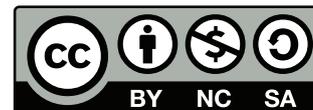


# Guía sobre direccionamiento IP, subredes y enrutamiento

Jonas P. Lüke

## Licencia

Este documento esta realizado bajo licencia Creative Commons «Reconocimiento-NoCommercial-CompartirIgual 4.0 Internacional».



## Cómo citar este documento

Para citar este documento debe utilizar el siguiente formato de cita:

Lüke, J.P. *Guía sobre direccionamiento IP, subredes y enrutamiento*, Versión 0.3, 2019-06-27.

## Control de versiones

Version:	0.3
Git Hash:	8ef2a67fa6b089731c786ffc89d607fb99d99f6e
Author name:	Jonas Lüke
E-mail:	jpluke@ull.es
Fecha:	2019-06-27 08:59:26 +0100



# Índice general

<b>1. Direccionamiento IP versión 4</b>	<b>1</b>
1.1. Direcciones IP versión 4 y máscaras de red . . . . .	1
1.2. Direccionamiento con clases . . . . .	2
1.2.1. Subredes . . . . .	2
1.2.2. Reparto de las direcciones IP . . . . .	4
1.3. Rangos de direcciones privadas . . . . .	6
1.4. <i>Variable Length Subnet Mask</i> (VLSM) . . . . .	6
1.5. <i>Classless Interdomain Routing</i> (CIDR) . . . . .	8
1.6. Desarrollo de esquemas de direccionamiento VLSM . . . . .	9
1.7. Tablas de enrutamiento . . . . .	11
1.8. Agregación de rutas o sumarización de rutas . . . . .	13
1.9. Direccionamiento para favorecer la agregación de rutas . . . . .	15
<b>2. Direccionamiento IPv6</b>	<b>21</b>
2.1. Direcciones IPv6 . . . . .	21
2.2. Máscaras de red . . . . .	21
2.3. Tipos de direcciones . . . . .	22
2.4. Subredes en IPv6 . . . . .	22
<b>3. Ejercicios</b>	<b>27</b>



# Capítulo 1

## Direccionamiento IP versión 4

### 1.1. Direcciones IP versión 4 y máscaras de red

Las direcciones IP versión 4 son un entero de 32 bits. Dicho entero se separa en cuatro bytes que se escriben en base decimal. En la figura 1.1 se muestra un ejemplo de dirección IP. En la parte superior se muestra la dirección en binario, mientras que en la parte inferior se muestra la misma dirección en formato decimal.

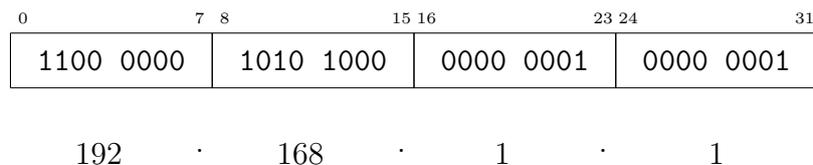


Figura 1.1: Dirección IP versión 4.

Cada interfaz de red deberá tener asignada una dirección IP para poder operar correctamente y la misma dirección no podrá asignarse a más de un host.

Dentro de la dirección IP se distinguen dos partes: La parte de red o prefijo de red y la parte host. La parte de red identifica a la red, mientras que la parte de host identifica a un host concreto dentro de una red. La parte de red corresponde a los  $N$  primeros bits, mientras que la parte host corresponde a los  $32 - N$  bits restantes, como se muestra en la figura 1.2.

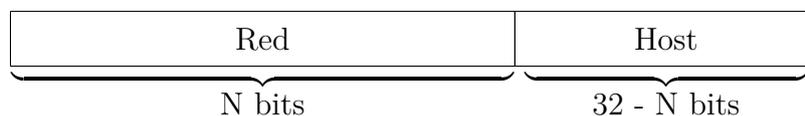


Figura 1.2: Prefijo y parte de host de la dirección IP.

Para distinguir la parte de red de la parte de host se necesita lo que se conoce como **máscara de red**, que no es más que un entero de 32, igual que las direcciones IP, en el que se fijan a 1 los bits de la parte de red y a 0 los bits de la parte de host. Al igual que las direcciones IP las máscaras de red se pueden expresar en notación decimal. Por ejemplo:

255.255.255.0      (11111111.11111111.11111111.00000000)

```

255.0.0.0      (11111111.00000000.00000000.00000000)
255.255.192.0 (11111111.11111111.11000000.00000000)
255.224.0.0   (11111111.11100000.00000000.00000000)

```

Es importante recalcar que las direcciones de los hosts pertenecientes a la misma red de área local deben compartir el mismo prefijo. Además, dentro de cada red se contemplan dos direcciones especiales (figura 1.3):

- **Dirección de red:** La dirección de red consiste en el prefijo de red fijando a '0' todos los bits de la parte de host. Esta dirección no se puede asignar a ningún host, pues su misión es identificar a la red. No se pueden enviar paquetes a esta dirección.
- **Dirección de broadcast:** La dirección de broadcast consiste en el prefijo de red fijando '1' todos los bits de la parte de host. Esta dirección no es asignable a ningún host. Cuando se envía un paquete a esta dirección, éste está destinado a todos los hosts de la red.

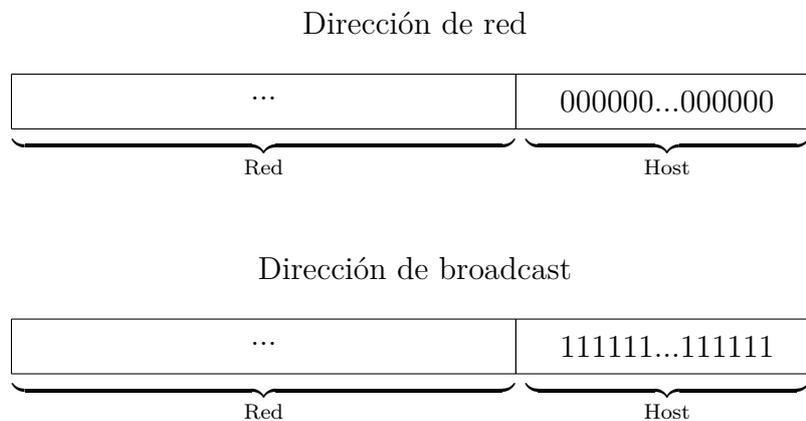


Figura 1.3: Direcciones de red y broadcast

## 1.2. Direccionamiento con clases

En las primeras redes IP se utilizaba lo que se denomina **direccionamiento con clases**, que se introdujo en 1981 como parte de la definición del protocolo IP en el [RFC 791], distinguiéndose distintas clases de direcciones. Las clases se establecen en base a los primeros bits de la dirección, como se muestra en la figura 1.4. Las direcciones de clases A, B y C están dedicadas al direccionamiento de hosts. Las direcciones de la clase D son de multidifusión o *multicast*, mientras que las direcciones de la clase E están reservadas para investigación.

En la figura 1.5, se muestran los tamaños de los prefijos de red para las clases A, B y C.

### 1.2.1. Subredes

Una vez que se asigna un prefijo principal a una organización, esta por necesidades de la topología física, tendrá que subdividir la red principal en redes de menor tamaño (subredes). Esta subdivisión inicialmente se hacía alargando el prefijo de modo que la dirección IP se dividía en tres partes en vez de en dos como hemos visto hasta ahora. Como se muestra en la figura 1.6,

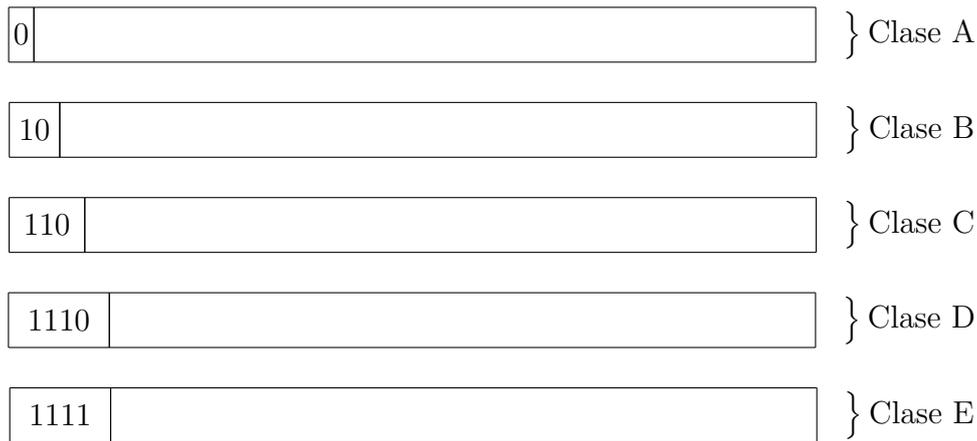


Figura 1.4: Clases de direcciones IP.

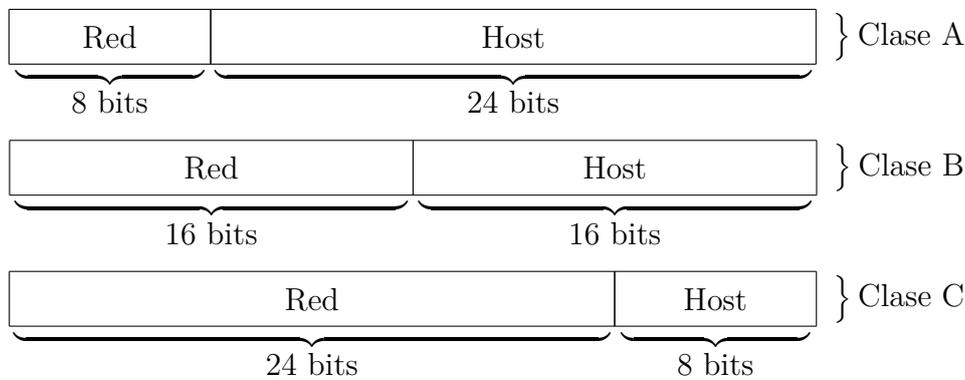


Figura 1.5: Prefijos de red de las clases A, B y C.

los  $N$  primeros bits corresponden a la red, luego este prefijo de  $N$  bits se aumenta hasta  $N+M$  bits que dan lugar a los prefijos de subred y finalmente quedan  $32-N-M$  bits para la parte de host. Al final se le “roban” algunos bits a la parte de host de la red original para crear subredes.

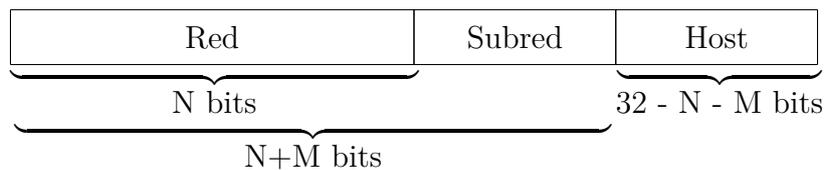


Figura 1.6: Prefijo y parte de host de la dirección IP.

