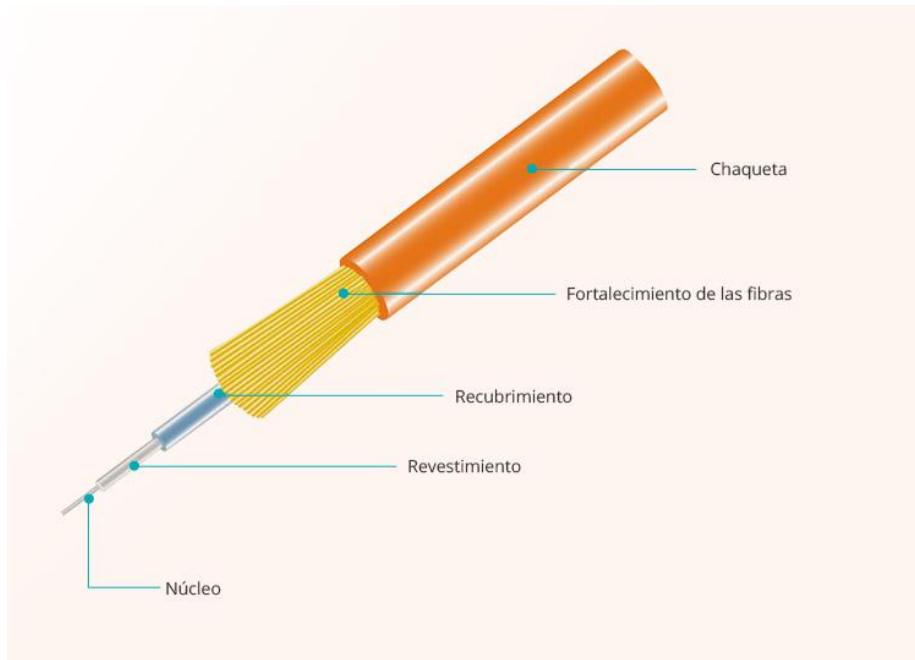
La fibra òptica permet la **transmissió de senyals lluminoses**. Sol ser de vidre o altres materials plàstics.



Al no emprar corrent elèctrica per a la transmissió és totalment **insensible a les interferències electromagnètiques (EMI)**.

Un cable de fibra òptica consta de:

- un nucli fibrós a través del qual viatja la senyal lluminosa.
- un revestiment que impedeix que es filtre la llum.
- una coberta que protegeix i aïlla el cable.



Com a **font del senyal** sol emprar-se:

- Làser
- Diodes LED

Carracterístiques generals de la fibra òptica

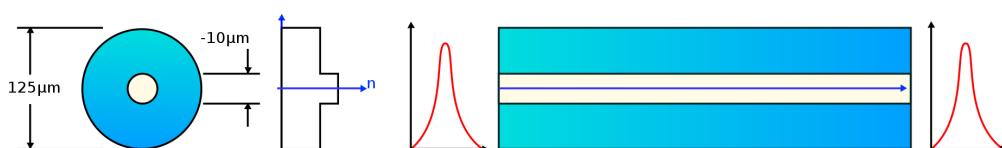
- Cobreix grans distàncies (km).
- Gran ample de banda: superior als 10 Gbps. Un sol cable de fibra òptica pot transportar desenes de milers de trucades telefòniques.
- Taxa d'error molt baixa.
- Sol instal·lar-se en grups, en forma de mangueres, amb un nucli metàlic que serveix de suport i protecció.
- Els principals inconvenients de la fibra són la fragilitat i la dificultat per a realitzar una bona connexió de diverses fibres. Un correcte connexionat evita reflexions de la senyal i una milloria de la qualitat de la transmissió.
- Actualment s'utilitzen dos tipus de fibres òptiques:
 - Fibres mono-mode
 - Fibres multi-mode

Fibra òptica mono-mode

Sols es propaga un mode de llum.

S'aconsegueix reduint el diàmetre de la fibra fins un tamany que sols permet un mode de propagació.

La seu transmissió és paral·lela a l'eix de la fibra. Grans distàncies (300 km) i elevades taxes de transferència (desenes de Gbps).



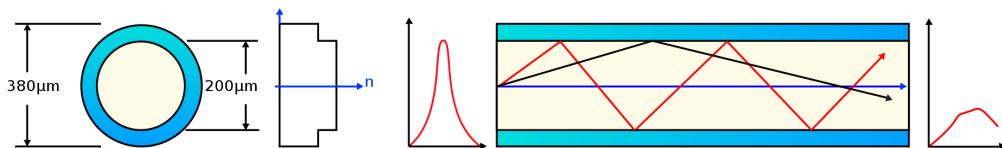
Fibra òptica multi-mode

Els rajos de llum poden circular per més d'un mode o camí. Se suposa que no arriben tots a la vegada.

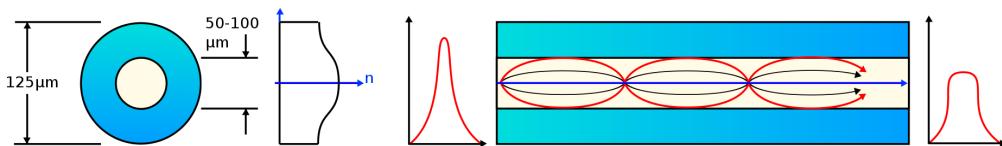
Pot tenir més de mil modes de propagació de llum. Les fibres multi-mode s'utilitzen comunament en aplicacions de curta distància, menors a 1 km; és simple de dissenyar i econòmic.

Tenim dos alternatives:

- **Índex escalonat:** té un índex de refracció constant en tota la secció cilíndrica.



- **Índex gradual:** l'índex de refracció a l'interior del nucli no és únic i decreix quan es desplaça del nucli fins la coberta.

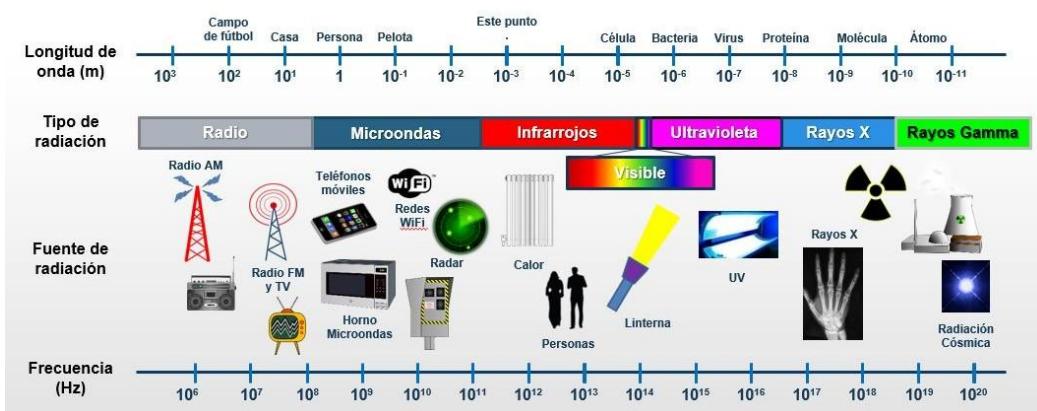


2.3 Transmissions sense fil

Les tecnologies sense fil empren **ones electromagnètiques** per transportar la informació entre els dispositius.

Alguns tipus d'ones electromagnètiques no son adequades per transportar dades. Altres, estan regulades per governs. Algunes àrees de l'espectre s'han reservat per a ús públic sense tindre que demanar permisos.

L'espectre electromagnètic inclou **bandes de transmissió de radio i televisió, llum visible, rajos X i rajos gamma**. Cadaascun d'aquests elements té un rang específic de longitud d'ona.



Les longituds d'ona més emprades per a comunicacions sense fil públiques son la **infraroja i la part de radiofreqüència (RF)**:

- Ona curta (freqüències de MHz): emprades en **radio i TV**.
- Microones (freqüències de GHz): emprades en **telefonia mòbil**.
- Transmissions via satèlit: emprades en **geolocalització** amb freqüències de fins a 1000 GHz.

Els **avantatges** que aporten les comunicacions sense fils a les LAN són:

- Comoditat
- Facilitat de configuració
- Flexibilitat

Tant l'emissor com el receptor han de tenir una **antena** que els permeta **enviar/rebre** la senyal.

Com a norma, a major freqüència, major velocitat. De la mateixa manera, a major velocitat, major atenuació.

Els **sistemes sense fils** emprats en xarxes informàtiques són:

- Bluetooth
- Infrarrojos
- Wifi
- WiMax

2.3.1 Infrarrojos (IR)

- Transmeten senyals de dades mitjançant diodes d'**emissió de llum** (LED o làser). La informació **no pot viatjar a través d'obstacles**.
- Emprat per connectar i transportar dades entre dispositius com PDA i PCs. Utilitza un **port de comunicacions especial** anomenat **irDA**.



2.3.2 Radiofreqüència (RF)

Algunes bandes de radiofreqüències s'han reservat per a l'ús de dispositius sense llicència, com les **LAN sense fil, telèfons sense fil, perifèrics d'ordinadors...**

- Les ones **poden atravesar parets i altres obstacles** i per tant tenen major cobertura que els IR.
- Per a **LAN sense fil existeixen diferents normes/estàndards**. Els més coneguts són:
 - IEEE 802.11b
 - IEEE 802.11a
 - IEEE 802.11g
 - IEEE 802.11n
 - IEEE 802.11ac
 - IEEE 802.11ax
- Altres tipus de comunicació per radiofreqüència són el **bluetooth** i les **microones**.

Bluetooth (BT)

Especificació per a xarxes sense fil d'àrea personal (WPAN) que possibilita la transmissió de veu i dades entre diferents dispositius mitjançant un enllaç per radiofreqüència en la banda dels **2'4GHz**.

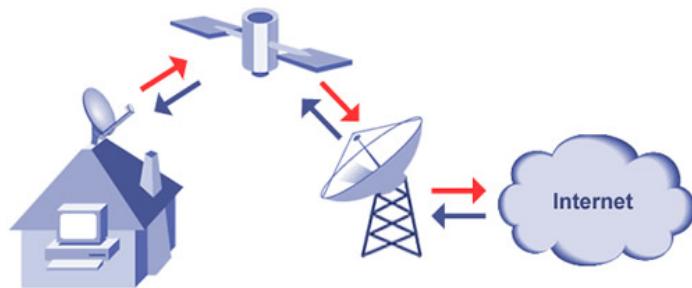
Aquesta norma facilita les comunicacions entre equips mòbils, elimina el cablejat i connectors i ofereix la possibilitat de crear xicotetes xarxes sense fil i facilitar la sincronització de dades entre equips personals.



Microones

Es tracta d'un tipus eficaç de transmissió de dades sense fils.

- **Terrestre:** empra dues torres de microones amb **camp de visió clar** entre elles; per tant, no han d'ahver-hi obstacles per interrompre l'esmentat camp visual. La freqüència de transmissió de dades dels sistemes terrestres és de 4 GHz a 23 GHz, mentre que les **velocitats soles** estar entre **1Mbps i 10 Mbps**.
- **Satèlit:** giren a vora 40.000 km sobre La Terra. Les estacions terrestres envien i reben senyals de dades cap i desde el satèl·lit amb freqüències que oscilen entre 11 GHz i 14 GHz, amb velocitats de desenes de Mbps.



LAN sense fils (WiFi)

Les transmissions en LANs sense fil arriben a velocitats de transmissió moderades, encara que amb l'aparició del 802.11n i posteriors s'arriben a "altes" velocitats (>300 Mbps). Les distintes versions de WiFi que existeixen estan descrites a la normativa [IEEE 802.11](#). A la següent taula podem veure les principals característiques de les variants que s'utilitzen actualment.

Norma IEEE	Nom WIFI	Freq.	Velocitat	Alcanç	Característiques
802.11b	Wifi1	2.4GHz	11Mbps	30-90m	Estàndar original
802.11a	Wifi2	5GHz	54Mbps	10-25m	No compatible amb b,g,n. Gestió d'energia roïn
802.11g	Wifi3	2.4GHz	54Mbps	30-45m	Més ràpid i compatible amb 802.11b
802.11n	Wifi4	2.4/5GHz	300-600Mbps	30-60m	Més ràpid i compatible amb b,g
802.11ac	Wifi5	5GHz	800Mbps-1.6Gbps	30-45m	Utilitza components que consumeixen menys energia
802.11ax	Wifi6	2.4/5/6GHz	5Gbps	30-60m	Millor gestió de dispositius amb xarxa congestionada.

WIMAX

Les transmissions en **WIMAX** segueixen la normativa IEEE 802.16. Semblant al WIFI però amb cobertures majors a canvi de velocitats menors.

	WIFI (802.11)	WIMAX (802.16)
Alcanç	100m	50km
Cobertura	Interior	Exterior
Freqüència	2.4GHz a 6GHz	20Mhz
Velocitat	1Gbps	75Mbps

3. UD3. Instal·lació física d'una xarxa (II). Dispositius de connexió

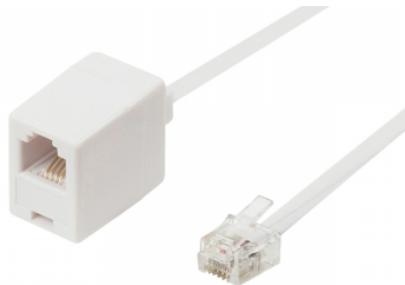
3.1 Connectors per a xarxes

La **funció** dels connectors és introduir el senyal de l'emissor al cable i adequar el senyal del cable a l'interfície del receptor.

Freqüentment, els connectors d'una mateixa família es dupliquen en forma de **mascle i femella**, que han d'acoplar-se mecànicament a la instal·lació.

3.1.1 Connector RJ11

- Emprat majorment per enllaçar xarxes de **telefonia**.
- Dimensions reduïdes i amb 2, 4 o 6 contactes.
- És el connector més difós globalment per a la connexió de dispositius telefònics convencionals, on es solen emprar generalment tan sols els dos pins centrals per a una línia simple.



3.1.2 Connector RJ45

- És el connector més emprat per connectar **xarxes de cablejat estructurat**. Sol emprar cables **UTP** o **STP**.
- Està format per **8 pins** als quals van connectats cadascun dels cables del parell trenat.



3.1.3 Connector BNC

- Emprat amb **cables coaxials** a les primeres **ethernet**, durant els anys 80.
- Consisteix en un connector de tipus mascle en cada extrem del cable. Aquest connector tenen un centre circular connectat al conductor del cable central i un tub metàlic connectat a la part exterior del cable. Un anell que rota a la part exterior assegura el cable mitjançant un mecanisme de bayoneta i permet la connexió a qualsevol connector BNC de tipus femella.



3.1.4 Connector DB9

- Originalment DE-9. S'empra principalment per **connexions en serie** perquè permet una **transmissió asíncrona de dades** segons els que estableix la normativa **RS-232**.
- Actualment poc emprats, tan sols en alguns dispositius específics.



3.1.5 Connector DB25

- Connector analògic de **25 pins**.
- S'emprava molt per connectar impresores i per aquest motiu se li coneix com **el port de la impressora (LTP)**.
- S'empra per a connexions en serie i en paral·lel, per aquesta raó, generalment, els ports de serie tenen connectors masclles i els ports paral·lels, femella.



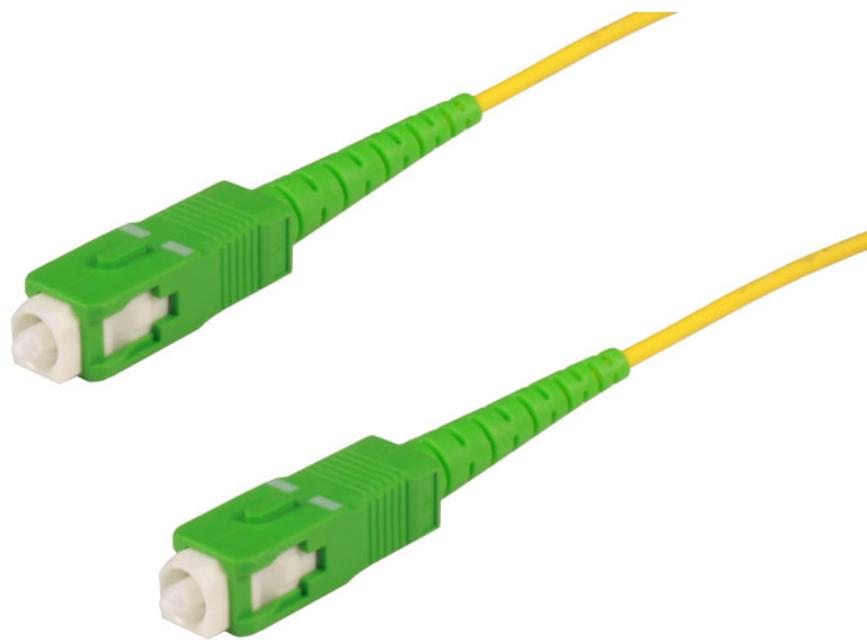
3.1.6 Connector ST (Fibra)

- Ha sigut durant molt de temps el més emprat per finalitzar **fibres òptiques multi-mode (FMM)**, avui en dia està en desús, no obstant segueix present en moltes instal·lacions.
- Presenta un sistema d'anclatge per **bayoneta** que el converteix en un model molt **resistent a les vibracions** i el feia especialment indicat en entorns exigents.



3.1.7 Connector SC (Fibra)

- S'empra habitualment en instal·lacions de fibra òptica. Sol gastar-se en **Switchs Gigabit Ethernet**.
- La connexió de la fibra al connector requereix d'un poliment de la fibra i la aliniació de la fibra amb el connector.
- Aquests connectors han anat substituint als connectors ST en cablejats estructurats, fonamentalment per ser **més fàcils de conectar**.



3.2 Ferramentes

La creació de les connexions de la xarxa ha de realitzar-se amb molta cura. La major part dels problemes de les xarxes d'àrea local estan relacionats amb problemes de cablejat o als connectors.

