Escuela Politécnica Superior
Universidad de Huelva

TERCER CURSO. TECNOLOGÍA DE REDES

Tema 1:
Redes IP. Nivel de Red.
Protocolo IP

Manuel Sánchez Raya
Versión 0.1
5 de Febrero de 2004

ÍNDICE

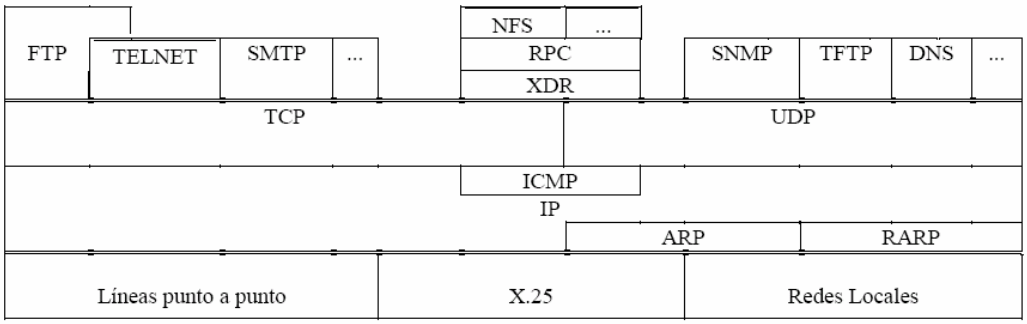
BIBLIOGRAFÍA

Apuntes año 2002-2003. Estefanía Cortés Ancos.
Apuntes Universidad de Oviedo. J.A.Sirgo, Rafael C. González
Academia de Networking de Cisco Systems. Guía del Primer Año.
Internetworking with TCP/IP. Vol. I. D.E. Comer.

1. Introducción. El protocolo TCP/IP.

La denominación TCP/IP recoge la descripción de una serie de protocolos, la topología y la arquitectura que sirven de base para una red de área extensa (WAN) como es el caso de Internet. Entre los protocolos descritos bajo esa denominación se encuentran el IP (*Internet Protocol*) y el TCP (*Transmision Control Protocol*) junto con varios más.

Todos ellos sirven de soporte a un conjunto de aplicaciones y servicios de aplicación, muy conocidos por su utilización en la red Internet. La descripción de todos los elementos que forman parte de la arquitectura TCP/IP y la mayor parte de las aplicaciones que hacen uso de ella, se encuentran recogidos como estándares "de facto" en los RFCs (*Request For Comments*). Se trata de documentos manejados por la comunidad de Internet donde se incluyen los protocolos y estándares de la red Internet, las propuestas de estándar, documentos puramente informativos, etc.

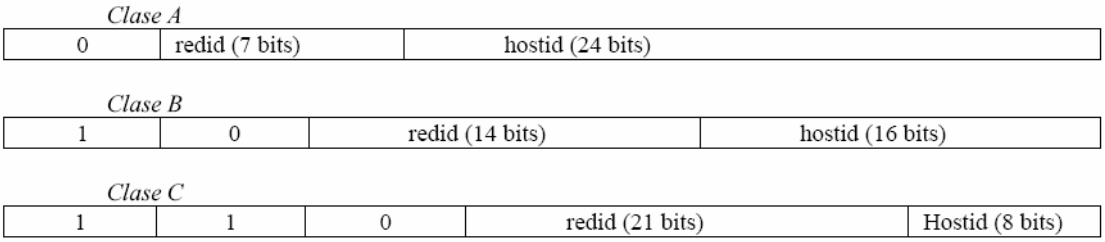


1.1.- Direcciones IP y encaminamiento mediante Routers.

Para hacer un sistema de comunicación universal, se necesita un método de identificar computadores aceptado globalmente. Cada computador tendrá su propio identificador, conocido como dirección IP o dirección Internet.

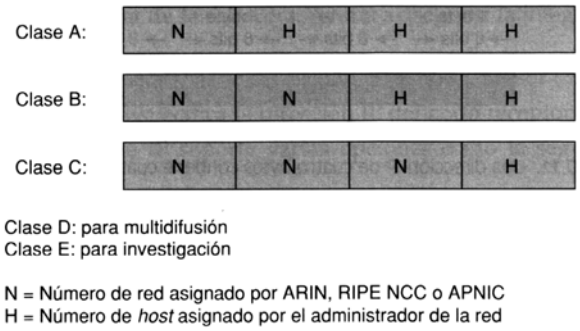
Puede pensarse en la red Internet como cualquier otra red física. La diferencia está en que la red Internet es una estructura virtual implementada enteramente en "software". Por tanto, los diseñadores fueron libres de escoger los tamaños y formatos de los paquetes, las direcciones, las técnicas de distribución de paquetes, etcétera. Para las direcciones, se escogió un sistema análogo al direccionamiento en redes físicas, en el cual a cada "host" se le asigna un número entero de 32 bits como identificador, llamado dirección internet. Estos enteros están cuidadosamente escogidos para hacer el proceso de *encaminamiento* o "routing" eficiente. Las direcciones internet codifican la identificación de la red a la que el "host" se encuentra conectado, así como la identificación de ese "host" dentro de la red. Por tanto, todos los computadores conectados a una misma red tienen en su número de dirección una serie de bits comunes (evidentemente, los bits de identificación de red).

Cada dirección internet es un par de identificadores (redid,hostid), donde *redid* identifica una red y *hostid* identifica a un computador dentro de esa red. En la práctica, hay tres clases distintas de direcciones (clases A,B y C), como se muestra en las figuras.



Dada una dirección IP, se puede determinar su clase a partir de los tres bits de orden alto, siendo sólo necesario dos bits para distinguir entre las clases primarias. Las direcciones de clase A se usan para computadores en redes que tienen más de 2^{16} estaciones o "hosts" (esto es, 65.636), utilizando 7 bits para *redid* y 24 bits para *hostid*. Las direcciones de clase B se usan para redes de tamaño intermedio, que tienen entre 2^8 (esto es, 256) y 216 "hosts", localizando 14 bits en *redid* y 16 bits en *hostid*. Finamente, las redes de clase C, que tienen menos de 2^8 "hosts", utilizan 21 bits para *redid* y solamente 8 bits para *hostid*.

La Clase D (multicast) utiliza 4 bits para redid (código 1110) y 28 bits para hostid, cubriendo las direcciones 224.0.0.0 a 239.255.255.255. La clase E (para uso futuro) utiliza 5 bits para redid (código 11110) y el resto de bits para hostid, cubriendo desde 240.0.0.0 a 247.255.255.255, son direcciones reservadas para uso futuro.



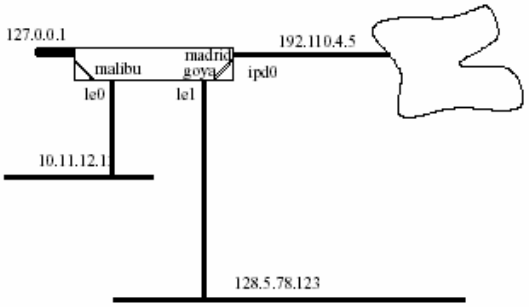
En cada red de clase A, B o C el administrador de la misma puede hacer uso de parte de los bits correspondiente al *hostid* para a su vez denominar distintas subredes dentro de su organización.

Los "routers" basan sus decisiones de encaminamiento en el *redid* del nodo destino, es decir en la red a la que van destinados los datos. Los "routers", por tanto, deciden dónde van a mandar los datos basándose en la red destino y no en el computador específico al que van destinados los datos, lo que disminuye las necesidades de memoria de los "routers" a medida que aumenta el número de estaciones conectadas a la red Internet.

