4. Entrega

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

Dr. Daniel Guasch Murillo

Enero de 2022

4. Entrega

4.1. Protocolo de internet

4.1. Características básicas de IP

Filosofía de trabajo del protocolo IP

- Protocolo de nivel de red
- Se debe poder utilizar en cualquier host, router, red
- Debe permitir crecer la red sin interrumpir el servicio
- Debe admitir sesiones de nivel superior y servicios orientados a mensajes

4.1. Características básicas de IP

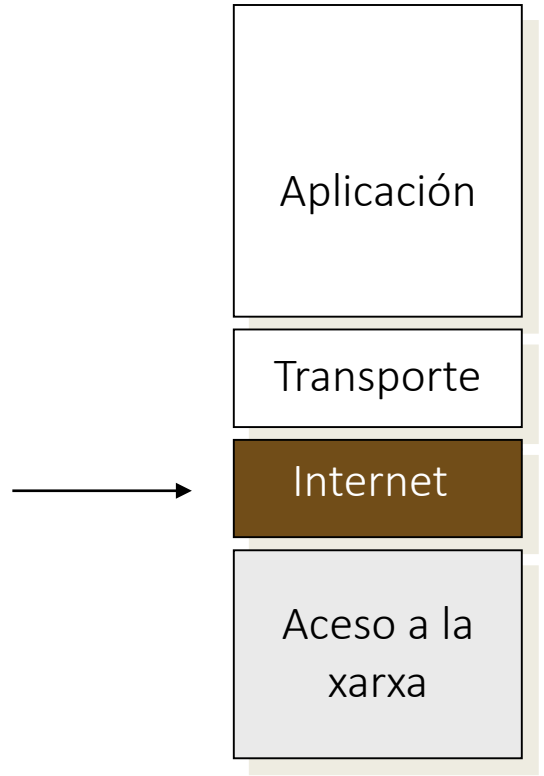
IP (Internet Protocol), RFC791

Es la base para los protocolos de la familia TCP/IP

IP ofrece:

- enlace entre redes.
- encaminamiento (Routing) y libremente de información entre máquinas de redes diferentes.

servicio de envío de paquetes sin conexión



Datagrama

- Unidad mínima de transferencia (PDU)

4.1. Características básicas de IP

Características del servicio

No orientado a conexión

- Cada datagrama se transmite de forma independiente.

Servicio sin fiabilidad

- No se garantiza que los paquetes lleguen correctamente
- Se pueden producir:
  - Perdidas, duplicados, desorden, ...

Servicio *Best effort* (se hará el mejor que se pueda).

La fiabilidad la proporcionan los niveles superiores.

Proporciona algunas funciones de control:

- Mediante ICMP (Internet Control message protocolo)

4.1. Características básicas de IP

Datagrama IP

El datagrama está formado por una cabecera y un campo de datos:

- La cabecera contiene :
  - Las direcciones IP del origen y del destino.
  - I otra información de control.
- El campo de datos contiene la información del protocolo superior

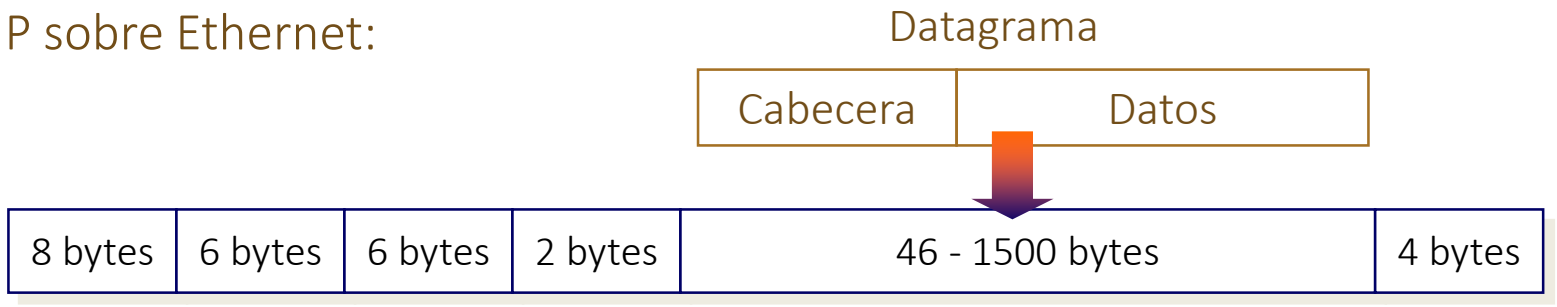
Datagrama IP

4.1. Características básicas de IP

Encapsulamiento IP

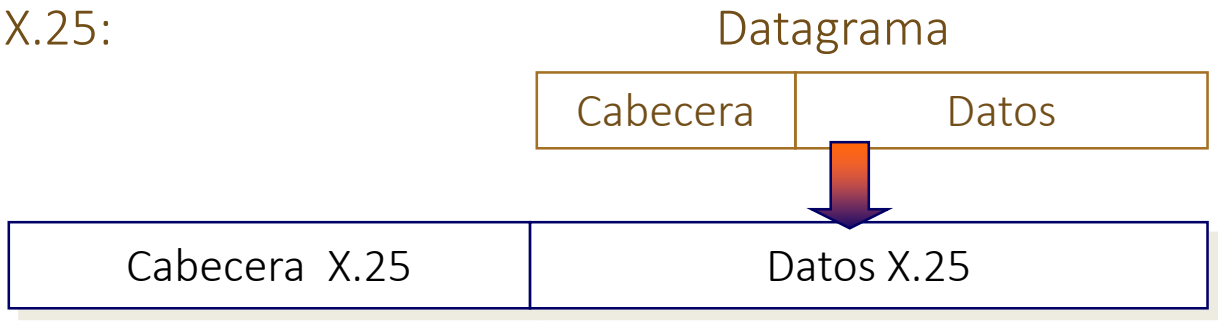
Los paquetes IP se transmiten dentro del campo de datos de una trama de nivel de enlace:

IP sobre Ethernet:



Hay casos especiales en que se transportan paquetes IP en otros niveles:

IP sobre X.25:

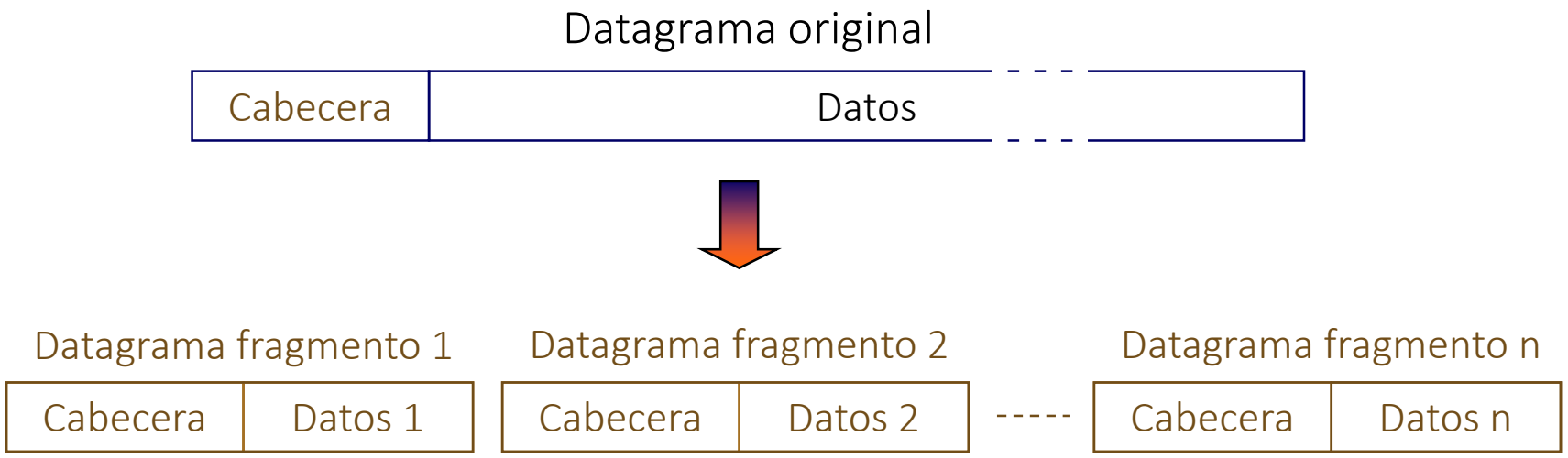


4.1. Características básicas de IP

Fragmentación de datagrames IP

La longitud del datagrama puede que sea superior a la capacidad del campo de datos de la trama física:

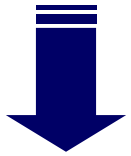
Hay que fragmentar el datagrama IP



4.2. Función de encaminamiento IP

Características del servicio

La función principal de IP es aceptar datos de TCP o UDP, crear los datagramas necesarios, encaminarlos por la red y entregarlos a la destinación correcta



Utiliza dos herramientas

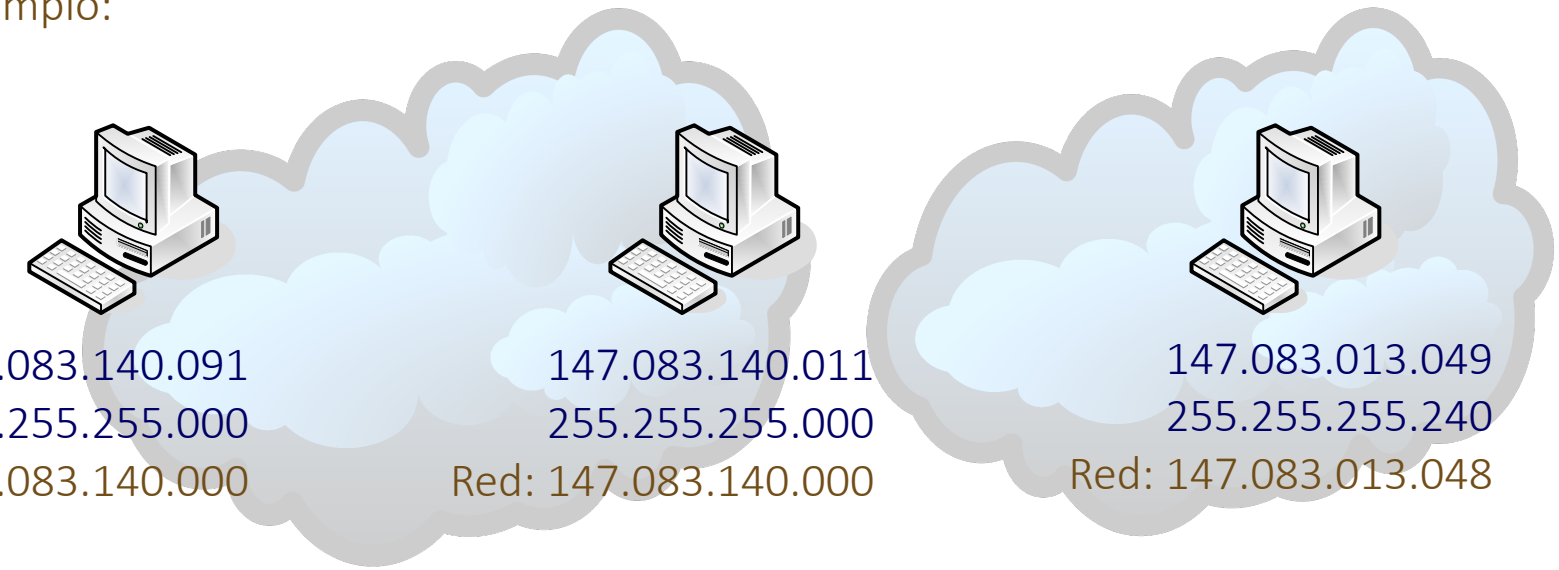
Máscara de subred
Tablas de encaminamiento IP

4.2. Función de encaminamiento IP

Máscara de subred

Mediante la máscara de subred, IP analiza si la dirección destino pertenece a la misma red que la dirección origen

Por ejemplo:



4.2. Función de encaminamiento IP

Tabla de encaminamiento

Indica a IP como dirigir los datagramas hacia sistemas que no se encuentran en su red

Concepto

- No describen el camino completo hasta el destino.
- A IP solo le hace falta conocer la dirección del siguiente salto y enviar el datagrama.
- IP solo define la estructura de la tabla, no la su gestión.
- La gestión de las tablas de encaminamiento es responsabilidad de los protocolos de encaminamiento.

4.2. Función de encaminamiento IP

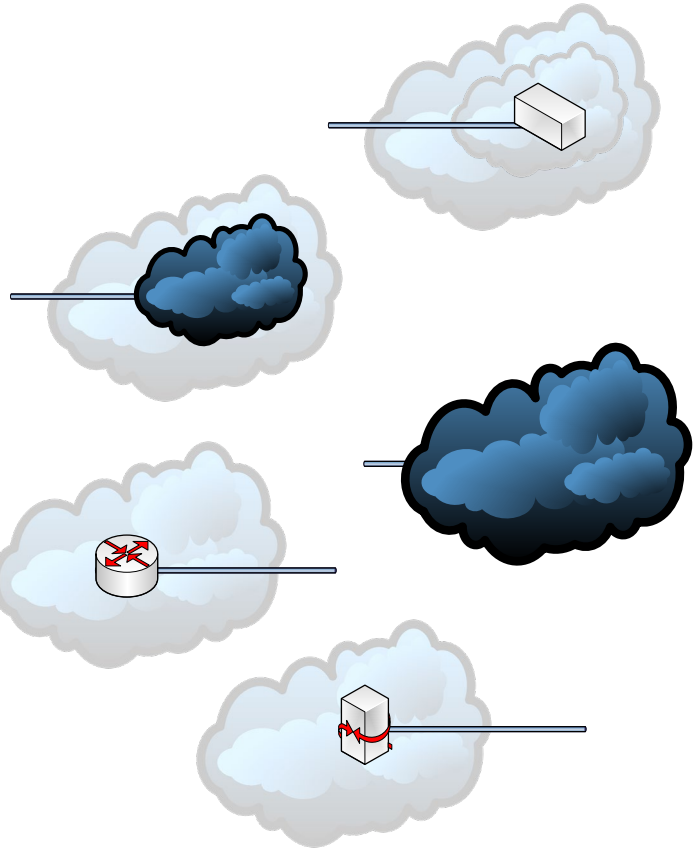
Características de les tablas de encaminamiento

- Toda estación de una red tiene una tabla de encaminamiento
- Las tablas de un host son muy simples
- Como mínimo deben incluir la entrada: *default n.n.n.n*
- Las tablas de los routers son complejas y se gestionan según dos filosofías:
  - Vector de distancia: tiene en cuenta el número y tipo de saltos a realizar
  - Estado del enlace: crea un mapa de la red y evalúa dinámicamente el camino

4.2. Función de encaminamiento IP

Reglas de búsqueda en las tablas de encaminamiento

1. Se busca una entrada que coincida con la dirección IP destino
2. Se busca una entrada que corresponda a la subred de destino
3. Se busca una entrada que corresponda a la red de destino
4. Se busca una entrada que corresponda a un router
5. Se utiliza el gateway por defecto.



