Protocolo IP versión 4

1. Principios

IP genera una entrega de paquetes sin conexión y sin garantía. Uno de sus principales inconvenientes es que necesita la implementación de un plan de direccionamiento explícito. Cada nodo de red se tiene que identificar con una dirección IP. Esta se divide en dos partes: un número de red lógico y una dirección de equipo en la red lógica.

Se podría representar el número de red IP como el nombre de una calle y el número de servidor como una dirección de esa calle.

Uno de los aspectos interesantes de IP es que se puede configurar para que se garantice un tipo de servicio específico. Entre estos, se puede citar la implementación de un envío urgente de un paquete que se debe transmitir rápidamente, o de políticas para incrementar la velocidad cuando se debe transferir una gran cantidad de información, o bien optimizar la fiabilidad en la transmisión para un flujo en el que no se puede permitir que haya ningún error.

2. Direccionamiento

a. La dirección IPv4

La utilización de TCP/IP requiere que el administrador defina un plan de direccionamiento, asignando una dirección IP para cada nodo activo de red.

Una dirección IP versión 4 se representa con 4 bytes. Se utiliza la notación decimal punteada, es decir, cada byte se separa con un punto: 132.148.67.2

Según el valor del primer byte, es posible conocer la clase de dirección IP, es decir, el número de bytes utilizados para el número de red y los que quedan para el equipo.

Esto no siempre es cierto. De hecho, es posible, en algunos casos, recurrir al *subnetting*, es decir, se utiliza una parte de los bits del servidor pertenecientes a cierta clase para cifrar un número de subred. Se habla de *supernetting* cuando es una parte del número de red de la clase predeterminada la que se utiliza para cifrar equipos suplementarios.

b. La máscara

Enfoque directo

Se utiliza una máscara de red secundaria para identificar la parte de la dirección IP que corresponde a la red, de la parte que identifica al nodo. Si se escribe la dirección IP en forma binaria, cualquier bit asociado al número de red se representará como ‘1’ en la máscara y como ‘0’ si no está asociado.

Un byte cuyo valor binario es 1111 1111 equivale a 255 en decimal. Como la dirección IP se representa con 4 bytes (32 bits), las máscaras pueden ser:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

Más adelante veremos que una máscara no puede tomar como valor 255.255.255.255.

Enfoque computacional

La tarjeta de red o el router que ejecuten IP efectuarán un cálculo simple para encontrar el número lógico de red:

RL = IP Y máscara binaria

En la calculadora de Windows en modo «Programador», el Y binario se representa con el operador «And».

Así, si A dispone de la siguiente información:

IPA = 131.107.8.1

mA = 255.255.0.0

RLA = IPA Y mA

RLA = 131 Y 255 . 107 Y 255. 8 Y 0. 1 Y 0

Luego RLA = 131.107.0.0

La descomposición opera como en la clase B, en dos bytes para el número de red y dos bytes para el número de equipo.

Si ahora la máscara utilizada es 255.255.255.0, el número de red lógico es el siguiente:

RLA = 131 Y 255. 107 Y 255. 8 Y 255. 1 Y 0

O sea:

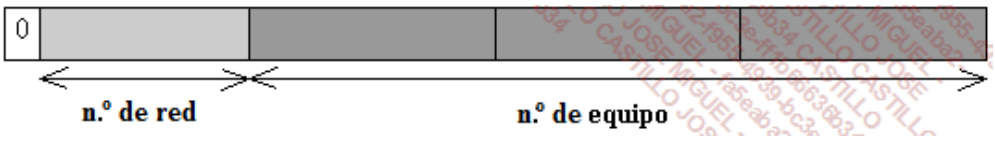
RLA = 131.107.8.0 y la descomposición opera en 3 + 1.

c. Clases de direcciones

Clases

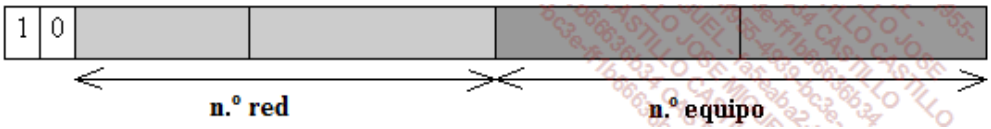
Para identificar un equipo de manera única, se definen tres clases de direcciones.

Clase A, el primer byte se ubica entre 1 y 126. Se utilizan 7 bits para el número de red y 24 bits para identificar el equipo. Una red de clase A puede soportar hasta 16 millones de equipos (2^{24}-2 posibilidades).



