

# SOC (Security Operations Center)

## Módulo 3



## Networking – Cisco

### Ejercicios

Sheila Fernández Cisneros – 11/06/2024

## Instrucciones comunes para todos los ejercicios

Una vez completados todos los pasos, se debe hacer click en “Check Results”, navegar hasta la pestaña “Assessment Items” y realizar una captura de pantalla de toda la ventana (se recomienda usar la combinación Windows + Shift + S para ello, en caso de que el dispositivo sea Windows), en la que se vea tanto el resultado final como el ejercicio. Por otro lado, hay que guardar el archivo (File > Save As) con el nombre: ej\_1\_1erApellido\_Nombre.pka

## Tarea 1: Configuración de cliente y enrutador inalámbrico (apartado 4.4.4. del curso)

### **Packet Tracer: Configurar un enrutador inalámbrico y clientes**

#### **Objetivos**

**Parte 1: Conectar los dispositivos**

**Parte 2: Configurar el enrutador inalámbrico**

**Parte 3: Configurar el direccionamiento IP y probar la conectividad**

#### **Aspectos básicos/Situación**

Su amiga, Natsumi, escuchó que usted está estudiando redes. Le pidió que viniera y la ayudara a conectar su nuevo hogar a la red de televisión por cable. Debe conectar los cables correctos a los dispositivos correctos, conectar los dispositivos a un router inalámbrico doméstico y configurar el router para proporcionar direcciones IP a los clientes de la red. Natsumi también desea que configure una LAN inalámbrica para su red doméstica, por lo que también deberá configurarla. Usted está seguro de que este será un proceso fácil y que la red se configurará en muy poco tiempo.

#### **Instrucciones**

**Parte 1: Conectar los dispositivos.**

El área de trabajo muestra el interior de la casa de su amigo. Desplácese por la ventana para tener una idea del diseño de la casa y la ubicación de los dispositivos. En esta parte, conectará todos los dispositivos etiquetados.

#### **Paso 1: Conectar los cables coaxiales**

La empresa de cable de Natsumi ofrece servicios de Internet y video a su hogar a través de un cable coaxial. El cable está conectado a una salida en su casa. Un dispositivo divisor separa el servicio de datos de Internet del servicio de video. Esto permite que los dos servicios se conecten a los dispositivos correspondientes. Conectará el servicio de Internet al cable módem y el servicio de video al televisor.

- a. En Componentes de red, haga clic en **Conexiones** (el rayo).
- b. Busque y haga clic en el ícono del cable **coaxial**. Es el ícono azul en zigzag.
- c. Haga clic en **Cable Splitter** y seleccione el puerto **Coaxial1**.
- d. Haga clic en **Cable Modem** y seleccione **Port 0**.
- e. Repita los pasos anteriores para conectar el cable **coaxial 2** en el **divisor de cable** al **puerto 0** del televisor.
- f. Haga clic en **TV** y luego en **ON** para **Estado**. Si las conexiones son correctas, verá una imagen que representa un programa de TV.

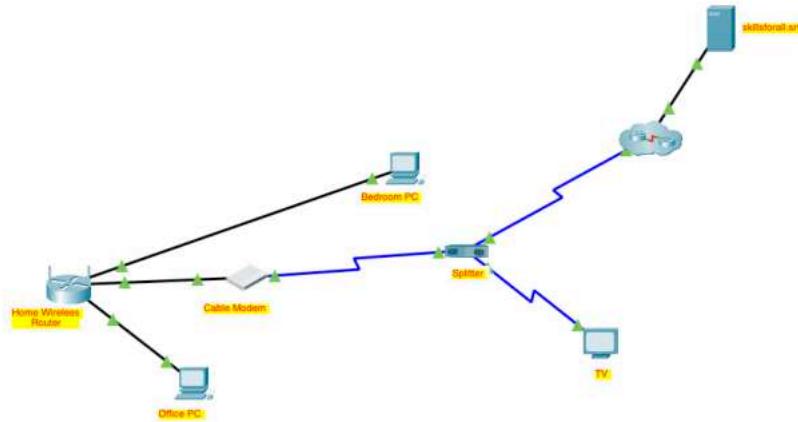
### **Paso 2: Conectar los cables de red.**

Hay dos PC en la casa de Natsumi. No tienen adaptadores LAN inalámbricos, por lo que se conectarán con cables Ethernet. El router inalámbrico doméstico es el centro de la red. Permite que los dispositivos configurados en la red doméstica se comuniquen entre sí y con Internet. El router incluye un switch de red que acepta conexiones cableadas para hasta cuatro hosts. Conectará las PC a estos puertos.

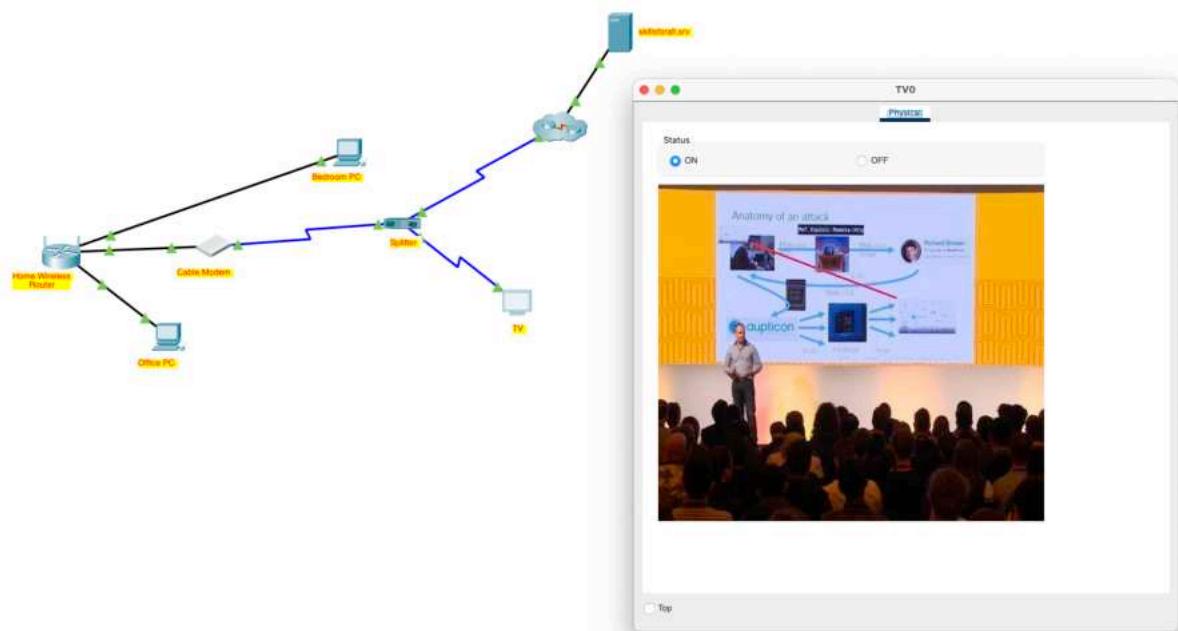
Para que el **router inalámbrico doméstico** acceda a Internet a través de la red del proveedor de televisión por cable, el cable módem debe estar conectado al puerto de Internet del router inalámbrico doméstico. Esto se hace con un cable directo de cobre.

- a. Haga clic en **Conexiones** y después en el **Cable de cobre directo**. Parece una línea negra sólida.
- b. Conecte el **puerto 1 del módem por cable** al puerto de **Internet** del **router inalámbrico doméstico**.
- c. Haga clic en la **PC de oficina** y conecte el cable al puerto **FastEthernet0**. Busque el **router inalámbrico doméstico** y haga clic en él. Conecte el otro extremo del cable al puerto **GigabitEthernet 1** para completar la conexión.
- d. Repita los pasos anteriores para conectar la **PC de dormitorio** al puerto **GigabitEthernet 2** del **router inalámbrico doméstico**.

La red doméstica cableada ahora está completamente conectada a Internet a través de la red del proveedor de televisión por cable.



Como podemos observar en la figura, se han usado cables “Ethernet” para conectar el cable modem con el router, y este último con los dos PC. Posteriormente, se ha usado un cable “coaxial” para conectar el splitter con el cable modem y la TV. Mostramos la conexión de la TV una vez conectada correctamente en la siguiente captura.



## Parte 2: Configurar el router inalámbrico

La mayoría de los routers inalámbricos domésticos se configuran mediante una interfaz gráfica de usuario (GUI) a la que se accede a través del navegador web de la computadora. En esta parte, accederá al router inalámbrico doméstico a través del navegador en la **PC de oficina** y configurará la red doméstica de Natsumi.

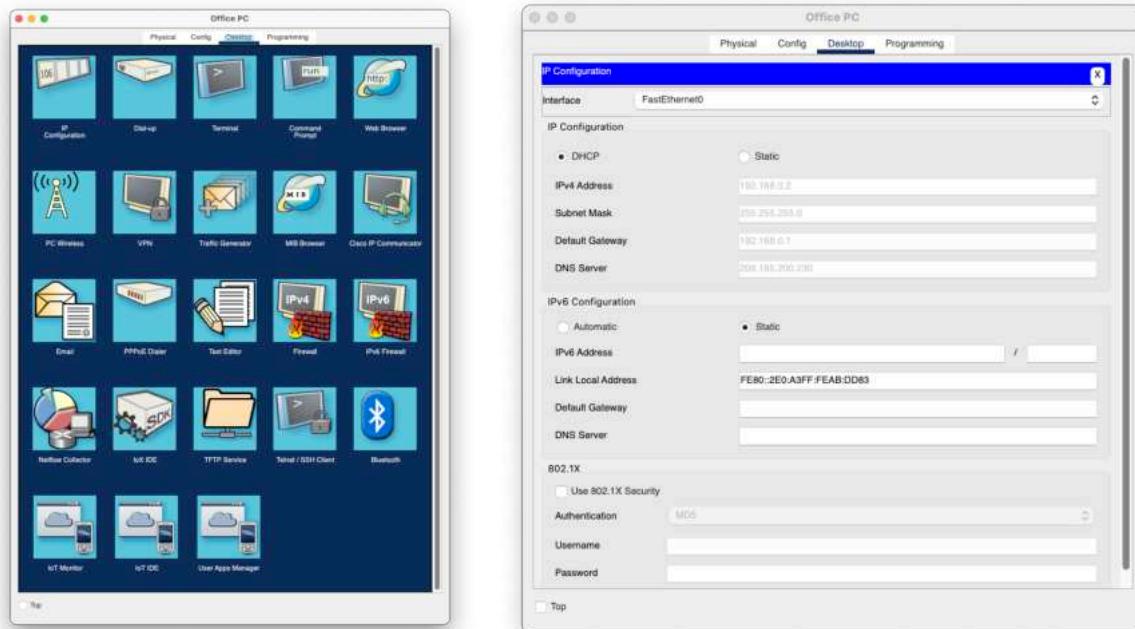
### Paso 1: Acceder a la GUI del router inalámbrico doméstico.

- Haga clic en **PC de la oficina**> pestaña **Escritorio** y luego en **Configuración de IP**.

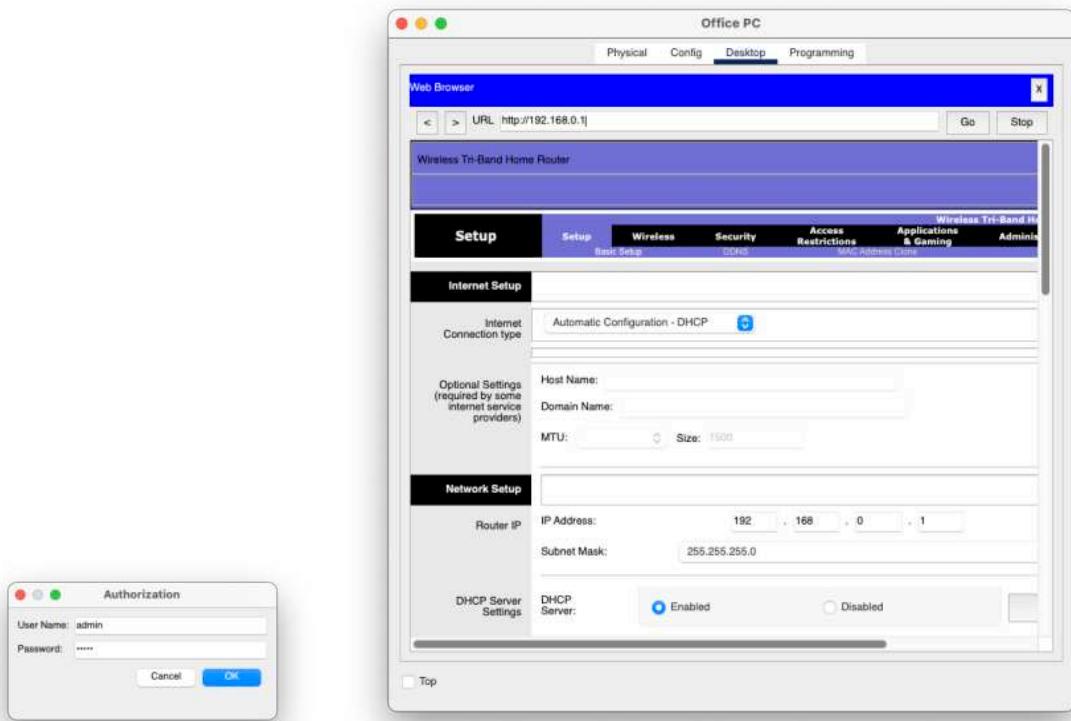
- b. Haga click en **DHCP**. DHCP configurará automáticamente la **PC de oficina** para que esté en la misma red IP que el **router inalámbrico doméstico**.
- c. Después de un breve retraso, los valores para la **configuración de IP** deben actualizarse automáticamente. La dirección IPv4 debe comenzar con el número 192. Si no es así, haga clic en **Fast Forward Time** (Tiempo de avance rápido), que se encuentra justo debajo de la topología de red en la esquina inferior izquierda. Esto acelerará la simulación de DHCP.
- d. Tome nota de la dirección de la puerta de enlace predeterminada. La puerta de enlace predeterminada es el dispositivo que proporciona a los dispositivos de la red doméstica acceso a redes externas, como Internet. En este caso, la dirección de la puerta de enlace predeterminada es la dirección del **enrutador inalámbrico doméstico**.
- e. Manteniendo la ventana de la **PC de oficina** abierta, cierre la ventana de **configuración de IP** y luego haga clic en el **navegador web**. Ingrese la dirección IP del **router inalámbrico doméstico** (la dirección de la puerta de enlace predeterminada) en el cuadro **URL** y haga clic en **Ir**.
- f. Los routers domésticos recién instalados se configuran con credenciales predeterminadas. Use **admin** tanto para el **nombre de usuario** y la **contraseña**. Ahora debería ver aparecer la GUI del **router inalámbrico doméstico** y estar listo para configurar la red de Natsumi. Ajuste el tamaño de la ventana, según sea necesario, para ver más de la interfaz.

**Nota:** Las contraseñas predeterminadas en dispositivos reales deben cambiarse inmediatamente porque es ampliamente conocido, incluyendo a los agentes de amenaza.

Seguimos los pasos que nos indica el enunciado y mostramos los resultados de los ajustes.



- Acceso al web browser: usuario: admin, contraseña: admin



## Paso 2: Configurar ajustes básicos.

En este paso, configurará un nuevo nombre de usuario y contraseña para el router inalámbrico y limitará la cantidad de direcciones IP que DHCP emitirá a hosts que estén conectadas a la red.

Natsumi solo tiene unos pocos dispositivos para conectar la red, y no tendrá muchos amigos. Ella piensa que no más de 10 dispositivos se conectarán a su red al mismo tiempo. Decide reducir el número de usuarios a 10. Su amiga vive en una parte densamente poblada de la ciudad, por lo que es posible que muchas personas puedan ver su red inalámbrica.

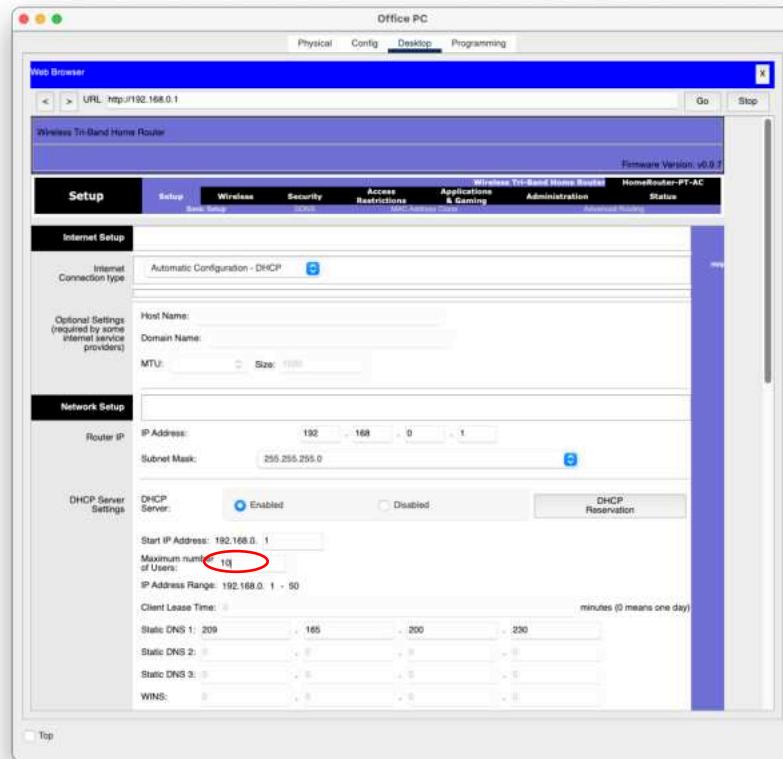
- Actualmente está viendo las opciones de configuración en la pestaña **Configuración**. Localice el área de **Network Setup** (Configuración de red). Aquí es donde puede configurar el servidor DHCP del router. Busque el campo **Número máximo de usuarios** e introduzca **10**. Desplácese hasta la parte de abajo de la página y haga clic en **Save Settings** (Guardar configuración). Debe guardar la configuración en cada página de la GUI en la que realice cambios.

**Nota:** es posible que pierda la conexión con el router. Haga clic en **Ir** en el navegador web para volver a cargar la página de la GUI. Es posible que deba cerrar el **navegador web**, hacer clic en **Configuración de IP** y alternar entre **DHCP** y **Estático** para actualizar el direccionamiento IP para **PC de oficina**. Luego verifique que la **PC de oficina** tenga una configuración de dirección IP que comience con 192, abra el **navegador web** nuevamente, ingrese la dirección IP del router y vuelva a autenticarse con **admin** como credenciales predeterminadas.

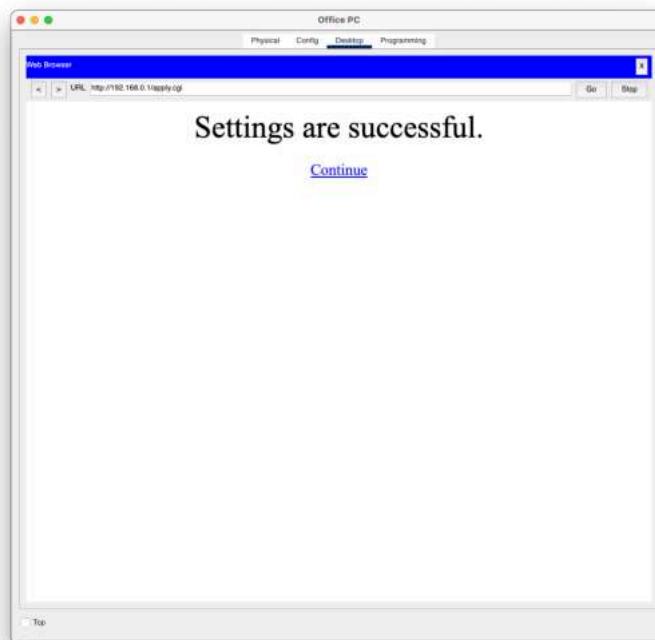
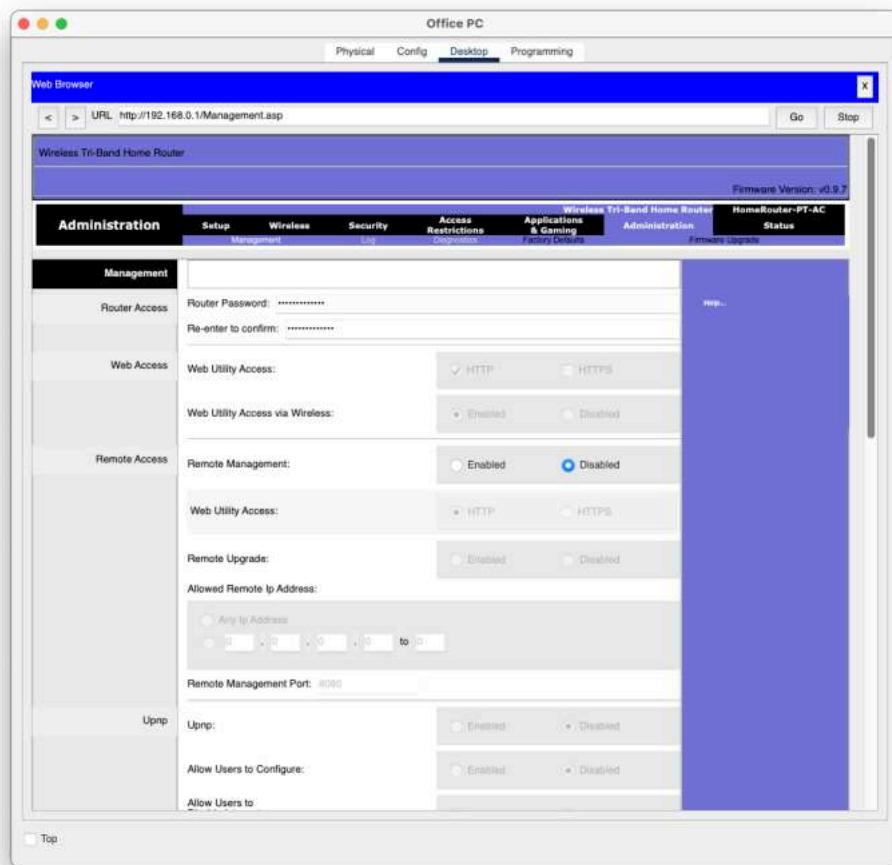
- b. Haga clic en la pestaña **administration**. Aquí, puede cambiar la contraseña **admin** predeterminada. Ingrese y confirme **MyPassword1!** como la nueva contraseña. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings** (Guardar configuración).

Se le pedirá que inicie sesión nuevamente. Ingrese **admin** como nombre de usuario y **MyPassword1!** como nueva contraseña y haga clic en **Continuar**.

- Limitamos el acceso a 10 usuarios tal y como se indica.



- Cambiamos la contraseña desde la pestaña administración.



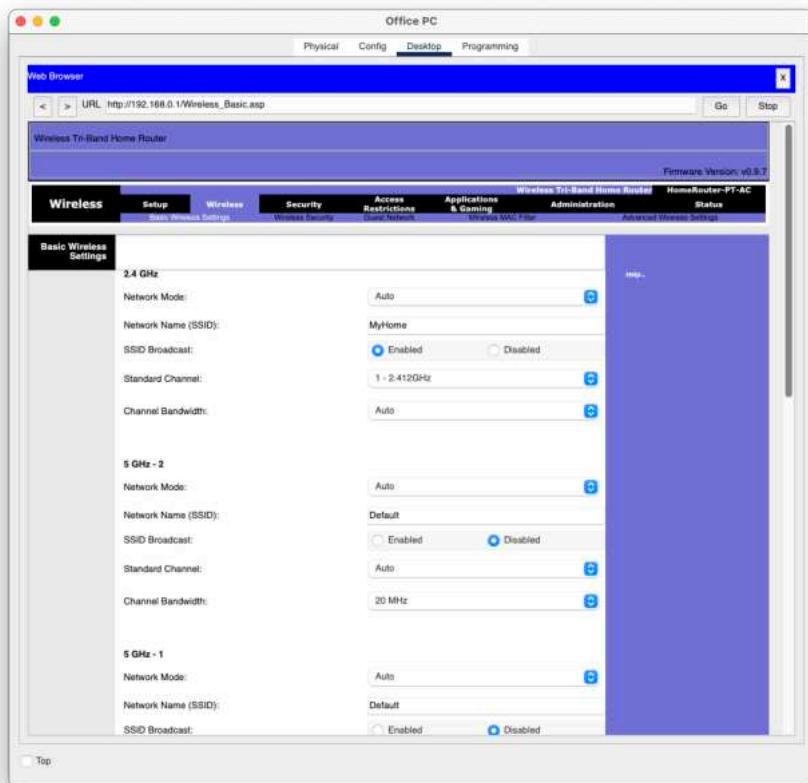
Efectivamente siguiendo los pasos marcados por el ejercicio conseguimos una conexión de forma exitosa.

