HOJA DE TRUCOS

# MÁSCARAS DE RED

|  |  |  |
| --- | --- | --- |
| CIDR | Máscara | Número de IPs |
| /30 | 255.255.255.252 | 4 |
| /29 | 255.255.255.248 | 8 |
| /28 | 255.255.255.240 | 16 |
| /27 | 255.255.255.224 | 32 |
| /26 | 255.255.255.192 | 64 |
| /25 | 255.255.255.128 | 128 |
| /24 | 255.255.255.0 | 256 |
| /23 | 255.255.254.0 | 512 |
| /22 | 255.255.252.0 | 1024 |
| /21 | 255.255.248.0 | 2048 |
| /20 | 255.255.240.0 | 4096 |

**Direcciones IP de Clase C**

* Para direcciones IP de Clase C, los primeros tres octetos (24 bits / 3 bytes) representan el ID de red, y el último octeto (8 bits / 1 bytes) es el ID de host.
* Las direcciones IP de Clase C van desde 192.0.0.0 hasta 223.255.255.255, con una máscara predeterminada 255.255.255.0 (o /24 en CIDR).
* La Clase C se traduce a 2,097,152 (221) redes y 254 (28-2) direcciones utilizables por red.

**Direcciones IP de Clase D y Clase E**

* Las últimas dos clases son la Clase D y la Clase E.
* Las direcciones IP de Clase D están reservadas para multidifusiones. Ellas ocupan el rango desde 224.0.0.0 hasta 239.255.255.255.
* Las direcciones IP de Clase E son experimentales, y son cualquiera arriba de 240.0.0.0

# TABLA DE RUTAS

|  |  |  |
| --- | --- | --- |
| Dirección Base | Máscara | Siguiente Salto |
| 192.168.45.0 | 255.255.255.128 | -- |
| 192.168.45.128 | 255.255.255.240 | 192.168.45.161 |

# FÓRMULAS DE SHANNON

## FORMULA ORIGINAL

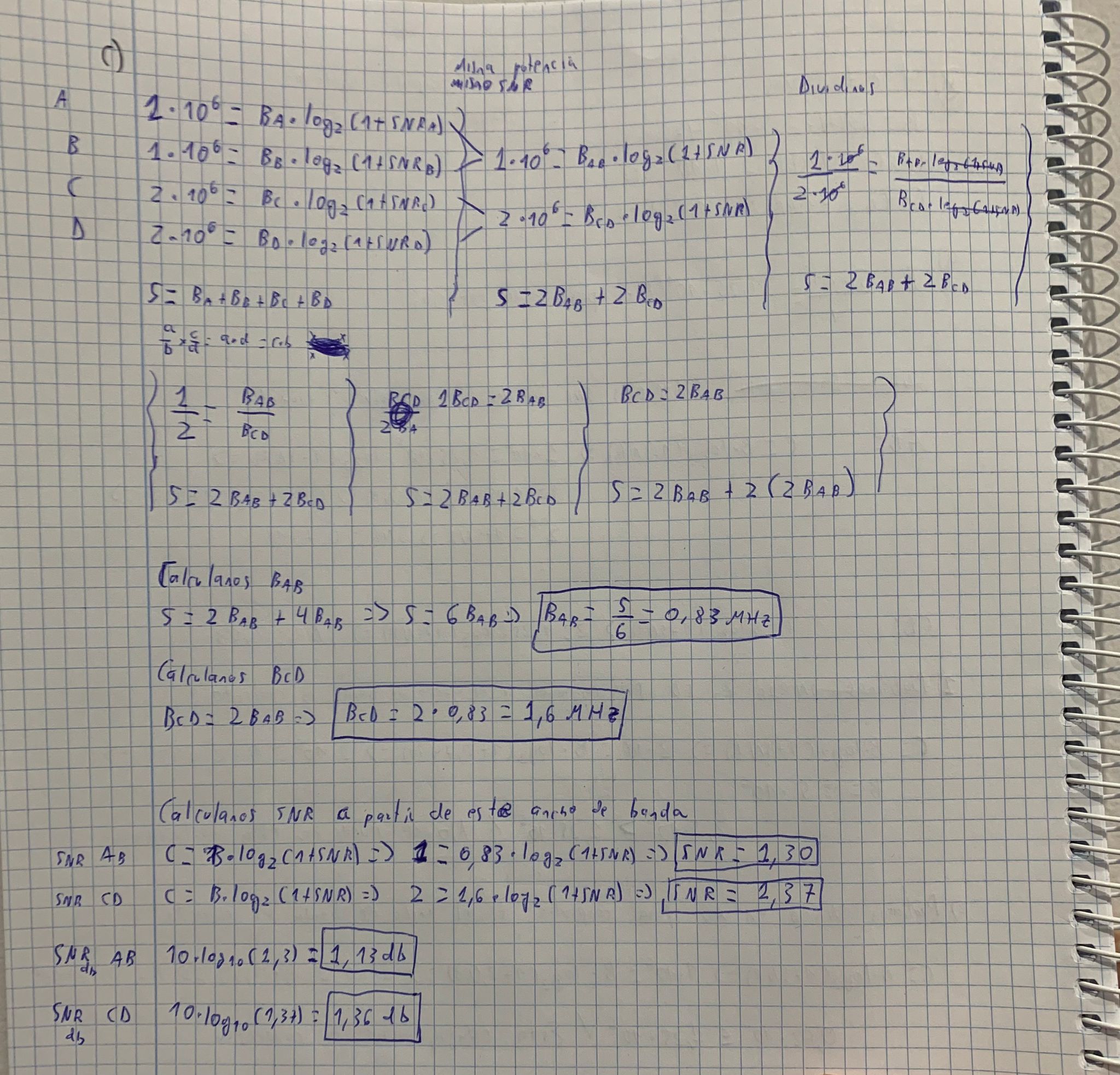
## DESPEJE DE B (ANCHO DE BANDA)

## DESPEJE DE SNR (RELACIÓN SEÑAL/RUIDO)

## DESPEJE DE SNR (DECIBELIOS)

## DESPEJE PARA SNR SOBRE SNRdb

Un ejemplo de como hacer el repato óptimo sería:



# TABLAS DE MENSAJES

## WIFI:

**RTS – CTS – Mensaje – ACK**

Correcto para redes Wi-Fi con control de acceso opcional RTS/CTS (Request to Send / Clear to Send), que se utiliza para evitar colisiones en redes con mucho tráfico o grandes distancias.

Flujo típico:

* RTS: El emisor solicita permiso para enviar.
* CTS: El receptor concede permiso.
* Mensaje: El emisor envía los datos.
* ACK: El receptor confirma la recepción de los datos (a nivel de enlace, obligatorio en 802.11).

## Ethernet:

**ARP Request – ARP Reply – Mensaje**

Correcto para escenarios en los que la dirección MAC del destino no está en la tabla ARP del emisor.

Flujo típico:

* ARP Request: Si el emisor no conoce la MAC asociada a una IP, hace una solicitud ARP por broadcast.
* ARP Reply: El dispositivo con esa IP responde directamente con su dirección MAC.
* Mensaje: Una vez resuelta la dirección, se envían los datos.

## TCP:

**SYN – SYN-ACK – ACK**

TCP requiere un handshake de tres vías para establecer una conexión fiable antes de transmitir datos:

Apertura:

* SYN (Synchronize): El cliente envía un paquete SYN al servidor para solicitar la conexión.
* SYN-ACK: El servidor responde con un paquete SYN-ACK indicando que acepta la conexión.
* ACK (Acknowledgment): El cliente envía un paquete ACK para confirmar la conexión.

Cierre:

* FIN: El nodo que desea cerrar la conexión (cliente o servidor) envía un paquete FIN.
* ACK: El receptor del FIN responde con un ACK para confirmar que ha recibido el FIN.
* FIN: El receptor envía su propio paquete FIN cuando esté listo para cerrar la conexión.
* ACK: El primer nodo responde con un ACK para confirmar el cierre.

## DNS:

**Consulta – Respuesta**

El DNS (Domain Name System) traduce nombres de dominio legibles para humanos en direcciones IP numéricas utilizadas por los dispositivos.

Flujo típico:

* Consulta DNS: El cliente envía una solicitud a un servidor DNS para resolver un nombre de dominio (por ejemplo, www.ejemplo.com).
* Respuesta DNS: El servidor DNS responde con la dirección IP correspondiente al nombre de dominio solicitado.

## DHCP:

**Discover – Offer – Request – Acknowledgement (DORA)**

El DHCP (Dynamic Host Configuration Protocol) asigna dinámicamente direcciones IP y otros parámetros de configuración a los dispositivos en una red.

Flujo típico:

* DHCP Discover: El cliente envía una solicitud broadcast buscando servidores DHCP disponibles.
* DHCP Offer: Los servidores DHCP responden ofreciendo una dirección IP y configuración de red.
* DHCP Request: El cliente acepta una de las ofertas y solicita esa configuración específica al servidor.
* DHCP Acknowledgement (ACK): El servidor confirma y asigna la dirección IP al cliente.

## ICMP (Internet Control Message Protocol):

**Echo Request – Echo Reply**

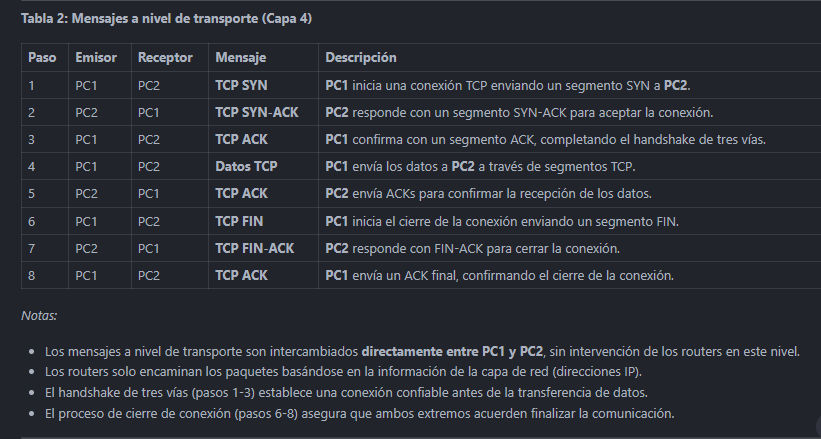
ICMP no establece conexiones; simplemente envía mensajes como ping (Echo Request y Echo Reply).

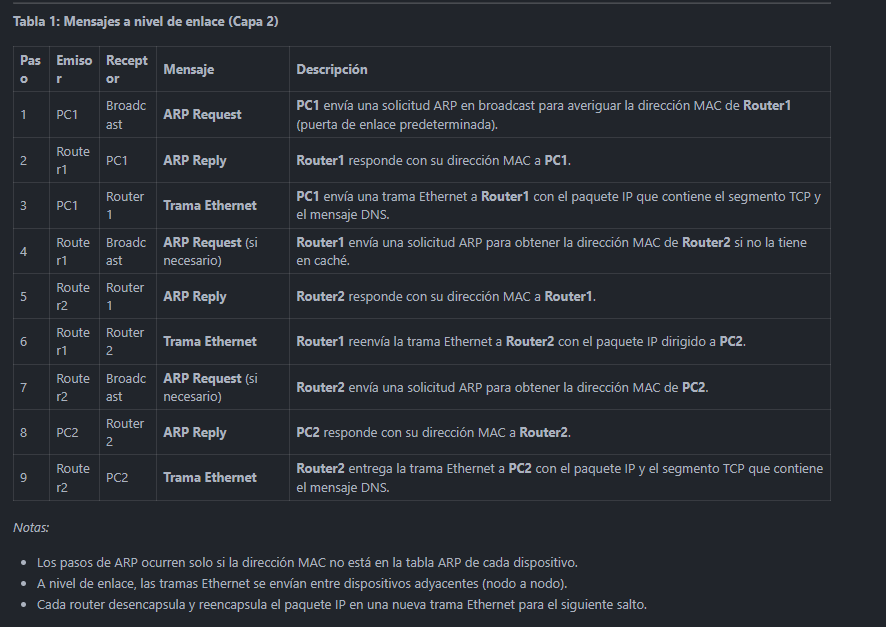
Los mensajes terminan cuando se recibe una respuesta o expira el tiempo.

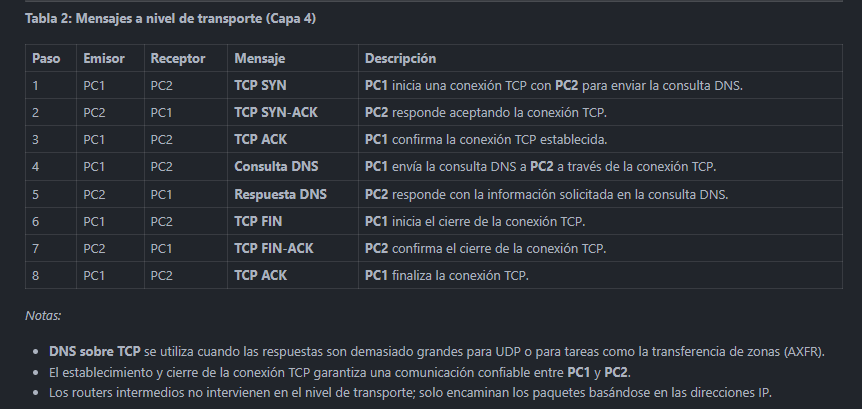
## EJEMPLOS

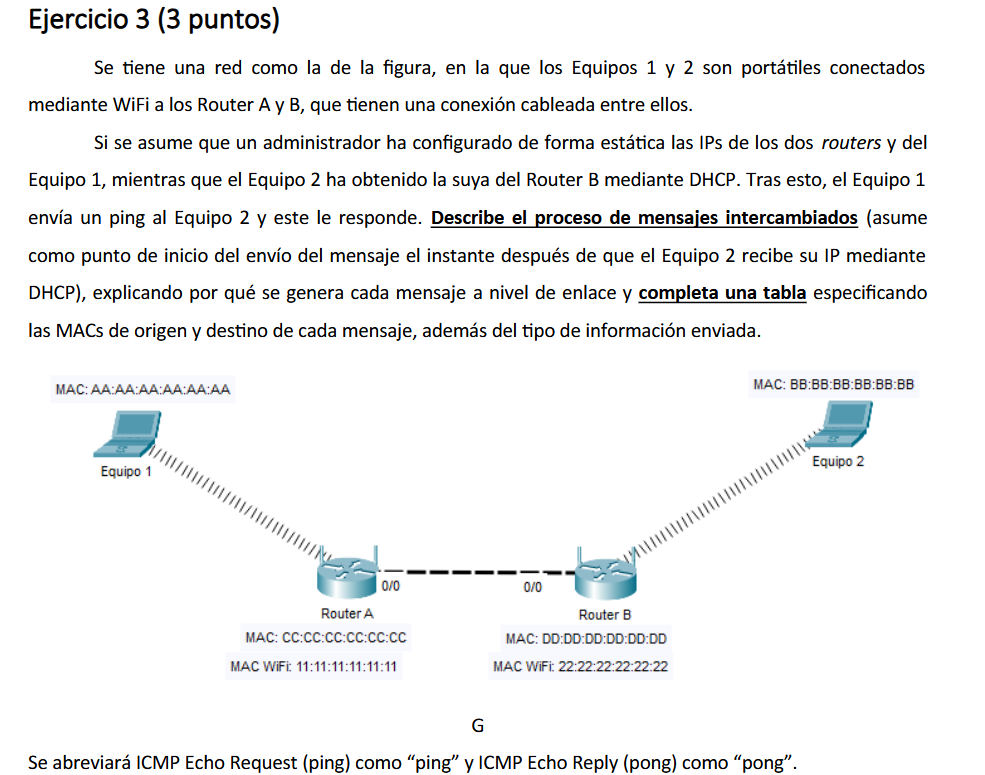
PC1 – ROUTER 1 – ROUTER 2- PC2 (todo por ethernet)

***Mensaje TCP de PC1 a PC2***

***Mensaje DNS por TCP***





No hacemos ARP en wifi, suponemos que equipo1 y router A ya se conocen. Muy largo si no.

|  |  |  |
| --- | --- | --- |
| Origen | Destino | Mensaje |
| E1 | R1 | RTS |
| R1 | E1 | CTS |
| E1 | R1 | Mensaje ping |
| R1 | E1 | ACK |
| R1 | BROADCAST | ARP Request |
| R2 | R1 | ARP Reply |
| R1 | R2 | Mensaje ping |
| R2 | E2 | RTS |
| E2 | R2 | CTS |
| R2 | E2 | Mensaje ping |
| E2 | R2 | ACK |
| E2 | R2 | RTS |
| R2 | E2 | CTS |
| E2 | R2 | Mensaje pong |
| R2 | E2 | ACK |
| R2 | R1 | Mensaje pong |
| R1 | E1 | RTS |
| E1 | R1 | CTS |
| R1 | E1 | Mensaje pong |
| E1 | R1 | ACK |

A nivel de Trasnporte si es TCP

|  |  |  |
| --- | --- | --- |
| Origen | Destino | Mensaje |
| E1 | E2 | TCP SYN |
| E2 | E1 | TCP SYN-ACK |
| E1 | E2 | TCP ACK |
| E1 | E2 | Mensaje ping |
| E2 | E1 | ACK |
| E2 | E1 | Mensaje pong |
| E1 | E2 | ACK |
| E1 | E2 | TCP FIN |
| E2 | E1 | TCP FIN-ACK |
| E1 | E2 | TCP ACK |

# EJEMPLO MENSAJE INVERSO:

