1 DIRECCIONAMIENTO Y RETRANSMISIÓN

1.1 El direccionamiento IP

La versión 4 del protocolo IP, que es la versión más extendida en la actualidad, define direcciones de 32 bits que se suelen representar en notación decimal con puntos. Por ejemplo, una dirección válida sería la siguiente:

200.27.4.112

Si bien el objetivo de dicha notación es simplificar la compresión y memorización de las direcciones IPs, en algunos casos puede llevar a confusión. Por este motivo, es de utilidad presentar también la notación binaria equivalente. Así, la dirección anterior en notación binaria es:

200.27.4.112 = 11001000.00011011.00000100.01110000

La notación binaria deja patente que en cada octeto estamos limitados a un número entre 0 y 255, lo que por otra parte es lógico.

El direccionamiento debe concebirse, en la medida de lo posible, para simplificar la comunicación. Pensemos por ejemplo en la numeración telefónica. Un número de teléfono en Granada capital está formado por el prefijo internacional (+34), el prefijo provincial (958) y tradicionalmente se han venido asignando numeraciones consecutivas por zonas. Esta división jerárquica del número de teléfono simplifica la instauración de las comunicaciones. Imaginemos por ejemplo una persona en Londres que quiera establecer una conversación telefónica con una empresa granadina. El comienzo del número con el prefijo +34 indicará a la central telefónica local que debe encaminar la llamada al exterior del país y en concreto a España. Dentro de España, sólo se deben comprobar los tres dígitos siguientes para saber que la llamada debe encaminarse hacia Granada, y así sucesivamente. Si no se siguiera dicho procedimiento, en cada central de telefonía sería necesario guardar una lista con todos los números de teléfono a nivel internacional. Dicha lista, de una envergadura gigantesca, sería más compleja de utilizar y retrasaría las comunicaciones. Otro problema fundamental sería la actualización de las listas de teléfono: una nueva contratación de línea telefónica implicaría una actualización en cada central telefónica en el mundo. No hace falta conocer el ratio de altas en líneas telefónicas para darse cuenta que dicha actualización sería inmanejable.

El direccionamiento IP sigue la misma estrategia. Para ello, utiliza la máscara de subred. La máscara de subred divide la dirección IP en dos partes: una correspondiente a la subred y otra al dispositivo dentro de la misma. El término subred viene determinado por motivos históricos, si bien cuando decimos subred nos referimos a la red donde está ubicado el dispositivo. La especificación de la máscara de (sub)red puede hacerse de dos maneras. La forma más intuitiva es siguiendo la misma notación que las direcciones IP: 32 bits con 4 octetos separados por puntos, bien en notación decimal, bien en notación binaria. Así, volviendo al ejemplo anterior tenemos:

Dirección IP ➔ 200.27.4.112 = 11001000.00011011.00000100.01110000

Máscara de (sub)red ➔ 255.255.255.0 = 11111111.11111111.11111111.00000000

En la máscara de subred, los 1s representan la porción de la dirección IP que representa la subred, mientras que los 0s representan la porción para direccionar el dispositivo (host) dentro de la red. Por simplicidad, las máscaras se restringen a presentar todos los 1s agrupados en la parte

izquierda y consecuentemente todos los 0s en la parte derecha (esta es la recomendación original en el RFC 950). Esto posibilita una representación comprimida de la máscara de subred, que es la más extendida en los documentos escritos (no así en los protocolos de comunicaciones), donde se especifican únicamente el número de 1s en la máscara. Así, podemos especificar la misma información anterior de la siguiente manera comprimida:

200.27.4.112/24

donde el /24 implica una máscara de subred 255.255.255.0.

Dada la información de la dirección IP y la máscara de subred, basta con realizar la operación AND binaria entre éstas para obtener la dirección de la subred a la que pertenece el dispositivo:

```
                200.27.4.112   = 11001000.00011011.00000100.01110000
                     &                              &
                255.255.255.0 = 11111111.11111111.11111111.00000000
                                ---------------------------------------------------
Subred ➔        200.27.4.0     = 11001000.00011011.00000100.00000000
```

Nótese que la elección de la máscara de subred está relacionada con el número de dispositivos o hosts que se quieren albergar en la misma, bien durante el diseño inicial bien teniendo en cuenta las posibilidades de crecimiento en el futuro. Así, una máscara /24 dispone de ocho 0s, por lo que es capaz de direccionar un total de 2^8 o 256 dispositivos (luego matizaremos este punto). En particular, todas las direcciones entre la 200.27.4.0 y la 200.27.4.255 pertenecerán a la misma subred que 200.27.4.112. Podemos comprobarlo siguiendo la misma estrategia de antes:

```
                200.27.4.0     = 11001000.00011011.00000100.00000000
                     &                              &
                255.255.255.0 = 11111111.11111111.11111111.00000000
                                ---------------------------------------------------
Subred ➔        200.27.4.0     = 11001000.00011011.00000100.00000000

                200.27.4.255   = 11001000.00011011.00000100.11111111
                     &                              &
                255.255.255.0 = 11111111.11111111.11111111.00000000
                                ---------------------------------------------------
Subred ➔        200.27.4.0     = 11001000.00011011.00000100.00000000
```

Si bien acabamos de decir que el número de dispositivos direccionables dentro de una subred es igual a 2 elevado al número de 0s de la máscara, esto no es en realidad así. Precisamente, la primera y última direcciones dentro de una subred, es decir, la dirección con la parte de host todo a 0s y a 1s, respectivamente, son direcciones reservadas. Así, en el ejemplo anterior, la 200.27.4.0 y la 200.27.4.255 son direcciones reservadas. La dirección IP donde la parte de host está a 0 coincide con la dirección de la subred como ente. Posteriormente veremos que el encaminamiento, con el objetivo de evitar un enorme consumo de memoria que por otra parte retrasaría las comunicaciones, se basa en direcciones de subred y no de hosts. La dirección IP donde la parte de

host está a 1s es la llamada de difusión (broadcast), y se utiliza cuando se necesita mandar información a todos los dispositivos de la subred.

