# TEMA 6
# INTERCONEXIÓN DE REDES (REDES IP). INTERNET

## 6.1. INTERCONEXIÓN DE REDES.

- Términos
  - Internet: colección de redes interconectadas.
  - Intranet: internet corporativa privada que utiliza los servicios de internet.
  - Bridge o puente: interconexión de redes LAN con el mismo protocolo de enlace (OSI) o de acceso a red (TCP/IP), en general MAC-LLC. Ejemplo Tocken-Ring <-> Ethernet. El puente no modifica los paquetes.

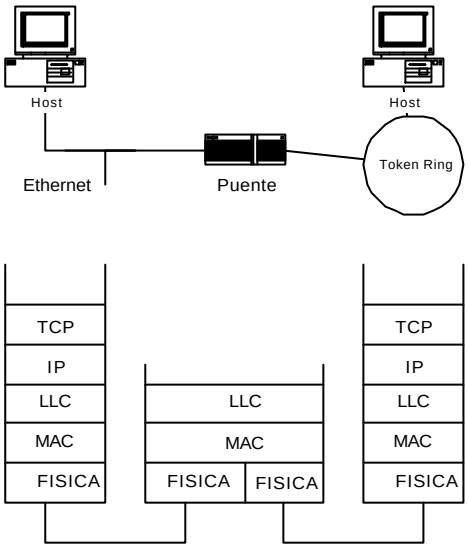



*Fig. 6.1*

  - Router: dispositivo de encaminamiento. Interconecta dos redes que pueden o no ser similares. El *router* puede almacenar e interpretar información sobre redes y encaminamiento en la red, y enviar paquetes a redes que no están directamente conectadas entre sí.
  - Gateways: termino genérico para dispositivo hardware o software que comunica entre sí redes con distintos protocolos.
  - Switches o conmutadores: dispositivos que reciben mensajes de distintos nodos de la red y los encaminan hacia su destino correcto. Ejemplo es el de la red telefónica convencional, pero son de uso común en redes de comunicación privadas.
  - Hub o distribuidor: dispositivo que distribuye los mensajes recibidos por los demás nodos o parte de ellos conectados a él.

- Generalidades:
  - La interconexión de redes como una red.
  - La interconexión de redes requiere varias cuestiones a tener en cuenta dada la diversidad de parámetros existentes como:
    - Esquemas de direccionamiento
    - Tamaños máximos de paquetes
    - Valores de temporizadores
    - Mecanismos de acceso

- Esto ha llevado a la fabricación de diferentes dispositivos para cada tipo de red, que resuelven parte de las diferencias, además de diferentes implementaciones de software desde las capas de firmware a las de aplicación.
- Tipo de servicio entre redes:
  - Servicio orientado a conexión. Circuitos Virtuales. Paquetes siempre a través del mismo camino y en el mismo orden.
  - Servicio sin conexión: datagramas (PDU's) en red de conmutación de paquetes. Cada paquete se trata individualmente y lleva información sobre direccionamiento. Las redes IP funcionan sobre servicios sin conexión.

- Ejemplo de esquema de interconexión de redes

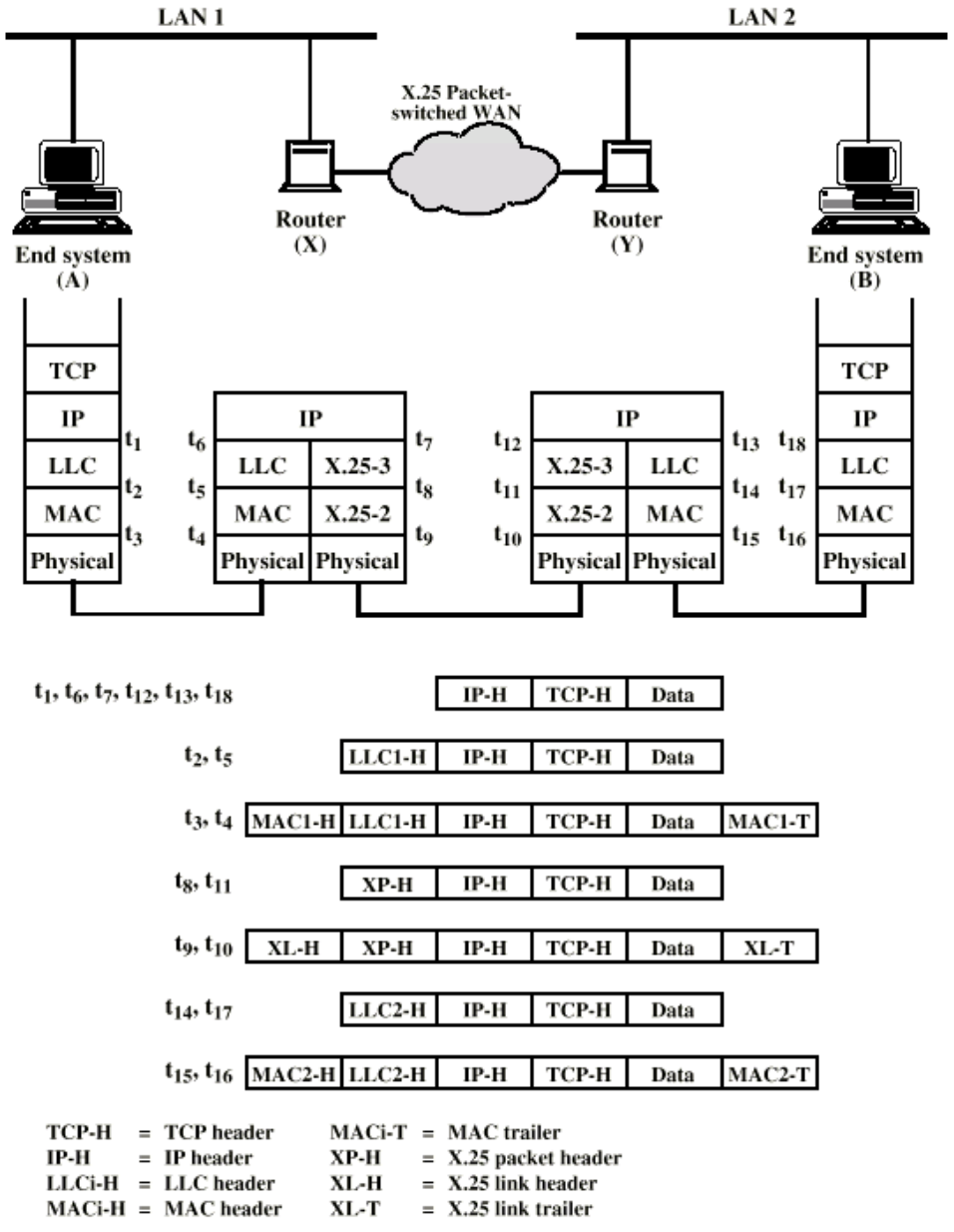



*Fig. 6.2*

- Cuestiones de diseño:
  - Encaminamiento: tabla en cada dispositivo de encaminamiento (router) que da para un destino dado el siguiente router al que se deberá enviar el datagrama de internet.
  - Tiempo de vida de los datagramas: para limitar los efectos de los paquetes perdidos. Se suele medir en nº de saltos.
  - Segmentación y ensamblado
  - Control de errores
  - Control de flujo

## 6.2. PROTOCOLO IP

Forma parte de la arquitectura TCP/IP. Es el protocolo de interconexión de redes mas utilizado. Otros protocolos como IPX cada vez en mas desuso.

Proporciona al protocolo TCP primitivas y parámetros.

- Primitivas
  - Send
  - Deliver
- Parámetros
  - Direcciones
  - Indicadores: tipo de servicio
  - Datos
  - Otros

### 6.2.1. Formato paquete IP.

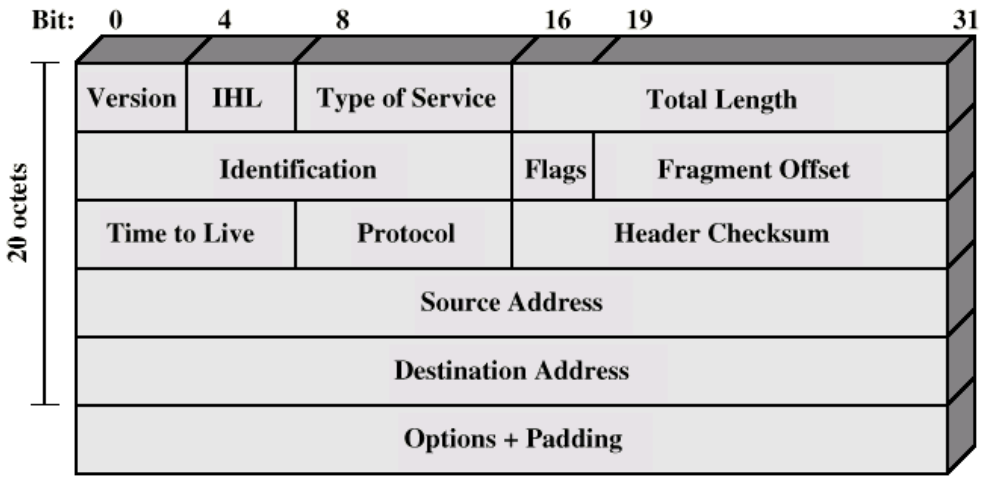



*Fig. 6.3*

Descripción:

- Versión (4 bits): Nº de versión del protocolo IP. Actualmente en la 4, y definiendo la 6.
- IHL, Longitud de cabecera de Internet (4 bits) expresada en bloques de 32 bits.
- Tipo de servicio (8 bits): parámetros de seguridad, prioridad, retardo y rendimiento.
- Longitud total (16 bits): longitud total del datagrama en octetos.
- Identificador (16 bits): nº de secuencia que identifica una “conexión” junto con los campos dirección origen, destino y protocolo.
- Indicadores (3 bits): 3 bits, fragmentación (1 no fragmentar), segmentación (bit Mas). El tercero no se usa.

- Desplazamiento del fragmento (13 bits): posición de los datos dentro del datagrama completo antes de ser fragmentado. Se mide en bloques de 64 bits (8 octetos).
- TTL, tiempo de vida (8 bits): nº de saltos que puede permanecer un paquete en una red. Cada router hace disminuir el contador en 1.
- Protocolo: protocolo de un usuario de IP (ICMP, TCP, UDP)
- Suma de comprobación de la cabecera (16 bits): control de error mediante análisis de la cabecera. (complemento a 1 de las palabras de 16 bits de la cabecera). Algunos campos cambian → se comprueba en cada salto.
- Dirección origen (32 bits): código de direccionamiento de 32 bits, dando un número de host (interfaz lógica IP) y/o un número de red.
- Dirección destino.
- Opciones (variable): contiene opciones del usuario a la red. Normalmente no se usa, salvo prioridades y QoS.
- Relleno: obliga a la cabecera del datagrama IP a tener un tamaño múltiplo de 32 bits (4 octetos).
- Datos: lleva información del protocolo y/o los datos del datagrama de la capa superior.

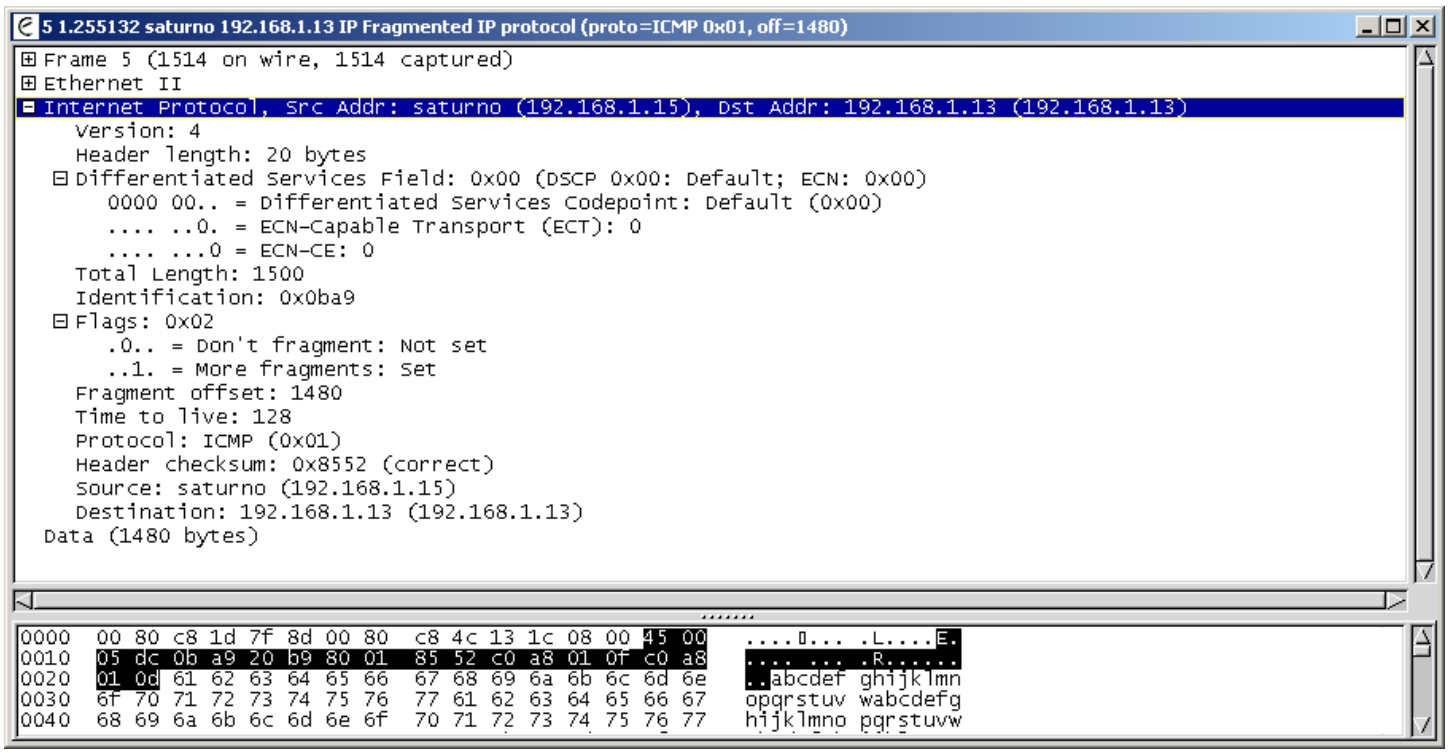



*Fig. 6.4 Captura de tramas ethernet de "ping – l 4095 192.168.1.13" (en Windows 2000)*

### 6.2.2. Direccionamiento, normas. Subneting, máscaras

- Direcciones IP: dirección de 32 bits única en la interred de trabajo (enmascaramiento). Consta de:
  - Número o identificador de red
  - Número o identificador de host
- Se representa en notación decimal con los octetos separados por puntos:
  - P.ejem. 172.16.122.204 es 10101100 00010000 01111010 11001100
- La asignación de estas direcciones es gestionada por la IANA (Internet Assigned Numbers Authority).

- La IP versión 4 es la utilizada hoy en día. La IEFT trabaja en la próxima generación de direcciones (próxima versión del protocolo), la IPv6. Esta última define direcciones de 128 bits en lugar de los 32 actuales; es compatible con la Ipv4 y cuando se implante, ambas coexistirán durante unos años.

6.2.2.1. Clases de direcciones IP

- Para facilitar la administración, las direcciones IP están divididas en clases:

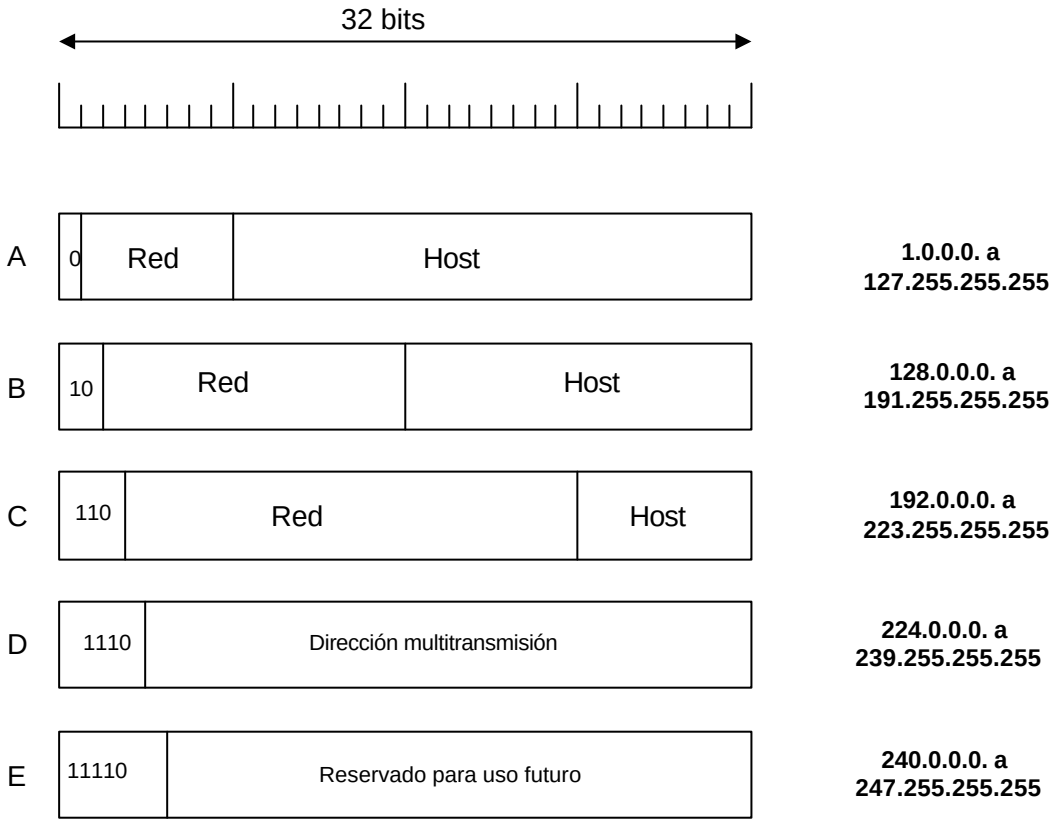



*Fig. 6.5*

  - Hay 126 Clases A, cada una con 16.777.214 direcciones de host ($2^{24}$ –2).
  - Hay 16.383 Clases B, cada una con 65.534 direcciones de host). ($2^{16}$ –2)
  - Hay 2.097.151 Clases C, cada una con 254 direcciones de host ($2^{8}$ –2)

- La falta de 2 hosts en cada clase, se debe a lo siguiente:
  - Un número de host todo ceros está reservado para identificar la red
  - Un número de host todo unos está reservado para un broadcast de red

- Se reserva la dirección 0.0.0.0 para un host desconocido y para cuando se arranca el protocolo.
- Se reserva la clase A 127.xxx.yyy.zzz para la loopback address, usada por un dispositivo para direccionarse a sí mismo (los paquetes enviados a estas direcciones salen a la red y se tratan como paquetes de entrada). Es útil para comprobar el funcionamiento de la capa IP y las que están por encima.

- Multicasting:

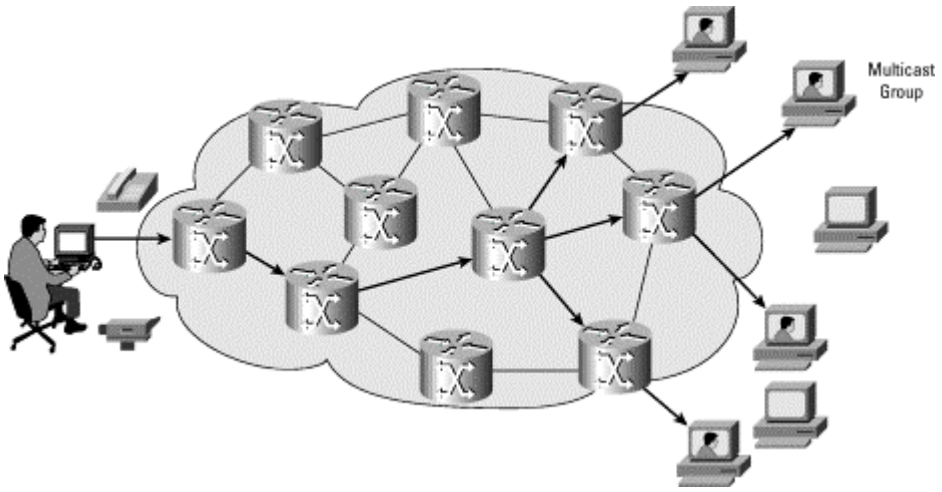



*Fig. 6.6*

  - Es la red clase D 224.0.0.0 → 239.255.255.255
  - Las direcciones 224.0.0.1 → 224.0.0.254 son de multicast en el segmento actual (LAN).
  - Las restantes son para funcionamiento a través de internet.
  - Cada grupo de multicast tiene la misma dirección IP de multicast.
  - Los routers tienen que tener soporte para protocolos multicast.

6.2.2.2. Direcciones privadas.

- La RFC 1597 ha reservado los siguientes bloques de direcciones para direcciones privadas de internet:

  - La clase A 10.0.0.0 a 10.255.255.255
  - Las 16 clases B 172.16.0.0 a 172.31.255.255
  - Las 256 clases C 192.168.0.0 a 192.168.255.255

- No necesitan darse de alta en el IANA
- Pueden existir varios hosts con la misma IP. Si existen dentro de la misma interred no pueden comunicarse entre sí y da lugar a conflictos de direccionamiento.

6.2.2.3. Configuración de direcciones IP

- El número de host de cualquier dispositivo o interfaz tiene que ser distinto de todos ceros y todos unos.
- El número de host todo ceros, identifica a todas las direcciones IP de una interred.
- Un router tiene varias interfaces de red. Su tabla de enrutado contiene información sobre que redes se pueden encontrar en cada una de sus interfaces.
- No es necesaria una asociación entre interface y dirección IP, por lo que pueden existir mas de una dirección IP para una sola interface.
- Los comandos típicos para configuración de interfaces a nivel IP son:

  - UNIX: *ifconfig, ip address, ip addr*
    - *Ifconfig eth0 192.168.1.100 netmask 255.255.255.0*
    - *Ip addr dev eth0 192.168.1.100/24*
  - IOS (Cisco): *ip address*
    *# interface ethernet 0*
    *# ip address 172.16.2.1 255.255.0.0*

6.2.2.4. Uso de Máscaras y subredes

- Si no se utilizan máscaras y subredes, se tiene una gran red con pobres prestaciones.

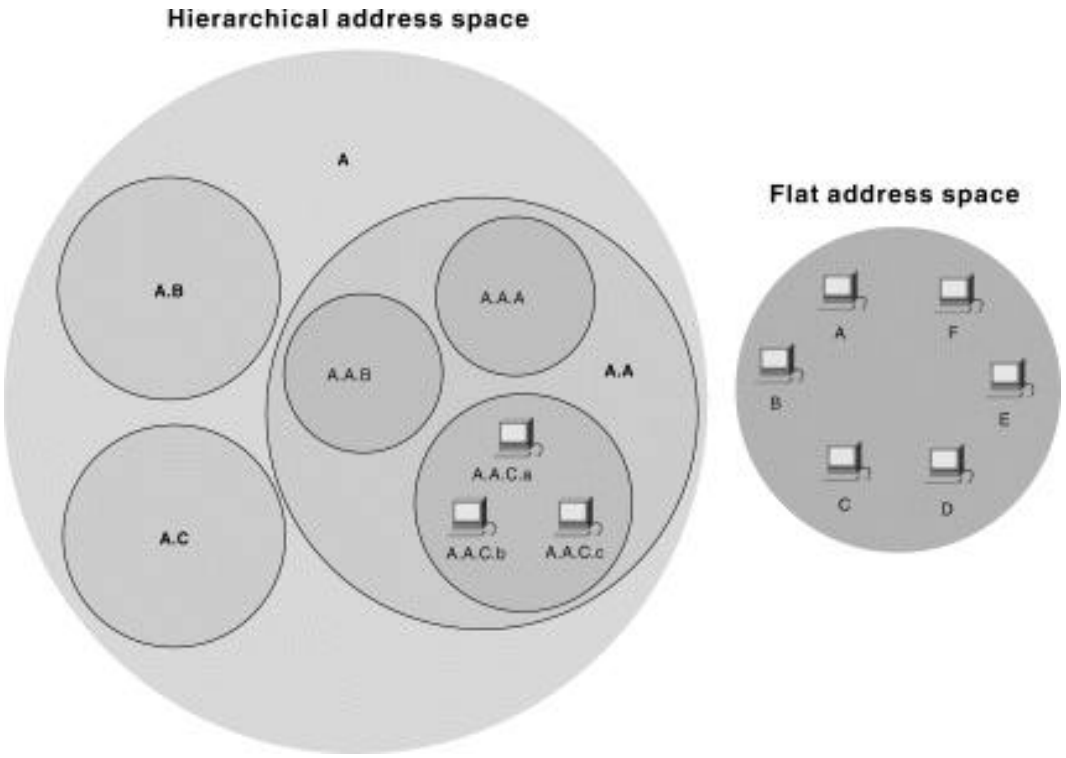



*Fig. 6.7*

- El uso de máscaras permite a un computador determinar si un datagrama de salida va destinado a otro computador en la misma LAN o a otra LAN.
- El mundo exterior (otras redes) sigue viendo la red como antes.
- Se puede dividir el número de host en dos campos
    - El primero indica una subred dentro de la red principal (clase A,B,C). Cada LAN tiene un número de subred.
    - El segundo indica un número de host dentro de la subred.

- De esa forma, una subred queda unívocamente determinada por su número de subred y su máscara.
- El número de subred se puede calcular con el número de un host cualquiera de la subred y la máscara de la subred.

- Uso de subredes:

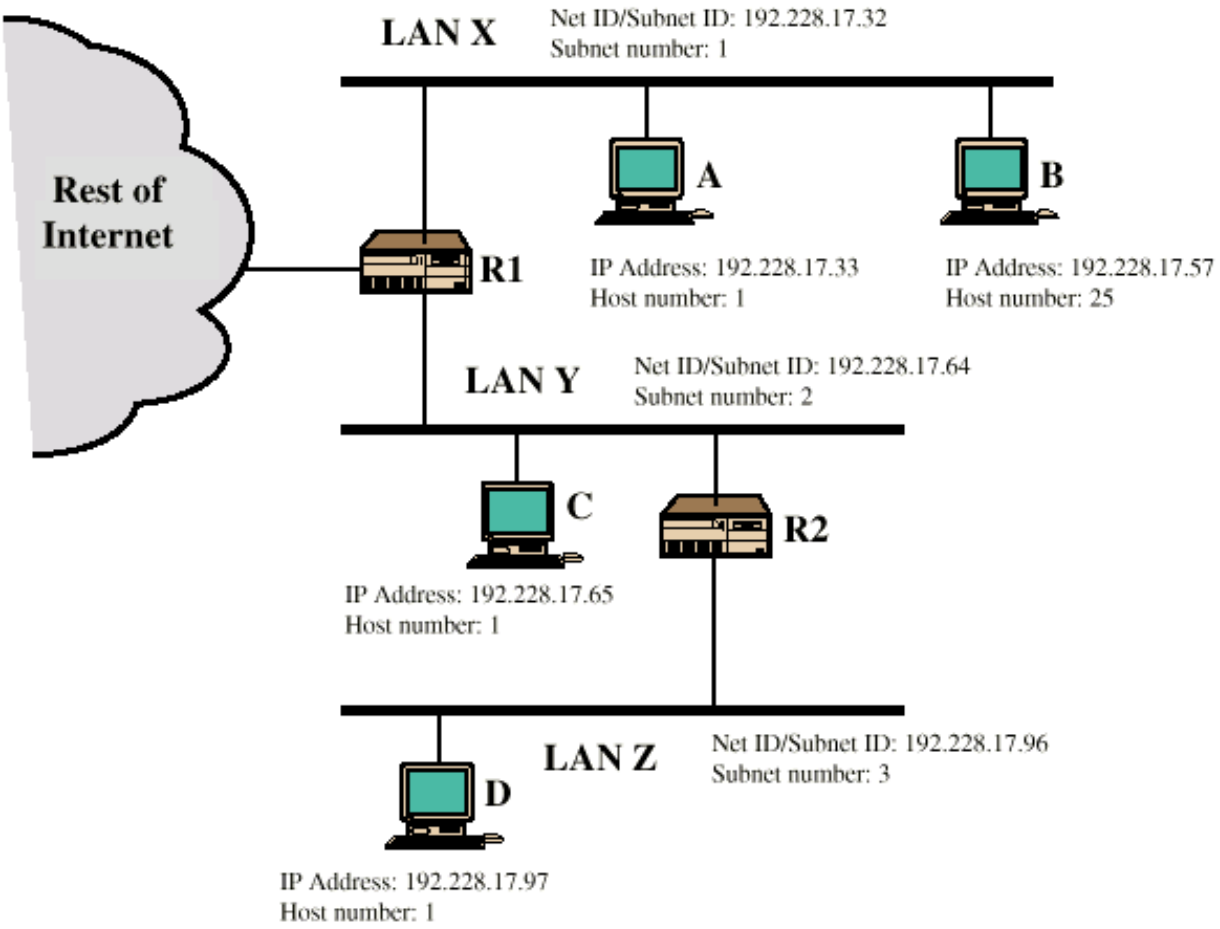



*Fig. 6.8*

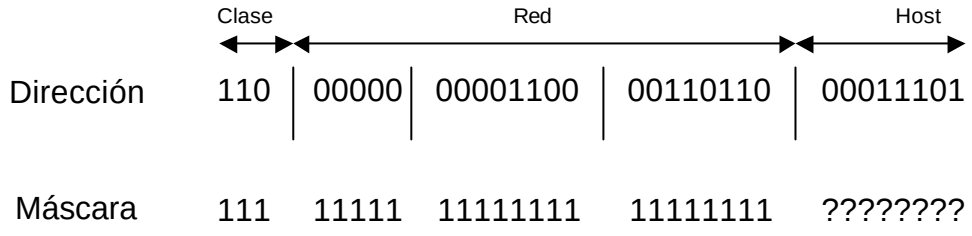
- La máscara de red indica qué parte de la dirección IP pertenece al número de subred, y qué parte de la dirección IP pertenece al número de host, es decir, la máscara separa los bits de host de los bits de red y subred.
- La máscara de subred es un conjunto de bits mas significativos que son todo 1's lógicos.

  - Tiene que haber al menos tantos 1's seguidos como bits hay en la cabecera de la clase de red y en la dirección de red de dicha clase; así, el valor de la máscara de subred de 32 bits será:

    - Unos para los bits de red y de clase de red
    - Unos para los bits de subred
    - Ceros para los bits de host

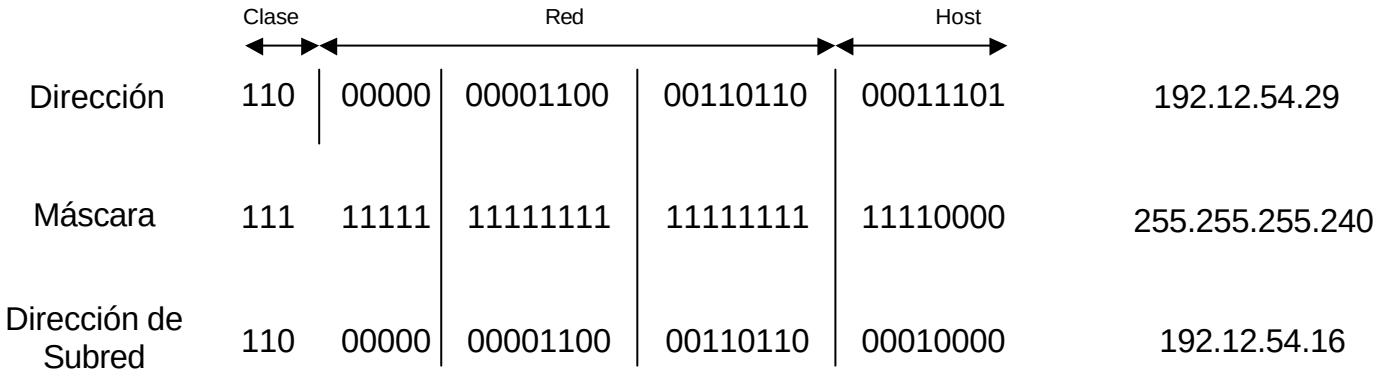
- P.ej.

Clase C: 192.12.54.29




o El cálculo de la dirección de subred se hace mediante un AND lógico binario entre la máscara de subred y la dirección IP del host.

- P.ej.




o La notación habitual indicando los decimales en grupos de 1 byte, pero se extiende por comodidad la notación CIDR, que consiste en dar directamente el número de 1's de la máscara.

