[UNIVERSIDAD TECNOLOGICA NACIONAL]
FRD
[FACULTAD REGIONAL DELTA]

Carrera: Ing. Sistemas de información

Materia: Redes de datos

Profesor: Ing. Juan Antonio González

Docente Laboratorio: Ing. Carlos José Alberto Carrizo

TP N° 1

Introducción

Alumna:

Apellido y Nombre	legajo
Enriquez, Sylvina	--------

Curso: 2025

CONSIGNA TRABAJO PRÁCTICO 1

Tema: **Red LAN, modelo TCP IP, Wireshark, Packet Tracer**

Herramientas a utilizar: PC con Windows, aplicación Wireshark, Packet Tracer.

1. Desde una PC con Windows que tenga acceso a internet: Ejecute desde línea de comandos (cmd) los siguientes comandos:
    - Ipconfig
    - netstat
    - ping www.frd.utn.edu.ar

    a. Analice las respuestas a cada comando y explique qué significan.

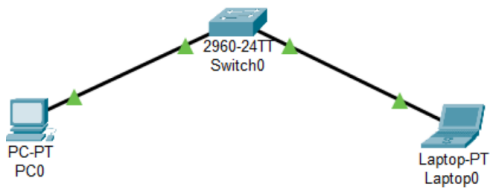
    b. Identificar la IP de la PC, Default Gateway y Máscara de red.

2. Desde una PC con Windows:
    - Instale la aplicación Wireshark.
    - Desde línea de comando ejecute: ipconfig /flushdns
    - Cierre todas las aplicaciones abiertas.
    - Ejecute la aplicación Wireshark como administrador e inicie el monitoreo sobre la placa de red mediante la cual tiene acceso a internet con el modo promiscuo desactivado.
    - Desde línea de comando ejecute un ping al dominio: frd.cvg.utn.edu.ar Detenga el monitoreo de Wireshark.

    a. En la captura de Wireshark seleccione un paquete correspondiente a la comunicación DNS e identifique y documente las distintas capas del modelo TCP/IP de ese paquete.

    b. En la captura de Wireshark seleccione un paquete del tipo ICMP y documente la capa de red donde se identifique la dirección IP del dominio: frd.cvg.utn.edu.ar

3. Desde una PC con Windows: · Instale la aplicación Packet Tracer. · Genere la siguiente red:



    a. Asigna una dirección IP y máscara de red a la PC y la Laptop.
    b. Documente el ping exitoso entre ambos equipos. c) Adjunte el archivo .pkt como evidencia.

Desarrollo del trabajo práctico 1

Introducción

1. Desde una PC con Windows que tenga acceso a internet: Ejecute desde línea de comandos (cmd) los siguientes comandos:
    - Ipconfig
    - netstat
    - ping www.frd.utn.edu.ar

a. Analice las respuestas a cada comando y explique qué significan.

ipconfig:

```
C:\Users\sylvi>ipconfig

Configuración IP de Windows


Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : home
   Dirección IPv6 . . . . . . . . . . . . . . : 2800:810:49c:a1c:3167:cd5b:cb7:42ab
   Dirección IPv6 . . . . . . . . . . . . . . : 2800:810:49c:a1c:b89d:99f2:66a6:4982
   Dirección IPv6 . . . . . . . . . . . . . . : fdaa:bbcc:ddee:0:aea8:61cb:b080:2de
   Dirección IPv6 temporal. . . . . . . . . . : 2800:810:49c:a1c:9d6e:7c7f:2694:4223
   Dirección IPv6 temporal. . . . . . . . . . : fdaa:bbcc:ddee:0:9d6e:7c7f:2694:4223
   Vínculo: dirección IPv6 local. . . . . . . : fe80::730e:fc41:5249:96d1%12
   Dirección IPv4. . . . . . . . . . . . . . . . . . . . . . . . : 192.168.0.9
   Máscara de subred . . . . . . . . . . . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . . . . . . . . . . . : fe80::9a1e:19ff:fe1d:5999%12
                                       192.168.0.1
```

Este comando (de Windows) se utiliza para mostrar la configuración de la red TCP/IP.

