

Informe de Laboratorio N°1



**UNIVERSIDAD DISTRITAL**  
**FRANCISCO JOSÉ DE CALDAS**

Michael Daniel Hernández O – 20202578071

Laura Catalina Laiton P - 20202578127

Gestión de redes telemáticas

Diego Fernando Huertas

Universidad Distrital Francisco José de Caldas

21 de febrero del 2024.

## Contenido

Introducción .....	3
Objetivos .....	4
<i>Principal</i> .....	4
<i>Secundarios</i> .....	4
Marco teórico .....	4
Topología de red .....	8
Desarrollo de laboratorio .....	9
Validación de una MAC (Media Access Control) .....	9
Desarrollo de la Simulación de Red.....	13
Pruebas y resultados.....	21
Conclusiones .....	23
Bibliografía .....	25

## **Introducción**

Las redes telemáticas son sistemas de comunicación que permiten la transferencia de datos entre dispositivos ubicados en diferentes lugares de la tierra. Estas redes posibilitan la interconexión de computadoras y otros dispositivos electrónicos para compartir recursos, como archivos, impresoras, aplicaciones y acceso a Internet.

Las redes telemáticas abarcan una amplia gama de tecnologías y protocolos, desde redes locales (LAN) hasta redes de área extensa (WAN) e incluso la Internet global.

Sin embargo, a lo largo del tiempo la implementación de estos avances también evoluciono por esto se creó un modelo recomendado para la operabilidad de estas conexiones a nivel mundial, por esto este modelo genero una parte importante en la cuestión conectividad global.

Por ello veremos cómo es que las redes se han desarrollado en una parte importante de este modelo, por esto no enfocaremos en la Capa 2 del modelo OSI, esta ha experimentado avances significativos para mejorar la eficiencia, la seguridad y la interoperabilidad de las comunicaciones de red. Algunos de estos avances incluyen nuevos protocolos y dispositivos para llevar a cabo estas conexiones de manera más eficiente.

El desarrollo de estas tecnologías trajo consigo un número de nuevas ventanas como Protocolos de Acceso al Medio Mejorados, Virtual LANs, protocolos de redes definidas por software, evolución en las conexiones wifi, en resumen, la Capa 2 del modelo OSI ha evolucionado junto con las redes telemáticas para satisfacer las crecientes demandas de conectividad, velocidad y seguridad en un entorno cada vez más interconectado.

## Objetivos

### *Principal*

Conocer los principios básicos en torno a las redes telemáticas y como son manejadas por los dispositivos conocidos como swiches en la capa 2 del modelo OSI, con la ayuda de herramientas virtuales como lo es el Packet Tracer de Cisco.

### *Secundarios*

- Aclararemos las propiedades de los switches y como se implementan las MAC (Media Access Control) para realizar conexiones entre dispositivos.
- Observaremos las propiedades de las MAC y la verificaremos virtualmente.
- Estableceremos las pautas básicas para la simulación de procesos de interconexión de dispositivos por medio de la herramienta “Packet-Tracer”, realizando un ejemplo práctico.

## Marco teórico

**Red Telemática:** Una red telemática es un sistema de comunicación que permite la transferencia de datos entre dispositivos ubicados en diferentes lugares geográficos. Estas redes facilitan la interconexión de computadoras y otros dispositivos electrónicos para compartir recursos y comunicarse entre sí. En una red telemática, los dispositivos pueden ser computadoras, servidores, teléfonos inteligentes, tabletas, dispositivos IoT (Internet de las cosas), entre otros.

Estos dispositivos pueden estar conectados mediante cables (redes cableadas) o de forma inalámbrica (redes inalámbricas) a través de tecnologías como Ethernet, Wi-Fi, Bluetooth, y 5G, entre otras.

**Modelo OSI:** El modelo OSI (del inglés Open Systems Interconnection o interconexión de sistemas abiertos) es un marco de trabajo conceptual que define cómo se comunican los sistemas de redes y cómo se envían datos de un remitente a un destinatario. El modelo se usa para describir los componentes de la comunicación de datos, para poder establecer reglas y estándares acerca de las aplicaciones y la infraestructura de red. El modelo OSI contiene siete capas que se apilan (conceptualmente) de abajo a arriba. Las capas OSI son: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

**Capa 2:** Nivel de Enlace de Datos, esta capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

**Switch:** Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3). La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch NO proporciona por sí solo conectividad con otras redes, y obviamente, TAMPOCO proporciona conectividad con Internet. Para ello es necesario un router.

**MAC:** La dirección MAC es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos como tu Chromecast. Sus siglas vienen del inglés, y significan Media Access Control. Como hay dispositivos con diferentes tarjetas de red, como una para Wifi y otra para Ethernet, algunos pueden tener diferentes direcciones MAC dependiendo de por dónde se conecten. Las direcciones MAC se forman por 48 bits representados por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios ( $48:4=12$ ), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guion o nada en absoluto. Así, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.

**Packet Tracer:** Cisco Packet Tracer es una herramienta de simulación multiplataforma, diseñada por Cisco Systems, que te va a permitir crear distintas simulaciones del funcionamiento o instalación de redes de telecomunicaciones e informáticas de Cisco. Este software permite a los usuarios simular distintos tipos de configuraciones para routers o conmutadores de Cisco mediante una interfaz de comandos simulada. En su interfaz, Cisco Packet Tracer emplea un sistema intuitivo y sencillo de usar que consiste en arrastrar y soltar, lo que permite que podamos añadir y quitar dispositivos de red como mejor nos parezca.

