**TL 5**

TEORIA

Análisis de trama

1. 6 pares [1-12] para MAC de destino
2. 6 pares [13-14]para MAC de origen
3. 2 pares para identificar si transporta IP. Ej: 08 00 => IP
   1. 1 bit para la versión del IP: Ej. 4 => IPV4
   2. 1 bit para el HLEN: Ej. 5 => HLEN5
4. 1 par para tipo de servicio
5. 2 pares para longitud total
6. 2 pares para ID de datagrama
7. 1 bits para el FLAG
8. 3 bits para el DESPLAZAMIENTO
9. 1 par para TLL => 80
10. 1 para Protocolo => 66 (TCP)
11. 2 pares para el CLC
12. 4 [53-60] pares para IP Fuente
13. 4 [61-68] pares para IP Destino
14. 2 [69-72] pares para Puerto Origen
15. 2 [73-76] pares para Puerto Destino

ETHERNET 2

Preambulo: No es mostrado en wireshark

Direccion de destino (6 bytes): Si está compuesta enteramente de 1 en binario, quiere decir que es un mensaje para el Broadcast.

Dirección de origen (6 bytes):

Tipo de protocolo: Indica el tipo de protocolo que está ocupando el formato de la trama (IP tiene un Ether Type de valor 0x0800, ARP tiene valor 0x0806, IPX tiene 0x8137.)

Datos

Secuencia de verificación: Frame check secuence (FCS o CRC) es un campo de 4 bytes que contiene el CHECKSUM que permite revisar la integridad del paquete recibido. No lo muestra el wireshark

**Ejercicios**

3. Tareas a. Análisis de la red en la que está configurada la estación de trabajo asignada. Ejecute la aplicación WINIPCFG ó desde MS-DOS, IPCONFIG. Seleccione Liberar Todo y luego Renovar Todo. Registre lo que ha verificado en la tabla que se encuentra a continuación:

Ejecutar => CMD => ipconfig /All

Nombre de la PC: LabAZUL-PC0191

Grupo de trabajo / Dominio: labsistemas.dom

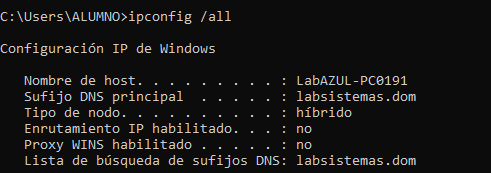
Dirección IP v4 de la PC : 192.168.2.166(Preferido)

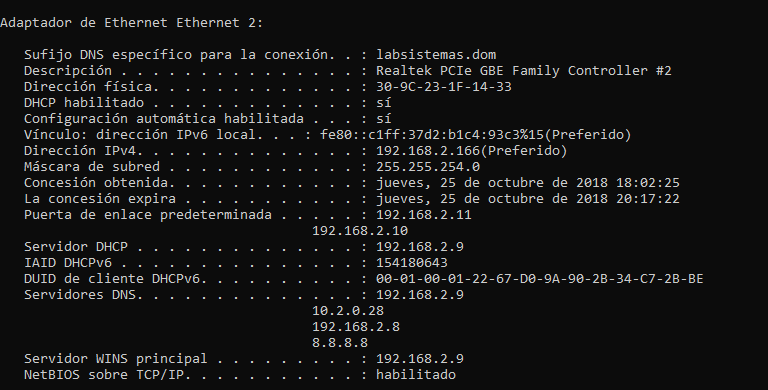
Máscara de Subred de la PC: 255.255.254.0

Puerta de enlace predeterminada: 192.168.2.11 y 192.168.2.10

Servidor DHCP de la Red: 192.168.2.9

Dirección MAC de la Placa de Red: 30-9C-23-1F-14-33





Responda las siguientes preguntas para cada item:

1) ¿De qué clase es la dirección IP de la PC?

Clase C (empieza con 192.168. - 2.166)

2) ¿Cuál es su máscara? ¿Es una máscara por defecto?

255.255.254.0

1\*8. 1\*8.11111110.00000000

No, es una máscara de subred, que deja 9 bits para hosts.

3) ¿La red tiene subredes?

