



Interconnexió de Xarxes

LA PILA OSI

Nivel de Aplicación
Servicios de red a aplicaciones.

Nivel de Presentación
Representación de los datos

Nivel de Sesión
Comunicación entre dispositivos de la red.

Nivel de Transporte
Comunicación extremo-a-extremo y fiabilidad de los datos.

Nivel de Red
Determinación de ruta e IP (Direccionamiento lógico)

Nivel de Enlace de Datos
Direccionamiento físico (MAC y LLC)

Nivel Físico
Señal y transmisión binaria

Índex

- Introducció
- Protocol d'Internet versió 4 (IPv4)
 - Datagrames IP
 - Fragmentació i agregació (*"assembling"*)
 - Adreces IP i Encaminament
 - Control de Flux
 - Qualitat de Servei
- Protocol d'enllaç punt a punt (PPP)
- IPv6

Definició Capa de Xarxa

- La capa 3 o de xarxa permet la interconnexió entre diferents xarxes.
- Aquesta interconnexió pot fer-se entre xarxes locals, com Ethernet o WiFi, interconnexió entre xarxes de transport com ATM, etc.

I després de les LAN?

- Les xarxes LAN permeten intercanviar informació entre equips
- En alguns casos, és necessari interconnectar xarxes LAN, fent servir la pròpia xarxa del proveïdor d'Internet o fent servir línies dedicades
- El camí seria: Xarxes LAN < Xarxes Accés < Xarxes WAN (*Wide Area Networks*)
- La capa d'enllaç varia entre els diferents tipus de xarxes
- La topologia que ens dona un protocol MAC és pla. No hi ha jerarquia (Excepció: Switchos VLAN).

Cap a IP

- Davant d'aquesta situació sorgeix la necessitat de disposar de una capa superior que permeti:
 - intercanviar informació entre diferents xarxes
 - Jerarquitzar la xarxa
- Aquesta és la capa de Xarxa i permet:
 - Intercanvi d'informació entre xarxes amb diferents capes d'enllaç
 - fer servir les adreces lògiques de xarxa (Jerarquia)
- El protocol més utilitzat en l'actualitat es IP

Intro: Topologia de xarxes

Xarxes: TIPUS DE PROTOCOLS DE XARXA

PROTOCOLS ENCAMINABLES

o

ROUTED PROTOCOLS

- IP
- IPX

PROTOCOLS D'ENCAMINAMENT

o

ROUTING PROTOCOLS

- RIP
- IGRP
- EIGRP
- BGP

Tipus de Xarxes

Introducció a l'encaminament o "routing"

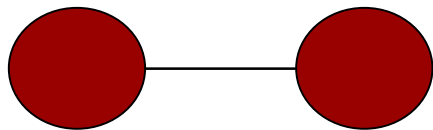
- Una xarxa de telecomunicacions és una col·lecció de terminals, enllaços i nodes que es connecten per tal de permetre la comunicació entre els usuaris, intercanviar fitxers i compartir recursos.

Classificació xarxes

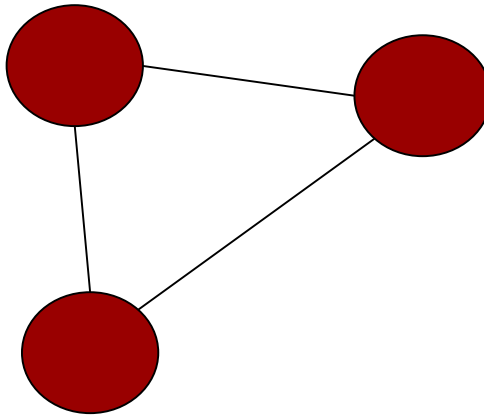
En funció de la topologia dels enllaços podem tenir els següents tipus de xarxes:

1. Xarxes dedicades

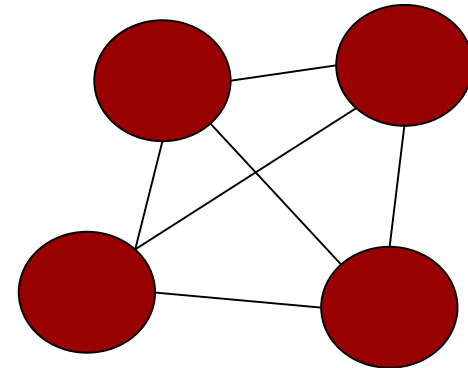
També conegudes com *xarxes punt a punt*, *connectivitat total* o *mallades*. Tots els equips estan connectats entre sí.



Nodes: 2
Connexions: 1



3
3



4
6

Classificació xarxes

En el cas de sistemes dedicats, l'evolució és...

Si tenim N nodes tindrem $N \times (N-1)/2$ enllaços

$N-1$ interfícies per node

Avantatges d'aquest tipus de xarxes:

- 1.- La seva senzillesa a l'hora de planificar-la

Desavantatges:

- 1.- Cost de la xarxa degut al nº d'interfícies i medis
- 2.- L'administració es complica quan incrementen els medis i les interfícies

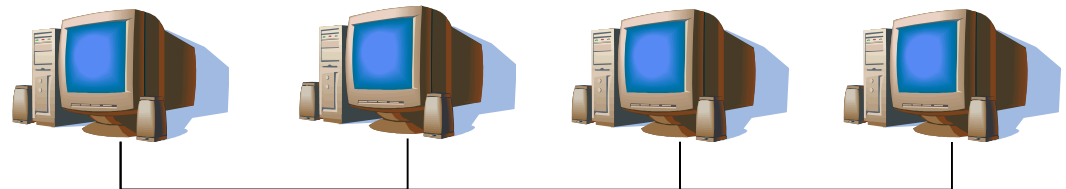
Classificació xarxes

2. Xarxes de Difusió

- Tenen un medi de connexió per connectar entre si tots els equips
- Necessita multiplexació de les dades per poder transmetre
- *REQUEREIX un Sistema per evitar col·lisions*

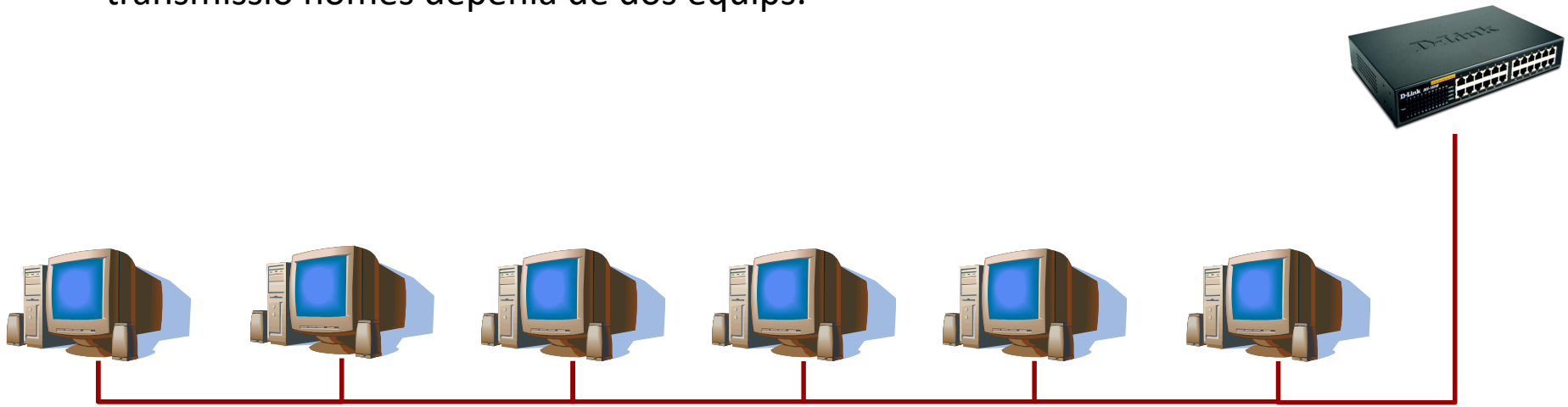
Exemples:

Xarxes d'àrea local
(Ethernet)



Classificació xarxes

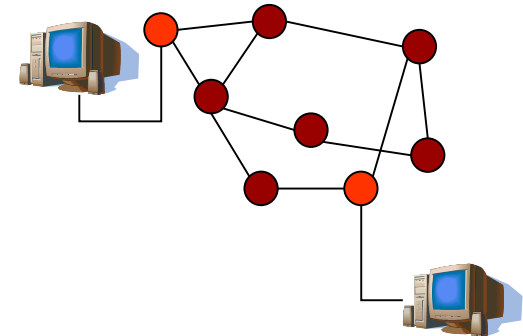
- En aquest tipus de xarxa, quan un equip transmet, tota la resta reben la informació, decidint individualment, si aquesta informació els interessa o no.
- L'accés al canal s'aconsegueix sent el més ràpid. El primer que arriba al canal, si està lliure, se'l queda i comença a transmetre
- Difereix per tant molt del cas anterior, on simplement la transmissió només depenia de dos equips.



Classificació xarxes

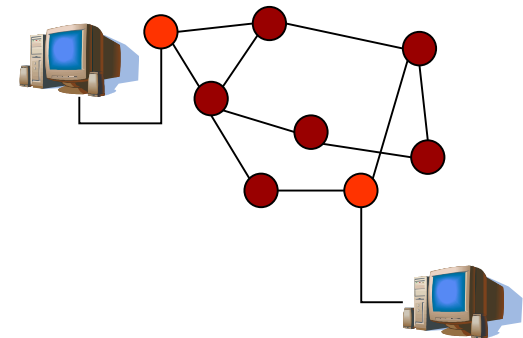
3. Xarxes de Commutació

- Fa servir mitjans per commutar els paquets que li arriben.
(d'aquí el seu nom)
- Els nodes de commutació transfereixen la informació que arriba a les seves entrades cap a la sortida corresponent.
- Els nodes poden ser de dos tipus:
 - a) Nodes de trànsit: Són aquells que no tenen cap equip (DTE) connectat a ells
 - b) Node perifèric: Són aquells que tenen un o més d'un equip (DTE) connectat directament



Classificació xarxes

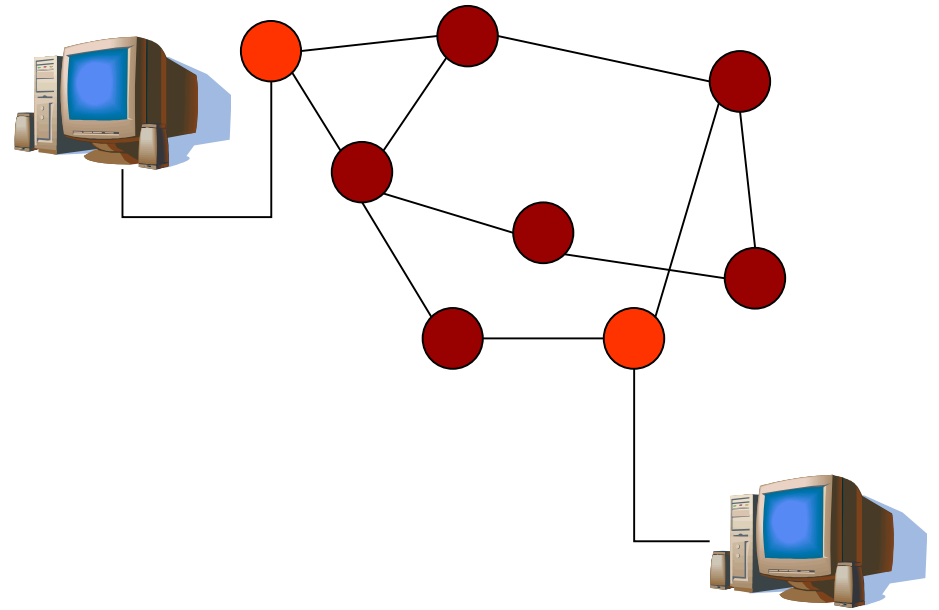
- Un node pot ser simultàniament de trànsit i perifèric
- Aquests nodes no actuen com un simple repetidor passiu sinó que fan tasques de:
 - a) Control d'errors i Flux
 - b) Detecció de saturació de la xarxa
 - c) Encaminament (decidir per on han d'anar (els paquets))
- Generalment els nodes de trànsit solen ser més ràpids que els perifèrics donat que han de commutar (els paquets) a gran velocitat
- Per raons de seguretat, es recomana tenir dos camins independents per anar d'un punt origen a un destí



Classificació xarxes

Tipus de xarxes de commutació:

- a. *Commutació de circuits*
- b. *Commutació de missatges*
- c. *Commutació de paquets*



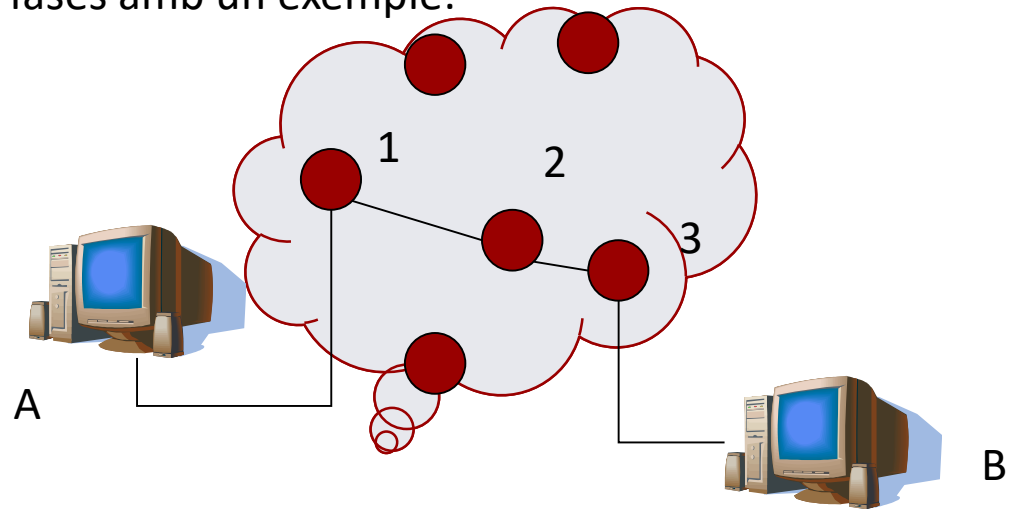
Classificació xarxes

a. Xarxes basades en la commutació de circuits

-El procés de comunicació implica 3 fases:

- 1.- Establiment de la connexió
- 2.- Transferència de la informació
- 3.- Alliberament de la connexió

Veiem com funcionen aquestes fases amb un exemple:

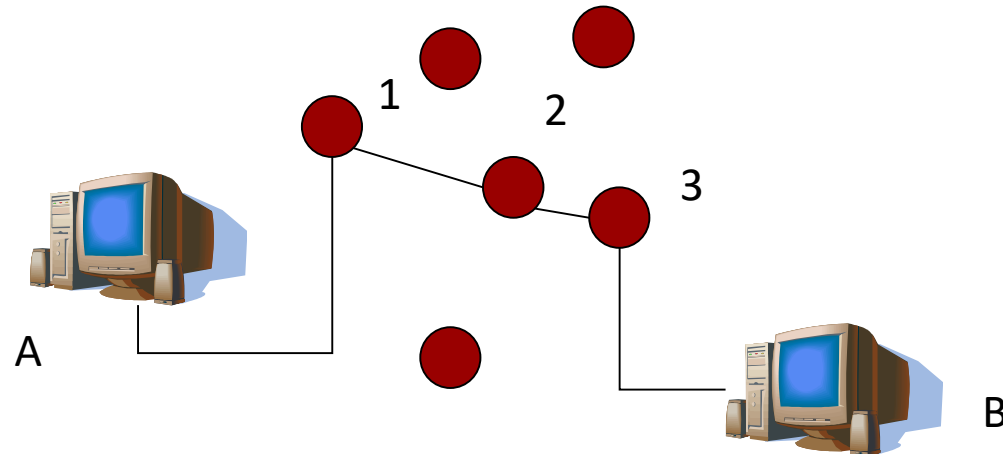


Classificació xarxes

Volem transferir un fitxer de A cap a B. La connexió requereix passar per tres nodes de commutació (#1, #2 i #3)

Fase 1: Establiment de la connexió:

Donat que A vol connectar-se amb B, la xarxa ha de reservar un camí per que les dades puguin circular entre A i B. Això implica que A enviarà a #1 l'adreça de B, sent 1 l'encarregat de buscar el segon pas. (#2)

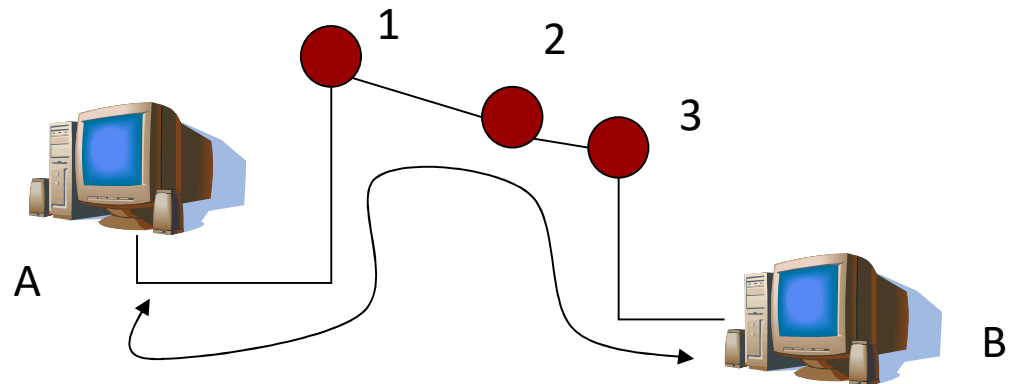


Classificació xarxes

Un cop la petició arriba a #2, busca quin és el millor camí per anar cap a B. Per tant, #2, veurà que ha d'establir la connexió amb #3

Finalment #3 veu que B està directament connectat a ell i l'indica que A vol establir la connexió. Si està d'acord, accepta.

El camí està establert i el canal reservat!! ***That's right!!***



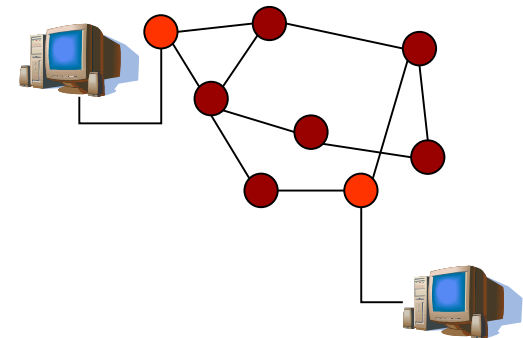
Classificació xarxes

Fase 2: Transferència de la informació.

Donat que el camí ja està creat, no hi ha cap retard en la transmissió de les dades.

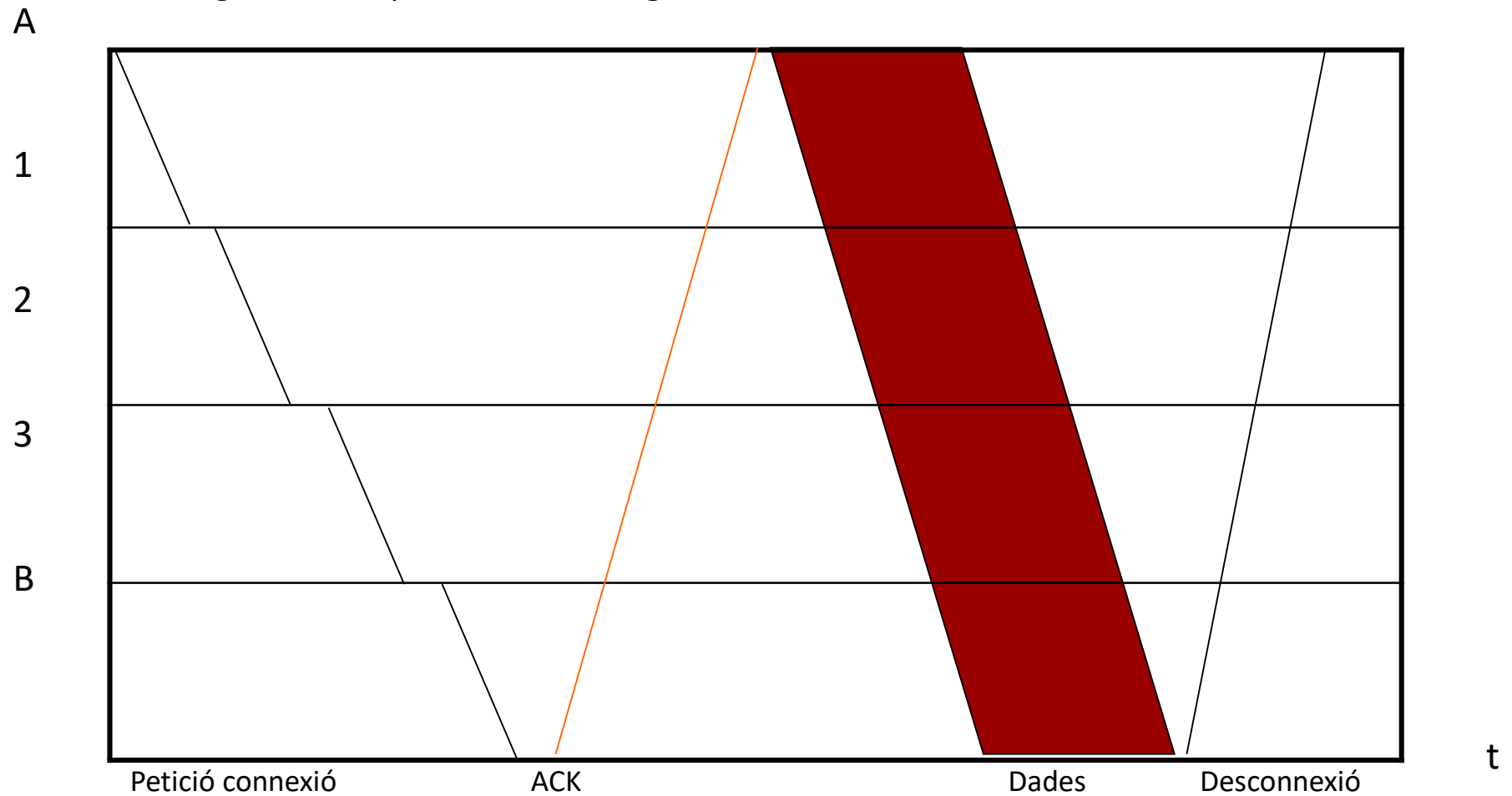
Fase 3: Alliberament de la connexió.

La transmissió finalitza quan s'envia la petició de desconnexió. Els nodes alliberen les connexions entre entrades i sortides que estableixen el circuit. Aquest senyal no pateix cap mena de retard.



Classificació xarxes

El diagrama temporal seria el següent:



Classificació xarxes

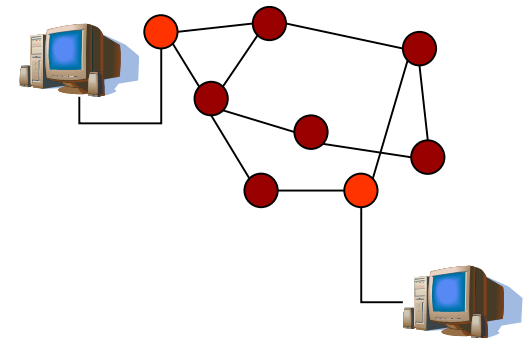
Característiques d'aquest tipus de xarxes.

Pros:

- Tenen el seu origen a les xarxes telefòniques (PSTN i XDSI)
- Permet tenir un canal dedicat, gaudint de tot l'ample de banda
- Tecnologia senzilla amb gran experiència

Contres:

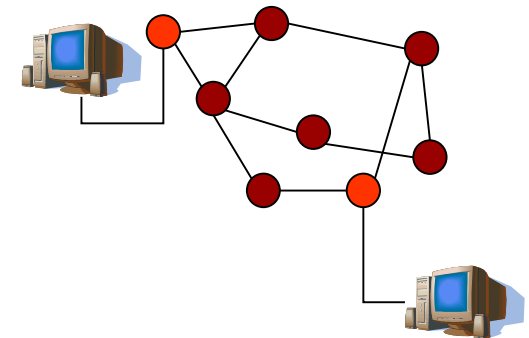
- Emissor i receptor han de transmetre a la mateixa velocitat
- Poc flexible
- Saturació de la xarxa



Classificació xarxes

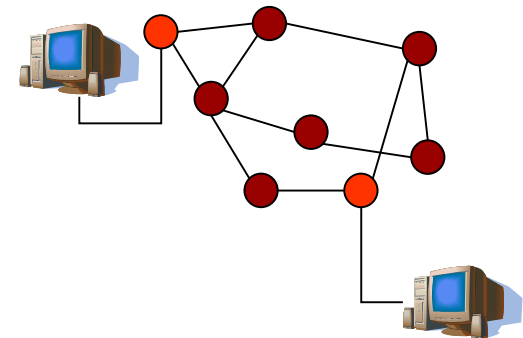
b. Xarxes basades en la commutació de missatges

- Específicament dissenyades per transmetre bits
- No s'estableix cap camí dedicat entre emissor i receptor
- Els DTEs transmeten pel canal que els uneix al commutador (DCE)
- Quan el missatge arriba al commutador, aquest és guardat, es busca la direcció destí i s'adreça el missatge pel camí idoni.
- Aquest procés es va repetint fins que arriba el missatge la destinació
- La transmissió es realitza a la màxima capacitat de la xarxa i.e. 64 Kb/s, 2 Mb/s,...)



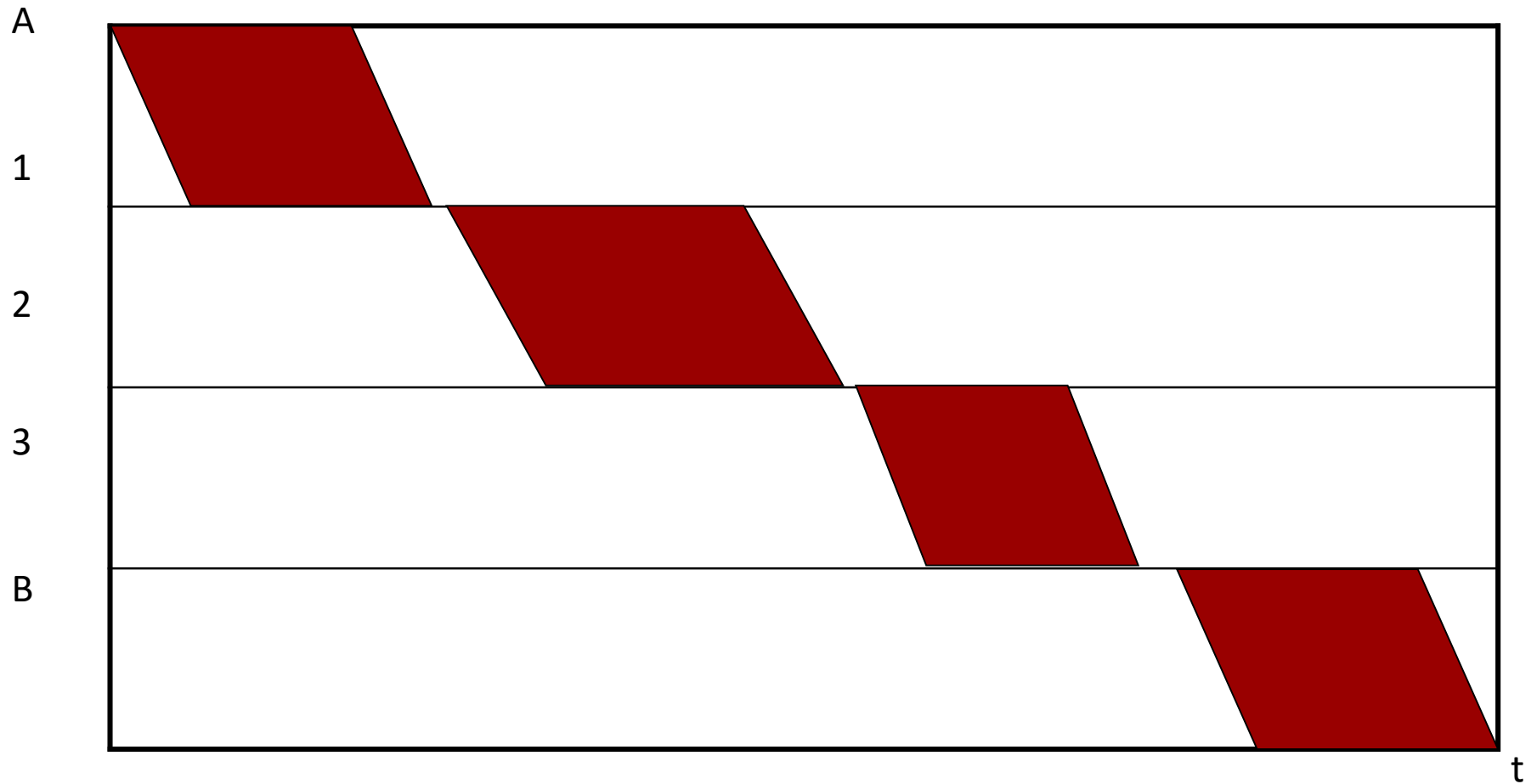
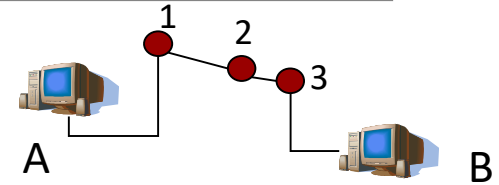
Classificació xarxes

- Cada node de commutació pot rebre tants missatges com enllaços tingui. Abans d'enviar-los haurà de guardar-los i decidir la millor ruta.
- El principal problema que veiem és el de la saturació del commutador, ja que enlloc s'especifica la mida màxima dels missatges.
- Aquest tipus de xarxa no pot implementar-se experimentalment.



