

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 Featuring the Internet 3rd* edition. Jim Kurose, Keith Ross Addison-Wesley, 2004.

- Un router en Internet tiene la tabla adjunta. Indique cuántas direcciones IP son resumidas en la entrada que sale 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

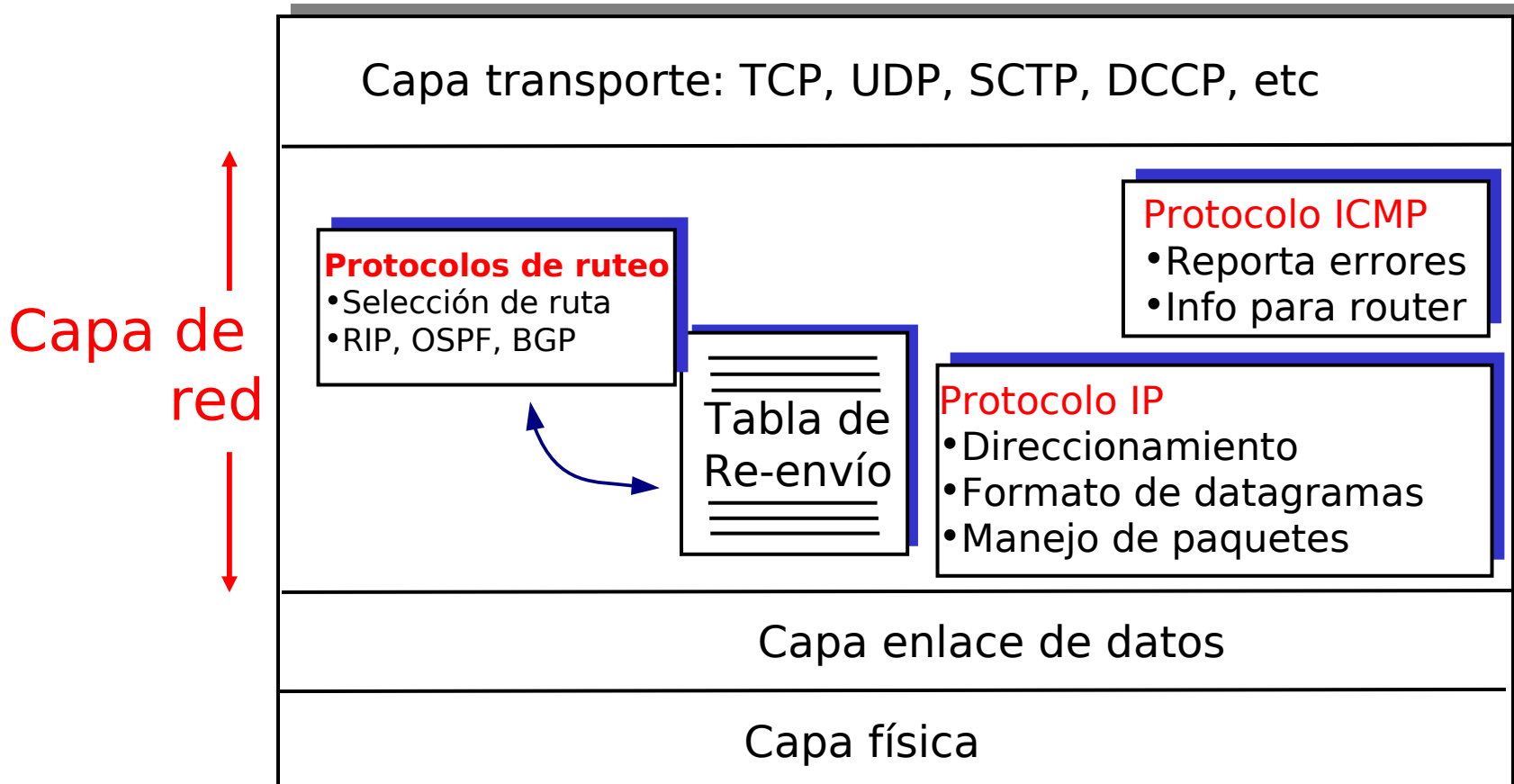
- Son todas la IP que parten con ese prefijo, menos las que tienen prefijo para enlace 1. Esto es $2^{(3+8)} - 2^8 = 2048 - 256 = 1792$

Capítulo 4: Capa de Red

- 4.1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- **4.4 IP: Internet Protocol**
 - Formato de Datagrama
 - Direccionamiento IPv4
 - ICMP
 - IPv6
- 4.5 Algoritmo de ruteo
 - Estado de enlace
 - Vector de Distancias
 - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
 - RIP
 - OSPF
 - BGP
- 4.7 Ruteo Broadcast y multicast

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)

Capítulo 4: Capa de Red

- ▣ 4.1 Introducción
- ▣ 4.2 Circuitos virtuales y redes de datagramas
- ▣ 4.3 ¿Qué hay dentro de un router?
- ▣ **4.4 IP: Internet Protocol**
 - ▣ **Formato de Datagrama**
 - ▣ Direccionamiento IPv4
 - ▣ ICMP
 - ▣ IPv6
- ▣ 4.5 Algoritmo de ruteo
 - ▣ Estado de enlace
 - ▣ Vector de Distancias
 - ▣ Ruteo Jerárquico
- ▣ 4.6 Ruteo en la Internet
 - ▣ RIP
 - ▣ OSPF
 - ▣ BGP
- ▣ 4.7 Ruteo Broadcast y multicast

Formato del datagrama IPv4

Número de versión
Protocolo IP = 4

Largo encabezado
(bytes)

“tipo” de datagrama

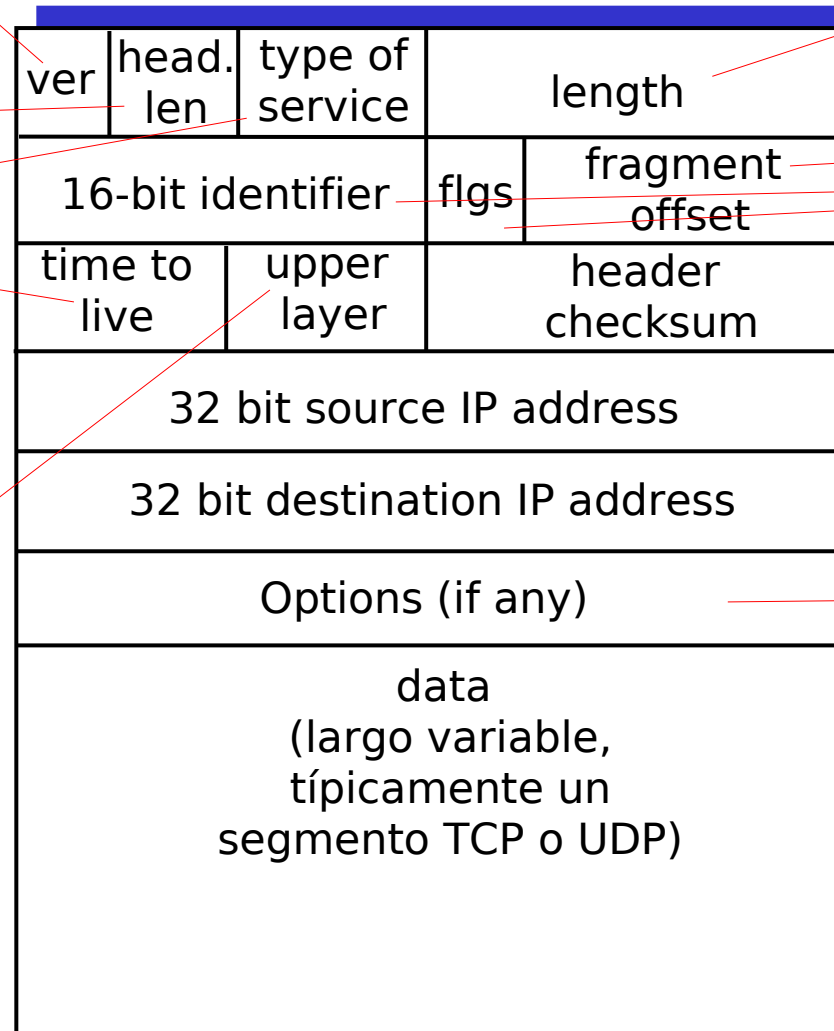
máx. número
de tramos restantes
(decrementado en
cada router)