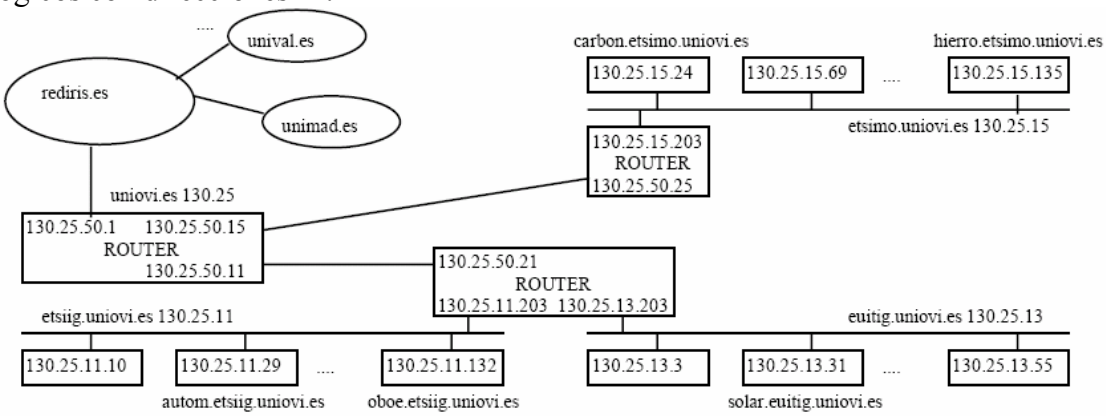
Sin embargo, siguiendo el criterio explicado hasta ahora no sería posible, por ejemplo, dar una dirección a un "router" que esté unido a dos redes, puesto que el *redid* de las dos redes no es el mismo. La solución a esto es asignar a este tipo de máquinas conectadas a más de una red, varias direcciones, una por cada red a que estén conectadas.
Las direcciones IP se representan como cuatro enteros decimales separados por puntos, donde cada entero da el valor de un octeto de la dirección. Así, por ejemplo, la dirección de 32 bits 10000000 00001010 00000010 00011110 se escribe 128.10.2.30.

Todas las direcciones IP en Internet son asignadas por una autoridad central, el *Centro de Información de Redes* (NIC, *Network Information Center*), localizado en los Estados Unidos de América. Esta autoridad central sólo asigna la parte de la dirección que identifica a la red, delegando la asignación de las direcciones de los "hosts" a la organización que ha formulado la petición de conexión a la red Internet.

Si no se pretende conectar una red a internet, la elección de las direcciones puede decidirla el administrador de la red. Aquellas máquinas conectadas a varias redes tendrán una dirección por cada interfaz de red. Es decir, con una dirección se identifica una conexión a la red.



Para que al usuario le resulte más cómodo recordar la identificación de los distintos "hosts" y dominios, se les dan nombres o alias. En algunos casos un nombre hace referencia a más de una dirección IP (generalmente varias direcciones de dominios) y en otras varios nombres (alias) hacen referencia a una misma dirección IP de "host" o de dominio. Esto obliga a que exista una base de datos en el "host" que relaccione nombres lógicos con direcciones IP.



Generalmente esta base de datos es un fichero de tipo texto que solo contiene unos pocos de los nombres existentes dentro de la red Internet. Sería inviable que cada "host" tuviese una base de datos completa y actualizada con todos los nombres y direcciones IP.

Si un "host" no tiene en su propia base de datos la identificación de un "host", consulta a un servidor DNS (*Domain Name Service*). Se trata de un "host" que mantiene la base de datos para uno o varios dominios y que da servicio de nombres a los ordenadores de ese dominio, que a su vez deben conocer cual o cuales son los servidores DNS que tienen más cercanos. Si el servidor DNS no contiene la identificación del "host" que le han solicitado, consulta a su vez a otros servidores DNS de la red Internet hasta encontrarlo.

1.1.1.- Direcciones de red y broadcast.

Se ha dicho que una de las ventajas de las direcciones IP es que codifican información sobre la red, con lo que se simplifica el encaminamiento. Otra ventaja es que una dirección IP puede referirse tanto a redes como a "hosts". Por convenio, *hostid* 0 no se asigna nunca a un computador, si no que una dirección IP con *hostid* igual a 0, se usa para referirse a la propia red.

Otra ventaja importante del direccionamiento *internet* es que soporta la dirección *broadcast*, que se refiere a todos los "hosts" conectados a la red. De acuerdo con el convenio, cualquier *hostid* con todos los bits valiendo 1 se reserva para *broadcast*. En muchas tecnologías de red (por ejemplo en la red Ethernet), la transmisión *broadcast* es tan eficiente como una transmisión normal; en otras redes se admiten las direcciones *broadcast*, aunque suponen un retraso considerable; otras redes no las admiten en absoluto. Por tanto, la existencia de direcciones *broadcast* no garantiza la eficacia de este tipo de transmisión.

De igual manera que un campo en la dirección IP con todos los bits 1 significaba "todos", el software IP interpreta un campo con todos los bits valiendo 0 como "éste". Así, una dirección con *hostid* igual a 0, se refiere a "ese" computador, y una dirección con *redid* igual a 0 se refiere a "esa" red. El uso de direcciones con *redid* igual a 0 es especialmente importante en aquellos casos en que un "host" quiere comunicarse sobre una red, pero todavía no sabe su dirección *internet*. El "host" utiliza temporalmente un *redid* igual a 0, y los otros computadores conectados a la red, interpretan esa dirección significando "esta" red. En la mayoría de los casos, las respuestas tendrán una dirección con el identificador de red especificado, permitiendo al "host" almacenarlo para futuros usos.

0.0.0.0	Este ordenador
00…0/ordenador	Un ordenador de esta red
255.255.255.255	Difusión en la red local
Red/111…1111111	Difusión en otra red
127/cualquier cosa	Loopback (Pruebas TCP/IP y comunicación entre procesos interno)
191.255.0.0	Reservada
128.0.0.0	Reservada
255.255.255.0	Reservada
240.0.0.0 – 255-255-255-254	Reservada
10.x.x.x	Reservada para redes privadas
172.16.x.x – 172.31.x.x	Reservada para redes privadas
192.168.x.x	Reservada para redes privadas

Nunca se asigna una dirección de host con todos sus dígitos a 1’s ó a 0’s. Las direcciones formadas por todos sus dígitos a “1” son de broadcast: el mensaje va destinado a todos los ordenadores de la red. Si lo que está a cero son los bits de red, se supone que es en la misma red, especificando sólo el número de ordenador: 0.0.0.9.

1.2.- Creación de Subredes.

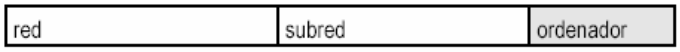
La división de los 32 bits entre red y ordenador ha provocado que el espacio de direcciones se llene.

Para paliar este problema se han desarrollado numerosas extensiones a IP. Dos de las más importantes son:

- Máscaras de subred
- Enrutamiento entre dominios sin clase (**CIDR**)

1.2.1.- Empleo de máscaras.

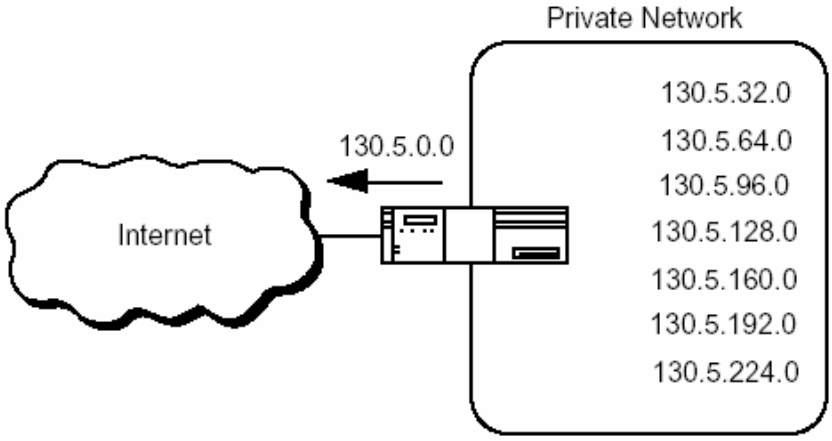
La jerarquía original de Internet de dos niveles (red, host) suponía que cada sitio sólo tendría una red, por lo que sólo necesitaría una única conexión a internet. Sin embargo, actualmente una organización puede contar con más de una red y tampoco tendría suficiente con una sola conexión a internet. La descomposición de una red en subredes permite descomponer la red en subredes de menor tamaño.



