



Tema 3: Capa de Red

1ª PARTE: Generalidades sobre IPv4

Redes de Computadores
Grado en Ingeniería Informática

Mercedes Rodríguez García

Índice

1. Funciones de la capa de red
2. Dispositivos de la capa de red
3. Protocolos de la capa de red
4. IPv4: Formato del datagrama
5. IPv4: asignación de direcciones
 - 5.1. Asignación estática
 - 5.2. Asignación dinámica
6. IPv4: direcciones privadas / direcciones públicas
7. IPv4: Tipos de comunicaciones
 - 7.1. Broadcast dirigido
 - 7.2. Broadcast limitado
 - 7.3. Multicast
8. IPv4: Direcciones reservadas
 - 8.1. Dirección loopback
 - 8.2. Dirección de ruta predeterminada
 - 8.3. Dirección Link-Local

1. Funciones de la capa de red

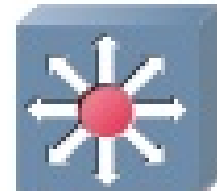
Funciones principales

- Direccionamiento lógico.
- Encapsular segmentos en paquetes.
- Establecer comunicación con otras redes.
- Enrutar paquetes.

2. Dispositivos de la capa de red



Router



Switch de capa 3
(también conocido como switch multicapa)

3. Protocolos de la capa de red



4. IPv4: Formato del datagrama

7. Aplicación

6. Presentación

5. Sesión

4. Transporte

3. Red

2. Enlace de datos

1. Física

El datagrama (paquete) tiene dos partes:

- **Encabezado**
- **Datos:** generalmente es la PDU de capa 4, pero no siempre es así, por ejemplo, podría ser un mensaje ICMP (este mensaje se genera en la capa 3).

PDU de capa 4: segmento

SEGMENTO



PDU de capa 3: paquete

Encabezado

DATOS



PDU de capa 2: trama

Encabezado

PAQUETE

Tráiler

4. IPv4: Formato del datagrama

**ENCABEZADO
del datagrama
(20 bytes)**



* Generalmente es la PDU de capa 4 (segmento), pero no siempre es así, por ejemplo, podría ser un mensaje ICMP (este mensaje se genera en la capa 3).

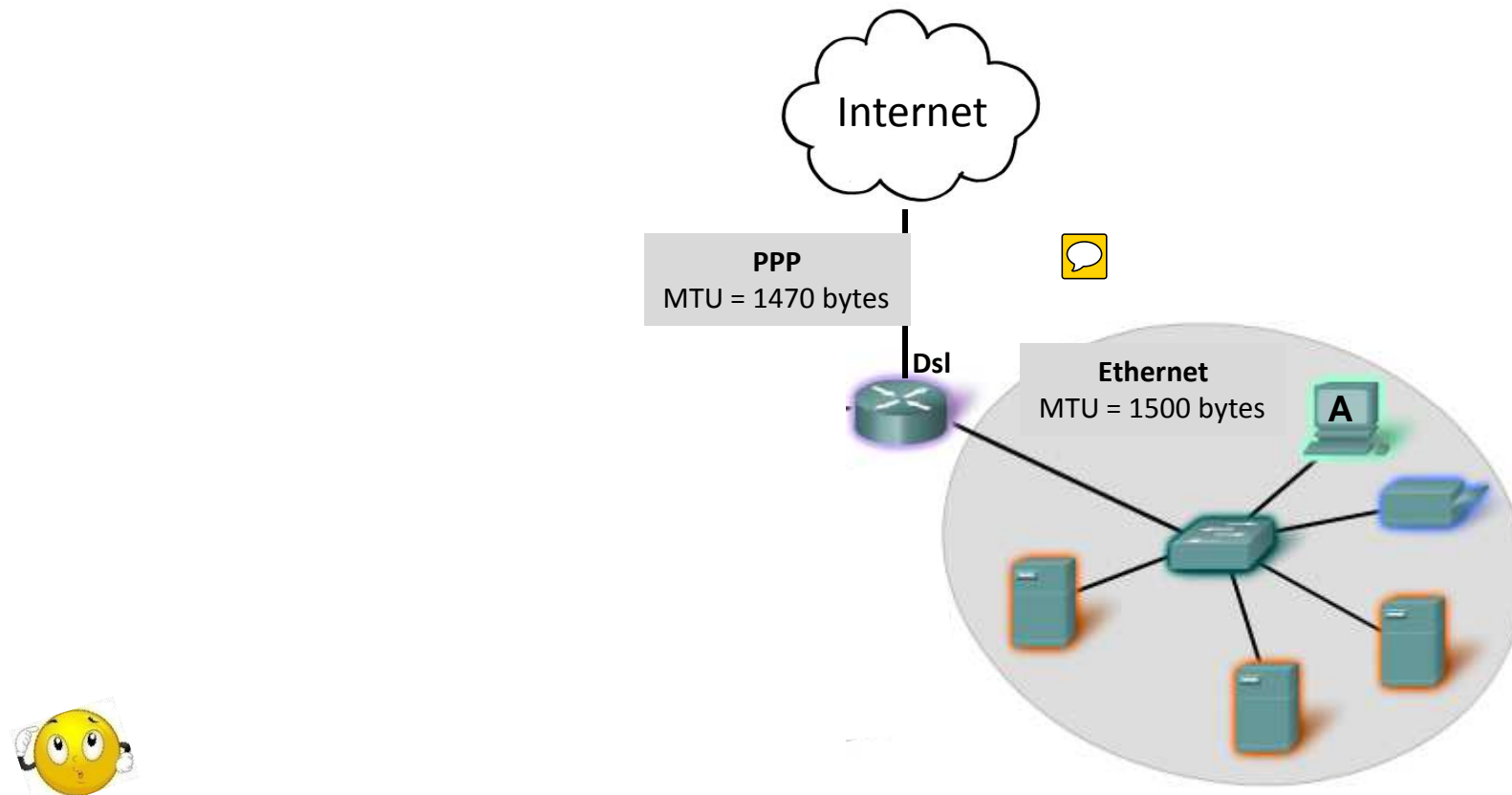
4. IPv4: Formato del datagrama

La capa de red opera independientemente de la tecnología de red. Esto significa que el transporte de paquetes IP no está limitado a una tecnología en particular (por ejemplo, los paquetes pueden circular por Wi-Fi, Ethernet o ATM indistintamente).

Es responsabilidad de la capa de enlace, tomar un paquete y prepararlo para su transmisión por una tecnología específica.

No obstante, existe una característica de la capa de enlace que sí tiene que tener en cuenta la capa de red, ésta es la Unidad Máxima de Transferencia (**MTU**). El tamaño de los paquetes nunca debe superar la MTU establecida por la capa de enlace.

4. IPv4: Formato del datagrama



Si en este ejemplo el PC A envía un datagrama de 1490 bytes a un servidor de Internet, ¿qué debería hacer el router?

4. IPv4: Formato del datagrama

Un router se ve obligado a fragmentar un paquete cuando éste va a pasar a una tecnología de red que tiene una MTU menor.

Señalizador de No Fragmentar (DF)

¿Está permitido fragmentar?

Si DF = 1, NO se permite fragmentar el paquete. Si un router necesitara fragmentarlo, no podría y tendría que descartar ese paquete.

Si DF = 0, SÍ se permite fragmentar el paquete.

Desplazamiento de fragmentos (Desp)

¿Qué lugar ocupa el fragmento dentro del paquete?

Cuando se produce una fragmentación, el host destino utiliza los campos Desp y MF para reconstruir el paquete. El campo Desp identifica el orden en el que ha de situarse ese fragmento durante la reconstrucción del paquete.

