

Escuela Colombiana de Ingeniería Julio Garavito

Laboratorio # 3: Plataforma base y capa de enlace

Juan Sebastián Frásica Galeano

Redes de Computadores

Profesora: Ing. Claudia Patricia Santiago Cely

Introducción:

En este laboratorio se analizará en detalle y de forma práctica algunas de las funciones que realiza la capa de enlace, como el control de flujo, el control de errores, etc.

Se va a conocer el modo de operación de las herramientas de redes, como Packet Tracer y análisis de tráfico de red como Wireshark. También se va a revisar la forma en la que opera el protocolo Ethernet en esta capa, viendo así su frame y toda su estructura.

Y finalmente aprender programación básica en el Shell de Linux.

Marco teórico:

Ethernet: Red de transmisión basada en topología bus o estrella con control de operación descentralizado. Está compuesto por:

- Frame.
- Protocolo de acceso al medio.
- Componentes de señalización.
- Medio físico.

En el subnivel MAC comprende:

- a. Especificaciones de Servicio MAC.
- b. Protocolos y unidades de datos (estructura del paquete y control de acceso al medio).

En el nivel físico:

- a. Especificaciones de servicio.
- b. Especificaciones del nivel físico.

Su método de operación es CSMA/CD y 1-persistent, es decir, es posible que los dispositivos escuchen la red para determinar si el canal y los recursos se encuentran libres. En caso afirmativo, se podrá realizar la transmisión para no colisionar con otros paquetes.

Cuando se habla de la capa de enlace, se debe nombrar a los bridges, hubs y switches, siendo estos últimos los más relevantes hoy en día.

Bridges: Son equipos que conectan distintos tipos de red, específicamente conectan redes con distintos protocolos o modos de acceso al medio. Los bridges conectan segmentos de red, nombre que se le da a cada red o porción de red conectada.



Hubs: Son equipos que actúan en topología bus, es decir, propagan la transmisión por todas sus salidas. Regeneran las señales que les llegan, por lo que son útiles en conexiones de grandes distancias. No segmentan las redes ni realizan procesos muy complejos.



Switches: Estos equipos desplazaron a los dos equipos anteriores ya que desempeñan las mismas funciones y las mejoran. Los switches, al igual que los hubs, pueden regenerar la señal, pero adicionalmente pueden enviar la señal como bus y también enviarla por salidas específicas, esto agrega eficiencia a la red. Adicionalmente segmenta las redes disminuyendo los dominios de colisión, función sumamente importante.



Desarrollo del tema:

Simulaciones

1. Conociendo Packet Tracer

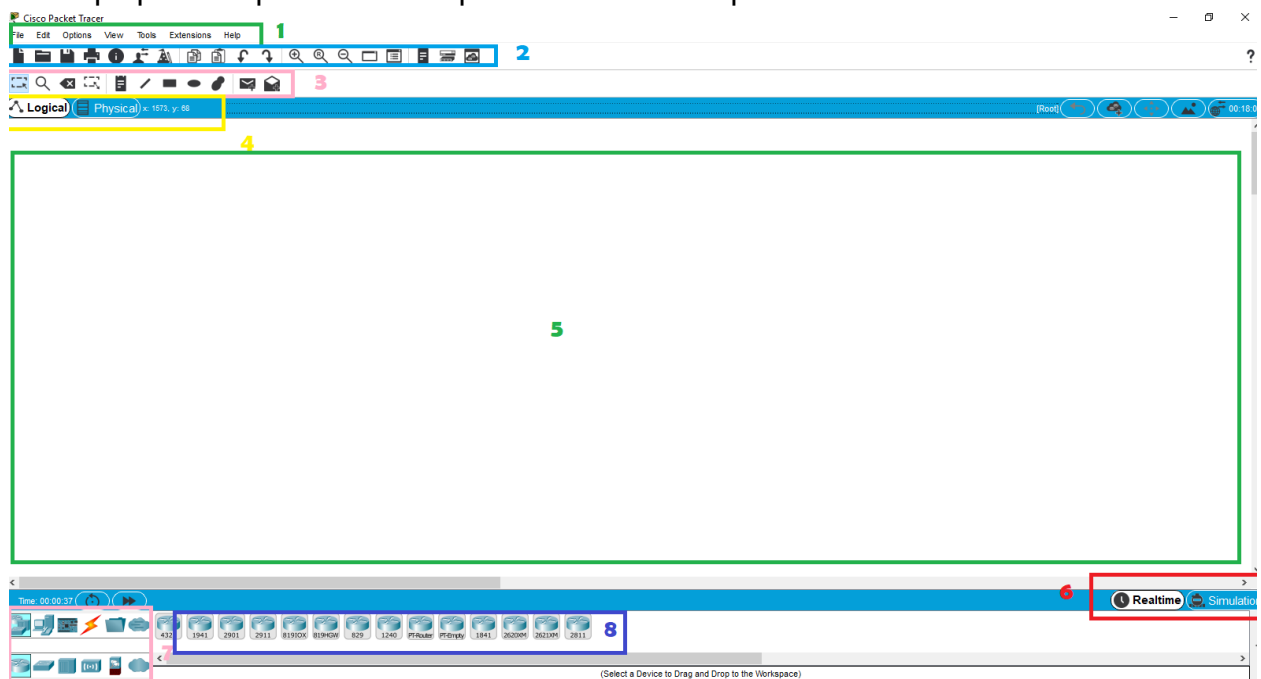
Responda las siguientes preguntas

1. ¿Qué es Packet Tracer?

Es una herramienta que permite la simulación de redes. Permite crear tipologías de red, simular una red con múltiples representaciones visuales, principalmente es una herramienta de apoyo didáctico.

Permite crear redes con un número casi ilimitado de dispositivos y experiencias de solución de problemas sin tener que comprar routers o switches reales.

2. Expliquen las partes en las que está dividida la pantalla de Packet Tracer.



- La parte 1 corresponde a la barra de menú, la cual contiene comandos básicos.
- En la parte 2 se encuentran las herramientas más usadas como guardar, copiar, undo, redo, zoom, imprimir, etc.
- En la parte 3 se encuentran otras herramientas utilizadas, pero con más detalle como buscar, seleccionar, eliminar, etc.
- En la parte 4 podemos alternar entre la topología lógica y física de la red.
- En la parte 5 es donde se desarrolla toda la red.

- En la sección 6 podemos alternar entre los modos de operación que tiene Packet Tracer: real time y simulation.
 - En la parte 7 se encuentran los dispositivos que se pueden utilizar en la red. En esta sección podemos escoger en términos generales el tipo de dispositivo que deseamos usar.
 - En la sección 8 están los dispositivos en detalle con su respectivo nombre.
3. Para qué sirven los siguientes modos de Packet Tracer:
 - “real time”: sirve para mostrar la estructura de la red y su topología. Ahí se ponen visibles los computadores, routers, y demás dispositivos con su respectivo nombre y sus conexiones.
 - “Simulation”: Sirve para mostrar la ejecución de la red después de que esta ya está estructurada y configurada, es como una representación de la realidad de esa red plasmada en pantalla. Se puede pausar cuando se requiera, y muestra información mas detallada de la red.
 4. Explique los grupos de dispositivos que pueden ser usados dentro del simulador (Pista: estos elementos se encuentran en el bloque inferior izquierdo de la ventana del simulador).

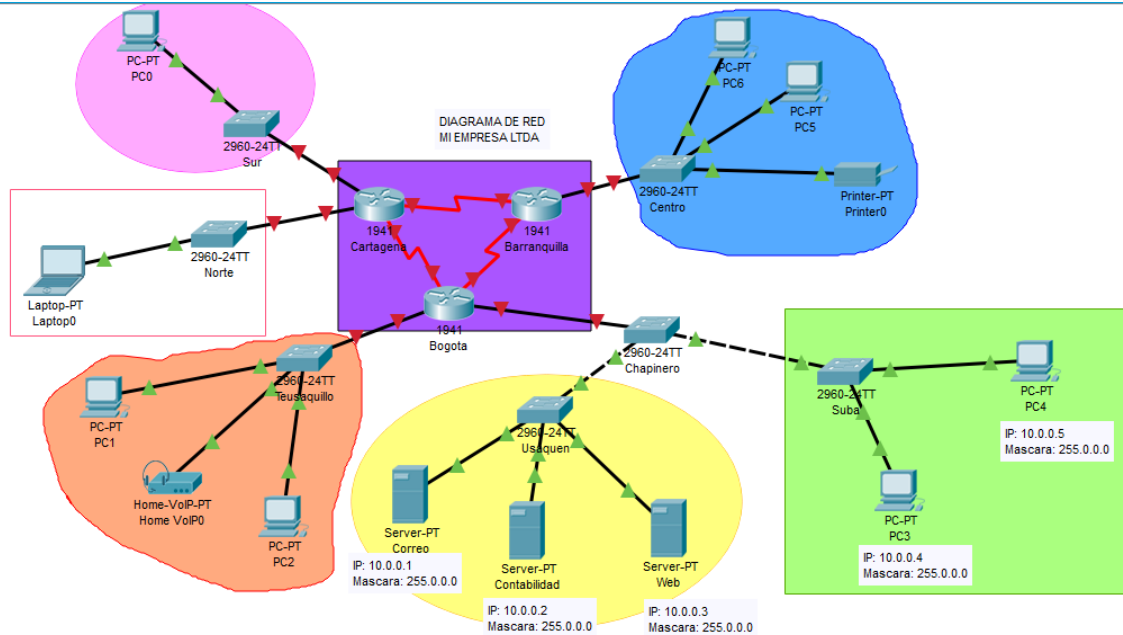
En Packet Tracer hay 6 grupos de dispositivos:

- Dispositivos de red: routers, switches, hubs, dispositivos inalámbricos, seguridad y emulación WAN.
- Dispositivos finales: dispositivos que finales como PC's, servidores, impresoras, etc. Estos dispositivos se pueden conectar desde casas, ciudades inteligentes, zonas industriales y redes eléctricas.
- Componentes: Tarjetas, actuadores y sensores.
- Conexiones y cableado estructurado.
- Misceláneas.
- Conexión multiusuario.