Es una herramienta útil para identificar las direcciones IP privadas que se están utilizando para las placas de red y la dirección del Gateway.

netstat:

```
C:\Users\sylvi>netstat

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:49677        Sylvina:49678          ESTABLISHED
  TCP    127.0.0.1:49678        Sylvina:49677          ESTABLISHED
  TCP    127.0.0.1:51732        Sylvina:51733          ESTABLISHED
  TCP    127.0.0.1:51733        Sylvina:51732          ESTABLISHED
  TCP    127.0.0.1:51936        Sylvina:51937          ESTABLISHED
  TCP    127.0.0.1:51937        Sylvina:51936          ESTABLISHED
  TCP    127.0.0.1:56360        Sylvina:56361          ESTABLISHED
  TCP    127.0.0.1:56361        Sylvina:56360          ESTABLISHED
  TCP    192.168.0.9:52913      52.123.187.9:https     ESTABLISHED
  TCP    192.168.0.9:52915      52.123.187.9:https     ESTABLISHED
  TCP    192.168.0.9:52958      edge-dgw-shv-01-eze1:https  ESTABLISHED
  TCP    192.168.0.9:52969      162.159.134.234:https  ESTABLISHED
  TCP    192.168.0.9:52979      134.224.240.218:https  ESTABLISHED
  TCP    192.168.0.9:53186      104.208.16.90:https    TIME_WAIT
  TCP    192.168.0.9:53196      server-3-160-117-130:https  ESTABLISHED
  TCP    192.168.0.9:53207      13.71.55.58:https      TIME_WAIT
  TCP    192.168.0.9:53217      20.42.65.89:https      ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:49461  [2603:1030:210:f::1]:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52922  [2603:1030:210:f::]:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52935  edge-z-p36-shv-01-eze1:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52936  [2407:30c0:100:723:ea70:82bb:711:9fa9]:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52937  [2603:1063:24::302]:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52942  [2603:1063:11::ee]:https  ESTABLISHED
  TCP    [2800:810:49c:a1c:9d6e:7c7f:2694:4223]:52952  edge-star6-shv-01-eze1:https  ESTABLISHED
```

Este comando se utiliza para observar cuáles son los puertos que se encuentran ocupados (conexiones activas cliente/servidor). Tiene cuatro campos (columnas).

i. Protocolo: nombre del mismo (UDP o TCP)

ii. Dirección local: muestra la dirección IP y el puerto que se están utilizando (socket)

iii. Dirección remota: muestra la dirección IP y el número de puerto de la computadora remota a la que el socket está conectado

iv. Estado: indica el estado de la conexión

ping www.frd.utn.edu.ar

```
C:\Users\sylvi>ping www.frd.utn.edu.ar
La solicitud de ping no pudo encontrar el host www.frd.utn.edu.ar. Compruebe el nombre y
vuelva a intentarlo.

C:\Users\sylvi>ping frd.cvg.utn.edu.ar

Haciendo ping a frd.cvg.utn.edu.ar [52.151.241.218] con 32 bytes de datos:
Respuesta desde 52.151.241.218: bytes=32 tiempo=162ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=162ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=158ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=157ms TTL=249

Estadísticas de ping para 52.151.241.218:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 157ms, Máximo = 162ms, Media = 159ms
```

Este comando envía paquetes a un destino para tener conocimiento acerca de si los equipos origen y destino se encuentran conectados. Pertenecen al protocolo ICMP.

