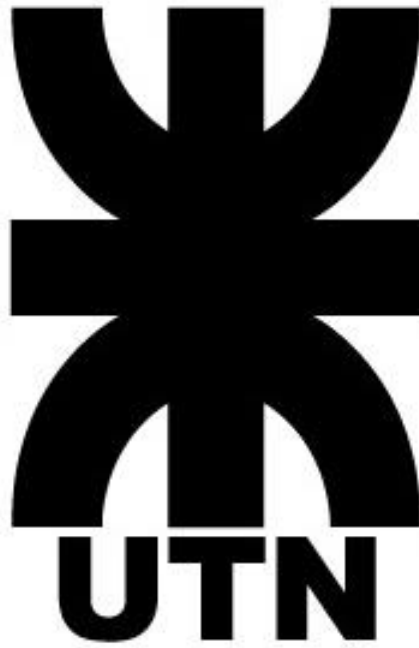


# **Universidad Tecnológica Nacional**



## **Facultad Regional Delta**

### **Laboratorio de Redes de Información**

### **Ciclo Lectivo 2024**

### **Trabajo Práctico N° | Introducción**

**Alumno: Gonzalez, Tomas**

**Profesor: Carrizo, Carlos**

Redes de información – Trabajo Practico N°1   Introducción		
Gonzalez Tomas	4to año	Ingeniería en Sistemas de información
Ciclo Lectivo 2024		

# Contenido

Consignas ..... 3

Resolución ..... 4

    Ejercicio 1 ..... 4

    Ejercicio 2 ..... 7

    Ejercicio 3 ..... 9

Conclusión. .... 10

## Consignas

- 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.
- Investigue y ejecute el comando para limpiar la caché DNS de Windows.
- Ejecute la aplicación Wireshark como administrador e inicie el monitoreo sobre la placa de red con el modo promiscuo desactivado.
- Ejecute los siguientes comandos en orden:

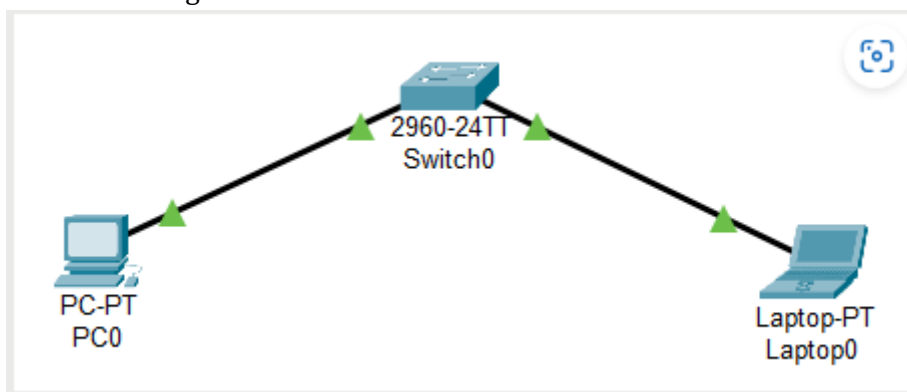
```
Nslookup(enter)  
Set q=any(enter)  
www.frd.utn.edu.ar (enter)  
Quit (enter)
```

- Detenga el monitoreo de Wireshark y guarde la captura hecha.

- 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) Del paquete anterior capturado, documente la consulta (query) realizada.

- 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.

# Resolución

## Ejercicio 1

- a) Luego de conectar la netbook a la red de internet de la facultad, se comienza ejecutando los comandos pedidos desde la CMD de Windows.

Comenzamos con el comando **ipconfig**, mediante el cual se puede observar información relacionada a la red a la cual estamos conectados. Entre esta información, destaca:

**Dirección IPv4:** La dirección IP es un identificador único para dispositivo de la red. En IPv4 hay 4 octetos, son 8 bits por cada octeto que pueden tomar o cero o uno, pasado a decimal, se obtiene un rango entre 0-255 por cada octeto.