Si. Puede tener una sola mas.

255.255.254.0 y 255.255.255.0

~~Tengo 2^7 – 2 = 128 – 2 = 126 => cantidad de sub redes posibles con esta mascara~~

4) ¿La red es pública o privada? ¿Qué direcciones de red de esta misma clase están reservadas?

Es una red privada

5) ¿Cuántos hosts puede haber en la red como máximo?

Mascara 255.255.254.0 => deja 9 bits para hosts.

Hosts desde: 192.168.254.1 =>Hasta: 192.168.255.254 (el ultimo para el broadcast)

Utilizo la cantidad de bits que están a cero en la máscara: 9

Puede tener 2^9 – 2 = 512 – 2 = 510 por hosts por sub redes

6) ¿Cuál es la dirección de broadcast de la red?

Mascara: 1111-1111. 1111-1111.1111-1110.00000000

Direccion de red: 192.168.254.0 /23

Direccion de broadcast: 192.168.255.255

7) ¿Es una red con colisiones? En caso afirmativo, ¿Cuántos dominios de colisión tiene?

No

8) ¿Es una red de broadcast? En caso afirmativo, ¿Cuántos dominios de broadcast tiene?

9) ¿Cómo se puede segmentar un dominio de colisión?

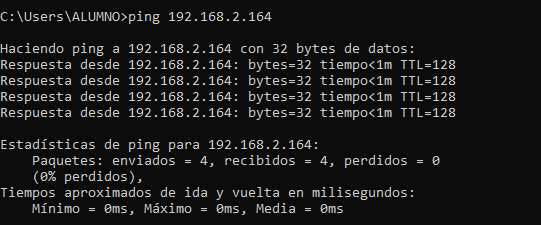
10) ¿Cómo se puede segmentar un dominio de broadcast?

11) ¿Esta red emplea direccionamiento IP estático o dinámico? ¿Cómo funciona el esquema empleado?

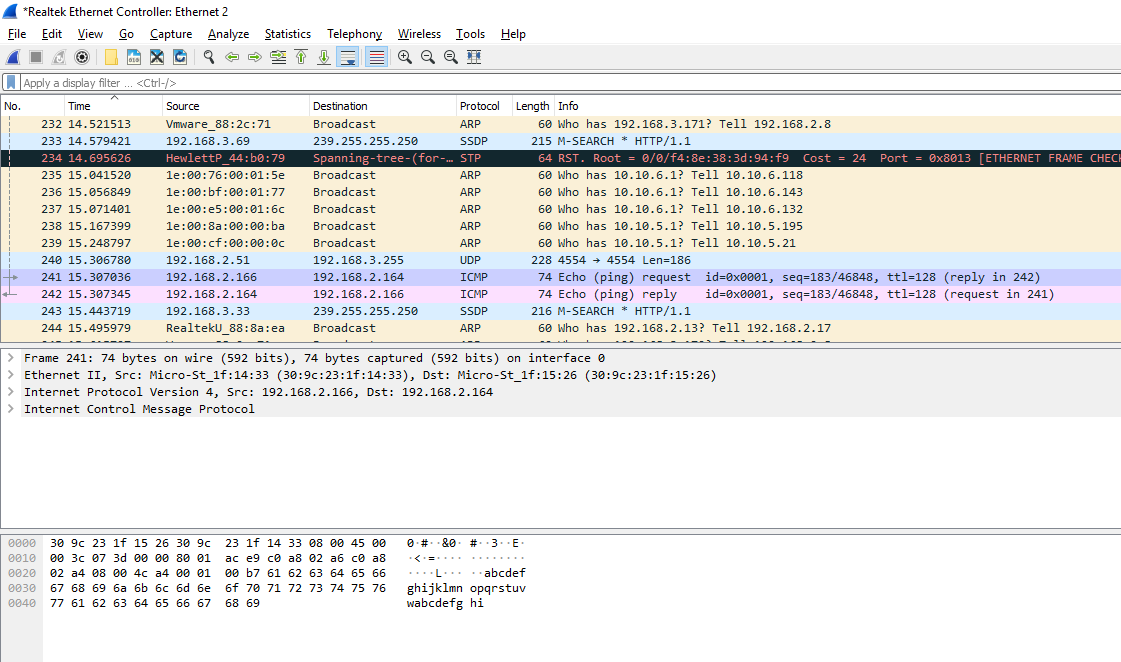
--

**B. Análisis de una trama Ethernet Inicie una captura con el Analizador y haga PING a otra PC de la misma LAN. Detenga la captura. Responda las siguientes preguntas, analizando una trama en particular:**

1) ¿Cómo accedió su host a la red? Compruebe el acceso de su host a la red para cierta comunicación.