Les ferramentes que gastarem, dependran del tipus de cable i connector utilitzat, però quan parlem de cablejat estructurat són molt comuns:

- **Grimpadora**
- **Aletes i ferramentes de tall**
- **Pela-cables**
- **Ferramentes d'impacte**
- **Comprovador de cables**



Altres ferramentes útils son:

- **Brides:** elements plàstics que amarren els cables entre sí als armaris o canaletes.
- **Etiquetes:** sistemes d'informació que s'adjunta a cada cable per tal de tenir-lo identificat en tot moment. Es poden fer servir etiquetes clàssiques o generades amb una **etiquetadora**.
- **Macarrons termoretràctils:** Cables buits contruits amb un material plàstic que s'arrupix quan se li aplica calor per tal de reforçar la unió del cable amb el connector.

3.3 La targeta de xarxa

Es tracta d'un xicotet circuit imprés que, habitualment, es coloca en un slot d'expansió de la placa base de l'ordinador; existeixen externes en format USB. També es coneixen com *Adaptador de xarxa* o *NIC (Network Interface Computer)*.

Treballa al **nivell 2** (enllaç) del model OSI.



Cada targeta de xarxa porta un nom codificat únic, denominat adreça de control d'accés al medi (**MAC**) i és únic en el mòn.

Aquesta adreça és molt important degut a que identifica perfectament i de forma única a l'ordinador orige i destí.

Factors a tenir en compte al moment de triar una targeta de xarxa:

- **Protocols:**

- Ethernet
- Token Ring
- FDDI

- **Tipus de medi:**

- Cable de parell trenat (RJ45)

- Cable coaxial (BNC)

- Sense fil

- Fibra Òptica

- **Connexions amb l'ordinador:**

- Bus PCI
- Bus PCI Express
- USB

- **Velocitat màxima:**

- 100 Mbps
- 1000 Mbps
- 10 Gbps

3.3.1 Configuració de l'adaptador de xarxa

Cada Sistema Operatiu té una forma d'accendir als adaptadors de xarxa. Quan accedeixes a les seues propietats pots consultar l'adreça IP, la porta d'enllaç o els DNS.