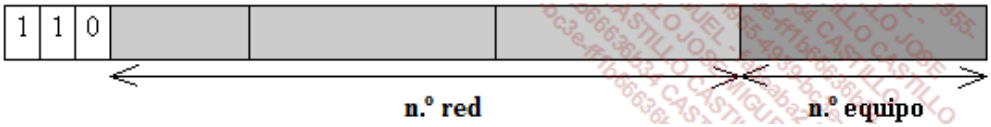
Por ejemplo, 112.2.1.4 es una dirección de clase A. ’112’ define el número de red y ’2.1.4’ el número de equipo.

En una clase B, el primer byte varia entre 128 y 191. Con 14 bits se hace el cifrado del número de red y con 16 bits el número de equipo. Se puede definir hasta 65.534 equipos en una misma red (2^{16}-2). La máscara por defecto es 255.255.0.0.



132.148.67.2 es de clase B. '132.148' es el número de red y '67.2' el número de equipo.

La clase C está definida por un primer byte variable de 192 a 223. Se utilizan 21 bits para la red y 8 para el equipo. Podemos tener hasta 254 equipos por red en clase C.



193.10.2.117 es de clase C. '192.10.2' es la parte que identifica la red y '117' el equipo.

Direcciones particulares

Un número de red o un número de equipo no pueden tener todos sus bits en 0 o en 1. Estos casos particulares se reservan para situaciones concretas.

Por ejemplo, para una difusión, todos los bits del «equipo» de la dirección IP se ponen a '1'.

Por ejemplo, la dirección 132.148.255.255 identifica a todos los equipos de la red 132.148.

Hay que tener en cuenta que en algunos sistemas Unix es posible configurar una difusión con todos los bits en '0', para mantener la compatibilidad con otros sistemas.

El número de red actual se anota poniendo todos los bits del equipo en '0'.

Por ejemplo, 132.148.0.0 se asocia con el número de red lógico 132.148.

A veces se puede identificar una estación de la red sustituyendo el número de red por '0'.

Por ejemplo, 0.0.67.2 corresponde al equipo 132.148.67.2 de la red 132.148.0.0.

En cuanto a la dirección de bucle local 127.0.0.1, pertenece a la propia tarjeta de red, sin salir a la red.

d. Direcciones privadas

Hay un cierto número de direcciones IP que se reservan para utilizarlas en la red interna. Estas direcciones definidas en RFC 1918 permiten asegurar a un servidor Proxy (que administra la conexión a Internet de una empresa) una diferenciación satisfactoria entre la red pública (Internet) y la red privada (intranet). Así, cada empresa conectada a Internet puede utilizar las mismas direcciones IP privadas internamente y diferenciar los accesos a Internet por medio de una única dirección IP pública externa.

Estas direcciones IP privadas son:

- 10.0.0.0 en 10.255.255.255.
- 172.16.0.0 en 172.31.255.255.
- 192.168.0.0 en 192.168.255.255.

e. Las direcciones APIPA

Microsoft utiliza la asignación automática de IP privadas o *Automatic Private IP Addressing* (APIPA) para proporcionar una dirección IP a aquellos ordenadores que no encuentran un servidor DHCP. De este modo, todos los ordenadores que se encuentran en la misma situación pueden comunicarse entre ellos a pesar de todo.

Este rango de direcciones va de 169.254.0.0 a 169.254.255.255.

Los dos últimos bytes de la dirección se generan utilizando como entrada la dirección MAC, que inicializa el algoritmo de generación aleatoria. La RFC 3927 describe las características de APIPA: http://tools.ietf.org/html/rfc3927

3. El direccionamiento sin clase

a. Principios

Con el creciente aumento del número de ordenadores conectados a Internet, las direcciones IP versión 4 aún disponibles se hacen cada vez más escasas. Gracias a la generalización de la utilización de servidores Proxy y rangos de direcciones IP privadas (RFC 1918), ha sido posible añadir grupos de miles de ordenadores, simplemente asignando una dirección IP pública al Proxy. Así, la escasez de IP se hace menos problemática de lo que se había previsto.

Sin embargo, la descomposición en clases generó un derroche colosal de direcciones, que se ha evitado reasignando algunos rangos.

Por ejemplo, imaginemos que a una empresa se le ha asignado un rango de direcciones de 60.0.0.0 a 60.255.255.255 y que, en realidad, solo utiliza desde la subclase 60.1 a 60.10. ¿Cómo hacer para recuperar las direcciones 60.11 a 60.255?

Basta con considerar las direcciones IP no como de clase A, sino más bien de clase B. Así, un router sabrá diferenciar entre las direcciones del primer tramo y las del segundo tramo.

Consideremos ahora que las clases de direcciones ya no existen y que, por lo tanto, la máscara utilizada no es necesariamente la de la clase predeterminada.