Classificació xarxes

El diagrama temporal seria el següent:



Classificació xarxes

c. Xarxes basades en la commutació de paquets

- Utilitza la mateixa filosofia que la commutació de missatges, però ara es produeix una fragmentació en paquets més petits per tal de facilitar la transmissió
- En funció del mecanisme d'encaminament, hi ha dos tipus de xarxes de commutació de paquets:

c.1) Commutació per datagrames

c.2) Commutació per circuits virtuals

Classificació xarxes

c.1) Commutació per datagrames

- Cada fragment té una longitud màxima que depèn de la xarxa.
- Cada fragment porta una capçalera on consta l'adreça del destinatari i la pròpia de l'origen
- Cada paquet pot anar-hi pel camí que en aquell instant de temps es consideri millor. Això implica que els paquets poden arribar amb un cert desordre.
- El destinatari és l'encarregat d'ordenar-los si fos necessari
- Un inconvenient d'aquesta xarxa és que ha de fer la mateixa feina moltes vegades. Si un missatge té N paquets, s'ha d'encaminar N vegades cap al mateix destí

Classificació xarxes

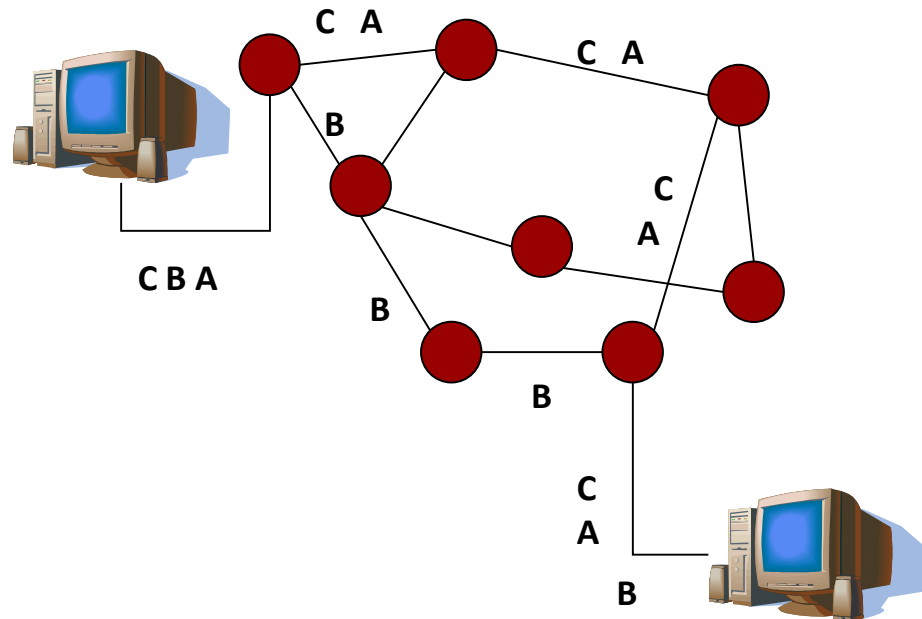
Missatge



Paquets



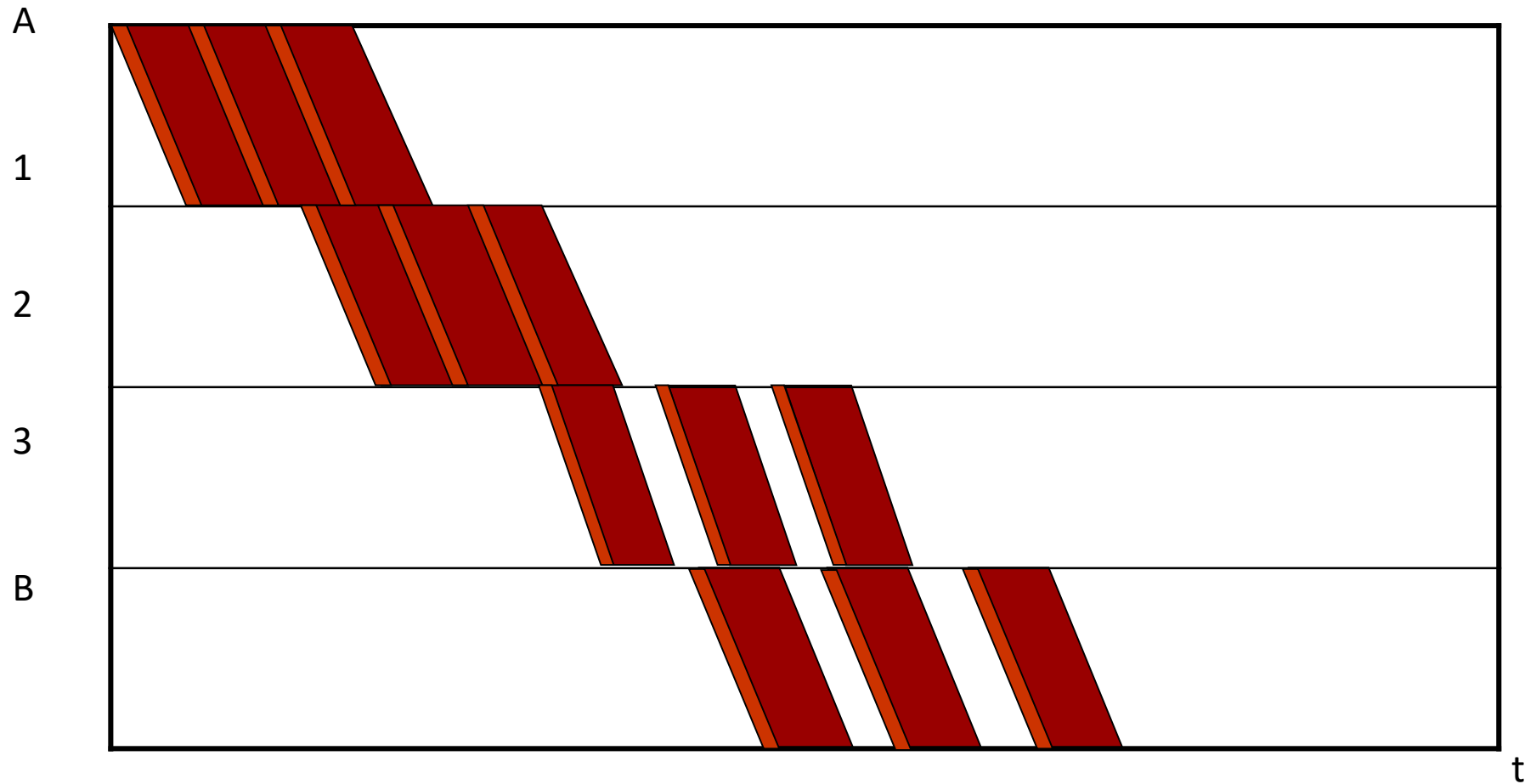
Paquets + capçalera



-Aquest tipus de commutació no té, en principi, qualitat de servei (QoS):
la pèrdua de paquets no té per que ser indicada a l'origen

Classificació xarxes

Commutació per datagrames



Classificació xarxes

c.2) Commutació per circuits virtuals

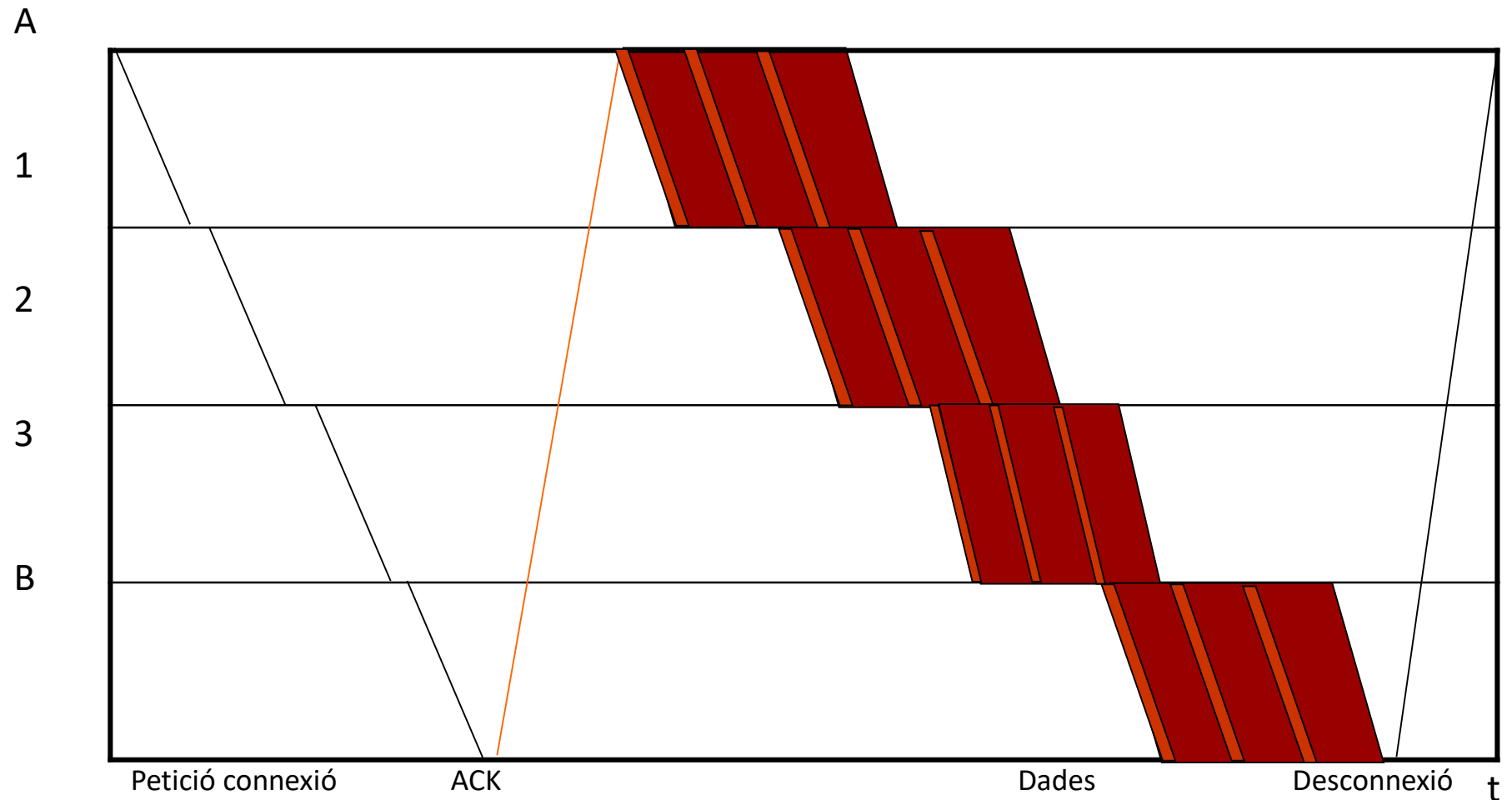
- Evita múltiples encaminaments dels diferents paquets d'un mateix missatge
- Evita per tant el desordre.
- El camí no es reserva, la xarxa pot utilitzar el canal per altres commutacions, però quan arriba el paquet per força ha de passar pel canal escollit a priori.
- Funcionament:
 1. S'envia un petit paquet de senyalització per demanar l'establiment del circuit virtual
 2. Aquest paquet al començament només porta l'adreça destí. A mesura que va passant pels diferents nodes es va establint el camí virtual i al paquet se li afegeix un identificador del circuit virtual per on ha passat
 3. El node destí confirma l'establiment i accepta la connexió amb un missatge de tornada

Classificació xarxes

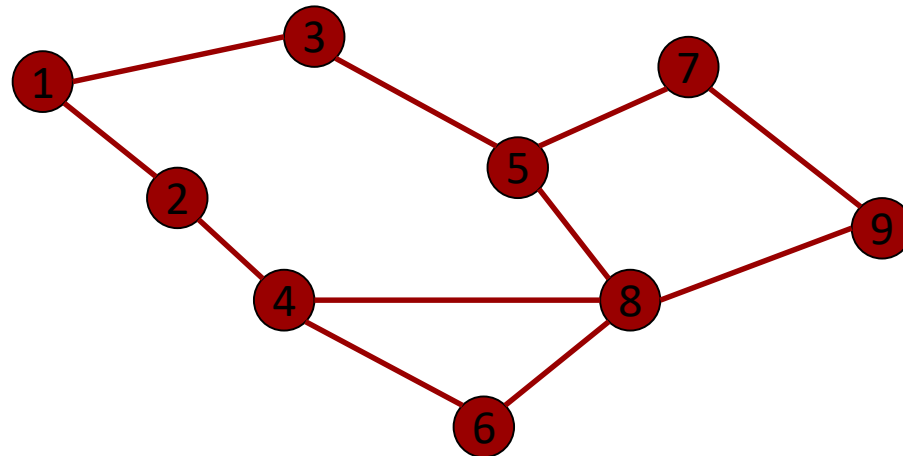
- Per tant, cada paquet que vagi al mateix destí i provingui del mateix origen anirà sempre pel mateix camí de senyalització.
- Els diferents paquets portaran a la capçalera l'identificador de circuit virtual, minimitzant el retard que es produiria en tornar a encaminar les dades.
- Finalment, s'allibera el circuit virtual.
- L'establiment del circuit, es diu virtual ja que el seu ús no és exclusiu.

