**INSTITUTO POLITÉCNICO NACIONAL**

**ESCUELA SUPERIOR DE CÓMPUTO******

Analizador ARP

***Mora Ayala José Antonio***

***Torres Carrillo Josehf Miguel Angel***

Profesora:

M. en C. NIDIA ASUNCIÓN CORTEZ DUARTE

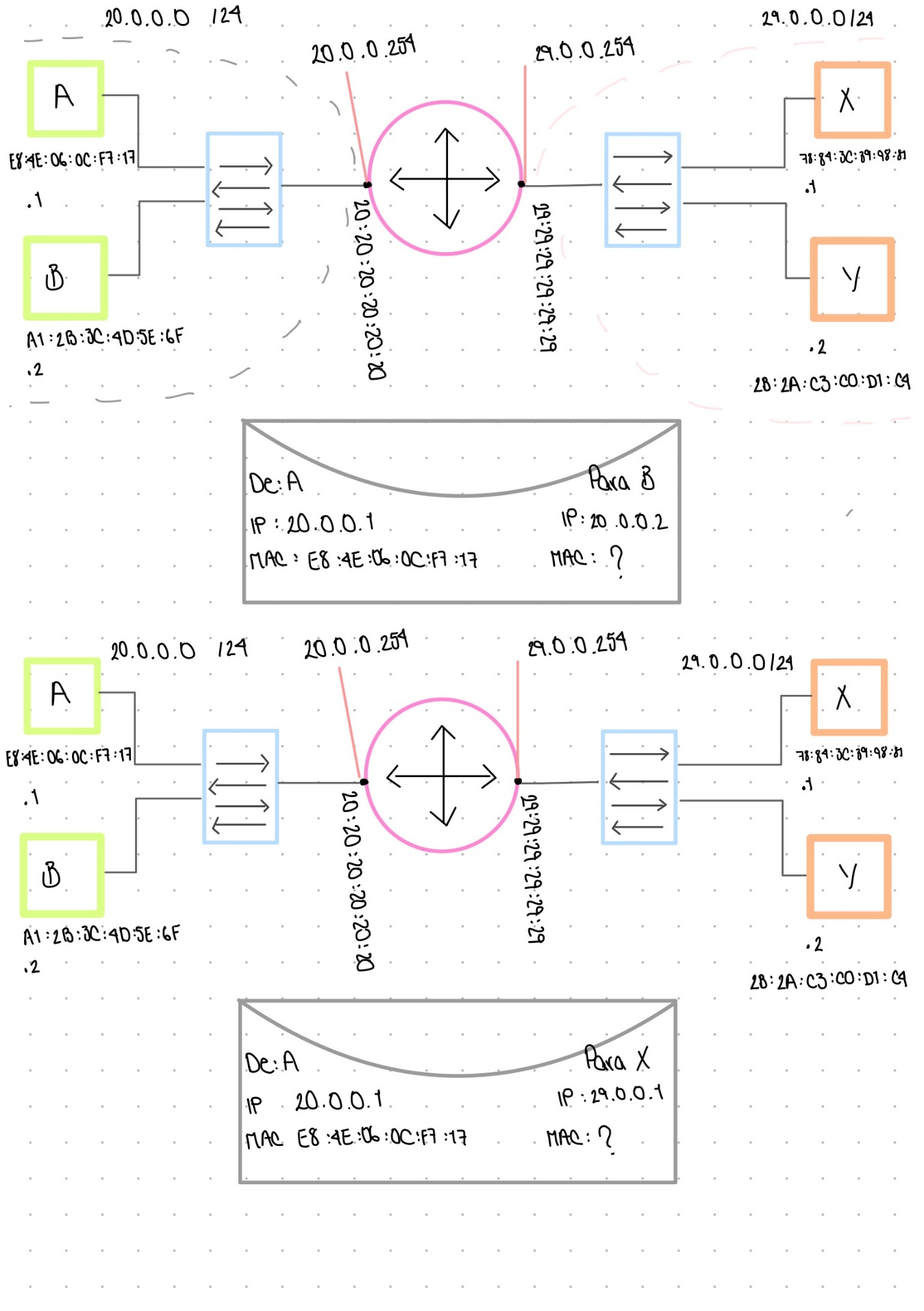
## Siglas ARP

Las siglas ARP significan Protocolo de resolución de direcciones o en ingles Addres Resolution Protocol