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

¿Cuánta ineficiencia
hay en TCP?

- 20 bytes de TCP
- 20 bytes de IP
- = 40 bytes + datos
capa aplicación

32 bits



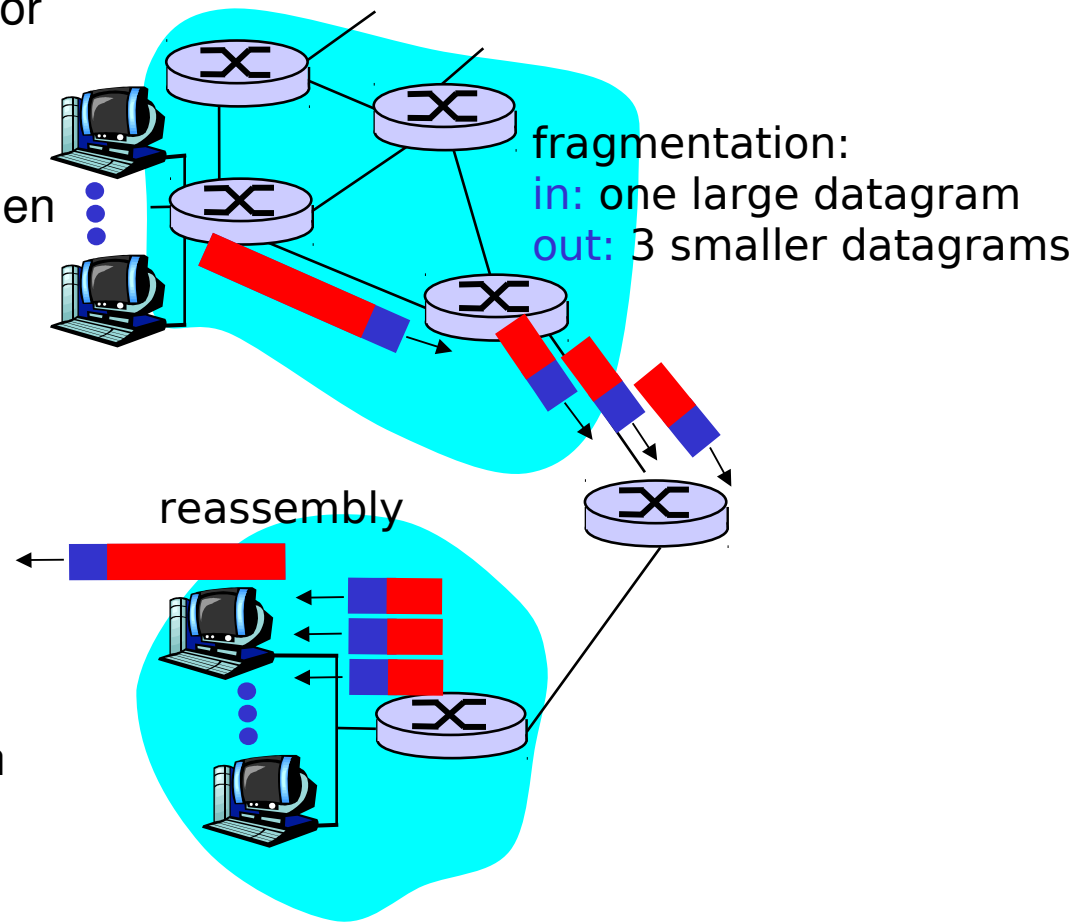
Largo total
datagrama
(bytes)

Para
fragmentación
y re-ensamble

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

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 “rearma” en el **destino final**
 - Bits del encabezado IP se usan para identificar y ordenar fragmentos relacionados



Fragmentación y re-ensamble IP

↖ Más fragmentos?

