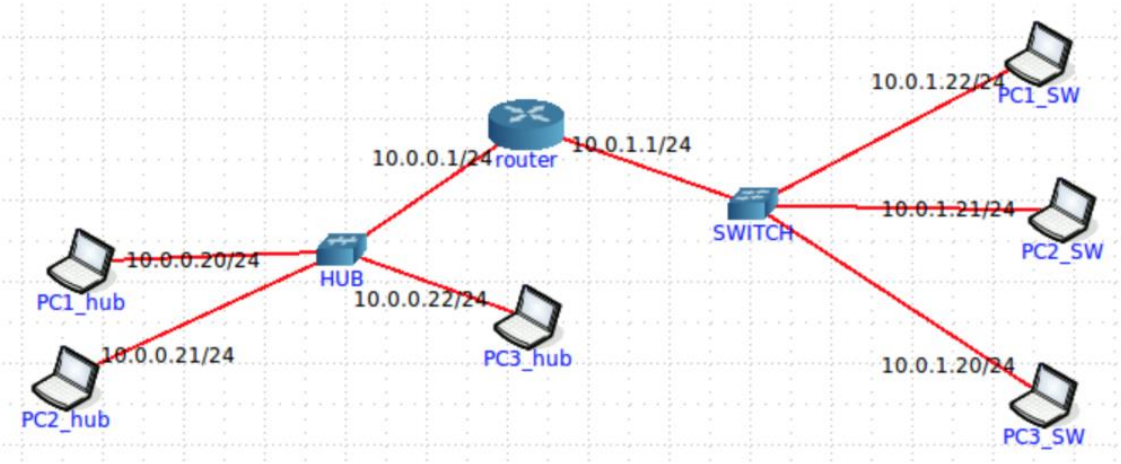
# Práctica 11

1. **Utilizando la máquina virtual provista por la cátedra, arme una red como la siguiente, con un segmento de LAN usando un HUB y otro segmento de LAN usando un SWITCH.**




   a. **Antes de empezar el ejercicio ejecute en una terminal el siguiente comando:**

      ```
      sudo iptables -P FORWARD ACCEPT
      ```

   b. **Analizar el funcionamiento de ARP.**
      i. **Indique para PC1_SW, PC2_SW y PC3_SW la IP y la dirección MAC de cada una.**

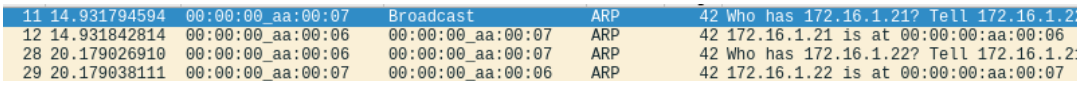
| | |
|---|---|
| PC1_SW | 00:00:00:aa:00:07 |
| PC2_SW | 00:00:00:aa:00:06 |
| PC3_SW | 00:00:00:aa:00:05 |

      ii. **Verifique el contenido de la tabla ARP de cada una de ellas.**

```
root@n4:/tmp/pycore.41113/n4.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.1.1               ether   00:00:00:aa:00:04   C                     eth0
root@n5:/tmp/pycore.41113/n5.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.1.1               ether   00:00:00:aa:00:04   C                     eth0
root@n6:/tmp/pycore.41113/n6.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.1.1               ether   00:00:00:aa:00:04   C                     eth0
```

      iii. **Inicie Wireshark en PC2_SW y luego envíe un ping desde la PC1_SW a la PC2_SW. Analice los paquetes ARP e ICMP capturados e indique:**

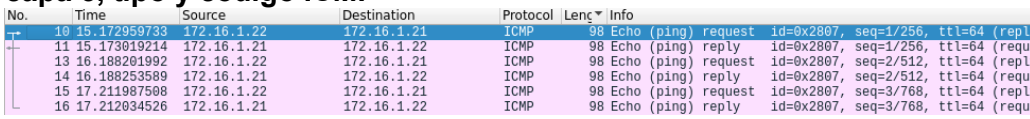
         - **Para ARP: tipo de paquete, direcciones de capa 2 y datos específicos del protocolo.**



| | | | | | |
|---|---|---|---|---|---|
| 11 | 14.931794594 | 00:00:00_aa:00:07 | Broadcast | ARP | 42 Who has 172.16.1.21? Tell 172.16.1.2 |
| 12 | 14.931842814 | 00:00:00_aa:00:06 | 00:00:00_aa:00:07 | ARP | 42 172.16.1.21 is at 00:00:00:aa:00:06 |
| 28 | 20.179026910 | 00:00:00_aa:00:06 | 00:00:00_aa:00:07 | ARP | 42 Who has 172.16.1.22? Tell 172.16.1.2 |
| 29 | 20.179038111 | 00:00:00_aa:00:07 | 00:00:00_aa:00:06 | ARP | 42 172.16.1.22 is at 00:00:00:aa:00:07 |

Se envía un paquete ARP a Broadcast preguntando quien tiene la dirección IP 172.16.1.2. PC2_swi responde directamente al que pregunto (PC1_swi) indicando que su MAC 00:00:00:aa:00:06. Lo mismo pasa en los dos últimos.

