Disseny de xarxes WAN i noves tecnologies

PID_00268536

Pere Barberán Agut

Temps mínim de dedicació recomenanat: 7 hores

Universitat Oberta de Catalunya

Pere Barberán Agut

Enginyer de Telecomunicacions per la Universitat Politècnica de Catalunya. Professor de l'Escola Universitària Politècnica de Mataró, on forma part de l'àrea de Xarxes i Serveis. De 2005 a 2010 ha estat director del Departament de Telecomunicacions i Arquitectura de Computadors. Actualment responsable tècnic del laboratori de *networking* TCM NetLab a la Fundació Tecnocampus Mataró-Maresme.

La revisió d'aquest recurs d'aprenentatge UOC ha estat coordinada pel professor: Ferran Adelantado Freixer (2019)

Segona edició: setembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

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 plantegem 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 noves tecnologies. Comencem amb el protocol IP i la seva evolució a IPv6. Més endavant, s'intenta veure les diferents tendències actuals en xarxes metropolitanes i xarxes d'àrea estesa. En el primer cas s'explica com Ethernet actualment va més enllà de la xarxa local. En el cas de les xarxes d'àrea estesa s'expliquen, per una banda, els usos que se sol donar a la tecnologia MPLS i, per altra banda, una nova tendència cada cop més important com és el Software-Defined WAN (SD-WAN).

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 metropolitanes.

5. Estudiar les diverses tecnologies actuals en entorns metropolitans i justificar-ne l'evolució cap a les xarxes metropolitanes Ethernet.

6. Conèixer el funcionament bàsic del protocol IPv6 i en especial el seu adreçament.

7. Conèixer l'evolució més important de la tecnologia MPLS per a donar qualitat i servei.

8. Comprendre el nou enfocament basat en menys maquinari per a implementar les xarxes WAN mitjançant SD-WAN.

1. Disseny de xarxes

1.1. Introducció al disseny de xarxes WAN

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

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?

VoIP són les sigles de veu sobre tecnologia IP.

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".

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.

Temps de convergència

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

- **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.

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.
- 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 predictible, consistent en rendiment, fiable i escalable.

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.

2. 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.

2.1. 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: el servei de NAT

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.

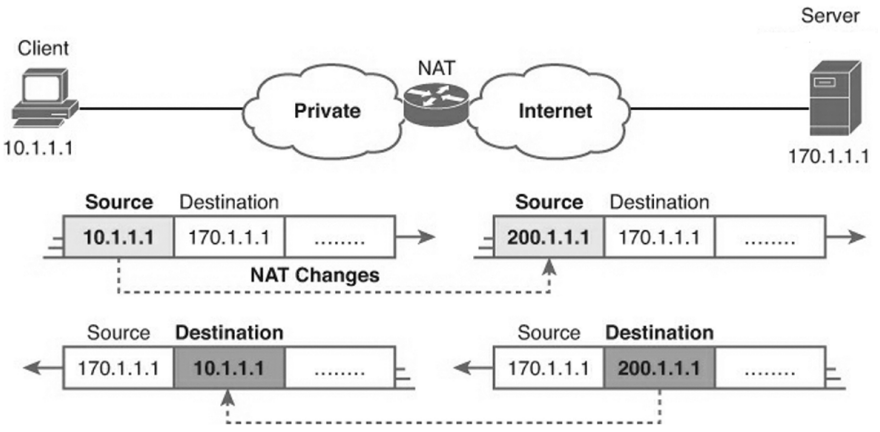
El mecanisme per a traslladar les adreces privades a públiques pot ser per mitjà de NAT o PAT.

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

Network Address Translation (NAT), conjuntament amb Classless Interdomain Routing (CIDR), és un protocol dissenyat per a l'estalvi i optimització en l'assignació d'adreces IP. Inicialment, NAT estava pensat per a reduir l'esgotament de l'espai d'adreces IP disponibles, i permetia que múltiples adreces IP privades poguessin ser representades per un grup molt més petit d'adreces públiques. Així, sense solucions com NAT, l'espai d'adreces s'hauria esgotat del tot a mitjan dècada de 1990 i internet no hauria pogut continuar creixent.

El servei NAT, definit al RFC 3022, permet que un equip que no té una adreça IP vàlida registrada es pugui comunicar per mitjà d'internet. Bàsicament, NAT mapeja un grup d'adreces en un altre grup d'adreces de manera transparent per a l'usuari. D'aquesta manera, permet que xarxes IP privades amb adreces IP no registrades es puguin connectar a internet. NAT treballa als encaminadors i converteix o tradueix les adreces privades que hi ha a la xarxa interna privada en adreces públiques, abans que els paquets surtin cap a la xarxa exterior.

Figura 1. Mapatge d'adreces IP de la xarxa privada a internet



Si ens fixem en la figura anterior, podem veure com l'encaminador efectua NAT canviant l'adreça IP origen del paquet (10.1.1.1) i transformant-la en una altra adreça, en aquest cas 200.1.1.1, quan aquest deixa la xarxa privada de l'organització. De la mateixa manera, l'encaminador torna a efectuar NAT i canvia l'adreça destí del paquet (200.1.1.1) quan aquest torna del servidor cap a la xarxa privada (10.1.1.1).

Però, NAT no només és beneficiós per aquest motiu. Altres avantatges que ofereix NAT poden ser els següents:

- Estalvi d'adreces IP: permet disminuir el nombre d'adreces IP necessàries.
- Flexibilitat: possibilitat de canviar de proveïdor d'internet sense haver de canviar les adreces de tota la nostra xarxa.
- Permet solucionar problemes de solapament d'adreces.
- Evita que els *hosts* de la xarxa externa vegin les adreces internes. De tota manera, NAT no és un mètode per a tenir seguretat a la xarxa privada.

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

- Augment de la latència.
- Dificultats de monitorització.
- Pèrdua de funcionalitats. Potser alguna aplicació no funciona amb el NAT activat.

Terminologia basada en funció de la localització del dispositiu

Quan es realitza NAT es fa servir la notació següent en funció d'on es trobi el paquet i quins en siguin l'origen i el destí:

- **Adreça local interna:** l'adreça IP assignada a un *host* de la xarxa interna, de manera estàtica o per mitjà d'una assignació dinàmica DHCP.

- **Adreça global interna:** adreça IP de la xarxa externa, normalment proporcionada pel proveïdor d'internet, que pot representar una o més adreces IP locals, en funció del tipus de NAT que realitzem. Ho tractarem en l'apartat següent.

- **Adreça local externa:** l'adreça IP d'un *host* extern tal com apareix a la xarxa interna. No cal que sigui l'adreça legítima.

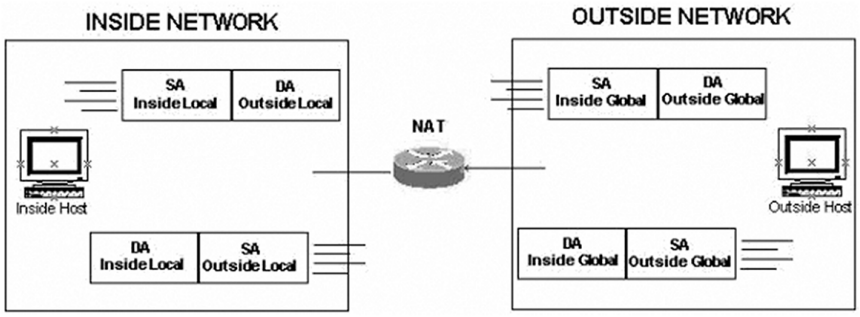
- **Adreça global externa:** l'adreça assignada a un *host* a la xarxa externa pel propietari del *host*.

Cal tenir present que els termes *interna* i *externa* són definicions de NAT. Les interfícies d'un encaminador NAT es defineixen com internes i externes amb els comandaments de configuració NAT del dispositiu. Així, les xarxes amb les quals es connecten aquestes interfícies es poden definir com a xarxes internes o com a xarxes externes:

- **Adreça local:** una adreça local és qualsevol adreçament que aparegui a la part interna de la xarxa.

- **Adreça global:** una adreça global és qualsevol adreçament que aparegui a la part exterior de la xarxa.

Figura 2. Exemple de notació. SA (*Source Address*) és l'adreça origen i DA (*Destination Address*) és l'adreça destí



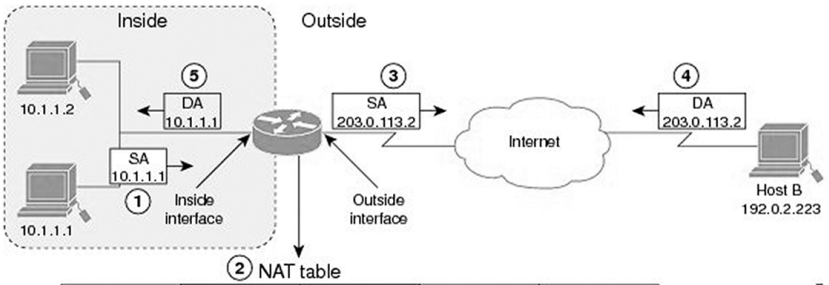
Els paquets originats a la part interna de la xarxa tenen una adreça local interna com a adreça origen, i adreça local externa com a adreça destí del paquet, mentre aquest paquet no surti de la part interna de la xarxa. Un cop aquest paquet ha estat commutat cap a l'exterior, l'adreça origen es coneix com a adreça global interna i el destí del paquet es coneix com a adreça global externa.

Inversament, quan un paquet és originat a la part exterior de la xarxa, la seva adreça origen es coneix com a adreça global externa mentre és a la xarxa externa. El destí del paquet es coneix com a adreça global interna. Per al mateix paquet, un cop commutat a la xarxa interna, l'adreça origen s'anomena adreça local externa i l'adreça destí del paquet es coneix com a adreça local interna.

Hi ha tres possibilitats a l'hora de fer el NAT. A continuació mostrarem els diferents tipus bàsics de NAT que hi ha:

1) NAT estàtic. Com indica el nom, el NAT estàtic fa un mapatge estàtic de cada adreça IP privada amb una adreça IP pública, de manera que cada cop que una adreça IP concreta de la xarxa privada surti cap a internet tindrà assignada la mateixa adreça IP pública.

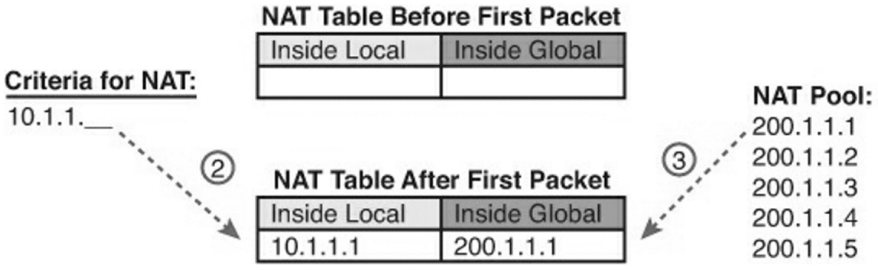
Figura 3. Exemple de funcionament de NAT estàtic



A l'exemple de la figura l'empresa té assignades les IP públiques del rang 203.0.113.0 /24. L'usuari de la xarxa interna 10.1.1.1/24 vol obrir una connexió amb el *host* B, que es troba a l'exterior. Quan l'encaminador rep el primer paquet de 10.1.1.1, aquest examina la seva taula de traducció d'adreces (NAT). Com que es treballa amb NAT estàtic, l'encaminador canvia l'adreça IP local interna 10.1.1.1 per l'adreça global 203.0.113.2 i commuta el paquet. El *host* B rep el paquet i respon al *host* 10.1.1.1 mitjançant l'adreça destí global interna (DA) 203.0.113.2. Quan l'encaminador rep el paquet de resposta amb l'adreça global interna, fa una cerca a la taula NAT. Llavors, trasllada l'adreça a l'adreça local interna i reenvia el paquet al *host* 10.1.1.1.

2) NAT dinàmic. El NAT dinàmic és similar al NAT estàtic, però amb alguna diferència. En el cas estàtic hi ha un mapatge previ un a un entre les adreces privades (adreces locals internes) i les adreces públiques (adreces globals internes). En el cas del NAT dinàmic això no és previ i es fa dinàmicament. Es defineix un grup d'adreces IP privades que poden sortir i un grup d'adreces públiques que cal assignar. L'assignació es fa en el moment que arriba un paquet de la xarxa interna a l'encaminador i aquest vol sortir cap a internet.

Figura 4. NAT dinàmic



A la figura es veu que l'equip amb adreça IP: 10.1.1.1 envia el primer paquet en direcció a internet. En aquest cas se li assigna dinàmicament l'adreça pública 200.1.1.1. Aquesta entrada dinàmica a la taula es mantindrà mentre hi hagi trànsit d'aquest usuari cap a l'exterior.

En aquest tipus de configuració podem tenir més adreces internes que adreces públiques. En el cas que l'encaminador hagi assignat totes les adreces públiques i li arribi un paquet d'un nou usuari intern que vol sortir a internet, l'encaminador descartarà el paquet. Si volem evitar aquest problema amb NAT dinàmic l'única solució és que el nombre d'adreces públiques sigui tan gran com el grup d'adreces privades que puguin sortir.

3) Port Address Translation (PAT)

Hi ha fabricants que anomenen la traducció d'adreces per port (PAT) *overloading*.

Port Address Translation soluciona el problema que s'ha vist en el cas de NAT estàtic o dinàmic, en què calen tantes adreces públiques com privades. PAT suporta que hi hagi molts clients privats que surten a internet a través de poques o fins i tot una sola adreça IP pública.

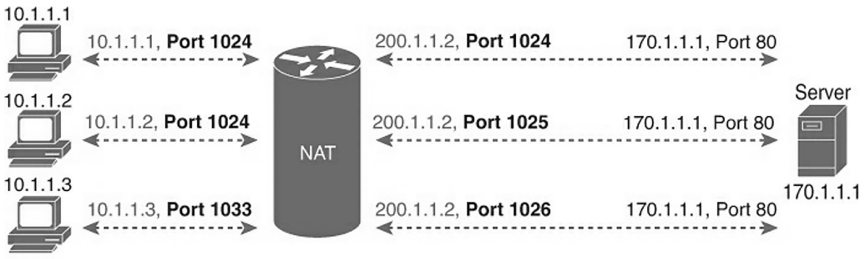
Per a entendre PAT cal recordar abans el concepte de connexió TCP entre dos dispositius.

Figura 5. Exemple de connexió TCP/IP

Si ens fixem en la figura anterior, cada connexió és fixada per una IP origen, un port origen, una IP destí i un port destí. Si aquestes connexions estan iniciades des d'un mateix origen i van cap a un mateix destí l'assignació de diferent port origen aconsegueix que no hi hagi dues connexions iguals.

PAT aprofita aquest fet a l'encaminador, en el qual no només es fa un mapatge de l'adreça, sinó també del port. D'aquesta manera s'aconsegueix que, encara que el mapatge entre adreces privades es faci sempre amb la mateixa IP pública, l'encaminador pugui diferenciar cadascun dels mapatges realitzats mitjançant el port.

Figura 6. PAT entre adreces 10.1.1.0 /24 amb adreça pública 200.1.1.2



Inside Local	Inside Global
10.1.1.1: **1024**	200.1.1.2: **1024**
10.1.1.2: **1024**	200.1.1.2: **1025**
10.1.1.3: **1033**	200.1.1.2: **1026**

A la figura es mostra un exemple de com quedaria la taula PAT de l'encaminador. Si ens fixem en els equips 10.1.1.1 i 10.1.1.2, inicialment tots dos tenen el mateix port origen. En fer NAT, tots dos tenen la mateixa IP global interna. Per tal de diferenciar-los, l'encaminador canvia el port origen de la segona connexió. L'usuari 10.1.1.1:1024 passa a tenir l'adreça global interna 200.1.1.2:1024 mentre que l'usuari 10.1.1.2:1024 passa a tenir l'adreça global interna 200.1.1.2:1025.

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.

2.2. 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

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.

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. Es 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*

Subnetting

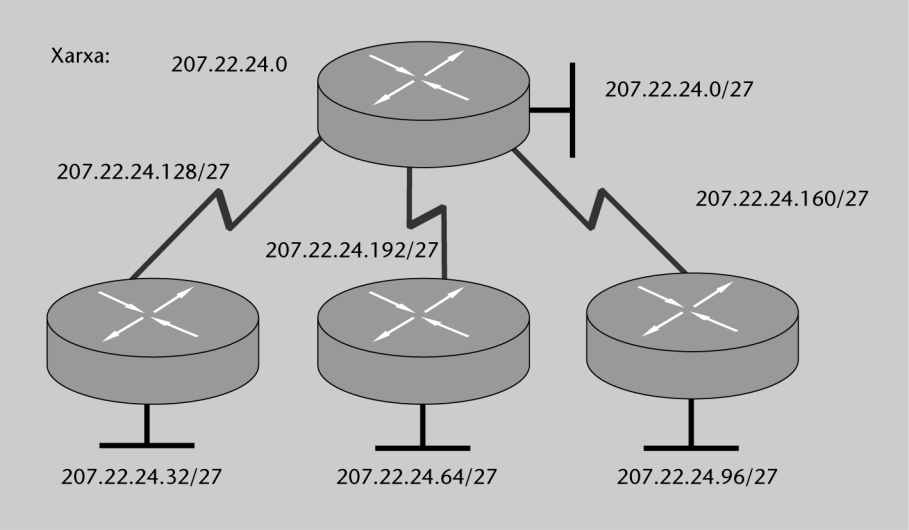
A partir d'una adreça amb classe el *subnetting* ens permet fer xarxes més petites totes amb la mateixa màscara (màscara de longitud fixa).

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 7, 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 7.

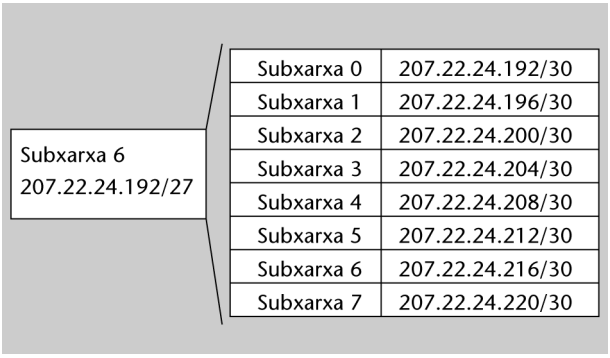
Figura 7. Topologia amb *subnetting*



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 8.

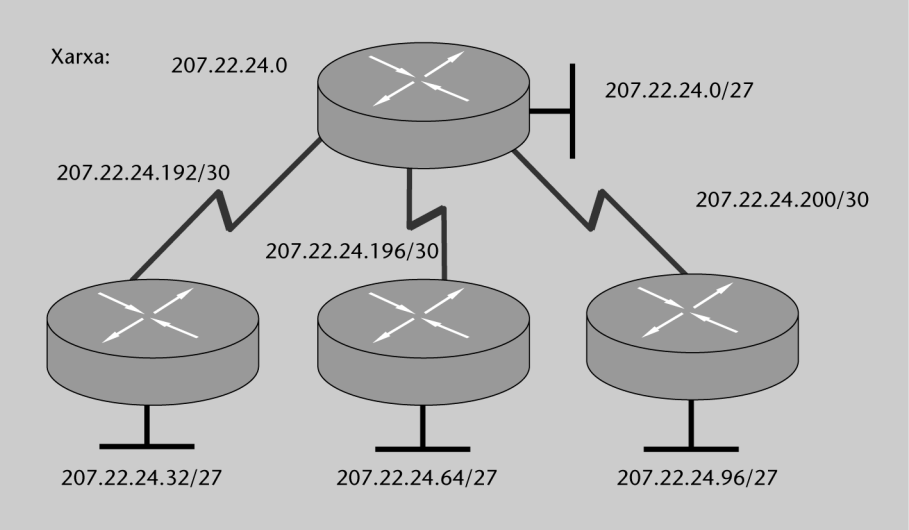
Figura 8. Exemple de VLSM



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 9.

Figura 9. Topologia aplicant VLSM



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

2.3. 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.

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 troncals continuïn funcionant, ja que se n'han reduït les taules d'encaminament.

Aconseguim 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 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 complerta.

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**	**00011**000	00000000	00000000
172.25.0.0/16	**10101100**	**00011**001	00000000	00000000
172.26.0.0/16	**10101100**	**00011**010	00000000	00000000
172.27.0.0/16	**10101100**	**00011**011	00000000	00000000
172.28.0.0/16	**10101100**	**00011**100	00000000	00000000
Adreces classe B consecutives. 13 bits comuns				
Adreça	**Primer octet**	**Segon octet**	**Tercer octet**	**Quart octet**
172.29.0.0/16	**10101100**	**00011**101	00000000	00000000
172.30.0.0/16	**10101100**	**00011**110	00000000	00000000
172.31.0.0/16	**10101100**	**00011**111	00000000	00000000

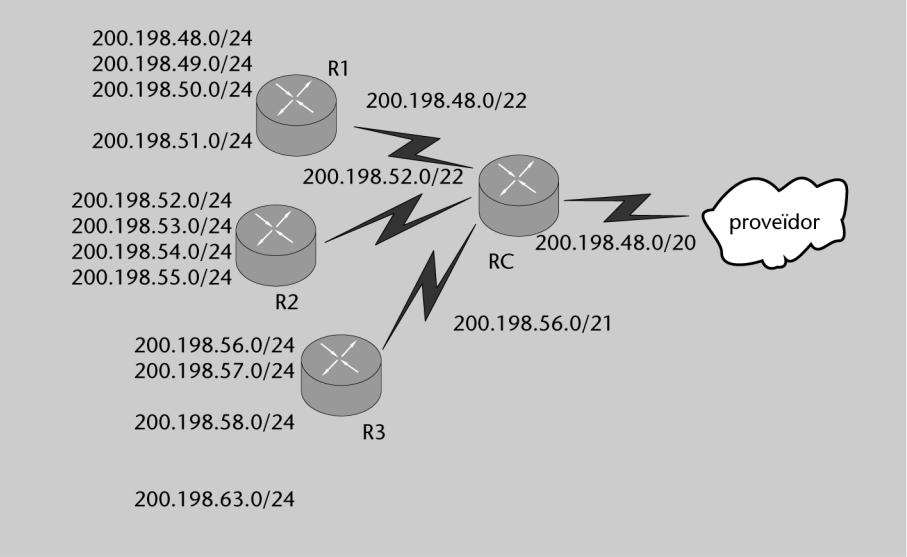
D'aquesta manera, l'encaminador pot sumaritzar aquestes vuit adreces amb una adreça única amb un prefix de 13 bits: 1010110000011

Obtenim l'adreça sumaritzada: 172.24.0.0/13

Exemple de sumarització aplicada a topologia de xarxa completa

En la figura 10 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 10. Sumarització de rutes



En la figura 10 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.

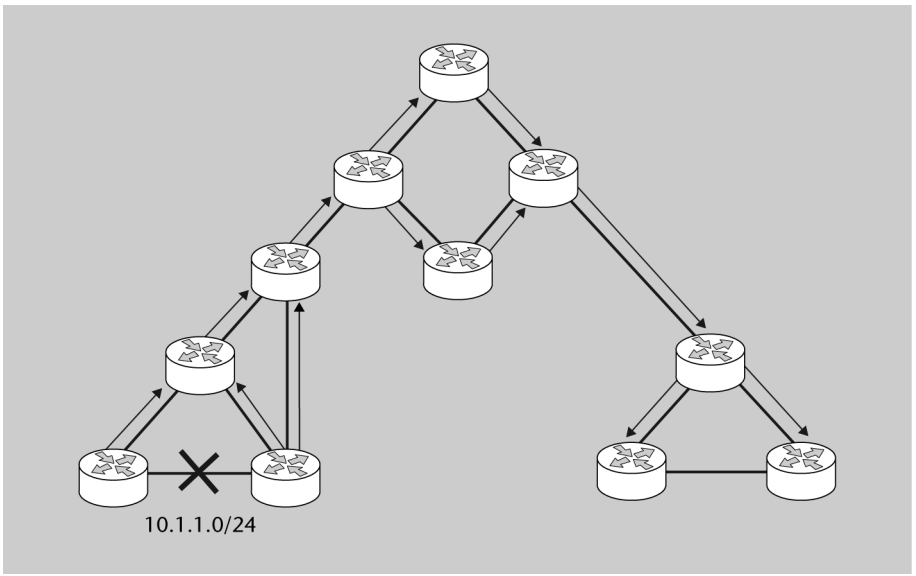
- **Agregació de rutes**. Redueix les taules d'encaminament i millora l'estabilitat i l'escalabilitat. Per a fer-ho, cal dividir la xarxa en grups IP que siguin contigus.

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 11). 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 11. Un adreçament incorrecte pot provocar un excés de trànsit d'encaminament



Alguns dels efectes que provoca un disseny dolent són:

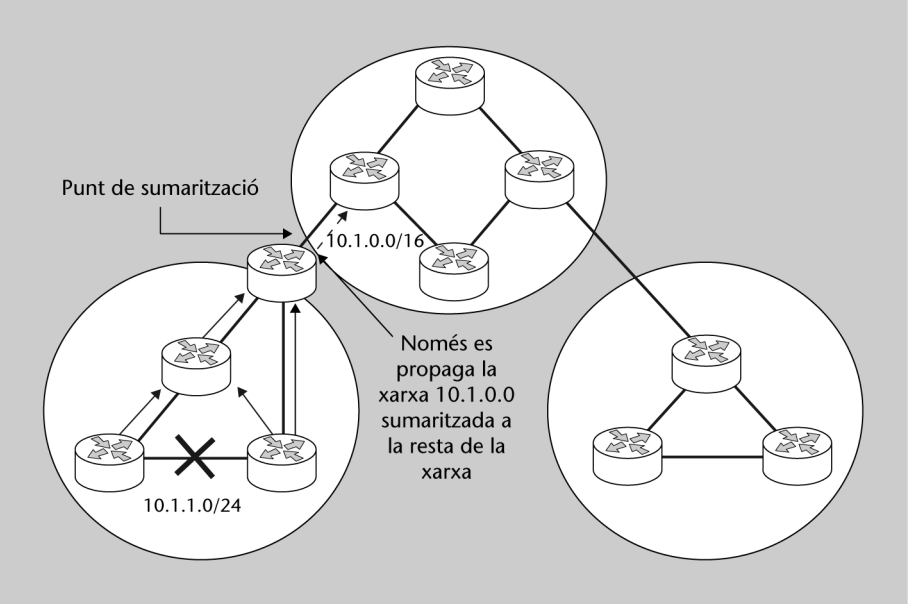
L'excés de trànsit d'encaminament consumeix amplada de banda. Quan hi ha un canvi en una ruta, els encaminadors s'envien actualitzacions. Sense sumarització hi ha més actualitzacions i més consum d'amplada de banda.

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 12. 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. Aconseguim, 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.

2.4. Conceptes sobre l'encaminament IP

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

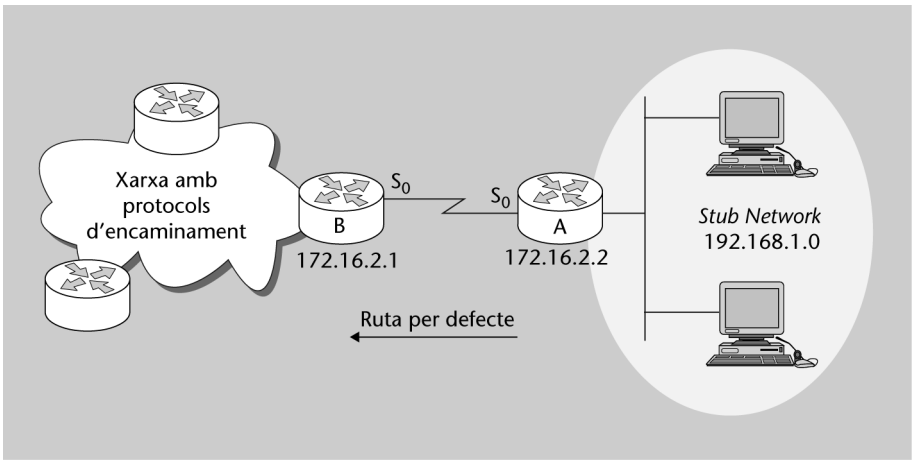
1) **Encaminament estàtic**. Apropiat en les circumstàncies següents:

- Enllaços amb molt 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 13. *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 discontínues o la possibilitat de configurar sumarització de rutes. Es pot dir que aquests protocols no són adequats per a les xarxes modernes.

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.

- **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.

Adreça recomanada

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

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*.

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 estandarditzat per Intenet Enginneering 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. Actu-

alment, 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 × amplada_de_banda) + (k2 × amplada_de_banda) / (256 – càrrega) + (k3 × retard)

Hi ha un paràmetre k5; si és diferent de 0, llavors l'expressió queda:

Mètrica = mètrica × k5 / (fiabilitat + k4)

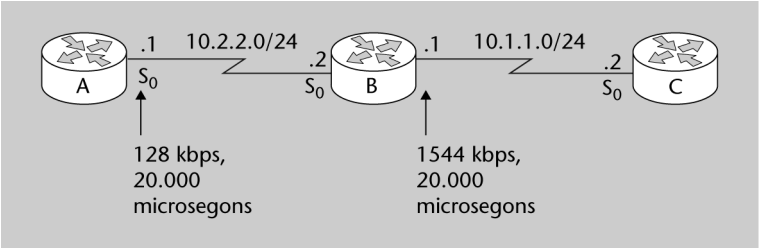
En general k1 = k3 = 1 i k2 = k4 = k5 = 0.

En aquest cas l'expressió és:

Mètrica = amplada_de_banda + 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 14. 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:

- Amplada_de_banda = (10000000/1544) × 256 = 1658031
- Retard = (20000/10) × 256 = 512000
- 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:

- Amplada_de_banda = (10000000/128) × 256 = 20000000 (considerant l'amplada de banda menor dels dos enllaços)
- Retard = ((20000 + 20000)/10) × 256 = 1024000
- 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 informa

ció 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.

3. IPv6

3.1. Introducció

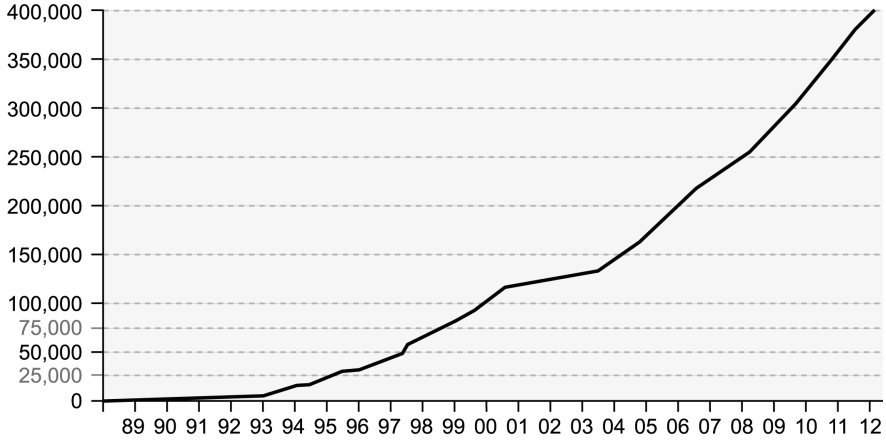
Internet Protocol versió 6 (IPv6) ha estat dissenyat com a successor del protocol IPv4. No cal explicar el ràpid creixement d'internet durant els últims anys que ha fet que avui en dia internet sigui molt més que un conjunt de pàgines web, serveis de correu electrònic o transferència de fitxers. S'ha produït un creixement del nombre de dispositius mòbils, les connexions *peer to peer*, jocs en xarxa, etc., cosa que fa que passem de l'internet dels ordinadors a l'internet de les coses.

Aquest creixement no va ser previst en el disseny inicial i, per tant, han sorgit problemes als quals cal fer front. Els principals problemes d'IPv4 són els següents:

- L'espai d'adreces IPv4 és insuficient per a adreçar la quantitat de dispositius connectats.

- Els encaminadors de la xarxa troncal (*backbone network*) d'internet mantenen un nombre excessiu d'entrades a les seves taules d'encaminament. Això és degut a la mala planificació a les fases inicials d'IPv4, de manera que hi ha blocs d'adreces IP que estan assignats de manera discontínua. Això dificulta la convergència de rutes.

Figura 15. Evolució de la mida de les taules BGP (1989-211)



A la figura anterior es mostra el creixement del nombre de xarxes a les taules d'encaminament a internet en el període entre 1989 i 2012. Si ens hi fixem, el creixement és especialment intens a partir de 1990.

- IPv4 no ajuda a solucionar els problemes de seguretat, cada vegada més importants.

S'han desenvolupat algunes solucions que resolen el problema de la manca d'adreces a curt termini, tal com ja hem vist anteriorment amb CIDR i NAT, però no representen una solució definitiva del problema.

3.1.1. Avantatges d'IPv6

- Estructura d'adreces de 128 bits que garanteix un espai d'adreçament suficient en comparació als 32 bits de les adreces IPv4. La disponibilitat d'un nombre quasi il·limitat d'adreces IP és el benefici més convincent per a implementar les xarxes IPv6. Passem de tenir $4{,}3 \cdot 10^9$ adreces disponibles a tenir-ne $(4{,}3 \cdot 10^9)^4$.

- Capçalera simplificada. La simplificació de la capçalera millora el rendiment alhora que fa més eficient l'encaminament; no utilitza suma de verificació (*checksum*); i l'extensió de capçalera és més senzilla i eficient.

- Elimina els *broadcast*: IPv6 no fa servir el *broadcast* de nivell 3. En comptes, treballa amb adreces *multicast*.

- Suport per a mobilitat i seguretat.

- Diversos mecanismes de transició d'IPv4 a IPv6.

- A més, incorpora altres avantatges com són:

– permet agregar prefixos que són anunciats a les taules d'encaminament
– és més fàcil de gestionar pel fet d'estar connectat a més d'un proveïdor d'internet
– permet l'autoconfiguració que inclou les adreces *link-layer* per disposar de la funcionalitat *plug and play* i la comunicació extrem a extrem sense necessitar NAT

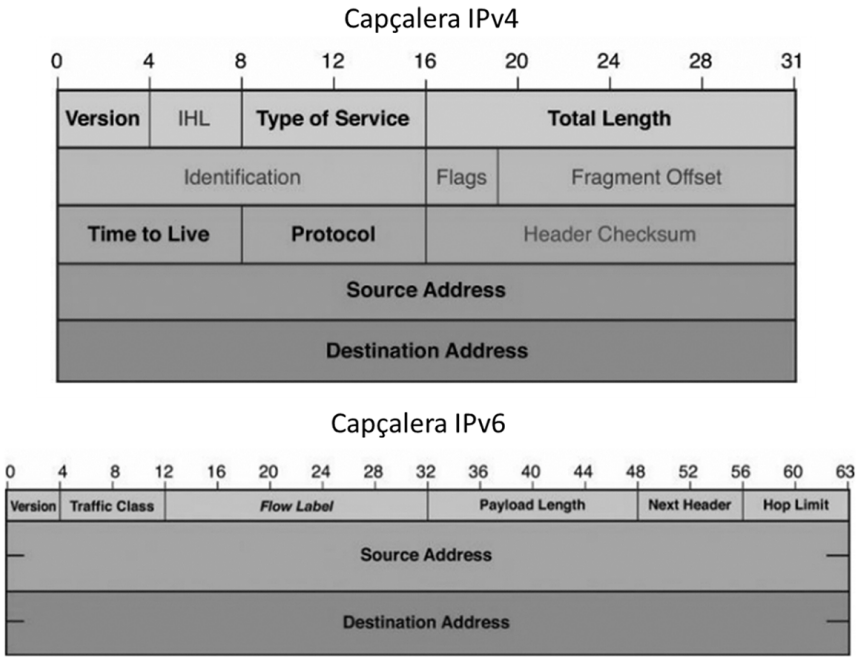
3.2. El protocol IPv6

Ja s'ha comentat que les adreces d'IPv6 són de 128 bits, la qual cosa fa que no tinguem cap problema pel que fa al nombre d'adreces. Malgrat això, cal tenir present que aquest increment en el nombre de bits fa que augmenti la mida de la capçalera IPv6, ja que passem de 64 bits pel camp d'adreces (32 bits de l'adreça origen i 32 bits de l'adreça destí) a 256 bits a IPv6 (128 bits per a cada adreça, la d'origen i la de destí).

3.2.1. Capçalera IPv6

La capçalera IPv6 té 40 octets, a diferència de la capçalera d'IPv4, que té 20 octets, tal com es mostra a la figura següent:

Figura 16. Capçalera IPv4 respecte a IPv6



IPv6 té menys camps, i la seva mida és múltiple de 64 bits per tal de millorar l'eficiència i la velocitat de processament. Els camps d'IPv6 s'expliquen a continuació:

- **Versió (*Version*) (4 bits):** camp de quatre bits similar al de la capçalera d'IPv4. Aquest camp té un valor de 6 per a indicar que es tracta de la versió 6 del protocol.

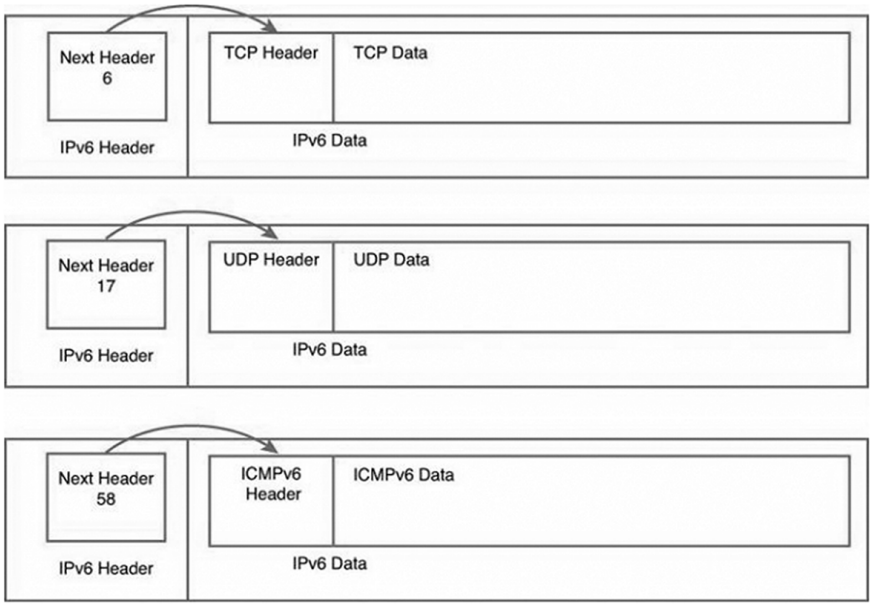
- **Classe de trànsit (*Traffic class*) (8 bits):** és similar al camp d'IPv4 anomenat tipus de servei (ToS). Etiqueta els paquets en serveis diferenciats de qualitat de servei. En disposar de 6 bits per a indicar el DSCP (*Differentiated Service Code Point*), permet una granularitat molt més gran en el marcatge respecte de l'existent a IPv4, que només disposava de 3 bits. A la figura es mostra en detall aquest camp tant per a IPv4 com per a IPv6.

- **Etiqueta de flux (*Flow Label*):** camp de 20 bits. El pot usar l'origen del paquet per a etiquetar el paquet com a part d'un flux específic, de manera que permet als encaminadors i *switchs* de nivell tres gestionar aquest trànsit com a part d'un flux, en comptes de fer-ho paquet per paquet. Això permet una commutació més ràpida.

- **Longitud de la càrrega (*Payload length*):** 16 bits similars als d'IPv4.

- **Següent capçalera (*Next Header*):** camp de 8 bits que indica el tipus d'informació que ve a continuació de la capçalera. A la figura següent es mostren tres exemples de com funciona aquest camp. Si el valor de *Next Header* és igual a 6, es tracta de TCP; si el valor és 17, es tracta d'UDP, i si el valor és 58, aleshores es tracta d'ICMP.

Figura 17. Camp *Next Header*



- **Límit de salts (*Hop límit*):** camp de 8 bits que indica el nombre màxim de salts que un paquet pot passar. És similar al temps de vida (TTL) d'IPv4 i cada encaminador en fa decréixer el valor en un. En no disposar de suma de verificació no cal recalcular-ne el valor.

- **Adreça origen:** camp de 128 bits que identifica l'origen del paquet.