Usando Packet Tracer haga el diagrama de red que se presenta en la página siguiente.
Nota:

- No tenga en cuenta los puntos de colores que aparecen en las puntas de los enlaces (los enlaces son las líneas de conexión entre dispositivos. Más adelante serán importantes los colores de dichos puntos, pero en su momento los revisaremos.
- Las conexiones o enlaces que se presentan en el diagrama son:
 - Las de color negro corresponden a cables Ethernet (Ethernet, FastEthernet o GigaEthernet).

- ¿Qué significan las conexiones negras continuas?
Representa cableado directo.
- ¿Qué significan las conexiones negras discontinuas?
Representa cableado cruzado.
- Las de color rojo son seriales (Conexiones típicamente WAN)



2. Siguiendo mensajes con Packet Tracer

- Configure las direcciones IP y máscara de los computadores del recuadro verde y servidores del recuadro amarillo.

Physical **Config** Services Desktop Programming Attributes

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00E0.A321.4B78
IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
IPv6 Configuration	
<input type="radio"/> DHCP	
<input type="radio"/> Auto Config	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address:	FE80::2E0:A3FF:FE21:4B78

Physical **Config** Services Desktop Programming Attributes

GLOBAL	
Settings	
Algorithm Settings	
INTERFACE	
FastEthernet0	

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0090.2170.0B55
IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
IPv6 Configuration	
<input type="radio"/> DHCP	
<input type="radio"/> Auto Config	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address:	FE80::290:21FF:FE70:B55

Physical **Config** Services Desktop Programming Attributes

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0060.70C9.37DC
IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IP Address	10.0.0.3
Subnet Mask	255.0.0.0
IPv6 Configuration	
<input type="radio"/> DHCP	
<input type="radio"/> Auto Config	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address:	FE80::260:70FF:FE09:37DC

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.97C8.9205

IP Configuration

☐ DHCP

☒ Static

IP Address 10.0.0.4

Subnet Mask 255.0.0.0

IPv6 Configuration

☐ DHCP

☐ Auto Config

☒ Static

IPv6 Address

Link Local Address: FE80::2D0:97FF:FE80:9205

☐ Top

PC4

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.58C4.C274

IP Configuration

☐ DHCP

☒ Static

IP Address 10.0.0.5

Subnet Mask 255.0.0.0

IPv6 Configuration

☐ DHCP

☐ Auto Config

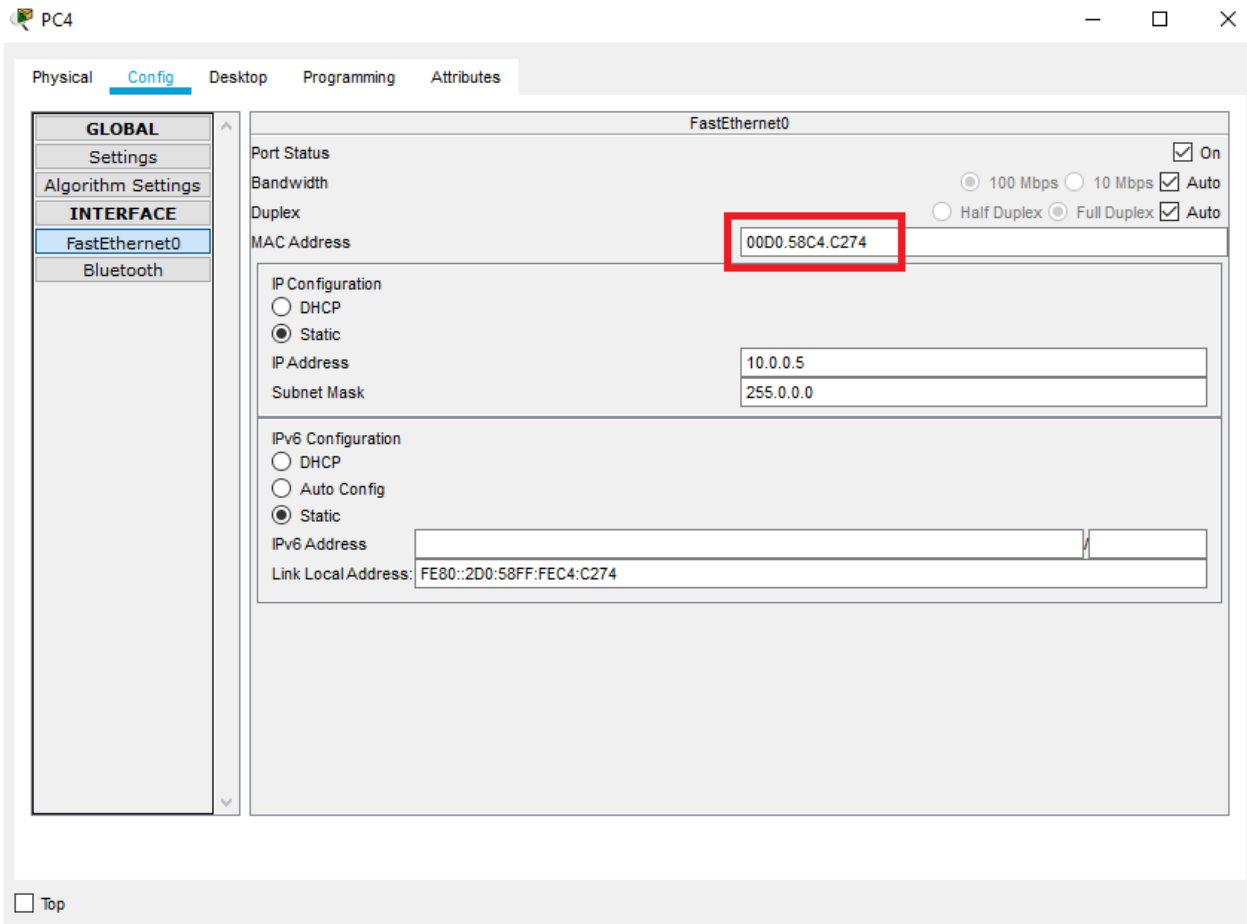
☒ Static

IPv6 Address

Link Local Address: FE80::2D0:58FF:FEC4:C274

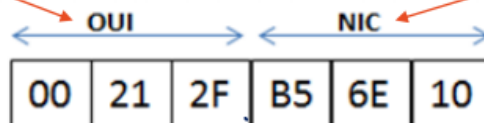
☐ Top

- Identifique la tarjeta de red del computador PC4. Indique dirección MAC
Es una dirección MAC de tipo EUI-48



Organizationally Unique Identifier

Network Interface Controller



EUI-48

- Usando el comando ping en la línea de comandos y el ambiente gráfico del simulador, verifique conectividad entre los 5 equipos.

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=128
Reply from 10.0.0.1: bytes=32 time=1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=3ms TTL=128
Reply from 10.0.0.2: bytes=32 time=3ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

```
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```

C:\>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.0.5

Pinging 10.0.0.5 with 32 bytes of data:

Reply from 10.0.0.5: bytes=32 time=5ms TTL=128
Reply from 10.0.0.5: bytes=32 time=1ms TTL=128
Reply from 10.0.0.5: bytes=32 time=3ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms

```

- Entre en el modo simulación con que cuenta Packet Tracer y revise los frames Ethernet. Para esto use la siguiente información como guía

Run the simulation and capture the traffic¹.

- In the far lower right of the PT interface is the toggle between Realtime and Simulation mode. Click on Simulation mode.
- Click in the Edit filters button and select only ICMP.
- Click the PC3. Choose the Desktop tab. Open the Command Prompt. Enter the command ping 10.0.0.2, the IP address of the server contabilidad. Pressing the Enter key will initiate four ICMP echo requests. Minimize the PC configuration window. Two packets appear in the Event List, the first ICMP echo request and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
- Click the Auto Capture / Play button to run the simulation and capture events. Click OK when the "No More Events" message is reached.

PacketTracer7

IPv4 IPv6 Misc

☐ ARP ☐ BGP ☐ DHCP

☐ DNS ☐ EIGRP ☐ HSRP

☒ ICMP ☐ OSPF ☐ RIP

Edit ACL Filters

Printer-PT
Printer0

PC-PT
PC4
IP: 10.0.0.5
Mascara: 255.0.0.0

PC-PT
PC3
IP: 10.0.0.4
Mascara: 255.0.0.0

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type

Reset Simulation ☒ Constant Delay Captured to: (no captures)

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=16ms TTL=128
Reply from 10.0.0.2: bytes=32 time=8ms TTL=128
Reply from 10.0.0.2: bytes=32 time=8ms TTL=128
Reply from 10.0.0.2: bytes=32 time=8ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 16ms, Average = 10ms

