

# TEMA 4: REDES CONMUTADAS E INTERNET

Las funciones y servicios en TCP/IP son: encaminamiento, conmutación, interconexión de redes y, en el modelo OSI, control de congestión. Ejemplo de protocolos de red son: X.25 e IP.

## 1. El protocolo IP

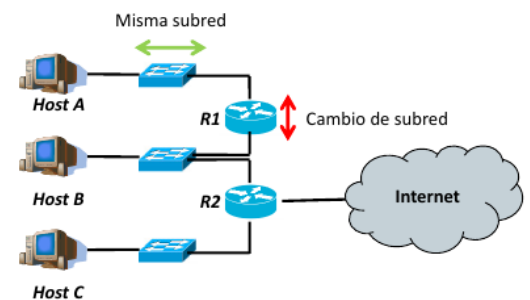
IPv4 es la versión más extendida del protocolo IP. Define direcciones de 32 bits que se suelen representar en notación decimal con puntos. Este protocolo realiza:

- Interconexión de redes y direccionamiento en Internet. El direccionamiento se concibe para simplificar la comunicación de una manera jerárquica.
- Retransmisión salto a salto entre hosts y routers.
- **No está orientado a conexión** y es **no fiable**: máximo esfuerzo (“best effort”).
  - No hay negociación o “handshake”.
  - No existe control de errores ni de flujo.
- La unidad de datos (paquete) de IP se denomina datagrama.
- IP gestiona la “fragmentación”.

### 1.1 Subred

*“Para determinar las subredes, separe cada interfaz de los hosts y routers, creando redes aisladas. Dichas redes aisladas se corresponden con las subredes.”*

Una subred es una red donde está ubicado el dispositivo, pero no es un router. Para interconectar dispositivos a una subred se utilizan conmutadores (switches).



### 1.2 Máscara

La máscara de subred es utilizada para el direccionamiento IP, que modo que ésta divide la dirección IP en dos partes: una correspondiente a la subred y otra al dispositivo dentro de la misma. La especificación de la máscara de (sub)red puede hacerse de dos maneras, siendo la más intuitiva aquella en la que se sigue la misma notación que las direcciones IP: 32 bits con 4 octetos separados por puntos.

- Dirección IP → 200.27.4.112 = 11001000.00011011.00000100.01110000
- Máscara de subred → 255.255.255.0 = 11111111.11111111.11111111.00000000

En la máscara de subred, los 1s representan la porción de la dirección IP que representa la subred, mientras que los 0s representan la porción para direccionar el dispositivo (host) dentro de la red. Por simplicidad, las máscaras se restringen a presentar todos los 1s agrupados a la izquierda para posibilitar una representación comprimida de la máscara de subred, donde se especifican únicamente el número de 1s en la máscara, de modo que en 200.27.4.112/24, el /24 implica una máscara de subred 255.255.255.0.

Dada la información de la dirección IP y la máscara de subred, basta con realizar la operación AND binaria entre éstas para obtener la **dirección de la subred** a la que pertenece el dispositivo:

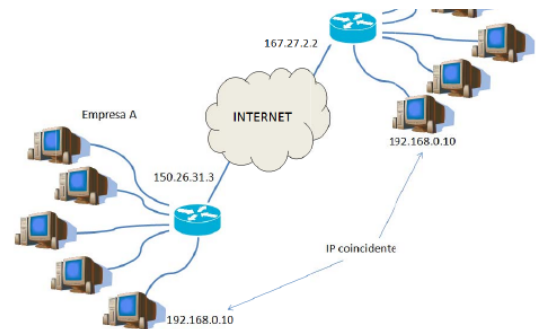
$$\begin{array}{r} 200.27.4.112 = 11001000.00011011.00000100.01110000 \\ \quad \quad \quad \& \quad \quad \quad \& \\ 255.255.255.0 = 11111111.11111111.11111111.00000000 \\ \hline \text{Subred} \rightarrow 200.27.4.0 = 11001000.00011011.00000100.00000000 \end{array}$$

Nótese que la elección de la máscara de subred está relacionada con el número de dispositivos o hosts que se quieren albergar en la misma, de modo que el número de dispositivos será igual a  $2^{\text{\#ceros}} - 2$  (el -2 se debe a que la **primera** y la **última** son reservadas para la **subred** como ente y para **difusión**, respectivamente). Por tanto, todas las direcciones entre la 200.27.4.0 y la 200.27.4.255 pertenecerán a la misma subred que 200.27.4.112.

### 1.3 Direcciones privadas

Son un conjunto de direcciones en Internet de carácter reservado. Las IP privadas sólo tienen sentido en el interior de una red corporativa; si se quiere conectar ésta a Internet se requerirá de, al menos, una dirección IP pública en su router de acceso, a través del cual se realizan las comunicaciones de los hosts en el interior de la red con Internet.

Mediante extensiones se posibilita la conexión a Internet de muchos más dispositivos que la limitación impuesta por el uso de 24 bits en las direcciones. A la par, se reduce el problema del encaminamiento, puesto que una única dirección IP de destino (la del router de acceso) permite llegar a todos los ordenadores de la red corporativa (no está exenta de problemas).