- P.ej. 255.255.255.240 → CIDR /28

- Los routers determinan la red de destino, limitando el tráfico en los otros segmentos de la red.

o La esquematización de subredes siempre se refiere a subredes lógicas, puesto que puede haber varias subredes dentro del mismo segmento. Se puede definir subred como un dominio de broadcast de nivel 3 (IP).

o En la red de la figura 6.9:

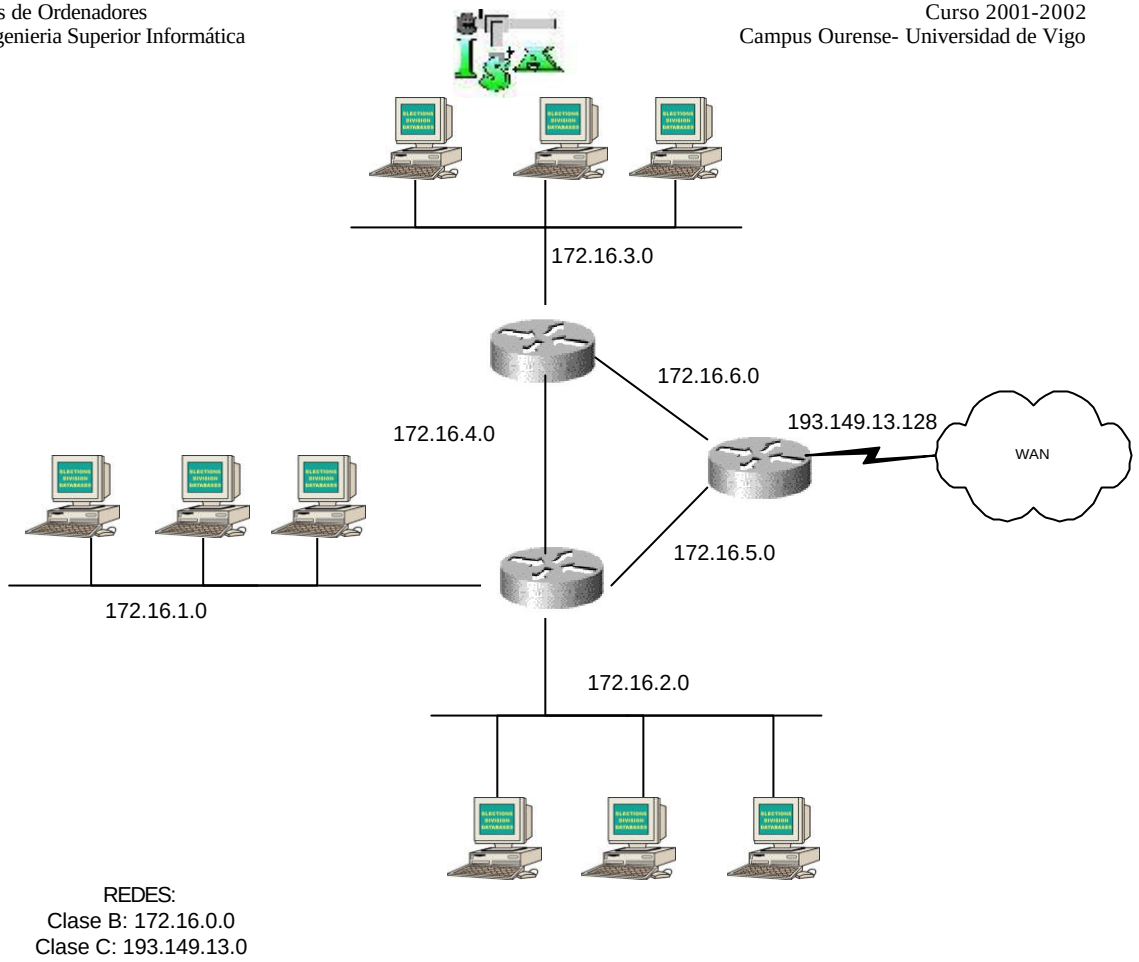



*Fig. 6.9*

- Si no se divide en subredes, la IP 172.16.2.160 tiene como máscara 255.255.0.0 (/16), es decir, su red es la clase B privada 172.16.0.0.
- Sin embargo, si en la red 172.16.0.0 se toman 8 bits para designar subredes, tendremos 254 subredes de 254 hosts. La máscara en este caso será 255.255.255.0 (/24) y la dirección de subred del host con la IP 172.16.2.160 será 172.16.2.0.

- Planificación de subredes
  - Si nuestra red tiene asignada la dirección clase C 201.222.5.0 y necesitamos 20 subredes con 5 hosts por subred, ¿cuáles son las subredes y los hosts por subred.
    - Las clase C admiten hasta 254 subredes de 1 host.
    - 20 subredes ➔ 5 bits para el campo de subred ➔ máscara de red 255.255.255.248 (/29)
    - Quedan 3 bits para direccionamiento de host ➔ 8 – 2 = 6 hosts ➔ planificación válida.
    - Las subredes serán todas las combinaciones de los 5 bits de subred dentro del último bloque de 8 bits. A saber:
      - 201.222.5.0, .8, .16, .24, .32, ....., .248.
      - Es muy recomendable no usar la primera subred (201.222.5.0/29) por posible confusión en el enrutamiento general con toda la clase C (201.222.5.0/24).
      - Tambien es muy recomendable no usar la última subred (201.222.5.248/24) por posible confusión con la dirección broadcast de toda la red clase C.

- La desventaja es la pérdida de direcciones IP para la organización del encaminamiento y como direcciones de subred y de broadcast.
  - Clase C:
    - 254 hosts
    - con máscara /25, 2 subredes, 126 x 2 = 252 hosts. Pero si seguimos la recomendación, se pierde la primera y la última subred → 0 hosts. Así no es recomendable usar la máscara /25.
    - Con máscara /26, 4 subredes, 62 x 4 = 248 hosts. Se pierde la 1ª y última subred → 124 hosts.
    - /27, 8 – 2 subredes, 30 x 6 = 180 hosts.
    - /28, 16 – 2 subredes, 14 x 14 = 196 hosts.
    - /29, 32 – 2 subredes, 6 x 30 = 180 hosts.
    - /30, 64 – 2 subredes, 2 x 62 = 124 hosts.
    - /31, /32 inviable.

- Agrupamiento de subredes. (VLSM Variable Lenght Subnet Mask ó Direccionamiento sin clases).

  - Las subredes pueden agregarse.
  - Es útil cuando una organización necesita mas de 254 direcciones, de modo que solicita varas clases C contiguas. También es útil cuando la cantidad de hosts para cada una de las subredes varía considerablemente.
  - Por ejemplo, la agrupación 194.14.240.0/20, representa a aquellas redes de clase C que tienen los 20 bits de mayor peso iguales.

## 6.3. PROTOCOLOS DE INTERNET.

- Protocolos necesarios para establecer conexiones TCP/IP.

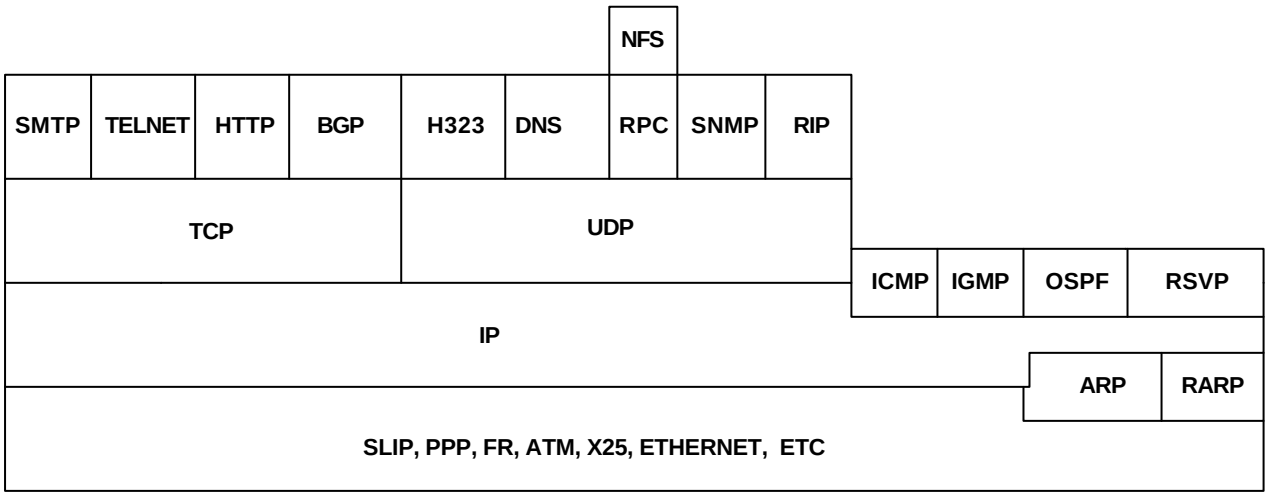



*Fig. 6.10*

### 6.3.1 Protocolo ARP.

- Está basado en el RFC 826
- La localización de equipos en una red es una tarea esencial en cualquier red de computadores. Nos interesa ahora enlazar dos niveles de direccionamiento:
  - Nivel de enlace mediante dirección MAC (en LAN o ATM).
  - Nivel de red, dirección IP, IPX, AppleTalk, (interconexión de redes).
- Es un protocolo de red que proyecta las direcciones de red (IP) y las direcciones de enlace (MAC).
- En medios compartidos es muy importante, pues permite disminuir las necesidades de procesamiento de las interfaces de los hosts al no "subir" los paquetes hasta la capa IP de cada uno de ellos y solo del host destino.
- Cada interfaz de red tiene asignada una dirección de nivel de enlace (dirección de hardware) de 48 bits (12 cifras hexadecimales) única. La IEEE (Institute of Electrical and Electronics Engineers) asignó los 3 primeros bytes a los fabricantes. El resto los asigna cada fabricante a su tarjeta.
- Funcionamiento:
  - En una sola red física, los hosts individuales se conocen en la red a través de su dirección física (MAC). Los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (dirección IP). Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, la interfaz de destino no la entiende.
  - Se crea una tabla (llamada caché ARP) que relaciona direcciones MAC con direcciones IP.
  - Hay dos casos de funcionamiento:

    - Si la máquina cuya dirección MAC se busca tiene una IP dentro de la misma red o subred (segmento), se manda una trama a nivel 2 de difusión (broadcast MAC FF:FF:FF:FF:FF:FF) pidiendo la dirección MAC de aquel host con la dirección de nivel 3 buscada (IP).

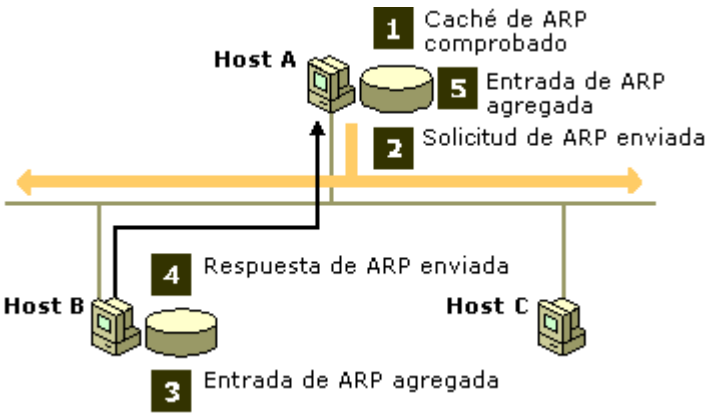



*Fig. 6.11*

    - Si no está en la misma subred, con ARP, el primer router que una ambos segmentos de red responde y da su dirección MAC. En soluciones óptimas, al ver que el host de dirección IP buscada está en otra red, la trama de datos se envía directamente al router.

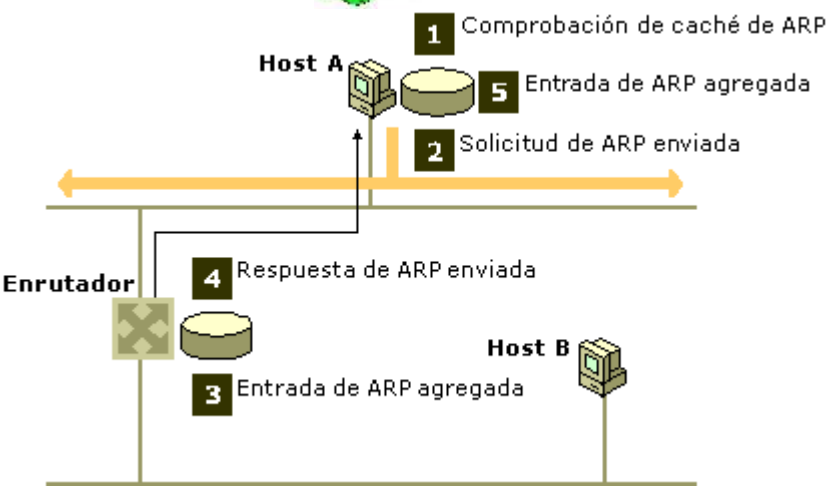



*Fig. 6.12*

- Ejemplo de captura de tramas ARP en una Ethernet
  - Formato de paquete ARP

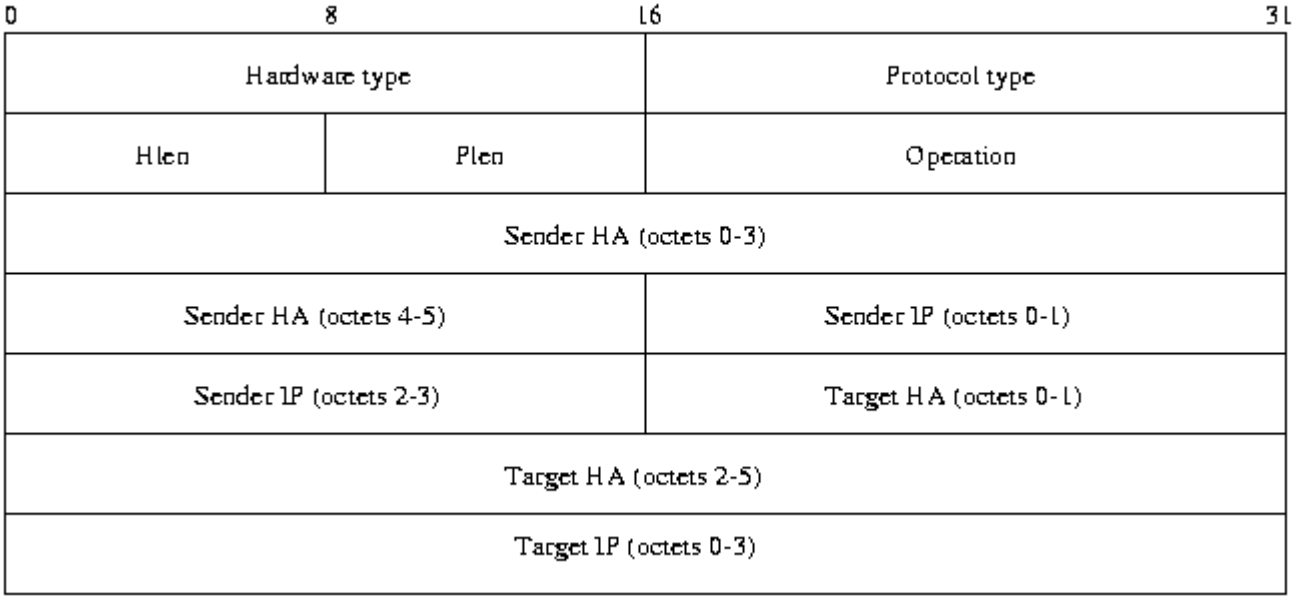



*Fig. 6.13*

- Captura de trama ARP con “Ethreal”

