4. Lliurament

Col·laboradors:
Sr. Lluís Casals Ibáñez
Dr. David Rincón Rivera
Sra. Immaculada Ruiz Vela
Dr. Rafael Vidal Ferré

Dr. Daniel Guasch Murillo

Gener 2022

Departament d'Enginyeria Telemàtica
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

4. Lliurament

4.1. Protocol d'internet

4.1. Característiques bàsiques d'IP

Filosofia de treball del protocol IP

- Protocol de nivell de xarxa
- S'ha de poder utilitzar en qualsevol host, router, xarxa
- Cal que permeti créixer la xarxa sense interrompre el servei
- Cal que admeti sessions de nivell superior y serveis orientats a missatges

4.1. Característiques bàsiques d'IP

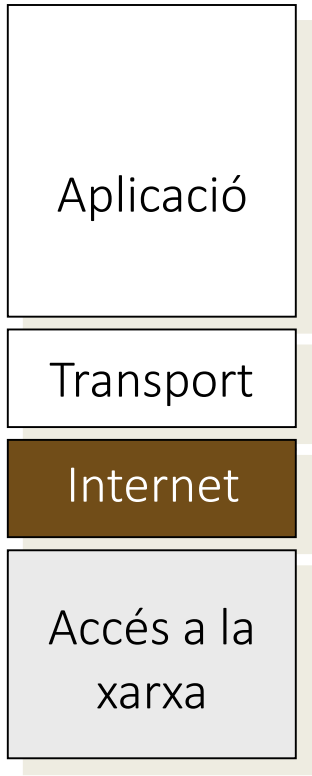
IP (Internet Protocol), RFC791

És la base per als protocols de la família TCP/IP

IP ofereix:

- Enllaç entre xarxes.
- Encaminament (Routing) i lliurement d'informació entre màquines de xarxes diferents.

Servei d'enviament de paquets sense connexió →



Datagrama

- Unitat mínima de transferència (PDU)

4.1. Característiques bàsiques d'IP

Característiques del servei

No orientat a connexió

- Cada datagrama es transmet de forma independent.

Servei sense fiabilitat

- No es garanteix que els paquets arribin correctament
- Es poden produir:
  - Pèrdues, duplicats, desordre, ...

Servei *Best effort* (es farà el millor que es pugui).

La fiabilitat la proporcionen els nivells superiors.

Proporciona algunes funcions de control:

- Mitjançant ICMP (Internet Control Message Protocol)

4.1. Característiques bàsiques d'IP

Datagrama IP

El datagrama està format per una capçalera i un camp de dades:

- La capçalera conté :
  - Les adreces IP de l'origen i del destí.
  - I altra informació de control.
- El camp de dades conté la informació del protocol superior

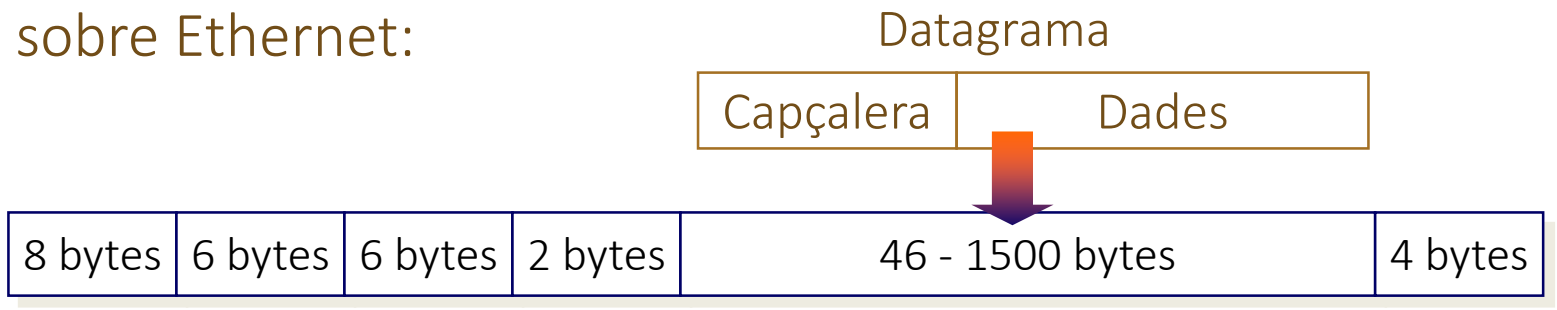
Datagrama IP

4.1. Característiques bàsiques d'IP

Encapsulament IP

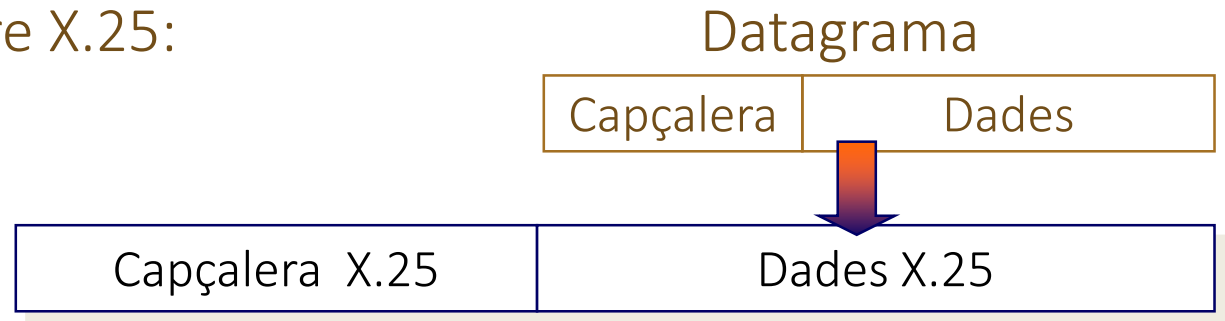
Els paquets IP es transmeten dins del camp de dades d'una trama de nivell d'enllaç:

IP sobre Ethernet:



Hi ha casos especials en que es transportar paquets IP en altres nivells:

IP sobre X.25:



4.1. Característiques bàsiques d'IP

Fragmentació de datagrames IP

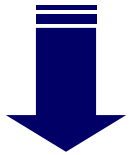
La longitud del datagrama pot ser que sigui superior a la capacitat del camp de dades de la trama física:

Cal fragmentar el datagrama IP

4.2. Funció d'encaminament IP

Característiques del servei

La funció principal de l'IP és acceptar dades de TCP o UDP, crear els datagrames necessaris, encamina'ls per la xarxa i lliurar-los a la destinació correcte



Utilitza dues eines

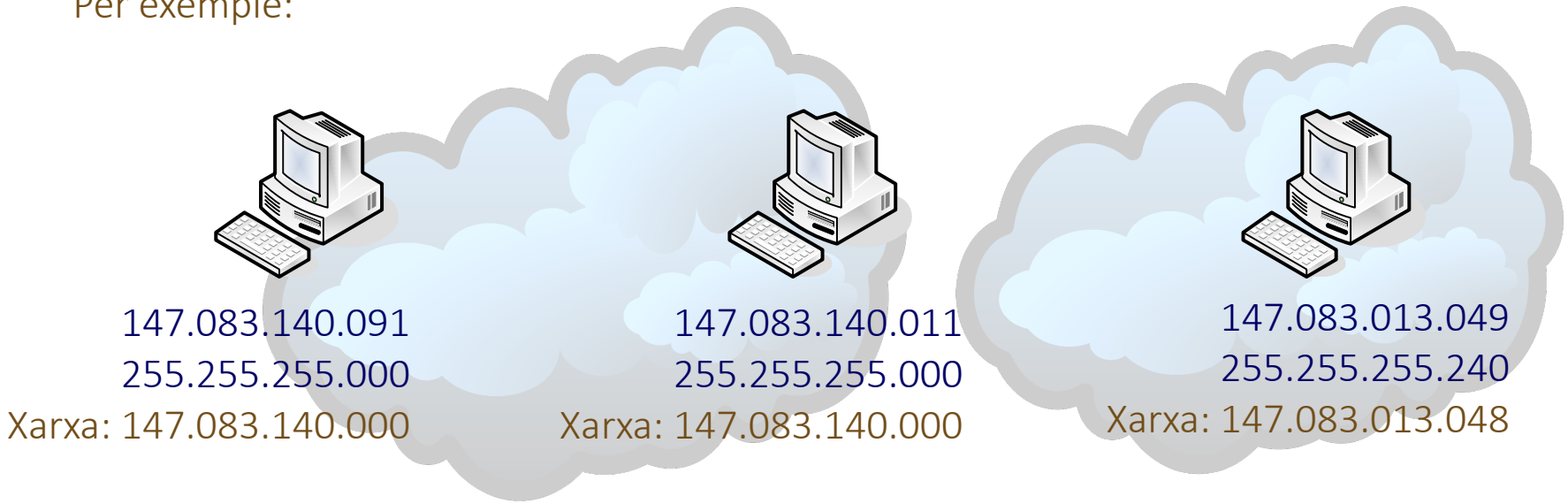
- Màscara de subxarxa
- Taules d'encaminament IP

4.2. Funció d'encaminament IP

Màscara de subxarxa

Mitjançant la màscara de subxarxa, IP analitza si l'adreça destí pertany a la mateixa xarxa que l'adreça origen

Per exemple:



4.2. Funció d'encaminament IP

Taula d'encaminament

Indica a IP com dirigir els datagrames cap a sistemes que no es troben a la seva xarxa

Concepte

- No descriuen el camí complert fins al destí.
- A IP només li cal conèixer l'adreça del proper salt i enviar-hi el datagrama.
- IP només defineix l'estructura de la taula, no la seva gestió.
- La gestió de les taules d'encaminament és responsabilitat dels protocols d'encaminament.

4.2. Funció d'encaminament IP

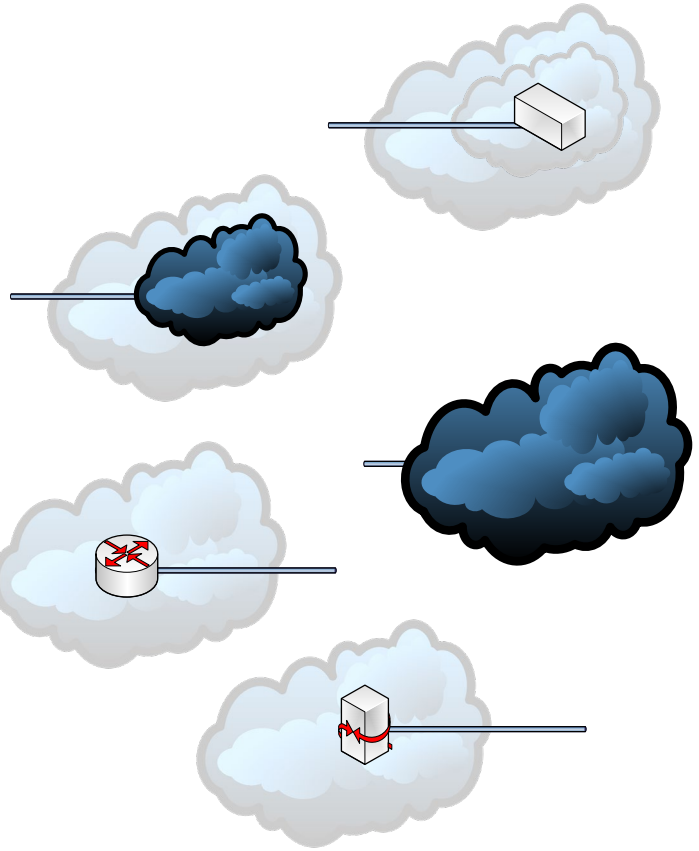
Característiques de les taules d'encaminament

- Tota estació d'una xarxa té una taula d'encaminament
- Les taules d'un host són molt simples
- Com a mínim cal que incloguin l'entrada: *default n.n.n.n*
- Les taules dels routers són complexes i es gestionen segons dues filosofies:
  - Vector de distància: té en compte el número i tipus de salts a realitzar
  - Estat de l'enllaç: crea un mapa de la xarxa i avalua dinàmicament el camí

4.2. Funció d'encaminament IP

Regles de recerca en les taules d'encaminament

1. Es busca una entrada que coincideixi amb l'adreça IP destí
2. Es busca una entrada que correspongui a la subxarxa de destí
3. Es busca una entrada que correspongui a la xarxa de destí
4. Es busca una entrada que correspongui a un router
5. S'utilitza el gateway per defecte.



4.2. Funció d'encaminament IP

Tipus de rutes

Ruta estàtica:

- Aquelles que estan predeterminades de forma fixa. Tenen poca flexibilitat però generen poc tràfic d'encaminament.