### Paso 3: Configurar la LAN inalámbrica.

En este punto, está listo para configurar la red inalámbrica de Natsumi para que pueda conectar sus dispositivos inalámbricos a Internet a través de Wi-Fi.

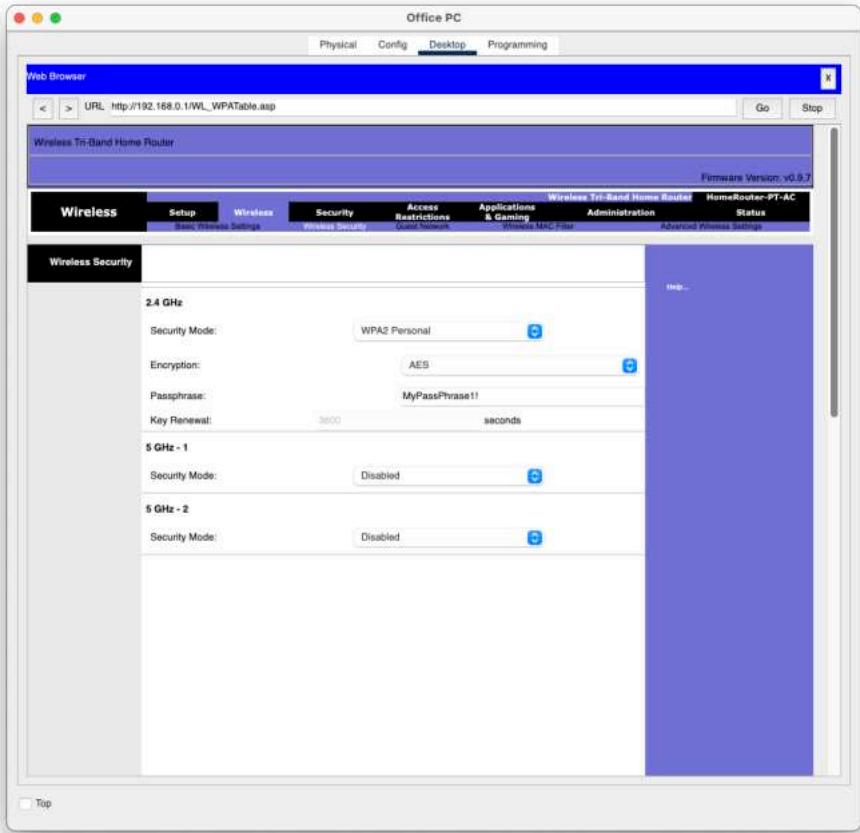
- a. Desplácese hacia la parte superior de la ventana y haga clic en la pestaña **Inalámbrico**.
- b. Para la red de **2,4 GHz**, haga clic en **Habilitar** para activar la radio de red.
- c. Cambie el **nombre de la red (SSID)** de **Default** a **MyHome**. Cuando las personas buscan redes Wi-Fi para conectarse, verán este nombre de red. El nombre de la red puede estar oculto, pero esto puede dificultar un poco la conexión de los invitados a la red. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings** (Guardar configuración).

Mostramos los resultados de establecer los ajustes que nos pide el ejercicio.



- d. Ahora configurará la seguridad en la red **MyHome**. Esto evitirá que personas no autorizadas se conecten a la red inalámbrica. Desplácese hasta la parte superior de la ventana y luego haga clic en **Seguridad inalámbrica** en la pestaña **Inalámbrico**.
- e. Tenga en cuenta que la seguridad está actualmente deshabilitada en las tres redes inalámbricas. Solo utiliza la red de **2,4 GHz**. Haga clic en el menú desplegable de la red de **2,4 GHz** y seleccione **WPA2 Personal**. Esta es la seguridad más sólida que ofrece este router para redes inalámbricas.
- f. Se revelan más configuraciones. WPA2 Personal requiere una frase de contraseña que debe introducir cualquier persona que desee conectarse a la red inalámbrica. Ingrese **MyPassPhrase1!** como la **frase de contraseña**. Tenga en cuenta que las mayúsculas son importantes.

- g. Desplácese hasta la parte inferior de la página, haga clic en **Guardar configuración** y cierre el navegador web de la PC de oficina.



### **Parte 3: Configurar el direccionamiento IP y probar la conectividad**

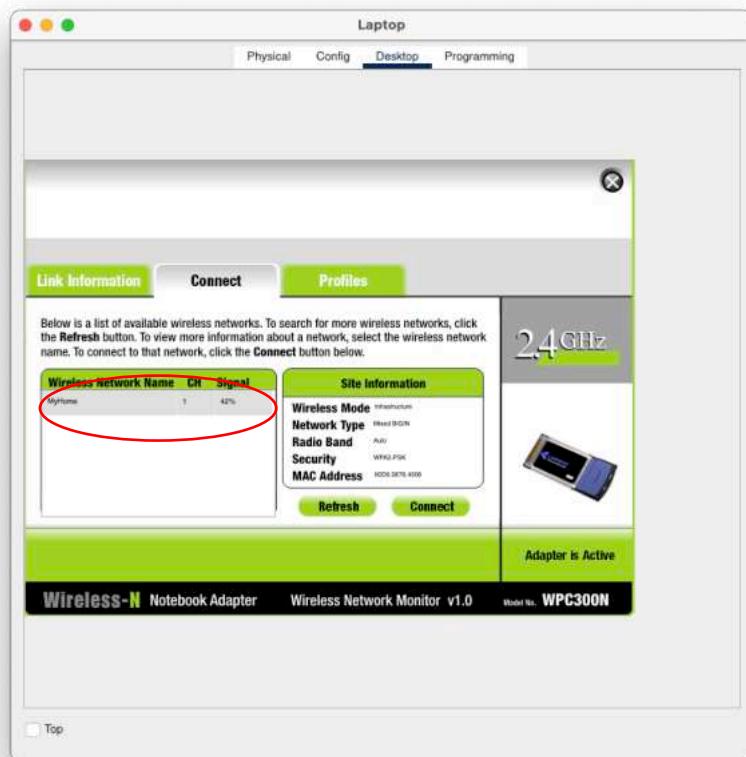
Ahora que el router está configurado, en esta parte configurará el direccionamiento IP para las PC y las computadoras portátiles y verificará que se puedan conectar a Internet.

#### **Paso 1: Conecte la computadora portátil a la red inalámbrica.**

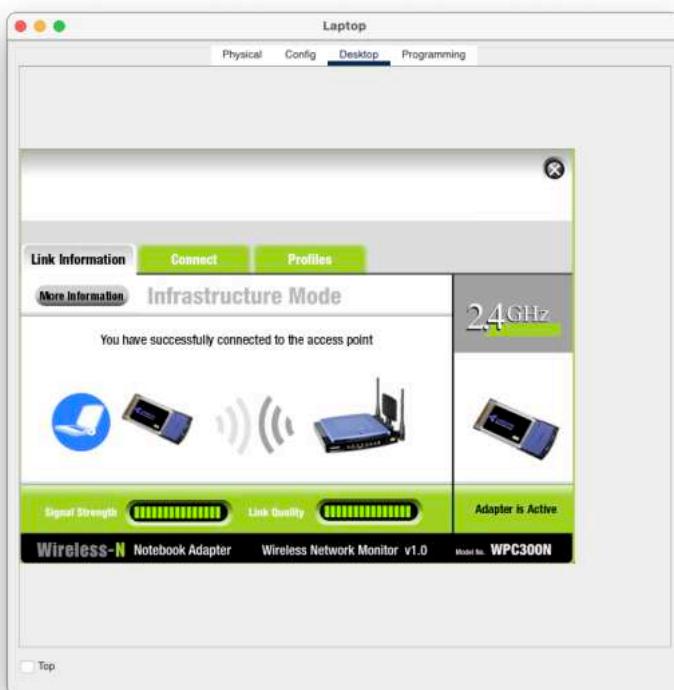
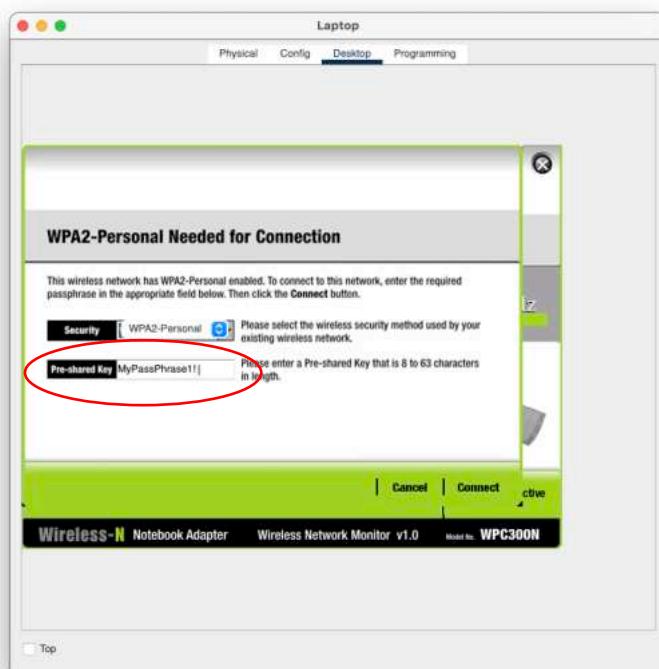
- Haga clic en la **computadora portátil** en la sala de estar y luego en la pestaña **Escritorio > PC inalámbrica**.
- Haga clic en la pestaña **Conectar**. Después de un breve retraso, la red inalámbrica que configuró anteriormente aparecerá en la lista de nombres de redes inalámbricas.
- Haga clic en el nombre de la red que creó y luego en el botón **Conectar**.
- Ingrese la frase de contraseña que configuró antes para la red inalámbrica en el campo **Clave precompartida** (Pre-shared Key) y haga clic en **Conectar**.
- Haga clic en la pestaña de **Información de enlace (Link Information)**. Debería ver el mensaje **You have successfully connected to the access point** (Se ha conectado correctamente al punto de acceso).

- f. Haga clic en el botón **Más Información (More Information)** para ver detalles sobre la conexión. Si la dirección IP no comienza con **192**, haga clic en **Fast Forward Time** varias veces para acelerar la simulación.
- g. Cierre la aplicación **PC Wireless** y abra el **navegador web**. Verifique que la **computadora portátil** ahora pueda conectarse a **skillsforall.srv**, haciendo clic en **Fast Forward Time** (Tiempo de avance rápido) hasta que se cargue la página. Esto verifica que la **computadora portátil** tenga conectividad a Internet.

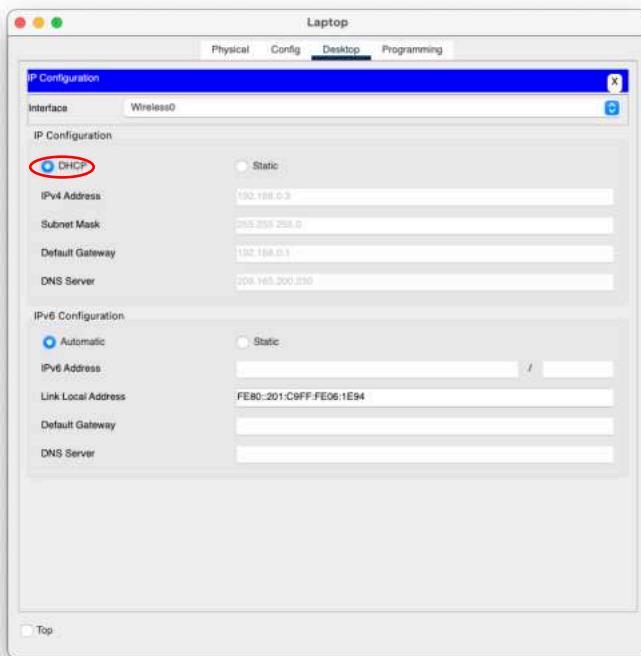
Con el círculo rojo se pretende mostrar donde nos aparece la red “MyHome” que hemos renombrado anteriormente.



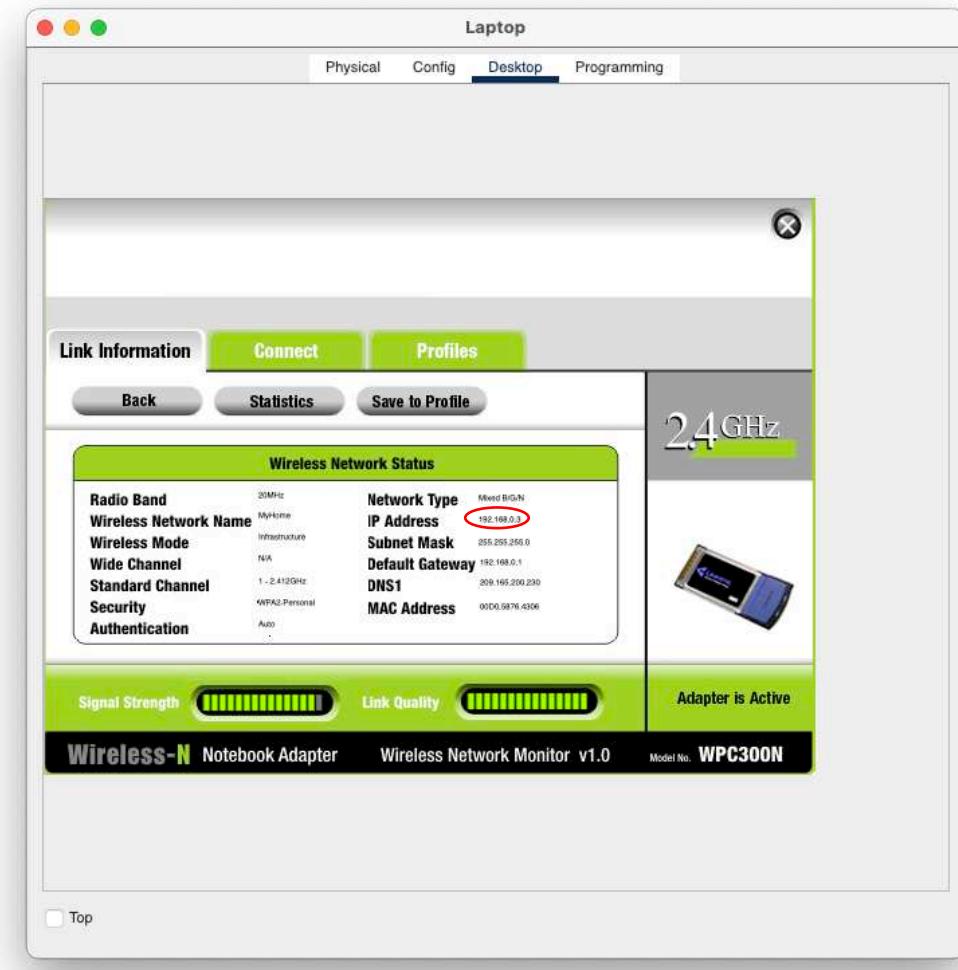
Realizamos los ajustes requeridos.



Siguiendo los pasos indicados la conexión no se establecía, cuando se le daba a “more information”, aparecía la IP address, subnet mask y Gateway a 0. Por tanto, tras investigar un poco, se añadió un paso; habilitar en la “IP configuration” del laptop, la opción “DHCP” y entonces sevconseguío establecer la conexión.



Ahora sí podemos ver los valores de IP, subnet mask y Gateway.



- Comprobamos la conexión del laptop en el “web browser” y verificamos que la conexión es exitosa.



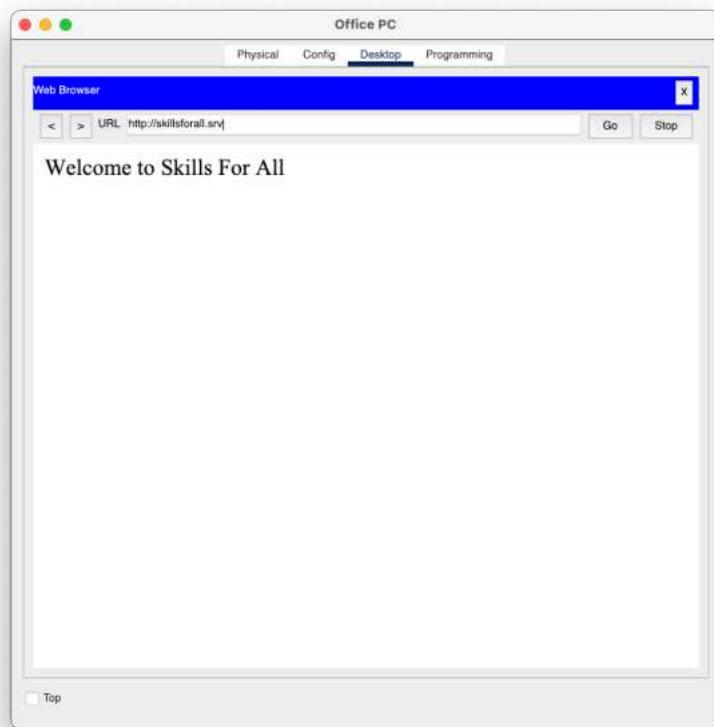
## **Paso 2: Pruebe la conectividad desde la PC de oficina.**

Usted sabe que la PC de Office puede conectarse a la red porque la utilizó para configurar el router. Sin embargo, ¿también puede acceder a Internet? Si puede, sabrá que la red cableada está correctamente conectada y configurada.

- Haga clic en **PC de oficina** > pestaña **Escritorio** > **Navegador web**.
- Ingrese **skillsforall.srv** y haga clic en **Ir**. Después de un breve retraso, verá aparecer la página web. Si es necesario, haga clic en **Fast Forward Time** varias veces para acelerar la convergencia.

Cargar un sitio web externo verifica que la conectividad a Internet para la **PC de oficina**.

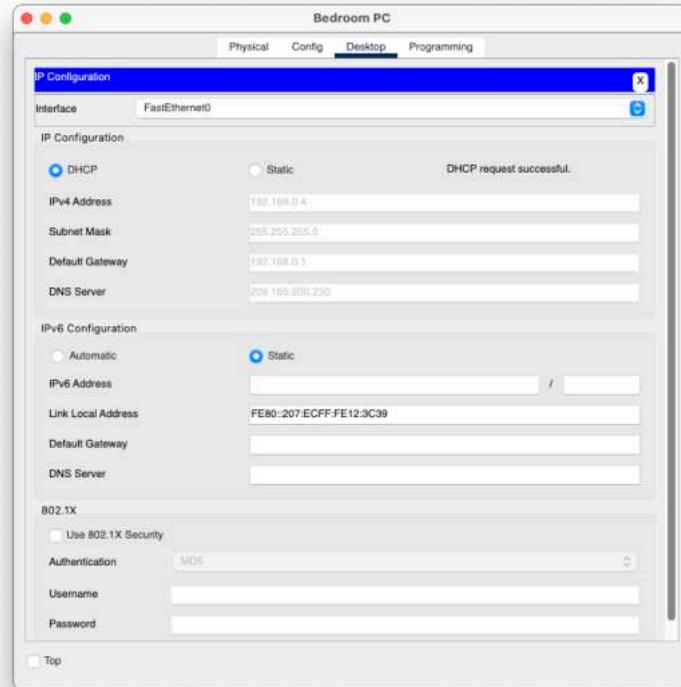
Realizamos la comprobación y vemos que hay conexión.



### Paso 3: Configurar la PC de dormitorio.

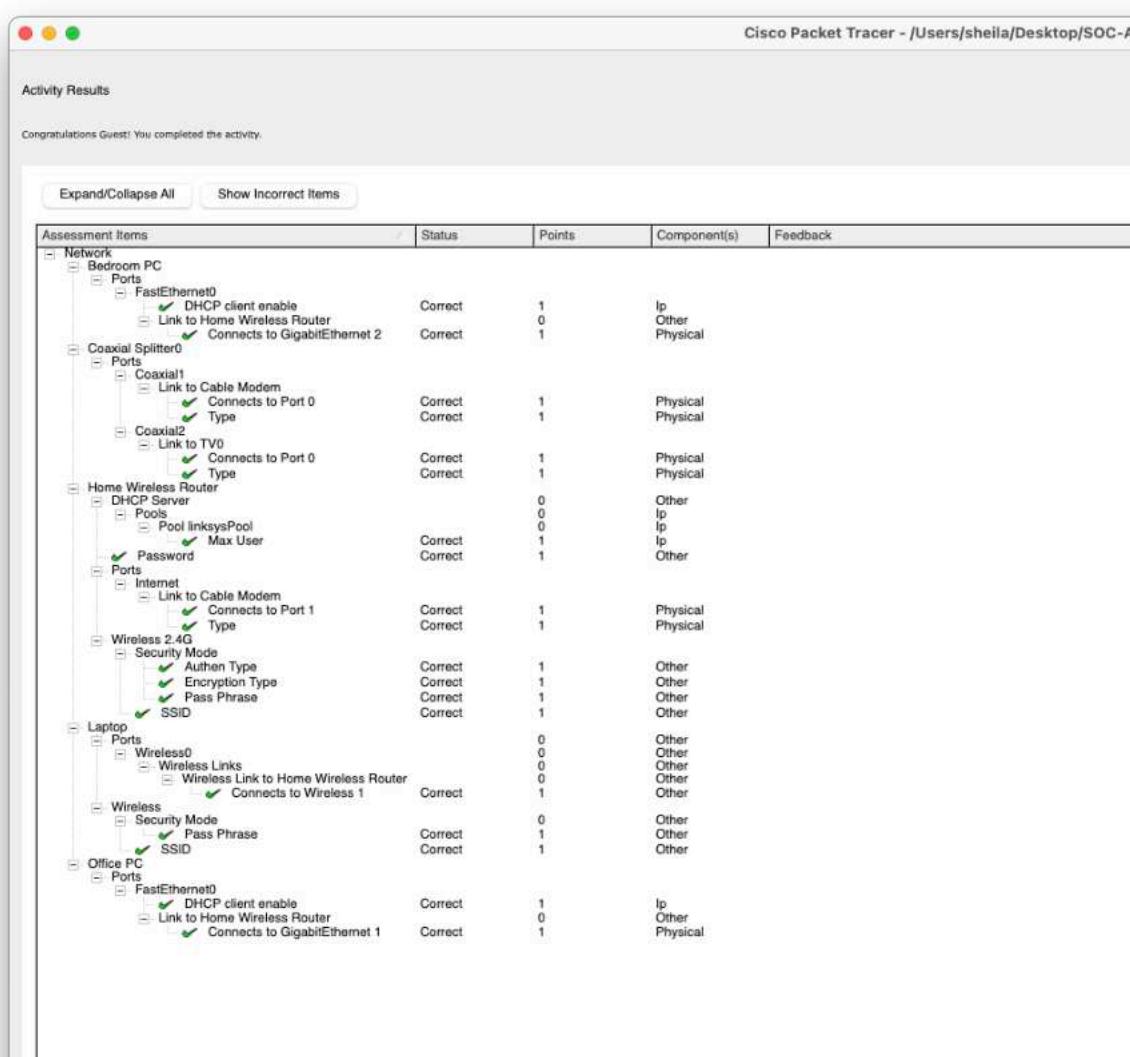
- Para la **PC de dormitorio**, abra **Configuración IP** y configúrela como **DHCP**. Verifique que la PC del dormitorio recibió una dirección IP que comienza con **192**.
- Cierre la ventana **Configuración IP** y haga clic en **Web Browser (Navegador web)**. Verifique que la **PC del dormitorio** ahora pueda conectarse a **skillsforall.srv**, haciendo clic en **Fast Forward Time** (Tiempo de avance rápido) hasta que se cargue la página. Esto verifica que la **PC del dormitorio** tenga conectividad a Internet.

Tras haber completado la conexión de dispositivos de red, la configuración del router, la LAN inalámbrica, y la configuración de hosts para conectarse a la red, todos los dispositivos deben poder conectarse a Internet. Su trabajo está hecho y Natsumi se ha ofrecido a prepararle la cena como recompensa por su ayuda.



Comprobamos la conexión y efectivamente, es exitosa. Este ejercicio presenta los enunciados muy detallados, y debido a que la realización era establecer conexiones ya descritas y comprobar conexiones, evitando caer en la repetición de información, está desarrollado con muy breves comentarios.

A continuación, se puede comprobar que todos los pasos se han realizado según lo esperado.