Por ejemplo, una empresa que quiere poner en línea algunos servidores puede pedir que se le asigne el siguiente rango de 8 direcciones: 61.178.203.56 a 61.178.203.63. Se le proporcionará con una máscara 255.255.255.248 (es decir, que 5 bits del 4.° byte se utilizarán para las redes y 3 bits para los huéspedes). El prefijo correspondiente es 61.178.203.56. El último byte, escrito en binario, proporciona los siguientes valores:

56 = 0011 1000

57 = 0011 1001

58 = 0011 1010

59 = 0011 1011

60 = 0011 1100

61 = 0011 1101

62 = 0011 1110

63 = 0011 1111

Los 5 bits de peso del último byte se asocian a una parte que define el número lógico de red.

Una máscara 255.255.255.248 en binario corresponde a 1111 1111.1111 1111.1111 1111.11111000.

11111000 representa la escritura binaria del último byte de la máscara y equivale a 248 (128 + 64 + 32 + 16 + 8).

b. La notación CIDR

La notación *Classless InterDomain Routing* (CIDR) ofrece una escritura sintética de la máscara de red secundaria.

Así, si la máscara es 255.0.0.0, significa que habrá 8 bits en 1 para la escritura binaria de la máscara, lo que se escribirá como /8.

Generalmente se anotará como **/n**, donde n representa el número de bits en 1 de la máscara, es decir, el número de bits de la dirección IP que servirán para cifrar una parte de la red lógica.

En la mayoría de los casos, los bits en 1 de la máscara serán los bits de peso (los del extremo izquierdo) y nunca se debe confundir el 1 con el 0 en la máscara.

Así, la máscara 255.255.0.0 se escribirá /16 en notación CIDR.

La máscara 255.255.255.0 se escribirá /24.

Según el ejemplo anterior, la máscara 255.255.255.248 se escribirá /29.

La utilización de una asignación de direcciones sin clase ofrece una descomposición de las direcciones IP por medio de máscaras /8 a /30.

Algún hardware implementa la introducción de la máscara en notación CIDR.

c. El papel de la máscara de red

Inicio de un paquete de datos

En el capítulo Estandarización de protocolos, hemos visto que una tarjeta de red comprueba si el destinatario se encuentra en la misma red lógica. Según sea el caso, esta tarjeta de red recurre a la puerta de enlace predeterminada o se dirige directamente a su destinatario.

Llamemos A al emisor. Conoce su dirección IP (IPA), su máscara (mA) y la dirección física de la tarjeta de red (PHYA).

Como emisora del paquete de datos, esta máquina A solo conoce del destino la dirección IP. En las explicaciones

siguientes, denominaremos B al equipo de destino, y a su dirección IP, IPB.

Para poder enviar el paquete de datos, A tiene que saber, en primer lugar, si la red lógica de B (RLB) es la misma que la suya (RLA). Ahora bien, A solo conoce la dirección IPB, pero no la máscara correspondiente. Por lo tanto, le es imposible encontrar RLB directamente.

Por eso A tiene que encontrar un modo de encontrar RLB. Para ello, A utiliza su propia máscara mA, conjuntamente con la dirección IPB. Efectúa su propia interpretación de lo que podría ser RLB.

Tampoco podemos olvidar el tratamiento de nivel 2. En efecto, A y B pueden o no estar sobre la misma red.

Citaremos para los siguientes ejemplos el protocolo ARP, que se explicará más adelante. Por ahora, debemos saber que ARP permite interrogar a la red de difusión para encontrar la dirección de nivel 2 de una estación y establecer la relación con su dirección IP. Para no efectuar sistemáticamente esta consulta, se mantiene una caché que permite guardar una lista de direcciones MAC y sus direcciones IP correspondientes.

Teóricamente, se pueden identificar cuatro casos:

1) A interpreta RLB como equivalente a RLA y A y B están en la misma red de nivel 2.

2) A interpreta RLB como no equivalente a RLA y A y B están en la misma red de nivel 2.

3) A interpreta RLB como equivalente a RLA y A y B no están en la misma red de nivel 2.

4) A interpreta RLB como no equivalente a RLA, A y B no están en la misma red de nivel 2.