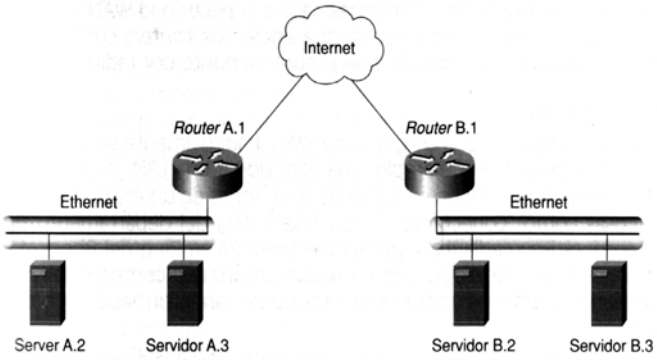
- Nº de subredes posibles (n bits para la subred):2 n -2
- Nº de equipos (m bits para los equipos): 2 m -2

De modo que las subredes serán redes físicas que comparten una misma dirección IP. Para diferenciar una de otra hay que hacer uso de máscaras de subred. Se define una máscara de red como una combinación de 32 unos y ceros, con los que se hace una operación AND con la dirección de 32 bits de algún equipo para obtener la dirección de subred. Por ejemplo:

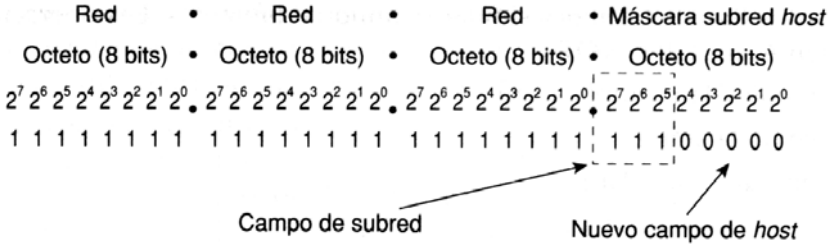
IP equipo, clase C: 148.206.250.2 Máscara: 255.255.255.0
El equipo está en la subred: 148.206.250.0



Esto reduce significativamente los requerimientos de enrutado de internet. La segmentación de redes permite manejar el crecimiento de las redes mediante un sistema de direccionamiento lógico para las subredes. La capa de red permite la comunicación entre redes separadas.

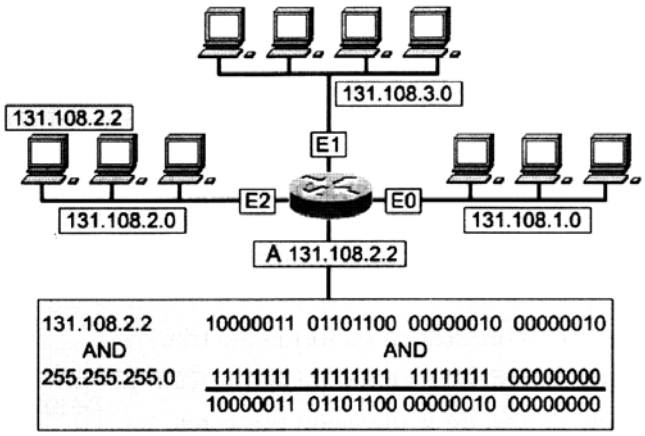


La capacidad de decidir como dividir la parte de host original genera el uso de subredes por parte del administrador de red. Se toman prestados bits de la parte de host original para la especificación de subred, como mínimo dos.

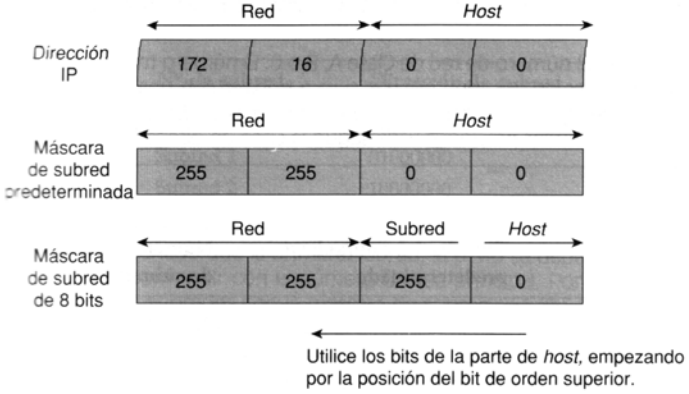


La Máscara de subred determina que parte de una dirección IP es el campo de red y cual el campo de host, tiene la misma longitud que una dirección IP.

La parte de host de la mascara tiene todos ceros, para enrutar los datos el router realiza un AND lógico para extraer la dirección de red.



Para crear subredes se amplia la parte de enrutamiento mediante la mascara de subred



Clase de dirección	Tamaño del campo *host* predeterminado	Número máximo de bits de subred
A	24	22
B	16	14
C	8	6

1.2.2.- CIDR. Enrutamiento interdominios sin clase.

Internet es víctima de su propio éxito. Las tablas de encaminamiento crecen. Las direcciones de la clase B son demasiado grandes, pero la mitad de ellas tienen solo 50 máquinas. Y las clase C parecen pequeñas para una organización entera. Las tablas ocupan memoria y gastan tiempo de CPU en los routers, y además hay que coordinarlas con las de otros routers.

Las direcciones de IPv4 se agotan y el tamaño de las tablas de enrutamiento se vuelve intratable. Como solución, se creó una modificación drástica de IPv4: **IPv6** que cuenta, entre otros aspectos, con un sistema de direcciones diferente.

Sin embargo, IPv6 es una solución a largo plazo, una solución apremiante fue **CIDR** (***Classless InterDomain Routing***) definido en la RFC 1519. El objetivo de CIDR es disminuir la velocidad de agotamiento de las direcciones restantes no asignadas. CIDR permite que los routers agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los routers principales. Con CIDR, un conjunto de redes IP aparece ante las redes ajenas al grupo como una entidad única de mayor tamaño.

Parte de esta solución consiste en eliminar las direcciones con clase:

Clase A: 8
Clase B: 16 } bits para host
Clase C: 24
Con CIDR: 192.125.61.8/20 (20 bits para host)

Ejemplo:
164.56.0.0/20 (clase B)
Máscara: 255.255.240.0
Los routers compatibles con CIDR miran el nº tras el "/" (BGP)

Además, reparte las redes clase C restantes (casi dos millones) en bloques consecutivos. Así el mundo se divide en 4 zonas:

194.0.0.0 a 195.255.255.255 Europa
198.0.0.0 a 199.255.255.255 Norteamérica
200.0.0.0 a 201.255.255.255 Centro y Sudamérica
202.0.0.0 a 203.255.255.255 Asia y Pacífico

Todo ello ayuda a disminuir considerablemente las tablas de encaminamiento.

1.3.- El protocolo ARP.

Se ha dicho anteriormente que una dirección IP era un número de 32 bits que se asignaba a las máquinas conectadas a la red para su identificación, y que esa identificación era suficiente para enviar y recibir paquetes. Sin embargo, las máquinas conectadas a una red física pueden comunicarse sólo si conocen sus respectivas direcciones físicas. Por tanto, cuando un "host" quiere comunicarse con otro, necesita "mapear" la dirección IP del destinatario en su correspondiente dirección física, si este se encuentra en la misma red física. Si el destinatario no esta el la misma red física, deberá "mapear" la dirección del encaminador o "router" que le permita enviar los datagramas IP fuera de la subred en la que se encuentra. De esto se encarga el protocolo ARP.