**IP:** La internet protocol address, es decir, la dirección IP o simplemente IP, se basa en el protocolo de Internet, que es, además, la base del funcionamiento de Internet. Se trata de la

dirección inequívoca de un dispositivo (por ejemplo, de un ordenador, de un servidor web o de una impresora) en una red interna o externa. Una dirección IP puede referirse también a un conjunto de dispositivos, como en el caso del broadcasting o del multicasting. Del mismo modo, a un único ordenador pueden asignársele varias direcciones IP. Lo que es seguro es que cada dirección IP de una red solo puede asignarse una vez al mismo tiempo.

**Consola:** La consola de PC es la interfaz que permite a los usuarios comunicarse con la computadora y ejecutar diversas tareas, como la gestión del sistema operativo, la ejecución de programas y la configuración de ajustes, todo por medios de ordenes o comandos.

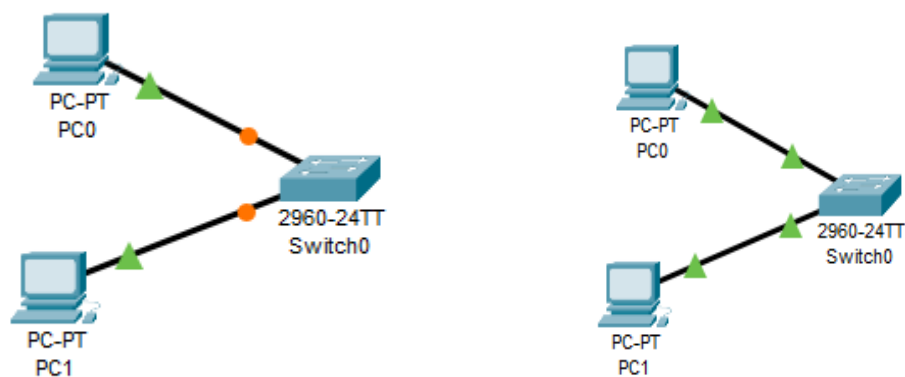
**Comando:** Es una instrucción específica que se proporciona a una computadora o sistema informático para que realice una tarea determinada. Los comandos pueden ser emitidos por un usuario directamente a través de una interfaz de línea de comandos (CLI por sus siglas en inglés) o indirectamente a través de programas de software que ejecutan comandos en segundo plano.

**Prueba ping:** Ping es una herramienta de diagnóstico que permite al usuario verificar que existe una dirección IP en particular y puede aceptar solicitudes. Una “ping test” (prueba de ping) ayuda a rastrear la comunicación entre la computadora y el router o cualquier dispositivo conectado a la red. El comando ping también se puede usar para la resolución de problemas para probar la conectividad y medir el tiempo de respuesta. Realizar una prueba de ping como parte de sus pasos de solución de problemas lo ayudará en gran medida a resolver problemas de conectividad para las computadoras con cable e inalámbricas.

## Topología de red

Se realizará una topología de red en estrella en la que el switch sea el elemento central en el que están conectados todos los nodos o dispositivos pertenecientes a la red. Esta red estará compuesta por un Switch0 2960-24TT y dos computadores como dispositivos de salida los cuales serán PC0 y PC1. Esta configuración es bastante común en redes de área local (LAN)

En esta topología cada nodo (computadoras, impresoras, etc) está conectado directamente al servidor central que en esta simulación es el switch al cual van conectados nuestros los dos PC de la red. El switch actúa como un punto focal con el cual los nodos se comunican de manera directa individualmente, este switch recibe paquetes de datos de cualquiera de los dos PC y los reenvía al otro PC conectado funcionando como servidor para controlar y gestionar las funciones de la red.





## **Desarrollo de laboratorio**

Como vimos anteriormente un concepto que manejaremos es el de la MAC (Media Access Control), veremos cómo funciona y como es que está compuesta, para poder ver sus características y así mismo aprenderemos a como acceder a este código, por medio de la consola de Windows empleando varios comandos los cuales iremos viendo.

Aprenderemos las capacidades de las redes empleando un pequeño ejemplo de simulación y configuración de una red básica, con topología muy básica, sin embargo, observaremos como podremos configurar una red domestica aplicando configuraciones y protocolos de red en la capa de enlace de datos o de red.

### **Validación de una MAC (Media Access Control)**

Inicialmente veremos qué es y cómo es la estructura básica de una dirección MAC y como consultarla en un sistema operativo de Microsoft.

Las siglas de la dirección MAC vienen de Media Access Control, aunque en español también se la conoce como dirección física, y su función básica radica en identificar una tarjeta de red de forma global. Este número es único y exclusivo para identificar tarjetas de red, puesto que son las encargadas de enviar y recibir información del exterior. La estructura de una dirección MAC sigue un formato específico y consta de seis bytes (48 bits) representados en formato hexadecimal.

Es un número hexadecimal de 48 bits separados en 6 bloques de 8 bits. Los primeros 3 bloques identifican al fabricante de la tarjeta, los 3 últimos es un número identificativo gestionado por la IEEE.