Señalizador de Más Fragmentos (MF)

¿Es el último fragmento del paquete?

Si MF = 1, NO es el último fragmento del paquete.

Si MF = 0 y Desp \neq 0, SÍ es el último fragmento del paquete.

Si MF = 0 y Desp = 0 significa que es un paquete **NO fragmentado**.

4. IPv4: Formato del datagrama

Tipo de servicio (Calidad de Servicio -QoS-)

Define la prioridad del paquete. El router puede ser configurado para enviar en primer lugar los paquetes que tengan mayor prioridad.

Protocolo

Indica el tipo de mensaje que contiene el campo datos del datagrama. Por ejemplo:

Si protocolo = 1 → datos = mensaje ICMP

Si protocolo = 6 → datos = segmento TCP

Si protocolo = 17 → datos = segmento UDP

Tiempo de vida (TTL) -8 bits-

Indica el número máximo de saltos que puede dar un paquete. Si el TTL es 64, significa que como máximo podrá dar 64 saltos. Cada vez que el paquete da un salto, es decir, que pasa por un router, el TTL se decrementa en una unidad. Si el TTL llega a valer 0 en un salto, ese router quitará el paquete de circulación. Este mecanismo sirve para **evitar que los paquetes circulen indefinidamente** por las redes cuando no encuentran el destino.

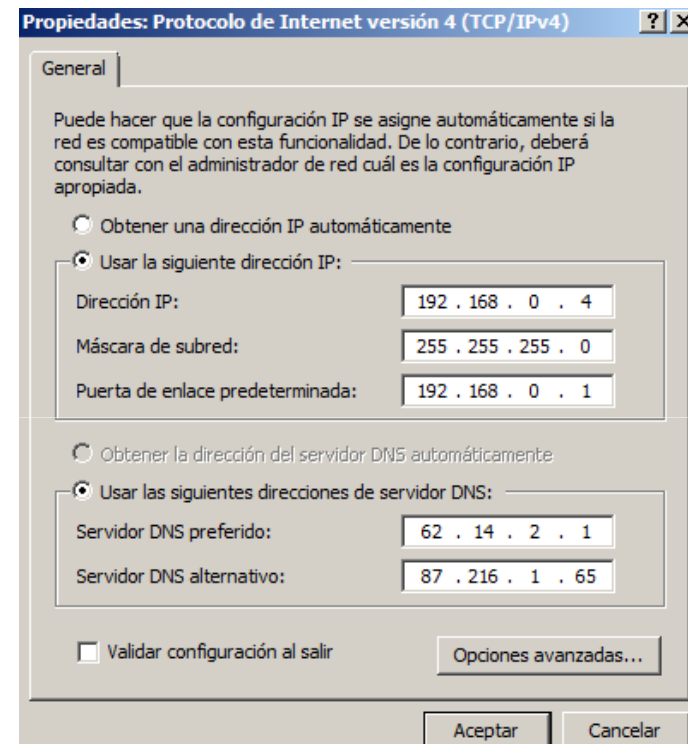
5. IPv4: asignación de direcciones

5.1. Asignación estática

Es el administrador de red el que configura manualmente el host. Debe introducir los siguientes datos: dirección IP, máscara, puerta de enlace y servidores DNS.

Es recomendable, incluso necesario, realizar asignación estática en:

- Impresoras de red,
- Servidores y
- Cualquier dispositivo de red que requiera una dirección fija.



-Configuración que hay que aplicar al host-

Listado de servidores DNS:

<http://www.adslayuda.com/dns.html>

<http://bandaancha.eu/analizador-dns>

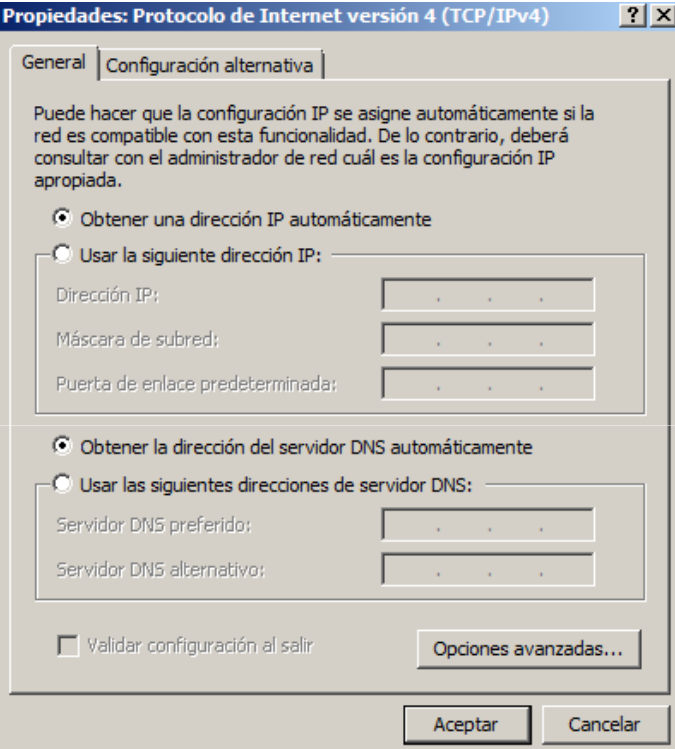
5. IPv4: asignación de direcciones

5.2. Asignación dinámica

Es el servidor DHCP (Dynamic Host Configuration Protocol) el que configura automáticamente los hosts de la red. El servidor se puede configurar para que asigne los siguientes datos: dirección IP, máscara, puerta de enlace y servidores DNS.

DHCP SERVER CONFIGURATION	
Starting IP Address:	192.168.1.10
End IP Address :	192.168.1.50
Subnet mask :	255.255.255.0
Gateway :	192.168.1.1
Primary DNS :	87.216.1.65
Secondary DNS :	87.216.1.66

-Servidor DHCP. ¿Qué dispositivo de la red puede funcionar como servidor DHCP? el router (la mayoría de los routers contienen un servidor DHCP) o cualquier equipo de la red que tenga instalado este servicio-



-Configuración que hay que aplicar al host-

En el servidor DHCP, hay que definir el bloque de direcciones que se utilizará para asignar IPs a los hosts de la red. Es necesario excluir de este **pool de direcciones** la IP de la puerta de enlace y las IPs que se vayan a asignar de forma estática.

6. IPv4: direcciones privadas / direcciones públicas

Si no existieran las direcciones privadas,
las IPs se habrían agotado hace tiempo.

Direcciones privadas.-

Direcciones utilizadas en **redes internas** de organizaciones, empresas y viviendas.

Cualquier vivienda u organización puede utilizar direcciones privadas en su red interna. Como consecuencia, las direcciones de red de distintas viviendas u empresas pueden coincidir (no importa: no da lugar a conflicto).

IMPORTANTE: Los paquetes que contienen estas direcciones no pueden circular (enrutarse) por una red pública como Internet.

Direcciones públicas.-

Direcciones utilizadas por dispositivos con **presencia en Internet**, como servidores web, servidores DNS, puerto ADSL de nuestro router, etc.