C:\>

```

The screenshot displays a network simulation interface. On the left, a window titled "PDU Information at Device: Usaquen" shows the OSI model details for an inbound packet. The packet is from PC3 (10.0.0.2) to PC4 (10.0.0.5). The layers are listed as follows:

In Layers	Out Layers
Layer 7	Layer 7
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4	Layer 4
Layer 3	Layer 3
Layer 2: Ethernet II Header 00D0.97C8.9205 >> 0090.2170.0B55	Layer 2: Ethernet II Header 00D0.97C8.9205 >> 0090.2170.0B55
Layer 1: Port FastEthernet0/4	Layer 1: Port(s): FastEthernet0/2

Below the layers, it states: "1. FastEthernet0/4 receives the frame." The interface also shows a "Simulation Panel" on the right with an "Event List" table:

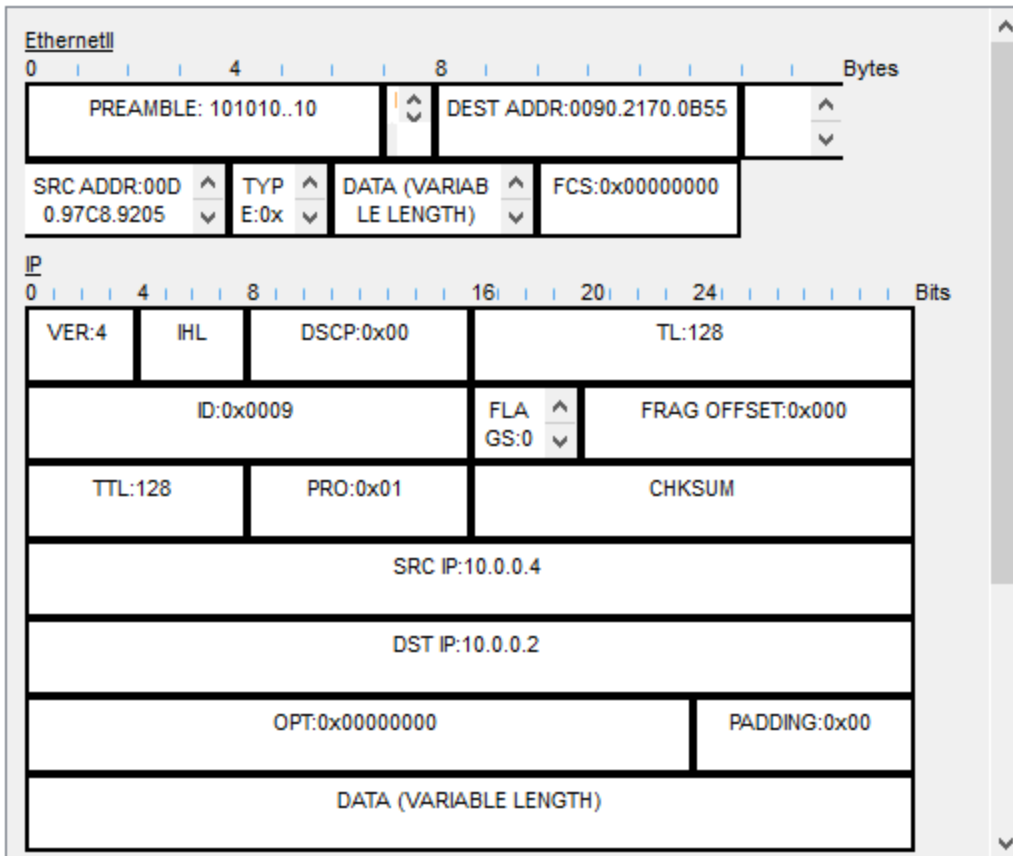
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC3	ICMP
	0.001	PC3	Suba	ICMP
	0.002	Suba	Chapinero	ICMP
	0.003	Chapinero	Usaquen	ICMP
	0.004	Usaquen	Contabilidad	ICMP
	0.005	Contabilidad	Usaquen	ICMP
	0.006	Usaquen	Chapinero	ICMP
	0.007	Chapinero	Suba	ICMP
	0.008	Suba	PC3	ICMP
	0.976	--	Teusaquillo	STP
	0.977	Teusaquillo	PC1	STP
	0.977	Teusaquillo	Home VoIP0	STP
	0.977	Teusaquillo	PC2	STP
	0.986	--	Centro	STP
	0.987	Centro	Printer0	STP
	0.987	Centro	PC5	STP
	0.987	Centro	PC6	STP

The interface also includes a "Simulation Panel" with "Play Controls" and "Event List Filters - Visible Events" (ACL Filter, Bluetooth, CAPWAP, CDP, DHCPv6, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REI, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP).

Se aprecia el funcionamiento de la capa física y la capa de enlace (específicamente en Ethernet) siguiendo el modelo OSI.

- Revise el contenido de los paquetes capturados. Revise el contenido del encabezado Ethernet.

PDU Formats



Acá se puede apreciar el detalle del frame de Ethernet.

Montaje real

1. Usando Wireshark

Wireshark es una herramienta multiplataforma utilizada para realizar análisis sobre paquetes de red. La utilizaremos dentro del curso para observar, en tiempo real, lo datos que pasan por la red y la manera de operación de los diferentes protocolos que estudiaremos. Por tal razón:

- Ejecute Wireshark en el computador en el que está trabajando
- Revise los siguientes videos
 - Wireshark Tutorial for Beginners.
<https://www.youtube.com/watch?v=TkCSr30UojM>.
 - Wireshark Tutorial for Beginners 2017 - Overview of the environment.

<https://www.youtube.com/watch?v=6LGw31TsP6E>.

- Wireshark demo (simple http).

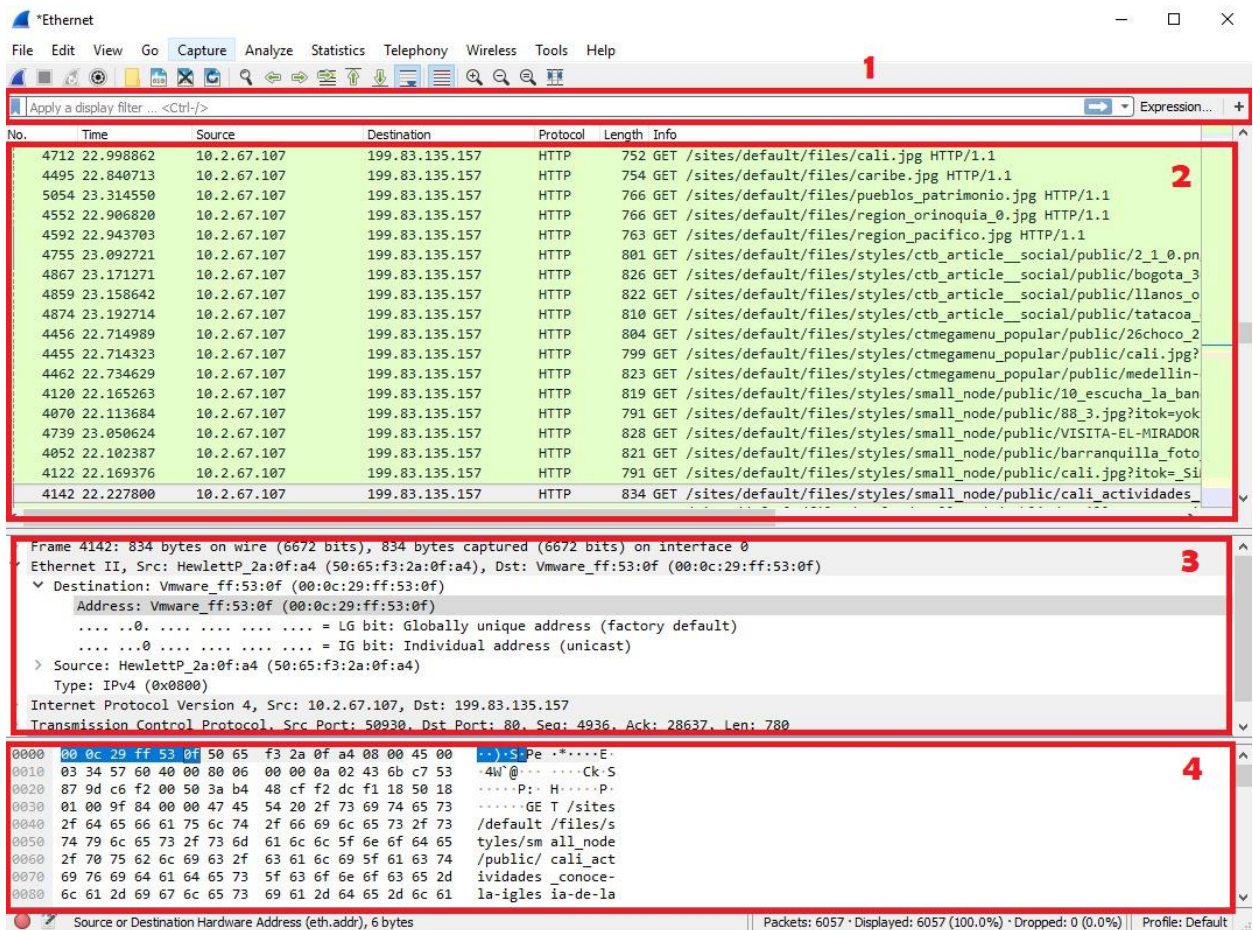
<https://www.youtube.com/watch?v=PYoXowOCppc>.

- ¿Qué es Wireshark?, describa las áreas en las que está dividida la interface gráfica de captura y análisis de tráfico.

Es un software gratuito que permite analizar el tráfico red en tiempo real. La herramienta intercepta el tráfico y lo convierte en un formato legible para las personas. Esto hace que sea más fácil identificar qué tráfico está cruzando la red, con qué frecuencia y la latencia que hay entre ciertos saltos.

La mayoría de los paquetes son TCP, UDP e ICMP.

Dado el gran volumen de tráfico que atraviesa una red comercial típica, las utilidades de Wireshark ayudan a filtrarlo. Los filtros de captura solo recopilan los tipos de tráfico que le interesan al comercio y los de visualización le ayudan a acercarse al tráfico que quiere inspeccionar. El analizador de protocolo de red proporciona herramientas de búsqueda, que incluyen expresiones regulares y resaltado en color, para que sea más fácil encontrar lo que se está buscando.



La sección 1 es el área de definición de filtros y permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que se requieran.

La sección 2 corresponde a la lista de visualización de todos los paquetes que se están capturando en tiempo real.

La sección 3 permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en la sección 2.

Por último, la sección 4 representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por la tarjeta de red.

- ¿Qué tipo de opciones de filtrado tiene?, ¿cómo se usan?

Los filtros de captura (Capture Filter) son los que se establecen para mostrar solo los paquetes de cumplan los requisitos indicados en el filtro.

Se aplican en Capture > Options

En el campo Capture Filter introducimos el filtro o pulsamos el botón Capture Filter para filtros predefinidos

Podemos combinar las primitivas de los filtros de la siguiente forma:

- Negación: **!** ó **not**
- Unión o Concatenación: **&&** ó **and**
- Alternancia: **||** ó **or**

Vamos ahora a los filtros:

Filtros basados en hosts	
Sintaxis	Significado
host host	Filtrar por host
src host host	Capturar por host origen
dst host host	Capturar por host destino
Ejemplos	
host 192.168.1.20	Captura todos los paquetes con origen y destino 192.168.1.20
src host 192.168.1.1	Captura todos los paquetes con origen en host 192.168.1.1
dst host 192.168.1.1	Captura todos los paquetes con destino en host 192.168.1.1
dst host SERVER-1	Captura todos los paquetes con destino en host SERVER-1
host http://www.terra.com	Captura todos los paquetes con origen y destino http://www.terra.com
Filtros basados en puertos	
Sintaxis	Significado
port port	Captura todos los paquetes con puerto origen y destino port
src port port	Captura todos los paquetes con puerto origen port
dst port port	Captura todos los paquetes con puerto destino port
not port port	Captura todos los paquetes excepto origen y destino puerto port
not port port and not port port1	Captura todos los paquetes excepto origen y destino puertos port y port1
Ejemplos	
port 21	Captura todos los paquetes con puerto origen y destino 21
src port 21	Captura todos los paquetes con puerto origen 21

not port 21 and not port 80	Captura todos los paquetes excepto origen y destino puertos 21 y 80
portrange 1-1024	Captura todos los paquetes con puerto origen y destino en un rango de puertos 1 a 1024
dst portrange 1-1024	Captura todos los paquetes con puerto destino en un rango de puertos 1 a 1024

Filtros basados en protocolos Ethernet / IP

Ejemplos

ip	Captura todo el tráfico IP
ip proto \tcp	Captura todos los segmentos TCP
ether proto \ip	Captura todo el tráfico IP
ip proto \arp	Captura todo el tráfico ARP

Filtros basados en red

Sintaxis	Significado
net net	Captura todo el tráfico con origen y destino red net
dst net net	Captura todo el tráfico con destino red net
src net net	Captura todo el tráfico con origen red net

Ejemplos

net 192.168.1.0	Captura todo el tráfico con origen y destino subred 1.0
net 192.168.1.0/24	Captura todo el tráfico para la subred 1.0 mascara 255.0
dst net 192.168.2.0	Captura todo el tráfico con destino para la subred 2.0
net 192.168.2.0 and port 21	Captura todo el tráfico origen y destino puerto 21 en subred 2.0
broadcast	Captura solo el tráfico broadcast
not broadcast and not multicast	Captura todo el tráfico excepto el broadcast y el multicast

Los filtros de visualización (Display Filer) establecen un criterio de filtro sobre los paquetes capturados y que estamos visualizando en la pantalla principal de Wireshark. Estos filtros son más flexibles y potentes.

Comparando Filtros.

- Igual a: **eq** ó **==**
- No igual: **ne** ó **!=**

- Mayor que: **gt** ó **>**
- Menor que: **lt** ó **<**
- Mayor o igual: **ge** ó **>=**
- Menor o igual: **le** ó **<=**

Combinando Filtros.

- Negación: **!** ó **not**
- Unión o Concatenación: **&&** ó **and**
- Alternancia: **||** ó **or**

Si queremos aplicar otro filtro pulsamos el botón **Clear**, introducimos el filtro y pulsamos **Apply**.

Ejemplos de filtros:

Filtros de visualización	
Sintaxis	Ejemplos
ip.addr == 192.168.1.40	Visualizar tráfico por host 192.168.1.40
ip.addr != 192.168.1.25	Visualizar todo el tráfico excepto host 192.168.1.25
ip.dst == 192.168.1.30	Visualizar por host destino 192.168.1.30
ip.src == 192.168.1.30	Visualizar por host origen 192.168.1.30
ip	Visualiza todo el tráfico IP
tcp.port == 143	Visualiza todo el tráfico origen y destino puerto 143
ip.addr == 192.168.1.30 and tcp.port == 143	Visualiza todo el tráfico origen y destino puerto 143 relativo al host 192.168.1.30
http contains "http://www.terra.com"	Visualiza el tráfico origen y destino http://www.terra.com . Visualiza los paquetes que contienen http://www.terra.com en el contenido en protocolo http.
frame contains "@miempresa.es"	Visualizamos todos los correos con origen y destino al dominio miempresa.es , incluyendo usuarios , pass , etc
icmp[0:1] == 08	Filtro avanzado con el que visualizamos todo el tráfico icmp de tipo echo request
ip.ttl == 1	Visualiza todos los paquetes IP cuyo campo TTL sea igual a 1
tcp.window_size != 0	Visualizar todos los paquetes cuyos campos Tamaño de Ventana del segmento TCP sea distinto de 0

ip.tos == x

Visualiza todos los paquetes IP cuyo campo TOS sea igual a x

ip.flags.df == x

Visualiza todos los paquetes IP cuyo campo DF sea igual a x

udp.port == 53

Visualiza todo el tráfico UDP puerto 53

tcp contains "terra.com"

Visualizamos segmentos TCP conteniendo la cadena terra.com

- Realice una consulta web al link <http://www.colombia.travel/> y capture el tráfico generado (para eso, ingrese al browser, inicie la captura con Wireshark y visite a la página indicada, termine la captura).
- Pare la captura
- Analice los datos encontrados (sólo revise los datos de la capa de enlace, es decir, revise el encabezado y datos generados a este nivel. Para facilitar la búsqueda, encuentre un paquete que contiene una de las solicitudes GET que se realizan).

Wireshark interface showing a packet capture on the Ethernet interface. The packet list shows several HTTP GET requests to the Colombia Travel website. The selected packet (No. 374) is an HTTP GET request to /live/red_lojson/300lo.json. The packet details pane shows the structure of the HTTP request, including the status bar at the bottom indicating 1099 bytes captured on interface 0.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
62	2.151704	Cisco_f8:91:06	CDP/VTP/DTP/PAGP/UD...	DTP	90	Dynamic Trunk Protocol
623	6.261708	205.180.87.204	10.2.67.106	TLSv1.2	85	Encrypted Alert
647	6.518188	205.180.87.204	10.2.67.106	TLSv1.2	85	Encrypted Alert
672	6.844064	23.7.144.218	10.2.67.106	TLSv1.2	85	Encrypted Alert
87	3.931870	Avaya_f3:2c:00	Nortel-autodiscovery	NDP	60	FlatNet Hello
556	5.581799	10.2.67.106	156.154.136.36	HTTP	784	GET /adscores/g.pixel?sid=92
107	4.138675	10.2.67.106	199.83.135.157	HTTP	762	GET /en HTTP/1.1
496	5.185833	10.2.67.106	68.67.179.228	HTTP	550	GET /getuid?http%3A%2F%2Fsu.
225	4.423309	10.2.67.106	23.61.3.177	HTTP	779	GET /js/300/addthis_widget.j
366	4.692948	10.2.67.106	23.61.3.177	HTTP	446	GET /live/boost/ra-558882012
374	4.705098	10.2.67.106	23.61.3.177	HTTP	1099	GET /live/red_lojson/300lo.j
852	9.566069	10.2.67.106	172.217.2.202	HTTP	576	GET /maps/api/js/Authenticat
536	5.393746	10.2.67.106	23.61.3.177	HTTP	679	GET /red/usync?pid=11114&pui
533	5.393434	10.2.67.106	23.61.3.177	HTTP	668	GET /red/usync?pid=6&puid=57
483	5.113719	10.2.67.106	23.46.193.117	HTTP	597	GET /site/21176?ret=html&lin
580	5.806624	10.2.67.106	23.46.193.117	HTTP	557	GET /site/2831?phint=zip=&ph
767	7.640467	10.2.67.106	199.83.135.157	HTTP	805	GET /sites/all/themes/sabros
881	11.094540	HewlettP_10:68:8d	Broadcast	ARP	60	Gratuitous ARP for 10.2.67.6
550	5.537372	3ComEuro_ca:65:9d	Broadcast	ARP	60	Gratuitous ARP for 169.254.1
862	10.153328	3ComEuro_ca:65:be	Broadcast	ARP	60	Gratuitous ARP for 169.254.1
590	5.962973	23.46.193.117	10.2.67.106	HTTP	556	HTTP/1.1 200 OK (GIF89a)
419	4.843442	23.61.3.177	10.2.67.106	HTTP	106	HTTP/1.1 200 OK (applicatio

< >

> Frame 852: 576 bytes on wire (4608 bits) 576 bytes captured (4608 bits) on interface 0

▼ Ethernet II, Src: HewlettP_25:7a:be (50:65:f3:25:7a:be) Dst: Vmware_ff:53:0f (00:0c:29:ff:53:0f)

> Destination: Vmware_ff:53:0f (00:0c:29:ff:53:0f)

> Source: HewlettP_25:7a:be (50:65:f3:25:7a:be)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.2.67.106, Dst: 172.217.2.202

> Transmission Control Protocol, Src Port: 51612, Dst Port: 80, Seq: 1, Ack: 1, Len: 522

> Hypertext Transfer Protocol

