

Protocolo Tcp/ip - Introducción. Apunte extraído de <http://www.saulo.net>

Todos sabemos en este momento lo importante que son las comunicaciones electrónicas en la vida del hombre, y las redes de computadoras forman parte de estas, ya que para que ellas existan son necesarios medios electrónicos de comunicación, desde la propia computadora a la placa de red de la misma, la cual se encargará de darle acceso al medio de red. Estas redes podrán tener cualquier estructura o topología y necesitarán un lenguaje de comunicación, un convenio o protocolo para que la comunicación pueda realizarse, existen distintos tipos de protocolos de comunicación pero en los últimos años las redes informáticas se han volcado, por sus características, al protocolo Tcp/ip, que en realidad es una familia de protocolos funcionando bajo Tcp.

La principal característica de Tcp/ip es que nos brinda una estandarización en cuanto a la conexión, pero la ventaja es que el mismo no depende del acceso a la red para establecer la comunicación, es decir que es independiente del hardware de los equipos a los cuales conecta. Esta ventaja nos permite conectar equipos muy distintos entre sí por ejemplo en la red de redes *Internet*.

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 (gracias a Tcp/ip). De esta manera, podemos transmitir información entre un servidor Unix y una computadora que utilice Windows 7. 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:

Capa de aplicación (HTTP, SMTP, FTP, TELNET...)
Capa de transporte (UDP, TCP)
Capa de red (IP)
Capa de acceso a la red (Ethernet, Token Ring...)
Capa física (cable coaxial, par trenzado...)

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 (computadoras) 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 espera? ¿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, es por esto que decimos que Tcp/ip es independiente del hardware. 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 (el que utilizamos cuando usamos el servicio ping), e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los encaminadores o enrutadores (*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, estos puertos no son físicos como el puerto serie o paralelo, sino lógicos.

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...

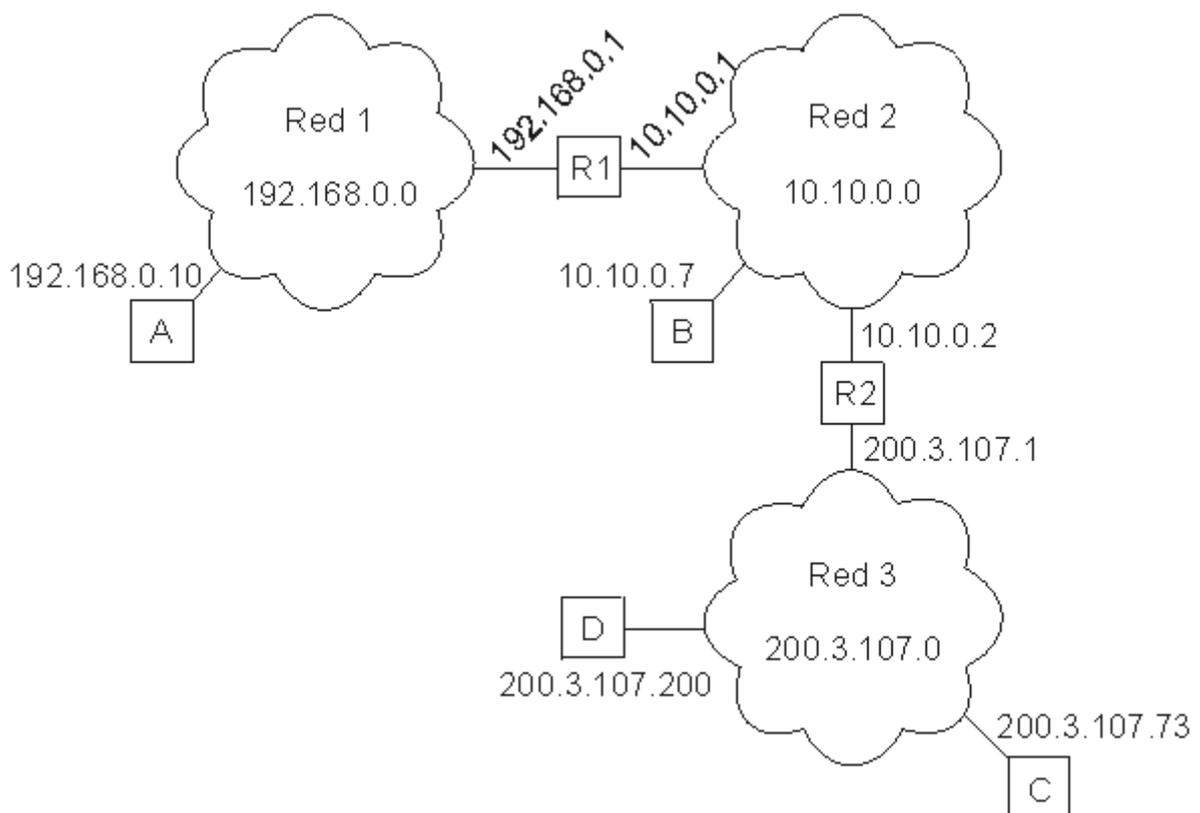
Capa de red

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 *routers*.

Una red privada que funcione siguiendo el mismo esquema de *Internet* se denomina *Intranet*. En una red Tcp/ip es posible tener, por ejemplo, servidores web y servidores de correo para uso interno. Obsérvese que todos los servicios de Internet se pueden configurar en pequeñas redes internas Tcp/ip, es por ello su gran utilidad.

A continuación veremos un ejemplo de interconexión de 3 redes. Cada *host* (computadora) 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 computadoras que pertenecen a la misma red. Para identificar globalmente una computadora 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	
R2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
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 computadora, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente las computadoras que permanezcan a una misma red podrán comunicarse entre sí. Para que las computadoras 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 equipo, o una computadora, 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 la computadora 200.3.107.200 (D) envía un mensaje a la computadora con 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que esa computadora se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si la computadora 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que la computadora destino no pertenece a su propia red y enviaría el mensaje al router R2 (es la computadora o equipo 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).

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 computadoras con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos computadoras 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. Una computadora con una IP pública es accesible (visible) desde cualquier otro equipo 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. Las computadoras 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 equipos 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 como ya sabemos 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 (combinaciones que se pueden lograr con 8 bits). 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).

RED	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 (en inglés).

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.

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 equipos 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 nuestra propia computadora. 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.

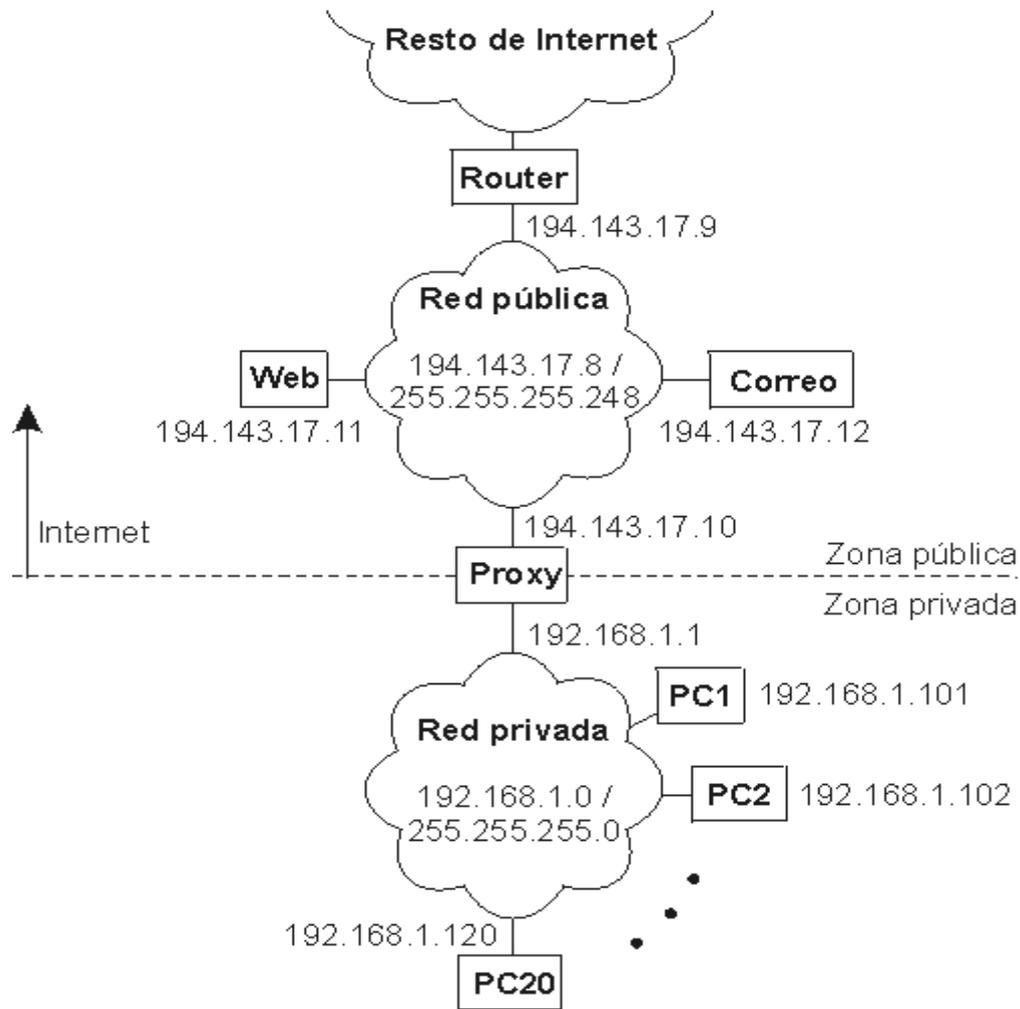
Extranet.-- Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

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

Por ejemplo, si estamos construyendo una red privada con un número de computadoras no superior a 254 podemos utilizar una red reservada de clase C. A la primera computadora 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 nuestras computadoras podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en una computadora de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

EJEMPLO.- 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 estas 20 computadoras 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 equipo 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 computadora 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.

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 una computadora 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 otra computadora, 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).

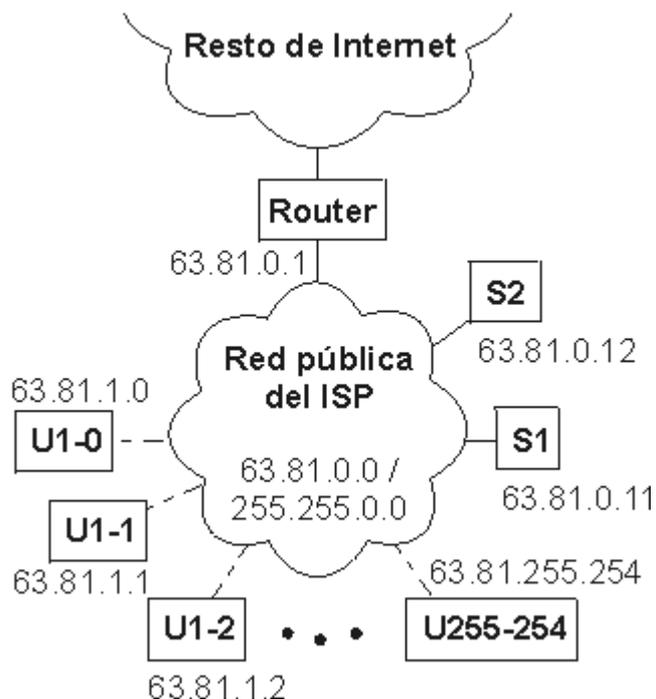
```
148.120.33.89 10010100.01111000.00100001.01011001 (dirección de una
máquina)
255.255.0.0    11111111.11111111.00000000.00000000 (dirección de su
máscara de red)
148.120.0.0    10010100.01111000.00000000.00000000 (dirección de su
subred)
```

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 (sino se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara una computadora sabe si otra, 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 63.81.0.0 y para ofrecer acceso a Internet a sus usuarios, las direcciones comprendidas entre la 63.81.1.0 hasta la 63.81.255.254 (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 visto 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 155.4.255.255
- **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 nuestra computadora 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:** nuestra computadora
- **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
(20=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=110111100, 192=110000000, 63=001111111, 255=111111111)

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
```