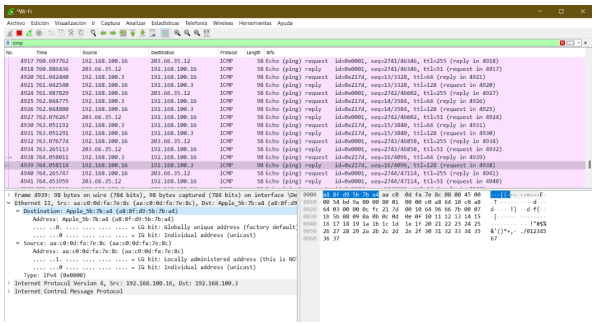
# 3.7.10-lab---use-wireshark-to-view-network-traffic_es-XL

viernes, 23 de junio de 2023 20:35

3.7.10-lab-

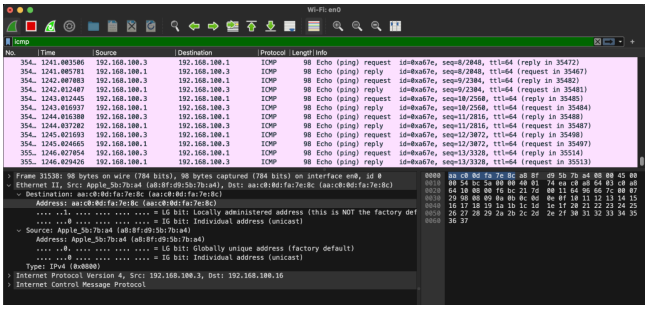
--use-



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : AA-C0-0D-FA-7E-8C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2806:2f0:99c1:fccf::10(Preferred)
   Lease Obtained. . . . . . . . . . : viernes, 23 de junio de 2023 08:49:01 p. m.
   Lease Expires . . . . . . . . . . : lunes, 26 de junio de 2023 08:41:42 p. m.
   IPv6 Address. . . . . . . . . . . : 2806:2f0:99c1:fccf:d98d:5ffd:2dbc:39e5(Preferred)
   Temporary IPv6 Address. . . . . . : 2806:2f0:99c1:fccf:38a7:21bf:7a32:cba1(Preferred)
   Link-local IPv6 Address . . . . . : fe80::ca91:9aa8:c6ea:5fe0%25(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.16(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : viernes, 23 de junio de 2023 08:48:59 p. m.
   Lease Expires . . . . . . . . . . : sábado, 24 de junio de 2023 08:48:58 p. m.
   Default Gateway . . . . . . . . . : fe80::1%25
                                       192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 436620685
   DHCPv6 Client DUID. . . . . . . . : 00-03-00-01-AA-C0-0D-FA-7E-8C
   DNS Servers . . . . . . . . . . . : 2806:2f0:91::13
                                       2001:4860:4860::8888
                                       192.168.100.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 5:
```



