ait

Tema 04
curso 2018/19

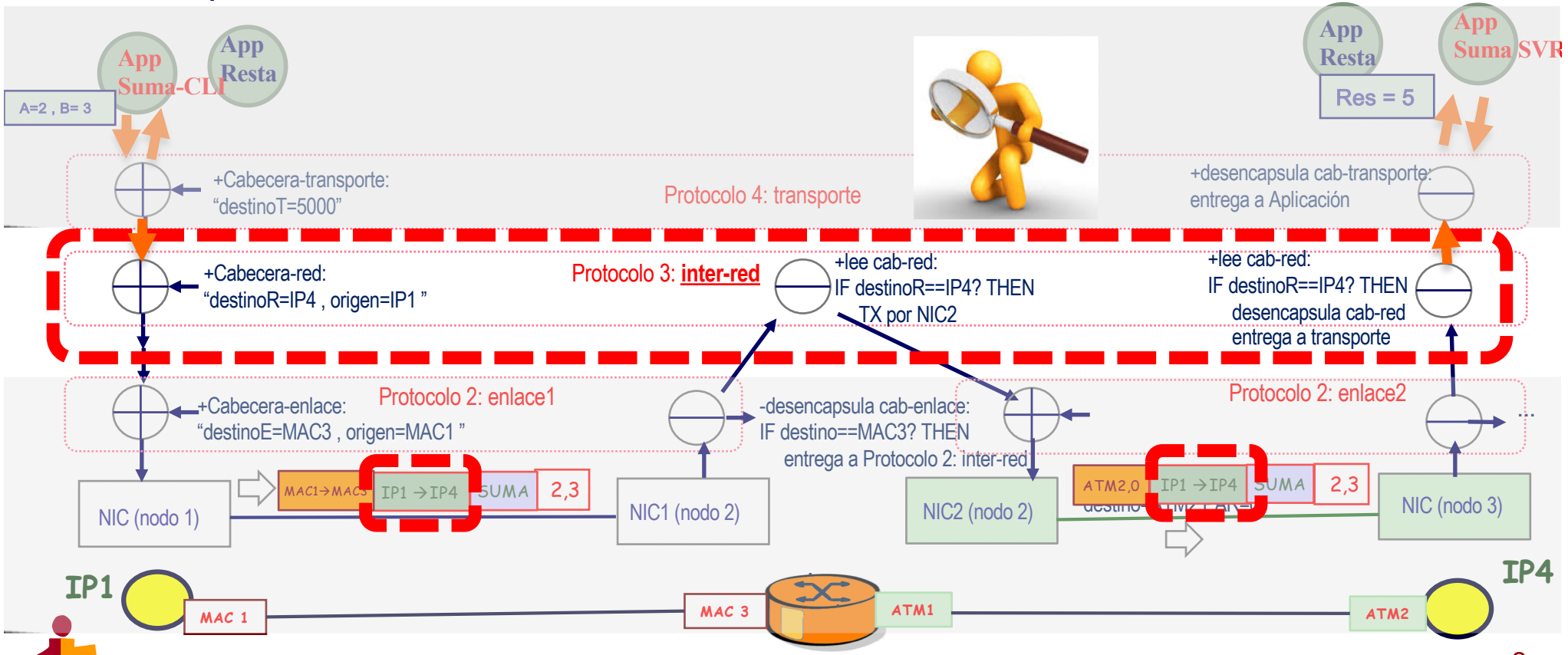
La Capa de Red: el protocolo IP

Antonio J. Estepa Alonso

Departamento de
Ingeniería Telemática

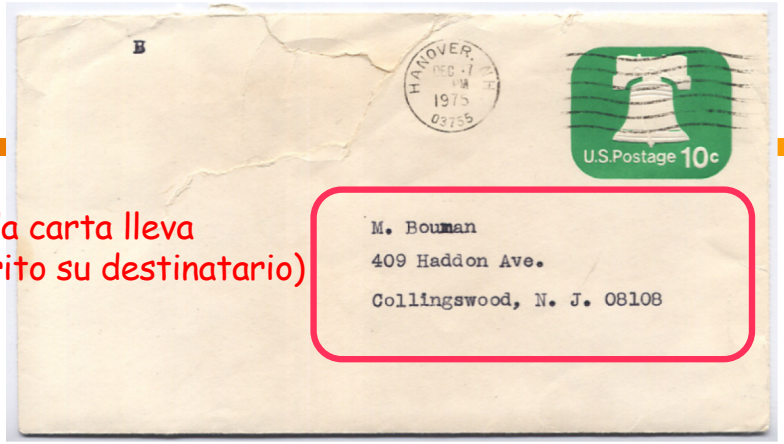
Tema 04: La capa de Red

4.1 Introducción a la capa de red: Servicios y protocolos
4.2 Estructura y funcionamiento básico de un Router
4.3 El protocolo IPv4.
4.4 Direccionamiento en IPv4
4.5 El reenvío en IP
4.6 El protocolo IPv6

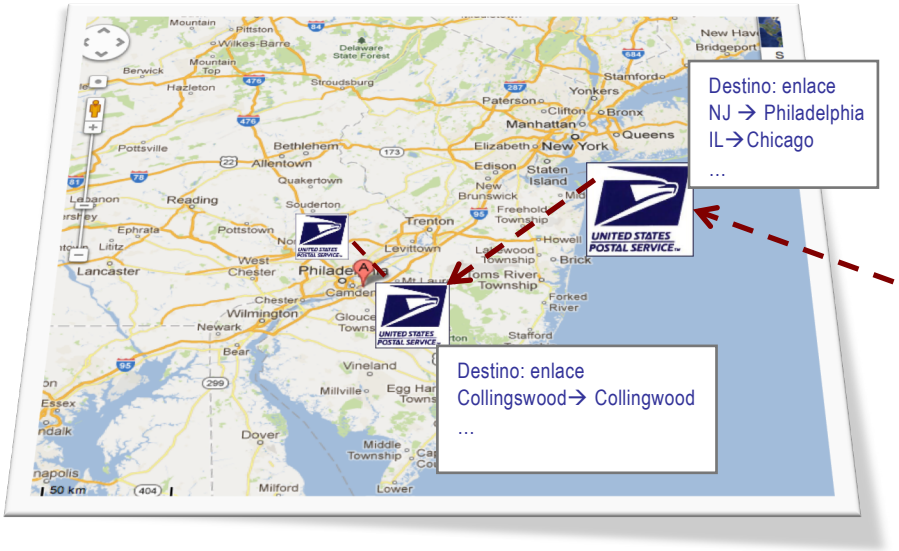


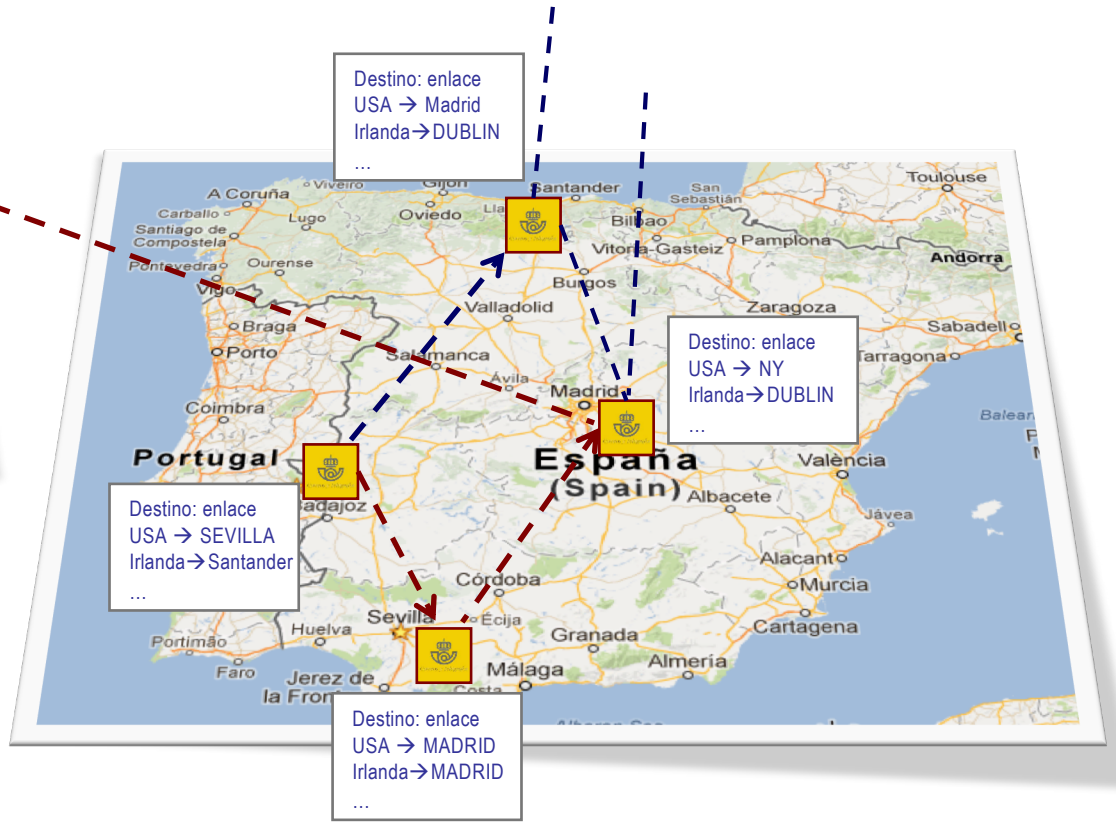
… Funcionamiento de correos

- Quiero enviar una carta:
  - Destinatario:
  - Remitente: yo (Badajoz)



(cada carta lleva escrito su destinatario)





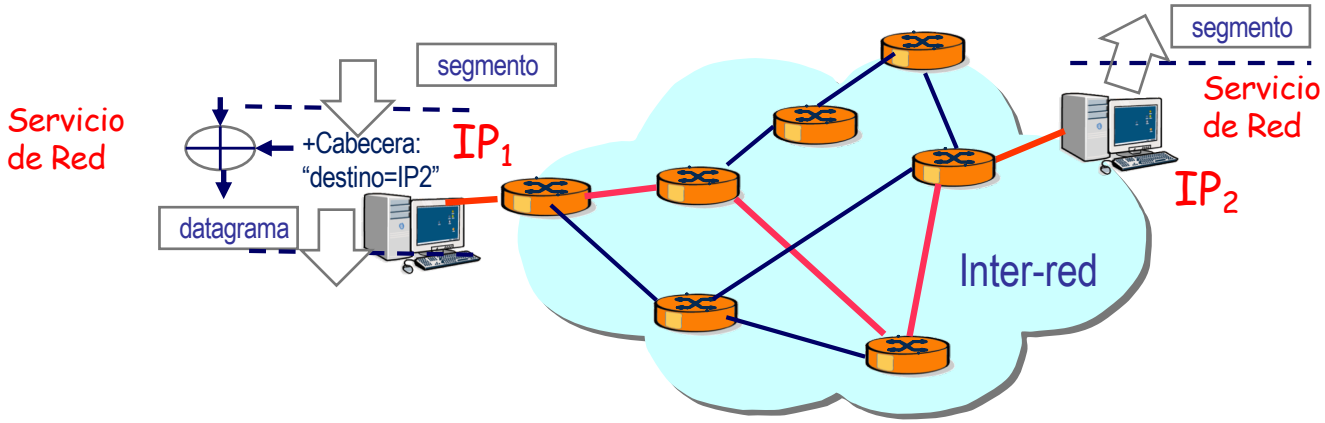
Cada "nodo" reenvía la carta según su **tabla local de reenvío**

Si todas las tablas de reenvío están bien hechas, la carta llega a su destino

Capa de Red : servicio y tareas principales

- Servicio: (según OSI, orientado o no a conexión)
  - Misión “Hacer llegar la información suministrada por la capa superior hasta su destino final, atravesando para ello los sistemas intermedios que fueran necesario, y eligiendo la ruta adecuada”
- Tareas principales: (según OSI)
  - Direccionamiento
  - Encaminamiento
  - Reenvío en cada nodo
  - [control congestión]

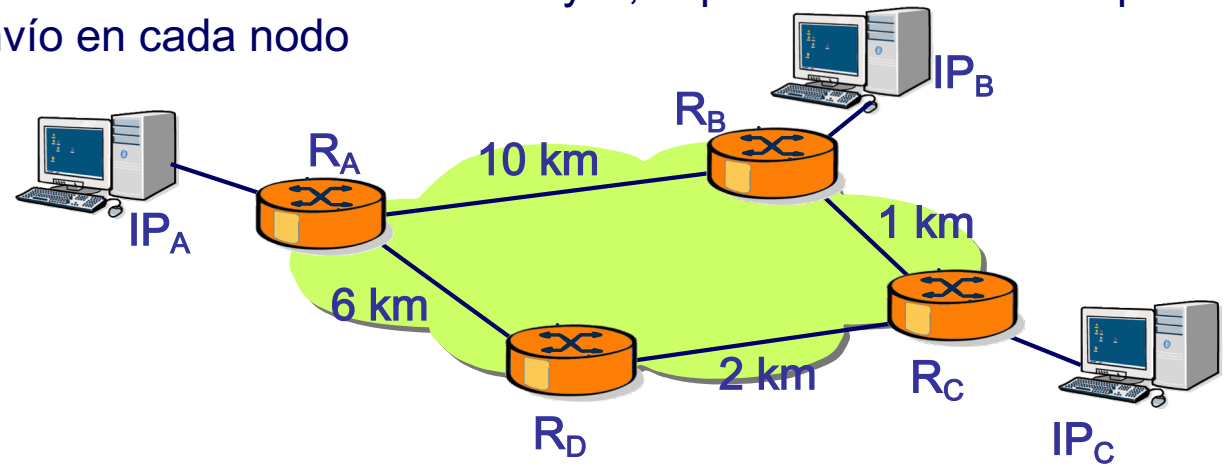
Modelo de Internet
- Red = inter-red
- Sistemas Intermedios = routers (reenvían datagramas entre redes)
- Servicio NO orientado a conexión.→ servicio datagrama



Conceptos previos …. Encaminamiento y reenvío

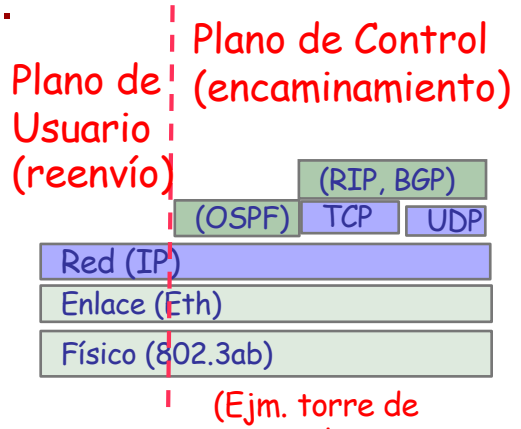
- **Encaminamiento (routing)**: determinación sistemática del **mejor** camino entre un origen y un destino (visión global de la red)
  - Necesita un criterio para valorar el mejor camino (p.ej. el más corto, más rápido..)
  - Es necesario realizar esta tarea de "control" antes de poder reenviar.
- **Reenvío (forwarding)**: determinación, **en cada nodo,** del siguiente salto del paquete (enlace de salida) (acción local)
  - Usa una tabla de reenvío almacenada localmente en cada nodo y la información que lleva cada paquete en su cabecera de red (local en cada nodo)
  - Un equipo re-envía los paquetes creados en los hosts (servicio al "usuario")

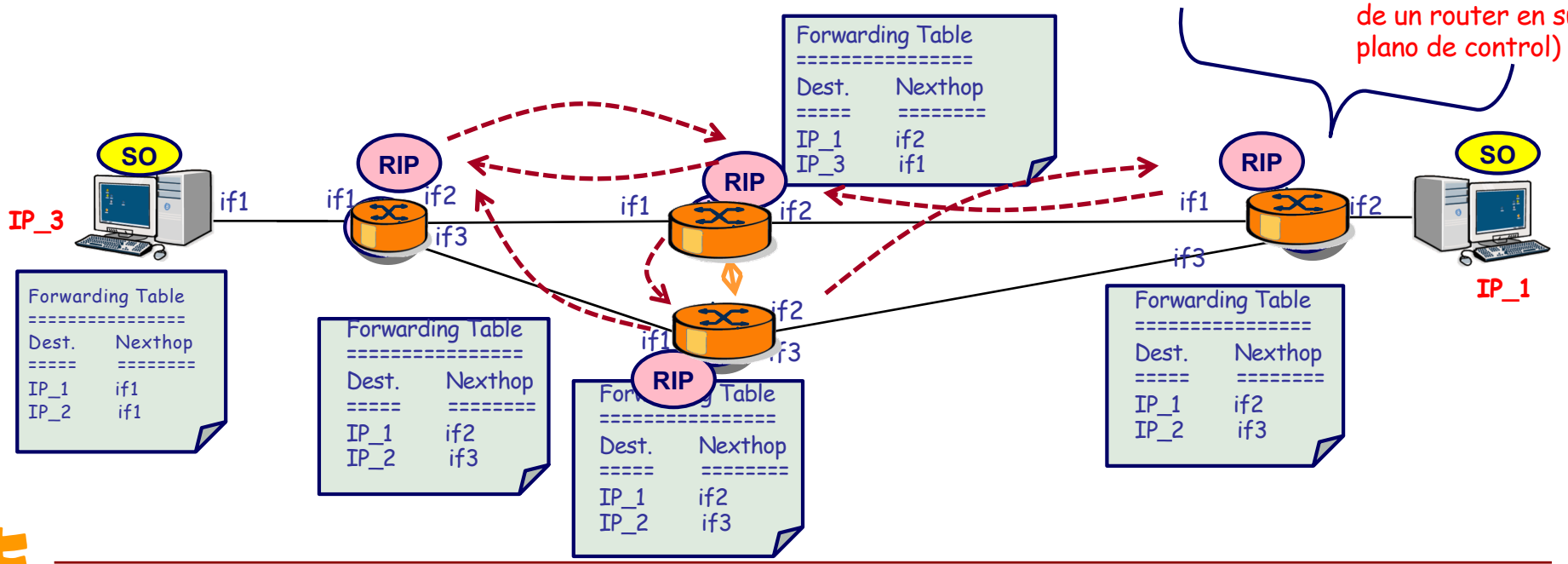
- Ejemplo: diseñe un camino entre A y B,C que sea el mas corto posible e indique la tabla de reenvío en cada nodo



Protocolos de Encaminamiento

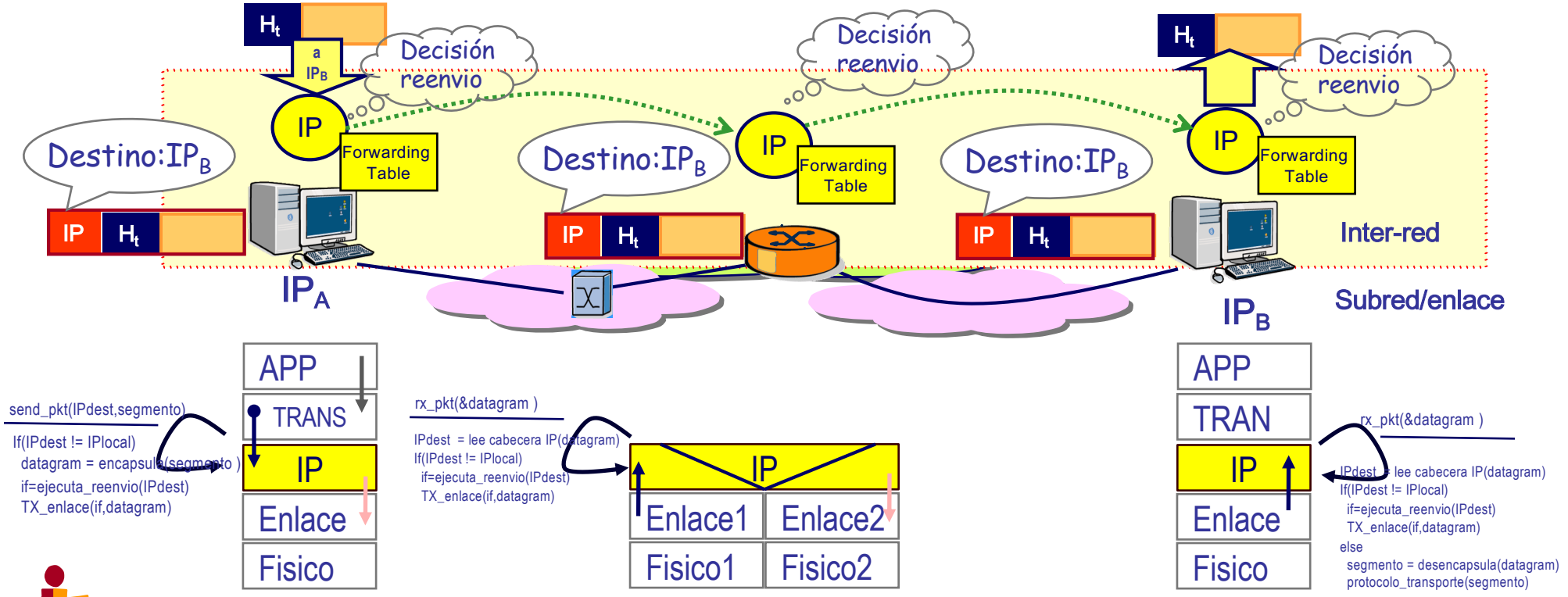
- Permiten automatizar la función de Encaminamiento:
  - "Aplicación" distribuida que se ejecuta entre los routers.
    - Ejemplos (varios protocolos posibles):
      - OSPF, RIP (dentro de un Sistema Autónomo (S.A.),
      - BGP (entre SS.AA)
    - **Como resultado**, cada nodo autoconfigura su tabla local de reenvío.
  - Permite cambios dinámicos de rutas





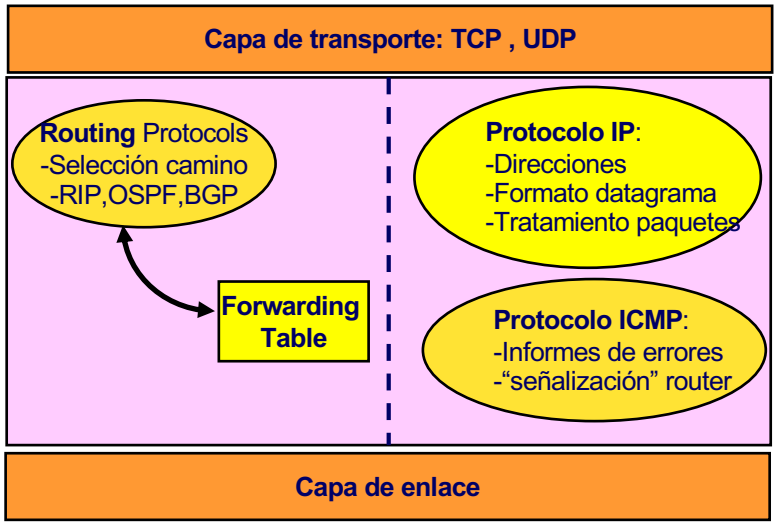
Reenvío (plano de usuario)

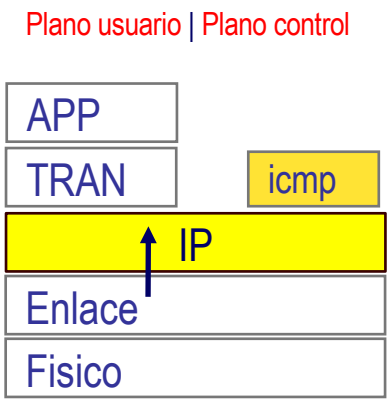
- **IP** (Internet Protocol) es un protocolo de reenvío.
  1. Al llegar un nuevo datagrama, lee la dirección destino de la cabecera IP
  2. Toma la decisión de reenvío por una de las interfaces (i.e. redes) **usando su tabla local de reenvío**.
  3. Solicita el envío del datagrama por el nuevo enlace

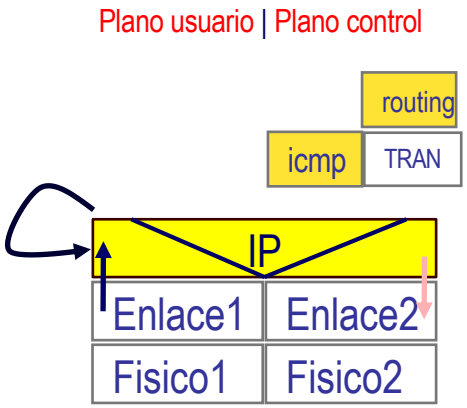


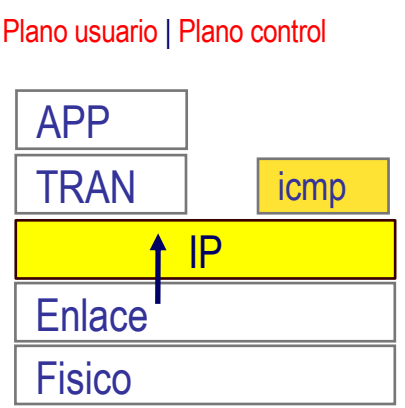
Resumen de la Introducción a la capa de red en Internet

