Practica 5

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.   
  
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 al 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 adyadentes, no entre hosts remotos.

2)Nombre cinco protocolos de capa de enlace. ¿Todos los protocolos en esta capa

proveen los mismos servicios?   
  
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 e impar:

(a) 11010110101001111 Paridad par: 1 | Paridad impar: 0

(b) 01011101011000010 Paridad par: 0 | Paridad impar: 1

(c) 00100010001000111 Paridad par: 0 | Paridad impar: 1  
  
Paridad par o impar es un bit mas que va al final, haciendo que todo el conjunto quede como indica ese bit.

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) = x5 + x4 + 1

Mensaje= 1100000111   
G=110001

110000011100000

110001

00000101110

110001  
 0111110

110001  
 00111100  
 110001  
 0011010   
  
Verificación:

110000011111010  
110001

00000101111

110001

0111101

110001

00110001  
 110001

000000

5)Encontrar el FCS si se utiliza la función generadora G=110011 y el mensaje M=11100011   
  
 1110001100000 → relleno con 0 los bits de G – 1, osea 5

XOR 110011 → hago un XOR con G y bajo los bits que me faltan de arriba, completando

00101111

XOR 110011 → XOR con G

0111000

110011

00101100

110011

0111110

110011

0011010  
  
Verificación:

1110001111010

XOR 110011

00101111  
 110011  
 0111001  
 110011  
 00101010  
 110011  
 0110011  
 110011  
 0000000  
  
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. FALSO. La inversión de una cantidad par de bits no es detectable bajo ningún esquema de paridad.

(b) CRC realiza detección de errores sólo en un bit. FALSO.

(c) CRC nunca falla. FALSO.

(d) 101011 es un valor válido para el polinomio generador. VERDADERO. La única condición necesaria es que comience con 1. Equivale a x^5 + x^3 + x + 1.

(e) 011111 es un valor válido para el polinomio generador. FALSO. Debe comenzar con 1.

7)¿De qué forma se identifican dos máquinas en una red Ethernet? ¿Qué características

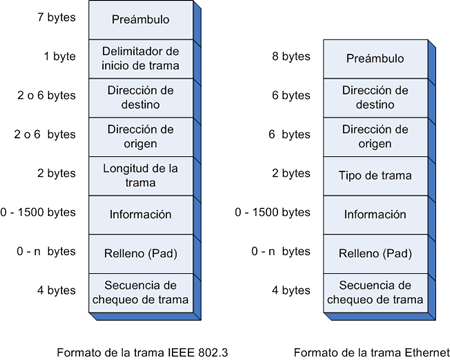
poseen estas direcciones?   
  
Las máquinas en una LAN se identifican a nivel de *Enlace* por la dirección LAN/Ethernet/Física/MAC asociada a su adaptador/NIC/placa de red -nomalmente grabada en su memoria ROM-. Para Ethernet, utilizan 6 bytes (48 bits), normalmente expresados en exadecimal.  
Estas direcciones son únicas (las administra la IEEE, utilizando 3 bytes para codificar el fabricante y 3 para el número de serie de la placa). Conforman un espacio de direcciones **plano** y no varía por más que la placa se conecte desde distintos lugares (a diferencia de las direcciones IP que forman una jerarquía y varían según la red a la que se conecte el equipo). Existe también una dirección de broadcast: FF-FF-FF-FF-FF-FF.  
Pese a existir las direcciones IP, las MAC son necesarias porque:

* Las LANs no sólo se diseñan para el protocolo de red IP.
* Usar sólo IP requeriría almacenarla en la RAM de la placa y configurarla cada vez que se conecte.

Si no se usaran direcciones y la capa de Enlace pasara todos los datagramas a la capa superior para que ella filtre, la interrumpiría muy seguido.

8)Describa el algoritmo de acceso al medio en Ethernet. ¿Es Ethernet 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). Para transmitir, el adaptador sensa el medio compartido (no utiliza ningún "*slot*"). Si está ocupado, espera hasta que se libere; si está libre, comienza a transmitir la trama. Durante la transmisión se compara la señal en el medio con la transmitida -otro nodo puede haber sensado el canal libre y comenzado a transmitir, detectándose después de un intervalo por el tiempo de propagación del medio-.  
Si se transmite toda la trama sin detectar colisión: se considera transmisión exitosa.  
Si se detecta colisión: se aborta la transmisión de la trama, se envía al medio una señal de "*taco*" (patrón de 48 bits, asegura que todos los nodos detecten la colisión) y se espera antes de volver a intentar retransmitir la señal un tiempo aleatorio que puede ser mayor según la cantidad de colisiones detectadas -**backoff exponencial**-.  
Ethernet NO es orientado a conexión (no hay handshaking) y NO es confiable (no hay acks/nacks). Eficiente con baja carga -habrá pocas colisiones-.

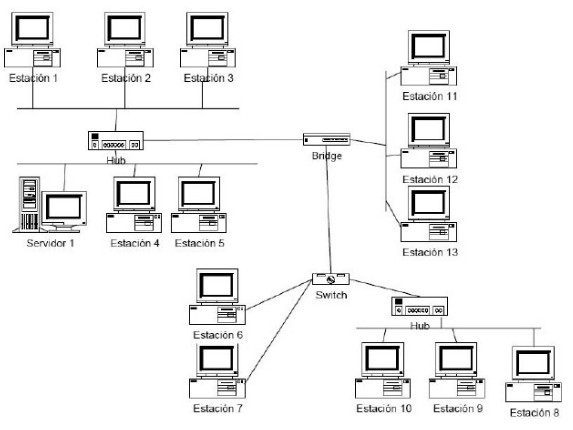
9)¿Qué es la IEEE 802.3? ¿Existen diferencias con Ethernet?   
  
Ethernet es una implementación que se convirtió en estándar *de facto* para LANs con acceso al medio tipo CSMA/CD, definiendo las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de 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.   
  
  
10)Describa el algoritmo de acceso al medio empleado por 802.5   
  
En redes **token ring** (estándar 802.5) los N nodos de la LAN se conectan por un enlace directo a un anillo.  
Se transmite un frame pequeño llamado "token" por la red. El orden en que pasa el *token* queda definido por la topología. Cuando un nodo obtiene el token vacío puede enviar su frame, que se propaga por el anillo. Al volver el token al nodo emisor, este no lo retransmite, y lo pasa, vacío, al siguiente nodo.  
El token se mueve en un solo sentido, así que si un nodo quiere transmitir al anterior, deberá recorrer toda la vuelta.

11)¿Qué es un bridge (o puente)? ¿Y un switch? ¿En qué se diferencian?   
  
Un switch/bridge es un dispositivo de **capa de enlace**, que permite interconectar segmentos de LAN formando **dominios de colisión separados**, pero un mismo dominio de broadcast.  
Al recibir una trama por una interfaz, consulta una tabla interna que construye automáticamente con MAC/interfaz, y reenvía la trama por la interfaz adecuada (si es la misma interfaz de entrada, no hace nada; si no estaba en la tabla, hace *flooding* reenviando la trama a todas las interfaces excepto por la que entró).  
El **bridge conmuta por software** y está pensado para conmutar entre redes, por lo que tienen pocas interfaces (2). Normalmente manejan de a una trama por vez. Utilizan ***store-and-fordware*** (mantienen buffers internos en los que almacenan las tramas de entrada, retransmitiéndolas recién cuando ingresaron por completo).  
El **switch conmuta por hardware** -más rápido- y se pensó para conectarse a hosts directamente. Pueden configurarse en modo ***store-and-fordware* o *cut-through***(comienza a enviar el frame ni bien reconoce la MAC destino). Pueden manejan múltiples tramas simultáneamente y mantener caminos paralelos. Los switchs tienen generalmente cada interfaz directamente conectada a un host, con lo que se logra una transferencia full-duplex (sin necesidad de detectar portadora ni detectar colisiones).

**Tanto bridges como switchs no tienen direcciones LAN (MAC).** Es decir, son “transparentes”.

12)¿Cuál es la función de un HUB? ¿Qué lo diferencia de un switch/bridge?   
  
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**.  
Un switch/bridge trabaja en capa de enlace, tiene buffers y reenvía las tramas basándose en la MAC y una tabla interna, evitando retransmitir por todas las interfaces -salvo que no posea la MAC destino-. **Utiliza CSMA/CD y permite interconectar distintas tecnologías ethernet.**

13)Dado el siguiente esquema de red, responda:

¿Quién escucha el mensaje si:

(a) La estación 1 envía una trama al servidor 1   
Esta trama la escuchan todos los nodos pertenecientes a la primer trama LAN (hasta el bridge, **menos el nodo que envia la trama**). Es decir: estación 2, 3, 4 y 5, servidor 1 y bridge. **El HUB es un dispositivo de capa 1, por lo tanto no interpreta tramas, no conoce lo que es una trama.**

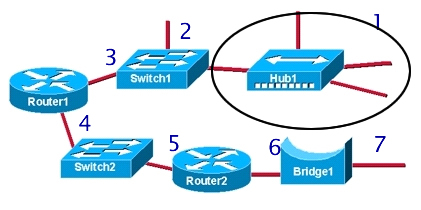
(b) La estación 1 envía una trama a la estación 11   
La primer trama LAN (menos la estacion 1 que envia), y la segunda (estacion 11, 12 y 13) pasando por el bridge.

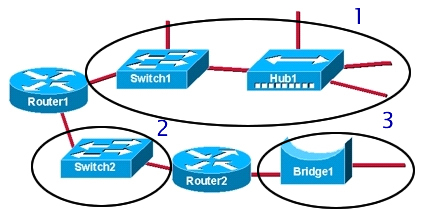
(c) La estación 1 envía una trama a la estación 9   
La primer trama LAN (menos estacion 1) mas las estaciones 8, 9 y 10 (con el switch y el bridge de por medio).

(d) La estación 6 envía una trama a la estación 7   
Escucha el mensaje solo la estacion 7 (pasando por el switch).

(e) La estación 6 envía una trama a la estación 10   
Las estaciones 8, 9 y 10, pasando por el switch.

ii. ¿En qué situaciones se pueden producir colisiones?   
Con hubs, dentro de la misma trama, si dos nodos transmiten al mismo tiempo.  
- Estaciones 1 a 5 o Servidor 1 transmiten simultáneamente, o mientras llega a su segmento una trama desde el bridge.  
- Estaciones 8 a 10 transmiten simultáneamente, o mientras llega a su segmento una trama desde el switch.  
- Estaciones 11 a 13 transmiten simultáneamente, o mientras llega a su segmento una trama desde el bridge.  
- Estación 6 o 7 transmiten mientras les llega un mensaje desde el switch.   
- Si el bridge envía una trama al switch y éste le envía otra al mismo tiempo.

iii. Si la estación 5 transmite un broadcast, ¿quiénes escuchan esta trama?   
**Escuchan todos. Un router separa dominio de boradcast.   
Con hubs, bridges y switches hay un *unico dominio de broadcast.***  
  
  
14)¿Qué dispositivos dividen dominios de broadcast? ¿y dominios de colisión?   
  
 -División de Dominios de Broadcast: router  
 -División de Dominios de Colisión: router, switch/bridge  
  
Los HUBs no dividen ni dominios de colisión, ni dominios de broadcast por ser de capa física.  
  
  
**7** dominios de colision(arriba).  
**3** dominios de broadcast:



15)¿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; ó
* 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).

16)Un host A debe conectarse a un host B. Si A desconoce la dirección MAC de B, qué

debería hacer suponiendo las siguientes situaciones:

(a) Las direcciones IP de A y B son 192.23.1.4/24 y 192.23.1.2/24, respectivamente   
*A utiliza ARP para comunicarse con B porque estan en la misma red. El host sabe esto al aplicar la mascara de red sobre la IP.*  
Host A aplica a IP de B la máscara y obtiene el mismo valor que su red (192.23.1): Los dos hosts están en la misma subred. A prepara un *ARP Request* para obtener la MAC de B, con:  
- IP Origen: 192.23.1.4/24, MAC Origen: MAC\_A  
- IP Destino: 192.23.1.2/24, MAC Destino: 00:00:00:00:00:00  
Luego envía el *Arp Request* en un frame de broadcast:  
- MAC Origen: MAC\_A  
- MAC Destino: MAC Broadcast (FF:FF:FF:FF:FF:FF).  
Una vez que B responda, A agrega la MAC en su tabla ARP y prepara el paquete de datos que debía enviar.

(b) Las direcciones IP de A y B son 192.23.1.4/24 y 192.23.2.2/24, respectivamente   
*A solo tendria que saber (o hacer) ARP al router (default gateway) porque B esta en otra red. No le interesa saber la MAC de B, no la guarda.*  
Host A aplica a IP de B la máscara y obtiene un valor distinto de red (192.23.2): Los dos hosts están en distintas subredes. A no intentará obtener la MAC de B. A precisa la MAC del router, consulta la tabla ARP y si no está prepara un *ARP Request* para el router (igual que en el caso anterior, pero con la IP del router que tenga configurada). Una vez con la MAC del router, A prepara un *datagrama IP* con:  
- IP Origen: 192.23.1.4/24  
- IP Destino: 192.23.1.2/24  
a nivel de Enlace, utilizará:  
- MAC Origen: MAC\_A  
- MAC Destino: MAC\_Router

17)¿Qué tipo de servicio ofrece Frame Relay? ¿Que ventaja tiene respecto de un enlace

dedicado?   
  
Frame Ralay ofrece **retransmisión de tramas** para redes de circuito virtual, con SVC (circuitos virtuales conmutados) o PVC (circuitos virtuales permanentes) respecto a un enlace dedicado este no ofrece ancho de banda compartido mientras que FrameRelay sí con sus circuitos virtuales.

18)¿Con FR las tramas llegan en orden al destinatario?   
  
Si usan todas la misma trama del circuito virtual, a menos que este se rompa todas van a llegar en el mismo orden**.**

19)¿Qué son los DLCI?   
  
*Data Link Connection Identifier* (DLCI) es el identificador de canal del circuito establecido en Frame Relay. Este identificador se aloja en la trama e indica el camino a seguir por los datos, es decir, el circuito virtual establecido.

El DLCI puede valer normalmente entre 0 y 1023 (10 bits), los valores del 0 al 15 y del 992 en adelante están reservados para funciones especiales.  
El DLCI tiene significado local, es decir, en el circuito virtual cada extremo puede tener un identificador de circuito diferente para identificar el mismo circuito.  
  
  
20)¿Qué es el CIR? ¿para qué se utiliza el bit DE?   
  
El CIR (Committed Information Rate) es la *velocidad media de transmisión* de cada Circuito Virtual. En frame relay se dedica la tasa de trasmisión especificada en CIR.  
DE es un bit de prioridad 0 = alta; 1= baja. Este bit "de desecho" permite seleccionar, cuando la red se "satura", a los que tienen este bit en 1 para descartarlos primero.  
El volumen de tráfico alcanzable transmitiendo a la velocidad media CIR se denomina Bc; si se transmite más de este volumen, las tramas *extras* son marcadas con DE en 1 para que se consideren desechables en caso de congestión.

21)Indique qué funcionalidad provee PPP y cuales descarta este protocolo   
  
**PPP (Point-to-Point Protocol)** es un protocolo para enlaces *punto a punto*, con un host en cada extremo (a diferencia de los *enlaces de broadcast* donde el medio puede ser compartido por múltiples hosts, y los marcos que cada uno envíe son visibles por todos, presentando el *problema del acceso múltiple*).  
El estándar de PPP requiere:

* Packet framing: debe crear los frames encapsulando a los paquetes de capa de red
* Transparencia: no debe imponer límites al contenido de los paquetes de capa de red (limita por ejemplo el uso indiscriminado de patrones de bits para identificar inicio/fin de frames; PPP utiliza un patrón para este fin, pero utiliza también un patrón de "escape" que antepone al primero si aparece en el contenido del frame -por ejemplo, en el datagrama encapsulado-. Si el patrón de escape debe aparece en el contenido,se lo duplica)
* Permitir múltiples protocolos de capa de red al mismo tiempo (esto hace necesario un campo de "tipo de protocolo" en la cabecera PPP para poder multiplexar).
* Múltiples tipos de tecnologías de enlaces -seriales/paralelas, síncronas/asíncronas, de alta/baja velocidad...)
* Detección de errores en los frames.
* Informar a la capa de red de fallas a nivel enlace
* Mecanismo para la negociación de direcciones de red (se utiliza IPCP -IP Control Protocol- en el caso de IP).
* Simplicidad.

Las características que NO requiere (apuntando a la simplicidad):

* Corrección de errores.
* Control de flujo.
* Secuenciamiento (entrega de frames en el mismo orden que se enviaron).
* Enlaces multipunto (sólo se precisa soportar un único emisor y un único receptor).

22)¿Qué son PAP y CHAP?   
  
CHAP (*Challenge Handshake Authentication Protocol*) es un método de autentificación usado por servidores accesibles vía PPP. Verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas:

1. Después del establecimiento del enlace, el agente autentificador manda un mensaje que "desafía" al usuario.

2. El usuario responde con un valor calculado usando una función hash de un sólo sentido, como la suma de comprobación MD5.

3. El autentificador verifica la respuesta con el resultado de su propio cálculo de la función hash. Si el valor coincide, el autentificador informa de la autentificación, de lo contrario terminaría la conexión.

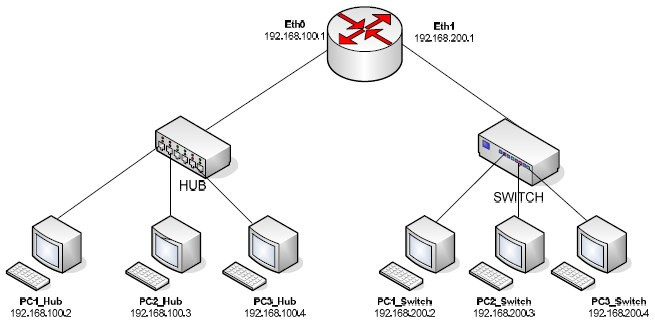
A intervalos aleatorios el autentificador manda un nuevo "desafío" con lo que se repite el proceso.

PAP (Password Authentication Protocol) transmite contraseñas o pasword en ASCII sin cifrar, por lo que se considera inseguro. Se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte. Los identificadores de protocolo están especificados en el RFC 1661. Los más importantes son:

* 0x0021 para IP.
* 0xc021 para LCP.
* 0xc023 para PAP.
* 0xc223 para CHAP.

23)Utilizando el LiveCD provisto por la cátedra, se simulará la red que muestra el

siguiente gráfico:

i. Abra una consola de usuario y ejecute el comando:

topologia capa-enlace start

ii. 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 titulo se corresponde con los nombres que muestra el gráfico:

PC1\_HUB, PC2\_HUB, PC3\_HUB, PC1\_SW, PC2\_SW, PC3\_SW y Router.

iii. 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

iv. 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?   
**Se ven los ECHO REQUEST de PC1\_HUB a PC\_2HUB, y los ECHO REPLY de PC2\_HUB a PC1\_HUB.**

(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)?   
**Al estar conectadas a traves de un SWITCH, PC3\_sw NO puede ver el echo request de PC1\_sw a PC2\_sw ni el echo reply. Esto es porque el hub trabaja en capa fisica y hace broadcast de todo lo que recibe por todas las interfaces, mientras que el switch utiliza la tabla ARP para sólo reenviar por la interfaz adecuada.**

v. Para analizar los paquetes del protocolo ARP realice las siguientes tareas:

(a) Ejecute el comando ifconfig -a en la PC1\_HUB.   
**Muestra todas las interfaces, esten activas o no.**

(b) Luego ejecute el comando arp -n en la PC1\_HUB para ver su tabla ARP.   
**La tabla ARP de PC1\_HUB esta vacia.**

(c) Monitoree el tráfico arp desde la PC3\_HUB ejecutando tcpdump -i eth0 -p

arp.   
**Captura todo el trafico de paquetes del protocolo ARP.**

(d) Envíe un ping desde la PC1\_HUB a la PC2\_HUB y vuelva a observar la tabla ARP

de la PC1\_HUB.   
**Ahora tiene una entrada en su tabla ARP (la PC1\_HUB) con la MAC de PC2\_HUB.**

(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).   
MAC destino 00:00:00 ? en ARP, en Ethernet FF:FF:FF (broadcast)???

arp who-has 192.168.100.3 tell 192.168.100.2 → quien tiene..? dice..  
arp reply 192.168.100.3 is-at fe:fd:00:00:03:00 → MAC de .3

arp who-has pc3\_hub tell 192.168.100.1  
arp reply pc3\_hub is-at fe:fd:00:00:04:00  
arp who-has 192.168.100.1 tell pc3\_hub  
arp reply 192.168.100.1 is-at fe:fd:00:00:01:00   
arp who-has 192.168.100.2 tell 192.168.100.3  
arp reply 192.168.100.2 is-at fe:fd:00:00:02:00

(f) Monitoree el tráfico arp desde la PC3\_SW ejecutando tcpdump -i eth0 -p arp.

(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.

arp who-has 192.168.200.3 tell 192.168.200.2  
arp who-has 192.168.200.1 tell pc3\_sw  
arp reply 192.168.200.1 is-at fe:fd:00:00:01:01

vi. 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.

(b) Monitoree el tráfico desde la PC3\_HUB ejecutando tcpdump -i eth0.

(c) Luego ejecute el comando arp -n en la PC1\_HUB para ver su tabla ARP.

(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?

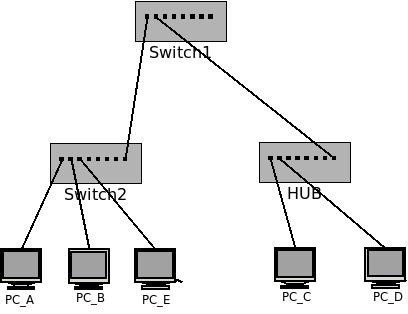
(e) Vea los resultados en la consola de PC3\_HUB a fin de observar tanto los

paquetes arp como los paquetes icmp teniendo en cuenta MAC origen, MAC

destino, IP origen e IP destino según corresponda.

Nota: para finalizar la captura de paquetes resultante del comando tcpdump ejecute ctrl.

+C.   
  
24)Para la siguiente topología de red indique:



1. ¿Cuántos dominios de colisión hay?   
5 dominios de colisiones. Uno el del HUB, otro de switch1 a swirch2, y otros 3 por cada PC al switch2 (PC\_A, PC\_B, PC\_E).  
*- PC A-switch 2,  
- PC B-switch 2,  
- PC E-switch 2,  
- switch 2-switch 1, y  
- switch 1-Hub-PC C-PC D*

2. ¿Cuántos dominios de broadcast hay?   
Solo **uno**, se necesitan routers para separar dominios de broadcast.

3. Indique cómo se va llenando la tabla de asociaciones MAC → PORT del switch SW1 y SW2 durante el siguiente caso:

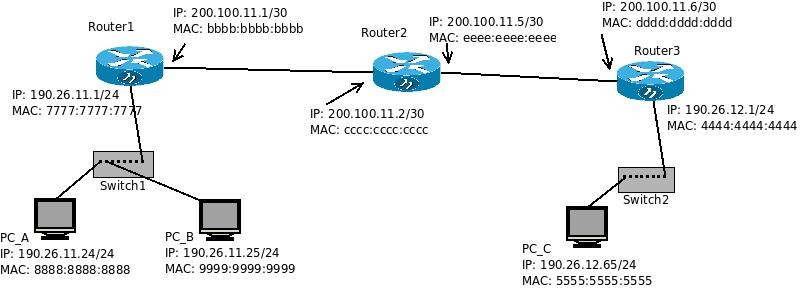
(a) A envía una solicitud ARP consultando la MAC de C   
SW2 agrega a MAC PC A en port #1. SW1 agrega a MAC PC A en port #1.

(b) C responde esta solicitud ARP   
SW1 agrega a MAC PC C en port #2. SW 2 agrega a MAC PC C en port #8.

(c) A envía una solicitud ARP consultando la MAC de B   
(no se alteran las tablas, excepto que pase un tiempo entre esta solicitud y la anterior y se haya quitado la entrada de PC A de las tablas por vencerse su TTL, en cuyo caso se agrega la misma información que en el paso (a))

(d) B responde esta solicitud ARP   
SW2 agrega a MAC PC B en port #2.

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 hubiese escuchado sólo las solicitudes ARP que hizo PC A -(a) y (c)-.  
PC D hubiese escuchado la solicitud ARP de PC A por la MAC de PC C (a), y la respuesta de PC C (b). También hubiese escuchado la solicitud ARP por la MAC de PC B (c), pero no hubiese escuchado la respuesta.  
  
  
25)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:

-¿Qué protocolos de capa 2 aparecen? ¿En qué dominios de broadcast?   
Hay **4 dominios de broadcast:**1 - del router 1 hacia el switch1/**PC\_A**/PC\_B  
2 - del router 1 al router 2  
3 - del router 2 al router 3  
4 - del router 3 hacia el switch2/**PC\_C**  
Ethernet y ARP -capa 2- aparece en todos.

-¿Qué protocolos de capa 3 aparecen? ¿En qué dominios de broadcast?   
  
ICMP e IP -capa 3 ambos (ICMP utiliza IP como si fuese de nivel superior aunque se considera también de nivel 3)- aparece en todos**.**

-¿Cuál es la secuencia correcta en la que se suceden los anteriores?   
  
 -PC A hace ARP Request para obtener la MAC de router 1.

-Router 1 envía su MAC con ARP response.

-PC A envía datagrama ICMP con IP destino 190.26.12.65/24 con MAC destino 7777:7777:7777. IP origen = PC\_A , MAC\_ORIGEN: MAC\_A

-Router 1 hace ARP Request para obtener MAC de router 2.

-Router 2 envía su MAC en ARP Response.

-Router 1 envía el datagrama ICMP cambiando la MAC origen por la suya propia y la MAC destino a cccc:cccc:cccc (**no toca la capa 3**)

-Router 2 hace un ARP Request para obtener la MAC de Router 3.

-Router 3 envía su MAC en ARP Response.

-Router 2 envía el datagrama ICMP cambiando la MAC origen por la suya propia y la MAC destino a dddd:dddd:dddd

-Router 3 detecta que la IP destino está en su misma subred. Hace un ARP request para obtener la MAC de PC\_C.

-PC\_C responde con su MAC en un ARP response.  
-Router 3 envía el datagrama modificando la MAC origen por la suya propia y la MAC destino a 5555:5555:5555 (PC\_C)  
**La capa 3 no se modifica** (IP origen y IP destino)

Para los paquetes del protocolo de capa 3 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 |