

Capítulo 4: Capa Red - II

ELO322: Redes de Computadores Agustín J. González

Este material está basado en:

- Material de apoyo al texto *Computer Networking: A Top Down Approach*. Jim Kurose, Keith Ross.

- Un router en Internet tiene la tabla adjunta. Indique cuántas direcciones IP son ruteadas por enlace 2.

<u>Prefijo Coincidente</u>	<u>Interfaz del Enlace</u>
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
Otro caso	3

- Son todas las IP que parten con ese prefijo, menos las que tienen prefijo para enlace 1. Esto es $2^{(3+8)} - 2^8 = 2048 - 256 = 1792$

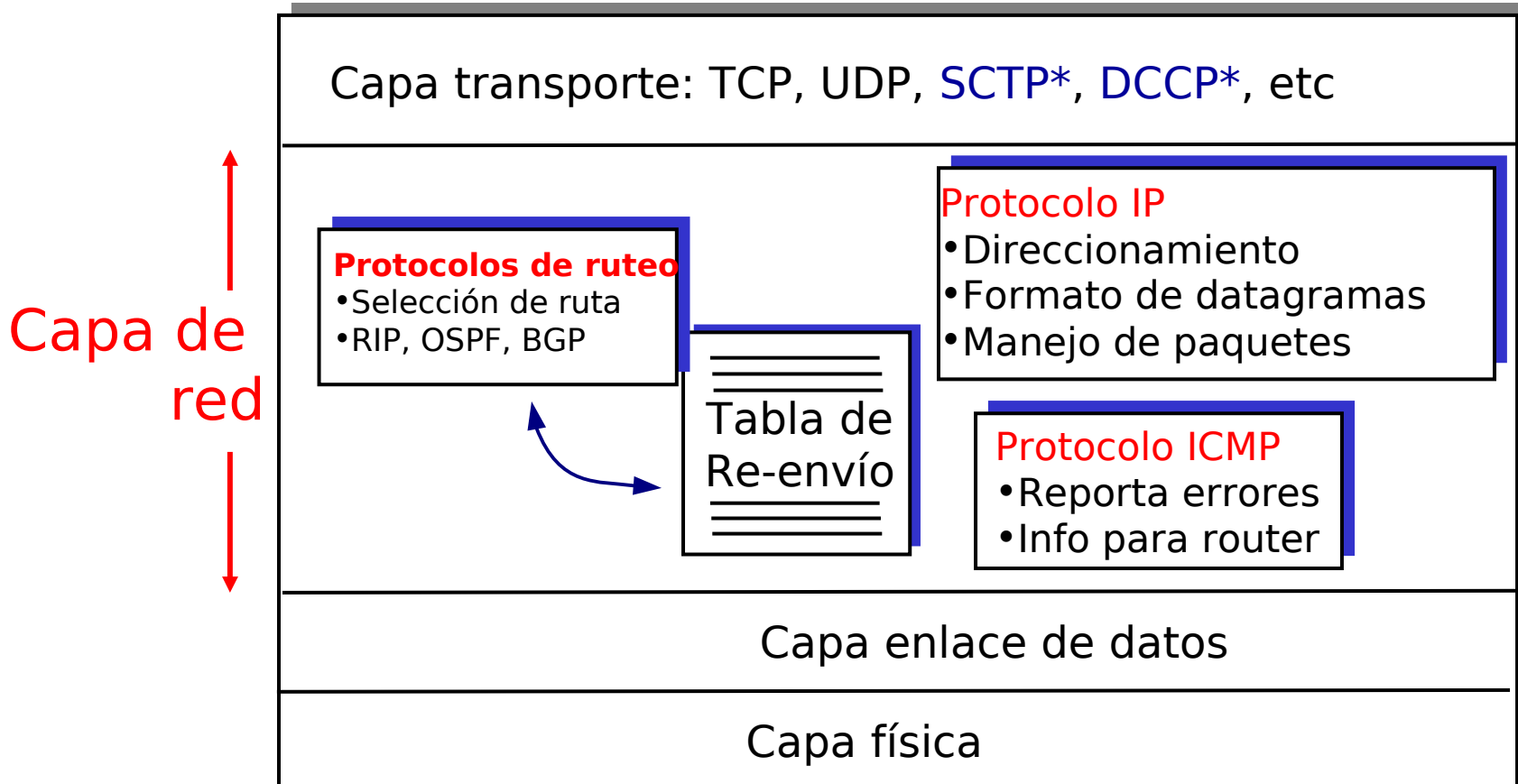
Capítulo 4: Capa de Red

- ❑ 4.1 Introducción
- ❑ 4.2 ¿Qué hay dentro de un router?
- ❑ 4.3 IP: Internet Protocol
 - Formato de Datagrama
 - Fragmentación
 - Direccionamiento IPv4
 - Network address transtation NAT
 - IPv6

Numeración según 7º edición
del texto guía

Capa de red en Internet

Funciones de la capa de red en host y router :



SCTP*: Stream Control Transmission Protocol (año 2000)

DCCP*: Datagram Congestion Control Protocol (año 2006)

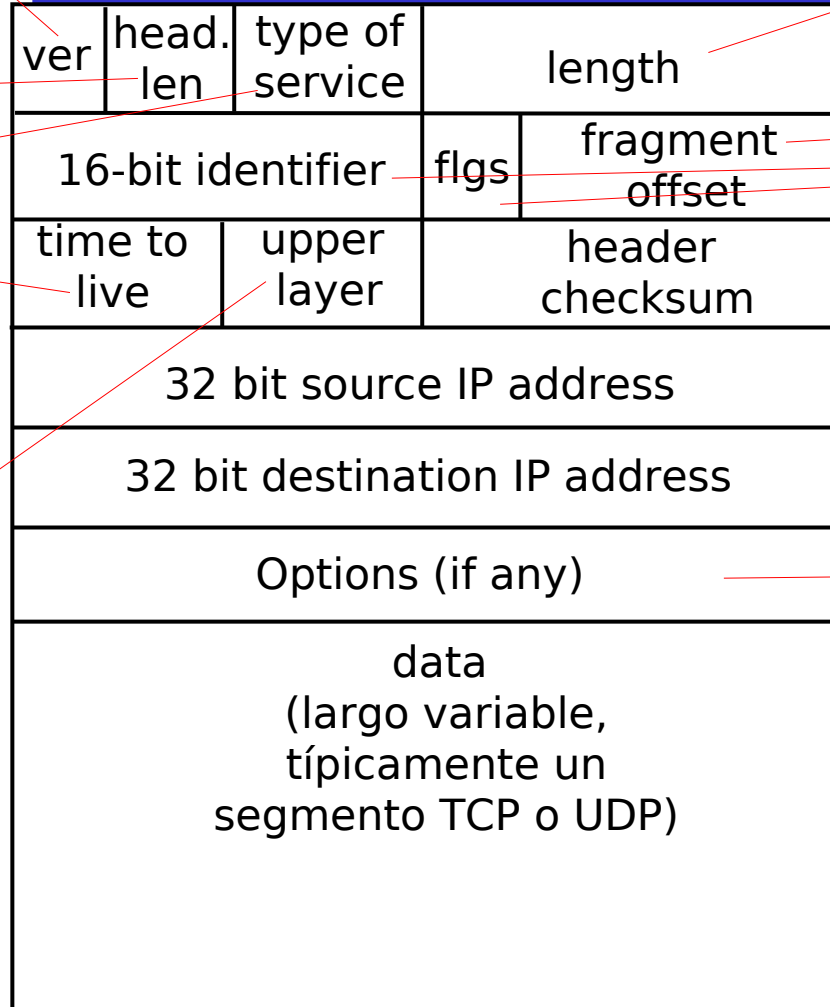
Formato del datagrama IPv4

Número de versión
Protocolo IP = 4

32 bits

Largo total datagrama (bytes)

Largo encabezado (en palabras de 32 bits)



Para fragmentación y re-ensamble

“tipo” de datagrama (bajo retardo, alto BW, confiabilidad)

máx. número de saltos entre routers restantes (decrementado en cada router)