4.2. Función de encaminamiento IP

Tipo de rutas

Ruta estática:

- Aquellas que están predeterminadas de forma fija. Tienen poca flexibilidad pero generan poco tráfico de encaminamiento.

Ruta per defecto:

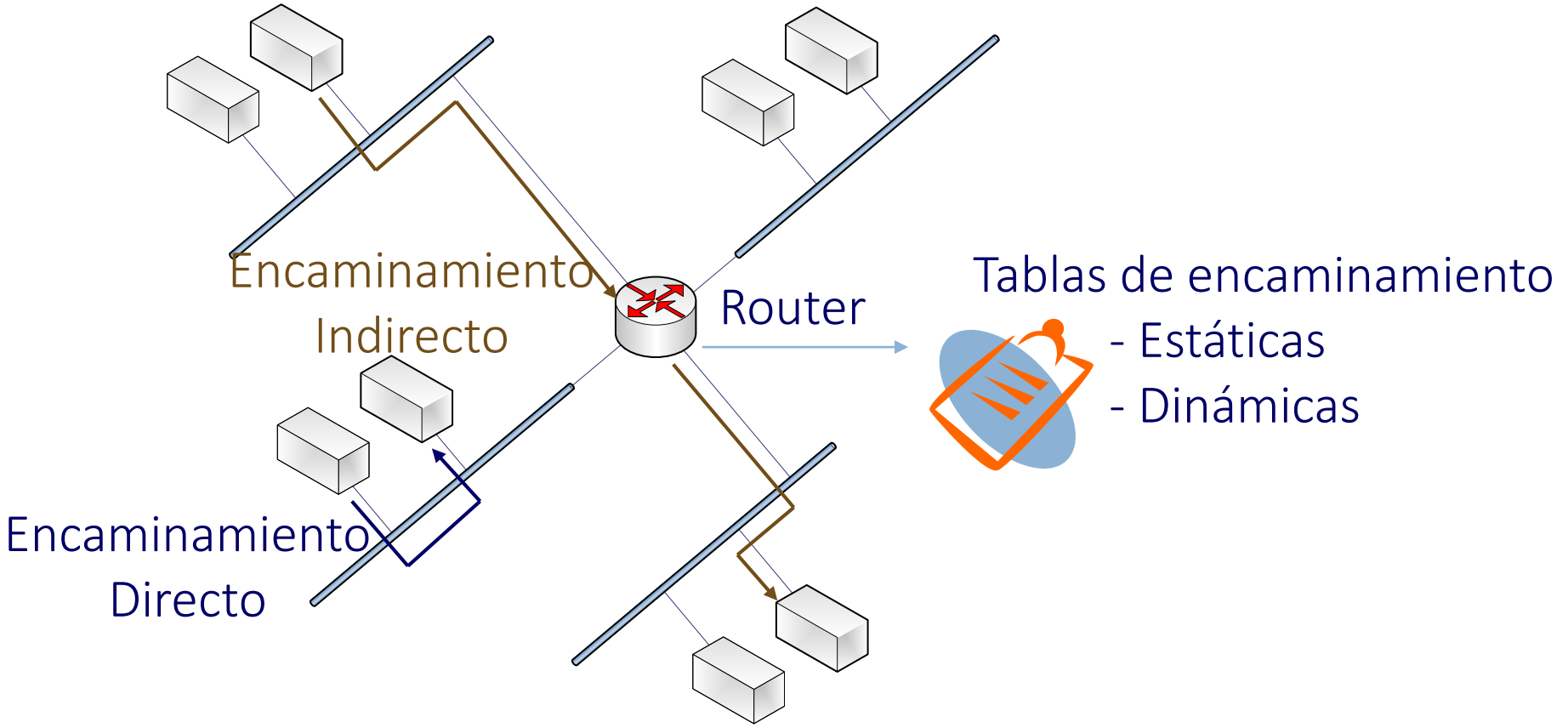
- Resultaría poco práctico que un router conociera todas las redes existentes. La ruta por defecto indica una ruta por donde saldrán todos los paquetes cuando no se indica una ruta específica para un destino concreto.

Ruta dinámica:

- Son rutas establecidas según determinadas variables de la red (distancia hasta al destino, coste del camino, utilización de los enlaces, etc.). Se utilizan unos protocolos específicos para realizar el intercambio de información de las tablas de encaminamiento y el cálculo de las rutas más adecuadas para cada destino.

4.3. Tipo de encaminamiento IP

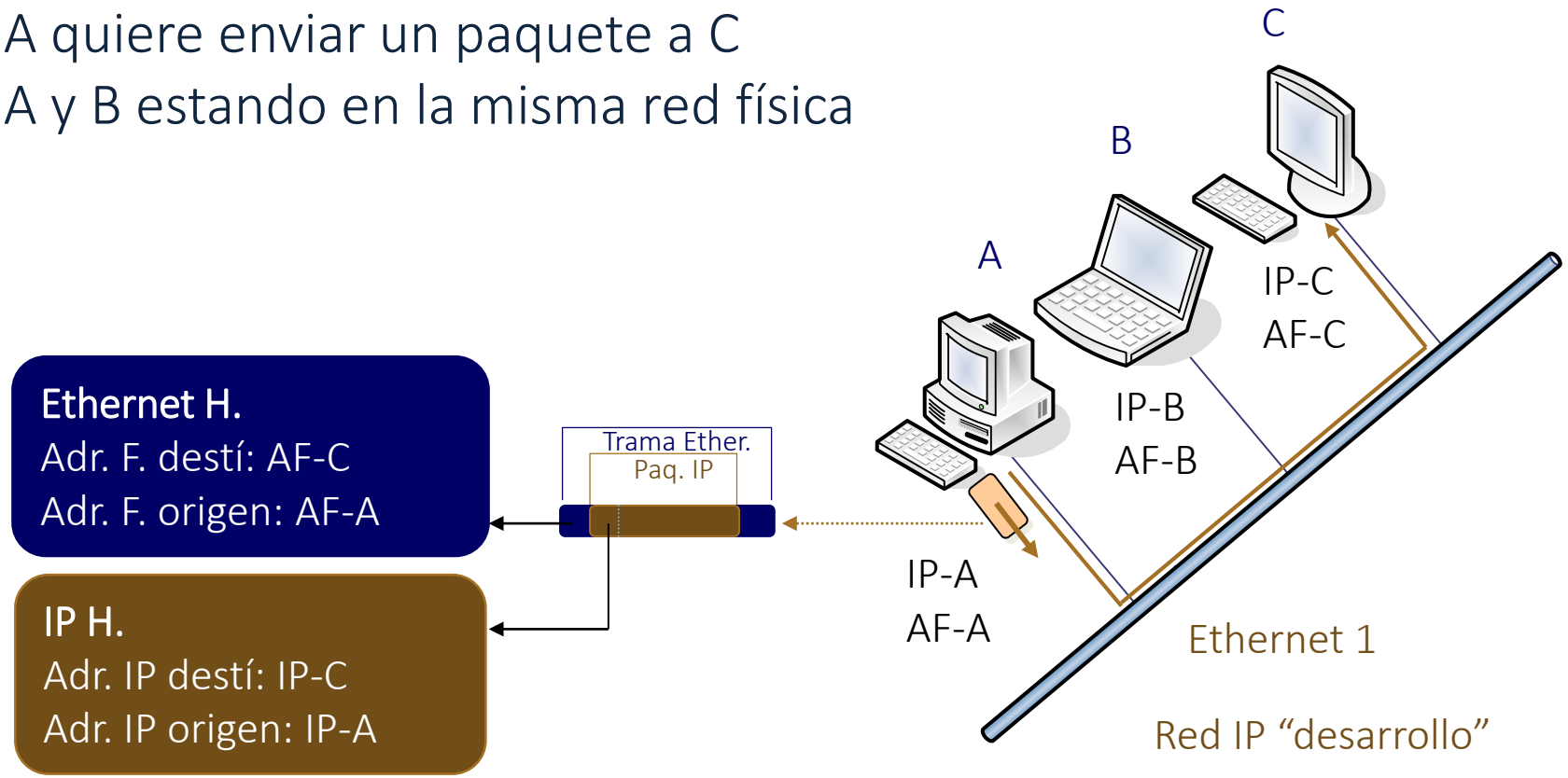
Encaminamiento directo/indirecto y estático/dinámico



4.3. Tipo de encaminamiento IP

Funcionamiento del encaminamiento directo

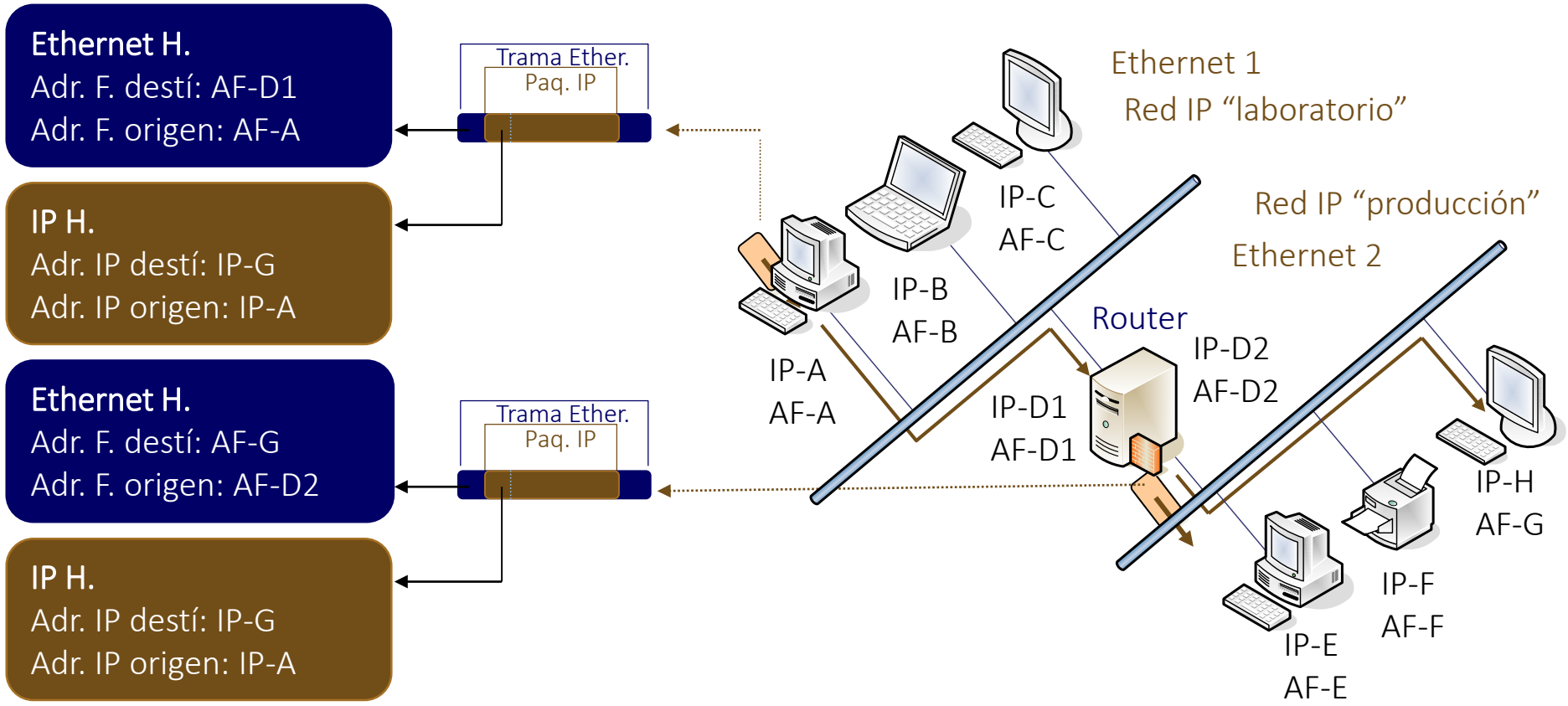
- A quiere enviar un paquete a C
- A y B estando en la misma red física



4.3. Tipo de encaminamiento IP

Funcionamiento del encaminamiento indirecto

- A quiere enviar un paquete a H.
- A y H estando en redes físicas diferentes.