**Mascara de subred:** Permite identificar a la red y al sistema terminal. Se compone de 4 octetos, que están divididos por parte alta, que son los primeros 2 octetos que identifican dirección de red y los últimos dos octetos, que son la parte baja e identifica dirección de host.

**Puerta de enlace predeterminada (o Default Gateway):** Es la dirección de la “Puerta” por donde salen y entran nuestros mensajes. Conecta al equipo con el resto de la red, fuera de la red local.

```
C:\Users\Tomi>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::d5fd:3733:38e2:d110%14
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

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. . . :
    Vínculo: dirección IPv6 local. . . : fe80::64e:acdb:6f89:d8b%10
    Dirección IPv4. . . . . : 172.16.10.161
    Máscara de subred . . . . . : 255.255.254.0
    Puerta de enlace predeterminada . . . . . : 172.16.10.1

Adaptador de Ethernet Conexión de red Bluetooth:

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

El siguiente comando es el **netstat**, el cual nos muestra el estado de los puertos (más sencillamente, permite ver las distintas conexiones activas en la red que se encuentra el equipo).

```
C:\Users\Tomi>netstat

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    127.0.0.1:49899       kubernetes:52294      ESTABLISHED
TCP    127.0.0.1:52294       kubernetes:49899      ESTABLISHED
TCP    172.16.10.161:52323   52.226.139.121:https   ESTABLISHED
TCP    172.16.10.161:52401   dns:https              CLOSE_WAIT
TCP    172.16.10.161:52402   205.185.115.5:4563     ESTABLISHED
TCP    172.16.10.161:52403   dns:https              CLOSE_WAIT
TCP    172.16.10.161:52404   dns:https              CLOSE_WAIT
TCP    172.16.10.161:52405   cdn-185-199-111-133:https CLOSE_WAIT
TCP    172.16.10.161:52406   cdn-185-199-111-133:https CLOSE_WAIT
TCP    172.16.10.161:57573   52.226.139.121:https   ESTABLISHED
TCP    172.16.10.161:57580   52.226.139.121:https   ESTABLISHED
TCP    172.16.10.161:57773   20.127.250.238:https   ESTABLISHED
TCP    172.16.10.161:57953   52.111.225.6:https     ESTABLISHED
TCP    172.16.10.161:58060   13.107.246.254:https   CLOSE_WAIT
TCP    172.16.10.161:58100   13.107.253.254:https   CLOSE_WAIT
TCP    172.16.10.161:58169   161-197-30-181:https   LAST_ACK
TCP    172.16.10.161:58170   161-197-30-181:https   LAST_ACK
TCP    172.16.10.161:58171   whatsapp-cdn-shv-01-eze1:https LAST_ACK
TCP    172.16.10.161:58172   whatsapp-cdn-shv-01-scl2:https LAST_ACK
TCP    172.16.10.161:58173   host96:https           LAST_ACK
TCP    172.16.10.161:58174   host34:https           LAST_ACK
TCP    172.16.10.161:58175   97-197-30-181:https    LAST_ACK
TCP    172.16.10.161:58176   97-197-30-181:https    LAST_ACK
TCP    172.16.10.161:58177   host34:https           LAST_ACK
TCP    172.16.10.161:58178   host96:https           LAST_ACK
TCP    172.16.10.161:58179   whatsapp-cdn-shv-01-eze1:https LAST_ACK
TCP    172.16.10.161:58232   20.42.73.27:https      TIME_WAIT
TCP    172.16.10.161:58243   a2-23-164-211:https    CLOSE_WAIT
TCP    172.16.10.161:58248   13.107.246.33:https    CLOSE_WAIT
TCP    172.16.10.161:58292   52.111.225.6:https     ESTABLISHED
TCP    172.16.10.161:58293   52.111.225.6:https     ESTABLISHED
TCP    172.16.10.161:58332   52.108.36.29:https     ESTABLISHED
TCP    172.16.10.161:58334   13.107.219.254:https   CLOSE_WAIT
TCP    172.16.10.161:58336   152.199.54.186:https   CLOSE_WAIT
TCP    172.16.10.161:58339   52.109.108.107:https   TIME_WAIT
TCP    172.16.10.161:58340   52.109.108.107:https   TIME_WAIT
TCP    172.16.10.161:58341   52.109.13.87:https     ESTABLISHED
TCP    172.16.10.161:58342   52.109.13.87:https     ESTABLISHED
TCP    172.16.10.161:58343   52.97.23.130:https     TIME_WAIT
TCP    172.16.10.161:58346   13.107.138.10:https    ESTABLISHED
```

Se observa que los distintos estados que obtuvimos fueron:

- **ESTABLISHED:** La conexión está establecida y los datos se están intercambiando activamente entre los dos dispositivos.
- **CLOSE\_WAIT:** Uno de los dispositivos ha cerrado la conexión, pero el otro todavía está esperando a que se confirme el cierre.
- **LAST\_ACK:** El último paquete de confirmación (ACK) se ha enviado, pero todavía no se ha recibido la confirmación de que se ha recibido correctamente.
- **TIME\_WAIT:** La conexión se ha cerrado, pero el dispositivo está esperando un tiempo determinado antes de eliminar la entrada de la tabla de conexiones. Esto se hace para evitar que los paquetes enviados durante el cierre de la conexión lleguen al dispositivo receptor y causen problemas.

Finalmente, se ejecuta el comando ping `www.frd.utn.edu.ar`. Este comando, sirve para saber si tengo conexión con un servidor o sistema terminal, y muestra cuantos paquetes llegan al destino. Se puede testear que la dirección a la que estamos enviando sirve (existe el Host), y para ver la latencia.