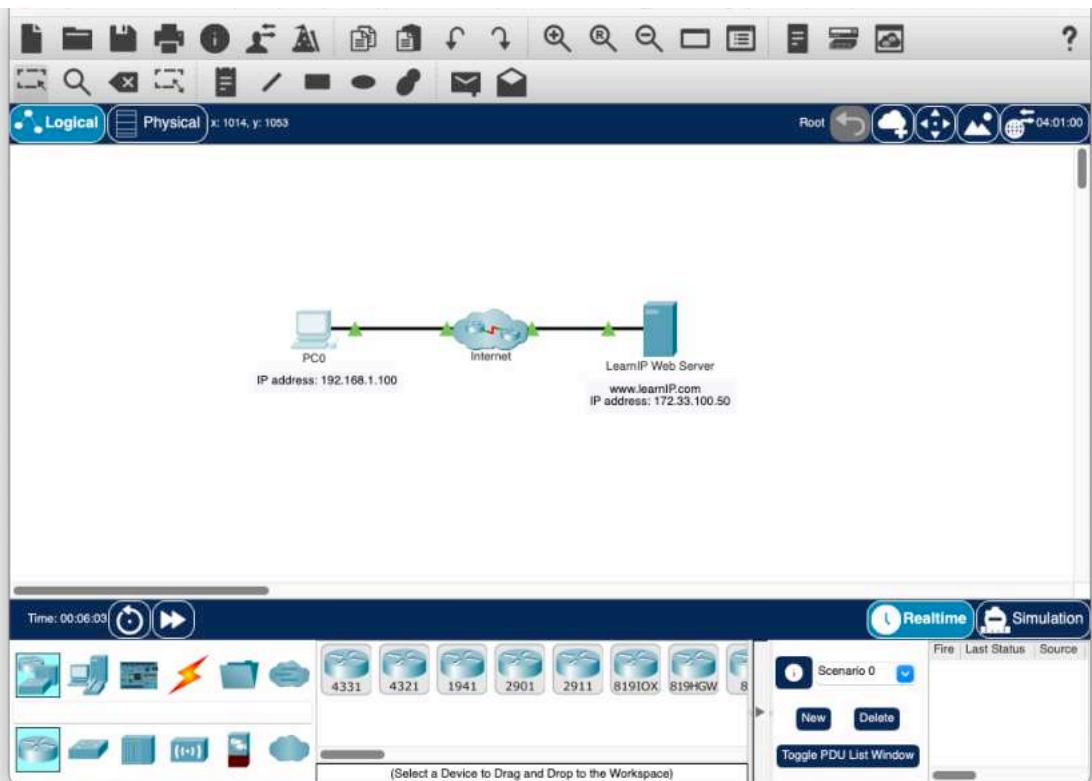
NOTA: debido a errores de la web, tras checkear los progresos de la actividad en el wizzard, se borró todo el avance en el .pka, por tanto al abrirlo no hay cambios guardados pero se puede comprobar mediante las capturas que el ejercicio se realizó exitosamente.

## Tarea 2: Conectarse a un servidor web (apartado 8.1.3. del curso)

### Packet Tracer: Conectarse a un servidor web

#### Objetivos

Observar cómo se envían los paquetes a través de Internet usando direcciones IP.



## Instrucciones

### Parte 1: Verifique la conectividad con el servidor Web

- Abra la ventana de la petición de entrada de comandos del host de origen. Seleccione **PC0**.
- Seleccione la ficha Desktop (Escritorio) > Command Prompt (Línea de comandos).
- Verificar la conectividad al servidor Web. En la línea de comandos, haga ping en la dirección IP del servidor web ingresando **ping 172.33.100.50**.

**PC> ping 172.33.100.50**

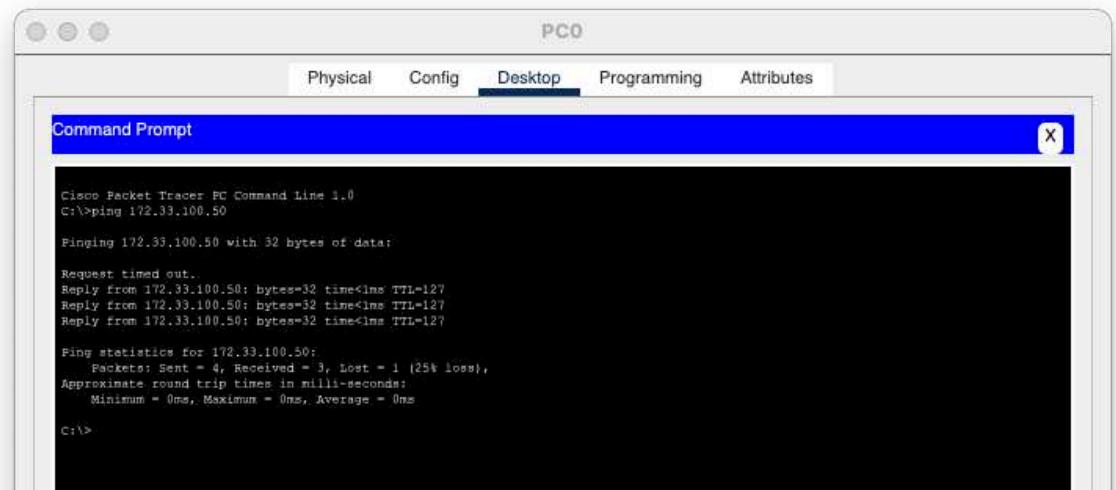
Pinging 172.33.100.50 with 32 bytes of data:

```
Reply from 172.33.100.50: bytes=32 time=0ms TTL=127
```

```
Ping statistics for 172.33.100.50:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Una respuesta verifica la conectividad desde el cliente al servidor web de destino. Inicialmente se puede agotar el tiempo de espera de la respuesta mientras se cargan los dispositivos y se ejecuta ARP.

- d. Cierre solamente la ventana de la línea de comandos haciendo clic en la cruz que se encuentra dentro de la ventana de la línea de comandos. Asegúrese de dejar abierta la ventana de configuración de PC0.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.33.100.50

Pinging 172.33.100.50 with 32 bytes of data:
Request timed out.
Reply from 172.33.100.50: bytes=32 time<1ms TTL=127
Reply from 172.33.100.50: bytes=32 time<1ms TTL=127
Reply from 172.33.100.50: bytes=32 time<1ms TTL=127

Ping statistics for 172.33.100.50:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

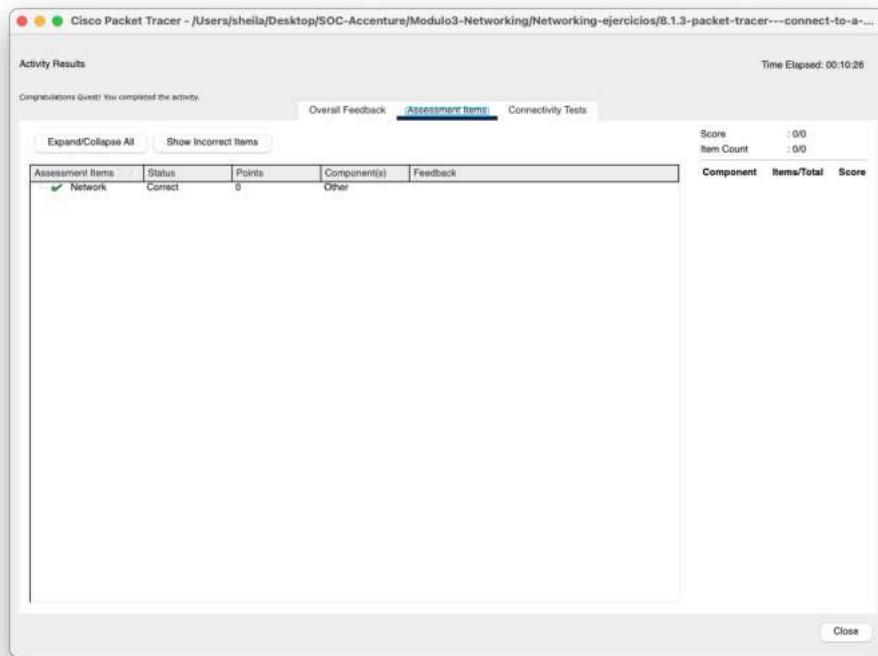
## Parte 2: Conéctese con el servidor Web a través del cliente Web

- a. En la ficha Desktop (Escritorio) de PC0, seleccione **Web Browser** (Navegador web).
- b. Escriba **172.33.100.50** en la URL y haga clic en **Go (Ir)**. El cliente web se conectará al servidor web a través de la dirección IP y abrirá la página web.

¿Qué mensajes se ven después de que la página web se terminó de cargar?

El mensaje de la web puede verse en la captura de imagen de la misma.



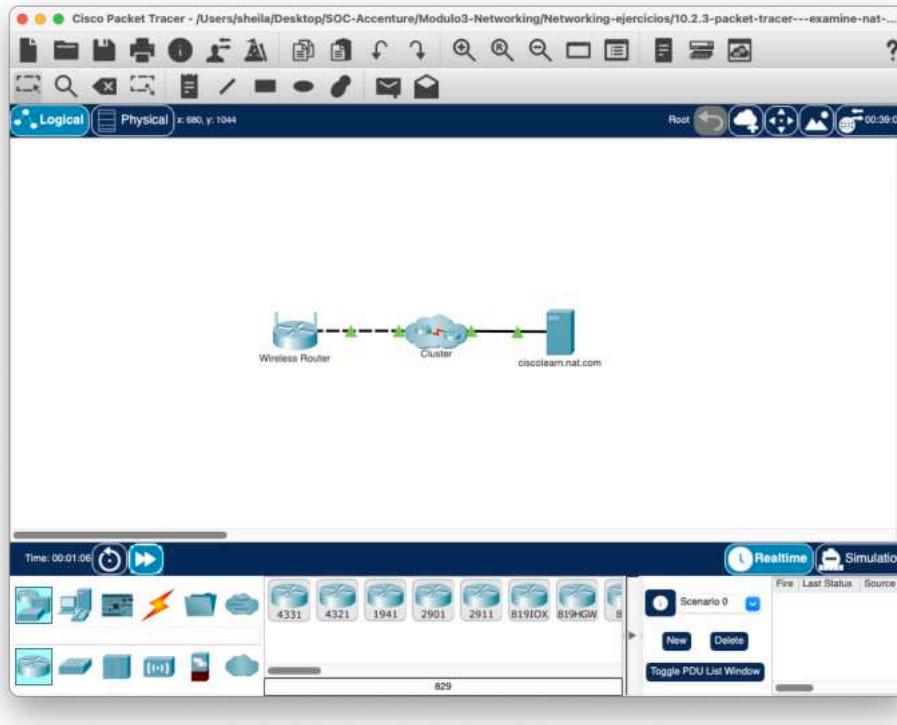


## Tarea 3: Examinar NAT en un Enrutador Inalámbrico (apartado 12.2.2. del curso)

### Packet Tracer: Examinar NAT en un enrutador inalámbrico

#### Objetivos

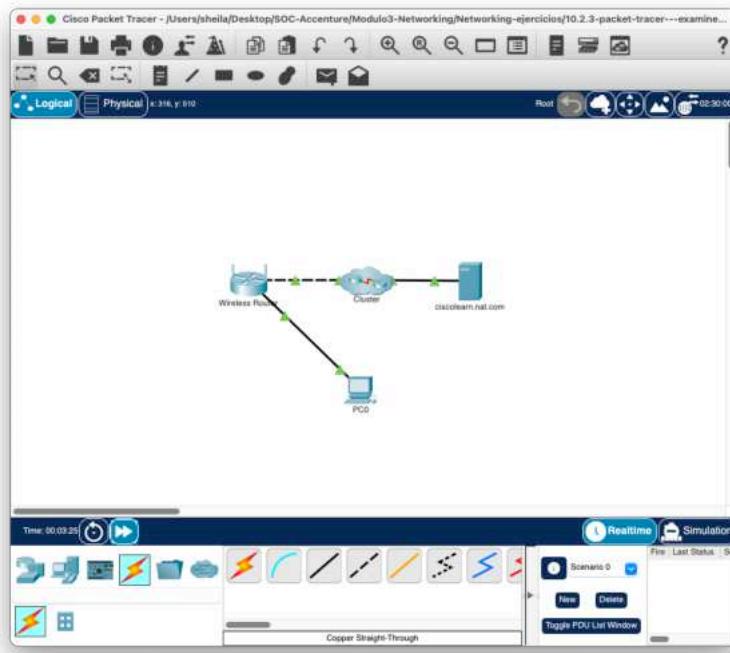
- Examinar la configuración NAT en un router inalámbrico
- Configurar 4 PC para que se conecten a un router inalámbrico mediante DHCP
- Examinar el tráfico que atraviesa la red mediante NAT



## Instrucciones

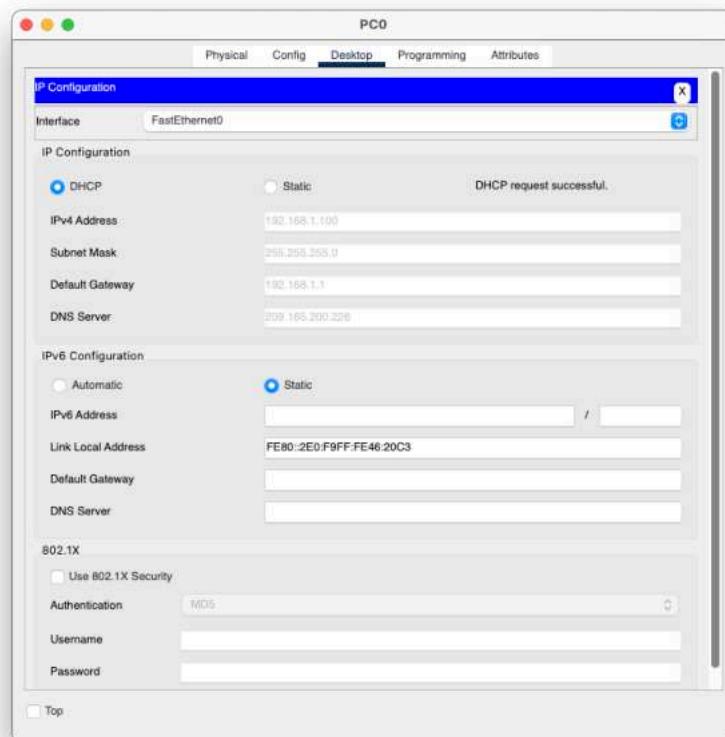
### Parte 1: Examine la configuración para acceder a la red externa.

1. Agregue 1 PC y conéctela al router inalámbrico con un cables directo. Espere a que todas las luces de enlace se vuelvan verdes antes de continuar con el siguiente paso o haga clic en Fast Forward (Adelantar).

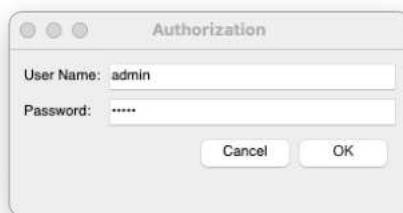


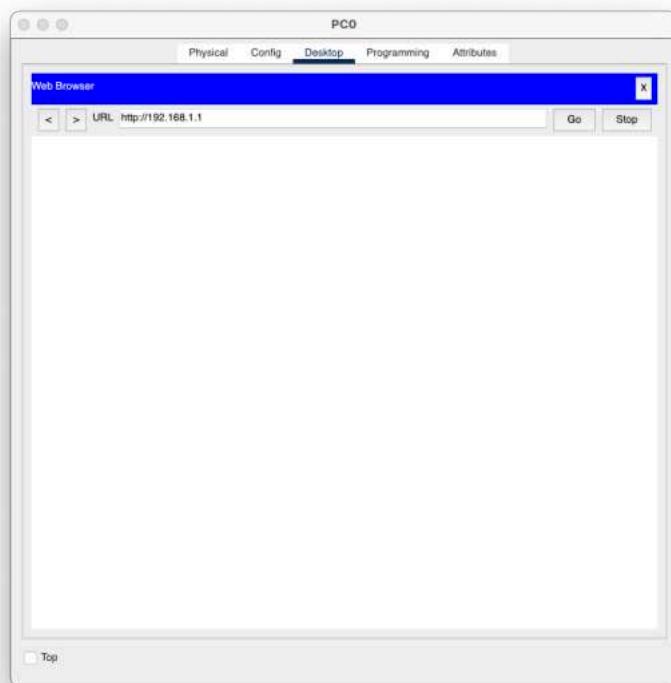
Para establecer la conexión se ha usado un cable Ethernet. Este se puede encontrar dentro de la categoría de cables que se muestra en la parte inferior de la captura de imagen. El icono que los representa es un rayo y los tipos de cables a seleccionar se muestran justo después que éste hacia la derecha con distintos colores.

2. En la PC, haga clic en Desktop (Escritorio). Seleccione IP Configuration. Haga clic en DHCP para habilitar cada dispositivo para que reciba una dirección IP mediante DHCP en el enrutador inalámbrico.



3. Anote la dirección IP de la puerta de enlace predeterminada. Cierre IP Configuration (Configuración IP) cuando termine.
4. Desplácese al navegador web e introduzca la dirección IP de la puerta de enlace predeterminada en el campo URL. Cuando se le solicite , ingrese admin como el nombre de usuario y admin como la contraseña.





PC0

Physical Config Desktop Programming Attributes

Web Browser

URL: http://192.168.1.1 Go Stop

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Internet Setup

Connection type: Automatic Configuration - DHCP

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server Settings: Enabled

Start IP Address: 192.168.1.100

Maximum number of Users: 50

IP Address Range: 192.168.1.100 - 149

Client Lease Time: minutes (0 means one day)

Static DNS 1: 209.165.200.226

Static DNS 2: 0.0.0.0

Static DNS 3: 0.0.0.0

WINS: 0.0.0.0

ISP Vlans

Enabled

VLAN ID: Internet: 10 VoIP: 20 IPTV: 30

- Haga clic en la opción de menú Status (Estado) en la esquina superior derecha. Cuando se selecciona, muestra la página de submenús del enrutador.
- Desplácese hacia abajo por la página del enrutador hasta la opción de conexión a Internet. La dirección IP asignada aquí es la dirección asignada por el ISP. Si no hay una dirección IP (aparece 0.0.0.0), cierre la ventana, espere unos segundos e inténtelo nuevamente. El enrutador inalámbrico se encuentra en el proceso de obtener una dirección IP del servidor DHCP del ISP.



¿Es una dirección privada o una pública?

### ***Dirección IP pública***

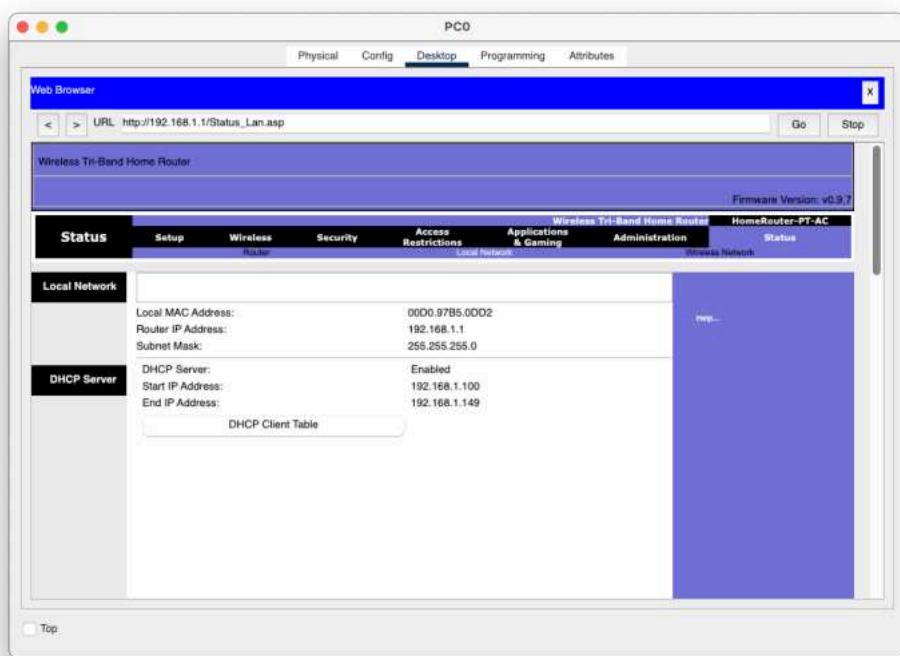
#### **Parte 2: Examinar la configuración para acceder a la red interna.**

- Haga clic en Local Network (Red local) dentro de la barra de submenús Status (Estado).
- Desplácese hacia abajo para analizar la información de la red local. Esta es la dirección asignada a la red interna.
- Desplácese aún más abajo para examinar la información del servidor DHCP y el rango de direcciones IP que se pueden asignar a los hosts conectados.

¿Son direcciones privadas o públicas?

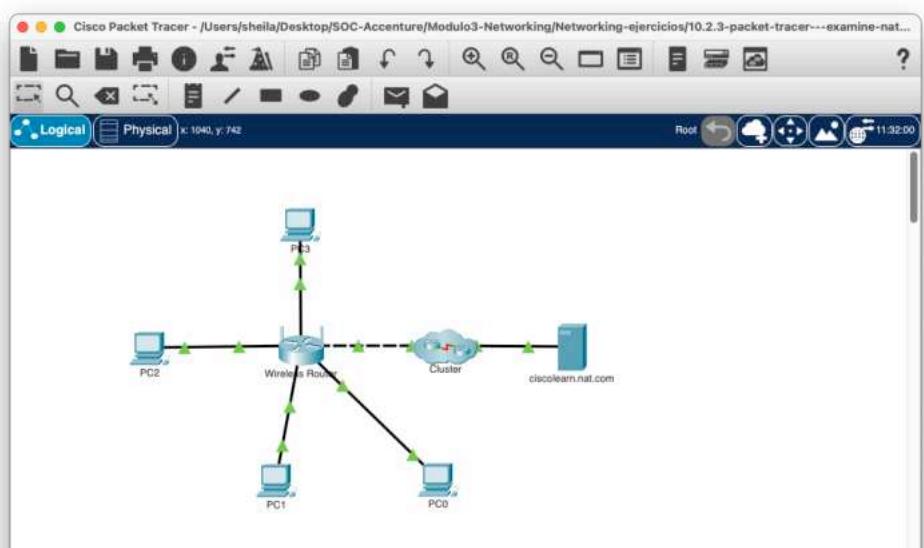
### Dirección IP privada

4. Cierre la ventana de configuración del router inalámbrico.

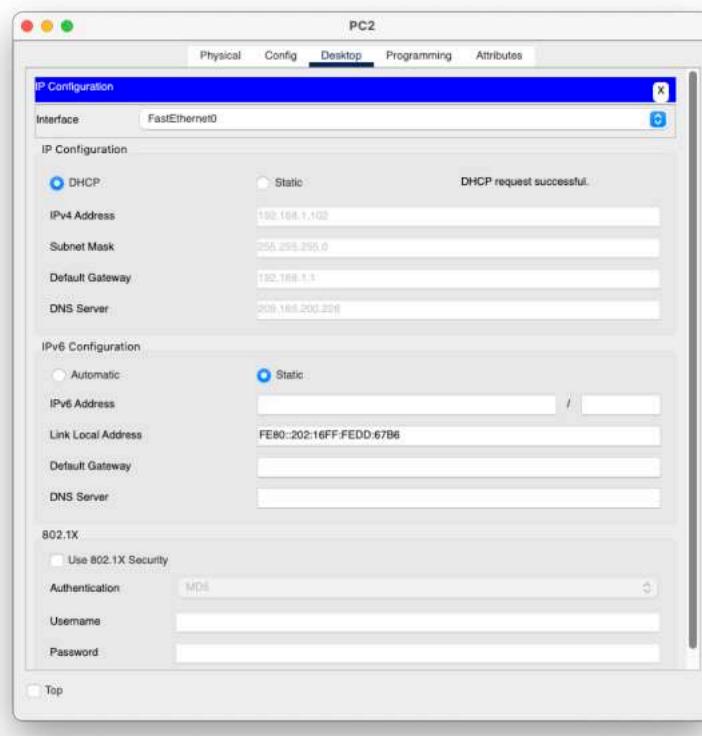
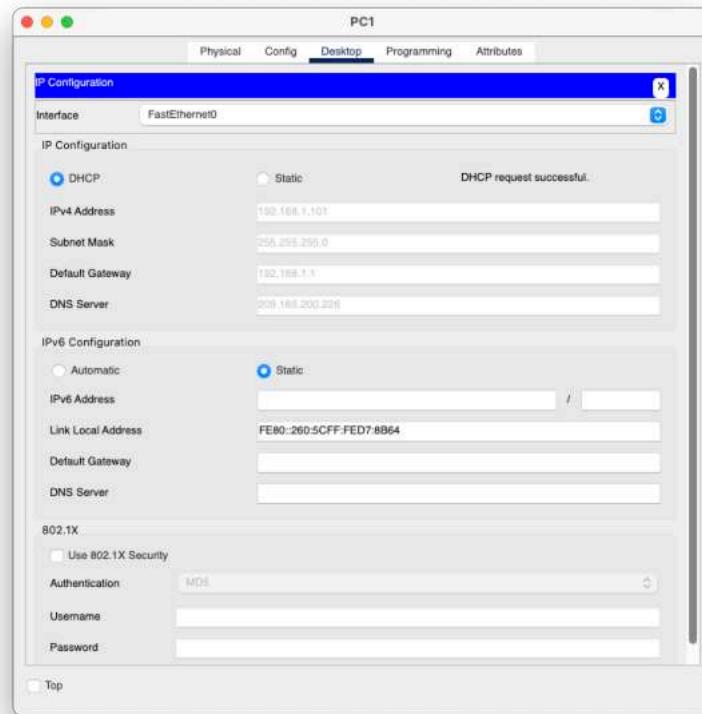


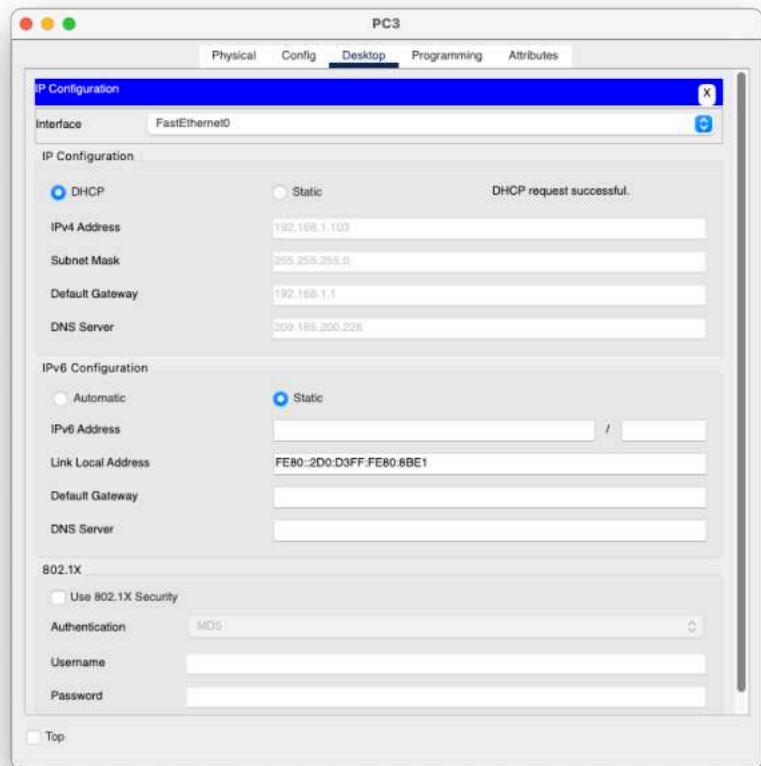
### Parte 3: Conectar 3 PC al enrutador inalámbrico.

1. Agregue 3 PCs mas y conéctelas al router inalámbrico con cables directos. Espere a que todas las luces de enlace se vuelvan verdes antes de continuar con el siguiente paso o haga clic en Fast Forward (Adelantar).



2. En cada PC, haga clic en Desktop (Escritorio). Seleccione IP Configuration. Haga clic en DHCP para habilitar cada dispositivo para que reciba una dirección IP mediante DHCP en el enrutador inalámbrico. Cierre IP Configuration (Configuración IP) cuando termine.





3. Haga clic en Command Prompt (Línea de comandos) para verificar la configuración IP de cada dispositivo con el comando ipconfig /all.  
 Nota: Estos dispositivos recibirán una dirección privada. Las direcciones privadas no pueden atravesar Internet; por lo tanto se debe realizar una traducción de NAT.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

  Connection-specific DNS Suffix...:
  Physical Address.....: 00E0.F946.20C3
  Link-local IPv6 Address....: FE80::2E0:F9FF:FE46:20C3
  IPv4 Address.....: 192.168.1.100
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: 192.168.1.1
  DHCP Servers.....: 192.168.1.1
  DHCPv6 IID.....: 
  DHCPv6 Client DUID.....: 00-0F-0B-01-95-D4-AC-50-00-E0-F9-46-20-C3
  DNS Servers.....: 209.165.200.226

Bluetooth Connection:

  Connection-specific DNS Suffix...:
  Physical Address.....: 00E0.BC30.B592
  Link-local IPv6 Address....: ::

C:\>

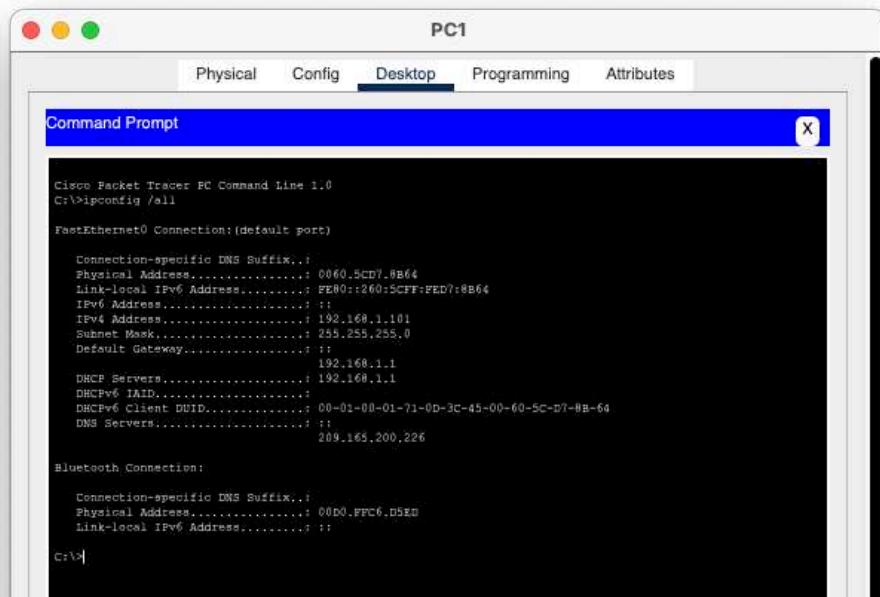
```

