

# Fundamentos de Software de Comunicaciones

---

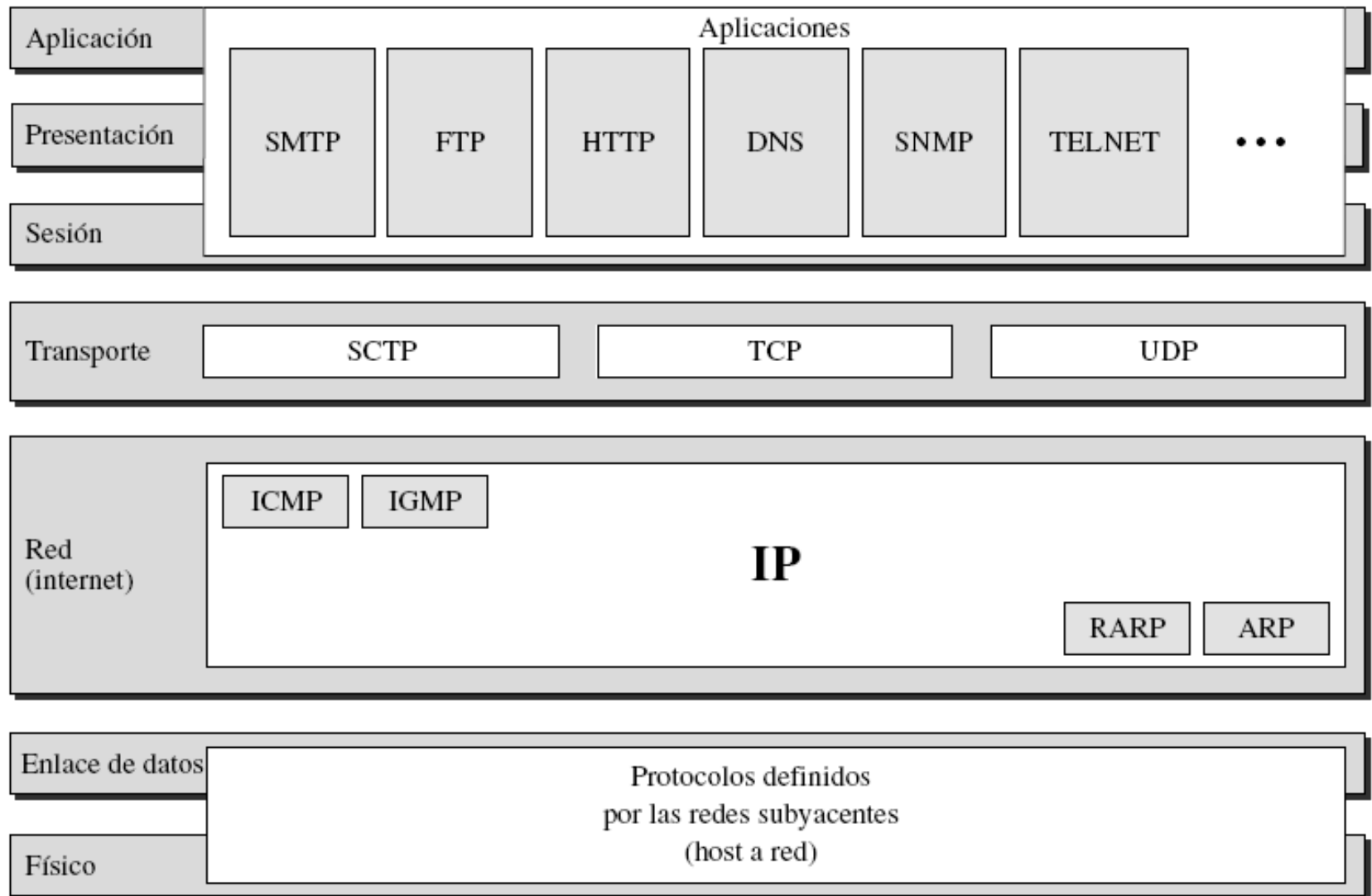
## Tema 4

### Introducción a TCP/IP

# Contenidos

- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- Interconexión en redes IP
- Protocolo IPv4
  - Direcciones IP. Máscaras de subred
- Protocolos asociados a IPv4
  - ARP
  - ICMP
- Nivel de Transporte: protocolos UDP y TCP

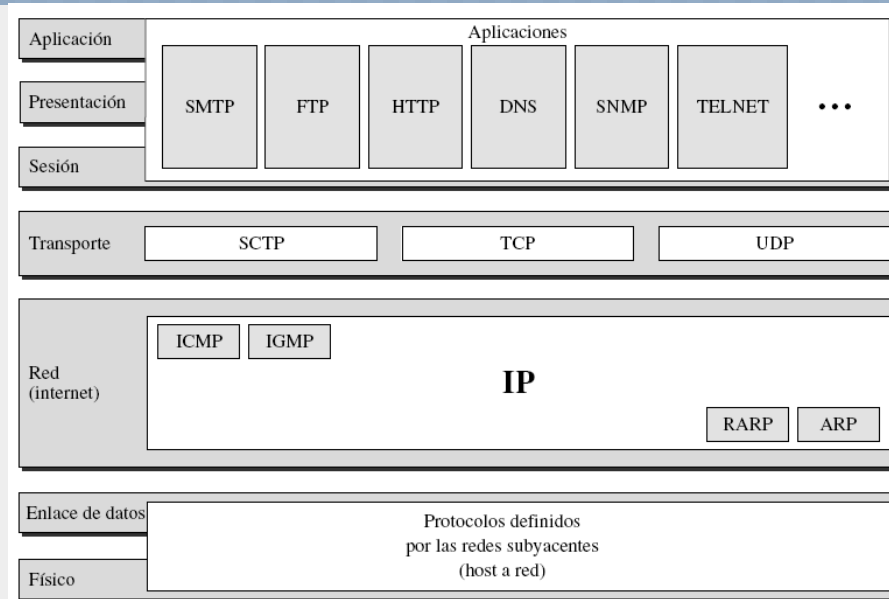
# Arquitectura de Protocolos TCP/IP



# Arquitectura de Protocolos TCP/IP

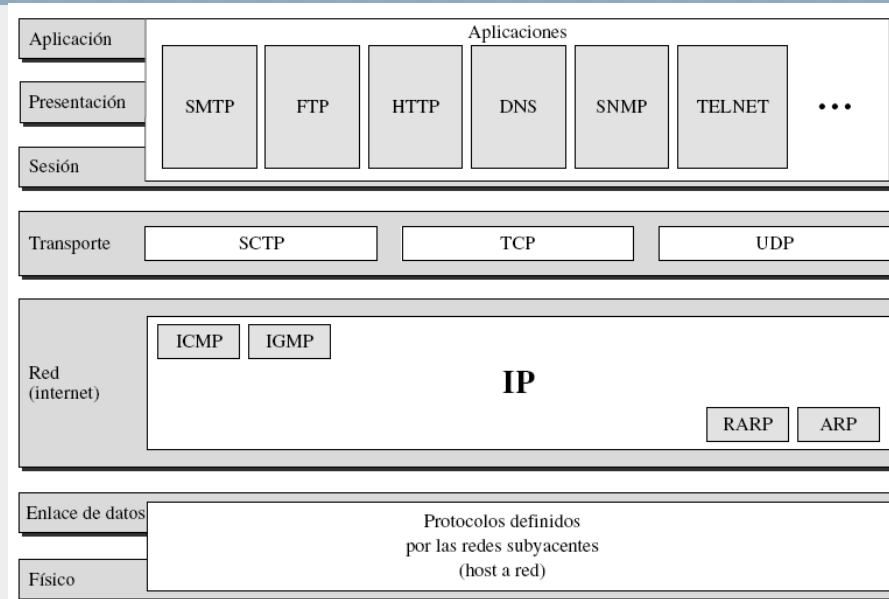
- TCP/IP es la **arquitectura comercial dominante** y constituye el núcleo de desarrollo de nuevos protocolos. Razones:
  - Se especificó y utilizó antes de la normalización de OSI (los costes de migración y la dificultad de sus capas superiores restó una mayor aceptación de OSI)
  - Su origen es ARPANET, la red de paquetes americana financiada por el Depto. de Defensa (DoD)
  - Internet está construida sobre los protocolos TCP/IP. El crecimiento de la Web ha contribuido a su extensión mundial
- En Internet existen nodos finales (**hosts**) e intermedios (**routers IP**). Las aplicaciones de Internet se ejecutan en los hosts. Los routers encaminan paquetes de red
- El conjunto de protocolos TCP/IP también considera que la tarea de la comunicación es compleja y diversa como para que la realice una sola entidad
  - Por ello se descompone en varios módulos (capas) que se comunican con sus entidades homólogas en otros nodos
  - Una entidad proporciona servicios a otras entidades, y a su vez utiliza servicios de otras

# Arquitectura de Protocolos TCP/IP



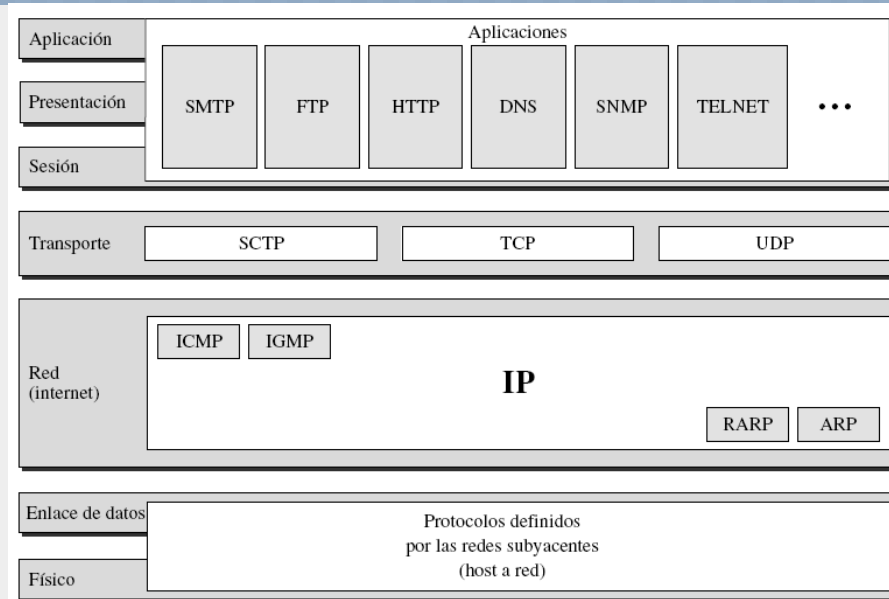
- **Capa de transporte (nivel 4):** proporciona un servicio de transferencia de datos extremo-a-extremo
  - **¿A quién?** A **procesos** o aplicaciones de los usuarios (sockets).
  - **¿En qué consiste?** Servicio orientado a conexión de tubería de bytes fiable (TCP) o servicio de mensajería no fiable y no orientada a conexión (UDP)
  - **Característica fundamental:** uso de **puertos** para distinguir los procesos receptores de mensajes de este nivel

# Arquitectura de Protocolos TCP/IP



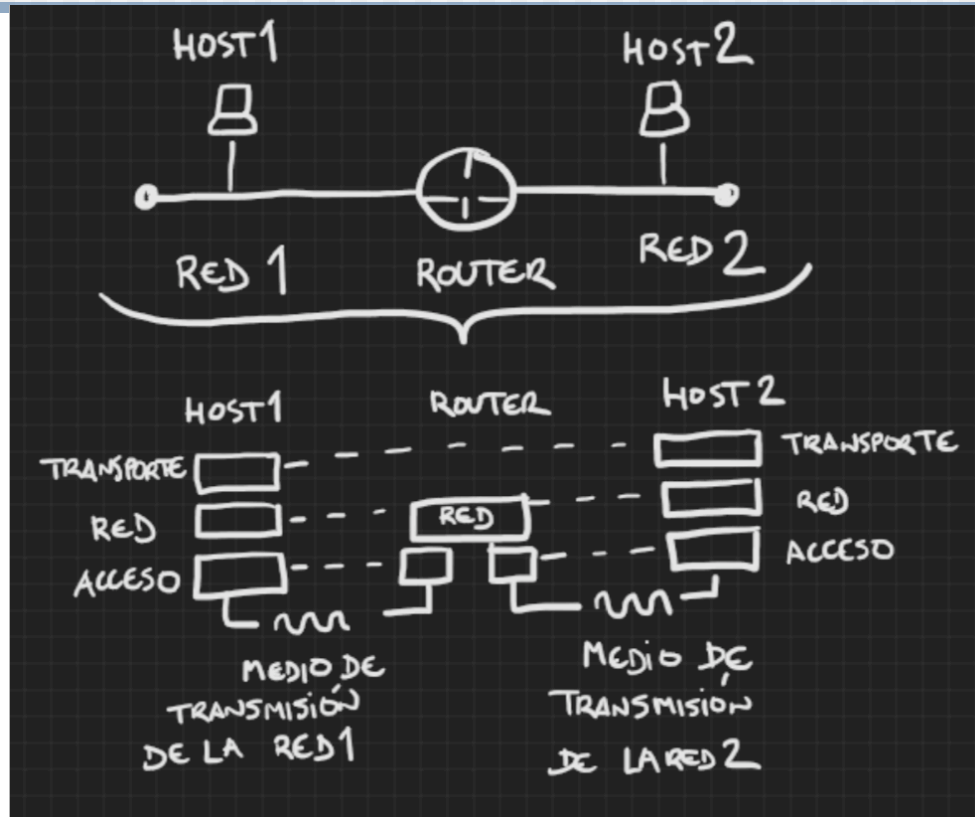
- **Capa Internet (nivel 3):** proporciona un servicio de encaminamiento de datos del nodo origen al destino a través de **una o más redes** conectadas por dispositivos de encaminamiento (routers IP)
  - **¿A quién?** A protocolos de transporte que necesitan utilizarlo para envíos y recepciones de datagramas de internet
  - **¿En qué consiste?** Servicio de **datagramas NO fiable y no orientado a conexión**
  - **Característica fundamental:** uso de **direcciones IP** para distinguir los equipos destino y origen

# Arquitectura de Protocolos TCP/IP



- **Capa de acceso a red (niveles 1 y 2):** relacionada con la interfaz lógica entre un sistema final y una subred. La parte de capa física define las características del medio de transmisión, el esquema de codificación de señales, etc.
  - **¿A quién?** A la capa de red
  - **¿En qué consiste?** Permite que los datagramas IP viajen por una red de ordenadores. Origen y destino deben estar en la misma red. Los mensajes se traducen a señales electromagnéticas (u ópticas) en transmisión (y se decodifican en recepción).
  - **Característica fundamental:** uso de **direcciones físicas** (MAC) asociadas a cada tarjeta de red, para distinguir origen y destino de los datos

# Arquitectura de Protocolos TCP/IP

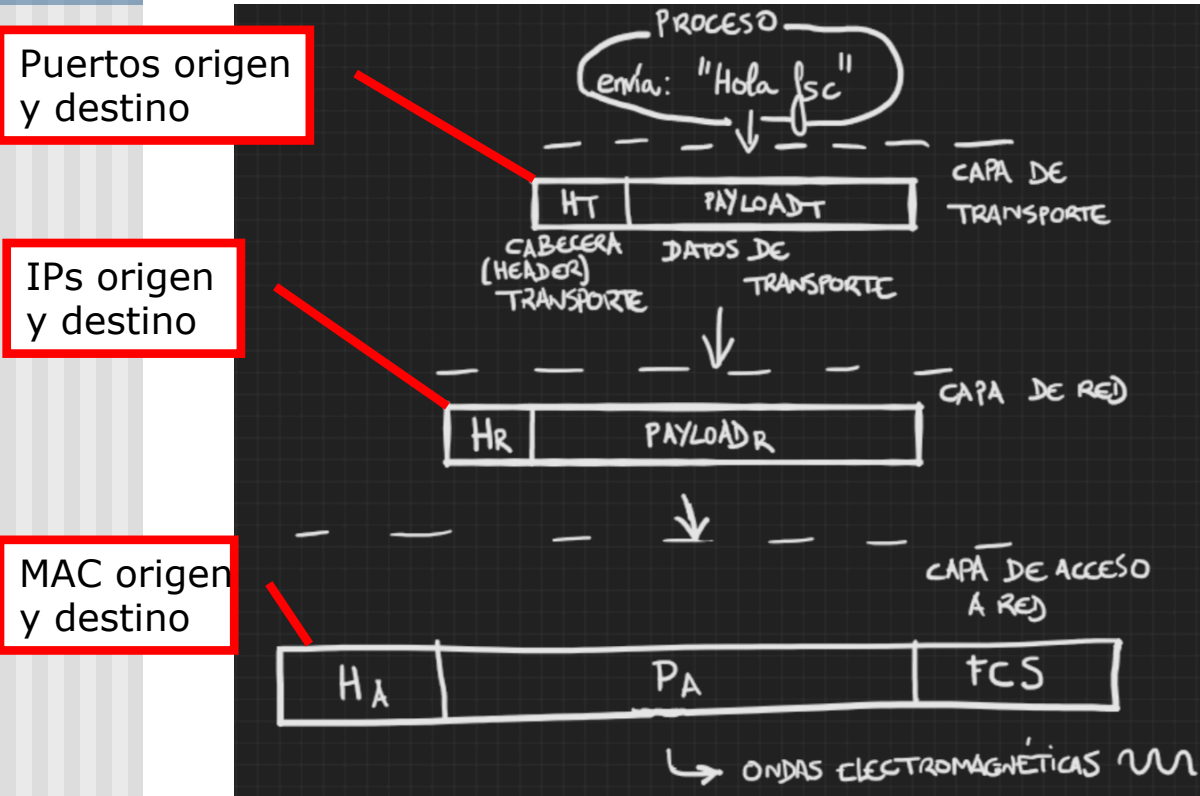


- Host implementan toda la pila
- Router sólo la capa de red y la de acceso
- Líneas discontinuas: diálogo entre capas
- Las PDUs de nivel superior pasan por el resto de capas sin que se interpreten

