Tema 3: Capa de Red

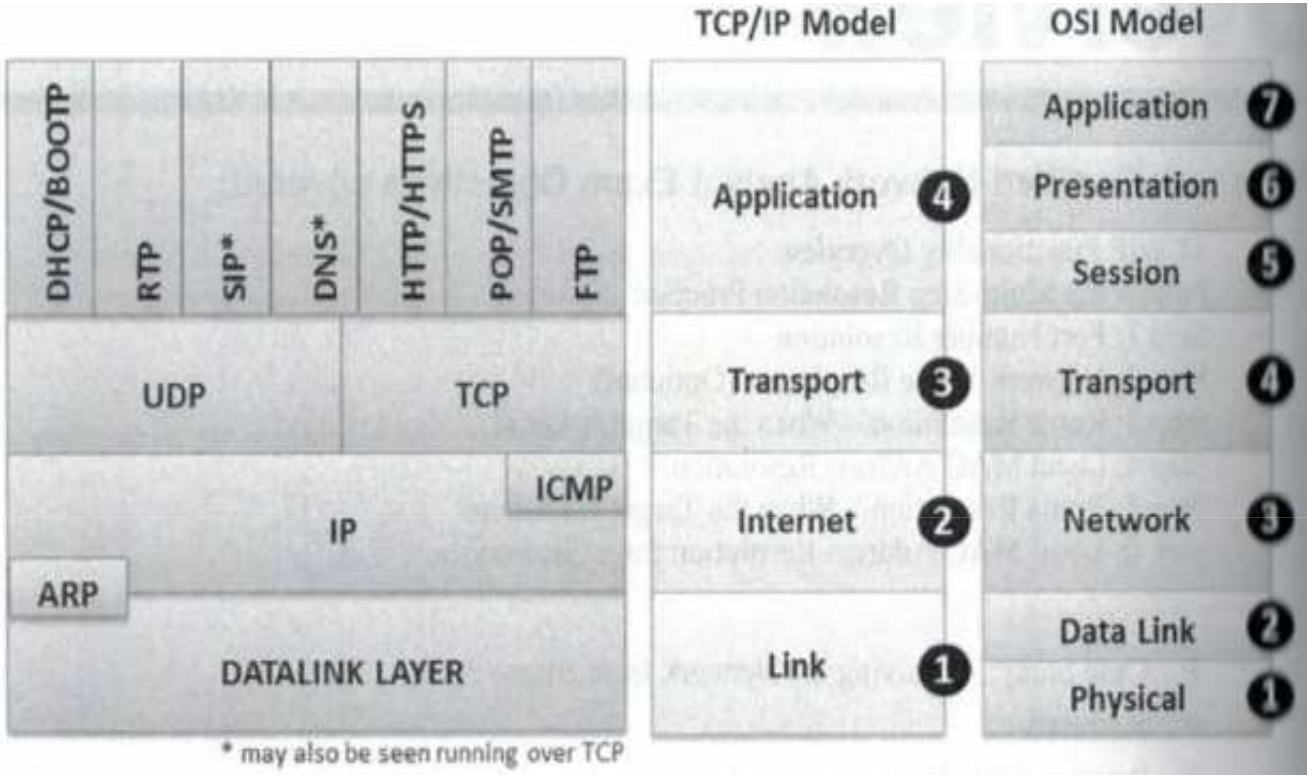
3ª PARTE: Protocolos ICMP, ARP

Redes de Computadores

Grado en Ingeniería Informática

Mercedes Rodríguez García

Índice



Fuente imagen: Laura Chappell. Wireshark Network Analysis. Chappell University, 2012

1. Protocolo ICMP

ICMP (Protocolo de Mensajes de Control de Internet).

ICMP es utilizado por los **DISPOSITIVOS** para:

- **Notificar errores** al dispositivo emisor.
- **Suministrar información de control** a otros dispositivos.

ICMP es utilizado por el **ADMINISTRADOR DE RED** para:

- **Diagnosticar** fallas de red.

Los mensajes ICMP se crean en la capa 3 (**no vienen de la capa 4**).