Verificamos así que el dispositivo PC0 recibe una dirección IP y otra información de red correcta desde el servidor DHCP.

#### Verificación de ipconfig /all:

- **IPv4 Address:** 192.168.1.100 (Es una dirección IP privada válida).
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 192.168.1.1 (Dirección IP del router).
- **DHCP Server:** 192.168.1.1 (El servidor DHCP está funcionando correctamente).
- **DNS Servers:** 209.165.200.226

Esto confirma que el dispositivo está configurado correctamente para la red local.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...: 
    Physical Address.....: 00E0:5CD7:8B64
    Link-local IPv6 Address.....: FE80::2E0:5CD7%8B64
    IPv6 Address.....: ::1
    IPv4 Address.....: 192.168.1.101
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 
                    192.168.1.1
    DHCP Servers.....: 192.168.1.1
    DHCPv6 IAIID.....: 
    DHCPv6 Client DUID.....: 00-01-00-01-71-00-3C-45-00-60-5C-D7-BB-64
    DNS Servers.....: 209.165.200.226

Bluetooth Connection:

    Connection-specific DNS Suffix...: 
    Physical Address.....: 00D0:FFC6:D5ED
    Link-local IPv6 Address.....: ::1

C:\>
```

Para el PC1, el comando “ipconfig /all” muestra la siguiente configuración:

- **IPv4 Address:** 192.168.1.101 (Es una dirección IP privada válida).
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 192.168.1.1 (Dirección IP del router).
- **DHCP Server:** 192.168.1.1 (El servidor DHCP está funcionando correctamente).
- **DNS Servers:** 209.165.200.226

Esto confirma que el PC1 también está configurado correctamente para la red local.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...: 0002.16DD.67B6
Physical Address....: 00:02:16:DD:67:B6
Link-local IPv6 Address....: FE80::202:16FF:FE00:67B6
IPv4 Address.....: 192.168.1.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DHCP Servers.....: 192.168.1.1
DHCPv6 IAID.....: 
DHCPv6 Client DUID.....: 00-01-00-01-E8-00-00-C2-00-02-16-00-67-B6
DNS Servers.....: 209.165.200.226

Bluetooth Connection:

Connection-specific DNS Suffix...: 0050.0FEA.NCA0
Physical Address....: 00:50:0F:EA:NCA0
Link-local IPv6 Address....: ::

C:\>

```

Para PC2, el comando “ipconfig /all” muestra la siguiente configuración:

- **IPv4 Address:** 192.168.1.102 (Es una dirección IP privada válida).
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 192.168.1.1 (Dirección IP del router).
- **DHCP Server:** 192.168.1.1 (El servidor DHCP está funcionando correctamente).
- **DNS Servers:** 209.165.200.226

Esto confirma que PC2 también está configurado correctamente para la red local.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...: 00D0.D300.0BE1
Physical Address....: 00:D0:D3:00:0B:E1
Link-local IPv6 Address....: FE80::2D0:D3FF:FE80:8BE1
IPv4 Address.....: 192.168.1.103
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DHCP Servers.....: 192.168.1.1
DHCPv6 IAID.....: 
DHCPv6 Client DUID.....: 00-01-00-01-74-02-32-C8-00-D0-D3-80-8B-E1
DNS Servers.....: 209.165.200.226

Bluetooth Connection:

Connection-specific DNS Suffix...: 0060.5C3D.C5A7
Physical Address....: 00:60:5C:3D:C5:A7
Link-local IPv6 Address....: ::