```

0000  00 0c 29 ff 53 0f 50 65 f3 25 7a be 08 00 45 00  ..).S·Pe·%z...E·
0010  02 32 1c 60 40 00 80 06 00 00 0a 02 43 6a ac d9  ·2·@...·Cj·
0020  02 ca c9 9c 00 50 ec a6 97 98 c9 7d 68 a7 50 18  ···P·...}h·P·
0030  01 02 ff 33 00 00 47 45 54 20 2f 6d 61 70 73 2f  ··3·GE T /maps/
0040  61 70 69 2f 6a 73 2f 41 75 74 68 65 6e 74 69 63  api/js/A uthentic
0050  61 74 69 6f 6e 53 65 72 76 69 63 65 2e 41 75 74  ationSer vice.Aut
0060  68 65 6e 74 69 63 61 74 65 3f 31 73 68 74 74 70  henticat e?1shttp
0070  25 33 41 25 32 46 25 32 46 77 77 77 2e 63 6f 6c  %3A%2F%2 Fwww.col
0080  6f 6d 62 69 61 2e 74 72 61 76 65 6c 25 32 46 65  ombia.tr avel%2Fe
0090  6e 26 34 73 41 49 7a 61 53 79 44 52 6f 51 31 32  n&4sAIza SyDRoQ12
00a0  52 7a 32 70 78 45 50 32 2d 4a 5a 45 4b 66 48 72  Rz2pxEP2 -JZEKfHc

```



