Conceptes avançats de LAN

Jaume Abella i Fuentes
José M. Barceló Ordinas
Guiomar Corral i Torruella
Enric Peig Olivé

P06/19026/01891

UOC
www.uoc.edu

Índex

Introducció 5

Objectius 6

1. Commutació a les LAN: dominis de col·lisió 7

2. Estàndards per a xarxes d'àrea local 13
2.1. Fast Ethernet i Gigabit Ethernet 14
2.1.1. Xarxes Fast Ethernet 100BaseT 15
2.1.2. Gigabit Ethernet 17
2.1.3. Funcionament de Gigabit Ethernet 19
2.1.4. Exemples d'aplicació de Gigabit Ethernet 20
2.2. Cablejat estructurat: EIA/TIA 568 22
2.2.1. Topologia 23
2.2.2. Medi físic 23
2.2.3. Certificació 24
2.3. Xarxes sense fil: norma IEEE802.11 26
2.3.1. Nivell físic 26
2.3.2. Control d'accés al medi 28
2.3.3. Topologia 28

3. Noves prestacions de les xarxes Ethernet 30
3.1. Ethernet *full-duplex* 30
3.2. Control de flux 31
3.3. Sistemes multiestàndard: autonegociació 31

4. Xarxes d'àrea local virtuals: VLAN 33
4.1. Característiques de les VLAN 33
4.2. Tipus de VLAN 35
4.2.1. VLAN estàtiques i VLAN dinàmiques 36
4.2.2. VLAN basades en el port o en el protocol 37
4.3. IEEE 802.1Q 37

5. NAT 41
5.1. NAT estàtic 42
5.2. NAT dinàmic 43
5.3. PAT (port address translation) 45
5.4. LSNAT (*load sharing NAT*) 48

Resum 51

Exercicis d'autoavaluació 53

Solucionari 55

Glossari 58

Bibliografia 59

Introducció

Un cop vistos els conceptes bàsics de xarxes d'àrea local, d'una banda, i del protocol IP, de l'altra, en aquest mòdul presentem una sèrie de millores que s'han anat introduint al món de les xarxes per poder oferir noves i millors prestacions.

Veurem, d'una banda, com s'han aplicat les tècniques de commutació de paquets a les xarxes d'àrea local, la qual cosa ha permès tenir xarxes més eficients amb els mateixos medis de transmissió. També els nous estàndards Ethernet, que han aparegut per poder aprofitar els avenços en el disseny de les línies de transmissió (com les fibres òptiques) i treure partit de l'increment de capacitat que això comporta. Un altre avenç molt important en el disseny i implementació de xarxes d'àrea local és el cablatge estructurat, que defineix on i com s'han de posar les línies de connexió.

D'aparició recent, però d'èxit rotund, cal considerar les tecnologies que permeten les xarxes d'àrea local sense fil. Dedicarem un apartat a descriure aquestes tecnologies.

Les xarxes locals tradicionals agrupen els usuaris segons la seva situació física i la connexió entre els dispositius. Però aquesta agrupació no sempre és adequada, ja que a vegades les necessitats són diferents. Veurem com les xarxes d'àrea local virtuals (VLAN) permeten l'agrupament lògic de dispositius o bé d'usuaris, en lloc de l'agrupament físic que oferien les xarxes tradicionals.

A causa del creixement exponencial d'Internet, la manca d'adreces es converteix en un problema. Veurem que un mètode per a solucionar aquest problema es basa en la traducció d'adreces de xarxa o NAT. Un altre problema que hi ha és la saturació dels servidors connectats a Internet. A causa que el trànsit a Internet és cada cop més gran, les peticions als servidors també augmenten en gran manera. Aquest fet provoca que els servidors cada cop estiguin més saturats i, tot i que les seves prestacions augmenten progressivament, en alguns casos potser és millor augmentar el nombre de servidors que donen el mateix servei. D'aquesta manera, es podrà distribuir la càrrega entre els diferents servidors. Per a solucionar aquest problema hi ha la tècnica anomenada *LSNAT* (*load sharing network address translation*), que permet de combinar la traducció d'adreces amb la distribució de la càrrega entre els servidors.

Objectius

En aquest mòdul didàctic l'estudiant disposa dels recursos necessaris per a assolir els objectius següents:

1. Entendre com es poden aplicar conceptes de commutació a les LAN, i com així augmenta l'eficiència de les xarxes.

2. Comprendre les diferències entre les xarxes Ethernet, Fast Ethernet, Gigabit Ethernet i les noves prestacions que utilitzen.

3. Conèixer les principals característiques del cablatge estructurat.

4. Conèixer les principals característiques de les xarxes sense fil.

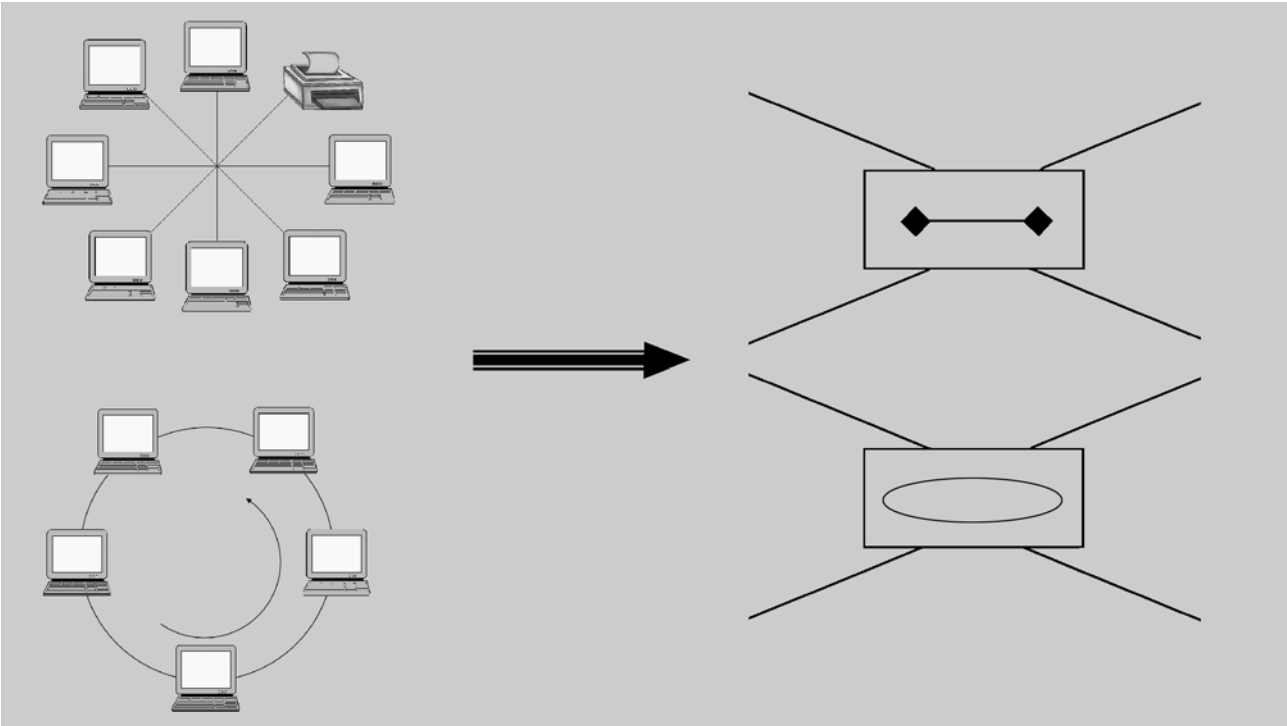
5. Entendre el funcionament i la utilitat de les xarxes d'àrea local virtuals.

6. Copsar la necessitat de la traducció d'adreces en el món Internet i comprendre el funcionament de NAT i LSNAT. Distingir els diferents tipus de traducció d'adreces i saber escollir el tipus adequat segons la situació i l'escenari.

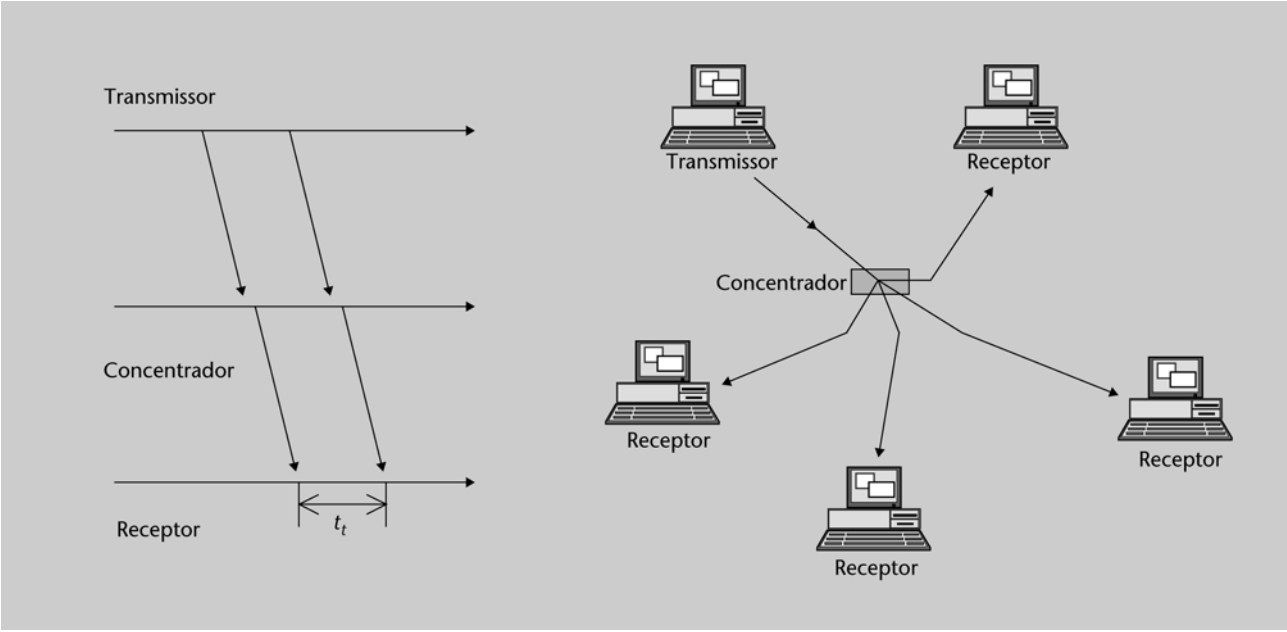
1. Commutació a les LAN: dominis de col·lisió

Recuperem la xarxa que vèiem abans, en què teníem una LAN amb topologia lògica en bus i topologia física en estrella.

A l'apartat 2.4 del mòdul 2 veureu la xarxa amb les topologies lògiques i les físiques.



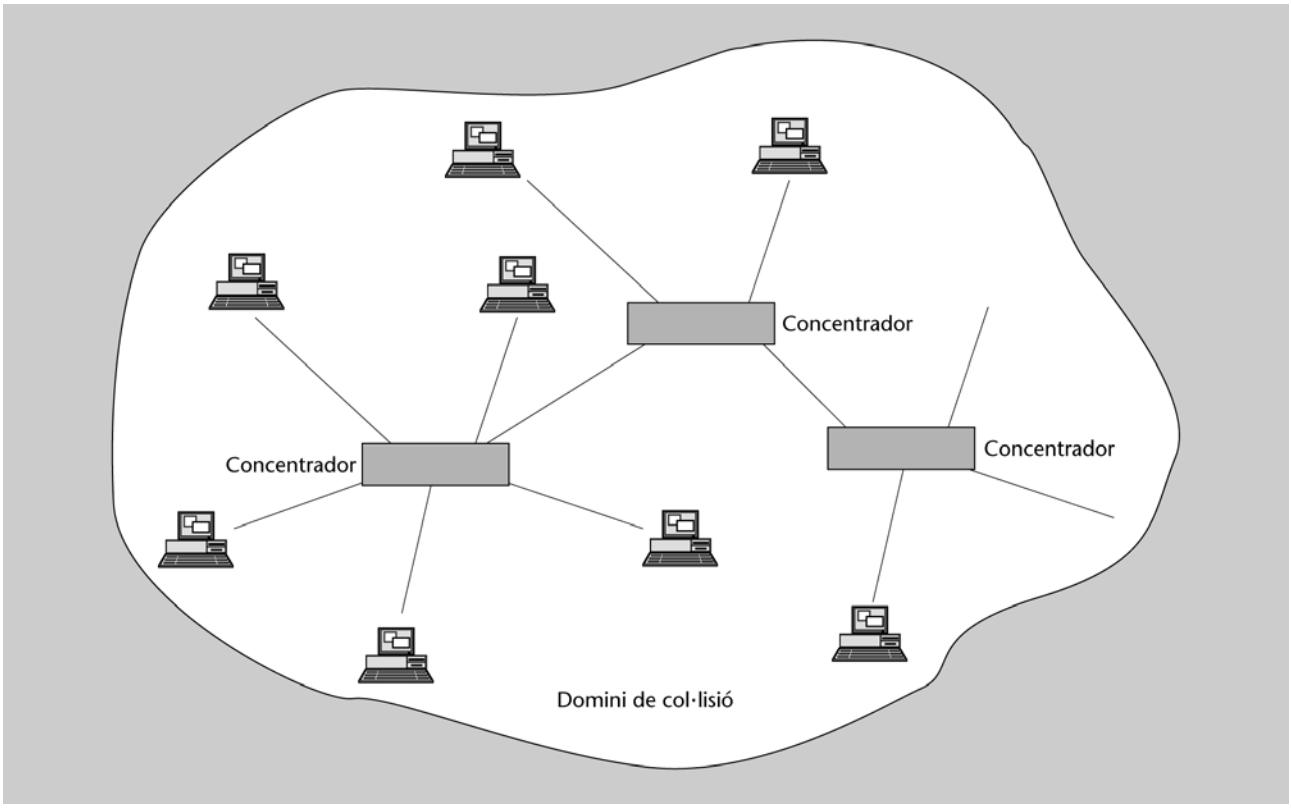
L'element que permet la interconnexió és un concentrador (o *hub*), que es comporta com un simple repetidor: tot el que hi arriba des de qualsevol port ho retransmet a tota la resta.



Tots els terminals han d'implementar el CSMA/CD. A efectes d'estudi, la presència del concentrador és anecdòtica, i podríem suposar-lo invisible. El senyal es difon pel medi fins a arribar a tots els terminals.

Al diagrama de temps s'ha reflectit un petit retard del senyal al seu pas pel concentrador. Aquest retard és degut al fet que el concentrador és un repetidor i, per tant, ha de regenerar la temporització dels bits. Això implica un cert retard d'uns pocs bits.

Concentrador, terminals i tot el cablejat estan dins d'un mateix medi. És el que anomenem **domini de col·lisió**. Un domini de col·lisió és un àmbit dins del qual un únic MAC governa les transmissions. Si dos terminals inicien la comunicació simultàniament en un mateix domini de col·lisió, hi haurà col·lisió. En un domini de col·lisió 10BaseT, cap terminal ni cap combinació de terminals pot arribar mai a transmetre en total més de 10 Mbps.



Per tant, si eixamplem una xarxa a còpia d'augmentar el nombre de terminals, fins i tot si hi afegim més concentradors, tanmateix, tindrem un únic domini de col·lisió i, per tant, cada cop la capacitat disponible per a cada terminal individual serà menor.

Només hi ha dues maneres d'augmentar la capacitat d'una xarxa:

- **Canviar l'estàndard** per un altre a major velocitat. Per exemple, passar de 10Base-T a 100Base-T o 1000Base-T. Aquesta solució és bastant dràstica. Penseu que no només s'han de canviar els concentradors (i potser el cablejat) sinó també totes les targetes dels terminals. Passar de 10 Mbps a 100 Mbps és car.

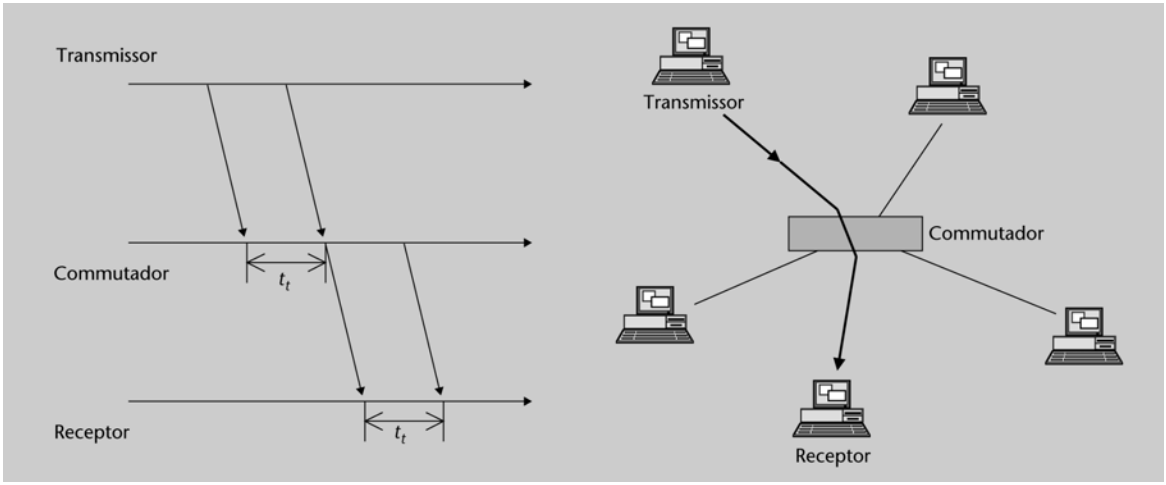
- **Segmentar el domini de col·lisió** de manera que el nombre de terminals per domini de col·lisió sigui inferior. Aquesta solució sovint és més senzilla. Per a dividir o interconnectar dominis de col·lisió necessitem un commutador. Els commutadors poden tenir vuit, setze o vint-i-quatre ports i, per tant, des d'aquest punt de vista són similars als concentradors. Però a diferència d'aquests, els ports d'un commutador tracten la informació individualment: cada trama que reben s'emmagatzema dins de la memòria del port (o la memòria assignada al port), s'analitzen els possibles errors i s'interpreta per decidir on es dirigeix.

En segmentar la xarxa, com que cada port rep la trama, l'emmagatzema i es retransmet pel port de sortida tornant a aplicar el CSMA/CD, estem parlant de dominis de col·lisió diferents. Cada port d'un commutador connecta dominis de col·lisió diferents.

Els ponts (*bridges*) són una solució similar. Funcionalment són el mateix que un commutador, però tècnicament es basen en arquitectures totalment diferents i s'han fet servir en altres èpoques. En l'actualitat s'utilitzen commutadors.

