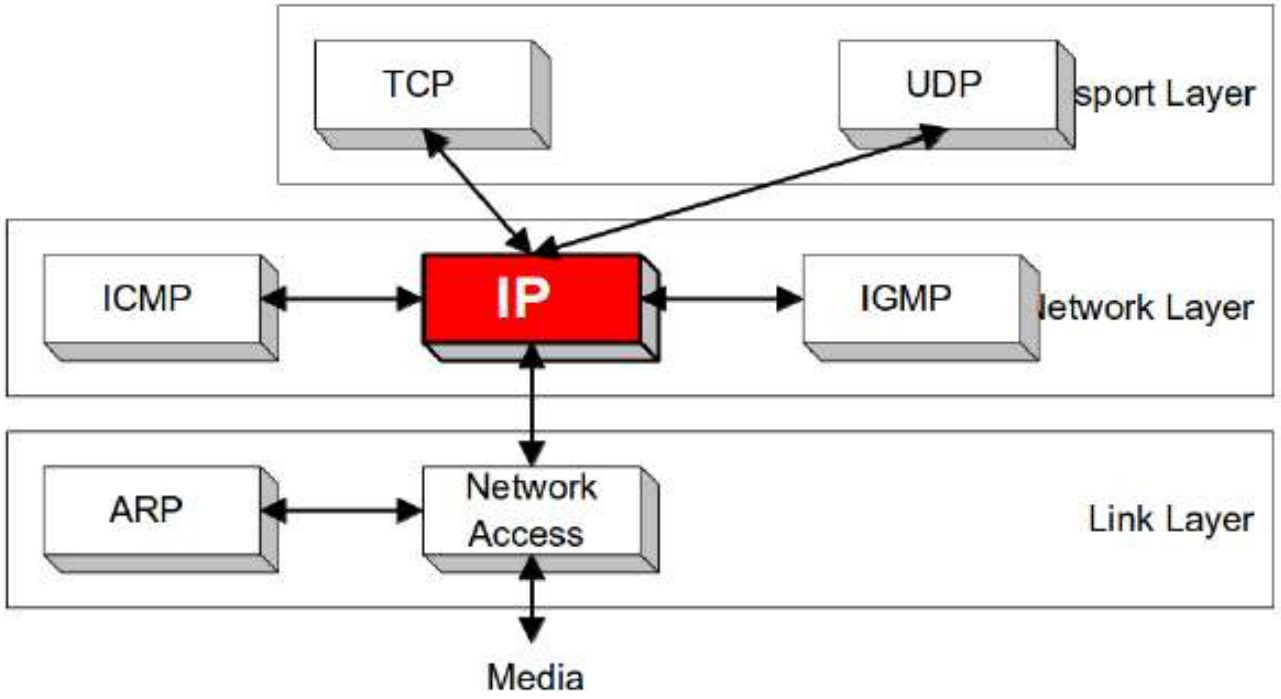
REDES DE COMPUTADORAS 1

Clase 4: La capa de RED

La Capa de Red

- Funciones claves.
- Modelos de servicio.
- Redes de Circuitos virtuales / Datagramas
- Interior de un Router
- IP: Internet Protocol
  - Formato de Datagrama
  - Direccionamiento IPv4
  - ICMP (Protocolo de mensajes de control de Internet)
  - IPv6
- Algoritmos de ruteo
- Ruteo en Internet
- Ruteo Broadcast y multicast

