REDES

Por Cayetano Borja Carrillo

Índice:

Ejercicio 1 – Clase y máscara de subred

Dadas las siguientes direcciones IPv4, calcula la clase a la que pertenecen y la máscara de red predeterminada que le corresponde a cada una.

a) 23.4.5.6

b) 128.3.45.6

c) 193.56.7.0

d) 122.3.41.6

e) 126.23.52.1

f) 221.56.3.6

g) 01111111.11110000.01100111.01111101

h) 10101111.11000000.11110000.00011101

i) 11100111.11110011.10000111.11011101

Solución

a) 23.4.5.6 → El primer octeto (23) está entre 0 y 127 (en binario empieza por 0) → Clase A y máscara 255.0.0.0

b) 128.3.45.6 → El primer octeto (128) está entre 128 y 192 (en binario empieza por 10) → Clase B y máscara 255.255.0.0

c) 193.56.7.0 → El primer octeto (193) está entre 192 y 223 (en binario empieza por 110) → Clase C y máscara 255.255.255.0

d) 122.3.41.6 → 122 está entre 0 y 127 → Clase A y máscara 255.0.0.0

e) 126.23.52.1 → 126 está entre 0 y 127 → Clase A y máscara 255.0.0.0

f) 221.56.3.6 → 221 está entre 192 y 223 → Clase C y máscara 255.255.255.0

g) 01111111.11110000.01100111.01111101 → Empieza por 0 → Clase A y máscara 255.0.0.0

h) 10101111.11000000.11110000.00011101 → Empieza por 10 → Clase B y máscara 255.255.0.0

i) 11100111.11110011.10000111.11011101 → Empieza por 1110 → Clase D y máscara 255.255.255.128

Ejercicio 2 – IP válidas

Dadas las siguientes direcciones IPv4, indica cuáles son direcciones válidas. Válida significa que se puede asignar a un servidor, impresora, router, etc.

a) 0.234.24.12

b) 150.100.255.255

c) 175.100.255.18

d) 195.234.253.0

e) 100.0.0.23

f) 188.258.221.176

g) 127.34.25.189

h) 224.254.217.73

Consideraciones previas

Hay que tener en cuenta que las IP que son válidas son las siguientes:

- Clase A → Rango 1.0.0.0 – 127.0.0.0 → Máscara predeterminada 255.0.0.0
- Clase B → Rango 128.0.0.0 – 191.255.0.0 → Máscara predeterm. 255.255.0.0
- Clase C → Rango 192.0.0.0 – 223.255.255.0 → Máscara predeter. 255.255.255.0

Cualquier IP que se salga de ese rango no es válida, aunque hay que tener en cuenta que algunas que están dentro de ese rango están reservadas y tampoco pueden usarse. Algunas direcciones IP especiales son las siguientes:

- Rango 0.0.0.0/8 (0.0.0.0 – 0.255.255.255) → Indican la red actual, sólo son válidas como dirección origen.
- Rango 127.0.0.0/8 (127.0.0.0 - 127.255.255.255) → Reservadas para direcciones *loopback*, que son direcciones especiales que los *hosts* utilizan para dirigir el tráfico hacia ellos mismos. Aunque normalmente se utilice solo la IP 127.0.0.1, se reserva todo el rango.
- Rango 224.0.0.0/4 (224.0.0.0 – 239.255.255.255) → Reservadas para asignar a grupos de multidifusión o *multicast*. De esta forma, se pueden enviar datos al conjunto de *hosts* que pertenecen a un grupo.
- Rango 240.0.0.0/4 (240.0.0.0 – 255.255.255.254) → Reservadas para usos futuros. No se pueden asignar.
- Rango 255.255.255.255/32 (255.255.255.255) → Dirección de *broadcast* o difusión. Se usa para enviar datos a todos los *hosts* de la red.
- Rangos 10.0.0.0/8 (10.0.0.0 – 10.255.255.255), 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) y 192.168.0.0/16 (192.168.0.0 – 192.168.255.255) → Son direcciones IP privadas. Una IP privada es una dirección que se utiliza únicamente dentro de una red interna (red local). Si un *host* de una red privada se quiere comunicar con el exterior, le manda el mensaje al *router* y éste realizará la petición al exterior con la dirección IP pública que el ISP ha proporcionado.

- Rango 192.0.2.0/24 (192.0.2.0 - 192.0.2.255): Reservadas para documentación. Este rango pertenece al grupo de IP privadas y no se pueden asignar.
- Rango 169.254.0.0/16 (169.254.0.0 – 169.254.255.255) → Direcciones de enlace local o *link-local*. Solo sirven para trabajar dentro de una red local (no se puede enrutar). Las asigna el sistema operativo por medio de APIPA cuando un servidor DHCP no puede asignarle una IP al *host* de forma dinámica. Este rango pertenece al grupo de IP privadas.

Solución

a) 0.234.24.12

Las IP del rango 0.0.0.0/8 sirven para indicar la red actual, así que **no es válida**.

b) 150.100.255.255

Al acabar en 255 es muy probable que sea una dirección de *broadcast*, pero no tiene por qué, habría que comprobarlo mirando su máscara de red.

El primer octeto (150) indica que es de clase B (127 – 192) y las direcciones de clase B usan una máscara de subred predeterminada de 255.255.0.0. Como los 16 últimos bits de la máscara están a cero, las direcciones de la red son las que van de la 150.100.0.0 a la 150.100.255.255. Como se puede ver, la IP del apartado es la última de esa red, por lo que se trata de una dirección de *broadcast* y **no son válidas** para asignar a *hosts*.

c) 175.100.255.18

Está dentro del rango de direcciones IP válidas y no tiene pinta de ser una dirección de *broadcast* ni de red, por lo tanto, **sí es una dirección válida**.

d) 195.234.253.0

Al acabar en 0 es muy probable que sea una dirección de red, pero no tiene por qué, habría que mirar su máscara de red.

El primer octeto (195) indica que es de clase C y las direcciones de clase C tienen una máscara predeterminada de 255.255.255.0. La IP del apartado es la primera de esa red, por lo que se trata de una dirección de red y **no es válida** para asignar a *hosts*.

e) 100.0.0.23

Está dentro del rango de direcciones IP válidas y no tiene pinta de ser una dirección de *broadcast* ni de red, por lo tanto, **sí es una dirección válida**.

f) 188.258.221.176

El segundo octeto tiene un valor mayor de 255 y eso es imposible porque cada octeto puede almacenar hasta 2^8=256 direcciones (de la 0 a la 255), así que **no es válida**.

g) 127.34.25.189

El rango 127.0.0.0/8 está reservado para direcciones *loopback*, por lo que **no es válida**.

h) 224.254.217.73

El rango 224.0.0.0/4 se usa para *multicast*, por lo que **no es válida** para *hosts*.

Ejercicio 3 – Direccionamiento

Dadas las siguientes direcciones IPv4, calcula la dirección de red, del primer *host*, del último *host*, del *broadcast* (difusión) y cantidad de *hosts* por red.

a) 125.34.12.56 / 16

b) 120.14.122.16 / 17

c) 140.11.36.22 / 19

d) 141.181.214.16 / 19

e) 200.34.22.156 / 28

Solución

a) 125.34.12.56 / 16

El /16 es la máscara de red expresado en notación diagonal o compacta y quiere decir que los primeros 16 bits de la máscara son "1" y el resto "0". La máscara expresada como octetos punteados es la siguiente:

Máscara = 11111111.11111111.00000000.00000000 → 255.255.0.0

Id de red | Hosts

Los bits que están a 1 indican qué bits de una dirección IP identifican la red y los que están a 0 se usan para identificar a los *hosts* o para hacer *subnetting*.

Obtener la dirección de red

Para calcular la dirección de red a la que pertenece el *host* 125.34.12.56, se puede de hacer de 2 formas equivalentes:

La primera forma consiste en pasar la dirección IP del *host* a binario, dejar los primeros 16 bits como están y el resto ponerlos a 0. Ejemplo:

Dirección IP → 125.34.12.56 → 01111101.00100010.00001100.00111000

Igual | Cero

Dirección de red → 01111101.00100010.00000000.00000000 → 125.34.0.0

La segunda forma consiste en hacer una operación AND de cada bit de la dirección IP con el correspondiente bit de la máscara de red. La operación AND devuelve 1 si los 2 bits que se comparan son 1 y 0 en el resto de los casos.

Dirección IP → 01111101.00100010.00001100.00111000
Máscara de red → 11111111.11111111.00000000.00000000

Dirección de red → 01111101.00100010.00000000.00000000 → 125.34.0.0

Obtener la cantidad de *hosts* que se pueden asignar

Para calcular los *hosts* que se pueden configurar en la red, se miran los bits de la máscara que están a 0. En este caso están a 0 los 16 últimos bits, por lo que caben 2^{16}-2 = 65534 *hosts* (se restan 2 porque la primera dirección se usa para identificar la red y la última es la de *broadcast*).

Obtener la dirección de *broadcast*

La dirección de *broadcast* es la última dirección de cualquier red y se obtiene poniendo a 1 los bits que se reservan para los *hosts*.

Broadcast → 01111101.00100010.11111111.11111111 = 125.34.255.255
Id de Red Hosts

Obtener la dirección del primer y último *host*

La dirección del primer *host* es la siguiente de la dirección de red → 125.34.0.1

La dirección del último *host* es la anterior de la de *broadcast* → 125.34.255.254

En la siguiente tabla se muestran los datos que se nos piden:

Dirección de red	Primer host	Último host	Broadcast	Cantidad
125.34.0.0	125.34.0.1	125.34.255.254	125.34.255.255	65534

b) 120.14.122.16 / 17

Los primeros 17 bits de esa dirección identifican la dirección de red, por tanto:

Dirección IP → 120.14.122.17 → 01111000.00001110.01111010.00010001
Red Hosts

Dirección de red → 01111000.00001110.00000000.00000000 → 120.14.0.0/17
IP primer host → 01111000.00001110.00000000.00000001 → 120.14.0.1
IP último host → 01111000.00001110.01111111.11111110 → 120.14.255.254
IP broadcast → 01111000.00001110.01111111.11111111 → 120.14.255.255
Cantidad de *hosts* = 2^{15}-2 = 32768 – 2 = 32766

c) 140.11.36.22 / 19

Los primeros 19 bits de esa dirección identifican la dirección de red, así que:

Dirección IP → 140.11.36.22 → 10001100.00001011.00100100.00010110
Red Hosts

Dirección de red → 10001100.00001011.00100000.00000000 → 140.11.32.0/19
IP primer host → 10001100.00001011.00100000.00000001 → 140.11.32.1
IP último host → 10001100.00001011.00111111.11111110 → 140.11.63.254
IP broadcast → 10001100.00001011.00111111.11111111 → 140.11.63.255
Cantidad de *hosts* = 2^{13}-2 = 8192 – 2 = 8190

d) 141.181.214.16 / 19

Los primeros 19 bits de esa dirección identifican la dirección de red, así que:

Dirección IP → 141.181.214.16 → 10001101.10110101.11010110.0010000
Red Hosts

Dirección de red → 10001101.10110101.11000000.00000000 → 141.181.192.0/19
IP primer host → 10001101.10110101.11000000.00000001 → 141.181.192.1
IP último host → 10001101.10110101.11011111.11111110 → 141.181.223.254
IP broadcast → 10001101.10110101.11011111.11111111 → 141.181.223.255
Cantidad de *hosts* = 2^{13}-2 = 8192 – 2 = 8190

e) 200.34.22.156 / 28

Los primeros 28 bits de esa dirección identifican la dirección de red, así que:

Dirección IP → 200.34.22.156 → 11001000.00100010.00010110.10011100
Red Hosts

Dirección de red → 11001000.00100010.00010110.10010000 → 200.34.22.144/28
IP primer host → 11001000.00100010.00010110.10010001 → 200.34.22.145
IP último host → 11001000.00100010.00010110.10011110 → 200.34.22.158
IP broadcast → 11001000.00100010.00010110.10011111 → 200.34.22.159
Cantidad de *hosts* = 2^{4}-2 = 16 – 2 = 14

Ejercicio 4 – Subredes

Dada la dirección IP 192.168.1.0 con máscara de subred de tamaño fijo 255.255.255.0, realiza los siguientes apartados:

a) Dividir la red en 2 subredes del mismo tamaño e indicar la máscara y la dirección IP de cada subred.

b) Dividir la red en 4 subredes del mismo tamaño e indicar la máscara y la dirección IP de cada subred.

c) Dividir la cuarta subred del apartado b) en 2 subredes del mismo tamaño e indicar la máscara, la dirección IP de cada subred y las direcciones válidas en cada subred.

Solución

a) Dividir la red en 2 subredes del mismo tamaño e indicar la máscara y la dirección IP de cada subred.

Mirando la máscara sabemos que los 3 primeros octetos (24 bits) sirven para identificar la red y el último (8 bits) para asignar a los *hosts* o hacer *subnetting*. Para dividir la red en 2 necesitamos 1 bit ya que $2=2^1$, por tanto, de los 8 bits disponibles, usaremos 1 para identificar cada subred y los otros 7 para los *hosts*, quedando:

Máscara → 11111111.11111111.11111111.10000000 → 255.255.255.128

Red Subred Hosts

IP subred 1 → 11000000.10101000.00000001.00000000 → 192.168.1.0/25
IP subred 2 → 11000000.10101000.00000001.10000000 → 192.168.1.128/25

b) Dividir la red en 4 subredes del mismo tamaño e indicar la máscara y la dirección IP de cada subred.

Para crear 4 redes necesitamos 2 bit ya que $4=2^2$ y quedan 6 para los *hosts*:

Máscara → 11111111.11111111.11111111.11000000 → 255.255.255.192

Red Subred Hosts

IP subred 1 → 11000000.10101000.00000001.00000000 → 192.168.1.0/26
IP subred 2 → 11000000.10101000.00000001.01000000 → 192.168.1.64/26
IP subred 3 → 11000000.10101000.00000001.10000000 → 192.168.1.128/26
IP subred 4 → 11000000.10101000.00000001.11000000 → 192.168.1.192/26

c) Dividir la cuarta subred del apartado b) en 2 subredes del mismo tamaño e indicar la máscara, la dirección IP de cada subred y las direcciones válidas en cada subred.

Para dividir la subred 4 en 2 subredes más, tomamos 1 bit de los que quedan disponibles, quedando:

Máscara → 11111111.11111111.11111111.11100000 → 255.255.255.224

Red Subred Hosts

IP subred 4.1 → 11000000.10101000.00000001.11000000 → 192.168.1.192/27
IP subred 4.2 → 11000000.10101000.00000001.11100000 → 192.168.1.224/27
Cantidad de direcciones disponibles en cada subred → 2^5-2 = 32 – 2 = 30

Ejercicio 5 – Subredes 2

A partir de la dirección IP 172.30.1.33 con máscara 255.255.255.0, calcular:

- Cantidad de bits de subred.
- Cantidad de subredes que se pueden crear.

- Cantidad de bits de *host* por subred.
- Cantidad de *hosts* disponibles por subred.
- Dirección IP de la subred.
- Dirección IP del primer *host* en esta subred.
- Dirección IP del último *host* en esta subred.
- Dirección de *broadcast* para esta subred.

Solución

Obtener la cantidad de bits de subred

El primer octeto de la IP es 172 y como está entre 128 y 192 (en binario empieza por 10), se observa que es una dirección de clase B, por lo que le correspondería una máscara de subred /16 o 255.255.0.0. Como la máscara adaptada es 255.255.255.0, el tercer octeto (**8 bits**) se utiliza para definir las subredes.

Obtener la cantidad de subredes que se pueden crear

Para calcular la cantidad de subredes que se pueden crear, se eleva 2 a la cantidad de bits destinados para las subredes: 2^8 = **256 subredes**.

Obtener la cantidad de bits de *host* por subred

La cantidad de 0 que tiene la máscara indica las direcciones que hay disponibles para ser usadas. Lo pasamos a binario:

Máscara = 255.255.255.0 → 11111111.11111111.11111111.00000000

Red Subred *Hosts*

Como se puede observar, **8 bits** por cada subred son para *hosts*.

Obtener la cantidad de *hosts* disponibles por subred

Como se utilizan 8 bits para los *hosts*, existen 2^8-2 = **254 direcciones** disponibles para asignar a *hosts* en cada subred.

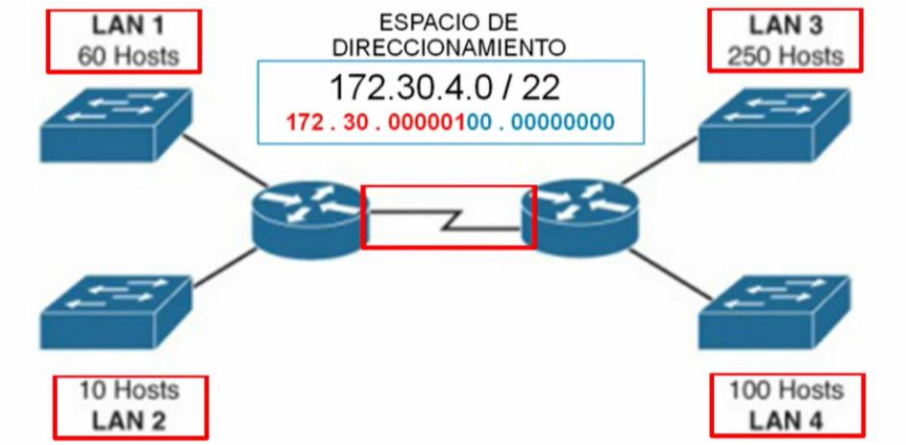
Obtener la dirección IP de la subred, del primer y último *host* y del *broadcast*

Los primeros 3 octetos de 172.30.1.33 identifican la dirección de red, por tanto:

Dirección de subred → 172.30.1.0
IP del primer host → 172.30.1.1
IP del último host → 172.30.1.254
IP de broadcast → 172.30.1.255

Ejercicio 6 – Máscara de subred variable (VLSM)

Dada la dirección IP 172.30.4.0/22 y la siguiente topología, crea las subredes necesarias utilizando VLSM e indica la dirección IP, máscara de subred, IP de broadcast y el rango de IP válidas de cada una.



