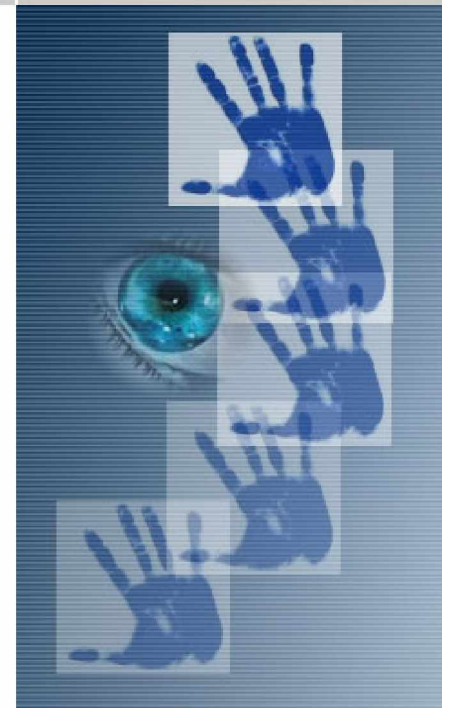


*Universidad Nacional de Ingeniería  
Facultad de Ingeniería Industrial y de Sistemas  
Instituto de Investigación*

**CSIRT-UNI**

# Protocolos TCP/IP

*Lic. José Zamora Ramírez*



*Apuntes del curso Máquinas de Computación  
Editada y publicada con permiso del Autor.*

# PROTOSCOLOS TCP/IP

Lic. José Zamora Ramírez

Edición:

Carlos Lazarte Chavez

César Orosco Pacora

Universidad Nacional de Ingeniería

Faculta de Ingeniería Industrial y de Sistemas.

Instituto de Investigación.

**CSIRT – UNI**

Equipo de Respuesta a Incidentes de Seguridad Informática - UNI

<http://www.csirtuni.org/>

# Índice

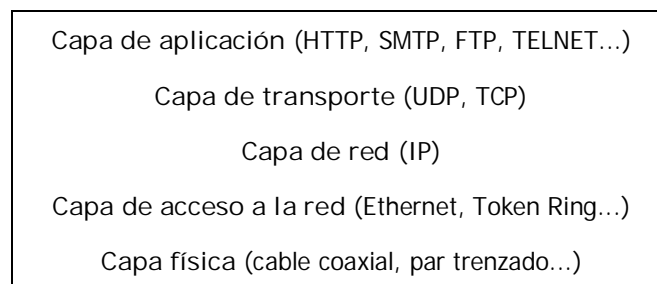
Capítulo 1 Introducción.....	4
Capítulo 2 Capa de red.....	6
2.1 Direcciones IP.....	7
2.2 Direcciones IP especiales y reservadas.....	9
2.3 Máscara de subred.....	12
2.4 Protocolo IP .....	15
2.5 Formato del datagrama IP .....	16
2.6 Fragmentación.....	17
2.7 Protocolo ARP .....	18
2.7.1 Tabla ARP (caché ARP).....	19
2.8 Protocolo ICMP .....	20
2.8.1 Solicitud y respuesta de eco .....	21

# Capítulo 1

## Introducción

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí. Internet no es dependiente de la máquina ni del sistema operativo utilizado. De esta manera, podemos transmitir información entre un servidor Unix y un ordenador que utilice Windows 98. O entre plataformas completamente distintas como Macintosh, Alpha o Intel. Es más: entre una máquina y otra generalmente existirán redes distintas: redes Ethernet, redes Token Ring e incluso enlaces vía satélite. Como vemos, está claro que no podemos utilizar ningún protocolo que dependa de una arquitectura en particular. Lo que estamos buscando es un método de interconexión general que sea válido para cualquier plataforma, sistema operativo y tipo de red. La familia de protocolos que se eligieron para permitir que Internet sea una Red de redes es TCP/IP. Nótese aquí que hablamos de familia de protocolos ya que son muchos los protocolos que la integran, aunque en ocasiones para simplificar hablemos sencillamente del protocolo TCP/IP.

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico...) particulares de cada sistema operativo. Todo esto nos sugiere el siguiente modelo de referencia:



El nivel más bajo es la capa física. Aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

La capa de acceso a la red determina la manera en que las estaciones (ordenadores) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

Las dos capas anteriores quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo. La capa de red define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los encaminadores (routers) que debe seguir un paquete desde el origen al destino.

La capa de transporte (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos, como veremos más adelante.

Una vez que tenemos establecida la comunicación desde el origen al destino nos queda lo más importante, ¿qué podemos transmitir? La capa de aplicación nos proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET...