```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : is.escuelaing.edu.co
    Description . . . . . : Intel(R) Ethernet Connection I217-LM
    Physical Address. . . . . : 50-65-F3-25-7A-BE
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::9d2e:23dd:136f:f7ed%11(Preferred)
    IPv4 Address. . . . . : 10.2.67.106(Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Lease Obtained. . . . . : Wednesday, February 13, 2019 10:17:02 AM
    Lease Expires . . . . . : Wednesday, February 13, 2019 10:17:02 PM
    Default Gateway . . . . . : fe80::20c:29ff:fe2c:4ef5%11
                                10.2.65.1
                                10.2.65.3
    DHCP Server . . . . . : 10.2.65.14
    DHCPv6 IAID . . . . . : 60871617
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-A6-FE-50-65-F3-25-7A-BE
    DNS Servers . . . . . : 10.2.65.62
                                10.2.65.2
                                10.2.65.61
                                10.2.65.60
                                10.2.65.12
                                10.2.65.16
    NetBIOS over Tcpip. . . . . : Enabled

```

La dirección MAC que tiene el source de Wireshak coincide con la MAC del computador. (50-65-F3-25-7A-BE)

2. Tarjeta de red

- Identifique la tarjeta de red del computador del Laboratorio de Redes de Computadores que está usando
- Documente
 - Modelo

```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : is.escuelaing.edu.co
    Description . . . . . : Intel(R) Ethernet Connection I217-LM
    Physical Address. . . . . : 50-65-F3-25-7A-BE
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::9d2e:23dd:136f:f7ed%11(Preferred)
    IPv4 Address. . . . . : 10.2.67.106(Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Lease Obtained. . . . . : Wednesday, February 13, 2019 10:17:02 AM
    Lease Expires . . . . . : Wednesday, February 13, 2019 10:17:01 PM
    Default Gateway . . . . . : fe80::20c:29ff:fe2c:4ef5%11
                                10.2.65.1
                                10.2.65.3
    DHCP Server . . . . . : 10.2.65.14
    DHCPv6 IAID . . . . . : 60871617
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-A6-FE-50-65-F3-25-7A-BE
    DNS Servers . . . . . : 10.2.65.62
                                10.2.65.2
                                10.2.65.61
                                10.2.65.60
                                10.2.65.12
                                10.2.65.16
    NetBIOS over Tcpip. . . . . : Enabled

```

Es el modelo Intel(R) Ethernet Connection I217-LM

- Velocidad

```

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.17134.441]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Redes>wmic nic where "speed is not null" get name,speed
Name                                     Speed
-----
VMware Virtual Ethernet Adapter for VMnet1 100000000
VMware Virtual Ethernet Adapter for VMnet8 100000000
Intel(R) Ethernet Connection I217-LM      100000000
VirtualBox Host-Only Ethernet Adapter    100000000

C:\Users\Redes>

```

O buscando la especificación del modelo Intel(R) Ethernet Connection I217-LM se encuentra la velocidad

Especificaciones de redes

Configuración de puerto	Single
Velocidad de datos por puerto	1GbE
Tipo de interfaz de sistema	Proprietary
Compatibilidad con tramas Jumbo	Sí
Interfaces admitidas	100Base-T, 1000Base-T

○ Dirección MAC

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : is.escuelaing.edu.co
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : 50-65-F3-25-7A-BE
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::9d2e:23dd:136f:f7ed%11(Preferred)
IPv4 Address. . . . . : 10.2.67.106(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Wednesday, February 13, 2019 10:17:02 AM
Lease Expires . . . . . : Wednesday, February 13, 2019 10:17:01 PM
Default Gateway . . . . . : fe80::20c:29ff:fe2c:4ef5%11
                             10.2.65.1
                             10.2.65.3
DHCP Server . . . . . : 10.2.65.14
DHCPv6 IAID . . . . . : 60871617
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-A6-FE-50-65-F3-25-7A-BE
DNS Servers . . . . . : 10.2.65.62
                             10.2.65.2
                             10.2.65.61
                             10.2.65.60
                             10.2.65.12
                             10.2.65.16
NetBIOS over Tcpip. . . . . : Enabled
```

La dirección MAC es la misma dirección física.

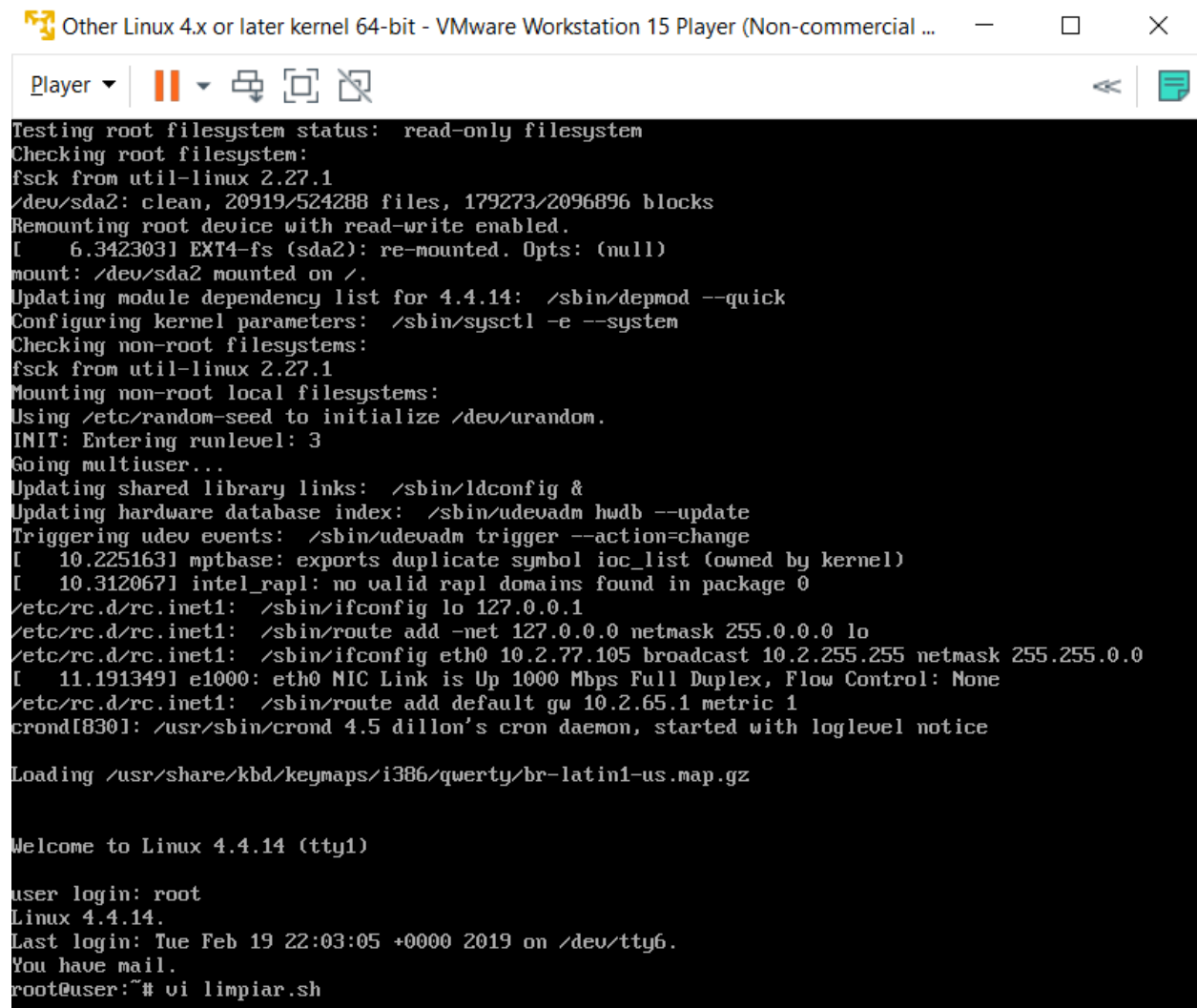
Bourne Shell programming- Unix

1. Ejecución automática de una secuencia de Usando Wireshark

Escriba un programa Shell que:

- Limpie la pantalla

Primero se crea en el editor VI un archivo llamado limpiar.sh el cual es un archivo ejecutable