La idea del ARP (*Address Resolution Protocol*) es sencilla. Cuando un "host" A desea comunicarse con otro B, del que conoce su dirección IP (I_B), pero no su dirección física (F_B), envía un paquete especial con dirección destino *broadcast*, pidiendo al "host" que tiene como dirección IP I_B que responda con su dirección física F_B. Todos los "hosts" conectados a la red reciben el paquete ARP, pero sólo el "host" B, que es al que iba dirigida la pregunta, responde con otro paquete ARP, enviando su dirección física.

Así, una vez completado el intercambio de información mediante el protocolo ARP, el "host" conoce la dirección física del otro con el que quiere comunicarse, de manera que puede enviarle sucesivos paquetes a él directamente. La experiencia demuestra que merece la pena mantener una tabla dinámica en la memoria volátil con las direcciones IP y las correspondientes direcciones físicas de los computadores con los que se ha establecido comunicación más recientemente, ya que, normalmente, la comunicación requiere el envío de varios paquetes. Así, cuando un "host" quiere comunicarse con otro, antes de enviar un paquete ARP, busca en la memoria para ver si tiene su dirección física, con lo que se reducen costes de comunicación. Sin embargo, las entradas de la tabla se eliminan si no son utilizadas durante un cierto tiempo o cuando el computador se apaga. Se evitan así problemas de comunicación si alguno de los ordenadores registrados ha cambiado de dirección física por avería de su interfase de comunicaciones o cualquier otra eventualidad.

Cuando un paquete ARP viaja por la red de una máquina a otra, lo hace encapsulado en una trama del nivel de enlace, como en el ejemplo de la figura.

Preámbulo	Destino	Origen	Tipo	Mensaje ARP tratado como datos	CRC

Mensaje ARP encapsulado en una trama Ethernet

Para identificar que la trama está llevando un paquete ARP, el computador fuente, asigna un valor especial al campo de tipo en la cabecera del paquete. Cuando la trama llega al destino, el "host" examina el campo tipo para determinar qué contiene esa trama. En el caso de la red Ethernet los paquetes ARP tienen un campo de tipo de valor 0806h (valor en notación hexadecimal).

Al contrario que la mayoría de los protocolos, los datos en paquetes ARP no tienen un formato de encabezamiento fijo. El mensaje está diseñado para ser válido con una variedad de tecnologías de transmisión y de protocolos. El ejemplo de la figura muestra

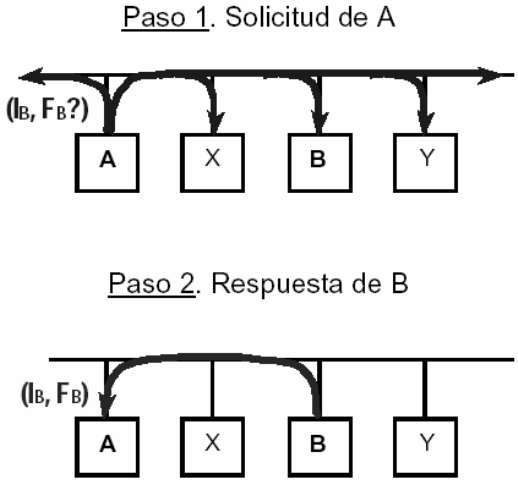
el mensaje ARP de 28 octetos usado para las redes Ethernet (en las que la dirección física tiene una longitud de 48 bits, 6 octetos) y protocolo de red IP (con dirección lógica de 32 bits, 4 octetos).

HARDWARE		PROTOCOLO
HLON	PLON	OPERACIÓN
DF ORIGEN (octetos 0-3)		
DF ORIGEN (octetos 4-5)		DL ORIGEN (octetos 0-1)
DL ORIGEN (octetos 2-3)		DF DESTINO (octetos 0-1)
DF DESTINO (octetos 2-5)		
DL DESTINO (octetos 0-4)		

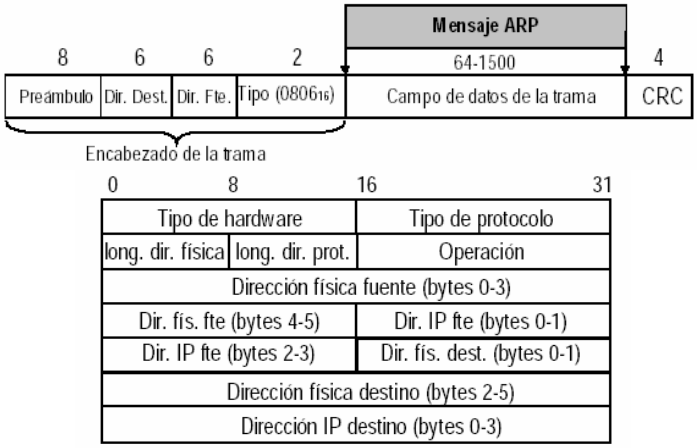
Formato del paquete ARP usado para redes Ethernet

A continuación se explica el significado de cada uno de los campos del paquete:

- **HARDWARE**: Especifica el tipo de interfase hardware para el que el computador fuente solicita la respuesta; el valor es 1 para la red Ethernet.
- **PROTOCOLO**: Contiene el número del protocolo al que corresponden las direcciones lógicas.
- **HLON y PLON**: Especifican, respectivamente, las longitudes de la dirección física y de la dirección de protocolo.
- **OPERACION**: Especifica el tipo de operación que realiza el mensaje: vale 1 para una petición ARP, 2 para una respuesta ARP, 3 para una petición RARP y 4 para una respuesta RARP. (El protocolo RARP se explicará a continuación).
- **DF ORIGEN:** Contiene la dirección física del "host" que realiza la petición ARP.
- **DL ORIGEN**: Contiene la dirección lógica (o de protocolo) del "host" que realiza la petición ARP.
- **DF DESTINO**: Es un campo vacío en una petición ARP y contiene la dirección física del "host" al que va destinada la petición en la respuesta.
- **DL DESTINO**: Contiene la dirección lógica del "host" al que va destinado la petición ARP.



El paquete ARP viaja encapsulado dentro de una trama física. Tiene el siguiente formato:



1.4.- Asignación de direcciones IP a Hosts.

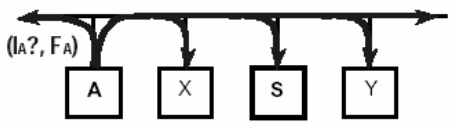
La asignación de direcciones puede ser:

- *Estática*.
- *Dinámica*. Diferentes métodos:
  - RARP
  - BOOTP
  - DHCP

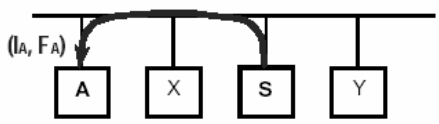
1.4.1.- RARP.

Las máquinas sin acceso a un tipo de almacenamiento secundario (por ejemplo, máquinas sin disco) conectadas a una red, no tienen posibilidad de guardar su dirección IP cuando se apagan. Por tanto, cuando estas máquinas se arrancan, tienen que usar la red para contactar con un servidor que les indique su dirección IP. El protocolo que usan las máquinas sin disco para obtener su dirección es el RARP (*Reverse Address Resolution Protocol*). Este protocolo está adaptado del ARP y usa su mismo formato de paquete. Al igual que el mensaje ARP, el mensaje RARP se transmite de una máquina a las otras encapsulado en una trama física. En el caso de redes Ethernet el campo de tipo de trama correspondiente a éste protocolo es el 0835h.

