**Práctica 10**

**Capa de Enlace - Parte I**

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

Para transmitir un datagrama a través de un enlace individual se utiliza un protocolo de la capa de enlace. El protocolo de la capa de enlace define el formato de los paquetes intercambiados por los nodos situados en los extremos del enlace, así como las acciones que estos nodos llevan a cabo cuando se envían y reciben los paquetes.

**Las unidades de datos intercambiadas por un protocolo de la capa de enlace se denominan tramas** (frames), y cada trama de la capa de enlace suele encapsular un datagrama de la capa de red.

**Mientras que la capa de red tiene asignada la tarea de mover los segmentos de la capa de transporte terminal a terminal desde el host de origen hasta el host destino, el protocolo de la capa de enlace tiene la tarea nodo a nodo, algo más simple, de mover los datagramas de la capa de red a través de un único enlace dentro de una ruta.** Un mismo datagrama de la capa de enlace puede ser transportado por diferentes protocolos de la capa de enlace en los distintos enlaces que forman la ruta. Es importante observar que los servicios proporcionados por los diferentes protocolos de la capa de enlace a lo largo de la ruta terminal a terminal pueden ser distintos.

SERVICIOS:

* ENTRAMADO o encapsulación: Casi todos los protocolos de la capa de enlace encapsulan 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 Control) especifica las reglas que se utilizan para transmitir una trama a través de un enlace.

Para los enlaces punto a punto que tengan un único emisor en un extremo del enlace y un único receptor en el otro extremo, el protocolo MAC es muy simple (o no existe).

Cuando hay varios nodos compartiendo un mismo enlace de difusión, en cuyo caso se presenta el denominado problema del acceso múltiple. En este caso, el protocolo MAC sirve para coordinar la transmisión de las tramas de los múltiples nodos.

* ENTREGA FIABLE: Cuando se implementa, garantiza que va a transportar cada datagrama de la capa de red a través del enlace sin que se produzcan errores.
* Para los enlaces inalámbricos es muy útil ya que tienen una alta tasa de errores.
* Para los cableados puede considerarse una sobrecarga innecesaria ya que tienen una baja tasa de errores.
* CONTROL DE FLUJO: Los nodos situados en cada extremo de un enlace tienen una capacidad limitada de almacenamiento en buffer de tramas. Esto puede ser un problema cuando el nodo receptor puede recibir las tramas a más velocidad de la que puede procesarlas. Sin control de flujo, el buffer del receptor puede desbordarse con lo que las tramas se perderían. La idea es que el nodo emisor no abrume al nodo receptor.
* DETECCION DE ERRORES: Los errores de bit se introducen debido a la atenuación de las señales y al ruido electromagnético. Muchos protocolos de la capa de enlace proporcionan un mecanismo para detectar dichos errores de bit. Esto se lleva a cabo haciendo que el nodo transmisor incluya bits de detección de errores en la trama y que el nodo receptor realice una comprobación de errores. En general es más sofisticada que la de la capa de transporte y se implementa en hardware.
* CORRECCION DE ERRORES: Es similar a la detección de errores, pero además, el receptor determina exactamente en qué puntos de la trama se han producido errores y los corrige. Algunos solo corrigen la cabecera y la cola (no el paquete completo).
* 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 puede transmitir 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, el servicio de entrega fiable. Aunque los mecanismos utilizados para esto son similares en las dos capas, 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 en un protocolo de la capa de enlace se proporciona entre dos nodos adyacentes.

◘ **Cada host y router que compone una red se lo llama nodo. La capa de transporte provee a los procesos comunicación host a host, utilizando routers y otros dispositivos de otras capas para poder proveer la comunicación. En cambio, la capa de enlace provee comunicación nodo a nodo, es decir, entre cada dispositivo que conforma la red para poder establecer la comunicación que la capa de transporte quiere establecer.**

La capa de enlace le brinda servicios a la capa de red, y la capa de transporte le brinda servicios a la capa de aplicación.

**3. Direccionamiento Ethernet:**

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

Las máquinas en una LAN se identifican a nivel de Enlace por la dirección LAN/Ethernet/Física/MAC asociada a su placa de red, normalmente grabada en su memoria ROM.

Se identifican a partir de dirección MAC (En realidad esto identifica a cada placa de red, a cada interfaz).

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

Dirección MAC (Media Access Control)

En la mayoría de las LAN (Redes Ethernet y LAN inalámbricas 802.11) **la dirección MAC tiene 48 bits de longitud, lo que da 2^48 posibles direcciones MAC.**

**Suelen expresarse en notación hexadecimal, indicándose cada byte de la dirección mediante una pareja de números hexadecimales.**

Nunca puede haber dos placas de red con la misma dirección MAC.

La IEE se encarga de gestionar el espacio de direcciones MAC, asignando espacios de direcciones a los fabricantes de placas.

Recuerde que la IP tiene una estructura jerárquica (una parte de red y una parte de host) y es necesario modificar la dirección IP de un nodo cuando el host se mueve, es decir, cuando cambia la red a la que el host está conectado.

**Dirección MAC es análogo al número de carnet de identidad. La IP es análogo a la dirección postal.**

**¿Cuál es la dirección de broadcast en capa de enlace? ¿Qué función cumple?**

En ocasiones, un adaptador de un emisor sí que quiere que todos los demás adaptadores de la LAN reciban y procesen la trama que va a enviar. En este caso, el adaptador emisor inserta una dirección de difusión MAC especial en el campo de la dirección de destino de trama. Para las redes LAN que utilizan direcciones de 48 bits, la dirección de difusión es una cadena compuesta por 48 unos (1) consecutivos (es decir, FF-FF-FF-FF-FF-FF en notación hexadecimal).

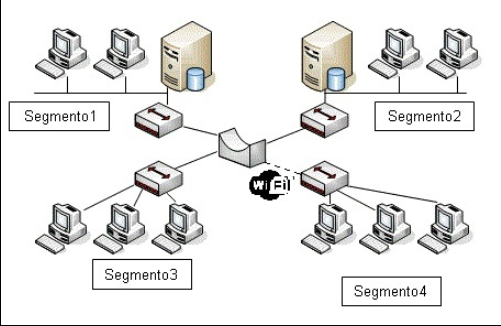
**4. Sobre los dispositivos de capa de enlace:**

**Enumere dispositivos de capa de enlace y explique sus diferencias.**

* Bridges: **son como switches que unen distintas tecnologías.** Son dispositivos de interconexión de redes de computadoras que **separan dominios de colisiones** y debido a esto pueden utilizarse para separar la red en partes más pequeñas.

**Funciona a través de una tabla de direcciones MAC**. Cuando detecta que un nodo de uno de los nodos en un segmento está intentando transmitir datos a un nodo de otro, el bridge copia la trama para la parte de la red, teniendo la capacidad de desechar la trama (filtrado) en caso de no tener dicho segmento como destino. **Para conocer por dónde enviar cada trama que le llega (encaminamiento) incluye un mecanismo de aprendizaje automático (auto aprendizaje) por lo que no necesitan configuración manual.**

Ejemplo de 4 subredes conectadas mediante un bridge:



* Repetidor: **Es un dispositivo electrónico que conecta dos segmentos de una misma red,** transfiriendo el tráfico de uno a otro extremo, bien por cable o inalámbrico. La principal diferencia con un bridge es que **éstos hacen pasar todas las tramas que llegan al segmento, independientemente de que se encuentre o no allí el dispositivo de destino. El bridge las descartaría reduciendo el tráfico.**

Los segmentos de red se limitan en cuanto a la distancia entre unos y otros; si es por cable, generalmente no superan los 100 M., debido a la perdida de señal y la generación de ruido en las líneas.

Con un repetidor se puede evitar este problema, ya que reconstruye la señal eliminando los ruidos y la transmite de un segmento al otro.

En la actualidad los repetidores se han vuelto muy populares a nivel de redes inalámbricas o WIFI.

El Repetidor amplifica la señal de la red LAN inalámbrica desde el router al ordenador. Un Repetidor, por tanto, actúa sólo en el nivel físico.

* HUB: Los hubs son repetidores multipuerto. Trabajan a nivel fisico.



* Switch: Los switches suelen ser bridges multipuerto, que trabajan con la misma tecnología de la capa de enlace y física en cada puerto. Utilizar switches **permite dividir la red, mejorar la seguridad, mejorar el rendimiento y evitar las colisiones**. Los switches también poseen menor delay. **Guardan las direcciones MAC asociadas a cada puerto y pueden filtrar tramas a través de estas direcciones de MAC** (y se evita el flooding). En otras palabras, **cuando llega información al conmutador éste tiene mayor conocimiento sobre qué puerto de salida es el más apropiado, y por lo tanto ahorra una carga (“bandwidth”) a los demás puertos del Switch.**
* Router: **Operan entre redes aisladas** que utilizan protocolos similares, encaminando la información de acuerdo con la mejor ruta posible.

**¿Qué es una colisión?**

Si dos o más nodos transmiten simultáneamente por el mismo enlace (half-duplex) se produce una colisión ya que se mezclan las señales. Hay que retransmitir.

**¿Qué dispositivos dividen dominios de colisión?**

Los **switches, bridges y routers** dividen los dominios de colisión. Los delimitan. **Hacen que no se propague la colision, que no se colisione en todos los lados conectados a ellos.**

En cambio, los repetidores y hubs PROPAGAN las colisiones. Hacen que el dominio de colision se haga mas extenso.

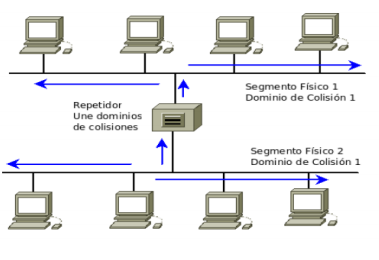
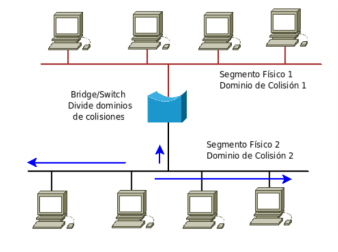
Los dominios de colisión representan un segmento físico de una red donde es posible que las tramas puedan interferir unas con otras. Estas colisiones se dan particularmente en el protocolo de red Ethernet. A medida que aumenta el número de nodos que utilizan una red aumenta también las posibilidades que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Cuando aumenta el número de colisiones disminuye el rendimiento de una red.

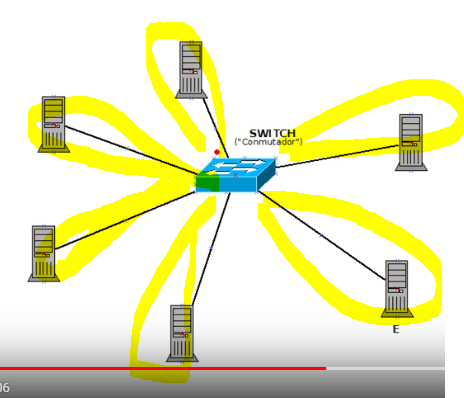
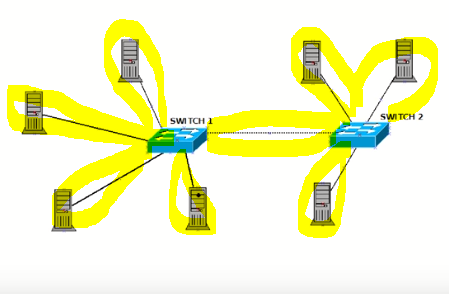
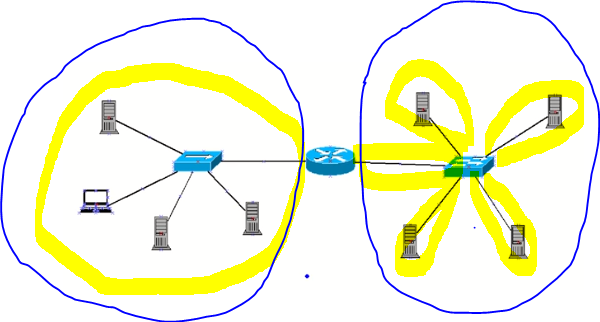
Cuando un host se conecta a un switch este crea una conexión dedicada. Esta conexión se considera un dominio de colisiones individual, ya que el tráfico se mantiene separado de cualquier otro, y por consiguiente se eliminan las posibilidades de colision.

Los switches eliminan las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que usan un ancho de banda dedicado para cada segmento de red.

UN SWITCH CONMUTA PAQUETES, ES DECIR LOS MANDA DIRECTAMENTE A SU DESTINO, GRACIAS A LA INFO QUE VA ALMACENANDO DE QUE MAC ESTA CONECTADA A QUE PUERTO. **ES INTELIGENTE**.

POR CADA BOCA TIENE UN DOMINIO DE COLISION.

* Ejemplo de un switch separando dominios de colisiones por c/ entrada (Notar es un único dominio de broadcast)
* Ejemplo con 2 switches. Cada boca es un dominio de colision diferente, incluso el enlace que une a los switches. Notar que igual que en el caso anterior, tenemos un solo dominio de broadcast, una sola red. 
* Ejemplo con un hub (repetidor multipuerto), un router y un switch. Tenemos 6 dominios de colision, y 2 de broadcast (hay 2 redes) 

**FUENTE IMPORTANTE:** [**https://www.youtube.com/watch?v=LqisP3H2SIA**](https://www.youtube.com/watch?v=LqisP3H2SIA)

**En cuanto a colisiones ...**

* **Los hubs/repetidores son dispositivos bobos. Lo que les llega desde algun dispositivo conectado a ellos se lo mandan a todos.**
* **En cambio, los switches, bridges y routers son dispositivos inteligentes, eligen a quien mandarle determinada trama segun la info que van recolectando. Por eso decimos habra un dominio de colision por cada BOCA del switch/bridge/router.**

**¿Qué dispositivos dividen dominios de broadcast?**

Los routers dividen los dominios de broadcast. Los delimitan.Un dominio de broadcast representa a una red. Sabemos los routers separan redes.

Los repetidores, hubs, bridges y switches los propagan.

**El dominio de broadcast es el conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto.**

Como el router es el dispositivo que se encarga de separar redes diferentes, los dominios de broadcast quedan delimitados por este, y entonces hay un dominio de broadcast por cada interfaz del router, por cada una de las redes separadas por un router (para que se haga el broadcast en los equipos de UNA red, la del que quiere difundir).

**Habrá un dominio de broadcast por cada BOCA de un router.**

**5. Describa el algoritmo de acceso al medio en Ethernet. ¿Es orientado a la conexión? (MAC)**

LAN Ethernet es una auténtica LAN de difusión; es decir, cuando un adaptador transmite una trama, todos los adaptadores de la LAN reciben esa trama. **Dado que Ethernet, puede emplear la comunicación por difusión, necesita un protocolo de acceso múltiple.** Utiliza protocolo de acceso múltiple CSMA/CD (Carrier Sense Multiple Access with Colision Detect).

En Ethernet se utiliza un canal simple de difusión compartida, con acceso aleatorio (cualquier nodo puede transmitir en un instante de tiempo, es decir, no está predefinido en ranuras qué nodo puede transmitir): 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 sondea el medio compartido (no utiliza ningún "slot”, ranura o partición de tiempo, frecuencia o código), es decir, utiliza un mecanismo de detección de colisiones. 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 bloqueo , 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-.

PASOS:

1. El adaptador recibe un datagrama de la capa de red y crea la trama.
2. Si el adaptador sensa que el canal está libre, éste comienza a transmitir la trama. Si éste sensa canal ocupado, espera hasta que esté libre y transmite.
3. Si el adaptador transmite la trama entera sin detectar colisión, se considera transmisión lograda.
4. Si el adaptador detecta otra transmisión mientras transmite, aborta y envía una señal de bloqueo (jam)
5. Después de abortar, el adaptador entra en backoff exponencial: después de la m-ésima colisión, el adaptador elige un K aleatorio entre {0, 1, 2, …, 2^m-1}. El adaptador espera K·512 periodos de 1 bit y retorna al paso 2

**6. Investigue los comandos arp e ip neigh.**

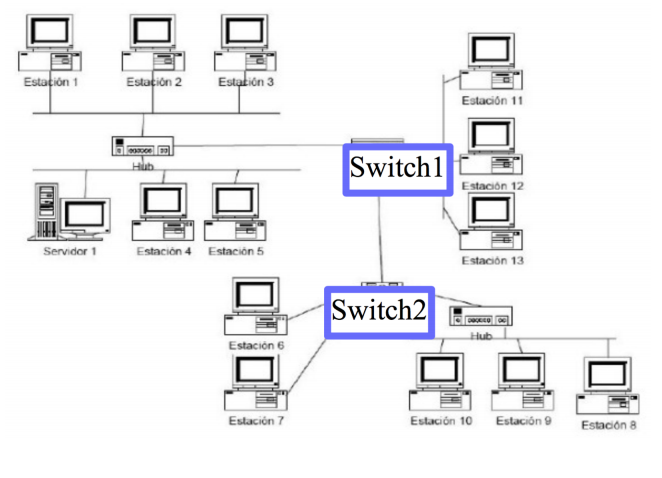
En red de computadoras, el protocolo de resolución de direcciones (**ARP,** del inglés Address Resolution Protocol) es un **protocolo de comunicaciones de la capa de enlace, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.**

ARP significa Address Resolution Protocol o protocolo de resolución de direcciones. ARP se utiliza para supervisar y modificar la tabla de asignaciones de direcciones IP y direcciones MAC (Media Access Control). ARP utiliza un cache que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones MAC y el nivel de red de las direcciones IP. ARP asocia direcciones IP a las direcciones MAC.

**Inicie una topología con CORE, cree una máquina y utilice en ella los comandos anteriores para:**

* **Listar las entradas en la tabla ARP.** 
  + arp -a
  + ip neigh
* **Borrar una entrada en la tabla de ARP.**
  + arp -d 10.0.1.2
  + ip neigh del 10.0.1.2 dev eth0
* **Agregar una entrada estática en la tabla de ARP.**
  + arp -s 10.0.0.2 00:0c:29:c0:94:bf (host con dirección IP 10.0.0.2 tiene MAC 00:0c:29:c0:94:bf)
  + ip neigh add 10.0.2.1 lladdr 10.0.0.2 00:0c:29:c0:94:bf dev eth0

**7. Dado el siguiente esquema de red, responda:**

****

**a. Suponiendo que las tablas de los switches están llenas con la información correcta (MAC-PORT), responda quién escucha el mensaje si:**

**i. La estación 1 envía una trama al servidor 1.**

Estaciones 2, 3, 4, 5 y el servidor 1. El switch 1 también escucha, pero no deja pasar porque el paquete no va dirigido a la subred que tiene al otro lado.

**ii. La estación 1 envía una trama a la estación 11.**

Estaciones 2, 3, 4, 5 y 11. También el servidor 1, y el switch 1.

**iii. La estación 1 envía una trama a la estación 9.**

Estaciones 2, 3, 4, 5, 10, 8 y 9. Servidor 1. El switch 1 redirige hacia el switch 2.

**iv. La estación 4 envía una trama a la MAC de broadcast.**

Lo escuchan todos. La única forma en que no lo escuchen todos es que haya algún router, es que es único dispositivo que separa dominios de broadcast.

**v. La estación 6 envía una trama a la estación 7.**

La estación 7 y el switch 2. El switch 2 crea un canal directo entre las estaciones.

**vi. La estación 6 envía una trama a la estación 10.**

Estaciones 8, 9 y 10. Switch 2.

Nota: Según Cami, no hay que poner los switches.

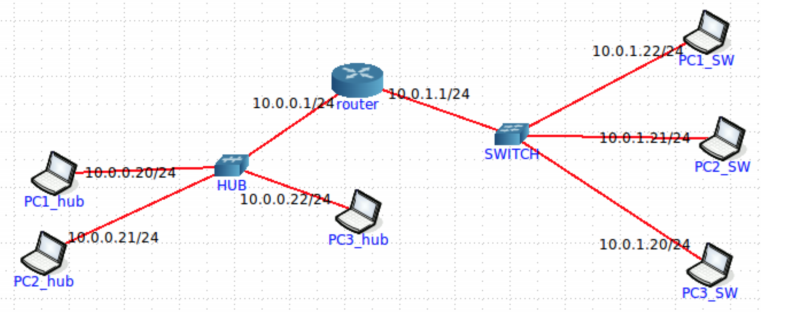
**b. ¿En qué situaciones se pueden producir colisiones?**

Puede haber colisiones en todas aquellas que pasaron por un hub, ya que a diferencia del switch, el hub no crea un “canal exclusivo”. Todos pueden enviar al mismo tiempo y podría haber.

Por ende, la única en la que no podría haber colisiones es en la V.

**8. Utilizando la máquina virtual provista por la cátedra, arme una red como la siguiente, con un segmento de**

**LAN usando un HUB y otro segmento de LAN usando un SWITCH:**

****

**a. Observar las diferencias en el funcionamiento de un hub y de un switch realizando las siguientes tareas:**

**i. Envíe un ping desde la PC1\_HUB a PC2\_HUB y monitoree el tráfico en PC3\_HUB (botón derecho ->Tcpdump ->eth0) ¿Se pueden ver los pings?**

Si, se puede ver que PC3\_HUB recibe las tramas enviadas a traves del hub.

**ii. Envíe un ping desde la PC1\_SW a PC2\_SW y monitoree el tráfico en la PC3\_SW (botón derecho ->Tcpdump ->eth0) ¿Se pueden ver los pings? ¿En PC3\_HUB debería poder ver algo?**

**No se pueden ver los pings en PC3\_SW**, pero se ve un who-has de parte de PC1\_SW (reenviado por el switch)

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

La finalidad del protocolo ARP es la resolución de direcciones IP en direcciones MAC y el mantenimiento de una caché de las asignaciones.

La necesidad por este protocolo surge de que para que una trama se coloque en los medios LAN primero es necesario que cuente con una dirección MAC destino. Para esto, el nodo primero consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos que se mapea a la direccion IP de destino, llamada tabla ARP. Cada entrada de la tabla cuenta con una dirección IP a la que se le corresponde una dirección MAC. Una manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud ARP. El ARP envía un broadcast a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud ARP con la dirección IP del host de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya responde enviando un paquete de respuesta de ARP al emisor con una trama unicast. Esta respuesta se utiliza para crear una entrada nueva en la tabla ARP. Para cada dispositivo, un temporizador de cache ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y sus sistema operativo. Ejemplo: en caso que un host salga de la red LAN, si no se borra la entrada caché de ARP en la tabla de otros hosts, es posible que intenten comunicarse con el host que salió de la red.

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

Los nodos crean sus tablas de ARP sin intervención del administrador. **AUTOAPRENDIZAJE**.

**10. Usando la topología anterior:**

**a. Analizar el protocolo ARP y su encapsulamiento Ethernet:**

**i. Visualice la dirección IP y la dirección MAC de la interface de red de PC1\_HUB.**

**ii. Obtenga las entradas cargadas en la tabla ARP en PC1\_HUB.**

**iii. Monitoree el tráfico ARP en PC3\_HUB ejecutando tcpdump -n -e -i eth0 -p arp o con botón derecho ->Tcpdump ->eth0.**

**iv. Envíe un ping desde PC1\_HUB a PC2\_HUB y vuelva a observar la tabla ARP de PC1\_HUB.**

**v. Analice la información capturada en PC3\_HUB a fin de observar la información tanto del ARP REQUEST y del ARP REPLY como la información de la trama Ethernet que los encapsula.**

**b. Analizar el protocolo ICMP y su encapsulamiento IP y Ethernet:**

**i. Envíe un ping desde PC1\_HUB a PC2\_HUB.**

**ii. Monitoree el tráfico ICMP en PC3\_HUB ejecutando tcpdump -n -e -i eth0 -p icmp o con botón derecho ->Tcpdump ->eth0.**

**iii. Analice la información capturada en PC3\_HUB a fin de observar la información de capa 2 y capa 3 que encapsulan el ICMP ECHO REQUEST y el ICMP ECHO REPLY.**

* **Capa 2 (Ethernet): MAC origen / MAC destino.**
* **Capa 3 (IP): IP origen / IP destino.**

**c. Conclusiones.**

**i. Borre todas las entradas de la tabla ARP de PC1\_HUB.**

**ii. Desde PC1\_HUB con la tabla ARP vacía, haga un ping a PC2\_SW. En base a lo observado previamente, ¿cuáles de los paquetes ARP e ICMP se deberían poder observar en PC3\_SW?**