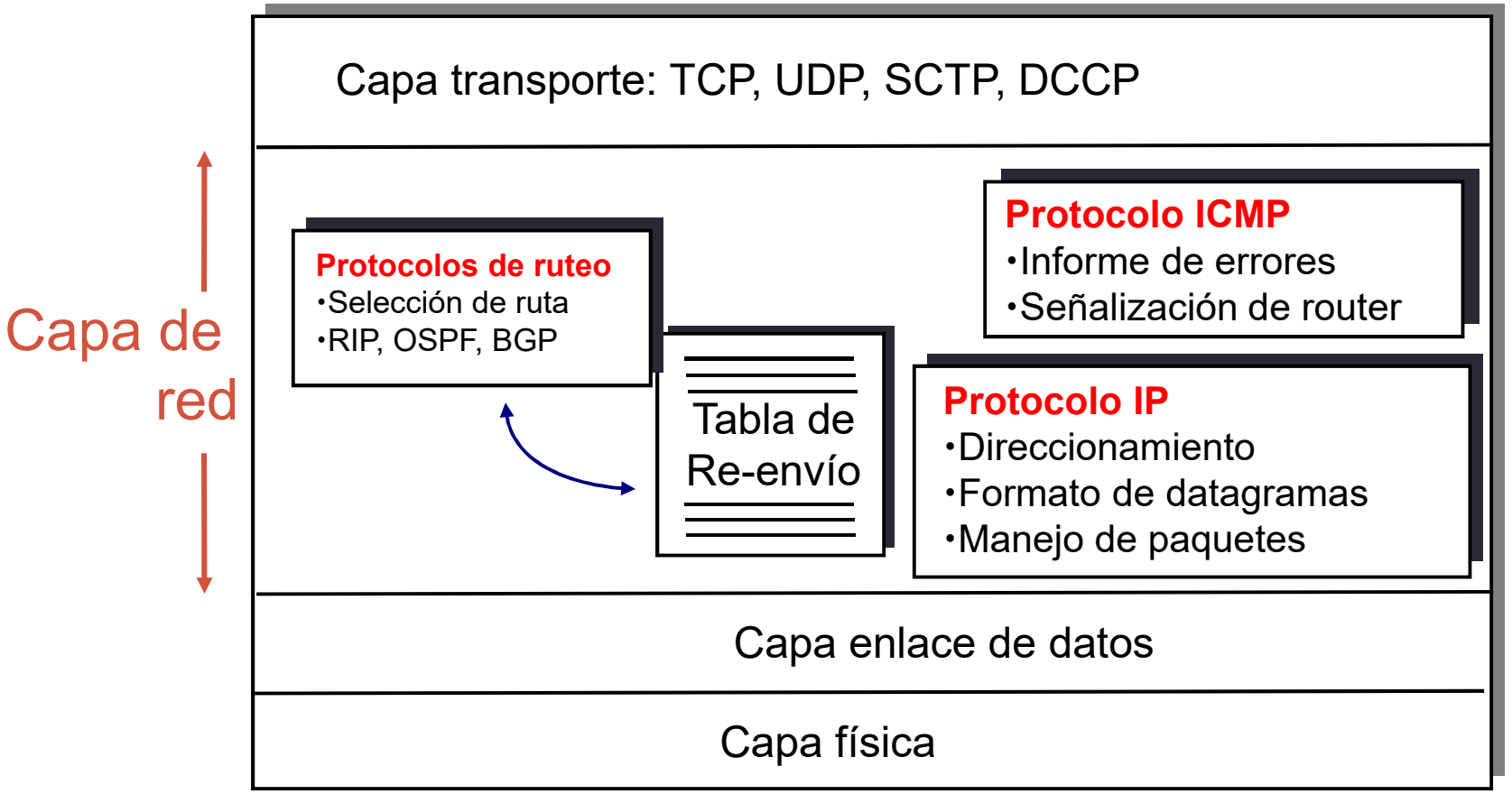
Esquema de IP en TCP/IP



- Es el núcleo de internet
- Requiere de protocolos

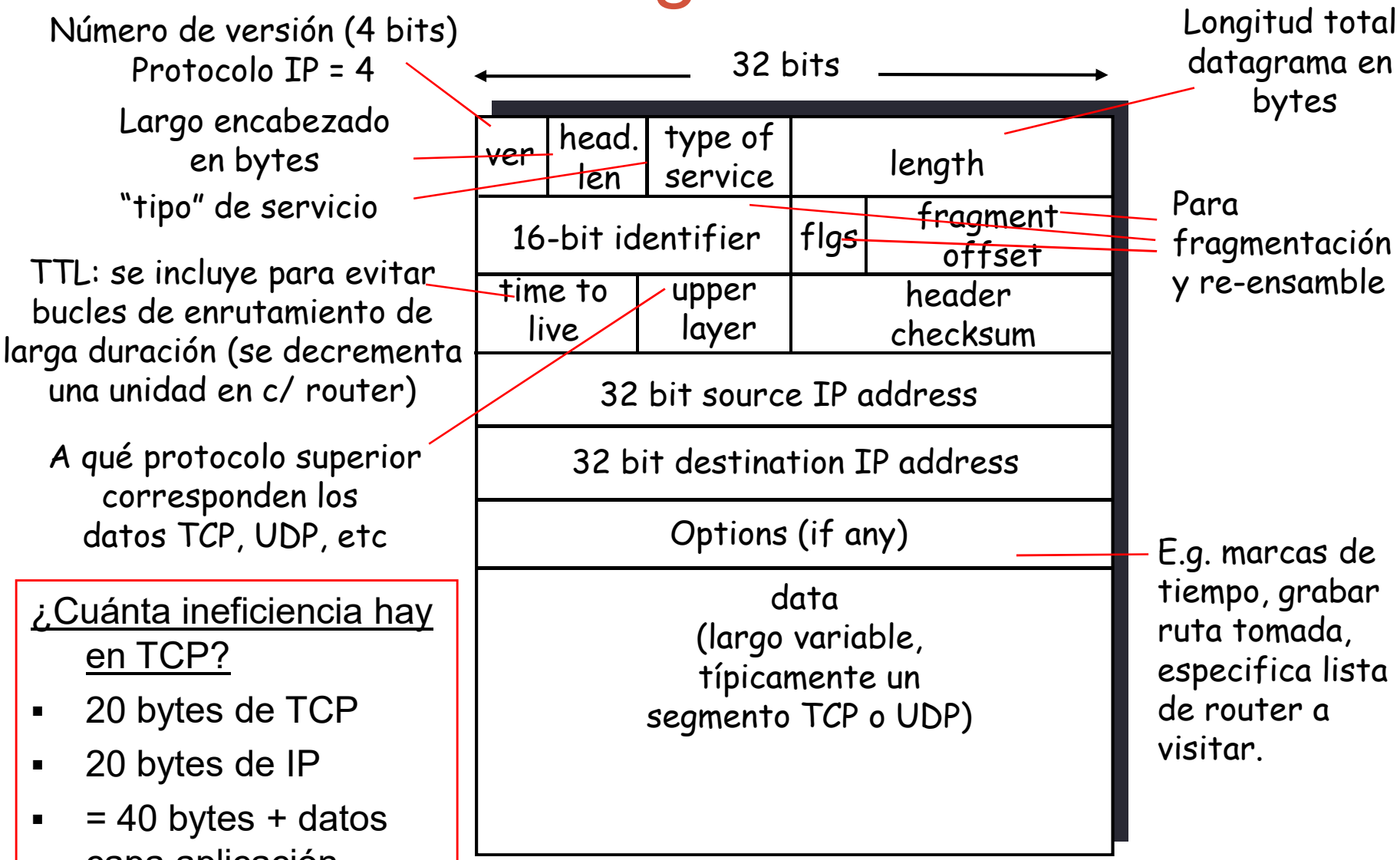
Capa de red en Internet

- 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

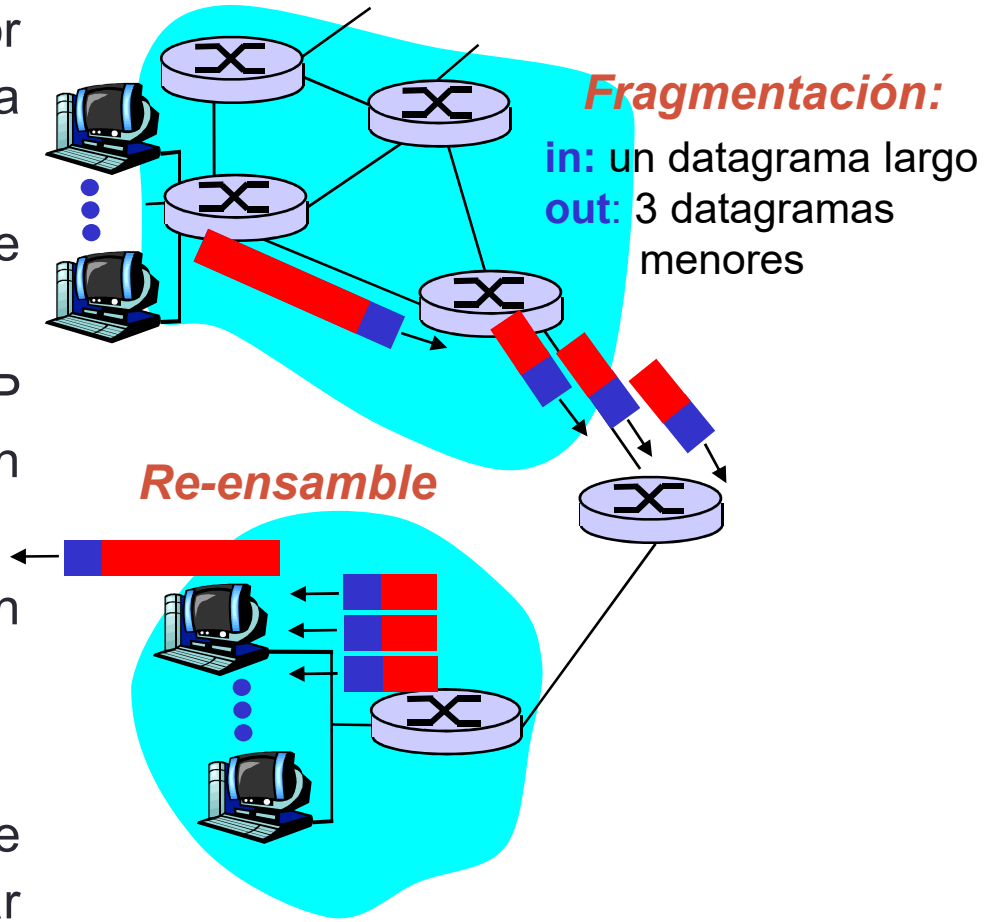


¿Cuánta ineficiencia hay en TCP?

