Crear una red local basada en TCP/IP no es una tarea excesivamente complicada

Conceptos básicos de TCP/IP

Javier Cáceres
jcaceres@pcw.idg.es

l exponencial crecimiento de Internet ha propiciado que prácticamente no exista hoy una gran empresa que no disponga de cierta presencia en la Red de redes. Internet ha cambiado la forma en la que la gente se comunica, adquiere y comparte información, pasando de ser poco más que una *curiosidad tecnológica*, a una herramienta indispensable de trabajo.

Paralelamente, el sucesivo abaratamiento del coste de los sistemas de comunicaciones y del software asociado, ha favorecido el acercamiento hasta de un masivo número de usuarios particulares, como de las pequeñas y medianas empresas. Nadie quiere quedarse fuera de este nuevo medio de comunicación, fuera de un mercado que sin duda gozará de un más que considerable crecimiento en los próximos años.

Los sistemas operativos actuales tienden a simplificar la conexión a Internet hasta un punto en el cual no es preciso conocer prácticamente nada del protocolo en el que se basa. Igualmente, crear una pequeña red local basada en TCP/IP tampoco resulta una tarea excesivamente complicada. No obstante, si pretende abordar algo más complejo, ya dentro del campo de las redes corporativas, como pueda ser diseñar intranets o extranets, interconectar varias redes locales, subdividir dominios, crear enlaces a redes externas, configurar servidores, pasarelas, etc., precisará de conocer más detalladamente este popular protocolo. El presente artículo pretende exponer con suficiente profundidad todos los conceptos precisos para la confección de redes TCP/IP de cualquier tamaño, bajo cualquier sistema operativo. Nos centraremos exclusivamente en lo que son los conceptos teóricos de este tipo de redes pues, por simple extensión, nos resultaría imposible incluir en una sola entrega todos los aspectos relacionados con el hardware y la topología de las redes que podemos emplear. Si desea documentarse al respecto, ambos temas fueron tratados en el artículo *Conceptos fundamentales de una red*, publicado en *PC World* nº 149, diciembre 98.

Conceptos básicos

Lo primero que hemos de dejar claro, en contra de la creencia popular, es que TCP/IP no es un protocolo, son dos. Erróneamente nos solemos referir a él como el protocolo TCP/IP, cuando debiéramos hablar del conjunto de protocolos TCP/IP. Por un lado, tenemos el protocolo IP (*Internet Protocol*), que como su propio nombre indica es la base de Internet, y de cualquier red desarrollada a partir de su tecnología. IP, como discutiremos más adelante, provee a protocolos de más alto nivel de los servicios de encapsulado y envío de datos. Por otro lado, tenemos un par de protocolos que suelen utilizar IP como base: TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*). TCP proporciona a las aplicaciones de red una serie de servicios que, por su sencillez, IP no puede facilitar. UDP por su parte, también emplea como base IP, ofreciendo otra clase de servicios más apropiados para ciertas aplicaciones de red.

Como no podría ser de otro modo, la historia del TCP/IP va estrechamente ligada a la propia historia de Internet. A mediados de la década de los 70 el departamento de defensa de los EE.UU. solicitó a ARPA (*Advanced Research Projects Agency*), que desarrollara un sistema de red entre los distintos laboratorios, universidades y oficinas estatales. El principal problema que se encontraron consistía en que las redes existentes, de cada uno de ellos, usaban distintos sistemas operativos y diversas topologías y tipos de red. Los diseñadores de lo que primero se conoció por ARPAnet (poste-

TCP/IP es el corazón de Internet y base de las emergentes intranets y extranets. Tener claros los conceptos básicos de las redes IP le permitirá concebir redes locales y corporativas de medio y gran tamaño

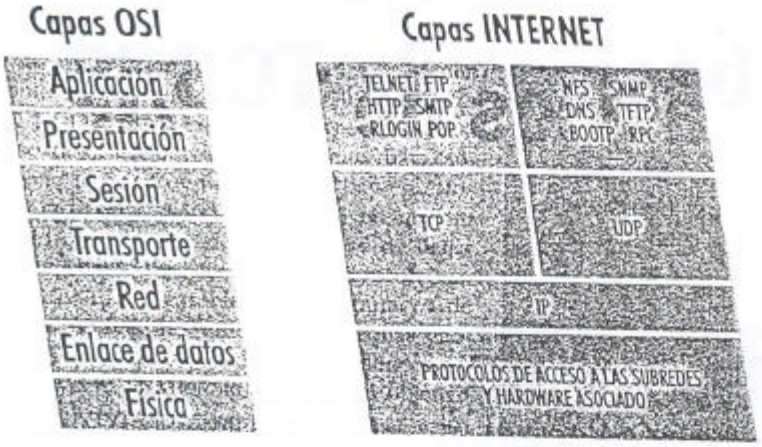
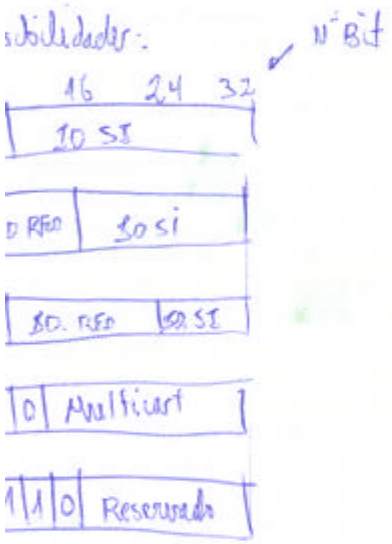


Figura 1. Correlación entre el modelo teórico de capas o niveles de red propuesto por OSI y el modelo empleado por las redes TCP/IP.



número de niveles, el acto de
tir datos de un sistema a otro.
de referencia, la ISO (*Inter*
Standards Organisation),
modelo para la interconexión
mas abiertos, conocido con
Dicho modelo divide en siete
proceso de transmisión de info
entre equipos informáticos, o
hardware físico, hasta las apli
de red que maneja el usuari
capas o niveles son: física, de
de datos, de red, de transpo
sesión, de presentación y, fina
de aplicación. Cada nuevo p
de red que se define se suele
uno (o varios) niveles del e
OSI. Internet dispone de un
más sencillo. No define n
cuanto al aspecto físico de los
o a la topología o clase de red
subredes y, por lo tanto, den
modelo OSI, solo existe una
ción con los niveles superiore
sulte Figura 1).

