Práctica 5

Capa de Enlace

**1. ¿Qué función cumple la capa de enlace? Indique qué servicios presta esta capa.**

La capa de enlace es la responsable de la transferencia fiable de información a través de un circuito de trasmisión de datos. Recibe peticiones de la capa de red y utiliza los servicios de la capa física. El objetivo de la capa de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente. Entre los posibles servicios que un protocolo de la capa de enlace pueden ofrecer se incluyen:

* Entramado: casi todos los protocolos de la capa de enlace encapsula cada datagrama de la capa de red dentro de una trama de la capa de enlace antes de transmitirla a través del enlace. Una trama consta de un campo de datos, en el que se inserta el datagrama de la capa de red, y de una serie de campos de cabecera.
* Acceso al enlace: un protocolo de control de acceso al medio (MAC, Medium Access) especifica las reglas que se utilizan para transmitir una trama a través del enlace.
* Entrega fiable: cuando un protocolo de la capa de enlace proporciona un servicio de entrega fiable, garantiza que va a transportar cada datagrama de la capa de red a través del enlace sin que se produzcan errores.
* Control de flujo: los nodos situados en cada extremo de un enlace tiene una capacidad limitada de almacenamiento en buffer de las tramas. Esto puede ser un problema cuando el nodo receptor puede recibir las tramas a más velocidad de las que puede procesarlas. Sin el control de flujo, el buffer del receptor puede desbordarse con lo que las tramas se perderían.
* Detección de errores: el hardware de la capa de enlace en un nodo receptor pudiera llegar a decidir, incorrectamente, que un bit contenido en una trama es 0 cuando fue transmitido como 1, y viceversa. Dichos errores de bit se introducen debido a la atenuación de las señales y ruido electromagnético. Puesto que no existe ninguna necesidad de reenviar un datagrama que contenga error, muchos protocolos de la capa de enlace proporcionan un mecanismo para detectar dichos errores de bit.
* Corrección de errores: la corrección de errores es similar a la detección de errores, salvo porque el receptor no solo detecta si hay bits erróneos en la trama, sino que también determina exactamente en qué puntos de la trama se han producido errores (y luego corrige esos errores).
* Semiduplex y full-duplex: con la transmisión full-duplex, los nodos de ambos extremos de un enlace pueden transmitir paquetes al mismo tiempo. Sin embargo, con la transmisión semiduplex un mismo nodo no puedo trasmitir y recibir al mismo tiempo.

**2. Compare los servicios de la capa de enlace con los de la capa de transporte**

Muchos de los servicios proporcionados por la capa de enlace presentan notables paralelismos con los servicios proporcionados en la capa de transporte.

Por ejemplo, tanto la capa de enlace como la capa de transporte pueden proporcionar un servicio de entrega fiable. Aunque los mecanismos para garantizar una entrega fiable en las dos capas son similares, los dos servicios de entregas fiables no son idénticos.

Un protocolo de transporte proporciona una entrega fiable de segmentos entre dos procesos, en modo terminal a terminal; un protocolo de la capa de enlace fiable proporciona una entrega fiable de tramas entre dos nodos conectados por un único enlace.

De forma similar, los protocolos de la capa de transporte como los de la capa de enlace pueden proporcionar servicios de control de flujo y detección de errores, pero de nuevo el control de flujo en un protocolo de la capa de transporte se proporciona en modo terminal a terminal, mientras que un protocolo de la capa de enlace se proporciona entre dos nodos adyacentes.

**3. Direccionamiento Ethernet:**

**• ¿Cómo se identifican dos máquinas en una red Ethernet?**

Se identifican mediante una dirección MAC (media acces control).

**• ¿Cómo se llaman y qué características poseen estas direcciones?**

Esta dirección consta de 6 bytes de longitud, lo que da 2^48 posibles direcciones de MAC. Suelen expresarse en notación hexadecimal, indicándose cada byte de la dirección mediante una pareja de números hexadecimales. Una propiedad de las direcciones MAC es que nunca puede haber dos adaptadores con la misma dirección, para esto la IEEE se encarga de gestionar el espacio de direcciones MAC.

**• ¿Cuál es la dirección de broadcast en capa de enlace? y ¿que función cumple?**

Broadcast es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo. Es posible la difusión de cualquier trama de datos a todas las paradas que se encuentren en el mismo segmento de la red. Para ello, se utiliza una dirección MAC especial. En el caso de Ethernet realiza la difusión recibiendo tramas con dirección MAC de destino FF.FF.FF.FF.FF.FF.

**4. ¿Que dispositivos dividen dominios de broadcast?**

Dividen dominios de broadcast: router

Dividen dominios de colisión: switch/bridge (cada puerto es un dominio de colisión distinto), router

**5. Dispositivos de capa de enlace:**

**• Enumere dispositivos de capa de enlace**

Hub

Switch

**• ¿Cuál es la función de un HUB?**

Un Hub es un dispositivo de la capa física: ingresa una señal por una interfaz, y la distribuye por el resto incrementando normalmente la potencia -actúa como un repetidor-. No interpreta la señal que repite. No realiza almacenamiento ni reenvío (no tiene buffers). No implementa CSMA/CD, por lo cual pueden producir colisiones. Permite interconectar segmentos de LAN siempre que utilicen la misma tecnología Ethernet (no puede interconectar 10Base2 con 100BaseT por ejemplo), pero forma un **único dominio de colisión**.

**• ¿Qué es una colisión?**

Una colisión ocurre cuando dos nodos trasmiten tramas al mismo tiempo, o sea que las tramas transmitidas colisionan en todos los receptores, y ninguno de los nodos receptores puede interpretar ninguna de las tramas recibidas. En cierto sentido, las señales de las tramas que han colisionados se entremezclan y no pueden separarse.

**• ¿Qué diferencia existe entre la operación de un HUB y la de un Switch?**

El Switch, a diferencia del HUB, envía los datos provenientes de la computadora de origen solamente a la computadora de destino. Esto se debe a que los switches crean una especie de canal de comunicación exclusiva entre el origen y el destino. **De esta forma, la red no queda "limitada" a una única computadora en el envío de información**. Esto aumenta la performance de la red ya que la comunicación está siempre disponible.

**• ¿Cuales de estos dividen dominios de colisión?**

Los switches (por cada puerto que tiene es un dominio de colisión distinto) y los routers dividen los dominios de colisión.

**6. Describa el algoritmo de acceso al medio en Ethernet. ¿Es orientado a la conexión?**

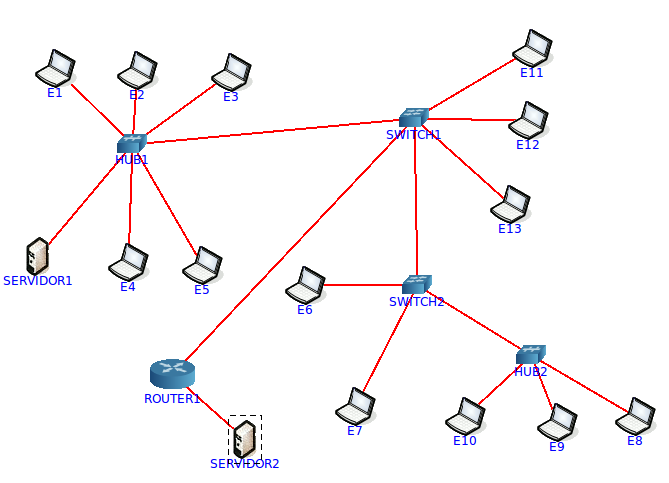
En Ethernet se utiliza un canal simple de difusión compartida, con acceso aleatorio: si dos nodos transmiten a la vez hay una colisión de la que deben recuperarse. Deben coordinarse utilizando el mismo canal que para transmitir (es *in-line*). El algoritmo de acceso al medio es **CSMA/CD** (Carrier Sense Multiple Access with Colision Detect).

CSMA/CD opera de la siguiente manera:

1. Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
2. Si en el medio ninguna otra estación está transmitiendo, se envía la transmisión.
3. Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.
4. Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.
5. Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
6. Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.
7. Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Ethernet NO es orientado a conexión (no hay handshaking) y NO es confiable (no hay acks/nacks). Eficiente con baja carga -habrá pocas colisiones-.

**7.**

****

1) ¿Quién escucha el mensaje si:

A) **La estación E1 envía una trama al servidor SERVIDOR1**

La trama es escuchada por todos los nodos pertenecientes a la primera trama LAN menos la estación que envía el mensaje ( E2, E3, E4, E5 y SERVIDOR1 y el SWITCH1). El HUB1 es un dispotivo de capa 1, por lo tanto no conoce lo que es una trama.

Si el SWITCH1 no tiene SERVIDOR1 en su tabla de asociación de puertos, entonces aplica la función de flooding.

B) **La estación E1 envía una trama a la estación E11**

El mensaje es escuchado por la primera trama LAN menos la E1 que envía, y la estación E11 (pasando por el SWITCH1 )

Si el SWITCH1 no conoce el puerto por el que enviar el mensaje a E11, entonces mandara un pedido por todos los puertos menos por el que le llegó el mensaje (E12 y E13)

C) **La estación E1 envía una trama a la estación E9**

El mensaje lo escuchan: E2, E3, E4, E5, SERVIDOR1, y pasando por SWITCH1 y SWITCH2: HUB2, E8, E9, E10

D) **La estación E4 envía una trama a la MAC de broadcast**

El mensaje lo escuchan todos los nodos, menos el SERVIDOR2.

El router separa dominios de broadcast.

El switch/bridge y hub responden a un único dominio de broadcast.

E) **La estación E6 envía una trama a la estación E7**

El mensaje lo escucha el nodo E7 (pasando por SWITCH2)

F) **La estación E6 envía una trama a la estación E10**

El mensaje lo escuchan los nodos E8, E9 y E10 (pasando por SWITCH2 y HUB2)

2) ¿En qué situaciones se pueden producir colisiones?

Se producen colisiones dentro de los dominios dados de los hubs si dos nodos transmiten al mismo tiempo. EJ:

* E1, E2, E3, E4, E5, SERVIDOR1 transmiten al mismo tiempo o transmiten al mismo tiempo que llega una trama desde SWITCH1
* E8, E9, E10 transmiten al mismo tiempo o transmiten mientras llega una trama desde SWTICH2
* E11, E12, E13 transmiten al mismo tiempo o transmite mientras llega una trama desde SWITCH1
* E6 transmite al mismo tiempo que llega una trama desde SWITCH2
* E7 transmite al mismo tiempo que llega una trama desde SWITCH2
* SWITCH1 y SWITCH2 transmiten entre sí al mismo tiempo

**8.**

**II.**

a) Si se pueden ver los pings

b) No se pueden ver. En PC3\_hub no se deberia poder ver algo ya que pertenecen a diferentes dominios en el switch

c) El ping lo reciben PC1\_hub, PC3\_hub y el router

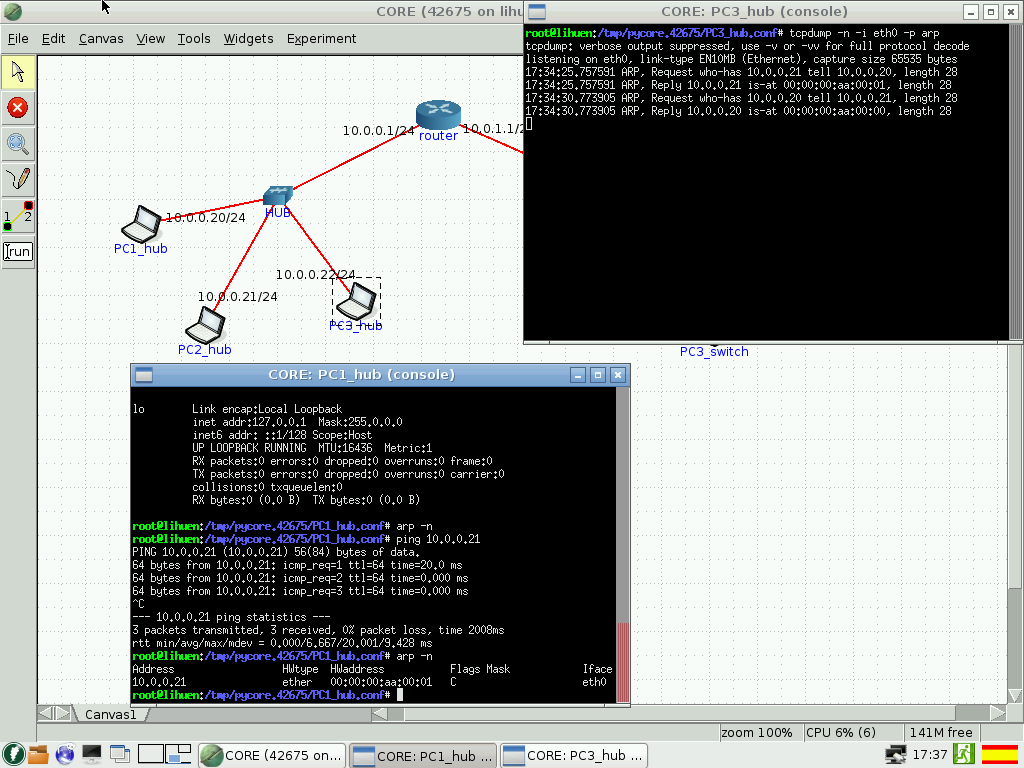
**9. ¿Cuál es la finalidad del protocolo ARP?**

El Protocolo de Resolución de Direcciones (**ARP**) permite la traducción entre los direccionamientos IP (de capa de *red)* y MAC (de capa de *enlace)*, **dentro de una misma LAN**. Se implementa con una tabla MAC->IP en cada host, incluyendo un TTL.  
Para enviar un datagrama IP de un host a otro, es preciso conocer tanto su dirección IP como su MAC. ARP permite obtener el último, consultando en la tabla. Si no se encuentra en la tabla, hay dos opciones:

* Que el destino sea del mismo segmento/subred: Se averigua la MAC con una consulta ARP al broadcast físico indicando la IP, y el adaptador que reconoce la IP destino responde con su MAC, que es agregada a la tabla del emisor
* Que esté en un segmento de red diferente (al aplicar la máscara de (sub)red, se obtiene una dirección distinta a la del origen): En este caso se envía el frame al gateway, que luego continúa retransmitiéndolo. El datagrama en el interior del frame contiene la IP del destino, pero el frame contiene la MAC del gateway (si no la conoce, utiliza ARP para solicitarla). Al enviarse el frame, es recibido por el router, sube a su capa de *red* y al ver una IP destino distinta de la suya, vuelve a bajar a *enlace* para ser retransmitida al próximo router que corresponda según la tabla de ruteo. Eventualmente un router conocerá al equipo destino, y le enviará el datagrama con la MAC correcta -si no la conoce, utiliza ARP-.

Al utilizar la dirección de broadcast para obtener la información que precisa, ARP es un protocolo *plug-and-play* (no precisa configuración).

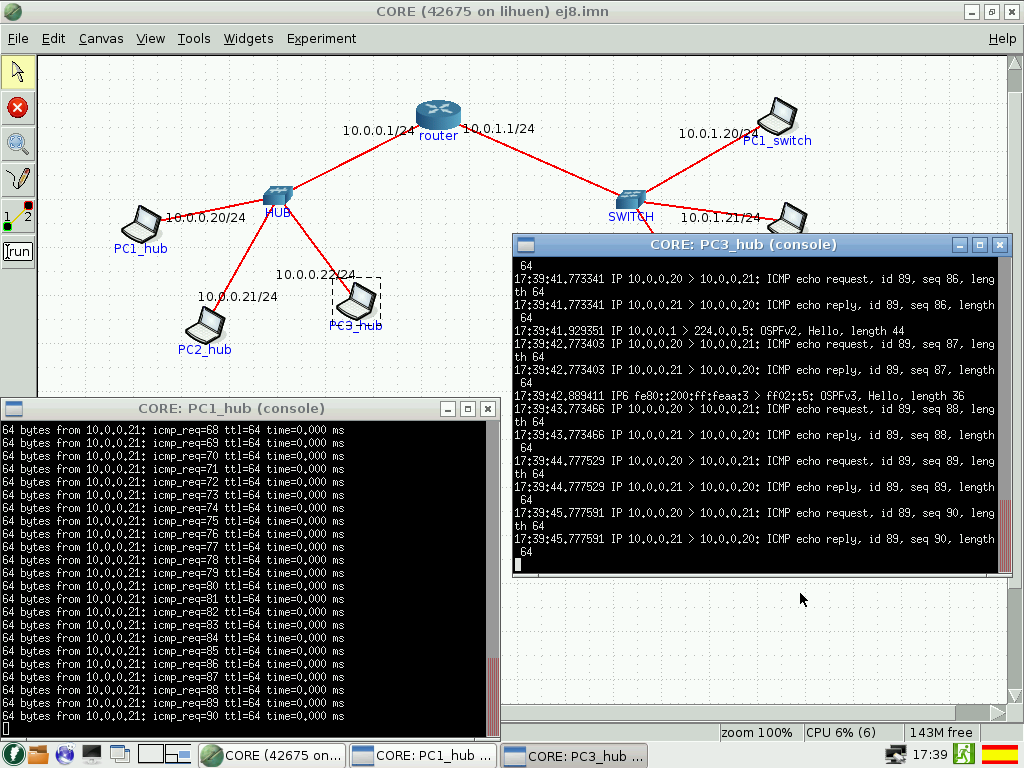
**10.**

**I.**

**En PC3\_hub se pudo capturar los ARP Request y ARP Reply para las PC1\_hub y PC2\_hub.**

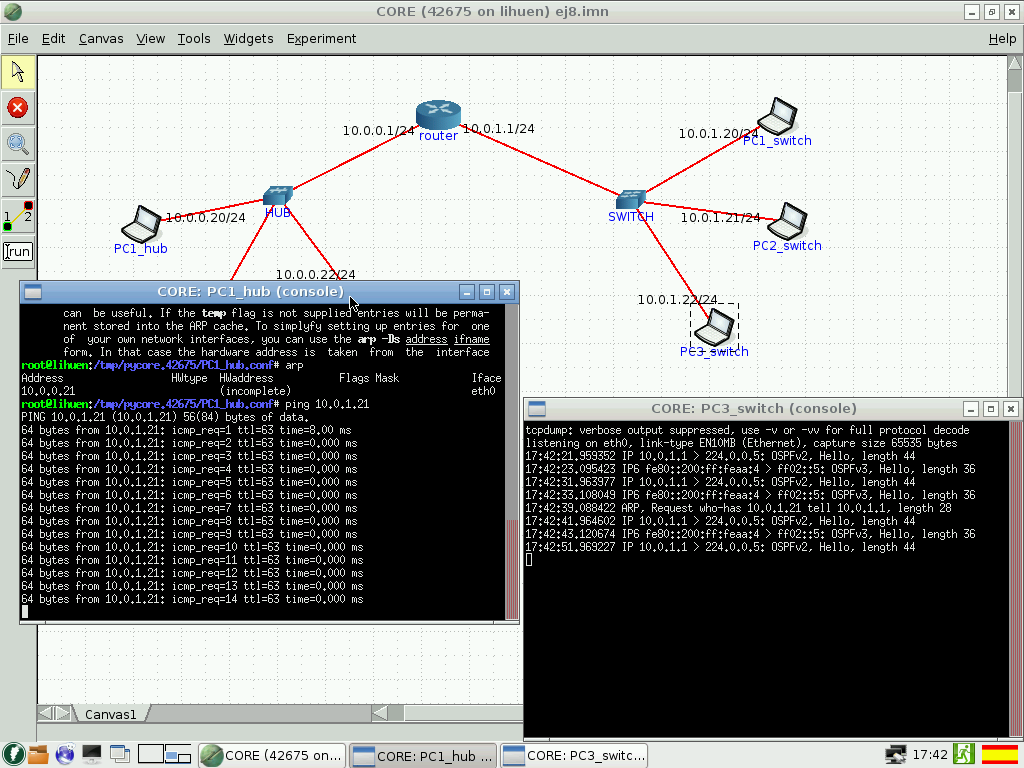
**Se envian dos requerimientos ARP: para saber MAC de PC2\_hub y luego para contestar a la MAC de PC1\_hub**

**II.**

****

**En PC3\_hub se pudieron capturar los mensajes ICMP echo request y echo reply entre las PC1\_hub y PC2\_hub.**

**Esto es debido a que están conectados mediante un HUB, que envía los mensajes por todos sus puertos.**

****

**III.**

**En PC3\_switch se pudo capturar el mensaje ARP Request que requiere la MAC de PC2\_switch.**

**Este mensaje se puede ver en PC3\_switch ya que los ARP son transmitidos en broadcast por el SWITCH. La respuesta no es capturada en PC3\_switch.**

**11. Si la PC A esta en una red y se quiere comunicar con la PC B que está en otra red:**

* **¿Como se da cuenta la PC A de esto?**

La PC A se da cuenta de esto al aplicar la máscara de red a la dirección IP de PC B y comparando con su dirección de red

* **Si la tabla ARP de la PC A esta vacía, ¿que dirección MAC necesita la PC A para poder comunicarse con la PC B?**

La PC A necesita la dirección MAC del default gateway (router) para poder comunicarse con la PC B. A la PC A no le interesa saber la MAC de PC B.

* **En base a lo anterior, ¿que dirección IP destino tiene el requerimiento ARP? ¿es la dirección IP del default gateway o es la dirección IP de la PC B?**

El requerimiento ARP de PC A tiene como ip destino la IP de la PC B a la que se quiere comunicar.

* **Ejecute de nuevo el experimento de ser necesario y complete los campos:**
* **Trama Ethernet: MAC origen:** MAC PC A

**MAC destino:** MAC ROUTER (si no la tiene en su tabla ARP, la pide)

* **Solicitud ARP: MAC origen:** MAC PC A

**MAC destino:** MAC ROUTER ?

**IP origen:** IP PC A

**IP destino:** IP PC B

* **En base a lo anterior, indique la información de capa 2 y 3 del ICMP ECHO REQUEST que la PC A le envía a la PC B cuando ejecuta un ping, en el segmento de LAN de la PC B**

El ICMP Echo Request tendrá la información:

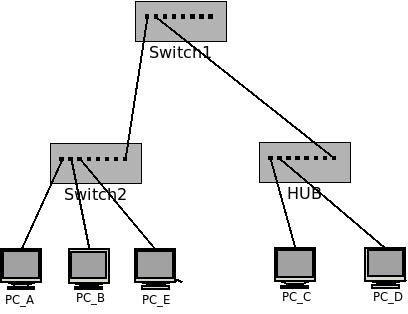
ip origen: ip PC A

ip destino: ip PC B

MAC origen: MAC de router, o de PC A?

MAC destino: MAC de PC B

**12.**

1. Hay 5 dominios de colisión

PC\_A – SWITCH2

PC\_B – SWITCH2

PC\_E – SWITCH2

SWITCH2 – SWITCH1

PC\_C – PC\_D (un grupo HUB)

1. Hay un único dominio de broadcast. Solo los routers separan broadcasts.
   1. **A envía una solicitud ARP consultando la MAC de C**  
      SWITCH2 += MAC A

SWITCH1 += MAC A

* 1. **C responde esta solicitud ARP**

SWITCH1 += MAC C

SWITCH2 += MAC C

* 1. **A envía una solicitud ARP consultando la MAC de B**

No se agrega la MAC de A en SWITCH 2(a menos que se haya vencido el TTL de la MAC A, en cuyo caso se agrega de nuevo)

* 1. **B responde esta solicitud ARP**

SWITCH2 += MAC B

1. Si la PC E y la PC D hubiesen estado realizando un tcpdump para escuchar todo lo que pasa por su interfaz de red, ¿Cuáles de los requerimientos/respuestas anteriores hubiesen escuchado cada una?

La PC E hubiera escuchado:

ARP Request de MAC PC\_C

ARP Request de MAC PC\_B

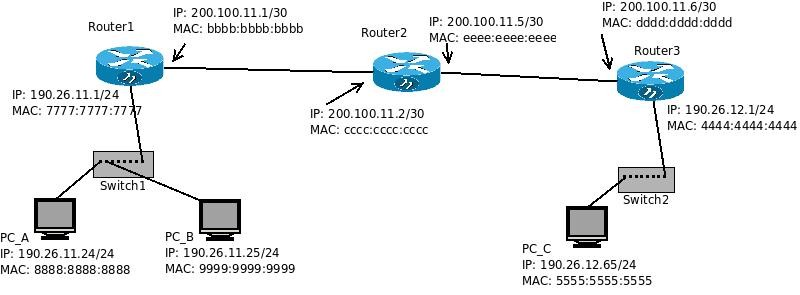
La PC D hubiera escuchado:

ARP Request de MAC PC\_C

ARP Reply a PC\_A

ARP Request de MAC PC\_B

**13.**

****

**Suponiendo que todas las tablas ARP están vacías, tanto de PCs como de Routers. Si la PC\_A le hace un ping a la PC\_C, indique:**

* **¿En que dominios de broadcast hay tráfico ARP?**

Hay tráfico ARP en los 4 dominios de broadcast

* **¿En qué dominios de broadcast hay tráfico ICMP?**

Hay tráfico ICMP en los 4 dominios de broadcast

* **¿Cuál es la secuencia correcta en la que se suceden los anteriores?**

1. PC\_A hace un ARP Request para saber la MAC de Router1
2. Router1 hace un ARP Reply para devolver su MAC a PC\_A
3. PC\_A envía datagrama ICMP Echo Request a la ip de PC\_C:

IP destino: IP PC\_C

MAC destino: MAC Router1

IP origen: IP PC\_A

MAC origen: MAC PC\_A

1. Router1 hace un ARP Request para saber la MAC de Router2
2. Router2 hace un ARP Reply con su MAC para Router1
3. Router1 envía el datagrama ICMP cambiando la MAC origen por la suya propia y la MAC destino a la del Router2 **(no cambia la capa 3)**
4. Router2 hace un ARP Request para saber la MAC de Router3
5. Router3 hace un ARP Reply con su MAC para Router2
6. Router2 envía el datagrama ICMP cambiando la MAC origen por la suya y la MAC destino por la del Router3
7. Router3 detecta que la ip destino está en su misma subred. Hace un ARP Request para saber la MAC de PC\_C
8. PC\_C hace un ARP Reply para el Router3
9. Router3 envía el datagrama a PC\_C modificando la MAC origen por la suya y la MAC destino por la de la PC\_C. **La capa 3 no se modifica (ip origen, ip destino)**

* **Para los paquetes ICMP que haya identificado:**
* **Especifique las direcciones (origen/destino) de capa 2 en los distintos dominios de broadcast.**
* **Especifique las direcciones (origen/destino) de capa 3 en los distintos dominios de broadcast.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Protocolo** | **Tipo** | **Dominio de Broadcast** | **MAC Origen** | **MAC Destino** | **IP Origen** | **IP Destino** |
| ICMP | ECHO request | 1 | 8888:8888:8888 | 7777:7777:7777 | 190.26.11.24/24 | 190.26.12.65/24 |
| ICMP | ECHO request | 2 | bbbb:bbbb:bbbb | cccc:cccc:cccc | 190.26.11.24/24 | 190.26.12.65/24 |
| ICMP | ECHO request | 3 | eeee:eeee:eeee | dddd:dddd:dddd | 190.26.11.24/24 | 190.26.12.65/24 |
| ICMP | ECHO request | 4 | 4444:4444:4444 | 5555:5555:5555 | 190.26.11.24/24 | 190.26.12.65/24 |
| ICMP | ECHO reply | 4 | 5555:5555:5555 | 4444:4444:4444 | 190.26.12.65/24 | 190.26.11.24/24 |
| ICMP | ECHO reply | 3 | dddd:dddd:dddd | eeee:eeee:eeee | 190.26.12.65/24 | 190.26.12.65/24 |
| ICMP | ECHO reply | 2 | cccc:cccc:cccc | bbbb:bbbb:bbbb | 190.26.12.65/24 | 190.26.12.65/24 |
| ICMP | ECHO reply | 1 | 7777:7777:7777 | 8888:8888:8888 | 190.26.12.65/24 | 190.26.12.65/24 |

**13.**

Para calcular el bit de paridad se cuentan la cantidad de unos en el dato

En paridad par:

Si cantidad de 1's es par: 0

Si cantidad de 1's es impar: 1

En paridad impar:

Si cantidad de 1's es par: 1

Si cantidad de 1's es impar: 0

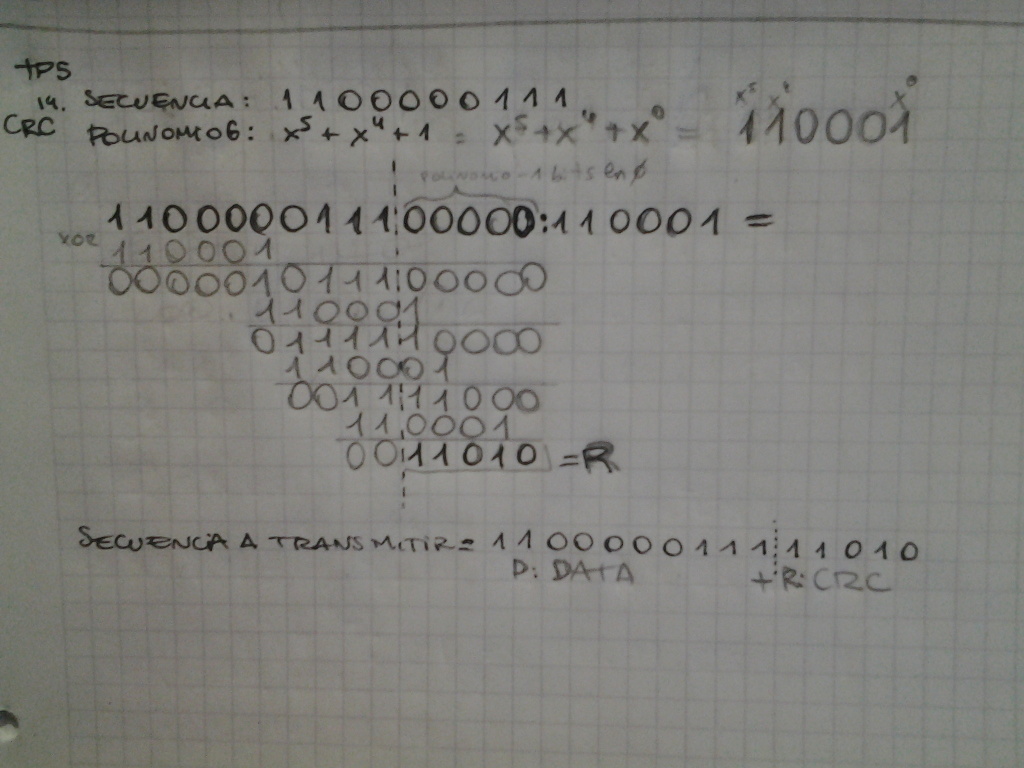
Se trata de agregar un bit al final del dato de modo que el número ahora sea par o impar según la paridad elegida.

(a) **11**0**1**0**11**0**1**0**1**00**1111**  Paridad par: 1 Paridad impar: 0

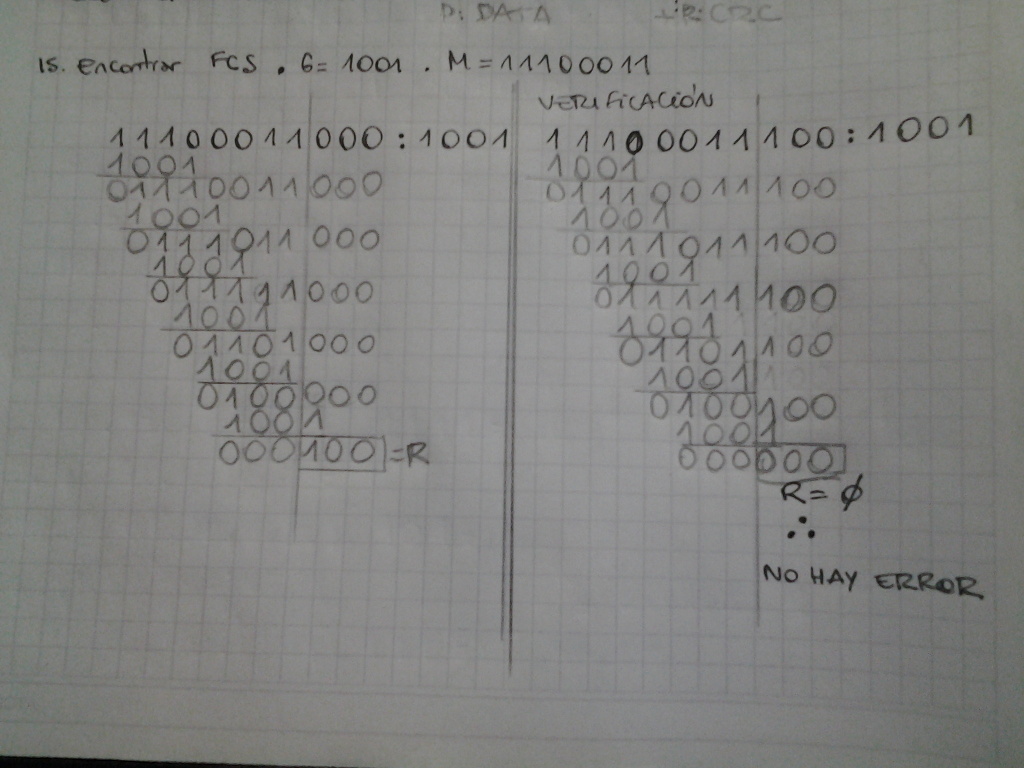
(b) 0**1**0**111**0**1**0**11**0000**1**0 Paridad par: 0 Paridad impar: 1