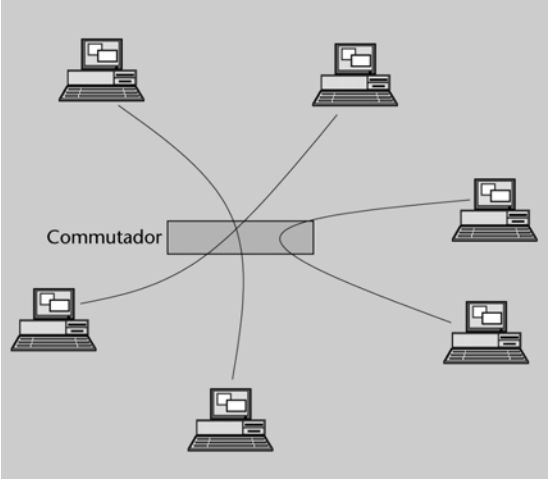
Un concentrador no du a terme cap d'aquestes operacions, la trama com a tal és irrellevant per a ell: quan en rep els primers bits els copia immediatament ("connecta" seria una paraula més gràfica) a tota la resta de ports. El concentrador no detecta errors ni interpreta ni res; des del punt de vista lògic, un concentrador és un sistema passiu.

Cal, però, reconèixer almenys un avantatge als concentradors sobre els commutadors. Per tal que un commutador pugui decidir què fa amb les trames entrants, cal que emmagatzemi les trames rebudes, encara que només sigui momentàniament, per poder processar-ne el contingut (bàsicament l'adreça de destinació i el CRC). Aquest emmagatmemament, com es reflecteix en el diagrama de temps següent, comporta un retard de transmissió:

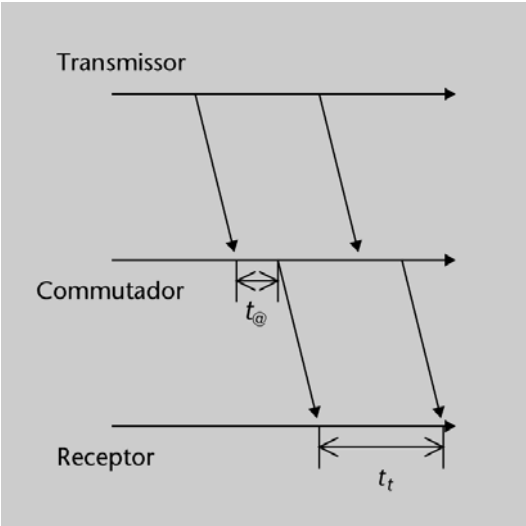


El retard de transmissió és, aproximadament, el doble que el que comporta l'ús de concentradors (si suposem retards de propagació negligibles). Com a

contrapartida, el commutador deixa els n–2 terminals restants amb el port lliure per a poder transmetre: un commutador pot, teòricament, mantenir $n/2$ transmissions simultànies de trames entre tots els ports:

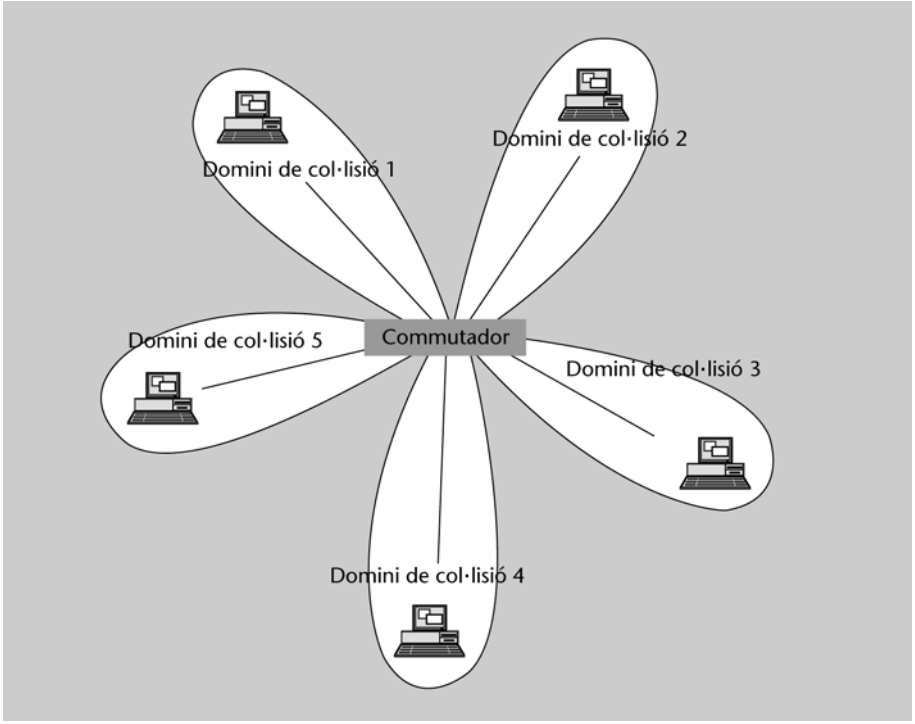


Hi ha commutadors que encaminen la trama abans fins i tot que hagi estat rebuda completament. Són els **commutadors ràpids** o *cut-through*, que tan bon punt reben el camp d'adreça (al 14è. byte) en decideixen el port de sortida i comencen a transmetre la trama. El retard és molt inferior, però en cas que la trama sigui errònia la transmetran igualment, ja que no ho poden saber.

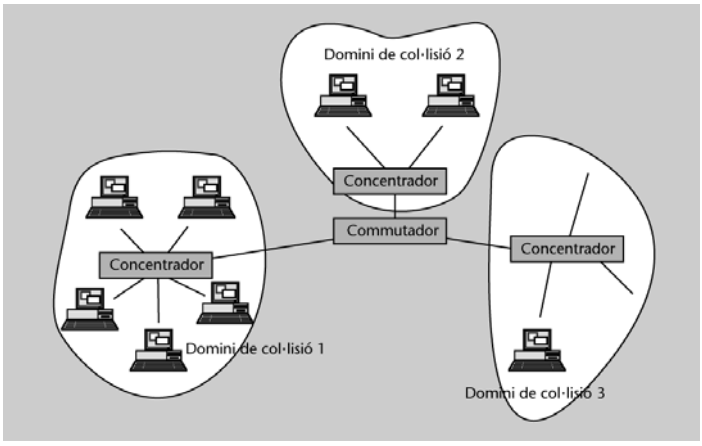


Els commutadors ràpids presenten un problema addicional: si hi ha una col·lisió al domini origen es propaga al domini destinació. Per a solucionar aquesta eventualitat, hi ha una variant de commutadors (*Run-free cut-through*) que espera la finestra de col·lisió (64 bytes) per assegurar-se que no hi ha col·lisió al domini origen.

A la figura anterior, cada terminal té el seu propi domini de col·lisió. De fet, les col·lisions encara són possibles, ja que es pot donar el cas que el port del commutador i el terminal associat decideixin casualment començar a transmetre de manera simultània.



Si en comptes de connectar directament al commutador els terminals connectem concentradors, el sistema també millora quant a rendiment respecte d'un connectat únicament amb concentradors:



En qualsevol cas, cada domini de col·lisió addicional suposa un increment de la capacitat agregada de la xarxa si les trames van majoritàriament adreçades a estacions situades en el mateix domini de col·lisió que l'estació origen. El commutador filtra aquestes trames de manera que no ocupin innecessàriament la resta de dominis de col·lisió. Teòricament, si segmentéssim el domini original perfectament, el commutador no retransmetria cap trama, amb la qual cosa la capacitat de la xarxa s'hauria multiplicat directament pel nombre de nous dominis de col·lisió.

Els commutadors coneixen la posició dels terminals per un procediment d'aprenentatge automàtic. Mentre que aquest procediment no hagi finalitzat (per exemple, quan el commutador arrenca), el commutador reparteix les trames per tots els ports: com que no coneix

encara la posició de les estacions, actua de manera similar a un concentrador. Quan rebi les primeres trames descobrirà, mirant l'adreça origen, la posició de totes les estacions.

En realitat, quan afegim un commutador, la segmentació mai no serà tan dràstica*; per tant, el commutador no filtra tot el trànsit. Conseqüentment, cada domini suporta el seu trànsit intern, més un percentatge del trànsit dels altres dominis. En general, si el trànsit no és intern, ocuparà només dos dominis de col·lisió; per tant, la resta de *n–2* dominis estarà lliures per a transmetre. En el pitjor dels casos, tot el trànsit ocuparà dos dominis i, per tant, la inserció d'un commutador augmenta la capacitat de la LAN agregada entre *n*/2 i *n* vegades, on *n* és el nombre de ports. Això suposant que es canvia un concentrador per un commutador. Si hi ha més commutadors, llavors una única trama pot arribar a ocupar tres o més dominis de col·lisió.

*** No estem parlant de terminals connectats accidentalment.**

Els commutadors es poden interconnectar com si fossin concentradors per fer xarxes més grans. De fet, com que cada domini de col·lisió té un MAC independentment, l'abast màxim d'una xarxa amb commutadors és teòricament il·limitat.

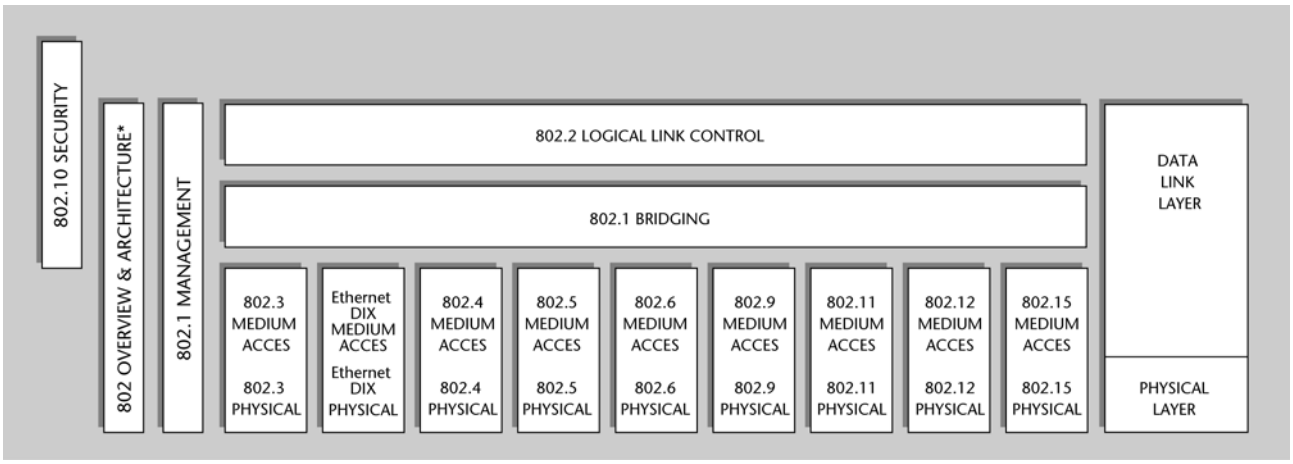
2. Estàndards per a xarxes d'àrea local

Gairebé tots els estàndards de LAN han estat creats per l'Institut d'Enginyers Elèctrics i Electrònics (IEEE) dels EUA, dins dels grups IEEE802.xx, i després els estàndards han estat acollits per l'Organització Internacional d'Estandardització (ISO), que ha anomenat els grups idèntiticament però fent servir el prefix ISO8802.xx.

Exemple

L'ISO8802.3 és totalment equivalent a l'IEEEE802.3.

Tots els estàndards IEEE802, a excepció de l'IEEE802.1 i l'IEEE802.2, es refereixen a protocols MAC.



- **IEEE802.1**: defineix procediments per a interconnexió i gestió de commutadors, protocols per a LAN virtuals i seguretat criptogràfica de la transmissió.

- **IEEE802.2**: defineix el nivell d'enllaç lògic adequat per a LAN.

- **Ethernet-DIX-II**: estàndard *de facto* de CSMA/CD a 10 Mbps. Variants de l'estàndard a bastament emprades són Fast Ethernet (100 Mbps) i Gigabit Ethernet (1 Gbps). Per a totes és comú el canvi del MAC CSMA/CD per commutadors.

- **IEEE802.3**: MAC CSMA/CD. Similar però no interoperable amb Ethernet-DIX-II.

- **IEEE802.4**: MAC *token bus*. Implementa un MAC equivalent a *token ring*, però sobre topologia física i lògica de bus. Actualment es troba en desús.

- **IEEE802.5**: MAC *token ring* derivat del protocol Token Ring d'IBM, i compatible amb ell.

- **IEEE802.6**: MAC DQDB o *Distributed Queue Dual Bus*. Està dissenyat per a xarxes d'àrea metropolitana. Tot i que és un bus lògic, físicament és un anell, el que li confereix tolerància a talls a la línia. Actualment es troba en desús.

Les xarxes d'àrea metropolitana (MAN, *Metropolitan Area Networks*) eren un concepte rellevant al començament dels noranta, quan faltaven estàndards per a xarxes l'abast de les quals estigues entre el d'una LAN i el d'una WAN. En l'actualitat, el concepte ha quedat marginat, perquè a les LAN ja es fan servir tecnologies de WAN com la commutació; per tant, l'espai teòric de les MAN ha quedat pinçat.

- **ANSI X3T12** o **FDDI** (*Fibre Distributed Data Interface*): MAC *token ring* doble amb propietats de tolerància a fallades. Inicialment estava dissenyat per a xarxes MAN, però va tenir un nínxol de mercat en xarxes de servidor (*clusters*). Actualment es troba en desús, però encara se'n poden trobar instal·lacions en funcionament.

- **IEEE802.11** o **WiFi**: (*Wireless Fidelity*): MAC CSMA/CA per a xarxes sense fils. Actualment és l'estàndard de LAN de major progressió.

- **IEEE802.12** o **100VG-AnyLAN***: estàndard a 100 Mbps aparegut als noranta com a substitució de l'Ethernet a 10 Mbps. És un MAC *token ring* amb prioritats i procediments per a facilitar la interoperabilitat amb l'IEEE802.3. Actualment es troba en desús a causa de l'èxit comercial de Fast Ethernet.

*** VG ve de *Voice Grade* (categoria de veu) en referència al tipus de cablejat per telefonia que permet aquest estàndard. AnyLAN fa referència al fet que permet interoperabilitat entre CSMA/CD i *token ring*.**

- **IEEE802.15** o **Bluetooth**: protocol similar a l'IEEE802.11 però ajustat als requeriments de les *piconets* (picoxarxes o xarxes molt petites). És molt apropiat per a interconnectar ratolins, teclats, mòbils, agendes electròniques, ordinadors portàtils i, en general, petits sistemes alimentats per bateries.

Bluetooth

El nom *Bluetooth* prové del rei víking Harald Blatand (segle X dC), que va unificar i controlar Dinamarca i Noruega. D'aquí ve la inspiració del nom: amb aquesta tecnologia es pretén unificar i interconnectar dispositius. Es creu que una de les aficions d'aquest rei era menjar móres, i per això tenia el "tint" blau de les dents (*bluetooth* vol dir 'dent blava' en anglès).

L'estàndard Ethernet ja s'ha descrit al mòdul 2. En els apartats següents ens centrarem en els aspectes que se citen a continuació:

- Variants d'Ethernet: FastEthernet i Gigabit Ethernet
- Cablejat estructurat
- Xarxes sense fils: norma IEEE802.11.

2.1. Fast Ethernet i Gigabit Ethernet

Fast Ethernet és una tecnologia de xarxes d'àrea local d'alta velocitat que ofereix una amplada de banda deu vegades més gran que Ethernet, tant a l'usuari final com als servidors d'una xarxa d'àrea local. Així, doncs, Fast Ethernet permet de transmetre a velocitats de 100 Mbps.

El grup IEEE Higher Speed Ethernet Study Group es va formar per a estudiar les possibilitats que hi havia de transmetre a velocitats de 100 Mbps utilitzant

la tecnologia Ethernet. Aquest grup va establir diferents objectius per a la nova Ethernet d'alta velocitat, però van sorgir divergències respecte de la manera d'accedir al medi físic. El debat es fonamentà en el fet que aquesta Ethernet d'alta velocitat pogués continuar suportant el CSMA/CD com a protocol d'accés al medi. Per això, el grup d'estudi es va dividir en dos grups separats: l'aliança Fast Ethernet i el Fòrum 100VG-AnyLAN. Cada grup va produir una especificació per a treballar amb Ethernet a altes velocitats:

– L'aliança Fast Ethernet va produir **100BaseT**, l'especificació IEEE per a la implementació d'Ethernet a 100 Mbps sobre parell trenat no apantallat (UTP) i parell trenat apantallat (STP). La capa de control d'accés al medi és compatible amb l'especificació IEEE 802.3. Per tant, es manté el protocol CSMA/CD i únicament es modifica la velocitat a 100 Mbps; tot i que, evidentment, aquest fet implica dividir per deu la longitud màxima de la xarxa per a poder conservar el mateix format de trama.

– **100VG-AnyLAN** és una especificació IEEE per a les implementacions de xarxes Ethernet i Token Ring sobre quatre parells trenats no apantallats. La capa d'accés al medi no és compatible amb l'especificació IEEE 802.3. El que es fa és crear un nou protocol d'accés al medi físic sense col·lisions i més eficient, però mantenint la mateixa estructura de trama.

Fast Ethernet es va estandarditzar per a IEEE mitjançant l'especificació IEEE 802.3u. En canvi, 100VG-AnyLAN es va estandarditzar per a IEEE mitjançant l'especificació IEEE 802.12.

2.1.1. Xarxes Fast Ethernet 100BaseT

Com hem comentat anteriorment, 100BaseT utilitza l'especificació IEEE 802.3 sobre el CSMA/CD que ja empraven les xarxes Ethernet. D'aquesta manera, 100BaseT manté el mateix format i mida de trama, el mateix mecanisme de detecció d'errors i el mateix mètode de detecció de col·lisions.

A més, 100BaseT suporta velocitats duals de 10 i 100 Mbps i, per tant, necessitarà mecanismes de detecció que seleccionin la millor velocitat segons les condicions de transmissió.

Targetes de xarxa

Hi ha targetes de xarxa que funcionen a 10 Mbps, d'altres a 100 Mbps i d'altres que poden treballar a totes dues velocitats.

Les xarxes 100BaseT presenten una característica opcional, anomenada ***autonegociació***, que permet a dos dispositius d'intercanviar informació sobre les seves capacitats per a crear un entorn de comunicacions òptim.

Exemple

Si dues estacions poden treballar a 10 Mbps o 100 Mbps i es volen intercanviar informació, escolliran la millor velocitat que suportin totes dues estacions: en aquest cas, 100 Mbps.

