

Disseny de xarxes WAN i noves tecnologies

Pere Barberán Agut

PID_00177136



Universitat Oberta
de Catalunya

www.uoc.edu

Índex

Introducció	5
Objectius	6
1. Disseny de xarxes	7
1.1. Introducció al disseny de xarxes WAN	7
1.1.1. Conceptes sobre xarxes WAN	8
1.1.2. Diferències entre xarxes LAN i WAN	8
1.1.3. Similituds entre xarxes LAN i WAN	8
1.2. Disseny de xarxes	9
1.3. Objectius en el disseny de xarxes	9
1.4. Tasques en el procés de disseny	10
1.5. Principis en el disseny de xarxa	10
1.6. Disseny IP	11
1.6.1. Planificació d'adreces IP	11
1.6.2. Subxarxes amb màscara de longitud variable (VLSM)	14
1.6.3. Sumarització de rutes	16
1.6.4. Conceptes sobre l'encaminament IP	20
2. Xarxes metropolitanas	28
2.1. Les xarxes metropolitanas	28
2.1.1. Nous requeriments de les xarxes metropolitanas	29
2.1.2. Reptes i oportunitats per als proveïdors de serveis	30
2.1.3. Restriccions d'SDH/SONET	31
2.2. Les xarxes Ethernet metropolitanas	31
2.2.1. Justificació MetroEthernet	33
2.3. Ethernet sobre SDH (EOS)	36
2.3.1. Concatenació virtual	38
2.3.2. Ajustar la capacitat de la connexió (LCAS)	38
2.4. Resilient packet ring (RPR) IEEE 802.17	39
3. Multiprotocol label switching	41
3.1. Problemes experimentats pels proveïdors de servei	41
3.2. Què és MPLS?	41
3.3. Beneficis d'MPLS	42
3.4. Pila d'etiquetes MPLS (MPLS label stack)	42
3.4.1. Capçalera inserida (shim header)	43
3.4.2. Forwarding equivalence class (FEC)	43
3.5. Arquitectura MPLS	43
3.6. Components de xarxa MPLS	44
3.6.1. Establiment de l'LSP	45

3.7. Protocol de distribució d'etiquetes (LDP)	46
Resum	48
Activitats	49
Exercicis d'autoavaluació	50
Solucionari	51
Glossari	52
Bibliografia	53

Introducció

El *boom* d'Internet ha provocat que el model de transport de dades que utilitzen les operadores de telecomunicacions en el nucli de les seves xarxes hagi anat quedant obsolet en el transcurs d'aquests darrers anys. Això ha portat a treballar en el desenvolupament de noves tecnologies de xarxa i protocols de comunicació que facin possible afrontar amb garantia d'èxit el creixement de les necessitats de transport de dades i els requeriments dels serveis previstos per al futur.

D'altra banda, a nivell d'empresa estar connectat a Internet ha estat un imperatiu, de manera que la societat actual està marcada per mesures associades a Internet i la seva ràpida evolució en el temps. Això obliga les organitzacions a desenvolupar-se i reaccionar de forma ràpida. Aquests fets provoquen que el disseny de les xarxes, que haurien de fer-se de manera òptima, escalable, segura, disponible, etc., acabin fent-se amb la manca d'alguna d'aquestes característiques bàsiques o de totes. La manca d'alguna d'elles acaba sent un factor crític dintre de la infraestructura.

Així, aquest mòdul didàctic es pot dividir en dues parts ben diferenciades. A la primera part es veuen els elements bàsics que cal que ens plantejem quan volem fer un bon disseny de xarxa. L'anàlisi de xarxes, l'arquitectura i el disseny han estat tradicionalment considerats un art en què es combinaven regles particulars en l'avaluació i l'elecció de les tecnologies de xarxa. Així, l'èxit o el fracàs d'un disseny de xarxa particular depenia bàsicament de qui estava fent el treball. Avui en dia, en canvi, les xarxes formen part del treball i per tant es consideren elements crítics. Això fa que tant l'arquitectura com el disseny de xarxa hagin de ser lògics i reproduïbles, i que es puguin defensar. Aquesta part per si sola podria ser un llibre sencer, de manera que el que es pretén és mostrar només els principis bàsics en el disseny de xarxes.

A la segona part del mòdul ens centrem en tecnologies i s'intenta veure les diverses tendències actuals en xarxes metropolitanes i xarxes d'àrea estesa. En tots dos casos es veurà que, d'una banda, el que es vol és portar Ethernet més enllà de les xarxes d'àrea local, i de l'altra, que el protocol cap on van totes les operadores és MPLS.

Objectius

Els materials didàctics d'aquest mòdul us han de permetre assolir els objectius següents:

- 1.** Entendre que un bon disseny de xarxa és bàsic a l'hora de tenir èxit en la implementació que es desenvolupi.
- 2.** Conèixer els principis bàsics que cal seguir quan es fa un disseny de xarxa.
- 3.** Conèixer els elements bàsics per a fer una bona planificació IP, la qual ha de permetre un correcte disseny lògic de la xarxa.
- 4.** Entendre l'evolució dels requeriments actuals per a les noves xarxes metropolitanas.
- 5.** Estudiar les diverses tecnologies actuals en entorns metropolitanas i justificar-ne l'evolució cap a les xarxes metropolitanas Ethernet.
- 6.** Conèixer les característiques bàsiques del protocol MPLS, la seva justificació, funcionament, etc.


1. Disseny de xarxes

1.1. Introducció al disseny de xarxes WAN

Abans de començar potser cal deixar clar que no hi ha una única possibilitat des de la idea inicial fins a la implementació real en el disseny de xarxes d'àrea estesa (WAN).

Xarxa d'àrea estesa, en anglès *wide area network* (WAN).

El que demana el client al final és una xarxa WAN el més ràpida possible sense perdre de vista les restriccions, és a dir, que tracti les dades de forma fiable, segura i a un cost raonable.

Per a aconseguir aquests principis bàsics, però a la vegada lògics, podem començar fent-nos una sèrie de preguntes: 

- És una instal·lació nova o estem substituint una infraestructura existent?
- Si ja existeix, quins problemes té l'usuari que li agradaria corregir?
- Quins són els requeriments?
- Quina és la taxa de transferència?
- La xarxa ha d'anar a alta velocitat en les dues direccions?

Aquestes preguntes inicials poden determinar els requeriments inicials de rendiment i fiabilitat. A partir d'aquí podem fer altres preguntes, com són:

- Quins nivells de seguretat necessitem?
- Si es vol que els encaminadors donin sortida a Internet llavors cal dissenyar polítiques de seguretat i tallafocs.
- Quines àrees es podrien comprometre?
- És l'alt rendiment prioritari per a totes les localitzacions?
- Hi ha àrees no tan prioritàries?
- S'enviaran només dades o es vol una solució que integri veu i dades?
- Es vol que la solució de veu sigui VoIP?
- Es volen estratègies de redundància?
- Quin cost representa per a l'empresa la caiguda de les connexions?

Podríem continuar fent preguntes afinant cada cop més els requeriments inicials. El que està clar és que no hi ha un camí únic en el disseny d'una xarxa.

Robert Cahn escriu: "no es pot dissenyar una xarxa a cap nivell sense algorismes", però a la vegada admet: "els problemes de disseny són massa complicats per a solucionar-se de forma exacta".

VoIP són les sigles de veu sobre tecnologia IP.

Importància de la redundància

La redundància és un aspecte molt important si volem que el sistema no pari de funcionar mai, però en moltes ocasions acaba essent un dels últims factors per considerar, atès que sempre s'intenta reduir despeses. Cal tenir sempre molt present l'efecte que pot tenir que caigui part o tota la xarxa pel que fa a la productivitat dels usuaris.

1.1.1. Conceptes sobre xarxes WAN

En el sentit més genèric, una xarxa WAN (*wide area network*) és una xarxa dispersa geogràficament. En el nostre cas definirem la xarxa WAN com una xarxa creada per a connectar dues o més xarxes d'àrea local (LAN). Així una xarxa WAN pot connectar LAN ubicades a la mateixa ciutat o que poden estar a qualsevol punt del món.

1.1.2. Diferències entre xarxes LAN i WAN


Normalment WAN es diferencia de la LAN en àrees com són cost, rendiment i expansió: 

- **Preu.** Les WAN és un cost recurrent. En la LAN, un cop instal·lada, l'usuari té en propietat tant el cablatge com els commutadors. En la WAN es paga a l'operadora pel lloguer de les línies i d'uns serveis.
- **Rendiment.** Entre les xarxes LAN i WAN hi ha diferències substancials en l'àmbit físic, de distàncies i de connexions. La LAN actualment es basa en Ethernet. En la WAN hi ha diverses possibilitats a nivell 2. Així, tenim aspectes com les latències, els paquets *broadcast* o altres que d'entrada es veuen afectats per les distàncies.
- **Expansió.** En les xarxes WAN el que estem connectant són dos punts a grans distància, els quals, en funció de l'expansió que puguin tenir, ens condicionarà el tipus de xarxa.

1.1.3. Similituds entre xarxes LAN i WAN

Podem trobar certes similituds quan parlem de localització dels recursos. Cal tenir clar i analitzar els fluxos de trànsit de les comunicacions. Mirant la infraestructura de xarxa del client hem de poder veure-hi com són certs aspectes:

- Protocols de xarxa i arquitectura d'interconnexió.
- Funcionament dels serveis de web i correu.
- Els requeriments de seguretat.
- Distribució de la topologia de la WAN. Quines localitzacions es volen interconnectar.
- El cost i rendiment que ofereixen els diversos proveïdors de servei i la logística i planificació per al seu desenvolupament.

Evidentment, per fer la planificació no heu d'oblidar de tenir en compte els canvis que es poden produir en el futur. 

1.2. Disseny de xarxes


Un bon disseny de xarxa és la base a l'hora de fer una bona implementació de la xarxa. La majoria de xarxes es poden agrupar en dues categories: aquelles que s'han anat fent en funció de les necessitats del moment i les que realment han estat pensades a partir d'un bon disseny. Aquest segon grup es caracteritza per la seva previsibilitat i consistència en relació amb els aspectes següents:

- **Rendiment.** Són xarxes amb un rendiment adequat en relació amb els paràmetres de rendiment establerts.
- **Disponibilitat.** S'hauria d'intentar que la caiguda de línies o dispositius de xarxa no afectessin les sessions client-servidor. Un paràmetre molt important és el temps de convergència.
- **Escalabilitat.** Una xarxa escalable és aquella que suporta de forma adequada el creixement sense haver de ser redissenyada de nou. Així, l'estructura de la topologia de xarxa i la tecnologia usades no han de ser redissenyades per a acomodar-se al creixement.
- **Cost de funcionament.** La xarxa no només ha de reunir certes especificacions tècniques, sinó que ha de ser rendible econòmicament en el seu disseny i implementació. Així, és important preveure que sigui una xarxa consistent quant a costos de funcionament.

Temps de convergència

El temps de convergència és l'interval de temps des d'una caiguda de la xarxa fins a la seva recuperació.

1.3. Objectius en el disseny de xarxes

És molt important aclarir els objectius des del principi dintre del procés de disseny de xarxes, ja que els paràmetres usats en el mateix serviran per a avaluar-lo. Cal tenir uns paràmetres de rendiment definits i uns nivells associats. Qui marca aquests nivells són les pròpies aplicacions i, en conseqüència, cal tenir clares les aplicacions tant quantitativament com qualitativament. Aquests paràmetres principals són l'amplada de banda, la pèrdua de paquets, el retard i la variació del retard. 

Un altre nivell que cal indicar en el disseny de la xarxa és la disponibilitat o temps de caiguda. És el temps que es permet que la xarxa estigui caiguda, en aquest cas està directament relacionat amb el tipus de funcionament, negoci, etc. de l'empresa.

Un paràmetre que cal tenir en compte, i en moltes ocasions s'oblida, és l'estimació de creixement potencial de la xarxa. Cal tenir clara l'evolució de l'empresa per saber el seu creixement en nombre d'usuaris, noves seus, etc. i poder preveure el trànsit de les aplicacions.

En últim cas, el plantejament ha de ser realista amb les possibilitats de la pròpia empresa.

Els objectius del disseny de xarxes són molt lògics, però normalment allò que és lògic és el que no es fa.

1.4. Tasques en el procés de disseny

A continuació es llisten unes quantes tasques que es poden considerar bàsiques en el procés de disseny de la xarxa: !

- Determinar els paràmetres de rendiment que millor especifiquen cadascun dels objectius de disseny.
- Identificar les restriccions en el disseny.
- Amb les restriccions a la mà, marcar els nivells de rendiment més rellevants de la xarxa.
- Començar sempre per un disseny d'alt nivell. No perdre's inicialment en els detalls.
- Comparar aquest disseny inicial amb les restriccions i realimentar el procés de disseny.
- Ara ja estem en disposició de dissenyar un pla específic.
- És important que tots els aspectes importants de la solució tècnica siguin testejats prèviament en el laboratori. Això ajudarà a refinar la solució.
- El disseny s'ha completat quan s'ha acabat de refinar completament.

1.5. Principis en el disseny de xarxa

A continuació resumim els principis clau que s'han de seguir per tenir èxit en el disseny de xarxa:

- Les aplicacions marquen els requeriments en el disseny. No es pot fer un bon disseny de xarxa si no s'entenen les característiques de les aplicacions.
- Cal provar els dissenys en el laboratori. Estan molt bé les eines de simulació, però la millor manera de comprovar un disseny de xarxa és testejant-lo en el laboratori. Aquí podrem resoldre detalls tècnics específics.
- No s'ha de plantejar el disseny d'una xarxa com a imatge de l'estructura corporativa.
- S'ha de procurar ser independent del venedor. Intentar no optar per solucions propietàries.
- S'ha d'intentar fer el disseny el més senzill possible. Complicar la solució en moltes ocasions només incrementa el cost i complica l'administració posterior.
- No s'ha de partir de models predefinits.

Independència del venedor

La independència del venedor és un principi molt interessant, però en moltes ocasions poc realista. Un cop et lligues amb un fabricant resulta complicat canviar, ja que el valor afegit que et donen els seus equips solen ser solucions propietàries.

- El disseny ha de ser prou robust perquè els canvis que hi pugui haver no facin modificar-lo tot. A la vegada, ha de ser prou flexible per a permetre canvis en l'estructura.
- Un aspecte bàsic per a un bon disseny és que cal que sigui previsible, consistent en rendiment, fiable i escalable.

1.6. Disseny IP

Com la majoria de dissenys de xarxa actuals estan muntats sobre IP, comentarem els elements principals que cal tenir en compte per a un disseny IP. No es pretén fer una explicació detallada d'aquests elements, sinó només explicar la importància de cadascun d'ells quan es vol fer un bon disseny lògic.

El pla de direccionament IP és bàsic per tenir èxit a l'hora de fer el disseny de xarxa. A continuació, veurem de forma molt breu els elements que cal tenir clars a l'hora de formular un pla de direccionament IP escalable que pugui suportar la xarxa, el seu creixement i els element clau.

1.6.1. Planificació d'adreces IP

Adreces públiques i privades

L'espai d'adreces IP està dividit en adreces públiques i privades. Les adreces privades estan reservades i només es poden utilitzar dintre de la xarxa interna de l'empresa però no a Internet. Així, aquestes adreces han de ser mapades per adreces públiques quan es vol sortir a Internet.

L'RFC 1918 (*address allocation for private Internets*) defineix els rangs següents d'adreces privades:

10.0.0.0 - 10.255.255.255.

172.16.0.0 - 172.31.255.255.

192.168.0.0 - 192.168.255.255.

criteris de selecció entre adreces privades i públiques

El nombre d'adreces IP públiques és petit, de manera que els proveïdors assignen poques IP als seus clients. En la majoria de casos és insuficient per a fer l'adreçament de totes les adreces de la xarxa.

La solució és treballar amb IP privades i traslladar-les a IP públiques quan sigui necessari. En el disseny de la xarxa cal tenir en compte les consideracions principals següents:

- Quins i quants dispositius han de sortir a l'exterior.
- Quins serveis requereixen, és a dir, si estan limitats els serveis o no. Els dispositius interns no han de ser visibles des de l'exterior.
- Quins dispositius (serveis normalment) han de ser visibles des de l'exterior. En aquests casos la IP no pot variar.

Interconnexió d'adreces privades i públiques

Com hem explicat, una empresa pot tenir adreces privades i públiques. Un encaminador o tallafocs actuarà d'interfície entre la xarxa privada i la pública.

El mecanisme per a traslladar les adreces privades a públiques pot ser per mitjà de NAT o PAT.

NAT és la sigla de network address translation.
PAT és la sigla de port address translation.

NAT permet que adreces IP no registrades o del rang d'adreces IP privades usades dintre de xarxes privades puguin tenir accés a la xarxa pública, com Internet.