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

Fragmentación y re-ensamble IP

- Cada enlace de red tienen MTU (max. transmission unit) – mayor tamaño de la trama en la capa enlace.
  - Diferentes tipos de enlace tienen diferentes MTUs
- Por esto es que un datagrama IP grande es dividido –fragmentado- 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



MTU (Maximum Transfer Unit)

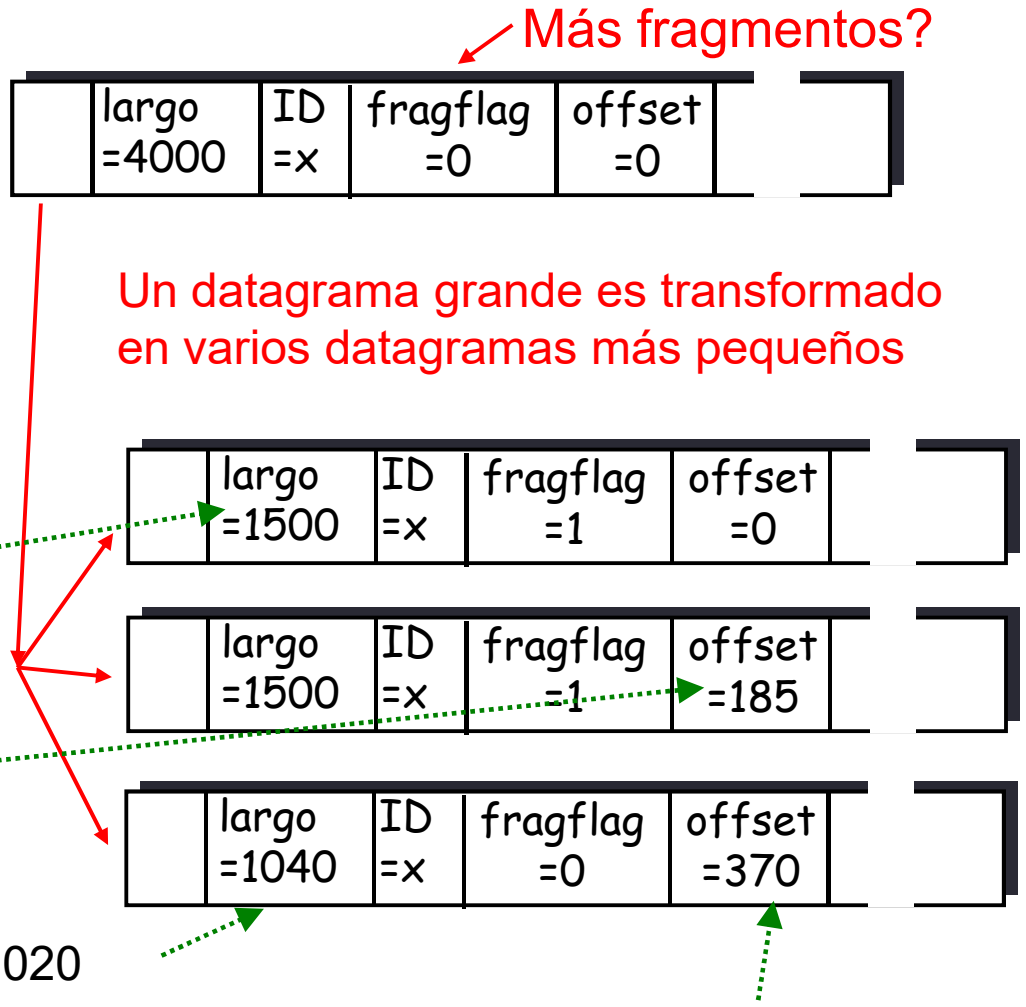
Protocolo a nivel de enlace	MTU(bytes)
PPP (valor por defecto)	1500
PPP (bajo retardo)	296
SLIP	1006 (límite original)
X.25	1600 (varía según las redes)
Frame relay	Al menos 1600 normalmente
SMDS	9235
Ethernet versión 2	1500
IEEE 802.3/802.2	1492
IEEE 802.4/802.2	8166
Token Ring IBM 16 Mbps	17914 máximo
IEEE 802.5/802.2 4 Mbps	4464 máximo
FDI	4352
Hyperchannel	65535
ATM	9180

Valor de MTU para los protocolos mas comunes a nivel de enlace.

Fragmentación y re-ensamble IP

Ejemplo

- Datagrama de 4000 bytes (20 bytes encabezado IP + 3980 en campo datos datagrama)
- MTU = 1500 bytes