4.4. Fragmentación de datagramas IP

Conceptos básicos

MTU (Maximum Transmission Unit)

- La trama tiene una longitud máx. de datos: MTU
- Depende de la red:

Xarxa física	MTU
Ethernet	1500 bytes
IEEE 802.3	1492 bytes
IEEE 802.5	màx. 4464 bytes
X.25	1600 bytes (puede variar por diferentes X.25)
FDDI	4352 bytes
Frame Relay	com a mínim 1600 bytes (normalmente)
ATM	9180 bytes (por defecto), màx. 16K - 1

Fragmentación:

- Cuando el paquete tiene una longitud mayor que la MTU
- El paquete se divide en paquetes con longitud ≤ MTU

4.4. Fragmentación de datagramas IP

Conceptos básicos

La fragmentación modifica las prestaciones:

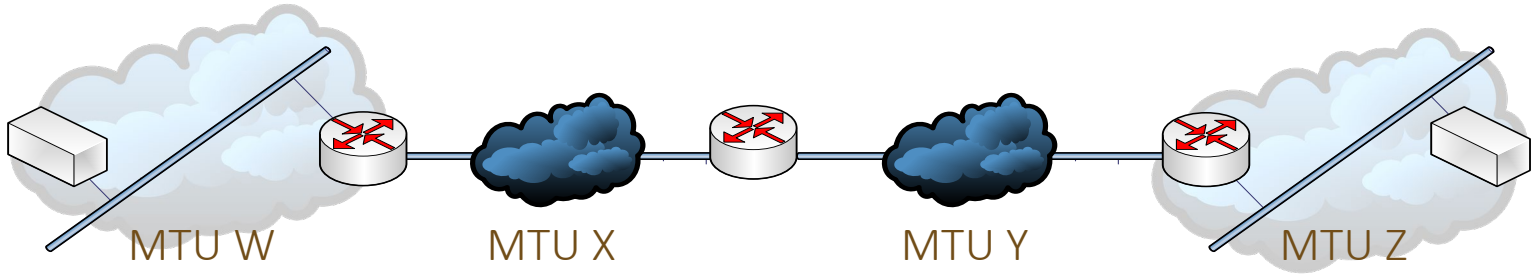
- Máxima longitud en el origen → Mucha fragmentación.
- Longitud de MTU para no fragmentar → Se pierde eficiencia.

Path MTU:

- La MTU de una ruta es la MTU máxima que no provoca fragmentación.

Mecanismo para averiguar el Path MTU:

- Path MTU discovery **(RFC 1191)**, basado en mensajes ICMP.

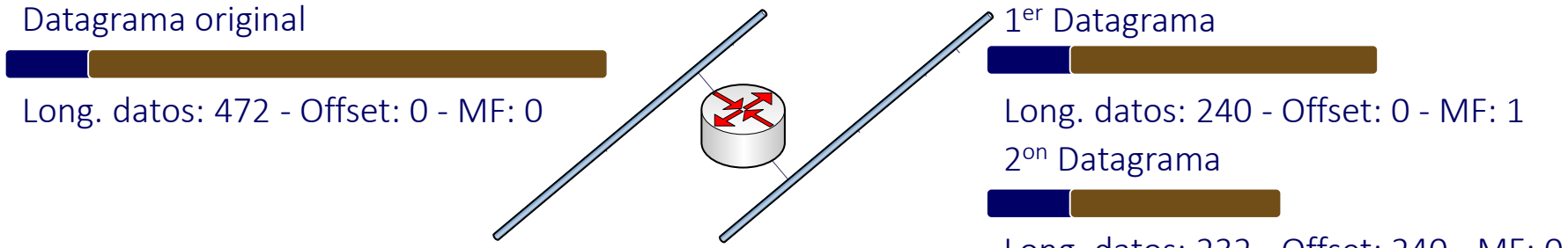


4.5. Fragmentación de datagramas IP

Proceso de fragmentación

Cuando un gateway fragmenta un datagrama hace los pasos:

- Se crean dos datagramas y se copia la cabecera en los dos
- Se divide el campo de datos en bloques múltiples de byte
- Se cargan los bloques de datos en los respectivos datagramas
- Se actualiza el campo "longitud del datagrama"
- Se actualiza el flag "MF" del primer fragmento: se pone a 1
- Se modifica el Offset del segundo datagrama



4.5. Fragmentación de datagramas IP

Reensamblamiento de los datagramas IP

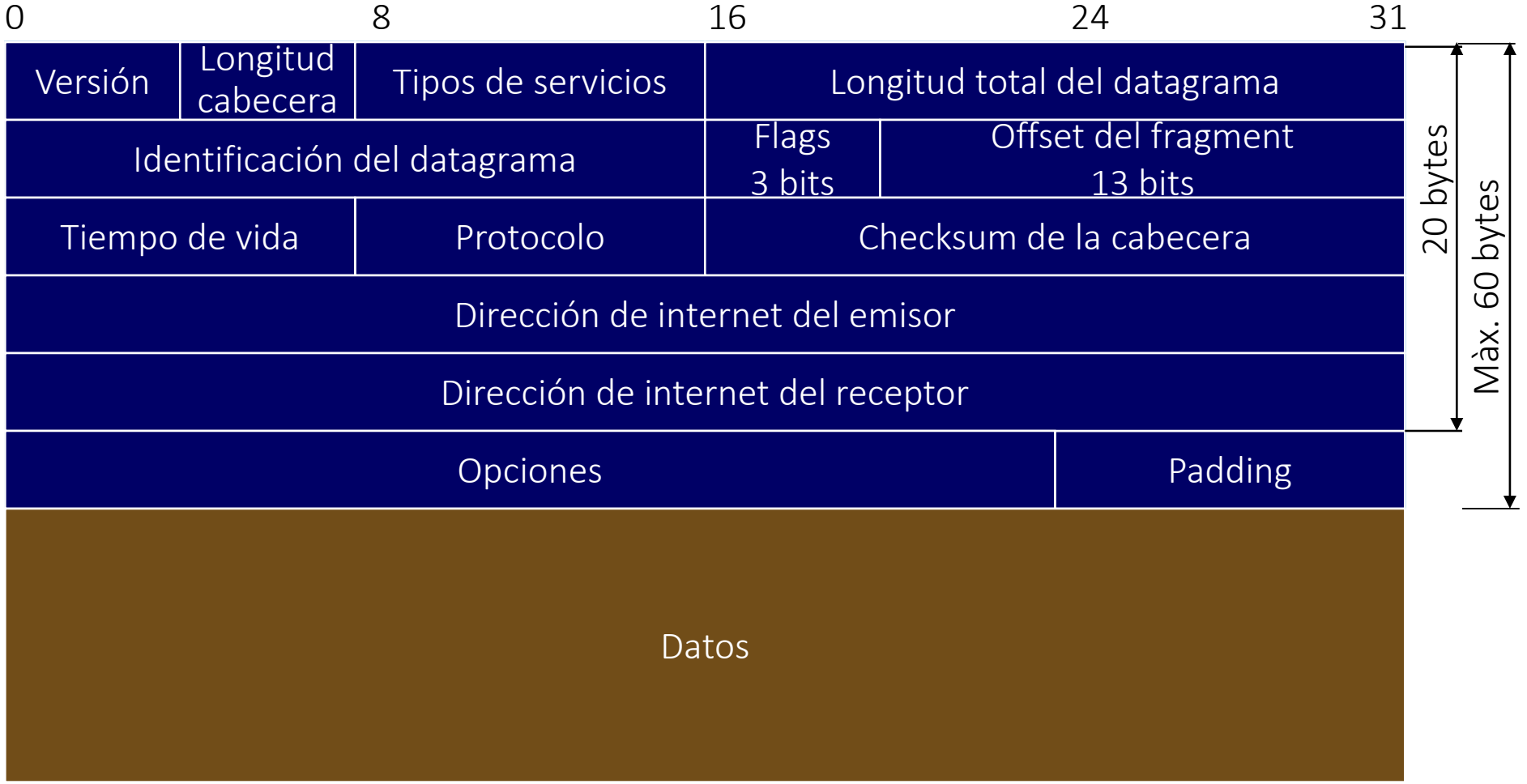
- Los fragmentos que tienen el mismo Identificador, dirección IP origen y destino, y protocolo perteneciente al mismo paquete.
- La fragmentación se puede dar en cualquier punto de la red.
- El reensamblamiento únicamente se hace en el destino.

- Problemas:
- Se desconoce el tamaño total del paquete original.
  - Memoria disponible en los router.
- Perdida de un fragmento

Se activa un temporizador cuando llega uno de los fragmentos. Si el temporizador llega a 0 y no han llegado todos los fragmentos, se descartan los fragmentos recibidos y se envía un mensaje de error.

4.6. Formato del datagrama IP

Estructura del datagrama



4.6. Formato del datagrama IP

Campos “Versión” y “longitud cabecera” del datagrama

Versión (4 bits)

- Versión del protocolo IP, para asegurar que el paquete se interpreta correctamente. Normalmente es 4, y para la nueva versión es 6.

Longitud cabecera (4 bits)

- Número de palabras de 32 bits de la cabecera, incluyendo las opciones.
- Si no hay opciones vale 5: la cabecera mínima es de 20 bytes.
- La longitud máxima de cabecera es de 60 bytes.

4.6. Formato del datagrama IP

Campo “tipo de servicio” del datagrama

Tipo de servicio (Type of Service) (8 bits)

- Especifica como hay que tratar el datagrama.
- Definidos en RFC 791

- **Precedencia**: Importancia o prioridad del paquete (8 niveles)
- **D T R M**: tipo de transporte que se desea (2 niveles):

D = 1 (poco retardo) T = 1 (caudal alto) ,

R = 1 (fiabilidad alta) M = 1 (coste económico bajo)

4.6. Formato del datagrama IP

campo “tipo de servicio” del datagrama

Significado de los bits de TOS (Type Of Service)

DTRM		DTRM	
0 0 0 0	Defecto	0 1 0 0	Maximiza cabal
0 0 0 1	Minimiza coste monetario	1 0 0 0	Minimiza retardo
0 0 1 0	Maximiza fiabilidad	1 1 1 1	Maximiza seguridad

Ejemplos del uso de los 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. Formato del datagrama IP

Campos “Longitud total” y “Identificador” del datagrama

Longitud total del datagrama (16 bits)

- Longitud total del datagrama, cabecera + datos, en bytes.
  Longitud máxima 2^{16} = 65.535 Bytes
  - Pero en Ethernet: 1500 Bytes,
  - En IEEE 802.3: 1492 Bytes
  - o en ATM: 9180 Bytes, máx. 16KB - 1

Identificador del datagrama (16 bits)

- Nº de 16 bits que identifica el datagrama. Se asigna secuencialmente.
  - Para controlar las duplicaciones.
  - Para facilitar el reensamblamiento de los fragmentos de un datagrama.
- Si el datagrama se fragmenta, todos los fragmentos tendrán el identificador del original.

4.6. Formato del datagrama IP

Campos “Flags” y “Offset del fragmento” del datagrama

Flags (3 bits)

- R: bit reservado.
- DF: No fragmentar. El datagrama no puede ser fragmentado.
  - Si fuera necesario fragmentarlo, se descartaría.
- MF: Siguen fragmentos. No es el ultimo fragmento del paquete.

Offset del fragmento (13 bits)

- Permite ordenar los fragmentos.
- Indica la posición del fragmento dentro del datagrama original.
- Se da en unidades de 64 bits (8 bytes).
- Excepto el ultimo, los fragmentos tienen una longitud múltiple de 8 bytes.

4.6. Formato del datagrama IP

Campos de direcciones y “Tiempo de vida” del datagrama

Dirección de Internet del emisor (32 bits)

- Dirección origen del paquete.

Dirección de Internet del receptor (32 bits)

- Dirección destino del paquete.

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

- Especifica el tiempo que el paquete puede permanecer circulando por la red.
- Se da en unidades de segundos (a la práctica será un límite máx. de la vida de un paquete).
- Se decrementa una unidad (para simplificar) cada vez que pasa un router:
  - cuando llega a 0 se tira el paquete.
- Lo inicializa el emisor (normalmente, a 32 o a 64).

4.6. Formato del datagrama IP

Campo de “protocolo” del datagrama

Protocolo (8 bits)

- Indica el protocolo del nivel superior que se transporta en el campo de datos.
- Se Codifica con un valor asignado 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. Formato del datagrama IP

Campo de “Checksum de la cabecera” del datagrama

Checksum de la cabecera (16 bits)

- Verificación de errores de la cabecera (no de los datos).
- Se recalcula en cada router.
- Para calcularlo, en el emisor: (RFC1624)
  - Se pone a 0 el campo Checksum
  - Se calcula la suma: complemento a 1 de la suma en complemento a 1 de 16 bits de toda la cabecera.
  - Se guarda el resultado en el campo Checksum.
- Para verificarlo, en el receptor:
  - Hace la suma complemento a 1 de toda la cabecera: Si el resultado es 0 es correcto, sino el datagrama tiene la cabecera errónea: se descarta el datagrama.

4.6. Formato del datagrama IP

Campos “Opciones” y “Padding” del datagrama

Opciones (longitud variable)

- Este campo lo llevan pocos paquetes.
- Proporcionan timestamp, seguridad y encaminamiento especial.
- Puede llevar una o más opciones.
- La estructura del campo de opciones tiene dos casos:
  - Caso 1: Un único byte de tipo de opción.
  - Caso 2: Un byte de tipo de opción, un byte de longitud de opción (medida en bytes) y los bytes de datos de la opción.
- Estructura del subcampo tipo de opción:
  - **C.F.,** Copia en fragmento (1 bit)
  - **Clase op.,** Clase de opción (2 bits)
  - **N. Opc.,** Número de opción (5 bits)

Padding: sirve para hacer la longitud de la cabecera múltiple de 32 bits.