## Capítulo 2

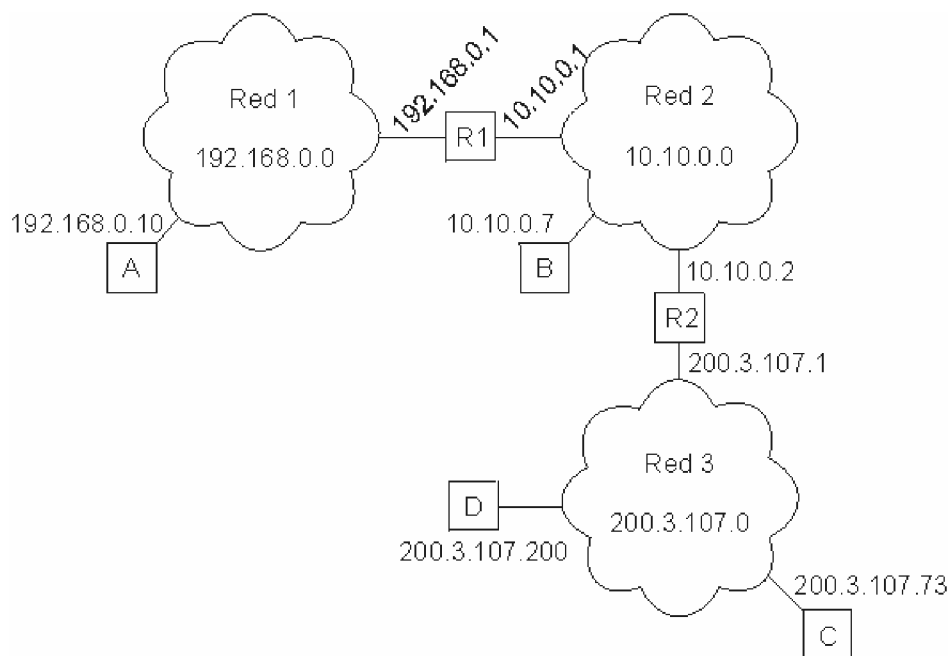
### Capa de red

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de un conjunto de redes unidas mediante encaminadores o routers.

En una red TCP/IP es posible tener, por ejemplo, servidores web y servidores de correo para uso interno. Todos los servicios de Internet se pueden configurar en pequeñas redes internas TCP/IP.

A continuación veremos un ejemplo de interconexión de 3 redes. Cada host (ordenador) tiene una dirección física que viene determinada por su adaptador de red. Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos ordenadores que pertenecen a la misma red. Para identificar globalmente un ordenador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números, según veremos más adelante).

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
	B2-42-52-12-37-BE	10.10.0.2	Red 3
R2	00-E0-89-AB-12-92	200.3.107.1	
C	A3-BB-08-10-DA-DB	200.3.107.73	Red 3
D	B2-AB-31-07-12-93	200.3.107.200	



El concepto de red está relacionado con las direcciones IP que se configuren en cada ordenador, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente los ordenadores que permanezcan a una misma red podrán comunicarse entre sí. Para que los ordenadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes. Un router o encaminador no es más que un ordenador con varias direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados datagramas IP y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

Nota: Cada vez que visitamos una página web o recibimos un correo electrónico es habitual atravesar un número de redes comprendido entre 10 y 20, dependiendo de la distancia de los hosts. El tiempo que tarda un datagrama en atravesar 20 redes (20 routers) suele ser inferior a 600 milisegundos.

En el ejemplo anterior, supongamos que el ordenador 200.3.107.200 (D) envía un mensaje al ordenador con 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que ese ordenador se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si el ordenador 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que el ordenador destino no pertenece a su propia red y enviaría el mensaje al router R2 (es el ordenador que le da salida a otras redes). El router entregaría el mensaje de forma directa porque B se encuentra dentro de una de sus redes (la Red 2).

## 2.1 Direcciones IP

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

- Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar la calculadora científica de Windows para realizar las conversiones).

(decimal) 128.10.2.30  
 (hexadecimal) 80.0A.02.1E  
 (binario) 10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el identificador de red y el identificador de host.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

	0	1	2	3	4	8	16	24	31	
Clase A	0	red				host				
Clase B	1	0	red				host			

Clase C	1	1	0	red		host
Clase D	1	1	1	0	grupo de multicast (multidifusión)	
Clase E	1	1	1	1	(direcciones reservadas: no se pueden utilizar)	

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	-

Nota: Las direcciones usadas en Internet están definidas en la RFC 1166.

Difusión (broadcast) y multidifusión (multicast).-- El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

## 2.2 Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
red	todos 0	Red indicada	192.168.1.0

todos 1		Difusión a mi red	255.255.255.255
red	todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

Difusión o broadcasting es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Intranet.-- Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

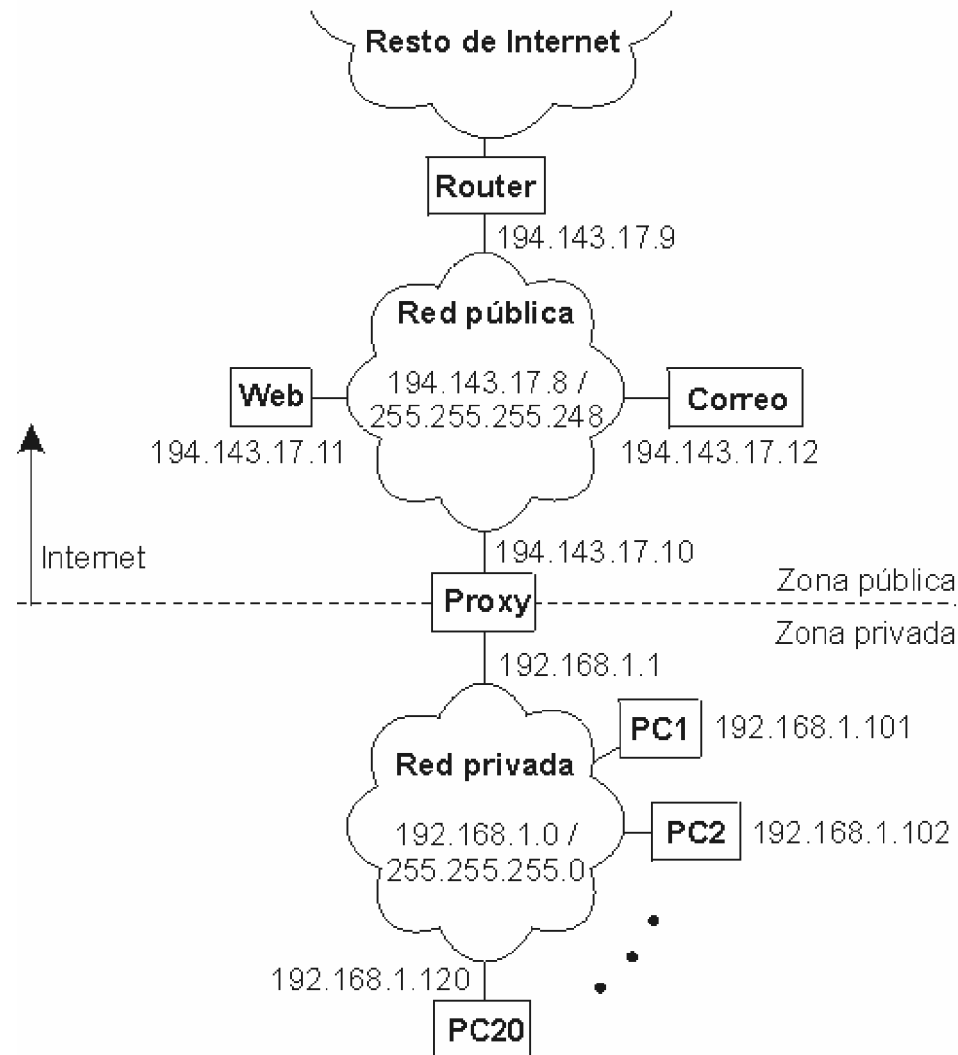
Extranet.-- Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

Internet.-- La mayor red pública de redes TCP/IP.

Por ejemplo, si estamos construyendo una red privada con un número de ordenadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer ordenador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas, tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros ordenadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un ordenador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

CASO PRÁCTICO.- Una empresa dispone de una línea frame relay con direcciones públicas contratadas desde la 194.143.17.8 hasta la 194.143.17.15 (la dirección de la red es 194.143.17.8, su dirección de broadcasting 194.143.17.15 y su máscara de red 255.255.255.248). La línea frame relay está conectada a un router. Diseñar la red para:

- 3 servidores (de correo, web y proxy)
- 20 puestos de trabajo



Los 20 puestos de trabajo utilizan direcciones IP privadas y salen a Internet a través del Proxy. En la configuración de red de cada uno de estos 20 ordenadores se indicará la dirección "192.168.1.1" en el cuadro "Puerta de enlace". La puerta de enlace (puerta de salida o gateway) es el ordenador de nuestra red que nos permite salir a otras redes. El Proxy tiene dos direcciones IP, una de la red privada y otra de la red pública. Su misión es dar salida a Internet a la red privada, pero no permitir los accesos desde el exterior a la zona privada de la empresa.

Los 3 servidores y el router utilizan direcciones IP públicas, para que sean accesibles desde cualquier host de Internet. La puerta de enlace de Proxy, Correo y Web es 194.143.17.9 (Router).

Obsérvese que la primera y última dirección de todas las redes son direcciones IP especiales que no se pueden utilizar para asignarlas a hosts. La primera es la dirección de la red y la última, la dirección de difusión o broadcasting. La máscara de subred de cada ordenador se ha indicado dentro de su red después de una barra: PC1, PC2, ... , PC20 y Proxy (para su IP 192.168.1.1) tienen la máscara 255.255.255.0 y Router, Web, Correo y Proxy (para su IP 194.143.17.10), la máscara 255.255.255.248. El concepto de máscara de subred se estudia a continuación.

## 2.3 Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

```
148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina)
255.255.0.0    11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0    10010100.01111000.00000000.00000000 (dirección de su subred)
<-----RED-----> <-----HOST----->
```

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera.

Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

```
148.120.33.89 10010100.01111000.00100001.01011001 (dirección de una máquina)
255.255.0.0    11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0    10010100.01111000.00000000.00000000 (dirección de su subred)
```

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

```
148.115.89.3 10010100.01110011.01011001.00000011 (dirección de una máquina)
255.255.0.0    11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.115.0.0    10010100.01110011.00000000.00000000 (dirección de su subred)
```

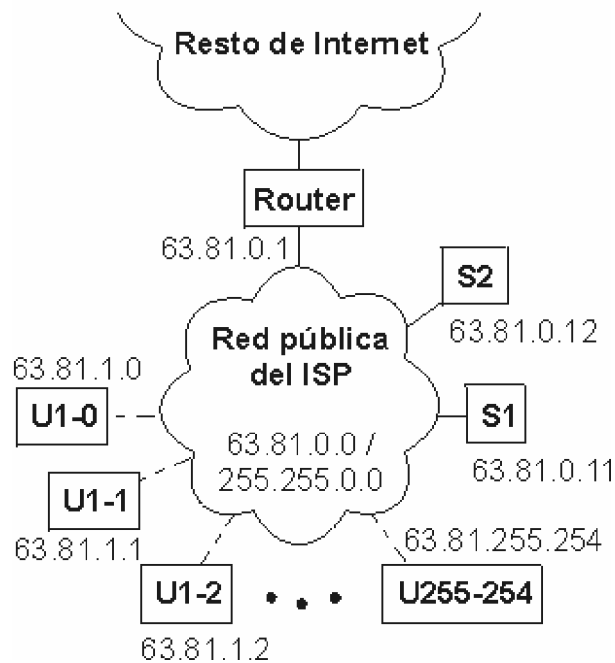
Cálculo de la dirección de difusión.-- Ya hemos visto que el producto lógico binario (AND) de una IP y su máscara devuelve su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su

clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

EJEMPLO.- Los proveedores de Internet habitualmente disponen de una o más redes públicas para dar acceso a los usuarios que se conectan por módem. El proveedor va cediendo estas direcciones públicas a sus clientes a medida que se conectan y liberándolas según se van desconectando (direcciones dinámicas). Supongamos que cierto ISP (proveedor de servicios de Internet) dispone de la red 63.81.0.0 con máscara 255.255.0.0. Para uso interno utiliza las direcciones que comienzan por 63.81.0 y para ofrecer acceso a Internet a sus usuarios, las direcciones comprendidas entre la 63.81.1.0 hasta la 63.81.1.254 (las direcciones 63.81.0.0 y 63.81.255.255 están reservadas).

Si un usuario conectado a la red de este ISP tiene la dirección 63.81.1.1 y quiere transferir un archivo al usuario con IP 63.81.1.2, el primero advertirá que el destinatario se encuentra en su misma subred y el mensaje no saldrá de la red del proveedor (no atravesará el router).



Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 hosts y para el caso de direcciones públicas, su contratación tiene un coste muy alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas. A continuación se muestran las posibles divisiones de una red de clase C. La división de una red en subredes se conoce como subnetting.

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0

255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

Obsérvese que en el caso práctico que explicamos un poco más arriba se utilizó la máscara 255.255.255.248 para crear una red pública con 6 direcciones de hosts válidas (la primera y última dirección de todas las redes se excluyen). Las máscaras con bytes distintos a 0 o 255 también se pueden utilizar para particionar redes de clase A o de clase B, sin embargo no suele ser lo más habitual. Por ejemplo, la máscara 255.255.192.0 dividiría una red de clase B en 4 subredes de 16382 hosts (2 elevado a 14, menos 2) cada una.

#### EJERCICIOS

1. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred (si no se especifica, se utiliza la máscara por defecto):

- 18.120.16.250: máscara 255.0.0.0, red 18.0.0.0, broadcasting 18.255.255.255
- 18.120.16.255 / 255.255.0.0: red 18.120.0.0, broadcasting 18.120.255.255
- 155.4.220.39: máscara 255.255.0.0, red 155.4.0.0, broadcasting 155.24.255.255
- 194.209.14.33: máscara 255.255.255.0, red 194.209.14.0, broadcasting 194.209.14.255
- 190.33.109.133 / 255.255.255.0: red 190.33.109.0, broadcasting 190.33.109.255

2. Suponiendo que nuestro ordenador tiene la dirección IP 192.168.5.65 con máscara 255.255.255.0, indicar qué significan las siguientes direcciones especiales:

- 0.0.0.0: nuestro ordenador
- 0.0.0.29: 192.168.5.29
- 192.168.67.0: la red 192.168.67.0
- 255.255.255.255: broadcasting a la red 192.168.5.0 (la nuestra)
- 192.130.10.255: broadcasting a la red 192.130.10.0
- 127.0.0.1: 192.168.5.65 (loopback)

3. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred:

- 190.33.109.133 / 255.255.255.128: red 190.33.109.128, broadcasting 190.33.109.255  
(133=10000101, 128=10000000, 127=01111111)
- 192.168.20.25 / 255.255.255.240: red 192.168.20.16, broadcasting 192.168.20.31  
(25=00011001, 240=11110000, 16=00010000, 31=00011111)
- 192.168.20.25 / 255.255.255.224: red 192.168.20.0, broadcasting 192.168.20.31  
(25=00011001, 224=11100000, 31=00011111)
- 192.168.20.25 / 255.255.255.192: red 192.168.20.0, broadcasting 192.168.20.63  
(25=00011001, 192=11000000, 63=00111111)
- 140.190.20.10 / 255.255.192.0: red 140.190.0.0, broadcasting 140.190.63.255  
(020=00010100, 192=11000000, 063=00111111)
- 140.190.130.10 / 255.255.192.0: red 140.190.128.0, broadcasting 140.190.191.255  
(130=10000010, 192=11000000, 128=10000000, 063=00111111, 191=10111111)
- 140.190.220.10 / 255.255.192.0: red 140.190.192.0, broadcasting 140.190.255.255  
(220=11011100, 192=11000000, 063=00111111, 255=11111111)

4. Viendo las direcciones IP de los hosts públicos de una empresa observamos que todas están comprendidas entre 194.143.17.145 y 194.143.17.158, ¿Cuál es (probablemente) su dirección de red, broadcasting y máscara?

Pasamos a binario las dos direcciones. La primera tiene que estar próxima a la dirección de red y la última, a la dirección de broadcasting:

```
194.143.017.145 11000010.10001111.00010001.10010001
194.143.017.158 11000010.10001111.00010001.10011110
```

Podemos suponer que la dirección de red es 194.143.17.144 y la de broadcasting, 194.143.17.159:

```
194.143.017.144 11000010.10001111.00010001.10010000
194.143.017.159 11000010.10001111.00010001.10011111
<-----RED-----><-->HOST
```

Entonces la máscara será:

```
255.255.255.240          11111111.11111111.11111111.11110000
<-----RED-----><-->HOST
```

## 2.4 Protocolo IP

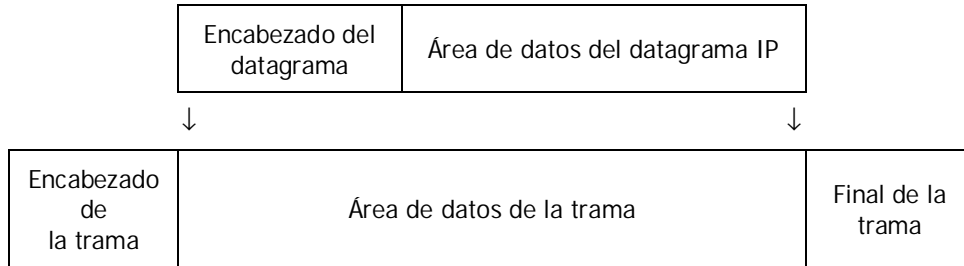
IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados datagramas IP) que tiene las siguientes características:

- Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.
- Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

Nota: El protocolo IP está definido en la RFC 791

## 2.5 Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la trama Ethernet) de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un router, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ATM, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.



0				10								20												30							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VERS				HLEN				Tipo de servicio				Longitud total																			
Identificación								Bandrs				Desplazamiento de fragmento																			
TTL				Protocolo				CRC cabecera																							
Dirección IP origen																															
Dirección IP destino																															
Opciones IP (si las hay)												Relleno																			
Datos																															
...																															

Campos del datagrama IP:

- **VERS (4 bits).** Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están preparando las especificaciones de la siguiente versión, la 6 (IPv6).
- **HLEN (4 bits).** Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.
- **Tipo de servicio (Type Of Service).** Los 8 bits de este campo se dividen a su vez en:

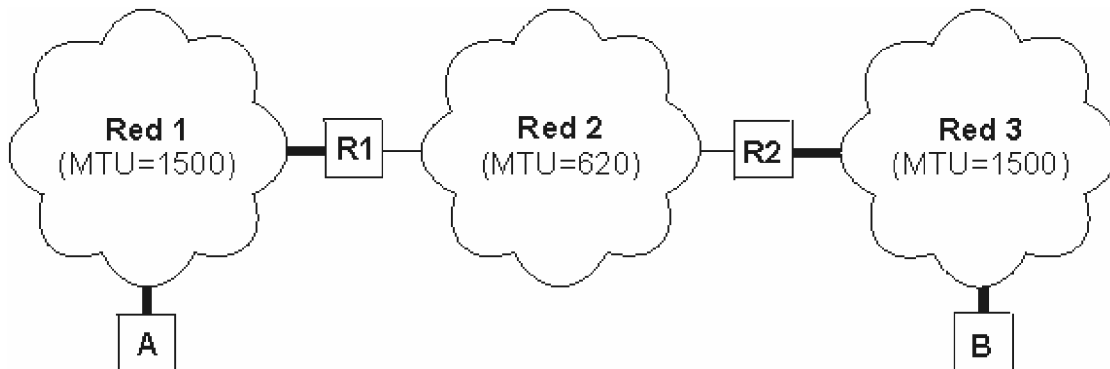
- Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima.
- Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los encaminadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.
- Bit D (Delay). Solicita retardos cortos (enviar rápido).
- Bit T (Throughput). Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
- Bit R (Reliability). Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).
- Los siguientes dos bits no tienen uso.
- Longitud total (16 bits). Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
- Identificación (16 bits). Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.
- Banderas o indicadores (3 bits). Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más fragmentos (MF) indica que no es el último datagrama. Y el bit de No fragmentar (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.
- Desplazamiento de fragmentación (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.
- Tiempo de vida o TTL (8 bits). Número máximo de segundos que puede estar un datagrama en la red de redes. Cada vez que el datagrama atraviesa un router se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.
- Protocolo (8 bits). Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.
- CRC cabecera (16 bits). Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.
- Dirección origen (32 bits). Contiene la dirección IP del origen.
- Dirección destino (32 bits). Contiene la dirección IP del destino.
- Opciones IP. Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).
- Relleno. Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

## 2.6 Fragmentación

Ya hemos visto que las tramas físicas tienen un campo de datos y que es aquí donde se transportan los datagramas IP. Sin embargo, este campo de datos no puede tener una longitud indefinida debido a que está

limitado por el diseño de la red. El MTU de una red es la mayor cantidad de datos que puede transportar su trama física. El MTU de las redes Ethernet es 1500 bytes y el de las redes Token-Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

Un encaminador (router) fragmenta un datagrama en varios si el siguiente tramo de la red por el que tiene que viajar el datagrama tiene un MTU inferior a la longitud del datagrama. Veamos con el siguiente ejemplo cómo se produce la fragmentación de un datagrama.



Supongamos que el host A envía un datagrama de 1400 bytes de datos (1420 bytes en total) al host B. El datagrama no tiene ningún problema en atravesar la red 1 ya que  $1420 < 1500$ . Sin embargo, no es capaz de atravesar la red 2 ( $1420 \geq 620$ ). El router R1 fragmenta el datagrama en el menor número de fragmentos posibles que sean capaces de atravesar la red 2. Cada uno de estos fragmentos es un nuevo datagrama con la misma Identificación pero distinta información en el campo de Desplazamiento de fragmentación y el bit de Más fragmentos (MF). Veamos el resultado de la fragmentación:

- Fragmento 1: Long. total = 620 bytes; Desp = 0; MF=1 (contiene los primeros 600 bytes de los datos del datagrama original)
- Fragmento 2: Long. total = 620 bytes; Desp = 600; MF=1 (contiene los siguientes 600 bytes de los datos del datagrama original)
- Fragmento 3: Long. total = 220 bytes; Desp = 1200; MF=0 (contiene los últimos 200 bytes de los datos del datagrama original)

El router R2 recibirá los 3 datagramas IP (fragmentos) y los enviará a la red 3 sin reensamblarlos. Cuando el host B reciba los fragmentos, recompondrá el datagrama original. Los encaminadores intermedios no reensamblan los fragmentos debido a que esto supondría una carga de trabajo adicional, a parte de memorias temporales. Nótese que el ordenador destino puede recibir los fragmentos cambiados de orden pero esto no supondrá ningún problema para el reensamblado del datagrama original puesto que cada fragmento guarda suficiente información.

Si el datagrama del ejemplo hubiera tenido su bit No fragmentar (NF) a 1, no hubiera conseguido atravesar el router R1 y, por tanto, no tendría forma de llegar hasta el host B. El encaminador R1 descartaría el datagrama.

## 2.7 Protocolo ARP

Dentro de una misma red, las máquinas se comunican enviándose tramas físicas. Las tramas Ethernet contienen campos para las direcciones físicas de origen y destino (6 bytes cada una):

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

El problema que se nos plantea es cómo podemos conocer la dirección física de la máquina destino. El único dato que se indica en los datagramas es la dirección IP de destino. ¿Cómo se pueden entregar entonces estos datagramas? Necesitamos obtener la dirección física de un ordenador a partir de su dirección IP. Esta es justamente la misión del protocolo ARP (Address Resolution Protocol, protocolo de resolución de direcciones).

Nota: El protocolo ARP está definido en la RFC 826

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
	B2-42-52-12-37-BE	10.10.0.2	Red 3
R2	00-E0-89-AB-12-92	200.3.107.1	
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

Vamos a retomar el ejemplo introductorio de este Capítulo. El host A envía un datagrama con origen 192.168.0.10 y destino 10.10.0.7 (B). Como el host B se encuentra en una red distinta al host A, el datagrama tiene que atravesar el router 192.168.0.1 (R1). Se necesita conocer la dirección física de R1.

Es entonces cuando entra en funcionamiento el protocolo ARP: A envía un mensaje ARP a todas las máquinas de su red preguntando "¿Cuál es la dirección física de la máquina con dirección IP 192.168.0.1?". La máquina con dirección 192.168.0.1 (R1) advierte que la pregunta está dirigida a ella y responde a A con su dirección física (00-E0-4C-AB-9A-FF). Entonces A envía una trama física con origen 00-60-52-0B-B7-7D y destino 00-E0-4C-AB-9A-FF conteniendo el datagrama (origen 192.168.0.10 y destino 10.10.0.7). Al otro lado del router R2 se repite de nuevo el proceso para conocer la dirección física de B y entregar finalmente el datagrama a B. El mismo datagrama ha viajado en dos tramas físicas distintas, una para la red 1 y otra para la red 2.

Observemos que las preguntas ARP son de difusión (se envían a todas las máquinas). Estas preguntas llevan además la dirección IP y dirección física de la máquina que pregunta. La respuesta se envía directamente a la máquina que formuló la pregunta.

### 2.7.1 Tabla ARP (caché ARP)

Cada ordenador almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada en su tabla. La primera vez que C envíe un mensaje a D tendrá que difundir previamente una pregunta ARP, tal como hemos visto. Sin embargo, las siguientes veces que C envíe mensajes a D ya no será necesario realizar nuevas preguntas puesto que C habrá almacenado en su tabla la dirección física de D. Sin embargo, para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla.

Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias. Pensemos ahora en distintas maneras para mejorar el rendimiento de la red. Después de una pregunta ARP, el destino conoce las direcciones IP y física del origen. Por lo tanto, podría insertar la correspondiente entrada en su tabla. Pero no sólo eso, sino que todas las estaciones de la red escuchan la pregunta ARP: podrían insertar también las correspondientes entradas en sus tablas. Como es muy probable que otras máquinas se comuniquen en un futuro con la primera, habremos reducido así el tráfico de la red aumentando su rendimiento.

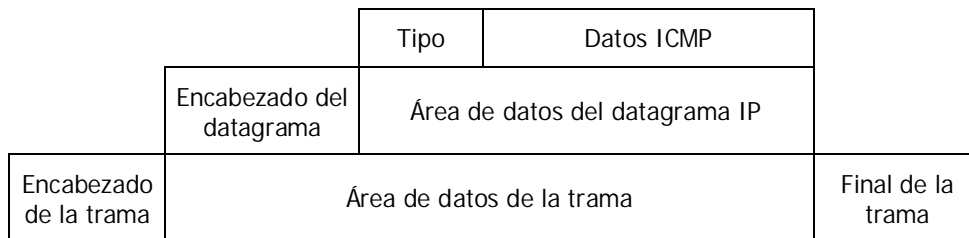
Esto que hemos explicado es para comunicar dos máquinas conectadas a la misma red. Si la otra máquina no estuviese conectada a la misma red, sería necesario atravesar uno o más routers hasta llegar al host destino. La máquina origen, si no la tiene en su tabla, formularía una pregunta ARP solicitando la dirección física del router y le transferiría a éste el mensaje. Estos pasos se van repitiendo para cada red hasta llegar a la máquina destino.

