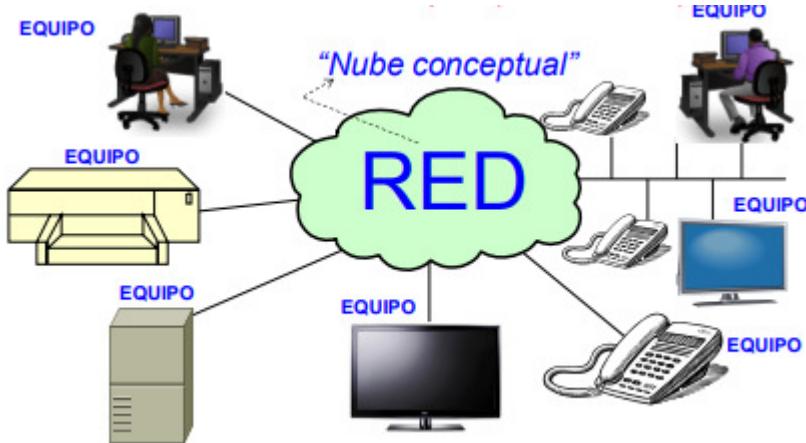


1. Redes y arquitecturas
2. Arquitecturas estructuradas de comunicaciones
3. Arquitectura TCP/IP
4. Nivel de enlace
5. Nivel de red

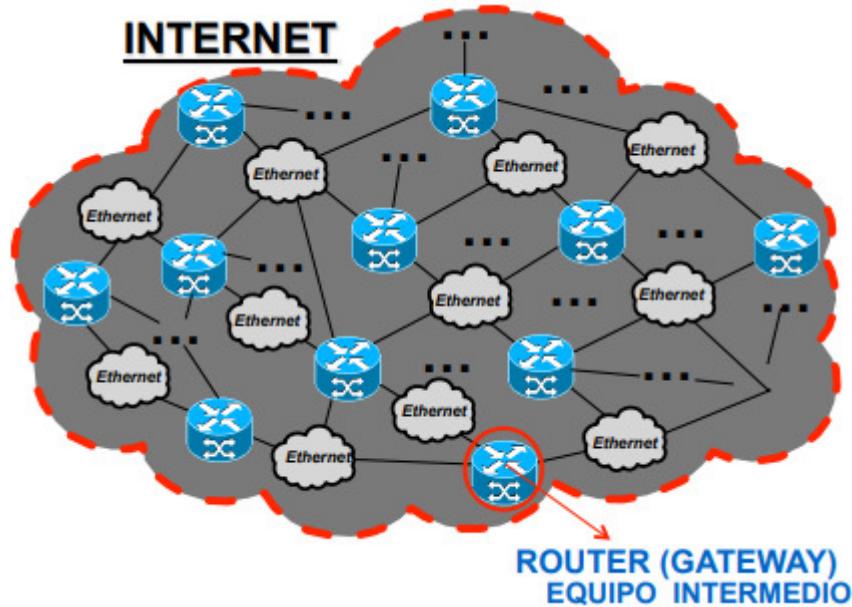
## 1. Redes y arquitecturas:



Para que dos sistemas compartan información, deben “hablar el mismo idioma”. Ese “idioma” es el **protocolo**: conjunto de reglas que rigen una comunicación entre sistemas.

- a. **Red**: medio físico de comunicación y compartición de recursos de información y computación entre equipos.
- b. **Sistema o equipo**: cualquier dispositivo conectado a una red, con una dirección en dicha red y capaz de “hablar un mismo idioma” con otros equipos conectados a la misma red mediante mensajes pertenecientes a un mismo conjunto de protocolos de comunicaciones.
  - i. **Dirección de red**: identificador de cada dispositivo conectado en red.
- c. **Dos tipos de redes para conectar equipos**:
  - i. **Redes de Comunicaciones (redes físicas)**: permiten conectar directamente a los equipos de usuarios.
    - 1. **Ejemplo**: red de cable Ethernet o una red inalámbrica WiFi.
  - ii. **Redes de Computadoras (redes abstractas)**: redes lógicas o virtuales, formadas por un número indeterminado de redes de comunicaciones. Es un

conjunto de redes físicas (**Ethernet**) unidas por **router** (equipo intermedio).



- a. **Internet:** inmensa red de computadores con tecnología TCP/IP y formato IP de direccionamiento común.
- b. **Router:** encamina paquetes de datos en función de la dirección Internet del equipo final destinatario.
- c. **Dos tipos de equipos:**
  - i. **Equipos intermedios:** se ocupan de **encaminar** la información dentro de una red.
    - 1. **Ejemplo:** router (enrutador o encaminador).
  - ii. **Equipos finales:** los que transmiten y reciben la información.
    - 1. **Origen y destino:** situados en los extremos de una comunicación.
    - 2. Conectados a un router de la red de computadoras (internet).
  - iii. Los equipos finales e intermedios deben compartir un protocolo y un formato de direccionamiento comunes al comunicarse.
- d. **Organización de Centros de Control en Internet:**
  - i. **Para gestionar la evolución tecnológica de Internet:**
    - 1. **IAB (Internet Advisory Board):** certifica los estándares.
    - 2. **IETF (Internet Engineering Task Force):** desarrolla protocolos.



- 2. **IETF (Internet Engineering Task Force):** desarrolla protocolos.



I E T F®

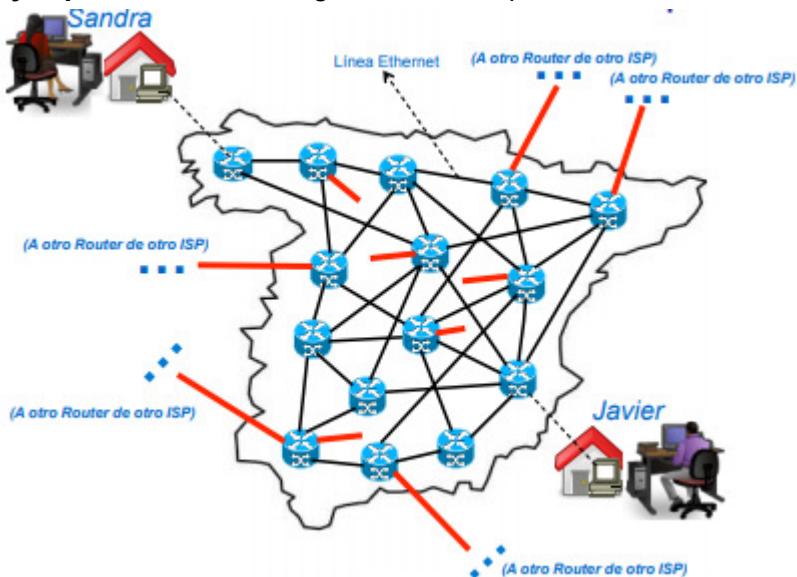
3. **IANA (Internet Assigned Numbers Authority)**: asigna recursos (por ejemplo, direcciones de los equipos conectados a Internet).



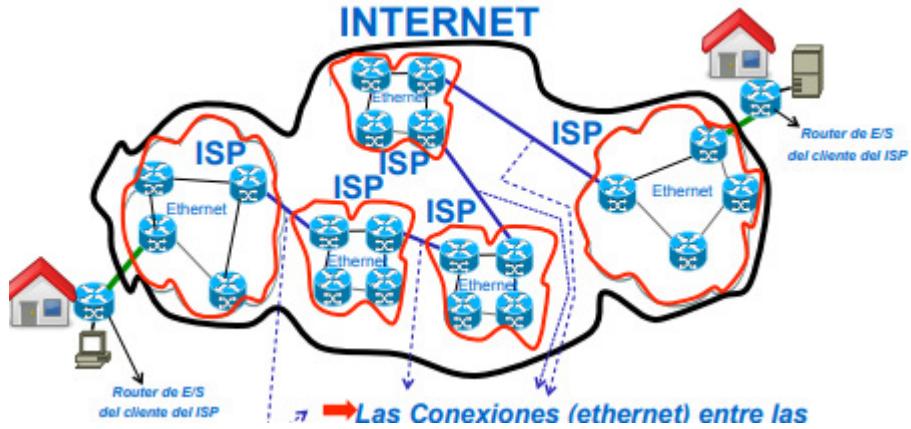
4. Los protocolos de comunicaciones, servicios y otras informaciones TCP/IP se publican en **RFCs (Request For Comments)**, cuyo editor es un miembro de la **IAB**.
- ii. **Acceso a Internet:**
- ISPs (Internet Service Providers)**: operadores de telecomunicaciones (Orange, Movistar, Vodafone, ...) que ofrecen servicios de Internet gracias a su infraestructura (red de routers distribuida por el país).



2. **Ejemplo:** red de un ISP genérico en España

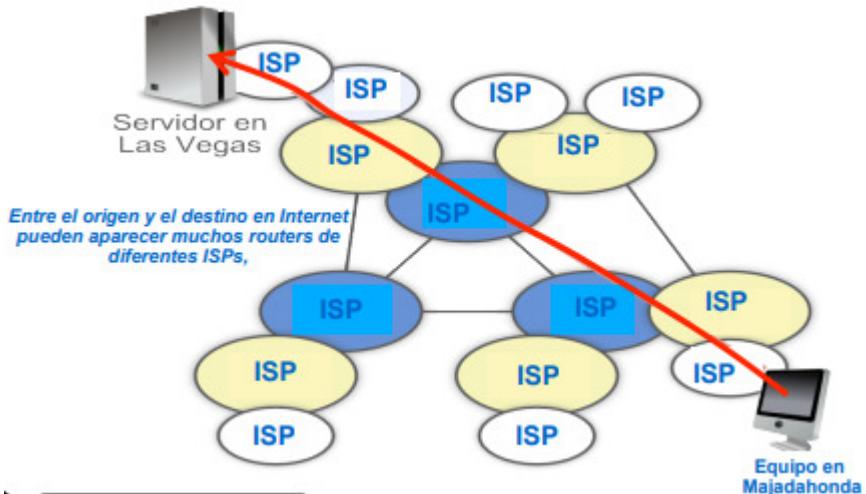


### 3. Ejemplo: red de ISPs distintas

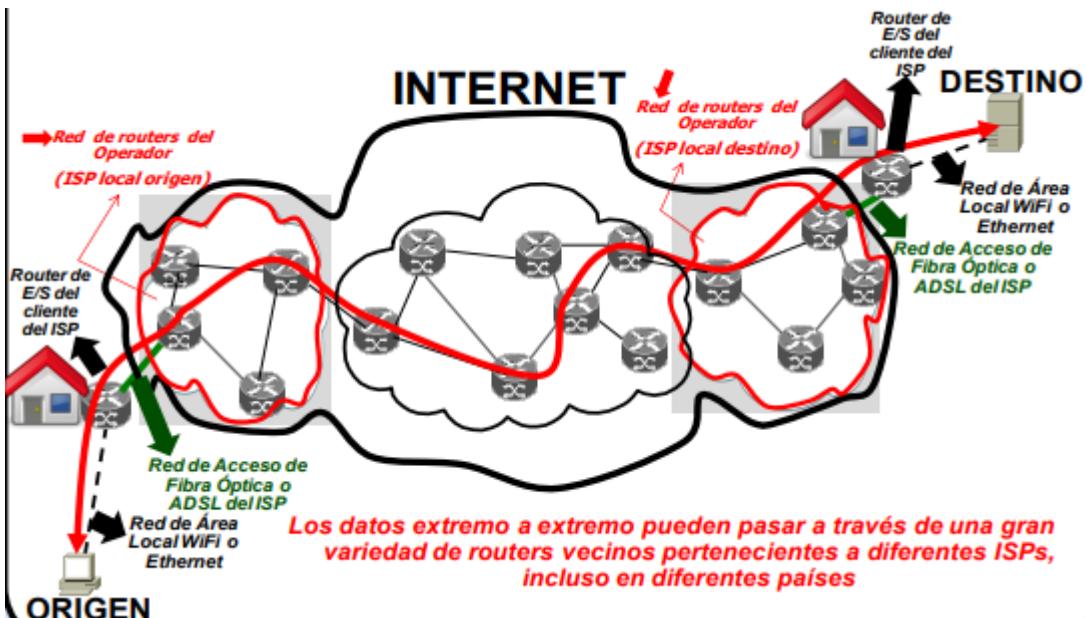


- a. Las conexiones Ethernet entre las redes de routers de distintas ISPs permite la formación de la Red Virtual Internet.

### 4. Ejemplo: comunicaciones extremo a extremo en Internet

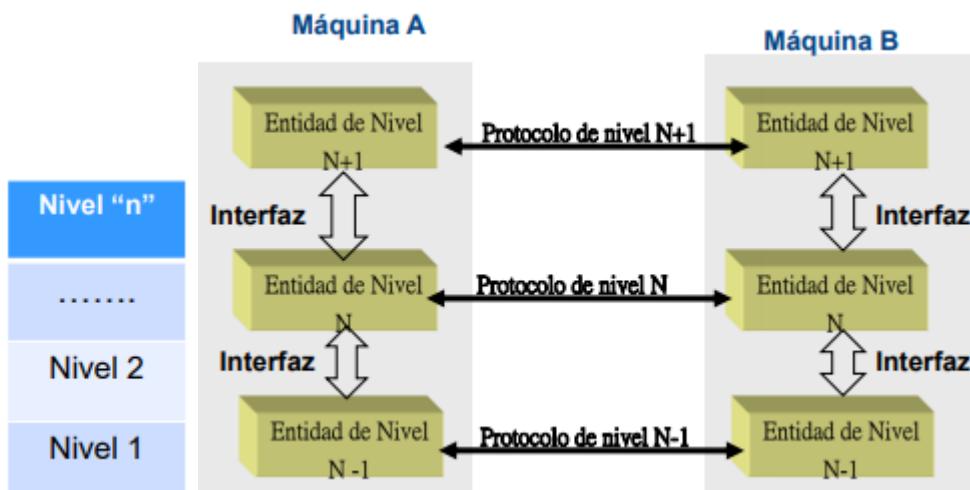
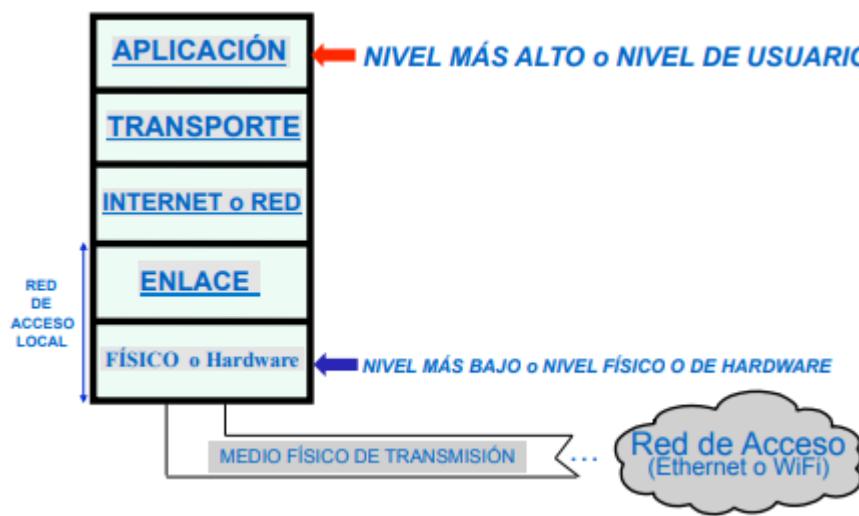


#### f. Tipos de red:



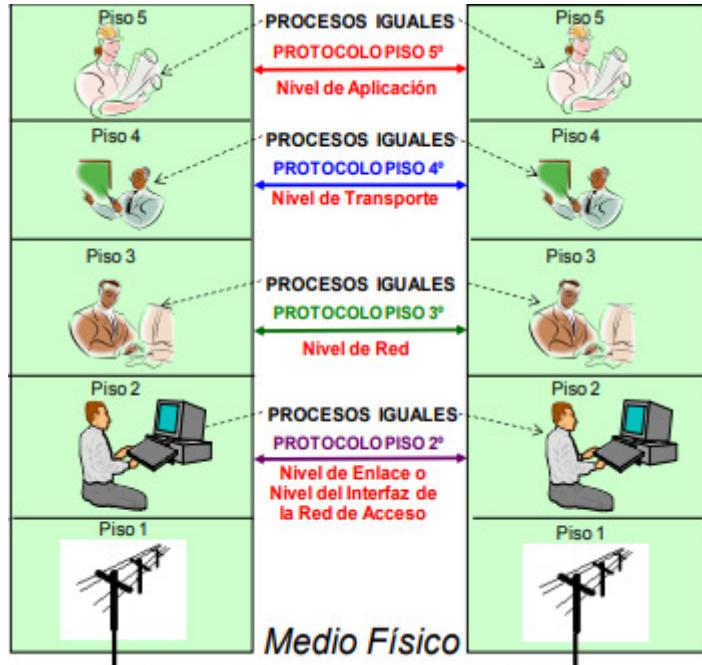
- i. **Red interna de acceso:** comunicación entre equipo y router de E/S del cliente del ISP.

1. Red de Área Local WiFi o Ethernet.
  - ii. **Red externa de acceso:** comunicación entre router del cliente y routers del ISP.
    1. Red de Acceso de Fibra Óptica o ADSL del ISP (cableado en las fachadas de edificios o en alcantarillas).
  - iii. **Red interna de routers de los ISPs:** Internet.
- g. Definiciones de Internet:**
- i. **Tecnológicamente:** red de computadoras TCP/IP.
  - ii. **Socialmente:** red democrática, descentralizada y sin dueño (la red Ethernet de routers de un ISP es ajeno al resto de redes ISPs).
- h. Números en Internet:**
- i. Más de 200 países conectados.
  - ii. 4.500 millones de usuarios de Internet en todo el mundo (58%).
  - iii. 33 millones de usuarios de Internet en España (70%).
- 2. Arquitecturas estructuradas de comunicaciones:**
- a. **Definición:** conjunto de protocolos de comunicaciones que se ejecutan de forma independiente en diferentes niveles, **exceptuando el nivel físico o de hardware**.
    - i. El nivel físico es el único nivel que no tiene protocolo de comunicaciones.
  - b. **Arquitectura TCP/IP (estructurada en 5 niveles de comunicaciones):**



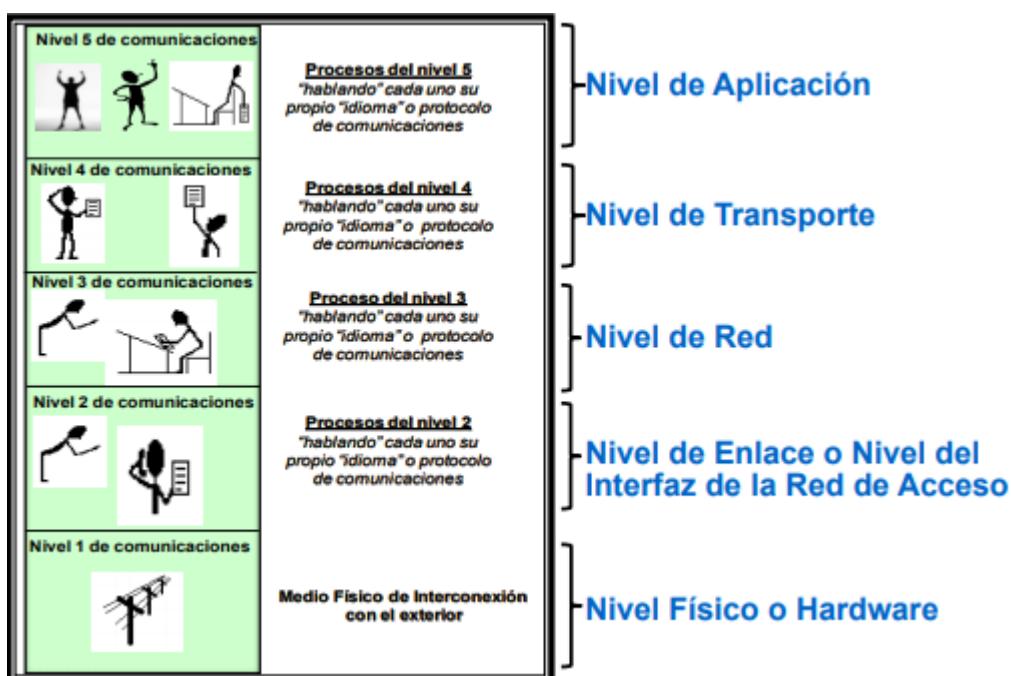
- i. **Estratificación en niveles:**

1. Al ser una estructura más comprensible en diferentes niveles de comunicaciones mutuamente independientes, reduce la **complejidad del desarrollo** y favorece la labor de diseño.
  2. Al ser niveles independientes, facilita el **cambio tecnológico** porque los cambios realizados en un nivel no afectan al resto de niveles.
- ii. **Ejemplo:** edificio de 5 pisos.



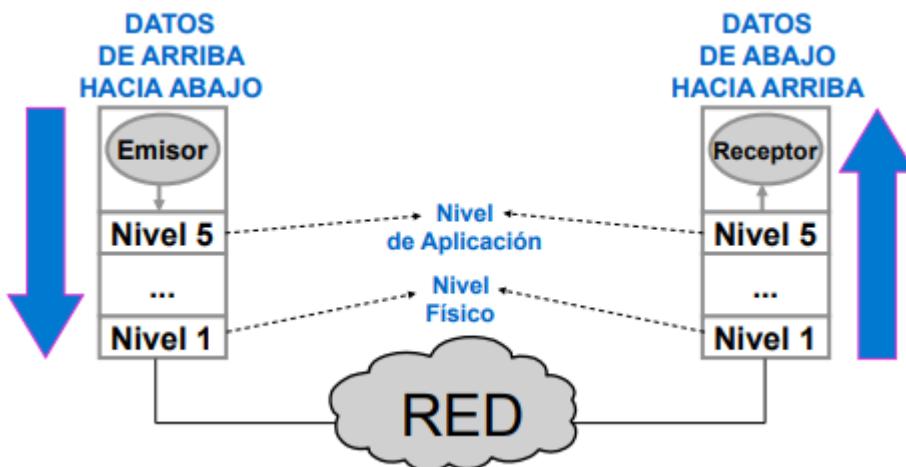
- c. **Protocolo de comunicaciones:** conjunto de reglas que definen el **formato y orden de los unidades de datos** intercambiados entre dos **entidades pares** (dos procesos iguales ejecutándose en equipos diferentes y manejando el mismo protocolo), así como las **acciones** que tienen que llevar a cabo dichas entidades pares para proporcionar un determinado **servicio**.



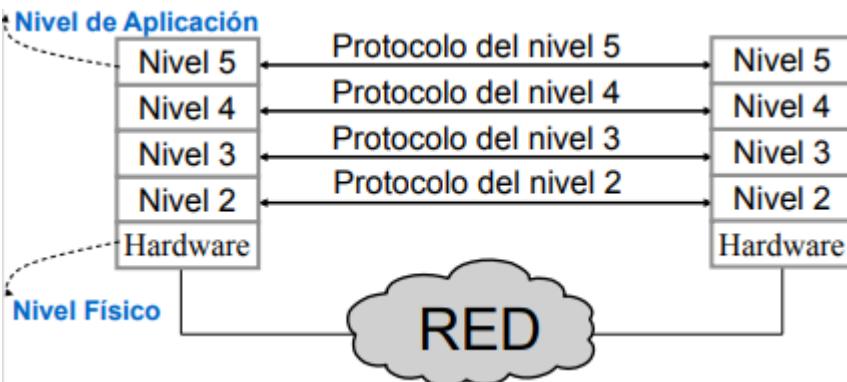


- i. En cada nivel (salvo el físico), puede haber uno o más vecinos o entidades con su propio protocolo de nivel ofreciendo servicios distintos.
- ii. **Nivel de aplicación:** aplicaciones de correo (SMTP, POP3, IMAP, ...), de navegación web (HTTP), de transferencia de ficheros (FTP), etc.
- iii. **Nivel de transporte:** protocolos TCP y UDP.
- iv. **Nivel de red:** protocolo IP → encamina una comunicación hacia la dirección IP destino.
- v. **Nivel de comunicaciones:** entidades Ethernet y WiFi, cada una con su propio protocolo.

d. Comunicación entre distintos niveles de un mismo equipo:



e. Comunicación entre distintos niveles de equipos diferentes:

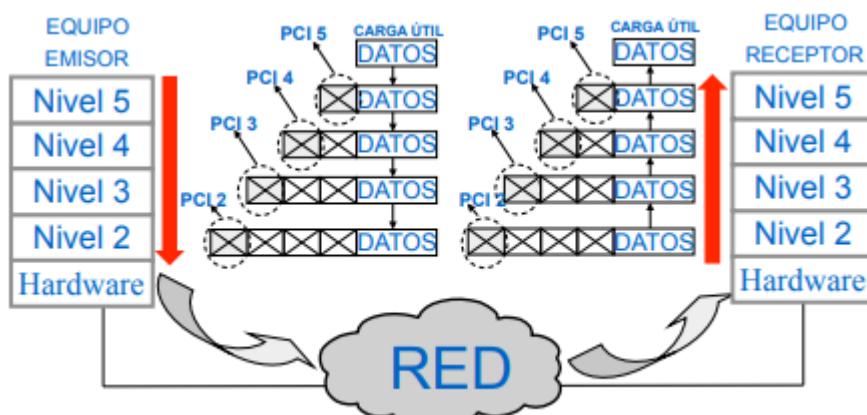


f. Unidad de datos de protocolo (PDU o *Protocol Data Unit*): unidad completa de información intercambiada por entidades pares.

i. Formato: PDU = PCI (cabecera) + SDU (datos)

1. PCI: *Protocol Control Information* = Información de Control de Protocolo
2. SDU: *Service Data Unit* = Unidad de Datos del Servicio.
  - a. Contiene las PCI y SDU de niveles superiores.

g. Encapsulación (arriba-abajo) y desencapsulación (abajo-arriba):



*La comunicación de arriba hacia abajo en el equipo emisor = Añadir cabeceras PCI a los datos de usuario*

*La comunicación de abajo hacia arriba en el equipo receptor = Eliminar cabeceras PCI a los datos de usuario*

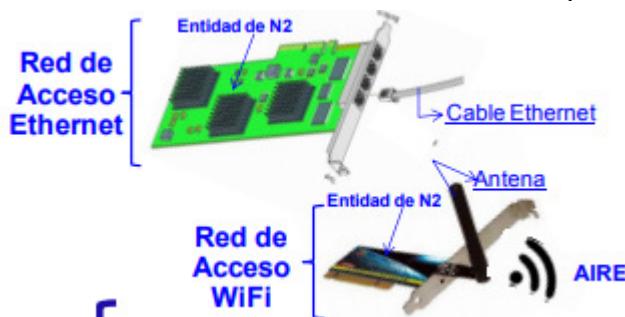
i. Encapsulación: el equipo emisor añade cabeceras PCI (información de control) en cada uno de los niveles salvo en el nivel físico o de hardware.

- ii. **Desencapsulación:** el equipo receptor realiza las **funciones** indicadas en función de la **cabecera PCI** recibida, **elimina dicha cabecera** y **pasa** el resto de cabeceras al **nivel superior**.
- iii. **Ejemplo (envío de un correo electrónico → datos o carga útil):**
  1. **Equipo emisor:** se irán añadiendo cabeceras con información sobre el destinatario del correo (nivel 5 o aplicación), el servicio de transporte (nivel 4 o transporte), la transmisión en la red (nivel 3 o red) y la transmisión de la PDU por red Ethernet (nivel 2 o enlace).
  2. **Equipo receptor:** al nivel 2 llegará una PDU y analizará solo la primera cabecera (nivel 2) para comprobar si es su dirección destino de nivel 2. En caso afirmativo, pasará la PDU sin la cabecera de nivel 2 al nivel superior. El resto de niveles harán lo mismo (cada nivel leyendo su cabecera indicada en el protocolo correspondiente) hasta que el correo (carga útil) pueda ser entregado por el nivel 5 al destinatario.

### 3. Arquitectura TCP/IP:

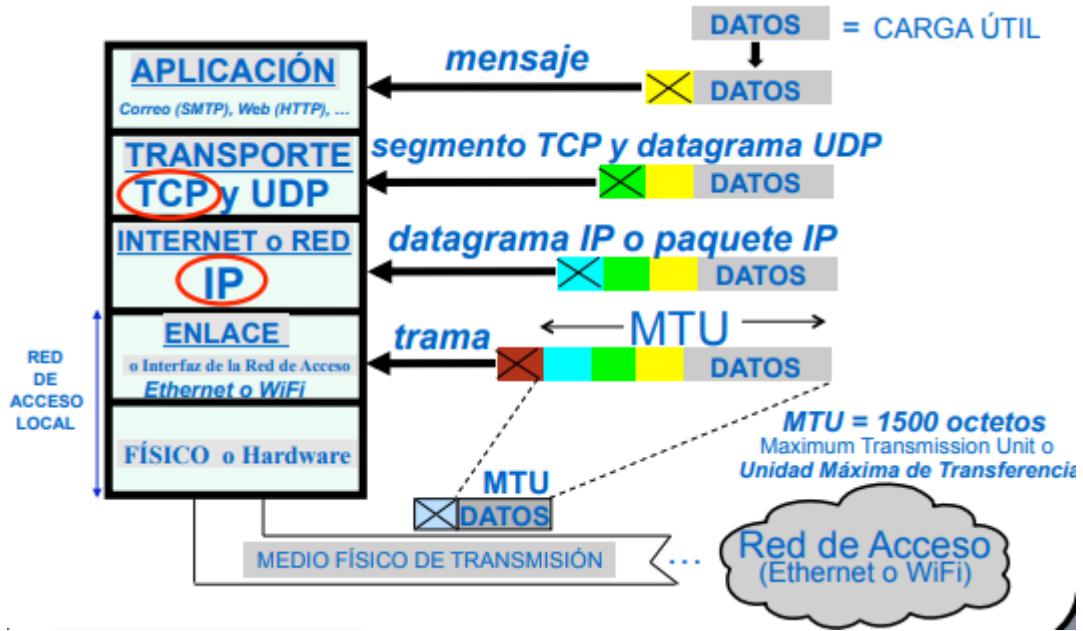


- a. **Red de Acceso Local:** Nivel 2 (**enlace**) + nivel 1 (**físico o hardware**).
- b. **Nivel 2 (enlace):** nivel más bajo de comunicaciones de la arquitectura TCP/IP.
  - i. El nivel de enlace es la **interfaz de la Red de Acceso Local**.
  - ii. **Protocolo de comunicaciones de nivel 2 (enlace):** Ethernet o WiFi.



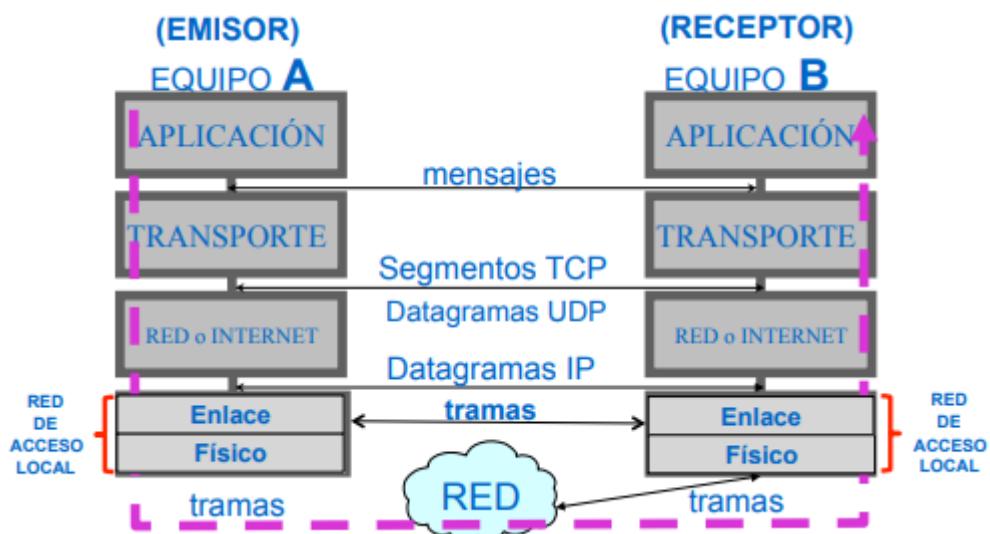
- 1. El equipo intermedio más común es el **router**, con una parte **LAN** (Local Area Network, Ethernet) y otra **WAN** (Wide Area Network, WiFi).

c. Protocolos y formato de las PDUs (cabeceras + datos) en arquitectura TCP/IP:

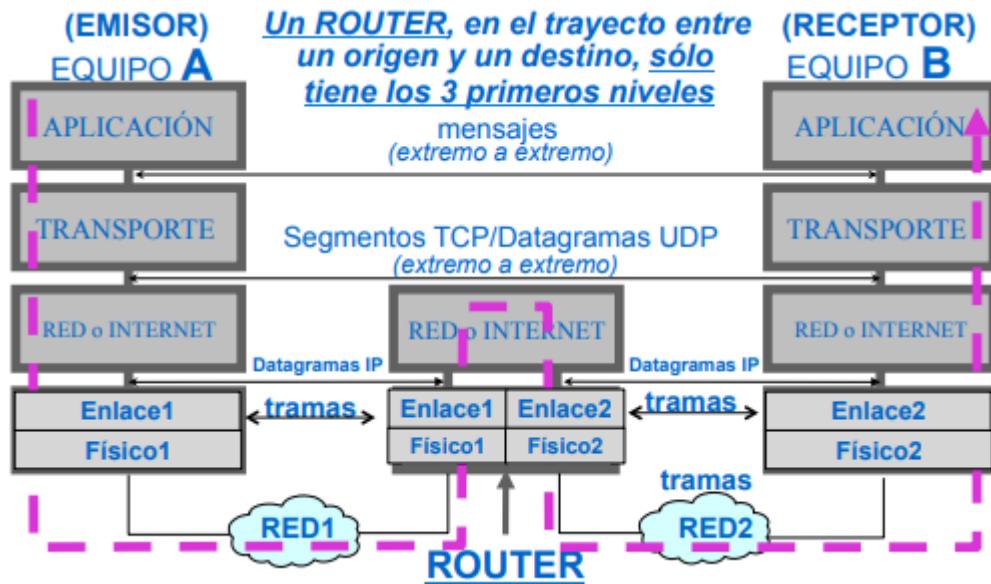


- PDU de nivel de aplicación:** mensaje.
- PDU de nivel de transporte:** segmento TCP y datagrama UDP. TCP y UDP son las dos entidades ejecutadas en el nivel 4 de todo equipo.
- PDU de nivel de Internet o red:** datagrama IP o paquete IP.
- PDU de nivel de enlace:** trama (lo que se transmite por un medio físico).
  - Está compuesto por el PCI de nivel 2 y la **MTU** (*Maximum Transmission Unit* o **Unidad Máxima de Transferencia**), de máximo 1.500 bytes.
  - La **MTU** es el “remolque del camión” en el medio físico de transmisión, siendo el camión la cabecera o PCI de nivel 2.
  - La **MTU** coincide con la capacidad máxima de un **payload** (carga de pago o información neta) transportado en un cable Ethernet.

d. Comunicación entre niveles de equipos vecinos (en la misma red de acceso):

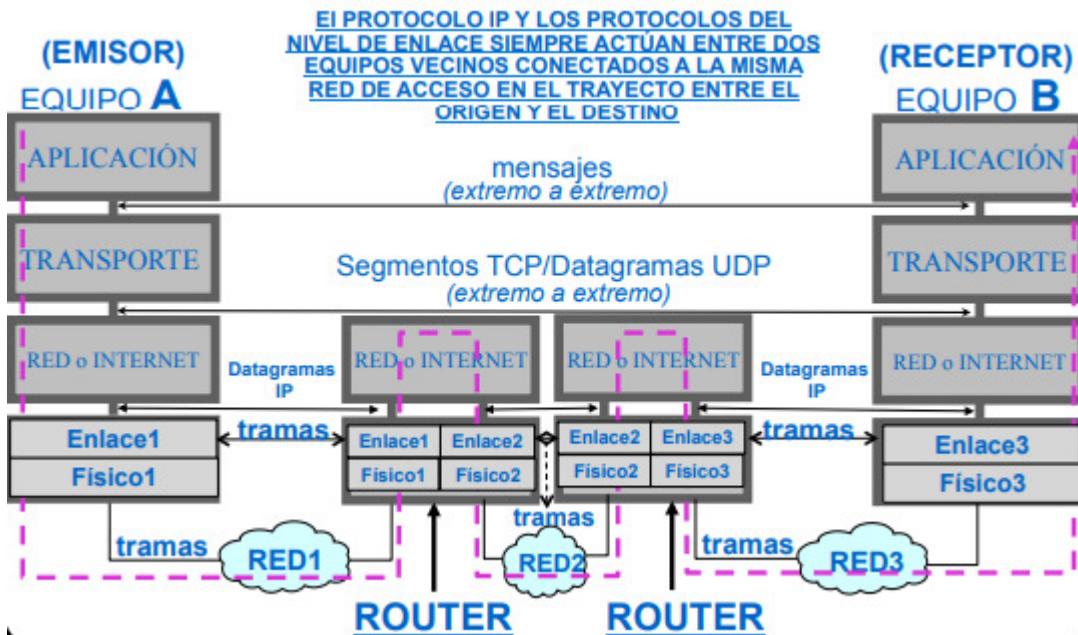


e. Comunicación entre niveles de equipos no vecinos (vía router):

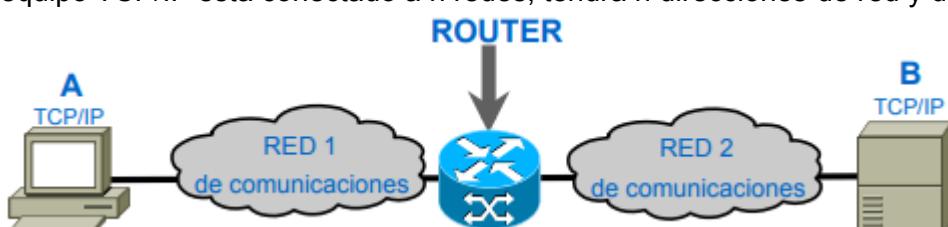


- Router:** solo tiene niveles 1, 2 y 3 (físico, enlace y red) porque su función es **encaminar** por Internet hacia un destino con la mayor rapidez posible.
- Por la **arquitectura de 3 niveles del router**, los protocolos IP y los de nivel de enlace (Ethernet o WiFi) solo actúan entre equipos vecinos.
- Extremo a extremo:** protocolo que puede actuar entre equipos no vecinos.

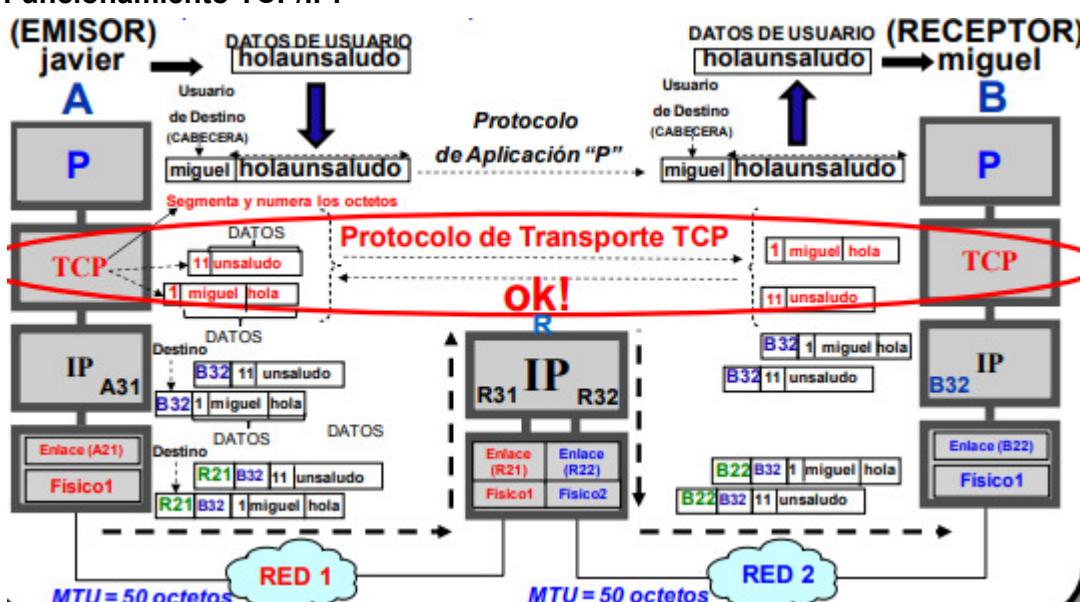
f. Comunicación entre niveles de equipos no vecinos (vía dos routers):



- g. Número de direcciones de nivel de enlace y nivel de red de un equipo: si un equipo TCP/IP está conectado a n redes, tendrá n direcciones de red y de enlace.



- i. **Equipos A y B:** tienen una dirección de enlace y otra de red para RED 1 y RED 2, respectivamente.
  - ii. **Router:** tiene dos direcciones de enlace y otras dos de red, una dirección de cada por cada red de comunicaciones a la que está conectado.
- h. **Funcionamiento TCP/IP:**



- i. **Datos de usuario:** *holaunsaludo* (mensaje).
- ii. **Protocolo de aplicación (genérico P):** añade la cabecera de aplicación (PCI de nivel 5) a la carga útil indicando el **usuario de destino**.
- iii. **Protocolo de transporte (TCP):** asegura el transporte fiable de los mensajes de aplicación **extremo a extremo**.

1. **Enumera** los bytes (octetos) del mensaje (PDU nivel 5).

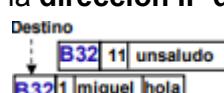


2. **Segmenta** el mensaje para poder transmitirlo por el medio físico por unidades **respetando la MTU** (50 bytes). Para ello, tiene en cuenta que las **cabeceras TCP e IP** tienen ambas **20 bytes** siempre.
  - a.  $MTU (50 B) \geq$  mensaje (10 B) + PCI TCP (20 B) + PCI IP (20 B)
3. **Añade** como cabecera de cada segmento el índice de su primer byte.



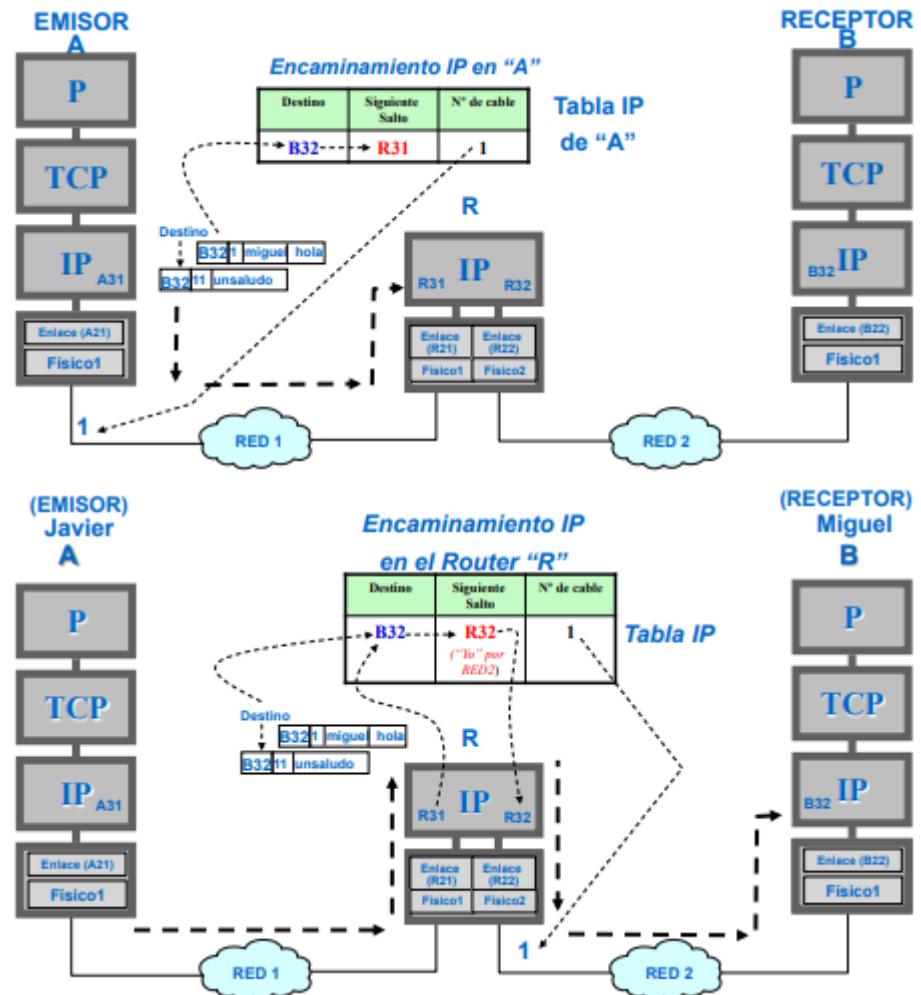
4. **Equipo destino:** ordena el mensaje que le llega por los índices de las cabeceras.

- iv. **Protocolo de red (IP):** añade la cabecera de red al segmento TCP indicando la **dirección IP del equipo destino** (ejemplo: B32 = equipo B, nivel 3, red 2).



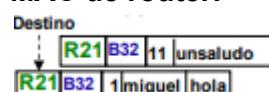
1. **Encaminamiento IP:** la **dirección IP destino** (cabecera) permitirá saber cuál es el siguiente equipo por el que pasar gracias a la **tabla IP**

del equipo emisor.

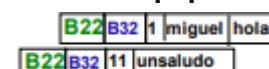


- v. **Protocolo de enlace (Ethernet o WiFi):** añade la cabecera de enlace al datagrama o paquete IP indicando la **dirección de Nivel de Enlace (MAC)** del equipo destino en la **misma red de acceso**.

1. **MAC de router:**

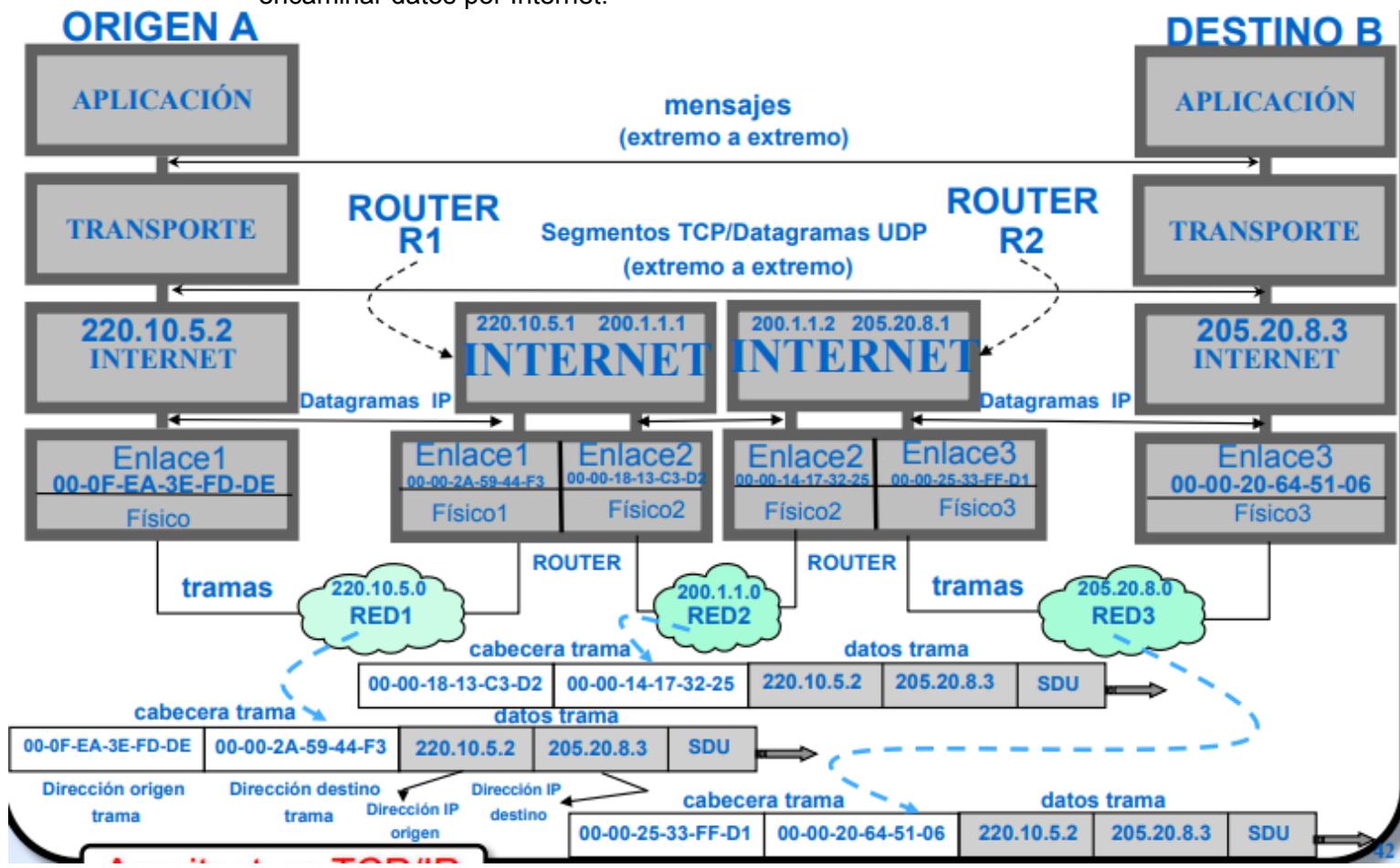


2. **MAC de equipo B:**



- i. **Dirección de nivel de enlace o MAC (Media Access Control):** asignada físicamente a la tarjeta de red del equipo (final o intermedio). Dirección invariable.
- i. **Formato:** 6 bytes en hexadecimal.
    1. **Ejemplo:** 00:0F:EA:3E:FD:DE
    2. **Primeros tres bytes (24 bits):** asignados por **IEEE** (Institute of Electrical and Electronics Engineers).
    3. **Últimos tres bytes (24 bits):** asignados por el fabricante de la tarjeta (Cisco, 3COM, Intel, ...).
  - ii. **Uso:** puntos contiguos en una red de área local (Ethernet o WiFi).
  - iii. La dirección MAC es **igual** independientemente de la red a la que se conecte.
  - iv. **Analogía:** el DNI (**identificador**) de una persona.

- j. **Dirección de nivel de red o IP (*Internet Protocol*)**: asignada a cada equipo por el administrador de la red a la que esté conectado. Dirección variable.
    - i. **Formato:** 4 bytes en decimal (0 - 255).
      - 1. **Ejemplo:** 220.10.5.0 (prefijo de red)
      - 2. Un equipo en esa red podrá tener como dirección IP la 220.10.5.x
    - ii. **Uso:** en Internet, sin importar la ubicación física del destinatario.
    - iii. El equipo tendrá **distintas** direcciones IP según la red a la que se conecte.
    - iv. **Analogía:** domicilio (**lugar de ejecución** de proceso TCP/IP) de una persona
  - k. **Diferencias entre dirección MAC y dirección IP**: ambas son necesarias para encaminar datos por Internet.

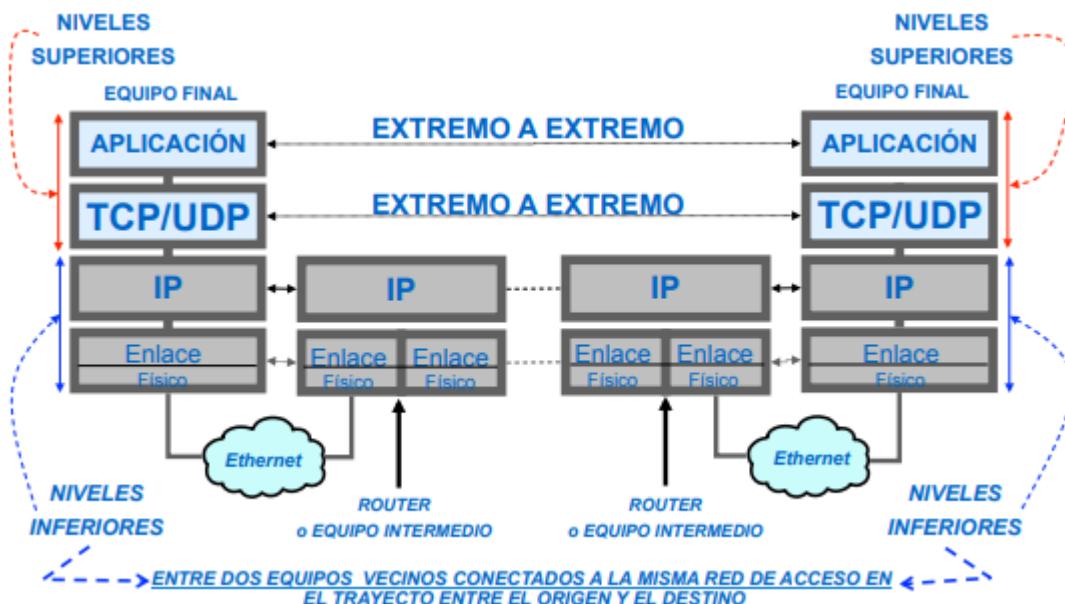


- (foto)

  - i. La **cabecera de la trama** contiene la **dirección MAC** origen y destino **en una misma red de comunicaciones**, no en Internet. Cambian en el trayecto origen-destino en Internet, pero no en una misma red de comunicaciones.
  - ii. La **cabecera del paquete IP** contiene la **dirección IP** origen y destino **en Internet**, no en una red de comunicaciones. No cambian en el trayecto origen-destino ni en una misma red de comunicaciones ni en Internet.
    - 1. Las direcciones están determinadas por el prefijo de red
  - iii. La **SDU** del paquete IP contiene el segmento TCP.
  - iv. **Ejemplo:** la comunicación entre un equipo en Madrid y otro en Sydney usará una **dirección MAC** por cada equipo involucrado en la transferencia de datos entre el equipo origen y el equipo destino; mientras que solo se utilizarán **dos direcciones IP**, la del equipo origen y la del equipo destino.

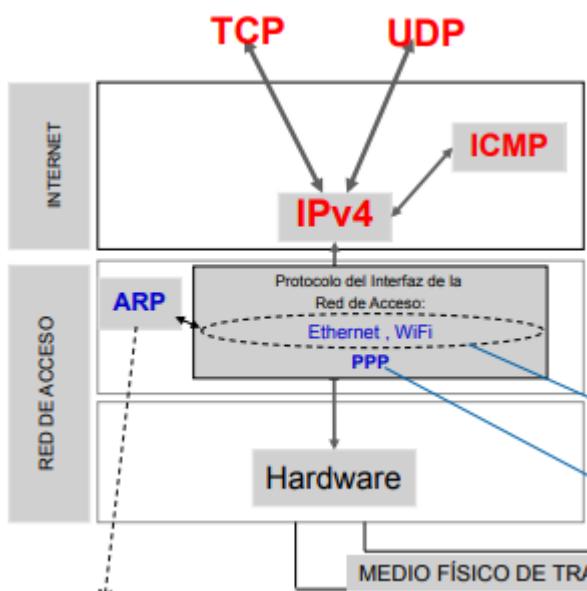
- I. **ipconfig /all** (**ipconfig -all**): comando TCP/IP que muestra todas las configuraciones de nivel 3 y nivel 2 manejadas en todas las interfaces de E/S de nuestro equipo. Si nuestro equipo está conectado a 5 redes Ethernet, por ejemplo, aparecerán todas las direcciones de las 5 interfaces (a nivel 3 como nivel 2).

**m. Niveles superiores e inferiores de la arquitectura TCP/IP:**



- i. **Niveles superiores:** sus cabeceras solo serán analizadas por su entidad par en el otro extremo de la comunicación (**extremo a extremo**). Es el caso de los niveles de transporte (4) y de aplicación (5).
- ii. **Niveles inferiores:** niveles con **entidades intermedias** (equipos contiguos o vecinos) en un trayecto origen-destino en Internet. Es el caso de los niveles de red (3), de enlace (2) y de hardware (1).

1. **Protocolos de niveles inferiores:** actúan entre dos equipos vecinos.



a. **Nivel de red:**

- i. **IP:** para el **encaminamiento** de paquetes IP en Internet.

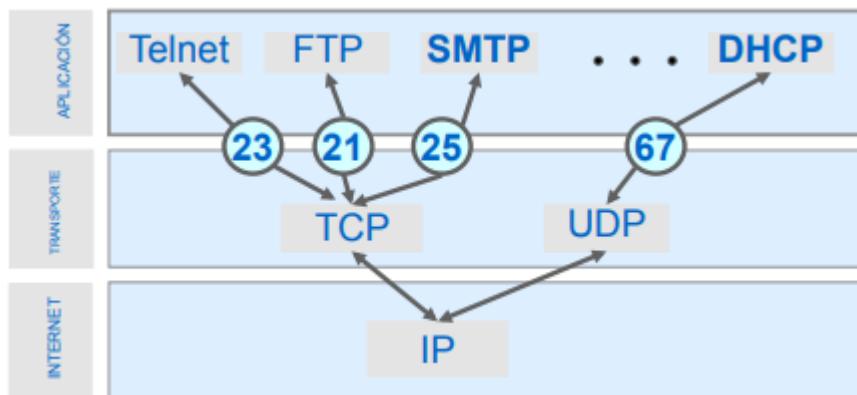
- ii. **ICMP**: para el envío de **mensajes de control** en Internet, generalmente cuando surge un problema con IP (ejemplo, consultar por qué se ha tirado un paquete IP válido).
- b. **Nivel de enlace**:
  - i. **Protocolo de Interfaz de la Red de Acceso**: redes de difusión 1:N (Ethernet y WiFi) y líneas serie o punto a punto 1:1 (PPP: cable de cobre telefónico ADSL y fibra óptica).
  - ii. **ARP**: permite obtener la dirección MAC asociada a la dirección IP de un equipo vecino en una misma red. Está en un subnivel superior a los protocolos de Ethernet y WiFi.
- c. **Nivel de hardware**: no tiene protocolos.

n. **Modelo cliente-servidor para nivel de aplicación (sobre TCP o UDP)**:



- i. **Cliente**: envía al servidor una solicitud específica de servicio.
- ii. **Servidor**: proporciona un servicio como respuesta. En constante “**escucha**”.
- iii. Es el funcionamiento común de la mayoría de aplicaciones en Internet (salvo herramientas TCP/IP como *ipconfig*, *netstat*, *ping*, ...).
- iv. **TCP**: ofrece un servicio **fiable**, pero lento (alta latencia) por las comprobaciones de fiabilidad implementadas en la cabecera de red.
  1. La cabecera TCP ocupa 20 bytes.
  2. **Ejemplo**: enviar correo (protocolo de aplicación SMTP).
- v. **UDP**: ofrece un servicio **rápido** (evita las comprobaciones de fiabilidad TCP).
  1. La cabecera UDP ocupa 8 bytes.
  2. **Ejemplo**: descargar página HTML (protocolo de aplicación HTTP).

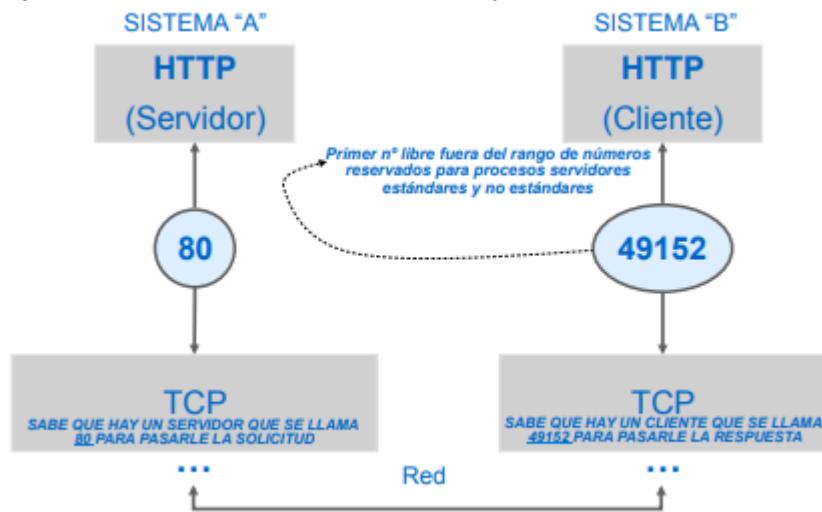
- Número de puerto: identificador de cada proceso cliente y servidor, manejado tanto por TCP como por UDP.



- Formato:** 16 bits en decimal (entero positivo) (0 - 65.535).
  - El campo nº de puerto origen y el nº de puerto destino de la cabecera TCP o UDP es de 16 bits.
- IANA:** organización que define los números de puerto.
  - 0 - 1.023:** procesos **servidores estándares** en Internet.
    - Son los mismos números de puerto para todo equipo (sin importar la dirección IP y el protocolo de transporte).
    - Ejemplos:** FTP (21), Telnet (23), SMTP (25), DHCP (67), ...
  - 1.024 - 65.535:** procesos **servidores no estándares** en Internet y procesos **clientes**.

El IAB recomienda asignar los números de puerto de todo equipo así:

  - 1.024 - 49.151:** procesos **servidores no estándares** en Internet de empresas o particulares desarrolladores de software.
  - 49.152 - 65.535:** procesos **clientes** (asignados por el SSOO).
- Ejemplo:** comunicación entre cliente y servidor HTTP remoto.



- Servidor:** protocolo HTTP siempre tendrá nº de puerto 80.
- Cliente:** nº de puerto fuera del rango de procesos servidores.

- p. **Socket (enchufe):** identificador local del extremo de una comunicación en Internet.

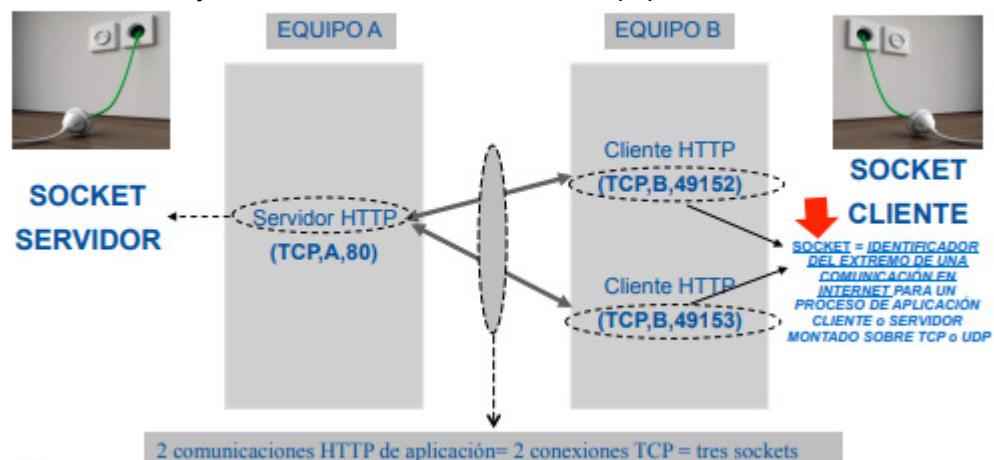


- "Enchufa" el proceso de aplicación con su protocolo de transporte (TCP/UDP)
- Formato:** IP : nº de puerto (socket para TCP o UDP).

**Ejemplo de socket: 138.10.1.16 : 80**

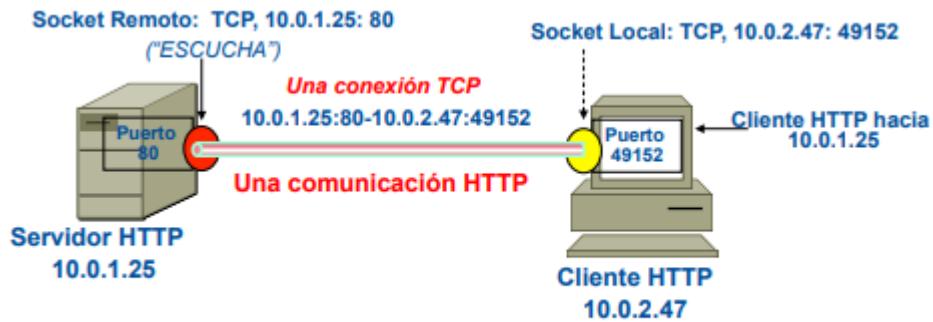


- Proceso cliente:** no puede haber dos procesos cliente con un mismo socket.
- Ejemplo:** identificación de dos comunicaciones de aplicación entre dos clientes HTTP y un mismo servidor HTTP en equipos diferentes.



- Formato conceptual:** socket(protocolo de transporte, dir. IP, nº puerto)
- Comunicación cliente-servidor:** definida por una pareja de sockets.

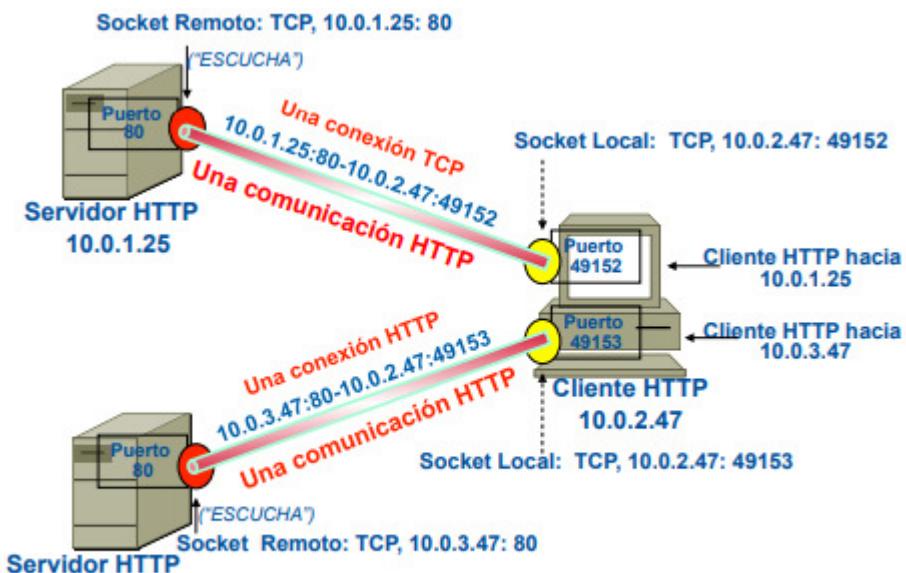
v. Comunicación HTTP vía TCP de un cliente con un servidor:



**Una comunicaciones HTTP, Una conexión TCP y Dos sockets**

1. Ejemplo: un navegador web (cliente) interactúa con un servidor.

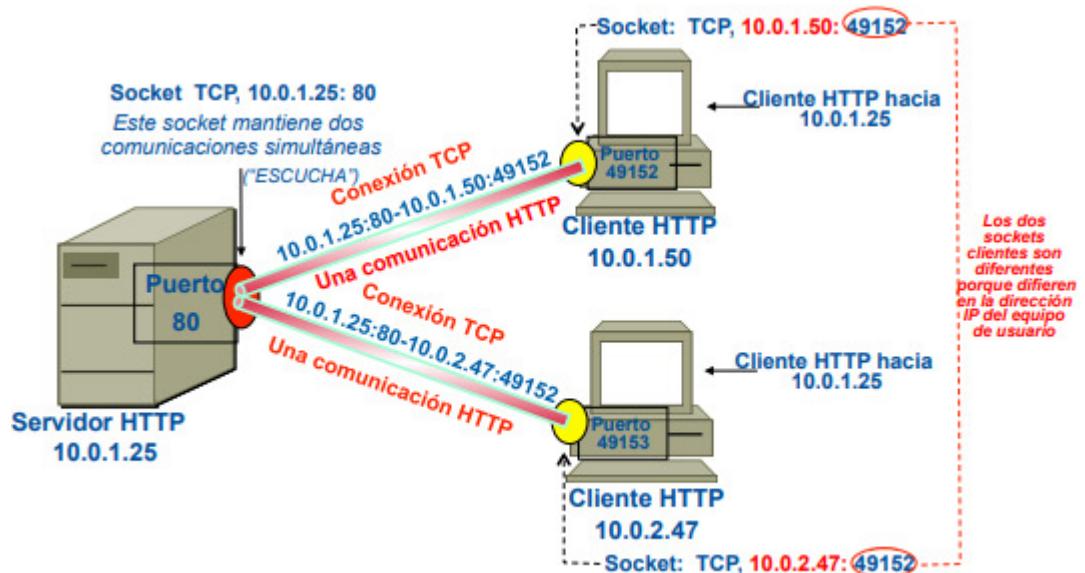
vi. Dos comunicaciones HTTP vía TCP de 2 clientes en un mismo equipo (misma dirección IP) con 2 servidores:



**Dos comunicaciones HTTP, Dos conexiones TCP y Cuatro sockets**

1. Ejemplo: dos navegadores web (cliente) interactúan con dos servidores distintos.

vii. Dos comunicaciones HTTP vía TCP de 2 clientes en 2 equipos distintos con un servidor (misma dirección IP):



**Dos comunicaciones HTTP, Dos conexiones TCP y Tres sockets**

- Ejemplo: dos navegadores web (cliente) interactúan con un mismo servidor.
- viii. **netstat -a -n** → muestra las conexiones activas en un equipo en un momento dado mediante su **protocolo de comunicación**, su **socket local** su **socket remoto** y su **estado** (escuchando, conexión establecida, ...).

```
C:\>netstat -a -n
Conexiones activas

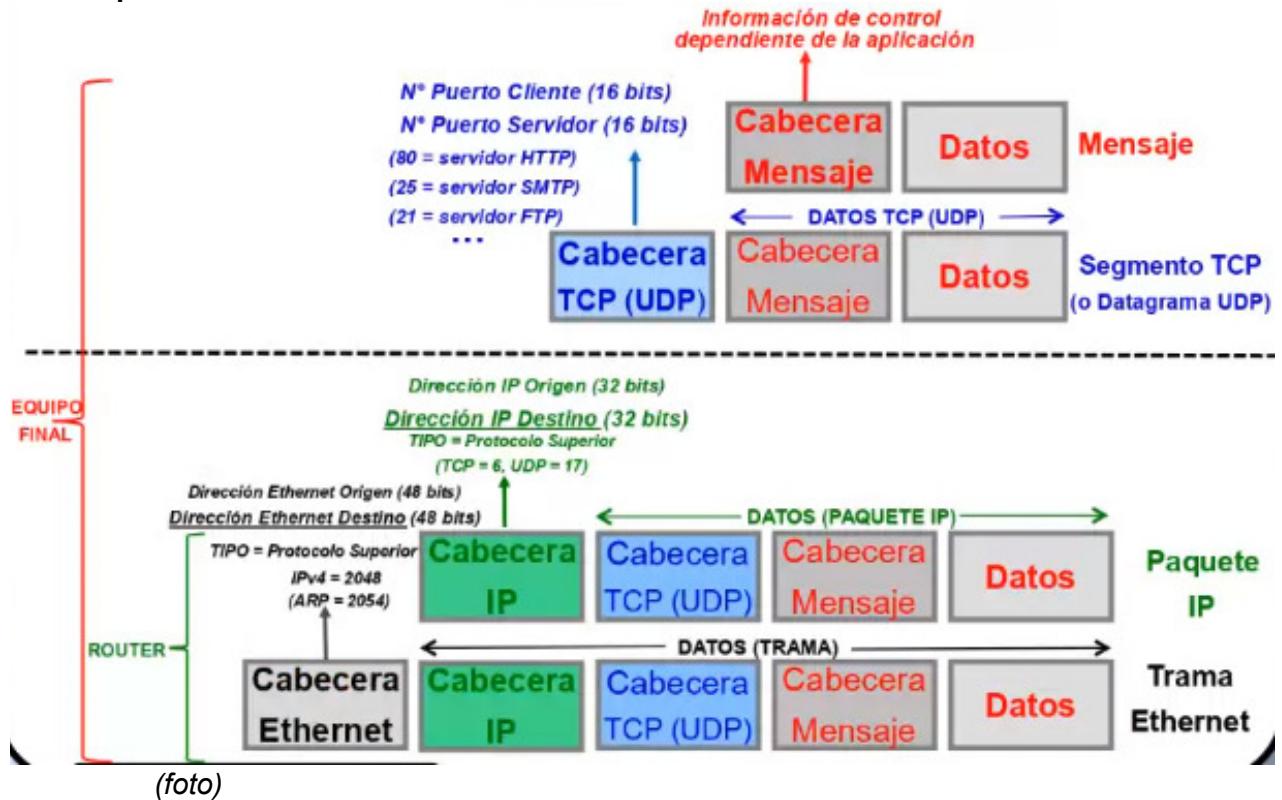
  Proto  Dirección Local          Dirección remota        Estado
  TCP    0.0.0.0:25              0.0.0.0:0             LISTENING
  TCP    0.0.0.0:80              138.100.9.10:12234   ESTABLISHED
  TCP    138.100.10.117:49152   138.100.8.1:143      ESTABLISHED
  UDP    0.0.0.0:2000            *:*                  LISTENING
```

Annotations on the netstat output:

- An arrow points to the first row (TCP 0.0.0.0:25) with the text: "Servidor local SMTP montado sobre TCP en un Equipo a la escucha de cualquier conexión con el equipo local, vía TCP, por cualquier dirección IP local o interfaz de entrada y desde cualquier dirección y puerto de cliente".
- An arrow points to the second row (TCP 0.0.0.0:80) with the text: "Conexión establecida, con el servidor local HTTP, vía TCP, a través de cualquier dirección IP local o interfaz de entrada,".
- An arrow points to the third row (TCP 138.100.10.117:49152) with the text: "Servidor local con nº de puerto 2000 a la escucha de cualquier acceso al equipo local, vía UDP, a través de cualquier dirección IP local o interfaz de entrada y desde cualquier dirección y puerto de cliente".

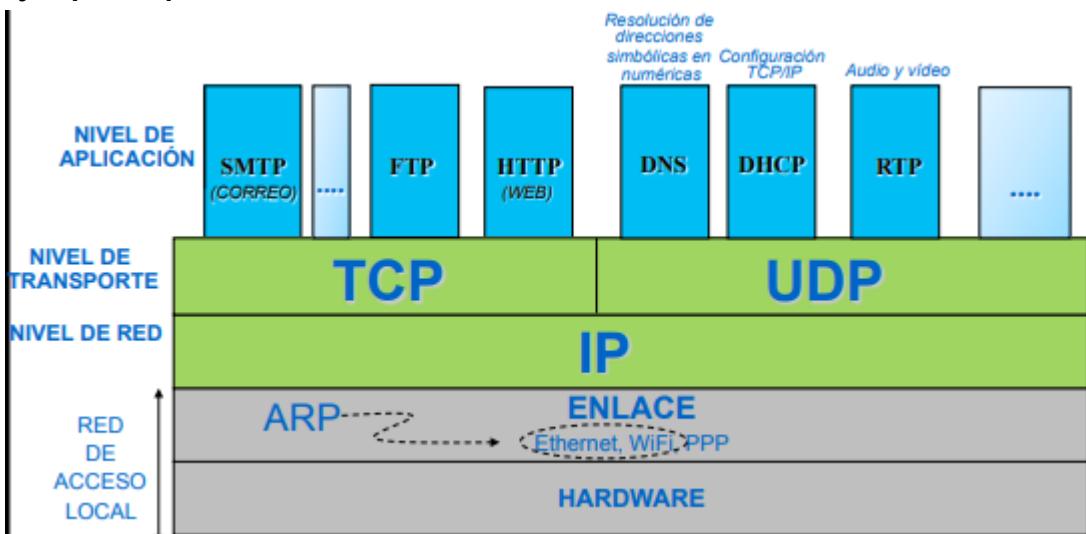
- 0.0.0.0 :** → cualquier dirección IP.
- : 0** → cualquier nº de puerto.
- \*** → metacaracter que indica “cualquiera” (dirección IP o nº de puerto).
- Conexión establecida:** indicada con una pareja única de sockets.

q. Cabeceras de información de control:



- Las tramas Ethernet son las más comunes, pero es igual para tramas WiFi.
- El campo **TIPO** llevará el identificador del protocolo superior.
- La cabecera Ethernet no siempre tiene como TIPO (protocolo superior) el identificador de IP, puede pasar antes por el subnivel ARP que por el nivel IP.

r. Ejemplo Arquitectura TCP/IP:



- DNS:** resolución de direcciones web simbólicas ([www.fi.upm.es](http://www.fi.upm.es)) en numéricas (138.100.243.18). Al introducir la dirección web, la dirección DNS vinculada indicará la dirección IP de la página web para poder acceder.
- DHCP:** protocolo que transporta toda la información de configuración TCP/IP que necesite un equipo de usuario.
- RTP:** protocolo que proporciona extremo a extremo soporte **en tiempo real** de paquetes de audio y vídeo entre servidor y cliente en una aplicación de

**streaming** (proceso que divide los datos multimedia en paquetes que permiten al cliente de streaming que reproduzca el primer paquete mientras decodifica el segundo y recibe el tercero, montado sobre transporte UDP, a diferencia de FTP o HTTP (TCP) que se asegura de recibir, decodificar y reproducir todos los paquetes correctamente).

1. **Ejemplo:** Skype → el protocolo RTP (sobre UDP) procura ordenar los paquetes a medida que llegan, pero no pide que se retransmitan paquetes que se han perdido. En el caso de perder algún paquete de datos de voz, la corrección la realiza el propio cliente diciendo “Se ha cortado, no te he oído”.

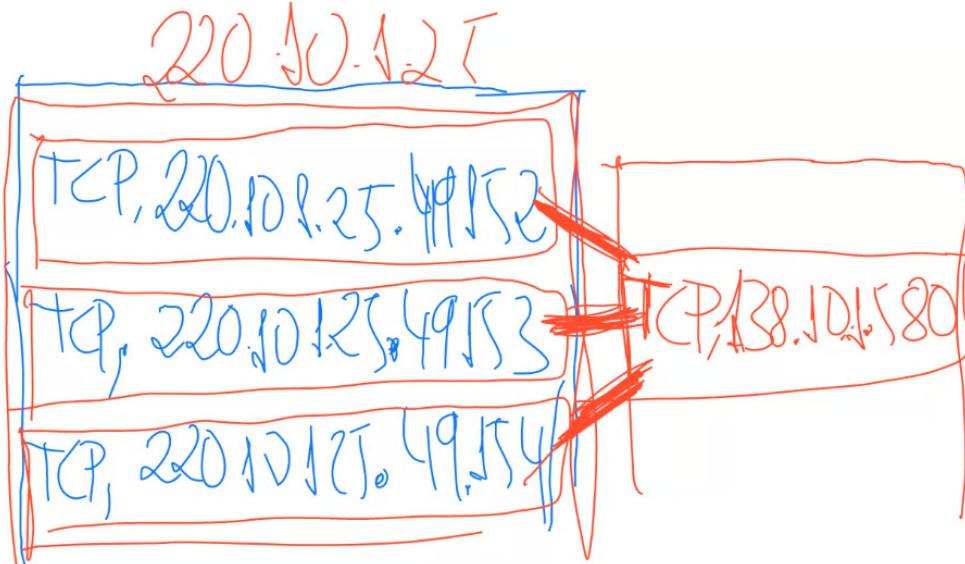
s. **Ejercicios:**

- i. **Siempre que recibe una trama, el proceso que ejecuta el protocolo del nivel de enlace de un router:**

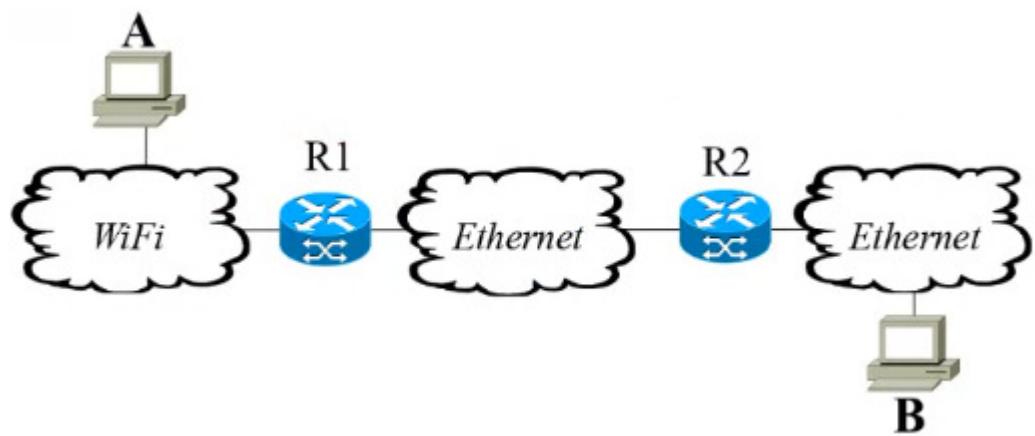
Analiza el campo TIPO de protocolo superior y pasa el contenido del campo DATOS al protocolo indicado del nivel superior.

- ii. **Desde un ordenador, con la dirección IP 220.10.1.25, se arrancan tres navegadores diferentes (Google Chrome, Mozilla Firefox y Safari), y se accede desde los tres a un mismo servidor HTTP en la dirección 138.10.1.5. ¿Cuántos sockets y cuántas comunicaciones del nivel de aplicación HTTP están implicados (lado cliente y lado servidor)?**

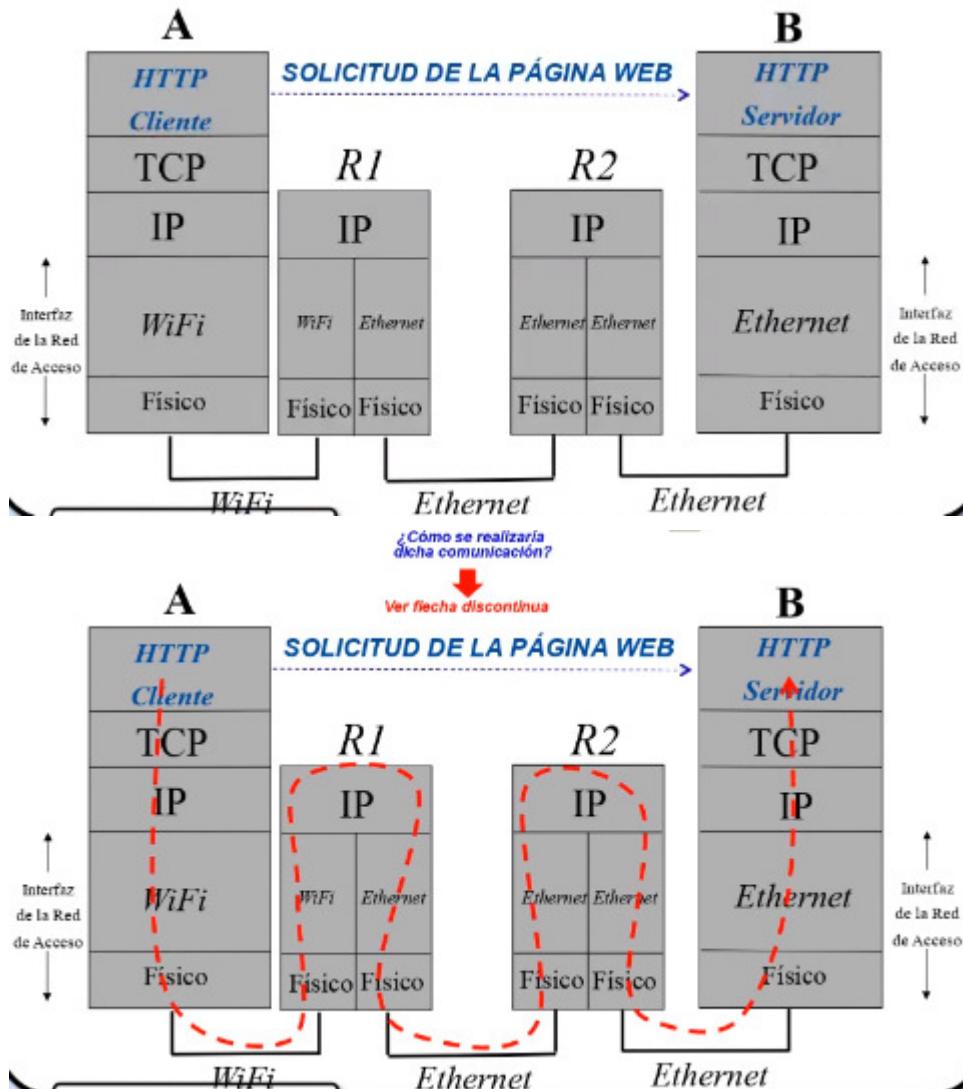
Cuatro sockets (tres procesos clientes y un servidor) y tres comunicaciones.



- iii. **Indique, gráficamente, el conjunto de protocolos de comunicaciones que intervienen en una solicitud de descarga de una página web entre los equipos “A” y “B”, suponiendo que la solicitud se hace desde el equipo “A”. Asimismo, indique, gráficamente, ¿cómo se realizaría dicha comunicación en función de los niveles de comunicaciones y máquinas intervenientes?**

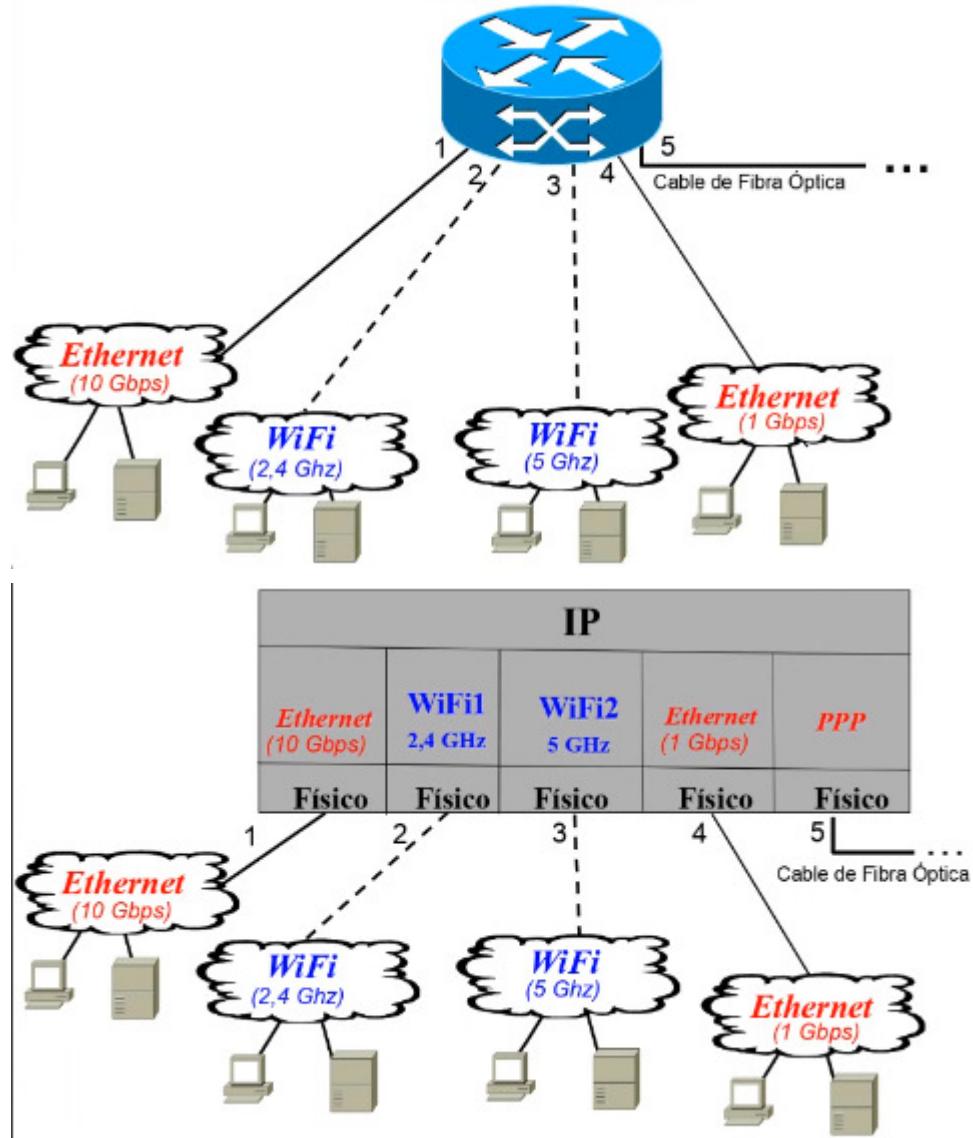


A es proceso cliente y B es proceso servidor.



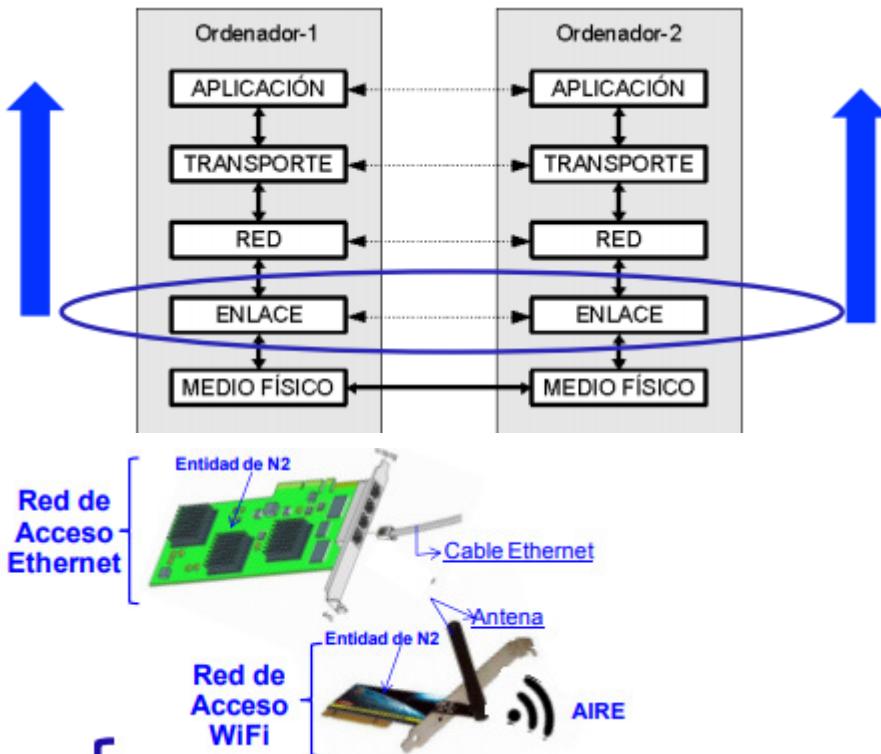
iv. Indicar gráficamente los niveles de comunicaciones de un router de N3:

### ROUTER DE N3

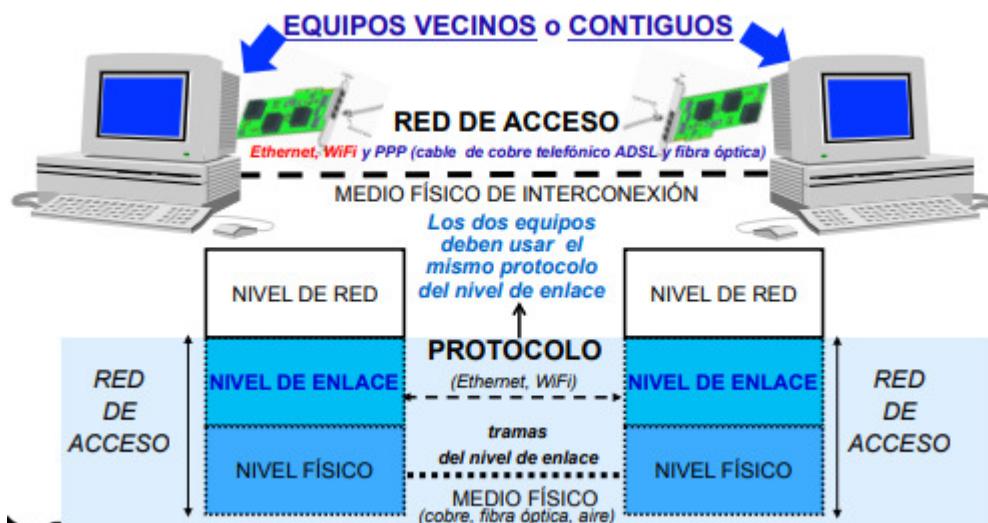


Solo una entidad IP con una tabla IP, que indica por qué "cable" (tarjetas de comunicaciones 1 - 5) debe enviarse una trama para llegar al equipo final.

#### 4. Nivel de enlace:

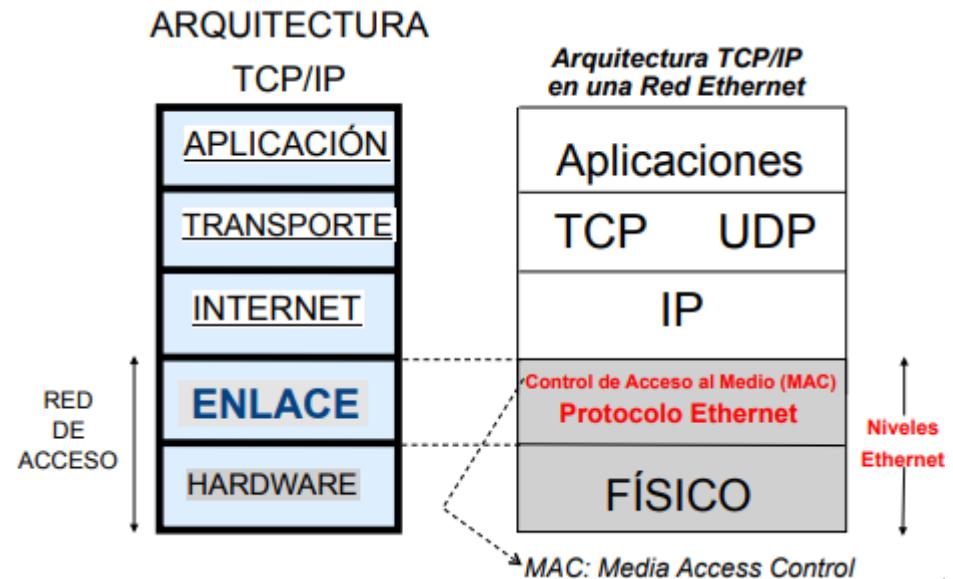


- a. Cada equipo puede tener muchas tarjetas de comunicaciones, cada una con su dirección MAC.
- b. Al intercambiar tramas (generalmente, paquetes IP encapsulados; otras veces, paquetes ARP encapsulados), los equipos vecinos deberán “hablar el mismo idioma” (comunicarse por el **mismo protocolo**: Ethernet, WiFi o PPP).

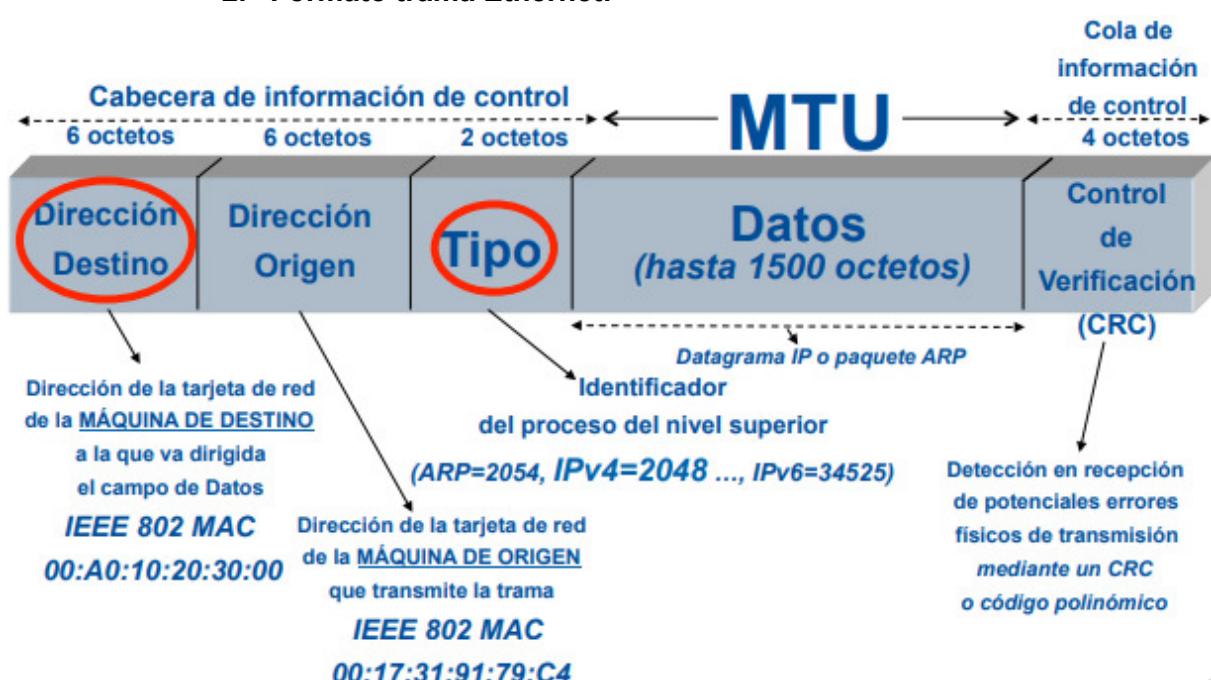


- c. **Direcciones MAC origen/destino:** cambian si origen y destino no son vecinos.
- d. **Direcciones IP origen/destino:** nunca cambian en los paquetes IP por Internet, independientemente de que el origen o destino sean o no vecinos.
- e. **Protocolos de nivel de enlace (N2):**

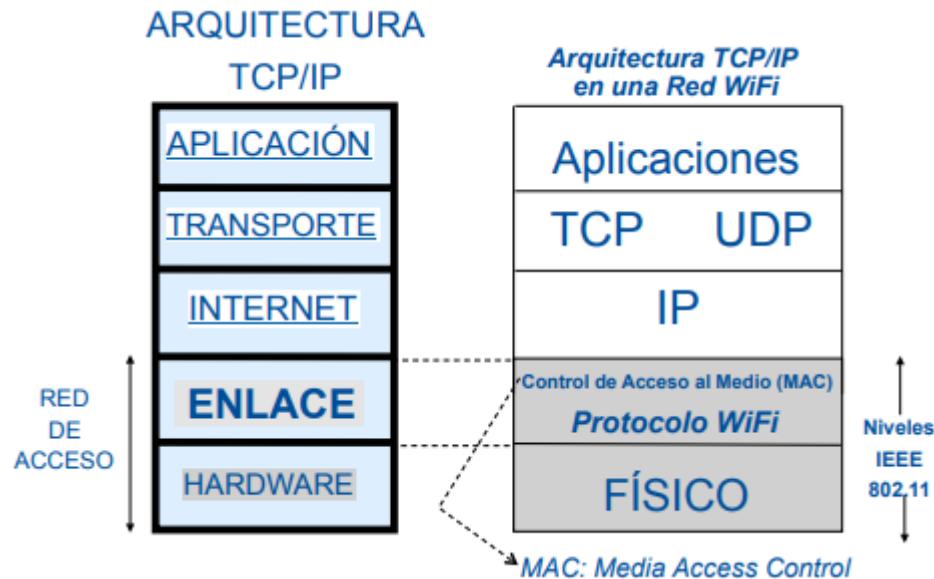
### i. Ethernet:



1. **Servicio no fiable:** es muy improbable que un cable Ethernet tenga fallos de transmisión por ser un cable de cobre protegido (más aún si es un cable de **fibra óptica**). Por eso, no se implementan funciones de fiabilidad, logrando agilizar la transmisión de datos.
  - a. **Sin control de fallos físicos:** bits cambiados en las tramas recibidas (se detectan, pero ni se corigen ni se recuperan). Deja que la corrección de errores la realice una entidad superior (o bien TCP o bien una aplicación fiable sobre UDP).
  - b. **Sin control de fallos lógicos:** tramas perdidas, desordenadas o duplicadas.
  - c. **Sin control de flujo:** una entidad Ethernet puede transmitir más rápidamente de lo que otra es capaz de almacenar y procesar.
2. **Formato trama Ethernet:**

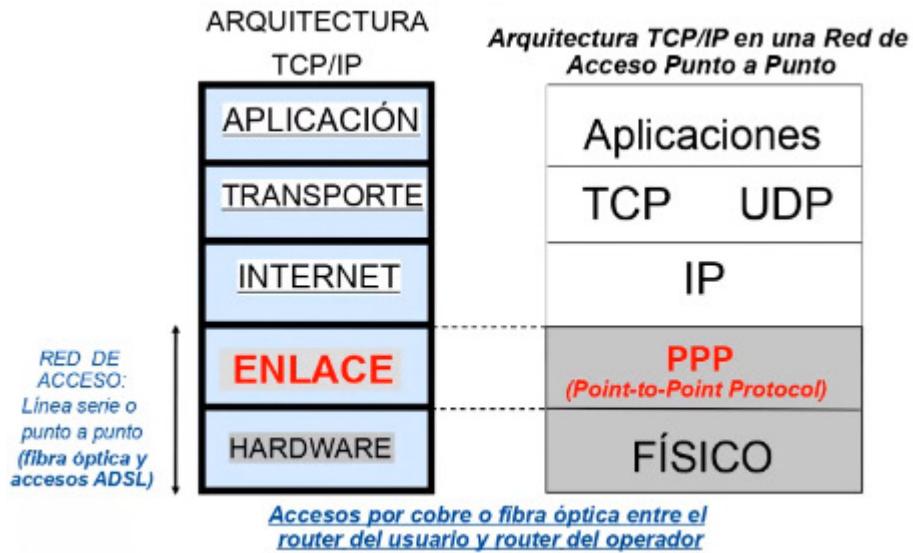


## ii. WiFi:



1. **Servicio fiable:** al usar un medio físico de interconexión débil (el aire), puede sufrir muchos fallos de transmisión (obstáculos como paredes o agua, interferencias con otras señales WiFi, ...).
  - a. **Control de fallos físicos:** bits cambiados en las tramas recibidas (Detección y Recuperación).
  - b. **Control de fallos lógicos:** tramas perdidas, desordenadas o duplicadas.
  - c. **Control de flujo:** una entidad WiFi no puede transmitir más rápidamente de lo que otra es capaz de almacenar y procesar.

## iii. PPP (Protocolo Punto a Punto):



- También se puede usar en líneas serie o punto a punto para conectar dos equipos cualesquier.
1. **Servicio no fiable:** PPP configurado por omisión (no se habilitan funciones de fiabilidad) → como por Ethernet, es muy poco probable que se den errores en la transmisión de tramas por PPP.
  2. **Servicio fiable:** PPP configurado con negociación previa de fiabilidad → menor velocidad de transmisión, pero con funciones de fiabilidad habilitadas.

3. Uso residual, fagocitado por el protocolo Ethernet.

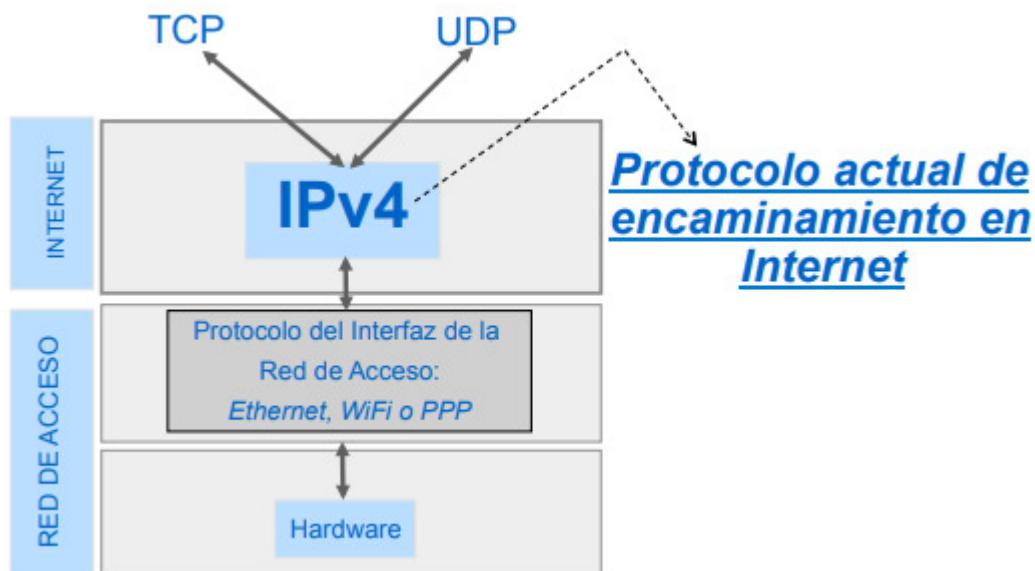
iv. **Resumen:**

1. **DETECCIÓN DE FALLOS FÍSICOS (BITS CAMBIADOS) sin recuperación (Ethernet)**
2. **CONTROL (Detección y Recuperación) DE FALLOS FÍSICOS Y LÓGICOS (WiFi PPP en modo fiable)**
3. **CONTROL DE FLUJO (WiFi y PPP en modo fiable)**

f. **Ejercicios:**

- i. ¿Qué protocolo asegura una transmisión fiable entre máquinas no vecinas? ¿HTTP, TCP, PPP o UDP?  
TCP (HTTP marginalmente no lo asegura, confía en TCP).
- ii. El protocolo Ethernet del nivel de enlace es un protocolo que detecta pero no corrige errores, dejando que sea...  
TCP o la propia aplicación fiable sobre UDP quien corrija dichos errores.

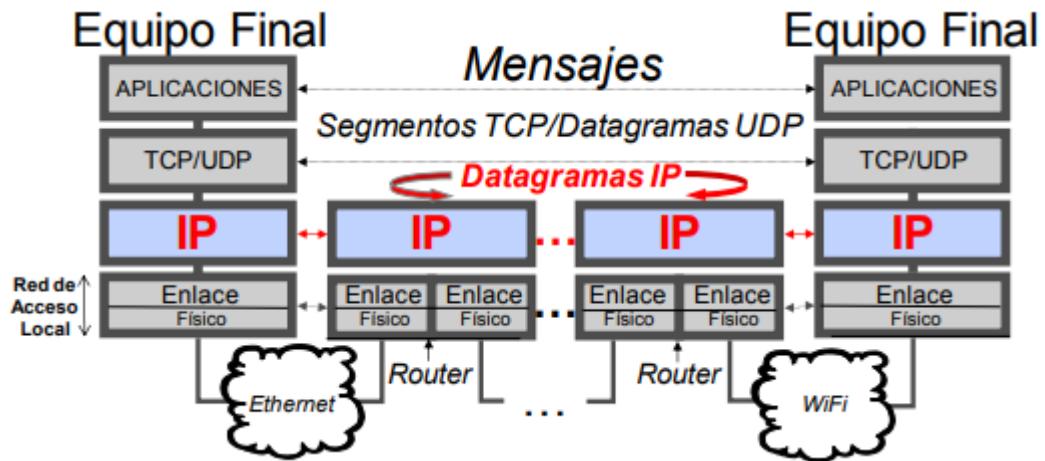
5. Nivel de red (IP o de Internet):



- Generalidades
- Tipos de transmisiones
- Direccionamiento IPv4
- Protocolo IPv4
- Protocolo ICMPv4

- a. Encaminamiento no fiable pero rápido mediante protocolo IP de segmentos TCP y datagramas UDP encapsulados en paquetes IP según la dirección IP destino entre

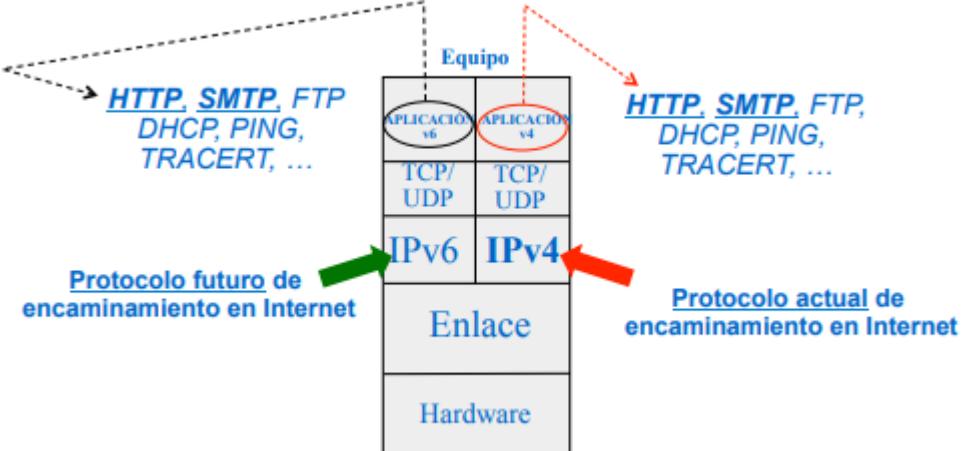
dos equipos vecinos (conectados a la misma red de acceso) entre origen y destino.



**b. Dos versiones del protocolo IP:**

- i. **IPv4:** protocolo de encaminamiento actual en Internet.
    1. Implementado por primera vez en 1983.
    2. Sigue funcionando incluso con aplicaciones en tiempo real basadas en voz (VoIP) y en streaming de audio y vídeo.
    3. **Deficiencia de diseño para la actual red Internet.**
  - ii. **IPv6:** protocolo de encaminamiento futuro en Internet.
    1. IPv6 es un IPv4 mejorado.
    2. **Diferencias con IPv4:**
      - a. **Direccionamiento:** de 4 bytes a 16 bytes (más direcciones IP).
      - b. **Flexibilidad y rapidez en el encaminamiento:** la cabecera PCI de nivel de red es más simple con la mitad de campos, haciendo su transferencia más rápida.
      - c. **Seguridad de paquetes IP:** implementación de mecanismos de seguridad con cabeceras de extensión opcionales para asegurar la autenticación, confidencialidad y la integridad de los datos transportados por los paquetes IP (en IPv4 estas funciones no están implementadas).

c. **Doble pila IPv4/IPv6:** instalada en cualquier distribución de sistema operativo.



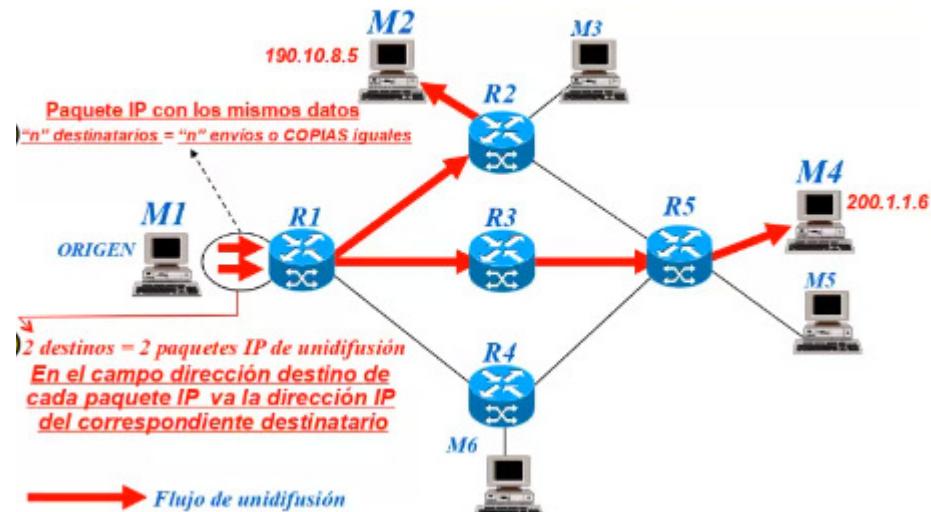
- d. **Direcciones IPv4:** las **redes de comunicaciones** en Internet (Ethernet y WiFi) y las **máquinas** conectadas a dichas redes siempre tienen una dirección IPv4.

e. **Actualmente, los routers en Internet son IPv4:** no cuentan con tablas completas de encaminamiento para IPv6, por lo que un paquete IP en protocolo IPv6 podría perderse (o incluso no salir de tu red local) porque todos los routers en el trayecto origen-destino deben ser IPv6.

- Se ha querido cambiar los routers de IPv4 a IPv6 desde 1993 y aún no se ha hecho.
- Las empresas de telecomunicaciones no quieren cambiar de IPv4 a IPv6 porque el formato pasa de ser de 4 bytes a ser de 16 bytes, y asignar una IPv4 pública al router de E/S de cada domicilio dejaría de ser un bien escaso. Gran parte de la factura de Internet va a pagar el mantenimiento de esta IP.

f. **Tipos de transmisiones IPv4:**

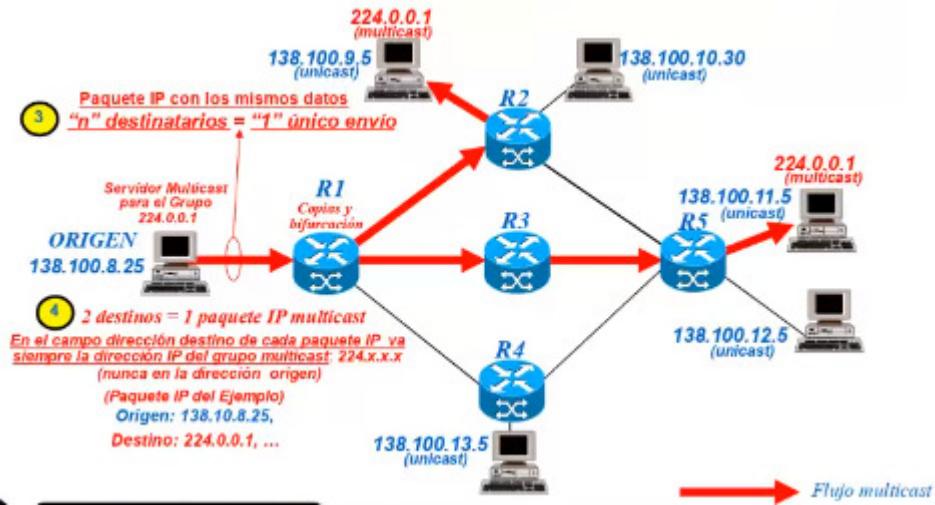
- Unidifusión (Unicast):** transmisión IP punto a punto entre 2 equipos (1:1).



- Para enviar un paquete IP a **n destinatarios**, habrá que realizar **n envíos o copias iguales**.

2. **Ejemplo:** transmisiones en Internet.

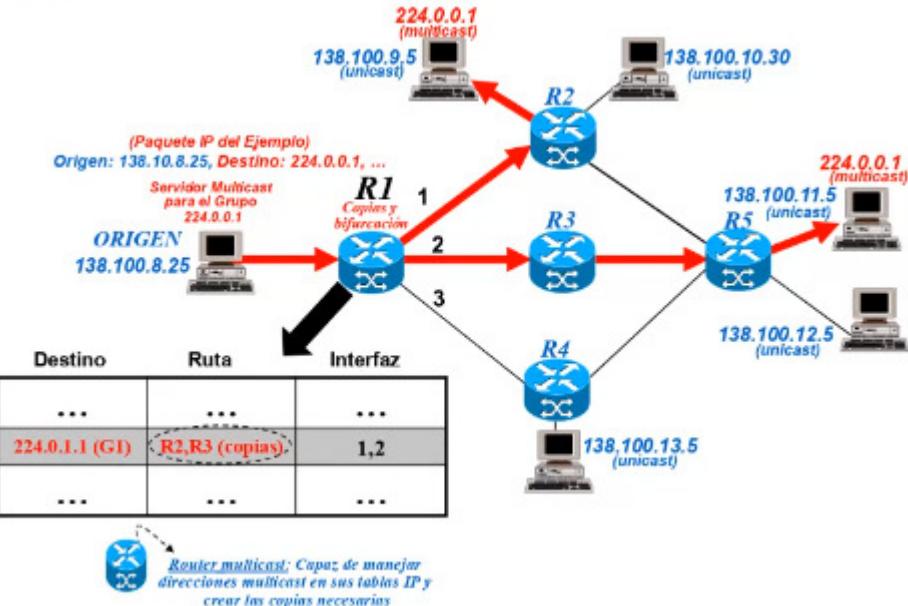
- Multidifusión (Multicast):** transmisión IP a un grupo **Multicast (1:N)**: equipos que comparten una misma dirección de multidifusión (**Multicast**).



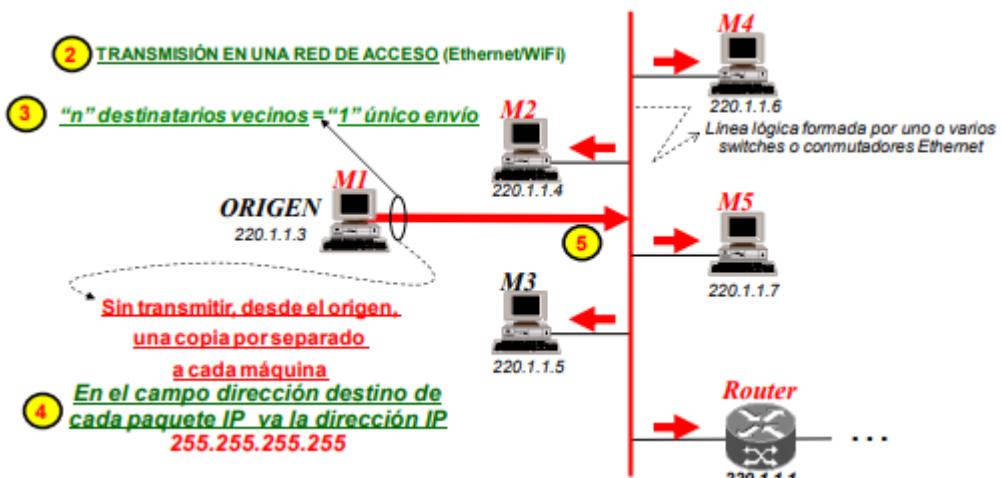
- Para enviar un paquete IP a **n destinatarios**, habrá que realizar un **solo envío** (sin copias desde el origen, a diferencia de **Unicast**).
- Los equipos destino deberán estar en el mismo grupo **Multicast**.
- Dirección IP destino:** prefijo de dirección IP **multicast** del grupo.

4. **Ejemplos:** actualizaciones de software, noticias, videoconferencias, teleeducación, juegos en red, Internet (en la red de routers de un mismo operador, porque entre operadores no hay acuerdo para IPs *multicast*), Intranet de una organización ...

5. **Ejemplo:** copiado y bifurcación *Multicast* en un router *Multicast*.

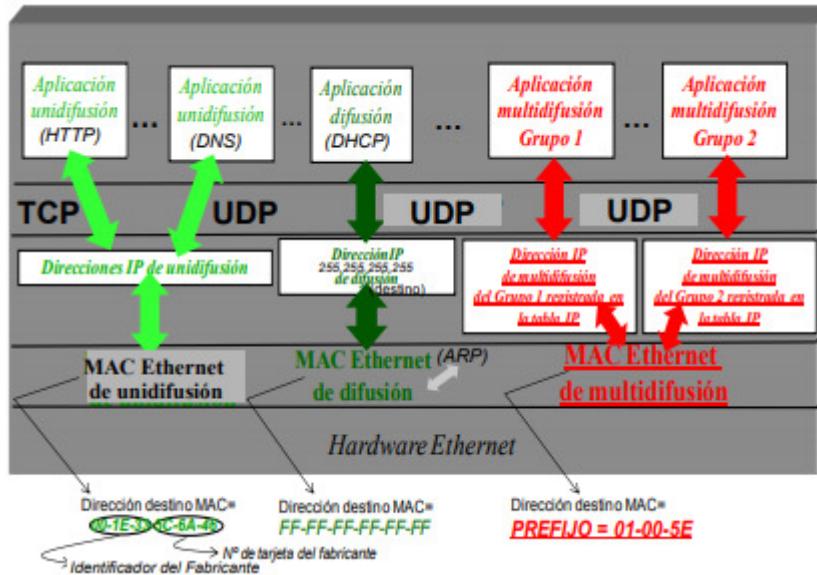


- a. Las copias de un paquete IP *multicast* se realizan desde un router *multicast* a partir de su tabla IP.
- iii. **Difusión (*Broadcast*):** transmisión IP a todos los equipos vecinos (1:N) de una red de acceso de difusión o *Broadcast* (Ethernet o WiFi).



1. Para enviar un paquete IP a **n destinatarios**, habrá que realizar un **solo envío** (sin copias desde el origen, a diferencia de **Unicast**).
  2. El paquete IP llegará a todo equipo en la misma red de acceso, **lo haya pedido o no** (a diferencia de **Multicast**).
  3. Dirección IP destino: 255.255.255.255.
- g. **Correspondencias IP-MAC:** el nivel de enlace debe ser capaz de transmitir a un equipo destino tramas de Unicast, Multicast y Broadcast. Cada trama tendrá sus

direcciones IP y MAC correspondientes.



- i. **Unicast:** "normal" para IP y MAC.
- ii. **Broadcast:** dirección IP y MAC todo 1s: IP 255.255.255.255 y MAC FF-FF-FF-FF-FF-FF.
- iii. **Multicast:** dirección IP de multicast correspondiente a cada grupo de multicast y dirección MAC con prefijo 01-00-5E.
- h. **Formato IPv4:** dirección de red + dirección de máquina (conectada a dicha red).
  - i. 4 bytes en decimal, separados por puntos.
- i. **Clases de direcciones IPv4:**
  - i. **Clase A:** redes grandes (muchas máquinas pueden conectarse).



Primer octeto clase A: 0000 0000 (0) - 0111 1111 (127)

**A = red.máquina.máquina.máquina**

- **red.0.0.0** (dirección de red)
- **red.255.255.255** (difusión dirigida a todas las máquinas en dicha red)

1. **Direcciones de red reservadas:** 00000000 (0) y 01111111 (127).
  2. **Direcciones máquina reservadas:** dirección de red clase A (0.0.0) o broadcast (255.255.255).
- ii. **Clase B:** redes medianas (varias máquinas pueden conectarse).



**Primer octeto clase B: 1000 0000 (128) - 1011 1111 (191)**

B = red.red.máquina.máquina

- red.red.0.0 (dirección de red)
- red.red.255.255 (difusión dirigida a todas las máquinas en dicha red)

1. **Direcciones máquina reservadas:** dirección de red clase B (0.0) o broadcast (255.255).
- iii. **Clase C:** redes pequeñas (pocas máquinas pueden conectarse).



**Primer octeto clase B: 1100 0000 (192) - 1101 1111 (223)**

C = red.red.red.máquina

- red.red.red.0 (dirección de red)
- red.red.red.255 (difusión dirigida a todas las máquinas en dicha red)

1. **Direcciones máquina reservadas:** dirección de red clase C (0) o broadcast (255).
- iv. **Clase D:** transmisiones en grupo.



- v. **Clase E:** sin uso o formato de investigación o experimental.



- vi. **Ejercicios:**

**La dirección 10.0.0.0 es una dirección IP:**

- a) De máquina de la clase A
- b) Reservada
- c) De red de la clase A
- d) Ninguna de las anteriores

1.

**La dirección 192.168.0.0 es una dirección numérica:**

- a) De máquina de la clase B
- b) Reservada
- c) *De red de la clase C*
- 2. d) Ninguna de las anteriores

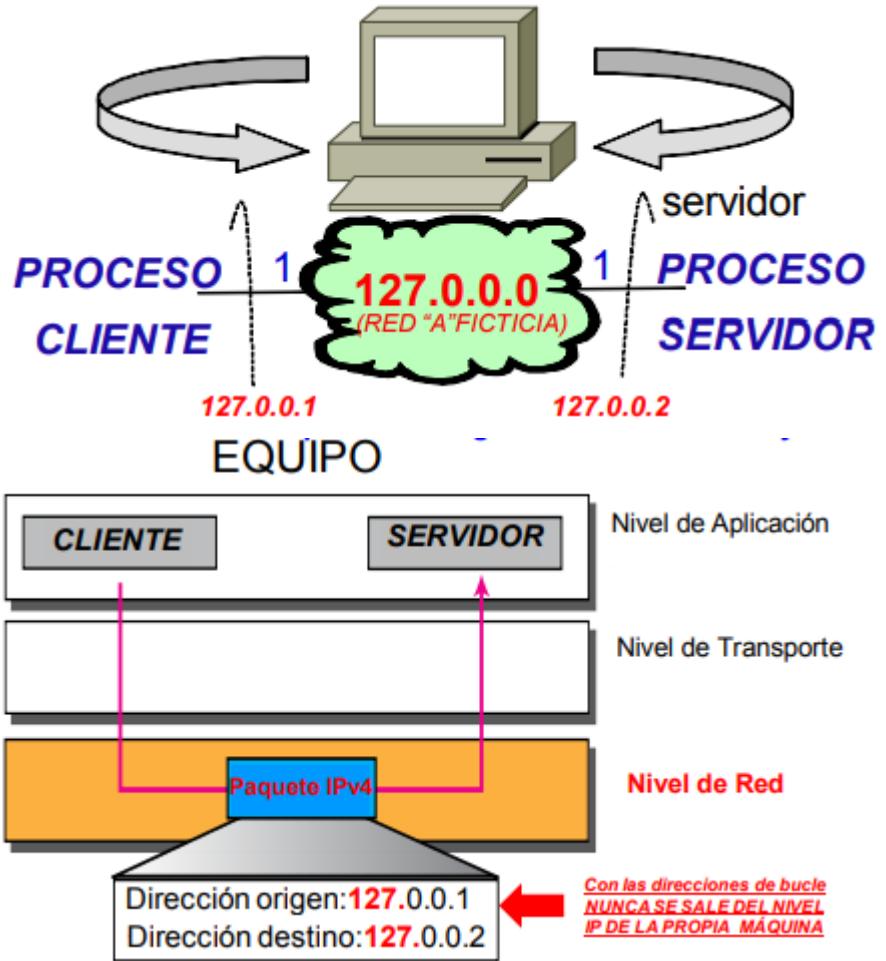
**La dirección 192.168.0.1 es una dirección numérica:**

- a) *De máquina de la clase C*
- b) Reservada
- c) De red de la clase C
- 3. d) Ninguna de las anteriores

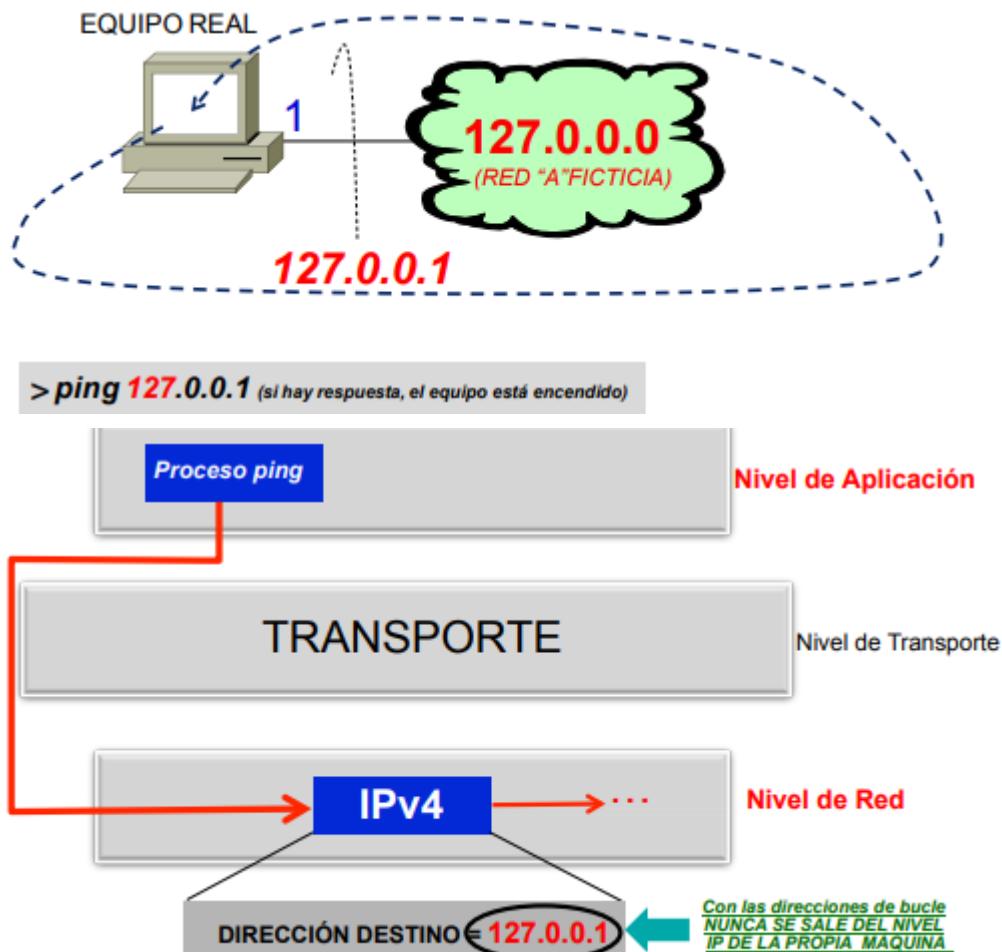
j. **Direcciones IPv4 reservadas:** no pueden ser usadas ni para identificar redes ni para identificar máquinas.

i. **Direcciones reservadas de red (2 de clase “A”):**

- 1. **0.0.0.0: ruta por omisión (by default) en una tabla IP, o una solicitud de configuración TCP/IP vía cliente DHCP (dirección IP cliente DHCP = 0.0.0.0).**
- 2. **127.0.0.0: Dirección de bucle (Loopback address):** dirección IP de máquina ficticia perteneciente a una dirección IP de red ficticia clase A (127.0.0.0) virtualmente dentro de la propia máquina, para que, sin salir a ninguna red física externa, se pueda:
  - a. Desarrollo de aplicaciones cliente y servidor en la propia máquina mediante un encaminamiento local de la entidad IP en la propia máquina, probando localmente su interacción.



- b. Prueba de acceso o ejecución de un proceso local (p.ej., **ping**) mediante un encaminamiento local de la entidad IP en la propia máquina.



- > ping 127.0.0.1 (si hay respuesta, el equipo está encendido)
- ii. Direcciones reservadas de máquina (2 de clase “A”, “B” y “C”):
  - 1. Dirección máquina = 0...0: dirección de red.
  - 2. Dirección máquina = 1...1: difusión dirigida (*Directed Broadcast*) a todas las máquinas de una red local o remota.
- iii. Dirección IP destino = 255.255.255.255: difusión limitada (*Limited Broadcast*) a todas las máquinas de una red local (Ethernet o Wifi).
- k. Tipos de direcciones IPv4: toda dirección de IPv4 tiene una **máscara asociada**, distintas según el tipo de dirección IPv4.
  - i. Direcciones de red:



- 1. **Estándar RFC-950:** parte de red de máscara deberá ser 1...1 (para toda clase de dirección IP de red).

2. **Formato: IP / máscara** (por bytes o por nº de 1s en la máscara).

CLASE DE DIRECCIÓN	MÁSCARA POR OMISIÓN (Decimal)
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

**Formato de 4 octetos en decimal**

**LOS CEROS DEFINEN LA PARTE LOCAL O LA DIRECCIÓN DE MÁQUINA EN LA DIRECCIÓN IP**

20.0.0.0/255.0.0.0 ó 20.0.0.0/8      *Formato /Nº en decimal que indica los bits a "unos" contiguos de la máscara*

136.15.0.0/255.255.0.0 ó 136.15.0.0/16

220.10.1.0/255.255.255.0 ó 220.10.1.0/24

- a. Todos los **bits de la máscara** que sean 0, sus correspondientes bits podrán ser **modificados** en la **dirección IP** (en rojo).

3. **Máscara de una tabla IP:** un bit no es significativo si en la máscara aparece un 0 en su posición; en caso contrario, aparecerá un 1.
- a. **128.1.1.0/255.255.255.0:** ningún bit del cuarto byte de la dirección IP de destino se va a usar en el encaminamiento.
  - b. **0.0.0.0/0.0.0.0:** ningún bit de la dirección por omisión se va a usar en el encaminamiento.
  - c. **128.1.1.1/255.255.255.255:** todos los bits de la dirección IP de destino se van a usar en el encaminamiento.

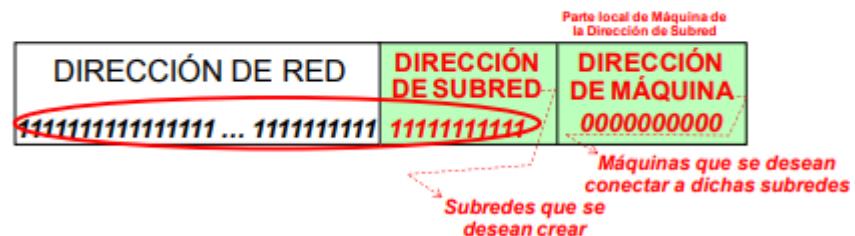
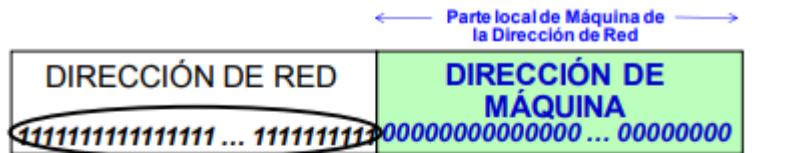
- ii. **Direcciones de máquina:** la máscara de máquina tiene todos sus bits en 1 porque todos los bits de la dirección IP destino son necesarios para el encaminamiento.

1. 20.1.2.3/255.255.255.255 (/32)
2. 136.15.22.3/255.255.255.255 (/32)
3. 220.10.1.1/255.255.255.255 (/32)

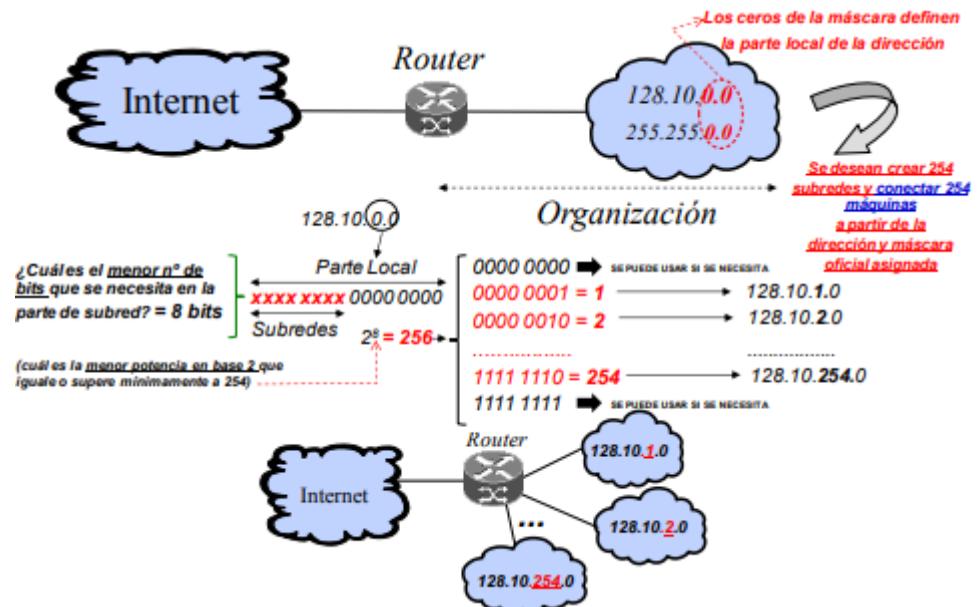
- iii. **Direcciones de subred:**

1. **Subred:** subconjunto de una red de comunicaciones.
2. **Creación de subredes:** el administrador de una red creará sus propias subredes y asignará direcciones IP a cada una a partir de:
  - a. La dirección IP pública de red asignada por el ISP.
  - b. La máscara de red asociada (su nº de ceros).
3. **Dirección de subred:** podrá ser todo ceros y todo unos.
4. **Dirección de máquina:** no podrá ser ni todo ceros ni todo unos, porque referencian la dirección de (sub)red y la difusión dirigida a todas las máquinas de la (sub)red, respectivamente.
5. **Máscara de subred:** siempre tiene más 1s que la máscara original de red porque "protege" la dirección IP pública de red asignada por el ISP

y limita el número de subredes creadas.

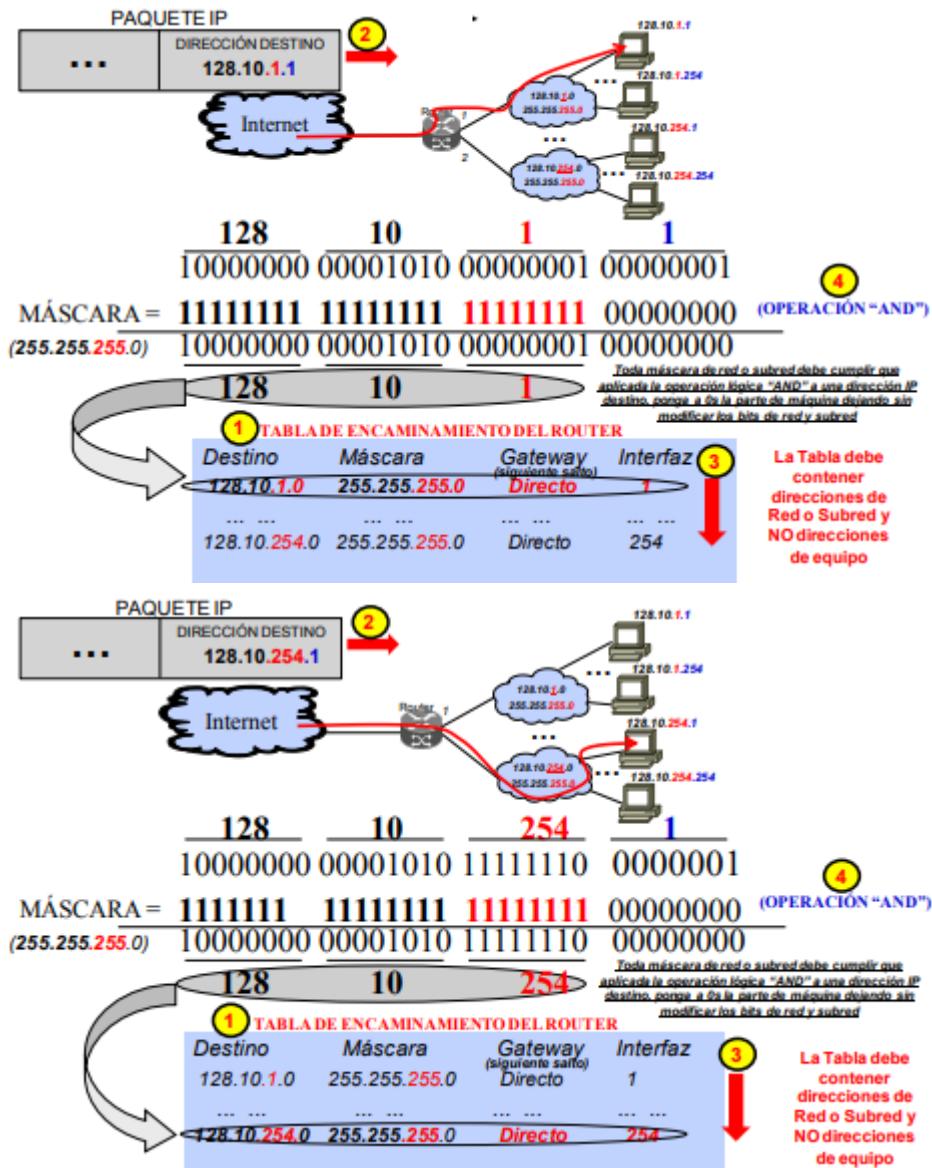


6. **Ejemplo:** creación de subredes clase B con una máscara común o conectando un mismo número máximo de máquinas por subred.



- Máscara de red:** “protege” de cambios la **dirección de red** (128.10.x.x).
- Dirección de subred:** 254 subredes → codificadas en 8 bits ( $2^8 = 256 > 254$ ). Puede haber hasta 256 subredes.
- Dirección de máquina:** 8 bits libres → puede haber hasta  $2^8 - 2$  (254) máquinas como máximo por subred.
- Máscara de subred:** bits de dirección de red + bits de dirección de subred = /16 + /8 = **/24** (255.255.255.0).

7. Op. lóg. AND(IP destino, máscara de (sub)red) = dirección de (sub)red.



- La máscara de (sub)red facilita el encaminamiento, encontrando en una operación la dirección de (sub)red.
  - La tabla de encaminamiento **no contiene** direcciones de equipo, solo direcciones de red y de subred.
  - Se llegará a la máquina indicada dentro de la subred consultando la dirección de máquina, añadiendo la cabecera de nivel de enlace al paquete y encaminándola al equipo final.
8. **Gateway:** Directo → el router de la tabla es **vecino** del equipo final (no hay que atravesar routers intermedios para llegar a la IP destino).
9. **Ejercicios:**

a. 1:

Dada la dirección de red 220.10.1.0 con máscara /27 y suponiendo que se desean crear 3 subredes; indicar el NÚMERO MÁXIMO DE MÁQUINAS que se pueden identificar en dichas subredes

- a) 14
- b) 8
- c) 6
- d) No existen bits para identificar máquinas

**220.10.1.0/255.255.255.1110 0000 (/27)**: deja 5 bits libres de la dirección IP de red para codificar las direcciones de subred y de máquina.

**Direcciones de subred**: 3 subredes → 2 bits para codificarlas.

**Direcciones de máquina**: 3 bits libres →  $2^3 - 2$  (direcciones reservadas) = **6 máquinas por subred**.

b. 2:

Dada la dirección de red 220.10.8.0 con máscara /25 y suponiendo que se desean crear 6 subredes; indicar el NÚMERO MÁXIMO DE MÁQUINAS que se pueden identificar en dichas subredes

- a) 14
- b) No existen bits para identificar máquinas
- c) 8
- d) Ninguna de las anteriores

**220.10.8.0/255.255.255.1000 0000 (/25)**: deja 7 bits libres de la dirección IP de red para codificar las direcciones de subred y de máquina.

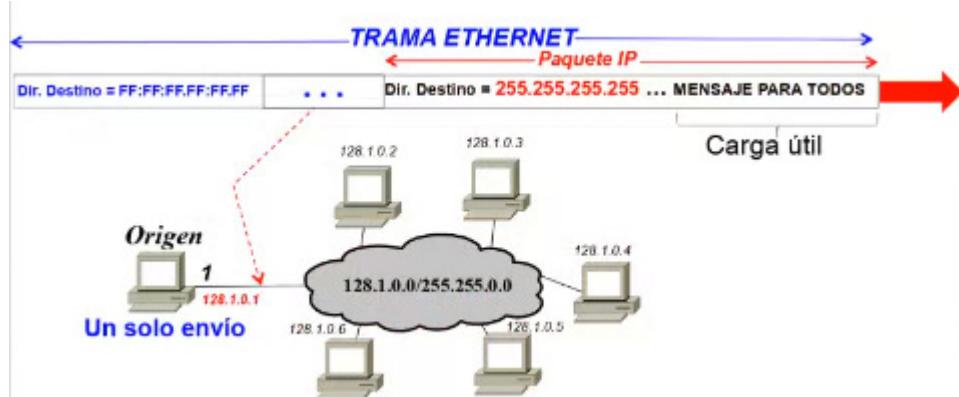
**Direcciones de subred**: 6 subredes → 3 bits para codificarlas.

**Direcciones de máquina**: 4 bits libres →  $2^4 - 2$  (direcciones reservadas) = **14 máquinas por subred**.

iv. **Direcciones de superred**: buscan reducir el tamaño de las tablas IP de los routers de los operadores en Internet o de una organización.

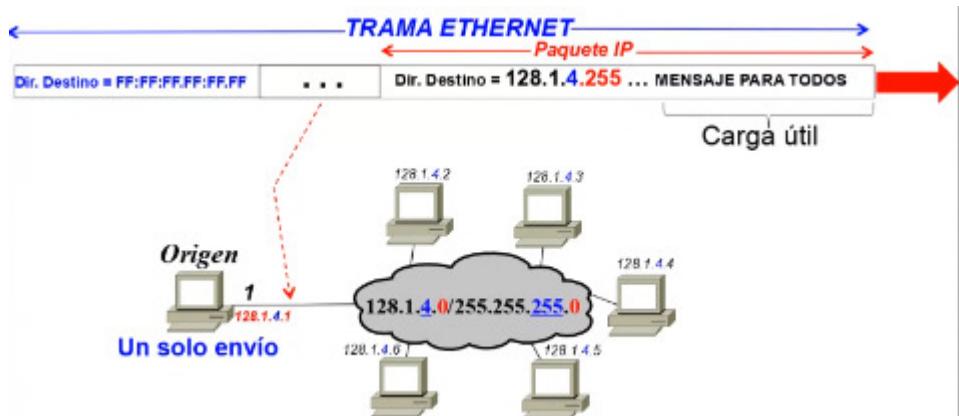
I. **Tipos de difusión (Broadcast)**:

i. **Difusión limitada (broadcast limitado o broadcast)**: transmisión de un mismo mensaje en un solo envío a todos los equipos conectados a la misma red o subred de difusión Ethernet/WiFi (aquella que permite difusión o *broadcast* a nivel de trama).



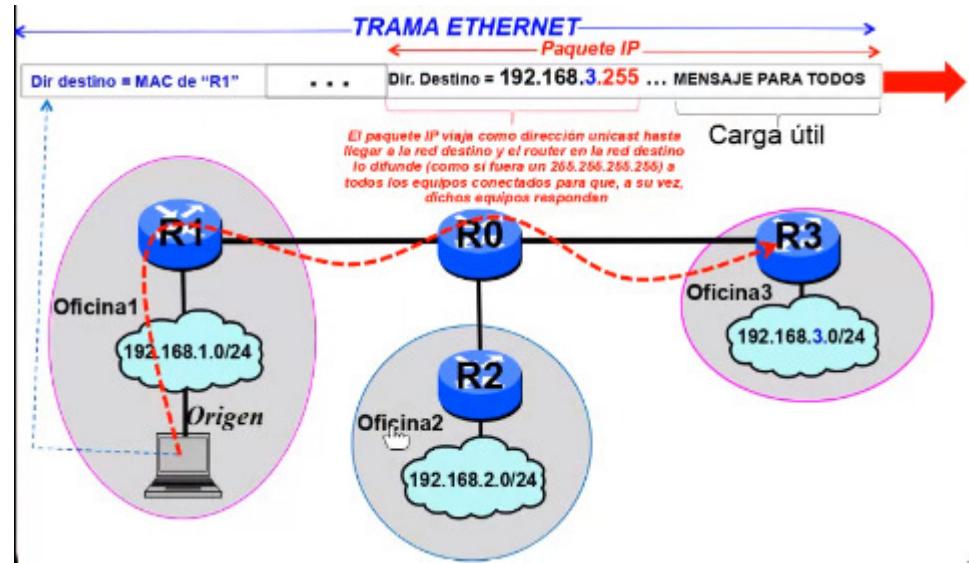
(difusión dirigida a red local)

1. Dirección MAC destino: FF:FF:FF:FF:FF:FF (todo a 1s).
2. Dirección IP destino: 255.255.255.255 (todo a 1s).
- ii. **Difusión dirigida (broadcast dirigido):** transmisión de un mismo mensaje en un solo envío a todos los equipos conectados a la misma red o subred de difusión Ethernet/WiFi o a todos los equipos conectados a una red o subred remota.



1. Dirección MAC destino: FF:FF:FF:FF:FF:FF (todo a 1s).
2. Dirección IP destino: dirección de máquina todo a 1s (dirección de red y de subred mantendrán sus valores).
3. **Red o subred remota (difusión a distancia):** el paquete IP viaja como dirección **unicast** hasta llegar a la red destino y el router en la red destino lo difunde (como si fuera un 255.255.255.255) a todos los

equipos conectados para que estos respondan.

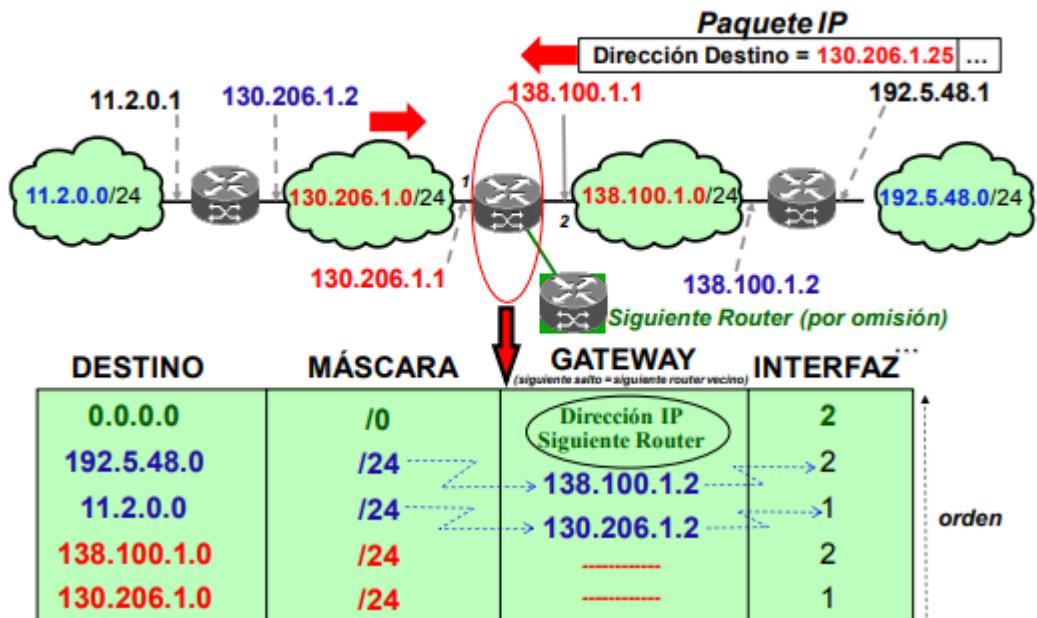


4. Una **difusión dirigida localmente** tiene el mismo efecto que una **difusión limitada**. Difieren en la dirección de red y subred.

#### m. Tipos de encaminamiento:

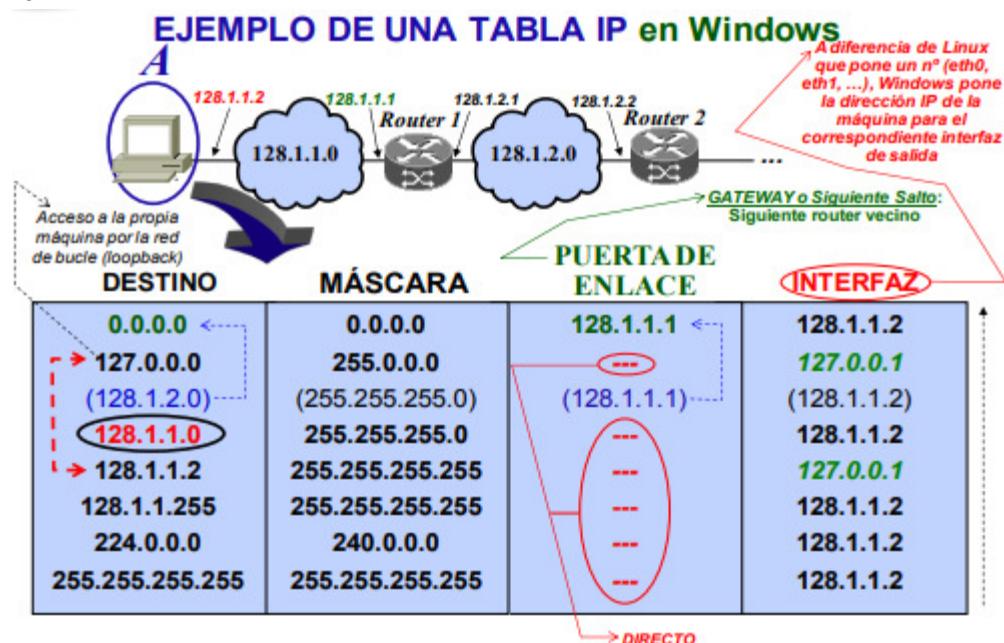
- i. **Directo:** el equipo final es vecino, **no** hay que pasar por un router vecino. La dirección de red del equipo final está registrada en la **tabla IP**.
  1. La dirección de red del router y del equipo final **coinciden**.
- ii. **Indirecto:** el equipo final **no** es vecino, hay que pasar por un router vecino. La dirección de red del equipo final está registrada en la **tabla IP**.
- iii. **Por omisión o by default (0.0.0.0):** el equipo final **no** es vecino, hay que pasar por un router vecino. La dirección de red del equipo final **no** está registrada en la **tabla IP** (se encaminará el paquete IP por el **gateway** de 0.0.0.0).
- iv. **Ejemplo:** tabla de encaminamiento directo.

#### ENCAMINAMIENTO DIRECTO, INDIRECTO Y POR OMISIÓN



1. Todo router tiene una dirección IP por cada red a la que esté conectado.

2. Todo router debe registrar en su tabla IP la dirección IP de sus routers vecinos (138.100.1.2 y 130.206.1.2).
  3. Toda tabla IP debe almacenar las direcciones IP destino de red, no las de máquina.
  4. El **orden** debe dejar la **dirección por omisión** en la última fila. Si se dejara el primero, todos los paquetes IP se encaminarían por **0.0.0.0**.
  5. **Interfaz (de salida):** dirección IP de la interfaz de salida (en Windows) o nº de salida (eth0, eth1, ...).
- v. **Ejemplo:** tabla IP en Windows.



1. La dirección IP destino 128.1.2.0 puede englobarse en la dirección por omisión porque comparten puerta de enlace, siendo redundante esa fila de la tabla IP (es recomendable hacer esto siempre que sea posible).
2. 128.1.1.0, al tener la misma interfaz que la de la dirección de bucle (loopback), tiene el mismo efecto que **Loopback**.
3. 128.1.1.255 (broadcast dirigido localmente) y 255.255.255.255 (broadcast limitado) tienen el mismo efecto.

vi. Ejemplo: tabla IP en Windows.

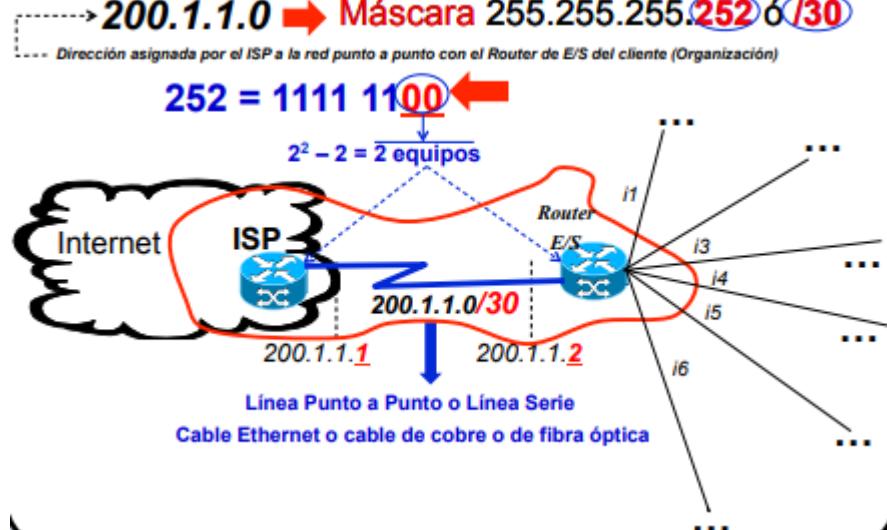
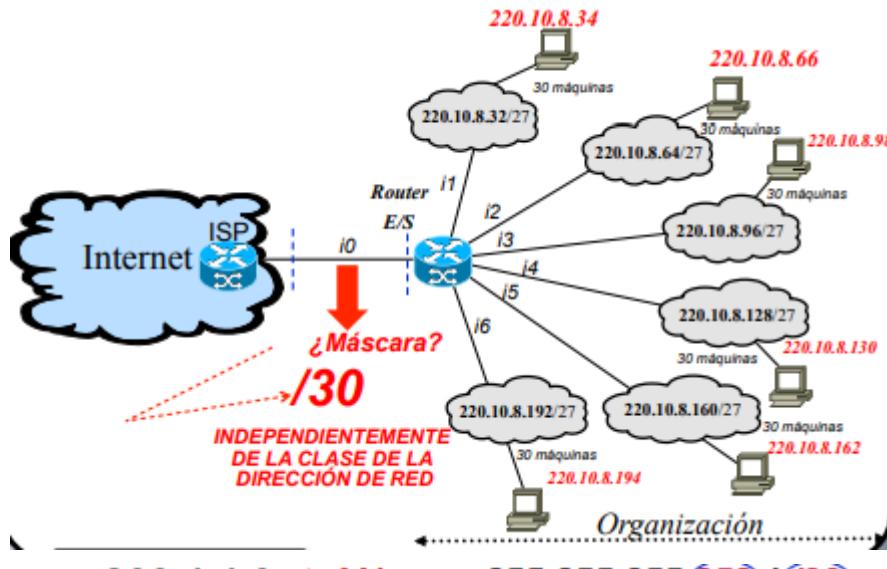
IPv4 Tabla de enrutamiento					
Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica	Dirección IP del Equipo
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.51	35	Encaminamiento por Omisión (BY DEFAULT)
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331	= Acceso Directo a cualquier dirección de bucle del propio equipo
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331	= Acceso Directo a la dirección de bucle del propio equipo
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331	= Broadcast Dirigido a todos los procesos NS del equipo por la Red de Bucle
192.168.1.0	255.255.255.0	En vínculo	192.168.1.51	291	= Encaminamiento Directo a cualquier equipo vecino de la Red de Acceso
192.168.1.51	255.255.255.255	En vínculo	192.168.1.51	291	= Encaminamiento Directo al propio equipo por la Red de Acceso
192.168.1.255	255.255.255.255	En vínculo	192.168.1.51	291	= Broadcast Dirigido a todos los equipos vecinos de la Red de Acceso
224.0.0.0	240.0.0.0	En vínculo	127.0.0.1	331	= Multicast a cualquier grupo multicast 224 del propio equipo por la Red de Bucle
224.0.0.0	240.0.0.0	En vínculo	192.168.1.51	291	= Multicast a cualquier grupo local multicast 224
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331	= Broadcast a todos los procesos NS del equipo por la Red de Bucle
255.255.255.255	255.255.255.255	En vínculo	192.168.1.51	291	= Broadcast a todos los equipos vecinos de la Red de Acceso
Rutas persistentes:					
Ninguno = El usuario no ha introducido ninguna ruta					
IPv6 Tabla de enrutamiento					
Rutas activas:					
Cuando destino de red métrica		Puerta de enlace			
1	331 ::1/128	En vínculo			
12	291 fe80::/64	En vínculo			
12	291 fe80::74c5:ad36:3bafe:d7f9/128	En vínculo			
		En vínculo			
1	331 ff00::/8	En vínculo			
12	291 ff00::/8	En vínculo			
Rutas persistentes:					
Ninguno					

IPv4 Tabla de enrutamiento					
Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica	Dirección IP del Equipo
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.51	35	Encaminamiento por Omisión (BY DEFAULT)
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331	= Acceso Directo a cualquier dirección de bucle del propio equipo
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331	= Acceso Directo a la dirección de bucle del propio equipo
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331	= Broadcast Dirigido a todos los procesos NS del equipo por la Red de Bucle
192.168.1.0	255.255.255.0	En vínculo	192.168.1.51	291	= Encaminamiento Directo a cualquier equipo vecino de la Red de Acceso
192.168.1.51	255.255.255.255	En vínculo	192.168.1.51	291	= Encaminamiento Directo al propio equipo por la Red de Acceso
192.168.1.255	255.255.255.255	En vínculo	192.168.1.51	291	= Broadcast Dirigido a todos los equipos vecinos de la Red de Acceso
224.0.0.0	240.0.0.0	En vínculo	127.0.0.1	331	= Multicast a cualquier grupo multicast 224 del propio equipo por la Red de Bucle
224.0.0.0	240.0.0.0	En vínculo	192.168.1.51	291	= Multicast a cualquier grupo local multicast 224
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331	= Broadcast a todos los procesos NS del equipo por la Red de Bucle
255.255.255.255	255.255.255.255	En vínculo	192.168.1.51	291	= Broadcast a todos los equipos vecinos de la Red de Acceso
Rutas persistentes:					
Ninguno					

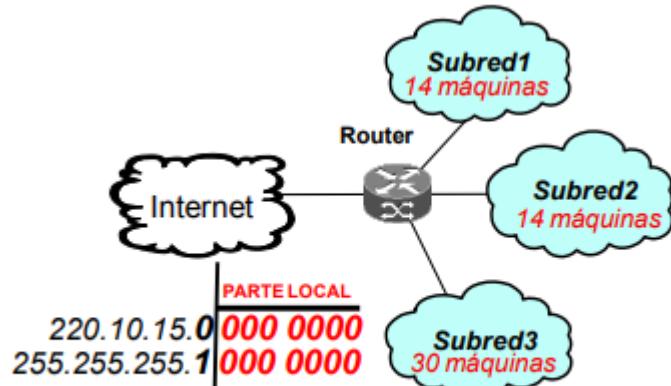
(foto)

n. Máscara de red PPP (punto a punto, entre 2 equipos):



- i. **Direcciones de máquina:** solo necesitamos 4: red (00), dos equipos (01 y 10) y broadcast dirigido (11).
- o. **Dos clases de máscaras de subred:**
  - i. **Máscaras de subred de longitud fija:** comunes para todas las subredes creadas. Asignan un mismo número máximo de máquinas por subred.
  - ii. **Máscaras de subred de longitud variable (VLSM: Variable Length Subnet Masks):** diferentes para cada subred creada. Asigna un distinto número máximo de máquinas a cada subred.
    - 1. **Objetivo:** usar el menor número de direcciones IP.

iii. **Ejemplo:** creación de subredes de longitud variable



*Se desea crear, a partir de la dirección y máscara oficial asignada, tres subredes con 30 máquinas en una y 14 máquinas en las dos restantes*

1. Ordenar las subredes de mayor a menor tamaño (número de máquinas) o viceversa.

**POR EJEMPLO, DE MENOR A MAYOR TAMAÑO,**

- Subred1: Máximo 14 máquinas + Router = 15 máquinas
- Subred2: Máximo 14 máquinas + Router = 15 máquinas
- Subred3: Máximo 30 máquinas + Router = 31 máquinas

- a. El orden de mayor a menor suele producir menos desperdicios de direcciones, pero en este ejemplo se hará de menor a mayor tamaño.
2. Se asigna la dirección IP original a la 1<sup>a</sup> subred en el orden escogido (en este caso, la menor → Subred1 = 220.10.15.0).
  - a. **Máscara asociada:** para conectar 15 máquinas a la subred 1, habrá que utilizar 5 bits →  $2^5 - 2 = 30 > 15$ . Entonces, la máscara de esta subred será /27 (/32 (todo 1s) - 5 bits).
  - b. **Dirección de red:** 220.10.15.000x xxxx
    - i. 220.10.15.0 → dirección de subred.
    - ii. 220.10.15.1 → dirección de equipo 1.
    - iii. 220.10.15.15 → dirección de equipo 15.
    - iv. 220.10.15.30 → última dirección assignable.
    - v. 220.10.15.31 → dirección de difusión dirigida.

### 3. Subred2:

5. SE CALCULA LA MÁSCARA de la siguiente subred de menor tamaño (Subred2) en función del nº máximo de máquinas que se desean conectar a Subred2. Los bits que se necesitan (para identificar equipos en la dirección IP) definen el nº de ceros de dicha máscara y el nº de ceros o bits para máquinas en la PARTE LOCAL DE MÁQUINA DE LA DIR IP asociada

- Si a la 2<sup>a</sup> subred se desean conectar 15 máquinas entonces  $2^5-2 > 15$ . Por tanto, necesitamos 5 bits (ceros), en la máscara y PARTE LOCAL DE MÁQUINA de la dirección IP, para direccionar máquinas
- La máscara es /27 (32 “unos” – 5 “ceros” = /27 “unos”)
- Por tanto, necesitamos 5 bits (ceros) en la máscara y 5 bits en la PARTE LOCAL DE MÁQUINA de la nueva dirección IP para direccionar máquinas

6. Y SE LE ASOCIA A DICHA MÁSCARA, UNA DIRECCIÓN IP, A PARTIR DE LA DIFUSIÓN DIRIGIDA A LA ANTERIOR SUBRED (220.10.15.31). LO MAS CERCANA POSIBLE A ÉSTA Y QUE TENGA EL MISMO N° DE CEROS QUE LA NUEVA MÁSCARA CALCULADA

- Se le asocia la dirección  $220.10.15.32/27 = 220.10.15.0\textcolor{blue}{100000}/27$

### 7. NUMERAMOS HASTA LA DIFUSIÓN DIRIGIDA

- Se numeran las máquinas de la 33 (220.10.15.0010 0001) a la 47 (220.10.15.0010 1111) y hasta como máximo la 62 (220.10.15.0011 1110)
- Se calcula la dirección de difusión dirigida = 220.10.15.63 (220.10.15.0011 1111)

(foto)

### 4. Subred3:

5. SE CALCULA LA MÁSCARA de la siguiente subred de menor tamaño (Subred3) en función del nº máximo de máquinas que se desean conectar a Subred3. Los bits que se necesitan (para identificar equipos en la dirección IP) definen el nº de ceros de dicha máscara y el nº de ceros o bits para máquinas en la PARTE LOCAL DE MÁQUINA DE LA DIR IP asociada

- Si a la 3<sup>a</sup> subred se desean conectar 31 máquinas entonces  $2^6-2 > 31$
- La máscara es /26 (32 “unos” – 6 “ceros” = /26 “unos”)
- Por tanto, necesitamos 6 bits (ceros) en la máscara y 6 bits en la PARTE LOCAL DE MÁQUINA de la nueva dirección IP para direccionar máquinas

6. SE LE ASOCIA A DICHA MÁSCARA, UNA DIRECCIÓN IP, A PARTIR DE LA DIFUSIÓN DIRIGIDA A LA ANTERIOR SUBRED (220.10.15.63). LO MÁS CERCANA POSIBLE A ÉSTA Y QUE TENGA EL MISMO N° DE CEROS QUE LA NUEVA MÁSCARA CALCULADA

- Se le asocia la dirección  $220.10.15.64/26 = 220.10.15.0\textcolor{blue}{100000}/26$

### 7. NUMERAMOS HASTA LA DIFUSIÓN DIRIGIDA

- Se numeran las máquinas de la 65 (220.10.15.0100 0001) a la 95 (220.10.15.0101 1111) y hasta como máximo la 126 (220.10.15.0111 1110)

- Se calcula la dirección de difusión dirigida 220.10.15.127 (220.10.15.0111111)

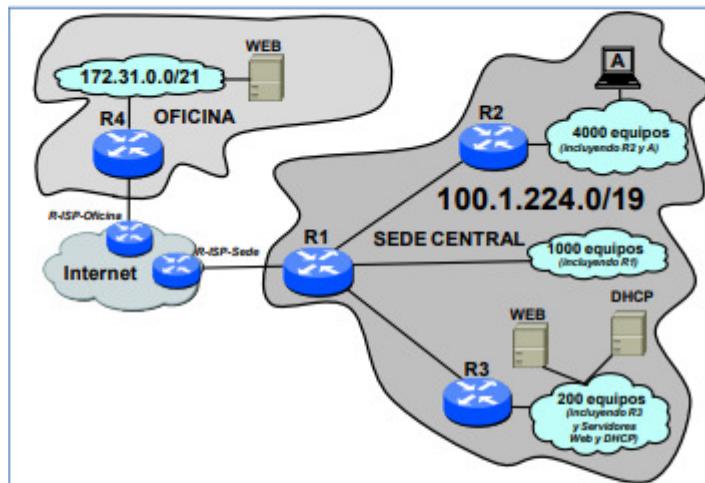
(foto)

### p. Ámbito de aplicación de direcciones IPv4:

- i. IP pública u oficial (externas): individuales, con coste. Salen a Internet.
- ii. IP privadas (internas): compartidas, gratuitas. Solo utilizadas en la red local.

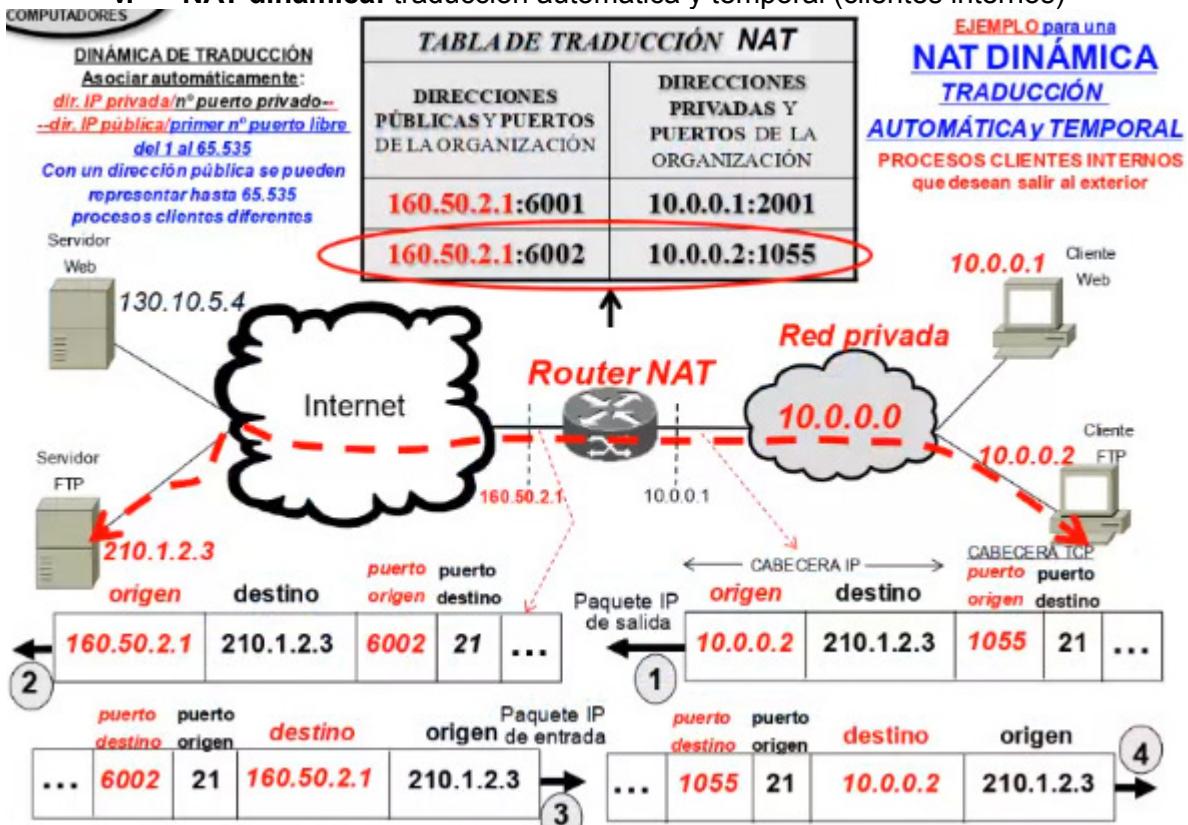
- iii. La IPv4 no permite que todos los equipos en Internet tengan una dirección IP pública propia, por lo que se utilizan IPs privadas mediante NAT en una red cualquiera para asignar a cada equipo y preservar el direccionamiento.
- q. **NAT o NAPT (Network Address (Port) Translation):** software o proceso de nivel de red del router E/S (no un protocolo de comunicaciones) que mantiene una tabla de traducción con las asociaciones de **sockets** públicos y privados (IP + nº puerto).
  - i. **Paquete IP de entrada:** traducción de sockets públicos a privados.
  - ii. **Paquete IP de salida:** traducción de sockets privados a públicos.
  - iii. **Objetivos:**
    1. No agotar el espacio de direccionamiento oficial (público) de IPv4.
    2. Minimizar el coste de direcciones IP públicas utilizando IPs privadas en entornos locales (domicilio, organización, ...).
    3. Asegurar que no haya un acceso directo desde Internet a la dirección real de un equipo, porque la dirección privada **no estará registrada** en ningún router en Internet.
  - iv. **Direcciones privadas de red (clase A, B y C):**
    - [10.0.0.0 hasta 10.255.255.255 \(una dirección de red clase A\)](#)
    - [172.16.0.0 hasta 172.31.255.255 \(16 direcciones de red contiguas de clase B\)](#)
    - [192.168.0.0 hasta 192.168.255.255 \(256 direcciones de red contiguas de clase C\)](#)
      - [192.168.1.0/255.255.255.0: Típica dirección de red clase C compartida en un organización o en el domicilio del usuario](#)

**Ejemplo:** supuesto 4



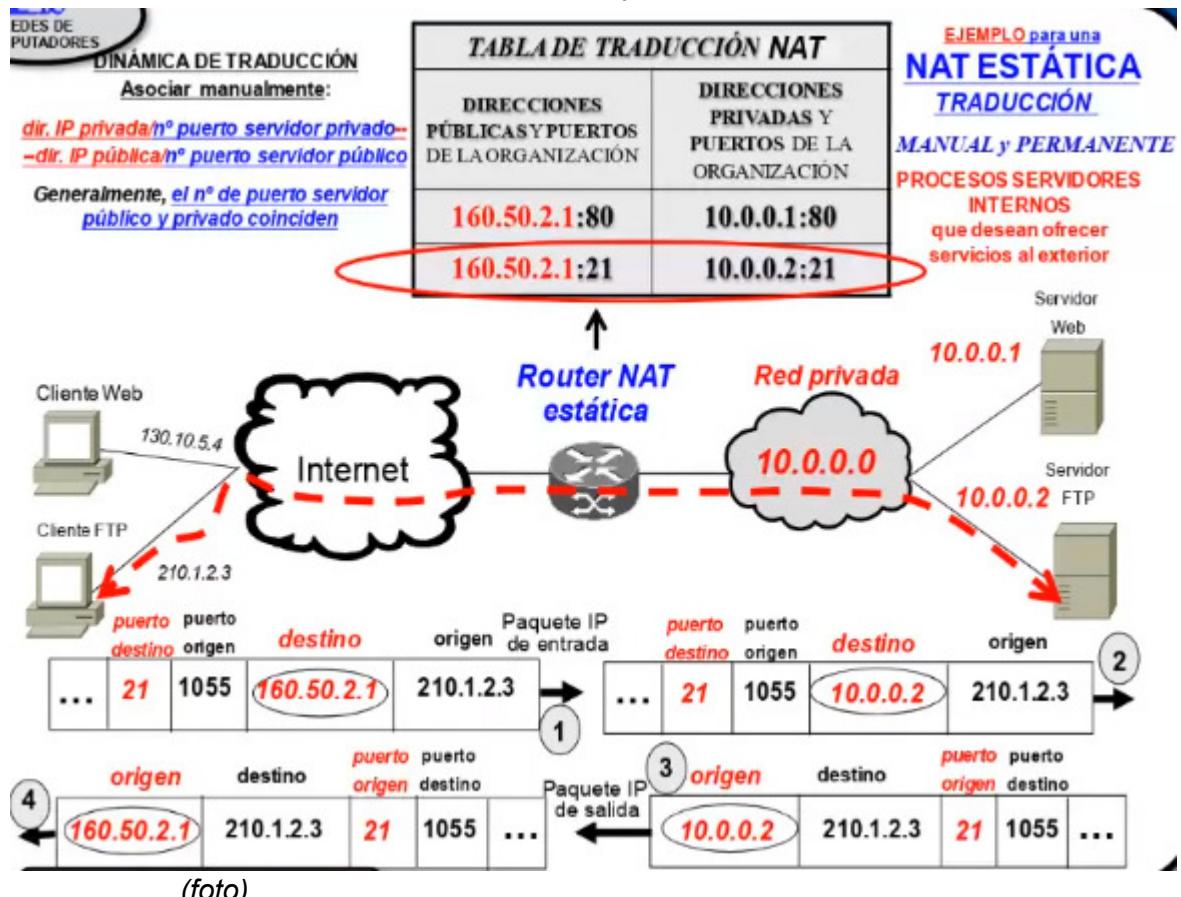
1. **Dirección clase B pública:** **100.1.224.0/19**
2. **Dirección clase B privada:** **172.31.0.0/21**
3. La traducción NAT es lenta. Por ello, se recomienda reservar las direcciones privadas a subredes sin muchos procesos conectados porque puede producir un cuello de botella en el router NAT. Es mejor optar por IPs públicas que sean encaminadas por Internet directamente.

## V. NAT dinámica: traducción automática y temporal (clientes internos)



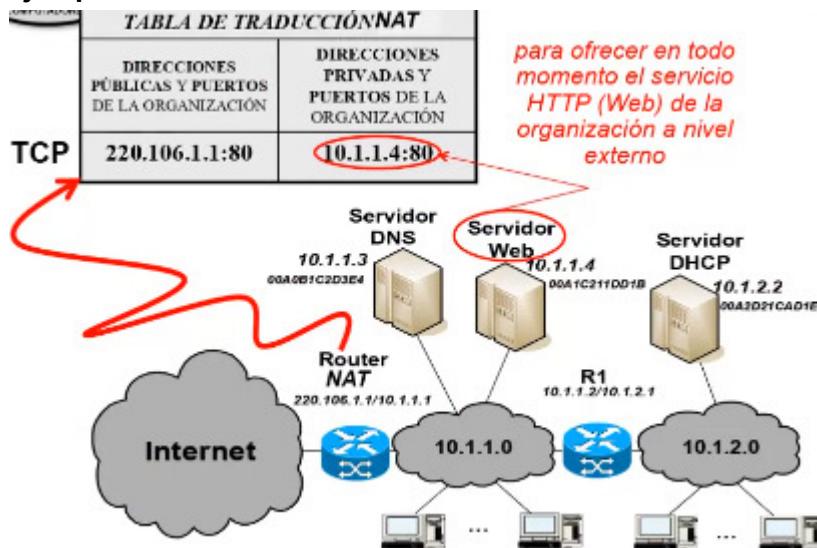
1. **Router NAT:** el más cercano al router del operador (ISP).
2. **Paquete IP de salida:**
  - a. **Dirección IP:** traduce **10.0.0.2** (IP privada, no encaminable) a **160.50.2.1** (IP pública de router asignada por ISP, encaminable).
  - b. **Nº puerto:** traduce de **1055** (nº puerto privado) a **6002** (primer nº puerto público libre del 1 al 65.535).
3. **Paquete IP de entrada:** cuando el router E/S detecta en el campo dirección IP destino **su dirección IP**, llama al proceso NAT para traducir la dirección pública por la privada asociada. Después, se hará lo mismo con el nº de puerto.

## vi. NAT estática: traducción manual y permanente (servidores internos)

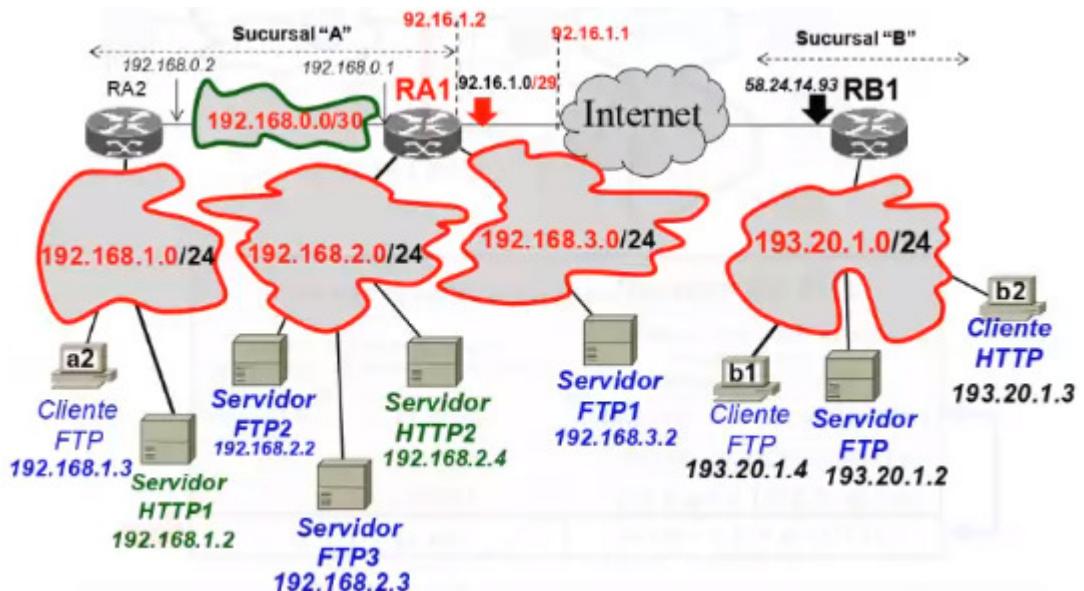


1. **Tabla de traducción NAT:** al ofrecer servidores al exterior, se deberán configurar manualmente las asociaciones de sockets. Será permanente, mientras no se borre la asociación manualmente.
2. **Dirección IP:** de pública a privada y viceversa.
3. **Nº puerto:** de pública a privada y viceversa. Generalmente, coinciden.
4. **Paquete IP de entrada:** cuando el router E/S detecta en el campo dirección IP destino **su dirección IP**, llama al proceso NAT para traducir la dirección pública por la privada asociada. Después, se hará lo mismo con el nº de puerto.

vii. **Ejemplo:**

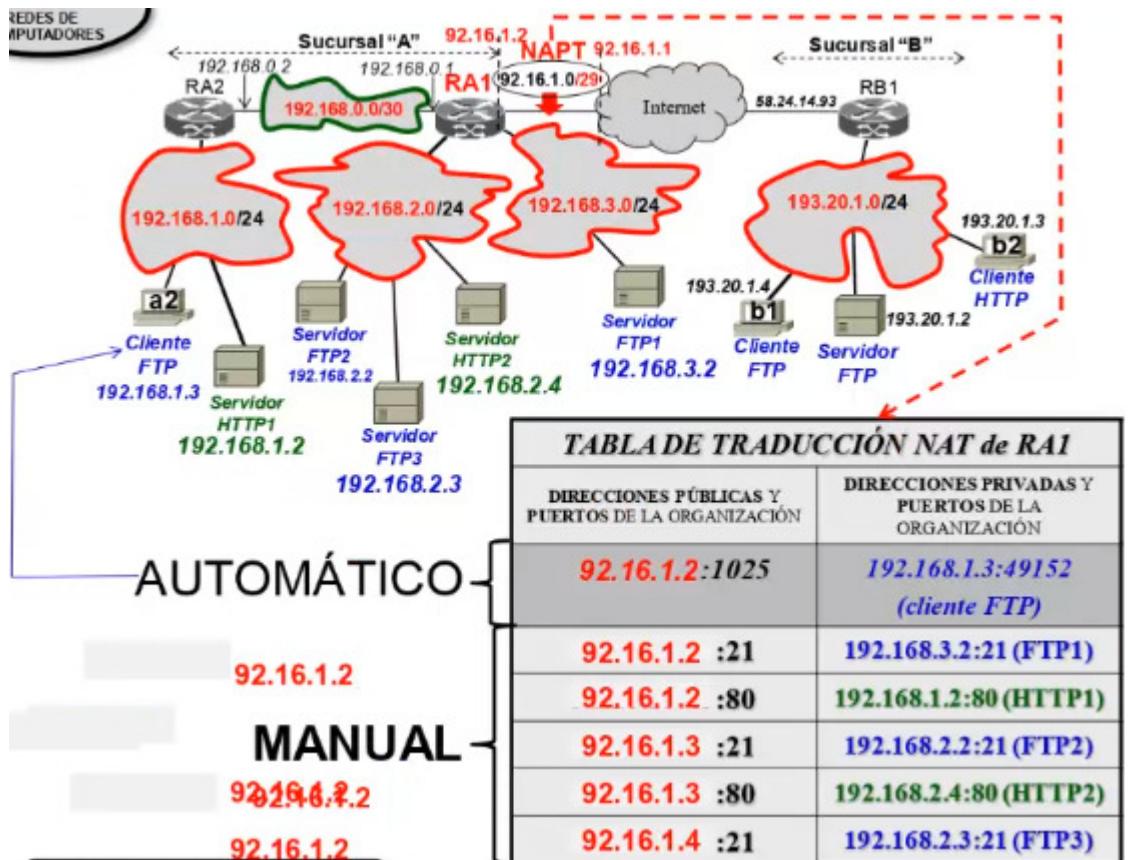


- viii. **Ejemplo:** una Organización dispone de 2 sucursales conectadas vía Internet. Se desea que todos los servicios de las dos sucursales sean accesibles para los clientes de dichas sucursales incluido cualquier cliente en Internet.



¿Qué funcionalidad extra tiene RA1 que no tiene RB1?

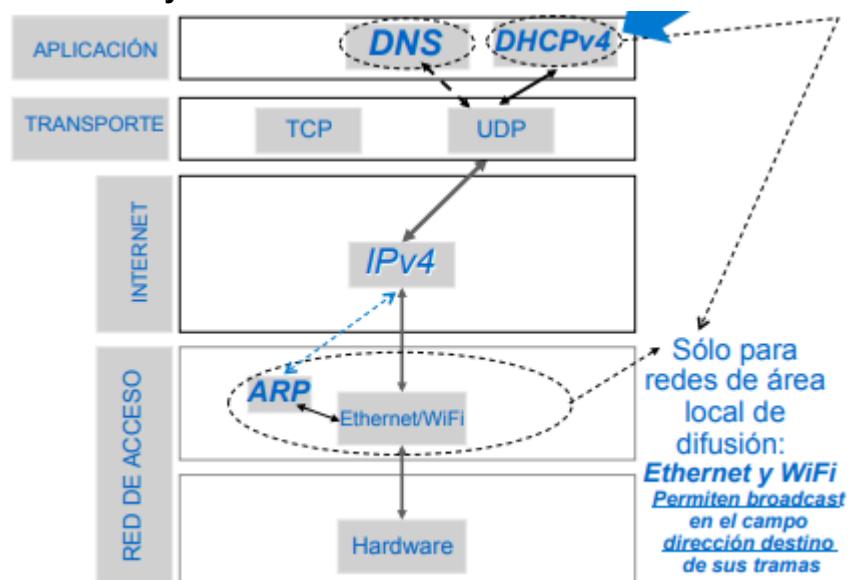
RA1 usa proceso NAT y RB1 no.



Hay dos servidores HTTP y tres servidores FTP. Si se quiere identificar públicamente a cada uno, coincidirían (IP de router E/S, TCP, 80). Para distinguirlos deben tener sockets distintos en la columna de sockets privados, pero no se puede cambiar ni el protocolo de transporte ni el nº de puerto (el nº puerto reservado de HTTP es 80 y el de FTP es 21).

Solo queda ampliar el nº de IPs que pueda tener el router E/S en su conexión con el router ISP para que pueda haber en una red privada tantos "servicios iguales" como IPs se tengan.

r. Protocolos y niveles TCP/IP relacionados con el direccionamiento IP:



- i. **ARP (Address Resolution Protocol):** protocolo de resolución de direcciones  
 → indica la dirección MAC Ethernet/WiFi asociada a la dirección IP de una máquina vecina en una red de comunicaciones de difusión (Ethernet o WiFi) (aquella que permite difusión a nivel de trama → MAC destino = 48 bits a 1) con una **Tabla ARP** o Caché ARP almacenada en memoria RAM.

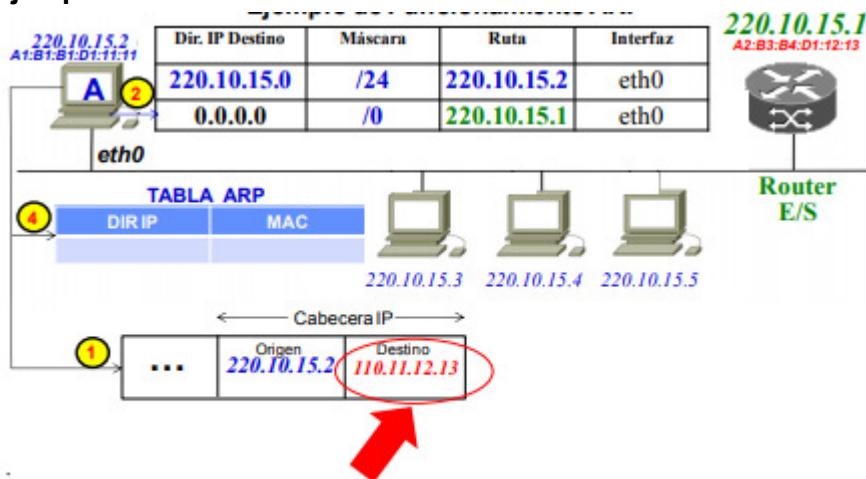
- *Dir IPv4 vecino1 --- MAC vecino1*
- *Dir IPv4 vecino2 --- MAC vecino2*
- *Dir IPv4 vecino3 --- MAC vecino3*
- *Dir IPv4 vecino 4 --- MAC vecino4*
- ...

**arp -a** → muestra tabla ARP

1. Solo da la dirección MAC del siguiente salto (vecino), no el siguiente a este (no vecino).
2. ARP fue diseñado por Xerox para sus equipos. Después, ese protocolo se adoptó en la arquitectura TCP/IP.
3. Cuando pasa un determinado tiempo de actividad (por ejemplo, 15 minutos) o se apaga el equipo, se pierde toda la información ARP. Se recuperará la información a medida que la máquina se vaya conectando con máquinas vecinas. Esto evita que el administrador de la máquina tenga que gestionar las altas o bajas puntuales de máquinas vecinas, incluyendo cambios en la tarjeta de comunicaciones (con direcciones MAC distintas).

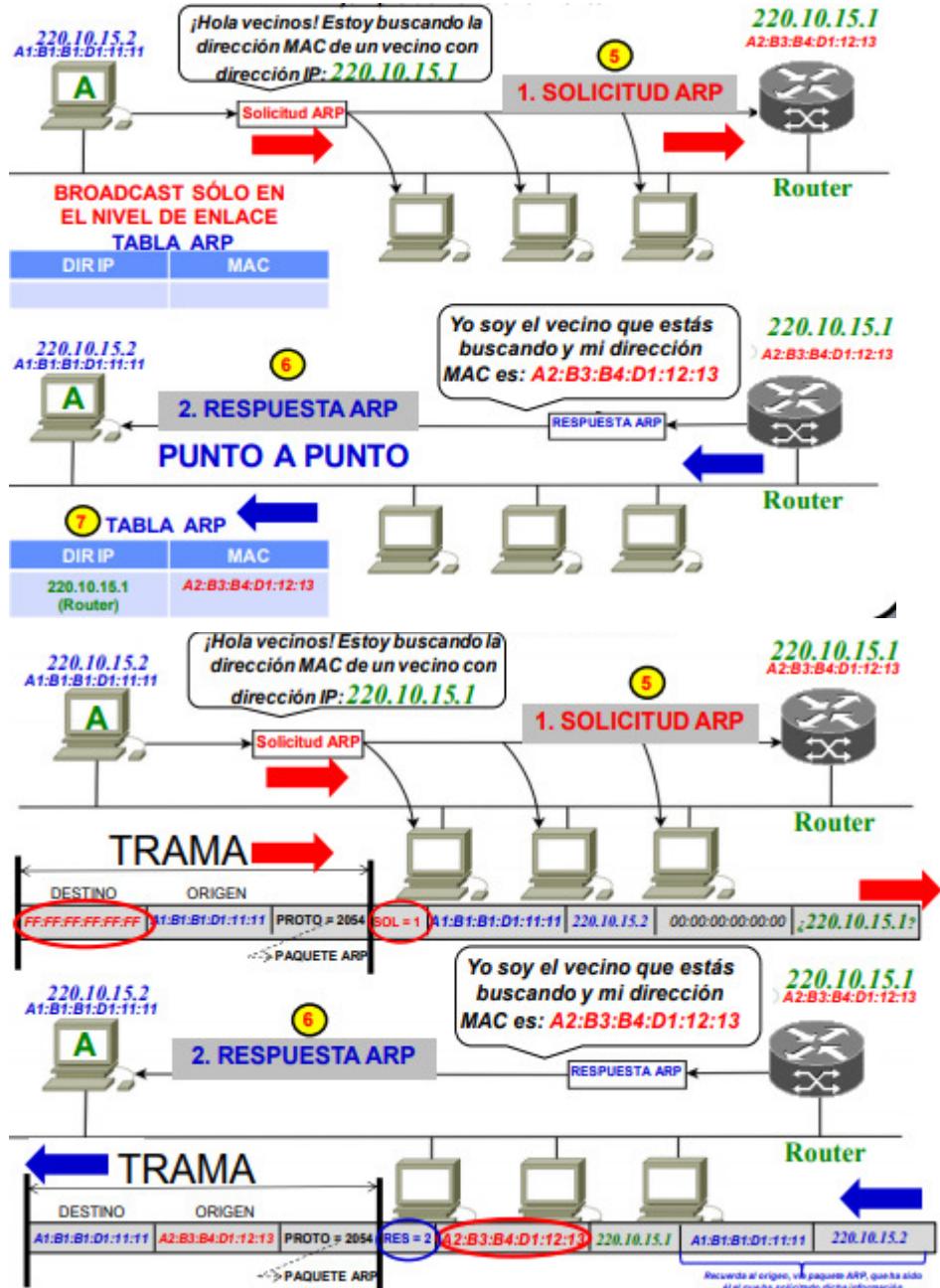
a. **arp -s** → añade entrada permanente a Tabla ARP.

#### 4. Ejemplo:



③ **Llamada de IP a la entidad ARP: Búscame la MAC de 220.10.15.1**

Como la tabla ARP no tiene dirección MAC vinculada a la dirección 220.10.15.1, pregunta por su dirección MAC para llenar la fila.

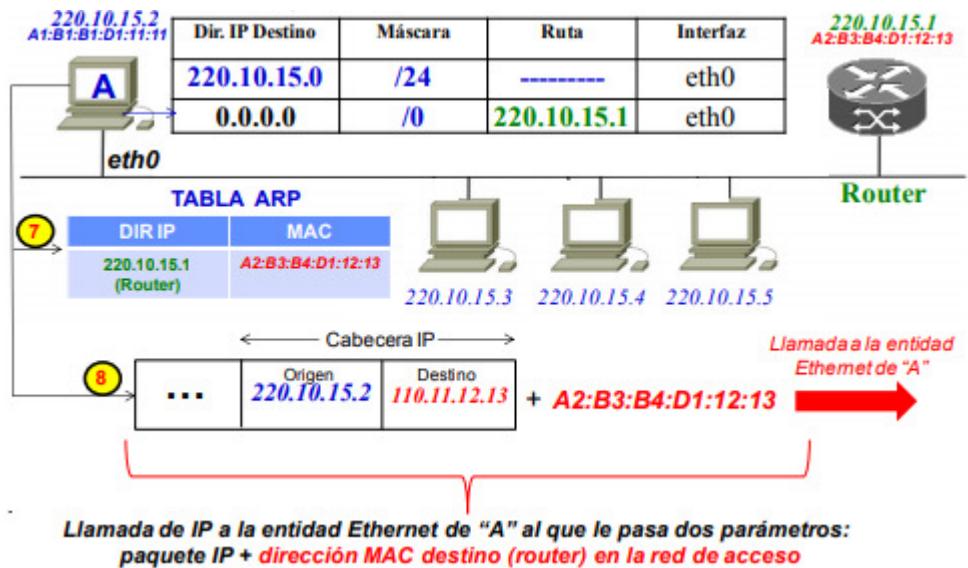


**TRAMA de solicitud ARP:** enviado a todo equipo vecino (MAC destino **broadcast**) + MAC origen + protocolo superior de paquete ARP (PROTO = 2054; PROTO = 2048 paquete IP).

**Solicitud ARP:** SOL=1 + MAC e IP origen + MAC vacío + IP destino. Se ponen MAC e IP origen para que todos los equipos vecinos pongan en sus tablas ARP la asociación para el equipo origen (para no tener que enviar una solicitud ARP en el futuro).

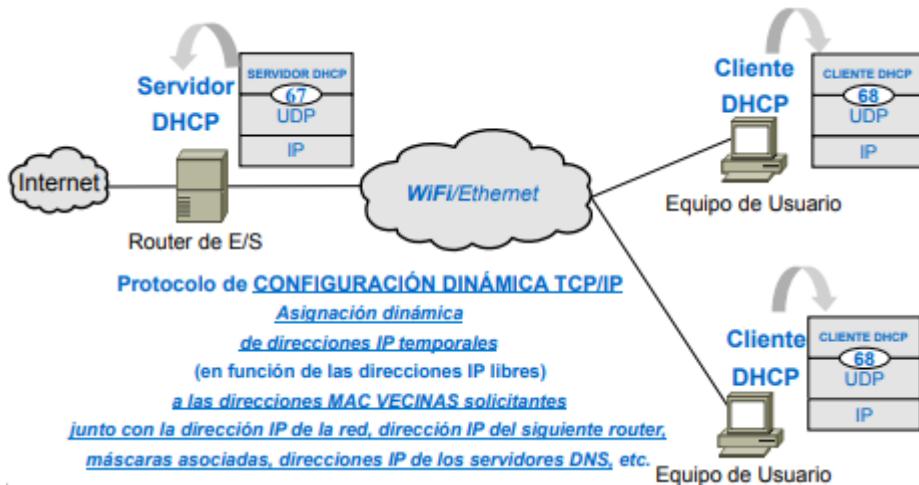
**TRAMA de respuesta ARP:** enviado de vuelta al equipo solicitante.

**Respuesta ARP:** RES = 2 + MAC e IP origen (MAC vacío relleno) + MAC e IP destino.

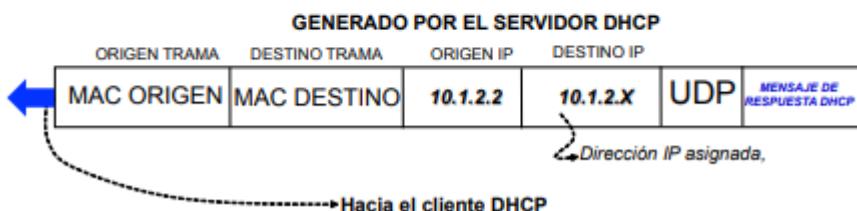
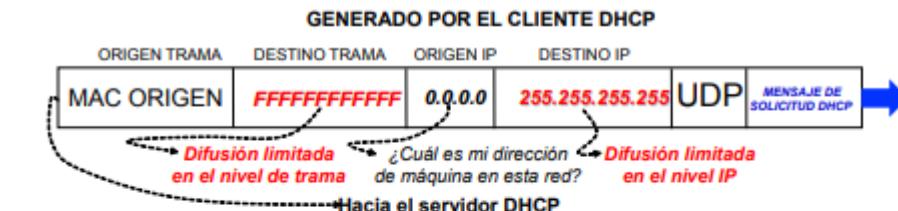


Ya puede rellenarse la tabla **ARP**. Se envían al nivel de enlace **dos parámetros**: paquete IP + MAC destino ⇒ trama Ethernet/WiFi.

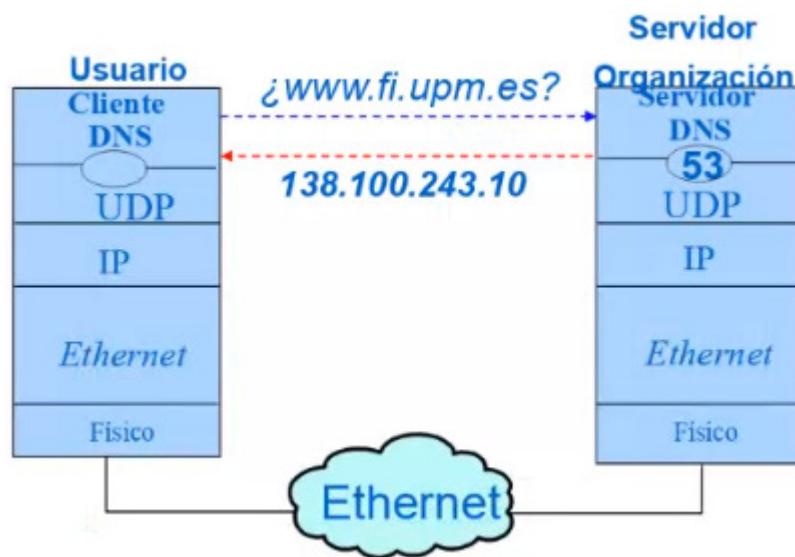
## ii. DHCPv4:



1. **Cliente DHCP:** nº puerto 68. Todo equipo (p. ej: un móvil) tiene uno.
2. **Servidor DHCP:** nº puerto 67. Generalmente, instalado en router E/S.
3. **Ejemplo:** persona entra a un bar y quiere conectarse a su WiFi desde su móvil.



- a. **Cliente DHCP (móvil)**: envía paquete DHCP en difusión limitada buscando el servidor DHCP del router E/S.
  - i. MAC origen y destino (*broadcast*) + IP origen (vacío) y destino (*broadcast*).
- b. **Servidor DHCP (router E/S)**: devuelve paquete DHCP con la dirección IP asignada al móvil para que utilice su servicio.
  - i. MAC origen y destino + IP origen (red) y destino (asignada a cliente DHCP).
- iii. **DNS**: traduce una dirección simbólica ([www.fi.upm.es](http://www.fi.upm.es)) a una dirección IP (138.100.243.18), mediante entidades DNS a nivel de aplicación sobre UDP. El servidor DNS lo tendrá el equipo que ofrezca **procesos servidores** en Internet. El **número de puerto** del servidor DNS es el 53.

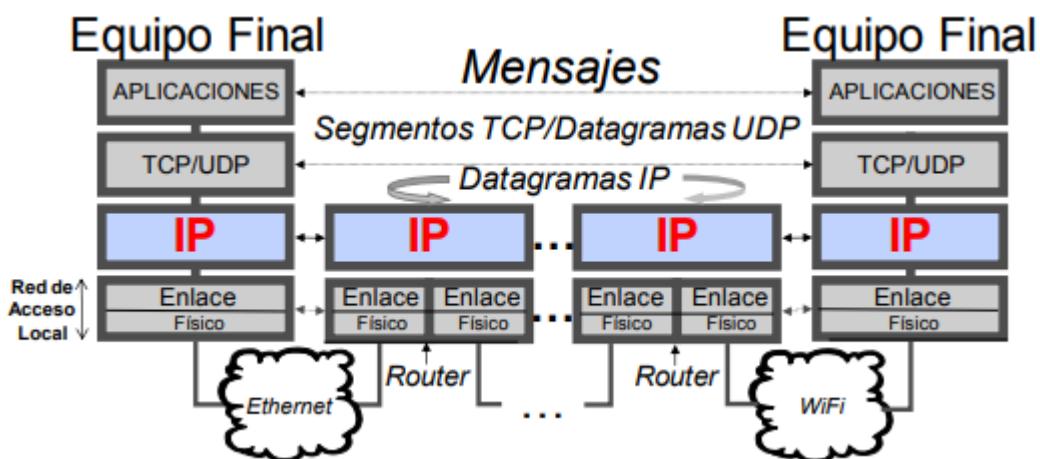
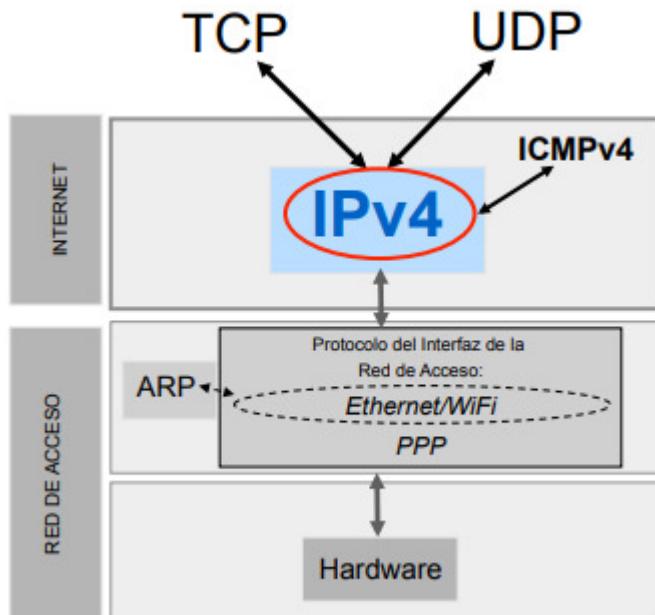


1. **Ejemplo:** cuando se pasa al cliente HTTP una dirección simbólica.



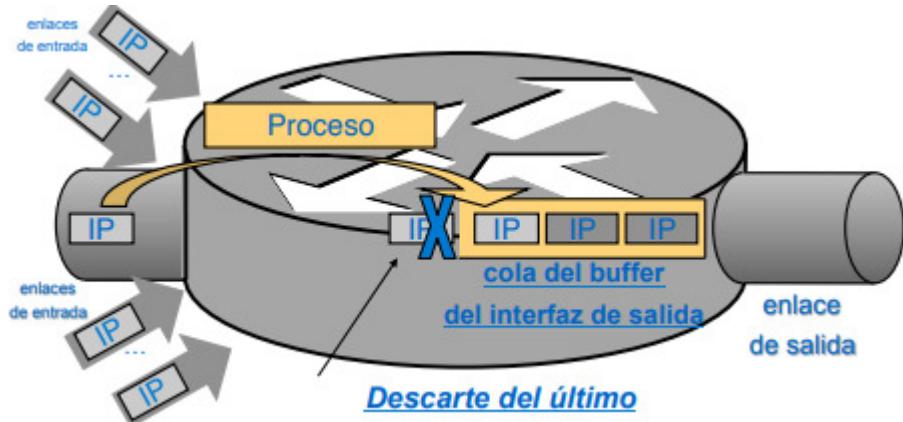
- Cuando se pasa al cliente HTTP una dirección simbólica, este llama al cliente DNS para que la envíe al servidor DNS.
- Servidor DNS**: devolverá la IP asociada a la dirección simbólica.

- c. Una vez obtenida la dirección IP de la página web buscada, se envía al servidor HTTP.
  - d. **Servidor HTTP:** devolverá la página web.
- s. **Protocolo IPv4:** encaminamiento rápido (no fiable) entre equipos vecinos, sin control de errores (recuperación) ni control de flujo. Es igual que Ethernet.



- i. **Congestión del router:** cuando no se dispone de almacenamiento en los buffers de salida, no pueden guardarse los **paquetes IP** y se eliminan (no se

recuperan). Es el principal motivo de **pérdida de paquetes IP** en Internet.



## ii. Formato de datagrama IP o paquete IP:

Longitud Total MÁXIMA



1. **Cabecera IP:** 20 bytes (sin opciones) - 60 bytes (máximo de opciones).
2. En el diseño original de IPv4, la longitud total máxima podía ser de 65.535 octetos o bytes ( $2^{16} - 1$ ).
3. Sin embargo, la MTU de salida (unidad máxima de transferencia) de la trama Ethernet es de 1.500 bytes, longitud que no debe superar.

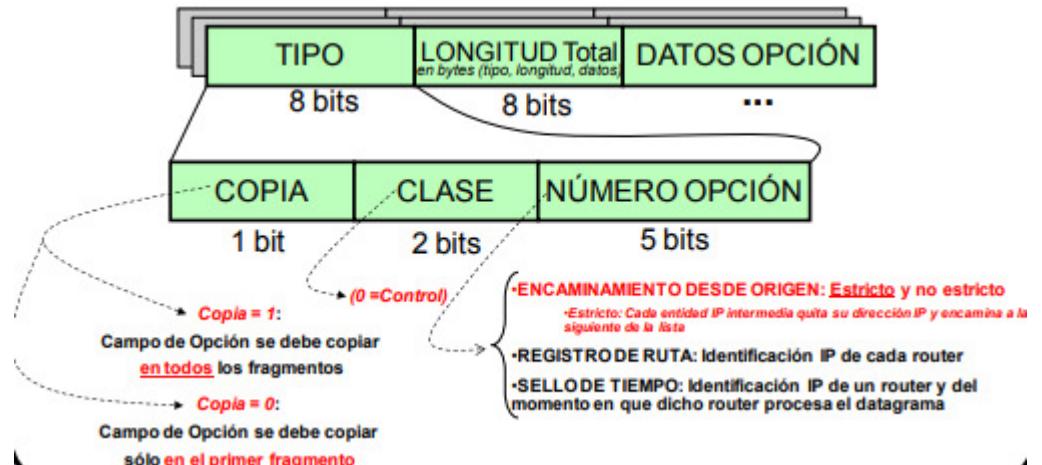
### iii. Formato de cabecera de datagrama IP o paquete IP:



(foto)

1. **Versión (4 bits):** 4
2. **Longitud de cabecera (4 bits):** nº de bloques de 4 bytes que aparecen en la cabecera (mínimo de 5 bloques, con máximo de 10 opciones).
3. **Tipo de servicio (TOS) (8 bits):** codificación particular dependiente de los servicios contratados al ISP (proveedor de servicios de Internet). Por ejemplo, que para una aplicación de videoconferencia se quiera la máxima calidad de servicio (todos los paquetes IP que encapsulen datos de audio y vídeo vayan por los routers menos congestionados en la red de routers del ISP).
4. **Longitud total (16 bits):** hasta 65.535 bytes ( $2^{16} - 1$ ). Sin embargo, al ser MTU = 1.500 bytes, ese será el máximo práctico.
5. **Identificador (16 bits):** de paquete.
6. **0 (1 bit):** reservado.
7. **DF (Don't Fragment) (1 bit):** a 1, no desea que se fragmente el paquete IP y, de ser de longitud mayor a la posible, se desecha.
8. **MF (More Fragments) (1 bit):** a 0, es el último fragmento del paquete.
9. **Desplazamiento (13 bits):** orden de fragmento en un paquete (de haber), según el nº de bloques de 8 bytes en fragmentos anteriores.
10. **TTL (time to live o tiempo de vida) (8 bits):** máximo de **entidades IP intermedias** que puede atravesar un paquete IP. En cada equipo intermedio, se decrementa TTL en una unidad. Si el valor llega a 0 en un equipo intermedio, se desecha el paquete IP.
  - a. Este campo evita los **viajes en bucle** por una mala configuración de las tablas de encaminamiento, por ejemplo.
11. **Protocolo (8 bits):** TCP = 6, UDP = 17, ICMP = 1.

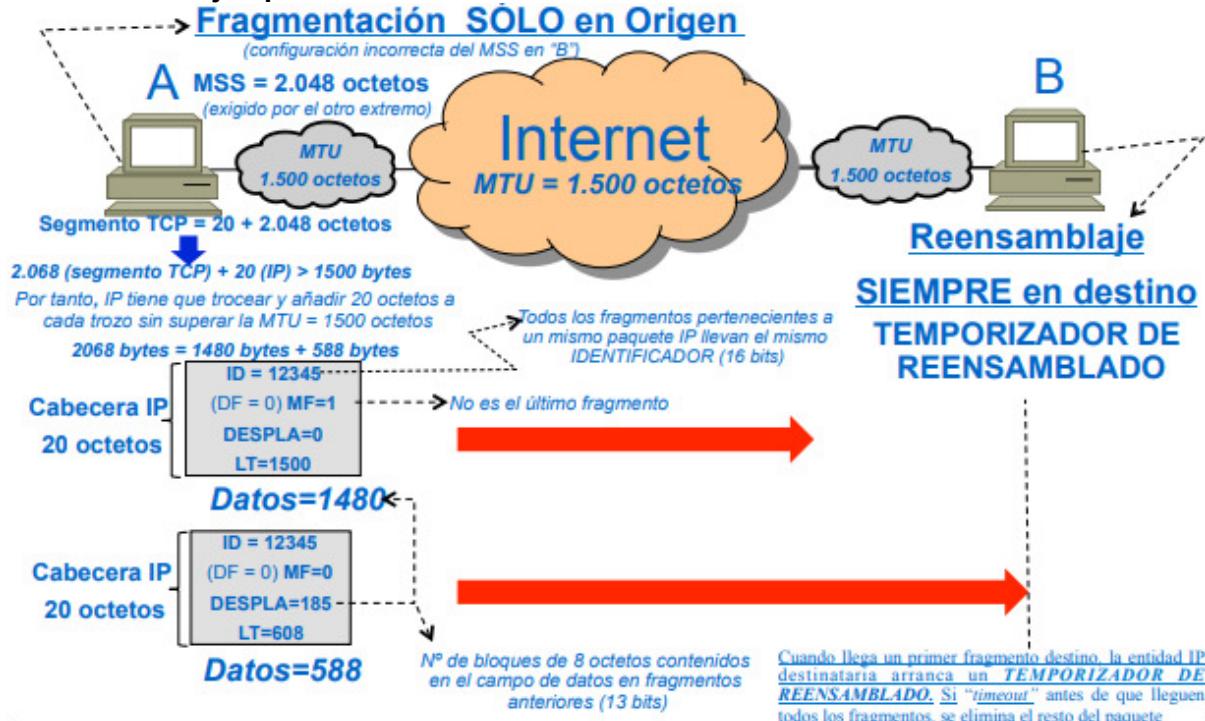
- 12. Suma de comprobación (suma XOR) (16 bits):** suma en bloques de 16 bits de la cabecera (redundancia) para detectar bits de error en la cabecera IP. Si tras la transmisión la suma de comprobación es distinta (XOR resalta los bits cambiados), se desecha el paquete IP.
- 13. IP origen (32 bits):** no es modificado en la comunicación en Internet (solo en routers de acceso con proceso NAT).
- 14. IP destino (32 bits):** no es modificado en la comunicación en Internet (solo en routers de acceso con proceso NAT).
- 15. Opciones de servicios adicionales (0 - 40 bytes):** formato TLV (Tipo-Longitud-Valor):



- Encaminamiento desde origen:** se especificará en el campo **datos** la ruta de IPs que deberá seguir el paquete IP.
    - Estricto:** se pasa **únicamente** por los routers indicados.
    - No estricto:** se puede pasar por IPs intermedias no indicadas entre las de paso obligatorio.
  - Registro de ruta:** el campo **datos** se deja vacío para que cada router que procese el paquete IP guarde en él su dirección IP. Cuando se llegue al destino, se verá por qué routers ha pasado el paquete.
  - Sello de tiempo:** el campo **datos** se deja vacío para que cada router que procese el paquete IP guarde en él su dirección IP y el instante en el que lo han procesado.
- iv. **Rutina de comprobación de la cabecera:**
- Suma de comprobación:** suma de bloques de 16 bits y, si coinciden las sumas, procesa la siguiente comprobación.
  - Versión:** comprueba que la versión es la 4.
  - Longitud de la cabecera:** comprueba que el valor esté dentro de los límites de la implementación del diseño de la cabecera IP.
  - Longitud total:** comprueba que el valor esté dentro de los límites de la implementación del diseño de la cabecera IP.
  - TTL - 1 (solo entidades IP intermedias):** si el resultado es diferente a 0, habrá que actualizar el campo TTL y la suma de comprobación. Si el resultado es 0, se elimina el paquete.
- v. **Fragmentación IPv4:** se realiza siempre que la longitud del paquete IP sea superior a 1.500 bytes, y solo en el equipo origen.

Hay que **evitar en todo momento** fragmentar un paquete IP porque, al crear más de una trama, aumenta el número de cabeceras por Internet (mayor carga de tráfico y proceso) y la probabilidad de perder un paquete IP (perder un fragmento del paquete IP provoca la pérdida del paquete IP completo).

**Ejemplo:**



(foto)

### 1. Fragmentación (en origen):

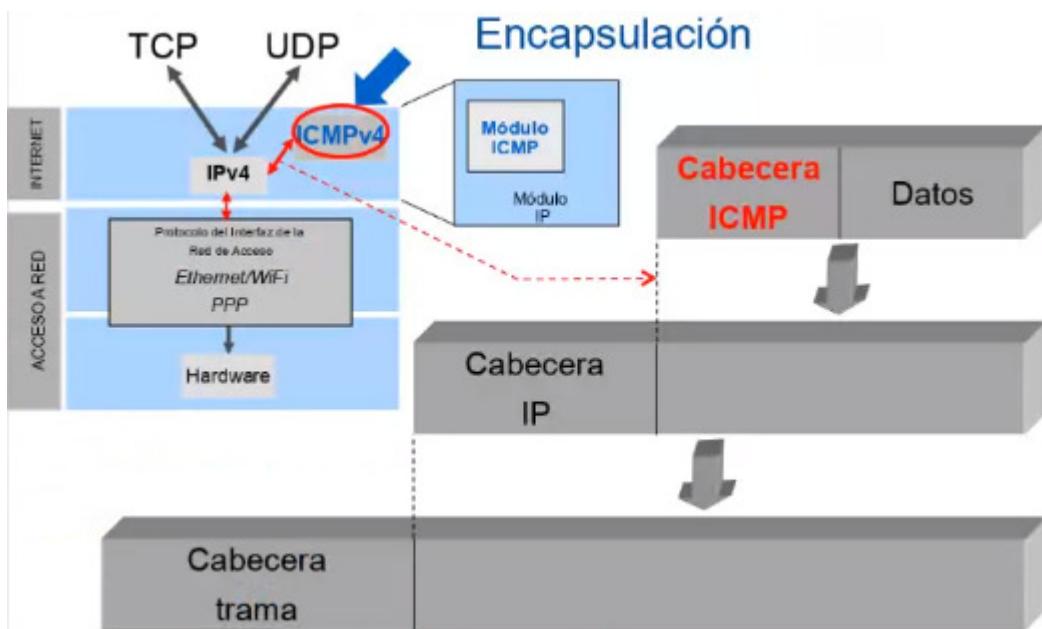
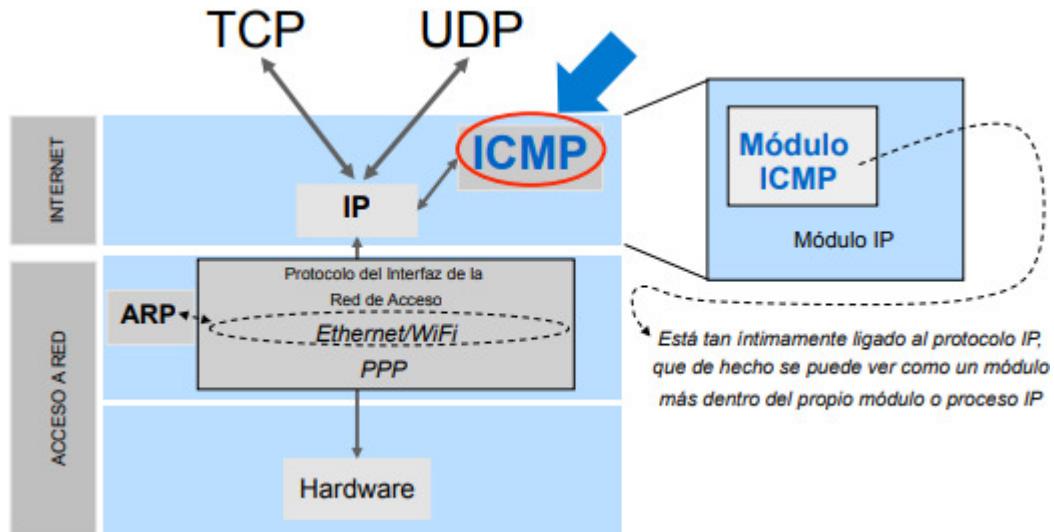
- El mensaje MSS es de 2.048 bytes, al que se le suman las cabeceras de TCP (20 bytes) e IP (20 bytes).
- Como supera la MTU (1.500 bytes), debe fragmentarse el **segmento TCP** en partes de máximo **1.480 bytes**, porque a cada una habrá que añadirle una cabecera IP (20 bytes).  
 $2.068 \text{ bytes (MSS + TCP)} = 1.480 \text{ bytes} + 588 \text{ bytes.}$
- Formato cabecera IP de un fragmento:**
  - ID (identificador):** igual para todos los fragmentos.
  - DF (Don't Fragment):** 0, si puede fragmentarse el paquete.
  - MF (More Fragments):** 1, si vienen más fragmentos.
  - Desplazamiento:** nº de **bloques de 8 bytes** contenidos en fragmentos anteriores.
  - LT (longitud total):** número de bytes del **paquete IP**.

### 2. Reensamblaje (en destino):

- Los fragmentos del paquete IP pueden llegar desordenados por seguir rutas distintas en Internet.
- En el equipo destino, se pausa el procesado de un fragmento si indica que **MF = 1 o DESPLA ≠ 0**, y se ordenan los fragmentos según DESPLA.
- Temporizador de reensamblado:** arranca cuando llega el primer fragmento de un paquete IP. Si se acaba el tiempo (**timeout**) y no

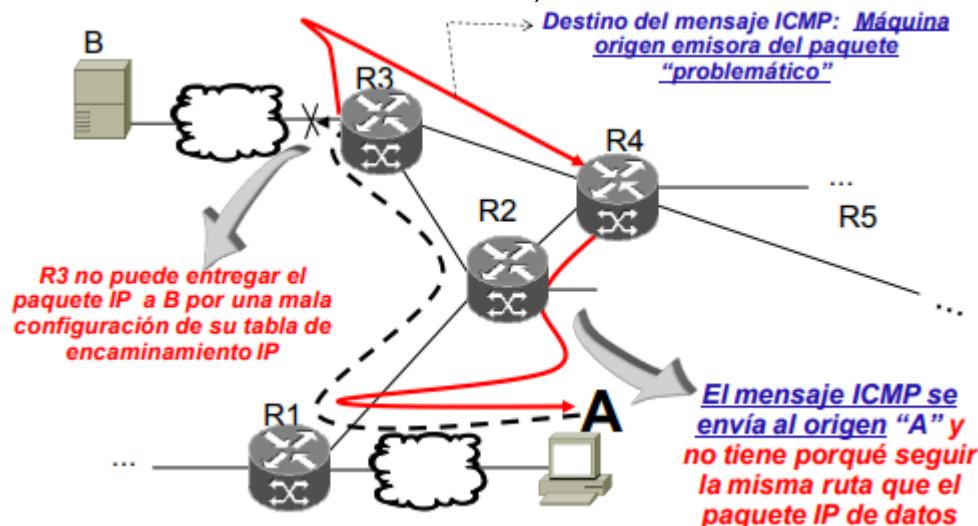
han llegado todos los fragmentos de un paquete IP, se eliminan los fragmentos de paquete que ya han llegado.

- t. **Protocolo ICMPv4 (Internet Control Message Protocol version 4):** protocolo de envío de mensajes de control en Internet (informes de fallos y consultas). Puede considerarse un módulo más dentro del módulo IPv4. Se encuentra en un subnivel superior a IPv4 dentro del nivel de red porque un mensaje ICMP se encapsula en un paquete IP.



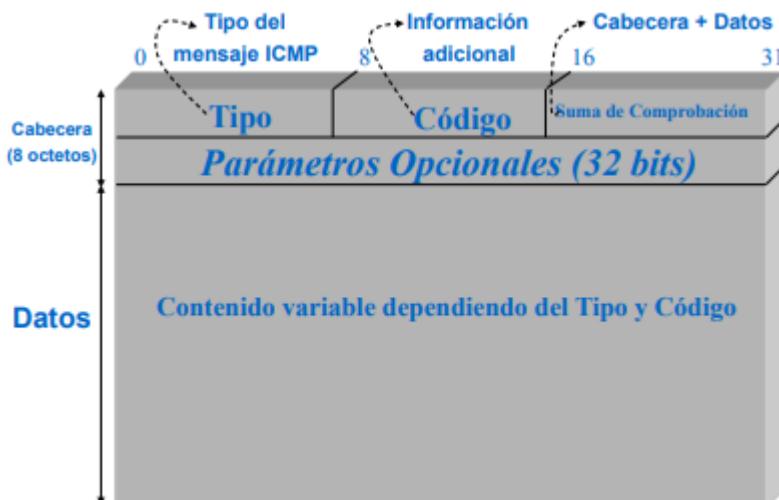
- i. ICMP no hace más fiable a IPv4.

- ii. **Ejemplo:** informe de fallo por destino inalcanzable (mala configuración en la tabla de encaminamiento IP de un router).



1. **Mensaje ICMP:** sale del router que ha dado el fallo indicando como IP destino la dirección IP origen del paquete IP problemático. No importa el camino de vuelta que realice el mensaje.

- iii. **Formato:** cabecera ICMP

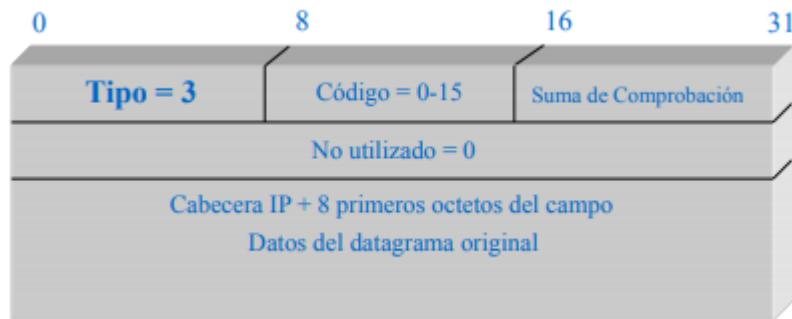


1. El **código** define el motivo del mensaje ICMP.
2. A diferencia de IP, ICMP aplica la suma de comprobación a todo el mensaje (PDU = cabecera + datos) en lugar de solo la cabecera (PCI).
3. Como MTU en Ethernet es de 1.500 bytes y el mensaje ICMP debe encapsularse con una cabecera IP (20 bytes, mínimo), podrá ser una longitud máxima de 1.480 bytes.

- iv. **Tipos de mensajes ICMPv4:**

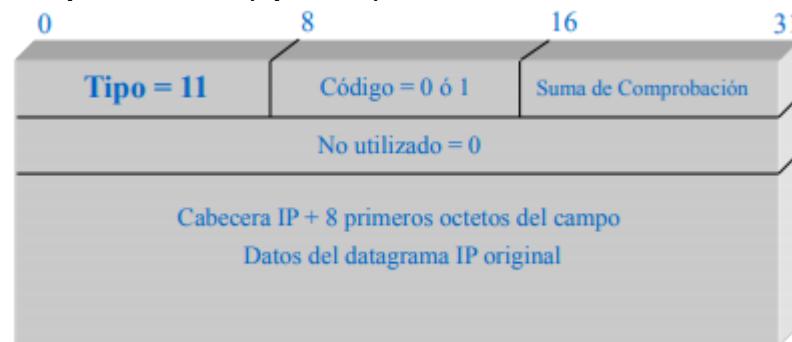
1. **Informes de fallos:** problemas que un equipo puede encontrar al procesar un paquete IP.

- a. **Destino inalcanzable (tipo = 3):** tabla de encaminamiento mal configurada.



- i. **(0):** red no alcanzable (desde un router o el equipo origen), por no tener información de encaminamiento en su tabla IP.
- ii. **(1):** equipo final no alcanzable o sin respuesta ARP. Hay información de encaminamiento IP, pero el equipo está apagado (por ejemplo).
- iii. **(2):** protocolo superior de transporte no coincidente.
- iv. **(3):** nº de puerto inactivo. Desde el nivel de transporte, se procura acceder a un servidor HTTP por el nº de puerto y está apagado.
- v. **(5):**

- b. **Tiempo excedido (tipo = 11):**

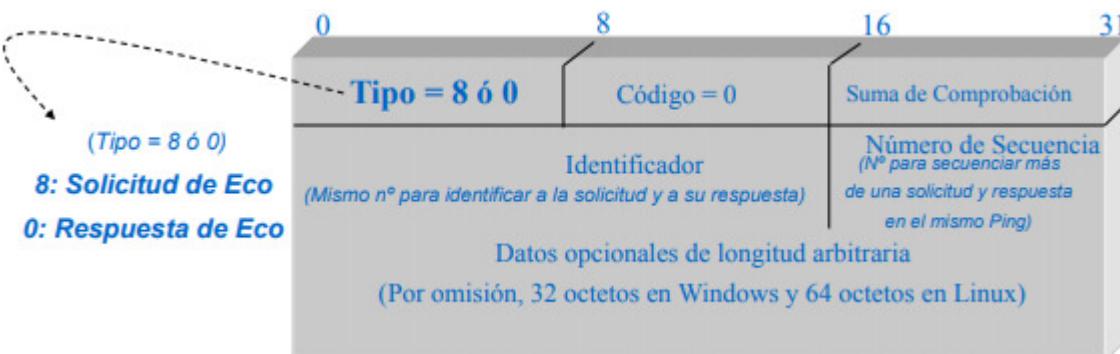


- i. **(0):** TTL = 0 en un router.
- ii. **(1):** timeout en equipo final (temporizador de reensamblado)

- c. **Problemas con los parámetros:** información ininteligible en la cabecera del paquete IP.

2. **Consultas:** datos sobre una máquina pedidos por otra.

- a. **Solicitud y respuesta de eco (tipo 8 o 0):** comprobación de si una máquina está conectada y responde a nivel IP o ICMP.



*(foto)*

- Identificador:** todos los paquetes enviados y recibidos en el mismo comando **ping** deben tener el mismo nº identificador.
- Nº de secuencia:** para diferenciar paquetes enviados y recibidos dentro de un mismo **ping**. Por ejemplo, Windows envía 4 paquetes por **ping**.

### 3. Usos básicos del comando **ping**:

- Saber si un equipo en Internet está conectado**
- Conocer el número de mensajes ICMP enviados, recibidos y perdidos por el camino**
  - Si hay pérdidas de mensajes ICMP, seguramente, hay congestiones de algún router en el trayecto por Internet
- Calcular el tiempo aproximado (mínimo, máximo y promedio) de ida y vuelta de las solicitudes y correspondientes respuestas ICMP**

**Round Trip Time (RTT):** tiempo de ida y vuelta del **ping**.

- Conocer el nº de routers entre el origen y destino, mediante el decremento del contenido del campo TTL inicial en la cabecera IP**
- Obtener la dirección IP asociada a una dirección simbólica**

```
C:\>ping www.movistar.com

Haciendo ping a www.movistar.com [194.224.110.42] con 32 bytes de datos:
Respuesta desde 194.224.110.42: bytes=32 tiempo=15ms TTL=247
Respuesta desde 194.224.110.42: bytes=32 tiempo=8ms TTL=247
Respuesta desde 194.224.110.42: bytes=32 tiempo=7ms TTL=247
Respuesta desde 194.224.110.42: bytes=32 tiempo=23ms TTL=247

Estadísticas de ping para 194.224.110.42:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 7ms, Máximo = 23ms, Media = 13ms
```

- IP:** 194.224.110.42 ([www.movistar.com](http://www.movistar.com)), encendido.
- Datos:** 32 bytes (Windows).
- 4 solicitudes de eco y 4 respuestas de eco.
- TTL = 247:** se han atravesado 8 routers (255 - 247). TTL se inicializa a 255 en el equipo destino (movistar).
- Si no se recibe respuesta a los paquetes, no tiene por qué estar apagado el equipo final, sino que haya deshabilitado por firewall las respuestas a solicitudes de eco. Suele hacerse para evitar que

crackers sepan si un equipo está encendido o no.

```
C:\>ping www.upm.es

Haciendo ping a www.upm.es [138.100.200.6] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 138.100.200.6:
  Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

f. Opciones:

- i. **ping -l 5 IP** → enviar paquetes de 5 bytes de datos a IP.
- ii. **ping -i TTL IP** → fijar máximo de routers a atravesar.

```
C:\>ping -i 5 www.movistar.com

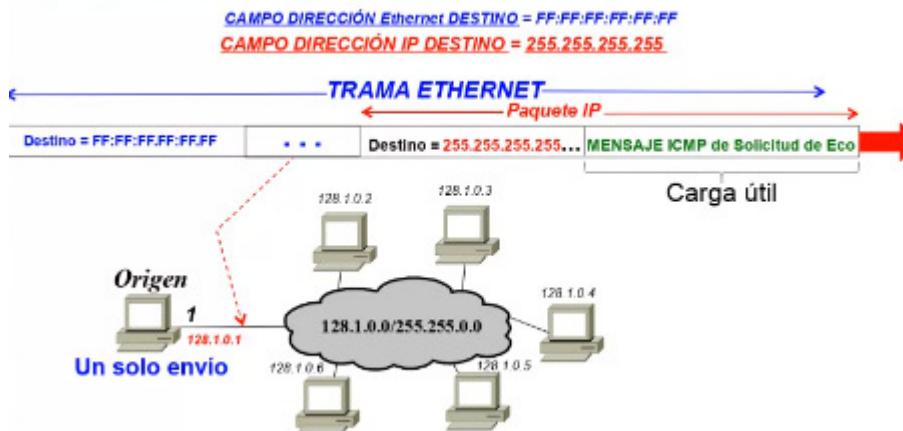
Haciendo ping a www.movistar.com [194.224.110.42] con 32
Respuesta desde 80.58.106.169: TTL expirado en tránsito.

Estadísticas de ping para 194.224.110.42:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

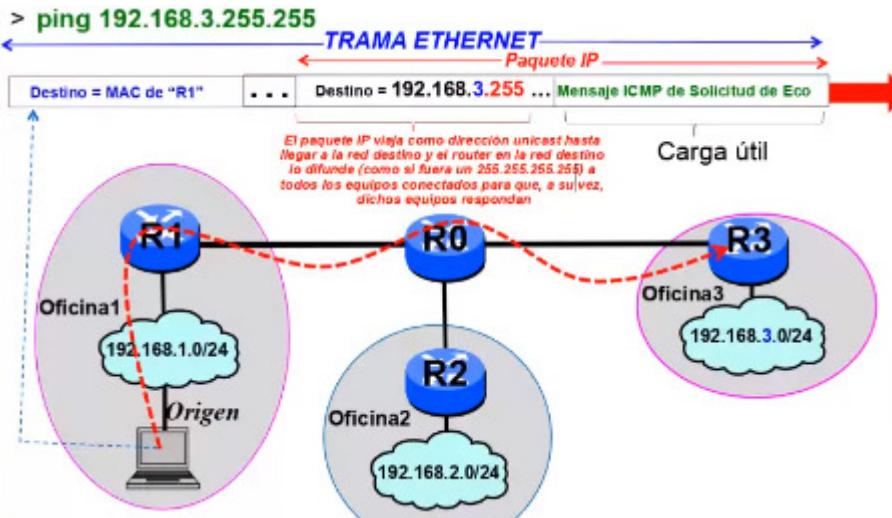
- iii. **ping -j host-list IP** → ruta de origen **no estricta**.
- iv. **ping -k host-list IP** → ruta de origen **estricta**.

4. Ejemplo: ping en difusión limitada (broadcast).

> **ping 255.255.255.255**



## 5. Ejemplo: ping en difusión dirigida.



**ERROR:** el *ping* es 192.168.3.255