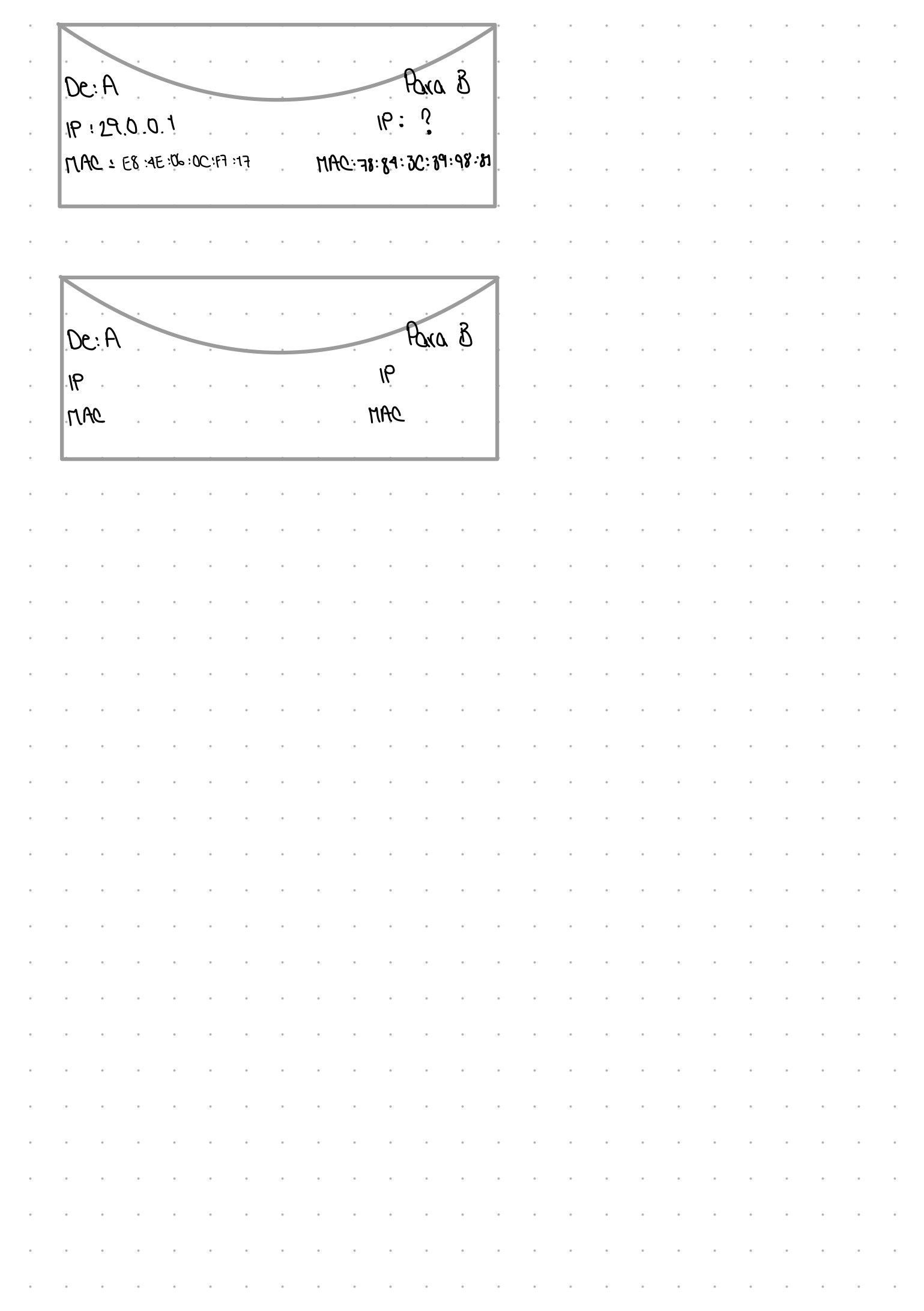
## Descripcion del Protocolo

Este protocolo nos permite obtener el conocimiento de la dirección física de una dirección IP dada, de tal forma que para que las direcciones físicas se puedan conectar con las direcciones lógicas el protocolo ARP va a realizar la interrogante a todos los equipos de la red para averiguar sus direcciones físicas y poder obtener la que se esta requiriendo en ese momento, entonces cuando un equipo debe comunicarse con otro, se realiza una solicitud ARP request con la dirección IP destino a todos los de la red (mediante una dirección de broadcast como destinatario), de tal forma que todos los equipos pertenecientes a este subred puedan comparar la IP destino con la propia en caso de que coincidiera va a mandar la respuesta y si no se encuentra en la misma subred, el remitente se dirige a la puerta de enlace estándar, donde se buscara en todas las tablas de enrutamiento y saldrá por la correspondiente, (la que coincida con la parte correspondiente de la ip) y es momento de volver a mandar un mensaje broadcast buscando la dirección IP adecuada, cuando esta es encontrada responderá y mandara su dirección física .

