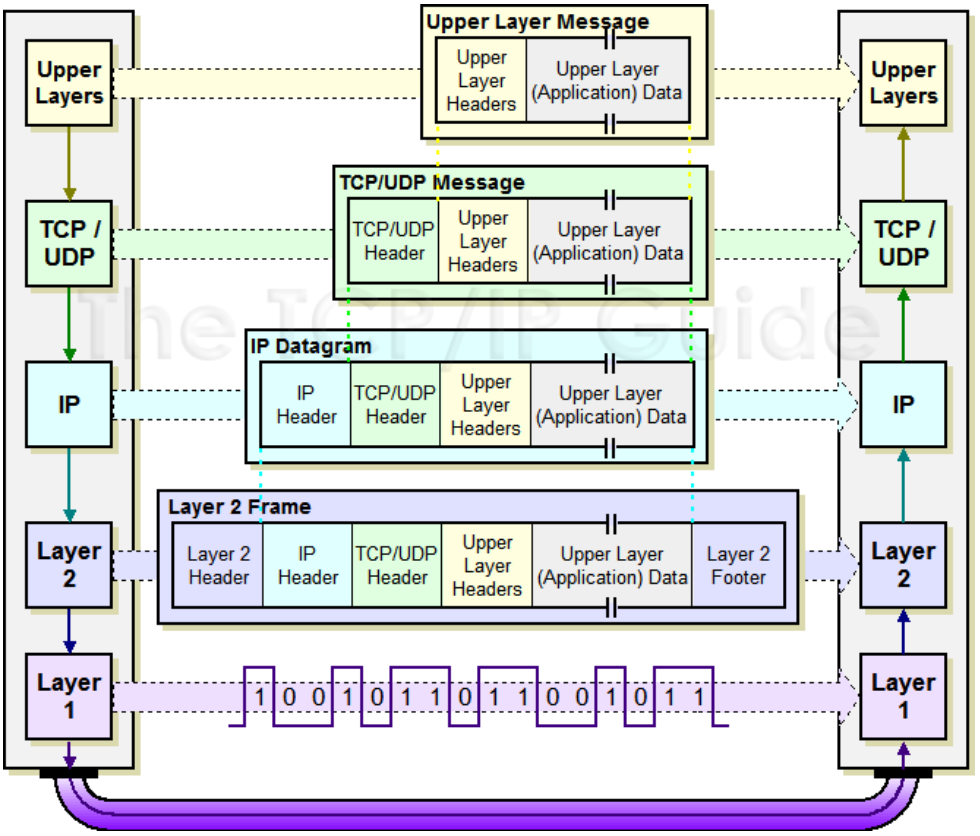
Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

Trabajo de laboratorio nº 5

Trabajo práctico Redes de Información

Alumna: Victoria Ruiz Schulze
Curso: K4573
2do cuatrimestre 2022



Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

Índice

a. Análisis de la WLAN

1. Ipconfig /all

Nombre del host	DESKTOP-U50EIUV
IP del host	192.168.0.149
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada	192.168.0.1
IP de broadcast de la red	192.168.0.255
Servidor DHCP de la red WIFI	192.168.0.1
Dirección MAC de la placa de red wifi	A0-F3-C1-F8-96-8C
Servidor(es) DNS reconocidos	192.168.0.1