- Paso 1. Solicitud de A



- Paso 2. Respuesta de S



El uso del protocolo RARP es similar al del ARP: el "host" que quiere conocer su dirección IP envía un mensaje de petición RARP *broadcast*, con su dirección física en el campo de dirección física de destino (DF DESTINO). Todas las máquinas conectadas a la red reciben el mensaje, pero sólo aquellas autorizadas procesan la petición y contestan. Estas máquinas se conocen con el nombre de servidores RARP. Los servidores contestan rellenando el campo de dirección de lógica de destino (DL DESTINO), y cambiando el tipo de operación a "respuesta RARP".

Hay que tener en cuenta que comunicación entre "hosts" buscando su dirección IP y servidores RARP tiene que hacerse usando solamente la red física a que están conectados ambos, pues la única identificación que tienen los "hosts" es su dirección física para esa red concreta.

1.4.2.- BOOTP.

BOOTP (**Bootstrap Protocol**, RFC 951). A diferencia de ARP utiliza mensajes UDP encapsulados en datagramas IP. Un host usa BOOTP para enviar un datagrama IP al servidor o de difusión en caso de que no conozca la dirección del servidor.

El servidor BOOTP recibe la petición y envía una difusión como respuesta. El cliente recibe la respuesta y verifica la dirección MAC. Si encuentra su dirección MAC en al campo de dirección hardware del cliente, pone la dirección IP en el campo de dirección IP. Proporciona información adicional a máquinas sin disco como la dirección IP del servidor de archivos que contiene la imagen de la memoria, la dirección IP del router predeterminado y la máscara de subred. Permite crear un archivo de configuración que especifique los parámetros para cada dispositivo.

1.4.3.- DHCP.

DHCP (**Dinamic Hosts Configuration Protocol**) ha sido propuesto como sucesor de BOOTP con nuevos campos normalizados. También utiliza mensajes UDP encapsulados sobre IP.

A diferencia de BOOTP, DCHP permite al host obtener las direcciones IP rápida y dinámicamente. Sólo se necesita un rango definido de direcciones IP en el servidor DCHP. Cuando los hosts arrancan, contactan con el servidor DCHP y piden una dirección. El servidor DCHP selecciona una dirección y la asigna a ese host. Además de la dirección IP también puede enviarle la máscara de subred.

Permite asignar temporalmente una dirección y reutilizarla posteriormente para otro equipo.

2.- Protocolo IP.

El protocolo IP (*Internet Protocol*) define la unidad básica de transmisión de datos, y el formato exacto de todos los datos cuando viajan por una red TCP/IP. Además, el protocolo IP incluye una serie de reglas que especifican como procesar los paquetes y como manejar los errores.

El protocolo IP se basa en la idea de que los datos se transmiten con un mecanismo **no fiable** y **sin conexión**.

El decir un mecanismo no fiable quiere decir que un paquete puede perderse, duplicarse o enviarse a otro destino del deseado. El mecanismo es sin conexión porque cada paquete se trata independientemente de los otros. Paquetes de una secuencia enviados de una máquina a otra pueden ir por distintos caminos, a la vez que unos pueden alcanzar su destino mientras que otros no.

El protocolo IP define tres aspectos importantes:

- Define la unidad básica para la transferencia de datos: el **datagrama**
- Realiza la función de **encaminamiento de los paquetes** (o *routing*) seleccionando la ruta.
- Incluye conjunto de reglas sobre cómo **procesar los paquetes** y condiciones bajo las cuales pueden descartarse.

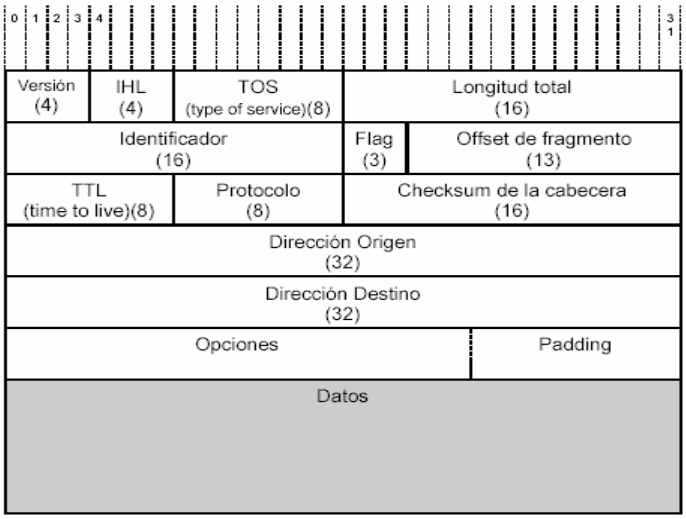
2.1.- Datagrama IP.

El datagrama es la unidad básica de transmisión de datos en la red Internet. El datagrama, al igual que las tramas en las redes físicas, se divide en encabezamiento y campo de datos. El encabezamiento contiene las direcciones IP de la fuente y el destino.

La longitud máxima de un datagrama es de 65.536 octetos (64 Kbytes). Sin embargo, para viajar de una máquina a otra, los datagramas lo hacen en el campo de datos de tramas de enlace, por lo tanto los datagramas de longitud excesiva deben ser divididos en fragmentos que "quepan" en las tramas.

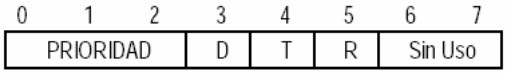
Cada fragmento perteneciente a un mismo datagrama tiene el mismo número de identificación que el datagrama original, con lo que es posible su reconstrucción.

El datagrama IP consta de un encabezado y un parte de datos. Su formato es el siguiente:



Los campos del datagrama son los siguientes:

- **Versión**: del protocolo IP (4)
- **IHL**: Longitud de la cabecera en palabras de 32 bits. Sin opciones: 20 octetos => 5. Máximo: 60 octetos =>15.
- **TOS**: Tipo de servicio (combinaciones de fiabilidad y velocidad). Ejemplo: voz digitalizada y transferencia de archivos. Su formato es el siguiente:



  Campo de precedencia: prioridad 0 (normal), prioridad 7 (paquete de control de red) Indicadores D, T y R: retardo, rendimiento y confiabilidad

- **Longitud total**: Número de octetos del datagrama completo (hasta 65535 bytes)

- **Identificador**: Todos los fragmentos de un datagrama contienen el mismo valor de indentificador.

- **Flags**: Un bit sin utilizar, DF (no fragmentar) y MF (a uno en el último fragmento)

- **Offset de fragmento**: Indica en qué parte del datagrama real va este fragmento

- **TTL:** Tiempo de vida. Número de saltos permitidos. Así se evita que datagramas perdidos viajen por la red indefinidamente. Es difícil estimar el tiempo exacto porque los "routers" normalmente no saben el tiempo que requieren para la transmisión las redes físicas. Para simplificar, "host" y "routers" suponen que cada red utiliza una unidad de tiempo en la transmisión; así deben decrementar el valor de este campo en uno cada vez que procesen un encabezamiento de datagrama. Si el valor del campo llega a cero el datagrama se destruye y se devuelve un mensaje de error ICMP.

- **Protocolo**: Indica la capa de transporte a la que debe ser entregado. Es un número que identifica cada uno de los protocolos posibles en /etc/protocols:

```
# Internet (IP) protocols
ip      0       IP # internet protocol, pseudo protocol number
icmp 1          ICMP # internet control message protocol
ggp     3       GGP # gateway-gateway protocol
tcp     6       TCP # transmission control protocol
egp     8       EGP # exterior gateway protocol
pup     12      PUP # PARC universal packet protocol
udp     17      UDP # user datagram protocol
hmp     20      HMP # host monitoring protocol
rdp     27      RDP # "reliable datagram" protocol
```

- **Checksum**: Asegura que el encabezamiento no tiene errores. El "checksum" se forma tratando el encabezamiento como una secuencia de enteros de 16 bits. Se suma con aritmética de complemento a uno, el complemento a uno de todos ellos. A efectos de calcular el "checksum" se supone que el campo CHECKSUM DEL ENCABEZAMIENTO tiene valor cero. Como sólo se chequean errores en el encabezamiento, los protocolos de nivel superior deberán añadir otro tipo de comprobación para detectar errores en los datos.