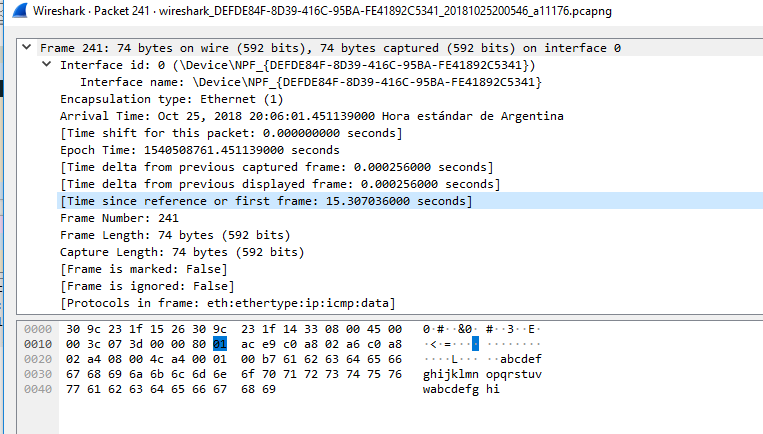


Para hacerlo en el programa, tiene que estar configurado únicamente la place de red física

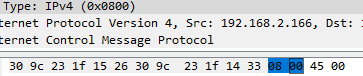


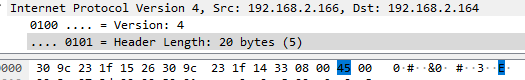


2) ¿Cuáles son los campos de la trama? ¿Qué valores tiene cada campo y cuál es su significado?

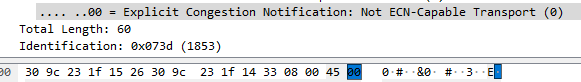


1. 6 pares [1-12] para MAC de destino: **30 9c 23 1f 15 26**
2. 6 pares [13-14]para MAC de origen: **30 9c 23 1f 14 33**
3. 2 pares para identificar si transporta IP (Ej: 08 00 => IP): **08 00 - IP**
   1. 1 bit para la versión del IP (Ej. 4 => IPV4) => **4 - IPV4**
   2. 1 bit para el (HLEN: Ej. 5) => **HLEN5**

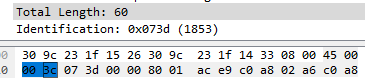




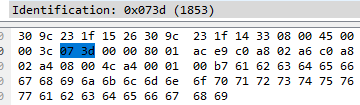
1. 1 par para tipo de servicio: 00



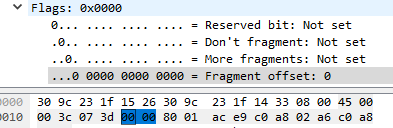
1. 2 pares para longitud total: **00 3c => 60**



1. 2 pares para ID de datagrama: **07 3d (1853)**



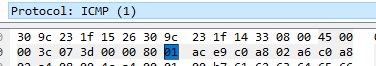
1. 1 bits para el FLAG
2. 3 bits para el DESPLAZAMIENTO



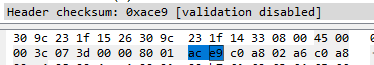
1. 1 par para TLL => 80



1. 1 par para Protocolo => 01 (ICPM)