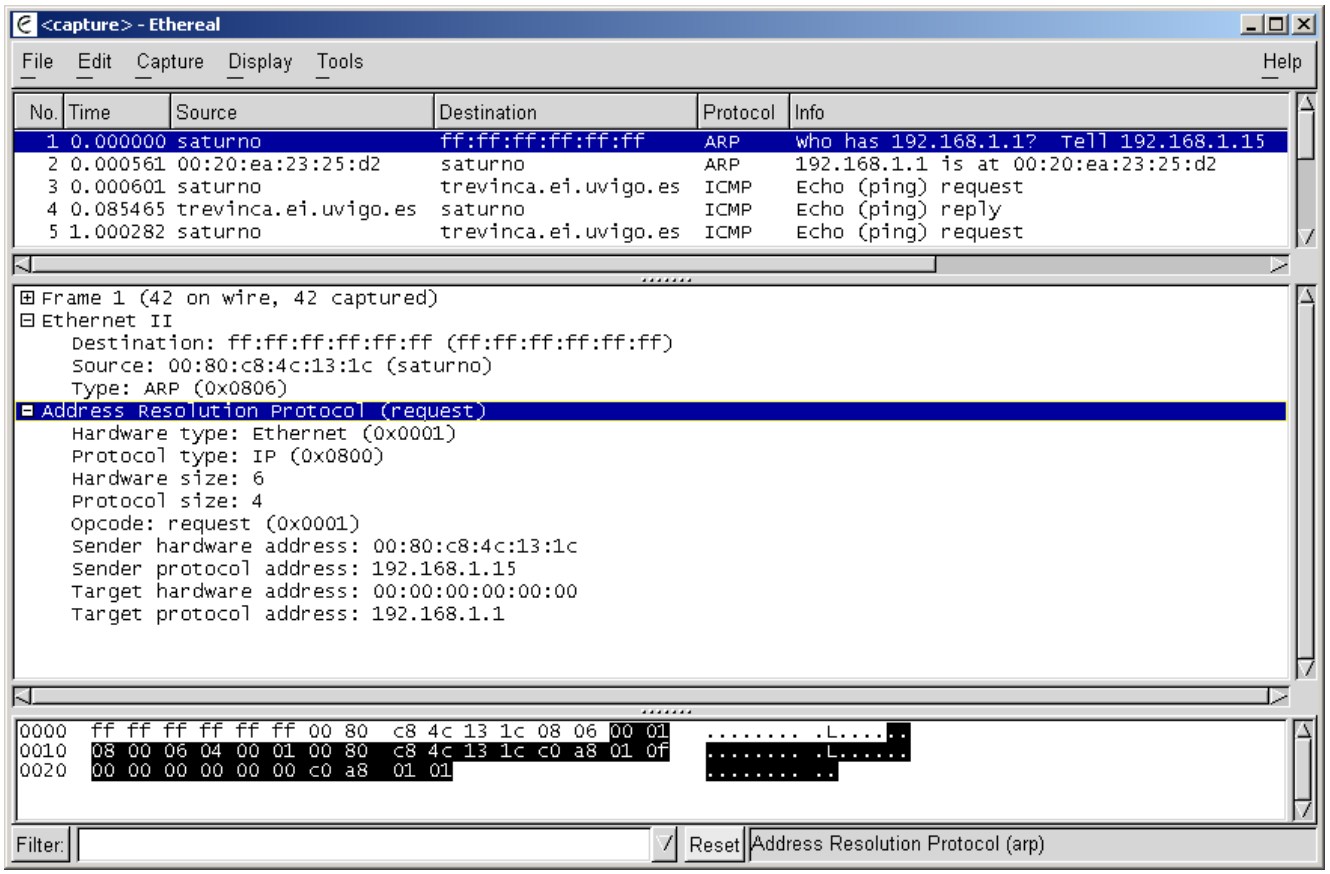



*Fig. 6.14*

- Aplicación
  - Tanto UNIX como Windows comando “arp”. Permite gestionar la tabla caché ARP.

**Windows 2000 Professional**

C:\>arp -a

Interfaz: 192.168.1.15 on Interface 0x1000003

| Dirección IP | Dirección física | Tipo |
|---|---|---|
| 192.168.1.1 | 00-20-ea-23-25-d2 | dinámico |
| 192.168.1.13 | 00-80-c8-1d-7f-8d | dinámico |

**Linux Debian 2.2.18**

venus:/home/redes# arp -a
? (192.168.1.1) at 00:20:EA:23:25:D2 [ether] on eth0
? (192.168.1.15) at 00:80:C8:4C:13:1C [ether] on eth0

### 6.3.2. Protocolo ICMP.

- RFC 792.
- Cuando un "router" o un host de destino debe informar al host fuente acerca del procesamiento de datagramas, utiliza ICMP ("Internet Control Message Protocol" *Protocolo de Mensajes de Control de Internet*). ICMP puede caracterizarse del modo siguiente:

  - ICMP usa IP como si ICMP fuera un protocolo del nivel superior (es decir, los mensajes ICMP se encapsulan en datagramas IP). ICMP es parte integral de IP y debe ser implementado por todo módulo IP.
  - ICMP se usa para informar de algunos errores. Aún puede ocurrir que los datagramas no se entreguen y que no se informe de su pérdida. La fiabilidad debe ser implementada por los protocolos de nivel superior que usan IP.
  - ICMP puede informar de errores en cualquier datagrama IP con la excepción de mensajes IP, para evitar repeticiones infinitas.
  - Para datagramas IP fragmentados, los mensajes ICMP sólo se envían para errores ocurridos en el fragmento cero. Es decir, los mensajes ICMP nunca se refieren a un datagrama IP con un campo de desplazamiento de fragmento.
  - Los mensajes ICMP nunca se envían en respuesta a datagramas con una dirección IP de destino que sea de broadcast o de multicast.
  - Los mensajes ICMP nunca se envían en respuesta a un datagrama que no tenga una dirección IP de origen que represente a un único host. Es decir, la dirección de origen no puede ser cero, una dirección de loooopback, de broadcast o de multicast.
  - Los mensajes ICMP nunca se envían en respuesta a mensajes ICMP de error. Pueden enviarse en respuesta a mensajes ICMP de consulta (los tipos de mensaje ICMP 0, 8, 9, 10 y 13 al 18).

- Formato paquete ICMP

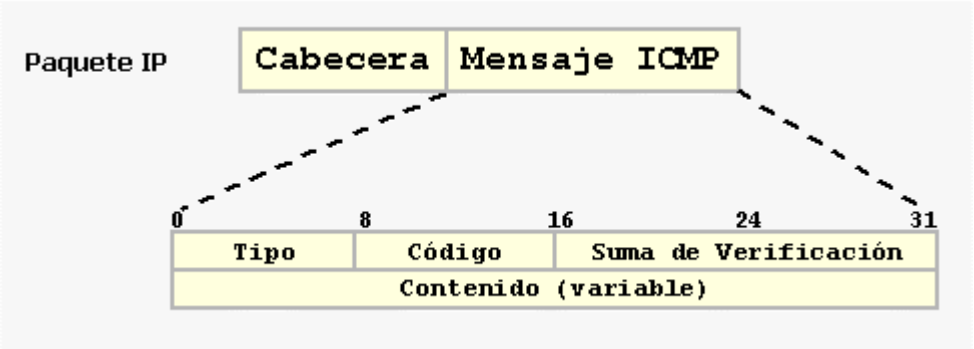



*Fig. 6.15*

  - El contenido depende del tipo de mensaje

- Principales tipos de mensajes ICMP

| identificador | tipo de mensaje |
|---|---|
| 0 | Echo Reply (respuesta de eco) |
| 3 | Destination Unreacheable (destino inaccesible) |
| 4 | Source Quench (disminución del tráfico desde el origen) |
| 5 | Redirect (redireccionar - cambio de ruta) |
| 8 | Echo (solicitud de eco) |
| 9 | Router-advertisement (Publicación de rutas). |
| 10 | Router-solicitation (Petición de ruta). |
| 11 | Time Exceeded (tiempo excedido para un datagrama) |
| 12 | Parameter Problem (problema de parámetros |
| 13 | Timestamp (solicitud de marca de tiempo) |
| 14 | Timestamp Reply (respuesta de marca de tiempo) |
| 15 | Information Request (solicitud de información) - obsoleto- |
| 16 | Information Reply (respuesta de información) - obsoleto- |
| 17 | Addressmask (solicitud de máscara de dirección) |
| 18 | Addressmask Reply (respuesta de máscara de dirección) |

- Funcionamiento básico:
  - Se utiliza como herramienta de resolución de problemas.
  - Algunos tipos de mensaje se implementan en algunos programas (nivel aplicación):
    - Ping. Programa de solicitud de confirmación de eco. Este comando está disponible en prácticamente todas las plataformas que existen. Puede tener diferentes opciones, a destacar:
      - Tamaño de paquete
      - No fragmentación
      - Registro de ruta
    - Trace. Programa de traceo de rutas. Este comando está disponible en prácticamente todas las plataformas. Tiene diferentes nombres en función de la plataforma:
      - Tracert: Windows 9X, 2000, NT ...
      - Traceroute: UNIX, Linux
      - Trace: cisco IOS.

- Se puede enviar como respuesta por un error detectado (detección de un problema en la red o en la cabecera IP de un paquete):

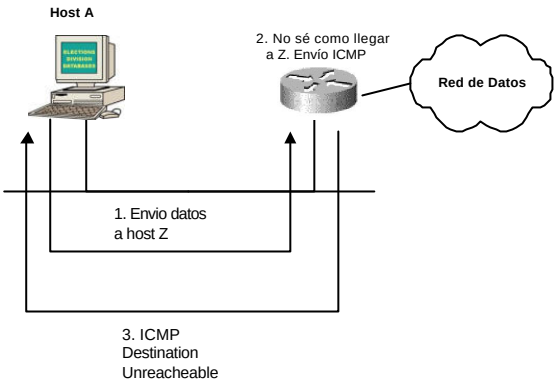



*Fig. 6.16*

- Se puede solicitar una comprobación, a voluntad del administrador (ping “hostB”):

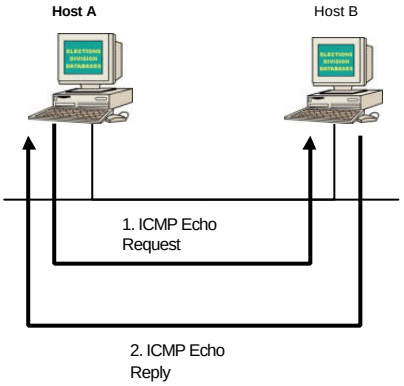



*Fig. 6.17*

- Se puede solicitar la ruta hacia un destino

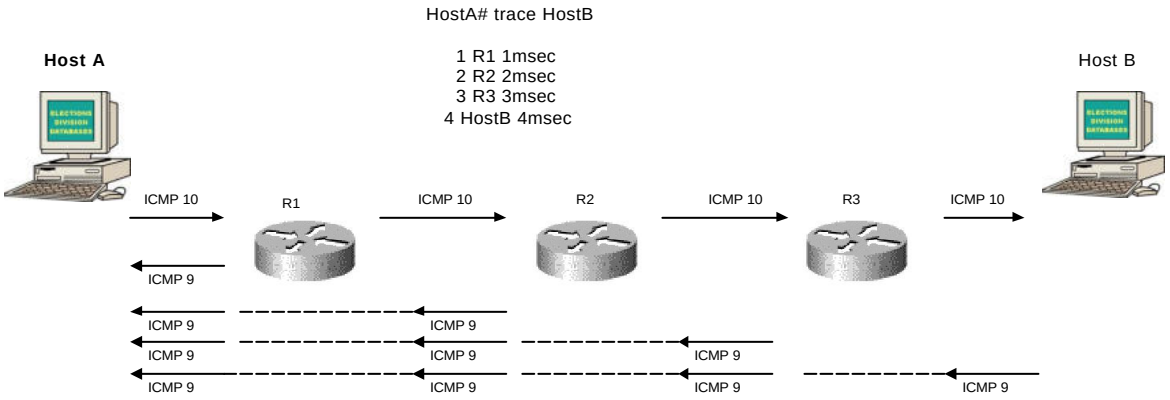



*Fig. 6.18*

- Captura de trama ICMP con Ethreal.

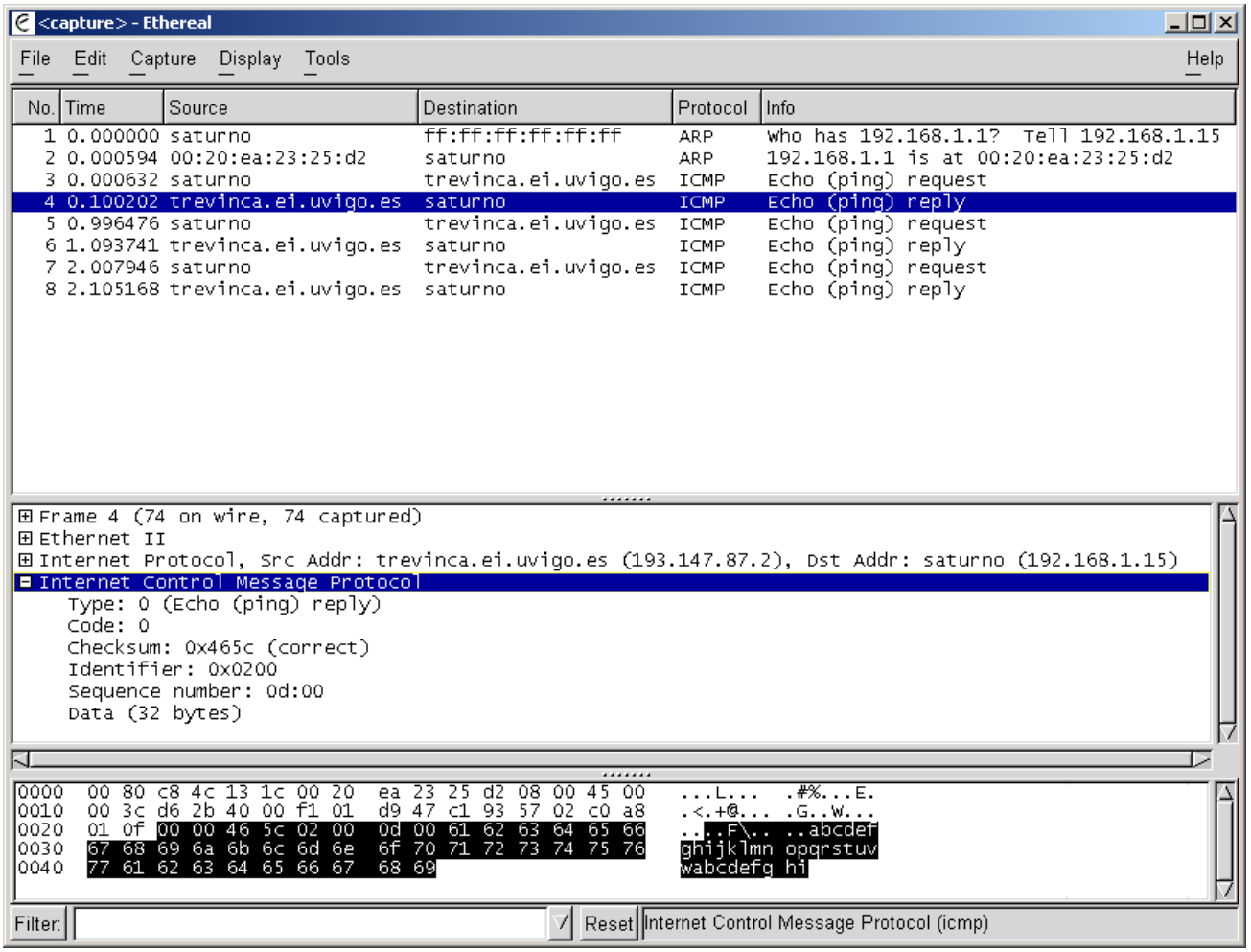



*Fig. 6.19 ping trevinca.ei.uvigo.es*

### 6.3.3. ENRUTAMIENTO. Protocolos de enrutamiento. SISTEMAS AUTÓNOMOS

- Enrutamiento.
    - El sistema de direccionamiento (los paquetes IP) IP necesita conocer el host de destino. Toda la electrónica de red intermedia necesita por tanto conocer tambien como llegar a ese destino.
    - El enrutamiento o encaminamiento se produce a varios niveles de la arquitectura de protocolos. Sobre todo en el “acceso al medio, MAC” y en “Interred, IP”.
    - Los routers conocen los destinos de tres formas:
        - Rutas estáticas (enrutamiento estático), dadas por el administrador.
        - Rutas por defecto (enrutamiento estático), dadas por el administrador. Son rutas de salida para los paquetes con un destino indeterminado por el router.
        - Rutas dinámicas (enrutamiento dinámico), dadas por el intercambio de información con otros routers. La información entre routers se hace a través de protocolos de enrutamiento (algoritmos de encaminamiento).

- La bidireccionalidad en la mayoria de las comunicaciones entre hosts obliga a conocer la ruta de los paquetes en ambos sentidos, aunque estas no tienen porqué ser las mismas.

- Configuración de un router. Rutas estáticas.