Consideraciones previas

Cuando una red que usa una máscara de red de tamaño fijo se divide en varias subredes, todas las subredes deben tener sí o sí el mismo tamaño. Si observamos la topología de este ejercicio, la subred más grande necesita 250 *hosts*, por lo que todas las subredes deben tener el mismo tamaño de 256 direcciones y eso produce 2 problemas:

1. Que la LAN2 solo necesita 10 equipos y se desperdiciarán 244 direcciones.
2. Que como se usan subredes de 256 direcciones, cada subred necesita 8 bits para identificar los *hosts* (2^8=256). Si 22 bits se usan para identificar la red, tan solo disponemos de 2 bits para realizar el *subnetting*. Eso nos permite crear un máximo de 4 subredes y se necesitan 5 (LAN1, LAN2, LAN3, LAN4 y WAN)

Para solucionar este problema, se utiliza la máscara de subred variable o VLSM (*Variable Length Subnet Mask*) que consiste en crear subredes lo más pequeñas posibles, siempre que sea múltiplo de 2. Ejemplos:

- Se necesitan 90 *hosts* → 2^7-2=126≥90 → Subred de 7 bits para *hosts*
- Se necesitan 10 *hosts* → 2^4-2=14≥10 → Subred de 4 bits para *hosts*
- Se necesitan 200 *hosts* → 2^8-2=254≥200 → Subred de 8 bits para *hosts*

Solución

Primero tenemos que identificar con cuántas redes vamos a trabajar y, después, las ordenamos en sentido decreciente empezando por la subred que necesita un mayor número de direcciones. En este caso necesitamos 5 subredes (4 LAN y 1 WAN) y el orden es LAN3, LAN4, LAN1, LAN2 y WAN.

LAN3 → 250 hosts

Necesitamos 8 bits para los *hosts* ya que 2^8-2=254≥250. Hay que tener en cuenta que, aunque con 9 bits también se podría hacer, siempre tenemos que elegir el menor número de bits posible para que el desperdicio de direcciones sea el mínimo.

Como vamos a usar 8 bits para *hosts*, nos quedan 2 bits para el *subnetting*, siendo la máscara de subred /24 (32–8=24) y de ahí obtenemos las siguientes posibles subredes (el tercer octeto está en binario, el resto en decimal):

Subred 0 → 172.30.00000100.0 → 172.30.4.0/24 → **Se usará esta para la LAN3**
Subred 1 → 172.30.00000101.0→ 172.30.5.0/24
Subred 2 → 172.30.00000110.0→ 172.30.6.0/24
Subred 3 → 172.30.00000111.0→ 172.30.7.0/24

Por tanto, la LAN3 se nos quedaría de la siguiente forma:

Dirección de subred → 172.30.00000100.00000000 → 172.30.4.0/24
Dirección de *broadcast* → 172.30.00000100.11111111 → 172.30.4.255
Rango de IP válidas → 172.30.4.1 – 172.30.4.254

LAN4 → 100 hosts

Podríamos asignarle una de las subredes que nos quedaron disponibles en el apartado anterior, sin embargo, se desperdiciarían muchas direcciones. Lo que vamos a hacer es dividir una de esas subredes en otras subredes más pequeñas y utilizar una de estas sub-subredes.

Necesitamos 7 bits para los *hosts* ya que 2^7-2=126≥100, por lo que la máscara será /25 (32-7=25). Con eso, podemos dividir la subred 1 en 2, quedando:

Subred 1: 172.30.00000101.0→ 172.30.5.0/24
Subred 1-0: 172.30.00000101.00000000 → 172.30.5.0/25 → **Esta para LAN2**
Subred 1-1: 172.30.00000101.10000000 → 172.30.5.128/25

Por tanto, la LAN2 se nos quedaría de la siguiente forma:

Dirección de subred → 172.30.00000101.00000000 → 172.30.5.0/25
Dirección de *broadcast* → 172.30.00000101.01111111 → 172.30.5.127
Rango de IP válidas → 172.30.5.1 – 172.30.5.126

LAN1 → 60 hosts

De todas las subredes que tenemos disponibles, tomamos la más pequeña (Subred 1-1) y vemos que, como para para almacenar 60 hosts necesitamos 6 bits (2^6-2=62≥60), podemos dividirla en 2.

Subred 1-1: 172.30.00000101.10000000 → 172.30.5.128/25
Subred 1-1-0: 172.30.00000101.10000000 → 172.30.5.128/26 → **LAN1**
Subred 1-1-1: 172.30.00000101.11000000 → 172.30.5.192/26

Por tanto, la LAN1 se nos quedaría de la siguiente forma:

Dirección de subred → 172.30.00000101.10000000 → 172.30.5.128/26
Dirección de *broadcast* → 172.30.00000101.10111111 → 172.30.5.191
Rango de IP válidas → 172.30.5.129 – 172.30.5.190

LAN2 → 10 hosts

De todas las subredes que tenemos disponibles, tomamos la más pequeña (Subred 1-1-1) y vemos que, como para para almacenar 10 hosts necesitamos 4 bits (2^4-2=14≥10), podemos dividirla en 4.

Subred 1-1-1: 172.30.00000101.11000000 → 172.30.5.192/26
- Subred 1-1-1-0: 172.30.00000101.11000000 → 172.30.5.192/28 → **LAN2**
- Subred 1-1-1-1: 172.30.00000101.11010000 → 172.30.5.208/28
- Subred 1-1-1-2: 172.30.00000101.11100000 → 172.30.5.224/28
- Subred 1-1-1-3: 172.30.00000101.11110000 → 172.30.5.240/28

Por tanto, la LAN2 se nos quedaría de la siguiente forma:

Dirección de subred → 172.30.00000101.10000000 → 172.30.5.192/28
Dirección de *broadcast* → 172.30.00000101.10001111 → 172.30.5.207
Rango de IP válidas → 172.30.5.193 – 172.30.5.206

WAN → 2 hosts

De todas las subredes que tenemos disponibles, tomamos la más pequeña (Subred 1-1-1-1) y vemos que, como para para almacenar 2 hosts necesitamos 2 bits (2^2-2≥2), podemos dividirla en 4.

Subred 1-1-1-1: 172.30.00000101.11010000 → 172.30.5.208/28
- Subred 1-1-1-1-0: 172.30.00000101.11010000 → 172.30.5.208/30 → **WAN**
- Subred 1-1-1-1-1: 172.30.00000101.11010100 → 172.30.5.212/30
- Subred 1-1-1-1-2: 172.30.00000101.11011000 → 172.30.5.216/30
- Subred 1-1-1-1-3: 172.30.00000101.11011100 → 172.30.5.220/30

Por tanto, la WAN se nos quedaría de la siguiente forma:

Dirección de subred → 172.30.00000101.11010000 → 172.30.5.208/30
Dirección de *broadcast* → 172.30.00000101.10000011 → 172.30.5.211
Rango de IP válidas → 172.30.5.209 – 172.30.5.210

A continuación, se muestra un esquema con las subredes ocupadas y libres.

172.30.4.0 → **LAN3**

172.30.5.0 → 172.30.5.00000000 → **LAN2**

172.30.6.0 172.30.5.10000000 → 172.30.5.10000000 → **LAN1**

172.30.7.0 172.30.5.11000000 → 172.30.5.11000000 → **LAN2**

172.30.5.11010000 → 172.30.5.11010000 → **WAN**

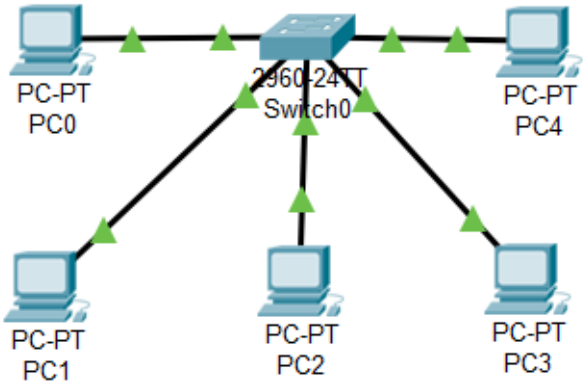
172.30.5.11100000 172.30.5.11010100

172.30.5.11110000 172.30.5.11011000

172.30.5.11011100

Ejercicio 7 – Tablas MAC y ARP

Dada la siguiente topología y tabla con direcciones IP y MAC:



Host	Dirección IP	Dirección física (MAC)
PC0	192.168.0.10	00:60:52:0B:B7:7D
PC1	192.168.0.11	00:E0:4C:AB:9A:FF
PC2	192.168.0.12	00:E0:4C:33:79:AF
PC3	192.168.0.13	B2:42:52:12:37:BE
PC4	192.168.0.14	A3:BB:08:10:DA:DB

Determina como quedarían las tablas ARP de cada *host* y la tabla de direcciones MAC del *switch* tras ejecutarse las siguientes operaciones y suponiendo que inicialmente las tablas están vacías:

- PC0 envía un mensaje a PC3
- PC3 envía un mensaje a PC4
- PC4 envía un mensaje a PC0
- PC4 envía un mensaje a PC1
- PC0 envía un mensaje a PC1

Solución

PC0 envía un mensaje a PC3

Como PC0 no conoce la MAC de PC3, no puede formar una trama y enviársela, así que crea un mensaje "ARP *request*" y lo envía a difusión (a todos los equipos de la red) preguntando cuál es la dirección MAC del equipo con IP 192.168.0.13.

MAC Origen	MAC Destino	Mensaje	IP Origen	IP Destino
00:60:52:0B:B7:7D	FF:FF:FF:FF:FF:FF	Solicitud ARP	192.168.0.10	192.168.0.13

Estructura del mensaje ARP *request*

El *switch* recibe el mensaje de PC0 y almacena en su tabla MAC un registro diciendo que en el primer puerto (o boca) está conectado el *host* con MAC 00:60:52:0B:B7:7D. El *switch* envía el mensaje ARP por todos sus puertos menos por el primero, ya que por ahí es por donde lo ha recibido.

El mensaje ARP llega a PC1, PC2, PC3 y PC4 y todos excepto PC3 lo desechan ya que no van dirigidos a ellos. PC3 almacena en su tabla ARP un registro indicando que la IP 192.168.0.10 corresponde con la MAC 00:60:52:0B:B7:7D. Finalmente, PC3 forma un mensaje "ARP *reply*" diciendo que la MAC del *host* con la IP solicitada es B2:42:52:12:37:BE.

MAC Origen	MAC Destino	Mensaje	IP Origen	IP Destino
B2:42:52:12:37:BE	00:60:52:0B:B7:7D	Respuesta ARP	192.168.0.13	192.168.0.10

Estructura del mensaje ARP *reply*

El *switch* recibe el mensaje de PC3 y almacena en su tabla MAC un registro diciendo que en el tercer puerto está conectado el *host* con MAC 00:E0:4C:33:79:AF. El *switch* envía el ARP por el puerto 1 y lo recibe PC0.

PC0 almacena en su tabla ARP un registro indicando que la IP 192.168.0.13 corresponde con la MAC B2:42:52:12:37:BE.

Ahora PC0 sí puede comunicarse y enviar datos a PC3.

PC3 envía un mensaje a PC4

El proceso es el mismo, por lo que no se van a dar tantos detalles. PC3 envía un "ARP *request"* a difusión preguntando por la MAC del equipo con IP 192.168.0.14, el *switch* lo reenvía a todos menos a PC3 y, finalmente, PC4 le responde. En este momento, cada nodo conoce a:

- PC0 → PC3
- PC1 →
- PC2 →
- PC3 → PC0, PC4
- PC4 → PC3
- Switch → PC0, PC3, PC4

PC4 envía un mensaje a PC0

PC4 envía un "ARP *request"* a difusión preguntando por la MAC del equipo con IP 192.168.0.10, el *switch* lo reenvía a todos menos a PC4 y, finalmente, PC0 le responde. En este momento, cada nodo conoce a:

- PC0 → PC3, PC4
- PC1 →
- PC2 →
- PC3 → PC0, PC4
- PC4 → PC0, PC3
- Switch → PC0, PC3, PC4

PC4 envía un mensaje a PC1

PC4 envía un "ARP *request"* a difusión preguntando por la MAC del equipo con IP 192.168.0.11, el *switch* lo reenvía a todos menos a PC4 y, finalmente, PC0 le responde. En este momento, cada nodo conoce a:

- PC0 → PC3, PC4
- PC1 → PC4
- PC2 →
- PC3 → PC0, PC4
- PC4 → PC0, PC1, PC3
- Switch → PC0, PC1, PC3, PC4

PC0 envía un mensaje a PC1

PC0 envía un "ARP *request*" a difusión preguntando por la MAC del equipo con IP 192.168.0.11, el *switch* lo reenvía a todos menos a PC0 y, finalmente, PC1 le responde. En este momento, cada nodo conoce a:

- PC0 → PC1, PC3, PC4
- PC1 → PC0, PC4
- PC2 →
- PC3 → PC0, PC4
- PC4 → PC0, PC1, PC3
- Switch → PC0, PC1, PC3, PC4

Las tablas ARP quedarían de la siguiente manera:

PC0

Dirección IP	Dirección MAC
192.168.0.11	00:E0:4C:AB:9A:FF
192.168.0.13	B2:42:52:12:37:BE
192.168.0.14	A3:BB:08:10:DA:DB

PC1

Dirección IP	Dirección MAC
192.168.0.10	00:60:52:0B:B7:7D
192.168.0.14	A3:BB:08:10:DA:DB

PC3

Dirección IP	Dirección MAC
192.168.0.10	00:60:52:0B:B7:7D
192.168.0.14	A3:BB:08:10:DA:DB

PC4

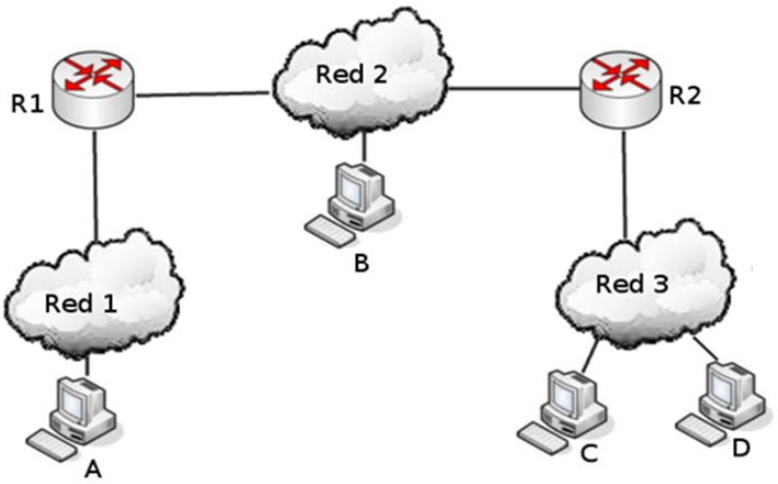
Dirección IP	Dirección MAC
192.168.0.10	00:60:52:0B:B7:7D
192.168.0.11	00:E0:4C:AB:9A:FF
192.168.0.13	B2:42:52:12:37:BE

Y la tabla de direcciones MAC del *switch* quedaría de la siguiente forma:

Dirección MAC	Puerto
00:60:52:0B:B7:7D	Fa0 (FastEthernet 0)
00:E0:4C:AB:9A:FF	Fa1 (FastEthernet 1)
B2:42:52:12:37:BE	Fa3 (FastEthernet 3)
A3:BB:08:10:DA:DB	Fa4 (FastEthernet 4)

Ejercicio 8 – ¿Cómo viajan?

Dada la siguiente topología y tabla con direcciones IP y MAC:



Nodo	Red	Dirección IP	Dirección física (MAC)
A	Red 1	192.168.0.10	00-60-52-0B-B7-7D
R1		192.168.0.1	00-E0-4C-AB-9A-FF
	Red 2	10.10.0.1	A3-BB-05-17-29-D0
B		10.10.0.7	00-E0-4C-33-79-AF
R2		10.10.0.2	B2-42-52-12-37-BE
	Red 3	200.3.107.1	00-E0-89-AB-12-92
C		200.3.107.73	A3-BB-08-10-DA-DB
D		200.3.107.200	B2-AB-31-07-12-93

Explica cómo sería el viaje de un paquete del host "D" hasta el host "A" sin tener en cuenta el protocolo ARP involucrando las capas 1, 2 y 3 del modelo OSI.

Solución

El *host* "D" quiere enviar un mensaje al *host* "A". "D" encapsula los datos del mensaje capa a capa hasta llegar a la capa 3 (capa de red). En esta capa le añade la IP destino que será la IP de "A" (192.168.0.10) y también le añade la IP origen que será la suya (200.3.107.200), formando un **paquete**.

"D" sigue encapsulando el mensaje y ahora llega a la capa 2 (capa de enlace de datos). En esta capa le añade la MAC origen que será la suya (B2-AB-31-07-12-93) y también le añade la MAC destino que es la MAC de "R2" (00-E0-89-AB-12-92), formando una **trama**.

La razón de que la MAC destino sea la MAC de "R2" y no la de "A" es porque "A" y "D" pertenecen a distintos dominios de difusión y la capa 2 realiza la comunicación por medio de tramas que no se pueden enrutar, por lo que la MAC destino será la del último dispositivo que hay en ese dominio de difusión (R2).

Finalmente, "D" coge la trama y la transforma en impulsos eléctricos, ondas electromagnéticas, fotones de luz o lo que emplee el medio y lo envía por el puerto correspondiente (capa 1) a "R2" a través de un canal de comunicaciones (cable de fibra óptica, cable de par trenzado, cable coaxial, Wi-Fi, etc.).