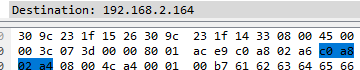
1. 2 pares para el CLC



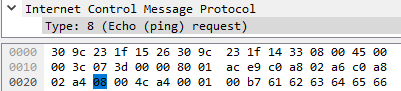
1. 4 [53-60] pares para IP Fuente



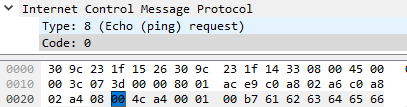
1. 4 [61-68] pares para IP Destino



1. 2 [69-72] pares para Puerto Origen



1. 2 [73-76] pares para Puerto Destino

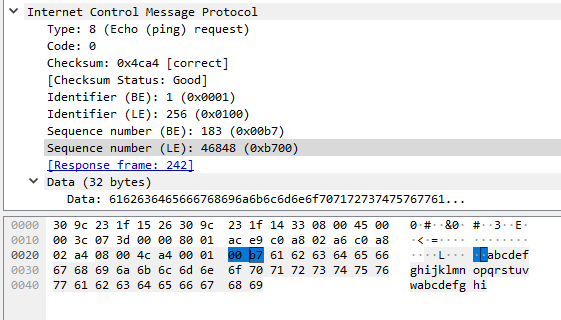


3) ¿Qué tamaño tiene el encabezado de la trama y cuáles son sus campos?

14 primeros bytes: 6 mac de destino + 6 mac de origen + 2 Ehternet type

4) ¿Qué tamaño tiene la cola de su trama? ¿Qué campo sirve para detectar errores y cuál es su valor?

60 bytes. El campo para detectar errores es el CRC, este campo no se está mostrando en wireshark



Nro de secuencia del 1er bit que transporta el segmento – 2 pares : 4c

Nro de acuse de recibo, del siguiente bit que espera recibir - 2 pares: a4

00

01

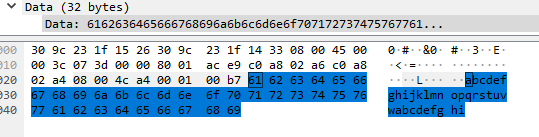
00

B7

61 EN ADELANTES SON LOS DATOS-

Para detectar los errores debería identificar el campo del ACKnowledgement

5) ¿Cuántos bytes corresponden a los datos? ¿Qué tamaño tiene este campo?



6) ¿Qué protocolos de nivel 3 (TCP/IP) se encapsularon en las tramas?

Hay encapsulado un datagrama IP que adentro tiene un datagraa ICMP

7) ¿Qué protocolos de nivel 4 y 5 (TCP/IP) se encapsularon en la trama?

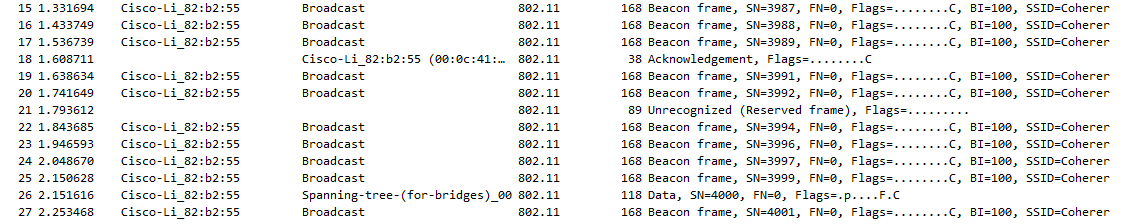
Ninguno

**---**

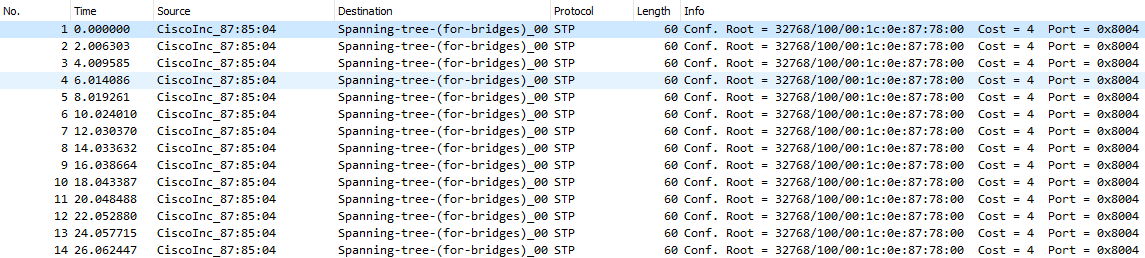
**c. Estudio comparativo de tramas típicas de LAN Ethernet**