### 1.4 Encaminamiento

El encaminamiento es llevar la información (paquetes/datagramas) de un origen a un destino en una red conmutada. Por sí mismo es el *routing* (decisión de rutas). Es la tarea fundamental en toda la interconexión de red.

Cada encaminador supone un cambio de subred. Las subredes se interconectan utilizando routers. El router de acceso (R2) posibilita la conexión de todos los dispositivos de la red con Internet. Las direcciones IP no se asocian a un dispositivo, sino a la interfaz del dispositivo con la red.

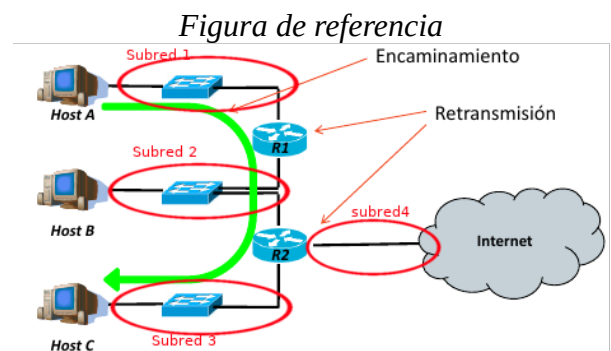
Utilizando un **conmutador** para cada subred se obtienen ventajas como son la capacidad plug-and-play (conexión sin configuración) de los conmutadores y mayor funcionalidad y eficiencia de éstos en comparación con los concentradores. Los **encaminadores** suponen un cambio de subred, mientras que los conmutadores, no.

En la figura de referencia, las subredes 1 y 3 tienen dos dispositivos cada uno: un host y un router. La subred 2 tiene tres: un host y dos routers. La subred 4 conecta dos dispositivos (routers); esta última no prevé crecer, mientras que el resto pueden hacerlo al añadir hosts adicionales.

Hay que distinguir dos operaciones relacionadas con el encaminamiento en Internet: el diseño del encaminamiento y su aplicación: la retransmisión (forwarding). Los algoritmos de encaminamiento buscan los caminos más o menos óptimos para su uso posterior en el envío de información.

### 1.5 Retransmisión

La retransmisión es la operación básica por la cual los dispositivos envían paquetes por alguna de sus interfaces de salida (utilizando tablas de encaminamiento). El encaminamiento más usado en Internet se basa en una resolución iterativa salto a salto (**resolución local** del camino en el dispositivo origen y todos los intermedios).



El host A quiere enviar un paquete al host C. El encaminamiento empieza en el mismo host A, que ha de determinar que para llegar a C tiene que enviar el paquete al router R1. Una vez hecho eso, la responsabilidad del host A en el encaminamiento del paquete desaparece. Una vez el paquete llega al router R1, éste tiene que determinar a dónde retransmitirlo considerando que el destino final es el host C. R1 decidirá que el siguiente nodo en el camino debe ser R2, y de nuevo habrá terminado su papel. Una vez llegue el paquete a R2, éste se lo hará llegar a C.

La solución salto a salto del encaminamiento está fundamentada en reducir al máximo el tamaño de las tablas de encaminamiento, de cara a reducir el retardo del procesamiento en las comunicaciones. De este modo las **tablas de encaminamiento** especifican tres elementos fundamentales para la retransmisión: dirección IP de subred destino, máscara asociada y siguiente nodo a donde enviar la información.

El procedimiento de retransmisión de un paquete se basa en dos pasos que se repiten iterativamente para cada fila de la tabla:

1. Aplicar la operación AND entre la dirección de destino del paquete y la máscara definida en la fila.
2. Comprobar si la dirección resultante coincide con la de destino en la misma fila. Si coincide, enviar al siguiente nodo correspondiente.

Si se cumple en más de una fila se elige la opción más restrictiva (con menos 0s en la máscara).

## 1.6 Fragmentación

Se produce siempre que un datagrama va a saltar de un segmento de red a otro en el que no cabe. Todos los segmentos de red tienen un MTU, que varía según la tecnología usada. La fragmentación de los datagramas IP se controla a través de los campos indicadores, desplazamiento e identificación.

El esquema basado en el *offset* (desplazamiento) es mucho más flexible, en el cual un puntero indica la posición relativa del primer byte del fragmento dentro del datagrama original. Lógicamente, todos los fragmentos especificarán en el campo de identificación el mismo valor de datagrama (el original). En ensamblado de los fragmentos se realizará en el destino.

El campo de indicadores del paquete IP está relacionado con la función de fragmentación, y será de interés el campo MF (*More Fragments*). El proceso IP de destino necesita saber cuándo finaliza el proceso de ensamblado, y para ello pueden darse dos situaciones:

1. Que haya huecos entre fragmentos (faltan por llegar).
2. Que los fragmentos estén ordenados (no se sabe si faltan por llegar). En este caso se consulta el flag MF, que estará a 0 cuando llegue el último fragmento.