  - El enrutamiento estático (o fijo) es posible en redes sencillas.
  - Son tablas mantenidas en los routers y en los hosts que como mínimo dan información de:
    - Red o host de destino
    - Siguiente salto (gateway) para el acceso a la red o host de destino. El router debe conocer como llegar al siguiente salto (gateway) o está directamente conectado a alguna de sus interfaces.

  - Suele ser necesario activar la labor de encaminamiento. (IOS *ip routing, no ip routing,* UNIX – LINUX *ip_forwarding*).
  - Varias implementaciones en función del sistema operativo:
    - IOS: *ip route network [mask] {address/interface} [distance]*
    - UNIX, Linux: *ip route add/delete ..... . route add/del .....*
    - LRP: *ip route add/del "red" via "gateway" dev "interface"*
    - Windows XX: *route add/delete.*
    - *Para visualizar las rutas entre otras funciones existe el comando "netstat".*

- Ejemplo de rutas estáticas.

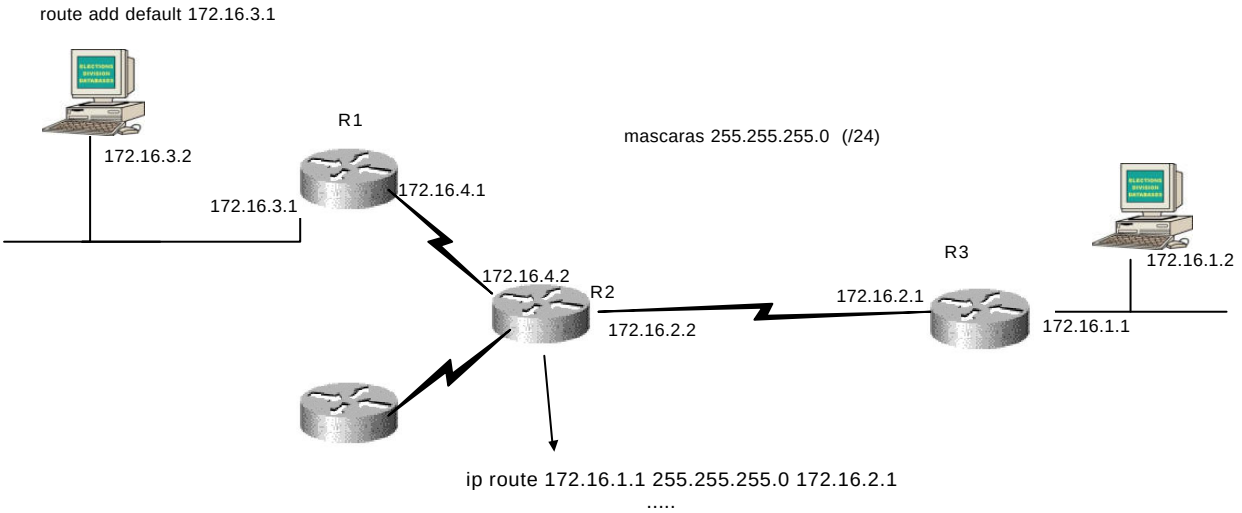



*Fig. 6.20*

- Problemática de conexiónes privadas-públicas.

  - El hecho que existan rangos de direcciones no gestionadas directamente por el IANA, sino por las organizaciones para sus redes privadas, hace que exista una gran duplicidad de direcciones IP susceptibles de ser interconectadas.
  - Los routers de internet no definen rutas para esas direcciones. Por tanto la problemática está en como acceder a un host que tenga dicha dirección, y por tanto en como un host con esa dirección accede a internet.
  - La solución se implementa en la capa de aplicación de los routers que hacen posible la comunicación pública-privada. Este router debe disponer de al menos una dirección pública que conecte a internet, y una dirección privada que conecte a la organización.
  - Varias soluciones:

- **Enrutamiento puro:** si tanto la electrónica de red intermedia, como los hosts origen y destino tienen implementadas las rutas correctas, no suele haber en principio problema para la comunicación entre IP's privadas e IP's públicas.

- **Gateway**: router de aplicación
  - Gatweay default: bloquea cualquier paquete cuyo destino u origen sea una dirección IP reservada. Mantiene completamente separada la red (o host) con direcciones IP reservadas de la red (o host) con dirección IP externa (Internet). Es un firewall básico.

- **NAT (Network to Address Translation)** (enmascaramiento). RFC 1631.

  - El concepto de NAT se aplica a varias soluciones de interconexión de IP's privadas con IP's públicas. RFC 2663.
  - Consiste en enmascarar la dirección privada del origen con la dirección pública del router.
  - En el router se mantiene una tabla que relaciona la "conexión" (IP destino, IP origen, protocolo, identificador de la conexión) privada con la "conexión" pública. Así se puede volver al host origen.
  - Se activa normalmente en el Kernel del sistema operativo (Windows, Linux – UNIX) (ip_masquerading), o viene por defecto (o como opción) en Sistemas operativos de red (IOS, LRP).
  - El cliente se configura para utilizar el router como dispositivo NAT de salida.
  - Existen dos variantes básicas del NAT:
    - Estático: el router dispone de mas IP's públicas de salida que IP's privadas a las que dar acceso a internet.
    - Dinámico: el router dispone de una sola IP pública y tiene que dar salida a mas de una IP privada. Este es el caso mas habitual, y puede funcionar de forma parecida al proxy, o con las tablas antes descritas.

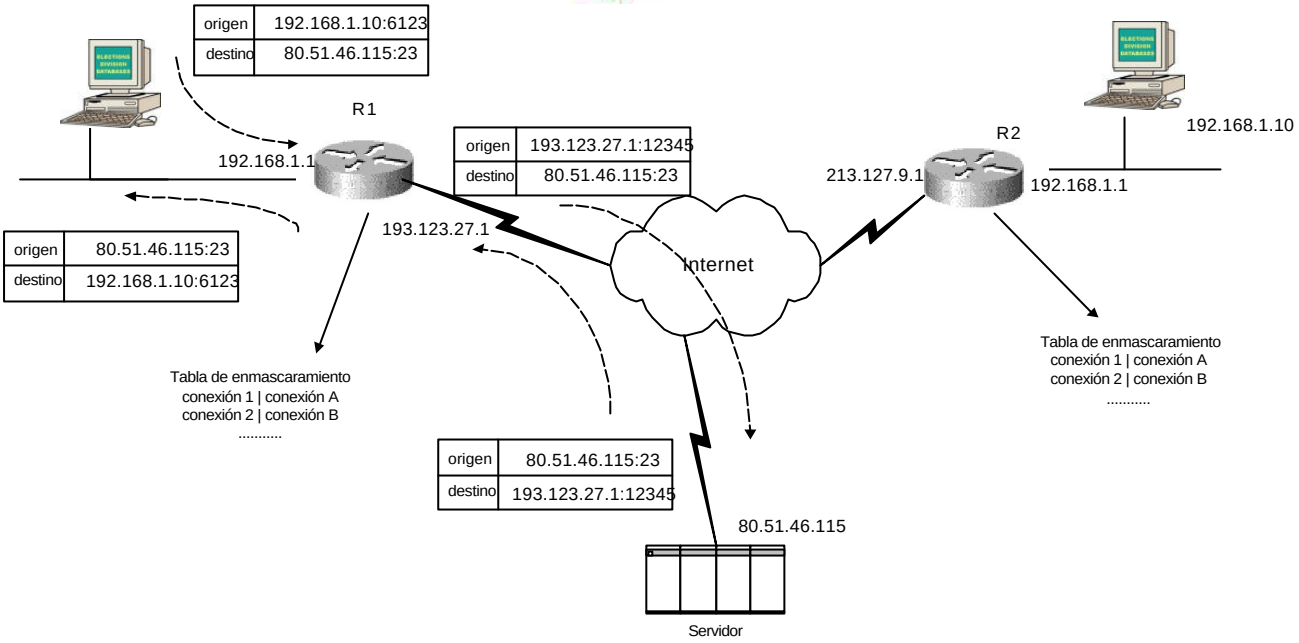
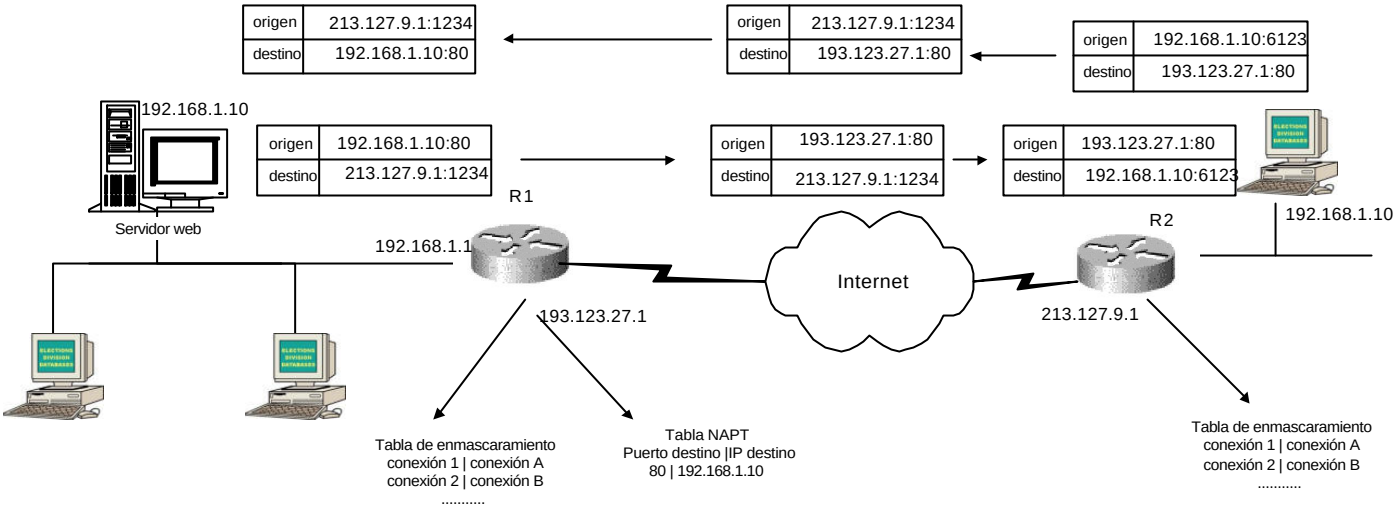



*Fig. 6.21*

- Los registros de las tablas internas tienen una vida limitada para no saturar la tabla. Si la respuesta no se recibe en ese tiempo, el registro se borra.
- Cuando la identificación de la conexión se establece mediante la relación IP privada, Puerto (transporte) privado → IP pública, Puerto público, se le conoce por NAPT (Network Address and Port Translation).
- Problemas:
  - Al trabajarse con tablas, demasiados registros, aumentan la necesidad de procesamiento de los routers NAT.
  - Necesidad de recalcular en el router determinados campos del paquete IP.
  - Si la dirección IP de destino tambien es necesaria en el protocolo de aplicación, (es decir, en el campo de datos), el sistema solo sigue funcionando, si el router tiene soporte para ese protocolo de aplicación. Problema habitual en protocolos de videoconferencia y de VoIP (protocolo H323).
  - El principal problema del sistema es el hecho de que los equipos de la red interna de la organización son clientes pasivos de las comunicaciones, los servidores tienen que estar en zona internet.

- NAT reverso (Network Address and Port Translation).
  - Soluciona el último problema descrito del NAT.
  - Cada router tiene una solución particular para esta problemática. Palabras clave NAPT, Port_forwarding, NAT-PAT, NAT reverso, etc.
  - La idea es la de utilizar como identificadores de la conexión, no sólo los de la conexión del paquete IP, sino también los puertos de la capa de transporte (TCP, UDP). Por tanto sería una solución de la capa de aplicación utilizando las capas de transporte e IP.

- El router determina un servidor mediante el puerto al que se conecta una IP pública a su IP privada. Realmente mapea cualquier conexión externa a un puerto UDP o TCP (capa de transporte) hacia la IP privada del servidor dado de alta.




## NAT-NAPT

*Fig. 6.22*

- **Proxy**: Es un gateway de aplicación. En realidad no hace ningún encaminamiento salvo a nivel de aplicación, pues no encamina ni enmascara los paquetes, sino simplemente analiza el contenido del protocolo de la aplicación cliente y hace el trabajo por ella.

  - El proxy está <u>generalmente</u> implementado en un ordenador con dos interfaces de red, una hacia la red lógica interna y otra hacia la red lógica externa (internet).

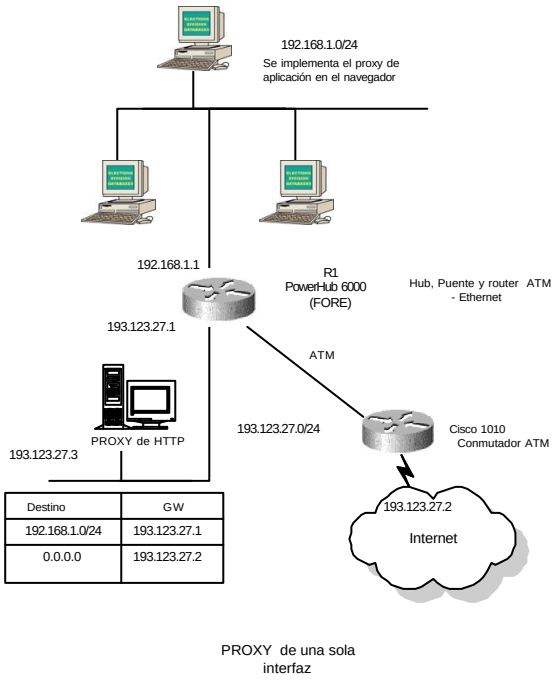



*Fig. 6.23*

- Cuando una aplicación cliente de una red interna necesita acceder a un servicio de un servidor externo, se lo solicita al proxy.
- El servidor proxy conecta con el servidor externo y devuelve los datos a la aplicación cliente.
- El funcionamiento se aprecia en el esquema (fig 6.24):

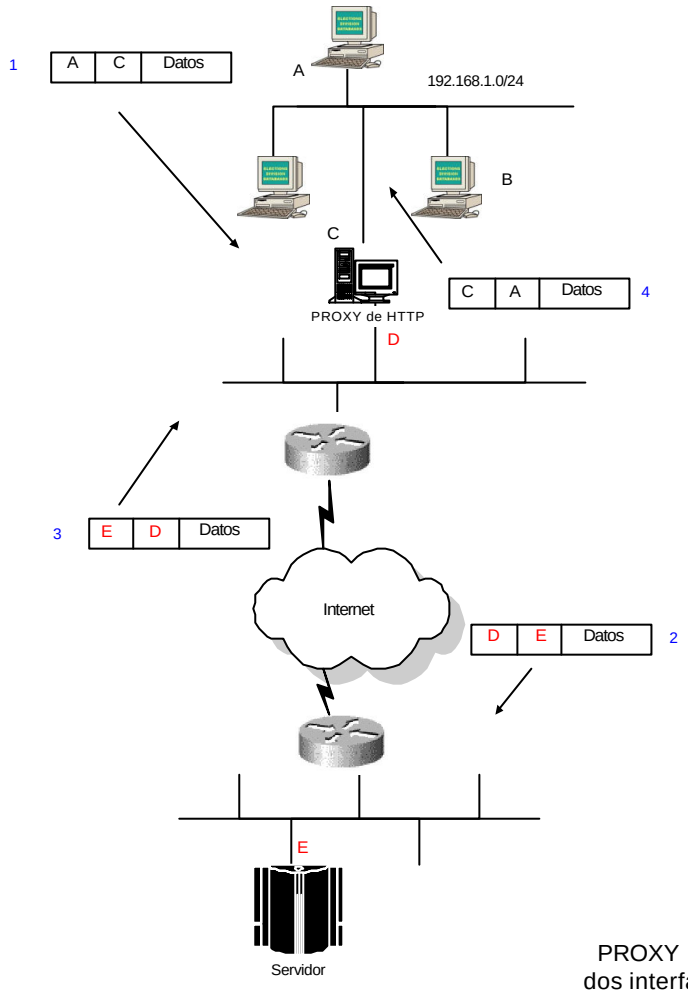



*Fig. 6.24*

- La dirección final de destino se averigua precisamente mediante el protocolo proxy de aplicación (protocolo socks). En la zona de datos del paquete IP está la dirección de destino final que reconoce el proxy.
- El servidor proxy puede ofrecer además otros servicios:
  - Autentificación
  - Caché
  - Restricción de acceso, por contenido, IP, horas etc.

- **Firewall**. Es una aplicación de filtrado de paquetes, que habitualmente se implementa en equipos de encaminamiento (routers) con varias tarjetas de red, filtrando los paquetes por el contenido de sus cabeceras, tanto a nivel IP como de transporte (es decir, por cualquiera de los campos que son identificativos de la conexión.)
  - Es muy utilizado como medida de seguridad y compatible con las soluciones anteriores.

- Problemática de conexiones privadas – públicas – privadas.
  - **Tunneling**: tiene como principio colocar una estructura de información dentro de otra. En el caso de tunneling de nivel 3 (el mas usado) consiste colocar la información real de la conexión dentro del paquete de datos de la estructura IP.
    - Normalmente va encriptada.
    - Es util para conectar diversas oficinas remotas de una organización con sensación de estar en la misma red.

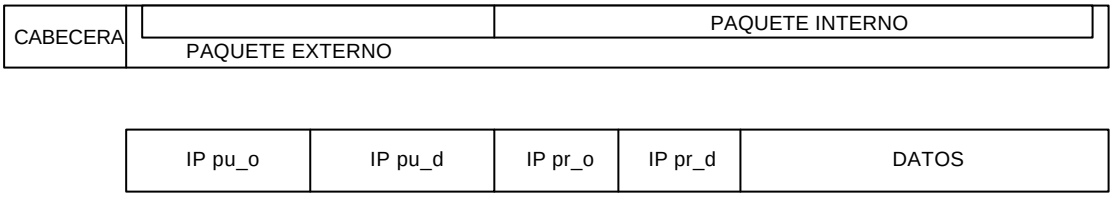



*Fig. 6.25*

- Ejemplo:

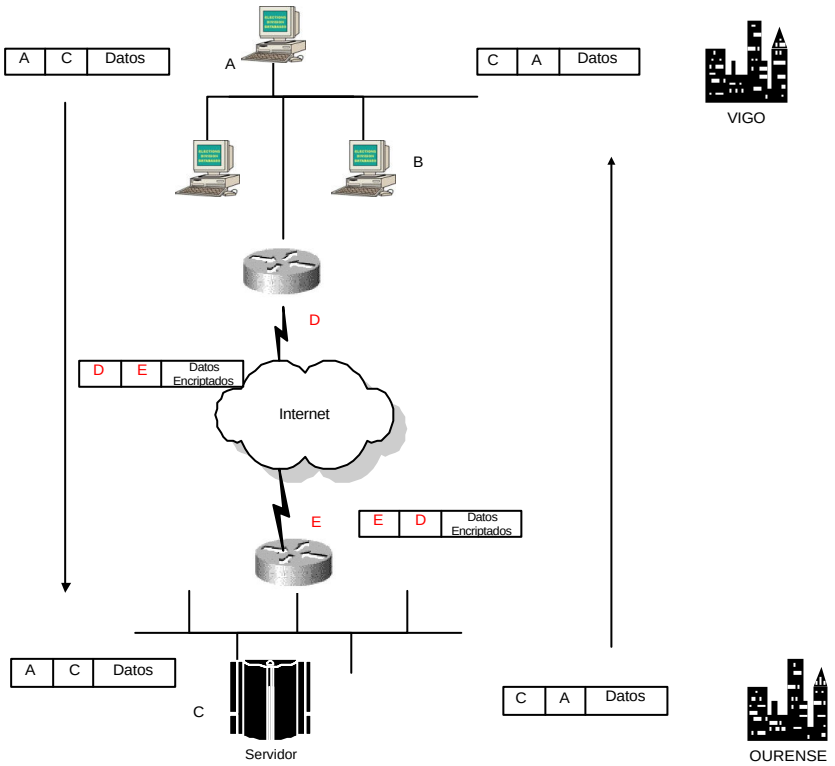



*Fig. 6.26*

- Se utiliza en un nivel de aplicación dentro del router. En ello se basan las diversas soluciones de redes privadas virtuales (VPN).

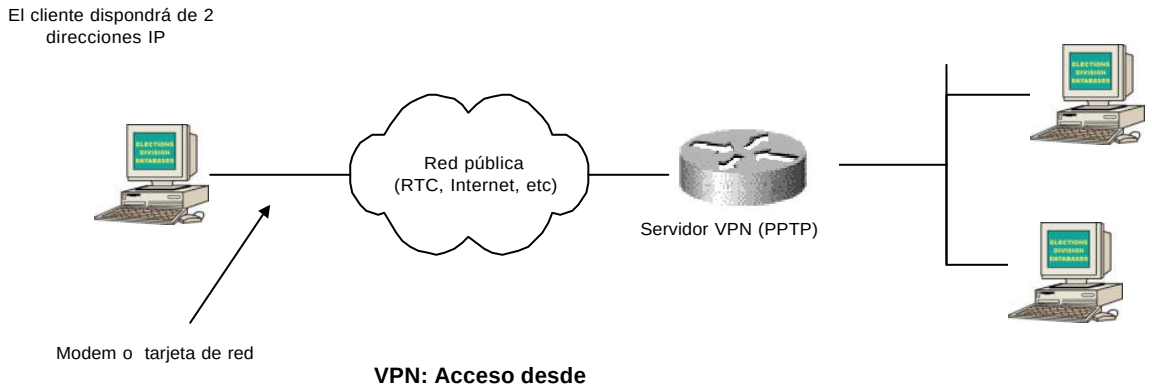
- **VPN**: solución mas común al problema de conexión privada-pública-privada. Es un concepto genérico con multiples soluciones propietarias.
  El uso de estas soluciones, sustituye a la adquisición de redes privadas a través de operadores como FR o ATM disminuyendo de esa forma los costes.
  - Novell BorderManager
  - IPsec. RFC 2401 y otras. (http://www.ietf.org/html.charters/ipsec-charter.html). La mas utilizada.
  - PPTP. RFC 2637
  - Etc.
  - Hay una solución a nivel de enlace comparable a VLAN bajo el protocolo MPLS (MultiProtocol Label Switching). RFC 3031.

  Se distinguen tres características básicas dentro de un sistema de VPN:
  - Tunneling
  - Autentificación
  - Encriptación

  En general se puede hacer mediante soluciones Software (p.ej. PC – PC, PC - Servidor ), o mediante soluciones Hardware propietarias (Router – Router)

  Desventajas:
  - Aumento de la necesidad de procesamiento de los routers o hosts
  - Mayor consumo de ancho de banda

  Posibles Configuraciones:
  - Acceso remoto desde el PC cliente.




**VPN: Acceso desde cliente**

*Fig. 6.27*

- Acceso entre subredes. Permite construir una intranet utilizando una red pública (Internet).

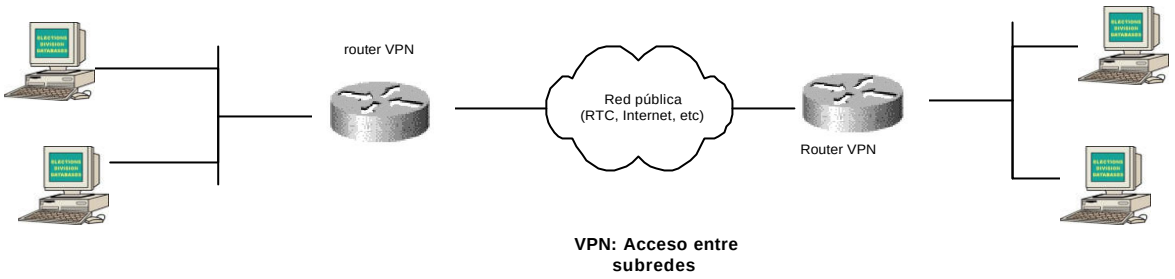



*Fig. 6.28*

- Protocolos de encaminamiento. Sistemas Autónomos
  - En un conjunto de redes, los dispositivos de encaminamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas.
  - La decisión se toma basándose en el conocimiento de la topología de la red y las condiciones del conjunto de redes como el coste (peso), velocidad, retardo etc.
  - Un encaminamiento fijo es posible en una red sencilla, pero en redes más complejas se utiliza un encaminamiento dinámico:
    - Los routers intercambian información entre ellos
    - Se debe evitar encaminar a través de redes que han sufrido fallos o estén saturadas.
  - Se distingue entre:
    - Información de encaminamiento, que es información que se intercambian los routers entre sí para generar en cada uno de ellos información sobre la topología de red, retardo etc.
    - Algoritmo de encaminamiento, usado por cada router para encaminar un datagrama particular basándose en la información de encaminamiento actual.

- Sistemas Autónomos (AS). RFC 1930
  - Los routers y redes u subredes se pueden agrupar como un sistema autónomo bajo la misma administración. Las condiciones para que varios routers pertenezcan a un mismo sistema autónomo son:
    - Estar interconectados
    - Ejecutar los mismos protocolos de enrutado
    - Estar gestionados por un mismo organismo
    - Tener el mismo identificador de sistema autónomo.
  - Existirá un IRP (Interior Routing Protocol) que pasará información entre routers dentro de un sistema autónomo. Los IRP pueden hacerse a medida de aplicaciones y requisitos específicos.
  - Existirá también un ERP (Exterior Routing Protocol) ) que intercambiará información entre sistemas autónomos diferentes.
  - Los AS están números del 0 al 65535. Los asigna el IANA (para internet) y los que están entre 64512 y 65535 están reservados.

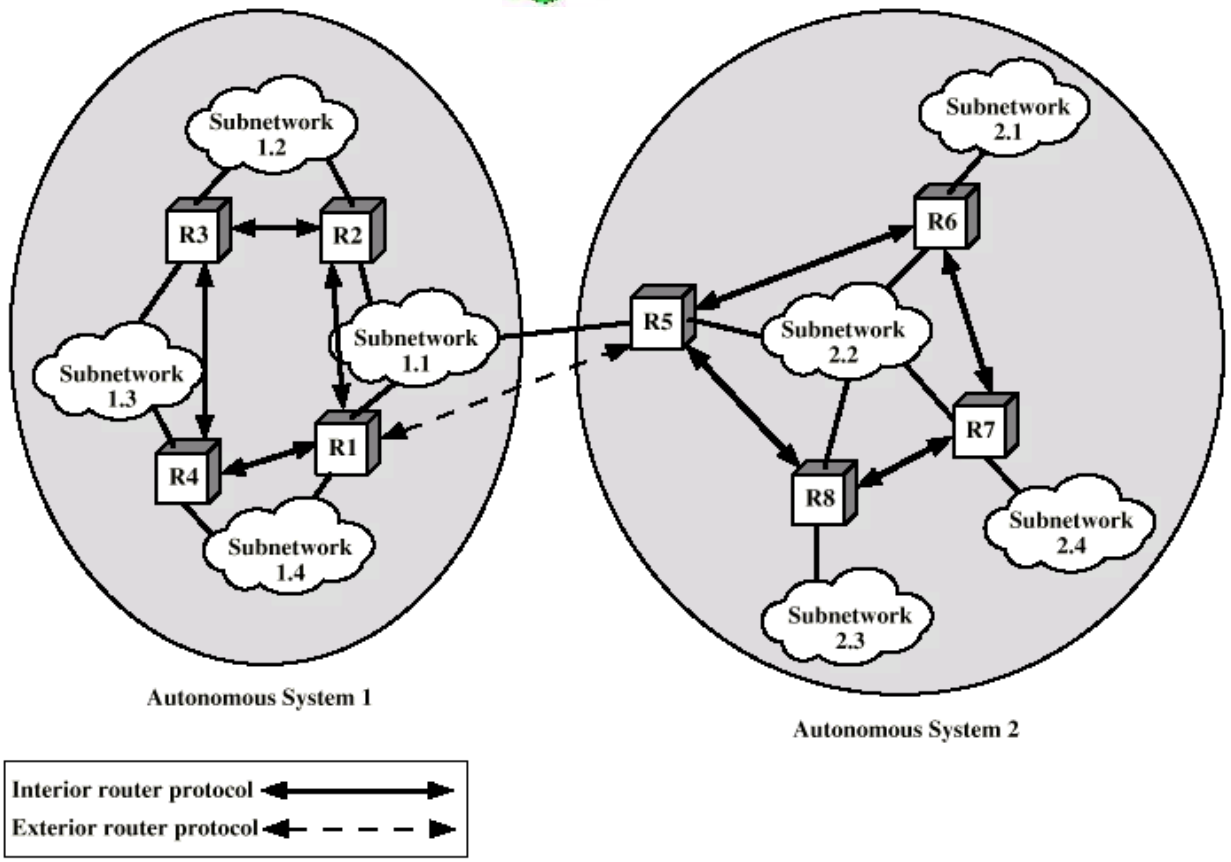



*Fig. 6.29*

- **RIP** (Routing Information Protocol). RFC 1058, RFC 1723.
    - Es un protocolo de encaminamiento interior (IRP).
    - Está pensado para redes homogéneas, conectados por enlaces iguales, por lo que la métrica basada en ancho de banda se reduce a una cuenta de saltos. Con diferenes tipos de medios, esta métrica puede no identificar el mejor medio.
    - Sus características clave son:
        - Protocolo de encaminamiento del tipo vector distancia
        - El máximo número de saltos permitido es 15.
        - Las tablas de encaminamiento se difunden cada 30 seg.
        - Es capaz de repartir el tráfico entre varios caminos de igual coste.
        - Usa el puerto UDP 520.
        - Es el mas usado historicamente por sistemas UNIX.

o Formato de paquete RIP (UDP)

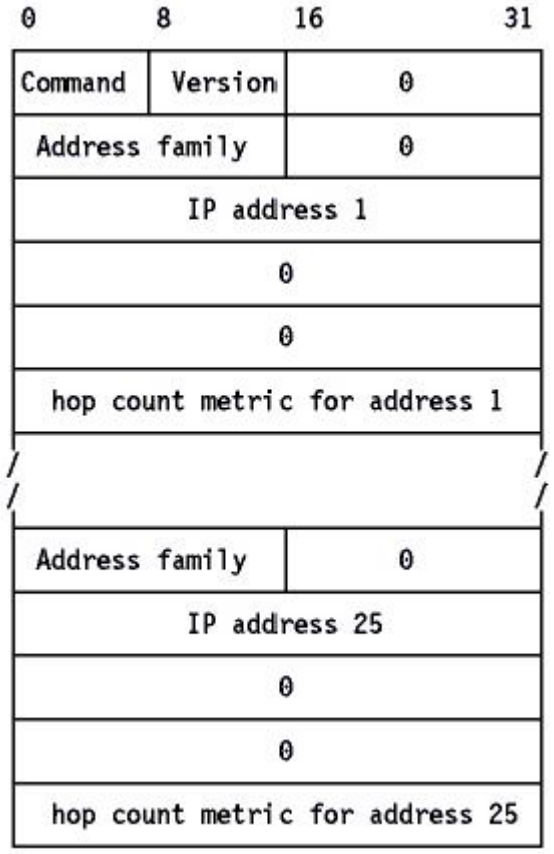



*Fig. 6.30*

- Command**:** Es 1 para una petición RIP o 2 para una respuesta.
- Version: Es 1 para RIP-1 o 2 para RIP-2.
- Address Family: Es 2 para direcciones IP.
- IP address: Es la dirección IP de para esta entrada de encaminamiento: un host o una subred (caso en el que el número de host es cero).
- Hop count metric: Es el número de saltos hasta el destino. La cuenta de saltos para una interfaz conectada directamente es de 1, y cada "router" intermedio la incrementa en 1 hasta un máximo de 15, con 16 indicando que no existe ruta hasta el destino.

o Visualización del formato de paquete RIP con Ethereal

*Linux 2.0.34*

- *HostA:~$ ripquery -n 192.168.1.1*
- *44 bytes from 192.168.1.1:*
- *192.168.1.0 metric 1*
- *217.127.82.0 metric 1*