C:\>

```

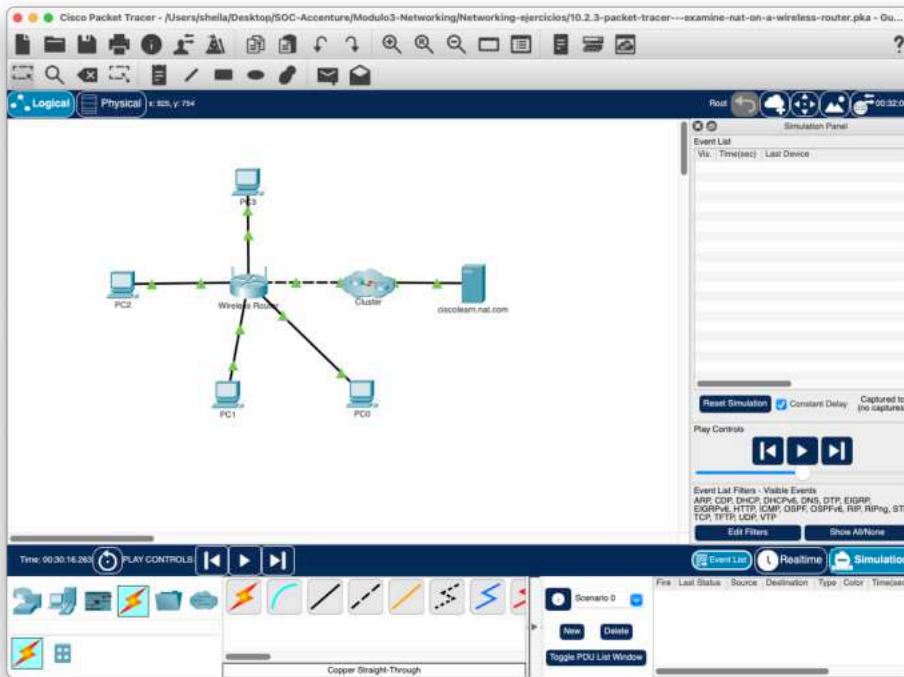
Para PC3, el comando “ipconfig /all” muestra la siguiente configuración:

- **IPv4 Address:** 192.168.1.103 (Es una dirección IP privada válida).
- **Subnet Mask:** 255.255.255.0
- **Default Gateway:** 192.168.1.1 (Dirección IP del router).
- **DHCP Server:** 192.168.1.1 (El servidor DHCP está funcionando correctamente).
- **DNS Servers:** 209.165.200.226

Esto confirma que PC3 también está configurado correctamente para la red local.

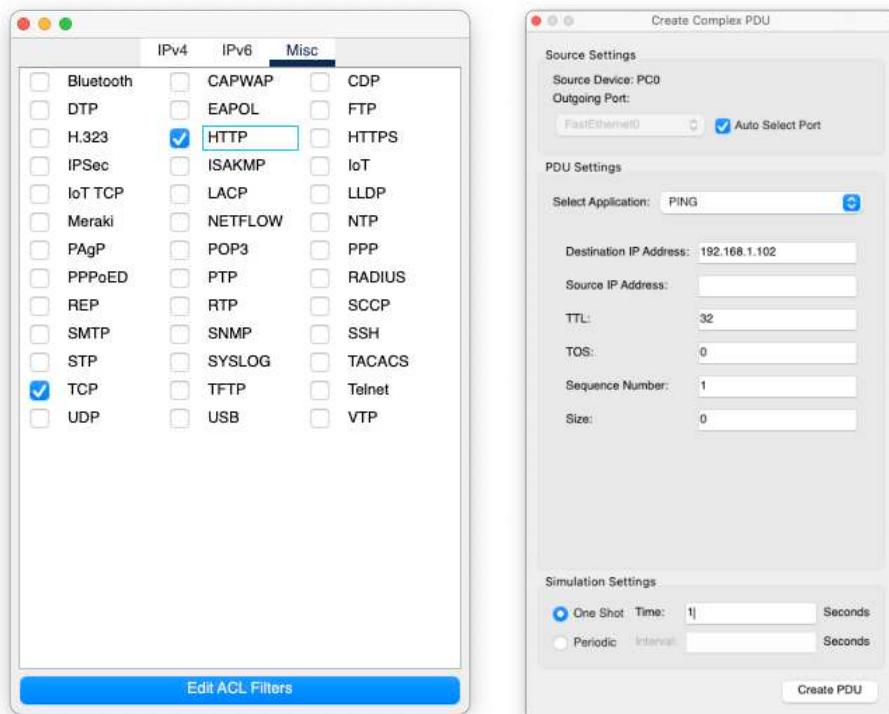
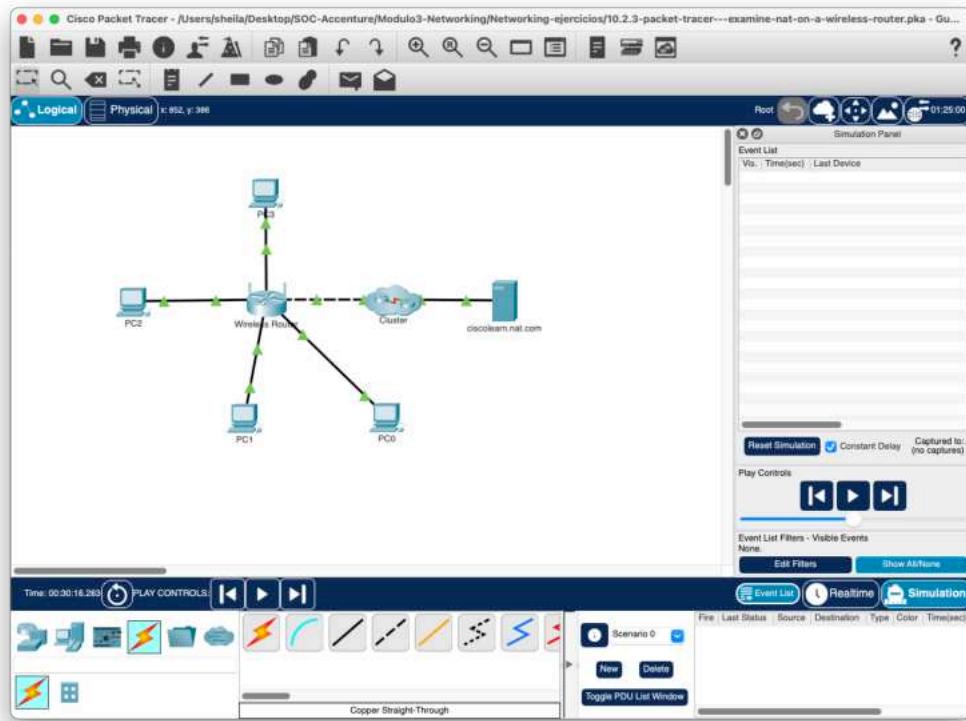
#### Parte 4: Ver la traducción NAT a través del enrutador inalámbrico.

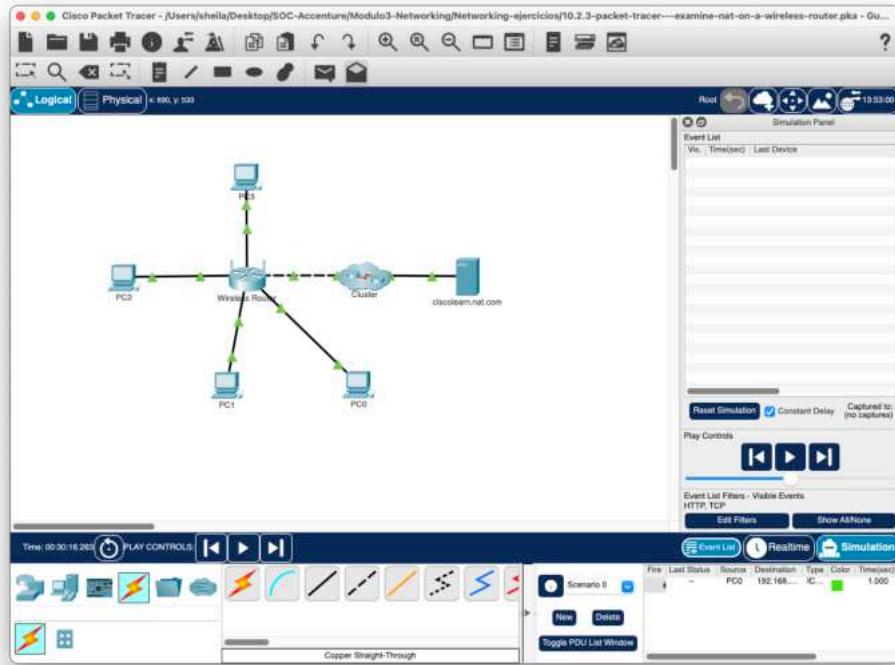
- Haga clic en la ficha Simulación de la esquina inferior derecha para acceder al modo Simulación. La pestaña de Simulation (Simulación) se encuentra detrás de la ficha Realtime (Tiempo real) y tiene el símbolo de un cronómetro.



- Cree una PDU compleja en el modo Simulación para ver el tráfico:
  - En el panel de simulación, haga clic en Show All/None (Mostrar todos/ninguno) para no ver ningún evento. Ahora haga clic en Edit Filters (Editar filtros) y en la pestaña Misc, marque las casillas de TCP y HTTP. Cierre la ventana cuando haya terminado.
  - Agregue una PDU Compleja haciendo clic en el sobre abierto ubicado en el menú superior.
  - Haga clic en una de las PC para especificarla como origen.

En esta parte del ejercicio se pide que se cree una PDU compleja para la cual puse los ajustes por mi cuenta ya que no se especifica.

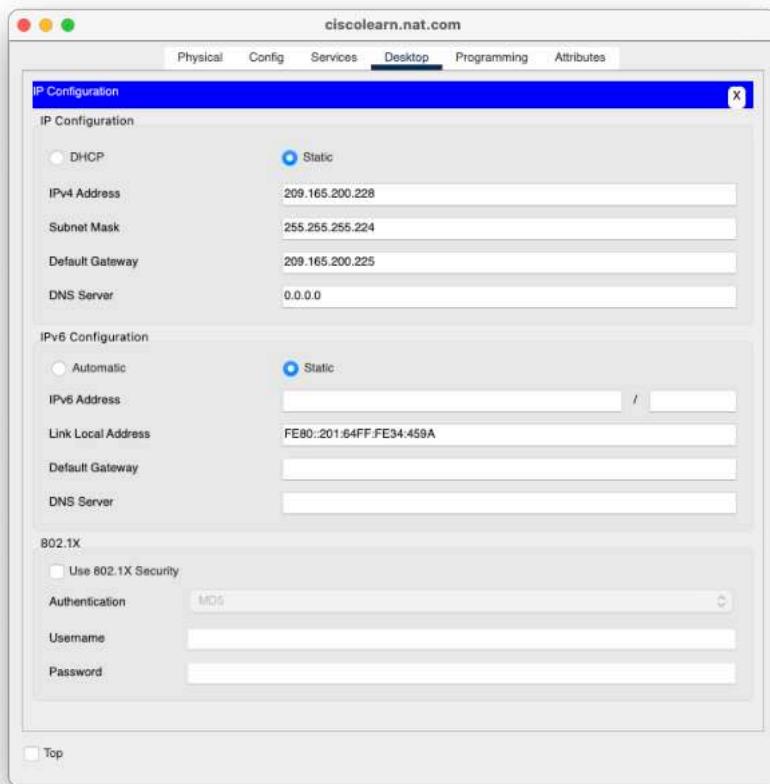




- c. Especifique la configuración de la PDU compleja cambiando lo siguiente en la ventana de la PDU compleja:
- En PDU Settings (Configuración de PDU), Select Application (Seleccionar aplicación) debe ser HTTP.
  - Haga clic en el servidor ciscolearn.nat.com para especificarlo como dispositivo de destino.
  - En Source Port (Puerto de origen), introduzca 1000.
  - En Simulation Settings (Configuración de simulación), seleccione Periodic (Periódica). Introduzca 120 segundos en Interval (Intervalo).
  - Haga clic en Create PDU (Crear PDU) en la ventana Create Complex PDU (Crear PDU compleja).

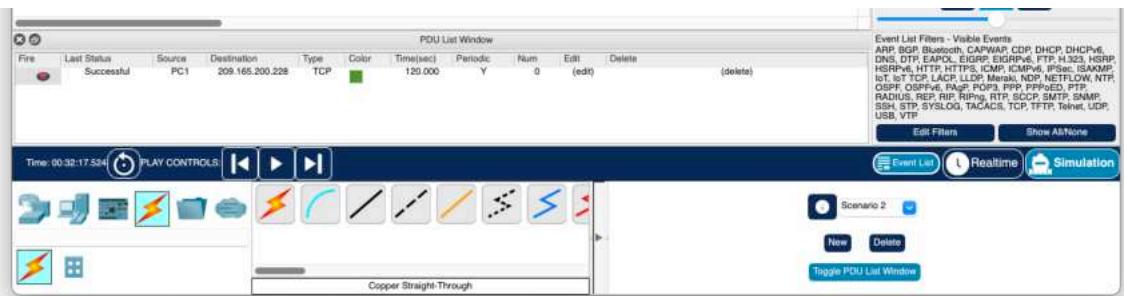
Al ver que en esta parte se especifican los ajustes de la PDU, decidí eliminar la PDU anterior y crear esta con los parámetros especificados.

No lo especifica, pero primero debemos averiguar que IP de destino necesitamos y para ello vamos a ciscolearn.nat.com y lo comprobamos.

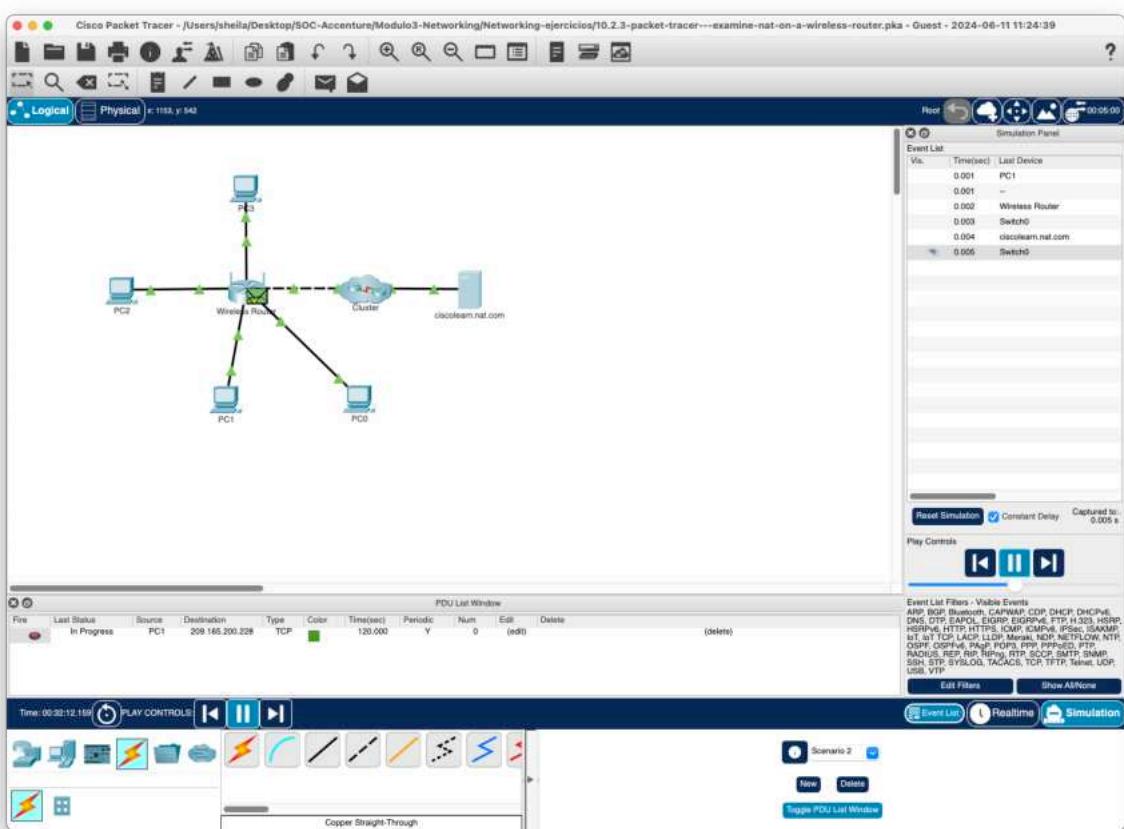


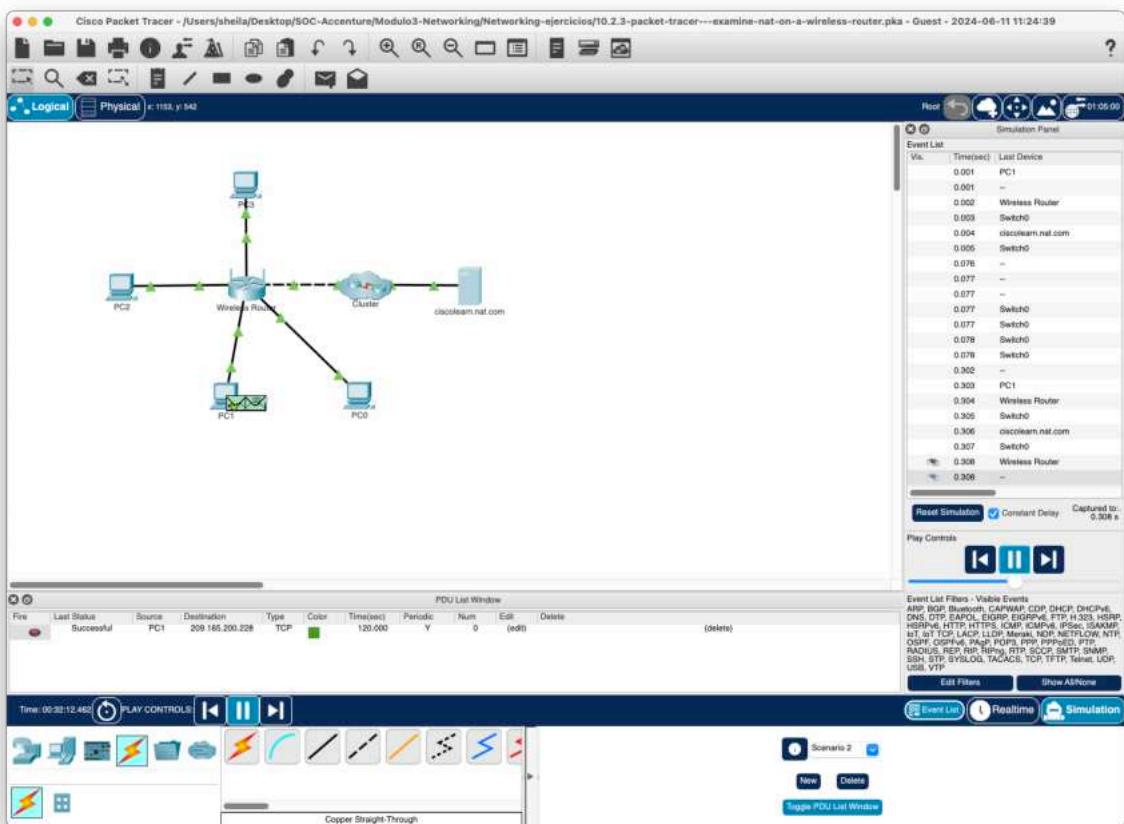
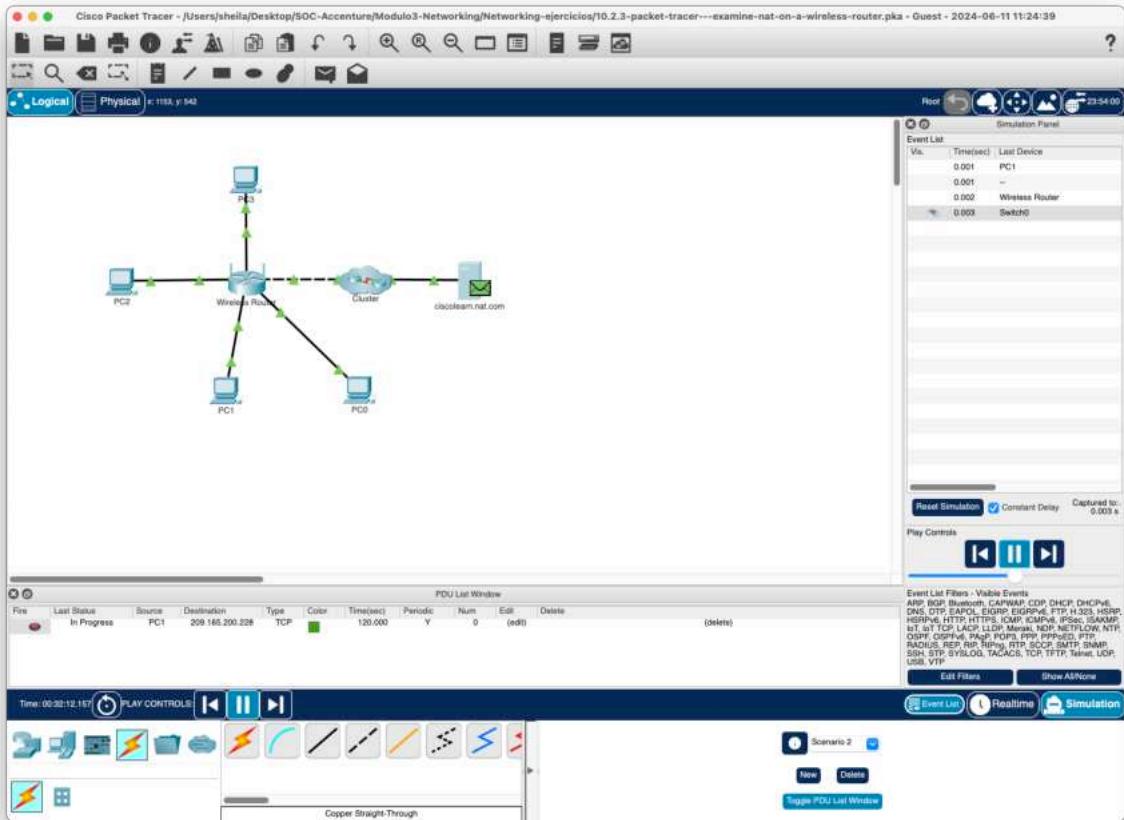
- Añadimos los ajustes dados por el enunciado mas la IP de ciscolearn.net.com:





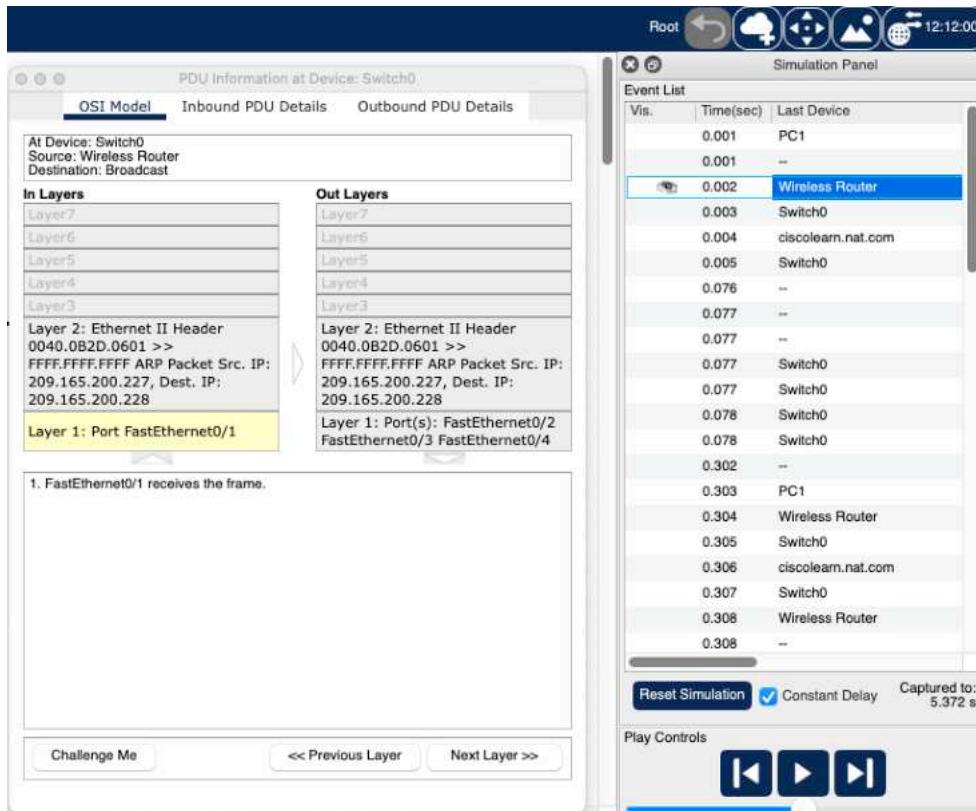
Observamos el flujo en la simulación:



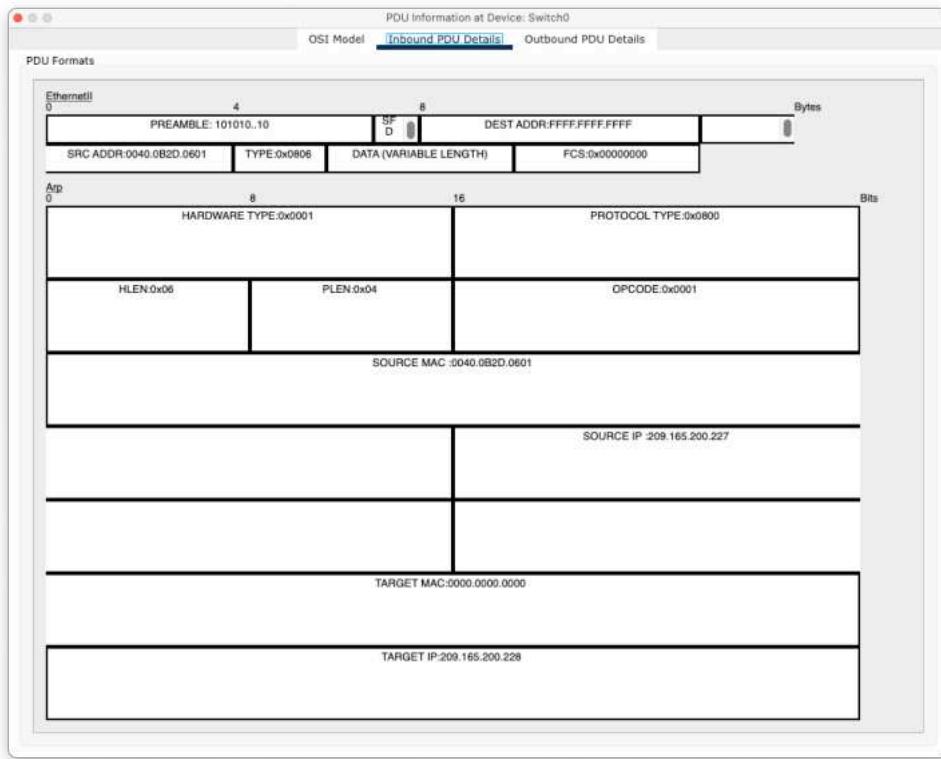


## Parte 5: Ver la información del encabezado de los paquetes que atravesaron la red.

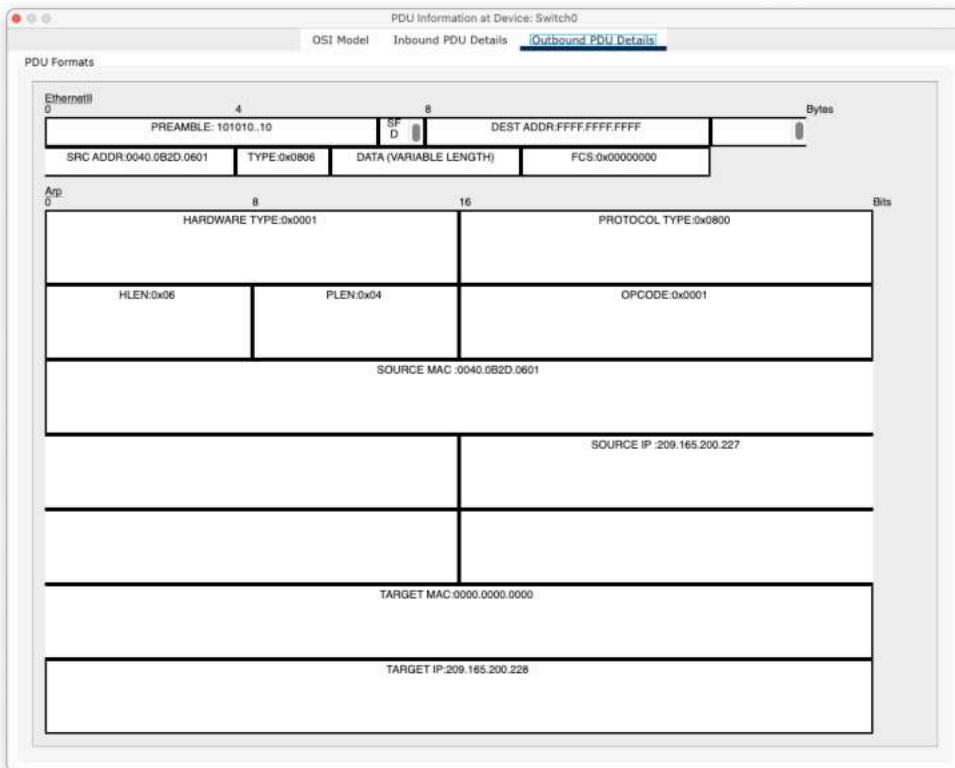
- a. Examine los encabezados de los paquetes enviados entre una PC y el servidor web.
  1. En el panel de simulación, haga doble clic en la tercera línea hacia abajo en la lista de eventos. Aparecerá un sobre en el área de trabajo que representa a esa línea.
  2. Haga clic en el sobre en la ventana del área de trabajo para ver la información del encabezado y el paquete.



- b. Haga clic en la ficha de detalles Inbound PDU (PDU entrante). Examine la información del paquete en busca de la dirección IP de origen (SRC) y la dirección IP de destino.

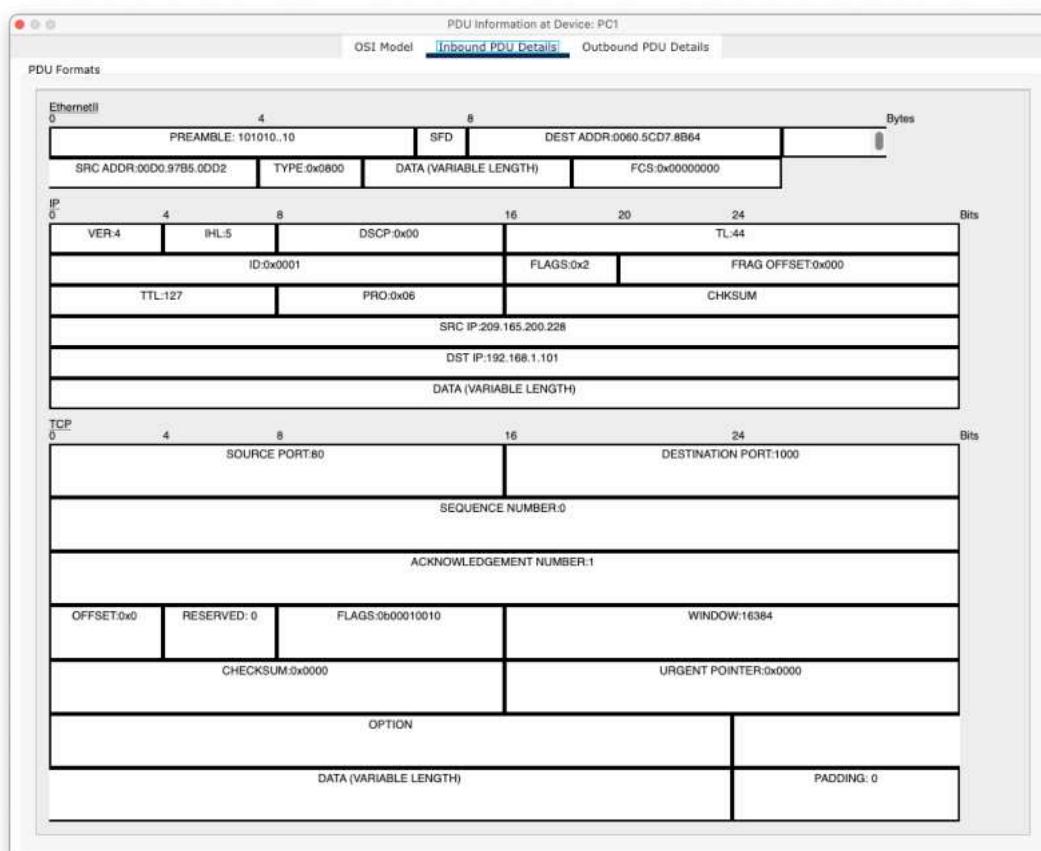
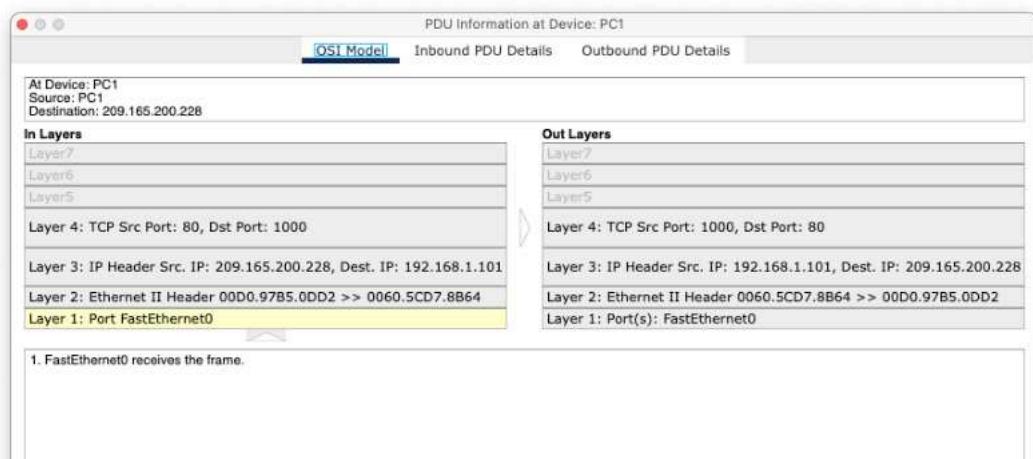


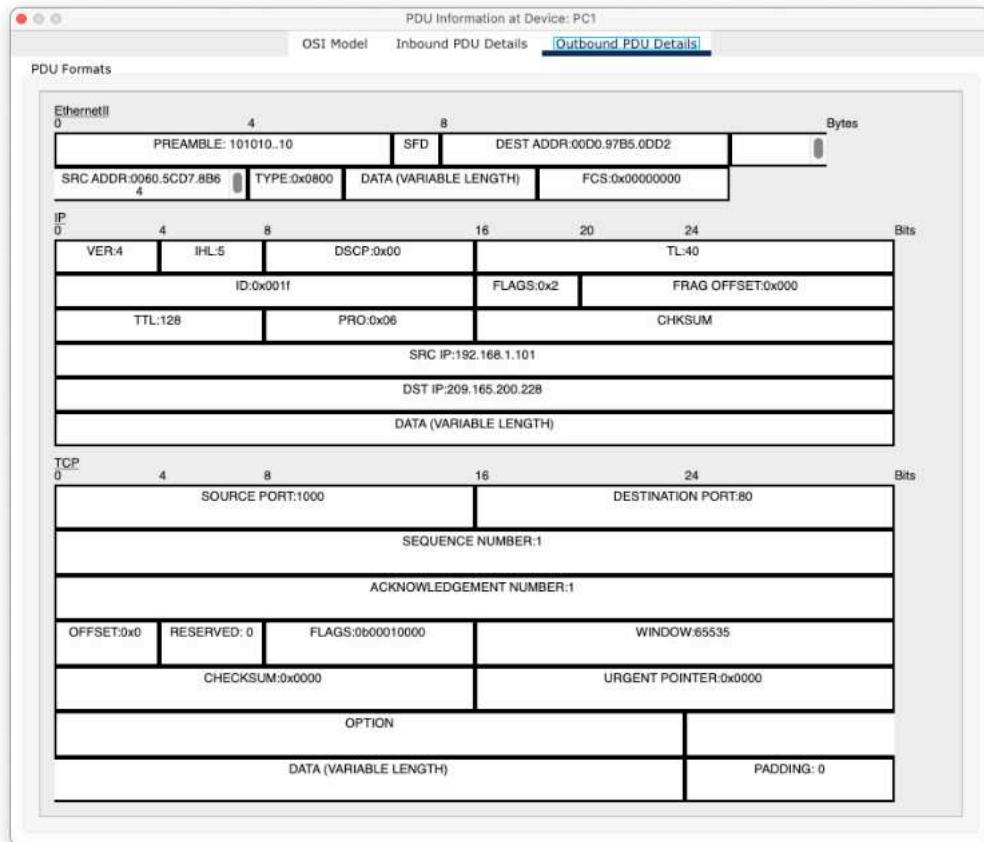
- c. Haga clic en la ficha de detalles Outbound PDU (PDU saliente). Examine la información del paquete en busca de la dirección IP de origen (SRC) y la dirección IP de destino.



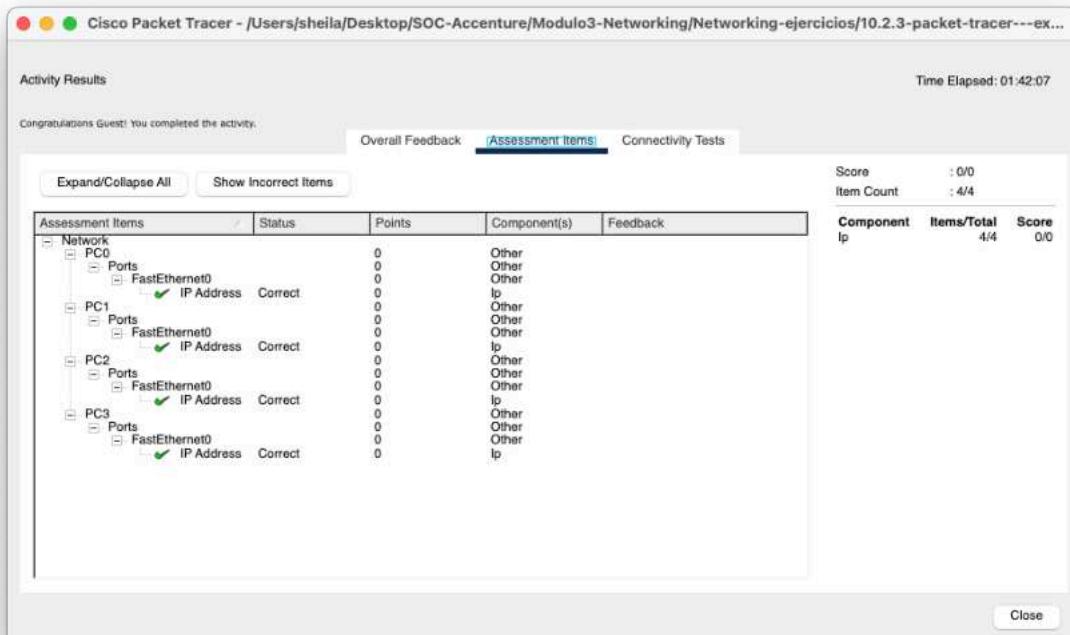
Observe el cambio en la dirección IP SRC.

- d. Haga clic en otras líneas de eventos para ver los encabezados correspondientes a lo largo del proceso.





- e. Al finalizar, ha de clic en Check Results (Verificar resultados) para verificar el trabajo.



## Tarea 4: Identificación de direcciones IP y MAC (apartado 13.1.3. del curso)

### Packet Tracer: Identificación de direcciones MAC y direcciones IP

#### Objetivos

**Parte 1: Recopilar información de PDU para la comunicación de red local**

**Parte 2: Recopilar información de PDU para la comunicación de red remota**

#### Aspectos básicos

Si está interesado en una carrera en administración de redes o seguridad de redes, es importante que comprenda los procesos de comunicación de red normales. En esta actividad de Packet Tracer, inspeccionará las tramas de Ethernet y los paquetes IP en diferentes puntos de la red a medida que viajan del origen al destino. Se centrará en la forma en que las direcciones MAC e IP cambian según el destino (local o remoto) y el lugar donde se capturan las PDU.

Packet Tracer tiene un modo de simulación que le permitirá investigar detalles sobre cómo viajan las PDU en las redes. Le permite verificar el direccionamiento MAC de capa 2 y el direccionamiento IPv4 de capa 3 de las PDU en diferentes ubicaciones de la red a medida que las PDU fluyen del origen al destino.

Esta actividad está optimizada para ver las PDU a medida que viajan en redes locales y remotas. Reunirá información de PDU en el modo de simulación de PT y responderá una serie de preguntas sobre los datos que obtenga. No se requiere ninguna configuración de dispositivo.

#### Instrucciones

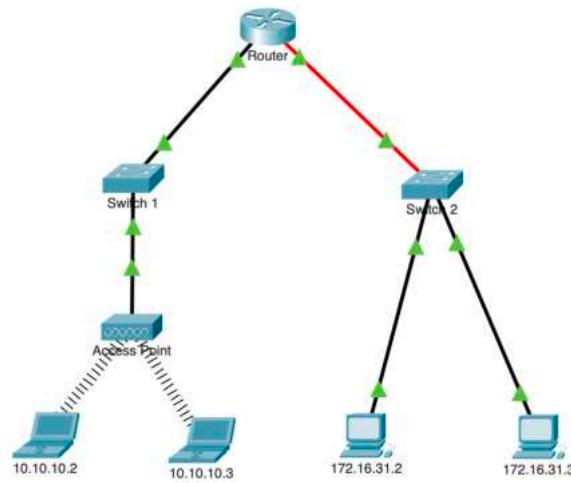
**Parte 1: Recopilar información de PDU para la comunicación de red local**

En esta parte, estudiará cómo un dispositivo en una red local no necesita una puerta de enlace predeterminada para comunicarse con otro dispositivo en la misma red local.

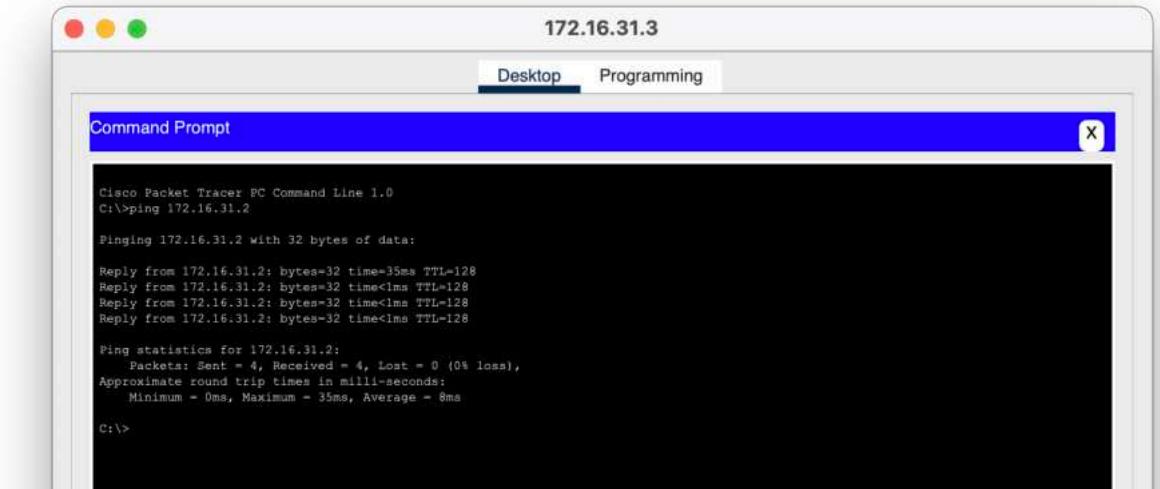
**Nota:** Revise las Preguntas de reflexión en la Parte 3 antes de continuar con esta parte. Le dará una idea del tipo de información que necesitará recopilar.

Para poder realizar este ejercicio, tal y como indica, revisaremos antes a las preguntas de reflexión. Pero antes de empezar, el enunciado hace mención a estas siglas cuyo significado se detallan a continuación.

- **PDU (Protocol Data Unit):** Una PDU es una unidad de datos en el contexto de un protocolo de red específico. En cada capa del modelo OSI, las PDUs tienen diferentes nombres: bits (Capa Física), tramas (Capa de Enlace de Datos), paquetes (Capa de Red), segmentos (Capa de Transporte), y datos (Capas de Sesión, Presentación y Aplicación).
- **PT (Packet Tracer)**



- Click host **172.16.31.3** and open the **Command Prompt**.
- Introduzca el comando **ping 172.16.31.2**. Este comando emitirá una serie de paquetes de solicitud de eco ICMP al destino. Si los paquetes llegan al destino, enviará un paquete de mensajes de respuesta de eco al origen de las solicitudes de ping.