En este punto es interesante d
que las aplicaciones que trabaja
cierto nivel o capa, sólo se com
con sus iguales en los sistemas
tos, esto es (por poner un ejem
nivel de aplicación, el navegad
se entiende con el servidor w
importarle en absoluto cómo le l
información. Este mismo princi
emplea para el resto de capas.
preguntado alguna vez qué
cuando solicita una página web
buen ejemplo para ilustrar más
mente el concepto de las capas
les: el navegador realiza una p
HTTP, petición que se i
en un paquete TCP, qu
vez es encapsulado y
mentado en uno o vario
gramas (unidad de d
nivel de red) IP. Dichos
gramas son igualmente
sulados en unidades de
(*frames*) PPP, que se en
su proveedor de Internet
vio paso por el módem
transforma tales unidades digital
datos en señales acústicas de ac
a una determinada norma (V.34
V.90, por ejemplo). Su ISP ensan
los paquetes PPP para convertirl
nuevo en datagramas IP, que so
vados a su destino, donde serán

riormente Internet), decidieron que, a fin de interconectar un gran número de distintos tipos de subredes, debían definir primero un protocolo fácil de implementar en todas ellas (lo que sería IP), y que sobre él, posteriormente emplearían protocolos más complejos (TCP, UDP, etc.). Precisamente la sencillez del protocolo IP es una de las causas por las cuales hoy día se encuentra soportado en todas las plataformas informáticas relevantes.

Protocolos sobre protocolos

A la hora de enfrentarse a un problema de tamaño considerable, la solución más optima empieza por dividirlo en pequeñas secciones, para posteriormente proceder a solventar cada una de ellas independientemente. El mismo principio de divide y vencerás es el que se sigue cuando diseñamos redes, esto es, separar en un buen

Tabla A. Clases de direcciones IP

Clase	Nodos por clase	Máscara asociada	Dirección de comienzo	Dirección final
A	2^{24}= 16.777.216	255.0.0.0	0.0.0.0	127.255.255.255
B	2^{16}= 65.536	255.255.0.0	128.0.0.0	191.255.255.255
C	2^{8}= 256	255.255.255.0	192.0.0.0	223.255.255.255
D	-	-	224.0.0.0	239.255.255.255
E	-	-	240.0.0.0	255.255.255.255

Tabla B. Rangos de direcciones IP reservadas

Clase	Máscara asociada	Dirección de comienzo	Dirección final
A	255.0.0.0	10.0.0.0	10.255.255.255
B	255.255.0.0	172.16.0.0	172.31.255.255
C	255.255.255.0	192.168.0.0	192.168.255.255

Consecuencias: RED | TODOS 0'S | ESTA RED
TODOS 0'S | ESTE ST

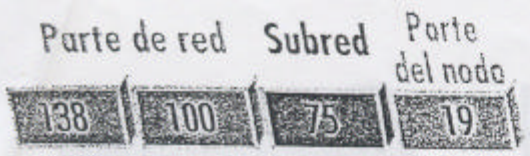


Figura 2. En la figura se puede apreciar lo que representan los distintos números de una dirección IP de un nodo perteneciente a una subred de clase B (máscara 255.255.x.0).

dificados en sentido inverso al realizado en nuestro equipo, hasta que alcancen el "nivel de aplicación", que supone el servidor web.

De lo aquí expuesto debemos quedarnos con tres ideas principales. En primer lugar, que TCP/IP opera sólo en los niveles superiores de red, resultándole indiferente el conjunto de protocolos que se entienden con los adaptadores de red (conexión física: Ethernet, Token-Ring, ARCNet, ATM, etcétera) que se encuentren por debajo. En segundo lugar, que IP es un protocolo de datagramas que proporciona una interfaz estándar a protocolos superiores y, por último, que dentro de esos protocolos superiores podemos incluir a TCP y UDP, los cuales ofrecen prestaciones adicionales que ciertas aplicaciones de red necesitan.

El protocolo IP

IP es un protocolo simple, fácilmente implementable, de pequeñas unidades de datos o datagramas, que provee una interfaz estándar a partir de la cual el resto de protocolos y servicios pueden ser construidos, sin tener que preocuparse de las diferencias que existan entre las distintas subredes por las cuales circulen los datos.

Como bien es sabido, todo dispositivo conectado a Internet o a cualquier red basada en TCP/IP, posee (al menos) una dirección IP, un identificador de 32 bits que define unívocamente al dispositivo que lo tiene asignado en la red. Este número se divide en cuatro octetos (bytes), en donde, según la clase de red que tengamos y la máscara, parte de ellos representan a la red, parte a la subred (donde proceda), y parte al dispositivo final o nodo específico de la red (véase Figura 2).

Por cuestiones de espacio, nos resulta imposible comentar con detalle la estructura interna de un datagrama IP. No obstante, conviene tener claro que se encuentra dividido en dos partes: cabecera y datos. Dentro de la cabecera, entre otros campos, se encuentran la dirección IP del equipo origen y la del destino, el tamaño y un número de orden.

IP opera entre un sistema local conectado a Internet y su *router* o encaminador más próximo, así como entre los distintos *routers* que forman la red. Cuando un datagrama llega a un *router*, éste determina, a partir de la dirección IP destino, hacia cuál de sus conexiones de salida ha de dirigir el datagrama que acaba de recibir. Lamentablemente, en cuanto al transporte, IP provee de un servicio que "intenta" entregar los datos al equipo destino, pero no puede garantizar la integridad, e incluso la recepción de los mismos. Por ello, la mayoría de las aplicaciones hacen uso de un protocolo de más alto nivel, que les ofrezca el grado de fiabilidad necesario.