**Agregue a la captura de tramas Ethernet: IEEE 802.3, las capturas en la red del laboratorio o ejemplos del sitio https://wiki.wireshark.org/ que se correspondan con:**

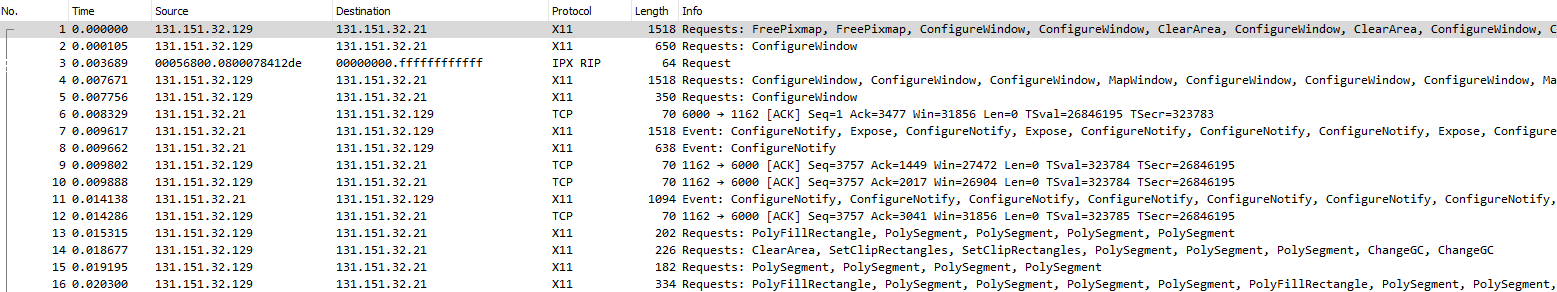
* IEEE\_802.11: IEEE 802.11 wireless LANs



* [STP:](https://wiki.wireshark.org/STP) IEEE 802.1D Spanning Tree Protocol



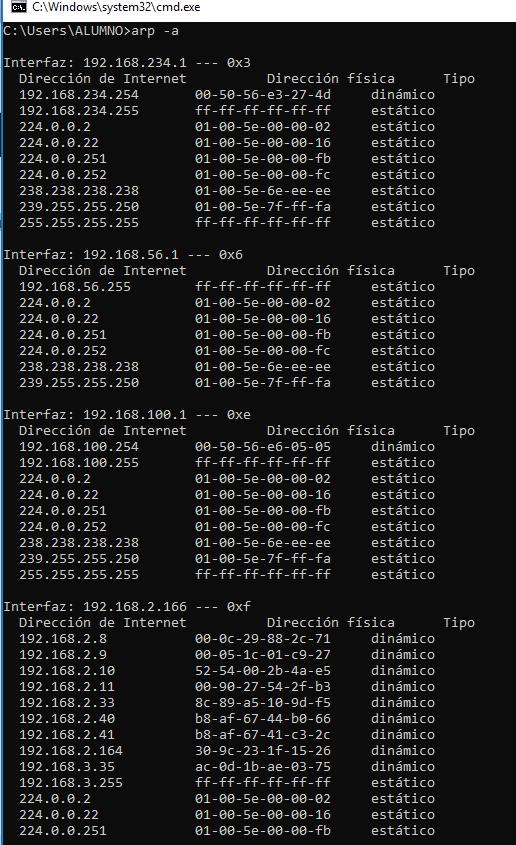
* [VLAN:](https://wiki.wireshark.org/VLAN) IEEE 802.1Q Virtual Bridged Local Area Networks