Ruta per defecte:

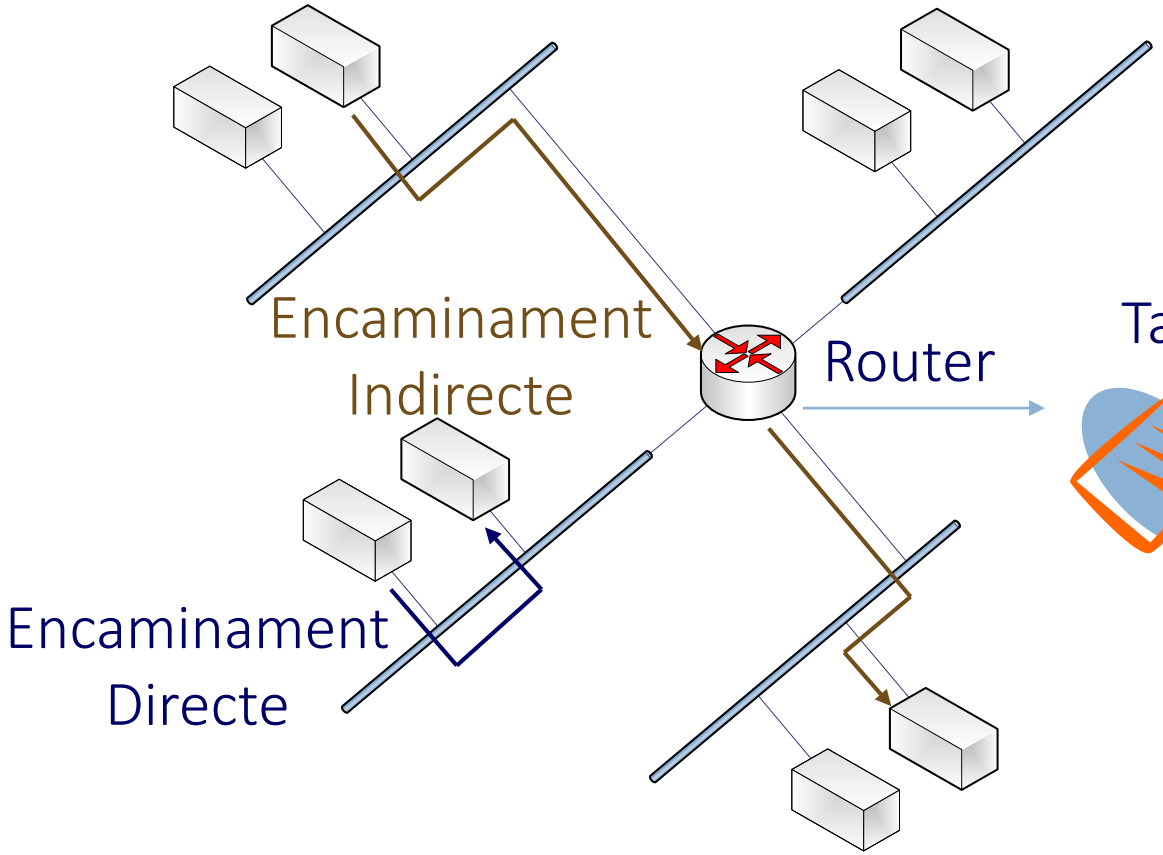
- Resultaria poc pràctic que un router conegués totes les xarxes existents. La ruta per defecte indica una ruta per on sortiran tots els paquets quan no s'indica una ruta específica per a un destí concret.

Ruta dinàmica:

- Són rutes establertes segons determinades variables de la xarxa (distància fins al destí, cost del camí, utilització dels enllaços, etc.). S'utilitzen uns protocols específics per realitzar l'intercanvi d'informació de les taules d'encaminament i el càlcul de les rutes més adequades per a cada destí.

4.3. Tipus d'encaminament IP

Encaminament directe/indirecte i estàtic/dinàmic

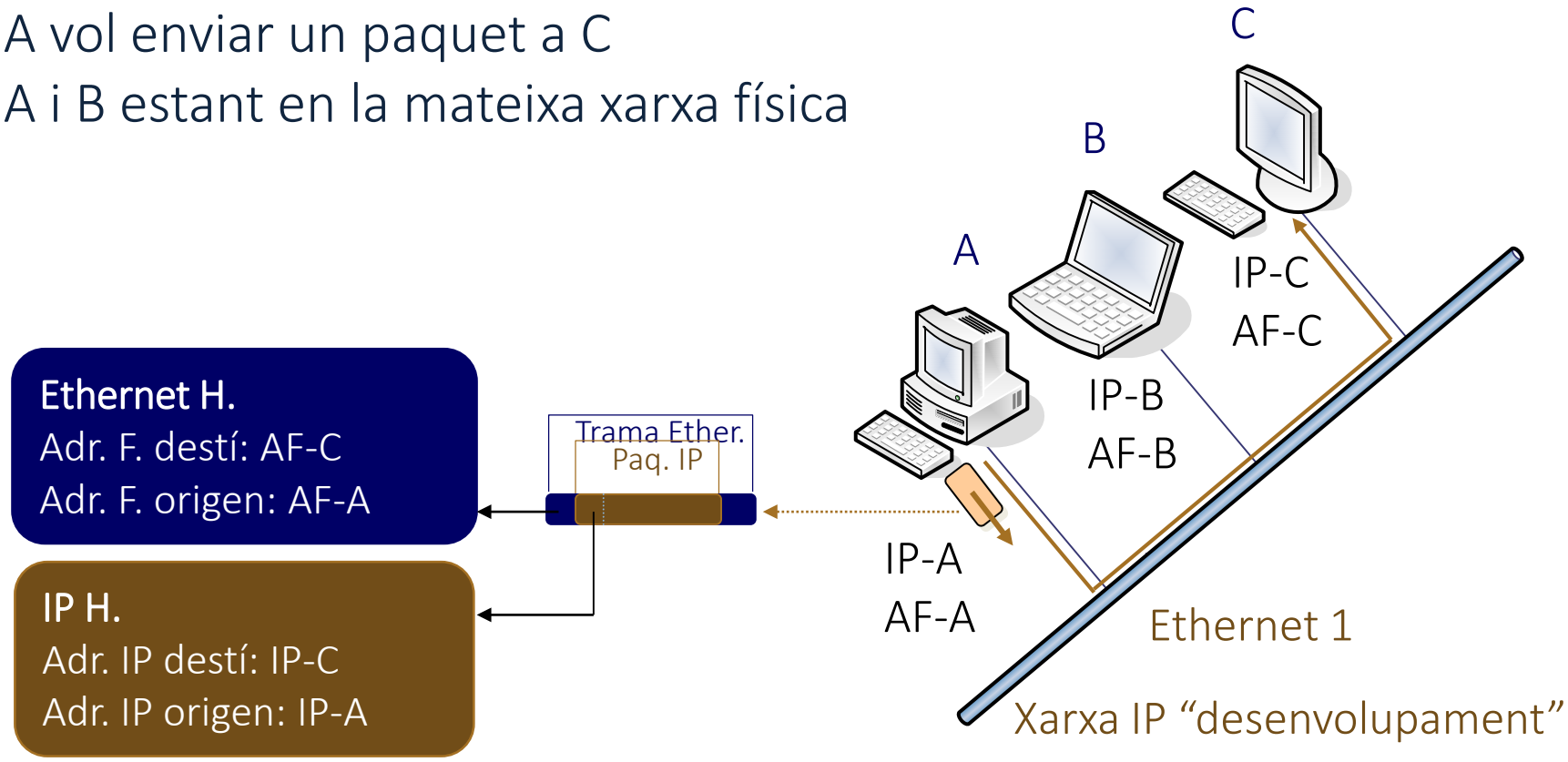


Taules d'encaminament:
- Estàtiques
- Dinàmiques

4.3. Tipus d'encaminament IP

Funcionament de l'encaminament directe

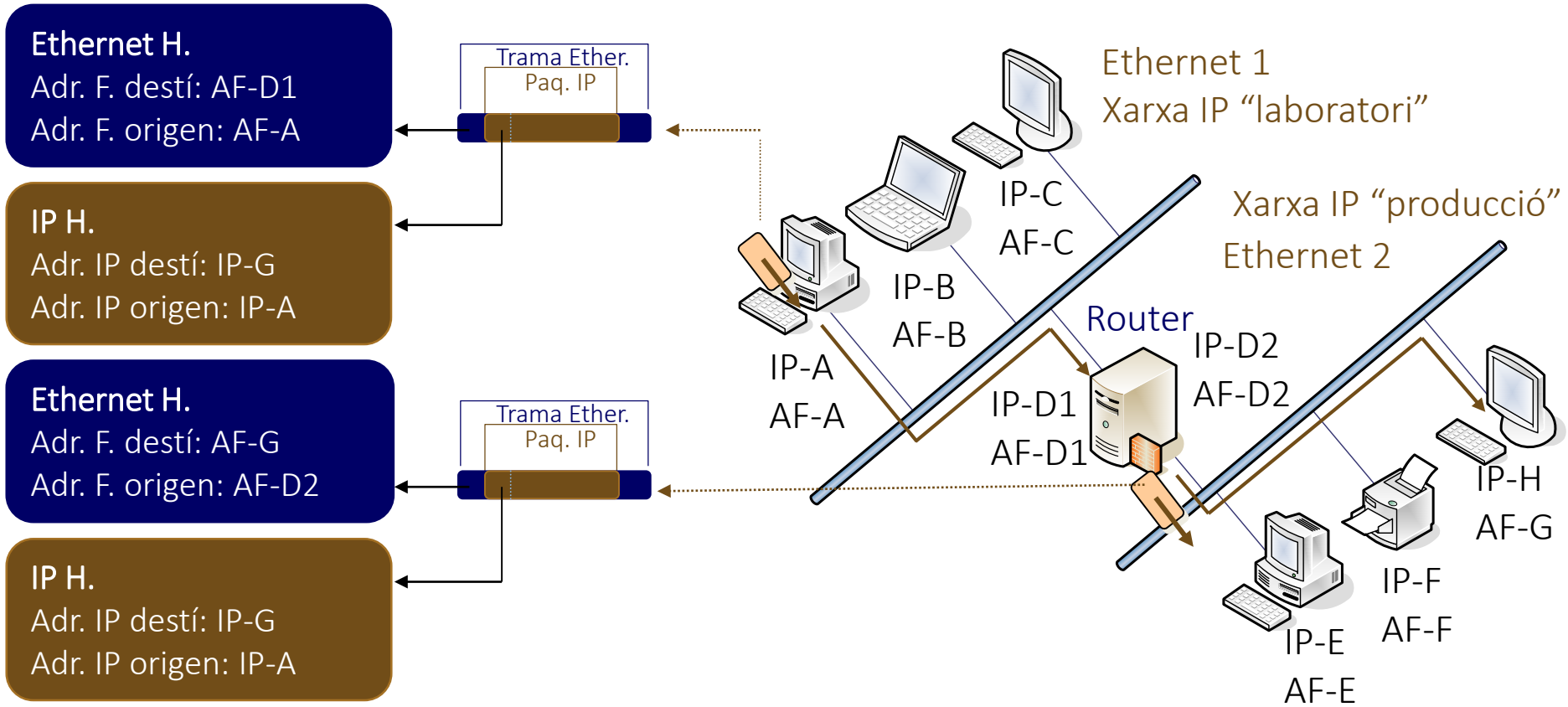
- A vol enviar un paquet a C
- A i B estant en la mateixa xarxa física



4.3. Tipus d'encaminament IP

Funcionament de l'encaminament indirecte

- A vol enviar un paquet a H.
- A i H estant en xarxes físiques diferents.



4.4. Fragmentació de datagrames IP

Conceptes bàsics

MTU (Maximum Transmission Unit)

- La trama té una longitud màx. de dades: MTU
- Depèn de la xarxa:

Xarxa física	MTU
Ethernet	1500 bytes
IEEE 802.3	1492 bytes
IEEE 802.5	màx. 4464 bytes
X.25	1600 bytes (pot variar per a diferents X.25)
FDDI	4352 bytes
Frame Relay	com a mínim 1600 bytes (normalment)
ATM	9180 bytes (per defecte), màx. 16K - 1

Fragmentació:

- Quan el paquet té una longitud major que la MTU
- El paquet es divideix en paquets amb longitud ≤ MTU

4.4. Fragmentació de datagrames IP

Conceptes bàsics

La fragmentació modifica les prestacions:

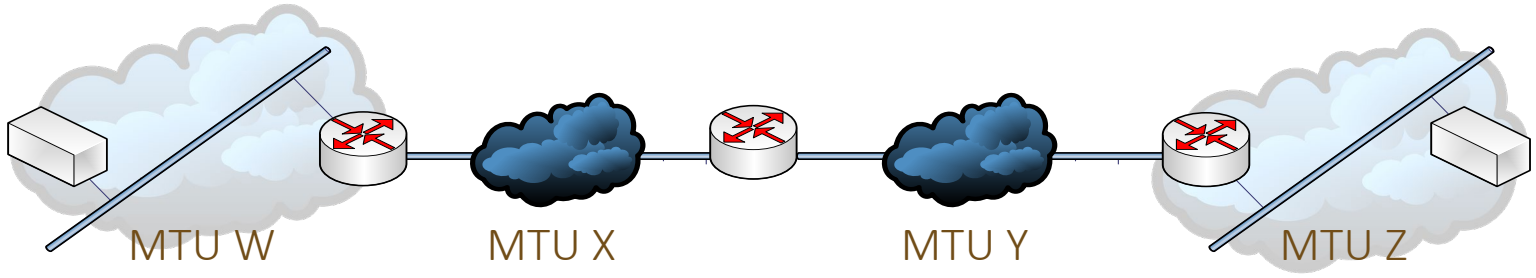
- Màxima longitud en l'origen → Molta fragmentacions.
- Longitud de MTU per no fragmentar → Es perd eficiència.