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
 $1480/8 = 185$

Un datagrama grande es transformado en varios datagramas más pequeños

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

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

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

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

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

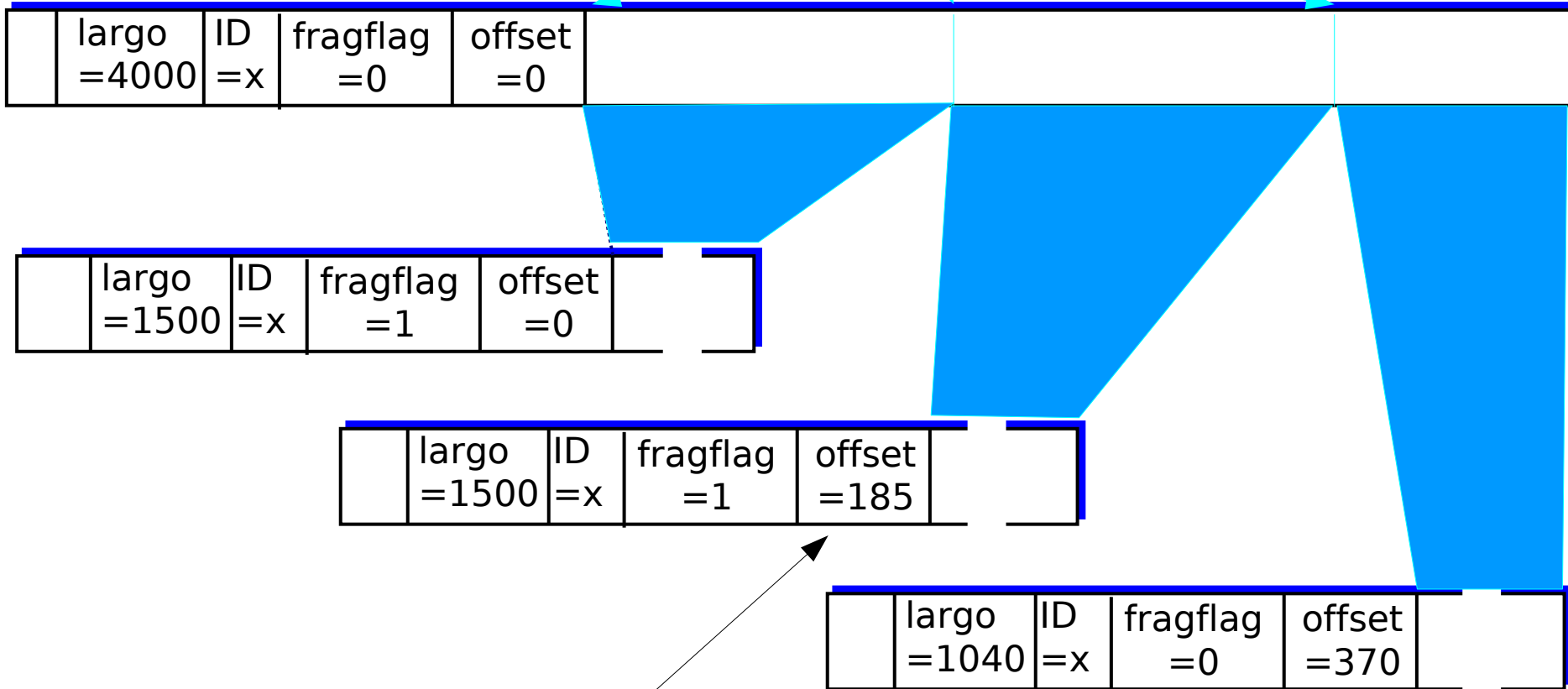
Más header => 1040

byte insertado en posición $370 * 8 = 2960$

Fragmentación y re-ensamble

Más fragmentos?

Múltiplo de 8



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

Un destino de una red IP recibe un 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?



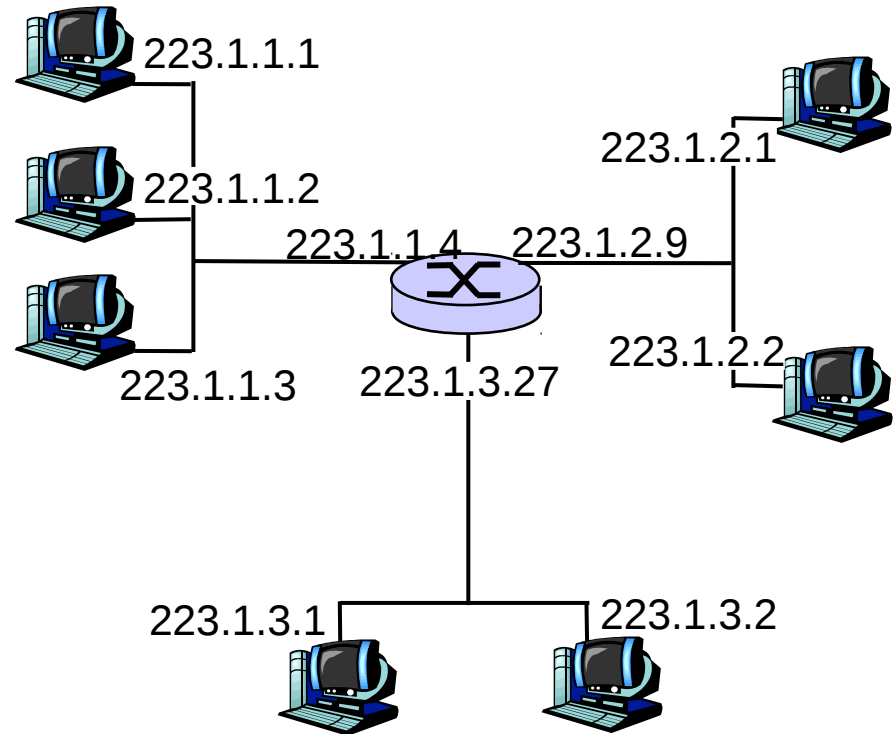
- Como se trata de fragmentos, el paquete original fue dividido en fragmentos que quepan en el MTU más pequeño de la ruta. El MTU debe ser superior o igual a 444, e inferior a $(20+424+8)=452$.
- Suponiendo que son los únicos fragmentos y no se ha perdido ninguno, el datagrama original es de tamaño $20+(444-20)+(444-20)+(253-20)=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

Capítulo 4: Capa de Red

- 4.1 Introducción
- 4.2 Circuitos virtuales y redes de datagramas
- 4.3 ¿Qué hay dentro de un router?
- **4.4 IP: Internet Protocol**
 - Formato de Datagrama
 - **Direccionamiento IPv4**
 - ICMP
 - IPv6
- 4.5 Algoritmo de ruteo
 - Estado de enlace
 - Vector de Distancias
 - Ruteo Jerárquico
- 4.6 Ruteo en la Internet
 - RIP
 - OSPF
 - BGP
- 4.7 Ruteo Broadcast y multicast

Direccionamiento IP: introducción

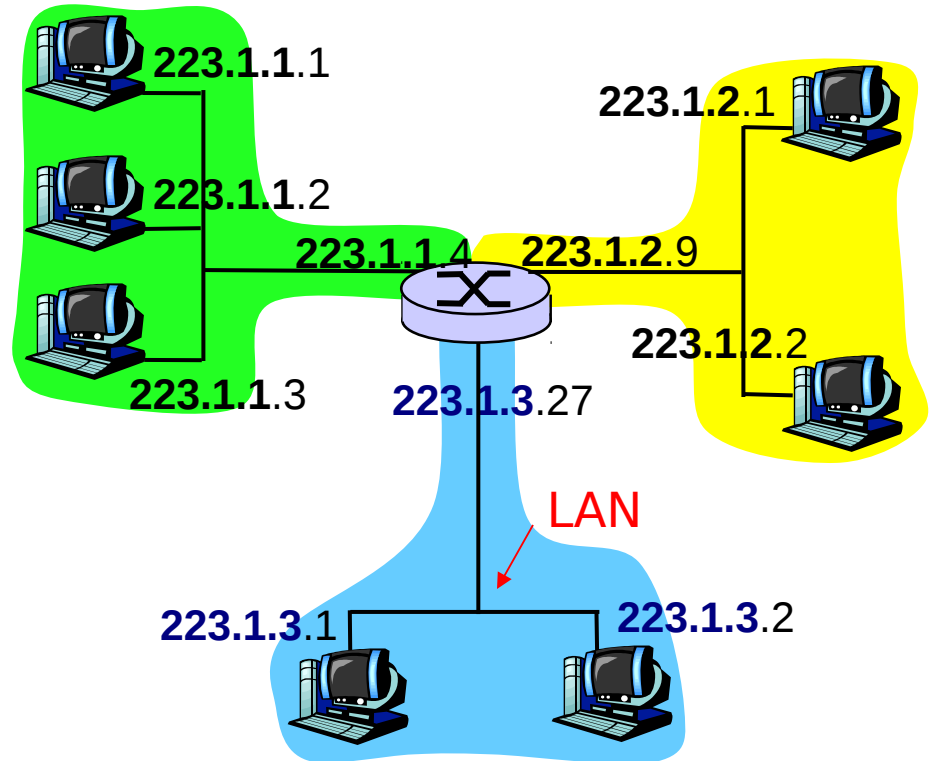
- ▣ **Dirección IP:** identificador de 32-bit del host, *interfaz* del router
- ▣ **Interfaz:** conexión entre host y router, enlace físico
 - ▣ Router típicamente tiene múltiples interfaces (bocas)
 - ▣ Host puede tener múltiples interfaces
 - ▣ Dirección IP está asociada a cada interfaz



$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_1 \underbrace{00000001}_1 \underbrace{00000001}_1$$

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 o hub)



