

Protocolos de Interconexión de Redes

Tema 01. Arquitectura TCP/IP



Luis Sánchez González

DPTO. DE INGENIERÍA DE COMUNICACIONES

Este tema se publica bajo Licencia:

[Creative Commons BY-NC-SA 3.0](https://creativecommons.org/licenses/by-nc-sa/3.0/)

Contenido

- Introducción
- Protocolo de resolución de direcciones
- Capa de Inter-red

Contenido

- Introducción
 - Motivaciones
 - Estructura de Internet
 - Gestión de Internet
 - Modelo TCP/IP
- Protocolo de resolución de direcciones
- Capa de Inter-red

Motivaciones

- Hoy:
 - Interconexión de redes = Internet = TCP/IP
- Orígenes:
 - Red de interconexión de redes de comando y control
 - Robusta e invulnerable a un ataque nuclear

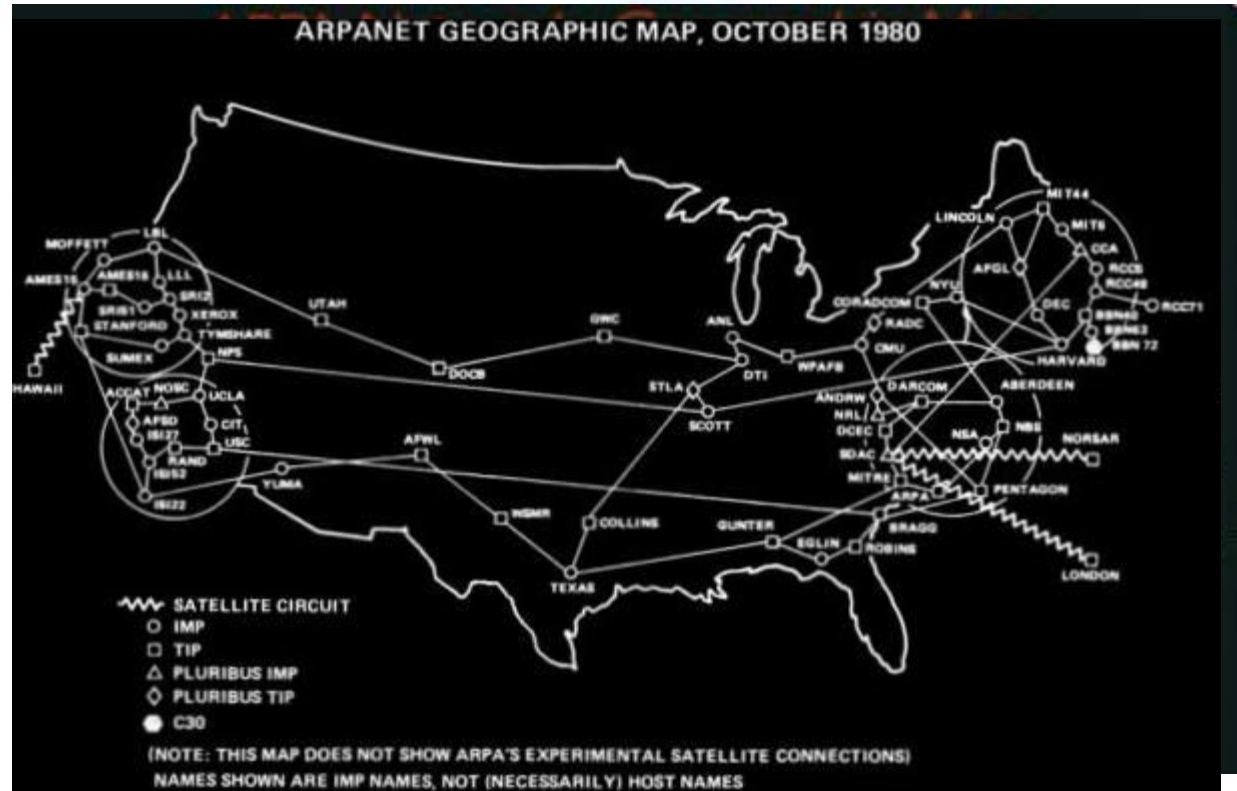
Internet: Evolución

1969

1971

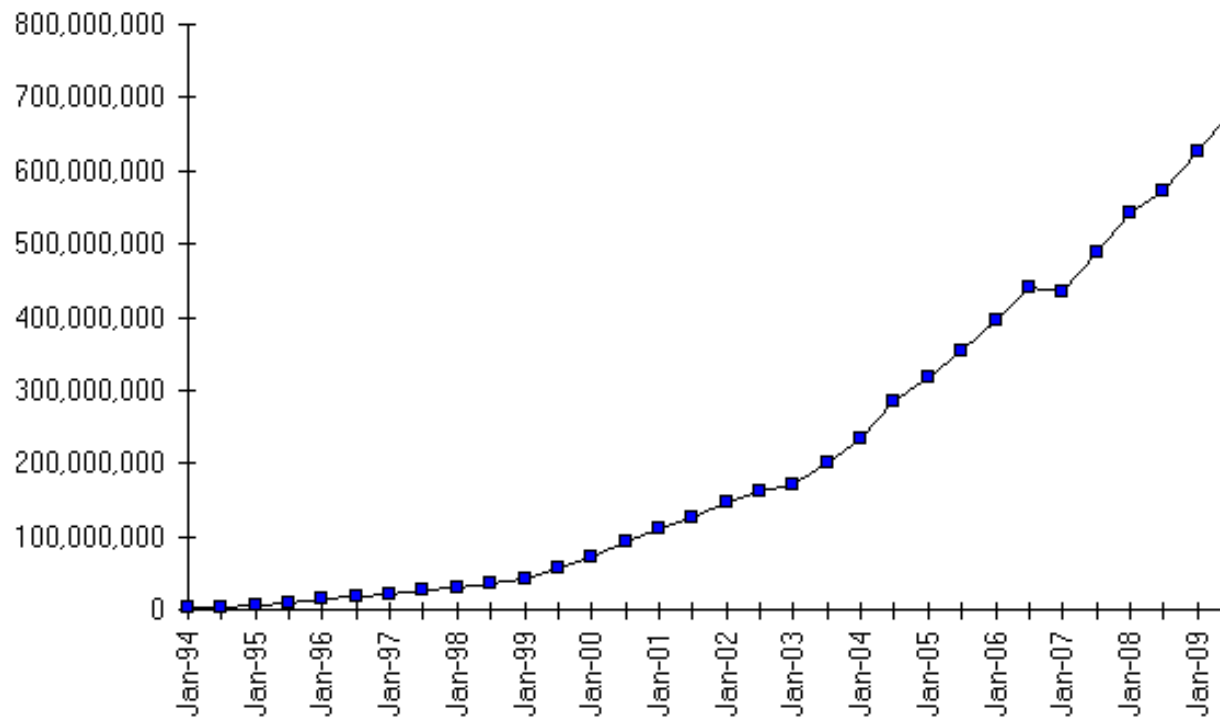
1973

1980



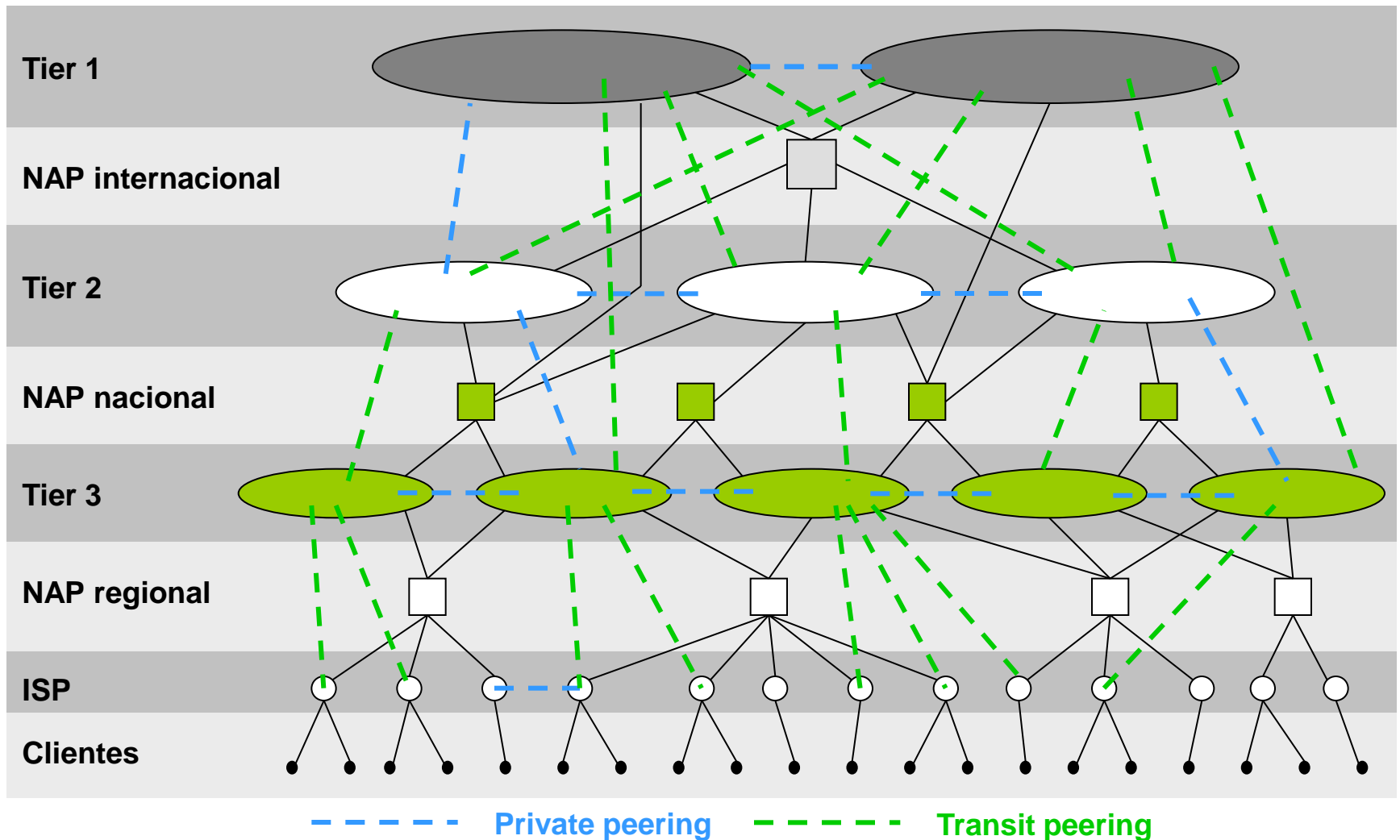
Hasta el infinito y más allá ...

Internet Domain Survey Host Count



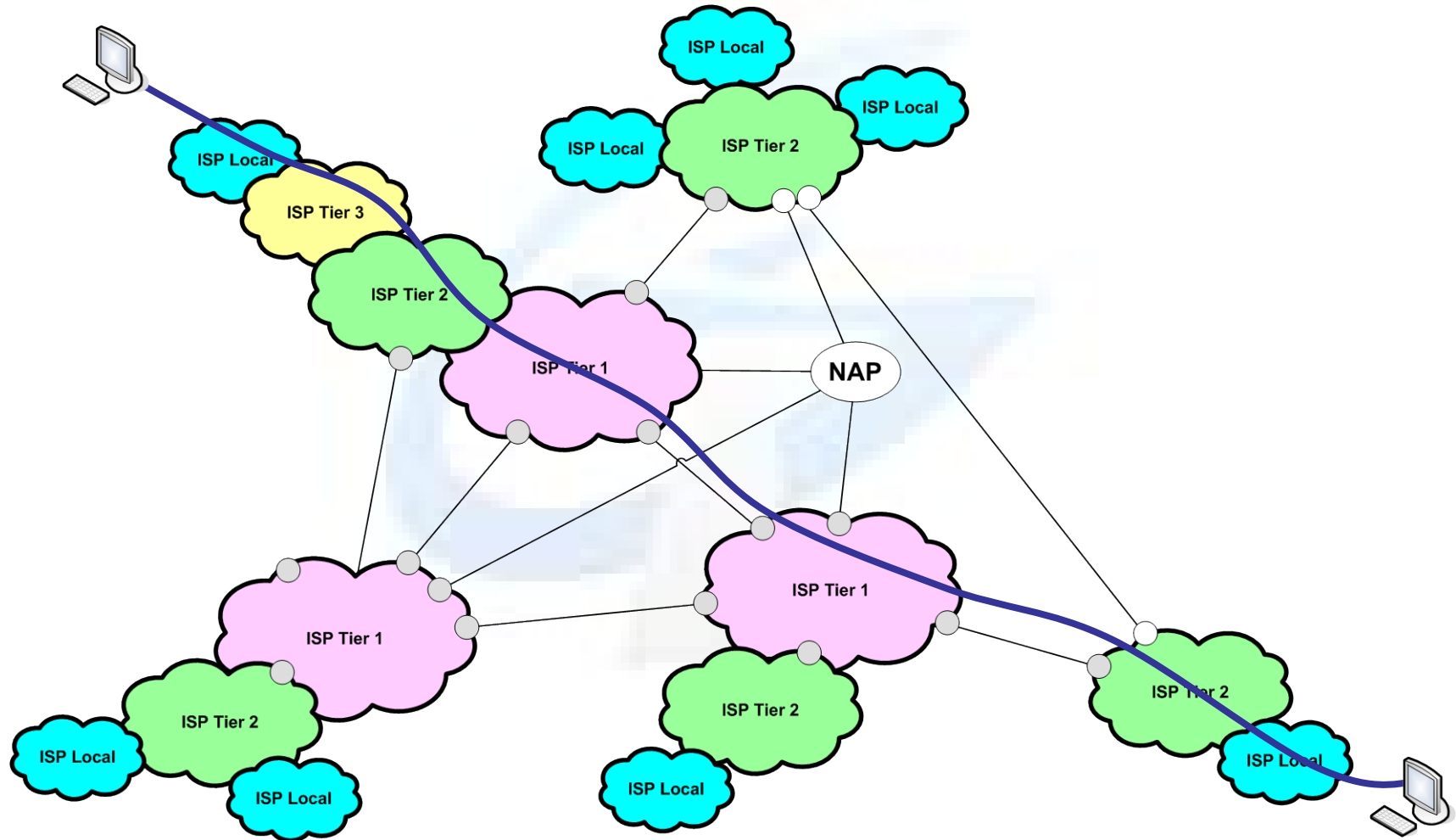
Source: Internet Systems Consortium (www.isc.org)

Internet: Estructura

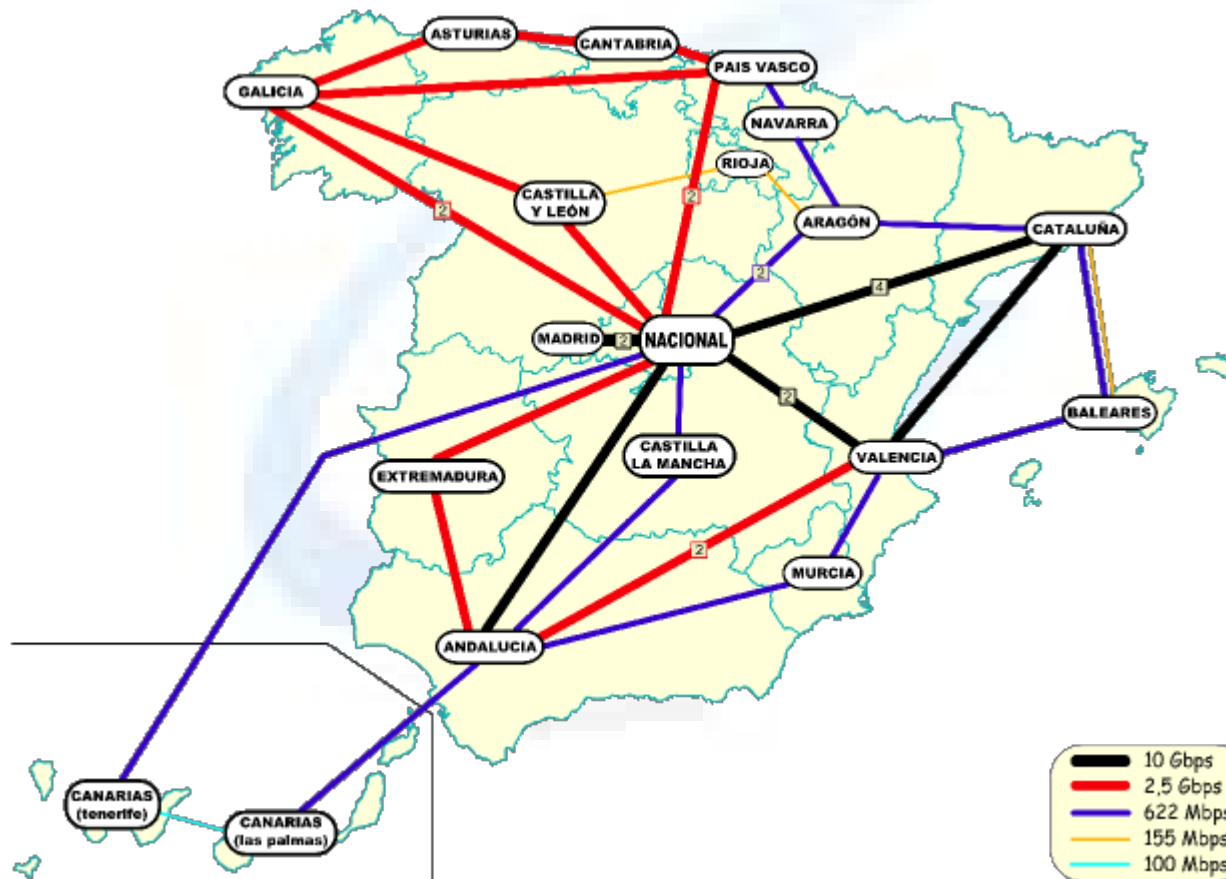


Protocolos para Interconexión de Redes

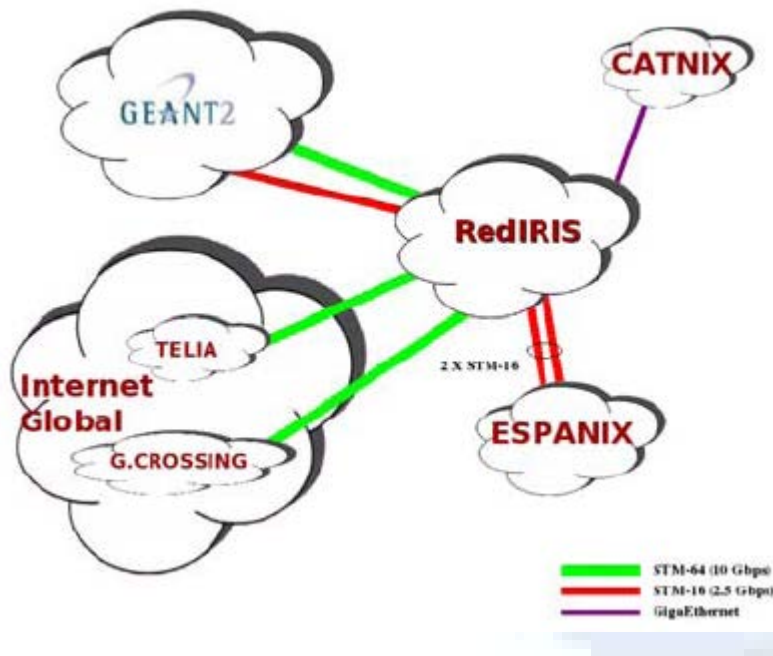
Internet Estructura



España: Ejemplo ISP – Red Iris



España: Ejemplo ISP – Red Iris



```
C:\Users\luis>tracert www.google.com
```

```
Traza a la dirección www.l.google.com [209.85.227.105]
sobre un máximo de 30 saltos:
```

```
 1  <1 ms    <1 ms    <1 ms    192.168.1.1
 2  1 ms     1 ms     1 ms     193.144.201.1
 3  1 ms     <1 ms    <1 ms     172.20.1.25
 4  1 ms     <1 ms    <1 ms     172.20.1.9
 5  2 ms     1 ms     1 ms     172.20.3.9
 6  2 ms     1 ms     1 ms     unican-router.red.rediris.es [130.206.199.22]
 7  2 ms     1 ms     1 ms     ge0-3-0.eb-santander0.red.rediris.es [130.206.199.211]
 8  5 ms     4 ms     4 ms     cab.so5-0-0.eb-bilbao0.red.rediris.es [130.206.250.93]
 9  17 ms    16 ms    17 ms    pav.as0-0.eb-iris4.red.rediris.es [130.206.250.51]
10  17 ms    16 ms    16 ms    mad-b1-link.telia.net [213.248.81.25]
11  41 ms    40 ms    39 ms    prs-bb2-link.telia.net [80.91.254.134]
12  47 ms    46 ms    46 ms    ldn-bb2-link.telia.net [80.91.254.210]
13  49 ms    49 ms    49 ms    ldn-b3-link.telia.net [80.91.254.17]
14  49 ms    48 ms    48 ms    google-ic-126258-ldn-b3.c.telia.net [213.248.67.66]
15  48 ms    48 ms    48 ms    64.233.175.27
16  54 ms    53 ms    53 ms    66.249.95.170
17  52 ms    51 ms    50 ms    72.14.236.191
18  53 ms    53 ms    54 ms    209.85.243.101
19  51 ms    51 ms    51 ms    wy-in-f105.google.com [209.85.227.105]
```

```
Traza completa.
```

Organismos de gestión de Internet

- Necesarios para evitar el aislamiento de redes en islas homogéneas



Internet: ISOC



- **Organización no gubernamental y sin ánimo de lucro dedicada al mantenimiento y mejora de Internet**
- **Desarrolla nuevos estándares y protocolos a través de sus comités**

- IAB - Internet Architecture Board <http://www.iab.org>
- IETF - Internet Engineering Task Force [<http://www.ietf.org>](http://www.ietf.org)
 - Evolución de arquitectura de Internet y su funcionamiento
 - “Comunidad abierta de diseñadores de red, operadores, fabricantes e investigadores y cualquier interesado”
 - RFCs
- IESG - Internet Engineering Steering Group
[<http://www.ietf.org/iesg.html>](http://www.ietf.org/iesg.html)
 - Dirección técnica de la IETF
- IRTF - Internet Research Task Force [<http://www.irtf.org>](http://www.irtf.org)
 - Investigación para la evolución de Internet

[<http://www.isoc.org>](http://www.isoc.org)