Capacidad máxima de campo de datos de datagrama: 1480 bytes

offset en bloques de 8 bytes
1480/8 = 185

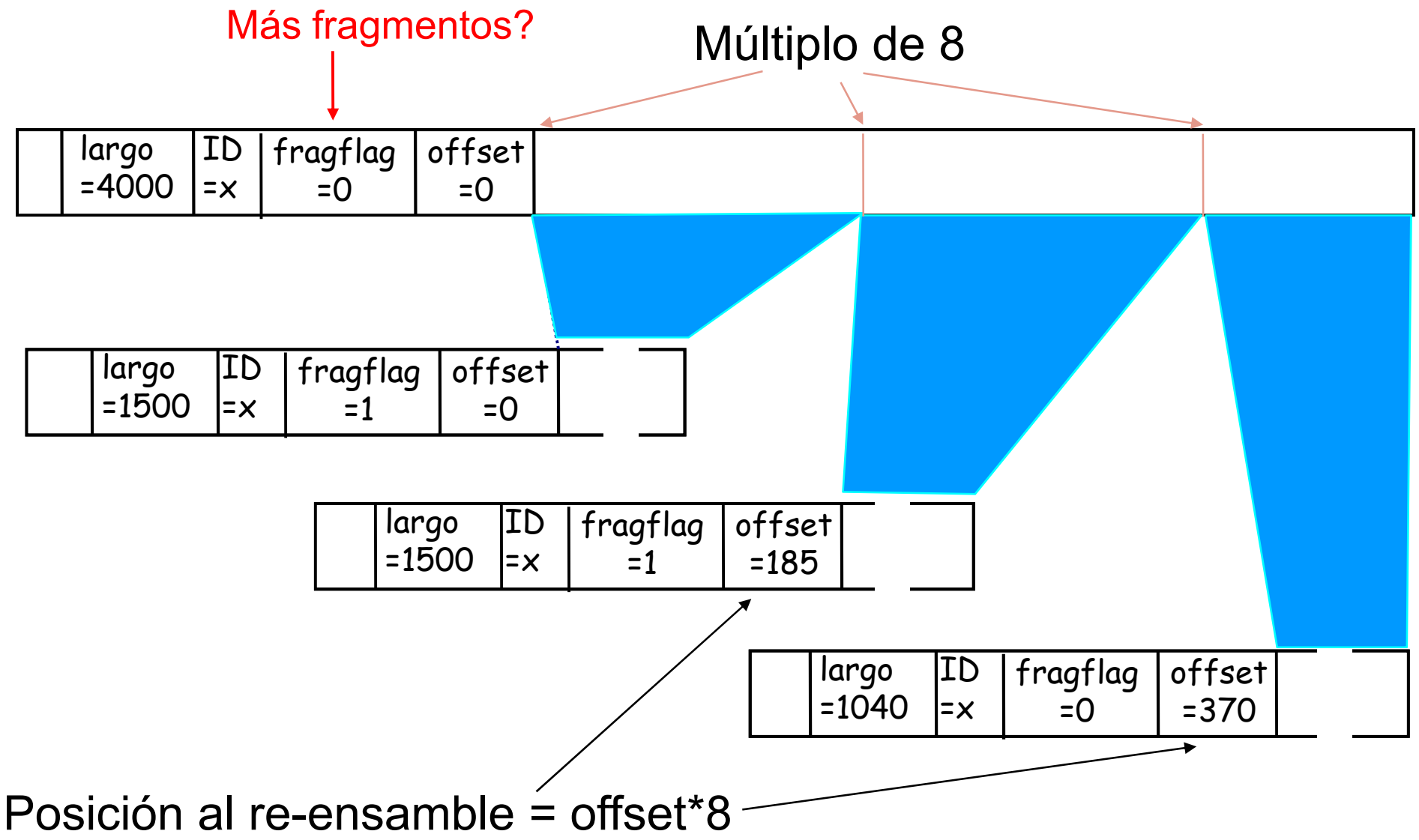
Largo datos último:

3980 - 1480 - 1480 = 1020

Más el encabezado ➔ 1040

byte insertado en posición 370*8=2960

Fragmentación y re-ensamble IP



Ejemplo

Un destino de una red IP recibe un fragmentos de tamaños 444, 444 y 253 bytes, ¿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.

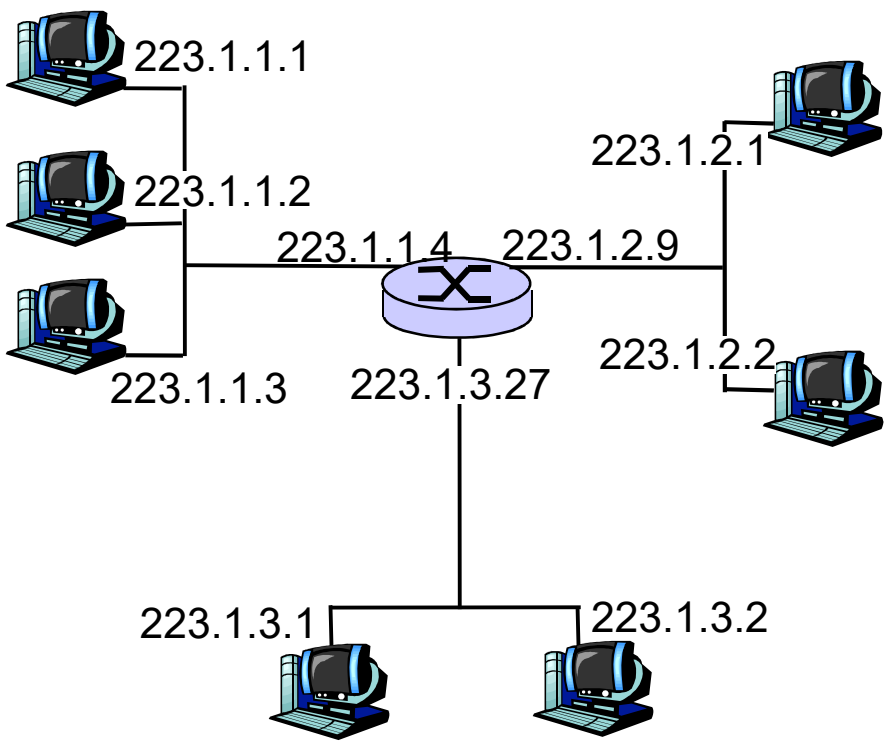
  ➔ 444 bytes ≤ MTU ≤ 444+8 = 452 bytes

- 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.

Direccionamiento IP: Introducción

- Interfaz: límite entre el host y el enlace físico; o entre el router y cualquiera de sus enlaces.
  - Router típicamente tiene múltiples interfaces (bocas)
  - Host puede tener múltiples interfaces
  - Dirección IP está asociada a cada interfaz
- Dirección IP: identificador de 32-bit del host y del interfaz del router

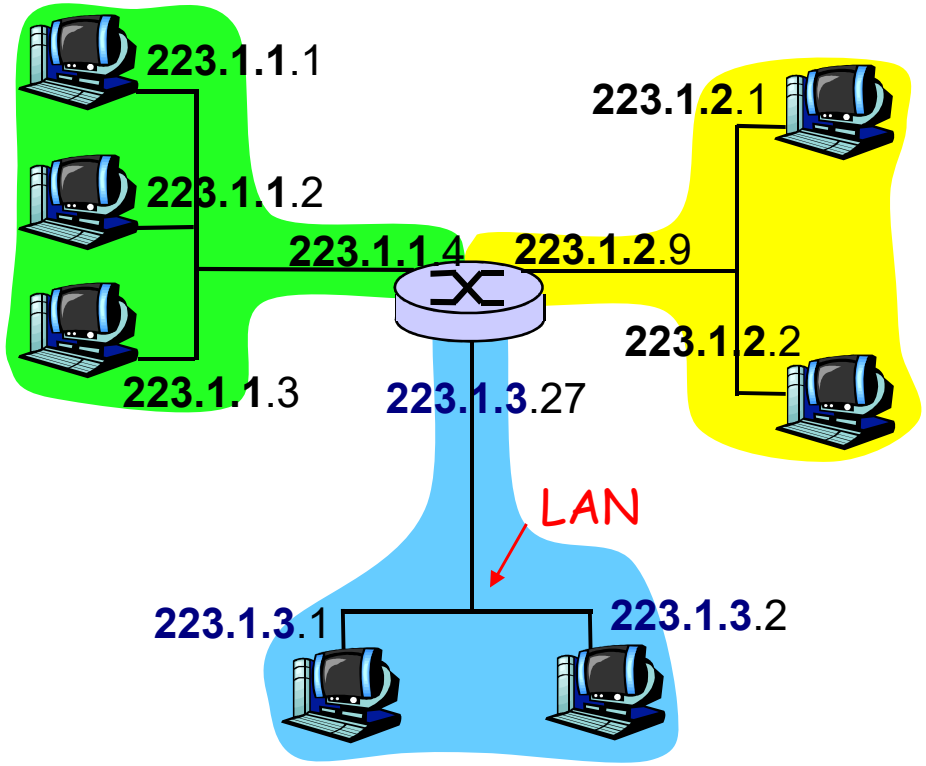


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Sub-redes

- Dirección IP:
  - Dirección de sub-red o netID (bits más significativos)
  - Dirección del host o hostID (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)