Inicialmente, en el [RFC 950] se consideró que las subredes debían ser todas del mismo tamaño, es decir, que la forma de hacer subredes era “robando” el número de bits suficiente de la parte de host original para indexar todas las subredes. Considere el siguiente ejemplo:

En la figura 1.7, se muestra una red que deberá dividirse en 5 subredes, puesto que existen 5 segmentos de red.

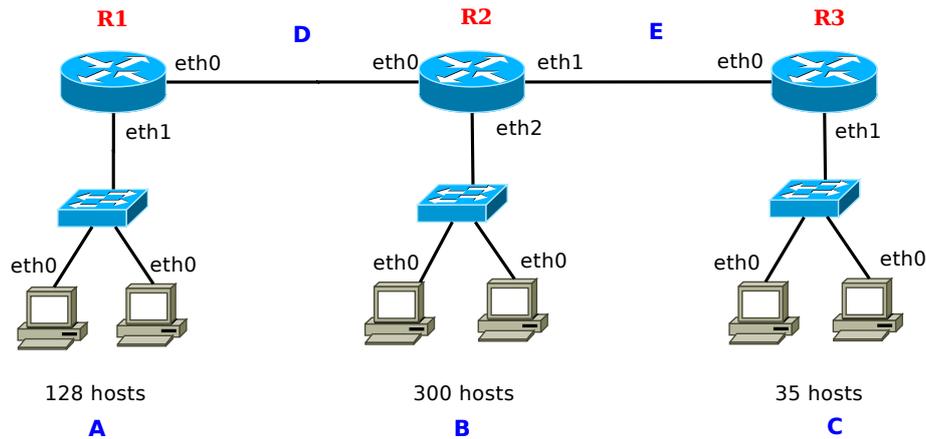


Figura 1.7: Esquema de red.

Para saber cuantos segmentos de red hay en un esquema de red eliminamos mentalmente los routers, puesto que estos dispositivos interconectan a las redes. Todas las partes que queden aisladas, aunque sólo sean un cable, son una red.

Cada segmento de red físico dará lugar a una subred dentro de la red principal. De esta manera, el procedimiento para crear las subredes que se consideró inicialmente, fue muy sencillo. Se reservan suficientes bits en la parte de subred para que se puedan alojar las subredes necesarias. En este ejemplo concreto, al tener cinco subredes, se necesitarán 3 bits que permiten hasta 8 subredes. Supongamos que el prefijo inicial obtenido del ISP es el 8.0.0.0/8. Entonces se reservan tres bits adicionales detrás del prefijo inicial y se identifican cada una de las subredes, dando lugar a las siguientes direcciones de red: 8.0.0.0, 8.32.0.0, 8.64.0.0, 8.128.0.0, 8.160.0.0. La máscara de subred es 255.224.0.0. Este procedimiento es extremadamente ineficiente en cuanto al uso de direcciones, ya que todas las subredes tienen que ajustarse al tamaño de la mayor. Así, por ejemplo, para los dos enlaces punto a punto, que sólo necesitan 4 direcciones, se reservarían  $2^{21}$  direcciones para cada uno.

### 1.2.2. Reparto de las direcciones IP

Vamos a analizar el espacio de direcciones de IP versión 4, para comprender por qué se abandona el direccionamiento con clases. En la figura 1.8, se muestra el reparto de direcciones entre las distintas clases. Se puede observar que la mitad de las direcciones IP versión 4 estaban destinadas a 128 redes de un tamaño considerable. Una cuarta parte va destinada a redes de clase B, que seguramente siguen siendo demasiado grandes para la mayoría de las organizaciones. Finalmente, una octava parte de las direcciones está destinada a redes de tamaño pequeño, que probablemente son demasiado pequeñas.

Debido a este reparto de direcciones se tuvo que cambiar el sistema de reparto de bloques de direcciones a las organizaciones, pasando del direccionamiento con clases al **direccionamiento sin clases**. De este modo, se comenzaron a admitir prefijos de tamaños distintos a los establecidos inicialmente para cada una de las clases. Debido a la escasez de direcciones IP versión

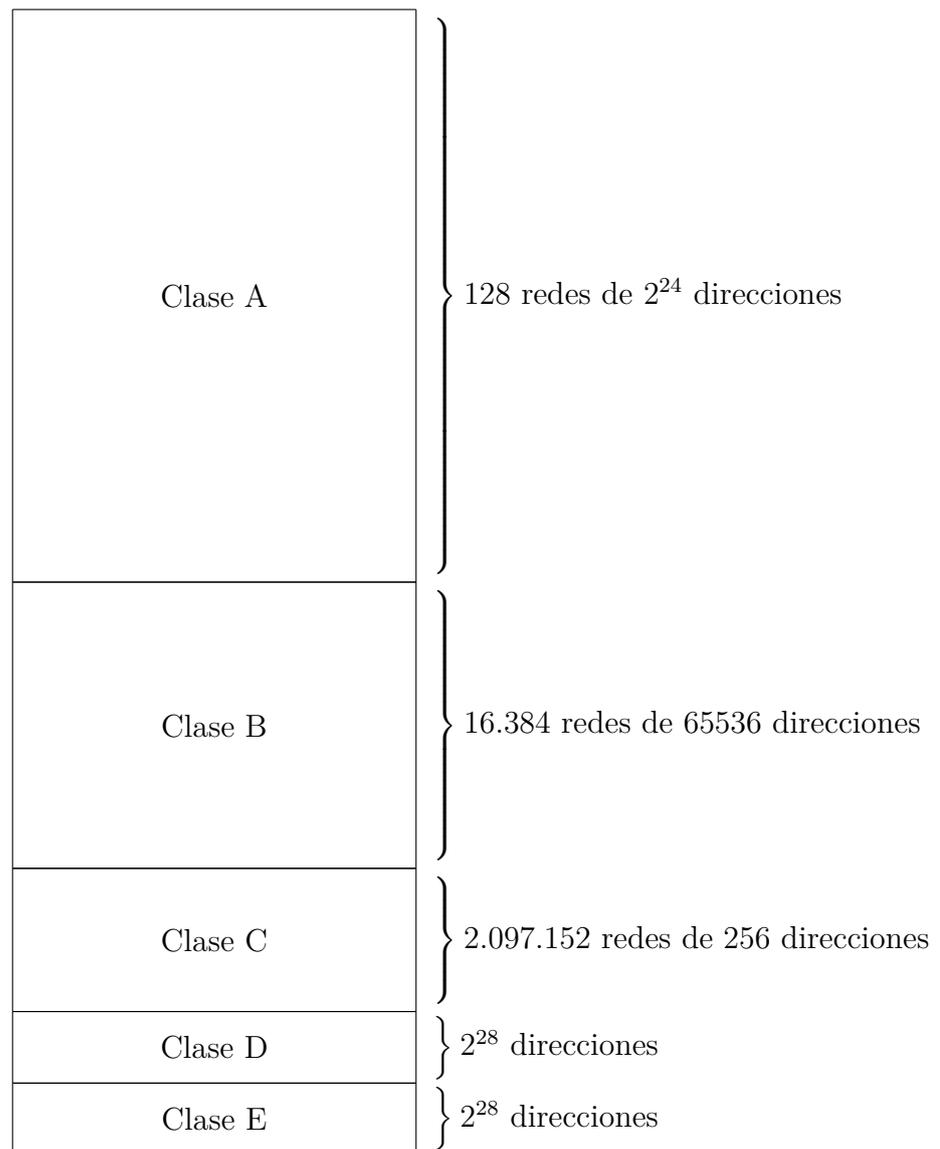


Figura 1.8: Reparto del espacio de direcciones IP.

Clase A	10.x.y.z
Clase B	172.16.0.0 - 172.31.255.255
Clase C	192.168.x.y

Tabla 1.1: Rangos de direcciones privadas.

4 se comenzó a aplicar VLSM/CIDR para el reparto de direcciones. Además, se desarrolla la nueva versión del protocolo IP, la versión 6, cuya principal característica es la ampliación del espacio de direcciones a 128 bits.

### 1.3. Rangos de direcciones privadas

La IANA definió unos rangos de direcciones privados, de libre disposición que pueden ser utilizados sin solicitarlo previamente a ningún registro de direcciones. Estos rangos se definieron en el [RFC 1918] y se muestran en la tabla 1.1. Estos rangos de direcciones privadas no son enrutables en Internet, es decir, que ningún router de Internet reenviará paquetes destinados a direcciones dentro de estos rangos. Estos rangos están reservados para las redes internas de las organizaciones que se encuentran, por ejemplo, tras una sistema NAT [RFC 2663], que ha permitido frenar durante un tiempo la escasez de direcciones IPv4 y su posterior agotamiento.

### 1.4. *Variable Length Subnet Mask (VLSM)*

Las máscaras de subred de longitud variable permiten ajustar el tamaño en bits de la parte host al número de hosts que se desean alojar en cada red. Esto, consecuentemente, lleva también a un ajuste del tamaño en bits del prefijo de la subred, de ahí el nombre: Máscara de subred de longitud variable [RFC 1519],[RFC 1878].

Lo que se persigue es paliar el desperdicio de direcciones IP que se produce debido al método de generar las subredes que se ha explicado en la sección 1.2.1 y para paliar los efectos del reparto ineficiente inicialmente propuesto, que se ha descrito en la sección 1.2.2.

Cuando se aplica VLSM, la dirección de red necesariamente deberá ir acompañada de una máscara de red que indique qué parte es prefijo y qué parte corresponde al host. Por ello, se introduce una nueva notación para las máscaras de red, que facilita su manejo: La notación CIDR. Esta notación simplemente consiste en acompañar a las direcciones de red mediante un número separado por un / que indica la longitud de prefijo o lo que es lo mismo la cantidad de bits a '1' que hay en la máscara de red. Algunos ejemplos son:

- 192.168.0.0/24
- 10.0.0.4/30
- 172.16.4.0/22

Una máscara de red se puede expresar tanto en notación decimal como en notación CIDR. Para pasar de una notación a otra conviene considerar que, al ser una secuencia de '1' seguidos de '0' en binario, en una máscara de red no puede aparecer cualquier número en notación

Nº de '1'	Valor binario	Valor decimal
0	0000 0000	0
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254
8	1111 1111	255

Tabla 1.2: Tabla de conversión entre la notación CIDR y la notación decimal y viceversa.

decimal. Considerando el número de '1' que pueden aparecer en cada byte sólo pueden aparecer los valores que figuran en la tabla 1.2.

Para convertir una máscara de red de notación decimal a notación CIDR sólo hay que buscar los cuatro bytes de la máscara expresados en decimal en la tercera columna de la tabla y sumarlos. Por ejemplo, para la máscara de red 255.255.224.0 tenemos  $8+8+3+0=19$  y en notación CIDR sería /19. Para la máscara 255.255.255.240 sería  $8+8+4+0 = 20$  con lo que en notación CIDR dicha máscara sería /20.

Para hacer la conversión inversa, es decir, de notación CIDR a notación decimal se utiliza la primera columna de la tabla. Supongamos que deseamos convertir la máscara de red /25 en notación CIDR a notación decimal. Para ello debemos buscar cuatro números de la primera columna de la tabla que sumen 25, utilizando primero los mayores. Así tendríamos  $8+8+8+1 = 25$ . Para construir la máscara tendremos que concatenar los cuatro números correspondientes de la tercera columna: 255.255.255.128. Otro ejemplo: /23 es la suma de  $8+8+7+0 = 23$  y la máscara en notación decimal es 255.255.254.0. Debe quedar claro que a la hora de sumar debemos elegir en primer lugar los números mayores.

Volviendo a VLSM, cada una de las redes tendrá un tamaño determinado que dependerá del número de hosts que se pretenden alojar en ella, en base a lo cual se asignan bloques de direcciones cada una de ellas, siempre pertenecientes a un bloque definido por un prefijo global asignado por el ISP u otro administrador de red. Dichos bloques de direcciones se definen mediante una dirección base, que es la dirección de red, y un tamaño de prefijo, que no es otra cosa que la máscara de subred. Los bloques de direcciones asignados a una red deben cumplir las siguientes premisas:

- El tamaño del bloque debe ser una potencia de dos.
- El bloque deberá comenzar en una dirección múltiplo de su tamaño.
- El bloque no debe solaparse con otros bloques asignados a otras redes.

Por ejemplo, para la red de la figura 1.7, los tamaños de bloque se obtienen sumando a las direcciones que se desean asignar a hosts, la dirección de red y broadcast y redondeando a la potencia de dos más cercana por arriba. Así los tamaños de bloque serían los que se indican en la tabla 1.3. Las máscaras de subred dependen directamente del tamaño de bloque. Para obtenerlas, simplemente hay que restar al número total de bits de la dirección (32) el número de

Red	Hosts	Tam. Bloque	Máscara de subred
A	128 (+2)	256	/24
B	300 (+2)	512	/23
C	35 (+2)	64	/26
D	2 (+2)	4	/30
E	2 (+2)	4	/30

Tabla 1.3: Tamaños de bloque para las redes de la figura 1.7.

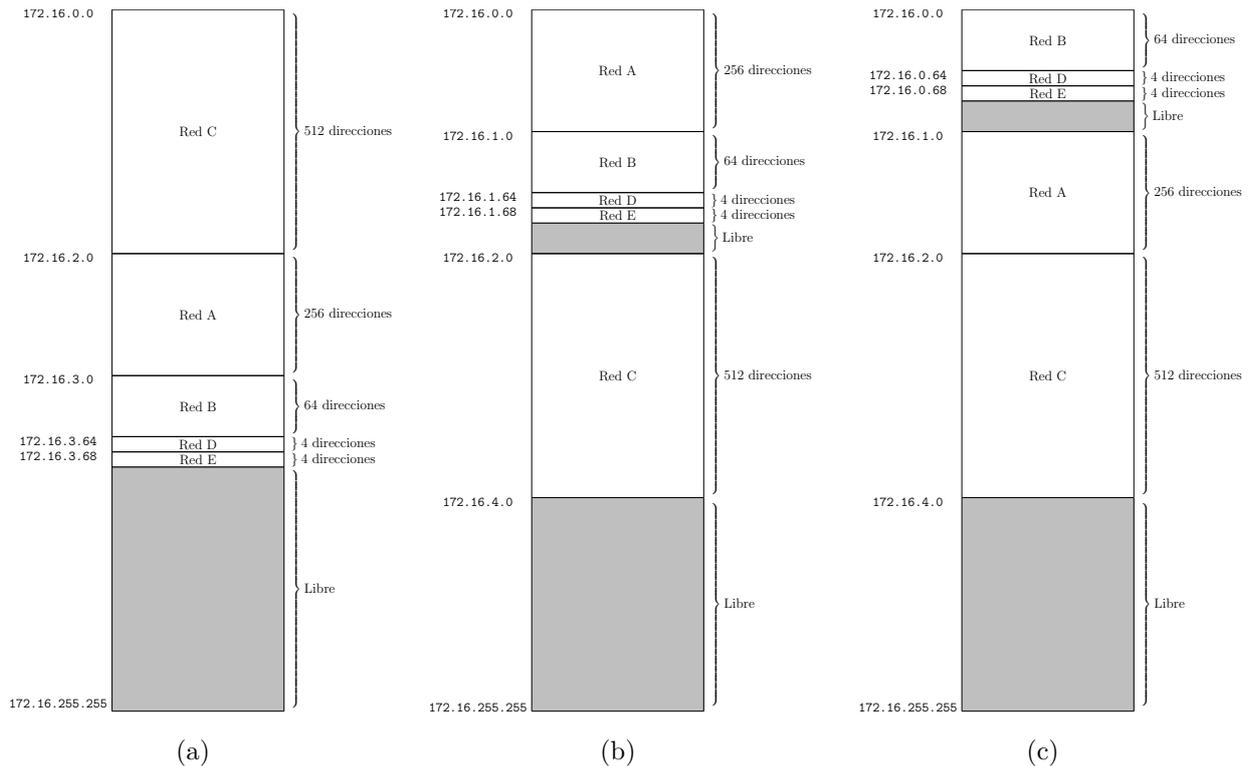


Figura 1.9: Ejemplos de esquemas de direccionamiento válidos.

bits que se van a asignar a la parte de host (nº de bits necesario para direccionar el número de direcciones correspondiente al tamaño de bloque). Así cada subred tiene un tamaño ajustado al número de hosts y, por tanto, una máscara de tamaño variable.

Teniendo en cuenta la segunda premisa y suponiendo un prefijo global 172.16.0.0/16, se podrían considerar múltiples esquemas para el reparto de direcciones tras el prefijo global. En la figura 1.9 se muestran tres ejemplos. Para generar un esquema de direccionamiento válido lo único que debe hacerse es situar los bloques de direcciones en el espacio de direcciones de forma que se cumplan las tres premisas.

## 1.5. *Classless Interdomain Routing (CIDR)*

A medida que la Internet primitiva se convirtió en Internet, la necesidad de nuevas formas de repartir direcciones se volvió cada vez más aparente. De este modo, se eliminaron las clases

de direccionamiento, apareciendo el direccionamiento sin clases. En los [RFC 1518] y [RFC 1519] la IETF publicó un nuevo procedimiento para la reserva de bloques de direcciones, así como un nuevo método para enrutar paquetes IPv4. CIDR se convirtió en el sustituto del direccionamiento con clases permitiendo el reparto de bloques de direcciones con un tamaño ajustado al número de hosts de las redes locales, utilizando para ello los conceptos de VLSM.

## 1.6. Desarrollo de esquemas de direccionamiento VLSM

A continuación, se mostrará un método para generar esquemas de direccionamiento que además cumplen con la restricción adicional de que todas las direcciones quedan contiguas al principio del espacio de direccionamiento, como el que se muestra en la figura 1.9a, lo que permite un aprovechamiento máximo del espacio de direcciones asignado. Esto se hará desarrollando el esquema de direccionamiento para la red de la figura 1.7. Para ello, se hará uso de una tabla que se rellenará mediante un procedimiento que se detalla a continuación:

### 1. Ordenar las subredes de mayor a menor número de hosts.

Red	Hosts	Tam. Bloque	Dir. de red	Máscara de subred	Dir. de broadcast
B	300				
A	128				
C	35				
D	2				
E	2				

### 2. Calcular el tamaño del bloque de direcciones a asignar a cada subred.

Para ello, hay que tener en cuenta las dos direcciones especiales (red y broadcast) y redondear a la potencia de dos más cercada por arriba.

Red	Hosts	Tam. Bloque	Dir. de red	Máscara de subred	Dir. de broadcast
B	300 (+2)	512			
A	128 (+2)	256			
C	35 (+2)	64			
D	2 (+2)	4			
E	2 (+2)	4			

### 3. Calcular las máscaras de red.

Como se indicó anteriormente, la máscara de red se obtiene restando a 32 el número de bits necesario para expresar el tamaño de bloque.

Red	Hosts	Tam. Bloque	Dir. de red	Máscara de subred	Dir. de broadcast
B	300 (+2)	512		/23	
A	128 (+2)	256		/24	
C	35 (+2)	64		/26	
D	2 (+2)	4		/30	
E	2 (+2)	4		/30	

### 4. Calcular las direcciones de red.

Las direcciones de red se calculan utilizando la dirección base del bloque asignado a la

red. Por ejemplo, el 172.16.0.0/16. La primera dirección de red se hace coincidir con esta dirección base. Para las siguientes, debemos movernos tantas direcciones en el espacio de direcciones como indica el tamaño de bloque anotado. En este caso, para la primera fila tenemos un tamaño de bloque de 512 y una dirección base de 512, por lo que la siguiente dirección asignable queda 512 direcciones más abajo, es decir, en 172.16.2.0, que es lo que se anota en la segunda fila. Para el resto de filas se procede igual, es decir, se toma como base la fila anterior y se le añaden tantas direcciones como sea el tamaño de bloque.

Red	Hosts	Tam. Bloque	Dir. de red	Máscara de subred	Dir. de broadcast
B	300 (+2)	512	172.16.0.0	/23	
A	128 (+2)	256	172.16.2.0	/24	
C	35 (+2)	64	172.16.3.0	/26	
D	2 (+2)	4	172.16.3.64	/30	
E	2 (+2)	4	172.16.3.68	/30	

### 5. Calcular las direcciones de broadcast.

La dirección de broadcast es la última dirección de cada bloque. Para obtenerla debemos sumar a la dirección de red el tamaño de bloque y restarle 1.

Red	Hosts	Tam. Bloque	Dir. de red	Máscara de subred	Dir. de broadcast
B	300 (+2)	512	172.16.0.0	/23	172.16.1.255
A	128 (+2)	256	172.16.2.0	/24	172.16.2.255
C	35 (+2)	64	172.16.3.0	/26	172.16.3.63
D	2 (+2)	4	172.16.3.64	/30	172.16.3.67
E	2 (+2)	4	172.16.3.68	/30	172.16.3.71

Con esto finaliza el cálculo del esquema de direccionamiento para esta red. Sin embargo, quedan dos pasos adicionales que se deben realizar para llevarlo a la práctica.

### 6. Plasmar las redes sobre el esquema.

En este momento las redes comienzan a nombrarse mediante su número de red y ya no se utilizan las etiquetas (A,B,C,...) que habíamos utilizado hasta el momento.

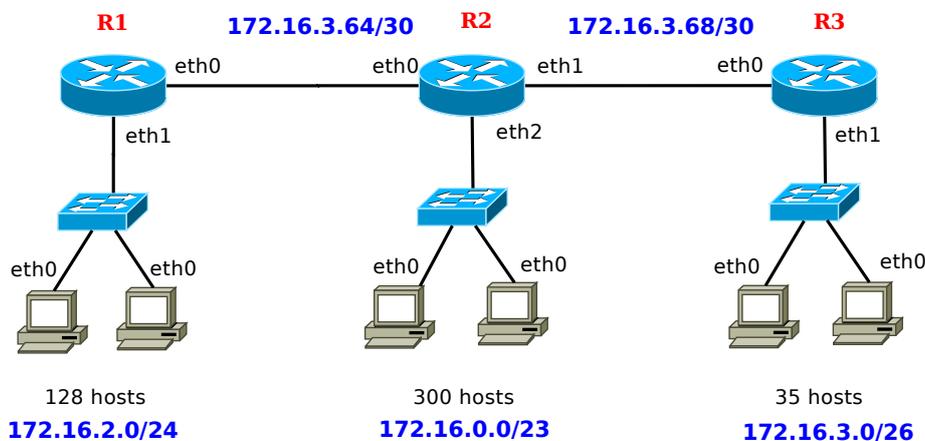


Figura 1.10: Esquema de red con direcciones asignadas a las redes.