Internet: IANA y W3C

- <<http://www.iana.org>>
 - Asignación de valores para protocolos Internet
 - Gestión de direcciones IP
 - Dominios de primer nivel de DNS (Top Level Domains)
 - Números de puertos según protocolo
 - Juegos de caracteres
- <<http://www.w3.org>>
 - Investiga, propone y define temas y protocolos
 - Referencia y coordinación en evolución e interoperabilidad del Web
 - Produce:
 - Especificaciones
 - Código de referencia
 - Prototipos demostradores



Factores del éxito de TCP/IP

- Sistema de direccionamiento integrado
 - Independiente del medio físico
 - Escalable
 - Gestionado centralizadamente
- Diseñado para el enrutamiento
 - Enfocado a la interconexión de redes más que a la interconexión de dispositivos
- Independiente de la tecnología subyacente
- Escalable
 - Núcleo de la tecnología ha soportado el crecimiento exponencial
- Universal
 - Todos lo usan porque todos lo usan

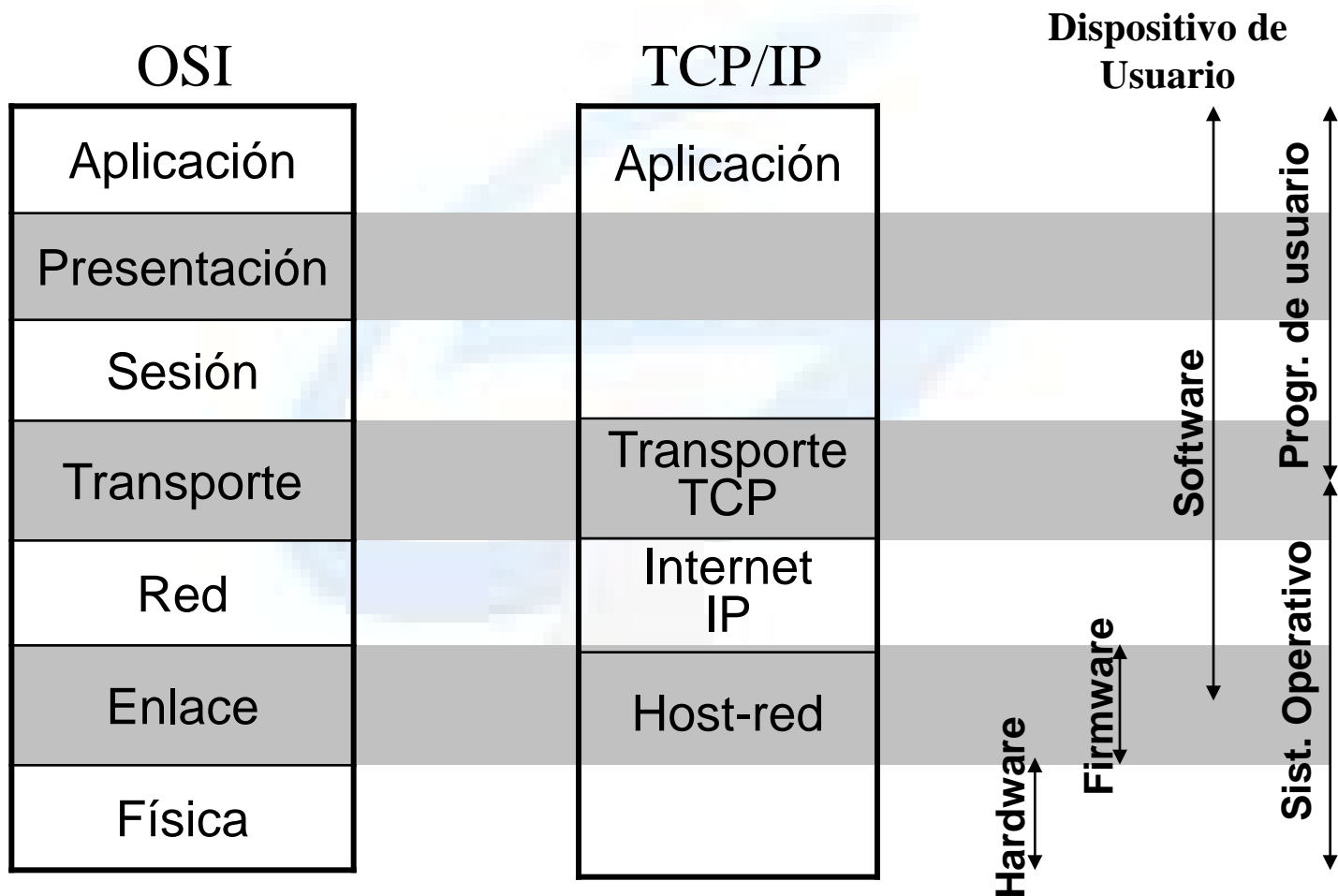
Las claves de la tecnología TCP/IP

- Basada en normas aceptadas por fabricantes y usuarios
 - Generadas en foros de expertos técnicos
 - Centros de investigación depuran la tecnología
 - Mercado absorbe con rapidez las innovaciones útiles
- La innovación no tiene propietarios
- El ciclo de innovación es muy corto
- Hasta la fecha mas de 3000 RFC: éxitos y fracasos. El mercado manda.

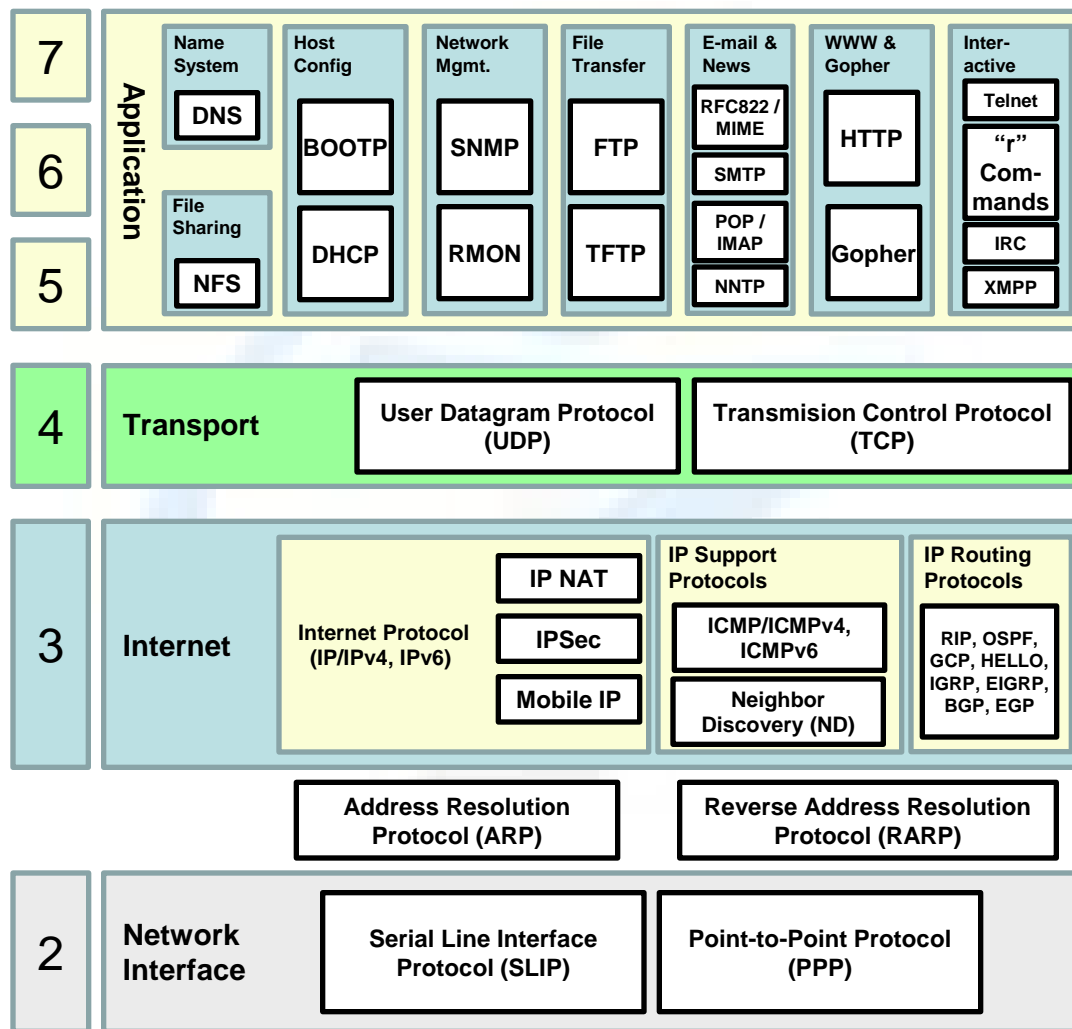
Modelos TCP/IP e híbrido

- Los protocolos TCP/IP nacieron por la necesidad de interconectar redes diversas (internetworking).
- El modelo TCP/IP se diseñó después de los protocolos (puede decirse que primero se hizo el traje y después los patrones).
- Por eso, a diferencia de OSI en el modelo TCP/IP hay unos protocolos 'predefinidos'.
- A menudo, se sigue un modelo híbrido, siguiendo el de OSI en las capas bajas (1 y 2) y el de TCP/IP en las altas (3 y 4). Además en LANs el nivel de enlace suele dividirse en dos subcapas. Esto da lugar a lo que denominamos el modelo híbrido.

Comparación de modelos OSI y TCP/IP



Protocolos TCP/IP



Protocolos para Interconexión de Redes

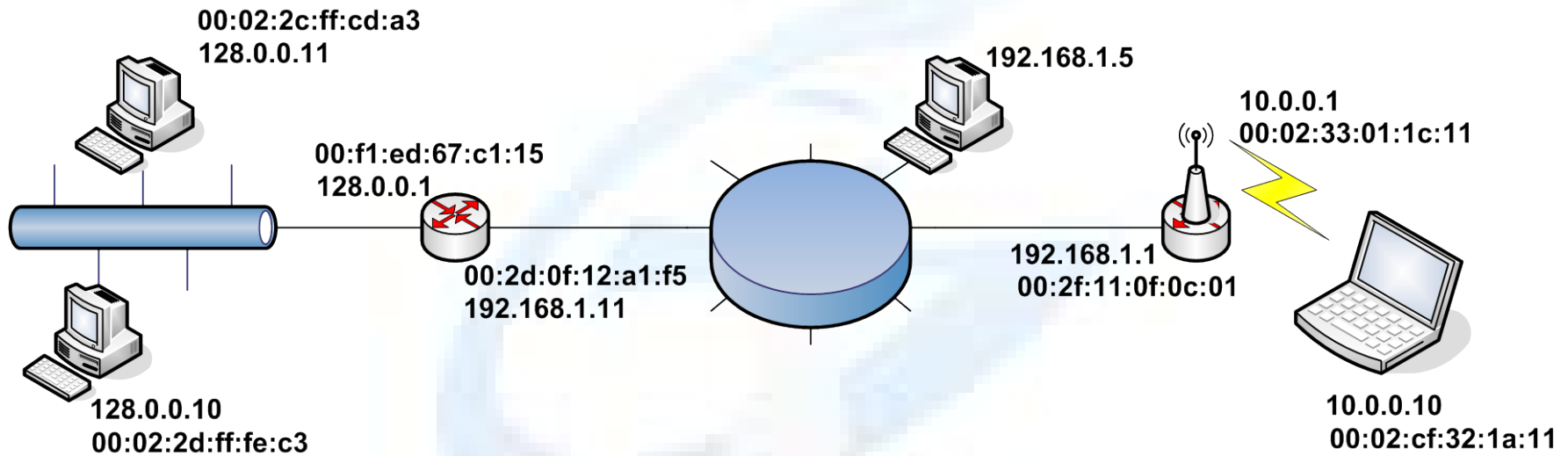
Contenido

- Introducción
- Protocolo de resolución de direcciones
 - Resolución de direcciones
 - Protocolo ARP
 - Protocolo RARP
- Capa de Inter-red

Resolución de direcciones

- En TCP/IP cada host tiene una dirección IP de 32 bits. ENVIA/RECIBE paquetes de/a esa dirección.
 - Dirección de nivel 3
- Las tarjetas de conexión a red tienen una dirección física única, determinada por un número correspondiente al fabricante y a esa tarjeta en concreto.
 - Dirección de nivel 2

Resolución de direcciones



- La cuestión que se plantea es “cómo obtener la dirección física de una máquina cuando se conoce su dirección IP”. Problema de asociación de direcciones.

Resolución de direcciones: Mapeo directo

- Usa un algoritmo para mapear una dirección IP en una dirección física
 - Ej: Usar el último byte de la dirección IP como dirección física
- Ventajas
 - La operación de mapeo es simple, rápida y no genera tráfico en la red.
- Inconvenientes:
 - Sólo es posible si el administrador tiene poder de decisión tanto sobre las direcciones IP, como sobre la dirección física.
 - No ofrece flexibilidad
 - A veces es imposible hacer el mapeo:
 - Las direcciones Ethernet son de 48 bits mientras que las direcciones IP son de 32 bits.
 - Las direcciones físicas en Ethernet II están preasignadas

Resolución de direcciones: Tabla de *Lookup*

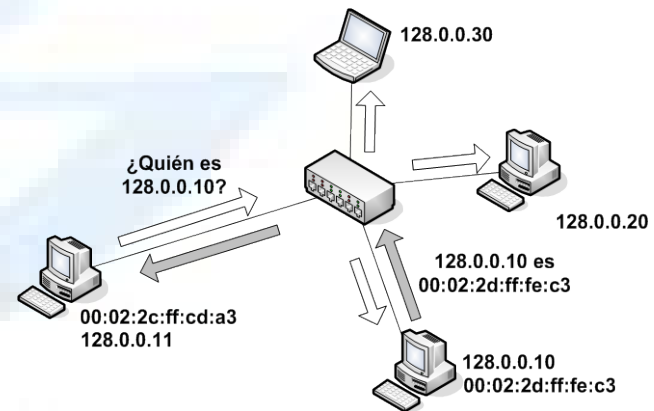
- Mediante búsqueda o indexado se obtiene la dirección MAC
 - Problema: cambio de la tarjeta de red => cambia la tabla



IP Address	MAC Address
197.15.3.1	0A:4B:00:00:07:08
197.15.3.2	0B:4B:00:00:07:00
197.15.3.3	0A:5B:00:01:01:03

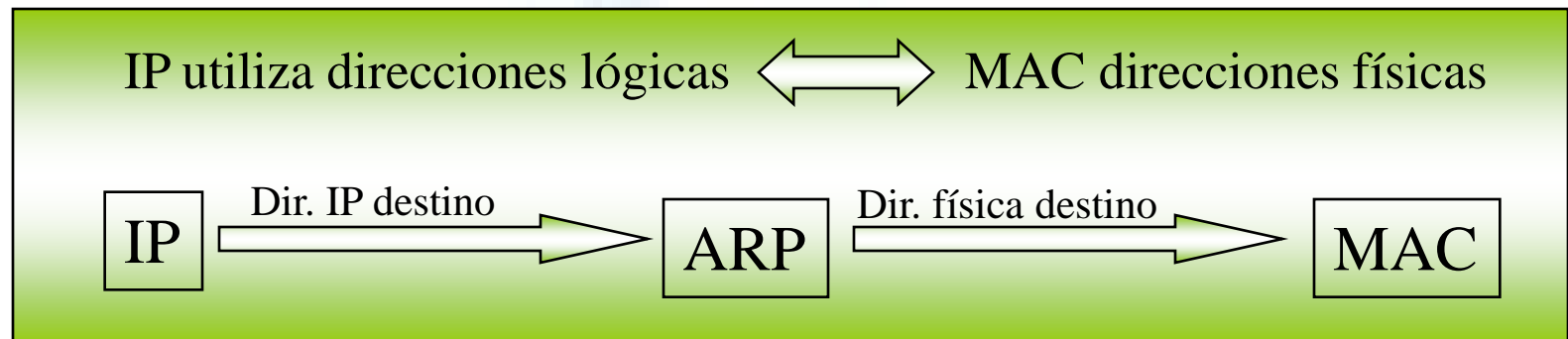
Resolución de direcciones: Resolución Dinámica

- Preguntar a todos en la red quien tiene una determinada dirección IP

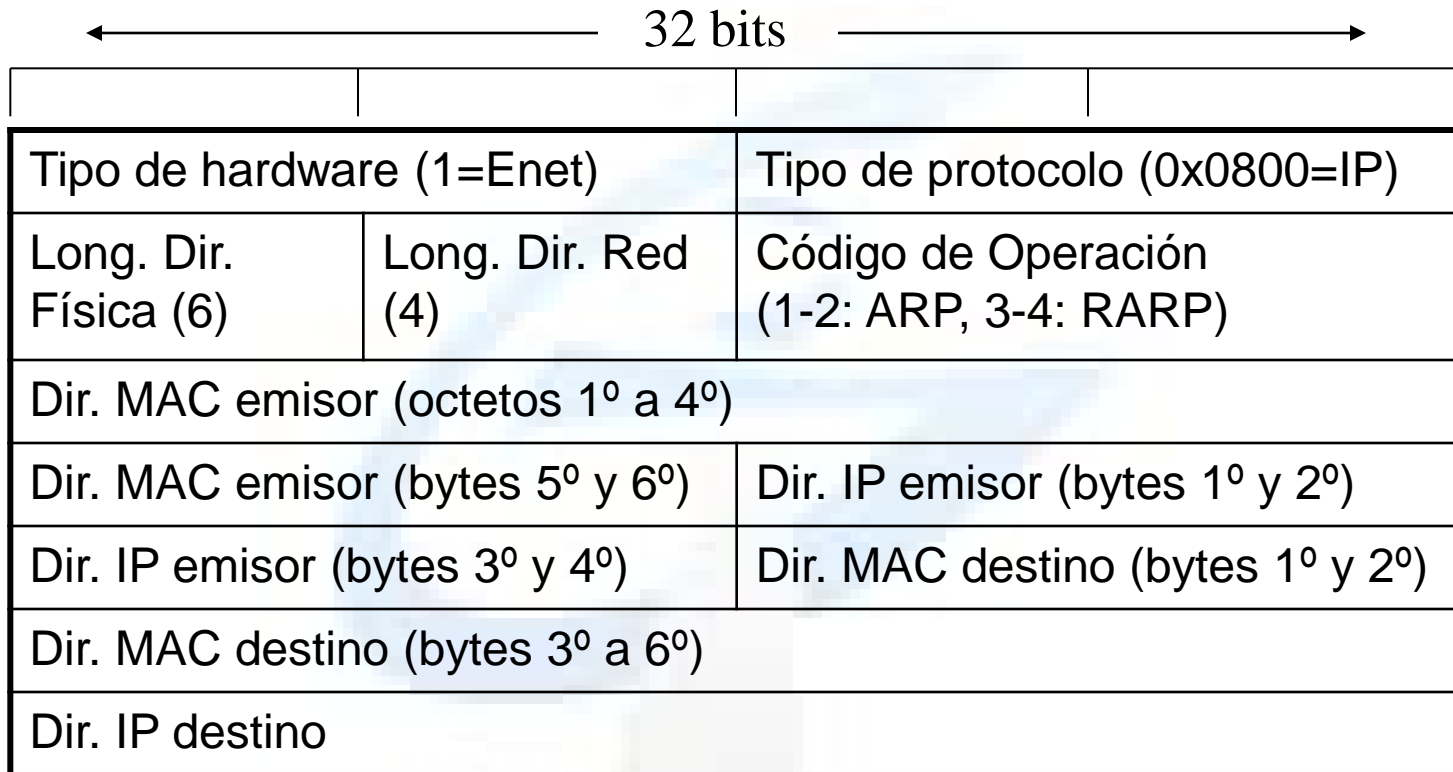


- Los tres métodos son válidos en las redes TCP/IP

Protocolo de Resolución de Direcciones (ARP)

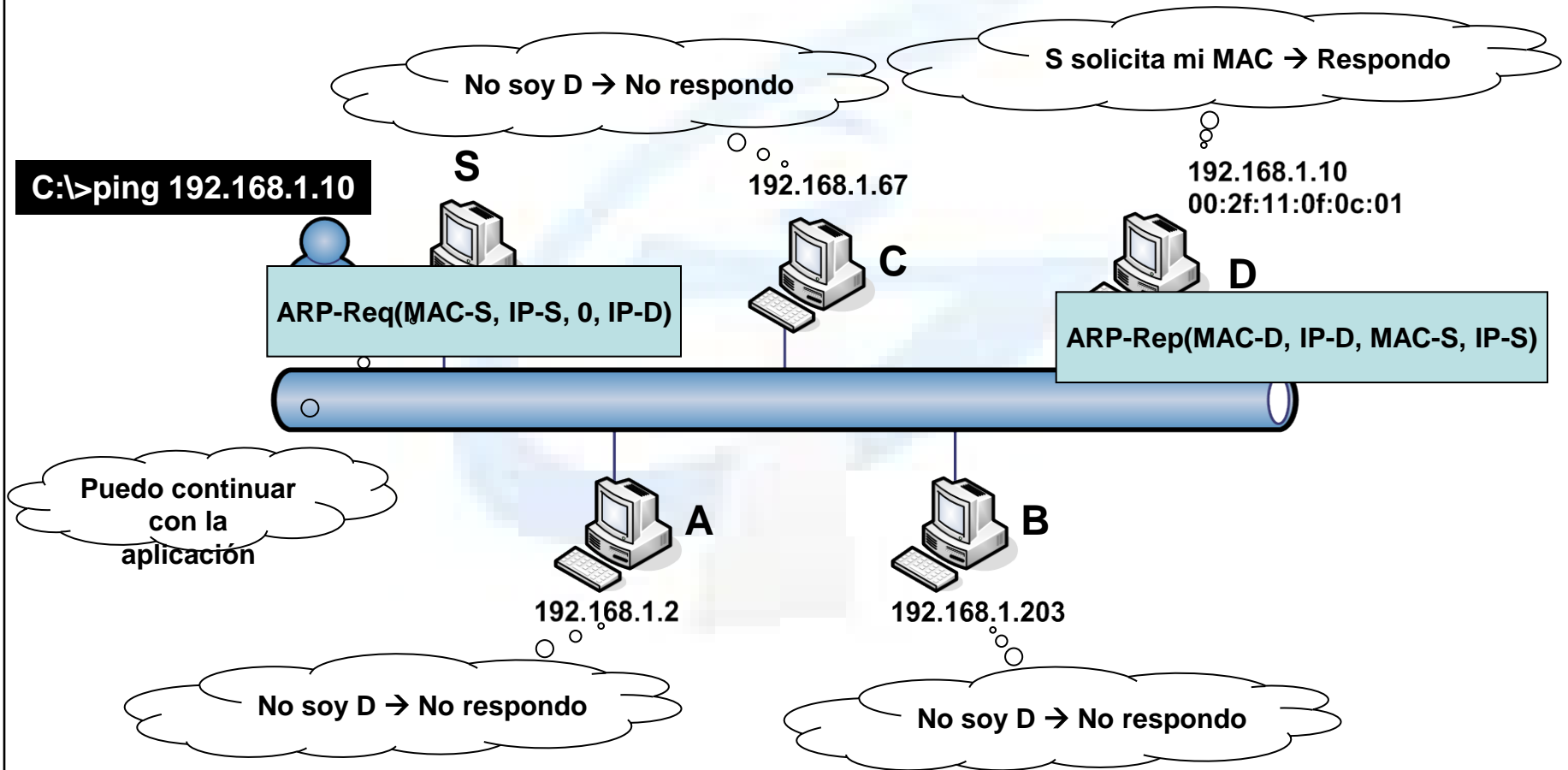


Formato de la trama ARP



- ARP es soportado por múltiples protocolos de capa 2 y 3
- 1=Request, 2=Response
- Los mensajes ARP son enviados directamente por la capa MAC
 - Tipo Ethernet: 0x0806