Classificació xarxes

El diagrama temporal seria el següent:



Example Routing

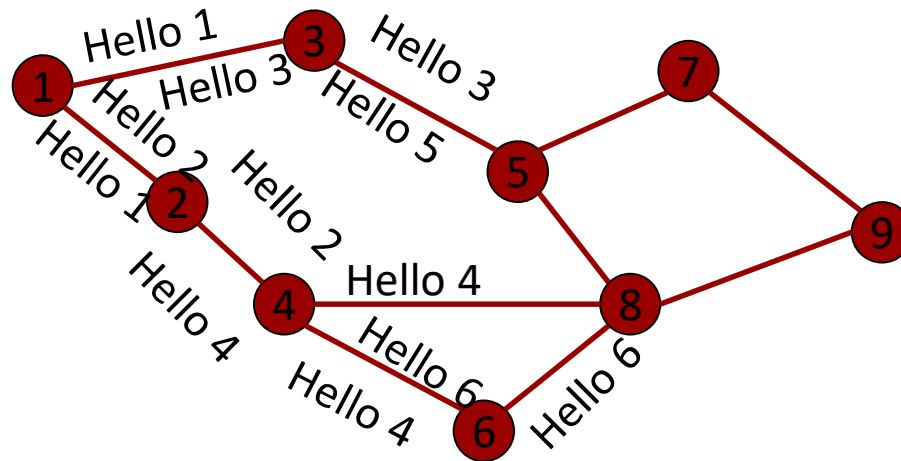


	Router 1	Router 2	Router 3	Router 4	Router 5	Router 6	Router 7	Router 8	Router 9
Router 1									
Router 2									
Router 3									
Router 4									
Router 5									
Router 6									
Router 7									
Router 8									
Router 9									

Enviament de paquets "hello" per les interfícies

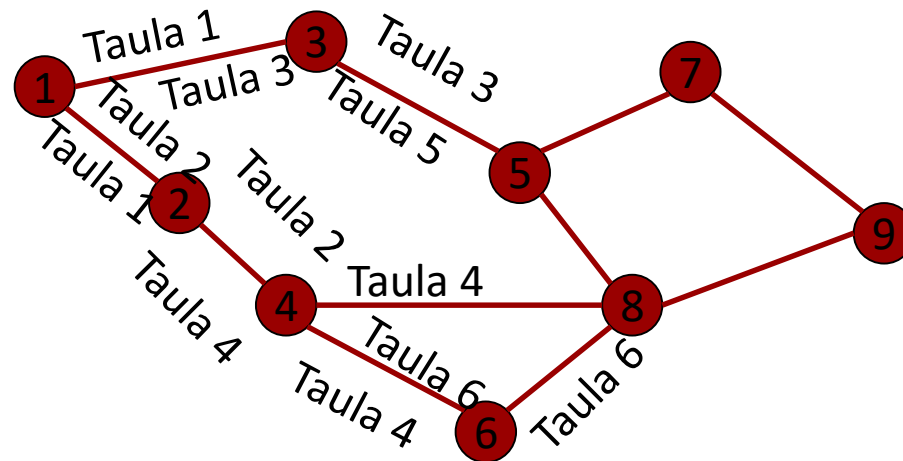
La mètrica definirà el millor camí per enviar dades entre un dispositiu i un altre. Tipus de mètrica:

- Ample de Banda
- Next hop
- Combinatòria balancejada
- Altres



	Router 1	Router 2	Router 3	Router 4	Router 5	Router 6	Router 7	Router 8	Router 9
Router 1		2	3						
Router 2	1			4					
Router 3	1				5				
Router 4		2				6		8	
Router 5			3				7	8	
Router 6				4				8	
Router 7					5				9
Router 8				4	5	6			9
Router 9							7	8	

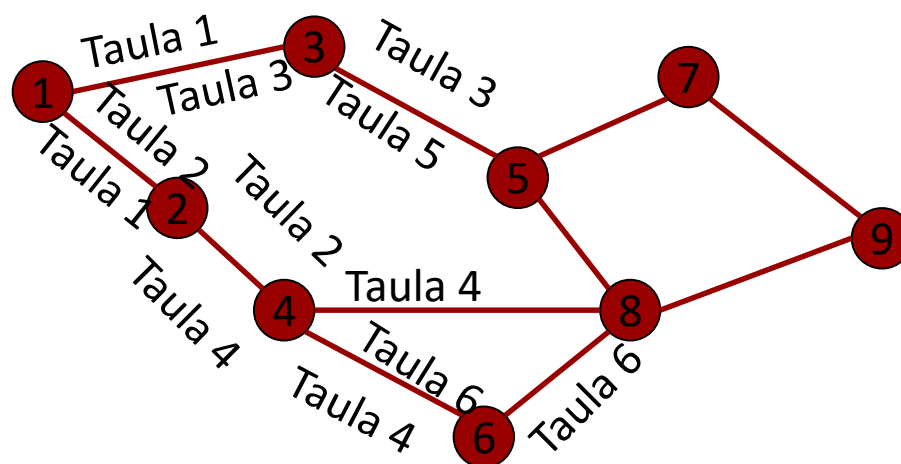
Retransmissió de les taules d'encaminament: Intercanvi Informació



	Router 1	Router 2	Router 3	Router 4	Router 5	Router 6	Router 7	Router 8	Router 9
Router 1		2	3	2	3				
Router 2	1		1	4		4		4	
Router 3	1	1			5		5	5	
Router 4	2	2			8	6 & 8		8	
Router 5			3				7	8	8
Router 6		4		4	8			8 & 4	8
Router 7			5		5			5 & 9	9
Router 8	5	4	5	4	5	6 & 4	5		9
Router 9				8	7 & 8	8	7	8	

Retransmissió de les taules (II)

En cas de no conèixer la ruta, tenim un enviament per defecte que s'encarregarà de gestionar el paquet



	Router 1	Router 2	Router 3	Router 4	Router 5	Router 6	Router 7	Router 8	Router 9
Router 1		2	3	2	3	2	3	2 & 3	
Router 2	1		1	4	4	4		4	
Router 3	1	1			5	4	5	5	5
Router 4	2	2	8		8	6 & 8		8	6
Router 5	3 & 8	8	3	8		8	7	8	8
Router 6	4	4	8	4	8		8	8 & 4	8
Router 7			5		5			5 & 9	9
Router 8	5 & 4	4 & 5	5	4	5	6 & 4	5		9
Router 9	8	8	8	8	7 & 8	8	7	8	

Requeriments per l'intercanvi d'informació entre xarxes

- Proporcionar una connexió entre les xarxes
 - Com a mínim es necessita una connexió física i un control d'enllaç
- Proporcionar serveis que permetin encaminar i entregar la informació entre processos localitzats en diferents xarxes
- Proporcionar un servei de control que sigui conscient de l'estat en que es troben les diferents xarxes i encaminadors

Requeriments per l'intercanvi d'informació entre xarxes

- Proporcionar els serveis de forma que siguin independents de les diferents xarxes
 - Diferents mètodes d'encaminament
 - Gestió de noms, adreces i directoris
 - Diferent mida màxima de paquets
 - Segmentació de la informació
 - Diferents mecanismes d'accés a la xarxa
 - Diferents temps d'espera
 - Evitar retransmissions degudes a temps d'espera d'ACKs

Requeriments per l'intercanvi d'informació entre xarxes

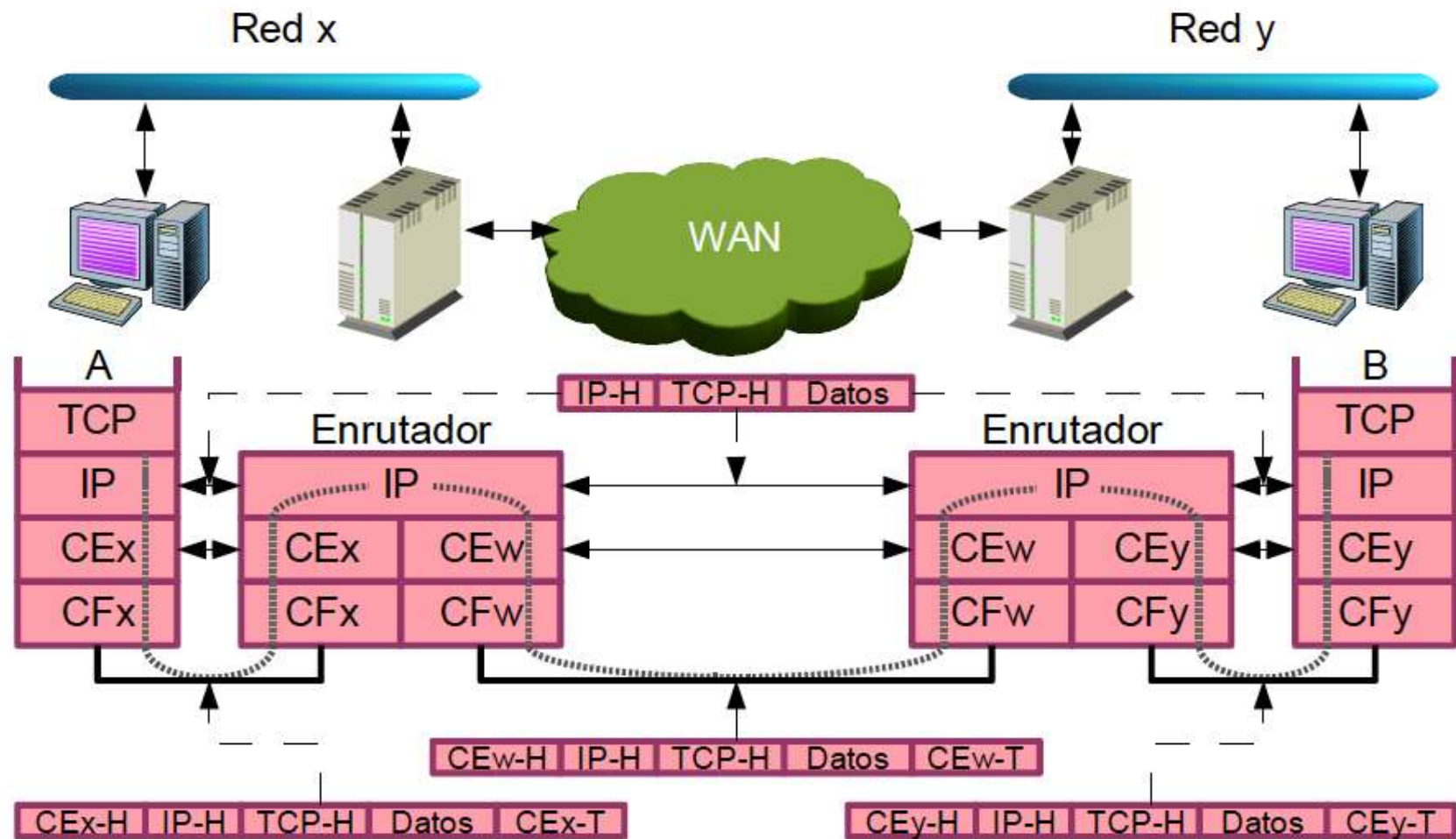
- Recuperació d'errors
 - La capa de xarxa no ha de dependre o no ha de veure's interferida per mètodes de recuperació d'errors de cada xarxa
- Informació de l'estat
 - Les diferents xarxes proporcionen informació de les prestacions i errors de forma diferent
- Tècniques d'encaminament
 - L'encaminament ha de tenir en compte l'estat de cada xarxa i ha d'adaptar-se adequadament
- Orientada a connexió o sense connexió
 - Independent de circuits virtuals i/o datagrames

A diagram of an IPv4 header structure. It consists of a dark gray rectangular block with the text 'IPv4' in white at the top right. Below this block is a horizontal bar divided into three colored segments: dark red, orange, and lime green.

IPv4

IP versió 4

IPv4



- Protocol no orientat a connexió
- Els paquets treballen en mode datagrama
- Pensat per:
 - L'encaminament és independent pels diferents paquets
 - No sobrecarrega la xarxa. Busca el camí més ràpid en aquell instant
 - No QoS

IPv4

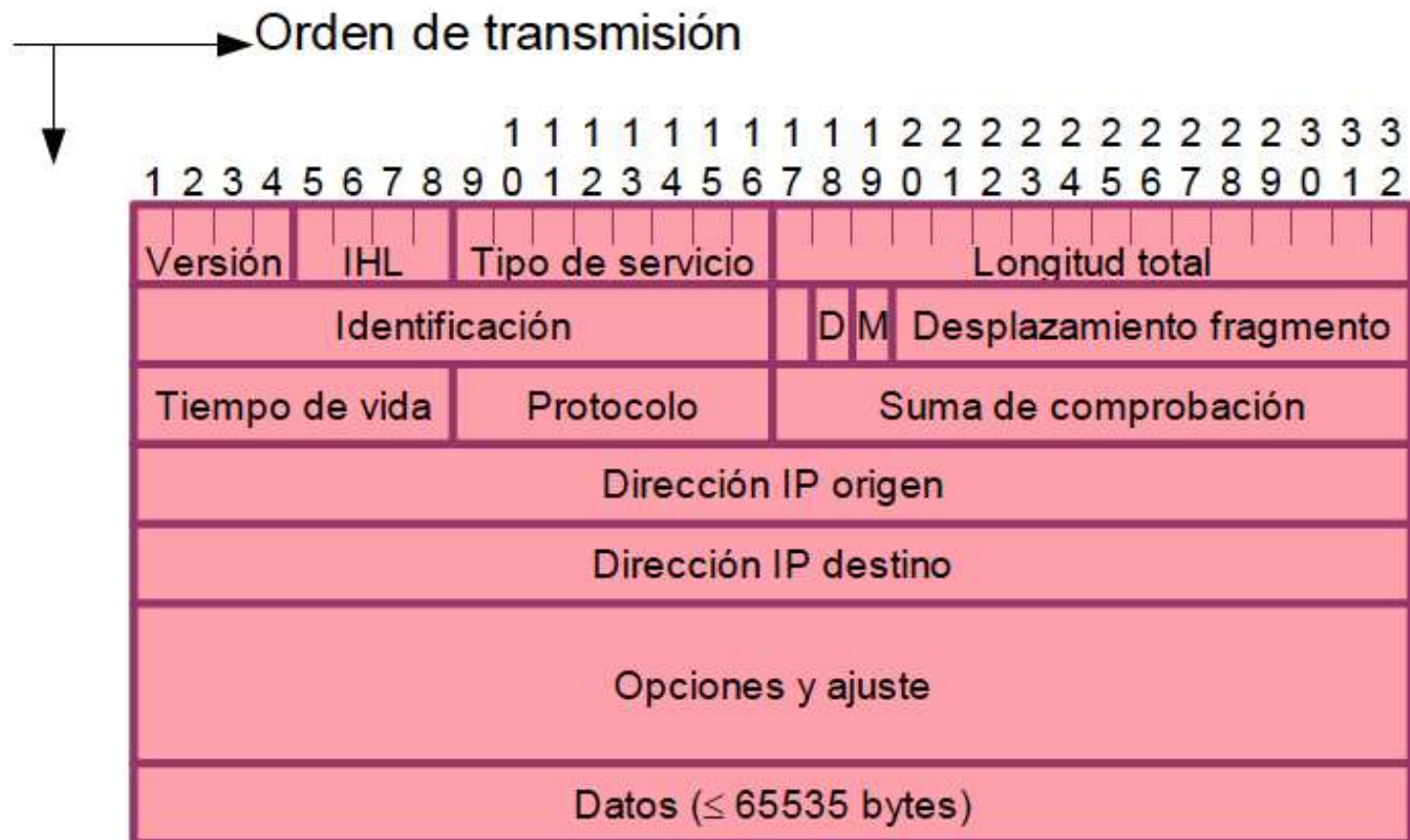
- IPv4 no garanteix que tota la informació sigui rebuda
- IPv4 no garanteix que la informació arribi en l'ordre correcte
- La fiabilitat recau sobre capes superiors (TCP)