2.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

```
C:\Users\Vic>arp -a

Interfaz: 192.168.0.149 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           4c-19-5d-cf-61-ac     dinámico
  192.168.0.74          00-71-47-8b-8f-a5     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

3 y 4.

HOST	IP	MAC
Celular	192.168.0.32	C2:71:DC:DB:F1:D0
Access Point (Gateway)	192.168.0.1	4C:19:5D:CF:61:AE (5GHz) 4C:19:5D:CF:61:AD (2.4)

5. La IP 192.168.0.149 es de clase C.

6. La máscara 255.255.255.0 es la máscara por defecto.

7. La red no tiene subredes.

8. Es una red privada. Las direcciones reservadas de clase C van entre 192.168.0.0 y 192.168.255.255.

9. En la red privada puede haber un máximo de 2^8 - 2 = 254 hosts.

10. Se trata de una red wifi, por lo que el estándar IEEE que se usa es el 802.11. Usa CSMA/CA.

11. No es una red que detecta colisiones.

12. Es una red que previene colisiones. CSMA/CA resuelve el problema del nodo fantasma.

13. No es una dirección MAC de broadcast.

14. Para reducir el tamaño de los dominios de colisión en una LAN (es decir, segmentarlos) se deben usar dispositivos que operan en la capa 2 o superiores del modelo OSI. Los hubs (capa 1) extienden los dominios de colisión, mientras que switches (capa 2) y routers (capa 3) los limitan.

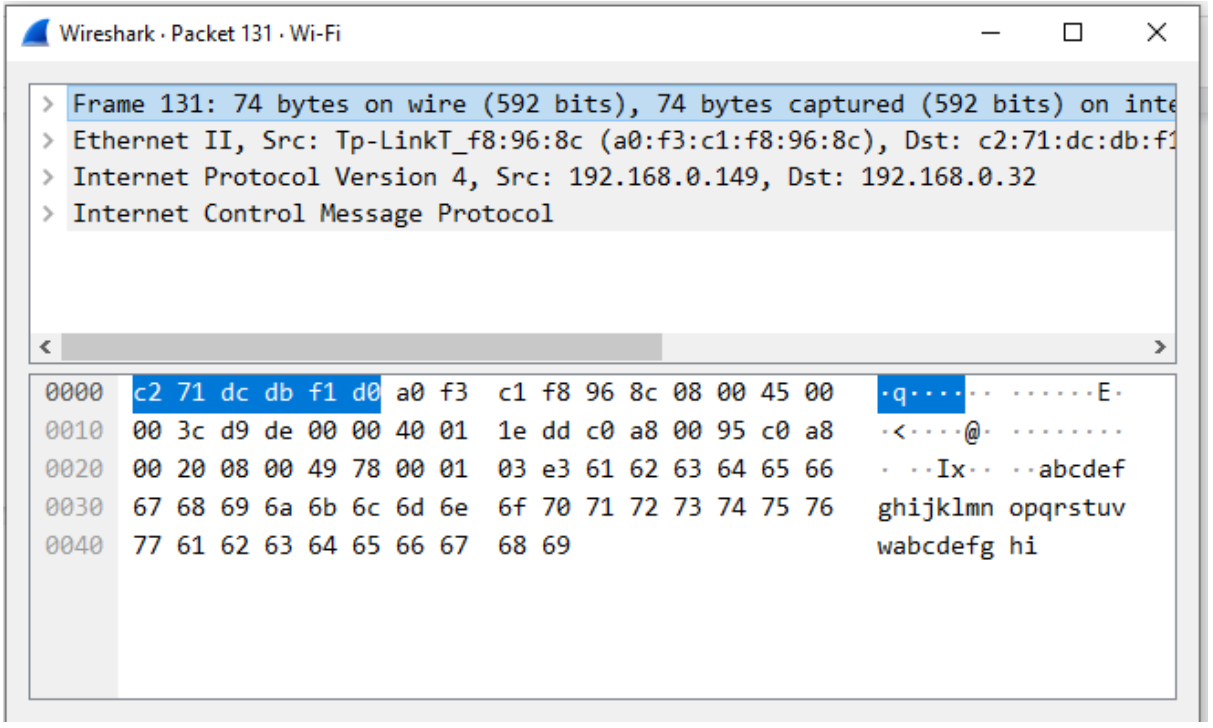
15. Para dividir dominios de broadcast en una LAN es necesario implementar VLANs o dispositivos que operan en la capa 3 del modelo OSI, tales como switches multilayer o routers.

16. Esta red usa el protocolo DHCP para la asignación dinámica de IP. Cuando se conecta por primera vez, el host envía un mensaje DHCP a toda la red solicitando una IP. El servidor DHCP responde a ese mensaje asignándole dirección IP.

17. Direcciones IP públicas conocidas por mi host: ninguna

b. Análisis de una trama Ethernet

Ping a celular 192.168.0.32, desde PC 192.168.0.149.



1. ¿Cuáles son los campos de la trama? ¿Qué valores tiene cada campo y cuál es su significado?
Se usa el protocolo ICMP, encapsulado en una trama IP, encapsulada en una trama Ethernet 2.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

Protocolo	Campo	Valor	Tamaño
Ethernet 2	Preámbulo	[No reportado por Wireshark]	8 bytes
	MAC Address Destino	C2:71:DC:DB:F1:D0	6 bytes
	MAC Address origen	A0-F3-C1-F8-96-8C	6 bytes
	Type	IPv4	2 bytes
	Carga	[Protocolo IP]	60 bytes (0 a 1500 bytes)
	Relleno	[No hay!]	
	CRC	[No reportado por Wireshark]	4 bytes
IP	Versión	4	4 bits
	Header length	20 bytes (5)	4 bits
	Tipo de Servicio	DSC = 0 ECN = 0	1 byte
	Longitud total	60	2 bytes
	Identificador	55774	2 bytes
	Flags	000	3 bits
	Offset de Fragmento	0	13 bits
	TTL	64	1 byte
	Protocolo	ICMP (1)	1 byte
	CRC cabecera	0x1edd (validación deshabilitada)	2 bytes
	Dir. IP origen	192.168.0.149	4 bytes
	Dir. IP destino	192.168.0.32	4 bytes
	Opciones		0
	Relleno		0
	Carga	[Protocolo ICMP]	40 bytes
ICMP	Tipo	8 (ping)	1 byte

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

	Código	0	1 byte
	Checksum	Correcto	2 bytes
	Resto del encabezado		4 bytes
	Datos (opcional)		32 bytes

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

- El encabezado Ethernet tiene 14 bytes, sin contar el preámbulo. Ver campos arriba (en lila)
- El encabezado IP tiene 20 bytes. Ver campos arriba (en verde).
- El encabezado ICMP itene 8 bytes. Ver campos arriba (en celeste)

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

- En Ethernet debería haber un campo de detección de errores con CRC al final, pero no es reportado por Wireshark. De existir, debería tener 4 bytes.
- En IP hay un campo de CRC de 2 bytes.
- En ICMP hay un campo de checksum de 2 bytes.

4. ¿Cuántos bytes corresponden a los datos? ¿Este campo es de tamaño fijo o variable? En este nivel ¿el campo de datos tiene una longitud mínima, máxima o no está especificado por su estándar?

- Ethernet.
    - Datos reales: 60 bytes
    - Mínimos: 0
    - Máximos: 1500 bytes
- IP:
    - Datos reales: 40 bytes
    - Mínimos: ??
    - Máximos: ??
- ICMP:
    - Datos reales: 32 bytes
    - Mínimo: 0
    - Máximo: 68 bytes

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

5) Revisando nuevamente la trama Ethernet ¿qué campos se corresponden con los especificados en IEEE 802.2 y cuáles a IEEE 802.3?
Se trata de una trama Ethernet 2, con Ethertype en vez de longitud. No usa LLC (802.2)

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

Ethernet 2	802.11 Wireless	802.1Q VLANs	802.1D STP
Campos: • MAC destino (6 bytes) • MAC origen (6 bytes) • Ethertype/Length (2 bytes) • [Datos] • Al final: padding	Campos: • Version • Type • Subtype • ToDS • FromDS • More Fragments • Retry • Power Management • More data • Protected • Duración • Address fields (3) • Sequence control • Address 4 • Datos • CRC	Campos: • MAC destino (6 bytes) • MAC origen (6 bytes) • Ethertype/Length (2 bytes): 0x8100 • PRI (3 bits) + Token Encapsulation Flag (1 bit) • VLAN ID (12 bits) • Type/Len (2 bytes) • [Datos] • Al final: padding VLAN tag en verde	Encapsulados en Trama 802.3 Ethernet + Trama 802.2 LLC Campos STP: • ID de protocolo • Versión • Tipo • Flags • ID raiz • Costo camino raiz • ID bridge • ID puerto • Antigüedad • Antigüedad máxima • Tiempo de saludo • Delay

d. Análisis del tráfico ARP

1. Estado inicial de memoria caché de ARP en mi PC.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