Modo de operación de ARP



Ejemplo de operación ARP

No. .	Time	Source	Destination	Protocol	Info
211	13.677574	Sony_64:58:81	Broadcast	ARP	who has 192.168.1.2? Tell 192.168.1.103
212	13.678297	HewlettP_f8:2b:e5	Sony_64:58:81	ARP	192.168.1.2 is at 00:11:85:f8:2b:e5

```

[+] Frame 211 (42 bytes on wire, 42 bytes captured)
[-] Ethernet II, Src: Sony_64:58:81 (00:1a:80:64:58:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    [+] Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    [+] Source: Sony_64:58:81 (00:1a:80:64:58:81)
        Type: ARP (0x0806)
[-] Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    [Is gratuitous: False]
    Sender MAC address: Sony_64:58:81 (00:1a:80:64:58:81)
    Sender IP address: 192.168.1.103 (192.168.1.103)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.2 (192.168.1.2)

```

No. .	Time	Source	Destination	Protocol	Info
211	13.677574	Sony_64:58:81	Broadcast	ARP	who has 192.168.1.2? Tell 192.168.1.103
212	13.678297	HewlettP_f8:2b:e5	Sony_64:58:81	ARP	192.168.1.2 is at 00:11:85:f8:2b:e5

```

[+] Frame 212 (60 bytes on wire, 60 bytes captured)
[-] Ethernet II, Src: HewlettP_f8:2b:e5 (00:11:85:f8:2b:e5), Dst: Sony_64:58:81 (00:1a:80:64:58:81)
    [+] Destination: Sony_64:58:81 (00:1a:80:64:58:81)
    [+] Source: HewlettP_f8:2b:e5 (00:11:85:f8:2b:e5)
        Type: ARP (0x0806)
        Trailer: 00000000000000000000000000000000
[-] Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    [Is gratuitous: False]
    Sender MAC address: HewlettP_f8:2b:e5 (00:11:85:f8:2b:e5)
    Sender IP address: 192.168.1.2 (192.168.1.2)
    Target MAC address: Sony_64:58:81 (00:1a:80:64:58:81)
    Target IP address: 192.168.1.103 (192.168.1.103)

```

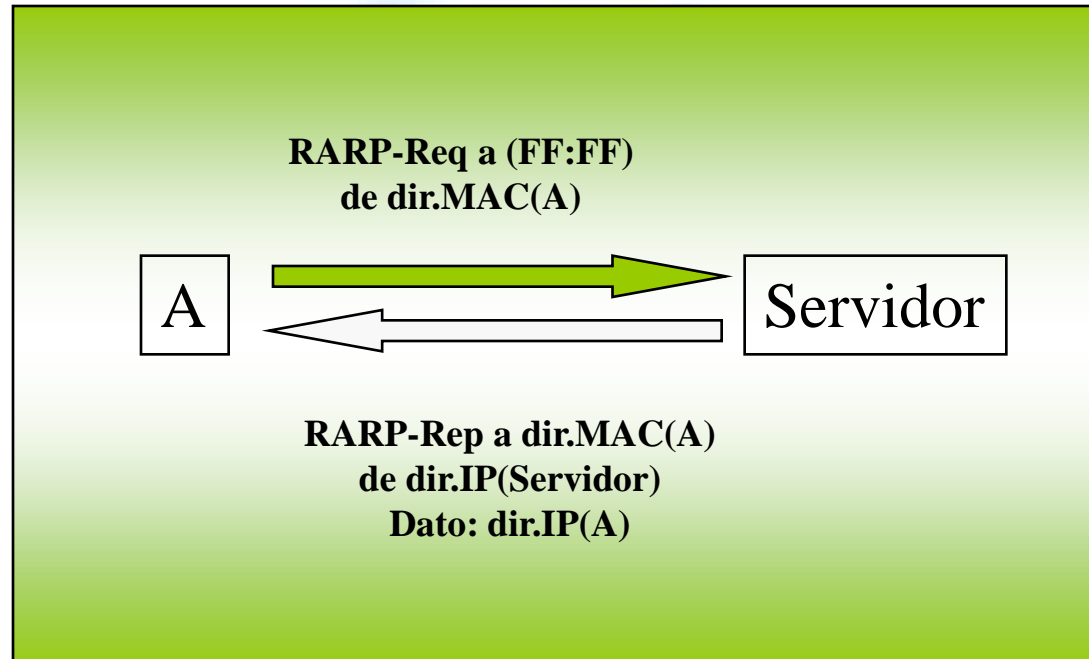
Aspectos de eficiencia en ARP

- **Caché ARP**
 - Las direcciones de los vecinos son introducidas en una tabla por un periodo de tiempo.
 - Principio de localidad
- **Resolución cruzada**
 - Con el ARP-Req D ya conoce la MAC de S → No hace falta lanzar otro proceso ARP
- **Aprovechar la difusión (overhearing)**
 - A, B y C se enteran de la MAC de S simplemente por estar en la red.
- **Proxy ARP**

Protocolo de Resolución Inversa de Direcciones (RARP)

- La dirección IP no forma parte del hardware de un equipo: está almacenada en los ficheros de configuración del sistema operativo.
- Existen terminales sin unidad de disco que obtienen de un servidor de red un kernel para poder arrancar.
- **Problema: ¿Cómo puede una máquina que no cuenta con disco determinar su propia dirección IP?**
- El terminal envía una solicitud al servidor a través de una conexión física de difusión, indicando su propia dirección física y solicitando su dirección IP.
- El problema es el inverso de la asociación de direcciones: protocolo RARP (Reverse ARP).

Protocolo de Resolución Inversa de Direcciones (RARP)



Arquitectura TCP/IP

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	Marquett_12:dd:88	Broadcast	RARP	who is 00:00:a1:12:dd:88? Tell 00:00:a1:12:dd:88

- + Frame 1 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Marquett_12:dd:88 (00:00:a1:12:dd:88), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - + Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - + Source: Marquett_12:dd:88 (00:00:a1:12:dd:88)
 - Type: ARP (0x0806)
 - Trailer: 00000000000000000000000000000000
- Address Resolution Protocol (reverse request)
 - Hardware type: Ethernet (0x0001)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - opcode: reverse request (0x0003)
 - [Is gratuitous: False]
 - Sender MAC address: Marquett_12:dd:88 (00:00:a1:12:dd:88)
 - Sender IP address: 0.0.0.0 (0.0.0.0)
 - Target MAC address: Marquett_12:dd:88 (00:00:a1:12:dd:88)
 - Target IP address: 0.0.0.0 (0.0.0.0)

```

0000  ff ff ff ff ff ff 00 00  a1 12 dd 88 08 06 00 01  .....
0010  08 00 06 04 00 03 00 00  a1 12 dd 88 00 00 00 00  .....
0020  00 00 a1 12 dd 88 00 00  00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00  00 00 00 00  .....

```


Consideraciones del protocolo RARP

- El protocolo RARP utiliza el mismo formato de trama que ARP.
- A diferencia de ARP, la solicitud sólo puede llevarse a cabo en la propia red física donde se encuentra la máquina que pregunta.
- La solicitud RARP puede perderse o corromperse: el propio software RARP deberá solucionar estos problemas.
Comportamientos posibles.
 - Reintentar hasta que un servidor responde.
 - Intentarlo un par de veces y luego avisar del error (evita cargar a la red con tráfico inútil).
- Limitaciones:
 - Orientado únicamente al nivel físico
 - Asignación manual de las direcciones
 - Protocolo limitado. Sólo da la dirección IP del equipo.
- Sustituido por BOOTP y DHCP

Contenido

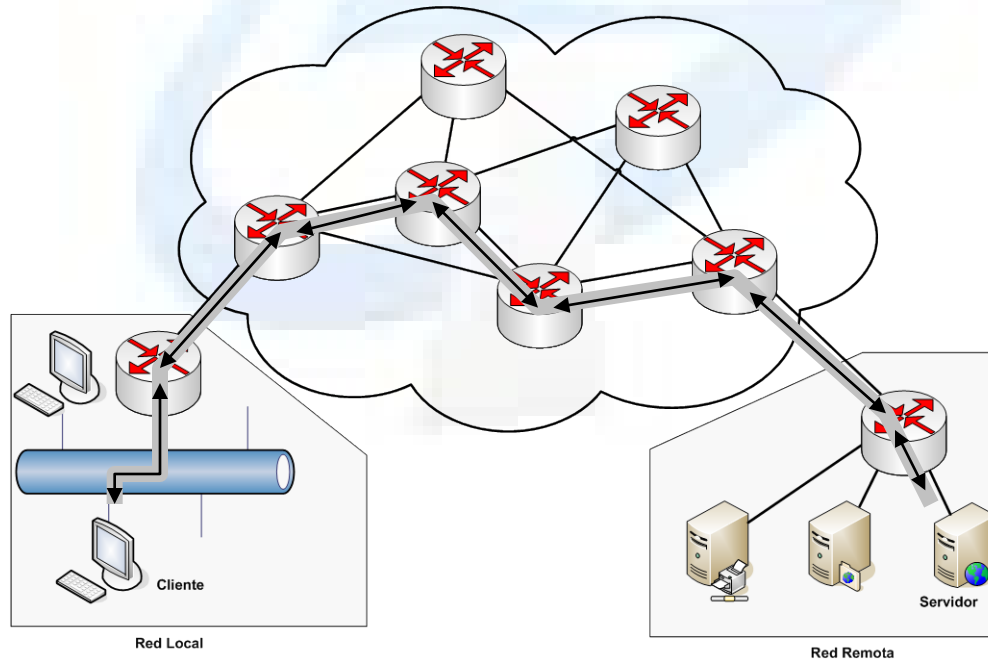
- Introducción
- Capa de acceso a la red
- Protocolo de resolución de direcciones
- **Capa de Inter-red**
 - Introducción a IPv4
 - Estructura del datagrama IPv4
 - Fragmentación
 - Direccionamiento
 - IPv4 Network Address Translation
 - Enrutamiento

IP: Historia

- Internet Protocol (IP) es el protocolo interred usado en la red Internet (definido en RFC 791 – IPv4 –)
 - IPv0 – Marzo 1977
 - IPv1 – Enero 1978
 - IPv2 – Febrero 1978 versión A
 - IPv3 – Febrero 1978 versión B
 - IPv6 – Diciembre 1998 – RFC 2460
- El IPv5 realmente nunca existió
 - Otro protocolo uso ese número y después para evitar problemas se pasó de IPv4 a IPv6.

IP: Características principales

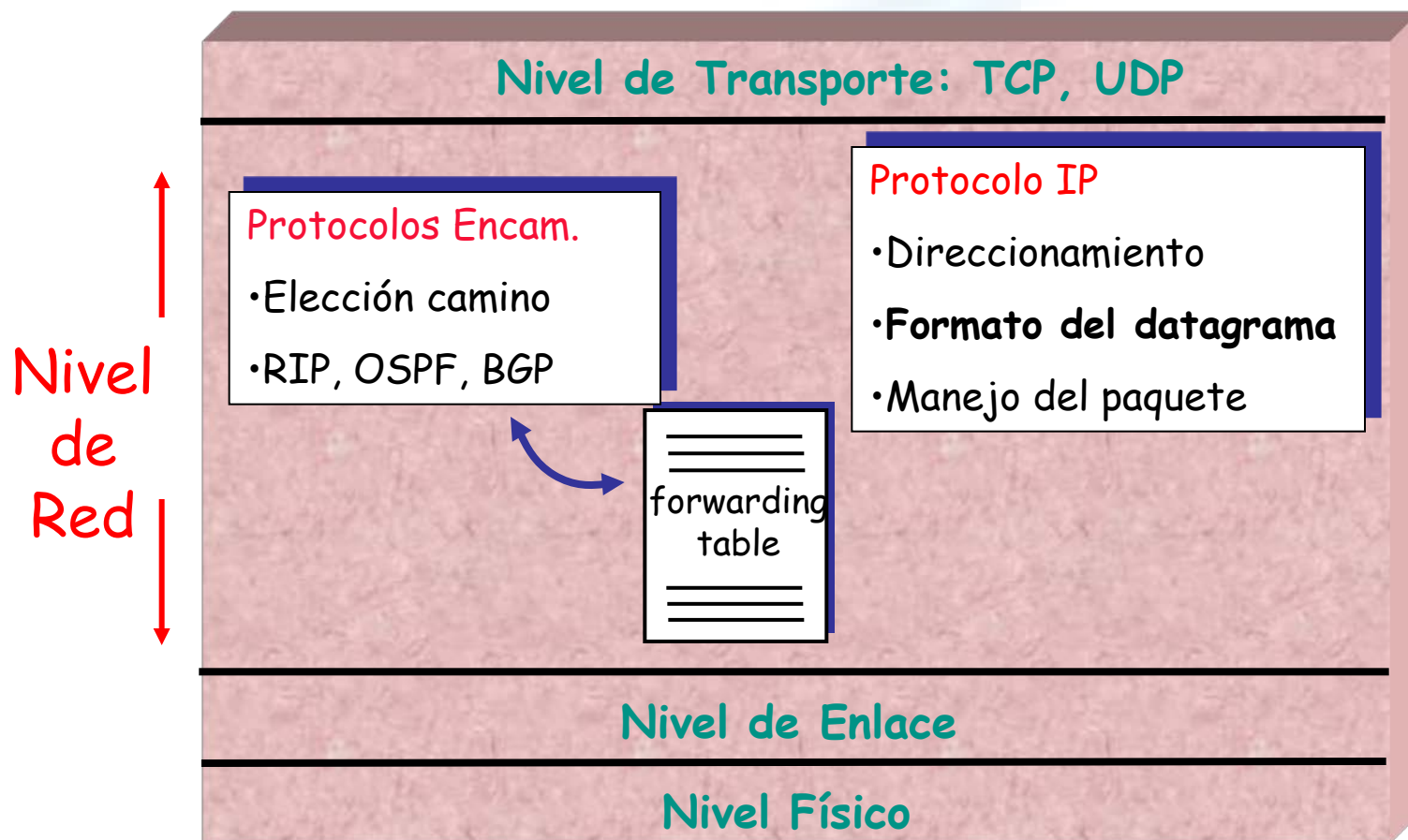
- Direccionamiento universal
- Independiente de la tecnología subyacente
- “Haz lo que puedas” (Best-effort)
 - Entrega no reconocida
 - Entrega no fiable
 - Comunicación sin conexión



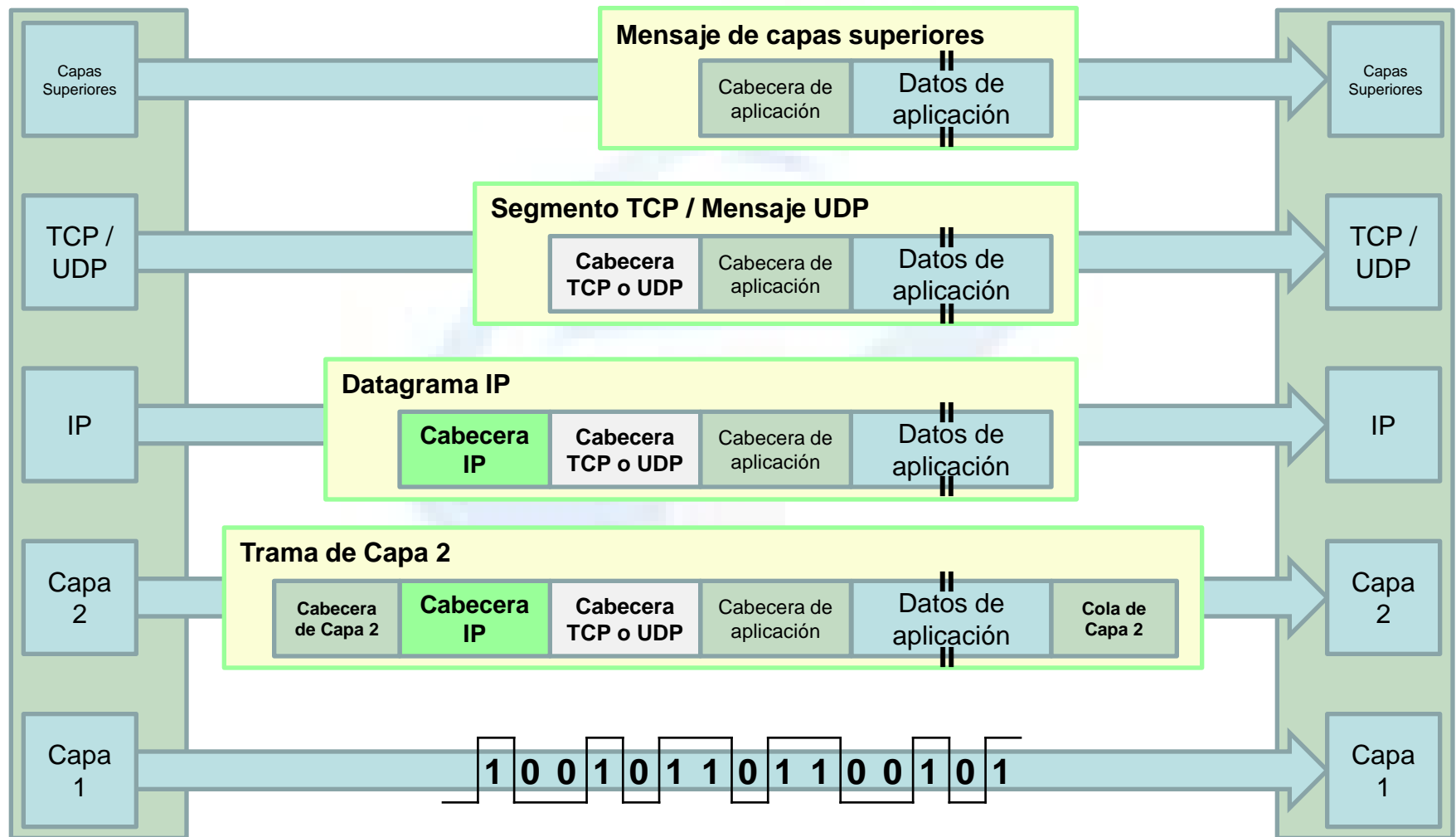
IP: Funcionalidades

- **Direccionamiento**
 - Imprescindible para saber a quien entregar los datagramas
- **Encapsulación y formato del datagrama**
- **Fragmentación y ensamblado**
 - Tamaño del datagrama depende de la MTU de la tecnología subyacente
- **Enrutamiento**
 - A través de “encaminadores” (routers). Una comunicación puede implicar un gran número de saltos

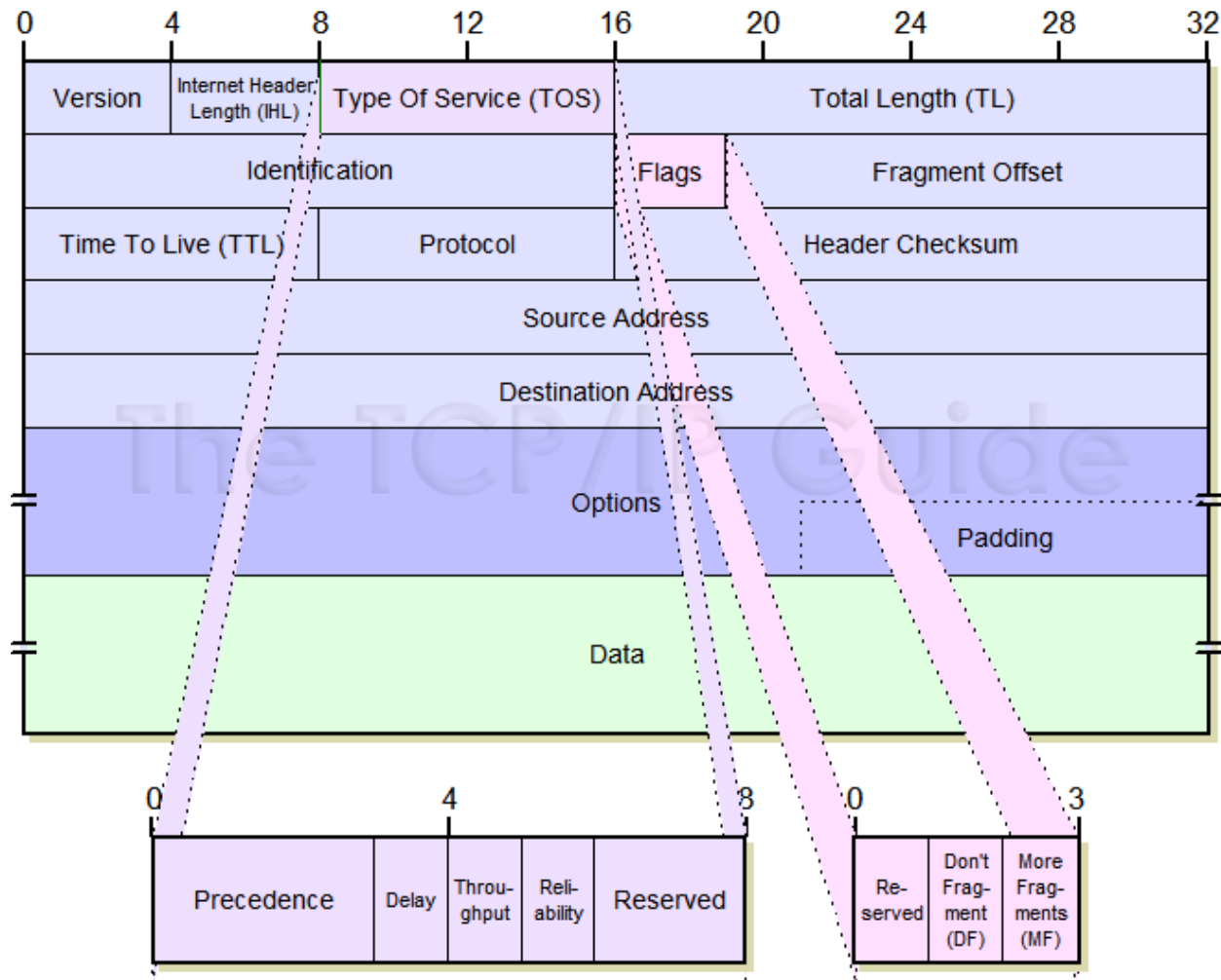
Capa de Interred – Estructura del Datagrama