- Misión principal: hacer llegar paquetes a su destino final
- Componentes: protocolos y tabla reenv.
- Funciones básicas:
  - Reenvío (forwarding)
  - Encaminamiento (routing)
- Implementada en
  - Sistemas finales (hosts)
  - Routers







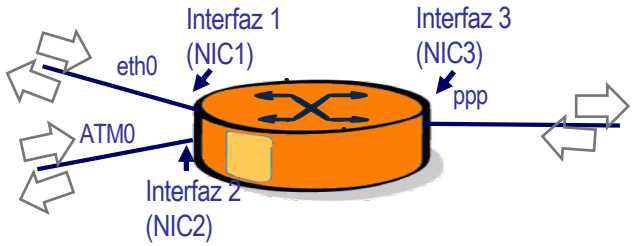


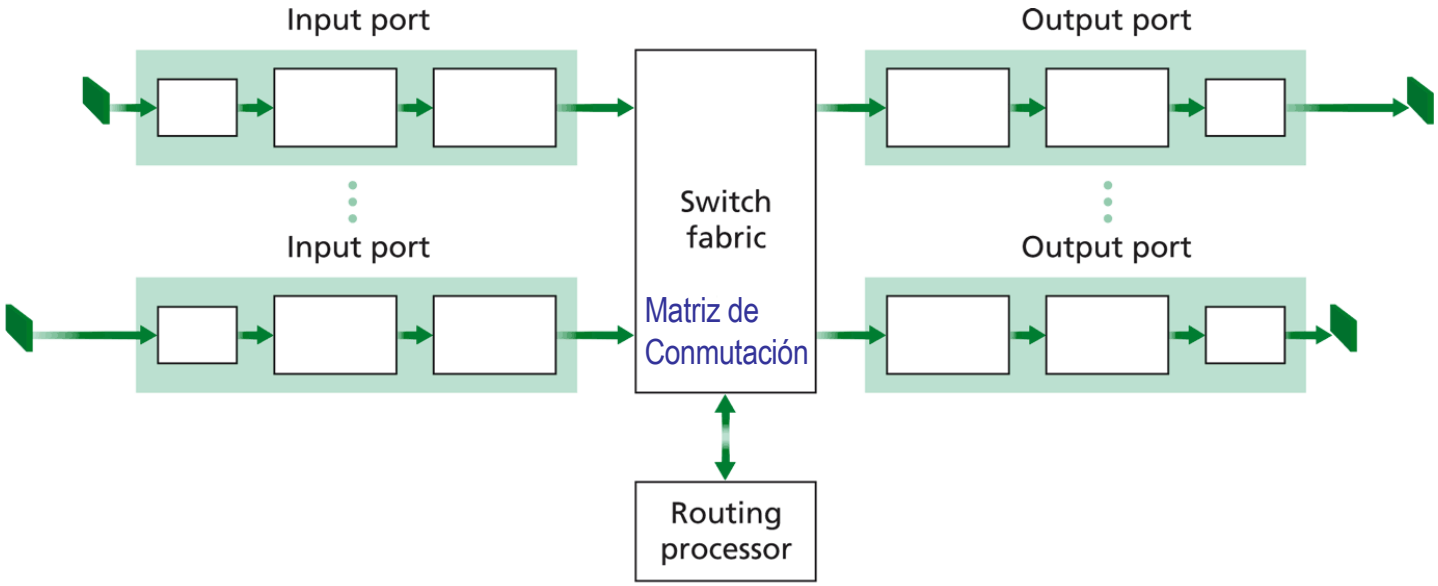
Tema 04: La capa de Red

Índice

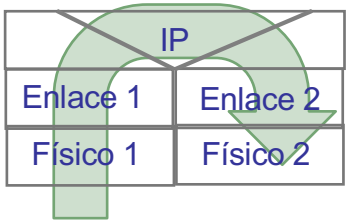
Descripción básica de un Router

- Esquema Simplificado del plano de datos (reenvío)
  - Plano de control encargado del encaminamiento y otros servicios
- Partes
  - Puertos de entrada
  - Switching Fabric
  - Puertos de Salida





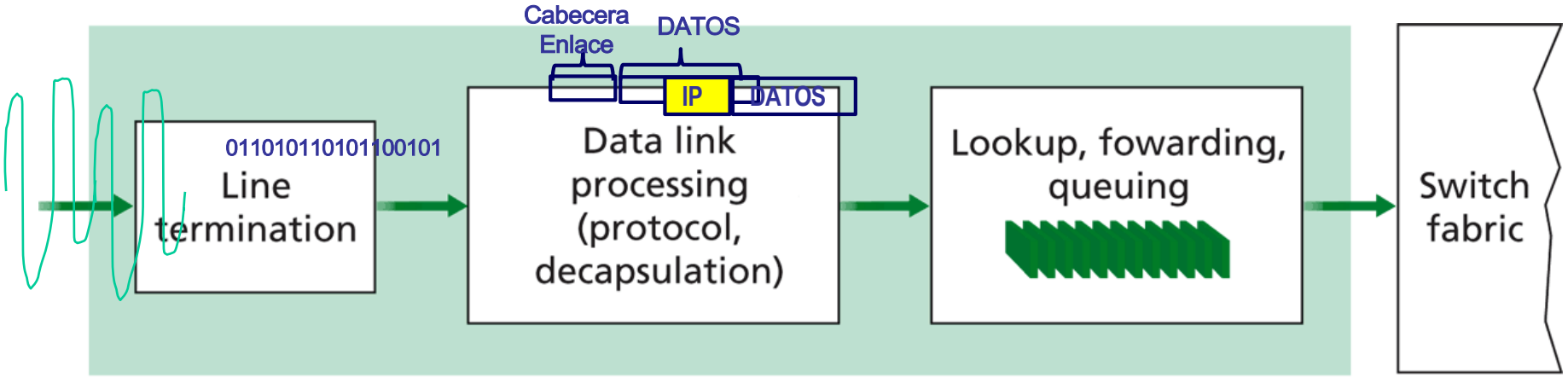
Modelo de Capas
(torre de protocolos
del plano de usuario)

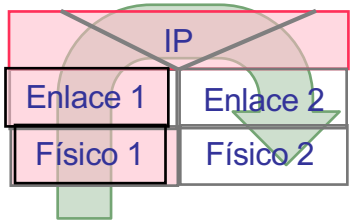


hitecture

Puertos de Entrada

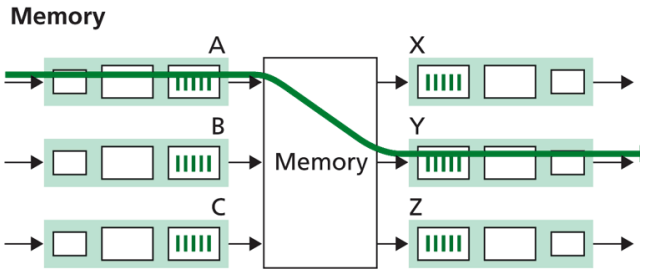
- Funciones principales
  - Terminación de línea (nivel 1 OSI)
  - Procesado del protocolo del enlace de datos (nivel 2 OSI)
  - Decisión sobre el puerto de salida más adecuado
    - Búsqueda de la mayor coincidencia en la tabla de reenvío lo más rápido posible (Content Addressable Memories CAM)… mientras menor sea el espacio de direcciones, mejor ..

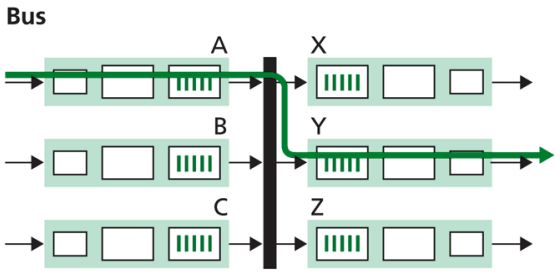


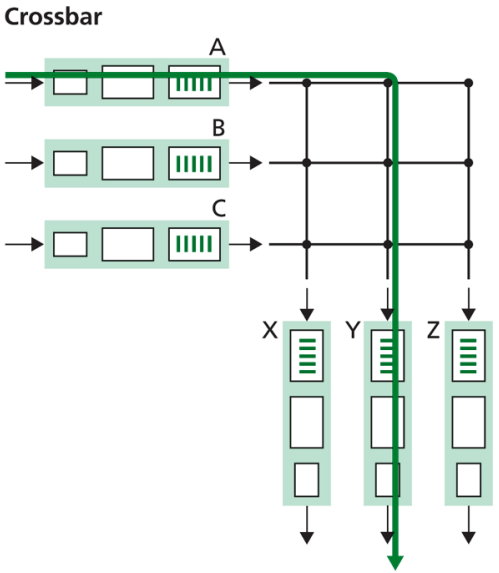


Switching Fabric (matriz de conmutación)

- Elemento de conmutación
- Las prestaciones se miden en caudal de la conmutación sin bloqueo
- Vía:
  - Memoria
  - Bus
  - Red de interconexión



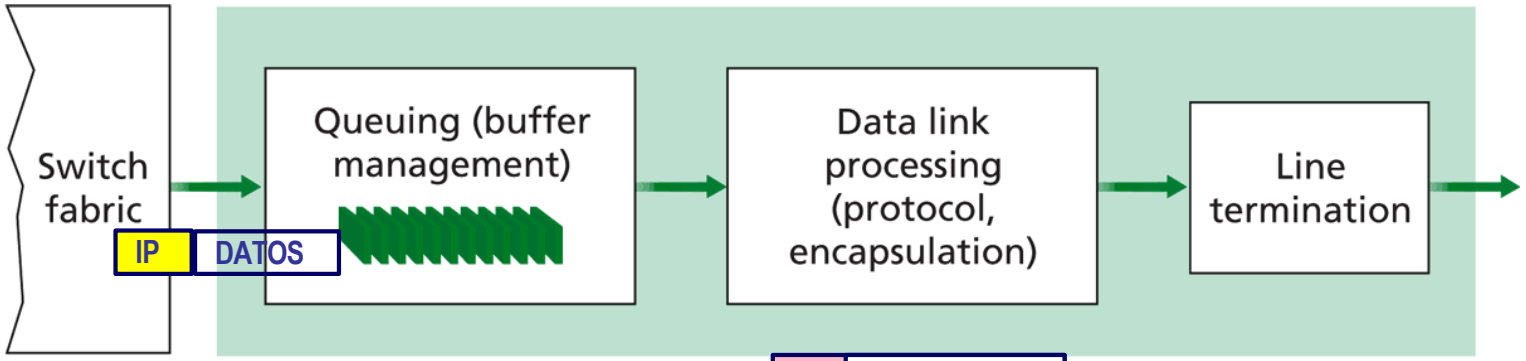


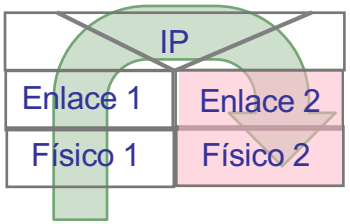


https://www.cse.wustl.edu/~jain/cis788-99/ftp/terabit_routing/index.html

Puertos de Salida

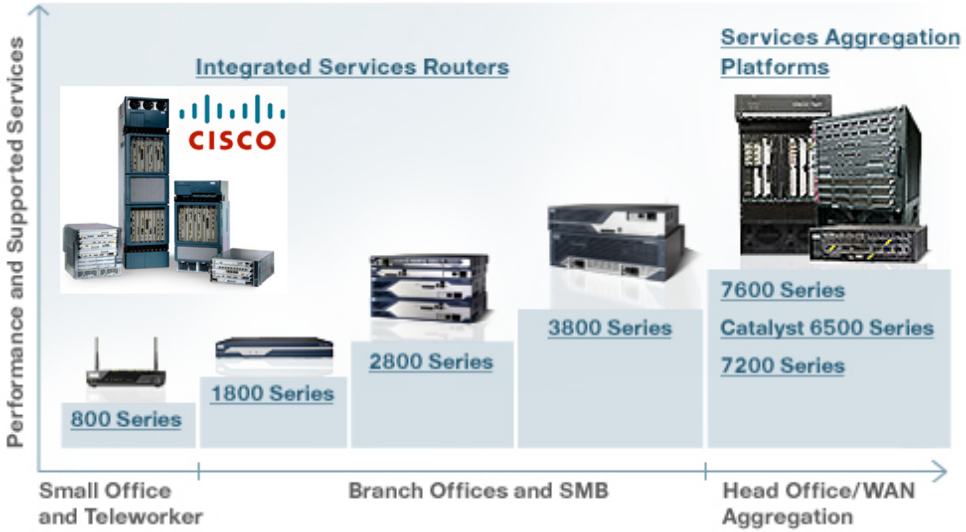
- Elementos parecidos a los puertos de entrada
  - Posible espera en cola … ¿recuerdas el tema 01?
    - Gestión de la cola: disciplinas de colas
  - Encapsulación en el nuevo protocolo de enlace
  - Transmisión física



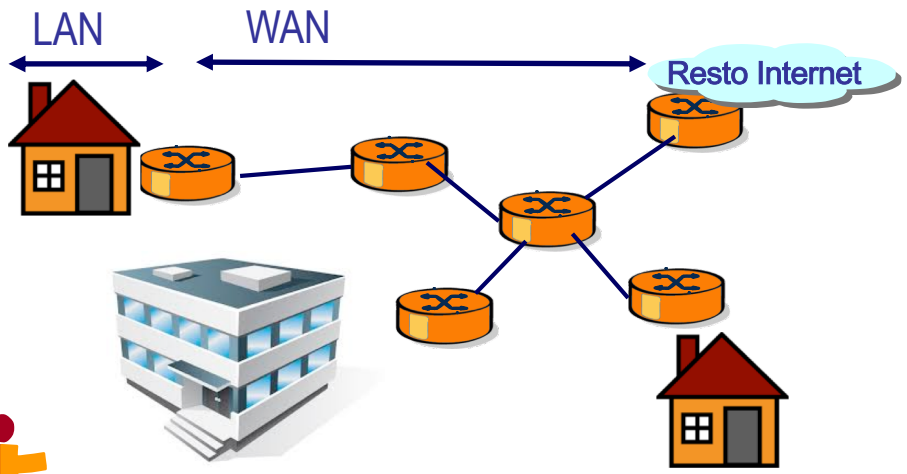


Modelos comerciales

- Diferentes prestaciones en función del uso



NICs que soportan
Puertos de Usuario (conmutados)
Velocidad de conmutación
Memoria interna
Escalabilidad
Robusted
Protocolos implementados etc…

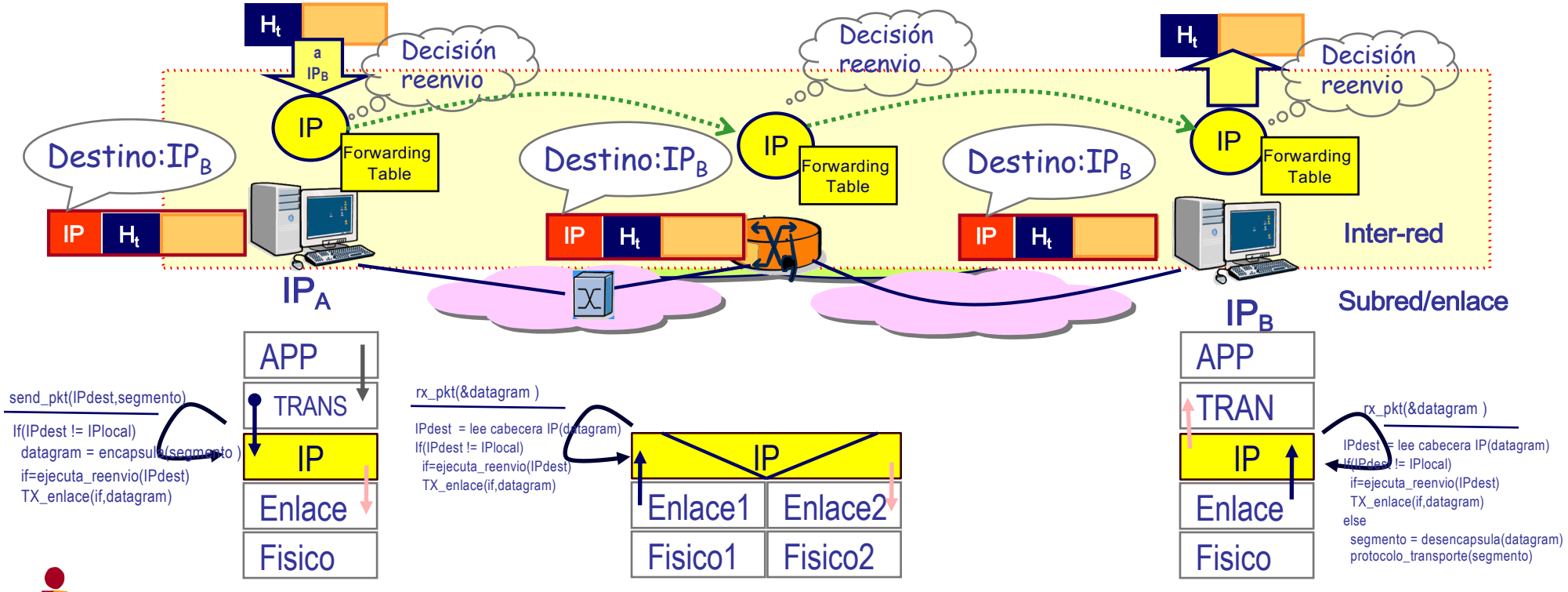


Tema 04: La capa de Red

Índice

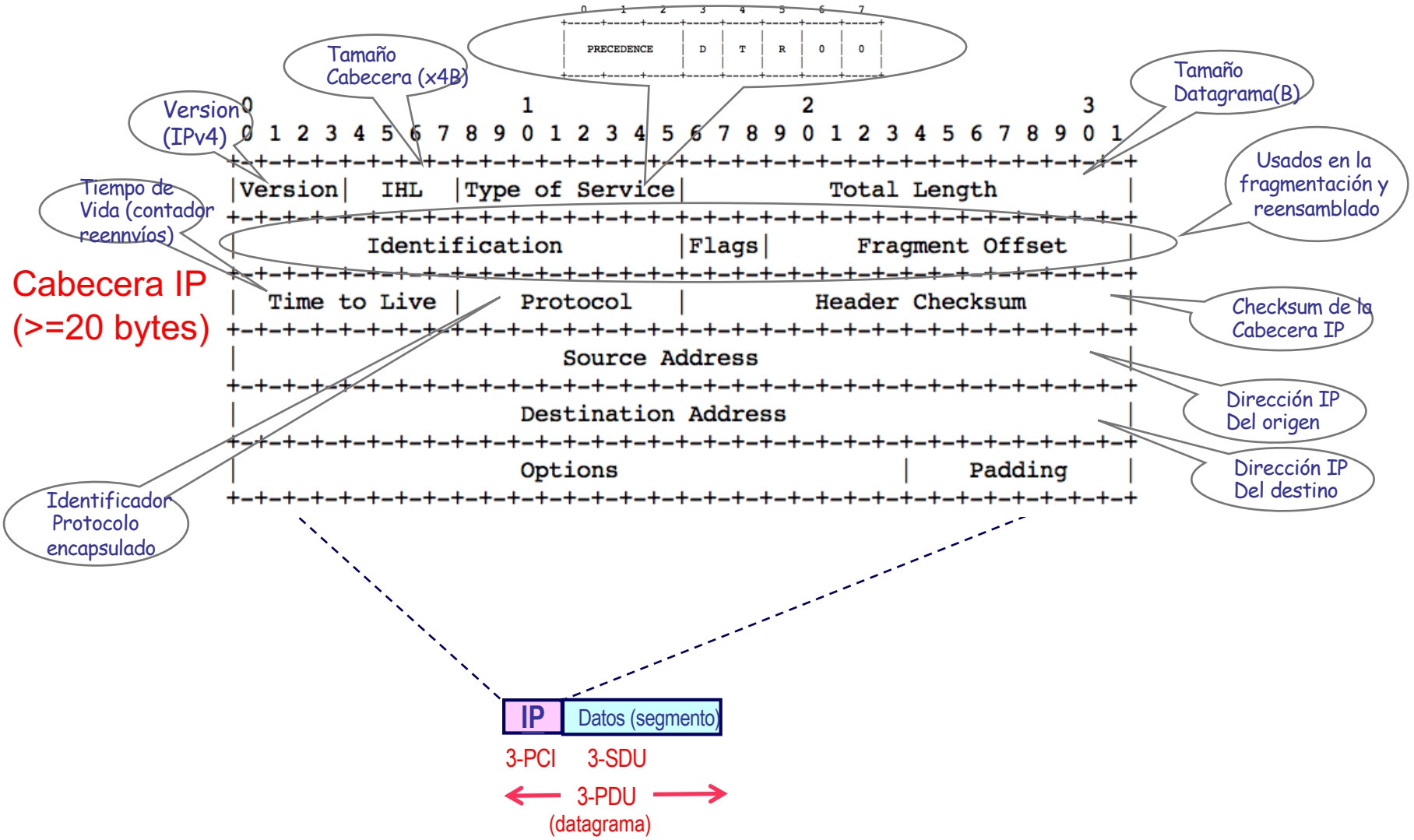
El Protocolo de Internet: IP (Internet Protocol)

- Usado en Internet para el reenvío de los datagramas
  - Versión actual: IPv4 (RFC 791) … en transición a IPv6(RFC 2460)
- Ofrece un servicio de red NO orientado a conexión (tipo datagrama).
- El servicio no ofrece garantías de reparto (best-effort delivering).
  - Los datagramas pueden perderse, duplicarse o desordenarse



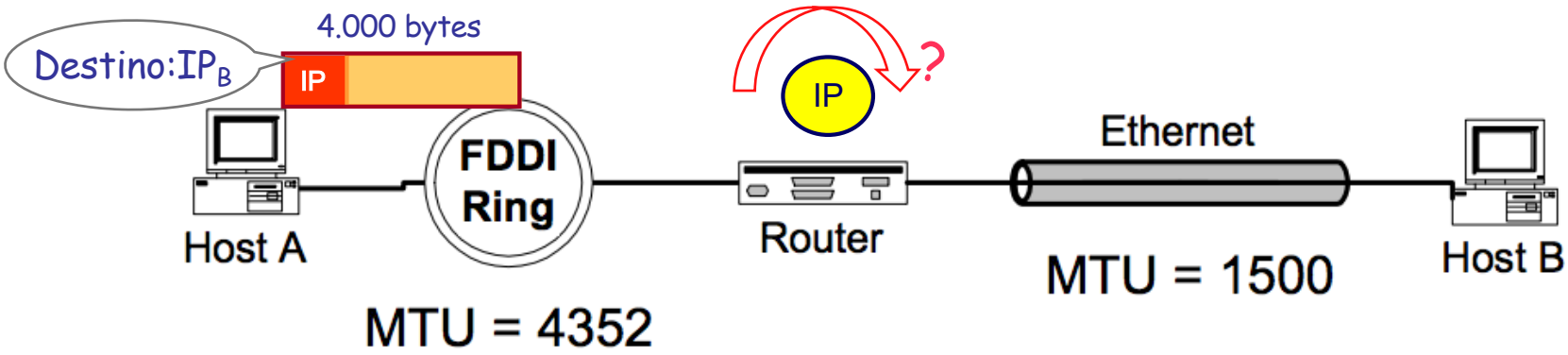
El protocolo IP: cabecera

- Estructura del datagrama IPv4 (versión 4, RFC 791, 1981)



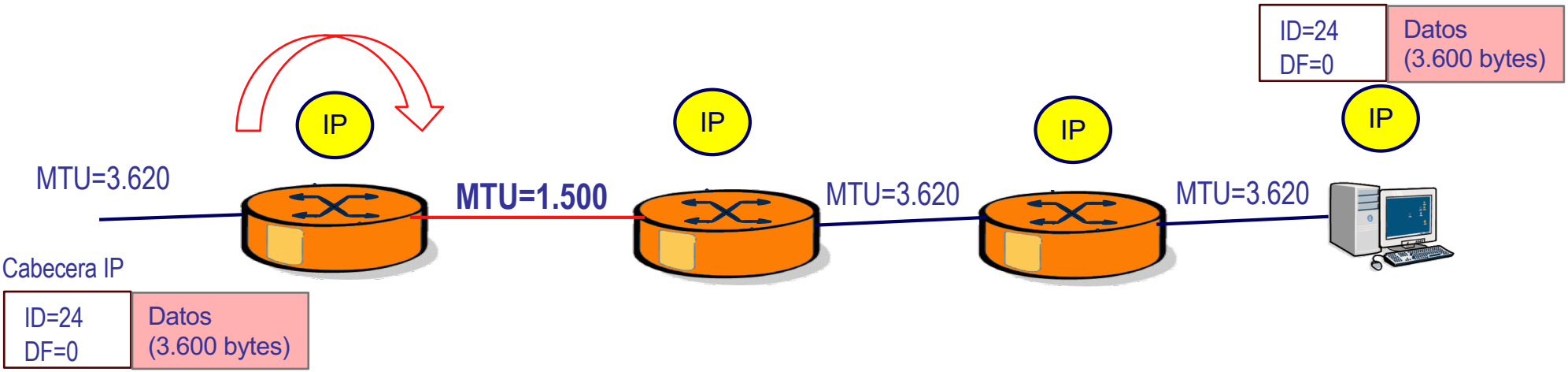
Fragmentación y reensamblado

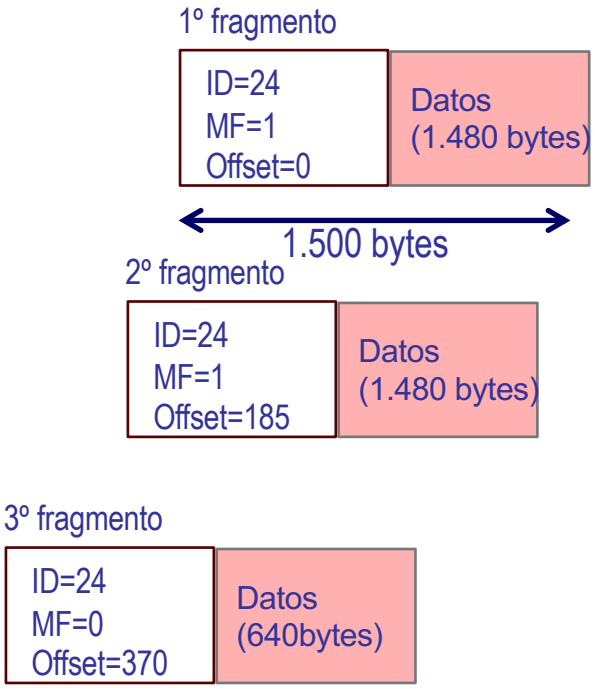
- Realizada por IP si al reenviar por un enlace si el tamaño del datagrama excede la MTU del enlace por donde va a ser reenviado.