b. Identificar la IP de la PC, Default Gateway y Máscara de red.

```
C:\Users\sylvi>ipconfig

Configuración IP de Windows

   Sufijo DNS específico para la conexión. . : home
   Dirección IPv6 . . . . . . . . . . . . . : 2800:810:49c:a1c:3167:cd5b:cb7:42ab
   Dirección IPv6 . . . . . . . . . . . . . : 2800:810:49c:a1c:b89d:99f2:66a6:4982
   Dirección IPv6 . . . . . . . . . . . . . : fdaa:bbcc:ddee:0:aea8:61cb:b080:2de
   Dirección IPv6 temporal. . . . . . . . . : 2800:810:49c:a1c:9d6e:7c7f:2694:4223
   Dirección IPv6 temporal. . . . . . . . . : fdaa:bbcc:ddee:0:9d6e:7c7f:2694:4223
   Vínculo: dirección IPv6 local. . . . . . : fe80::730e:fc41:5249:96d1%12
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.9
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::9a1e:19ff:fe1d:5999%12
                                               192.168.0.1
```

IP de la PC: 192.268.0.9
Default Gateway: 192.168.0.1 (en IPv4)
Máscara de red: 255.255.255.0

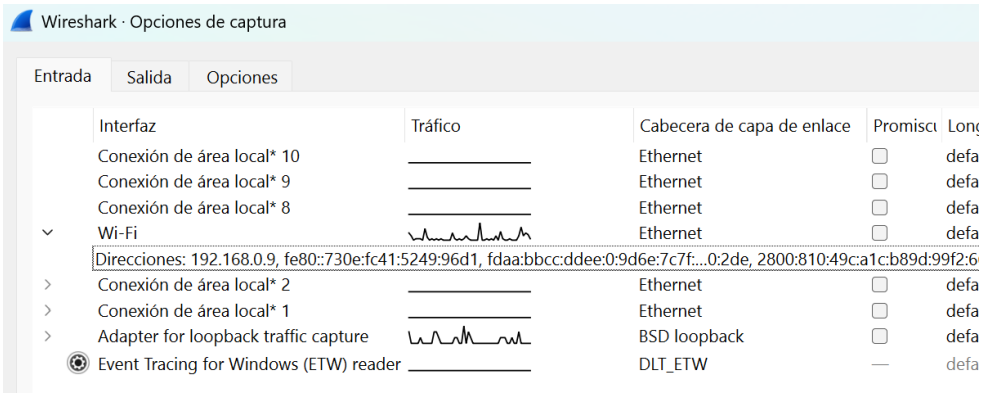
2. Desde una PC con Windows:

- Instale la aplicación Wireshark.
- Desde línea de comando ejecute: **ipconfig /flushdns**

```
C:\Users\sylvi>ipconfig/flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.
```

(el comando utilizado limpia la caché)
- Cierre todas las aplicaciones abiertas.
- Ejecute la aplicación Wireshark como administrador e inicie el monitoreo

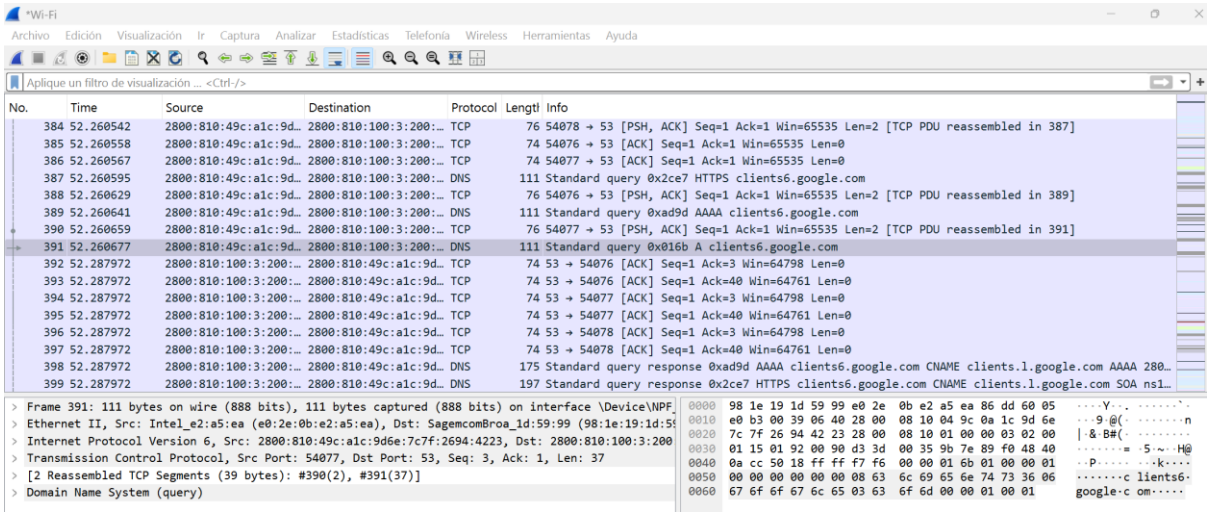
sobre la placa de red mediante la cual tiene acceso a internet con el modo promiscuo desactivado.