```
C:\Users\Vic>arp -a

Interfaz: 192.168.0.149 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           4c-19-5d-cf-61-ac     dinámico
  192.168.0.32          c2-71-dc-db-f1-d0     dinámico
  192.168.0.74          00-71-47-8b-8f-a5     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

a) ¿En nivel del modelo OSI funciona el protocolo ARP?
Nivel 2. Se maneja a nivel físico (MAC) para obtener IPs.

b) ¿Cuántas PDU intervienen en la resolución ARP?
2 PDU

247	5.827458	142.251.133.46	192.168.0.149	UDP	68 443 → 62862 Len=26
248	6.147099	Tp-LinkT_f8:96:8c	Broadcast	ARP	42 Who has 192.168.0.32? Tel
249	6.226228	192.168.0.149	18.231.65.122	TLSv1.2	110 Application Data
250	6.227057	192.168.0.149	18.231.65.122	TLSv1.2	110 Application Data
251	6.227887	192.168.0.149	18.231.65.122	TLSv1.2	110 Application Data
252	6.301966	18.231.65.122	192.168.0.149	TCP	60 443 → 56473 [ACK] Seq=1 A
253	6.301969	18.231.65.122	192.168.0.149	TCP	60 443 → 56470 [ACK] Seq=1 A
254	6.304947	c2:71:dc:db:f1:d0	Tp-LinkT_f8:96:8c	ARP	60 192.168.0.32 is at c2:71:
255	6.305004	192.168.0.149	192.168.0.32	ICMP	74 Echo (ping) request id=0
256	6.316846	18.231.65.122	192.168.0.149	TCP	60 443 → 56472 [ACK] Seq=1 A
257	6.383657	34.120.83.142	192.168.0.149	TLSv1.2	92 Application Data

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

1. Un equipo envía un broadcast, solicitando la dirección física (MAC) del que tiene la IP 192.168.0.32
2. El equipo con la IP correspondiente, responde un mensaje unicast a la MAC de quien solicitaba la información.