4.6. Formato del datagrama IP

Subcampo “Identificador de la opción” del datagrama

Identificador de la opción (8 bits)

- **C.F.,** Copia en fragmento (1 bit):
  - Especifica que las opciones se deben copiar a todos los fragmentos del datagrama original.
- **Clase op.**: tipo de clase (2 bits)
  - 0 → control
  - 2 → depuración y medidas
  - 1 i 3 → uso reservado
- **N. Opc.**: Número de opción (5 bits)
  - 2 - Seguridad
  - 3 - Ruta específica por donde debe pasar el datagrama
  - 4 - Timestamp: medidas de retardos entre nodos
  - 7 - Grabar ruta por donde pasa el datagrama

4.6. Formato del datagrama IP

Subcampo “Identificador de la opción” del datagrama

Algunas opciones en función de la clase y el número:

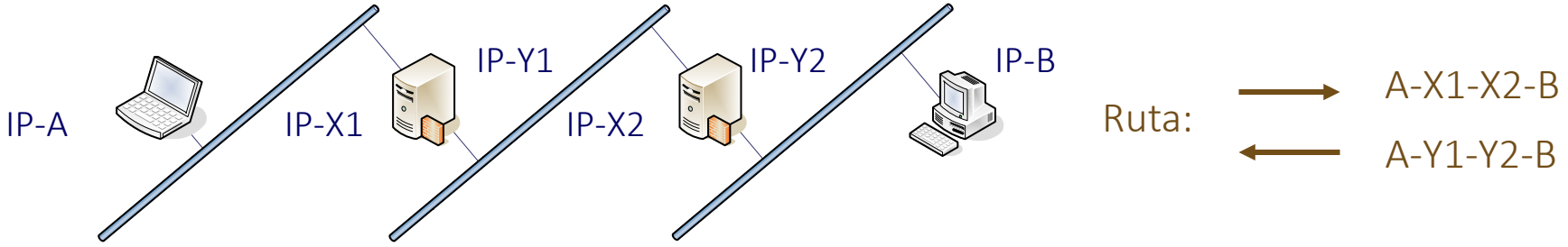
Clase	Número	Longitud	Descripción
0	0	-	Final de llista d’opcions
0	1	-	No operation (No hi ha res)
0	2	11	Security DoD IP
0	3	variable	Loose source routing
0	7	variable	Record route
0	8	4	Obsolet
0	9	variable	Strict Source Routing
2	4	variable	Timestamp

4.6. Formato del datagrama IP

Opciones de encaminamiento de fuente del datagrama

Encaminamiento de fuente:

- La ruta que deben seguir los paquetes está dada por la fuente
- Los paquetes que viajan des del destino hacia la fuente deben utilizar la misma ruta que los paquetes que van de fuente a destino.
- Tipo: Estricto (strict) y desconectado (Loose).
- Problema

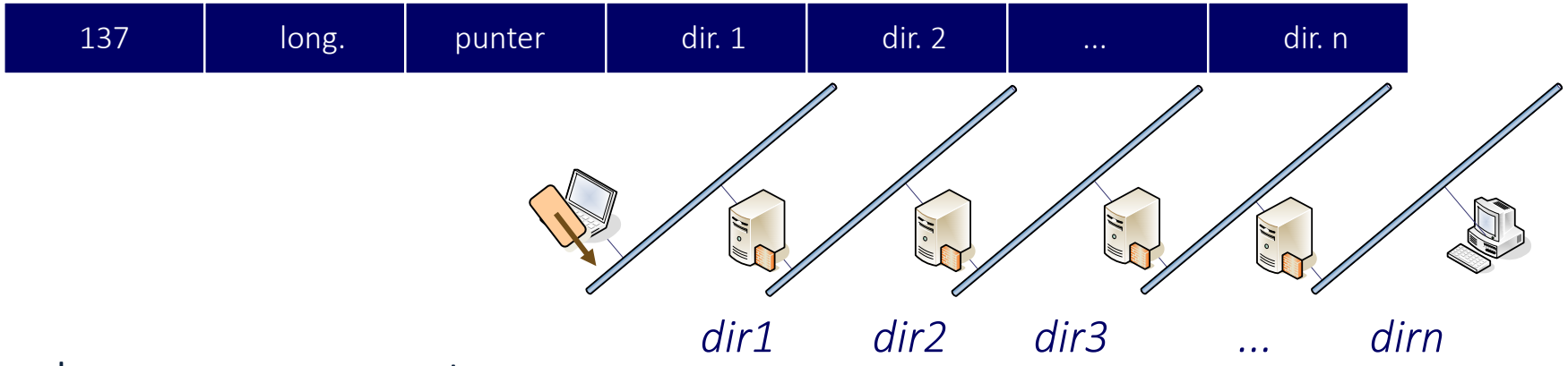


No se puede utilizar la descripción de ruta dada por A.
- Los routers modifican las direcciones de entrada por las de salida.

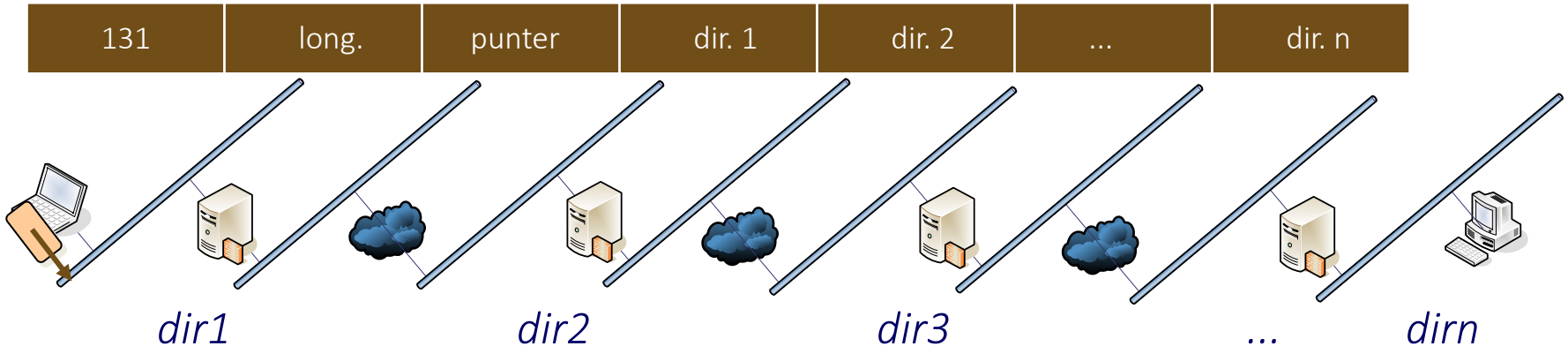
4.6. Formato del datagrama IP

Opciones de encaminamiento de fuente del datagrama

- Strict source route:



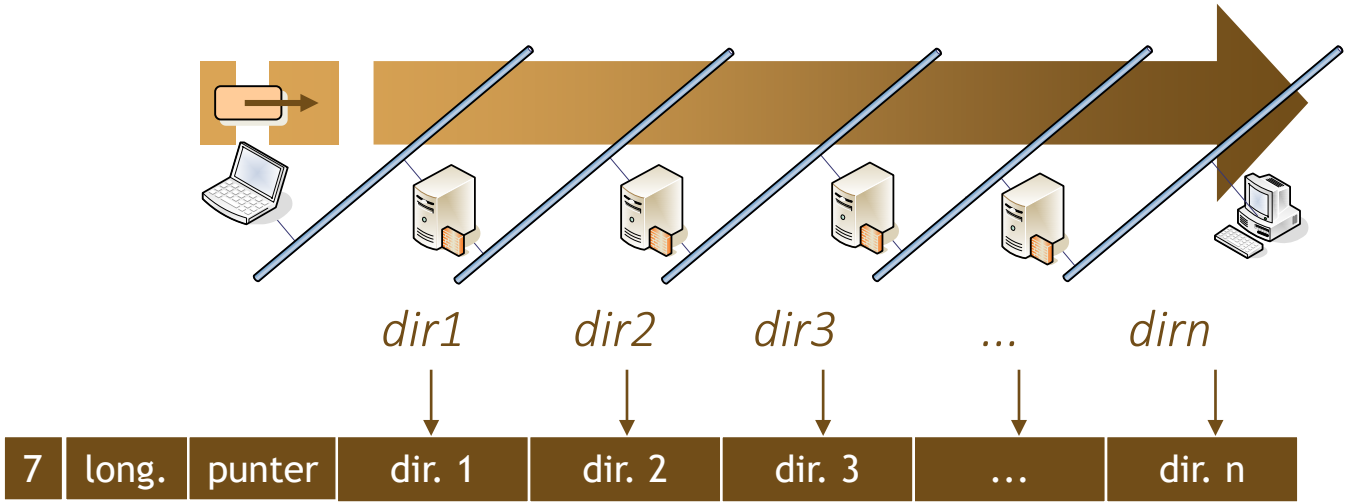
- Loose source route:



4.6. Formato del datagrama IP

Opciones de encaminamiento de fuente del datagrama

- Record route: Se van añadiendo direcciones



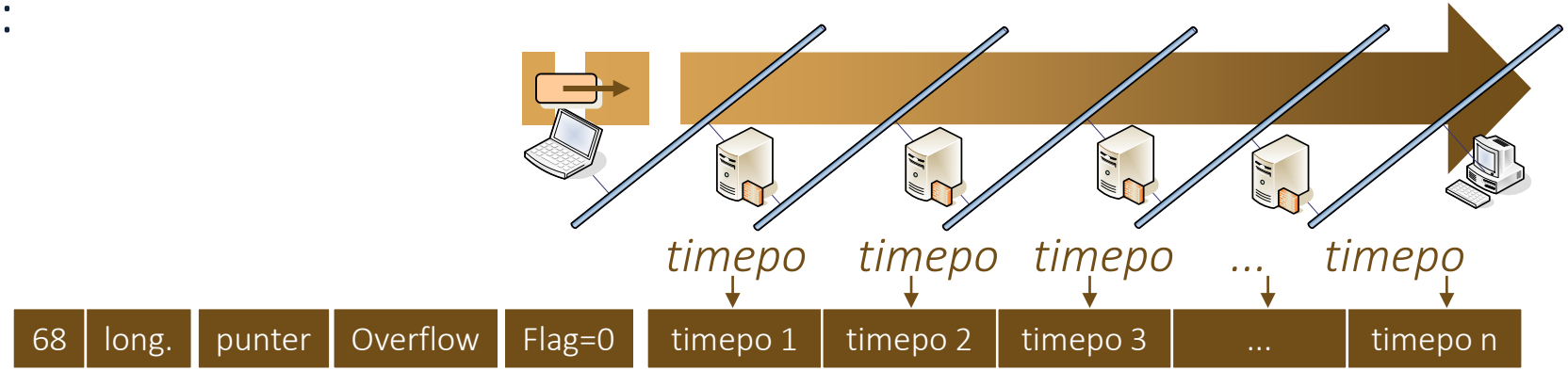
puntero (en bytes): indica la posición en la dirección. Empieza por el cuarto octeto y se incrementa en 4.

Si puntero > longitud: Se han consumido todas las direcciones y se encamina por la dirección del destino.

4.6. Formato del datagrama IP

Opciones de encaminamiento de fuente del datagrama

- Timestamp:



- Flag (4 bits): tipo de Formato

  0 → En cada salto se guarda el tiempo en el espacio reservado y se incrementa el puntero en 4.

- Overflow (4bits): es el nombre de módulos IP que no pueden registrar el timestamp por falta de espacio.

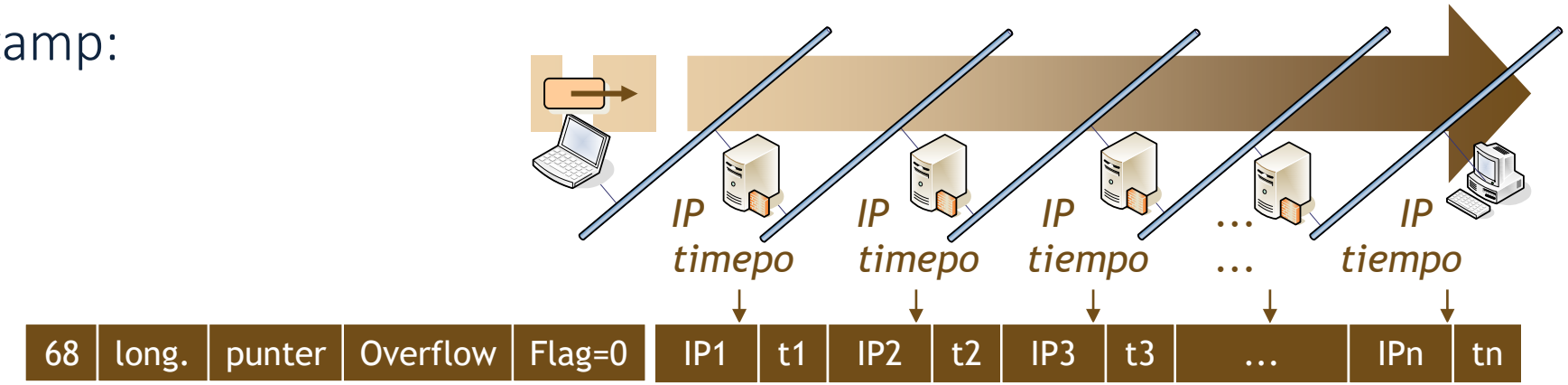
  Si se supera el espacio reservado se incrementa el campo de Overflow en 1.

  Si el campo de Overflow se agota (>15) se descarta el datagrama.

4.6. Formato del datagrama IP

Opciones de encaminamiento de fuente del datagrama

- Timestamp:



Timestamp. Flag = 1 i 3

1 → En cada salto se guarda el tiempo y la dirección del router. Se reserva espacio para los dos campos y se incrementa el puntero en 8.

3 → El origen indica en que nodos pueden grabar el tiempo. Si el router encuentra su dirección en la lista añade el timestamp.