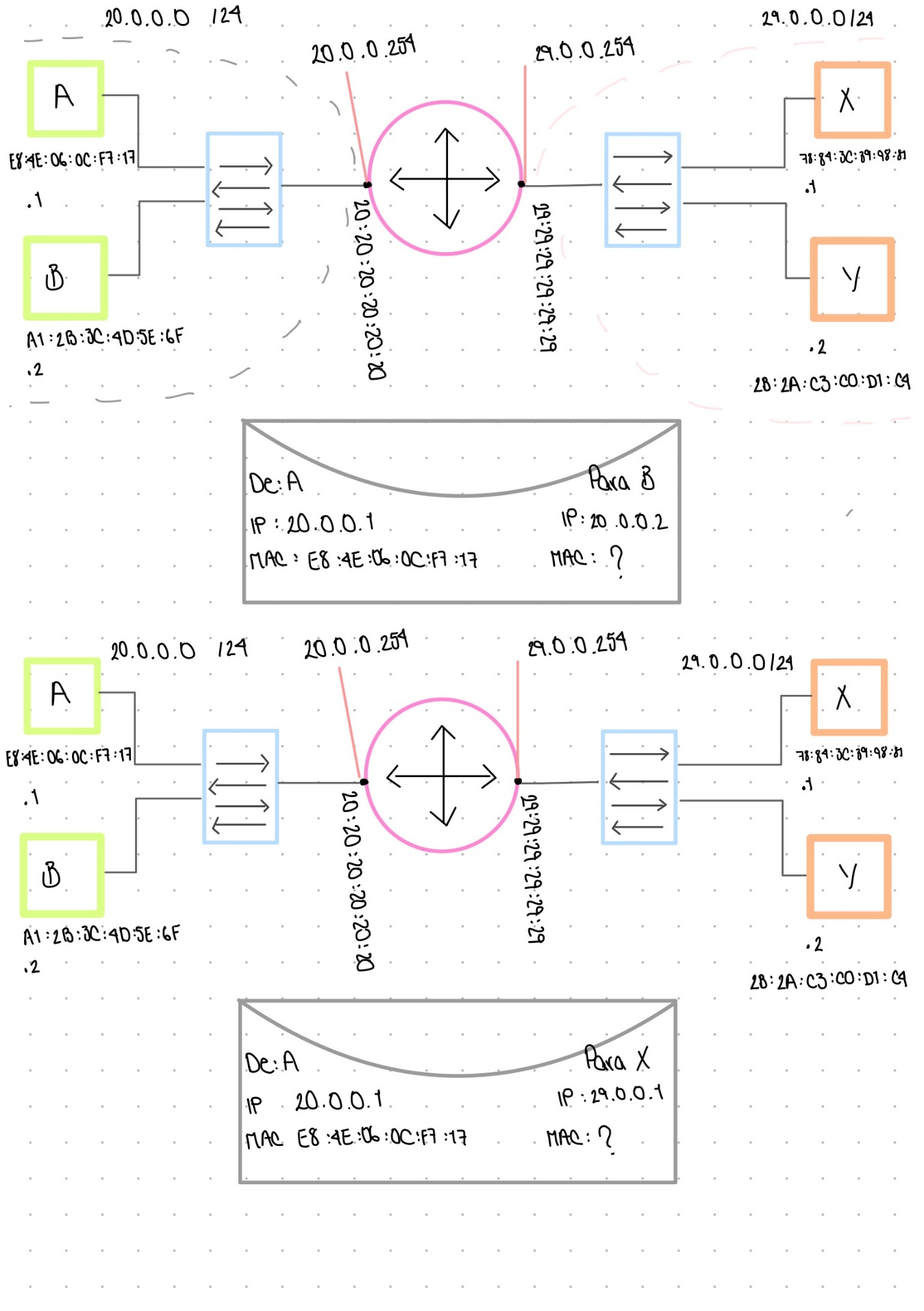
## Dibujar 2 sobres y con ellos explicar la diferencia de arp y arp inverso