d) ¿Cuál es el estado actual de la memoria caché de ARP?
La memoria cache fue borrada antes de hacer el ping. Después de hacer el ping volvió a este estado:

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

```
C:\Windows\System32>arp -a

Interfaz: 192.168.0.149 --- 0x6
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           4c-19-5d-cf-61-ac     dinámico
  192.168.0.32          c2-71-dc-db-f1-d0     dinámico
  192.168.0.74          00-71-47-8b-8f-a5     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

e) Volver a ejecutar el comando Ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?
No aparecieron tramas ARP, ya que la IP se encuentra en el cache ARP gracias al intercambio ARP que surgió con el ping anterior.

f) ¿Qué formato tiene una PDU ARP?

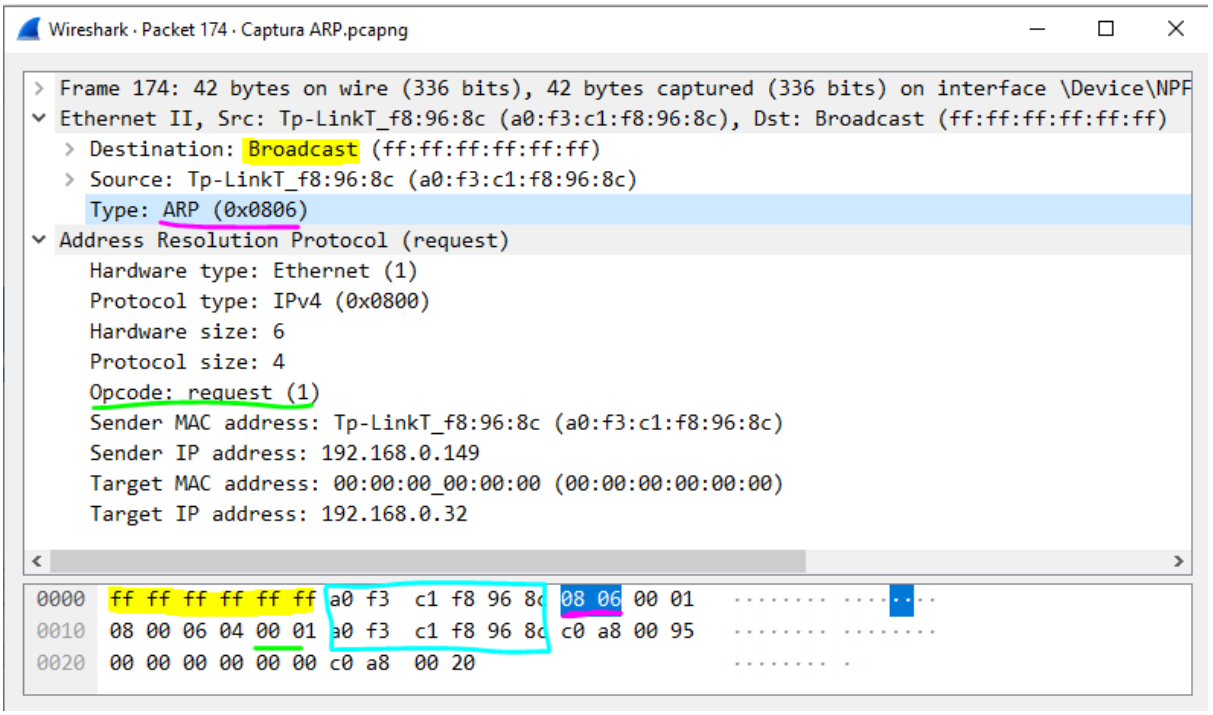
Formato general:

- Hardware type (2 bytes)
- Protocolo (2 bytes) - ARP: 0x0806 / RARP: 0x8035
- Long dirección física en bytes (1 byte)
- Long dirección lógica en bytes (1 byte)
- Operación (2 bytes)
- Dirección física del emisor - MAC (6 bytes)
- Dirección lógica del emisor - IP (4 bytes)
- Dirección física del destino - MAC (6 bytes)
- Dirección lógica del destino - IP (4 bytes)

Caso concreto - ARP Request:

- En el header Ethernet