### 7. Asignación de direcciones a las interfaces.

Una vez que las redes están identificadas mediante su dirección de red, se procede a asignar una dirección a cada una de las interfaces de red que tienen presencia en la red. Aunque a nivel funcional se puede asignar cualquier dirección asignable (la que está entre la dirección de red y la dirección de broadcast, excluyendo estas) a cualquier host, generalmente es costumbre asignar la primera dirección de la red al router o puerta de enlace y el resto se reparten entre los host.

La asignación de direcciones se puede llevar a cabo de forma manual configurando de forma estática las interfaces de red de cada uno de los hosts. Esto se haría en el caso de routers y servidores, ya que su dirección deberá permanecer fija lo largo del tiempo. Para el caso de los hosts, se pueden aplicar procedimientos automáticos de asignación de direcciones basados en el protocolo DHCP [RFC 2131].

Para el esquema de la figura 1.10, vamos a realizar una asignación estática sobre el esquema, que se muestra en la figura 1.11. Los dos últimos bytes de las direcciones asignadas cada interfaz dentro de la red se muestran en verde.

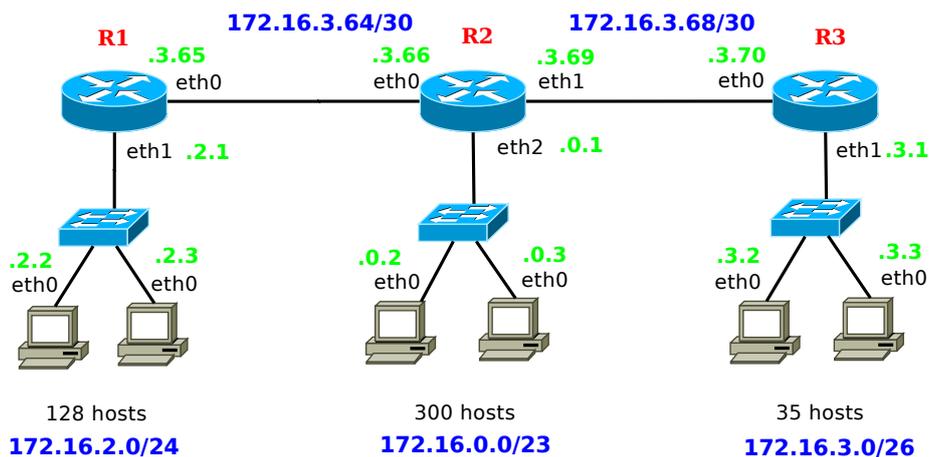


Figura 1.11: Esquema de red con direcciones asignadas a las interfaces de red.

## 1.7. Tablas de enrutamiento

Para que un paquete IP pueda llevarse a su destino, los routers deben tener configurada su tabla de enrutamiento. La **tabla de enrutamiento** indica para cada red de destino la interfaz por la que se reenviará el paquete y en su caso el siguiente router (*gateway*) al que se reenviará dicho paquete. Aunque en general la tabla puede tener más columnas las esenciales son: Dirección de red de destino, máscara de la red de destino, interfaz de salida y el *gateway*. Si se pretende alcanzar una cierta red desde un router, su tabla de enrutamiento deberá contener una entrada (fila) aplicable. Se dice que una entrada de la tabla de enrutamiento es aplicable si al calcular la dirección de red con la máscara indicada para esa entrada, el resultado es el número de red indicado en la tabla para esa entrada. Entre las entradas aplicables, se seleccionará

aquella cuyo prefijo sea más largo o lo que es lo mismo que tenga el mayor número de '1' en la máscara. Para entenderlo mejor, veamos un ejemplo. Suponga la tabla de enrutamiento que se muestra en la tabla 1.4.

Red	Máscara	Interfaz	Gateway
192.168.0.0	/24	eth0	-
172.16.1.0	/24	eth1	-
172.16.0.0	/16	eth1	172.16.1.1
0.0.0.0	/0	eth0	192.168.0.1

Tabla 1.4: Ejemplo de tabla de enrutamiento

Si el paquete IP que se debe reenviar en este router tiene dirección de destino:

- **192.168.0.5:** Se considera la primera entrada, cuya máscara es /24. Al calcular la dirección de red con esta máscara se obtiene 192.168.0.0, que coincide con la dirección de red indicada en la primera columna. Por tanto, la entrada es aplicable. La segunda entrada tiene la misma máscara, /24, pero, al calcular la dirección de red, ésta no va a coincidir con la dirección de red indicada en la primera columna para esta entrada y por ello no es aplicable. Lo mismo sucede con la tercera entrada. Al calcular la dirección de red para la cuarta entrada, obtenemos 0.0.0.0, que coincide y tenemos una segunda entrada aplicable. Finalmente, entre las dos entradas aplicables se toma aquella con un mayor número de unos en su máscara, en este caso, la primera. Por tanto, este paquete IP se reenviaría sin más por la interfaz eth0.
- **172.16.1.68:** Se considera la primera entrada. Con la máscara /24 la dirección de red sería 172.16.0.0, que no coincide con 192.168.0.0, por lo que esta entrada no es aplicable. Al revisar la segunda entrada se obtiene que los números de red coinciden, por lo que la segunda entrada sí es aplicable. La tercera entrada tiene máscara /16. Al calcular la dirección de red ésta es 172.16.0.0, por lo que la entrada es aplicable. Finalmente, la última entrada, también es aplicable porque al calcular la dirección de red con la máscara /0, se obtiene 0.0.0.0. Por lo tanto, para este caso, se obtienen tres entradas aplicables. La entrada con mayor número de '1' en la máscara es la segunda, por lo que este paquete se reenviará sin más por la interfaz eth1.
- **172.16.0.5:** La primera entrada no es aplicable. La segunda tampoco lo es, mientras que la tercera y la cuarta si lo son. La entrada con el prefijo más largo, es la tercera, lo que hace que este paquete se reenvíe a través de eth1 al siguiente router con dirección 172.16.1.1

La última entrada de esta tabla de enrutamiento tiene una característica especial y es que siempre es aplicable, porque no tiene ningún '1' en su máscara. Esta entrada se denomina **ruta por defecto** o **ruta predeterminada**, puesto que se aplicará si ninguna otra es aplicable. Por ello, esta entrada se utiliza para indicar la salida de una subred hacia la red principal o la salida de la red hacia Internet.

Para el esquema de red de la figura 1.11, las tablas de enrutamiento de cada uno de los routers se muestran en las tablas 1.5, 1.6 y 1.7.

Red	Máscara	Interfaz	Gateway
172.16.0.0	/23	eth0	172.16.3.66
172.16.2.0	/24	eth1	-
172.16.3.0	/26	eth0	172.16.3.66
172.16.3.64	/30	eth0	-
172.16.3.68	/30	eth0	172.16.3.66

Tabla 1.5: Tabla de enrutamiento del router R1 de la figura 1.11.

Red	Máscara	Interfaz	Gateway
172.16.0.0	/23	eth2	-
172.16.2.0	/24	eth0	172.16.3.65
172.16.3.0	/26	eth1	172.16.3.70
172.16.3.64	/30	eth0	-
172.16.3.68	/30	eth1	-

Tabla 1.6: Tabla de enrutamiento del router R2 de la figura 1.11.

En las tablas de enrutamiento, se pueden distinguir dos tipos de entradas. Por un lado, las entradas correspondientes a redes directamente conectadas al router, es decir, aquellas redes en las que el router tiene una interfaz con dirección en esa red, y , por otro lado, las redes indirectamente conectadas, que son las que para llegar a ellas desde un router se debe pasar por otro router. Las entradas correspondientes a redes directamente conectadas no tienen gateway, mientras que las redes indirectamente conectadas requieren especificar la dirección del gateway, que es la dirección del siguiente router en el camino que se ha elegido para llegar a la red de destino.

## 1.8. Agregación de rutas o sumarización de rutas

Tal y como se ha visto hasta el momento, todas las redes que se pretenden alcanzar desde un router, deberían tener una entrada en la tabla de enrutamiento. Sin embargo, debemos tener en cuenta que cada vez que un paquete pasa por un router, dicho router deberá examinar la tabla de enrutamiento, para determinar la entrada que se va utilizar para reenviar ese paquete. Cuantas más entradas haya en la tabla de enrutamiento, más tiempo tiempo se necesitará para llevar a cabo el proceso de reenvío. Una forma de reducir el número de entradas de la tabla de enrutamiento, consiste en agrupar en una única entrada aquellas entradas que van ejecutar la misma acción de reenvío. Esto se consigue buscando el prefijo común más largo de todas las entradas a agrupar, y sustituyendo las entradas afectadas por una entrada que en la parte de red y máscara lleve el prefijo común más largo. Este proceso se conoce como **sumarización de rutas** o **agregación de rutas**.

Para ilustrar esta idea vamos a tomar como ejemplo la red que se muestra en la figura 1.12. La tabla de enrutamiento del router R1 es la que se muestra en la tabla 1.8. En la tabla de la izquierda se muestra la tabla de enrutamiento con todas las redes, mientras que en la tabla de la derecha se han agregado las entradas correspondientes a las redes 172.17.0.0/16 y 172.19.0.0/16. La condición necesaria para agregar o sumarizar dos rutas es que la acción que

Red	Máscara	Interfaz	Gateway
172.16.0.0	/23	eth1	172.16.3.69
172.16.2.0	/24	eth1	172.16.3.69
172.16.3.0	/26	eth1	-
172.16.3.64	/30	eth1	172.16.3.69
172.16.3.68	/30	eth0	-

Tabla 1.7: Tabla de enrutamiento del router R3 de la figura 1.11.

se lleve a cabo sea la misma, en este caso, reenviar a través de eth0 hacia el 10.0.0.2, y que se trate de rutas correspondientes a redes indirectamente conectadas al router. La forma de llevar a cabo la sumarización o agregación de rutas es buscando el prefijo común más largo de las rutas a agregar. En este caso:

```
172.17.0.0 (1010110.0001000|01.00000000.000000000)
172.19.0.0 (1010110.0001000|10.00000000.000000000)
```

De modo que el prefijo común más largo es: 1010110.00010000.00000000.000000000, donde los primeros 14 bits coinciden en ambas direcciones. De este modo el prefijo en decimal queda 172.16.0.0/14.

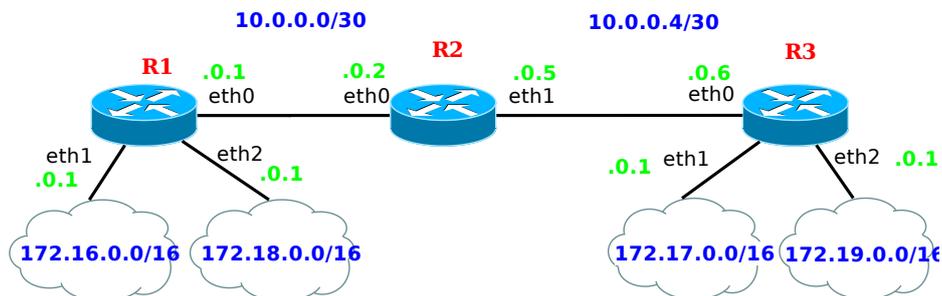


Figura 1.12: Esquema de ejemplo para la realización de la agregación de rutas.