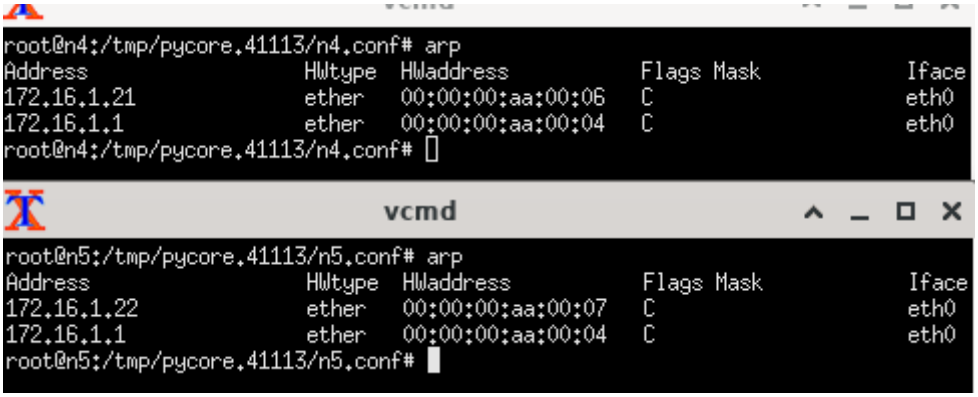
- **Para ICMP: tipo de paquete, direcciones de capa 2, de capa 3, tipo y código ICMP**



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 10 | 15.172959733 | 172.16.1.22 | 172.16.1.21 | ICMP | 98 | Echo (ping) request id=0x2807, seq=1/256, ttl=64 (repl |
| 11 | 15.173019214 | 172.16.1.21 | 172.16.1.22 | ICMP | 98 | Echo (ping) reply id=0x2807, seq=1/256, ttl=64 (requ |
| 13 | 16.188201992 | 172.16.1.22 | 172.16.1.21 | ICMP | 98 | Echo (ping) request id=0x2807, seq=2/512, ttl=64 (repl |
| 14 | 16.188253589 | 172.16.1.21 | 172.16.1.22 | ICMP | 98 | Echo (ping) reply id=0x2807, seq=2/512, ttl=64 (requ |
| 15 | 17.211987508 | 172.16.1.22 | 172.16.1.21 | ICMP | 98 | Echo (ping) request id=0x2807, seq=3/768, ttl=64 (repl |
| 16 | 17.212034526 | 172.16.1.21 | 172.16.1.22 | ICMP | 98 | Echo (ping) reply id=0x2807, seq=3/768, ttl=64 (requ |

Se envía un paquete ICMP con Echo Request (tipo 8, código 0) a la IP 172.16.1.21 (PC2_swi) y esta responde con un paquete ICMP con un Echo Replay (tipo 0, código 0) a 172.16.1.22 (PC1_swi)

iv. **Verifique nuevamente el contenido de la tabla ARP de las PCs ni bien termine de ejecutar el comando ping. ¿Qué entradas aparecen en cada tabla y por qué? ¿Qué estado tienen (ip neigh ls)?**




Aparece la IP y la MAC asociada de la otra PC involucrada en el ping. Esto sucede porque ambas guardaron la dirección MAC de la otra PC luego de los mensajes ARP. Tiene el estado de STALE.

v. **Borre las entradas de las tablas ARP de ambas PC y agregue de forma estática en PC1_SW la entrada que corresponde a PC2_SW y en PC2_SW la que corresponde a PC1_SW. Si hiciera un ping de PC1_SW a PC2_SW, ¿se verían paquetes de ARP? Verifíquelo en la máquina virtual iniciando una captura de tráfico en PC2_SW. ¿Qué estado tienen ahora las entradas ARP?**

No, no se ven los paquetes ARP puesto que cada PC ya sabe la dirección MAC de la otra. Tienen el estado PERMANENT

vi. **En PC1_SW modifique la entrada ARP que agregó en el punto anterior poniendo una MAC que no exista en la red. Vuelva a intentar hacer el ping. ¿Qué ocurre y por qué?**