- Es importante entender que los diálogos se producen entre capas, es decir, un protocolo de transporte sólo se entiende con otro protocolo de transporte



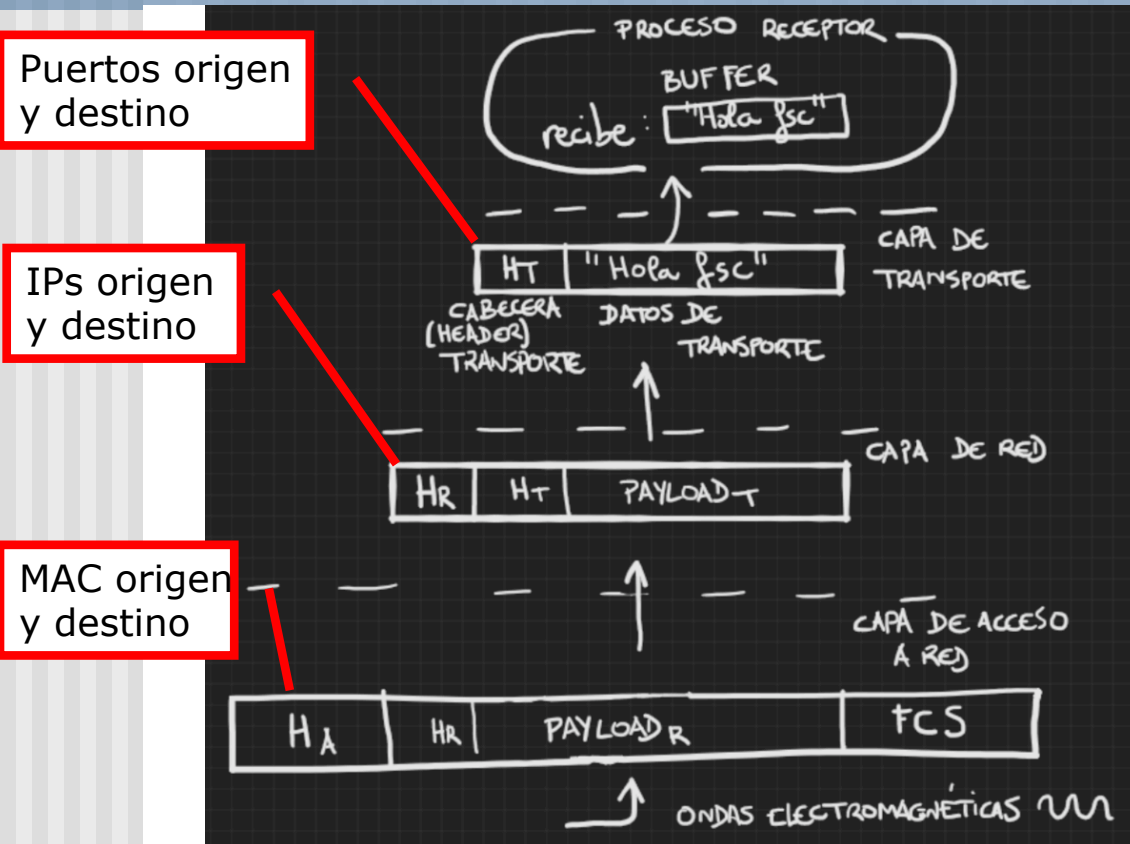
# El viaje de los datos: envío



- Cada capa, para realizar un envío, monta su propio paquete de datos: PDU (Protocol Data Unit)
- **Cabecera:** información para que la capa del mismo nivel que recibe la PDU entienda qué es ese mensaje y qué contiene
  - Puerto origen y destino
- **Datos:** la información que la capa superior (o el proceso) quiere enviar

- Una vez que ha montado la PDU, solicita a la capa inferior que la envíe
- El proceso se repite hasta que el mensaje llega a la capa de acceso, que le añade normalmente una cola (FSC: Frame Control Sequence) para control de errores

# El viaje de los datos: recepción

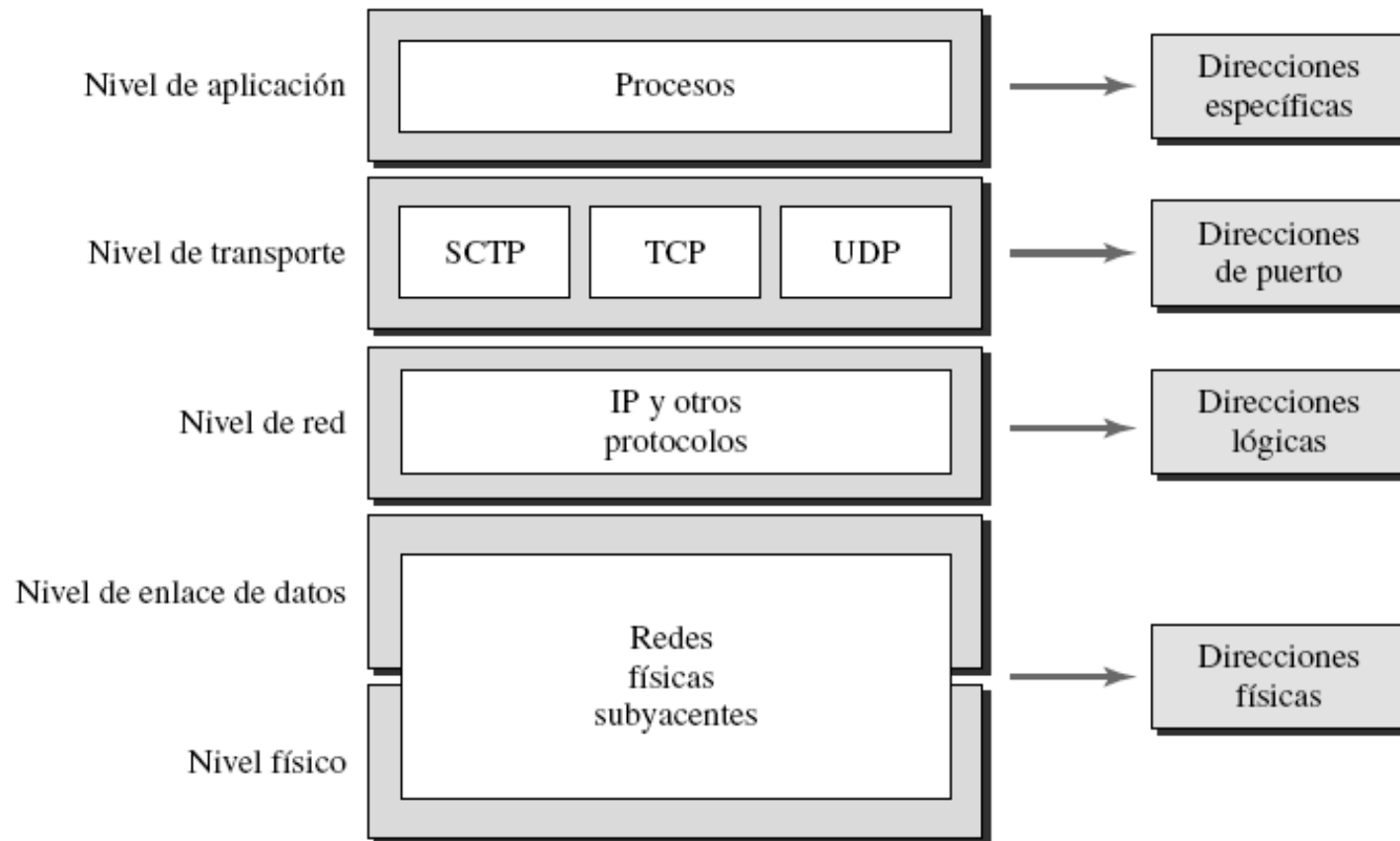


- Ahora vamos de abajo a arriba
- La capa de acceso a la red comprueba el FCS para comprobar que no hay errores en la transmisión
- Si la dirección MAC coincide con la suya, extrae los datos y la pasa a la capa de red
- La capa de red analiza la cabecera y, dependiendo de si es un host o un router, actúa de manera diferente

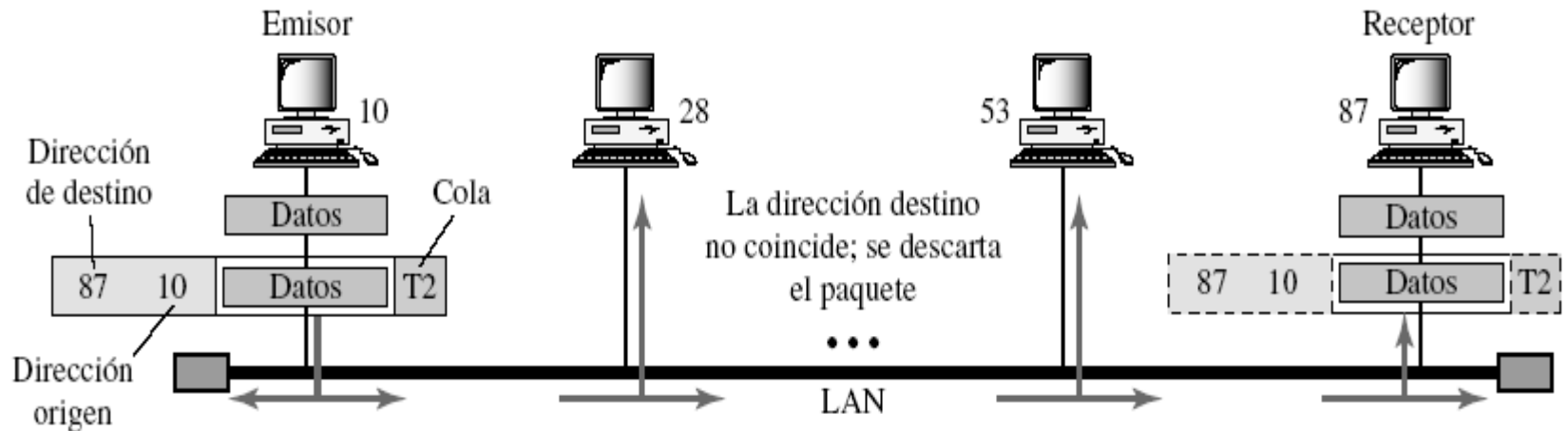
- Si la IP coincide, entonces extrae los datos (PDU de transporte) y los pasa a la capa superior
- La capa de transporte comprueba el puerto y coloca los datos en la cola del socket vinculado a ese puerto
- El proceso receptor en algún momento hará un **read()/recvfrom()** para recoger el mensaje "Hola fsc"

# Direccionamiento en TCP/IP

- Direcciones físicas
- Direcciones lógicas (de interred)
- Direcciones de puertos
- Direcciones específicas de aplicaciones



# Direcciones físicas



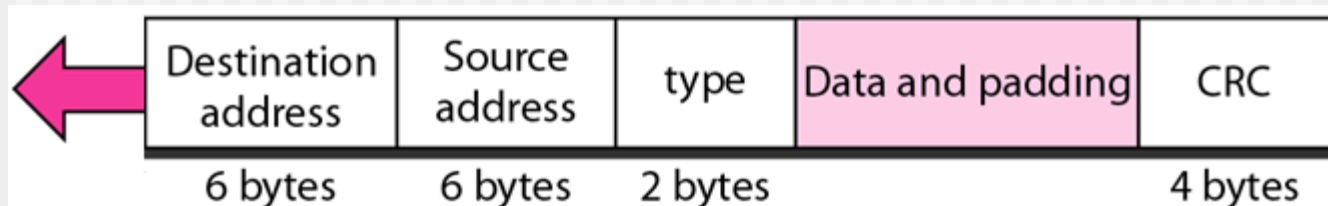
**Redes Ethernet:** La tarjeta de red proporciona al nodo una dirección física (MAC) de 6 bytes. Ejemplo: 06:01:02:01:2C:4B

- Las direcciones MAC destino pueden ser:

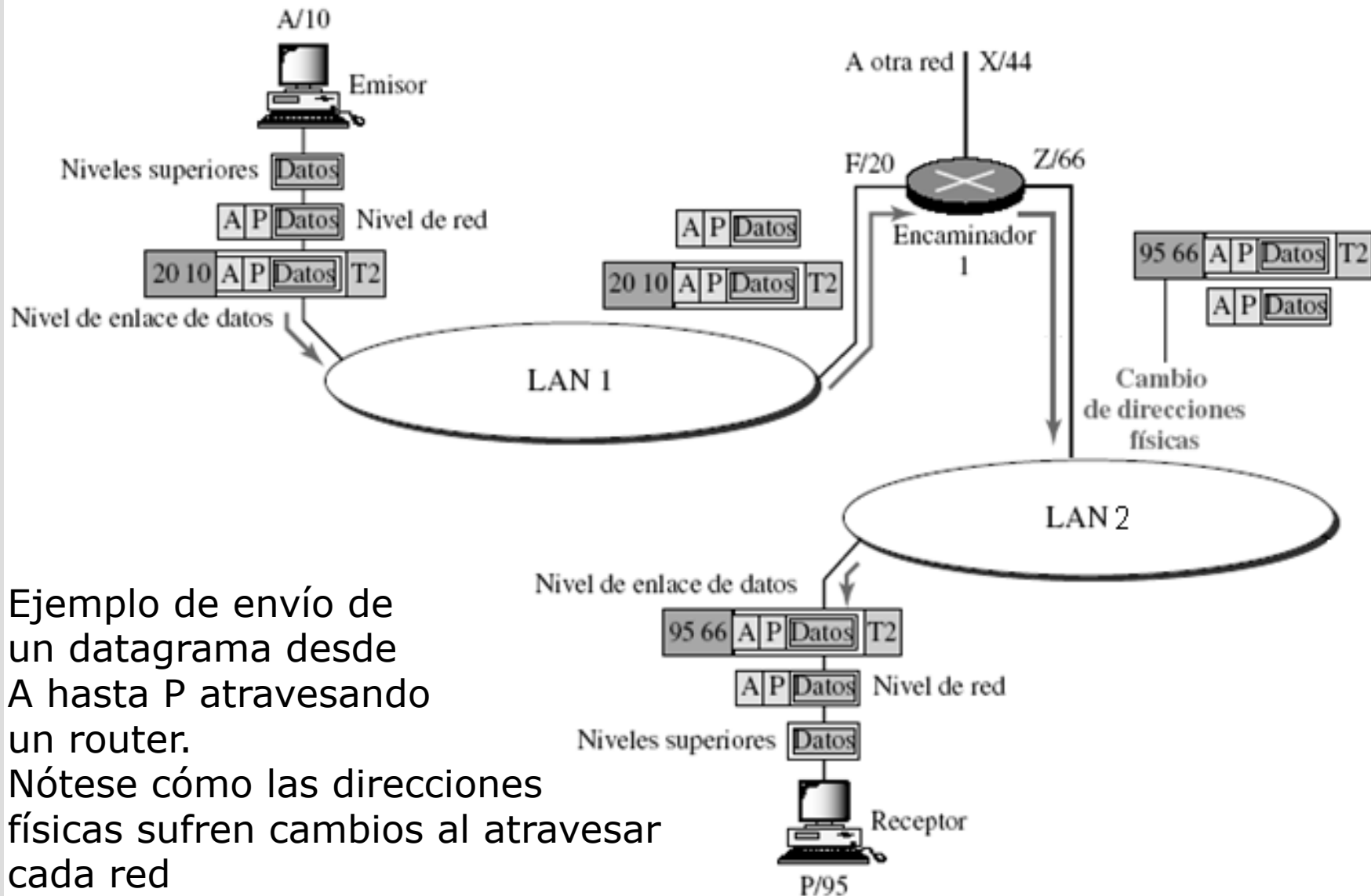
- A un nodo (Unicast): el bit menos significativo del primer byte es 0

- A un grupo de nodos (Multicast): el bit menos significativo del primer byte es 1

- A todos en la red (Broadcast): FF:FF:FF:FF:FF:FF



# Direcciones lógicas

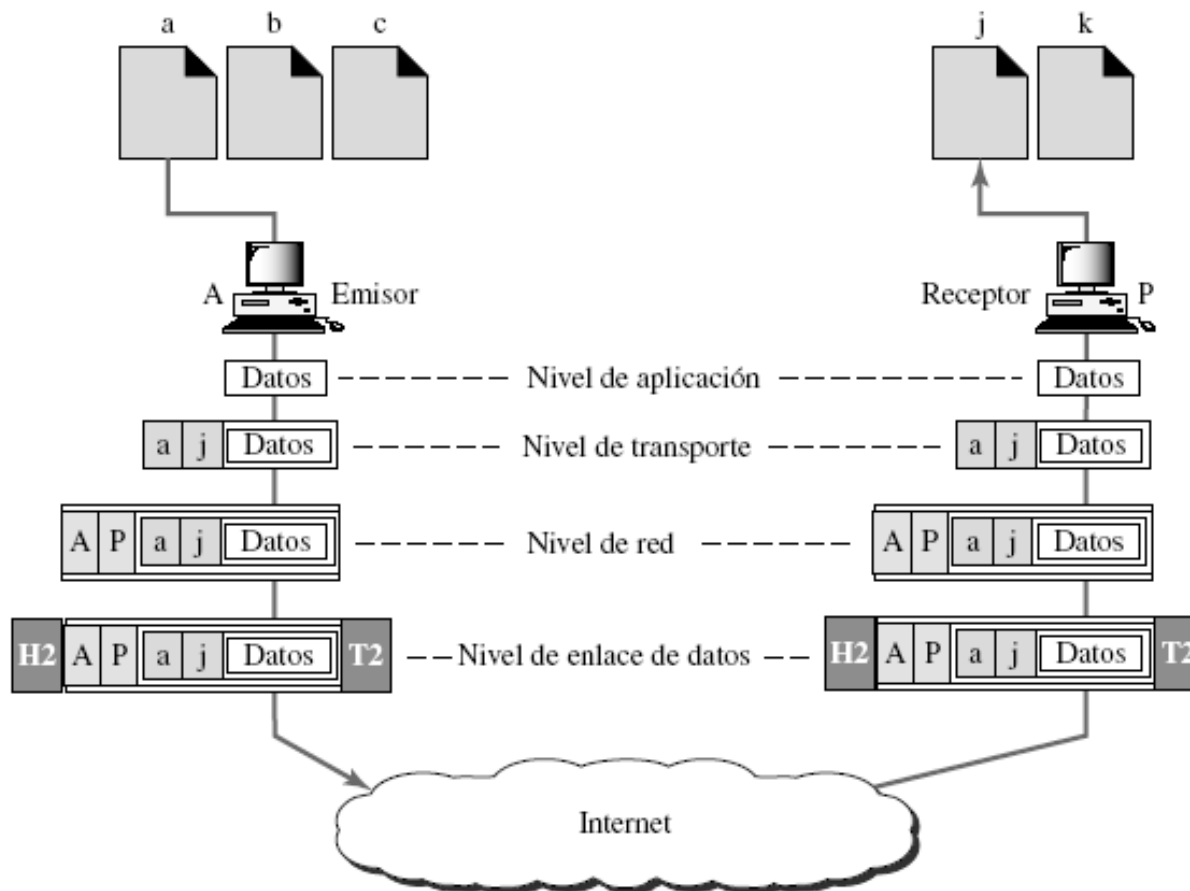


Ejemplo de envío de un datagrama desde A hasta P atravesando un router.