Existen también otro conjunto de direcciones en Internet que son de carácter reservado: las direcciones privadas. Dichas direcciones tienen una funcionalidad similar a las extensiones en una centralita telefónica. En una centralita de una empresa, por ejemplo en la UGR, se pueden configurar gran cantidad de teléfonos que utilizan un número reducido de líneas de salida a la Red Telefónica Conmutada (RTC). Esto tiene dos beneficios económicos claros: las llamadas dentro de la empresa pueden ser gratuitas y el coste de instalación es el asociado al reducido número de líneas al exterior, y no al número de teléfonos empleados. Por otro lado, el mecanismo para acceder a los teléfonos desde fuera de la empresa pasa por llamar en primer lugar a la centralita, que dispondrá de un número de teléfono convencional (en Granada, un 958…) y que ésta pase la llamada (automáticamente o no) a la terminal de destino. Esto tiene otro beneficio adicional: se puede utilizar la misma numeración dentro de empresas distintas puesto que no hay confusión posible. Por tanto, los números en una centralita pueden ser de longitud reducida. Por ejemplo, en la UGR se utilizan 5 dígitos en las extensiones.

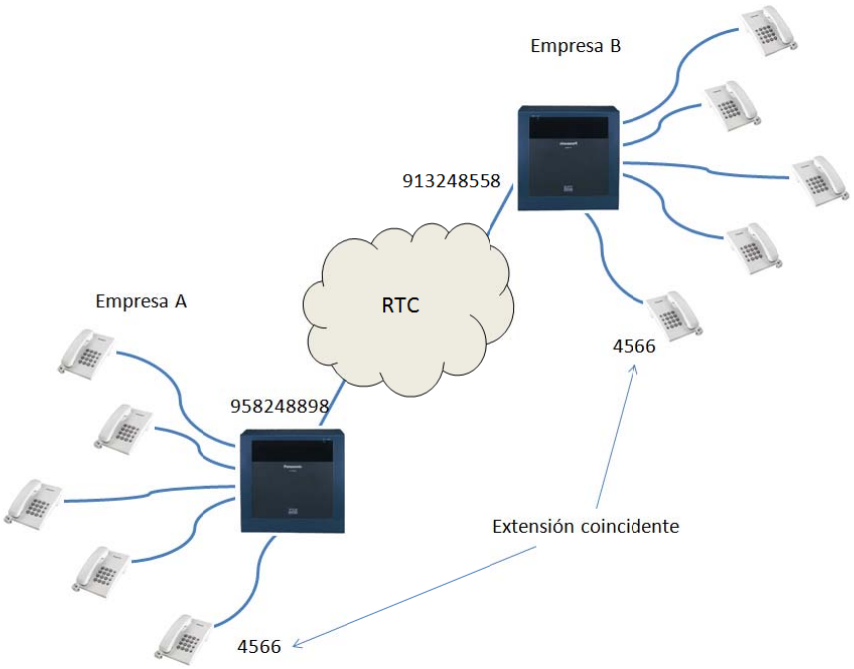
El objetivo de las direcciones IP privadas es el mismo. Las IP privadas sólo tienen sentido en el interior de una red corporativa. Si se quiere conectar ésta con Internet se requerirá de, al menos, una dirección IP pública en su router de acceso, al igual que pasa con las líneas de salida en las centralitas. Las comunicaciones de los hosts en el interior de una red corporativa con Internet se realizan a través de dicho router de acceso.

Las direcciones IP privadas son:

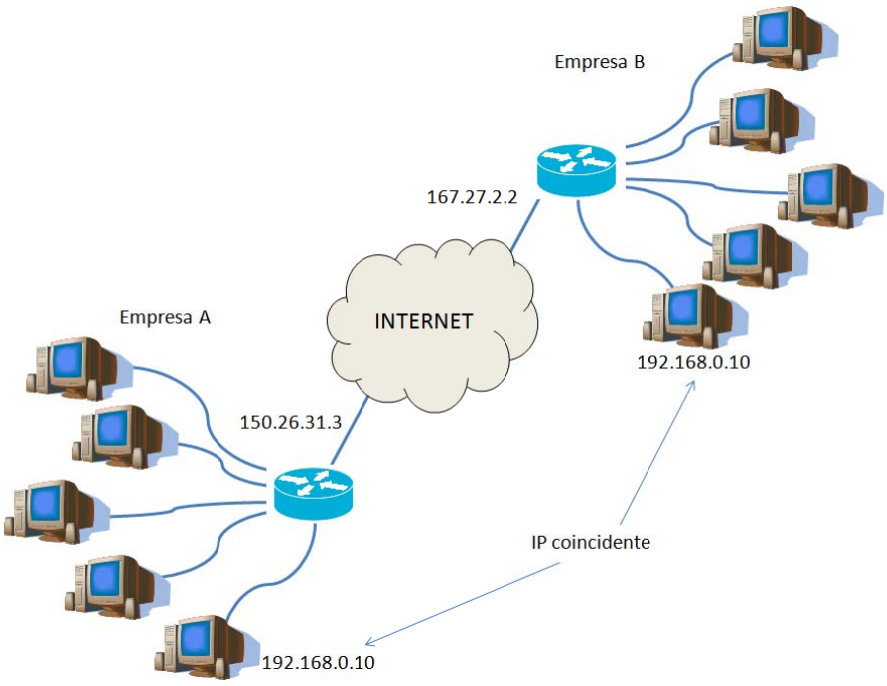
- Las pertenecientes a la subred 10.0.0.0/8
- Las pertenecientes a la subred 172.16.0.0/11
- Las pertenecientes a la subred 192.168.0.0/16

En la Figura 1 se ilustra la similitud entre las extensiones en una centralita y las direcciones IP privadas. Nótese que esta estrategia posibilita la conexión a Internet de muchos más dispositivos que la limitación impuesta por el uso de 24 bits en las direcciones. A la par, se reduce el problema del encaminamiento, puesto que una única dirección IP de destino (la del router de acceso) permite llegar a todos los ordenadores de la red corporativa. No obstante, dicha estrategia también introduce problemas adicionales que estudiaremos más adelante en la asignatura.