ARP tiene 2 formas de enviar y de recibir los datos estos 2 son los modos ARP y ARP inverso, ambos son sencillos perse con un pequeña diferencia entre sí, tenemos el primer sobre, donde conocemos el destino y el origen, conocemos del origen tanto su IP como su dirección MAC, pero en caso contrario no conocemos la dirección MAC de B por ello primero enviaremos mensaje a todos los que se encuentren en nuestra Red, preguntando sobre quien tiene la IP 20.0.0.2, como todos los usuarios dentro de nuestra red tienen una IP única solo uno podrá responder nuestra solicitud, y ahora que sabemos la MAC de destino podemos mandar el mensaje sin ningún problema a nuestro destino

Pero que pasaria si en lugar de conocer la IP conocemos la MAC y no conocemos la IP? Entonces este seria un caso inverso de ARP, donde ahora en lugar de preguntar quien tiene la direccion IP, ahora preguntamos quien tiene la direccion MAC que tenemos, de igual manera la respuesta sera unica, es decir una direccion MAC es igual unica por cada dispositivio, por ello la respuesta unicamente la hara un dispositivo, permitiendo indentificar la MAC y establecer esta conexion

En pocas palabras la diferencia entre un ARP y un ARP inverso es que, en el inverso en lugar de preguntar por la MAC con la IP, preguntaremos la IP con la MAC, es decir en uno conocemos la IP pero no la MAC y en el otro conocemos la MAC pero no la IP

## Poner un escenario (Tú puedes poner las direcciones IP y MAC que gustes)

* Explicar con tus propias palabras cuando se comunicará de A -> B y dibujas el sobre para la solicitud ARP y la respuesta ARP (en el sobre poner las direcciones correspondientes)

Como ya pudimos observar gracias a la previa explicación nos damos cuenta de la forma en que son mandados los mensajes cuando se trata de este tipo de Tramas, la forma de ver esto con sobre resulta bastante práctica, pues nos da una idea gráfica de lo que esta sucediendo al momento de estar realizando el envío de un mensaje con el tipo ARP.

Comenzamos viendo quien es quien desea realizar el envío de información, ya que hemos identificado que se trata de nuestra terminal A y que busca tener una comunicación con B procedemos a realizar las consideraciones necesarias que se llevan a cabo para poder completar esta operación.

Como observamos necesitamos de información indispensable para poder entablar dicha comunicación, gráficamente la conocemos toda, aunque en la realidad no sucede de esta forma.

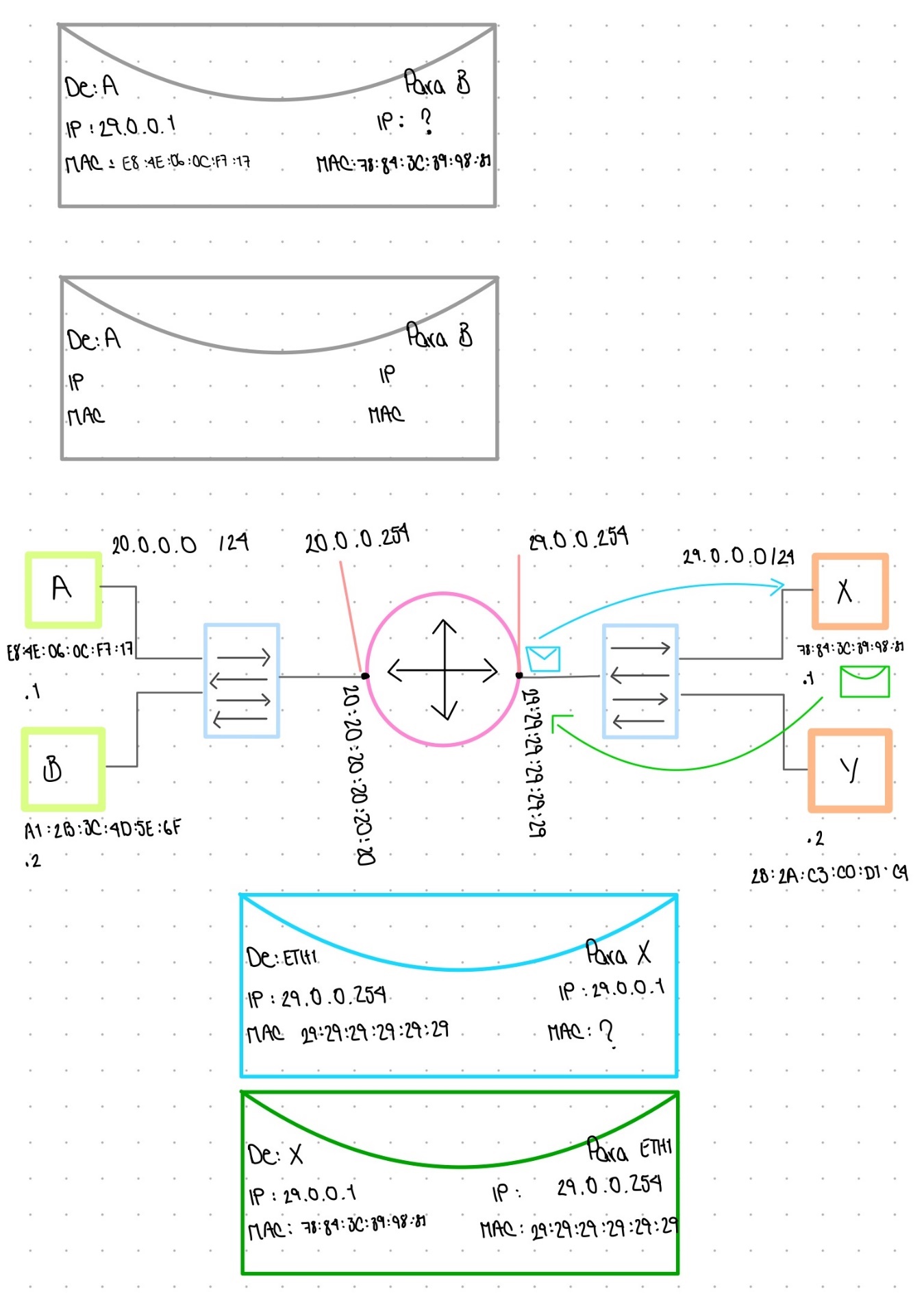
Realmente solo se dispone de

* MAC Origen
* IP Origen
* IP Destino

Como observamos nos falta la **MAC destino** la cual buscamos obtener para entablar la comunicación correspondiente por lo que se procede a mandar el mensaje de forma 1 a Todos, haciendo de cierta forma la pregunta de: “Oigan quiero mandar este mensaje y busco a tal IP (ya que esta si es conocida y es la que nos llevara a poder realizar una búsqueda)”, tal que se realizar un mensaje de tipo BROADCAST ya que como tal desconocemos el especifico de quien debe recibir el mensaje, aunque recordemos que si sabemos la IP en cuestión.

Dado que las IP corresponden al mismo rango como tal el router no interviene en esta operación, pues no es necesario que realice la búsqueda en su tabla, dado que el mensaje no va a salir ya que se encuentran en el mismo rango.

Posteriormente una de todas nuestras terminales conectadas reconoce que le estan buscando mediante la IP especificada, es esta la que realiza la respuesta de tipo **unicast**, quedando como (Origen: B Destino: A), dado que se está realizando la comunicación directa en este momento ya se puede mandar la información completa, pues nuestra terminal B evidentemente conoce su MAC por lo cual al momento de realizar la respuesta a A ya la puede mandar

* Explicar de A -> X (realizar el mismo procedimiento que se solicitó en el punto anterior)

Ya que vimos cómo se manda un ARP en la misma RED ahora lo haremos para cuando el destino se encuentra en otra RED totalmente diferente, para ello lo que haremos será primero mandar una solicitud desde nuestro origen A a todos los miembros de nuestra red mediante broadcast, en este caso como ningún de los miembros de la red tiene la dirección IP que buscamos ninguno va a responder

Ahí es cuando entra nuestro Router con su Default Gateway, como la dirección IP que intentamos buscar no se encuentra en nuestra red interna lo que haremos es mandarle nuestro mensaje al Router mediante su DG, de forma que el mensaje se está enviando a través del Router, esto con el fin de evitar cambios de IP, o incluso cambios de MAC si se cambia el dispositivo, pero la IP sigue siendo la misma

Entonces tendremos un sobre donde nuestro Origen será nuestro dispositivo A, con la dirección IP 20.0.0.1 con la MAC E8:4E:06:0C:F7:17, y nuestra dirección destino será la dirección de IP que buscamos siendo la IP 29.0.0.1 y la dirección MAC que no sabemos

Como no esta en nuestra no obtendremos respuesta directamente de la dirección IP que estamos buscando, en cambio como esto lo tiene que gestionar nuestro Router la respuesta que tendremos de este será de nuestro Router, entonces el sobre correspondiente que tendremos como respuesta para nuestra primera petición será el siguiente donde tenemos como dirección IP origen 20.0.0.254 que es la DG de nuestro Router y tendremos como MAC la siguiente dirección 20:20:20:20:20:20 que es la dirección MAC de nuestro Router y como dirección destino tendremos la dirección del usuario que hizo la petición en este caso tendremos la dirección IP de A que es 20.0.0.1 y su dirección MAC que es la E8:4E:06:0C:F7:17

Como ya vimos no nos fue posible establecer una comunicación con la IP de nuestro destino, dado que el router detecto que no se encontraba en el host, razón por la cual el router revisa la tabla de enrutamiento y se da cuenta dada la ip que recibió que

1. No se encuentra dentro del mismo rango que aquella que realizo el envío de mensaje
2. Que la ip buscada si está en su tabla de enrutamiento por lo cual pasamos a la interfaz de ETH1 (Primer sobre de la imagen)

Ahora nuestra interfaz ETH1 está realizando una comunicación de tipo **Broadcast** buscando a aquella terminal que posee la **IP** deseada en un inicio, dado que nuevamente tenemos la mayoría de la información necesaria del sobre solo hace falta obtener la dirección MAC, la cual es obtenida mediante la respuesta que se da una vez que la terminal se da cuenta que está siendo buscada, cuando esta responde es momento en el cual realiza la inserción de su dirección MAC para que todo el proceso ya pueda ser realizado.

## Colocar una trama ARP de solicitud (Courier new) y la salida de tu programa (captura de pantalla)

Usaremos como trama solicitud una de las tramas de los ejemplos anteriores siendo la siguiente

FF FF FF FF FF FF E8 4E 06 0C F7 17 08 06 00 01  
08 00 06 04 00 01 E8 4E 06 0C F7 17 14 00 00 01  
00 00 00 00 00 00 1D 00 00 01 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

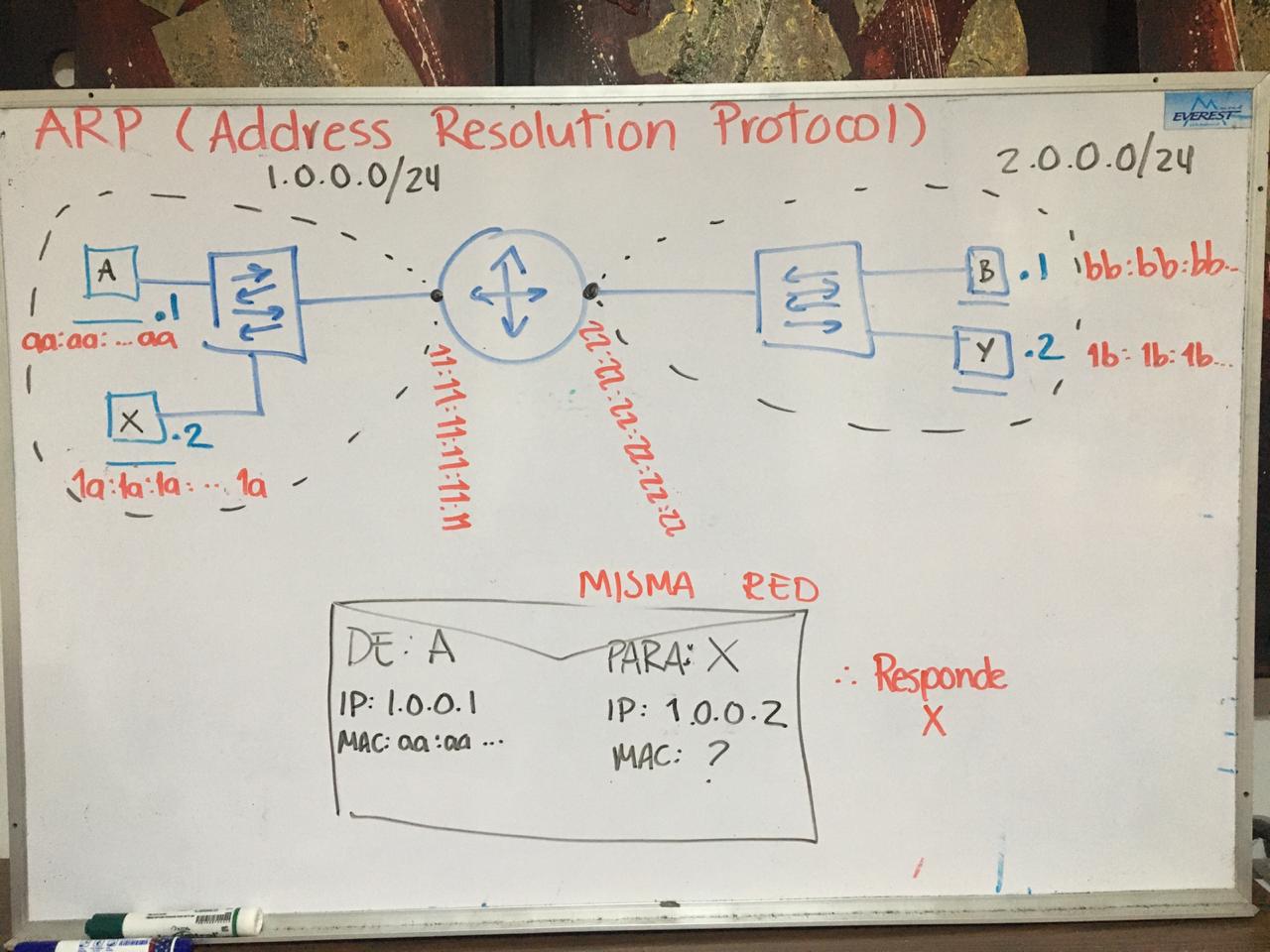
## Colocar una trama ARP (Courier new) y la salida de tu programa (captura de pantalla)

Usaremos la trama de respuesta cuando enviamos un mensaje de A -> X usando la que va de X -> DG Router

29 29 29 29 29 29 78 84 3C 39 98 81 08 06 00 01  
08 00 06 04 00 02 78 84 3C 39 98 81 1D 00 00 01  
29 29 29 29 29 29 1D 00 00 FE 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente



ARP SOLICITUD (Alicia ->TODOS ) Broadcast

FF FF FF FF FF FF AA AA AA AA AA AA 08 0600 01

08 00 06 04 00 01 AA AA AA AA AA AA 01 00 00 01

00 00 00 00 00 00 01 00 00 02 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

ARP RESPUESTA (Ximena - > Alicia ) Unicast

AA AA AA AA AA AA 1A 1A 1A 1A 1A 1A 08 06 00 01

08 00 06 04 00 02 1A 1A 1A 1A 1A 1A 01 00 00 02

AA AA AA AA AA AA 01 00 00 0100 00 00 00 00 00

Texto

Descripción generada automáticamente00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ARP DISTINTAS REDES

PRIMERA PARTE

ARP SOLICITUD (ALICIA -> TODOS)

FF FF FF FF FF FF AA AA AA AA AA AA 08 0600 01

08 00 06 04 00 01 AA AA AA AA AA AA 01 00 00 01

00 00 00 00 00 00 02 00 00 02 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

ARP RESPUESTA (DG ROUTER1 (ETH0) -> ALICIA)

AA AA AA AA AA AA 11 11 11 11 11 11 08 0600 01

08 00 06 04 00 02 11 11 11 11 11 11 01 00 00 FE

AA AA AA AA AA AA 01 00 00 01 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

SEGUNDA PARTE

ARP SOLICITUD (DG ROUTER2 (ETH1) -> TODOS)

FF FF FF FF FF FF 22 22 22 22 22 22 08 06 00 01  
08 00 06 04 00 01 22 22 22 22 22 22 02 00 00 FE  
00 00 00 00 00 00 02 00 00 02 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