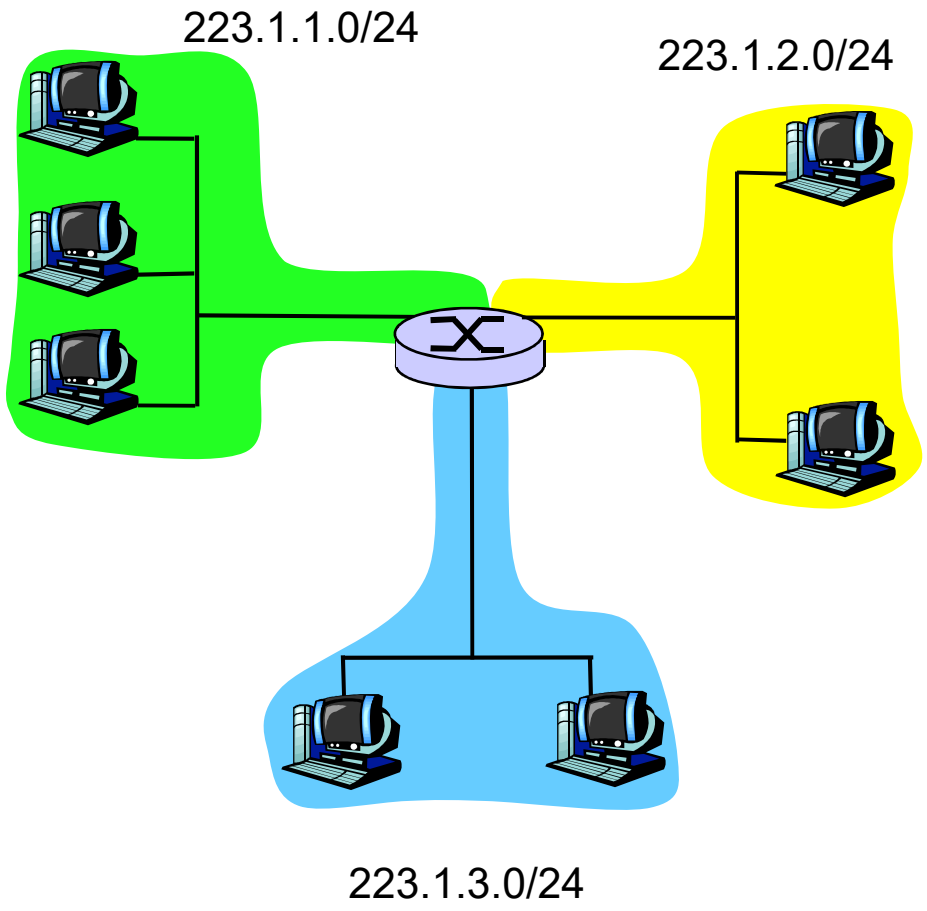
Red consiste de 3 sub-redes

Las direcciones IP están organizadas jerárquicamente

Sub-redes

Receta

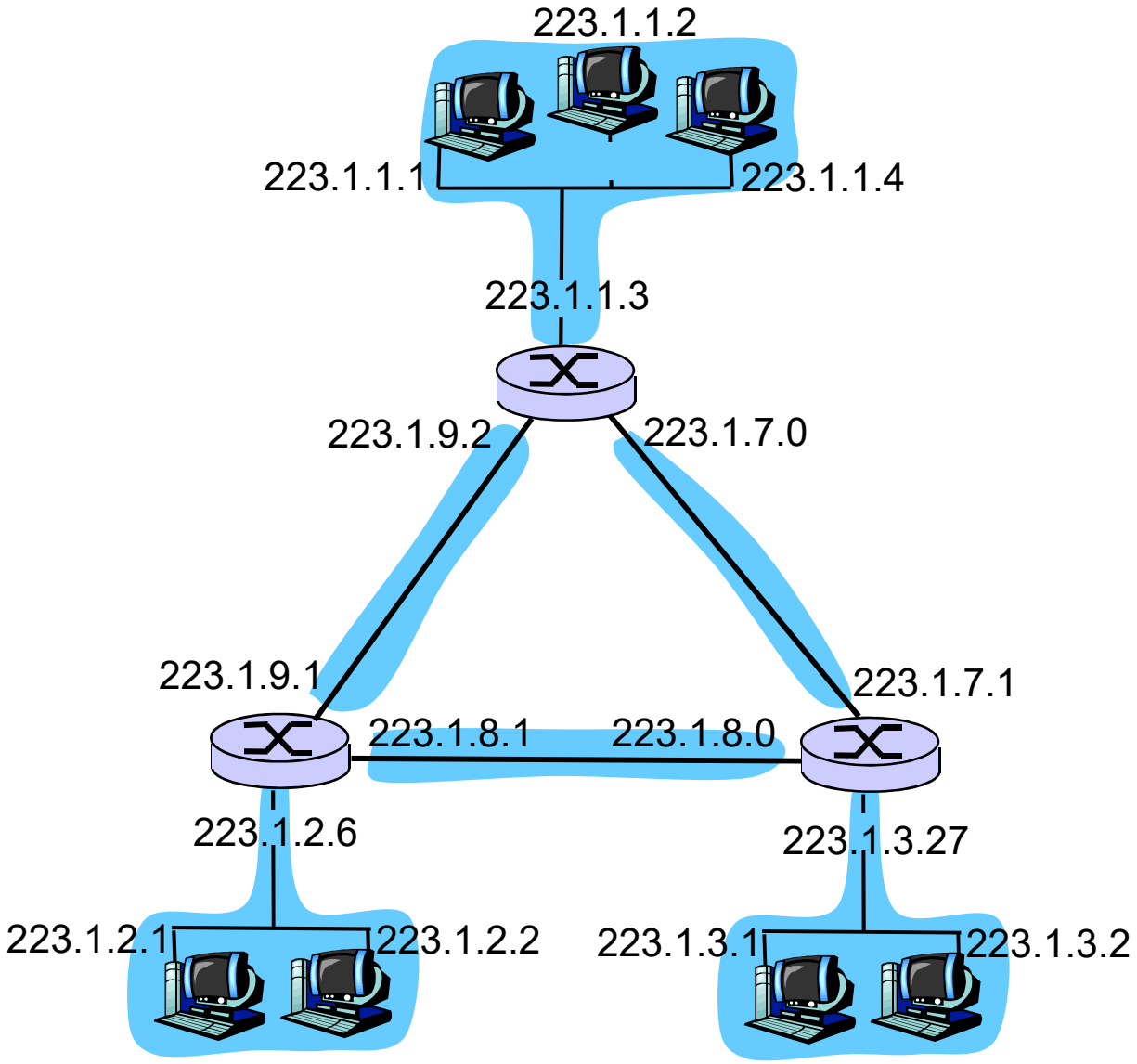
- Para determinar las sub-redes, desconectar las interfaces del router para crear redes tipo islas independientes.
- Cada red independiente es una sub-red.