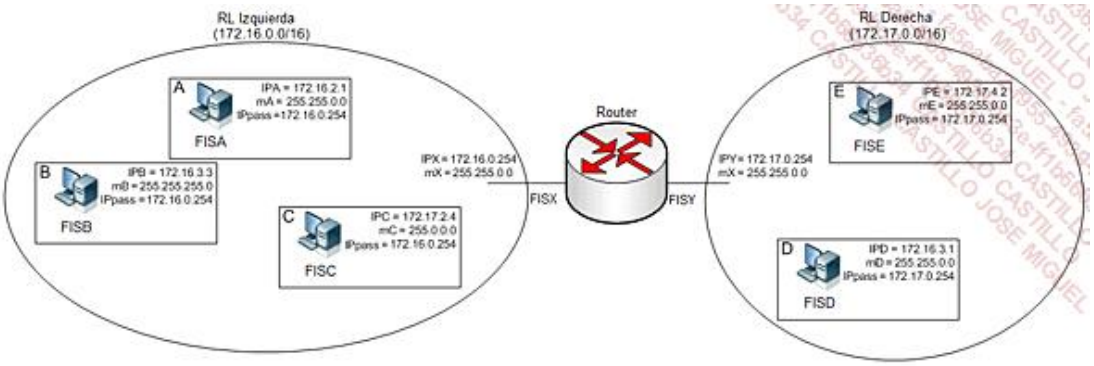
Podemos señalar que el tercer caso parece incoherente. De hecho, puede parecer ilógico prolongar una misma red IP más allá del espacio de difusión de nivel 2.

Vamos a estudiar las interpretaciones de direcciones con ejemplos sencillos: el funcionamiento de una consulta «ping». La comunicación es necesariamente doble, con el tratamiento de la ida (pregunta) y el de la vuelta (retorno) de los paquetes de datos.

Incidencias de máscaras erróneas sobre la distribución de los paquetes de datos IP

Aquí vamos a examinar una comunicación en una red que dispone de una asignación de direcciones incorrecta o de máscaras erróneas.

En la configuración que se presenta a continuación, podemos observar que mA, mB y mC son distintas entre sí. Además, mB y mC no corresponden a la máscara del router (puerta de enlace) mX. La red lógica que puede ser determinada al nivel de la puerta de enlace es 172.16.0.0. Observemos que la IPC no puede corresponder a una dirección en esta red lógica. Por el otro lado de nuestro router, RLD es diferente a RLE y RLY.



Vamos a explicar esta arquitectura para estudiar la incidencia de una máscara errónea en la distribución de los paquetes de datos. Para ello vamos a desglosar los mecanismos subyacentes relacionados con la instalación de la comunicación.

Envío de A hacia B

Como hemos visto anteriormente, el emisor A trata de comparar su red lógica con la del destinatario B. Los datos de cada uno son los siguientes:

IPA = 172.16.2.1 y mA = 255.255.0.0, por lo que RLA es igual a 172.16.0.0.

IPB = 172.16.3.3 y mA = 255.255.0.0, por lo que RLB visto por A es igual a 172.16.0.0.

Observamos que hay igualdad entre RLA y RLB supuesta por A. Por otra parte, A y B están en la misma red de nivel 2. Por este motivo es normal considerar que A y B estén en la misma red lógica.

Para crear su paquete de datos, A busca en primer lugar la dirección de nivel 2 (MAC) de B. Si no dispone de esta información en memoria, difunde una consulta de nivel 2, ARP. Esta consulta llegará al conjunto de equipos de la parte izquierda del diagrama. El router bloquea esta difusión.

Cuando dispone de su propia dirección física y de la de B, A emite una trama de FISA hacia FISB (nivel 2) y un paquete de datos de IPA hacia IPB (nivel 3).

El destinatario B recibe los datos.

Envío de B hacia A

El proceso es igual que en el caso anterior: B intenta encontrar la red lógica de A para compararla con la suya.

IPB = 172.16.3.3 y mB = 255.255.255.0, por lo que RLB es igual a 172.16.3.0.

IPA = 172.16.2.1 y mB = 255.255.255.0, por lo que RLA visto por B es igual a 172.16.2.0.

Observamos que la asignación de direcciones de nivel 3 es diferente entre los dos equipos, aunque pertenecen a la misma red de difusión y parecen pertenecer a la misma subred IP. Esto parece poco lógico.

Tanto es así que B, al constatar que debe cambiar de red lógica para llegar a A, se dirige a la IP de enlace, el router de la red lógica.

En primer lugar, se debe conocer a través de una consulta ARP de la caché correspondiente de B la dirección física FISX correspondiente a IPX. La trama está construida de FISB hacia FISX, para dirigir la información hacia el router. El paquete de datos, por su parte, informa que IPB es el emisor e IPA el destinatario.

Una vez que ha llegado al router, este debe tratar la información.

Distribución de un paquete de datos a través del router

Cuando recibe el paquete de datos, el router consulta su tabla de transporte para encontrar una ruta que corresponda a la red supuesta de A, aplicando la máscara especificada.