L'encaminador que connecta la xarxa privada amb la xarxa pública usará el servei de NAT per a traslladar les adreces privades a adreces públiques registrades. Aquesta translació d'adreces pot ser estàtica o dinàmica.

Però NAT no solament és beneficiós per aquest motiu. Altres poden ser:

- Conservació d'adreces.
- Flexibilitat: possibilitat de canviar de proveïdor d'Internet sense haver de pensar a canviar les adreces de tota la nostra xarxa.
- Pot solucionar problemes de superposició d'adreces.
- Seguretat.

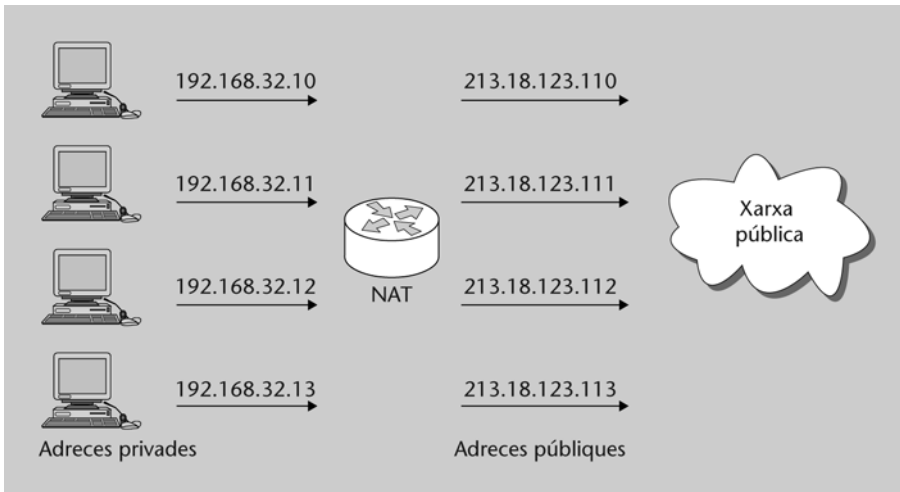
S'ha de tenir present, però, que també la implementació de NAT a la nostra xarxa pot comportar certs problemes. Alguns poden ser:

- Augment de la latència.
- Dificultats de monitoratge.
- Pèrdua de funcionalitats.

Hi ha diverses possibilitats a l'hora de fer el NAT:

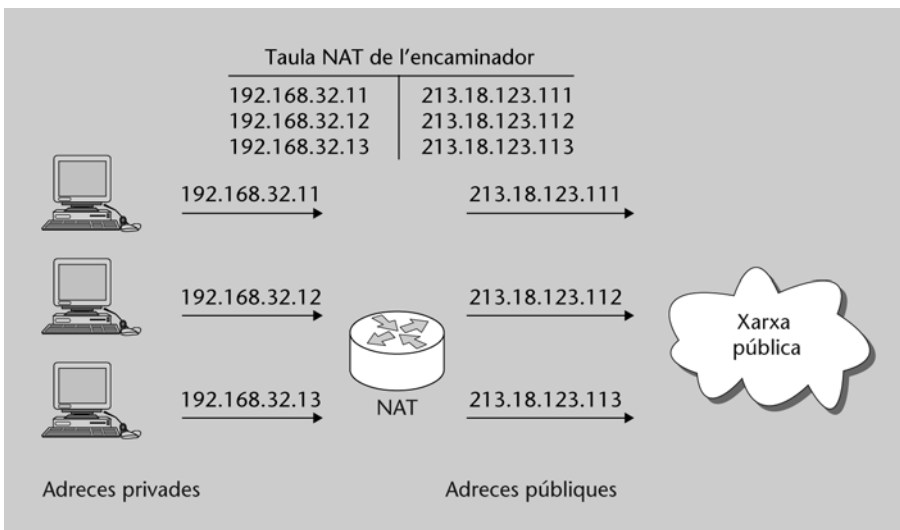
a) NAT estàtic: es fa un mapatge entre adreces de la xarxa interna amb adreces públiques en una relació d'un a un (figura 1).

Figura 1. NAT estàtic



b) **NAT dinàmic**: mapatge d'adreces privades a adreces públiques a partir d'un grup d'adreces públiques reservades per a sortir cap a l'exterior. Es van assignant les adreces públiques en funció de l'usuari que en necessita.

Figura 2. NAT dinàmic



c) **Overloading**: és una forma particular de NAT dinàmic en què múltiples usuaris de la xarxa privada surten a l'exterior amb una única IP pública. L'encaminador diferencia cada usuari a partir dels ports (UDP o TCP) que utilitza. Aquest mecanisme és conegut habitualment com a PAT.

Assignació d'adreces IP als dispositius. Adreces estàtiques i dinàmiques

Quan es vol fer un pla d'adreçament IP cal conèixer la mida de la xarxa per a poder establir el nombre de subxarxes i el nombre d'adreces IP per subxarxa. Per tant, cal tenir clar les localitzacions, el nombre de dispositius per localització i els requisits d'adreçament per a les localitzacions específiques.

Anem a veure l'efecte des del punt de vista administratiu del mecanisme d'assignació d'adreces IP als dispositius finals.

L'assignació d'adreces inclou donar una IP, una porta d'enllaç, servidors de DNS, etc. Per tant, cal tenir clara la resposta a una sèrie de preguntes, com ara:

- Quants dispositius necessiten IP?
- Quins dispositius requereixen IP estàtica?
- Hi pot haver canvis d'adreçament en el futur?
- L'administrador necessita fer un seguiment dels dispositius i les seves adreces IP?
- Hi ha requisits de disponibilitat?
- Hi ha requisits de seguretat?

Hi ha dues estratègies bàsiques per a assignar adreces:

a) Estàtic: s'assignen tant la IP com els possibles paràmetres associats de manera manual. Implica una sobrecàrrega per a l'administrador, sobretot en xarxes grans.

b) Dinàmic: s'assignen les IP de manera automàtica. Allibera d'aquesta tasca a l'administrador. Aquest el que fa és configurar un servidor que s'encarrega d'aquestes tasques. El protocol més comú és DHCP.

Quan usarem una estratègia o l'altra? Per a usar un tipus o l'altre o el dos cal tenir present les consideracions següents:

- **Tipus de node:** en general els dispositius com encaminadors, commutadors o servidors tenen IP estàtiques. Els dispositius finals (PC), IP dinàmiques.
- **Nombre de dispositius:** és preferible usar IP dinàmiques quan el nombre de dispositius és elevat.
- **Seguiment d'adreces:** si es vol poder fer un control (seguiment) de les adreces per polítiques de xarxa és millor usar adreces dinàmiques. Es pot fer amb DHCP configurant adequadament el servidor.
- **Paràmetres addicionals:** si cal configurar paràmetres addicionals és més senzill amb DHCP.
- **Alta disponibilitat:** la IP dinàmica depèn d'un servidor. Si volem que estigui sempre disponible caldrà tenir mecanismes de redundància.

1.6.2. Subxarxes amb màscara de longitud variable (VLSM)

Una subxarxa permet crear xarxes més petites a partir de l'assignació inicial per classes. Si fem això hem de definir un nou paràmetre, que anomenem màscara. La màscara ens permet saber en aquesta nova assignació quants bits representen la xarxa creada i quants el *host* concret dintre de la mateixa.

IP amb classe. Les adreces IP es poden classificar en classe A, B, C.
 Classe A: 8 bits part de xarxa, 24 bits part de *host*. Bit de més pes = 0
 Classe B: 16 bits part de xarxa, 16 bits part de *host*. Bits de més pes = 10
 Classe C: 24 bits part de xarxa, 8 bits part de *host*. Bits de més pes = 110

Subxarxa amb màscara de longitud variable significa la implementació de subxarxes amb màscares diferents provinent de la mateixa adreça de xarxa basada en classe.

Aquesta possibilitat permet un ús més eficient de l'espai d'adreces IP, tant en termes de subxarxes possibles com de dispositius per subxarxa. És bàsic en xarxes on es disposa de rangs petits d'adreces IP. Lligat a VLSM cal que hi hagi un protocol d'encaminament que suporti VLSM. Aquests protocols d'encaminament s'anomenen protocols d'encaminament sense classe i el que fan és que quan es genera informació de les noves rutes (xarxes) s'hi incorpora la màscara associada a cadascuna d'aquestes xarxes.

Alguns exemples de protocols sense classe són RIPv2, OSPF, IS-IS i BGP.

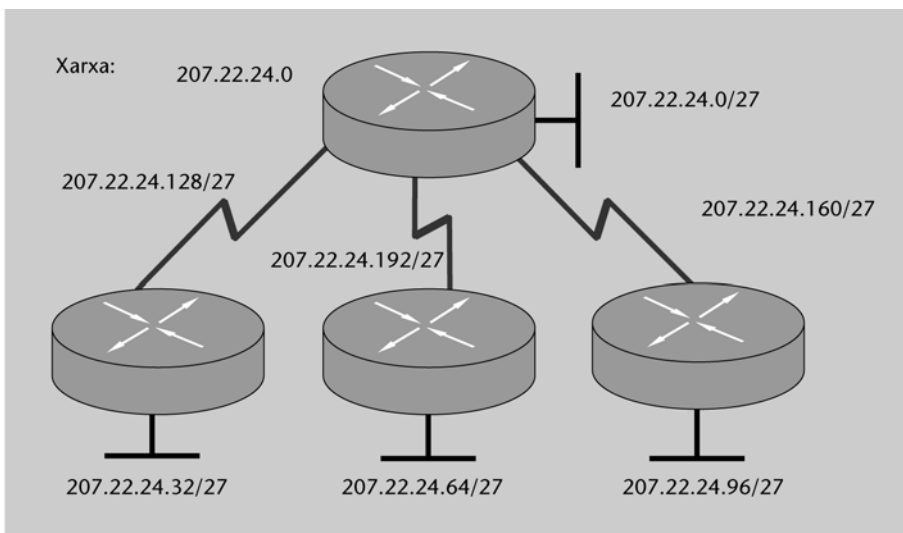
Exemple de subnetting

A continuació, es mostra un exemple de *subnetting* on donada l'adreça de xarxa de classe C, 207.22.24.0, hi apliquem una màscara de 27 bits i queda de la manera següent:

Subxarxa 0	207.22.24.0/27
Subxarxa 1	207.22.24.32/27
Subxarxa 2	207.22.24.64/27
Subxarxa 3	207.22.24.96/27
Subxarxa 4	207.22.24.128/27
Subxarxa 5	207.22.24.160/27
Subxarxa 6	207.22.24.192/27
Subxarxa 7	207.22.24.224/27

Aquest exemple el podríem aplicar directament a la xarxa de la figura 3, on tenim set xarxes diferents. Podem imaginar que és una empresa amb una seu central i tres subseus connectades entre elles a través de línies WAN punt a punt (tres en total). Cada seu a la vegada disposa de la seva xarxa Ethernet. Si ens hi fixem, aquesta empresa està formada per un total de set subxarxes. Aprofitant el *subnetting* de l'exemple anterior quedaria com es mostra a la figura 3.

Figura 3. Topologia amb *subnetting*



Divisió en classes de l'espai d'adreces IP

L'espai d'adreces IP està dividit inicialment en classes. Classe A, B i C bàsicament. En funció de la classe podem saber quina part de l'adreça representa en la xarxa i quina en l'equip concret de la mateixa xarxa.

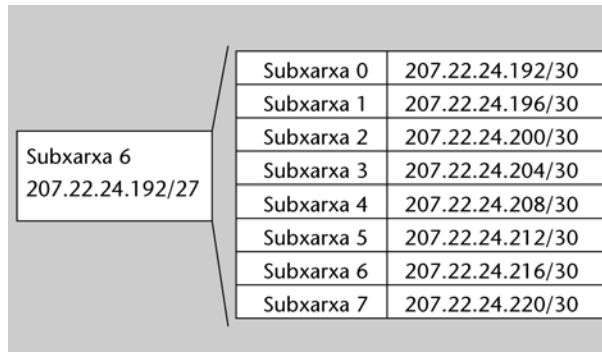
Subnetting

A partir d'una adreça amb classe el *subnetting* ens permet fer xarxes més petites totes amb la mateixa màscara (màscara de longitud fixa).

Si ens fixem amb la solució adoptada, el que tenim és que hem assignat un rang de 30 adreces per a cadascuna de les subxarxes. Aquest rang pot ser correcte per a les xarxes Ethernet, però és totalment ineficient per a les línies WAN, que només necessiten dues adreces (una per a cada extrem de la connexió).

Una solució molt més adequada per a aquesta empresa seria el fet d'aplicar VLMS. Aplicant VLSM podem fer una subxarxa d'una de les subxarxes anteriors com mostra la figura 4.

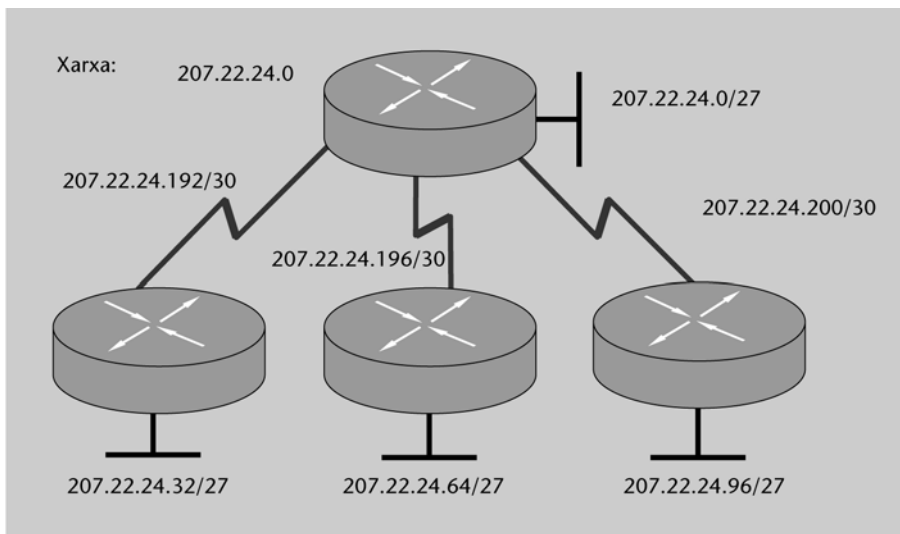
Figura 4. Exemple de VLSM



Aquestes subxarxes es podrien usar per a fer l'adreçament en una xarxa WAN dels diversos enllaços punt a punt que pugui tenir, que només necessiten dues adreces IP, una per a cada punt de l'enllaç.

En el nostre cas concret el *subnetting* final quedaria com es mostra a la figura 5.

Figura 5. Topologia aplicant VLSM



Hem aconseguit alliberar uns rang d'adreces que ens poden ser útils en cas que l'empresa creixi.

1.6.3. Sumarització de rutes

La sumarització de rutes és la possibilitat d'agrupar una sèrie de rutes perquè es puguin anunciar com una de sola. El resultat d'aquesta sumarització és la reducció de la mida de les taules d'encaminament als nodes de la xarxa.

Aconsegüim entre altres efectes reduir el temps de latència associat en la cerca en les taules d'encaminament cada cop que arriba un paquet IP.

Un altre aspecte aconseguit amb la sumarització és que millorem l'estabilitat de la xarxa, ja que la caiguda puntual d'algun enllaç no es propaga per tota la xarxa

Usos de la sumarització de rutes

La sumarització és molt interessant per a xarxes molt grans. A Internet la sumarització ha permès que els encaminadors troncal continuïn funcionant, ja que se n'han reduït les taules d'encaminament.

fent recalcular les taules de tots els encaminadors, és a dir, evitem actualitzacions d'encaminament innecessàries i fem que la convergència sigui més ràpida.

Per poder fer la sumarització de rutes és vital que l'esquema de direccionament IP es faci de manera que permeti aquesta sumarització i, per tant, és un element estratègic en el disseny de la xarxa WAN. Els rangs d'adreces han d'estar formats per blocs contigus.

Vegem un parell d'exemples de sumarització. En el primer explicarem la mecànica del mateix. En el segon cas veurem com s'aplica en una topologia de xarxa completa.

Exemple de sumarització

Suposem que tenim les adreces consecutives que es veuen en la taula següent. Sense sumarització l'encaminador ha de mantenir entrades individuals per a cadascuna de les xarxes de la taula.

Adreces classe B consecutives				
Adreça	Primer octet	Segon octet	Tercer octet	Quart octet
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

En la taula anterior en negreta tenim la part corresponent a xarxa per a cada adreça. Si apliquem sumarització el que fem és mirar dintre de la part de xarxa quins bits són comuns per a totes elles. Així, en la taula següent es veu en negreta la part de xarxa comuna.

Adreces classe B consecutives. 13 bits comuns				
Adreça	Primer octet	Segon octet	Tercer octet	Quart octet
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000

Adreces classe B consecutives. 13 bits comuns				
Adreça	Primer octet	Segon octet	Tercer octet	Quart octet
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

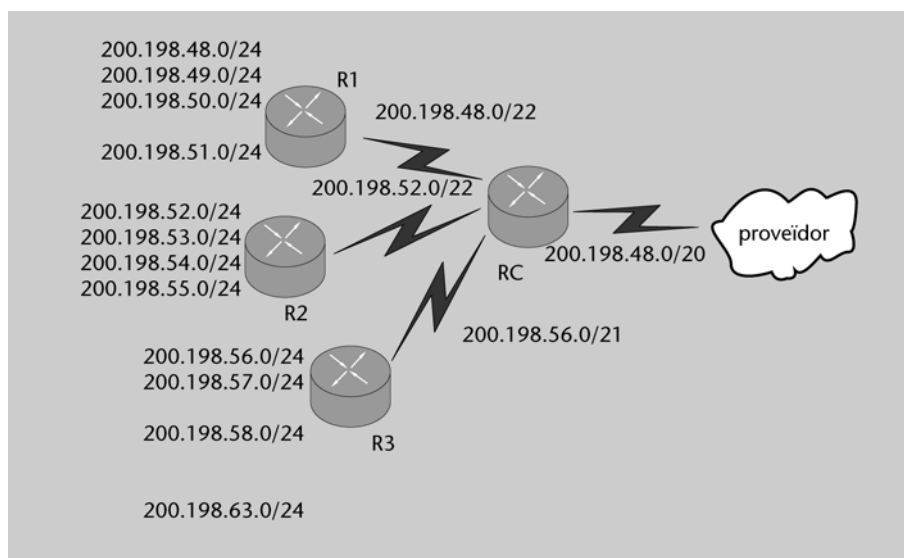
D'aquesta manera, l'encaminador pot sumaritzar aquestes vuit adreces amb una adreça única amb un prefix de 13 bits: 1010110000011

Obtenim l'adreça sumaritzada: 172.24.0.0/13

Exemple de sumarització aplicada a topologia de xarxa completa

En la figura 6 es mostra una topologia concreta on un proveïdor de xarxa té un encaminador (RC) al qual estan connectats diversos encaminadors d'accés (poden ser per exemple clients). Aquest és un exemple on és interessant fer sumarització.

Figura 6. Sumarització de rutes



En la figura 6 la ruta sumaritzada que arriba al proveïdor conté un prefix de 20 bits comú a totes les xarxes que arriben a RC: 200.199.48.0 /20 o 11001000 11000111 0001.

En aquest cas, les taules d'RC se simplifiquen pel fet d'arribar-hi sumaritzades pels encaminadors d'accés i a la vegada RC quan envia les actualitzacions al proveïdor (als encaminadors que estan al nucli de la seva xarxa) li envia una única ruta. La sumarització de rutes, per tant, redueix la mida de les taules d'encaminament fent agregació de rutes de múltiples xarxes en una única superxarxa.

D'altra banda, perquè la sumarització funcioni correctament cal tenir cura a l'hora de fer l'assignació d'adreces de forma jeràrquica per tal de poder fer després l'agregació.

Planificació d'un adreçament IP jeràrquic

Una bona planificació IP farà que tinguem una solució d'encaminament millor o pitjor. Com sabeu, les adreces IP tenen un esquema d'adreçament jeràrquic en què les adreces estan dividides en part de xarxa (prefix) i part d'amfitrió. Els encaminadors prenen les decisions en funció del prefix i el salt següent per fer, és a dir, el node següent al qual cal passar el datagrama sense necessitat de conèixer els detalls per a arribar a la destinació.

Beneficis d'un adreçament jeràrquic

Com s'ha explicat, l'adreçament IP es fa en funció de la mida, la localització geogràfica i la topologia de la xarxa. En xarxes grans, un adreçament jeràrquic és bàsic, fins i tot perquè les taules d'encaminament dels encaminadors siguin estables.

Així, una bona planificació afectarà en el següent:

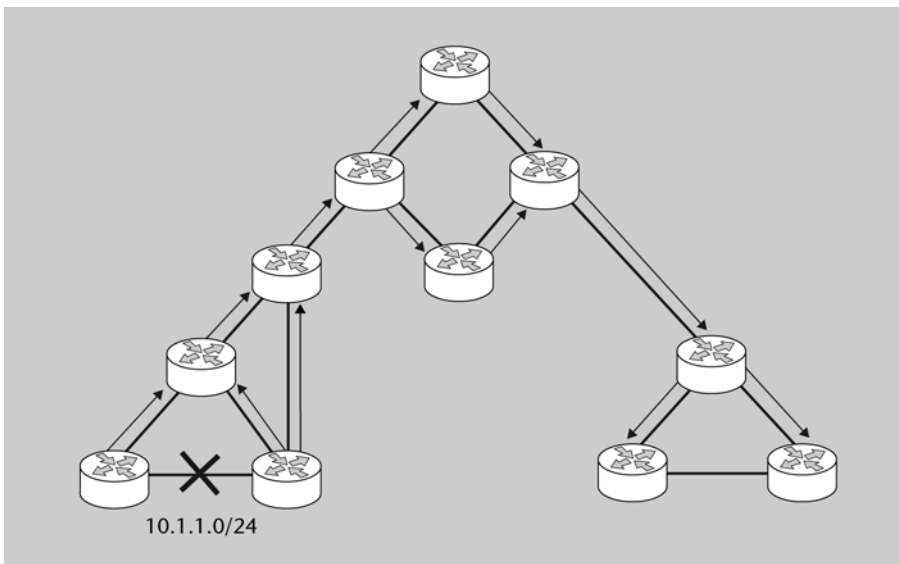
- **Encaminament.** Una bona planificació IP pot millorar l'estabilitat d'encaminament, la disponibilitat del servei, l'escalabilitat i la modularitat de la xarxa.
- **Disseny modular i escalable.** Permet l'agregació d'encaminament sense afectar el disseny existent.
- **Agregació de rutes.** Redueix les taules d'encaminament i millora l'estabilitat i l'escalabilitat. Per a fer-ho, cal dividir la xarxa en grups IP que siguin contigus.

Impacte d'un disseny IP dolent

És el cas que l'assignació d'adreces IP s'hagi fet en funció del creixement de la xarxa, el repartiment d'IP és aleatori i, per tant, sense crear grups o sumarització. Això provoca que no es pugui dividir la xarxa en grups d'adreces contigus i no puguem implementar la sumarització de rutes.

L'exemple típic de l'impacte d'un disseny dolent és quan tenim una xarxa amb encaminament dinàmic i un dels enllaços va canviant d'estat periòdicament (figura 7). Com que usem encaminament dinàmic, cada cop que hi hagi un canvi d'estat a l'enllaç, aquest es propagarà per tota la xarxa a la vegada que farà actualitzar les taules d'encaminament de tots els encaminadors.

Figura 7. Un adreçament incorrecte pot provocar un excés de trànsit d'encaminament



Alguns dels efectes que provoca un disseny dolent són:

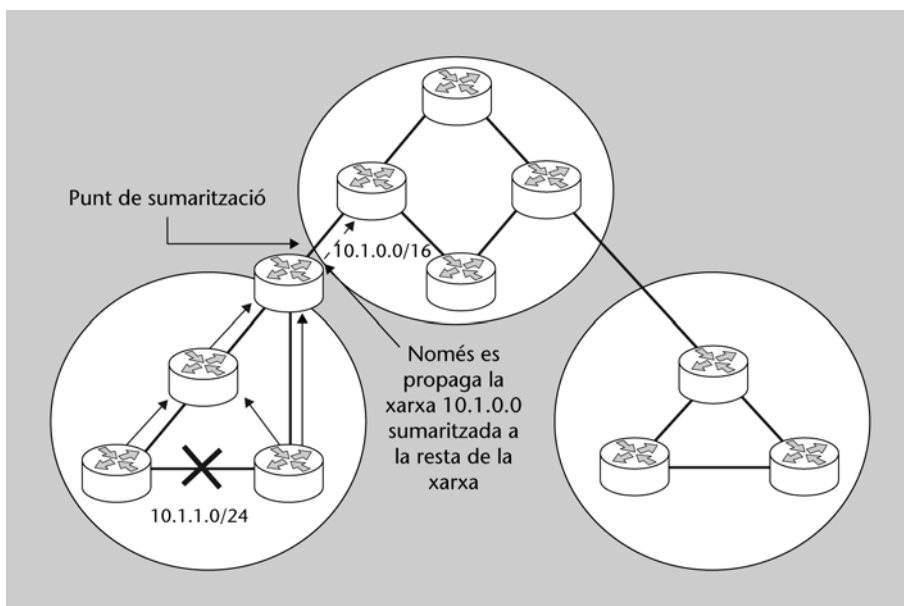
L'excés de trànsit d'encaminament consumeix amplada de banda. Quan hi ha un canvi en una ruta, els encaminadors s'envien actualitzacions. Sense sumarització hi ha més actualitzacions i més consum d'amplada de banda.

Augment del nombre d'actualitzacions en els encaminadors. Afectarà el rendiment dels encaminadors.

Beneficis de l'agregació de rutes

La implementació d'agregació de rutes en els nodes frontera entre àrees d'adreces contigües controla la mida de les taules d'encaminament. A la figura hi ha un exemple del que acabem d'explicar.

Figura 8. Un adreçament jeràrquic permet distribuir només les rutes sumaritzades



En aquest cas si un enllaç dintre d'una àrea cau, aquest no es propaga a la resta de la xarxa, ja que només s'envia una ruta sumaritzada i, per tant, no es veu reflectit el canvi. La informació de la ruta que ha fallat es propaga només dintre de l'àrea. Aconsegüim, per tant, reduir el consum d'amplada de banda associat a l'actualització d'encaminadors entre veïns, i a més disminueix el nombre de càlculs que ha de fer l'encaminador cada cop que rep una nova actualització.

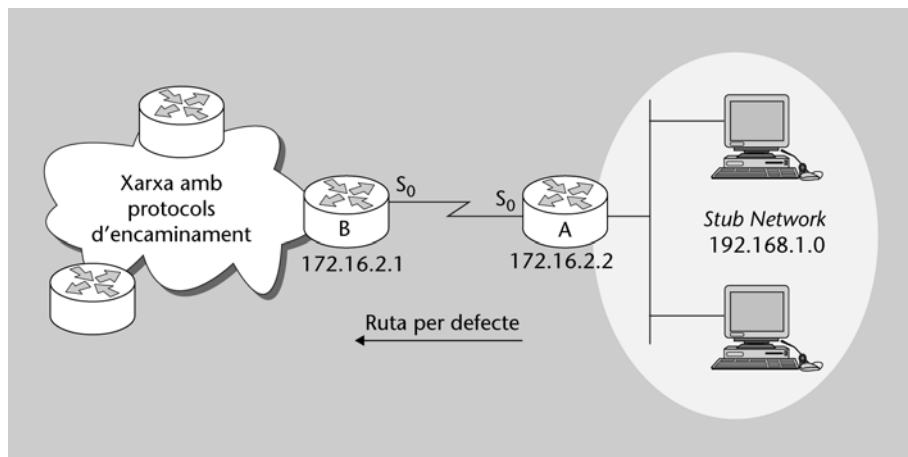
1.6.4. Conceptes sobre l'encaminament IP

Hi ha dues maneres de configurar l'encaminament, cadascuna amb els seus avantatges i inconvenients:

1) **Encaminament estàtic.** Apropiat en les circumstàncies següents:

- Enllaços amb molta baixa velocitat en què no sigui desitjable enviar actualitzacions d'encaminament.

- En cas que l'administrador necessiti control absolut sobre les rutes.
- Quan només hi ha una ruta d'accés a la resta de la xarxa (**stub network**).
A la figura següent es mostra aquesta situació.

Figura 9. *Stub network*

Cal tenir present que configurar i mantenir rutes estàtiques implica temps, i a més requereix un coneixement complet de tota la xarxa.

2) **Encaminament dinàmic.** Permet a la xarxa ajustar els canvis de la topologia als canvis de la xarxa de manera automàtica. Una ruta estàtica no pot respondre de manera dinàmica als canvis de la xarxa. Això és evident en el cas que tinguem caigudes de les línies o que afegim línies noves, i pot fer que l'administrador hagi de dedicar molt de temps i esforç a aquests canvis.

Què demanem que compleixin els protocols d'encaminament?

- Trobar fonts que els proporcionin informació d'encaminament; normalment els encaminadors veïns.
- Seleccionar el millor camí en funció de la informació rebuda.
- Mantenir la informació d'encaminament.
- Tenir mecanismes que permetin verificar i actualitzar aquesta informació.

Els principals protocols d'encaminament actuals es mostren a la taula següent:

Protocols d'encaminament IP	
Categoria	Protocol d'encaminament
Vector-distància	RIPv1, RIPv2
Estat-enllaç	OSPF, IS-IS
Híbrid	EIGRP

Característiques del protocol d'encaminament

A continuació comentarem les diverses característiques que avaluen els diversos protocols. Aquestes característiques ens han de permetre fer la millor elecció del protocol en funció de la nostra topologia i les nostres necessitats concretes:

- **Estabilitat.** El protocol d'encaminament ha de ser estable contra bucles d'encaminament, que poden perjudicar la xarxa en cas que es generin actualitzacions cada cop que hi hagi fluctuacions en algun enllaç.
- **Velocitat de convergència.** Quan hi ha un canvi en la topologia, com pot ser supressió o inclusió d'una subxarxa, transcorre un temps abans que tots els encaminadors tenen coneixement d'aquest canvi. Durant aquest interval de temps, anomenat temps de convergència, alguns encaminadors operen amb informació inconsistent.
- **Mètrica.** L'encaminador escull la mètrica com a mecanisme per a determinar el millor camí per a arribar a una destinació determinada. Cada protocol usa una mètrica diferent, és a dir, cada protocol usa un mecanisme diferent per a determinar quin és el millor camí.
- **VLSM.** Ja hem parlat en l'apartat anterior de VLSM. Els protocols d'encaminament sense classe suporten VLSM, ja que incorporen la màscara de les xarxes en les seves actualitzacions.
- **Sumarització de rutes.** Igual que en el cas anterior, la sumarització de rutes ja ha estat explicada i com s'ha vist és imprescindible per a xarxes amb creixement que el protocol suporti la possibilitat de configurar sumarització de rutes.
- **Protocols amb classe o sense classe.** La diferència entre un protocol d'encaminament amb classe i un sense classe és senzilla. Els protocols sense classe incorporen la màscara en les seves actualitzacions, mentre que els altres no ho fan. Aquesta diferència és bàsica perquè implica que els protocols amb classe no suporten VLSM, xarxes discontinües o la possibilitat de configurar sumarització de rutes. Es pot dir que aquests protocols no són adequats per a les xarxes modernes.
- **Escalabilitat.** L'escalabilitat està relacionada amb la possibilitat de creixement de la xarxa IP. Així, l'escalabilitat porta associada aspectes comentats, com són la possibilitat de sumarització o velocitat de convergència. També són importants els mecanismes utilitzats per a informar de les actualitzacions.

Un cop vistes les característiques principals vegem un parell de protocols que són actualment bàsics per a les xarxes modernes: *l'open shortest path first* i el *border gateway protocol*.

Protocol RIP

Un protocol d'encaminament molt conegut i àmpliament utilitzat és el protocol RIP. Aquest protocol és un protocol amb classe i, per tant, és un protocol que no escala de forma adequada.

Adreça recomanada

Podeu trobar una descripció del protocol RIP a http://es.wikipedia.org/wiki/RIP_%28protocolo%29.

Open shortest path first

Open shortest path first (OSPF) és un protocol d'estat enllaç, és a dir, que el que envia són les actualitzacions de l'estat dels enllaços. És un protocol estandaritzat per Internet Engineering Task Force i està pensat per a xarxes escalables. Està descrit en diversos RFC, el més recent dels quals és RFC 2328. El primer objectiu del protocol és reduir la freqüència d'actualització del trànsit. Un segon objectiu és la ràpida convergència. L'inconvenient d'aquests dos objectius és el major consum de recursos de memòria i CPU en comparació amb els encaminadors que treballen amb protocols de vector-distància.

Els protocols d'encaminament

Els protocols d'encaminament es poden classificar de dues maneres: per la classe (amb classe o sense classe) i per si són protocols que treballen amb vector distància o amb estat enllaç.

Protocols d'encaminament vector distància o estat enllaç

Recordeu que els protocols d'encaminament es poden classificar com vector distància o estat enllaç. Aquesta classificació descriu l'algorisme que usen els encaminadors per a calcular l'intercanvi d'informació d'encaminament. Els encaminadors que treballen amb vector distància normalment envien les seves taules d'encaminament completes als encaminadors veïns a intervals regulars de temps.

La capacitat d'escalabilitat d'OSPF s'aconsegueix a través d'un disseny jeràrquic. Podem dividir la xarxa OSPF en múltiples àrees, la qual cosa permet un major control de les actualitzacions d'encaminament. Fer un bon disseny de la xarxa en àrees permet a l'administrador reduir la sobrecàrrega de paquets d'encaminament i millorar el rendiment dels encaminadors.