## Dirección MAC

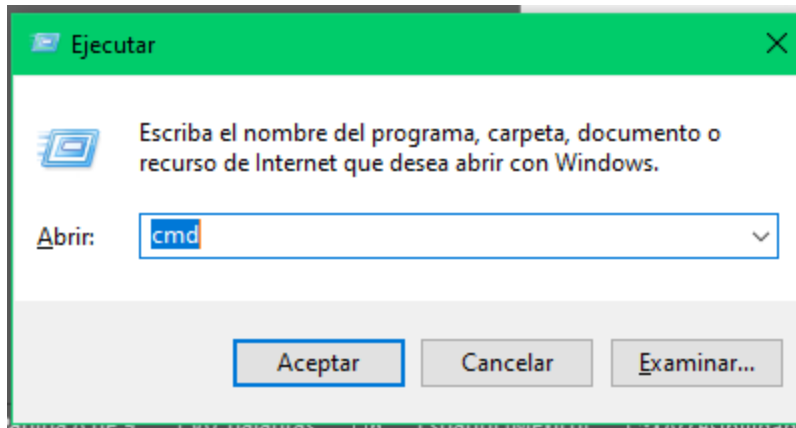
**01:3A:1D:54:6B:32**

Identificador del fabricante   Identificador del producto

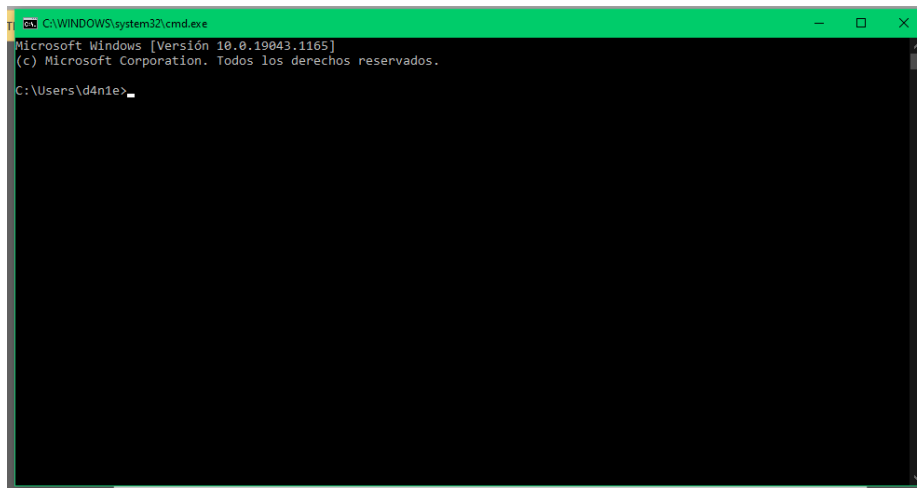
En resumen, la estructura de una dirección MAC sigue un formato específico de seis bytes (48 bits) representados en formato hexadecimal, con los primeros tres bytes identificando al fabricante del dispositivo y los siguientes tres bytes identificando de manera única el dispositivo dentro de su rango de asignación.

### *¿Cómo la consulto en mi pc?*

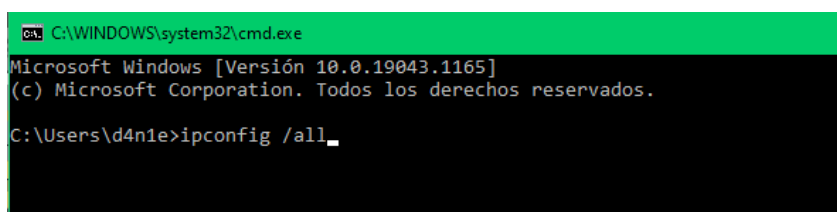
- Inicialmente oprimimos la tecla WIN + R:
- Nos aparece el recuadro de “Ejecutar”, en la barra de búsqueda escribimos CMD, lo que nos traduce a la consola o terminal del sistema operativo



Una vez en la terminal:



- Ingresamos las palabras “ipconfig /all”, ingresándolas en la consola por el teclado (importante que sean en el mismo orden), y luego damos la tecla “Enter” esto se conoce como comando.



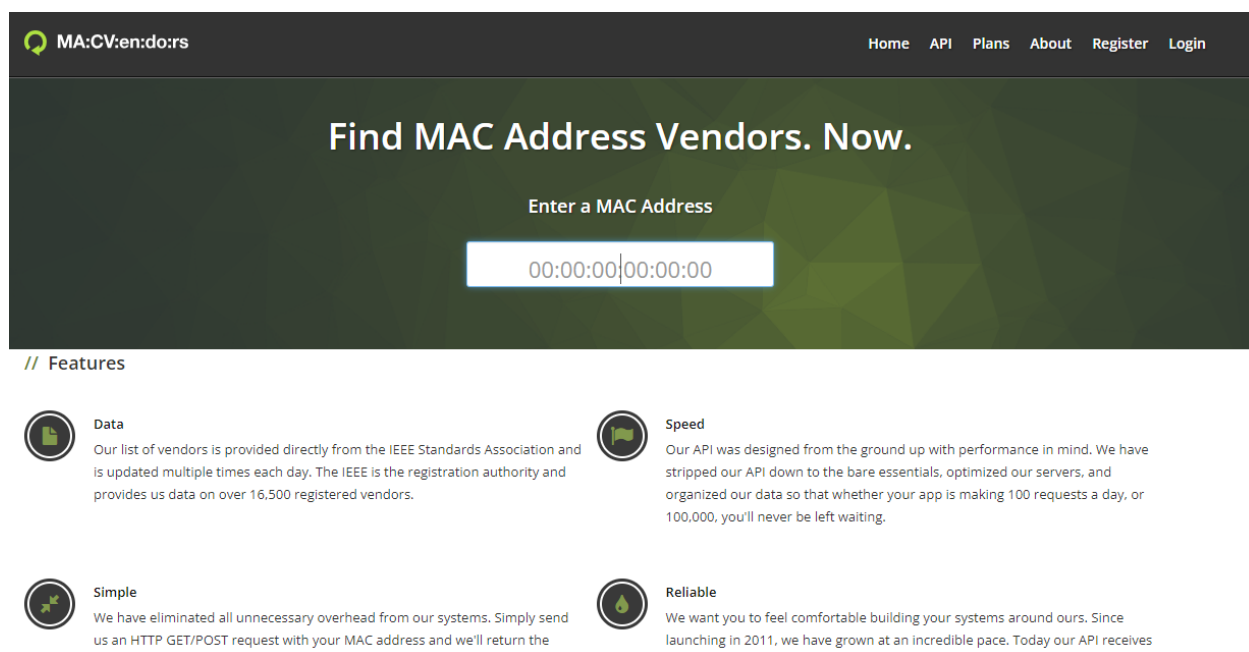
- Nos cargara una información acerca de nuestro computador en la pantalla de la consola, buscaremos el que indica “Dirección física”, este serial corresponde a la dirección MAC de nuestro equipo.