La siguiente tabla de transporte es la de un ordenador Linux equipado con dos tarjetas de red que simula nuestro router.

```
[root@linus /root]# netstat -rn
Kernel IP routing table
Destination   Gateway       Genmask        Flags MSS Window  irtt Iface
172.17.0.2    0.0.0.0         255.255.255.255 UH        0 0      0 eth0
192.168.6.0   172.16.206.1    255.255.255.0   UG        0 0      0 eth1
192.168.5.0   172.16.205.1    255.255.255.0   UG        0 0      0 eth1
192.168.4.0   172.16.104.1    255.255.255.0   UG        0 0      0 eth1
192.168.3.0   172.16.103.1    255.255.255.0   UG        0 0      0 eth1
192.168.2.0   172.16.102.1    255.255.255.0   UG        0 0      0 eth1
192.168.1.0   172.16.101.1    255.255.255.0   UG        0 0      0 eth1
192.168.16.0  172.16.206.1    255.255.255.0   UG        0 0      0 eth1
192.168.15.0  172.16.205.1    255.255.255.0   UG        0 0      0 eth1
192.168.14.0  172.16.104.1    255.255.255.0   UG        0 0      0 eth1
192.168.13.0  172.16.103.1    255.255.255.0   UG        0 0      0 eth1
192.168.12.0  172.16.102.1    255.255.255.0   UG        0 0      0 eth1
192.168.11.0  172.16.101.1    255.255.255.0   UG        0 0      0 eth1
10.108.2.0    172.17.208.208  255.255.255.0   UG        0 0      0 eth0
192.168.8.0   172.16.208.1    255.255.255.0   UG        0 0      0 eth1
172.16.0.0    0.0.0.0         255.255.0.0     U         0 0      0 eth1
172.17.0.0    0.0.0.0         255.255.0.0     U         0 0      0 eth0
127.0.0.0     0.0.0.0         255.0.0.0       U         0 0      0 lo
[root@linus /root]#
```

En la red 172.16, se declaran varias rutas que permiten el acceso a otras redes lógicas.

Por ejemplo, se puede acceder a las redes 192.168.5.0/24 y 192.168.15.0/24 a partir del router que tiene la dirección IP 172.16.205.1, en la red 172.16.0.0/16.

Para identificar una dirección de destino exacta con relación a una entrada de la tabla de enrutamiento, se utiliza una máscara 255.255.255.255, es decir, que la dirección IP comparada deberá volver a dar exactamente la dirección IP examinada.

Por el contrario, se definirá una ruta predeterminada con 0.0.0.0 con una máscara 0.0.0.0. Cualquiera que sea la dirección de destino examinada, encontrará inevitablemente el resultado 0.0.0.0. Esta ruta ineludiblemente se examina en último lugar en un tabla y corresponde a una clase de itinerario BIS o de «Otras direcciones» en un router.

De esta manera, el router conoce la existencia de las redes lógicas 172.16.0.0/16 (izquierda) y 172.17.0.0/16 (derecha). Dispone de sus propias máscaras para las redes lógicas que conoce.

Cuando recibe el paquete de datos, el router compara las rutas y se da cuenta de que la red lógica de A está a la izquierda. Entonces, reconstruye un paquete de datos utilizando IPA y PHYA.

La información llegará a su destino, incluso aunque la dirección lógica parezca errónea. Por el contrario, aunque A y B estén en la misma red de nivel 2, no pueden comunicarse directamente y la información tiene que circular por el router.

Envío de A hacia C

Después de superponer su máscara en IPC, A ve a C en una red lógica distinta de la suya y por tanto se dirige al router. Sin embargo, al contrario que en el caso anterior, el router envía el paquete de datos por el lado derecho a la red lógica 172.17.0.0. El equipo C no puede responder a la consulta ARP porque no está en esa red lógica. Por lo tanto, la información no se puede transmitir al destinatario final.

Envío de A hacia D

A interpreta la dirección IPD como si estuviera en la misma red lógica que la suya, IPA. Por lo tanto, intenta dirigir directamente la información mediante una difusión ARP. Esta no puede pasar el router y no llega a destino. La comunicación se detiene.

Envío de A hacia E

Este caso presenta una coherencia completa en cuanto a asignación de direcciones lógica respecto al espacio de difusión. El paquete de datos se envía al router y llega a su destino.

d. La descomposición en subredes

Contexto

Primera hipótesis

Imaginemos que trabajamos en una gran empresa que dispone de varios emplazamientos, una sede y cinco sucursales. Cada sucursal se conecta a Internet pasando por la sede por medio de una conexión dedicada. Solo la sede dispone de conexión directa a Internet.

Somos los responsables de la implementación del plan de asignación de direcciones a nivel local. Por ejemplo, el arquitecto que definió el plan de asignación de direcciones nacional nos impone utilizar un único rango de direcciones privadas (según la RFC 1918), que es 172.16.0.0 - 172.16.255.255.

Ahora bien, *in situ* tenemos un gran número de puestos de red y varios routers.

Necesariamente debemos utilizar este prefijo impuesto para efectuar una descomposición de este rango en varios rangos distintos para cada una de las redes lógicas.

Segunda hipótesis

Nos asignan un pequeño rango de direcciones IP públicas para publicar servidores en Internet. Sin embargo, a causa de la infraestructura de red existente, debemos utilizar este único rango de direcciones para desplegar dos rangos en vez de uno.

Primera solución (enfoque intuitivo)

Imaginemos que en la sucursal deben disponer de 5 redes lógicas. Por tanto, debemos dividir el rango que tenemos en 5 rangos de direcciones.

Una primera solución sencilla y evidente consiste en pasar de un identificador de red lógico cifrado de 2 bytes a un identificador cifrado de 3 bytes.

Así, podríamos tener:

- RL1 = 172.16.1.0/24, como rango de direcciones 172.16.1.0 a 172.16.1.255.
- RL2 = 172.16.2.0/24, como rango de direcciones 172.16.2.0 a 172.16.2.255.
- RL3 = 172.16.3.0/24, como rango de direcciones 172.16.3.0 a 172.16.3.255.
- RL4 = 172.16.4.0/24, como rango de direcciones 172.16.4.0 a 172.16.4.255.
- RL5 = 172.16.5.0/24, como rango de direcciones 172.16.5.0 a 172.16.5.255.

Estos rangos son teóricos. Hay que reservar las direcciones utilizables: aquellas en las que todos los bits del equipo son 0 o 1. Los rangos irán realmente de 172.16.x.1 a 172.16.x.254.

Una red lógica 172.16.0.0/16 tiene 65.534 (2^{16} - 2) direcciones IP utilizables.

Estas redes lógicas con una máscara de 24 bits solo pueden direccionar 254 direcciones IP cada una, es decir, 5 x 254 = 1270 direcciones.

La diferencia con las direcciones utilizables es notable. Como contrapartida, la máscara de clase C simplifica este planteamiento.

Por el contrario, a menos que necesitemos 254 redes lógicas, la pérdida de direcciones IP es muy elevada.

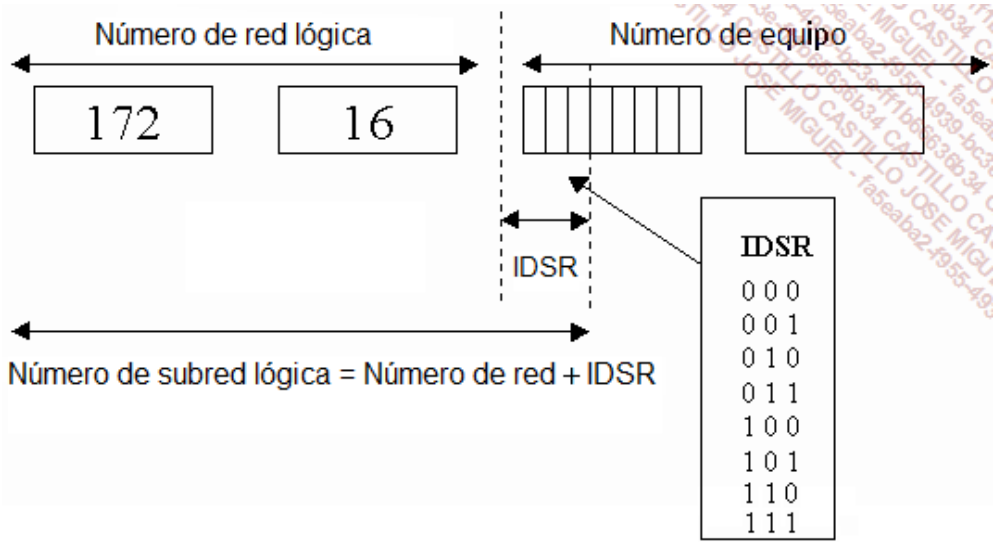
Segunda solución (la buena)

Hipótesis básica

Ahora, el objetivo consiste en encontrar una descomposición que optimice el número de redes secundarias requeridas. Si retomamos el ejemplo anterior, se busca una codificación que permita conservar un máximo de equipos en función del número de redes lógicas.

Por ejemplo, dada una subred 172.16.0.0 y un número de redes lógicas NmRL = 5, y considerando que el número máximo de equipos por red lógica es NmH = 200, ¿cuántos bits de la parte equipo inicialmente disponible son necesarios para cifrar NmRL redes lógicas?

Cada una de estas RL será de hecho una subred, cuyo número está compuesto por el de la red lógica y el identificador de subred (IDSR).



Etapa 1: cálculo del número de bits para cifrar el número de redes lógicas

Es necesario encontrar el número de bits (NmBITS) necesario para cifrar el número de redes lógicas (NmRL).

