

Resumen modulo q "Resolución de dirección"



q.1 MAC e IP

● Destino en la misma red → Hay 2 direcciones primarias asignadas a un dispositivo en una LAN Ethernet: **Dirección física (MAC)** → Se utiliza para comunicaciones NIC a NIC en la misma red Ethernet. **Dirección lógica (IP)** → Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino.

Las direcciones MAC se utilizan para entregar la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra NIC que está en la misma red. La trama Ethernet contiene una dirección MAC destino y una de origen en la capa 2. Y un paquete IP de capa 3 contiene IPv4 de origen y IPv4 destino.

● Destino en una red remota → Cuando la IP destino está en una red remota, la dirección MAC de destino será la dirección de gateway predeterminada del host. Cuando se desea enviar un paquete a una PC de una red remota, la MAC destino es la del gateway en el router. Los routers **examinan** la dirección IPv4 de destino para determinar la mejor ruta. Cuando recibe una trama desencapsula la información de capa 2. Por la IP destino, determina el siguiente salto y desencapsula el paquete IP en una nueva trama de enlace de datos para la salida. Por último encapsula la nueva información de dirección de capa 2. En IPv4 **ARP** y en IPv6 **ICMPv6** se utilizan para asociar las IP de los paquetes en un flujo de datos con las direcciones MAC en cada enlace.

q.2 ARP

● Descripción general → Cuando un dispositivo envía una trama de capa 2 contiene: **MAC destino** → La MAC del dispositivo de destino en el mismo segmento de red local. Gateway predeterminado en router si es la red es remota. **MAC origen** → MAC de origen. Un dispositivo utiliza el **Protocolo de resolución de direcciones (ARP)** para determinar la MAC de destino de un dispositivo local cuando conoce su dirección IPv4. **ARP Funciona:** - Resolución de direcciones IPv4 a direcciones MAC. - Mantener una tabla de asignaciones de direcciones IPv4 a MAC.

● **Funciones del ARP** → Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama, el dispositivo consulta una tabla ubicada en la RAM y se denomina tabla **ARP**. Si la dirección IPv4 destino del paquete está en la misma red que el de origen el dispositivo lo busca en la tabla ARP. Si no, lo busca en el gateway. ARP contiene temporalmente (en caché) la asignación para los dispositivos de la LAN. Permitiendo saber la MAC mediante la IPv4. Si el dispositivo localiza la IPv4, se utiliza la MAC como MAC destino. Si no el dispositivo envía una solicitud de ARP.

● Video - Solicitud de ARP → Se envía una solicitud ARP cuando un dispositivo no necesita determinar la MAC con esa IPv4 y no tiene una entrada en su tabla ARP. La solicitud ARP se encapsula en una trama con el encabezado; **MAC destino** → Dirección broadcast que requiere que todas las NIC de la LAN acepten y procesen la solicitud ARP.

MAC origen → Dirección MAC del remitente de la solicitud ARP. **Tipo** → Los mensajes ARP tienen un campo de tipo 0x806. Informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP. Como son de broadcast el switch las envía por todos los puertos. Todos los dispositivos deben procesar la solicitud ARP para ver si la IPv4 objetivo coincide con la suya. Un router no reenvía broadcast por otras interfaces.

● Video - Funcionamiento de ARP - Respuesta de ARP → La respuesta ARP se encapsula en una trama con un encabezado, contiene MAC destino, MAC de origen y tipo. Solamente el dispositivo que envió inicialmente la solicitud recibe la respuesta ARP de unicast. Cuando la recibe el dispositivo agrega la IP y MAC en su tabla ARP para enviar el paquete y crear la trama. **Si ningún dispositivo** responde a la solicitud el paquete se **descarta** porque no se puede crear una trama. Las entradas de la tabla ARP tienen marcas de tiempo. Si un dispositivo no recibe una trama antes que caduque el tiempo la trama se **elimina** de la tabla ARP. Las entradas **estáticas no caducan con el tiempo** y se eliminan de forma manual.

● Video - Rol ARP en comunicaciones remotas → La dirección IPv4 del gateway se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara las IP para ver si están en la misma capa 3. Si no está, el origen busca en la tabla ARP una entrada que contenga la IPv4 del gateway. Si no existe una entrada, utiliza el proceso ARP para determinar la MAC del gateway.

● Eliminación de entradas de una tabla ARP → Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas ARP que no se han utilizado durante un período. Los tiempos varían según el S.O. Windows es de 15 a 45 segundos. Los comandos también la eliminan manualmente.

● Tablas ARP en dispositivos de red → En un router se utilizan **show ip arp** para mostrar la tabla ARP. En un host windows 10 el **arp -a** para mostrarla.

● Problemas de ARP - Difusión ARP y Suplantación ARP → Todos los dispositivos de la red local reciben y procesan una solicitud ARP ya que es difusión. Hay problemas cuando se enciendan un gran número de dispositivos que acceden a los servicios al mismo tiempo, influye en el rendimiento.

En algunos casos, el uso de ARP puede coincidir en un riesgo potencial de seguridad. Un atacante puede usar la su plantación para realizar un ataque de envenenamiento ARP. El atacante envía una respuesta de ARP con su propia MAC. El emisor recibe la respuesta ARP y la registra en su tabla ARP y envía los paquetes al atacante. Los switches incluyen técnicas de mitigación conocidas como "Inspección dinámica de ARP" (DAI).

9.3 Detección de vecinos IPv6

● Video - Detección de vecinos IPv6 → Si la red para comunicarse usa IPv6, el protocolo de detección de vecinos ND es lo que se necesita para coincidir las IPv6 con las MAC. IPv6 también cuenta con el comando para encontrar las dirección MAC con una tabla similar a ARP. Solo se usan 4 hexetos por protección. Al igual que IPv4 se envía un paquete de difusión al switch para que salte los puertos y todos reciben la dirección y la comparan con la suya para enviar la respuesta. Si la computadora compara y no es su dirección la ignora sin tener que pasarlo a un proceso de nivel superior dando ventaja sobre ARP. También un router lo ignora porque la IPv6 detecta esto y no permite que la reenvíe fuera del área local.

● Mensajes de descubrimiento de vecinos IPv6 → Se conoce al protocolo como ND o NDP. ND proporciona servicios de resoluciones de direcciones, detección de routers y redirección para IPv6 mediante ICMPv6. Utiliza 5 mensajes: **NS** → Mensajes de solicitud de vecinos. **NA** → Mensaje de anuncio de vecino. **RS** → Mensaje de solicitud del router. **RA** → Mensaje de anuncio del router. Mensaje de * redirección

NS y **NA** se utilizan para mensajería de dispositivo a dispositivo, como la resolución de direcciones. Y **RS**, **RA** son para mensajes entre dispositivos y routers. La detección de routers se utiliza para la asignación dinámica de direcciones y sin estado (**SLAAC**). El quinto mensaje **ICMPv6 ND** es un mensaje de redirección que se utiliza para selección de salto.

● Descubrimiento de vecinos IPv6 : resolución de direcciones → Las direcciones IPv6 utilizan IPv6 ND para determinar la MAC de un dispositivo que tiene un IPv6 conocida. Los mensajes ICMPv6 solicitud de vecino y anuncio de vecino se utilizan para la resolución de la dirección MAC. Similar a solicitud y respuesta ARP. Se envían utilizando direcciones multi-broadcast Ethernet e IPv6 especiales. Esto permite que la NIC determine si el mensaje es para sí mismo sin tener que enviarlo al s.o. para su procesamiento.