    - MAC destino: Es un broadcast: 0xFFFFFFFFFFFF.
    - MAC origen:
    - Type: ARP (0x0806)
- En el header ARP
    - Opcode: indica que es request (0x0001)

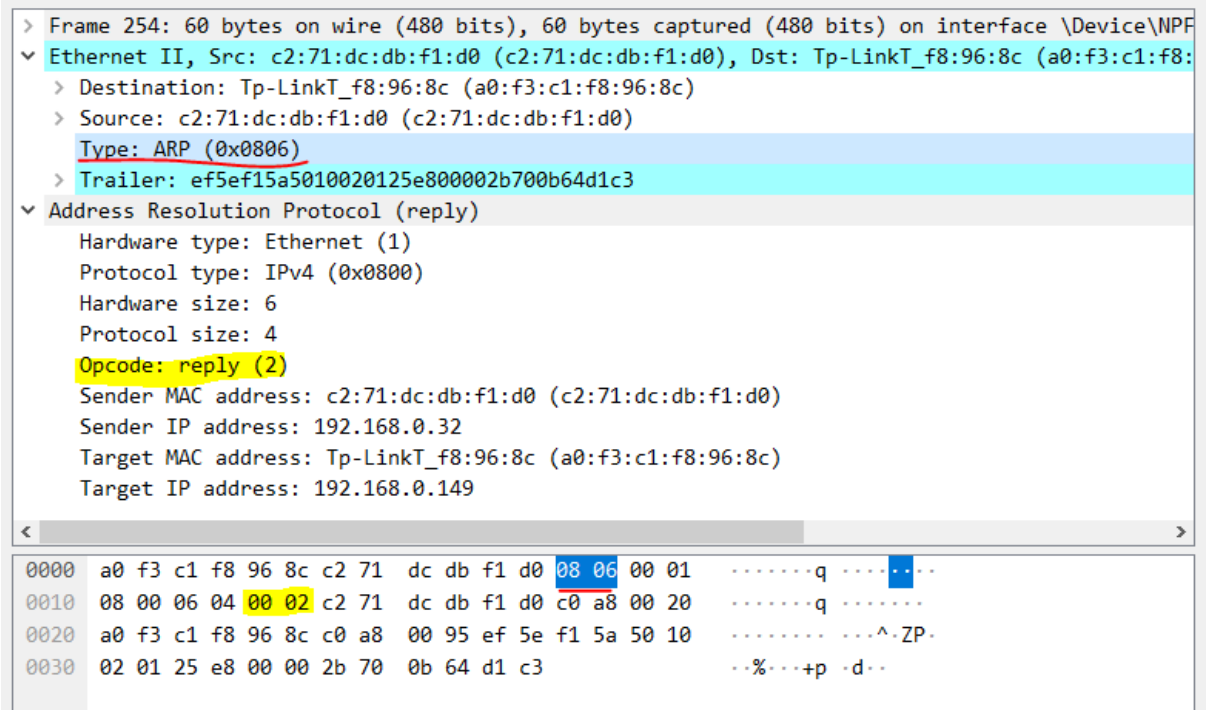
- Sender MAC: MAC del emisor (conocida). Coincide con la MAC de origen del encabezado de Ethernet.
- Sender IP: IP del emisor (conocida)
- Target MAC: 0x000000000000 ya que es desconocida.
- Target IP: la IP buscada (últimos 8 dígitos)



Caso concreto - ARP reply

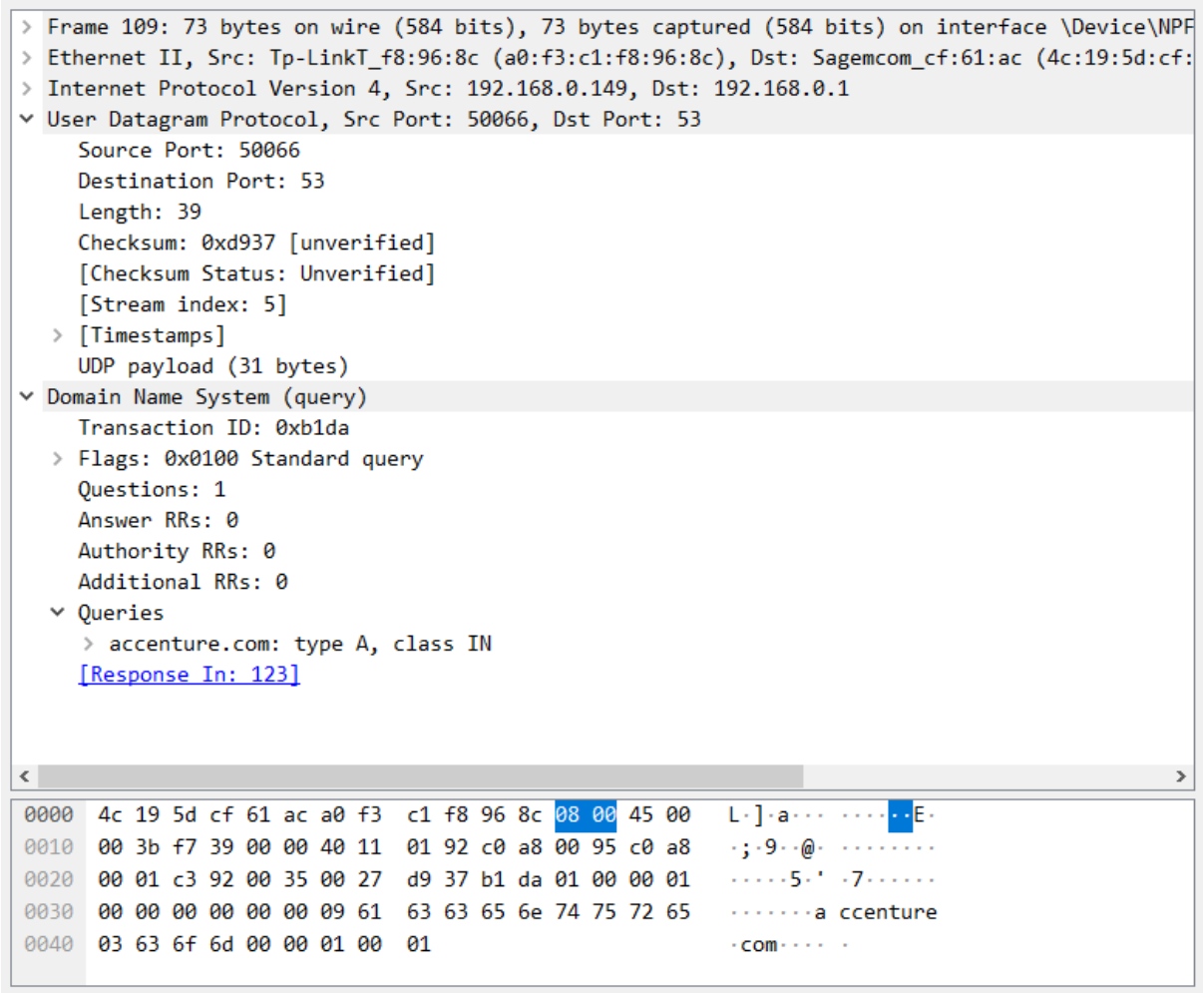
- Encabezado Ethernet
  - MAC unicast de destino y destino
  - Type: 0x0806 (ARP)
- Encabezado ARP
  - Opcode: 0x0002 (reply)
  - Hay coincidencia entre MACs en encabezado Ethernet y ARP.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022



4) Abra una página en Internet no haya abierto desde que encendió la PC. Capture el tráfico involucrado y responda las mismas preguntas que en el ejercicio anterior. ¿Los Hosts que intervienen en esta captura son los mismos que en el caso anterior?
Cuando abro un sitio no visitado recientemente se dispara, entre otras cosas, un request de DNS. En particular, abrí accenture.com.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022



DNS es un protocolo de nivel aplicación, que se encapsula de la siguiente manera: Ethernet > IP > UDP.