## 2.8 Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

Nota: El protocolo ICMP está definido en la RFC 792

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:



Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP.

Nota: El formato y significado de cada mensaje ICMP está documentado en la RFC 792.

Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Disminución del tráfico desde el origen (Source Quench)
5	Redireccionar (cambio de ruta) (Redirect)
8	Solicitud de eco (Echo)

11	Tiempo excedido para un datagrama (Time Exceeded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Reply)
15	Solicitud de información (obsoleto) (Information Request)
16	Respuesta de información (obsoleto) (Information Reply)
17	Solicitud de máscara (Addressmask)
18	Respuesta de máscara (Addressmask Reply)

### 2.8.1 Solicitud y respuesta de eco

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden PING envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

1. A envía un mensaje ICMP de tipo 8 (Echo) a B
2. B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (Echo Reply) a A
3. A recibe el mensaje ICMP de B y muestra el resultado en pantalla



```
A>ping 172.20.9.7 -n 1
Haciendo ping a 172.20.9.7 con 32 bytes de datos:
Respuesta desde 172.20.9.7: bytes=32 tiempo<10ms TDV=128
```

En la orden anterior hemos utilizado el parámetro "-n 1" para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

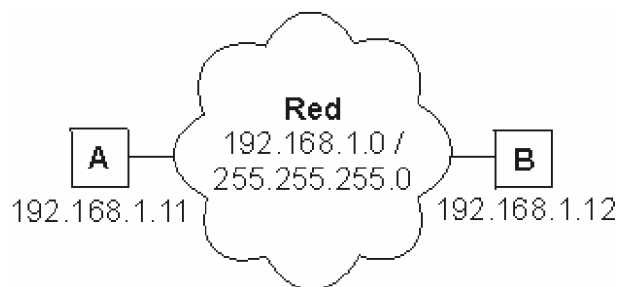
Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (Time Exceeded).

```
A>ping 192.168.0.6 -n 1
Haciendo ping a 192.168.0.6 con 32 bytes de datos:
Tiempo de espera agotado.
```

Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los routers no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (Destination Unreachable).

```
A>ping 1.1.1.1 -n 1
Haciendo ping a 1.1.1.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: Host de destino inaccesible.
```

## Utilización de PING para diagnosticar errores en una red aislada



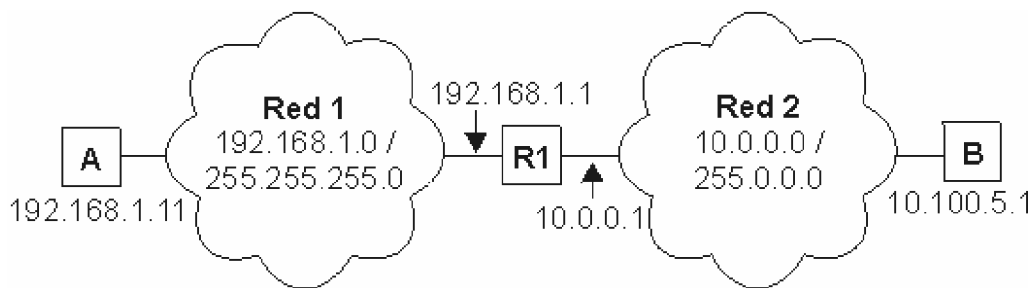
```
A>ping 192.168.1.12
```

- Respuesta. El cableado entre A y B, las tarjetas de red de A y B, y la configuración IP de A y B están correctos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre A y B.
- Host de destino inaccesible. Comprobar las direcciones IP y máscaras de subred de A y B porque no pertenecen a la misma red.
- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar A>ping 127.0.0.1 para asegurarse.

Nota: El comando ping 127.0.0.1 informa de si están correctamente instalados los protocolos TCP/IP en nuestro host. No informa de si la tarjeta de red de nuestro host está correcta.

## Utilización de PING para diagnosticar errores en una red de redes

A continuación veremos un ejemplo para una red de redes formada por dos redes (1 solo router). La idea es la misma para un mayor número de redes y routers.



A>ping 10.100.5.1

- Respuesta. El cableado entre A y B, las tarjetas de red de A, R1 y B, y la configuración IP de A, R1 y B están correctos. El router R1 permite el tráfico de datagramas IP en los dos sentidos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre R1 y B. Para asegurarnos que el router R1 está funcionando correctamente haremos A>ping 192.168.1.1
- Host de destino inaccesible. Comprobar el router R1 y la configuración IP de A (probablemente la puerta de salida no sea 192.168.1.1). Recordemos que la puerta de salida (gateway) de una red es un host de su propia red que se utiliza para salir a otras redes.
- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar A>ping 127.0.0.1 para asegurarse.

En el caso producirse errores de comunicación en una red de redes con más de un router (Internet es el mejor ejemplo), se suele utilizar el comando PING para ir diagnosticando los distintos routers desde el destino hasta el origen y descubrir así si el fallo es responsabilidad de la red de destino, de una red intermedia o de nuestra red.

Nota: Algunos hosts en Internet tienen deshabilitadas las respuestas de eco (mensajes ICMP tipo 0) como medida de seguridad. En estos casos hay que utilizar otros mecanismos para detectar si responde (por ejemplo, la apertura de conexión a un puerto).

## Mensajes ICMP de tiempo excedido

Los datagramas IP tienen un campo TTL (tiempo de vida) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (Time Exceeded) para informar al origen.

Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario). El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.

La orden TRACERT (traceroute en entornos Unix) hace una traza a un determinado host. TRACERT funciona enviando mensajes ICMP de solicitud de eco con distintos TTL; traceroute, en cambio, envía mensajes UDP. Si la comunicación extremo a extremo no es posible, la traza nos indicará en qué punto se ha producido la incidencia. Existen algunas utilidades en Internet, como [Visual Route](#), que conocen la localización geográfica de los principales routers de Internet. Esto permite dibujar en un mapamundi el recorrido que siguen los datagramas hasta llegar a un host.

A>tracert 130.206.1.2

Traza a la dirección sun.rediris.es [130.206.1.2]  
sobre un máximo de 30 saltos:

```
 1  1 ms  1 ms  1 ms PROXY [192.168.0.1]
 2 122 ms 118 ms 128 ms MADR-X27.red.retevision.es [62.81.1.102]
 3 143 ms 232 ms 147 ms MADR-R2.red.retevision.es [62.81.1.92]
 4 130 ms 124 ms 246 ms MADR-R16.red.retevision.es [62.81.3.8]
 5 590 ms 589 ms 431 ms MADR-R12.red.retevision.es [62.81.4.101]
 6 612 ms 640 ms 124 ms MADR-R10.red.retevision.es [62.81.8.130]
 7 259 ms 242 ms 309 ms 193.149.1.28
 8 627 ms 752 ms 643 ms 213.0.251.42
 9 137 ms 117 ms 118 ms 213.0.251.142
10 109 ms 105 ms 110 ms A1-2-1.EB-Madrid00.red.rediris.es [130.206.224.81]
11 137 ms 119 ms 122 ms A0-0-0-1.EB-Madrid3.red.rediris.es [130.206.224.86]
12 109 ms 135 ms 115 ms sun.rediris.es [130.206.1.2]
```

Traza completa.

Ejemplo de Visual Route a una dirección IP de Taiwan (203.69.112.12):



## 2.9 Encaminamiento

Una red de redes está formada por redes interconectadas mediante routers o encaminadores. Cuando enviamos un datagrama desde un ordenador hasta otro, éste tiene que ser capaz de encontrar la ruta más adecuada para llegar a su destino. Esto es lo que se conoce como encaminamiento.

Los routers (encaminadores) son los encargados de elegir las mejores rutas. Estas máquinas pueden ser ordenadores con varias direcciones IP o bien, aparatos específicos. Los routers deben conocer, al menos parcialmente, la estructura de la red que les permita encaminar de forma correcta cada mensaje hacia su destino. Esta información se almacena en las llamadas tablas de encaminamiento. Observemos que debido al sistema de direccionamiento IP esta misión no es tan complicada. Lo único que necesitamos almacenar en las tablas son los prefijos de las direcciones (que nos indican la red). Por ejemplo, si el destino es la máquina 149.33.19.4 con máscara 255.255.0.0, nos basta con conocer el encaminamiento de la red 149.33.0.0 ya que todas las que empiecen por 149.33 se enviarán hacia el mismo sitio.

La orden Route muestra y modifica la tabla de encaminamiento de un host. Todos los hosts (y no sólo los routers) tienen tablas de encaminamientos. A continuación se muestra una tabla sencilla para un host con IP 192.168.0.2 / 255.255.255.0 y puerta de salida 192.168.0.1.

A>route print

Rutas activas:

Dirección de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.2	1 (7)
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1 (6)
192.168.0.0	255.255.255.0	192.168.0.2	192.168.0.2	1 (5)
192.168.0.2	255.255.255.255	127.0.0.1	127.0.0.1	1 (4)
192.168.0.255	255.255.255.255	192.168.0.2	192.168.0.2	1 (3)
224.0.0.0	224.0.0.0	192.168.0.2	192.168.0.2	1 (2)
255.255.255.255	255.255.255.255	192.168.0.2	0.0.0.0	1 (1)

Esta tabla se lee de abajo a arriba. La línea (1) indica que los datagramas con destino "255.255.255.255" (dirección de difusión a la red del host) deben ser aceptados. La línea (2) representa un grupo de multidifusión (multicasting). La dirección "224.0.0.0" es una dirección de clase D que se utiliza para enviar mensajes a una colección de hosts registrados previamente. Estas dos líneas se suelen pasar por alto: aparecen en todas las tablas de rutas.

La línea (3) indica que todos los mensajes cuyo destinatario sea "192.168.0.255" deben ser aceptados (es la dirección de difusión a la red del host). La línea (4) se encarga de aceptar todos los mensajes que vayan destinados a la dirección del host "192.168.0.2".

La línea (5) indica que los mensajes cuyo destinatario sea una dirección de la red del host "192.168.0.0 / 255.255.255.0" deben salir del host por su tarjeta de red para que se entreguen directamente en su subred. La línea (6) es la dirección de loopback: todos los paquetes con destino "127.0.0.0 / 255.0.0.0" serán aceptados por el propio host.

Finalmente, la línea (7) representa a "todas las demás direcciones que no se hayan indicado anteriormente". En concreto son aquellas direcciones remotas que no pertenecen a la red del host. ¿A dónde se enviarán? Se enviarán a la puerta de salida (gateway) de la red "192.168.0.1".

Nótese que la tabla de rutas es la traducción de la configuración IP del host que habitualmente se escribe en las ventanas de Windows:

