**Capa de Enlace - Parte I Redes y comunicaciones - 2022**

**Práctica 10. Capa de Enlace - Parte I**

**5, 9, 12**

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

Teoría:

La capa de enlace transfiere datagramas desde un nodo (host y routers) a otro adyacente, a través de un link (Canal de comunicación que conecta nodos adyacentes mediante caminos. Pueden ser cableados, inalámbricos o LANs).

La PDU de esta capa es el frame o trama, que encapsula un datagrama de la capa de red.

Los datagramas son transferidos por diferentes protocolos de enlace sobre distintos enlaces, es decir, pueden ser transportados por diferentes protocolos en los distintos enlaces que forman la ruta.

Estos protocolos definen el formato de los paquetes intercambiados por los nodos del enlace, así como las acciones que estos nodos llevan a cabo cuando se envían y reciben los paquetes. Son:

* Ethernet en el primer enlace,
* frame relay en los intermedios,
* 802.11 en el último enlace

Cada protocolo de enlace brinda diferentes tipos de servicios. Puede o no proveer RTD (Reliable data transfer) sobre el enlace.

Analogia transporte:

Viaje desde montevideo a MDP.

Turista: Datagrama.

Segmento de transporte: Enlace de comunicación.

Modo de transporte: Protocolo de capa de enlace

Agencia de viaje: Algoritmo de enrutamiento

Práctica larga:

Capa de red 🡪 mueve segmentos de la capa de transporte terminal a terminal desde el host de origen hasta el host destino,

Capa de enlace 🡪 mueve los datagramas de la capa de red a través de un único enlace dentro de una ruta, es decir, nodo a nodo.

Ej: De un Router → Switch, Switch → PC, PC → Repetidor, etc.

Servicios:

(Lo que esta sin el punto negro es de la otra practica)

**Entramado (framing):**

* Encapsulado del datagrama en la trama, agregando encabezado (header) y cola (trailer)

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:**

* Acceso al canal si es un medio compartido (medium access control)
* Direcciones "MAC" addresses utilizados en los encabezados de las tramas para identificar el origen y el destino
  + Distintas de las direcciones IP

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 confiable:**

* Entre nodos adyacentes
* ¡Ya aprendimos como hacer esto (Teo capa de transporte)
* Rara vez utilizados en enlaces de pocos errores (Fibra óptica, algunos pares trenzados)
* Enlaces inalámbricos: Alta tasa de error.

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.

**Control de flujo:**

* Acuerdo entre los nodos emisor y receptor (Aquí, adyacentes)
* Recordar: buffers y capacidad de procesamiento

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.

**Detección de errores**

* Errores causados por atenuación de la señal, por ruido
* El receptor detecta presencia de errores: Señaliza al emisor para una retransmisión o descarta la trama

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 (FEC: forward error correction):

* El receptor identifica y corrige el/los error/es en bit/s sin necesidad de retransmision

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).

Half-duplex and full-duplex:

* Con half-duplex, los nodos en los extremos del enlace pueden transmitir, pero no al mismo tiempo

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 servicios proporcionados por estas capas tienen similitudes:

* Servicio de entrega fiable. Los mecanismos utilizados son similares en las dos capas, pero no 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.
* Servicios de control de flujo y detección de errores: 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.
* Comunicación. 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. La capa de enlace provee comunicación nodo a nodo, es decir, entre cada dispositivo que conforma la red.
* 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 (En realidad esto identifica a cada placa de red, a cada interfaz) asociada a su placa de red, normalmente grabada en su memoria ROM.

Se identifican con direcciones físicas, las de capa de enlace.

**¿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 (N° de 30 cifras anda a escribirlo) 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 IEEE gestiona el espacio de direcciones MAC, asignándolos a los fabricantes de placas.
* Los 24 bits más significativos identifican al fabricante; los menos significativos son el número de serial, dentro del fabricante
* 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 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.
* Se agrupan de a octetos, separados por “:”
* No se repiten, aunque se puede editar por software

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

En ocasiones, un emisor quiere que todos los demás adaptadores de la LAN, o hosts pertenecientes a ese mismo dominio de broadcast, reciban la trama que va a enviar. En este caso, la dirección de difusión es una cadena compuesta por 48 unos (1) consecutivos (es decir, FF:FF:FF:FF:FF:FF en notación hexadecimal).

Si la IP es de broadcast, la MAC a usar también lo será. Útil para ARP y DHCP de IPv4

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

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

De la teoría:

Dispositivos: Repetidor. Bridge. Switch. Router.

**Repetidor/Hub**

* Repetidor: amplificador digital, dos puertos. Regenera la señal un dominio de colisión generando un

único, permite extensión.

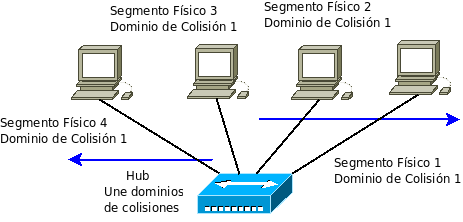
La trasferencia se limita según la distancia: si es por cable, generalmente no supera los 100m, debido a la pérdida de señal y el ruido en las líneas. Con un repetidor se soluciona esto, ya que reconstruye la señal eliminando los ruidos y la transmite de un segmento al otro.

Conecta dos segmentos de una misma red, transfiriendo el tráfico de uno a otro extremo, por cable o inalámbrico.

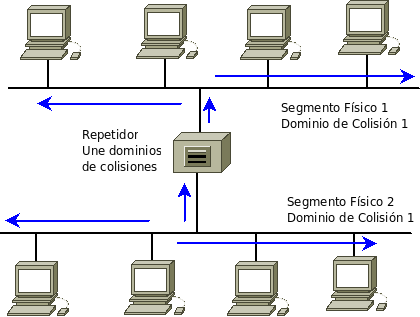
Diferencia con un bridge: Los hubs hacen pasar todas las tramas que llegan, independientemente de que se encuentre o no allí el dispositivo de destino, mientras que el bridge las descartaría reduciendo el tráfico.

* Hub: repetidor multipuerto. Usado en 10BaseT y 100BaseT.

➔ HUB: Los hubs son repetidores multipuerto. Trabajan a nivel físico.

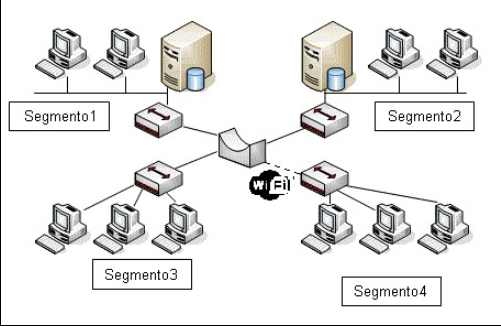


Repetidor:



Tipos de Hubs

* Hubs pasivos: solo envían la señal por todos los puertos restantes.
* Hubs activos: regeneran la señal, mayor alcance.
* Hubs inteligentes: pueden poseen administración, permiten detectar problemas.
* Los hubs pueden detectar colisiones y generar JAMs.