Para finalizar esta introducción al direccionamiento, es necesario determinar la noción de subred en una topología de red. De forma general, podemos establecer que cada encaminador supone un cambio de subred. Esto contrasta con lo que ocurre con otros dispositivos de interconexión asociados a capas inferiores, como los conmutadores y concentradores. Dichos dispositivos NO suponen un cambio de subred. Para ilustrar esta idea, imaginemos la topología en la Figura 2, que bien podría representar la red corporativa de una empresa con tres departamentos, interconectados cada uno de ellos con una subred. Las subredes de los tres departamentos se interconectan utilizando dos routers. El segundo de ellos, el router de acceso, posibilita la conexión de todos los dispositivos de la red con Internet a través de una última subred. En este punto cabe resaltar que las direcciones IPs no se asocian a un dispositivo, sino a la interfaz del dispositivo con



(a)



(b)

Figura 1: Similitud entre las extensiones en centralitas telefónicas (a) y las direcciones IPs privadas en redes corporativas (b).

la red. Así, el dispositivo A tendrá una dirección IP para su interfaz con la subred 1, mientras que el router 2 tendrá tres direcciones IP: una para la interfaz con la subred 2, otra para la interfaz con la subred 3 y finalmente otra para la interfaz con la subred 4.

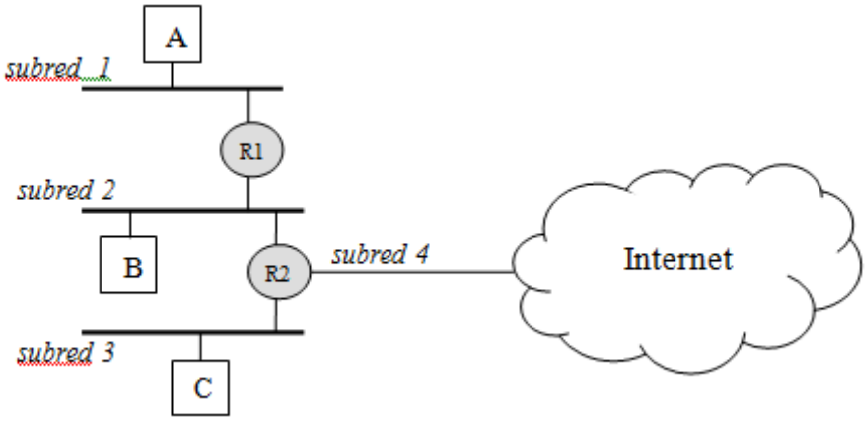


Figura 2: Topología ejemplo

Una forma directa de instanciar la topología anterior sería utilizando un conmutador para cada subred de la red corporativa, como se muestra en la Figura 3. Las ventajas de dicho despliegue son principalmente dos: capacidad plug-and-play de los conmutadores y mayor funcionalidad y eficiencia de los conmutadores en comparación a los concentradores, como se ha discutido previamente en la asignatura. El despliegue de la Figura 3 muestra lo comentado anteriormente: los encaminadores suponen un cambio de subred, mientras que los conmutadores no lo suponen.

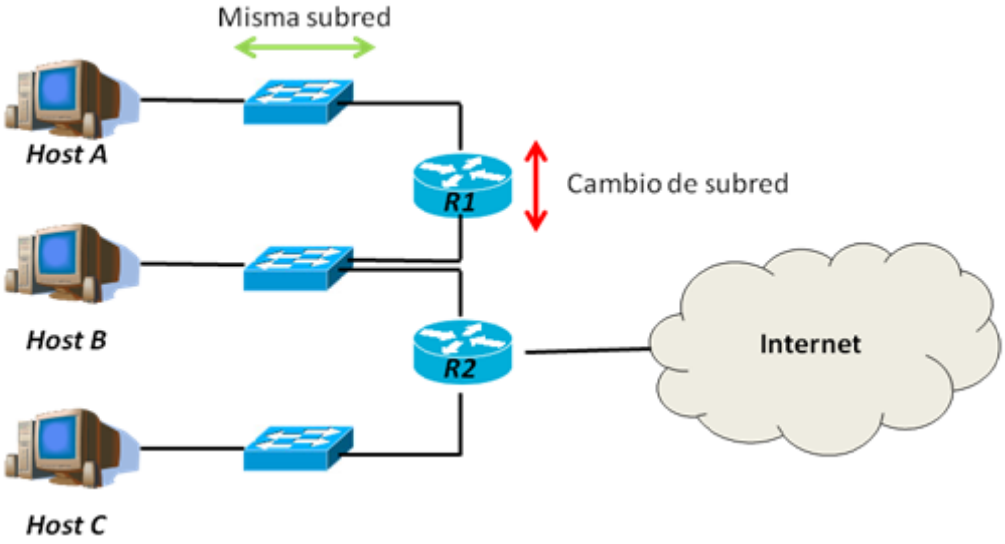


Figura 3: Topología ejemplo desplegada utilizando conmutadores por cada subred de la red corporativa.

Una estrategia muy intuitiva para determinar las subredes de una topología viene especificada en el *Computer Networking. A Top-down Approach.* de James F. Kurose y Keith W. Ross: "Para determinar las subredes, separe cada interfaz de los hosts y routers, creando redes aisladas. Dichas redes aisladas se corresponden con las subredes." Así, en el ejemplo de la Figura 3, las subredes se pueden determinar fácilmente de acuerdo a la Figura 4:

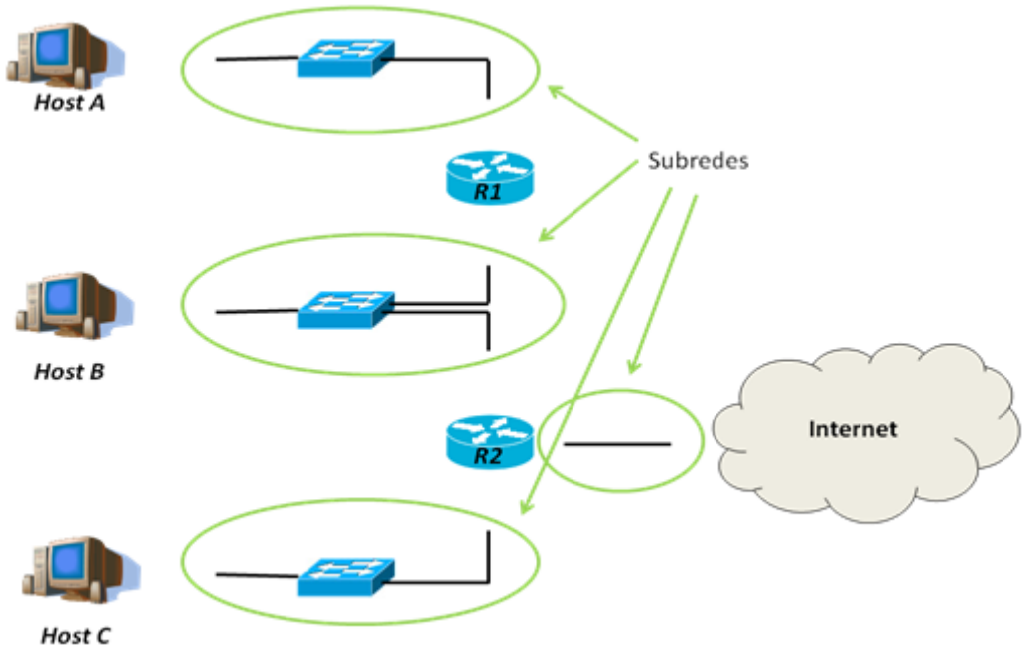


Figura 4: Subredes en la topología ejemplo.

Como ejemplo ilustrativo, diseñaremos las direcciones IP considerando las subredes de las Figuras 2-4. Las subredes 1 y 3 tienen dos dispositivos cada una: un host y un router. La subred 3 tiene tres dispositivos: un host y dos routers. La subred 4 conecta dos dispositivos, en este caso dos routers. Si bien ésta última se quedará así en el futuro, puesto que establece la conexión de la red corporativa con el proveedor de servicios de Internet (ISP por sus siglas en inglés), las otras subredes pueden crecer en el futuro al añadir hosts adicionales. Elegiremos una máscara con un total de 5 ceros (/27) para direccionar la porción de direcciones del host, lo que equivale a una capacidad máxima de cada subred de incluir 2^5-2 (recordemos las dos direcciones reservadas) o 30 dispositivos. Partiremos de la dirección privada 192.168.0.0 para la subred 1. Así, las direcciones en dicha red serían:

Subred ➔ 192.168.0.0 = 11000000.10101000.00000000.00000000

Disp. #1 ➔ 192.168.0.1 = 11000000.10101000.00000000.00000001

Disp. #2 ➔ 192.168.0.2 = 11000000.10101000.00000000.00000010

Disp. #3 ➔ 192.168.0.3 = 11000000.10101000.00000000.00000011

…

Disp. #30 ➔ 192.168.0.30 = 11000000.10101000.00000000.00011110

Broadcast ➔ 192.168.0.31 = 11000000.10101000.00000000.00011111

donde la parte subrayada es porción de la dirección destinada a diferenciar el host. Vemos que la numeración decimal es muy intuitiva en este caso: la dirección acabada en 0 es la dirección de red y la acabada en *n* hasta 30 hace referencia al host *n*.

Si queremos asignar las direcciones de la subred 2 inmediatamente a continuación de las de la subred 1, para evitar dejar direcciones IP entre medias sin asignar, éstas serían:

Subred ➔ 192.168.0.32 = 11000000.10101000.00000000.00100000

Disp. #1 ➔ 192.168.0.33 = 11000000.10101000.00000000.00100001

Disp. #2 ➔ 192.168.0.34 = 11000000.10101000.00000000.00100010

Disp. #3 ➔ 192.168.0.35 = 11000000.10101000.00000000.00100011

…

Disp. #30 ➔ 192.168.0.62 = 11000000.10101000.00000000.00111110

Broadcast ➔ 192.168.0.63 = 11000000.10101000.00000000.00111111

Si bien la notación binaria sigue siendo intuitiva, la decimal no lo es ya tanto. Podemos observar que, tanto en binario como en decimal, la dirección de subred de la subred 2 sucede inmediatamente a la dirección de broadcast de la subred 1. Adicionalmente, si aplicamos una operación AND con la máscara /27 a cualquiera de las direcciones anteriores, obtenemos la dirección de subred 192.168.0.32.

Finalmente, para la subred 3:

Subred ➔ 192.168.0.64 = 11000000.10101000.00000000.01000000

Disp. #1 ➔ 192.168.0.65 = 11000000.10101000.00000000.01000001

Disp. #2 ➔ 192.168.0.66 = 11000000.10101000.00000000.01000010

Disp. #3 ➔ 192.168.0.67 = 11000000.10101000.00000000.01000011

…

Disp. #30 ➔ 192.168.0.94 = 11000000.10101000.00000000.01011110

Broadcast ➔ 192.168.0.95 = 11000000.10101000.00000000.01011111

De nuevo, la dirección de subred de la subred 3 sucede inmediatamente a la dirección de broadcast de la subred 2 y si aplicamos una operación AND con la máscara /27 a cualquiera de las direcciones anteriores, obtenemos la dirección de subred 192.168.0.64.

Finalmente, la subred 4, que no tiene perspectivas de crecer, puede utilizar una máscara de 2 0s (/30). En este caso utilizaremos direcciones públicas:

Subred ➔ 150.214.190.0 = 10010110.11010110.10111110.00000000

Disp. #1 ➔ 150.214.190.1 = 10010110.11010110.10111110.00000001

Disp. #2 ➔ 150.214.190.2 = 10010110.11010110.10111110.00000010

Broadcast ➔ 150.214.190.3 = 10010110.11010110.10111110.00000011

donde el Disp. #2 será la dirección del punto de acceso que nos ofrece el ISP para la conexión a Internet.

Siguiendo las especificaciones anteriores, una asignación de direcciones potencial para la topología de ejemplo aparece en la Figura 5.