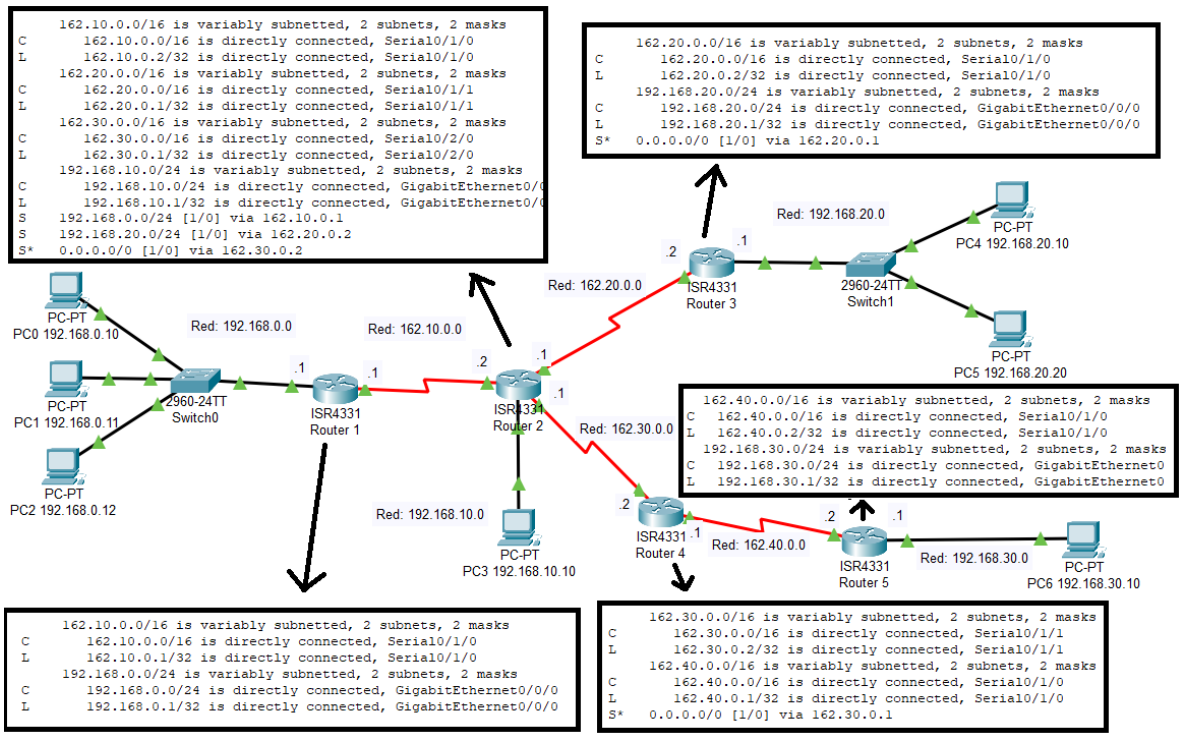
"R2" recibe las ondas, los impulsos eléctricos, los pulsos de luz, etc. y forma una trama. "R2" lee la MAC destino y ve que él es el destinatario, así que sigue desencapsulando hasta formar un paquete. Lee la IP destino del paquete y ve que el paquete no va dirigido a él ya que la IP que hay (192.168.0.10) no es la suya, así que encapsula el paquete en una **nueva trama** cuya MAC origen será la suya, pero la de la boca que da a la red 2 (B2-42-52-12-37-BE) y MAC destino la de "R1" (A3-BB-05-17-29-D0)

"R2" le envía la trama a "R1". "R1" la recibe y comprueba que la MAC origen corresponde con la suya, por lo que sigue desencapsulando hasta formar un paquete. Lee la IP destino del paquete y ve que no es la suya, así que encapsula el paquete en una nueva trama cuya MAC origen será 00-E0-4C-AB-9A-FF y MAC destino 00-60-52-0B-B7-7D.

"R1" le envía la trama a "A" y éste comprueba que la MAC origen corresponde con la suya, así que sigue desencapsulando hasta formar un paquete. Lee la IP destino y ve que también corresponde con su IP, así que sigue desencapsulando capa a capa hasta leer el contenido.

Ejercicio 9 – Tablas de enrutamiento

Dada la siguiente topología y tablas de enrutamiento. Contesta a las preguntas.



a) PC0 envía un paquete a PC3 ¿llegará?

b) Al router 1 se le añade la puerta de enlace 162.10.0.2 como ruta predeterminada. PC0 envía un paquete a PC4, ¿llegará ahora?

c) El router 1 sigue teniendo como ruta predeterminada la dirección anterior. PC0 envía un paquete a PC6, ¿llegará?

Solución

a) PC0 envía un paquete a PC3 ¿llegará?

El paquete tiene como origen la IP 192.168.0.10 y como destino la IP 192.168.10.10. El paquete sale de PC0 y llega al router 1, que comprueba en su tabla de enrutamiento si conoce algún camino que llegue a la red 192.168.10.0, pero no lo conoce y tampoco tiene configurada una ruta predeterminada, así que el paquete **no llega** a su destino.

b) Al router se le añade la puerta de enlace 162.10.0.2 como ruta predeterminada. PC0 envía un paquete a PC4, ¿llegará ahora?

El paquete tiene como origen la IP 192.168.0.10 y como destino la IP 192.168.10.10. El paquete sale de PC0 y llega al router 1, que comprueba en su tabla de enrutamiento si conoce algún camino que llegue a la red 192.168.20.0, pero no lo conoce, así que envía el paquete a la puerta de enlace 162.10.0.2 (ruta predeterminada) y llega al router 2.

El router 2 comprueba en su tabla *routing* si conoce algún camino a la red 192.168.20.0 y sí conoce una ruta, que es enviándola al dispositivo con IP 162.20.0.2 (router 3).

El paquete llega al router 3 y éste comprueba en su tabla de enrutamiento si conoce una ruta que llegue a la red 192.168.20.0 y sí conoce una, es más, está directamente conectada, por lo que el paquete **sí llega** a PC4.

c) El router 1 sigue teniendo como ruta predeterminada la dirección anterior. PC0 envía un paquete a PC6, ¿llegará?

El paquete tiene como IP origen 192.168.0.10 y como IP destino 192.168.20.10. El paquete sale de PC0 y llega al router 1, que comprueba en su tabla de enrutamiento si conoce algún camino que llegue a la red 192.168.20.0, pero no lo conoce, así que envía el paquete a la puerta de enlace 162.10.0.2 (ruta predeterminada) y llega al router 2.

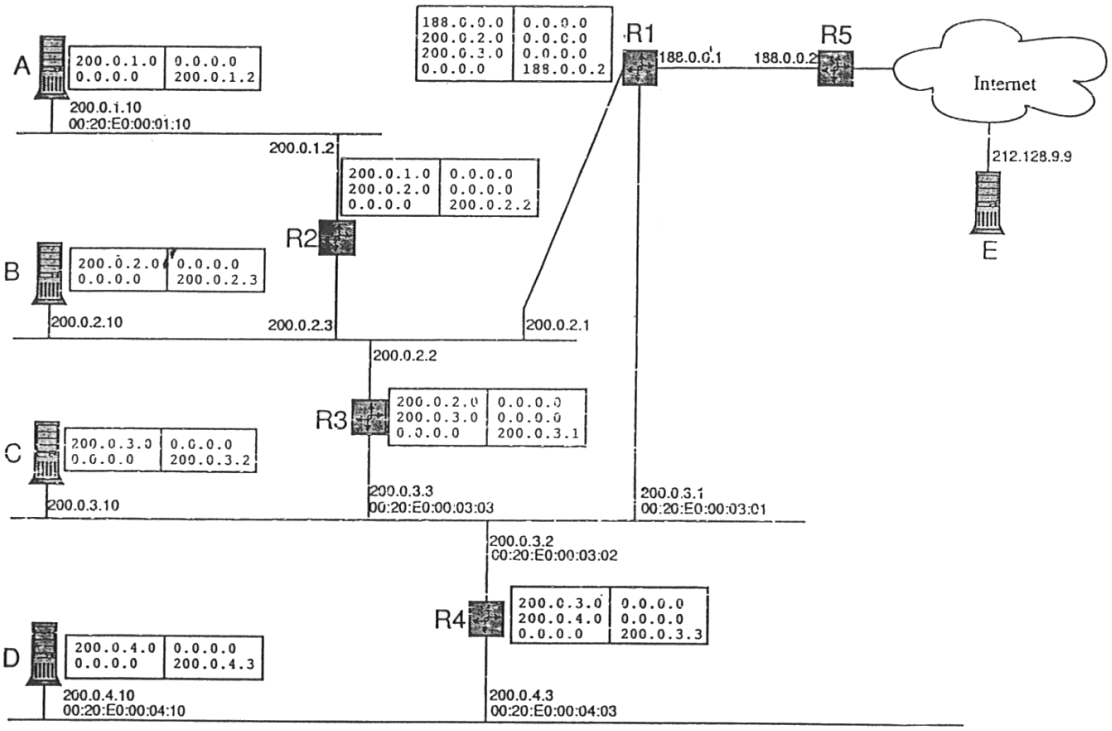
El router 2 comprueba en su tabla *routing* si conoce algún camino que llegue a la red 192.168.30.0, pero no conoce ninguno, así que envía el paquete por su ruta predeterminada que es al *gateway* 162.30.0.2, llegando al router 4.

El router 4 comprueba en su tabla *routing* si conoce algún camino que llegue a la red 192.168.30.0, pero no conoce ninguno, así que envía el paquete por su ruta predeterminada que es 162.30.0.1 y llega al router 2 de nuevo.

El paquete irá rebotando del router 2 al router 4 hasta que se agote su tiempo de vida (TTL) y se deseche, por lo que **no llega** a su destino.

Ejercicio 10 – Comprobar la comunicación

La siguiente figura corresponde con la red interna de una organización que permite la interconexión entre sus máquinas, así como que éstas accedan a Internet. Dicha red interna se compone de 4 subredes Ethernet interconectadas a través de 4 routers. Uno de ellos, R1, es el que proporciona el acceso a Internet a toda la organización, a través de una línea punto a punto con R5. La máscara en todas las subredes es 255.255.255.0. Al lado de cada interfaz de comunicaciones aparece la dirección IP que tiene asignada.



a) Explica razonadamente si las tablas de encaminamiento de la figura impiden la conectividad con Internet de A, B, C y D.

b) Explica razonadamente si las tablas de enrutamiento de la figura impiden alguna comunicación entre las máquinas A, B, C, D.

c) Teniendo en cuenta las tablas de encaminamiento de la figura y el comportamiento correcto de los protocolos ARP e IP, indica si cada una de las siguientes tramas puede aparecer en la red de la figura. En caso afirmativo, indica en qué subredes puede aparecer.

1)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Solicitud	200.0.4.3

2)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Solicitud	200.0.3.3

3)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	Eth. Pedida
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Respuesta	00:20:E0:00:04:10

4)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
FF:FF:FF:FF:FF:FF	00:20:E0:00:09:09	ARP	Solicitud	200.0.4.10

5)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:02	IP	200.0.3.2	200.0.3.1

6)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:02	IP	200.0.4.10	212.128.9.9

7)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:03	IP	200.0.4.10	212.128.9.9

Solución

a) Explica razonadamente si las tablas de encaminamiento de la figura impiden la conectividad con Internet de A y B.

Para resolver este apartado hay que comprobar si existe comunicación entre cada uno de los *hosts* y la salida del router 1, que es quién da acceso a Internet. Cuando se habla de comunicación, se refiere a que es capaz de enviar y recibir mensajes de R1.

Conexión entre A y R1:

1) A → R1 (enviar datos)

El *host* "A" no conoce ninguna ruta que lleve a "R1", así que tomaría su ruta predeterminada (200.0.1.2) llegando a "R2". "R2" tampoco sabe cómo llegar a la red 188.0.0.0, así que tomaría su ruta predeterminada (200.0.2.2) llegando a "R3". "R3" tampoco sabe cómo llegar a la red 188.0.0.0, así que tomaría su ruta predeterminada (200.0.3.1) llegando a "R1", es decir, a Internet. Por tanto, sí hay conexión A → R1.

El viaje sería: A → R2 → R3 → R1

2) R1 → A (recibir datos)

El router 1 no conoce ningún camino que llegue a la red que pertenece el *host* "A" (200.0.1.0), así que tomaría su ruta predeterminada (188.0.0.2) llegando a "R5", es decir, a Internet. Por tanto, no hay conexión R1 → A.

Con esto se concluye que, aunque "A" sí puede enviar datos a "R1", no puede recibirlos y, por tanto, **no hay comunicación completa** entre "A" e Internet.

Conexión entre B y R1:

1) B → R1

El *host* "B" no conoce ninguna ruta que lleve a "R1", así que tomaría su ruta predeterminada (200.0.1.3) llegando a "R2". Anteriormente se ha comprobado que "R2" tiene conectividad con Internet, por lo que no es necesario volver a explicarlo.

El viaje sería: B → R2 → R3 → R1

2) R1 → B

El router 1 sí conoce un camino a la red que pertenece el *host* "B" (200.0.2.0) y se observa que, además, la red destino está localmente conectada con "R1" ya que el *gateway* es 0.0.0.0, por lo que sí hay comunicación.

El viaje sería: R1 → B

Con esto se concluye que **sí hay comunicación completa** entre B e Internet.

Conexión entre C y R1:

1) El viaje sería: C → R1 : C → R4 → R3 → R1
2) El viaje sería: R1 → C : R1 → C

Con esto se concluye que **sí hay comunicación completa** entre C e Internet.

Conexión entre D y R1:

1) El viaje sería: D → R1 : D → R4 → R3 → R1
2) El viaje sería: R1 → D : R1 → R5 (no hay comunicación)

Con esto se concluye que **no hay comunicación completa** entre D e Internet.

b) Explica razonadamente si las tablas de enrutamiento de la figura impiden alguna comunicación entre las máquinas A, B, C, D.

Conexión entre A y B:

1) El viaje sería: A → B : A → R2 → B
2) El viaje sería: B → A : B → R2 → A

Sí hay comunicación completa entre A y B.

Conexión entre A y C:

1) El viaje sería: A → C : A → R2 → R3 → C
2) El viaje sería: C → A : C → R4 → R3 → R1 → R5 (NO)

No hay comunicación completa entre A y C.

Conexión entre A y D:

1) El viaje sería: A → D : A → R2 → R3 → R1… (NO)
2) El viaje sería: D → A : B → R4 → R3 → R1… (NO)

No hay comunicación completa entre A y D.

Conexión entre B y C:

1) El viaje sería: B → C : B → R2 → R3 → C
2) El viaje sería: C → B : C → R4 → R3 → B

Sí hay comunicación completa entre B y C.

Conexión entre B y D:

1) El viaje sería: B → D : B → R2 → R3 → R1… (NO)
2) El viaje sería: D → B : D → R4 → R3 → B

No hay comunicación completa entre B y D.

Conexión entre C y D:

1) El viaje sería: C → D : C → R4 → D
2) El viaje sería: D → C : D → R4 → C

Sí hay comunicación completa entre C y D.

c) Teniendo en cuenta las tablas de encaminamiento de la figura y el comportamiento correcto de los protocolos ARP e IP, indica si cada una de las siguientes tramas puede aparecer en la red de la figura. En caso afirmativo, indica en qué subredes puede aparecer.

1)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Solicitud	200.0.4.3

2)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Solicitud	200.0.3.3

3)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	Eth. Pedida
00:20:E0:00:04:03	00:20:E0:00:04:10	ARP	Respuesta	00:20:E0:00:04:10

4)

Eth. Destino	Eth. Origen	Protocolo	Solicitud / Respuesta	¿IP?
FF:FF:FF:FF:FF:FF	00:20:E0:00:09:09	ARP	Solicitud	200.0.4.10

5)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:02	IP	200.0.3.2	200.0.3.1

6)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:02	IP	200.0.4.10	212.128.9.9

7)

Eth. Destino	Eth. Origen	Protocolo	IP Origen	IP Destino
00:20:E0:00:03:01	00:20:E0:00:03:03	IP	200.0.4.10	212.128.9.9

1) **NO ES POSIBLE:** El protocolo ARP sirve para averiguar la dirección física o Ethernet MAC del *host* que tiene configurada una determinada IP. Para ello, se envía una trama "ARP *request*" a difusión o *broadcast* (todos los *hosts* de esa subred) y solo responderá el *host* que tenga esa IP. En este caso, el ARP *request* no se está enviando a difusión (FF:FF:FF:FF:FF:FF), sino que se está enviando a 00:20:E0:00:04:03 y eso no es posible.

2) **NO ES POSIBLE:** Al igual que el anterior, el "ARP *request"* no se está enviando a difusión (FF:FF:FF:FF:FF:FF), sino que se está enviando a 00:20:E0:00:04:03.

3) **SÍ ES POSIBLE:** Se trata de una trama "ARP *reply"*, en el que el *host* con MAC 00:20:E0:00:04:10 le está informando al *host* con MAC 00:20:E0:00:04:03 su dirección MAC. Como los equipos pertenecen a la misma subred (200.0.4.0), no hay problema y sí es posible.

4) **NO ES POSIBLE:** Aunque esta vez sí se está enviando la trama "ARP *request"* a difusión (FF:FF:FF:FF:FF:FF), no es posible porque el *host* está preguntando por la MAC de un equipo que no está en su misma subred y los ARP solo se envían a los equipos que pertenecen al mismo dominio de difusión (el equipo con MAC 00:20:E0:00:09:09 y el equipo con IP 200.0.4.10 no están en la misma subred).