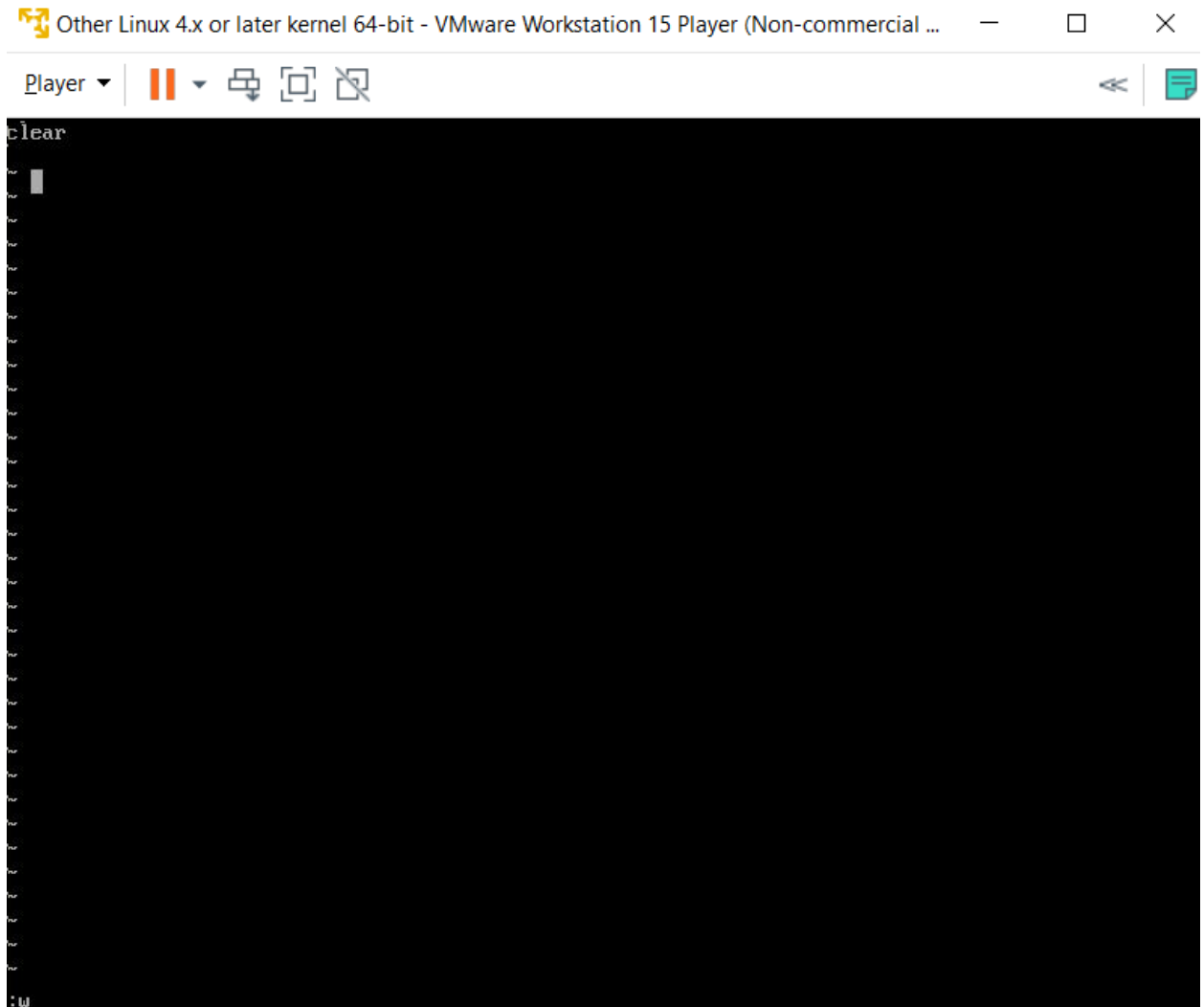
```
Other Linux 4.x or later kernel 64-bit - VMware Workstation 15 Player (Non-commercial ...
Player
Testing root filesystem status: read-only filesystem
Checking root filesystem:
fsck from util-linux 2.27.1
/dev/sda2: clean, 20919/524288 files, 179273/2096896 blocks
Remounting root device with read-write enabled.
[ 6.342303] EXT4-fs (sda2): re-mounted. Opts: (null)
mount: /dev/sda2 mounted on /.
Updating module dependency list for 4.4.14: /sbin/depmod --quick
Configuring kernel parameters: /sbin/sysctl -e --system
Checking non-root filesystems:
fsck from util-linux 2.27.1
Mounting non-root local filesystems:
Using /etc/random-seed to initialize /dev/urandom.
INIT: Entering runlevel: 3
Going multiuser...
Updating shared library links: /sbin/ldconfig &
Updating hardware database index: /sbin/udevadm hwdb --update
Triggering udev events: /sbin/udevadm trigger --action=change
[ 10.225163] mptbase: exports duplicate symbol ioc_list (owned by kernel)
[ 10.312067] intel_rapl: no valid rapl domains found in package 0
/etc/rc.d/rc.inet1: /sbin/ifconfig lo 127.0.0.1
/etc/rc.d/rc.inet1: /sbin/route add -net 127.0.0.0 netmask 255.0.0.0 lo
/etc/rc.d/rc.inet1: /sbin/ifconfig eth0 10.2.77.105 broadcast 10.2.255.255 netmask 255.255.0.0
[ 11.191349] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
/etc/rc.d/rc.inet1: /sbin/route add default gw 10.2.65.1 metric 1
crond[830]: /usr/sbin/crond 4.5 dillon's cron daemon, started with loglevel notice

Loading /usr/share/kbd/keymaps/i386/qwerty/br-latin1-us.map.gz

Welcome to Linux 4.4.14 (tty1)

user login: root
Linux 4.4.14.
Last login: Tue Feb 19 22:03:05 +0000 2019 on /dev/tty6.
You have mail.
root@user:~# vi limpiar.sh
```

Posteriormente se escribe “clear” en el modo texto del editor y se entra al modo comando de VI con la tecla ESC. Luego se coloca el comando “:w” para poder guardar los cambios en el archivo.

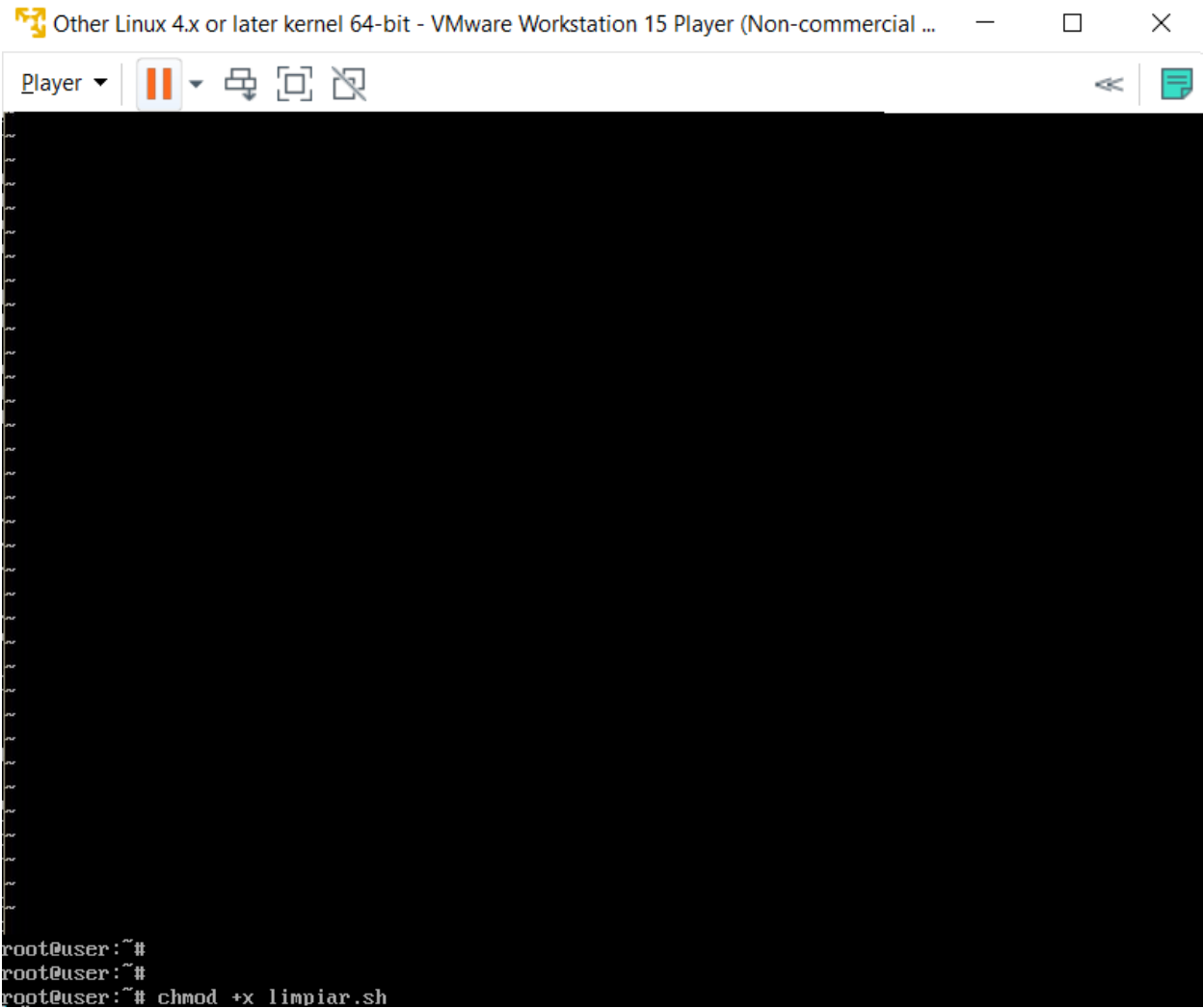


Se dan permisos de ejecución al archivo con el comando “chmod +x limpiar.sh” para ejecutar el archivo con el comando ./limpiar.sh

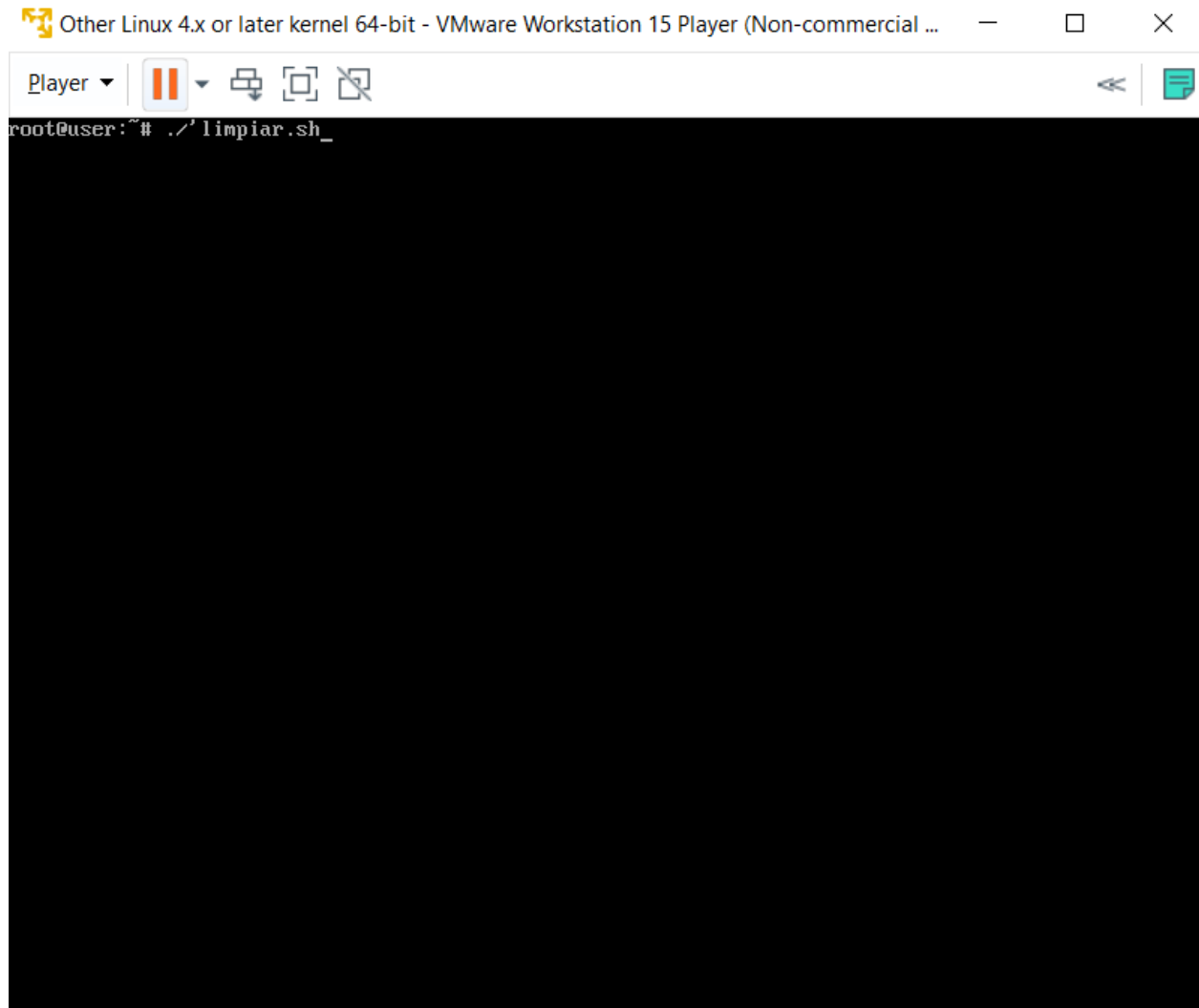
Player ▾



```
root@user:~# chmod +x limpiär.sh
root@user:~# sadkja.j
-bash: sadkja.j: command not found
root@user:~# wodkoqwkdq
-bash: wodkoqwkdq: command not found
root@user:~# wqkdowqkodkwq
-bash: wqkdowqkodkwq: command not found
root@user:~# wqokodjuqi.jd
-bash: wqokodjuqi.jd: command not found
root@user:~# wq0kf9ew9f
-bash: wq0kf9ew9f: command not found
root@user:~# 0eo0wo
-bash: 0eo0wo: command not found
root@user:~# ./limpiär.sh
```

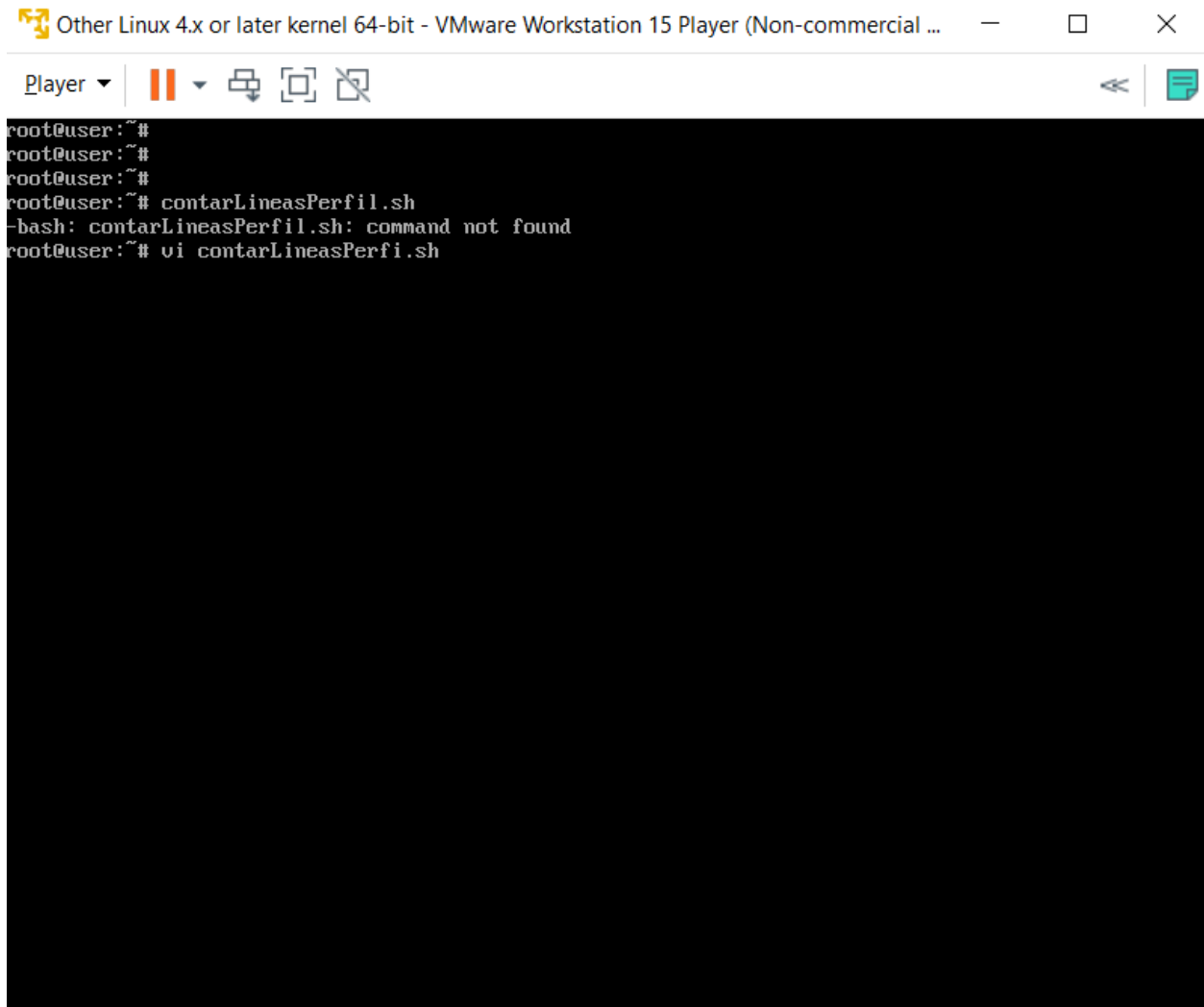


Y efectivamente se limpió la pantalla:



- Imprima el mensaje “El número de líneas del archivo /etc/profile es:” y el número de líneas encontrados.

Se crea un archivo en el editor VI llamado contarLineasPerfil.sh



```
root@user:~#
root@user:~#
root@user:~#
root@user:~# contarLineasPerfil.sh
-bash: contarLineasPerfil.sh: command not found
root@user:~# vi contarLineasPerfi.sh
```

Se utiliza el comando echo para imprimir, se imprime el string que es requerido en el ejercicio y mediante el comando “\$(wc -l /etc/profile |awk '{print \$1})” se imprimirá solamente el número de filas, debido a que wc imprime el número de filas y el nombre del archivo el “awk '{print \$1})” imprimirá solo el número de líneas del archivo profile...

Other Linux 4.x or later kernel 64-bit - VMware Workstation 15 Player (Non-commercial ...

Player ▾ | [Icons: Run, Copy, Paste, Full Screen, Exit Full Screen] | [Icons: Previous, Next]

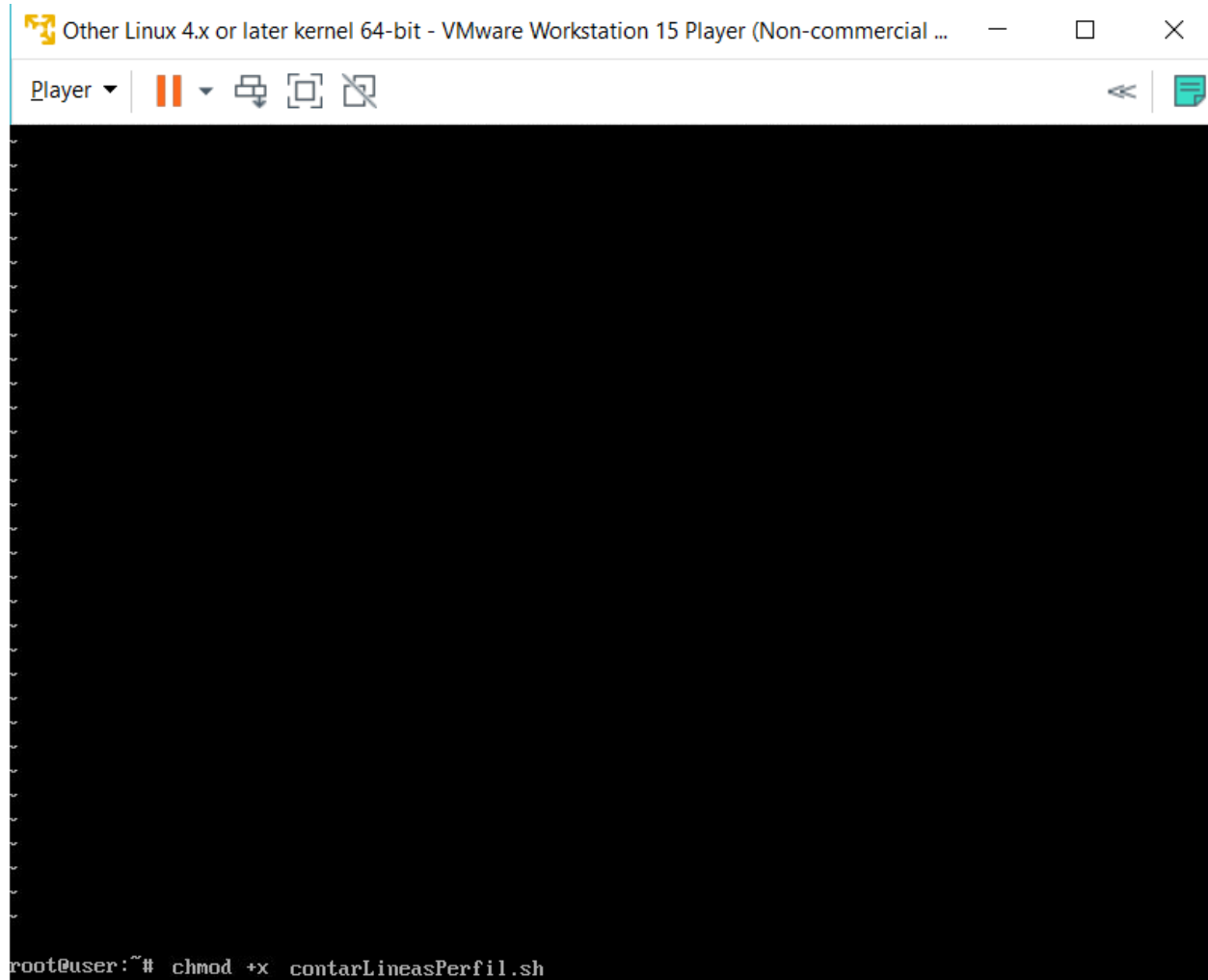
```

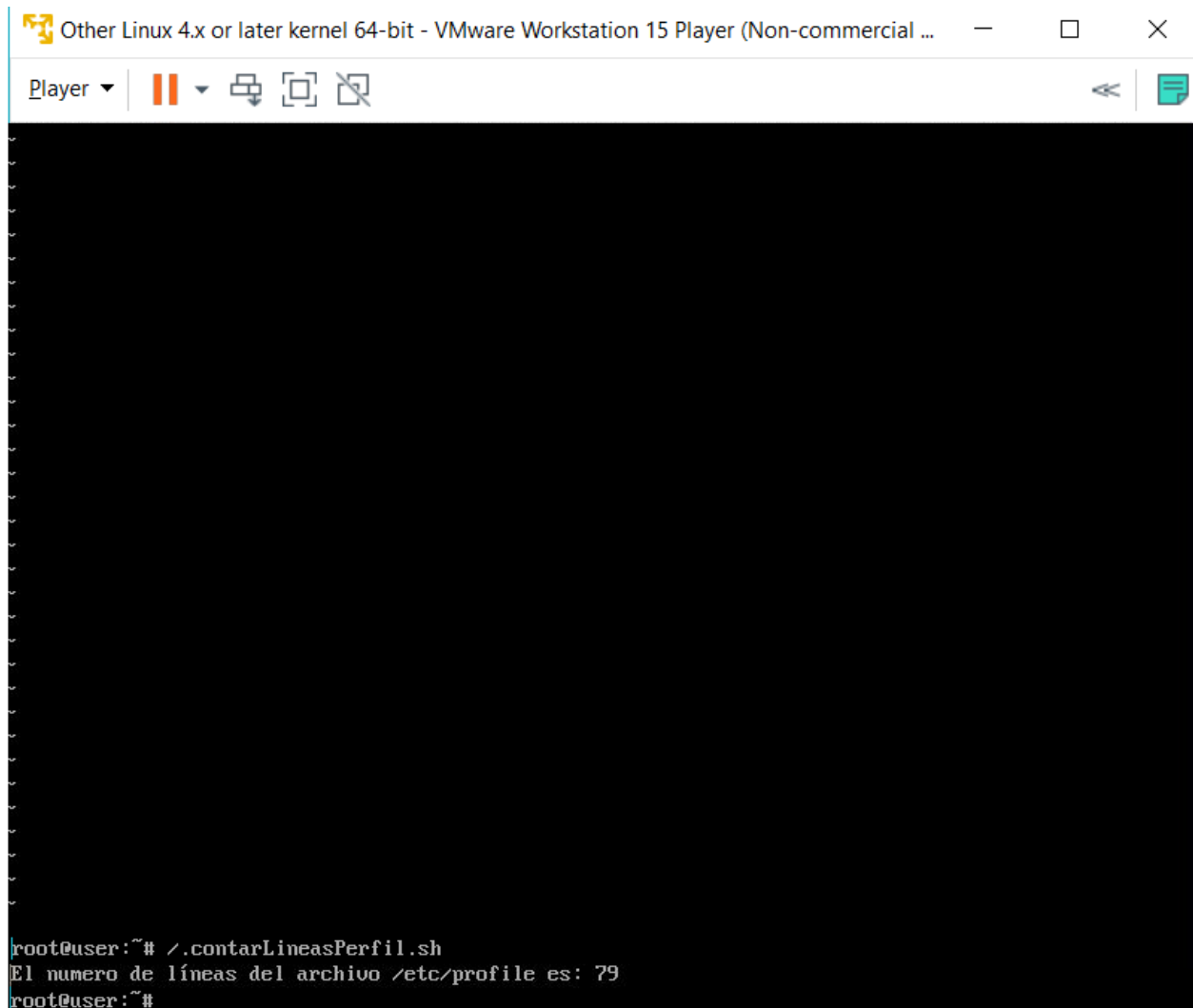
echo El numero de líneas del archivo /etc/profile es: $(wc -l /etc/profile | awk '{print $1}')

```

Read contarLineasProfile.sh, 2 lines, 96 chars 1,1 Command

Luego se dan permisos al archivo para ejecutarlo





```
Other Linux 4.x or later kernel 64-bit - VMware Workstation 15 Player (Non-commercial ...  
Player ▾ | [Pause] [Full Screen] [Close]  
root@user:~# ./contarLineasPerfil.sh  
El numero de líneas del archivo /etc/profile es: 79  
root@user:~#
```

Y como se evidencia: el script retorna el número de líneas del archivo “profile”.

Conclusiones:

- Mediante este laboratorio se aprendió de manera clara el funcionamiento del protocolo Ethernet en la capa de enlace, ya que se evidenciaron algunos de los frames que envía a través de la red.
- Se aprendió acerca del direccionamiento a nivel de enlace, es decir, las direcciones MAC: qué son, su función, y su implementación en herramientas de redes.
- Se aprendió a estructurar una red en la herramienta Packet Tracer.
- Se entendió el manejo de herramientas como Packet Tracer y Wireshark para el funcionamiento de las redes.
- Se aprendió a realizar scripts básicos en el Shell de Linux.

Bibliografía:

- Anónimo. Análisis de red con Wireshark [online]. Filtros [consulta: 19 de febrero de 2019] Disponible en:
<https://seguridadyredes.wordpress.com/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacia/>
- Claudia Santiago. *Capa de Enlace* [online]. [consulta: 19 de febrero de 2019]. Disponible en:
http://campusvirtual.escuelaing.edu.co/moodle/pluginfile.php/149311/mod_resource/content/2/03-capaEnlace_20191_p1.pdf
- Anónimo. ¿Qué es Wireshark? Así funciona la nueva tendencia esencial en seguridad [online]. [consulta: 19 de febrero de 2019] Disponible en:
<https://cso.computerworld.es/tendencias/que-es-wireshark-asi-funciona-la-nueva-tendencia-esencial-en-seguridad>
- Borja Merino. Análisis de tráfico con Wireshark [online]. Inteco [consulta: 19 de febrero de 2019] Disponible en:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf
- Francisco Jiménez. Programación Shell-script en Linux. [consulta: 19 de febrero de 2019] Disponible en:
<http://trajano.us.es/~fifi/shell/shellscript.htm>