Així, les característiques més importants del protocol són les següents: 


- Velocitat de convergència. En xarxes grans RIP pot trigar uns minuts en convergir, ja que tota la taula d'encaminament de cadascun dels encaminadors es copia i comparteix amb els encaminadors veïns directament connectats. Amb OSPF la convergència és més ràpida, ja que només s'envien entre encaminadors OSPF els canvis d'encaminament.
- Suporta VLSM. RIPv1 és un protocol amb classe i no suporta VLSM. OSPF com a protocol sense classe suporta VLSM.
- Mida de la xarxa. En entorns RIP, si una xarxa és a més de 15 salts es considera que no s'hi pot accedir. Aquesta restricció limita l'ús de RIP a topologies petites. OSPF no té aquesta limitació i per tant està pensat per a xarxes mitjanes i grans.
- Ús de l'amplada de banda. RIP envia actualitzacions als seus veïns de totes les seves taules en forma de *broadcast* cada 30 segons. És especialment problemàtic en enllaços WAN de baixa velocitat, ja que les actualitzacions consumeixen amplada de banda. OSPF només envia actualitzacions quan es produeixen canvis.
- Selecció del camí. RIP selecciona la millor ruta en funció del nombre de salts sense tenir en compte altres factors, com ara retard de la línia, amplada

de banda, etc. OSPF busca la millor ruta en funció d'un paràmetre anomenat cost que calcula a partir de l'amplada de banda de la línia.

- Agrupació de membres. RIP usa una topologia plana, de manera que tots els encaminadors formen part de la mateixa xarxa. Així, els canvis han de viatjar per tota la xarxa. OSPF utilitza un concepte anomenat àrea i crea grups d'encaminadors. Això fa que la comunicació dels canvis es faci dintre de l'àrea sense que afecti la resta d'àrees. Amb això aconseguim que el rendiment d'una àrea no afecti la resta d'àrees.

Border gateway protocol


Quan mirem Internet des de la perspectiva de l'usuari apareix com una col·lecció de recursos als quals pots accedir a través de l'ISP. L'estructura de la topologia d'Internet, els processos que permeten la comunicació entre les diferents entitats de tot el món, són irrellevants des del punt de vista de l'usuari. En canvi, si el que volem és entendre el funcionament del protocol BGP és útil tenir unes nocions sobre la topologia Internet i la comunicació entre diferents empreses.

Una *Internetwork* és un grup de xarxes més petites que són independents. Cadascuna d'aquestes petites xarxes poden ser propietat i operar per a diferents organitzacions, com ara universitats, empreses o altres grups. Per tant, no sorprèn que qui opera amb aquestes xarxes vulgui autonomia, administració pròpia amb els seus propis sistemes. En moltes ocasions, l'encaminament i les polítiques de seguretat d'una organització poden entrar en conflicte amb les polítiques d'altres. Així Internet està dividida en dominis o sistemes autònoms. Cada sistema autònom representa una organització independent on aplica la seva política d'encaminament i seguretat. 

Els protocols anomenats EGP faciliten l'intercanvi d'informació d'encaminament entre sistemes autònoms.

Es pot definir que un sistema autònom està format per un grup d'encaminadors que comparteixen polítiques d'encaminament similars i operen dintre d'un mateix domini administratiu. Un sistema autònom pot ser un grup d'encaminadors corrent tots un mateix protocol IGP o poden ser una col·lecció d'encaminadors corrent diferents protocols però que pertanyen a una mateixa organització. En qualsevol dels casos, des del món exterior el sistema autònom es veu com una única entitat.

Els sistemes autònoms queden identificats per un número assignat per un registre d'Internet o per un operador de serveis entre els valors 1 i 65535. Actualment, el protocol BGP4 és el protocol estàndard en el món d'Internet d'encaminament entre sistemes autònoms.

En general, Internet és una col·lecció arbitrària de sistemes autònoms. Els protocols EGP s'usen per a comunicar sistemes autònoms, mentre que dintre dels sistemes autònoms el seu ús és irrellevant. 

Una empresa que vulgui usar BGP per a intercanviar informació de direccionament amb l'ISP ha de tenir el seu número d'AS. La connexió entre un encaminador d'un sistema autònom i un altre encaminador d'un altre sistema autònom s'anomena connexió BGP externa (*external BGP*).

Els encaminadors que parlen BGP entre ells es comuniquen sobre una sessió entre iguals (*peer*). Els encaminadors que formen la parella s'anomenen veïns (*neighbors*).

Un cop s'estableix la comunicació entre encaminadors amb una sessió BGP s'envien actualitzacions que inclouen rangs d'adreces sumaritzades i el número d'AS corresponent. Els missatges BGP s'envien en una connexió TCP a través del port 179.

A diferència dels protocols que treballen amb mètriques a BGP una ruta no és una xarxa o una subxarxa, sinó que és una informació que té el parell destinació i atributs de camí.

Mètriques

Les mètriques són els valors que utilitzen els protocols d'encaminament per a decidir el millor camí fins a una destinació.

Els protocols d'encaminament basen les seves mètriques en mesures diferents, com són el nombre de salts, la velocitat de l'enllaç, el retard o altres mètriques més complexes. La majoria de protocols d'encaminament incorporen bases de dades que contenen totes les xarxes que el protocol d'encaminament reconeix i tots els camins per a cada xarxa. Si el protocol reconeix més d'un camí per a arribar a la xarxa de destinació, compara la mètrica de cada camí i agafa el de mètrica menor.

Així, tenim protocols amb mètriques molt senzilles, com són RIPv1 i RIPv2, amb mètrica de nombre de salts. N'hi ha d'altres més complexos, com el protocol EIGRP.

Exemple. Càlcul de la mètrica del protocol EIGRP

EIGRP calcula la seva mètrica per mitjà de pesos en diferents característiques de la línia des de l'origen fins a la destinació. L'expressió és la següent:

Mètrica = $(k1 \times \text{amplada_de_banda}) + (k2 \times \text{amplada_de_banda}) / (256 - \text{càrrega}) + (k3 \times \text{retard})$

Hi ha un paràmetre k_5 ; si és diferent de 0, llavors l'expressió queda:

$$\text{Mètrica} = \text{mètrica} \times k_5 / (\text{fiabilitat} + k_4)$$

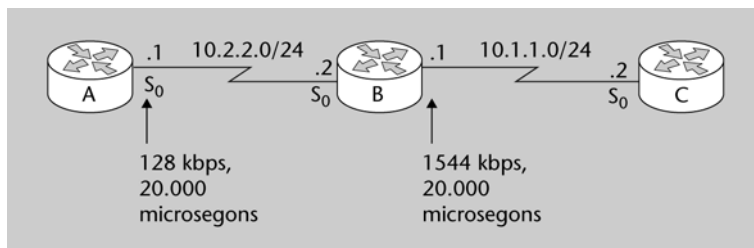
En general $k_1 = k_3 = 1$ i $k_2 = k_4 = k_5 = 0$.

En aquest cas l'expressió és:

$$\text{Mètrica} = \text{amplada_de_banda} + \text{retard}$$

L'amplada de banda es calcula agafant l'amplada de banda del pitjor enllaç entre origen i destinació en kbps. Llavors es divideix 10^7 per aquest valor i el resultat es multiplica per 256. El retard és la suma de retards en microsegons multiplicat per 256.

Figura 10. Topologia d'exemple de càlcul de la mètrica EIGRP



Anem a calcular la mètrica que obtindrà l'encaminador A de la xarxa 10.1.1.0 en l'exemple de la figura anterior:

a) L'encaminador B enviarà l'actualització de la xarxa 10.1.1.0 a l'encaminador A amb la mètrica següent:

- $\text{Amplada_de_banda} = (10000000/1544) \times 256 = 1658031$
- $\text{Retard} = (20000/10) \times 256 = 512000$
- $\text{Mètrica} = 2170031$

b) L'encaminador A calcula la seva mètrica de 10.1.1.0 i posa el següent a la seva taula d'encaminament:

- $\text{Amplada_de_banda} = (10000000/128) \times 256 = 20000000$ (considerant l'amplada de banda menor dels dos enllaços)
- $\text{Retard} = ((20000 + 20000)/10) \times 256 = 1024000$
- $\text{Mètrica} = 21024000$

Convergència dels protocols d'encaminament

Sempre que es produeix un canvi en la topologia de la xarxa, tots els encaminadors han d'aprendre la nova topologia. Aquest procés és a la vegada col·laboratiu i independent. Els encaminadors han de compartir informació entre ells, però han de calcular l'impacte del canvi de topologia de manera independent.

Es considera que la xarxa ha convergit quan totes les taules d'encaminament estan sincronitzades i cadascuna conté una ruta correcta cap a totes les xarxes de destinació.

Les propietats de convergència inclouen la velocitat de propagació de la informació d'encaminament i el càlcul del millor camí. Com més ràpida és la convergència, el protocol d'encaminament és millor.

2. Xarxes metropolitanes

En aquest apartat veurem les característiques principals de les xarxes metropolitanes, la seva evolució en els últims anys i les noves tecnologies que estan emergint a causa dels nous serveis i necessitats dels clients. Introduïrem Ethernet com una tecnologia de connectivitat dintre de la xarxa metropolitana i descriurem les diverses tecnologies que es poden usar sobre la infraestructura Ethernet, a la vegada que inclourem la integració amb les tecnologies ja existents, com SDH/SONET o tecnologies emergents com “l’anell de paquets fiable” (RPR).

2.1. Les xarxes metropolitanes

La xarxa metropolitana *metropolitan area network* (MAN) és un tipus de xarxa que sempre s’ha classificat com una xarxa que està entre LAN i WAN. Una xarxa MAN pel fet de tenir ordres de magnitud cobriria una àrea que pot anar de 5 a 50 km, encara que aquests valors són sempre relatius. !

LAN: local area network. WAN: wide area network.

La xarxa metro és el primer tram de la xarxa que connecta usuaris finals i empreses a la xarxa WAN. La part de xarxa metro que arriba a l’usuari final s’anomena “l’última milla”, per tal d’indicar que és l’últim tram de la xarxa portadora.

El concepte de MAN no és nou. Sorgeix al voltant dels anys noranta. En aquella època els anells TDM (*time division multiplexing*) formaven la xarxa MAN amb amplificadors òptics per a complir els objectius de distància. A mitjan anys noranta va ser ATM la tecnologia dominant en les xarxes MAN, pel fet que hi havia la promesa que ATM seria la tecnologia que permetria la convergència de dades, veu i vídeo. A més, ATM permetia usar ATM per sobre de l’anell SDH. El problema va ser el fet que mentre SDH va anar incrementant la seva estructura, ATM no va aconseguir introduir-se com la solució usada per l’usuari final.

Si mirem en perspectiva la xarxa metro es pot veure que està bàsicament dividida en tres parts:

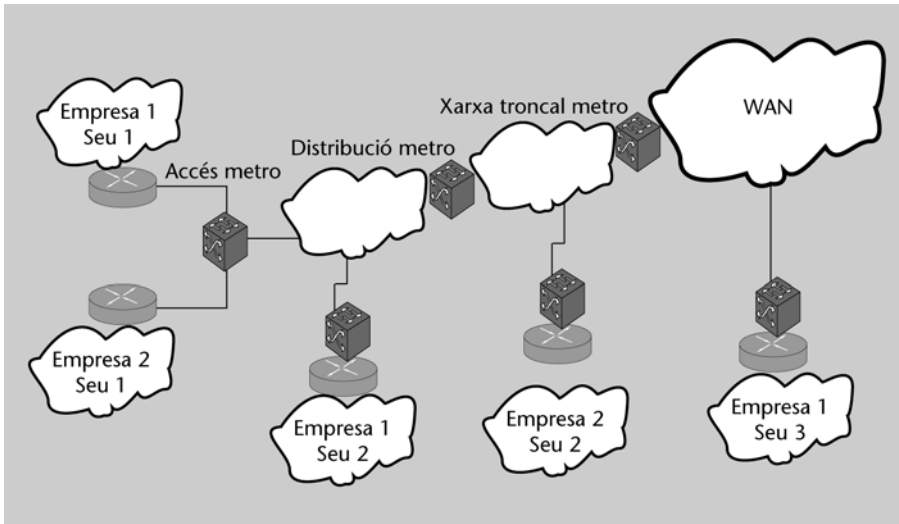
1) **Accés metro** (*access metro*). Aquests segment constitueix l’última milla, la qual, com sabeu, és la part que tocaria a l’usuari final.

2) **Distribució metro** (*metro edge*). Aquest segment constitueix el primer nivell de l’agregació metro. Les connexions que surten dels edificis són agregades a la CO en connexions més grans que successivament són transportades a través de la xarxa metro o la xarxa WAN.

CO: oficina central

3) **Xarxa troncal (metro core).** Aquest segment constitueix el segon nivell d'agregació, on les CO llindar són agregades en una CO central. A la vegada, les CO centrals es connecten amb unes altres de manera que formen una xarxa troncal metro des d'on el trànsit és enviat a través de la WAN.

Figura 11. Topologia de la xarxa metro



2.1.1. Nous requeriments de les xarxes metropolitanes

L'evolució que han tingut les xarxes metropolitanes ha estat lligada a una sèrie de nous requeriments que s'han demanat a la xarxa:

- **Augment del trànsit de dades i connectivitat de banda ampla.** Potser el repte dominant en entorns MAN és l'increment exponencial de trànsit enviat a la xarxa, atès majoritàriament a l'explosió en l'ús d'Internet en tots els entorns. A més de l'increment en nombre d'usuaris, la mateixa naturalesa de les aplicacions Internet cada cop requereixen més amplada de banda.
- **Convergència i serveis heterogenis.** Un altre factor clau que ha marcat quina ha de ser l'evolució de les xarxes MAN és la convergència de serveis. Les infraestructures tradicionals MAN van ser creades i optimitzades per transportar trànsit de veu, sense preveure la possibilitat que sorgissin noves necessitats relacionades amb les dades.
- **Expansió de la capacitat de la fibra.** Un altre aspecte ha estat l'increment de la capacitat de la fibra. De la mateixa manera, quan es fan infraestructures se solen tirar més fibres del que es necessita i, per tant, hi ha fibra infrautilitzada.

Un aspecte relacionat amb fibra, encara que no sigui físicament, és l'increment de capacitat que ofereix el multiplexat per longitud d'ona (WDM). WDM actualment suporta fins a quaranta canals en una fibra i té la capacitat de suportar-ne fins a vuitanta per fibra.

WDM

WDM (*wavelength division multiplexing*) és una tecnologia que permet multiplexar diversos senyals sobre una fibra òptica mitjançant portadores òptiques de diferents longituds d'ona usant llums procedents d'un làser o un LED.

2.1.2. Reptes i oportunitats per als proveïdors de serveis

Els nous requeriments en les xarxes MAN descrites a l'apartat 2.1.1 donen als operadors de serveis importants oportunitats competitives, que no estan lligades a les antigues infraestructures. Fins fa pocs anys, els usuaris corporatius estaven en mans dels proveïdors de serveis de telecomunicacions tradicionals per moure dades a través de la xarxa MAN, ja que havien de llogar circuits mantinguts pels proveïdors. A més del temps d'aprovisionament o taxes que s'havien de pagar un funció del trànsit sol·licitat calia afegir la redundància en capçaleres necessària per passar d'Ethernet en la xarxa LAN als protocols de xarxa MAN.

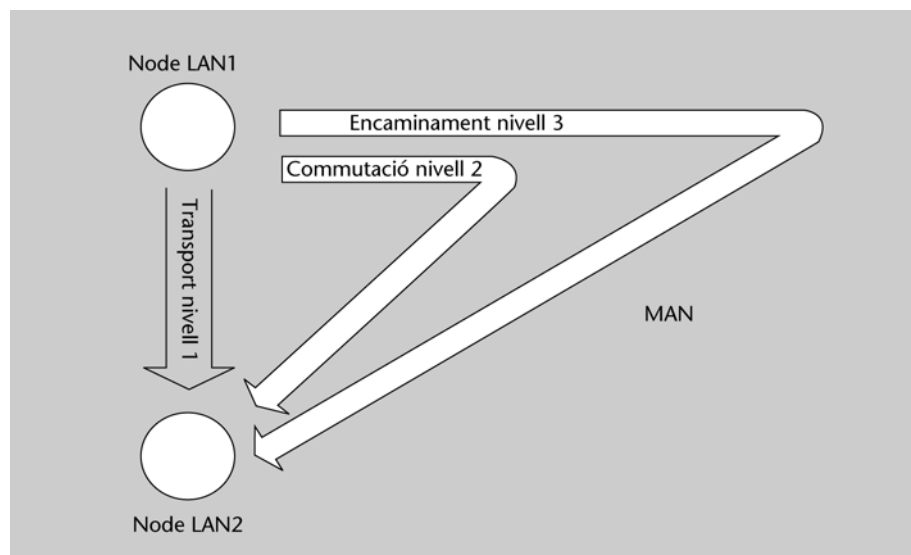
Per al client és més còmode, evidentment, poder estar connectat a la xarxa MAN i usar protocols que siguin compatibles a les dues xarxes.