Para obtener una IP pública hay que solicitarla al ISP o a un registro regional de Internet (en Europa, IANA delega esta función en RIPE <http://www.ripe.net>)

6. IPv4: direcciones privadas / direcciones públicas

CLASE	1 ^{er} OCTETO (decimal)	1 ^{er} OCTETO (binario)	MÁSCARA	Nº DE HOSTS	DIRECCIONES PRIVADAS (decimal)
A	1-126	0XXXXXXX	255.0.0.0	$2^{24} - 2$	10.x.x.x
B	128-191	10XXXXXX	255.255.0.0	$2^{16} - 2$	172.16.x.x – 172.31.x.x 169.254.x.x*
C	192-223	110XXXXX	255.255.255.0	$2^8 - 2$	192.168.x.x
D	224-239	1110XXXX	Direcciones Multicast		
E	240-255	1111XXXX	Direcciones Experimentales**		

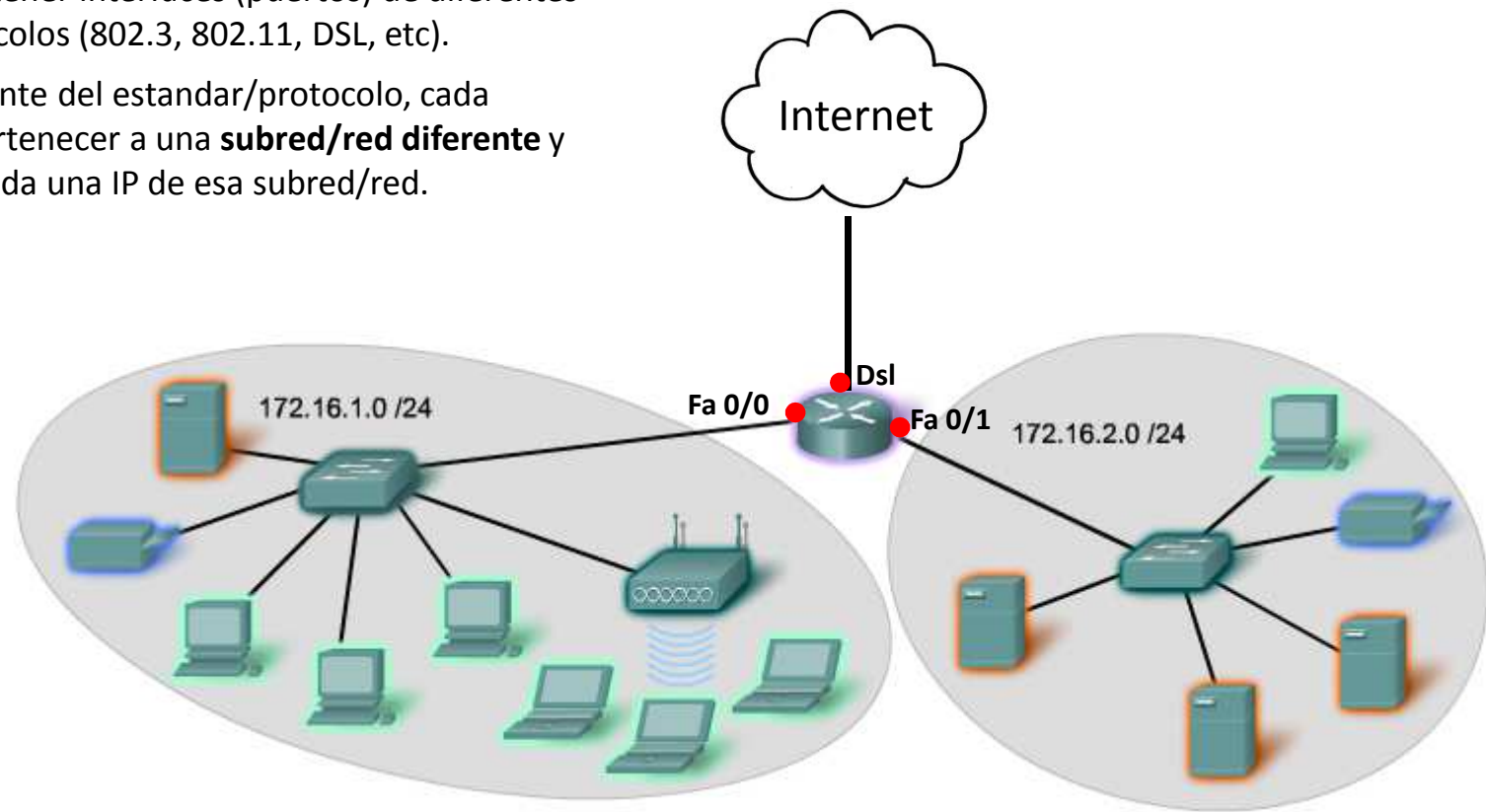
* Direcciones Link-Local.

** Estas direcciones están reservadas para fines de investigación o experimentación.

6. IPv4: direcciones privadas / direcciones públicas

Un router puede tener interfaces (puertos) de diferentes estándares/protocolos (802.3, 802.11, DSL, etc).

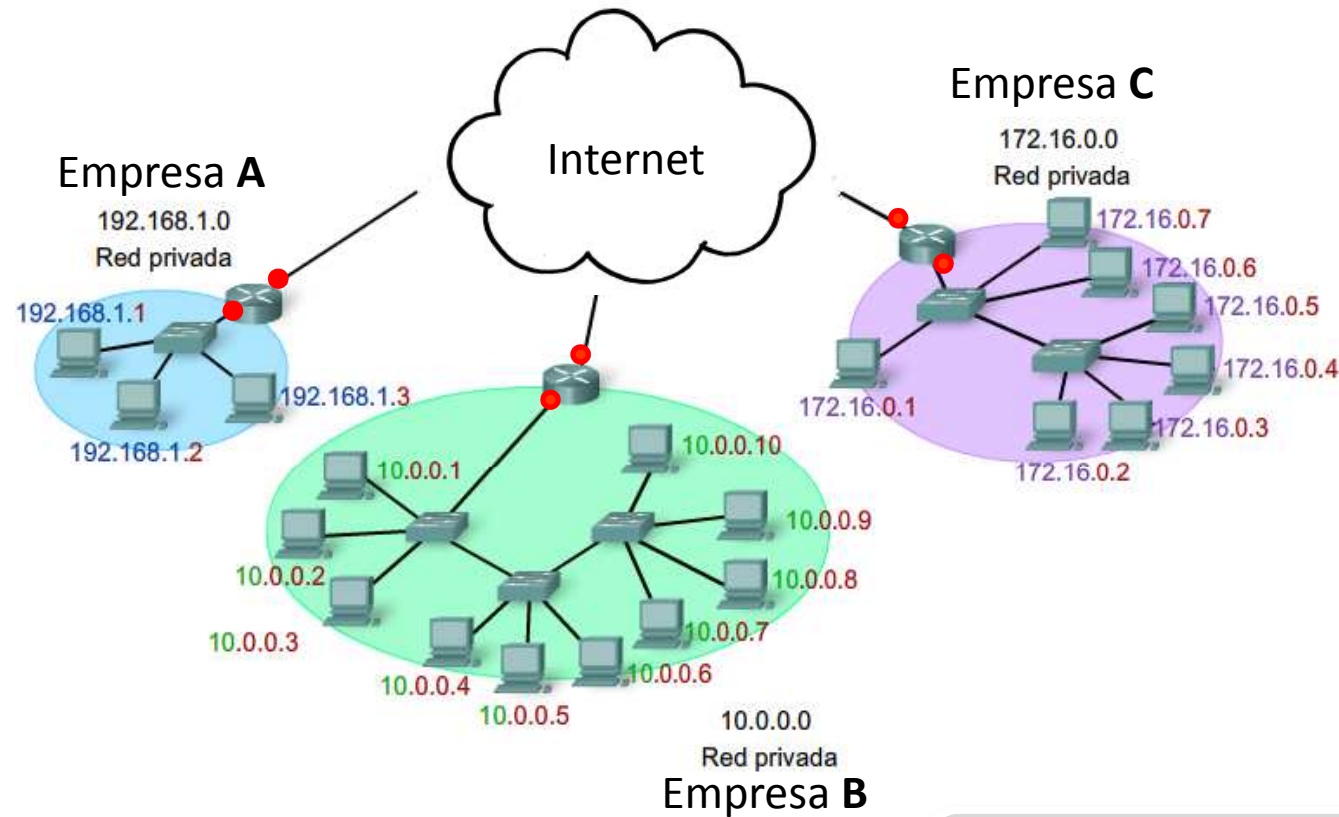
Independientemente del estándar/protocolo, cada interfaz, debe pertenecer a una **subred/red diferente** y debe tener asignada una IP de esa subred/red.



¿Cuántas IPs debe tener este router?

Los **switches** y **puntos de acceso** no requieren direcciones IP para funcionar. Sólo necesitamos asignarles una IP, si queremos acceder a ellos vía Telnet/SSH/Web para administrarlos.

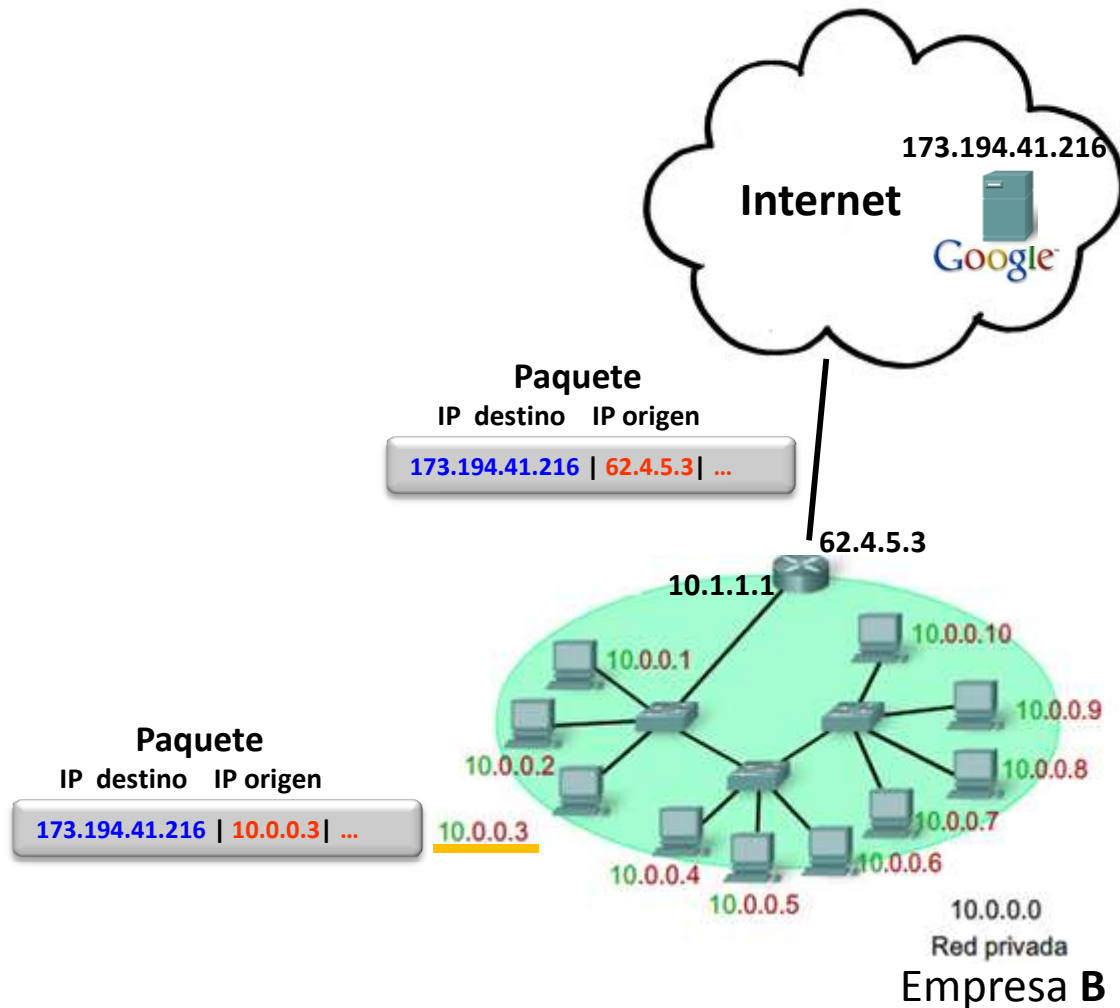
6. IPv4: direcciones privadas / direcciones públicas



¿Qué direcciones IPs tendrían los puertos de cada router ?

Si la empresa C necesitase utilizar para su red interna el mismo rango de direcciones que la empresa A ¿podría?

6. IPv4: direcciones privadas / direcciones públicas



PROBLEMA:


Los paquetes que tienen una dirección IP origen privada no pueden circular por Internet, un router nunca los dejará pasar.


SOLUCIÓN:

El router convertirá esa IP privada en pública gracias al sistema de traducción NAT.

Sin NAT un host con dirección IP privada no podría acceder a Internet.

6. IPv4: direcciones privadas / direcciones públicas

NAT (Network Address Translation) mapea una dirección IP privada a una dirección pública. El router asignará a cada dirección privada una dirección pública distinta. Las correspondencias entre direcciones privadas y públicas se registran en una tabla del router denominada tabla NAT. 

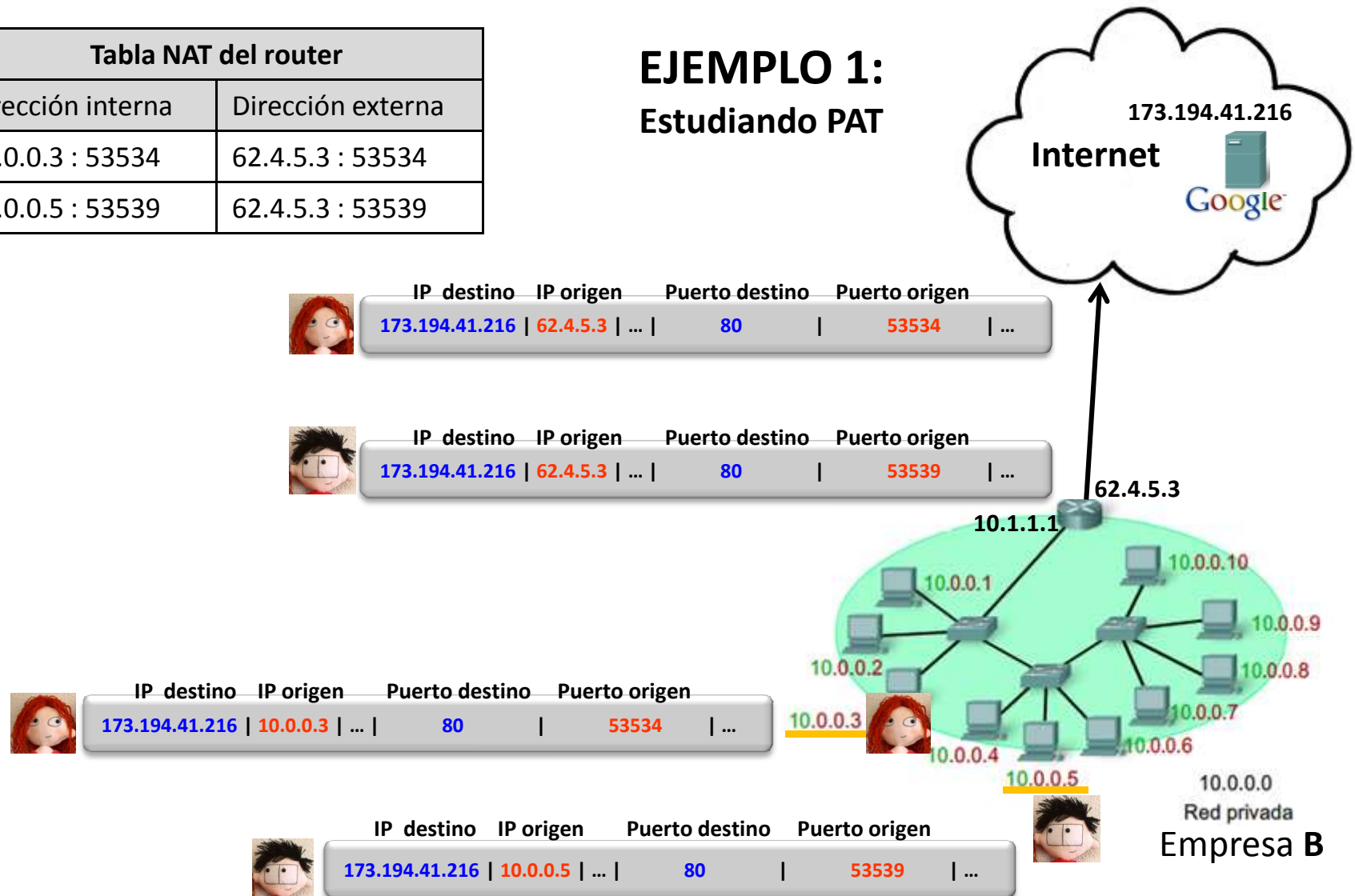
PAT (Port Address Translation). Variante NAT, conocida también como NAT con sobrecarga. En este caso, el router asigna la misma dirección pública a todas las direcciones privadas de la red (o a un conjunto de ellas). Para diferenciar las entradas en la tabla NAT, se utilizan los números de puerto. Los ejemplos de las siguientes diapositivas muestran el funcionamiento de PAT. 