- **Dirección IP origen y destino:** Número de red y número de ordenador

- **Opciones:** No es un campo necesario en todos los datagramas. Se incluyen normalmente para chequear o depurar la red. La longitud de las opciones varía dependiendo de cuáles de éstas se seleccionan. Algunas opciones son de longitud un octeto, mientras que otras son de longitud variable. Cada opción consiste en un octeto de código de opción, un octeto de longitud y una serie de octetos para la opción. El código de opción se divide en tres campos, como aparece en la figura.

COPIA (1 bit)	CLASE DE OPCION(2 bits)	NUMERO DE OPCION(5 bits)

Cuando el bit COPIA está a 1, especifica que la opción sólo debe ser copiada al primer fragmento, y no a los demás. Los campos CLASE DE OPCION y NUMERO DE OPCION, especifican la clase general de la opción y dan la opción específica dentro de esa clase. En la tabla siguiente se muestra la asignación de las clases.

Clase de opción	Significado
0	Control de datagrama o red
1	Reservado para futuro uso
2	Depuración y medida
3	Reservado para futuro uso

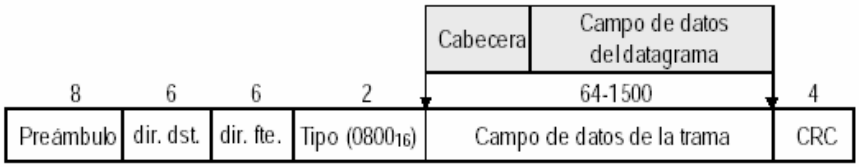
La tabla siguiente muestra las posibles opciones que pueden acompañar a un datagrama y da su clase y número de opción. La mayoría de ellas se usan para propósitos de control.

Clase de opción	Número de opción	Longitud	Descripción
0	0	1	Fin de lista de opción. Usado si las opciones no acaban al final del datagrama.
0	1	1	No operación.
0	2	11	Restricciones de seguridad y manejo.
0	3	variable	Encaminamiento fuente impreciso. Usado para encaminar un datagrama a lo largo de un camino fijado.
0	7	variable	Grabar ruta. Usado para localizar el camino seguido.
0	8	4	Secuencia identificadora. Usado para llevar una secuencia SATNET identificadora.
0	9	variable	Encaminamiento fuente estricto. Usado para encaminar un datagrama por una vía determinada.
2	4	variable	Tiempos Internet. Usado para grabar tiempos durante la ruta.

- **Relleno (padding):** Grupo de bits a cero que hace que la cabecea sea un múltiplo exacto de 32 bits.

- **DATOS**: Es la zona de datos del datagrama.

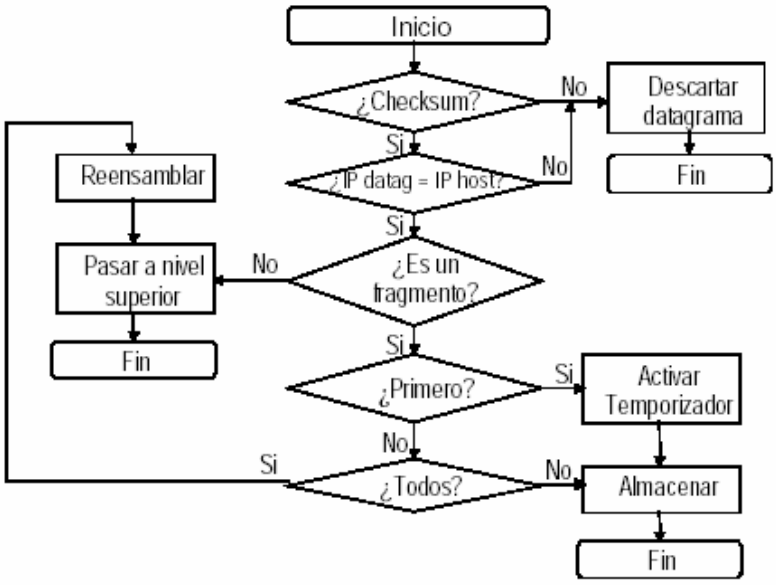
Cada datagrama será encapsulado en el campo de datos de las tramas de la red física y viajará con las direcciones de las máquinas origen y destino. Por ejemplo, para el caso de Ethernet:



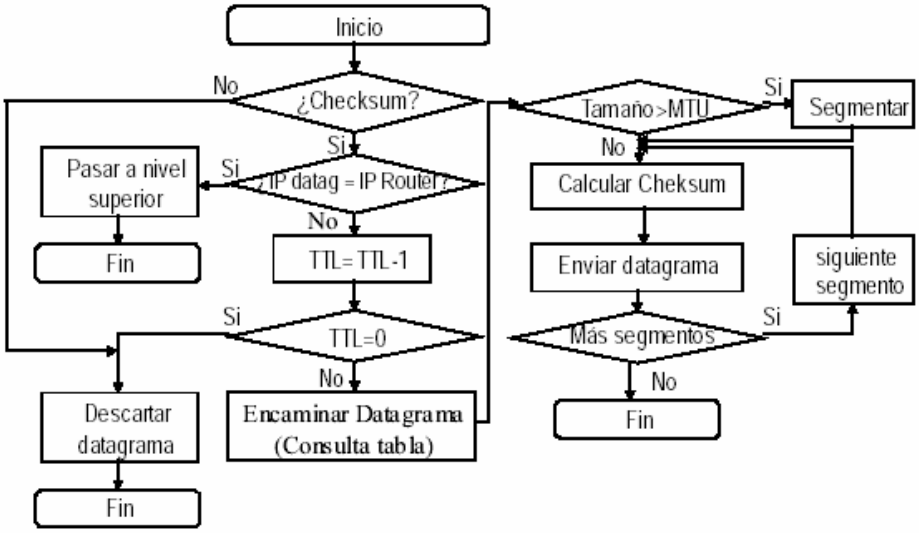
El camino seguido por cada datagrama puede ser diferente en función del tráfico de los enlaces (la comunicación es extremo a extremo). Los datagramas pueden perderse, llegar en un orden diferente al de envío, llegar duplicados... Incluso por el camino pueden haber sido troceados.

2.2.- Manejo de datagramas.

En un host:



En un router

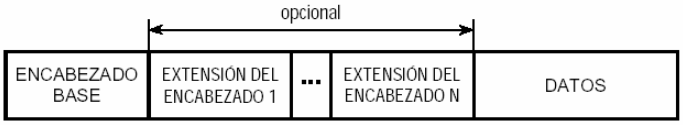


2.3.- La nueva versión del protocolo IP: IPv6.

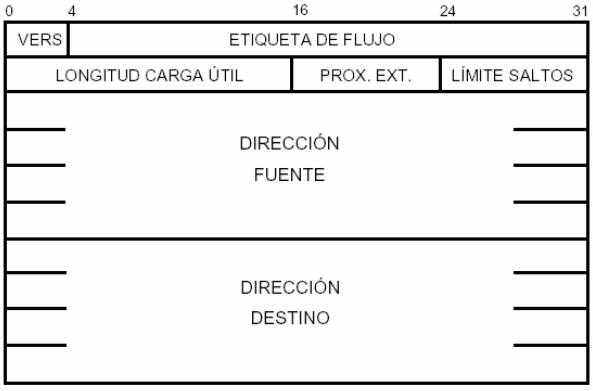
En un futuro próximo, la actual versión del protocolo IP (la versión cuatro, IPv4) será sustituida por una nueva versión, la seis, con el denominado IPv6 o IPng (*IP new generation*). El principal motivo es la ampliación del campo de direcciones IP que pasará ahora de 32 a 128 bits. Con 2^{32} direcciones, es decir, aproximadamente 4000 millones, debería ser suficiente, pero la ineficaz distribución de direcciones en subredes provoca que se desaprovechen la mayor parte de ellas. Las mejoras del IPv6 incluyen los siguientes aspectos:

- Espacio de direcciones ampliado: 128 bits.
- Notación hexadecimal con dos puntos.
- Mecanismo de opciones mejorado: Las opciones van en cabeceras opcionales separadas a partir de la principal. Hay hasta ocho tipos diferentes que sólo se incluyen y/o procesan cuando son necesarias.
- Direcciones de autoconfiguración: Permiten la asignación dinámica de direcciones.
- Mayor flexibilidad en el direccionamiento.
- Facilidad de asignación de recursos al tráfico de alta prioridad: Desaparece el campo de TIPO DE SERVICIO y se incluye uno de PRIORIDAD que clasifica el tráfico en función de sus necesidades especiales como el vídeo en tiempo real.
- Capacidades de seguridad: Incluyen la autentificación y la privacidad de los datos.