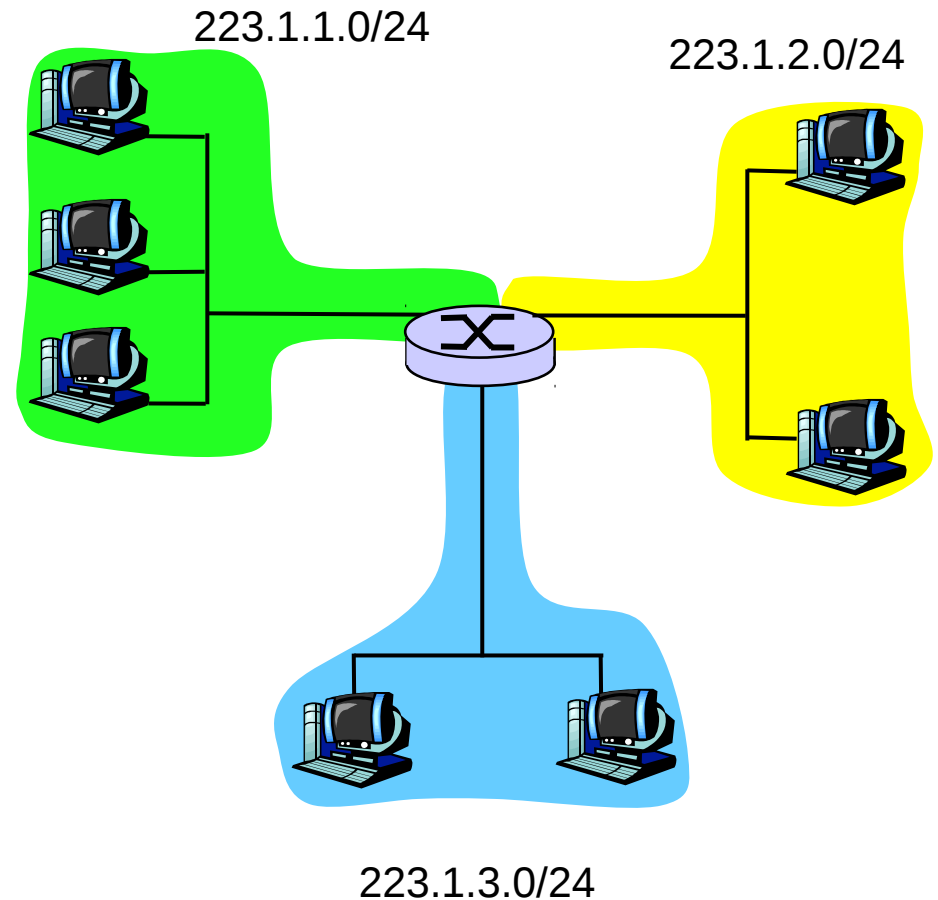
Red consiste de 3 sub-redes

Las direcciones IP están organizadas jerárquicamente

Sub-redes

Receta

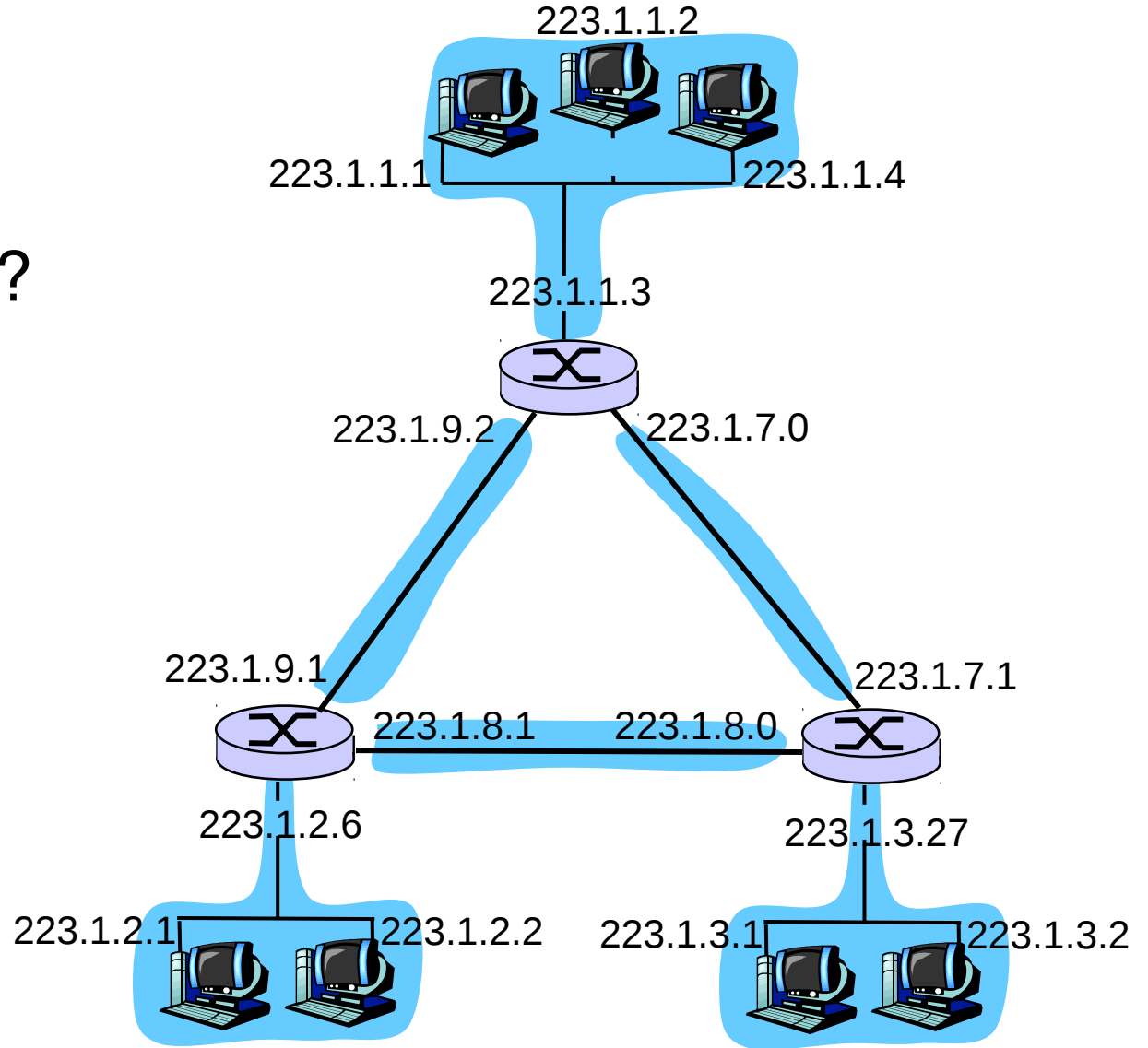
- Para determinar las sub-redes, desconectar las interfaces del router para crear redes tipo islas independientes.
- Cada red independiente es una **sub-red**.