- Haga clic en el botón **Modo de simulación** para cambiar al modo de simulación. Repita el comando **ping 172.16.31.2**. Aparece un ícono de sobre que representa una PDU junto a 172.16.31.3.

Cisco Packet Tracer - /Users/ahmed/Desktop/SOC-Accenture/Module3-Networking/Networking-exercises/H3.1.3-packet-tracer-identify-mac-and-ip-addresses.pka - Guest - 2024-06-13 07:01:46

**Nota:** Revise las Preguntas de reflexión en la Parte 3 antes de continuar con esta parte. Le dará una idea del tipo de información que necesitará recopilar. Haga clic en host 172.16.31.3 y abra el símbolo del sistema.

- Introduzca el comando **ping 172.16.31.2**. Este comando emitirá una serie de paquetes de solicitud de eco ICMP al destino. Si los paquetes llegan al destino, enviará un paquete de mensajes de respuesta de eco al origen de las solicitudes de ping.
- Haga clic en el botón **Modo de simulación** para cambiar al modo de simulación. Repita el comando **ping 172.16.31.2**. Aparece un icono de sobre que representa una PDU junto a 172.16.31.3.
- Haga clic en la PDU y localice la siguiente información en las pestanas **Modelo OSI** y **Detalles de PDU de salida**. La ficha **Outbound PDU Details** (Detalles de PDU de salida) muestra encabezados de paquetes y paquetes simplificados para la PDU. Debe observar los siguientes detalles sobre el direccionamiento para la PDU.

En el dispositivo: 172.16.31.3

Time Elapsed: 00:18:21

✓ Dock Check Results Back Next

Time: 00:19:26.874 PLAY CONTROLS ▶ | ▶ | ▶

(Select a Device to Drag and Drop to the Workspace)

Scenario 0 New Delete Toggle PDU List Window

Event List

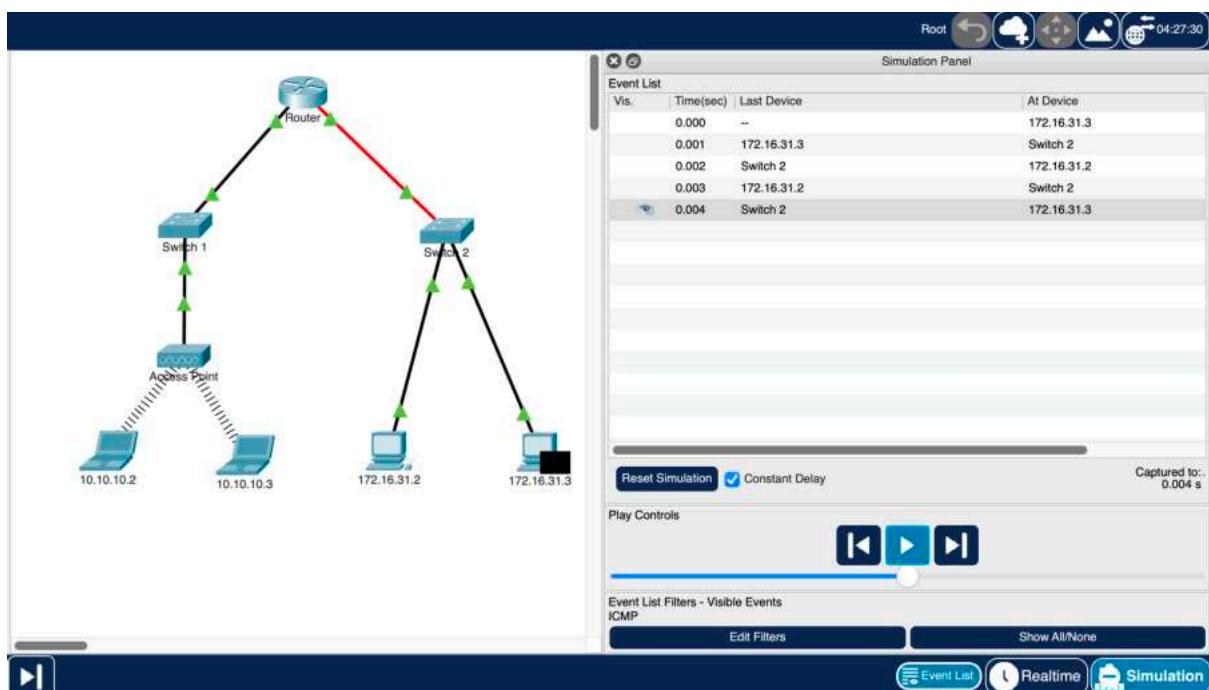
VIS.	Time(sec)	Last Device	At Device
150.251	--		
150.252	172.16.31.3		
150.253	Switch 2		
150.254	172.16.31.2		
150.255	Switch 2		

Reset Simulation Constant Delay Captured to: 150.255 s

Play Controls

Event List Filters - Visible Events ICMP Edit Filters Show All/None

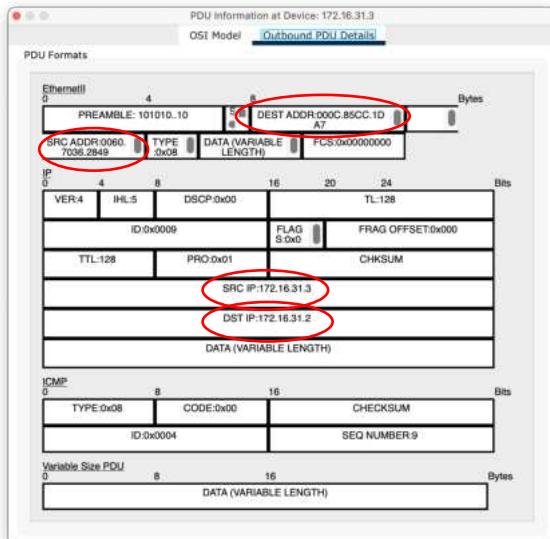
Event List Realtime Simulation



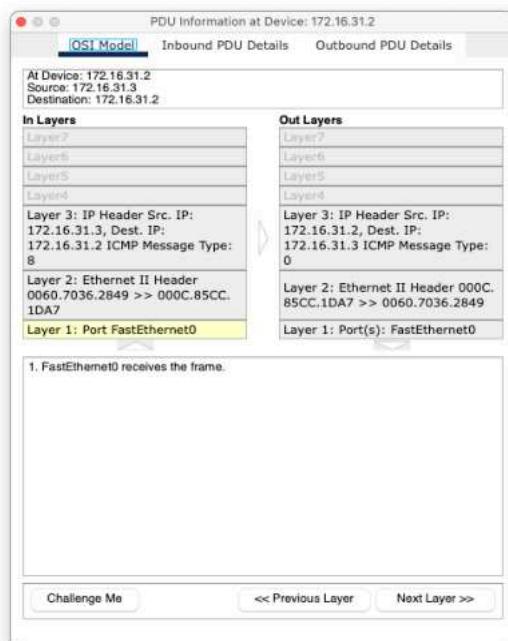
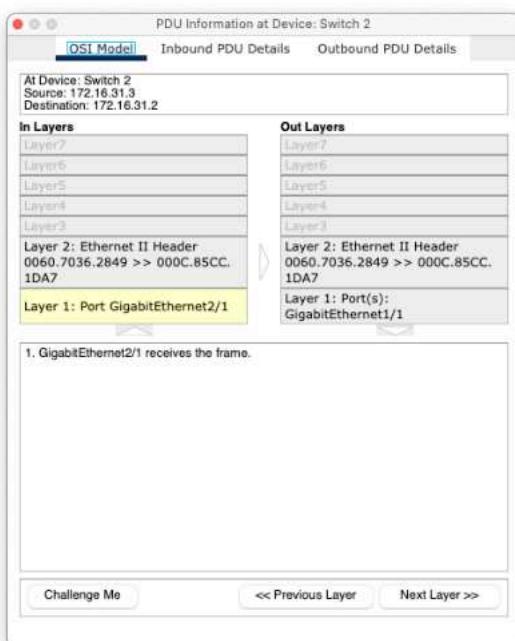
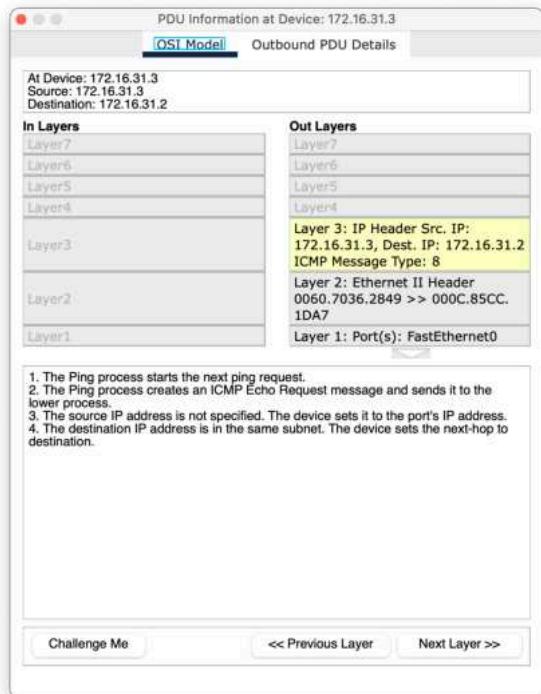
- Haga clic en la PDU y localice la siguiente información en las pestanas **Modelo OSI** y **Detalles de PDU de salida**. La ficha **Outbound PDU Details** (Detalles de PDU de salida) muestra encabezados de paquetes y paquetes simplificados para la PDU. Debe observar los siguientes detalles sobre el direccionamiento para la PDU.
  - En el dispositivo: **172.16.31.3**
  - Dirección MAC de origen: **0060.7036.2849**
  - Dirección MAC destino:**000C:85CC:1DA7**
  - Dirección IP de origen:**172.16.31.3**

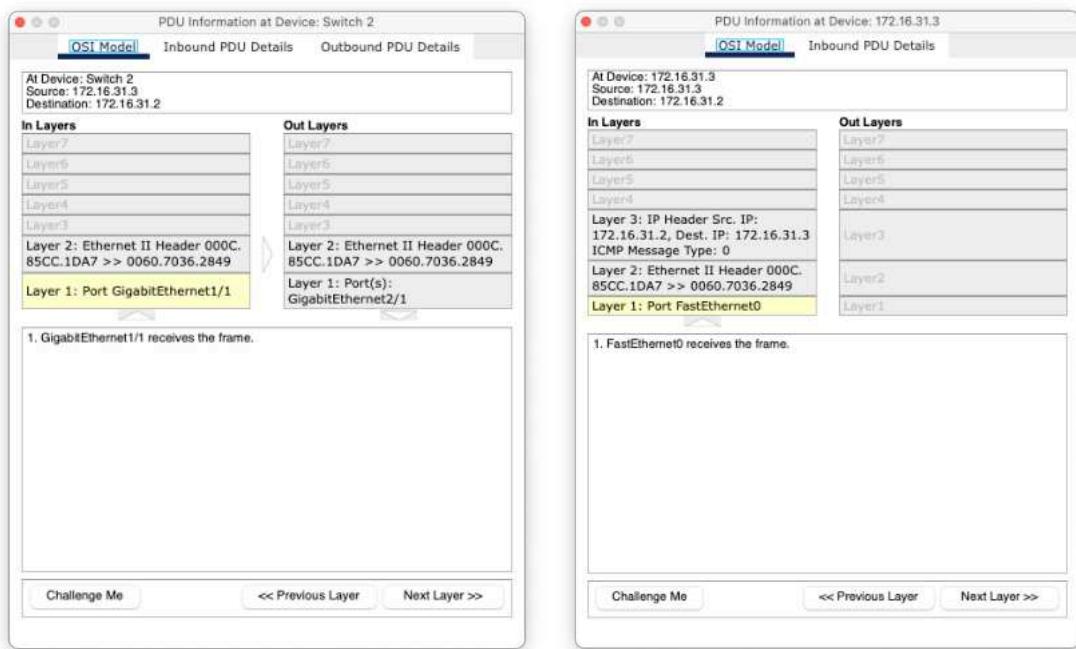
- Dirección IP destino: **172.16.31.2**

Procedemos a hacer click en cada uno de los pasos de la simulación para obtener los detalles de la ficha output de la PDU como se muestra a continuación.



- Haga clic en **Capture / Forward (la flecha derecha seguida de una barra vertical)** para mover la PDU al siguiente dispositivo. Use la pestaña del modelo OSI para recopilar la misma información del Paso 1d. Repita este proceso hasta que la PDU llegue al destino. Para cada paso de la ruta de entrega, registre la información de cada PDU en una hoja de cálculo que utilice un formato como el de la tabla que se muestra a continuación. La información para el primer paso se muestra en la tabla.
- Mostramos las pestañas del modelo OSI de cada paso de la PDU.



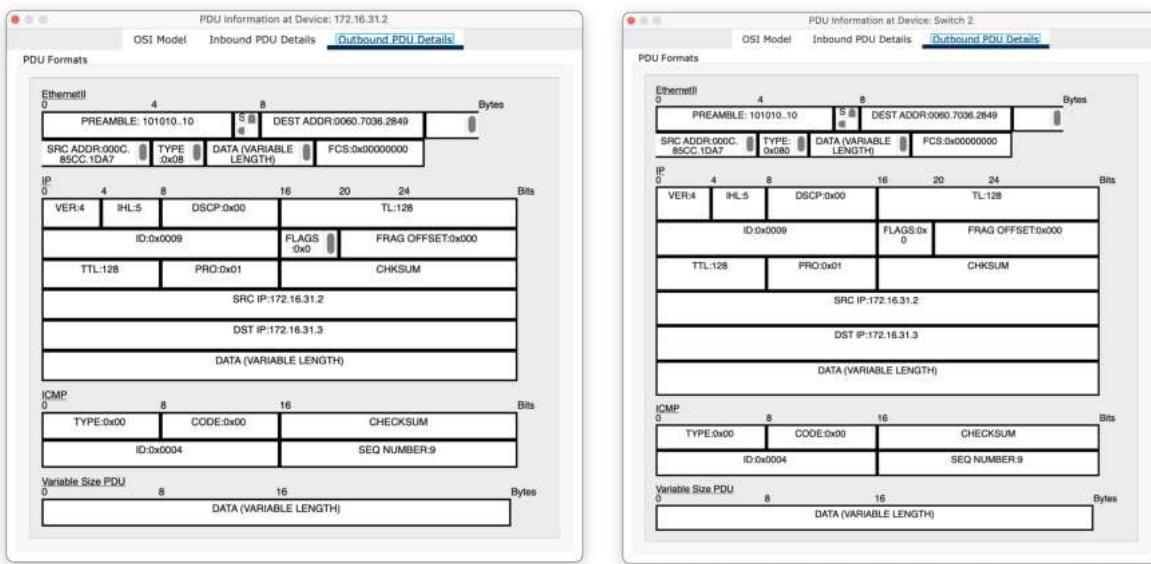
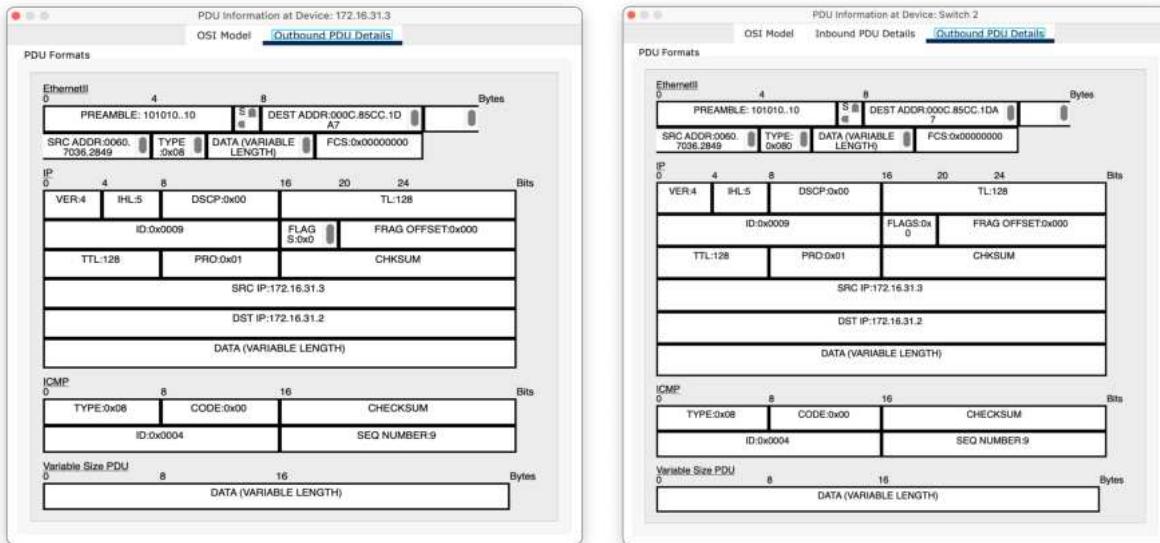


En dispositivo	MAC de origen	MAC de destino	IPv4 de origen	IPv4 de destino
172.16.31.3 (origen)	0060.7036.2849	000C:85CC:1DA7	172.16.31.3	172.16.31.2
Switch 2 (entrada y salida)	0060.7036.2849	000C:85CC:1DA7	-	-
172.16.31.2 (in) (destino entrada)	0060.7036.2849	000C:85CC:1DA7	172.16.31.3	172.16.31.2
172.16.31.2 (out) (destino salida)	000C:85CC:1DA7	0060.7036.2849	172.16.31.2	172.16.31.3

f. Notará que la información para la PDU entrante no cambia. En la ventana de información de la PDU, haga clic en la ficha de la PDU saliente. ¿En qué se diferencia el direccionamiento y por qué? Registre el direccionamiento en su tabla.

Al observar la información en la pestaña “OSI Model”, la información de las direcciones MAC e IP de la PDU entrante no cambia a medida que pasa por los switches, pero cambia cuando llega y sale del dispositivo de destino 172.16.31.2.

- Información Outbound:



### Diferencias en el Direcciónamiento:

- En la PDU saliente desde 172.16.31.3, la dirección MAC de origen es 0060.7036.2849 y la dirección MAC de destino es 000C:85CC:1DA7.
- Cuando la PDU llega a 172.16.31.2, la dirección MAC de destino se convierte en la dirección MAC del dispositivo 172.16.31.2.
- En la PDU saliente desde 172.16.31.2, las direcciones MAC se intercambian. Ahora, la dirección MAC de origen es 000C:85CC:1DA7 y la dirección MAC de destino es 0060.7036.2849.

### Razón de la Diferencia:

- Los cambios en las direcciones MAC se deben al funcionamiento de la capa 2 del modelo OSI, donde cada salto en la red utiliza direcciones MAC para identificar el siguiente dispositivo en la ruta hacia el destino final.

- En este caso específico, la dirección de origen y de destino se invierten tanto en la trama como en el paquete porque esta PDU se enviará de vuelta al host 172.16.31.3. Este mensaje será una respuesta de eco de ping, por lo que las direcciones se intercambian para que la respuesta pueda regresar al host original.

g. Vuelva al modo **Realtime**.

## **Parte 2: Recopilar información de PDU para la comunicación de red remota**

Para comunicarse con redes remotas, es necesario un dispositivo de puerta de enlace predeterminada. El dispositivo de puerta de enlace predeterminada conecta dos o más redes. En esta parte, estudiará el proceso que tiene lugar cuando un dispositivo se comunica con otro dispositivo que está en una red remota. Preste mucha atención a las direcciones MAC utilizadas.

**Nota:** Pase el mouse por el **Router**. Verá información sobre el direccionamiento de las interfaces del router. Consulte estas direcciones mientras observa el flujo de la PDU a través del router.

- Regrese al **símbolo del sistema** para **172.16.31.3**.
- Introduzca el comando **ping 10.10.10.2**. Los primeros pings pueden agotar el tiempo de espera.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.31.2

Pinging 172.16.31.2 with 32 bytes of data:
Reply from 172.16.31.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 35ms, Average = 8ms

C:\>ping 172.16.31.2

Pinging 172.16.31.2 with 32 bytes of data:
Reply from 172.16.31.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

E:\>clear
Invalid Command.

C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.

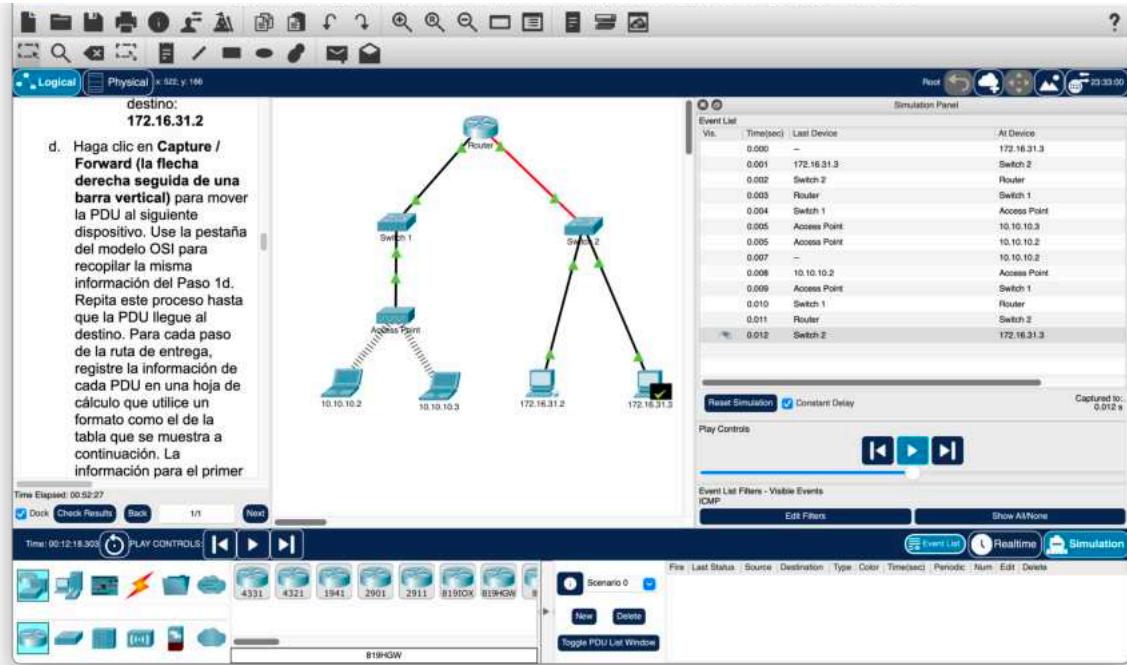
Reply from 10.10.10.2: bytes=32 time=25ms TTL=127
Reply from 10.10.10.2: bytes=32 time=3ms TTL=127
Reply from 10.10.10.2: bytes=32 time=3ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 37ms, Average = 31ms

C:\>