**Bridge**

* Adaptar dos protocolos de nivel de enlace o físico.
* Dividir la red en partes más pequeñas: dominios de colisiones. Permitir escalabilidad.
* Implementado por software.
* Dos puertos en general.
* Bridge Ethernet podría adaptar dos tecnologías de nivel físicas, e.g.: 10Base2 y 10BaseT.

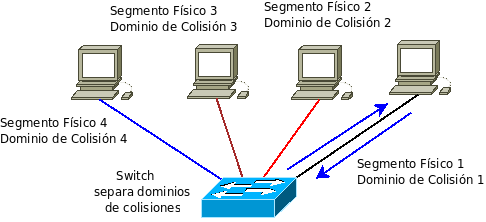
Funciona a través de una tabla de direcciones MAC. Cuando un nodo está intentando transmitir datos a un nodo de otro segmento, el bridge copia la trama para la parte de la red, pudiendo desechar la trama (filtrado) en caso de no tener dicho segmento como destino.

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.

* Tiene dos puntos de conexión, alámbricos o inalámbricos, donde cada uno se conecta a una red distinta
* Examina las tramas de cada red, “aprendiendo” hacia cual se dirigen (según la MAC destino), y en función de eso decide si transmitirlo al otro lado o no

**Switch**

* Bridge multipuerto que trabaja con la misma tecnología de enlace y física en c/u. Sus puertos son alámbricos o inalámbricos, y cada uno se conecta a un host o a otro switch
* Trabaja en hardware, ASIC, múltiples puertos.
* Puertos trabajan en FDX, micro-segmentación.
* Examina las tramas entrantes por cada punto, “aprendiendo” hacia qué nodo se dirigen (según la MAC destino), y en función de eso filtra

Permite dividir la red, mejorar la seguridad, mejorar el rendimiento y evitar las colisiones. Guarda las direcciones MAC asociadas a cada puerto y pueden filtrar tramas a través de estas direcciones de MAC (y se evita el flooding). Cuando le llega información sabe qué puerto de salida es el más apropiado, y por lo tanto ahorra una carga (“bandwidth”) a los demás puertos del Switch.

Razones para usar switches en una red:

* Dividir la red en partes más pequeñas (dominios de colisiones, micro-segmentación).
* Seguridad: VLANs, admin.
* Mejorar el rendimiento de la red. FDX vs. HDX.
* No hay colisiones.
* Los switches tienen menor delay.
* Actualidad Switches multilayers o L3/capa3.

Funciones

* Aprender direcciones MAC: El dispositivo guarda las direcciones MAC asociadas a cada puerto.
* Reenviar / filtrar paquetes: Al recibir una trama, el switch revisa su base de datos MAC para determinar a través de que puerto puede alcanzar la dirección de destino.
* Evitar bucles de capa 2: Los switches administran los bucles de redundancia con STP. Bridges solo unainstancia de STP, switches podrían correr varias,

● Router: Operan entre redes aisladas que utilizan protocolos similares, encaminando la información de acuerdo con la mejor ruta posible.

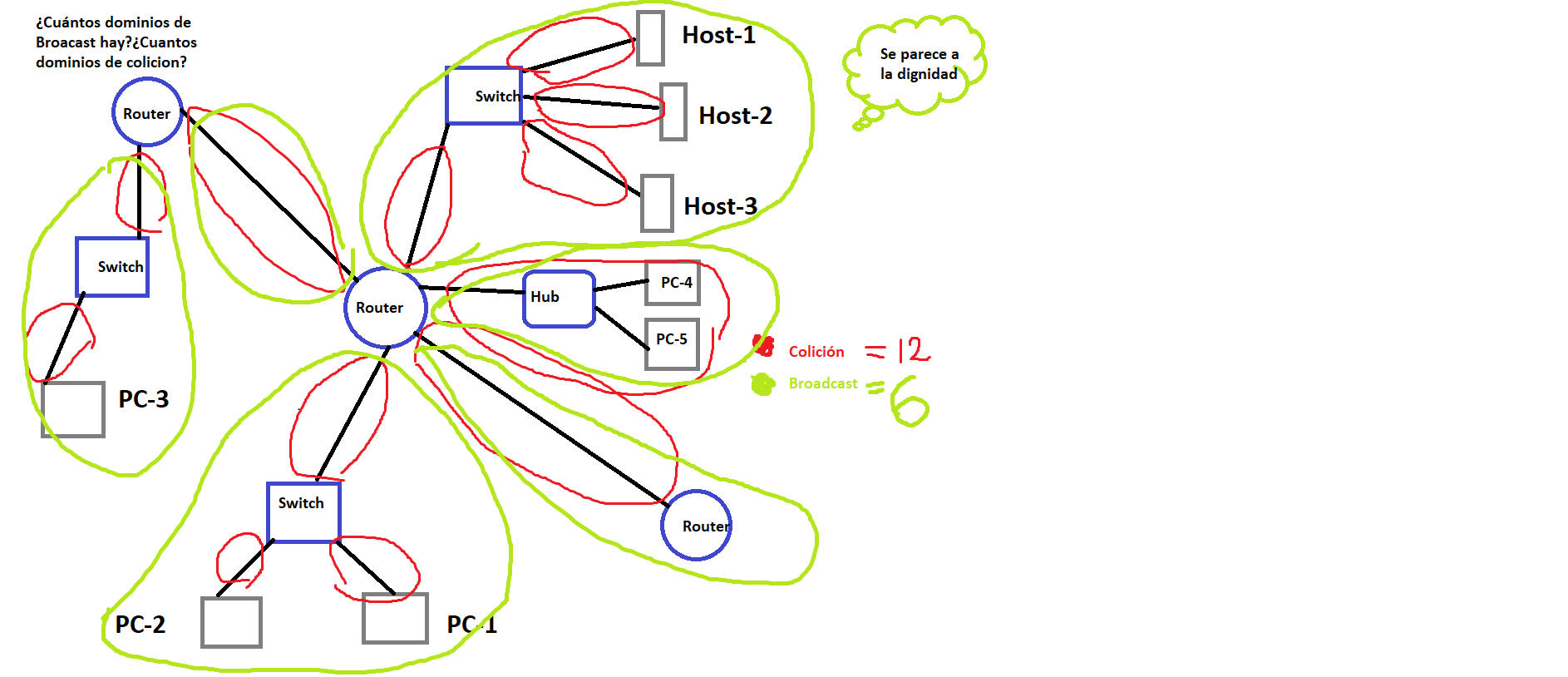
**¿Qué es una colisión?**

b) Una colisión se da cuando dos dispositivos, pertenecientes a un mismo dominio de colisión, emiten datos al mismo tiempo. La señal que produce cada una se mezcla con la otra, resultando en una ruidosa

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. Similar a cuando hablas con alguien, si hablan al mismo tiempo no se entiende completamente lo que dice y hay que repetir lo dicho.

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

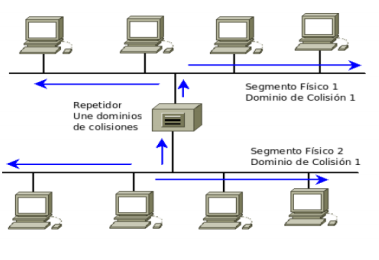
El dominio de broadcast es el conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto.

Un dominio de broadcast representa a una red y los routers separan redes, por lo tanto, estos dividen o delimitan los dominios de broadcast.

Los repetidores, hubs, bridges y switches los propagan.

Como el router separa redes, los dominios de broadcast quedan delimitados por este, y hay un dominio de broadcast por cada interfaz del router.

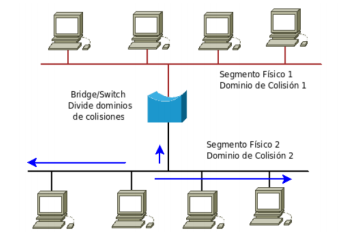
Habrá un dominio de broadcast por cada BOCA de un router. Otro Ej. de Dominio de colisión y broadcast



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

Los switches, bridges y routers dividen y delimitan los dominios de colisión, hacen que no se propague la colisión, 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 colisión se haga más extenso.

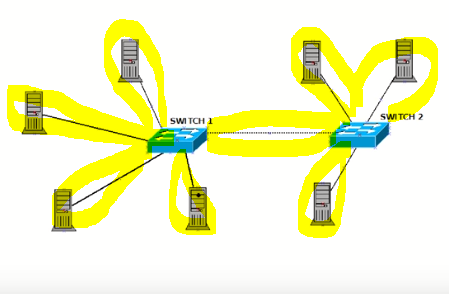
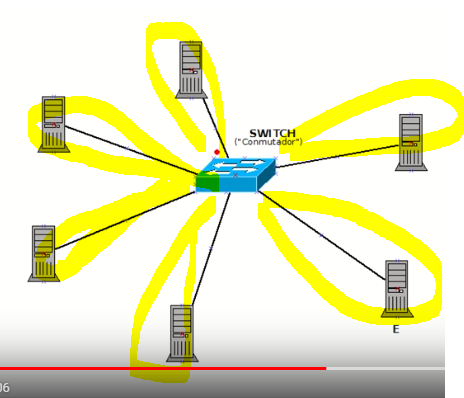
Los dominios de colisión representan un segmento físico de una red donde es posible que las tramas puedan interferir unas con otras. Estas colisiones se dan particularmente en el protocolo de red Ethernet. A medida que aumentan los nodos, aumentan posibilidades que dos de ellos transmitan a la vez. Esta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

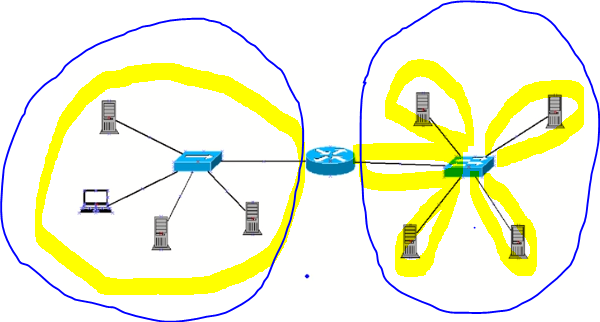
UN SWITCH CONMUTA PAQUETES, ES DECIR LOS MANDA DIRECTAMENTE A SU DESTINO, GRACIAS A LA INFO QUE VA ALMACENANDO DE QUE MAC ESTA CONECTADA A QUE PUERTO. ES INTELIGENTE.

POR CADA BOCA TIENE UN DOMINIO DE COLISIÓN.



● 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 colisión diferente, incluso el enlace que une a los switches. Hay 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)

<https://www.youtube.com/watch?v=LqisP3H2SIA>

En cuanto a colisiones ...

- Los hubs/repetidores son dispositivos bobos. Lo que les llega desde algún 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 según la información que van recolectando. Por eso decimos que habrá un dominio de colisión por cada BOCA del switch/bridge/router.

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

No, no está orientado a conexión.

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

**ARP (Address Resolution Protocol)**

Protocolo de L2, a veces considerado L3, “Helper” de IP que mapea Dir. Lógicas (IP) a Dir. Hardware (MAC). Trabaja conjuntamente con Ethernet (u otros protocolos de L2 multiacceso con broadcast: Token Ring,

FDDI, 802.11). Trabaja de forma dinámica, con auto-aprendizaje, sin configuración, aunque puede configurarse de forma estática.

Su finalidad es la resolución de direcciones IP en direcciones MAC y el mantenimiento de una caché de las asignaciones.

Para que una trama se coloque en los medios LAN debe contar con una dirección MAC destino. Para esto, el nodo 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.

Para que un dispositivo obtenga un par de direcciones:

1. Se emite una solicitud ARP, que se envía en 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.
2. El nodo receptor que es dueño de esa IP responde enviando un paquete de respuesta de ARP al emisor con una trama unicast.
3. Con esta respuesta se crea una entrada nueva en la tabla ARP.
4. Para cada dispositivo, un temporizador de cache ARP elimina las entradas ARP que no se hayan utilizado durante un período que varía dependiendo del dispositivo y SO. Esto es necesario debido a que, en caso de 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.

**Otra definición:**

ARP es un helper de IP que asocia direcciones de red a direcciones de enlace

Si un host A necesita hablarle a otro B, A no conoce la MAC de B (la tabla ARP no contiene esa entrada) pero sí su IP:

* A emite un ARP Request con: MAC origen (la de esa interfaz de A), MAC destino (la de broadcast), IP y MAC de A (origen) y IP de B y MAC en blanco (solicitada)
* B lo recibe, guarda en su tabla ARP la MAC e IP de A, y emite un ARP Reply con: MAC origen, la de esa interfaz de B, MAC destino, la de esa interfaz de A (mensaje unicast), IP y MAC de B (respuesta), IP y MAC de A (a quien le está respondiendo)
* A lo recibe, guarda en su tabla ARP la MAC e IP de B
* A le habla a B con los datos que necesitaba enviarle, éste responde, etc. De forma unicast