NmRL tiene que ser inferior o igual a 2^{NmBITS}.

Para simplificarlo, a continuación se puede ver un cuadro para realizar los cálculos.

La primera columna indica el número de bits utilizados (NmUtil).

La segunda expresa el número de posibilidades de cifrado para NmUtil (NmPos). La primera línea muestra dos posibilidades, 0 o 1. La siguiente línea se multiplica por 2.

La tercera columna, NmRetenidos, contiene el número de direcciones realmente utilizadas una vez hemos eliminado todas aquellas en que todos los bits son 0 o 1. Para esto, siempre se resta 2 de la anterior.

Tenga en cuenta que, desde la RFC 1878, un identificador de subred (IDSR) puede tener todos sus bits a 0 o todos sus bits a 1. Sin embargo, determinado hardware no actualizado puede ser un problema en este caso. No lo tendremos en cuenta para nuestros cálculos.

mSRbin representa en binario la máscara de subred lógica, a partir del tercer byte. mSRdec da la misma información en formato decimal.

Lo que nos da el siguiente cuadro:

NmUtil	NmPos	NmRetenidos	mSRbin	mSRdec
1	2	0	1000 0000	128
2	4	2	1100 0000	192
3	**8**	**6**	**1110 0000**	**224**
4	16	14	1111 0000	240
5	32	30	1111 1000	248
6	64	62	1111 1100	252
7	128	126	1111 1110	254
8	256	254	1111 1111	255
9	512	510	11111 1111. 1000 0000	255.128

10	1024	1022	11111 1111. 1100 0000	255.192
11	2048	2046	11111 1111. 1110 0000	255.224
12	4096	4094	11111 1111. 1111 0000	255.240
13	8192	8190	11111 1111. 1111 1000	255.248

El valor que debemos encontrar para NmBits lo encontramos en el cuadro buscando en la columna NmRetenidos el valor inmediatamente superior o igual.

En el ejemplo, para NmRL = 5, el valor correspondiente es NmRetenido = 6, y por tanto NmUtil = NmBITS = 3, que es el valor que leemos en la misma línea.

El cuadro nos indica que son necesarios 3 bits para cifrar 5 subredes lógicas.

Etapa 2: obtención de la máscara CIDR

La máscara en notación CIDR se obtiene sumando al valor inicial el número de bits encontrados.

Así, /16 + 3 pasa a ser /19.

Etapa 3: obtención de la máscara decimal

Al leer el cuadro, en la columna mSRbin y mSRdec, es fácil leer el byte en binario o en decimal que corresponde a la máscara.

En este ejemplo, la máscara retomará los 16 primeros bits del prefijo inicial, al cual se añadirá el byte mSRbin, y luego un byte a 0.

La máscara que se obtiene es 255.255.224.0.

Etapa 4: cálculo de los IDSR

Para enumerar los identificadores de subred (IDSR), basta con contar en binario de 0 a NmPos - 1.

Así, en el caso que nos ocupa, vamos a trabajar con 3 bits (NmBITS).

La enumeración nos lleva a:

Decimal	Binario en NmBITS
0	*000*
1	001
2	010
3	011
4	100
5	101
6	110
7	*111*

Etapa 5: obtención de los números de subred

El prefijo de los dos primeros bytes sigue siendo: 172.16.

El tercer byte comienza en binario por 001. Los dos últimos bytes variables en binario son: 001x xxxx.xxxx xxxx.

x representa un valor 0 o 1 asignado.

El identificador de subred lógica escrito en binario en realidad será un prefijo cifrado de 19 bits:

172	.16	.?	.0
10101100	.0001 0000	.001 x xxxx	.xxxx xxxx

Así, este tercer byte, al considerar el identificador de red secundaria lógico (todos los bits del equipo a 0), tendrá como valor:

0010 0000, o sea, 32 en decimal, y por tanto el valor 172.16.32 /19 para RL1.

Lo mismo sucede para el resto de las redes lógicas.

Para RL2:

172	.16	.?	.0
10101100	.0001 0000	.010 x xxxx	.xxxx xxx

Así obtenemos como tercer byte 0100 0000, o sea 64 en decimal y por tanto 172.16.64 /19 para RL2.

Del mismo modo:

- RL3 = 172.16.96.0/19
- RL4 = 172.16.128.0/19
- RL5 = 172.16.160.0/19
- RL6 = 172.16.192.0/19 (no solicitado en este caso)

Podemos observar que el identificador de subred lógica aumenta en 32 cada vez. Este valor se denomina **incremento**.