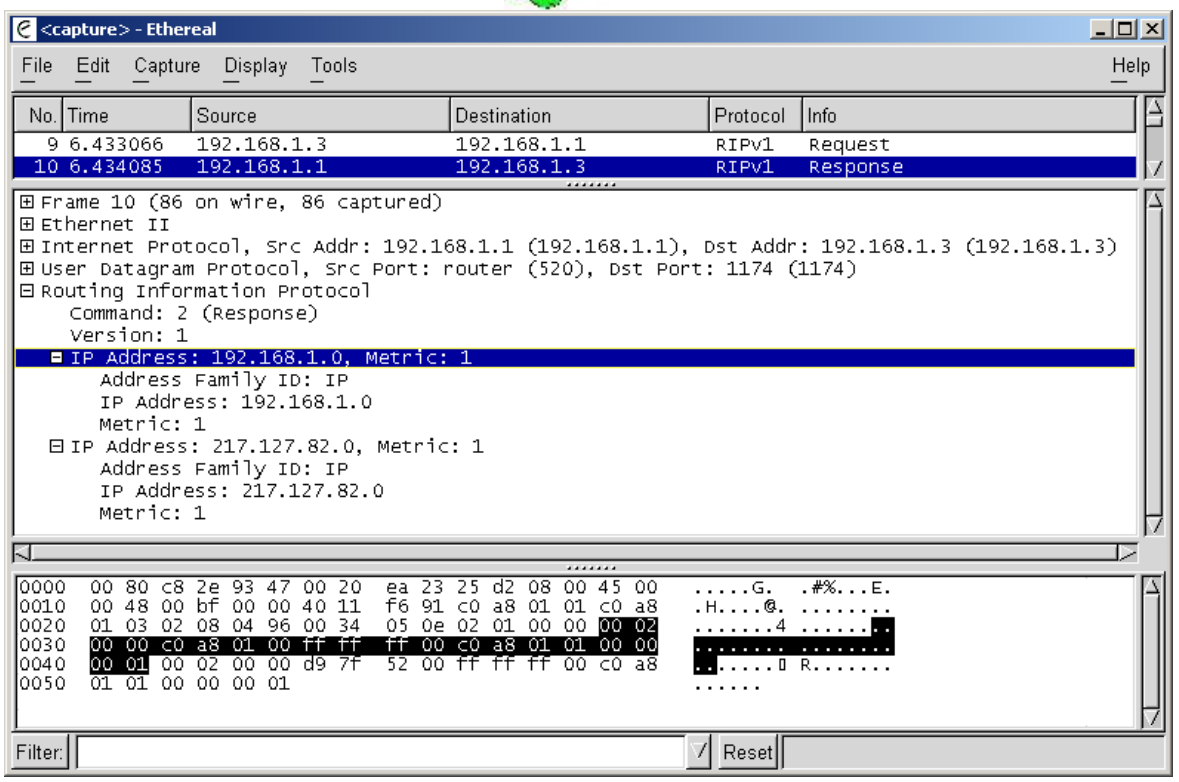



*Fig. 6.31*

- Desventajas de RIP

  - Útil solo en pequeñas redes con pocos routers
  - El tamaño de paquete de RIP es de 512 bytes máximo. Entonces con tablas grandes de rutas hay que enviar varios paquetes RIP, pues se envían todos los identificadores de red.
  - Una actualización de tablas cada 30 segundos hace que se necesite un importante ancho de banda.
  - Solo reconoce hasta 15 saltos, el 16 significa ruta no encontrada. Para redes grandes es una desventaja importante.
  - En la versión 1, no contempla máscaras de subred, la versión 2 sí.
  - Es un protocolo inseguro (no existe forma de limitar los mensajes a un determinado grupo de routers).
  - RIP utiliza métricas fijas para evaluar el coste de los enlaces basadas en el número de saltos. Esto no siempre es la mejor solución para alcanzar una red.

- Funcionamiento:

  - Cuando RIP se inicia, envía un mensaje a cada uno de sus vecinos pidiendo una copia de la tabla de encaminamiento del vecino. Este mensaje es una solicitud (el campo "command" se pone a 1) con "address family" a 0 y "metric" a 16. Los "routers" vecinos devuelven una copia de sus tablas de encaminamiento.

- Cuando RIP está en modo activo envía toda o parte de su tabla de encaminamiento a todos los vecinos (por broadcast y/o con enlaces punto a punto). Esto se hace cada 30 segundos. La tabla de encaminamiento se envía como respuesta ("command" vale 2, aunque no haya habido petición).
- Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás "routers".
- Cuando RIP recibe una respuesta, el mensaje se valida y la tabla local se actualiza si es necesario.

Para mejorar el rendimiento y la fiabilidad, RIP especifica que una vez que un "router" (o host) a aprendido una ruta de otro, debe guardarla hasta que conozca una mejor (de coste estrictamente menor). Esto evita que los "routers" oscilen entre dos o más rutas de igual coste.

- Cuando RIP recibe una petición, distinta de la solicitud de su tabla, se devuelve como respuesta la métrica para cada entrada de dicha petición fijada al valor de la tabla local de encaminamiento. Si no existe ruta en la tabla local, se pone a 16.
- Las rutas que RIP aprende de otros "routers" expiran a menos que se vuelvan a difundir en 180 segundos (6 ciclos de broadcastadcast). Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

o Ejemplo

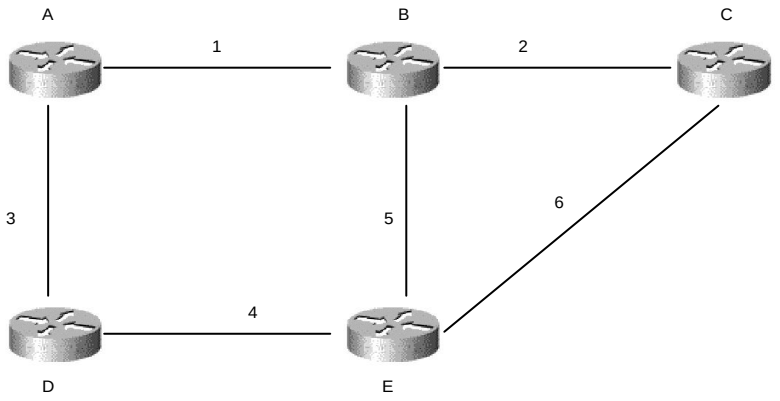



*Fig. 6.32*

- A tiene inicialmente la ruta, al igual que el resto.

| Destino | Sig. Salto | Métrica |
|---|---|---|
| A | 0 | 0 |

- A envía su tabla a sus vecinos B y D, quedando la tabla de B (p.ej.)

| Destino | Sig. Salto | Métrica |
|---|---|---|
| B | 0 | 0 |
| A | 1 | 1 |

- Al actualizar B y D sus tablas, B transmite sus tablas para sus vecinos A, C y E. A al recibir los mensajes de B y D quedan sus tablas como sigue:

| Destino | Sig. Salto | Métrica |
|---|---|---|
| A | 0 | 0 |
| B | 1 | 1 |
| D | 3 | 1 |

- El router C recibirá un mensaje de B a través del enlace 2 y quedarán sus tablas de la siguiente forma

| Destino | Sig. Salto | Métrica |
|---|---|---|
| C | 0 | 0 |
| B | 2 | 1 |
| A | 2 | 2 |

- Cuando un router recibe una tabla de actualización de otro router, verifica cada ruta de modo que da preferencia a las rutas con menor métrica para el mismo destino. Así lastablas van convergiendo. Así quedaría la tabla de A:

| Destino | Sig. Salto | Métrica |
|---|---|---|
| A | 0 | 0 |
| B | 1 | 1 |
| D | 3 | 1 |
| C | 1 | 2 |
| E | 3 | 2 |

- **OSPF** (Open Shortest Path First, Protocolo Abierto del Primer Camino mas Corto). RFC 1583, RFF 2328)

  - Las características clave del OSPF son:
    - Protocolo de estado de enlace.
    - La métrica utilizada es definida por el usuario.
    - Puede utilizarse el retardo, la velocidad de transmisión, el coste y otros factores.
    - Es capaz de repartir el tráfico entre varios caminos de igual coste (balanceo de carga).
    - Reconocimiento de sistemas jerárquicos.
    - Es el IRP recomendado en internet.

  - Principios:
    - Por un lado, cada dispositivo de encaminamiento mantiene la información del estado de cada uno de sus enlaces locales a las subredes y periodicamente transmite esta información actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento.
    - Por otro lado, cada dispositivo mantiene una base de datos que refleja la topología conocida del sistema autónomo expresado como un grafo dirigido que consta de:
      - Vértices o nodos (routers y redes)
      - Arcos (unión de routers y redes)
    - Se utiliza el algorítmo de Dijstra para calcular el camino mas corto de un nodo a todos los otros.

  Ejemplo del RFC:

  Topología inicial y estructura de grafos:

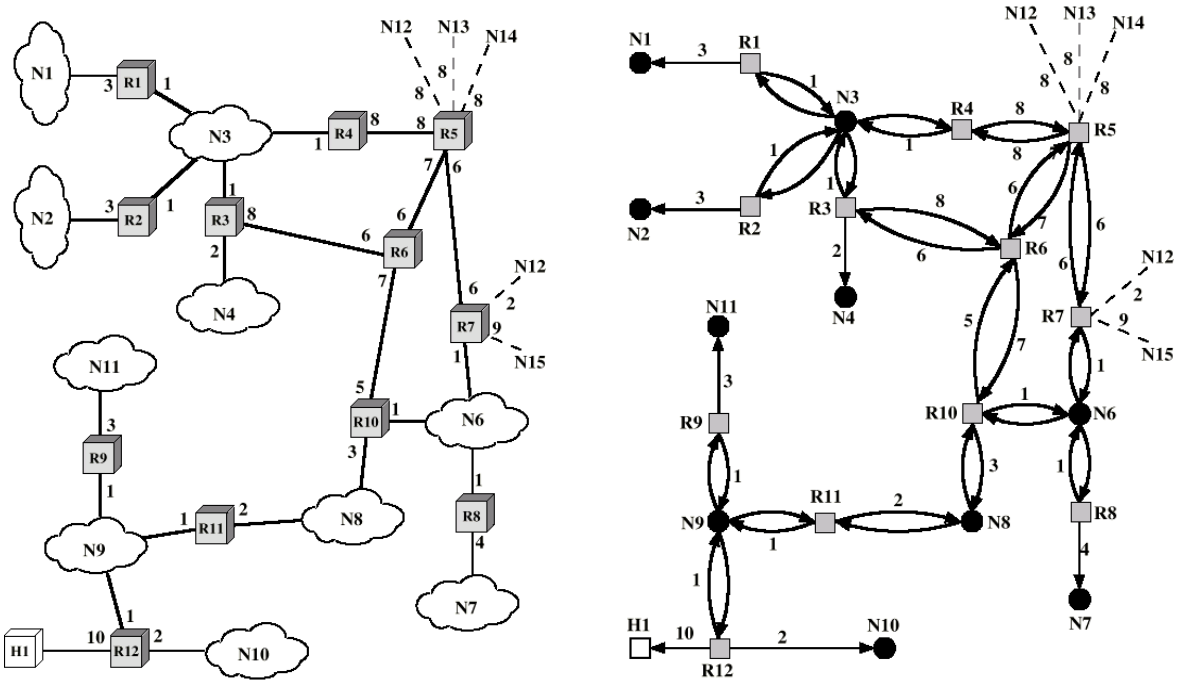
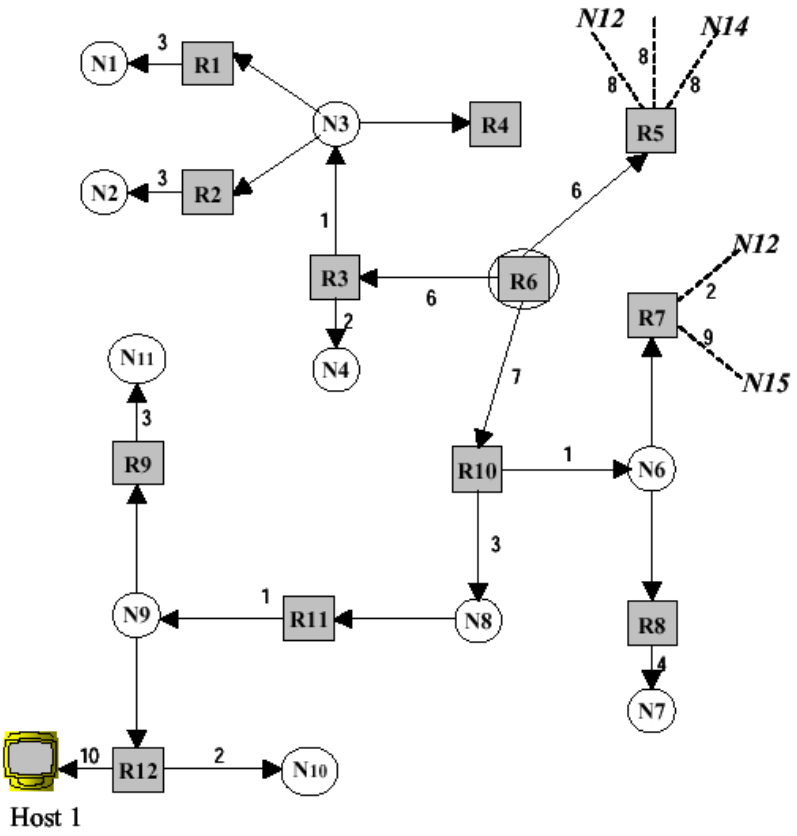



*Fig. 6.33*

Arbol OSPF para R6:




Arbol de expansión OSPF (Dijstra) en R6

*Fig. 6.34*

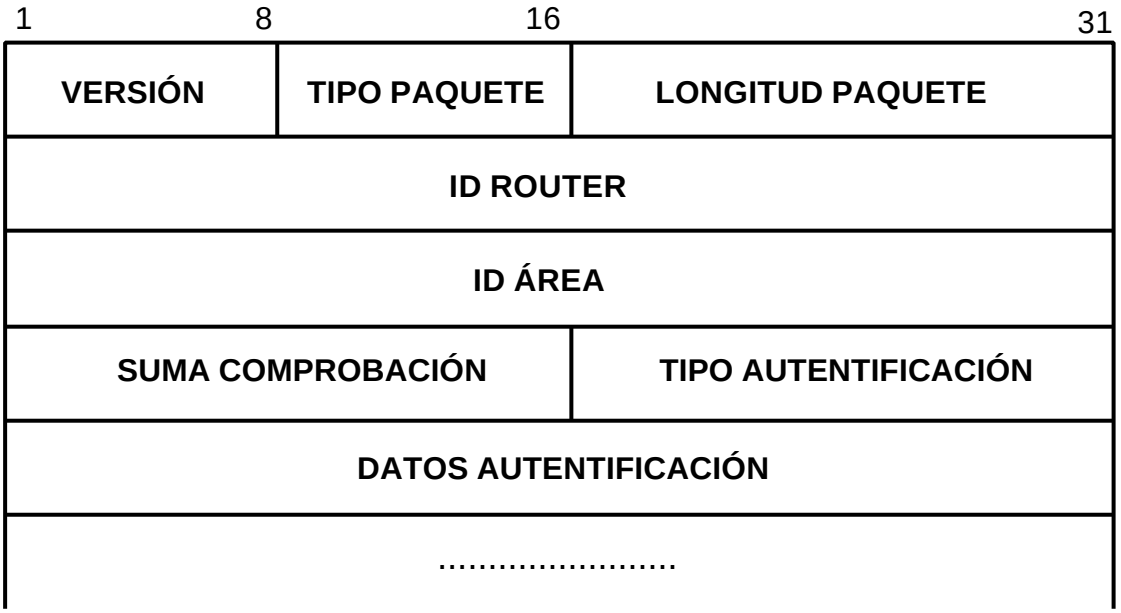
| Destino | Enrutador siguiente | Coste |
|---|---|---|
| N1 | R3 | 10 |
| N2 | R3 | 10 |
| N3 | R3 | 7 |
| N4 | R3 | 8 |
| N6 | R10 | 8 |
| N7 | R10 | 12 |
| N8 | R10 | 10 |
| N9 | R10 | 11 |
| N10 | R10 | 13 |
| N11 | R10 | 14 |
| N12 | R10 | 10 |
| N13 | R5 | 14 |
| N14 | R5 | 14 |
| N15 | R10 | 17 |
| H1 | R10 | 21 |
| RT5 | R5 | 6 |

Tabla de encaminamiento del router 6

*Fig. 6.35*

- Estructura jerárquica:
  - OSPF permite la división de un AS en áreas numeradas (un área es una red o grupo de redes contiguas). Cada AS tiene un área principal o backbone y todas las demas están unidas a ella mediante topología en estrella. Cada área actualizará un conjunto de tablas de sus routers.
  - Así, los cálculos de actualizaciones y de costes de rutas están limitados a un área.
  - OSPF distingue cuatro tipos de enrutadores:
    - Enrutadores internos: pertenecen a un área.
    - Enrutadores de borde de área: conectados a varias áreas. Tienen información de todas ellas.
    - Enrutadores de backbone. Aceptan información de enrutadores de borde de área, y la distribuyen a los mismos, por lo que su información llega finalmente a todos los routers.
    - Enrutadores frontera. Relacionan un AS con otro AS.

- Formato del paquete:




*Formato cabecera OSPF*

*Fig. 6.36*

- **Version:** versión del protocolo (2 en la actualidad).
- **Tipo de paquete:** tipo de paquete. Cada tipo de paquete lleva tras la cabecera un formato distinto.
  1 = hello (saludo). Para detectar cambios en los enlaces o routers vecinos.
  2 = DD, database description (descripción de la base de datos)
  3 = link state request (solicitud de información). Para detectar cambios en general
  4 = link state update (actualización de información)
  5 = link state acknowledment (reconocimiento de actualización). Paquetes de reconocimiento.

- **Longitud de paquete:** número de octetos del paquete.
- **Router ID:** dirección IP del enrutador emisor.
- **Area ID:** identificador del área a la que pertenece el paquete.
- **Checksum:** código de error (similar al utilizado en IP).
- **Tipo de autentificación:**
  0 = sin autentificación
  1 = con clave simple
  2-255 = actualmente indefinido
- **Datos de autentificación:** clave de 64 bits

o Comandos:
- Ip ospf cost "valor". Normalmente el coste en funció nde l ancho de banda del enlace se asigna:
  - $10^8$/BW (Ethernet 10Mbps, coste 10. T1 –1'5 Mbps, coste 64)
- router ospf (no router ospf)
- network "dirección de red" area "id area".

o Mas información interesante en http://www.cisco.com/warp/public/104/1.html

- **BGP**, Border Gateway Protocol (Protocolo de pasarela frontera). RFC 1771.

o Protocolo de encaminamiento exterior (ERP) estándar en Internet. Diseñado para intercambio de información entre pasarelas (dispositivos de encaminamiento entre sistemas autónomos, también "gateways") de AS's diferentes. Reemplaza al EGP.
o Funciona sobre el nivel TCP, por tanto el intercambio de información es confiable. Utiliza habitualmente el puerto 179 TCP.
o La vesión mas usada es BGP-4.
o Tiene cuatro tipos de mensajes:
- Open: establece relación de vecindad (router en la misma subred). Lleva además información del tiempo de vida del router emisor, por lo que este debe mandar paquetes Keepalive antes de la finalizacion de ese tiempo.
- Update: se usa para:
  - Transmitir información de una ruta y/o
  - Transmitir información de rutas a eliminar
- Keepalive: se usa para:
  - Confirmar mensaje de "open", y
  - Confirmar periódicamente relación de vecindad
- Notification: notifica condiciones de error

o Realiza tres procesos funcionales:
- Adquisición de vecino. Los vecinos son gateways de la misma subred. Los vecinos tiene que ponerse de acuerdo para intercambiar información de enrutamiento. Saber qué routers son vecinos, requiere configuración del gestor de red. Es posible que un vecino no esté interesado en establecer relación de vecindad por diversas causas. Funcionamiento:
  - R1 → Open → R2,  R1 ← Keepalive ← R2.
- Detección de vecino alcanzable. Sirve para mantener la relación. Se envian periódicamente mensajes de Keepalive.
- Detección de red alcanzable. Por medio de mensajes "Update", los dispositivos de encaminamiento (routers) pueden mantener una base de datos con información de las redes alcanzables y la ruta preferida hacia ellas.

- Formato de paquete. Recordar que están encapsulados en paquetes TCP.

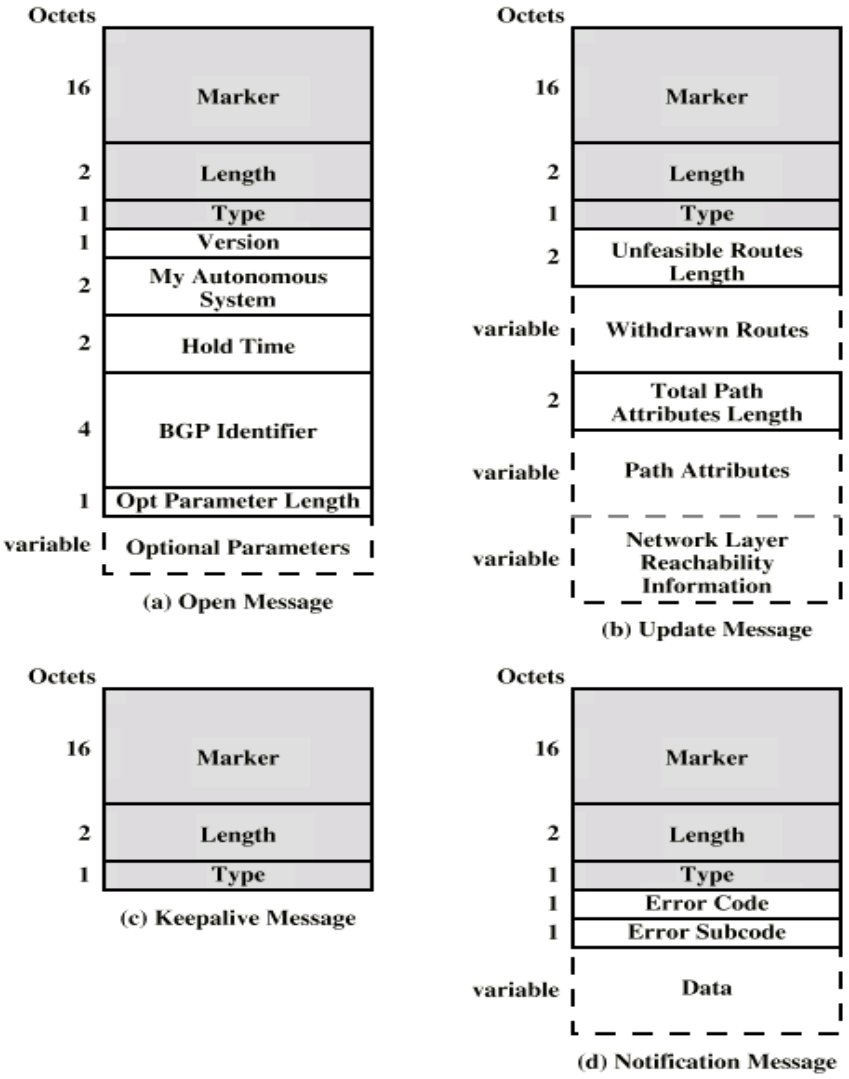



*Fig. 6.37*

- Formato de la cabecera:
  - **Marker:** el emisor puede insertar un valor de hasta 16 bytes en este campo. Este valor sería usado como parte de un mecanismo de autentificación que permita al destinatario verificar la identidad del emisor. En realidad, este campo se reserva (tanto en BGP como en otros protocolos que incorporan un campo similar) para el día en que se desarrolle un esquema de autentificación eficaz. Actualmente tiene todos sus bits asignados a uno.
  - **Length:** longitud en bytes del paquete, incluyendo la cabecera.
  - **Type:** tipo de paquete. Los cuatro posibles:
    - 1 = open
    - 2 = update
    - 3 = notification
    - 4 = keepalive

- Paquete Open:

  - **Version:** versión del protocolo, actualmente la 4.
  - **My autonomous system:** indica el numero de AS del emisor.
  - **Hold time:** tiempo que tiene que esperar el receptor antes de asumir que el emisor a caído. El emisor debe continuar emitiendo paquetes antes de que este tiempo se agote.
  - **BGP identifier:** dirección IP del emisor. BGP considera como identificador de cada enrutador su propia dirección IP.
  - **Authentification code:** define el sistema de autentificación empleado. En la actualidad este campo se asigna a cero.
  - **Authentification data:** datos destinados a la autentificación del paquete. La longitud y el contenido de este campo dependen del campo anterior. De momento este campo no se utiliza y tiene una longitud de cero bytes.

- Paquete Update

  - **Path attributes length:** longitud de rutas no factibles. Número de atributos de la ruta.
  - **Flags:** diversos bits que indican la opcionalidad, transitividad y parcialidad del atributo.
  - **Attribute type:** existen cinco tipos de atributos:
    - 1 = *origin*; el atributo ocupa 1 byte e indica si la información fue generada por un protocolo de encaminamiento interior (como OSPF) o por un protocolo de encami-namiento exterior (en particular, BGP).
    - 2 = *AS path*; el atributo es de longitud variable y enumera una lista de AS que atraviesa la ruta.
    - 3 = *next hop*; el atributo ocupa 4 bytes y proporciona la dirección IP del dispositivo de encaminamiento frontera que se debe usar para alcanzar los destinos indicados en el campo *network*.
    - 4 = *unreachable*; el atributo no ocupa lugar adicional.
    - 5 = *inter-AS metric*; el atributo ocupa 2 bytes

- Paquete Notification
  - **Error code:** para cada código de error existen diversos subcódigos que no se detallan:
    - 1 = cabecera corrupta. El tipo de paquete es inaceptable, bien por errores de sintaxis o por cuestiones de autentificación.
    - 2 = paquete *open* corrupto.
    - 3 = paquete *update* corrupto.
    - 4 = tiempo de *hold down* expirado.
    - 5 = Error en la máquina de estados finitos (errores de procedimiento).
    - 6 = Cese (cierre voluntario de una conexión).
  - **Data:** contiene el comando erroneo.

- Breve descripción de funcionamiento. Figura 6.38

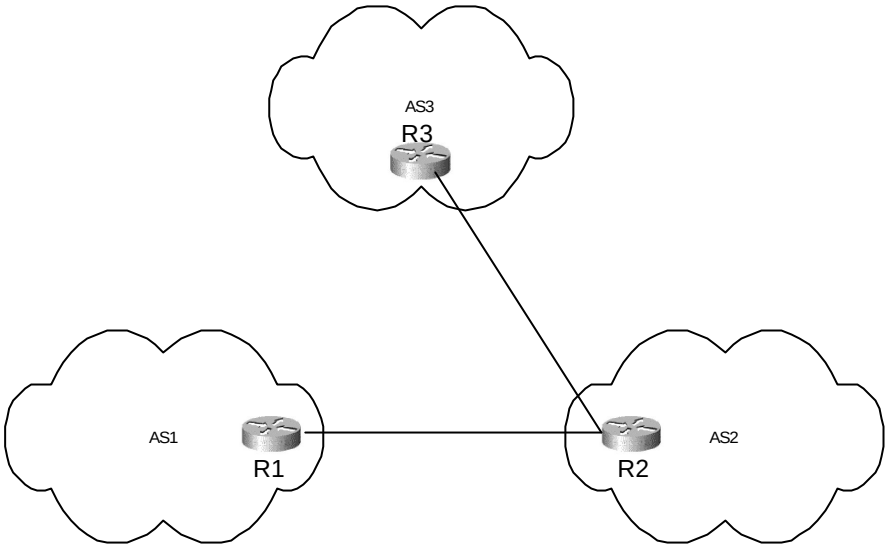



*Fig. 6.38*

  - Cada pasarela, implementa normalmente un IRP (RIP, OSPF) que le permite disponer de información sobre todas las rutas de su AS.
  - R1 envía un mensaje "Update" a R2 que incluye:
    - Camino_AS: Identificación de AS1
    - Siguiente_salto: dirección IP de R1
    - NLRI: lista de redes de AS1.

    Esto significa que se informa a R2 de todas las redes disponibles en AS1 y que hay que atravesar AS1 para llegar a ellas.
  - R2 envía la información recibida de R1 a R3 en un mensaje "Update" nuevo que incluye lo siguiente:
    - Camino_AS: Identificación de AS2 y AS1
    - Siguiente_salto: dirección IP de R2
    - NLRI: lista de redes de AS1.

    Este mensaje significa que se informa a R3 que todas las redes indicadas en NLRI se alcanzan via R2 y que atraviesan AS2 y AS1. Ahora R3 decide si estos caminos son aceptables según los criterios establecidos por sus gestores. Si es aceptable, R3 difundirá la información a sus vecinos.

- Seguridad:
  - BGP impone motivos políticos de implementación.
    - Un AS puede no querer transmitir paquetes en tránsito, es decir, con origen y destino en otro AS.
    - Sistema de tarificación, es decir, si se abonan cuotas económicas se permiten tránsitos de vecinos.
  - Impone además motivos de seguridad o económicos
    - Prohibición de tránsito a través de ciertos AS.
    - P.ej. No poner IRAK en una ruta que comience en el pentágono.
    - No transitar por Corea del Norte si hay otra ruta posible.
    - El tráfico con origen y destino SUN que no transite por AS de Microsoft.
  - Las políticas se configuran manualmente en cada router.

## 6.4. IPv6

- RFC 1752, 2460, 2373
- Motivación:
  - Evolución del IPv4.
  - Espacio de direcciones:
    - IPv4: $2^{32}$ (aprox 4000 millones)
    - IPv6: $2^{128}$ (aprox $6 * 10^{23}$ por metro$^2$ de superficie terrestre).
  - Mecanismo de opciones mejorado. No será necesario examinar ni procesar las opciones en el enrutamiento.
  - Mejora en el sistema multicast.
  - Mejora en la asignación de recursos

- Estructura y formato cabecera IPv6

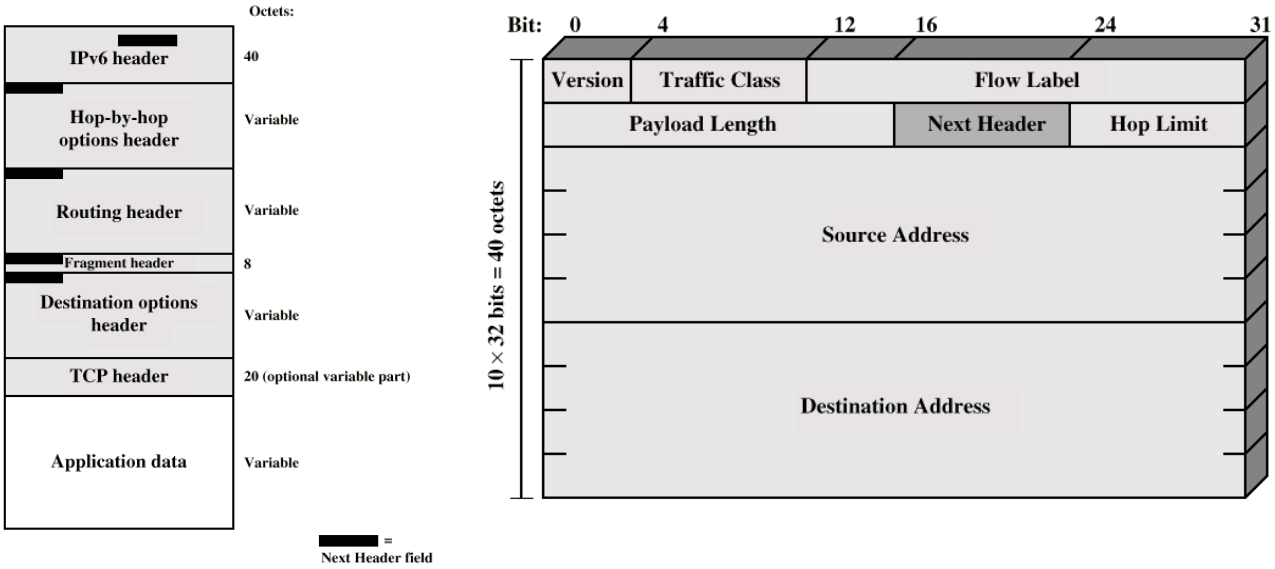



*Fig. 6.39*

  - cabecera de opciones salto a salto: opciones de procesamiento en cada salto
  - cabecera de encaminamiento: información de encaminamiento
  - cabecera de fragmentación: información de fragmentación y reensamblaje
  - cabecera de autentificación: información de error y autentificación
  - cabecera de seguridad: a definir
  - cabecera de opciones para el destino.

Cabecera IPv6
  - Versión (4 bits): valor 6
  - Clase de tráfico (8 bits): campo en estudio. Servirá para distinguir clases y prioridades de paquetes
  - Etiqueta de flujo (20 bits): para tratamiento especial dentro de la red.
  - Longitud de carga útil (16 bits): longitud de todas las cabeceras en octetos (salvo la principal) y la PDU de transporte.
  - Cabecera siguiente (8 bits): tipo de cabecera que sigue a la actual.
  - Límite de saltos (8 bits): El antiguo TTL de IPv4.
  - Dirección origen (128 bits)
  - Dirección destino (128 bits)



Bibliografía:

Stallings, comunicaciones y redes de computadores.
Charlie Scott, Virtual Private Networks.
http://ditec.um.es/laso/docs/tut-tcpip/
http://www.cisco.com