Path MTU:

- La MTU d'una ruta és la MTU màxima que no provoca fragmentació.

Mecanisme per esbrinar el Path MTU:

- Path MTU discovery (RFC 1191), basat en missatges ICMP.

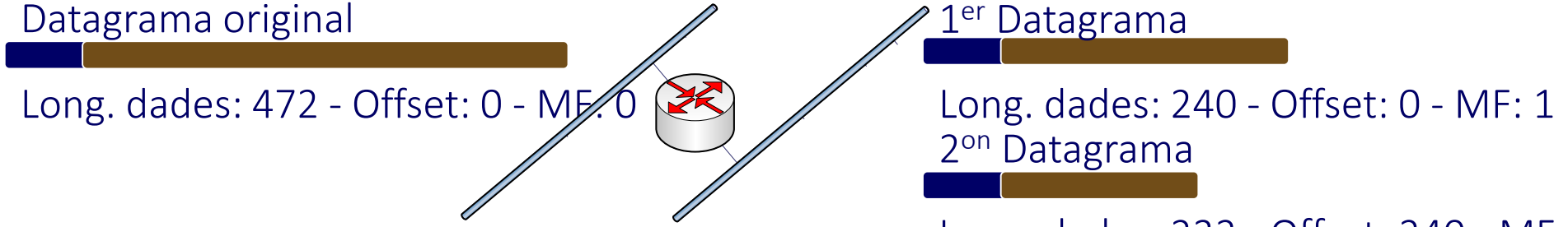


4.5. Fragmentació de datagrames IP

Procés de fragmentació

Quan un gateway fragmenta un datagrama fa els passos:

- Es creen dos datagrames i es còpia la capçalera en els dos
- Es divideix el camp de dades en blocs múltiples de byte
- Es carreguen els blocs de dades en els respectius datagrames
- S'actualitza el camp "longitud del datagrama"
- S'actualitza el flag "MF" del primer fragment: es posa a 1
- Es modifica l'Offset del segon datagrama



4.5. Fragmentació de datagrames IP

Reensamblament dels datagrames IP

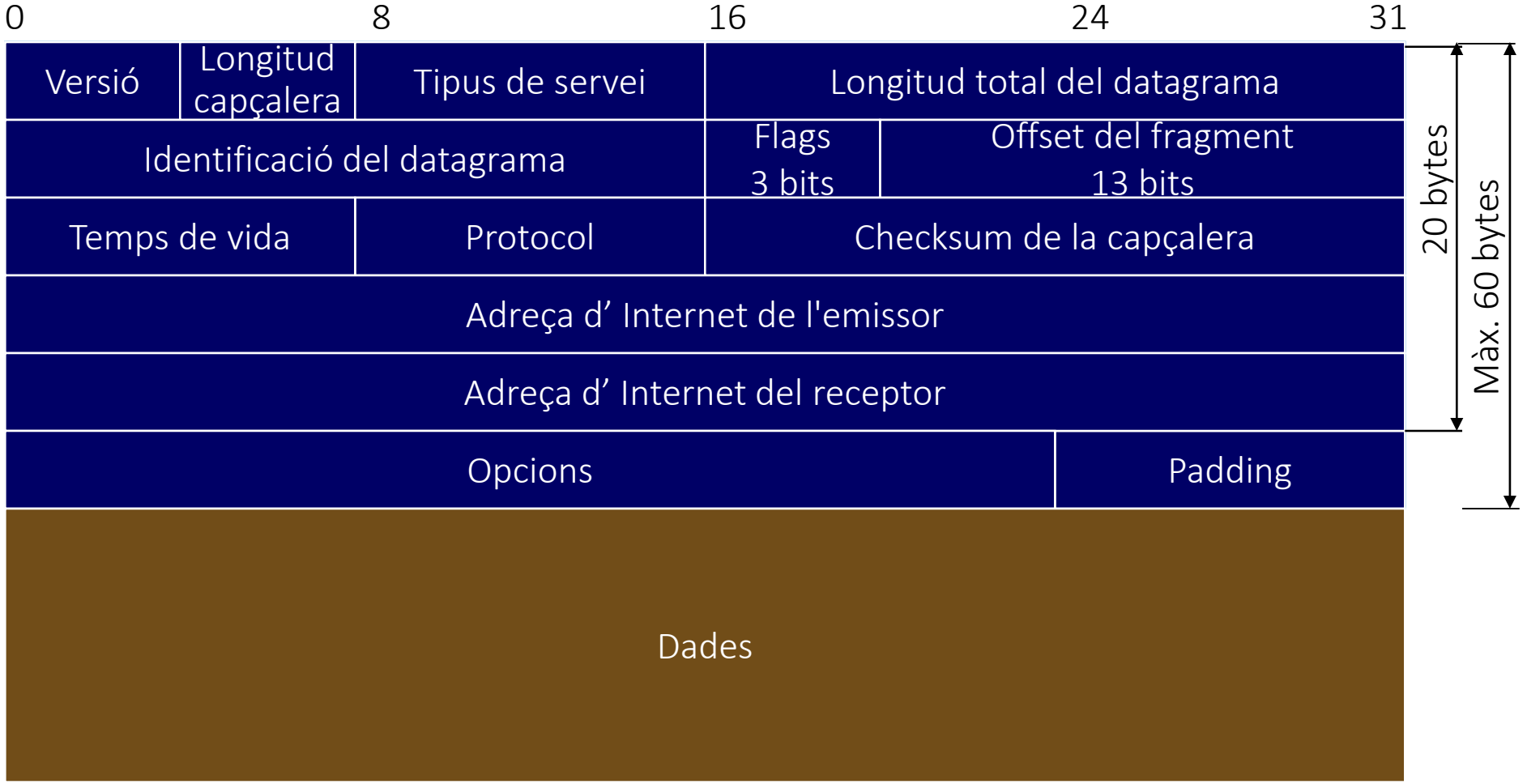
- Els fragments que tenen el mateix Identificador, Adreça IP origen i destí, i Protocol pertanyen al mateix paquet.
- La fragmentació es pot donar en qualsevol punt de la xarxa.
- El reensamblament únicament es fa en el destí.
- Problemes:
  - Es desconeix la mida total del paquet original.

    Memòria disponible en els routers
  - Pèrdua d'un fragment

    S'activa un temporitzador quan arriba un dels fragments. Si el temporitzador arriba a 0 i no han arribat tots els fragments, es descarten els fragments rebuts i s'envia un missatge d'error.

4.6. Format del datagrama IP

Estructura del datagrama



4.6. Format del datagrama IP

Camps "versió" i "longitud capçalera" del datagrama

Versió (4 bits)

- Versió del protocol IP, per assegurar que el paquet s'interpreta correctament. Normalment és 4, i per a la nova versió és 6.

Longitud capçalera (4 bits)

- Nombre de paraules de 32 bits de la capçalera, incloent les opcions.
- Si no hi ha opcions val 5: la capçalera mínima és de 20 bytes.
- La longitud màxima de capçalera és de 60 bytes.

4.6. Format del datagrama IP

Camp "Tipus de servei" del datagrama

Tipus de servei (Type of Service) (8 bits)

- Especifica com s'ha de tractar el datagrama.
- Definits en RFC 791

- Precedència: Importància o prioritat del paquet (8 nivells)
- D T R M: Tipus de transport que es desitja (2 nivells):

D = 1 (poc retard) T = 1 (cabal alt) ,

R = 1 (fiabilitat alta) M = 1 (cost econòmic baix)

4.6. Format del datagrama IP

Camp "Tipus de servei" del datagrama

Significat dels bits de TOS (Type Of Service)

DTRM		DTRM	
0 0 0 0	Defecte	0 1 0 0	Maximitza cabal
0 0 0 1	Minimitza cost monetar	1 0 0 0	Minimitza retard
0 0 1 0	Maximitza fiabilitat	1 1 1 1	Maximitza seguretat

Exemples de l'ús dels bits de TOS

	D	T	R	M
TELNET	1	0	0	0
FTP control	1	0	0	0
FTP dades	0	1	0	0
SNMP	0	0	1	0
NNTP	0	0	0	1

4.6. Format del datagrama IP

Camps "Longitud total" i "Identificador" del datagrama

Longitud total del datagrama (16 bits)

- Longitud total del datagrama, capçalera + dades, en bytes.
  Longitud màxima 2^{16} = 65.535 Bytes
  - Però en Ethernet: 1500 Bytes,
  - En IEEE 802.3: 1492 Bytes
  - o en ATM: 9180 Bytes, max 16KB - 1

Identificador del datagrama (16 bits)

- Nº de 16 bits que identifica el datagrama. S'assigna seqüencialment.
  - Per controlar les duplicacions.
  - Per facilitar el reensamblament dels fragments d'un datagrama.
- Si el datagrama es fragmenta, tots els fragments tindran l'identificador de l'original.

4.6. Format del datagrama IP

Camps "Flags" i "Offset del fragment" del datagrama

Flags (3 bits)

- R: bit reservat.
- DF: No fragmentar. El datagrama no pot ser fragmentat.
  - Si fos necessari fragmentar-lo, es descartaria.
- MF: Segueixen fragments. No és l'últim fragment del paquet.

Offset del fragment (13 bits)

- Permet ordenar els fragments.
- Indica la posició del fragment dins del datagrama original.
- Es dóna en unitats de 64 bits (8 bytes).
- Excepte l' últim, els fragments tenen una longitud múltiple de 8 bytes.

4.6. Format del datagrama IP

Camps d'adreces i "Temps de vida" del datagrama

Adreça d' Internet de l'emissor (32 bits)

- Adreça origen del paquet.

Adreça d' Internet del receptor (32 bits)

- Adreça destí del paquet.

Temps de vida (TTL: Time To Live) (8 bits)

- Especifica el temps que el paquet pot romandre circulant per la xarxa.
- Es dóna en unitats de segons (a la pràctica serà un límit màx. de la vida d'un paquet).
- Es decrementa una unitat (per simplificar) cada cop que passa un router:
  - Quan arriba a 0 es llença el paquet.
- L'inicialitza l'emissor (normalment, a 32 o a 64).

4.6. Format del datagrama IP

Camp de "Protocol" del datagrama

Protocol (8 bits)

- Indica el protocol del nivell superior que es transporta en el camp de dades.
- Es codifica amb un valor assignat en el RFC1700:

Decimal	Hexa	Protocol	Descripció
1	01	ICMP	Internet Control Message Protocol
2	02	IGMP	Internet Group Management Protocol
3	03	GGP	Gateway-to-gateway Protocol
4	04	IP	Internet Protocol
6	06	TCP	Transmission Control Protocol
8	08	EGP	Exterior Gateway Protocol
9	09	IGP	Interior Gateway Protocol
17	11	UDP	User Datagram Protocol
29	1D	ISO-TP4	ISO Transport Protocol 4
88	58	IGRP	Internet Gateway Routing Protocol
89	59	OSPFIGP	Open Shortest Path First Protocol

4.6. Format del datagrama IP

Camp de "Checksum de la capçalera" del datagrama

Checksum de la capçalera (16 bits)

- Verificació d'errors de la capçalera (no de les dades).
- Es recalcula en cada router.
- Per calcular-lo, en l'emissor: (RFC1624)
  - Es posa a 0 el camp Checksum
  - Es calcula la suma: complement a 1 de la suma en complement a 1 de 16 bits de tota la capçalera.
  - Es guarda el resultat en el camp Checksum.
- Per verificar-lo, en el receptor:
  - Fa la suma complementa a 1 de tota la capçalera: Si el resultat és 0 és correcte, sinó el datagrama té la capçalera errònia: es descarta el datagrama.

4.6. Format del datagrama IP

Camps "Opcions" i "Padding" del datagrama

Opcions (longitud variable)

- Aquest camp el porten pocs paquets.
- Proporcionen timestamp, seguretat i encaminament especial.
- Pot portar una o més opcions.
- L'estructura del camp d'opcions té dos casos:
  - Cas 1: Un únic byte de tipus d'opció.
  - Cas 2: Un byte de tipus d'opció, un byte de longitud d'opció (mesurada en bytes) i els bytes de dades de l'opció.
- Estructura del subcamp tipus d'opció:
  - C.F., Còpia en fragment (1 bit)
  - Classe op., Classe d'opció (2 bits)
  - N. Opc., Número d'opció (5 bits)

Padding: serveix per fer la longitud de la capçalera múltiple de 32 bits.