Encapsulado del Datagrama IP



Estructura del Datagrama IP



Arquitectura TCP/IP

No. .	Time	Source	Destination	Protocol	Info
142	6.065968	192.168.1.103	130.206.5.142	HTTP	GET / HTTP/1.1
143	6.068341	130.206.5.142	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
149	6.200573	192.168.1.103	209.85.227.113	HTTP	GET /__utm.gif?utmwv=4.5.8&utmn=1596523994&utmhn=www.unican.es&utmcs=
151	6.253358	209.85.227.113	192.168.1.103	HTTP	HTTP/1.1 200 OK (GIF89a)
152	6.260896	192.168.1.103	130.206.5.142	HTTP	GET /favicon.ico HTTP/1.1

+ Frame 142 (601 bytes on wire, 601 bytes captured)
 + Ethernet II, Src: Sony_64:58:81 (00:1a:80:64:58:81), Dst: Cisco-Li_28:20:0b (00:1d:7e:28:20:0b)
 + Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 130.206.5.142 (130.206.5.142)

Version: 4
 Header length: 20 bytes
 + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 587
 Identification: 0x71af (29103)
 + Flags: 0x04 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (0x06)
 + Header checksum: 0x3c92 [correct]
 Source: 192.168.1.103 (192.168.1.103)
 Destination: 130.206.5.142 (130.206.5.142)

+ Transmission Control Protocol, Src Port: 49686 (49686), Dst Port: http (80), Seq: 1, Ack: 1, Len: 547
 + Hypertext Transfer Protocol

```

0000  00 1d 7e 28 20 0b 00 1a 80 64 58 81 08 00 45 00  ..~( ... .dx...E.
0010  02 4b 71 af 40 00 80 06 3c 92 c0 a8 01 67 82 ce  .Kq.@... <....g..
0020  05 8e c2 16 00 50 78 04 1d 46 88 e2 dc 41 50 18  ....Px. .F...AP.
0030  40 29 4c a9 00 00 47 45 54 20 2f 20 48 54 54 50  @)L...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: www.
0050  75 6e 69 63 61 6e 2e 65 73 0d 0a 55 73 65 72 2d  unican.e s..User-
0060  41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35  Agent: M ozilla/5
0070  2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20  .0 (wind ows; U;
0080  57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 30 3b 20  windows NT 6.0;
0090  65 6e 2d 47 42 3b 20 72 76 3a 31 2e 39 2e 31 2e  en-GB; r v:1.9.1.
00a0  34 29 20 47 65 63 6b 6f 2f 32 30 30 39 31 30 31  4) Gecko /2009101
00b0  36 20 46 69 72 65 66 6f 78 2f 33 2e 35 2e 34 20  6 Firefo x/3.5.4
00c0  28 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30  (.NET CL R 3.5.30
  
```

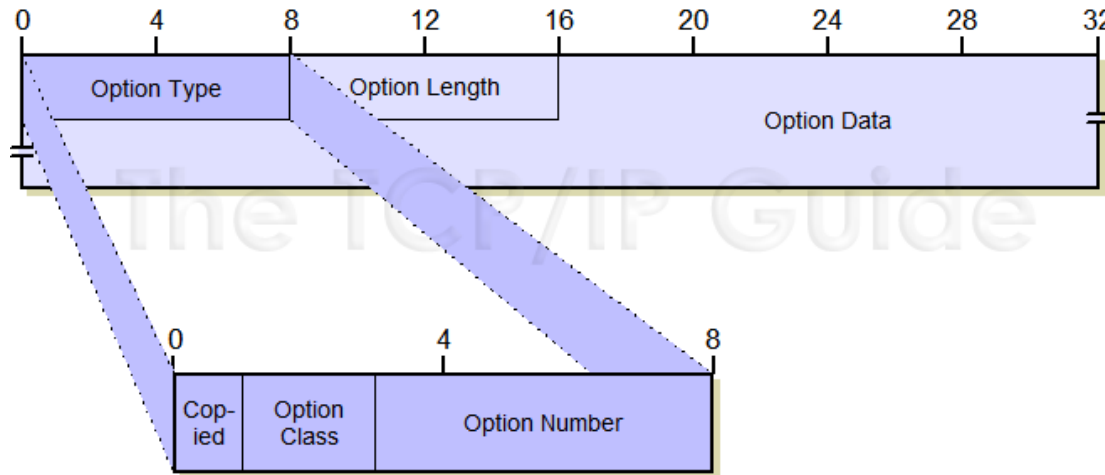
Estructura del Datagrama IP

- **Version:** Identifica la versión de IP
- **IHL:** Especifica la longitud de la cabecera IP. Se expresa como el número de bloques de 32 bits de los que se compone (mínimo es 5)
- **TOS:** Utilizado para soportar Calidad de Servicio (QoS). Priorización de ciertos datagramas. Usados para la estrategia DiffServ
- **TL:** Indica la longitud total del datagrama IP
- **Identification:** Identifica a cada uno de los fragmentos de un mismo datagrama
- **Flags:** 2 de los 3 bits se usan en caso de que exista fragmentación
 - DF: Si va a 1 el datagrama no puede fragmentarse. Si no fuera posible su transmisión, el datagrama se descarta
 - MF: Si va a 1 indica que hay más fragmentos de ese datagrama por llegar.
- **Offset:** Indica la posición en la que los datos de ese fragmento van en el datagrama original en unidades de 8 bytes.

Estructura del Datagrama IP

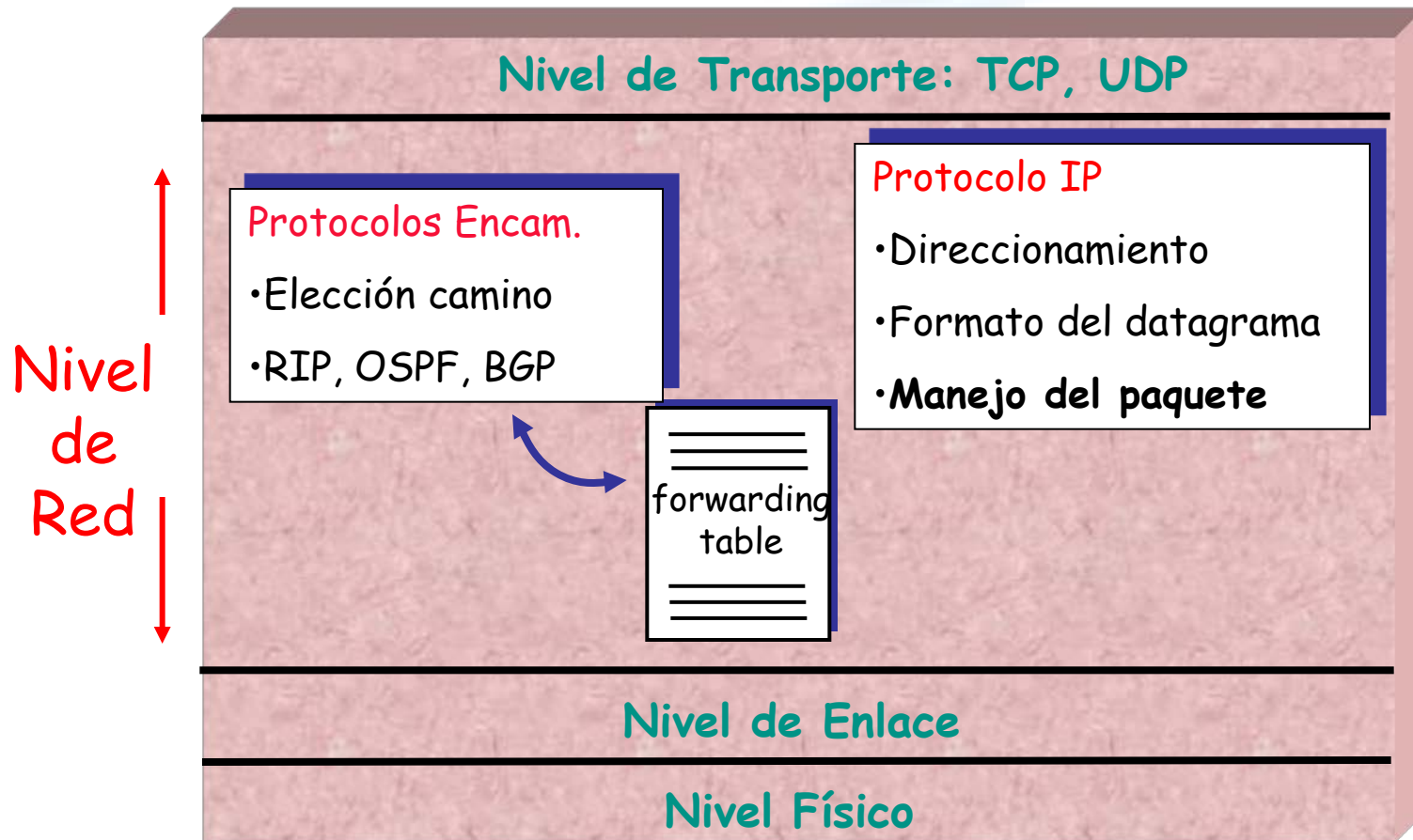
- **TTL:** Indica cual es el número máximo de routers que el datagrama puede atravesar en su camino al destino
- **Protocol:** Identifica al protocolo de nivel superior que viaja en el campo de datos del datagrama IP. (RFC 1700 – IANA)
- **Checksum:** Se trata de un código de verificación que asegura que la cabecera IP no se ha visto corrompida. Se verifica y recalcula en cada salto de la ruta
- **Source y Destination Address:** Son las direcciones IP tanto del dispositivo que ha generado el paquete como del destinatario final de éste
- **Options:** (RFC 791)
- **Padding:** Rellena la cabecera para que su longitud se pueda expresar en bloques de 32 bits
- **Data:** La información de nivel superior

Estructura del Datagrama IP: Opciones



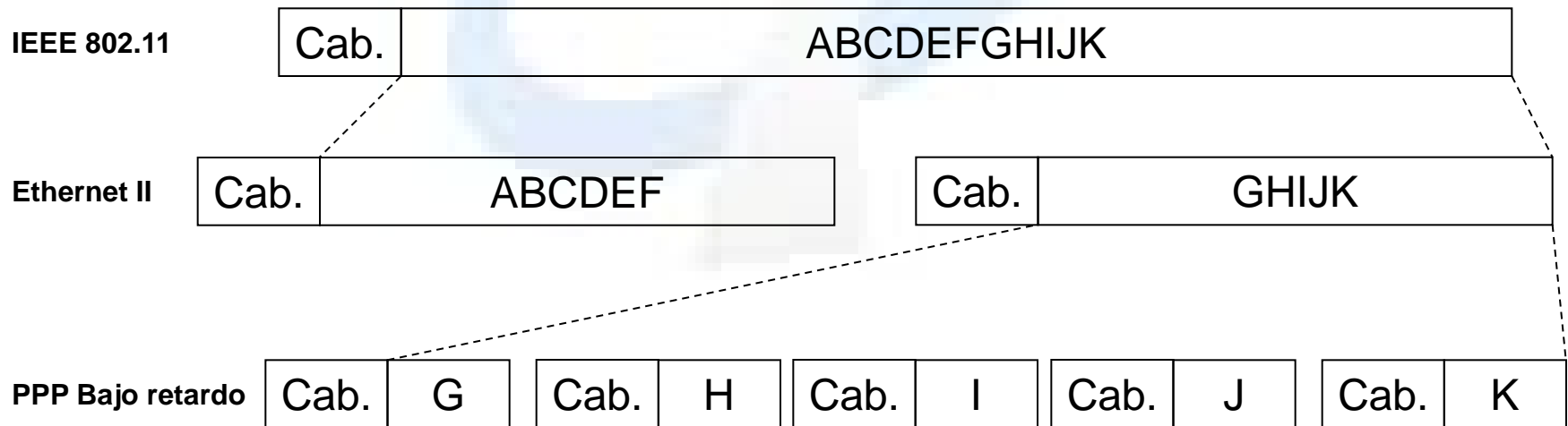
- **Copied Flag:** Indica si tiene que incluirse esta opción en todos los fragmentos del datagrama
- **Option Class:** Especifica uno de las cuatro clases potenciales. En realidad sólo se usan dos de ellas: 0 para opciones de control y 2 para medidas y detección de errores
- **Option Number**

Capa de Interred – Fragmentación



Fragmentación

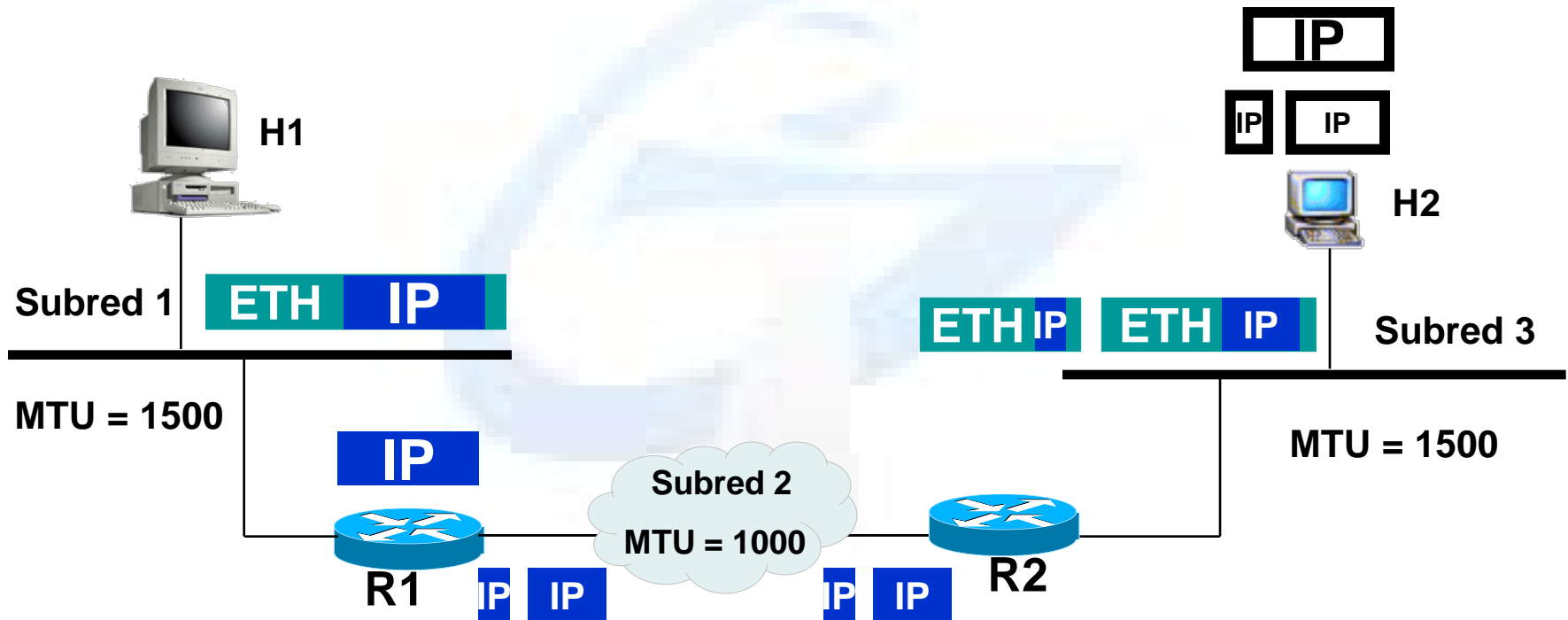
- Cada tipo de red pone un limite a la mayor longitud del tamaño de la trama. No pueden llevar mas datos. Ese limite de la longitud de la trama es lo que se conoce como MTU.



Fragmentación

- El nivel de red ha de acomodar un datagrama en una trama del nivel de enlace.
- Cada tecnología tiene un valor máximo de paquete que puede aceptar, Ej.:
 - Ethernet: 1500 bytes (Ethernet II), 1492 (LLC-SNAP).
 - Token Ring: 4440 bytes (4 Mb/s).
- Este valor es la MTU (Maximum Transfer Unit).
- Si el datagrama no cabe se ha de fragmentar. Ej: datagrama de más de 1500 bytes creado en red Token Ring que pasa a Ethernet.
- También puede que el host genere datagramas demasiado grandes, ej: NFS, 8 KB.

Fragmentación IP



Fragmentación IP

- Los fragmentos reciben la misma cabecera que el datagrama original salvo por los campos 'MF' y 'Desplazamiento del Fragmento' (Offset).
- Los fragmentos de un mismo datagrama se identifican por el campo 'Identificación'.
- Todos los fragmentos, menos el último, tienen a 1 el bit MF (More Fragments).
- La unidad básica de fragmentación es 8 bytes. Los datos se reparten en tantos fragmentos como haga falta, todos múltiplos de 8 bytes (salvo quizá el último).
- Toda red debe aceptar un MTU de al menos 68 bytes (60 de cabecera y 8 de datos). Recomendado 576 bytes

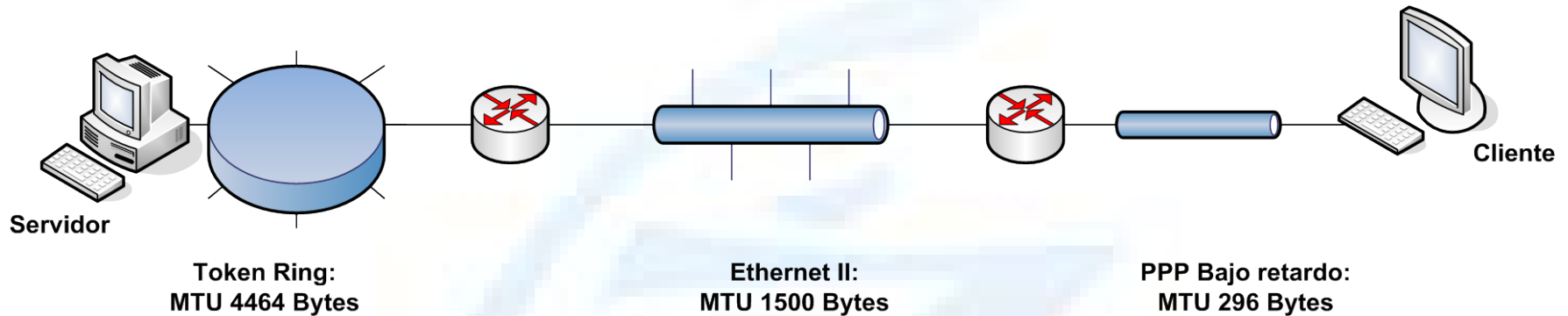
Fragmentación IP

- Cuando un host no está capacitado para reensamblar (ej.: estaciones 'diskless').
- Se aplica la técnica de 'Path MTU discovery'
 - Enviar datagrama con DF=1 y MTU máxima
 - Si no pasa, probar con MTU menor
- Generalmente si se rechaza el mensaje de error indica la MTU máxima que se aceptaría.

PROBLEMA 1: *Un datagrama IP con Payload de 452 bytes va a ser transmitido desde un PC a través de su bus Ethernet (MTU=1500B) para salir a través de una línea serie (MTU=280B)*

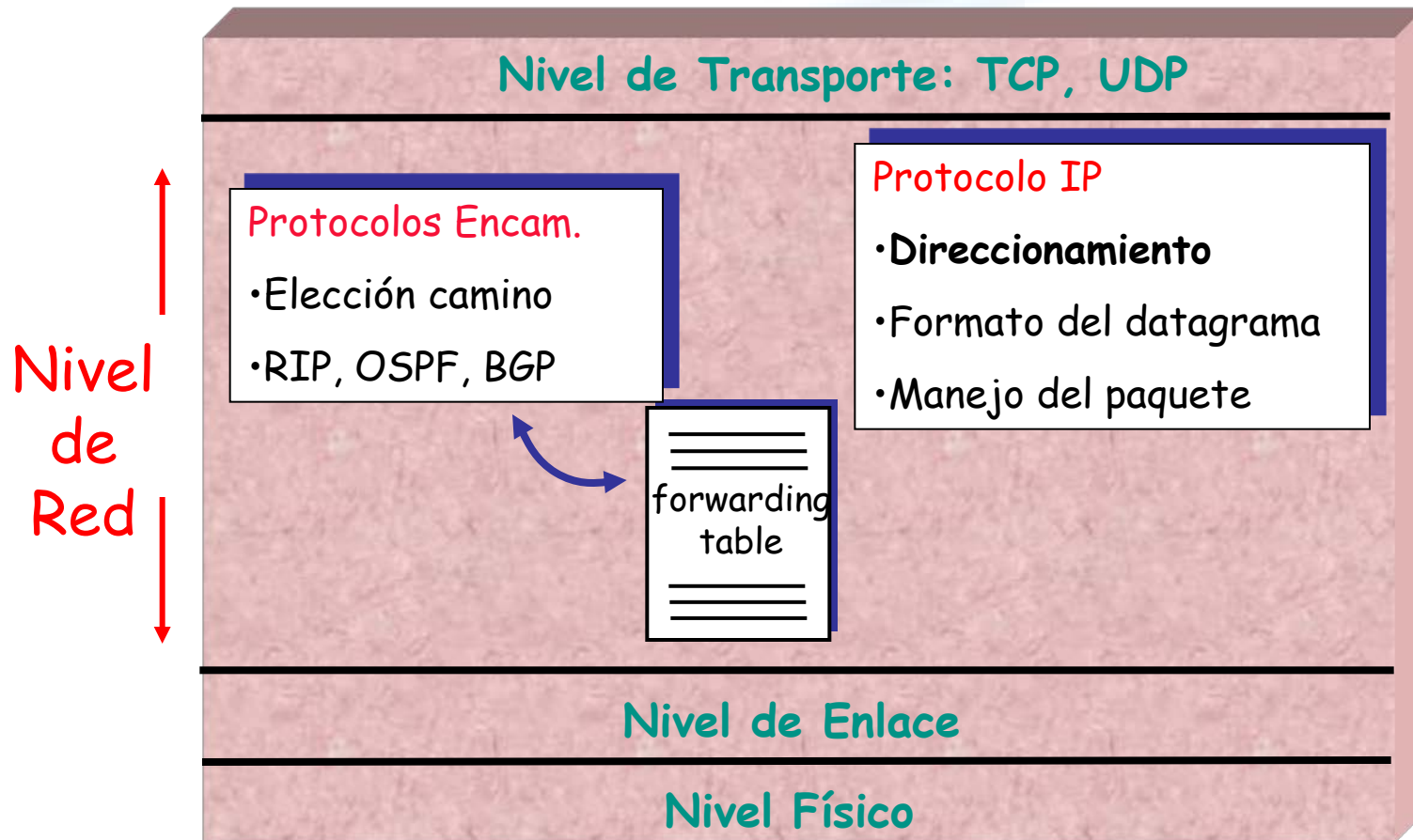
PREGUNTA: *¿Cuántos bytes recibe la capa de red en el otro extremo ?*

Problema 2:



- Descarga de archivos FTP. La capa de transporte del servidor le entrega a IP bloques de 4000 Bytes.
- Calcular cuantos fragmentos llegan al cliente por cada bloque original y los valores de los campos DF, MF y Offset de la cabecera de cada uno de los fragmentos.

Capa de Interred – Direcccionamiento



Direccionamiento IP

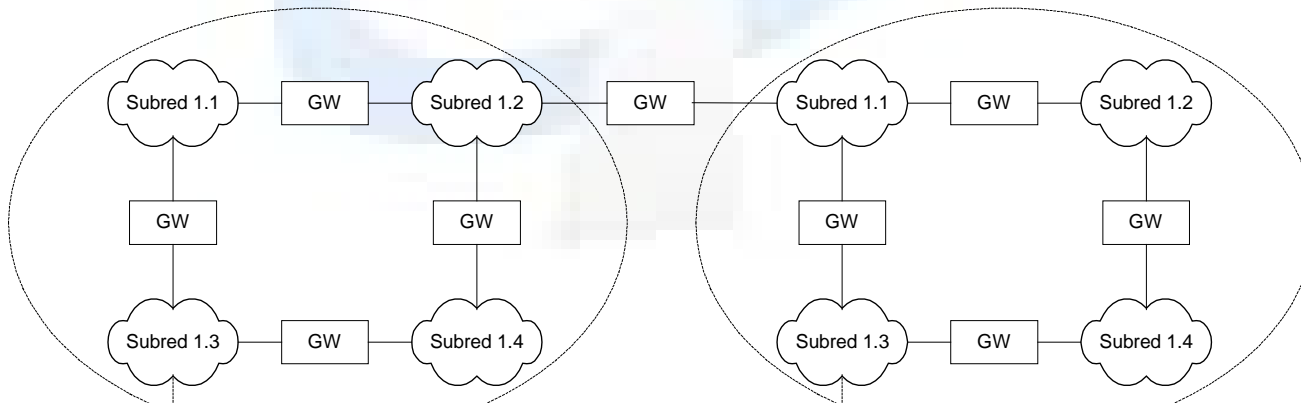
- Funcionalidad básica de IP es la entrega de datagramas a través de redes
- Necesario facilitar esta entrega:
 - Identificar el **interfaz** entre un dispositivo y la red
 - Facilitar la elección de la ruta cuando la entrega debe atravesar múltiples redes
- Características fundamentales de las direcciones IP
 - Únicas en el mismo dominio de colisión
 - Direcciones públicas y privadas
- Notación
 - 11100011010100101001101110110001 no es muy manejable
 - Transformarlo a notación “dotted-decimal”: 227.82.157.177

Direccionamiento IP

- Espacio de direccionamiento: 32 bits
 - 2^{32} direcciones = 4294967296 direcciones
- Dividido en 2
 - Identificador de red
 - Identificador de dispositivo

Hosts con mismo identificador de red \Rightarrow Igual red

Hosts con distinto identificador de red \Rightarrow Gateway/Router intermedio



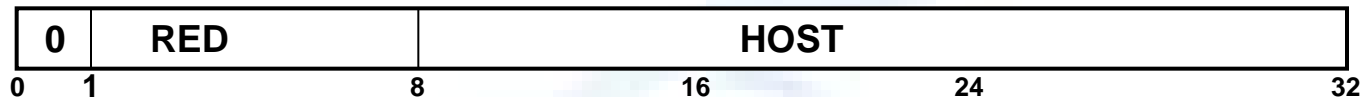
INTERNET: Red de redes interconectadas por Gateways/Routers

Direccionamiento IP

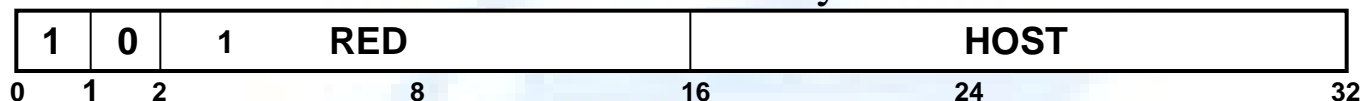
- ¿Dónde establecer el límite entre red y dispositivo?
- Tres posibles escenarios:
 - Pocas redes con muchos dispositivos
 - Aproximadamente el mismo número de redes que de dispositivos
 - Muchas redes con pocos dispositivos

Direccionamiento IP: Basado en clases

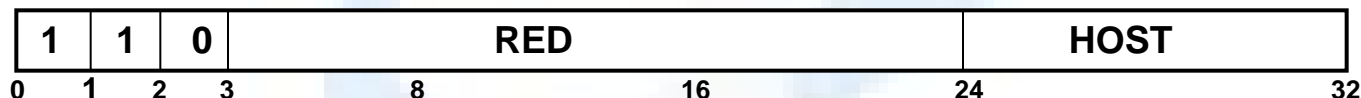
Clase A: Redes con más de 2^{16} hosts.



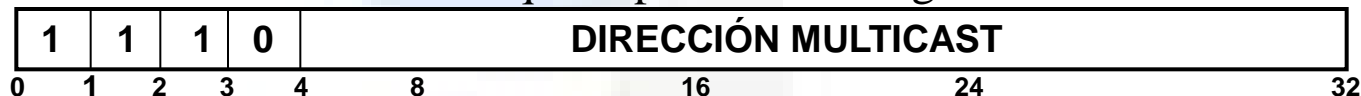
Clase B: Redes entre 2^8 y 2^{16} hosts.



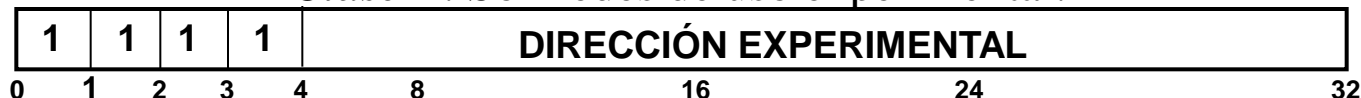
Clase C: Redes con menos de 2^8 hosts.



Clase D: Para redes que soportan la entrega multidifusión.



Clase E: Son redes de uso experimental.



Direccionamiento IP: Basado en clases

Clase	Primer Octeto de la dirección IP	Número de octetos en la parte de red y en la de host	Número máximo de redes posibles	Número máximo de hosts posibles	Rango de direcciones
Clase A	0xxx xxxx	1 / 3	$2^7 - 2 = 126$	$2^{24} - 2 = 16.777.214$	1.0.0.0 a 126.255.255.255
Clase B	10xx xxxx	2 / 2	$2^{14} = 16.384$	$2^{16} - 2 = 65.534$	128.0.0.0 a 191.255.255.255
Clase C	110x xxxx	3 / 1	$2^{21} = 2.097.152$	$2^8 - 2 = 254$	192.0.0.0 a 223.255.255.255
Clase D	1110 xxxx	—			224.0.0.0 a 239.255.255.255
Clase E	1111 xxxx	—			240.0.0.0 a 255.255.255.255

Direccionamiento IP: Direcciones IP especiales

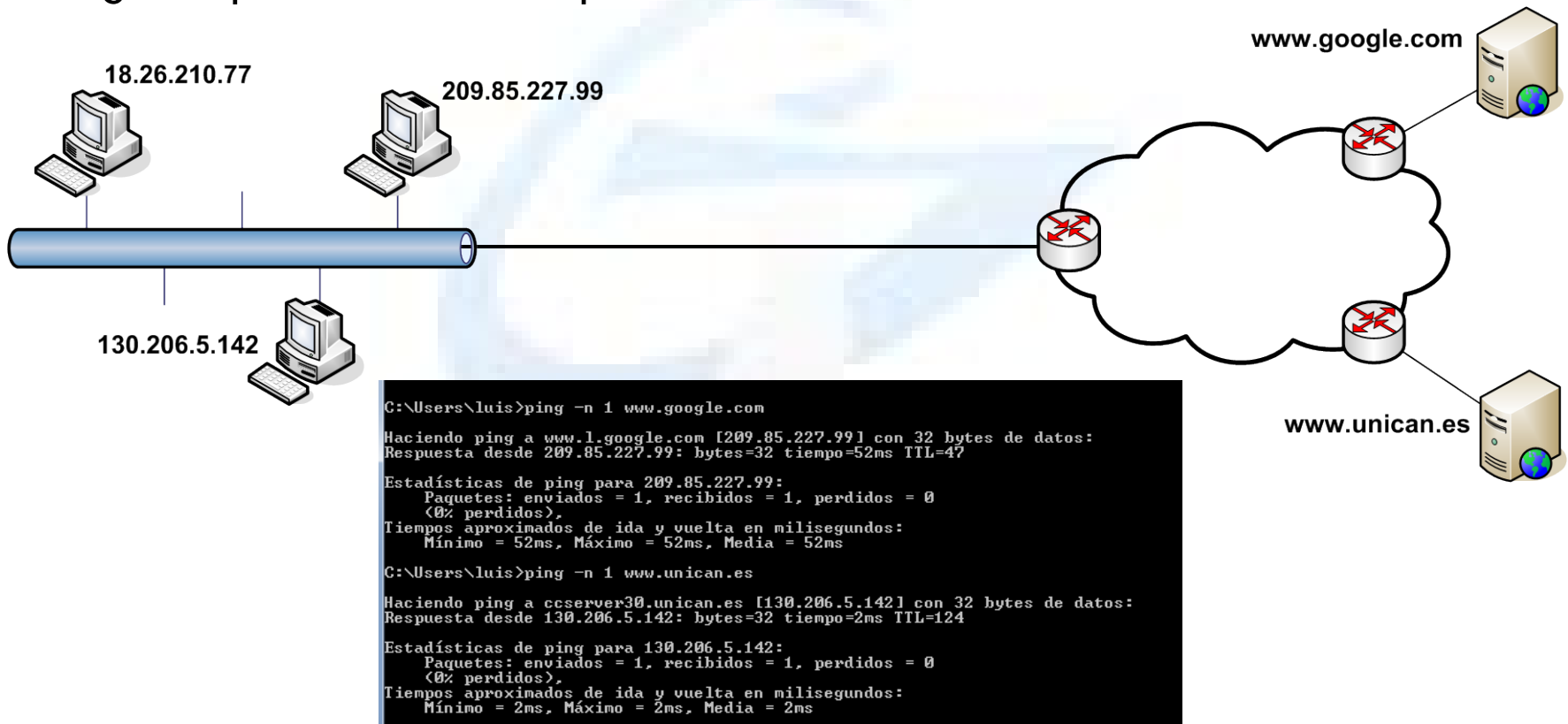
Dirección	Significado	Ejemplo
255.255.255.255	Broadcast en la propia red o subred	
0.0.0.0	Identifica al host que envía el datagrama. También se usa como dirección por defecto o indeterminada.	
Host a ceros	Identifica una red (o subred)	147.156.0.0
Host a unos	Broadcast en la red (o subred)	147.156.255.255
Red a ceros	Identifica un host en esa red (o subred)	0.0.1.25
127.0.0.1	Loopback	
224.0.0.1	Todos los hosts multicast	

Interfaz de loopback

- Permite comunicarse a un cliente y a un servidor en el MISMO host. El datagrama IP no saldrá del ordenador.
- Dirección 127.0.0.1 y nombre “localhost” (driver loopback).

Direccionamiento IP: Direcciones públicas, privadas y reservadas

- En una red todas las direcciones IP deben ser únicas
- ¿Por qué no usar cualquier dirección?



Direccionamiento IP: Direcciones públicas, privadas y reservadas

Red o rango	Uso
127.0.0.0	Reservado (fin clase A)
128.0.0.0 – 128.0.255.255	Reservado (ppio. clase B)
191.255.0.0 – 191.255.255.255	Reservado (fin clase B)
192.0.0.0 – 192.0.0.255	Reservado (ppio. Clase C)
223.255.255.0 – 223.255.255.255	Reservado (fin Clase C)
240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0 – 10.255.255.255	Privado (clase A)
172.16.0.0 – 172.31.0.0	Privado (clase B)
192.168.0.0 – 192.168.255.0	Privado (clase C)

Direccionamiento IP: Direcciones públicas, privadas y reservadas

- Las direcciones privadas no son accesibles por sistemas externos a la organización.
 - Los routers deben filtrar estas redes a la hora de enviar información de encaminamiento.
- Utilización de **NAT** (Network Address Translation) para conversión.

Direccionamiento IP: Problemas del direccionamiento basado en clases

- Falta de flexibilidad para el direccionamiento interno
 - Los bloques de direcciones que se asignaban no se ajustaban a la estructura de las redes.
 - No era posible crear jerarquías.
- Uso ineficiente del espacio de direccionamiento
 - Con sólo 3 clases se desperdiciaba demasiado el limitado espacio de direccionamiento.
- Incremento de las entradas en las tablas de rutas
 - Si se trata de evitar el uso ineficiente, cargas sobremanera los routers.

Direccionamiento IP: Subredes

- Ante las ineficiencias del direccionamiento basado en clases, se define el sub-direccionamiento (subnetting). RFC 950.
- Ventajas frente al sistema de clases:
 - Mejor ajuste a la estructura física de la red
 - Flexibilidad para gestionar las subredes
 - Invisible hacia la Internet
 - No hacían falta nuevos bloques de direcciones
 - No se incrementaban las tablas de rutas

Direccionamiento IP: Subredes

- Si no se utiliza subred:

$$\text{Dir. IP} = \text{id. de red} + \text{id. de host}$$

- Si se utiliza subredes:

$$\text{Dir. IP} = \text{id. de red} + \text{id. de subred} + \text{id. de host}$$

- Hace falta más información para saber cual es la parte de subred

Máscara de subred

	161	117	183	183
Dir.IP	1 0 1 0 0 0 0 1	0 1 1 1 0 1 0 1	1 0 1 1 0 1 1 1	1 0 1 1 0 1 1 1
	255	255	240	000
Máscara	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0	0 0 0 0 0 0 0 0
	1 0 1 0 0 0 0 1	0 1 1 1 0 1 0 1	1 0 1 1 0 1 1 1	1 0 1 1 0 1 1 1
	Id. de red		Id. Subred	Id. de Host

Id de red: **161.117**

Id de Subred: **11**

Id de Host: **1975**

Máscaras por defecto:

Clase A: 255.0.0.0

Clase B: 255.255.0.0

Clase C: 255.255.255.0

Direccionamiento IP: Subredes

Ejm.: Establecer el esquema de subdireccionamiento correspondientes a la red 195.100.205.0 con máscara 255.255.255.224 :

Red: (11000011 01100100 11001101 00000000)

Máscara: (11111111 11111111 11111111 11100000)

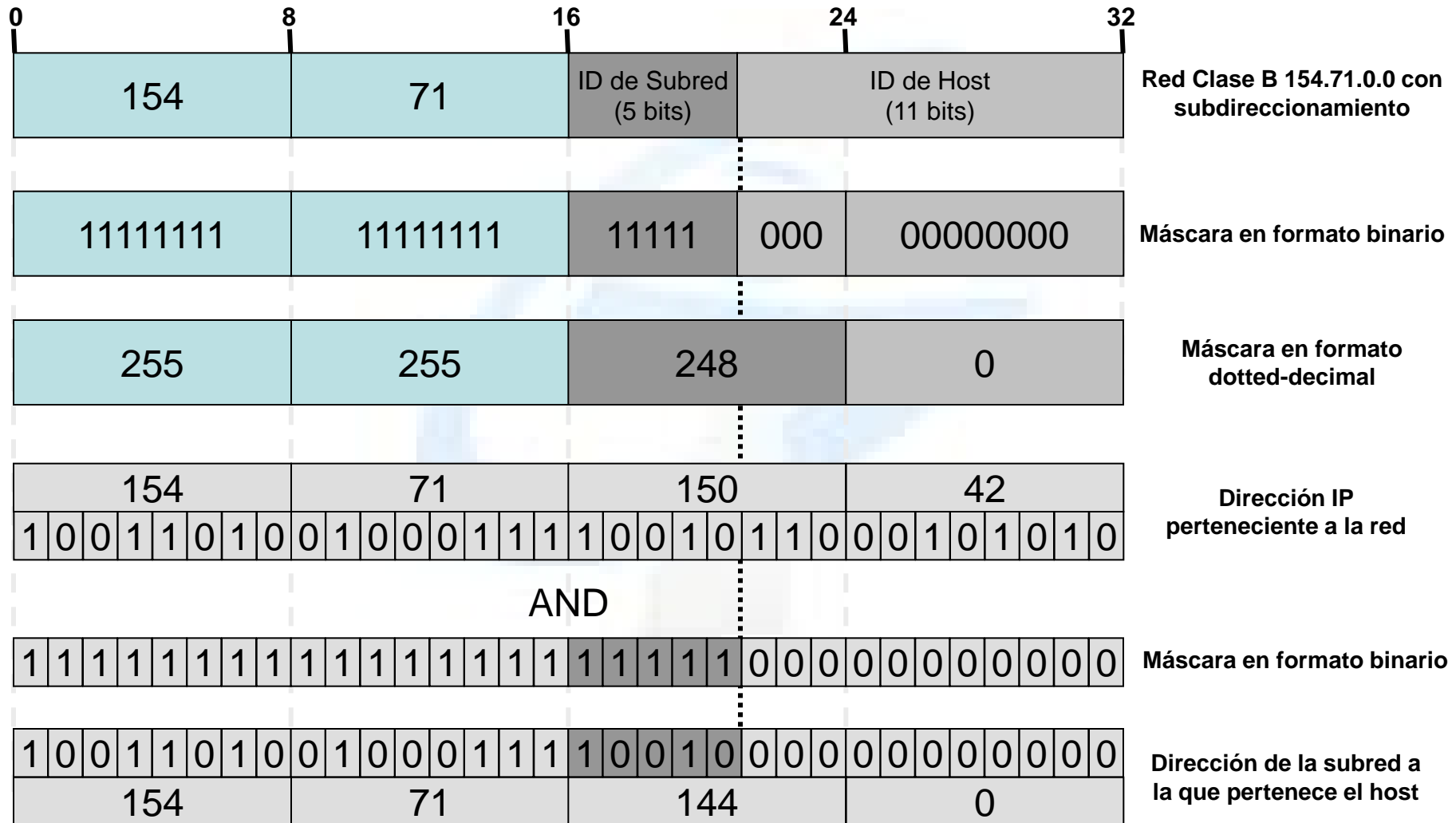
Subredes posibles = {

001 → 32 →	Hosts: (33-62)
010 → 64 →	Hosts: (65-94)
011 → 96 →	Hosts: (97-126)
100 → 128 →	Hosts: (129-158)
101 → 160 →	Hosts: (161-190)
110 → 192 →	Hosts: (193-222)

Direccionamiento IP: Subredes

- Red 156.134.0.0, máscara 255.255.255.0
- 256 subredes (de 156.134.0.0 a 156.134.255.0) pero
 - ¿Dirección 156.134.0.0 identifica red o subred?
 - ¿Dirección 156.134.255.255 identifica broadcast en la red o en la subred?
- Solución: no utilizar la primera y la última subred (las que tienen el campo subred todo a ceros o todo a unos).
- Esta norma se puede infringir (se hace a menudo) con la declaración de 'subnet zero'.

Direccionamiento IP: Subredes



Direccionamiento IP: Notación en subredes

- Sólo con la dirección IP no tenemos información suficiente. Es necesario incluir información de la máscara
 - 154.71.150.42 pertenece a:
 - 154.71.144.0 con máscara 255.255.248.0
 - 154.71.148.0 con máscara 255.255.252.0
- Arrastrar un número binario de 32 bits es tedioso y no práctico
- La notación dotted-decimal es más práctica
- La potencia de computo de los routers actuales hace la notación más extendida la “slash notation”
 - 154.71.144.0 con máscara 255.255.248.0 = 154.71.144.0/21
 - 154.71.148.0 con máscara 255.255.252.0 = 154.71.144.0 /22

Direccionamiento IP: Diseño de subredes

Bits de subred	Número de subredes	Nº subredes (subred cero)	Bits de host	Número de hosts	Máscara
0	0	0	16	65534	255.255.0.0
1	0	2	15	32766	255.255.128.0
2	2	4	14	16382	255.255.192.0
3	6	8	13	8190	255.255.224.0
4	14	16	12	4094	255.255.240.0
5	30	32	11	2046	255.255.248.0
6	62	64	10	1022	255.255.252.0
7	126	128	9	510	255.255.254.0
8	254	256	8	254	255.255.255.0
9	510	512	7	126	255.255.255.128
10	1022	1024	6	62	255.255.255.192
11	2046	2048	5	30	255.255.255.224
12	4094	4096	4	14	255.255.255.240
13	8190	8192	3	6	255.255.255.248
14	16382	16384	2	2	255.255.255.252
15	32766	32768	1	0	255.255.255.254
16	65532	65536	0	0	255.255.255.255

Bits de subred	Número de subredes	Nº subredes (subred cero)	Bits de host	Número de hosts	Máscara
0	0	0	8	254	255.255.255.0
1	0	2	7	126	255.255.255.128
2	2	4	6	62	255.255.255.192
3	6	8	5	30	255.255.255.224
4	14	16	4	14	255.255.255.240
5	30	32	3	6	255.255.255.248
6	62	64	2	2	255.255.255.252
7	126	128	1	0	255.255.255.254
8	254	256	0	0	255.255.255.255

Protocolos para Interconexión de Redes

Direccionamiento IP: Diseño de subredes

- ¿Cuántos bits uso para la subred y cuántos para los hosts?
- Depende de las características de la red que se esté desplegando.
 - Para maximizar el número de hosts disponibles trataremos de reservar más bits para el *host ID*
 - Para maximizar el número de subredes posibles trataremos de reservar más bits para el *subnet ID*

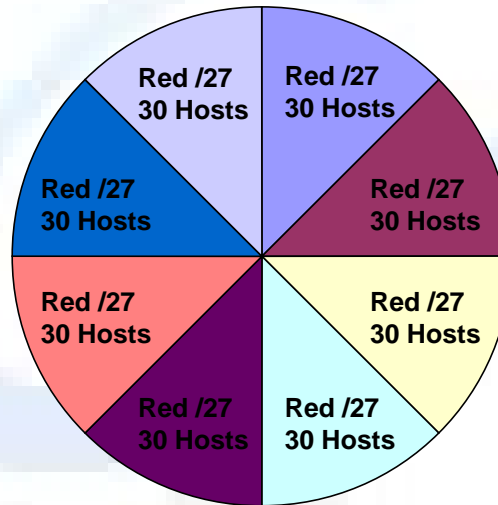
Direccionamiento IP: Diseño de subredes

- Red 172.16.0.0/16 a dividir en 8 subredes

Subnet Address	Subnet Mask	Broadcast Address	Valid Host Range
172.16.0.0	255.255.224.0	172.16.31.255	172.16.0.1 to 172.16.31.254
172.16.32.0	255.255.224.0	172.16.63.255	172.16.32.1 to 172.16.63.254
172.16.64.0	255.255.224.0	172.16.95.255	172.16.64.1 to 172.16.95.254
172.16.96.0	255.255.224.0	172.16.127.255	172.16.96.1 to 172.16.127.254
172.16.128.0	255.255.224.0	172.16.159.255	172.16.128.1 to 172.16.159.254
172.16.160.0	255.255.224.0	172.16.191.255	172.16.160.1 to 172.16.191.254
172.16.192.0	255.255.224.0	172.16.223.255	172.16.192.1 to 172.16.223.254
172.16.224.0	255.255.224.0	172.16.255.255	172.16.224.1 to 172.16.255.254

Direccionamiento IP: Diseño de subredes

- En ocasiones esto no es suficiente.



Red Clase C /24 (254 Hosts)

- En redes heterogéneas se necesita una solución más flexible.

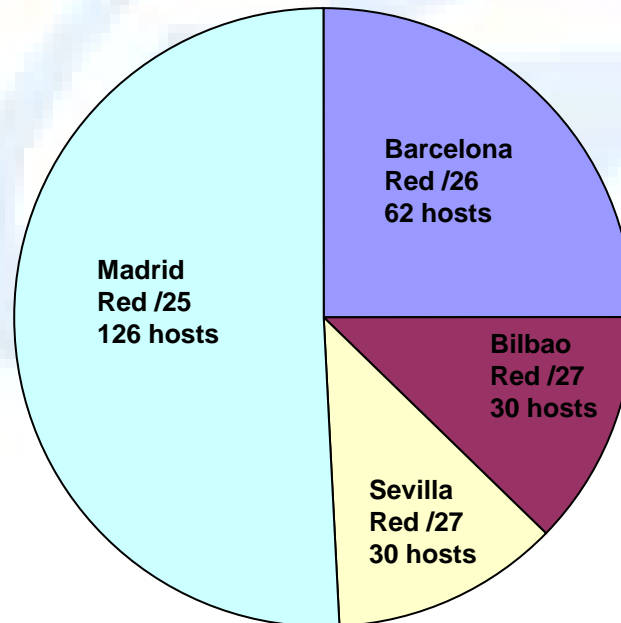
Direccionamiento IP: Diseño de subredes

- Supuesto: tenemos subredes con n° de equipos distintos
 - Problema: Desaprovechamos direcciones en las subredes con menos equipos
 - Solución: Asignar rangos de tamaño variable
 - **VLSM** (Variable Length Subnet Mask)

Oficina	Subred	Máscara	Rango	Direcciones útiles
Madrid	194.100.100.0	255.255.255.128	194.100.100.0-127	126
Barcelona	194.100.100.128	255.255.255.192	194.100.100.128-191	62
Bilbao	194.100.100.192	255.255.255.224	194.100.100.192-223	30
Sevilla	194.100.100.224	255.255.255.224	194.100.100.224-255	30

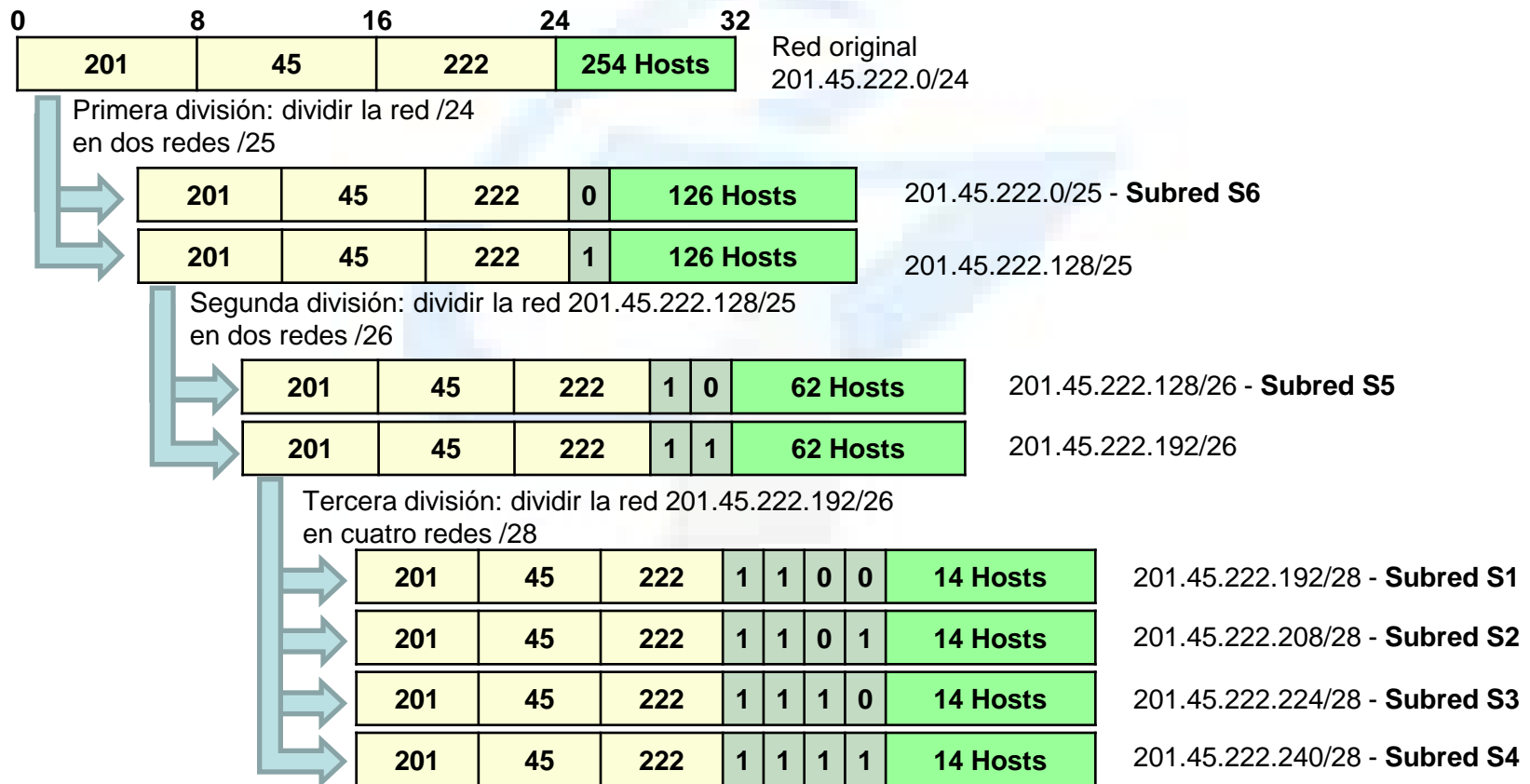
Direccionamiento IP: Diseño de subredes

- Uso más adaptado del espacio de direccionamiento que nos ofrece una red Clase C.



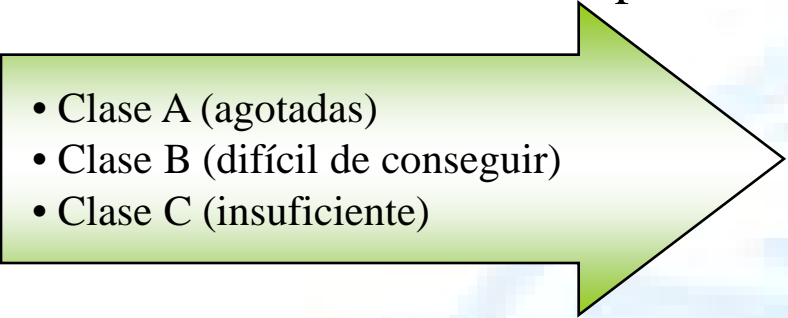
Direccionamiento IP: Diseño de subredes

- Red 201.45.222.0/24 asignada a una empresa con 6 redes de 100, 50, 10, 10, 5 y 2 dispositivos respectivamente. ¿Cómo configurar su red?

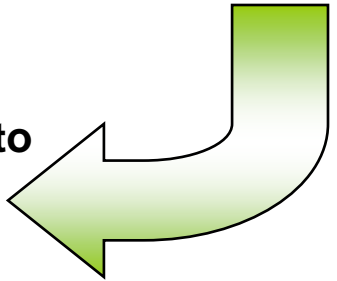


Direccionamiento IP: Superredes

PROBLEMA: Internet crece exponencialmente \Rightarrow Agotamiento de direcciones

- 
- Clase A (agotadas)
 - Clase B (difícil de conseguir)
 - Clase C (insuficiente)

SOLUCIÓN: Asignar redes C en donde antes había redes B



PROBLEMA: Las tablas de enrutamiento aumentan conforme nos acercamos al backbone: una misma red utilizaría varias dir. C, por tanto entradas en router

El nº redes se duplica cada 9 meses mientras que la capacidad y potencia de los routers se duplica cada 18 meses

SOLUCIÓN:

1993 – RFC 1519 : CIDR (Classless InterDomain Routing)

Protocolos para Interconexión de Redes

Direccionamiento IP: Superredes

CIDR

1º Asignación jerárquica de direcciones:

GEOGRÁFICA

194.0.0.0 a 195.255.0.0 para Europa
198.0.0.0 a 199.255.0.0 para Norteamérica
200.0.0.0 a 201.255.0.0 para Centro y Sudamérica
202.0.0.0 a 203.255.0.0 para Asia y zona del Pacífico

- Las entradas en los routers se agrupan

2º Asignaciones múltiples con máscaras similares (para 1,2,4,8, etc)

Ejemplo:

provisión de dir. IP a 1200 ordenadores
dentro del rango 195.100.0.0 a

195.100.255.0. *Nota: Ocupado hasta la 195.100.12.0*

```
ip route 195.100.16.0 255.255.255.0 interfaz
ip route 195.100.17.0 255.255.255.0 interfaz
ip route 195.100.18.0 255.255.255.0 interfaz
ip route 195.100.19.0 255.255.255.0 interfaz
ip route 195.100.20.0 255.255.255.0 interfaz
ip route 195.100.21.0 255.255.255.0 interfaz
ip route 195.100.22.0 255.255.255.0 interfaz
ip route 195.100.23.0 255.255.255.0 interfaz
```



Los 21 primeros bits de la máscara deben ser iguales

El primer rango con máscara común es de

195.100.16.0 a 195.100.23.0, resto libres

```
ip route 195.100.16.0 255.255.248.0 interfaz
```

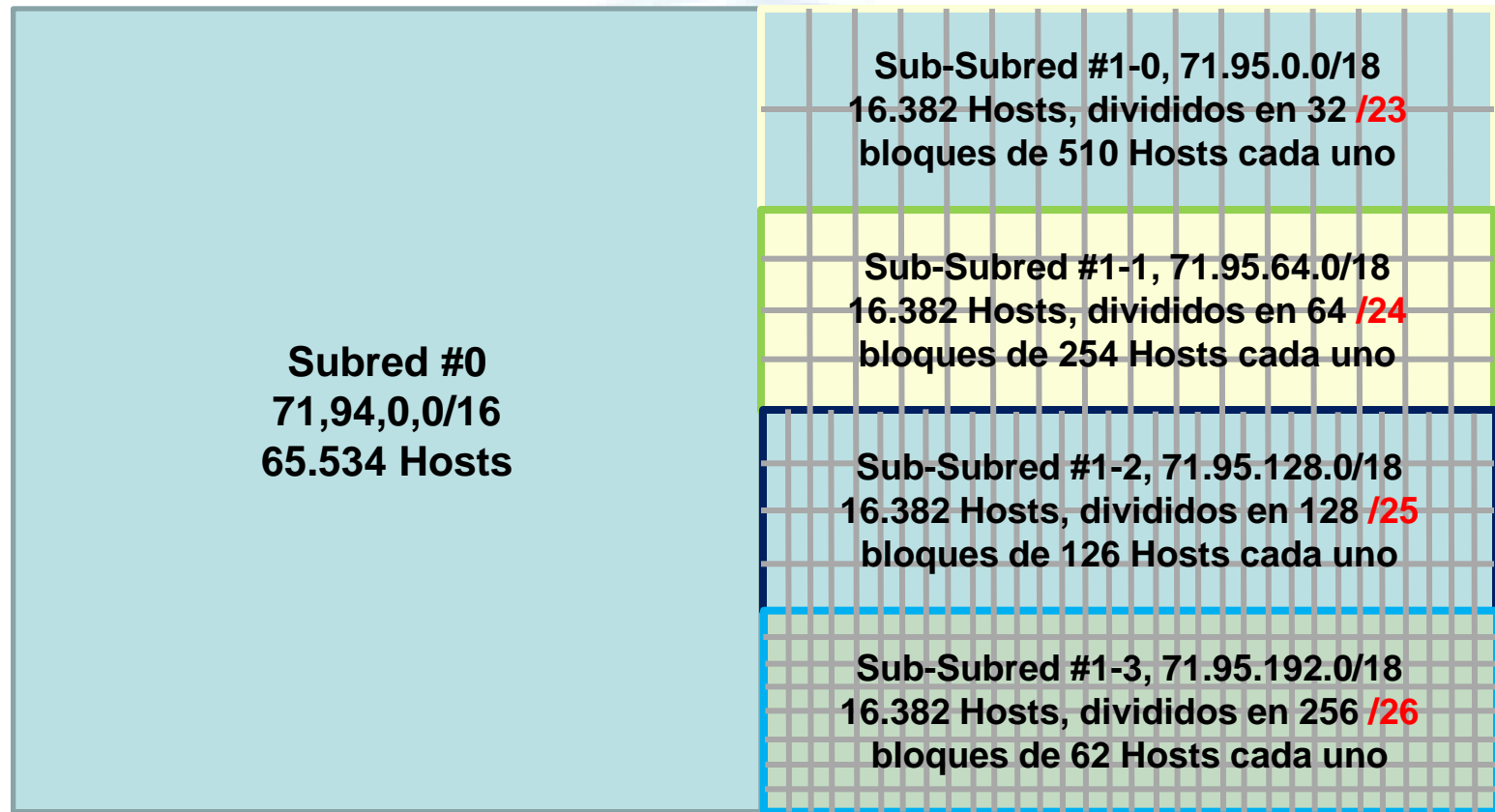
- Host en distintas redes conectan a través de router
- No hay referencia directa al grupo, solo a redes C indiv.
- No hay dirección broadcast para el grupo completo
- El 50% de redes A podrían ser utilizadas en CIDR

SUPERNETTING

Protocolos para Interconexión de Redes

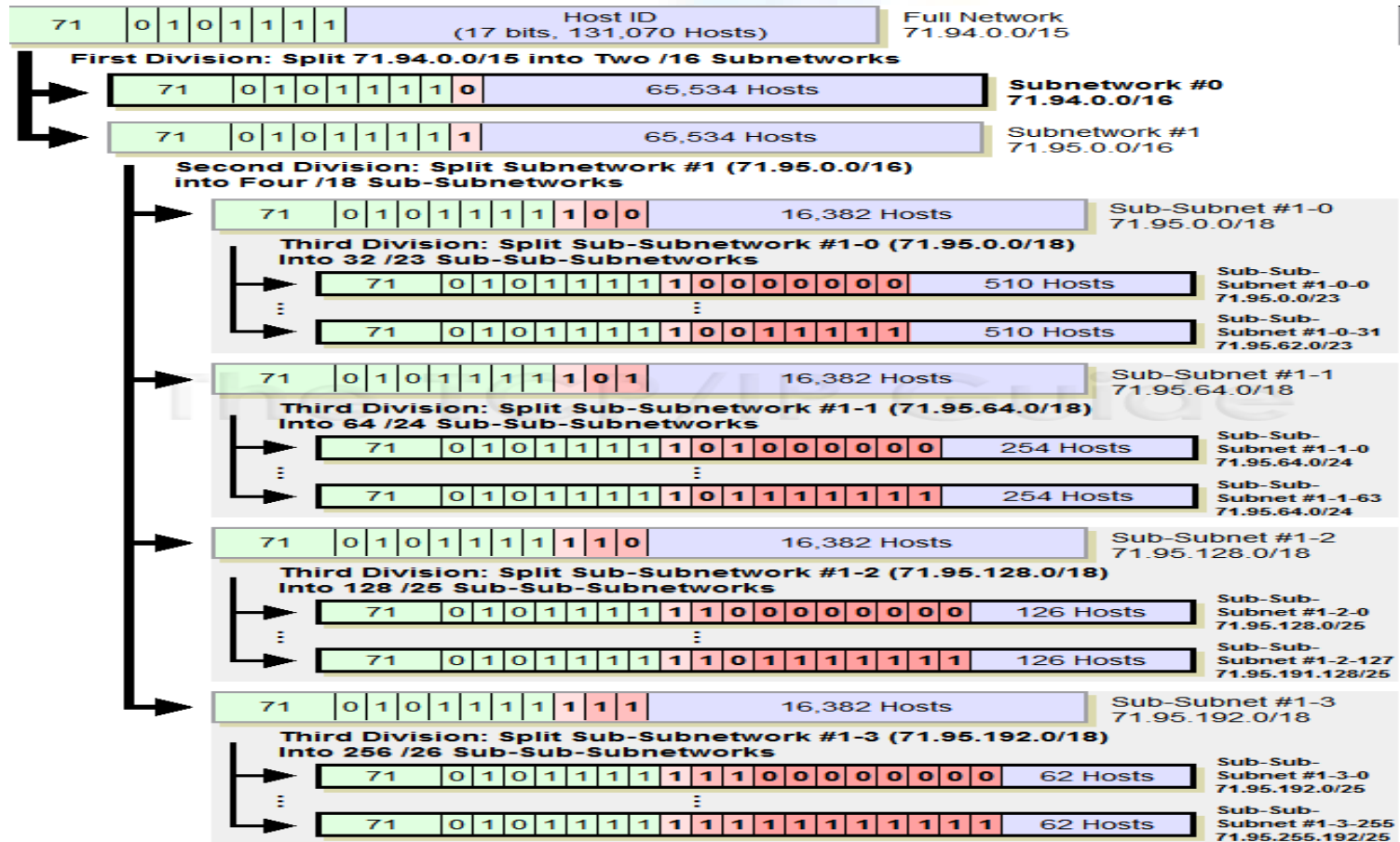
Direccionamiento IP: Ejemplo de Supernetting (II)

- Red 71.94.0.0/15 fragmentada a gusto (sobre un total de 131.070 dispositivos posibles)



Direccionamiento IP: Ejemplo de Supernetting (II)

- Red 71.94.0.0/15 fragmentada a gusto

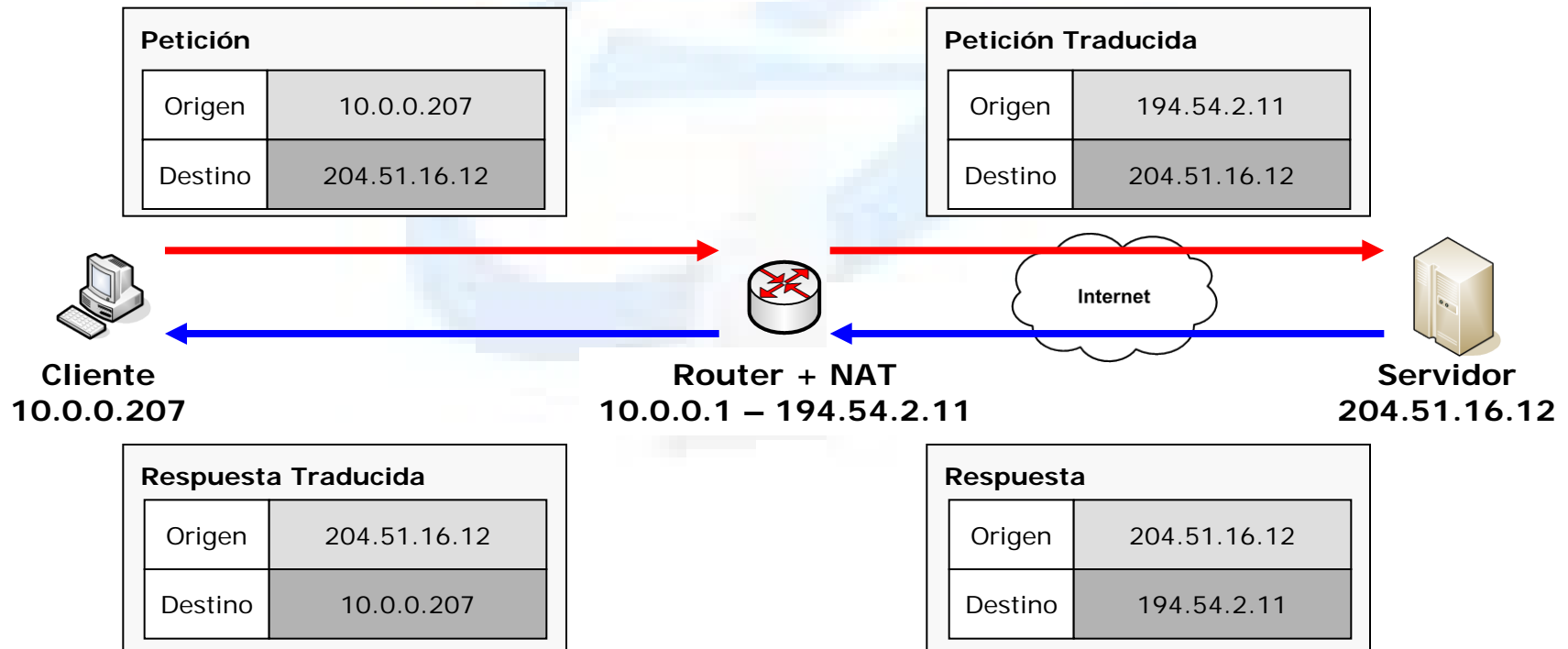


IPv4 Network Address Translation

- El espacio de direccionamiento público de IPv4 no es suficiente para el número de equipos que existen en la actualidad.
- IPv4 definió el direccionamiento público y privado para solventar esto.
- Es necesario un mecanismo que permita que equipos con direcciones privadas puedan comunicarse con el exterior.
- El diseño se basó en una serie de características sobre el propio uso de Internet:
 - Modelo cliente-servidor: Sólo los servidores tienen que ser conocidos públicamente
 - Complementariedad en el acceso: No todos los equipos de una red acceden a la vez al exterior
 - Comunicaciones enrutadas: Todos los accesos se hacen a través de un enrutador

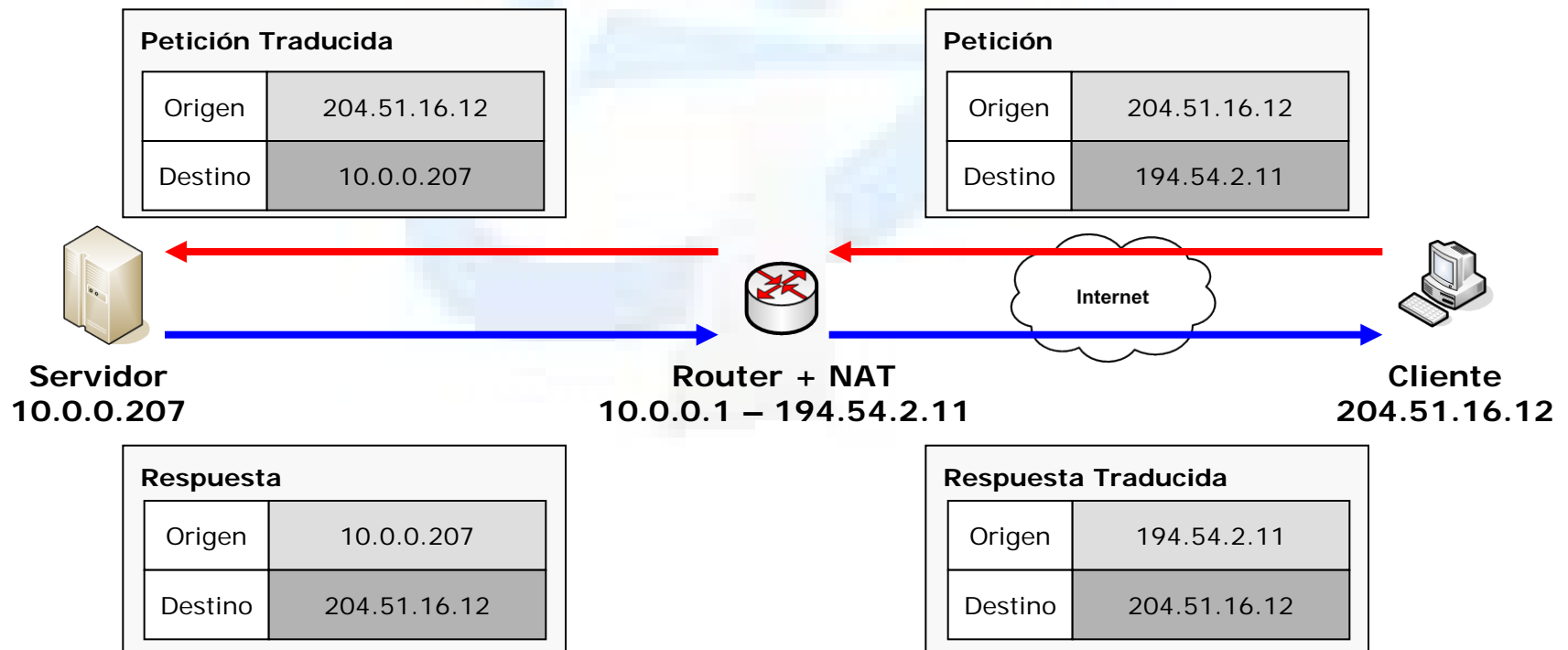
NAT: Modo unidireccional (salida)

- Modo original (RFC 1631)
- Se diseñó para el caso de un cliente en una red privada accediendo a un servidor en una red pública.



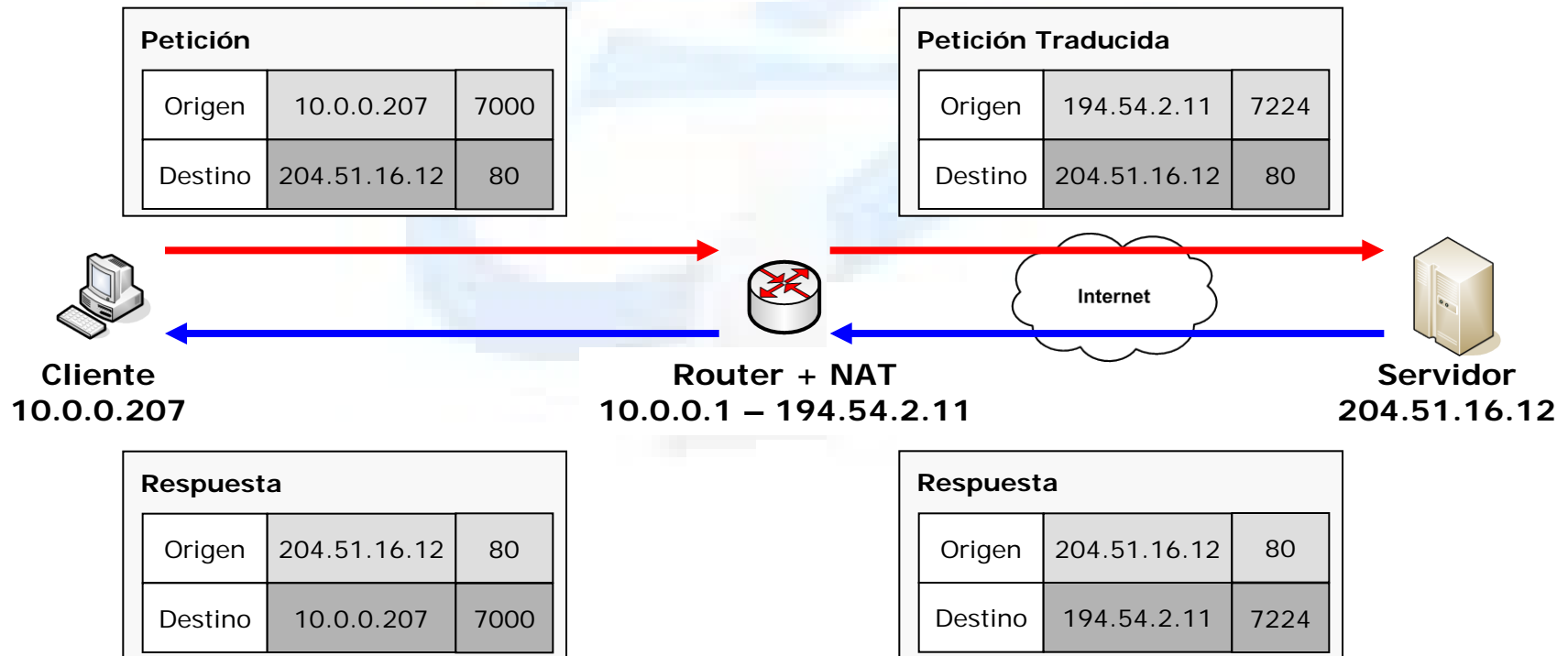
NAT: Modo bidireccional

- Soporte del caso en el que un cliente en Internet quiera acceder a un servidor en una red privada.
- Combinado con DNS_ALG (RFC 2694) o con IP/Port Forwarding



NAT: Modo basado en puertos (NAPT)

- El mapeo interno que se hace en el router se extiende y usa no sólo información de red sino también de nivel de transporte



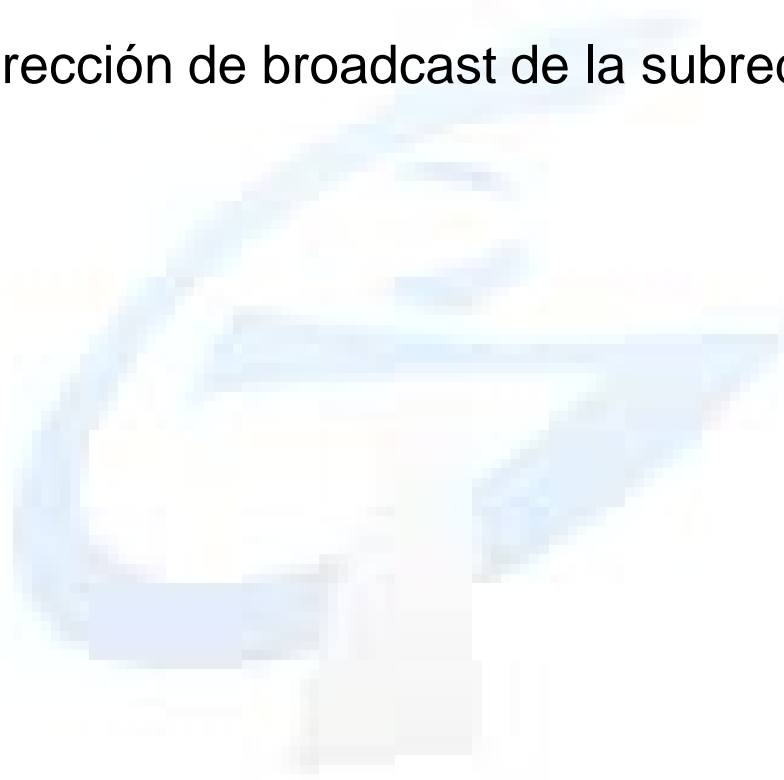
Direccionamiento IP: Ejercicios (I)

- ¿A qué subred pertenece el host 138.8.149.32/17?



Direccionamiento IP: Ejercicios (II)

- ¿Cuál es la dirección de broadcast de la subred 138.8.16.0/21?



Direccionamiento IP: Ejercicios (III)

- Una empresa con 5 departamentos de 1500, 800, 400, 100 y 50 PCs cada uno recibe de su ISP el bloque de direcciones 170.35.80.0/20.

Organizar su red interna en las subredes correspondientes y especificar de cada una de ellas:

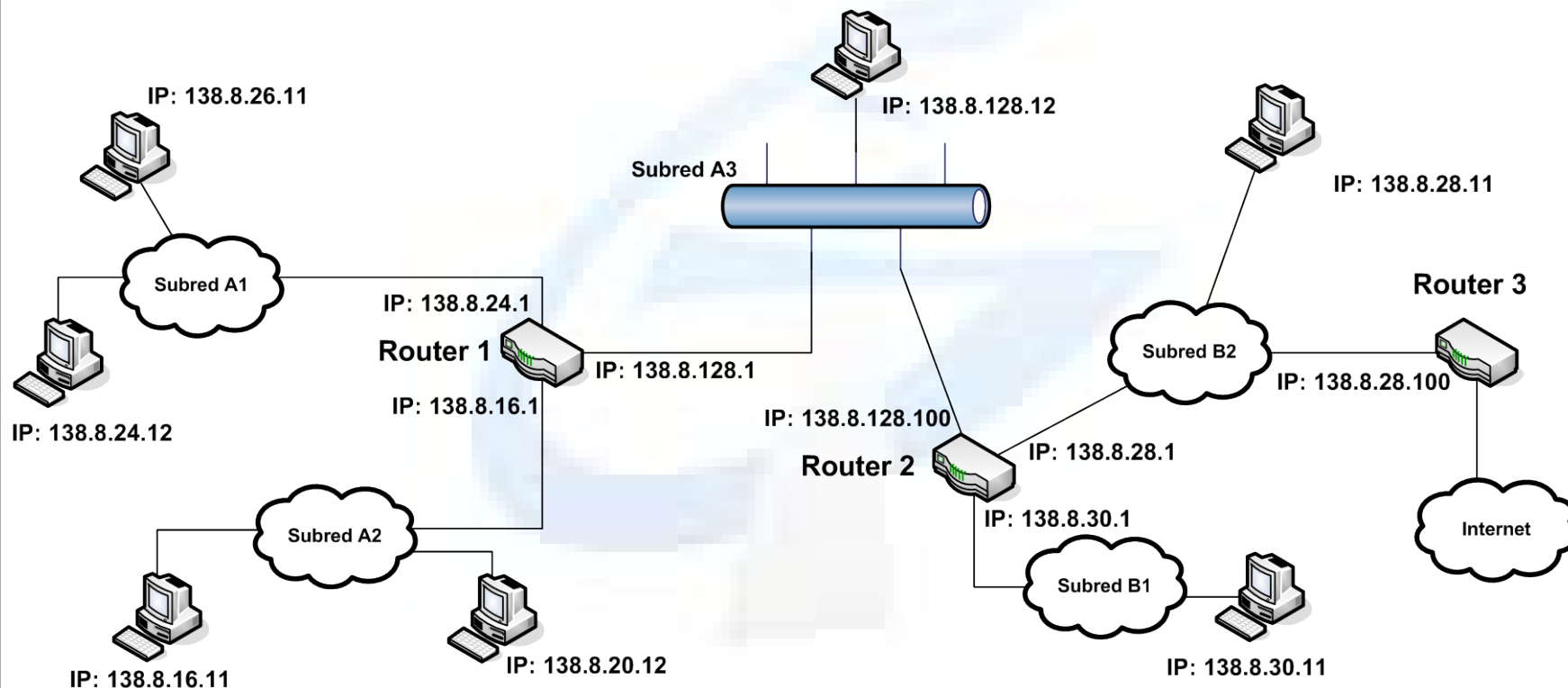
Dirección de red	Máscara	Dirección de Broadcast	Número máximo de direcciones posibles	Rango de direcciones

Direccionamiento IP: Ejercicios (IV)

- Una empresa dispone de la dirección de red 138.8.0.0/16. Las subredes A1, A2 y A3 pertenecen al departamento A, y las subredes B1 y B2 pertenecen al departamento B. Dicha red corporativa se conecta a Internet a través del encaminador Router 3.
 - Si se utiliza como criterio de diseño el **disponer del mayor número de direcciones IP asignables en cada subred**, complete la siguiente tabla:

Dirección de red	Máscara	Dirección de Broadcast	Número máximo de direcciones posibles	Rango de direcciones

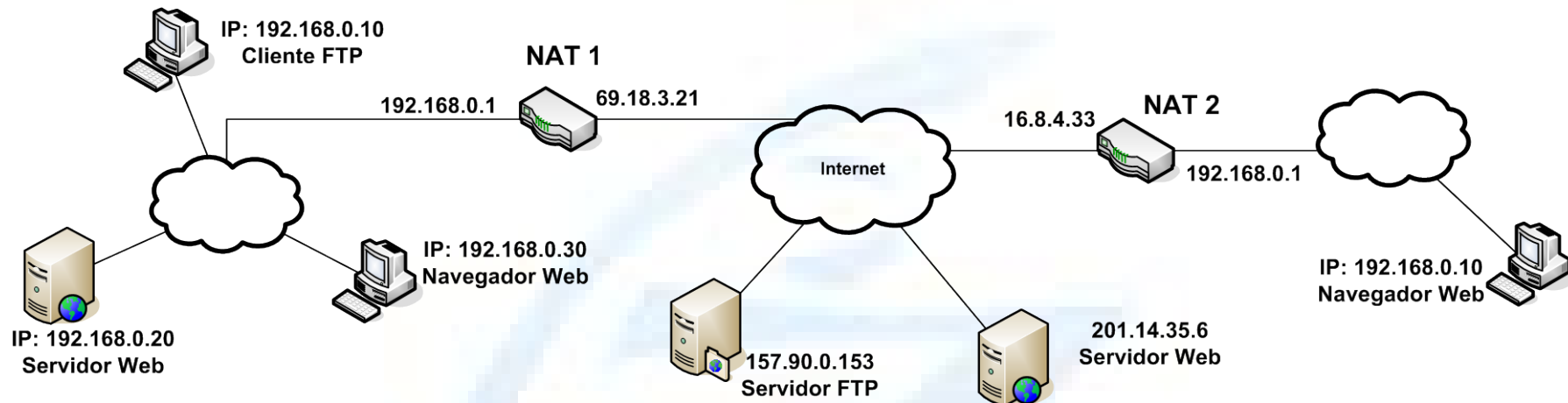
Direccionamiento IP: Ejercicios (IV)



Direccionamiento IP: Ejercicios (IV)

- ¿Qué dirección IP destino debe utilizar un equipo perteneciente a la subred B2 si desea transferir un datagrama IP a todos los equipos de la subred A2?
- ¿Podrá transferir, un equipo perteneciente a la subred B1, un datagrama IP únicamente a todos los equipos del departamento A? En caso de que la respuesta sea afirmativa, indicar la dirección IP destino que se debe utilizar.

NAT: Ejercicios (I)



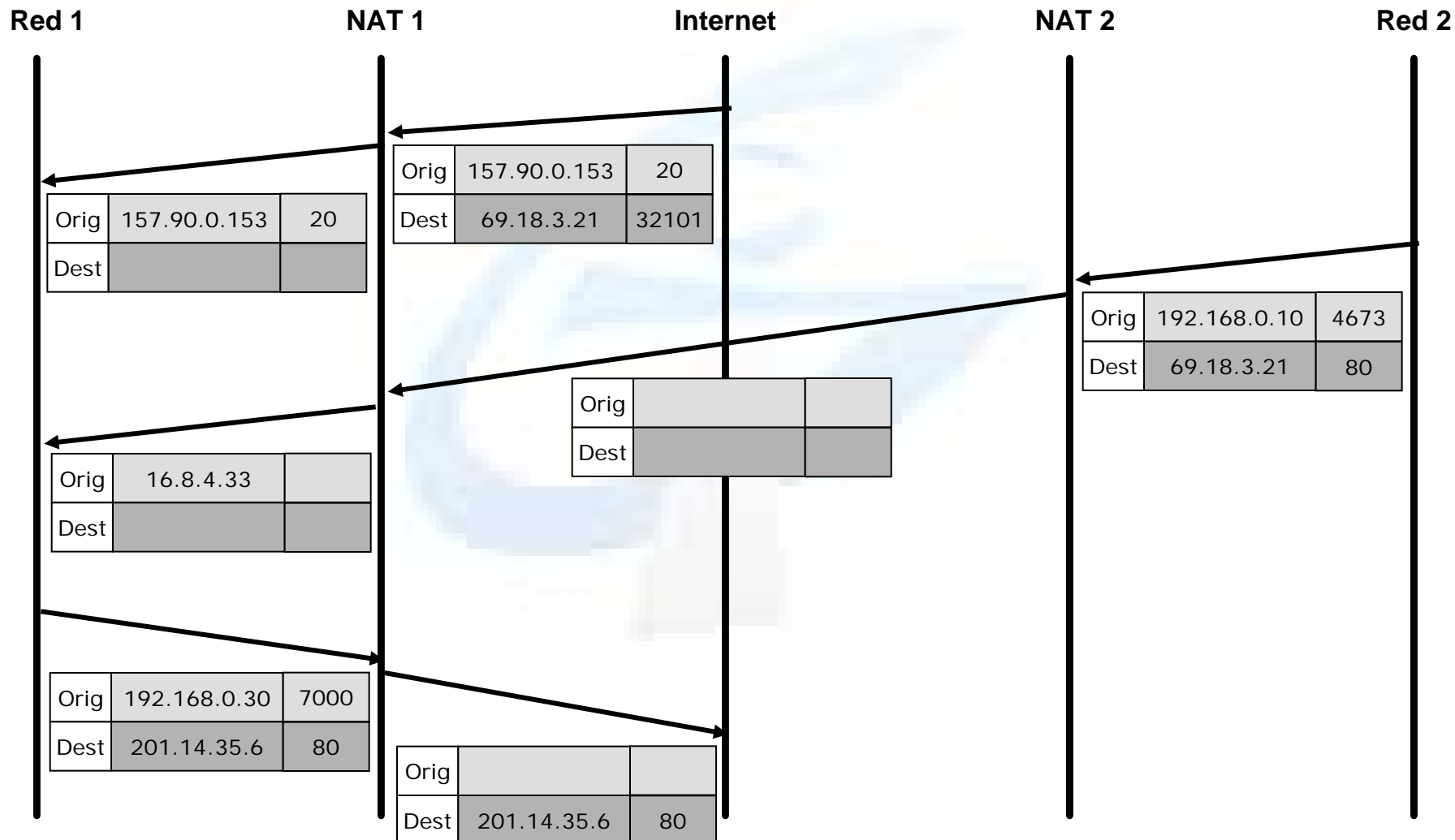
NAT 1:

Dirección IP interna	Puerto inteno	Dirección IP externa	Puerto externo
192.168.0.10	35213	69.18.3.21	32101
192.168.0.20	80	69.18.3.21	80
192.168.0.30	7000	69.18.3.21	6532