El ping nunca es respondido. Esto sucede porque no existe la dirección MAC indicada en la red. Todos las PCs van a recibir el mensaje y todas lo van a descartar.

c. **Analizar y comparar el funcionamiento de un HUB y de un SWITCH.**

i. **Antes de empezar asegúrese que todas las tablas estén vacías. Puede hacerlo deteniendo e iniciando la topología nuevamente.**

ii. **Inicie Wireshark en PC3_HUB y luego envíe un ping desde la PC1_HUB a PC2_HUB. Analice el origen y destino de cada uno de los paquetes ARP e ICMP capturados. ¿Alguno se origina en o va destinado a PC3_HUB? ¿Por qué observa cada uno de esos paquetes?**

No, ninguno se origina en o va destinado a PC3_HUB. Se observa cada uno de esos paquetes porque se tiene un HUB que lo único que hace es retransmitir a todos los puertos.

iii. **Inicie Wireshark en PC3_SW y luego envíe un ping desde la PC1_SW a PC2_SW. Analice el origen y destino de cada uno de los paquetes ARP e ICMP capturados. ¿Alguno se origina en o va destinado a PC3_SW? ¿Por qué observa cada uno de esos paquetes?**

No, ninguno va dirigido a PC3_SW. Se observan los enviados a Broadcast de ARP (porque se envían a todos)

iv. **¿Qué diferencia observa entre los dos casos anteriores? Explique por qué ocurre así.**

La diferencia que se observa es que si se tiene un HUB todos los mensajes les llegan a todos, ya que el HUB se lo envia a todos los conectados, mientras que si se tiene un SWITCH solo le llega a la maquina a la cual está destinado el mensaje.

v. **Indique cómo queda la tabla CAM del SWITCH una vez realizado el ping. ¿Cómo se arma y en qué orden?**

| MAC | PORT |
|---|---|
| MAC_PC1_SWI | 0 |
| MAC_PC2_SWI | 1 |

Se sabe primero la entrada de la MAC de PC1 porque es el que realiza la consulta ARP primero y cuando la PC2 le responde se arma la entrada de esta.

2. **¿Qué es 802.11? Compare las direcciones MAC que contiene el encabezado de una trama 802.11 con los de una trama Ethernet, ¿cuál es la principal diferencia que encuentra? Investigue por qué cambian en 802.11 y para qué se usan.**

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

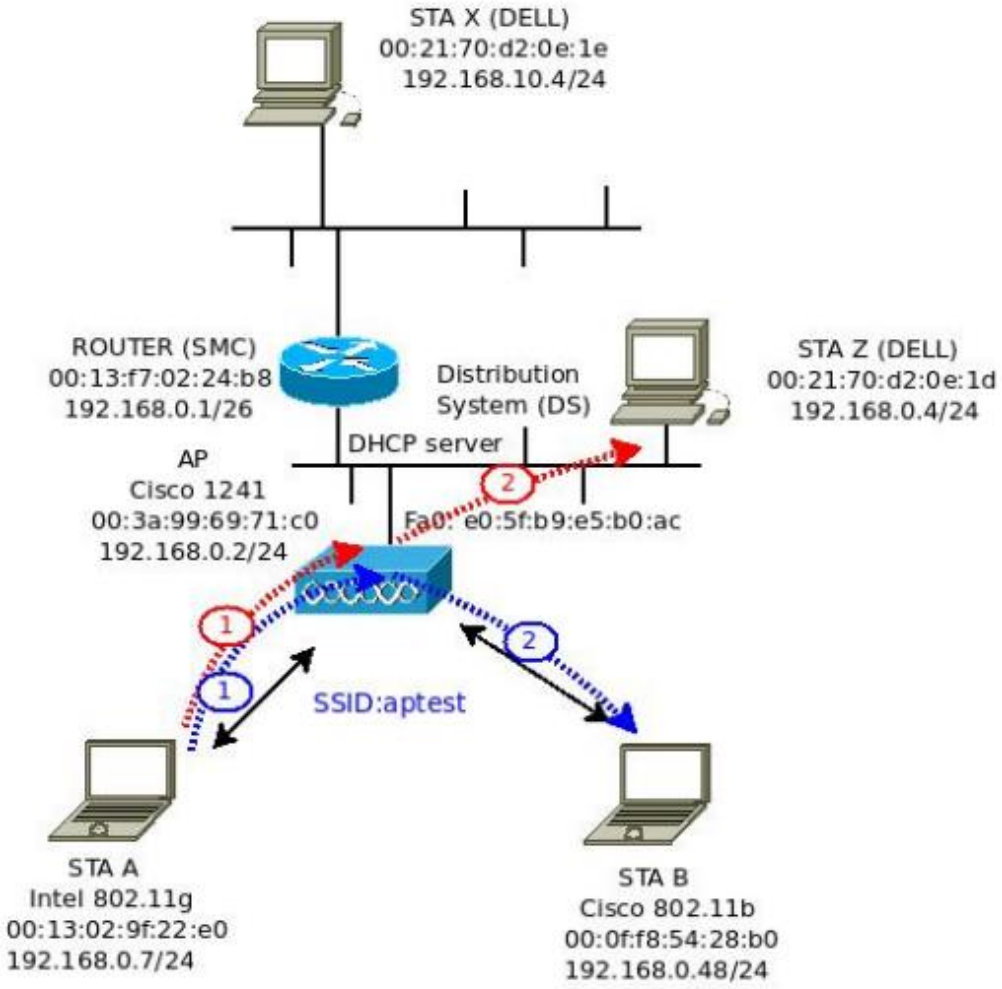
   Las direcciones MAC, tanto en las tramas 802.11 como en las tramas Ethernet, se utilizan para identificar de manera única los dispositivos de red en una red local2.
   En una trama Ethernet, solo se necesitan dos direcciones MAC: la dirección MAC de origen y la dirección MAC de destino.
   En una trama 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.