- **Adreça destí:** camp de 128 bits que identifica el destinatari del paquet.

Si comparem les capçaleres d'IPv4 i d'IPv6 podem concloure el següent:

- Es manté el camp de Versió a ambdós protocols amb el mateix nombre de bits.

- Passem d'adreces de 32 bits a IPv4 a adreces de 128 bits a IPv6, tal com ja s'ha indicat.

- El camp Tipus de servei (*Type of Service*) a IPv4 passa a ser el camp Classe de servei (*Traffic Class*) a IPv6, amb un major nombre de bits per a diferenciar serveis.

- El camp Longitud total (*Total length*) definit a IPv4 inclou la longitud de les dades i de la capçalera, mentre que el camp Longitud de càrrega útil (*Payload length*) a IPv6 només inclou la part de dades.

- El Temps de vida (*Time to Live*) a IPv4 passa a ser Límit de salts (*Hop Limit*) a IPv6, tot i que manté la mateixa funcionalitat.

- El camp Protocol (*Protocol*) d'IPv4 passa a ser el camp Capçalera següent (*Next Header*), també amb la mateixa funcionalitat.

- A IPv6 s'han eliminat els camps següents: longitud de la capçalera (*Internet Header Length*), Identificador (*Identification*), Banderes (*flags*), Offset del fragment (*Fragment offset*), suma de verificació, opcions (*options*), farciment (*padding*).

- S'ha inclòs el camp Etiqueta de flux (*flow label*).

Una última característica interessant que incorpora IPv6 respecte a IPv4 és el que s'anomena Descobriment de l'MTU. IPv4 ha de tractar amb la possibilitat de fragmentació de paquets en l'encaminament des de l'origen fins al destí. IPv6 ja no realitza fragmentació. Per a aconseguir-ho, utilitza un procés de descobriment que li permet determinar l'MTU òptim que cal fer servir durant una sessió determinada. En aquest procés de descobriment, el dispositiu origen intenta enviar un paquet (paquet de descobriment) amb la mida especificada per la seva capa superior (capa de transport). Si rep un missatge IMCP on se li indica que el paquet és massa gran, torna a repetir el procés, però amb un paquet de descobriment amb MTU més petita. Aquest procés el repetirà fins que el destinatari li enviï un paquet de resposta de descobriment que indiqui que ha arribat correctament.

3.2.2. Estructura de les adreces IPv6

Com s'ha dit, l'adreça IPv6 és un conjunt de 128 bits dividit en grups de 16 bits expressat en hexadecimal. Els grups de 16 bits estan separats per dos punts (:). Una adreça IPv6, per tant, té la forma següent:

X : X : X : X : X : X : X : X

On cada X representa 4 nombres hexadecimals de manera que la X pot prendre valors que van de 0000 fins a FFFF. Els nombres hexadecimals poden estar expressats en majúscula i minúscula. Així, una adreça IPv6 pot ser, per exemple:

FDEC:BA58:5678:3210:FDEC:BC98:7654:3210

L'adreça es pot simplificar si hi ha zeros consecutius dintre de l'adreça i s'expressa com a (::). Vegem-ne algun exemple:

1080:0:0:0:8:800:200c:417a és equivalent a 1080::8:800:200c:417a

Altres exemples de simplificació o equivalències:

Adreça	Adreça equivalent
FF01:0:0:0:0:0:0:101	FF01::101
0:0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0:0	::

En canvi, si tenim l'adreça 2001:0:0:0012:0:0:1234:5456, aleshores no es pot fer

2001::0012::1234:5456. El motiu és que en aquest cas no podem saber quants zeros han estat eliminats en cadascun dels dos conjunts. Així, l'expressió reduïda hauria de ser, per exemple: 2001::0012:0:0:1234:5456.

Exercici

Expressa de manera comprimida les adreces següents:

a) 2001:0db8:0000:0000:0000:0000:0000:0c50

b) 2001:0db8:0000:0000:b450:0000:0000:00b4

Solució:

a) En aquest cas podem simplificar els zeros intermedis i quedarà:

2001:db8::c50

b) En aquest segon cas no es pot fer com a l'apartat a) ja que, com s'ha explicat, no sabríem quants zeros hem eliminat a cada conjunt. La solució llavors serà:

2001:db8::b450:0000:0000:b4

Prefix

De manera similar a IPv4, els prefixos a IPv6 segueixen el format següent:

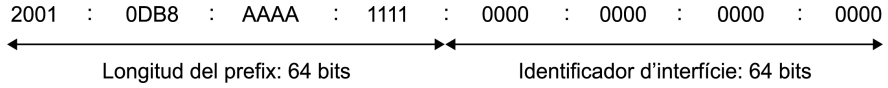
adreça IPv6 / longitud del prefix

La longitud del prefix és un nombre decimal que indica la part de xarxa de l'adreça.

Amb aquesta notació tindrem, per exemple, per a l'adreça:

2001:0BD8:AAAA:1111:0000:0000:0000:0000 / 64

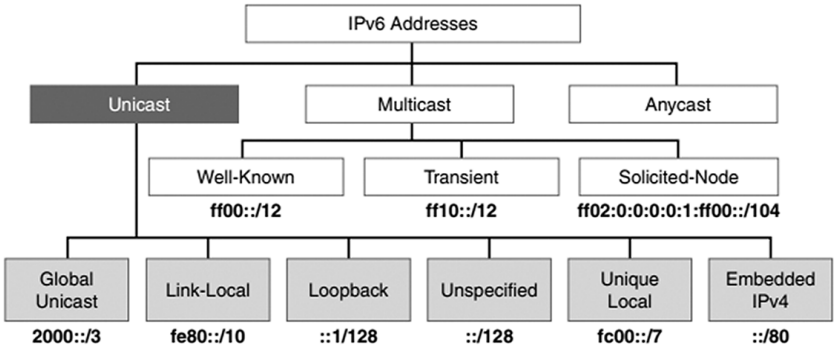
Figura 18.



3.3. Tipus d'adreces

Si ho recordem, a IPv4 disposem d'adreces *unicast*, *broadcast* i *multicast*. En el cas d'IPv6 aquestes tres possibilitats es modifiquen i s'introdueixen les adreces *anycast*. A més, a IPv6 s'han eliminat les adreces *broadcast*. Mirem el funcionament de cadascun dels tipus d'adreces:

- ***Unicast:*** els paquets enviats a una adreça *unicast* es transmeten a una única interfície. Una interfície pot tenir diverses adreces IPv6, a més d'una adreça IPv4. Al gràfic següent es mostren els diferents tipus d'adreces, tot destacant les diverses opcions per al cas d'*unicast*. D'aquestes possibilitats les dues més importants són: adreça *unicast* global (*global unicast address*) i adreça d'enllaç local (*link-local address*).



Diferents tipus d'adreces a IPv6

- **Adreces *multicast:*** com sabem, el *multicast* permet que un usuari enviï un paquet a diferents destinataris simultàniament. Una adreça *multicast* defineix un grup de dispositius conegut com a grup *multicast*. IPv6 fa servir el prefix ff00::/8 per a les adreces *multicast* de manera equivalent a les adreces 224.0.0.0/4 utilitzades en IPv4. Cal recordar que una adreça origen mai no pot ser *multicast*. A més, tal com s'ha dit, IPv6 no disposa d'adreces *broadcast*.

- **Adreces *anycast*:** una adreça *anycast* és una adreça que pot ser assignada a més d'una interfície (normalment diferents dispositius). És a dir, múltiples dispositius poden tenir la mateixa adreça *anycast*. Un paquet enviat a una adreça *anycast* s'encamina a la interfície més propera que tingui aquesta adreça, segons la taula d'encaminament de l'encaminador.

Les adreces *anycast* utilitzen el mateix rang d'adreces que les adreces globals *unicast*. Cada dispositiu participant es configura amb la mateixa adreça *anycast*. Així, per exemple, podem tenir tres servidors DHCPv6. Tots tres tenen la mateixa adreça *anycast*. L'encaminador més proper al client reenviarà la petició al servidor «més proper» identificat a la seva taula d'encaminament. Les adreces *anycast* no s'han de fer servir com a adreces origen dels paquets IPv6.

A continuació, explicarem amb més detall cadascuna d'elles.

3.3.1. Les adreces *unicast* globals

Les adreces *unicast* globals (2000::/3) són les adreces públiques i es poden encaminar a internet. Són equivalents a les adreces públiques IPv4. Les adreces globals comencen a l'adreça 2000::/3.

A la figura següent es veu com s'estructuren les adreces *unicast*. L'adreça *unicast* global es pot dividir en tres parts:

- **Prefix d'encaminament global (*Global Routing Prefix*):** és la part de xarxa de l'adreça assignada pel proveïdor. Aquest prefix és equivalent a la part de xarxa de les adreces IPv4 i és la part que els encaminadors examinen per a decidir per quin port de sortida commuten els paquets que els arriben.

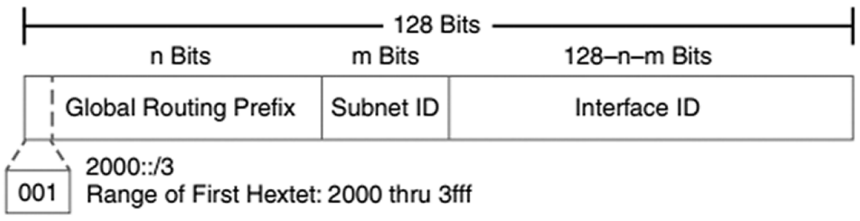
- **ID de subxarxa (*Subnet ID*):** a diferencia d'IPv4, on la part de subxarxa l'obteníem agafant uns bits de la part de *host*, a IPv6 l'identificador de subxarxa és un camp separat i no s'agafa de la part de *host*. Serveix com a IPv4 per a crear diferents subxarxes dintre d'una organització, seu, departament, etc.

- **Identificador d'interfície (*Interface ID*):** identifica la interfície dintre de la subxarxa.

A la figura següent es poden veure les tres parts en què es divideix una adreça *unicast* global.

Una diferència important amb IPv4 és que a IPv6 són legals les adreces on a la part del *host* hi té tot zeros o tot uns.

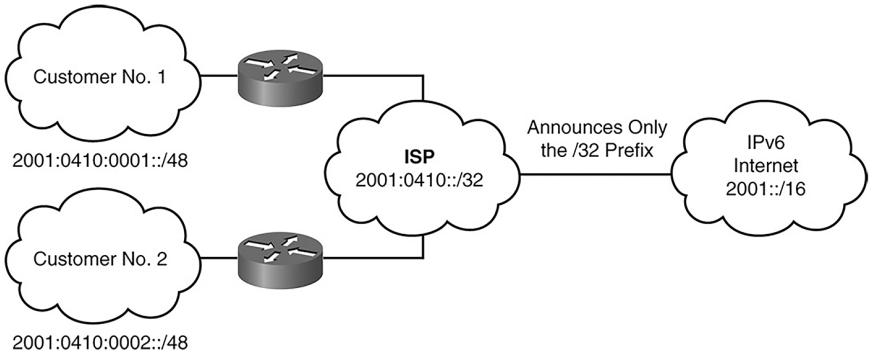
Figura 19. Adreça *unicast* global



L'estructura de les adreces *unicast* globals permet l'agregació de prefixos d'encaminament, de manera que el nombre d'entrades a les taules d'encaminament global es pot reduir.

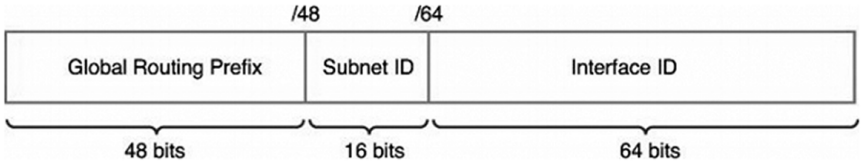
Les adreces *unicast* globals que es fan servir als enllaços s'agreguen cap amunt a través de les organitzacions i, finalment, als proveïdors (ISP).

Figura 20. Exemple d'agregació de prefixos



L'adreça *unicast* global està formada en general per un prefix d'encaminament global de 48 bits, 16 bits d'identificador de subxarxa, i 64 bits d'identificador d'interfície.

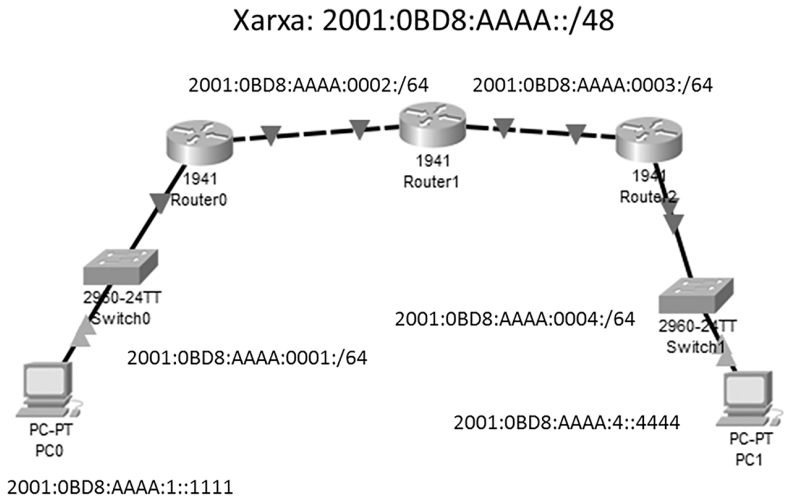
Figura 21. Estructura típica d'una adreça global unicast



Una manera fàcil d'identificar cadascuna de les parts en cas que sigui una adreça típica és la regla 3-1-4, on tenim 3 grups de 16 bits que identifiquen el prefix d'encaminament global, 1 grup que identifica la subxarxa i 4 grups que identifiquen la interfície.

A la topologia següent es mostra un exemple d'adreçament:

Figura 22. Topologia IPv6



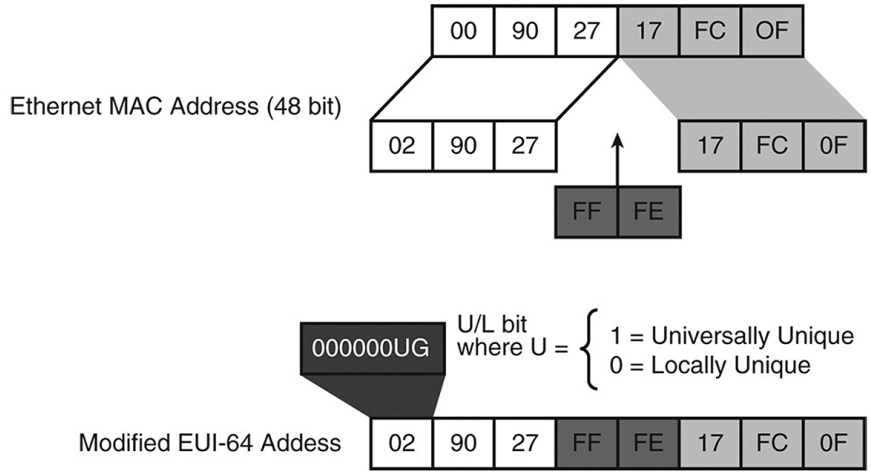
A la figura anterior tenim inicialment una adreça de xarxa /48 que indica el prefix d'encaminament global. A partir d'aquesta adreça s'han creat quatre subxarxes /64, les quals mantenen el prefix global 2001:0BD8:AAAA i es diferencien mitjançant els 16 bits de subxarxa.

Un aspecte important que cal destacar és la part d'identificador d'interfície. L'identificador d'interfície (ID) a IPv6 serveix per a identificar una interfície única en un enllaç. Quan l'identificador d'interfície deriva directament de l'adreça del nivell d'enllaç de la interfície, l'abast d'aquest identificador se suposa que és global.

Els identificadors d'interfícies són sempre de 64 bits i es creen de manera dinàmica d'acord amb el nivell 2 del medi i l'encapsulament.

En el cas, per exemple, d'Ethernet, l'ID es crea a partir de l'adreça MAC de la interfície. El que es fa és inserir el nombre hexadecimal FFFE entre els tres bytes de més pes de l'adreça MAC i els tres de menys pes.

Figura 23. Identificador d'interfície en el cas Ethernet



A més, el segon bit del byte de més pes de l'adreça MAC es posa a 1 per a indicar que l'adreça és única. Com es veu a la figura aquest bit s'indica com a *U*.

A la figura següent es mostra com queda l'identificador d'interfície IPv6 en el cas concret d'una interfície Fast Ethernet en un PC. Tal com s'ha explicat, es genera a partir de l'adreça MAC del dispositiu i amb el prefix FE80::