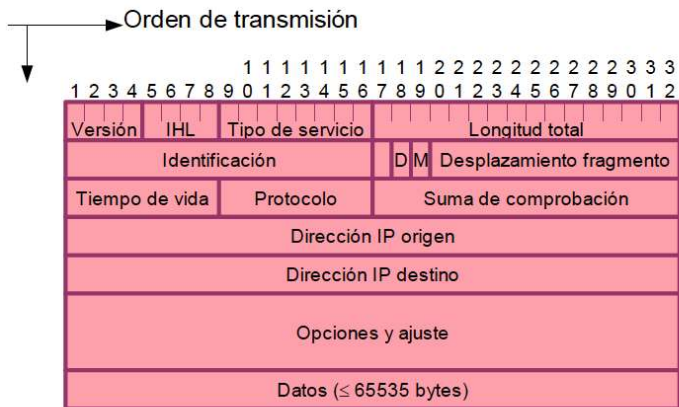
- El datagrama es divideix en dues parts
 - Capçalera: Proporciona la info necessària per el protocol IP
 - Càrrega: Porta la info associada a les capes superiors
- IPv4 és un protocol **enrutable**. Els protocols que s'encarreguen d'encaminar els datagrames IP s'anomenen protocols **de routing**

IPv4

Protocols enrutables	Protocols de routing
IP	RIP (v1 i v2)
IPX	IGRP /EIGRP
AppleTalk	OSPF, ISIS, BGP-4,...

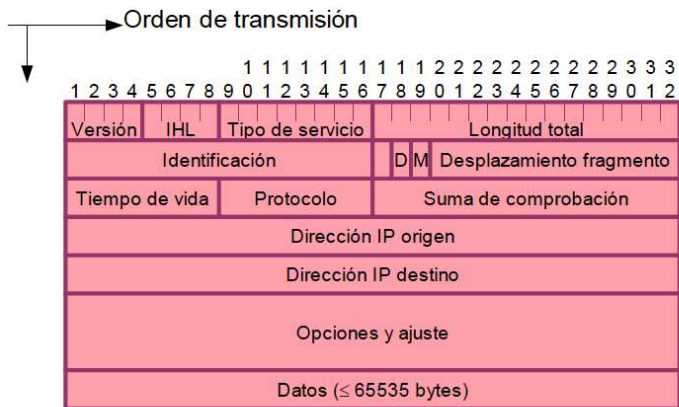
IPv4





➤ Camps de capçalera:

- Versió: indica el nombre de versió (4 bits)
- Longitud de capçalera d'Internet (en blocs de 32 bits)->(Internet Header Length) (4 bits)
- Tipus de servei: Fiabilitat, precedència, retard, velocitat (8 bits)
- Longitud total del datagrama en bytes (16 bits)
- Identificació: N^o de seqüència que juntament amb l'adreça origen i destí i el protocol de usuari identifiquen de forma unívoca el datagrama (16 bits)



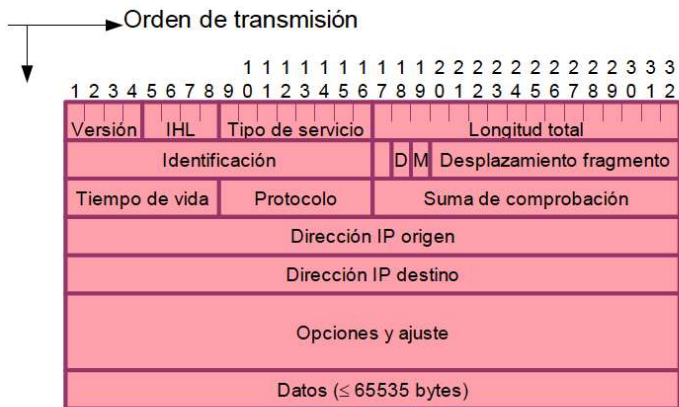
➤ Camps de capçalera (continuació):

➤ Flags: Es fan servir 2 dels 3 bits disponibles:

- **More:** indica si un datagrama prové d'una fragmentació i que no és l'últim
- **Don't fragment:** El datagrama s'ha de transmetre sencer o no es transmet

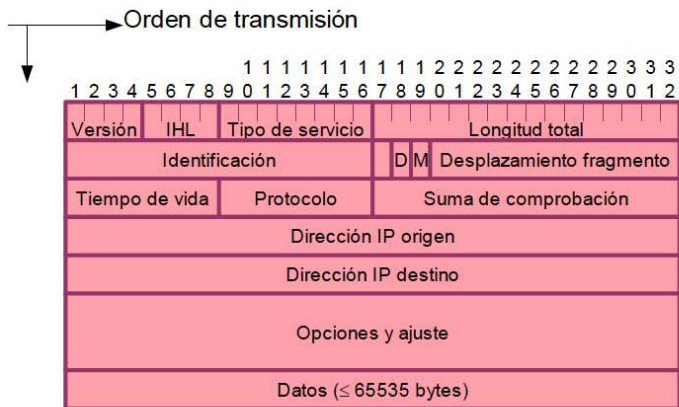
➤ Desplaçament del fragment: Indica a quina part del datagrama original pertany en unitats de 64 bits (13 bits)

➤ Temps de vida: És un comptador que indica el temps màxim que un datagrama pot estar en Internet. Cada router ha de descomptar una unitat com a mínim (8 bits)

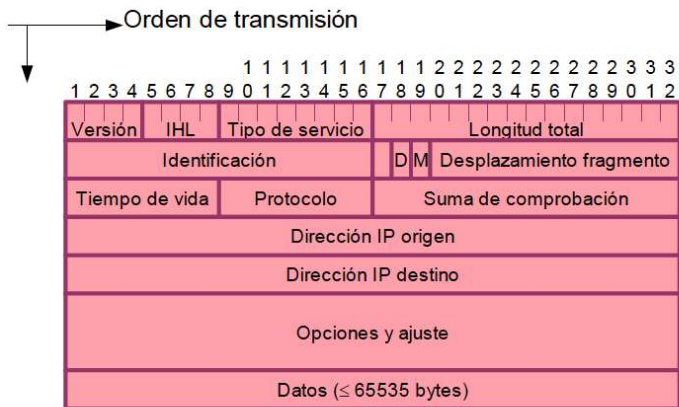


➤ Adreces IP

- 32 bits (4 bytes)
- Separació amb punts cada 8bits. Expressat en format decimal. E.g. 147.36.5.69
- NetId -> Identifica la xarxa
- HostId -> identifica l'equip connectat
- Una adreça IP identifica una interfície: Un punt d'unió a la xarxa
- Totes les adreces públiques a Internet han de ser diferents. Per tal d'aconseguir aquesta fita, la Internet Assigned Numbers Authority (IANA) assigna blocs d'adreces a registres regionals d'internet (RIR)
 - RIPE: Europa
 - ARIN: USA
 - APNIC: Asia
 - LATNIC: Latinoamerica
- RIR assigna adreces als ISP, i els ISP als seus clients.

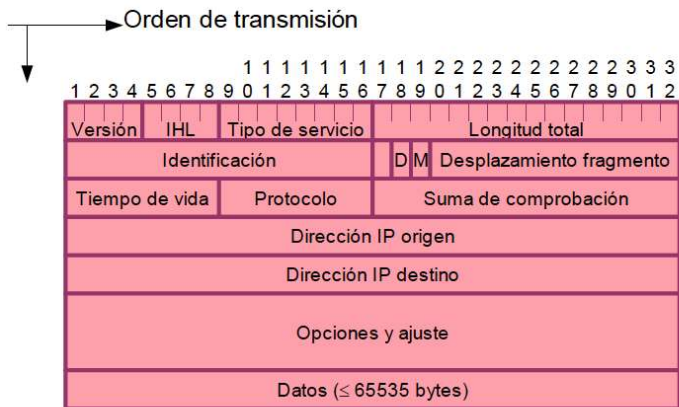


- Opcions. Paràmetres addicionals que es poden incloure:
 - Seguretat
 - Ruta a priori
 - Gravació
 - Identificació de flux
 - Temps
- Ajust: Es fa servir per assegurar que la capçalera tingui una longitud proporcional a 32 bits



➤ Fragmentació i **ensamblat**

- Diferents xarxes poden tenir diferents longituds de paquet
- Pot ser necessari dividir el paquet original en datagrames més petits
- En aquest moment apareix la pregunta de qui **ensambla** els fragments
 - L'estació destí
 - Qualsevol node
- La resposta és que l'**ensamblat** es fa al destí

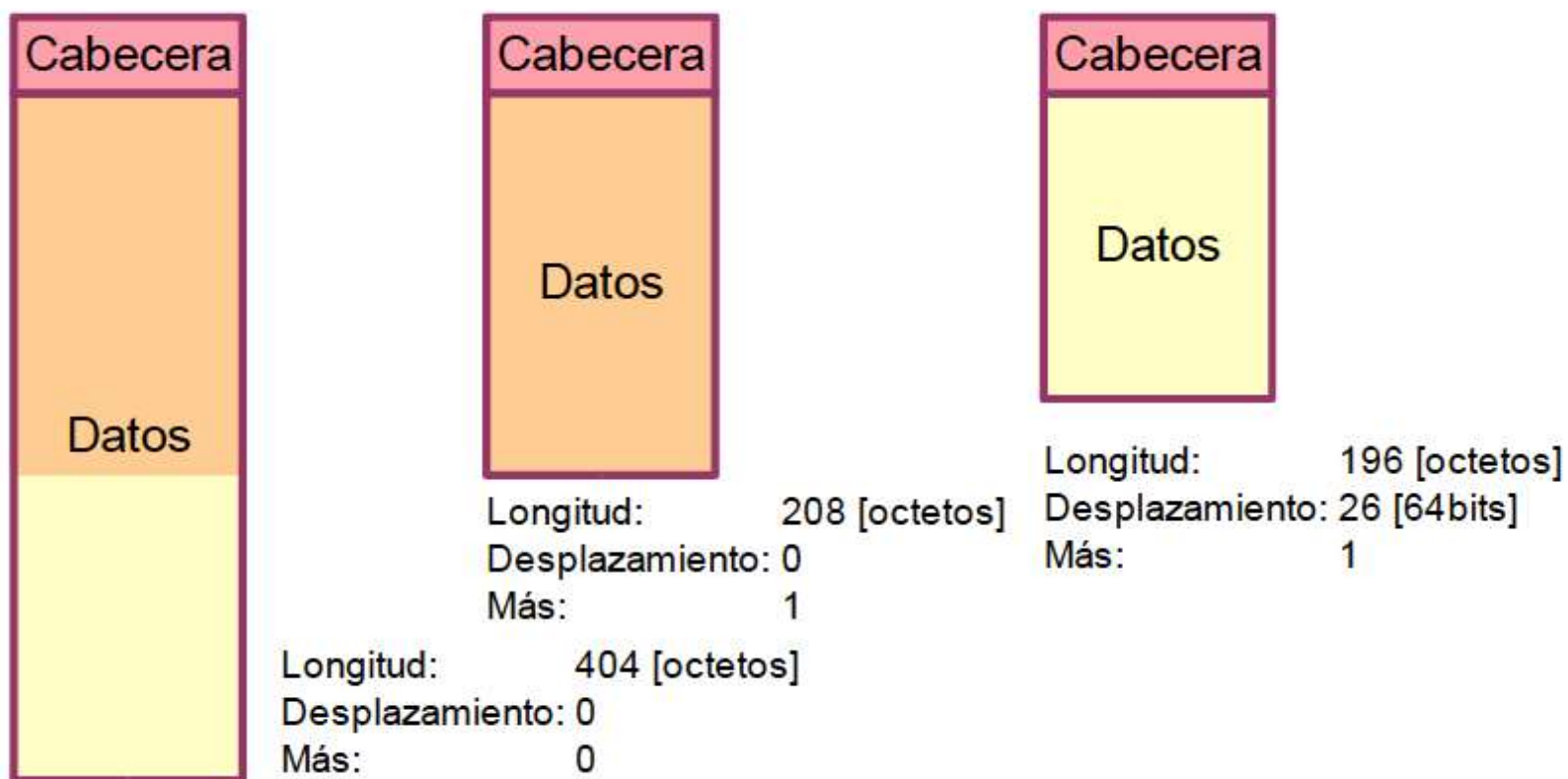


- Recordem que el procés d'**ensamblat** requereix tocar a la capçalera IP els següents camps:
 - Identificador de unitat de dades
 - Longitud de dades
 - Desplaçament
 - Bandera de Més

- L'estació origen genera un datagrama amb desplaçament i bandera Més a 0

- El router que fa la fragmentació realitza les següents tasques:
 - Crea dos datagrames amb idèntica capçalera a l'original
 - Divideix el camp de dades en dos parts approx. Iguals
 - El primer ha de ser múltiple de 64 bits
 - Canvia el camp de longitud del primer datagrama i posa la bandera de Més a 1
 - Canvia el camp de longitud del segon datagrama i el camp de desplaçament

IPv4



Format de les adreces IPv4

Les adreces IP es descomposen en:

Identificador de Xarxa (netid)

Identificador d'estació (hostid)

Les adreces s'estableixen en funció de la classe:

Les classes A, B i C indiquen adreces úniques

Les classes D són per a grups

La classe E està reservada

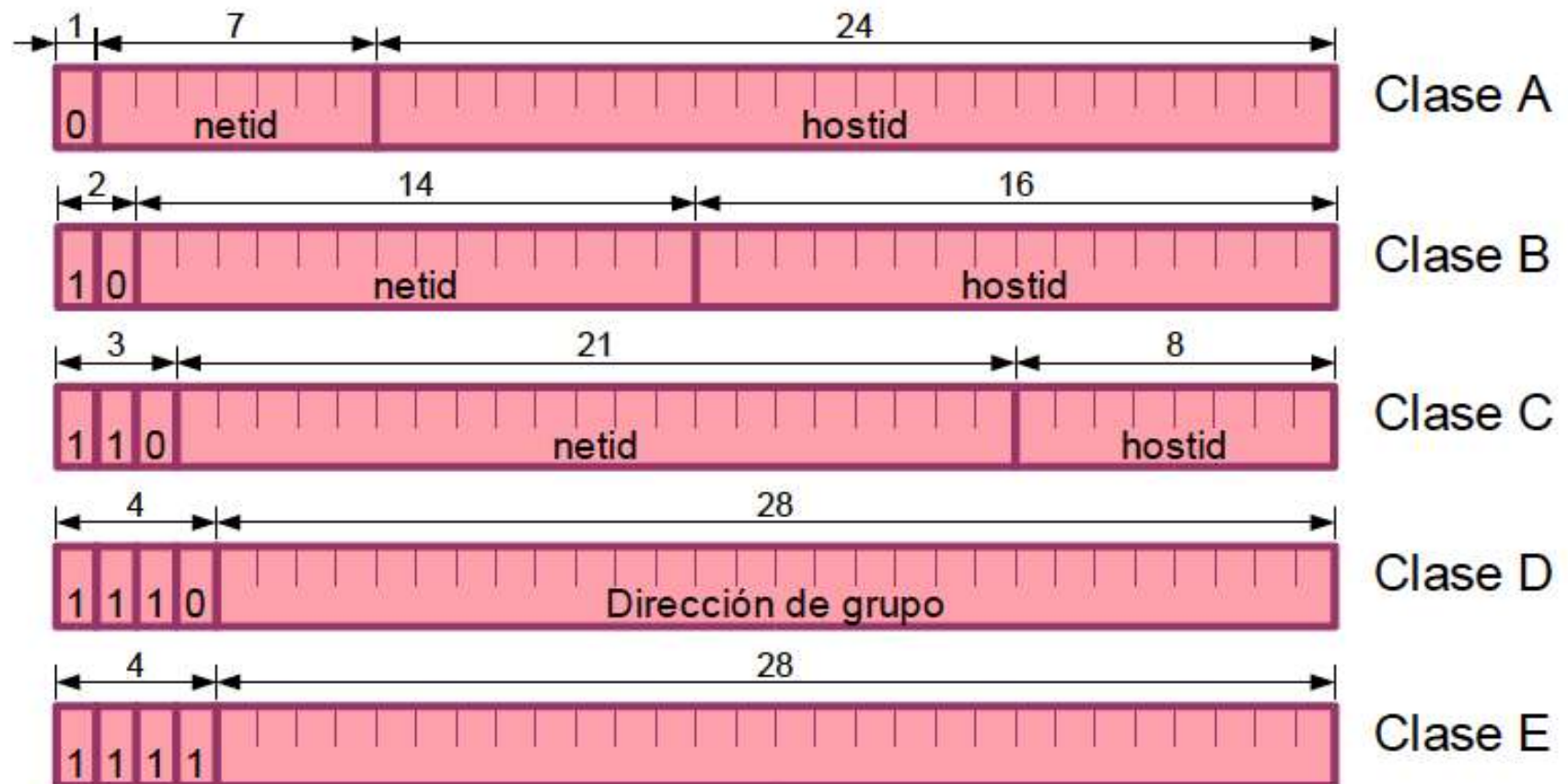
IPv4

Reserved address blocks

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 6890
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 6890
169.254.0.0/16	Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 6890
192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5737
192.88.99.0/24	IPv6 to IPv4 relay (includes 2002::/16)	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	RFC 919

Name	Address range	Number of addresses	Classful description	Largest CIDR block
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks	192.168.0.0/16

IPv4



➤ Adreces especials

- Si el hostid és 0 es refereix a l'adreça de xarxa
- Si el netid és 0 implica la xarxa origen
- Si és tot 1 significa difusió a tota la xarxa origen (broadcast)
- Si el hostid és tot 1 indica difusió en la xarxa destí
- Si és una adreça de classe A amb el netid tot a 1 indica que és una adreça de test, retorn o loopback

- Per fer més fàcil la seva lectura i escriptura, els bits s'agrupen en bytes i es representen en notació decimal separada per punts
- 00001010 00000000 00000000 00000000 = 10.0.0.0, classe A, netid 10
- 10000000 00000011 00000010 00000011 = 128.3.2.3, classe B, netid 128.3 hostid 2.3
- 11000000 00000000 00000001 11111111 = 192.0.1.255, classe C, difusió netid 192.0.1

- IP permet transmetre informació entre i a grups
- En aquest cas es fan servir les adreces de classe D
- Aquestes adreces identifiquen grups, que poden ser estables o temporals
- Els routers han de realitzar la conversió del grup específic a l'adreça de capa d'enllaç correcta

- L'estructura d'adreces IP es bona organitzativament
- Introdueix molta càrrega en els routers si es treballa amb múltiples xarxes locals
- Per simplificar l'adreçament s'estableixen subxarxes que identifiquen LANs
- En aquest cas el hostid és dividit en un subhostid i una subnetid
- Això permet independitzar els routers

IPv4

➤ Adreces especiales (ZOOM):

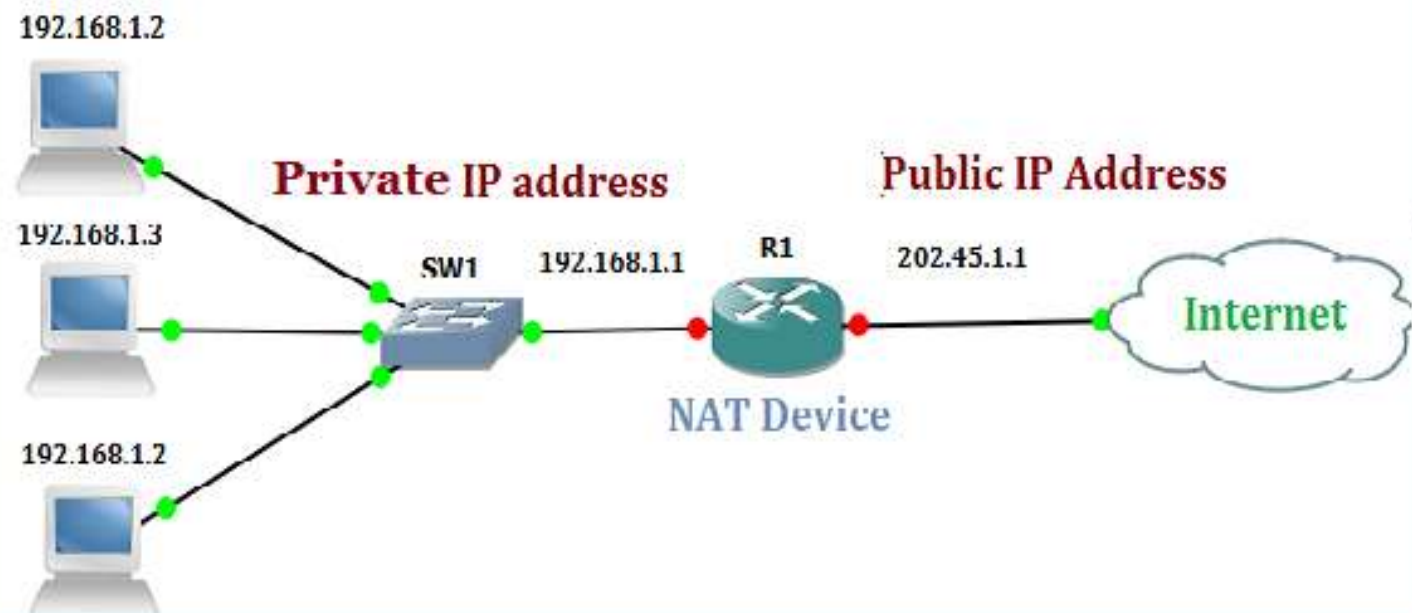
NetId	HostId	Meaning
xxx	All '0'	Identifies a network. It is used in routing tables
xxx	All '1'	Broadcast in the net xxx
All '0'	All '0'	Identifies "this host" in "this net". Used as source address in configuration protocols, e.g. DHCP
All '1'	All '1'	Broadcast in "this net". Used as destination address in configuration protocols, e.g. DHCP
127	xxx	Host loopback: Interprocess communication with TCP/IP

- Adreces privades (RFC 1918)
 - Cada cop més dispositius comercials inclouen la pila TCP/IP
 - Això permet interconnectar gran quantitat de dispositius electrònics
 - Les adreces assignades per IANA als RIRs s'anomenen públiques, globals o registrades
 - Que passa si assignem arbitràriament una IP a un dispositiu? Aquesta pot ser filtrada pel nostre ISP o pot causar problemes a l'usuari propietari d'aquesta IP
 - Adreces Privades: Són adreces reservades per dispositius que no requereixen una connexió a la xarxa pública. Aquestes adreces no són assignades per cap RIR. Tenim adreces privades per a cada classe:
 - 1 Classe A. Xarxa 10.0.0.0
 - 16 Classe B. Xarxes 172.16.0.0 – 172.31.0.0
 - 256 classe C. Xarxes 192.168.0.0 – 192.168.255.0

- El procés de canvi de IP privada a IP pública es realitza mitjançant un protocol anomenat NAT
- NAT ➔ Network Address Translation
- Hi ha diverses formes de fer NAT (practiques)
 - Canvi una a una
 - Canvi dinàmic...

IPv4

Network Address Translation - NAT



➤ Les Màscares

➤ Una màscara és una successió de 1's i 0's que permet identificar la netid i el hostid.

Classe	Rang IP	Màscara
A	1.0.0.0 – 126.0.0.0	255.0.0.0
B	128.0.0.0 – 191.255.0.0	255.255.0.0
C	192.0.0.0 – 223.255.255.0	255.255.255.0

➤ ADREÇA XARXA = ADREÇA IP & MÀSCARA

- Estructura jeràrquica de la xarxa. Subnetting (RFC 950)
 - En funció del nombre de IP's assignades, podem generar més o menys subxarxes que faciliten l'encaminament de la nostra xarxa
 - Donada una IP qualsevol, si fem:
$$\text{IP} \& \text{Màscara} = \text{IP xarxa}$$
 - Coneguts els bits de xarxa, veiem que ens queden "n bits" restants per la identificació dels nodes
 - **Subnetting** consisteix en assignar m bits per crear subxarxes i m-n per nodes

➤ Problema exemple. Partim de l'adreça IP:

130.206.0.0/16 (això s'explica a classe)

➤ El pretenen crear 200 subxarxes. Identificar quina serà la nova màscara i com seran les adreces de les subxarxes i les IP's dels nodes associats

➤ Si volem crear 200 subxarxes s'ha de complir que:

$$2^n \geq 200$$

Per $n = 8$ tindrem 256

➤ La nova màscara serà:

130.206.0.0/24 ó 130.206.0.0 255.255.255.0

IPv4

➤ Quines són les adreces de les subxarxes?

10000010.11001110.00000001.00000000 130.206.1.0

10000010.11001110.00000010.00000000 130.206.2.0

10000010.11001110.11111110.00000000 130.206.254.0

➤ Per veure les adreces dels host, escollim per exemple la tercera xarxa:

➤ 130.206.3.0/24

Nombre de hosts: $2^8 - 2 = 254$

130.206.3.1 primer host

130.206.3.2 segon host ...

130.206.3.254 darrer host

- Subnetting variable: Variable Length Subnet Mask (VLSM)
- ☐ Les subxarxes creades no tenen perquè tenir la mateixa mida. Es poden crear subxarxes de diferents mides. Exemple:
 - Tenim una adreça IP de classe C => Tenim 1 byte per fer subnetId + hostId
 - Agafem el bit més significatiu per començar a fer subnetting.
 - Tindrem 0000
 - 1000 => Fem subnetting d'aquesta subxarxa
 - 1000
 - 1100 => Fem subnetting d'aquesta subxarxa
 - 1100
 - 1101
 - 1110
 - 1111