- Fragmentación (si el bit DF (don't fragment) vale FALSE)
  - Se crean varios datagramas de menor tamaño (fragmentos)que sustituyen al original
  - Proceso:
    - El valor del campo identification (ID) del datagrama original se copia en la cabecera IP de todos los fragmentos.
    - El bit MF (more fragments) vale 0 en el último fragmento y 1 en el resto
    - El campo offset de cada fragmento indica el desplazamiento relativo de los datos de cada segmento frente a los datos originales (en múltiplos de 8B)

Ejemplo de fragmentación





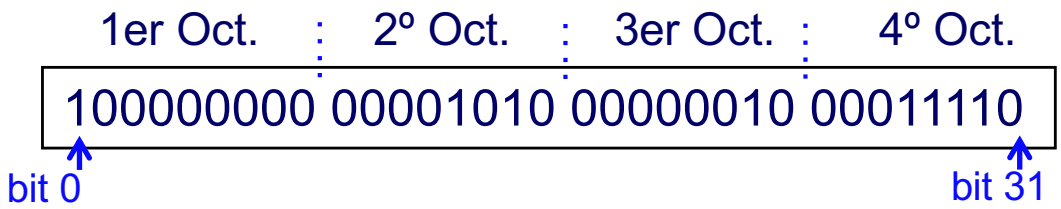
- Cada fragmento IP es tratado como un paquete IP independiente.
- Se re-ensamblan en el destino
  - Si se pierde un fragmento se descartan todos
- Un fragmento puede a su vez ser fragmentado

Tema 04: La capa de Red

Índice

El protocolo IP: direccionamiento

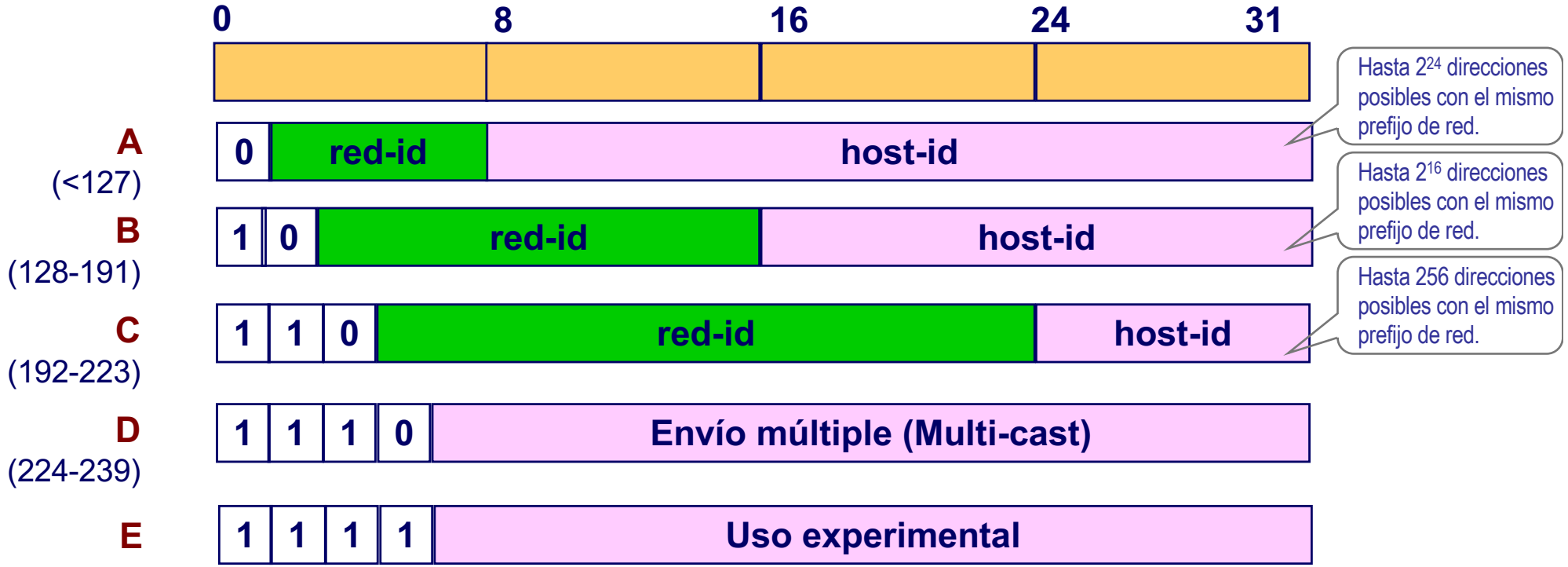
- Cada sistema tiene asignado una dirección de 32 bits
- Jerárquicas no geográficas
- Asignadas por una autoridad central: InterNIC
  - Centros Regionales
- Direccionamiento
  - Una dirección IP **identifica a un equipo conectado a una red**
    - Identificación única en la red
  - Direcciones IP v4
    - 4 bytes u octetos.
    - Notación decimal punto



Notación Decimal punto → ejemplo 128.10.2.30

Direccionamiento: formato y clases originales

- Dirección IP: identifica a una red (red-id) y un equipo en ella (host-id).
  - Un equipo que pertenece a dos redes debe tener 2 direcciones diferentes
- Redes de diferente tamaño
  - Diferentes clases de dirección en función del primer octeto (sol. original)



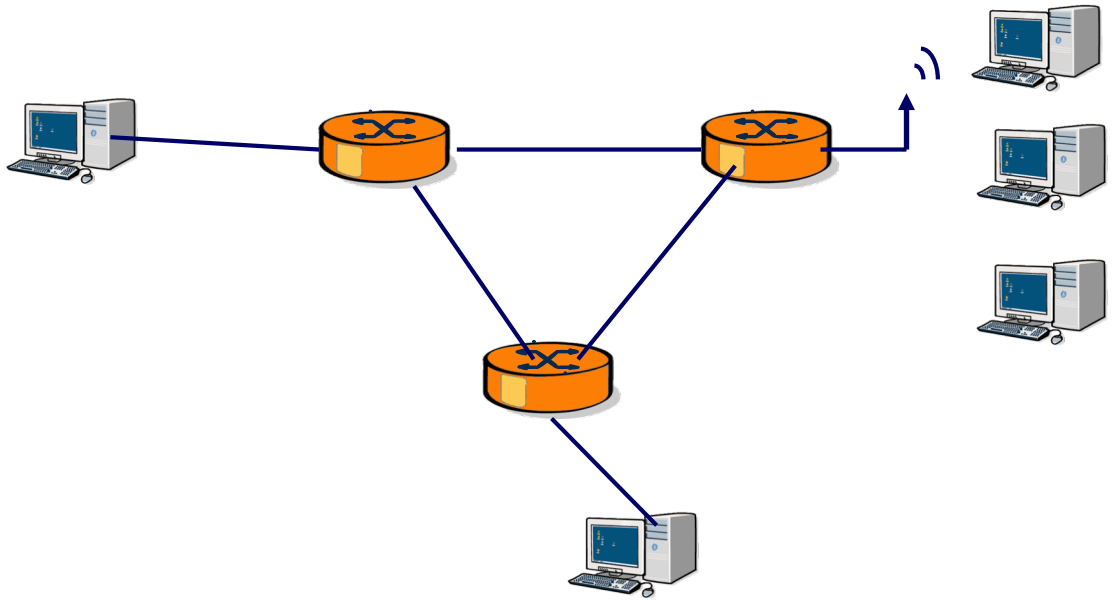
Direcciones especiales y direcciones de uso privado

- Algunas direcciones *especiales*. https://tools.ietf.org/html/rfc5735
  - Difusión local (a todos los equipos de esta red). bits (host-id) a '1'
    - » Ejemplos: 193.123.143.255, 190.31.255.255, 34.255.255.255
  - Difusión total (a todos los equipos de todas las redes): 255.255.255.255
  - Bucle local (identifica al propio equipo):127.0.0.1
  - Direcciones de red (identifican a una red): bits (host-id) a '0'
    - » Ejemplos: 193.123.12.0 , 190.31.0.0 , 34.0.0.0
  - Dirección desconocida: 0.0.0.0
    - (también: dirección inválida y cualquier equipo de "esta" red, RFC5735)
    - (también: cualquier direccíon IP de este equipo)

- Rango de direcciones privadas (RFC 1918). Prohibido su uso en Internet
  - Clase A: 10.0.0.0 - 10.255.255.255. 1 red de clase A
  - Clase B: 172.16.0.0 - 172.31.255.255. 16 redes de clase B
  - Clase C: 192.168.0.0 - 192.168.255.255. 256 redes de clase C

Ejercicio: (direccionamiento con clases)

- Asigne direcciones de clase C a todos los hosts y routers de la red.
- Identifique las direcciones especiales de red y difusión local en cada red



Solución

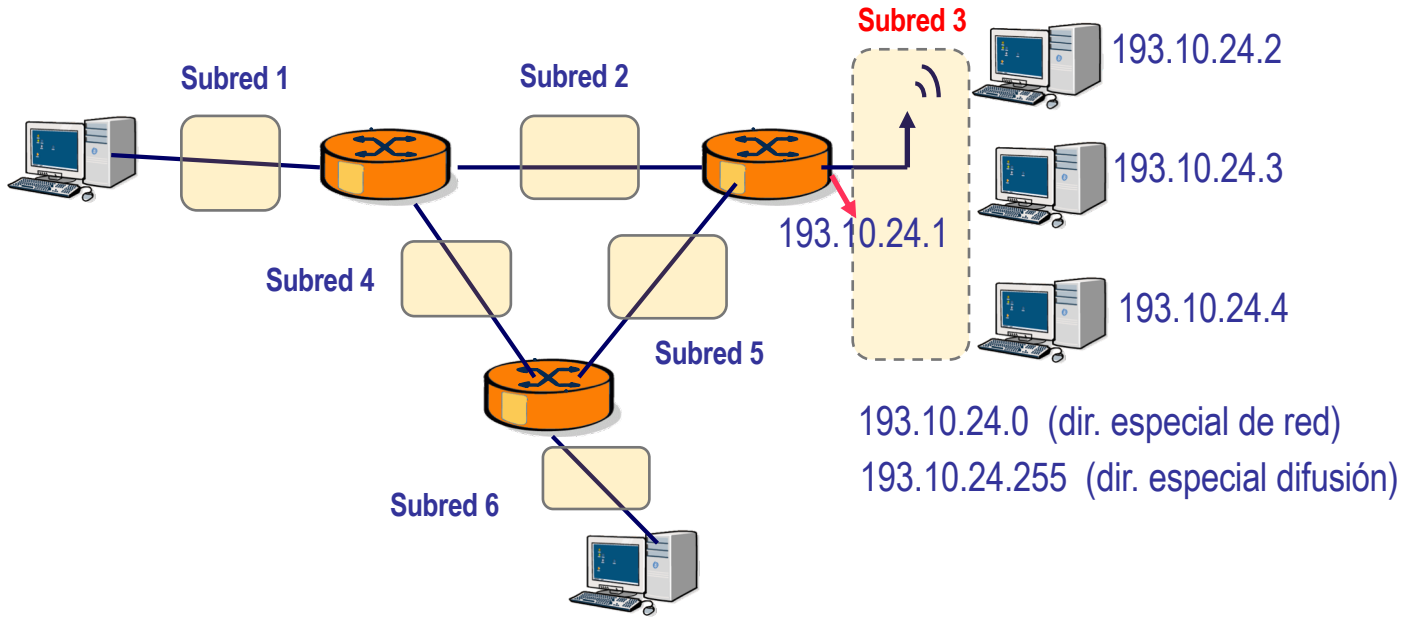
1) identificar las sub-redes (o redes que componen la internet)

2) para cada sub-red,

asignar una dirección especial de red y otra de difusión.

3) asignar direcciones a los equipos dentro del rango válido de cada subred

los routers deben tener una dirección válida por cada puerto



Problema: Las direcciones IPv4 libres se agotan !!

- Problemas con las direcciones IPv4: **agotamiento de direcciones**
  - División jerárquica estricta
    - Clase A (126 redes de 16777214 *host-id*),
    - Clase B(65536 *host-id*),
    - Clase C (255 *host-id*)
  - Ejemplo: una red con 260 equipos necesita clase B: desperdicia el 99%

https://en.wikipedia.org/wiki/IPv4_address_exhaustion

- Soluciones:
  - Temporal: Direccionamiento sin clases **CIDR**
    - RFC 1519, (Sept.1993)
    - Identificadores de red de tamaño variable
      - Mayor flexibilidad para separar el *host-id* y el *net-id*
  - Temporal: direccionamiento privado (NAT)
  - **Definitiva: IPv6**
    - Mayor rango de direcciones (16 octetos (128b), hasta … direcciones)

Direccionamiento Inter-Dominios sin Clases, RFC 1519

- Usado actualmente en Internet
- Direccionamiento CIDR (Class-less Inter-Domain Routing)
  - La frontera entre la red y el host la define una **máscara**

Dirección IP	134.23.133.29	**10000110.00010111.10000011.00011101**
Máscara	255.255.255.0	**11111111.11111111.11111111.00000000** *tamaño del prejifo de red (24b)* *id. de host*

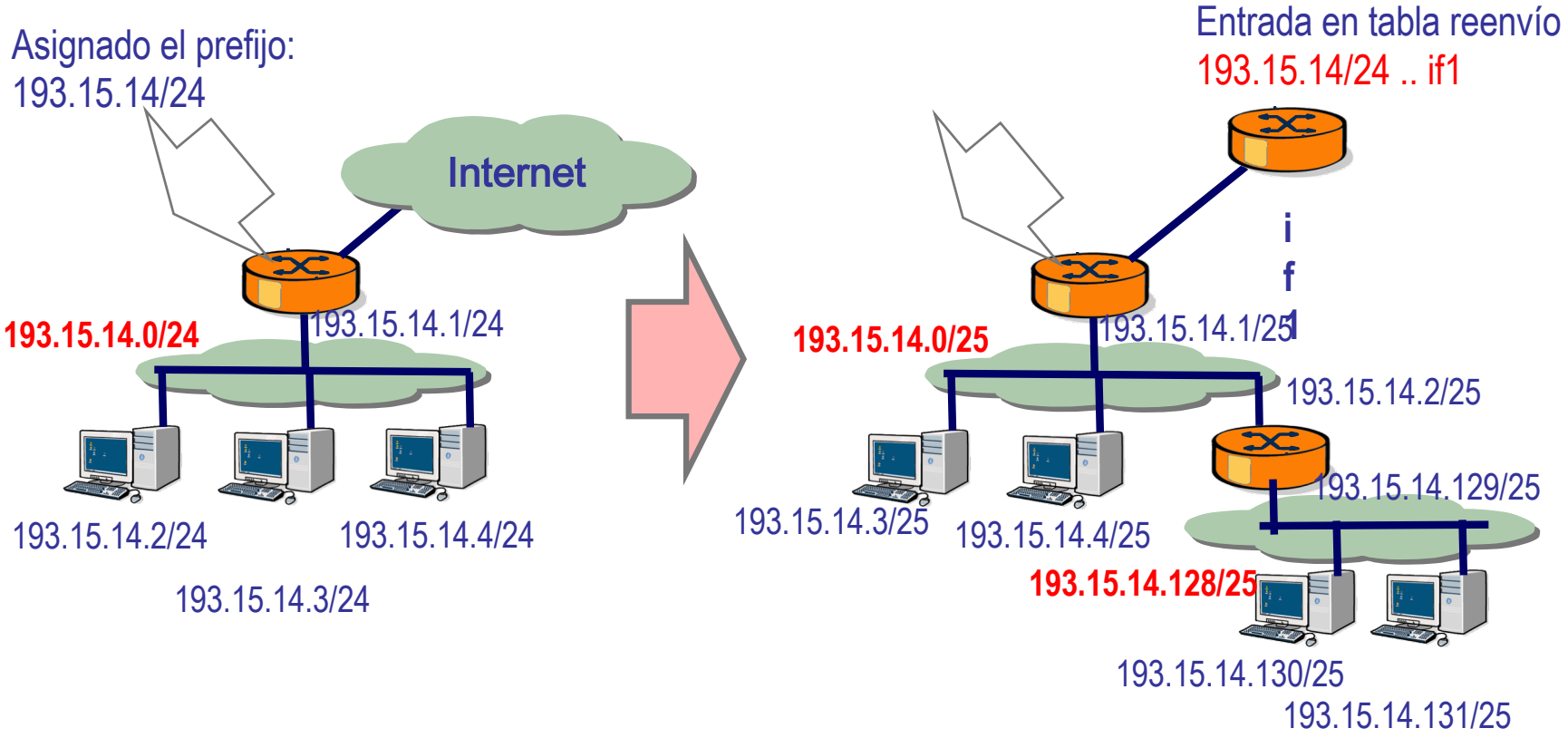
  - Extracción de identificador de red: operación AND
  - **Notación para escribir direcciones CIRD**
    - Dirección IP y máscara: 193.123.23.123, 255.255.255.0
    - Dirección IP / número de unos de la máscara: 193.123.23.123/24

- Ejemplo: examinar un ordenador del CdC o de la clase.

Por compatibilidad con el direccionamiento original
Máscaras por defecto
Direcciones clase A: 255.0.0.0 (/8)
Direcciones clase B: 255.255.0.0 (/16)
Direcciones clase C: 255.255.255.0 (/24)

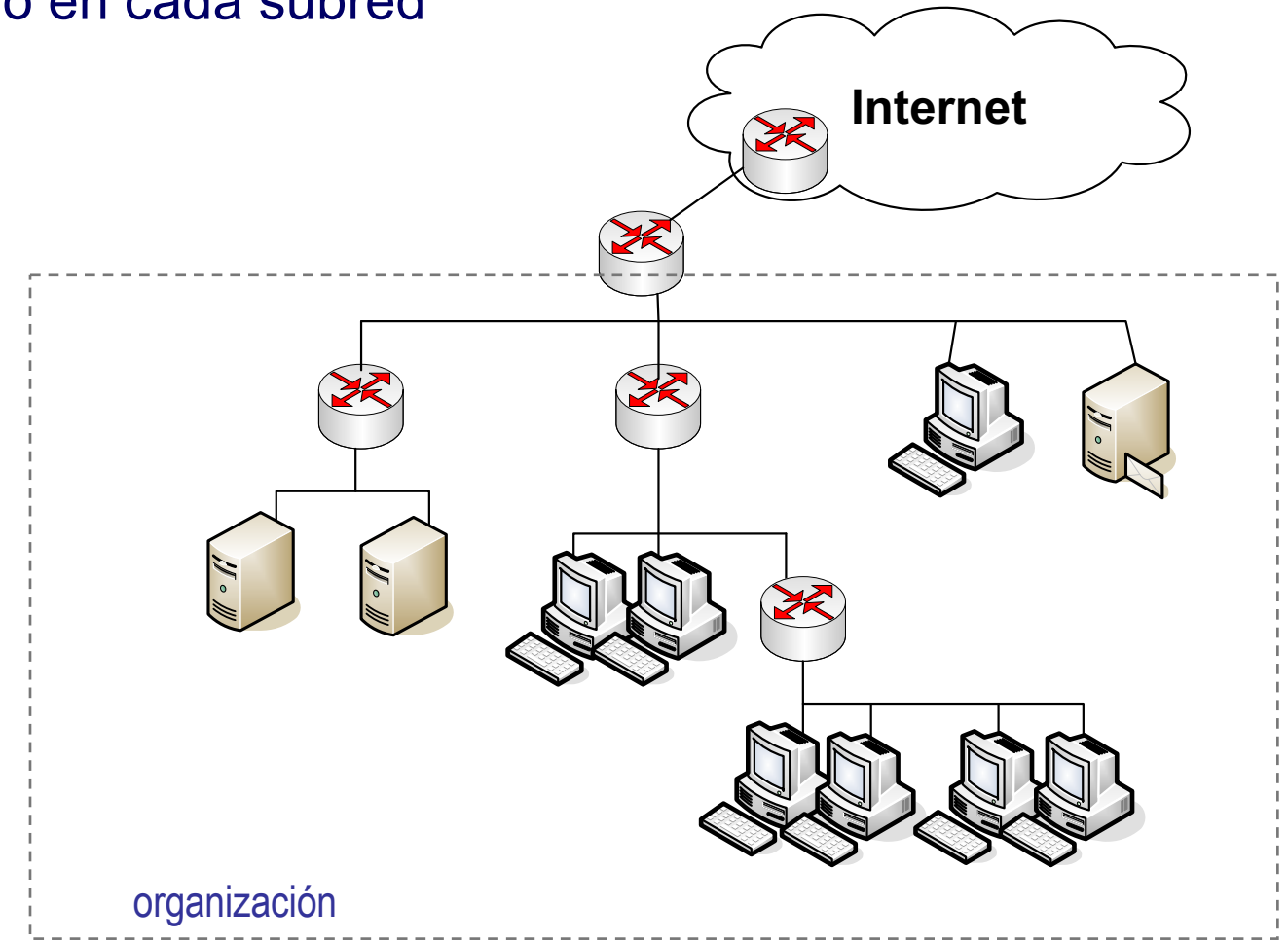
Utilidad del direccionamiento CIRD

- Aprovecha mejor las direcciones asignadas (subnetting)
- Permite hacer tablas de reenvío con menos filas (agregamiento)
- Ejm. Una organización que tenía asignadas las direcciones públicas 193.15.14.0/24, amplia su red haciendo un nuevo segmento (subred) pero no necesita nuevos prefijos de red.