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Dirección física. . . . . : 4E-EB-BD-03-13-E3
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
```

Esta sería la dirección física del dispositivo que se consultó, en este caso una laptop.

- Para el siguiente paso debemos ingresar a la web a la dirección:  
<https://macvendors.com>.

Donde nos cargara la siguiente página web:




MA:CV:en:do:rs Home API Plans About Register Login

## Find MAC Address Vendors. Now.


Enter a MAC Address

### // Features




**Data**

Our list of vendors is provided directly from the IEEE Standards Association and is updated multiple times each day. The IEEE is the registration authority and provides us data on over 16,500 registered vendors.




**Speed**

Our API was designed from the ground up with performance in mind. We have stripped our API down to the bare essentials, optimized our servers, and organized our data so that whether your app is making 100 requests a day, or 100,000, you'll never be left waiting.



**Simple**

We have eliminated all unnecessary overhead from our systems. Simply send us an HTTP GET/POST request with your MAC address and we'll return the



**Reliable**

We want you to feel comfortable building your systems around ours. Since launching in 2011, we have grown at an incredible pace. Today our API receives

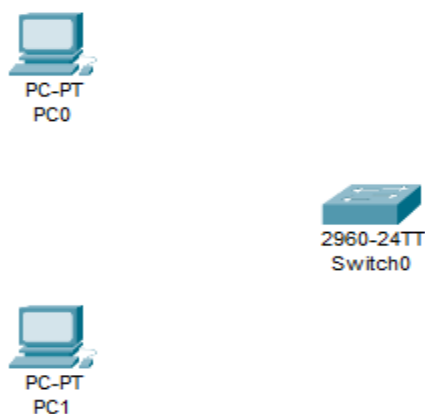
- Desde la consola copiamos los dígitos que corresponden a la MAC y los pegamos en el cuadro de búsqueda de la página web a la que ingresamos anteriormente.



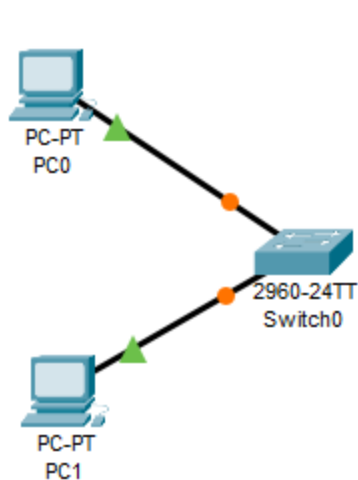
En consecuencia, nos cargara el proveedor de la MAC en este caso es una empresa china, la encargada de ensamblar esta parte para la computadora usada en el ejemplo.

### Desarrollo de la Simulación de Red

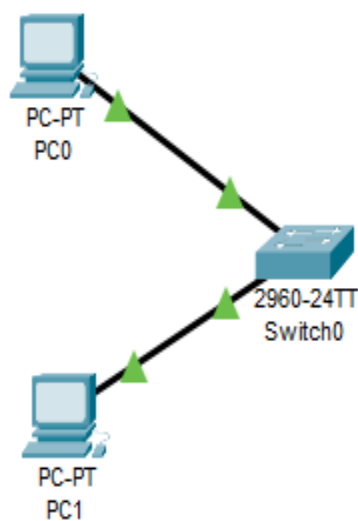
1. Se usarán dos PC llamados PC0 y PC1 respectivamente además de un switch que funcionara como intermediario entre los dos además de como punto central de toda la red.



2. Los dos PC se conectarán al Switch para que de esta forma al ser intermediario los dos PC queden conectados también entre sí. Esto hará que se genere la conexión entre los tres elementos de la red



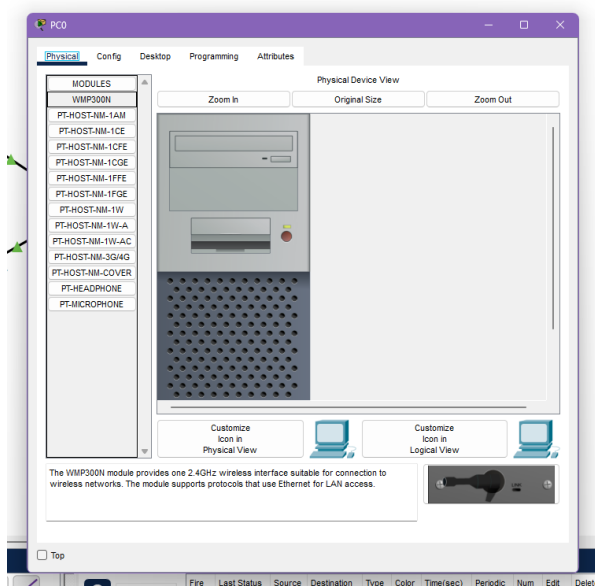
Conectando



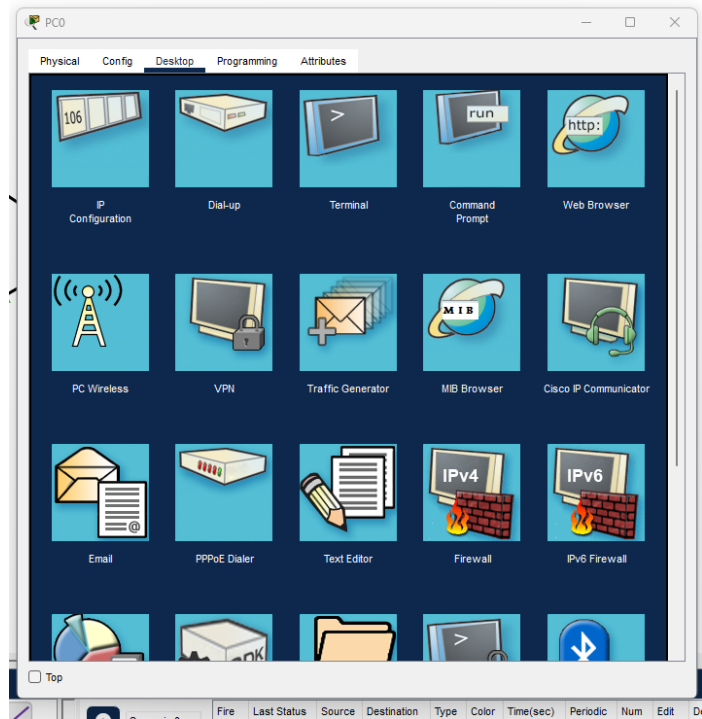
Conectado

3. A continuación, configuramos la dirección IP de los PC de la siguiente manera:

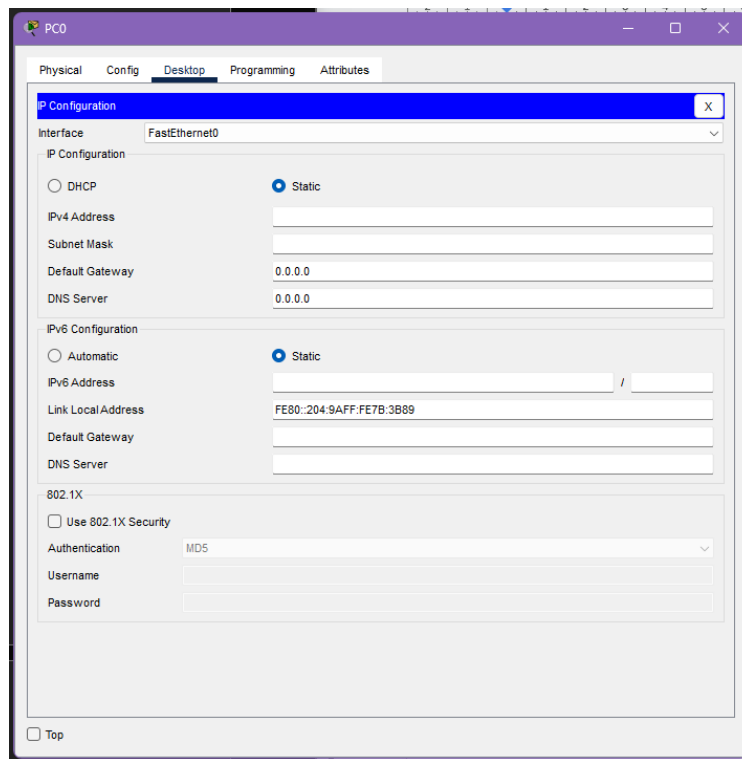