L'autonegociació permet la comunicació de certs paràmetres, com ara la velocitat de transmissió (10 Mbps o 100 Mbps), si el mode d'operació és *full duplex*, o bé la configuració de la senyalització entre dispositius.

Una de les diferències més importants entre 100BaseT i 10BaseT és el diàmetre de la xarxa: el diàmetre màxim d'una xarxa 100BaseT és de dos-cents cinc metres, aproximadament deu vegades més petit que el d'una xarxa Ethernet de 10 Mbps.

Podeu veure més sobre autonegociació en l'apartat 3.3 d'aquest mòdul didàctic.

El motiu d'aquesta reducció del diàmetre de la xarxa és que 100BaseT utilitza el mateix mecanisme de detecció de col·lisions que 10BaseT. Si recordem, en 10BaseT les limitacions de distància es definien perquè una estació que transmetia un paquet de mida mínima a l'estació més llunyana de la xarxa pogués detectar una col·lisió. Aquesta mida mínima de la trama era de 64 bytes.

Si volem mantenir aquesta mida mínima de 64 bytes en Fast Ethernet, hem de recordar que ara la velocitat de transmissió és deu vegades més gran, però la velocitat de propagació del medi no ha canviat (continuem parlant del mateix medi de transmissió). Consegüentment, haurem d'escurçar el domini de col·lisió: una estació que transmet a una velocitat deu vegades més gran haurà d'estar a una distància màxima deu vegades més petita. Així aconseguirem que qualsevol estació pugui detectar si s'ha produït una col·lisió mentre transmet la seva trama.

100BaseT suporta tres medis de transmissió en la capa física:

- 100BaseTx
- 100BaseFx
- 100BaseT4

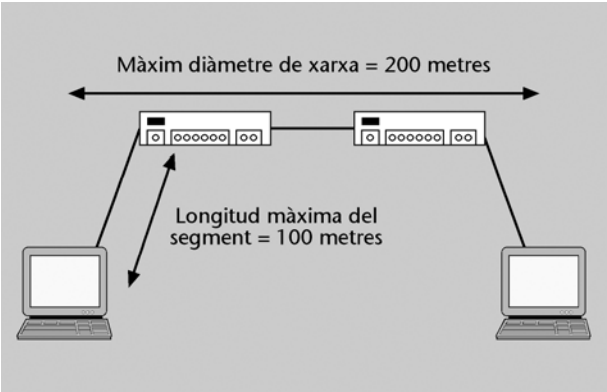
Les característiques del medis físics de 100BaseT es poden resumir en la taula següent:

Característiques	100BaseTx	100BaseFx	100BaseT4
Cable	Categoria 5 UTP o STP	62,5 / 125μ fibra multimode	Categoria 3, 4 o 5 UTP
Nombre de cables	2 parells	2 fibres	4 parells
Longitud màxima del segment	100 metres	400 metres	100 metres
Màxim diàmetre de la xarxa	200 metres	400 metres	200 metres

100BaseTx

100BaseTx suporta la transmissió de dades sobre cablejat UTP i STP. En concret, requereix que el cablatge UTP sigui de categoria 5, com a mínim, i funciona sobre dos parells.

L'especificació IEEE 802.3u permet un màxim de dos repetidors i un diàmetre màxim de xarxa d'uns dos-cents metres. A més, un segment, que es defineix com una connexió punt a punt entre dos dispositius, serà de cent metres, com a màxim.



Limitacions de 100BaseTx i 100BaseT4

100BaseFx

100BaseFx utilitza dues fibres òptiques multimode com a medi de transmissió. L'especificació IEEE 802.3u defineix que la distància màxima entre dos equips de dades ha de ser d'uns quatre-cents metres aproximadament. En cas que es necessiti un repetidor, la longitud màxima serà d'uns tres-cents metres.

100BaseT4

Si volem disposar de la tecnologia Fast Ethernet en una xarxa ja cablejada anteriorment i que utilitza un cablatge de categoria 3, haurem d'emprar l'especificació 100BaseT4. 100BaseT4 necessita els quatre parells de coure per a la transmissió de dades. Per això, en aquest cas només podrem parlar d'una xarxa *half duplex*.

L'especificació IEEE 802.3u permet un màxim de dos repetidors i un diàmetre màxim d'uns dos-cents metres. La longitud màxima d'un segment serà de cent metres, tal com es mostra en la figura anterior.

2.1.2. Gigabit Ethernet

La xarxa Fast Ethernet es va estendre molt ràpidament, i va superar les expectatives més optimistes. Com a conseqüència, els preus van baixar i se'n va popularitzar l'ús fins a l'usuari final. Això generava requeriments de velocitats superiors en la xarxa troncal (*backbone*) que no es podien atendre amb la tecnologia del moment, exceptuant ATM a 622 Mbps, que tenia uns preus astronòmics. Això va provocar que l'any 1995 el subcomitè 802.3 iniciés un nou grup de treball, que va crear la **Gigabit Ethernet**. El treball va acabar amb èxit el 29 de juny de 1998 amb l'aprovació del suplement 802.3z.

Per a augmentar la velocitat de 100 Mbps de Fast Ethernet fins a 1 Gbps, va ser necessari fer diversos canvis en la interfície física. Per això, Gigabit Ethernet és idèntic a l'especificació Ethernet des de la capa d'enllaç en endavant: s'ha mantingut el mateix format de trama que en la 802.3. Les variacions del nivell físic s'han produït per la fusió de dues tecnologies: l'especificació Ethernet 802.3 i ANSI X3T11 Fiber Channel.

La influència d'aquestes dues tecnologies significa que l'estàndard pot extreure benefici de la tecnologia de la interfície a alta velocitat de Fiber Channel, alhora que manté la compatibilitat amb el format de trama Ethernet 802.3 amb les xarxes ja instal·lades i l'ús de modes de transmissió *full duplex* o *half duplex*.

Les especificacions elaborades aprofiten els estàndards ANSI d'FDDI, de la mateixa manera que a Fast Ethernet, i augmenta deu vegades la velocitat i utilitza com a nivells físics els següents:

- Emissors làser amb fibra multimode i monomode
- Parell trenat apantallat
- Parell trenat no apantallat de categoria 5

La dificultat del repte tecnològic de la Gigabit Ethernet sobre UTP-cat.5 va fer que aquesta especificació se separés en un nou grup que finalment es va especificar el març de 1999 com a suplement 802.3ab.

Gigabit Ethernet funciona a 1 Gbps i està orientada a connectar servidors, *bridges* o commutadors; és a dir, a funcionar com a nivell físic de la xarxa troncal d'una xarxa corporativa i, incidentalment, pot servir per a connectar un usuari final amb el seu servidor.

Respecte de Gigabit Ethernet hi ha dos estàndards, el corresponent a IEEE 802.3z i el corresponent a IEEE 802.3ab.

L'estàndard IEEE 802.3z funciona amb dues fibres òptiques i té comportament *full duplex*; per tant, no utilitza CSMA/CD com a mode d'accés al medi físic. Aquesta especificació està orientada a la connexió punt a punt d'elements de xarxa troncal emprant fibra òptica.

L'estàndard IEEE 802.3ab funciona amb quatre parells de coure de categoria cinc, és similar al 100BaseT i sí que utilitza CSMA/CD com a mètode d'accés al medi físic.

2.1.3. Funcionament de Gigabit Ethernet

L'estàndard IEEE 802.3z especifica tres tipus de medis físics:

- 1000BaseLX: làser d'ona llarga sobre fibra monomode i multimode
- 1000BaseSX: làser d'ona curta sobre fibra multimode
- 1000BaseCX: cable de coure apantallat balancejat

L'estàndard IEEE 802.3ab especifica com a medi de transmissió el cable UTP: 1000BaseT.

El nivell d'enllaç de Gigabit Ethernet és semblant a l'estàndard Ethernet i Fast Ethernet explicats anteriorment. Així, les característiques d'Ethernet –com la detecció de col·lisions, el diàmetre de la xarxa i el format de la trama– seran les mateixes per a Gigabit Ethernet. A més, igual que Fast Ethernet, Gigabit Ethernet suporta transmissions *full duplex* i *half duplex*. Però per a poder fer transmissions *half duplex*, s'afegeixen dues noves funcionalitats: extensió de portadora i *packet bursting*.

Transmissió *half-duplex*

Per a les transmissions *half-duplex* s'utilitza CSMA/CD amb l'objectiu d'assegurar que les estacions es poden comunicar per un sol enllaç i que poden fer una correcta detecció de col·lisions. La implementació de CSMA/CD per a Gigabit Ethernet és la mateixa que per a Ethernet o Fast Ethernet i permet la creació d'una xarxa compartida mitjançant concentradors (*hubs*) o connexions punt a punt *half-duplex*.

Transmissió *full duplex*

En una transmissió *full duplex* no es produeixen col·lisions i, conseqüentment, no és necessari utilitzar el protocol d'accés al canal CSMA/CD.

CSMA/CD és un protocol sensible al retard i, per tant, recordem que és necessari definir la mida mínima de trama o bé la màxima distància entre dues estacions que comparteixen el mateix segment. Així, les estacions podran detectar possibles col·lisions. A mesura que la velocitat de la xarxa augmenta, el temps de transmissió mínim de la trama disminueix, com també la màxima distància entre estacions.

L'augment de velocitats des d'Ethernet fins a Gigabit Ethernet ha creat certs problemes en la implementació de CSMA/CD. Quan IEEE va definir l'especificació 802.3u (100BaseT) va mantenir el mateix format de trama que a Ethernet, i també la mínima llargària de trama. Evidentment, si la velocitat és deu vegades més gran que Ethernet, la trama és deu vegades més curta (des del punt de vista temporal). Com que la velocitat de propagació en el cable és constant, la distància de col·lisió ha de ser deu vegades inferior, això és, dos-cents metres.

En la mesura que la 100BaseT confia en els *bridges* o commutadors en lloc de confiar en els concentradors o repetidors, amb aquesta distància n'hi ha de sobres, però quan IEEE es planteja augmentar deu vegades més la velocitat de transmissió amb Gigabit Ethernet, apareix un greu problema: la distància de col·lisió es redueix a vint metres, cosa que és del tot impensable, ja que el parc instal·lat de parell trenat està limitat a cent metres.

Per a resoldre el problema de la distància de col·lisió, IEEE subministra dues solucions:

- Extensió de portadora
- *Packet bursting*

Gigabit Ethernet

Si volem treure un bon rendiment a una xarxa Gigabit Ethernet mai no hauríem d'utilitzar el mode de transmissió *half duplex,* ja que presenta una ineficiència molt gran.

La tècnica d'**extensió de portadora** consisteix a afegir bits a la trama Ethernet mínima fins a arribar a 512 bytes, i així s'obté una trama de durada similar a una trama de 64bytes a 100 Mbps. Atès que l'extensió de portadora es fa des del punt de vista físic, no cal canviar cap mena de programari que hi hagi escrit fins al moment. Naturalment, l'extensió de portadora redueix el rendiment de la Gigabit Ethernet a nivells alarmants, ja que una trama de 64 bytes s'envia a un ritme de 120 Mbps, la qual cosa només augmenta en un 12% el rendiment respecte a la 100BaseT. És clar que les estacions no solament envien trames mínimes i que la longitud de trama depèn de les capes de programari que hi hagi en el servidor, però el valor esperat de longitud de trama en la majoria de les xarxes locals se situa, actualment, entre els 200 i els 500 bytes.

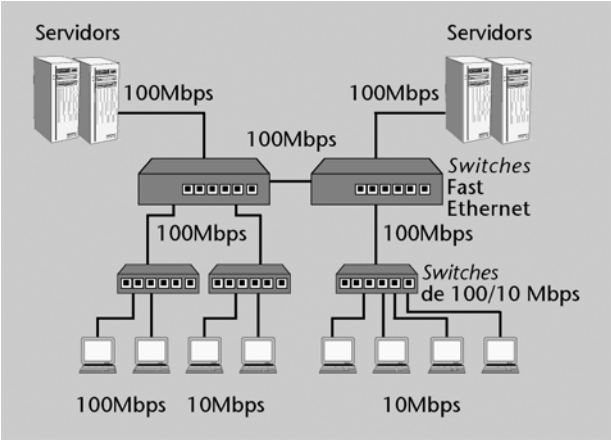
La tècnica de ***paquet bursting*** consisteix a encabir diverses trames Ethernet clàssiques en una supertrama major o igual que 512 bytes. Així, les altres estacions veuran la línia com a ocupada i no transmetran fins que l'estació origen no hagi transmès tota la supertrama.

2.1.4. Exemples d'aplicació de Gigabit Ethernet

A continuació veurem alguns escenaris en què seria útil l'aplicació de la tecnologia Gigabit Ethernet.

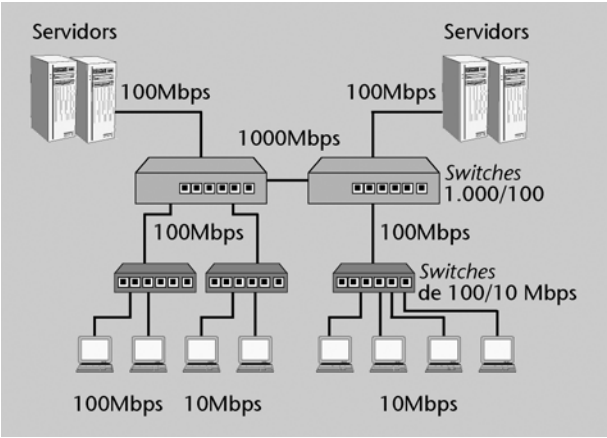
Escenari inicial per a una migració a Gigabit Ethernet

Esquema d'una corporació basada en una xarxa troncal format per dos commutadors de 100 Mbps connectats entre ells que deriven cap a repetidors de 100 Mbps i commutadors de 100 a 10. Òbviament, tenim un desequilibri que es posarà de manifest a mesura que augmenti el trànsit creuat entre les dues branques de la xarxa troncal.



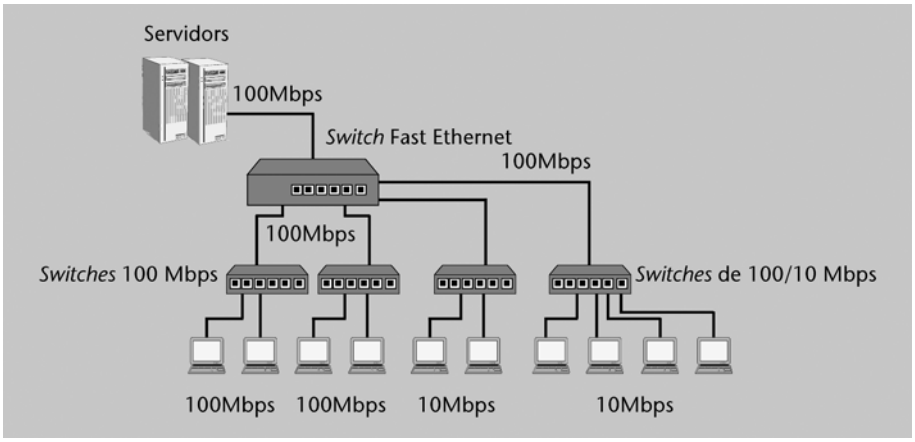
Migració a Gigabit Ethernet

Una primera migració que es pot fer és canviar els dos commutadors 100/100 per un parell de commutadors 100/1.000:

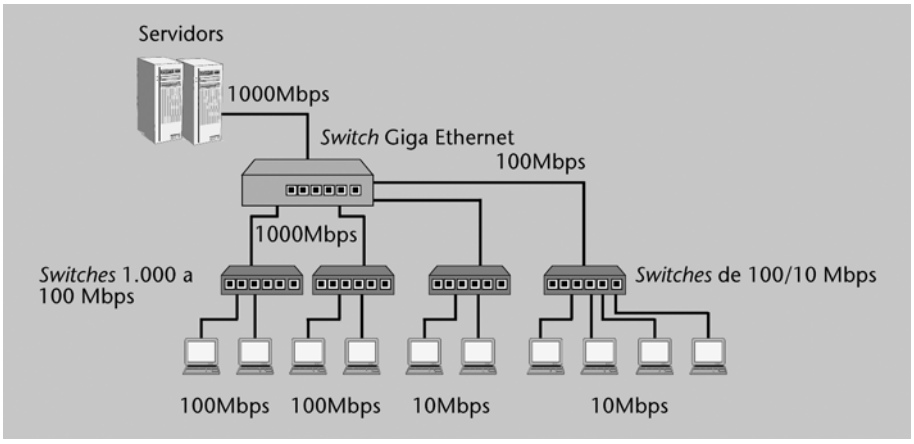


Segon escenari de migració a Gigabit Ethernet

Un altre exemple podria ser el d'una corporació amb una única xarxa troncal de 100 Mbps, però amb una bateria de servidors molt utilitzats per la xarxa i, a més, amb una necessitat d'amplada de banda notable que prové de les estacions de treball de 100 Mbps.



El trànsit entre les estacions de 100 MB i els servidors no està equilibrat. Una possible solució seria migrar la xarxa troncal a Gigabit Ethernet i connectar els servidors i les estacions que necessiten més amplada de banda a 1.000 Mbps.



Solució al segon escenari de migració a Gigabit Ethernet

2.2. Cablejat estructurat: EIA/TIA 568

Des del final dels vuitanta va sorgir una pressió per part dels fabricants per normalitzar les comunicacions dins dels edificis i independitzar-les dels serveis, ja fossin de dades, de telefonia, etc. El 1991 es va publicar l'EIA/TIA 568* referent al cablejat de telecomunicacions per a edificis comercials. Aqust estàndard tenia els objectius següents:

*** La versió actual és l'EIA/TIA 568B.**

- Ser universal, tant en serveis suportats com en fabricants compatibles.
- Ser la base per al desenvolupament d'altres estàndards de comunicacions (veu, imatge, LAN, WAN, etc.). Bàsicament per comunicacions en oficines.
- Definir paràmetres que permetin definir i establir el cablejat de l'edifici abans fins i tot que l'empresa s'hi estableixi. Es concep el cablejat com un servei més de l'edifici (llum, aigua... i dades).

L'abast de l'estàndard cobreix l'especificació del senyal i la mecànica (tant pel que fa a l'ús de parells trenats com de fibra òptica):

- Definició de **senyal**: prestacions, amplada de banda, soroll i interferències límit.
- Definició **mecànica**: els connectors, disposició de contactes, armaris, geometria del cablejat, abast, etc.

Tot i que l'estàndard defineix tant l'ús de fibres òptiques multimode com monomode, actualment, l'alternativa més utilitzada és el parell trenat. Tard o d'hora, la fibra substituirà el coure com a suport de les comunicacions a causa de la seva major capacitat teòrica, però per ara les successives millores en la fabricació del cablejat, i sobretot, la millora dels equips terminals de circuit de dades han fet que la vida prevista del parell trenat s'allargui.