3. **Complete el siguiente cuadro y luego investigue qué estándar utilizan los dispositivos inalámbricos que tiene en su poder (su celular, su computadora, etc.).**

| 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 |

4. **Dada la siguiente topología, donde se pueden apreciar cuatro estaciones de trabajo, dos conectadas mediante un cable UTP y dos de forma inalámbrica, responda las siguientes preguntas.**




- **Suponiendo que las tablas ARP están completas y que STA A realiza un ping a STA B:**

  a. **Indique, entre STA A y el AP (1 azul) y entre el AP y STA B (2 azul):**
     - **Tipo de trama MAC (indicar si es 802.11 o Ethernet).**
     - **Direcciones MAC de la trama.**
     - **IP origen e IP destino.**

     En ambos casos la trama es de tipo 802.11

     Direcciones

     1) Primer Trama
        - Direccion 1: aptest
        - Direccion 2: 00:13:02:9f:22:e0
        - Direccion 3: 00:0f:f8:54:29:b0
     2) Segunda Trama
        - Direccion 1: 00:0f:f8:54:28:b0
        - Direccion 2: aptest
        - Direccion 3: 00:13:02:9f:22:e0

     IP Origen: 192.168.0.7/24

     IP Destino: 192:168.0.48/24

- **Suponiendo que las tablas ARP están completas y que STA A realiza un ping a STA Z:**

  a. **Indique, entre STA A y el AP (1 rojo) y entre el AP y STA Z (2 rojo):**
     - **Tipo de trama MAC (indicar si es 802.11 o Ethernet).**
     - **Direcciones MAC de la trama.**
     - **IP origen e IP destino.**

     En el caso 1) la trama es de tipo 802.11 y en el caso 2) la trama es de tipo Ethernet.

     Direcciones

     1) Primer Trama
        - Direccion 1: aptest
        - Direccion 2: 00:13:02:9f:22:e0
        - Direccion 3: 00:21:70:d2:0e:1d
     2) Segunda Trama
        - Direccion Origen: 00:13:02:9f:22:e0
        - Direccion Destino: 00:21:70:d2:0e:1d

     IP Origen: 192.168.0.7/24

     IP Destino: 192:168.0.4/24

- **Suponiendo que las tablas ARP están vacías y que STA A debe realizar un ARP Request para averiguar la MAC de STA B:**

  a. **Indique, entre STA A y el AP (1 azul) y entre el AP y STA B (2 azul):**
     - **Tipo de trama MAC (indicar si es 802.11 o Ethernet).**
     - **Direcciones MAC de la trama.**

     En ambos casos la trama es de tipo 802.11

     Direcciones

     1) Primer Trama
        - Direccion 1: aptest
        - Direccion 2: 00:13:02:9f:22:e0
        - Direccion 3: ff:ff:ff:ff:ff:ff
     2) Segunda Trama
        - Direccion 1: ff:ff:ff:ff:ff:ff
        - Direccion 2: aptest
        - Direccion 3: 00:13:02:9f:22:e0

- **¿Cómo sería el ARP Reply que va desde STA B hacia el AP? Indique las direcciones MAC de la trama.**

  Segunda Trama

  - Direccion 1: aptest
  - Direccion 2: 00:0f:f8:54:28:b0
  - Direccion 3: 00:13:02:9f:22:e0