Figura 24. Identificador d'interfície IPv6 d'un ordinador

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 00D0.BC7D.29B0
   Link-local IPv6 Address.........: FE80::2D0:BCFF:FE7D:29B0
   IP Address.......................: 0.0.0.0
   Subnet Mask......................: 0.0.0.0
   Default Gateway..................: 0.0.0.0
   DNS Servers......................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID...............: 00-01-00-01-B3-B3-5C-11-00-D0-BC-7D-29-B0
```

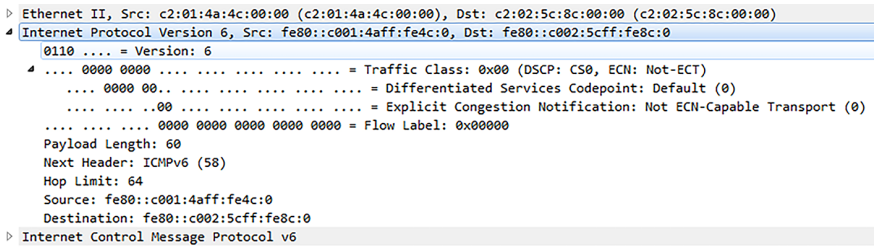
La MAC en aquesta captura és: 00D0.BC7D.29B0.

Per a obtenir l'adreça IPv6 es divideix l'adreça MAC en dues parts separades per FFFE. Les dues parts separades per FFFE són 00D0BC i 7D29B0.

Finalment, el segon bit del byte de més pes es posa a 1 de manera que queda: 02D0BC, com mostra la figura.

Exercici

Mentre s'envia un missatge ICMP (*ping*) entre dos dispositius es fa una captura del trànsit. A continuació, es mostra el detall d'un dels paquets enviats.



Es demana:

a) Indica quina és l'adreça MAC origen i destí.

b) Indica quina és l'adreça IPv6 origen i destí.

c) Explica com s'obté l'adreça IPv6 sabent que el *ping* s'ha fet per mitjà de l'identificador de la interfície IPv6.

Solució:

a) Examinant la captura, a la capçalera Ethernet II podem obtenir l'adreça MAC origen i destí:

Origen: c2:01:4a:4c:00:00

Destí: c2:02:5c:8c:00:00

b) Adreça IPv6 origen i destí

Origen: FE80::C001:4AFF:FE4C:0

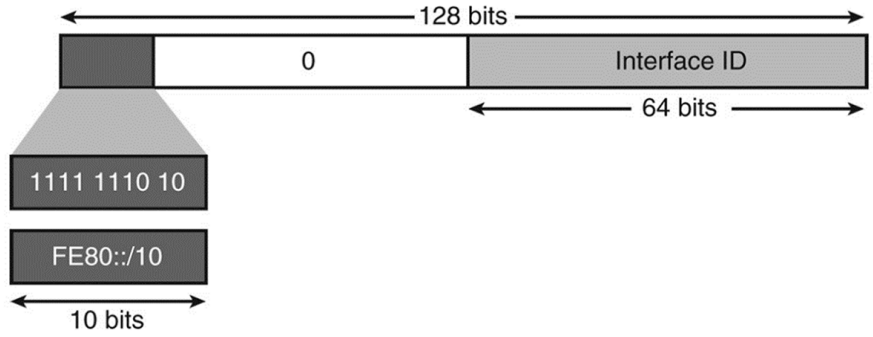
Destí: FE80::C002:5CFF:FE8C:0

c) L'adreça IPv6, tal com s'ha explicat, s'obtindria a partir de l'adreça MAC. En concret, l'adreça MAC es divideix en dues parts separades per FFFE.

3.3.2. Adreces *unicast* d'enllaç local

Aquestes adreces tenen, tal com ja s'ha explicat, un abast local i es creen dinàmicament en totes les interfícies IPv6 mitjançant un prefix d'enllaç local, FE80::/10, i 64 bits de l'identificador d'interfície. Es fan servir per a la configuració automàtica d'adreces, descobriment de veïns, descobriment d'encaminador i per a diversos protocols d'encaminament. A la figura següent es mostra la forma d'una adreça d'enllaç local.

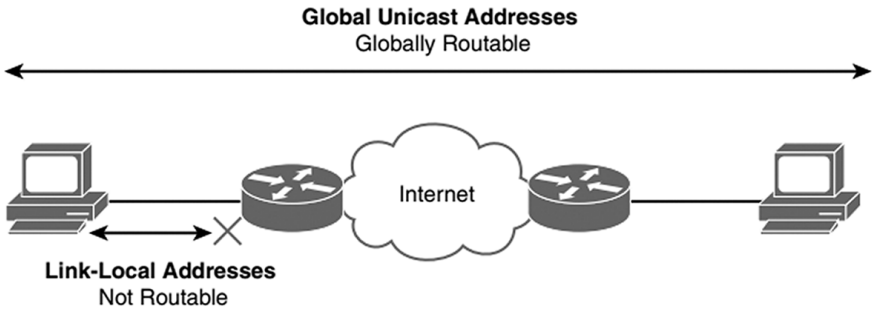
Figura 25. Adreça d'enllaç local



Un dispositiu IPv6 no ha de tenir necessàriament una adreça *unicast* global, sinó una adreça *unicast* d'enllaç local. Normalment, les adreces locals comencen per fe80: i les sol crear automàticament el sistema operatiu del dispositiu.

A la figura següent es mostra la diferència en àmbit d'actuació entre adreça *unicast* global i local.

Figura 26. Comparació entre adreça global i local IPv6



3.3.3. Adreces *anycast*

Com ja s'ha avançat anteriorment, les adreces *anycast* són adreces *unicast* globals que s'assignen a més d'una interfície. De vegades hi ha serveis a la xarxa que s'ofereixen per mitjà de més d'un *host* o encaminador. D'aquesta manera s'aconsegueix:

- **Redundància:** el servei no depèn d'un únic servidor, de manera que si un equip falla, els altres n'assumeixen les tasques i el servei continua disponible.

- **Balanceig de càrrega:** els diferents servidors es reparteixen la feina de manera que no hi hagi un equip sobrecarregat i altres servidors inactius.

Quan un usuari, aplicació o *host* vol accedir al servei, no li importa quin dels múltiples servidors que l'ofereix l'atén.

Les adreces *anycast* permeten aquest mode de funcionament. Quan un *host* envia un datagrama a una adreça *anycast*, la infraestructura de xarxa buscarà el

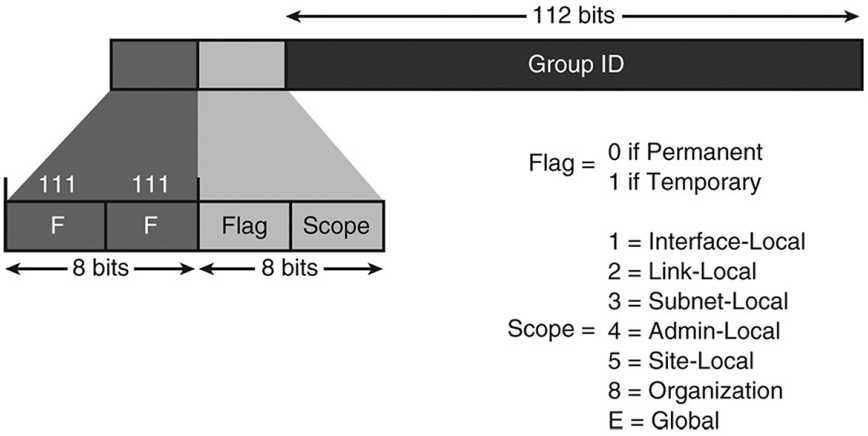
camí més curt fins a un dels equips que accepten datagrames adreçats a l'adreça *anycast* utilitzada.

L'avantatge més important d'*anycast* és que simplifica la cerca del servidor més apropiat, que sol ser el més proper.

3.3.4. Adreces *multicast*

El format de les adreces multicast es mostra a la figura següent. Les adreces *multicast* tenen el prefix FF00::/8. El segon octet defineix el temps de vida (*flag*) i l'abast de l'adreça *multicast*, com es mostra a la figura.

Figura 27. Format d'adreça multicast



Així, una adreça que comenci per FF02::/16 és una adreça permanent *multicast* amb un abast local. L'ID del grup multicast el formen els 112 bits de menys pes de l'adreça *multicast*. El rang comprès entre FF00:: i FF0F:: té el *flag* a 0 i està reservat.

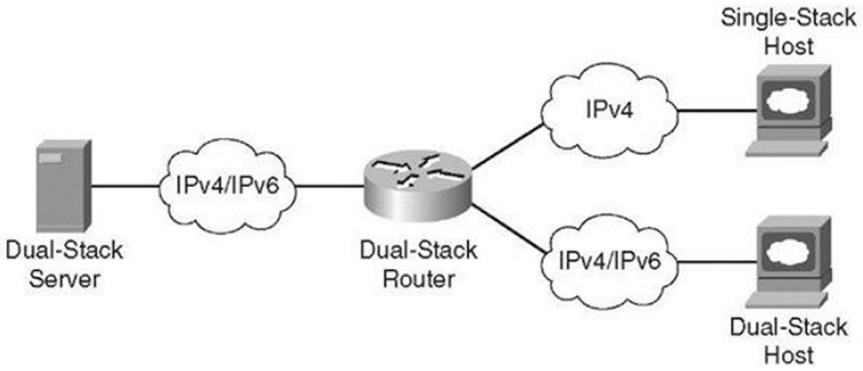
3.4. Tecnologies per a fer la transició d'IPv4 a IPv6

Hi ha dos mètodes bàsics de compatibilitat entre IPv4 i IPv6: *dual-stack* i *tunneling*. A continuació s'expliquen amb una mica més de detall.

- ***Dual-stack:*** el dispositiu es configura per a disposar de les dues piles (*stacks*) IPv4 i IPv6. La configuració de *dual-stack* es pot implementar a una interfície o a múltiples interfícies. En aquest cas el dispositiu decideix com envia el trànsit en funció de l'adreça de l'altre dispositiu de manera que escull quina pila utilitzar en funció de l'adreça destí.

  A la figura es veu l'exemple d'un encaminador amb *dual-stack*.

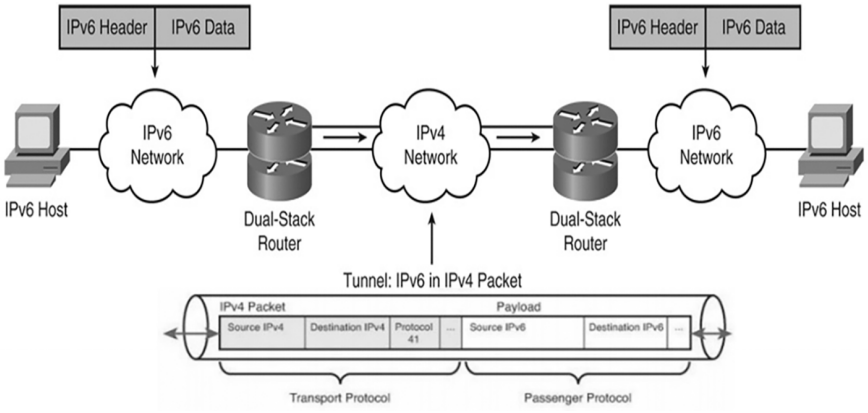
Figura 28. Exemple d'encaminador amb dual-stack



- ***Tunneling***: quan s'utilitza aquesta tècnica, l'encaminador transmet les dades IPv6 per mitjà de la xarxa IPv4 col·locant el paquet IPv6 al camp de dades del paquet IPv4. És a dir, tot el paquet IPv6 (capçaleres incloses) esdevé el camp de dades (*payload*) d'un paquet IPv4. El camp «protocol» de la capçalera IPv4 indica que la part de dades correspon a la capçalera IPv6 encapsulada.

  Els túnels involucren dos dispositius, que són els punts finals del túnel: punt d'entrada del túnel (*tunnel entry point*) i punt de sortida del túnel (*tunnel exit point*).

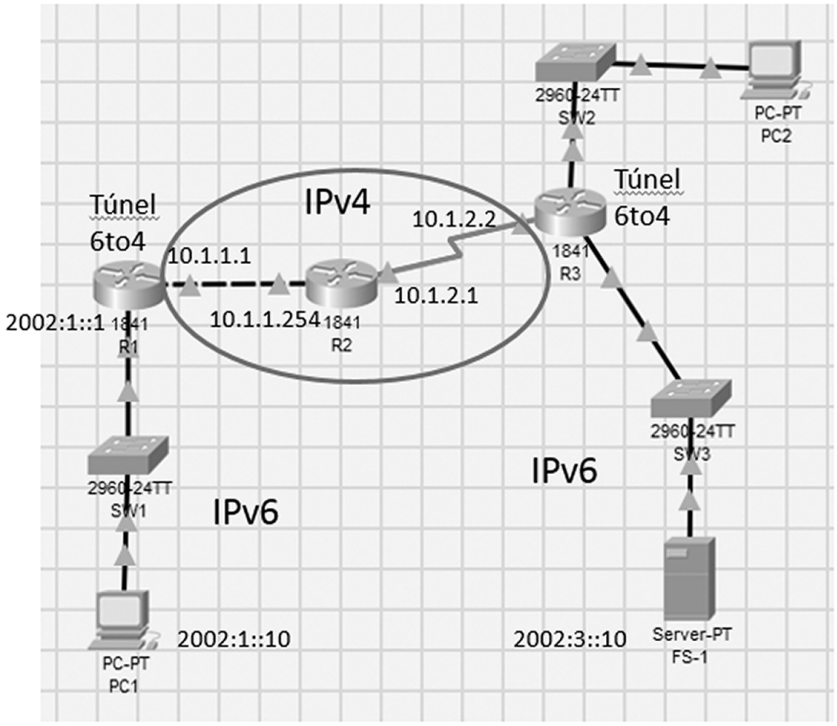
Figura 29. Exemple de *tunneling*: IPv6 per mitjà d'una xarxa IPv4



Exemple

A continuació, s'ha configurat la topologia que mostra la figura següent per a veure el funcionament del *tunneling*. La topologia està formada per dues xarxes IPv6 que són: 2002:1::/64 i 2002:3::/64. Aquestes dues xarxes estan connectades entre elles mitjançant una xarxa que funciona amb IPv4. La configuració que s'ha realitzat és amb *tunneling* i el que es vol mostrar és com aquest realitza l'encapsulament i el desencapsulament de la capçalera IPv6. Per a comprovar el funcionament correcte es fa un *ping* entre PC1 i FS-1 (ambdós estan configurats amb IPv6). Tal com es veu a la figura, la transició d'una xarxa IPv6 a una xarxa IPv4 s'anomena 6to4, mentre que la transició d'una xarxa IPv4 a una xarxa IPv6 s'anomena 4to6.

Figura 30. Exemple de funcionament del *tunneling*



Per a poder visualitzar les diferents capçaleres dels datagrames enviats en el *ping* s'ha fet una captura dels datagrames en els encaminadors R1 i R3 que són respectivament els que fan l'encapsulament i el desencapsulament.

Així, a la figura 32 es mostren les capçaleres d'un dels datagrames enviats per PC1 quan arriba a l'encaminador R1. Posteriorment a la figura 33 es mostra com l'encaminador encapsula el datagrama IPv6 en IPv4. Comentem amb detall els passos realitzats per l'encaminador:

Un cop li arriba el paquet a R1, examina la seva taula d'encaminament (figura 31) per a saber per on ha d'encaminar per arribar al destí. A la taula de l'encaminador tenim l'entrada següent:

Figura 31. Taula del *tunneling* a l'encaminador R1