2.2.1. Topologia

La topologia bàsica d'aquest estàndard és l'estrella, que es fa servir en el **cablejat de planta**. El cablejat de planta distribueix des d'un punt central o **armari de planta** (també anomenat IDF, *intermediate distribution frame*) a tots els punts de la superfície o **connectors**. L'estàndard defineix l'ús previst de connectors.

Com que la definició del cablejat és prèvia a la instal·lació de les oficines, la localització dels connectors no es pot basar en la distribució final, ja que no es coneix.

Hi ha diversos mecanismes de distribució, però el més utilitzat és el de superfície, que estableix la instal·lació d'un connector doble cada 10 m^2 d'espai de treball. Aquest és l'espai que es considera que ocupa un lloc de treball i se li preveu l'ús d'un terminal informàtic i un telèfon.

Els diferents armaris de planta (usualment un per planta si les dimensions ho permeten) estan connectats a la **sala d'equipaments** (o MDF, *main distribution frame*). Aquesta sala concentra els baixants dels armaris de planta, amb el cablejat extern (telefonia, WAN, etc). El cablejat entre armaris de planta i la sala d'equipaments pot fer fins a 90 m si és de coure i fins a 3 km si és de fibra.

Tant l'armari de planta com la sala d'equipaments contenen *racks*. Dins dels *racks* hi ha dues parts, que corresponen a dues funcions. Les **entrades de planta** (*patch panels*) identifiquen els connectors distribuïts per la planta. Mitjançant **cables o ponts** (*patch cords*) es connecta al servei desitjat: concentrador, commutador, centraleta telefònica, etc. El cablejat horitzontal pot fer com a molt 90 m (tant si és coure com fibra), que sumats a la longitud dels ponts de l'armari i els ponts per a connectar els terminals fan un total de 100 m com a màxim.

Els *racks* dels armaris de planta tenen connexió amb la sala d'equipaments. Per això normalment es parla de topologia en **estrella jeràrquica**. La principal té el punt central a la sala d'equipaments i cada punta, els armaris de planta, són els nusos de les estrelles subordinades.

2.2.2. Medi físic

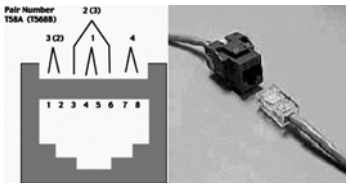
Com a medi físic, hi ha diferents tipus de parell trenat i de fibra òptica:

	Amplada de banda	Serveis possibles
UTP Categoria 1	Sense definir	Telefonia
UTP Categoria 3	16 MHz	LAN de baixa velocitat: Ethernet 10BaseT
UTP Categoria 4	20 MHz	LAN de baixa velocitat: Token Ring 16 Mbps
UTP Categoria 5e	100 MHz	LAN d'alta velocitat: Fast Ethernet, Gigabit Ethernet, Fiber Channel, CDDI, etc.
UTP Categoria 6	250 MHz	Sense serveis exclusius a hores d'ara, però permet els serveis anteriors i serveis de major amplada de banda
F.O. multimode de salt d'índex	100 MHz	LAN d'alta velocitat: Fast Ethernet, FDDI, etc.
F.O. multimode de gradient d'índex	>1 GHz	LAN d'alta velocitat: Gigabit Ethernet, Fiber Channel
F.O. monomode	>1 GHz	Transmissió a llarga distància.

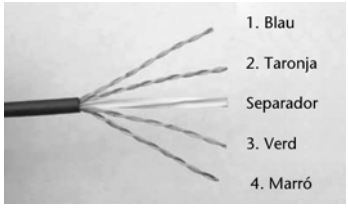
Els medis conductors estan dividits en categories que es diferencien bàsicament pels sistemes de connexió (connectors, panells), el cablejat (densitat del trenat dels parells) i els mecanismes de certificació. En l'actualitat, el cablejat més utilitzat és el de categoria 5e.

De fet, la categoria 5e és una variació en els paràmetres de certificació de l'antiga categoria 5 per garantir el correcte funcionament de les LAN Gigabit Ethernet i Fiber Channel (llavors en procés de definició). Teòricament, un cablejat categoria 5 és capaç de suportar trànsit Gigabit Ethernet (per amplada de banda, interferències, etc.), però es recomana afegir els tests addicionals categoria 5e.

Cadascun dels terminals rep quatre parells trenats que permeten suportar tot tipus de serveis. El servei el reben per mitjà d'un connector RJ45:



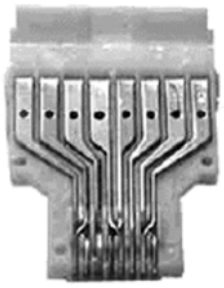
Cada connector rep un cable amb quatre parells de fils amb colors distintius:



Cable categoría 5 al descobert.

És molt delicat treballar amb cablejats categoria 5e i superior, ja que la geometria de la trena està especialment estudiada per a evitar les interferències entre els quatre parells i la resta de cables que hi pugui haver a les rodalies. Un error en el "grimpat" del connector que desfés només una volta de trena podria convertir una instal·lació categoria 5 o 5e en categoria 3.

El trenat s'ha de continuar, fins i tot, en els connectors:



2.2.3. Certificació

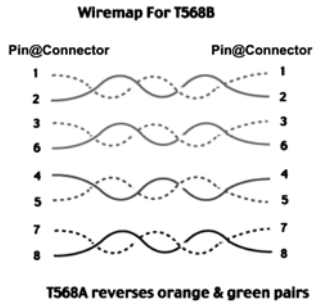
El procés de certificació homologa una instal·lació (sencera) com d'una categoria o d'una altra. Usualment, es fan servir equips que realitzen totes les ope-

racions que tot seguit comentarem, de manera automàtica. Els mesuraments bàsics que fan els equips de tests són els següents:

El test

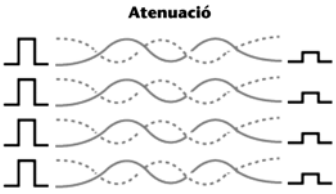
Cadascun dels valors que mencionem té una cota definida, que el test verifica que es compleixi. Per passar el test cal que totes les mesures siguin positives: una instal·lació passa o no passa el test, no hi ha termes internitjos.

Continuïtat. Es mesura que la connexió pin a pin sigui correcta.



Connectors terminals i d'armari.
La connexió als ponts és just a la inversa

Longitud. Es llancen polsos de senyal i es cronometra el senyal de l'eco. D'aquesta manera es comprova que el cablejat no supera la longitud màxima permesa. Amb aquest mesurament també es poden identificar problemes d'homogeneïtat de la línia segons els ecos addicionals que es puguin detectar.

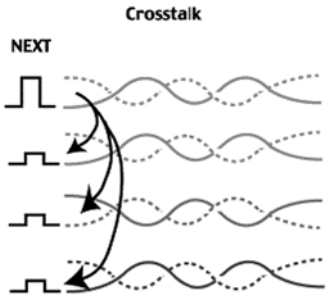


Atenuació. S'envia un senyal patró des d'un emissor i es mesura l'atenuació amb un receptor a tots quatre parells a l'altre extrem del cable. El senyal de mesura ha de tenir una freqüència que ocupi sobretot la banda alta de freqüències, ja que les freqüències altes són les que més atenuació pateixen.

NEXT o **autointerferència**. El NEXT* es mesura aplicant un senyal a potència nominal i freqüència màxima en un parell i mesurant el senyal que passa per radiació als altres tres parells en el mateix extrem. Aquesta mesura es repeteix per a tots quatre parells.

*** NEXT és la sigla de *Near End Cross(X)-Talk*.**

Un valor més gràfic que el NEXT és l'ACR (*Attenuation to Crosstalk Ratio*), que mesura la diferència entre el NEXT i l'atenuació. Com més gran sigui l'ACR, millor.



Altres tests

Amb l'aparició de serveis sobre cablejat estructurat, com la Gigabit Ethernet, que fan servir els quatre parells en les dues direccions simultàniament, s'han anat afegint altres mesures, com per exemple el càlcul del retard diferencial als quatre parells, els ecos, etc.

2.3. Xarxes sense fil: norma IEEE802.11

L'IEEE802.11 especifica un MAC CSMA/CA per a xarxes sense fil. L'estàndard especifica diverses bandes possibles, i fins i tot LAN per infrarojos, però les més utilitzades són les bandes ISM* de 2,4 GHz i 5 GHz.

*** ISM és la sigla de *Industrial, Scientific and Medical.***

Banda ISM

La banda ISM defineix les bandes d'accés lliure regulat de 0,9 GHz, 2,4 GHz i 5,7 GHz:

ISM	$f_{mín}$	$f_{màx}$
Banda 0,9 GHz	902 MHz	928 MHz
Banda 2,4 GHz	2,4000 GHz	2,4835 GHz
Banda 5 GHz	5,150 GHz	5,825 GHz

La banda de 5 GHz està dividida en dues subbandes, separades per un buit d'entre 5,35 GHz i 5,725 GHz.

L'IEEE802.11 defineix dos modes de funcionament, l'un basat en un punt central anomenat punt d'accés (mode infraestructura) i l'altre sense aquest punt (mode *ad-hoc*).

En el primer mode de funcionament, a part del control d'accés CSMA/CA, es pot reservar, sota petició al punt d'accés, una fracció del temps per a trànsit síncron (per veu o imatge en temps real). Nosaltres ens centrarem exclusivament en el trànsit de dades, per tant, controlat per CSMA/CA.

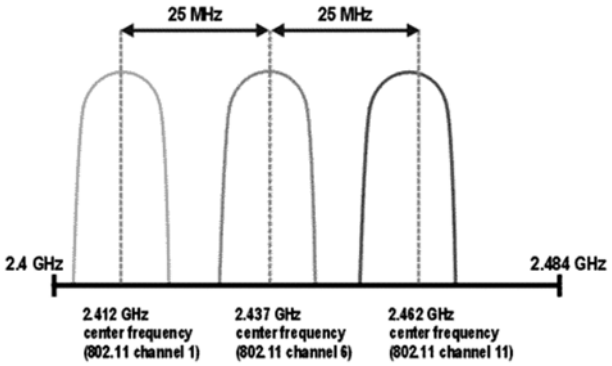
2.3.1. Nivell físic

L'IEEE802.11 defineix diversos nivells físics d'entre 1 Mbps i 54 Mbps. Però els més utilitzats en l'actualitat són els següents:

- **IEEE802.11b.** (11 Mbps). Fa servir la banda de 2,4 GHz de la ISM. És el més emprat actualment. Disposa de catorze canals amb una amplada de banda de 22 MHz cadascun. En cas que l'SNR empitjori, automàticament la velocitat baixa a 5,5 Mbps, 2 Mbps i 1Mbps.

  Els catorze canals es reparteixen els 83,5 MHz disponibles. Per tant, és obvi que no es poden utilitzar simultàniament, ja que s'interferirien. Com a mà-

xim es poden fer servir tres canals dins d'una àrea determinada (per exemple l'1, el 6 i l'11).



El nombre de canals disponibles varia en cada país, ja que la banda regulada pot variar.

Com es pot veure a la taula següent, les legislacions espanyola i francesa són particularment restrictives, tot i que s'espera que això canviï tal com ja ha passat al Japó:

Identificació de canal	Freqüència (MHz)	Dominis reguladors						
		X'10' FCC	X'20' IC	X'30' ETSI	X'31' Espanya	X'32' França	X'40' Japó	X'41' Japó
1	2412	X	X	X	—	—	—	X
2	2417	X	X	X	—	—	—	X
3	2422	X	X	X	—	—	—	X
4	2427	X	X	X	—	—	—	X
5	2432	X	X	X	—	—	—	X
6	2437	X	X	X	—	—	—	X
7	2442	X	X	X	—	—	—	X
8	2447	X	X	X	—	—	—	X
9	2452	X	X	X	—	—	—	X
10	2457	X	X	X	X	X	—	X
11	2462	X	X	X	X	X	—	X
12	2467	—	—	X	—	X	—	X
13	2472	—	—	X	—	X	—	X
14	2484	—	—	—	—	—	X	—

Font: IEEE802.11b

Els països marcats com ETSI són els europeus, excepte França i Espanya. FCC són els EUA, i IC, el Canadà.

- **IEEE802.11a** (54 Mbps). Fa servir la banda de 5 GHz de la ISM. Té un abast una mica inferior a l'IEEE802.11b i ha estat superat per l'IEEE802.11g. En cas que l'SNR empitjori, la velocitat de transmissió s'ajusta a 24 Mbps, 12

Mbps i 6 Mbps (encara que algunes altres velocitats intermèdies es poden implementar opcionalment).

- **IEEE802.11g** (54 Mbps). És equivalent a l'IEEE802.11a, però fa servir la banda de 2,4 GHz de la ISM, que és menys vulnerable als obstacles (major abast) i és interoperable amb targetes IEEE802.11b.

2.3.2. Control d'accés al medi

En aquest estàndard no es pot fer servir el CSMA/CD com a control d'accés al medi perquè requereix que l'electrònica de transmissió sigui capaç de transmetre i rebre alhora. Per a aconseguir que en radiotransmissió es pogués transmetre i rebre alhora caldria utilitzar bandes de freqüència diferents per a transmetre i per a rebre. Això exigeix dividir l'amplada de banda en subbandes més petites, cosa que ens faria perdre prestacions*.

*** En aquest cas, parlaríem d'FDMA.**

CSMA/CD no és aplicable per a controlar l'accés al medi en aquest estàndard perquè la detecció de col·lisions (CD) exigeix tenir un transmissor-receptor *full-duplex*.

Cal no confondre el fet que l'electrònica de transmissió del CSMA/CD sigui *full duplex*, amb que el MAC CSMA/CD sigui *full duplex*. El CSMA/CD i tota la resta de protocols MAC són *half duplex* per definició. Això ve del fet que el que un terminal transmet ho reben els n–1 restants. Si transmetessin dos, els n–2 rebrien la suma dels dos senyals sense tenir oportunitat d'entendre res.

Els enginyers van haver d'escollir un control d'accés al medi alternatiu al CSMA/CD.

MAC dinàmic estava fora de discussió, ja que una de les premisses del disseny era el suport de sistemes mòbils en moviment (*roaming*): anar-se movent per l'espai saltant d'una LAN a una altra implicaria una reconstrucció de l'anell (lògic forçosament) que va ser descartada des d'un bon principi.

Entre els sistemes aleatoris, el CSMA és el millor dels que no requereixen transmissors-receptors *full-duplex*. El problema és que es degrada ràpidament quan es treballa en xarxes on la cobertura de senyal no és completa.

Tal com hem vist a l'apartat anterior, el més adequat és un CSMA/CA.

De totes maneres, l'IEEE802.3 permet treballar amb CSMA en els casos on la durada de la col·lisió es consideri un factor secundari (xarxes amb pocs terminals i/o poc trànsit). Amb això la velocitat efectiva (si el medi està lliure) augmenta degut a l'estalvi de trames RTS i CTS que es produeix.

2.3.3. Topologia

Ja hem vist que l'única topologia possible per a xarxes sense fil és el bus. Cada domini de col·lisió s'anomena BSS o *Basic Service Set*. Dins una mateix volum només hi pot haver un BSS per a cada canal.

Amb tot, WiFi aporta dos modes de funcionament alternatius, cadascun amb els seus avantatges:

- **Mode *ad-hoc***. És el més pur dels dos, ja que el bus (l'aire) és compartit sense intermediaris. Les estacions seleccionen la banda de freqüències que volen fer servir i poca cosa més. Cada banda de freqüències, el canal, és un domini de col·lisió independent.

- **Mode amb infraestructura**. El BSS està comandat per un punt d'accés (*Access Point* o AP). Totes les transmissions són entre l'AP i els terminals, mai entre terminals. És aproximadament equivalent* a una topologia en estrella, on l'AP és el repetidor o concentrador: totes les transmissions d'estació a estació han de passar forçosament a través de l'AP.

Recordeu

Els estàndards IEEE802.11b i IEE802.11g defineixen catorze canals.

*** Algú podria discutir –i amb raó– que és una falsa estrella, ja que les estacions es connecten al concentrador a través de la mateixa línia. En un concentrador Ethernet, el domini de col·lisió és únic, però les línies són individuals per terminal.**

El mode *ad-hoc* té l'avantatge que no necessita maquinari addicional a les targetes de les estacions: dos terminals amb les corresponents targetes ja es poden posar a treballar.

El mode amb infraestructura té l'avantatge que els terminals poden connectar-se encara que no tinguin connexió ("visió") directa. Això, que a primer cop d'ull sembla una trivialitat, no ho és tant ja que els terminals normalment estan sobre taules i es mouen; en canvi, els AP se solen posar aixecats del terra en posicions fixes i estudiades. És molt més fàcil garantir connexió de tots contra l'AP, que de tots contra tots.

En definitiva, el mode *ad-hoc* és més útil per a xarxes casuals (per exemple, una reunió) que per a treball diari.

3. Noves prestacions de les xarxes Ethernet

3.1. Ethernet *full-duplex*

Les xarxes Ethernet es van dissenyar com una tecnologia *half-duplex*, és a dir, que la transmissió de dades entre una estació origen i una estació destinació només es pot produir en un únic sentit a la vegada. Així doncs, qualsevol estació Ethernet abans de transmetre informació comprova que el medi no estigui ocupat. Si està lliure, l'estació comença a transmetre i l'ocupa. Però tal com hem vist, això pot provocar col·lisions si dues estacions o més comencen a transmetre simultàniament i, per tant, calen mecanismes per a evitar aquesta situació, o si més no, per a recuperar-se si es produeix.

Estàndard

Ethernet *full-duplex* ha estat estandarditzada a l'IEEE802.3x.

Afegir les tècniques de commutació a les LAN amb l'ús dels commutadors ha permès incorporar la possibilitat de transmissions *full-duplex* a Ethernet, i així augmentar el rendiment de la xarxa. El perquè els commutadors permeten transmissions *full-duplex* és clar: els enllaços entre el commutador i les estacions són independents entre ells. Dit d'una altra manera, cada estació té el seu propi domini de col·lisió. Per tant, el commutador pot intercanviar trames amb totes les estacions simultàniament, i en *full-duplex*.

Òbviament no es poden construir concentradors *full-duplex*, ja que en cada domini de collisió només hi pot haver una transmissió activa en cada instant. De fet, el concepte *domini de collisió* és de poca o nul·la aplicació en ports *full-duplex*.

De fet, això ja no és una xarxa local CSMA/CD. El que tenim són enllaços punt a punt entre les estacions i el commutador que anecdòticament fan servir com a format de trama l'Ethernet i com a codificació 10baseT, 100baseT, etc.