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

Sub-redes

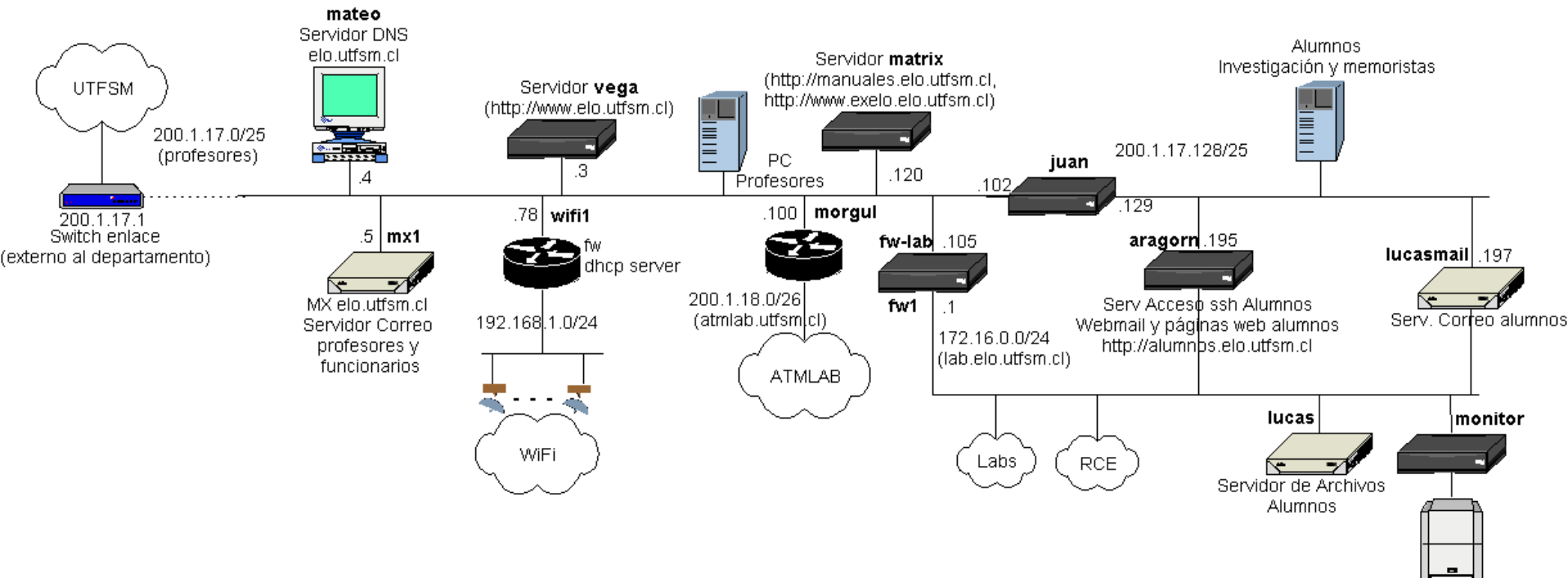
Cuántas hay?



RED ELO año 2004

http://www.elo.utfsm.cl/~rce/images/stories/rce/diagrama_red_elo_todo.png

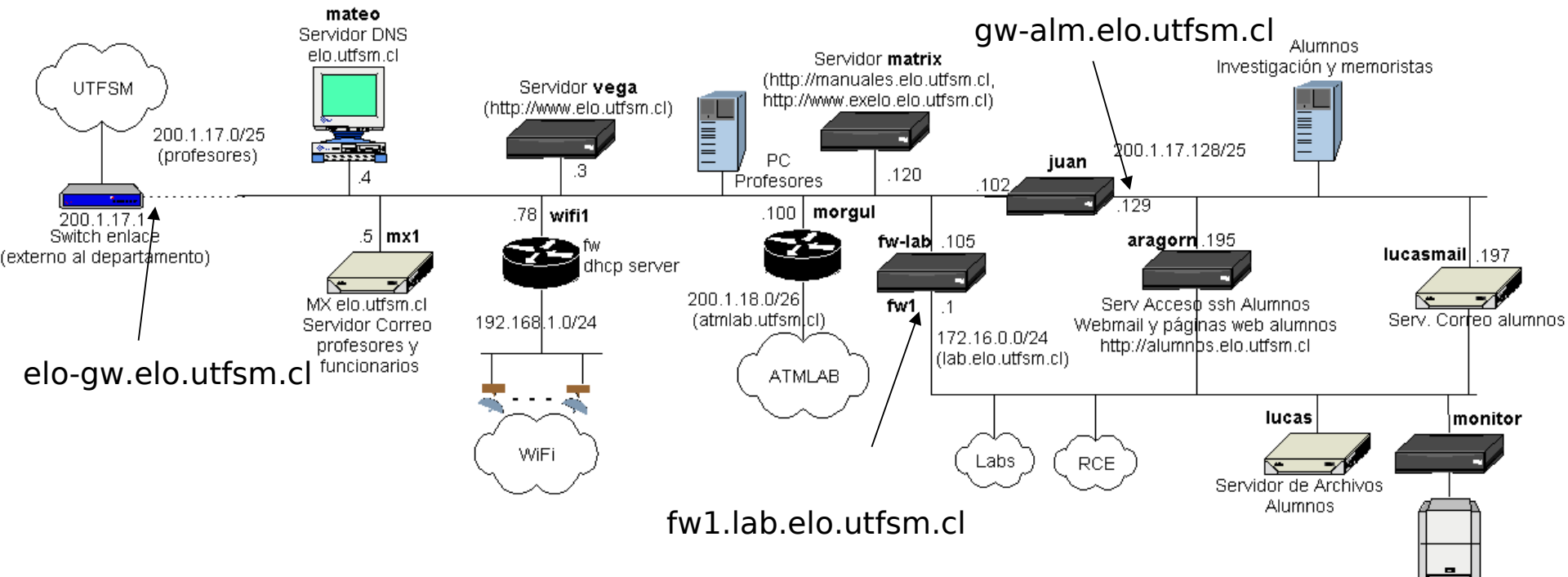
Diagrama de conexiones lógicas en Elo.



Nota: Las IPs: 192.168.1.0 y 10.0.0.0 son para redes privadas. Para que estas máquinas sean vistas de afuera se tiene que usar NAT.

Ejemplo: traceroute desde red ELO años atrás

Diagrama de conexiones lógicas en Elo.



```
aragorn:~$ traceroute www.google.com
```

```
traceroute: Warning: www.google.com has multiple addresses; using 216.239.37.104
```

```
traceroute to www.l.google.com (216.239.37.104), 30 hops max, 38 byte packets
```

```
1 gw-alm (200.1.17.129) 0.151 ms 0.128 ms 0.130 ms
```

```
2 elo-gw (200.1.17.1) 0.668 ms 2.125 ms 0.590 ms
```

```
3 * * *
```

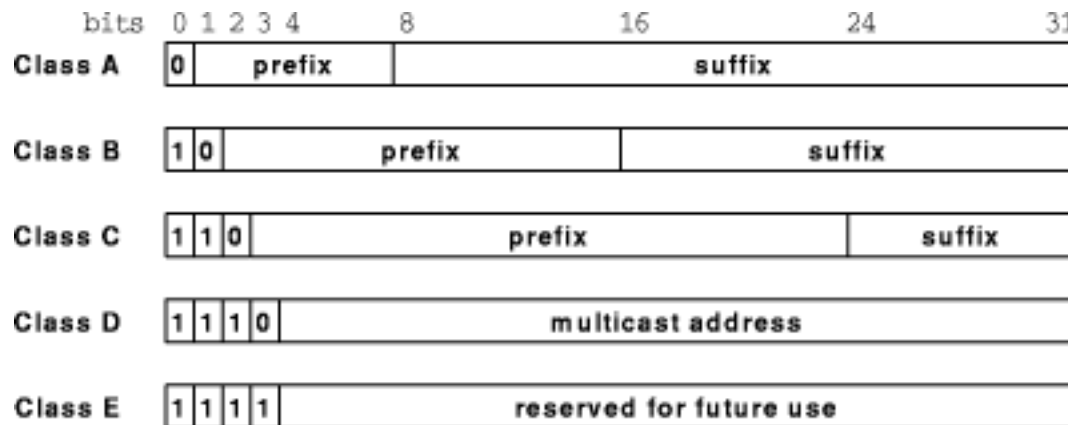
Direccionamiento IP: CLASES

Clases (el pasado, algo del lenguaje se ha mantenido)