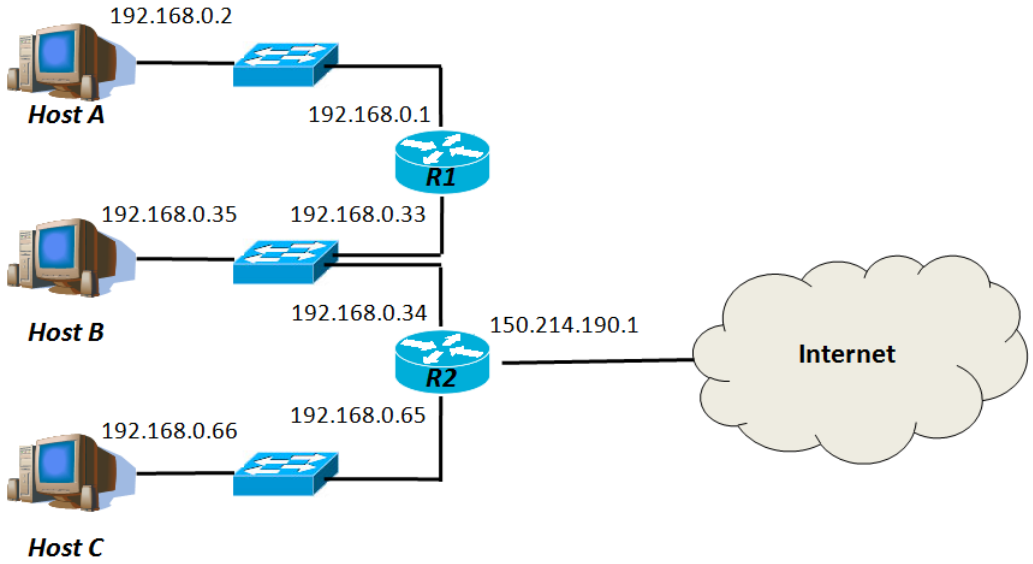


Figura 5: Asignación posible de direcciones IP.

1.2 La retransmisión

Debemos de distinguir dos operaciones relacionadas con el encaminamiento en Internet: el diseño del encaminamiento y su aplicación: la retransmisión (forwarding) En la literatura especializada, se denominan algoritmos de encaminamiento a aquellos que se utilizan para decidir y mantener la información de encaminamiento: es decir, los que buscan los caminos (más o menos) óptimos para su uso posterior en el envío de información. Algunos algoritmos de encaminamiento, imprescindibles en un entorno de interconexión de redes como Internet, se verán con posterioridad en la asignatura. La retransmisión es la operación básica por la cual los dispositivos derivan los paquetes por alguna de sus interfaces de salida. En este apartado trataremos cómo se lleva a cabo dicha retransmisión utilizando tablas de encaminamiento. Nótese que aunque el término retransmisión es más adecuado para los dispositivos de interconexión (los routers), la operación de retransmisión como tal también tiene que realizarse en los dispositivos origen de la información.

El encaminamiento más utilizado en Internet y el que se va a explicar en esta sección, se basa en una resolución iterativa salto a salto. Cada dispositivo que participa en la comunicación, bien como dispositivo inicial (origen) bien como nodo intermedio, toma la decisión de en qué dirección enviar el paquete. Así, pensemos en el siguiente ejemplo, considerando la topología de la Figura 5: el host A quiere enviar un paquete al host C. El encaminamiento empieza en el mismo host A, que ha de determinar que para llegar a C tiene que enviar el paquete al router R1. Una vez hecho eso, la responsabilidad del host A en el encaminamiento del paquete desaparece: ya ha acabado su trabajo. Una vez el paquete llega al router R1, éste tiene que determinar a dónde retransmitirlo considerando que el destino final es el host C. R1 decidirá que el siguiente nodo en el camino debe ser R2, y de nuevo habrá terminado su papel. Una vez llegue el paquete a R2, éste se lo hará llegar a C.

Esta solución salto a salto del encaminamiento está fundamentada en reducir al máximo el tamaño de las tablas de encaminamiento, de cara a reducir el retardo de procesamiento en las comunicaciones. Así, cada dispositivo se debe asegurar de resolver el encaminamiento correctamente a nivel local, asumiendo que el resto de dispositivos harán lo mismo. Con este objetivo, las tablas de encaminamiento especifican tres elementos fundamentales para la retransmisión: la dirección de subred destino, la máscara asociada y el siguiente nodo a donde enviar la información. Como ya se comentó, el hecho de encaminar con destino a subredes en lugar de hosts específicos es análogo al encaminamiento basado en prefijos en telefonía.

Así, por ejemplo, la tabla de encaminamiento en el host A, de acuerdo a la Figura 5, se podría especificar como sigue:

Tabla 1: Tabla de encaminamiento en el host A

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	**255.255.255.224**	**-**
192.168.0.32	**255.255.255.224**	**192.168.0.1**
192.168.0.64	**255.255.255.224**	**192.168.0.1**
150.214.190.0	**255.255.255.252**	**192.168.0.1**

El procedimiento de retransmisión de un paquete se basa en dos pasos que se repiten iterativamente para cada fila de la tabla:

i) Aplicar la operación AND entre la dirección destino del paquete y la máscara definida en la fila.
ii) Comprobar si la dirección resultante coincide con la de destino en la misma fila. En caso que coincida, enviar al siguiente nodo correspondiente.

En el caso en que en más de una fila se cumpla ii) se elige la opción más restrictiva (con menos 0s en la máscara). En algunos sistemas operativos se aplica dicha selección ordenando convenientemente la tabla, si bien en otros no se lleva a cabo de esa manera.

Volvamos al ejemplo anterior, en el que el host A quiere mandar un paquete al host C. El paquete, como veremos más adelante, tendrá embebida la dirección IP de destino (192.168.0.66). El host A comenzará a repetir los dos pasos anteriores para cada entrada de la Tabla 1:

Fila 1 ➔ i) 192.168.0.66 = 11000000.10101000.00000000.01000010
&
255.255.255.224 = 11111111.11111111.11111111.11100000

192.168.0.64 = 11000000.10101000.00000000.01000000

ii) ¿192.168.0.64 == 192.168.0.0? ➔ NO

Fila 2 ➔ i) 192.168.0.66 = 11000000.10101000.00000000.01000010
&
255.255.255.224 = 11111111.11111111.11111111.11100000

192.168.0.64 = 11000000.10101000.00000000.01000000

ii) ¿192.168.0.64 == 192.168.0.32? ➔ NO

Fila 3 ➔ i) 192.168.0.66 = 11000000.10101000.00000000.01000010
&
255.255.255.224 = 11111111.11111111.11111111.11100000

192.168.0.64 = 11000000.10101000.00000000.01000000

ii) ¿192.168.0.64 == 192.168.0.64? ➔ SÍ

Fila 4 ➔ i) 192.168.0.66 = 11000000.10101000.00000000.01000010
&
255.255.255.252 = 11111111.11111111.11111111.11111100

192.168.0.64 = 11000000.10101000.00000000.01000000

ii) ¿192.168.0.64 == 150.214.190.0? ➔ NO

El primer (y único) éxito en el punto ii) aparece en la Fila 3, por lo que el siguiente nodo a donde hay que enviarlo es 192.168.0.1. Es decir, el router R1.