Ethernet en mode full-duplex permet la transmissió i la recepció de dades entre dues estacions de manera simultània.

Perquè una xarxa Ethernet pugui treballar en mode *full-duplex* s'han de complir diverses condicions:

- El medi físic ha de permetre la transmissió *full-duplex*.
- Només hi poden haver dos dispositius connectats entre ells.
- Les targetes de xarxa de tots dos equips han de suportar la transmissió *full-duplex*.

No tots els medis físics poden suportar transmissions *full-duplex*. Per exemple, 10Base5, 10Base2 o 100Base-T4 no les permeten. En canvi, 10BaseT, 100BaseT o 100BaseFl sí que les permeten.

Fins ara, la substitució d'un concentrador per un commutador no exigia cap més canvi. Però amb Ethernet *full-duplex* cal canviar les targetes de les estacions, ja que les normals aplicarien el CSMA/CD de manera contumaç, avortant qualsevol transmissió simultània en les dues direccions.

Una altra característica important d'una xarxa Ethernet *full-duplex* és la supressió de la restricció sobre la distància màxima. Recordem que aquesta restricció la imposava el protocol d'accés al medi per tal de poder detectar les possibles col·lisions. Tanmateix, si en el mode *full-duplex* tenim un domini lliure de col·lisions, podem veure que aquesta restricció ja no és necessària. Ara serà l'atenuació del senyal que provoqui el medi físic emprat qui imposarà la limitació de distància.

Així doncs, l'ús d'Ethernet *full-duplex* augmenta el rendiment de la xarxa, permet distàncies més grans i en simplifica el funcionament, perquè ja no s'utilitza el protocol de control d'accés al medi. A més, la transmissió *full-duplex* en les xarxes Gigabit Ethernet permet de suprimir les tècniques d'extensió de portadora i de ràfegues de trames, ja que en aquest entorn no són necessàries.

3.2. Control de flux

Inicialment, diferents fabricants van implementar el mode de transmissió *full-duplex* com una extensió no estàndard. Tanmateix, el 1997 es va estandarditzar mitjançant el subcomitè 802.3x i s'hi va incloure la funció de control de flux.

El control de flux s'utilitza entre estacions que es transmeten dades en mode *full-duplex*. Quan l'estació receptora detecta que no pot acceptar més trames entrants, envia una comanda anomenada *pause*. Aquesta comanda indica a l'emissor que pari d'enviar informació durant el període de temps que s'especifica en la mateixa trama. Durant aquest temps, el receptor pot enviar noves comandes *pause* que allarguin, redueixin o eliminin la pausa que ha anunciat prèviament.

> El control de flux és una tècnica que vol evitar el desbordament de les memòries intermèdies (*buffers*) d'emmagatzematge del receptor, juntament amb la conseqüent eliminació de trames que aquest fet comportaria.

3.3. Sistemes multiestàndard: autonegociació

Els sistemes Ethernet moltes vegades suporten els diferents estàndards vistos en anteriors apartats. Poden treballar amb diferents medis físics (100BaseTx, 100BaseT4, 10BaseT...), amb diferents velocitats de transmissió i amb *half-duplex* o *full-duplex*. A més, els commutadors permeten que diferents ports treballin de manera diferent.

La tècnica d'autonegociació permet a dos dispositius intercanviar informació sobre les seves capacitats per tal de crear un entorn de comunicacions eficient.

Així, cada vegada que un dels ports d'un commutador es reinicia, engega un procediment d'autonegociació que consisteix a acordar amb l'oponent l'estàndard de més prestacions que tinguin en comú.

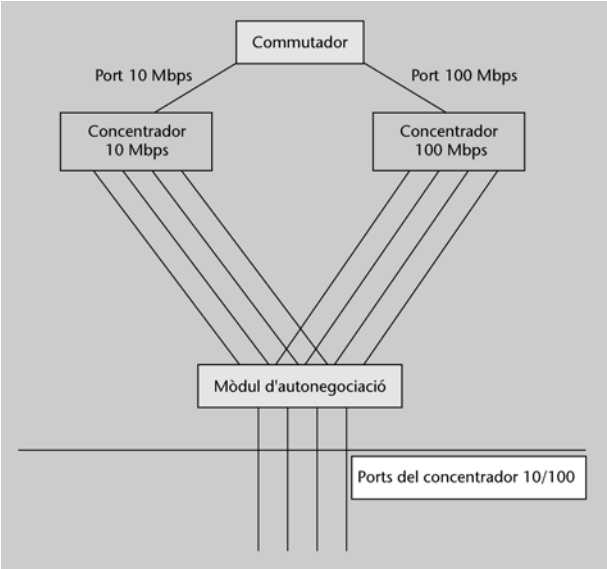
Estàndard

Aquest procediment ha estat estandarditzat en la mateixa revisió que la Fast Ethernet: IEEE802.3u.

En el cas de dispositius amb RJ-45, en primer lloc es negocia el medi físic i la velocitat de transmissió, que comença per Gigabit Ethernet i acaba amb l'Ethernet clàssic. A continuació es negocia el mode de transmissió *half-duplex* o *full-duplex* i, finalment, el control de flux i l'establiment simètric o asimètric d'aquest. Amb la fibra òptica el medi físic no és negociable i, per tant, només s'intercanvien informació sobre el mode de funcionament i el control de flux.

En canvi, un concentrador no pot actuar de la mateixa manera: no pot tenir ports *full-duplex* i tampoc ports de diferents velocitats. Un concentrador és simplement un repetidor del senyal que rep; per tant, no és possible que un senyal rebut a una velocitat es retransmeti a una velocitat diferent.

Cal tenir present que parlem de concentradors reals. El mercat és ple de concentradors multivelocitat, a 10/100 Mbps i a 10/100/1000 Gbps (*half-duplex* tots ells, això sí) i amb capacitat d'autonegociació. L'entrellat es resol quan n'estudiem l'arquitectura, i és que no es tracta d'un concentrador, sinó de dos (o tres) concentradors interconnectats mitjançant un commutador de dos o tres ports. L'arquitectura per a un concentrador 10/100 és la següent:



Un concentrador 10/100 crea dos dominis de col·lisió (un concentrador 10/100/1000 en crea tres) interconnectats per un commutador. Per tant, la capacitat del concentrador serà 10 Mbps + 100 Mbps = 110 Mbps (1,11 Gbps en un concentrador 10/100/1000).

4. Xarxes d'àrea local virtuals: VLAN

La configuració d'una xarxa d'àrea local típica depèn, en gran manera, de la infraestructura física de les seves connexions. Així, doncs, l'agrupació d'usuaris es fa segons la seva situació física, la seva connexió a un determinat concentrador o commutador i el seu cablatge corresponent. Si el dispositiu que interconnecta els diferents concentradors és un encaminador (*router*), aquest proporcionarà segmentació i evitarà que el trànsit de difusió (*broadcast*) passi d'una xarxa a una altra. En canvi, si el dispositiu que interconnecta els diferents concentradors és un commutador, aquest no podrà evitar que el trànsit de difusió passi d'un segment a un altre. A més, aquest tipus de segmentació no permet d'agrupar els usuaris segons el tipus de tasca que fan, el departament al qual pertanyen o l'amplada de banda que necessiten.

Una LAN virtual, o VLAN, és una agrupació lògica de dispositius o d'usuaris. Aquesta agrupació no està restringida pel segment físic on estan connectats, sinó que els dispositius o usuaris es poden agrupar per la funció que duguin a terme, el departament del qual formen part o l'aplicació que utilitzen, per exemple.

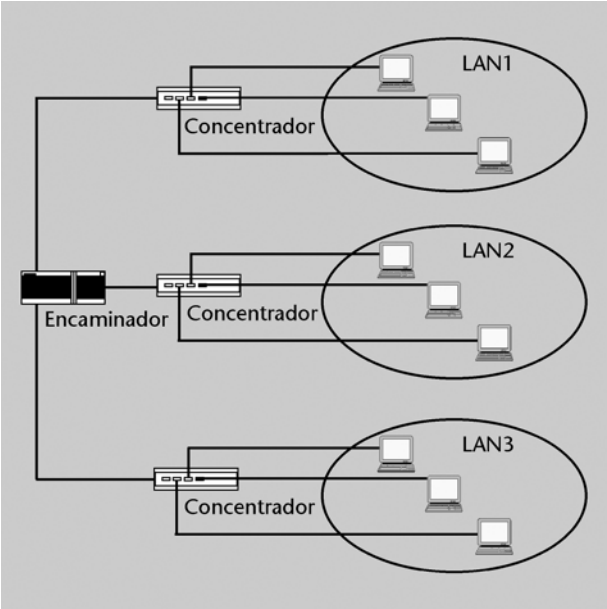
Una VLAN crea un domini de difusió únic que no està restringit a un segment físic. Així, doncs, el trànsit de difusió no es propaga entre les LAN virtuals. Per tant, perquè dos usuaris de VLAN diferents es puguin comunicar entre ells, serà necessari que un encaminador interconnecti totes dues VLAN. Dos usuaris que estiguin connectats en el mateix commutador i que pertanyin a VLAN diferents no es podran comunicar entre ells mentre no hi hagi un encaminador entre totes dues VLAN.

És important destacar que la implementació de VLAN es fa mitjançant programari instal·lat en els commutadors. Consegüentment, cada fabricant implementa la seva versió per a la creació i gestió de VLAN.

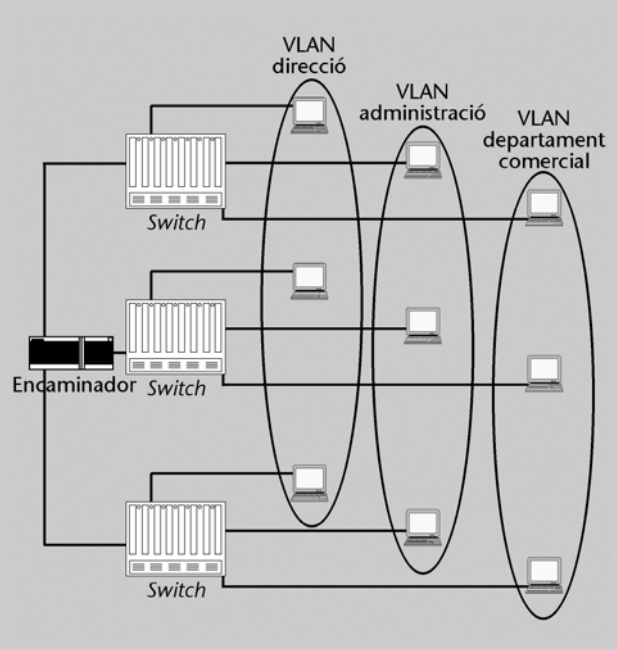
4.1. Característiques de les VLAN

Les VLAN segmenten de manera lògica la infrastructura física de les xarxes d'àrea local. Aquest fet permet d'agrupar usuaris que estan separats geogràficament en una mateixa VLAN. A més, amb aquesta agrupació lògica s'aconsegueix que el trànsit de difusió que genera una estació d'una VLAN es transmeti només als ports que pertanyen a la mateixa VLAN.

Les figures següents mostren la diferència entre la segmentació LAN i VLAN:



Implementació típica d'una LAN



Implementació mitjançant VLAN

En una xarxa que ja utilitza elements de commutació i que, a més, els commutadors suporten la programació de VLAN, la migració cap a un entorn amb LAN virtuals és molt senzill. En aquest cas, només cal decidir quin serà el criteri d'agrupació dels dispositius i configurar els commutadors de manera adient. En cas que la xarxa no sigui commutada i utilitzi concentradors, el primer pas consistirà a substituir-los per commutadors que suportin VLAN. Però si tots els dispositius connectats a un determinat concentrador han de pertànyer a la mateixa VLAN, només caldrà connectar un dels ports del concentrador a un commutador.

Les característiques més importants de les VLAN són les següents:

- Les VLAN treballen en els nivells 2 i 3 del model de referència OSI.
- El trànsit de difusió només es propaga entre els ports d'una mateixa VLAN, però no es transmet entre VLAN.
- La comunicació entre VLAN necessita un dispositiu d'encaminament de nivell de xarxa.
- Les VLAN es configuren mitjançant programari i és l'administrador de xarxa qui assigna els diferents usuaris a cada VLAN.
- La configuració de les VLAN depèn de cada commutador: cada fabricant disposa d'una implementació propietària de gestió de VLAN en els seus commutadors.
- La definició de VLAN millora la seguretat d'una xarxa, perquè permet de definir quines comunicacions entre VLAN estan permeses i quines no.
- L'agrupació de dispositius es pot fer per departament o pel tipus d'aplicacions que utilitzen els usuaris, per exemple.

En una arquitectura VLAN és important poder transportar informació entre els diferents commutadors i encaminadors que formen part de tota la xarxa. Recordem que usuaris d'una mateixa VLAN poden estar connectats en diferents commutadors i, conseqüentment, aquests han de ser capaços de poder intercanviar-se informació. Així, doncs, la troncal de la xarxa estarà formada per enllaços entre aquests commutadors i els encaminadors. A més, haurà de suportar grans volums d'informació entre els dispositius, i també informació de les VLAN i dels dispositius que les formen.

Xarxa troncal

Com que la troncal d'una xarxa ha de suportar grans volums d'informació, haurà de ser, com a mínim, Fast Ethernet.

L'encaminador és el dispositiu encarregat de dur a terme la interconnexió entre les diferents VLAN.

L'encaminador, dispositiu de nivell de xarxa, proporciona la comunicació entre els grups de treball definits lògicament, les diferents VLAN. A més, proporciona accés als recursos compartits com, per exemple, els servidors. També permet la connexió amb altres zones de la xarxa que no segueixin l'arquitectura de VLAN.

El commutador és el dispositiu fonamental de l'arquitectura VLAN. Aquest dispositiu ha de ser capaç de filtrar les trames segons els criteris escollits per l'administrador de xarxa a l'hora de crear les VLAN.

4.2. Tipus de VLAN

Mitjançant VLAN podem disposar d'una xarxa commutada que està segmentada lògicament segons les aplicacions, els protocols i les funcions dels usuaris,

sense que importi on estan situats físicament aquests usuaris. Així, doncs, podríem definir que cada port d'un commutador forma part d'una VLAN diferent, si és necessari.

Les VLAN es poden classificar segons la forma d'assignació dels ports d'un commutador a una VLAN. Però, una altra manera de classificar les VLAN dependrà del tipus d'informació que utilitzi el commutador per a agrupar els dispositius d'una manera lògica.

A continuació analitzarem les diferents VLAN, que es poden classificar en els tipus següents:

- VLAN estàtiques o dinàmiques
- VLAN basades en el port o en el protocol

4.2.1. VLAN estàtiques i VLAN dinàmiques

En una VLAN estàtica l'administrador de xarxa defineix de manera permanent la relació entre els ports d'un commutador i la VLAN a la qual pertanyen.

En una VLAN estàtica els ports d'un commutador s'assignen estàticament a una VLAN determinada. Així, doncs, la configuració només canviarà si l'administrador de xarxa canvia un port d'una VLAN a una altra. En cas contrari, aquesta configuració es mantindrà fixa.

Aquest tipus de VLAN comporta un control molt gran de l'administrador, però són fàcils de configurar, monitoritzar i gestionar. Això és perquè és l'administrador qui té el control total.

En una VLAN dinàmica els ports d'un commutador determinen de manera automàtica la seva assignació a una VLAN.

L'assignació automàtica del port en les VLAN dinàmiques pot dependre de les adreces de nivell d'enllaç, de les adreces lògiques o bé del tipus de protocol dels paquets.

Procediment d'assignació automàtica del port en les VLAN dinàmiques

Imaginem que el criteri de selecció és l'adreça de nivell d'enllaç. Quan una estació està connectada a un port que no pertany a cap VLAN i transmet una trama, el commutador detecta l'adreça de nivell d'enllaç en la trama, busca a quina VLAN ha de pertànyer en la seva base de dades de VLAN i, automàticament, configura el port amb les característiques de la VLAN corresponent.

Aquest tipus de VLAN requereix menys administració en cas que un usuari canviï de situació geogràfica, ja que no és necessari definir per a cada port la seva assignació de VLAN. Tanmateix, cal disposar d'una base de dades actualitzada amb tots els usuaris i el criteri d'assignació de VLAN escollit.

4.2.2. VLAN basades en el port o en el protocol

En les VLAN basades en el port el commutador utilitza els números de port per a fer l'agrupació lògica d'usuaris.

És a dir, a cada VLAN li correspondrà tot un seguit de ports determinats. En el fons, haurem d'entendre que es tracta d'una VLAN estàtica, com l'estudiada anteriorment.

Quan parlem de VLAN basada en el protocol, el commutador classificarà el trànsit rebut segons el tipus de protocol del paquet de nivell de xarxa.

En el cas de VLAN basades en el protocol la informació discriminant serà el tipus de protocol de nivell 3. Així, doncs, podrem tenir VLAN IP, VLAN IPX, etc.

4.3. IEEE 802.1Q

El commutador és el dispositiu encarregat de filtrar i permetre el pas de les trames segons els criteris de VLAN i, a més, ha de compartir aquesta informació amb altres commutadors i encaminadors de la xarxa.

Si tenim usuaris d'una mateixa VLAN connectats a diferents commutadors serà necessari que aquests es passin informació entre ells i que coneguin a quina VLAN pertanyen les trames que commuten. Es pot donar el cas que un usuari connectat a un commutador enviï trames a un altre usuari de la mateixa VLAN que penja d'un altre commutador. A més, recordem que les trames de difusió arriben a tots els membres d'una VLAN. Per tant, un commutador haurà de reconèixer i associar les trames que rep amb la VLAN corresponent.

La tècnica d'identificació de trames assigna un identificador determinat per a cada trama. Aquesta tècnica introdueix un identificador a la capçalera de la trama de nivell d'enllaç. Aquest identificador es transmet per la xarxa troncal i és examinat pels diferents commutadors i encaminadors que travessa. Quan la trama està a punt de sortir de la xarxa troncal, el commutador elimina aquest identificador, a fi i efecte que no arribi fins a l'estació destinació.

Aquesta solució,...

... tot i que requereix més capacitat de procés, és més escalable per xarxes grans. És per això que l'organització IEEE la va escollir i la va normalitzar com a IEEE 802.1q.

IEEE 802.1q defineix que la tècnica d'identificació de trames és la solució emprada en la implementació de VLAN.