Máscara de sub-red: /24
=> 24 primeros bits comunes en la subred

Sub-redes

- Cuantas hay?



Máscara

- Una mascara de subred es una secuencia de 32 bits que sirve para distinguir con facilidad que parte de una dirección codifica la subred y que parte el host.

- La máscara permite hacer variable el límite entre el NetID y el HostID de una dirección IP.

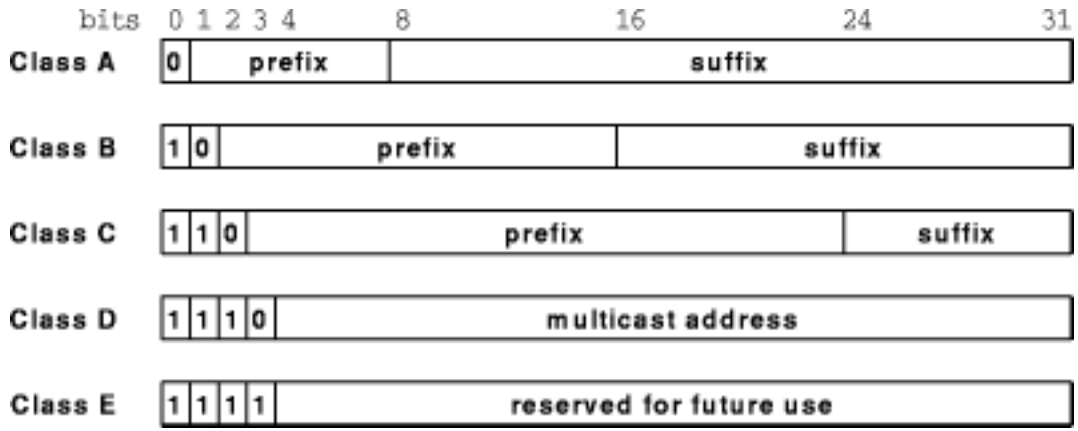
- Poniendo a 1 los bits más significativos de la máscara se identifica el NetID, y el resto de bits a 0 para señalizar el HostID.

Direccionamiento IP: Clases

Clases (***obsoleto***, algo del lenguaje se ha mantenido)

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

Classful addresing: 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

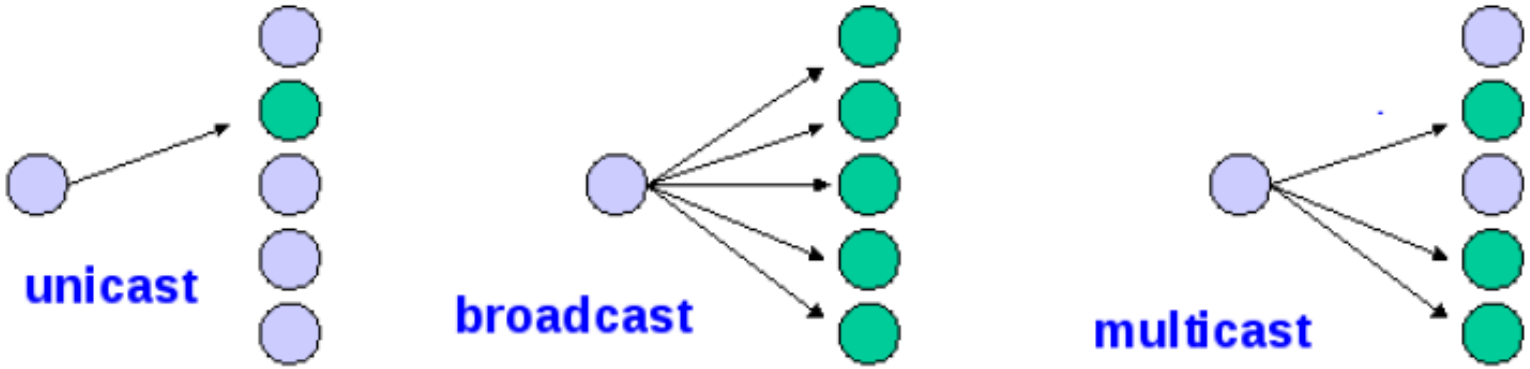
  172.16.0.0/12 con 2^{20} direcciones => **10101100.0001**xxxx.X.X

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

Tipos de Direcciones IP

- **Unicast:** destino a un host/interfaz en particular, son las más comunes.
  - Ej: 172.16.4.21
- **Broadcast:** destino a todos los hosts en una red.
  - Ej: 255.255.255.255
- **Multicast:** destinada a un grupo de hosts en una red o varias redes.
- **Anycast:** destinada al primero que resuelva. IPv4 no hay casos especiales.

Tipos de Direcciones IP



Direcciones IP especiales

- Loopback: unicast, red clase A. 127.0.0.1
  - La más utilizada: 127.0.0.1, local host.
  - Aunque podría ser cualquier otra:
    - 127.10.0.1
    - 127.34.34.1, etc.
- Dirección de una subred: la primera de las direcciones de la subred
  - Ej: 172.16.0.0, 192.168.1.0
- Dirección de broadcast:
  - Directed Broadcast: la última (unos)
    - Ej: 172.16.255.255, 192.168.1.255
  - Limited Broadcast: (all ones)
    - 255.255.255.255
- “Este host”, cuando aún no tiene asignada una dirección
  - 0.0.0.0

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 sub-redes: surge Classless InterDomain Routing (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
- Formato de dirección: a.b.c.d/x, donde x es el # de bits de la dirección de sub-red

Dirección de la subred (ceros en la parte del host):

200.23.16.0/23

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

- 32-26=6 ➔ hay 2^6 = 64 direcciones IP
  ➔ puedo asignar a máquinas: 62

Direcciones IP: ¿Cómo obtener una?

¿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
- DHCP: Dynamic Host Configuration Protocol: el host obtiene la dirección dinámicamente desde un servidor
  - “plug-and-play” (más adelante)

Direcciones IP: ¿Cómo obtener una?

¿Cómo la red obtiene la dirección de subred parte de la dirección IP?

Obteniendo una porción del espacio de direcciones del proveedor ISP.