```

- c. Cambie al **modo de simulación** y repita el comando **ping 10.10.10.2**. A PDU appears next to 172.16.31.3.



- d. Haga clic en la PDU y observe la siguiente pestaña de información:

- En el dispositivo: 172.16.31.3
- Dirección MAC de origen: 0060.7036.2849
- Dirección MAC destino: 00D0:BA8E:741A
- Dirección IP de origen: 172.16.31.3
- Dirección IP destino: 10.10.10.2

¿Qué dispositivo tiene la MAC de destino que se muestra?

Pasamos el ratón por encima del router como se indica y vemos la siguiente información:

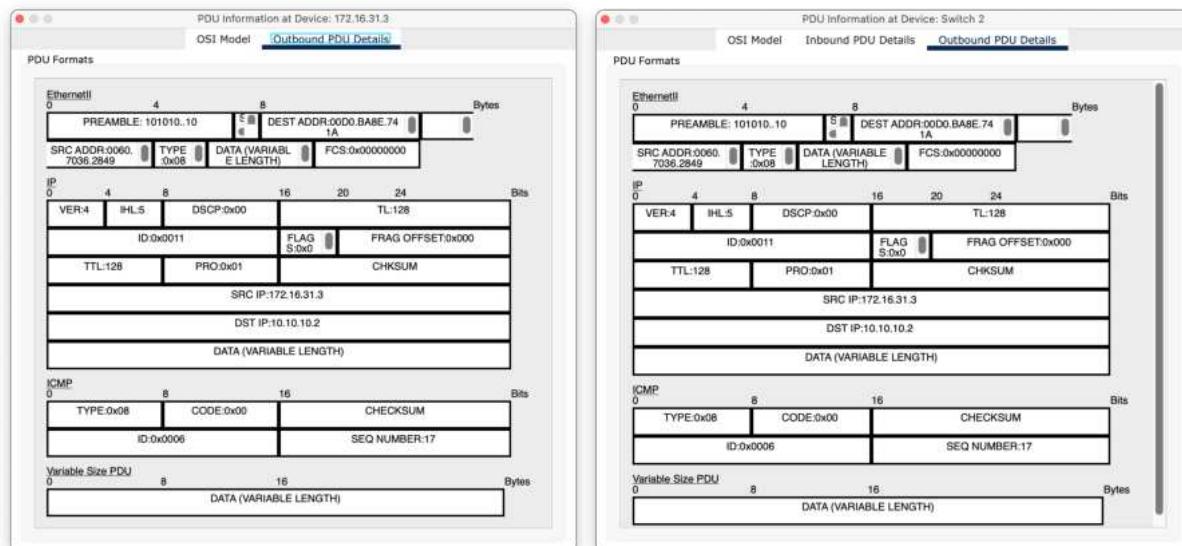
Device Name: Router				
Device Model: 2621XM				
Hostname: Router				
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	10.10.10.1/24	<not set>	00D0.588C.2401
FastEthernet0/1	Down	<not set>	<not set>	00D0.588C.2402
Serial0/0	Down	<not set>	<not set>	<not set>
Serial0/1	Down	<not set>	<not set>	<not set>
FastEthernet1/0	Up	172.16.31.1/24	<not set>	00D0.BA8E.741A
Physical Location: Intercity > Home City > Office Building > Primary Network > Rack > Router				

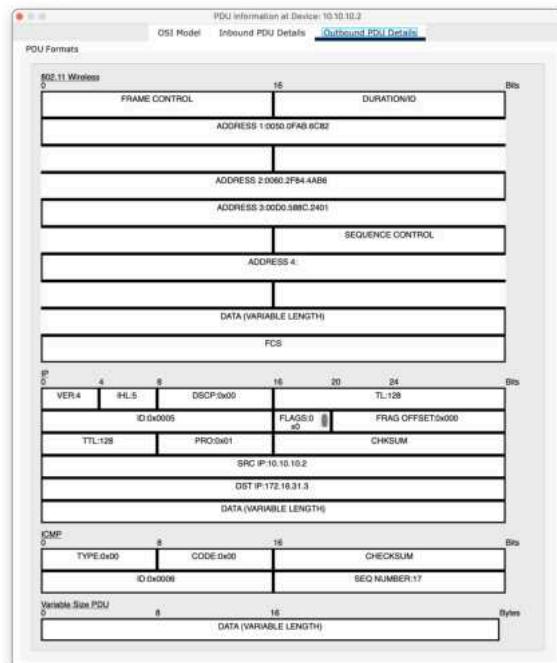
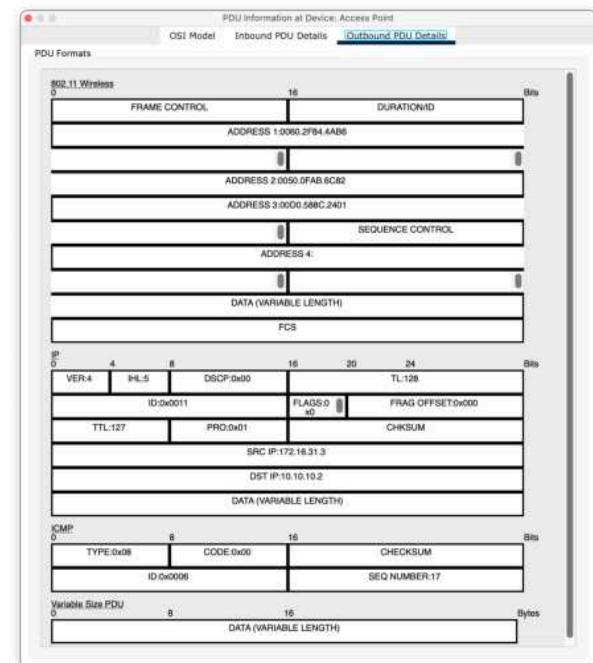
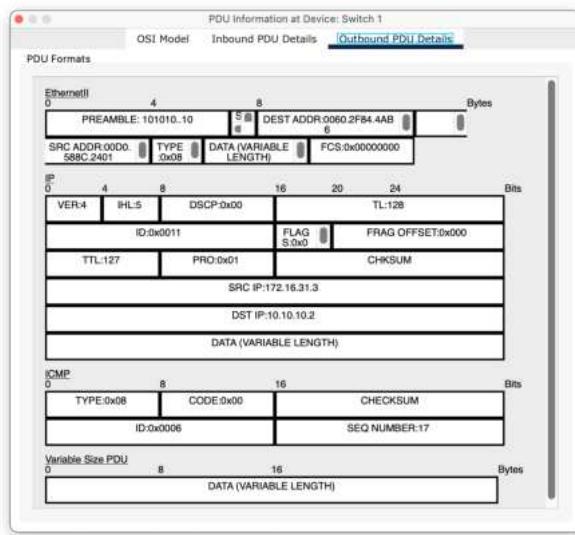
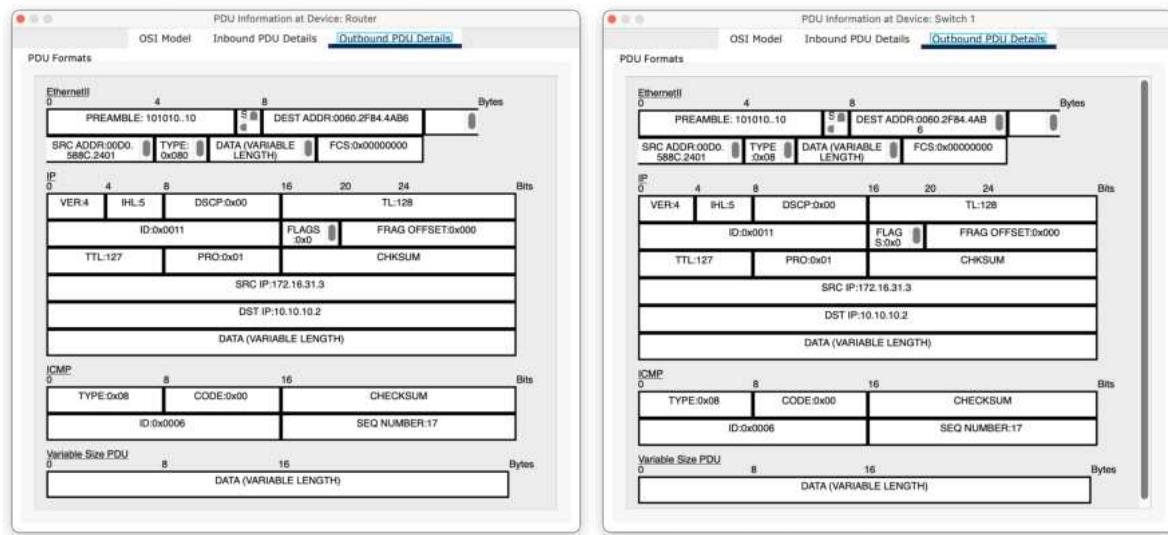
Aquí se puede ver que efectivamente en este caso la solución del ejercicio coincide y es correcta. La MAC de destino 00D0:BA8E:741A corresponde al puerto de la interfaz del router FastEthernet1/0.

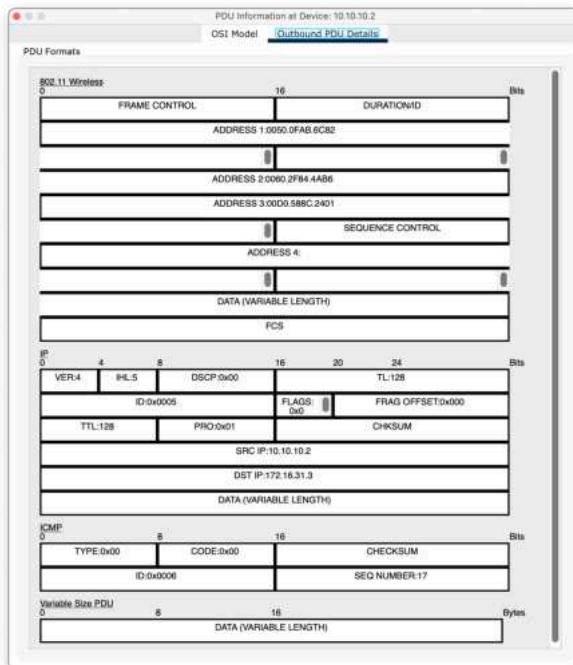
>La interfaz del router FasteEthernet1 / 0

- e. Haga clic en **Capture / Forward** (la flecha derecha seguida de una barra vertical) para mover la PDU al siguiente dispositivo. Reúna la misma información del paso 1d. Repita este proceso hasta que la PDU llegue al destino. Registre la información de la PDU que recopiló del ping 172.16.31.3 a 10.10.10.2 en una hoja de cálculo utilizando un formato como la tabla de muestra que se muestra a continuación. Ingrese los detalles de las PDU entrantes y salientes en el router.

En dispositivo	MAC de origen	MAC de destino	IPv4 de origen	IPv4 de destino
172.16.31.3	0060.7036.2849	00D0:BA8E:741A	172.16.31.3	10.10.10.2
Switch 2	0060.7036.2849	00D0:BA8E:741A	172.16.31.3	10.10.10.2
Router	00D0:588C:2401	0060:2 F84:4AB6	172.16.31.3	10.10.10.2
Switch 1	00D0:588C:2401	0060:2 F84:4AB6	172.16.31.3	10.10.10.2
Access Point	00D0:588C:2401	0060:2 F84:4AB6	172.16.31.3	10.10.10.2
10.10.10.2	0060:2 F84:4AB6	00D0:588C:2401	10.10.10.2	172.16.31.3

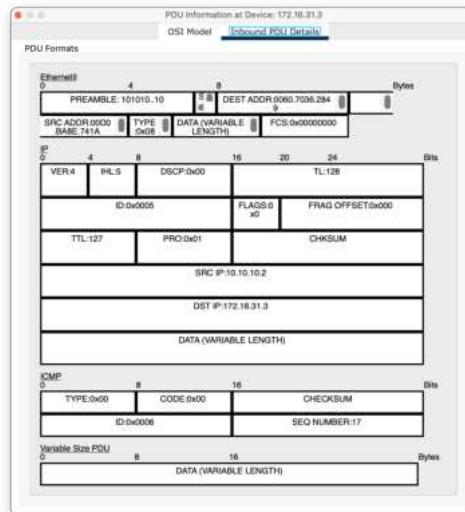
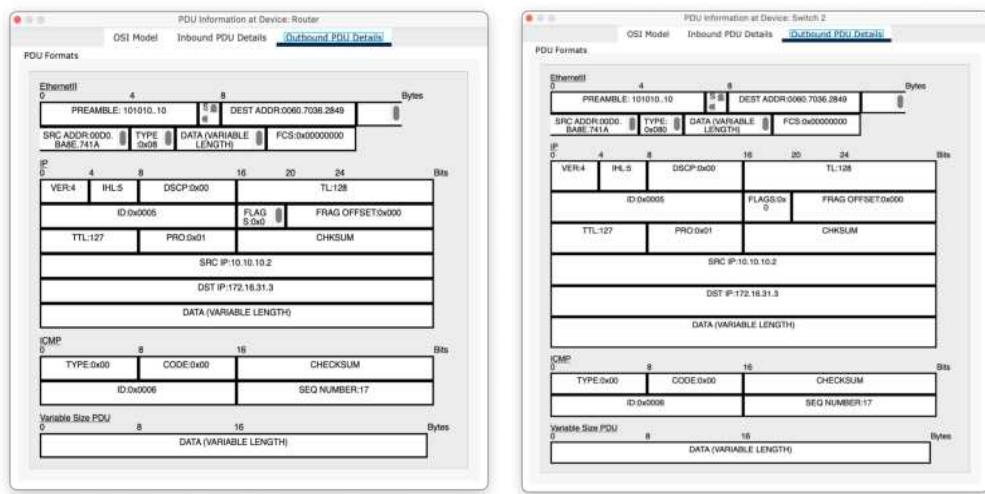
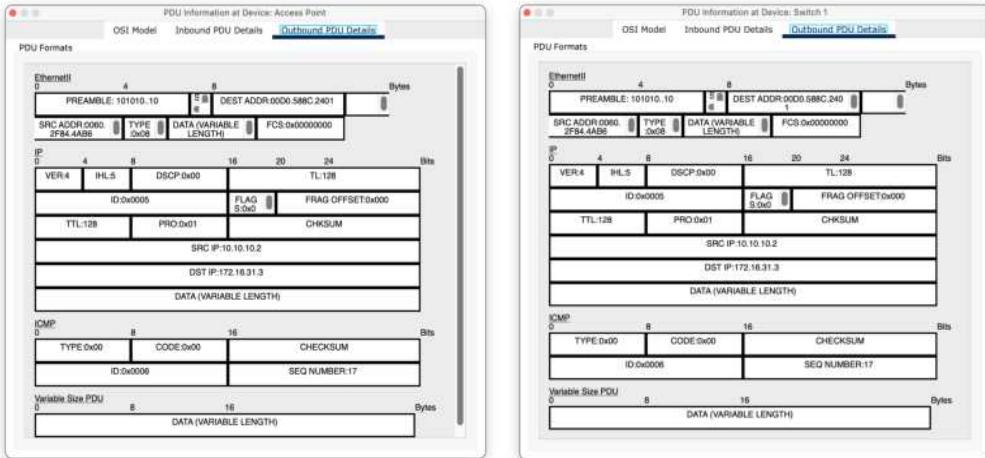


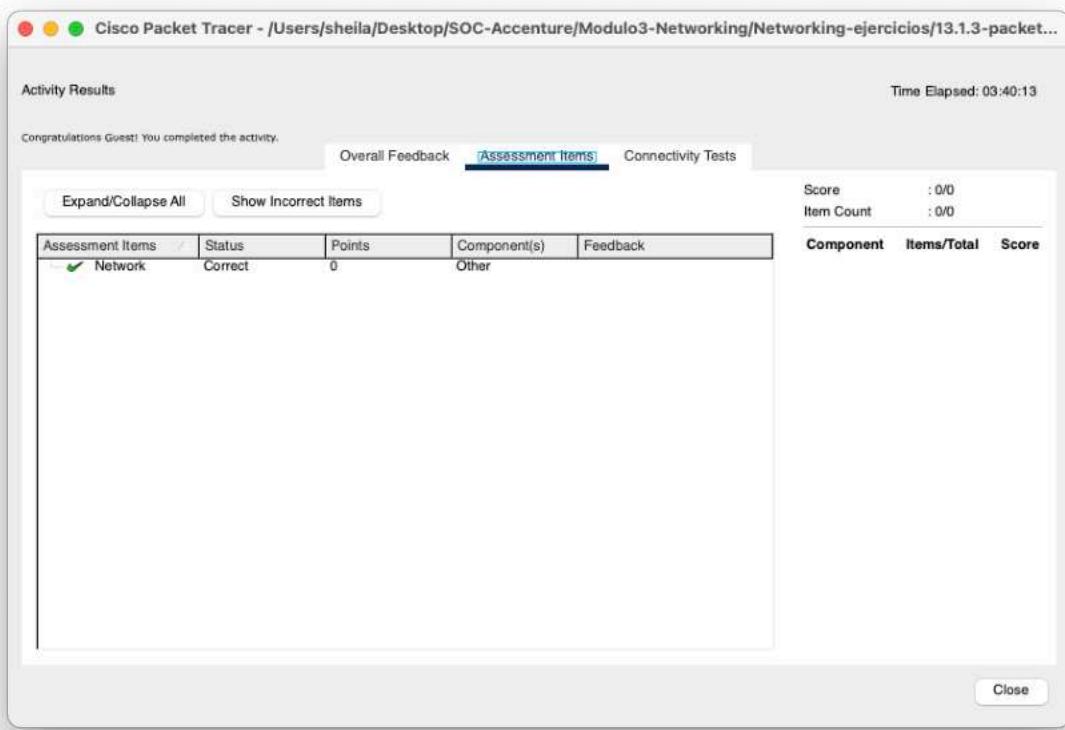




f. Repita el proceso para el mensaje de respuesta de eco que se origina en el host 10.10.10.2. Complete la tabla para cada paso.

En dispositivo	MAC de origen	MAC de destino	IPv4 de origen	IPv4 de destino
10.10.10.2	00:00:00:00:0F:AB:6C82	00:D0:58:8C:24:01	10.10.10.2	172.16.31.3
Access Point	00:00:00:00:00:00	00:D0:58:8C:24:01	10.10.10.2	172.16.31.3
Switch 1	00:00:00:00:00:00	00:D0:58:8C:24:01	10.10.10.2	172.16.31.3
Router	00:D0:BA:8E:74:1A	00:00:00:00:00:00	10.10.10.2	172.16.31.3
Switch 2	00:D0:BA:8E:74:1A	00:00:00:00:00:00	10.10.10.2	172.16.31.3
172.16.31.3	00:D0:BA:8E:74:1A	00:00:00:00:00:00	10.10.10.2	172.16.31.3





## Tarea 5: Observar el flujo de tráfico en una red enrutada (apartado 14.3.3. del curso)

### Packet Tracer: observe el flujo de tráfico en una red enrutada

#### Objetivos

**Parte 1: Observar el flujo de tráfico en una LAN no enrutada**

**Parte 2: Reconfigurar la red para enrutar entre las LAN**

**Parte 3: Observar el flujo de tráfico en la red enrutada**

#### Aspectos básicos/Situación

Se le ha pedido a la empresa para la que trabaja que proponga un nuevo diseño de red para XYZ LLC. XYZ es una empresa nueva que recientemente ha tenido éxito con sus ofertas de productos. Se expandirán y su red deberá crecer con ellos. Actualmente, la red está configurada con una única red IP para hosts en todos los departamentos. Este diseño se ha vuelto ineficiente y las demoras en la red son cada vez más notorias. Se le ha pedido que ayude a preparar la propuesta con el equipo de ventas. El equipo de ventas propondrá una solución en la que se mejorará la eficiencia de la red mediante la implementación de enrutamiento entre redes de departamentos separadas. Está trabajando en una demostración de cómo tener varias redes

enrutadas en una empresa puede mejorar la eficiencia de la red. Siga las instrucciones para realizar la demostración y proponer una nueva red a XYZ LLC.

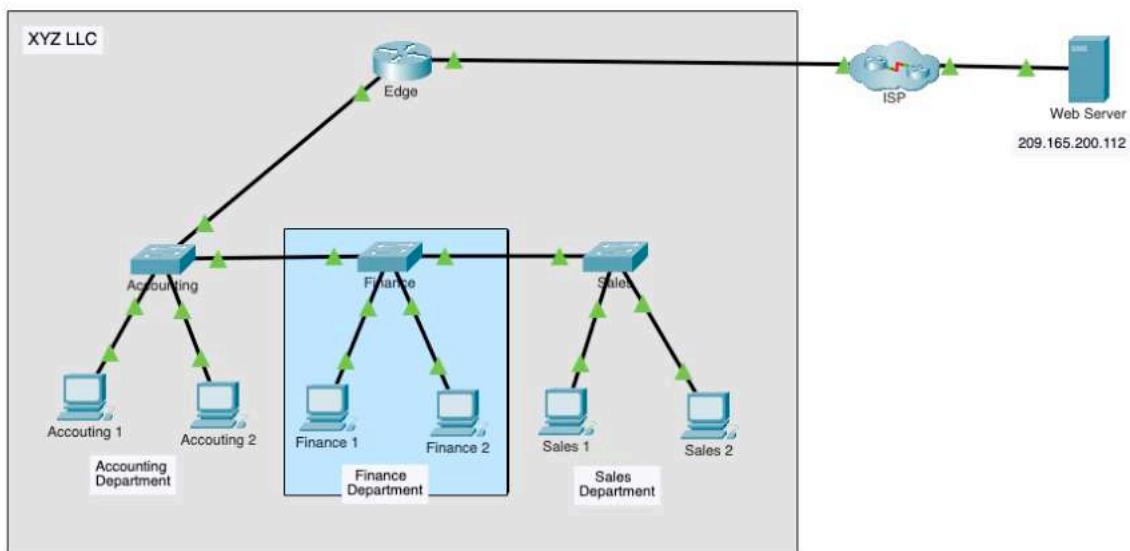
## Instrucciones

### Parte 1: Observar el flujo de tráfico en una LAN no enrutada

La red XYZ consta de aproximadamente 150 dispositivos que están conectados a una LAN. La LAN está configurada en una sola red IPv4. Los hosts en diferentes departamentos se conectan a switches que luego se conectan al router **Edge**. El router solo enruta el tráfico entre la LAN e Internet, representado por la nube del **ISP**. Dado que solo se utiliza una red IP en la LAN, todos los departamentos están en la misma red.

