



Actividades capítulo 9

UNIVERSIDAD DEL CAUCA

FECHA:24/09/2023

NOMBRE: Daniel Santiago Muñoz Rodríguez

CODIGO: 104619011190



1. Leer el capítulo 9 del curso de Cisco.

Preguntas de lectura capítulo 9

1 Nombre las dos subcapas de Enlace de Datos y enumere sus fines.

Subcapa LLC: se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. Su fin es tomar los datos del protocolo de la red y agregar información de control para ayudar a entregar el paquete al nodo de destino.

Subcapa MAC: se encarga de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios. Su fin es establecer la comunicación con las capas superiores a través del LLC y se implementa en el software, generalmente como el controlador de la Tarjeta de interfaz de red.

2 Describa la estructura de una dirección MAC de Ethernet. ¿Por qué son necesarias?

La dirección MAC de Ethernet es una dirección única de 48 bits que se utiliza para identificar de manera exclusiva un dispositivo en una red Ethernet.

La estructura de una dirección MAC de Ethernet es la siguiente:

Los primeros 3 bytes bits corresponden al Identificador Único Organizacional.

Los últimos 3 bytes son asignados por el fabricante y se utilizan para identificar de manera única cada dispositivo dentro de la red.

Las direcciones MAC de Ethernet son necesarias porque permiten que los dispositivos se comuniquen entre sí en una red local.

3 Describir la función y las características del método de control de acceso a los medios utilizado por el protocolo Ethernet. Utiliza ejemplos para describir el proceso.

El método de control de acceso a los medios utilizado por el protocolo Ethernet es el Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD). Este método se utiliza para coordinar el acceso de múltiples dispositivos a un medio compartido, como un cable Ethernet.

Detección de portadora:

Cada dispositivo escucha el medio para detectar si hay actividad o señales de otros dispositivos antes de transmitir.

Multiacceso:

Si dos dispositivos, por ejemplo, "A" y "B", están demasiado distantes entre sí y no pueden escucharse mutuamente, ambos pueden comenzar a transmitir al mismo tiempo, sin darse cuenta de la actividad del otro debido a la latencia de la señal.

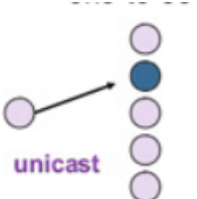

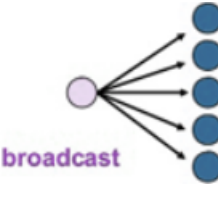
Detección de colisiones:

Durante la transmisión, si un dispositivo detecta un aumento en la amplitud de la señal por encima del nivel normal (lo que indica una colisión), detendrá su transmisión.

Señal de congestión y postergación aleatoria:

Cuando se detecta una colisión, los dispositivos que participaron en la colisión envían una señal de congestión para notificar a otros dispositivos sobre la colisión.

4 Describa como la Ethernet implementa: comunicaciones unicast, multicast y broadcast. Explicar, con ayuda de un dibujo o diagrama, en que consiste cada una de ellas.

Unicast	Multicast	Broadcast
un dispositivo envía un mensaje a un único dispositivo de destino específico. El mensaje se envía directamente al dispositivo de destino y solo ese dispositivo lo recibe	un dispositivo envía un mensaje a un grupo de dispositivos de destino específicos. El mensaje se envía a una dirección de grupo multicast y todos los dispositivos que pertenecen a ese grupo reciben el mensaje.	un dispositivo envía un mensaje a todos los dispositivos de la red. El mensaje se envía a una dirección de broadcast especial y todos los dispositivos en la red reciben el mensaje.
		

5 Explicar la en que consiste la temporización y sincronización en Ethernet.

La temporización y sincronización en Ethernet se refiere al proceso de coordinar la transmisión y recepción de datos entre los dispositivos en una red Ethernet. Esto es especialmente importante en el modo half-duplex, donde los datos solo pueden viajar en una dirección a la vez.

6 Los switches Ethernet reenvían selectivamente tramas individuales desde un puerto receptor hasta el puerto en el que esté conectado el nodo de destino. Explicar en qué consiste.

Los switches Ethernet implementan el reenvío selectivo, que consiste en analizar la dirección MAC de destino de una trama y reenviarla únicamente al puerto correspondiente. Este proceso permite establecer una conexión punto a punto momentánea entre los nodos de transmisión y recepción.

Cuando una trama llega a un switch, este analiza la dirección MAC de origen y busca en su tabla de direcciones MAC si ya tiene una entrada para esa dirección. Si no existe una entrada, el switch crea una nueva entrada en la tabla asociando la dirección MAC de origen con el puerto en el que llegó la trama. Finalmente el switch reenvía la trama al puerto correspondiente al nodo de destino.

7 Describa un dominio de colisiones Ethernet.

Un dominio de colisiones en Ethernet se refiere a un conjunto de dispositivos conectados a un mismo segmento de red en el que las colisiones pueden ocurrir si dos o más dispositivos transmiten datos al mismo tiempo. En un dominio de colisiones, los dispositivos comparten el mismo medio de transmisión y

compiten por el acceso a ese medio.

8 Los switches LAN Ethernet realizan cinco operaciones básicas, explique cada una de ellas

Aprendizaje: El aprendizaje en un switch Ethernet se refiere al proceso mediante el cual el switch registra las direcciones MAC de origen de las tramas que llegan a sus puertos.

Actualización: La actualización en un switch Ethernet se refiere al proceso de renovar el tiempo de vida de las entradas en la tabla de direcciones MAC.

Inundación: La inundación en un switch Ethernet se refiere al proceso de reenviar una trama a todos los puertos, excepto al puerto en el que llegó la trama.

Reenvío selectivo: El reenvío selectivo en un switch Ethernet se refiere al proceso de analizar la dirección MAC de destino de una trama y reenviarla únicamente al puerto correspondiente al dispositivo de destino.

Filtrado: El filtrado en un switch Ethernet se utiliza para evitar que ciertas tramas no deseadas o potencialmente peligrosas se propaguen en la red.

9 Comparar y contrastar los hubs y switches de Ethernet.

Switch	Hub
Un switch es un dispositivo de capa de enlace de datos que realiza funciones más avanzadas. Un switch analiza la dirección MAC de destino de una trama y la reenvía únicamente al puerto correspondiente al dispositivo de destino. Esto se logra mediante el aprendizaje de direcciones MAC y la creación de una tabla de direcciones. Al reenviar selectivamente las tramas, los switches evitan la congestión y mejoran el rendimiento de la red.	Un hub es un dispositivo de capa física que simplemente replica las señales que recibe y las envía a todos los demás puertos. Esto significa que todos los dispositivos conectados a un hub comparten el mismo ancho de banda y están en un dominio de colisión común.

10 El protocolo ARP ofrece dos funciones básicas, explique cada una de ellas.

Resolución de direcciones Ipv4 a direcciones MAC:

Cuando se envía un paquete a la capa de Enlace de datos para que se lo

encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de Enlace de datos que se mapea a la dirección Ipv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Mantenimiento de una caché de las asignaciones:

Esta tabla almacena las asociaciones entre direcciones IP y direcciones MAC de los dispositivos de la red. A medida que se realizan las resoluciones de direcciones, se actualiza la tabla ARP con las nuevas asociaciones.

11 Explicar en qué consiste la eliminación de mapeos de direcciones en ARP.

Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo

12 Explicar los principales problemas del broadcast ARP.

Sobrecarga en los medios:

En redes locales las solicitudes de ARP se transmiten como tramas de broadcast, lo que significa que todos los dispositivos en la red las reciben y procesan.

En situaciones normales, estos broadcasts no afectan significativamente el rendimiento de la red. Sin embargo, en momentos de gran actividad, como cuando muchos dispositivos se conectan simultáneamente, puede haber una disminución temporal del rendimiento.

Seguridad:

El ARP spoofing (suplantación ARP o envenenamiento ARP) es una técnica de ataque en la que un atacante emite solicitudes ARP falsas para introducir asociaciones de direcciones MAC incorrectas en la red.

Esto permite al atacante redirigir tráfico a destinos equivocados o interceptar datos en la red.