Nótese cómo las direcciones físicas sufren cambios al atravesar cada red

# Direcciones de puertos y específicas

- Las direcciones de puertos identifican procesos (a, b, c, j, k) a nivel de transporte
- Las direcciones específicas de aplicación discriminan objetos de servicio de alto nivel, como una página web (<http://www.redes.uma.es>) o un buzón de correo ([usuario@redes.uma.es](mailto:usuario@redes.uma.es))



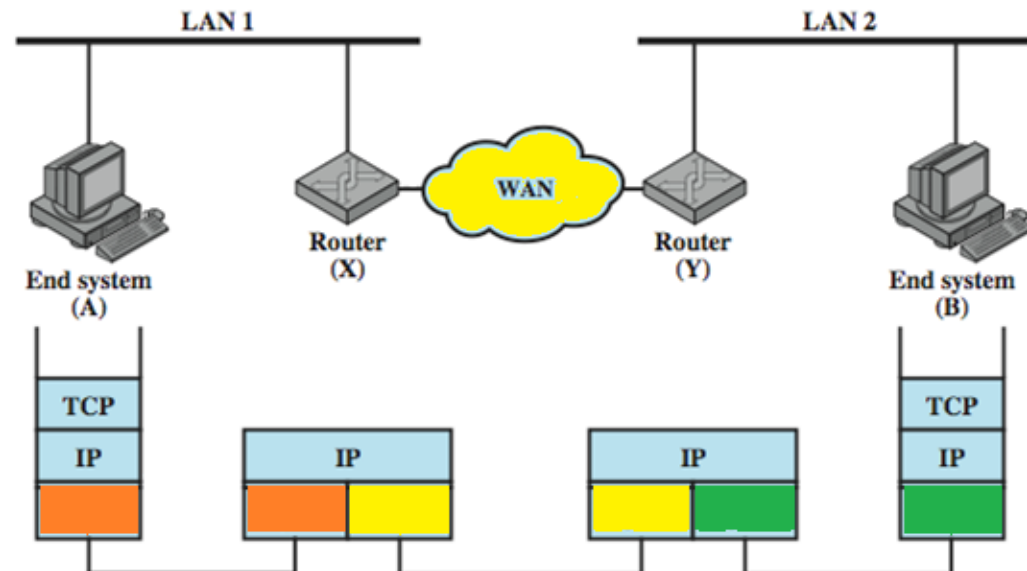
# Contenidos

- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- **Interconexión en redes IP**
- Protocolo IPv4
  - Direcciones IP. Máscaras de subred
- Protocolos asociados a IPv4
  - ARP
  - ICMP
- Nivel de Transporte: protocolos UDP y TCP

# Interconexión entre redes, sin conexión

## ■ Características básicas:

- Se corresponde con un mecanismo de datagramas de una red de conmutación de paquetes (cada PDU se trata independientemente)
- Se necesita un **protocolo de red común** a todos los nodos y dispositivos de encaminamiento (el protocolo IP):
- Este protocolo de red utiliza el protocolo específico de la capa inferior necesario para acceder a una tecnología red particular (Ethernet, Wifi ...)





# Interconexión entre redes, sin conexión

## ■ Ventajas:

- Flexible y robusto (admite bien las caídas de enlaces)
- No impone información suplementaria innecesaria en los paquetes de datos

## ■ El servicio de red suele ser **no fiable**:

- No garantiza que todos los datos se entreguen al destino
- No garantiza que los datos que se entregan lleguen en el orden adecuado:
  - Porque los paquetes pueden seguir diferentes caminos
- La fiabilidad será responsabilidad de la capa superior (por ejemplo, TCP)

# Cuestiones de diseño de un nivel de red

## ■ Encaminamiento:

- Se efectúa por medio del mantenimiento de una tabla de encaminamiento en cada dispositivo de encaminamiento y en cada sistema final
  - La tabla puede ser estática o dinámica
  - Una tabla estática puede contener rutas alternativas por si no está disponible algún dispositivo de encaminamiento
  - Una tabla dinámica es más flexible a la hora de enfrentarse a condiciones de error y congestión

## Cuestiones de diseño de un nivel de red (II)

- Tiempo de vida de los datagramas:
  - Existe la posibilidad de que un datagrama viaje indefinidamente a través del conjunto de redes
    - Problema: Consume recursos
  - Para evitar estos problemas cada datagrama se puede marcar con un tiempo de vida
    - Una vez transcurrido ese tiempo se descarta el datagrama
  - Se implementa con un contador de saltos, o con un mecanismo de sincronización entre los dispositivos

## Cuestiones de diseño de un nivel de red (III)

### ■ Segmentación y Reensamblado:

- Dentro del conjunto de redes cada una puede especificar tamaños máximos de paquete diferentes
- Sería ineficiente imponer un tamaño uniforme a través de las redes, por lo que los dispositivos de encaminamiento pueden necesitar segmentar los datagramas en fragmentos
- ¿Dónde reensamblarlos?
  - Solución fácil: en el destino, como se hace en IP.  
Desventaja: Poco eficiente
  - Otra solución: en los propios dispositivos de encaminamiento. Desventajas:
    - Se requieren grandes memorias temporales en los dispositivos de encaminamiento
    - Puede que la memoria temporal se use para almacenar fragmentos
    - Todos los fragmentos deben pasar a través del mismo dispositivo de encaminamiento (imposibilita encaminamiento dinámico)

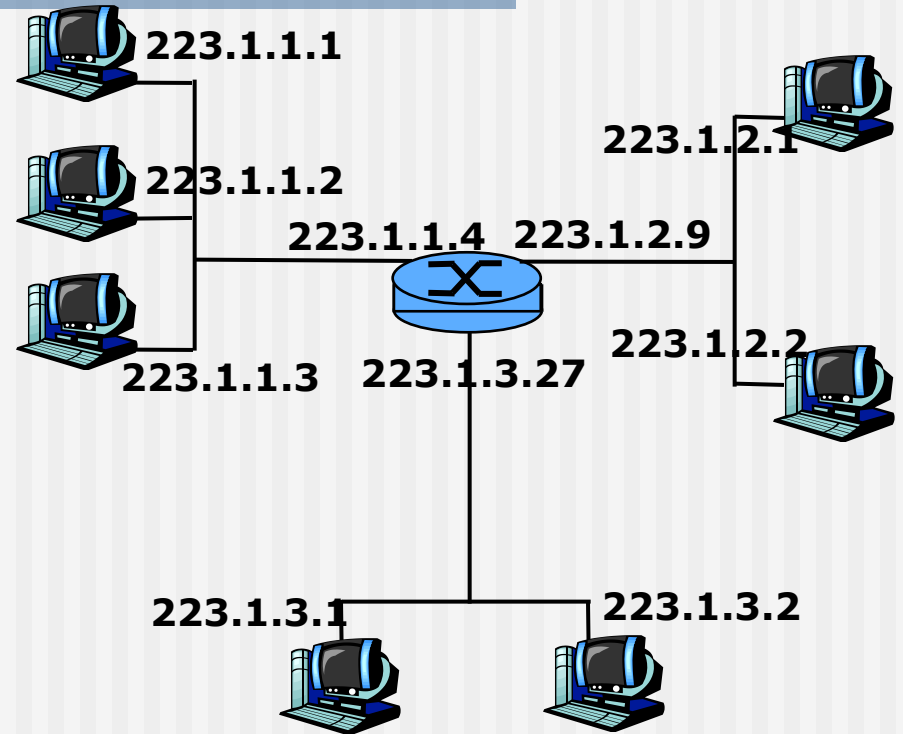
# Contenidos

- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- Interconexión en redes IP
- **Protocolo IPv4**
  - Direcciones IP. Máscaras de subred
- Protocolos asociados a IPv4
  - ARP
  - ICMP
- Nivel de Transporte: protocolos UDP y TCP

# Direcciones IP

Direcciones de 32 bits en IPv4

- Cada interfaz de host o router tiene una dirección única
- **Interfaz:** conexión de host/router a red física
  - Los routers tienen varios interfaces
  - Los hosts *pueden tener* múltiples interfaces
  - La dirección IP se asocia al interfaz
- Los 32 bits se dividen en:
  - Un prefijo para red,
  - Sufijo para ordenador
  - La asignación de identificadores de red es global
  - La asignación de direcciones a ordenadores es local



223.1.1.1 = 11011111 00000001 00000001 00000001

223	1	1	1
-----	---	---	---

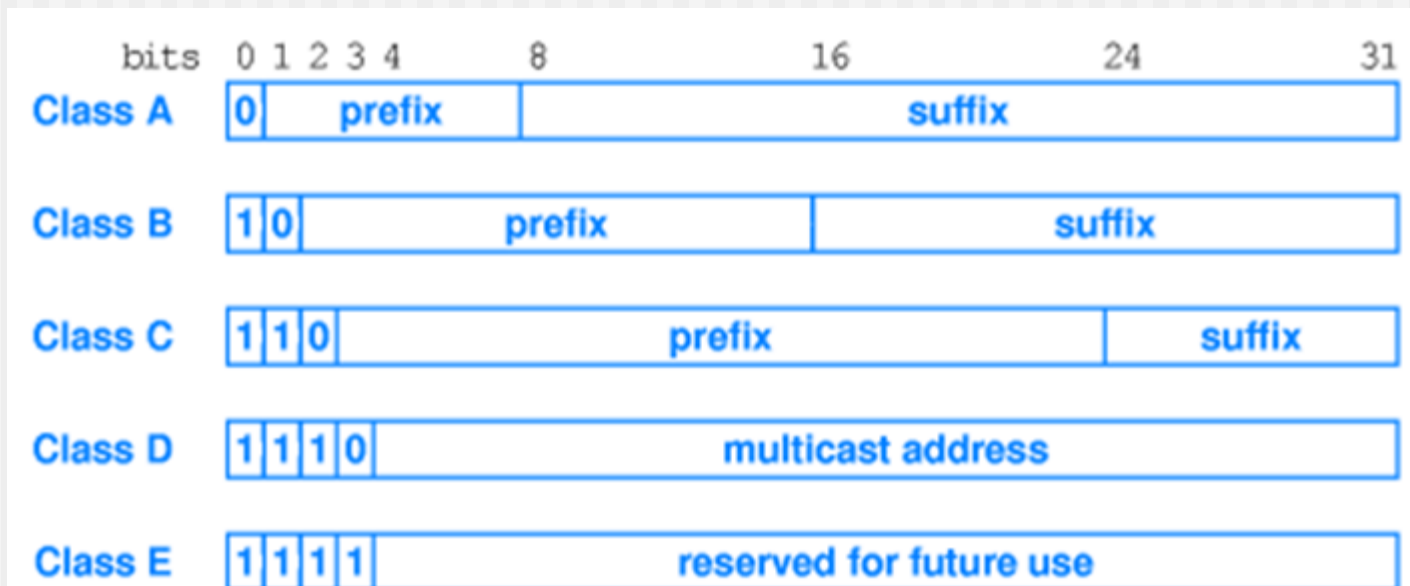
(Stallings)

# Direcciones IP clásicas (I)

- La notación clásica para direcciones permitía identificar las clases de direcciones IP y de las redes
  - Redes de Clase A → los últimos 3 octetos identifican el host
  - Redes de Clase B → los últimos 2 octetos identifican el host
  - Redes de Clase C → el último octeto identifica el host

**bits de prefijo: identificador numérico de la red**

**bits de sufijo: identificador numérico del host**



## Direcciones IP clásicas (II)

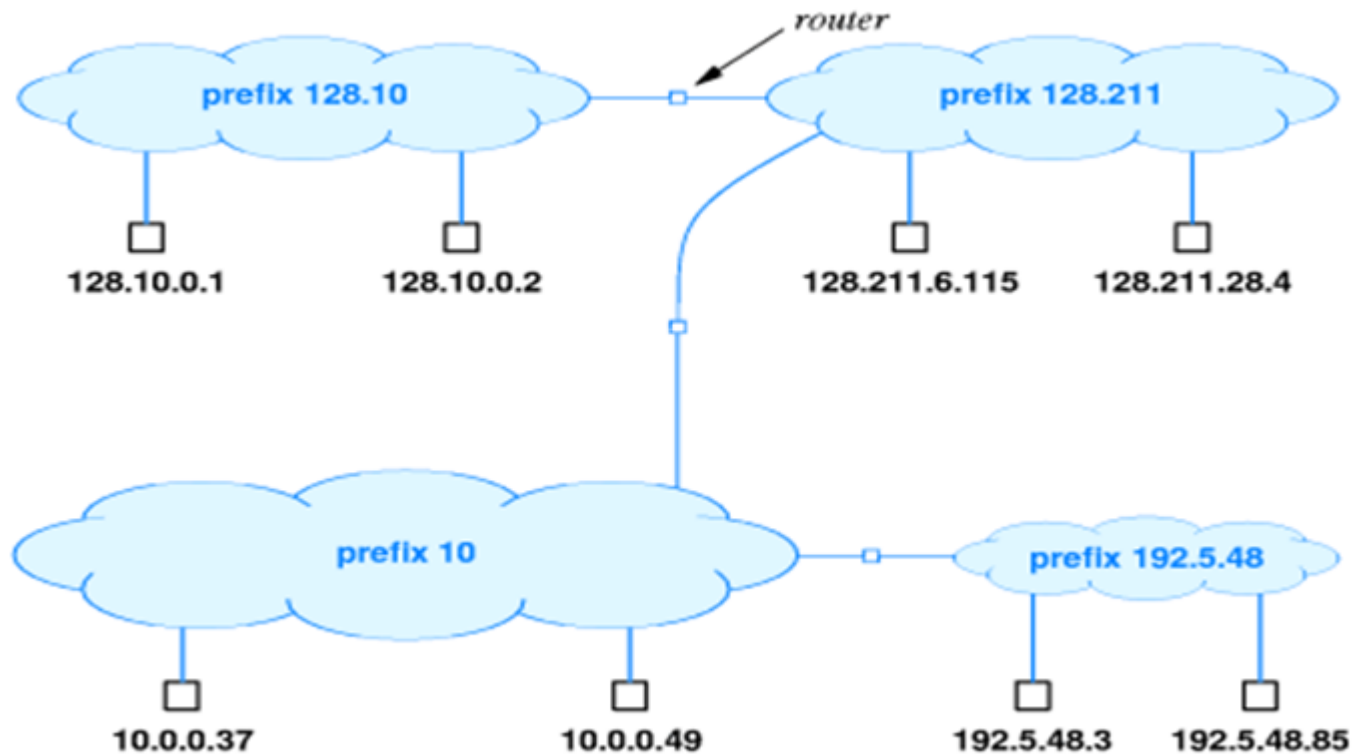
- Clase A: (1 octeto + 3 octetos)
  - 7 bits para identificar la red = 128 redes
  - Entre las direcciones 1.x.x.x y 126.x.x.x.
- Clase B: (2 octetos red + 2 octetos host)
  - 14 bits para identificar la red= 16.384 redes
  - Entre las direcciones 128.x.x.x y 191.x.x.x.
- Clase C: (3 octetos red + 1 octeto host)
  - 21 bits para identificar la red= 2.097.152 redes
  - Entre las direcciones 192.x.x.x y 223.x.x.x.
- Clase D: (multicast, 28 bits para identificar al grupo de difusión)
  - A partir de 224.x.x.x



# Máscaras

- En el direccionamiento con clases el identificador de host y el de red está predeterminado
- Se pueden suelen usar **máscaras**
  - Son números de 32 bits (como las IP) compuestos por 1s contiguos (identifican la red) y 0s contiguos (identifican el id de host)
  - Para el direccionamiento clásico, son máscaras por defecto para cada clase:
    - Clase A: **255.0.0.0**
    - Clase B: **255.255.0.0**
    - Clase C: **255.255.255.0**
  - Notación
    - 150.214.108.30/24 → 24 bits a 1

# Ejemplo ¿De qué clase son estas redes?



# Las direcciones IPv4 se han acabado

## ■ Problemas

- Necesidad de emplear varias redes clase C juntas
- Direcciones clase A, B asignadas pero sin usar completamente
- Según previsiones de los años 90, las direcciones de 32 bits estarían agotadas en 2008. Las últimas se asignaron hace poco

## ■ Soluciones

- Nuevos esquemas de direccionamiento: CIDR (asignación de paquetes de direcciones sin usar clases -classless interdomain routing)
- Direcciones privadas con acceso a Internet: proxy, NAT y DHCP
- Nuevo protocolo IPv6 (direcciones de 128 bits)

## IANA entrega los últimos paquetes con direcciones de Internet IPv4

Es urgente que los proveedores de acceso hagan la transición al protocolo IPv6 que admite 340 sextillones de direcciones

Fuente: El País  
3/2/2011

# Direccionamiento IP moderno

- Con el esquema clásico se desperdiciaban direcciones, así que ahora se asignan direcciones sin clase (CIDR: classless interdomain routing)
- Para un mejor ajuste, se utilizan las **máscaras de subred**:
  - Son un conjunto de bits a 1 que indican qué parte de la dirección es de la red
  - Notación decimal con puntos. Ejemplo: Red 14.0.0.0 con máscara 255.255.255.0 --> los tres primeros bytes corresponden a la red (14.0.0) y el último byte identificará al host (es la máscara para una dirección clásica de tipo C).
  - Notación con barra: 14.0.0.0/24 -> los 24 primeros bits de la dirección IP identifican a la red. En este ejemplo, la máscara es la misma que en el anterior
  - Ejemplo: ¿pertenece esta IP: 130.197.16.132 a la red 130.197.16.128/25?