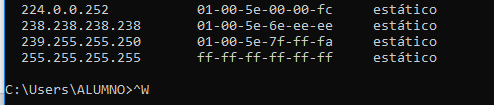


--

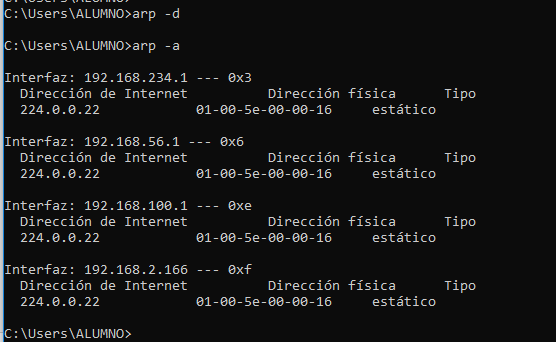
Análisis del tráfico ARP Realice las siguientes tareas en el intérprete de comandos y capture una o más tramas auxiliándose con el analizador de protocolos:

1) Observe el estado de la memoria caché de ARP en su PC. C:\>WINDOWS>arp –a





2) Borre la memoria caché de ARP en su PC. C:\>WINDOWS>arp -d <dirección IP>

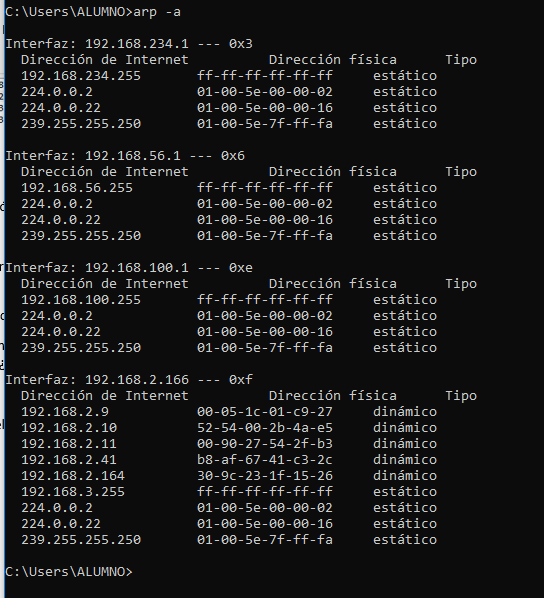


3) Inicie una captura con el Analizador y haga PING a otra PC de la misma LAN. Detenga la captura.



Responda:

a) ¿Cuántas PDU intervienen en la resolución ARP?



b) Describa la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen

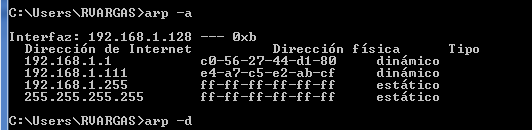
c) ¿Cuál es el estado actual de la memoria caché de ARP?

d) Volver a ejecutar el comando Ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?

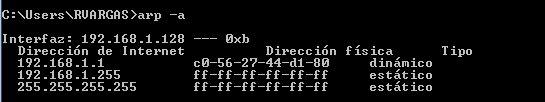
e) ¿Qué formato tiene una PDU ARP?

PDU: Lineas en el Wireshark

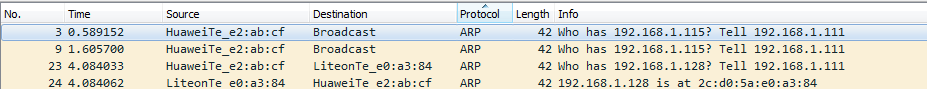
1. Vemos que aparece la IP 192.168.1.11
2. Limpiamos la lista.



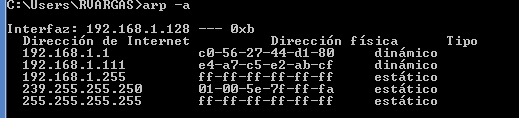
1. Volvemos a consultar, ya no está la IP en la lista