Ahora, como ejemplo alternativo, imaginemos que el usuario del host A abre el explorador para hacer una búsqueda en www.google.com. Tras la traducción del nombre de dominio, la dirección IP obtenida es 172.194.34.209. El paquete donde se encapsula la petición HTTP tendrá, pues, la dirección de destino especificada. Repitiendo el proceso de retransmisión anterior, se puede comprobar que no hay ningún éxito para ninguna de las filas de la tabla. Ante esta eventualidad, el host descarta el envío del paquete dando el pertinente mensaje de error y, por tanto, el usuario no consigue conectarse con el servidor de Google. ¿Qué ha ocurrido? La solución propuesta en la tabla de encaminamiento permite direccionar los dispositivos en la red corporativa, pero no todas las direcciones en Internet, lo que claramente limita la funcionalidad de la red. La red, aún estando conectada físicamente a Internet, no sabe cómo llegar a la misma. Por supuesto, añadir una entrada en la tabla por cada subred de Internet es una solución inviable, ya que la tabla de encaminamiento sería demasiado grande para su manejo eficiente (sería equivalente a introducir todos los números de teléfono del mundo en cada central telefónica) Por otro lado, no parece necesario que, en la situación en la que se encuentra el host A, donde el único camino al "resto del mundo" es el router R1, haya tantas entradas en la tabla de encaminamiento como se muestran en la Tabla 1. Por tanto, esta solución no es completa ni eficiente.

Efectivamente, el diseño de la tabla de encaminamiento puede optimizarse para reducir el número de entradas en la tabla y a la vez permitir un encaminamiento global. El mecanismo es simple: jugar con la máscara de subred. Si en la máscara de subred de una determinada entrada sustituimos 1s por 0s, hacemos la entrada más genérica. Por ejemplo, las últimas dos entradas en la Tabla 1:

Subred ➔ 192.168.0.32/27 = 11000000.10101000.00000000.00100000

Subred ➔ 192.168.0.64/27 = 11000000.10101000.00000000.01000000

se pueden combinar en una única entrada:

Subred ➔ 192.168.0.0/25 = 11000000.10101000.00000000.00000000

Recordemos que para comprobar que las dos subredes anteriores están contenidas en esta otra, basta con realizar la operación AND de sus direcciones con la máscara /25. Equivalentemente, se puede comprobar poniendo a 0 los últimos 32-25=7 bits de las direcciones anteriores, obteniendo en ambos casos 192.168.0.0. Con esta generalización, simplificaríamos la tabla en una entrada:

Tabla 2: Tabla de encaminamiento en el host A

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	**255.255.255.224**	**-**
192.168.0.0	**255.255.255.128**	**192.168.0.1**
150.214.190.0	**255.255.255.252**	**192.168.0.1**

En este caso, las direcciones de subred correspondientes a las dos primeras entradas coinciden, pero recordemos que la prioridad es siempre para la más restrictiva. Así, si se pasa una dirección de la subred 1, por ejemplo la del router R1: 192.168.0.1, se produce el siguiente resultado:

Fila 1 ➔ i) 192.168.0.1 = 11000000.10101000.00000000.00000001
&
255.255.255.224 = 11111111.11111111.11111111.11100000

192.168.0.0 = 11000000.10101000.00000000.00000000

ii) ¿192.168.0.0 == 192.168.0.0? ➔ SÍ

Fila 2 ➔ i) 192.168.0.1 = 11000000.10101000.00000000.00000001
&
255.255.255.128 = 11111111.11111111.11111111.10000000

192.168.0.0 = 11000000.10101000.00000000.0000000

ii) ¿192.168.0.0 == 192.168.0.0? ➔ SÍ

Fila 3 ➔ i) 192.168.0.1 = 11000000.10101000.00000000.00000001
& &
255.255.255.252 = 11111111.11111111.11111111.11111100

192.168.0.0 = 11000000.10101000.00000000.00000000

ii) ¿192.168.0.0 == 150.214.190.0? ➔ NO

Las Filas 1 y 2 tienen éxito, siendo la Fila 1 la más restrictiva (mayor número de 1s) y por tanto la escogida. El paquete se mandará en la subred propia directamente a su destino. Si ahora la dirección es de la subred 2, por ejemplo la otra dirección del router R1: 192.168.0.33, se produce el siguiente resultado:

Fila 1 ➔ i) 192.168.0.33 = 11000000.10101000.00000000.00100001
& &
255.255.255.224 = 11111111.11111111.11111111.11100000

192.168.0.32 = 11000000.10101000.00000000.00100000

ii) ¿192.168.0.32 == 192.168.0.0? ➔ NO

Fila 2 ➔ i) 192.168.0.33 = 11000000.10101000.00000000.00100001
& &
255.255.255.128 = 11111111.11111111.11111111.10000000

192.168.0.0 = 11000000.10101000.00000000.0000000

ii) ¿192.168.0.0 == 192.168.0.0? ➔ SÍ

Fila 3 ➔ i) 192.168.0.33 = 11000000.10101000.00000000.00100001
& &
255.255.255.252 = 11111111.11111111.11111111.11111100

192.168.0.32 = 11000000.10101000.00000000.00100000

ii) ¿192.168.0.32 == 150.214.190.0? ➔ NO

En este caso, no hay conflicto, y por tanto se retransmite la información al siguiente nodo de acuerdo a la Fila 2.

