Redes y Comunicaciones 2017
Práctica 10

Autor: Fermín Minetto (http://www.github.com/ferminmine)

1) ¿Qué función cumple la capa de enlace? Indique que servicios presta esta capa. (Preguntar)

El objetivo de la capa de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a la conexión). Para lograr este objetivo tiene que montar bloques de información llamados tramas, dotarles de una dirección de capa de enlace llamadas direcciones MAC, gestionar la detección o corrección de errores, y ocuparse del "control de flujo" entre equipos.

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

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.

Similitudes:

- Ambos protocolos proveen un servicio de entrega fiable, aunque son parecidos, funcionan de manera distinta.
- Ambos protocolos encapsulan los datos que reciben de capas superiores en uno propio de la capa, en caso de transporte en segmentos, en caso de red en tramas.
- Ambos protocolos proporcionan servicios de control de flujo y de detección de errores.

3) Ethernet

El protocolo Ethernet es una familia de tecnologías de red LAN más utilizadas en la actualidad. Funciona en la capa de enlace y la capa física. También conocido como IEEE 802.3, esta norma define , además de dlas características eléctricas de longitud y diámetro de cables, todos los elementos en juego dentro de una red, es decir como debe estar conectado en cada escenario en partiular y muchos otros parámetros.

Basicamente, es el método más simple, seguro y económico de montar una red entre computadoras, debido fundamentalmente a su flexibilidad, ya que entre otras tantas características es posible utilizarse desde cable coaxial hasta fibra óptica.

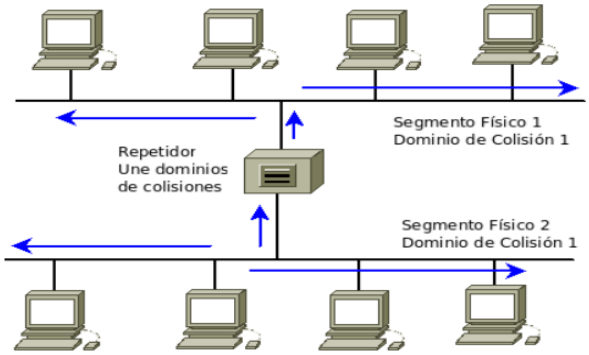
La idea básica detras de Ethernet es que todas las Pcs dentro de una red envíen y reciban datos de una forma en que se evite cualquier tipo de superposición. Los datos que se reciben o envían mediante este estándar se dividen en tramas. Estas tramas son enviadas a todos los dispositivos de la red, siendo tarea de estos dispositivos descartar tramas no dirigidas hacia ellos o aceptar las que si lo están. CSMA/CD es un protocolo empleado por las redes ethernet para evitar las colisiones, es decir, que los dispositivos no envíen al mismo tiempo tramas por la red.

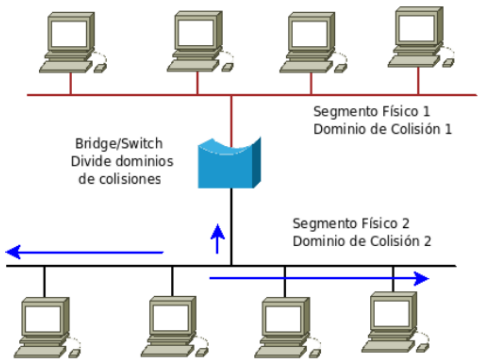
El direccionamiento en la capa de enlace se realiza mediante direcciones MAC (o direcciones LAN). Estas direcciones MAC son únicas en cada dispositivo y están compuestas por 48 bits.
La dirección de broadcast en la capa de enlace es la FF:FF:FF:FF:FF:FF.

4) Dispositivos de la capa de enlace: dominios de colisión y broadcast

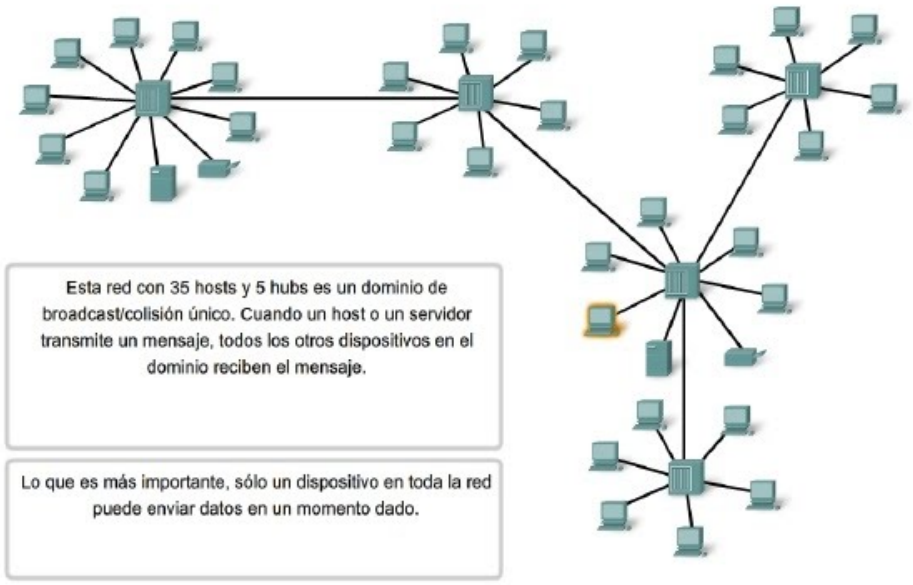
Los dominios de colisión es un segmento físico de una red donde es posible que las tramas puedan interferir unas con otras. Estas colisiones se dan particularmente en el protocolo de red Ethernet. A medida que aumenta el número de nodos que utilizan una red aumenta también las posibilidades que dos de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

Los dispositivos de la capa de enlace son los switches, los repetidores, los bridges y los routers.
Los *repetidores* son dispositivos electrónicos que conectan dos segmentos de una misma red, transfiriendo el tráfico de uno a otro extremo. *Los hubs son repetidores multipuerto.* **Consulta: ninguna PC conectada a HUB/REPETIDOR puede enviar a vez.**





La utilización de hubs en topologías en estrella extendidas puede crear grandes dominios de colisión



Los ***bridges*** son dispositivos que *separan* dominios de colisiones y debido a esto pueden utilizarse para separar la red en partes más pequeñas. Permiten escalabilidad y suelen tener dos puertos.
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. Los switches también guardan las direcciones MAC asociadas a cada puerto y pueden filtrar tramas a través de estas direcciones de MAC (y se evita el flooding).

El ***dominio de broadcast*** es el conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto. Los dominios de broadcast generalmente están delimitados por los *routers.* Si bien los switchs filtran la mayoría de las tramas según la direcciones MAC, no hacen lo mismo con las tramas de broadcast. Cuando un switch recibe una trama de broacast, la reenvía a cada uno de sus puertos excepto al puerto de origen por el que recibió la trama.

5) Algoritmo de acceso al medio Ethernet

Ethernet se divide en dos capas para funcionar: capa LLC y MAC. La subcapa LLC se podría definir como el controlador de la NIC y se implementa por software. La subcapa MAC tiene dos responsabilidades principales: *encapsular los datos y* ***el control de acceso al medio.*** El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el desarmado de la trama en el momento en que se la recibe. Acá se incluye el direccionamiento MAC.

El algoritmo de control de acceso al medio es el responsable de la ubicación y la remoción de tramas en los medios. Ethernet proporciona un método para controlar la forma en que los nodos comparten el acceso mediante el uso de una tecnología de acceso múltiple por detección de portadora (CSMA).
El proceso CSMA se utiliza para detectar si los medios transportan una señal. El CSMA se suele implementar con un método para resolver la contienda de los medios. Estos métodos son ***la detección de colisiones*** y ***la prevención de colisiones***.

En el método CSMA/CD todos los dispositivos de la red que tienen mensajes para enviar deben escuchar antes de transmitir. Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar

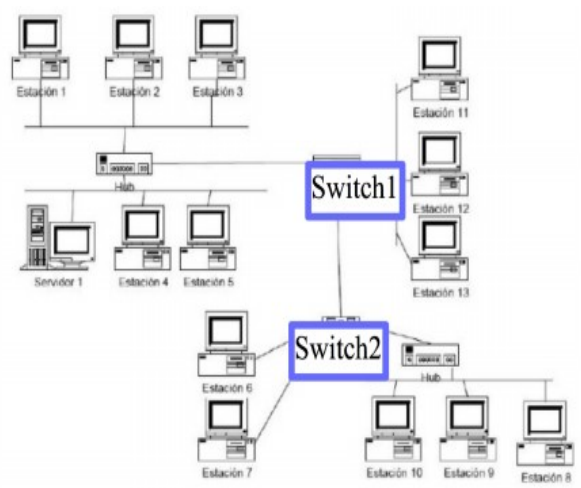
transmitir. Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN. Una vez que se envía el mensaje el dispositivo regresa a su modo de escucha predeterminado.
Puede darse el caso *que un segundo dispositivo no detecte las señales y comience también a transmitir.* Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren, se mezclen y se destruyan. La detección de una colisión es posible ya que los dispositivos *pueden detectar un aumento de la amplitud de la señal por encima del nivel normal.* Una vez detectada la colisión, todos los dispositivos transmisores *continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.*

Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión, lo cual inicia el algoritmo de postergación. Este algoritmo de postergación hace que *todos los dispositivos dejen de transmitir por un tiempo aleatorio* lo que permite que las señales de colisión disminuyan. Finalizado ese período los dispositios regresan al modo escuchar antes de transmitir.
El período aleatorio de postergación garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso.

6) Comando *arp* e *ip neigh*

- ***Listar entradas en tabla ARP:*** *arp -a -n*
- ***Borrar entrada de tabla 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)
- ***Agregar entrada estática a tabla ARP:*** *arp -d 10.0.0.2 (borra la entrada para el host con IP 10.0.0.2)*

7) Ejercicio práctico



Suponiendo que las tablas de los switches están llenas con la información correcta, responder quienes escuchan el mensaje:

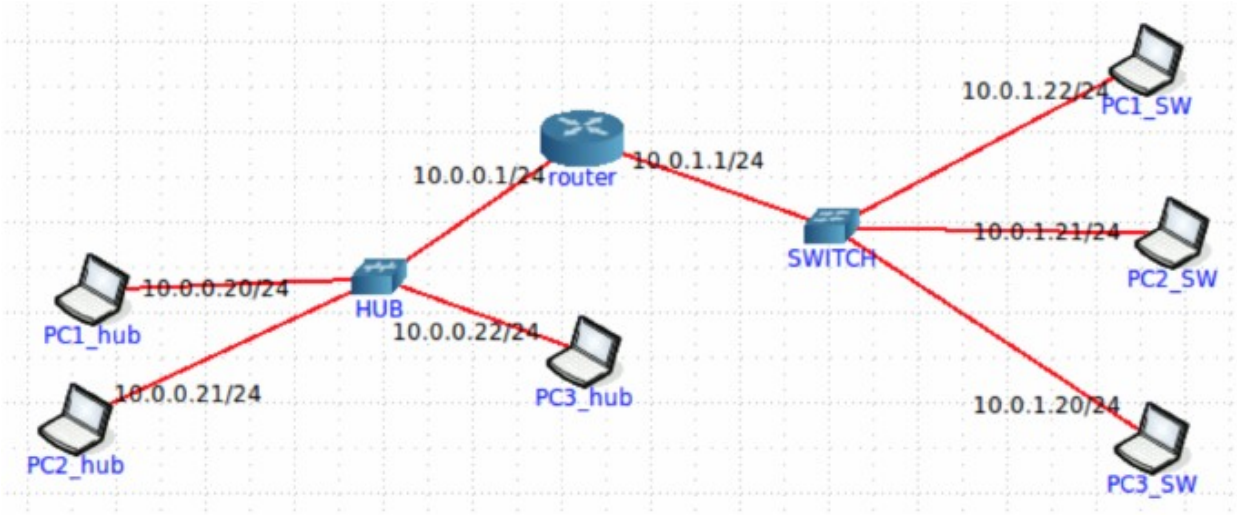
1. **La estación 1 envía una trama al servidor 1:** *Estación 2, 3, 4, 5 y servidor 1*
2. **La estación 1 envía una trama a la estación 11:** *E2,3,4,5 ; S1; E11*
3. **La estación 1 envía una trama a la estación 9: Chequear** *E2,3,4,5 ; S1; Switch 1; Switch 2; E10, E8, E9*
4. **La estación 4 envía una trama a la MAC de broadcast:** *Lo reciben todos los dispositivos*
5. **La estación 6 envía una trama a la estación 7:** *E7*

6. ***La estación 6 envía una trama a la estación 10: Chequear*** *Switch2, E10,9,8*

¿En que situacione se pueden producir colisiones?

- E1, 2, 3, 4, 5 y S1 envían una trama al mismo tiempo
- E11, 12 y 13 envían una trama al mismo tiempo
- E6 y 7 envían una trama al mismo tiempo
- E10, 9 y 8 envían una trama al mismo tiempo

8) Diferencias de HUB y SWITCH usando VM



Si se hace un ping desde PC2_hub a PC1_hub también se va a poder ver el paquete o datagrama ICMP desde PC3_hub con tcpdump puesto que el HUB retransmite la trama a todos los dispositivos conectados a él.

Si se hace un ping desde PC2_SW a PC1_SW no se va a poder ver el paquete o datagrama ICMP desde PC3_hub ya que el switch *tiene la capacidad para filtrar las tramas unicast por dirección MAC (si están en su tabla ARP).* En PC3_hub no se va a poder ver nada porque por empezar están en otra red LAN, y segundo, en el caso que estuviera conectada por el mismo switch se seguiría filtrando.

9) ¿Cuál es la finalidad del protocolo ARP?

La finalidad del protocolo ARP es la resolución de direcciones IPv4 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 IPv4 de destino, llamada *tabla ARP.* Cada entrada de la tabla cuenta con una dirección IPv4 a la que se le correspnde una dirección MAC.
Una manera en la que un dispositivo puede obtener un par de direcciones es emitir uan 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 nose 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.

10) Analizar ARP

La finalid