4.7. Internet Control Message Protocol

Problemática asociada al protocolo IP

Protocol IP → No fiable
No orientdo a connexió

- Se necesita un mecanismo de control:
  - Porque un datagrama no se ha podido entregar ?
    - La máquina destino no está conectada a la red
    - El temporizador a expirado
    - Congestión en la red
  - Indicación de errores acaecidos en el tratamiento de datagramas
  - Descubrimiento de nuevas rutas
  - Un router no tiene suficiente buffer para almacenar paquetes

4.7. Internet Control Message Protocol

Fundamentos del protocolo ICMP

Inicialmente fue desarrollado porque los routers informaran de las causas de error en la Entrega de paquetes.

El protocolo ICMP no hace el protocolo IP más fiable, solo notifica errores a la máquina origen, pero no los nodos intermedios.

- La fiabilidad se consigue con los protocolos de los niveles superiores.

El mensajes ICMP de notificación de error se dirige al host origen (el que envió el paquete que provoca el error).

- Los routers intermedios no tendrán conocimiento de los errores y no podrán actuar.

Los paquetes ICMP también pueden tener errores. En este caso no se genera ningún otro paquete ICMP (para evitar recurrencia).

4.7. Internet Control Message Protocol

Encapsulamiento de los mensajes ICMP

Los mensajes ICMP viajan en el campo de datos del protocolo IP, pero no es un protocolo de alto nivel.

Normalmente se considera como una parte del nivel IP.

El destinatario es el modulo IP, no el usuario origen o destino.

Los mensajes ICMP pueden ser:

Mensajes de error (utilizados por los routers)

Mensajes de consulta (utilizados por los hosts)

4.7. Internet Control Message Protocol

Condiciones de generación de los mensajes ICMP

Un mensaje de error ICMP no se genera nunca como a respuesta a:

- Otro mensaje de error ICMP (excepto para mensajes ICMP de consulta).
- Un paquete con dirección destino de broadcast o multicast.
- Un paquete enviado como a broadcast para la capa de enlace.
- Un fragmento de un paquete (que no sea el primer caso).
- Un paquete la dirección origen del cual no define a un host único (dirección origen no puede ser 0, Loopback, broadcast o multicast).

4.8. Mensajes ICMP

Formato de los mensajes ICMP

- Tipo: tipo de mensaje ICMP. Hay 15 posibles mensajes.
- Código: Identifica alguna condición adicional para cada tipo de mensaje ICMP.
- Checksum: Para proteger el mensaje ICMP de los errores. Se calcula sobre todo el mensaje ICMP y usa el mismo algoritmo que para la cabecera IP.
- Parámetros: Parámetros del mensaje.
- información: cabecera y 8 primeros bytes del datagrama que ha provocado la generación del mensaje ICMP.

4.8. Mensajes ICMP

Tipo de mensajes ICMP

0 - Respuesta de Eco: Para testear si se puede llegar a una máquina (ping)
3 - Destino no asumible
4 - Control de flujo (source quench): una memoria se desborda
5 - Cambio de ruta: para indicar que hay una ruta mejor
8 - Petición de Eco (ping)
11 - Tiempo de datagrama agotado: rutas circulares o demasiado largas
12 - Problema en un parámetro del datagrama
13 - Petición de timestamp: control del tiempo de la ruta utilizada
14 - Respuesta de timestamp
15 - Petición de información (obsoleto)
16 - Respuesta de información (obsoleto)
17 - Petición de la máscara de subred
18 - Respuesta de la máscara de subred

4.8. Mensajes ICMP

Tratamiento de los mensajes ICMP

Destino no asumible:
- Entregar el mensaje ICMP a la capa de transporte.
- La acción siguiente dependerá de la causa de este error.

Cambio de ruta (redirect):
- El host debe actualizar la tabla de encaminamiento.

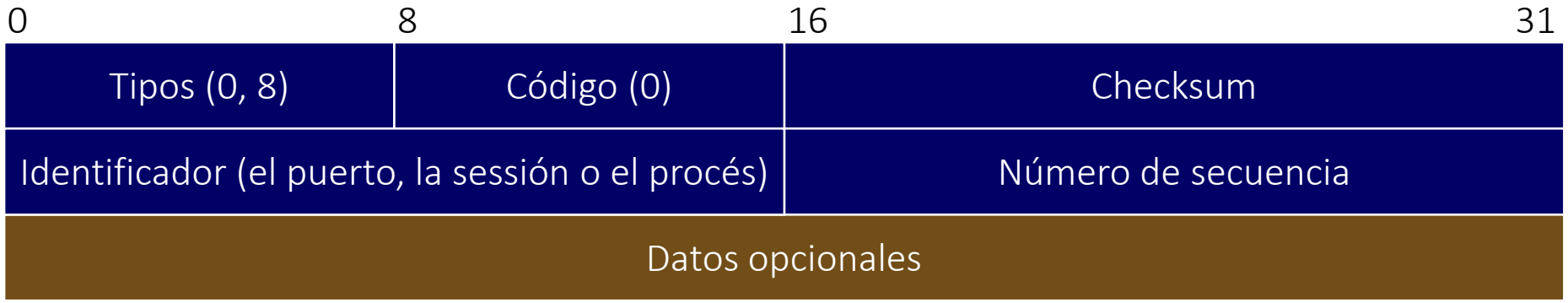
Source quench:
- Entregar el mensaje a la capa de transporte o a un modulo de procesamiento ICMP.

Tiempo agotado:
- Entregar el mensaje a la capa de transporte

Parámetros incorrectos:
- Entregar el mensaje a la capa de transporte; opcionalmente notificar al usuario.

4.8. Mensajes ICMP

Mensajes de ECO



Tipo: respuesta → 0, petición → 8

Identificador: Para identificar cual es el origen dentro del host origen.

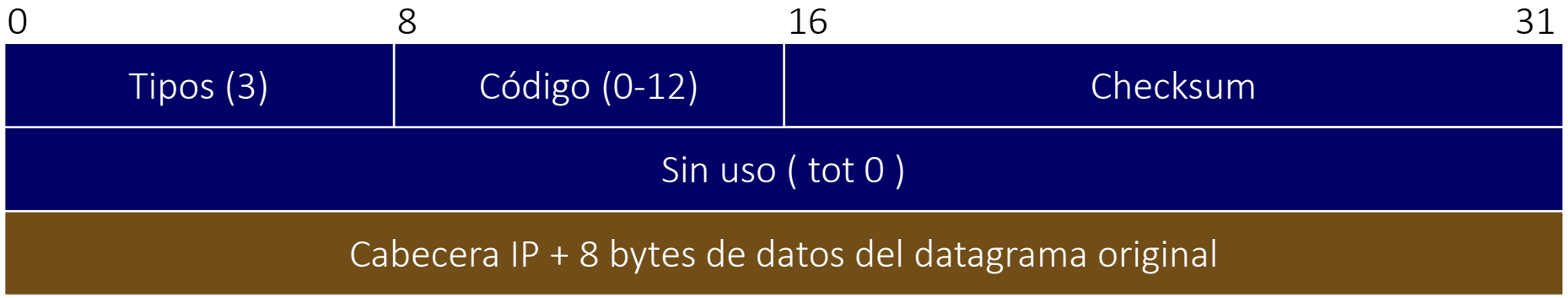
Datos opcionales: El originador puede poner datos que el destino retornaré en el ECO de respuesta.

Número de secuencia: para identificar los mensajes ECO de una misma ráfaga (los que tendrán el mismo identificador).

Utilizado por el servicio *ping.*

4.8. Mensajes ICMP

Mensajes de error: destino no alcanzable



Enviado por routers y hosts:

- **Routers**: no se conoce la red, no se puede fragmentar, host no disponible, etc.
- **Hosts**: protocolo del paquete IP no esta disponible, puerto no asumible, etc.

4.8. Mensajes ICMP

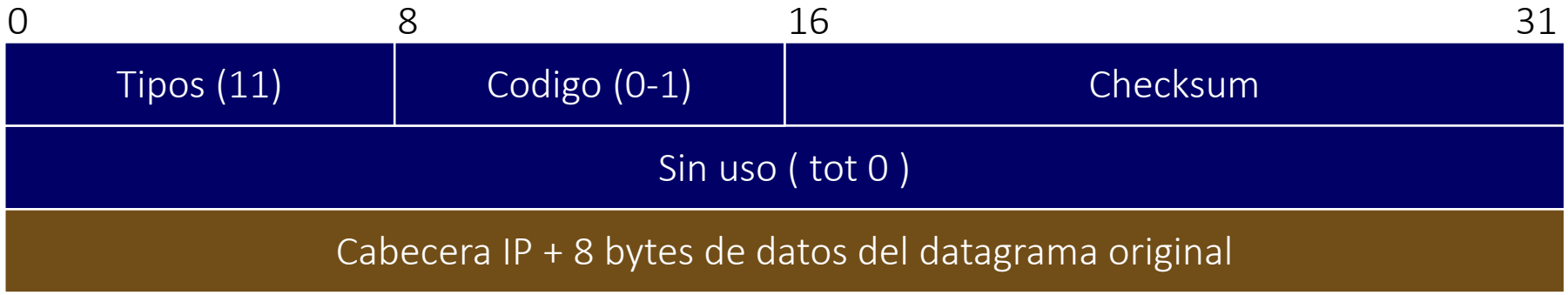
Mensajes de error: destino no alcanzable

- El campo Código identifica la causa del 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 administratively prohibited
11 - Network unreachable for type of service
12 - Host unreachable for type of service

4.8. Mensajes ICMP

Mensajes de error: tiempo agotado



Código: 0 – Se ha agotado el Time to Live

1 – Se ha agotado el temporizador de reensamblamiento

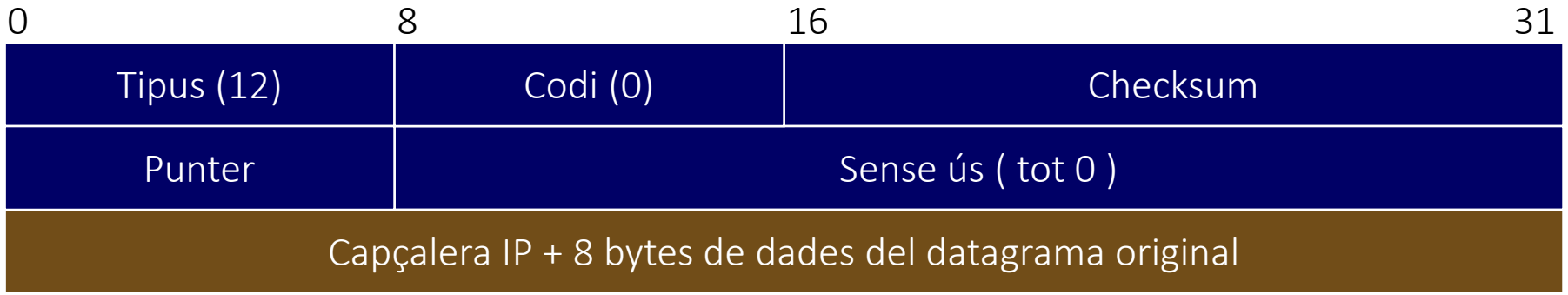
Debido a rutas circulares o excesivamente largas.

Cuando el tiempo de vida de un paquete se acaba, el router lo descarta y envía un mensaje de error ICMP.

Agotar el temporizador en el reensamblamiento de un datagrama (enviado des del host destino).

4.8. Mensajes ICMP

Mensajes de error: Parámetros incorrectos



Código: 0 - El puntero indica donde se encuentra el problema.
1 - Aplicaciones militares: falta una opción; no se utiliza el puntero.

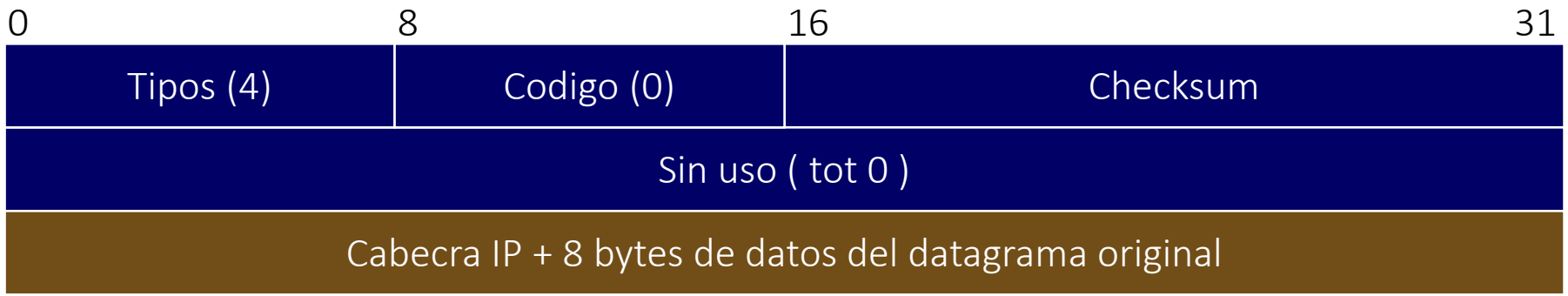
Debido a algún problema en la cabecera del datagrama.

El datagrama se descarta y se envía el mensaje ICMP.

El puntero indica el byte de la cabecera donde se ha detectado el error.

4.8. Mensajes ICMP

Mensajes de control de flujo: Source Quench



Enviado por routers y hosts que reciben datos más rápido del que pueden procesar.

Si el buffer de entrada se llena los datagramas se perderán.

Cuando se pierde un paquete se envía un ICMP para que se pueda reenviar.

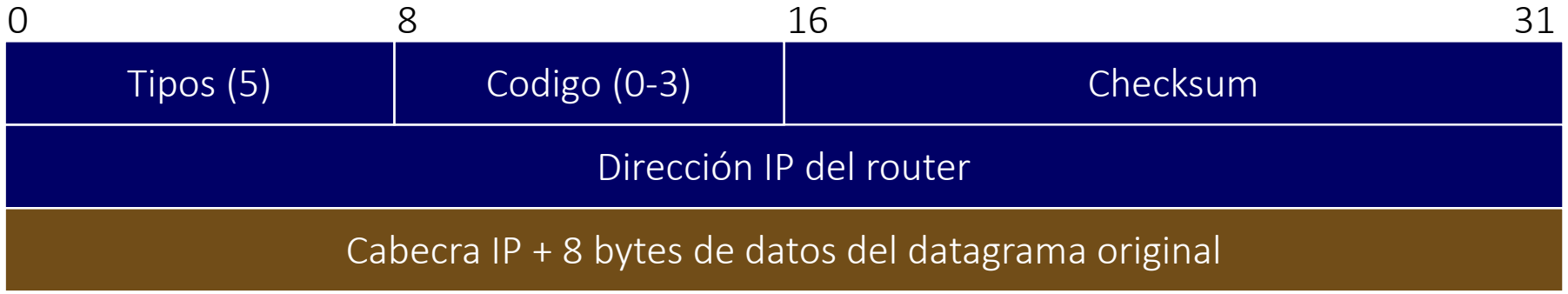
Cuando se recibe un mensaje ICMP de este tipo la fuente envía los paquetes de forma más lenta.

Posteriormente, se vuelve a incrementar el ritmo, lentamente.

este tipo de mensajes prácticamente no se utilizan.

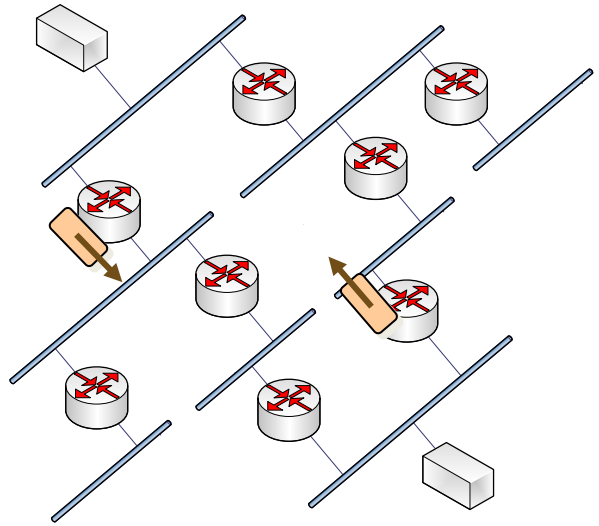
4.8. Mensajes ICMP

Mensajes de encaminamiento: redirigir (cambio de ruta)



Solo los envían los routers.

Informan que hay una ruta mejor.



4.8. Mensajes ICMP

Mensajes de encaminamiento: redirigir (cambio de ruta)

Cuando se utiliza un protocolo de encaminamiento dinámico, los routers se enteran de las nuevas rutas pero los hosts no.

Los routers envían información a los hosts para que actualicen la entrada de router por defecto en la tabla de rutas.

Los hosts dependen de los routers para mantener la información de encaminamiento.

Códigos de mensaje ICMP de redirección (Cambio de Ruta):

0 → Redireccionamiento de datagramas de la misma red (obsoleto)

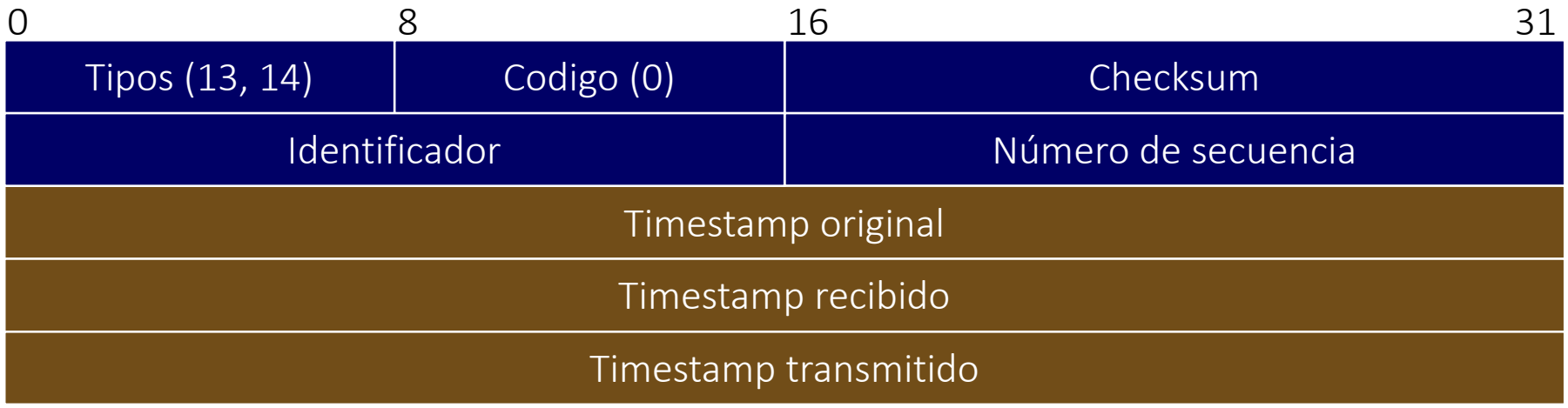
1 → Redireccionamiento de datagramas del mismo host

2 → Redireccionamiento de datagramas del mismo tipo de servicio y red

3 → Redireccionamiento de datagramas del mismo tipo de servicio y host

4.8. Mensajes ICMP

Mensajes de encaminamiento: Marcas de tiempo



Código: 13 - mensaje ; 14 - respuesta

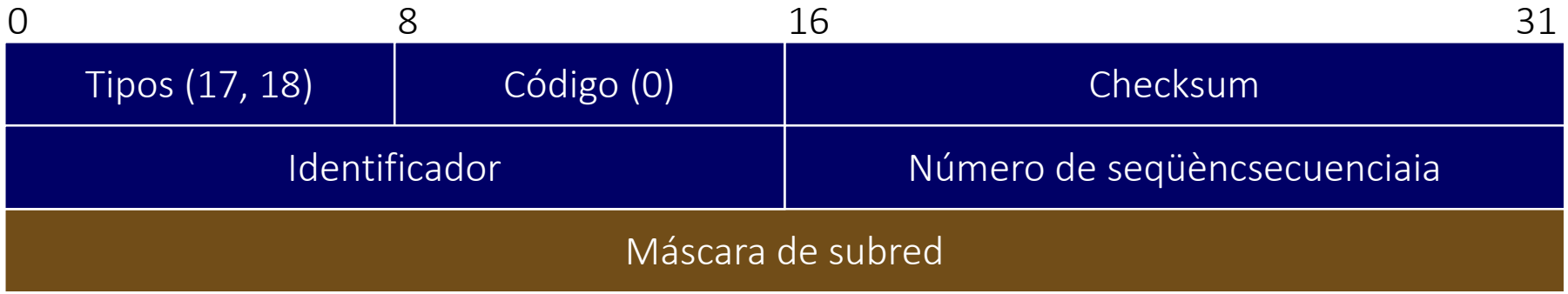
Máquinas independientes → Relojes desincronizados

El mensaje de timestamp sirve para sincronizar máquinas y estimar el tiempo de transito del paquete.

Problema: el tiempo de transito de un paquete puede variar mucho de un intento a otro.

4.8. Mensajes ICMP

Mensajes de encaminamiento: Obtención de máscara



Codi: 17 - Petición
18 - Respuesta

Cuando el host no sabe que máscara de subred se utiliza en la su subred la puede pedir a un router (o un servidor de máscaras).

La petición se puede enviar a un router directamente, si se sabe la dirección, o, si no, se puede hacer un broadcast a la red.

4.8. Mensajes ICMP

Mensajes de encaminamiento: Descubrimiento de rutas

Los routers envían información periódicamente y así los hosts pueden descubrir nuevas rutas.

Los hosts también pueden solicitar esta información.

Los mensajes se pueden enviar a las direcciones:

Multicast, todos los sistemas:	224.0.0.1
Multicast, todos los routers:	224.0.0.2
Broadcast:	255.255.255.255

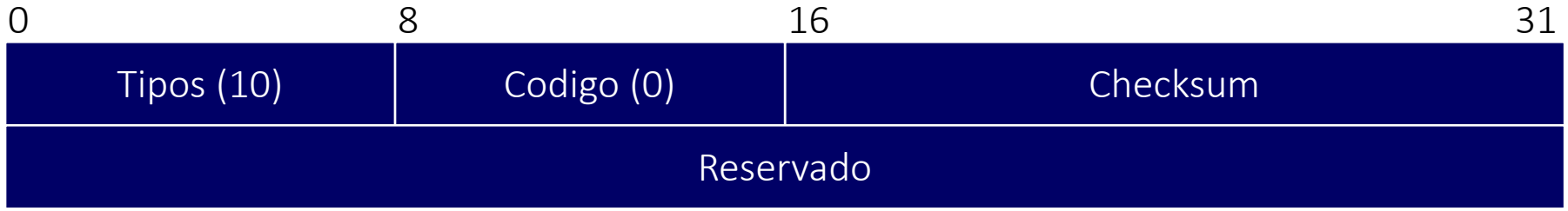
Necesidad de un router por defecto → Fichero → Procedimiento no dinámico → mensajes ICMP de mejores rutas

- Algunos hosts interpretan protocolos de encaminamiento
  Router Discovery Protocol (RDP)

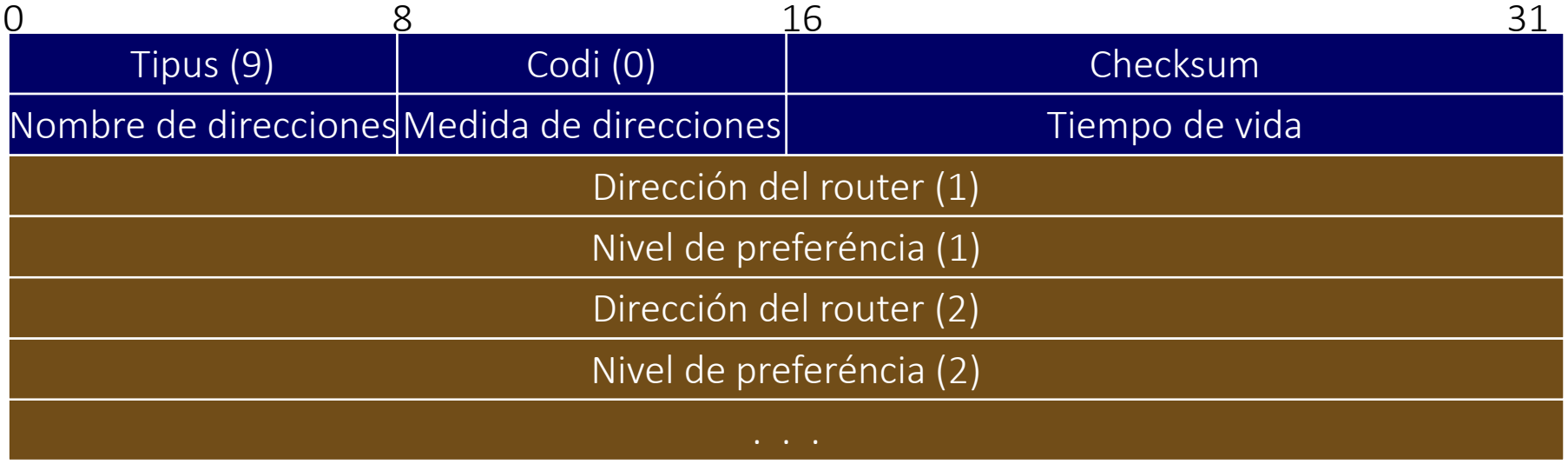
4.8. Mensajes ICMP

Mensajes de encaminamiento: Descubrimiento de rutas

Petición



Anuncio - Respuesta



4.8. Mensajes ICMP

Mensajes de encaminamiento: Descubrimiento de rutas

Nombre de direcciones:

- De cuantas direcciones informa el mensaje.

Tamaño de direcciones:

- Cuantas palabras de 32 bits se utilizan para describir una dirección. Actualmente es si 2.

Tiempo de vida:

- Tiempo durante el cual las direcciones pueden considerarse válidas

Dirección del router (n) :

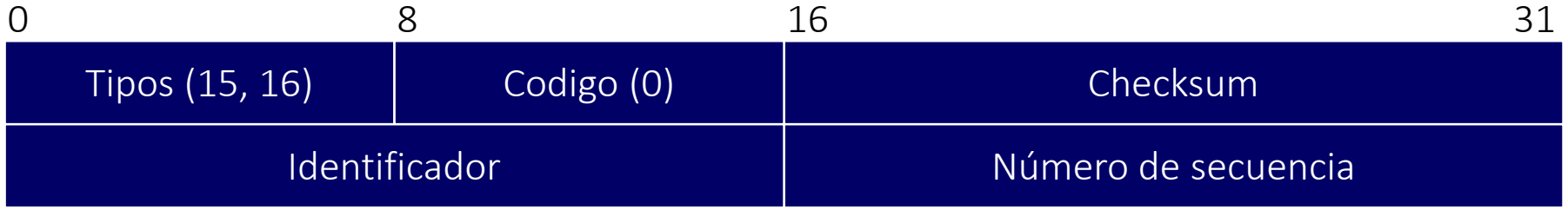
- Direcciones IP n del router de la interfaz por donde ha enviado el anuncio.

Nivel de preferencia (n):

- Cuanto más alto sea este valor más recomendada es la utilización de este router.

4.8. Mensajes ICMP

Mensajes de información



Código: 15 - Petición
16 - respuesta

Estos mensajes se consideran obsoletos.