De hecho, esto ocurre porque, en binario, cuando se añade 0 a la derecha se multiplica por 2. Aquí añadimos 5 ceros, por lo tanto multiplicamos los valores numéricos decimales de 1 a 6 por 32 ($=2^5$= 2 x 2 x 2 x 2 x 2).

Etapa 6: expresión de los rangos de direcciones de redes secundarias

En esta última etapa, solo nos queda expresar todas las posibilidades, es decir, la lista de las direcciones IP que se asignarán a los equipos en el entorno de red.

A cada equipo se le asignará la misma máscara, cualquiera que sea la subred en cuestión, es decir /19 o 255.255.224.0 en decimal.

Finalmente, retomamos los números de red secundaria encontrados y exponemos todas las posibilidades:

- RL1 = 172.16.32.0/19

- RL2 = 172.16.64.0/19
- RL3 = 172.16.96.0/19
- RL4 = 172.16.128.0/19
- RL5 = 172.16.160.0/19

Para cada red lógica, expresaremos en binario la escritura de las direcciones del equipo. Para encontrar el valor más pequeño, todos los bits de la parte del equipo se ponen a 0. Para encontrar el valor más alto, pondremos todos los bits del equipo a 1.

Así, para RL1, tendremos:

172	.16	.32	.0
10101100	.0001 0000	.001 x xxxx	.xxxx xxxx

La dirección en que todos los bits del equipo están a 0 nos da:

10101100	.0001 0000	.001 0 0000	.0000 0000

que es el propio número de red.

Y con todos los bits a 1, obtendremos:

10101100	.0001 0000	.001 1 1111	.1111 1111

De ahí el rango de direcciones, Rango RL1: 172.16.32.0 a 172.16.63.255

Ahora debemos quitar las dos direcciones en que todos los bits del equipo son 0 y aquellas en que todos los bits son 1, que son, 172.16.32.0 (que es la de la red lógica) y 172.16.63.255 (dirección de difusión de la red lógica).

De igual modo, se deduce:

- Rango RL2: 172.16.64.1 a 172.16.95.254.
- Rango RL3: 172.16.96.1 a 172.16.127.254.
- Rango RL4: 172.16.128.1 a 172.16.159.254.
- Rango RL5: 172.16.160.1 a 172.16.191.254.

A continuación asignaremos todas estas direcciones IP con la máscara calculada, es decir /19 o 255.255.224.0.

e. Factorización de las tablas de enrutamiento

En cuanto hemos definido una asignación de direcciones de subred, podemos seguir la operación a partir del resultado anteriormente obtenido. Así pues, podríamos asignar el rango de subred RL4 para servir de punto de partida a un nuevo plan de asignación de direcciones basándose, por ejemplo, en 172.16.128.0/19 y así sucesivamente... Por ello es fácil comprender que se asignen algunos prefijos IP para Europa, que un país como España pueda necesitar una asignación mucho más grande y que a Barcelona, por ejemplo, se le asigne un rango del tipo 60.189.235.56/29.

La máscara también puede variar de una tabla de transporte a otra para finalmente ser cada vez más precisa.

Esto solo es posible si las direcciones IP se han asignado de manera óptima y los routers están conectados jerárquicamente.

Esto es lo que llamaremos *Variable Length Scalable Mask* (VLSM) o máscara de subred de longitud variable.

De acuerdo con esta atribución inteligente de las direcciones, puede ser fácil conocer con precisión, en función de un prefijo dado, el origen geográfico del destinatario y, en consecuencia, construir tablas de enrutamiento simplificadas.

Imaginemos, por ejemplo, el caso de una tabla de enrutamiento con la siguiente información:

Red	Máscara	Interfaz	Puerta de enlace
193.19.32.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.33.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.34.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.35.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.36.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.37.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.38.0	255.255.255.0	197.2.1.254	197.2.1.253
193.19.39.0	255.255.255.0	197.2.1.254	197.2.1.253

¿Qué ruta podría sustituir a las rutas existentes?

En este caso, basta con comprobar que la interfaz y la puerta de enlace son idénticas y que el conjunto de las rutas puede descomponerse en factores. En el ejemplo, el prefijo común a todas las redes es 193.19.32 para una máscara de 21 bits.

Decimal	Escritura binaria del tercer byte
193.19.**32**.0	**0010 0**000
193.19.**33**.0	**0010 0**001
193.19.**34**.0	**0010 0**010
193.19.**35**.0	**0010 0**011
193.19.**36**.0	**0010 0**100
193.19.**37**.0	**0010 0**101
193.19.**38**.0	**0010 0**110
193.19.**39**.0	**0010 0**111

Así, queda claro que solo varían los 3 bits importantes del tercer byte.

La ruta equivalente que sustituirá a los 8 restantes será en este caso:

193.19.32.0	255.255.248.0	197.2.1.254	197.2.1.253