- Desde línea de comando ejecute un **ping** al dominio: **frd.cvg.utn.edu.ar** Detenga el monitoreo de Wireshark.

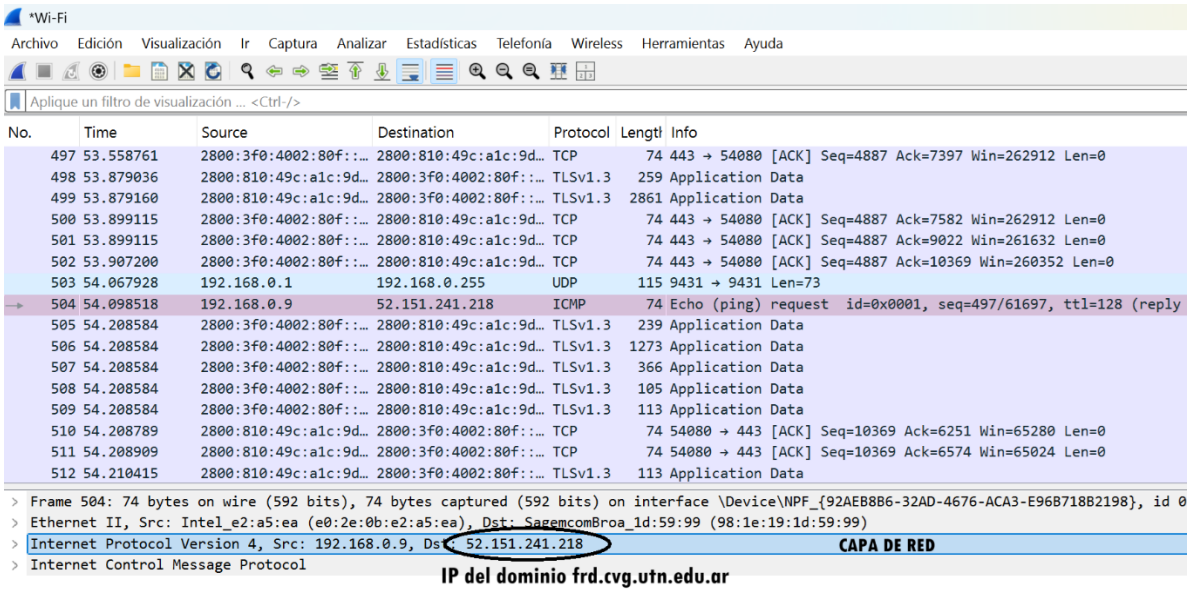
```
C:\Users\sylvi>ping frd.cvg.utn.edu.ar

Haciendo ping a frd.cvg.utn.edu.ar [52.151.241.218] con 32 bytes de datos:
Respuesta desde 52.151.241.218: bytes=32 tiempo=161ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=162ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=162ms TTL=249
Respuesta desde 52.151.241.218: bytes=32 tiempo=162ms TTL=249

Estadísticas de ping para 52.151.241.218:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 161ms, Máximo = 162ms, Media = 161ms
```

a. En la captura de Wireshark seleccione un paquete correspondiente a la comunicación DNS e identifique y documente las distintas capas del modelo TCP/IP de ese paquete.