**7. Investigue los comandos arp e ip neigh. Inicie una topología con CORE, cree una máquina y utilice en ella**

**los comandos anteriores para:**

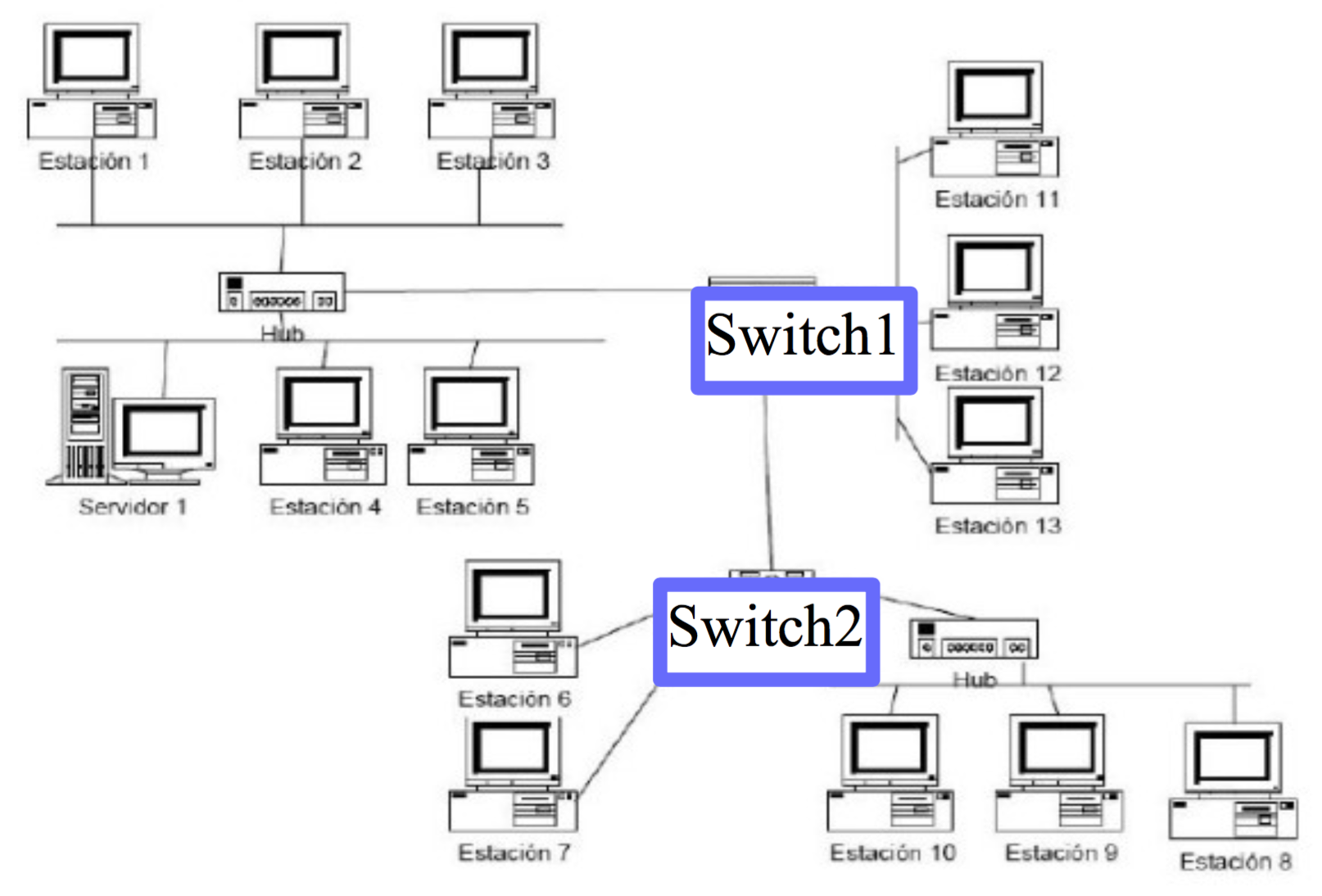
**Listar las entradas en la tabla ARP.**

**Borrar una entrada en la tabla de ARP.**

**Agregar una entrada estática en la tabla de ARP.**

**PUNTO NUEVO**

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



**a. Suponiendo que las tablas de los switches están llenas con la información correcta, responda quién**

**escucha el mensaje si:**

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

Estación 1 le manda al hub y este a 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.**

Estación 1 le manda al hub y este a 2, 3, 4, 5, servidor 1, y el switch 1 que reenvía a estación 11.

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

Estación 1 al hub y este reenvía a 2, 3, 4, 5, servidor 1 y switch 1. Este reenvía a switch 2 que reenvía al hub y este a 10, 8 y 9.

**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 el único dispositivo que separa dominios de broadcast.

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

La estación le manda al switch 2, y este a la estación 7. El switch 2 crea un canal directo entre las estaciones.

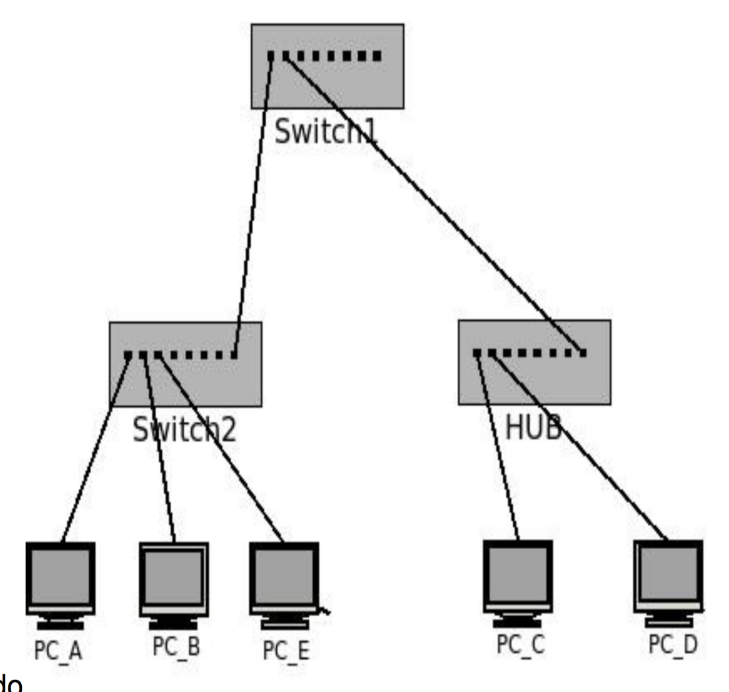
**vi. La estación 6 envía una trama a la estación 10.**

Estación 6 le manda a switch 2, que le manda al hub y este a las estaciones 8, 9 y 10

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

Se da cuando dos o más dispositivos, pertenecientes a un mismo dominio de colisión, emiten tramas (unicast o broadcast) al mismo tiempo. Por lo tanto, puede haber colisiones en todas aquellas que pasaron por un hub, ya que a diferencia del switch, este 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