A qué protocolo superior corresponden los datos TCP, UDP, etc

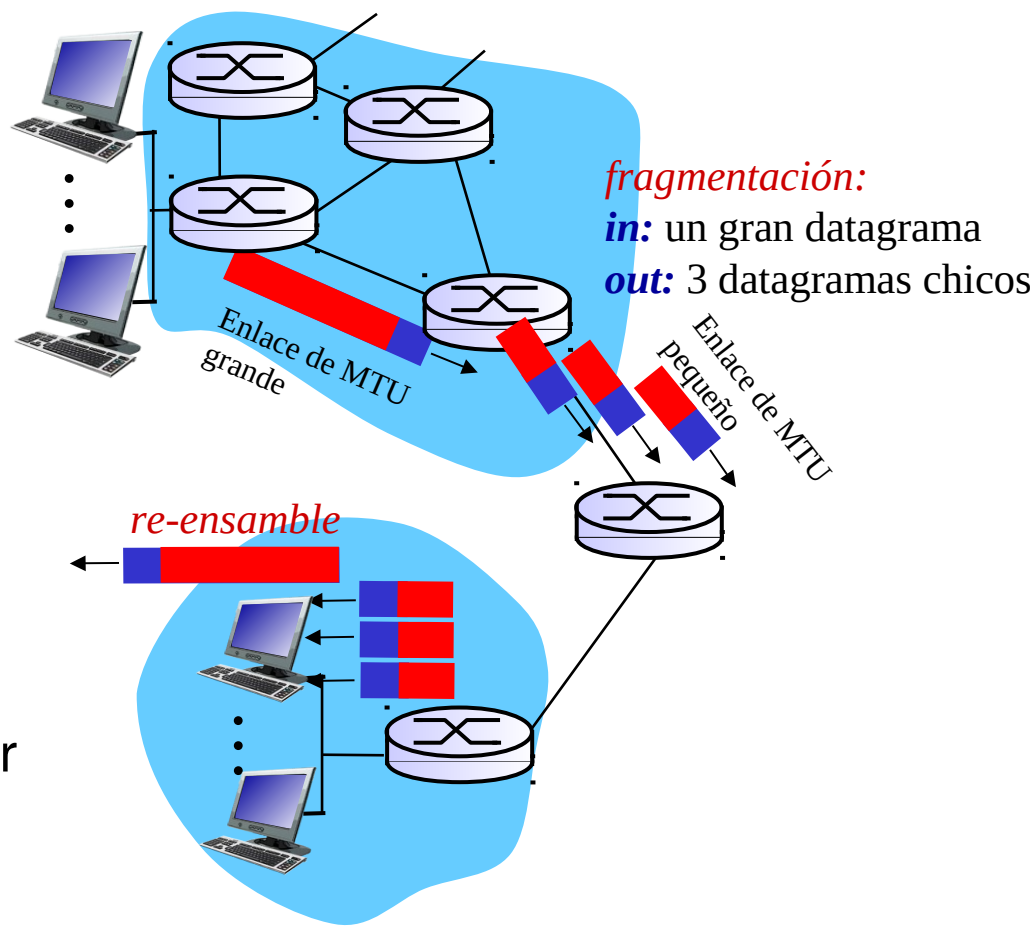
E.g. marcas de tiempo, grabar ruta tomada, lista específica de router a visitar.

¿Cuánta ineficiencia hay en TCP?

- 20 bytes de TCP
- 20 bytes de IP
- =40 bytes + header de capa enlace
- (sin opcionales)

Fragmentación y re-ensamble IP

- ❑ Cada enlace de red tiene un MTU (max. transmission unit), es el mayor tamaño de un frame en la capa enlace.
 - Diferentes tipos de enlaces tienen diferentes MTUs
- ❑ Por esto es que un datagrama IP grande debe ser dividido (“*fragmented*”) en la capa de red
 - Un datagrama se convierte en varios datagramas
 - Se “re-ensambla” en el **destino final**
 - Bits del encabezado IP se usan para identificar y ordenar fragmentos relacionados



Fragmentación y re-ensamble IP

➤ Más fragmentos? 0 => No

Ejemplo

- ❑ 4000 byte datagram (20 bytes header IP + 3980 en campo datos datagrama)
- ❑ MTU = 1500 bytes

1480 bytes en campo de datos de datagrama

offset en bloques de 8 bytes
 $1480/8 = 185$

Largo datos último = $3980 - 1480 - 1480 = 1020$

Más header => 1040

datos insertados en posición $370 * 8 = 2960$

	largo =4000	ID =x	fragflag =0	offset =0	
--	----------------	----------	----------------	--------------	--

Un datagrama grande es transformado en varios datagramas más pequeños

	largo =1500	ID =x	fragflag =1	offset =0	
--	----------------	----------	----------------	--------------	--

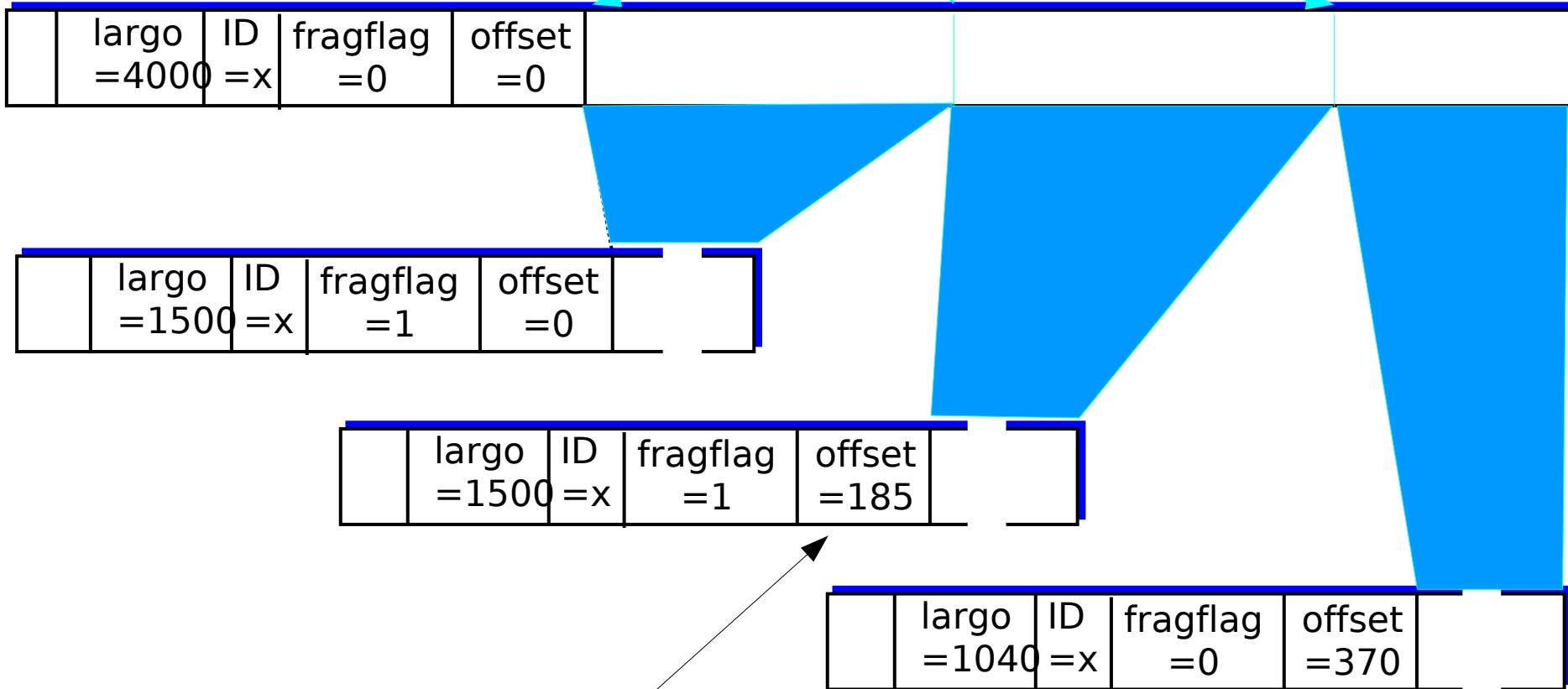
	largo =1500	ID =x	fragflag =1	offset =185	
--	----------------	----------	----------------	----------------	--

	largo =1040	ID =x	fragflag =0	offset =370	
--	----------------	----------	----------------	----------------	--

Fragmentación y re-ensamble

Más fragmentos?

Debe ser múltiplo de 8



Posición al re-ensamble = $\text{offset} * 8$

Un destino de una red IP recibe fragmentos de tamaños 444, 444 y 253, ¿Qué puede decir usted respecto del MTU más pequeño de la ruta? Si los tres fragmentos corresponden al mismo datagrama original ¿Cuál es el tamaño del datagrama enviado?



- ❑ Como se trata de fragmentos, el paquete original fue dividido en fragmentos que quepan en el MTU más pequeño de la ruta. El MTU debe ser superior o igual a 444, e inferior a $(20+424+8)=452$.
- ❑ Suponiendo que son los únicos fragmentos y no se ha perdido ninguno, el datagrama original es de tamaño $20+(444-20)+(444-20)+(253-20)= 1101$ bytes.