```
C:\Users\Tomi>ping www.frd.utn.edu.ar

Haciendo ping a nginx.frd.utn.edu.ar [192.168.0.37] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
```

Se observa qué para el dominio propuesto, está bloqueado el acceso, probamos en cambio a continuación con el dominio de Google.

```
C:\Users\Tomi>ping www.google.com

Haciendo ping a www.google.com [172.217.172.100] con 32 bytes de datos:
Respuesta desde 172.217.172.100: bytes=32 tiempo=15ms TTL=115
Respuesta desde 172.217.172.100: bytes=32 tiempo=15ms TTL=115
Respuesta desde 172.217.172.100: bytes=32 tiempo=15ms TTL=115
Respuesta desde 172.217.172.100: bytes=32 tiempo=14ms TTL=115

Estadísticas de ping para 172.217.172.100:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 15ms, Media = 14ms
```

En este caso, se obtuvo una respuesta exitosa. Detallamos lo que indica cada línea a continuación:

**“Respuesta desde 172.217.172.100”:** La dirección IP obtenida desde `www.google.com` es 172.217.172.100

**“Bytes = 32”:** Se envían paquetes de prueba con un tamaño de 32 bytes.

**“tiempo=15ms”:** También conocido como tiempo de latencia. Indica cuanto tiempo tarda el paquete en ir desde el origen hasta la dirección de destino y volver nuevamente hasta el origen. En este caso indica 15ms.

**“TTL=115”:** Significa "Time to Live" y representa el tiempo de vida que tiene un paquete en la red, es decir el tiempo que puede permanecer un paquete en la red antes de ser descartado. De esta manera, se evita que los paquetes circulen indefinidamente en la red.

**“Paquetes enviados”:** Cantidad de paquetes de prueba enviados. Muestra los paquetes recibidos y los no recibidos(perdidos), con un porcentaje de estos últimos.

**“Tiempos aproximados”:** Indica los tiempos máximos y mínimos de latencia del conjunto de paquetes de prueba enviados. Además, muestra un promedio obtenido de estos tiempos.

b) Según lo realizado en el apartado A), obtuvimos:

**Dirección Ipv4:** 172.16.10.161

**Máscara de subred:** 255.255.254.0

**Puerta de enlace predeterminada/Default Gateway:** 172.16.10.1

## Ejercicio 2

Luego de investigar, se encontró que el comando utilizado para borrar la caché DNS en Windows es */flushdns*, utilizado junto con el comando *ipconfig*.

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

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\Users\Tomi>
```