Per tant, per als proveïdors de serveis MAN sorgeix una oportunitat si ofereixen noves xarxes amb serveis convergents basats en les capacitats que pot oferir Ethernet.

Des del punt de vista del mercat cal tenir clar el següent:

- Capa òptica de transport: transporta sempre que puguis.
- Capa de commutació Ethernet: commuta quan ho hagi de fer.
- Capa d'encaminament IP: encamina si no queda una altra alternativa.

Figura 12. Entorn d'aplicació de cadascuna de les capes

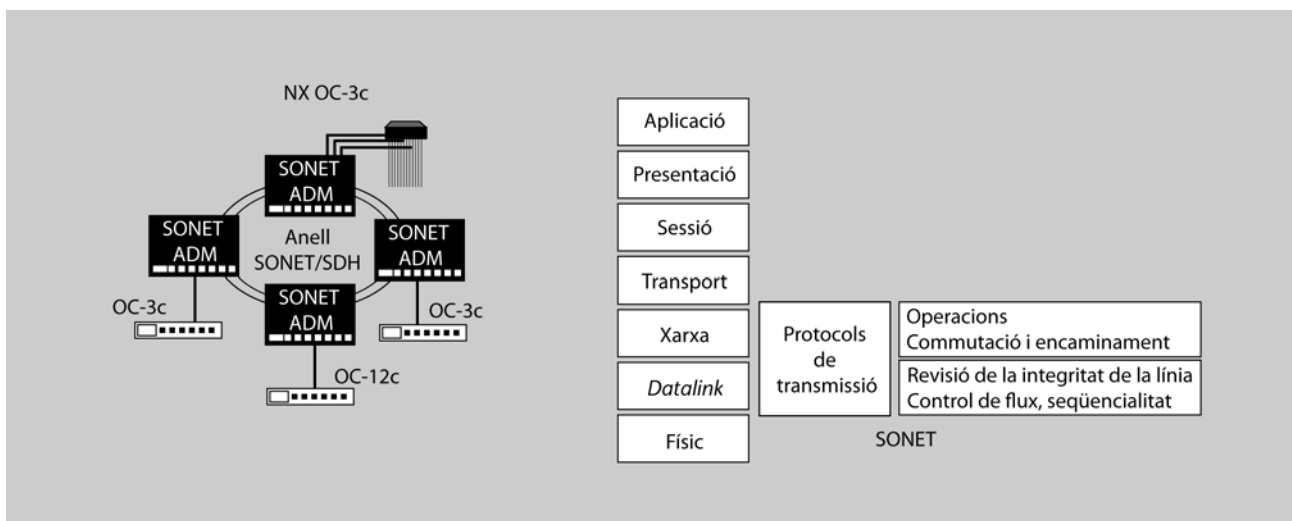


2.1.3. Restriccions d'SDH/SONET

Encara que SDH/SONET està molt estès per algunes de les seves característiques, com són la recuperació davant de falles, la interoperabilitat entre fabricants, etc., té una sèrie de limitacions lligades al seu propi origen:

- **Està pensada principalment per veu.** SONET és una tecnologia de multiplexat (commutació de circuits), la qual cosa vol dir que implementa una arquitectura de telecomunicacions molt rígida. Va molt bé per veu (amplada de banda i latència constants), però no compleix bé les necessitats bàsiques de dades, com són la flexibilitat i l'escalabilitat.
- **Té un cost d'expansió molt elevat.** L'alt cost dels equips SONET dificulta als proveïdors de serveis encarar les necessitats de la MAN associades a l'espectacular augment del trànsit de dades. Els commutadors (*switchs*) de nova generació ofereixen preus molt més baixos.
- **Té redundància de capçaleres.** SONET/SDH proporciona protecció dels circuits i integritat a costa d'incorporar una nova capa d'enllaç a la ja existent. En el cas de transport IP el que fa és que aquesta nova capçalera consumeix capacitat de l'amplada de banda total (figura 13).

Figura 13. Redundància de capçaleres en els anells SONET/SDH



- **Pateix una dificultat de tarifació.** Una altra limitació per als proveïdors és la dificultat de tarifar adequadament aquests nous serveis, ja que, com sabeu, no es comporten de manera uniforme com el trànsit de veu.

2.2. Les xarxes Ethernet metropolitanes

El primer que cal fer és intentar definir què s'entén per xarxa Ethernet Metropolitana (MEN). Es defineix com una xarxa que commuta o connecta empreses LAN geogràficament separades, mentre que també connecta amb les xarxes

MEN: *metro ethernet network*.

Les xarxes MAN basades en tecnologia Ethernet s'anomenen MEN.

backbone o WAN de les operadores. La xarxa MEN proporciona serveis de connectivitat a la geografia metropolitana utilitzant Ethernet com a protocol central i permetent aplicacions *broadcast*. !

Com s'ha dit, Ethernet és una tecnologia àmpliament estesa a un preu adequat i, a la vegada, la majoria de dispositius de telecomunicacions disposen d'interfície Ethernet. Les interfícies poden anar a velocitats de 10/100/1.000 Mbps i des de l'any 2002 està ratificat per l'IEEE l'estàndard a 10 Gbps.

En entorns metropolitans Ethernet té un gran potencial, atesa la capacitat que té d'incrementar la xarxa a un cost efectiu, i al fet que ofereix la possibilitat d'introduir nous serveis de forma escalable, senzilla i flexible. Alguns proveïdors estan estenent Ethernet a la xarxa WAN.

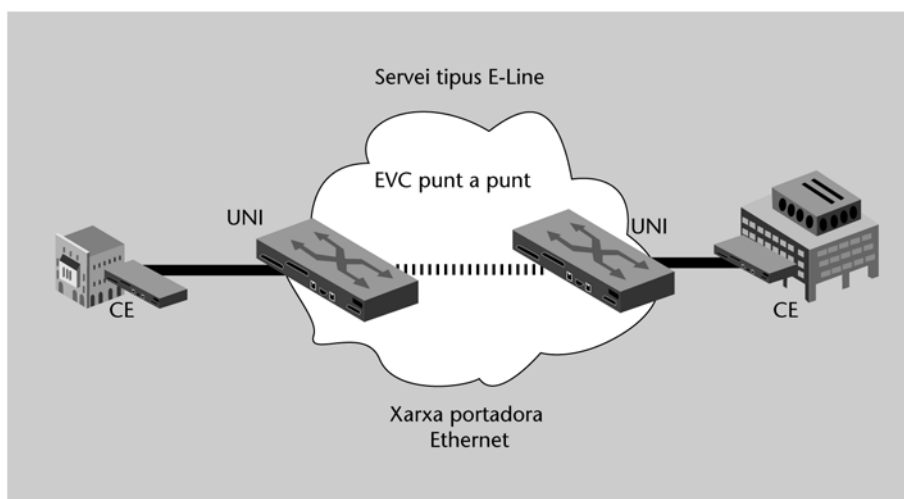
A nivell d'empresa Ethernet té dos serveis d'aplicació clau: per una banda, connectivitat amb la xarxa Internet i, per l'altra, la connectivitat entre seus geogràficament separades a través d'extensions LAN.

Els enllaços normalment són punt a punt. Els nodes poden ser o *switchs* o en-caminadors, en funció de la seva localització.

Un altre aspecte important dintre del serveis Ethernet metropolitans són les connexions virtuals Ethernet (EVC). Aquests EVC connecten dos o més seus d'usuari (UNI). Els serveis Ethernet en funció de la topologia d'EVC es poden classificar en:

- E-Line: enllaços punt a punt (figura 14).
- E-LAN: enllaços multipunt a multipunt (figura 15).

Figura 14. Exemple d'E-Line



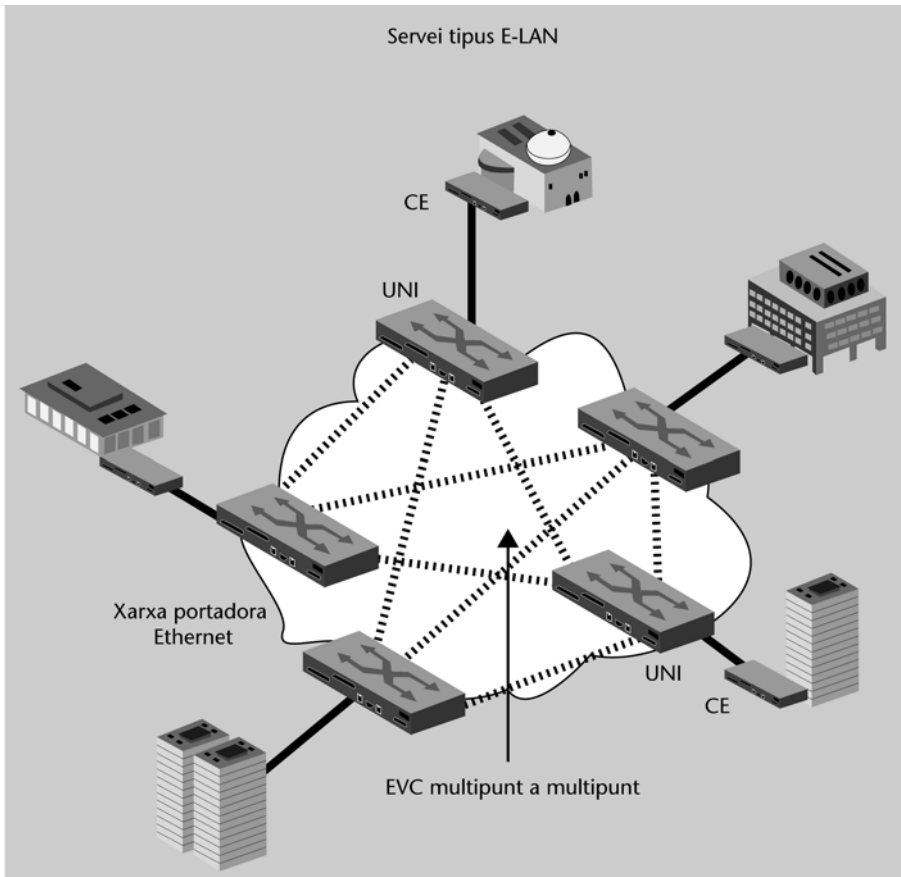
Adreça recomanada

Podeu trobar informació, diversos documents i presentacions amb informació detallada de les xarxes Metro Ethernet a <http://metroethernetforum.org/>.

UNI

L'UNI (*user network interface*) és la interfície física o port que és la demarcació entre l'usuari i el servei de l'operador. L'UNI el proporciona l'operador del servei.

Figura 15. Exemple d'E-LAN



Els serveis també es poden classificar en funció de l'amplada de banda provisionada, de manera que poden ser exclusius o compartits entre diversos usuaris.

2.2.1. Justificació MetroEthernet

Les antigues xarxes metro (com s'ha dit en apartats anteriors) es basaven en tecnologia TDM (*time division multiplexing*), la qual està optimitzada per a transportar serveis de veu. Una xarxa metro clàssica consisteix en un equip TDM instal·lat a la planta baixa de l'edifici del client i a la central de l'operadora. Els equips TDM són bàsicament multiplexors digitals.

La instal·lació d'una xarxa TDM és cara de desenvolupar, ja que TDM és una tecnologia rígida i no té la flexibilitat d'escalabilitat econòmica que necessita l'usuari. Per a l'operadora un cop feta la instal·lació, com menys hagi de modificar els espais habilitats per a l'usuari i la central local per a incrementar els serveis a l'usuari més gran serà el retorn de la inversió inicial feta. Així, un dels problemes de la tecnologia TDM és que l'amplada de banda de les interfícies TDM no creix de manera lineal a la demanda dels usuaris, sinó de manera esglaonada. ⚠

La tecnologia Ethernet està extensament acceptada en la majoria d'empreses i hi ha milions de ports Ethernet instal·lats. La senzillesa d'aquesta tecnologia permet escalar les interfícies Ethernet augmentant l'amplada de banda a un preu controlat.

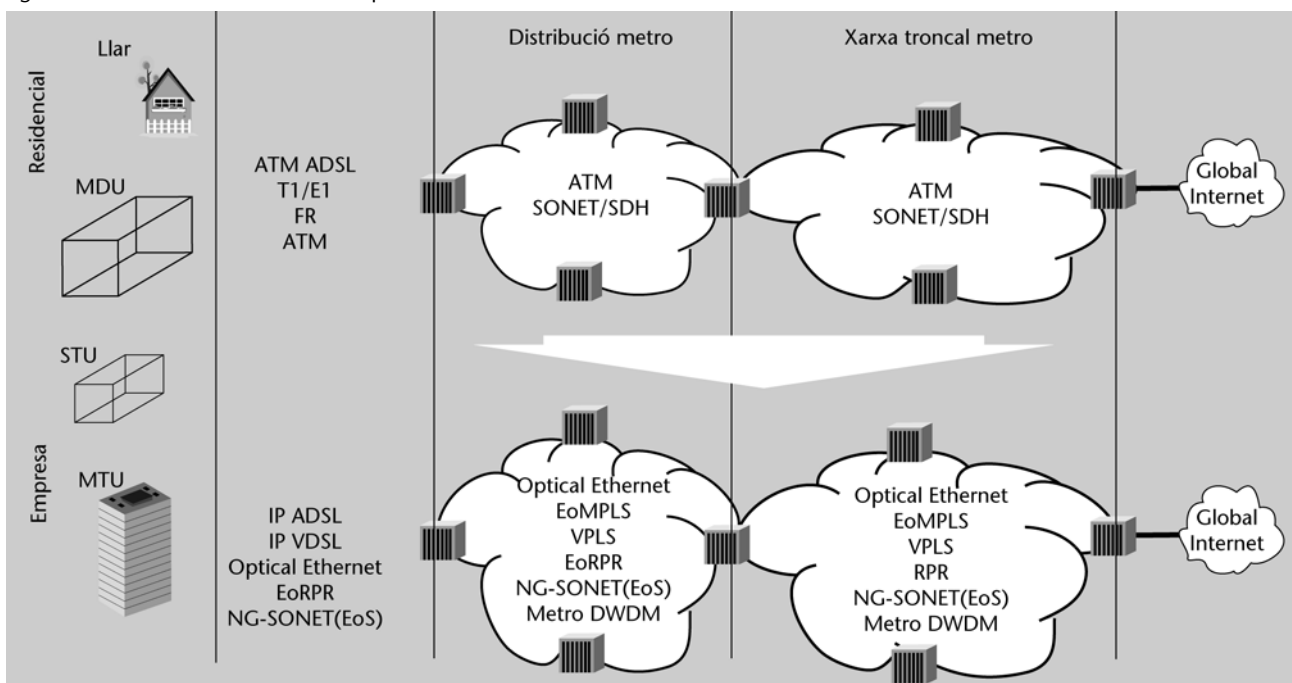
Tant els preus com el rendiment i la simplicitat d'ús estan fent que les operadores de xarxa es plantegin Ethernet com un tecnologia d'accés. En aquest nou model l'usuari té una interfície Ethernet en comptes d'una interfície TDM.

Els aspectes següents són els que donen valor afegit a Ethernet respecte a les línies privades TDM:

- **Efectiu en costos.** El cost d'infraestructura en Ethernet és menor al d'altres solucions, com són ATM o Frame Relay. Això es deu a dos motius:
 - La relativa simplicitat tècnica d'Ethernet.
 - L'economia d'escala, és a dir, el fet que hi hagi una base instal·lada Ethernet assegura la millora en preus. A la vegada, els costos d'aprovisionament són menors en comparació amb altres solucions.
- **Escalabilitat en l'amplada de banda.** Des del punt de vista de l'operador la velocitat de servei és una de les claus que el diferencia respecte als competidors. Els sistemes lligats a TDM o ATM tenen poca flexibilitat i a la vegada no permeten gaire joc a l'hora d'assignar l'amplada de banda que requereixen en cada moment els clients.
- **Basat en paquets.** Un altre avantatge respecte a altres tecnologies és que Ethernet és una tecnologia de trames asíncrona, la qual cosa dona més flexibilitat que les que són síncrones o basades en cel·les.
- **Fàcil d'interconnectar.** Aquest aspecte està associat al ja comentat anteriorment, ja que la simplicitat d'interconnexió simplifica l'aprovisionament i permet migracions a més alta velocitat i amb un cost molt menor.

En la figura 16 es mostra l'evolució de les xarxes metropolitanas cap a una xarxa MetroEthernet.