```
R    2002:3::/64 [120/3]
      via FE80::201:C7FF:FED9:CCA, Tunnel1
```

que ens diu que per arribar a la xarxa destí cal fer-ho via FE80::201:C/FF:FED9:CCA.

Decrementa el TTL de la capçalera IPv6. A la figura 33 on es mostra el paquet d'entrada ho indica amb *Hop Limit* = 128 i a la figura 35 on es mostra el paquet de sortida de l'encaminador ha passat a 127.

El paquet ha de sortir pel túnel i, per tant, s'encapsula amb la capçalera IPv4 (figures 34 i 35) indicant en el camp protocol de la capçalera IPv4 valor 41 (0x29), que indica que en el camp de dades es troba la capçalera IPv6. Si examinem la capçalera IPv4 (figura 35) veiem que el destinatari del paquet IPv4 és l'encaminador R3, ja que el túnel està fet entre R1 i R3 (R2 només funciona amb IPv4).

Figura 32. Resum de les capçaleres del datagrama a l'arribada a l'encaminador R1

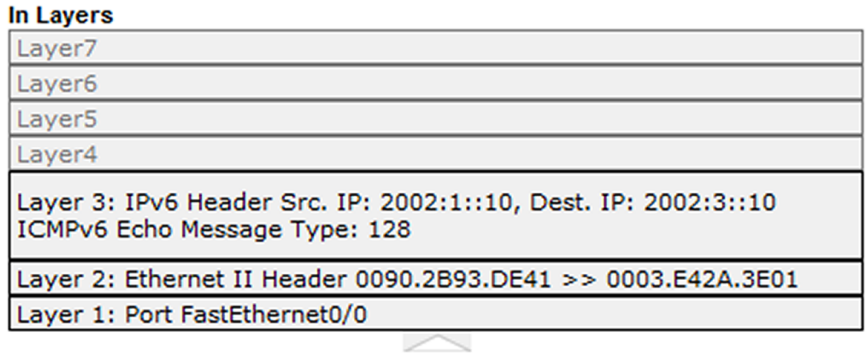


Figura 33. Detalls dels camps de les capçaleres del datagrama enviat per PC1 quan arriba a l'encaminador R1

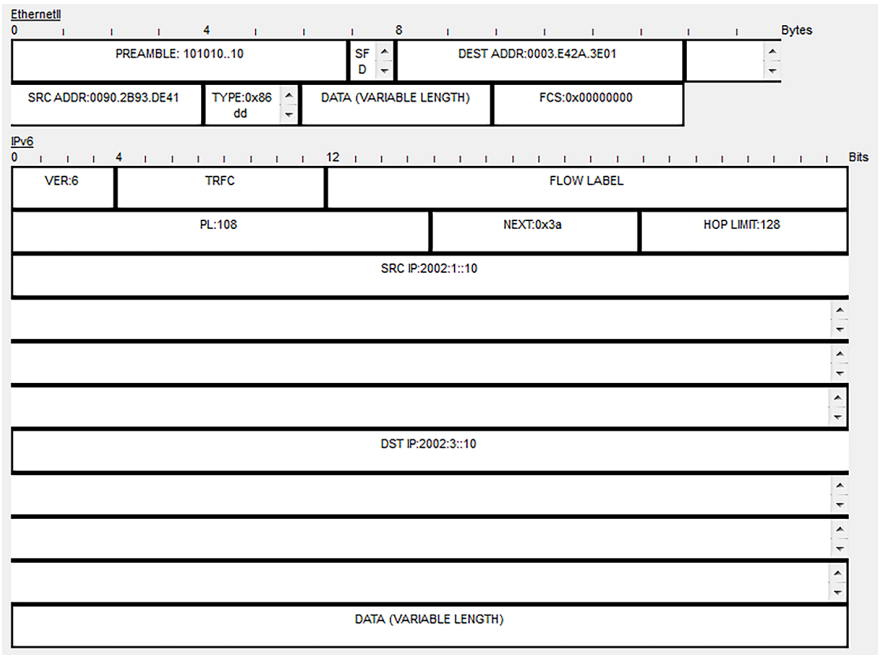


Figura 34. Resum de les capçaleres del datagrama un cop fet el *tunneling* a encaminador R1

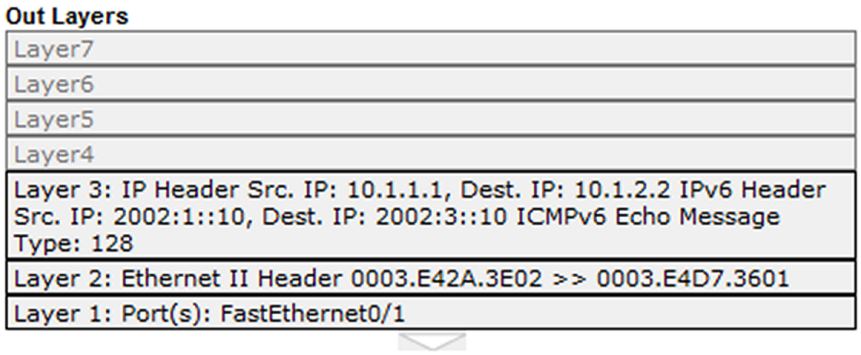
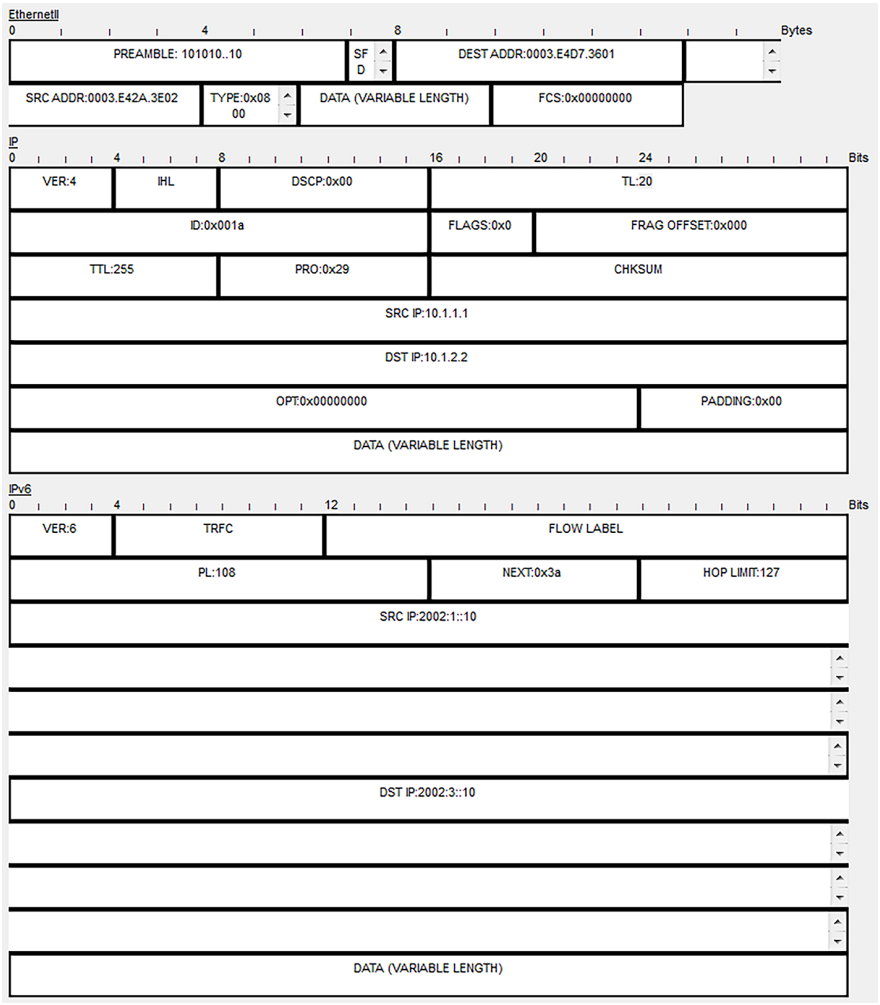


Figura 35. Detalls de les capçaleres del datagrama enviat per R1 un cop fet el *tunneling*



A R3 es faria el procés de desencapsulat. És a dir, es trauria la capçalera IPv4 i el datagrama es continuaria enviant amb IPv6.

4. 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. Introduirem 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).

4.1. 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:

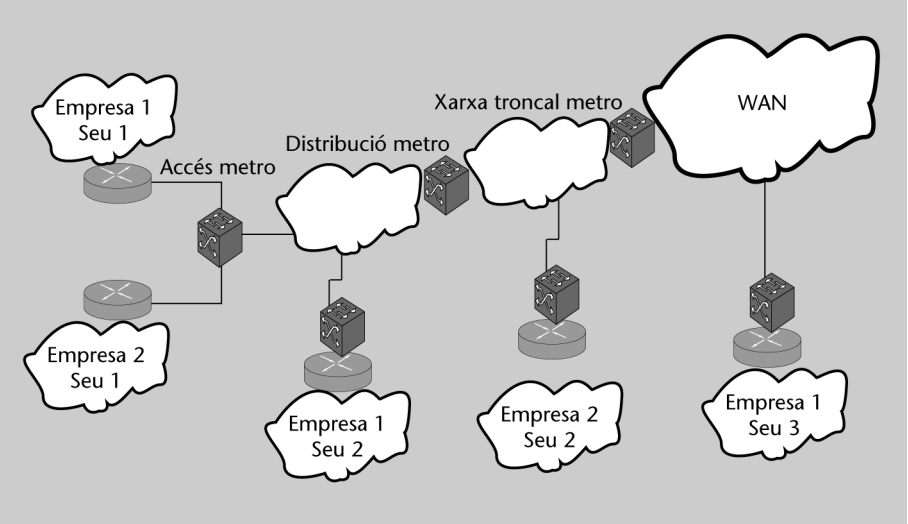
1) Accés metro (*access metro*). Aquests segment constitueix l'última milla, la qual, com sabeu, és la part que tocaria a l'usuari final.

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 36. Topologia de la xarxa metro



4.1.1. 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

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.

WDM actualment suporta fins a quaranta canals en una fibra i té la capacitat de suportar-ne fins a vuitanta per fibra.

4.1.2. 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.

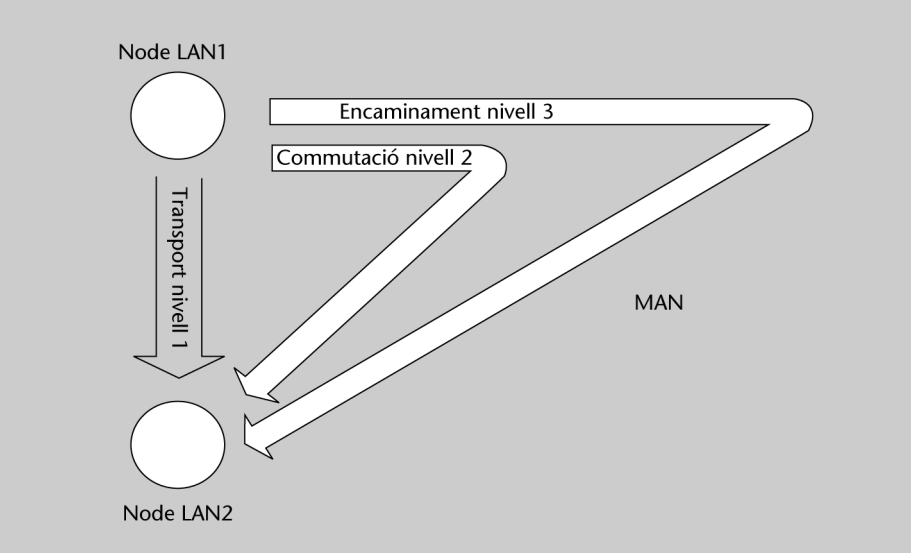
Per al client és més còmode, evidentment, poder estar connectat a la xarxa MAN i usar protocols que siguin compatibles a les dues xarxes.

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 hagis de fer.
- Capa d'encaminament IP: encamina si no queda una altra alternativa.

Figura 37. Entorn d'aplicació de cadascuna de les capes



4.1.3. Restriccions d'SDH/SONET

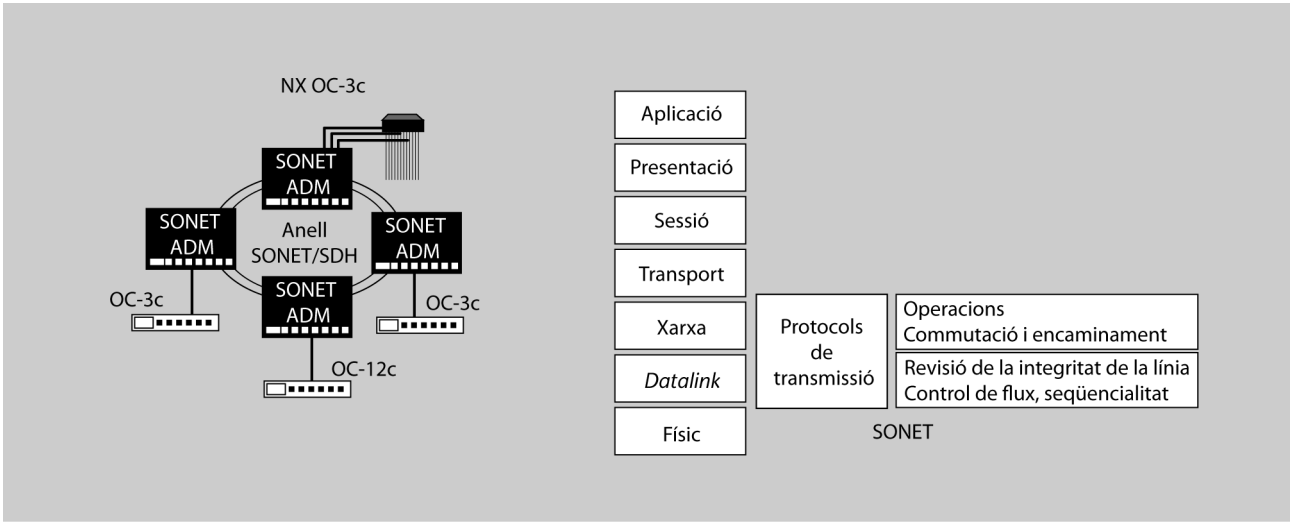
Encara que SDH/SONET està molt estès per algunes de les seves característiques, com són la recuperació davant de falles, la interoperabilitat entre fabricants, etc., té una sèrie de limitacions lligades al seu propi origen:

- **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 circuïts 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 38).

Figura 38. 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.

4.2. Les xarxes Ethernet metropolitanes

MEN: *metro ethernet network*.

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 *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*.

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

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.

Adreça recomanada

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

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 encaminadors, 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:

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.

- E-Line: enllaços punt a punt (figura 39).
- E-LAN: enllaços multipunt a multipunt (figura 40).

Figura 39. Exemple d'E-Line

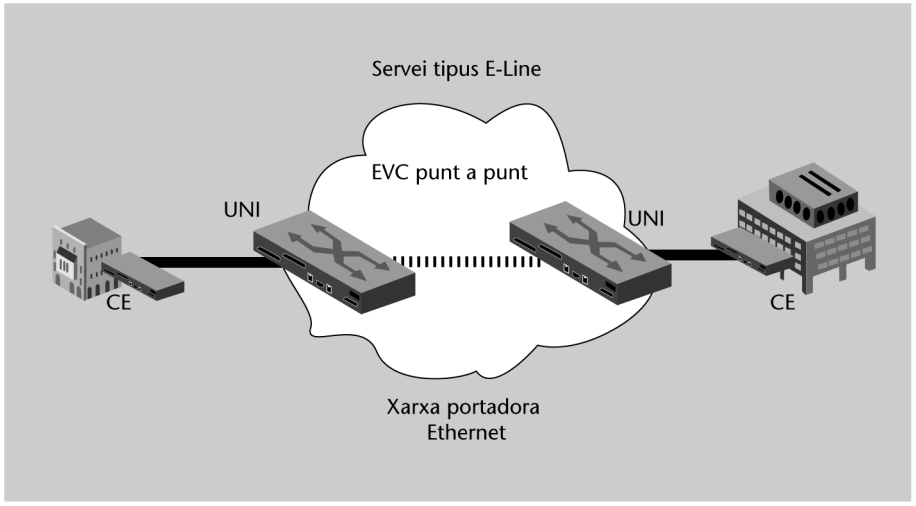
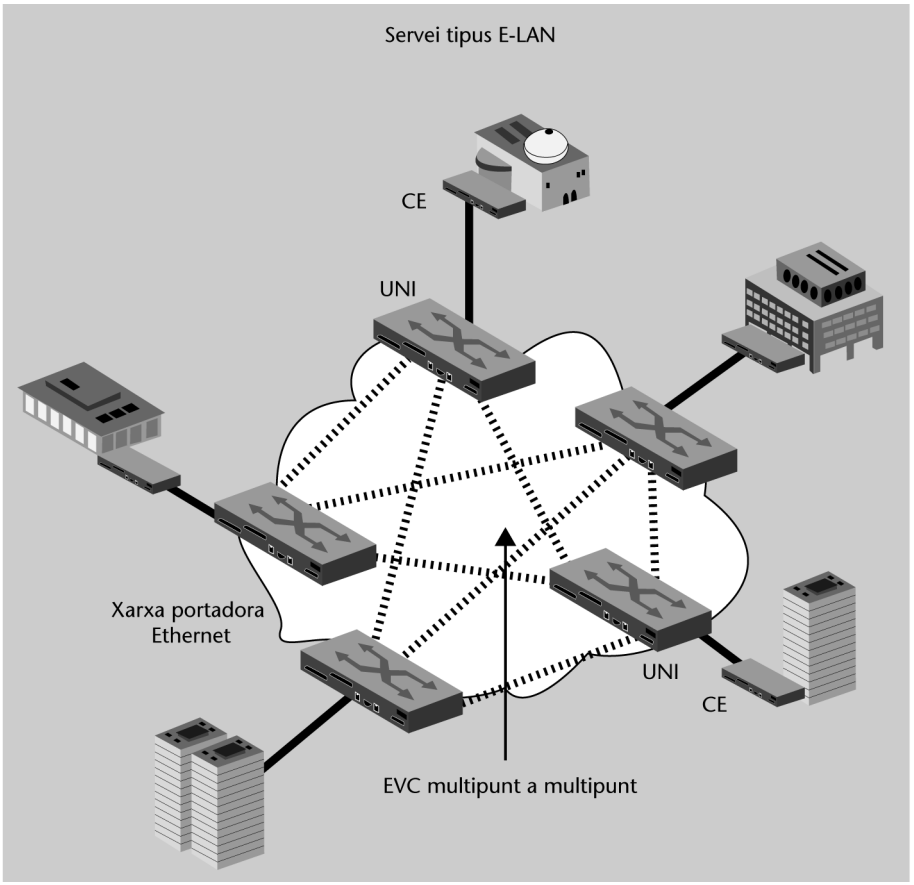


Figura 40. Exemple d'E-LAN



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

4.2.1. 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 quest 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.

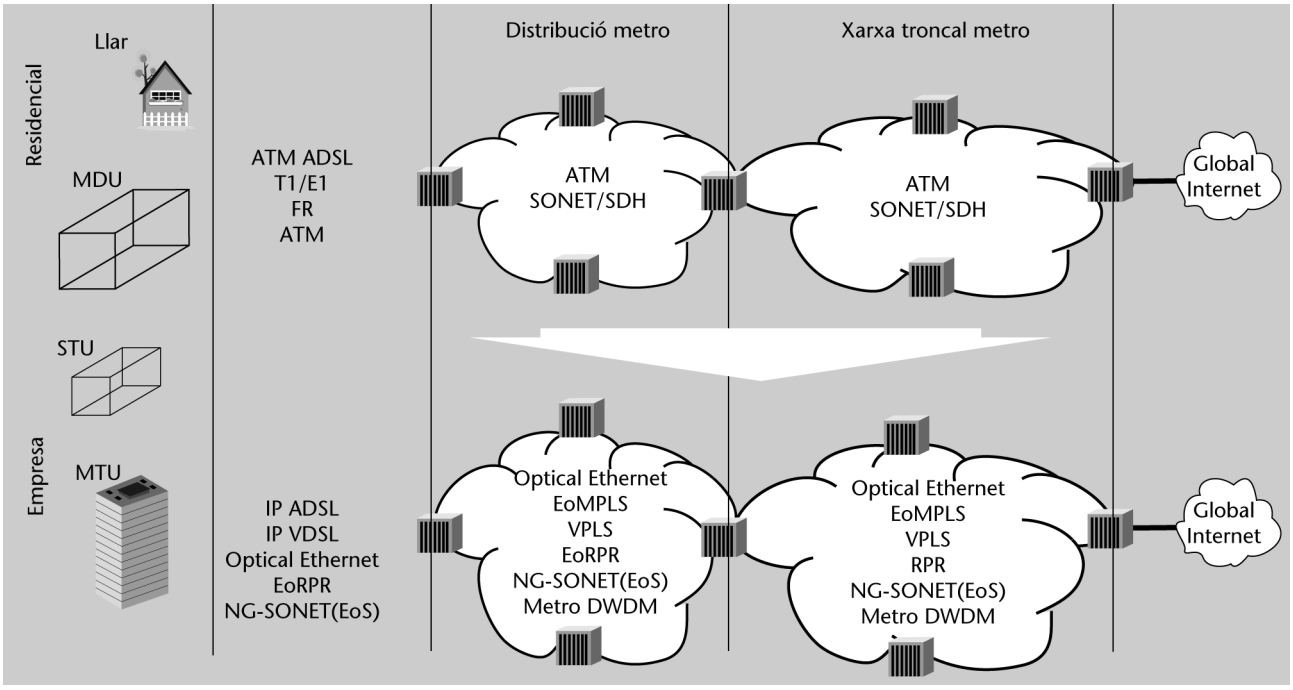
- **Escalabilitat en l'amplada de banda**. Des del punt de vista de l'operador la velocitat de servei és una de les claus que el diferencia respecte als competidors. Els sistemes lligats a TDM o ATM tenen poca flexibilitat i a la vegada no permeten gaire joc a l'hora d'assignar l'amplada de banda que 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 dóna 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 41 es mostra l'evolució de les xarxes metropolitanes cap a una xarxa MetroEthernet.

Figura 41. Evolució de les xarxes metropolitanes



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.

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

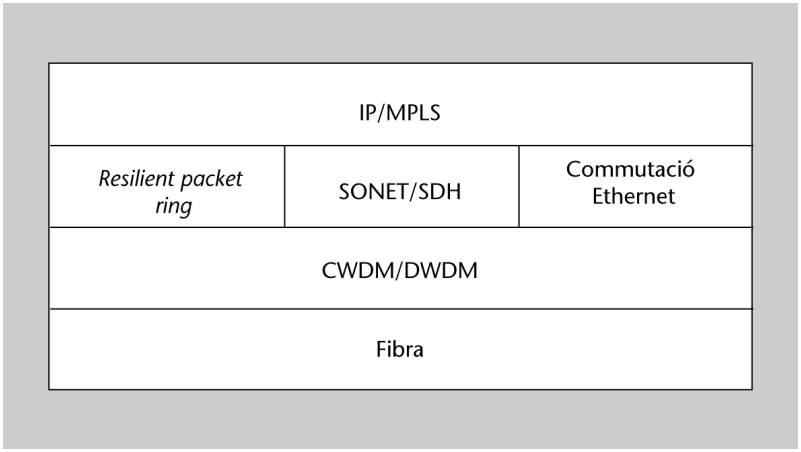
- **Operació, administració i manteniment (OAM)**. Ethernet no disposa de les característiques específiques d'SDH per a la gestió i manteniment de la xarxa.

  OAM: ***operation, administration and maintenance.***

- **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.

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 42 es mostren les diverses possibilitats existents.

Figura 42. Ethernet en relació amb altres tecnologies dels proveïdors



4.3. Ethernet sobre SDH (EOS)

EOS: ***Ethernet over SONET/SDH.***

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 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 43 es mostra l'encapsulat que fa.

Figura 43. Encapsulat Ethernet en SDH

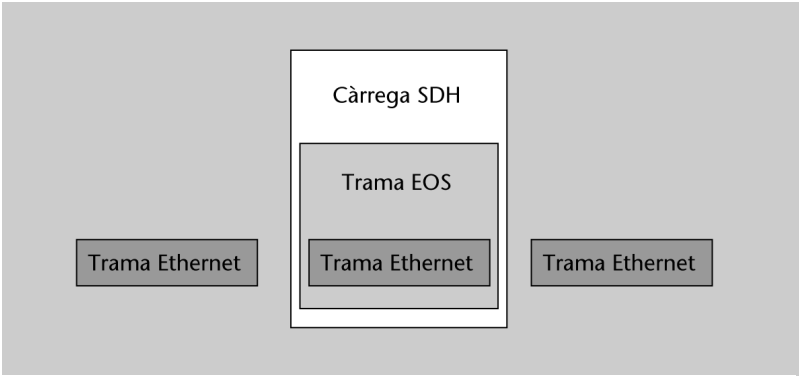
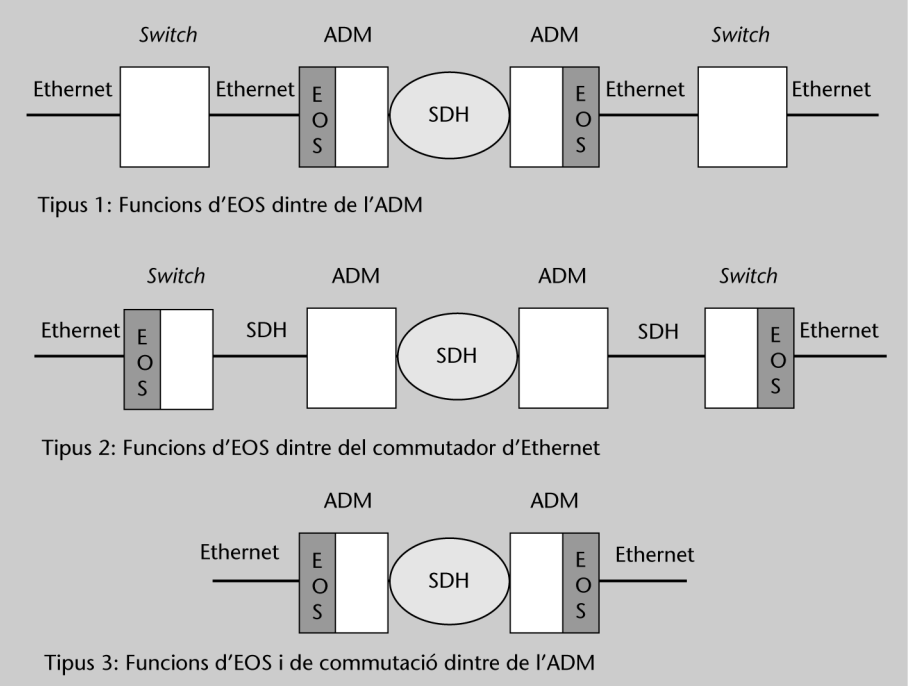


Figura 44. Diferents escenaris de connexió EOS



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

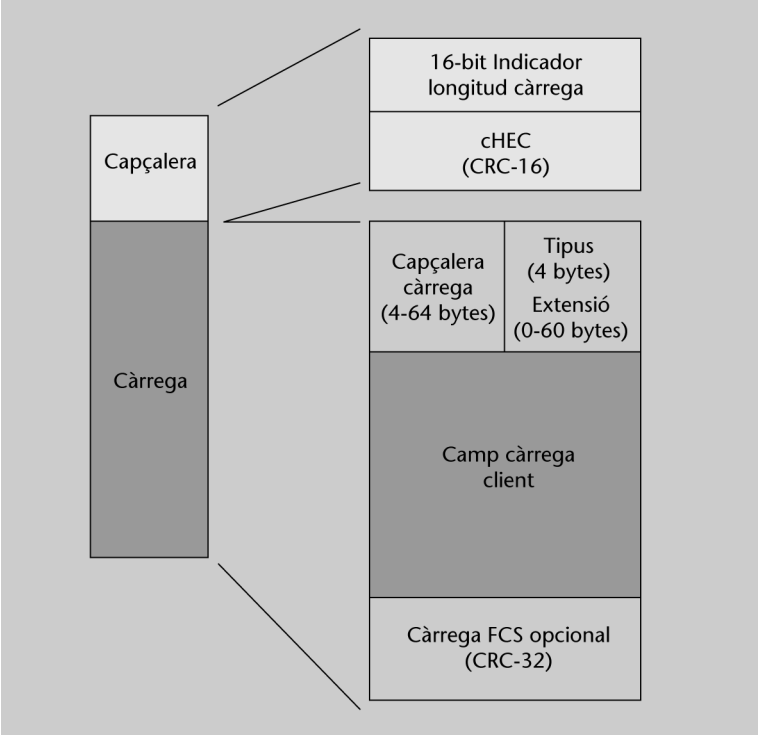
- **LAPS.** Està definit per la ITU-T, que va publicar l'estàndard X.86 el febrer de 2001. LAPS és un protocol no orientat a connexió similar al protocol HDLC.

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

- **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 45).

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

Figura 45. 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 granuralitat dels circuïts 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.***

4.3.1. 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.

4.3.2. Ajustar la capacitat de la connexió (LCAS)

LCAS: ***link capacity adjustment scheme.***

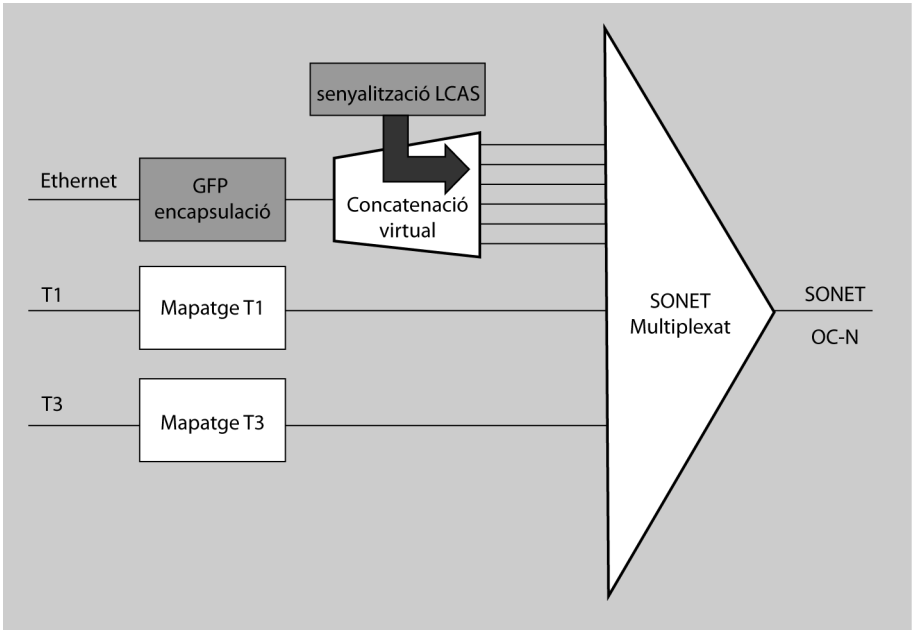
Un segon aspecte que cal solucionar en el transport Ethernet o dades en general és el fet que l'amplada de banda que necessita l'usuari va canviant en el temps i cal que les connexions es tornin a redimensionar.

LCAS és un protocol que permet redimensionar els canals sense haver d'interrompre 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 46. Senyalització LCAS que permet canviar l'amplada de banda sota demanda



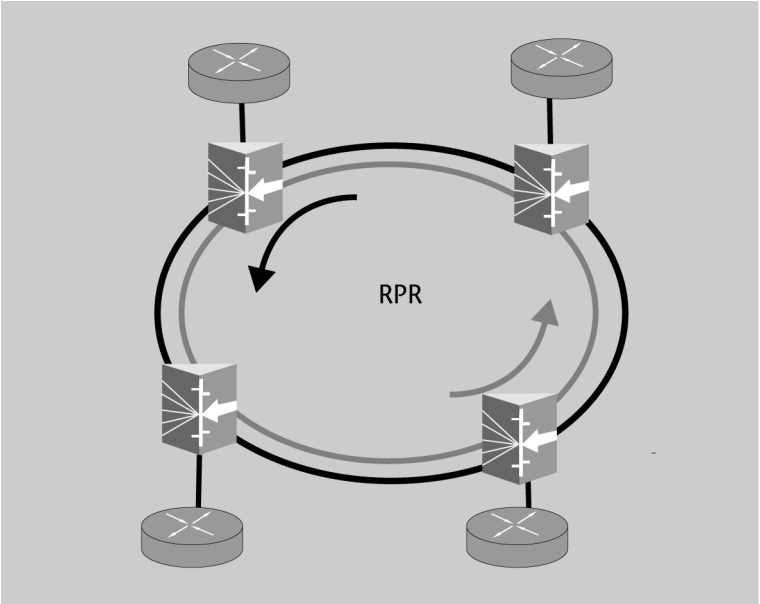
4.4. *Resilient packet ring* (RPR) IEEE 802.17

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 47).

Figura 47. Topologia en anell a RPR



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

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.

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

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

5. Enginyeria de trànsit i VPN a MPLS

En un mòdul anterior hem estudiat MPLS, però aquest protocol ha evolucionat substancialment des dels inicis del seu desenvolupament. Els motius d'ús d'MPLS a les xarxes també ha canviat, ja que actualment no s'utilitza per a proporcionar una drecera per a l'encaminament IP. Els dos canvis més significatius de la tecnologia MPLS són els següents:

- El protocol RSVP s'estén per donar suport a la distribució d'etiquetes MPLS, que en aquest cas és conegut com a RSVP-TE. Les lletres TE volen dir *Traffic Engineering* i aporten una sèrie de característiques importants a l'enginyeria del trànsit i la tecnologia del túnel MPLS.

- MPLS VPN: aquesta característica permet a l'operadora que utilitza la tecnologia MPLS crear canals virtuals dintre de la xarxa i fer-los servir per a transmetre de manera privada el trànsit d'usuari entre múltiples localitzacions.

5.1. Enginyeria de trànsit MPLS

MPLS: *Traffic Engineering* (MPLS TE)

Com hem vist a l'apartat 2.4, els protocols d'encaminament intenten determinar, mitjançant l'ús de les mètriques, el millor camí per a encaminar els paquets. De fet, el paradigma de commutació a IP es basa en l'encaminament dels paquets per mitjà del camí de menor cost. Més enllà d'això, hem de tenir present que en l'encaminament de paquets IP es donen les característiques següents:

- Els paquets IP es commuten a cada node en funció només de l'adreça IP destí, independentment del camí que han agafat tota la resta de paquets.

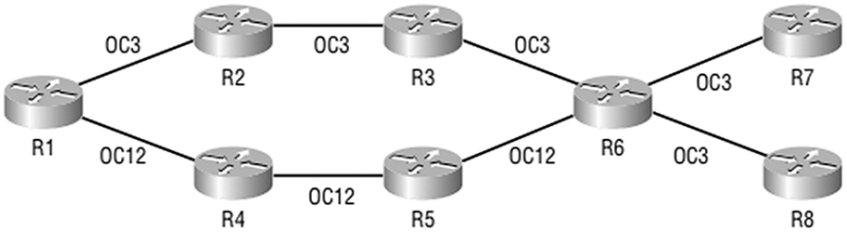
- No es té en compte la disponibilitat d'amplada de banda de la línia en funció del trànsit, la qual cosa és diferent al cost que té assignat aquesta línia.

- El commutador pot continuar commutant paquets per una línia malgrat que aquesta descarti paquets per falta d'amplada de banda. Això succeeix perquè l'encaminament es fa en funció de la taula de commutació i no pas del volum de trànsit.

En conseqüència, el paradigma d'encaminament IP pot provocar situacions en què alguns enllaços poden estar sobreutilitzats i, alhora, altres enllaços poden estar infrautilitzats.

Habitualment s'utilitza una xarxa amb forma de peix com a exemple il·lustratiu que permet explicar i justificar l'ús de l'enginyeria de trànsit. A la figura es veu una xarxa amb diversos commutadors amb connexions a diferents velocitats indicades per OC3 i OC12.

Figura 48. Xarxa senzilla per a justificar l'enginyeria de trànsit



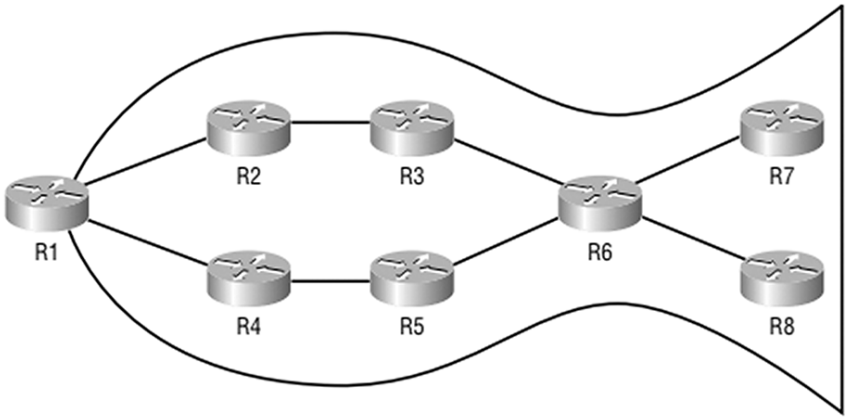
En primer lloc, l'objectiu és trobar quin és el millor camí per a un flux de trànsit des de l'encaminador R1 fins a R7. Si el protocol d'encaminament utilitza l'amplada de banda com a mètrica, llavors el trànsit seguirà el camí R1-R4-R5-R6 i R7.

Imaginem que ara tenim un segon flux de trànsit que surt d'R8 i arriba a R1. Aleshores, i de la mateixa manera que passava en el cas anterior, el trànsit seguirà la mateixa ruta, però en sentit contrari: R8-R6-R5-R4-R1. Si miréssim el trànsit que va des d'R7 fins a R1, el trànsit seguiria el mateix camí. Per tant, si ens hi fixem, sempre es fa servir la mateixa ruta per a encaminar el trànsit mentre els encaminadors R2 i R3 no s'utilitzen.

Protocols àmpliament utilitzats, com ara l'OSPF, no suporten balanceig de càrrega per costos no iguals (per exemple, velocitats diferents). Això fa que, malgrat que hi ha dos camins possibles entre l'origen i el destí, només s'utilitzarà un dels camins en funció de la mètrica, fins i tot si aquesta ruta se satura i arriba a perdre paquets.

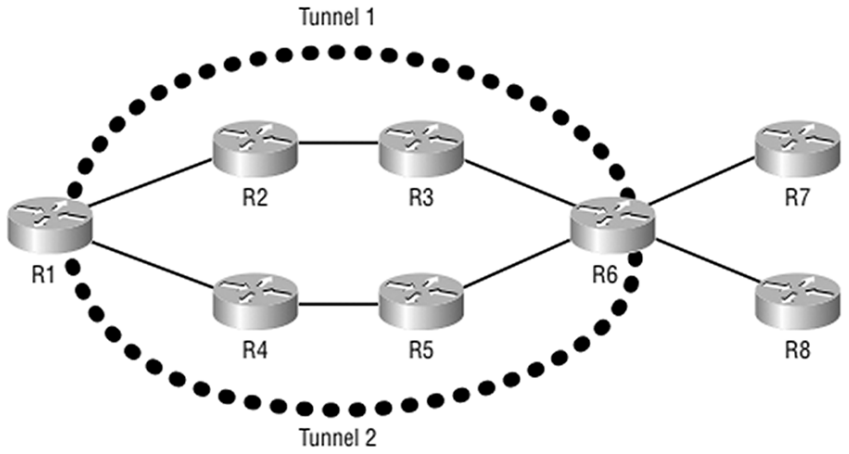
Ens trobem, en conclusió, que la meitat dels enllaços que s'han desplegat no es fan servir. Aquest problema s'anomena «el peix» (*The fish*) per la forma de la xarxa.

Figura 49. El problema del peix