- Damos clic en el pc que deseamos configurar para que nos abra la ventana correspondiente



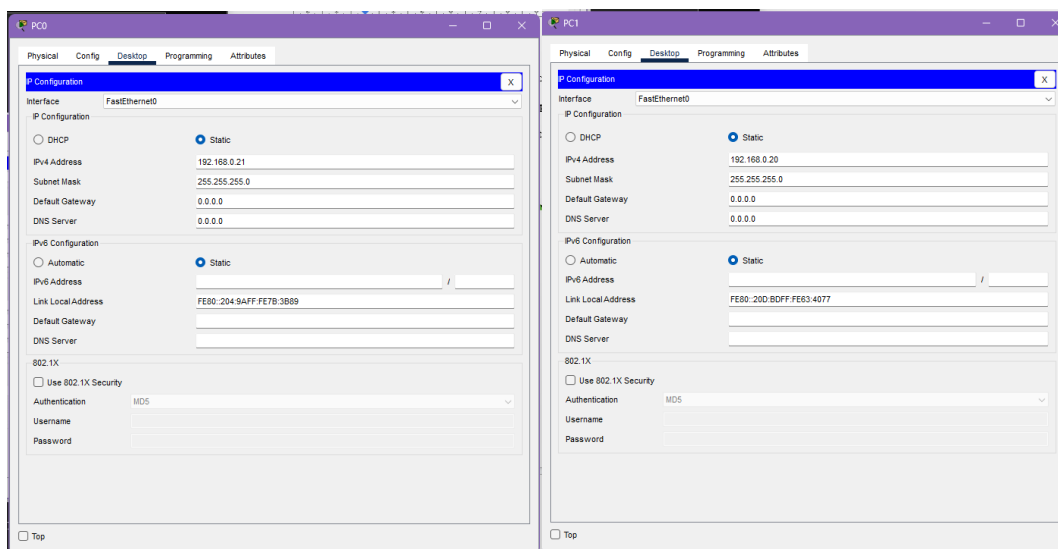
- En la parte superior de esta ventana iremos a la pestaña “Desktop”



- Una vez allí daremos clic en el botón “IP Configuration”



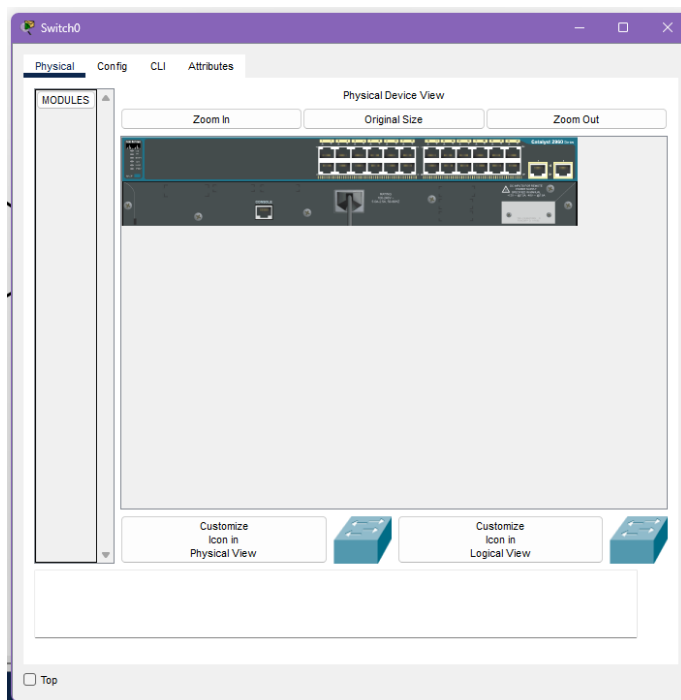
- En la casilla de “IPv4 Address” ingresaremos el IP “192.168.0.21” para el PC0 y “192.168.0.20” para el PC1.



PC0

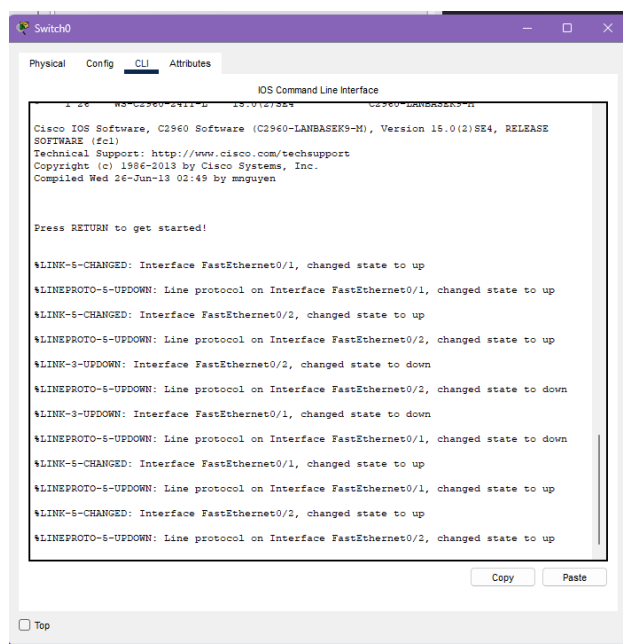
PC1

- Seguido a esto cerraremos la ventana de configuración del PC y daremos click en el switch para abrir la ventana correspondiente a este





- Ya dentro de la ventana iremos a la pestaña “CLI” en la parte superior.



Al ingresar a CLI ingresamos en modo no privilegiado o modo usuario que es el modo de operación inicial al conectarse a un dispositivo Cisco, el indicador de comandos muestra un símbolo de mayor que “>” y solo tenemos acceso a comandos y funciones limitados. Como se requiere el acceso a comandos más avanzados tendremos que pasar a modo “Enable o modo privilegiado” para poder realizar las configuraciones.

- Dentro de la consola de comandos que encontramos en la pestaña “CLI” daremos Enter para ingresar en modo usuario

```

IOS Command Line Interface

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch>

```

- Dentro de la línea de comandos escribiremos “Enable” para ingresar en el modo privilegiado o modo enable, en el momento en que ingresemos en este modo lo sabremos porque se remplazara el símbolo de mayor que (>) por el símbolo de numeral (#) para distinguir uno del otro

```

Switch>enable
Switch#

```

- Para saber la versión del sistema operativo ingresamos el comando “show versión”

```

Switch Ports Model          SW Version  SW Image
-----
*    1 26    WS-C2960-24TT-L  15.0(2)SE4  C2960-LANBASEK9-M

Configuration register is 0xF

```

- Para conocer el estado de la interfaz usaremos el comando “show interface status”, aquí podremos observar que los dos PC están conectados al switch

```
Switch#show interface status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa0/1     connected  1           auto      auto    10/100BaseTX
Fa0/2     connected  1           auto      auto    10/100BaseTX
Fa0/3     notconnect 1           auto      auto    10/100BaseTX
Fa0/4     notconnect 1           auto      auto    10/100BaseTX
Fa0/5     notconnect 1           auto      auto    10/100BaseTX
Fa0/6     notconnect 1           auto      auto    10/100BaseTX
Fa0/7     notconnect 1           auto      auto    10/100BaseTX
Fa0/8     notconnect 1           auto      auto    10/100BaseTX
Fa0/9     notconnect 1           auto      auto    10/100BaseTX
Fa0/10    notconnect 1           auto      auto    10/100BaseTX
Fa0/11    notconnect 1           auto      auto    10/100BaseTX
Fa0/12    notconnect 1           auto      auto    10/100BaseTX
Fa0/13    notconnect 1           auto      auto    10/100BaseTX
Fa0/14    notconnect 1           auto      auto    10/100BaseTX
Fa0/15    notconnect 1           auto      auto    10/100BaseTX
Fa0/16    notconnect 1           auto      auto    10/100BaseTX
Fa0/17    notconnect 1           auto      auto    10/100BaseTX
Fa0/18    notconnect 1           auto      auto    10/100BaseTX
Fa0/19    notconnect 1           auto      auto    10/100BaseTX
Fa0/20    notconnect 1           auto      auto    10/100BaseTX
Fa0/21    notconnect 1           auto      auto    10/100BaseTX
--More--
```

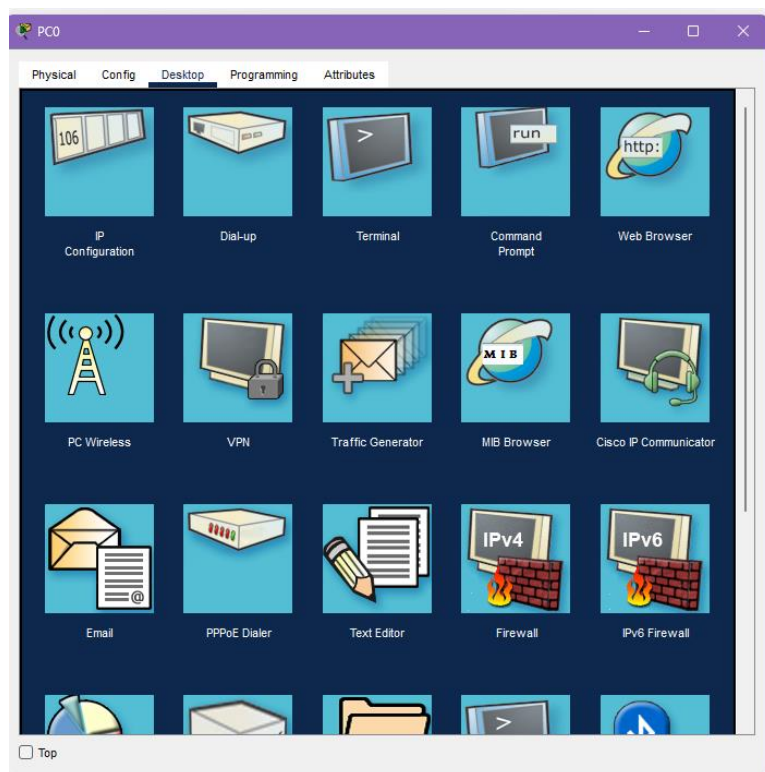
- A continuación, configuraremos el nombre de la terminal, para esto ingresaremos el comando “configure terminal” que nos pedirá saber que queremos configurar, en este caso como es el nombre usaremos “hostname” seguido del nombre que deseemos ponerle, en nuestro caso le pondremos “LAB1”. Al dar Enter podremos ver que la terminal nos da el nombre que ingresamos.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname LAB1
LAB1(config)#
```

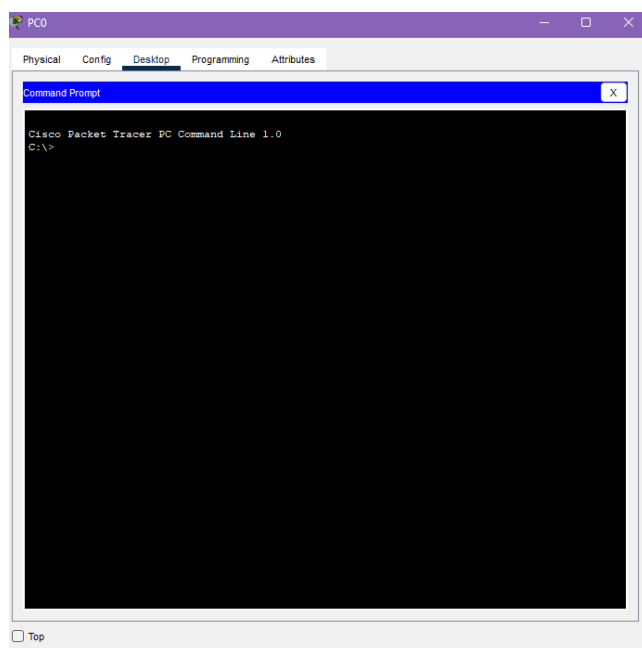
- Para finalizar saldremos y guardaremos la configuración con los comandos “exit” y “wr” respectivamente.

```
LAB1(config)#exit
LAB1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
LAB1#
```

- Continuaremos cerrando la ventana y dando click de nuevo en cada uno de los PC para abrir la ventana de cada uno.



- Esta vez daremos click en el botón “Command Prompt” para comprobar el ping de cada PC



- Ingresaremos el comando “ping -t 192.168.0.21” para el PC0 y “ping -t 192.168.0.20” para el PC1 debido a que son sus IP correspondientes y saldremos de la ejecución con ctrl+c para comprobar que el PC está recibiendo la información adecuadamente

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 192.168.0.21

Pinging 192.168.0.21 with 32 bytes of data:
Reply from 192.168.0.21: bytes=32 time<1ms TTL=128
Reply from 192.168.0.21: bytes=32 time=8ms TTL=128
Reply from 192.168.0.21: bytes=32 time<1ms TTL=128
Reply from 192.168.0.21: bytes=32 time=8ms TTL=128
Reply from 192.168.0.21: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.21:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 3ms

Control-C
^C
C:\>

```

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:
Reply from 192.168.0.20: bytes=32 time=2ms TTL=128
Reply from 192.168.0.20: bytes=32 time=8ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time=8ms TTL=128
Reply from 192.168.0.20: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.0.20:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 5ms

Control-C
^C
C:\>

```

Ping PC0

Ping PC1

- Cerraremos la ventana para dar clic de nuevo en el switch e ingresaremos el comando “show mac address-table” para asegurarnos de que los dos PC estén conectados correctamente al switch

```

LAB1#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0004.9a7b.3b89   DYNAMIC Fa0/1
1       000d.bd63.4077   DYNAMIC Fa0/2
LAB1#

```

## Pruebas y resultados

- Ingreso correcto al modo enable o modo privilegiado

```

Switch>enable
Switch#