ISP's block	**11001000 00010111 0001**0000	00000000	200.23.16.0/20

Podría dividir su bloque en 8 bloques de direcciones contiguos de igual tamaño:

Organization 0	**11001000 00010111 0001000**0	00000000	200.23.16.0/23
Organization 1	**11001000 00010111 0001001**0	00000000	200.23.18.0/23
Organization 2	**11001000 00010111 0001010**0	00000000	200.23.20.0/23
...	.....	....	....
Organization 7	**11001000 00010111 0001111**0	00000000	200.23.30.0/23

Direccionamiento IP: la última palabra…

¿Cómo un ISP obtiene un bloque de direcciones?

ICANN: Internet Corporation for Assigned Names and Numbers

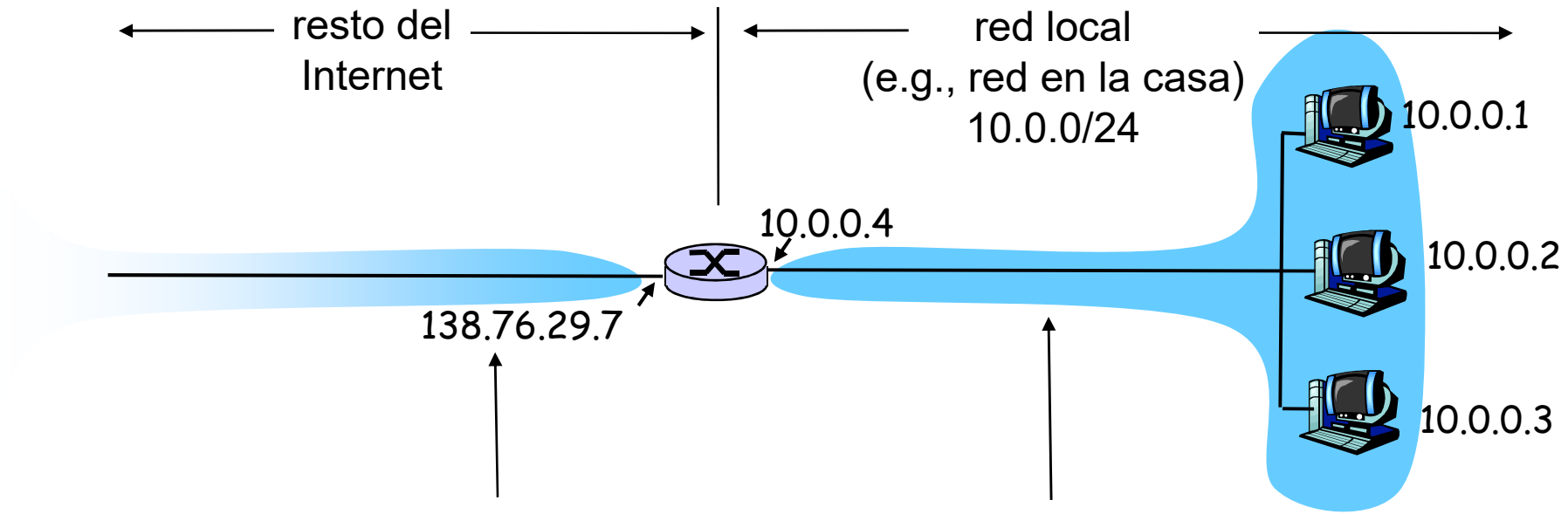
- Asigna direcciones
- Administra DNS
- Asigna nombre de dominio, resuelve disputas

Para América Latina la oficina es LACNIC: http://lacnic.net/

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:

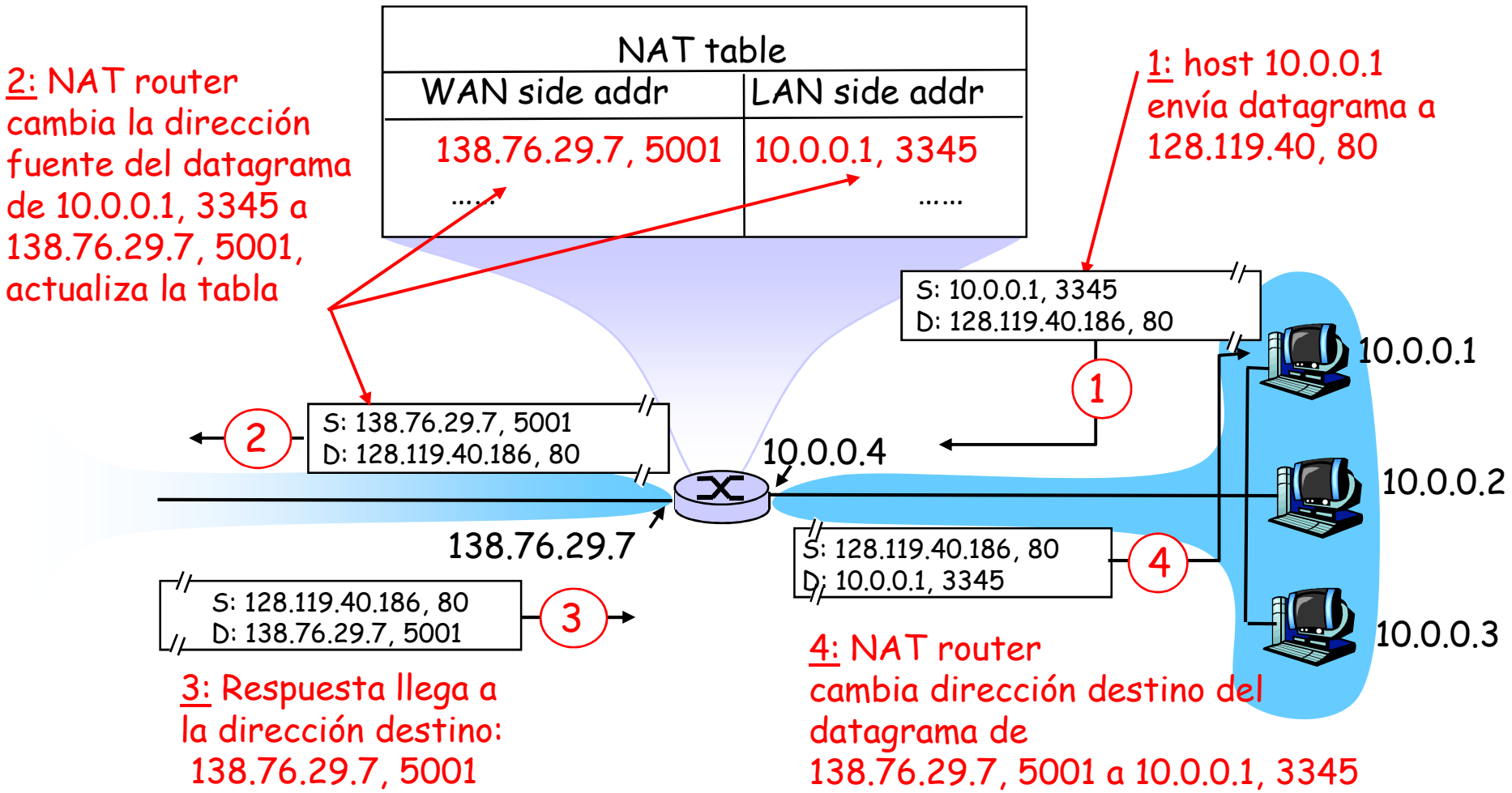
- Para Datagramas salientes: remplazar (IP fuente, # puerto) de cada datagrama saliente por (IP NAT, nuevo # puerto)