Capas protocolo TCP/IP	
FÍSICA	> Frame 391: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF_{92AEB8B6-
ENLACE	> Ethernet II, Src: Intel_e2:a5:ea (e0:2e:0b:e2:a5:ea), Dst: SagemcomBroa_1d:59:99 (98:1e:19:1d:59:99)
RED	> Internet Protocol Version 6, Src: 2800:810:49c:a1c:9d6e:7c7f:2694:4223, Dst: 2800:810:100:3:200:115:192:90
TRANSPORTE	> Transmission Control Protocol, Src Port: 54077, Dst Port: 53, Seq: 3, Ack: 1, Len: 37
	> [2 Reassembled TCP Segments (39 bytes): #390(2), #391(37)]
APLICACIÓN	> Domain Name System (query)

b. En la captura de Wireshark seleccione un paquete del tipo ICMP y documente la capa de red donde se identifique la dirección IP del dominio: frd.cvg.utn.edu.ar

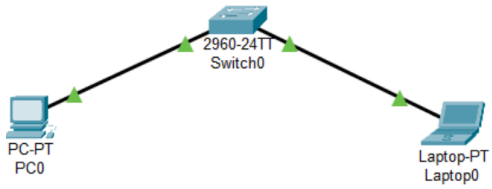


En la línea marcada con una flecha → ,donde se observa un paquete del tipo ICMP, se analiza la capa de red, marcada en celeste. Ahí se puede observar la IP del dominio frd.cvg.utn.edu.ar, pues figura como destino (Dst) del comando ping que se había realizado previamente a esa dirección: 52.151.241.218

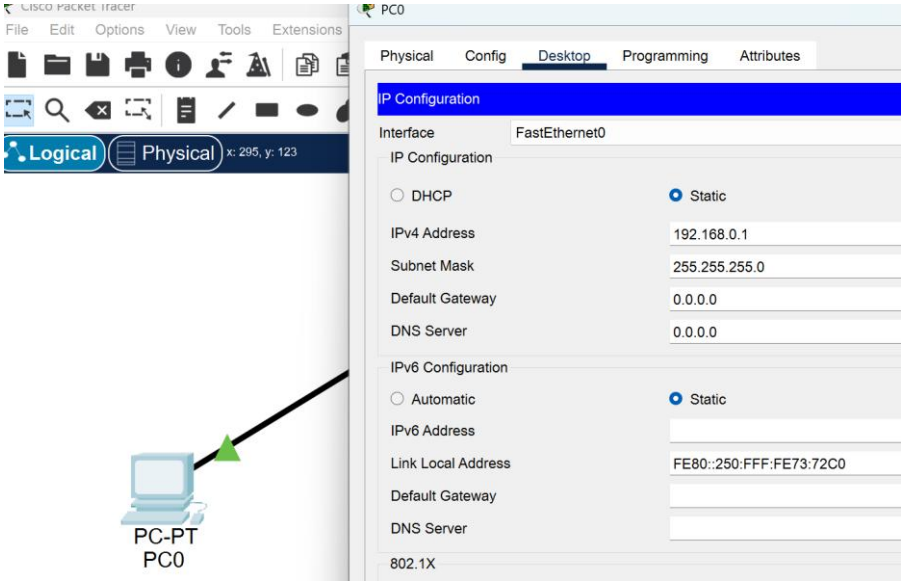
3. Desde una PC con Windows:

· Instale la aplicación Packet Tracer.