Si bien hemos reducido el número de entradas, no hemos solucionado el problema de direccionar Internet. Para ello, basta con llevar el truco anterior al extremo: introducir la máscara /0 = 0.0.0.0. Si a cualquier dirección se le aplica la operación AND con la máscara 0.0.0.0 el resultado es precisamente 0.0.0.0. La entrada donde la dirección de destino y la máscara de subred es 0.0.0.0 es lo que se conoce como la entrada por defecto, ya que permite especificar un camino para todas

aquellas direcciones que no se hayan resuelto en otra entrada de la tabla, y que por tanto tendrían prioridad al ser más restrictivas. Es fácil comprobar que la siguiente tabla permite direccionar correctamente las mismas direcciones que la Tabla 2 e incluye adicionalmente todas las de Internet:

Tabla 3: Tabla de encaminamiento en el host A

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.0	**255.255.255.224**	**-**
0.0.0.0	**0.0.0.0**	**192.168.0.1**

En realidad, ésta es la disposición típica que se tiene en los hogares, donde típicamente hay un único router de acceso que conecta al ordenador personal a los servicios en Internet (dependiendo del Sistema Operativo, pueden especificarse más entradas) Un ejercicio interesante para el alumno puede ser comprobar la tabla de encaminamiento que tiene en los ordenadores de la casa e intentar interpretar las distintas entradas en la misma. Para sistemas Windows, esto se puede llevar a cabo en la línea de comandos (cmd) con la opción "route print". Para sistemas Unix, se puede usar la orden "route".

Ahora, volviendo a la Figura 5, vamos a diseñar la tabla de encaminamiento en el router R2. Algunas recomendaciones para el diseño son las siguientes:

a) Incorporar todas las redes directamente conectadas.
b) Incorporar la entrada por defecto (si es que se necesita) asociada al camino con más entradas
c) Añadir todas las entradas adicionales necesarias.

Así, la tabla queda:

Tabla 4: Tabla de encaminamiento en el router R2

Dirección IP destino	Máscara	Siguiente nodo
192.168.0.32	**255.255.255.224**	**-**
192.168.0.64	**255.255.255.224**	**-**
150.214.190.0	**255.255.255.252**	**-**
0.0.0.0	**0.0.0.0**	**150.214.190.2**
192.168.0.0	**255.255.255.224**	**192.168.0.33**

donde las primeras tres entradas se corresponden con redes directamente conectadas (paso a)), la cuarta es la entrada por defecto (paso b)) y la quinta es necesaria para direccionar la subred 1. Nótese que el siguiente nodo para salir a Internet es el nodo de acceso provisto por el ISP y que para ir a la subred 1 se pasa por el router R1, especificando la dirección asociada a la subred 2, que es a donde el router R2 ya sabe llegar.

Finalmente, la flexibilidad que otorga el uso de la máscara de red puede utilizarse para simplificar las tablas de encaminamiento también en los routers en el núcleo de Internet. Así, pensemos en el ejemplo de la Figura 6, donde se realiza una asignación jerárquica de direcciones IP basada en el uso de una máscara de longitud variable. Varios ISPs obtienen sus direcciones de un ISP de mayor envergadura, que a su vez pudo obtener sus direcciones de la Internet Corporation for Assigned Names and Numbers (ICANN). En los casos presentados, los ISPs contratan un

paquete de direcciones contiguas con 2^{16} direcciones, usando una máscara /16. A su vez, los ISPs pueden ofrecer a sus clientes (distintas empresas en el ejemplo) porciones de sus direcciones aplicando máscaras más restrictivas (con mayor número de 1s). En el ejemplo, dos empresas contratan un número distinto de direcciones IP. La empresa A podrá direccionar hasta 2^{12}-2 dispositivos y la empresa Z hasta 2^{8}-2.

ISP (Pequeño) ➔ 150.224.0.0/16 = 10010110.11100000.00000000.00000000

Empresa A ➔ 150.224.0.0/20 = 10010110.11100000.00000000.00000000

…

Empresa Z ➔ 150.224.255.0/24 = 10010110.11100000.11111111.00000000

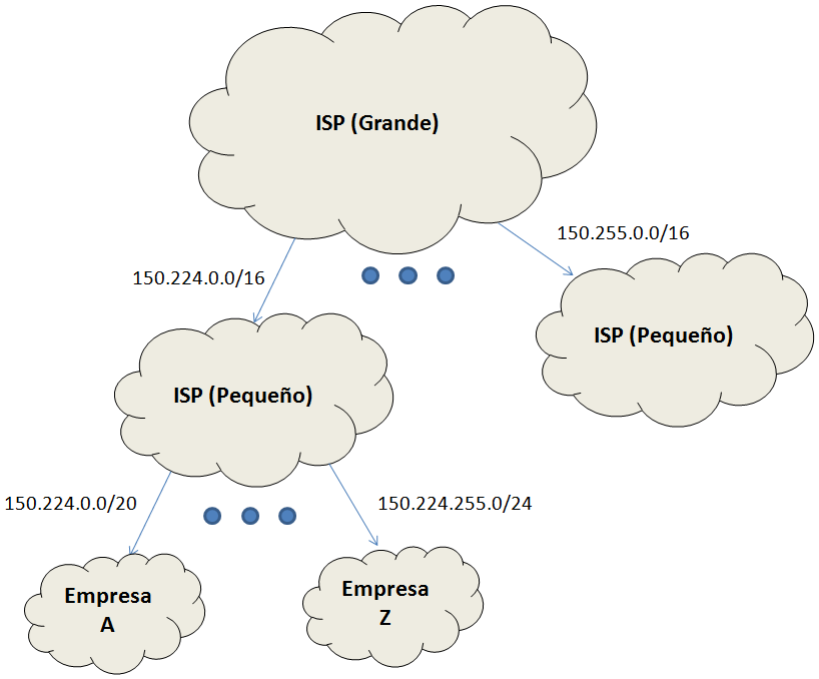


Figura 6: Asignación jerárquica de direcciones IP.