4.6. Format del datagrama IP

Subcamp"Identificador de l'opció" del datagrama

Identificador de l'opció (8 bits)

- **C.F.,** Còpia en fragment (1 bit):
  - Especifica que les opcions s'han de copiar a tots els fragments del datagrama original.
- **Classe op.**: Tipus de classe (2 bits)
  - 0 → control
  - 2 → depuració i mesures
  - 1 i 3 → ús reservat
- **N. Opc.**: Número d'opció (5 bits)
  - 2 - Seguretat
  - 3 - Ruta específica per on ha de passar el datagrama
  - 4 - Timestamp: mesures de retards entre nodes
  - 7 - Gravar ruta per on passa el datagrama

4.6. Format del datagrama IP

Subcamp"Identificador de l'opció" del datagrama

Algunes opcions en funció de la classe i el número:

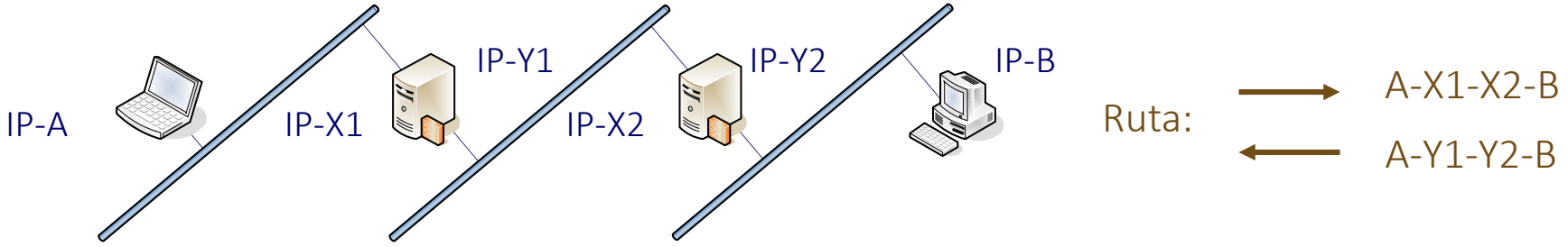
Classe	Número	Longitud	Descripció
0	0	-	Final de llista d'opcions
0	1	-	No operation (No hi ha res)
0	2	11	Security DoD IP
0	3	variable	Loose source routing
0	7	variable	Record route
0	8	4	Obsolet
0	9	variable	Strict Source Routing
2	4	variable	Timestamp

4.6. Format del datagrama IP

Opcions d'encaminament de font del datagrama

Encaminament de font:

- La ruta que han de seguir els paquets està donada per la font
- Els paquets que viatgen dels del destí cap a la font han d'utilitzar la mateixa ruta que els paquets que van de font a destí.
- Tipus: Estricte (strict) i desconnectat (Loose).
- Problema

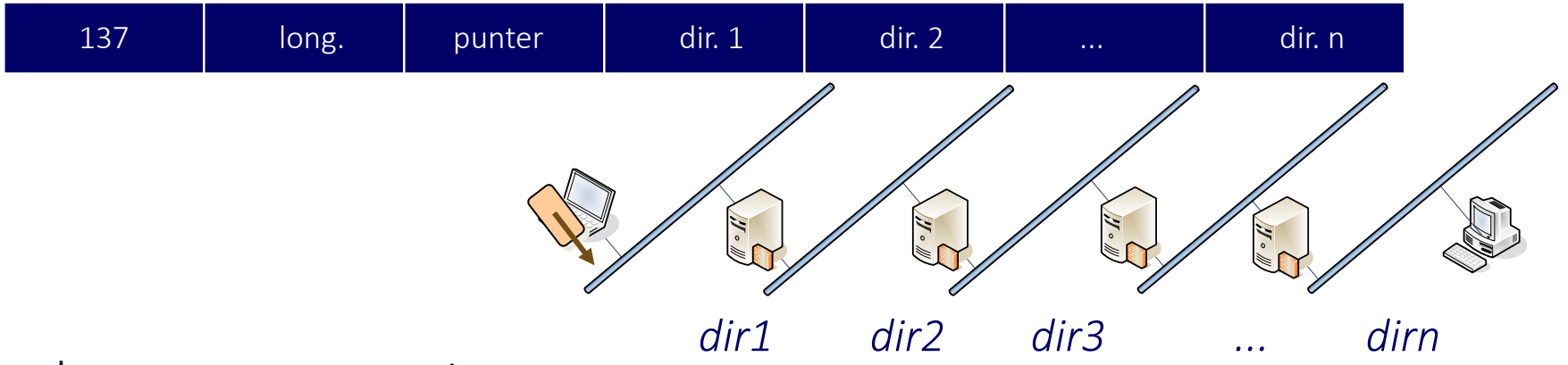


- No es pot utilitzar la descripció de ruta donada per A.
- Els routers modifiquen les adreces d'entrada per les de sortida.

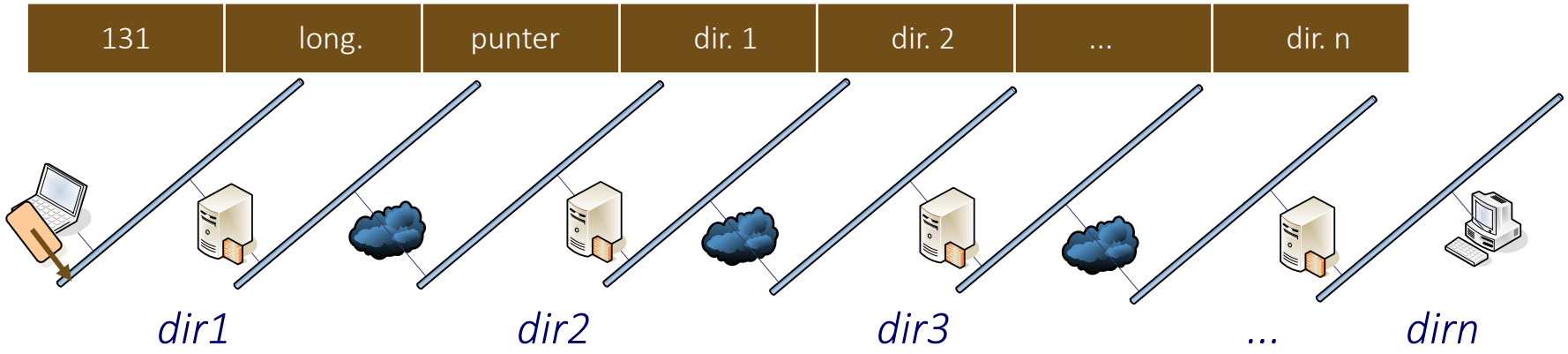
4.6. Format del datagrama IP

Opcions d'encaminament de font del datagrama

- Strict source route:



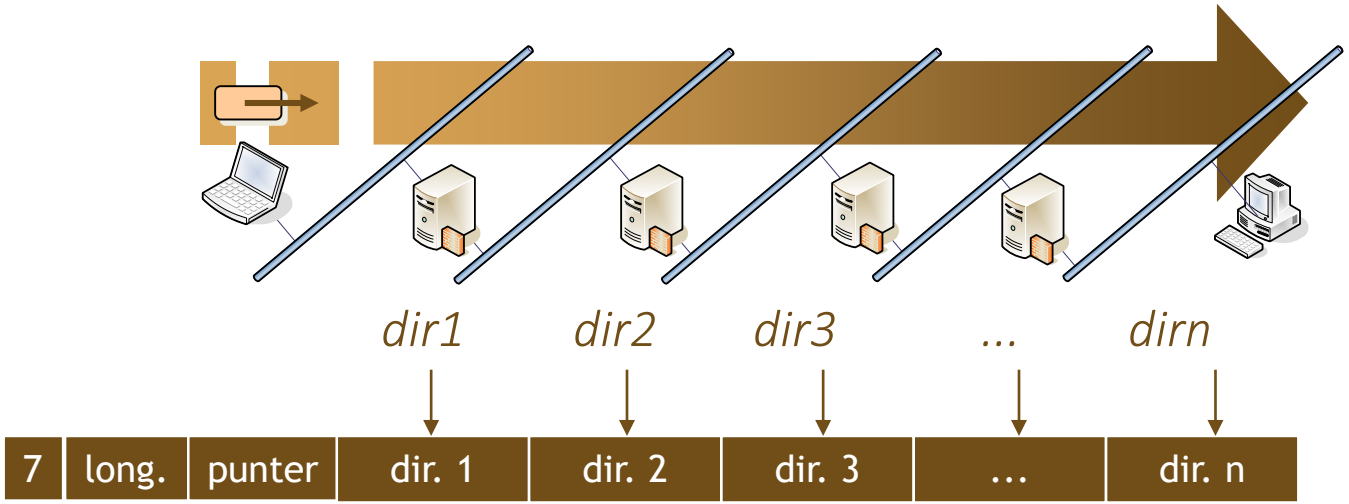
- Loose source route:



4.6. Format del datagrama IP

Opcions d'encaminament de font del datagrama

- Record route: Es van afegint adreces



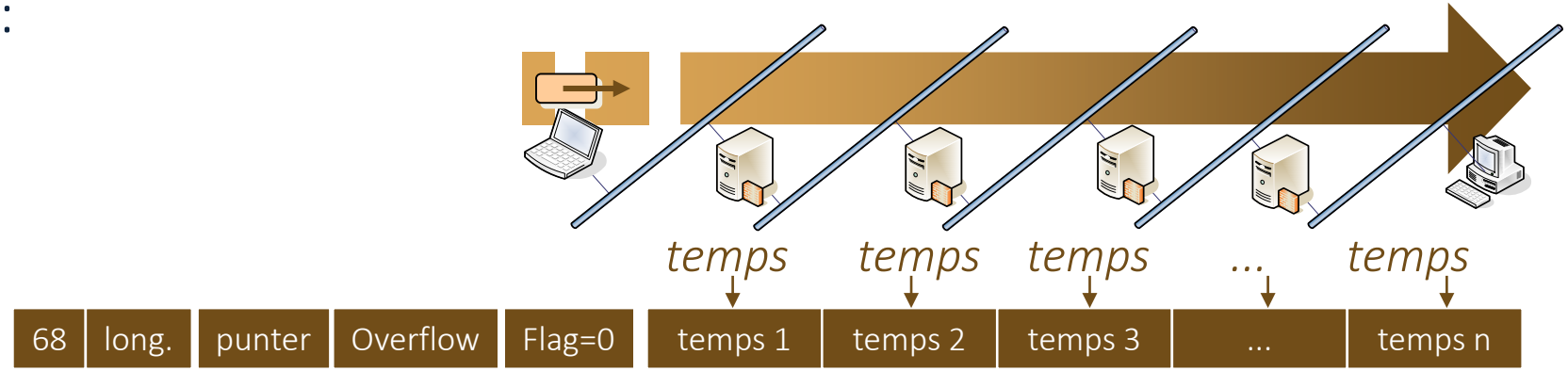
Punter (en bytes): indica la posició en l'adreça. Comença pel quart octet i s'incrementa en 4.

Si punter > longitud: S'han consumit totes les adreces i s'encamina per l'adreça del destí.

4.6. Format del datagrama IP

Opcions d'encaminament de font del datagrama

- Timestamp:



- Flag (4 bits): tipus de format

0 → En cada salt es guarda el temps en l'espai reservat i s'incrementa el punter en 4.

- Overflow (4bits): És el nombre de mòduls IP que no poden enregistrar el timestamp per manca d'espai.

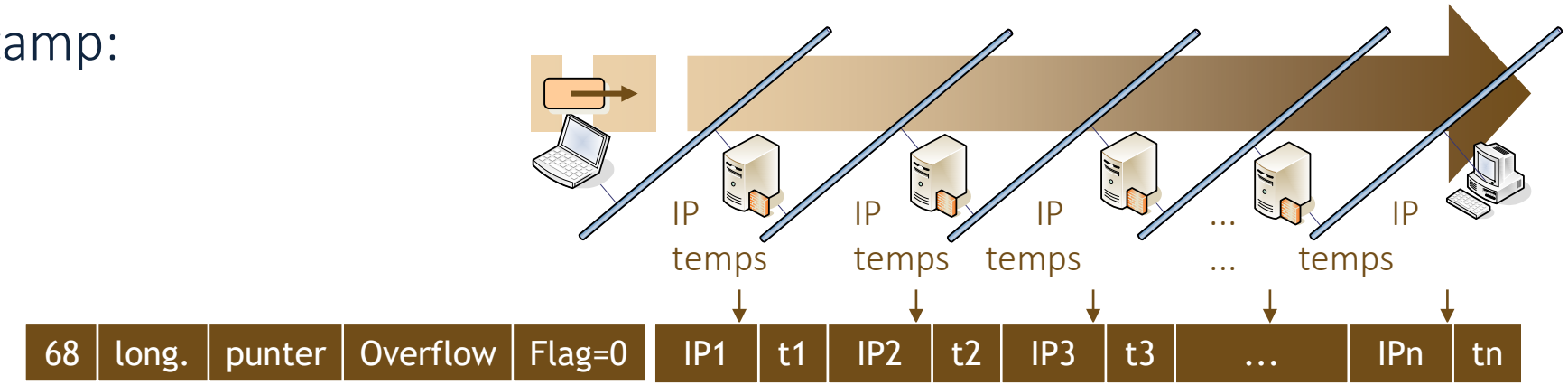
Si se supera l'espai reservat s'incrementa el camp d'Overflow en 1.

Si el camp d'Overflow s'esgota (>15) es descarta el datagrama.

4.6. Format del datagrama IP

Opcions d'encaminament de font del datagrama

- Timestamp:



Timestamp. Flag = 1 i 3.

1 → En cada salt es guarda el temps i l'adreça del router.

Es reserva espai per als dos camps i s'incrementa el punter en 8.

3 → L'origen indica en quins nodes poden gravar el temps.

Si el router troba la seva adreça en la llista afegeix el timestamp.