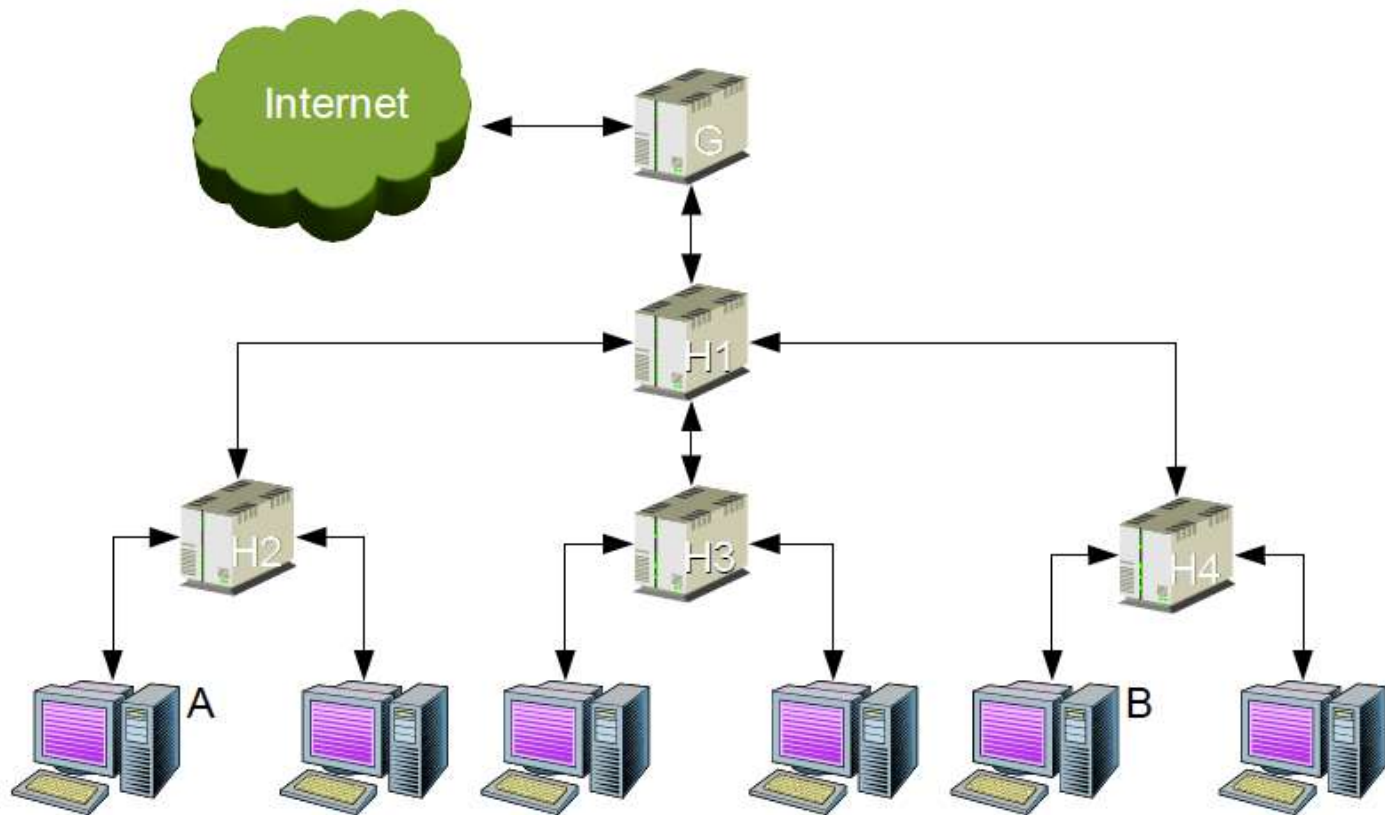
IPv4

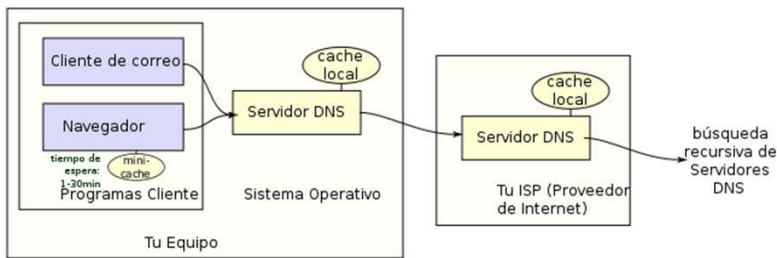
➤ Obtenim la següent taula:

subnet	subnetid	IP net. addr	range	broadcast	available
S1	0	B.0/25	B.0 – B.127	B.127	126
S2	10	B.128/26	B.128 – B.191	B.191	62
S3	1100	B.192/28	B.192 – B.207	B.207	14
S4	1101	B.208/28	B.208 – B.223	B.223	14
S5	1110	B.224/28	B.224 – B.239	B.239	14
S6	1111	B.240/28	B.240 – B.255	B.255	14

- Cada estació té per tant dos adreces:
 - Adreça Física 48 bits associada a la MAC
 - Adreça IP
- Quan arriba un datagrama des d'internet, només inclou la IP
- És necessari establir un protocol per obtenir l'adreça física a partir de la IP
- Aquest protocol és el de resolució d'adreça o ARP

IPv4





Descubrimient de IPs

- Memoritzar la IP de un determinat servidor no és una tasca senzilla
- Ens recordem més fàcilment del nom de la companyia a la que volem contactar que la seva adreça IP associada.
- En aquest sentit, el DNS (Domain Name System) és un procotol de APLICACIÓ encarregat de traduir les adreces IP a noms de domini.
- DNS funciona amb una estructura client – servidor.
 - Un programa client DNS s'executa en la computadora de l'usuari, generant peticions DNS de resolucions de noms al servidor DNS
 - Servidors DNS. Contesten al client proporcionant la IP associada al nom del domini sol·licitat. Si no la coneixen, reenvien la petició a un servidor de superior nivell

- I un cop tenim la IP? ➔ Protocols de Routing
 - Els routers són els responsables de rebre i reenviar els paquets a través d'un conjunt de xarxes interconnectades
 - Cada enrutador pren decisions referents al camí que han de seguir els paquets en funció de:
 - La topologia
 - Estat d'Internet

➤ Protocols de routing

- Un router és un dispositiu que treballa sobre unes taules d'adreçament.
- Aquestes taules poden ser:
 - Fixes: Amb camins predefinitos
 - Dinàmiques: Els camins s'estableixen en temps real en base a la informació disponible a la xarxa
- Això permet una certa cooperació entre dispositius per evitar errors en la xarxa (caiguda de nodes)

- Les taules de routing també poden proporcionar un cert control sobre seguretat
- Un segment de la xarxa pot estar autoritzat per rebre informació d'un determinat nivell de seguretat
- Un router és l'encarregat d'evitar que un paquet que tingui un nivell no permès en el segment passi per ell
- També es possible el routing a priori, on l'estació origen estableix el camí

- Existeix un servei que permet guardar en el datagrama informació dels routers per on va passant.
- És útil per veure el correcte funcionament de la xarxa i dels routers

➤ Control de flux

- El control de flux en Internet es porta mitjançant el protocol de missatges de control de Internet (ICMP)
- Aquest protocol estableix una sèrie de missatges que permeten l'intercanvi d'informació entre els diferents routers i estacions
- ICMP fa servir datagrames IP per transmetre la seva informació

https://es.wikipedia.org/wiki/Internet_Control_Message_Protocol

➤ Control de Flux:

➤ Els missatges més utilitzats són:

➤ Destí no accessible

- El router no sap com fer arribar el datagrama
- L'estació receptora pot enviar-lo si el protocol o servei del datagrama no està disponible
- Si el datagrama indica una ruta a priori que es pot seguir
- Si el router necessita fragmentar un datagrama que no és fragmentable

➤ Temps exhaurit

- Si el comptador arriba a 0
- Si l'estació destí no pot reensamblar un datagrama en un temps determinat

➤ Control de Flux:

➤ Problema de paràmetre:

- Si apareix un error sintàctic o semàntic en una capçalera IP
- En el missatge s'inclou informació de l'octet on s'ha trobat l'error

➤ Extinció d'origen

- Quan un node no pot rebre més datagrames per que deixin d'enviar-li paquets temporalment

➤ Control de Flux:

➤ Redirigir

- Si un servidor està connectat a vàries passarel·les i envia un paquet a una que no és òptima, aquesta pot indicar-li el camí adequat

➤ Echo

- Permet comprovar l'accés a un servidor

➤ Marca de temps:

- Permet sol·licitar i rebre una marca de temps per veure els retards entre dos nodes



IPv4

- Control de Flux:

- Màscara d'adreça

- Permet sol·licitar al router local la màscara d'una estació

➤ Qualitat de servei

- Una xarxa es congestiona quan la demanda de recursos supera un determinat punt
- Si s'envia una ràfega de paquets a un router per diferents línies d'entrada i tots han de sortir per la mateixa sortida, aquesta es col·lapsarà
- Per gestionar aquesta situació, cada sortida té associada una cola FIFO que permet mantenir un determinat nombre de datagrames

IPv6. Motivació

- El 3 de febrer de 2011 es van terminar les adreces IPv4 en el registre de la IANA (Autoritat d'Assignació de números en Internet).
- Els proveïdors de serveis d'Internet acceleren per tant el desplegament de IPv6 a les seves xarxes
- La transició és transparent per els usuaris SOHO, ja que l'adreça proporcionada pel proveïdor sol ser una IP privada, sent responsabilitat d'aquest el fer NAT i passar a una IP pública

IPv6. La Transició

- El protocol predominant avui dia és IPv4 i, donada les característiques de Internet, no és possible la substitució directa, i.e. No es possible apagar la xarxa i canviar a IPv6.
- Perquè??
 1. L'elevat cost que suposaria aquest canvi. Les companyies volen amortitzar els routers i switches actuals. Volen per tant un canvi gradual
 2. La pèrdua de dades i el cost econòmic seria enorme

IPv6. La Transició

- La IETF (Internet Engineering Task Force) va dissenyar amb IPv6, els mecanismes de transició i coexistència.
- Els dos protocols coexistiran durant un cert temps: coexistència
- És com una balança. Avui dia amb un major pes representat per transit IPv4. Poc a poc, gràcies a la coexistència, quant majors siguin els continguts i serveis disponibles amb IPv6 el pes de la balança s'anirà desplaçant cap a IPv6 fins que aquest sigui predominant: Transició

IPv6 – IPv4. Transició

- El grup de treball NGTrans ha definit tres principals tècniques de transició:
- 1. Doble pila de protocols. Format senzill d'implementació. Requereix que els hosts i els routers suportin les dues versions de IP -> Serveis i aplicacions per v4 i v6. Aquesta tècnica és fonamental per introduir IPv6 a les actuals architectures IPv4. L'inconvenient que presenta és que obliga a que cada màquina mantingui una adreça IPv4. Aquesta tècnica, a mesura que v6 es difon, s'aplicarà on específicament ajudi al procés de transició (routers i servers). Per aquells casos on el nombre de IPv4 siguin insuficients es defineix una combinació del model de conversió i de doble pila de protocols conegut com DSTM (Dual Stack Transition Mechanism)

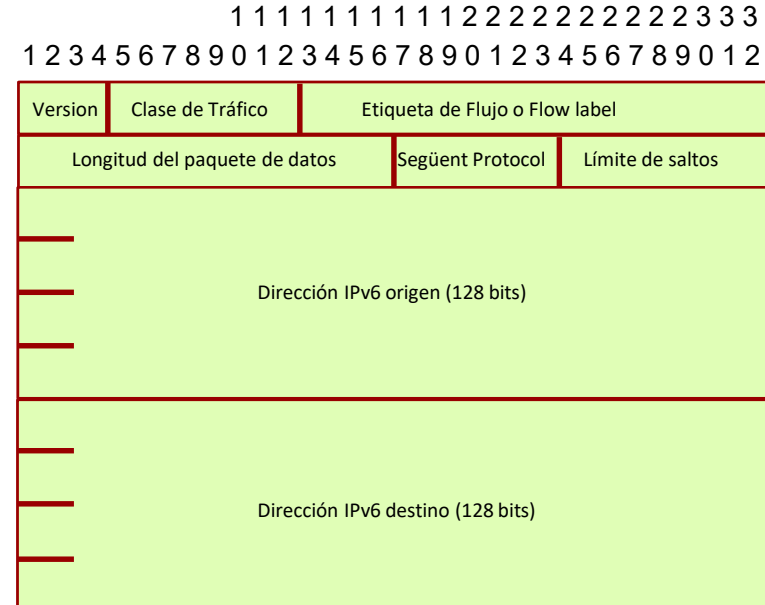
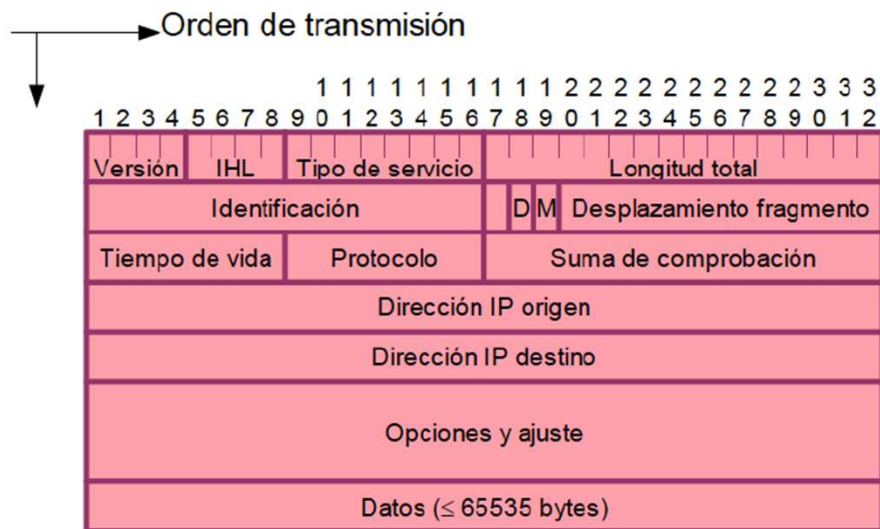
IPv6 – IPv4. Transició

2. Tunneling. Permet interconnectar núvols IPv6 a través d'un servei IPv4 natiu implementant un túnel. Els paquets IPv6 són encapsulats per un router d'extrem abans de ser transportat a través de la xarxa IPv4, sent des-encapsulat a l'altre extrem, a l'entrada del núvol IPv6 receptor. Els túnels es poden configurar estàticament o dinàmicament. S'estan proposant tècniques per gestionar automàticament els túnels i evitar la configuració manual dels túnels: TB (Tunnel Broker) o ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Als estadis finals de la transició també es faran servir els túnels per interconnectar els núvols IPv4 residuals a través de la infraestructura IPv6

IPv6 – IPv4. Transició

3. Mecanisme de traducció o conversió de protocols. Necessari quan un host IPv6 s'ha de comunicar amb un host IPv4. Mecanisme complex ja que no basta amb canviar les adreces, implica canviar la capçalera IP
- ✓ La transició NO SEMPRE és la solució. És important tenir present que algunes aplicacions innovadores necessiten de IPv6 per al seu desplegament massiu. Desplegar mecanismes de transició a gran escala pot implicar problemes d'escalabilitat i limitar enormement el rendiment de IPv6
- ✓ Coexistència. Allà on els dos protocols han de coexistir, s'ha de mantenir sota control la transició per evitar el desplegament de dos infraestructures internet paral·leles.
- ✓ La transició no només afecta a IPv6. IP NO ÉS una tecnologia aïllada. Implica interaccions amb tecnologies actuals i emergents. Per exemple és fonamental definir com transportar transit IPv6 sobre una arquitectura MPLS a mesura que el nou IP aconsegueixi beneficis directes de les millores introduïdes en aquest estàndard

Format Overhead IPv6



Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to Service Field in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded

Flow Label/QoS management (20 bits) The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a **non-zero** Flow label.