Així, doncs, un commutador pot tenir dos tipus de ports, que es classifiquen segons la seva funcionalitat. Aquests ports s'anomenen:

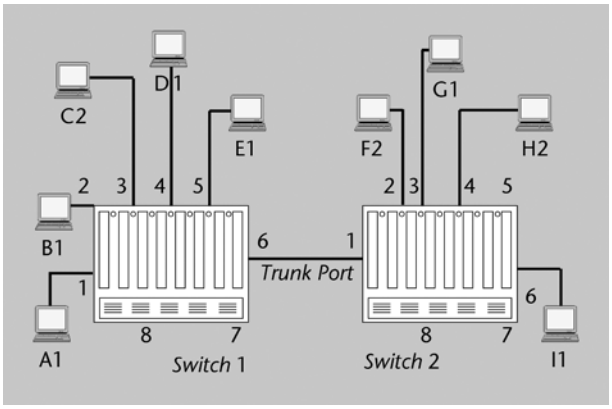
– *Access port*: port que pertany a una determinada VLAN
– *Trunk port*: port que pertany a diferents VLAN.

Qualsevol port, per defecte, sempre és *access port* i, per tant, només pot pertànyer a una única VLAN. En canvi, un *trunk port* permetrà la interconnexió de commutadors i, conseqüentment, haurà de pertànyer a totes les VLAN de les quals transmeti trames. En un *trunk port* la informació viatjarà acompanyada amb l'etiqueta de la VLAN corresponent. En canvi, les trames que surten d'un port d'accés sempre estaran sense marcar (*untagged*) i això significa que no portaran informació especial respecte a quina VLAN en particular pertanyen.

Els *trunk ports* s'utilitzen usualment per a interconnectar diferents commutadors, sense tenir en compte a quina VLAN pertanyen les trames intercanviades. Per exemple, en una situació com la de la figura següent, les trames que surten d'un commutador cap a l'altre commutador han de mantenir la informació respecte a quina VLAN pertanyen perquè puguin arribar a la seva destinació. En canvi, qualsevol trama que surti d'un port d'accés és *untagged*. Això vol dir que no podem utilitzar un port d'accés per a unir tots dos commutadors.

Pels *trunk ports* circulen trames que poden pertànyer a més d'un tipus de VLAN. Si aquests dos commutadors estan interconnectats, el port d'unió entre tots dos commutadors ha de treballar amb trames que poden pertànyer a totes dues VLAN, i és per això que haurà de ser un *trunk port*, ja que si una trama arriba al commutador 1 s'haurà d'enviar al commutador 2, tant si pertany a la VLAN1 com si pertany a la VLAN2. El *trunk port* haurà de ser capaç de distingir a quina VLAN pertany la trama per a dirigir-la allà on calgui.

Ús dels *trunk ports*

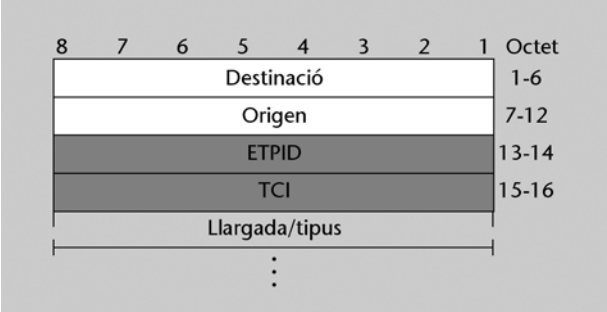


En aquesta xarxa, si inferim que el número de cada estació indica la VLAN a la qual pertany, hauríem de configurar els commutadors de la manera següent:

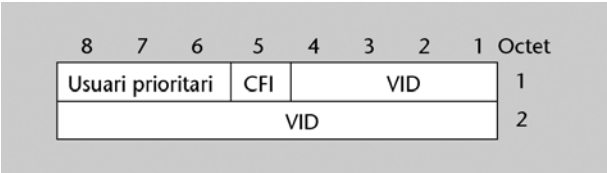
Commutador 1:
Port 6: *trunk port*
Ports 1, 2, 4, 5 i 6: VLAN 1
Ports 3, 6: VLAN 2
Commutador 2:
Port 1: *trunk port*
Ports 1, 3, 6: VLAN 1
Ports 1, 2, 4: VLAN 2

Com hem comentat anteriorment, els *trunk ports* sempre transmeten i reben trames *tagged*, és a dir, trames marcades. L'estàndard IEEE 802.1Q especifica el format d'aquesta marca. L'única excepció són les trames del protocol Spanning Tree que es transmeten *untagged*.

L'estàndard 802.1Q inclou la definició del format de trama d'una VLAN que porta la identificació de la VLAN i la informació de la prioritat de l'usuari. Aquesta informació addicional s'inclou en un nou camp conegut amb el nom de ***tag header*** i que està situat immediatament després dels camps de les adreces MAC destinació i origen existents en la trama original.



Format del camp *Tag header* definit per l'IEEE 802.1q



Format del camp TCI

Els camps que formen la trama d'identificació de VLAN, definida pel IEEE 802.1q, són els següents:

- ETPID (*Ethernet-coded tag protocol identifier*): el seu valor és 81-00.
- TCI (*tag control information*), que es descompon en els camps següents:
  - *User priority*: 3 bits que representen vuit nivells de prioritat.
  - CFI: *canonical format indicator*.
  - VID (VLAN *identifier*): identifica a quina VLAN pertany la trama.

- 0: indica que no hi ha informació VLAN, és a dir, que el *tag header* només conté informació de prioritat.
- 1: *default value*.
- FFF: reservat.
- Els altres valors queden disponibles per a l'ús d'identificadors de VLAN.

5. NAT

El creixement exponencial d'Internet fa que la mancança d'adreces es converteixi en un problema. Un mètode per a solucionar aquest problema és la traducció d'adreces de xarxa, també conegut com a *NAT*. NAT, definit en l'RFC 1631, és el procés d'intercanviar una adreça per una altra en la capçalera del paquet IP.

NAT

NAT és la sigla de *network address translation*.

NAT té com a objectiu solucionar el problema de la manca d'adreces IP públiques disponibles a Internet. Per a fer-ho utilitza adreçament privat en la xarxa local i únicament publica (tradueix) a l'exterior les adreces que realment siguin necessàries.

Aquest procés s'aplica en l'encaminador que separa la xarxa interna (privada) de la xarxa externa (pública).

Així, doncs, la tecnologia NAT permet que les xarxes privades que utilitzen adreces IP no registrades es puguin connectar a xarxes públiques com, per exemple, Internet. Quan una estació de la xarxa privada enviï un paquet cap a la xarxa pública, l'encaminador de sortida traduirà l'adreça privada d'aquesta estació en una adreça pública, és a dir, una adreça legal en la xarxa externa. Sense aquesta traducció, l'estació de la xarxa privada mai no arribaria a transmetre informació cap a la xarxa externa.

Adreces privades

Les adreces IP privades són adreces d'ús intern i no seran encaminades dins d'Internet.

Hi ha un conjunt d'adreces reservades que es poden utilitzar en qualsevol xarxa interna. Les adreces IP privades definides en l'RFC 1918 són les següents:

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255

Hi ha diferents formes d'operació de NAT, segons el tractament que fa sobre les adreces. Els tipus de traducció d'adreces que estudiarem a continuació són les següents:

PAT

PAT és la sigla de *port address translation* ('traducció d'adreces de port').

- NAT estàtic
- NAT dinàmic
- NAT amb sobrecàrrega del TCP (també conegut com a *PAT*)
- LSNAT: NAT amb balanceig de càrrega

LSNAT

LSNAT és la sigla de *load sharing NAT*.

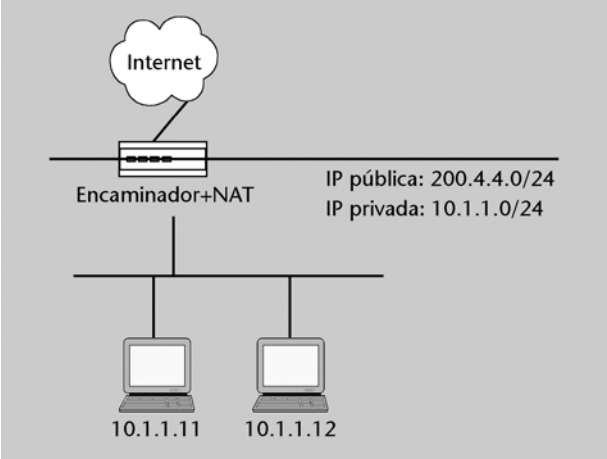
5.1. NAT estàtic

La traducció estàtica d'adreces és el cas més senzill de NAT. En aquest cas, s'aplica una traducció d'adreces una a una i, conseqüentment, caldrà definir cadascuna de les traduccions que es vulguin fer. Aquest fet implicarà una gran dificultat de gestió si el nombre de traduccions és elevat.

Quan s'utilitza NAT estàtic, cada adreça privada té la seva adreça pública equivalent. Per això, serà necessari que l'administrador faci aquesta relació d'equivalència, una a una.

Exemple d'implementació de NAT estàtic

La imatge següent presenta un escenari amb una xarxa interna, la xarxa externa o Internet, i l'encaminador que interconnecta aquestes dues xarxes.



Per a configurar el NAT en l'encaminador de connexió a Internet caldrà definir la taula següent:

Tipus de NAT	Adreça privada	Adreça pública
Estàtic	10.1.1.11	200.4.4.11
Estàtic	10.1.1.12	200.4.4.12

Com podem observar, cal una adreça pública per a cada estació que tingui una adreça privada. Evidentment, aquest tipus de NAT no comporta cap estalvi d'adreces IP, però és necessari per a tots els servidors que hagin de ser accessibles des d'Internet. Per a aconseguir un estalvi real respecte de les adreces IP públiques caldrà utilitzar NAT dinàmic.

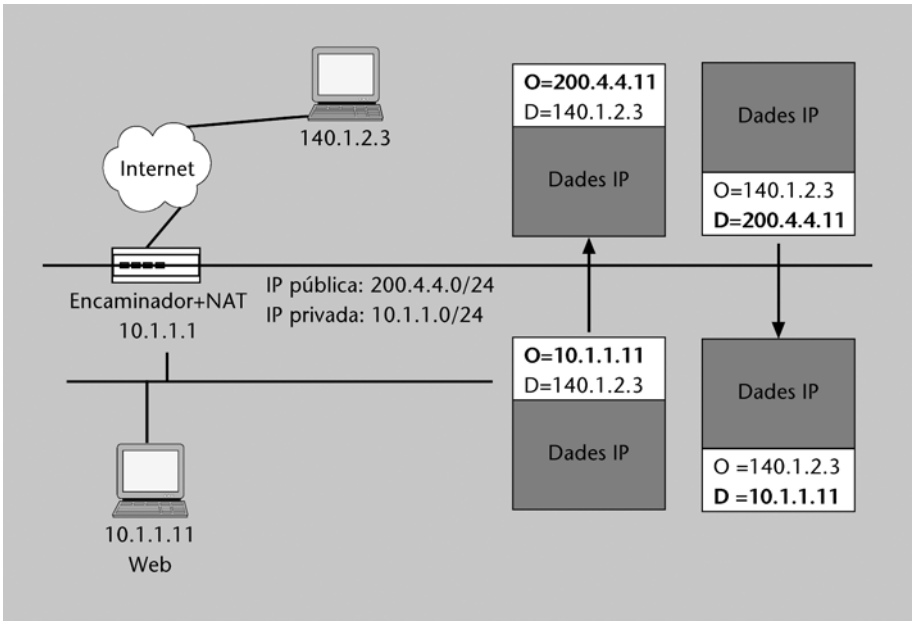
Relació d'adreces

La relació estàtica entre l'adreça pública i la privada serà a la taula de NAT fins que l'administrador decideixi d'esborrar-la.

El procés d'operació de NAT sobre els paquets IP és el següent: quan una màquina de la xarxa interna envia un paquet a la xarxa externa, el valor de l'adreça IP origen serà l'adreça privada de l'estació origen (per exemple, 10.1.1.11). Un cop el paquet arribi a l'encaminador, aquest aplicarà la traducció d'adreces correspo-

nent, i el paquet IP viatjarà ara amb l'adreça IP origen pública corresponent (200.4.4.11 en aquest cas). La resposta de la màquina destinació anirà encaminada cap a 200.4.4.11 (adreça IP destinació), que es convertirà en 10.1.1.11 en travessar l'encaminador.

L'escenari següent mostra el mode d'operació de NAT i la traducció de les diferents adreces:



És important destacar que s'aplica el mateix procés quan l'origen del trànsit és extern, ja que qualsevol màquina que disposa d'una traducció NAT estàtica serà accessible des de l'exterior. Així, doncs, si una estació externa es vol connectar amb una estació de la xarxa interna (per exemple, 10.1.1.11), l'adreça destinació que utilitzarà serà l'adreça pública (200.4.4.11), corresponent a l'adreça interna de l'estació. Quan l'encaminador rebi un paquet destinat a aquesta adreça pública, la traduirà per l'adreça privada que pertoca i enviarà el paquet cap a la xarxa interna.

5.2. NAT dinàmic

La traducció dinàmica d'adreces té lloc quan l'encaminador de sortida de la xarxa coneix el conjunt d'adreces internes que ha de traduir i el rang d'adreces que pot emprar com a adreces públiques. I és aquest dispositiu qui estableix la relació entre aquests dos conjunts d'adreces de manera dinàmica.

El NAT dinàmic assigna dinàmicament la relació entre adreça privada i adreça pública, i es basa en el fet que no totes les màquines de la nostra organització estaran connectades a Internet alhora i, per tant, no cal disposar de tantes adreces públiques com adreces privades hi hagi.

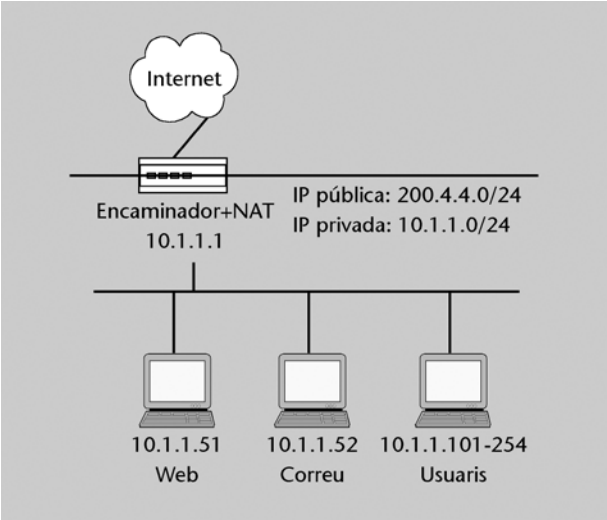
Per a definir el NAT dinàmic caldrà fixar els rangs d'adreces utilitzades. Això significa que l'administrador de la xarxa haurà d'haver definit prèviament la política d'assignació d'adreces IP per aquesta xarxa.

Imaginem, per exemple, la xarxa de l'apartat anterior en la qual tenim, ara, un nombre elevat d'usuaris que s'han de connectar a Internet. Per a tots ells utilitzarem NAT dinàmic. A més, també tenim dos servidors que cal publicar a Internet, per als quals utilitzarem NAT estàtic.

Inferirem que la política d'assignació d'adreces IP és la següent:

- Encaminadors: valors de *host* d'1 a 20
- Servidors: valors de *host* de 50 a 100
- Usuaris: valors de *host* de 101 a 254
- La resta de valors els reservem per a aplicacions futures.

Les adreces públiques i les adreces privades són les mateixes que en l'exemple de l'apartat anterior. Per tant, l'escenari d'aquest exemple el podem representar amb l'esquema següent:



La taula de traduccions de NAT de l'encaminador de sortida de la xarxa podria ser la següent:

Tipus de NAT	Adreça privada	Adreça pública
Estàtic	10.1.1.51	200.4.4.1
Estàtic	10.1.1.52	200.4.4.2
Dinàmic	Rang: 10.1.1.101 a 10.1.1.254	Rang: 200.4.4.10 a 200.4.4.110

En aquest cas, el rang d'adreces privades és superior en nombre al rang d'adreces públiques. Aquest cas es dóna quan hem de connectar a Internet un nombre de màquines superior al d'adreces públiques disponibles. No hi haurà cap problema mentre no hi hagi més màquines connectades simultàniament a Internet que adreces al rang d'adreces públiques.

Cada vegada que una màquina enviï un paquet IP cap a Internet, a la seva adreça privada se li assignarà una adreça pública que es guardarà en una taula de traduccions. Cada traducció tindrà un temps de caducitat, després del qual s'esborrarà de la taula de manera que pugui ser utilitzada per noves adreces privades.

Exemple

Inferim que les màquines 10.1.1.113, 10.1.1.197 i 10.1.1.225 accedeixen simultàniament a Internet en un moment determinat. La taula de traduccions de l'encaminador que aplica el NAT dinàmic podria ser la següent:

Adreça privada	Adreça pública
10.1.1.113	200.4.4.10
10.1.1.197	200.4.4.11
10.1.1.225	200.4.4.12

Qualsevol trànsit originat a l'exterior de la xarxa privada i destinat a alguna de les adreces públiques utilitzades en el NAT dinàmic, encara que en aquell moment aparegui en la taula de traduccions dinàmiques, serà automàticament descartat en l'encaminador. Això és així perquè la correspondència (IP privada-IP pública) cada vegada pot ser diferent.

En aquest cas ja aconseguim una primera mesura de seguretat: amaguem part de la nostra infraestructura de xarxa a l'exterior i únicament publiquem amb NAT estàtic els serveis que realment cal publicar a l'exterior.

5.3. PAT (*port address translation*)

PAT és un tipus de NAT dinàmic que permet de reduir al màxim (fins a 1) el nombre d'adreces IP públiques utilitzades dinàmicament. Per a aconseguir-ho, PAT utilitza el port TCP/UDP amb l'objectiu identificar l'origen de la comunicació (usuari de la nostra xarxa interna).

Així, doncs, la seva configuració serà similar a la del NAT dinàmic però afegint el rang dels ports que s'han d'utilitzar. Cal, però, tenir en compte que no es pot utilitzar qualsevol port, sinó els ports assignats per la IANA als clients.