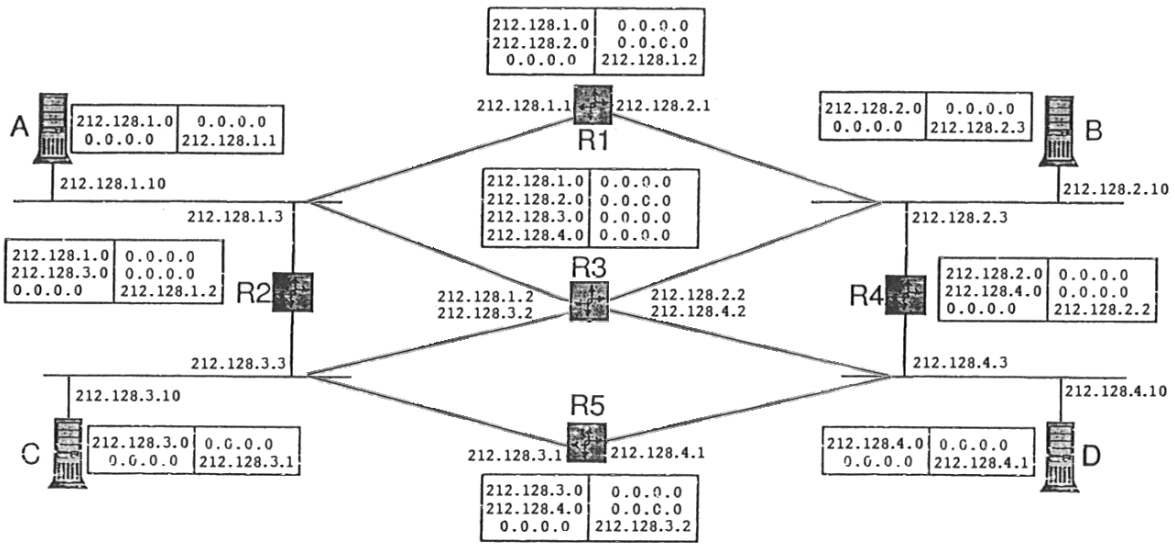
5) **NO ES POSIBLE:** Las MAC son correctas, pero las IP no. Las IP origen y destino deben ser las de los *hosts* originarios, no la de los *routers* que hay en el camino.

6) **NO ES POSIBLE:** El origen de los datos es "D" y destino final es "E". En este momento, la trama la tiene "R4" y va a enviársela a "R1", pero eso no ocurriría. En la tabla de enrutamiento de "R4" no existe ninguna ruta a la red destino, así que la enviaría por su predeterminada a "R3" y no a "R1". El viaje desde "D" a "E" sería: D → R4 → R3 → R1 → R5 → E

7) **SÍ ES POSIBLE:** Estamos en la misma situación que el anterior, pero esta vez "R4" va a enviarle la trama a "R3" y es así como ocurriría.

Ejercicio 11 – Modificar tablas de enrutamiento

La figura que se muestra corresponde con 4 redes Ethernet interconectadas a través de 5 routers. La máscara de subred en todas ellas es 255.255.255.0. Al lado de cada interfaz de comunicaciones aparece la dirección IP asignada.



Supongamos que se cae la interfaz superior izquierda de R3 (IP:212.128.1.2). Modifica las tablas de los routers para que no se pierda conectividad. No pueden modificarse las tablas de A, B, C ni D. Se valorará efectuar el menor número de cambios necesarios.

Solución

Se va a comprobar la conectividad de todos los *hosts* de la red teniendo en cuenta la interfaz caída (212.128.1.2) y se arreglará el fallo en aquellos casos que lo necesiten.

Conexión entre A y B:

1) A → B

El *host* "A" no tiene ninguna ruta en su tabla de enrutamiento que llegue a la red donde se encuentra "B" (212.128.2.0), así que tomaría su ruta predeterminada (212.128.1.1) llegando a "R1". "R1" sí conoce una ruta para llegar a la subred de "B" (212.128.2.0) y, por lo que se observa, está directamente conectada ya que la puerta de enlace es 0.0.0.0, por tanto, sí le llega el paquete a "B".

2) B → A

El *host* "B" no tiene ninguna ruta en su tabla de encaminamiento que llegue a la red donde se encuentra "A" (212.128.1.0), así tomaría su ruta predeterminada (212.128.2.3) y el paquete llega a "R4". "R4" tampoco tiene ninguna ruta que llegue a la red 212.128.1.0, así que tomaría su ruta predeterminada (212.128.2.2) y llega a "R3". "R3" sí conoce una ruta para llegar a la red 212.128.1.0, pero el camino está cortado, así que el paquete no llegaría.

Para arreglar esto, la mejor opción es modificar la tabla de "R4" para que, en caso de querer enviar un paquete a la subred 212.128.1.0, lo envíe por la pasarela 212.128.2.1 (R1). La tabla de encaminamiento de "R4" quedaría:

R4

212.128.2.0	0.0.0.0
212.128.4.0	0.0.0.0
212.128.1.0	212.128.2.1
0.0.0.0	212.128.2.2

Conexión entre A y C:

1) A → C

El *host* "A" no tiene ninguna ruta en su tabla de encaminamiento que llegue a la red donde se encuentra "C" (212.128.3.0), así que tomaría su ruta predeterminada (212.128.1.1) y el paquete llega a "R1". "R1" tampoco conoce una ruta que llegue a 212.128.3.0, así que lo intenta enviar a la interfaz 212.128.1.2 (R3), pero está cortada, así que el camino no llegaría.

Para arreglar esto, se le puede añadir a "R1" la ruta a la red 212.128.3.0 por la puerta de enlace 212.128.1.3, así llegará a "R2" y de ahí al *host* "C".

R1

212.128.1.0	0.0.0.0
212.128.2.0	0.0.0.0
212.128.3.0	212.128.1.3
0.0.0.0	212.128.1.2

2) C → A

El *host* "C" no tiene ninguna ruta en su tabla que llegue a la red donde se encuentra "A" (212.128.1.0), así que tomaría su ruta predeterminada (212.128.3.1) y el paquete llega a "R5". "R5" tampoco tiene ninguna ruta que llegue a la red 212.128.1.0, así que tomaría su ruta predeterminada (212.128.3.2) y llega a "R3". "R3" sí conoce una ruta para llegar a la red 212.128.1.0, pero el camino está cortado, así que el paquete no llegaría.

Para arreglar esto, lo más sencillo es añadir a "R5" la ruta a la red 212.128.1.0 por la puerta de enlace 212.128.3.3, así llegará a "R2" y de ahí al *host* "A".

R5	212.128.3.0	0.0.0.0
	212.128.4.0	0.0.0.0
	212.128.1.0	212.128.3.3
	0.0.0.0	212.128.3.2

Conexión entre A y D:

Siguiendo la misma metodología que la anterior, comprobamos la conexión sin dar más detalles que las rutas que toman. En cada comprobación, se tendrá en cuenta las modificaciones anteriores.

1) A → D

La ruta que tomaría es: A → R1 → (cortada, no llega)

Se añade "R1" una ruta que llegue a 212.128.4.0.

R1	212.128.1.0	0.0.0.0
	212.128.2.0	0.0.0.0
	212.128.3.0	212.128.1.3
	212.128.4.0	212.128.2.3
	0.0.0.0	212.128.1.2

La ruta que tomaría ahora es: A → R1 → R4 → D

2) D → A

La ruta que tomaría es: D → R4 → R1 → A (llega)

Conexión entre B y C:

1) B → C

La ruta que tomaría es: B → R4 → R3 → C (llega)

2) C → B

La ruta que tomaría es: C → R5 → R3 → B (llega)

Conexión entre B y D:

1) B → D

La ruta que tomaría es: B → R4 → D (llega)

2) D → B

La ruta que tomaría es: D → R5 → R3 → B (llega)

Conexión entre C y D:

1) C → D

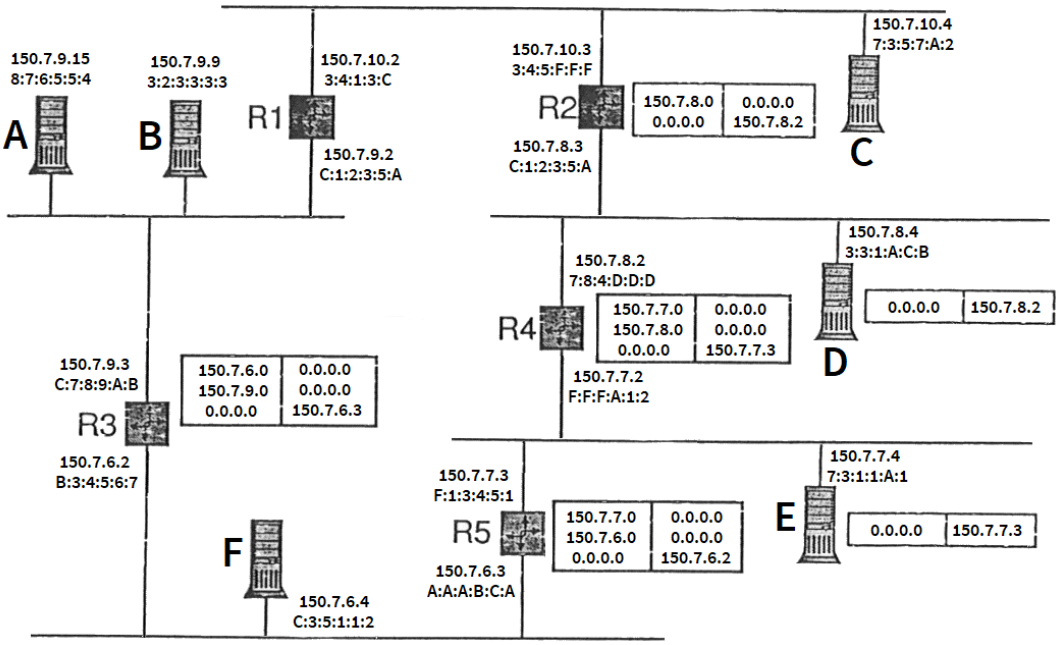
La ruta que tomaría es: C → R5 → D (Llega)

2) D → C

La ruta que tomaría es: D → R5 → C (Llega)

Ejercicio 12 – Describir el viaje de los mensajes

La figura que se muestra corresponde con la red interna de una organización. Todas las subredes son Ethernet y la máscara de red en todas es de 255.255.255.0. Al lado de cada interfaz aparece la dirección IP asignada y debajo la dirección Ethernet (MAC).



Contesta:

a) En la máquina "D" se ejecuta el comando "ping 150.7.6.23". Sin embargo, no existe ninguna máquina que tenga asignada esa dirección IP. ¿Quién detecta este hecho, A, B, C, D, E, F, R1, R2, R3, R4 o R5? Explica cómo lo detecta y qué hace a partir de entonces

b) La máquina "E" envía un datagrama IP (paquete) a la máquina "A" con TTL 3. Describe los pasos que realiza cada dispositivo, indicando las direcciones MAC que intervienen y la variación del campo TTL, ordenadas temporalmente, hasta que el datagrama alcanza el destino.

c) Modifique las tablas de encaminamiento necesarias para que la máquina "E" puede enviar datagramas IP a la máquina "C" por la ruta más corta (menor número de routers).

Solución

a) En la máquina "D" se ejecuta el comando "ping 150.7.6.23". Sin embargo, no existe ninguna máquina que tenga asignada esa dirección IP. ¿Quién detecta este hecho, A, B, C, D, E, F, R1, R2, R3, R4 o R5? Explica cómo lo detecta y qué hace a partir de entonces

Lo detecta "R5". A continuación, se muestra la explicación:

El comando ping genera un paquete "ICMP *echo request*" con dirección IP origen 150.7.8.4 e IP destino 150.7.6.23. "D" envía ese paquete por su ruta predeterminada (150.7.8.2) llegando a "R4".

"R4" comprueba la IP destino y, como no conoce ninguna ruta a la red 150.7.6.0, lo envía por su ruta predeterminada (150.7.7.3) llegando a "R5".

"R5" sí conoce una ruta para llegar a la red 150.7.6.0 ya que está directamente conectada. Como "R5" no conoce la MAC del *host* con IP 150.7.6.23 (no es posible que esté en su tabla ARP ya que el *host* no existe), desecha el paquete original, manda un mensaje "ARP *request*" a difusión y genera un paquete "ICMP *host unreachable*" con dirección IP origen 150.7.6.3 (R5) y destino 150.7.8.4 (D) para notificarle a "D" que el *host* 150.7.6.23 no pudo ser localizado.

b) La máquina "E" envía un datagrama IP (paquete) a la máquina "A" con TTL 3. Describe los pasos que realiza cada dispositivo, indicando las direcciones MAC que intervienen y la variación del campo TTL, ordenadas temporalmente, hasta que el datagrama alcanza el destino.

La máquina "A" no se encuentra en la misma subred que "E", así que "E" envía una trama "ARP *request*" a difusión preguntando por la MAC del dispositivo con IP 150.7.7.3 (R5).

"R4" recibe la trama "ARP *request"*, pero como no va dirigido a él, lo desecha. "R5" también lo recibe y como sí va dirigido a él, contesta con una trama "ARP *reply"* a "E" diciéndole que su MAC es F:1:3:4:5:1.

Como "E" ya tiene la MAC destino, forma un paquete con dirección IP origen 150.7.7.4, IP destino 150.7.9.15 y TTL de 3. "E" sigue encapsulando el mensaje y forma una trama con dirección MAC origen 7:3:1:1:A:1 (E) y MAC destino F:1:3:4:5:1 (R5) y lo envía.

La trama llega a "R5" y comprueba que la MAC destino es la suya, así que desencapsula la trama formando un paquete. "R5" comprueba si la IP destino es la suya, pero no lo es, así que tiene que reenviar el paquete.

"R5" comprueba en su tabla de enrutamiento si conoce una ruta para llegar a la red 150.7.9.0, pero como no conoce ninguna, envía el paquete por la ruta predeterminada al router con IP 150.7.6.2 (R3).

"R5" no puede encapsular el paquete y formar una trama porque no conoce la MAC de "R3", así que desecha el paquete original y envía un "ARP *request*" a difusión para que el dispositivo con IP 150.7.6.2 le responda con su dirección MAC. "R5" recibe un "ARP *reply*" de "R3" diciendo que su MAC es B:3:4:5:6:7. Por esta razón, cuando se hace ping a un equipo de otra subred, se pierden tantos paquetes como saltos hay (saber más).

"R5" ya no tiene el paquete original, pero vamos a suponer que en el paso anterior "R5" no desechó el paquete o que "E" lo vuelve a enviar y llega de nuevo a "R5". En este momento, "R5" ya sabe la MAC de "R3", así que le resta 1 al TTL del paquete dejándolo en 2 y lo encapsula en una trama con MAC origen A:A:A:B:C:A (R5) y MAC destino B:3:4:5:6:7 (R3) y lo envía.

La trama llega a "R3", éste comprueba que la MAC destino es la suya y desencapsula la trama formando un paquete. "R3" comprueba que la IP destino no es la suya, por lo que tiene que reenviar el paquete.

"R3" comprueba en su tabla de enrutamiento si conoce una ruta que llegue a la red 150.7.9.0 y sí conoce una, que es por la puerta de enlace 0.0.0.0 (directamente conectada), así que se dispone a enviar el paquete al *host* "A" (150.7.9.15).

"R3" no puede encapsular el paquete y formar una trama porque no conoce la MAC de "A", así que desecharía el paquete y enviaría un "ARP *request*" a difusión para que el dispositivo con IP 150.7.9.15 (A) le responda con su dirección MAC. "R3" recibe un "ARP *reply*" de "A" diciendo que su MAC es 8:7:6:5:5:4.

"R3" ya no tiene el paquete original, pero vamos a volver a suponer que "R3" no desechó el paquete o que "E" lo vuelve a enviar y llega de nuevo a "R3". En este momento "R3" ya sabe la MAC de "A", así que le resta 1 al TTL del paquete dejándolo el 1 y lo encapsula en una trama con MAC origen C:7:8:9:A:B y MAC destino 8:7:6:5:5:4.

La trama llega a "A" y éste comprueba que la MAC destino es la suya, así que lo desencapsula formando un paquete. "A" comprueba que la IP destino del paquete es la suya, así que lo desencapsula formando un segmento y sigue desencapsulando el mensaje hasta leer los datos.

c) Modifique las tablas de encaminamiento necesarias para que la máquina "E" puede enviar datagramas IP a la máquina "C" por la ruta más corta (menor número de routers).

La ruta más corta es E → R4 → R2 → C.

Para que "E" lo envíe a "R4", se modifica su tabla de enrutamiento dejándola:

E	150.7.10.0 0.0.0.0	150.7.7.2 150.7.7.3

Para que "R4" lo envía a "R2", se modifica su tabla de enrutamiento dejándola:

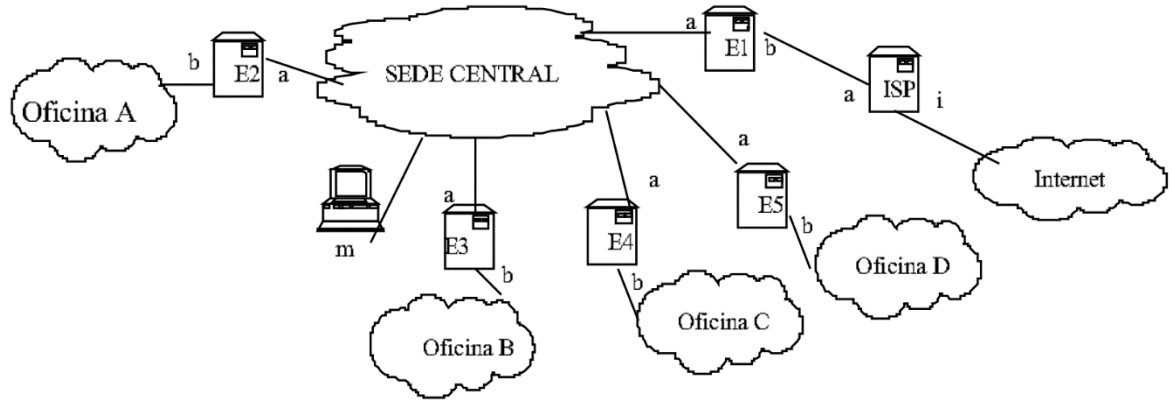
R4	150.7.7.0 150.7.8.0 150.7.10.0 0.0.0.0	0.0.0.0 0.0.0.0 150.7.8.3 150.7.7.3

"R2" está directamente conectado a la subred 150.7.10.0, pero no la tiene en su tabla de enrutamiento. Se modifica dejándola:

R2	150.7.8.0	0.0.0.0
	150.7.10.0	0.0.0.0
	0.0.0.0	150.7.8.2

Ejercicio 13 – Subnetting

La red de una organización se estructura en 5 subredes tal y como se muestra en la siguiente figura:



La organización propietaria de la red dispone del espacio de direcciones 155.221.80.0/22 para su gestión. En la sede central se necesitan en este momento 300 direcciones IP, mientras que en las oficinas se necesitan entre 70 y 90 (en cada una de ellas). Se pide:

a) Establecer las direcciones de red y máscaras de red de cada una de las subredes de la organización (central, oficina A, oficina B, oficina C y oficina D) y asignar una dirección IP a cada una de las interfaces de red que aparecen nombradas en la figura, excepto E1/b, ISP/a e ISP/i.

b) Escribir la tabla de encaminamiento de una máquina "m" ubicada en la red central, indicando las columnas "@destino", "máscara" y "siguiente router". Escribir así mismo las líneas que aparezcan en la tabla del router ISP relacionadas con la red de la organización.

c) Supongamos que se abre una nueva oficina, A2, cuya red se conecta a la red de la organización a través de una nueva interfaz en E2. Como quedan pocas direcciones IP libres, la organización solicita otro bloque y se le asigna el espacio de direcciones 157.24.51.0/25.

    a. Asignar una dirección de red a A2, teniendo en cuenta que la nueva oficina necesita 50 direcciones IP y que se prevé la apertura de otra oficina para la cual queremos reservar al menos otras 50. No olvides indicar también la máscara de red.

    b. Indica los cambios que habrá que realizar en la tabla de enrutamiento de la máquina "m".