Capítulo 4: Capa de Red

- ❑ 4.1 Introducción
- ❑ 4.2 ¿Qué hay dentro de un router?
- ❑ 4.3 IP: Internet Protocol
 - Formato de Datagrama
 - Fragmentación
 - **Direccionamiento IPv4**
 - Network address translation NAT
 - IPv6

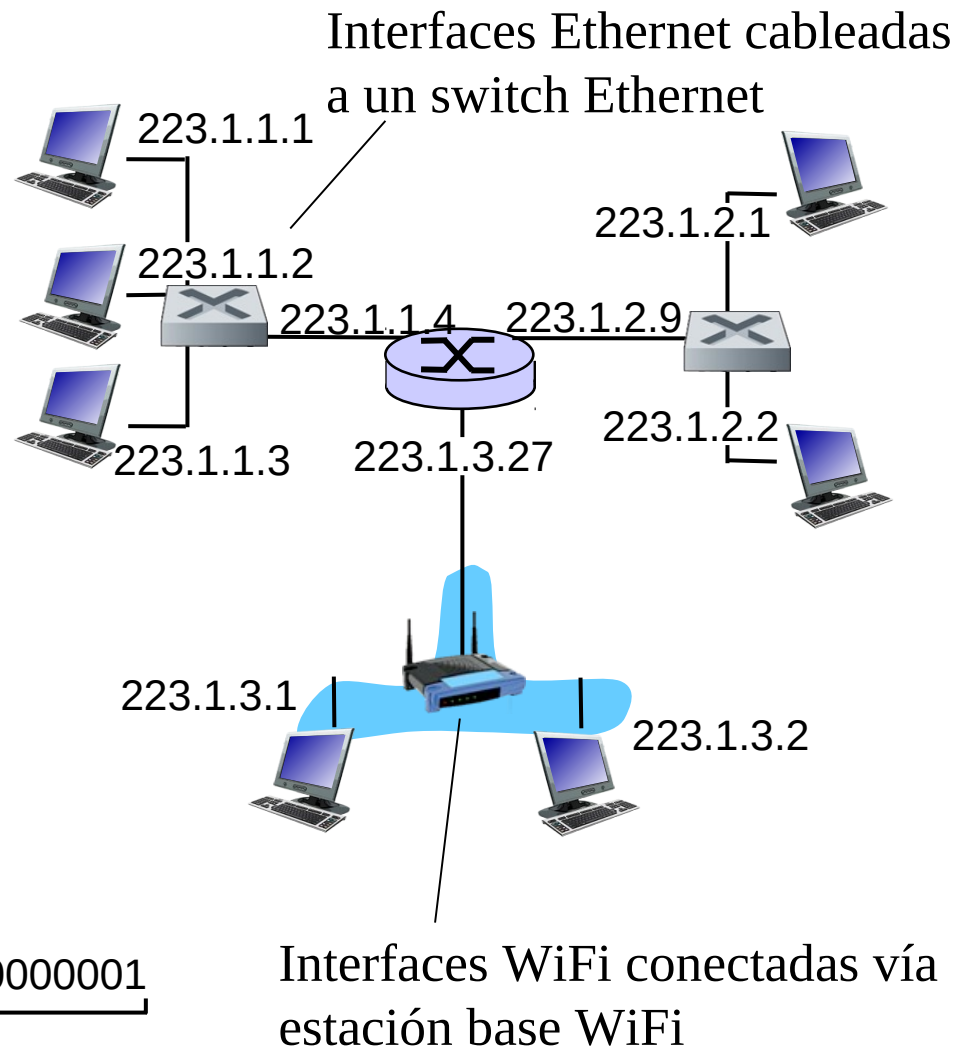
Numeración según 7º edición
del texto guía

Direccionamiento IP: introducción

- ❑ **Dirección IP:** identificador de 32-bit del host, *interfaz* del router
- ❑ **Interfaz:** conexión entre host y router, enlace físico
 - Router típicamente tiene múltiples interfaces (bocas)
 - Host puede tener múltiples interfaces (Ethernet, WiFi)
 - Dirección IP está asociada a cada interfaz

Una Interfaz <=> al menos 1 direc. IP

223.1.1.1 = 11011111 00000001 00000001 00000001
 223 1 1 1



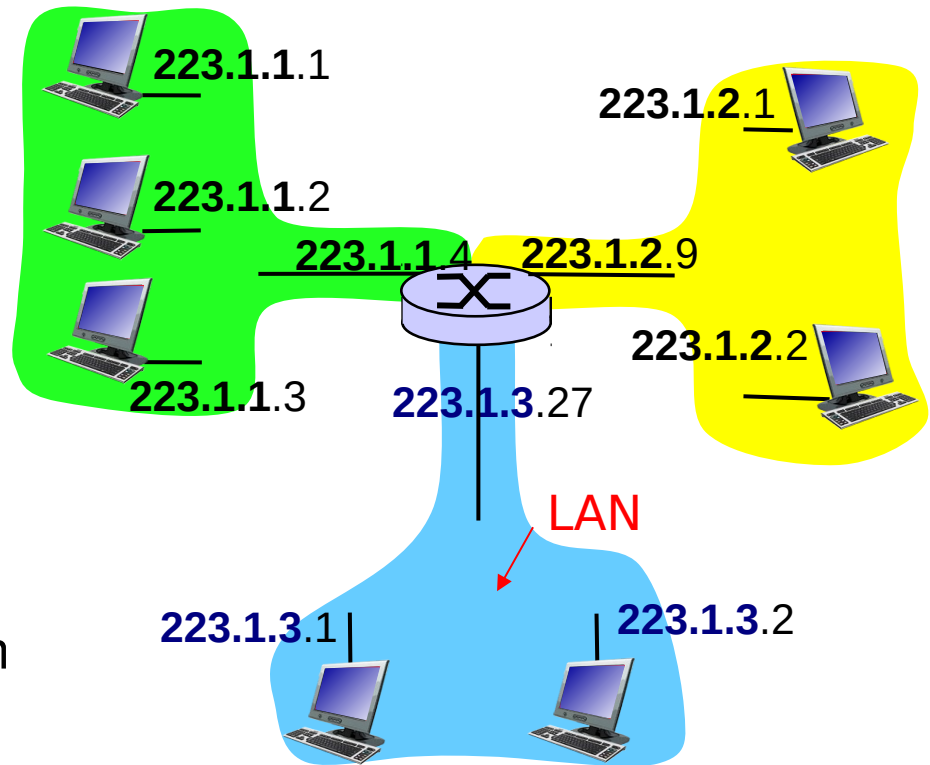
Sub-redes

□ Dirección IP:

- Direc. sub-red (bits más significativos)
- Direc. del host (bits menos significativos)

□ *¿Qué es una sub-red?*

- Grupo de máquinas que poseen la misma dirección de sub-red (parte más significativa)
- Se podrían interconectar sin tener un router (e.g. con un switch, hub, Punto de acceso)
- Cada una de las zonas coloreadas mostradas.