NAT y PAT pueden funcionar a la vez en el mismo router.

6. IPv4: direcciones privadas / direcciones públicas

Tabla NAT del router	
Dirección interna	Dirección externa
10.0.0.3 : 53534	62.4.5.3 : 53534
10.0.0.5 : 53539	62.4.5.3 : 53539

EJEMPLO 1: Estudiando PAT

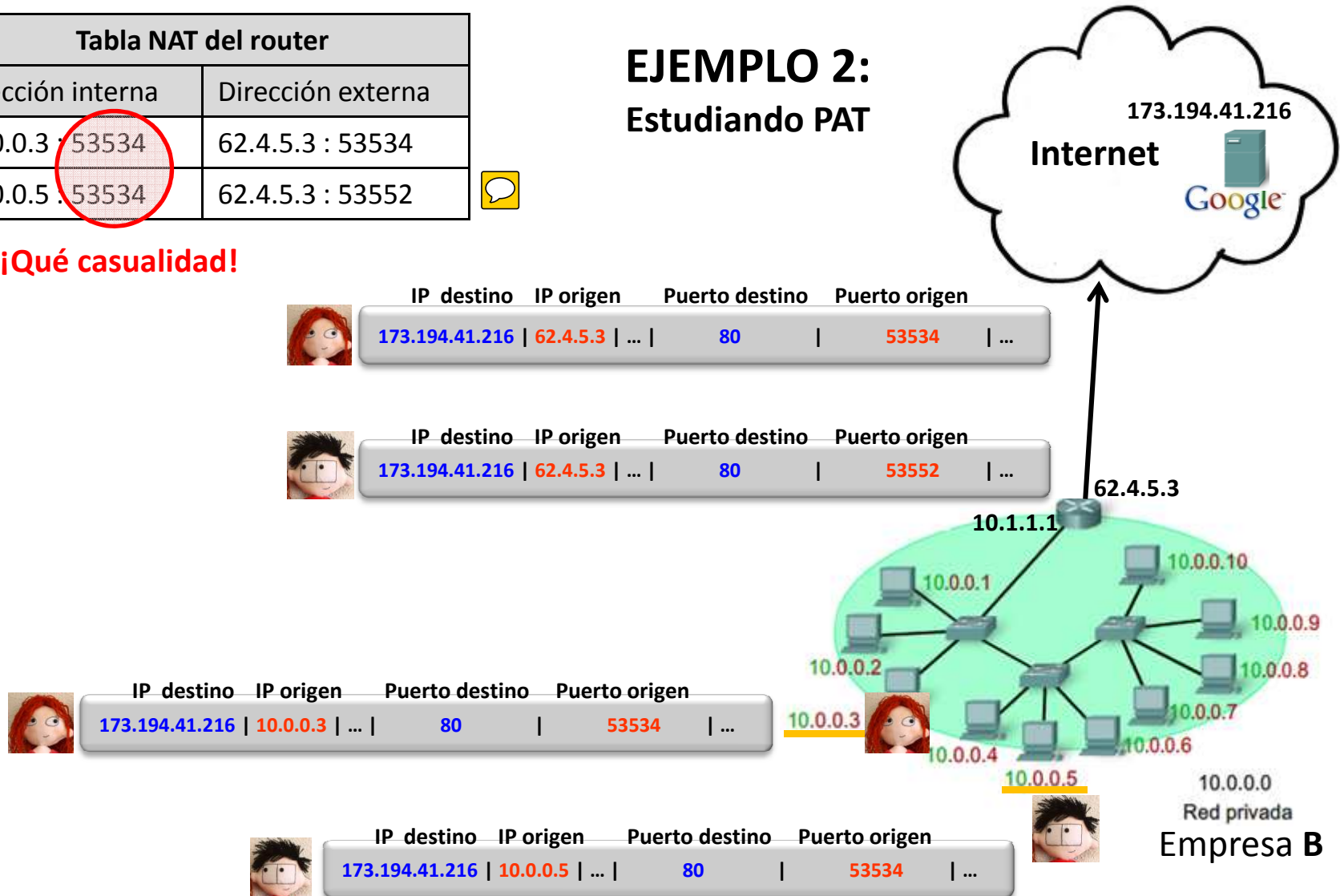


6. IPv4: direcciones privadas / direcciones públicas

Tabla NAT del router	
Dirección interna	Dirección externa
10.0.0.3 : 53534	62.4.5.3 : 53534
10.0.0.5 : 53534	62.4.5.3 : 53552

¡Qué casualidad!