4.7. Internet Control Message Protocol

Problemàtica associada al protocol IP

Protocol IP → No fiable
No orientat a connexió

- Es necessita un mecanisme de control:
  - Per què un datagrama no s'ha pogut entregar ?
    - La màquina destí no està connectada a la xarxa
    - El temporitzador a expirat
    - Congestió en la xarxa
  - Indicació d'errors esdevinguts en el tractament de datagrames
  - Descobriment de noves rutes
  - Un router no té prou buffer per emmagatzemar paquets

4.7. Internet Control Message Protocol

Fonaments del protocol ICMP

Inicialment va ser desenvolupat perquè els routers informessin de les causes d'error en el lliurament de paquets.

El protocol ICMP no fa el protocol IP més fiable, només notifica errors a la màquina origen, però no als nodes intermitjos.

- La fiabilitat s'aconsegueix amb els protocols del nivells superiors.

El missatges ICMP de notificació d'error es dirigeixen al host origen (el que va enviar el paquet que provoca l'error).

- Els routers intermitjos no tindran coneixement dels errors i no podran actuar.

Els paquets ICMP també poden tenir errors. En aquest cas no es genera cap altre paquet ICMP (per evitar recurrència).

4.7. Internet Control Message Protocol

Encapsulament dels missatges ICMP

Els missatges ICMP viatgen en el camp de dades del protocol IP, però no és un protocol d'alt nivell.

Normalment es considera com una part del nivell IP.

El destinatari és el mòdul IP, no l'usuari origen o destí.

Els missatges ICMP poden ser:

- Missatges d'error (utilitzats pels routers)
- Missatges de consulta (utilitzats pels hosts)

4.7. Internet Control Message Protocol

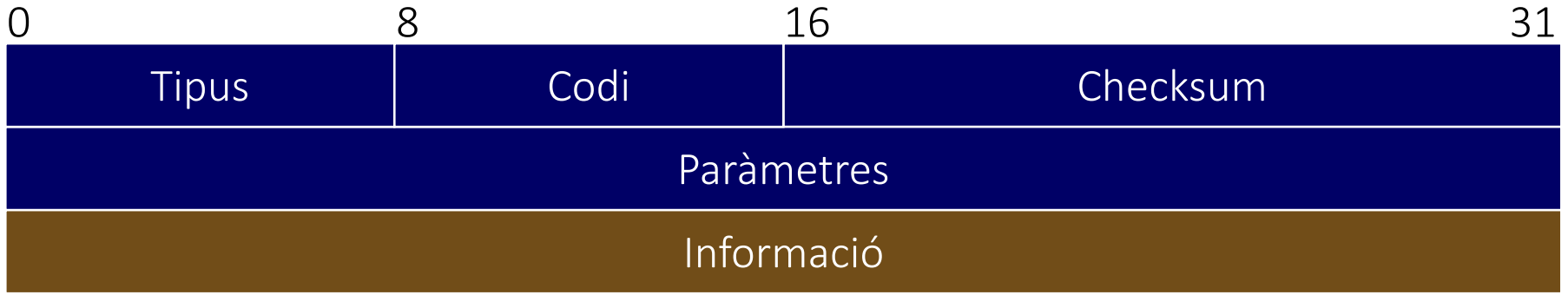
Condicions de generació dels missatges ICMP

Un missatge d'error ICMP no es genera mai com a resposta a:

- Un altre missatge d'error ICMP (excepte per a missatges ICMP de consulta).
- Un paquet amb adreça destí de broadcast o multicast.
- Un paquet enviat com a broadcast per la capa d'enllaç.
- Un fragment d'un paquet (que no sigui el primer cas).
- Un paquet l'adreça origen del qual no defineix a un host únic (Adreça origen no pot ser 0, Loopback, broadcast o multicast).

4.8. Missatges ICMP

Format dels missatges ICMP



- **Tipus:** Tipus de missatge ICMP. Hi ha 15 possibles missatges.
- **Codi:** Identifica alguna condició addicional per a cada tipus de missatge ICMP.
  - **Checksum:** Per protegir el missatge ICMP dels errors. Es calcula sobre tot el missatge ICMP i fa servir el mateix algorisme que per a la capçalera IP.
- **Paràmetres:** Paràmetres del missatge.
- **Informació:** Capçalera i 8 primers bytes del datagrama que ha provocat la generació del missatge ICMP.

4.8. Missatges ICMP

Tipus de missatges ICMP

0 - Resposta d'Eco: Per testejar si es pot arribar a una màquina (ping)
3 - Destí no assolible
4 - Control de flux (source quench): una memòria es desborda
5 - Canvi de ruta: per indicar que hi ha una ruta millor
8 - Petició d'Eco (ping)
11 - Temps de datagrama esgotat: rutes circulars o massa llargues
12 - Problema en un paràmetre del datagrama
13 - Petició de timestamp: control del temps de la ruta utilitzada
14 - Resposta de timestamp
15 - Petició d'informació (obsolet)
16 - Resposta d'informació (obsolet)
17 - Petició de la màscara de subxarxa
18 - Resposta de la màscara de subxarxa

4.8. Missatges ICMP

Tractament dels missatges ICMP

Destí no assolible:
- Lliurar el missatge ICMP a la capa de transport.
- L'acció següent depèn de la causa d'aquest error.

Canvi de ruta (redirect):
- El host ha d'actualitzar la taula d'encaminament.

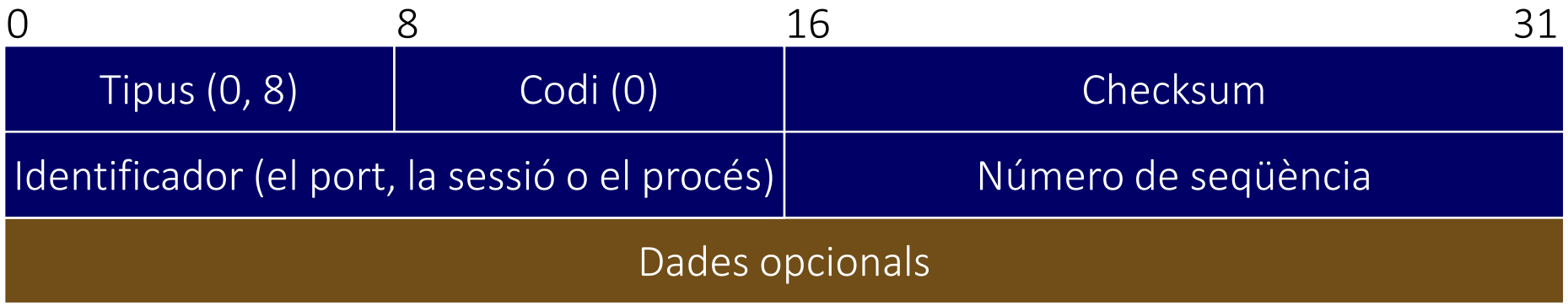
Source quench:
- Lliurar el missatge a la capa de transport o a un mòdul de processament ICMP.

Temps esgotat:
- Lliurar el missatge a la capa de transport

Paràmetres incorrectes:
- Lliurar el missatge a la capa de transport; opcionalment notificar a l'usuari.

4.8. Missatges ICMP

Missatges d'ECO



Tipus: Resposta → 0, petició → 8

Identificador: Per identificar quin és l'origen dins del host origen.

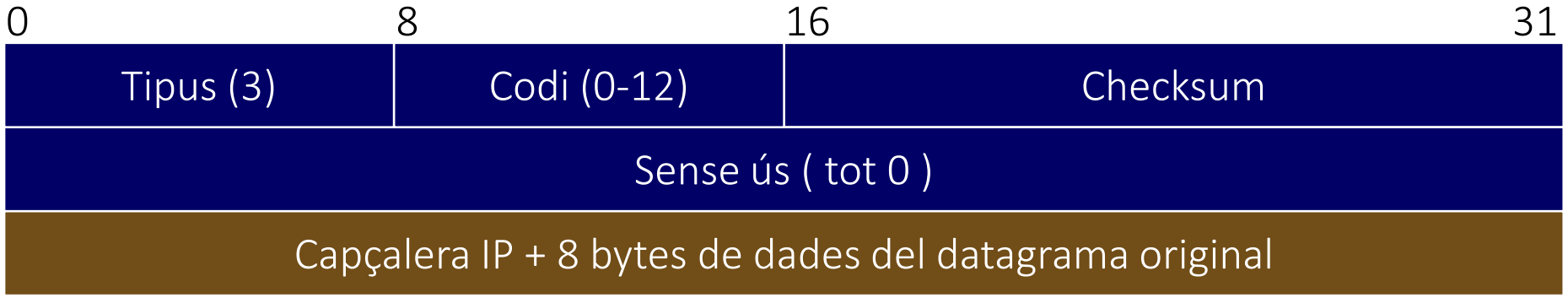
Dades opcionals: L'originador pot posar dades que el destí retornarà en l' ECO de resposta.

Número de seqüència: per identificar els missatges ECO d'una mateixa ràfaga (els que tindran el mateix identificador).

Utilitzat pel servei *ping.*

4.8. Missatges ICMP

Missatges d'error: Destí no abastable



Enviat per routers i hosts:

- **Routers**: no es coneix la xarxa, no es pot fragmentar, host no disponible, etc.
- **Hosts**: protocol del paquet IP no està disponible, port no assolible, etc.

4.8. Missatges ICMP

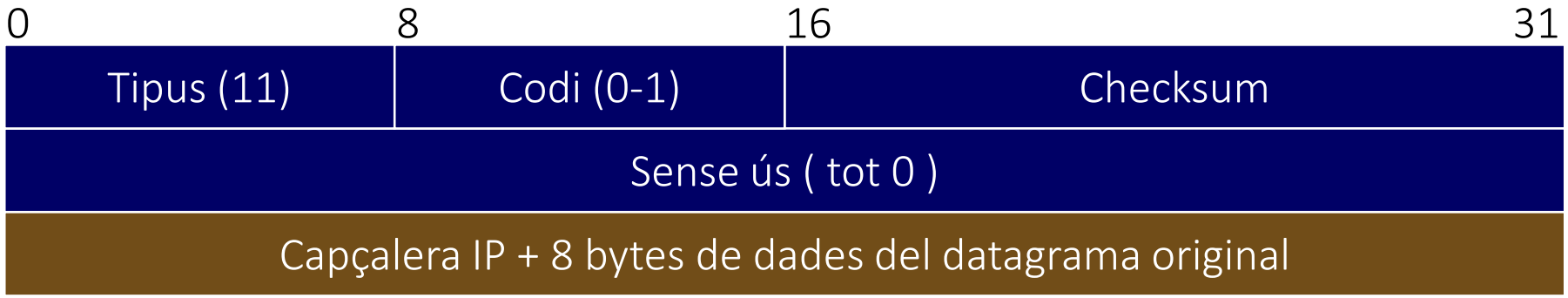
Missatges d'error: Destí no abastable

- El camp **Codi** identifica la causa de l'error:

0 - Network unreachable
1 - Host unreachable
2 - Protocol unreachable
3 - Port unreachable
4 - Fragmentation needed and Do Not Fragment flag is set
5 - Source route failed
6 - Destination network unknown
7 - Destination host unknown
8 - Source host isolated
9 - Communication with destination network administratively prohibited
10 - Communication with destination host administratevely prohibited
11 - Network unreachable for type of service
12 - Host unreachable for type of service

4.8. Missatges ICMP

Missatges d'error: Temps esgotat



Codi: 0 - S'ha esgotat el Time to Live
1 - S'ha esgotat el temporitzador de reensamblament

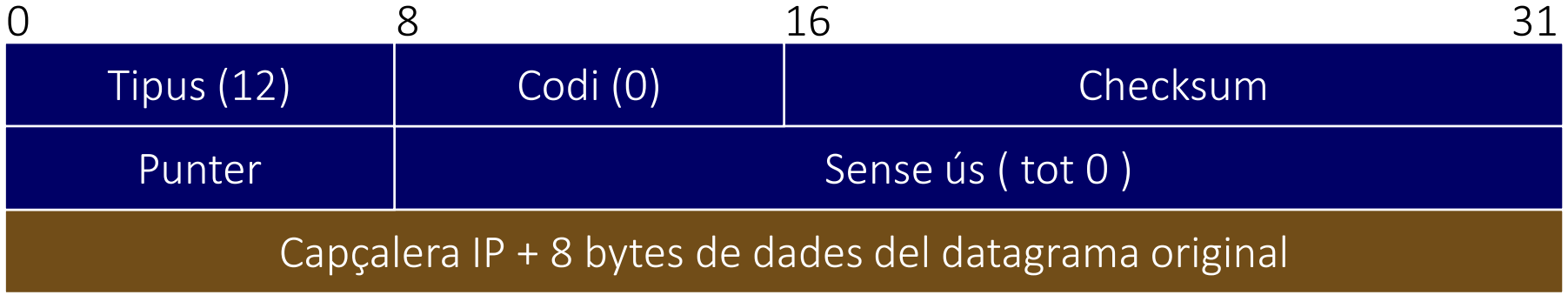
Degut a rutes circulars o excessivament llargues.

Quan el temps de vida d'un paquet s'acaba, el router el descarta i envia un missatge d'error ICMP.

Esgotar el temporitzador en el reensamblament d'un datagrama (enviat des del host destí).