Red	Máscara	Interfaz	Gateway
172.16.0.0	/16	eth1	-
172.18.0.0	/16	eth2	-
10.0.0.0	/30	eth0	-
172.17.0.0	/16	eth0	10.0.0.2
172.19.0.0	/16	eth0	10.0.0.2
10.0.0.4	/30	eth0	10.0.0.2

Red	Máscara	Interfaz	Gateway
172.16.0.0	/16	eth1	-
172.18.0.0	/16	eth2	-
10.0.0.0	/30	eth0	-
172.16.0.0	/14	eth0	10.0.0.2
10.0.0.4	/30	eth0	10.0.0.2

Tabla 1.8: Tabla de enrutamiento del router R1 (izquierda) y la sumarización de algunas de sus rutas (derecha).

De igual modo, en el router R3 se pueden sumarizar las rutas correspondientes a las redes 172.16.0.0 y 172.18.0.0, tal y como se muestra en la tabla 1.9.

Red	Máscara	Interfaz	Gateway
172.17.0.0	/16	eth1	-
172.19.0.0	/16	eth2	-
10.0.0.4	/30	eth0	-
172.16.0.0	/16	eth0	10.0.0.5
172.18.0.0	/16	eth0	10.0.0.5
10.0.0.0	/30	eth0	10.0.0.5

Red	Máscara	Interfaz	Gateway
172.17.0.0	/16	eth1	-
172.19.0.0	/16	eth2	-
10.0.0.0	/30	eth0	-
172.16.0.0	/14	eth0	10.0.0.5
10.0.0.0	/30	eth0	10.0.0.5

Tabla 1.9: Tabla de enrutamiento del router R3 (izquierda) y la sumarización de algunas de sus rutas (derecha).

Red	Máscara	Interfaz	Gateway
172.16.0.0	/16	eth0	10.0.0.1
172.18.0.0	/16	eth0	10.0.0.1
172.17.0.0	/16	eth1	10.0.0.6
172.19.0.0	/16	eth1	10.0.0.6
10.0.0.0	/30	eth0	-
10.0.0.4	/30	eth1	-

Tabla 1.10: Tabla de enrutamiento del router R2. En este caso la sumarización no es posible.

Ahora bien, este procedimiento debe aplicarse con cautela. Veámos qué ocurre si deseamos sumarizar las rutas del router R2, cuya tabla de enrutamiento se muestra en la tabla 1.10. Si observamos la tabla de enrutamiento, se podrían sumarizar las rutas correspondientes a las redes 172.16.0.0/16 y 172.18.0.0/16 y las rutas correspondientes a las redes 172.17.0.0/16 y 172.19.0.0/16. Si hacemos el prefijo común más largo, resulta que en ambos casos es 172.16.0.0/14, con lo que en la tabla de enrutamiento habría dos entradas hacia el mismo destino reenviando paquetes por caminos distintos. Aquí surge un conflicto que se resolvería sumarizando una de las parejas o no sumarizando ninguna.

El hecho de que no se puedan sumarizar las rutas de la tabla 1.10 podría haberse evitado estructurando correctamente el esquema de direccionamiento, de forma que las direcciones de las redes a sumarizar estuviesen en un bloque contiguo de direcciones. Por ejemplo, que las redes de la izquierda fuesen 172.16.0.0/16 y 172.17.0.0/16 y las de la derecha fuesen 172.18.0.0/16 y 172.19.0.0/16. La comprobación de que con este esquema de direccionamiento la sumarización si es posible queda como ejercicio para el lector.

## 1.9. Esquemas de direccionamiento que favorecen la agregación de rutas

Como se indicó en la sección anterior, la disposición adecuada del esquema de direccionamiento, puede favorecer la agregación de rutas en las tablas de enrutamiento de los routers. En esta sección se desarrollarán las técnicas necesarias para obtener esquemas de direccionamiento que permiten la sumarización de rutas. Lo haremos con un ejemplo, desarrollando el esquema de direccionamiento de la red de la figura 1.13.

Para agregar las rutas correspondientes a los tres agrupamientos de redes que se muestran

en la figura 1.13, los bloques de direcciones correspondientes a estas redes deben formar parte de un bloque de direcciones mayor que permita establecer un prefijo común para todas las redes agrupadas.

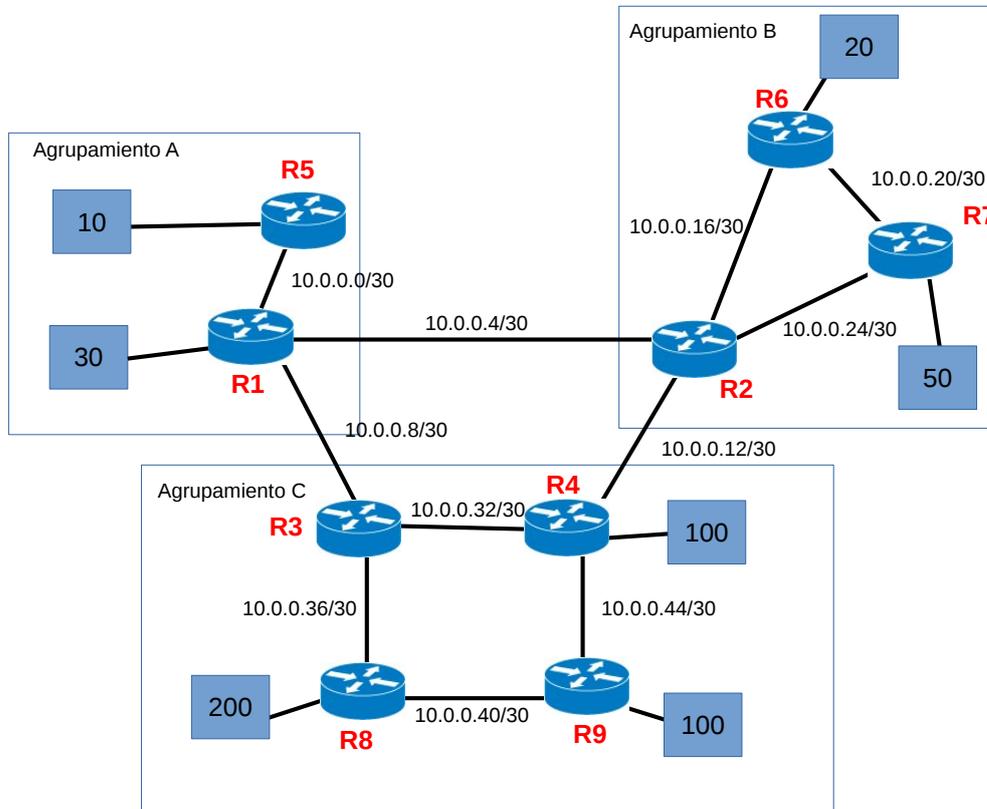


Figura 1.13: Esquema de red.

En este ejemplo, nos centraremos sólo en las redes que contengan hosts y no en las redes de interconexión.

El primer paso es contabilizar los tamaños de los bloques de direcciones necesarios para cada una de las redes físicas (segmentos de red), como se muestra en la segunda columna de la tabla 1.11. Seguidamente, buscaremos el tamaño de bloque para cada una de las redes (teniendo en cuenta la dirección de red y la dirección de broadcast) en función del número de hosts que deseamos alojar en cada una de ellas. Después, se suman estos tamaños (cuarta columna) y se obtiene el tamaño del súper-bloque en la quinta columna (en este caso no se tiene en cuenta las direcciones de red y de broadcast, porque se trata de prefijos, no de redes físicas). Nótese que dentro de cada súper-bloque ordenamos las redes de mayor a menor tamaño.

Ahora deberemos alojar los súper-bloques en el espacio de direcciones disponible. Supongamos que para este caso tenemos el bloque 172.16.0.0/16. Las direcciones se reservan del mismo modo que se hizo cuando se explicó el método VLSM, reservando primero las de mayor tamaño, pues los súper-bloques deben cumplir las mismas premisas que los bloques:

- Deben tener tamaño potencia de dos.
- Deben comenzar en un múltiplo de su tamaño.

Agrupamiento	Hosts	Tam. bloque	Total	Tam. súper-bloque
A	30	32	48	64
	10	16		
B	50	64	96	128
	20	32		
C	200	256	512	512
	100	128		
	100	128		

Tabla 1.11: Tamaños de los súper-bloques.

Agrupamiento	Prefijo
A	172.16.2.128/26
B	172.16.2.0/25
C	172.16.0.0/23

Tabla 1.12: Prefijos correspondientes a los agrupamientos.

La reserva de los súper-bloques se muestra en la figura 1.14. Al igual que en el caso de VLSM se han reservado primero los bloques de mayor tamaño.

Los súper-bloques quedarían identificados a través de los prefijos que se muestran en la tabla 1.12. De este modo, las redes que pertenecen a un agrupamiento, pueden ser enrutadas desde el exterior del agrupamiento utilizando el prefijo sumario correspondiente. Esto resulta especialmente ventajoso cuando el número de redes dentro de un agrupamiento es elevado. Por ejemplo, desde el router 1 las redes dentro del agrupamiento B se alcanzarían mediante el prefijo 172.16.2.0/25 y las del agrupamiento C mediante el prefijo 172.16.0.0/23.

Una vez definidos los súper-bloques vamos a definir las direcciones de red de cada una de las redes. Esto se hará siguiendo el procedimiento que se ha visto en clase (VLSM), pero esta vez dentro de cada uno de los súper-bloques. Haciendo la asignación de cada una de las redes dentro de cada agrupamiento, el reparto de direcciones quedaría tal y como se muestra en la figura 1.15.

Finalmente se asignan las direcciones a cada una de las redes, como se muestra en la figura 1.16.

La ventaja de realizar el esquema de direccionamiento de este modo es que ahora se pueden agregar los prefijos de cada agrupamiento a las tablas de enrutamiento de aquellos routers externos al agrupamiento, sin que sea necesario añadir todas las redes interiores.