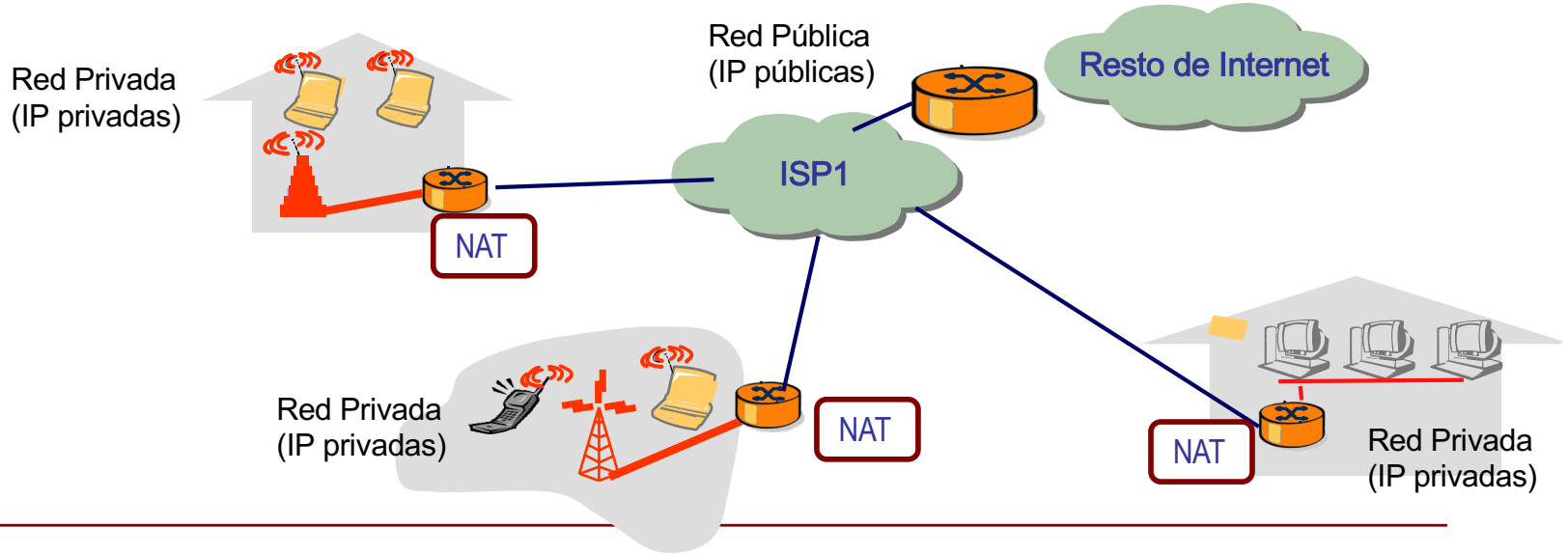
Ejercicio. (direccionamiento CIDR)

- Asigne direcciones IP en los equipos de la organización si dispone de la dirección 123.12.4.0/24 e indique el rango de direcciones válido en cada subred



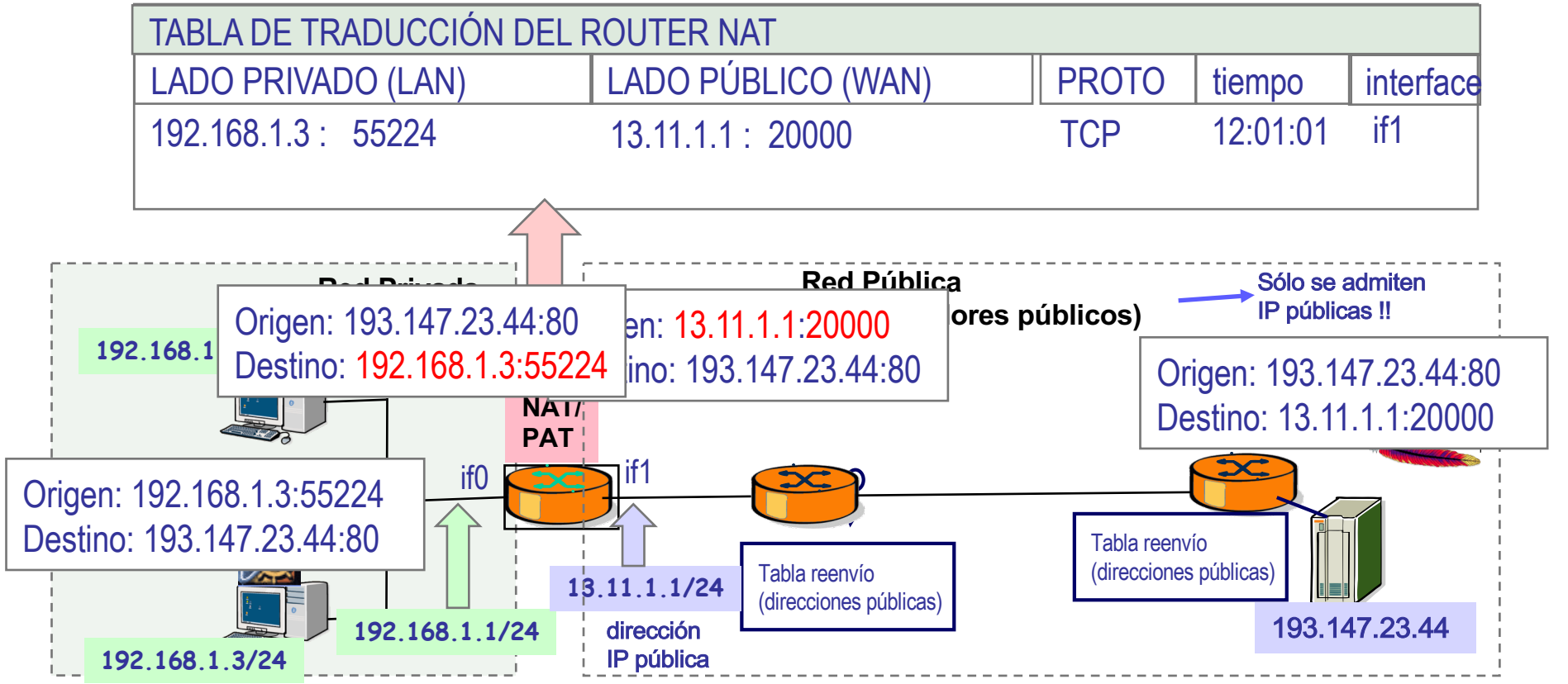
Network Address Translation: NAT

- El objetivo fundamental de NAT (RFC 2663, RFC 3022) es aliviar la escasez de direcciones IPv4 permitiendo el uso de direcciones IP privadas (RFC 1918) en los hosts conectados a Internet
  - 192.168.x.x (192.168/16)
  - 172.16.x.x – 172.31.x.x, (172.16/12)
  - 10.x.x.x (10/8)
  - Pueden repetirse dentro de distintas redes de acceso
- Idea: el router que ejecuta NAT esta conectado a la red privada y a Internet (público) y realiza cambios en las cabeceras de los paquetes que lo atraviesan.



Funcionamiento detallado de NAT

El router usa una tabla de traducción que contiene 6 campos y se actualiza dinámicamente en tiempo real

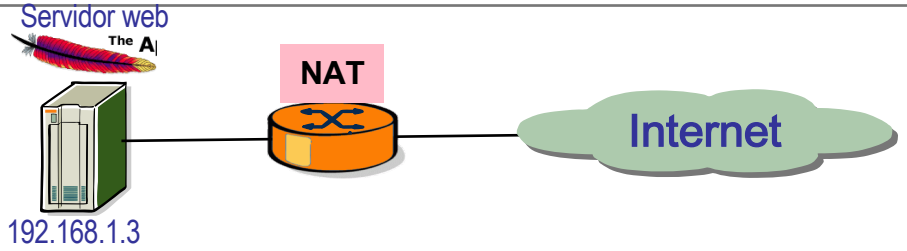


Varios modos de funcionamiento de NAT según cuándo se crea una nueva fila y cuándo se aceptan respuestas (p.ej. full-cone NAT → nueva fila según IP:pto privados; symmetric NAT → nueva fila según origen y destino)

NAT: servidores en una red privada

- NAT no permite el inicio de ninguna comunicación desde el exterior con un host de la LAN. De hecho, para el exterior sólo existe el router NAT y no los equipos finales
  - NAT proporciona un nivel extra de seguridad dentro de la LAN
- No obstante, los routers NAT suelen incorporar mecanismos para permitir de forma controlada que se pueda iniciar una comunicación desde el exterior, típicamente para acceder a un servicio (web, correo, ftp, etc..) ubicado en algún host de la LAN
  - Redirección de puertos ("abrir los puertos") → edición manual de la tabla de NAT del router

TABLA DE TRADUCCIÓN DEL ROUTER NAT			
LADO PRIVADO (LAN)	LADO PÚBLICO (WAN)	PROTO	tiempo
192.168.1.3 : 80	13.11.1.1 : 80	TCP	



NAT

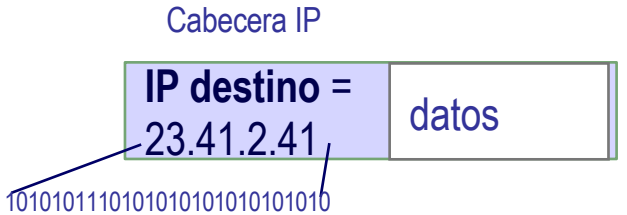
- Existen múltiples formas de atravesar un NAT:
  - Conexión inversa, protocolo STUN, protocolo UPnP, Hole Punching, …
- Con 16 bits para el puerto, un router NAT puede mantener más de 60.000 conexiones simultáneas
- NAT viola el principio de independencia entre niveles
- NAT presenta problemas con protocolos como ICMP y algunos protocolos de aplicación que incluyen direcciones IP o números como parte de su carga últil
  - Application-Level Gateways, NAT que reconocen ciertos protocolos de aplicación y realizan los cambios oportunos (H.323, SIP, FTP, etc…)
- Por eso NAT tiene algunos detractores ya que esta retrasando la entrada de IPv6

Tema 04: La capa de Red

Índice

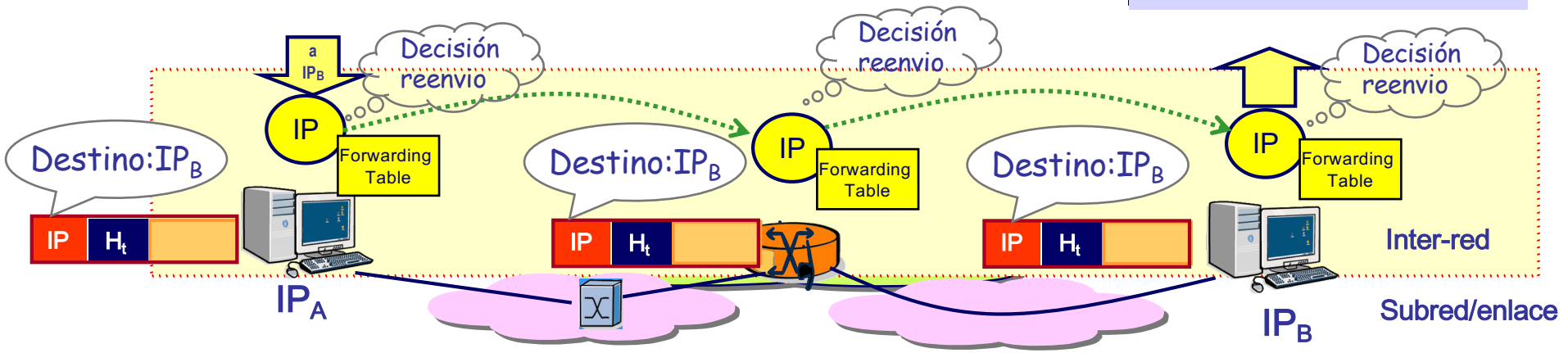
Recortadorio: El Protocolo IP → reenvío de datagramas

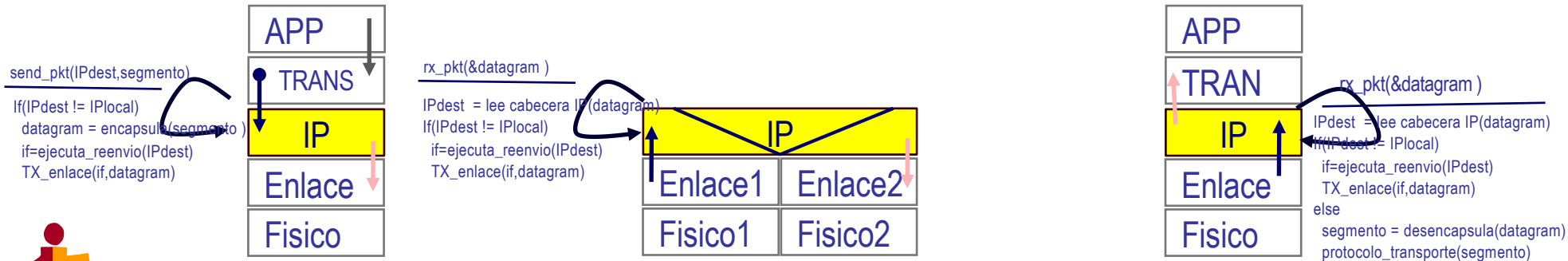
- Necesita:
  1) una cabecera donde leer el destino;
  2) una tabla de reenvío local
  3) un algoritmo para decir la NIC por donde reenviar



Destino:	enlace salida
192.168.0.2 /24	interfaz 1
23.24.1.24 / 24	interfaz 2
0.0.0.0 /0	interfaz 3

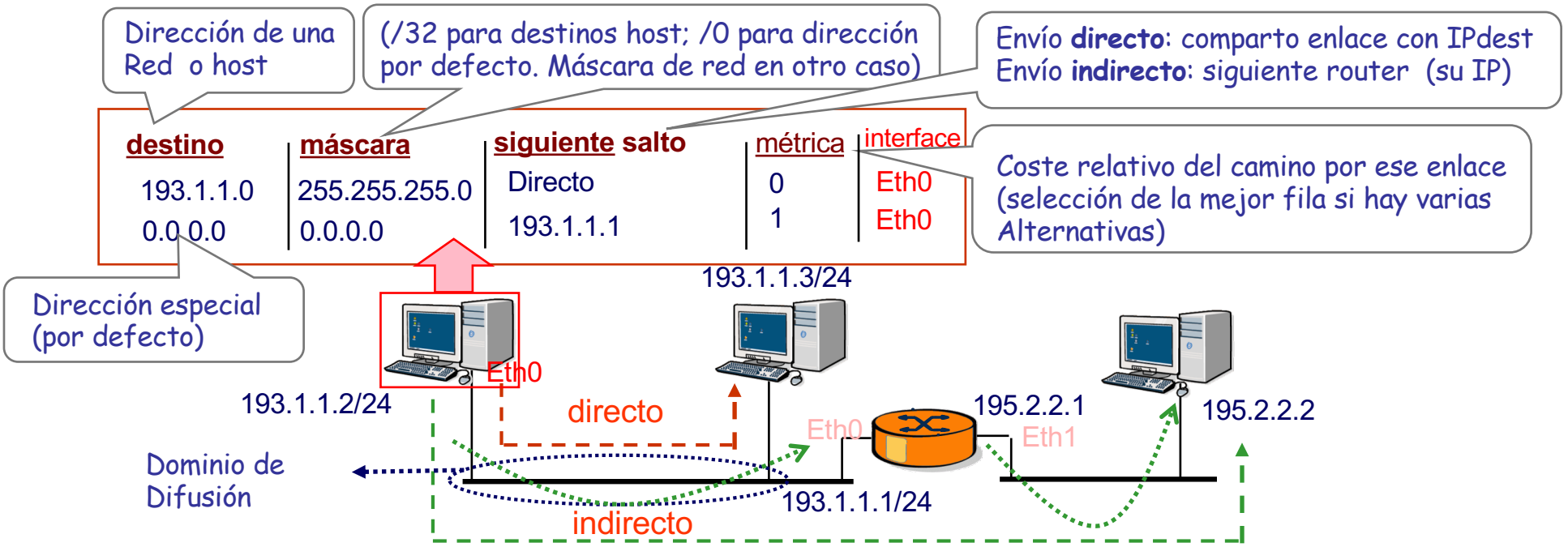
Tabla de Reenvío





Tablas de reenvío

- Cada fila contiene información sobre cómo llegar a un destino
  - Campos: destino; máscara ; siguiente salto; métrica; interface



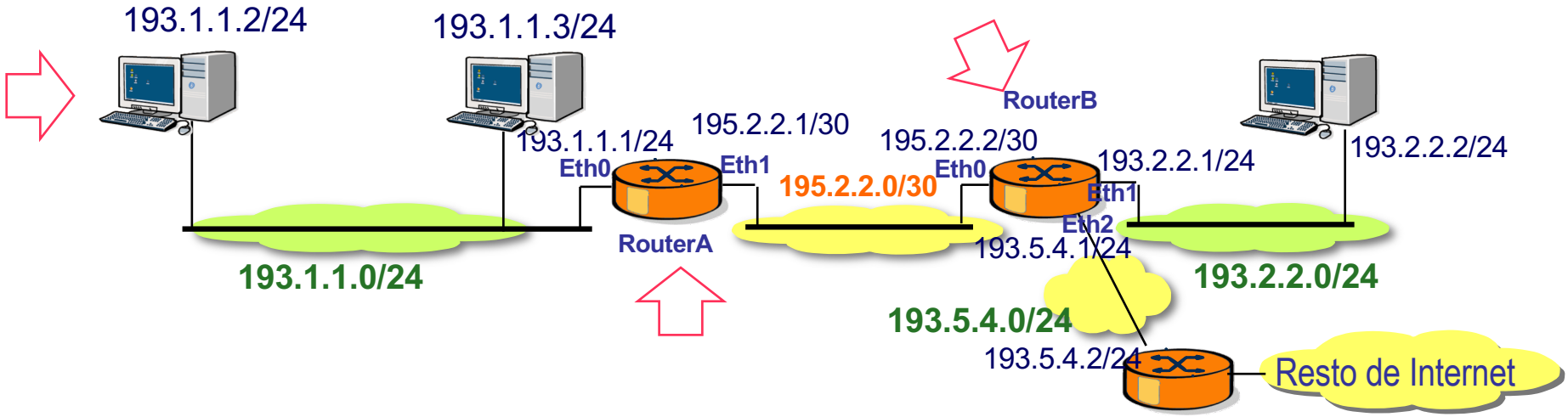
- Las filas se crean
  - Manualmente
  - Automáticamente (el S.O. o el protocolo de routing)
    - Al asignar una IP a un interfaz (fila de envío directo)
    - Por el algoritmo de encaminamiento

Configuración manual: tabla de reenvío en un router

APRENDER DE MEMORIA

- 3 Pasos:

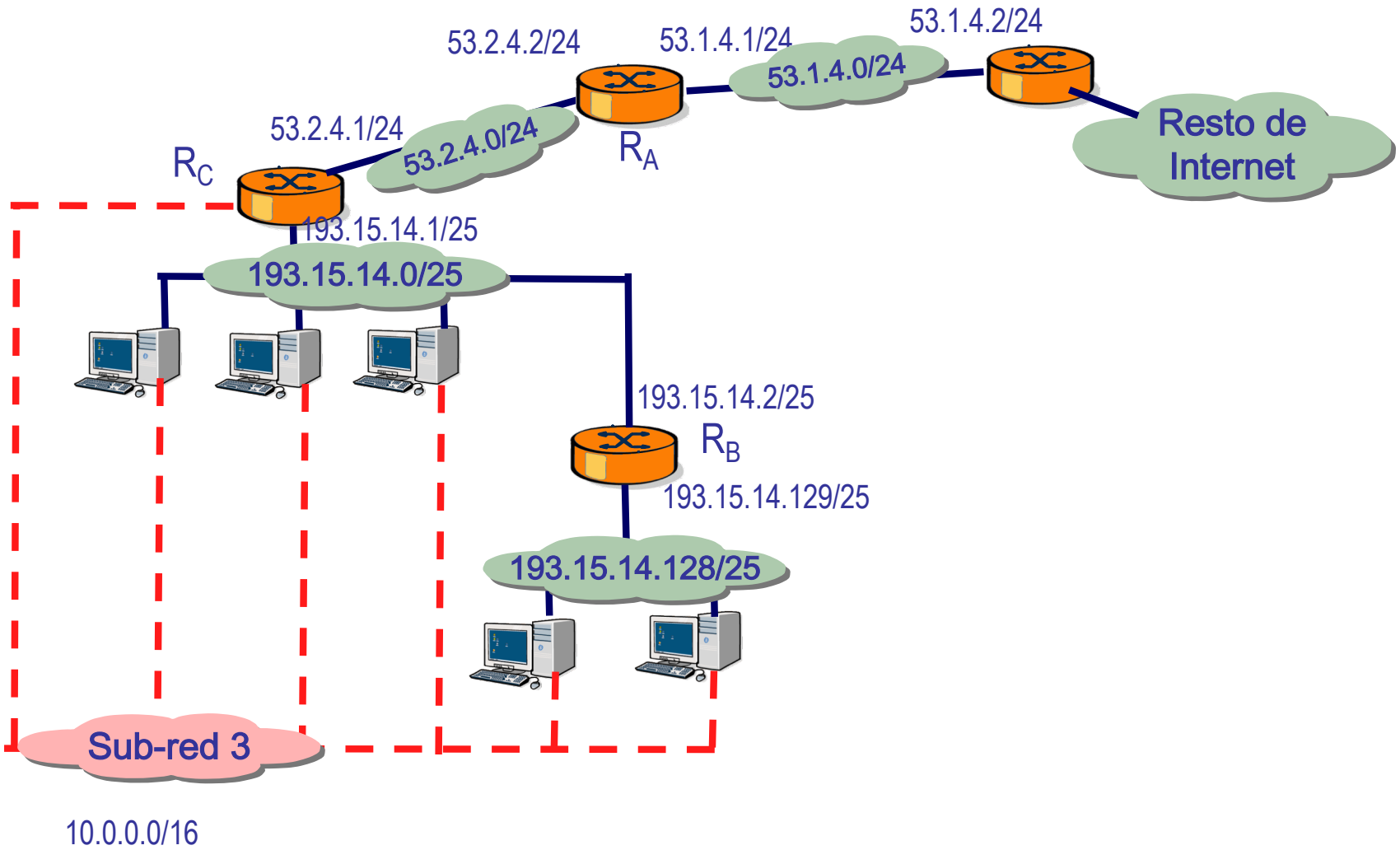
1. ¿a qué redes está directamente conectado? → filas de envío directo
   - SS: Se identifica cada interfaz (puerto) con un nombre (p.e. if0, if1, etc..)
2. ¿qué otras redes existen en la inter-red?→ filas reenvío indirecto
   - SS: dirección IP del siguiente router del camino
   - El siguiente salto debe tener conexión directa por algún interfaz.



3. Utilizar la dirección por defecto 0.0.0.0/0 y agregar prefijos de red para disminuir el número de filas cuando sea posible

Ejercicio

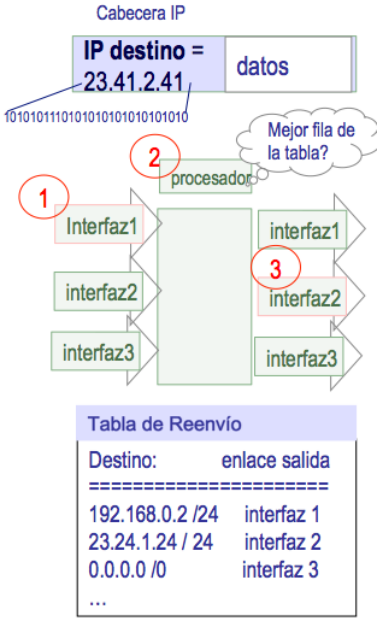
- Configura las tablas de reenvío de R_A, R_B, R_C



El protocolo IP: algoritmo de reenvío

APRENDER DE MEMORIA

- **Lógica utilizada por IP para reenviar cada paquete que le llega**



Extraer dirección IP destino del paquete: IPd

¿ IPdest = IP$_{equipo}$?

SI

Entregar el Datagrama a La capa de transporte

NO (reenvío)

Encontrar la mejor fila en la tabla de reenvío

Para cada fila:

1.- Aplicar la máscara a IPd

2.- Compara el resultado con la dirección destino de la fila

3.- Si coincide, añadir ésta fila a la lista de posibles destinos

4.- Entre los posibles destinos, tomar el de mayor coincidencia (mayor nº de bits en máscara)

5.- Si hay varios de la misma, tomar el de menor métrica

Enviar el paquete por la interfaz de salida correspondiente

Envío directo

Envío indirecto

Ejercicio

- Ejecute el algoritmo de selección de la mejor fila en R_A y R_C si el host 195.3.3.21 envía un paquete a 192.1.1.12

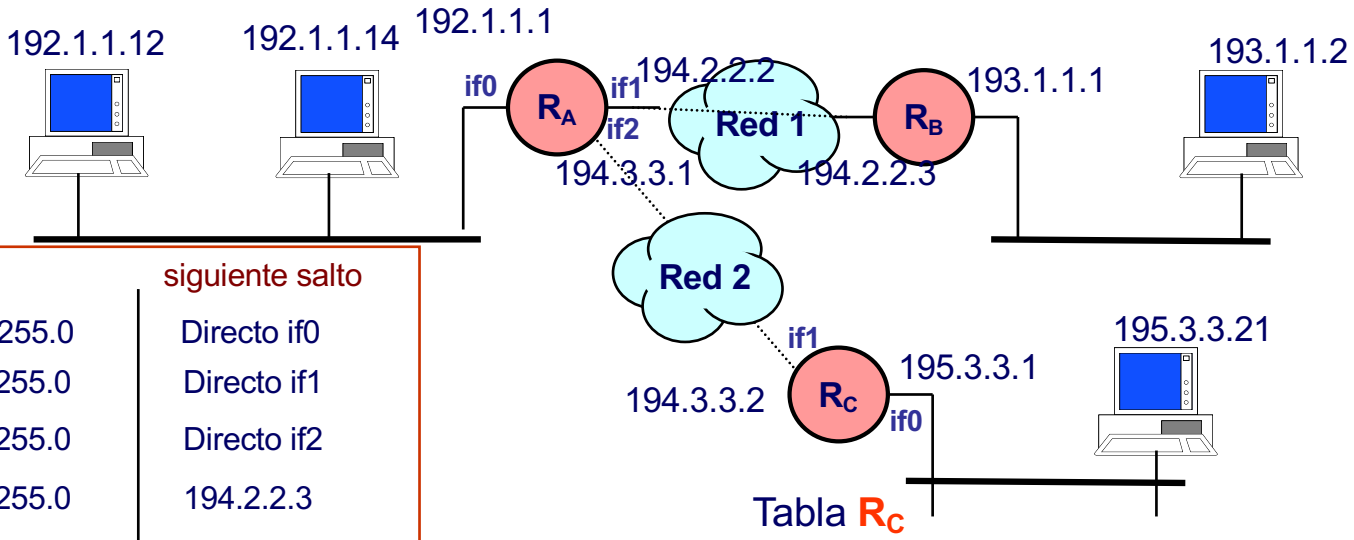


Tabla R_A

destino	máscara	siguiente salto
192.1.1.0	255.255.255.0	Directo if0
194.2.2.0	255.255.255.0	Directo if1
194.3.3.0	255.255.255.0	Directo if2
193.1.1.0	255.255.255.0	194.2.2.3
195.3.3.0	255.255.255.0	194.3.3.2

Tabla R_C

destino	máscara	siguiente salto
195.3.3.0	255.255.255.0	Directo if0
194.3.3.0	255.255.255.0	Directo if1
0.0.0.0	0.0.0.0	194.3.3.1

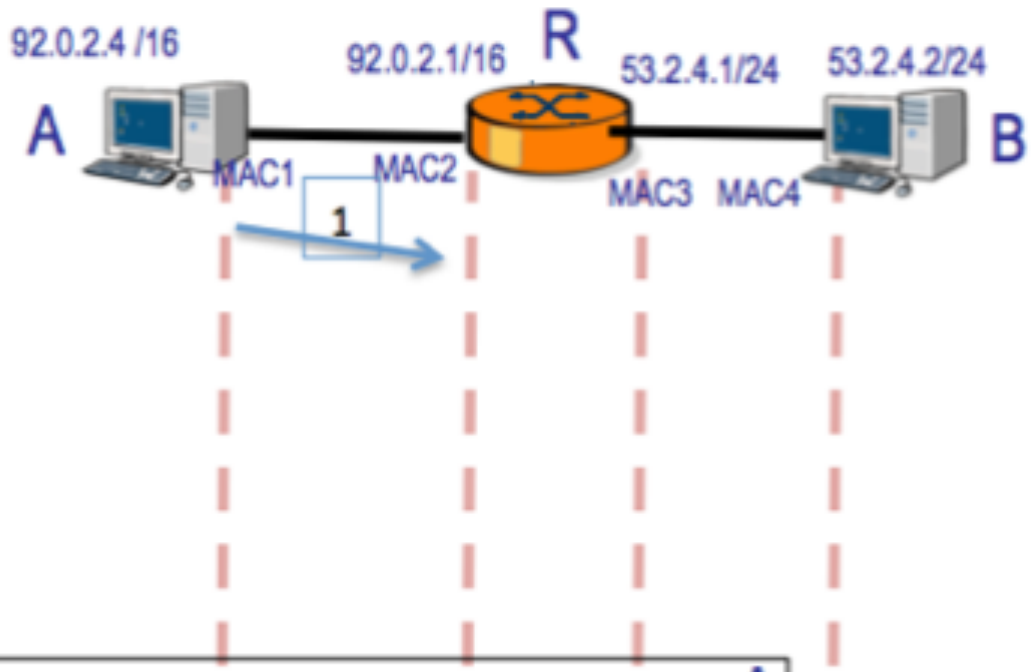
Para cada fila:
1.- Aplicar la máscara a IPd
2.- Compara el resultado con la dirección destino de la fila
3.- Si coincide, añadir ésta fila a la lista de filas candidatas
4.- Entre las filas candidatas, tomar el de mayor máscara
5.- Si hay varios de la misma, tomar el de menor métrica

Tabla **host**

destino	máscara	siguiente salto
195.3.3.0	255.255.255.0	Directo if0
192.1.1.12	255.255.255.255	195.3.3.1
0.0.0.0	0.0.0.0	195.3.3.1

Pregunta: ¿llega o no llega?