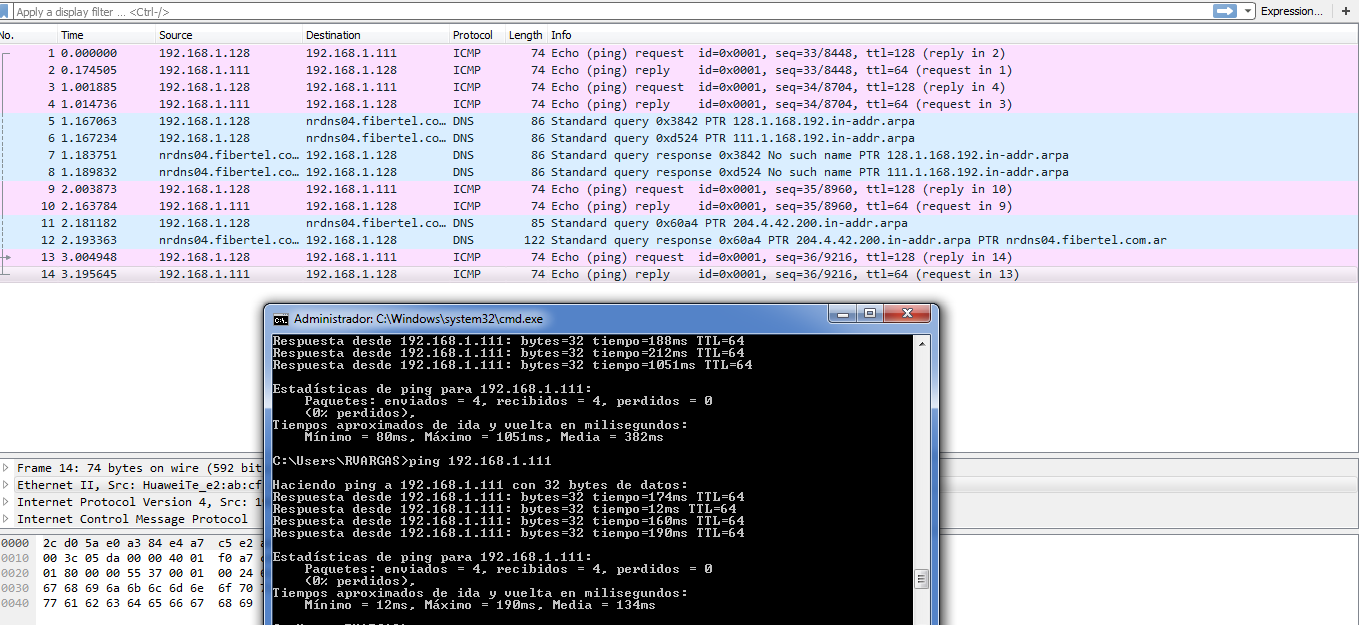
1. Hacemos ping e identificamos las líneas referidas a ARP => Son 4. Mi PC solicita / consulta al Broadcasta la MAC de la IP de destino, este responde