MPLS soluciona el problema gràcies a l'enginyeria de trànsit MPLS. MPLS permet crear túnels mitjançant una pila d'etiquetes. A la figura es veu com es poden crear dos túnels, un per a cadascuna de les dues rutes. Com que MPLS suporta túnels amb balanceig de càrrega de diferent cost, el trànsit serà balancejat per mitjà d'aquests dos túnels.

Figura 50. Enginyeria de trànsit amb túnels



MPLS TE és la solució al problema anterior, ja que:

- Proporciona una distribució eficient del trànsit per mitjà de la xarxa, evitant que hi hagi enllaços sobreutilitzats i altres infrautilitzats.

- Té en compte l'amplada de banda configurada dels enllaços. Per exemple, en cas que hi hagi dos enllaços, no distribueix el trànsit de manera igual, sinó que té en compte l'amplada de banda de cada enllaç.

- Té en compte mètriques de l'enllaç, com ara el retard o les diferències de retard.

- S'aplica encaminament basat en la càrrega de l'origen i no només en l'adreça destí.

Per a aconseguir-ho, MPLS TE fa servir les funcionalitats/mecanismes següents per a un funcionament correcte:

- Tenir en compte les restriccions dels enllaços. És a dir, quant de trànsit pot suportar cada enllaç.

- Un algorisme que calcula el millor camí des de l'origen LSR fins al destí LSR.

Recordeu que LSR (*Label Swith Router*) és un encaminador/*switch* que és capaç de commutar paquets basat en etiquetes.

- Un protocol de senyalització que crea el túnel per mitjà de la xarxa. Aquest protocol és una ampliació d'RSVP.

- Mecanisme per a commutar el trànsit per mitjà del túnel.

5.2. MPLS VPN

VPN (*Virtual Private Network*): xarxa privada virtual

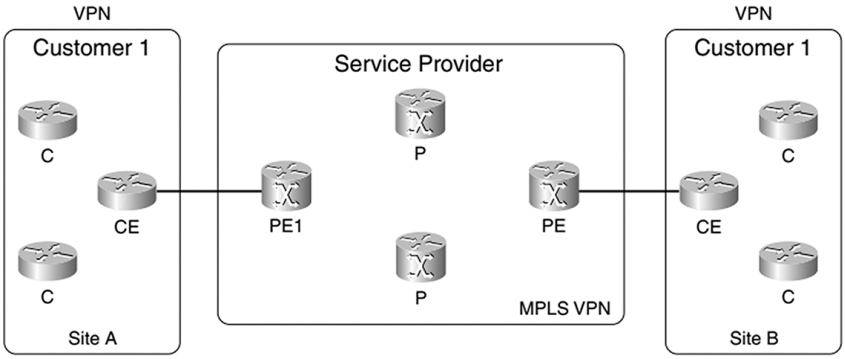
Una xarxa VPN és una xarxa que emula una xarxa privada, però sobre una infraestructura comuna. La VPN pot proporcionar comunicació als nivells 2 i 3 d'OSI.

Així, una xarxa privada virtual és una manera fàcil de crear una xarxa segura a sobre d'una xarxa compartida per a permetre connectar diferents seus o l'accés remot d'usuaris a seus. En comptes de disposar de connexions dedicades entre xarxes, la VPN encamina les seves connexions mitjançant túnels per mitjà de les xarxes públiques, que són el que ofereixen normalment els operadors.

A l'RFC 4364 es defineix la xarxa VPN sobre MPLS, en què es fa servir la xarxa compartida MPLS per a muntar una VPN i poder tenir els clients separats malgrat que comparteixin els elements comuns de la xarxa MPLS. El protocol d'intercanvi d'etiquetes usat en aquesta xarxa és MP-BGP (Multiprotocol-BGP).

Al dibuix es mostren els elements de xarxa que formen el model MPLS VPN.

Figura 51. Esquema d'MPLS VPN



Si ho recordeu, el PE (*Provider Edge*) és l'encaminador que té connexió directa amb l'encaminador CE (*Customer Edge*) a nivell 3. Un encaminador P (*Provider*) és un encaminador sense connexió directa als encaminadors dels usuaris. A la implementació MPLS VPN, tant els encaminadors P com els PE treballen amb MPLS. Això vol dir que han de poder distribuir etiquetes entre ells i commutar els paquets en funció de l'etiqueta.

L'encaminador C (*Customer*) és un encaminador sense connexió directa amb l'encaminador PE. L'encaminador CE no necessita treballar amb MPLS.

Per a aconseguir un funcionament correcte MPLS VPN cal l'ús d'un protocol d'encaminament, que en aquest cas seria el Multiprotocol BGP, que explicarem a continuació.

5.2.1. Multiprotocol BGP

BGP: *Border Gateway Protocol*

BGP és el protocol d'encaminament a la xarxa troncal d'internet. És el protocol de comunicació mitjançant el qual s'intercanvia informació d'encaminament entre sistemes autònoms. Els proveïdors (ISP) registrats a internet solen estar formats per diversos sistemes autònoms i en aquest cas el protocol de comunicació entre ells és BGP. Dintre dels sistemes autònoms és on s'aplicarien els protocols d'encaminament com ara RIP o OSPF. BGP, a diferència d'aquests altres protocols, no treballa amb mecanismes de vector distància o estat enllaç. En canvi, realitza un intercanvi de prefixos o vectors de rutes entre els diferents sistemes autònoms. Aquests vectors de rutes tenen una sèrie d'atributs que poden influir en l'encaminament del trànsit. L'avantatge d'aquest protocol és la personalització. Així, quan es combinen els atributs BGP amb polítiques d'encaminament, la personalització del trànsit és molt alta.

Com que BGP no és capaç de transmetre la informació MPLS, ha calgut crear una extensió del protocol que suporti la creació d'MPLS VPN. Aquest protocol és l'anomenat Multiprotocol BGP (MP-BGP). En concret, s'ha estès algun dels atributs perquè proporcionin les eines necessàries per a desenvolupar la solució VPN.

5.2.2. VPN de nivell 2 i nivell 3

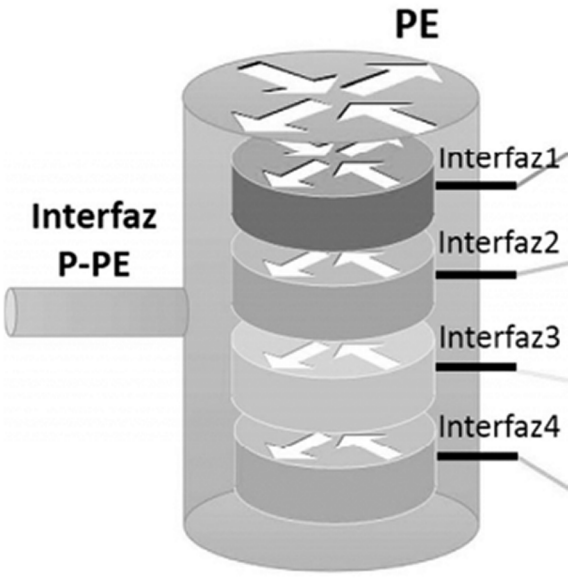
La tecnologia MPLS suporta dos tipus de serveis VPN: VPN de nivell 2 i VPN de nivell 3.

La VPN de nivell 2 també és coneguda com a Servei Virtual Privat LAN (VPLS: *Virtual Private LAN Service*). Aquest servei crea un canal virtual entre les seus d'usuari que es manté totalment privat per a la resta de trànsit de la xarxa de l'operadora. Cal destacar que, amb VPN de nivell 2, l'encaminament es fa a la seu del client. És a dir, al dispositiu CE. Es pot considerar que l'operadora és cega acceptant el trànsit de nivell 2 i transportant-lo per mitjà d'interfícies de nivell 2 dins de la xarxa MPLS.

Amb VPN de nivell 3, és l'operadora qui s'encarrega de tot l'encaminament entre les diferents seus del client. La VPN de nivell 3 fa servir les taules VRP (taula d'encaminament VPN).

Per a mantenir la xarxa dels clients aïllada i que el seu trànsit no es barregi a cada PE, es crea un PE virtual dintre del mateix PE que té la seva pròpia taula d'encaminament VPN (VRF). Aquest encaminador virtual PE té els recursos necessaris per a operar com si fos un encaminador independent; d'aquesta manera es poden compartir els PE i no cal muntar PE per a cada client, cosa que generaria un augment de cost en material i manteniment. A la figura es mostra aquest concepte. Es veu un PE que conté quatre PE virtuals, cosa que permet aïllar el trànsit de cadascun dels clients.

Figura 52. VRF als PE per a donar accés a diferents VPN

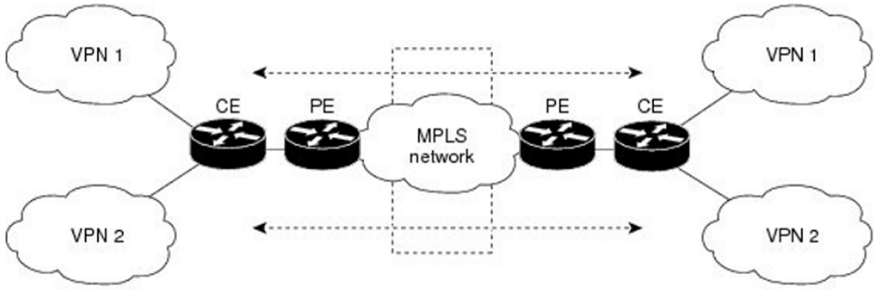


Amb aquesta tecnologia VRF es pot reutilitzar l'adreçament privat, ja que tant el trànsit com les rutes estan separades als PE. Quan a un PE li arriba un paquet IP d'un CE per una interfície, sap a quin VRF pertany i busca l'adreça IP destí

a la seva taula d'encaminament per a determinar el destí i saber l'etiqueta que ha d'inserir per a commutar-lo al P següent i per quina interfície.

Aquest model és molt escalable perquè si introduïm una altra seu, només cal configurar un o dos PE perquè rebi les rutes que el CE anuncia al PE.

Figura 53. Multi VRF



5.2.3. Avantatges de les xarxes MPLS VPN

Hi ha diversos avantatges d'aquestes xarxes. Les més importants són les següents:

- **Flexibilitat de la tecnologia d'accés.** La xarxa MPLS permet fer servir qualsevol tecnologia d'accés per a connectar la seu del client.

- **Flexibilitat d'adreçament:** amb VPN-MPLS els clients poden continuar fent servir l'adreçament que tinguin, ja que es permet el solapament de xarxes entre clients.

- **Escalabilitat:** quan incorporem una nova seu a la xarxa només cal instal·lar un nou CE i donar-li accés al PE. A la resta de la xarxa del client no cal fer cap modificació addicional.

- **Qualitat de servei:** es poden configurar diferents classes de servei per a prioritzar certs tipus de flux.

- **Disponibilitat:** aquesta xarxa permet diversos nivells de redundància, la qual cosa minimitza els problemes de connectivitat i millora la disponibilitat global de la xarxa.

6. SD-WAN

Software-Defined Networking (SDN) és un concepte que va sorgir al voltant del 1990 i el seu objectiu principal era aportar programabilitat al sector de les xarxes (*Networking*) amb la finalitat de proporcionar més innovació en aquest camp. El que impulsa la necessitat d'SDN és l'evolució de les tecnologies en el núvol (*cloud*) i la virtualització.

6.1. Introducció

A les xarxes tradicionals, la majoria de les funcionalitats de xarxa s'implementen directament en els dispositius, com ara els encaminadors o *switchs*. A més, dins d'aquests dispositius dedicats, la majoria de funcionalitats s'implementen en maquinari dedicat. Aquest mode de funcionament té una sèrie de característiques:

- L'evolució del maquinari està sota el control del fabricant del dispositiu.
- Els dispositius són propietaris.
- Cada dispositiu està configurat de manera individual.
- Tasques com l'aprovisionament o la gestió del canvi requereixen molt de temps i són susceptibles als errors.

Per altra banda, és clar que el món digital es mou tot cap al núvol. Aplicacions al núvol, màquines virtuals que es mouen (migren) dinàmicament entre servidors de manera molt ràpida, etc. En canvi, en el model tradicional, es pot trigar força temps a configurar els equips de xarxa si es vol donar servei en una nova ubicació.

Utilitzant els principis de la xarxa definida per programari (Software-Defined Network, SDN), SD-WAN permet a les empreses encaminar i prioritzar la connectivitat de xarxa a les diferents seus per mitjà del núvol, a la vegada que simplifica i agilitza el desplegament i redueix el cost de les despeses de maquinari associades, normalment, a les solucions WAN tradicionals. SD-WAN està dissenyat per a permetre a les empreses no només connectar seus remotes, com pot fer MPLS, sinó també una ràpida connectivitat a totes les aplicacions del núvol que necessitin.

SD-WAN utilitza programari i tecnologies basades en el núvol per a simplificar el lliurament de serveis WAN a les diferents seus de l'empresa. La virtualització basada en programari permet l'abstracció de la xarxa i, en conseqüència, la simplificació de les seves operacions. SD-WAN permet als administradors de

tecnologies de la informació i de negoci desplegar connectivitat basada en internet de manera fàcil, ràpida i amb qualitat, fiabilitat i seguretat.

Les xarxes definides per programari són un nou enfocament de xarxa que permet que la xarxa sigui controlada de manera central i intel·ligent mitjançant aplicacions programari. L'objectiu és que els operadors gestionin la xarxa de manera integral independentment de la tecnologia de xarxa subjacent. L'aplicació de les xarxes definides per programari al sector WAN es fa per mitjà del que hem anomenat SD-WAN.

6.2. SDN (Software-Defined Network)

Tal com s'ha explicat, la xarxa definida per programari (SDN) és un concepte que emergeix al voltant del 1990 i que té per objectiu portar la programabilitat al sector de les xarxes.

SDN permet la programació del comportament de la xarxa d'una manera centralitzada mitjançant aplicacions de programari que utilitzen API obertes. Amb l'obertura de les plataformes de xarxa (normalment tancades) i la implementació d'una capa de control SDN comuna, els operadors poden gestionar tota la xarxa i els seus dispositius de manera consistent i, com s'ha dit, de manera independent de la complexitat de la tecnologia subjacent.

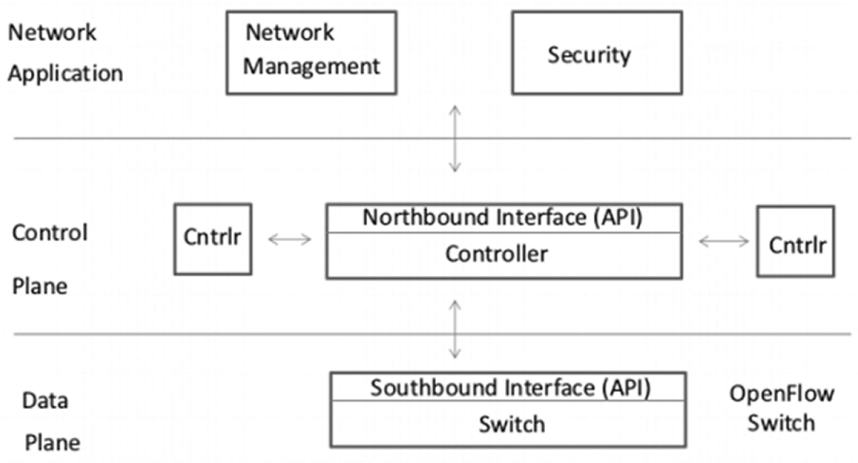
6.2.1. Fonaments SDN

Les àrees en què la tecnologia SDN pot marcar la diferència segons l'Open Networking Foundation (ONF) són les següents:

- **Programabilitat o automatització i virtualització de la xarxa:** SDN permet que el comportament de la xarxa es controli mitjançant programari, que no està lligat als dispositius que proporcionen la connectivitat física. Així, es desacobla el maquinari del programari, de manera que els operadors poden introduir nous serveis diferenciats de manera ràpida.

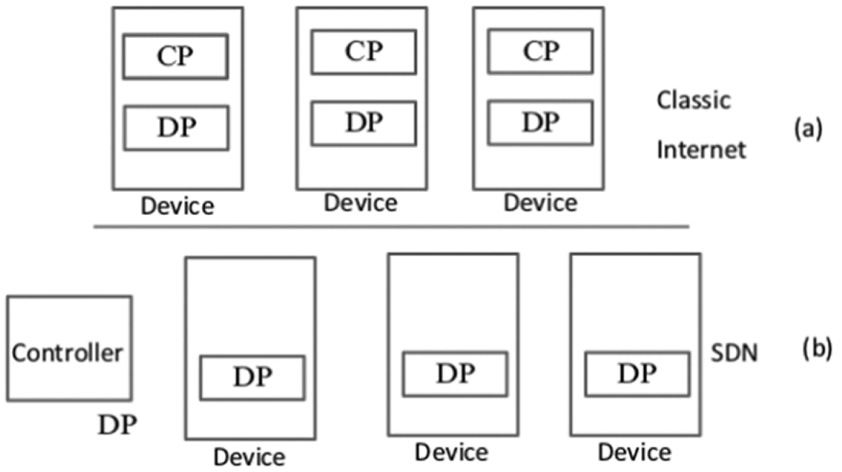
  Aquesta abstracció permet la virtualització de les funcions de xarxa i una major productivitat. Aquesta virtualització és la que permet que SDN no sigui específica del venedor. A la figura es veu una arquitectura SDN amb els seus dos tipus d'enllaços (API) anomenats interfícies *northbound* i *southbound*. L'API *northbound* es fa servir per a connectar el controlador al pla de gestió on resideixen totes les aplicacions. Aquest tipus d'interfície pot servir com a passarel·la cap a l'automatització dels nivells alts de la xarxa. L'API *southbound* permet al controlador configurar de manera dinàmica la commutació dels dispositius de xarxa. L'API més important actualment és OpenFlow.

Figura 54. Arquitectura SDN segons l'Open Networking Foundation



- **Intel·ligència centralitzada i control lògic:** SDN permet tenir una visió integral de la xarxa, de manera que l'administració, restauració, seguretat i polítiques d'amplada de banda poden ser òptimes. A la figura següent es mostra una comparació entre la internet clàssica i els models en plans SDN. L'arquitectura de la internet clàssica fa possible els plans de dades i control en cada dispositiu. Això duu a una aproximació centrada en el maquinari i fa que sigui necessari configurar cada dispositiu de manera individual amb els comandaments específics de cada fabricant. Com a conseqüència, la implementació en entorns de xarxes grans significa una feina costosa en temps i recursos econòmics. Per contra, tal com es mostra a l'apartat b) de la figura, l'arquitectura SDN proporciona un model centralitzat per mitjà del qual un element anomenat controlador distribueix les configuracions necessàries als altres dispositius.

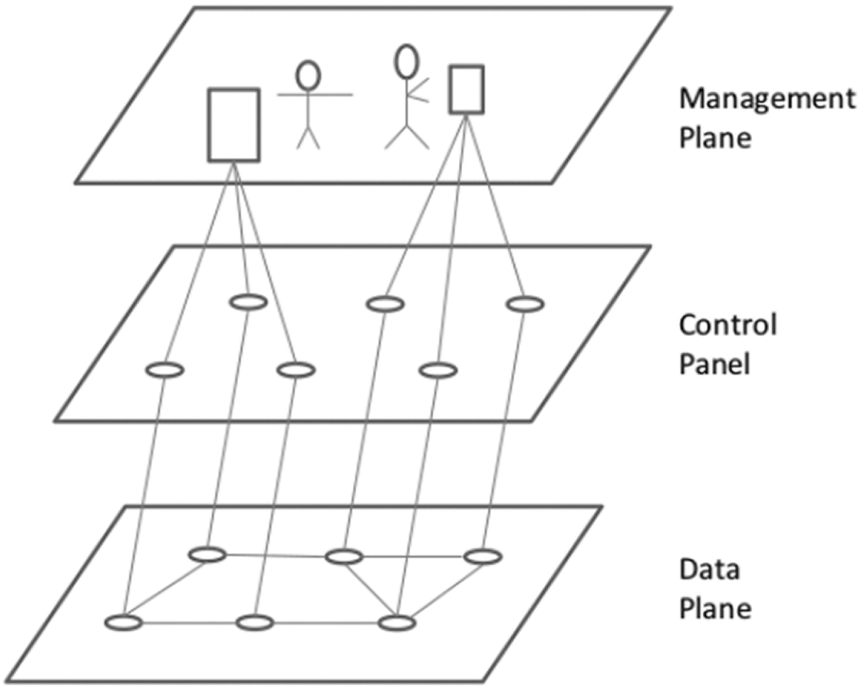
Figura 55. Internet clàssic i arquitectura SDN



- **Abstracció de la xarxa:** els serveis i aplicacions que s'executen en la tecnologia SDN s'abstrauen de les tecnologies subjacents i del maquinari que proporciona la connectivitat física de control de xarxa. Les aplicacions interactuen amb la xarxa per mitjà d'API en comptes de fer-ho amb interfícies d'administració estretament lligades al maquinari.

L'abstracció de la xarxa es concreta en la separació en tres plans. El pla de dades o commutació, que és responsable de la transmissió dels paquets basada en les taules de commutació. El pla de control, on tenim els protocols que es fan servir per a manipular els mecanismes de commutació de les dades. El pla de gestió, que es recolza en eines de programari que s'usen per a interactuar amb els protocols en el pla de control.

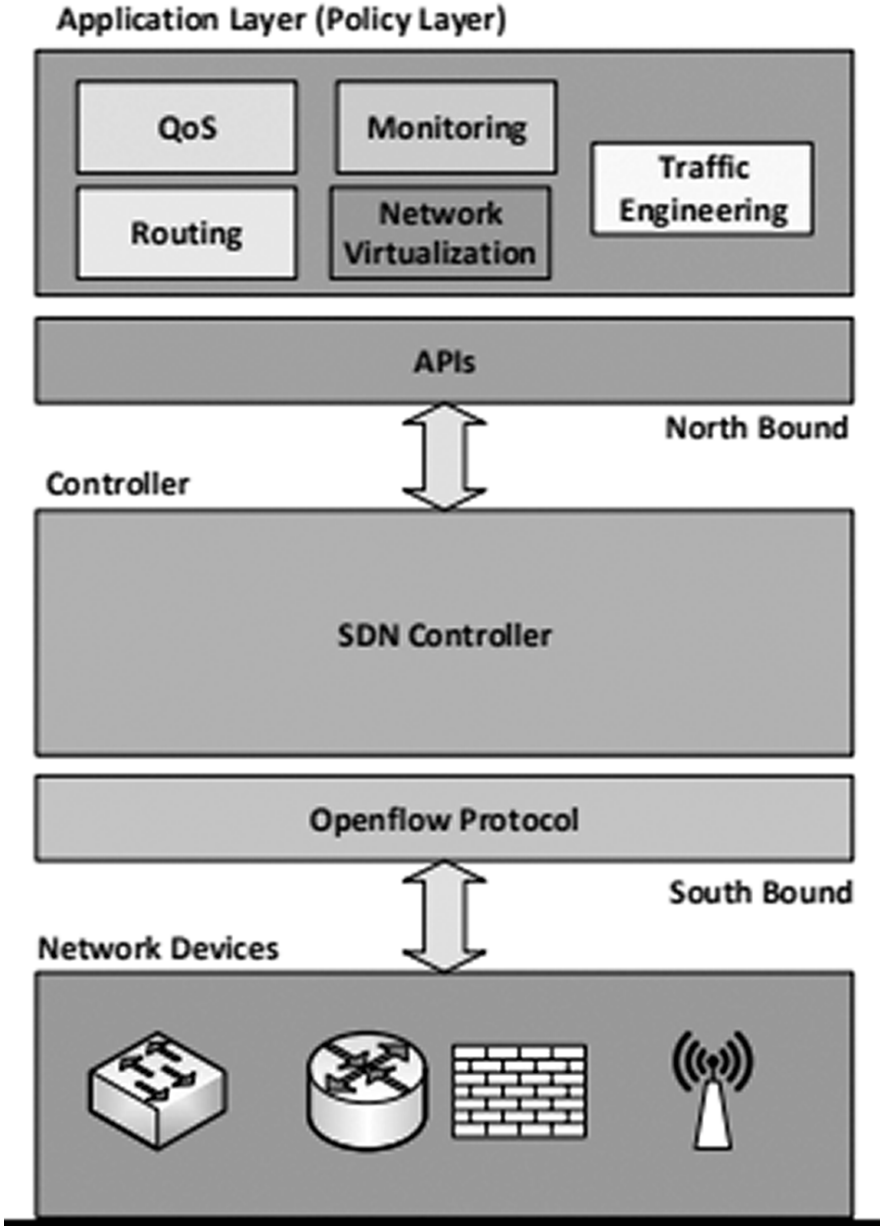
Figura 56. Xarxa a tres nivells



- **Obertura:** l'arquitectura SDN permet la interoperabilitat de diferents proveïdors i la possibilitat de no estar-hi vinculat. El programari intel·ligent pot controlar el maquinari de múltiples proveïdors amb interfícies de programació obertes, com per exemple OpenFlow. Des d'SDN els serveis de xarxa i les aplicacions intel·ligents poden executar-se dintre d'un entorn de programari comú.

En la figura següent es mostra un exemple d'arquitectura SDN en el qual es pot veure que està dividit en tres capes. En la capa inferior tenim els servidors, tallafocs, equips de xarxa, etc. que correspondrien al pla de dades de l'arquitectura SDN. El controladors (*controllers*), els quals estarien a la capa de control, prenen decisions sobre la destinació del trànsit i es comuniquen amb els equips mitjançant una interfície estàndard, com pot ser OpenFlow. En xarxes grans aquests controladors estan gestionats pel que s'anomena orquestrador (*orchestrator*) per mitjà d'interfícies estàndards com Open Stack. Finalment, al nivell superior hi ha el nivell d'aplicació.

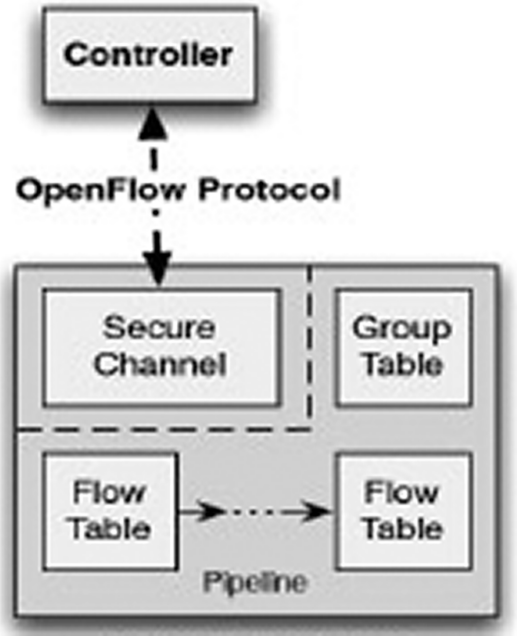
Figura 57. Exemple de xarxa aplicant l'arquitectura SDN



6.3. OpenFlow

OpenFlow en els seus orígens va ser creat a la Universitat de Stanford amb propòsits experimentals i posteriorment va ser estandarditzat per l'ONF. OpenFlow és un protocol obert de comunicacions que permet a un servidor de programari determinar el camí de commutació de paquets en una xarxa de *switchs*. En una xarxa convencional, cada commutador té programari propietari que determina quines accions (és a dir, quin encaminament) ha de fer. Gràcies a l'ús d'OpenFlow, una part de l'encaminament resideix en el mateix *switch*, però és el controlador el que realitza les decisions d'encaminament d'alt nivell. La comunicació entre els dos es fa mitjançant el protocol OpenFlow. Utilitzant aquest protocol, el controlador indica al commutador com ha de tractar els paquets que li arriben.

Figura 58. Commutador OpenFlow



Font: ONF OpenFlow 1.3.0 Switch Specification

El commutador OpenFlow pot ser programat per a realitzar les funcions següents:

- Identificar i categoritzar paquets d'un port d'entrada basat en diversos camps de la capçalera del paquet.
- Processar els paquets de diverses maneres, inclosa la modificació de la capçalera.
- Eliminar o commutar els paquets per un port de sortida o al controlador OpenFlow.

Les instruccions transmeses des del controlador OpenFlow al commutador OpenFlow s'estructuren com a fluxos. Cada flux individual conté uns camps de concordança de paquet, prioritat del flux, instruccions de processament, *timeout* del flux, etc. Els fluxos s'organitzen en taules. Un paquet d'entrada pot ser processat per diverses taules de fluxos abans de ser commutat pel port de sortida.

6.4. SD-WAN

Hi ha tres grans factors que condueixen l'evolució de les WAN:

- El núvol transforma la xarxa.
- Les comunicacions unificades es converteixen en una part crítica de l'empresa. La computació tradicional pren una aproximació centrada en la xarxa.

SD-WAN és una tecnologia que té el potencial de revolucionar el sector de les xarxes WAN. Facilita un nou concepte per al sector de les xarxes que ha de permetre que aquestes xarxes s'adaptin a les necessitats de les aplicacions (xarxa centrada en les aplicacions). Aquest concepte permet a les SD-WAN de convertir-se en un substitut dels serveis d'optimització de xarxes WAN, reduir els costos de gestió, etc.

6.4.1. Arquitectura SD-WAN

Com es mostra a la figura següent, SD-WAN té una arquitectura basada en tres nivells:

- **Xarxa al núvol (*cloud network*).** Facilita la capacitat d'establir connexions per mitjà tant d'infraestructura privada com d'infraestructura pública. Està dissenyada per a facilitar la comunicació entre localitzacions separades geogràficament, i també amb aplicacions al núvol i serveis. Una part molt important de les seves funcionalitats se centra en la seguretat, ja que SD-WAN fa servir la infraestructura d'internet com a xarxa de transport.

- **Serveis virtuals (*virtual services*).** Combina tres tipus de serveis: serveis a seus, serveis als centres de dades (*data centers*) i serveis al núvol. És responsable de l'optimització de la comunicació dels fluxos per a cadascun dels diferents tipus de serveis.

- **Orquestració i anàlisi (*orchestration and analytics*).** Com s'ha explicat quan parlàvem dels principis de funcionament d'SDN, SDN es basa en la separació entre plans de control i de dades. Els principis d'operació a SD-WAN faciliten el mateix mecanisme, aïllant el pla de control en el que s'anomena nivell d'orquestració.

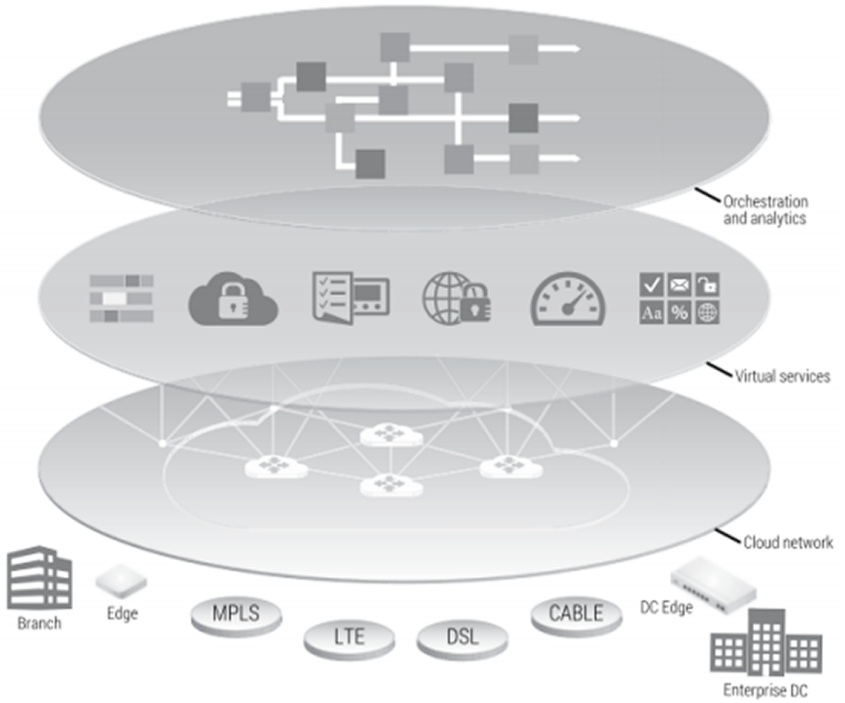
Aquest nivell té tres funcions principals:

1) Pla de gestió: representa un nivell alt d'abstracció per al desenvolupament de polítiques, gestió de la configuració, gestió d'errors, monitorització i presentació d'informes. La consolidació d'aquestes característiques crea una interfície superior de gestió on no cal configurar individualment cada equip local de client (CPE), sinó que la configuració es descarrega des del pla de control centralitzat un cop ha estat autenticat. Aquesta automatització elimina la necessitat de personal qualificat en cadascuna de les seus.

2) Pla de control amb alta disponibilitat i flexibilitat: permet una transició sense problemes de les tecnologies WAN tradicionals a SD-WAN. Les funcions de gestió del pla de control són accessibles per mitjà de serveis web o API.

3) Marc de política empresarial: que s'ocupa de les polítiques de garantia de servei i les estratègies de governança empresarial.

Figura 59. Arquitectura SD-WAN



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.

Un cop explicat el disseny de xarxa, s'ha explicat l'evolució del protocol IPv4 a IPv6. S'han explicat les millores, les característiques més importants i ens hem centrat en dos aspectes importants: el canvi en l'adreçament a IPv6 i la transició d'IPv4 a IPv6.

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.

En l'àmbit de xarxa troncal de les operadores i internet s'han explicat les dues tendències més importants del mercat. Per una banda, l'ús d'MPLS amb l'enginyeria de xarxa i les xarxes privades virtuals, i per l'altra la possibilitat de treballar amb xarxes definides per programari (SD-WAN). Tal com s'ha explicat, són un nou enfocament de xarxa que permet que la xarxa sigui controlada de manera central i intel·ligent mitjançant aplicacions de programari.

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

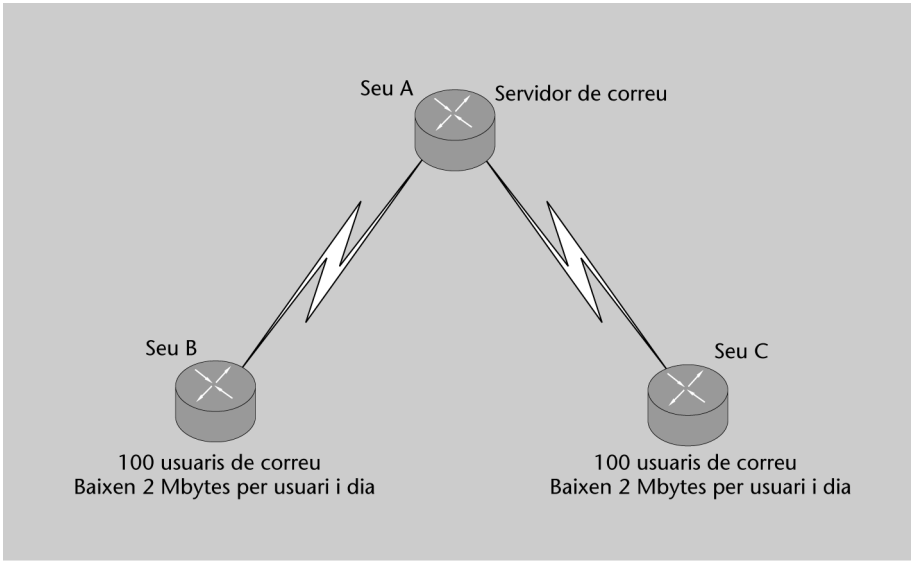
Podeu consultar la *Viquipèdia* a l'adreça http://www.wikipedia.org.

Exercicis d'autoavaluació

1. A la figura 60 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:

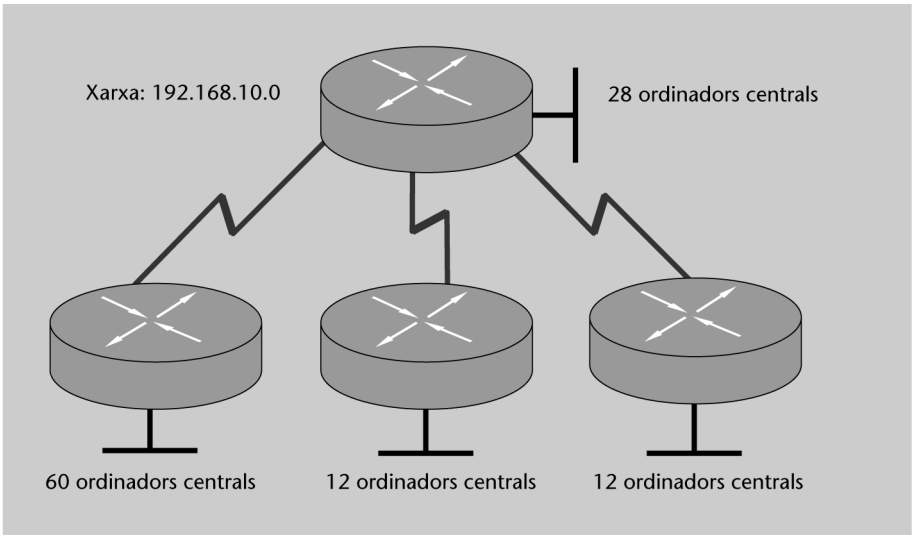
a) El correu es descarrega durant tot el dia.
b) Hi ha un pic de trànsit al matí quan arranquem l'Outlook entre les 8 i les 8.15 hores.

Figura 60.



2. Realitzeu l'adreçament IP de longitud variable (VLSM) adequat per a la topologia de xarxa de la figura 61.

Figura 61.

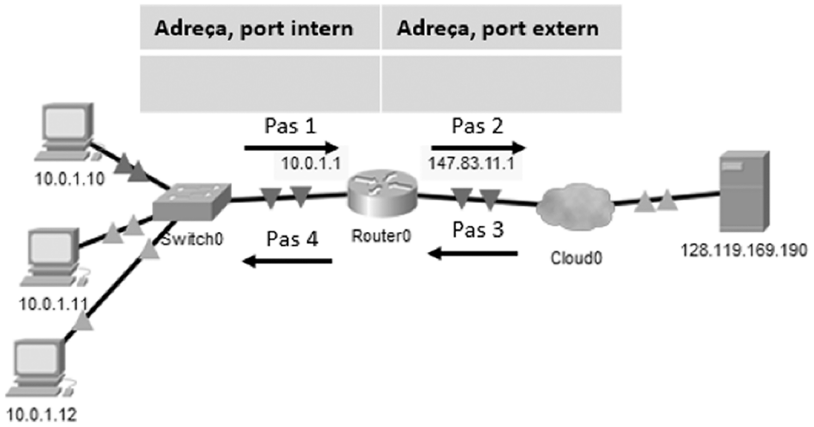


3. Suposeu l'escenari de la figura en què hi ha tres *hosts* amb adreces IP 10.0.1.10, 10.0.1.11 i 10.0.1.12 en una xarxa local Ethernet darrere de l'encaminador que realitza NAT per a sortir a internet. L'encaminador té a la interfície Ethernet l'IP 10.0.1.1, mentre que a la banda internet té l'IP 147.83.11.1. Suposeu que el *host* amb IP 10.0.1.12 envia un datagrama amb destí 128.119.174.185. El port origen és el 3344 i el destí el 80.

Sabent que es realitza NAT *overloading* amb l'IP externa de l'encaminador, indica per a cadascun dels casos que es mostren a la figura (Pas 1, Pas 2, Pas 3 i Pas 4) quines són les

adreces IP origen i destí del datagrama i quins són els números del port origen i destí dels segments TCP dins del datagrama.

Figura 62.



4. A continuació, es mostren les taules NAT de dos encaminadors. Es demana que justifiqueu el tipus de NAT que realitzen en cadascun dels dos casos:

Figura 63.