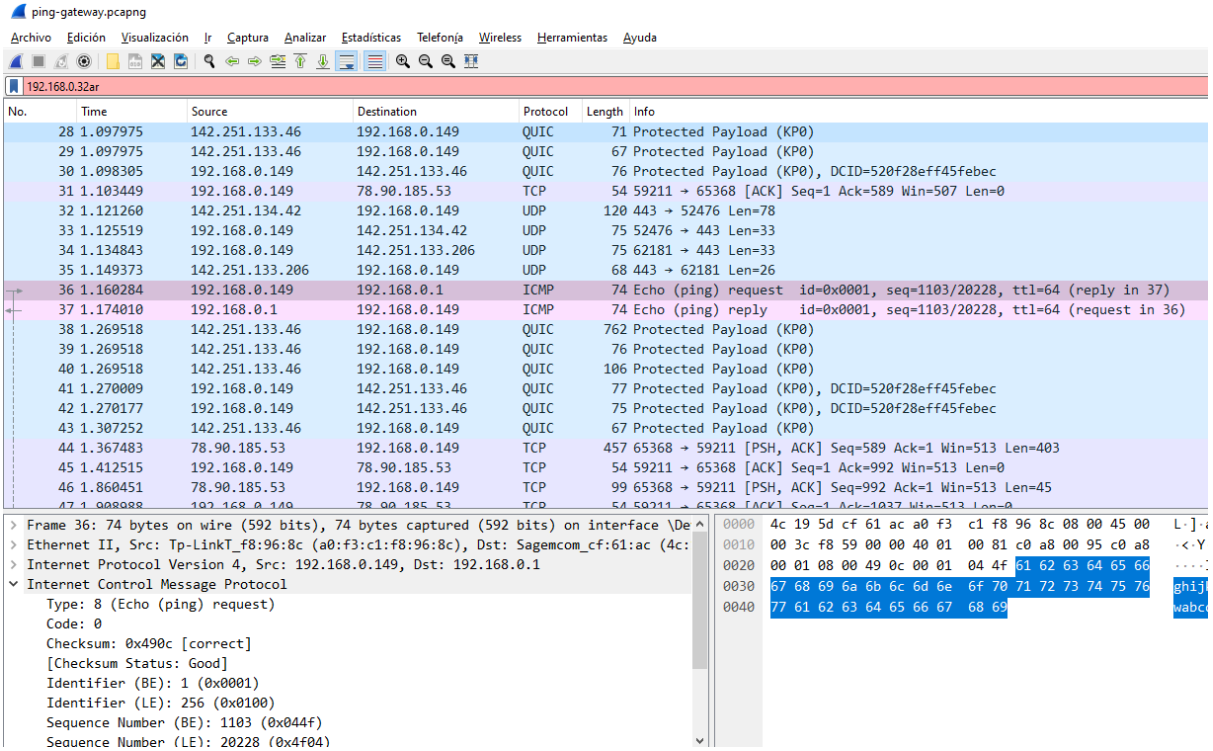
e. Análisis del tráfico IP e ICMP

	1. Ping a IP propia	2. Ping a gateway	3. Ping a google.com
¿Se ejecutó la aplicación Ping?	Sí.	Sí	
¿Salen paquetes hacia la red? ¿Cuántos?	No por la LAN, sino por un adaptador de “Loopback”	2 de DNS	2 de DNS (request + reply) 8 ICMP (4x request + reply)

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

¿Qué tamaño tiene cada paquete?	64 bytes	74 bytes	DNS: 81 bytes request, 111 reply ICMP: 74 bytes c/u
¿Cuántos bytes corresponden a cada protocolo?	Cabecera loopback: 4 bytes Cabecera IP: 20 bytes PDU ICMP: 40 bytes	Cabecera Ethernet: 14 bytes (incluye preámbulo) Cabecera IP: 20 bytes PDU ICMP: 40 bytes	ICMP: Cabecera Ethernet: 14 bytes (incluye preámbulo) Cabecera IP: 20 bytes PDU ICMP: 40 bytes
¿Cuántos bytes corresponden a los datos transmitidos?	32 bytes	32 bytes	DNS: 27 bytes req + 30 bytes response (que también tiene 27 adicionales de request) ICMP: 32 bytes

Ping a gateway 192.168.0.149. Salen 2 PDUs de tipo ICMP, que son request y reply.



4) Al hacer Ping ¿cuántas capas del Modelo OSI y qué protocolos intervienen? ¿Qué tipos y códigos de mensaje ICMP se observaron en los casos analizados?