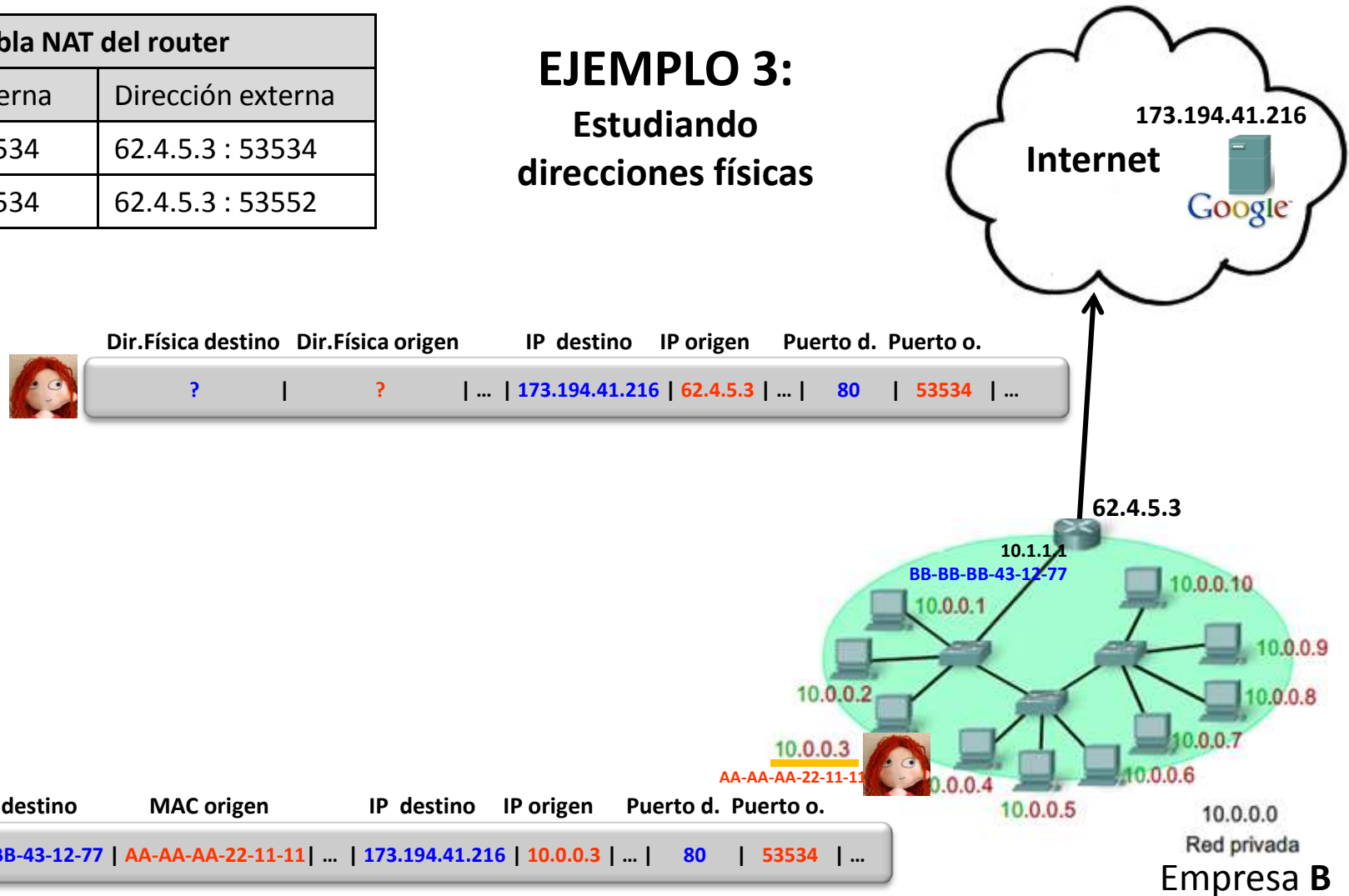
EJEMPLO 2: Estudiando PAT



6. IPv4: direcciones privadas / direcciones públicas

Tabla NAT del router	
Dirección interna	Dirección externa
10.0.0.3 : 53534	62.4.5.3 : 53534
10.0.0.5 : 53534	62.4.5.3 : 53552

EJEMPLO 3: Estudiando direcciones físicas



6. IPv4: direcciones privadas / direcciones públicas

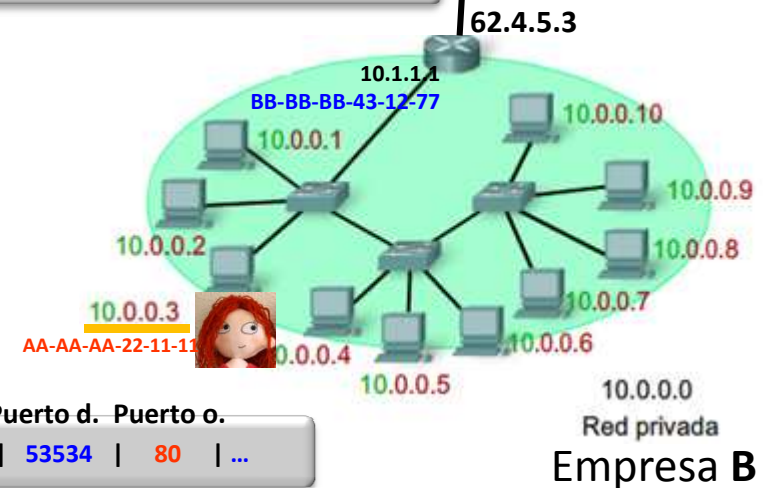
Tabla NAT del router	
Dirección interna	Dirección externa
10.0.0.3 : 53534	62.4.5.3 : 53534
10.0.0.5 : 53534	62.4.5.3 : 53552

EJEMPLO 3: Estudiando direcciones físicas



Google

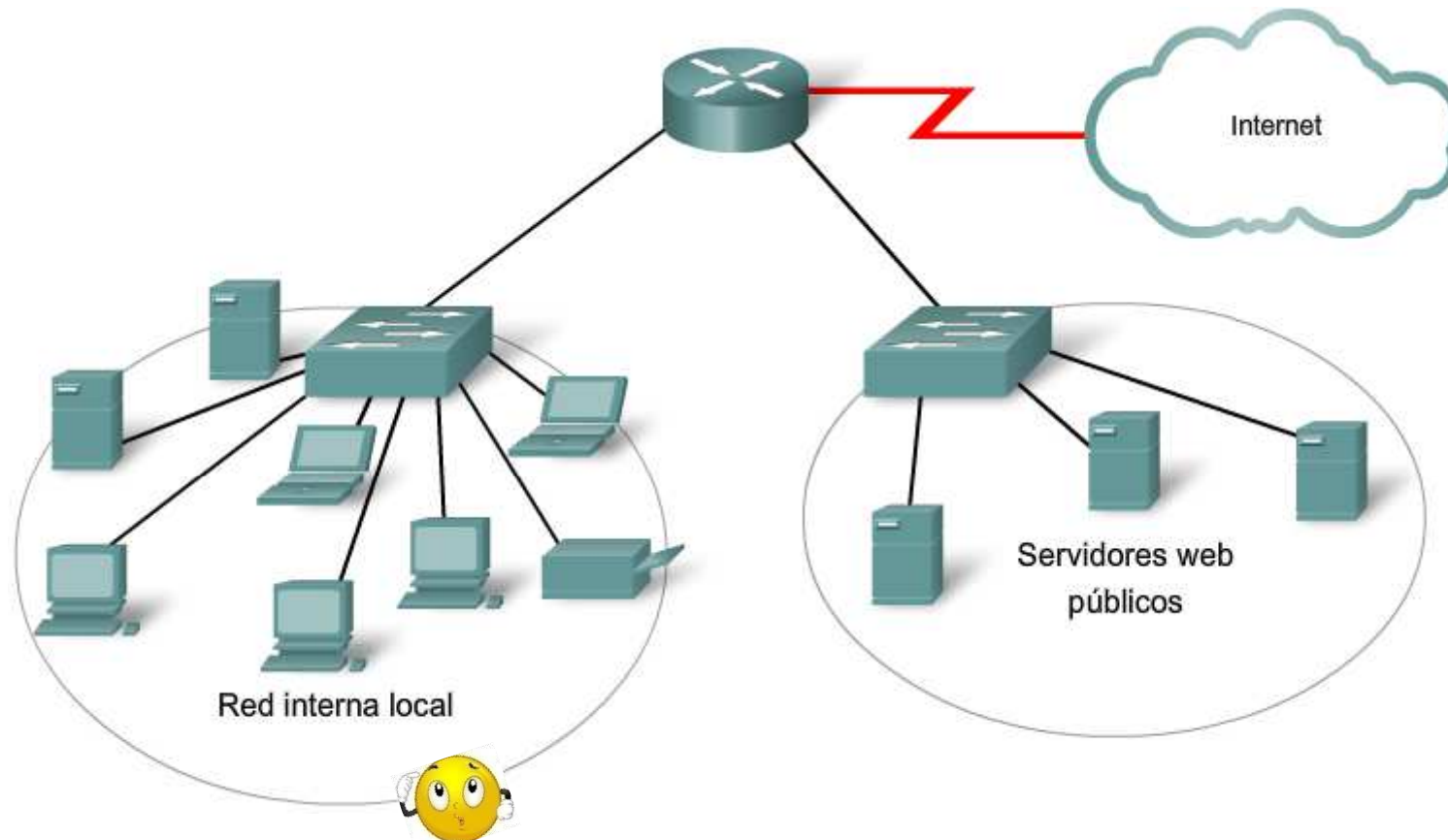
Dir.Física destino	Dir.Física origen	IP destino	IP origen	Puerto d.	Puerto o.			
?	?	...	62.4.5.3	173.194.41.216	...	53534	80	...



Google

Dir.Física destino	Dir.Física origen	IP destino	IP origen	Puerto d.	Puerto o.			
AA-AA-AA-22-11-11	BB-BB-BB-43-12-77	...	10.0.0.3	173.194.41.216	...	53534	80	...

6. IPv4: direcciones privadas / direcciones públicas



Nuestra organización tiene una serie de servidores públicos en sus instalaciones,
¿Qué tipo de dirección le asignamos? ¿Privada o Pública?

7. IPv4: Tipos de comunicaciones

- Unicast. Los datos se envían a un único host.
- Broadcast. Los datos se envían a todos los hosts de una subred/red.
- Multicast. Los datos se envían a un conjunto específico de hosts.
- Anycast. Los datos se envían a cualquier host de un conjunto determinado, ese host generalmente es el que está más cerca del dispositivo emisor.

Tipo de Comunicación	Receptores
Unicast	Uno específico
Broadcast	Todos los hosts de una subred/red
Multicast	Un conjunto específico de hosts
Anycast	Cualquier host de un conjunto determinado



7. IPv4: Tipos de comunicaciones

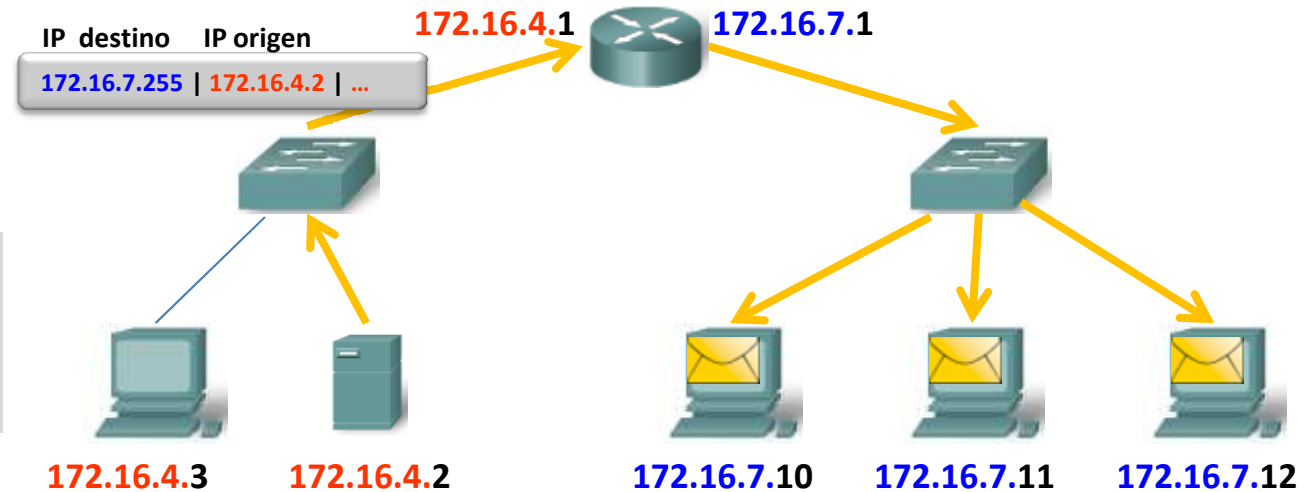
7.1. Broadcast dirigido

Utilizado cuando un dispositivo quiere comunicarse con todos los hosts de una subred/red **distinta** a la suya.

Dirección IP destino: **dirección broadcast de esa subred/red**, es decir, dirección cuyo HOST-ID tiene todos los bits a 1.

Por defecto, los routers no reenvían broadcasts dirigidos a otras subredes/redes. Pero pueden configurarse para que sí lo hagan.

Ejemplo: el servidor de la subred 172.16.4.0/24 quiere enviar un broadcast a la subred 172.16.7.0/24.



7. IPv4: Tipos de comunicaciones

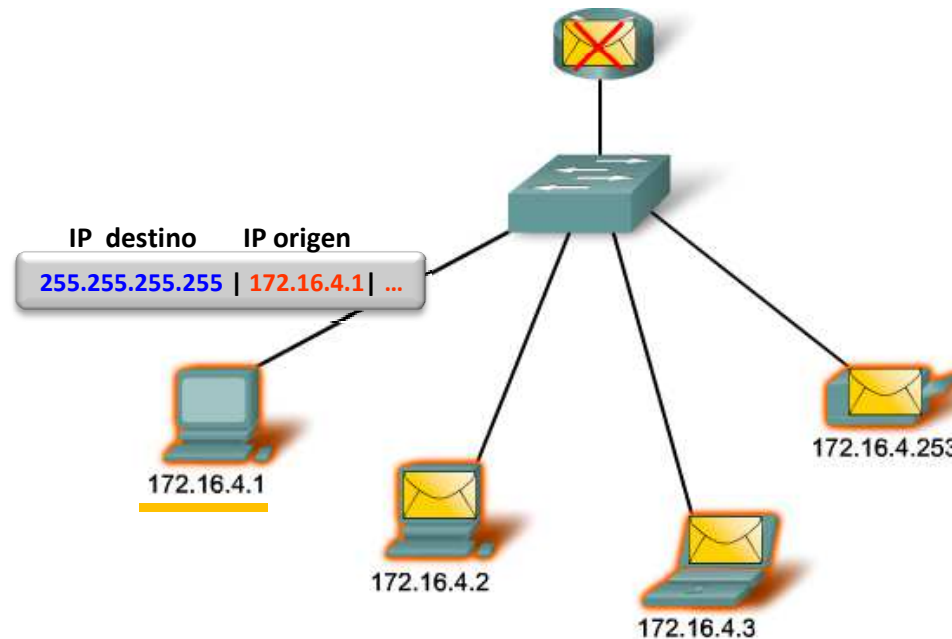
7.2. Broadcast limitado

Utilizado cuando un dispositivo quiere comunicarse con todos los hosts de **su propia** subred/red.

Dirección IP destino: **255.255.255.255**.

Los routers nunca reenvían broadcasts limitados a otras subredes/redes. Por ello, se dice que un router demarca el **dominio de broadcast**.