```
Router#show ip nat trans
Pro   Inside global   Inside local   Outside local   Outside global
---   192.2.2.1       10.1.1.1       ---             ---
---   192.2.2.2       10.1.1.2       ---             ---
```

```
Router#sh ip nat trans
Pro Inside global      Inside local       Outside local      Outside global
tcp 170.168.2.1:11003  10.1.1.1:11003     172.40.2.2:23      172.40.2.2:23
tcp 170.168.2.1:1067   10.1.1.1:1067      172.40.2.3:23      172.40.2.3:23
```

5. Expressa de forma comprimida les adreces següents:

a) 2000:0000:0000:0000:0000:ABCD:0000:0025

b) 3FFF:FF00:0000:0000:ACAD:0025:0000:0127

c) FF00:ACAD:0000:0000:1234:0000:0000:0001

6. A partir de les adreces simplificades següents, obté l'adreça sense simplificar:

a) ::1

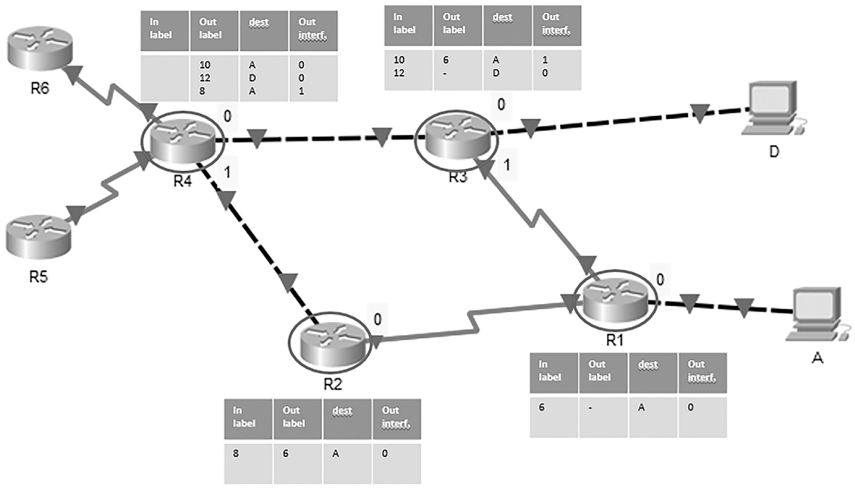
b) 3E80:0070::0098:0000:0001

c) FFFF::4E00:1235:0:34

7. Considereu la xarxa següent amb els encaminadors R1 a R4 amb MPLS. Suposem que els encaminadors R5 i R6 passen a formar part de la xarxa MPLS. Es vol realitzar enginyeria de trànsit de manera que els paquets des d'R6 amb destí A siguin encaminats per R6-R4-R3-R1 i els paquets des d'R5 destinats a A siguin encaminats per R5-R4-R2-R1. Obté les taules MPLS a R5 i R6 i les modificacions necessàries a la taula R4 per a un funcionament correcte.

Nota: etiqueta a R6 amb destí A: 7, etiqueta a R5 amb destí A: 5

Figura 64.


R6
R5
R4
R3
R2
R1
D
A
0
1
0
1
0
0
0
In label | Out label | dest | Out interf.
10 12 8 | A D A | 0 0 1
In label | Out label | dest | Out interf.
10 12 | 6 - | A D | 1 0
In label | Out label | dest | Out interf.
8 | 6 | A | 0
In label | Out label | dest | Out interf.
6 | - | A | 0

Solucionari

1. Mirant la figura 60 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 bytes × 8 bits/byte) / 8 hores × 3.600 segons/hora = 556 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 bytes × 8 bits/byte)/15 minuts × 60 segons/minut = 88,9 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 *hosts*
	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

3.

Pas 1:

Adreça origen del datagrama: 10.0.1.12

Adreça destí del datagrama: 128.119.174.185

Port origen: 3344

Port destí: 80

Pas 2:

Adreça origen del datagrama: 147.83.11.1

Adreça destí del datagrama: 128.119.174.185

Port origen: 5066

Port destí: 80

Un cop rep el datagrama, l'encaminador genera un nou número de port que no estigui ja utilitzat a la taula NAT. S'ha escollit el 5066. A més, en aquest cas, com s'ha indicat, es fa NAT *overloading* amb la mateixa IP externa de l'encaminador.

Adreça, port intern	Adreça, port extern
10.0.1.12 - 3344	147.83.11.1 - 5066

Pas 3:

Adreça origen del datagrama: 128.119.174.185

Adreça destí del datagrama: 147.83.11.1

Port origen: 80

Port destí: 5066

Pas 4:

Adreça origen del datagrama: 128.119.174.185

Adreça destí del datagrama: 10.0.1.12

Port origen: 80

Port destí: 3044

En el Pas 4 l'encaminador rep el datagrama, examina la seva taula NAT per a obtenir l'IP i el port corresponents a la xarxa interna.

4. En el primer cas es pot tractar tant de NAT estàtic com dinàmic ja que hi ha una translació un a un de l'adreça local interna a l'adreça global externa. En conseqüència, només mirant la taula no podem saber amb quin dels dos tipus de NAT es treballa. El que es pot garantir és que no es treballa amb PAT.

En el segon cas, en canvi, s'utilitza NAT *overload*. El protocol de sortida és TCP, i l'adreça global interna és la mateixa per a les dues entrades de la taula.

5.

a) S'eliminen els zeros consecutius del primer conjunt de l'adreça.

2000::ABCD:0:25

b) S'eliminen els zeros consecutius del primer conjunt de l'adreça.

3FFF:FF00::ACAD:25:0:127

c) En aquest cas, com que els zeros consecutius en tots dos conjunts poden permetre expressar l'adreça comprimida de dues formes possibles, mostrarem les dues possibilitats. Recordeu que :: per a representar conjunts de zeros consecutius només es pot utilitzar una única vegada en una adreça IPv6.

FF00:ACAD::1234:0:0:1 o també FF00:ACAD:0:0:1234::1

6. Recordeu que l'adreça IPv6 és un conjunt de 128 bits dividit en grups de 16 bits expressat en hexadecimal. Això fa que una adreça IPv6 tingui sempre 8 grups. Per tant, sempre que hi hagi :: caldrà afegir tants grups de zeros com calgui per a arribar a 8 grups.

a) 0000:0000:0000:0000:0000:0000:0000:0001

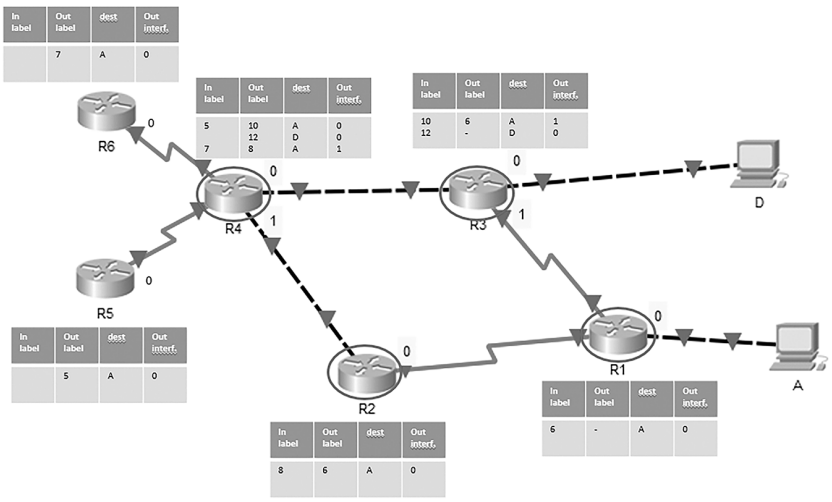
a) 3EF8:0070:0000:0000:0000:0098:0000:0001

a) FFFF: 0000: 0000: 0000:4E00:1235:0000:0034

7. Com s'ha indicat, cal crear les taules MPLS d'R5 i R6, en què només tenim l'etiqueta de sortida, destí i interfície de sortida.

A més, cal modificar la taula MPLS d'R4. A la figura inicial, si examinem les taules MPLS, es mostra que el trànsit amb destí A va per dues rutes: per R4-R3-R1 i per R4-R2-R1. Sabent això, l'única modificació que cal fer a la taula MPLS d'R4 és incloure quina etiqueta d'entrada es vol que vagi per una interfície de sortida o una altra. A la nova taula d'R4 es mostra que el trànsit amb etiqueta 5 s'enviarà per la interfície 0, mentre que el trànsit de l'etiqueta 7 s'enviarà per la interfície 1.

Figura 65.



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***.

contenidor 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 ***synchonous digital hierarchy***.

SONET *m* Vegeu ***synchonous optical network***.

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

synchonous 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 **contenidor 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.

Citrix. «SDN 101: Introducción a Software Defined Networking». https://www.citrix.com/content/dam/citrix/en_us/documents/oth/sdn-101-an-introduction-to-software-defined-networking-es.pdf

Ghein, L. de (2007). *MPLS Fundamentals*. Cisco Press.

Göransson, P.; Black, C. (2014). *Software Defined Network. A comprehensive approach*. Elsevier.

Graziani, R. (2017). *IPv6 Fundamentals*. Second Edition. Indianàpolis: Cisco Press.

Hagen, S. *IPv6 Essentials*. O'Reilly.

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.or

Metzler, J.; Metzler, A. (2015). *Guide to WAN Architecture Design*. Webtorials.

Nadeau, T. D.; Gray, K. (2013). *SDN. Software Defined Network*. O'Reilly.

Open Networking Foundation Website. https://www.opennetworking.org/software-defined-standards/overview/

Rubio, Jaime H. *¿Qué es SDN?* https://www.ciena.com.mx/insights/what-is/What-is-SDN_es_LA.html

Uppal, S. (2015). *Software Defined WAN for Dummies*. John Wiley & Sons, Ltd.