(c) 00**1**000**1**000**1**000**111** Paridad par: 0 Paridad impar: 1

**14.**

****

**15.**

****

**16. Indicar si es verdadero o falso. Justifique su respuesta**

**(a) Si se utiliza paridad par y se invierte el valor de 2 bits a causa de errores en la transmisión, el receptor detectará el error.**

FALSO. La inversión de una cantidad par de bits no es detectable bajo ningún esquema de paridad.

**(b) 00101011 es un valor válido para ser usado como polinomio generador y el resto sería de 7 bits de longitud.**

FALSO. El polinomio debe ser de la forma x + 1, es decir que comience con 1. Ej: 101011

**(c) Los FCS calculados con el polinomio generador 11001 tendrán una longitud de 4 bits**

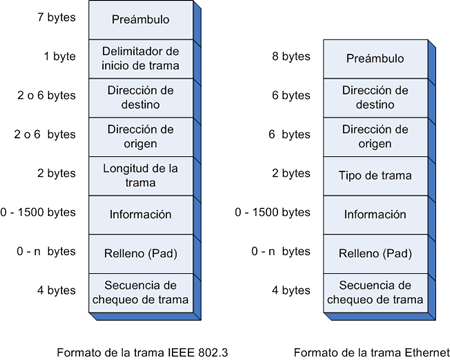
VERDADERO.

**17. Nombre cinco protocolos de capa de enlace. ¿Todos los protocolos en esta capa proveen los mismos servicios?**

1. Ethernet, Token Ring, FDDI, PPP, 802.11 -wireless-... ATM y Frame Relay pueden considerarse protocolos de enlace en determinados contextos.  
   No todos ofrecen los mismos servicios; la transmisión confiable y la corrección de errores por ejemplo no están presentes en todos.
2. ARP, CSMA/CD, paso de testigo, ALOHA, PPP (point to point protocol).

Cual está bien?

**18. ¿Qué es la IEEE 802.3? ¿Existen diferencias con Ethernet?**

Ethernet es una implementación que se convirtió en estándar *de facto* para LANs con acceso al medio tipo CSMA/CD, definiendo las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. Las primeras versiones surgieron en los '70. Se tomó como base, en el '83, para la redacción del estándar formal IEEE 802.3, manejándose usualmente como sinónimos, aunque se diferencian en uno de los campos de la trama de datos.  
Las tecnologías más comunes de tipo Ethernet están agrupadas en el estándar 802.3 (10Base2, 10BaseT, 100BaseT, Gigabit Ethernet...). Se suele hacer referencia a Ethernet como una LAN 802.3.  
  


La diferencia más significativa entre la tecnología Ethernet original y el estándar IEEE 802.3 es la diferencia entre los formatos de sus tramas. **Esta diferencia es lo suficientemente significativa como para hacer a las dos versiones incompatibles**.   
Una de las diferencias entre el formato de las dos tramas está en el preámbulo. El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse a si mismos a la trama entrante. El preámbulo en Ethernet tiene una longitud de 8 bytes pero en IEEE 802.3 la longitud del mismo es de 7 bytes, en este último el octavo byte se convierte en el comienzo del delimitador de la trama.   
La segunda diferencia entre el formato de las tramas es en el campo tipo de trama que se encuentra en la trama Ethernet. Un campo tipo es usado para especificar al protocolo que es transportado en la trama (IP, IPX...). Esto posibilita que muchos protocolos puedan ser transportados en la trama. El campo **tipo** fue reemplazado en el estándar IEEE 802.3 por un campo **longitud** de trama, el cual es utilizado para indicar el número de bytes que se encuentran en el campo da datos (puede diferenciarse una trama Ethernet de una 802.3 porque *tipo* toma valores superiores a 1500 y *longitud* valores menores o iguales).   
La tercera diferencia entre los formatos de ambas tramas se encuentra en los campos de dirección, tanto de destino como de origen. Mientras que el formato de IEEE 802.3 permite el uso tanto de direcciones de 2 como de 6 bytes, el estándar Ethernet permite solo direcciones de 6 Bytes.   
El formato de trama que predomina actualmente en los ambientes Ethernet es el de IEEE 802.3, pero la tecnología de red continua siendo referenciada como Ethernet.