Se utilizaban porque determinados hosts pudieran obtener su dirección Internet al ponerse en funcionamiento. Actualmente se utiliza el RARP (o otros protocolos).

4.9. Ejemplos prácticos

Comandos útiles en entornos IP

Utilizar la función *hostname* para obtener el nombre de un host.

Utilizar la función *ping* para conocer la dirección IP de un host.

Utilizar la función *nslookup* para obtener información del servidor de DNS.

Utilizar la función *netstat –r* o *netstat –nr* para conocer la tabla de encaminamiento del host.

Utilizar la función *netstat* i *netstat –a* para conocer las conexiones TCP/IP activas del host.

Utilizar la función *netstat –s* para obtener información de los mensajes ICMP que circulan por el host.

Utilizar la función *tracert* para descubrir el camino que seguiría un paquete IP hasta el destino

4.10. IP versión 6

Conceptos generales sobre IP versión 6

Problemes en el direccionamiento → IPng (next generation) IP versión 6

IPv6 se encuentra definido a RFC 1883, RFC 2460

Mejoras respecto a la versión 4:

- Más capacidad de direcciones: **32 bits** → **128 bits**
- Formato de cabecera simplificado: campos no necesarios o redundantes
- Facilita la configuración y la localización de routers
- Mejores extensiones y opciones
- Concepto de tipo de transito
- Seguridad: autenticación, integridad, confidencialidad

4.10. IP versión 6

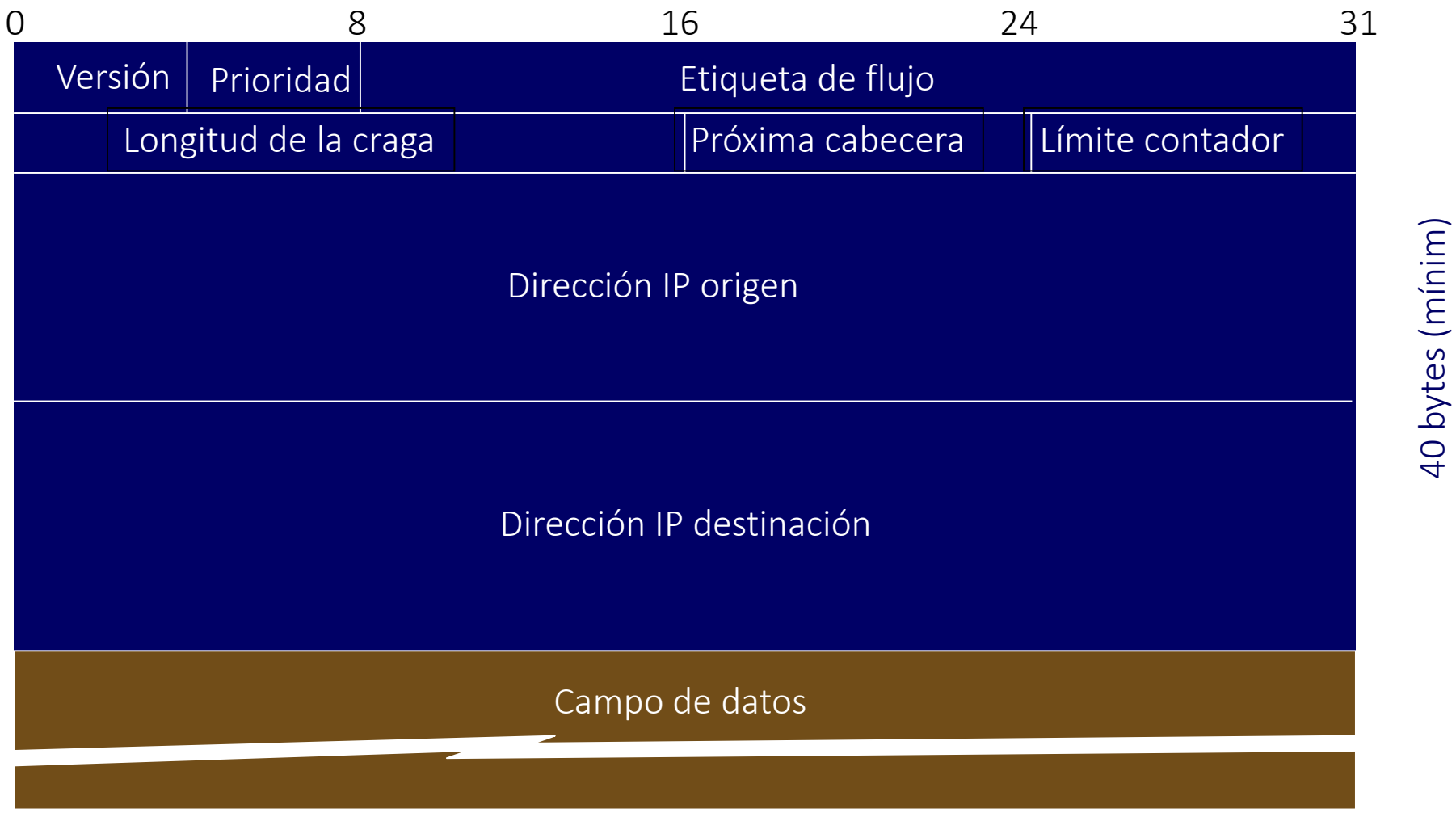
Formato del paquete IP versión 6

Formato más simple

- No hay checksum
  - La protección la hacen los protocolos inferiores y superiores
  - Se asume que el enlace es “bueno” (fibra, etc.)
- Se elimina la fragmentación
  - Para hacer más eficiente el protocolo
  - En caso necesario se hace en fuente.
- Las Opciones no están incluidas
  - Extensión de cabeceras

4.10. IP versión 6

Formato del paquete IP versión 6



4.10. IP versión 6

Formato del paquete IP versión 6

Versión (4 bits)
- Identifica la versión

Prioridad (4 bits)
- Ordena Prioridad del transito
- Dos tipo de transito
  - 0-7 aplicaciones que permiten control de congestión (por ej. TCP)
  - 8-15 aplicaciones que no soporta control de congestión
    - La red los puede descartar sin afectar la integridad de la información

4.10. IP versión 6

Formato de la cabecera IP versión 6

Valores de la prioridad (más alta ⇒ más prioritario)

- 0 transito sin caracterizar
- 1 transito de relleno (news,..)
- 2 transito de datos no atendido(e-mail)
- 3 reservado
- 4 transito de datos atendido, transferencia de ficheros (NFS,FTP..)
- 5 reservado
- 6 transito interactivo (Telnet, Xwindows,..)
- 7 transito de control de Internet (encaminamiento, SNMP,..)

4.10. IP versión 6

Formato de la cabecera IP versión 6

Etiqueta de flujos (24 bits)

- Identifica el tipo de transito, siempre al mismo destino
- encaminamiento más rápido (solo se procesa el primer paquete)
- Reserva de recursos

Longitud de la carga (16bits)

- con 16 bits ⇒ 65535 bytes
- paquetes más grandes ⇒ Jumbograma
  - Definidos mediante extensiones

Next header (8 bits)

- Indica si existe otra cabecera, y su tipo

4.10. IP versión 6

Formato de la cabecera IP versión 6

Hop limite (8 bits)

- Misma función que el TTL
- Pero se trata de un contador “real”

Direcciones origen y destinación (128 bits)

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

Con una asignación ineficiente se puede disponer de 1564 direcciones por m^2 (planeta Tierra)

4.10. IP versión 6

Extensión de les cabeceras IP versión 6

Para realizar tareas más complejas (información de fragmentación, de encaminamiento) se utilizan cabeceras especiales.

Extensión de cabeceras

- Hop by Hop: Contiene Opciones IP para cada sistema en la ruta del datagrama
- Encaminamiento: Permite que la fuente encamine el datagrama, similar a IPv4
- Fragmentación: información de fragmentación que envía la fuente al destino. Los nodos intermedios no fragmentan.
- Datos encriptados: Asegura que el datagrama no ha sido alterado durante la transmisión
- Autenticación: información de autenticación del origen
- Opciones de destino: Dos tipos de cabeceras para definir

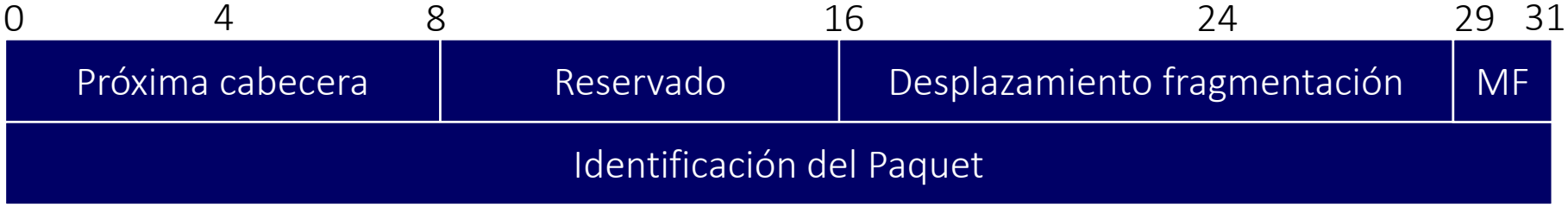
Extensión de cabecera: fragmentación

Información de fragmentación que envía la fuente al destino.

- Los nodos intermedios no fragmentan, la fragmentación está restringida a la fuente.
- Proceso de path MTU discovery previo a enviar el paquete, para hacer una fragmentación de extremo a extremo.

Cada fragmento debe ser un múltiple de 8 bytes.

El bit MF indica si hay más fragmentos



Extensión de cabecera: fragmentación

Identificador de paquete

- Identificar los fragmentos que pertenecen a un paquete
  - Identificador de 32 bits para adaptarse a las redes de alta velocidad.

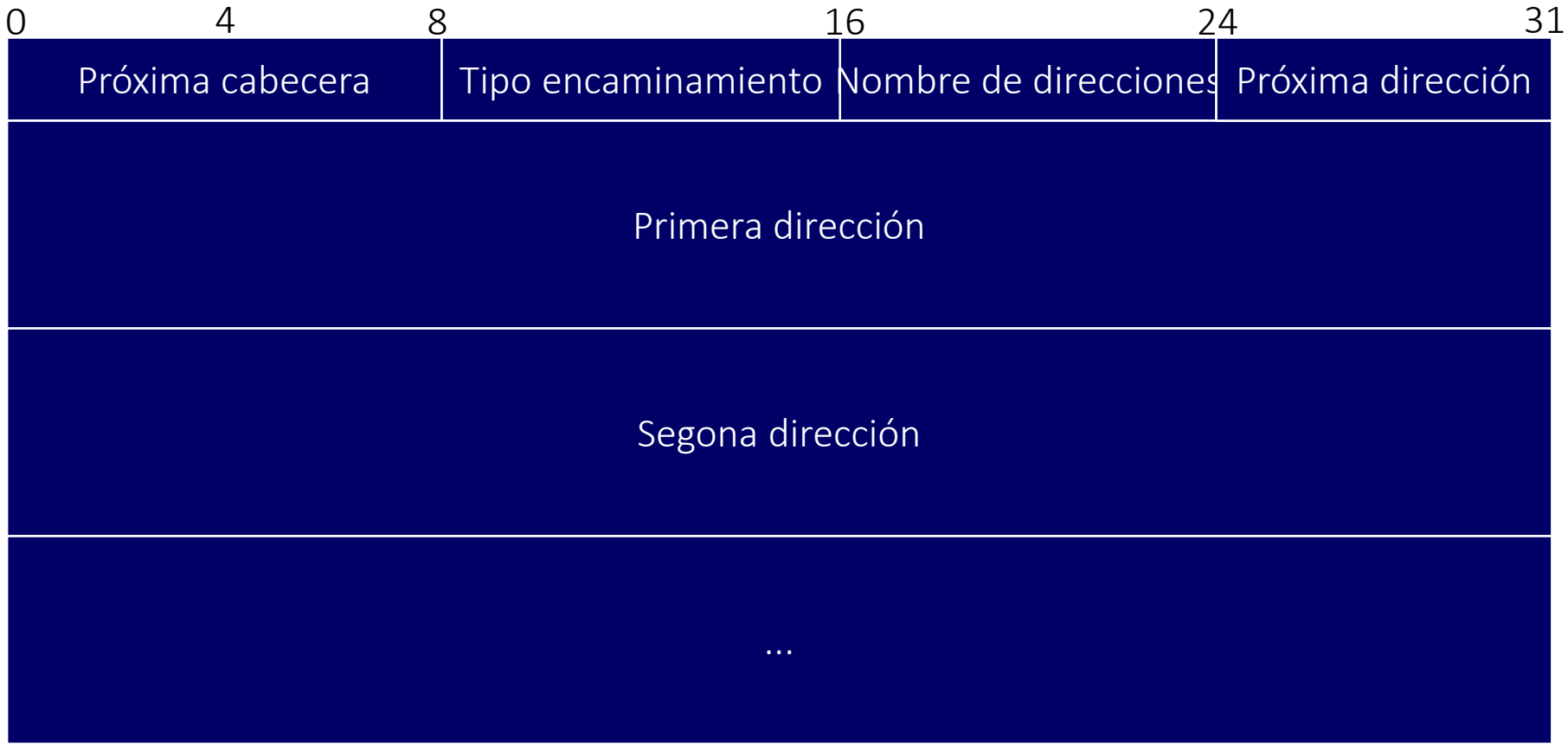
Qué pasa si hay un cambio de ruta?

- Si cambia el *path MTU,* el router que deba aplicar fragmentación realiza un túnel IPv6 sobre IPv6 para transportar los fragmentos del paquete original.

4.10. IP versión 6

Extensión de cabecera: encaminamiento de origen

Es similar a las opciones de encaminamiento de origen de IPv4.

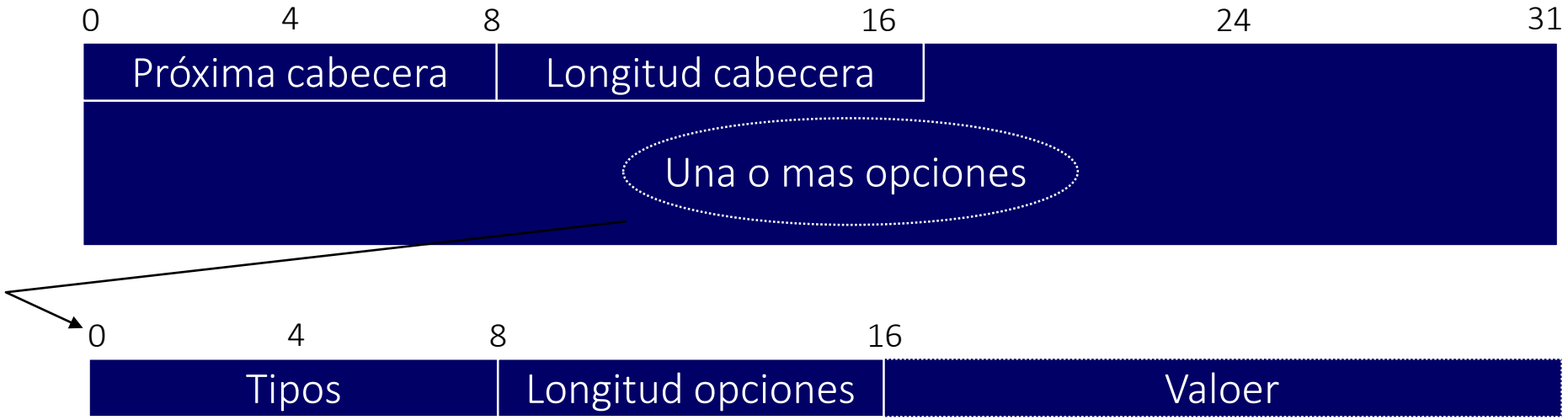


4.10. IP versión 6

Extensión de cabecera: Opciones de l'IPv6

Se definen 2 extensiones de cabecera adicionales para adaptarse a cualquier tipo de información no incluida en las cabeceras de información ya definidas.

- Hop by hop Extension Header: Opciones interpretadas a cada salto.
- End to End Extension Header: Opciones interpretadas al extremo final



4.11. IPsec

IP Security Protocol

- Permite una comunicación segura entre servicios y aplicaciones basados en IP.
- Hay que modificar la pila IPv4 para integrarlo
- Está incorporado por defecto a IPv6.
- Prestaciones
  - Autenticación/integridad
  - Confidencialidad
  - Gestión de llaves
  - Control de acceso
  - Anti repetición
  - Compresión

4.11. IPsec

IPSec es el estándar de comunicación segura a nivel 3

- Desarrollado por el grupo de trabajo de seguridad de IP de la IETF
- Estándar de 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

Características

- Transparente a las aplicaciones
  - APIs TCP/UDP no se modifican
- Transparente a los usuarios
  - No es necesario que tengan conocimientos de seguridad
- IPSec puede implementarse en un *firewall* o *router*
  - Se asegura todo el tráfico que cruza el perímetro
  - No es necesario cambiar los *programas:* la conversión la realizan el *firewall* o el *router.*
- *Aplicaciones*
  - *Virtual Private Networks* (VPN) a Internet
  - Acceso remoto seguro a Internet

4.11. IPsec

Características

Aplicable entre:

- 2 hosts: seguridad entre máquinas
- 2 routers: proteger un enlace de la red
- 1 host y un router: acceso seguro

2 modos de funcionamiento

- transporte: ídem IP pero con funciones de seguridad
- Túnel: se convierte en una opción para hacer VPNs

Es flexible y extensible

- No define completamente las especificaciones de los algoritmos a utilizar
- Permite escoger entre diferentes opciones y incorporar de nuevas

4.11. IPsec

Protocolos que se utilizan

Protocolos de seguridad de tráfico

- *Authentication Header* (AH)
  - Garantiza integridad, autenticación y detección de duplicados
- *Encapsulating Security Payload* (ESP)
  - Proporciona confidencialidad (cifrado) y puede autenticar

Protocolos de gestión de llaves(IKE)

- *Internet Security Asociation and Key Management protocolo* (*ISAKMP)*
  - Para la gestión de asociaciones de seguridad
- *Oakley*
  - Para la generación y gestión de llaves

AH/ESP se aplican por cada paquete independiente.

4.11. IPsec

Asociaciones de seguridad (SA)

- IPSec se basa en el concepto de Asociaciones de seguridad
  - Establecen toda la información necesaria para la comunicación segura entre dos dispositivos
  - Son relaciones unidireccionales entre emisor i receptor
  - Para comunicaciones bidireccionales se necesitan dos SAs
- Cada SA se identifica por:
  - *Security Parameter Index* (SPI)
    - Cadena de bits que actúa como identificador local
  - Dirección IP del destinatario
  - Identificador del protocolo de seguridad (AH/ESP)

4.11. IPsec

Asociaciones de seguridad (SA)

- *Security Asociation Database* (SADB)
  - Base de datos que contiene los parámetros de las SA.
  - Define los parámetros asociados a cada SA.
  - Todo nodo IPSec tiene una.
  - Son posibles diferentes implementaciones
- Funcionamiento
  - El transmisor:
    - Al enviar un paquete, consulta la SA en su SADB, lo procesa y incorpora el SPI
  - El receptor:
    - Analiza la dirección destino y el SPI, consulta la correspondiente SA en su SADB y lo procesa

4.11. IPsec

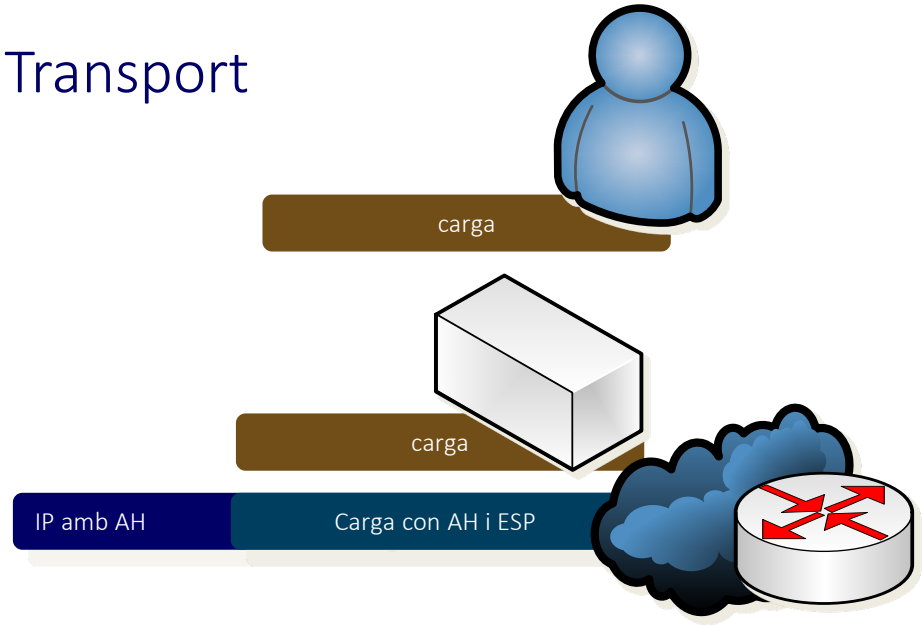
Parámetros de les SA

- SA l*ifetype* y *lifetime*
  - tipo de unidades (segundos o kilobytes) y el TTL de la SA
- *Group description*
  - El grupo Oakley utilizado en la negociación de llaves
- *Encapsulation mode*
  - Túnel o transporte
- *Authentication Algorithm*
- *Key Length and rounds*
- *ESP Information*
  - algoritmos de cifrado, llaves, tiempo de vida de llaves, ...
- *Sequence Number Counter*, Sequence Number Overflow, *Anti-Replay Window*
  - Mecanismos anti-repetición

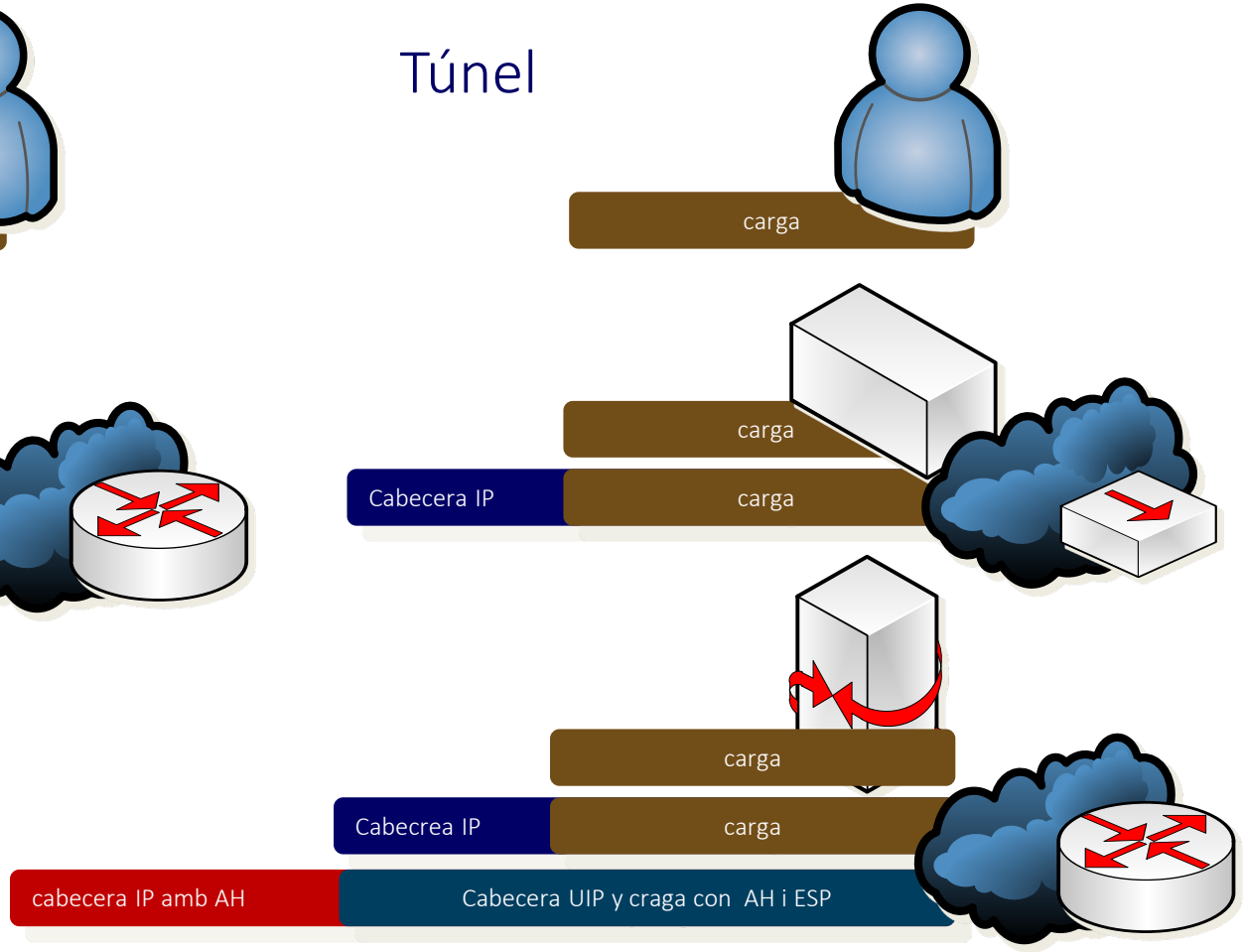
4.11. IPsec

Modos de funcionamiento

Transport



Túnel



4.11. IPsec

Modo transporte

Proporciona protección

- A los protocolos de la capa superior
  - Es decir, a la carga de los paquetes IP
- Toda la comunicación es segura (cifrada y/o autenticada)
  - Los equipos intermedios no pueden descifrar los paquetes

Se aplica normalmente en comunicaciones extremo a extremo entre equipos finales

Antes de que se añada la cabecera IP al paquete, se añaden las de seguridad

AH autentica la carga IP y partes de la cabecera IP

ESP cifra, y autentica opcionalmente, la carga IP, la cabecera IP no está protegida

Modo túnel

Protege el paquete IP entero

Se aplica normalmente en comunicaciones entre gateways

- Para proteger datagramas generados o destinados a sistemas no-IPSec (como con VPNs).
- Se aplica cuando la cabecera IP extremo a extremo ya se ha adjuntado al paquete

Funcionamiento

- Las cabeceras AH/ESP se añaden al paquete IP
- Todo el paquete se trata como si fuera la carga de un nuevo paquete con una nueva cabecera IP

Los paquetes viajan a través de un túnel

- Los routers del camino no son capaces de examinar el paquete original

4.12. Conclusiones

Conclusiones sobre IP y ICMP

Protocolo IP

- Protocolo de nivel de red, encamina y entrega información entre máquinas de redes diferentes.
- Unidad de info: datagrama IP (una cabecera y un campo de datos).
- No orientado a conexión y ofrece un servicio *Best effort*, la fiabilidad la proporcionan los niveles superiores.
- Utiliza la máscara de subred y tablas de encaminamiento para el establecimiento de rutas.
- Debido a las MTU aparece fragmentación y reensamblamiento

Protocolo ICMP

- Parte de IP que proporciona funciones de control, pero no hace el protocolo IP más fiable, solo notifica errores a la máquina origen.
- Los mensajes ICMP viajan en el campo de datos del protocolo IP, pero no es un protocolo de alto nivel.

Protocolo IPSec incorporar seguridad a IP