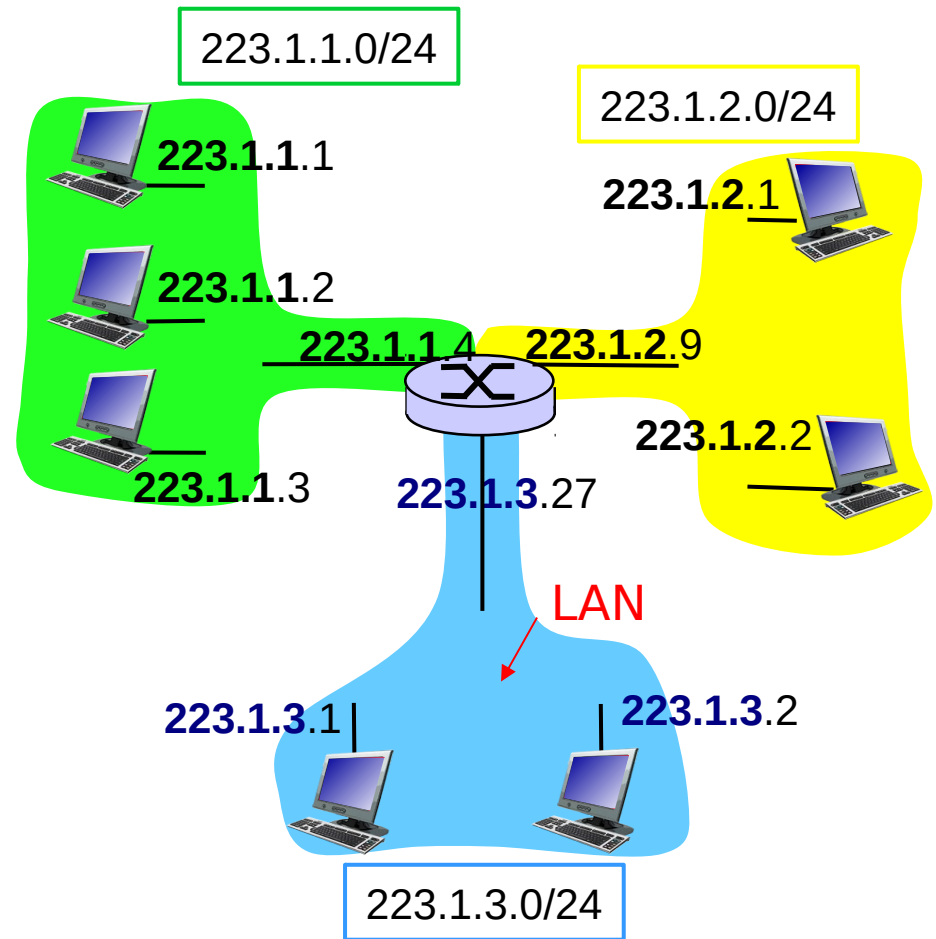
Red consiste de 3 sub-redes

Las direcciones IP están organizadas jerárquicamente

Sub-redes

Receta

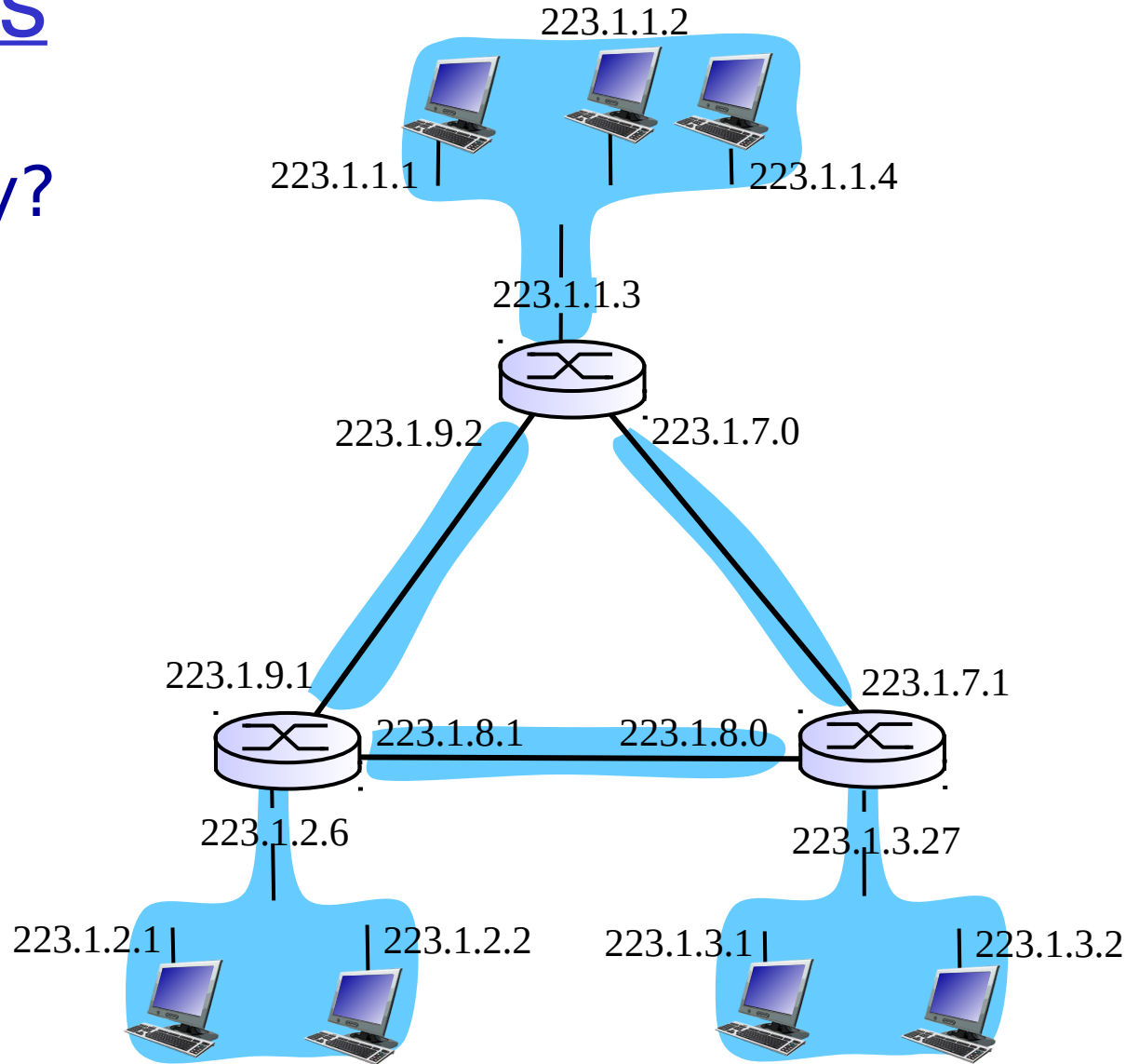
- Para determinar las sub-redes, desconectar las interfaces del router para crear redes tipo islas independientes.
- Cada red independiente es una **sub-red**.



Máscara de sub-red: /24
=> 24 primeros bits
Comunes, dirección de subred

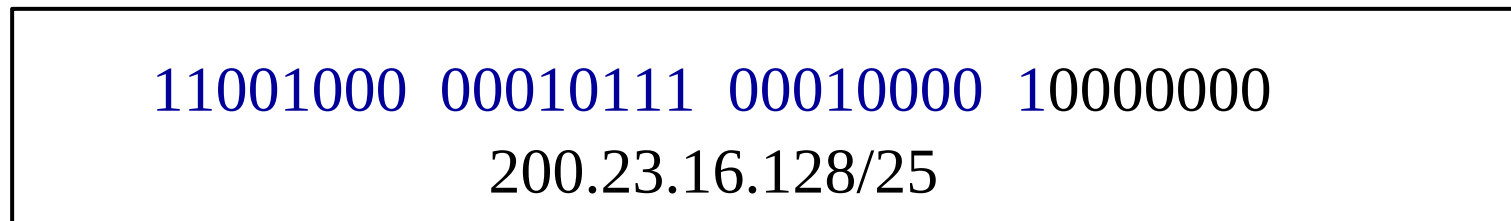
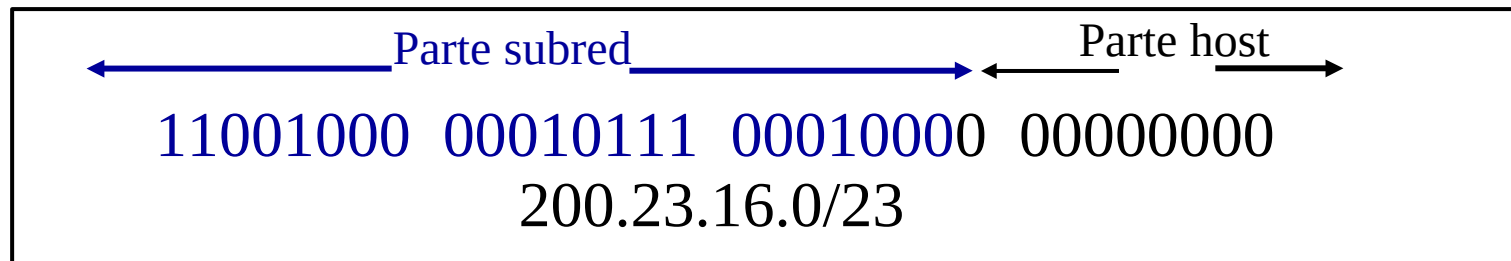
Sub-redes

¿Cuántas hay?



Direccionamiento IP: CIDR

- Se refiere a estructura de una dirección IP: parte dirección común de sub-red y dirección de host dentro de la red.
- **CIDR: C**lassless **I**nterDomain **R**outing
 - Porción de sub-red de la dirección es de largo arbitrario
 - Formato de dirección: **a.b.c.d/x**, donde x es # bits de la dirección de la sub-red



¿Qué es una dirección IP privada?

- ❑ Al comienzo se pensó que cada máquina debía tener una dirección única en el planeta.
- ❑ Esto no fue siempre necesario pues redes privadas, como aquellas que conectan máquinas en una industria, no requerían conexión a Internet.
- ❑ Para este propósito se reservó algunas subredes para crear redes privadas. Éstas son:
 - 10.0.0.0/8** con 2^{24} direcciones \Rightarrow **00001010.xxxxxxxx.X.X**
 - 172.16.0.0/12** con 2^{20} direcciones \Rightarrow **10101100.0001xxxx.X.X**
 - 192.168.0.0/16** con 2^{16} direcciones \Rightarrow **11000000.10101000.X.X**
- ❑ Como la idea era que estas sub-redes no estuvieran conectadas a Internet, las mismas sub-redes pueden utilizarse en varios lugares mientras no se conecten a Internet.

¿Cuántas máquinas puede usted conectar a la sub-red 200.1.17.128/26?



- ❑ $32-26=6 \Rightarrow$ Número de IPs es $2^6=64$ direcciones IP, de las cuales 62 pueden ser asignadas a máquinas.
- ❑ La dirección de sólo 0's y sólo 1's están reservadas. Sólo 1's es la de broadcast.

Direcciones IP: ¿Cómo obtener una?

Q: ¿Cómo obtiene un *host* su dirección IP?