Solución

a) Establecer las direcciones de red y máscaras de red de cada una de las subredes de la organización (central, oficina A, oficina B, oficina C y oficina D) y asignar una dirección IP a cada una de las interfaces de red que aparecen nombradas en la figura, excepto E1/b, ISP/a e ISP/i.

1º Analizar la situación

El ejercicio no dice si la máscara de subred es de tamaño fijo o variable (VLSM), por lo que primero vamos a comprobar si se puede hacer usando una máscara de tamaño fijo.

Como la máscara de subred es /22, podemos usar 10 bits (32-22) para asignar a *hosts* o hacer *subnetting*. La subred más grande necesita 300 *hosts* y, para conectar esos *hosts*, necesitamos 9 bits (2^9-2=510≥300). Si el espacio de direcciones dispone de 10 bits y cada subred necesita 9, tan solo podemos usar 1 bit para crear subredes, lo que nos da un máximo de 2 subredes (2^1=2). Por tanto, no es posible hacerlo con una máscara de tamaño fijo y es necesario utilizar una máscara de tamaño variable o VLSM.

2º - Obtener la dirección IP de cada subred y su máscara de red

Oficina central → 300 *hosts*

Para asignar 300 *hosts* necesitamos 9 bits. Con el bit que nos sobra, podemos dividir la red en 2 subredes de 512 direcciones cada una.

Subred 0 → 155.221.01010000.00000000 → 155.221.80.0/23 → **Oficina central**
Subred 1 → 155.221.01010010.00000000 → 155.221.82.0/23

Oficinas → 90 *hosts* cada una

Para asignar 90 *hosts* necesitamos 7 bits (2^7-2=126≥90). Como vamos a dividir la subred 1, nos sobrarían 2 bits, por lo que podemos dividirla en 4, quedando:

Subred 1: 155.221.01010010.00000000 → 155.221.82.0/23
- Subred 1-0: 155.221.01010010.00000000 → 155.221.82.0/25 → **Oficina A**
- Subred 1-1: 155.221.01010010.10000000 → 155.221.82.128/25 → **Oficina B**
- Subred 1-2: 155.221.01010011.00000000 → 155.221.83.0/25 → **Oficina C**
- Subred 1-3: 155.221.01010011.10000000 → 155.221.83.128/25 → **Oficina D**

3º Asignar direcciones IP a las interfaces

E1/a = 155.221.80.1
E2/a = 155.221.80.2
E2/b = 155.221.82.1
E3/a = 155.221.80.3
E3/b = 155.221.82.129
E4/a = 155.221.80.4
E4/b = 155.221.83.1
E5/a = 155.221.80.5
E5/b = 155.221.83.129
m = 155.221.80.6

b) Escribir la tabla de encaminamiento de una máquina "m" ubicada en la red central, indicando las columnas "@destino", "máscara" y "siguiente router". Escribir así mismo las líneas que aparezcan en la tabla del router ISP relacionadas con la red de la organización.

Máquina m:

@destino	máscara	siguiente router
155.221.80.0	255.255.254.0	155.221.80.6
155.221.82.0	255.255.255.128	155.221.80.2
155.221.82.128	255.255.255.128	155.221.80.3
155.221.83.0	255.255.255.128	155.221.80.4
155.221.83.128	255.255.255.128	155.221.80.5
0.0.0.0	0.0.0.0	155.221.80.1

Enrutador ISP:

@destino	máscara	siguiente router
155.221.80.0	255.255.252.0	E1/b

c) Supongamos que se abre una nueva oficina, A2, cuya red se conecta a la red de la organización a través de una nueva interfaz en E2. Como quedan pocas direcciones IP libres, la organización solicita otro bloque y se le asigna el espacio de direcciones 157.24.51.0/25.

   a. Asignar una dirección de red a A2, teniendo en cuenta que la nueva oficina necesita 50 direcciones IP y que se prevé la apertura de otra oficina para la cual queremos reservar al menos otras 50. No olvides indicar también la máscara de red.

El espacio de direcciones 157.24.51.0/25 nos da 7 bits (32-25) para asignar a *hosts* o hacer *subnetting*. Para conectar 50 *hosts* necesitamos 6 bits (2^6-2=62≥50), por lo que nos sobra 1 bit que nos permite dividir la red en 2 subredes.

Subred 0: 157.24.51.00000000 → 157.24.51.0/26 → **Oficina A2**
Subred 1: 157.24.51.01000000 → 157.24.51.64/26 → **Oficina futura**

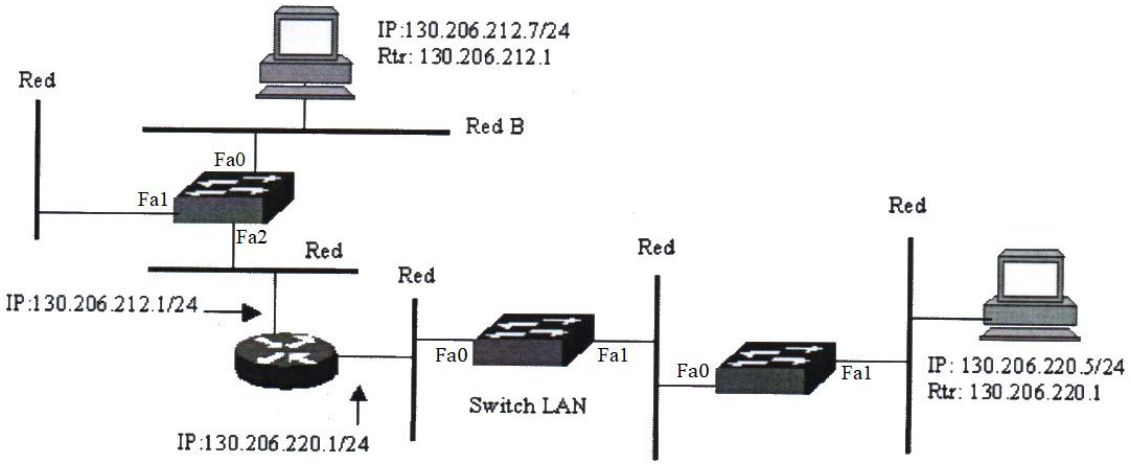
   b. Indica los cambios que habrá que realizar en la tabla de enrutamiento de la máquina "m".

Máquina m:

@destino	máscara	siguiente router
155.221.80.0	255.255.254.0	155.221.80.6
155.221.82.0	255.255.255.128	155.221.80.2
155.221.82.128	255.255.255.128	155.221.80.3
155.221.83.0	255.255.255.128	155.221.80.4
155.221.83.128	255.255.255.128	155.221.80.5
157.24.51.0	255.255.255.192	155.221.80.2
0.0.0.0	0.0.0.0	155.221.80.1

Ejercicio 14 – Tramas Ethernet

En la red de la figura adjunta se acaban de arrancar los seis equipos que aparecen y, a continuación, un usuario teclea en el ordenador 130.206.212.7 el comando "ping 130.206.220.5" para saber si está operativo el otro ordenador de la red. Instantes más tarde comprueba que en efecto el otro ordenador responde correctamente.



Describa con detalle todas las tramas Ethernet generadas en cada una de las redes que aparecen en la figura como consecuencia de dicha acción, y en que secuencia se producen. Explique el significado de cada una de las tramas.

Supongamos que las direcciones Ethernet MAC de cada IP son las siguientes:

Dirección IP	Dirección MAC
130.206.212.7	00:00:00:AA:AA:AA
130.206.212.1	00:00:00:BB:BB:BB
130.206.220.1	00:00:00:CC:CC:CC
130.206.220.5	00:00:00:DD:DD:DD

Solución

El equipo origen va a enviar un paquete "ICMP *echo request*" (mensaje ping) a un equipo que está en una red distinta, por lo que necesita enviarlo a su puerta de enlace (*router*) para que éste se encargue de enrutarlo a otra red. Vamos a ver cómo es este viaje.

Viaje de equipo origen al *router*

Si las máquinas acaban de arrancar, todos los nodos tienen inicialmente su tabla ARP vacía. Esto significa que el equipo origen no conoce la MAC del *router* y, por tanto, no puede enviarle la trama Ethernet (capa 2) con el ping.

Para averiguarlo, el equipo origen crea una trama "ARP *request*" preguntando cuál es la dirección MAC del nodo con IP 130.206.212.1 (*router*) y la envía a difusión. La trama generada es la siguiente:

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:AA:AA:AA	FF:FF:FF:FF:FF:FF	ARP (solicitud)	130.206.212.7	130.206.212.1

Esa trama llega al *switch*, que la retransmite por las 2 salidas que tiene (Fa1 y Fa2). Por la salida "Fa1" nunca obtendrá respuesta y por "Fa2" llega al *router*. En el momento de retransmitir la trama, el *switch* registra en su tabla MAC que en el puerto "Fa0" hay conectado un equipo con MAC 00:00:00:AA:AA:AA (equipo origen).

Cuando la trama llega al *router*, éste la lee y le responde al equipo origen con una trama "ARP *reply*" diciendo que su MAC es 00:00:00:BB:BB:BB. La trama de respuesta es:

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:BB:BB:BB	00:00:00:AA:AA:AA	ARP (respuesta)	130.206.212.1	130.206.212.7

Esta trama llega al *switch* y la retransmite únicamente por el puerto "Fa0" porque en su tabla MAC ya sabe en ese puerto está conectado el equipo origen. El *switch* registra que en el puerto "Fa2" está conectado el equipo con MAC 00:00:00:BB:BB:BB (*router*).

El equipo origen recibe el "ARP *reply*" y apunta en su tabla ARP que el equipo con IP 130.206.212.1 tiene la MAC 00:00:00:BB:BB:BB. Como el equipo origen ya conoce la MAC del *router*, ahora le puede enviar la trama Ethernet que contiene el ping.

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:AA:AA:AA	00:00:00:BB:BB:BB	IP	130.206.212.7	130.206.212.5

Viaje del *router* al equipo destino

Ahora la trama la tiene el *router*, pero para enviársela al equipo destino necesita saber su MAC y no la sabe. Así pues, el *router* desecha la trama que contiene el ping (este ping se pierde) y crea una nueva trama de tipo "ARP *request*". Esta trama la envía a difusión preguntando cuál es la dirección MAC del nodo con IP 130.206.220.1 (equipo destino). La trama generada es la siguiente:

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:CC:CC:CC	FF:FF:FF:FF:FF:FF	ARP (solicitud)	130.206.220.1	130.206.220.5

La trama ARP llega al *switch* LAN, que lo retransmite a difusión (también registra que en el puerto "Fa0" está la MAC del *router*). La trama llega al otro *switch*, que lo retransmite también a difusión (y hace el registro correspondiente en su tabla MAC). Finalmente, la trama llega al equipo destino y éste le contesta con un "ARP *reply*" diciendo que su MAC es 00:00:00:DD:DD:DD. La trama de respuesta es:

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:DD:DD:DD	00:00:00:CC:CC:CC	ARP (respuesta)	130.206.220.5	130.206.220.1

Esa trama llega al *switch*, que lo retransmite al *switch LAN* y el *switch LAN* lo retransmite al *router*.

El *router*, que ya conoce la MAC del equipo destino, genera la trama que contiene el ping (suponemos que el equipo origen vuelve a enviar otro ping o que el paquete con el ping original no se desechó). La trama es:

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:CC:CC:CC	00:00:00:DD:DD:DD	IP	130.206.212.7	130.206.220.5

Esa trama la recibe el primer *switch*, luego el otro y, finalmente, llega al equipo destino. El equipo destino la lee y responde con un paquete "ICMP *echo reply*" para que el equipo origen sepa que sí hay conexión.

El equipo destino genera una trama y se la transmite al *router* donde está conectado.

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:DD:DD:DD	00:00:00:CC:CC:CC	IP	130.206.220.5	130.206.212.7

La trama llega a un *switch*, que lo envía al *switch* LAN y éste al *router*. El *router* lee la trama y genera otra trama con el equipo origen como destino.

MAC Origen	MAC Destino	Protocolo	IP Origen	IP Destino
00:00:00:BB:BB:BB	00:00:00:AA:AA:AA	IP	130.206.220.5	130.206.212.7

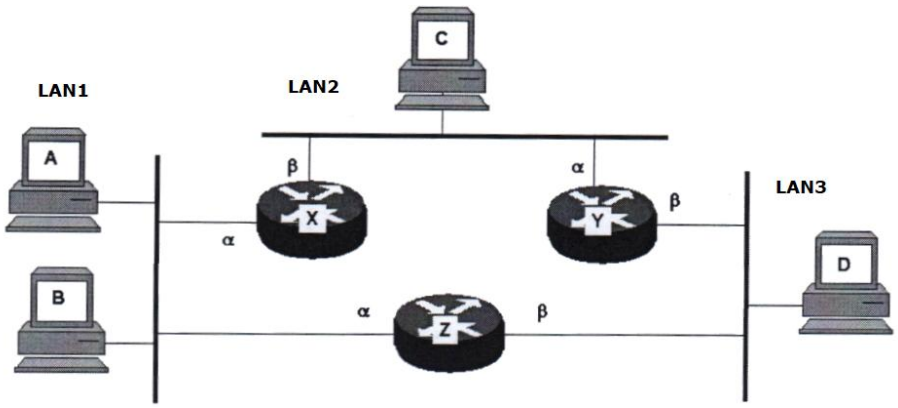
El *router* envía la trama al *switch* y éste, finalmente, se lo envía al equipo origen.

Suponiendo que el *router* no desecha el primer ping antes de enviar el "ARP *request*", entre los *switches* y el resto de los nodos, se generan 21 tramas en total.

origen → switch (2) → router → switch → origen → switch → router → switch LAN → switch → destino → switch → switch LAN → router → switch LAN → switch → destino → switch → switch LAN → router → switch → origen

Ejercicio 15 – Subnetting y tablas de enrutamiento

Se quiere montar una red como la de la figura adjunta.



Se dispone para ello las direcciones del rango 194.12.252.0/22. Se prevé que la LAN 1 necesitará como máximo 500 direcciones, la LAN 2 100 y la LAN 3 200. Se pide:

a) Elija y asigne las direcciones de red que debe haber en cada LAN y su máscara.

b) Asigne direcciones IP a las interfaces de los *routers* y defina las rutas que sean precisas.

Solución

a) Elija y asigne las direcciones de red que debe haber en cada LAN y su máscara.

El espacio de direcciones 194.12.252.0/22 nos deja 10 bits (32-10) para asignar a *hosts* y/o hacer subredes. Como la LAN más grande necesita 500 direcciones (9 bits), nos sobra 1 bit para crear subredes, lo que nos da un máximo de 2 subredes si usamos máscara de subred de tamaño fijo. Como necesitamos 3 subredes, vamos a suponer que la máscara de red no es de tamaño fijo y es variable (VLSM).

Para crear las subredes con una máscara de tamaño variable o VLSM, empezamos a hacer *subnetting* a la LAN más grande (LAN1) y terminamos con la más pequeña (LAN2).

LAN1 → 500 *hosts*

Para asignar 500 *hosts* necesitamos 9 bits (2^9-2=510≥500). Con el bit que nos sobra, podemos dividir la red en 2 subredes de 512 direcciones cada una.

Subred 0 → 194.12.111111110**0**.00000000 → 194.12.252.0/23 → **LAN1**
Subred 1 → 194.12.111111111**0**.00000000 → 194.12.254.0/23

LAN3 → 200 *hosts*

Para asignar 200 *hosts* necesitamos 8 bits (2^8-2=254≥200). Como vamos a dividir la subred 1, nos sobraría 1 bit, por lo que podemos dividirla en 2, quedando:

Subred 1: 194.12.111111111**0**.00000000 → 194.12.254.0/23
Subred 1-0: 194.12.111111111**0**.00000000 → 194.12.254.0/24 → **LAN3**
Subred 1-1: 194.12.111111111**1**.00000000 → 194.12.255.0/24

LAN2 → 100 *hosts*

Para asignar 100 *hosts* necesitamos 7 bits (2^7-2=126≥100). Como vamos a dividir la subred 1-1, nos sobraría 1 bit, por lo que podemos dividirla en 2, quedando:

Subred 1-1: 194.12.111111111**1**.00000000 → 194.12.255.0/24
Subred 1-0: 194.12.111111111**1**.**0**0000000 → 194.12.255.0/25→ **LAN2**
Subred 1-1: 194.12.111111111**1**.**1**0000000 → 194.12.255.128/25

b) Asigne direcciones IP a las interfaces de los *routers* y defina las rutas que sean precisas.

