Tema-2FR.pdf

mhm01

Fundamentos de Redes

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación
Universidad de Granada

TEMA 2: CAPA DE RED

1. Funcionalidades

---------- Funciones y Servicios en TCP/IP

El objetivo de la capa de red en Internet es la interconexión de redes, con independencia de la tecnología subyacente. En el modelo OSI el control de congestión se realiza en esta capa.

La conmutación es la acción de cursar trafico entre los nodos de la red.

El encaminamiento (routing) consiste en encontrar la mejor ruta desde un origen a un destino.

----- Funciones del Protocolo TCP

En el **emisor**:
- divide la información en paquetes
- agrega un código detector de errores para comprobar si el paquete llega correctamente a su destinos
- pasa el paquete al protocolo IP para que gestione su envío.

En el **receptor**:
- recibir los paquetes que pasa el protocolo IP
- ordena los paquetes, y comprueba que están todos que son correctos
- extrae la información útil de los paquetes
- si detecta un paquete que no ha llegado o que es incorrecto, genera un paquete para ser enviado al emisor, indicándole que lo ha de enviar de nuevo.

2. Conmutación

La conmutación es el proceso donde se pone en comunicación un host con otro, a través de una infraestructura de comunicaciones común, para la transferencia de información. Se necesita establecer un sistema de comunicación entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de equipos/nodos de transmisión.

La conmutación para conectar redes entre sí funciona en la Capa 3 del modelo OSI (capa de red). Los servicios fundamentales que emplean técnicas de conmutación son: el servicio telefónico, el servicio telegráfico y el servicio de datos.

Las tecnologías de conmutación pueden ser de circuitos o de paquetes (datagramas o circuitos virtuales)

---------- Conmutación de Circuitos

Consiste en el mantenimiento de un circuito físico previo al envío de información, que se mantiene abierto durante todo el tiempo que dura la transmisión. El camino físico se elige entre los disponibles, empleando diversas técnicas de señalización: “por canal asociado” si viaja en el mismo canal o “por canal común” si lo hace por otro distinto, encargadas de establecer, mantener y liberar dicho circuito.

Los pasos para la conmutación de circuitos es :

1) Conexiones
2) Transmisión
3) Desconesxión

- **Establecimiento del circuito:** el host emisor solicita a un cierto nodo de conmutación el establecimiento de conexión hacia un host receptor. Este nodo es el encargado de dedicar uno de sus canales lógicos al emisor. También será el encargado de encontrar los nodos intermedios para llegar al receptor, teniendo en cuenta ciertos criterios de encaminamiento, coste, etc.

- **Transferencia de datos:** una vez establecido el circuito exclusivo para esta transmisión, se transmite desde el emisor hasta el receptor conmutando sin demoras de nodo en nodo (los nodos tienen reservado un canal lógico para ello) .

- **Desconexión del circuito:** Terminada la transferencia, el emisor o el receptor indican a su nodo de conmutación más inmediato que ha finalizado la conexión. Este nodo informa al siguiente de este hecho y luego libera el canal dedicado, así hasta liberar el canal dedicado completo en el otro extremo.

----- Ventajas e Inconvenientes de la Conmutación de Circuitos

- Ventajas:

  - Recursos dedicados (circuito en exclusiva).
  - Facilita las comunicaciones en tiempo-real (voz y vídeo).
  - No hay colisiones, es decir, no hay contienda por acceder al medio.
  - No hay contención. El medio está disponible completamente por lo que se transmite a la máxima velocidad posible.
  - No hay encaminamiento una vez establecido el circuito por lo que hay una transmisión más rápida.
  - Simplicidad de gestión en nodos. Se recibe siempre por la misma entrada y se transmite siempre por la misma salida.

- Inconvenientes:

  - Retraso para el establecimiento de la conexión. Hay que resolver toda la ruta.
  - Bloqueo y posible infrautilización de recursos. La línea está reservada aunque no se aproveche.
  - Poca flexibilidad para adaptarse a cambios. No se reajusta la ruta si surgen posibles rutas alternativas mejores.
  - Poco tolerante a fallos por lo que si falla un nodo del camino, se cae todo el circuito.

---------- Conmutación de Circuitos

Para este tipo de conmutación no es necesario establecer una conexión previa.
Un paquete consta de dos partes: los datos útiles y la información de control que es la que nos sirve para determinar la ruta a seguir a lo largo de la red hasta el destino. Los paquetes permanecen muy poco tiempo en memoria, por lo que resulta muy rápida. La conmutación de paquetes admite dos variantes distintas, según el modo de funcionamiento: el datagrama y los circuitos virtuales.

KEEP CALM AND ESTUDIA UN POQUITO

WUOLAH + #QuédateEnCasa

----- Procedimiento

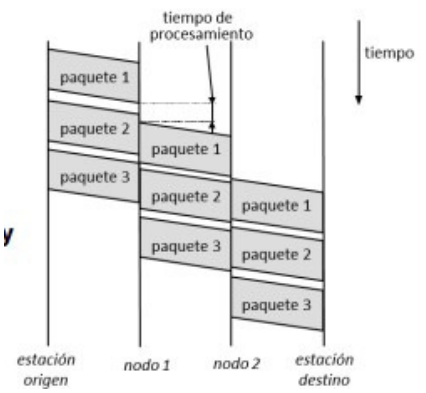
Cuando un host quiere enviar información a otro lo divide en paquetes. Se lo pasará a un nodo intermedio que será el encargado de transmitirlo al siguiente hacia el destino. Cada nodo intermedio realiza las siguientes funciones:

- **Almacenamiento y retransmisión** (store and forward): el paquete se detiene (se almacena) el tiempo necesario para procesarlo.
- **Control de Ruta** (routing): selección de un nodo del camino por el que deben retransmitirse los paquete para hacerlos llegar a su destino.

Los paquetes toman diversos caminos pero nadie puede garantizar que todos los paquetes vayan a llegar en un momento determinado ni en un orden.

----- Conmutación de Datagramas

En este tipo de conmutación no hay conexión. El envío se realiza en unidades de datos (paquetes) independientes. En cada salto se realiza un almacenamiento y un re-envío. Cada paquete debe contener las direcciones origen y destino. Los paquetes pueden seguir rutas diferentes y pueden llegar desordenados.



----- Conmutación con Circuitos Virtuales

Esta orientado a conexión. Antes de la transmisión se establece una ruta entre el origen y el destino (puede ser diferente en cada sentido). Se envían unidades de datos (paquetes) independientes. No se acaparan los recursos, se comparten. En cada salto, hay un almacenamiento y re-envío. Pata ello, se debe comprobar antes si los recursos están libres. Los paquetes llegaran ordenados.

----- Ventajas e Inconvenientes de Circuitos Virtuales frente a Datagramas

- Ventajas:
  - El encaminamiento en cada nodo sólo se hace una vez para todo el grupo de paquetes. Por lo que los paquetes llegan antes a su destino.
  - Todos los paquetes llegan en el mismo orden del de partida ya que siguen el mismo camino.
  - En cada nodo se realiza detección de errores, por lo que si un paquete llega erróneo a un nodo, este lo solicita otra vez al nodo anterior antes de seguir transmitiendo los siguientes.

- Desventajas:

    - Los datagramas son mas flexibles por lo que si hay congestión en la red, una vez que ya ha partido algún paquete, los siguientes pueden tomar caminos diferentes. En circuitos virtuales, esto no se hace.
    - En datagramas no hay que establecer la conexión. Para pocos paquetes es mas rápida la conmutación en datagramas.
    - El envío mediante datagramas es mas fiable. Si un nodo falla, se perderá solo un paquete. En circuitos virtuales se perderán todos si no hay algún mecanismo de recalculo de la ruta.

3. El Protocolo IP

---------- Introducción a IP

----- IPv4

Esta especificado en el RFC 791. Es un protocolo para la interconexión de redes también llamadas subredes. Resuelve el encaminamiento en Internet encontrando la ruta para llegar al destino. Es un protocolo de salto a salto. Involucra hosts y routers. Ofrece un servicio no orientado a conexión y no fiable. No hay una negociación o "handshake" ya que no hay una conexión lógica entre las entidades. No existe control de errores, ni control de flujo ni control de congestión.

La unidad de datos (paquete) de IP se denomina datagrama. IP es un protocolo de máximo esfuerzo ("best-effort") o buena voluntad: los datagramas se pueden perder, duplicar, retrasar o llegar desordenados. IP gestiona la fragmentación adaptando el tamaño del datagrama a las diferentes Maximum Transfer Units (MTUs) de las subredes hasta llegar al destino.

Cada entidad en Internet se identifica por su dirección IP.

---------- Direcciones IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica a una interfaz de un sistema dentro de una red que utilice el protocolo IP. Internet adopta un direccionamiento jerárquico que simplifica las tablas de routing.

Las direcciones IPv4 tienen 32 bits, agrupados en bloques de 8 bits cada uno. Se representan mediante una dotación decimal (entre 0 y 255) separada por puntos. Por ejemplo: 200.110.23.77.

Cada dirección IP tiene dos partes bien diferenciadas: un identificador de la subred o prefijo (parte izquierda de la IP) y un identificador del dispositivo dentro de esa subred (parte derecha de la IP). Cada subred tiene un identificador (o prefijo) único en la intranet (red privada). Cada dispositivo (interfaz) tiene un identificador único en la subred.

La máscara de red es un patrón de '1s' que determina que bits de la IP completa corresponden al identificador de subred.
Ejemplo:

- Dirección IP: 200.27.4.112 → 11001000.00011011.00000100.01110000
- Máscara: 255.255.255.0 → 11111111.11111111.11111111.00000000

La máscara se puede representar de forma compacta, indicando el número de '1s' que tiene.
Ejemplo:

255.255.255.0 → 11111111.11111111.11111111.00000000 → /24

La dirección anterior con la máscara sería: 200.27.4.112/24

Dada una IP, para obtener la dirección o identificador de la subred, se realiza una operación lógica "&" (AND) con la máscara de red. Ejemplo:

200.27.4.112 → 11001000.00011011.00000100.01110000

& &

255.255.255.0 → 11111111.11111111.11111111.00000000

Subred ➔ 200.27.4.0 11001000.00011011.00000100.00000000

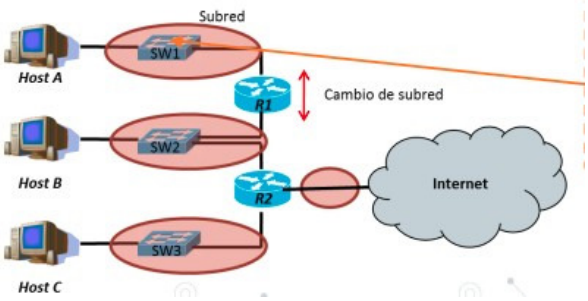
---------- **Subredes**

Podemos considerar Internet como un conjunto de subredes interconectadas.

Una subred son unas líneas de transmisión e infraestructura de red que permite que la conexión directa de dispositivos IP sin intermediarios.

Un switch o conmutador se usa para crear redes de computadoras. Son "transparentes" y trabaja a nivel de enlace (capa 2 de OSI).

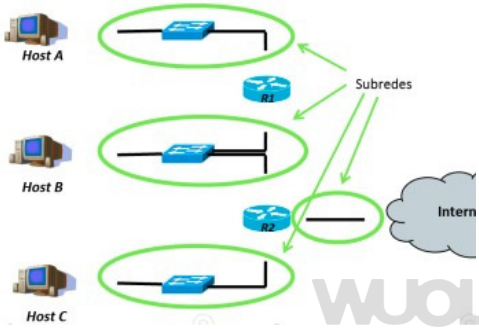
Un router o encaminador se usa para conectar redes entre si. Es un punto de separación, ya que limita el trafico entre las redes. Redirige los paquetes hacia el destino de una transmisión. Trabaja a nivel de red (capa 3 de OSI).



---------- **Subnetting**

----- **Como determinar las subredes en un esquema de red**

Para determinar las subredes, separe cada interfaz de los hosts y routers, creando redes aisladas. Dichas redes aisladas se corresponden con las subredes.
Tendrán dirección IP cada una de las interfaces de los hosts y de los routers. Los switches no tiene dirección IP.



----- Como se elige la máscara

Según el número de dispositivos que necesitemos direccionar en la subred, tal que se ajusta para no desaprovechar direcciones. Ejemplo:

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

- Número de dispositivos = $2^{número\_ceros}$ - 2
Ej: 8 ceros (/24) permite 254 dispositivos
El -2 viene de que la primera IP y última son reservadas

Cada subred tiene un identificador único en nuestra intrared.

La dirección de red/subred tiene todo a 0s en la parte de host. La dirección de difusión/broadcast tiene todo 1s en la parte del host.

- 200.27.4.0 = 11001000.00011011.00000100.00000000 ➔ Reservada (subred)
- 200.27.4.1 = 11001000.00011011.00000100.00000001 ➔ Dispositivo #1 …
- 200.27.4.254 = 11001000.00011011.00000100.11111110 ➔ Dispositivo #254
- 200.27.4.255 = 11001000.00011011.00000100.11111111 ➔ Reservada (difusión)

---------- Tipos de Direcciones IP

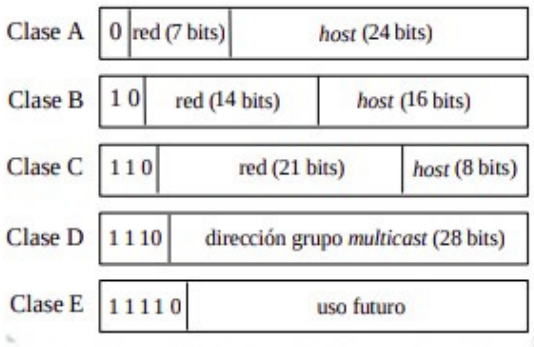
- **Publicas**: cada dirección se asigna a sólo un dispositivo (una interfaz) en toda la Internet global. Se asignan centralizadamente.

- **Privadas**: sólo sirven para tráfico dentro de las intranets. Se pueden repetir en distintas intranets. Las asigna el usuario según su criterio. Rangos de las IPs privadas:
10.0.0.0/8 ➔ de 10.0.0.0 a 10.255.255.255
172.16.0.0/16 ➔ de 172.16.0.0 a 172.31.255.255
192.168.0.0/24 ➔ de 192.168.0.0 a 192.168.255.255

---------- Clases y Rangos de Direcciones IP

----- Clases:

Especificadas en RFCs 1166 y 5737. Originariamente se definieron 5 clases de direcciones IP, clases A, B, C, D, E. Las tres primeras clases (A,B,C) son jerárquicas a dos niveles: el identificador de red y el identificador de dispositivo (host).



----- **Rangos:**

- Según su clase:

```
A → 0.0.0.0   - 127.255.255.255 ⇒         128 redes x 16.777.216 hosts
B → 128.0.0.0 - 191.255.255.255 ⇒      16.384 redes x     65.536 hosts
C → 192.0.0.0 - 223.255.255.255 ⇒   2.097.152 redes x        256 hosts
D → 224.0.0.0 - 239.255.255.255 ⇒   para multicast
E → 240.0.0.0 - 255.255.255.255 ⇒   usos futuros
```

- Reglas especiales:
  - host = 00…0 → identifica a una red, nunca es una dirección origen, no se usa para dispositivos
  - host = 11…1 → difusión en la red especificada, es una dirección destino, no se usa para dispositivos
  - 127.0.0.0 → autobucle (loopback)

- Reserva de direcciones privadas (RFC 1918):

```
A → 10.0.0.0 → 1 Red privada de Clase A
B → 172.16.0.0 - 172.31.0.0 → 16 redes privadas de Clase B
C → 192.168.0.0 - 192.168.255.0 → 256 redes privadas de Clase C
```

---------- **Agotamiento de IPs**

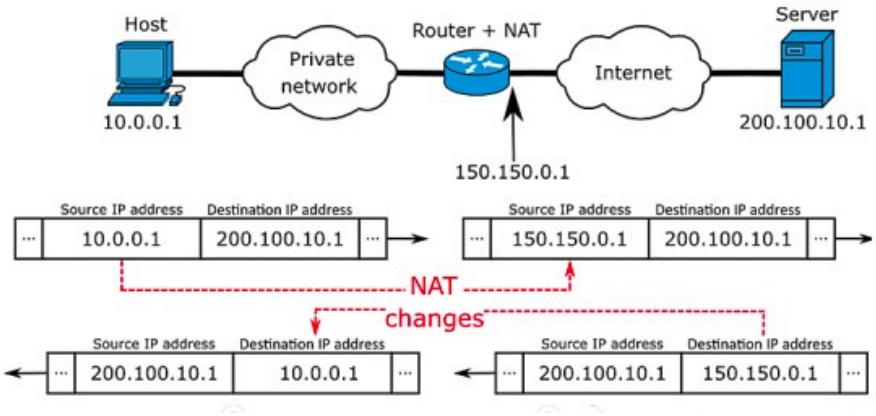
Los bloques de direcciones IPv4 se "agotaron en Noviembre de 2019. Sólo quedan disponibles bloques de /24 (256 direcciones) a /32 (1 dirección). Se van recopilando direcciones de sitios obsoletos, empresas que hayan desaparecido, proyectos terminados, hosting que ya no está en uso…

----- **IPv6**

Usa un esquema de direccionamiento de 128 bits. Hace uso de la notación decimal. (grupos de 4 dígitos, separados por ":" . Cada código hexadecimal corresponde a 4 dígitos en binario (4 bits). El rango va de 0000:0000:0000:0000:0000:0000:0000:0000 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Por lo que tenemos 340 sextillones de direcciones diferentes. Son compatibles con IPv4.

---------- **NAT (Network Address Translation)**

Consiste en traducir un conjunto de direcciones IPv4 en otras. Permite que una red con direccionamiento privado se pueda conectar a Internet (direccionamiento público). Cambia la dirección IP privada por una dirección publica al reenviar un paquete hacia el exterior de la red (hacia Internet). Cambia la dirección IP publica por la correspondiente privada al reenviar un paquete hacia el interior. Utiliza una tabla de traducciones, que contiene direcciones IP y puertos. Los puertos se asocian a los equipos de la red privada (para dirigir el trafico entrante).



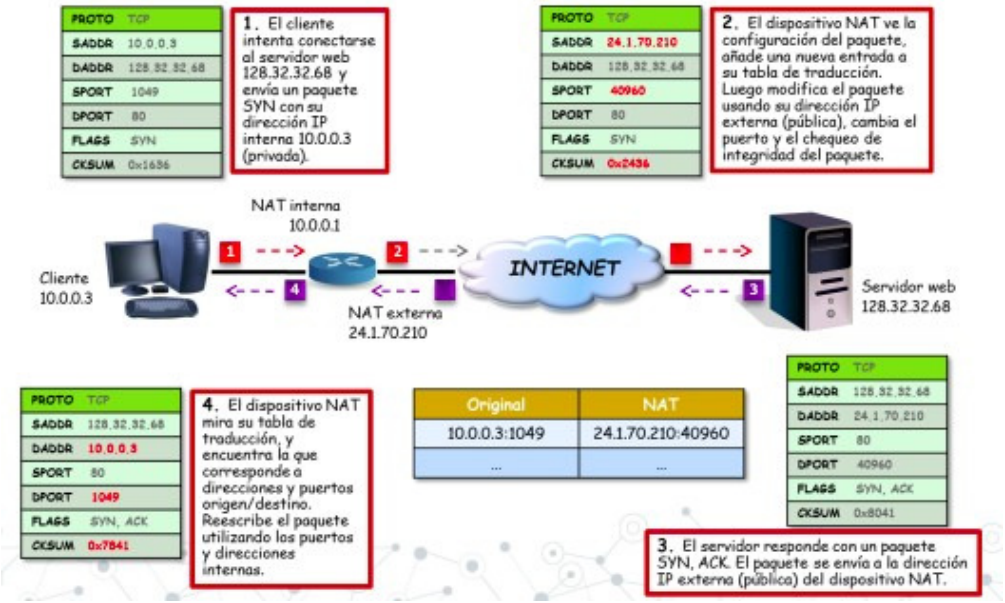
----- Problema de la Escasez de Direcciones IP

Se necesitan m direcciones pero se dispone de n, siendo n<m. Si n=1, se denomina enmascaramiento. Se usa ISPs, para así poder dar acceso a mas usuarios que direcciones IP tenga el ISP. Se supone que no todos los usuarios acceden simultáneamente. Las direcciones se asignan a los usuarios de forma dinámica.

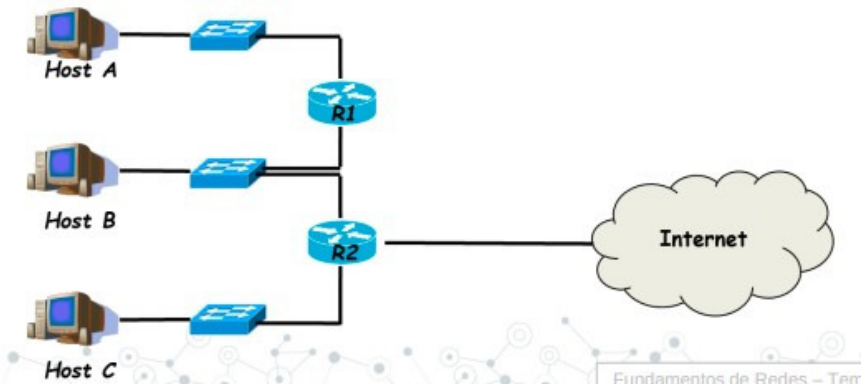
----- Tipos de NAT

- **SNAT (Source NAT):** el origen de los datos está en la red privada. Cambia la dirección IP de origen.

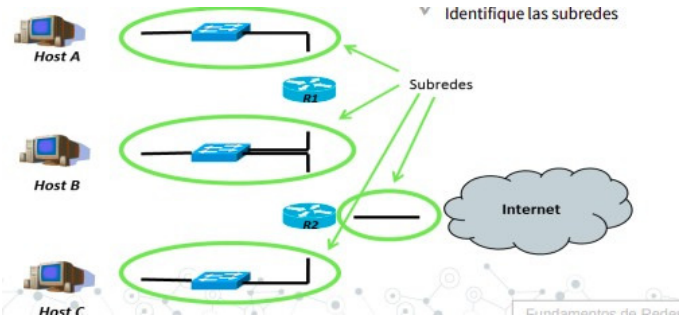
- **DNAT (Destination NAT):** el origen de los datos está en la red pública. Cambia la dirección Ip de destino. Requiere configurar en el router qué puerto irá dirigido a qué máquina.



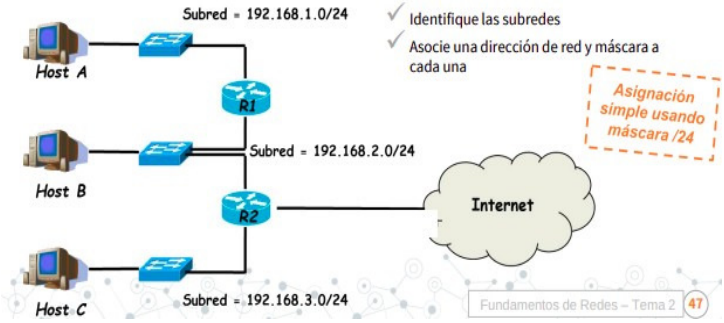
---------- Ejercicio: Asignación de Direcciones IP



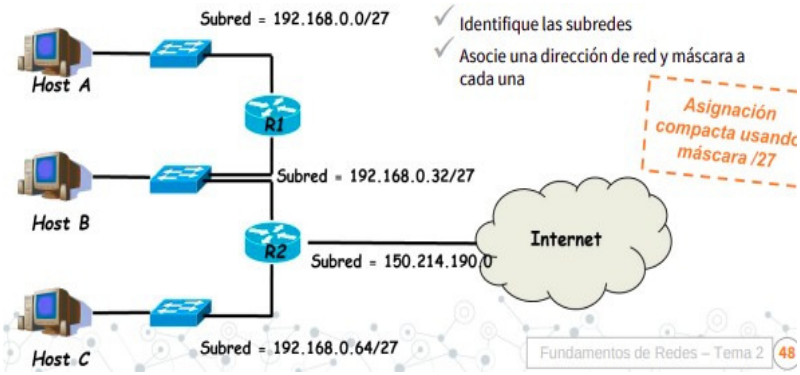
1. Identificar las subredes.



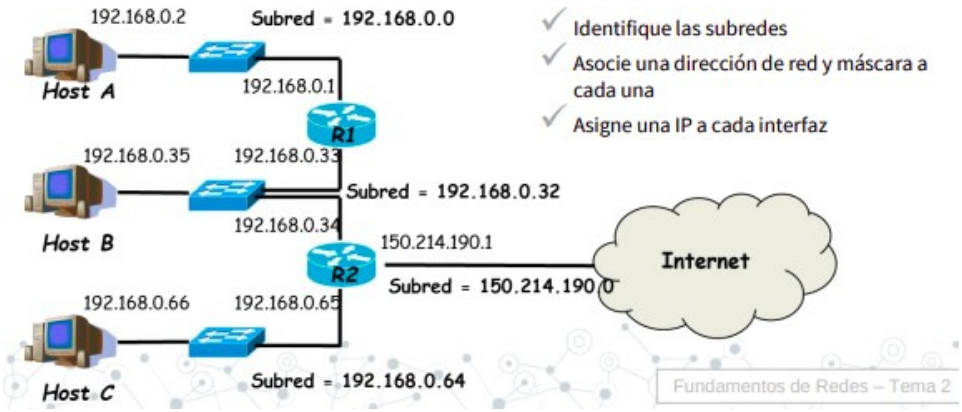
2. Asociar una dirección de red y máscara a cada una.



Para direccionar 30 dispositivos: 5 bits en la parte del hosts. 32-5=27 bits para red. Por lo que la máscara será /27.
La dirección pública ISP: 2 bits, /30, consideramos por ejemplo 150.214.190.0



3. Asignar una IP a cada interfaz.



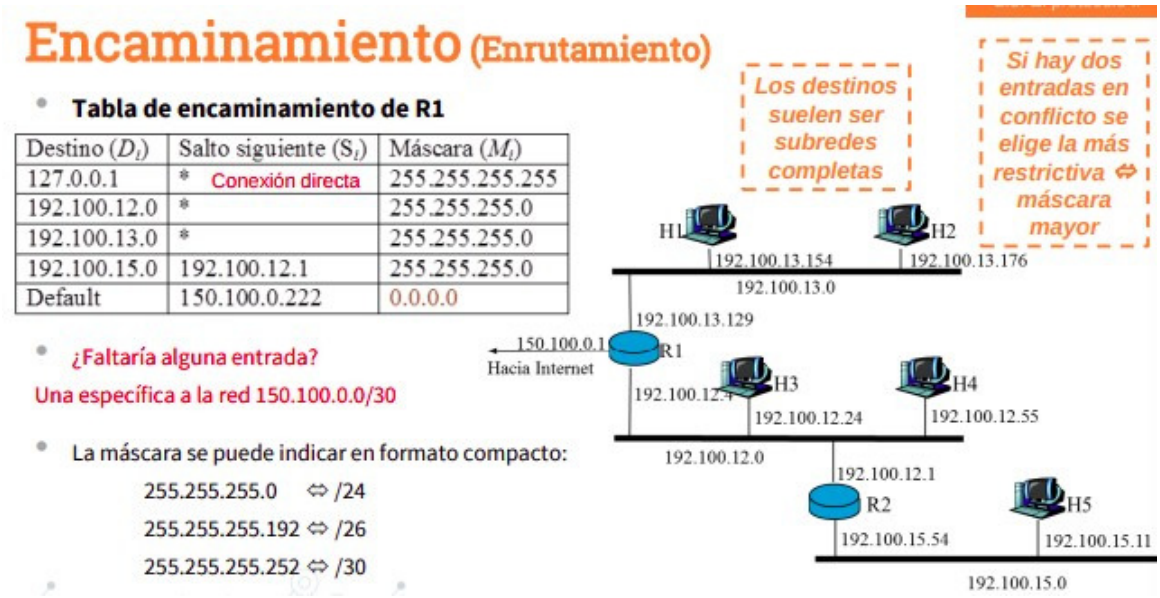
---------- Encaminamiento (Enrutamiento)

El encaminamiento consiste en encontrar el mejor camino para llevar la información (paquete) de un origen a un destino dado. Se realiza paquete a paquete y salto a salto, en función de la IP destino del paquete y de las Tablas de Encaminamiento residentes en cada una de las entidades IP (host origen y destino). En cada salto (router) se hace un almacenamiento y una retransmisión.

El encaminamiento se realiza salto a salto y datagrama a datagrama. Los modos de encaminamiento son:

- Directo: lo resuelve el propio router.
- No Directo: lo resuelve el router siguiente en la ruta.

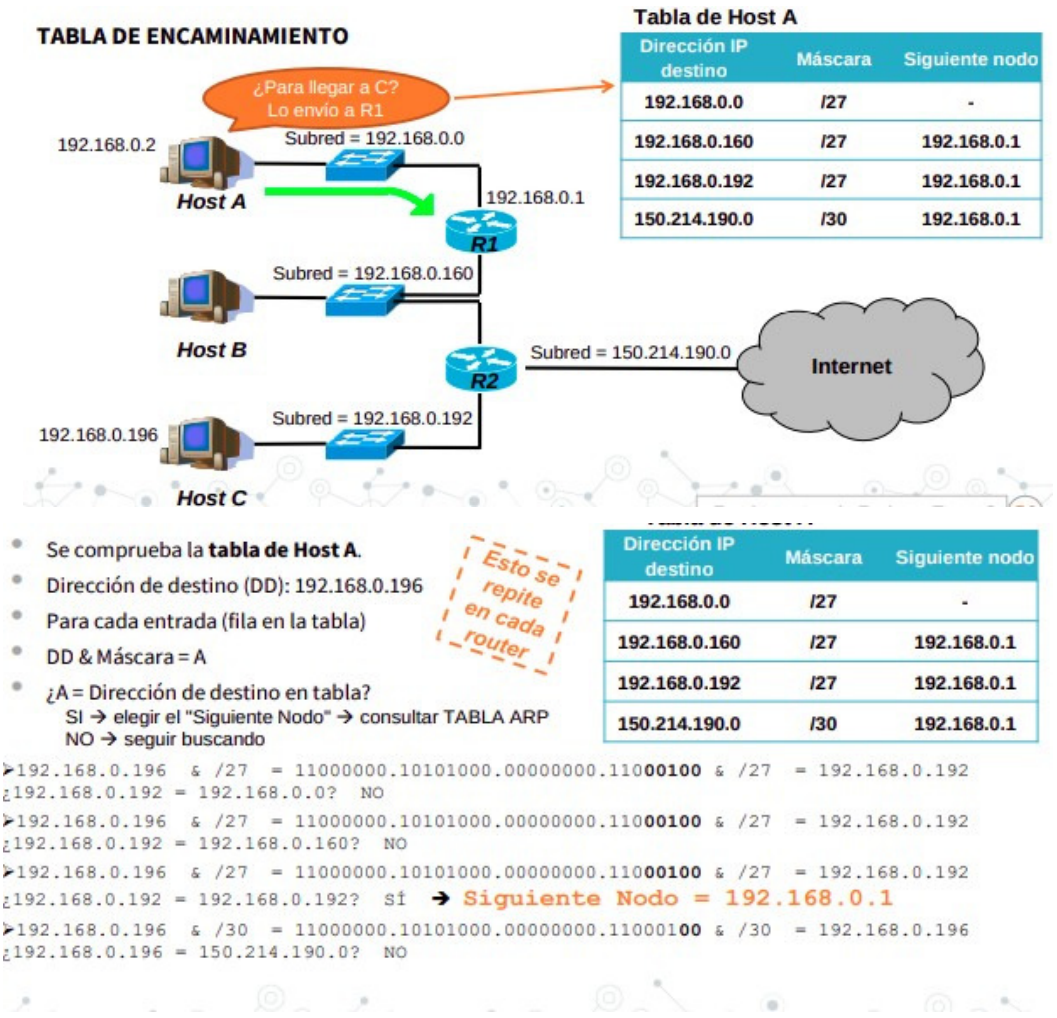
Cada dispositivo tiene una Tabla de Encaminamiento o de Enroutamiento. Un router suele estar en varias redes distintas, un host suele estar en solo una.



----- Proceso de Encaminamiento (en cada nodo y para cada datagrama)

1. Se extrae la dirección destino: IP_DESTINO del datagrama.
2. Por cada entrada i=1….N de la tabla de encaminamiento se calcula:
Ipii = IP_DESTINO AND(&) MASCARA_i
3. Si Ipi = Di y si:
- es routing directo: reenviar el datagrama al destino final por la interfaz i.
- es routing no directo: reenviar el datagrama al salto siguiente por la interfaz i.
4. Si hay varias coincidencias se elige el destino con la máscara más larga (con más 1s).
5. Si se ha barrido toda la tabla y no hay coincidencia con ninguna fila, entonces hay un error.

----- Ejemplo



Podemos agrupar entradas de la tabla que tengan distinto destino, pero el mismo salto siguiente.

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
192.168.0.160	/27	192.168.0.1
192.168.0.192	/27	192.168.0.1
192.168.190.0	/30	192.168.0.1

Buscamos los bits en común (iguales):
192.168.0.160 → 11000000.10101000.00000000.10100000
192.168.0.192 → 11000000.10101000.00000000.11000000

La máscara del agrupamiento indicará el número de bits iguales → /25.
La dirección agrupada será la parte común y el resto de bits estarán a 0:
11000000.10101000.00000000.10000000. Por lo tanto la entrada quedaría como 192.168.0.128/25.

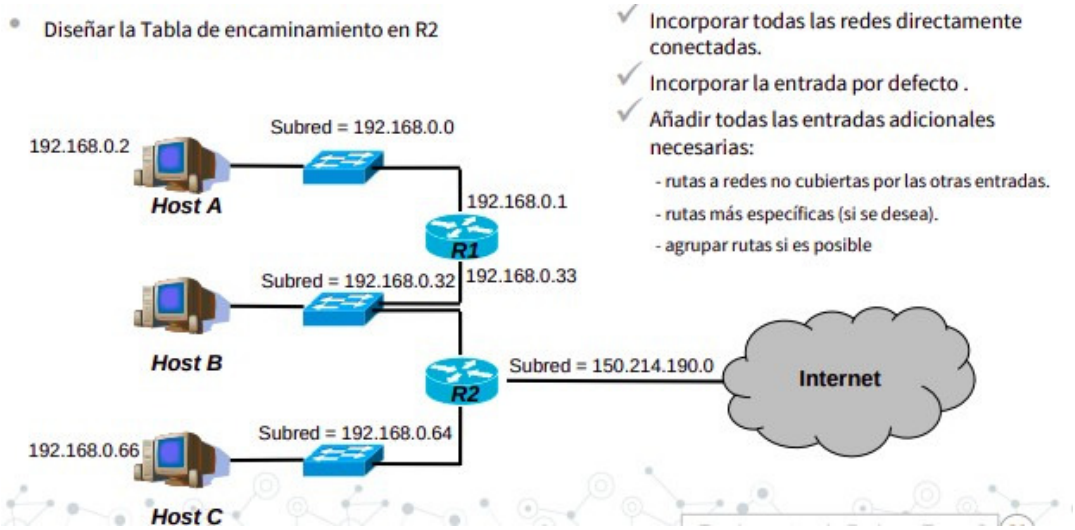
No merece la pena agrupar direcciones muy diferentes, porque la entrada agrupada será muy genérica.

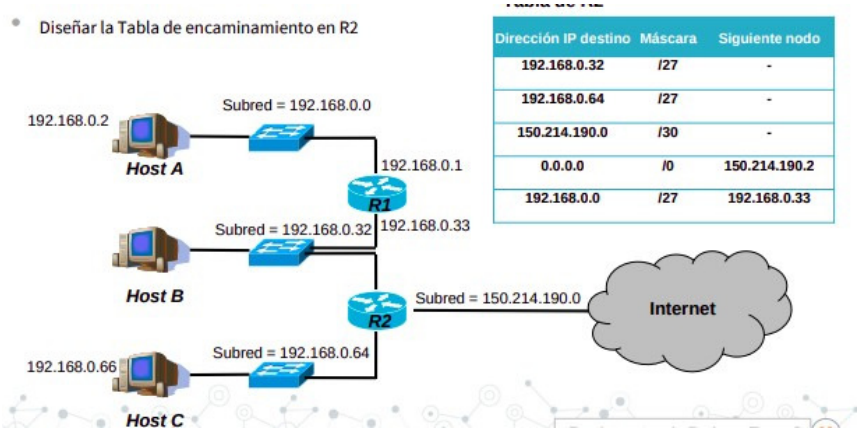
Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
192.168.0.128	/25	192.168.0.1
192.168.190.0	/30	192.168.0.1

La entrada por defecto (/0) se suele añadir para dirigir el tráfico hacia fuera de la red (hacia Internet). Aunque en este ejemplo se puede usar para dirigir el tráfico a las demás subredes también.

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	/27	-
0.0.0.0	0.0.0.0	192.168.0.1

----- Ejercicio





Dirección IP destino	Máscara	Siguiente nodo
192.168.0.32	/27	-
192.168.0.64	/27	-
150.214.190.0	/30	-
0.0.0.0	/0	150.214.190.2
192.168.0.0	/27	192.168.0.33

---------- **Sistemas Autónomos**

Para facilitar la administración y aumentar la escalabilidad Internet se jerarquiza en Sistemas Autónomos (SA). Un SA es un conjunto de redes y routers administrados por una autoridad. Cada SA informa a los otros SA de las redes accesibles. Existe un router responsable de esto, denominado router exterior (o router frontera). Cada SA se identifica por un entero de 16 bits aunque desde 2007 es de 32 bits.

----- **Intercambio de Tablas**

Internet se jerarquiza en Sistemas Autónomos. Existe encaminamiento dinámico mediante algoritmos automáticos. Se definen 2 niveles de encaminamiento (intercambio de tablas):
- Algoritmo IGP: los que se usan dentro de un SA (el administrador tiene liberta de elección): RIP, OSPF, HELLO…
- Algoritmo EGP: los que se usan entre SAS (norma única en Internet): BGP.

---------- **Algoritmos de Encaminamiento**

----- **Vector Distancia**

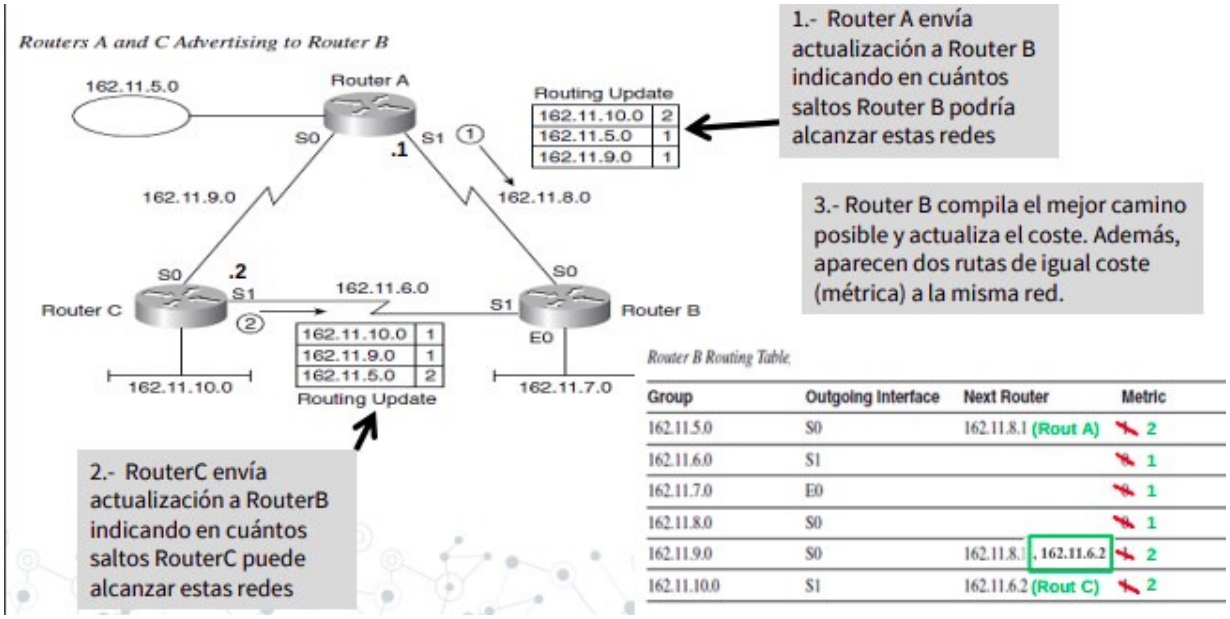
Los routers construyen su tabla de rutas con el único conocimiento de la distancia (métrica) y el siguiente salto (next hop) para llegar a la red de destino. Esta distancia puede ser un número que indica: longitud del enlace, número de saltos, latencia (tiempo medio) u otros valores. Requiere intercambiar información periódicamente con los routers vecinos para recalcular la distancia. Cada router envía su tabla de encaminamiento a los demás. Ejemplo: RIP.

----- **Estado del Enlace**

Los router necesitan conocer previamente toda la topología de la red (conexiones existentes entre los nodos) para calcular el camino al destino y generar su tabla de enrutamiento. Ejemplo: OSPF.

----- **RIP (Routing Information Protocol)**

Protocolo de la capa de aplicación que opera sobre UDP puerto 520. Adopta un algoritmo vector-distancia (métrica basada en número de saltos). No considera la congestión de la red ni la velocidad de los enlaces. Una red directamente conectada a un router tiene coste 1. Hay un máximo de 15 saltos, 16 sería considerada distancia infinita o no alcanzable. Periódicamente (por defecto cada 30 segundos) cada router RIP recibe de todos sus vecinos y envía a todos sus vecinos (dirección multicast 224.0.0.9) los vectores-distancia para todos los posibles destinos. De entre ellos, para un destino dado, se selecciona como salto siguiente el vecino que anuncie el menor coste, actualizando la métrica para ese destino sumando uno al coste anunciado (coste para alcanzar ese vecino desde el router actual).

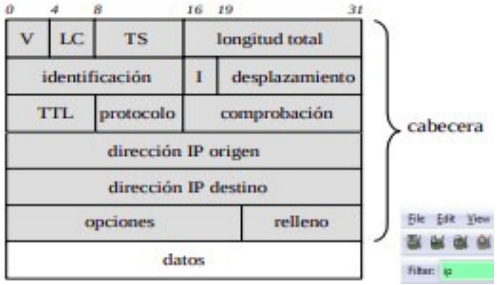


----- OSPF (Open Shortest Path First)

Está basado en el estado del enlace. Se publican los estado por difusión/inundación. El coste por defecto que se considera en OSPF para cada enlace es: coste 10^8/BW. Ejemplo: para un enlace con BW = 1 Mbps → coste= 10^8 /10^6 = 100. El coste de los enlaces se podrá determinar en tiempo real por un administrador o un algoritmo automático. Permite calcular rutas alternativas y hacer balanceo de carga. Se pueden considerar distintas métricas. Así se conseguirá dar prioridad a unos enlaces sobre otros mediante el balanceo de carga.

Al conocer toda la red, las rutas se calculan usando un algoritmo de Dijkstra. A partir de las rutas se construyen la tablas de encaminamiento de cada router. La gestión se realiza en base a áreas independientes de la red. Se minimiza la difusión mediante routers designados (son los que envían y reciben el estado de la red). Hay una mayor convergencia, ya que no hay que hacer cálculos sobre las rutas a difundir. Las actualizaciones se hacen sólo cuando hay cambios en la red. Maneja distintas tablas (BD): vecinos, topología, rutas. Los mensajes que usa son: *hello, database description, link status request/update/ack.*

---------- Formato del Datagrama IP



- **Versión:** 0100 → 4
- **Tamaño Cabecera:** en palabras de 32 bits (entre 5 y 15) → entre 20 y 60 bytes
- **Tipo de Servicio**: preferencia de envío (mínimo retardo, máximo rendimiento, mínimo coste)
- **Longitud Total**: tamaño en bytes del datagrama completo (incluyendo datos).

- **Identificador:** número de orden del paquete en un mensaje.
- **Flags:** indican si hay fragmentación.
- **Posición de Fragmento:** desplazamiento del fragmento respecto del paquete original para reconstruirlo.

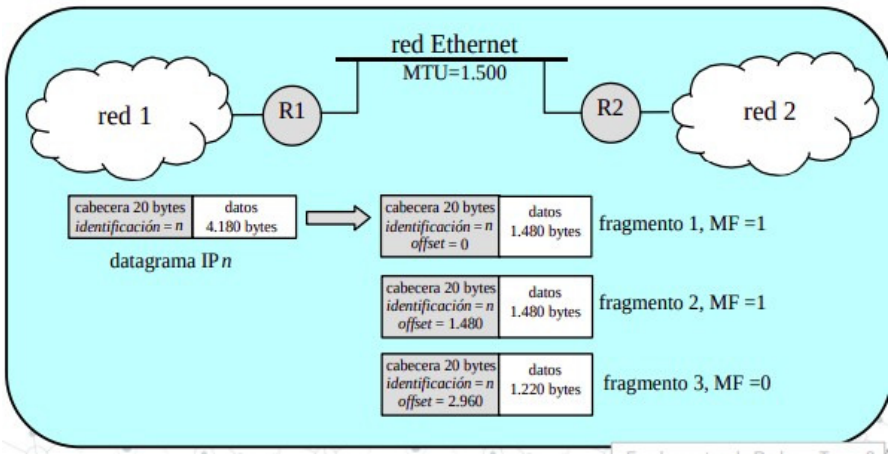
- **Tiempo de Vida (TTL):** tiempo que puede estar el paquete en una red.
- **Protocolo:** TCP, UDP, ICMP, etc
- **Suma de Control de Cabecera:** número para comprobar la corrección de la cabecera.

- **Opciones:** Hasta 40 bytes. Puede hacer funciones de test y depuración sobre la red (sello de tiempo, registro de ruta, etc):
- **Relleno:** Bits a 0 para completar una palabra de 32 bits en la cabecera.

---------- Fragmentación IP

- **Tamaño máximo datagrama** (incluyendo datos): 2^{16}-1 = 65.535 bytes
- Adaptarse a la MTU (Maximum Transfer Unit).
- Ensamblado en destino final:
    - **desplazamiento**: offset respecto del comienzo del paquete.
    - **indicadores** (I): “Don´t Fragment”, “More Fragments”

Nivel de enlace	MTU (bytes)
PPP normal	1500
PPP bajo retardo	296
X.25	1600 (RFC 1356)
Frame Relay	1600 (normalmente)
Ethernet DIX	1500
Ethernet LLC-SNAP	1492
Token Ring 4 Mb/s	4440 (THT 8ms)
Classical IP over ATM	9180



4. Asociación con la Capa de Enlace: El Protocolo ARP

---------- Direcciones MAC

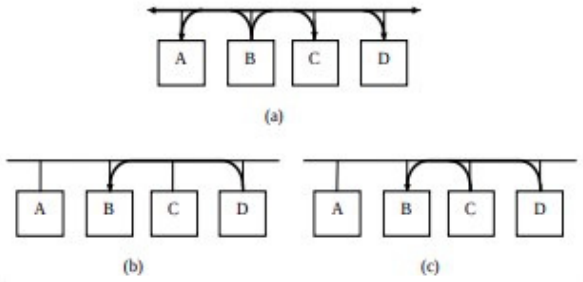
Para transmisiones a nivel de enlace (físicas). Tras la redirección IP, enviar a la MAC del siguiente nodo.

---------- ARP

Tras la redirección IP, enviar a la dirección MAC (Medium Access Control) del siguiente nodo. Se usan en redes Ethernet (cableadas) y Wifi. El formato que utiliza es de 6 bytes hexadecimal: HH-HH-HH-HH-HH-HH. Ejemplo: 00-24-21-A8-F7-6A. Son únicas, asignadas por IEEE en lotes de 2^{24} para cada fabricante. La dirección de difusión (broadcast) FF-FF-FF-FF-FF-FF.

- ARP (Address Resolution Protocol) : Obtener MAC a partir de IP: B pregunta MAC de D [(a) y (b)]

- RARP: reverse ARP. Obtener IP a partir de MAC: (a) y (c).



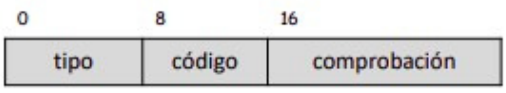
----- Formato ARP

0	8	16	31
Htipo		Ptipo	
Hlen	Plen	Operación	
Hemisor (bytes 0-3)			
Hemisor (bytes 4-5)		Pemisor (bytes 0-1)	
Pemisor (bytes 2-3)		Hsol (bytes 0-1)	
Hsol (bytes 2-5)			
Psol (bytes 0-3)			

5. El Protocolo ICMP

Internet Control Message Protocol. Informa sobre situaciones de error en IP por lo que es un protocolo de señalización. Suelen ir (excepto eco y solicitudes) hacia el origen del datagrama IP original. ICMP se encapsula en IP. Tiene una cabecera de 32 bits donde:

- Tipo (8 bits): tipo de mensaje
- Código (8 bits): subtipo de mensaje
- Comprobación (16 bits)



Mensaje ICMP

Campo *tipo*	Mensaje ICMP
8/0	Solicitud/respuesta de eco (ping)
3	Destino inalcanzable
4	Ralentización del origen
5	Redireccionamiento
11	Tiempo de vida excedido
12	Problema de parámetros
13/14	Solicitud/respuesta de sello de tiempo
17/18	Solicitud/respuesta de máscara de red

6. Autoconfiguración de Red: El Protocolo DHCP

Para asignar las direcciones se usa DHCP, protocolo del usuario UDP (puerto 67). La asignación de IPs se realiza de forma dinámica en una red privada.

- El host (cliente) envía un mensaje broadcast. *DHCP discover.*
- El server DHCP responde con un mensaje *DHCP offer.*
- El host solicita una dirección IP, mensaje *DHCP request.*
- El server DHCP envía la dirección IP: mensaje *DHCP ack.*