- A envía un datagrama a B



A

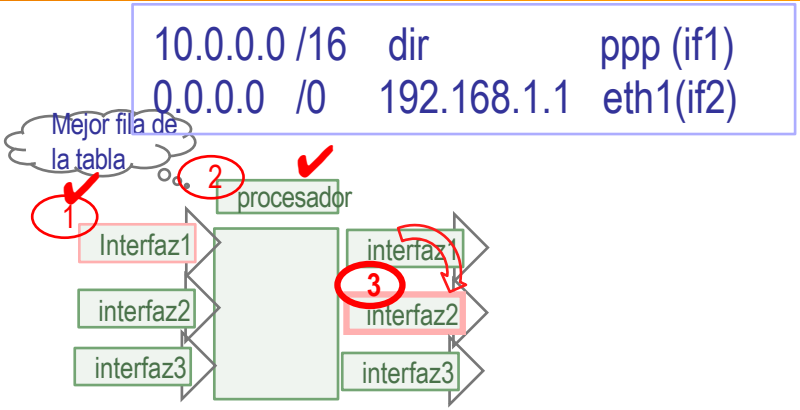
Destino	Mask	SS
92.0.2.0	/16	dir(MAC1)
0.0.0.0	/0	92.0.2.1

R

Destino	Mask	SS
92.0.2.0	/16	dir(MAC2)
53.2.4.2	/24	dir(MAC3)

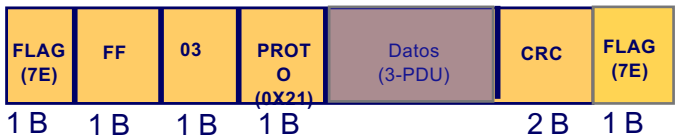
Ya tenemos la mejor fila … ¿y ahora qué?

- **Solicitud del servicio de enlace (3)**
  - **Encapsulamiento del datagrama**
  - **Depende del protocolo de enlace usado en el interfaz elegido**



Caso 1:
Enlace salida tipo punto a punto (p.ej. Protocolo PPP, puerto serie)

RFC 1661
(encapsulación de datagrama IP sobre PPP)

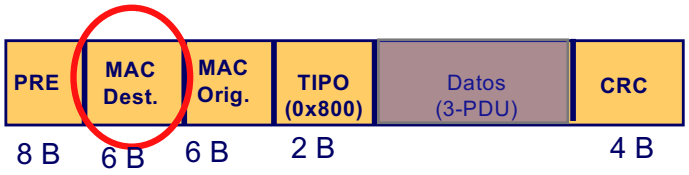


Servicio de un puerto PPP
(orientado a conexión, sin direcciones)

https://technet.microsoft.com/en-us/library/cc957975.aspx

Caso 2:
Enlace salida tipo acceso múltiple
(cada NIC tiene una dirección física que es parte de la cabecera)
(p.ej. Protocolo IEEE 802.3 Ethernet)

RFC 894
(encapsulación de datagrama IP sobre Ethernet)

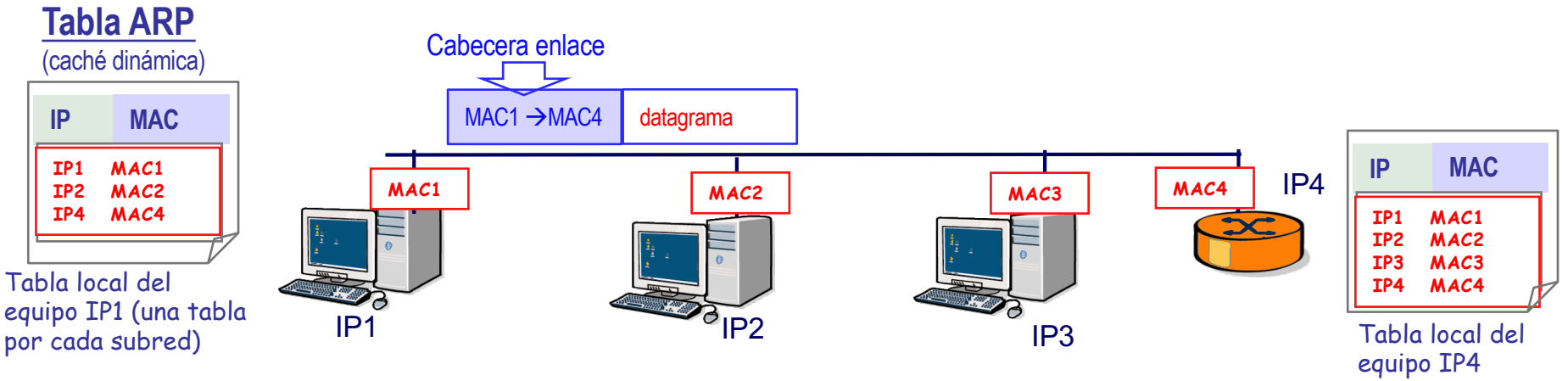


Servicio de un puerto IEEE 802.3
(no O.C. (datagrama), con direcciones)

Caso 2: tabla arp

- En algunos protocolos de enlace, para encapsular el datagrama se necesita conocer la dirección física de la NIC destino. (p.ej. enlaces acceso múltiple)

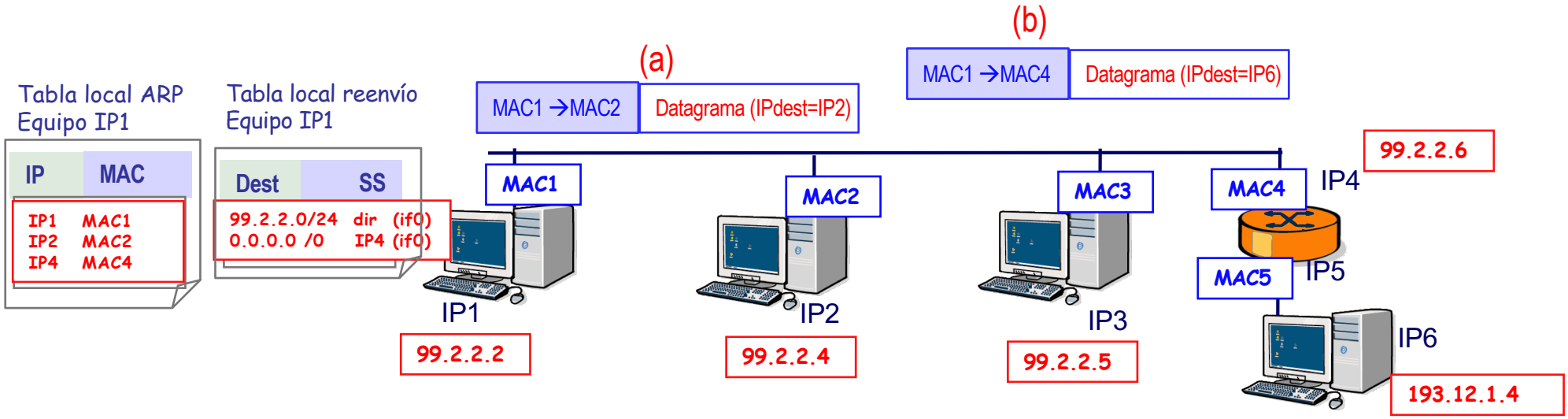
- Solución: tabla local en cada equipo. Contiene la dirección física (MAC) de otros equipos que están en el mismo enlace (identificados por su dirección IP)
  - Un router mantiene una tabla arp por cada enlace (NIC)



(mirar el ordenador de clase con arp /a)

Ejemplo de uso: reenvío directo e indirecto

- Dos casos de reenvío:
  - (a) reenvío directo (IP1→IP2) (necesito conocer la dirección MAC2)
  - (b) reenvío indirecto (IP1->IP6) (necesito conocer la dirección MAC4)

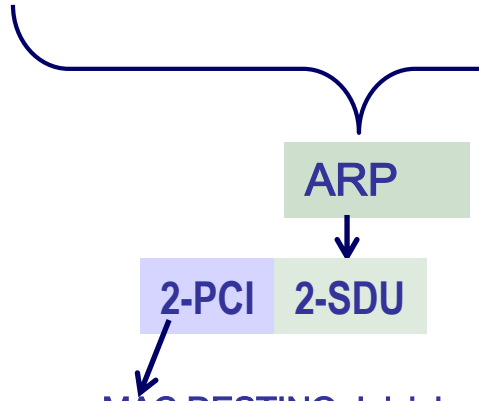


- ¿Y si IP1 quiere encapsular un datagrama destinado a IP3?

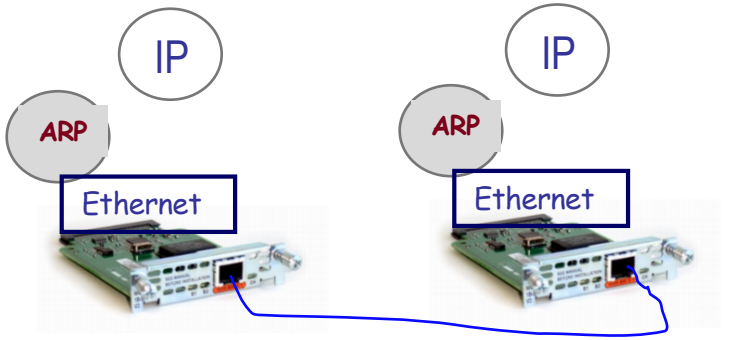
Protocolo ARP [RFC 826]

- Protocolo REQ/RES que usa la difussión en el enlace para traducir cualquier dirección de red a cualquier dirección física
  - No sólo sirve para IP y para Ethernet
  - ARP viaja encapsulado dentro de la trama
- Implementado en las NICs (se usa a nivel de enlace)
- Formato de los mensajes ARP

PROTOCOLO NIVEL ENLACE	PROTOCOL O NIVEL RED	TAMAÑO DIRECCIONES FISICAS (ENL)	TAMAÑO DIRECCIONES DE RED	OPERACIÓN (1 –REQ) (2 – RES)	SHA SENDER HARDWARE ADDRESS	SPA SENDER PROTOCOL ADDRESS	THA TARGET HARDWARE ADDRESS	TPA TARGET PROTOCOL ADDRESS
1 (ETHERNET)	0X0800 (IPV4)	6 (B)	4 (B)	1 (REQ)	0XA8F2FF234212 (MAC SOURCE)	0X48F2FF23 (IP SOURCE)	0x0000000000 (MAC TARGET)	0X48F2FF23 (IP TARGET)



MAC DESTINO. Inicialmente difusión: 0xFFFFFFFFFFFF
Identifica al protocolo encapsulado (p.ej. ARP, o IP)

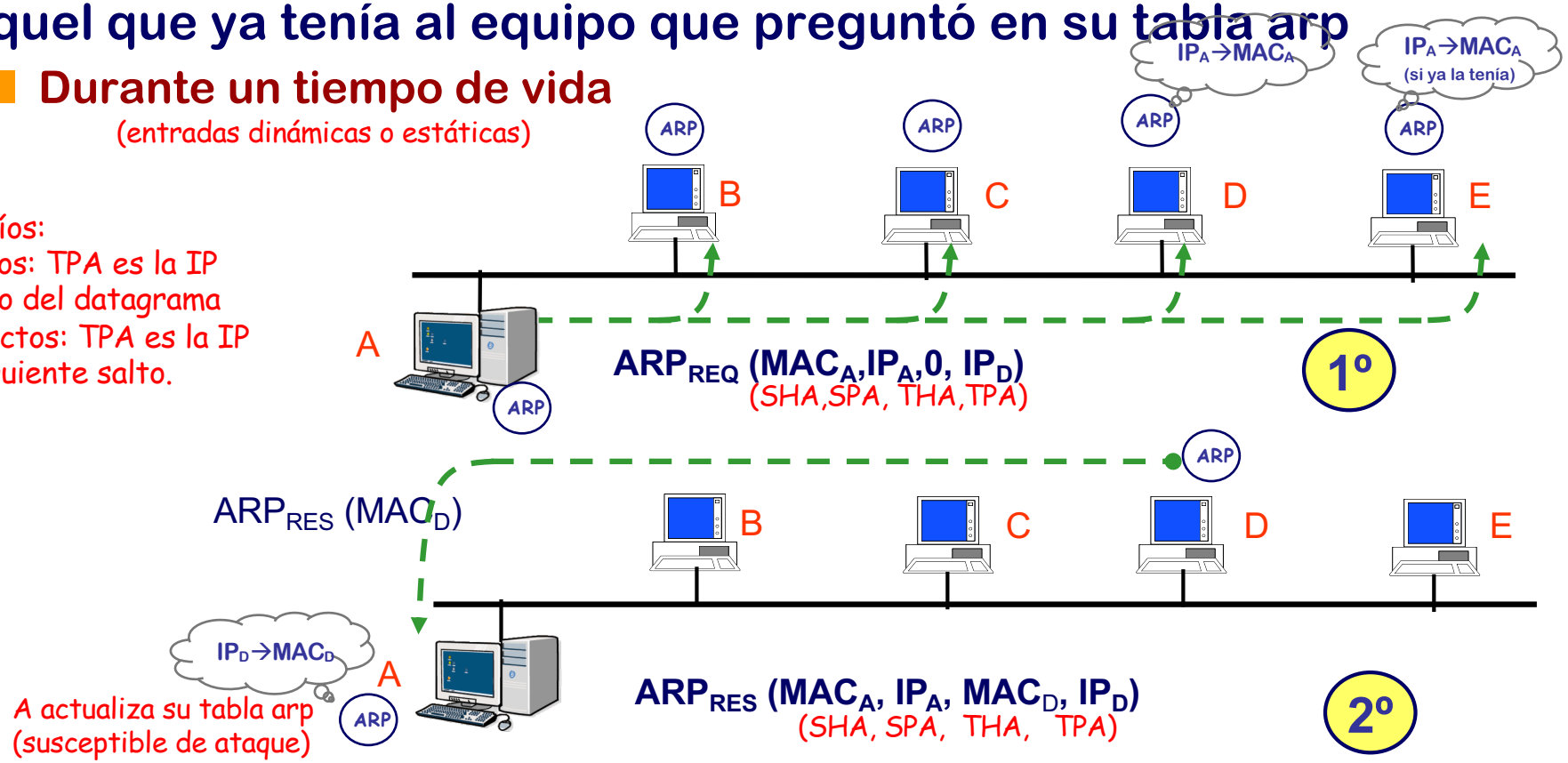


Ejemplo: Ethernet usa direcciones MAC IEEE 802.1.

Ejemplo:

- **Protocolo de resolución de direcciones** APRENDER DE MEMORIA
  - **Ventajas: fácil crecimiento, independiza las direcciones de red de las direcciones físicas.**
- **Actualizan su tabla arp: Los equipos origen y destino y todo aquel que ya tenía al equipo que preguntó en su tabla arp**
  - **Durante un tiempo de vida**
    (entradas dinámicas o estáticas)

En reenvíos:
- directos: TPA es la IP destino del datagrama
- Indirectos: TPA es la IP del siguiente salto.

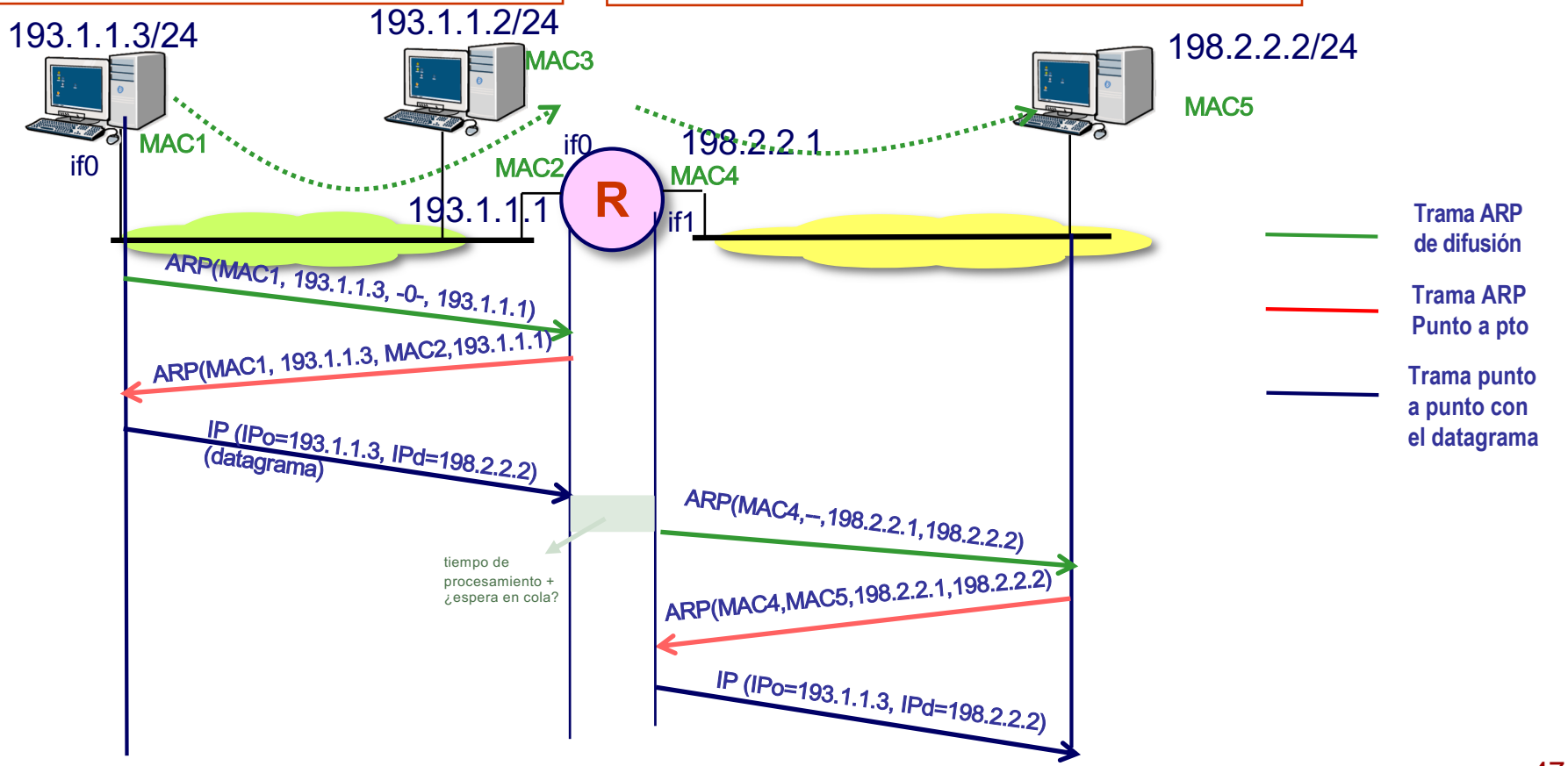


Ejemplo

- Datos de las tramas intercambiadas para que el equipo 193.1.1.3 pueda hacer llegar un datagrama al 198.2.2.2

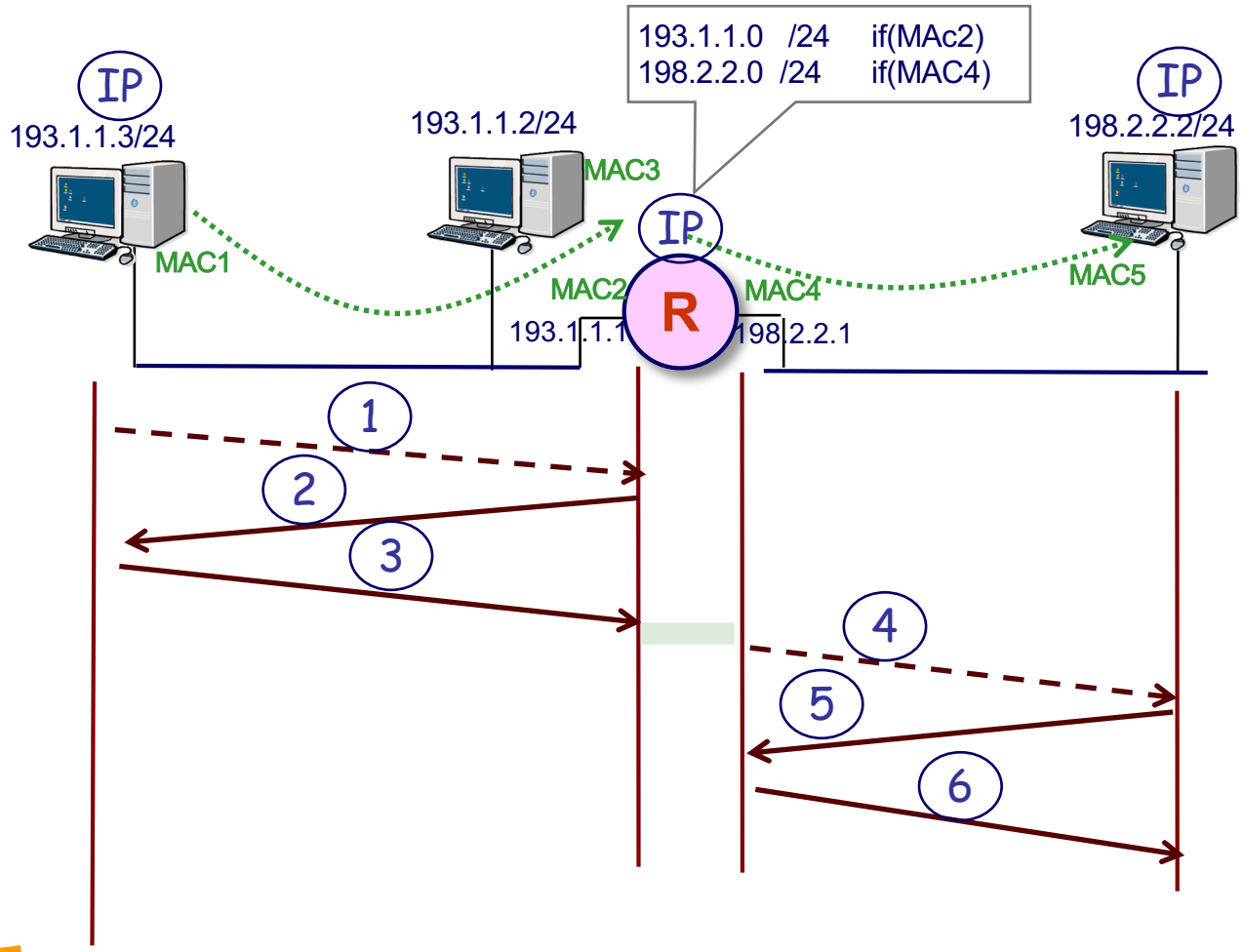
destino	máscara	siguiente salto
193.1.1.0	255.255.255.0	Directo if0
0.0.0.0	0.0.0.0	193.1.1.1

destino	máscara	siguiente salto
193.1.1.0	255.255.255.0	Directo if0
198.2.2.0	255.255.255.0	Directo if1