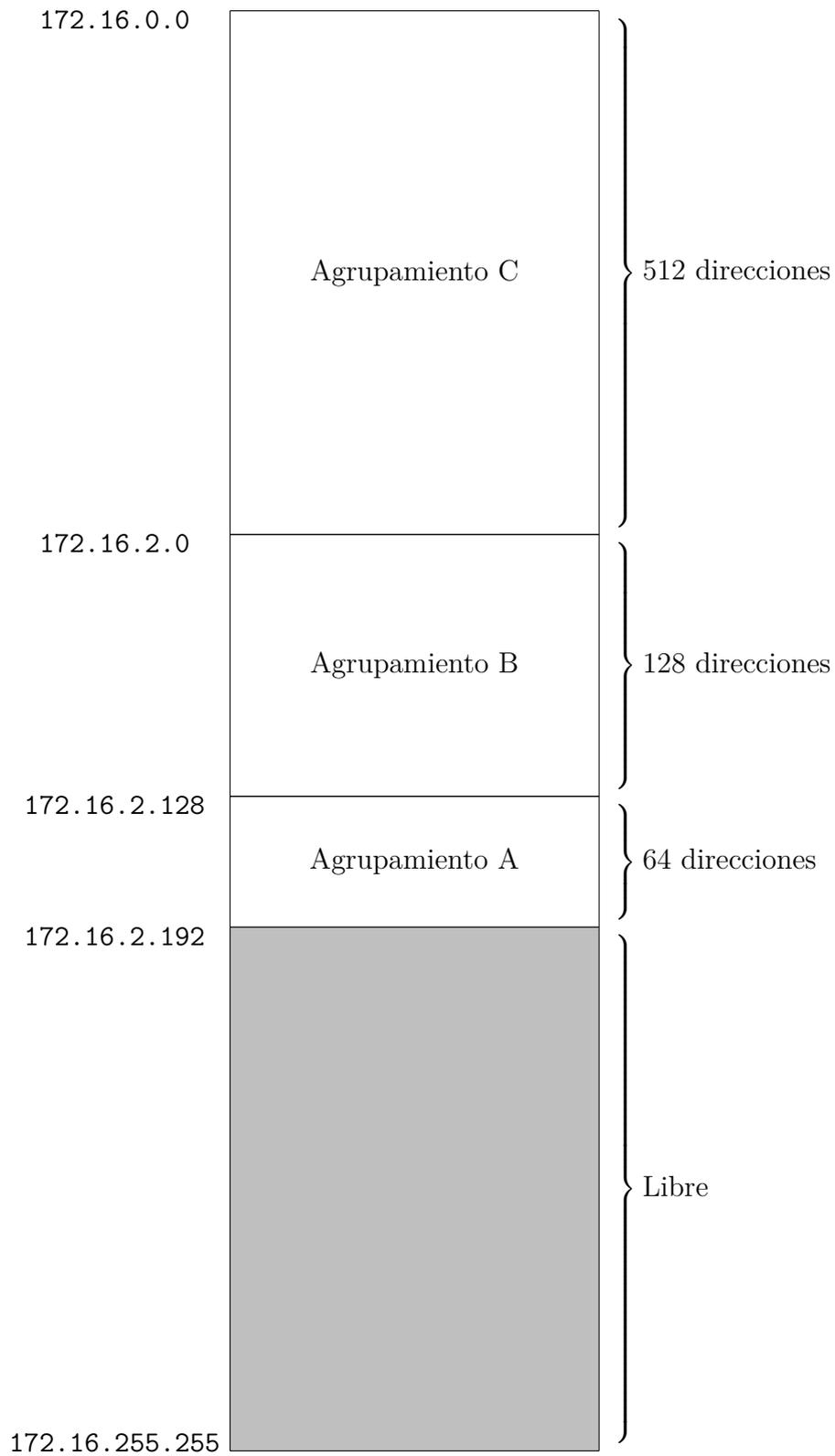


Figura 1.14: Reserva de los súper-bloques.

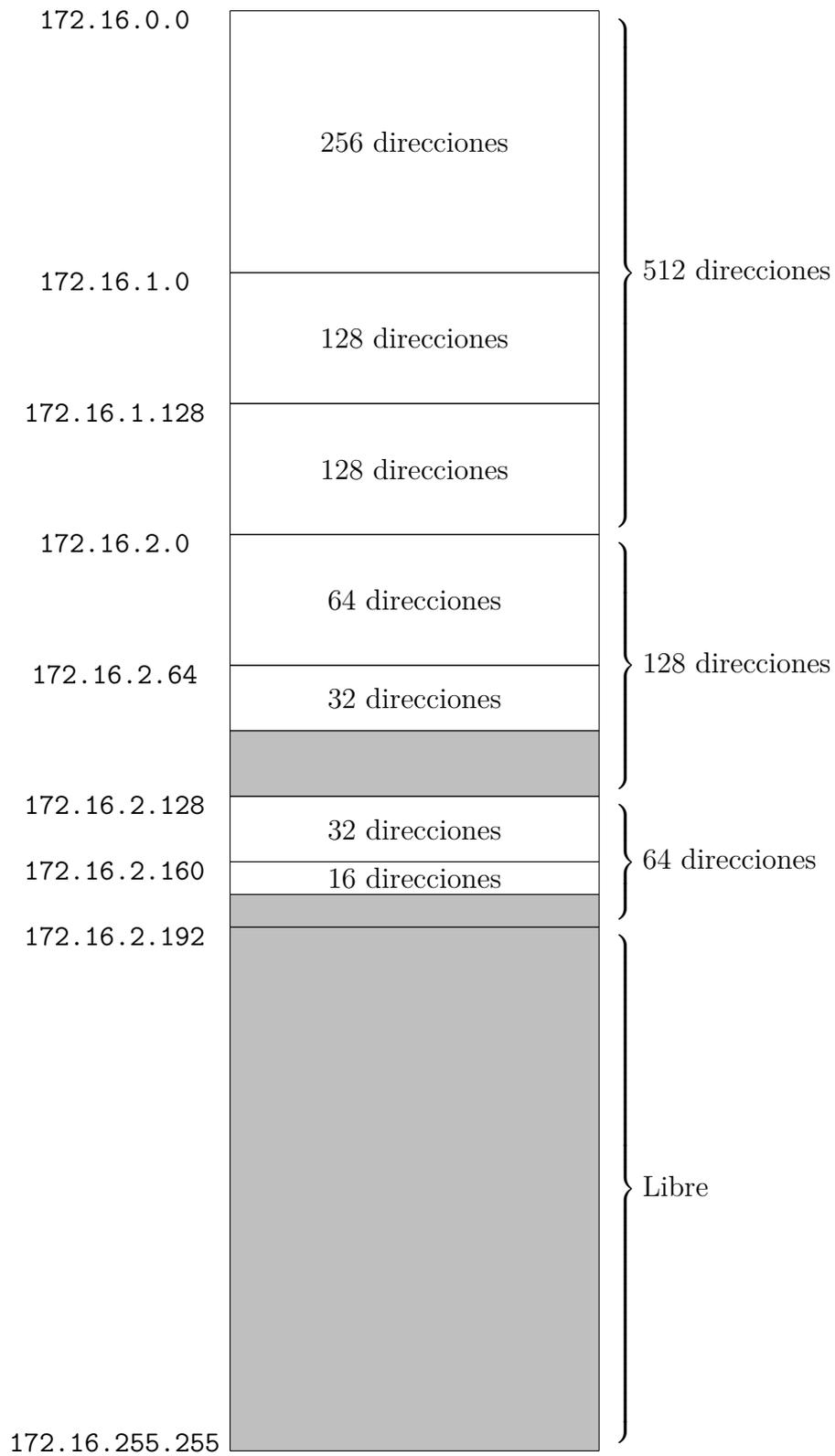


Figura 1.15: Reserva de los bloques dentro de cada súper-bloque.

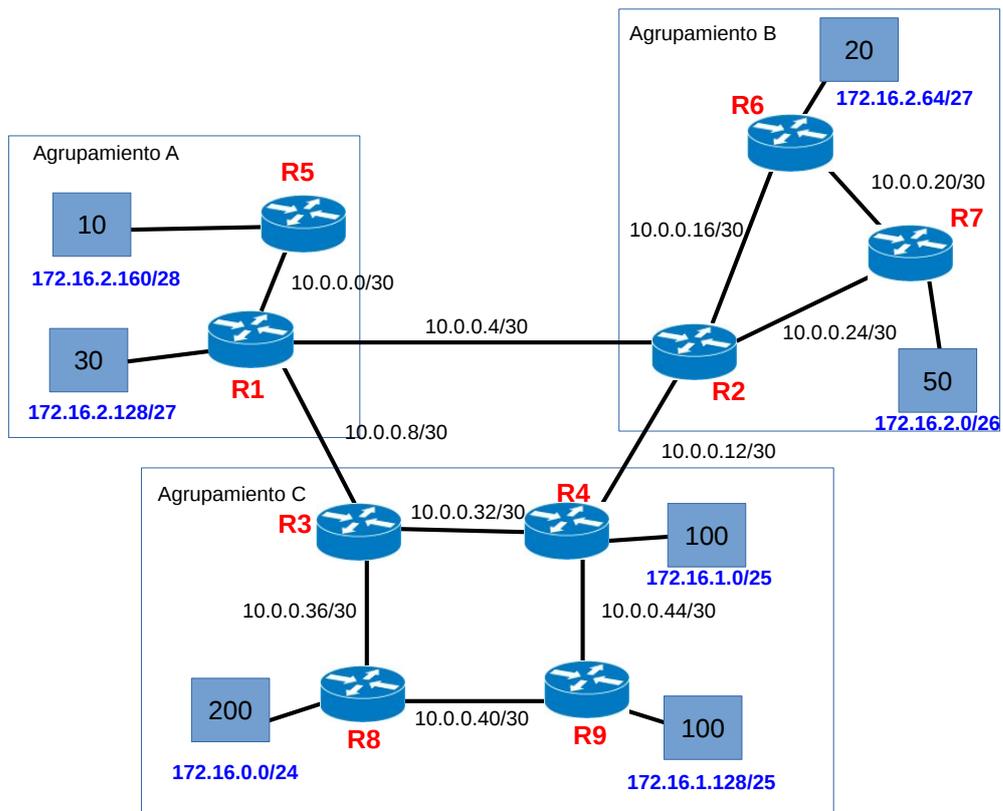


Figura 1.16: Asignación de direcciones a las redes.

# Capítulo 2

## Direccionamiento IPv6

### 2.1. Direcciones IPv6

El cambio más significativo de IPv6 respecto de IPv4 es la aplicación del espacio de direcciones de 32 a 128 bits. Esto, que a priori parece complicar el direccionamiento, favorece enormemente la agregación de rutas. La segunda diferencia importante es que ya no se emplean números decimales, sino que se pasan a utilizar conjuntos de cuatro dígitos hexadecimales separados por `:`. Cada dirección al estar formada por 128 bits queda representada por 8 conjuntos de este tipo. Pongamos un ejemplo de dirección IPv6:

```
2001:0DB8:0000:0000:0002:0000:5555:4777
```

Como las direcciones IPv6 son largas, los grupos de ceros iniciales se pueden omitir y los grupos formados por cuatro ceros se pueden sustituir por `0`. De este modo, la dirección anterior quedaría así:

```
2001:DB8:0:0:2:0:5555:4777
```

Para compactar aún más la notación, las cadenas de ceros se reemplazan con `::`. Como se muestra a continuación:

```
2001:DB8::2:0:5555:4777
```

Sin embargo, esto sólo se puede hacer una única vez, pues para recuperar la dirección habrá que rellenar el espacio entre los `:` con ceros hasta llegar a la longitud total de la dirección. Si lo hiciéramos varias veces no sabríamos cuántos ceros debemos insertar en cada uno de esos puntos.