- ❑ Configurada por el administrador en un archivo
 - Windows: ver versión específica
 - Linux: ver versión específica
- ❑ **Vía protocolo de configuración dinámica DHCP: Dynamic Host Configuration Protocol:** el host obtiene la dirección dinámicamente desde un servidor
 - “plug-and-play”, es decir, el usuario enciende su computador y puede trabajar con dirección asignada por DHCP

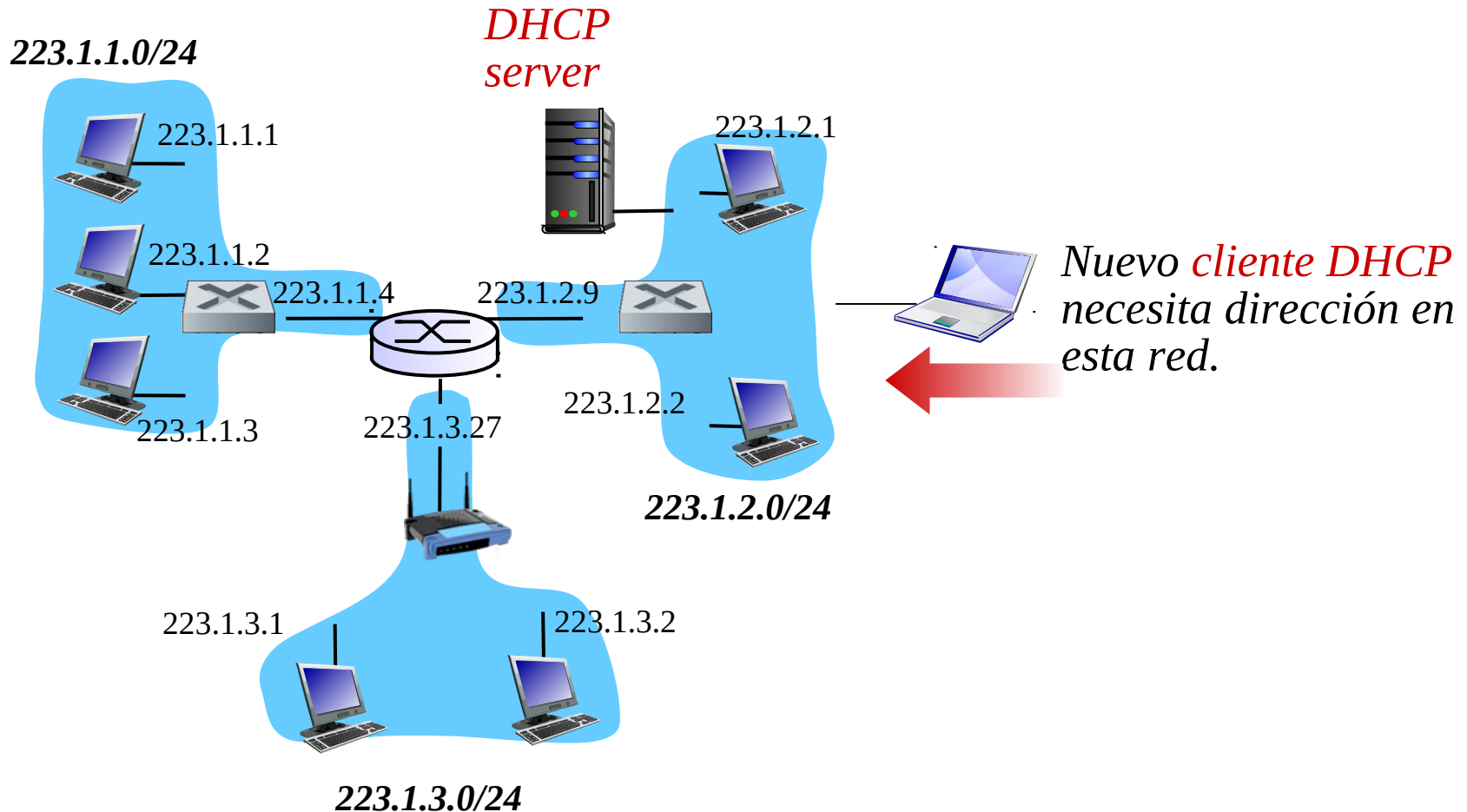
DHCP: Dynamic Host Configuration Protocol

- Objetivo:** permitir a un host obtener *dinámicamente* su dirección IP desde un servidor en la red cuando el host se integra a la red.
- El host puede renovar y extender el uso de su dirección
 - Permite el reuso de direcciones (la dirección sólo se mantiene mientras se esté conectado).
 - Conveniente para usuarios móviles que se conectan por corto tiempo.

Cómo DHCP funciona en general:

- host difunde (broadcasts) mensaje “DHCP discover”
- Servidor DHCP responde con mensaje “DHCP offer”
- Host pide una dirección IP mensaje: “DHCP request”
- Servidor DHCP envía mensaje con dirección: “DHCP ack”

Escenario cliente-servidor DHCP



Escenario cliente-servidor DHCP

DHCP server: 223.1.2.5



DHCP discover

Broadcast: hay servidor DHCP por allí?

arriving client



yiaddr: your Internet address

DHCP offer

Broadcast: Yo soy un servidor DHCP! Puedes usar esta dir. IP

DHCP request

Broadcast: OK. Tomaré esa dirección IP

DHCP ACK

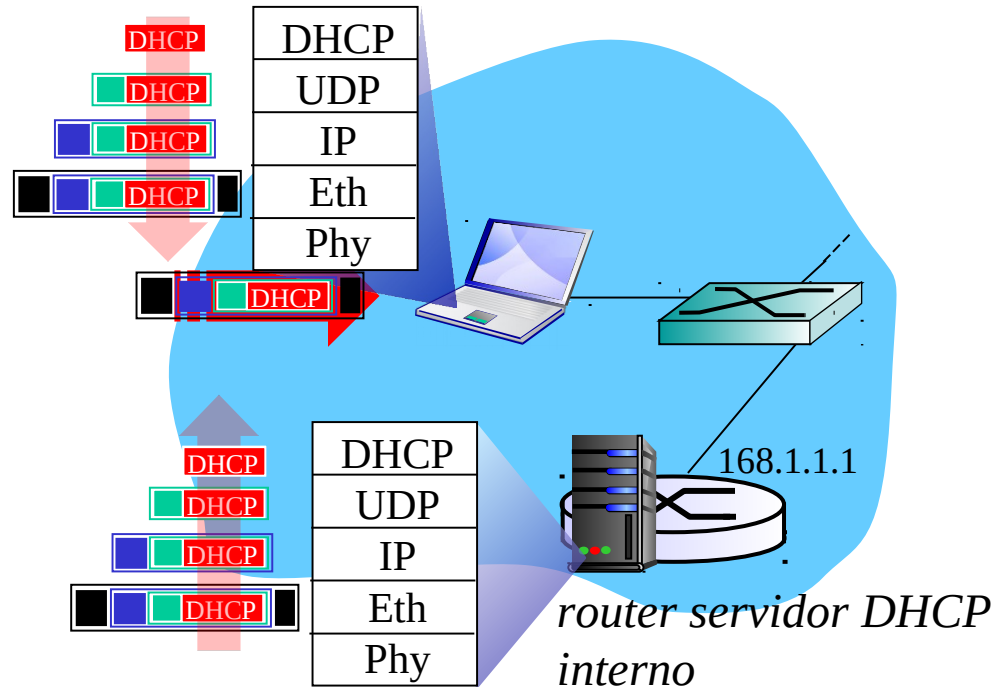
Broadcast: OK. Se te asigna esa dir. IP!

DHCP: más que direcciones IP

DHCP puede retornar además de la dirección IP:

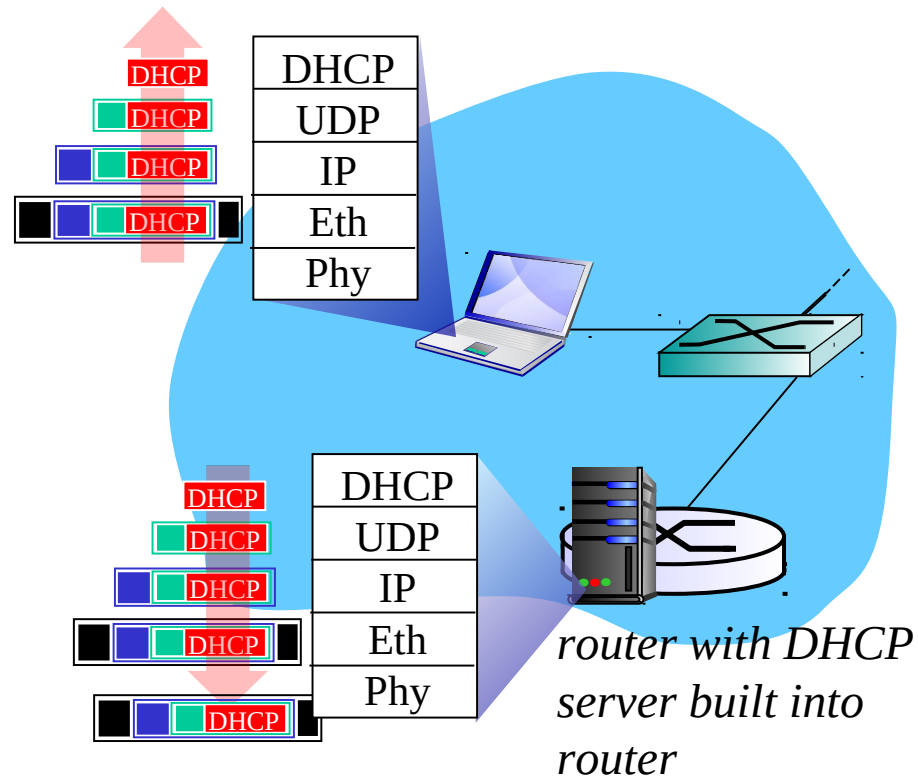
- Dirección del router de salida para ese cliente
- Nombre y dirección IP del servidor DNS
- Máscara de la subred (indicando la porción de la dirección de red de la porción de la dirección del host)

DHCP: ejemplo



- ❖ Notebook necesita dirección IP, dirección de router, dir de servidor DNS: usa DHCP
- ❖ Notebook envía requerimiento DHCP encapsulado en UDP, encapsulado en IP, encapsulado en Ethernet
- ❖ Trama Ethernet (dest: FFFFFFFF) en LAN es recibida en el router que corre el servidor DHCP
- ❖ Ethernet, IP, UDP demultiplexan trama DHCP

DHCP: ejemplo



- ❖ Servidor DHCP prepara mensaje DHCP ACK con la dirección IP del cliente, dirección IP del primer router para el cliente, nombre & dir IP del servidor DNS
- ❖ Servidor DHCP encapsula el mensaje DHCP ACK, trama es enviada al cliente, allí se demultiplexa y pasa al DHCP en cliente
- ❖ Cliente ahora conoce su dir IP, nombre y dir IP del servidor DNS local, dir IP del primer router para salir de la LAN.