4.8. Missatges ICMP

Missatges d'error: Paràmetres incorrectes



Codi: 0 - El punter indica on es troba el problema.
1 - Aplicacions militars: manca una opció; no s'utilitza el punter.

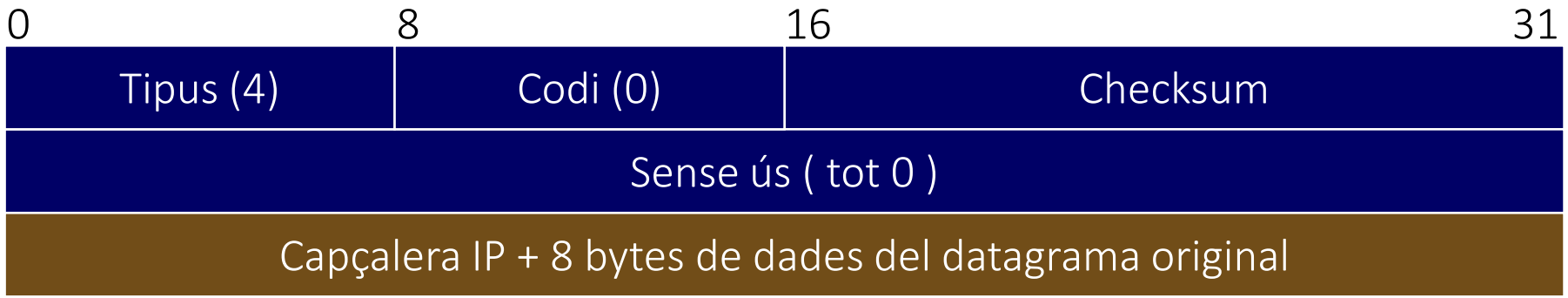
A causa d'algun problema en la capçalera del datagrama.

Ell datagrama es descarta i s'envia el missatge ICMP.

El punter indica el byte de la capçalera on s'ha detectat l'error.

4.8. Missatges ICMP

Missatges de control de flux: Source Quench



Enviat per routers i hosts que reben dades més ràpid del que poden processar.

Si el buffer d'entrada s'omple els datagrames es perdran.

Quan es perd un paquet s'envia un ICMP per a que es pugui reenviar.

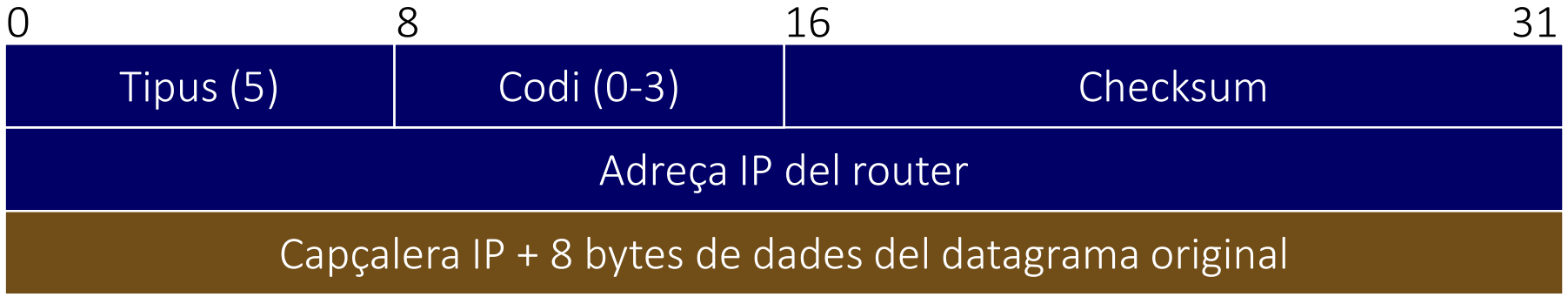
Quan es rep un missatge ICMP d'aquests tipus la font envia els paquets de forma més lenta.

Posteriorment, es torna a incrementar el ritme, lentament.

Aquest tipus de missatges pràcticament no s'utilitzen.

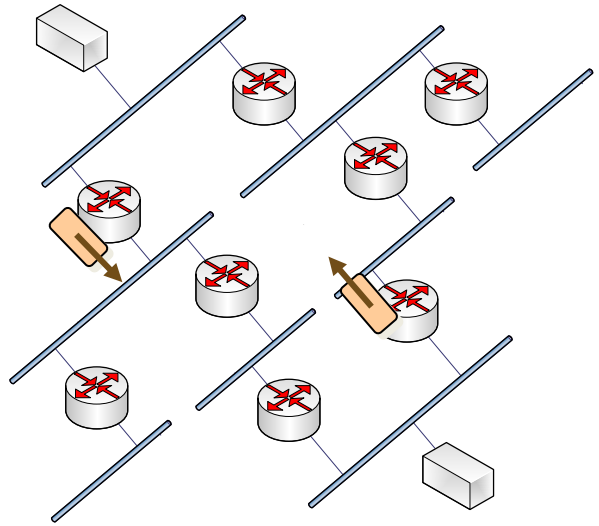
4.8. Missatges ICMP

Missatges d'encaminament: redirigir (canvi de ruta)



Només els envien els routers.

Informen que hi ha una ruta millor.



4.8. Missatges ICMP

Missatges d'encaminament: redirigir (canvi de ruta)

Quan s'utilitza un protocol d'encaminament dinàmic, els routers s'assabenten de les noves rutes però els hosts no.

Els routers envien informació als hosts perquè actualitzin l'entrada de router per defecte en la taula de rutes.

Els hosts depenen dels routers per mantenir la informació d'encaminament.

Codis de missatge ICMP de redirecció (Canvi de Ruta):

0 → Redireccionament de datagrames de la mateixa xarxa (obsolet)

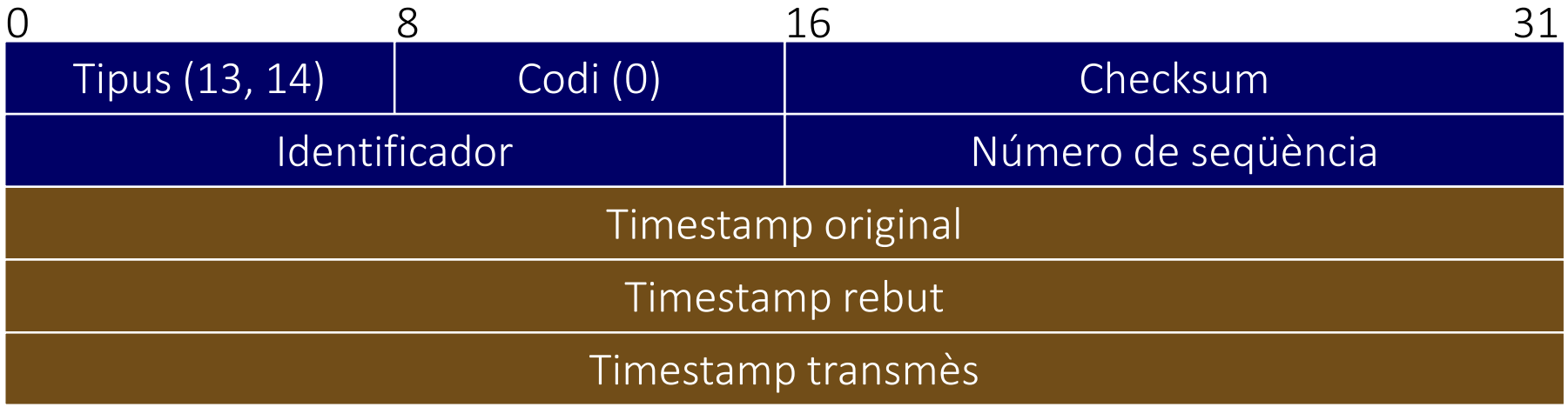
1 → Redireccionament de datagrames del mateix host

2 → Redireccionament de datagrames del mateix tipus de servei i xarxa

3 → Redireccionament de datagrames del mateix tipus de servei i host

4.8. Missatges ICMP

Missatges d'encaminament: Marques de temps



Codi: 13 - missatge ; 14 - resposta

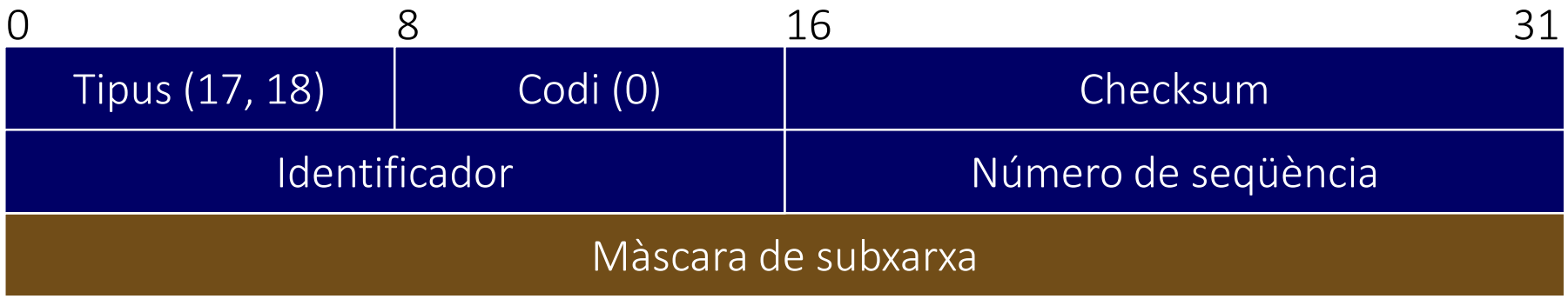
Màquines independents → Rellotges desincronitzats

El missatge de timestamp serveix per sincronitzar màquines i estimar el temps de trànsit del paquets.

Problema: el temps de trànsit d'un paquet pot variar molt d'un intent a un altre.

4.8. Missatges ICMP

Missatges d'encaminament: Obtenció de màscara



Codi: 17 - Petició
18 - Resposta

Quan el host no sap quina màscara de subxarxa s'utilitza en la seva subxarxa la pot demanar a un router (o un servidor de màscares).

La petició es pot enviar a un router directament, si se sap l'adreça, o, si no, es pot fer un broadcast a la xarxa.

4.8. Missatges ICMP

Missatges d'encaminament: Descobriment de rutes

Els routers envien informació periòdicament i així els hosts poden descobrir noves rutes.

Els hosts també poden sol·licitar aquesta informació.

Els missatges es poden enviar a les adreces:

Multicast, tots els sistemes:	224.0.0.1
Multicast, tots els routers:	224.0.0.2
Broadcast:	255.255.255.255

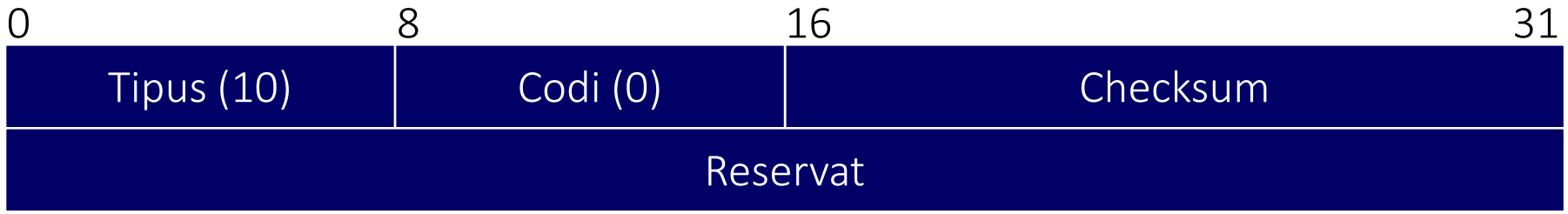
Necessitat d'un router per defecte → Fitxer → Procediment no dinàmic → Missatges ICMP de millors rutes

- Alguns hosts interpreten protocols d'encaminament
  Router Discovery Protocol (RDP)

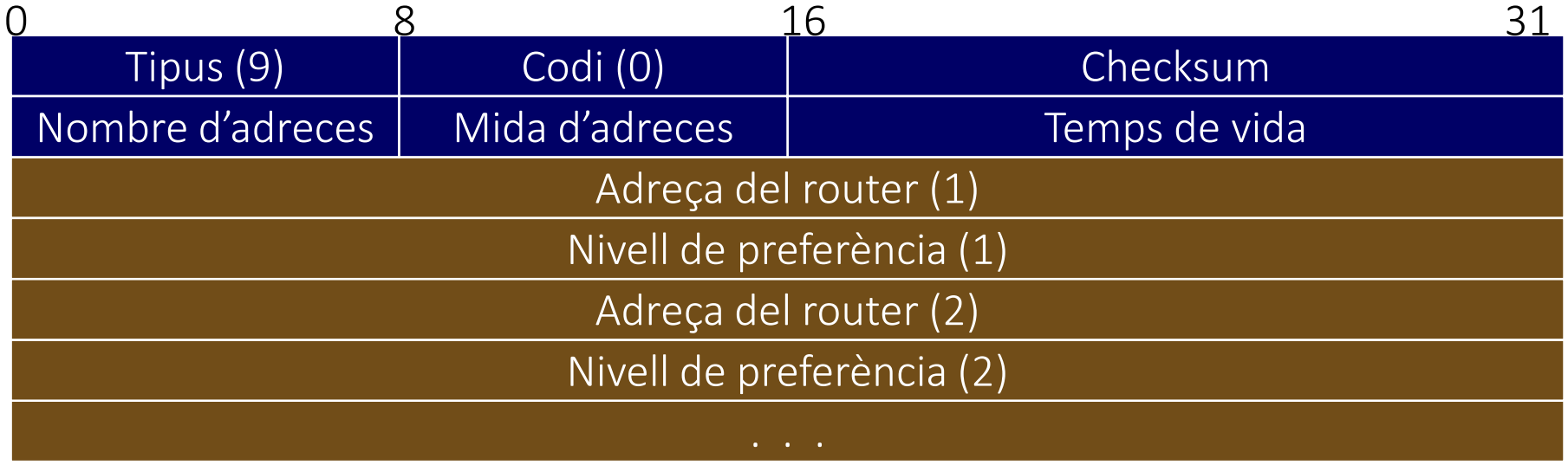
4.8. Missatges ICMP

Missatges d'encaminament: Descobriment de rutes

Petició



Anunci - Resposta



4.8. Missatges ICMP

Missatges d'encaminament: Descobriment de rutes

Nombre d'adreces:

- De quantes adreces informa el missatge.