○ La IP en binario es 130.197.16.132	= 10000010.11000101.00010000.10000100
○ La máscara es 255.255.255.128 y en binario	= 11111111.11111111.11111111.10000000
○ Al hacer el AND binario de las dos resulta	= 10000010.11000101.00010000.10000000

que, efectivamente, corresponde a la subred es 130.197.16.128

# Direcciones IP especiales

- Direcciones reservadas que nunca se asignan a hosts

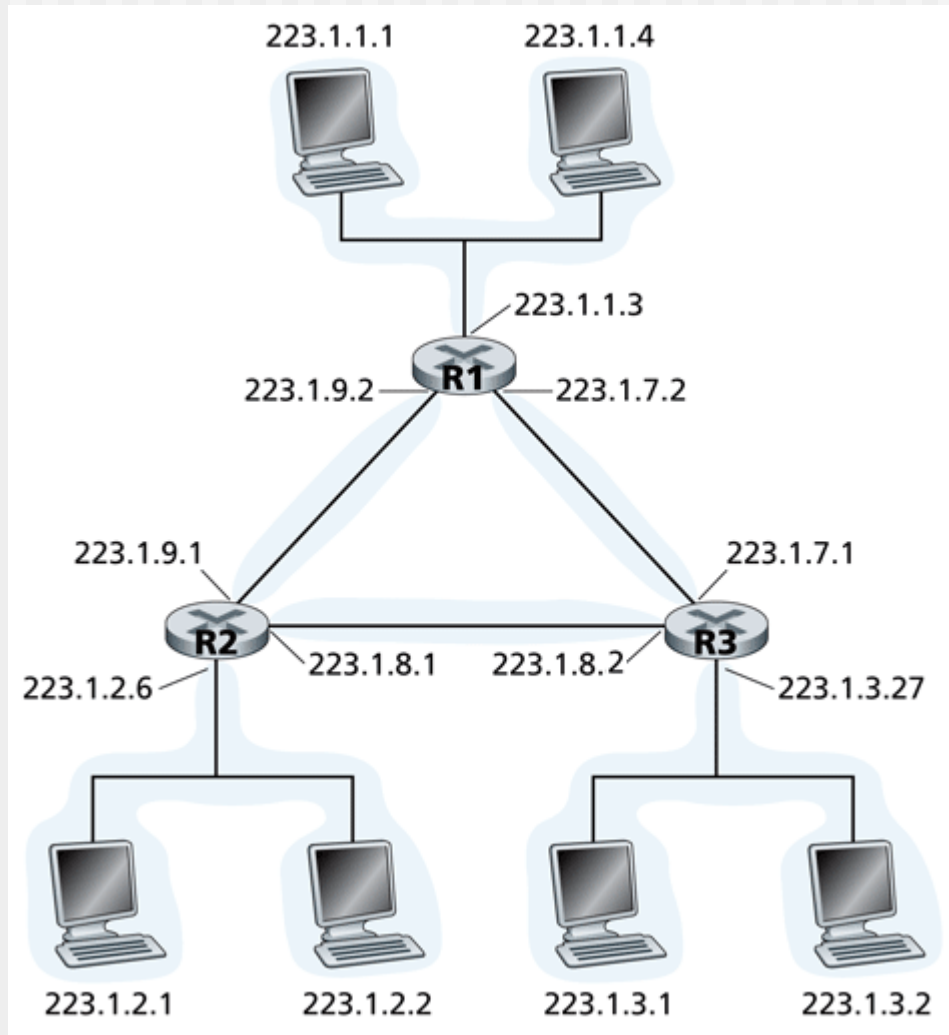
Los datagramas con estas IP destino NO atraviesan el router

- 0.0.0.0 el propio host, se usa en arranque
- Red + todos 1 broadcast directo
- 255.255.255.255 broadcast limitado a la subred
- 127.x.x.x Loopback (ej. 127.0.0.1)

# Direcciones privadas

- Direcciones en cada clase que no están asignadas. No está permitido enrutarlas
  - Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
  - Clase B: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
  - Clase C: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).
- Para atravesar el router, los datagramas con origen IP privada necesitan usar la técnica NAT (Network Address Translation)

# Ejemplo: ¿Cuántas redes hay?



## Ejemplos con máscaras de subred

Número de direcciones IP necesarias	Número de bits de máscara	Máscara resultante
hasta 2	30	255.255.255.252
hasta 6	29	255.255.255.248
hasta 14	28	255.255.255.240
hasta 30	27	255.255.255.224
hasta 62	26	255.255.255.192
hasta 126	25	255.255.255.128



# ¿Qué debo tener claro hasta aquí?

- ¿Qué partes tiene una dirección IP?
- ¿Qué diferencia hay entre las IP con clase y sin clase? ¿Por qué existen ambas?
- ¿Qué es una máscara de red (también llamada de subred) y para qué se utiliza?
- ¿Qué es el concepto de broadcast?
- ¿Por qué hay direcciones IP públicas y privadas?

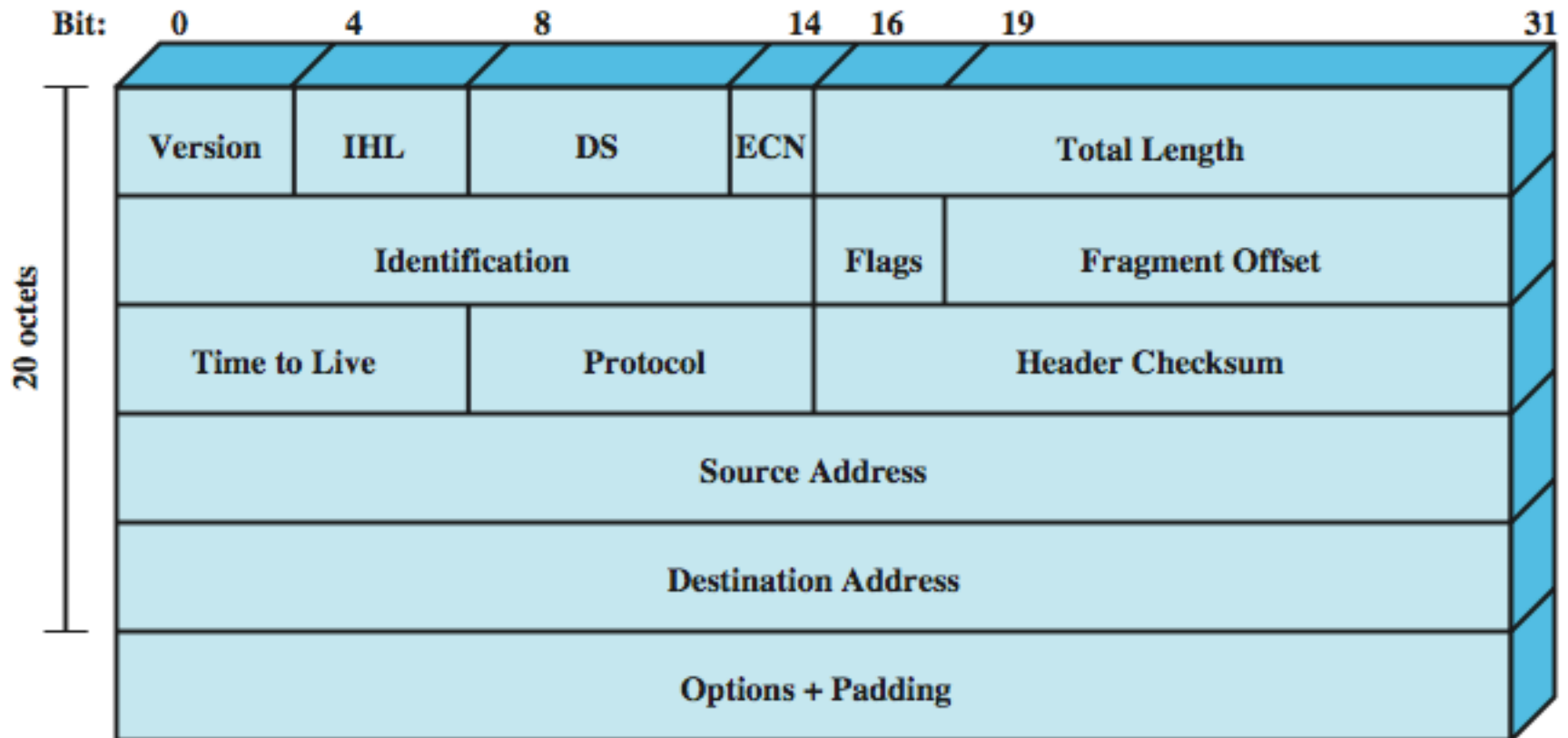
# Protocolo IP (version 4)

- Forma parte del conjunto de protocolos de TCP/IP, y es el protocolo más usado de interconexión de redes
- Servicios:
  - IP proporciona dos funciones para que las use la capa superior:
    - Envío: para solicitar la transmisión de una PDU de nivel de transporte
    - Entrega: para notificar a un usuario la llegada de una PDU

Envío( Dirección origen,  
Dirección destino,  
Protocolo,  
Indic. tipo servicio,  
Identificador,  
Ident. no fragmentación,  
Tiempo de vida,  
Longitud de datos,  
Datos de opción,  
Datos,  
);

Entrega( Dirección origen,  
Dirección destino,  
Protocolo,  
Indic. tipo servicio,  
  
Longitud de datos,  
Datos de opción,  
Datos  
);

# Formato del datagrama IPv4



# Formato del datagrama IP (II)

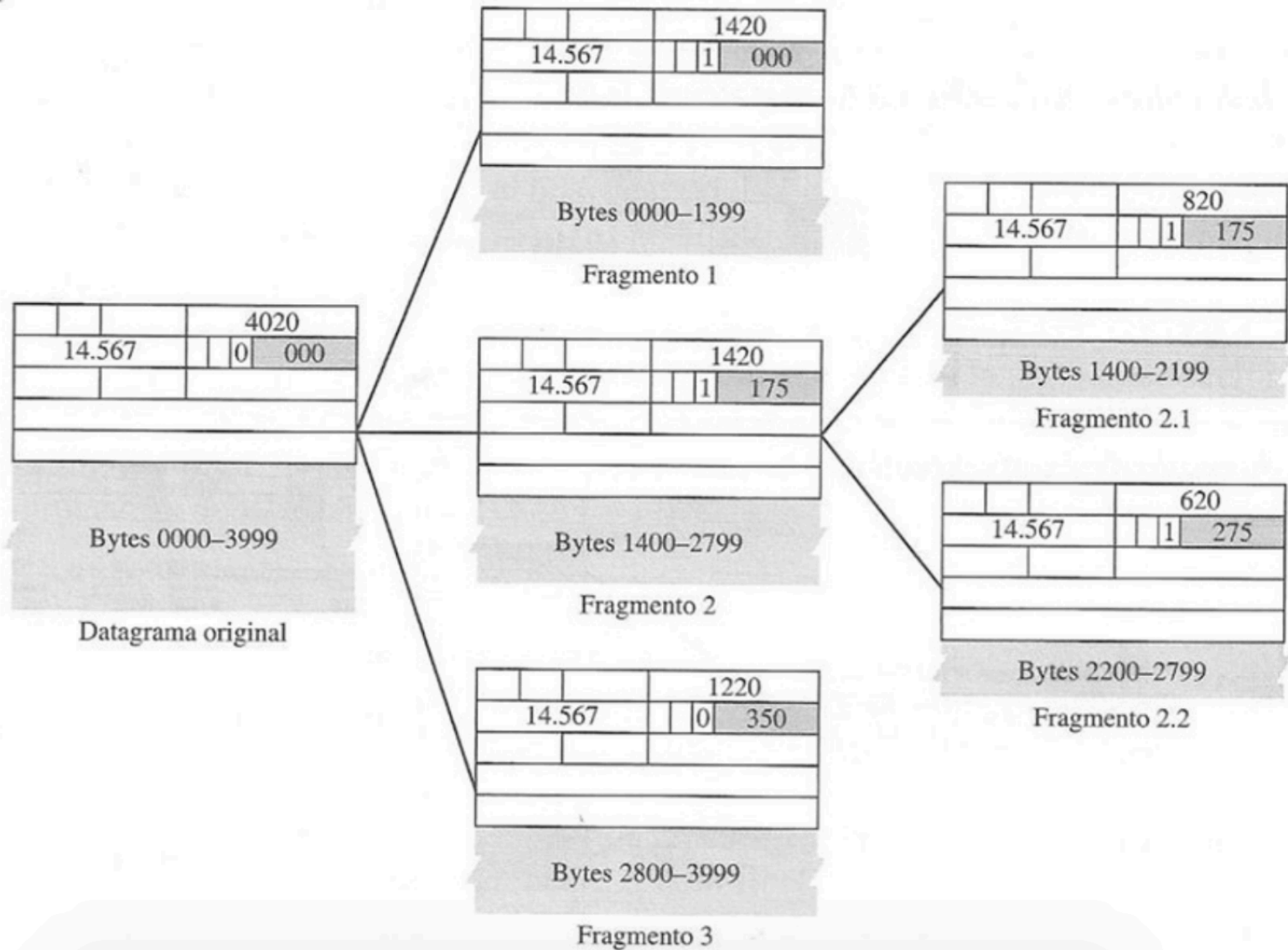
## ■ Campos del datagrama:

- Versión: Lleva el registro de la versión del protocolo al que pertenece el datagrama. El valor 4 indica el IPv4 (normal) y El valor 6 es el IPv6
- Longitud de la cabecera Internet (IHL): Longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es 5. El máximo (15) limita la cabecera a 60 bytes
- DS/ECN:
  - DS para gestión de servicios diferenciados (calidad de servicio en IP)
  - ECN: explicit congestion notification (estándar para notificaciones sobre el grado de congestión de los enlaces)

## Formato del datagrama IP (III)

- **MTU:** Maximum Transmission Unit o Unidad de Transferencia Máxima
  - Tamaño máximo del campo de datos (payload) de un paquete en una capa de una pila de protocolos
  - Depende de cada protocolo
    - Ethernet: 1500 bytes
- Campos del datagrama:
  - Longitud total: longitud total de cabecera y datos. El máximo es de 65 Kbytes
  - Identificador: Para que el host de destino determine a qué datagrama pertenece el fragmento recién llegado
  - Flags (Indicadores): tres bits con información
    - 1- bit no se usa
    - 2- DF (Don't fragment). con 0 se permite la fragmentación, con 1 no se permite
    - 3- MF (More fragments) Un 0 significa que se trata del último fragmento del datagrama; Un 1 que no es el último.
  - Desplazamiento del fragmento: Indica en qué parte del datagrama actual va este fragmento

# Ejemplo de fragmentación



## Formato del datagrama IP (IV)

### ■ Campos del datagrama:

- Tiempo de vida (TTL): Medido en saltos de dispositivos de encaminamiento (routers). Cuando el contador llega a cero, el paquete se descarta y se envía un paquete de aviso al host de origen
- Protocolo: Indica la capa a la que debe entregarse el datagrama una vez ensamblado. 1: ICMP, 6: TCP, 17: UDP, etc.
- Suma de comprobación de la cabecera: Se verifica y recalcula en cada dispositivo de encaminamiento. Es el complemento a uno de la suma complemento a uno de todas las palabras de 16 bits de la cabecera
- Dirección origen y Dirección destino: Número de red y número de host de origen y destino

# Formato del datagrama IP (V)

## ■ Campos del datagrama:

### ○ Opciones:

- De longitud variable
- Para incluir información no presente en el diseño original del protocolo IP
- Un byte inicial identifica el tipo de opción

### • Ejemplos:

- Opción "Registro de la ruta": Se registra la secuencia de dispositivos de encaminamiento por los que atraviesa el datagrama
- Opción "Sello de tiempo": Los dispositivos de encaminamiento incorporan una sello de tiempo y su dirección IP cuando el datagrama pasa por ellos



# ¿Qué debo tener claro de esta parte?

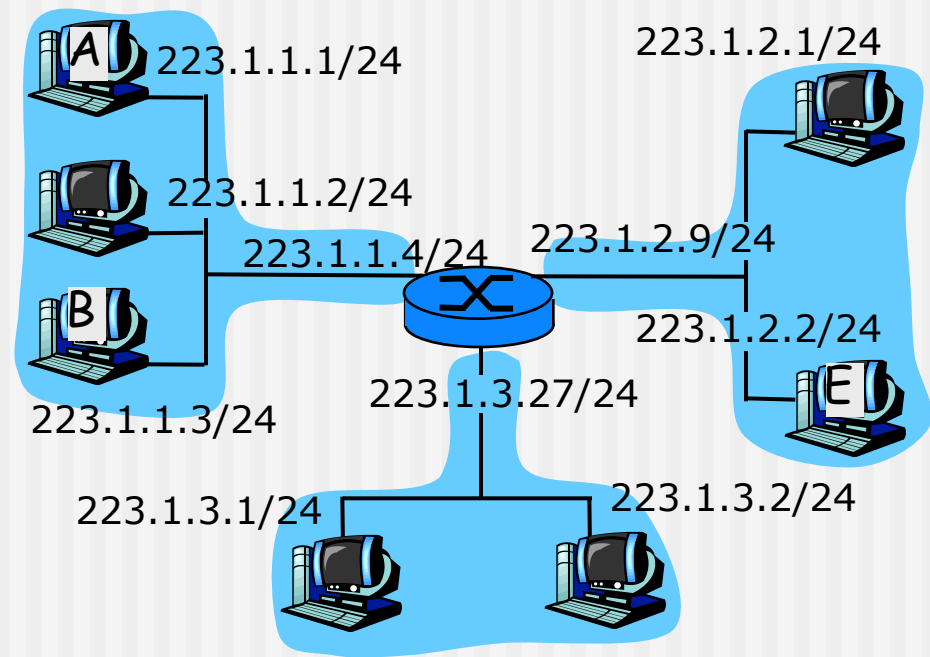
- ¿Cuál es la diferencia entre el campo hlen y el campo longitud total?
- ¿Qué pasa si un datagrama intenta atravesar una red donde no cabe? ¿Qué es la MTU de una red?
- Si un datagrama debe atravesar un router y sigue su camino, ¿cuántos campos de la cabecera debe cambiar el router antes de depositarlo en la siguiente red?