En sistemes **Linux**, es pot accedir a molta d'aquesta informació mitjançant el comandament `ip` a llançat en un terminal.

```
[paco@tufdash ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
    altname enp0s31f6
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
    inet 192.168.200.45/24 brd 192.168.200.255 scope global dynamic noprefixroute wlo1
        valid_lft 569sec preferred_lft 569sec
    inet6 fe80::6f75:fb11:e814:f9ba/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Per altra banda, en sistemes **Windows**, aquesta informació està disponible mitjançant el comandament `ipconfig /all` del terminal de Windows (Símbol del sistema)

3.4 Model TCP/IP

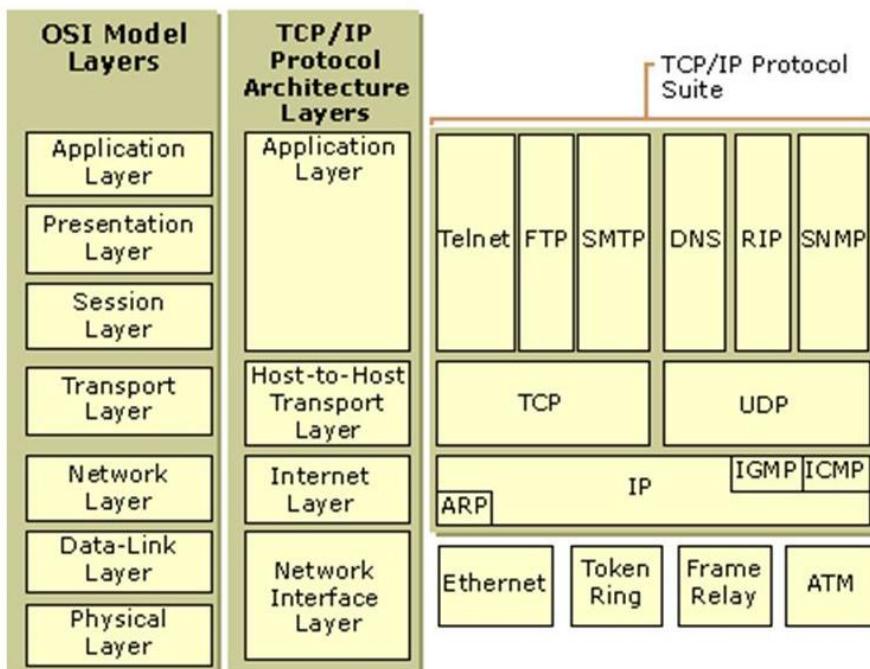


Per què el model OSI no tingué èxit i el model TCP/IP sí?

- El **model OSI** fou creat abans d'implementar la programació de cadascuna de les capes. Al portar-lo a la pràctica no tingué la repercusió que s'esperava perquè era un **model molt complexe**, amb capes de distinta "grossor" i algunes funcionalitats mal situades, per exemple, el xifrat.
- El **model TCP/IP** és un model **més pràctic**. Primerament es varen dissenyar els protocols i a posteriori s'integraren per capes a l'arquitectura.
- El **model TCP/IP** és molt **més simple**, de fet redueix les capes de 7 a 4.

El model TCP/IP és l'arquitectura en la qual es basa Internet. És un model de 4 capes i reb el nom dels seus protocols majoritaris:

- **TCP (Transmission Control Protocol)**: treballa en el nivell 4 de OSI i per tant realitza tasques de **transport**.
- **IP (Internet Protocol)**: treballa al nivell 3 del model OSI i per tant realitza tasques d'**encaminament**.



Les capes del model TCP/IP són:

- **Subxarxa (Accés a la xarxa)**: proporciona la transmissió de les dades independentment de la xarxa que estiga configurada. És la capa encarregada de convertir el senyal analògic/digital. També realitza el **control de fluxe** per evitar que els equips ràpids colapsen als més lents.
- **Interxarxa (Internet)**: És la capa més important donat que és l'encarregada de transmetre **datagrames** emprant com adreçament l'**adreça IP**. Durant la transmissió pot passar per distintes xarxes diferents i les dades poden arribar al destí desordenades.
- **Transport**: S'encarrega d'establir una comunicació entre origen i destí. Introduceix el concepte de **port** per comunicar diverses aplicacions d'una mateixa màquina. S'encarrega de dividir els **segments** de dades que li arriben de la capa d'aplicació, **ordenar les dades** que li arriben de la capa inferior i controlar errors.
- **Aplicació**: Conté les **aplicacions de xarxa** que empraran els serveis oferts per les capes inferiors per enviar **dades**.

3.4.1 Protocol IP

- El protocol IP realitza tasques bàsiques d'encaminament per conseguir transportar dades des d'un origen fins un destí.
- L'origen i el destí pot estar en xarxes amb tecnologies totalment diferents i pot hi haver diverses rutes possibles pel que haurà de prendre decisions i triar la millor.
- No hi ha seguretat a l'entrega.

- No hi ha control d'errors.
- Els paquets poden arribar desordenats.
- Els equips d'una xarxa tenen associat un número anomenat adreça IP (adreça lògica, no confondre amb el número MAC de l'adaptador de xarxa que és l'adreça física) que permet identificar-los en tot Internet. L'adreça IP està formada per 4 números separats per punts, cadascun dels quals pot prendre valors entre 0 i 255. Exemple: 192.168.0.1
- Màscara de xarxa: És un número similar a l'adreça IP i determina quina part de l'adreça IP pertany a l'equip i quina part pertany a la xarxa. S'utilitza per crear subxarxes. Exemple: 255.255.255.0

3.4.2 Protocol TCP

- El TCP és un protocol per al control de la transmissió de dades.
- Es va dissenyar per a realitzar connexions segures en xarxes insegures.
- Soluciona els problemes existents en IP:
- Aporta control d'errors.
- Seguretat a l'entrega.
- Control de fluxe. Els paquets arriben ordenats.
- Es complementa de manera perfecta amb IP per aportar una comunicació de dades fiables i ordenada. Per això, en ocasions, es fa referència a TCP/IP com si d'un protocol es tractara, però realment son dos.
- Els punts d'accés al servei (SAP en OSI) en la capa de transport s'anomenen **sockets**, ports o connectors TCP/IP. Darrere de cada socket s'implanta un servei de xarxa. Per exemple: 80 és el port que identifica les peticions de xarxa cap a un servidor web. Quan algú a la xarxa requereix un servei, envia un missatge al socket o port que identifica el servei. Alguns serveis requereixen més d'un socket per al seu funcionament.

3.5 Ethernet

Ethernet és un estàndard de xarxes d'àrea local per a ordinadors. Es tracta d'un estàndard *de facto* perquè no ha sigut desenvolupat per ninguna organització, ha nascut a partir de productes de la indústria amb un gran èxit al mercat.

El terme *Ethernet* ve de la unió de dues paraules: *Ether* (*Éter; matèria que uneix totes les coses*) i *net* (*xarxa*). Per tant, en termes informàtics, **Ethernet** significa **Xarxa que uneix tots els equips**.

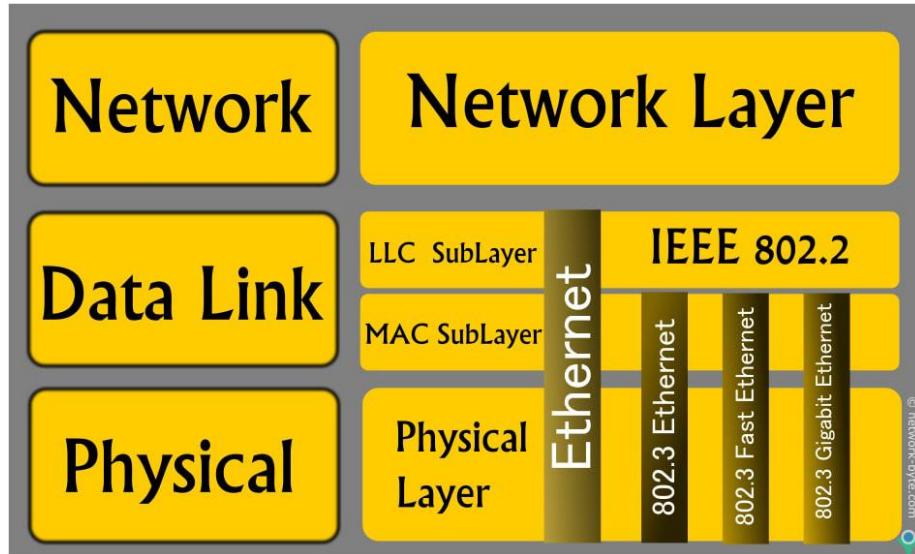
Defineix les caraterístiques de cablejat i senyalització del nivell físic (OSI) i els formats de les *trames de dades* del nivell d'enllaç (OSI). Començà amb xarxes de velocitat de 10Mbps i actualment existeixen xarxes Ethernet a 10Gbps.

3.5.1 Projecte 802

- Ethernet pertany al projecte **IEEE 802**. Aquest és un conjunt d'estàndards pertanyents a l'Institut d'Enginyers Elèctrics i Electrònics (IEEE), que actua sobre xarxes d'ordinadors, concretament i segons la seua propia definició, sobre xarxes d'àrea local (LAN) i xarxes d'àrea metropolitana (MAN). Alguns dels quals són ben coneeguts: Ethernet (IEEE 802.3) o Wi-Fi (IEEE 802.11).

- Es centra en definir els nivells més baixos (segons el model de referència OSI), concretament subdivideix el segon nivell, el d'enllaç, en dos subnivells: enllaç lògic (802.2) i el d'accés al medi (MAC). La resta dels estàndards recullen tant el nivell físic (OSI), com el subnivell d'accés al medi (MAC).

Projecte	Descripció
IEEE 802.1	Normalització interfície i relació amb el model OSI
IEEE 802.2	Control d'enllaç lògic (LLC)
IEEE 802.3	Mòduls MAC. CSMA/CD
IEEE 802.4	Bus amb pas de testic (Token bus)
IEEE 802.5	Anell amb pas de testic (Token ring)
IEEE 802.6	MAN
IEEE 802.8	FDDI (Fibra òptica)
IEEE 802.9	Veu i dades en LANs
IEEE 802.10	Seguretat
IEEE 802.11	Xarxes sense fil (WLAN)
IEEE 802.15	Bluetooth
IEEE 802.16	WiMAX



Nivell LLC (Logic Link Control)

Nivell compartit per tots els protocols de la família Ethernet. S'encarreha de:

- La lògica dels reenviaments
- Control de fluxe
- Comprovació d'errors

Nivell MAC (Medium Acces Control)

- S'encarrega del control d'accés al medi compartit (cables en bus, radio...).
- No s'utilitza en protocols punt a punt (no hi ha medi compartit).

- **Adreça MAC:** sistema d'adreçament de nivell 2 (enllaç).
- **Protocols MAC** de nivell d'enllaç:
 - Token Ring | Token Bus
 - CSMA/CD (emprat per Ethernet)

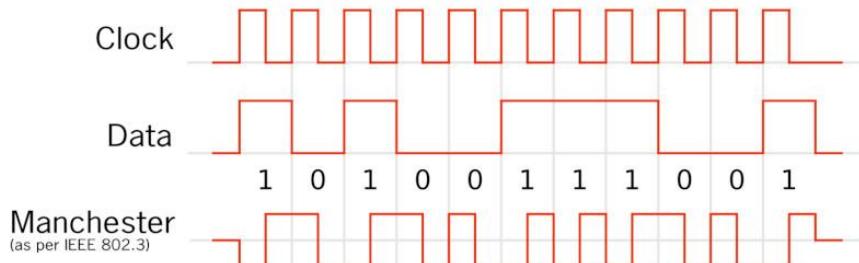
Nivell Físic Ethernet

- Quan s'utilitza la **norma 802.3 per a xarxes Ethernet** s'utilitza com a sistema de transmissió digital (0's i 1's) la codificació **Manchester**.



La codificació MANCHESTER

- **Avantatge:** És una senyal molt **robusta**. Evita problemes típics d'altres sistemes de codificació (unipolar, NRZ, RZ).
- **Desavantatge:** Consumex el doble de temps (ample de banda) al tractar-se d'una comunicació **bifàsica**.
- **0 lògic:** es representa mitjançant una **baixada** de senyal de +0.85V fins a -0.85V.
- **1 lògic:** es representa mitjançant una **pujada** de senyal de -0.85V fins a +0.85V.
- **Canal inactiu:** es representa mitjançant una senyal a 0V.



3.5.2 Comprovació d'errors al nivell d'enllaç LCC

Existeixen distints **codis detectors** d'errors per comprovar si una trama té bits erronis o no. Un dels més senzills és l'anomenat **codi de paritat simple**. Es basa en comptar el nombre de 1's que té la cadena de bits a transmetre i afegir al final de la cadena un dígit més: un 0 (si té un nombre parell de 1's) o un 1 (si la cadena original té un nombre imparell de 1's).



Exemple de codi de paritat simple

La cadena "11001" conté 3 1's, al ser un nombre imparell, la cadena final emprant codi de paritat simple seria "110011".

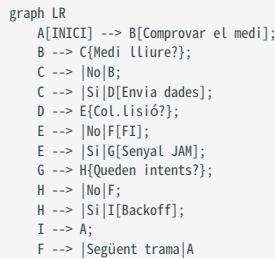
Altres codis que existeixen, i que per la seua complexitat no anem a veure en aquest curs, són:

- Codi basat en la **redundància cíclica (CRC)**
- **Codi de Hamming**

3.5.3 Algorisme CSMA/CD

- **Carrier Sense (Sentit de Portadora):** Les estacions escolten el medi abans d'enviar dades per assegurar-se que està lliure.
- **Multiple Access (Accés Múltiple):** Múltiples estacions tenen l'accés simultani al medi compartit, com un cable d'una xarxa local.
- **Collision Detection (Detecció de Collisions):** Si dues estacions intenten transmetre alhora i es produeix una col·lisió, aquesta és detectada. Les estacions interrompen la transmissió, esperen un temps aleatori i tornen a intentar.

Aquest algorisme era utilitzat en les primeres implementacions de **xarxes Ethernet amb topologia de bus**, però ha disminuït amb l'ús de topologies més eficients com estrelles i commutadors (*switches*). Les xarxes modernes prefereixen protocols com **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*) per una gestió més eficient dels recursos i la prevenció de col·lisions.



3.5.4 Tipus d'Ethernet

Ethernet	Medi transmissió	Longitud màxima per segment	Característiques
10Base5	Coaxial 50W	500m	Especificació original de Ethernet i utilitza coaxial gros
10BaseTX	UTP	100m	Empra cables de parell trenat UTP per a transmissions fins a 10Mbps
1000BaseTX	4 parells UTP	100m	Velocitats fins a 1000Mbps amb cablejat mínim de cat 5e
1000BaseLX	Fibra Òptica	550m	Velocitats de 1000Mbps però emprant la fibra com a medi de transmissió

Tíuc nemotècnic

- Normalment la **primera part** identifica la **velocitat** de la xarxa: 10 = 10Mbps, 100 = 100Mbps, 1000 = 1000Mbps
- La **segona part** indica el **tipus de senyal** que es transmet: digital de banda base (BASE) o senyal modulada (BROAD).
- La **tercera part** pot ser un número o una lletra:
 - Si és un número indica la **distància** que permet: 5 = 500m, 2 = 200m
 - Si és una lletra sol indicar el **tipus del cable**: T = Parell trenat (Twisted) F / SX / LX = Fibra òptica

3.6 Cablejat de xarxa

3.6.1 Enrutament del cablejat

La forma més senzilla de posar el cablejat és **posar-lo a la vista**. Sols podrem emprar aquest mètode si estem segurs que el cablejat no serà colpejat ni estirat.

Per montar cables sobre la paret necessitarem dispositius que puguen fixar-los:

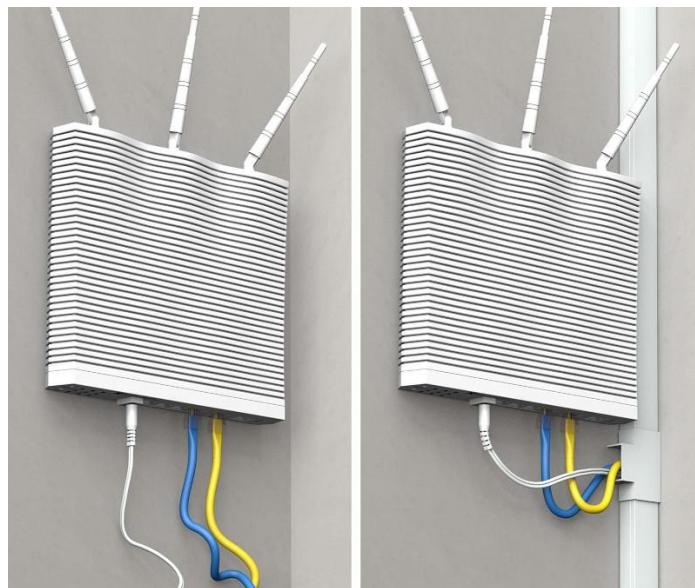
- Brides de cables adhesives (si no hem de moure'l's mai).
- Brides de cables amb forats perforats (si hem de moure'l's alguna vegada).
- MAI** emprarem grapes! (TIA/EIA-568A)



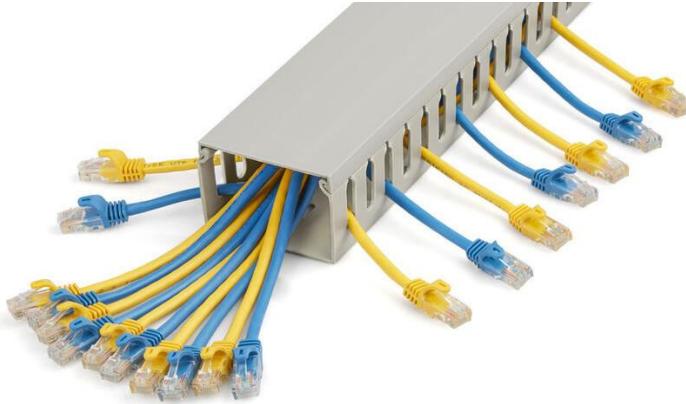
3.6.2 Muntatge de cables en canaletes

Podem muntar els cables emprant diferents tipus de canaletes:

- Canal montat sobre la paret amb coberta móvil:
- Canaleta decorativa
- Millor acabament
- S'empra per col·locar el cable sobre una paret on quedarà visible.



- Canal:
- Alternativa menys atractiva
- Suficientment gran com per contindre diferents cables
- Emprada generalment en espais poc visibles



Normes de seguretat personal en el muntatge de canaletes

1. Desconectar de la llum tots els circuits que passen per el lloc de treball.
2. Abans de treballar, tenir localitzats els extintors d'incendis.
3. Emprar roba adequada.
4. Si es treballa amb sostres falsos s'ha d'inspeccionar la zona.
5. Si hem de tallar o serrar, cal protegir-nos els ulls amb ulleres de seguretat.
6. Consultar al tècnic de manteniment si hi han materials perillosos.
7. Mantenir la zona de treball ordenada i protegida.

3.6.3 Suport de cablejat horitzontal

- Molts instaladors extenen el cablejat per àtics o falsos sostres, així no queden a la vista.
- No s'han de col·locar els cables directament sobre els panells de sostre, hem d'emprar suports especials o bastiments.



3.6.4 Muntatge d'armaris i patch-pannels

El panell de connexions o *patch pannel* és un dispositiu d'interconnexió que agrupa pins i ports i solen presentar la següent estructura:

- Part frontal: Ports de connexió RJ45 mascle.
- Part posterior: Fils i pins per a connexions RJ45 femella.
- Connexions elèctriques



3.6.5 Personal

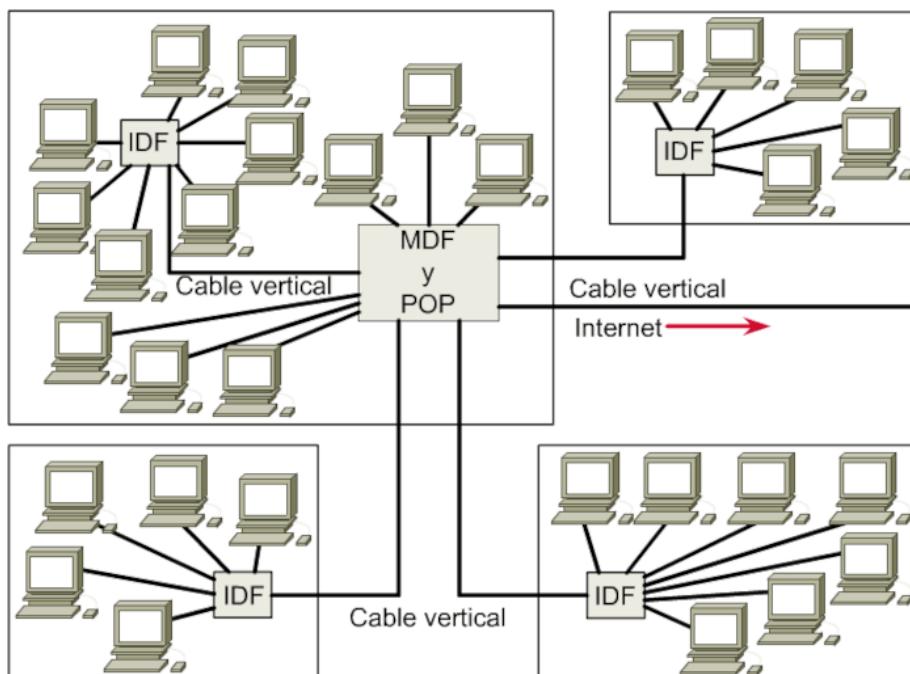
En instal·lacions de xarxes mitjanes o grans, podem trobar-nos amb diferents persones, cadascuna d'elles amb tasques distintes:

- **Gerent de projecte:** s'encarrega d'escriure la documentació, supervisar el projecte, controlar el personal, les dates d'inici i acabament, certificacions, normatives de seguretat...
- **Gerent de materials:** s'encarrega de les caixes de ferramentes, materials, cablejat, rosetes, switchs, routers... que facen falta per a la instal·lació. Tracta amb proveïdors i ajuda a gerent a establir calendaris d'execució de la instal·lació.
- **Planificador/Col·locador de cables:** planifica per on passen els cables i els col·loca seguint la normativa vigent.
- **Acabador de cables:** realitza les terminacions dels cables (rosetes, connexió) de les àrees de treball.

3.6.6 Termes

Termes habituals que podem trobar-nos en instal·lacions de xarxa:

- **POP (point of presence), punt de presència:** és el punt on arriben els serveis de telecomunicacions a l'edifici i on es connecten amb les instal·lacions de comunicacions a prop de l'edifici.
- **MDF (main distribution facility), centre de distribució principal:** és el lloc de l'edifici on es concentra tota la infraestructura de cablejat i on es connecta amb la companyia telefònica que presta els serveis de veu, dades...
- **IDF (intermediate distribution facility), centro intermedio de distribución:** en edificis de moltes plantes o molt extensos és convenient concentrar previament parts del cablejat en centres més xicotets que es connectaran al *MDF* a través de *backbone* o cable principal.
- **WA (working area), àrea de treball:** és on posem els equips, impressores, dispositius finals de l'usuari.
- **TR (telecommunications room), armari de telecomunicacions:** son els armaris es situen a la planta i recullen el cablejat horitzontal.
- **Cablejat horitzontal:** els cables que es tiren desde les àrees de treball fins l'armari de telecomunicacions situat a la mateixa planta.
- **Cablejat vertical (backbone):** cablejat que connecta entre sí els diferents armaris de telecomunicacions verticalment, entre les diferents plantes de l'edifici. Quan no hi ha armaris també s'asocia al cablejat que uneix distints dispositius de xarxa (*hub, switch, router...*).



3.6.7 Organismes i normativa

El cablejat estructurat està definit com un sèrie de normatives que tenen com objectiu **construir xarxes que treballen al màxim rendiment i que siguin fàcils de modificar o ampliar**. Aquestes normatives no sols afecten al cablejat de xarxa, també al telefònic, CCTV...

Algunes de les organitzacions que creen els estàndards són:

- **ANSI (American National Standards Institute)**, és una organització encarregada de definir estàndards, particularment relacionats amb xarxes de telecomunicació.
- **EIA (Electronic Industry Association)** desenvolupa normativa referent a equips electrònics, targetes de xarxa...
- **TIA (Telecommunications Industry Association)** que ha creat entre d'altres les normes **TIA 568A** i **TIA 568B** que especificuen com s'ha d'instal·lar el cablejat en edificis comercials. En particular, hi han algunes normatives TIA importants:
 - TIA/EIA 568B1: especifica requeriments generals.
 - TIA/EIA 568B3: especifica requeriments de cablejat de parell trenat i fibra òptica.
 - TIA/EIA 569A: especifica com fer passar el cablejat per l'edifici.
 - TIA/EIA 570: normativa de telecomunicacions per a edificis residencials.

4. UD4. Dispositius específics d'una xarxa local

4.1 Introducció

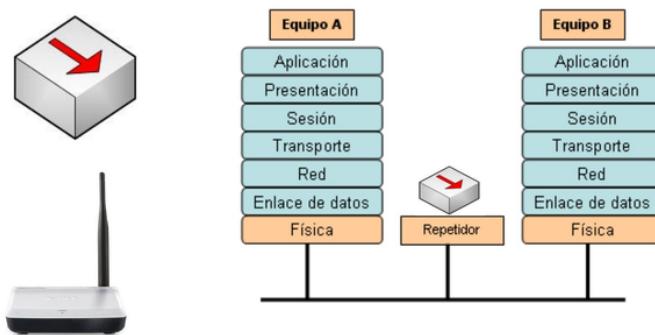
Els dispositius d'interconnexió de xarxes treballen entre els nivells 1 i 3 del model OSI, és a dir, físic, enllaç i xarxa.

Repetidor		Puente	
Hub 10BASE-T		Switch de grup de treball	
Hub 100BASE-T		Router	
Hub		Nube de red	

4.2 Repetidor

El repetidor **rep un senyal atenuat i retorna el senyal al seu estat original**. Per exemple: hem vist que la distància màxima del cablejat UTP és de 100 m, és per això que necessitarem repetidors per tal d'amplificar la cobertura.

Els repetidors treballen a nivell 1 (físic):



L'anomenarem **amplificador** si s'encarrega de regenerar senyals **analògics** i li direm **repetidor** si regenera senyals **dígitals** a escala de bits.

Els repetidors i amplificadors presenten algunes **limitacions**:

- **ATENUACIÓ:** si el senyal arriba massa atenuada, no pot reconstruir-se correctament, per la qual cosa, existeixen distàncies màximes de separació dependent del medi de transmissió.
- **NOMBRE DE DISPOSITIUS:** cada vegada que s'amplifica un senyal analògic s'afegeix un component de soroll. Un senyal no pot travessar un nombre infinit d'amplificadors perquè es distorsionaria massa i no seria una còpia reconstruïda de l'original.

De vegades, **els repetidors es poden emprar per a convertir el senyal d'un sistema de cablejat a altre**. Per exemple, un repetidor podria tindre una entrada 10Base2 (coaxial) i altra 10BaseT (parell trenat).

Els repetidors s'empren tant en **cables de coure** portadors de senyals elèctrics com en **cables de fibra òptica** portadors de llum.

S'empren també als **cables transcontinentals i transoceànics** perquè l'atenuació (pèrdua de senyal) en aqueixes distàncies seria completament inaceptable sense ells.

Un **repetidor wifi**, també anomenat **amplificador wifi** compleix amb les característiques de funcionalitat d'un repetidor perquè recull un senyal que rep i l'amplifica amb l'objectiu d'augmentar el rang del senyal.

4.3 Hub

El hub o concentrador s'encarrega de **regenerar els senyals de xarxa** d'igual forma que un repetidor, però **permets més d'un dispositiu**, per això, de vegades, se'l anomena repetidors multiports.

Els **hubs** es consideren, per tant, dispositius de **capa 1** donat que sols regeneren el senyal i l'envien mitjançant un *broadcast* (envien informació a tota la resta d'equips) a tots els ports.



- **AVANTATGES:**

- Crea un **punt de connexió central** per als ordinadors.
- Augmentem la **fiabilitat** de la xarxa en regenerar el senyal i independitzar cada connexió.
- **Ràpids** perquè no han de processar el senyal. Es limiten a copiar bits.

- **No requereixen configuració.**

- **Barats.**

- **DESAVANTATGES:**

- **No segmenten la xarxa:** si es produueix una col·lisió, aquesta es propaga a tots els segments de la xarxa.
- **Problemes de privadesa:** no és capaç de decidir on s'envia el senyal i ho envia a tots.



Actualment, els hubs estan en desús perquè han sigut substituïts pels switchs i sols podem trobar-ne en instal·lacions antigues.

4.3.1 Tipus de Hubs

- **Hubs pasius:** la seua funció principal consisteix a interconnectar tota la xarxa.
- **Hubs actius:** a banda de la seua funció bàsica de concentrador, també amplifiquen i regeneren el senyal rebut abans de reenviar-lo.

4.3.2 Tipus de connexions al Hub

- **Connectors per unir estacions de treball.**
- **Connectors per a unir-se a altres Hubs:** permeten la connexió de diversos Hubs mitjançant **enllaços especials (creuats)**. De vegades existeix un botó, anomenat *crossover* que ha de mantenir-se actiu per poder unir Hubs. Altres vegades aquest enllaç està sempre actiu i sol tenir el nom d'**uplink**.



4.3.3 Connexió entre Hubs

- **Connexió en cascada:** es permeten fins a 4 Hubs si la xarxa treballa a 10 Mbps o 2 si la xarxa treballa a 100 Mbps. Si es volen connectar més serà necessari emprar repetidors intermedis o emprar connexions en estrela (més recomanable).
- **Connexió en estrela:** Cada Hub connecta el seu port 1 al Hub central. Els cables que els connecten són iguals al de les estacions de treball. Això permet que l'única limitació siga el nombre de ports del Hub.

4.3.4 Topologia Hubs

- **FÍSICA:** s'estableix una **topologia en estrela**.
- **LÒGICA:**
- **BUS(HUB):** la xarxa es comporta com un bus, enviant els senyals que els arriben per totes les eixides. Inconvenient: Si 2 estacions transmeten a la vegada, es produueixen col·lisions.
- **ANELL(MAU):** s'envia el senyal que li arriba per un port al següent.

En ambdós casos el protocol corresponent haurà de controlar qui pot transmetre per tal d'evitar col·lisions.

Info

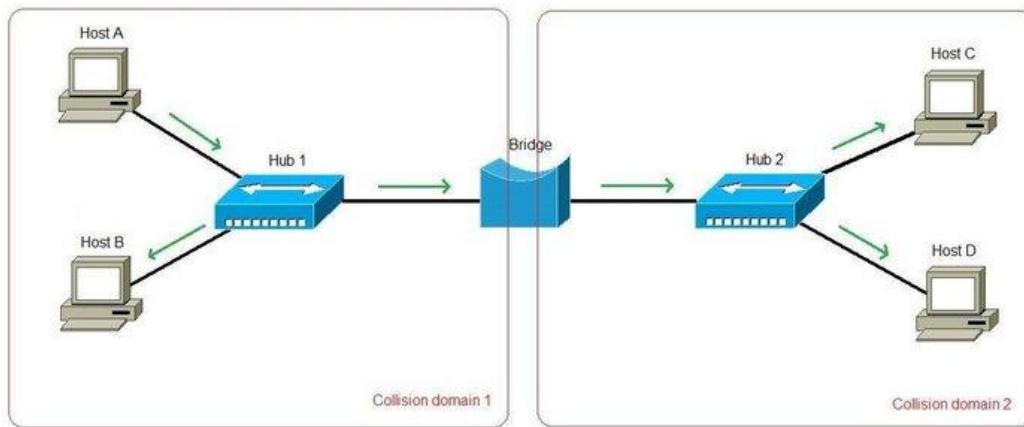
- A les xarxes locals antigues sense concentradors si fallava algun enllaç, tota la xarxa deixava de funcionar i el tècnic havia de comprovar un per un tots els cables i totes les connexions perquè no sabia amb antelació quin havia fallat. Xafar un cable de xarxa o enganxar-se amb ell podia posar "de volta" el departament o l'empresa sencera.
- A les xarxes amb concentradors, en compte de distribuir les connexions, el concentrador les centralitza en un únic dispositiu, mantenint indicadors lluminosos del seu estat i impedint que una d'elles puga fer fallar tota la xarxa. Cada estació es connecta directament al concentrador mitjançant el cable corresponent i, si eixe enllaç falla, la xarxa segueix funcionant i sols queda aïllat l'ordinador afectat.

4.4 Pont o Bridge

Un pont és un **dispositiu de capa 2 (enllaç)** dissenyat per **connectar dos segments LAN**, que poden tenir **diferents topologies i diferents protocols** a nivell MAC i d'enllaç. Per exemple, poden connectar una xarxa *Ethernet* amb una *Token ring*.

Un pont és un dispositiu amb dos ports que tenen certa **capacitat de control**, permetent acceptar i reexpedir trames en funció del seu contingut.

El propòsit d'un pont és **filtrar el tràfic d'una LAN**, perquè el tràfic local seguís essent local, però **permeter la connectivitat a altres parts (segments) de la LAN** per tal d'enviar tràfic dirigit a aquestes altres parts.



Què és un segment d'una xarxa?

Quan la xarxa es divideix en 2 segments es consideren dues parts distintes de la xarxa. Per exemple, la xarxa del pis 1 i la del pis 2 que estan connectades; en una petita empresa que té dues oficines en dos edificis i estan connectats entre si...

Si un pont permet la connectivitat entre 2 segments, com pot detectar el pont quin és el tràfic d'un segment i quin no?

Emprant el mateix sistema que el servei de correus, mitjançant adreces físiques (MAC) un pont identifica de quin segment és el tràfic que li arriba.

Cada dispositiu de xarxa té una adreça MAC exclusiva a la targeta de xarxa, el pont **rastreja quines són les adreces MAC que estan ubicades a cada costat d'ell** i pren les seues decisions basant-se en un llistat d'adreces MAC.

4.4.1 Domini de col·lisió

Grup de dispositius connectats al mateix medi físic, de manera que si dos dispositius accedeixen al medi al mateix temps, el resultat serà una col·lisió entre els dos senyals.

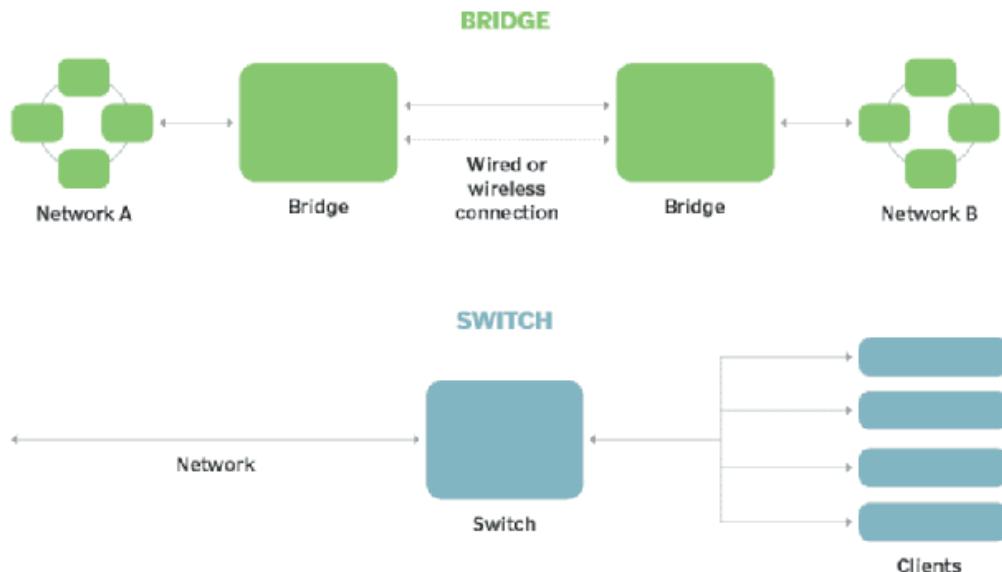
A causa d'aquestes col·lisions es produeix un consum inadequat de recursos i d'amplada de banda que pot dur a congestions serioses de la xarxa. Com menor siga la quantitat de dispositius en un domini de col·lisió, millor funcionarà la xarxa.

Els repetidors o els hubs no poden aïllar el tràfic *broadcast* que es genera a la xarxa en treballar al nivell 1 d'OSI. El **pont** no pot prendre decisions d'encaminament (com arribar a un destí) perquè no treballa a nivell 3 d'OSI. Tanmateix, en operar al **nivell 2**, pot treballar amb adreces MAC i saber per la seua **taula d'adreces MAC** a quin port reexpedir la trama si l'equip es troba a l'esmentat segment.

En la pràctica, **el pont divideix un domini de col·lisió en 2 segments separats, augmentant el rendiment de la xarxa pel fet d'evitar col·lisions.**

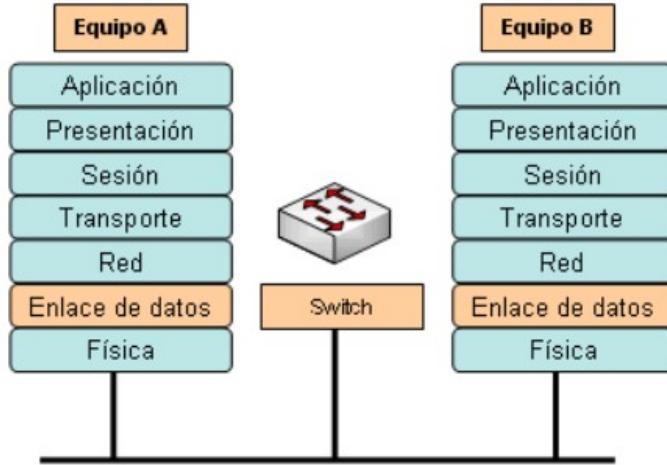
Els ponts poden crear-se mitjançant:

- **Software:** Un ordinador amb dues targetes de xarxa i una aplicació que li permeta actuar com a pont.
- **Hardware:** dispositiu específic.



4.5 Switch o Commutador

Permet la interconnexió de xarxes a nivell d'enllaç.



Emprant l'adreça MAC, els switchs són capaços d'**enviar les dades tan sols cap al port de destí**.

El commutador permet **repartir l'amplada de banda** de la xarxa d'una manera apropiada en cada segment de la xarxa de forma transparent als usuaris.

Existeixen al mercat alguns commutadors de nivell 3 que incorporen funcions d'encaminament però amb la velocitat de la commutació.

Els switchs són gestionables mitjançant **protocols** típics de gestió de xarxa: SNMP, RMON... La majoria d'ells són **gestionables via web**.

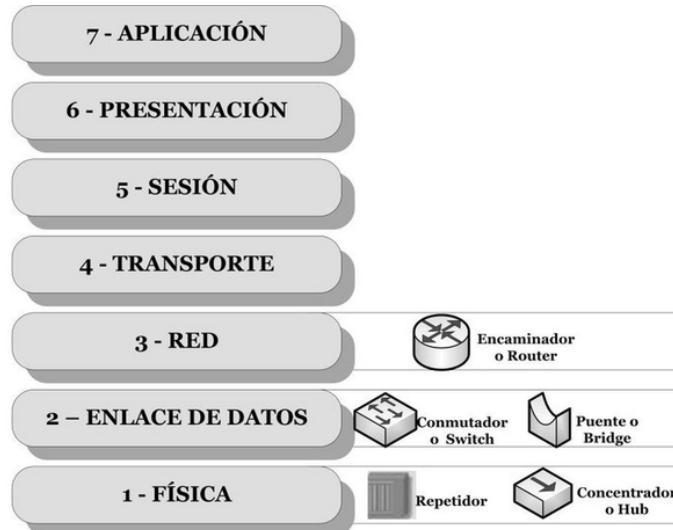
La majoria dels switchs son **apilables i fàcilment escalables**. Solen connectar-se entre ells mitjançant el port **MDIX o MDI-X (Medium Dependent Interface Crossover)**.

Emprant tecnologia específica dels switchs, les xarxes d'àrea local virtuals (**VLANs**) permeten que els nodes de la xarxa es connecten a xarxes lògiques en compte de xarxes físiques.



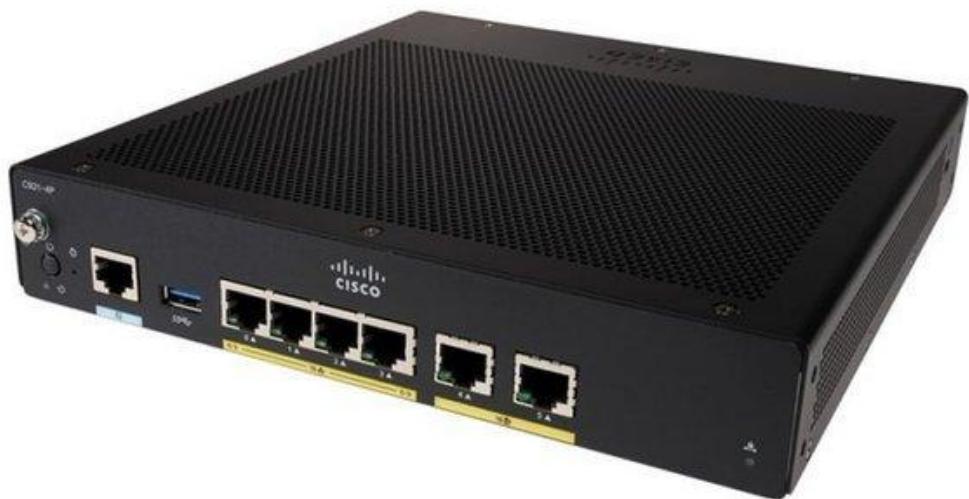
4.6 Router o Encaminador

Permet la **interconnexió de xarxes a nivell de xarxa (nivell 3)**. S'encarrega de seleccionar la millor ruta per tal que els paquets (datagrames) arriben al seu destí.



Els encaminadors s'han convertit en el nucli d'Internet al ser els reguladors del tràfic. Prenen **decisions basades en grups d'adreses de xarxa (mitjançant les adreces IP i les màscares)** emprant el protocol IP.

Els routers també poden **connectar distintes tecnologies de capa d'enllaç**. Per exemple Ethernet, Token-ring i FDDI (fibra òptica).

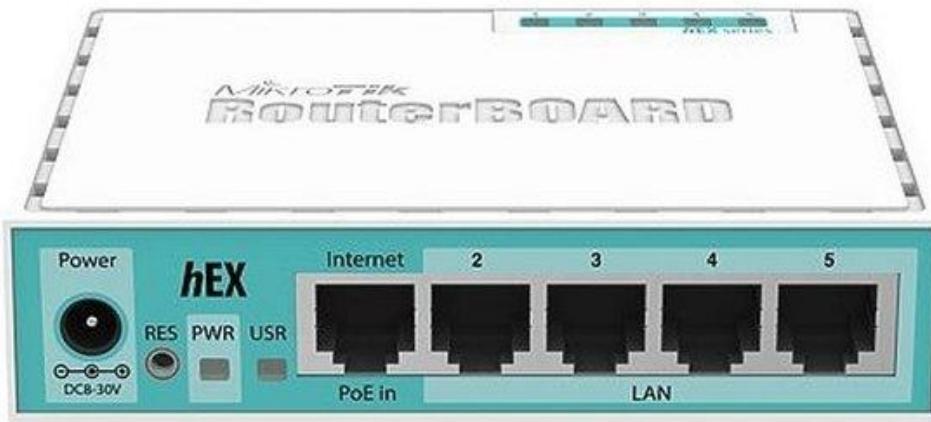


4.6.1 Características

- **Interpreten les adreces lògiques (adreces IP)** de la capa 3 (xarxa), en compte de les adreces MAC de la capa d'enllaç com fan els ponts o commutadors.
- En treballar en un nivell superior són capaços de **canviar el format d'una trama** per a permetre operar amb tecnologies d'enllaç distintes: Ethernet, Token-ring, FDDI i ATM.
- **Proporcionen seguretat** a través de sofisticats filtres de paquets (datagrames) actuant de tallafocs o *firewalls*.
- **Redueixen la congestió de la xarxa** aillant el tràfic i els dominis de col·lisió a les distintes subxarxes a les quals estan connectats.
- Permeten l'existència de diferents **rutes alternatives contra congestions i fallades** a les comunicacions.
- Els protocols de nivell 3 (xarxa) més emprats pels encaminadors són: **IP, IPX, AppleTalk, DECnet, XNS**.

Els routers comercials es poden classificar en 2 segons com reompli la seu taula d'encaminament:

- **Encaminadors amb algorisme d'encaminament estàtic (static routing):** la taula d'encaminament és programada per l'administrador de xarxa.
- **Avantatges:**
 - Ràpids i senzills
- **Desavantatges:**
 - No té capacitat per aprendre la topologia de la xarxa.
 - Qualsevol canvi requereix una intervenció de l'administrador de l'encaminador.
- **Encaminador amb algoritmes d'encaminament adaptatiu (dynamic routing):** són capaços d'aprendre per ells mateixos la topologia de la xarxa.
- **Avantatges:**
 - Són capaços d'aprendre per ells mateixos.
 - Són més flexibles.
- **Desavantatges:**
 - Complexos i amb rendiment menor en haver de confeccionar dinàmicament la taula d'encaminament.



4.6.2 Protocols d'encaminament

Un protocol d'encaminament és el que empra el router per a comunicar-se amb altres routers i aprendre la topologia de la xarxa. És utilitzat per calcular quin és el millor camí (**best path**) per tal d'arribar al destí.

El millor camí dependrà de l'activitat de la xarxa (enllaços actius, velocitat de transmissió entre enllaços...)

El **cost d'una ruta** és un valor numèric que representa que bo és el camí que la representa: a menor cost, millor camí.

Existeixen **protocols basats en el vector-distància** (RIP, RIPv1, RIPv2, BGP) i altres **basats en l'estat de l'enllaç**.

4.6.3 Temps de convergència

Quan es produeix una **alteració topològica** a la xarxa (s'afig un node o deixa d'estar disponible, una nova ruta al destí...) s'han de **recalcular les rutes** per tal d'adaptar-se a la nova situació.

El **temps de convergència** és el temps que tarda l'encaminador a trobar el millor camí quan es produeix una alteració topològica a la xarxa.

Cal dissenyar protocols d'encaminament que tinguen **menor temps de convergència** possible per tal que siguin més flexibles davant un canvi.

4.6.4 Passarel·les

Moltes vegades es confon el terme passarel·la amb el terme encaminador o router.

A l'arquitectura TCP/IP una passarel·la és un dispositiu que s'encarrega de l'encaminament de la informació i la interconnexió de xarxes diferents.

La passarel·la (porta d'enllaç o gateway) és molt més que un router, perquè s'encarrega de **comunicar xarxes amb distinta arquitectura**: TCP/IP, ATM, OSI, X.25...

Els problemes que poden sorgir en la comunicació entre dues xarxes amb diferents tecnologies són diversos. Alguns d'ells són:

- **Diferents protocols de comunicació:** Les xarxes amb diferents tecnologies poden utilitzar protocols de comunicació diferents. Això pot dificultar la comunicació entre elles. Les passarel·les han de ser capaces de traduir els protocols de comunicació per permetre la comunicació entre les xarxes.
- **Diferents formats de dades:** Les xarxes amb diferents tecnologies poden utilitzar formats de dades diferents. Això també pot dificultar la comunicació entre elles. Les passarel·les han de ser capaces de convertir els formats de dades per permetre la comunicació entre les xarxes.
- **Problemes de seguretat:** Les passarel·les poden ser punts vulnerables en la xarxa. Si no estan ben configurades o no es mantenen actualitzades, poden ser atacades per pirates informàtics. Això pot posar en perill la seguretat de les dades que es transmeten entre les xarxes.



... i els Routers de casa?

Una vegada vists els dispositius principals de xarxa, podem dire que els *Routers* que ens instal·len les operadores d'Internet son un *Frankenstein*, fruit del agrupament de diversos dispositius com ara: *Routers*, *Switchs*, Passarel·les, Punts d'accés sense fils...



5. UD5. Instal·lació i configuració d'equips de xarxa

5.1 El sistema operatiu en xarxa

La xarxa està formada per nodes i gran **part de la funcionalitat d'una xarxa depen del software de xarxa que està instal·lat als seus nodes.**

Al mateix temps, cadascun d'aquests nodes **pot tenir corrent un sistema operatiu distint.**

El sistema operatiu de **cada node pot tenir instal·lats i configurats protocols de xarxa distints.** Son aquests protocols de xarxa els qui seran capaços d'entendre i processar la informació que reba altre node.

Actualment tots els sistemes operatius empren el protocol TCP/IP, el que facilita la interconnexió.

- **Microsoft Windows:** tenia com a protocol de xarxa natiu *NetBeui* i era accessible a través de NetBIOS. Conserva aquesta interfície per compatibilitat, però el **protocol natiu actual és TCP/IP.**
- **UNIX i distribucions GNU/Linux:** GNU/Linux engloba a tots els sistemes operatius que seguisquen la tecnologia UNIX, però que es distribueixen sota llicència GP (GNU Public License). La tecnologia de **xarxa nativa** de Linux és **TCP/IP**, però per compatibilitat incorpora software amb les piles de protocols de **Microsoft y Novell Netware.**
- **Apple Mac OS X:** Antigament emprava la pila de protocols *AppleTalk*, però actualment el seu **protocol de xarxa natiu és TCP/IP.**

Documentació

Hem de conservar sempre una **documentació bàsica del software** que opera a la xarxa. Hi ha que **identificar els sistemes operatius de cada ordinador connectat a la xarxa (clients i servidors).** La identificació ha de tenir la **versió del sistema, l'idioma, els parxes** que tinga instal·lats.

Per exemple:

- Linux amb Ubuntu versió 23.04
- Windows 10 SP2

5.1.1 Components del sistema

Un sistema operatiu és molt complexe i per a realitzar les seues funcions relacionades amb la cimunicació en xarxa necessita recolzar-se en:

- **Controladors (drivers) de l'adaptador de xarxa:** Software que comunica el *hardware* de la targeta de xarxa amb el sistema operatiu. Si no tenim el controlador adequat es poden produir errors que impedeixen l'arranc del sistema o el deixen en una situació irrecuperable.
- **Serveis en Xarxa:** Un servei en un SO és una **tasca que s'executa en segon plà (background)** proporcionant una utilitat determinada als clients que realitzen peticions a l'esmentat servei. En Linux, aquestes tasques s'anomenen **dimonis**. Un servei de xarxa és aquella tasca a la que s'accedeix mitjançant un **socket** (protocol + port) i rep peticions a través de la xarxa. Per exemple, el **servei d'accés a fitxers en xarxa o el servei d'impressió en xarxa.**
- **Piles de protocols:** Son les famílies de protocols que instalem en els Sistemes Operatius. Per exemple: TCP/IP, SPX/IPX, NetBeui i AppleTalk. De vegades s'instalen amb el software del SO i altres vegades és necessari que instalem altres piles de protocols o serveis de xarxa.

5.2 Families de protocols en Microsoft

- **Protocol NetBEUI:** sols pot emprar-se en xarxes locals perquè no és capaç d'encaminar-se per a dirigir-se a altres xarxes. Si la xarxa és xicoteta i no es pensa en un creixement a curt termini es podria emprar per donar suport per ser molt simple i fàcil d'emprar. De totes formes, es recomana TCP/IP.

- **Protocol IPX/SPX:** protocol contruit per Novell per al seu sistema *NetWare*. Permet oferir un servei bàsic d'encaminament a xarxes xicotetes i mitjanes. Recomanable quan les estacions de treball de Microsoft han de conviure amb servidors NetWare.
- **Protocol TCP/IP:** especialment dissenyat per poder encaminar-se entre distintes xarxes d'àrea local. Recomanable si la xarxa d'àrea local ha d'estar connectada a Internet o deu estar molt segmentada.

5.3 Família de protocols TCP/IP

El model TCP/IP és un model **més pràctic** que el model OSI. Primerament es dissenyaren els protocols y després s'integraren per capes en l'arquitectura.

El model TCP/IP és molt **més simple**, doncs redueix les capes de 7 a 4.

Arquitectura OSI	Arquitectura TCP/IP	Funció
Aplicació	Aplicació	Conté protocols utilitzats per a les comunicacions de procés a procés, com HTTP, FTP, SMTP, etc.
Presentació	-	Proporciona una representació comuna de les dades transferides entre els serveis de la capa d'aplicació, com la codificació, el xifratge i la compressió.
Sessió	-	Gestiona l'establiment, el manteniment i la finalització de les sessions entre els processos d'aplicació.
Transport	Transport	Proporciona serveis de comunicació fiables i no fiables entre els hosts, com TCP i UDP.
Xarxa	Internet	S'encarrega de l'enrutament dels paquets a través de la xarxa, utilitzant protocols com IP, ICMP i ARP.
Enllaç de dades	Host-xarxa	S'encarrega de la transmissió de les dades entre els dispositius de la xarxa, utilitzant protocols com Ethernet, Wi-Fi i PPP.
Física	Host-xarxa	S'encarrega de la conversió de les dades en senyals elèctrics, òptics o sense fils que es poden transmetre pel medi físic.

5.3.1 Protocol IP

- El protocol IP realitza tasques bàsiques d'encaminament per a conseguir transportar dades desde un origen a un destí.
- L'**origen i el destí poden estar en xarxes amb tecnologies totalment diferents** i pot haver-hi diverses rutes possibles per el que deurà prendre decisions i triar la millor.
- **No hi ha seguretat a l'entrega.**
- **No hi ha control d'errors.**
- **Els paquets poden arribar desordenats.**
- Els equips d'una xarxa tenen asociat un número d'**adreça IP** (direcció lògica, no confondre amb el número MAC de l'adaptador de xarxa que és l'adreça física) que permet identificar-los en tot Internet.
- L'**adreça IP és un número binari de 32 bits**. La seua representació en decimal està formada per 4 números separats per punts, cadascún dels quals pot prendre valors entre 0 i 255.

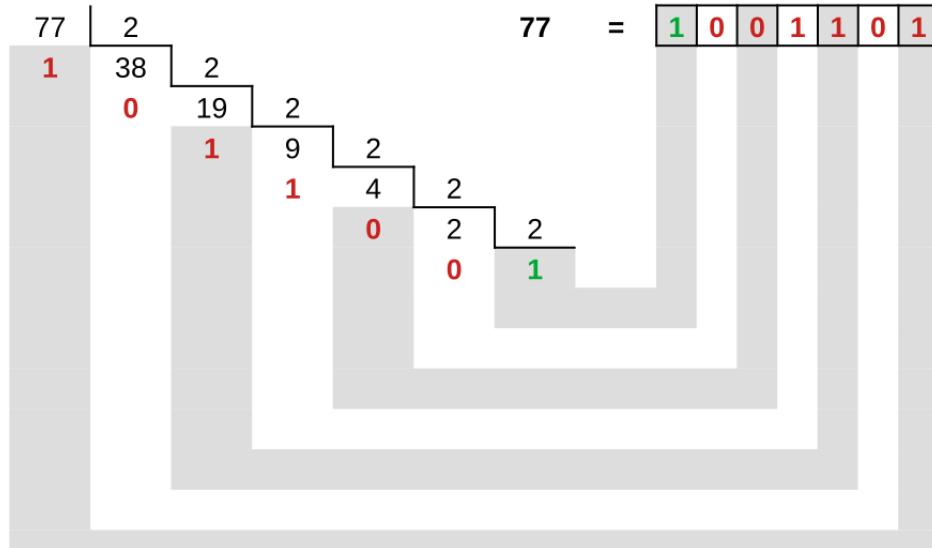
Adreça IP binària de 32 bits

11000000 . 10101000 . 00100010 . 00001011 = 192.168.100.15

Conversió de sistema decimal a sistema binari

Per convertir un número decimal en binari es realitzen successives divisions entre 2 (base del sistema) i van recollint-se els residus de cada divisió **en ordre invers**.

Exemple de pas de decimal a binari



Conversió de sistema binari a sistema decimal

Per tal de convertir un número binari a decimal haurem d'aplicar el **Teorema fonamental de la numeració**.

Exemple de pas de binari a decimal

$$ABCD = A \cdot \text{Base}^{\text{posició}} + B \cdot \text{Base}^{\text{posició}} + C \cdot \text{Base}^{\text{posició}} + D \cdot \text{Base}^{\text{posició}}$$

$$1547 = 1 \cdot 1000 + 5 \cdot 100 + 4 \cdot 10 + 7 \cdot 1$$

$$1547 = 1 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0$$

$$100101_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

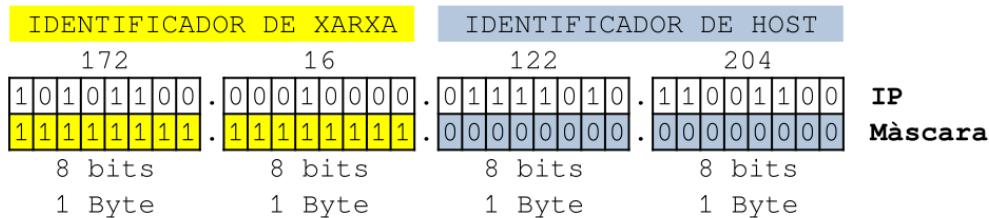
$$100101_2 = 2^5 + 2^2 + 2^0 = 32 + 4 + 1 = 37$$

TRUC:

1	0	0	1	0	1	
5	4	3	2	1	0	
2^5	2^4	2^3	2^2	2^1	2^0	
32	16	8	4	2	1	=
$32 + 4 + 1$						= 37

Parts de l'adreça IP

- L'adreça IP d'un dispositiu està **estructurada en dues parts**:
- Identificador de xarxa** a la que està connectat el dispositiu
- Identificador del dispositiu**
- Aquesta estructura facilita l'**encaminament dels routers**, de forma que per encaminar un datagrama, els routers analitzaran l'identificador de xarxa al qual pertany i ho encaminaran cap a ella. Una vegada dintre de la xarxa, el o els routers de dita xarxa tindran que analitzar l'indicador del host de destí per encaminar el datagrama fins ell.
- L'identificador de xarxa pot tenir el tamany que es desitge, en funció del tamany de la xarxa.



MÀSCARA DE XARXA

És un número similar a l'adreça IP i **determina quina part de l'adreça IP pertany a l'equip i quina part pertany a la xarxa**. Per definir el prefixe de l'adreça IP, és a dir, el que es coneix com identificador de xarxa, s'utilitza la denominada màscara de xarxa, que és un número binari de 32 bits que defineix a les posicions a "1" el prefixe o identificador de xarxa i a les posicions a "0" el dufixe o identificador de host.

- Actualment per tal d'identificar la màscara de cada PC se li afeg /XX a l'adreça IP. Éssent XX el nombre de bits a "1" de la màscara de xarxa.

La "màscara curta"

- IP = 192.168.2.200 -- Màscara: 255.255.255.0
- Nomenclatura equivalent: IP = 192.168.2.200/24

ADREÇA DE XARXA

L'adreça de la xarxa és la part de l'adreça IP que identifica la subxarxa on es troba el dispositiu. Com ja hem vist, la màscara de xarxa és un nombre que indica quants bits de l'adreça IP pertanyen a la xarxa i quants al host.

Per calcular l'adreça de la xarxa, hem de fer una operació **AND lògica** entre l'adreça IP i la màscara de subxarxa. Això significa que si els dos bits són 1, el resultat és 1; si no, el resultat és 0.

Exemple de càlcul d'adreça de xarxa

Suposem que tenim l'adreça IP **192.168.1.100** i la màscara de subxarxa **255.255.255.0**. En binari, això seria:

IP: 11000000.10101000.00000001.01100100

Mask: 11111111.11111111.11111111.00000000

Fent l'operació AND entre els dos, obtenim:

Adreça de xarxa: 11000000.10101000.00000001.00000000

Aquest és el resultat en binari de l'adreça de la xarxa. Si el convertim a decimal, obtenim:

Adreça de xarxa: 192.168.1.0

5.3.2 Protocol TCP

- El TCP és un protocol per al control de la transmissió de les dades.
- Es dissenyà per realitzar connexions segures en xarxes insegures.
- Soluciona els problemes existents en IP:
- **Aporta control d'errors.**
- **Seguretat a l'entrega.**
- **Control de fluxe. Els paquets arriben ordenats.**
- Es complementa de manera perfecta amb IP per **aportar una comunicació de dades fiable i ordenada**. Per això en ocasions es fa referència a TCP/IP com si fos un únic protocol, però realment en son dos.
- Els punts d'accés al servei en la capa de transport s'anomenen **sockets, ports o connectors TCP/IP**. Darrere de cada socket s'implanta un servei de xarxa. Per exemple, 80 és el port que identifica les peticions de xarxa cap a un servidor web.
- Quan algú a la xarxa requereix un servei, envia un missatge al socket o port que identifica el servei. Alguns serveis requereixen més d'un socket per al seu funcionament.

5.4 Adreçament IP (Classful)

Per tal de facilitar la administració, els dissenyadors de l'esquema d'adreçament IP varen determinar l'existència de 5 classes úniques: A, B, C, D i E.

Primer octet		Adreces IP				
Primers bits	Rang de valors	Classe	Màscara de xarxa	Xarxa i hosts	Nombre de xarxes	Nombre de hosts
0	0–127	A	255.0.0.0	X.h.h.h	$2^7 = 128$	16777214
10	128–191	B	255.255.0.0	X.X.h.h	$2^{14} = 16384$	65534
110	192–223	C	255.255.255.0	X.X.X.h	$2^{21} = 2097152$	254
1110	224–239	D	No aplicable	Reservat	No aplicable	No aplicable
1111	240–255	E	No aplicable	Reservat	No aplicable	No aplicable

5.4.1 Classes de una adreça IP: classe A

- Una **adreça IP de classe A** sempre té el primer bit (el que es troba més a l'esquerra) a '0', és a dir, **el primer octet té un valor decimal entre 0 i 126**. La xarxa 127.0.0.0 no pot emprar-se per estar reservada per a proves de l'adaptador de xarxa.
- Les adreces IP de classe A empren solament els **8 primers bits per identificar la part de xarxa** de l'adreça, la resta (**tres octets s'utilitzen per especificar la part del host** de l'adreça).
- Les **adreces IP de classe A que NO es poden utilitzar** son:
- Una **primera adreça IP per a l'identificador de la xarxa** (primer octet amb el valor de la xarxa corresponent i la resta d'octets amb els seus bits a valor zero).
- Una **adreça IP per a difusió o broadcast**, que tindrà el primer octet amb el valor de la xarxa i la resta d'octets amb els bits a valor 1, és a dir 255 en decimal.
- La **màscara de xarxa per defecte** de les adreces IP de classe A son **255.0.0.0**

5.4.2 Classes de una adreça IP: classe B

- Una **adreça IP de classe B** sempre té els seus dos primers bits a valor binari '10', és a dir, **el primer octet tindrà un valor decimal entre 128 i 191**.
- La **màscara de xarxa per defecte** de les adreces IP de classe B son **255.255.0.0**

- Les adreces de classe B utilitzen els **dos primers octets per a l'identificador de xarxa**, i els **dos últims octets per a l'identificador de host**. En una xarxa de classe B existiran 65.536 IPs distintes, de les quals dues estan reservades per a la xarxa (bits de host TOTS a zero) i per al *broadcast* (bits de host TOTS a uns). Per tant, 65534 nombre màxim de connexions.

5.4.3 Classes de una adreça IP: classe C

- Una adreça de classe C sempre té els seus tres primers bits al valor binari '110', és a dir, **el primer octet tindrà un valor decimal entre 192 i 223**.
- La **màscara de xarxa per defecte** de les adreces IP de classe C és **255.255.255.0**
- Les adreces de classe C utilitzen els **tres primers octets per a l'identificador de xarxa** i **l'últim octet per a l'identificador de host**. En una xarxa classe C existiran un màxim de 256 IPs distintes, de les quals dues estan reservades (xarxa i *broadcast*), per tant tindrem 254 connexions reals.

5.4.4 Classes de una adreça IP: classe D

- Les adreces IP de classe D són adreces **multicast o multienviament** que s'utilitzen únicament **el primer octet com identificatiu de xarxa** i els **tres octets restants** s'utilitzen com **identificatiu de grup de host**.

5.4.5 Classes de una adreça IP: classe E

- Les adreces IP de classe E estan reservades per a usos experimental en projectes d'investigació en la xarxa. S'utilitzen únicament per a futurs projectes i experimentacions.

5.5 Adreces públiques i privades

Una **adreça IP pública** és aquella que **identifica de forma única una connexió a Internet**.

Les **adreces IP privades** són adreces IP que s'utilitzen únicament en **xarxes d'àrea local** perquè no poden ixir a navegar per Internet, de fet, si un datagrama d'una xarxa privada ixquera accidentalment a Internet seria descartat perquè eixa adreça no existeix en Internet.

Quan des d'una **xarxa local s'ix a navegar per Internet** haurem d'emprar un **router amb tecnologia NAT** (Network Address Translation). De forma resumida, el NAT farà que siga el router l'encarregar d'emmagatzemar l'adreça privada en una taula, assignar-li un identificador i substituir l'adreça d'origen per la pública del router. Quan se li conteste no tindrà més que consultar en la seua taula el valor de l'adreça provada corresponent a l'identificador i enviar-li a ella el datagrama de resposta.

5.5.1 Adreces IP privades reservades

TIPUS IP	Des de...	Fins a...
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

5.6 Adreces IP estàtiques i dinàmiques

- ESTÀTIQUES (fixes)**: Un host que es connecta a la xarxa amb una adreça IP estàtica, sempre ho farà amb la mateixa IP. Les adreces IP públiques estàtiques són les que utilitzen els servidors d'Internet amb l'objectiu d'estar sempre localitzables per els usuaris d'Internet. Aquestes adreces hi ha que contractar-les.
- DINÀMIQUES**: Un equip que es connecta a la xarxa mitjançant una adreça IP dinàmica, cada vegada ho farà amb una IP distinta. Els proveïdors d'Internet (ISP) emprén adreces IP dinàmiques perquè tenen més clients que adreces IP (és molt improbable que tots es connecten al mateix temps).

- Les adreces IP emprades en Internet estan definides en la **RFC1166**.

5.7 Adreces IP especials

Aquestes adreces són especials i no es poden passar fora de la xarxa local o tenen un ús específic:

Bloc d'adreces	Rang	Número d'adreces	Abast	Descripció
0.0.0.0/8	0.0.0–0.255.255.255	16.777.216	Software	Xarxa actual (només vàlid com a adreça d'origen).
10.0.0.0/8	10.0.0.0–10.255.255.255	16.777.216	Xarxa privada	Utilitzat per a les comunicacions locals dins d'una xarxa privada.
100.64.0.0/10	100.64.0.0–100.127.255.255	4.194.304	Xarxa privada	Espai d'adreces compartit per a les comunicacions entre un proveïdor de serveis i els seus subscriptors quan s'utilitza un NAT de nivell d'operador.
127.0.0.0/8	127.0.0.0–127.255.255.255	16.777.216	Host	S'utilitza per a les adreces de loopback.
169.254.0.0/16	169.254.0.0–169.254.255.255	65.536	Subxarxa	S'utilitza per a les adreces de enllaç local entre dos hosts en un sol enllaç quan d'altra manera no s'especifica cap adreça IP, com normalment s'hauria recuperat d'un servidor DHCP.
172.16.0.0/12	172.16.0.0–172.31.255.255	1.048.576	Xarxa privada	Utilitzat per a les comunicacions locals dins d'una xarxa privada.
192.0.0.0/24	192.0.0.0–192.0.0.255	256	Xarxa privada	Assignacions de protocol de l'IETF.
192.0.2.0/24	192.0.2.0–192.0.2.255	256	Documentació	Assignat com a TEST-NET-1, per a documentació i exemples.
192.88.99.0/24	192.88.99.0–192.88.99.255	256	Internet	Reservada. Previament utilitzada per a relay IPv6 a IPv4. (incloent el bloc d'adreces IPv6 2002::/16).
192.168.0.0/16	192.168.0.0–192.168.255.255	65.536	Xarxa privada	Utilitzat per a les comunicacions locals dins d'una xarxa privada.
198.18.0.0/15	198.18.0.0–198.19.255.255	131.072	Xarxa privada	Utilitzat per a proves de rendiment entre dos dispositius separats.
198.51.100.0/24	198.51.100.0–198.51.100.255	256	Documentació	Assignat com a TEST-NET-2, per a documentació i exemples.
203.0.113.0/24	203.0.113.0–203.0.113.255	256	Documentació	Assignat com a TEST-NET-3, per a documentació i exemples.
224.0.0.0/4	224.0.0.0–239.255.255.255	268.435.456	Internet	Adreces multicast.
240.0.0.0/4	240.0.0.0–255.255.255.254	268.435.456	Internet	Reservada per a usos futurs.
255.255.255.255/32	255.255.255.255	1	Subxarxa	Adreça de difusió limitada.

5.8 Càlcul de l'adreça de broadcast

Per a calcular l'adreça de broadcast de la xarxa a la que pertany una adreça IP i la seu màscara, haurem de seguir aquests passos:

1. **Converteix l'adreça IP i la màscara a format binari.** Per exemple, si l'adreça IP és 192.168.1.100 i la màscara és 255.255.255.0, en binari serien:
 - IP: 11000000.10101000.00000001.01100100
 - Màscara: 11111111.11111111.11111111.00000000
2. Fes una operació AND lògica entre l'adreça IP i la màscara per a **obtenir l'adreça de xarxa**. Aquesta operació consisteix a comparar els bits de cada octet i retornar 1 si tots dos són 1, o 0 en cas contrari. Per exemple:
 - IP: 11000000.10101000.00000001.01100100
 - Màscara: 11111111.11111111.11111111.00000000
 - Xarxa: 11000000.10101000.00000001.00000000
3. Per a trobar l'adreça de broadcast, has de **canviar tots els bits de la part del host de l'adreça de xarxa per 1**. La part del host són els bits que corresponen als 0 de la màscara. Per exemple, si l'adreça de xarxa és 192.168.1.0 i la màscara és 255.255.255.0, la part del host és l'últim octet, per tant, l'adreça de broadcast seria 192.168.1.255. En binari, seria:
 - Xarxa: 11000000.10101000.00000001.00000000
 - Broadcast: 11000000.10101000.00000001.11111111

5.9 Adreçament *Classful*

L'adreçament basat en classes (A, B, C, D i E) i les seues màscares de xarxa predeterminades és conegut com **adreçament classful**. Quan fou **creat a l'any 1981** Internet era una xarxa molt petita i nungú imaginava que arribaria a tindre la quantitat d'equips que té actualment.

De fet, abans de l'adreçament *classful*, a les primeres etapes del desenvolupament del protocol d'Internet, les adreces IP eren concebudes com un primer octet (8 bits) per dessignar la xarxa i els altres tres octets següents per als equips dins de eixa xarxa.

L'adreçament *classful* en el seu dia va aportar diversos **avantatges**:

- **Facilitat i claredat:** Hi ha **poques classes** per tirar i és molt fàcild'entendre com es divideixen les adreces. La distinció entre classes és clara i evident. Les divisions entre els ID de xarxa i l'ID de hosts a les classes A, B i C estan als límits de l'octet i això fa fàcil dir quin és l'identificador de qualsevol adreça.
- **Flexibilitat raonable:** Els tres nivells de **granularitat** coincideixen raonablement bé amb els tamans de les organitzacions (grans, mitjanes i petites).
- **Facilitat d'enrutament:** La classe de l'adreça va codificada just en l'adreça (primers bits del primer octet) perquè siga **fàcil per als routers** saber quina part de qualsevol adreça és l'**identificador de xarxa i quina l'identificador de host**. No ho ha necessitat d'informació anexa, com la màscara de subxarxa.
- **Adreces reservades:** Algunes adreces estan reservades per a **propòsits especials**. Açò inclou no sols les classes D i E, també rangs especials d'adreces reservades per a l'adreçament "privat".

Ningú esperava que Internet arribaria a ser una xarxa amb la magnitud actual. Això ha produït que siguin més evidents els **problemes** de l'adreçament *classful*:

- **Falta de flexibilitat:** Quan se li assigna a una empresa una adreça de xarxa (A, B o C) estem **limitant e un nombre d'ordinadors concret per a la nostra xarxa** ($A = 2^{24} - 2 = 16.777.214$, $B = 2^{16} - 2 = 65.534$, $C = 2^8 - 2 = 254$) que no té el perquè de coincidir amb les necessitats reals de l'empresa.
- **Ús inefficient de l'espai d'adreces:** L'existència de sols tres tamans de bloc de classes (A, B i C) dona peu a la **pèrdua d'espai d'adreces IP**.

Desaprofitament d'adreces

Si tens una empresa amb 5.000 ordenadors necessites una adreça de xarxa de classe B per poder incorporar-los tots i desperdiaries 60.000 adreces de les 65.000 de la xarxa de classe B.

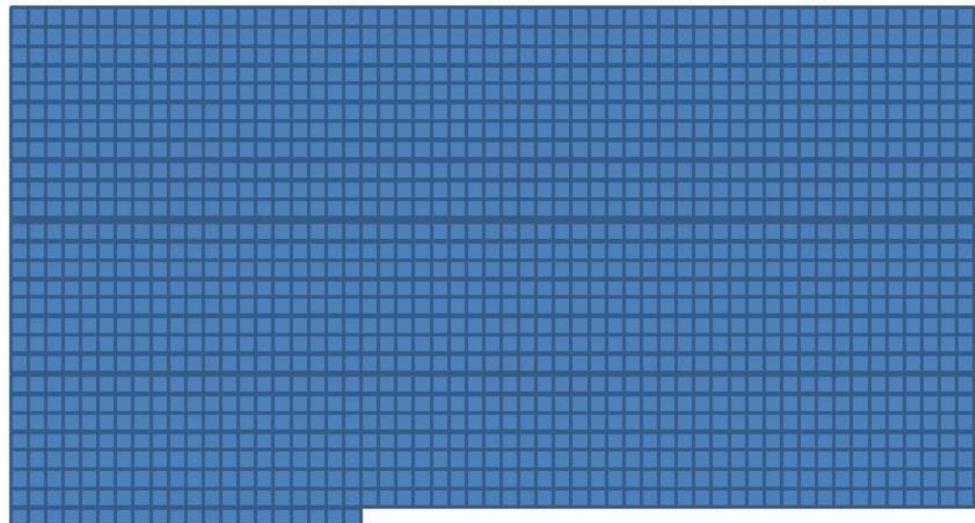
Hosts en una red clase C (254)



Hosts necesitados por la organización (5000)



Hosts en una red clase B (65,534)

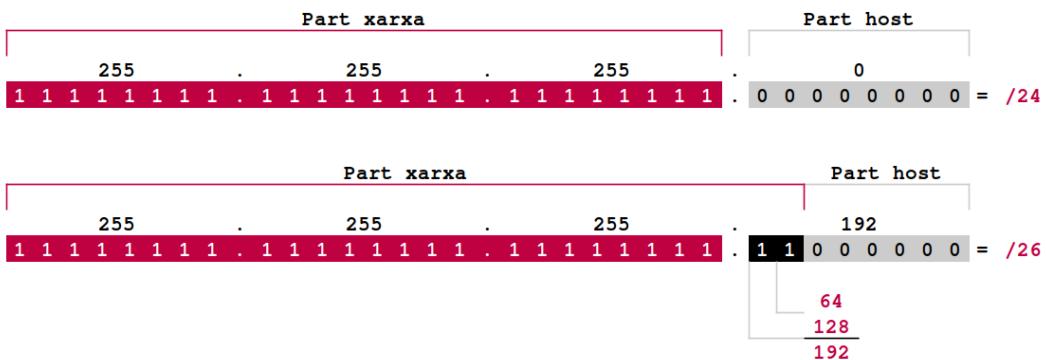


- **Baixa granularitat:** Tres tamanys (A, B i C) semblen correctes, en principi, però **les diferències entre els tamanys son enormes**. La diferència de tamany entre les xarxes de classe C i classe B és massa gran (un bot de 254 hosts fins a més de 65.000). Per altra banda, **quantes empreses necessiten una classe A (16 milions d'adreces IP)?**

5.9.1 Subnetting

- En el sistema d'adreçament de subxarxes *classful*, la divisió xarxa/host de l'adreça IP es converteix en un sistema de tres nivells (A, B i C). Si emprem una adreça de classe C tenim 24 bits per a l'ID de xarxa i els 8 bits restants per a l'ID del host.
- Emprant el **subnetting** podem dividir la nostra xarxa en diverses subxarxes:

Exemple subnetting



Al cas anterior de l'adreça de classe C, l'ID de host pot dividir-se en, per exemple, 2 bits per a un ID de subxarxa i 6 per a l'ID del host. Això permetrà tindre $2^2 = 4$ subxarxes (00, 01, 10 i 11).

La màscara de subxarxa seria 26 '1' seguits de 6 '0', els zeros indiquen quina part de l'adreça és el host. En la notació decimal amb punts, això seria 255.255.255.192

- Mitjançant el *subnetting* podem dividir una adreça IP de la classe que siga en diverses subxarxes dependent d'eles nostres necessitats.

Exemple subnetting. Descomposició en subxarxes

A continuació podem veure les 6 primeres subxares de les 16 en les quals s'ha descompost una **adreça de classe C emprant 4 bits per subnetting**:

IP	Mascara en Binari	Mascara Decimal	Classe	Subxarxes	Host
192.168.10.0/28	11111111.11111111.11111111.11110000	255.255.255.240	C	$2^4=16$	$2^4-2=14$
24b xarxa + 4b subxarxa + 4b host					
Subxarxa 0	11000000.10101000.00001010.00000000	11000000.10101000.00001010.00001111			
Subxarxa 1	11000000.10101000.00001010.00010000	11000000.10101000.00001010.00011111			
Subxarxa 2	11000000.10101000.00001010.00100000	11000000.10101000.00001010.00101111			
Subxarxa 3	11000000.10101000.00001010.00110000	11000000.10101000.00001010.00111111			
Subxarxa 4	11000000.10101000.00001010.01000000	11000000.10101000.00001010.01001111			
Subxarxa 5	11000000.10101000.00001010.01010000	11000000.10101000.00001010.01011111			
...			

5.10 Adreçament Classless

Per tal de solucionar la problemàtica de l'adreçament IP amb classes (Classful), naix l'adreçament IP **sense classes o CIDR**.

CIDR, en essència, aplica el mateix que el *subnetting* però ampliant el concepte.

En CIDR **no existeixen classes A, B o C**. El valor de l'adreça IP no implica ninguna màscara implícita, com ocorria abans amb els primers bits de l'adreça. **Tota definició d'una xarxa IP deu anar acompañada d'una adreça de màscara** que concreta la xarxa.

Per exemple, quan parlem en termes de CIDR no podem afirmar que l'adreça 172.17.25.12 pertany a la xarxa 172.17.0.0 si no ve especificada com 172.17.25.12/16

En CIDR ja no s'empra el terme "classe d'una xarxa", perquè no hi han classes com a tal, sinó xarxes definides per el sufix que acompanya a l'adreça de xarxa.

Com es pot entendre en CIDR tampoc podem aplicar el concepte de *subnetting* tradicional. CIDR defineix una jerarquia de xarxes, cadascuna amb el seu tamany específic, i que algunes poden encaixar dintre d'altres.

CIDR va fer seu la nomenclatura de barra invertida, del tipus /xx (on xx representa el bits marcats a '1' de la màscara en binari) i està basada en el que es va denominar ***variable-length subnet masking (VLSM)***.

6. UD6. Escenaris de xarxes

6.1 Configuració de la xarxa

Anem a veure comandes de terminal que existeixen per poder comprovar la nostra configuració de la xarxa i com modificar alguns paràmetres:

- *Hostname* o nom de l'equip
- Adreça MAC
- Adreça IP, màscara de xarxa, adreça de xarxa i adreça de *broadcast*
- *Gateway* o porta d'enllaç
- Servidor DNS
- Propietats d'una connexió de xarxa

6.1.1 Nom de l'equip

El **hostname** d'un equip és el nom que s'assigna a aquest dispositiu dins d'una xarxa i algunes de les seues funcions son:

1. **Identificació de l'equip:** El **hostname** és una etiqueta única que permet identificar un ordinador o dispositiu en una xarxa. És com el nom propi de l'equip dins del context de la xarxa.
2. **Resolució de noms:** Quan es realitza una comunicació a través de la xarxa, els dispositius utilitzen adreces IP per trobar-se. El **hostname** es tradueix a una adreça IP mitjançant el **DNS (Domain Name System)**. Això permet que els usuaris puguin accedir als recursos de xarxa utilitzant noms amigables en lloc d'adreces IP numèriques.
3. **Configuració de serveis:** El **hostname** també es fa servir per configurar serveis i aplicacions en un servidor. Per exemple, quan configures un servidor web, pots associar un **hostname** (com "www.example.com") a una determinada carpeta o aplicació web.

En resum, el **hostname** és una etiqueta que identifica un equip a la xarxa i facilita la comunicació entre els dispositius mitjançant noms amigables.

```
paco@tufdash:~$ hostname
tufdash
paco@tufdash:~$ █
```

6.1.2 Adreça IP, Màscara, MAC i Adreça de broadcast

El comandament que emprarem en sistemes Linux per obtindre informació rellevant de la xarxa és `ip a`. Amb aquest comandament obtindrem: adreça IP i màscara en format curt (etiqueta *inet*), Adreça MAC (etiqueta *link/ether*) i adreça de broadcast (etiqueta *brd*) de cadascun dels adaptadors de xarxa que tinguem instal·lats. L'adreça de la xarxa no ens la mostra, però com em vist en unitats anteriors, la podem obtindre realitzant l'operació **IP AND Màscara**.

A sistemes Windows, el comandament equivalent és `ipconfig /all`.

```
xal@virtual:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000      MAC
    link/ether 08:00:27:3a:f4:fd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        IP   valid_lft 86386sec Máscara Broadcast
        inet6 fe80::a1fb:800b:c9ce:a972/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

6.1.3 Porta d'enllaç

En Linux, la **porta d'enllaç** o **gateway** s'obtenen gràcies al comandament `ip r`. La línia que indica la porta d'enllaç és la que està etiquetada com a *default*.

En sistemes Windows, la porta d'enllaç ve indicada també amb el comandament `ipconfig /all`.

```
paco@tufdash:~$ ip r
default via 172.20.10.1 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.20.10.0/28 dev wlo1 proto kernel scope link src 172.20.10.14 metric 600
```

6.1.4 Servidors DNS

Per obtindre informació referent als servidors DNS configurats en sistemes Linux, haurem de consultar un fitxer mitjançant el comandament `cat /etc/resolv.conf`. Si al fitxer ens diu que el nameserver és el 127.0.0.X significa que *NetworkManager* està configurat per iniciar una instància de la aplicació `dnsmasq` que és un servei local de reenviament de servidor de noms. Podem llavors, obtindre més infomació amb el comandament `resolvectl status`.

Novament, a sistemes Windows, aquesta informació ens la donarà el comandament `ipconfig /all`.

6.1.5 Informació del driver i de la connexió

A sistemes Linux, aquesta informació l'obtemim amb el comandament `ethtool`:

- **Informació del driver:** `ethtool -i <adaptador_xarxa>`
- **Informació de la connexió:** `ethtool <adaptador_xarxa>`

6.1.6 Coneixions sense fils

A sistemes Linux, emprarem el comandament `iwlist scan` per veure informació extra, el comandament `iwconfig`. Sols mostrarà informació d'aquells adaptadors sense fils presents al sistema, evidentment.

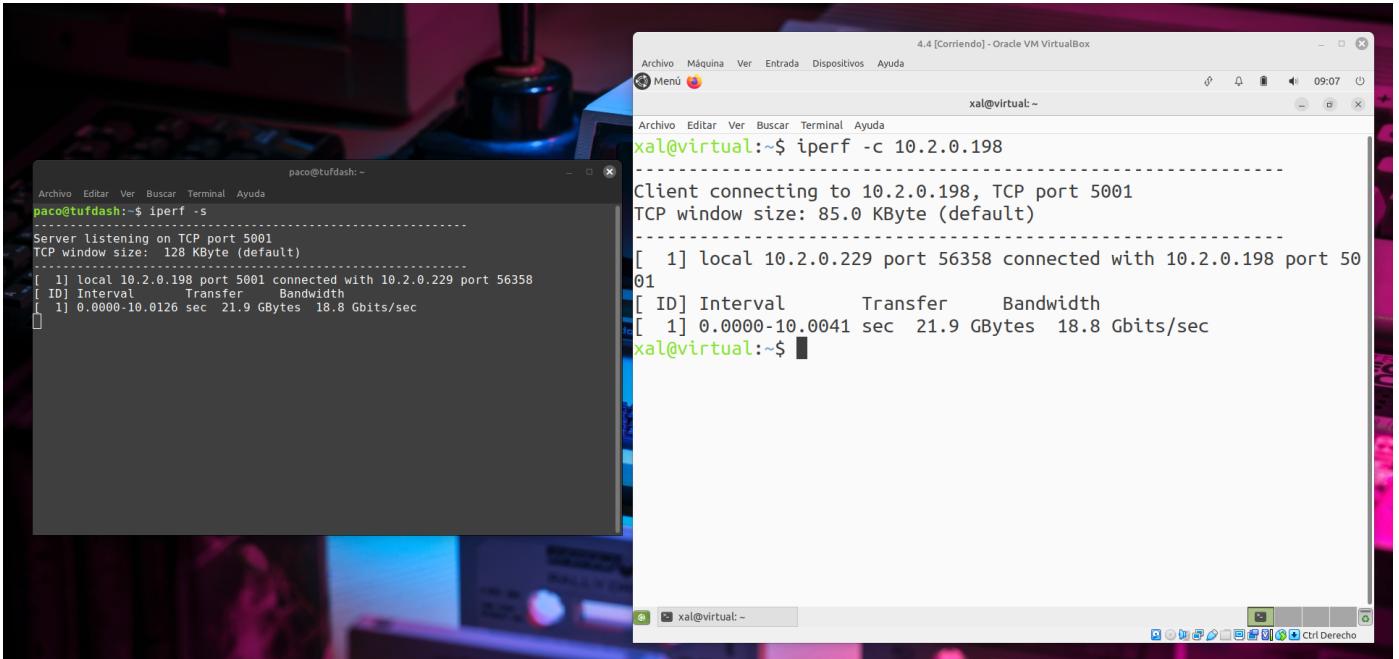
6.2 Test de velocitat de la xarxa local

Iperf és una ferramenta que s'utilitza per fer proves de velocitat en xarxes. *Iperf* crea fluxos de dades TCP i/o UDP i realitza un informe amb marques de temps amb la quantitat de dades transmeses i el rendiment mig. Això pot ser d'utilitat per **comparar la velocitat de les tomes d'equips de xarxa cablejats i sense fils** de forma imparcial.

Es tracta de *software* de codi obert i pot executar-se en diverses plataformes incloent Linux, Unix i Windows. Per instalar-lo en sistemes Debian (Ubuntu) hem d'executar `sudo apt install iperf`.

Iperf pot funcionar com a **client (-c)** o com a **servidor (-s)** i pot mesurar el rendiment entre els dos extrems de la comunicació, unidireccional o bidireccionalment. Quan l'executem com a client (-c) hem d'afegir també l'adreça IP de l'equip que actua com a servidor (-s).

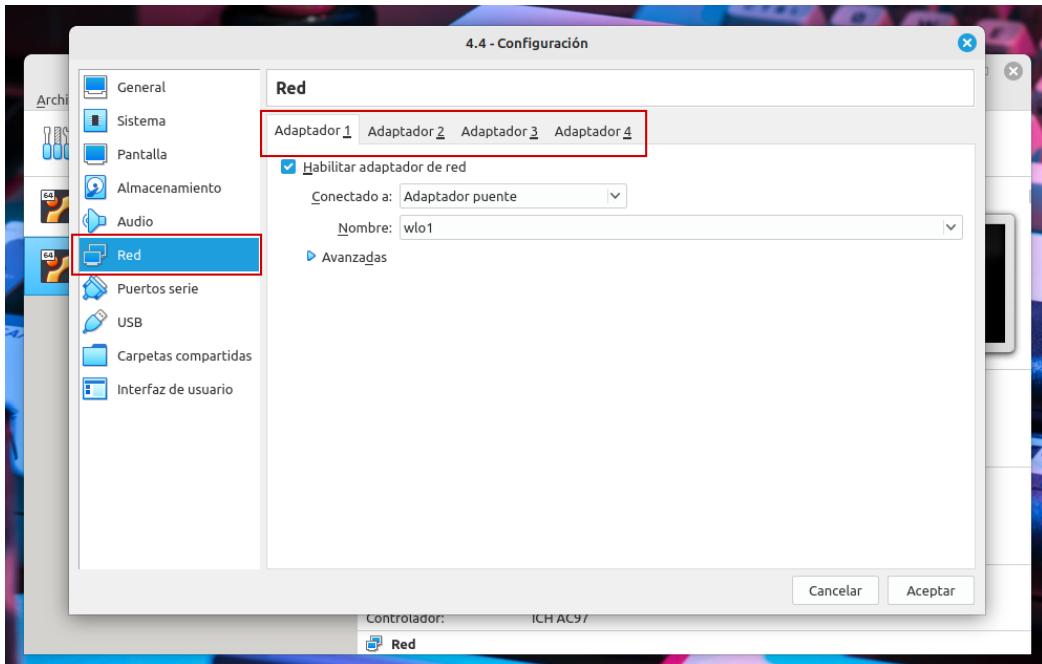
[Pàgina web del software Iperf](#)



6.3 Adaptadors de xarxa en VirtualBox

Una màquina virtual (MV) en VirtualBox (VB) pot tenir fins a **8 targetes de xarxa PCI Ethernet**, i cadascuna d'elles, de manera independent, pot tenir assignat el tipus de hardware a virtualitzar i **el seu propi mode de configuració**. Des de l'administrador de VB es poden configurar 4 de les 8 targetes de xarxa, si ens feren falta més, hauríem de configurar-les per terminal mitjançant el programa **VBoxManage**.

Per tal de configurar la xarxa del sistema virtualitzat, haurem de seleccionar la MV a la pantalla principal del VB i entrar en "Configuració" --> "Xarxa".

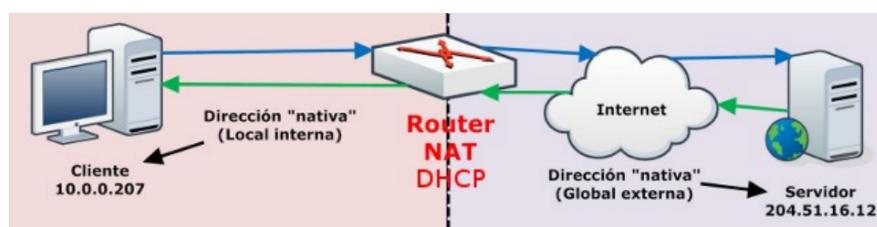


Mitjançant el desplegable "Connectat a:" tindrem, en general, les següents opcions:

- NAT
- Xarxa NAT
- Adaptador pont
- Adaptador sols-amfitrió
- Xarxa interna
- No connectat

Per a què serveix el protocol NAT?

NAT és un protocol que fou creat per traduir les IPs privades de la xarxa en una IP pública perquè la xarxa poguera enviar paquets a l'exterior; i traduir després eixa IP pública, de nou a la IP privada de l'equip que havia enviat el paquet, per tal que poguera rebre'l una vegada arribada la resposta.



6.3.1 NAT en VirtualBox

A VB és el **mode per defecte** de la targeta de xarxa virtual. Amb aquesta opció el servei virtualitzat utilitza la targeta de xarxa de la **màquina real (amfitrió)** per navegar. En mode NAT, VB col·loca un **router entre l'amfitrió (cap on fa NAT) i la màquina virtual**.

Aquest router poseeix un servidor DHCP que serveix cap a l'interior i mapeja el tràfic des de i cap a la MV de manera transparent. D'aquesta forma, si tenim configurat el client DHCP en el SO de la MV (opción habitualmente por defecto), en **mode NAT tindrem Internet automàticament a la MV**.

Cada MV en mode NAT tindrà el seu propi router, per la qual cosa **estaran en xarxes aïllades**, el que implica que, per defecte, les MMVV que tenen la seua targeta en mode NAT **no poden veure's entre elles**.

L'adreça que el router (intern) serveix (DHCP) va a dependre del número de targeta de xarxa que estiga assignat en mode NAT. Les 8 targetes de xarxa que VB permet a cada MV van numerades del 0 al 7 i les adreces de xarxa dels routers segueixen el patró **10.0.[x + 2].0/24**, on x és el número de la targeta de xarxa (10.0.2.0/24, 10.0.3.0/24, ..., 10.0.9.0/24). L'adreça IP de la targeta de xarxa serà 10.0.x+2.15/24 i la porta d'enllaç (router intern) 10.0.x+2.2/24.

Canvi d'adreçament NAT en VirtualBox

Pot ser interessant **canviar la numeració** motivats per el problema que estiguem resolent en un moment donat, i per fer-ho és necessari recòrrer al comandament **VBoxManage** de la següent forma:

```
VBoxManage modifyvm "Nom_de_la_MV" --natnet1 192.168.0.0/16
```

Amb l'ordre anterior, l'adaptador de xarxa número 0 (--natnet1) de la MV "Nom_de_la_MV" pendrà l'adreça de xarxa 192.168.0.15/16 i la porta d'enllaç 192.168.0.2/16.

Un **desavantatge** d'aquest mode, com hem vist, és que **la MV és invisible i inalcaçable fora de la seu xarxa** i per tant, **no podem instal·lar un servidor d'aquesta manera, a no ser que configurem el reenviament de ports**. La qual cosa no està mal des del punt de vista de la seguretat.

Reenviament de ports en xarxa NAT de VirtualBox

Si per exemple, a la MV col·loquem un servidor SSH i volem que les peticions SSH al port 2222 de l'amfitrió passen al port 22 del convidat (MV), on està el servidor SSH, redireccioarem els ports de la següent forma:

```
VBoxManage modifyvm "Nom_de_la_MV" --natpf1 "servidorSSH, tcp,, 2222,, 22"
```

Al posar **--natpf1**, estem dient que l'adaptador de xarxa 0 està en mode NAT i per ell rebrà les peticions el servidor SSH

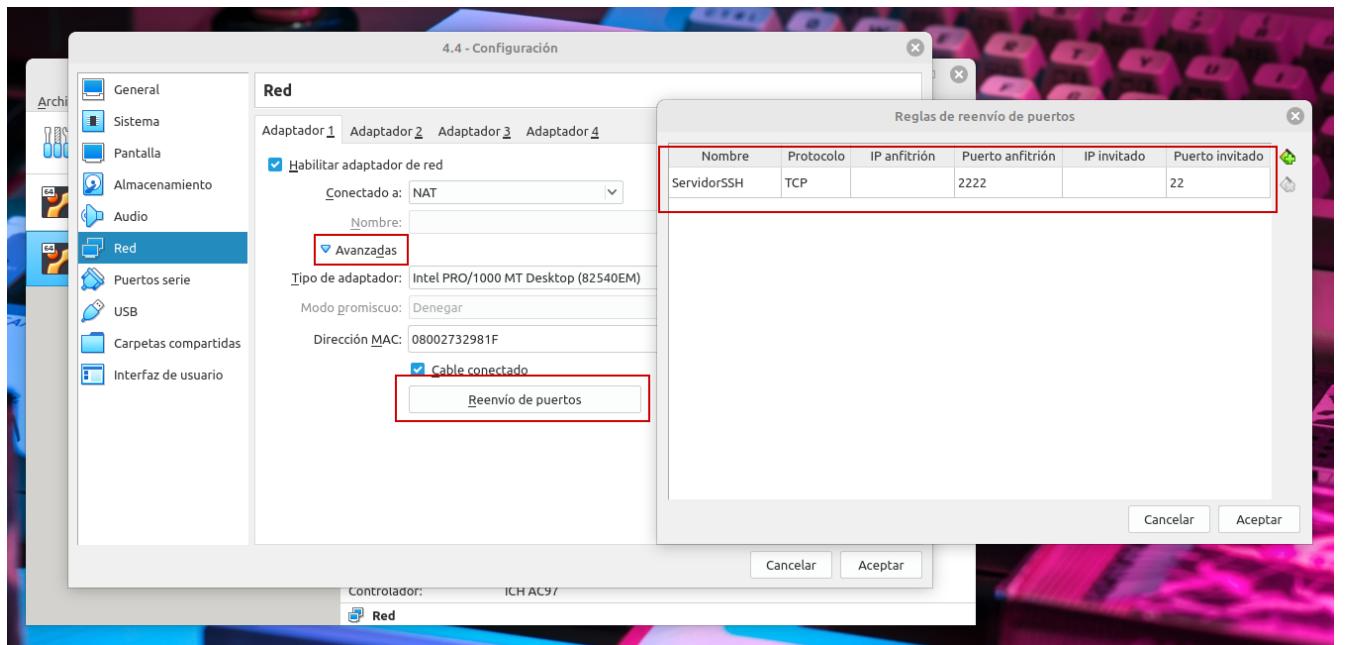
El nom **servidorSSH** és un nom simbòlic que emprarem per gestionar aquesta redirecció, per exemple, si volem eliminar-la:

```
VBoxManage modifyvm "Nom_de_la_MV" --natpf1 delete servidorSSH
```

En una redirecció hem d'especificar les IPs, per exemple, l'**amfitrió té varies targetes i el convidat l'hem configurat de forma estàtica*** (a pesar que la targeta estiga en mode NAT i per tant es tinga un servidor DHCP), la IP de l'amfitrió va davant del port de l'amfitrió i la IP de convidat, davant del port del convidat:

```
VBoxManage modifyvm "Nom_de_la_MV" --natpf1 "servidorSSH, tcp, 192.168.1.5, 2222, 10.0.2.50, 22"
```

El redirecccionament de ports es pot fer també de forma gràfica mitjançant la secció de "Xarxa de la MV".

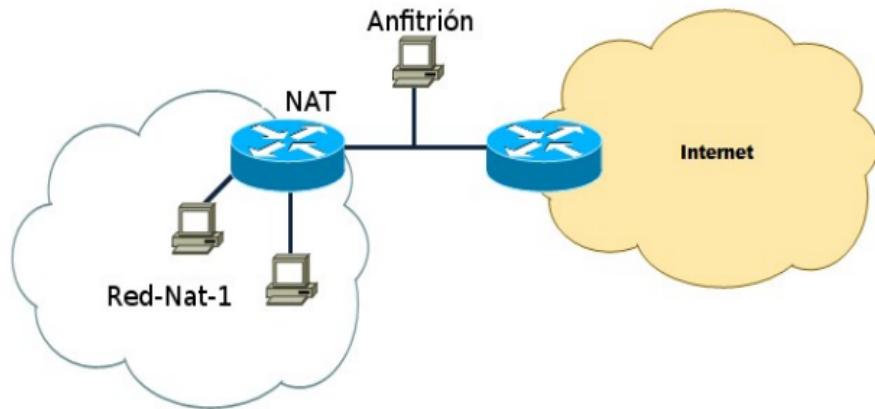


i Per a què serveix el protocol DHCP?

- DHCP és un protocol que es **configura en servidors**.
- Un servidor té un **llistat d'adreces IP dinàmiques i les va assignant** als clients conforme aquestes van quedant lliures, sabent en tot moment qui ha estat en possessió d'aixes IP, quan de temps la ha tingut i qui se li ha assignat després.
- Així **els clients d'un xarxa IP poden aconseguir els seus paràmetres de configuració automàticament**.
- Aquest protocol es va publicar en octubre de 1993 i la seua implementació actual està en RFC 2131.
- Per a DHCPv6 es publica el RFC 331.
- **VirtualBox permet configurar el servei DHCP en diverses modalitats: NAT, Xarxa Nat, Xarxa sols-amfitrió.**

6.3.2 Xarxa NAT en VirtualBox

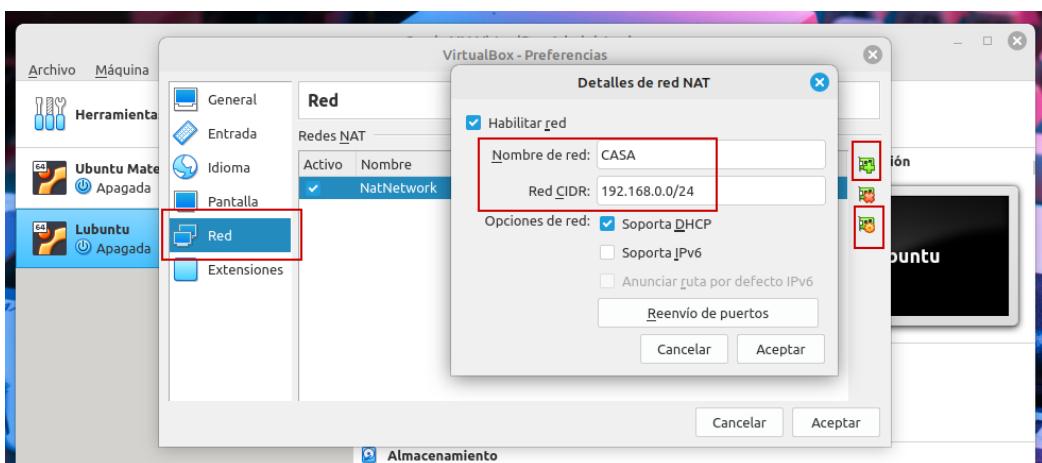
Funciona com el router de la nostra casa, és a dir, **els equips que estiguem dins de la mateixa Xarxa NAT podran comunicar-se entre ells, i esta és la diferència amb el mode NAT vist anteriorment, el qual sempre construïa una xarxa amb un únic equip i no de dicsos com ara és el cas.



Creació d'una xarxa NAT

Podem fer-ho de dues formes:

- Des de l'intèrpret de comandes escriure'm `VBoxManage natnetwork add --netname CASA --network 192.168.0.0/24`.
- Des del menú del VB (les imatges corresponen a la versió 6 de VB): "Fitxer --> Preferències --> Xarxa"



Des de l'entorn gràfic podrem, també, configurar el **reenviament de ports**.

Podem **llistar la informació de les xarxes NAT** disponibles i així comprovar els paràmetres que acabem de crear:

```
VBoxManage list natnets
```

Com podem veure, sols hi ha en aquest moment una única xarxa NAT anomenada **CASA** i podem destacar la següent informació:

```
paco@tufdash:~$ VBoxManage list natnets
NetworkName:      CASA
IP:               192.168.0.1
Network:          192.168.0.0/24
IPv6 Enabled:     No
IPv6 Prefix:      fd17:625c:f037:2::/64
DHCP Enabled:    Yes
Enabled:          Yes
loopback mappings (ipv4)
                  127.0.0.1=2
```

El servidor DHCP pot detindre's o activar-se de manera independent, amb els següents comandaments:

```
VBoxManage natnetwork modify --netname CASA --dhcp off
```

```
VBoxManage natnetwork modify --netname CASA --dhcp on
```

La xarxa NAT pot detindre's i seria com apagar el router, és a dir, la xarxa quedaría sense eixida a l'exterior encara que tindria connexió entre els equips connectats a la mateixa xarxa NAT:

```
VBoxManage natnetwork stop --netname CASA
```

```
VBoxManage natnetwork start --netname CASA
```

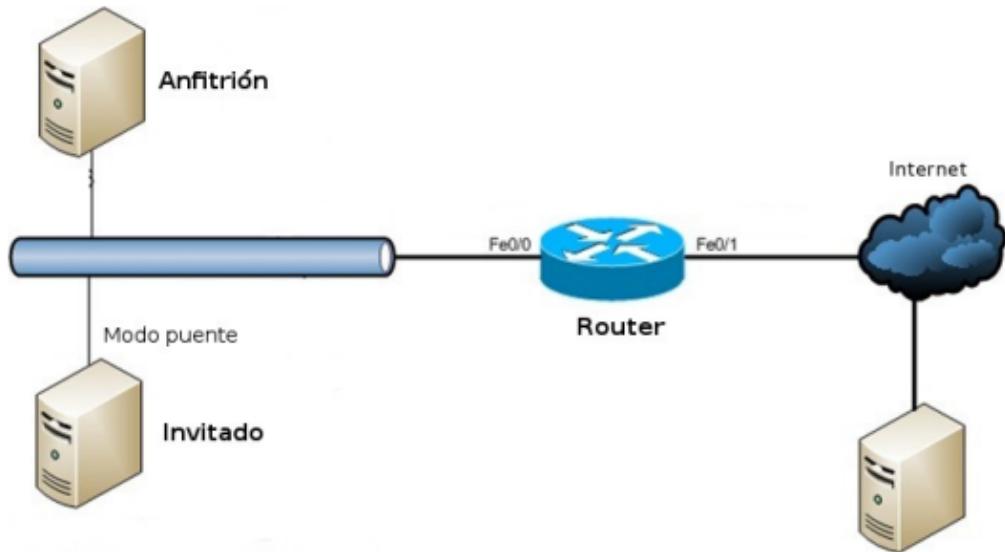
Finalment, per **eliminar la xarxa NAT** executariem:

```
VBoxManage natnetwork remove --netname CASA
```

Aquestes opcions també **poden fer-se des de l'entorn gràfic de VB**.

6.3.3 Adaptador pont en VirtualBox

El mode "Adaptador pont" **simula que la targeta virtual està connectada al mateix switch que la targeta física de l'amfitrió**, per tant, la MV va a comportar-se com si fos un equip més dins de la mateixa xarxa física en la que està l'equip amfitrió. Així doncs, si l'amfitrió obté una adreça IP per DHCP, el host també la conseguirà. L'esquema de xarxa seria el següent:

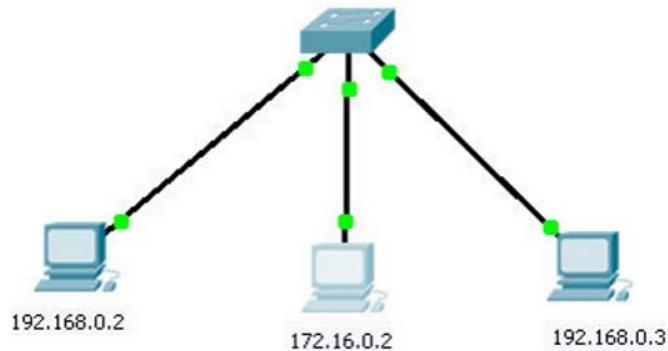


Com aconsegueix VB simular-ho?

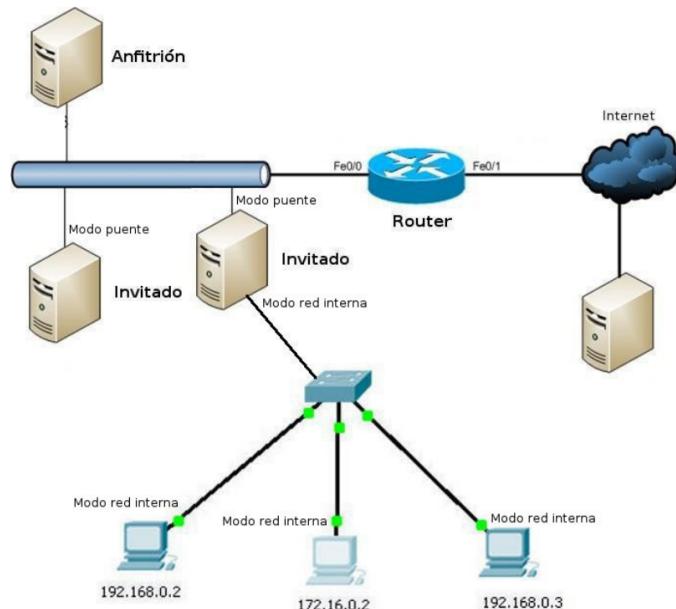
Un **bridge** afegí un nivell d'inteligència a una connexió entre xarxes. Connecta dos segments de xarxes iguals o distints. Podem veure un *bridge* com un classificador de correu que mira les adreces dels paquets i els col·loca a la **xarxa** adequada.

6.3.4 Xarxa interna

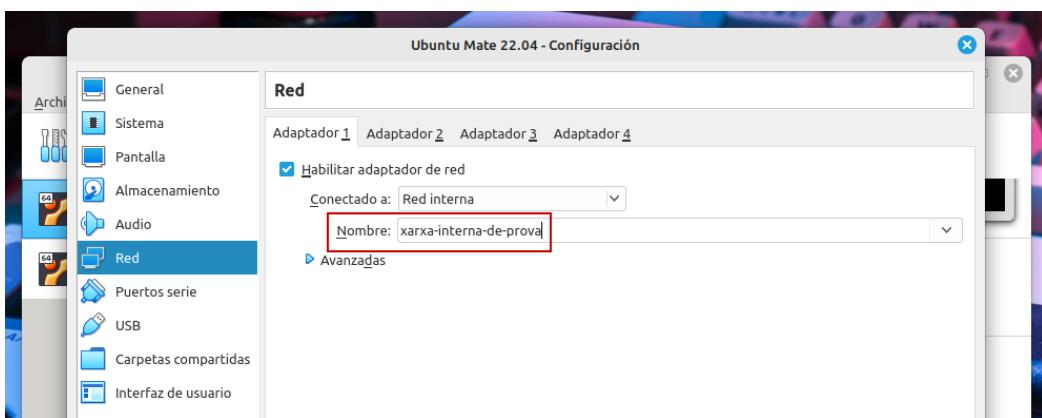
Amb aquesta configuració de targetes de xarxa, podem construir xarxes aïllades, en les quals **sols hi haurà comunicació entre les MVMV que pertanyen a la mateixa xarxa interna**.



Per tal de connectar xarxes internes a l'exterior, haurem de crear MMVV que funcionen com **routers** i disposen de dues targetes de xarxa, d'aquesta forma podrem construir un camí cap a Internet. Aquesta màquina que funcionaria com a router, haurà de tindre alguna de les seues targetes en NAT o pont, per poder ixir físicament a l'exterior.



Les xarxes internes de VB s'identifiquen a través d'un nom i **totes les MMVV que tinguen una targeta en mode xarxa interna amb el mateix nom formaran una única xarxa**. El nom de la xarxa interna s'especifica després de triar el mode; si no s'especifica, s'emprarà la xarxa interna per defecte de VB, anomenada **intnet**.



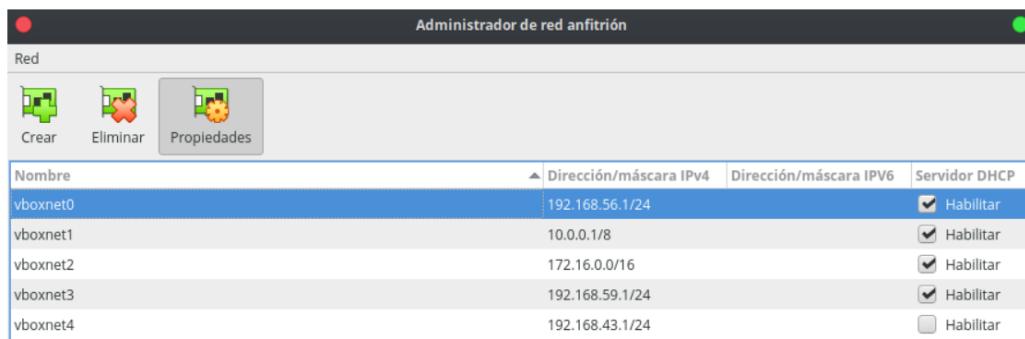
6.3.5 Adaptador sols-amfitrió

El mode "sols-amfitrió" s'empra per **crear un xarxa interna a la que pertanyerà també l'equip amfitrió, cosa que no succeeix al mode "xarxa interna"**.

Justificació

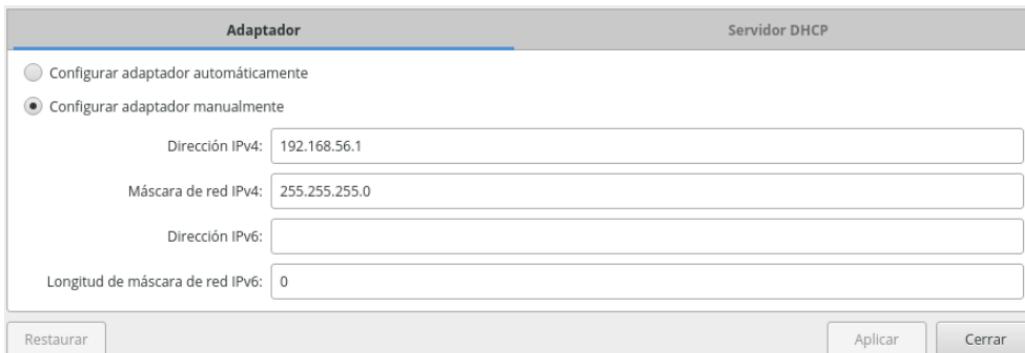
La connexió directa en una mateixa xarxa, de l'amfitrió amb una o més MMVV, ha de fer-se emprant el "mode pont" el qual necessita per funcionar, que el cable físic de xarxa estiga connectat a la targeta de xarxa de l'amfitrió. En cas contrari, és com si estiguera apagat el switch que connecta a l'amfitrió amb les MMVV, i per tant, no existeix connexió entre elles, ni amb l'amfitrió. Si estiguésssem en una **situació en la qual no tinguérem connexió de xarxa**, no podríem treballar amb la configuració anterior; aquest **problema el resol el mode sols-amfitrió**, doncs no empra la targeta física de la xarxa de l'amfitrió sino que es crea una virtual que estarà connectada al mateix switch virtual al que estaran connectades les targetes de xarxa de les MMVV amb el mateix mode de xarxa.

Per poder fer ús d'aquest mode, haurem de **crear la targeta de xarxa virtual a l'equip amfitrió**, per a tal cosa a l'administració de VB anirem a **Fitxer -> Administrador de xarxa-amfitrió**.



A partir d'aquest moment **existeixen tantes targetes noves de xarxa com creem**.

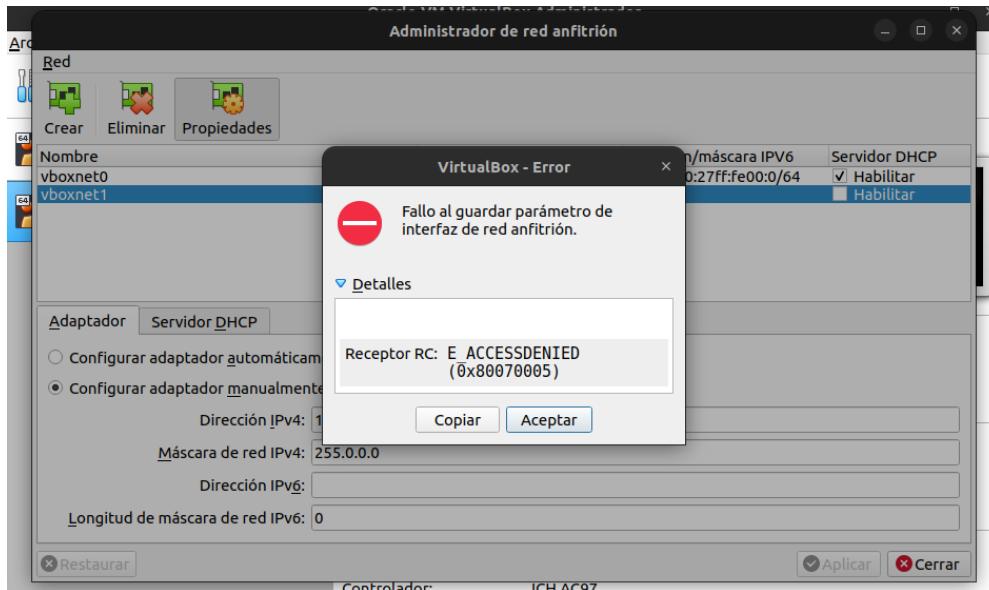
Aquestes targetes hi ha que **assignar-les una IP** de la xarxa que hagèm triat, i ações fa configurant els camps del recuadre situat en la part inferior de la finestra. Ho farem seleccionant previament vboxnet0:



També podrem activar un servidor DHCP per evitar configurar manualment les targetes de xarxa de les MMVV que es connecten...

Error E_ACCESSDENIED

Algunes de les activitats i pràctiques proposades necessiten de la modificació de les xarxes **sols anfitrió**, però podem trobar-nos davant errors al moment de configurar-ho com el següent:



Aquest error es deu a que a partir de la versió 6.1.28 van afegir unes noves configuracions, que entre altres coses aceten el rang vàlid de xarxes disponibles per a xarxes **sols anfitrió**.

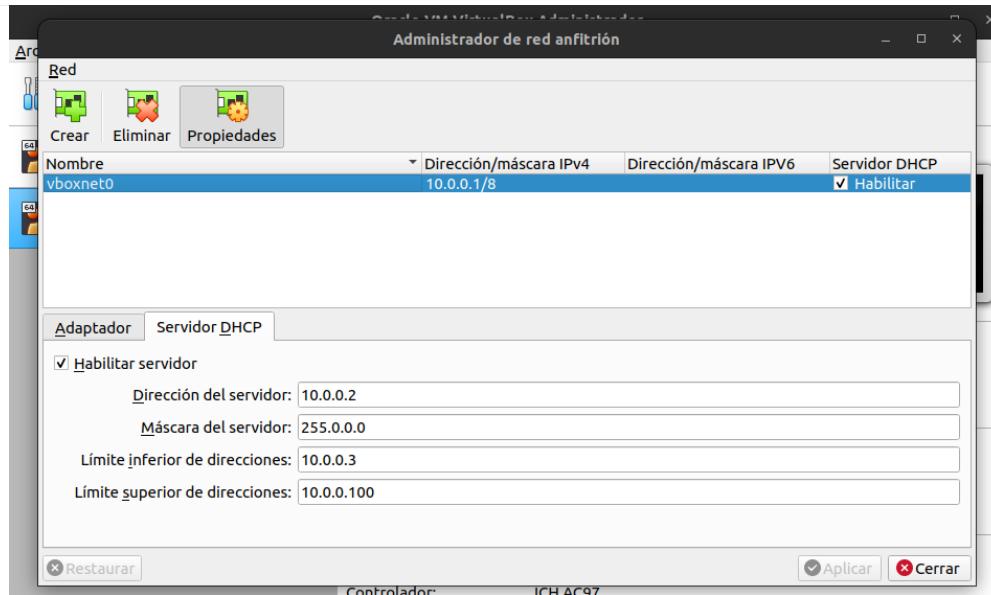
Açò desemboca en que sols s'accepten xarxes **sols anfitrió** en el rang 192.168.56.0/21.

Per deshabilitar aquesta restricció, editarem el fitxer /etc/vbox/networks.conf (que pot no existir i haurem de crear-lo) i afegirem el rang

```
1 * 0.0.0.0/0 ::/0
```

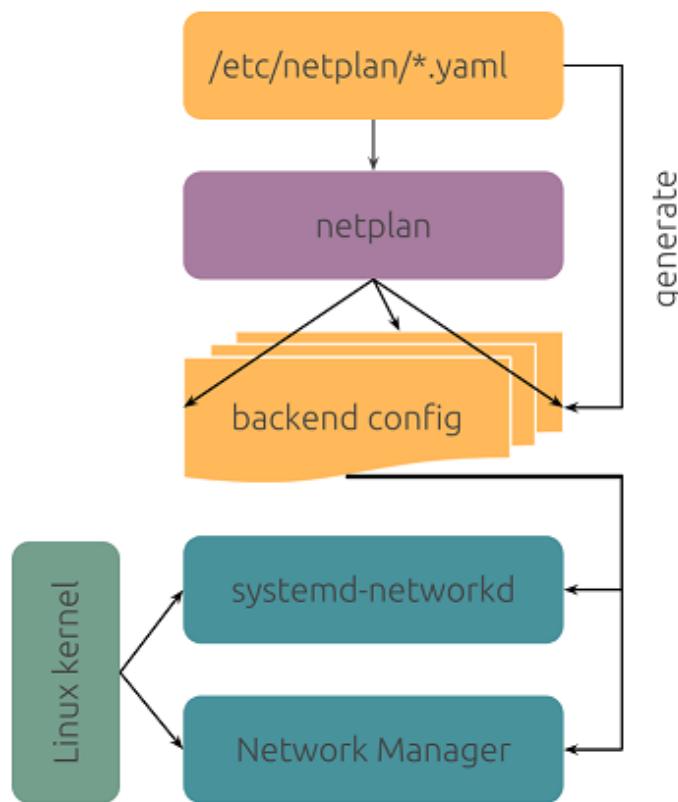
que bàsicament habilita totes les xarxes. D'aquesta forma podrem emprar qualsevol xarxa en mode **sols anfitrió**.

```
paco@tufdash:~$ sudo mkdir /etc/vbox
paco@tufdash:~$ sudo touch /etc/vbox/networks.conf
paco@tufdash:~$ sudo nano /etc/vbox/networks.conf
paco@tufdash:~$ cat /etc/vbox/networks.conf
* 0.0.0.0/0 ::/0
paco@tufdash:~$
```



6.4 Netplan

Amb l'arribada d'**Ubuntu 18.04** arribaren canvis a la configuració dels serveis de xarxa.



A les versions anteriors, tota la configuració es realitzava per interfície gràfica o mitjançant fitxers de configuració, situats en **/etc/network**. A partir d'ara, tindrem les dues opcions, però els fitxers de configuració es troben a **/etc/netplan** i tenen extensió **yaml**.

```
xal@mate:~$ ls /etc/netplan/
01-network-manager-all.yaml
xal@mate:~$
```

Aquest fitxer és el que tindrem que modificar per tal d'aconseguir la configuració de xarxa que necessitem en cada cas.

```
GNU nano 6.2          /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
```

Aquesta és la configuració per defecte de la xarxa. Amb aquesta configuració és la interfície gràfica l'encarregada de controlar tots els dispositius de la xarxa. Aquesta opció s'estableix a la línia: `renderer: NetworkManager`.

A la majoria dels casos amb aquesta configuració tindrem suficient però no tindrem control sobre els dispositius de la xarxa.

Per tal d'indicar que anem a ser nosaltres els qui definim el comportament i configuració de les interfícies de xarxa, haurem de modificar la línia anterior per: `renderer: networkd`.

A partir d'aquest moment haurem d'especificar tota la informació necessària per al funcionament dels dispositius de xarxa.

Anem a veure diferents exemples de configuracions de **netplan**, aquests exemples són bàsics però suficients per poder realitzar exercicis.

Informació

Abans de veure els exemple, hi ha que tindre en compte que els fitxers en format **yaml** no acceptaven tabulacions al principi i per tal de realitzar les sangries del text havíem d'emprar espais.

A les versions més noves d'Ubuntu **el fitxers yaml ja suporten la tabulació**.

6.4.1 Configurar targeta de xarxa per DHCP

```
1  network:
2    version: 2
3    renderer: networkd
4    ethernets:
5      enp0s3:
6        dhcp4: yes
```

On podem veure:

- `renderer: networkd` -- configurem nosaltres el dispositiu de xarxa
- `ethernets` -- interfícies de xarxa a configurar
- `enp0s3` -- nom de la interfície de xarxa a configurar
- `dhcp4: yes` -- DHCP activat

Aquest tipus de configuació la utilitzarem quan tinguem una targeta de xarxa sobre un adaptador de VirtualBox que accepte DHCP, és a dir, NAT, Xarxa NAT i Sols anfitrió.

6.4.2 Configurar targeta de xarxa amb IP fixa

```

1 network:
2   version: 2
3   renderer: networkd
4   ethernets:
5     enp0s3:
6       addresses: [10.0.2.10/24]
7       nameservers:
8         addresses: [8.8.8.8, 8.8.4.4]
9       routes:
10      - to: default
11        via: 10.0.2.2

```

A banda dels punts anteriors podem veure:

- **addresses**: [10.0.2.10/24] -- adreça de xarxa en format CIDR
- **nameservers**: -- a partir d'aquesta línia, configuració dels DNS.
- **routes**: -- gestió d'enrutament local, per exemple: porta d'enllaç (to: default - via...)

Gateway4 deprecated

```

1 network:
2   version: 2
3   renderer: networkd
4   ethernets:
5     enp0s3:
6       address: [10.10.10.2/24]
7       gateway4: 10.10.10.1
8       nameservers:
9         addresses: [8.8.8.8, 8.8.4.4]

```

6.4.3 Aplicar les configuracions

La modificació del fitxer ubicat en **/etc/netplan** no implica que s'apliquen els canvis. Cada vegada que modifiquem aquest fitxer **yaml** haurem de realitzar algunes accions:

- **sudo netplan -debug try** : tracta d'aplicar la configuració que hem definit. Si no hi ha errades ixirà un contador per tornar a la configuració anterior o pulsant **ENTER** aplicar la nova.
- **sudo netplan apply** : aplica directament la configuració que hem definit. S'ha d'emprar en el cas d'estar completament segur que tot és correcte.

```

xal@mate:~$ sudo netplan -debug try
[sudo] contraseña para xal:
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 94 seconds

```



<https://pgalera.github.io/xal/>