## 2. Conmutación

La conmutación no es exactamente igual a la redirección. Los esquemas típicos son circuitos (red telefónica) y paquetes (Internet). El esquema de paquetes usa datagramas, aunque a veces en capa de enlace se usan circuitos virtuales. Existen dos esquemas de conmutación:

- **Conmutación de circuitos:** se establece la conexión previamente a la transmisión. Los recursos son dedicados, es decir, la línea queda reservada durante toda la llamada (en el ejemplo del teléfono), que usa una porción de cable (fibra óptica). La transmisión de información es muy rápida y no tiene *delay* (ventaja), pero se ocupa la red (desventaja). Siempre se dan tres pasos: conexión → transmisión (secuencial) → desconexión.
- **Conmutación de paquetes:** el envío se realiza en bloques denominados **paquetes** sin reserva previa de recursos, lo cual genera *delay* al almacenar los paquetes en una cola de salida. Varios circuitos pueden ocupar la misma parte del camino, por tanto los recursos no están dedicados.

- Conmutación mediante datagramas: no hay conexión origen-destino y el envío es independiente, de forma que pueden seguir caminos distintos y llegar desordenados. (ej.: IP)
- Conmutación de paquetes con circuitos virtuales: Los pasos a seguir son: conexión → transmisión → desconexión. A diferencia de la conmutación de circuitos, los recursos no son dedicados. (ej.: ATM - *Asynchronous Transfer Mode* (troncales))

### 3. Asociación con capa de enlace: protocolo ARP

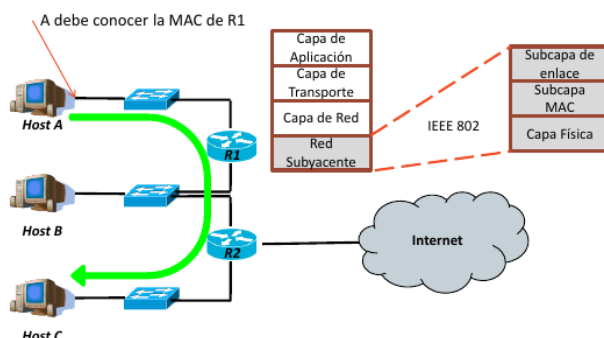
Las distintas capas copan diferentes funcionalidades que utilizan las capas de arriba. Para la capa IP, cómo se retransmite la información es algo abstracto. Tras la redirección IP, se envía a la MAC del siguiente nodo. Se usa en redes Ethernet y WiFi.

Formato: HH-HH-HH-HH-HH-HH. Son únicas, asignadas por IEEE en lotes de  $2^{24}$ .

Dirección de difusión (broadcast): FF-FF-FF-FF-FF-FF

Asumiendo que la conexión entre el Host A y el Host C es Ethernet:

Ether	IP	TCP	HTTP
MAC Or	IP Or	Puerto Or	-----
MAC D	IP D	Puerto D	-----



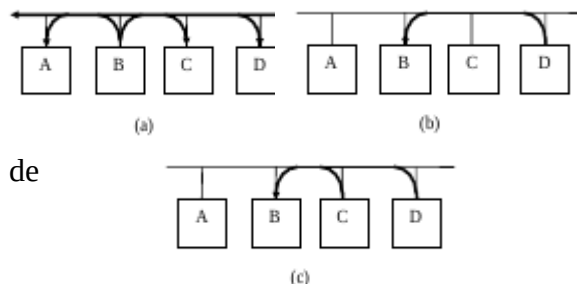
(A) → R1	R1 → R2	R2 → (C)
MAC Or → MAC A	MAC Or → MAC R1	MAC Or → MAC R2
MAC D → MAC R1	MAC D → MAC R2	MAC D → MAC C
IP Or → IP A	IP Or → IP A	IP Or → IP A
IP D → IP C	IP D → IP C	IP D → IP C
PTO Or → 40000	PTO Or → 40000	PTO Or → 40000
PTO D → 80	PTO D → 80	PTO D → 80

Con las tablas NAT es distinto porque cambia.

Protocolo ARP: obtener MAC a partir de IP. <sup>(a) y (b)</sup>

Normalmente existe una caché ARP que va añadiendo entradas para no tener que volver a preguntar. Es un protocolo de interacción-red.

Protocolo RARP: IP a partir de MAC. <sup>(a) y (c)</sup>



### 4. El protocolo ICMP

El protocolo de mensajes de control en Internet (*Internet Control Message Protocol*) es un protocolo muy básico de gestión de red. Es, al igual que IP, un protocolo de la capa de red, siendo complementario a éste. Además ICMP es usuario de IP, es decir, los mensajes ICMP se encapsulan dentro de los paquetes IP. Informa sobre situaciones de error (señalización). Va hacia el origen del datagrama IP. Su cabecera es de 32 bits: tipo (8b), código (8b) y comprobación (16b). Dispone de checksum.

0	8	16
tipo	código	comprobación