### 2.2. Máscaras de red

Para definir los prefijos de red, en IPv6 se utiliza un mecanismo similar a las máscaras de red de IPv4. Lo único que ocurre es que, al ser las direcciones de mayor tamaño, los prefijos de red pueden ser más largos. Mientras que en IPv4, sin clases, podíamos encontrar prefijos

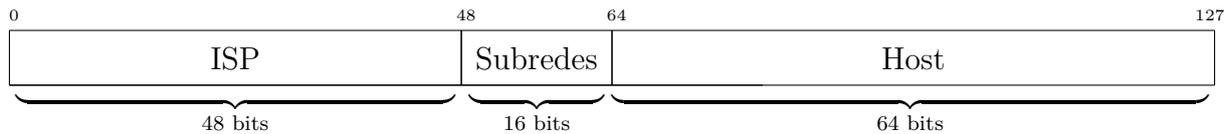


Figura 2.1: Distribución de bits en la dirección IPv6

CIDR de casi cualquier longitud entre 0 y 32 bits, en IPv6 existen unas reglas más estrictas, pues los primeros 48 bits están reservados para el enrutamiento en internet y los fija el ISP, los siguientes 16 son para subredes y los 64 restantes son para asignar direcciones a los dispositivos, tal y como se muestra en la figura 2.1.

Aunque es posible asignar prefijos más largos que 64 bits a las direcciones de los hosts, este proceder no se recomienda. Mientras que en IPv4 teníamos una escasez de direcciones, que obligaba a ahorrar, en IPv6 hay tal exceso que no supone un problema gastar  $2^{64}$  direcciones para un enlace punto a punto, que en realidad sólo requiere cuatro direcciones. Por tanto, a menos que trabajemos para un ISP o en un registro de direcciones de internet, sólo vamos a manejar los bits del 48 al 63 (16 bits) para crear el esquema de direccionamiento de la organización. En estas condiciones se pueden crear hasta  $2^{16} = 65536$  subredes, detrás del prefijo principal de la organización. En los dispositivos siempre se manejarán máscaras del tipo /64. Mientras que en las tablas de enrutamiento de los routers internos de la organización deberían manejarse prefijos entre 48 y 64 bits. La disponibilidad de 16 bits para la creación de subredes, sin que esto suponga un desperdicio de direcciones, permite crear esquemas de direccionamiento jerarquizados. Otro cambio importante es que en IPv6 **ya no existen las direcciones de broadcast**.

## 2.3. Tipos de direcciones

Hay que distinguir distintos tipos de direcciones IPv6, que se describen a continuación y cuyos prefijos se muestran en la tabla 2.1.

- **Direcciones de unidifusión global:** Son direcciones que se asignan a hosts y que tienen validez a nivel global (Internet).
- **Direcciones únicas globales:** Son direcciones que tienen validez únicamente dentro de un ámbito limitado como un sitio.
- **Direcciones de multidifusión:** Son direcciones que permiten hacer envíos de multidifusión.
- **Direcciones de bucle local:** Son direcciones que se emplean para depuración y se refieren al propio host. Sólo son válidas a nivel de host. Sustituyen a las direcciones del tipo 127.0.0.1 de IPv4.

## 2.4. Subredes en IPv6

Como se indicó anteriormente, en IPv6 disponemos de 16 bits para la creación de subredes. Esto permite crear esquemas de direccionamiento jerárquicos que van a facilitar la agregación

Tipo	Binario	Hexadecimal
Unidifusión global	001	2000::/3
Enlace local	1111 1110 10	FE80::/10
Multidifusión	1111 0000	F000::/8
Bucle local	00...1	::1/128
Única local	1111 1100	FC00::/7

Tabla 2.1: Prefijo de los distintos tipos de direcciones IPv6.

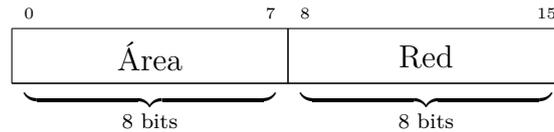


Figura 2.2: Reparto de bits dentro de la parte de subred de la dirección IPv6

de rutas.

La forma más sencilla de crear subredes es simplemente asignar un número a cada una de las subredes y ponerlo en la porción de 16 bits de la dirección. Por ejemplo, si el ISP nos asigna un prefijo 2001:60:60::/48, queremos 10 subredes, los prefijos serían:

```

2001:60:60::/64
2001:60:60:1::/64
2001:60:60:2::/64
2001:60:60:3::/64
2001:60:60:4::/64
2001:60:60:5::/64
2001:60:60:6::/64
2001:60:60:7::/64
2001:60:60:8::/64
2001:60:60:9::/64

```

La primera novedad que debemos advertir es que para elaborar este esquema de direccionamiento no ha hecho falta preocuparse por el número de hosts en cada subred, pues tenemos  $2^{64}$  direcciones en cada una de ellas.

Supongamos que tenemos una red que vamos a dividir en áreas. Para favorecer la agregación de rutas, debemos asignar un prefijo común a las redes pertenecientes cada área. Suponiendo que tenemos cuatro áreas y que cada área debe contener hasta 256 redes, repartimos los bits correspondientes a cada subred en dos partes, una para el área y otra para las redes dentro de ésta. Si asignamos los 8 primeros bits de la parte de subred al área y los 8 siguientes a las redes dentro del área, ya habremos resuelto nuestro problema. Esto es, establecemos una frontera a la mitad de la parte de subred de la dirección IPv6, como se muestra en la figura 2.2. Las redes quedarían definidas como se muestra en la tabla 2.2.

El reparto de bits dentro de la parte de subred de la dirección IPv6 también se podría haber hecho utilizando 4 bits para las áreas y 12 bits para las redes. El resultado se muestra en la tabla 2.3.

De los dos ejemplos anteriores, se deduce que lo más sencillo para obtener los distintos niveles de jerarquía es hacer las divisiones en fronteras de 4 bits, de modo que las divisiones

	Área 0	Área 1	Área 3	Área 4
Redes	2001:60:60:0::/64	2001:60:60:100::/64	2001:60:60:200::/64	2001:60:60:300::/64
	2001:60:60:1::/64	2001:60:60:101::/64	2001:60:60:201::/64	2001:60:60:301::/64
	2001:60:60:2::/64	2001:60:60:102::/64	2001:60:60:202::/64	2001:60:60:302::/64
	2001:60:60:3::/64	2001:60:60:103::/64	2001:60:60:203::/64	2001:60:60:303::/64
	2001:60:60:4::/64	2001:60:60:104::/64	2001:60:60:204::/64	2001:60:60:304::/64
	2001:60:60:5::/64	2001:60:60:105::/64	2001:60:60:205::/64	2001:60:60:305::/64
	2001:60:60:6::/64	2001:60:60:106::/64	2001:60:60:206::/64	2001:60:60:306::/64
	2001:60:60:7::/64	2001:60:60:107::/64	2001:60:60:207::/64	2001:60:60:307::/64
	2001:60:60:8::/64	2001:60:60:108::/64	2001:60:60:208::/64	2001:60:60:308::/64
	.	.	.	.
.	.	.	.	
.	.	.	.	
2001:60:60:FF::/64	2001:60:60:1FF::/64	2001:60:60:FF::/64	2001:60:60:3FF::/64	
Prefijo	2001:60:60::/56	2001:60:60:100::/56	2001:60:60:200::/56	2001:60:60:300::/56

Tabla 2.2: Subredes con jerarquía por áreas, utilizando 8 bits para el área y 8 para las redes dentro de cada área.

	Área 0	Área 1	Área 3	Área 4
Redes	2001:60:60:0::/64	2001:60:60:1000::/64	2001:60:60:2000::/64	2001:60:60:3000::/64
	2001:60:60:1::/64	2001:60:60:1001::/64	2001:60:60:2001::/64	2001:60:60:3001::/64
	2001:60:60:2::/64	2001:60:60:1002::/64	2001:60:60:2002::/64	2001:60:60:3002::/64
	2001:60:60:3::/64	2001:60:60:1003::/64	2001:60:60:2003::/64	2001:60:60:3003::/64
	2001:60:60:4::/64	2001:60:60:1004::/64	2001:60:60:2004::/64	2001:60:60:3004::/64
	2001:60:60:5::/64	2001:60:60:1005::/64	2001:60:60:2005::/64	2001:60:60:3005::/64
	2001:60:60:6::/64	2001:60:60:1006::/64	2001:60:60:2006::/64	2001:60:60:3006::/64
	2001:60:60:7::/64	2001:60:60:1007::/64	2001:60:60:2007::/64	2001:60:60:3007::/64
	2001:60:60:8::/64	2001:60:60:1008::/64	2001:60:60:2008::/64	2001:60:60:3008::/64
	.	.	.	.
.	.	.	.	
.	.	.	.	
2001:60:60:FFF::/64	2001:60:60:1FFF::/64	2001:60:60:2FFF::/64	2001:60:60:3FFF::/64	
Prefijo	2001:60:60::/52	2001:60:60:1000::/52	2001:60:60:2000::/52	2001:60:60:3000::/52

Tabla 2.3: Subredes con jerarquía por áreas, utilizando 4 bits para el área y 12 para las redes dentro de cada área.

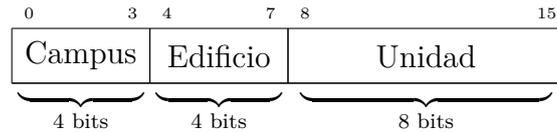


Figura 2.3: Ejemplo de reparto de bits dentro de la parte de subred de la dirección IPv6 para tres niveles de jerarquía

coincidan también con las fronteras de los dígitos hexadecimales. Si fuese necesario, se podría realizar la división en fronteras que no fuesen de 4 bits, y nos enfrentaríamos a las mismas dificultades que en IP versión 4. En la mayoría de los casos, los niveles de jerarquía pueden ajustarse fácilmente a fronteras de 4 bits.

Veamos un ejemplo de una jerarquía de direccionamiento con 3 niveles. Una red compuesta por 3 campus, cada uno de los cuales tiene una serie de edificios interconectados entre sí, y dentro de cada edificio se harán redes separadas para las distintas unidades organizativas, por ejemplo, departamentos. Con fronteras alineadas a 4 bits, podemos utilizar 4 bits para el identificador de campus, lo que nos permite un máximo de 16 campus, los siguientes 4 bits los podríamos utilizar para identificar los edificios y los 8 restantes para identificar las redes de cada una de las unidades organizativas. Esta división se muestra en la figura 2.3. De este modo, las redes dentro de cada campus quedarían agregadas con un prefijo de 52 bits, mientras que las redes dentro de cada edificio quedarían agregadas mediante un prefijo de 56 bits.



# Capítulo 3

## Ejercicios

### Ejercicio 1. Cálculo de direcciones de red

Indique si las dos direcciones IP que se indican en la tabla pertenecen o no la misma subred.

Dirección IP 1	Dirección IP 2	Máscara de red	¿Misma subred?
192.168.25.23	192.168.25.62	255.255.255.224	
192.168.25.64	192.168.25.129	255.255.255.224	
10.213.4.56	10.213.100.25	/16	
175.13.192.93	175.13.193.1	255.255.224.0	
137.85.67.111	137.85.67.112	/30	
206.195.18.22	206.196.16.20	255.248.0.0	

### Ejercicio 2. Cálculo de direcciones de red y broadcast

Calcule las direcciones de red y de broadcast correspondientes a una dirección IP dada la máscara de subred.