Ejemplo (II)

- Indique las tramas intercambiadas para que el equipo 193.1.1.3 pueda hacer llegar un segmento SYN al 198.2.2.2:80



1
L4
L3
L2

Ori	Des	Encap
MAC1	0xFFFF..F	ARP(RQ)

2
L4
L3
L2

MAC2	MAC1	ARP(RES)

3
L4
L3
L2

23921	80	
193.1.1.3	198.2.2.2	TCP
MAC1	MAC2	IP

4
L4
L3
L2

Ori	Des	Encap
MAC4	0xFFFF..F	ARP(RQ)

5
L4
L3
L2

MAC5	MAC4	ARP(RES)

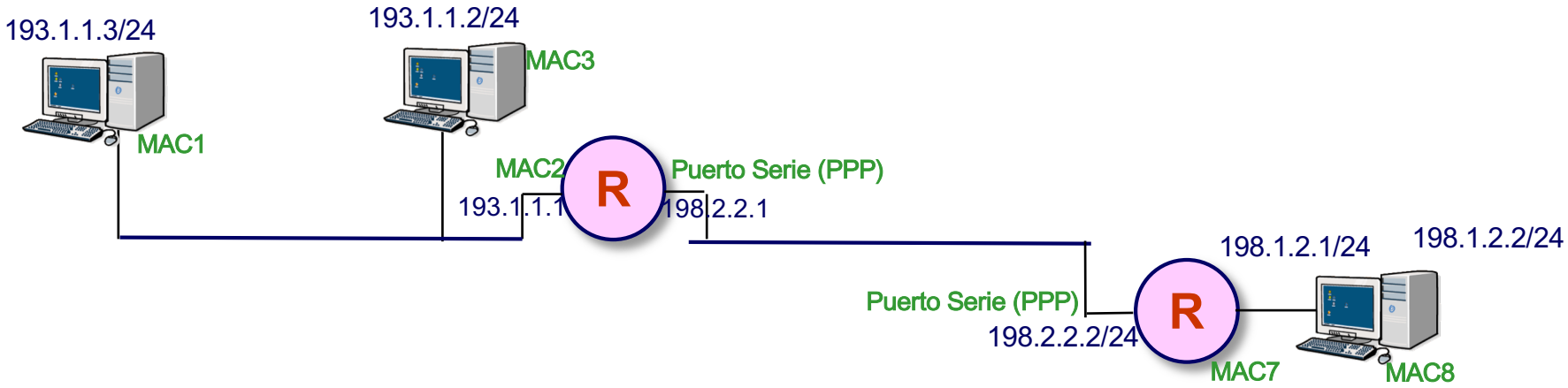
6
L4
L3
L2

23921	80	
193.1.1.3	198.2.2.2	TCP
MAC4	MAC5	IP

Ejercicio

- Indique las tramas intercambiadas para que el equipo 193.1.1.3 pueda hacer llegar un segmento UDP al 198.1.2.2:53
  - Escriba primero las tablas de reenvío de los routers

1	Ori	Des	Encap
L4			
L3			
L2			



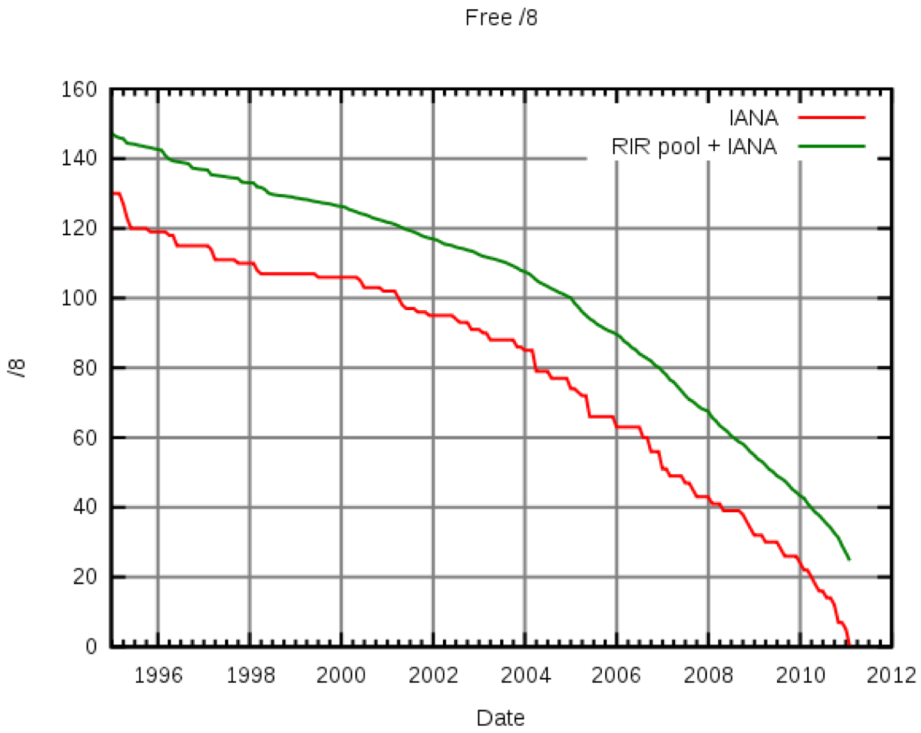
Tema 04: La capa de Red

Índice

IPv6

- **Motivación Inicial**: el espacio de direcciones libres de IPv4 esta prácticamente agotado

  - Otras motivaciones para cambiar la cabecera:
    - Ayudar a acelerar el procesado/reenvío
    - Ayudar a facilitar QoS



http://www.ripe.net/internet-coordination/news/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

Cabecera IPv6 (RFC2460)

- Tamaño fijo: 40 bytes (320bits)
  - Dirección IPv6 (16 bytes)
  - Notación: (cada 2 bytes : en hex)

```
0010000000000001 → 2001
0000110110111000 →    0DB8
0000000000000000 →         0000
0000000000000000 →              0000
0000001010101010 →                   02AA
0000000011111111 →                        00FF
1111111000101000 →                             FE28
1001110001011010 →                                  9C5A
```

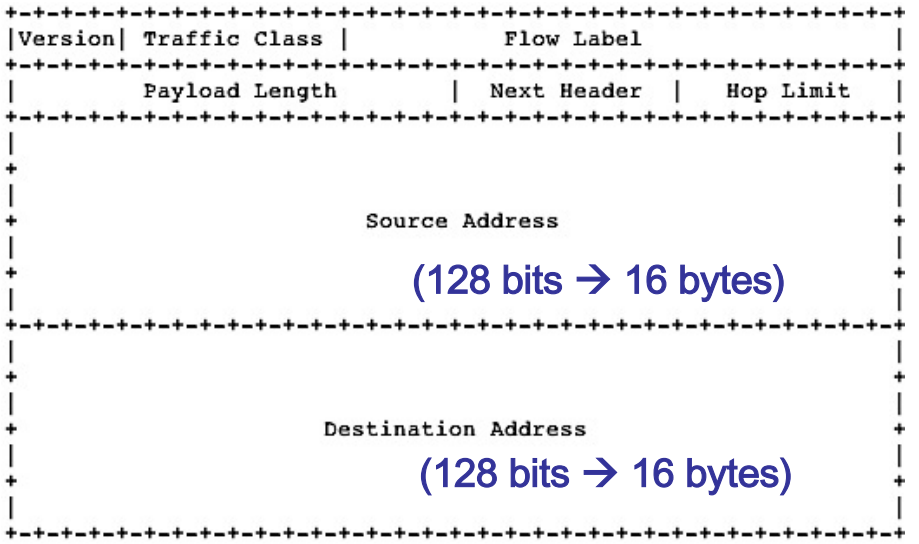
2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A

↓

2001:DB8::2AA:FF:FE28:9C5A

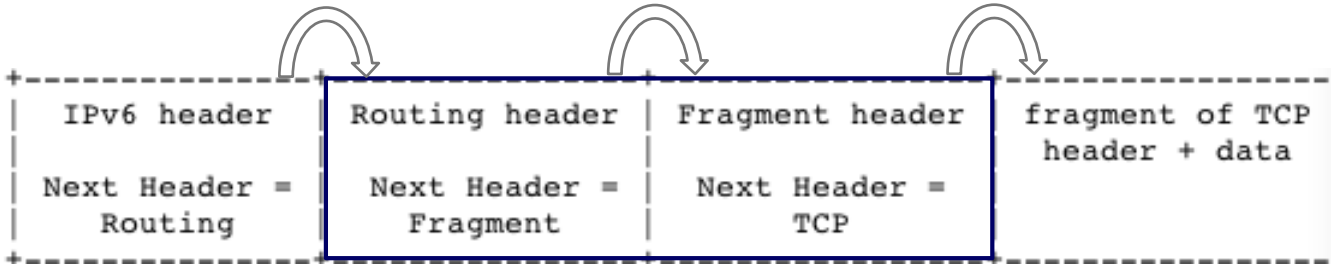
- Concepto de Flujo: secuencia de paquetes entre IP_{origen} e $IP_{destino}$ para los que la fuente desea que los routers dispensen un trato especial
  - Vale 0 para los que no tienen flujo

- Campos (nuevos):
  - Class (Prioridad): identifica la prioridad entre datagramas de un "flujo"
  - Flow Label: identifica datagramas pertenecientes al mismo flujo
  - Next Header: identifica al protocolo encapsulado (nivel superior)



Otros cambios respecto a IPv4

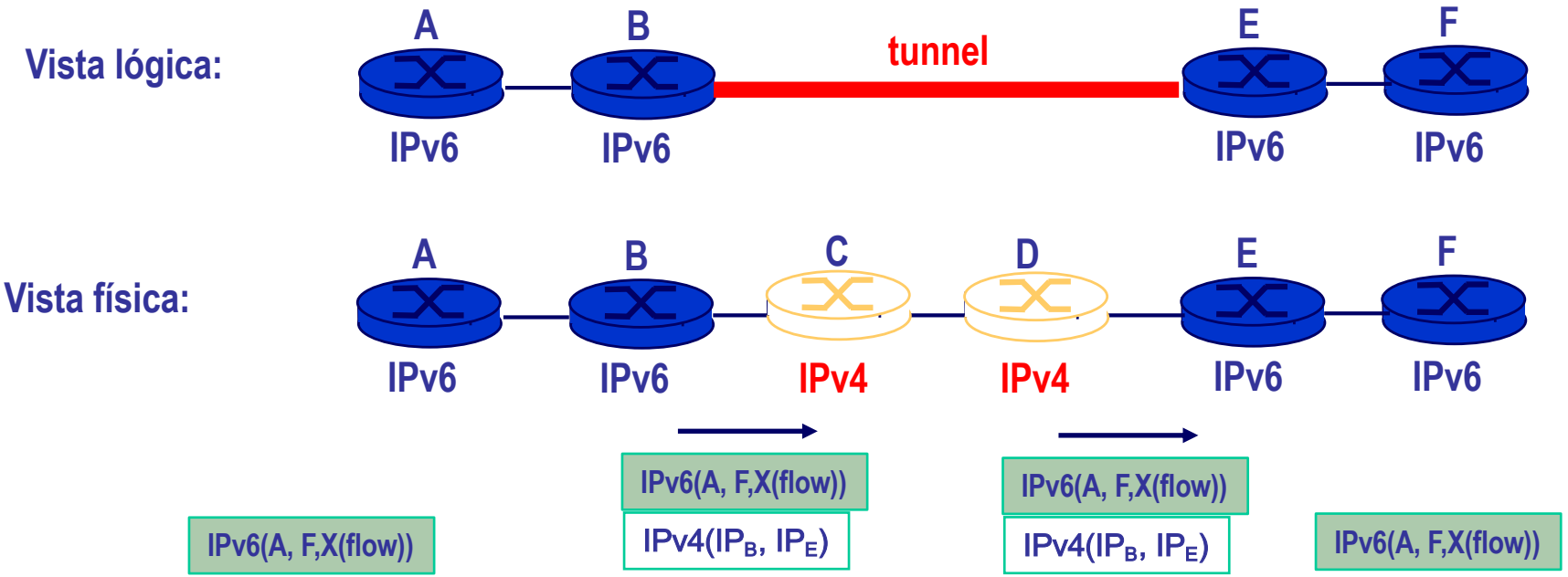
- Checksum eliminado→ ahorra tiempo de procesamiento en cada router
- Opciones: permitidas, pero fuera de la cabecera, indicadas como nuevas cabeceras por el campo “Next header”.
  - Protocolos a implementar en los mismos sitios donde se implementa IPv6 (debajo de transporte)
  - p.e. La fragmentación pasa a ser opcional con una cabecera propia (tb cabeceras de encaminamiento, etc..)



- ICMPv6: nueva versión
  - Tipos de mensajes adicionales, p.e. “Packet too big”
  - Funciones de gestión de grupos multicast
- NDP (Network Discovery Protocol) → ARP para IPv6

Transición IPv4 → IPv6

- Todos los routers no pueden ser cambiados a la vez (mapa)
  - No hay “banderazo”
  - ¿cómo opera Internet con una mezcla de IPv4 e IPv6?
- **Túneles**: IPv6 es encapsulado como protocolo usuario de IPv4 entre aquellos routers IPv4



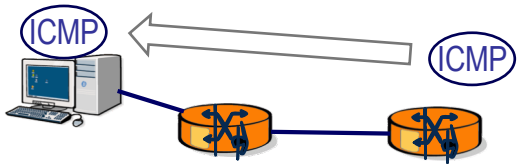
Tema 04: anexos

-CONTROL DE ERRORES: PROTOCOLO ICMP

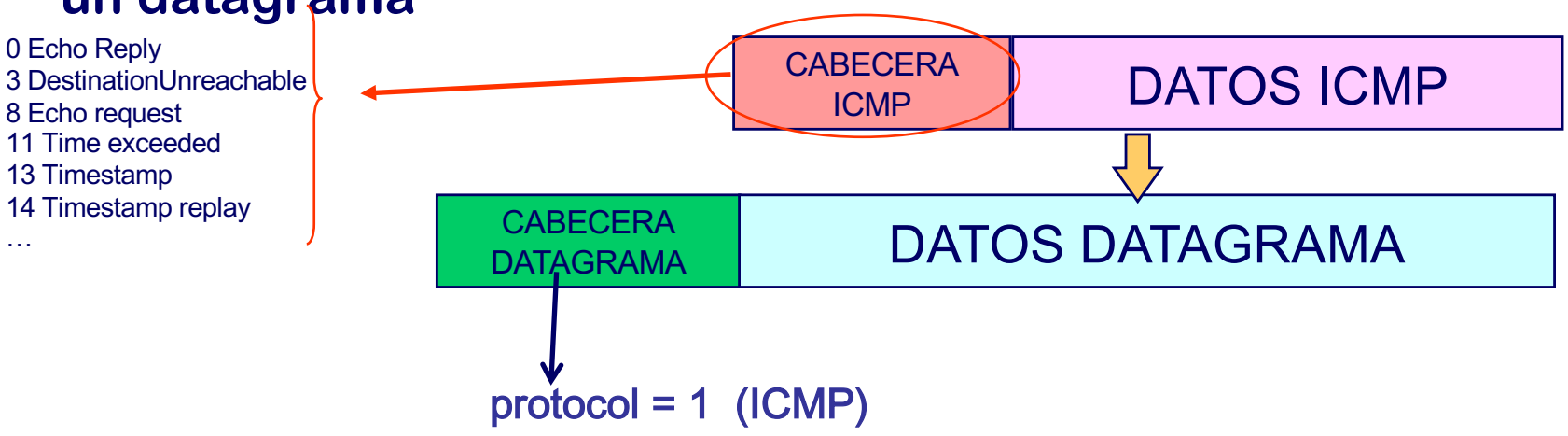
- ASIGNACIÓN DE DIRECCIONES: PROTOCOLO DHCP

El protocolo IP: control de errores

- Señalización de condiciones excepcionales en IP
  - ICMP (Internet Control Message Protocol, RFC 792)
    - Proporciona mecanismos para suministrar información sobre errores o condiciones excepcionales (también para diagnóstico)
      - Destino inalcanzable, tiempo de vida excedido, redirección, eco, …
    - Se informa solamente al remitente del datagrama (no a nodos intermedios) aunque colaboran los routers (protocolo de nivel 3)



- Los mensajes (PDUs) de ICMP van encapsulados como datos en un datagrama



Formato del mensaje ICMP

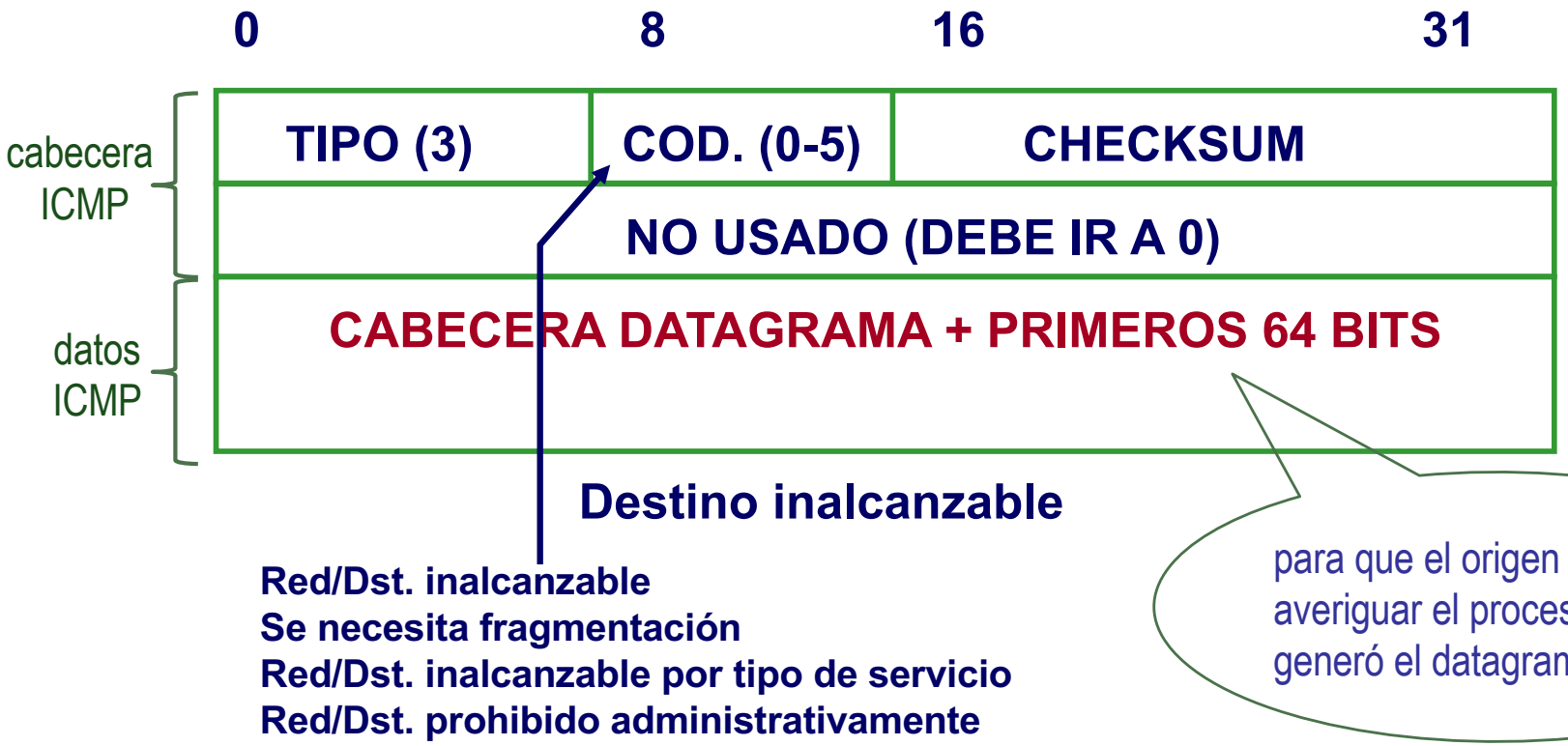
- Cabecera (8 bytes) + datos opcionales (después de la cabecera)
  - Tipo y subtipo (código) determinan el resto de la cabecera y los datos
  - Checksum sobre toda la PDU (cabecera + datos)

- Tipos de mensajes:
  - Solicitud de eco
  - Respuesta a un eco
  - Destino inalcanzable
  - Tiempo de vida excedido
  - Redirección (cambio de ruta)
  - Congestión ("Source Quench")

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Información de destino inalcanzable

- Causa: no puede entregarse un datagrama
- PDU de ICMP del router al origen



Mensaje de eco

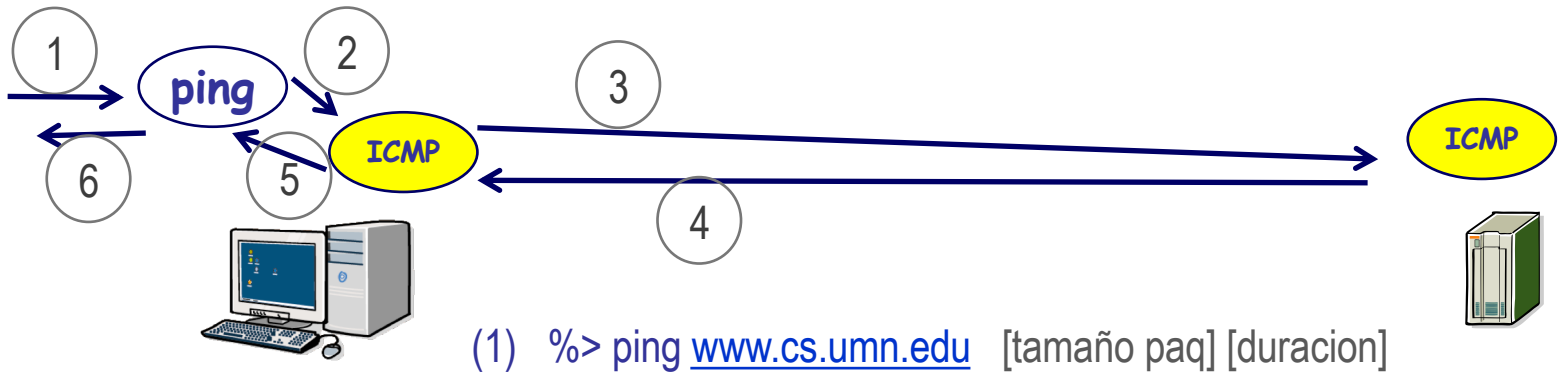
- Causa: Petición/Respuesta de Eco
  - ICMP ECHO REQUEST (tipo 8)/REPLY (tipo 0), código 0 en ambos casos
- Utilidad: Comprueba:
  - el funcionamiento del encaminamiento
  - el funcionamiento de IP y ICMP del destinatario

Datos opcionales que serán devueltos al origen sin alteración

Sirven al remitente para comparar las respuestas con las peticiones

ping: aplicación que usa los mensajes de eco ICMP

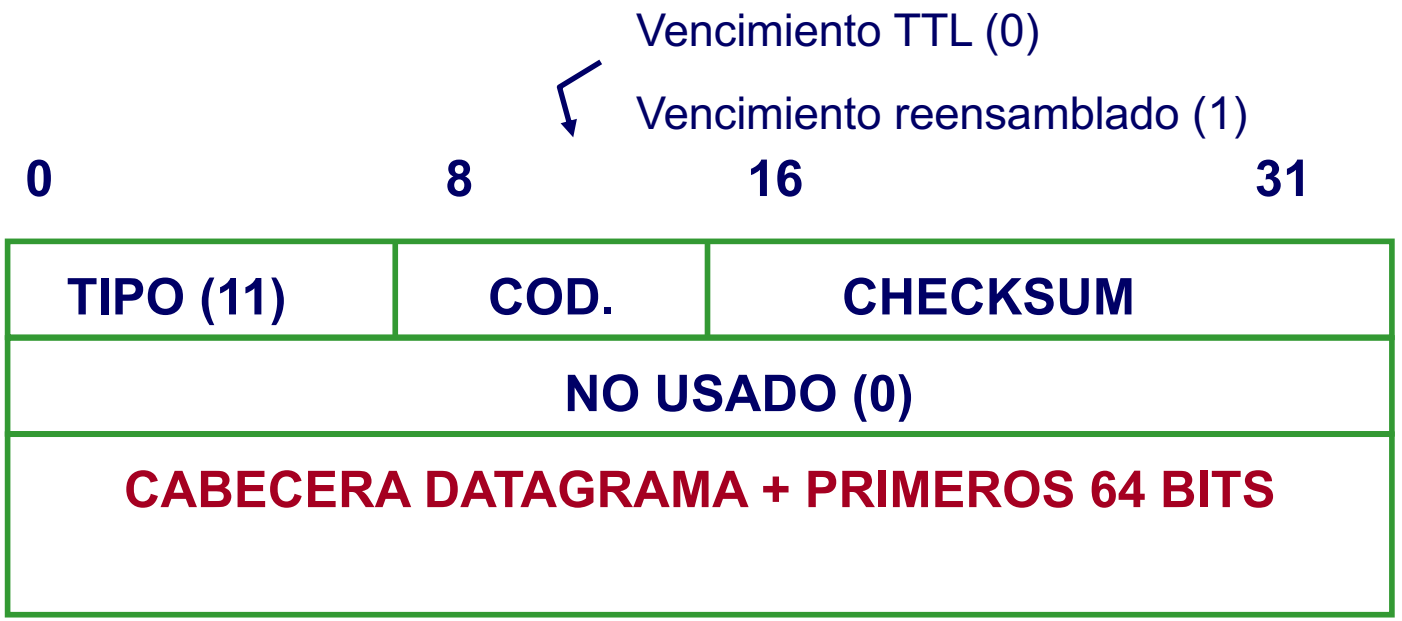
- **Utilidad: averiguar si un sistema está accesible a nivel 3**
- **Ping usa envía mensajes de eco a un destino IP y recibe respuesta.**
  - **El destino es seleccionable por el usuario (IP o hostname)**
  - **Envía varias peticiones de echo (cada una con un número de secuencia diferente) y aprovecha las respuestas para recolectar estadísticos (retardos y pérdidas)**



(1) %> ping www.cs.umn.edu [tamaño paq] [duracion]
(2) Resuelve nombre y crea un bucle
(3) ICMP echo request
(4) ICMP echo reply
(5) Correlación de respuestas y recolección estadísticos
(6) Representación en pantalla para el usuario

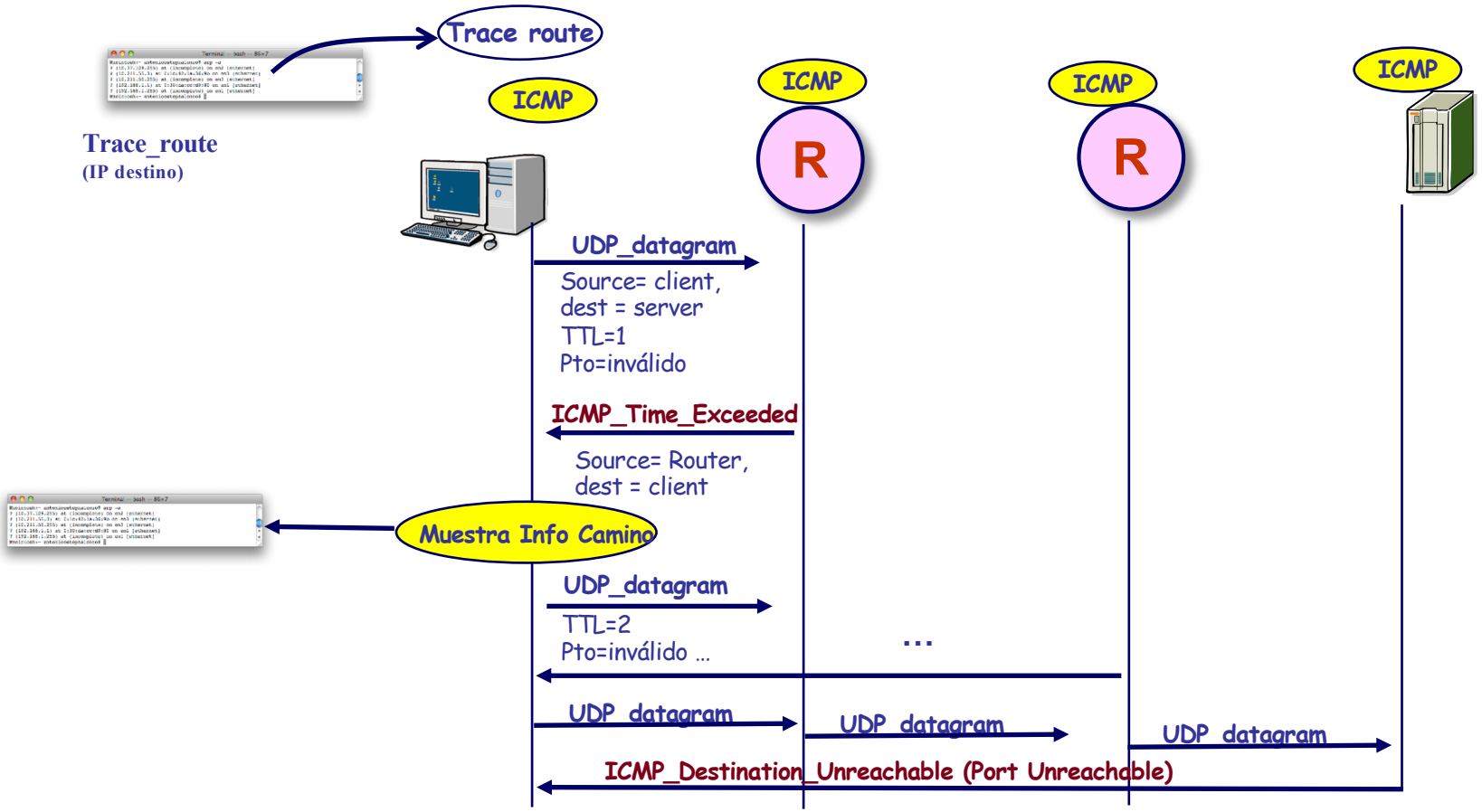
Detección de Bucles

- Causa: expiración del TTL de un datagrama o del plazo de reensamblado en la fragmentación
  - Se descarta el datagrama
  - Se envía un mensaje ICMP hacia el origen



Traceroute: (tracert)
aplicación que usa mensajes ICMP (eco y TTL excedido)

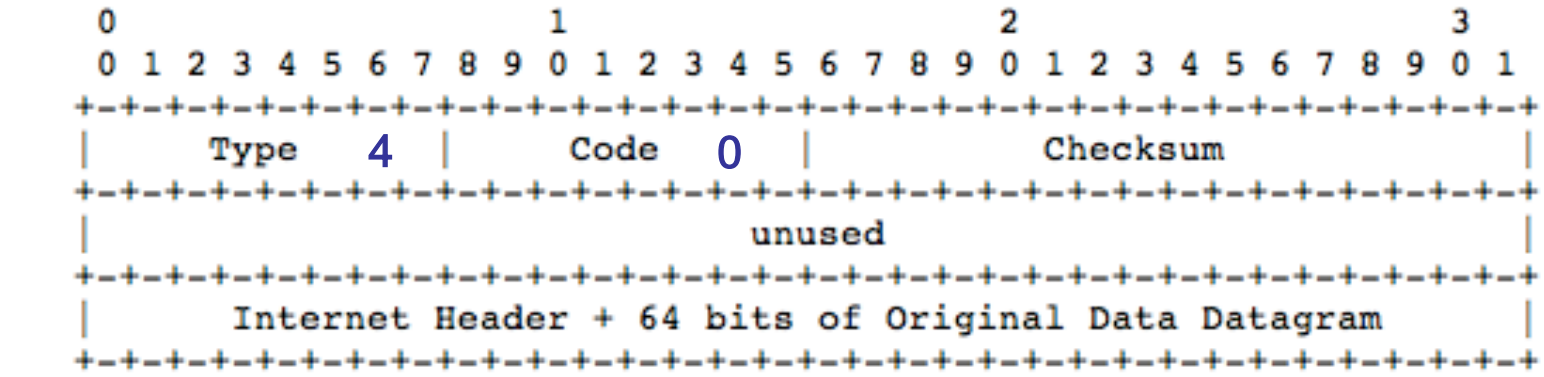
- **Utilidad:** permite conocer la ruta por un datagrama IP.
- Envía ecos ICMP con tiempos de vida bajos para provocar que los routers atravesados generen mensajes de error (Tiempo de vida excedido) y así conocer el camino seguido.



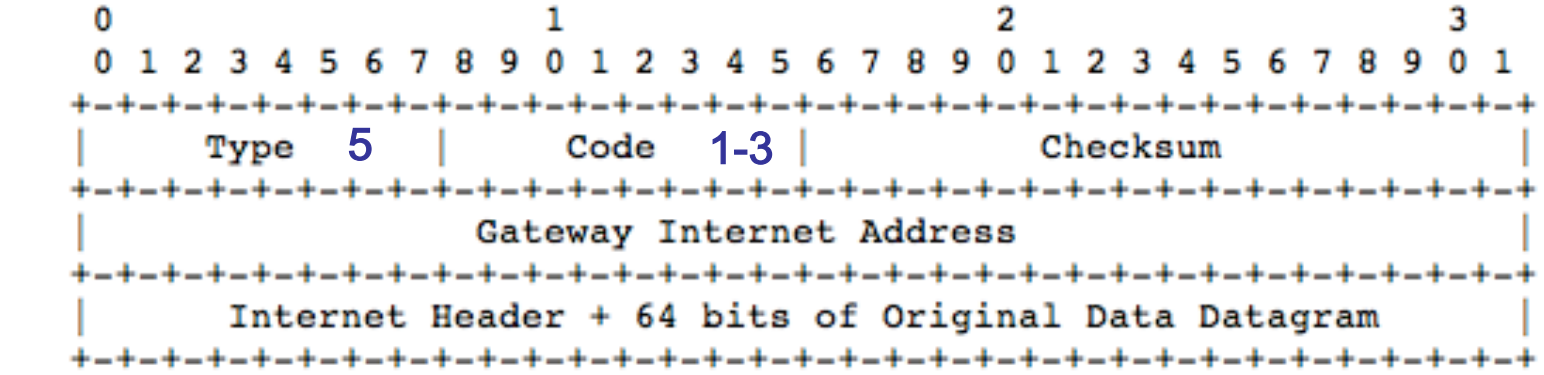
Otros mensajes ICMP ...

- Ojear la RFC 792

Source Quench Message



Redirect Message



Tema 04: anexos

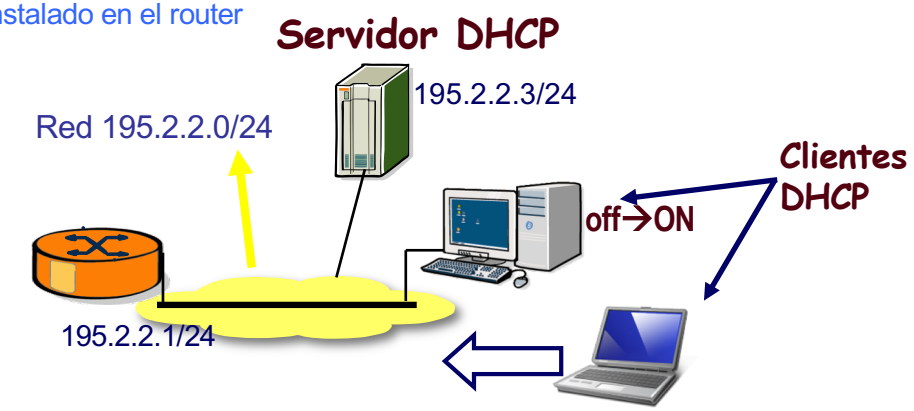
NOTAS PARA LAS PRÁCTICAS

-CONTROL DE ERRORES: PROTOCOLO ICMP

- **ASIGNACIÓN DE DIRECCIONES: PROTOCOLO DHCP**

Dynamic Host Control Protocol, RFC 2131 (1997)

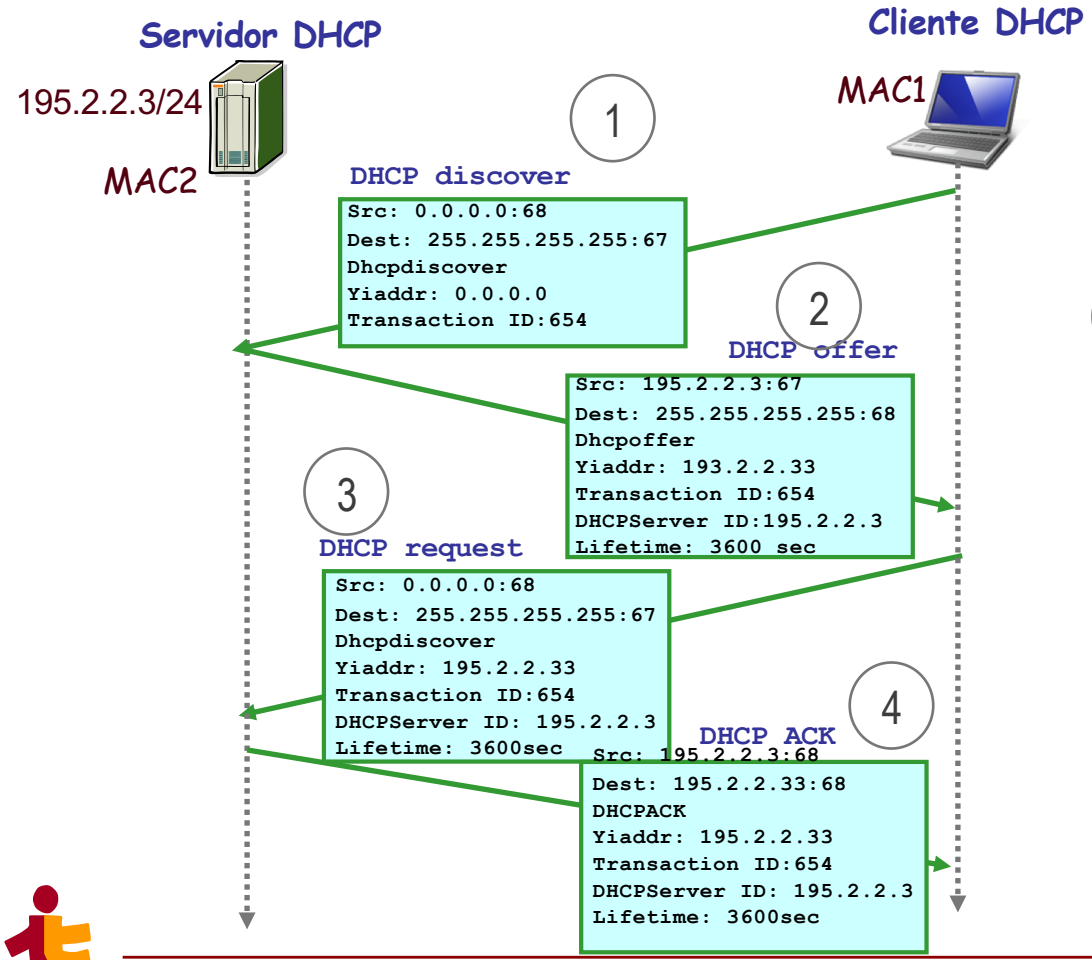
- No es bueno que cada usuario configure su propio equipo
  - Al menos: IP propia y máscara, IP router (GW), IP servidores DNS
- DHCP es una aplicación para la configuración automática de hosts controlada por un administrador (al menos dirección IP, GW y DNS)
  - DHCP usa un protocolo cliente/servidor (puertos 68/UDP (C), 67/UDP(S))
    - Cliente: suele ser un host que acaba de iniciarse y desea obtener la configuración necesaria para conectarse a la red/Internet (incluyendo su propia IP).
    - Servidor: atiende las peticiones de los clientes DHCP asignándoles su configuración (préstamo dinámico, asignación automática o manual en función de la dirección física)
      - El servidor también puede estar instalado en el router



  - En el caso mas simple, cada subred tendrá su servidor DHCP, si no, es necesario un agente de reenvío (p.e. router) que conozca la dirección IP del servidor DHCP

Ejemplo DHCP: funcionamiento básico en 4 pasos

- Caso simple: cliente y servidor en la misma subred
  - Puede haber más de un servidor DCHP en la subred
  - El cliente deberá renovar sus valores cuando termine el tiempo de préstamo



ver en RFC 2131

1
DHCP: "Yipadd:0.0.0.0 , transac. ID=654"
UDP: 68 → 67 (DHCP)
IP:0.0.0.0→ 255.255.255.255 (UDP)
L2:MAC1 → FF:FF .. (IP)

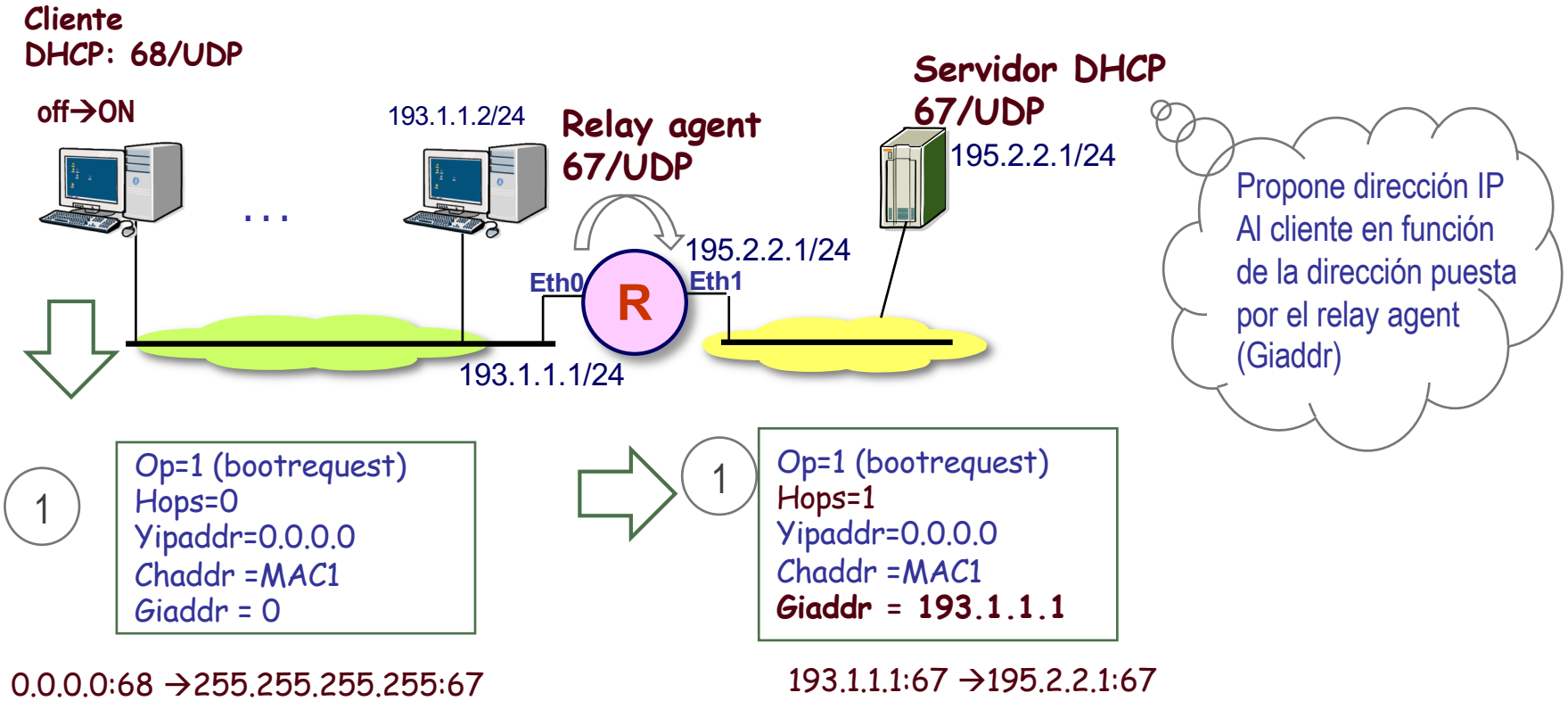
2
DHCP: "Oferta, Servidor, transac. ID=654"
UDP: 67 → 68 (DHCP)
IP:195.2.2.3→ 255.255.255.255 (UDP)
L2:MAC2 → MAC1 (IP)

3
DHCP: "oferta selecionada, trans. ID=654"
UDP: 68 → 67 (DHCP)
IP:0.0.0.0→ 255.255.255.255 (UDP)
L2:MAC1 → FF:FF… (IP)

4
DHCP: "oferta selecionada, trans. ID=654"
UDP: 67 → 68 (DHCP)
IP:195.2.2.3→ 195.2.2.33 (UDP)
L2:MAC2 → MAC1… (IP)

DHCP con servidor en distinta sub-red (RFC 1532)

- Router hace de agente de reenvío (BOOTP relay agent)
  - Pasa los mensajes DCHP entre el cliente y el servidor DHCP
  - Conoce la IP del servidor DHCP (configuración local: unicast o difusión)
  - Usa el campo giapp (Gatewat IP address) para identificarse



Utilidad de DHCP

- Es una magnífica forma de administrar los parámetros de red de clientes y servidores a través de un solo punto (o un grupo de servidores redundantes)
- Se puede usar para configurar muchas más cosas que la conectividad a Internet (p.e. servidores de email, DNS, etc…)
  - Ver http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
- Potenciales problemas de DHCP
  - Seguridad
    - Clientes o Servidores no autorizados
      - ¿qué ocurre si me instalo un servidor DHCP en mi PC?
      - ¿qué ocurre si un cliente “loco” inunda de peticiones al servidor?
  - Clientes móviles
    - Cuando un portátil se conecta a una nueva subred obtiene una nueva IP … no se pueden mantener sesiones (conexiones) abiertas previamente.
    - Solución en RFC 5944 (agentes de IP móvil)