**9. En la siguiente topología de red indique:**

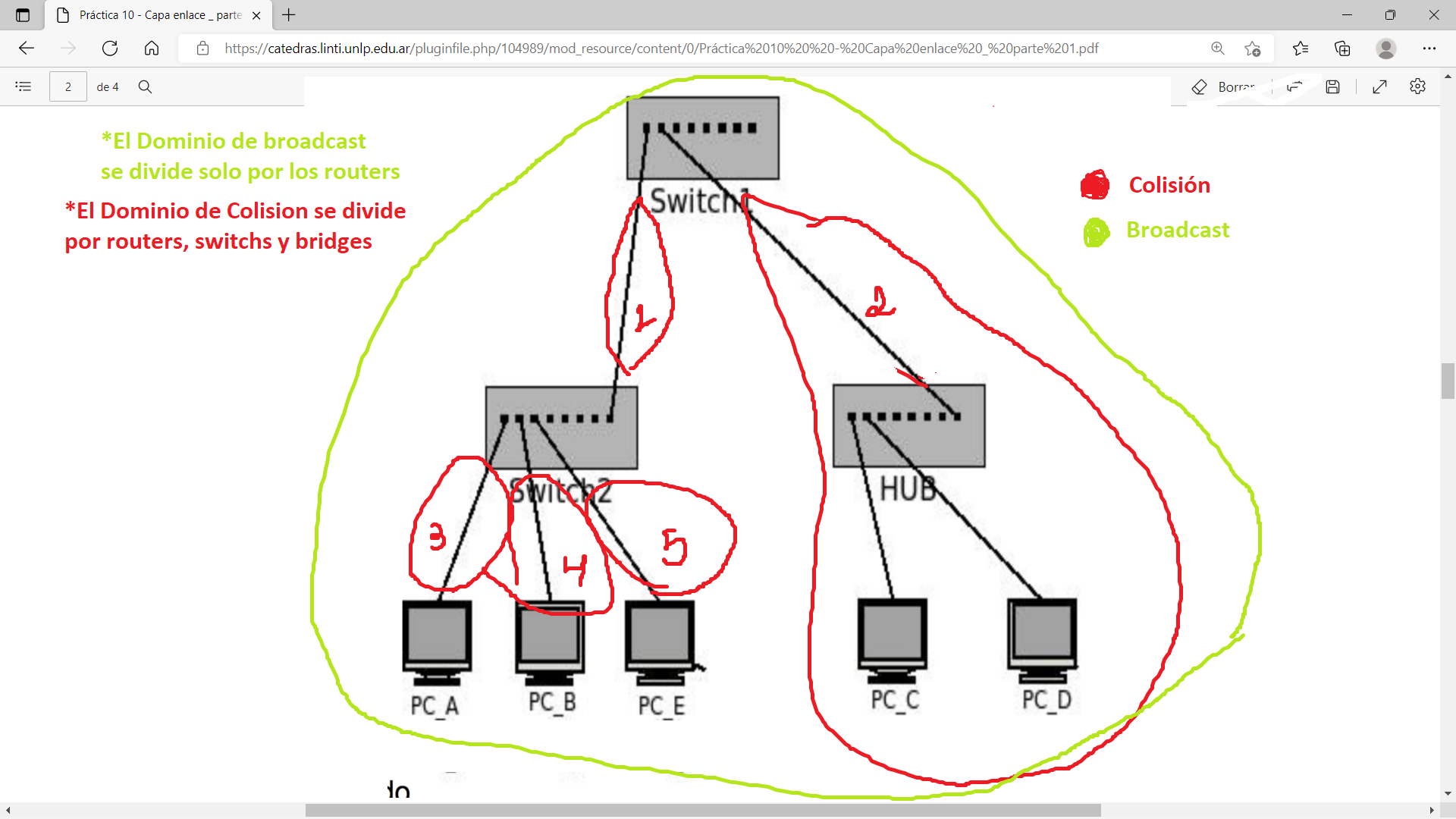


**a. ¿Cuántos dominios de colisión hay?**

5: {Switch1,Switch2}, {Switch2,PC\_A}, {Switch2,PC\_B}, {Switch2,PC\_E}, {Switch1,HUB,PC\_C,PC\_D}

**b. ¿Cuántos dominios de broadcast hay?**

Hay 1 sólo dominio de broadcast, toda la subred entera



**c. Indique cómo se va llenando la tabla de asociaciones MAC ->PORT de los switches SW1 y SW2**

**durante el siguiente caso:**

**i. A envía una solicitud ARP consultando la MAC de C.**

Envía el ARP Request de **PC\_A** a **PC\_C**, con dir. destino = broadcast (FF:FF:FF:...). En el transcurso del mensaje:

* Le llega el ARP Request a Switch 2, como no tiene la dir. MAC de **PC\_A** la guarda y la asocia con el puerto 1, al que está conectado **PC\_A**.
* Switch propaga el ARP Request a todos sus puertos **MENOS AL QUE LO ENVIO???**
* Les llega el ARP Request a PC\_B y PC\_E, estos desarman la trama y comparan la dir. IP destino con la suya. Como es diferente no responden.
* Le llega el ARP Request a Switch 1, como no tiene la dir. MAC de **PC\_A** la guarda y la asocia con el su puerto 1 y Switch 1 propaga el mensaje por sus puertos restantes, o sea el 2.
* Le llega el ARP Request a el HUB y este repite el mensaje por los puertos 1 y 2.
* Les llega el ARP Request a **PC\_C** y PC\_D, ambos comparan su propia IP con la que contiene la trama, en el caso de PC\_D no es la misma por lo que no hace nada, y en el caso de PC\_C es la misma IP, por lo que hace un ARP Replay (El mismo mensaje con Dir. MAC destino de PC\_A y Dir. MAC fuente de PC\_C, y sus respectivas IPs).

**Tablas CAM:**

|  |  |
| --- | --- |
| Switch 1 | |
| Dirección MAC | Puerto |
| PC\_A | 1 |

|  |  |
| --- | --- |
| Switch 22 | |
| Dirección MAC | Puerto |
| PC\_A | 1 |

**ii. C responde esta solicitud ARP.**

El camino es el mismo que el de ida, con la diferencia de que Switch 2 solo propaga el mensaje por el puerto 1 mientras que el HUB repite el mensaje por todos sus puertos.

El Switch 1 solo tiene 2 puertos, pero si tuviera más solo enviará el ARP Replay por el puerto 1, que es el que tiene asociado a la MAC de PC\_A. La Tabla se completa en el sentido contrario, y ahora conoce la MAC de PC\_C

|  |  |
| --- | --- |
| Switch 1 | |
| Dirección MAC | Puerto |
| PC\_A | 1 |
| PC\_C | 2 |

|  |  |
| --- | --- |
| Switch 2 | |
| Dirección MAC | Puerto |
| PC\_A | 1 |
| PC\_C | 8 |

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

Al momento de armar el ARP Request añade la dir. broadcast, porque en su tabla de ARP no tiene la dir. MAC de PC\_B. Envía el ARP Request de PC\_A a PC\_B, con dir. destino = broadcast(FF:FF:FF:...). En el transcurso del mensaje:

* Le llega el ARP Request a Switch 2.
* Switch propaga el ARP Request a todos sus puertos, menos por el que recibió el ARP Request.
* Les llega el ARP Request a PC\_B y PC\_E, estos desarman la trama y comparan la dir. IP destino con la suya. En el caso de PC\_E como la dir. IP que contiene la Trama no la misma que su IP no responde, pero para la PC\_B la IP si es la misma, por lo que arma un ARP Replay y lo envia.
* Le llega el ARP Request a Switch 1, que propaga el mensaje por sus puertos excepto el 1, que es por donde recibio el ARP Request.
* Le llega el ARP Request a el HUB y este repite el mensaje por los puertos 1 y 2.
* Les llega el ARP Request a PC\_C y PC\_D, ambos comparan su propia IP con la que contiene la trama, en ambos casos no es la misma por lo que no hacen nada.

No hay cambios en las tablas porque “A” ya estaba.

**iv. B responde esta solicitud ARP.**

El camino es el mismo que el de ida, con la diferencia de que Switch 2 solo propaga el mensaje por el puerto 1, y como ahora conoce la MAC de PC\_B actualiza su tabla MAC → Port.

Tabla de switch 1 sin cambios.

|  |  |
| --- | --- |
| Switch 2 | |
| Dirección MAC | Puerto |
| PC\_A | 1 |
| PC\_C | 8 |
| PC\_B | 2 |

**d. Si la PC E y la PC D hubiesen estado ejecutando un tcpdump (**Herramienta para analizar el trafico que circula por la red a la que la PC eta conectada) **para escuchar todo lo que pasa por su interfaz de red, ¿cuáles de los requerimientos/respuestas anteriores hubiesen escuchado cada una?**

PC\_E y PC\_D escuchan todos los todos los ARP Request.

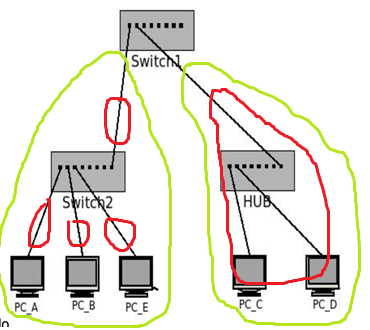
Además, PC\_D escucha el ARP Replay de PC\_C ya que ambos están conectados a un HUB.

Explicación: Esto se debe a la dir. de broadcast que se usa.

|  |  |  |
| --- | --- | --- |
| **Mensaje** | **PC\_E** | **PC\_D** |
| i) | Sí (es un mensaje broadcast) | Sí (es un mensaje broadcast) |
| ii) | No (el switch detecta la MAC unicast y sólo reenvía a ese puerto) | Sí (el hub siempre reenvía a todos los demás puertos) |
| iii) | Sí (es un mensaje broadcast) | Sí (es un mensaje broadcast) |
| iv) | No (el switch detecta la MAC unicast y sólo reenvía a ese puerto) | No (la PC está en otro dominio de colisión) |

*ESTE PUNTO NO EXISTE EN LA OTRA, PERO ESTA PIOLA(?*

**e. Si se reemplaza a switch1 por un router, ¿cuántos dominios de colisión y de broadcast quedarían?**

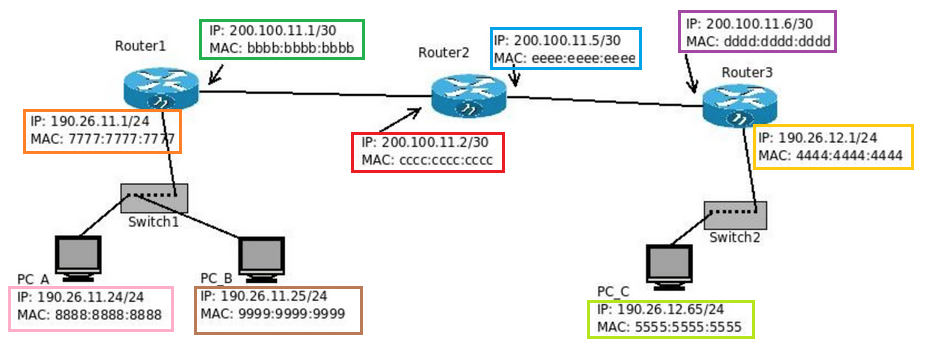
Dominios de colisión:

* {Router,Switch2}
* {Switch2,PC\_A}
* {Switch2,PC\_B}
* {Switch2,PC\_E}
* {Router,HUB,PC\_C,PC\_D}

Dominios de broadcast:

* {Router,Switch2,PC\_A,PC\_B,PC\_E}
* {Router,HUB,PC\_C,PC\_D}

**10. 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? ¿Con qué direcciones de origen y destino?**

Al estar todas las tablas vacías y al ser la consulta de una punta de la red a otra, entonces tenemos tráfico ARP por todos los dominios de broadcast. Ninguna de las PCs conoce la dir. MAC de las otras PCs, por lo que hace un ARP Request, lo que indica que ya hay trafico ARP.

* 1. La secuencia de ida es:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocolo** | **MAC origen** | **MAC destino** | **IPv4 origen** | **IPv4 destino** |
| ICMP | 8888:8888:8888 (pc a) | - | 190.26.11.24/24 (pc a) | 190.26.12.65/24 (pc c) |
| ARP de ida | 8888:8888:8888 (pc a) | 0000:0000:0000 | 190.26.11.24/24 (pc a) | 190.26.11.1/24 (router 1) |
| ARP de vuelta | 7777:7777:7777 (router 1) | 8888:8888:8888 (pc a) | 190.26.11.1/24 (router 1) | 190.26.11.24/24 (pc a) |
| ICMP | 8888:8888:8888 (pc a) | 7777:7777:7777 (router 1) | 190.26.11.24/24 (pc a) | 190.26.12.65/24 (pc c) |
| ARP de ida | BBBB:BBBB:BBBB (router 1 salida) | 0000:0000:0000 | 200.100.11.1/30 (router 1 salida) | 200.100.11.2/30 (router 2) |
| ARP de vuelta | CCCC:CCCC:CCCC (router 2) | BBBB:BBBB:BBBB (router 1 salida) | 200.100.11.2/30 (router 2) | 200.100.11.1/30 (router 1 salida) |
| ICMP | BBBB:BBBB:BBBB (router 1 salida) | CCCC:CCCC:CCCC (router 2) | 190.26.11.24/24 | 190.26.12.65/24 |
| ARP | EEEE:EEEE:EEEE | 0000:0000:0000 | 200.100.11.5/30 | 200.100.11.6/30 |
| ARP | dddd:dddd:dddd | EEEE:EEEE:EEEE | 200.100.11.6/30 | 200.100.11.5/30 |
| ICMP | EEEE:EEEE:EEEE | dddd:dddd:dddd | 190.26.11.24/24 | 190.26.12.65/24 |
| ARP | 4444:4444:4444 | 0000:0000:0000 | 190.26.12.1/24 | 190.26.12.65/24 |
| ARP | 5555:5555:5555 | 4444:4444:4444 | 190.26.12.65/24 | 190.26.12.1/24 |
| ICMP | 4444:4444:4444 | 5555:5555:5555 | 190.26.11.24/24 | 190.26.12.65/24 |

\*Este mensaje lo recibirá tanto Router1 como PC\_B

* 1. La secuencia de vuelta (asumiendo que las tablas ARP conservan sus entradas) es:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocolo** | **MAC origen** | **MAC destino** | **IPv4 origen** | **IPv4 destino** |
| ICMP | 5555:5555:5555 (pc c) | 4444:4444:4444 (Entrada de router 3) | 190.26.12.65/24 (pc c) | 190.26.11.24/24 (pc a) |
| ICMP | dddd:dddd:dddd (router 3) | EEEE:EEEE:EEEE (Entrada de router 2) | 190.26.12.65/24 (pc c) | 190.26.11.24/24 (pc a) |
| ICMP | CCCC:CCCC:CCCC (router 2) | BBBB:BBBB:BBBB (Entrada de router 1) | 190.26.12.65/24 (pc c) | 190.26.11.24/24 (pc a) |
| ICMP | 7777:7777:7777 (router 1) | 8888:8888:8888 (pc a) | 190.26.12.65/24 (pc c) | 190.26.11.24/24 (pc a) |

*CAM asocia MAC con puerto, ARP asocia MAC con IP*

*La dirección origen y destino son salto a salto*

*En la vuelta no hay tráfico ARP, porque el camino ya conoce las MACs para volver, ya tiene esas entradas en la tabla*

*Tráfico ICMP hay en todos los dominios de broadcast*

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

El ICMP se usa para el comando ping, asi que en todos

En el dominio de broadcast entre los Routers.

**• ¿Con qué direcciones de origen y destino de capa 2?**

Las dir. de origen y destino van a ser las MAC.

**• ¿Con qué direcciones de origen y destino de capa 3?**

Las dir. de origen y destino van a ser las dir. IP

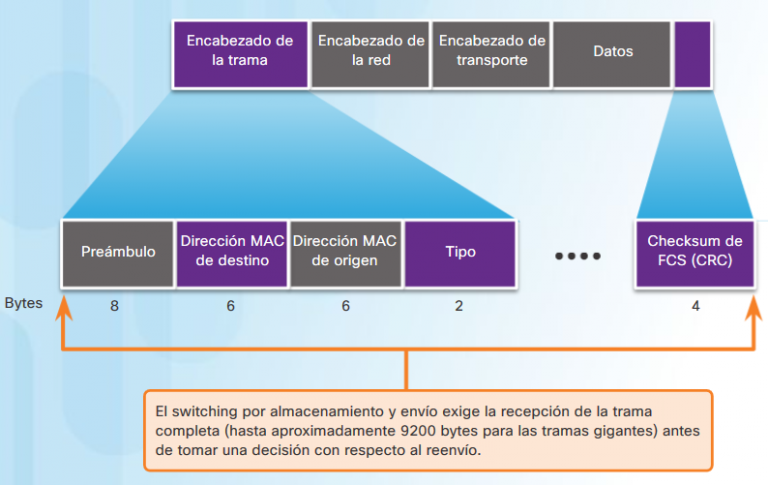
**¿Cuál es la secuencia correcta en la que se suceden los anteriores?**

La secuencia es la siguiente:

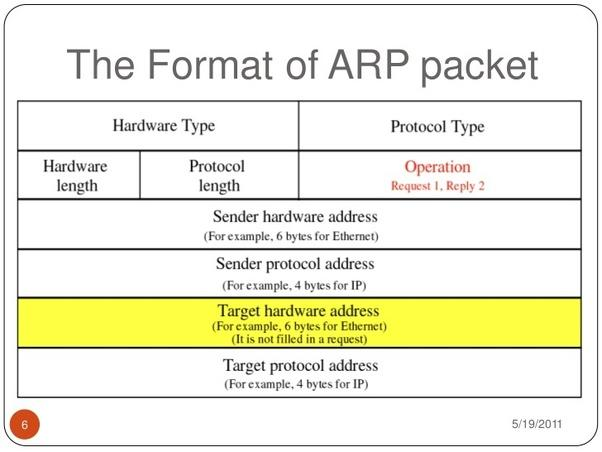
1- PC\_A hace un ping hacia la ip de PC\_C 190.26.12.65/24, para enviar el mensaje se arma la trama, mediante un proceso ANDing determina que la PC\_C está fuera de la LAN por lo que necesita la dirección MAC del default gateway, el Router 1 con interfaz 190.26.11.1/24, entonces:

2-Realiza un ARP request, que la enviará en una trama así:

-La dir. MAC es ffff:ffff:ffff, no confundir con la dir. MAC que va en el ARP Request que ahí es la 00:00:00:00:00:00 que quiere decir que no la conoce.



En la sección de datos va el ARP Request con este formato:



Los datos más importantes son el Sender hardware (dir. MAC fuente) Sender protocol (dir. IP fuente), Target Protocol (IP destino) y Target hardware (MAC destino), como no se sabe la MAC destino va la dir. 00:00:00:00:00:00

Sender🡪 Quien envía

Target 🡪 Quien recibe

3-El ARP Request llega al Switch y este lo repite hacia el router 1 y PC\_B, y guarda la dir. MAC de PC\_A en su tabla MAC → Port(aprendizaje automático)

4-PC\_B desarma la trama, compara su IP(190.26.11.25) como es diferente a la del Target protocol, descarta el mensaje.

5-El ARP Request llega al Router 1, guarda la MAC y la IP en su tabla ARP, el router desarma la trama, compara la IP y determina el ARP es para él y contesta con un ARP Response, que usa el mismo formato que ARP Request, solo cambia la operación de 1 a 2 y claro las fuentes por los destinos, la fuente es su propia MAC(7777:7777:7777)

6-Le llega el mensaje al Switch y lo repite, solo por el puerto de la MAC de PC\_A que había aprendido y guarda la MAC del router.

7-La PC\_A le llega el ARP Response, completa su tabla de ARP, asocia a la dir. IP a la MAC del router y comienza a enviar el ping. La tabla ARP, jamás tendrá una dir. MAC fuera de la red LAN, solo puede

tener dir. MAC de la misma LAN o del Router.

Este proceso se repite entre los nodos de las distintas redes hasta que llega a C y luego comienza el proceso otra vez hasta que le llegue la respuesta a PC A, posiblemente de manera más sencilla puesto que los dispositivos de las distintas LANs ya conocen las direcciones MAC de los otros dispositivos involucrados en la ruta. No vuelven a hacer ARP requests/replies.

DETALLE:

1- Como la PC A al aplicarle a la ip de la PC C su mascara de red se da cuenta que la PC C se encuentra en OTRA red, necesita comunicarse con la interfaz de salida del router al que esta conectado. Por eso, hace lo siguiente:

ARP (WHO-IS) PC\_A -> BROADCAST

Trama Ethernet: (mac origen: MAC\_PC\_A mac destino: BROADCAST )

Solicitud ARP: (mac origen: MAC\_PC\_A ip origen: IP\_PC\_A)

(mac destino: 00:00:00:00:00:00 ip destino: 190.26.11.1/24 →

IP\_DEFAULTGATEWAY )

2- ARP (REPLY) ROUTER1 -> PC\_A

Trama Ethernet: (mac origen: MAC\_ROUTER1 mac destino: MAC\_PC\_A)

Solicitud ARP: (mac origen: MAC\_ROUTER1 ip origen: IP\_ROUTER1)

(mac destino: MAC\_PC\_A ip destino: IP\_PC\_A)

3- ICMP (echo request) PC\_A -> PC\_C (ROUTER1)

