Redes y Comunicaciones

Práctica 5 - Capa de Enlace

Puntos que faltan: 4, 5, 6(b), 6(c)

*En **esta** práctica, se referirá a los siguientes términos (FCS, CRC y checksum) indistintamente.*

1. ¿Qué función cumple la capa de enlace? Indique qué servicios presta esta capa y luego compárelos con los servicios prestados por la capa de transporte.

Práctica de Alternativa:

La Capa de Enlace tiene la responsabilidad de transferir datagramas desde un nodo al nodo adyacente a través de un enlace individual (direccionamiento físico), contrastando con la capa de Transporte que ofrece comunicación entre hosts remotos (en realidad proceso a proceso).

Define el formato de los "frames" que se intercambian entre los nodos a los extremos del enlace y las acciones que llevan a cabo para transmitir y recibir frames. Ofrece servicios de:

- **Entramado y acceso al medio.** Encapsula el datagrama en el frame (fragmentando de ser necesario). Incluye direcciones MAC -físicas, según el NIC (placa de red)-. Controla el acceso al medio si es compartido, coordinando las transmisiones de los nodos.
- **Transferencia confiable.** Basado en confirmaciones y retransmisiones como TCP. Usado principalmente si el enlace no es confiable para evitar retransmisiones a nivel de red o aplicación -se utiliza en wireless por ejemplo, pero no con fibra óptica, coaxial ni algunas versiones de par trenzado para no sobrecargar duplicando funciones-.
- **Control de flujo.**
- **Detección de Errores**. Producidos por atenuación de la señal o ruido electromagnético. Muy común; se implementa en hardware y es más sofisticado que el realizado por capas superiores.
- **Corrección de Errores** (algunos protocolos; ATM permite la detección sólo en el header).
- **Conexiones Full-Dulpex y Half-Duplex**. En las primeras un nodo puede transmitir y recibir a la vez; en las segundas no.

Si bien algunas de estas funciones se "solapan" con las de Transporte, la capa de Enlace las implementa entre nodos adyacentes, no entre hosts remotos.

Kurose-Ross (redactado por Gonzalo):

Al analizar la capa de enlace encontraremos dos tipos de canales, los canales de difusión y los canales de comunicación punto a punto. Nos referiremos a router y hosts simplemente como **nodos**, y a los canales de comunicación como **enlaces**, un nodo transmisor encapsula el datagrama en una trama(frame) y lo transmite a través del enlace, el nodo receptor recibe la trama y extrae el datagrama.

El **protocolo de la capa de enlace** define el formato de los paquetes intercambiados por los nodos. Por lo tanto mientras la **capa de red** tiene asignada la tarea de mover los segmentos de la **capa de transporte** terminal a terminal desde el host origen al host destino, el **protocolo de la capa de enlace** tiene la tarea nodo a nodo de mover los datagramas de la **capa de red** a través de un único enlace dentro de la ruta.

Para entender la responsabilidad que tiene la capa de enlace ver la analogía del turista, libro de Kurose (pag 419).

Los servicios que da la capa de enlace son: Entramado, Acceso al enlace, Entrega fiable, Control de Flujo, detección de errores, corrección de errores, semiduplex y full-duplex.

Muchos servicios proporcionados por la capa de enlace presentan notables paralelismos con los servicios proporcionados en la capa de transporte, por ejemplo ambas capas proporcionan un servicio de control de flujo y detección de errores, pero el control del flujo en un protocolo de la capa de transporte se proporciona en modo terminal a terminal, mientras que en un protocolo de la capa de enlace se proporciona entre dos nodos adyacentes.

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

Práctica de Alternativa:

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.

3. Calcule los códigos de detección de error para las siguientes cadenas de bits utilizando paridad par y luego utilizando paridad impar:

(**Paridad par**: # de bits en 1 debe ser par; **Paridad impar**: # de bits en 1 debe ser impar)

	Paridad Par	Paridad Impar
110101101010011111	1	0
010111010110000010	0	1
001000100010000111	0	1

4. Se desea enviar la secuencia de bits 1100000111. Calcular la secuencia completa (datos+FCS) a transmitir considerando que el polinomio generador a utilizar es: G(x) = x^5 + x^4 + 1.

5. Encontrar el FCS si se utiliza la función generadora G=1001 y el mensaje M=11100011

6. 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.

No se detectará el error porque cuando la cantidad de errores sea par se mantendrá la paridad. Si la cantidad de unos es par y hay un error (uno 0 pasa a ser 1 o un 1 pasa a ser 0), la cantidad de unos pasará a ser impar y cuando ocurra un segundo error la cantidad de unos será par nuevamente.

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

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

7. ¿De qué forma se identifican dos máquinas en una red Ethernet? ¿Qué características poseen estas direcciones?

Las direcciones de la capa de enlace se conocen como MAC (también llamadas dirección LAN o dirección física). Las MAC (Media Access Control) son las direcciones asignadas a los adaptadores instalados en cada nodo. La dirección MAC tiene 6 bytes de longitud, un total de 2^{48} direcciones distintas, que se expresan en notación hexadecimal. **Las direcciones MAC son únicas para cada dispositivo (al menos teóricamente), los primeros 24 bits corresponden a la empresa fabricante (asignado por la IEEE) y los últimos 24 son para cada dispositivo fabricado por esa empresa.**

La dirección MAC de broadcast es los 6 bytes con todos los bits en 1, que en hexadecimal es FF-FF-FF-FF-FF-FF.

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

Definición de CSMA/CD (fuente):

El estándar IEEE 802.3 especifica el método de control del medio (MAC) denominado CSMA/CD por las siglas en ingles de acceso múltiple con detección de portadora y detección de colisiones (carrier sense multiple access with collision detection). 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 el medio esta tranquilo (ninguna otra estación esta 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.

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

Diferencia con Ethernet (fuente):

Si bien IEEE 802.3 y Ethernet son similares, no son idénticos. Las diferencias entre ellos son lo suficientemente significativas como para hacerlos incompatibles entres sí.

Todas las versiones de Ethernet son similares en que comparten la misma arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD (carrier sense multiple access with collision detection). Sin embargo, el estándar IEEE 802.3 ha evolucionado en el tiempo de forma que ahora soporta múltiples medios en la capa física, incluyendo cable coaxil de 50 Ω y 75 Ω, cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP), cable par trenzado con blindaje (Shielded Twisted Pair o STP) y fibra óptica. Otras diferencias entre los dos incluyen la velocidad de transmisión, el método de señalamiento y la longitud máxima del cableado.

10. ¿Cuál es la función de un HUB? ¿Qué lo diferencia de un switch o bridge?

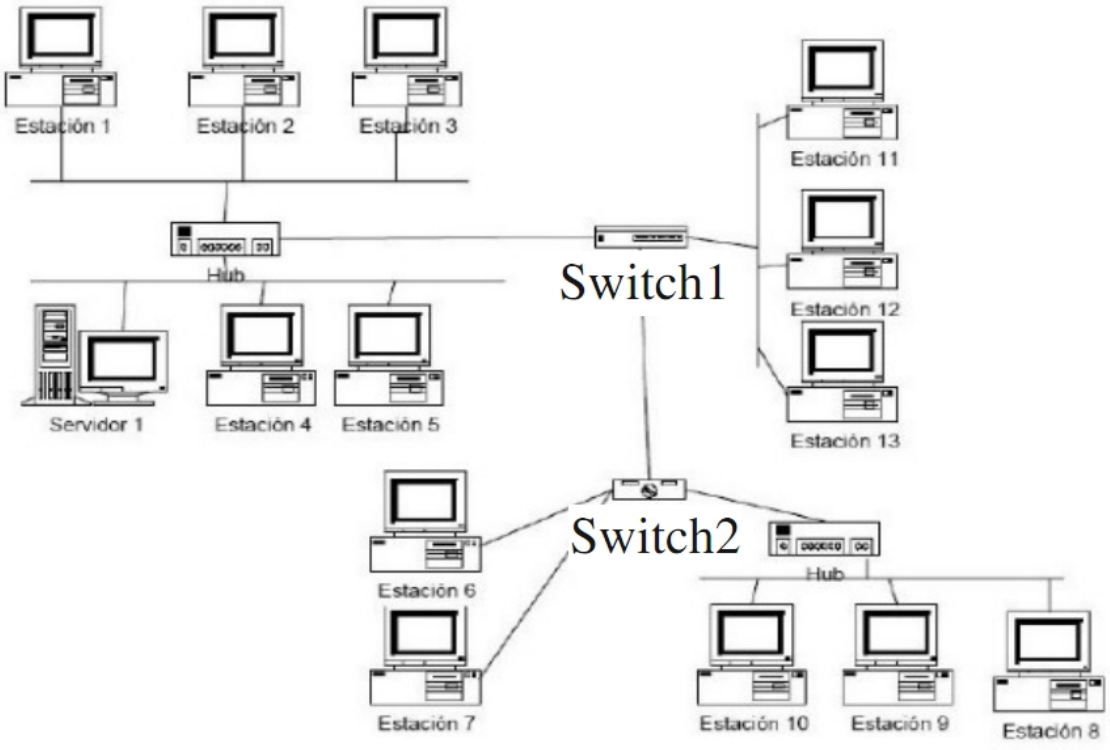
Hub (concentrador):

Es un dispositivo de capa física. Su función es difundir la señal entrante por todos los canales salientes. Actúa como un repetidor. Envía la señal recibida a todos los dispositivos conectados, sin importar cuales sean, no aplica ningún filtro ni examina la trama recibida.

Switch y bridge:

Dispositivos que conectan múltiples partes de una red en la capa 2. Tienen un dominio de colisión aislado por cada puerto, a diferencia del Hub que tiene uno en total: aprenden en qué puerto están ubicadas las MACs y así evitan mandar las tramas en broadcast.

11. Dado el siguiente esquema de red, responda:



1. **¿Quién escucha el mensaje si:**
    a. **La estación 1 envía una trama al servidor 1?**

        E2, .. E5, SR1, SW1

    b. **La estación 1 envía una trama a la estación 11?**

        E2, .. E5, SR1, SW1, E11, E12, E13

    c. **La estación 1 envía una trama a la estación 9?**

        E2, .., E5, SR1, SW1, SW2, E8, E9, E10

    d. **La estación 6 envía una trama a la estación 7?**

        SW2, E7

    e. **La estación 6 envía una trama a la estación 10?**

        SW2, E8, E9, E10

2. **¿En qué situaciones se pueden producir colisiones?**

    Se pueden producir colisiones entre las estaciones conectadas a un Hub y las que comparten un medio (como la 11, 12 y 13), es decir, las que estén dentro de un mismo dominio de colisión. Las únicas que no producen/sufren colisiones son la 6 y la 7.

3. **Si la estación 5 transmite un broadcast, ¿quienes escuchan esta trama?**

   Todos los equipos, ya que ese es el rango del broadcast. Los delimitadores de broadcast son los routers.

12. ¿Qué dispositivos dividen dominios de broadcast? ¿y dominios de colisión?

Dominio de colisión:

Parte de la topología donde se pueden producir colisiones. Un HUB tiene un solo dominio de colisión, donde todas las máquinas conectadas pueden producir colisiones; en cambio el SWITCH tiene un dominio de colisión por cada puerto. Los que separan dominios de colisión son los SWITCH y los ROUTERS.

Dominio de broadcast:

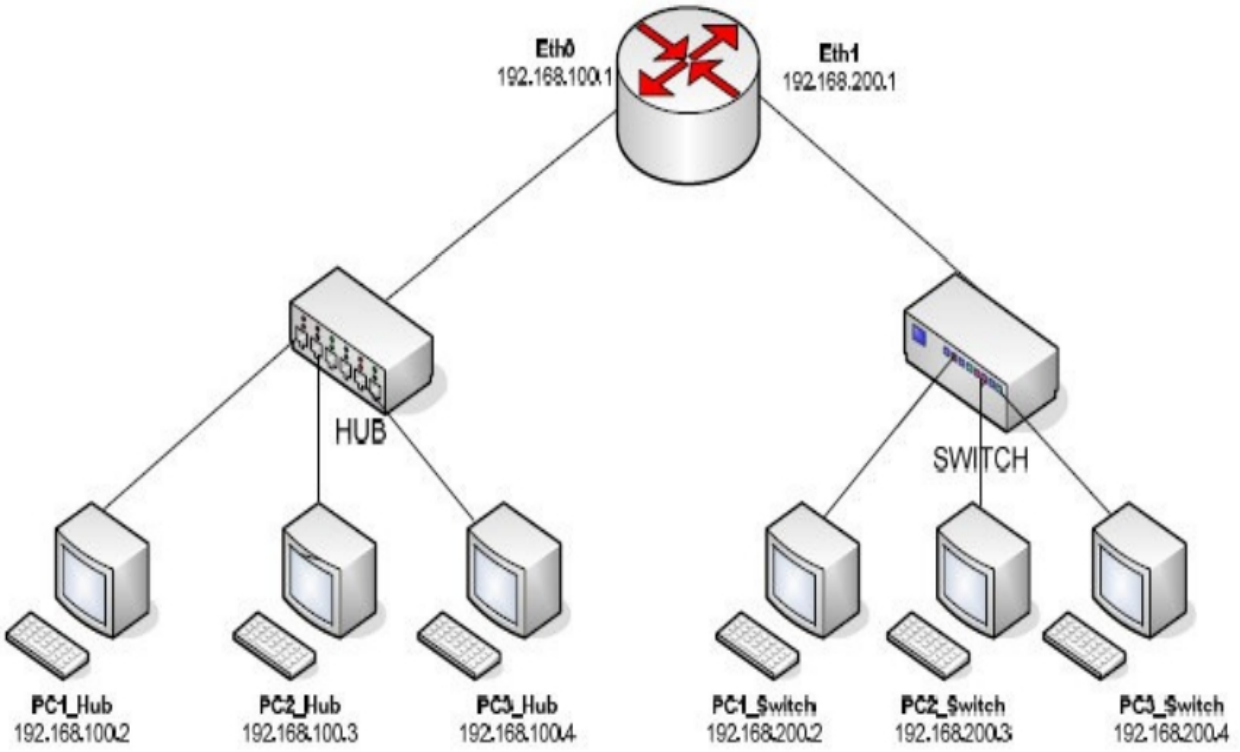
Parte de la topología donde llega una señal de broadcast. Los que separan dominios de broadcast son los routers.

13. ¿Cuál es la finalidad del protocolo ARP?

ARP (Address Resolution Protocol) surge por la necesidad de traducir direcciones de capa de red (IPs) a direcciones de capa de enlace (MACs). ARP funciona para nodos dentro de una misma subred, todo nodo tiene una tabla de correspondencias entre MAC e IP para otros nodos en su subred (puede que la tabla solo contenga algunos nodos y no todos).

Cuando un nodo A quiere averiguar la MAC de un nodo B debe enviar un paquete de consulta ARP. "A" crea un paquete IP que contiene IP-origen, MAC-origen, IP-destino y MAC 00-00-00-00-00-00 (esta es la MAC que le tienen que devolver). "A" le pasa el paquete al adaptador de red indicando que debe ser enviado a la dirección de broadcast (FF-FF-FF-FF-FF-FF). La trama es enviada a todos los nodos de la subred, recibida por todos los adaptadores existentes y cada adaptador pasa la consulta ARP contenida en la trama al módulo ARP de dicho nodo. Solo el nodo B, cuya IP coincide con la IP-destino, responderá con una respuesta ARP en la que incluye como IP-origen y MAC-origen sus IP y MAC, y MAC e IP-destino los de A; esta segunda trama se envia de forma unicast y no broadcast. Cuando A recibe la respuesta actualiza su tabla de ARP para la IP de B.

14. Utilizando el LiveCD provisto por la cátedra, se simulará la red que muestra el siguiente gráfico:



1. *Abra una consola de usuario y ejecute el comando:*
   topologia capa-enlace start
2. *Aguarde a que la consola devuelva el prompt y que aparezcan cada una de las máquinas involucradas en el gráfico. Cada máquina se representa por una ventana xterminal cuyo título se corresponde con los nombres que muestra el gráfico: PC1_HUB, PC2_HUB, PC3_HUB, PC1_SW, PC2_SW, PC3_SW y Router.*
3. *Cada equipo de la de red ya se encuentra configurado con sus respectivas direcciones IP y el nombre de usuario de las máquinas y del router es root y su contraseña xxxx*
4. *Para observar cómo se comportan el hub y el switch realice las siguientes tareas:*
   a. *Envíe un ping desde la PC1_HUB a la PC2_HUB y monitoree el tráfico desde la PC3_HUB utilizando el siguiente comando tcpdump -i eth0 -p icmp. Vea los resultados en la consola de PC3_HUB. ¿Qué pudo observar?*

```
pc1_hub:~# ping -nR 192.168.100.3

pc3_hub:~# tcpdump -i eth0 -p icmp | head -n 30 > tcpdump.pc3_hub.1
15:55:34.773598 IP 192.168.100.2 > 192.168.100.3: ICMP echo request, id 11781, seq 268, length 64
15:56:14.856908 IP 192.168.100.3 > 192.168.100.2: ICMP echo reply, id 11781, seq 268, length 64
15:55:34.778709 IP 192.168.100.1 > pc3_hub: ICMP net 80.58.61.250 unreachable, length 80
15:55:35.781317 IP 192.168.100.2 > 192.168.100.3: ICMP echo request, id 11781, seq 269, length 64
15:55:35.781504 IP 192.168.100.3 > 192.168.100.2: ICMP echo reply, id 11781, seq 269, length 64
15:55:36.793338 IP 192.168.100.2 > 192.168.100.3: ICMP echo request, id 11781, seq 270, length 64
15:55:36.793341 IP 192.168.100.3 > 192.168.100.2: ICMP echo reply, id 11781, seq 270, length 64
```

   b. *Envíe un ping desde la PC1_SW a la PC2_SW y monitoree el tráfico desde la PC3_SW utilizando el siguiente comando tcpdump -i eth0 -p icmp. Vea los resultados en la consola de PC3_HUB. ¿Qué pudo observar? ¿Cuáles son las diferencias respecto a lo observado*

en el punto (a)?

5. *Para analizar los paquetes del protocolo ARP realice las siguientes tareas:*
   a. *Ejecute el comando ifconfig -a en la PC1_HUB*
   b. *Luego ejecute el comando arp -n en la PC1_HUB para ver su tabla ARP.*

```
pc1_hub:~# arp -n
rtt min/avg/max/mdev = 0.208/0.267/0.302/0.044 ms
Address                  HWtype  HWaddress           Flags Mask            Iface
```

   c. *Monitoree el tráfico arp desde la PC3_HUB ejecutando tcpdump -i eth0 -p arp.*

```
pc3_hub:~# tcpdump -i eth0 -p arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
16:33:44.715875 arp who-has 192.168.100.2 tell 192.168.100.3
16:33:44.716082 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
16:33:44.727780 arp who-has pc3_hub tell 192.168.100.1
16:33:44.727794 arp reply pc3_hub is-at fe:fd:00:00:04:00 (oui Unknown)
16:33:54.726485 arp who-has 192.168.100.1 tell pc3_hub
16:33:54.726758 arp reply 192.168.100.1 is-at fe:fd:00:00:01:00 (oui Unknown)
16:34:14.764279 arp who-has pc3_hub tell 192.168.100.1
16:34:14.764296 arp reply pc3_hub is-at fe:fd:00:00:04:00 (oui Unknown)
16:34:28.126818 arp who-has 192.168.100.2 tell 192.168.100.3
```

   d. *Envíe un ping desde la PC1_HUB a la PC2_HUB y vuelva a observar la tabla ARP de la PC1_HUB.*

```
pc1_hub:~# ping 192.168.100.3 -c 3; arp -n
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.208 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.292 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.302 ms

--- 192.168.100.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.208/0.267/0.302/0.044 ms
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.100.3            ether   fe:fd:00:00:03:00   C                     eth0
```

   e. *Vea los resultados en la consola de PC3_HUB a fin de observar las características de los paquetes arp (MAC Origen, MAC Destino, etc).*

```
117:06:24.565167 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
17:06:55.817534 arp who-has 192.168.100.2 tell 192.168.100.3
17:06:55.817705 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
17:07:27.117829 arp who-has 192.168.100.2 tell 192.168.100.3
17:07:27.117838 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
17:07:58.406168 arp who-has 192.168.100.2 tell 192.168.100.3
17:07:58.406171 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown7:06:24.565167 arp reply
192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
17:06:55.817534 arp who-has 192.168.100.2 tell 192.168.100.3
17:06:55.817705 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
17:07:27.117829 arp who-has 192.168.100.2 tell 192.168.100.3
17:07:27.117838 arp reply 192.168.100.2 is-at fe:fd:00:00:02:00 (oui Unknown)
```

   f. *Monitoree el tráfico arp desde la PC3_SW ejecutando tcpdump -i eth0 -p arp.*

```
pc3_sw:~# tcpdump -i eth0 -p arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
18:24:09.194789 arp who-has 192.168.200.3 tell 192.168.200.2
18:24:09.212160 arp who-has 192.168.200.1 tell pc3_sw
18:24:09.212529 arp reply 192.168.200.1 is-at fe:fd:00:00:01:01 (oui Unknown)
18:24:14.205911 arp who-has pc3_sw tell 192.168.200.1
18:24:14.205926 arp reply pc3_sw is-at fe:fd:00:00:07:00 (oui Unknown)
18:24:39.246694 arp who-has 192.168.200.1 tell pc3_sw
18:24:39.246900 arp reply 192.168.200.1 is-at fe:fd:00:00:01:01 (oui Unknown)
18:25:04.295961 arp who-has pc3_sw tell 192.168.200.1
18:25:04.295984 arp reply pc3_sw is-at fe:fd:00:00:07:00 (oui Unknown)
```

g. *Haga un ping a la PC2_SW y vuelva a observar la tabla ARP de la PC1_SW.*

h. *Vea los resultados en la consola de PC3_HUB a fin de observar cuáles son las diferencias respecto a lo observado en el punto (e) en cuanto a cuáles son los paquetes que se ven en este caso.*

6. *Para analizar el encapsulamiento a nivel de capa 2 y 3 realice las siguientes tareas:*

a. *Ejecute el comando ifconfig -a en la Router y en la PC1_SW.*

```
router:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr FE:FD:00:00:01:00
          inet addr:192.168.100.1  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:100/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3704 (3.6 KiB)  TX bytes:4080 (3.9 KiB)
          Interrupt:5

router:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr FE:FD:00:00:01:01
          inet addr:192.168.200.1  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:101/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2048 (2.0 KiB)  TX bytes:1472 (1.4 KiB)
          Interrupt:5

pc1_sw:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr FE:FD:00:00:05:00
          inet addr:192.168.200.2  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:500/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1664 (1.6 KiB)  TX bytes:1532 (1.4 KiB)
          Interrupt:5

pc1_hub:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr FE:FD:00:00:02:00
          inet addr:192.168.100.2  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:200/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5612 (5.4 KiB)  TX bytes:1532 (1.4 KiB)
          Interrupt:5
```

b. *Monitoree el tráfico desde la PC3_HUB ejecutando tcpdump -i eth0.*

```
pc3_hub:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:03:45.740587 arp who-has 192.168.100.1 tell 192.168.100.2
20:04:25.824310 arp reply 192.168.100.1 is-at fe:fd:00:00:01:00 (oui Unknown)
20:04:25.825431 IP 192.168.100.2 > 192.168.200.2: ICMP echo request, id 11525, seq 1, length 64
20:03:45.752803 IP 192.168.200.2 > 192.168.100.2: ICMP echo reply, id 11525, seq 1, length 64
20:03:45.752821 arp who-has 192.168.100.1 tell pc3_hub
20:03:45.752937 arp reply 192.168.100.1 is-at fe:fd:00:00:01:00 (oui Unknown)
```

c. *Luego ejecute el comando arp -n en la PC1_HUB para ver su tabla ARP.*

```
pc1_hub:~# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.100.1            ether   fe:fd:00:00:01:00   C                     eth0
```

d. *Envíe un ping a la PC1_HUB a la PC1_SW y vuelva a observar la tabla ARP de la PC1_HUB. ¿A qué dispositivo corresponde la asociación IP-MAC agregada en la tabla?*

e. *Vea los resultados en la consola de PC3_HUB a fin de observar tanto los paquetes arp como los paquetes icmp teniendo en cuenta MAC origen, MAC destino, IP origen e IP destino según corresponda.*

```
pc3_hub:~# head tcpdump -n 39
19:21:10.947428 arp who-has 192.168.100.1 tell 192.168.100.2
19:21:51.028560 arp reply 192.168.100.1 is-at fe:fd:00:00:01:00 (oui Unknown)
19:21:51.029346 IP 192.168.100.2 > 192.168.200.2: ICMP echo request, id 12805, seq 1, length 64
19:21:10.954915 arp who-has 192.168.100.1 tell pc3_hub
19:21:10.955373 arp reply 192.168.100.1 is-at fe:fd:00:00:01:00 (oui Unknown)
19:21:10.955382 IP pc3_hub.54994 > 80.58.61.250.domain:  16908+ PTR? 1.100.168.192.in-addr.arpa. (44)
19:21:10.955640 IP 192.168.100.1 > pc3_hub: ICMP net 80.58.61.250 unreachable, length 80
19:21:10.957108 IP 192.168.200.2 > 192.168.100.2: ICMP echo reply, id 12805, seq 1, length 64
19:21:11.943183 IP 192.168.100.2 > 192.168.200.2: ICMP echo request, id 12805, seq 2, length 64
19:21:11.943235 IP 192.168.200.2 > 192.168.100.2: ICMP echo reply, id 12805, seq 2, length 64
19:21:12.955073 IP 192.168.100.2 > 192.168.200.2: ICMP echo request, id 12805, seq 3, length 64
```

15.Cuando una PC que esta en una red, se quiere comunicar con otra que no esta en la misma red, esta se da cuenta observando su tabla de rutas. Por ende, para comunicarse debe usar el default gateway de la misma. Si la tabla ARP de la PC esta vacía, cuando la PC realiza un ARP para obtener la MAC del router, ¿que dirección IP destino tiene el requerimiento ARP? ¿es la dirección IP del default gateway o la dirección IP de la máquina destino?

Complete:

Trama Ethernet: (mac origen: MAC-PC-ORIGEN ***mac destino:*** FF-FF-FF-FF-FF-FF***)***
Solicitud ARP: (mac origen: MAC-PC-ORIGEN ***ip origen:*** IP-PC-ORIGEN
mac destino: 00-00-00-00-00-00 ***ip destino:*** DEFAULT-GATEWAY***)***

16. En base a lo anterior, suponiendo que un host A debe conectarse a un host B. Si A desconoce la dirección MAC de B, analice las diferencias tanto en ARP como en la comunicación subsecuente suponiendo las siguientes situaciones:

1. **Las direcciones IP de A y B son 192.23.1.4/24 y 192.23.1.2/24, respectivamente**

   Dado que A y B están en la misma subred, A necesita conocer la dirección de B para poder comunicarse. Con una consulta ARP por parte de A alcanzará para que A y B se puedan comunicar entre sí.

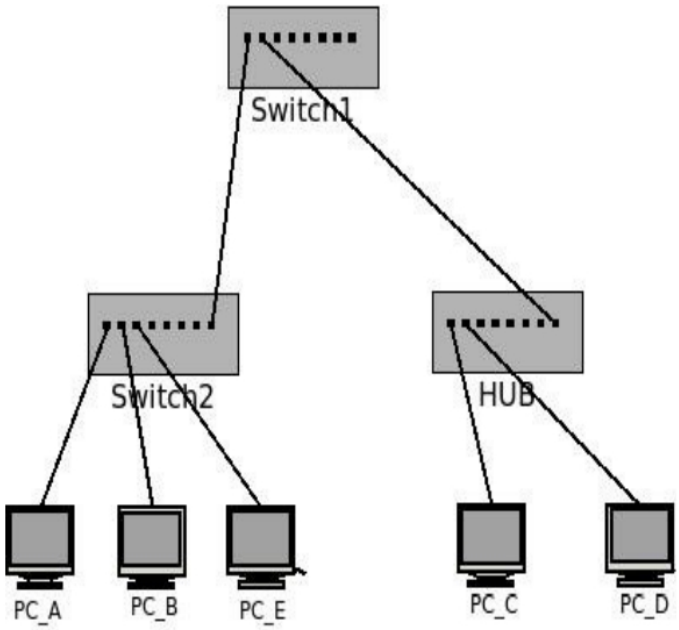
2. **Las direcciones IP de A y B son 192.23.1.4/24 y 192.23.2.2/24, respectivamente**

   Como A y B están en distintas subredes, A deberá comunicarse con el router para poder comunicarse con B. Por lo tanto no necesita conocer la MAC de B, pero sí necesita conoce la MAC del router.

17.Cuando una PC que esta en una red, se quiere comunicar con otra que no esta en la misma red, esta se da cuenta observando su tabla de rutas. Por ende, para comunicarse debe usar el default gateway de la misma. Si la tabla ARP de la PC esta vacía, cuando la PC realiza un ARP para obtener la MAC del router, ¿que dirección IP destino tiene el requerimiento ARP? ¿es la dirección IP del default gateway o la dirección IP de la máquina destino?

La IP destino será el DEFAULT GATEWAY.

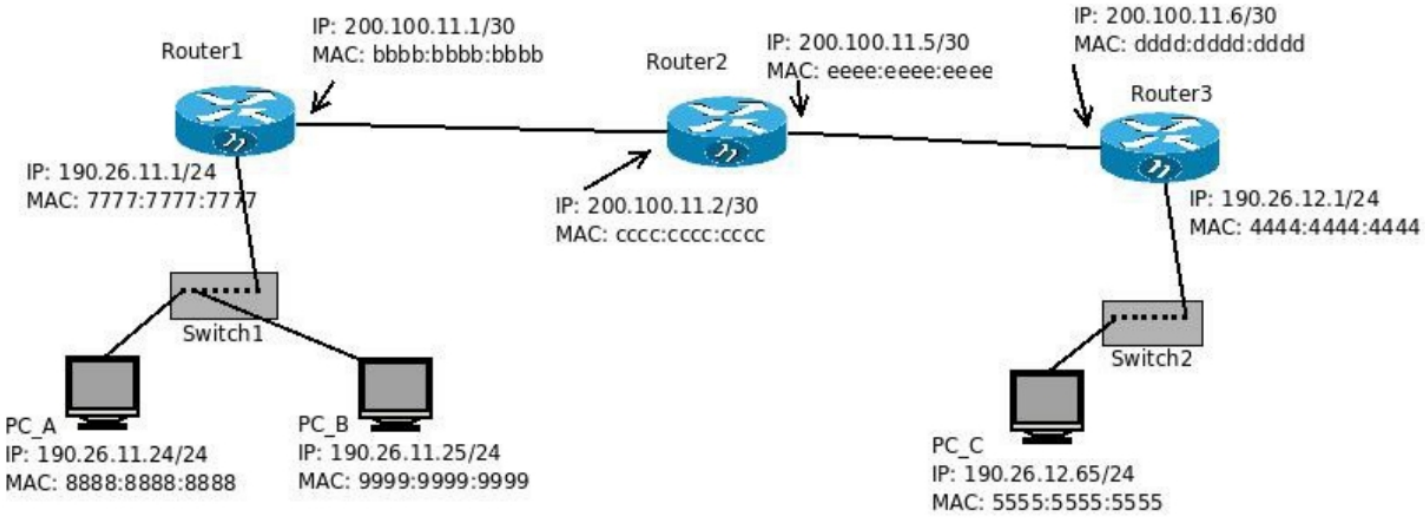
18.Para la siguiente topología de red indique:



1. *¿Cuántos dominios de colisión hay?*
   5
2. *¿Cuántos dominios de broadcast hay?*
   1
3. *Indique cómo se va llenando la tabla de asociaciones MAC → PORT del switch SW1 y SW2 durante el siguiente caso:*
   (Cada **switch** anota la **MAC** origen de cadla consulta/respuesta ARP que recibe y la asocia al puerto de donde llega)
   a. ***A envía una solicitud ARP consultando la MAC de C***
      SW2 MAC_PC_A → Port_1
      SW1 MAC_PC_A → Port_1
      (**PC_A** hace un ARP request que llega al **SW_2**, este asocia la **MAC** de **PC_A** con el puerto 1 y propaga el broadcast que le llega a **SW_1** y este asocia la **MAC** de **PC_A** con el puerto 1)
   b. ***C responde esta solicitud ARP***
      SW1 MAC_PC_C → Port_2
      (**PC_C** responde con un ARP response que le llega al **SW_1**)
      SW2 MAC_PC_C → Port_8
      (**PC_C** responde el ARP request y la respuesta llega al **SW_1**, este asocia la **MAC** de **PC_C** con el puerto 2 y forwardea la respuesta por el puerto 1 hacia **SW_2** y este asocia la **MAC** de **PC_C** con el puerto 8)
   c. ***A envía una solicitud ARP consultando la MAC de B***
      (aca no pasa nada porque tanto **SW_1** como **SW_2** ya tenían asociada la **MAC** de **PC_A**)
   d. ***B responde esta solicitud ARP***
      SW2 MAC_PC_B → Port_2
      (**PC_B** responde el ARP request y la respuesta llega a **SW_2**, este asocia la **MAC** de **PC_B** con el puerto 2 y forwardea la respuesta por el puerto 1 hacia **PC_A**)

4. *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?*
   PC E: escucha (a) y (c)
   PC D: escucha (a), (b) y (c)

19.En la siguiente topología



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 qué dominios de broadcast hay tráfico ARP?***
  En todos.
- ***¿En qué dominios de broadcast hay tráfico ICMP?***
  En todos
- ***¿Cuál es la secuencia correcta en la que se suceden los anteriores?***
  a. PC_A manda una consulta ARP para averiguar la de MAC R1 y este le contesta.
  b. PC_A manda el ping al R1 pero este no tiene la MAC del R2.
  c. R1 manda una consulta ARP para averiguar la MAC del R2.
  d. R2 responde el ARP y router1 envía el ping al R2.
  e. R2 envia ARP para R3, este contesta y R2 manda ping a R3.
  f. R3 envía ARP para PC_C, esta contesta y R3 envía ping a PC_C.
  g. PC_C responde el ping que pasa directamente porque las tablas ARP estan completas para ese enlace.

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

ICMP	Emisor	MAC Destino	MAC Origen	IP Origen	IP destino
Ping	PC_A	7777:7777:7777	8888:8888:8888	190.125.11.24	190.26.12.65
Ping	R_1	cccc:cccc:cccc	bbbb:bbbb:bbbb	190.125.11.24	190.26.12.65
Ping	R_2	dddd:dddd:dddd	eeee:eeee:eeee	190.125.11.24	190.26.12.65
Ping	R_3	5555:5555:5555	4444:4444:4444	190.125.11.24	190.26.12.65
Echo	PC_C	4444:4444:4444	5555:5555:5555	190.26.12.65	190.125.11.24
Echo	R_3	eeee:eeee:eeee	dddd:dddd:dddd	190.26.12.65	190.125.11.24
Echo	R_2	bbbb:bbbb:bbbb	cccc:cccc:cccc	190.26.12.65	190.125.11.24
Echo	R_1	8888:8888:8888	7777:7777:7777	190.26.12.65	190.125.11.24