Direcciones a las interfaces de los *routers*:

X_α= 194.12.252.1/23 (Está en la LAN 1)
X_β= 194.12.255.1/25 (Está en la LAN 2)
Y_α= 194.12.255.2/25 (Está en la LAN 2)
Y_β= 194.12.254.1/24 (Está en la LAN 3)
Z_α= 194.12.252.2/23 (Está en la LAN 1)
Z_β= 194.12.254.2/24 (Está en la LAN 3)

Tabla de enrutamiento de X:

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
194.12.252.0	255.255.252.0	194.12.252.1	α
194.12.255.0	255.255.255.0	194.12.255.1	β
194.12.254.0	255.255.254.0	194.12.255.2	β
0.0.0.0	0.0.0.0	194.12.255.2	β

Tabla de enrutamiento de Y:

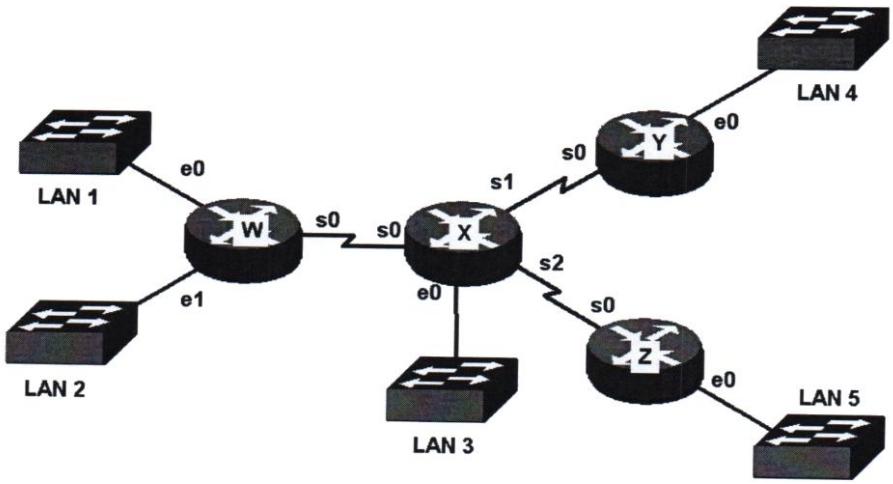
Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
194.12.255.0	255.255.255.0	194.12.255.2	α
194.12.254.0	255.255.254.0	194.12.254.1	β
194.12.252.0	255.255.252.0	194.12.255.1	α
0.0.0.0	0.0.0.0	194.12.255.1	α

Tabla de enrutamiento de Z:

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
194.12.252.0	255.255.252.0	194.12.252.2	α
194.12.254.0	255.255.254.0	194.12.254.1	β
194.12.255.0	255.255.252.0	194.12.254.1	β
0.0.0.0	0.0.0.0	194.12.254.1	β

Ejercicio 16 – Subnetting

Se quiere montar una red IP con una topología como la de la siguiente figura.



Para las LAN 1, 2, 3, y 4 se necesita disponer de 30 direcciones útiles (para cada una). En el caso de la LAN 5 se necesitan 60 direcciones. En todos los casos la primera de las direcciones se reservará para la interfaz del router. Se plantean los siguientes requisitos:

a) Diseñe la asignación completa de redes o subredes IP utilizando direccionamiento privado. Indique las direcciones que podrán utilizarse para los hosts en cada LAN.

b) Asigne direcciones y máscaras a todas las interfaces de los *routers*.

Solución

a) Diseñe la asignación completa de redes o subredes IP utilizando direccionamiento privado. Indique las direcciones que podrán utilizarse para los hosts en cada LAN.

Se nos pide que utilicemos direccionamiento privado, por tanto, tenemos que seleccionar un rango de direcciones privadas. Para este ejercicio se ha elegido el rango 192.168.0.0/16, lo que nos da 16 bits (32-16) para asignar a *hosts* o hacer *subnetting.*

La LAN más grande es al 5, que necesita 60 direcciones. Para asignar 60 direcciones, necesitamos al menos 6 bits (2^6-2=62≥60). Por, tanto:

Subred → 192.168.00000000.00000000 → 192.168.0.0/26 → **LAN5**

Como en las LAN 1, 2, 3 y 4 se van a asignar 30 *hosts*, necesitamos 5 bits (2^5-2=30≥30). Por tanto:

Subred → 192.168.00000000.01000000 → 192.168.0.64/27 → **LAN1**
Subred → 192.168.00000000.01100000 → 192.168.0.96/27 → **LAN2**
Subred → 192.168.00000000.10000000 → 192.168.0.128/27 → **LAN3**
Subred → 192.168.00000000.11000000 → 192.168.0.192/27 → **LAN4**

b) Asigne direcciones y máscaras a todas las interfaces de los *routers*.

Para asignar direcciones IP a las conexiones con cable serie (interfaces que empiezan por "s"), tenemos que saber la dirección de la red a las que pertenecen estas interfaces. Como no nos lo dice el ejercicio, vamos a asignarlas como subredes de 192.168.2.0/24, quedando de la siguiente forma:

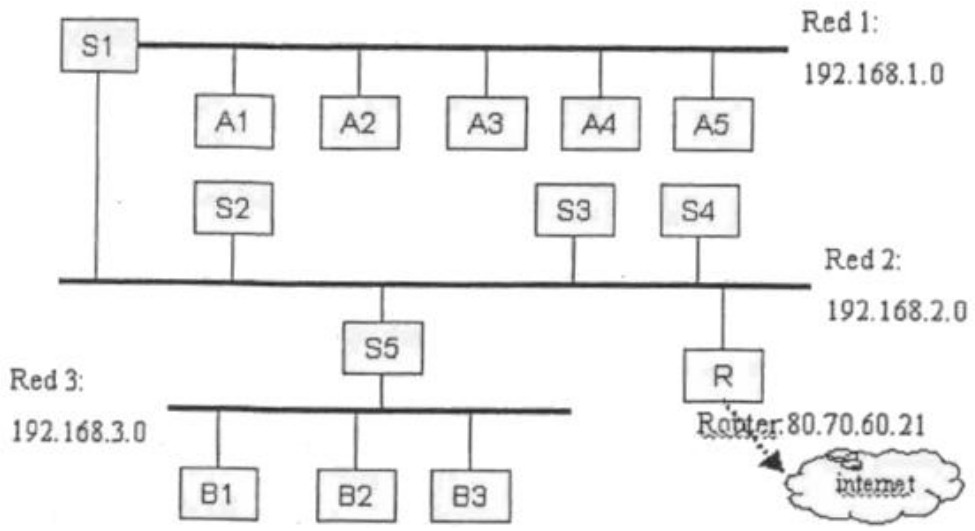
Red W-X = 192.168.2.0/30
Red X-Y = 192.168.2.4/30
Red X-Z = 192.168.2.8/30

Las direcciones de las interfaces de las LAN son las siguientes:

We0 = 192.168.0.65/27
We1 = 192.168.0.97/27
Ws0 = 192.168.2.1/30
Xs0 = 192.168.2.2/30
Xe0 = 192.168.0.129/27
Xs1 = 192.168.2.5/30
Xs2 = 192.168.2.9/30
Ys0 = 192.168.2.6/30
Ye0 = 192.168.0.193/27
Zs0 = 192.168.2.10/30
Ze0 = 192.168.0.1/26

Ejercicio 17 – Examen oposiciones PES 2002

Se tiene el siguiente esquema de redes:



Donde:

- El interfaz de S1 con la Red 1 es eth0, y con la Red 2 es eth1.
- El interfaz de S5 con la Red 2 es eth1, y con la Red 3 es eth0.
- El interfaz del resto de los equipos es eth0.

Hacer:

a) Asignar direcciones IP privadas de clase C a todos los equipos.

b) Definir la tabla de rutas de los equipos A1, S1, S2, S3, S4, S5, B1 y R, de forma que se cumplan las siguientes condiciones:

   - Todos los equipos pueden acceder directamente sin proxy a Internet.
   - Los equipos de la red 1 pueden conectar con el servidor S2.
   - Los equipos de la red 3 pueden conectar con el servidor S3.
   - Todos los equipos pueden conectar con el servidor S4.

Nota: prescindir de la ruta a la red *loopback* en todos los equipos por ser idéntica.

Máquina	Ruta	Destino	Máscara	Pasarela	Interfaz
…….	loopback	127.0.0.0	255.0.0.0	127.0.0.1	lo

El formato de la tabla deberá ser el siguiente:

Máquina	Ruta	Destino	Máscara	Pasarela	Interfaz

Solución

a) Asignar direcciones IP privadas de clase C a todos los equipos.

Red 1 (192.168.1.0):

S1 (eth0): 192.168.1.1
A1: 192.168.1.11
A2: 192.168.1.12
A3: 192.168.1.13
A4: 192.168.1.14
A5: 192.168.1.15

Red 2 (192.168.2.0):

S1 (eth1): 192.168.2.1
S2: 192.168.2.2
S3: 192.168.2.3
S4: 192.168.2.4
S5 (eth1): 192.168.2.5
R: 192.168.2.10

Red 3 (192.168.3.0):

S5 (eth0): 192.168.3.1
B1: 192.168.3.11
B2: 192.168.3.12
B3: 192.168.3.13

b) Definir la tabla de rutas de los equipos A1, S1, S2, S3, S4, S5, B1 y R, de forma que se cumplan las siguientes condiciones:

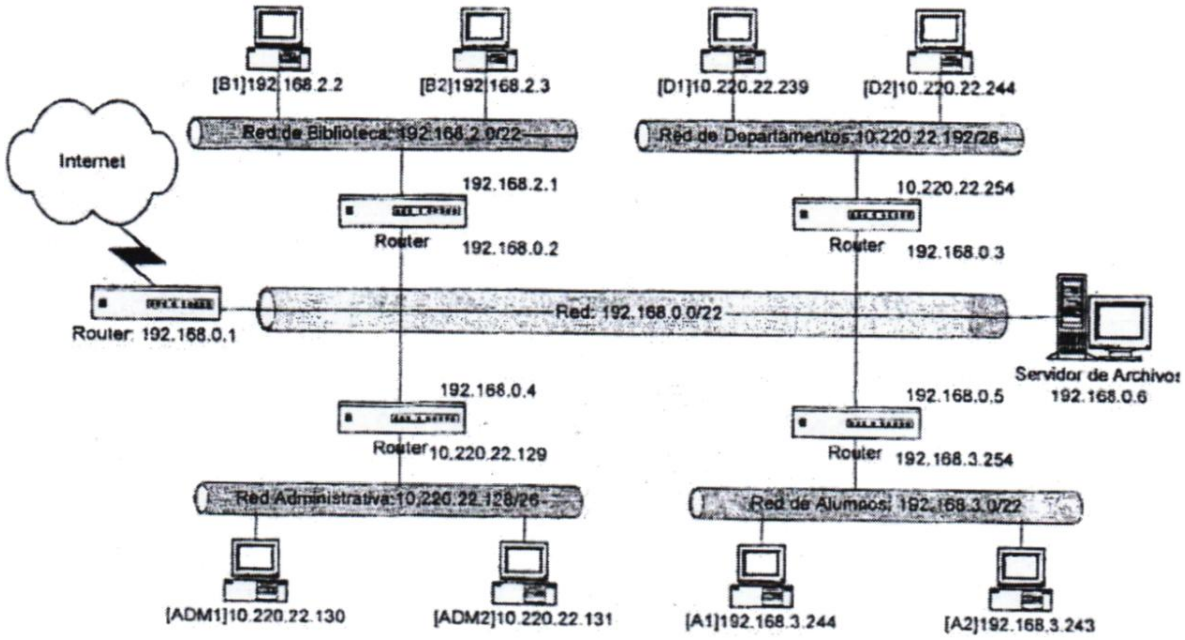
- Todos los equipos pueden acceder directamente sin proxy a Internet.
- Los equipos de la red 1 pueden conectar con el servidor S2.
- Los equipos de la red 3 pueden conectar con el servidor S3.
- Todos los equipos pueden conectar con el servidor S4.

Máquina	Ruta	Destino	Máscara	Pasarela	Interfaz
A1	red1	192.168.1.0	255.255.255.0	192.168.1.11	eth0
	default	0.0.0.0	0.0.0.0	192.168.1.1	eth0
S1	red1	192.168.1.0	255.255.255.0	192.168.1.1	eth0
	red2	192.168.2.0	255.255.255.0	192.168.2.1	eth1
	default	0.0.0.0	0.0.0.0	192.168.2.10	eth1
S2	red2	192.168.2.0	255.255.255.0	192.168.2.2	eth0
	red1	192.168.1.0	255.255.255.0	192.168.2.1	eth0
	default	0.0.0.0	0.0.0.0	192.168.2.10	eth0
S3	red2	192.168.2.0	255.255.255.0	192.168.2.3	eth0
	red3	192.168.3.0	255.255.255.0	192.168.2.5	eth0
	default	0.0.0.0	0.0.0.0	192.168.2.10	eth0
S4	red2	192.168.2.0	255.255.255.0	192.168.2.4	eth0

	red1	192.168.1.0	255.255.255.0	192.168.2.1	eth0
	red3	192.168.3.0	255.255.255.0	192.168.2.3	eth0
	default	0.0.0.0	0.0.0.0	192.168.2.10	eth0
S5	red2	192.168.2.0	255.255.255.0	192.168.2.5	eth1
	red3	192.168.3.0	255.255.255.0	192.168.3.1	eth0
	default	0.0.0.0	0.0.0.0	192.168.2.10	eth1
B1	red3	192.168.3.0	255.255.255.0	192.168.3.11	eth0
	default	0.0.0.0	0.0.0.0	192.168.3.1	eth0
R(router)	red2	192.168.2.0	255.255.255.0	192.168.2.10	eth0
	red1	192.168.1.0	255.255.255.0	192.168.2.1	eth0
	red3	192.168.3.0	255.255.255.0	192.168.2.3	eth0
	default	0.0.0.0	0.0.0.0	80.70.60.21	puerto

Ejercicio 18 – Examen oposiciones PES 2004

El siguiente esquema representa la red de un centro TIC:



Teniendo en cuenta las siguientes condiciones:

- Cada ordenador puede conectarse con su propia red.
- Todos los ordenadores tienen acceso a Internet y al servidor de archivos.
- Los ordenadores de la red de alumnos tienen acceso a la red de biblioteca y viceversa.
- Los ordenadores de la red de departamentos tienen acceso a la red administrativa y viceversa.

Calcular:

a) La máscara de red de la red departamentos, red de alumnos y red administrativa.

b) La tabla de encaminamiento de los equipos A1, B1, router de la red de alumnos y router de salida a Internet.

Nota: En las tablas de encaminamiento se debe especificar: máquina origen, dirección destino, máscara de red, pasarela (router) e interfaz (máquina origen).

Solución

a) La máscara de red de la red departamentos, red de alumnos y red administrativa.

Red departamentos:

La dirección de la red departamentos es 10.220.22.192/26. El /26 indica la máscara de red expresada en notación en diagonal o compacta. Eso significa que los primeros 26 bits de la máscara de red son "1" y el resto "0", por tanto, la máscara de red con notación punteada es la siguiente:

Máscara = 11111111.11111111.11111111.11000000 → 255.255.255.192

Red de alumnos:

En la dirección de red, la máscara se expresa como /22, así que:

Máscara = 11111111.11111111.11111100.00000000 → 255.255.252.0

Red administrativa:

En la dirección de red, la máscara se expresa como /26, así que:

Máscara = 11111111.11111111.11111111.11000000 → 255.255.255.192

b) La tabla de encaminamiento de los equipos A1, B1, router de la red de alumnos y router de salida a Internet.

Tabla de enrutamiento de A1:

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
192.168.3.0	255.255.252.0	192.168.3.254	192.168.3.224
192.168.0.0	255.255.252.0	192.168.3.254	192.168.3.224
192.168.2.0	255.255.252.0	192.168.3.254	192.168.3.224
0.0.0.0	0.0.0.0	192.168.3.254	192.168.3.224

Tabla de enrutamiento de B1:

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
192.168.2.0	255.255.252.0	192.168.2.1	192.168.2.2
192.168.0.0	255.255.252.0	192.168.2.1	192.168.2.2
192.168.3.0	255.255.252.0	192.168.2.1	192.168.2.2
0.0.0.0	0.0.0.0	192.168.2.1	192.168.2.2

Tabla de enrutamiento de R(Alumnos):

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
192.168.3.0	255.255.252.0	192.168.3.254	192.168.3.254
192.168.0.0	255.255.252.0	192.168.0.1	192.168.0.5
0.0.0.0	0.0.0.0	192.168.0.5	192.168.0.5

Tabla de enrutamiento de R(Internet):

Red destino	Máscara	Pasarela (siguiente salto)	Interfaz salida
192.168.0.0	255.255.252.0	192.168.0.1	192.168.0.1
192.168.2.0	255.255.252.0	192.168.0.2	192.168.0.1
192.168.3.0	255.255.252.0	192.168.0.5	192.168.0.1
10.220.22.128	255.255.255.192	192.168.0.4	192.168.0.1
10.220.22.192	255.255.255.192	192.168.0.3	192.168.0.1

Ejercicio 19 – Examen oposiciones PES 2018

Responda a las siguientes cuestiones:

a) Dibuje un diagrama de flujo que pueda explicar el algoritmo de encaminamiento IP.

b) Defina el concepto de tabla de enrutamiento y escriba un ejemplo sencillo de ello.

c) Describa brevemente los cuatro primeros niveles o capas (1 al 4) ISO (en inglés (OSI) en cuanto a los estándares que permiten la comunicación entre equipos.

d) Defina brevemente el funcionamiento de 3 topologías físicas diferentes para redes de área local y acompáñelo con una sencilla ilustración.

e) Si en una red de ordenadores tiene configurado el TCP/IP con la máscara de subred como 255.255.255.240