Figura 16. Evolució de les xarxes metropolitanas



Encara que com veiem les xarxes Ethernet metropolitanes (MEN) tenen una sèrie d'avantatges si ho comparem amb altres xarxes actuals com són ATM o Frame Relay, podem trobar-hi algunes limitacions, encara que tenen solució:

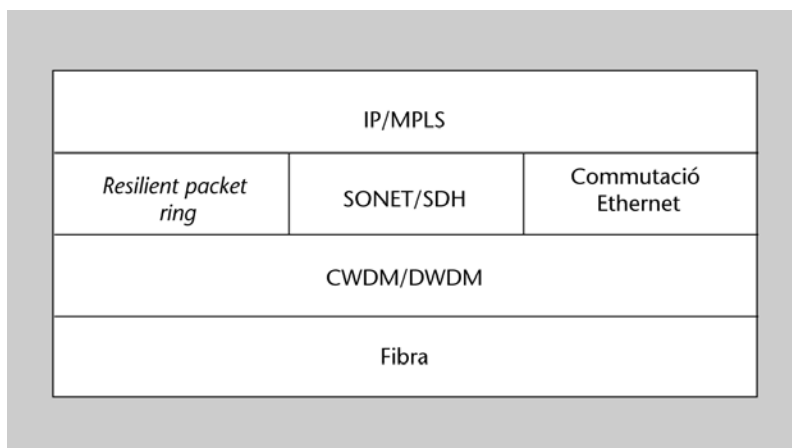
- **Qualitat de servei garantida extrem a extrem.** Així, Ethernet necessita incorporar mecanismes per dur a terme el següent:
 - Control d'admissió per demanda de nous serveis. La incorporació d'un nou servei en cap cas pot comprometre el rendiment dels serveis existents.
 - Polítiques per a tenir un accés just. Mecanismes per a assegurar que en moments de congestió es pot disposar de l'amplada de banda en igualtat de condicions.
 - Establiment d'un camí òptim a través de la xarxa. L'algorisme d'STP no busca el camí òptim.
 - Marcatge dels paquets. Poder marcar els paquets per donar prioritats, polítiques d'accés, etc.
- **Mecanismes de protecció.** En estar pensat inicialment per a entorns LAN no disposa de bons mecanismes de protecció contra interrupcions a la xarxa. Així mateix, té una lenta recuperació contra fallades. Ethernet usa l'algorisme d'arbre estès (*spanning tree*) per a solucionar problemes en els enllaços, que triga ordres de magnitud de segons per a recuperar la xarxa. Per contra, en entorns SONET la recuperació es fa en aproximadament 50 ms, que són ordres de magnitud pensats per a aplicacions crítiques, veu i vídeo.
- **Operació, administració i manteniment (OAM).** Ethernet no disposa de les característiques específiques d'SDH per a la gestió i manteniment de la xarxa.
- **Escalabilitat i utilització dels recursos de la xarxa.** Un dels avantatges d'Ethernet és la possibilitat de fer particions lògiques sobre la mateixa xarxa mitjançant LAN virtuals (VLAN). Si aquest concepte usat àmpliament en entorn empresarial l'estenem a nivell de xarxa metropolitana incorpora nous reptes a aconseguir. EL problema que tenim és que l'espai d'etiquetes de VLAN és limitat. L'estàndard 801.Q defineix un espai d'adreces de 4.096 etiquetes disponibles. Aquest valor és insuficient per a un proveïdor de serveis.

L'algorisme d'arbre gestiona els bucles en una xarxa commutada.

OAM: operation, administration and maintenance.

Actualment hi ha diverses solucions que conjuguen el millor de les diverses tecnologies existents. Per una banda, cal aprofitar la infraestructura muntada però per l'altra cal aprofitar els avantatges que proporcionen les noves tecnologies. En la figura 17 es mostren les diverses possibilitats existents.

Figura 17. Ethernet en relació amb altres tecnologies dels proveïdors



2.3. Ethernet sobre SDH (EOS)

Moltes de les grans operadores de xarxa han gastat molts diners en la seva infraestructura d'SDH a la xarxa metropolitana. A aquests operadors els agradaria poder usar aquesta infraestructura com a base per a transmetre la nova generació de serveis Ethernet. El repte principal que tenen és la millora en l'optimització de l'ús de l'amplada de banda i el comportament del trànsit del servei de dades.

EOS: Ethernet over SONET/SDH.

EOS permet introduir els serveis Ethernet preservant els atributs que proporciona la infraestructura SDH: ràpida recuperació, monitoratge de la qualitat de la línia i la gestió OAM&P.

Pel que fa al funcionament, EOS encapsula tota la trama Ethernet a l'entrada de la xarxa SDH i la desencapsula a la sortida.

A la figura 18 es mostra l'encapsulat que fa.

Figura 18. Encapsulat Ethernet en SDH

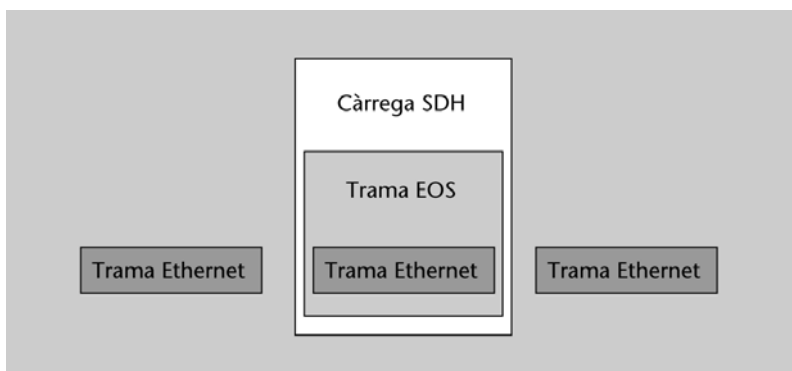
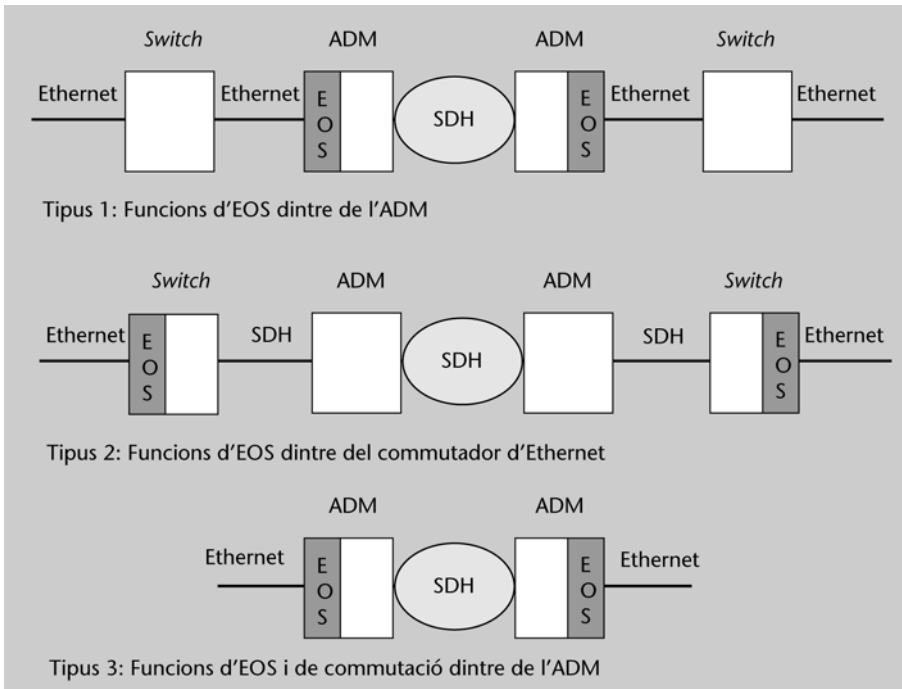


Figura 19. Diferents escenaris de connexió EOS



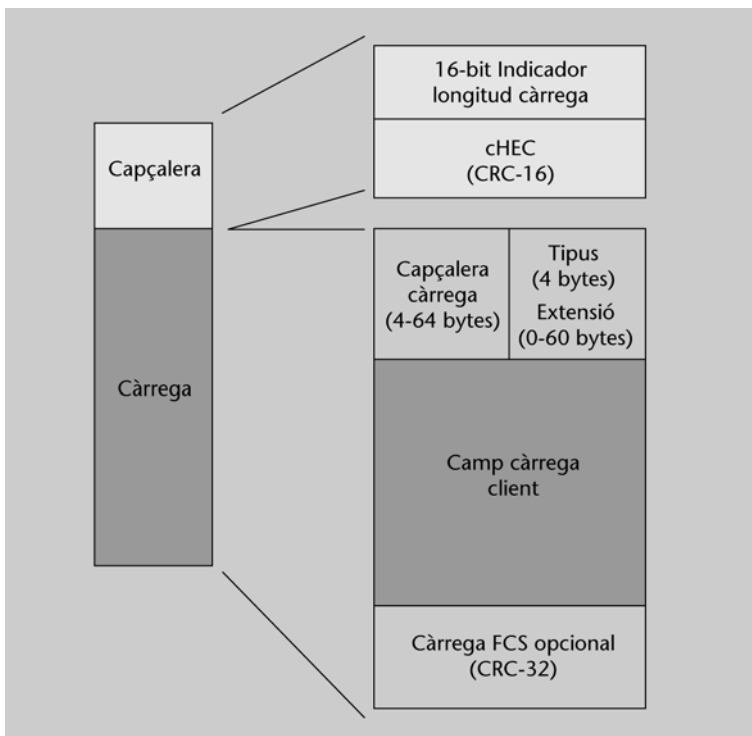
Hi podem trobar dos estàndards per a transportar Ethernet sobre la xarxa SDH:

- **LAPS**. Està definit per la ITU-T, que va publicar l'estàndard X.86 el febrer de 2001. LAPS és un protocol no orientat a connexió similar al protocol HDLC.
- **GFP**. També és un estàndard de la ITU que usa el protocol SDL com a punt d'inici. Una de les diferències entre LAPS i GFP és que aquest segon pot acomodar trames que no siguin Ethernet, com són PPP, canals de fibra (*fiber channel*), etc. (figura 20).

LAPS: *link access procedure sdh*.
 HDLC: *high level data link control*.

Per a ampliar la informació sobre les tecnologies d'accés, podeu veure el mòdul "WAN".

Figura 20. Format de trama GFP



Les funcions EOS poden residir dintre dels equips SONET/SDH o dintre dels equips de commutació de paquets. Això és bo perquè genera diversos escenaris de competència entre venedors d'equips de commutació i venedors d'equips de transport per a oferir connexions Ethernet.

Un dels aspectes que cal solucionar és l'ineficient ús de l'amplada de banda dels circuits SDH en transmetre Ethernet. Aquestes ineficiències estan lligades a la poca granularitat dels circuits SDH/SONET i el difícil lligam amb els requeriments d'amplada de banda d'Ethernet. Per a millorar-ho, s'incorpora el mecanisme de concatenació virtual (VCAT).

VCAT: *virtual concatenation*.

2.3.1. Concatenació virtual

La concatenació virtual, com ja heu vist quan es parlava d'SDH, és un mecanisme per a reduir la ineficient amplada de banda de TDM en els anell SDH/SONET. Per tant, SDH dintre del seu estàndard incorpora la concatenació, que intenta ajustar l'amplada de banda dels circuits TDM en els anell SDH als requeriments d'amplada de banda que necessiten en cada moment.

VCAT permet fer millor aquest ajustament de l'amplada de banda. Així, la concatenació virtual permet agrupar $n * VT$, la qual cosa permet, alhora, la creació de connexions que es poden ajustar a l'amplada de banda que es necessita.

2.3.2. Ajustar la capacitat de la connexió (LCAS)

Un segon aspecte que cal solucionar en el transport Ethernet o dades en general és el fet que l'amplada de banda que necessita l'usuari va canviant en el temps i cal que les connexions es tornin a redimensionar.

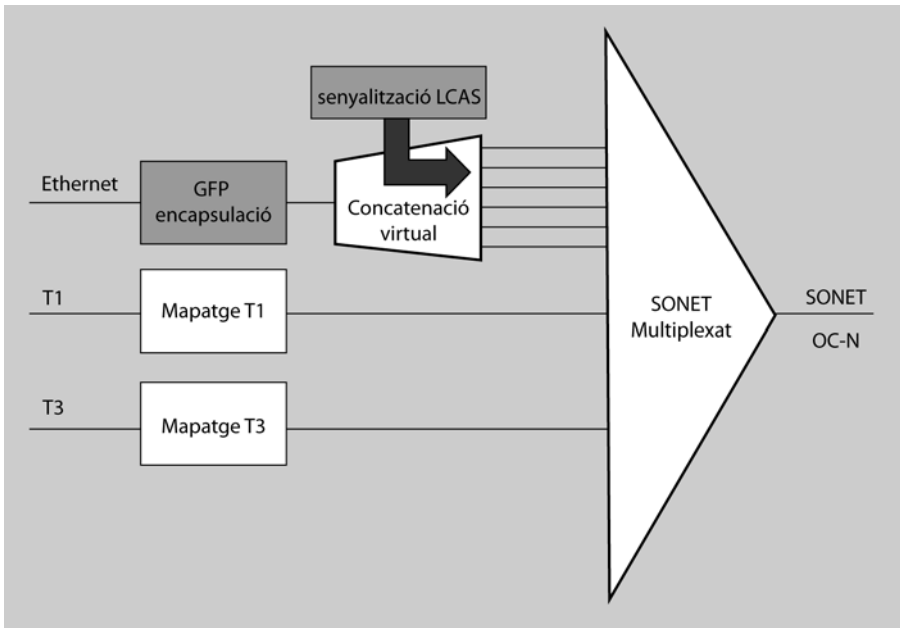
LCAS: *link capacity adjustment scheme*.

LCAS és un protocol que permet redimensionar els canals sense haver d'intromoure el trànsit de la línia. LCAS també fa un seguiment de les fallades de la línia, de manera que poden ser eliminades i s'hi poden afegir noves línies de forma dinàmica sense interrupcions de la línia.

Com a conclusió, podem dir que per a transmetre serveis Ethernet sobre SDH el que proporciona una millor eficiència és la combinació d'EOS, VCAT i LCAS.

Quant a servei, OES ofereix un servei comparable als serveis de commutació de paquets en línies dedicades punt a punt.

Figura 21. Senyalització LCAS que permet canviar l'amplada de banda sota demanda



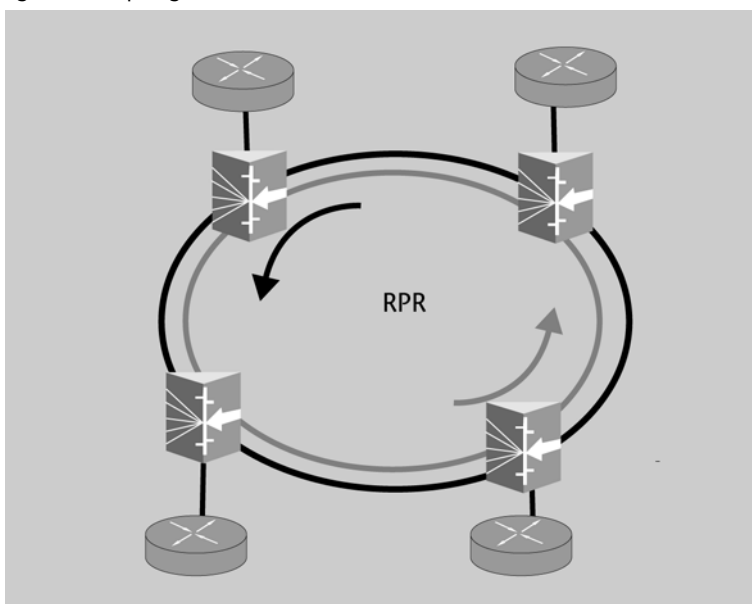
2.4. Resilient packet ring (RPR) IEEE 802.17

RPR és un nou protocol de control d'accés al medi dissenyat per a optimitzar la gestió d'amplada de banda i facilitar el desenvolupament de serveis de dades sobre una xarxa en anell. L'origen és una tecnologia propietària de Cisco, *data packet transport* (DPT).

Per als operadors amb infraestructura SDH no resulta una tecnologia atractiva, ja que és complicat corre RPR sobre SDH.

RPR és per a commutació de paquets en xarxes en anell desenvolupada sobre fibra fosca o WDM (figura 22).

Figura 22. Topologia en anell a RPR




Es pot dir que RPR i EOS competeixen entre elles en l'entorn de xarxes metropolitanas.

El principal avantatge de l'estàndard RPR 802.17 és el fet que els nodes commuten el paquet sense emmagatzemar-lo si el trànsit no pertany a aquest node. Això redueix el treball del mateix node.

L'avantatge respecta a SDH és que com que RPR és commutació de paquets es comparteix l'amplada de banda de l'anell. La tasca d'RPR consisteix a gestionar aquesta amplada de banda.

L'altre punt fort d'RPR és que el temps de recuperació de l'anell és de 50 ms, comparable a SDH.