. . . 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: remplazar (IP NAT, nuevo # puerto) en campo destino de cada datagrama entrante por correspondiente (IP fuente, # puerto) almacenado en tabla NAT

NAT: Network Address Translation

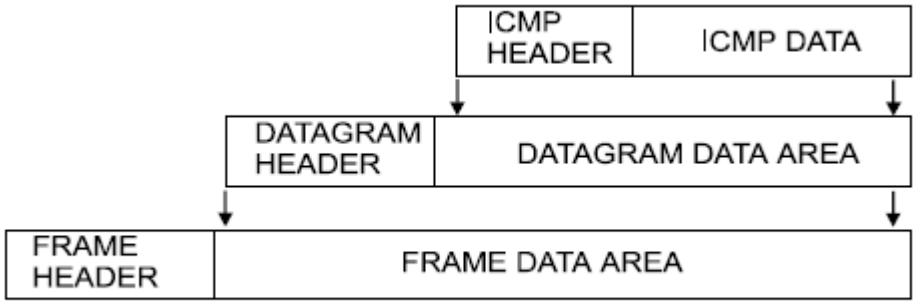


NAT: Network Address Translation

- 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

ICMP: Internet Control Message Protocol

- Protocolo IP no es fiable, los datagramas IP pueden perderse o llegar defectuosos a su destino.
- ICMP informa al origen si hubo algún error en la entrega del mensaje.
- Informa errores y mensajes de control.
- Informa sobre errores pero no toma decisiones sobre estos Mensaje ICMP
- Los mensajes ICMP se encapsulan como parte del área de datos del protocolo IP:



ICMP: Internet Control Message Protocol

- Usado por hosts & routers para comunicar información a nivel de la red
  - Reporte de errores: host, red, puerto o protocolo inalcanzable.
  - Solicitud/ respuesta de eco (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 cabecera y primeros 8 bytes del datagrama que causó el error

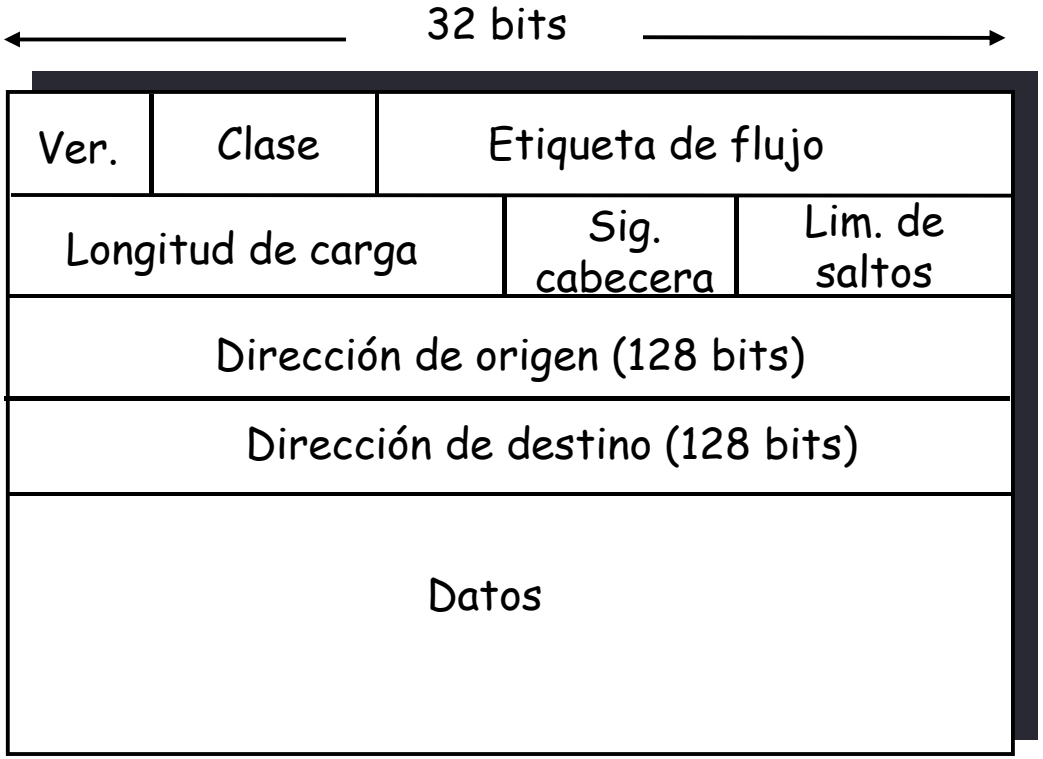
Tipo	Cód	Descripción
0	0	Respuesta de eco (ping)
3	0	Red destino inalcanzable
3	1	Host destino inalcanzable
3	2	Protocolo destino inalcanzable
3	3	Puerto de destino inalcanzable
3	6	Red de destino desconocido
3	7	Host de destino desconocido
4	0	Regulación del origen (control de congestión)
8	0	Solicitud de eco (ping)
9	0	Anuncio de router
10	0	Descubrimiento de router
11	0	TTL caducado
12	0	Cabecera IP errónea

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
  - Cambiar encabezado para facilitar QoS
- Formato de datagrama IPv6:
  - Capacidad ampliada de direccionamiento (de 32bits a 128 bits)
  - Encabezado de largo fijo de 40 bytes (se duplicó)
  - Fragmentación no es permitida
  - Permite direcciones **anycast**

Encabezado IPv6

- Clase: identifica prioridad entre datagramas en flujo
- Etiqueta de flujo: identifica un flujo de datagramas (20 bits)
- Longitud de carga útil: longitud en bytes de los datos.
- Siguiente cabecera: identifica protocolo de capa de transporte (igual de IPv4).
- Límite de saltos: ídem a TTL de IPv4.



Otros cambios de IPv4 a IPv6

- **Fragmentación y Reensamblado**: No se permiten en routers intermedios (sólo en origen y destino) Estas operaciones consumen tiempo, por lo que eliminándolas de los routers se acelera considerablemente el reenvío IP dentro de la red.
- **Checksum:** eliminada enteramente para reducir tiempo de procesamiento en cada router al ser redundante, ya está en capa de transporte y de enlace (Ethernet).
- **Opciones:** la cabecera estándar no incluye el campo de opciones. Este campo es una de las posibles "siguientes cabeceras" apuntadas (al igual que las cabeceras de TCP o UDP).
- **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

Vista lógica:

Vista física: