Practica/Laboratorio de Capa de Enlace

1. Genere la topología de la figura 1, asigne las direcciones IP y arme el ruteo para que todos sean “visibles” por IP.

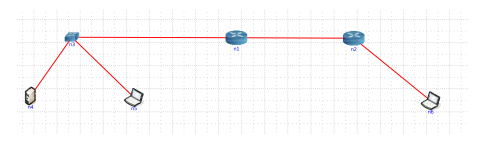


Figura 1: topología

a) Ejecute un ping (echo request) de n5 a n6 y capture el tráfico. Muestre encabezados Ethernet, y de los contenidos indique tipo de paquete, IP origen, IP destino cuando corresponda. Analice la diferencia entre las tramas IP y los mensajes ARP.

Al ejecutar el echo resquest, podemos notar que el encabezado de la trama ethernet para los paquetes de tipo ARP son:

* Mac destino: mac\_pcDestino o broadcast
* Mac origen: mac\_pcOrigen
* Tipo: ARP (0x0806)

Ademas tenemos los mensajes de ICMP request y reply con los encabezados de trama ethernet: (que se modifica el campo tipo)

* Mac destino: mac\_pcDestino o broadcast
* Mac origen: mac\_pcOrigen
* Tipo: IP (0x0800)

Por otro lado, los encabezados de los mensajes ARP son:

* Hardware type: Especifica el hardware por el cual se transmitió el mensaje arp (para ethernet valor 1).
* Protocol type: A cada protocolo se le asigna un valor (ARP=0x0806).
* Hardware adderss length: longuitud de la direccion fisica (normalmente con valor 6).
* Protocol adderss length: longuitud de direccion de protocolo (para IPv4 valor 4).
* Opcode: Mensaje arp enviado (valor 1 para resquest, 2 para reply).
* Source mac: Direccion MAC del remitente.
* Source ip: Direccion IP del remitente.
* Destination mac: Direccion MAC del destino.
* Destination ip: Direccion IP del destino.

*\* Los encabezados de trama IP fueron explicados con detalles en el trabajo anteriormente entegado.*

Entonces, la diferencia entre la trama IP y los mensajes ARP, es que en la trama IP, tiene como campos principales ipOrigen e ipDestino que son de capa de red (tambien podemos tomar como campos importantes el protocolo, checksum y ttl). En cambio los mensajes ARP los campos principales son la direccion MAC origen y destino (pertenecientes a la capa de enlace) sumados a la direccion IP destino y origen.

b) Con la captura anterior analice los mensajes ARP involucrados en el ruteo

Los hosts en una red LAN se identifican a nivel de enlace por la dirección MAC. Por este motivo es sumamente importante que no convivan dos direcciones mac iguales en la misma red, ya que, atraería demasiados problemas a la hora que el router o el switch intenten entregar una trama. Es una dirección de 48 bits expresada en pares de valores en hexadecimal (ej: 08:00:27:fd:3c:8e).

Toda trama ethernet tiene una mac origen y una mac destino. Puede que el que emisor no tenga en su tabla de arp la mac correspondiente a la ip destino, cuando esto sucede entra en juego el protocolo de resolución de direcciones ARP, cuyo objetivo es el encontrar la dirección mac que corresponde a una determinada dirección IP. Para lograrlo envía un paquete arp (arp request) por la dirección de broadcast que contiene la dirección ip por la que se pregunta y se espera una respuesta un arp reply (unicast ) con la dirección mac que le corresponde.

Analizando el tráfico de la captura anterior, podemos concluir que, el host de origen (n5) compara (AND) su propia dirección IP con su propia máscara de subred. El resultado de ANDing es la identificación de la red en la que reside el host de origen. Entonces compara las direcciones IP de destino con su propia máscara de subred. El resultado del segundo ANDing será la red en la que está el host de destino(n6). Si la dirección de la red de origen y la dirección de la red de destino son iguales, se pueden comunicar directamente por enlace. Si los resultados son distintos, están en diferentes redes o subredes, y se necesitara realizar un arp request del default getaway (esperando por su arp reply) por cada salto entre host-router o router-router hasta que el resultado del proceso de anding de como resultado que la dirección red origen y la dirección de red destino sean iguales. Entonces lo ultimo a realizarse es:

ARP REQUEST (WHO-IS): n1 -> n6 (Pregunta broadcast)

TRAMA ETHERNET = (macOrigen: MAC\_N1; macDestino: FF:FF:FF:FF:FF:FF)

Solicitud ARP = (macOrigen: MAC\_N1; IpOrigen: IP\_N5 ;

MacDestino: 00:00:00:00:00:0; IpDestino: IP\_N6)

ARP REPLY: n6 -> n1 (Respuesta unicast)

TRAMA ETHERNET = (macOrigen: MAC\_N6 ; macDestino: MAC\_N1) (SE OBTIENE LA MAC QUE BUSCABAMOS)

Solicitud ARP = (macOrigen: MAC\_N6; IpOrigen: IP\_N5 ;

MacDestino: MAC\_N1; IpDestino: IP\_N1)

Una vez llegado al destino, ya tenemos todas las tablas ARP completas para enviarle la respuesta (echo reply) a n5 sin tener que realizar consultas ARP.

c) Limpie la tabla de ARP en n5 y n1, borre el default gateway de n5. Vuelva a realizar el ping y capture el tráfico. ¿Qué diferencia hay con el punto b) ?

Para visualizar el contenido de una tabla arp de un nodo, solo hace falta ejecutar el comando arp –an, para eliminar una entrada de la tabla podemos utlizar el comando arp –d ip.

Una vez limpias las tablas de n5, n1 y eliminado el default getaway de n5. Al hacer un echo request a n6, la diferencia es que el resultado es “connect: Network is unreachable”, tampoco se generó tráfico sobre el echo request. Esto es así porque al realizar el proceso de anding anteriormente detallado, n5 sabe que el destino no está en su red, motivo por el cual debe obtener la dirección de default getaway (para salir a buscarlo a otra red), al no tenerla no puedo salir más allá de su red y por lo tanto la red destino es inalcanzable.