- Porción de dirección de la red (sub-red) se hace de tamaño fijo
- Ejemplo: Clase C



Classful addressing: Esquema original (con clases A, B, C, D, E)



Clase A = subnet /8
Clase B = subnet /16
Clase C = subnet /24

¿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 requieren conexión a Internet.
- Para este propósito se reservó una subred de cada clase para crear redes privadas. Éstas son:

10.0.0.0/8 con 2^{24} direcciones => **00001010.xxxxxxxx.X.X**

172.16.0.0/12 con 2^{20} direcciones => **10101100.0001xxxx.X.X**

192.168.0.0/16 con 2^{16} direcciones => **11000000.10101000.XX**

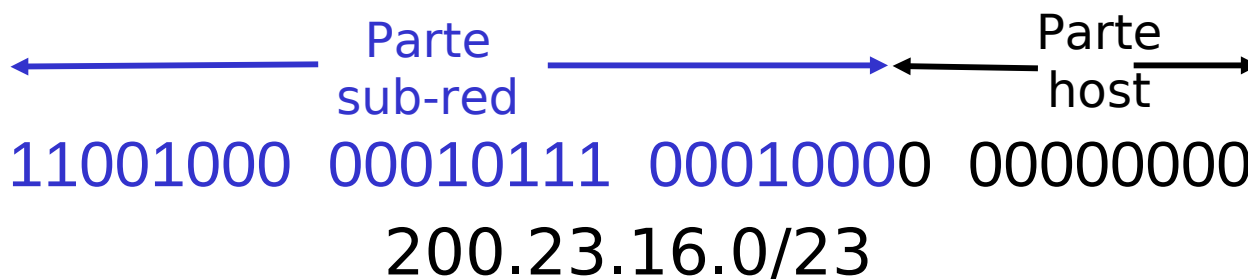
Agotamiento de Direcciones IP

- Conforme más subredes se crearon y conectaron a Internet, las direcciones IP se comenzaron a agotar.
- 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)

Direccionamiento IP: CIDR

CIDR: Classless InterDomain Routing

- Porción de dirección de la red (subred) se hace de tamaño arbitrario (no múltiplo de 8)
- Formato de dirección: **a.b.c.d/x**, donde x es el # de bits de la dirección de sub-red



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



- $32-26=6 \Rightarrow$ hay 64 direcciones IP, de las cuales 62 puedo asignar a máquinas.

Direcciones IP: ¿Cómo obtener una?

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

- Configurada por el administrador en un archivo
 - Windows: control-panel->network->configuration->tcp/ip->properties
 - Linux: /etc/network/interfaces
- Vía protocolo de configuración dinámica **DHCP: Dynamic Host Configuration Protocol**: el host obtiene la dirección dinámicamente desde un servidor
 - “plug-and-play” (más adelante)

Direcciones IP: ¿Cómo obtener una?

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.

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 **C**orporation for **A**ssigned **N**ames and **N**umbers

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

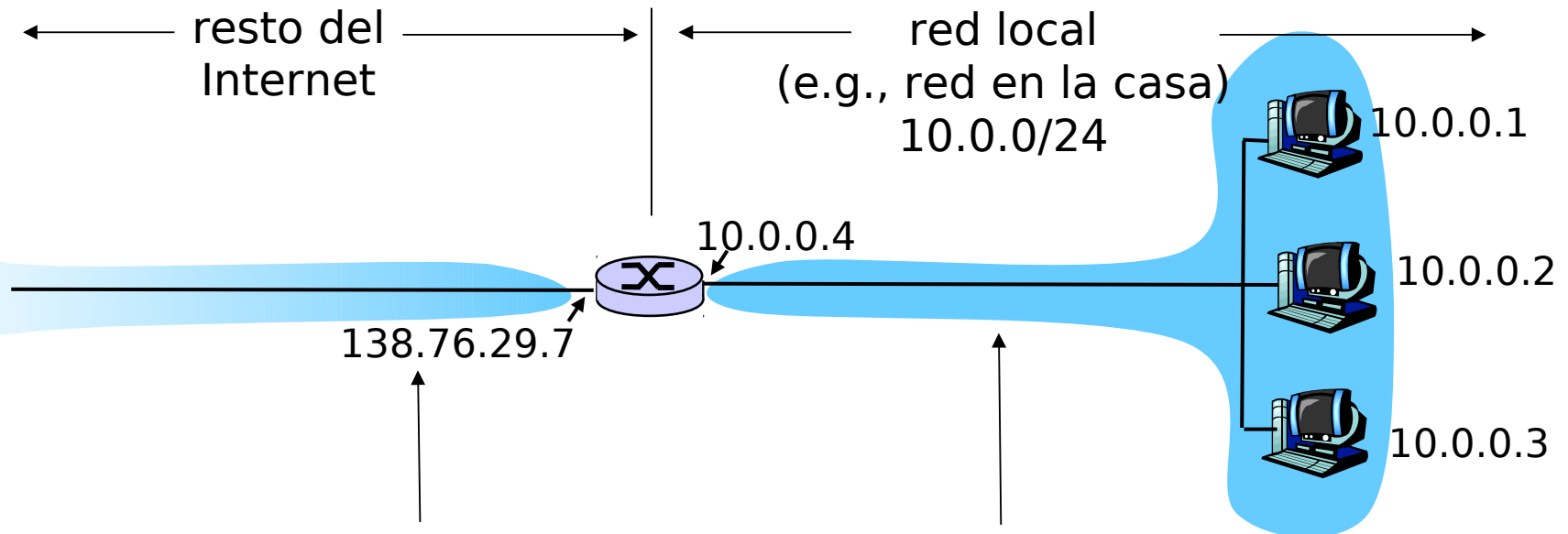
Para América Latina la oficina es LACNIC:

<http://lacnic.net/>

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

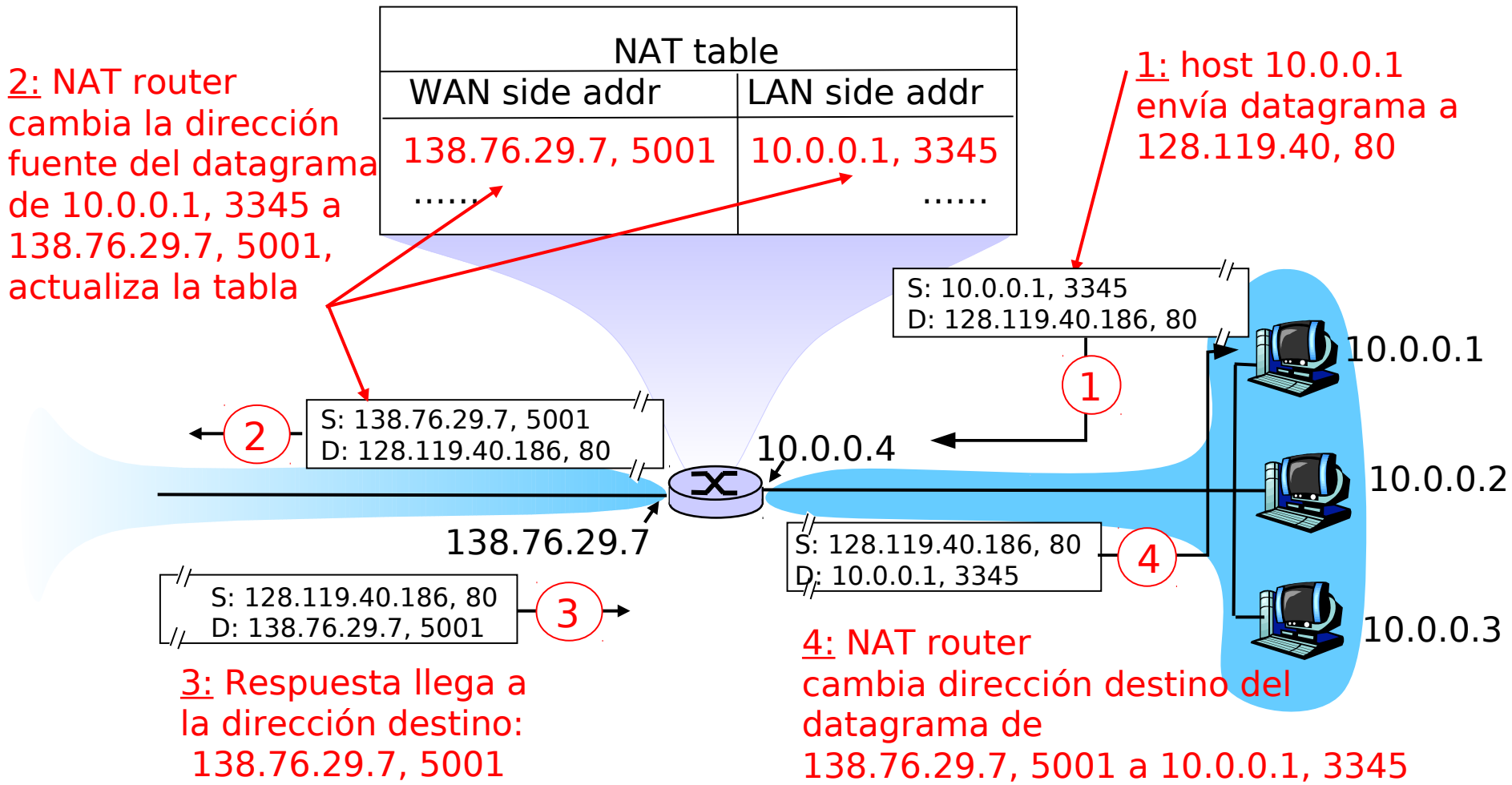
Datagramas con fuente o destino en esta red tienen direcciones 10.0.0/24 (También se puede usar: 192.168.0/24 ó 172.16.0/24)

NAT: Network Address Translation

Implementación ruteador 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 con una única dirección IP dentro de la LAN!
- 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

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 Circuitos virtuales y redes de datagramas
- ▣ 4.3 ¿Qué hay dentro de un router?
- ▣ **4.4 IP: Internet Protocol**
 - ▣ Formato de Datagrama
 - ▣ Direccionamiento IPv4
 - ▣ **ICMP**
 - ▣ IPv6
- ▣ 4.5 Algoritmo de ruteo
 - ▣ Estado de enlace
 - ▣ Vector de Distancias
 - ▣ Ruteo Jerárquico
- ▣ 4.6 Ruteo en la Internet
 - ▣ RIP
 - ▣ OSPF
 - ▣ BGP
- ▣ 4.7 Ruteo Broadcast y multicast

ICMP: Internet Control Message Protocol

- Usado por hosts & routers para comunicar información a nivel de la red
 - Reporte de errores: host inalcanzable, o red, o puerto, o protocolo
 - Echo request/reply (usado por ping)
 - Usado por traceroute (TTL expired, dest port unreachable)
- Opera en capa transporte:
 - ICMP son llevados por datagramas IP
- **Mensajes ICMP:** tipo y código de error, más primeros 8 bytes del datagrama que causó el error

<u>Type</u>	<u>Code</u>	<u>description</u>
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - seldom used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute e ICMP

- La fuente envía una serie de segmentos UDP al destino
 - Primero usa TTL=1
 - Luego usa TTL=2, etc.
 - Número de puerto (probablemente) no usado en destino
 - Cuando el n-ésimo datagrama llega a n-ésimo router:
 - Router descarta el datagrama, y
 - Envía a la fuente un mensaje ICMP “TTL expirado” (tipo 11, código 0)
 - Mensaje incluye nombre del router y dirección IP
 - Cuando mensaje ICMP llega, la fuente calcula el RTT
 - Traceroute hace esto 3 veces
- ### Criterio de parada
- Segmento UDP eventualmente llega al host destino
 - Host destino retorna paquete ICMP “puerto inalcanzable” (tipo 3, código 3)
 - Cuando la fuente recibe este ICMP, para.

Capítulo 4: Capa de Red

- ▣ 4.1 Introducción
- ▣ 4.2 Circuitos virtuales y redes de datagramas
- ▣ 4.3 ¿Qué hay dentro de un router?
- ▣ **4.4 IP: Internet Protocol**
 - ▣ Formato de Datagrama
 - ▣ Direccionamiento IPv4
 - ▣ ICMP
 - ▣ **IPv6**
- ▣ 4.5 Algoritmo de ruteo
 - ▣ Estado de enlace
 - ▣ Vector de Distancias
 - ▣ Ruteo Jerárquico
- ▣ 4.6 Ruteo en la Internet
 - ▣ RIP
 - ▣ OSPF
 - ▣ BGP
- ▣ 4.7 Ruteo Broadcast y multicast