Cada datagrama IP es independiente del resto, por lo que cada uno de ellos es llevado a su destino por separado. Asimismo, la longitud del datagrama es variable, pudiendo almacenar hasta un máximo de 65KB de datos. Si el paquete de datos (TCP o UDP) que ha de encapsular sobrepasa ese límite, o el tamaño de la unidad de datos de la red que se encuentra por debajo es más pequeño que el datagrama IP, el mismo protocolo IP lo fragmenta, asigna un número de orden y distribuye empleando el número de datagramas que precise.

TCP y UDP

Ambos protocolos fueron diseñados para funcionar principalmente sobre redes IP, situándose en el nivel inmediatamente superior.

TCP ofrece un servicio de transporte de datos fiable, que garantiza la integridad y entrega de los datos entre dos procesos o aplicaciones de máquinas remotas. Es un protocolo orientado a la conexión, es decir, funciona más o menos como una llamada de teléfono. En primer lugar, el equipo local solicita al remoto el establecimiento de un canal de comunicación. Sólo cuando ese canal ha sido creado, y ambas máquinas están preparadas para la transmisión, empieza la transferencia de datos real.

UDP por su parte ofrece servicios similares a TCP, si bien no está orientado a la conexión y la transmisión de datos no es tan fiable. Los procesos que hagan uso de UDP han de implementar (si es necesario), sus propias

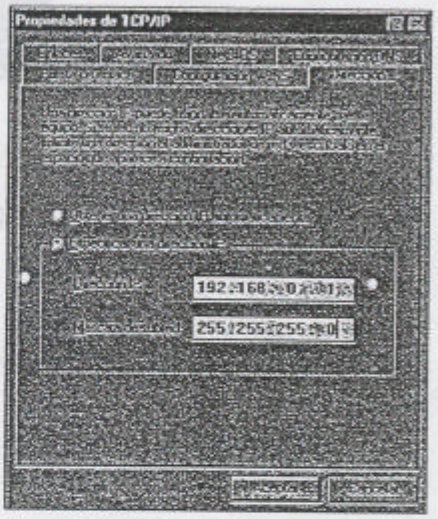


Figura 3. La dirección IP y la máscara de subred son los dos parámetros indispensables de todo dispositivo que pretenda enviar y recibir paquetes en una red IP.

Figura 4. Para que un nodo pueda enviar paquetes fuera de su red local, ha de conocer cuál es su *gateway*, o puerta de enlace con el exterior.

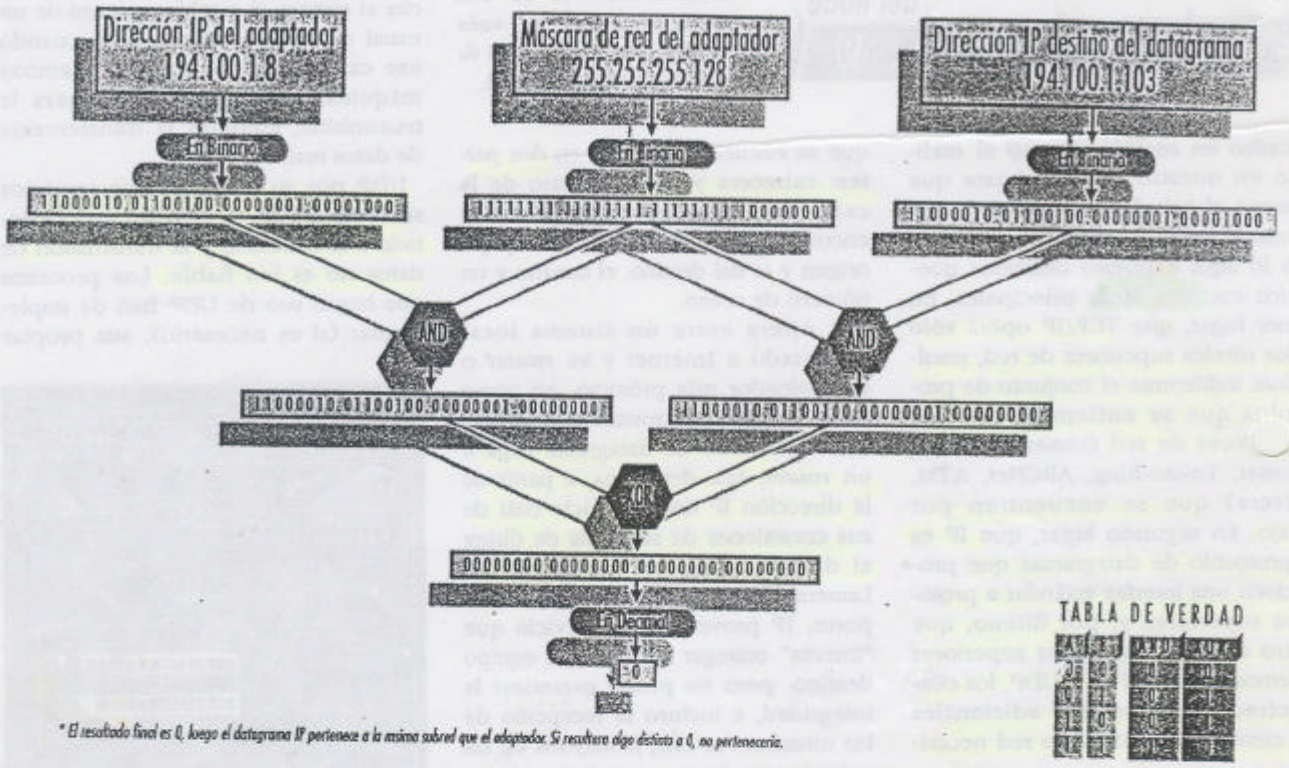


Figura 5. Proceso por el cuál se determina si un determinado datagrama pertenece o no a una ruta de datos concreta, esto es, una dirección IP y una máscara asociada.

rutinas de verificación de envío y sincronización.

TCP y UDP transmiten y reciben unidades de datos conocidas como paquetes. Cada uno (al igual que los datagramas), se compone de cabecera y un área de datos donde se almacena la información a transmitir. Dentro de su cabecera, los campos más importantes son el puerto de origen y el de destino. El puerto es un número de 16 bits (de 0 a 65535), que identifica el lugar donde se encuentra el proceso o aplicación que solicita o al que se le requiere información. Los números de puerto suelen ir asociados a un determinado protocolo de aplicación: 80 al HTTP, 23 al TELNET, 21 al FTP, etcétera. De no existir estos identificadores, sólo podríamos ofrecer un único servicio por máquina. Nótese que el protocolo IP, no sabe nada al respecto de números de puerto, al igual que TCP y UDP no se preocupan en absoluto por las direcciones IP. Digamos que IP pone en contacto a máquinas, mientras que TCP y UDP establecen un canal de comunicación entre determinados procesos que se ejecutan en tales equipos. Los números de puerto los podemos entender como números de oficinas dentro de un gigantesco edificio. El edificio (equipo), tendrá pues una única dirección IP, pero dentro de él encontramos que cada tipo de negocio (en este caso HTTP, FTP, etc.), dispone de una oficina individual.

Subdivisión de redes

A la hora de administrar una red se suele seguir, de nuevo, el principio de divide y vencerás, especialmente si tratamos con redes de gran tamaño. Internet sin ir más lejos, es a menudo referida como la Red de redes. Ésta es una definición muy ajustada pues Internet, no es más que una gigantesca red formada por miles de subredes. Que, a su vez, también suelen estar compuestas por un importante número de redes locales.

Por razones administrativas, en los primeros tiempos del desarrollo del protocolo IP, se establecieron subrangos de direcciones, dentro rango total de 32bits de direcciones disponibles. A dichos subrangos se lo denominó clases. Cuando una determinada organización requiere conectarse a Internet, solicita una cierta clase, de acuerdo al número de nodos que precise tener conectados a la Red. La administración referente a la cesión de rangos de direcciones IP la efectúa InterNIC (*Internet Network Information Center*), si bien, existen autoridades que, según la zona, gestionan dominios locales.

Los subrangos se definen en orden ascendente de direcciones IP, por lo cual, a partir de la dirección IP, es fácil averiguar el tipo de clase de Internet a la que estamos conectados. El tipo de clase bajo la que se encuentra una dirección IP concreta viene determinado por el valor del primer octeto de los cuatro que la componen o, lo que

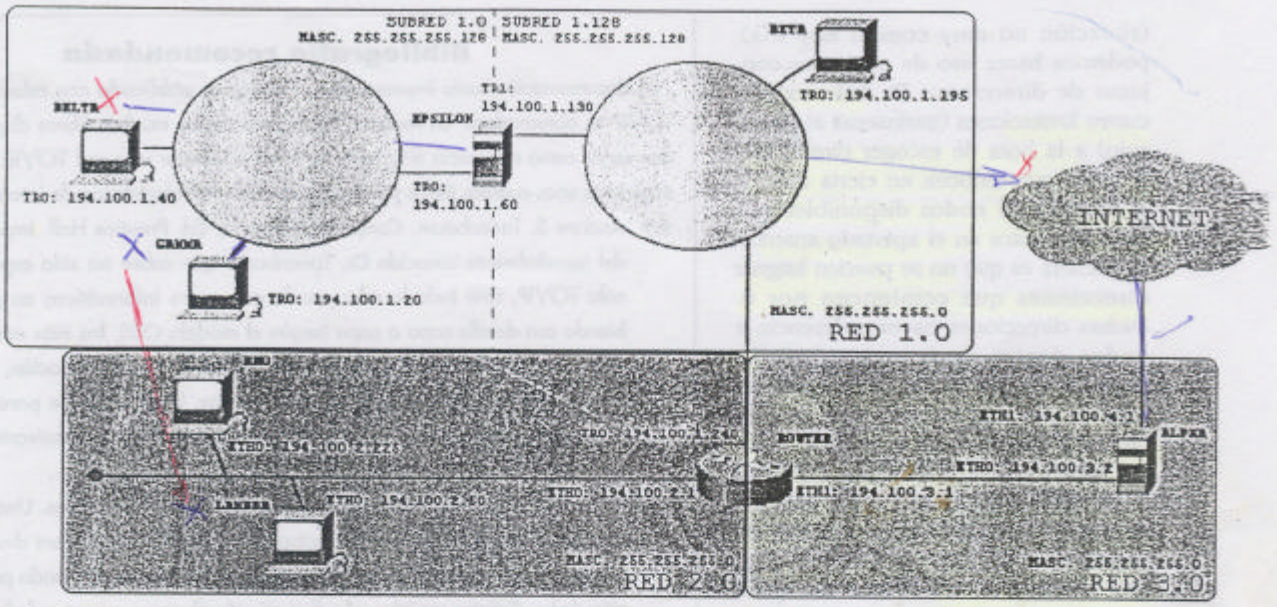


TABLA DE RUTAS DE GAMMA

RUTA	RED DESTINO	MASCARA	GATEWAY	ADAPTADOR
1	194.100. 1 . 0	255.255.255.128	-	TR0
2	default	0 . 0 . 0 . 0	194.100. 1 .60	TR0

TABLA DE RUTAS DE EPSILON

RUTA	RED DESTINO	MASCARA	GATEWAY	ADAPTADOR
1	194.100. 1 . 0	255.255.255.128	-	TR0
2	194.100. 1 .128	255.255.255.128	-	TR1
3	default	0 . 0 . 0 . 0	194.100. 1 .240	TR1

TABLA DE RUTAS DE BETA

RUTA	RED DESTINO	MASCARA	GATEWAY	ADAPTADOR
1	194.100. 1 .128	255.255.255.128	-	TR0
2	194.100. 1 . 0	255.255.255.128	194.100. 1 .130	TR0
3	default	0 . 0 . 0 . 0	194.100. 1 .240	TR0