```
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether a8:8f:d9:5b:7b:a4
        inet6 fe80::8db:7ba6:79f3:b84%en0 prefixlen 64 secured scopeid 0xc
        inet 192.168.100.3 netmask 0xffffff00 broadcast 192.168.100.255
        inet6 2806:2f0:99c1:fccf:14e0:92a0:c686:6f4f prefixlen 64 autoconf secured
        inet6 2806:2f0:99c1:fccf:83:3921:2b94:a99b prefixlen 64 autoconf temporary
        inet6 2806:2f0:99c1:fccf::2 prefixlen 64 dynamic
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

```
kikin@Macbook-Air-03 ~ % arp -a
? (192.168.100.1) at 6c:d7:19:c8:90:78 on en0 ifscope [ethernet]
? (192.168.100.2) at 96:ab:36:20:11:8e on en0 ifscope [ethernet]
? (192.168.100.16) at aa:c0:d:fa:7e:8c on en0 ifscope [ethernet]
? (192.168.100.19) at 6e:a4:a4:98:ef:25 on en0 ifscope [ethernet]
? (192.168.100.24) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.47) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.48) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.68) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.70) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.71) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.75) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.78) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.83) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.95) at (incomplete) on en0 ifscope [ethernet]
? (192.168.100.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
kikin@Macbook-Air-03 ~ %
```

```
kikin@Macbook-Air-03 ~ % ifconfig | grep "inet " | grep -v 127.0.0.1
        inet 192.168.100.3 netmask 0xffffff00 broadcast 192.168.100.255
kikin@Macbook-Air-03 ~ %
```

```
kikin@Macbook-Air-03 ~ % ping www.yahoo.com
PING new-fp-shed.wg1.b.yahoo.com (74.6.231.20): 56 data bytes
64 bytes from 74.6.231.20: icmp_seq=0 ttl=51 time=64.687 ms
64 bytes from 74.6.231.20: icmp_seq=1 ttl=51 time=68.924 ms
64 bytes from 74.6.231.20: icmp_seq=2 ttl=51 time=65.138 ms
64 bytes from 74.6.231.20: icmp_seq=3 ttl=51 time=66.926 ms
64 bytes from 74.6.231.20: icmp_seq=4 ttl=51 time=63.491 ms
64 bytes from 74.6.231.20: icmp_seq=5 ttl=51 time=67.108 ms
64 bytes from 74.6.231.20: icmp_seq=6 ttl=51 time=63.182 ms
^C
--- new-fp-shed.wg1.b.yahoo.com ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 63.182/65.637/68.924/1.943 ms
kikin@Macbook-Air-03 ~ % ping www.cisco.com
PING e2867.dsca.akamaiedge.net (23.33.109.84): 56 data bytes
64 bytes from 23.33.109.84: icmp_seq=0 ttl=56 time=6.023 ms
64 bytes from 23.33.109.84: icmp_seq=1 ttl=56 time=9.397 ms
64 bytes from 23.33.109.84: icmp_seq=2 ttl=56 time=8.135 ms
64 bytes from 23.33.109.84: icmp_seq=3 ttl=56 time=6.321 ms
64 bytes from 23.33.109.84: icmp_seq=4 ttl=56 time=6.022 ms
^C
--- e2867.dsca.akamaiedge.net ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.022/7.180/9.397/1.360 ms
kikin@Macbook-Air-03 ~ % ping www.google.com
PING www.google.com (142.251.35.4): 56 data bytes
64 bytes from 142.251.35.4: icmp_seq=0 ttl=59 time=8.705 ms
64 bytes from 142.251.35.4: icmp_seq=1 ttl=59 time=11.382 ms
64 bytes from 142.251.35.4: icmp_seq=2 ttl=59 time=8.802 ms
64 bytes from 142.251.35.4: icmp_seq=3 ttl=59 time=10.149 ms
64 bytes from 142.251.35.4: icmp_seq=4 ttl=59 time=10.634 ms
64 bytes from 142.251.35.4: icmp_seq=5 ttl=59 time=12.043 ms
64 bytes from 142.251.35.4: icmp_seq=6 ttl=59 time=9.175 ms
64 bytes from 142.251.35.4: icmp_seq=7 ttl=59 time=11.872 ms
^C
--- www.google.com ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.705/10.345/12.043/1.267 ms
kikin@Macbook-Air-03 ~ %
```

Networking Academy

**Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red**

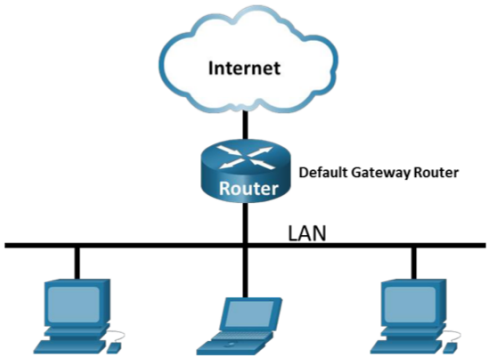
**Topología**

**Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red**

**Instrucciones**

**Parte 1: Captura y análisis de datos ICMP locales en Wireshark**

En la parte 1 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solici respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados d transmitir datos al destino.