Recordeu que SDH és commutació de circuits i el que assigna són unitats de temps (*time slots*) a cada circuit.

3. Multiprotocol label switching

El Multiprotocol Label Switching (MPLS) és un mecanisme de transport de dades estàndard creat per la IETF i definit al RFC 3031.

La indústria ha estat buscant una solució que combini les millors característiques d'IP i ATM. Això ha conduït a MPLS. El desenvolupament d'MPLS en les xarxes dels operadors d'Internet és possible ja que és transparent per a l'usuari. D'altra banda, té grans conseqüències per a l'arquitectura. MPLS ha canviat el model de commutació unicast basat en la destinació, que s'havia mantingut pràcticament inalterable des del principi d'Internet. A la vegada, també ha impactat en l'arquitectura d'encaminament fent que els protocols d'encaminament executin noves i més complexes tasques.

3.1. Problemes experimentats pels proveïdors de servei

Veiem primer quins problemes de les xarxes actuals han fet plantejar a les operadores la cerca d'una nova tecnologia: 

- IP i ATM són dues tecnologies desenvolupades de forma separada sense nexes d'unió. Els *switchs* ATM s'encarreguen de moure trànsit en funció dels VCI/VPI dels quals els encaminadors d'accés (en els POP) no tenen coneixement. El mateix passa a la inversa. Els encaminadors fan l'encaminament sense tenir en compte els *switchs* (són transparents per a l'encaminador).
- Escalabilitat. Per a tenir màxima redundància i encaminament òptim cal crear una topologia de circuits virtuals *full mesh*. Això crea un problema d'escalabilitat.
- *Traffic engineering*. TE és el procés pel qual el trànsit es fa òptim per a seguir certs camins basat en requeriments específics. ATM disposa de moltes característiques per a TE. IP també en té alguna. El problema és que en tenir dues tecnologies totalment separades resulta complicat combinar-les per tenir TE extrem a extrem.
- QoS. Passa el mateix que en el cas anterior. Totes dues tecnologies disposen de mecanismes per a proporcionar QoS, però resulta complicat combinar-les.

3.2. Què és MPLS?

MPLS és un mètode d'encaminament de paquets a través de la xarxa que usa per a fer-ho etiquetes inserides en el paquet IP.

Les etiquetes s'insereixen entre la capçalera de nivell 2 i 3 en tecnologies basades en trames i estan contingudes en el VPI/VCI en les tecnologies basades en cel·les.

MPLS combina commutació de nivell 2 i encaminament de nivell 3.

Amb commutació d'etiquetes l'anàlisi de la capçalera nivell 3 es fa només un cop, en ingressar a la xarxa MPLS. En aquest punt, la capçalera nivell 3 és mapejada en una etiqueta de longitud fixa.

3.3. Beneficis d'MPLS

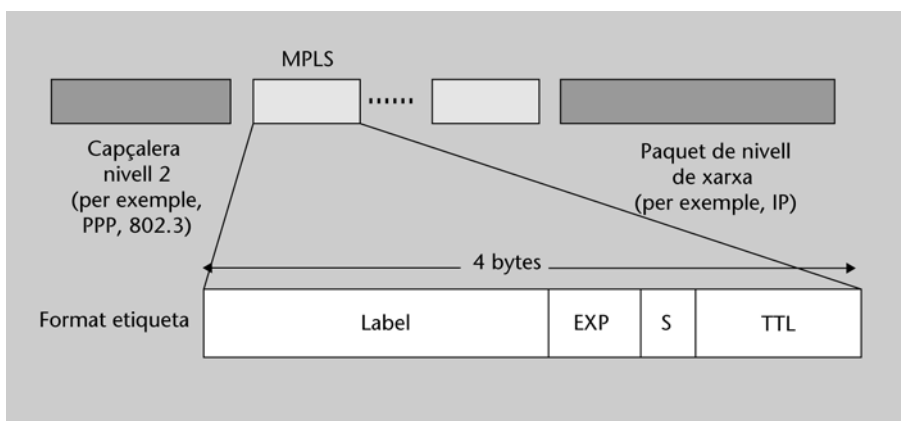
La commutació basada en etiquetes permet als encaminadors i als *switchs* ATM-MPLS prendre decisions d'enviament basades en una senzilla etiqueta en comptes de fer una cerca de ruta basada en la IP destinació. El beneficis que aporta a la xarxa IP són els següents:

- VPN. Els proveïdors poden crear VPN nivell 3 a través del seu *backbone* de xarxa per a diferents clients, usant la mateixa infraestructura sense necessitat d'encriptació i aplicacions d'usuari.
- *Traffic engineering*. Permet optimitzar la utilització de l'amplada de banda de la xarxa i optimitzar els camins.
- QoS. Possibilita aprofitar les característiques de QoS d'IP i ATM.
- Integra IP i ATM.

3.4. Pila d'etiquetes MPLS (MPLS label stack)

MPLS, per tant, apareix inicialment com una tecnologia que permet "enganxar" ATM i IP. La pila d'etiquetes MPLS té quatre octets i és com la de la figura 23.

Figura 23. Etiqueta MPLS



Els camps que es mostren en la figura 23 són:

- **Label:** té l'etiqueta i és de 20 bits.
- **Experimental (EXP):** tres bits i serveix per a fer un mapatge al camp ToS d'IP en el camp EXP per a MPLS CoS.
- **S:** MPLS permet incorporar més d'una etiqueta.
- **TTL:** temps de vida del paquet.

3.4.1. Capçalera inserida (*shim header*)

Un cop hem vist com és l'etiqueta cal saber on va. L'etiqueta s'incrusta entre la capçalera de nivell 2 i la capçalera de nivell 3. Com es veu, l'etiqueta MPLS va abans de la capçalera IP, de manera que els encaminadors poden commutar en funció de l'etiqueta en comptes de la capçalera IP.

3.4.2. *Forwarding equivalence class (FEC)*

Conjunt de paquets de nivell 3 que són reenviats de la mateixa manera pel mateix camí i amb el mateix tractament en l'enviament.

Exemples de FEC

Alguns exemples de FEC poden ser:

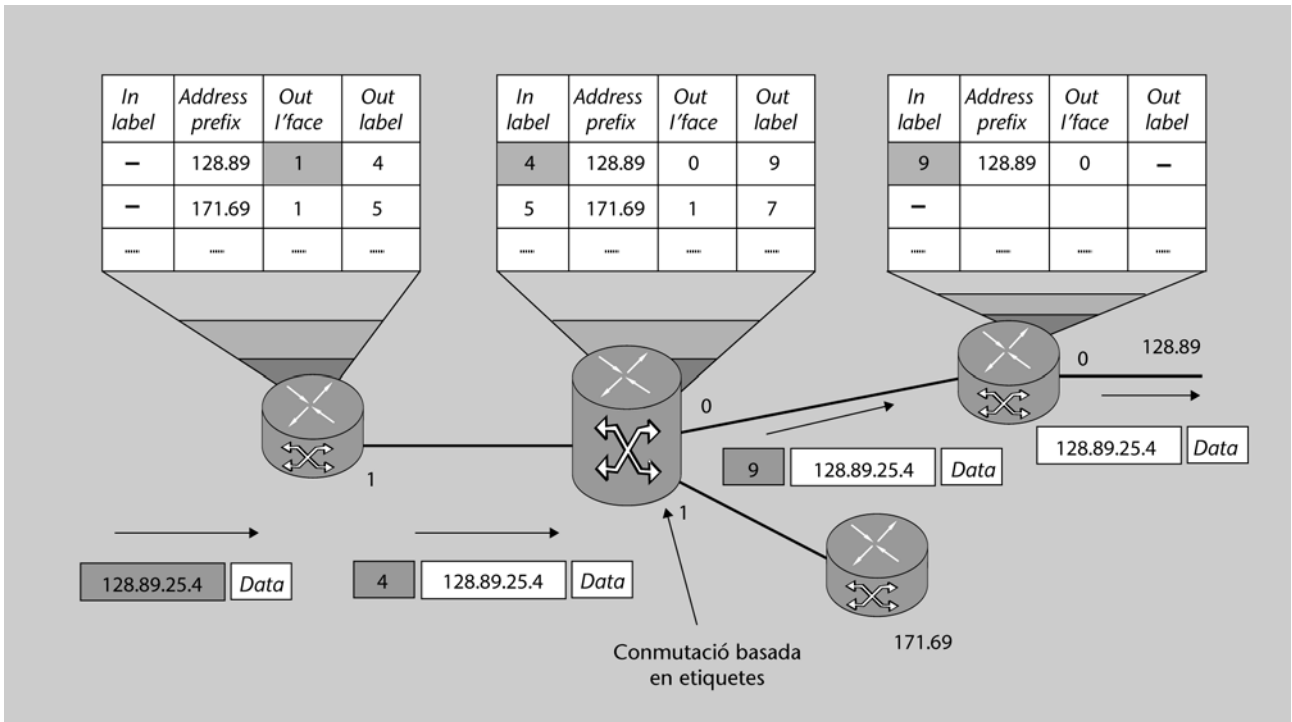
- Paquets de nivell 3 que tenen cert prefix de xarxa.
- Paquets de nivell 3 que van a una destinació concreta.

3.5. Arquitectura MPLS

L'arquitectura MPLS està formada per dos plànols:

- **Control.** El plànol de control és responsable d'unir una etiqueta a les rutes de la xarxa (FEC) i redistribuir aquesta unió als altres encaminadors MPLS. Com que estem dient que s'uneix l'etiqueta a una ruta de xarxa cal que l'encaminador tingui una taula d'encaminament. Per a redistribuir les etiquetes el protocol bàsic és LDP (*label distribution protocol*). El LIB (*label information base*) és un mapatge d'etiquetes d'entrada amb etiquetes de sortida, juntament amb interfície de sortida i informació de la línia. Com s'ha comentat anteriorment el FEC (*forwarding equivalence class*) és un grup de paquets IP que són tractats de la mateixa manera. Per exemple, una sub-xarxa destinació pot correspondre a un FEC. FEC està basat en diversos criteris, com poden ser IP ToS bits, números de port, etc.
- **Encaminament (*forwarding*).** Un encaminador MPLS commuta els paquets IP en comptes d'encaminar-los. Així, la taula LIB es construeix en el plànol de control i només aquelles etiquetes en ús resideixen en *label forwarding information base* (LFIB). Per tant, LFIB és un subconjunt de LIB. Un altre component del plànol de *forwarding* és la taula *forwarding information base* (FIB). La crea Cisco quan usa *Cisco express forwarding* (CEF).

Figura 24. Commutació MPLS

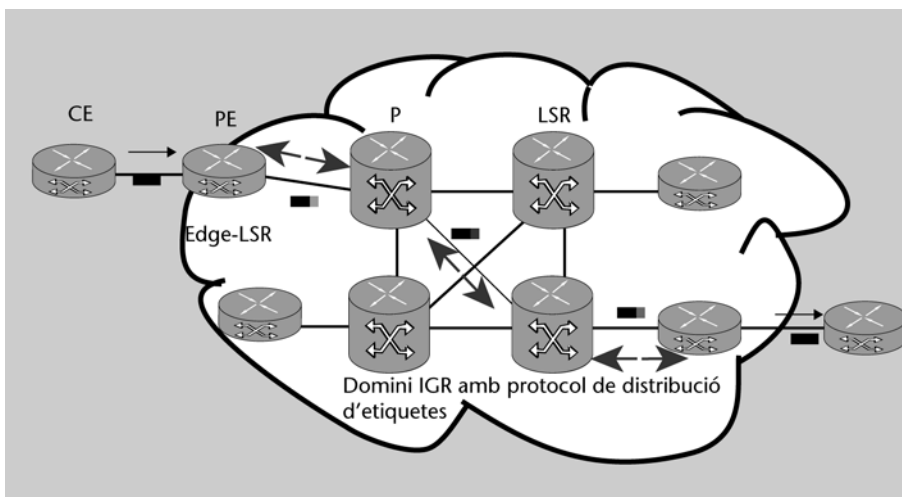


3.6. Components de xarxa MPLS

Els components de xarxa MPLS són els següents (figura 25):

- **CE (customer edge)**. Encaminador que connecta la xarxa d'usuari amb el proveïdor de servei
- **PE (provider edge)**. Encaminador de l'operadora que connecta a l'usuari amb la xarxa del proveïdor.
- **P (provider)**. Equip que està en la xarxa del proveïdor i que només està connectat amb altres equips de l'operadora.

Figura 25. Components de la xarxa MPLS



Els equips PE i P són *label switch routers* (LSR). Es poden distingir dos tipus d'LSR:

- **LSR** és un encaminador/*switch* que és capaç de commutar paquets basat en etiquetes. El CE no és un equip LSR.
- **Edge-LSR**. Terme més específic per als encaminadors PE. En el cas de les xarxes MPLS és l'equip que agafa trànsit IP no etiquetat i posa una etiqueta per a enviar-lo al següent LSR. També fa el procés invers. Quan rep un paquet d'un LSR treu l'etiqueta abans d'enviar-lo al següent node de la xarxa IP.
- **Label switched path (LSP)**. És el conjunt d'LSR que el paquet ha de seguir en el seu flux cap a la destinació.

LSP són adequats usant diversos protocols en funció dels diversos mòduls de control necessaris: LDP, *resource reservation protocol* amb *traffic engineering extensions* (RSVP-TE), *constraint-based routed LDP* (CR-LDP) o extensions de protocols d'encaminament com *multiprotocol BGP*.

L'LSP pot ser considerat el camí sobre un conjunt d'LSR que els paquets que pertanyen a cert FEC usen en el seu viatge per a obtenir la seva destinació.

3.6.1. Establiment de l'LSP

L'establiment de l'LSP es pot fer de dues maneres:

- Amb control independent.
- Amb control per ordre.

Tots dos mètodes tenen els seus avantatges i inconvenients. El control independent permet una convergència més ràpida, mentre que el control per ordre permet una capacitat més gran de prevenció de bucles.

Establiment LSP amb control independent

En el mètode de control independent per a establir els LSP, cada LSR divideix els seus prefixos de destinació en FEC. Les etiquetes s'assignen a cada FEC, i la unió d'etiquetes és informada a cada veí LSR. Els LSR creen una LFIB fent un mapatge entre els FEC i els seus salts següents. L'LSR normalment corre un protocol d'encaminament unicast tipus OSPF, i usa la informació proporcionada per aquests per crear el mapatge FEC en el salt següent.

Després de crear la unió local, l'LSR distribueix informació de les unions locals als seus veïns LSR usant LDP o extensions d'un protocol d'encaminament modificat.

Quan un LSR adjacent rep informació d'una etiqueta d'unió d'un veí, examina la presència d'una unió local en els seus LFIB. Si hi ha unió local, actualitza

l'etiqueta de sortida per a aquella entrada amb el valor de la nova etiqueta rebuda. L'LSR té ara una entrada LFIB completa i preparada per a reenviar paquets.

La unió d'etiquetes es distribueix només entre encaminadors adjacents.

En casos com d'enginyeria de trànsit MPLS, la distribució d'informació basada en restriccions ha de ser executada en ordre per trobar els camins adequats a través de la xarxa. La informació de les restriccions ha de ser distribuïda de manera consistent a través de la xarxa MPLS.

Establiment LSP amb control per ordre

En el mètode de control per ordre per establir els LSP, els LSR *ingress o egress* inicien el procés. El que inicia fa la selecció de FEC, i tots els LSR a través de l'LSP usen el mateix FEC. El control per ordre de l'establiment LSP requereix que la unió d'etiquetes es propagui per tots els LSR abans que es puguin establir els LSP. Això fa que la convergència sigui més lenta. En canvi té una capacitat millor per a prevenir bucles.

Se sol usar el mode de control independent per a l'establiment en entorns basat en paquets i el mode de control per a ordre en ATM.

3.7. Protocol de distribució d'etiquetes (LDP)

El protocol de distribució d'etiquetes (LDP) s'usa conjuntament amb protocols d'encaminament de nivell 3 per a distribuir informació d'etiquetes entre els dispositius LSR en una xarxa commutada per etiquetes. LDP distribueix etiquetes entre veïns mitjançant el protocol TCP port 646.

LDP: *label distribution protocol.*

L'objectiu d'LDP és ajudar en l'establiment d'LSP usant una sèrie de procediments per a distribuir les etiquetes entre veïns LSR.

LDP proporciona un mecanisme per a descobrir els veïns i establir comunicació. Defineix quatre classes de missatges:

- **Descobriment (*discovery*)**. Corren sobre UDP i usen missatges HELLO multicast per a aprendre sobre els veïns LSR que tenen directament connectats. Llavors estableixen una connexió TCP i una sessió LDP eventual. Les sessions LDP són bidireccionals. L'LSR a l'altre extrem pot informar o demanar informació d'unions de l'altre extrem de la connexió.
- **Adjacència (*adacency*)**. Corre sobre TCP i proporciona inici de sessió, de manera que permet negociar certs paràmetres de funcionament entre veïns.
- **Informació d'etiquetes (*label advertisement*)**. Proporciona informació de les etiquetes i el FEC corresponent.

- Notificació (*notification*). Permet enviar missatges d'avís per a informar bàsicament de problemes.

La distribució i assignació d'etiquetes amb LDP es pot executar de diferents modes:

- *Downstream-on-demand mode LDP*. Permet a l'LSR demanar de forma explícita al següent salt per a un FEC particular, l'etiqueta que cal unir a aquest FEC.
- *Unsolicited downstream mode LDP*. Permet a l'LSR distribuir una unió al veí LSR encara que aquest no l'hagi demanat explícitament.

Qualsevol dels dos modes poden ser usats en la mateixa xarxa simultàniament. Això es negocia entre LSR durant la fase d'inicialització (*initialization*).

Figura 26. Negociació LDP

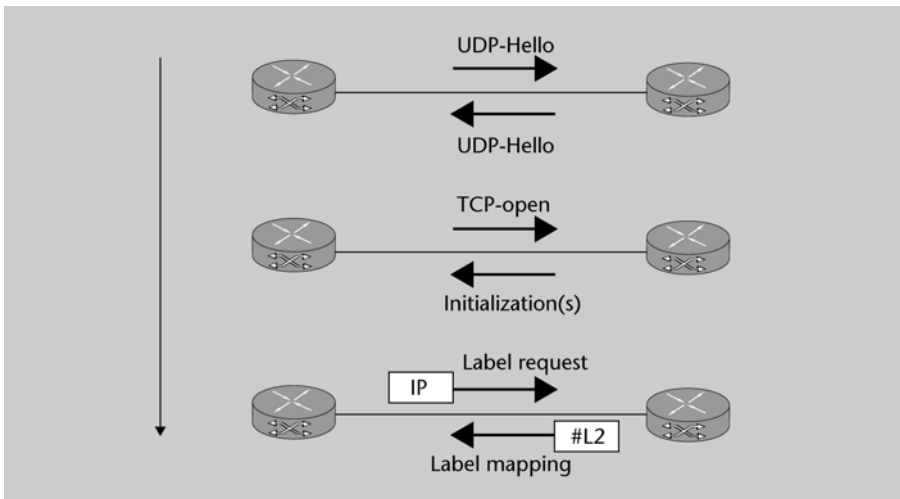
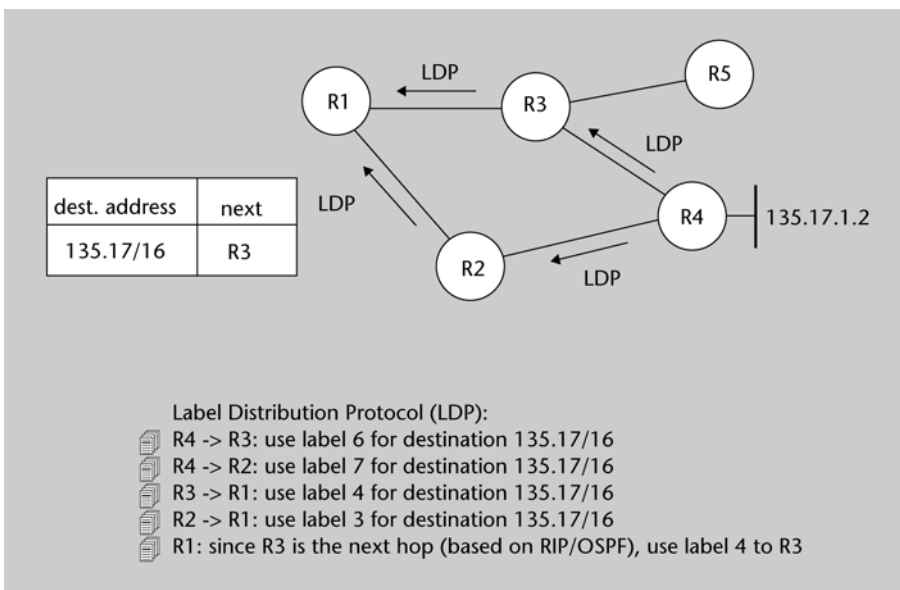


Figura 27. Exemple de distribució d'etiquetes



Resum

En aquest mòdul didàctic s'han intentat cobrir dos grans objectius. Per una banda, veure els elements bàsics en el disseny de xarxes. En cap moment s'ha volgut fer un receptari del que ha de ser el disseny, sinó fer una petita introducció al tema. La informació del que es vol i cap on es vol anar són dos dels elements clau en el disseny.

En la segona part del mòdul s'ha intentat fer un salt cap endavant introduint noves tecnologies que estan sorgint amb molta força en dos àmbits. D'una banda, el món Internet amb MPLS i de l'altra, a nivell de xarxa metropolitana amb Metro Ethernet.

A nivell de xarxa metropolitana s'ha explicat l'entorn d'actuació, solucions actuals amb les seves limitacions per a cobrir les noves necessitats existents. A partir d'aquestes limitacions s'han volgut introduir les noves propostes actuals com és Metro Ethernet i les diverses solucions per a fer conviure les tecnologies ja implantades (SDH) amb Metro Ethernet.

A nivell de la xarxa troncal de les operadores i Internet s'han explicat les característiques principals del protocol MPLS. S'ha justificat la motivació d'aquesta tecnologia i els elements clau per al seu funcionament.

En tot moment, ha de quedar clar que aquestes noves tecnologies no són úniques i que no sempre són la millor solució per a tots els casos. Els requeriments ens han de marcar quina ha de ser la solució, i no ha de ser la solució qui ens marqui els requeriments.

Activitats

1. Busqueu a la *Viquipèdia* informació sobre el protocol d'encaminament RIPv1. Determineu-ne les característiques principals i els inconvenients.
2. Justifiqueu per quin motiu una xarxa commutada amb commutadors (*switchs*) no pot tenir bucles.
3. Busqueu informació sobre l'estàndard 802.1p
4. Determineu les característiques segons el mercat del sistema ideal en xarxes metropolitanes.

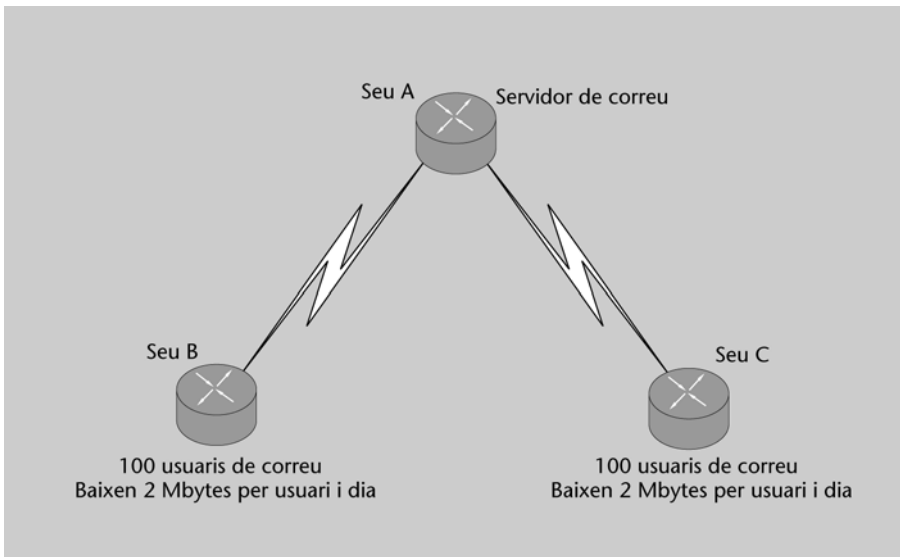
Adreça recomanada

Podeu consultar la *Viquipèdia* a l'adreça <http://www.wikipedia.org>.

Exercicis d'autoavaluació

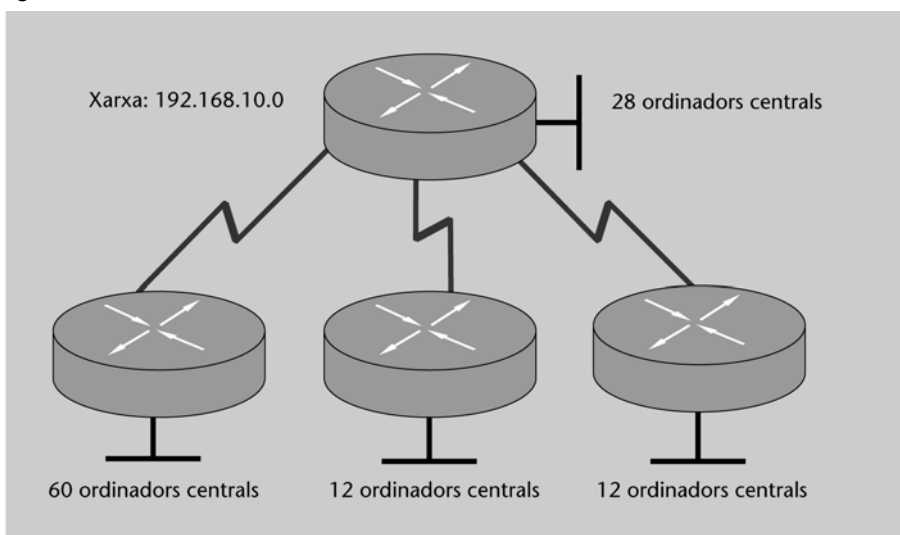
1. A la figura 28 teniu l'esquema de la topologia d'una empresa on es mostren uns requeriments mínims. Determineu l'amplada de banda requerida per a cadascuna de les seus en els casos següents:
 - a) El correu es descarrega durant tot el dia.
 - b) Hi ha un pic de trànsit al matí quan arranquem l'Outlook entre les 8 i les 8.15 hores.

Figura 28



2. Realitzeu l'adreçament IP de longitud variable (VLSM) adequat per a la topologia de xarxa de la figura 29.

Figura 29



Solucionari

1. Mirant la figura 28 tenim el següent: les seus A i B requereixen 2 Mbytes de dades en una direcció per usuari i dia.

a) Si el correu es va descarregant en període laboral (8 hores) tenim:

$$(2.000.000 \text{ bytes} \times 8 \text{ bits/byte}) / 8 \text{ hores} \times 3.600 \text{ segons/hora} = 556 \text{ bps}$$

Si com s'ha indicat tenim 100 usuaris ens dóna 55,6 kbps.

b) Si el que tenim és un pic de trànsit concentrat en 15 minuts, en aquest cas els requeriments d'amplada de banda seran:

$$(2.000.000 \text{ bytes} \times 8 \text{ bits/byte}) / 15 \text{ minuts} \times 60 \text{ segons/minut} = 88,9 \text{ kbps}$$

Si tenim 100 usuaris necessitem una amplada de banda de 889 kbps. En aquest cas haurien de contractar una línia que ens donés un mínim d'1 Mbps.

2. Si ens fixem en la topologia de la figura 23 tenim que ens donen una adreça IP de classe C. A partir d'aquesta adreça hem de fer VLSM per a quatre xarxes amb 28, 60, 12 i 12 *hosts* respectivament. En aquest cas el que fem és crear quatre subxarxes amb 62 adreces cadascuna. La primera l'assignarem a la xarxa que necessita 60 IP. Em queden ara tres subxarxes. Agafem la primera i tornem a repetir el procés creant dos subxarxes més.

192.168.10.0 /24	192.168.10.0 255.255.255.192	Adreçament per la xarxa amb 60 <i>hosts</i>
	192.168.10.64 255.255.255.192	
	192.168.10.128 255.255.255.192	
	192.168.10.192 255.255.255.192	

192.168.10.64 255.255.255.192	192.168.10.64 255.255.255.224
	192.168.10.96 255.255.255.224

Hem creat dues xarxes de 30 IP cadascuna. El primer rang ens serveix per a la xarxa que necessita 28 IP.

Ara repetirem el mateix procés per cobrir les necessitats de les xarxes de 12 IP. Agafem el rang 192.168.10.96 255.255.255.224 i fem *subnetting*:

192.168.10.96 255.255.255.224	192.168.10.96 255.255.255.240
	192.168.10.112 255.255.255.240

Amb aquesta solució tenim encara dos rangs d'adreces per a futures ampliacions:

192.168.10.128 255.255.255.192
192.168.10.192 255.255.255.192

Glossari

border gateway protocol *m* Protocol per a l'intercanvi d'informació d'encaminament entre encaminadors normalment entre sistemes autònoms.
sigla BGP

BGP *m* Vegeu *border gateway protocol*.

contenedor virtual *m* Senyal SDH que transporta una càrrega que és més petita que una càrrega STM-0.
sigla VC

enginyeria de trànsit *f* Tècnica i mètodes usats que fan que el trànsit encaminat a través d'una ruta o camí determinat no segueixi els estàndards dels protocols d'encaminament.
en traffic engineering

E-LAN *m* Vegeu *Ethernet LAN service*.

EOS *m* Vegeu *Ethernet sobre SONET/SDH*.

Ethernet LAN service *m* Servei Ethernet multipunt a multipunt.
sigla E-LAN

Ethernet sobre SONET/SDH *m* Tecnologia que permet als paquets Ethernet ser transportats a través d'una xarxa SONET/SDH.
sigla EOS

Ethernet virtual connection *m* Servei Ethernet punt a punt.
sigla EVC

EVC *m* Vegeu *Ethernet virtual connection*.

FEC *m* Vegeu *forwarding equivalence class*.

forwarding equivalence class *m* Conjunt de paquets de nivell tres que són commutats de la mateixa manera pel mateix camí, amb el mateix tractament de commutació.
sigla FEC

GE *m* Vegeu *gigabit Ethernet*.

gigabit Ethernet *m* Estàndard d'Ethernet a alta velocitat, aprovat per l'IEEE 802.3z el 1996.
sigla GE

label distribution protocol *m* Protocol estàndard que permet als encaminadors MPLS negociar etiquetes (adreces) que s'usen per a reenviar els paquets.
sigla LDP

label edge router *m* Encaminador que fa la imposició de les etiquetes.
sigla LER

label forwarding information base *m* Estructura usada en la commutació d'etiquetes per a mantenir informació de les etiquetes d'entrada i sortida, interfícies i FEC associat.
sigla LFIB

label switch path *m* Camí que els paquets MPLS travessen entre dos LSR frontera.
sigla LSP

LAN *f* Vegeu *xarxa d'àrea local*.

LDP *m* Vegeu *label distribution protocol*.

LER *m* Vegeu *label edge router*.

LFIB *m* Vegeu *label forwarding information base*.

LSP *m* Vegeu *label switch path*.

MAN *f* Vegeu *xarxa d'àrea metropolitana*.

multiprotocol label switching *m* Mètode de commutació que permet reenviar paquets IP usant etiquetes.
sigla MPLS

OAM and P *f* Operació, administració, manteniment i aprovisionament. Proporciona les facilitats i el personal requerit per a gestionar la xarxa.

open shortest path first *m* Protocol d'encaminament entre encaminadors dintre dels sistemes autònoms, millora l'antic protocol d'encaminament RIP.
sigla OSPF

OSPF *m* Vegeu *open shortest path first*.

SDH *m* Vegeu *synchronous digital hierarchy*.

SONET *m* Vegeu *synchronous optical network*.

synchronous digital hierarchy *m* Estàndard per a la transmissió de dades a través de la fibra òptica. SDH s'usa a Europa.
sigla SDH

synchronous optical network *m* Estàndard per a la transmissió de dades a través de la fibra òptica. SONET s'usa a Amèrica del Nord i parts d'Àsia.
sigla SONET

TDM *m* Vegeu *time division multiplexing*.

time division multiplexing *m* Tècnica en la qual la informació de diversos canals en un únic cable es pot assignar a una amplada de banda basat en espais de temps prèviament assignats. S'assigna l'amplada de banda de cada canal sense mirar si la estació està transmetent.
sigla TDM

UNI *m* Vegeu *user to network interface*.

user to network interface *m* Especificació de la interfície entre un sistema final i el sistema *backbone*.
sigla UNI

VC *m* Vegeu *contenedor virtual*.

xarxa d'àrea local *f* Grup de computadors i dispositius associats que comparteixen línies de comunicació i recursos dintre d'una àrea geogràfica petita.
sigla LAN

xarxa d'àrea metropolitana *f* Xarxa que connecta usuaris en una àrea superior a la LAN però inferior al que cobriria una xarxa d'àrea estesa.
sigla MAN

Bibliografia

Alwayn, V. (2001). *Advanced MPLS Design and Implementation*. Indianàpolis: Cisco Press.

Halabi S. (2003). *Metro Ethernet Forum*. Indianàpolis: Cisco Press.

McCabe, J. (2003). *Network Analysis, Architecture and Design*. San Francisco: Elsevier Science.

Metro Ethernet Forum
<http://www.metroethernetforum.org>

WAN Design Guide (2006, enero)
http://www.hp.com/rnd/pdfs/WANDesignGuide_lower_layers.pdf