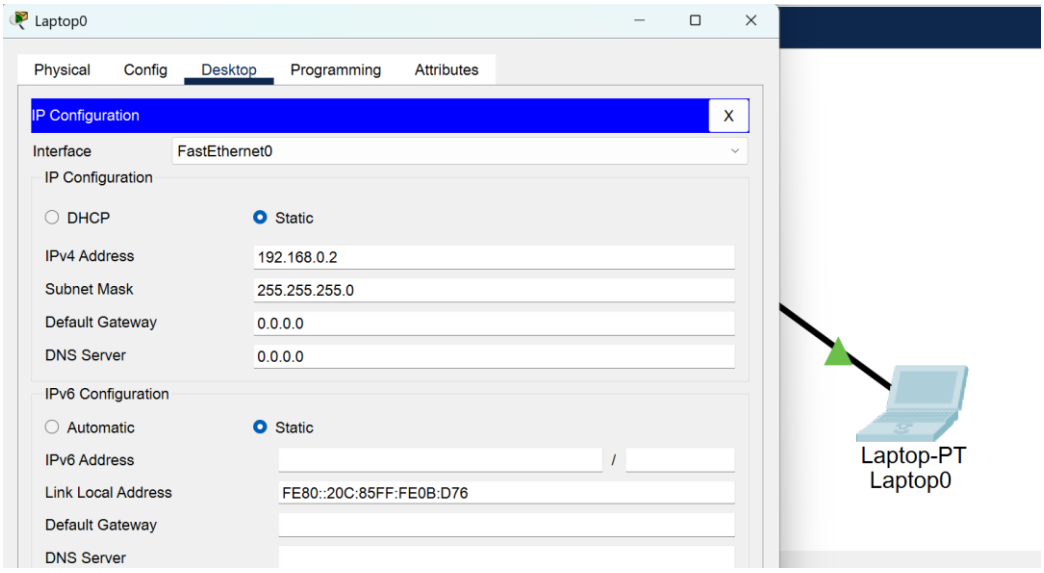
· Genere la siguiente red:



a. Asigna una dirección IP y máscara de red a la PC y la Laptop.

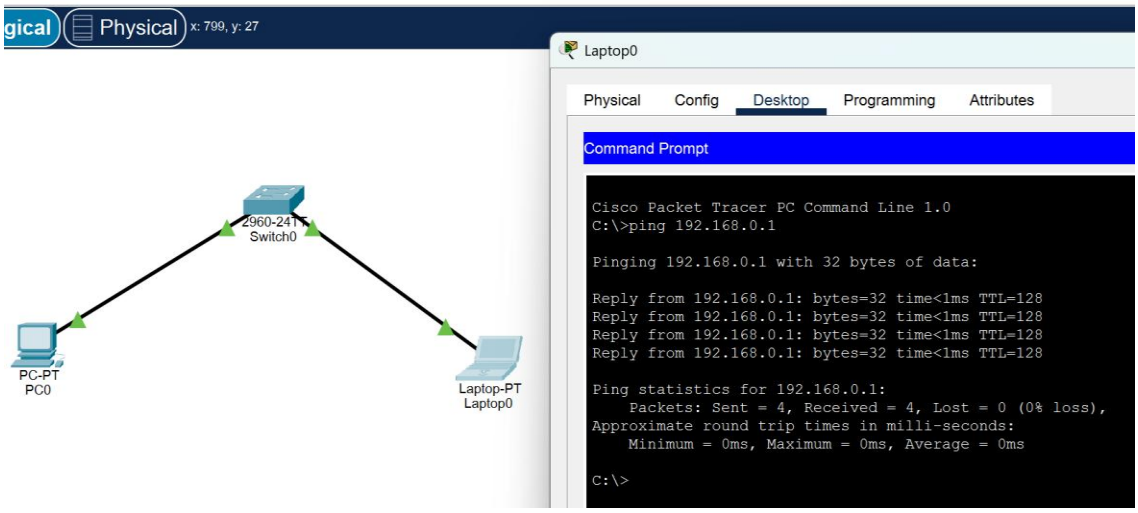


Asignación de IP y máscara de red a la PC



Asignación de IP y máscara de red a la Laptop

b. Documente el ping exitoso entre ambos equipos.



c. Adjunte el archivo .pkt como evidencia.

Nombre del archivo: ***TP1-Enriquez.pkt***

Conclusiones

Este trabajo práctico de laboratorio es introductorio para comenzar a utilizar las herramientas de simulación de redes: *packet Tracer* y de un analizador de tráfico de protocolos: *Wireshark*. Se vuelcan, con estos programar, todos los conocimientos teóricos incorporados previamente.

Estas herramientas son útiles porque nos brindan información sobre la red, IPs, conexiones, que utilizaremos en otros trabajos prácticos.