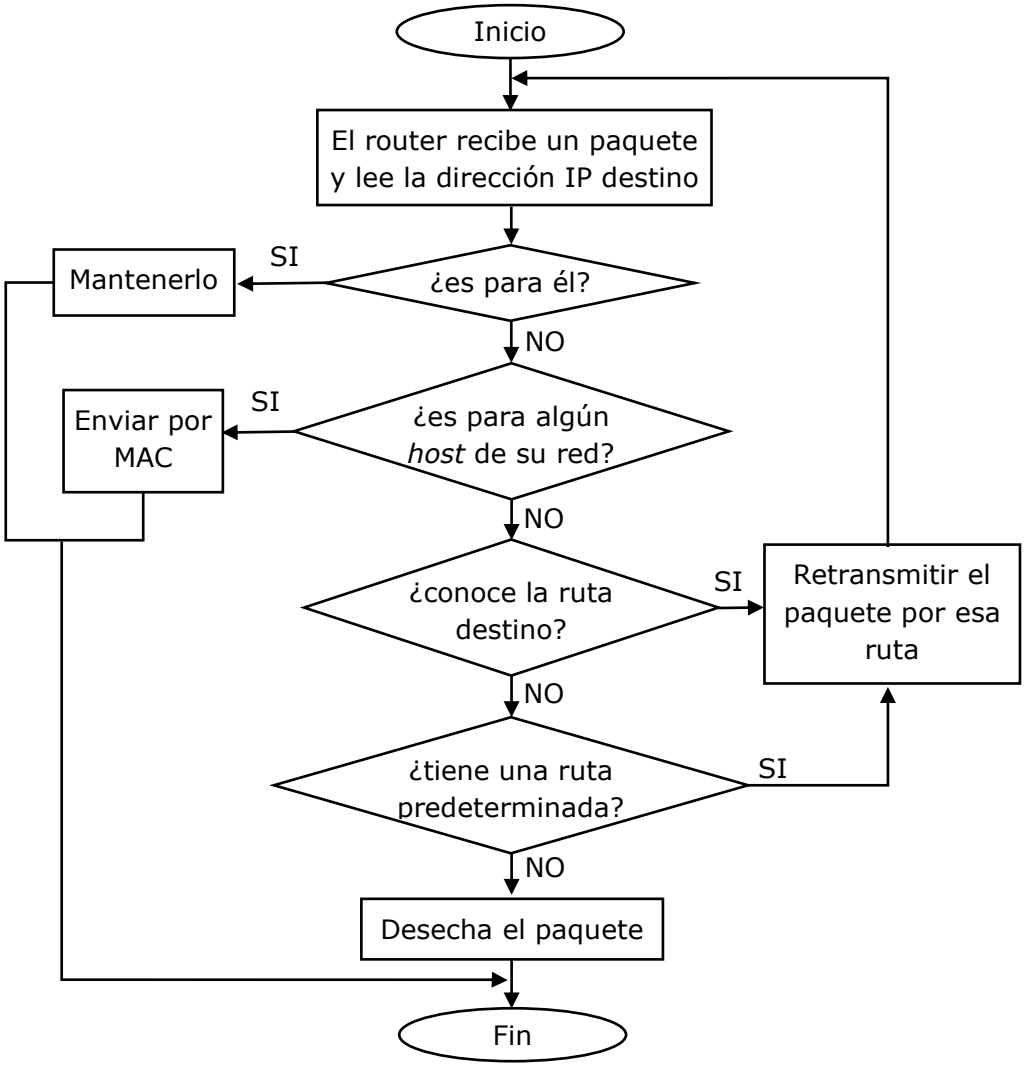
   1. ¿Cuántos ordenadores podrían conectarse?

   2. Si en dicha red, la puerta de enlace del router tiene como IP 192.168.0.1, escriba 7 direcciones IP que pudieran tener los equipos de dicha red.

f) Indique en qué posibles materias de ESO y Bachillerato podría encuadrarse el concepto de niveles OSI referenciado en el apartado c).

Solución

a) Dibuje un diagrama de flujo que pueda explicar el algoritmo de encaminamiento IP.



b) Defina el concepto de tabla de enrutamiento y escriba un ejemplo sencillo de ello.

Una tabla de enrutamiento es un archivo (se aloja en la RAM del *router*) que tiene registradas rutas o caminos a otras redes. Cada ruta debe contener como mínimo la dirección de la red destino, la dirección IP del siguiente salto (pasarela o puerta de enlace) y el coste de la ruta (distancia administrativa o métrica). De forma adicional, puede almacenar el puerto de salida por donde saldrá el paquete para llegar al siguiente salto. Ejemplo de tabla de enrutamiento:

Red destino	Máscara	Pasarela (Gateway)	Puerto salida	Coste
150.1.0.0	255.255.0.0	134.134.0.1	GigaByte0	20
150.2.0.0	255.255.0.0	123.43.5.2	Serial0	1
0.0.0.0	0.0.0.0	134.134.0.1	GigaByte0	20

Para hacer que el paquete llegue a la red 150.1.0.0, el router original lo retransmite al router con IP 134.134.0.1 a través del puerto GigaByte0. Una vez llegue al nuevo router, éste consultará su tabla de enrutamiento y lo retransmitirá de nuevo. La operación hasta llegar al destino o hasta agotar el tiempo de vida (TTL) del paquete.

La ruta con dirección 0.0.0.0 se llama ruta predeterminada y se redirigirán los paquetes por esta ruta cuando no se conoce ninguna ruta a la red destino.

c) Describa brevemente los cuatro primeros niveles o capas (1 al 4) ISO (en inglés (OSI) en cuanto a los estándares que permiten la comunicación entre equipos.

Capa 1 – Capa física

Este nivel se encarga de definir cómo se transmiten físicamente los bits de datos entre nodos. Esto incluye las características de las conexiones físicas (conectores, cables, antenas, etc.), así como la conversión entre distintas señales de datos (señales eléctricas, ópticas, ondas electromagnéticas, etc.).

Durante la transmisión pueden ocurrir efectos no deseados que alteran la calidad de la señal, contaminándola y modificándola, dando como resultado una señal distinta. La capa física dispone de mecanismos que lo evitan (trenzar los hilos, blindarlos, etc.) o lo corrigen (uso de ecualizadores, repetidores, etc.).

Capa 2 – Capa de enlace de datos

Este nivel se encarga de garantizar una transferencia libre de errores entre nodos que pertenecen al mismo dominio de difusión (misma red o subred) y ofrece servicios a las capas superiores.

La capa 2 recibe bloques de datos llamados paquetes de la capa 3 y le añade un encabezado y un tráiler formando una trama.

ENCABEZADO	PAQUETE	TRAILER

Esquema de una trama

En el encabezado se especifican, entre otras cosas, las direcciones físicas o MAC de los dispositivos origen y destino.

En el tráiler se especifica un código llamado CRC (*Cyclic Redundancy Check)*, que sirve para que el receptor compruebe si la trama recibida está libre de errores y, en caso de llegar corrupta, solicitar una retransmisión.

Otras funciones de este nivel son la de controlar el flujo de datos para evitar que el emisor transmita más tramas de las que el receptor puede asumir y la de controlar el acceso al medio para evitar la colisión de datos.

Capa 3 – Capa de red

Este nivel se encarga de definir cómo viajan los datos entre nodos que pertenecen a distintos dominios de difusión (distintas redes o subredes).

La capa 3 recibe bloques de datos de la capa 4 y le añade un encabezado formando un paquete.

ENCABEZADO	PDU DE LA CAPA 4

Esquema de un paquete

El contenido del encabezado varía según el protocolo que se utilice (IPv4, IPv6, etc.). En la mayoría de los casos se incluyen las direcciones IP de los dispositivos origen y destino

y el tiempo de vida o TTL (*Time To Live*), que indica la cantidad de saltos que puede dar un paquete entre *routers* antes de darse como perdido.

Capa 4 – Capa de transporte

Este nivel se encarga de dividir los bloques de datos que recibe del nivel 5 en fragmentos pequeños para facilitar su gestión y de multiplexar las conversaciones (datos que fluyen) a la aplicación correcta.

A cada fragmento le añade un encabezado formando un segmento si se usa protocolo TCP o datagrama si se usa UDP.

ENCABEZADO	PDU DE LA CAPA 5

Esquema de un segmento o datagrama

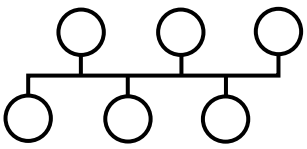
El contenido del encabezado varía según el protocolo utilizado, pero en todos los casos incluye el número de puerto origen y destino, que indican la aplicación con la que debe de reproducirse. Por ejemplo, si el puerto es 25 se trata de una petición SMTP (correo electrónico) y si es 443 se trata de una petición HTTPS (página web).

El protocolo TCP se usa para transmitir archivos, ya que los segmentos tienen que reensamblarse en el orden correcto cuando llegan al receptor.

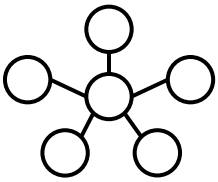
El protocolo UDP se usa en transmisiones donde la pérdida de un datagrama no afecta de forma sensible a las comunicaciones y se puede asumir su pérdida. Por ejemplo, en transmisiones de vídeo en *streaming* o llamadas de voz por VoIP.

d) Defina brevemente el funcionamiento de 3 topologías físicas diferentes para redes de área local y acompáñelo con una sencilla ilustración.

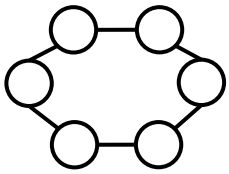
En bus: Todos los nodos de la red se conectan a un único canal de comunicaciones llamado bus troncal o *backbone*. Como los nodos comparten el mismo canal, la red puede saturarse y se puede producir una degradación de la señal.



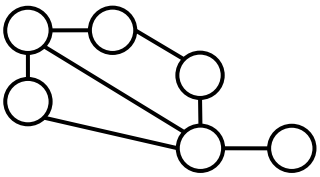
En estrella: Todos los *hosts* se conectan a un nodo central, por ejemplo, un *switch* o *router*, que será el encargado de gestionar todas las comunicaciones. Esta topología es la más común en redes de área local o LAN.



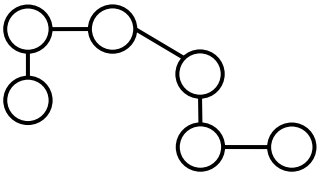
En anillo: Cada nodo se conecta directamente a los 2 nodos adyacentes, formando una única ruta de comunicaciones en forma de anillo. En esta topología, un nodo defectuoso puede crear problemas en toda la red.



En malla: Cada nodo está conectado a uno o varios nodos, pudiendo existir varios canales de comunicación entre 2 nodos. Si todos los nodos están conectados entre sí, se llama topología en malla completa.



En árbol: Cada nodo está conectado a uno o varios nodos, pero solo existe un único canal de comunicaciones entre 2 nodos. Al no tener redundancias en las conexiones, es más sencillo y barato de implementar que la topología en malla, pero es menos fiable ya que un fallo en un nodo puede provocar problemas en toda la red.



e) Si en una red de ordenadores tiene configurado el TCP/IP con la máscara de subred como 255.255.255.240

1. ¿Cuántos ordenadores podrían conectarse?

Máscara = 255.255.255.240 → 11111111.11111111.11111111.11110000

Red Hosts

4 bits son para *hosts*, por lo que pueden conectarse 2^4 - 2 = **14 ordenadores** (se restan 2 porque una dirección es para identificar la red y otra para la dirección de difusión o *broadcast*)

2. Si en dicha red, la puerta de enlace del router tiene como IP 192.168.0.1, escriba 7 direcciones IP que pudieran tener los equipos de dicha red.

192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7 y 192.168.0.8

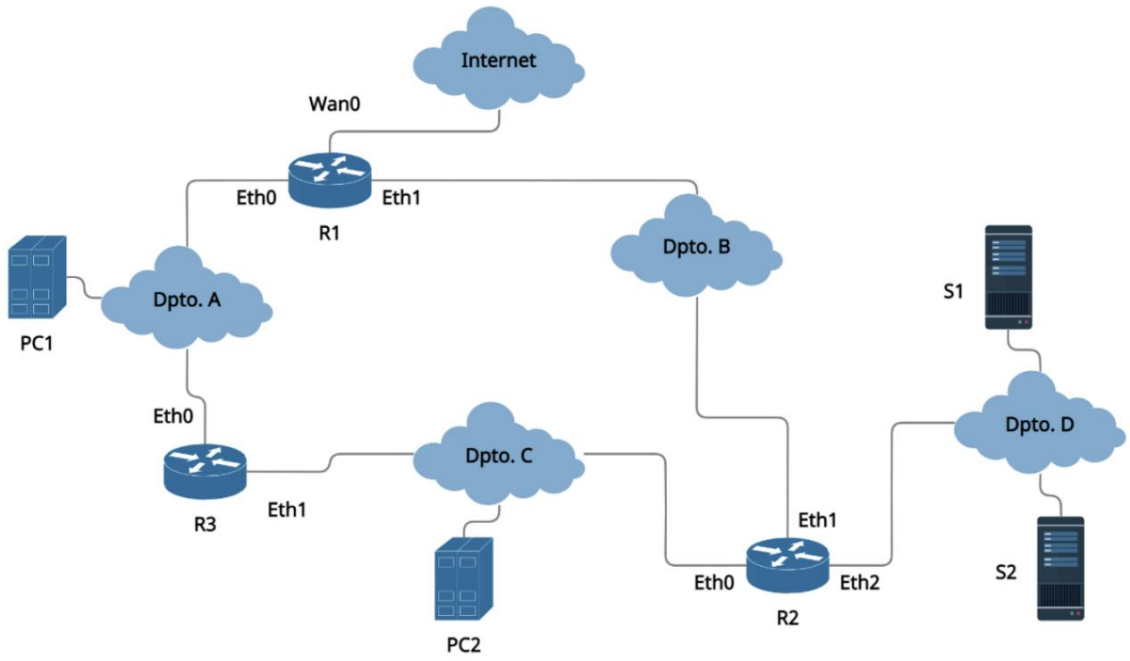
f) Indique en qué posibles materias de Educación Secundaria Obligatoria y Bachillerato, podría encuadrarse el concepto de niveles OSI referenciado en el apartado c) de este ejercicio.

En Tecnologías la Información y Comunicación I (1º de Bachillerato)

Ejercicio 20 – Examen oposiciones SAI 2021

Una empresa de ingeniería presenta la topología de red que se puede visualizar a continuación. Dispone de 4 departamentos (Dpto. A, B, C y D). El departamento A debe ser capaz de proporcionar servicio a 2000 hosts. El departamento B y C deben de ser capaces de proporcionar servicio a 1000 hosts cada uno. El departamento D debe de ser capaz de proporcionar servicio a 50 hosts. Debe definir el direccionamiento IP de la subred teniendo en cuenta las siguientes instrucciones:

- Se nos indica que la dirección IP del Eth0 del R1 es 172.22.0.1
- Debe usar la técnica subnetting VLSM teniendo en cuenta que se quiere segmentar la red 172.22.0.0/16
- Las IPs de la red "Dpto. A" son las de inferior valor (números más pequeños), a continuación, deben ir las IPs de la red "Dpto. B", posteriormente las del "Dpto. C" y finalmente las direcciones IP del "Dpto. D" deben de ser las de mayor valor numérico. Direcciones IP: Dpto A < Dpto B < Dpto C < Dpto D
- Las IPs de los interfaces de los routers deben ser las de menor valor numérico.
- Mientras no se indique lo contrario se responderá siempre con IPv4
- R1, R2 y R3 son enrutadores



1. ¿Cuál es la máscara de subred del Eth0 del R1?
   a) /21
   b) /22
   c) /23
   d) Ninguna de las anteriores

2. ¿Cuál es la dirección de broadcast de la subred del Dpto. A?
   a) 172.22.5.255
   b) 172.22.6.255
   c) 172.22.7.255
   d) Ninguna de las anteriores

3. Indique la primera IPv4 válida para host de la subred del Dpto. B e indique su formato en IPv6.
    a) 172.22.6.1 o 0:0:0:ffff:ad16:0601
    b) 172.22.7.1 o ::ffff:ac16:0701
    c) 172.22.8.1 o 0000:0000:0000:ffff:ac16:0801
    d) Ninguna de las anteriores

4. Si el PC2 dispone de la última IP válida para host de la subred del Dpto. C, ¿Cuál sería esa IP y su máscara de red en formato CIDR?
    a) 172.22.13.254/255.255.252.0
    b) 172.22.14.254/23
    c) 172.22.15.254/22
    d) Ninguna de las anteriores

5. Si el S2 dispone de la última IP válida para host de la subred del Dpto. D, ¿Cuál sería esa IP y su máscara de red?
    a) 172.22.16.62/255.255.255.192
    b) 172.22.16.63/255.255.255.192
    c) 172.22.17.62/255.255.255.128
    d) Ninguna de las anteriores

6. Si en el servidor S1 requiere usar protocolos/servicios para compartir archivos en red, ¿cuál es la respuesta correcta?
    a) Se puede optar por usar CIFS
    b) Se puede optar por usar NFS
    c) Las dos respuestas anteriores son correctas
    d) Ninguna de las anteriores

7. Le solicitan un cable par trenzado usando TIA-568A, ¿cuál es el orden de los colores estándares desde el pin 1 hasta el pin 8 del conector RJ45)?
    a) BV-V-BN-A-BA-N-BM-M (B=blanco N=naranja A=azul V=verde M=marrón)
    b) BN-N-BV-A-BA-V-BM-M (B=blanco N=naranja A=azul V=verde M=marrón)
    c) BN-N-BA-V-BV-A-BM-M (B=blanco N=naranja A=azul V=verde M=marrón)
    d) Ninguna de las anteriores

8. El administrador de la red le solicita que aumente la eficiencia de transferencia de los archivos del servidor NAS a través de la habilitación de _____ en el switch, de manera que mejore la eficiencia en la transmisión de los datos de archivos grandes destinados al backup.
    a) Jumbo Frame
    b) Spanning Tree Protocol
    c) IGMP Snooping con una MTU superior a 1500 bytes
    d) Ninguna de las anteriores

9. Si el PC1, de la subred planteada en el gráfico anterior, quisiera averiguar la dirección física MAC del PC2, ¿qué procedimiento sería el correcto usando una consola de Debian/Ubuntu?
    a) Realizaría un ping a PC2 y posteriormente ejecutaría "arp -a" para averiguar la MAC del PC2
    b) Realizaría un ping a PC2 y posteriormente ejecutaría "arp -g" para averiguar la MAC del PC2

c) Las respuestas anteriores, a y b, son correctas
d) Ninguna de las anteriores

10. ¿Qué afirmación es cierta sobre bonding LACP?
    a) LACP(802.3ad) y su sigla significa "Link Aggregation Control Protocol"
    b) LACP(802.16ac) es similar a PAgP de Cisco
    c) LACP(802.20) y se utiliza para la agregación de enlaces
    d) Ninguna de las anteriores

Solución

1. ¿Cuál es la máscara de subred del Eth0 del R1?