Recordem quins són aquests ports:

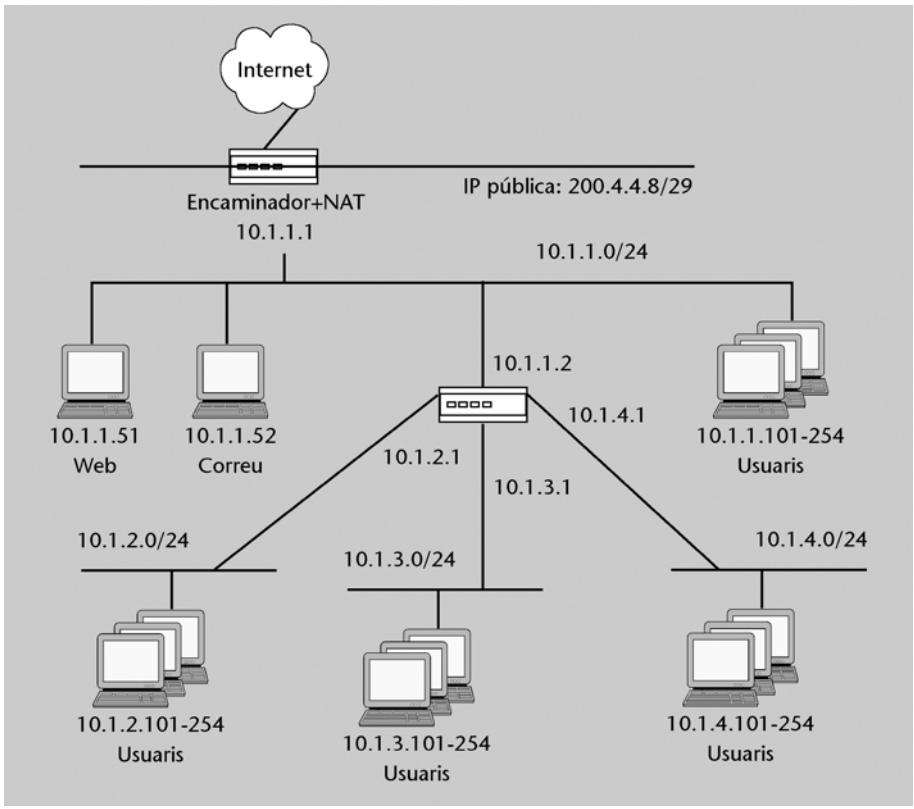
- De l'1 al 1023(*well-known-ports*): ports definits per la IANA per als seveis estàndards TCP/IP. Exemple: FTP (21), SMTP (25), Telnet (23), web (80).
- Del 1024 al 5000: ports utilitzats per les aplicacions client. D'altra banda, seran els ports que PAT podrà utilitzar.
- Majors de 5000: ports per a aplicacions no estàndards.

IANA

La IANA (Internet Assigned Number Authority) és l'organització que, inicialment, es va encarregar de distribuir i assignar l'adreçament públic a Internet. Actualment depèn de l'organització anomenada *ICANN* (Internet Corporation for Assigned Names and Numbers).

PAT permet de traduir diferents adreces privades d'una xarxa interna en una única adreça pública. Així, doncs, per a poder distingir les diferents comunicacions utilitza, a més, els identificadors de port TCP/UDP.

A continuació complicarem l'exemple anterior per veure que el PAT realment permet de reduir al màxim el nombre d'adreces públiques necessàries. Pensem novament en la xarxa anterior, amb els dos servidors de web i correu, que continuaran utilitzant NAT estàtic. En aquesta xarxa el nombre d'usuaris que requereixen accés a Internet ha augmentat fins a quatre-cents, separats en quatre xarxes diferents (uns cent usuaris per xarxa). En la il·lustració següent es representa el nou escenari:



A més, el nostre proveïdor de serveis a Internet ha fet canvis en l'adreçament IP i ara únicament ens pot oferir l'adreça IP 200.4.4.8/29 per a tot el nostre sistema. Fixem-nos que, tot i que sembla que l'adreça IP és la mateixa, la màscara associada ara és de 29 bits (255.255.255.248), i això limita el nombre d'adreces públiques disponibles a sis:

Adreces IP disponibles
200.4.4.9
200.4.4.10
200.4.4.11

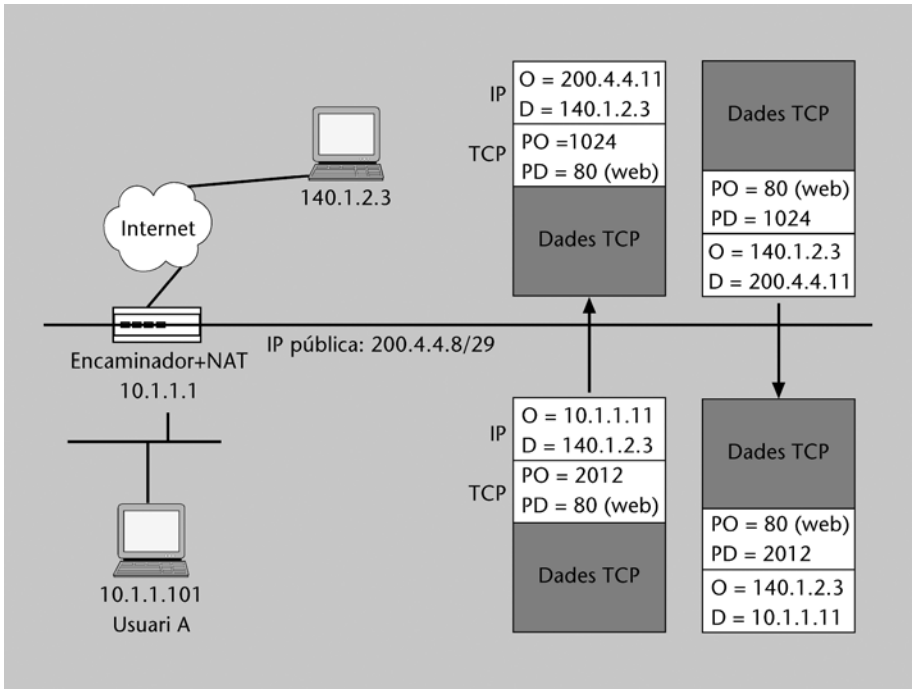
Adreces IP disponibles
200.4.4.12
200.4.4.13
200.4.4.14

Davant aquesta limitació d'adreces públiques decidim d'utilitzar PAT perquè els usuaris de la xarxa tinguin accés a Internet. Utilitzarem únicament una adreça IP per al PAT, dues per als servidors (NAT estàtic) i la resta per als possibles nous servidors que hàgim de publicar a Internet. Evidentment, sempre podem posar més d'un servei en un mateix servidor (per exemple, web i correu en el mateix servidor), amb la qual cosa estalviaríem novament adreces IP, però caldrà tenir en compte que massa serveis poden col·lapsar el nostre servidor.

Davant aquesta tria, la configuració del nostre NAT, utilitzant la mateixa política d'assignació d'adreces IP, podria ser la següent:

Tipus de NAT	Adreça privada	Adreça pública
Estàtic	10.1.1.51	200.4.4.9
Estàtic	10.1.1.52	200.4.4.10
PAT	Rangs: 10.1.1.101 a 10.1.1.254 10.1.2.101 a 10.1.2.254 10.1.3.101 a 10.1.3.254 10.1.4.101 a 10.1.4.254	200.4.4.14 Ports: 1024 al 5000

Analitzem ara com actua l'encaminador que aplica PAT per a poder gestionar tantes connexions TCP/IP contra servidors externs amb una única adreça IP pública:



Cada vegada que l'encaminador de sortida rep una nova connexió TCP o UDP contra l'exterior, li assigna un port lliure del rang especificat. D'aquesta manera, totes les connexions es publiquen a l'exterior amb la mateixa adreça IP, però són distingides segons el port TCP o UDP assignat. Aquesta relació es guarda en la taula dinàmica de traduccions perquè, en arribar la resposta de l'exterior, es pugui reencaminar cap al client corresponent.

Per exemple, pensem en el cas plantejat en la figura anterior, en què l'usuari A vol establir una connexió web (port 80) contra el servidor 140.1.2.3. Imaginem que hi ha dos usuaris més que també volen establir connexions web contra aquest servidor. Un cop establertes aquestes connexions, la taula de traduccions PAT de l'encaminador de sortida tindrà un aspecte com el de la taula següent:

Origen privat	Destinació	Origen públic
10.1.1.101 : 2012	140.1.2.3 : 80	200.4.4.14 : 1024
10.1.2.120 : 3378	140.1.2.3 : 80	200.4.4.14 : 1025
10.1.4.220 : 1906	140.1.2.3 : 80	200.4.4.14 : 1026

5.4. LSNAT (*load sharing* NAT)

Aquest tipus de NAT està pensat per a solucionar el problema que presenten els servidors d'aplicacions sobresaturats, com ara els portals o els cercadors. Si es dóna el cas que el servei que oferim a Internet rep tantes sol·licituds que no les pot absorbir, la primera solució que se'ns pot plantejar és la de comprar un servidor més potent. Normalment això té un cost molt elevat i un problema greu: i si falla aquest únic servidor?

La solució a tots dos problemes és replicar el nostre servidor; és a dir, cal comprar més servidors, però de les mateixes prestacions que el que ja tenim, opció que segurament és més econòmica que comprar un servidor més potent. Un cop fet això, aplicarem un sistema que publiqui tots els servidors a Internet com si fossin un únic servidor, i repartirem la càrrega entre tots; d'aquesta manera, en cas que un falli, redirigirà les peticions cap a la resta, de manera que l'usuari no en rebi les conseqüències.

En aquest cas tindrem *n* servidors amb diferents adreces privades, els quals estaran identificats per la mateixa adreça pública o *virtual* IP *address*.

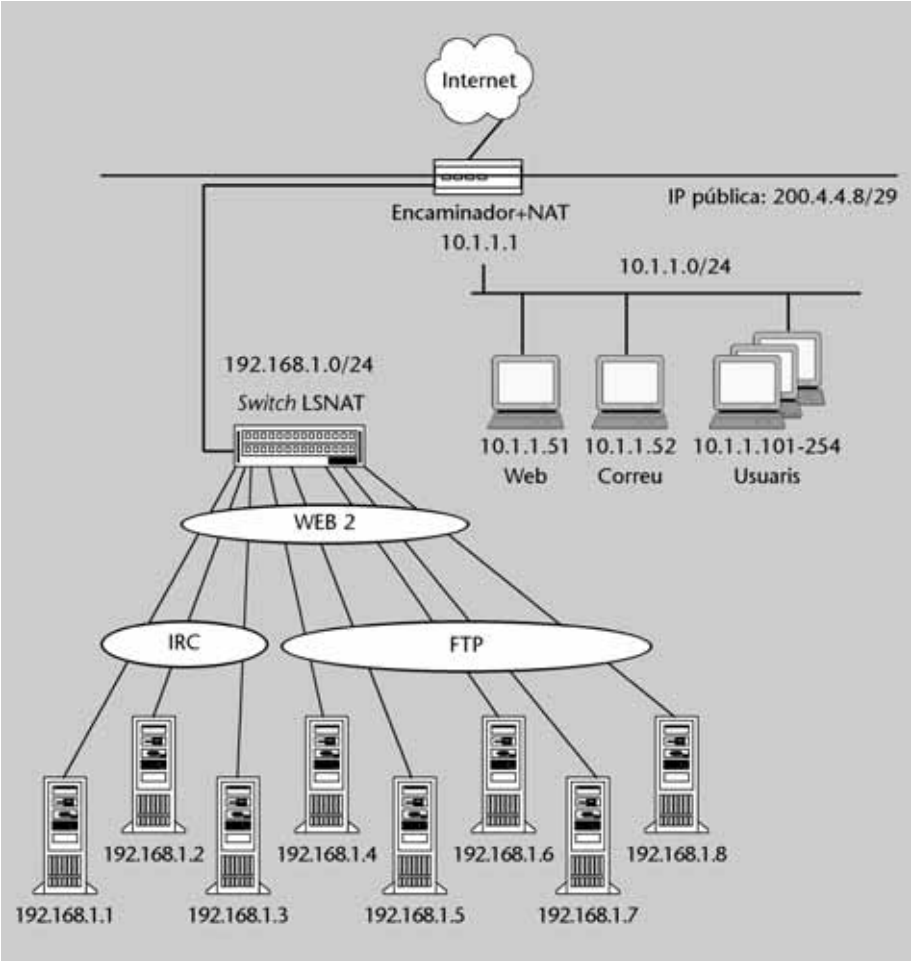
Normalment l'LSNAT requereix una alta càrrega del processador, per la qual cosa se sol fer en un commutador d'altes prestacions, i no en l'encaminador perimetral.

LSNAT permet la distribució de la càrrega entre diversos servidors d'aplicacions de manera que, a Internet, aquests servidors són publicats amb una adreça pública única.

Exemple d'aplicació d'LSNAT

Plantegem ara un nou cas en què volem oferir a Internet tres serveis: web2, FTP i IRC (xat). Després d'analitzar el trànsit que esperem tenir decidim de comprar vuit servidors iguals, entre els quals repartirem tots tres serveis de la manera següent:
El servei web2 estarà replicat en tots vuit servidors. Serà un servei web nou addicional al que ja tenim.
El servei FTP en cinc d'aquests.
El servei IRC en els tres que no tenen el servei d'FTP.

Per a poder mantenir el disseny de l'apartat anterior, afegirem un nou port a l'encaminador perimetral, que estarà connectat a un commutador d'altes prestacions amb capacitat d'LSNAT. L'adreça privada de xarxa que utilitzarem en aquest cas serà la 192.168.1.0/24, i les adreces públiques dels nous serveis seran les tres adreces lliures que queden:
Web: 200.4.4.11
FTP: 200.4.4.12
IRC: 200.4.4.13



Amb aquestes dades, la configuració LSNAT del commutador d'altes prestacions seria la següent:

Tipus de NAT	Adreça privada	Adreça pública
LSNAT	Rang: 192.168.1.1 a 192.168.1.8	200.4.4.11 : 80
LSNAT	Rang: 192.168.1.4 a 192.168.1.8	200.4.4.12 : 21
LSNAT	Rang: 192.168.1.1 a 192.168.1.3	200.4.4.13 : IRC

Qualsevol usuari que vulgui accedir al servei web utilitzarà l'adreça virtual IP (VIP) 200.4.4.11. Internament, aquesta adreça es correspon amb vuit adreces privades diferents, una per a cada servidor web. És a dir, que el commutador d'altes prestacions escollirà l'adreça privada més adient, tot i que aquest procés serà completament transparent a l'usuari, que pensarà que es connecta a un únic servidor web.

Resum

En aquest mòdul hem descrit com es poden dissenyar xarxes d'àrea local amb característiques de commutació de paquets, amb els dispositius anomenats **commutadors**. A continuació hem descrit les característiques més importants i les millores introduïdes per les xarxes Fast Ethernet. Després hem estudiat els fonaments de la tecnologia Gigabit Ethernet. Hem vist els medis físics que normalitzen i hem estudiat la problemàtica que apareix amb la distància de col·lisió, ja que Gigabit Ethernet treballa a velocitats molt més elevades que no pas Ethernet o Fast Ethernet. Hem vist igualment el concepte de cablatge estructurat i hem descrit les característiques de les xarxes d'àrea local sense fil.

Hi ha diferents prestacions en les xarxes Ethernet que s'utilitzen per a millorar-ne l'eficiència. Hem analitzat els avantatges del mode de transmissió *full-duplex*, que permet que dues estacions puguin transmetre i rebre dades simultàniament; hem vist que les estacions s'envien missatges per controlar el flux de la informació, així, en cas de congestió, poden avisar l'origen perquè pari d'enviar informació fins que la congestió es resolgui; i també hem vist el concepte d'autonegociació, que permet als dispositius d'anunciar les seves possibilitats per aprofitar al màxim les prestacions dels elements de la xarxa.

A continuació hem descrit la diferència entre les xarxes amb una arquitectura commutada tradicional i les LAN virtuals, que fan una agrupació lògica dels usuaris o dispositius i que, per tant, comporten una independència entre la topologia física i la topologia lògica. Hem analitzat les característiques principals de les VLAN, i també els dispositius que les formen. També hem classificat les VLAN segons l'assignació dels usuaris i elements per a cada VLAN. Finalment, hem estudiat el protocol IEEE-802.1q i hem vist la necessitat de marcar les trames entre els commutadors.

Per acabar, hem estudiat dos conceptes relacionats amb la traducció d'adreces: NAT i LSNAT. El primer relaciona adreces privades d'una xarxa amb adreces públiques, per tal que les estacions que no tinguin una adreça IP "legal" puguin accedir a Internet. A continuació hem vist la gran utilitat d'LSNAT, que permet de disminuir els colls d'ampolla que es creaven en els accessos als servidors. Aquest fet s'ha aconseguit a partir d'adreces IP virtuals, que estableixen una correspondència amb tot un seguit de màquines i permeten de fer una distribució de la càrrega de xarxa.

Exercicis d'autoavaluació

Pregunta 1

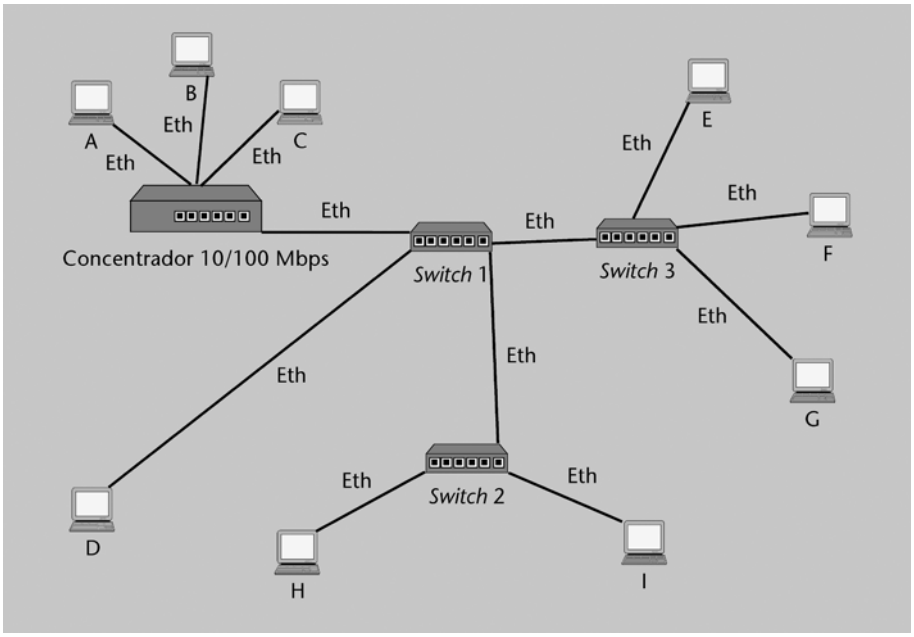
Quina de les afirmacions següents no és un avantatge quan s'utilitzen VLAN estàtiques?
a) Les VLAN estàtiques són segures.
b) Les VLAN estàtiques són fàcils de configurar.
c) Les VLAN estàtiques són fàcils de monitoritzar.
d) Les VLAN estàtiques configuren automàticament els ports quan s'hi afegeixen noves estacions.

Pregunta 2

Quin tipus de dispositiu proporciona la comunicació entre les VLAN creades en una xarxa?
a) Commutador.
b) *Bridge*.
c) Concentrador.
d) Encaminador.

Problema 1

Responeu de manera raonada les preguntes següents referents a aquest esquema tenint en compte que tots tres commutadors disposen de vuit ports 10/100 Eternet.



a) En Ethernet, Fast Ethernet i Gigabit, i en mode *full duplex*, quin mètode d'accés al medi s'utilitza?

b) Com podem augmentar la velocitat de comunicació entre el commutador 1 i el commutador 2?

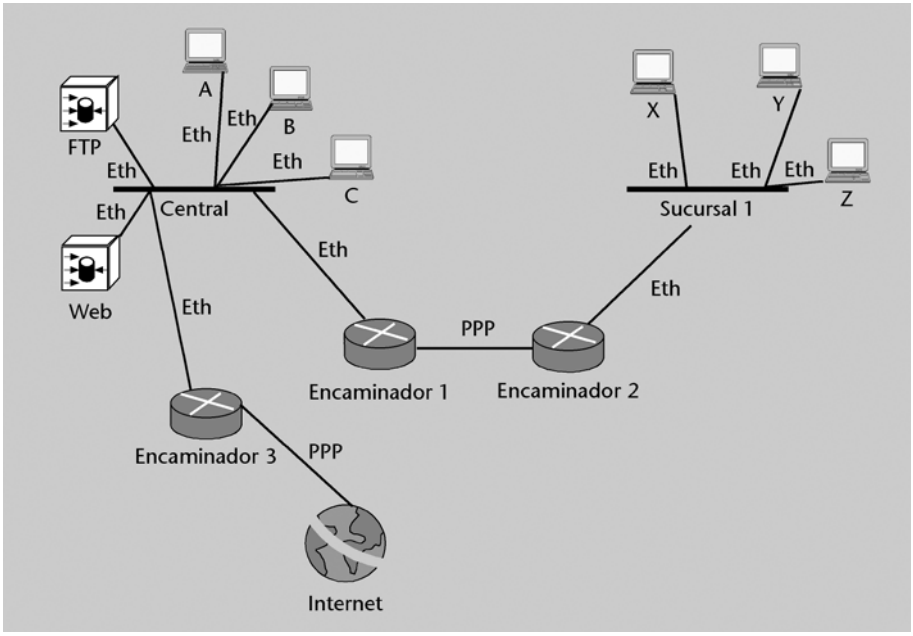
c) Indiqueu quins elements de la xarxa cal configurar per a crear les VLAN següents:
- VLAN 1: *hosts* A, B, E, F, I
- VLAN 2: *hosts* C, D, G, H

Descriviu, també, la nova configuració de cadascun d'ells.

d) Indiqueu quins canvis (equips, connexions, configuració dels equips, etc.) cal introduir per a aconseguir la comunicació entre totes dues VLAN?

Problema 2

Tenim la xarxa de l'empresa Germans Associats SA, amb un enllaç punt a punt entre la central i la sucursal, segons mostra la figura següent:



Les adreces de les xarxes són les següents:
– Xarxa de la central: 169.33.78.0 / 24
– Xarxa de la sucursal 1: 169.33.79.0 / 24
– Enllaç punt a punt entre l'encaminador 1 i l'encaminador 2: 169.33.80.4 / 30

a) El servidor web i el d'FTP reben massa "sol·licituds" des d'Internet i estan massa saturats. Per això, se'ns demana dissenyar un nou sistema per a absorbir quatre vegades més trànsit de l'actual, i saben que no hi ha cap tipus de servidor més potent que el que ja tenen.

b) Per qüestions de seguretat volen dissenyar la xarxa per tal que les adreces IP dels usuaris STAFF no siguin visibles des de l'exterior, però que continuïn tenint accés a Internet. Per això se'ns demana el següent:
– Modificar la xarxa de l'apartat a) per a aconseguir-ho.
– Reassignar les adreces IP necessàries.
– Indicar quines són les adreces IP dels encaminadors 1 i 2.

c) Escriviu la taula de configuració de NAT de l'encaminador en què s'apliqui les traduccions d'adreces.

Solucionari

Solució pregunta 1

La resposta correcta és la d).

Les VLAN estàtiques no configuren automàticament els ports quan s'hi afegeixen noves estacions. És l'administrador de la xarxa qui ha de configurar els commutadors perquè reconeguin les noves estacions. Tanmateix, aquesta configuració és molt fàcil, ja que només cal indicar a quina VLAN pertanyerà el port que s'utilitza de nou. També són fàcils de monitoritzar, i les VLAN, tant les dinàmiques com les estàtiques, introdueixen un element més de seguretat.

Solució pregunta 2

La resposta correcta és la d).

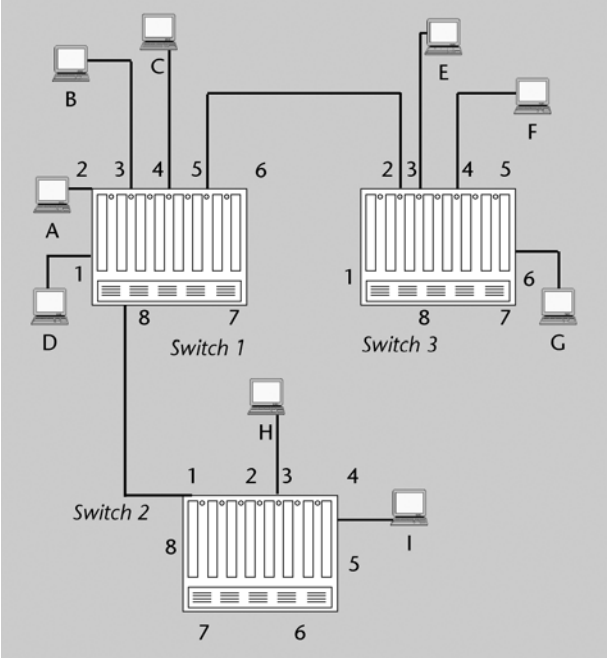
L'encaminador és l'únic dispositiu que permet que dues estacions de VLAN diferents es puguin comunicar entre elles. Sense un dispositiu de nivell 3, la comunicació entre LAN no serà possible.

Solució problema 1

a) En mode *full duplex* no s'utilitza cap protocol d'accés al medi, com és el CSMA/CD en Ethernet *half duplex*, ja que en configuracions *full duplex* el medi no és un medi compartit, sinó que és un enllaç amb dos canals independents: un per a transmissió i un per a recepció.

b) Utilitzant els ports lliures, podem agrupar *n* enllaços Fast Ethernet com si fos un únic enllaç de $n \times 100$ Mbps. Només cal tenir en compte el següent:
- Tots els enllaços han de tenir la mateixa velocitat (100 Mbps, per exemple).
- Tots els enllaços han de funcionar en mode *full duplex*.
- Cal desactivar el protocol Spanning Tree entre els enllaços.

c) En l'escenari podem veure que les estacions A, B i C estan connectades al mateix concentrador. En l'enunciat ens demanen que les estacions A i B han de pertànyer a la VLAN 1 i que, en canvi, l'estació C ha de pertànyer a la VLAN2. Per tant, haurem de canviar la connexió i fer que les estacions A, B i C estiguin connectades a diferents ports del commutador 1. Així podrem aconseguir que les estacions pertanyin a VLAN diferents:



La configuració dels commutadors haurà de ser la següent:

- Commutador 1:
– Ports 5, 8: *trunk ports*
– Ports 2, 3, 5, 8: VLAN 1
– Ports 1, 4, 5, 8: VLAN 2

- Commutador 2:
– Port 1: *trunk port*
– Ports 1, 5: VLAN 1
– Ports 1, 2: VLAN 2

- Commutador 3:
– Port 2: *trunk port*
– Ports 2, 3, 4: VLAN 1
– Ports 2, 6: VLAN 2

d) Quins canvis (equips, connexions, configuració dels equips, etc.) cal introduir per a aconseguir la comunicació entre totes dues VLAN?

Si volem aconseguir la comunicació entre totes dues VLAN, serà necessari connectar un encaminador. Tenim diferents opcions:

–- Podem utilitzar un encaminador i connectar dues de les seves interfícies a dos ports de qualsevol dels commutadors. Així configurarem un port per a la VLAN 1 i un altre port per a la VLAN 2.

–- Podem utilitzar un encaminador amb un únic port físic que suporti 802.1q, en què internament li definiríem dues interfícies IP, una per a cada VLAN. Aquest port físic el podem connectar a un port de qualsevol dels tres commutadors. Caldrà configurar, llavors, aquest port com a *trunk port*.

Solució problema 2

a) Si volem dissenyar un sistema que absorbeixi quatre vegades més trànsit de l'actual sense poder disposar de servidors més potents, haurem d'utilitzar més servidors i distribuir la càrrega entre aquests. Per tant, si teníem dos servidors, ara caldrà tenir-ne vuit, per a poder absorbir el nou trànsit.

Imaginem que el creixement de trànsit serà el mateix per al servidor FTP i el servidor web. Per tant, utilitzarem quatre servidors FTP i quatre servidors web i emprarem LSNAT per a distribuir la càrrega entre aquests.

L'adreça pública disponible és la 169.33.78.0 / 24. Connectarem l'encaminador perimetral (encaminador 3) a un commutador d'altes prestacions amb capacitat d'LSNAT. L'adreça privada de xarxa que utilitzarem serà la 192.168.1.0/24, i les adreces públiques dels nous serveis seran les adreces següents:

– Web: 169.33.78.11
– FTP: 169.33.78.12

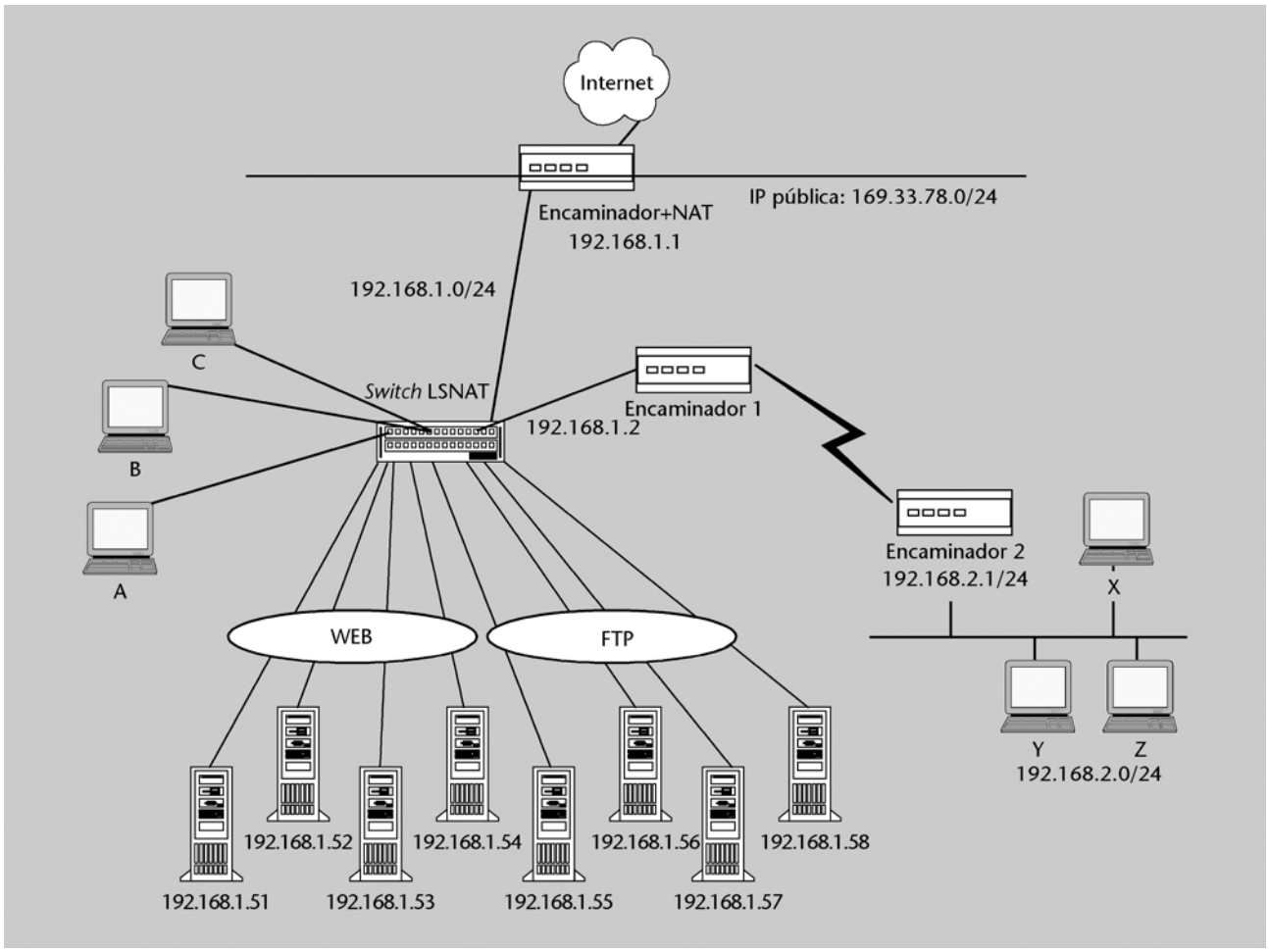
Amb aquestes dades, la configuració LSNAT del commutador d'altes prestacions seria la següent:

Tipus de NAT	Adreça privada	Adreça pública
LSNAT	Rang: 192.168.1.51 a 192.168.1.54	169.33.78.11 : 80
LSNAT	Rang: 192.168.1.55 a 192.168.1.58	169.33.78.12 : 21

b) Per a aconseguir que els usuaris interns no siguin visibles des de l'exterior, però que continuïn tenint accés a Internet, cal posar, com a mínim, un equip que implementi NAT. Aquest serà l'encaminador perimetral, l'encaminador 3.

En la figura següent es pot veure la implementació d'LSNAT mitjançant el commutador d'altes prestacions i l'assignació de les adreces privades en totes les xarxes. La política d'assignació d'adreces seguida en aquest escenari ha estat la següent:

– Encaminadors: valors de *host* d'1 a 20
– Servidors: valors de *host* de 50 a 100
– Usuaris: valors de *host* de 101 a 254
– La resta de valors els reservem per a aplicacions futures.



Podem utilitzar PAT per a minimitzar el nombre d'adreces públiques que s'han fet servir. Així, doncs, la configuració seria la següent:

Tipus de NAT	Adreça privada	Adreça pública
PAT	Rangs: 192.168.1.101 a 192.168.1.254 192.168.2.101 a 192.168.2.254	169.33.78.15 Ports: 1024 al 5000

c) L'encaminador en què s'aplica la traducció d'adreces és l'encaminador perimetral, l'encaminador 3. La seva taula de traduccions serà la següent:

Tipus de NAT	Adreça privada	Adreça pública
PAT	Rangs: 192.168.1.101 a 192.168.1.254 192.168.2.101 a 192.168.2.254	169.33.78.15 Ports: 1024 al 5000
LSNAT	Rang: 192.168.1.51 a 192.168.1.54	169.33.78.11 : 80
LSNAT	Rang: 192.168.1.55 a 192.168.1.58	169.33.78.12 : 21

Glossari

encaminador *m* Dispositiu de la capa de xarxa que utilitza una o més mètriques per a trobar el camí òptim pel qual ha de viatjar la informació. Passa la informació d'una xarxa a una altra segons la informació de la capa de xarxa. **en**: router

full duplex *f* Capacitat per a la transmissió i recepció de dades de manera simultània entre una estació origen i una estació destinació.

half duplex *f* Capacitat per a la transmissió de dades en una única direcció a la vegada entre una estació origen i una estació destinació.

IEEE *m Vegeu* Institute of Electrical and Electronics Enginneers.
Institute of Electrical and Electronics Enginneers *m* Organització professional que s'encarrega, entre altres temes, del desenvolupament d'estàndards de comunicacions i de xarxa. Els estàndards LAN de l'IEEE són els estàndards predominants en xarxes d'àrea local d'avui en dia.
sigla: IEEE

LAN virtual *f* Grup de dispositius d'una LAN que es configuren de manera que es puguin comunicar com si realment estiguessin connectats al mateix medi físic quan, en realitat, estan situats en segments de LAN diferents. VLAN estan basades en connexions lògiques, no físiques.
sigla: VLAN

màscara de xarxa *f* Màscara de 32 bits emprada en IP per a indicar els bits d'una adreça IP que s'utilitzen com una adreça de subxarxa. Moltes vegades, simplement se l'anomena *màscara*.
en: subnet mask

NAT *f Vegeu* network address translation.

network address translation *f* Tècnica que proporciona una adreça pública a usuaris d'una xarxa que treballen amb adreçament privat. D'aquesta manera els usuaris poden accedir a Internet.
sigla: NAT

open systems interconnection *m* Model de comunicació entre dispositius que cooperen entre ells. Defineix una arquitectura de set capes de funcions de comunicació.
sigla: OSI

OSI *m Vegeu* open systems interconnection.

PAT *m Vegeu* port address translation.

port address translation *m* Juntament amb NAT, PAT utilitza adreces de port per a fer una correspondència entre adreces IP locals i globals.
sigla: PAT

router *m Vegeu* encaminador.

shielded twisted pair *m* Medi de transmissió format per dos cables de coure aïllats trenats l'un amb l'altre. Entre la coberta exterior de plàstic i el parell, es col·loca un apantallament metàl·lic.
sigla: STP

STP *m Vegeu* shielded twisted pair.

subxarxa *f* Es parla de subxarxa en xarxes IP, quan una xarxa té una adreça de subxarxa particular. Les xarxes i subxarxes són xarxes que l'administrador de la xarxa acostuma a segmentar arbitràriament per obtenir una estructura d'encaminament jeràrquica, i mantenir la mateixa adreça de xarxa per al conjunt.
en: subnet

subnet *f Vegeu* subxarxa.

subnet mask *f Vegeu* màscara de xarxa.

TCP/IP *m Vegeu* transmission control protocol / Internet protocol.

transmission control protocol / Internet protocol *m* Model de comunicació entre dispositius que cooperen entre ells i que s'intercanvien informació. És la base de funcionament d'Internet.
sigla: TCP/IP

unshielded twisted pair *m* Medi de transmissió format per dos cables de coure aïllats trenats l'un amb l'altre. La coberta exterior del parell és de plàstic.
sigla: UTP

UTP *m Vegeu* unshielded twisted pair.

VLAN *f Vegeu* LAN virtual.

Bibliografia

Amato, V. (1999). *Cisco Networking Academy Program: Second-Year Companion Guide*. Cisco Press.

Black, U. (1997). *Tecnologías emergentes para redes de computadoras* (2a. ed.). Pearson Educación.

Garcia, J. (1997). *Redes de alta velocidad*. Editorial Ra-ma.

Stallings, W. (2000). *Data and Computer Communications* (6a. ed.). Prentice Hall.