DHCP: Wireshark output (home LAN)

Message type: **Boot Request (1)**

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x6b3a11b7

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 0.0.0.0 (0.0.0.0)

Next server IP address: 0.0.0.0 (0.0.0.0)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Server host name not given

Boot file name not given

Magic cookie: (OK)

Option: (t=53,l=1) **DHCP Message Type = DHCP Request**

Option: (61) Client identifier

Length: 7; Value: 010016D323688A;

Hardware type: Ethernet

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Option: (t=50,l=4) Requested IP Address = 192.168.1.101

Option: (t=12,l=5) Host Name = "nomad"

Option: (55) Parameter Request List

Length: 11; Value: 010F03062C2E2F1F21F92B

1 = Subnet Mask; 15 = Domain Name

3 = Router; 6 = Domain Name Server

44 = NetBIOS over TCP/IP Name Server

.....

request

Message type: **Boot Reply (2)**

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x6b3a11b7

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.1.101 (192.168.1.101)

Your (client) IP address: 0.0.0.0 (0.0.0.0)

Next server IP address: 192.168.1.1 (192.168.1.1)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Server host name not given

Boot file name not given

Magic cookie: (OK)

Option: (t=53,l=1) DHCP Message Type = DHCP ACK

Option: (t=54,l=4) Server Identifier = 192.168.1.1

Option: (t=1,l=4) Subnet Mask = 255.255.255.0

Option: (t=3,l=4) Router = 192.168.1.1

Option: (6) Domain Name Server

Length: 12; Value: 445747E2445749F244574092;

IP Address: 68.87.71.226;

IP Address: 68.87.73.242;

IP Address: 68.87.64.146

Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

reply

Esta lámina es referencial,
no se requiere su estudio
detallado

Direcciones IP: ¿Cómo obtener varias?

Q: ¿Cómo la red obtiene la dirección de subred?
parte común más significativa de la dirección IP.

A: Obteniendo una porción del espacio de direcciones del proveedor ISP.

Ejemplo:

ISP's block	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/20
Organization 0	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/23
Organization 1	<u>11001000</u>	<u>00010111</u>	<u>00010010</u>	00000000	200.23.18.0/23
Organization 2	<u>11001000</u>	<u>00010111</u>	<u>00010100</u>	00000000	200.23.20.0/23
...
Organization 7	<u>11001000</u>	<u>00010111</u>	<u>00011110</u>	00000000	200.23.30.0/23

También podrían haberse definido redes de distinto tamaño.

Direccionamiento IP: la última palabra...

Q: ¿Cómo un ISP obtiene un bloque de direcciones?

A: **ICANN:** Internet Corporation for Assigned Names and Numbers

- Asigna direcciones
- Administra DNS
- Asigna nombre de dominio, resuelve disputas

Para América Latina la oficina es LACNIC:

<http://lacnic.net/>

Hay otras cuatro para otras regiones del mundo.

Capítulo 4: Capa de Red

- ❑ 4.1 Introducción
- ❑ 4.2 ¿Qué hay dentro de un router?
- ❑ 4.3 IP: Internet Protocol
 - Formato de Datagrama
 - Fragmentación
 - Direccionamiento IPv4
 - Network address transtation NAT
 - IPv6

Numeración según 7º edición
del texto guía

Agotamiento de Direcciones IP

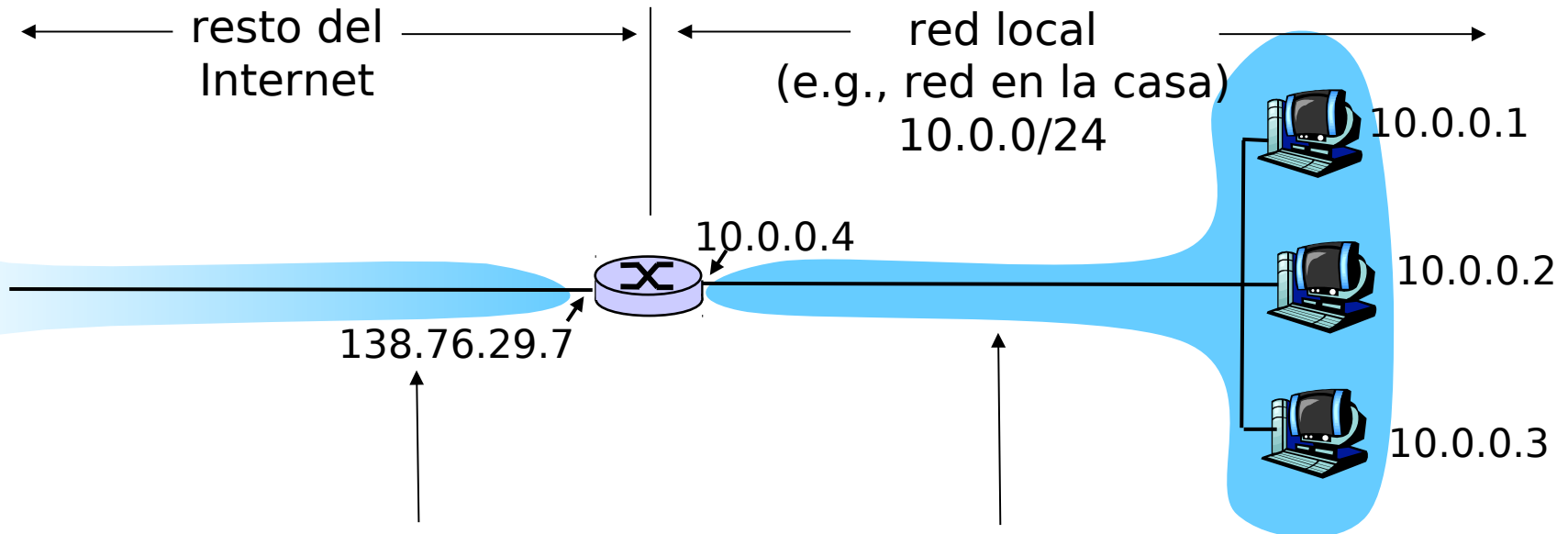
- ❑ Conforme más subredes se crearon y conectaron a Internet, las direcciones IP se comenzaron a agotar. Hoy 4 de las 5 regiones de mundo no tienen nuevas direcciones para asignar.
- ❑ Se desarrollaron dos estrategias para extender el uso de Ipv4:
 - Flexibilizar el tamaño de las subredes: surge **C**lassless **I**nter**D**omain **R**outing (CIDR) *.
 - Permitir acceso a Internet de redes privadas a través del uso de **NAT** (Network Address Translation)

(*) Antes el número de bits de la dirección de sub-red era 8 bits, Clase A; 16 bits, Clase B, ó 24 bits, Clase C.

NAT: Network Address Translation

- ❑ **Motivación:** ¿Cómo podemos dar salida a Internet a una red con direcciones privadas? Usamos un representante.
- ❑ La **idea** es usar sólo una dirección IP para acceder al mundo exterior:
 - No necesitamos asignación de un rango del ISP: sólo una dirección externa es usada por todos los equipos internos
 - Podemos cambiar la dirección de equipos en red local sin notificar al mundo exterior
 - Podemos cambiar ISP sin cambiar direcciones de equipos en red local
 - Equipos dentro de la red no son explícitamente direccionables o visibles desde afuera (una ventaja de seguridad).

NAT: Network Address Translation



Todos los datagramas *saliendo* de la red local tienen la *misma* dirección NAT IP: 138.76.29.7, pero diferentes números de puerto

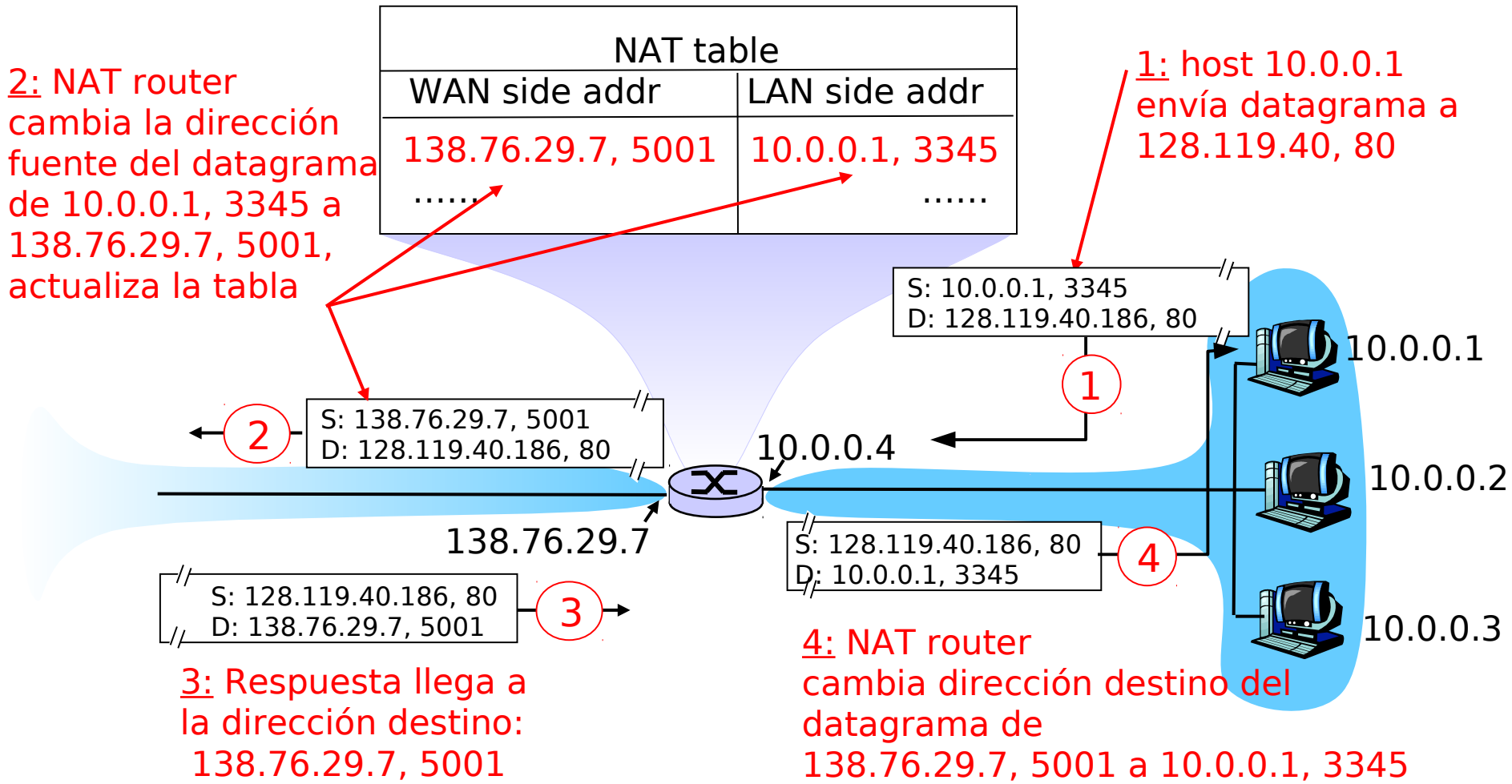
Datagramas con fuente o destino en esta red tienen direcciones 10.0.0/24 (También se puede usar: 192.168.0/24 ó 172.16.0/24)

NAT: Network Address Translation

Implementación: tareas del router con NAT:

- Para Datagramas salientes: **reemplazar** (IP fuente, # puerto) de cada datagrama saliente por (IP NAT, nuevo # puerto)
 - . . . Clientes y servidores remotos responderán usando (IP NAT, nuevo # puerto) como dirección destino.
- Recordar (en tabla de traducción NAT) cada par de traducción (IP fuente, # puerto) a (IP NAT, nuevo # puerto)
- Para Datagramas entrantes: **reemplazar** (IP NAT, nuevo # puerto) en campo destino de cada datagrama entrante por correspondiente (IP fuente, # puerto) almacenado en tabla NAT

NAT: Network Address Translation



NAT: Network Address Translation

- ❑ Campo número de puerto es de 16 bits:
 - Máx. ~65,000 conexiones simultáneas pueden salir con sólo una dirección IP válida en Internet!
- ❑ NAT es controversial:
 - Routers deberían procesar sólo hasta capa 3
 - Viola argumento extremo-a-extremo
 - Los NAT deben ser tomados en cuenta por los diseñadores de aplicaciones, eg, aplicaciones P2P
 - En lugar de usar NAT, la carencia de direcciones debería ser resuelta por IPv6
- ❑ Si Ud. tiene una máquina detrás de un NAT, ésta puede ser visible usando UPnP (Universal Plug and Play). Importante: hay formas de entrar.

La red wifi de la USM usa direcciones IP privadas ¿Qué hace posible que usted pueda acceder a Internet? ¿Puede usted instalar un servidor (web por ejemplo) conectado a esta red inalámbrica? ¿Sería accesible desde la misma red wifi? ¿Sería accesible desde Internet?



- ❑ La presencia de un NAT. Sí. Sí. No. Nota: Lo último puede ser Sí indicando el uso de “port forwarding en el NAT (tema no cubierto en el ramo, pero puede ser de su conocimiento)

Un alumno se conecta vía ssh desde la red con NAT en su casa a un servidor en la Universidad. Si deja su conexión inactiva por un largo rato, al volver detecta que está caída. Explique cómo el servidor NAT puede causar tal pérdida de conexión. ?

- El servidor NAT mantiene una tabla con los puertos que han sido asignados a flujos provenientes de la red privada. Si no hay actividad luego de un rato, este puerto es liberado para ser asignado a otros flujos de datos. En este caso la conexión ssh ya no funciona porque el puerto asignado en el NAT ya no pertenece a esa conexión.

- En un “cyber café” todos los usuarios navegan en Internet y salen a través de un único NAT. Analizando el tráfico que sale del “cyber café” hacia Internet ¿cómo podría usted estimar cuántos clientes están usando su red? Se sabe que la capa IP de cada computador usa números de identificación secuenciales en cada datagrama saliente.

- Basta con observar cuántas secuencias de números de identificación están saliendo. El número de secuencias indicará el número de capas IP enviando paquetes y será el número de clientes del cyber café.

Capítulo 4: Capa de Red

- ❑ 4.1 Introducción
- ❑ 4.2 ¿Qué hay dentro de un router?
- ❑ 4.3 IP: Internet Protocol
 - Formato de Datagrama
 - Fragmentación
 - Direccionamiento IPv4
 - Network address transtation NAT
 - IPv6

Numeración según 7º edición
del texto guía

IPv6

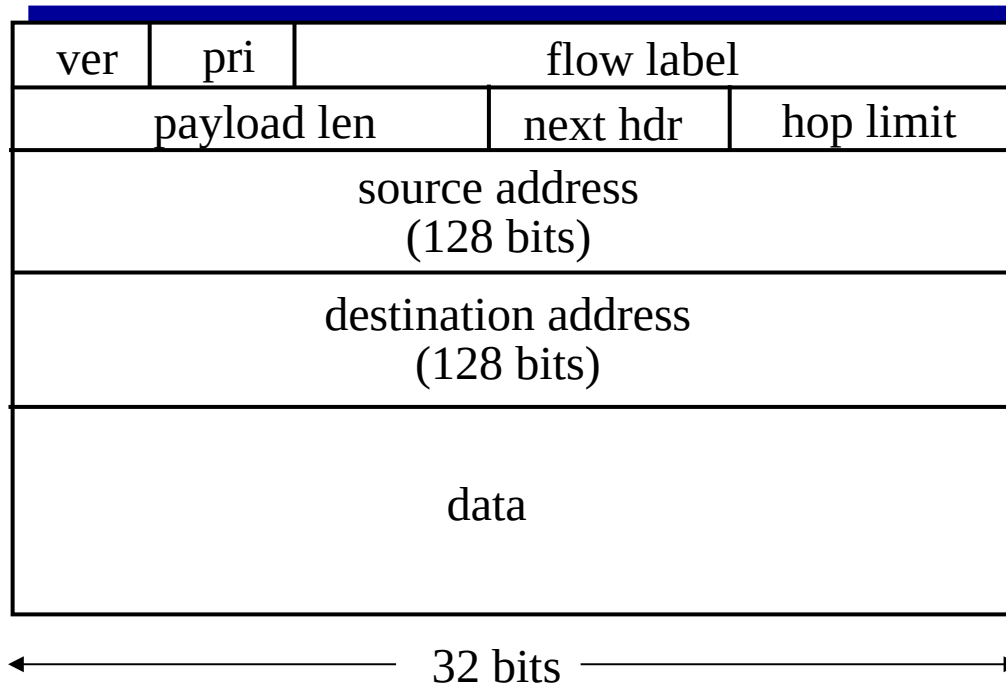
- ❑ **Motivación Inicial:** espacio de direcciones de 32-bit pronto serán completamente asignadas.
- ❑ **Motivación adicional:**
 - Formato de encabezado debería ayudar a acelerar el procesamiento y re-envío (por aumento de tasas en red)
 - Cambiar encabezado para facilitar QoS (Quality of Service)

Formato de datagrama IPv6:

- Encabezado de largo fijo de 40 bytes (se duplicó)
- Fragmentación no es permitida

Encabezado IPv6

- ❑ *Prioridad (8bits)*: identifica prioridad entre datagramas en flujo
- ❑ *Flow Label*: identifica datagramas del mismo “flujo.”
(concepto de “flujo” no está bien definido).
- ❑ *Next header*: identifica protocolo de capa superior de los datos

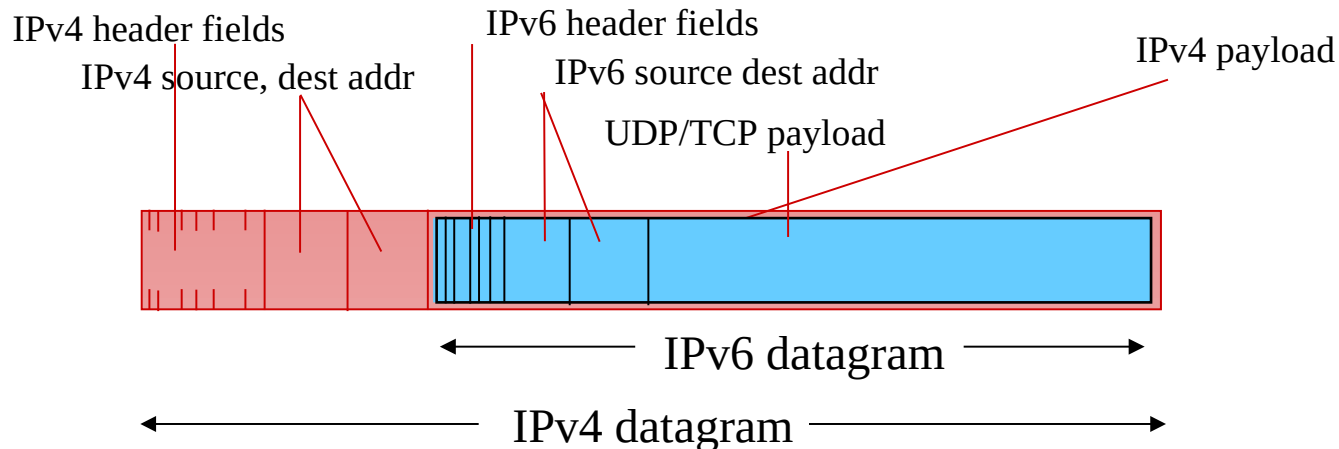


Otros cambios de IPv4 a v6

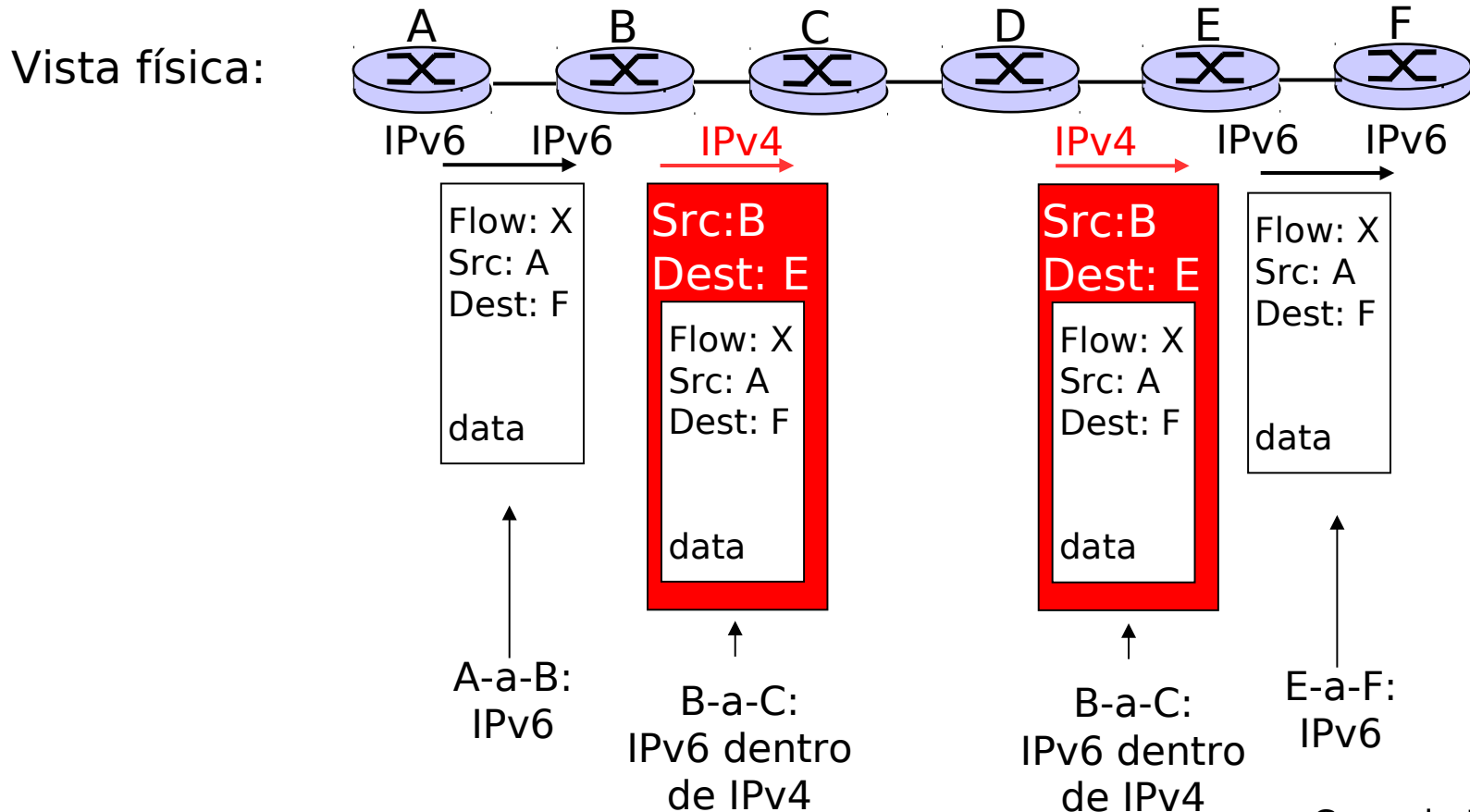
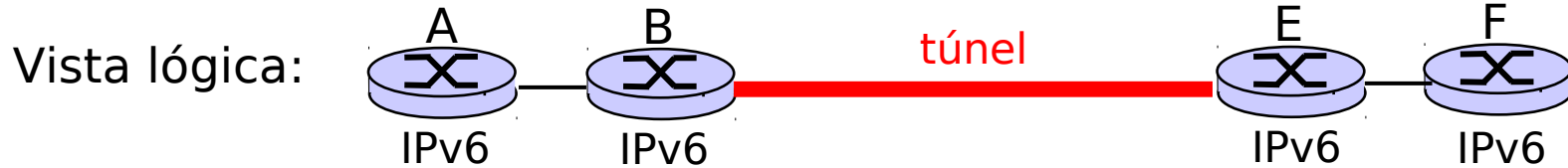
- ❑ *Checksum*: eliminada enteramente para reducir tiempo de procesamiento en cada router al ser redundante, ya está en capa transporte y enlace (Ethernet)
- ❑ *Options*: permitidas, pero fuera del encabezado, indicado por campo “Next Header”
- ❑ *ICMPv6*: nueva versión de ICMP
 - Tipos de mensajes adicionales, e.g. “Paquete muy grande” (usado en el descubrimiento de MTU: unidad máxima de transmisión)
 - Funciones para administrar grupos multicast

Transición de IPv4 a IPv6

- ❑ No todos los routers pueden ser actualizados (upgraded) simultáneamente
 - No es posible definir un día para cambio “día de bajada de bandera”
 - ¿Cómo operará la red con routers IPv4 e IPv6 mezclados?
- ❑ **“Tunneling”**: IPv6 es llevado como carga en datagramas IPv4 entre routers IPv4



Tunneling



IPv6: Adopción

- ❑ Google: 8% de clientes acceden sus servicios vía IPv6
- ❑ NIST: 1/3 de todos los dominios del gobierno de USA manejan IPv6

- ❑ **Tiempo muy largo de adopción**, ha pasado
 - 20 años y seguimos contando!
 - Comparar con cambios a nivel aplicación de últimos 20 años: WWW, Facebook, streaming media, Skype, ...
 - Por qué?

NIST: National Institute of Standards and Technology

- ¿Por qué el protocolo IPv6 decidió eliminar el campo de suma de chequeo que sí tiene IPv4?

- Porque así cada paquete puede ser procesado más rápidamente al no requerir recalcular una suma de chequeo cada vez que el “hop limit” cambiaba.