Existen muchos tipos de mensajes ICMP (estos son sólo algunos):

Tipo	
0	**Respuesta de eco**
3	**Destino inalcanzable**
8	**Petición de eco**
11	**Tiempo agotado**
12	Cabecera IP errónea

Mensajes de **notificación de errores**

Tipo	
4	Control de cogestión
9	Anuncio de router
10	Descubrimiento de router
13	Petición de marca horaria
14	Respuesta de marca horaria

Mensajes de **control**

Un paquete puede no llegar a su destino por diversas razones:

- Fallas de hardware.
- Configuración de red inadecuada.
- Información de enrutamiento incorrecta.

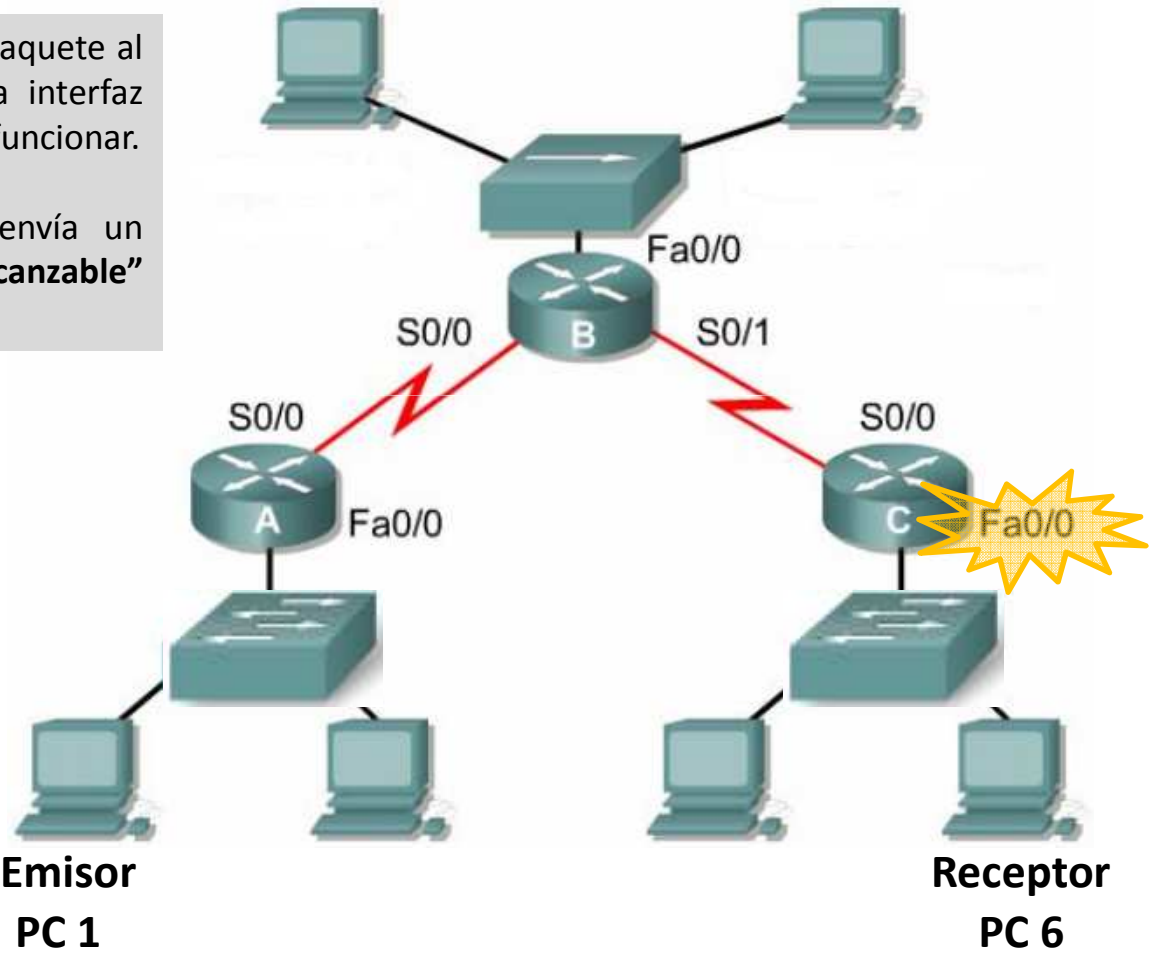
La capa de red de un dispositivo utiliza ICMP para notificar de estos errores al equipo emisor.

ICMP **no corrige** el problema, sólo informa.

Dado que los paquetes ICMP se transmiten del mismo modo que cualquier otro paquete, **están sujetos a las mismas fallas** en la entrega.

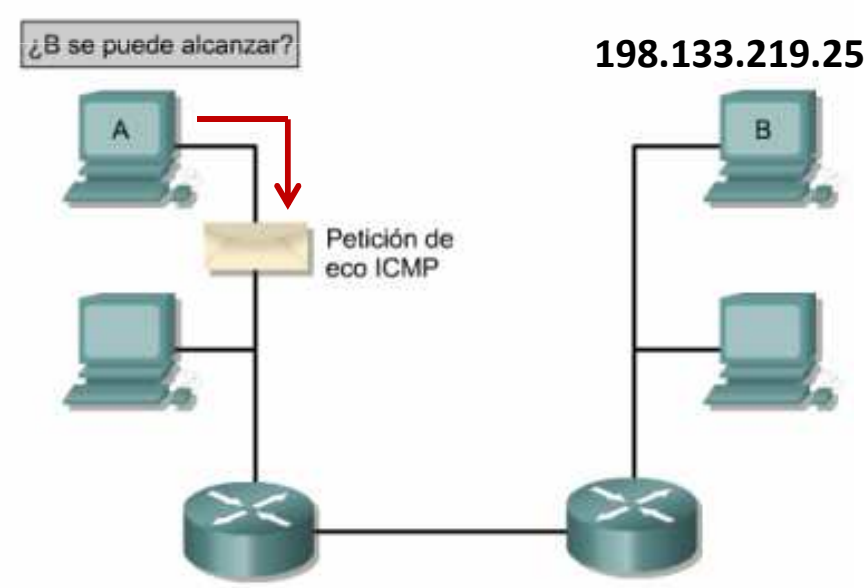
En este ejemplo, PC1 envía un paquete al PC6. Pero hay un problema: la interfaz Fa0/0 del router C ha dejado de funcionar.

Para notificarlo, el router C envía un mensaje ICMP de **"destino inalcanzable"** al PC1.



El protocolo ICMP se puede usar para verificar la conectividad con un destino en particular. Para ello, se utiliza el comando ping.

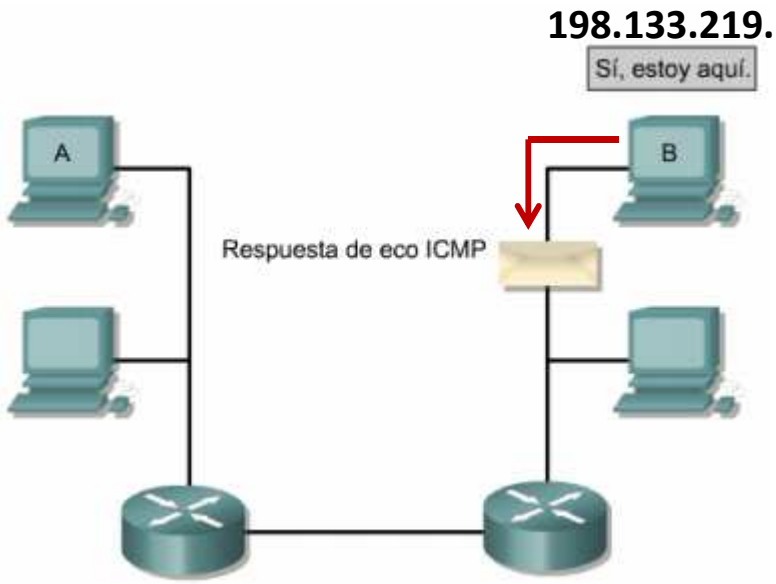
Cuando se ejecuta el comando ping, por defecto, **se generan cuatro mensajes de petición de eco** ICMP.




```
C:\> ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:
```

Cuando el destino recibe un mensaje de petición de eco, crea un mensaje de **respuesta de eco** y lo envía al dispositivo origen.

Si el emisor recibe la respuesta, se confirma que el dispositivo destino se puede alcanzar (hay conectividad).




```
C:\> ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:

Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Recieved = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 16ms, Average = 16ms
C:\>
```

El comando tracert informa del camino exacto que siguen los paquetes de datos desde el equipo origen hasta el equipo destino.

Va mostrando **información de cada salto**:

- Número del salto.
- Tiempo empleado en ir y volver desde el equipo emisor al salto.
- Dirección IP del salto.

Un **salto** es un equipo intermediario de capa 3 o superior, normalmente un router.

¿Cómo lo consigue? **ENVIANDO paquetes de petición de eco ICMP**.

Para averiguar el primer salto de la ruta, el equipo origen envía paquetes eco con TTL igual a 1 (por defecto envía 3 paquetes). Cuando los paquetes eco llegan al primer salto, el TTL se decrementa en una unidad. Como, ahora, el TTL vale 0, el equipo intermediario envía un mensaje ICMP de **"Tiempo agotado"** al equipo origen.

Con este hecho, el equipo origen conoce la IP del primer salto.

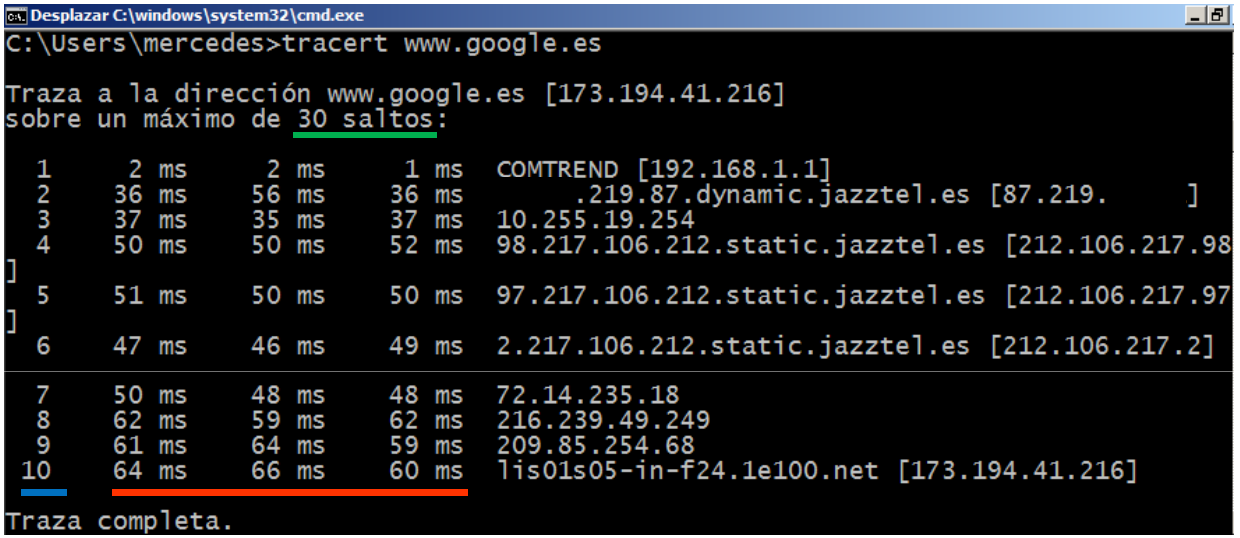
Para averiguar el segundo salto de la ruta, el equipo origen envía paquetes eco con TTL igual a 2 (por defecto envía 3 paquetes). Cuando los paquetes eco llegan al primer salto, el TTL se decrementa en una unidad. Ahora, el TTL vale 1. Cuando llegan al segundo salto, el TTL se vuelve a decrementar en una unidad. Como, ahora, el TTL vale 0, el segundo equipo intermediario envía un mensaje ICMP de **"Tiempo agotado"** al equipo origen.

Con este hecho, el equipo origen conoce la IP del segundo salto.

Este es el modo de proceder hasta llegar al equipo destino.

Por defecto se imprimen trazas con un **máximo de 30 saltos**. Con la opción -h del comando tracert se puede modificar este valor.

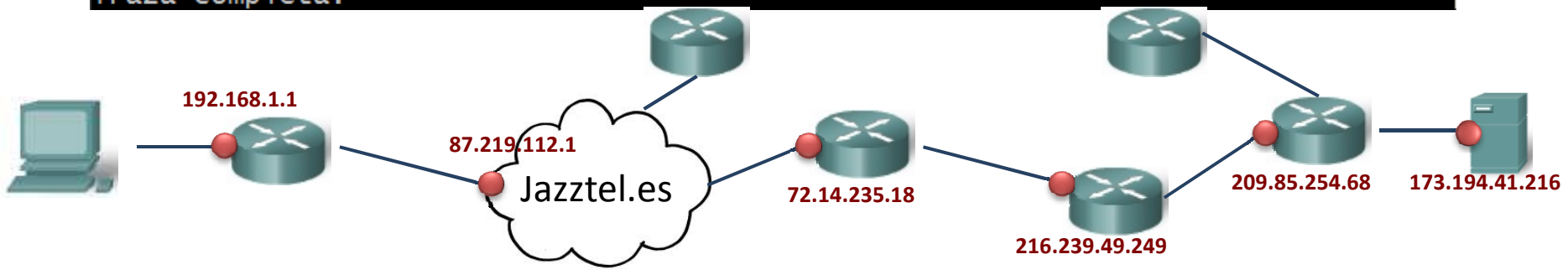
Esta ruta tiene **10 saltos**.



En cada salto, se indican los **tiempos** que han empleado los tres paquetes eco en ir y volver desde el equipo origen hasta el equipo intermediario. Un asterisco (*) indica que no se obtuvo respuesta.

Se puede utilizar tracert para averiguar **en qué lugar se detuvo la conexión**.

```
Desplazar C:\windows\system32\cmd.exe
C:\Users\mercedes>tracert www.google.es

Traza a la dirección www.google.es [173.194.41.216]
sobre un máximo de 30 saltos:

  1     2 ms     2 ms     1 ms  COMTREND [192.168.1.1]
  2    36 ms    56 ms    36 ms  1.112.219.87.dynamic.jazztel.es [87.219.112.1]
  3    37 ms    35 ms    37 ms  98 . 217 . 105 . 45
  4    50 ms    50 ms    52 ms  98.217.106.212.static.jazztel.es [212.106.217.98
]
  5    51 ms    50 ms    50 ms  97.217.106.212.static.jazztel.es [212.106.217.97
]
  6    47 ms    46 ms    49 ms  2.217.106.212.static.jazztel.es [212.106.217.2]

  7    50 ms    48 ms    48 ms  72.14.235.18
  8    62 ms    59 ms    62 ms  216.239.49.249
  9    61 ms    64 ms    59 ms  209.85.254.68
 10    64 ms    66 ms    60 ms  lis01s05-in-f24.1e100.net [173.194.41.216]

Traza completa.
```



ANALIZANDO POSIBLES PROBLEMAS en este ejemplo:

Si no hubiese respuesta en el salto 1, el problema lo tenemos en la puerta de enlace de nuestra propia red.

Si la respuesta se pierde entre los saltos 2 y 6, quien está interrumpiendo la conexión es nuestro proveedor de acceso a Internet (en nuestro ejemplo, Jazztel).

En los saltos intermedios intervienen otras redes de tránsito de diferentes operadores. A veces, se deja de tener respuesta porque están congestionadas de tráfico. En estos casos, es recomendable repetir la orden tracert pasado un tiempo.

Si no hubiese respuesta a partir del salto 9, el problema estaría en las instalaciones de google.

2. Protocolo ARP

El protocolo ARP (Address Resolution Protocol) se encarga de descubrir la dirección MAC de un dispositivo sabiendo su dirección IP.

Cada dispositivo mantiene en memoria una tabla de equivalencias entre direcciones IP y direcciones MAC (esta tabla se llama tabla ARP). El contenido de esta tabla se puede ver con el comando **arp –a**.

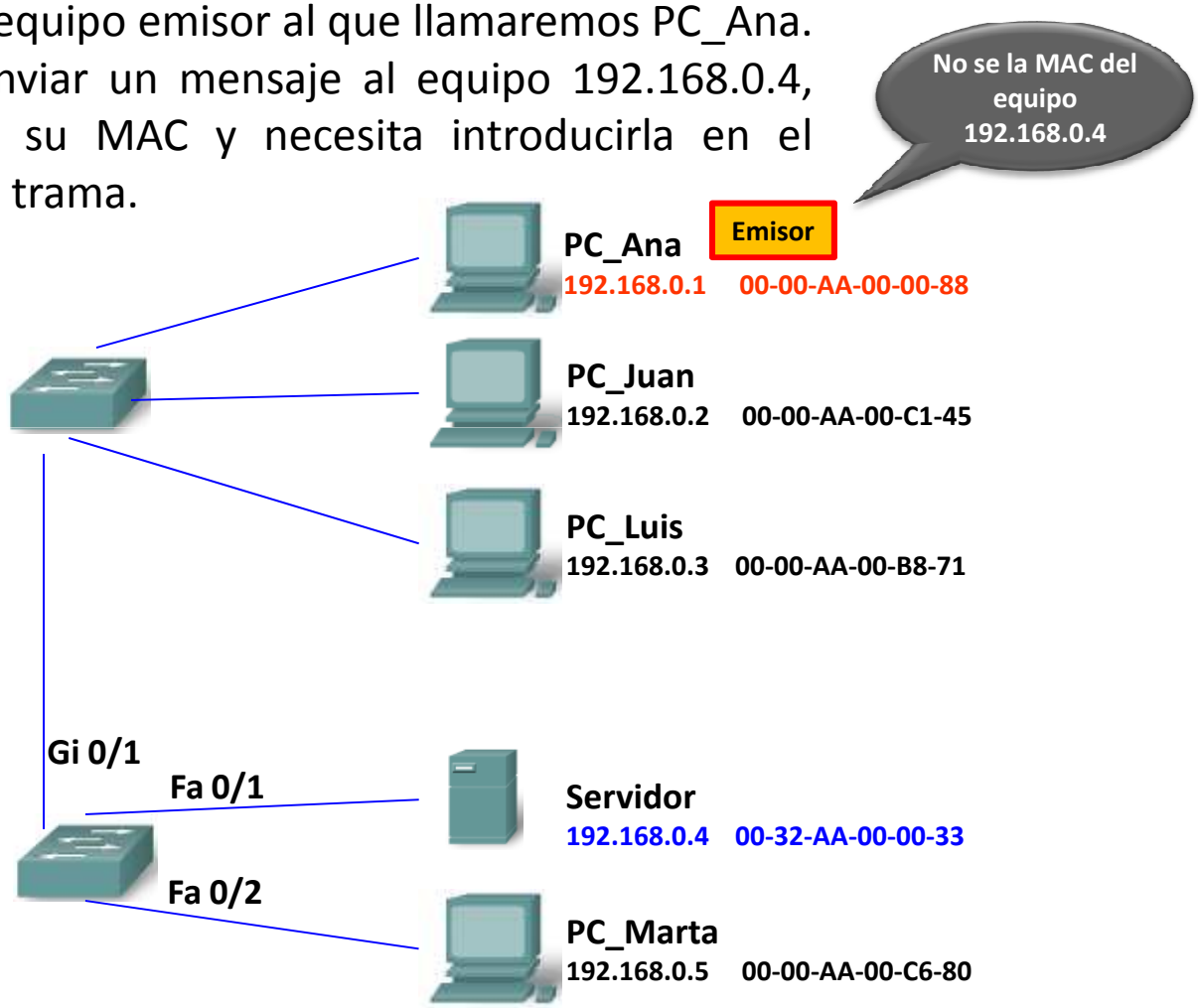
```
C:\Users\mercedes>arp -a

Interfaz: 10.141.153.174 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  10.141.1.1            2c-6b-f5-3c-40-00     dinámico
  10.141.1.3            aa-30-0a-8d-01-03     dinámico
  10.141.1.4            aa-30-0a-8d-01-04     dinámico
  10.141.2.139          00-e0-4d-0c-a5-9f     dinámico
```

¿Para qué necesitamos saber la MAC del dispositivo con el que queremos comunicarnos?

Las entradas dinámicas permanecen en la tabla ARP sólo unos minutos.

2. Protocolo ARP

Ejemplo: Sea un equipo emisor al que llamaremos PC_Ana. PC_Ana desea enviar un mensaje al equipo 192.168.0.4, pero no conoce su MAC y necesita introducirla en el encabezado de la trama.



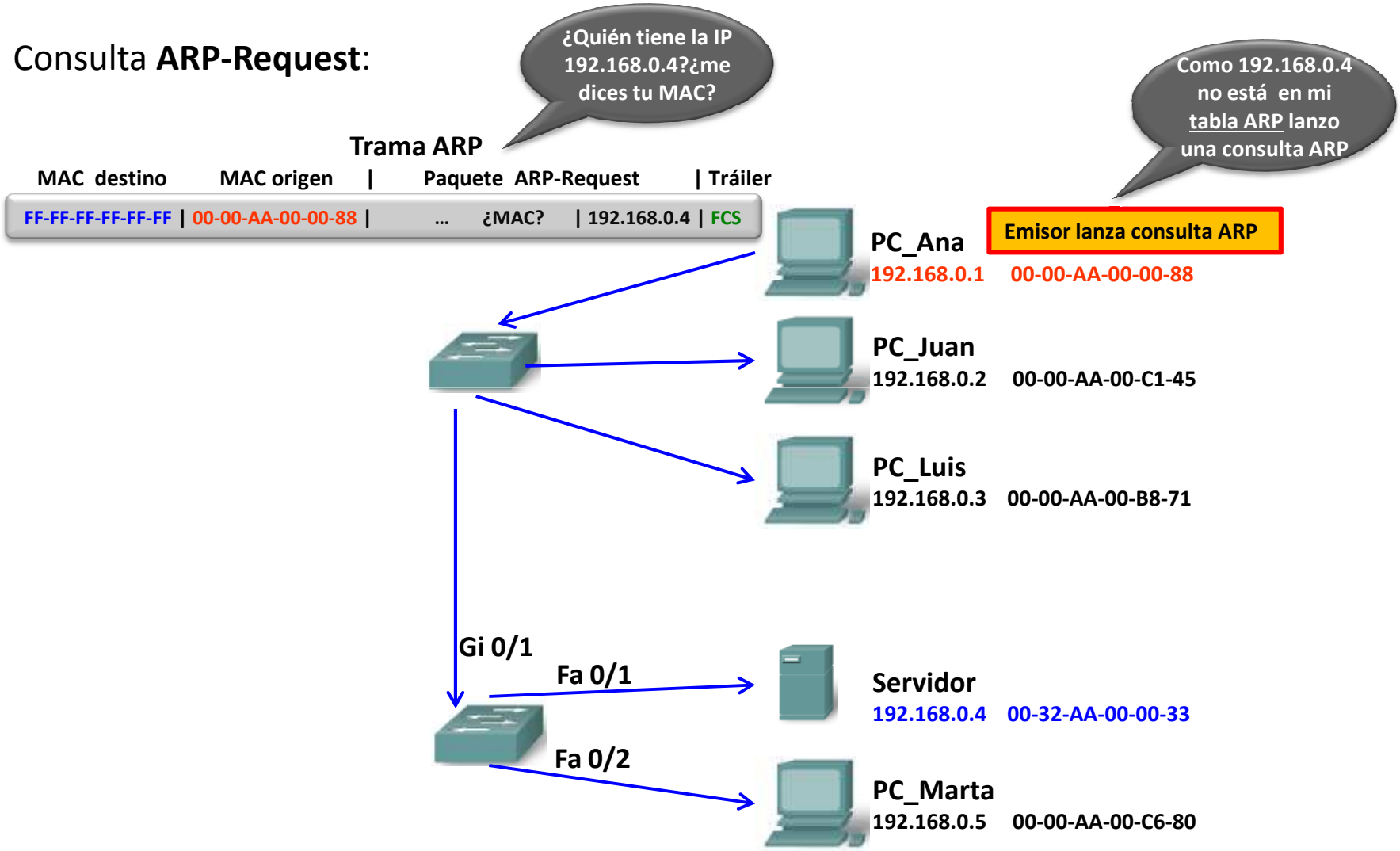
2. Protocolo ARP

PC_Ana, para averiguar la MAC del equipo 192.168.0.4 debe seguir estos pasos:

1. PC_Ana consulta su tabla ARP, comprueba si la dirección MAC está en la tabla.
2. Si **la dirección MAC está en la tabla ARP**, PC_Ana toma esa dirección y la inserta en el encabezado de la trama. **FIN**
3. Si **la dirección MAC no está en la tabla ARP**, entonces
    1. PC_Ana envía una consulta (**ARP-Request**) a todos los equipos de la subred/red.
    2. El equipo de la red que tiene esa IP envía una respuesta (**ARP-Reply**) a PC_Ana comunicándole su MAC.
    3. Cuando PC_Ana averigua la MAC, la registra en su tabla ARP para uso futuro. Finalmente, inserta la MAC en el encabezado de la trama. **FIN**

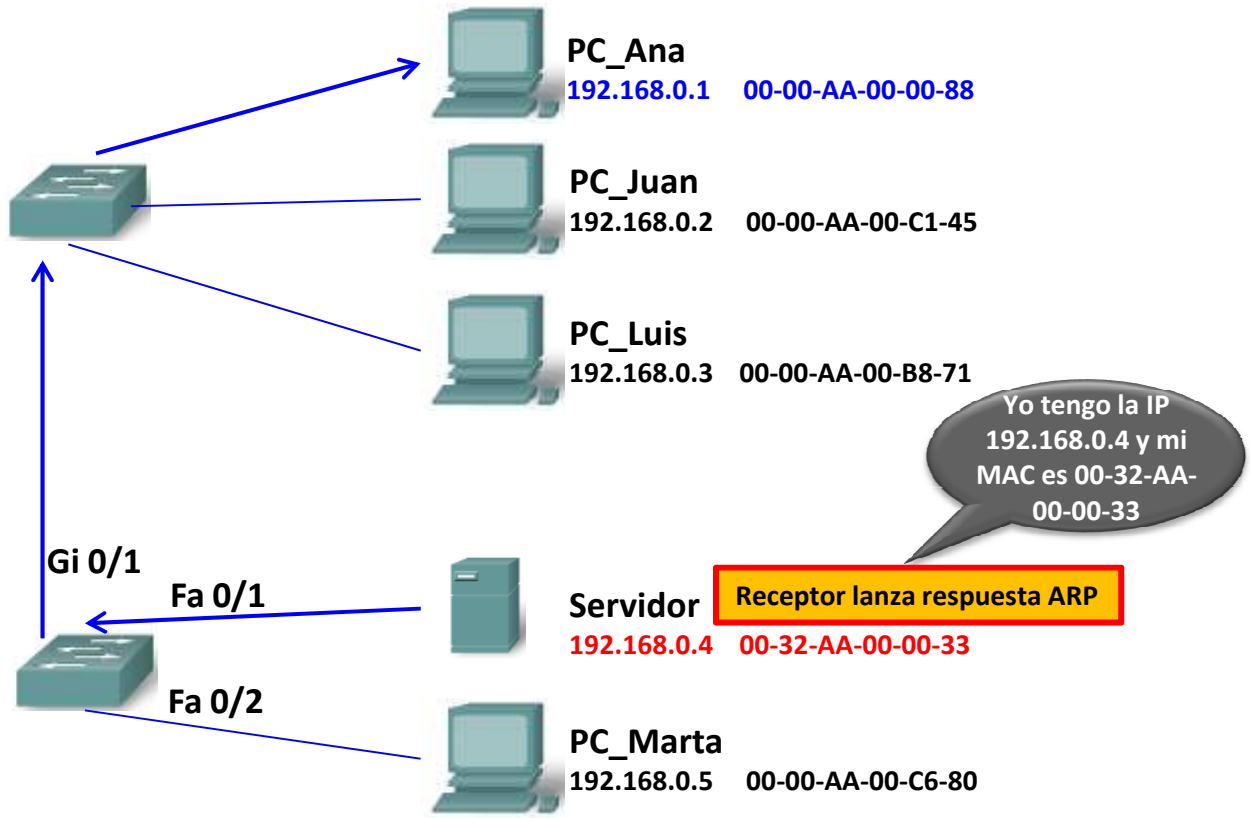
2. Protocolo ARP

Consulta **ARP-Request**:



2. Protocolo ARP

Respuesta **ARP-Reply**:



Trama ARP

MAC destino	MAC origen	Paquete ARP-Reply	Tráiler
00-00-AA-00-00-88	00-32-AA-00-00-33	... Respuesta: 00-32-AA-00-00-33	FCS

2. Protocolo ARP

Los mensajes ARP se crean en la capa 3 (**no vienen de la capa 4**).

NOTA: un paquete ARP no tiene la típica cabecera de capa 3.

2. Protocolo ARP

El equipo 10.0.0.3 desea enviar un mensaje a Google

¿Cuál es la dirección IP-destino del mensaje?

¿Cuál es la dirección Física-destino del mensaje?

Si el dispositivo origen no tiene en su tabla ARP la dirección Física-destino ¿Cómo sería la trama ARP-Request?