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

Al hacer PING intervienen:

- Ethernet (capa 2)
- IP (capa 3)
- ICMP (capa 3)

Hay mensajes ICMP de tipo request y reply. 4 de cada uno, porque en el ping se envían 4 paquetes.

cmp

	Time	Source	Destination	Protocol	Length	Info
57	1.473783	192.168.0.149	147.135.71.240	ICMP	74	Echo (ping) request id=0x0001, seq=1147/3
67	1.664294	147.135.71.240	192.168.0.149	ICMP	74	Echo (ping) reply id=0x0001, seq=1147/3
107	2.482305	192.168.0.149	147.135.71.240	ICMP	74	Echo (ping) request id=0x0001, seq=1148/3
115	2.684259	147.135.71.240	192.168.0.149	ICMP	74	Echo (ping) reply id=0x0001, seq=1148/3
142	3.492921	192.168.0.149	147.135.71.240	ICMP	74	Echo (ping) request id=0x0001, seq=1149/3
151	3.683733	147.135.71.240	192.168.0.149	ICMP	74	Echo (ping) reply id=0x0001, seq=1149/3
180	4.509140	192.168.0.149	147.135.71.240	ICMP	74	Echo (ping) request id=0x0001, seq=1150/3
189	4.699010	147.135.71.240	192.168.0.149	ICMP	74	Echo (ping) reply id=0x0001, seq=1150/3

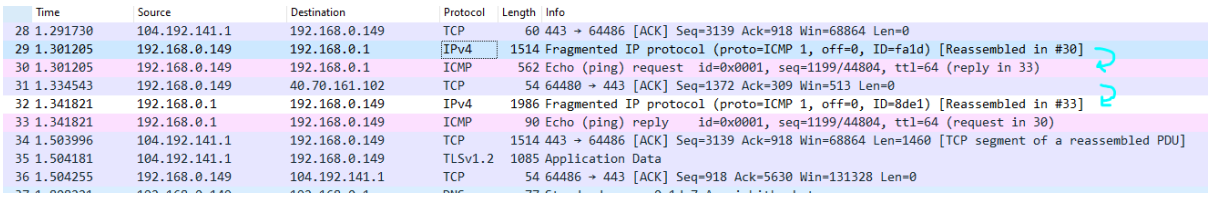
f. Análisis del MTU de la red

El MTU de la red es 1500 bytes. El máximo de bytes que se pueden enviar en un PING sin que se fragmente el paquete es: 1472 bytes (a los que se agregan: 20 de cabecera IP, 8 de cabecera ICMP).