1. Reviso nuevamente la lista ARP; ahora debería aparecer la IP

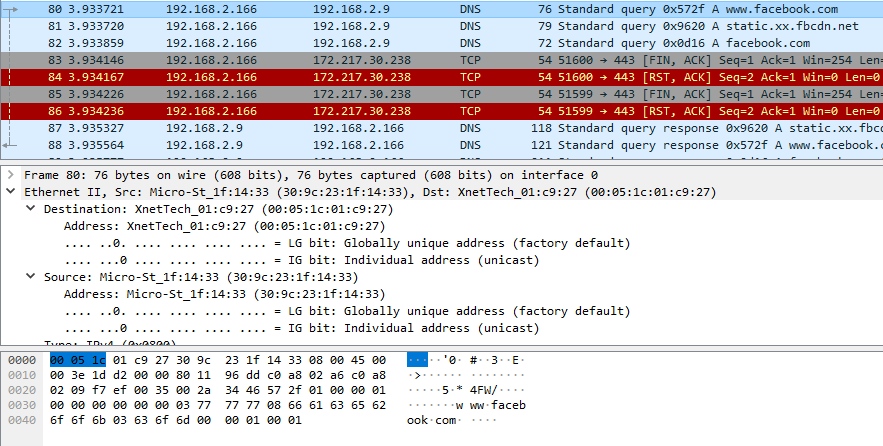


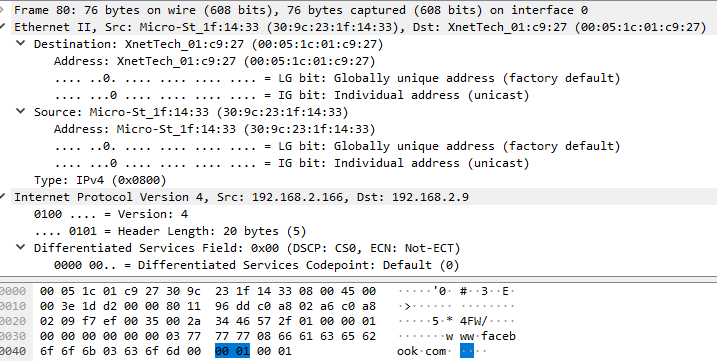
1. Vuelo a hacer una PING, esta vez ya no aparecen las líneas de ARP. MI PC ya conoce la MAC destino



4) Abra una página en Internet. Capture el tráfico involucrado y responda las mismas preguntas que en el ejercicio anterior.

Consulta a Facebook





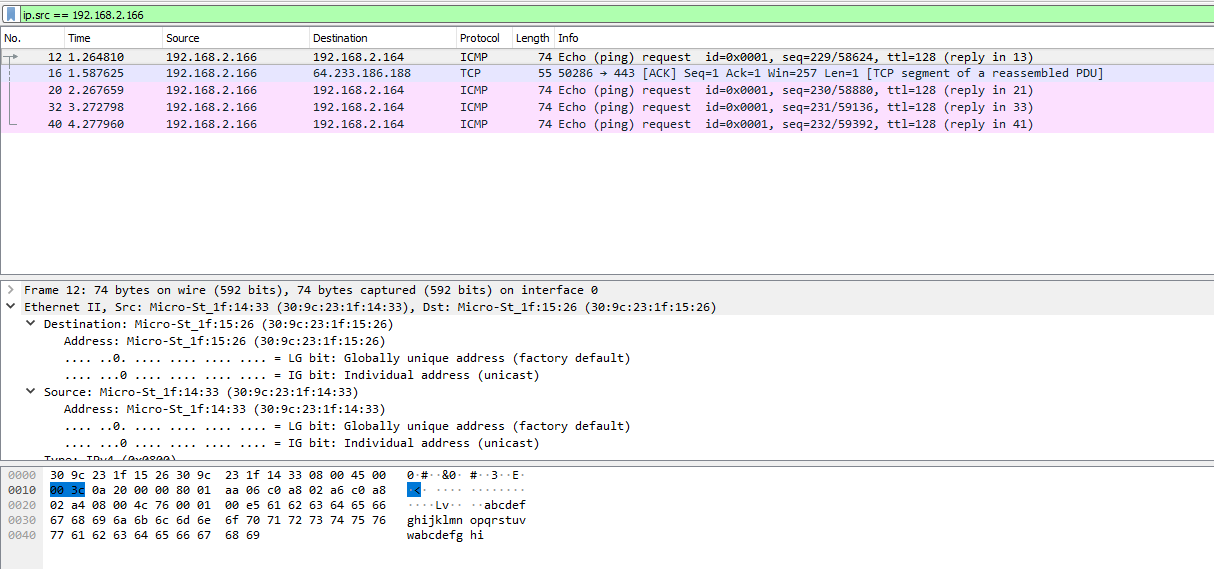


Análisis del tráfico IP e ICMP Realice las siguientes tareas en el intérprete de comandos y registre lo obtenido, auxiliándose con el analizador de protocolos:

1) Ping a la dirección IP de su PC.

2) Ping a otra PC de la LAN.

Cuando hago PING la máquina envía paquetes del protocolo ICMP, justamente es el que debo seleccionar para analizar la trama.



3) Ping a la dirección IP de un sitio de Internet no disponible en caché. Responda las siguientes preguntas para cada item:

a) ¿Se ejecutó la aplicación Ping?

SI

b) ¿Salen paquetes hacia la red? ¿Cuántos?

Si hago PIN a mi red, no salen ninguno.

c) ¿Qué tamaño tiene cada paquete?

0 para el ping a mi pc. No se identificar una línea ICMP, ya que nunca sale de mi placa de red.

74 bytes para la otras

d) ¿Cuántos bytes corresponden a cada protocolo?

e) ¿Cuántos bytes corresponden a los datos transmitidos?