Segmentació IPv6

- La segmentació consisteix en crear nivells de jerarquia en adreces IP.
- Tres nivells: Xarxa, Subxarxa i num. Estació (Subnetting)

PEL QUE FA A LA FRAGMENTACIÓ DEL DATAGRAMA

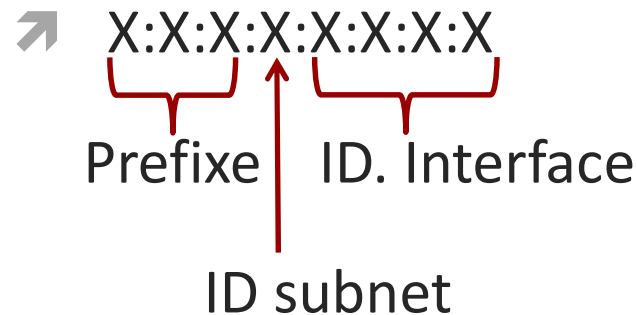
- Els paquets no es poden fragmentar un cop surten de la IP origen

SOBRE LA IMPLEMENTACIÓ D'ALGUN TIPUS DE CRC EN IPv6

- No s'aplica cap suma de CRC d'errors a diferència de IPv4

Segmentació i estructura de l'adreça

- 128 bits dividits en 8 camps de 16 bits. Cada camp s'uneix per dos punts. Els valors s'expressen en format hexadecimal





➤ Exemple:

2001:3C4D:0DB8:0015:0000:0000:1A2F:1A2B

The address is shown with red brackets underneath. The first three segments (2001:3C4D:0DB8) are bracketed together. The fourth segment (0015) is bracketed separately. The last four segments (0000:0000:1A2F:1A2B) are bracketed together.

Prefixe de lloc: (48 bits). Topologia pública que el ISP proporciona al lloc

ID de subxarxa: (16 bits). Descriu la topologia privada del lloc.

ID de la interface/usuari: (48 bits). Es configura automàticament des de l'adreça MAC

Aquesta adreça es pot abreviar de la següent forma:

2001:3C4D:0DB8:0015::1A2F:1A2B

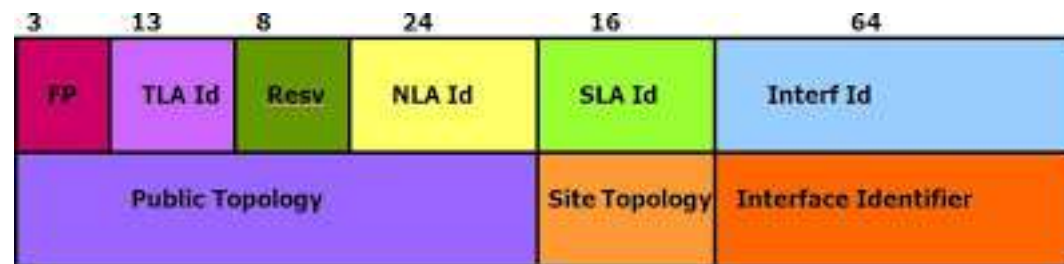
Format de l'adreça IPv6

- Una adreça IPv6 té 3 nivells jeràrquics
 - Topologia pública (48 bits). Identifica als proveïdors de la connexió a Internet
 - FP (Formal Prefix): Identifica unicast, multicast, anycast
 - TLA ID (Top Level Agregation) Identifica l'autoritat de major nivell dins de la jerarquia d'encaminament
 - Resv: Reservat
 - NLA ID (Next-Level Aggregation): Identifica l'ISP



➤ Nivells jeràrquics (cont)

- Topologia de la organització (16 bits) Identifica a la organització a la que pertany el node IP
 - SLA ID (Site Level Aggregation). Permet a una organització crear la seva pròpia jerarquia d'adreces
- Identificador de la Interfície (64 bits): Identifica Unívocament el node. Coincideix amb els bits d'una adreça MAC . Es fa servir per autoconfiguració



Tipus d'adreces IPv6

- Les adreces són identificadors de 128 bits. Les adreces es classifiquen en tres tipus:
 - Unicast. Identificador per a una sola interfície. Un paquet enviat a una adreça unicast s'entrega a una interfície identificada amb aquesta adreça. Equivalent a les adreces IPv4 actuals
 - Subnetting aplicable també aquí!!
 - Anycast. Adreça assignada més de una interfície. Un paquet enviat a una adreça anycast s'encamina a la interfície més propera que tingui aquesta adreça d'acord amb les mètriques dels protocols d'encaminament.
 - No hi ha cap distinció amb les adreces Unicast
 - Una adreça anycast no pot ser utilitzada com a direcció origen de un paquet IPv6
 - Una adreça anycast no pot ser assignada des de un host IPv6. Només pot ser assignada a un router IPv6

Adreça anycast del router de la subxarxa

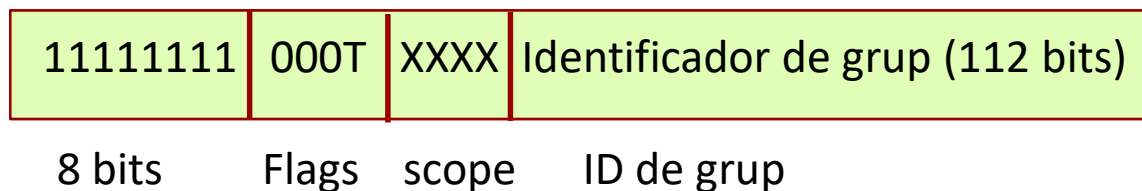
Prefix de subxarxa (n bits)

128 – n bits

- Els paquets enviats a l'adreça anycast Subnet – Router s'entreguen a un router de la subxarxa
- L'adreça anycast subnet-router està dissenyada per ser utilitzada en aplicacions on un node necessita comunicar-se amb algun del conjunt de routers
- El prefix de subxarxa en una adreça Anycast és el prefix que identifica un enllaç específic. Aquesta adreça Anycast és sintàcticament igual a una adreça unicast per a una interfície en l'enllaç amb la ID de interfície posat a 0

➤ Adreces Multicast IPv6

- És un identificador per a un grup de interfícies (Normalment en diferents nodes). Una interfície pot ser comú a qualsevol nombre de grups multicast.



8 bits a 1 identifica el paquet com Multicast

T = 0 adreça multicast permanent. T = 1 indica adreça multicast temporal

IPv6

Scope:

0	Reservat	9	No assignat
1	Àmbit local del node	A	No assignat
2	Àmbit local de l'Enllaç	B	No assignat
3	No assignat	C	No assignat
4	No assignat	D	No assignat
5	Àmbit local de lloc	E	Àmbit global
6	No assignat	F	Reservat
7	No assignat		
8	Àmbit local de organització		



➤ Quantes adreces em permet assignar IPv4?

IPv4 implica adreces de 32 bits

El nombre màxim d'adreces* serà $2^{32} =$

4.294.967.296 adreces

➤ Quantes adreces em permet assignar IPv6?

IPv6 implica adreces de 128 bits

El nombre màxim d'adreces serà $2^{128} =$

$3,4028236692093846346337460743177 \cdot 10^{38}$

➤ I això pot esgotar-se?

IPv6 pot proporcionar uns 670 mil bilions d'adreces per cada milímetre quadrat de la superfície de la Terra



- Podem assignar IP a qualsevol objecte que volem!!
- Qualsevol dispositiu pot connectar-se a Internet fent servir IPv6
- Implica una connectivitat total!!!





- Internet ens proporciona connectivitat:
 - Usuari – Usuari
 - Usuari – Màquina
 - Màquina – Màquina

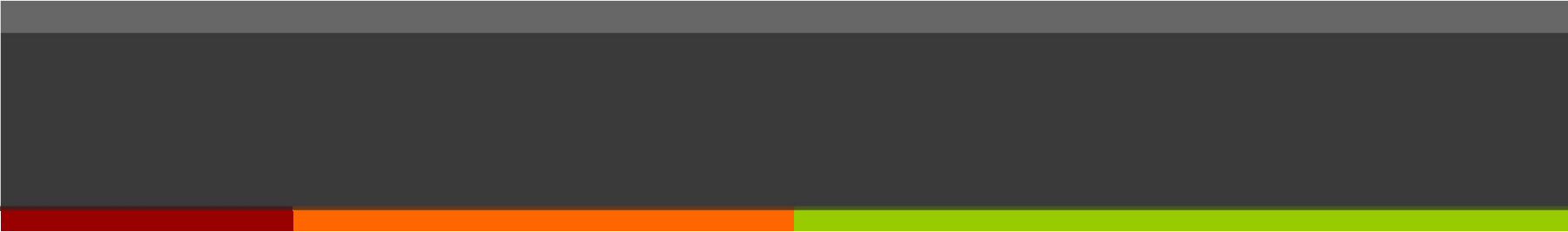
- La interconnexió total, l'intercanvi d'informació ens porta a la nova versió d'internet => La Internet de les coses.

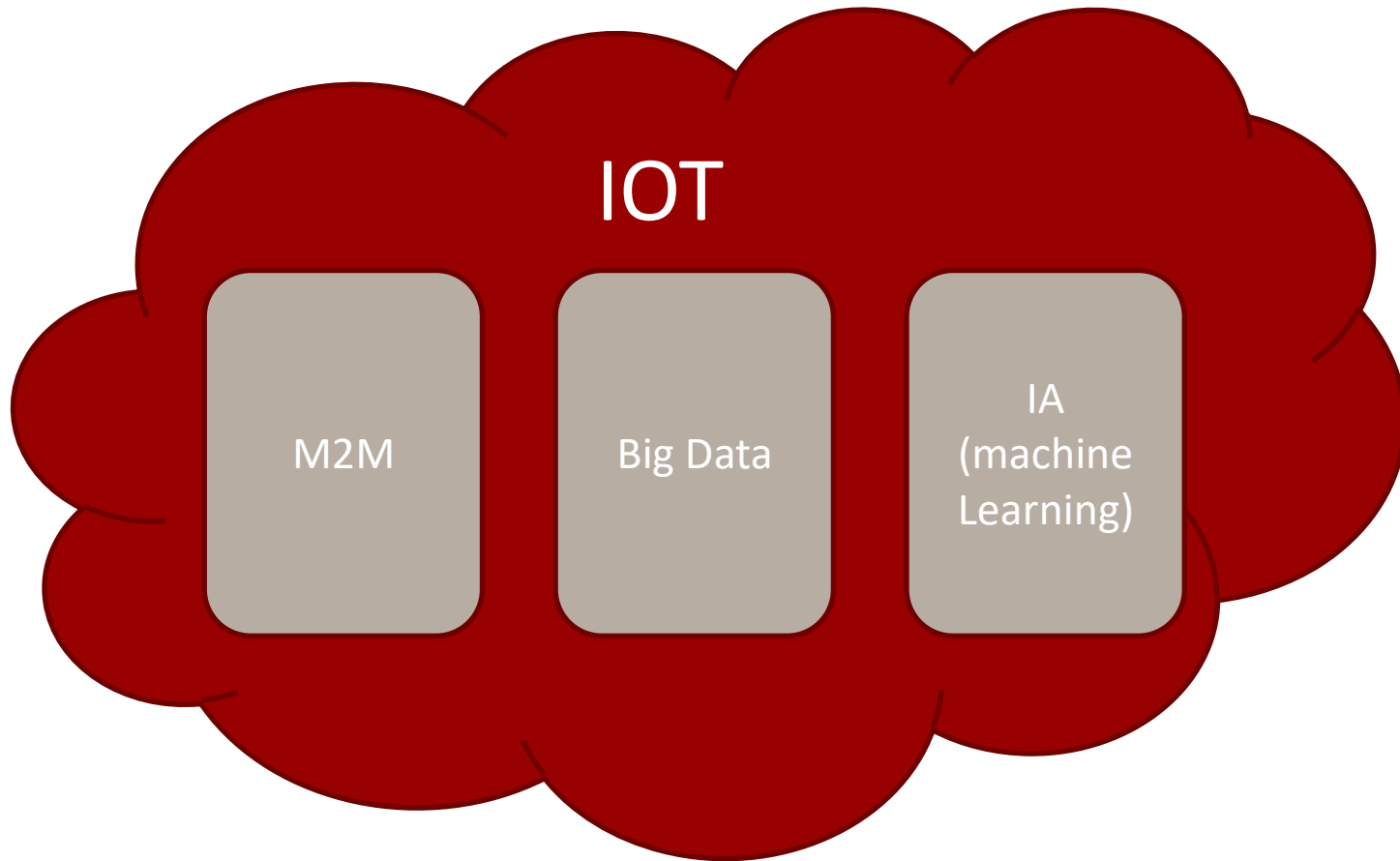
Frequency	Percentage
Never	1%
Sometimes	19%
Often	80%

➤ Què és IoT?

➤ Què és IoT?



- 
- La primera vegada que apareix el terme IoT és al 2009
 - El terme va ser dit públicament per primera vegada per Kevin Ashton, professor del MIT en el RFID Journal.
 - Ell mateix ha comentat que era un terme d'ús freqüent en cercles d'investigació des del 1999





➤ Apliquem IoT a:

➤ “Consumer Applications” => Home:

- Monitorització de casa nostra (calefacció, sistema de reg...)
- Vigilància
- Monitorització de nen@s petits
- Monitorització de l'estat de la nevera

➤ Health care:

- Persones amb discapacitats
- Portem l'atenció hospitalària a casa
- Dispositius integrats en el pacient

➤ Apliquem IoT a:

➤ Feina =>

- Detecció de presència
- Accés a zones restrictives
- Transmissió de dades de forma automàtica...

➤ Jocs i activitats lúdiques

➤ Smart Cities



Aplicació
FTP, SMTP, HTTP, telnet...

TCP - UDP

IP

MAC



Aplicació
FTP, SMTP, HTTP, telnet...

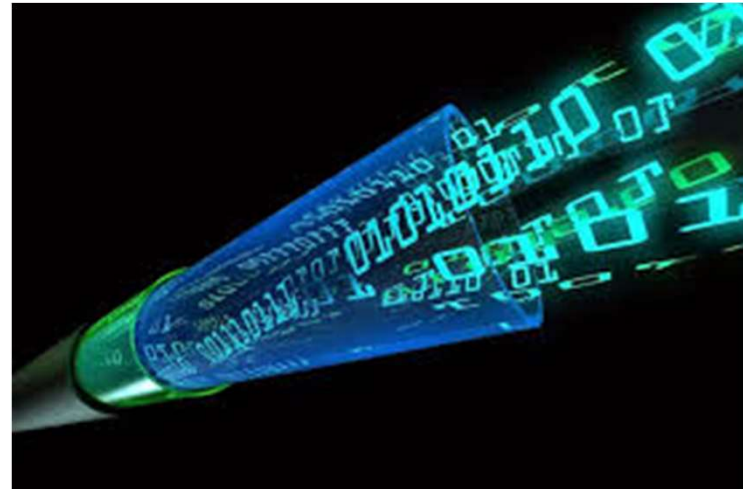
TCP - UDP

IP

MAC



- Quin ample de banda necessitem??
- De quin ample de banda estem parlant
 - Coordenades
 - Geolocalització
 - T, P, H...
 - Alarmes, ofertes
 - Anuncis, audio, video



➤ Com és un dispositiu IOT?

➤ Hardware

➤ Software (aplicació)

