Capa de Enlace – Resumen

PDU ⇨ Trama

La función de la capa de enlace es mover un datagrama desde un nodo hasta otro adyacente a través de un único enlace de comunicaciones. Su función principal es proporcionar una interfaz entre la capa de red (capa 3) y el medio físico subyacente, como cables, fibra óptica o enlaces inalámbricos. En red LAN (es una red concentrada en un área geográfica concreta)

La capa de enlace facilita la comunicación directa entre dispositivos. Su protocolo define el formato de los paquetes intercambiados entre nodos en un enlace y las acciones realizadas al enviar y recibir estos paquetes. A diferencia de la capa de red, que se encarga de mover segmentos desde el host de origen hasta el destino, el protocolo de la capa de enlace se ocupa de transferir datagramas de nodo a nodo a lo largo de un único enlace en 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 de la ruta, y 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 que presta:

1. Entramado (framing):
    - Encapsulado del datagrama en la trama, agregando encabezado (header) y cola (trailer).
2. Acceso al enlace:
    - Acceso al canal si es un medio compartido.
    - Direcciones “MAC” utilizadas en los encabezados de las tramas para identificar el origen y el destino.
3. Entrega confiable:
    - Entre nodos adyacentes.
    - Rara vez utilizados en enlaces de pocos errores (fibra óptica).
4. Control de flujo:
    - Acuerdo entre nodos emisor y receptor (adyacentes).
5. Detección de errores
    - Errores causados por atenuación de señal.
    - El receptor detecta presencia de errores.
6. Corrección de errores.
7. Half-duplex y Full-duplex:

Los servicios de detección y corrección de errores y control de flujo también son ofrecidos también por la capa de transporte. La diferencia entre ambos recae en que la capa de enlace se enfoca en aspectos locales del enlace, mientras que la capa de transporte aborda la transferencia extrema a extremo a través de redes más amplias. Además transporte proporciona una fiabilidad y garantías que enlace no.

La mínima MTU es 64B y la máxima es 1518B.

MAC

Están grabadas en la ROM de la NIC, en algunos casos es configurable por software.

La función que tiene es para que se pueda llevar la trama de una interfaz a otra interfaz físicamente conectada.

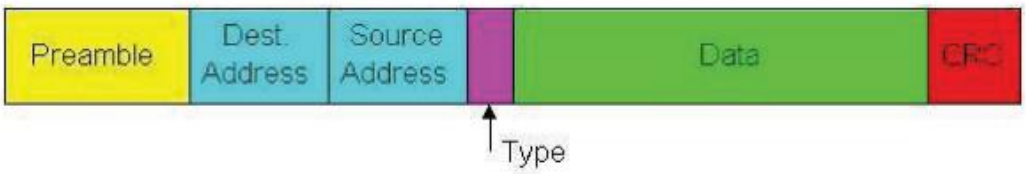
Las direcciones MAC también se conocen como direcciones de capa de enlace. Son direcciones físicas de 48 bits (6 bytes) y se expresan en hexadecimal. Los primeros 24 bits (3 bytes) identifican al fabricante de la tarjeta (OUI) y los siguientes 24 bits son únicos para interfaz de red.

Ethernet

Tecnología LAN cableada dominante. La topología en bus fue popular hasta mediado de los 90s. En este caso todos los nodos estaban en el mismo dominio de colisión con cualquiera de los otros nodos.

Hoy en día prevalece la topología estrella en donde hay un switch activo en el centro. En este caso los nodos no pueden colisionar con los otros.

Estructura de la trama Ethernet



El adaptador del emisor encapsula el datagrama IP (u otro de otro protocolo)

Preamble

- Relacionado con la capa física no lo veremos.

Direcciones

- 6 bytes cada una (dirección MAC destino y dirección MAC origen)
- Si el adaptador recibe una trama con dirección destino suya o dirección broadcast pasa los datos en la trama al protocolo de capa de red. Si no, se descarta la trama

Type:

- 2 bytes
- Multiplexación
- Indica el protocolo de la capa superior.

Data:

- De 46 a 1500 bytes

CRC:

- 4 bytes
- Chequeado en el receptor.
- Si hay un error se descarta la trama
- Para calcularlo se usa todo menos el Preamble

Ethernet es no orientado a la conexión y no es confiable. El protocolo MAC de Ethernet es CSMA/CD y la detección de colisiones es un servicio de la Capa Física.

Hay varios estándares Ethernet con protocolo MAC y formato de trama único, cada uno con diferentes velocidades y diferentes medios físico (cable, fibra óptica)

802.3

IEEE 802.3 fue el primer intento para estandarizar redes basadas en ethernet, incluyendo las especificaciones del medio físico subyacente. La IEEE 802.3 es un estándar desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que especifica las características técnicas y de funcionamiento para las redes de área local (LAN) que utilizan tecnologías de acceso al medio basadas en la transmisión de tramas.

Aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits Ethernet), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

La especificación IEEE para Ethernet es la 802.3, que define que 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. Más tarde se añadió la posibilidad de utilizar otros tipos de cables: Coaxial delgado; pares de cables trenzados, y fibra óptica.

Colisión

- Si un nodo recibe dos o mas señales al mismo tiempo
- Simultaneidad en el tiempo y en la frecuencia de dos o mas tramas en el mismo medio físico.
- Básicamente dos envían al mismo tiempo sobre el mismo medio físico causando una interferencia y resultando en la pérdida de datos.

Half-duplex y Full-duplex

Con Half-duplex los nodos en los extremos del enlace pueden trasmitir, pero no recibir al mismo tiempo. Con Full-duplex si

Dominio de Colisión

- Hasta donde pueden extenderse las colisiones.
- Hasta dónde llega la señal de una trama unicast.
- Todas las estaciones en el mismo dominio de colisiones ven los datos transmitidos de cada una.
- Un repetidor o un HUB extienden un dominio de colisión.
- Dividido por switch, router o bridge.

Dominio de Broadcast

- Una porción de la red donde un mensaje broadcast puede ser recibido por todos los nodos.
- Son separados por un router.
- Es la cantidad de subredes
- En la capa de enlace FF:FF:FF:FF:FF:FF es la dirección Broadcast. La función principal de la dirección de broadcast es enviar información a todos los dispositivos en la red sin la necesidad de conocer sus direcciones MAC individuales.
- Dividido por router.

Repetidor/HUB

Repetidor: amplificador digital, dos puertos. Regenera la señal une dominios de colisión generando un único, permite extensión.

HUB: repetidor multipuerto. Simplemente repite las señales a todos los puertos. No divide dominios de colisión ni de broadcast.

- 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 (basura para limpiar el medio)

Son Half-duplex

Bridge/Switch

Bridge: conecta dos segmentos de red, examina las direcciones MAC y aprende las ubicaciones de las direcciones MAC en ambos lados. Puede dividir dominios de colisión, no divide dominios de broadcast (es como el switch solo que tiene menos puertos). Tiene el poder adaptar entre dos protocolos de nivel de enlace o físico, pueden ser diferentes. Divide la red en partes más pequeñas: dominios de colisiones. Permitir escalabilidad. Esta implementado por software y tiene dos puertos en general.

Switch: un bridge multipuerto que trabaja con la misma tecnología de enlace y física en c/u. Trabaja en hardware y con múltiples puertos. Examina las direcciones MAC para enviar tramas solo al puerto específico donde se encuentra el destinatario.

Son full-duplex

Se codifican mediante un conector a la computadora (es serial) que es USB a DB-9 *(obviamente la computadora debe tener driver)*

El Swtich envía siempre un STP mensaje para ver si hay alguien.

Razones para usar Switching

- Dividir la red en partes más pequeñas (dominios de colisiones, microsegmentación).
- 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 del switch

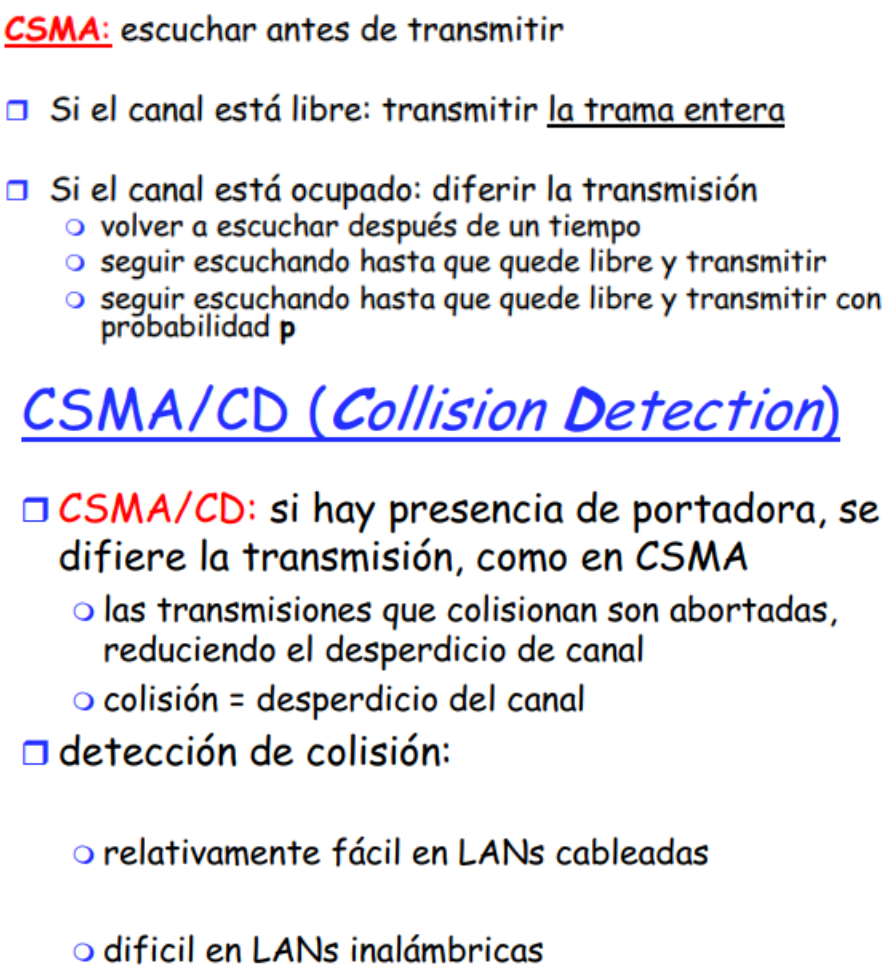
- Aprender direcciones MAC: El dispositivo guarda las direcciones MAC asociadas a cada puerto en una base de datos (tabla CAM). Se aprende cuando se envía (no cuando se recibe puesto que si no la tiene en la tabla CAM lo envía por broadcast).
  Las tramas de broadcast y multicast normalmente inundan todos los puertos excepto el puerto de origen. El switch nunca aprende direcciones de este tipo, dado que nunca aparecen como direcciones de origen de una trama
- 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 una instancia de STP, switches podrían correr varias.

Métodos de Conmutación

- Store and Forward (Almacena y Envía):
  - Lee toda la trama y chequea CRC.
  - Mas seguro.
- Fragment Free (Libre de Fragmentos):
  - Lee los primeros 64 bytes.
- Cut-through (de corte):
  - Lee hasta la dirección destino.
  - Más rápido.

CSMA/CD

- Carrier Sense:
  Antes de transmitir, una estación de trabajo escucha el medio para verificar si está ocupado o no. Si el medio está ocupado, espera hasta que esté libre.
- Multiple Access:
  Si el medio está libre, la estación de trabajo transmite sus datos. Sin embargo, debido a que varias estaciones pueden intentar transmitir al mismo tiempo, existe la posibilidad de colisiones.
- Collision Detection:
  Mientras se transmite, la estación de trabajo sigue escuchando el medio para detectar colisiones. Si detecta una colisión (dos estaciones transmitiendo al mismo tiempo), ambas estaciones interrumpen la transmisión y esperan un período de tiempo aleatorio antes de intentar transmitir nuevamente.
- Backoff y Retransmisión:
  Después de una colisión, las estaciones afectadas esperan un tiempo aleatorio antes de volver a intentar transmitir. Este proceso se conoce como "backoff". La esperanza es que las estaciones que colisionaron inicialmente seleccionen tiempos de espera diferentes, reduciendo la probabilidad de una nueva colisión. En un principio se espera entre 0 y 1, si hay colisión de nuevo, se va agrandando el rango de espera.



ARP

Mapea direcciones Lógicas (IP) a direcciones Hardware (MAC). Es un protocolo “Helper” de IP. Trabaja conjuntamente con Ethernet. Trabaja de forma dinámica, autoaprendizaje, sin configuración aunque puede configurarse de forma estática. Las tablas ARP residen solamente en los routers y en las PCs.

¿Cómo funciona?

Cuando se va a realizar por ejemplo un ping (mensaje ICMP), el emisor construye un paquete IP que se debe encapsular en una trama Ethernet. Como no se sabe la dirección MAC del destinatario esto se debe resolver para completar la trama. Para ello se recurre a un ARP Request que, como no sabe la MAC, debe ser broadcast L2. En este request se pregunta básicamente “¿Quién es xxx.xxx.xxx.xxx (dirección IP)?”. El que efectivamente tiene esa dirección IP responderá con un ARP Reply indicando “Yo soy xx:xx:xx:xx:xx:xx” de forma unicast. Allí es cuando el emisor terminar de construir la trama Ethernet que enviará de forma unicast. El receptor luego la recibirá y lo responderá.

Si se quiere comunicar con otras redes se utiliza la MAC del Default GW. Esto se debe a que la trama se construye y destruye en las diferentes redes. Se pierde la MAC Origen (la de la PC) puesto que esta solo tiene sentido en mi red directamente conectada.

RARP

Protocolo de L2, utilizado para mapear direcciones físicas (MAC) a direcciones Lógicas (IP). Utilizados en redes multiacceso como Ethernet. Utilizado por estaciones sin disco para obtener su dirección IP. Hoy es un protocolo en desuso, superado por BOOTP/DHCP.

Neighbor Discovery Protocol

Cumple funciones muy similares a ARP, solamente que en este caso esta encapsulada en IPv6. Los puntos importantes a tener en cuenta es que no se utiliza broadcast, si no que se utiliza multicast. NDP también presta una funcionalidad muy similar a DHCP de autoconfiguración.

NDP incluye los siguientes componentes principales:

1. Neighbor Solicitation: Similar a la solicitud ARP en IPv4, se utiliza para descubrir la dirección MAC asociada a una dirección IPv6 específica.
2. Neighbor Advertisement: Similar a la respuesta ARP en IPv4, se utiliza para informar a otros nodos sobre la dirección MAC asociada a una dirección IPv6.
3. Router Advertisement: Anuncia la presencia de routers en la red y proporciona información necesaria para la autoconfiguración de direcciones.

WLAN (LAN inalámbrica)

802.11

IEEE 802.11 es un conjunto de estándares que rigen los métodos de transmisión en redes inalámbricas. 802.11n es la forma más apropiada de llamar a la tecnología Wi-Fi

Las direcciones MAC, tanto en las tramas 802.11 como en las tramas Ethernet, se utilizan para identificar de manera única los dispositivos de red en una red local2.

En una trama Ethernet, solo se necesitan dos direcciones MAC: la dirección MAC de origen y la dirección MAC de destino.

En una trama 802.11, debido a la naturaleza de las redes inalámbricas, se pueden usar hasta cuatro direcciones MAC:

- Dirección 1: Indica el receptor que puede ser AP (Punto de Acceso) o PC dependiendo del salto.
- Dirección 2: Indica el emisor que puede ser AP o PC dependiendo el salto.
- Dirección 3: Si el mensaje va de PC a AP, indica la PC receptora. Si el mensaje va de AP a PC indica la PC emisora. Si el mensaje va de AP a AP indica la PC receptora.
- Dirección 4: Solamente está presente si el intercambio es entre APs. En este caso indica cual es la dirección MAC de la PC que origino el mensaje.

Estándar	Año	Frecuencia	Velocidad máxima
802.11a	1999	5GHz	54Mbps
802.11ac	2013-2014	5GHz	1.3Gbps
802.11b	1999	2,4GHz	11Mbps
802.11g	2003	2,4GHz	54Mbps
802.11n	2009	2,4GHz - 5GHz	600Mbps

Continuara…