1.3 Evolución histórica del direccionamiento IP

El direccionamiento y encaminamiento en Internet ha sufrido una intensa evolución como consecuencia de los problemas derivados de un diseño original realizado cuando nada parecía prever el papel que la Red de Redes estaba llamada a jugar en nuestras vidas. Si bien los conceptos explicados se corresponden con los procedimientos imperantes hoy en día en Internet, todavía existen dispositivos que utilizan versiones obsoletas de protocolos que pueden no entender determinados tipos de direccionamiento. Por este motivo, es interesante conocer la evolución histórica del direccionamiento en Internet.

El direccionamiento original se basaba en la definición de 5 clases de direcciones IP, organizadas de acuerdo a los primeros bits de la dirección tal y como se ilustra en la Figura 7. La primeras tres clases hacen referencia a direcciones de un único dispositivo (unicast), la cuarta de

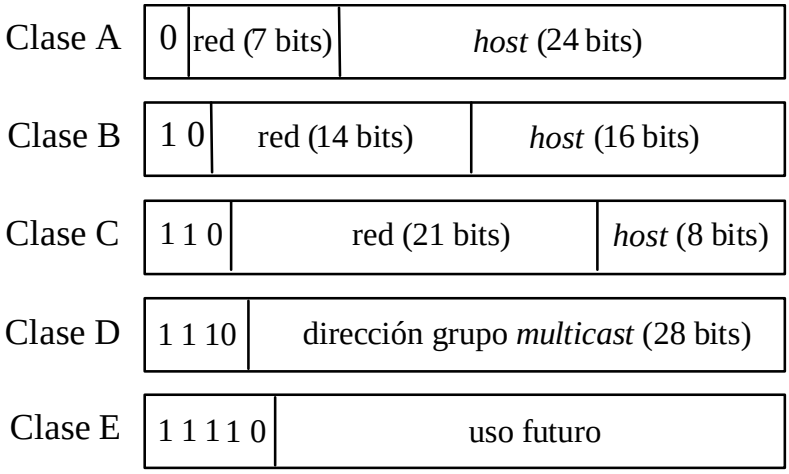


Figura 7: Clases de direcciones IP.

varios dispositivos (multicast) y la última se reserva para uso futuro. La organización de las clases de acuerdo a los primeros bits implica una limitación obvia en el número de direcciones de cada clase: se definen 2^{31} direcciones de clase A, 2^{30} direcciones de clase B, y así sucesivamente.

Este diseño original es demasiado rígido y no fomenta un buen aprovechamiento del espacio de direcciones. Así, cada vez que una empresa solicitaba direcciones a un ISP, debía contratar como mínimo una red de tipo C. Si la empresa excedía los dispositivos direccionables con la red de tipo C (254) debía elegir entre solicitar varias redes de tipo C, posiblemente no contiguas, y una red de tipo B, posiblemente desmesurada. Si bien la primera opción parece más lógica, también lleva a incrementar significativamente las tablas de encaminamiento. Debido a estos problemas, tan sólo 15 años después de la estandarización del protocolo IP en septiembre de 1981, el crecimiento de Internet, que para aquel entonces doblaba su tamaño cada 9 meses, hacía patentes las limitaciones del diseño original:

- El número de direcciones IP disponibles, fundamentales para el funcionamiento de los servicios en Internet, era ocupado a tal velocidad que quedaría exhausto en poco tiempo, lo que imposibilitaría el crecimiento de la red y el acceso de nuevos usuarios y servicios.

- Las tablas de encaminamiento, necesarias para la comunicación entre cualesquiera dos puntos de Internet, crecían a una velocidad alarmante, lo que las haría complejas de procesar por parte de los encaminadores y en definitiva supondría una pérdida de eficiencia en las comunicaciones, sino su imposibilidad práctica.

La solución parcial a estos problemas adoptada en 1985 fue la introducción de la máscara de subred, que permitía dividir las direcciones de clase A, B y C en tres partes: la dirección de red (de acuerdo a la Figura 7), la dirección de subred (de acuerdo a la máscara de subred) y la dirección de host. Posteriormente, en 1987, se introduce la idea de máscara de subred de longitud variable (VLSM) que posibilita el direccionamiento jerárquico, lo que aún permite optimizar mejor las tablas de encaminamiento en el núcleo de Internet. En 1993 se introduce el encaminamiento entre dominios sin clase (CIDR) que elimina la noción de clases en las direcciones unicast. Poco después, en 1996, se definirían las direcciones privadas para la configuración de redes corporativas.

Algunas versiones de protocolos obsoletas, como es el caso de la versión 1 del protocolo de enrutamiento RIP, siguen haciendo uso de direcciones basadas en clases y sin máscara de red, por lo que es necesario tener en cuenta esta eventualidad a la hora de elegir el conjunto de protocolos a

configurar en una red. También es frecuente que al hacer la configuración de un sistema, si se permite la introducción de la dirección IP sin máscara asociada, se asume la máscara de acuerdo a la clase de la dirección. Esto ocurre, al menos, en algunos sistemas Unix.

Como se discutió en los temas precedentes, la mayoría de los servicios en Internet siguen el paradigma cliente/servidor, donde tanto el cliente como el servidor deben poseer una dirección IP que los identifique de forma unívoca en Internet. Esta restricción es extensible a las aplicaciones P2P. El uso de direcciones de 32 bits limita el número de dispositivos direccionables a 2^{32}, lo que equivale a algo más de 4000 millones de dispositivos. Este número puede parecer elevado, más aún pensando en las extensiones posibles utilizando direccionamiento privado. No obstante, dicho número es del todo insuficiente en especial pensando en la evolución hacia un mundo globalmente interconectado siguiendo la noción del "Internet de las cosas". De acuerdo a la comunidad especializada, el protocolo IPv6, que define direcciones de 128 bits, es la solución a estos problemas.

2 BIBLIOGRAFÍA

[1] Pedro García Teodoro, Jesús Díaz Verdejo y Juan Manuel López Soler. Transmisión de Datos y Redes de Computadores. Ed. Pearson, 2007, ISBN**:** 9788420539195.

[2] James F. Kurose y Keith W. Ross. Computer Networking: A Top-Down Approach, 5ª Edición, Addison-Wesley, 2010, ISBN: 9780136079675.

[3] Understanding IP Addressing: Everything You Ever Wanted to Know. 3Com. 2001.

Para leer más… http://www.learntosubnet.com/