La cabecera del IPv6 pasa a tener 40 en lugar de 60 bytes, sin embargo es más simple y el número de campos que incluye es menor.



Opciones mejoradas: campos que antes eran obligatorios, ahora son opcionales. El formato del datagrama es el siguiente:



La alineación se realiza ahora en base a 64 bytes en lugar de 32. Las direcciones origen y destino se incrementan en 16 bytes cada una. La información acerca de la fragmentación viene reflejada en las extensiones del encabezado. El campo "tipo de servicio" es sustituido por el de "próxima extensión".

3.- Direccionamiento privado. NAT.

Ciertas direcciones de cada clase de direcciones IP no se asignan. Se conocen como: **direcciones privadas:**

- Clase A: 10.0.0.0 – 10.255.255.255
- Clase B: 172.16.0.0 – 172.16.255.255
- Clase C: 192.168.0.0 – 192.168.255.255

Las direcciones privadas pueden ser utilizadas por todos los hosts que empleen la conversión de direcciones de red NAT (Network Address Traslation), por hosts que no se conecten a internet o junto con un servidor de conversión de direcciones de red (NAT).

La conversión de direcciones de red NAT (RFC 1631) consiste en el proceso de cambiar una dirección por otra en la cabecera IP del datagrama para permitir que los hosts direccionados de forma privada accedan a internet (por acuerdo, cualquier tráfico con una dirección de destino dentro de uno de los rangos de direcciones privadas no se enrutará en internet).

Un dispositivo habilitado con NAT opera dentro de un dominio de colisión único. Cuando un host dentro de ese dominio de colisión quiere transmitir a un host exterior, envía el paquete al servidor NAT:

- El proceso NAT entonces mira la cabecera IP y, si es necesario, sustituye la dirección IP local por una dirección IP globalmente única.

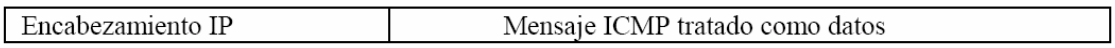
- Cuando un host exterior envía una respuesta, el proceso NAT lo recibe, comprueba la tabla de conversiones de direcciones de red y sustituye la dirección de destino por la original dirección de destino interna.

NAT es una ayuda para las organizaciones que crecen más que su espacio de direcciones o frente a un cambio de proveedor ISP, para evitar tener que direccionar todos los hosts.

4. Protocolo ICMP: Mensajes de error y control.

Se ha visto que el protocolo IP proporciona un servicio no fiable y sin conexión; y que los mensajes viajan de "router" en "router" hasta alcanzar el nodo destino. El sistema funciona bien si todas las máquinas trabajan adecuadamente y los "routers" están de acuerdo en los encaminamientos. En caso contrario ocurren errores. Para permitir a las máquinas en la red Internet informar sobre errores o circunstancias inesperadas está el protocolo ICMP (*Internet Control Message Protocol*), que es considerado como una parte del protocolo IP.

Los mensajes ICMP viajan en la porción de datos de los datagramas IP, como se muestra en la figura:



Los datagramas que llevan mensajes ICMP, se encaminan como los demás, por lo que pueden producirse errores. El protocolo dice que en este caso se produce una excepción, y especifica que no se deben generar mensajes ICMP sobre errores resultantes de datagramas llevando mensajes ICMP. Los mensajes ICMP facilitan también el control de congestión.

Aunque cada tipo de mensaje ICMP tiene su propio formato, todos empiezan con los mismos tres campos: Un entero de 8 bits indicando TIPO. Un campo de 8 bits, (CODIGO) dando más información sobre el tipo de mensaje y un campo de 16 bits con el "checksum" (se usa el mismo algoritmo que para los datagramas IP, pero incluye sólo el mensaje ICMP). Además, los mensajes ICMP incluyen el encabezamiento del datagrama IP que causó el problema, así como los primeros 64 bits de datos, para ayudar a determinar qué protocolo y qué programa de aplicación causaron el problema. El campo TIPO define el tipo del mensaje ICMP y el formato del resto del paquete. Los tipos son:

Campo TIPO	Tipo de mensaje ICMP
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de flujo de la fuente
5	Redireccionar (cambiar la ruta)
8	Petición de eco
11	Tiempo excedido por el datagrama
12	Problema de parámetro en un datagrama
13	Petición de grabar tiempos
14	Respuesta de grabar tiempos
15	Petición de información
16	Respuesta de información
17	Petición de máscara de direcciones
18	Respuesta de máscara de direcciones

5.- Tuneling

El tunneling está de moda por cuestiones de seguridad. Consiste en la colocación de cada paquete de información dentro de un paquete que hace de "envoltorio".

El protocolo del paquete que hace de envoltorio sólo es conocido por el emisor y el receptor. Esto es muy importante para las VPN's (Redes Privadas). Este proceso es transparente para los usuarios que utilizan estos routers. Por ejemplo, en accesos de un usuario a una oficina, es muy habitual encontrarse con el protocolo PPP, que forma parte de TCP/IP.

5.1.- Líneas punto a punto: PPP

PPP (Point to Point Protocol) es estándar Internet: RFCs 1171 y 1172. Es robusto y tiene 3 capas:

- LCP. Link Control Protocol: establecimiento, control de la calidad del enlace, negociación de la compresión y autenticación.

- NCP. Network Control Protocol: configuración y control, negociando opciones de nivel 3 (direcciones...).

- DLLP. Data Link Layer Protocol: Soporta enlaces asíncronos de 8 bits sin paridad o enlaces síncronos orientados a bit. El campo "protocolo" permite llevar tráfico de múltiples protocolos de red, no solo IP: Así 0x0021 es IP, 0xc012 LCP, 0x8021 NCP... Las tramas se delimitan sin ambigüedades. Existe detección de errores.

6.- Encaminamiento.

Encaminamiento es el proceso de selección de un camino sobre el que se mandarán los datagramas. El encargado de realizar la tarea de encaminamiento en la red es el router.

Los routers son nodos de red activos e inteligentes, pasa paquetes de datos entre redes basándose en las direcciones IP y tiene la capacidad para elegir la mejor ruta para la entrega de datos en la red. No solo la capacidad del hardware (número de paquetes conmutados por segundo) o el número de salidas LAN y WAN de que dispongan, distinguen a unos routers de otros. El software que incorporan es lo que las diferencia (la flexibilidad para usar máscaras, versiones mejoradas de los algoritmos de encaminamiento, filtrado...). Hay routers multiprotocolo, que encaminan tráfico IP y de otros tipos.

Un router cuenta con varios interfaces de red. Conectando dos o más redes, cada una de ellas ha de tener un número de red único para que el enrutamiento tenga éxito. Reenvía los datagramas que recibe por uno de ellos cuando la dirección destino se corresponde a

la dirección de red de otro interfaz o tiene un camino definido a través de otro router directamente accesible para él. Siempre ha de ser directamente accesible.