Luego de eliminar la caché de DNS en Windows, iniciamos la captura en Wireshark y luego pasamos a ejecutar el comando nslookup, el cual devuelve una llamada al DNS. Sirve para ver si el sistema DNS está resolviendo los nombres correctamente

```
C:\Users\Tomi>nslookup
Servidor predeterminado: frdwdc05.delta.utn
Address: 172.16.2.1

> set q=any
> www.frd.utn.edu.ar
Servidor: frdwdc05.delta.utn
Address: 172.16.2.1

www.frd.utn.edu.ar canonical name = nginx.frd.utn.edu.ar
> quit
```

En este caso, muestra el nombre del servidor DNS, el cual es “frdwdc05.delta.utn”, y su dirección IP es “172.16.2.1”

A continuación, se ejecuta la sentencia “set q=any”, Esto significa que el comando devolverá todos los registros de recursos disponibles para el nombre de dominio especificado. Luego se especifica el nombre del dominio que se quiere buscar, para este caso [www.frd.utn.edu.ar](http://www.frd.utn.edu.ar). En este caso, el comando nslookup devuelve todos los registros disponibles para el dominio establecido. Entre la información más relevante, se observa que el nombre canónico del dominio consultado es “nginx.frd.utn.edu.ar”. En este punto, se detiene la captura de la aplicación Wireshark.

a) En el Wireshark, se obtuvo qué:

179	30.105617	172.16.10.161	172.16.2.1	DNS	78 Standard query 0x0002 ANY www.frd.utn.edu.ar
180	30.109299	172.16.2.1	172.16.10.161	DNS	98 Standard query response 0x0002 ANY www.frd.utn.edu.ar CNAME nginx.frd.utn.edu.ar
219	31.500556	172.16.10.161	172.16.2.1	DNS	92 Standard query 0x2300 A mobile.events.data.microsoft.com
223	31.765014	172.16.2.1	172.16.10.161	DNS	212 Standard query response 0x2300 A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.n...
65	5.520417	172.16.10.161	142.251.134.42	QUIC	1292 Initial, DCID=e914d5e0444c588e, PKN: 1, CRYPTO
66	5.520882	172.16.10.161	142.251.134.42	QUIC	1292 Initial, DCID=e914d5e0444c588e, PKN: 2, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, CRYP...
67	5.521541	172.16.10.161	142.251.134.42	QUIC	123 0-RTT, DCID=e914d5e0444c588e
68	5.538390	142.251.134.42	172.16.10.161	QUIC	1292 Initial, SCID=e914d5e0444c588e, PKN: 1, ACK, PADDING
69	5.561798	142.251.134.42	172.16.10.161	QUIC	987 Protected Payload (KP0)
70	5.561798	142.251.134.42	172.16.10.161	QUIC	74 Protected Payload (KP0)

>	Frame 179: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{45653E68-6171-4CF3-A157-CD9E969EBFDC}, id 0
>	Ethernet II, Src: IntelCor_98:75:c9 (a0:af:bd:98:75:c9), Dst: ac:71:2e:14:3e:6c (ac:71:2e:14:3e:6c)
>	Internet Protocol Version 4, Src: 172.16.10.161, Dst: 172.16.2.1
>	User Datagram Protocol, Src Port: 58713, Dst Port: 53
>	Domain Name System (query)

```
0000  ac 71 2e 14 3e 6c a0 af bd 98 75 c9 08 00 45 00  .q..>1...u...E.
0010  00 40 be 4a 00 00 80 11 17 a0 ac 10 0a a1 ac 10  @.J.....
0020  02 01 e5 59 00 35 00 2c 6e 65 00 02 01 00 00 01  ..Y.S.,ni.....
0030  00 00 00 00 00 00 03 77 77 77 03 66 72 64 03 75  ....w ww.frd.u
0040  74 6e 03 65 64 75 02 61 72 00 00 ff 00 01      tn.edu.a .....
```