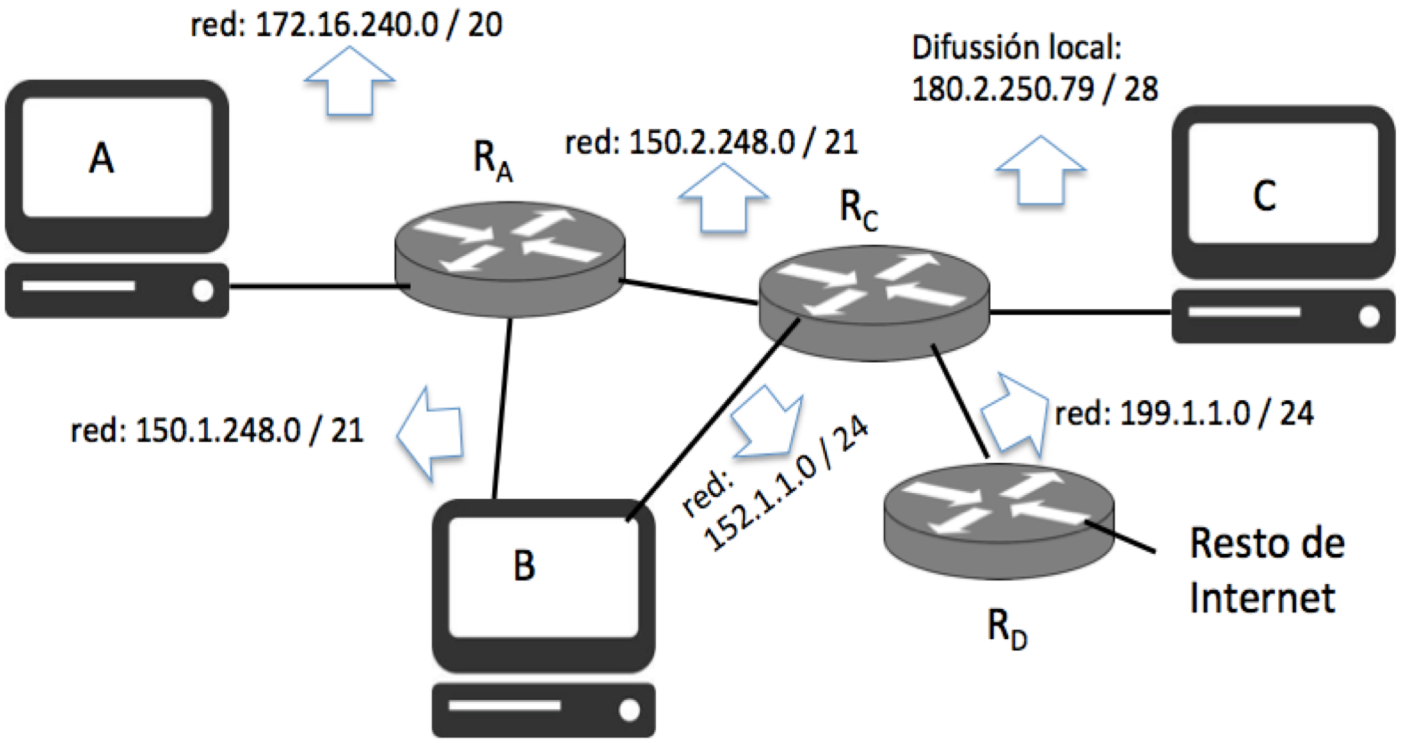
EJERCICIOS IP

Tipos de Ejercicios

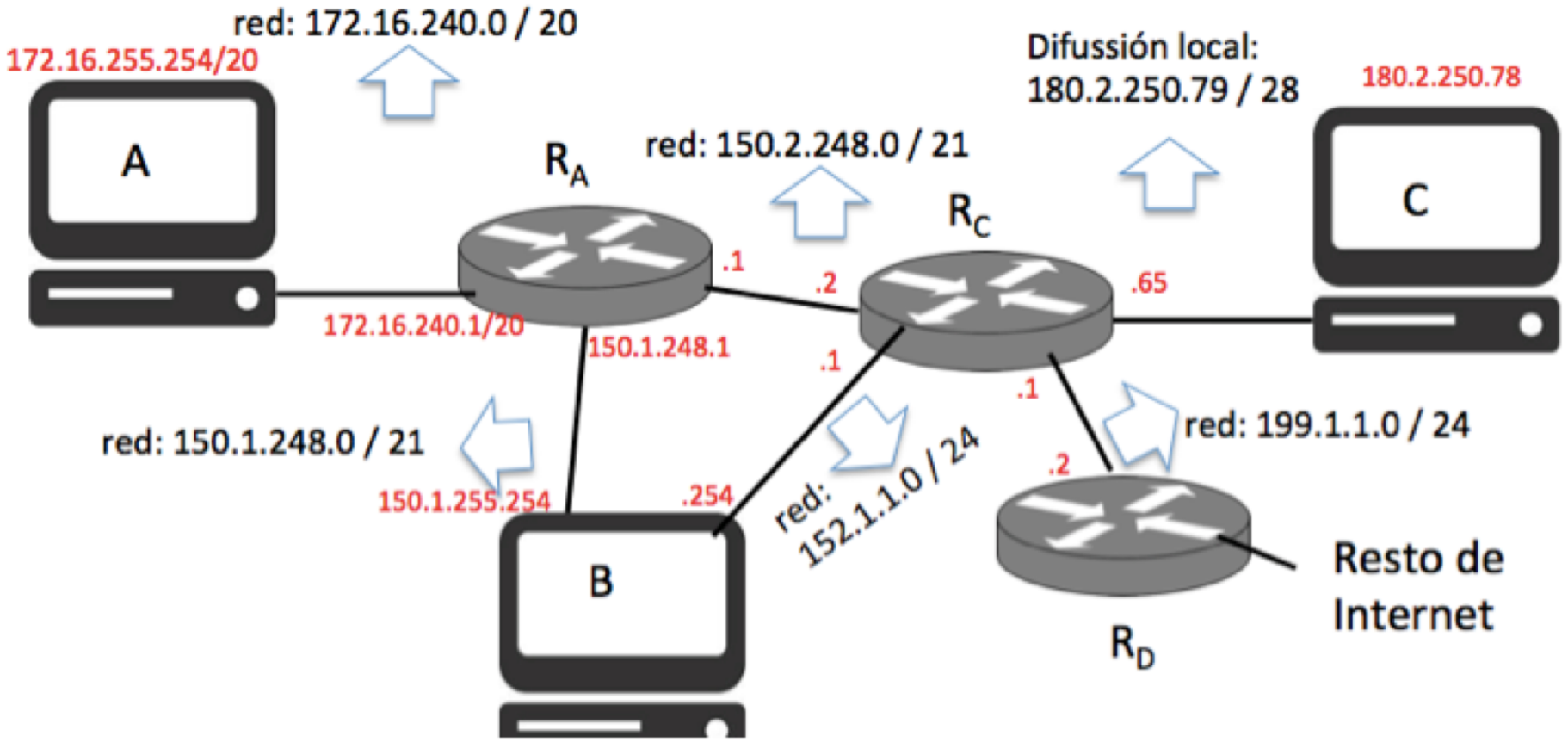
Cuestión	Conceptos relacionados
Direccionamiento en una red	• Direcciones CIDR (máscara) • Direcciones Especiales (red, difusión local)
Tablas NAT	• Rango de direcciones privadas • NAT por traducción de puertos en origen • Apertura de puertos en servidores (conf. Manual)
Configuración de tablas de reenvío	• Campos de la tabla de reenvío • Procedimiento de configuración manual (3 pasos)
Selección de filas en tablas de reenvío	• Algoritmo de reenvío IP
Proceso de reenvío	• Algoritmo reenvío IP • Operación ARP • Fragmentación IP • Operación de NAT

Ejercicio 1) Direccionamiento

- En la red de la figura asigne direcciones a los hosts y a los routers. (las más bajas posibles a los routers, y las más altas a los hosts). Tenga en cuenta las pistas que se ofrecen sobre cada red que compone la inter-red.



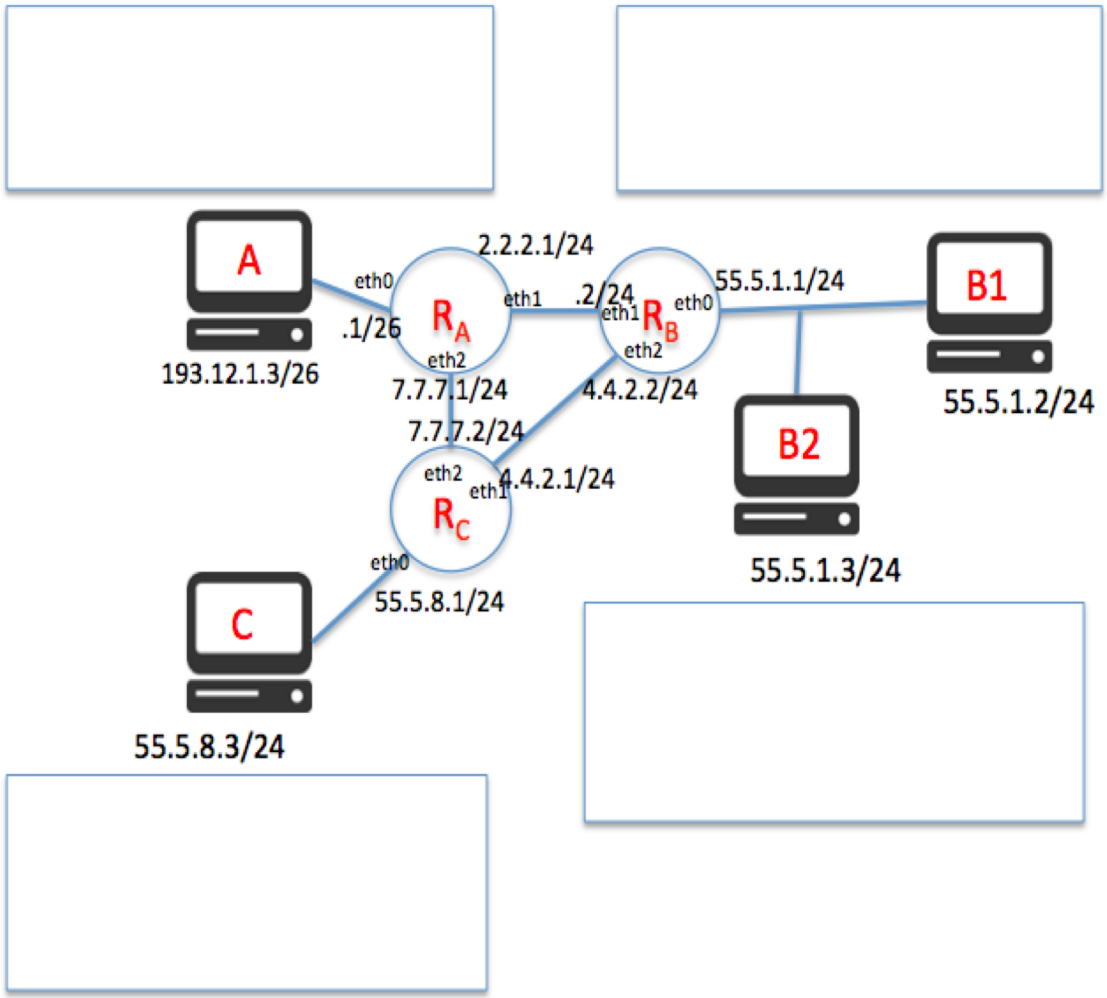
Ejercicio 2): Escriba las tablas de reenvío de Ra,Rc, B



Regla general: menor número de saltos, a igualdad de saltos, siguiente router con menor letra

Otro ejercicio de lo mismo …

- Rellenar las tablas de reenvío cumpliendo



R_A

R_B

R_C

Como norma general:

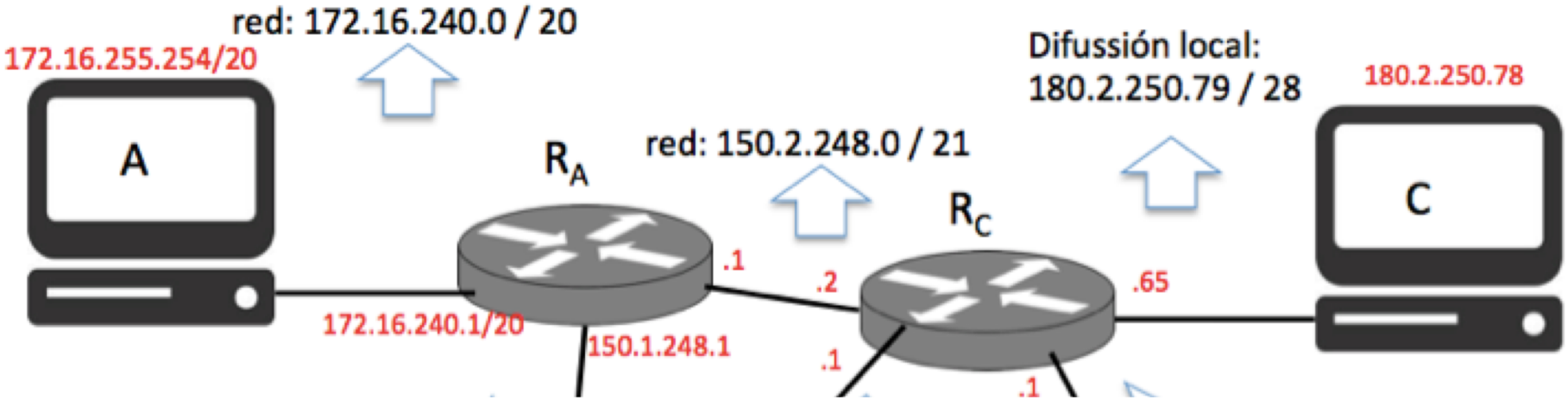
* Los paquetes deben viajar al destino por el menor número de saltos posible. A igualdad de saltos por el nombre menor (p.ej. A < B < C).
* Las tablas de reenvío deben tener el menor número de filas posible.

Condicionantes específicos:

* Los datagramas que genera el equipo A con destino a la red de los equipos B pasan por el Router C.
* Todos los datagramas que recibe el Router C con destino a la red del equipo A son tirados por el Router C.
* Todos los datagramas que genera el equipo B2 con destino B1 son enviados al Router B.

Ejercicio 3): tabla NAT y tabla de sockets

- El equipo A ejecuta un servidor Web, un cliente web y dos clientes DNS
- El equipo C ejecuta un servidor DNS y un cliente web.

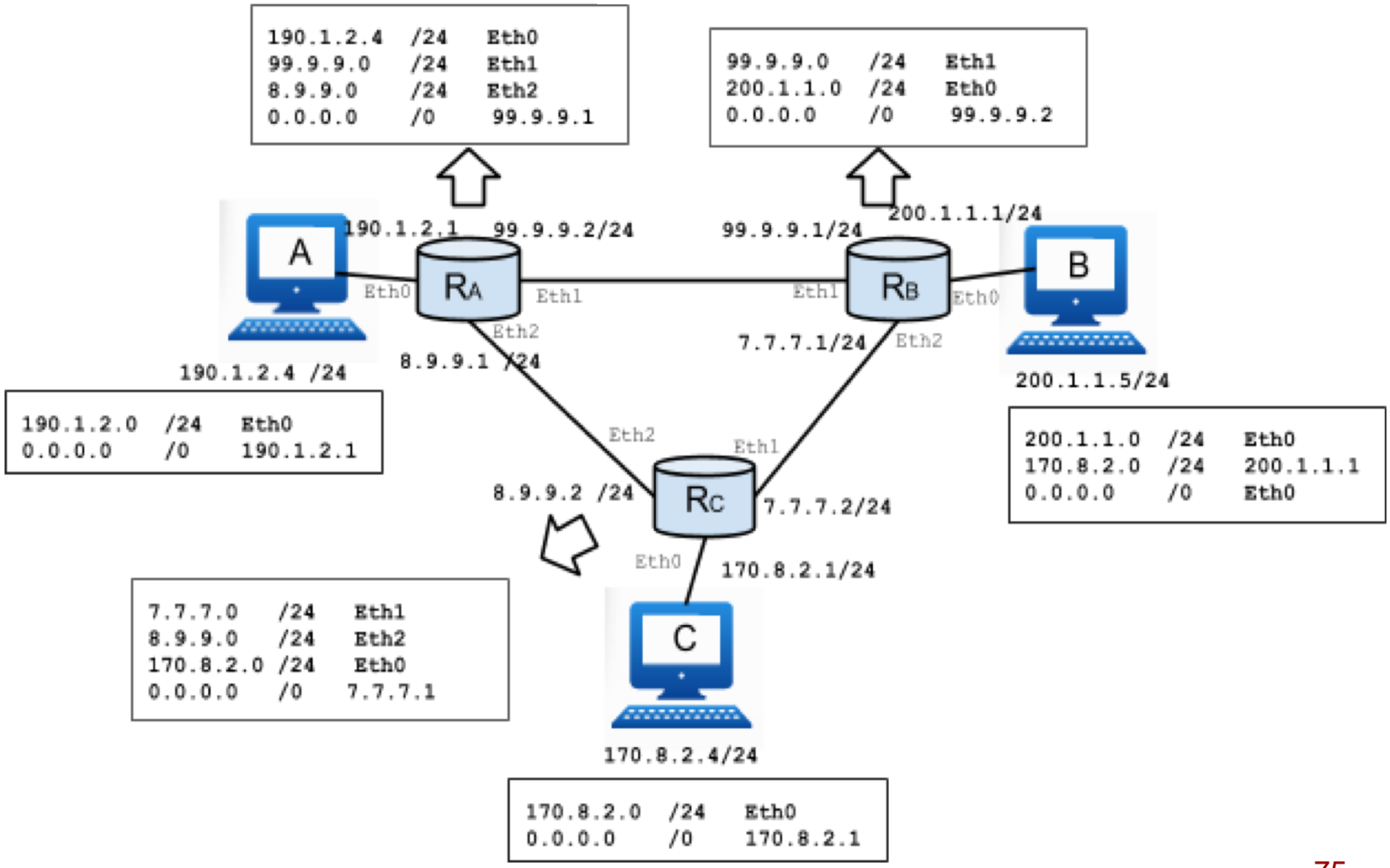


Ejercicio 4): algoritmo de reenvío

- Cada host crea un datagrama destinado a otro. ¿llegará?

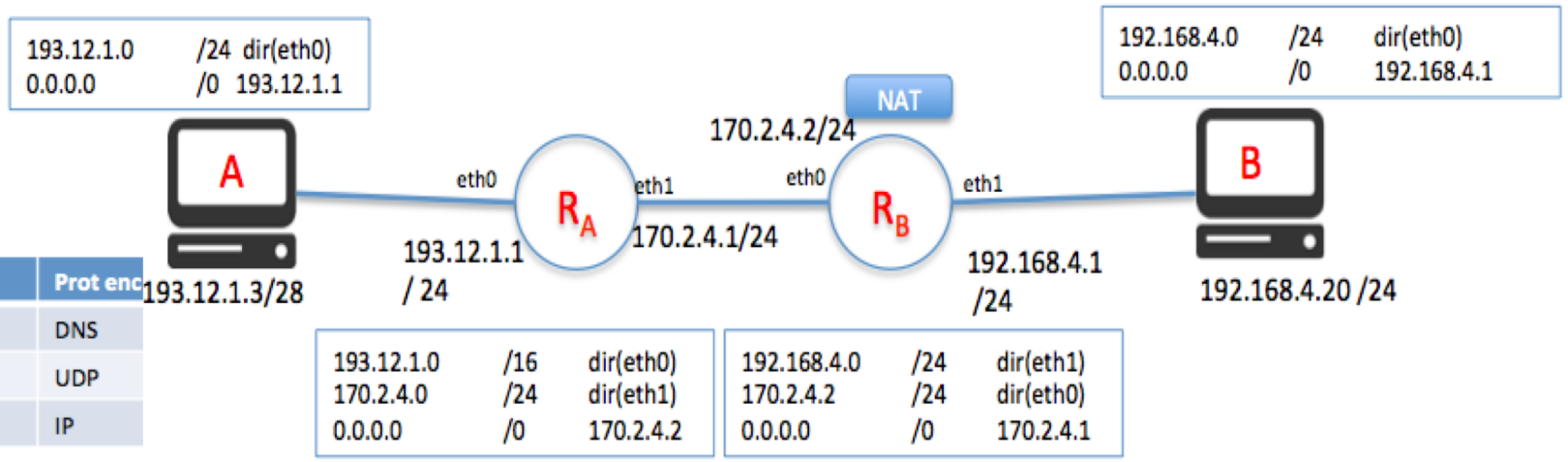
)rigen -> destino	Camino seguido?	Llega al destino?	Motivo (en caso de que no llegue)
A →B			
A →C			
B →A			
B →C			
C →A			
C →B			

-El datagrama llega a su destino por el camino A-Ra-Rc-Rb-B
-El Rc no encuentra ninguna fila válida y tira el datagrama;
-El datagrama se quedaría en un bucle entre Rc y Rb
-El Rc haría una petición arp(12.3.1.3) por su interfaz Eth0 pero nadie respondería



Ejercicio 5): proceso completo de reenvío

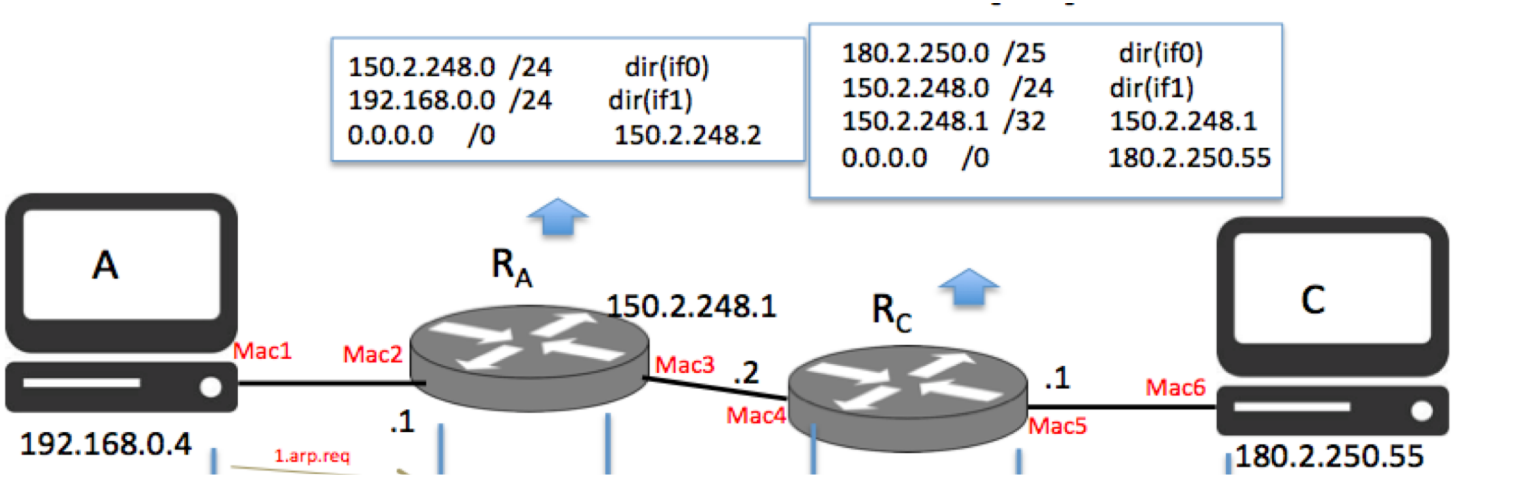
- En los ordenadores recién arrancados A y B se ejecutan un cliente y servidor web. Suponiendo las tablas de reenvío indicadas en la figura, y que R_B tiene abierto el puerto 80 (reenvía el puerto 80 público al puerto 80 de B), se pide:
  - Dibujar un diagrama de envío de tramas por cada enlace (desde que A envía la solicitud de conexión TCP hasta que recibe la respuesta (segmento SYN+ACK) (o hasta donde sea posible (máximo 12 tramas).
  - Para cada trama dibujada en el diagrama, las direcciones origen y destino y los protocolos encapsulados. Escriba direcciones MAC simbólicas en el propio dibujo para todos los equipos.



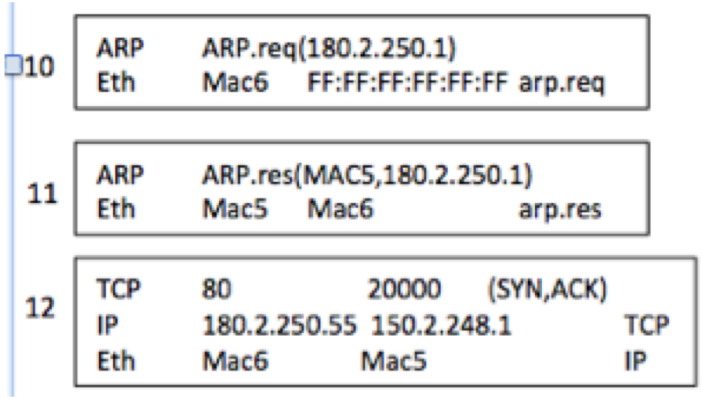
3	Orig	Dest	Prot enc
L4	52.500	53	DNS
L3	10.0.255.251	53.2.4.2	UDP
L2	MAC1	MA2	IP

Otro ejercicio de lo mismo …

- En el escenario (suponiendo que los equipos A y C tienen sus tablas de reenvío correctamente configuradas).

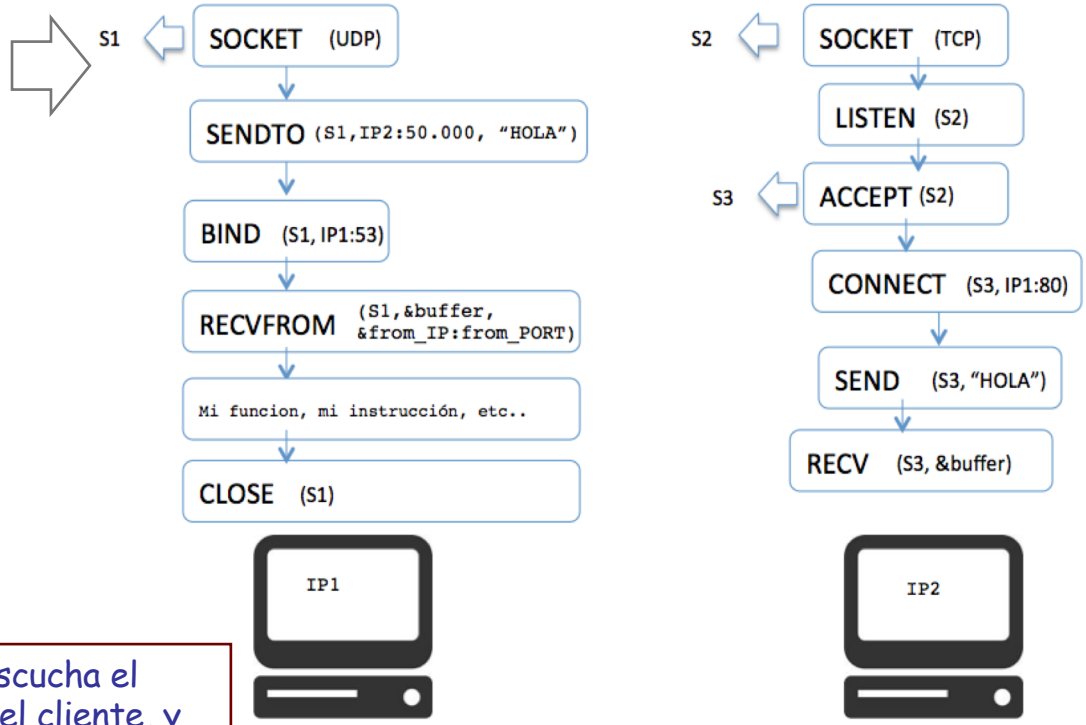


- Dibujar las tramas e indicar la información correpondiente



Ejercicio 6): prácticas (diagramas)

- Dibuje un diagrama con las funciones de sockets.
- Tome como ejemplos



cliente

El **cliente** se ejecuta en un equipo con la dirección IP1. El cliente envía un mensaje al puerto 4.000/udp del servidor. Dicho mensaje es simplemente un número entero (p.ej. el "55000"). A continuación, el cliente se pone a escuchar peticiones de conexión en el puerto cuyo número coincide con el enviado en el mensaje. Cuando le llega una petición de conexión la acepta y lee el mensaje recibido. Después cierra todos sus sockets

servidor

El **servidor**, escucha el mensaje udp del cliente, y solicita una conexión tcp con el cliente al mismo puerto que el recibido en el mensaje. Después de establecer la conexión le envía el mensaje "Hola". Después cierra todos sus sockets