# Contenidos

- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- Interconexión en redes IP
- Protocolo IPv4
  - Direcciones IP. Máscaras de subred
  - **Tablas de encaminamiento**
- Protocolos asociados a IPv4
  - ARP
  - ICMP
- Nivel de Transporte: protocolos UDP y TCP

# Tablas en routers y hosts

Ejercicio: dibuja la tabla de encaminamiento de los ordenadores A, E y del router



Destino	Máscara	Pasarela	Interfaz de salida
...		...	...



# Misión del router IP (básica)

1. Recibe una trama destinada a su dirección MAC, pero con una IP distinta a la suya
2. Decrementa en 1 el campo TTL de la cabecera IP
3. Inspecciona la tabla de encaminamiento para determinar por dónde enviar el datagrama
4. Genera fragmentos si el datagrama no cabe por la red de salida
5. En cada trama de nivel de enlace, la dirección MAC origen es la del interfaz de salida del router
6. La dirección MAC destino de la/s trama/s es la dirección MAC del próximo nodo de salto
7. Recalcula los checksums del datagrama IP (o fragmentos) y de la/s trama/s de nivel dos (en este orden)
8. Coloca la/s trama/s en la cola del interfaz de salida correspondiente

# Creación de tablas de encaminamiento

- Elementos de la red:
  - Se distinguen routers y nodos finales
  - Los nodos finales no sirven para reenviar datagramas (forwarding) y, por tanto, sólo encamina los datagramas que él mismo genera
  - Salida a Internet
    - Si la hay, pueden aparecer datagramas que no van destinados a ningún equipo de la red y para los cuales hay que definir también una regla en la tabla.
    - Si no la hay, se asume que todos los datagramas que se generan son equipos existentes en la red.
  - Pueden existir ciclos en la red, con lo que hay que determinar caminos más cortos

# Creación de tablas de encaminamiento

Destino	Máscara	Pasarela	Interfaz de salida
...		...	...
...		...	...

## ■ Elementos una tabla de encaminamiento:

### ○ Columnas

#### • Destino y máscara

- Dirección IP de destino a la que se envía el datagrama
- Máscara de la dirección IP
- Suelen aparecer juntas con una dirección de red: 150.214.108.**0**/24
- En la última regla en aplicarse aparece de la forma:
  - Default
  - 0.0.0.0/0.0.0.0

#### • Pasarela/Siguiente salto

- Dirección IP por la que se envía el datagrama
- Si el destino está en la misma red, aparece "Entrega directa"

#### • Interfaz de salida

- Dirección IP del interfaz de red por donde debe salir el datagrama para llegar al destino
- Es necesario puesto que los nodos pueden tener más de un interfaz de red (los routers, al menos, dos)

### ○ Filas

- Cada fila es una regla de encaminamiento
- Se aplican desde la más estricta a la más genérica

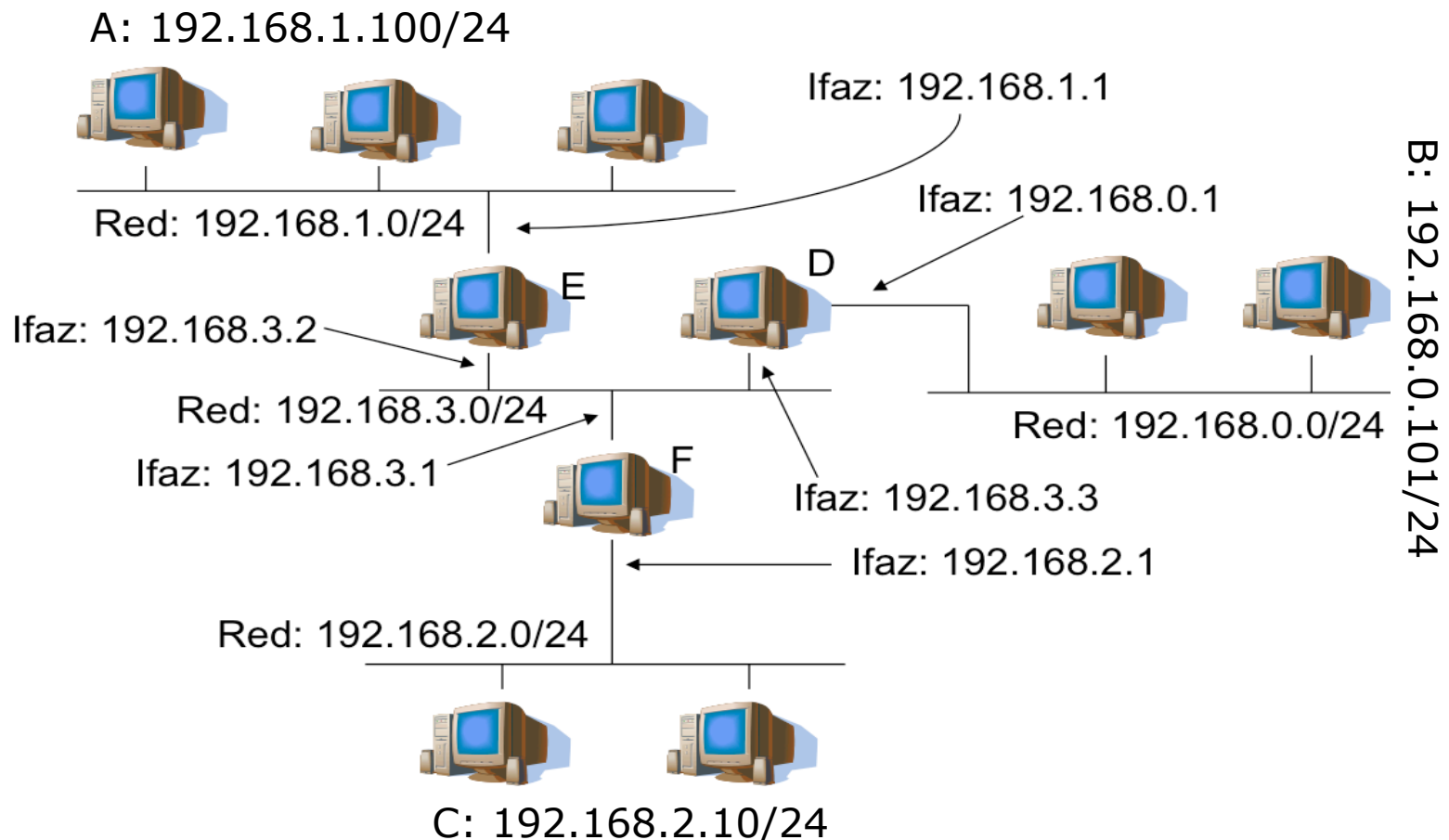
# Creación de tablas de encaminamiento

- Por cada router/host hay que seguir los siguientes pasos
- Procedimiento
  1. Añadir los posibles destinos (redes) y salida al exterior (si existe).
  2. Determinar el siguiente salto
    1. Entrega directa (si se está en la misma red), o
    2. Entrega indirecta (puerta de enlace para el siguiente salto)
    3. Ciclos, en caso de existir varios caminos para llegar a un destino, se ha de elegir el camino más corto
  3. Determinar el interfaz de salida
  4. Reducir la tabla

# Tablas en routers y hosts

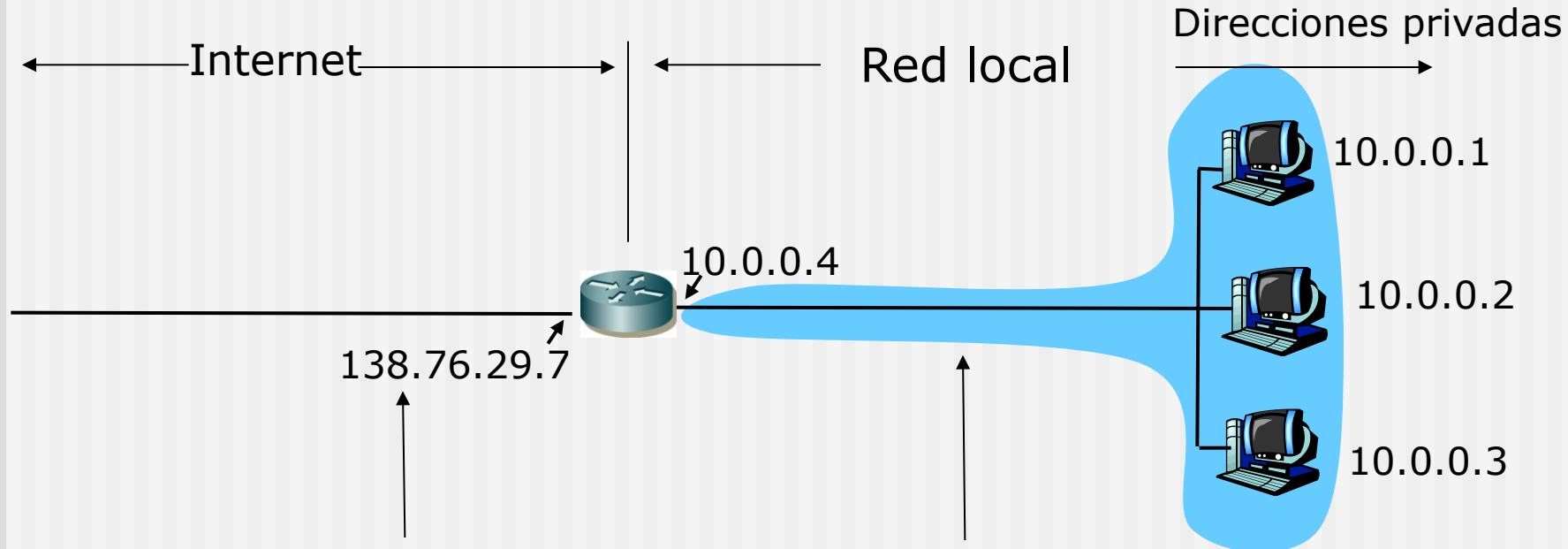
Ejercicio: dibuja la tabla de encaminamiento de los hosts A, B y C, y de los routers D, E y F.

Destino	Máscara	Pasarela	Interfaz de salida
...		...	...





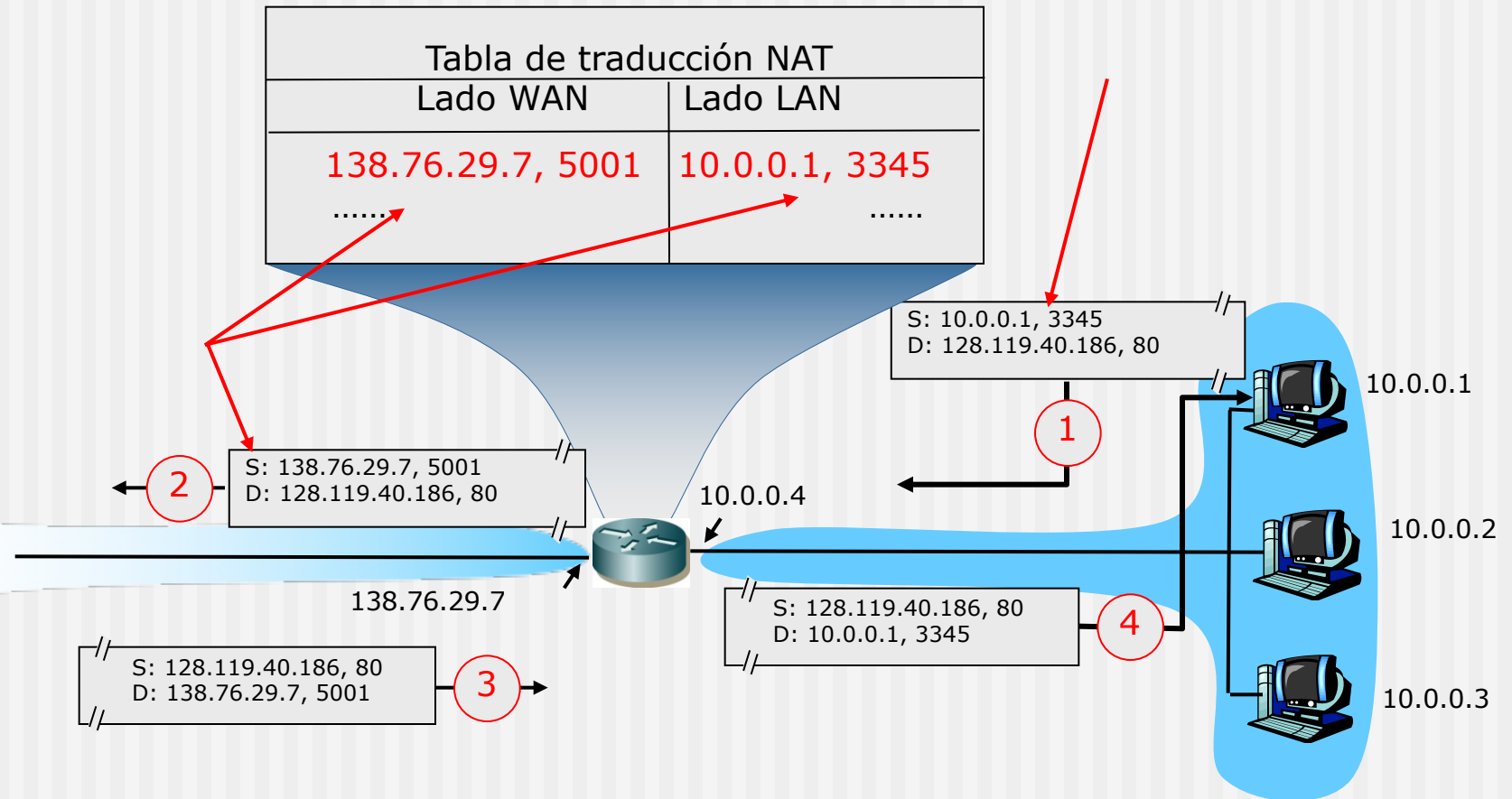
# Cómo funciona NAT



*Todos* los datagramas *que abandonan* la red local tienen la misma IP origen NAT: 138.76.29.7, y diferentes puertos origen

Los datagramas con origen o destino en esta red no cambian

# Cómo funciona NAT (II)



# Contenidos

- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- Interconexión en redes IP
- Protocolo IPv4
  - Direcciones IP. Máscaras de subred
- **Protocolos asociados a IPv4**
  - ARP
  - ICMP
- Nivel de Transporte: protocolos UDP y TCP

# Protocolo ARP (Address Resolution Protocol)

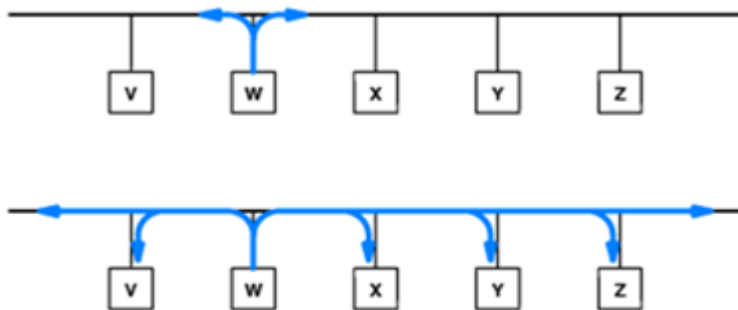
- La correspondencia entre dirección IP y dirección física (p.e. Ethernet), se guarda en una tabla
- Un router/host usa la información de esta tabla antes de enviar un paquete IP encapsulado en una trama de nivel de enlace
  - La IP destino del datagrama o la IP del router indican la MAC destino de la trama
- La resolución es local y nunca se puede guardar la dir. física de un nodo remoto más allá de la propia red
- Si la información no está en la tabla
  - Se usa el protocolo de resolución ARP (para preguntar en la red quién tiene la dirección física buscada)

IP	Física (MAC)
223.1.1.2	0A:07:4B:12:82:36
223.1.1.4	0A:9C:28:12:82:8D

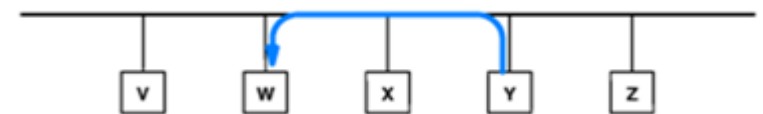
# Protocolo ARP (II)

## ■ ¿Cómo funciona ARP?

1. Envío de ARP petición a todos los equipos de la red
  - La petición consiste en un paquete ARP encapsulado en una trama de enlace, cuyo campo destino es la dirección física de broadcast de la red (para que todos la reciban)
  - El paquete ARP contiene esta pregunta: ¿qué dirección física tiene el equipo con esta IP?
2. Procesamiento a nivel ARP en todos los hosts/routers
  - Cada nodo comprueba si la IP solicitada corresponde con la suya
3. Respuesta desde el nodo que cumpla esta condición
  - Envío directo al nodo que hizo la petición (con su dirección física como origen)
4. La correspondencia se almacena en la tabla ARP



1. El equipo con IP W pregunta:  
¿Qué MAC tiene el equipo cuya  
IP es Y?

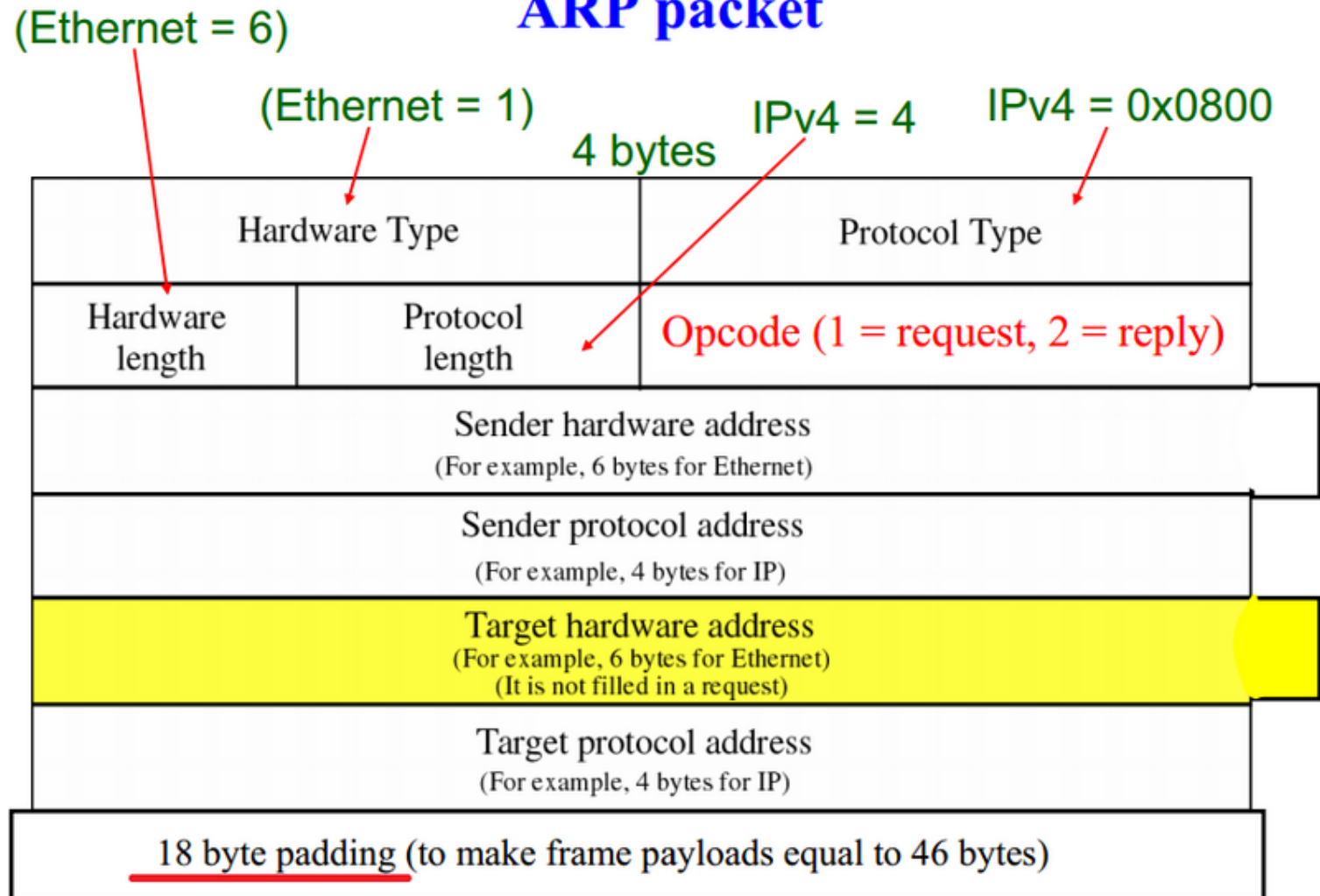


2. Y responde con su MAC  
a la estación W

# Protocolo ARP (III)

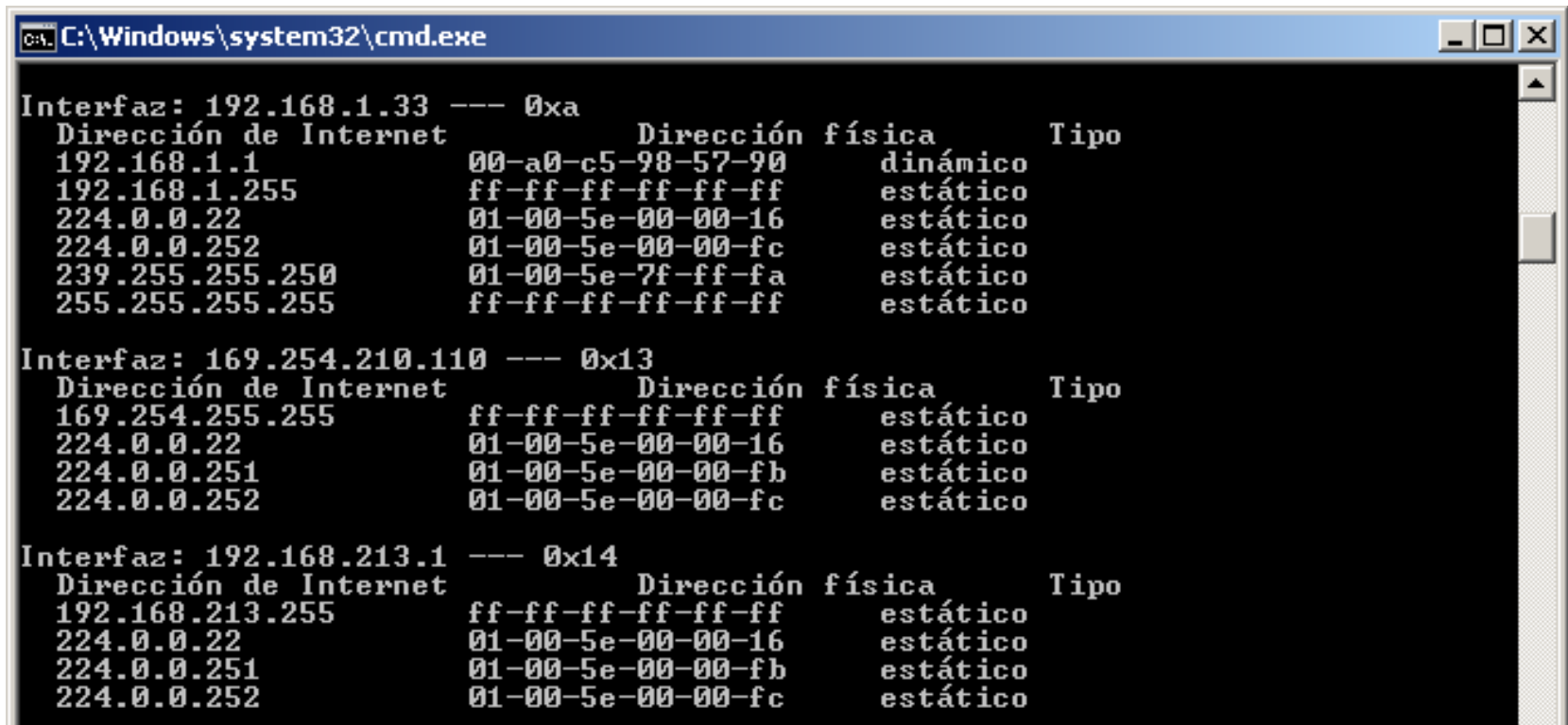
7-5

## ARP packet



# Protocolo ARP (IV)

- Comando de consola **arp** disponible para monitorizar y gestionar la resolución.
- Ejemplo: `arp -a` (muestra la tabla de correspondencias por cada interfaz del nodo)



```
C:\Windows\system32\cmd.exe

Interfaz: 192.168.1.33 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.1.1                00-a0-c5-98-57-90     dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16     estático
224.0.0.252                01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 169.254.210.110 --- 0x13
Dirección de Internet      Dirección física      Tipo
169.254.255.255            ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16     estático
224.0.0.251                01-00-5e-00-00-fb     estático
224.0.0.252                01-00-5e-00-00-fc     estático

Interfaz: 192.168.213.1 --- 0x14
Dirección de Internet      Dirección física      Tipo
192.168.213.255            ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16     estático
224.0.0.251                01-00-5e-00-00-fb     estático
224.0.0.252                01-00-5e-00-00-fc     estático
```

# Diagnóstico de la red

Algunas herramientas software (comandos del sistema operativo) para conocer/modificar las direcciones e información de encaminamiento

- ping

- Determina si un nodo está accesible o no

- traceroute (tracert en Windows)

- Muestra ruta origen-destino con todos los routers por los que se pasa

- ifconfig (ipconfig en Windows)

- Información/Gestión de interfaces de red

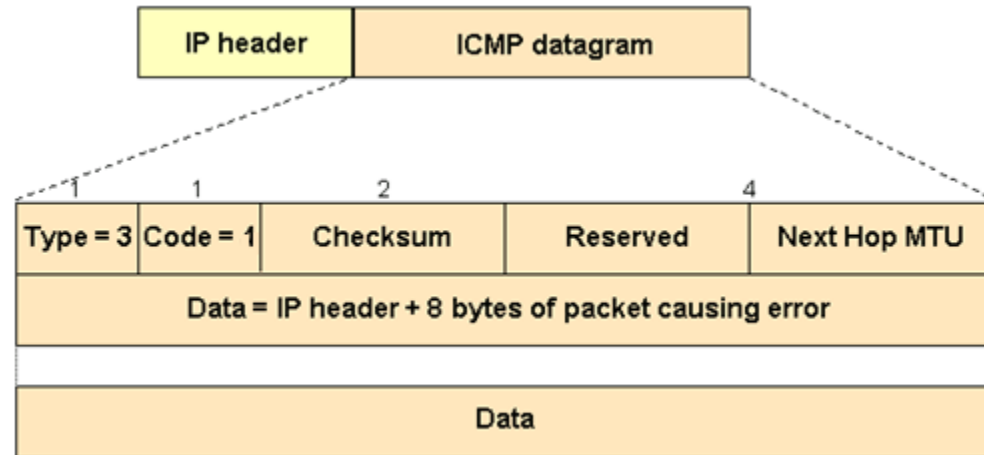
- route

- Información/Gestión de tablas de encaminamiento



# Protocolo ICMP

- Internet Control Message Protocol
- Empleado por routers y host para comunicación a nivel de red
  - Informe de errores: host, red o protocolo no alcanzable
  - Pregunta/respuesta de echo (utilizado en ping)
- Protocolo "sobre" IP:
  - Los mensajes ICMP se transportan dentro de datagramas IP
- **Mensaje ICMP** : tipo + código + parte del datagrama IP que causa el problema



Tipo	Código	Descripción
<b>0</b>	<b>0</b>	<b>echo reply (ping)</b>
3	0	dest. network unreachable
<b>3</b>	<b>1</b>	<b>dest host unreachable</b>
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
<b>8</b>	<b>0</b>	<b>echo request (ping)</b>
9	0	route advertisement
10	0	router discovery
<b>11</b>	<b>0</b>	<b>TTL expired</b>
12	0	bad IP header

# Contenidos

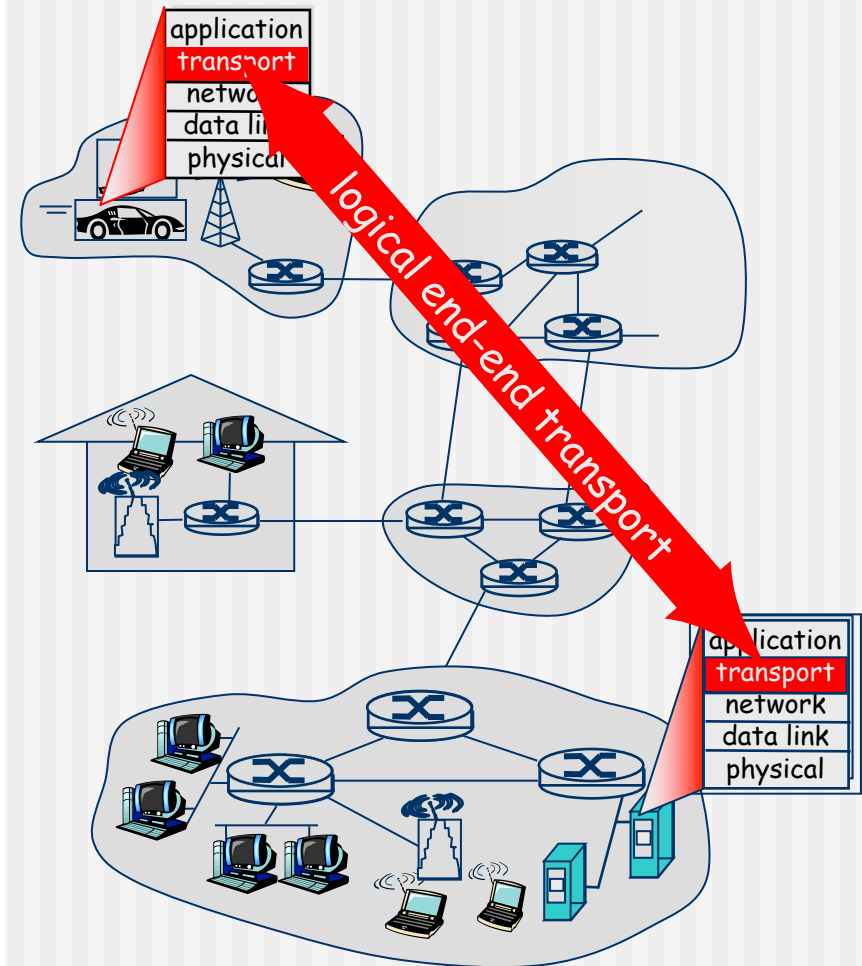
- Capas de protocolos
- Arquitectura TCP/IP
  - Direccionamiento en la pila TCP/IP
- Interconexión en redes IP
- Protocolo IPv4
  - Direcciones IP. Máscaras de subred
- Protocolos asociados a IPv4
  - ARP
  - ICMP
- **Nivel de Transporte: protocolos UDP y TCP**

# Protocolos de transporte

- Funciones de la capa de transporte:
  - (diálogo extremo-a-extremo)
- Protocolos de la capa de transporte en Internet
  - Protocolo UDP
  - Protocolo TCP

# Funciones de la capa de transporte

- Comunicación extremo-a-extremo de datos entre aplicaciones
- Multiplexado / demultiplexado para las aplicaciones
- Fiabilidad de la transferencia (recuperación de errores)
- Control de flujo, de congestión y otros parámetros de calidad en la comunicación (velocidad, retardo, tasa de errores, etc.)
- Si la capa de transporte ofrece servicio de conexiones:
  - establecimiento/ liberación/ recuperación ante caídas
  - aunque la capa de red sea no orientada a conexión



# Protocolos de transporte en Internet

## ■ Protocolo UDP

- Envío sin garantías adicionales a las ofrecidas por IP
- Se emplea en aplicaciones que no requieren fiabilidad total y necesitan evitar sobrecarga (multimedia en la red)

## ■ Protocolo TCP:

- Conexiones con control total de errores
- Empleado en aplicaciones que requieren fiabilidad de los datos (telnet, ftp, web, correo smtp)

## ■ Otros protocolos:

- SCTP (Stream Control Transmission Protocol) (2000)
  - Híbrido entre TCP y UDP
- DCCP (Datagram Congestion Control Protocol) (2006)
  - No fiable, como UDP, pero con control de congestión

# Protocolos de transporte en Internet

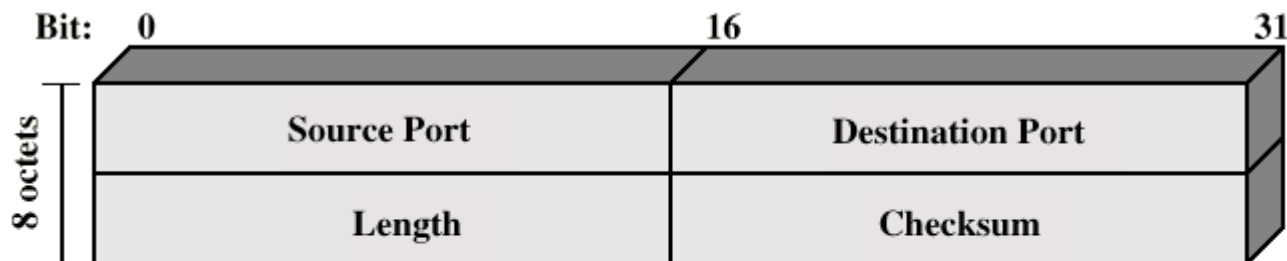
- Características comunes a UDP y TCP
  - Uso de **puertos** para multiplexación/demultiplexación y para identificar las aplicaciones
  - Las aplicaciones siguen el esquema cliente-servidor, con asignación pública de puertos en los servidores
  - Bloqueo de puertos como mecanismo de seguridad
  - Uso del interfaz **socket** (proporcionado por el sistema operativo) para acceso a los servicios desde diferentes lenguajes (C, C++, Java, etc.)

# Protocolo UDP

## ■ Funciones

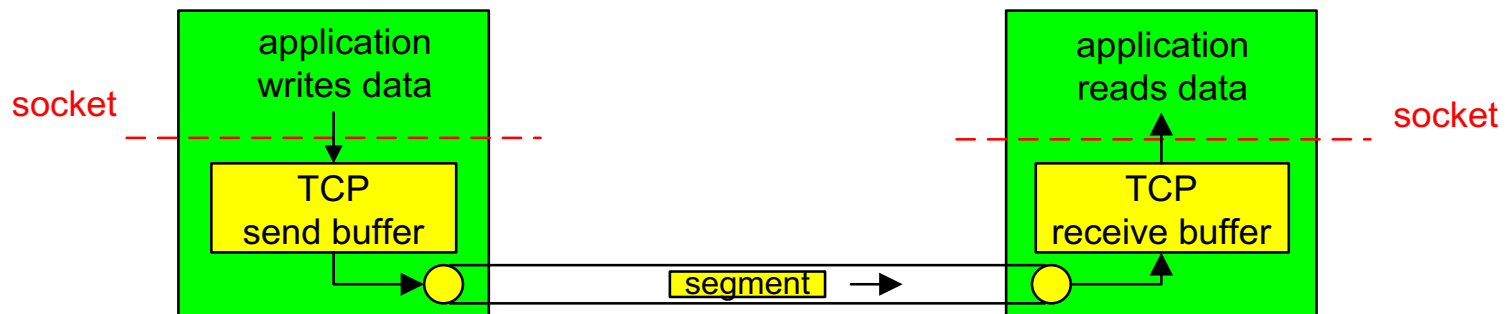
- Ofrece servicio de envío/recepción de datagramas para varios procesos en un host
- No añade calidad a IP (es un protocolo no fiable no orientado a conexión)
- Reduce la sobrecarga
- Aplicaciones: gestión de red (snmp), multimedia (videostreaming/audio), resolución de nombres (dns)

## ■ Cabecera del segmento UDP (datagrama de usuario):



# Características generales de TCP

- Orientado a conexión punto a punto
- Fiabilidad completa en la recepción de datos
- Conexiones full-duplex (en ambos sentidos)
- Interfaz tipo “flujo de bytes” (stream), y no de datos estructurados
- Uso de buffers en envío y recepción para optimizar la comunicación





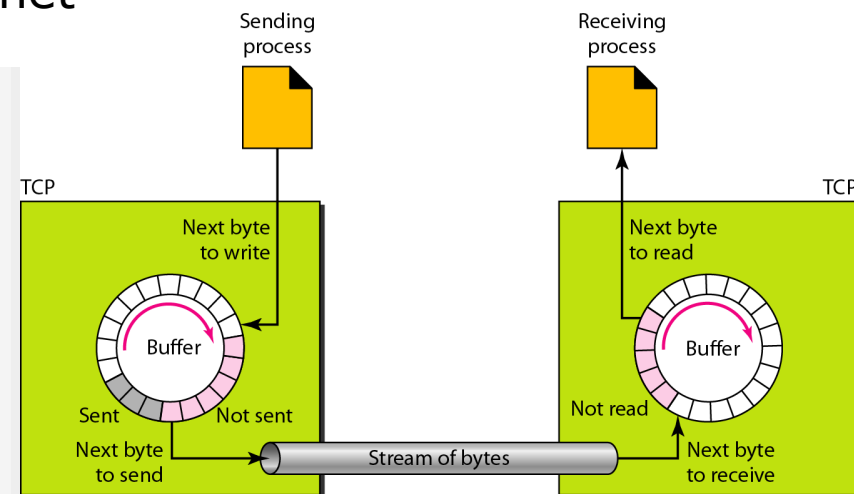
# Características generales de TCP

## ■ Buffering

- Los **segmentos TCP** se envían a un buffer de envío
- TCP enviará los datos en el buffer de envío cuando lo estime oportuno
- Existe también un buffer de recepción

## ■ MSS (*Maximum Segment Size*)

- Máxima cantidad de datos que puede llevar un segmento TCP
- Se negocia durante el establecimiento de conexión
- Depende de la implementación
- Ejemplo: 1460 bytes en ethernet



# Formato del segmento TCP

Offsets	Octeto	0								1								2								3							
Octeto	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Puerto de origen																Puerto de destino															
4	32	Número de secuencia																															
8	64	Número de acuse de recibo (si ACK es establecido)																															
12	96	Longitud de Cabecera				Reservado				N S	C W R	E C R E	U R G	A C K	P S H	R S T	S Y N	F I N	Tamaño de Ventana														
16	128	Suma de verificación																Puntero urgente (si URG es establecido)															
20	160	Opciones (Si la Longitud de Cabecera > 5, relleno al final con "0" bytes si es necesario)																															
...	...																																

## Flags más importantes:

URG: datos urgentes

ACK: mirar el nº del ACK

PSH: envío inmediato

sin encolar el segmento

RST, SYN, FIN: conexiones

checksum 16  
de todo el  
segmento  
(como en UDP)

nº de bytes  
que se pueden  
aceptar para que  
lo sepa el otro  
extremo

Cuentan bytes  
ino segmentos!

# Números de secuencia y ACKs

## ■ Números de secuencia:

- TCP utiliza el **número de byte** para numerar los datos
  - TCP numera todos los bytes de datos que se transmiten
  - La numeración no comienza desde 0 → nº aleatorio  $[0 - 2^{32}-1]$
  - El número de secuencia es el del primer byte que transporta el segmento

Ejemplo:

Nº aleatorio = 1057

y el total de datos = 6000 bytes

→ Los bytes se enumeran de 1057 a 7056

- Si un segmento no lleva datos de usuario no consume número de secuencia
  - Excepción: segmentos de control (SYN y FIN de conexiones)

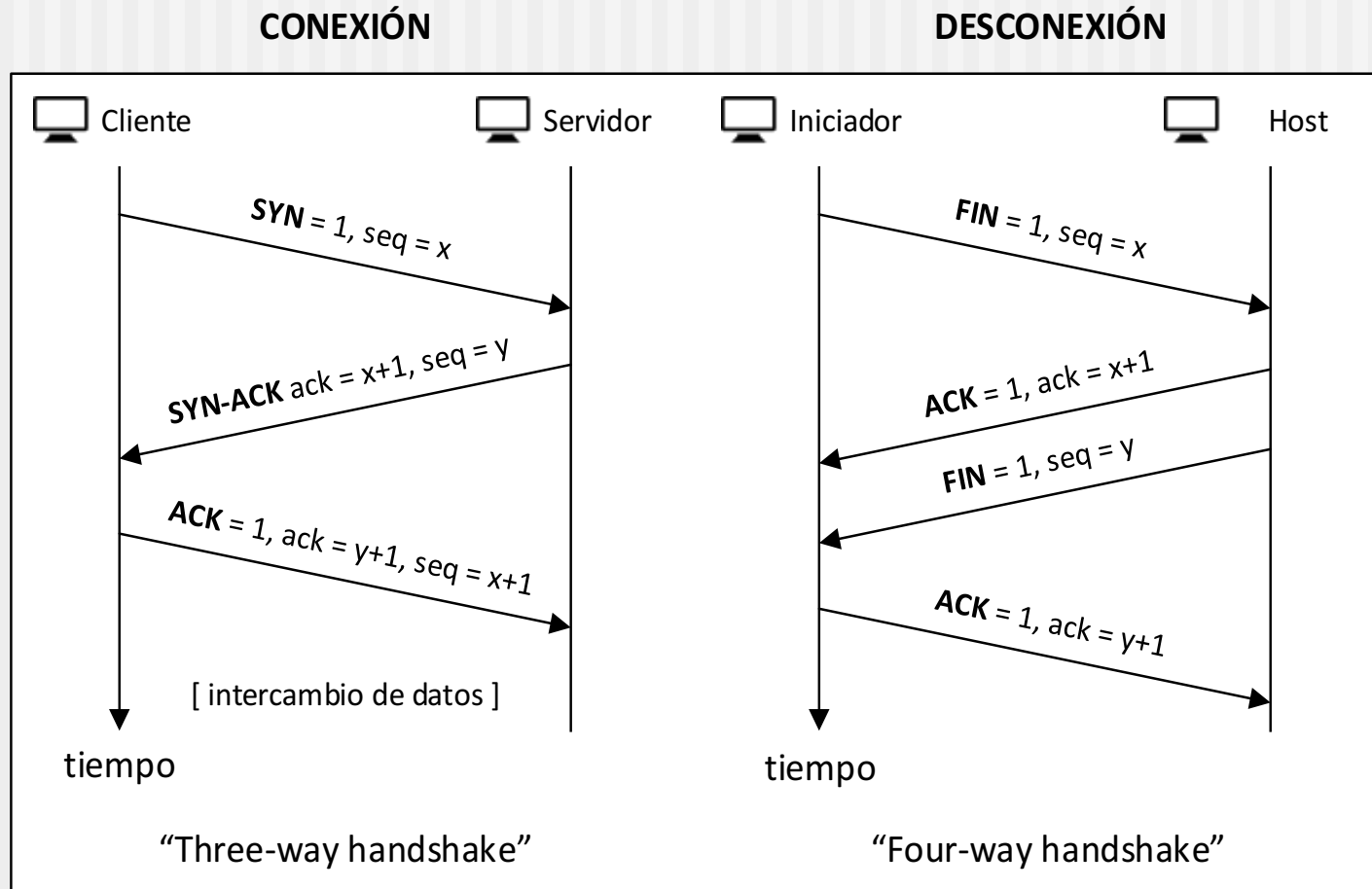
## ■ ACKs:

- Número de secuencia del siguiente byte que se espera recibir, reconociendo la llegada de todo lo anterior (acumulativo)

# Conexiones en TCP

- Funcionalidad ofrecida a las capas superiores:
  - Permite establecer una conexión activa
    - La inicia el **cliente**, previo conocimiento de la dirección IP y puerto en el que está esperando el servidor
  - O permite establecer una conexión pasiva
    - En el **servidor**, que espera conexiones de clientes
  - La conexión se crea completamente cuando se sincronizan el cliente y el servidor

# Conexión y desconexión en TCP



- Los segmentos SYN y SYN+ACK no llevan datos pero consumen números de secuencia
- En el caso de la desconexión, tanto el cliente como el servidor pueden iniciarla.

# Transferencia de datos en TCP (tiene que estar conectado)

## Campo Seq (nº secuencia):

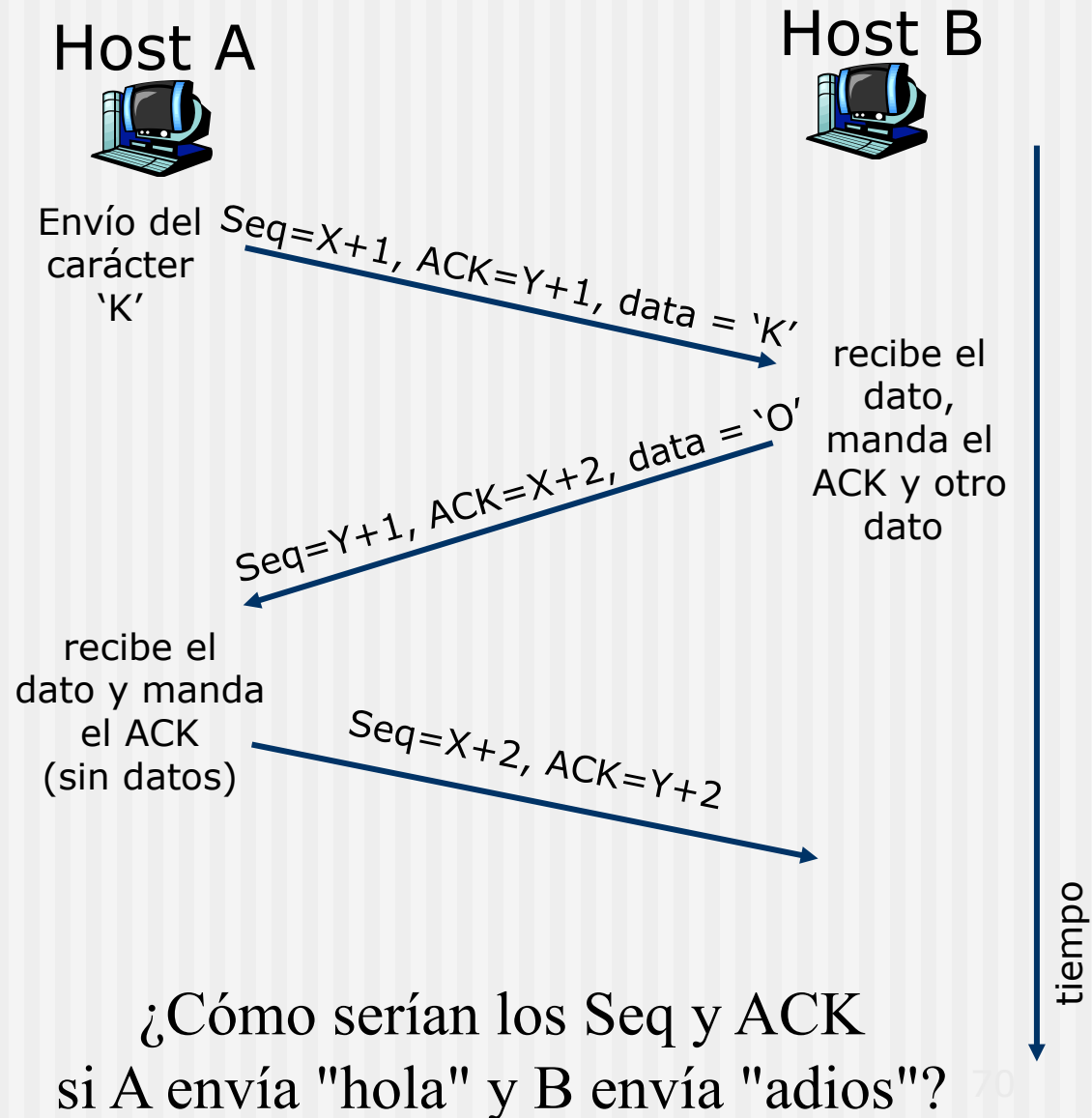
Se incrementa por cada byte de datos enviado

Campo ACK: indica el número de secuencia del siguiente byte de datos esperado

- El ACK es acumulativo, aceptando los datos anteriores a él

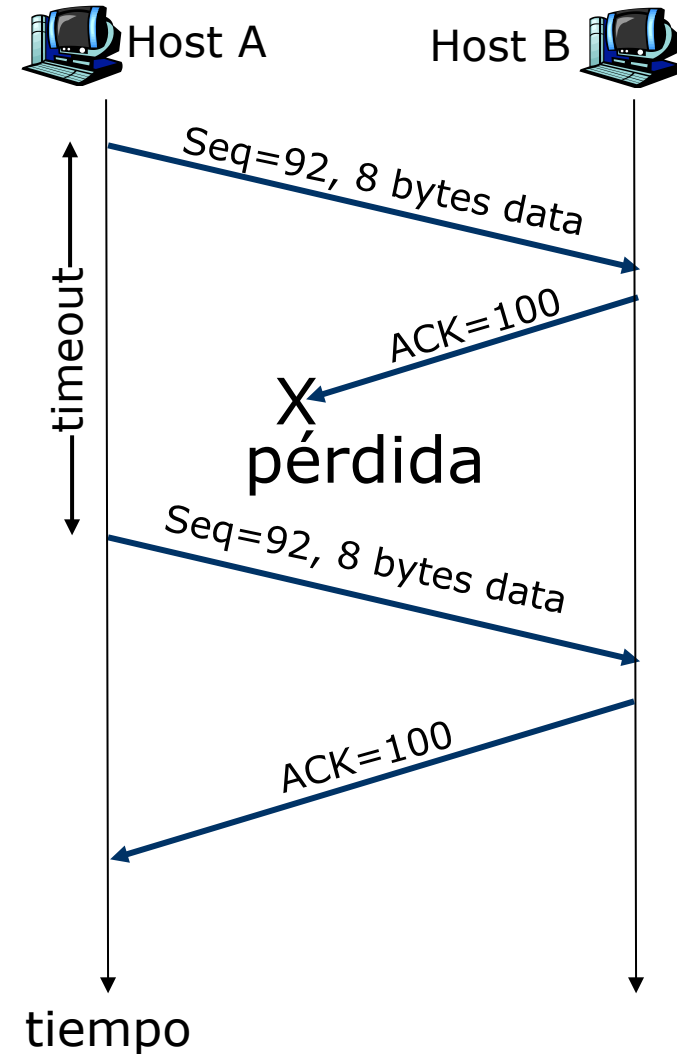
¿Y si llegan los segmentos fuera de orden?

Según la implementación se pueden almacenar o rechazar



# Fiabilidad y retransmisiones TCP: temporizadores

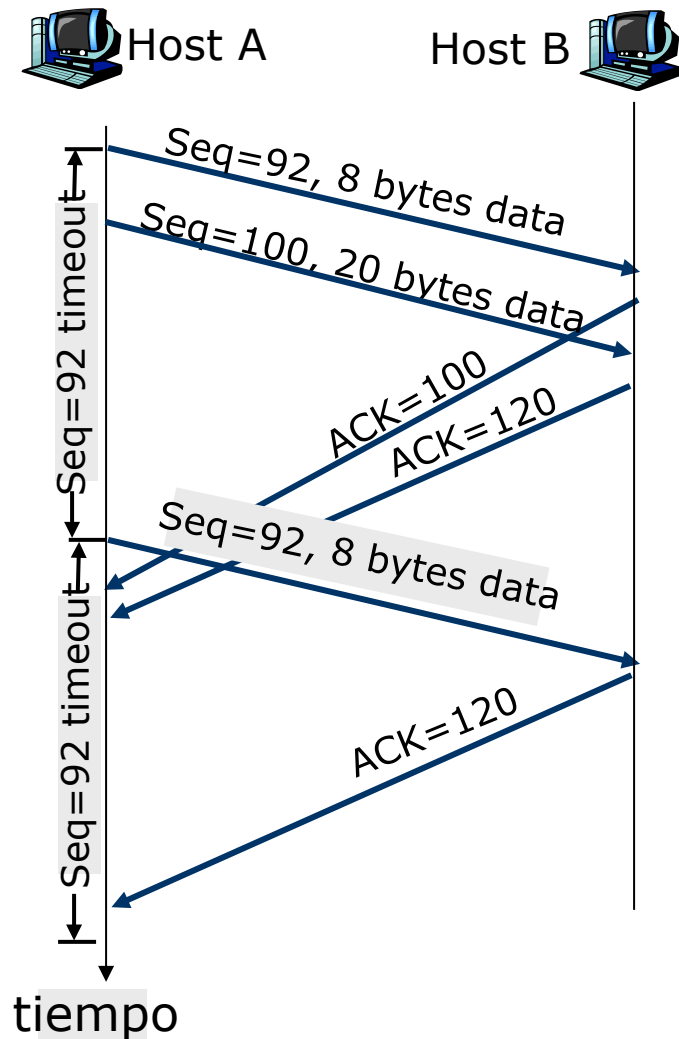
- Los paquetes perdidos se detectan mediante **timeouts**.
  - Se activa un temporizador cuando se envía un segmento.
  - Se cancela el temporizador cuando se recibe el ACK.
  - Si salta el temporizador, se retransmiten los datos perdidos.



Se pierde el ACK

# Fiabilidad y retransmisiones TCP: temporizadores

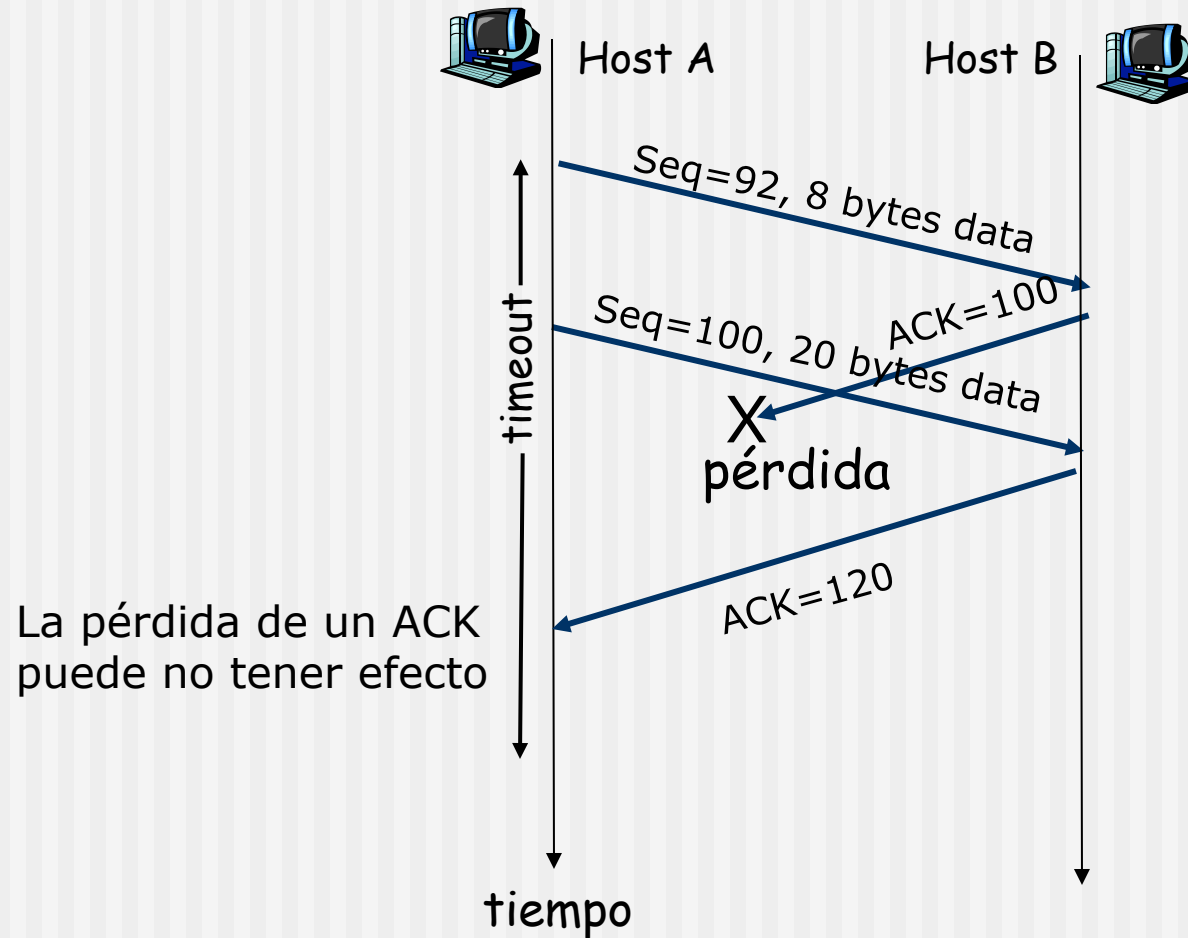
- Es importante elegir un valor apropiado para el timeout
  - Si es demasiado alto, perderemos mucho tiempo esperando, sin enviar datos (se desaprovecha la red).
  - Si es demasiado corto, reenviaremos segmentos innecesariamente.
  - Por eso, los temporizadores en TCP no son fijos, sino que se van adaptando a la velocidad de la red



Salta el timeout prematuro

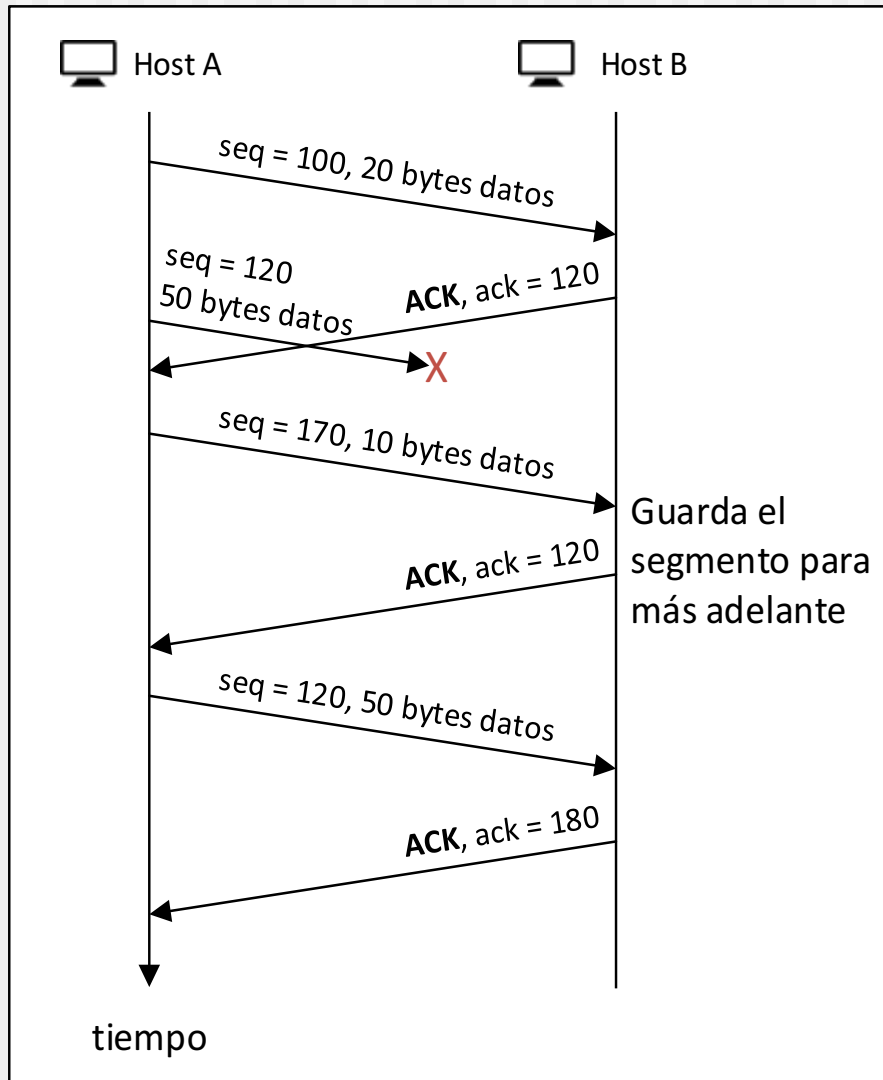


# Fiabilidad y retransmisiones TCP: ACK acumulativo



Escenario de ACK acumulativo

# Fiabilidad y retransmisiones TCP: ACK acumulativo



Escenario: segmento de datos perdido

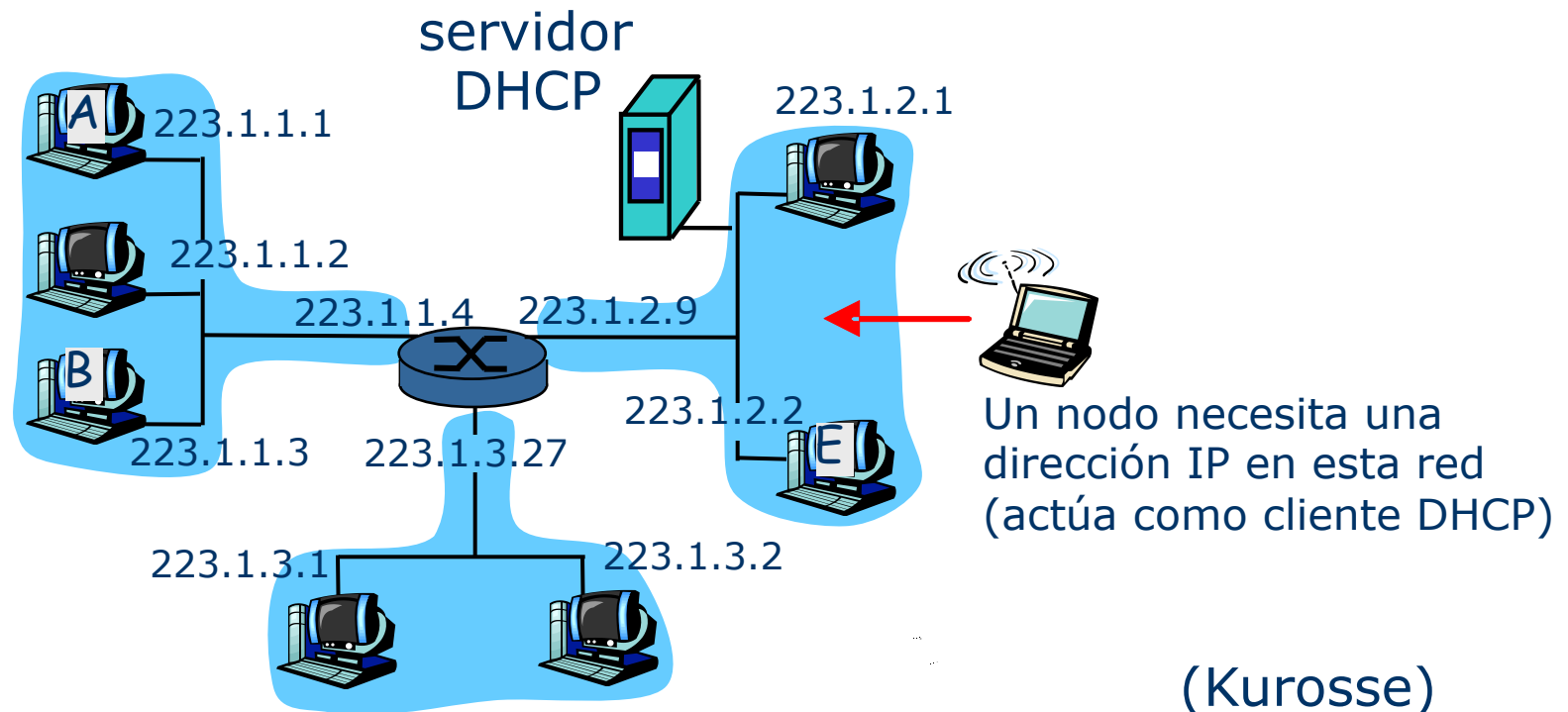
# Anexo: Internet en casa

- Una configuración doméstica, con un router y equipos, suele contar con que:
  - No hace falta asignar de forma manual las direcciones IP a cada equipo, ni el gateway. Todo ello lo proporciona un servicio que está en el router, denominado DHCP, de forma automática
    - La dirección IP que consigue cada equipo en la red debe ser renovada cada cierto tiempo
    - Con la información que suministra el router, cada equipo construye su tabla de encaminamiento básica
  - El identificador de la red es una dirección privada, por ejemplo una 192.168.x.x/24. Como datagramas originados por estas direcciones no atraviesan el router, éste cambia la IP origen del paquete por la suya, mediante una técnica que se denomina NAT (Network Address Translation).
    - Para datagramas IP entrantes, realiza la función inversa, cambiando la dirección IP originaria del paquete por la IP del router en la red doméstica

# DHCP

## ■ Protocolo de configuración dinámica de host

- (Dynamic host configuration protocol)
- Resuelve la incorporación dinámica de hosts a una red, porque necesitan obtener una IP, pasarela y otros parámetros de configuración sin ayuda manual del administrador de la red



# Nociones acerca del servidor DHCP

## Mecanismos básicos

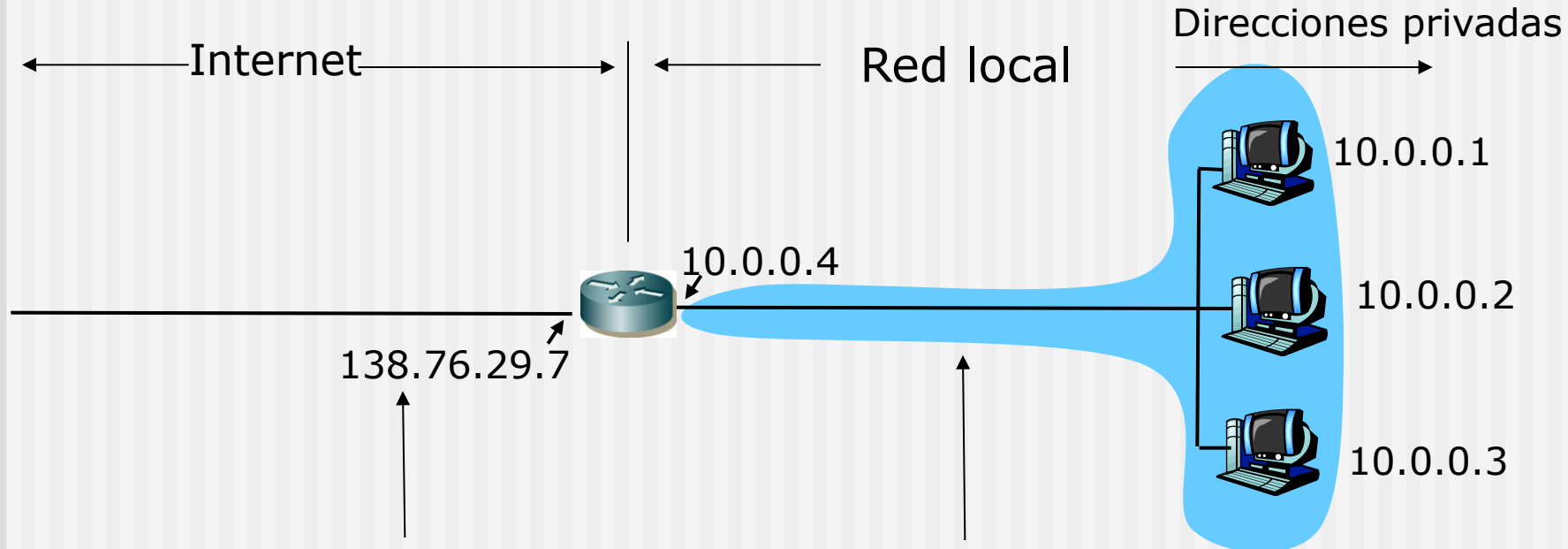
- Envío de parámetros de configuración al host
- Asignación dinámica de dirección IP

## Interesante para el administrador:

- Permite reutilizar direcciones de un conjunto limitado, ya que sólo los hosts activos en la red usan direcciones IP
- Ofrece cierta movilidad de los usuarios entre redes, aunque no mantiene las conexiones
- Permite la asignación de direcciones fijas en función de la dirección física del host
- Es compatible con la existencia de host configurados manualmente en la misma red
- Los routers ADSL domésticos actúan como servidores DHCP

Ver normas RFCs 2131 y 2132

# Cómo funciona NAT



*Todos* los datagramas *que abandonan* la red local tienen la misma IP origen NAT: 138.76.29.7, y diferentes puertos origen

# Cómo funciona NAT (II)