Haciendo enfoque en la captura, se ve:

```
> Frame 179: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{45653E68-6171-4CF3-A157-CD9E969EBFDC}, id 0
> Ethernet II, Src: IntelCor_98:75:c9 (a0:af:bd:98:75:c9), Dst: ac:71:2e:14:3e:6c (ac:71:2e:14:3e:6c)
> Internet Protocol Version 4, Src: 172.16.10.161, Dst: 172.16.2.1
> User Datagram Protocol, Src Port: 58713, Dst Port: 53
> Domain Name System (query)
```

Que muestra los distintos protocolos que utiliza el paquete en las distintas capas de la red, detallando:

- Capa de enlace: Utiliza Ethernet II
- Capa de red: Utiliza IPv4
- Capa de transporte: User Datagram Protocol
- Capa de aplicación: Domain Name System.

b) Especificando en el Domain name System, observamos el contenido de la query

179	30.105617	172.16.10.161	172.16.2.1	DNS	78 Standard query 0x0002 ANY www.frd.utn.edu.ar
180	30.109299	172.16.2.1	172.16.10.161	DNS	98 Standard query response 0x0002 ANY www.frd.utn.edu.ar CNAME nginx.frd.utn.edu.ar
219	31.500556	172.16.10.161	172.16.2.1	DNS	92 Standard query 0x2300 A mobile.events.data.microsoft.com
223	31.765014	172.16.2.1	172.16.10.161	DNS	212 Standard query response 0x2300 A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.n...
65	5.520417	172.16.10.161	142.251.134.42	QUIC	1292 Initial, DCID=e914d5e0444c588e, PKN: 1, CRYPTO
66	5.520882	172.16.10.161	142.251.134.42	QUIC	1292 Initial, DCID=e914d5e0444c588e, PKN: 2, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, CRYP...
67	5.521541	172.16.10.161	142.251.134.42	QUIC	123 0-RTT, DCID=e914d5e0444c588e
68	5.538390	142.251.134.42	172.16.10.161	QUIC	1292 Initial, SCID=e914d5e0444c588e, PKN: 1, ACK, PADDING
69	5.561798	142.251.134.42	172.16.10.161	QUIC	987 Protected Payload (KP0)
70	5.561798	142.251.134.42	172.16.10.161	QUIC	74 Protected Payload (KP0)

Additional RRs: 0

Queries

- www.frd.utn.edu.ar: type ANY, class IN
  - Name: www.frd.utn.edu.ar
  - [Name Length: 18]
  - [Label Count: 5]
  - Type: \* (A request for all records the server/cache has available) (255)
  - Class: IN (0x0001)

[Response In: 180]

```
0000  ac 71 2e 14 3e 6c a0 af bd 98 75 c9 08 00 45 00  .q.>1...E.
0010  00 40 be 4a 00 00 00 11 17 a0 ac 10 0a a1 ac 10  .@J.....
0020  02 01 e5 59 00 35 00 2c 6e 69 00 02 01 00 00 01  .Y.5, ni....
0030  00 00 00 00 00 00 03 77 77 77 03 66 72 64 03 75  .....w ww.frd.u
0040  74 6e 03 65 64 75 02 61 72 00 00 ff 00 01      tn-edu-a .....
```