La información necesaria para el encaminamiento se almacena en tablas, presentes tanto en hosts como en routers, en las que se almacenan prefijos de red para dirigir datagramas hacia su destino. El datagrama no se ve alterado, ya que las direcciones IP origen y destino son siempre las mismas. Se encapsula a nivel 2 con direcciones origen y destino completamente nuevas. Sólo hay modificaciones importantes cuando hay que fragmentar. También puede darse que TTL valga 0 y se descarte el reenvío.

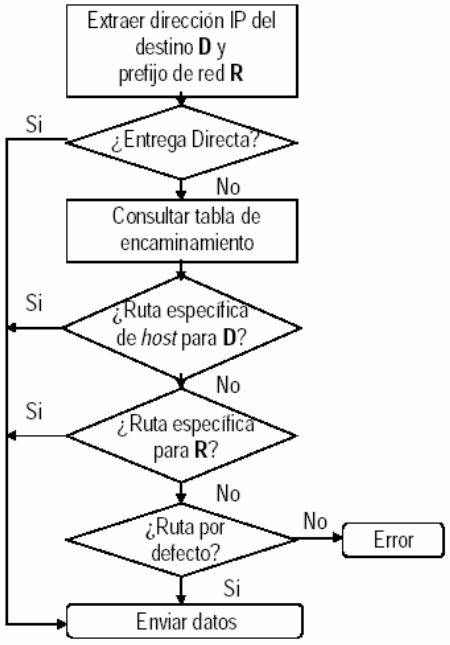
Para que haya comunicación entre dos máquinas, deben estar configurados los caminos de ida en ambos sentidos y en todos los tramos, ya que los protocolos de nivel superior necesitan contestaciones cuando menos. Si los enlaces de salida de un router están congestionados, cuando las colas de entrada se llenen los datagramas se irán descartando sin más.

Toda máquina guarda unos caminos definidos. Una entrada a la tabla suele ser un par (**dir. IP red destino**, **dir. IP siguiente destino en el camino a la red destino**). Otros tipos de entrada son:

- *Rutas por defecto*: Para aquellos casos en los que la red destino no aparezca explícitamente en la tabla.
- *Ruta específica:* Responde a propósitos de control y seguridad.

6.1.- Algoritmos.

Si una máquina quiere enviar un datagrama, el software IP determina la dirección del destino y extrae su porción de red. La porción de red se utiliza para tomar una decisión de encaminamiento, seleccionando un *encaminador* que se pueda alcanzar directamente. El algoritmo es el siguiente:



Ejemplo:

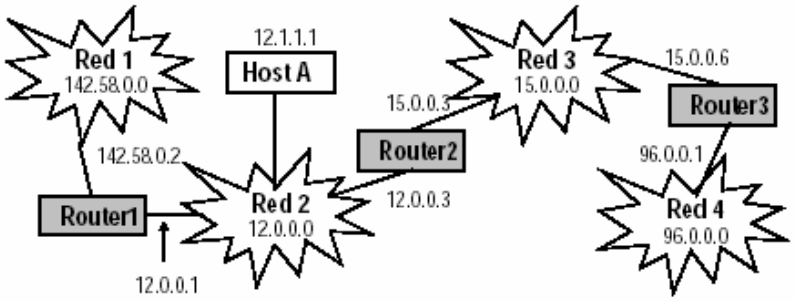


Tabla de encaminamiento del host A

destino	*ruta*
12.0.0.0	Entrega directa
142.58.0.0	12.0.0.1
defecto	12.0.0.3

Tabla de encaminamiento del Router2

destino	*ruta*
15.0.0.0	Entrega directa
12.0.0.0	Entrega directa
142.58.0.0	12.0.0.1
96.0.0.0	15.0.0.6

En el caso de empleo de direccionamiento de subredes, se debe guardar información adicional en la tabla de encaminamiento. Cada entrada estará formada por tres elementos: *Máscara de subred*, *dirección de red*, *salto siguiente.*

Ahora, el algoritmo de encaminamiento será:

1. Extraer la dirección IP destino D y su prefijo de red R.
2. Si es entrega directa (¿esta máquina y el destino están en la misma red?), enviar datos y FIN.
3. Si no, para cada entrada de la tabla (M, R, S) hacer:
    a. N=D and M
        i. Si N=R, encaminar el datagrama hacia S y FIN
        ii. Si no ERROR (descartar envío).
4. La ruta específica se especificaría con un máscara todo a 1's y con dirección de red R igual a la del host.
5. La ruta por defecto se implementa estableciendo M=R= todos 0's.

6.2.- Protocolos

Un sistema autónomo es un conjunto de redes conectado por dispositivos de encaminamiento homogéneos. Existen *protocolos de encaminamiento internos* y *externos*. Los primeros comunican dispositivos encaminadores dentro de un sistema autónomo y los segundos comunican enccaminadores situados en diferentes sistemas autónomos.

6.2.1.- Internos

Aplicados dentro de un sistema autónomo para optimizar rutas. Son los siguientes:

- **RIP** (*Routing Information Protocol*) es el original en Internet, basado en vector de distancia, y funciona bien en sistemas pequeños (converge lentamente). Los mensajes van sobre UDP, y hay una versión (RIPv2) que añade autenticación, multicast. Cada dispositivo de encaminamiento ha de transmitir su tabla de encaminamiento completa.

- **IS-IS** (*Intermediate System - Intermediate System*) es un protocolo de estado del enlace. Cada dispositivo de encaminamiento mantiene información acerca del estado de sus enlaces locales a subredes. Periódicamente envía esta información actualizada a todos los dispositivos de encaminamiento que conoce.

- **OSPF** (*Open Shortest Path First, RFC 1247*). Parecido a IS-IS, las tablas se difunden sobre UDP por inundación, sólo a routers adyacentes. Calcula una ruta a través del conjunto de redes que suponga el menor coste de acuerdo a una métrica configurable por el usuario. Soporta encaminamiento basado en función del retardo, tipo de servicio, y múltiples métricas.

6.2.2.- Externos.

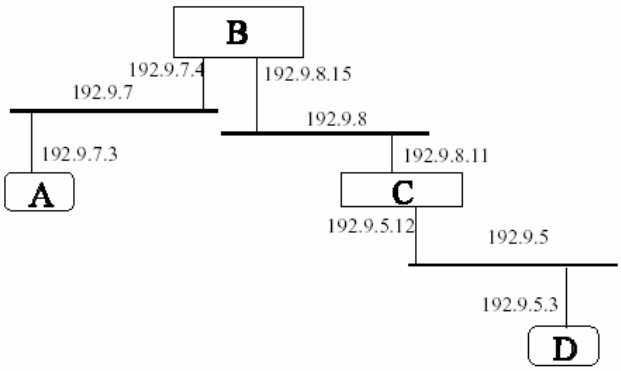
Aplicados entre sistemas autónomos. Son los siguientes:

BGP (Border Gateway Protocol. Es un protocolo de vector de distancia pero en lugar del coste enumera las rutas a cada destino. Opera en términos de mensajes que se envían utilizando conexiones TCP.

Tres procedimientos funcionales:

- Adquisición de vecino
- Detección de vecino alcanzable (periódicamente)
- Detección de red alcanzable (si cambio en base de datos con las subredes que se pueden alcanzar y la ruta preferida)

6.3.- Ejemplos de tablas de enrutado.



A a D

A:	192.9.7	192.9.7.4	0
	192.9.5	192.9.7.4	2
	192.9.8	192.9.7.4	1
B:	192.9.8	192.9.8.15	0
	192.9.5	192.9.8.11	1
C:	192.9.5	192.9.5.12	0

D a A

D:	192.9.7	192.9.5.12	2
C:	192.9.7	192.9.8.15	1
B:	192.9.7	192.9.7.4	0

6.4.- Ejemplo de utilización de ARP