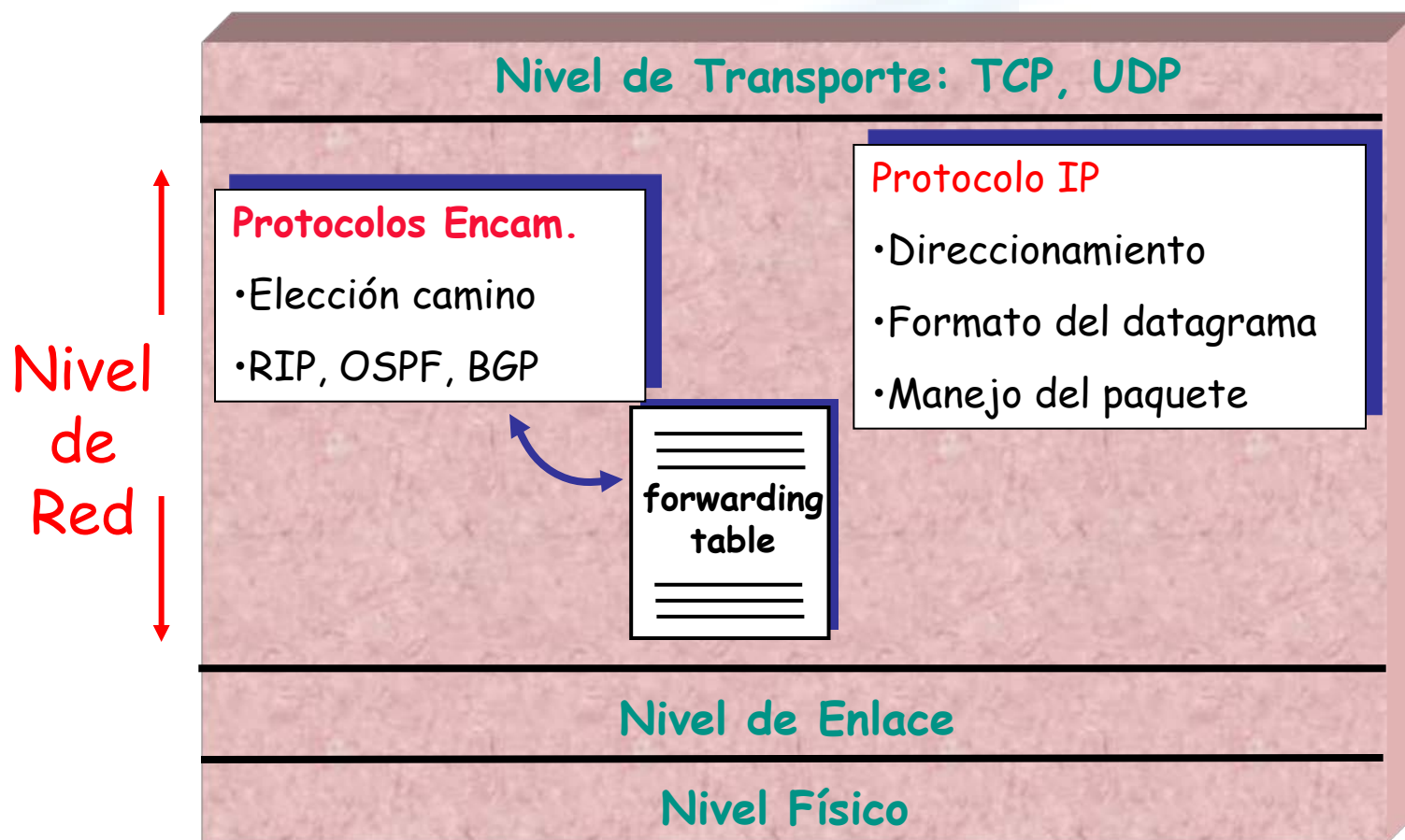
NAT 2:

Dirección IP interna	Puerto inteno	Dirección IP externa	Puerto externo
192.168.0.10	4673	16.8.4.33	5122

NAT: Ejercicios (I)

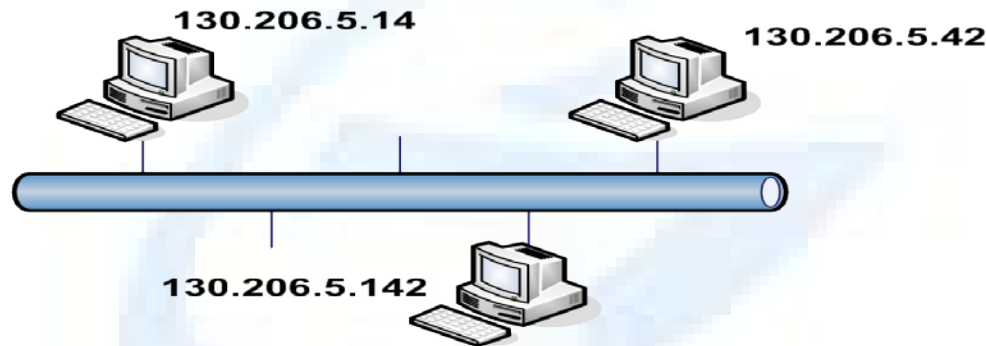


Capa de Interred – Enrutamiento



Entrega de Datagramas IP

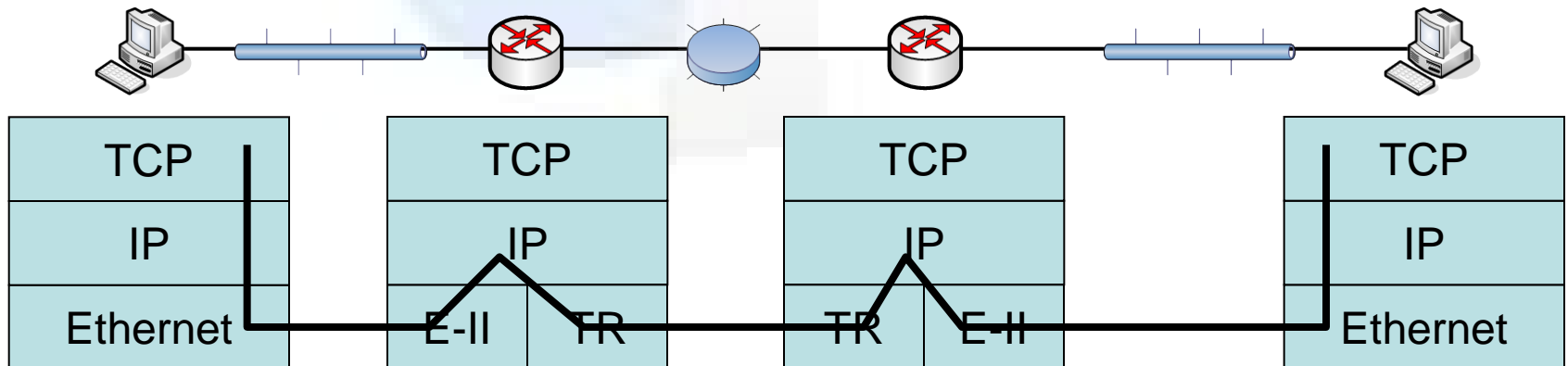
- Entrega directa
 - Entre nodos en la misma red física



- Entrega indirecta (Enrutamiento)
 - Entre nodos en distintas redes físicas
 - Necesario que nodos intermedios re-envíen los datagramas IP

Entrega de Datagramas IP

- Entrega indirecta (Enrutamiento)
 - Concepto de próximo salto
 - Evita tener que conocer la ruta completa entre origen y destino
 - Sólo los enrutadores hacen enrutamiento
 - Los nodos sólo tienen dos opciones: 1) Entrega directa; 2) Entregarle el datagrama IP al enrutador de su red



Enrutamiento: Reenvío de Datagramas

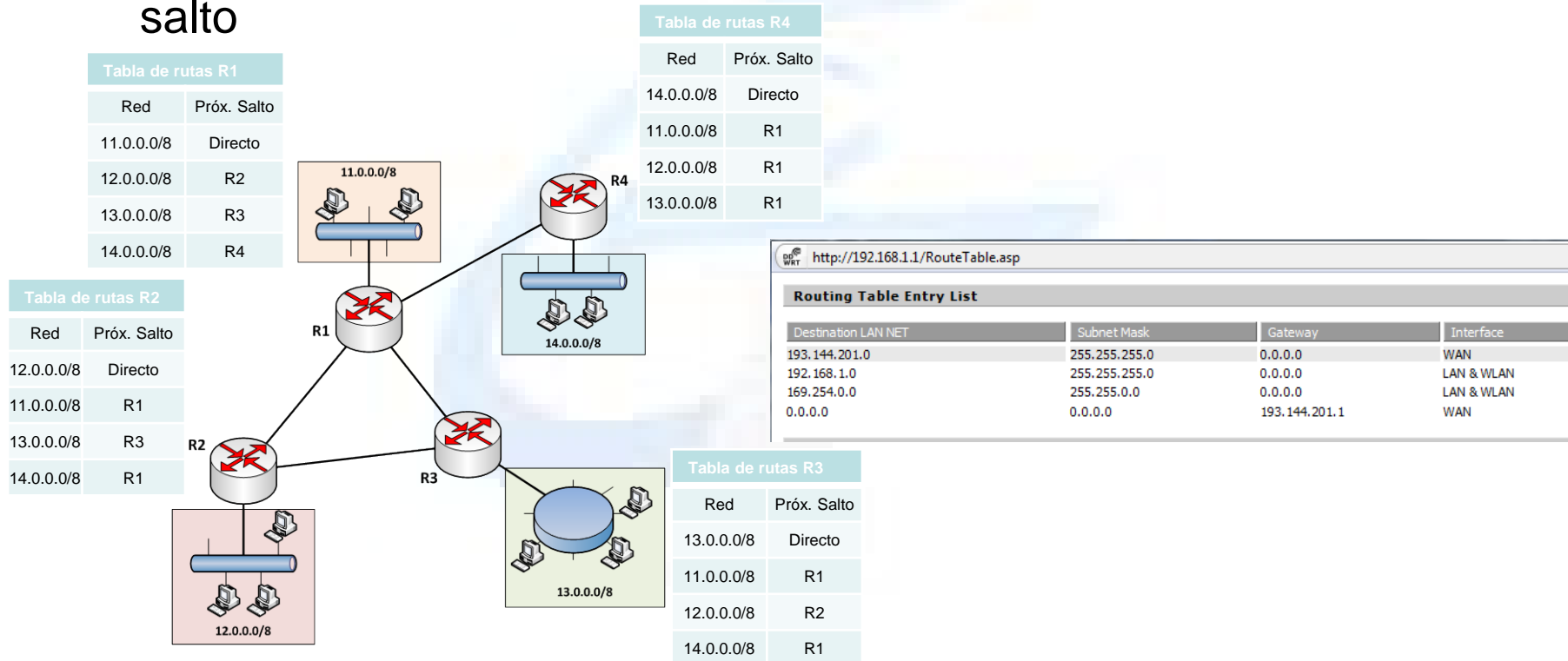
- Búsqueda de la Dirección destino en tabla de enrutamiento
 - Si existe, reenvío al puerto correspondiente.
 - Sino, descarta el paquete.
- Decrementa el contador TTL, actualiza cabecera y checksum.
- Envía el paquete al interfaz de salida.
- Transmite el paquete/trama al enlace.

Enrutamiento: Determinación de Ruta

- **Algoritmos de encaminamiento estático:**
 - Tabla de encaminamiento programada por el administrador de red.
 - Carece de inteligencia para aprender la topología.
 - No contempla modificaciones dinámicas de la red.
- **Algoritmos de encaminamiento adaptativo:**
 - Aprenden por sí mismos la topología de la red.
 - Son más flexibles.
 - Su rendimiento es menor debido a los mensajes de control intercambiados.

Enrutamiento: Tablas de enrutamiento

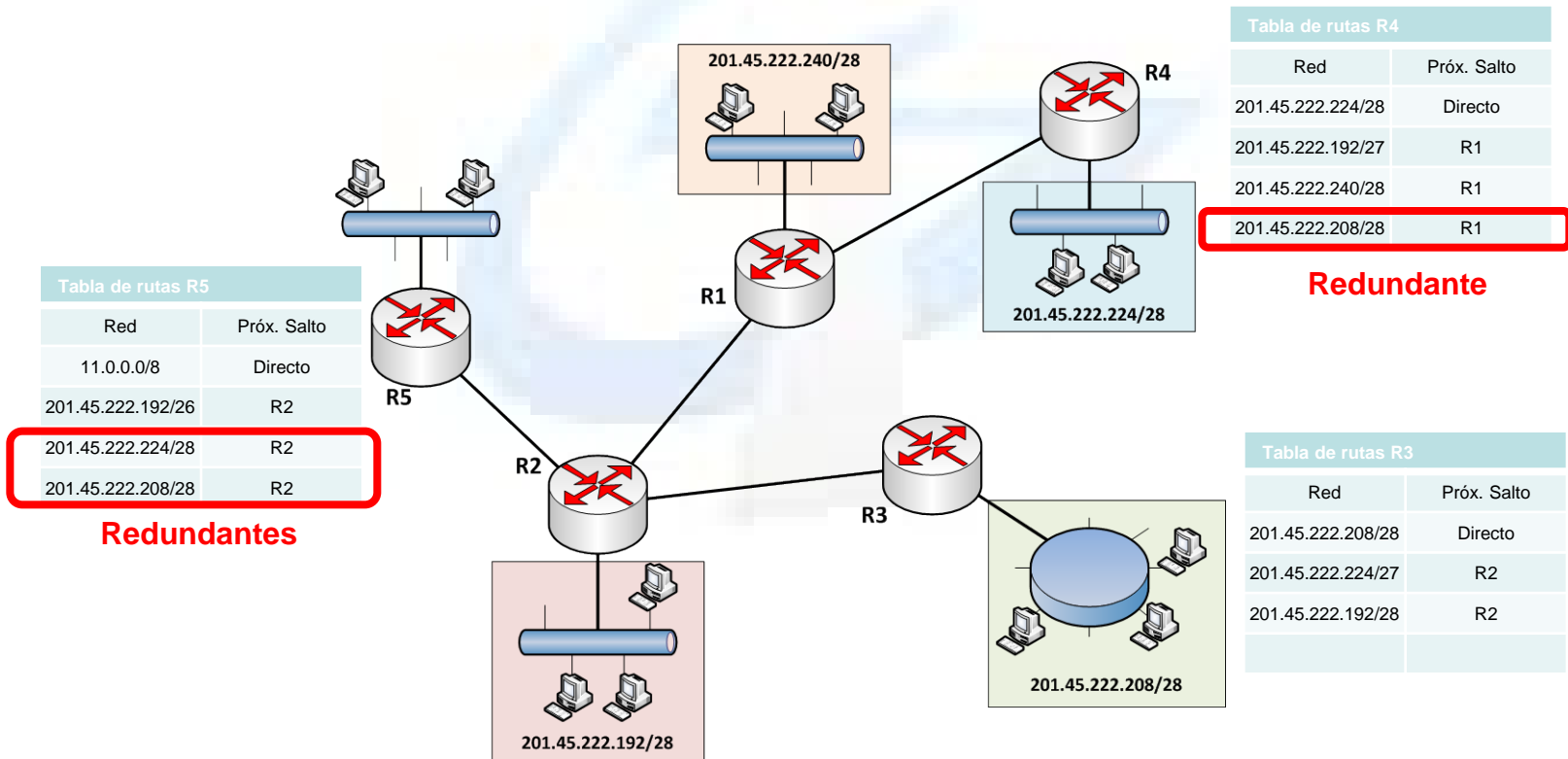
- Los enrutadores mantienen una tabla de rutas donde existe una entrada por cada subred de la que sabe cual es su siguiente salto



- Los nodos también tienen tablas de enrutamiento pero contienen la información de su subred y de su(s) enrutador(s)

Enrutamiento: Tablas de enrutamiento

- Minimizar el número de entradas y evitar bucles
- Se empieza a enrutar por la entrada más restrictiva
- Una entrada con el mismo siguiente salto que otra más genérica es redundante y por lo tanto perjudicial



Capa de Interred: Limites del protocolo IP

Propiedad	Protocolo implementador
Fiabilidad extremo a extremo + Control de flujo	TCP o protocolos de aplicación
Secuenciamiento	TCP
Detección de errores	TCP, UDP u otras capas de transporte
Reporte de errores	ICMP
Información de tablas de ruta	RIP, OSPF, BGP
Escasez de direcciones	Direccionamiento privado (NAT, NAPT)
Resolución de direcciones / nombres	ARP, RARP, DNS
Configuración	BOOTP, DHCP
Multicast	IGMP, MBONE

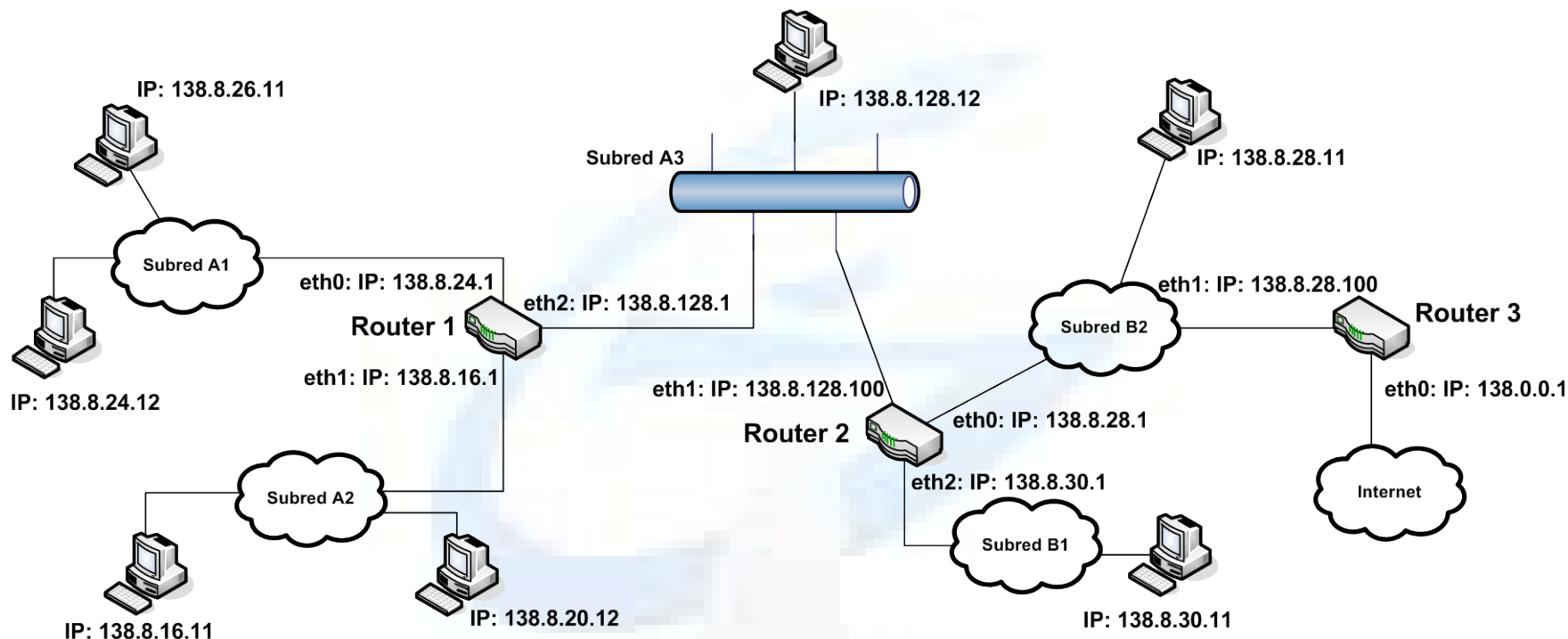
Aplicaciones asociadas a IP: Ping (*Packet InterNet Groper*)^{"Tanteador"} y Traceroute

- Ping usa los mensajes Eco y Respuesta al Eco("Echo", "Echo Reply") de ICMP
- Traceroute permite determinar la ruta que siguen los datagramas IP de host a host
 - Se basa en ICMP
 - Envía un datagrama IP con un tiempo de vida(TTL) de 1 al host de destino
 - El primer "router" que vea el datagrama decrementará el TTL a 0 y devolverá el mensaje ICMP "Tiempo excedido"("Time Exceeded"), además de eliminar el datagrama
 - Este proceso se repite sucesivamente incrementando el TTL en cada iteración con el fin de identificar la serie de "routers" que se encuentran en el camino hasta el host de destino

Arquitectura TCP/IP



Enrutamiento: Ejercicios (I)



Dirección de red	Máscara	Dirección de Broadcast	Rango de direcciones
138.8.128.0	/17	138.8.255.255	138.8.128.1 – 138.8.255.254
138.8.16.0	/21	138.8.23.255	138.8.16.1 – 138.8.23.254
138.8.24.0	/22	138.8.27.255	138.8.24.1 – 138.8.27.254
138.8.28.0	/23	138.8.29.255	138.8.28.1 – 138.8.29.254
138.8.30.0	/23	138.8.31.255	138.8.30.1 – 138.8.31.254

Enrutamiento: Ejercicios (I)

Router 1:

Destino	Máscara	Próximo Salto	Interfaz

Router 2:

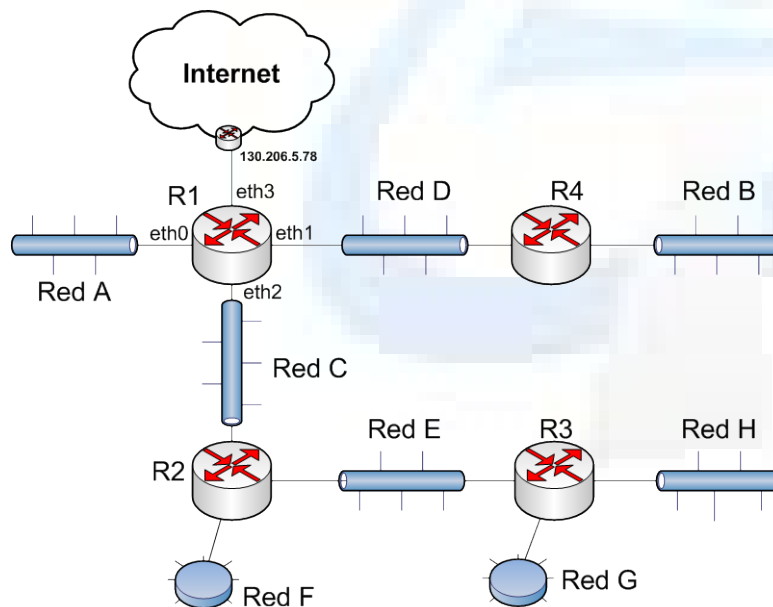
Destino	Máscara	Próximo Salto	Interfaz

Router 3:

Destino	Máscara	Próximo Salto	Interfaz

Enrutamiento: Ejercicios (II)

- Sea la red de un departamento la que se muestra en la siguiente figura:



	Dirección de Red	Máscara (Prefijo)
A	192.168.0.0	/27
B	192.168.0.32	/28
C	192.168.0.84	/30
D	192.168.0.48	/28
E	192.168.0.104	/29
F	192.168.0.96	/29
G	192.168.0.88	/29
H	192.168.0.112	/28

Enrutamiento: Ejercicios (II)

- **Completar la configuración (con el menor número de entradas posible) de la tabla de rutas de R1**, de forma que se pueda alcanzar cualquier equipo de la red. Si fuera necesario, asignar direcciones IP a los routers según convenga para poder rellenar la tabla.
- Utilizar el siguiente formato para la tabla de rutas:

Router: R1			
Destino (Red)	Máscara	Próximo Router (Dirección IP)	Interfaz
0.0.0.0	/0	130.206.5.78	eth3