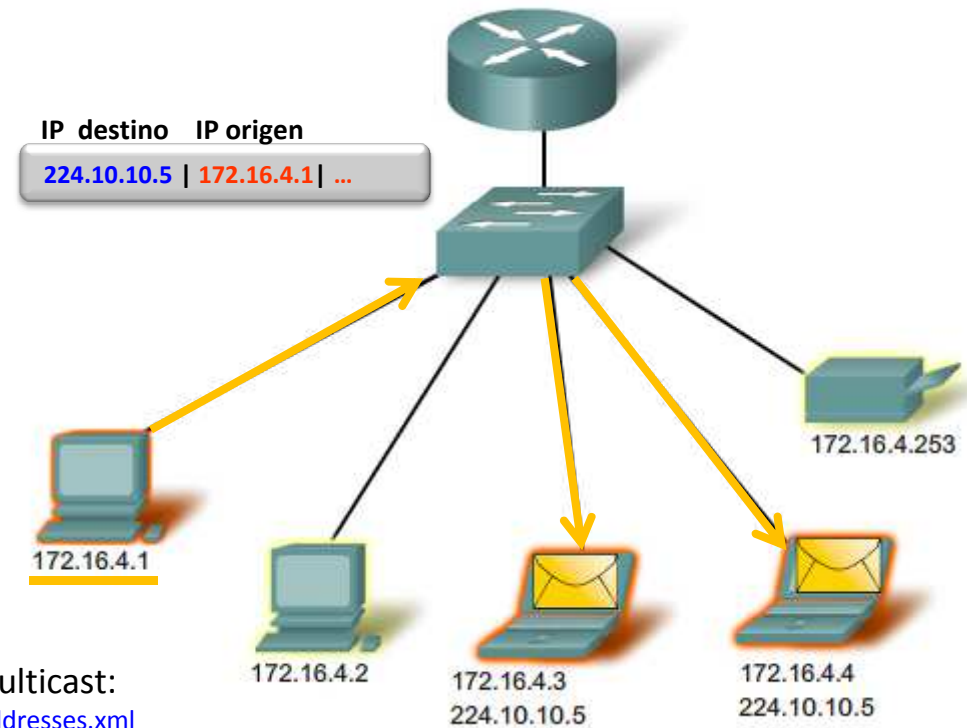
Ejemplo: un host que pertenece a la subred 172.16.4.0/24 quiere enviar un broadcast a todos los hosts de su subred.



7. IPv4: Tipos de comunicaciones

7.3. Multicast

Utilizado cuando un dispositivo quiere comunicarse sólo con un conjunto de hosts.









Mas información sobre el espacio de direcciones multicast:
<http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>

Algunos usos:

- Distribución de audio y video en tiempo real (**streaming**) a un grupo de hosts. Para curiosear, puedes buscar información sobre la implantación de video streaming muticast con la solución VLC.
- Distribución de software, como imágenes de arranque de sistemas operativos.
- Intercambio de información de **enrutamiento** por medio de protocolos de enrutamiento.

8. IPv4: Direcciones reservadas

Existen una serie de direcciones IP especiales que no se pueden asignar a ningún host. Estas son:

- Dirección de broadcast limitada 
- Dirección de broadcast dirigida 
- Dirección de red/subred
- Dirección Loopback 
- Dirección “sin especificar” 
- Dirección destino de una ruta por defecto. 
- Dirección Link-Local 

8. IPv4: Direcciones reservadas

8.1. Dirección Loopback

Direcciones loopback: desde 127.0.0.0 hasta 127.255.255.255 (**127.x.x.x** \equiv 127.0.0.0 /8).
Generalmente se utiliza 127.0.0.1

Es una dirección especial que los hosts utilizan para **dirigir el tráfico hacia ellos mismos**.

Un ping a la dirección de loopback sirve para verificar si la pila de protocolos TCP/IP de ese host está funcionando correctamente.

8. IPv4: Direcciones reservadas

8.2. Sin especificar

Es la dirección **0.0.0.0** y representa la ausencia de dirección.



¿Cuál puede ser su uso? **Pregunta de examen**



La dirección **0.0.0.0** también es utilizada para definir la dirección de red en una ruta por defecto.

El router/switch_capa3/host enviará los paquetes por esta ruta cuando no exista en su tabla de enrutamiento otra ruta más específica para llegar al destino del paquete.

Otras denominaciones de ruta por defecto: ruta predeterminada, gateway de último recurso.

8. IPv4: Direcciones reservadas

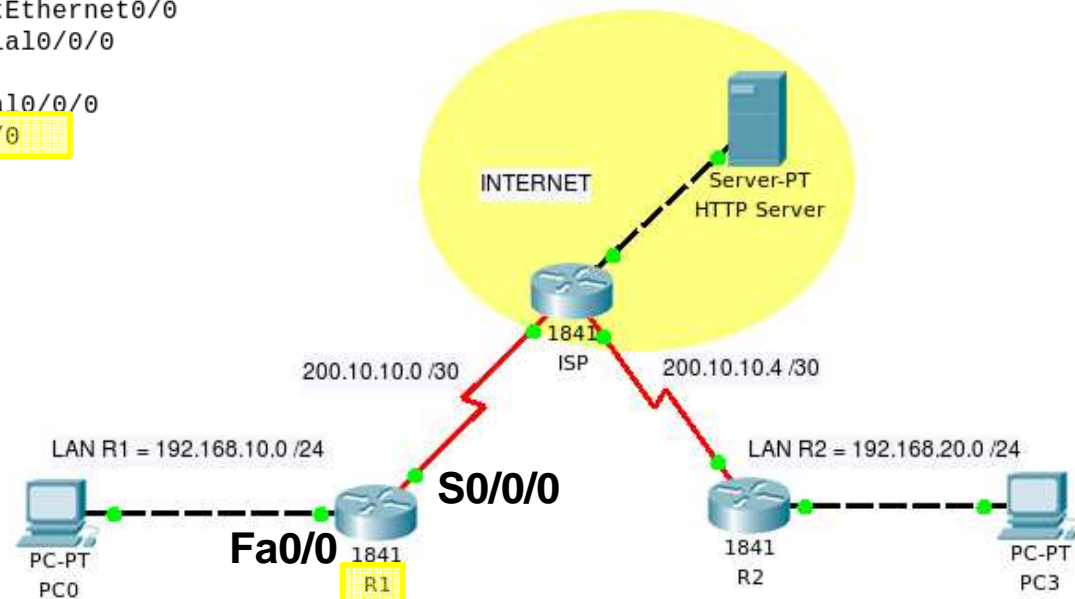
8.3. Ruta predeterminada

Esta es la tabla de enrutamiento del router R1 de la figura

```
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
S    192.168.20.0/24 is directly connected, Serial0/0/0
    200.10.10.0/30 is subnetted, 1 subnets
C        200.10.10.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
R1#
```



8. IPv4: Direcciones reservadas

8.4. Dirección Link-Local

Direcciones Link-Local: desde 169.254.0.0 hasta 169.254.255.255 (**169.254.x.x** \equiv 169.254.0.0 /16).

Función de **autoconfiguración** (también denominada auto-IP, APIPA o Zeroconf).- Si un equipo no tiene asignada una dirección IP (o no consigue contactar con el servidor DHCP para que le proporcione una dirección IP) y su sistema operativo tiene habilitada la función de autoconfiguración, configurará automáticamente una IP Link-Local. El método de asignación es el siguiente:

1. El equipo se asigna una IP aleatoria del rango Link-Local.
2. El equipo lanza a la red una consulta ARP para asegurarse de que esa IP no está en uso. Si la dirección ya está en uso, se reasigna otra IP.

Los equipos que tienen una dirección Link-Local no tienen acceso a Internet, sólo pueden comunicarse con equipos que están en la misma red.

Aplicaciones:

- Redes Ad-Hoc.

Más información:

<http://www.ietf.org/rfc/rfc3330.txt>

<http://www.ietf.org/rfc/rfc3927.txt>