Trama Ethernet: (mac origen: MAC\_PC\_A mac destino: MAC\_ROUTER1)

ICMP: (ip origen: IP\_PC\_A ip destino: IP\_PC\_C)

4- ARP (WHO-IS) ROUTER1 -> ROUTER2 (Default Gateway)

Trama Ethernet: (mac origen: MAC\_ROUTER1 mac destino: BROADCAST )

Solicitud ARP: (mac origen: MAC\_ROUTER1 ip origen: IP\_ROUTER1)

(mac destino: 00:00:00:00:00:00 ip destino: IP\_ROUTER2 )

5- ARP (REPLY) ROUTER2 -> ROUTER1

Trama Ethernet: (mac origen: MAC\_ROUTER2 mac destino: MAC\_ROUTER1)

Solicitud ARP: (mac origen: MAC\_ROUTER2 ip origen: IP\_ROUTER2)

(mac destino: MAC\_ROUTER1 ip destino: IP\_ROUTER1)

6- ICMP (echo request) PC\_A (ROUTER1) -> PC\_C (ROUTER2)

Trama Ethernet: (mac origen: MAC\_ROUTER1 mac destino: MAC\_ROUTER2)

ICMP: (ip origen: IP\_PC\_A ip destino: IP\_PC\_C) → se mantiene

7- ARP (WHO-IS) ROUTER2 -> ROUTER3 (Default Gateway)

Trama Ethernet: (mac origen: MAC\_ROUTER2 mac destino: BROADCAST )

Solicitud ARP: (mac origen: MAC\_ROUTER2 ip origen: IP\_ROUTER2)

(mac destino: 00:00:00:00:00:00 ip destino: IP\_ROUTER3 )

8- ARP (REPLY) ROUTER3 -> ROUTER2

Trama Ethernet: (mac origen: MAC\_ROUTER3 mac destino: MAC\_ROUTER2)

Solicitud ARP: (mac origen: MAC\_ROUTER3 ip origen: IP\_ROUTER3)

(mac destino: MAC\_ROUTER2 ip destino: IP\_ROUTER2)

9- ICMP (echo request) PC\_A (ROUTER2) -> PC\_C (ROUTER3)

Trama Ethernet: (mac origen: MAC\_ROUTER2 mac destino: MAC\_ROUTER3)

ICMP: (ip origen: IP\_PC\_A ip destino: IP\_PC\_C)

10- ARP (WHO-IS) ROUTER3 -> PC\_C

Trama Ethernet: (mac origen: MAC\_ROUTER3 mac destino: BROADCAST )

Solicitud ARP: (mac origen: MAC\_ROUTER3 ip origen: IP\_ROUTER3)

(mac destino: 00:00:00:00:00:00 ip destino: IP\_PC\_C )

11- ARP (REPLY) PC\_C -> ROUTER3

Trama Ethernet: (mac origen: MAC\_PC\_C mac destino: MAC\_ROUTER3)

Solicitud ARP: (mac origen: MAC\_PC\_C ip origen: IP\_PC\_C)

(mac destino: MAC\_ROUTER3 ip destino: IP\_ROUTER3)

12- ICMP (echo request) PC\_A (ROUTER3) -> PC\_C

Trama Ethernet: (mac origen: MAC\_ROUTER3 mac destino: MAC\_PC\_C)

ICMP: (ip origen: IP\_PC\_A ip destino: IP\_PC\_C)

**11. ¿Existe ARP en IPv6? ¿Por qué? ¿Quién cumple esa función?**

No existe ARP en IPv6, porque en IPv6 no hay broadcast (sólo soporta unicast, multicast y anycast) y ARP funciona con esto, por lo tanto, es reemplazado por NDP (Neighbor Discovery Protocol), que usa multicast, Neighbor Advertisement y Neighbor Solicitation para consultar por las dir. IPv6 y sus respectivas dir. MAC´s.

* Para que funcione los Switchs deben poder implementar IGMP.
* Envía sus mensajes a través de ICMPv6
* En vez de tener tablas de ARP, se tienen tablas de vecinos, con un temporizador por cada dir.
* Para ver la tabla de vecinos, se utiliza el comando: ip nei
* Neighbor Discovery (ND) es un protocolo de IPv6, y es equivalente al protocolo Address Resolution Protocol (ARP) en IPv4, aunque se distingue porque también incorpora funcionalidades de ICMP.

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

IEEE 802 es un conjunto de estándares del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que cubre las capas físicas y de enlace de datos del modelo de interconexión de sistemas abiertos (OSI).

La especificación IEEE para Ethernet es la 802.3 fue el primer intento para estandarizar Ethernet y define qué tipo de cableado se permite y cuáles son las características de la señal que transporta. La especificación 802.3 original utilizaba un cable coaxial grueso de 50 ohm, que permite transportar una señal de 10 Mbps a 500 m pero se amplió a, cable coaxial delgado, pares trenzados y fibra óptica.

Existen diferencias entre el Ethernet original y el Ethernet 802.3:

|  |  |
| --- | --- |
| **Ethernet original** | **Ethernet IEEE 802.3** |
| Preámbulo (8 bytes) | Preámbulo (7 bytes) |
| Delimitador de inicio de trama (1 byte) |
| MAC destino (6 bytes) | MAC destino (2 a 6 bytes) |
| MAC origen (6 bytes) | MAC origen (2 a 6 bytes) |
| Tipo de trama (2 bytes) | Longitud de trama (2 bytes) |
| Payload (0 a 1500 bytes) | |
| Padding (0 a N bytes) | |
| Código de verificación CRC (4 bytes) | |

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

**Ejercicio de parcial**

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

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

Se da cuenta por la tabla de ruteo de PC B, que tiene que salir por el default gateway

**Si la tabla ARP de la PC A esta vacía, ¿qué dirección MAC necesita la PC A para poder comunicarse**

**con la PC B?**

Necesita la MAC de la interfaz del router (default gateway) a la que está conectado

**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? De ser necesario, ejecute de nuevo el experimento**

**de ser necesario y complete los campos:**

Será la IP de la interfaz del router (default gateway) a la que está conectado

**Trama Ethernet:** (mac origen: *MAC de interfaz de PC A---* mac destino: *FF:FF:FF:FF:FF:FF*)

**Solicitud ARP:** (mac origen: *MAC de interfaz de PC A (Por la que se conecta al router*

ip origen: *IPv4 de interfaz de PC A*)

mac destino: *00:00:00:00:00:00*

ip destino: IP de interfaz del router por la que se conecta a PC\_A)

**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.**

* 1. d
     1. Trama Ethernet:
        1. MAC origen: MAC de interfaz del router, por la cual se conecta a PC B
        2. MAC destino: MAC de interfaz de PC B, por la cual se conecta al router
     2. ICMP Echo Request:
        1. IP origen: IPv4 de interfaz de PC A, por la cual se conecta al router
        2. IP destino: IPv4 de interfaz de PC B, por la cual se conecta al router (en otras palabras, la usada como destino al ejecutar el comando PING)