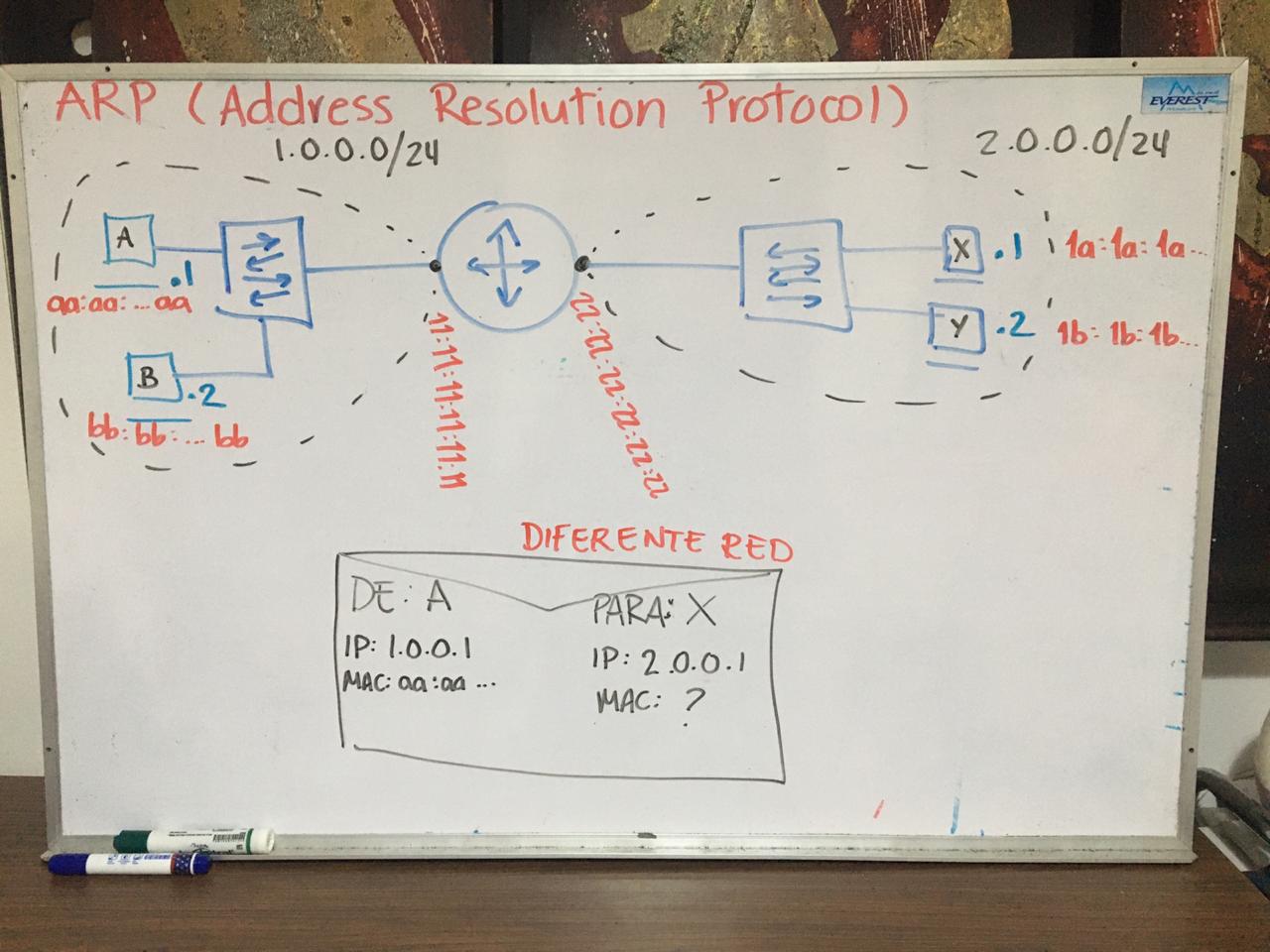
ARP RESPUESTA (YOYIS -> DG ROUTER2 (ETH1))

22 22 22 22 22 22 1B 1B 1B 1B 1B 1B 08 06 00 01  
08 00 06 04 00 02 1B 1B 1B 1B 1B 1B 02 00 00 02  
22 22 22 22 22 22 02 00 00 FE 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente



Construir las primeras tramas (DIFERENTE RED – salto 1)

ARP SOLICITUD (Alicia - > TODOS )

FF FF FF FF FF FF AA AA AA AA AA AA 08 0600 01

08 00 06 04 00 01 AA AA AA AA AA AA 01 00 00 01

00 00 00 00 00 00 02 00 00 0100 00 00 00 00 00

Texto

Descripción generada automáticamente00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ARP RESPUESTA (DG router -> Alicia )

AA AA AA AA AA AA 11 11 11 11 11 11 08 06 00 01

08 00 06 04 00 02 11 11 11 11 11 11 01 00 00 02

AA AA AA AA AA AA 01 00 00 0100 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

Construir las primeras tramas (DIFERENTE RED – salto 2)

ARP SOLICITUD (router - > TODOS en red 2.0.0.0 )

FF FF FF FF FF FF 22 22 22 22 22 22 08 0600 01

08 00 06 04 00 01 22 22 22 22 22 22 02 00 00 FE

00 00 00 00 00 00 02 00 00 0100 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Texto

Descripción generada automáticamente

ARP RESPUESTA (Ximena -> DG router )

22 22 22 22 22 22 1A 1A 1A 1A 1A 1A 08 06 00 01

08 00 06 04 00 02 1A 1A 1A 1A 1A 1A 02 00 00 01

22 22 22 22 22 22 02 00 00 FE00 00 00 00 00 00

Texto

Descripción generada automáticamente00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00