```

- Conexión correcta de los PC al switch

```
Switch#show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	1	auto	auto	10/100BaseTX
Fa0/2		connected	1	auto	auto	10/100BaseTX
Fa0/3		notconnect	1	auto	auto	10/100BaseTX
Fa0/4		notconnect	1	auto	auto	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9		notconnect	1	auto	auto	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11		notconnect	1	auto	auto	10/100BaseTX
Fa0/12		notconnect	1	auto	auto	10/100BaseTX
Fa0/13		notconnect	1	auto	auto	10/100BaseTX
Fa0/14		notconnect	1	auto	auto	10/100BaseTX
Fa0/15		notconnect	1	auto	auto	10/100BaseTX
Fa0/16		notconnect	1	auto	auto	10/100BaseTX
Fa0/17		notconnect	1	auto	auto	10/100BaseTX
Fa0/18		notconnect	1	auto	auto	10/100BaseTX
Fa0/19		notconnect	1	auto	auto	10/100BaseTX
Fa0/20		notconnect	1	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	10/100BaseTX

```
--More--
```

- Hostname configurado correctamente

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname LAB1
LAB1(config)#
```

- Configuración guardada

```
LAB1(config)#exit
LAB1#
%SYS-5-CONFIG_I: Configured from console by console
w
Building configuration...
[OK]
LAB1#
```

- Los PC están recibiendo adecuadamente la información

<pre>Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ping -t 192.168.0.21  Pinging 192.168.0.21 with 32 bytes of data:  Reply from 192.168.0.21: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.0.21: bytes=32 time=8ms TTL=128 Reply from 192.168.0.21: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.0.21: bytes=32 time=8ms TTL=128 Reply from 192.168.0.21: bytes=32 time&lt;1ms TTL=128  Ping statistics for 192.168.0.21:     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 8ms, Average = 3ms  Control-C ^C C:\&gt;</pre>	<pre>Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ping -t 192.168.0.20  Pinging 192.168.0.20 with 32 bytes of data:  Reply from 192.168.0.20: bytes=32 time=2ms TTL=128 Reply from 192.168.0.20: bytes=32 time=8ms TTL=128 Reply from 192.168.0.20: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.0.20: bytes=32 time=8ms TTL=128 Reply from 192.168.0.20: bytes=32 time=9ms TTL=128  Ping statistics for 192.168.0.20:     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 9ms, Average = 5ms  Control-C ^C C:\&gt;</pre>
---	---

- Conexión de los PC al Switch comprobada por medio del comando “mac address-table”

```
LAB1#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0004.9a7b.3b89    DYNAMIC     Fa0/1
1       000d.bd63.4077    DYNAMIC     Fa0/2
LAB1#
```

- En este caso como las direcciones MAC ya están registradas en la tabla de direcciones, esto nos indica que los dispositivos están conectados correctamente, esto se valida con la prueba ping realizada con anterioridad.

## Conclusiones

- Se pudieron conocer los comandos básicos usados en “packet tracer” por medio de la creación de una simulación sencilla de redes que nos deja claros los pasos a seguir y como es que se generan las conexiones entre los elementos de la red.
- Al realizar comprobaciones virtuales y en “packet tracer” de cada uno de los procesos que se llevaron a cabo, se despejaron dudas con respecto a el funcionamiento de cada código y el porqué de cada paso realizado dentro del laboratorio.
- El software empleado nos da muchas facilidades al momento de conocer las herramientas que son necesarias para la comprensión de una red telemática, y así mismo poderla implementar en un proyecto concreto.

- El ejemplo práctico realizado para el laboratorio dio las bases necesarias para que se pueda generar una simulación con resultados satisfactorios que ayudaron al cumplimiento del objetivo de aprendizaje.
- Con la ayuda del software la conexión de los dispositivos y el manejo de estos fue más intuitiva



## Bibliografía

- Movildata. (2020, April 7). *¿Qué es la telemática?* Movildata; MovilData.  
<https://movildata.com/recursos/que-es-la-telematica/>
- ¿Qué es el modelo OSI? (2023, May 2). Proofpoint.  
<https://www.proofpoint.com/es/threat-reference/osi-model>
- Capa 2: Nivel Enlace de datos – Todo de Redes. (2018). Tododeredes.com.  
<https://tododeredes.com/modelo-osi/capa-2/>
- Switch, Routers y Acces Point Conceptos Generales Switch. (n.d.).  
[https://www.trabajosocial.unlp.edu.ar/uploads/docs/switch\\_routers\\_y\\_acces\\_point\\_conceptos\\_generales.pdf](https://www.trabajosocial.unlp.edu.ar/uploads/docs/switch_routers_y_acces_point_conceptos_generales.pdf)
- Yúbal Fernández. (2017, October 6). Qué es la dirección MAC de tu ordenador, del móvil o de cualquier dispositivo. Xataka.com; Xataka Basics.  
<https://www.xataka.com/basics/que-es-la-direccion-mac-de-tu-ordenador-del-movil-o-de-cualquier-dispositivo>
- Esteban Canle Fernández. (2021, March 13). Principales funciones de Cisco Packet Tracer | Tokio. Tokio School. <https://www.tokioschool.com/noticias/cisco-packet-tracer/>
- Qué es la dirección MAC. (2020, May 12). Odisea Geek; Odisea Geek.  
<https://odiseageek.es/posts/que-es-la-direccion-mac/>
- Getting Started with Cisco Packet Tracer - Skills for All. (2024). Skillsforall.com.  
[https://skillsforall.com/es/course/getting-started-cisco-packet-tracer?utm\\_source=netacad.com&utm\\_medium=referral&utm\\_campaign=packet-tracer&courseLang=es-XL&userlogin=0](https://skillsforall.com/es/course/getting-started-cisco-packet-tracer?utm_source=netacad.com&utm_medium=referral&utm_campaign=packet-tracer&courseLang=es-XL&userlogin=0)
- Cisco Packet Tracer - Networking Simulation Tool. (2020, March 24). Networking Academy. <https://www.netacad.com/es/courses/packet-tracer>