TABLA DE RUTAS DE LAMBDA

RUTA	RED DESTINO	MASCARA	GATEWAY	ADAPTADOR
1	194.100. 2 . 0	255.255.255.0		ETH0
2	default	0 . 0 . 0 . 0	194.100. 2 . 1	ETH0

TABLA DE RUTAS DEL ROUTER

RUTA	RED DESTINO	MASCARA	GATEWAY	ADAPTADOR
1	194.100. 1 . 0	255.255.255.128	194.100. 1 .130	TR0
2	194.100. 1 .128	255.255.255.128		TR0
3	194.100. 2 . 0	255.255.255. 0		ETH0
4	194.100. 3 . 0	255.255.255. 0		ETH1
5	default	0 . 0 . 0 . 0	194.100. 3 . 2	ETH1

Figura 6. Modelo de red que incluye buena parte de los dispositivos y técnicas que podemos encontrar en todo tipo de redes IP.

es lo mismo, el primer número que aparece en la dirección IP. Las clases toman nombre de la A, a la E, si bien A, B, y C son las más conocidas. En Internet, las redes de clase A son las que comienzan su dirección con un número entre el 1 y el 126. Otorgan el mayor número de direcciones IP (16.7 millones) y, por consiguiente, se asignan a grandes instituciones educativas o gubernamentales. Las clases B (65.536 direcciones IP por clase), suelen concederse a grandes empresas o corporaciones, y en general a cualquier organización que precise un importante número de nodos. Las redes de clase C (256 direcciones) son las más comunes y habitualmente se asignan sin demasiados problemas a cualquier empresa u organización que lo solicite. La clase D se reserva a la transmisión de mensajes de difusión múltiple (*Multicast*), mientras que la E es la destinada a investigación y desarrollo (véase referencia en Tabla A).

Como decíamos, las subredes IP conectadas a Internet, e incluso las que no lo están, a menudo están compuestas por un importante número de redes locales, enlazadas entre sí mediante una serie de equipos conocidos como puertas de enlace o *gateways*. Las razones para ello, no son simplemente administrativas (distintos departamentos, secciones, etc.), son fruto también de otra serie de consideraciones. Segmentar una intranet en varias redes locales conlleva (según el caso) poder dividir las direcciones IP asignadas de Internet entre los puestos de la subred, un aumento de la velocidad (el que la red contabilidad esté saturada, no afecta a la red de m ting), un aumento de la seguridad empleados del departamento de ración no tienen la capacidad de capturar los mensajes que entre los directivos del departa de gestión), aislamiento de problemas (un fallo de una de las redes no afecta al resto) y, por último mayor interoperatividad (traba con routers multiprotocolo pue intercambiar datos entre redes tas, como Ethernet, Token Ring, etcétera).

Direcciones especiales

Lo anteriormente descrito refer las clases, atañe exclusivamente asignación de direcciones IP den la Internet. Si diseñamos una red que no vaya a estar conectada a

(situación no muy común hoy día), podemos hacer uso de cualquier conjunto de direcciones IP. Sólo existen cuatro limitaciones (intrínsecas al protocolo) a la hora de escoger direcciones IP, pero que reducen en cierta medida el número de nodos disponibles por clase expuestos en el apartado anterior. La primera es que no se pueden asignar direcciones que comiencen por 0. Dichas direcciones hacen referencia a nodos dentro de la red actual. La segunda es que la red 127 se reserva para los procesos de resolución de problemas y diagnosis de la red. De especial interés resulta la dirección 127.0.0.1, bucle interno (*loopback*) de la estación de trabajo local. La tercera consiste en que las direcciones IP de nodos no pueden terminar en 0 (en 0, o cualquier otro valor base del rango de una subred), pues así concluyen las redes. Por último tenemos que, cuando asignamos direcciones IP a nodos, no podemos emplear el valor 255 (o cualquier otro valor final del rango de una subred). Este valor se usa para enviar mensajes a todos los elementos de una red (*broadcast*). Por ejemplo, si enviásemos un mensaje a la dirección 192.168.2.255, estaríamos enviando el mensaje a todos los nodos de la red de clase C 192.168.2.xx

Ahora bien, si queremos crear una red local que tenga acceso exterior, hemos de tener en cuenta una serie de restricciones adicionales. Si nos han concedido un rango de direcciones IP, lo suficientemente amplio como para asignar una dirección a cada puesto de nuestra red, no tendremos más problemas. En caso contrario (lo más habitual), para poder ofrecer acceso a Internet a los nodos de nuestra red, hemos de emplear un servidor proxy, o cualquier otro mecanismo que enmascare las direcciones IP de nuestra intranet, esto es, una o varias máquinas (con acceso a Internet), solicitarán los paquetes que requieran todos los puestos de nuestra red local. Cuando un paquete es recibido, éste es reenviado al puesto que originalmente lo solicitó. No obstante, bajo este esquema, la elección del rango de direcciones IP de nuestra red no puede ser aleatoria. En Internet (y en cualquier red IP), no pueden existir dos direcciones IP idénticas al mismo tiempo. Por ello, no podemos elegir un conjunto de direcciones IP al azar, asignarlos a los nodos de nuestra red, y conectarlos a Internet directamente.

En este punto introducimos los conceptos de lo que se conoce como direcciones IP reales, y direcciones IP reservadas. Las reales son las direcciones que pueden tomar los nodos conectados a Internet, excluyendo por un lado las reservadas y, por otro, las indicadas en el párrafo anterior. Las reservadas son una serie determinada de rangos de direcciones IP que, a fin de que pudieran usarse para la confección de redes locales, fueron excluidas de Internet. Si está considerando crear una intranet, escoja las direcciones IP de su red entre alguno de los rangos "reservados", incluidos en la tabla B. Si se conecta a Internet a través de Infovía, evite emplear la red 10.xx.xx.xx, pues le puede dar problemas.

Máscaras de red

La elección del término "máscara" no fue en absoluto arbitrario. Las máscaras en general y por definición, aplicadas sobre un objeto, implican ocultar o modificar el aspecto final del mismo. En este caso, la máscara de red es un valor con el mismo formato e importancia que la dirección IP. Aplicada sobre la dirección IP de un adaptador de red, establece dónde termina la dirección de la red externa y dónde

Bibliografía recomendada

La documentación tanto impresa como electrónica publicada con relación al protocolo TCP/IP es abrumadora. En realidad cualquiera de los muchos libros disponibles le pueden servir como referencia a la hora de idear e instalar una red TCP/IP. Desde aquí les sugerimos unos cuantos títulos y cierta documentación electrónica de interés.

- Andrew S. Tanenbaum; *Computer Networks*; Ed. Prentice Hall. Impresionante obra del mundialmente conocido Dr. Tanenbaum que cubre no sólo aspectos del protocolo TCP/IP, sino todo lo relacionado con redes informáticas en general, describiendo con detalle capa a capa (según el modelo OSI), las más eminentes tecnologías de cada una de ellas, desde la capa física a la de aplicación, incluyendo una fuerte base teórica/matemática de las mismas. Imprescindible para estudiantes de carreras técnicas interesados en éstas tecnologías, si bien, excesivamente complejo y profundo para usuarios en general.
- Craig Hunt; *Network Administration*; Ed. O'Reilly & Associates. Una guía completa de cómo configurar, mantener y actualizar redes TCP/IP. Cubre desde los aspectos teóricos, hasta la configuración final de las aplicaciones, pasando por la configuración de los distintos servicios y la discusión de diversos aspectos de la seguridad.
- Raya J.L. y Rodrigo V.; *Domine TCP/IP*; Ed. RA-MA. Una amplio manual de aprendizaje que de forma sencilla introduce al lector en todo lo relacionado con la teoría de las redes locales. Cubre desde los aspectos físicos de las redes hasta la configuración de servidores.
- S. Feit; *TCP/IP Arquitectura, protocolos, implementación y seguridad*; Ed. Mc Graw Hill. Obra tan completa como su propio título. De fácil lectura abarca todos los aspectos precisos para la confección de redes TCP/IP de cualquier tipo. A destacar el interesante apartado dedicado a la seguridad.
- Varios; *RFC791.txt, RFC950.TXT, RFC1180.TXT, RFC1208, RFC1219.TXT*; http://www.rfc-editor.org/rfc.html. Documentación electrónica (*Request for Coments*), referente a temas relacionados con TCP/IP. Los documentos aquí indicados cubren respectivamente: protocolo Internet, Procedimiento estándar de subred in Internet, Tutorial TCP/IP, Términos sobre redes IP, e Información sobre la numeración de subredes.

comienza la dirección de la red local o segmento al que se encuentra conectado dicho adaptador. Si nos pusiéramos en el caso de un simple cliente de red con un adaptador y una sola dirección IP, la máscara del adaptador definiría las direcciones IP de las máquinas que nos podremos encontrar conectadas al mismo segmento de red (mismo "cable") que nuestro equipo.

Igualmente, los segmentos son la base de lo que más adelante definiremos como rutas de datos, las cuales, son base a su vez del método que nos permite transferir información entre distintas redes locales IP. Así pues, las máscaras dividen redes en subredes y esas subredes, por medio de otras máscaras, pueden dividirse igualmente en redes de menor tamaño. A partir de una máscara de red resulta muy sencillo calcular el número de nodos que pertenecen al mismo segmento. Supongamos la máscara de una red de clase C (255.255.255.0), representada en binario: 11111111.11111111.11111111.0000000. Ahora simplemente hemos de asociar mentalmente los 1 con la parte de la red externa y los 0 con la red local. El número total de nodos por segmento en esta red será el máximo número que podamos representar con un número binario de tantas cifras como ceros (de red local), tengamos. En este caso tenemos 8 ceros, luego son 2^8 nodos, o lo que es lo mismo: 256 (habría que excluir aquellos nodos con direcciones IP no permitidas).

Por otro lado, como ya mencionamos, podemos dividir una red en subredes de menor tamaño. La máscara de cada uno de los nodos de los nuevos segmentos de red vendrá determinada por el número máximo de puestos de cada segmento. Podemos crear subredes capaces de albergar cualquier número de puestos, aunque en la medida de lo posible, deberán evitarse números que no sean potencia de 2 (2, 4, 8, 16...). Siguiendo esta recomendación, hallar la máscara de red es sencillo. Tan sencillo como construir un número binario dividido en octetos, con tantos ceros al final como bits precisemos para representar el número de puestos. Por ejemplo, suponga que deseamos dividir una clase C (256 nodos), en 8 redes de 32 puestos. Necesitaríamos 5 bits para representar los 32 puestos (pues 2^5=32), luego la máscara en binario de cada uno de los puestos sería: 11111111.11111111.11111111.1110000, o lo que es lo mismo, 255.255.255.224 en decimal.

Tablas de rutas

En el apartado anterior discutimos cómo han de emplearse las máscaras a la hora de dividir una red IP. Ahora describiremos cómo se realiza la transmisión de datos tanto entre los nodos de una red local, como entre nodos de distintas redes locales conectadas mediante *gateways*. Esto nos dará ya una visión completa de lo que es el protocolo. Entender cómo se realiza el transporte de datos implica haber asimilado correctamente todos los conceptos hasta aquí expuestos.

Los sistemas operativos actuales tienden a simplificar la conexión a Internet hasta un punto en el cual, no es preciso conocer prácticamente nada del protocolo en el que se basa

Una dirección IP, combinada con una máscara devuelve la dirección base de la subred a la que pertenece la dirección IP. Como se expuso en el apartado previo, el rango de direcciones disponibles a partir de la dirección base de la subred, dependerá de la máscara. Para hallar tal dirección base, pasamos la dirección IP y la máscara a binario. A continuación generamos un nuevo número a partir de la dirección IP, sustituyendo con un 0 los bits que igualmente son 0 en la máscara.

Cuando a un segmento de este tipo se le asocia un *gateway* y un dispositivo de salida, tenemos una ruta de datos. Las rutas son como los caminos que sirven para dirigir datagramas de datos en una red IP. Dentro de la ruta (y a efectos prácticos), el segmento (red destino) es algo similar a un patrón contra el cuál se irán contrastando las direcciones IP de los datagramas que van recibiendo o generando los adaptadores de red. Si la dirección destino del datagrama IP pertenece al segmento de red de la ruta de datos, se reenviará a través del adaptador y a la dirección IP asociada a tal ruta.

De esta forma, todo nodo conectado a una red IP ha de tener una tabla de rutas, que no es otra cosa que un conjunto de rutas de datos. La tabla de rutas de un nodo, si está correctamente configurada, debería poder determinar siempre el camino que ha de tomar cualquier paquete de datos que el nodo envíe o reciba. A grosso modo, cuando un nodo recibe un datagrama, consulta su dirección de destino. Posteriormente, y de acuerdo a su tabla de rutas, consulta si dicha dirección pertenece a alguna de las subredes a las cuales el nodo tiene acceso. Para ello, en primer lugar toma la dirección y máscara de cada una de las rutas. Averigua su dirección base mediante el procedimiento arriba descrito. Una vez hecho esto, aplica el mismo algoritmo a la dirección destino del datagrama, empleando la misma máscara de la ruta. Si el resultado de ambas operaciones es idéntico, implica que el datagrama va destinado a dicha subred, y por tanto hemos de reenviarlo a través del adaptador pertinente y a la máquina especificada en la ruta (este proceso se describe más técnicamente en la Figura 5).

En caso de no encontrar ruta válida, los nodos suelen disponer de una ruta por defecto o *default* (si disponen de acceso al exterior), que

Glosario de términos relacionados con TCP/IP

ARP: *Address Resolution Protocol*. Protocolo que realiza la conversión de direcciones IP a las direcciones hardware de los dispositivos asociados.

Broadcast: dirección que se emplea para mandar mensajes a todos los puestos de una red. Las direcciones de *broadcast* han de incluir el valor 255. Por ejemplo, 192.168.255.255 hace referencia a la red 192.168.

Datagrama: unidad de datos de formato simple.

CRC: *Cyclic Redundancy Check*. Método matemático que aplicado a un conjunto de datos produce una salida que contrastada en el equipo remoto, incrementa notablemente la fiabilidad de los datos transmitidos.

Dirección IP: dato de 32bits dividido en octetos que identifican unívocamente nodos de una internet (con i en minúsculas, véase más abajo el significado).

DNS: *Domain Name System*. Servidor de dominios. Base de datos distribuida a través de Internet. A partir de un nombre de máquina es capaz de devolver su número IP y viceversa.

Dominio: parte de la jerarquía del nombre de una máquina. Por ejemplo: idg.es.

Encapsulado: técnica por la cual un protocolo almacena entre sus datos la integridad del paquete de datos del protocolo superior.

Fragmentación: proceso por el cual un datagrama IP es dividido en piezas más pequeñas, a fin de cumplir los requerimientos de tamaño de un tipo de red determinado.

FTP: *File Transfer Protocol*. Protocolo de transferencia de archivos. Ampliamente usado en Internet.

Gateway: puerta de enlace entre dos o más redes.

HTTP: *Hyper Text Transfer Protocol*. Protocolo base de la Web.

internet: (con i en minúsculas). Un grupo de redes conectadas mediante routers.

Internet: (nótese I mayúscula). La Red de redes.

IP: *Internet Protocol*. Base del conjunto de protocolos que forman Internet.

NFS: sistema de archivos de red desarrollado por Sun Microsystems.

NIC: *Network Information Center*. Responsable de la administración de Internet, encargado de asignar direcciones IP y nombres de red.

OSI: *Open Systems Interconnection*. Estándar internacional para facilitar la comunicación entre ordenadores.

Puerto: abstracción empleada por los protocolos de transporte a fin de distinguir entre múltiples conexiones simultáneas en un solo nodo de la red.

Proxy: mecanismo que permite compartir una única conexión a una red externa entre todos los puestos de una red local.

RIP: *Routing Information Protocol*. Protocolo empleado por los *routers* para intercambiar información.

SMTP: *simple Mail Transfer Protocol*. Protocolo de envío de correo electrónico.

SNMP: *simple Network Management Protocol*. Protocolo que gestiona información sobre el estado de la red.

TCP: *Transmission Control Protocol*. El protocolo de transporte de datos más popular de Internet.

Telnet: protocolo para establecer conexiones entre terminales remotos.

UDP: *User Datagram Protocol*. Protocolo de transporte de datos no tan fiable como TCP.

apunta a una máquina, una puerta de enlace, que supuestamente será capaz de gestionar los paquetes no pertenecientes al grupo de subredes directamente accesibles.

Un caso práctico

La mejor forma de asimilar el proceso de transporte de datos en redes TCP/IP (comúnmente denominado rutado o encauzado de datos), es trabajar directamente sobre un caso práctico. En la Figura 6 hemos representado una red IP formada por tres redes de clase C, interconectadas mediante un *router* multiprotocolo (Token Ring/Ethernet). Nótese que este esquema no pretende ser un modelo óptimo, ni tan siquiera asemejarse a uno real. El criterio seguido en su desarrollo ha sido el de intentar integrar en el menor espacio, el mayor número de elementos y combinaciones distintas que podemos encontrarnos en una red IP. Así pues, y como podemos ver, la red 1 es una subred tipo Token Ring de clase C (194.100.1.0), dividida a su vez en dos redes de 127 nodos (máscara 255.255.255.128), conectadas entre sí mediante un *gateway*. Por su parte las subredes 2 y 3 son de tipo Ethernet con cabida para 254 nodos (máscara 255.255.255.0). El acceso a Internet se hace a través del único nodo de la red 3, que se conecta al exterior a través del adaptador con dirección 194.100.4.1. Igualmente, en la parte inferior del gráfico, incluimos las tablas de rutas de algunos de los nodos de la red que nos ayudarán a clarificar los dos casos descritos (sólo las rutas externas, excluyendo el *loopback* y la ruta propia del adaptador).

Por regla general, la tabla de rutas del típico cliente de red, perteneciente a una red local con un único acceso exterior, se compone de tres

rutas de datos. La primera e indispensable es ruta del bucle interno (*loopback*): IP 127.0.0.0, máscara 255.0.0.0. La segunda es la que hace referencia a la propia red local, por ejemplo: 194.100.2.0, máscara 255.255.255.0. Si la red local dispone de acceso exterior, restaría incluir la ruta por defecto (*default route*), apuntando a la máquina que ejerza de puerta de enlace (*gateway*), 194.100.2.1 por ejemplo. Por su parte, los *gateways* disponen de al menos una ruta adicional por cada conector (entrada) de red de más instalado.

Vamos a estudiar dos casos de cómo se realizaría el paso de mensajes. El primero entre dos nodos de la red, y el segundo entre un nodo de la red y el exterior.

De GAMMA a LAMBDA. Supongamos que nuestro DNS (*Domain Name System*), ha devuelto a GAMMA la dirección IP de LAMBDA: 194.100.2.50. Como sucederá en cada uno de los pasos posteriores, aplicamos la máscara de GAMMA (255.255.255.128) a la dirección de LAMBDA, dando por resultado 194.100.2.0. No encaja con la red destino de la ruta 1, luego mediante la ruta 2 (*default*) se envía a EPSILON. En EPSILON se le aplican también a la dirección IP destino las máscaras de sus rutas con idéntico resultado: no pertenece a la subred 194.100.1.0, ni a la 194.100.1.128. En consecuencia, de igual forma se emplea la ruta por defecto. Llegamos al ROUTER, donde encaja con la máscara y dirección de la tercera ruta, con lo que el datagrama es enviado a la red local 2.0 a través del adaptador ETH0. Una vez en la red local 2.0 LAMBDA recibe y retira el mensaje de la red.

De BETA a Internet. Lo primero que llama la atención es que pese a que BETA es un simple cliente de red, dispone de tres rutas. Esto se debe a que su red local, la 194.100.1.128, está conectada a dos redes: a la 194.100.1.0, y al resto de la intranet. Por lo tanto (y aunque no sea imprescindible), dispone de un segundo *gateway*, aparte del indicado en la ruta por defecto, para poder enviar paquetes a ambas redes. Observe el detalle de la máscara de red 255.255.255.128, que divide a la 1.0 en dos subredes con nodos que van por un lado, desde el 1.1 hasta el 1.127, y por otro, desde el 1.129 hasta el 1.254. Si al datagrama le suponemos una dirección aleatoria de Internet, por ejemplo 200.100.200.100, no encajará con ninguna de las rutas de la tabla de BETA, con lo que sería enviado al ROUTER. Una vez allí, tampoco encajaría con ninguna de sus rutas, pues no pertenece a la red 194.100.1, a la 194.100.2, ni a la 194.100.3, con lo que de nuevo se enviaría a la ruta por defecto, en este caso ALPHA, que lo único que hace es de nuevo determinar si el paquete pertenece a alguna de las redes interiores (1.0, 2.0, o 3.0), y en caso contrario, lo envía al exterior a través del adaptador 194.100.4.1.

Conclusiones

El crecimiento exponencial y la popularización de Internet han propiciado que el conjunto de protocolos TCP/IP y asociados sean actualmente los de mayor relevancia en el mundo de las redes. El número de aplicaciones desarrolladas para el conjunto de protocolos de Internet crece día a día. Al estar basadas en un protocolo abierto y contar con un mercado potencial tan grande como pueda ser Internet, las aplicaciones TCP/IP y derivados, gozan de una excelente calidad y mejor precio. De esta situación se favorecen las actuales intranets (redes IP privadas de carácter corporativo) y las emergentes extranets, pues tienen a su disposición la más avanzada tecnología por sólo una fracción del coste que les supondría implantar el mismo nivel de servicios bajo un conjunto de protocolos de red privados.

Según el modelo actual (IPv4), el rango de direcciones de Internet puede dar cabida a más de cuatro mil millones de ordenadores. Esta cifra, que en principio puede parecer más que suficiente, se verá tremendamente incrementada en la nueva versión del protocolo: IPv6 (IP versión 6). Las direcciones de esta nueva versión pasarán a ser de 128 bits, bajo un protocolo totalmente compatible con su predecesor, si bien incluirá un buen número de mejoras que harán de las futuras redes IP un tipo de red mucho más manejable que el actual.

Routers y bridges

Los routers y bridges son dispositivos que se utilizan para compartir información entre redes y sistemas. A menudo ambos términos se confunden y son usados indistintamente.

Los routers trabajan a nivel de la capa de red, y se les suele asociar a un protocolo, como por ejemplo IP o IPX, en cuyo caso hablamos de un router IP, un router IPX e, incluso, de router IP/IPX en el caso de que pueda gestionar los dos. Este tipo de dispositivos reducen el tráfico de datos de la red, puesto que al trabajar a nivel de red, disponen de la "inteligencia" necesaria para distinguir qué paquetes pertenecen a una red y qué paquetes pertenecen a otra. Ningún paquete es enviado a una red no apropiada, con lo que la congestión se reduce al distribuirse la carga de la red global entre los distintos segmentos de la misma.

Los bridges, sin embargo, gestionan el tráfico de datos a nivel de la capa física y, por tanto, no se preocupan en absoluto del protocolo que se encuentre por encima. La transición de datos de una red a otra se realiza muy rápidamente pero tiene el inconveniente de que, al ser un simple puente, toda la información que se produzca en una red es transmitida a la otra y viceversa. Ello conlleva un considerable aumento de la congestión.

Una buena medida sería utilizar bridges sólo si se van a conectar redes que utilicen protocolos múltiples y que intercambien un gran volumen de información. En cualquier otro caso, un router es la elección más apropiada. ◆

Javier Cáceres.
Experto en Sistema operativo Unix y en redes.