IPv6

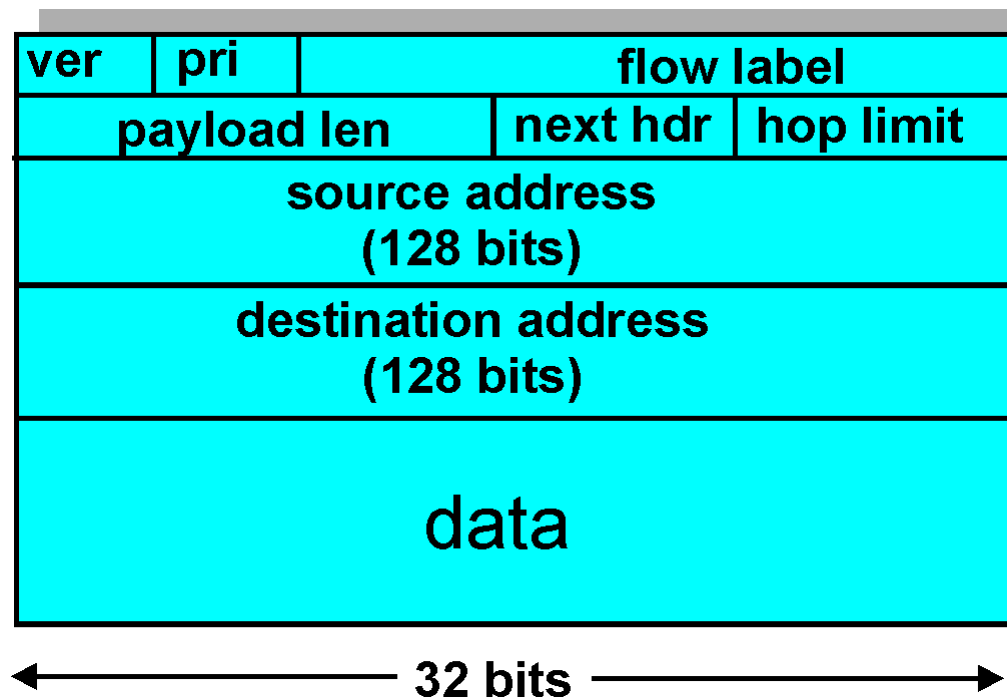
- ▣ **Motivación Inicial:** espacio de direcciones de 32-bit pronto serán completamente asignadas.
- ▣ Motivación adicional:
 - ▣ Formato de encabezado debería ayudar a acelerar el procesamiento y re-envío (por aumento de tasas en red)
 - ▣ Cambiar encabezado para facilitar QoS (Quality of Service)

Formato de datagrama IPv6:

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

Encabezado IPv6

- **Prioridad:** 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



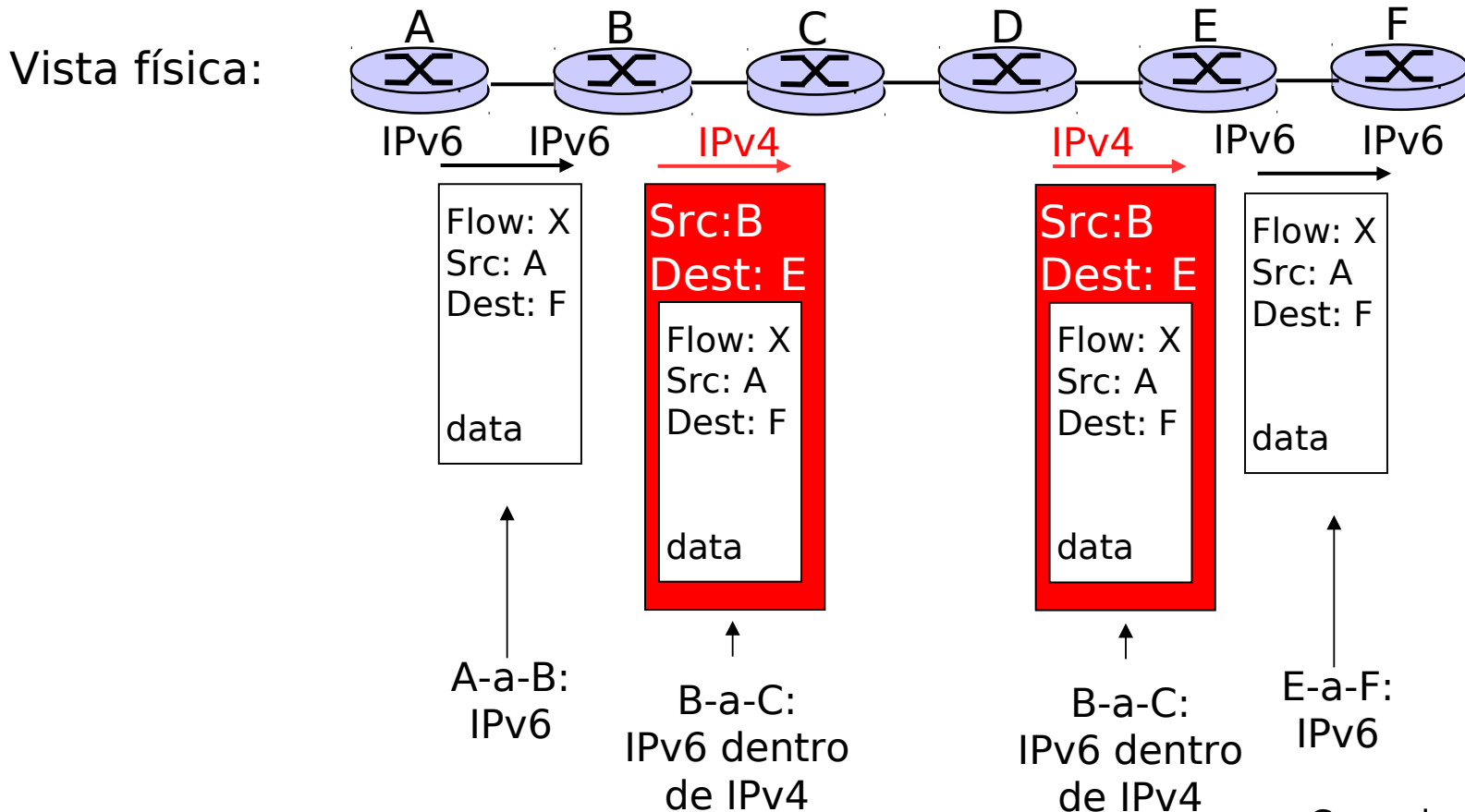
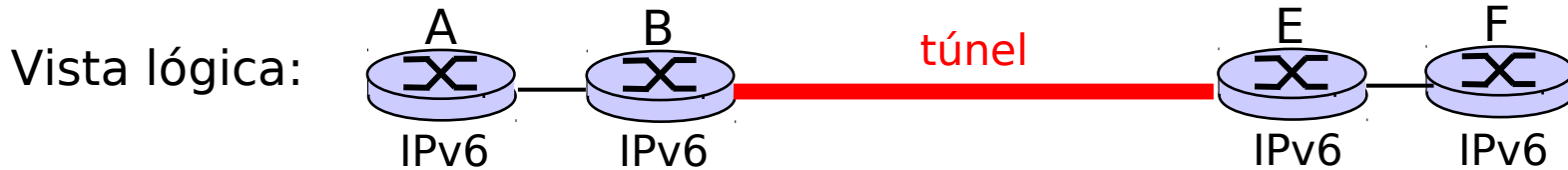
Otros cambios de IPv4 a v6

- ▣ *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



- ¿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.

Capítulo 4: Capa de Red

- ▣ 4.1 Introducción
- ▣ 4.2 Circuitos virtuales y redes de datagramas
- ▣ 4.3 ¿Qué hay dentro de un router?
- ▣ 4.4 IP: Internet Protocol
 - ▣ Formato de Datagrama
 - ▣ Direccionamiento IPv4
 - ▣ ICMP
 - ▣ IPv6
- ▣ 4.5 **Algoritmos de ruteo**
 - ▣ Estado de enlace
 - ▣ Vector de Distancias
 - ▣ Ruteo Jerárquico
- ▣ 4.6 Ruteo en la Internet
 - ▣ RIP
 - ▣ OSPF
 - ▣ BGP
- ▣ 4.7 Ruteo Broadcast y multicast