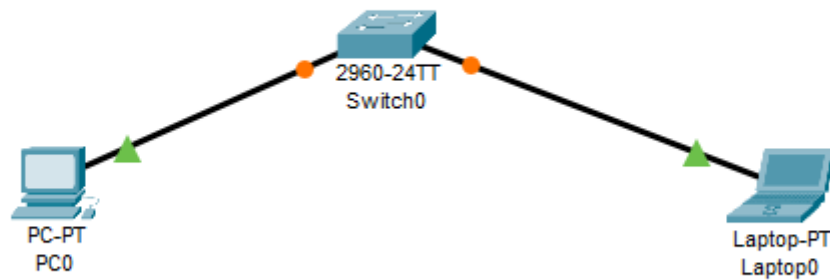
```
Additional RRs: 0
Queries
  www.frd.utn.edu.ar: type ANY, class IN
    Name: www.frd.utn.edu.ar
    [Name Length: 18]
    [Label Count: 5]
    Type: * (A request for all records the server/cache has available) (255)
    Class: IN (0x0001)
    [Response In: 180]
```

En la cual, se muestra toda la información capturada de la consulta que se realizó con el nslookup.



## Ejercicio 3

Dentro del Packet tracer, se modela la siguiente red:



Se asigna una dirección IP y una mascara de red a la PC-PT:

Physical Config **Desktop** Programming Attributes

**IP Configuration** [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.24.21

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:43FF:FE84:A4A9

Default Gateway:

DNS Server:

802.1X

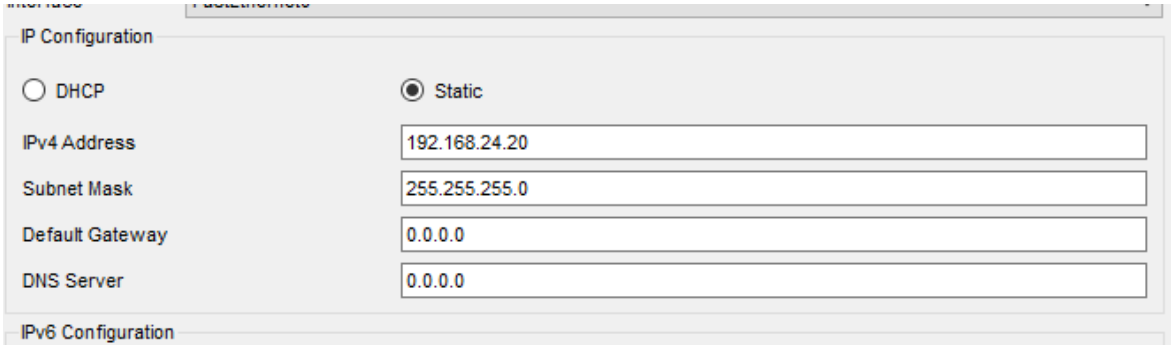
☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

Se le asigna una dirección IP y una máscara de subred a la Laptop-PT



IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.24.20

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

Luego, como cada sistema terminal tiene una dirección IP y una máscara de subred asignada, podemos establecer una comunicación entre ambos. Para corroborar que la conexión es exitosa, desde el command prompt de cualquiera de los sistemas terminales se realiza la ejecución del comando *ping* hacia la dirección IP del otro sistema terminal en la red. Entonces, se obtiene, desde la command prompt de PC-PT

```
C:\>ping 192.168.24.20

Pinging 192.168.24.20 with 32 bytes of data:

Reply from 192.168.24.20: bytes=32 time=6ms TTL=128
Reply from 192.168.24.20: bytes=32 time<1ms TTL=128
Reply from 192.168.24.20: bytes=32 time=3ms TTL=128
Reply from 192.168.24.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.24.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>|
```

Confirmando que la conexión entre los sistemas terminales es exitosa.

## Conclusión.

Gracias al trabajo de introducción, se pudo obtener una visión práctica de los comandos de consola estudiados teóricamente, además del conocimiento de dos herramientas tales como Wireshark y Packet Tracer, que nos permiten un estudio más profundo de la red. Además, mediante esta práctica pude comprender mejor los conceptos teóricos tratados (como puede ser dirección IP, máscara de subred y default Gateway, tiempo de latencia, DNS) y verlos en un contexto de red real y funcional.