```
C:\Windows\System32>ping -f -l 1472 192.168.0.1

Haciendo ping a 192.168.0.1 con 1472 bytes de datos:
Respuesta desde 192.168.0.1: bytes=1472 tiempo=23ms TTL=64

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 23ms, Media = 23ms
Control-C
^C
C:\Windows\System32>ping -f -l 1473 192.168.0.1

Haciendo ping a 192.168.0.1 con 1473 bytes de datos:
Es necesario fragmentar el paquete pero se especificó DF.

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

a) Al hacer ping con 1200, 1499 y 2000 bytes, los paquetes se fragmentaron en los últimos 2 casos.

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022



	Time	Source	Destination	Protocol	Length	Info
28	1.291730	104.192.141.1	192.168.0.149	TCP	60	443 → 64486 [ACK] Seq=3139 Ack=918 Win=68864 Len=0
29	1.301205	192.168.0.149	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=fa1d) [Reassembled in #30]
30	1.301205	192.168.0.149	192.168.0.1	ICMP	562	Echo (ping) request id=0x0001, seq=1199/44804, ttl=64 (reply in 33)
31	1.334543	192.168.0.149	40.70.161.102	TCP	54	64480 → 443 [ACK] Seq=1372 Ack=309 Win=513 Len=0
32	1.341821	192.168.0.1	192.168.0.149	IPv4	1986	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8de1) [Reassembled in #33]
33	1.341821	192.168.0.1	192.168.0.149	ICMP	90	Echo (ping) reply id=0x0001, seq=1199/44804, ttl=64 (request in 30)
34	1.503996	104.192.141.1	192.168.0.149	TCP	1514	443 → 64486 [ACK] Seq=3139 Ack=918 Win=68864 Len=1460 [TCP segment of a reassembled PDU]
35	1.504181	104.192.141.1	192.168.0.149	TLSv1.2	1085	Application Data
36	1.504255	192.168.0.149	104.192.141.1	TCP	54	64486 → 443 [ACK] Seq=918 Ack=5630 Win=131328 Len=0

Para el ping de 2000 bytes:
El mensaje se fragmenta a nivel IPv4 en 2 mensajes:

- Primer mensaje: datos IP de 1480 bytes (MTU - encabezado IP).
- Segundo mensaje: datos IP de 528 bytes.

En total a nivel IP se transmiten 2008 bytes, que equivalen a los datos enviados + la cabecera ICMP de 8 bytes.

b) ¿Qué campos de que protocolos intervienen en la fragmentación?
La fragmentación se realiza a nivel IP:

- Flag more fragments. En el primer paquete, su valor es 1. En el 2o, es 0.
- Fragment offset. En el primer paquete su valor es 0, en el 2o, es a 0.

c) ¿Qué tamaño tiene cada paquete?
Tomando el primer paquete (primer fragmento IP), el tamaño es de 1514 bytes.
Tomando el segundo paquete (último fragmento IP), el tamaño es de 562 bytes.

d) ¿Cuántos bytes corresponden a cada protocolo?
e) ¿Cuántos bytes corresponden a los datos transmitidos?
Primer paquete:

- Ethernet (cabecera incluyendo preámbulo): 14 bytes
- IP (cabecera): 20 bytes
- Datos (1a parte del mensaje ICMP): 1480 bytes

Segundo paquete:

- Ethernet (cabecera incluyendo preámbulo): 14 bytes
- IP (cabecera): 20 bytes
- Datos (1a parte del mensaje ICMP): 528 bytes

Victoria Ruiz Schulze
Curso: K4573
Entrega: 7/11/2022

f) ¿Qué valor de tamaño de paquete tiene el umbral de fragmentación? ¿es constante o variable?
El tamaño de fragmentación es constante y corresponde al MTU de la red, que es 1500 bytes.

4) Calcule un valor umbral de Bytes, que deben ser configurados como parámetro en la aplicación Ping, para que el datagrama IP se fragmente en 15 paquetes. Verifíquelo en la PC.
El datagrama IP tiene espacio para 1480 bytes de mensaje ICMP.
Largo del mensaje ICMP completo para ocupar 14 paquetes: 14 * 1480 = 20720 bytes.
Largo mínimo del mensaje ICMP completo para ocupar 15 paquetes: 14 * 1480 + 1 = 20721 bytes.
Parametro de datos de ping = 20721 bytes - 8 bytes correspondientes a la cabecera ICMP. Total: 20713 bytes.
Esto fue confirmado en Wireshark.