La interfaz Eth0 de R1 se encuentra en la red "Dpto. A", por lo que hay que obtener la máscara de dicha subred. Como la red "Dpto. A" debe de dar servicio a 2000 *hosts*, necesitamos 11 bits (2^{11}-2=2048≥2000) para asignar a *hosts*. Si 11 bits son para *hosts*, los 21 bits restantes (32-11) son para indicar la subred (máscara de subred).

Máscara = 11111111.11111111.11111000.00000000 → 255.255.248.0
(Red: 11111111.11111111 — Subred: 11111 — Hosts: 000.00000000)

La respuesta es a) /21

2. ¿Cuál es la dirección de broadcast de la subred del Dpto. A?

Espacio de direcciones que se nos da → 172.22.0.0/16

Dirección subred "Dpto A"→ 172.22.00000000.00000000 → 172.22.0.0/21
Dirección de *broadcast* → 172.22.00000111.11111111 → 172.22.7.255

La respuesta es c) 172.22.7.55

3. Indique la primera IPv4 válida para host de la subred del Dpto. B e indique su formato en IPv6

En el apartado se menciona que las IPs de valor inferior son para la red "Dpto. A" y después van las de la red "Dpto. B", por tanto, si la última dirección de la subred "Dpto. A" es 172.22.7.255, la siguiente (172.22.8.0) es la dirección de la red "Dpto. B" y la que viene a continuación (172.22.8.1) es la primera válida.

La respuesta es c) 172.22.8.1 o 0000:0000:0000:ffff:ac16:0801

4. Si el PC2 dispone de la última IP válida para host de la subred del Dpto. C, ¿Cuál sería esa IP y su máscara de red en formato CIDR?

Como la red "Dpto. B" y "Dpto. C" deben dar servicio a 1000 *hosts*, necesitamos 10 bits (2^{10}-2=1022≥1000) para asignar a *hosts*. Si 10 bits son para *hosts*, los 22 bits restantes (32-10) son para indicar la subred (máscara de subred).

De ahí obtenemos lo siguiente:

Dirección subred "Dpto B" → 172.22.00001000.00000000 → 172.22.8.0/22
Dirección subred "Dpto C" → 172.22.00001100.00000000 → 172.22.12.0/22
IP último *host* "Dpto C" → 172.22.00001111.11111110 → 172.22.15.254/22

El formato CIDR es el formato compacto /22, no se debe confundir con el formato punteado 255.255.252.0

La respuesta es c) 172.22.15.254/22

5. Si el S2 dispone de la última IP válida para host de la subred del Dpto. D, ¿Cuál sería esa IP y su máscara de red?

El "Dpto. D" debe dar servicio a 50 *hosts*, por lo que necesita 6 bits (2^6-2=62≥50) para asignar a *hosts*. Si 6 bits son para *hosts*, los 26 bits restantes (32-6) son para indicar la subred (máscara de subred), que en formato punteado es:

Máscara de subred = 11111111.11111111.11111111.11000000 → 255.255.255.192

Dirección subred "Dpto D" → 172.22.00010000.00000000 → 172.22.16.0/26
IP último *host* "Dpto D" → 172.22.00010000.00111110 → 172.22.16.62

La respuesta es a) 172.22.16.62/255.255.255.192

6. Si en el servidor S1 requiere usar protocolos/servicios para compartir archivos en red, ¿cuál es la respuesta correcta?

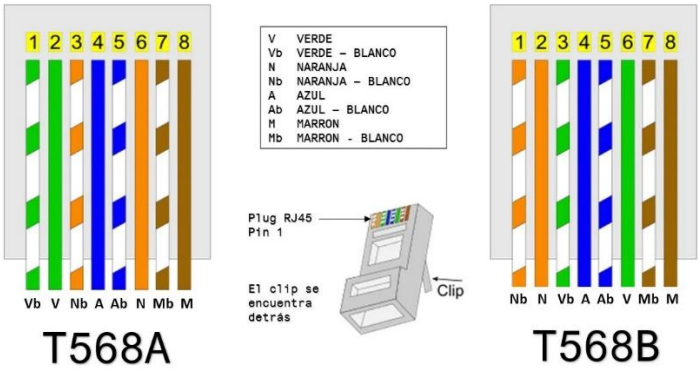
CIFS es un protocolo de red que permite compartir archivos, impresoras, etc. entre nodos en una red de computadoras, mientras que NFS es un protocolo que posibilita que distintos sistemas conectados a la misma red accedan a ficheros como si se trataran de archivos locales.

Aunque el protocolo CIFS tiene más desventajas y no se recomienda su uso, ambos permiten compartir archivos en red, por lo que los 2 son válidos.

La respuesta es c) Las dos respuestas anteriores son correctas

7. Le solicitan un cable par trenzado usando TIA-568A, ¿cuál es el orden de los colores estándares desde el pin 1 hasta el pin 8 del conector RJ45 (B=blanco N=naranja A=azul V=verde M=marrón)?

En la siguiente imagen se puede ver cómo han de ir ordenados los cables.



La respuesta es a) BV-V-BN-A-BA-N-BM-M

8. El administrador de la red le solicita que aumente la eficiencia de transferencia de los archivos del servidor NAS a través de la habilitación de _____ en el switch, de manera que mejore la eficiencia en la transmisión de los datos de archivos grandes destinados al backup.

Jumbo Frame es una función soportada por las tarjetas de red y los *switches* que se diseñó específicamente para las redes Gigabit que requerían de paquetes de información superiores en tamaño. Gracias a los Jumbo Frame podemos hacer un mejor uso de nuestras redes Gigabit, aumentando la efectividad de sus transferencias un 50%-100%.

Spanning Tree Protocol o STP es un protocolo de capa 2 del modelo OSI que gestiona la presencia de bucles en la red debido a la existencia de enlaces redundantes. STP permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

IGMP *snooping* consiste en escuchar el tráfico producido por el protocolo de red IGMP. Esta característica permite a los conmutadores de red escuchar la conversación que se produce entre los *routers* y los *hosts*.

La respuesta es a) Jumbo Frame

9. Si el PC1, de la subred planteada en el gráfico anterior, quisiera averiguar la dirección física MAC del PC2, ¿qué procedimiento sería el correcto usando una consola de Debian/Ubuntu?

Vamos a analizar qué es lo que hacen los apartado a) y b):

Realizando un ping a PC2, enviaríamos un paquete a la red "Dpto. C" y, en caso de que R3 no supiera la MAC de PC2, mandaría un mensaje "ARP *request*" a difusión para averígualo, es decir, se añade la MAC de PC2 en la caché ARP de R3 si no está de antes.

Los comandos "arp -a" y "arp -g" hacen lo mismo: enumeran todos los dispositivos que hay en la caché ARP del *host*, en este caso, de PC1, pero PC1 no tiene la MAC de PC2, ya que el ping anterior añadió la MAC de PC2 en la caché ARP de R3, pero no de PC1.

Por tanto, ni el apartado a) ni el b) nos permite conocer la MAC de PC2 desde PC1.

Otra forma de llegar a esa conclusión es que PC1 y PC2 están en subredes distintas y las tablas ARP almacenan las direcciones MAC de los *hosts* que están en su misma red. Si PC1 y PC2 están en subredes distintas, jamás podrán conocer su MAC entre ellos.

La respuesta es d) Ninguna de las anteriores

10. ¿Qué afirmación es cierta sobre bonding LACP?

LACP (*Link Aggregation Control Protocol*) o IEEE 802.3ad se encarga de agregar enlaces físicos de forma eficiente.

La respuesta es a) LACP(802.3ad) y su sigla significa "Link Aggregation Control Protocol"

Ejercicio 21 – Examen oposiciones PES 2021

1. Dada la siguiente red 192.168.1.80/28 responda razonadamente las siguientes cuestiones:

    a) ¿Cuántas direcciones ip válidas para equipos hay disponibles?

    b) ¿Cuál es la dirección de la red?

    c) ¿Cuál es la dirección de *broadcast*?

    d) ¿Cuál es la máscara de la red en notación decimal?

    e) ¿Pertenece la dirección 192.168.1.83 a esta red?

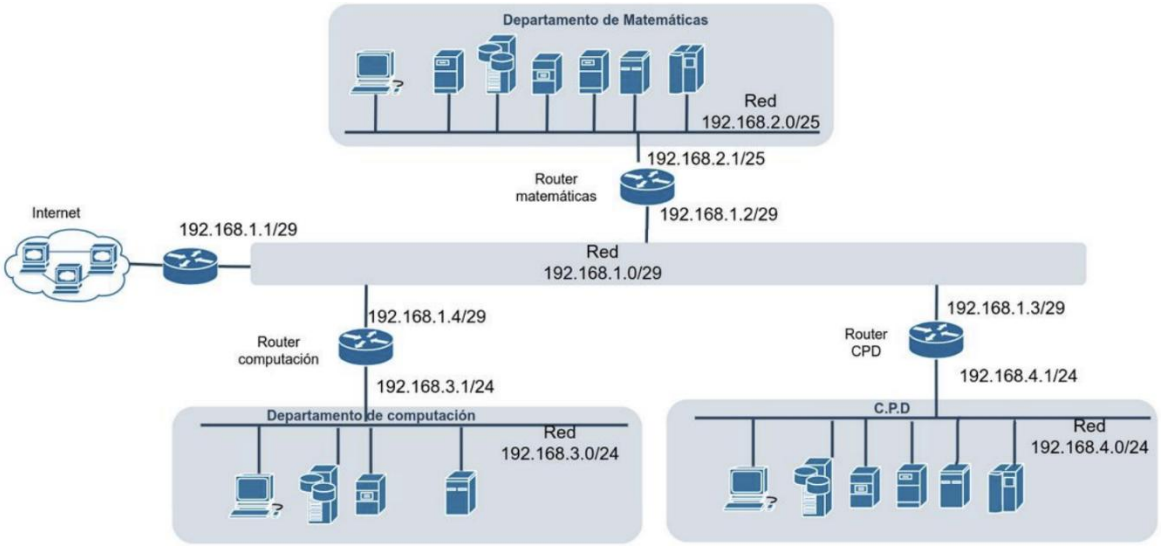
    f) ¿Pertenece la dirección 192.168.1.112 a esta red?

    g) ¿Cuál es la máscara de la red por defecto (en notación decimal y simplificada) de la IP 10.10.4.5?

    h) ¿Para qué se utiliza una dirección de enlace local?

    i) ¿Cuál sería la dirección ipv6 de la interfaz de enlace local si la MAC de nuestra tarjeta es 82:f9:a5:ff:bb:a4 y utilizamos SLAAC y EUI-64?

2. Dada la siguiente estructura de red, especificar la tabla de encaminamiento de los cuatro routers existentes. Se debe especificar la dirección de red de destino, máscara de red de destino, la ip siguiente salto y la ip de la interfaz por la que envía el paquete.



Se debe de tener en cuenta que el enrutamiento y la configuración del cortafuegos de la red están configurados de forma adecuada para cumplir los siguientes requerimientos:

- Cada ordenador puede conectarse con su red
- Todos los equipos pueden conectarse con Internet menos los del CPD que no tienen acceso a Internet.
- Todos los equipos pueden conectarse con el CPD
- El departamento de matemáticas no puede conectarse con el departamento de computación.

Solución

Apartado 1:

a) ¿Cuántas direcciones IP válidas para equipos hay disponibles?

La máscara de subred es /28, lo que nos indica que los primeros 28 bits de la dirección IP identifican a la red y los 4 restantes (32-28) sirven para asignar a *hosts*. Por tanto, hay disponibles 2^4 - 2 = 16 - 2 = **14** direcciones IP válidas (se quitan 2 porque la primera se reserva a la dirección de red y la última a la dirección de *broadcast*).

b) ¿Cuál es la dirección de la red?

Los primeros 28 bits los dejamos igual y los 4 últimos los ponemos a 0.

Dirección IP → 192.168.1.80 → 11000000.10101000.00000001.01010000

Igual Cero

Dirección de red → 11000000.10101000.00000001.01010000 → **192.168.1.80**

c) ¿Cuál es la dirección de *broadcast*?

La dirección de *broadcast* es la última que se puede asignar en esa red, por lo que tenemos que poner a 1 los 4 últimos bits.

Dirección de *broadcast* → 11000000.10101000.00000001.01011111 → **192.168.1.95**

d) ¿Cuál es la máscara de la red en notación decimal?

/28 quiere decir que los primeros 28 bits de la máscara están a 1 y el resto a 0

Máscara de subred → 11111111.11111111.11111111.11110000 → **255.255.255.240**

e) ¿Pertenece la dirección 192.168.1.83 a esta red?

Sí. Todas las direcciones del rango 192.168.1.81 a 192.168.1.94 pertenecen a esa red.

f) ¿Pertenece la dirección 192.168.1.112 a esta red?

No. La dirección es superior a la de *broadcast*, que es la última dirección de esta red.

g) ¿Cuál es la máscara de la red por defecto (en notación decimal y simplificada) de la IP 10.10.4.5?

La dirección IP 10.10.4.5 es de clase A ya que el primer octeto está entre 0 y 127. La máscara de red por defecto de las direcciones IP de clase A es **255.0.0.0** (notación decimal) o /8 (simplificada)

h) ¿Para qué se utiliza una dirección de enlace local?

Las direcciones de enlace local o *link-local* solo sirven para trabajar dentro de una red local (no se puede enrutar). Las asigna el sistema operativo por medio de APIPA cuando un servidor DHCP no puede asignarle una IP al *host* de forma dinámica.

i) ¿Cuál sería la dirección ipv6 de la interfaz de enlace local si la MAC de nuestra tarjeta es 82:f9:a5:ff:bb:a4 y utilizamos SLAAC y EUI-64?

Para convertir una MAC a dirección de *link-local* ipv6, hay que seguir los siguientes pasos:

1- Convertir el primer octeto de hexadecimal a binario: $82_{(16}$ → $10000010_{(2}$

2- Invertimos el séptimo bit: 10000000

3- Convertimos el octeto de binario a hexadecimal: $10000000_{(2}$ → $80_{(16}$

4- Reemplazamos el primer octeto por el obtenido: 80:f9:a5:ff:bb:a4

5- Agregamos ff:fe en la mitad de la MAC: 80:f9:a5:ff:fe:ff:bb:a4

6- Agregamos fe80:: al inicio de la dirección: fe80::80:f9:a5:ff:fe:ff:bb:a4

7- Agrupamos y listo: fe80::80f9:a5ff:feff:bba4

Apartado 2:

Tabla de enrutamiento del router matemáticas

Red destino	Máscara	Pasarela (siguiente salto)	IP interfaz salida
192.168.2.0	255.255.255.128	192.168.2.1	192.168.2.1 (Ge0)
192.168.1.0	255.255.255.248	192.168.1.2	192.168.1.2 (Ge1)
192.168.3.0	255.255.255.0	192.168.2.1	192.168.2.1 (Ge0)
192.168.4.0	255.255.255.0	192.168.1.3	192.168.1.2 (Ge1)
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.2 (Ge1)

Cosas a tener en cuenta:

- La salida a Internet la obtiene por la ruta predeterminada (0.0.0.0).
- En la columna "IP interfaz salida" se ha puesto entre paréntesis el puerto físico de salida Ge (GigabitEthernet) porque es así como viene en las tablas de enrutamiento reales.
- Para bloquear la conexión con el departamento de computación (192.168.3.0/24), se ha añadido una ruta para que se envíe el paquete así mismo hasta agotar el TTL.

Tabla de enrutamiento del router computación

No dice si computación puede conectarse con matemáticas, pero como sí se indica que matemáticas no puede comunicarse con computación, suponemos que éste tampoco.

Red destino	Máscara	Pasarela (siguiente salto)	IP interfaz salida
192.168.3.0	255.255.255.0	192.168.3.1	192.168.3.1 (Ge0)
192.168.1.0	255.255.255.248	192.168.1.4	192.168.1.4 (Ge1)
192.168.2.0	255.255.255.128	192.168.3.1	192.168.3.1 (Ge0)
192.168.4.0	255.255.255.0	192.168.1.3	192.168.1.4 (Ge1)
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.4 (Ge1)

Tabla de enrutamiento del router CPD

Red destino	Máscara	Pasarela (siguiente salto)	IP interfaz salida
192.168.4.0	255.255.255.0	192.168.4.1	192.168.4.1 (Ge0)
192.168.1.0	255.255.255.248	192.168.1.3	192.168.1.3 (Ge1)
192.168.2.0	255.255.255.128	192.168.1.2	192.168.1.3 (Ge1)
192.168.3.0	255.255.255.0	192.168.1.4	192.168.1.3 (Ge1)
0.0.0.0	0.0.0.0	192.168.4.1	192.168.4.1 (Ge0)

Para que el router CPD no tenga salida a Internet, se ha puesto la red CPD como ruta predeterminada, para que se envíe los paquetes así mismo hasta agotar el TTL. Otra forma de hacerlo es eliminar la ruta predeterminada.

Tabla de enrutamiento del router que da salida a Internet

Red destino	Máscara	Pasarela (siguiente salto)	IP interfaz salida
192.168.1.0	255.255.255.248	192.168.1.1	192.168.1.1 (Ge0)
192.168.2.0	255.255.255.128	192.168.1.2	192.168.1.1 (Ge0)
192.168.3.0	255.255.255.0	192.168.1.4	192.168.1.1 (Ge0)
0.0.0.0	0.0.0.0	Internet	Internet (Serial0)

Como no se indica la dirección IP del siguiente salto ni de la interfaz de salida que conecta con Internet, se ha puesto simplemente “Internet”.