## Objetivos

**Parte 1: Capturar y analizar datos ICMP locales en Wireshark**

**Parte 2: Capturar y analizar datos ICMP remotos en Wireshark**

## Información básica/situación

Wireshark es un analizador de protocolos de software o una aplicación "husmeador de paquetes" que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolo y software y educación. Mientras el flujo de datos va y viene en la red, el husmeador "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos de CCNA para el análisis de datos y la solución de problemas. En esta práctica de laboratorio, usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

## Recursos necesarios

- 1 PC (Windows con acceso a internet)
- Se utilizarán PC adicionales en una red de área local (LAN) para responder a las solicitudes de ping.





### Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección físi de interfaz de red (NIC), que también se conoce como "dirección MAC".

a. En una ventana del símbolo del sistema, ingrese **ipconfig /all**, a la dirección IP de la inte su descripción y su dirección MAC (física).

```
C:\Users\Student> ipconfig /all

Configuración IP de Windows

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adaptador Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network C
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .: fe80: :d809:d 939:110 f:1b7f%20 (Pr
   IPv4 Address. . . . . . . . . . . : 192.168.1.147 (Preferido)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

b. Solicite a un miembro o a los miembros del equipo la dirección IP de su PC y proporción esta instancia, no proporcione su dirección MAC.

### Paso 2: Inicie Wireshark y comiene a capturar datos

a. Navegue a Wireshark. Haga doble clic en la interfaz deseada para iniciar la captura de p Asegúrese de que la interfaz deseada tenga tráfico.

b. La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las aparecen en diferentes colores según el protocolo.

Es posible desplazarse muy rápidamente por esta información según la comunicación qu entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los d Wireshark.






Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro **Filter** en la parte superior de Wireshark y presione **Enter,** o haga clic en el botón **Apply** (signo de flecha) para ver solo las PDU ICMP (ping).

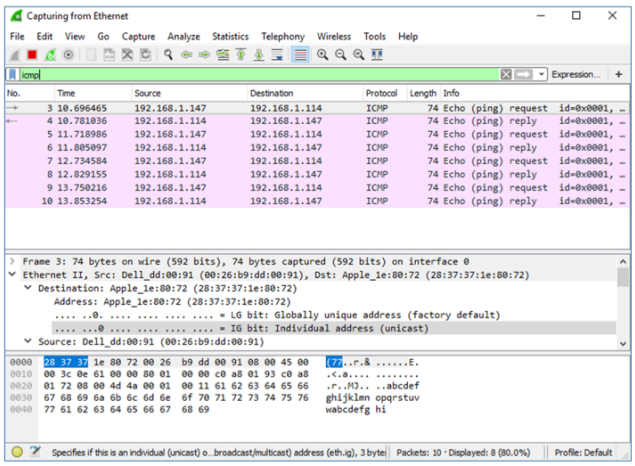
c. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Navegue a la ventana del símbolo del sistema y haga ping a la dirección IP que recibió de un miembro de su equipo.

```
C:\ > ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.










**Nota**: Si la PC del miembro de su equipo no responde a sus pings, es posible que el firew miembro del equipo bloquee estas solicitudes. Consulte Apéndice A: Permitir el tráfico ICM un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firew Windows.

d. Detenga la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).

### Paso 3: Examine los datos capturados

En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC d equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) l media indica información de la PDU para la trama seleccionada en la parte superior de la pant una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los d procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decim

a. Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior d Observe que la columna **Source** contiene la dirección IP de su PC y la columna **Destinati** dirección IP de la PC del compañero de equipo a la que hizo ping.

b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la secció clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direccione origen y destino.

¿La dirección MAC de origen coincide con la interfaz de su PC?

**Si**

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del compañero

**Si**

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

**Nota**: En el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encap de una PDU del paquete IPv4 (encabezado de IPv4), que luego se encapsula en una PDU Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

## Parte 2: Capture y analice datos ICMP remotos en Wireshark

En la parte 2, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los d a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examir parte 1.

### Paso 1: Comience a capturar datos en la interfaz

a. Vuelva a iniciar la captura de datos.

b. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving**

c. Con la captura activa, haga ping a las siguientes tres URL de sitios web desde un símbolo Windows:

1) www.yahoo.com
2) www.cisco.com






3) www.google.com

**Nota**: Cuando haga ping a las URL enumeradas, observe que el servidor de nombres de dominio (DNS) traduce la URL a una dirección IP. Observe la dirección IP recibida para cada URL.

d. Puede detener la captura de datos haciendo clic en el ícono **Stop Capture**.

### Paso 2: Inspeccione y analice los datos de los hosts remotos

Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las tres ubicaciones a las que hizo ping. Indique las direcciones IP y MAC de destino para las tres ubicaciones en el espacio proporcionado.

Dirección IP de **www.yahoo.com**:

74. 6.231.20

Dirección MAC para **www.yahoo.com**:

6C : d7:19: c8: 90 : 78

Dirección IP para **www.cisco.com**:

23.33.69.84

Dirección MAC para **www.cisco.com**:

6C: d7:19: c8:90:78

Dirección IP de **www.google.com**:

142.251. 5.4

Dirección MAC para **www.google.com**: 6C: d7:19:c8:90:78

¿Qué es importante sobre esta información?

tenemos IPV4 distintas, pero la MAC es la misma por ser la MAC del gateway

¿En qué se diferencia esta información de la información de ping local que recibió en la parte 1?

IP local: puedes obtener su MAC exacta
IP remota: MAC del gateway

### Pregunta de reflexión

¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

No es posible conocer las MAC remota, pero sí la del último gateway q se pasa.

### Apéndice A: Permitir el tráfico ICMP a través de un firewall

Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio.

### Parte 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

a. Navegue hasta el **Control Panel** y haga clic en la opción **System and Security** en la categoría view.

b. En la ventana **System and Security**, haga clic en **Windows Defender Firewall** o **Windows Firewall**.




c. En el panel izquierdo de la ventana **Windows Defender Firewall** o **Windows Firewall** ha **Advanced settings**.

d. En la ventana de **Advanced Security** haga clic en la opción **Inbound Rules** en la barra la y luego haga clic en **New Rule…** en la barra lateral derecha.

e. Se inicia el asistente **New Inbound Rule** En la pantalla **Rule Type** haga clic en el boton clic en **Next**.

f. En el panel izquierdo, haga clic en la opción **Protocol and Ports** y, en el menú desplegab **Type**, seleccione **ICMPv4**; luego, haga clic en **Next**.

g. Compruebe que se ha seleccionado **Cualquier dirección IP** para las direcciones IP locale Haga clic en **Next** para continuar.

h. Seleccione **Allow the connection**. Haga clic en **Next** para continuar.

i. De forma predeterminada, esta regla se aplica a todos los perfiles. Haga clic en **Next** para

j. Nombre la regla con **Allow ICMP Requests**. Haga clic en **Finish** para continuar. Esta nue permitir que los miembros del equipo reciban respuestas de ping de su PC.

### Parte 2: Deshabilite o elimine la nueva regla ICMP.

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso elin regla que creó en el paso 1. La opción **Disable Rule** le permite volver a habilitar la regla en ur posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de reglas de entrad

a. En la ventana de **Advanced Security**, haga clic en **Inbound Rules** en el panel izquierdo la regla que creó anteriormente.

b. Haga clic con el botón derecho en la regla ICMP y seleccione **Disable Rule** si así lo desea puede seleccionar **Delete** si desea eliminarlo permanentemente. Si elige esta opción, debe crear la regla para permitir las respuestas de ICMP.