Mida d'adreces:

- Quantes paraules de 32 bits s'utilitzen per descriure una adreça.

  Actualment és sempre 2.

Temps de vida:

- Temps durant el qual les adreces poden considerar-se vàlides

Adreça del router (n) :

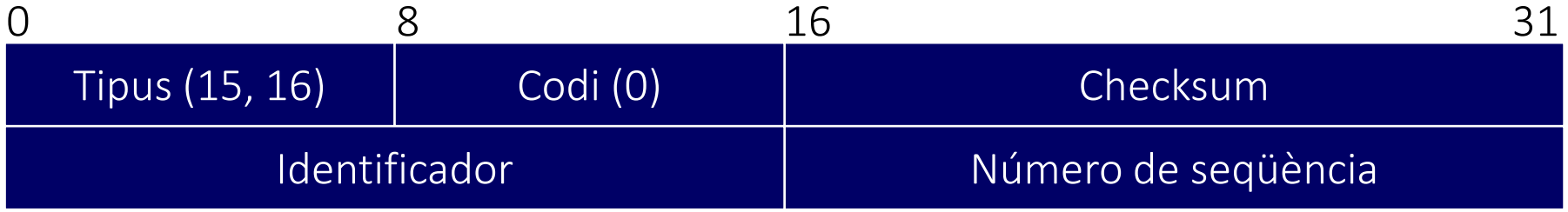
- Adreces IP n del router de la interfície per on ha enviat l'anunci.

Nivell de preferència (n):

- Com més alt és aquest valor més recomanada és la utilització d'aquest router.

4.8. Missatges ICMP

Missatges d'informació



Codi: 15 - Petició
16 - Resposta

Aquests missatges es consideren obsolets.

S'utilitzaven perquè determinats hosts poguessin obtenir la seva adreça Internet al posar-se en funcionament. Actualment s'utilitza el RARP (o altres protocols).

4.9. Exemples pràctics

Comandes útils en entorns IP

Utilitzar la funció *hostname* per obtenir el nom d'un host.
Utilitzar la funció *ping* per conèixer el l'adreça IP d'un host.
Utilitzar la funció *nslookup* per obtenir informació del servidor de DNS.
Utilitzar la funció *netstat –r* o *netstat –nr* per conèixer la taula d'encaminament del host.
Utilitzar la funció *netstat* i *netstat –a* per conèixer les connexions TCP/IP actives del host.
Utilitzar la funció *netstat –s* per obtenir informació dels missatges ICMP que circulen pel host.
Utilitzar la funcio *tracert* per descobrir el camí que seguiria un paquet IP fins al destí

4.10. IP versió 6

Conceptes generals sobre IP versió 6

Problemes en l'adreçament → IPng (next generation) IP versió 6

IPv6 es troba definit a RFC 1883, RFC 2460

Millores respecte a la versió 4:

- Més capacitat d'adreces: 32 bits → 128 bits
- Format de capçalera simplificat: camps no necessaris o redundants
- Facilita la configuració i la localització de routers
- Millors extensions i opcions
- Concepte de tipus de trànsit
- Seguretat: autenticació, integritat, confidencialitat

Format del paquet IP versió 6

Format més simple

- No hi ha checksum
  - La protecció la fan els protocols inferiors i superiors
  - S'assumeix que l'enllaç és "bo" (fibra, etc)
- S'elimina la fragmentació
  - Per fer més eficient el protocol
  - En cas necessari es fa a la font.
- Les opcions no estan incloses
  - Extensió de capçaleres

4.10. IP versió 6

Format del paquet IP versió 6

4.10. IP versió 6

Format la capçalera IP versió 6

Versió (4 bits)
- Identifica la versió

Prioritat (4 bits)
- Ordena prioritat del trànsit
- Dos tipus de trànsit
  - 0-7 aplicacions que permeten control de congestió (per ex. TCP)
  - 8-15 aplicacions que no suporten control de congestió
    - La xarxa els pot descartar sense afectar la integritat de la informació

Format la capçalera IP versió 6

Valors de la prioritat (més alt ⇒ més prioritari)

- 0 Trànsit sense caracteritzar
- 1 Trànsit de farciment (news,..)
- 2 Trànsit de dades no atès (e-mail)
- 3 Reservat
- 4 Trànsit de dades atès, transferència de fitxers (NFS,FTP..)
- 5 Reservat
- 6 Trànsit interactiu (Telnet, Xwindows,..)
- 7 Trànsit de control d'Internet (encaminament, SNMP,..)

4.10. IP versió 6

Format la capçalera IP versió 6

Etiqueta de fluxos (24 bits)

- Identifica el tipus de trànsit, sempre al mateix destí
- Encaminament més ràpid (només es processa el primer paquet)
- Reserva de recursos

Longitud de la càrrega (16bits)

- Amb 16 bits ⇒ 65535 bytes
- Paquets més grans ⇒ Jumbograma
  - Definits mitjançant extensions

Next header (8 bits)

- Indica si existeix una altra capçalera, i el seu tipus

4.10. IP versió 6

Format la capçalera IP versió 6

Hop limit (8 bits)

- Mateixa funció que el TTL
- Però es tracta d'un comptador "real"

Adreces origen i destinació (128 bits)

- 665.570.793.348.866.943.898.599 adreces
  - 6,7 x 10^{23} adreces

Amb una assignació ineficient es pot disposar de 1564 adreces per m^2 (planeta Terra)

Extensió de les capçaleres IP versió 6

Per realitzar tasques més complexes (informació de fragmentació, d'encaminament) s'utilitzen capçaleres especials.

Extensió de capçaleres

- Hop by Hop: Conté opcions IP per a cada sistema en la ruta del datagrama
- Encaminament: Permet que la font encamini el datagrama, similar a IPv4
- Fragmentació: Informació de fragmentació que envia la font al destí. Els nodes intermitjos no fragmenten
- Dades encriptades: Assegura que el datagrama no ha estat alterat durant la transmissió
- Autenticació: Informació d'autenticació de l'origen
- Opcions de destí: Dos tipus de capçaleres per definir

4.10. IP versió 6

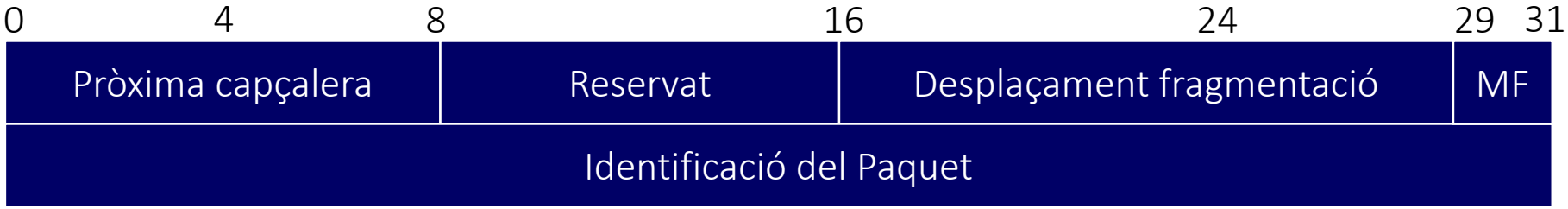
Extensió de capçalera: Fragmentació

Informació de fragmentació que envia la font al destí.

- Els nodes intermitjos no fragmenten, la fragmentació està restringida a la font.
- Procés de path MTU discovery previ a enviar el paquet, per fer una fragmentació d'extrem a extrem.

Cada fragment ha de ser un múltiple de 8 bytes.

El bit MF indica si hi ha més fragments



Extensió de capçalera: Fragmentació

Identificador de paquet

- Identificar els fragments que pertanyen a un paquet
  - Identificador de 32 bits per adaptar-se a les xarxes d'alta velocitat.

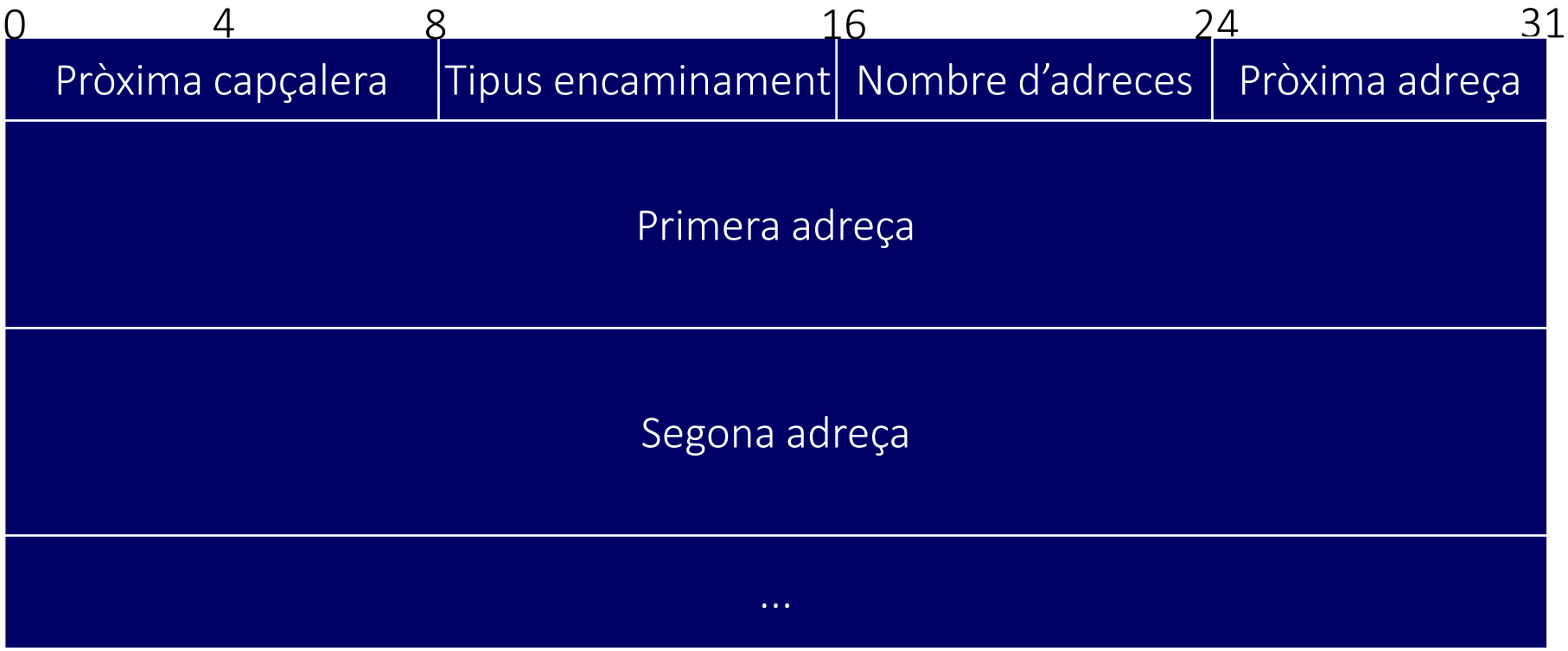
Què passa si hi ha un canvi de ruta?

- Si canvia el *path MTU,* el router que hagi d'aplicar fragmentació realitza un tuner IPv6 sobre IPv6 per transportar els fragments del paquet original.

4.10. IP versió 6

Extensió de capçalera: Encaminament d'origen

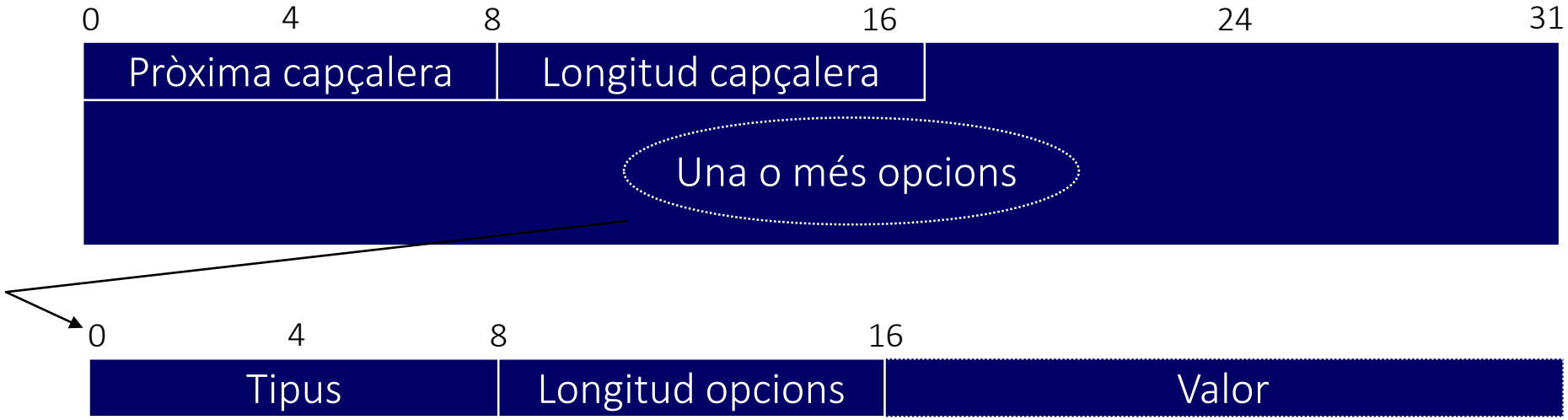
És similar a les opcions d'encaminament d'origen de IPv4.



Extensió de capçalera: Opcions de l'IPv6

Es defineixen 2 extensions de capçalera addicionals per adaptar-se a qualsevol tipus d'informació no inclosa en les capçaleres d'informació ja definides.

- Hop by hop Extension Header: opcions interpretades a cada salt.
- End to End Extension Header: opcions interpretades a l'extrem final



4.11. IPsec

IP Security Protocol

- Permet una comunicació segura entre serveis i aplicacions basats en IP.
- Cal modificar la pila IPv4 per integrar-lo
- Està incorporat per defecte a IPv6.
- Prestacions
  - Autenticació/integritat
  - Confidencialitat
  - Gestió de claus
  - Control d'accés
  - Antirepetició
  - Compressió

4.11. IPsec

IPSec és l'estàndard de comunicació segura a nivell 3

- Desenvolupat pel grup de treball Seguretat d'IP de l'IETF
- Estàndard d'Internet des de 1998-99
- RFCs
  - RFC 2401, "Security Architecture for the Internet Protocol"
  - RFC 2402, "IP Authentication Header"
  - RFC 2406, "IP Encapsulating Security Payload"
  - RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP"

4.11. IPsec

Característiques

- Transparent a les aplicacions
  - APIs TCP/UDP no es modifiquen
- Transparent als usuaris
  - No cal que tinguin coneixements de seguretat
- IPSec pot implementar-se en un *firewall* o *router*
  - S'assegura tot el tràfic que crua el perímetre
  - No cal canviar el *programari:* la conversió la realizen el *firewall* o el *router.*
- *Aplicacions*
  - *Virtual Private Networks* (VPN) a Internet
  - Accés remot segur a Internet

4.11. IPsec

Característiques

Aplicable entre:

- 2 hosts: seguretat entre màquines
- 2 routers: protegir un enllaç de la xarxa
- 1 host i un router: accés segur

2 modes de funcionament

- Transport: idem IP però amb funcions de seguretat
- Túnel: es converteix en una opció per a fer VPNs

És flexible i extensible

- No defineix completament les especificacions dels algoritmes a utilitzar
- Permet triar entre diferents opcions i incorporar-ne de noves

4.11. IPsec

Protocols que s'utilitzen

Protocols de seguretat de tràfic

- *Authentication Header* (AH)
  - Garanteix integritat, autenticació i detecció de duplicats
- *Encapsulating Security Payload* (ESP)
  - Proporciona confidencialitat (xifrat) i pot autnticar

Protocols de gerstió de claus (IKE)

- *Internet Security Association and Key Management Protocol* (*ISAKMP)*
  - Per a la gestió de asociacions de seguretat
- *Oakley*
  - Per a la generació i gestió de claus

AH/ESP s'apliquen per cada paquet independent.

4.11. IPsec

Associacions de Seguretat (SA)

- IPSec es basa en el concepte d'Associacions de Seguretat
  - Estableixen tota la informació necessària per a la comunicació segura entre dos dispositius
  - Son relacions unidireccionals entre emissor i receptor
  - Per a comunicacions bidireccionals calen dos SAs
- Cada SA s'identifica per:
  - *Security Parameter Index* (SPI)
    - Cadena de bits que actua com a identificador local
  - Adreça IP del destinatari
  - Identificador del protocol de seguretat (AH/ESP)

Associacions de Seguretat (SA)

- *Security Association Database* (SADB)
  - Base de dades que conté els paràmetres de les SA.
  - Defineix els paràmetres associats a cada SA.
  - Tot node IPSec en té una.
  - Són possibles diferents implementacions
- Funcionamient
  - El transmissor:
    - A l'enviar un paquet, consulta la SA en la seva SADB, el processa i incorpora el SPI
  - El receptor:
    - Analitza l'adreça destí i el SPI, consulta la corresponent SA en el seu SADB i el processa

4.11. IPsec

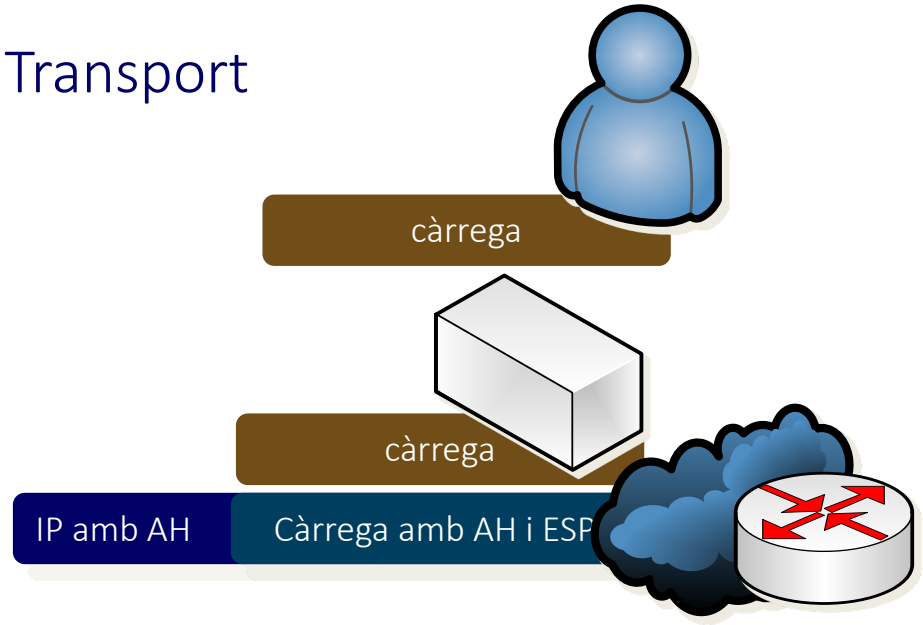
Paràmetres de les SA

- SA l*ifetype* i *lifetime*
  - Tipus d'unitats (segons o kilobytes) i el TTL de la SA
- *Group description*
  - El grup Oakley utilizat en la negociació de claus
- *Encapsulation mode*
  - Túnel o transport
- *Authentication Algorithm*
- *Key Length and rounds*
- *ESP Information*
  - Algorismes de xifrat, claus, temps de vida de claus, ...
- *Sequence Number Counter*, Sequence Number Overflow, *Anti-Replay Window*
  - Mecanismes d'anti-repetició

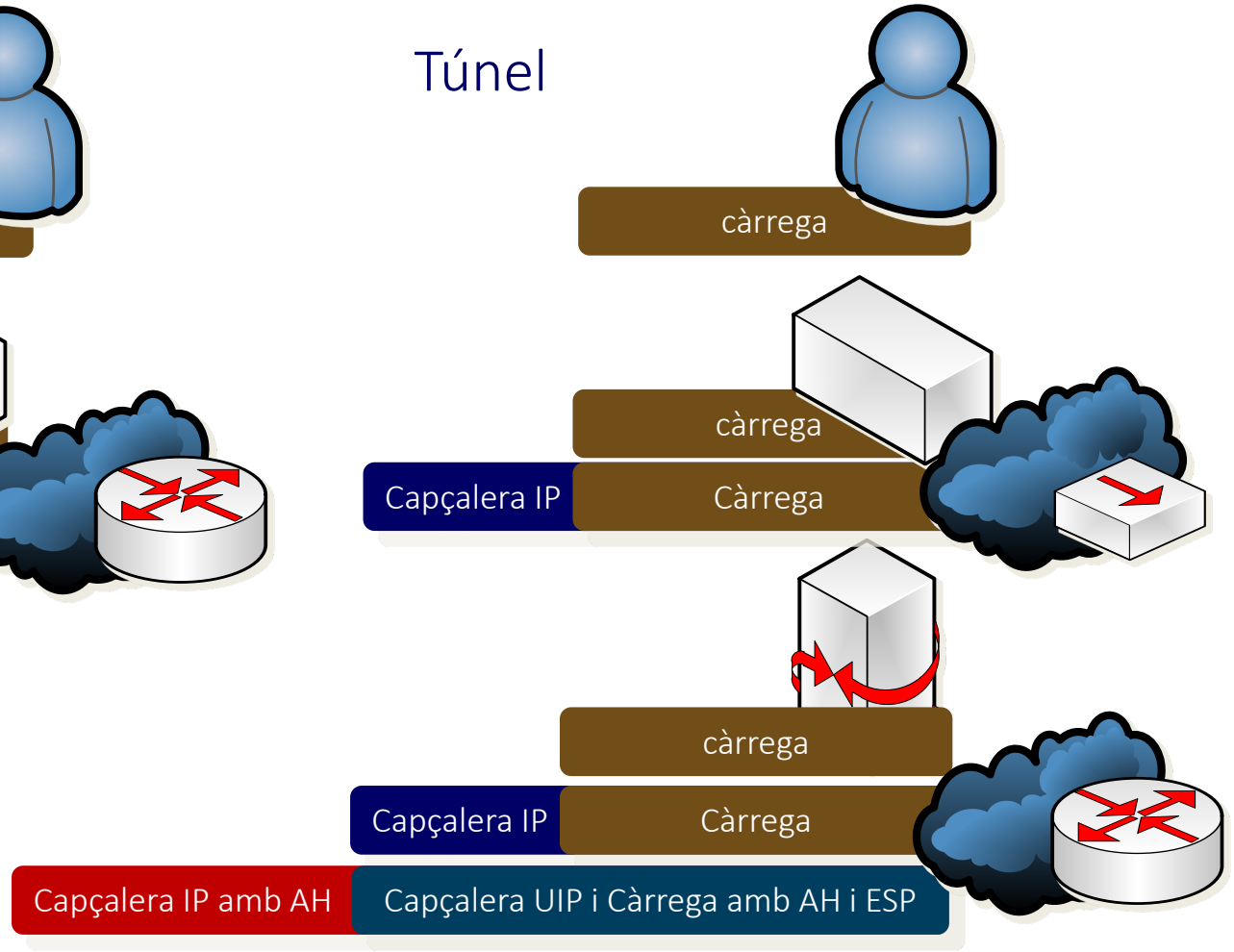
4.11. IPsec

Modes de funcionament

Transport



Túnel



Mode transport

Proporciona protecció

- Als protocols de la capa superior
  - Es a dir, a la càrrega dels paquets IP
- Tota la comunicació és segura (xifrada i/o autenticada)
  - Els equips entremitjos no poden desxifrar els paquets

S'aplica normalment en comunicacions extrem a extrem entre equips finals

Abans de que s'afegeixi la capçalera IP al paquet, s'afegeixen les de seguretat

AH autentica la carrega IP i parts de la capçalera IP

ESP xifra, i autentica opcionalment, la càrrega IP, la capçalera IP no està protegida

Mode túnel

Protegeix el paquet IP sencer

S'aplica normalment en comunicacions entre gateways

- Per a protegir datagrames generats o destinats a sistemes no-IPSec (com amb VPNs).
- S'aplica quan la capçalera IP extrem a extrem jaa s'ha adjuntat al paquet

Funcionament

- Les capçaleres AH/ESP s'afegeixen al paquet IP
- Tot el paquet es tracta com si fos la càrrega d'un nou paquet amb una nova capçalera IP

Els paquets viatgen a través d'un túnel

- Els routers del camí no són capaços d'examinar el paquet original

4.12. Conclusions

Conclusions sobre IP i ICMP

Protocol IP

- Protocol de nivell de xarxa, encamina i lliura informació entre màquines de xarxes diferents.
- Unitat d'info: datagrama IP (una capçalera i un camp de dades).
- No orientat a connexió i ofereix un servei *Best effort*, la fiabilitat la proporcionen els nivells superiors.
- Utilitza la màscara de subxarxa i taules d'encaminament per l'establiment de rutes.
- Degut a les MTU apareix fragmentació i reensamblament

Protocol ICMP

- Part d'IP que proporciona funcions de control, però no fa el protocol IP més fiable, només notifica errors a la màquina origen.
- Els missatges ICMP viatgen en el camp de dades del protocol IP, però no és un protocol d'alt nivell.

Protocol IPSec incorporar seguretat a IP