Dirección IP	Máscara de subred	Dirección de red	Dirección de broadcast
192.168.1.15	255.255.255.0		
192.168.1.1	/27		
10.213.100.34	255.255.0.0		
126.84.76..221	255.255.255.224		
206.195.18.35	255.192.0.0		

### Ejercicio 3. Cálculo de subredes

Rellene los datos que faltan en la siguiente tabla.

Prefijo de red	Máscara de subred	Nº de subredes	Nº de hosts en cada subred
/23	/27		
/13		8	
	/24	256	
		16	6

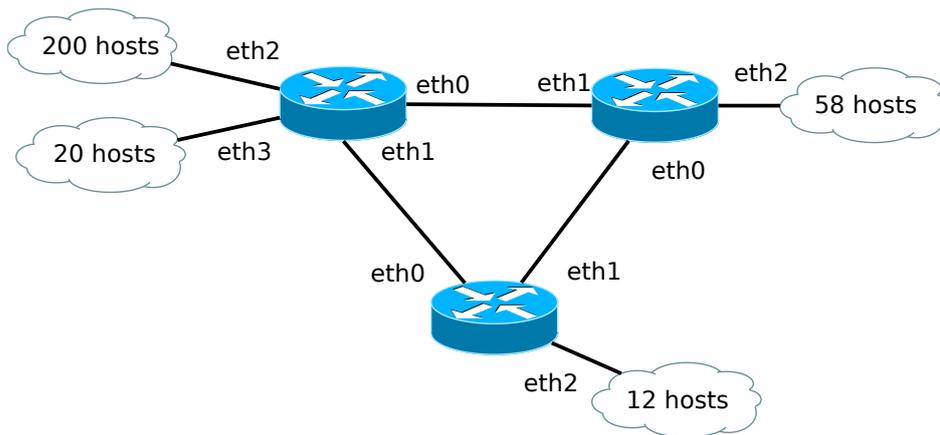


Figura 3.1: Esquema de red.

#### Ejercicio 4. Enrutamiento

Dada la siguiente tabla de enrutamiento:

Red	Máscara	Interfaz	gateway
192.168.0.0	/24	eth1	-
192.168.1.0	/24	wlan0	-
172.16.0.0	/16	eth1	192.168.0.1
172.16.1.0	/24	wlan0	192.168.1.1
0.0.0.0	/0	eth1	192.168.0.1

- Indique qué entradas son aplicables a un paquete IP dirigido a la dirección 172.16.1.58. Seleccione la entrada que finalmente se aplicará.
- Indique qué entrada se aplicará a un paquete dirigido a la dirección 192.168.0.25.
- Indique cuál es la ruta por defecto.

#### Ejercicio 5. Direccionamiento IPv4 y enrutamiento

Dado el esquema de la figura 3.1.

- Elabore el esquema de direccionamiento VLSM (no es necesario favorecer la agregación de rutas) para la red suponiendo que el prefijo global es 80.0.0.0/16.
- Elabore las tablas de enrutamiento para cada uno de los routers, utilizando el número de saltos como métrica para obtener las rutas óptimas.

#### Ejercicio 6. Direccionamiento favoreciendo la agregación de rutas

Elabore un esquema de direccionamiento favoreciendo la agregación de rutas para el esquema que se muestra en la figura 3.2. Asuma el prefijo global 11.0.0.0/8. Decida los agrupamientos de redes que deben sumarse.

Una vez creado el esquema de direccionamiento, escriba la tabla de enrutamiento del router R1. La puerta de enlace a internet es la dirección IP 7.7.8.7.

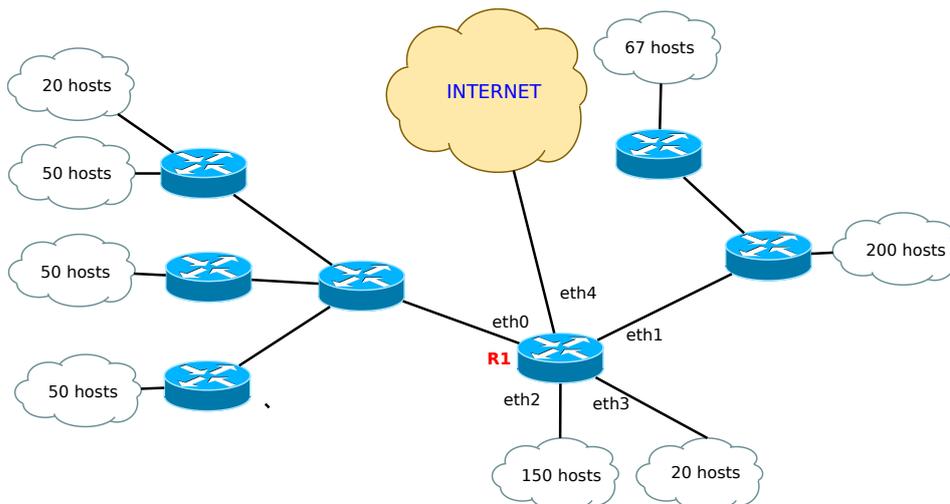


Figura 3.2: Esquema de red.

### Ejercicio 7. Direccionamiento IPv6

Elabore un esquema de direccionamiento IPv6 para el esquema de red de la figura 3.1. Asuma que el prefijo global de la organización es el  $2001:5:5::/48$

### Ejercicio 8. Direccionamiento IPv6 favoreciendo la agregación de rutas

Elabore un esquema de direccionamiento IPv6 para la red que se muestra en la 3.2. Asuma que el prefijo global de la red es  $2001:0:1::/48$ . Luego escriba la tabla de enrutamiento del router R1.

### Ejercicio 9. Direccionamiento IPv6 favoreciendo la agregación de rutas

Elabore un esquema de direccionamiento IPv6 para las redes que se muestran en la figura 3.3 (las redes se indican con los cuadrados rellenos de color azul). Prepare el esquema de direccionamiento para favorecer la agregación de rutas. Asuma que el prefijo de red asignado por el ISP a la organización es  $2001:AAAA:AAAA::/48$ . No olvide incluir las redes de interconexión entre los router.

### Ejercicio 10. Enrutamiento

Escriba la tabla de enrutamiento del router etiquetado como R1 del ejercicio 9.

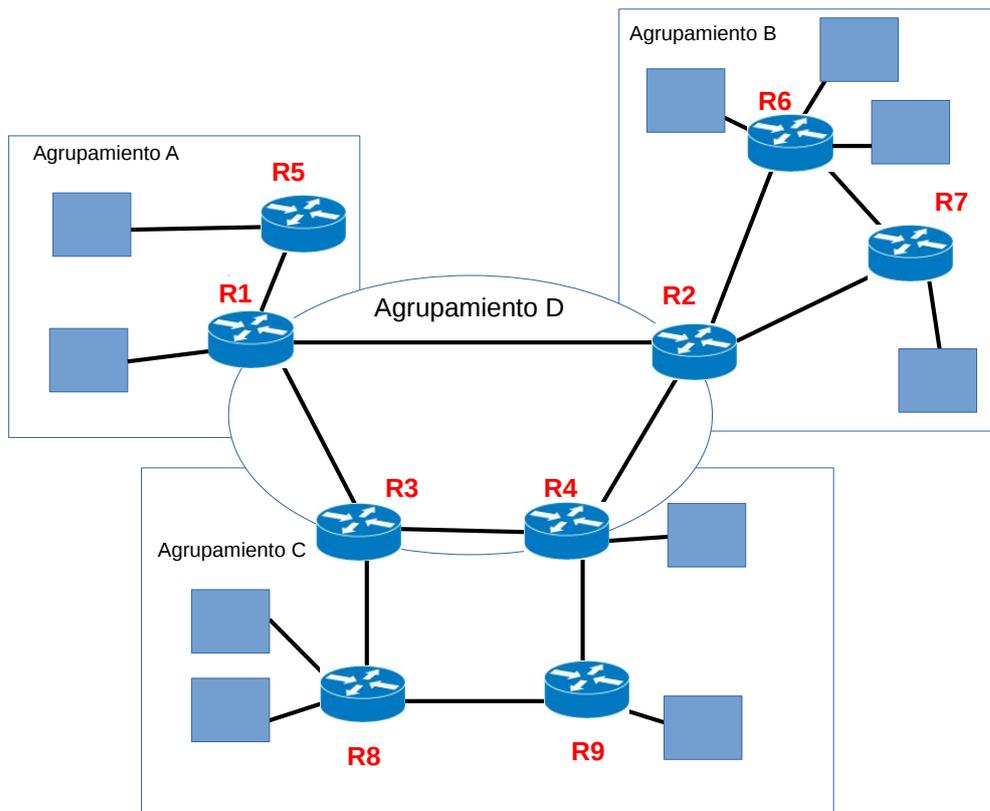


Figura 3.3: Esquema de red.

# Bibliografía

- [RFC 791] J. Postel. *Internet Protocol*. RFC 791 (INTERNET STANDARD). Updated by RFCs 1349, 2474, 6864. Internet Engineering Task Force, sep. de 1981. URL: <http://www.ietf.org/rfc/rfc791.txt>.
- [RFC 950] J. Mogul y J. Postel. *Internet Standard Subnetting Procedure*. RFC 950 (INTERNET STANDARD). Updated by RFC 6918. Internet Engineering Task Force, ago. de 1985. URL: <http://www.ietf.org/rfc/rfc950.txt>.
- [RFC 1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot y E. Lear. *Address Allocation for Private Internets*. RFC 1918 (Best Current Practice). Updated by RFC 6761. Internet Engineering Task Force, feb. de 1996. URL: <http://www.ietf.org/rfc/rfc1918.txt>.
- [RFC 2663] P. Srisuresh y M. Holdrege. *IP Network Address Translator (NAT) Terminology and Considerations*. RFC 2663 (Informational). Internet Engineering Task Force, ago. de 1999. URL: <http://www.ietf.org/rfc/rfc2663.txt>.
- [RFC 1519] V. Fuller, T. Li, J. Yu y K. Varadhan. *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*. RFC 1519 (Proposed Standard). Obsoleted by RFC 4632. Internet Engineering Task Force, sep. de 1993. URL: <http://www.ietf.org/rfc/rfc1519.txt>.
- [RFC 1878] T. Pummill y B. Manning. *Variable Length Subnet Table For IPv4*. RFC 1878 (Historic). Internet Engineering Task Force, dic. de 1995. URL: <http://www.ietf.org/rfc/rfc1878.txt>.
- [RFC 1518] Y. Rekhter y T. Li. *An Architecture for IP Address Allocation with CIDR*. RFC 1518 (Historic). Internet Engineering Task Force, sep. de 1993. URL: <http://www.ietf.org/rfc/rfc1518.txt>.
- [RFC 2131] R. Droms. *Dynamic Host Configuration Protocol*. RFC 2131 (Draft Standard). Updated by RFCs 3396, 4361, 5494, 6842. Internet Engineering Task Force, mar. de 1997. URL: <http://www.ietf.org/rfc/rfc2131.txt>.