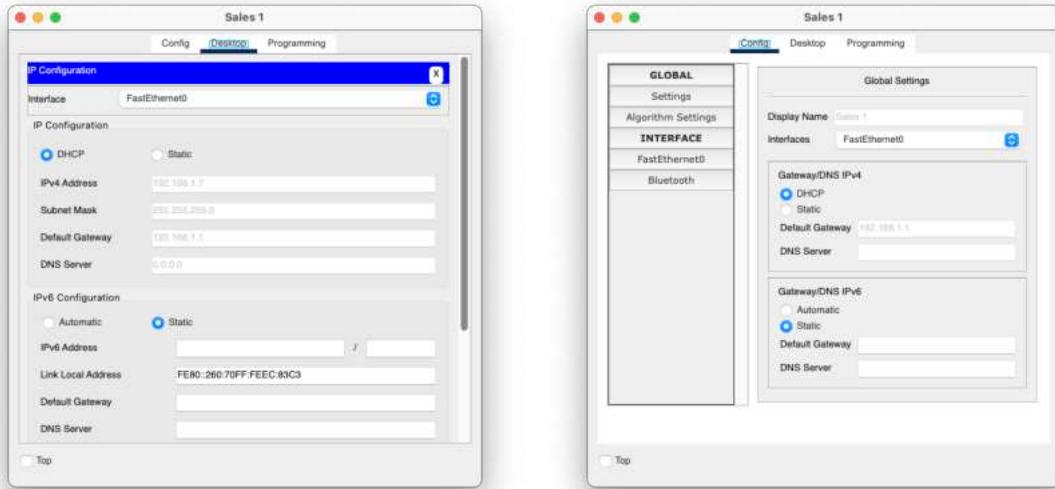
La topología de Packet Tracer está simplificada. Solo muestra algunos de los departamentos y hosts. Suponga que el comportamiento que demostrará sucede a una escala mucho mayor que la que se muestra en la red de PT.

En esta parte, utilizará el modo de simulación de Packet Tracer para observar cómo fluye el tráfico a través de una LAN no enrutada.



### Paso 1: Borre la caché de ARP en el host de Sales 1.

Pase el mouse sobre el host de **Sales 1** para ver su dirección IP. Anótelo.



Si ponemos el ratón sobre Sales 1 tal y como pide el ejercicio obtenemos la información que obtenemos es la siguiente:

```

Device Name: Sales 1
Device Model: PC-PT

Port      Link    IP Address        IPv6 Address          MAC Address
FastEthernet0 Up      192.168.1.3/24 <not set>           0060.70EC.83C3
Bluetooth   Down   <not set>       <not set>           0090.2B7A.3D31

Gateway: 192.168.1.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Sales 1
  
```

Este ejercicio se tuvo que volver a descargar y entonces haciendo lo mismo se obtuvo otra IP:

```

Device Name: Sales 1
Device Model: PC-PT

Port      Link    IP Address        IPv6 Address          MAC Address
FastEthernet0 Up      192.168.1.2/24 <not set>           0060.70EC.83C3
Bluetooth   Down   <not set>       <not set>           0090.2B7A.3D31

Gateway: 192.168.1.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Sales 1
  
```

Para corroborar se realiza un ipconfig en Sales 1.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....:: FE80::260:70FF:FE0C:83C3
IPv6 Address.....:: ::1
IPv4 Address.....:: 192.168.1.2
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: 192.168.1.1

Bluetooth Connection:

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....:: ::1
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: 0.0.0.0

C:\>

```

- Haga clic en **Sales 1**> pestaña **Desktop** (Escritorio)> **Símbolo del sistema** y escriba el comando **arp -a**. No debe haber direcciones MAC en la caché de ARP. Si hay entradas en la caché de ARP, utilice el comando **arp -d** para eliminarlas.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>

```

ARP (Address Resolution Protocol) es un protocolo utilizado en redes para mapear direcciones IP a direcciones MAC (Media Access Control). Esencialmente, ARP permite que los dispositivos de una red local encuentren la dirección MAC correspondiente a una dirección IP para poder comunicarse entre sí.

En este caso no tenemos caché de ARP como se esperaba, por tanto, no ha sido necesario borrarlo.

### **Paso 2: Observe el flujo de tráfico en la red.**

- Haga clic en el botón **Modo de simulación** en la esquina inferior derecha de la ventana del PT para pasar del modo **tiempo real** al de **simulación**.
- Abra el **símbolo del sistema** para **Sales 2** e introduzca el comando **ping** seguido de la dirección IP de **Sales 1**.

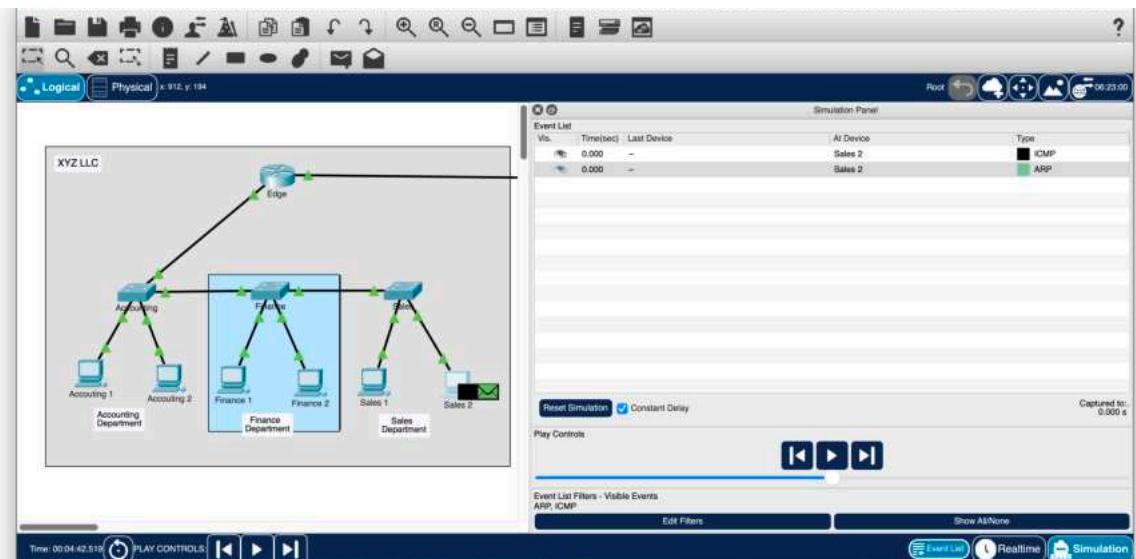
Sales 2

Config Desktop Programming

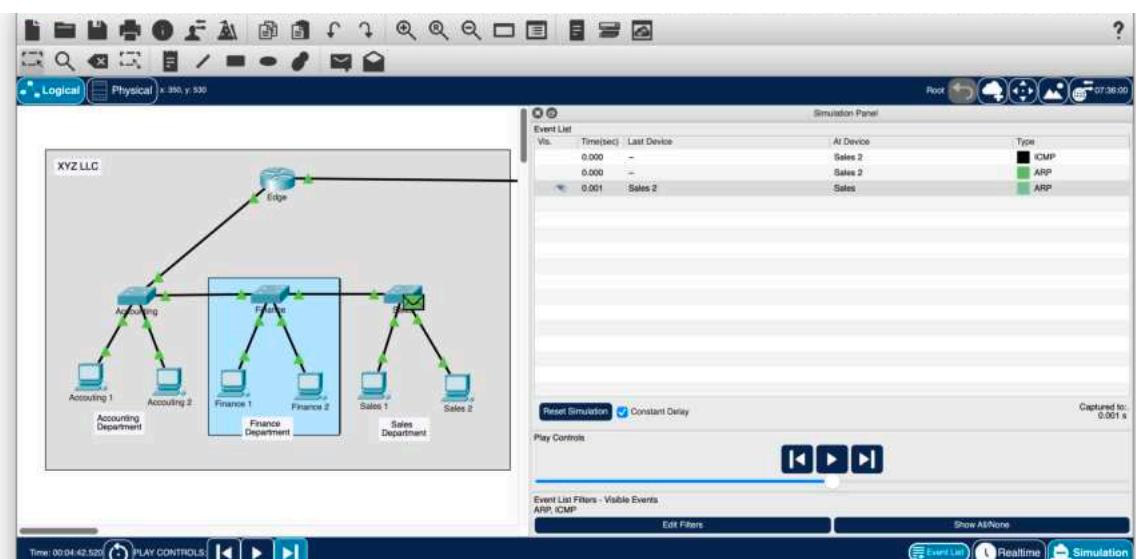
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2
Ping request could not find host 192.168.2. Please check the name and try again.
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
```

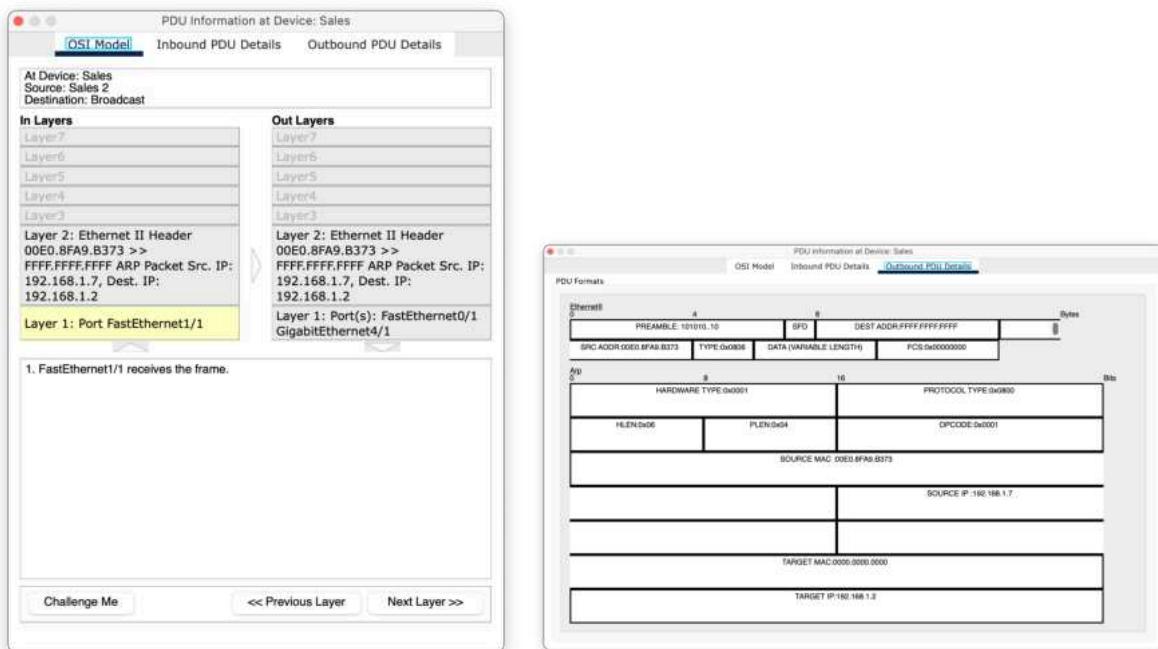
- c. Utilice el botón **Capture then Forward** (Capturar y Avanzar) (el triángulo que apunta hacia la derecha con una barra vertical adjunta) en los **controles de reproducción del panel de simulación** para comenzar a ejecutar el comando ping. Verá un ícono de sobre de color junto a Ventas 2. Esto representa una PDU. Haga clic en el botón **Capture then Forward** para mover la PDU al primer dispositivo en su ruta al dispositivo de destino. Haga clic en el sobre de la PDU para inspeccionar el contenido.



Se realiza el Capture then Forward:



Clicamos el paquete y obtenemos la siguiente ficha:



### ¿Cuáles son las direcciones IP y MAC de origen y destino para la trama y el paquete?

- IP de origen: 192.168.1.7
- MAC de origen: 00E0.8FA9.B373
- IP de destino: 192.168.1.2
- MAC de destino: FFFF.FFFF.FFFF (esta es una dirección MAC de broadcast, lo que significa que el paquete está siendo enviado a todos los dispositivos de la red local).

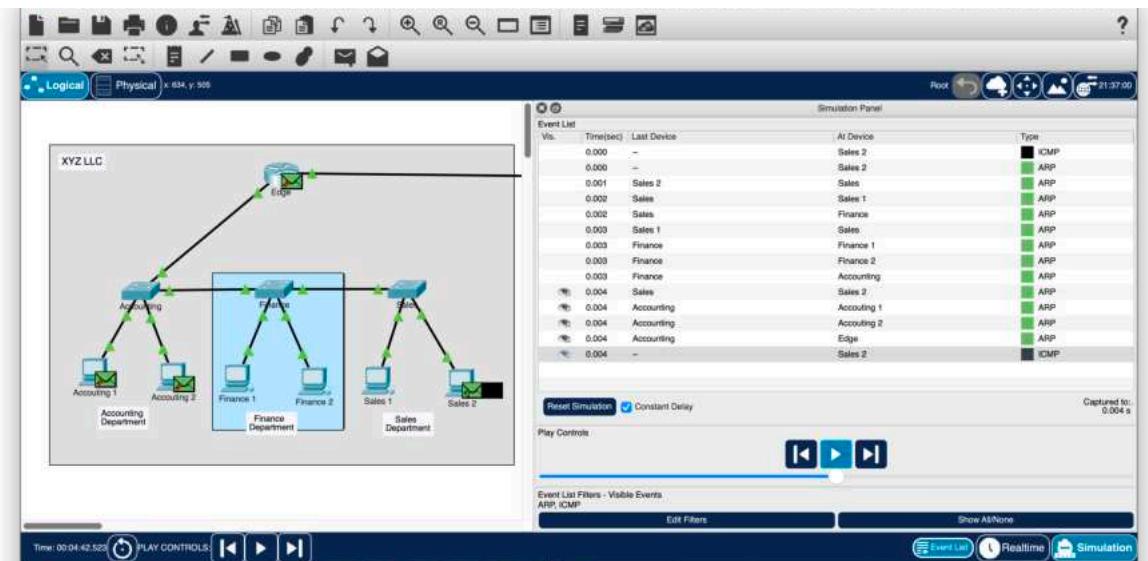
**La dirección MAC de origen de la trama es la dirección MAC de Sales 1. La dirección MAC de destino es la dirección de difusión MAC de FFFF.FFFF.FFFF. La dirección IP de origen del paquete es la dirección IP de Sales 1. La dirección IP de destino es el destino de Sales 2.**

### ¿Por qué la dirección MAC de destino es la dirección de difusión?

La dirección MAC de destino es la dirección de difusión (broadcast) FFFF.FFFF.FFFF en este caso porque el paquete es un mensaje ARP (Address Resolution Protocol) request.

**Debido a que la memoria caché ARP del host está vacía, el host primero debe emitir una solicitud ARP para obtener la dirección MAC de destino para que la trama pueda dirigirse a Sales 1.**

- Avance las PDU a través de la red hasta que se cree una nueva PDU (color diferente) en Sales 2.



## ¿Qué hosts y otros tipos de dispositivos necesitaban procesar los paquetes de solicitud de ARP?

Para determinar qué hosts y dispositivos procesaron los paquetes de solicitud de ARP (ARP requests), debemos observar la lista de eventos y el diagrama de red.

### Dispositivos que procesaron los ARP Requests

Se puede observar en la lista de eventos que las solicitudes ARP han sido procesadas por todos los hosts y dispositivos en la red.

Los siguientes hosts y dispositivos de red procesaron los paquetes de solicitud de ARP:

- **Hosts:**
  - Sales 2
  - Sales 1
  - Finance 2
  - Finance 1
  - Accounting 1
  - Accounting 2
- **Dispositivo de red:**
  - Edge Router

Estos dispositivos recibieron y procesaron los ARP requests según se detalla en la lista de eventos de la simulación. La razón de este procesamiento es que los ARP requests son difundidos en la red local para obtener la dirección MAC correspondiente a una dirección IP específica, como se explicó anteriormente.

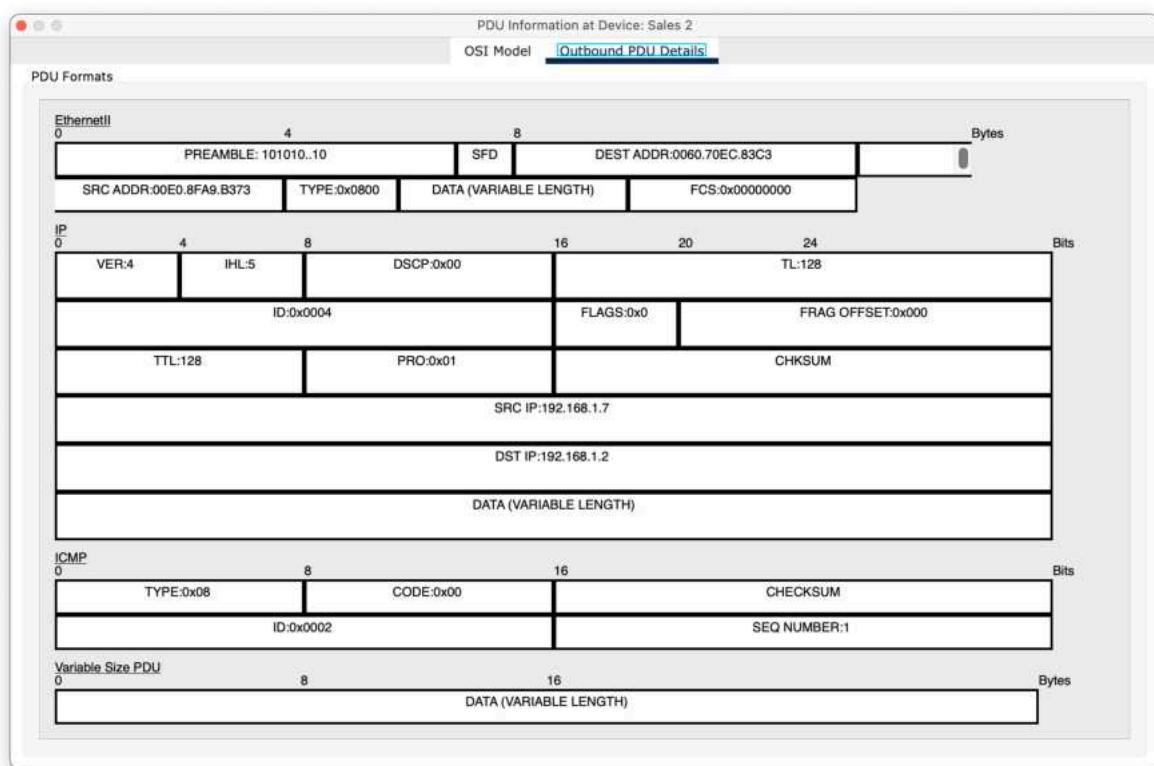
**Todos los hosts y la interfaz del router.**

¿Cuál es el impacto de esto en el funcionamiento eficiente de la red como está configurada actualmente?

**Aunque el destino de las solicitudes de ping puede ser adyacente al origen solicitante, si el host tiene una memoria caché ARP vacía, se envía una solicitud ARP que debe ser procesada por cada host en la red. Las entradas de caché ARP se eliminan después de un período de tiempo predeterminado. Con muchos hosts en una red, las transmisiones ARP se emitirán con más frecuencia. Esto requiere que se tomen recursos de la red de debería ser para tráfico relacionado con el trabajo.**

- e. En Sales 2, apareció una nueva PDU con un color diferente. Haga clic en la nueva PDU e inspeccione su contenido. Mire los detalles de la PDU de salida.

¿Qué tipo de PDU es esta?



**Es el primer paquete de solicitud de eco ICMP emitido por ping desde el host Sales 2.**

- f. Vuelva al modo Realtime.

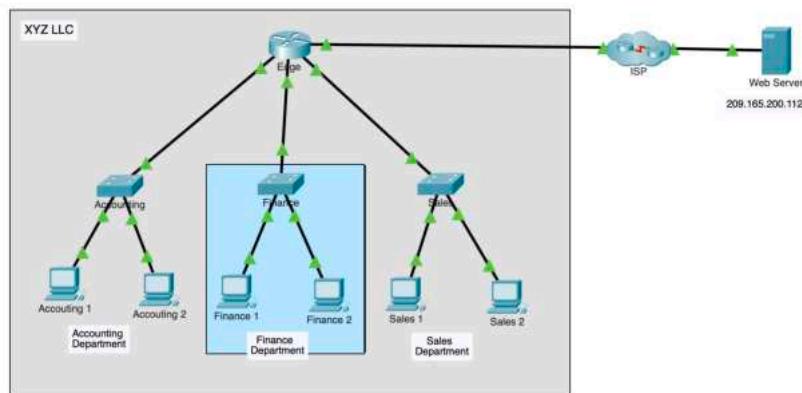
## Parte 2: Reconfigurar la red para enrutar entre las LAN.

En esta parte, demostrará los beneficios del enrutamiento entre redes de departamentos. Primero, cableará cada switch de red para conectarse directamente a una interfaz de router. Luego, reconfigurará los hosts para recibir direcciones en dos redes IPv4 nuevas creadas por el router.

### Paso 1: Cambie las conexiones de los dispositivos.

Los tres switches están conectados entre sí con cables directos de cobre.

- Para el cable que conecta el switch de **contabilidad** con el switch de **finanzas**, haga clic en el triángulo verde en el lado del enlace del switch de **contabilidad**.
- Arrastre el extremo del cable al router **Edge** y conéctelo al puerto **GigabitEthernet 1/0**.
- Repita este paso para el enlace entre **finanzas** y **ventas**. Conéctese al puerto GigabitEthernet disponible.

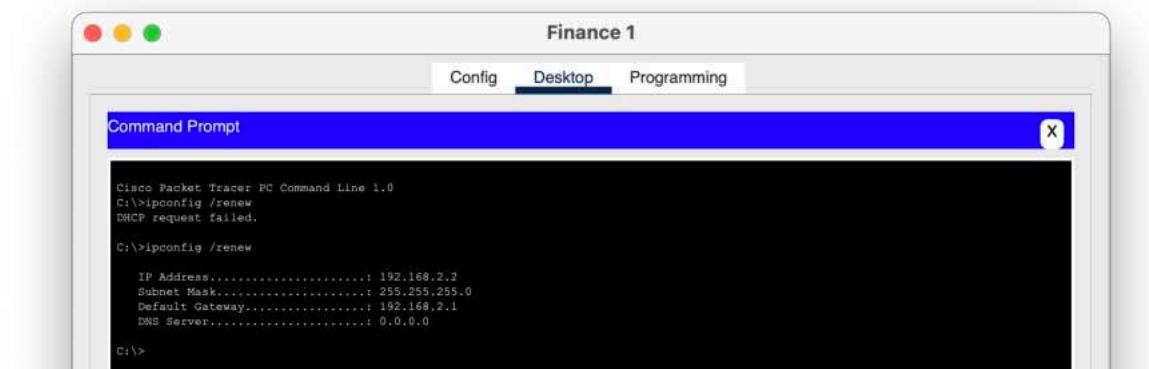


## Paso 2: Configure los hosts con direcciones en las nuevas LAN.

Cada interfaz del router **Edge** se configuró previamente para poner a cada departamento en su propia red IPv4. Los hosts recibirán sus nuevas direcciones IP del router. Sin embargo, llevará tiempo para que los hosts en las redes de **finanzas** y **ventas** reciban sus nuevas direcciones IP. (Los hosts en la red de contabilidad permanecerán en 192.168.1.0/24).

- Para acelerar el proceso de obtención de nuevas direcciones IP, abra un **símbolo del sistema** en cada uno de los cuatro dispositivos en las redes de **finanzas** y **ventas**.
- Ingrese el comando **ipconfig /renew**. Esto obligará al host a solicitar una nueva dirección IP del servidor DHCP que corre en el router **Edge**. Debería ver la confirmación del nuevo direccionamiento IP.

¿Qué red IPv4 se asigna a la red de **finanzas**?



- El comando **ipconfig /renew** parece no haber funcionado en finance 2.

- Sin embargo, la dirección IP 192.168.2.3 es correcta y parece haber sido asignada correctamente tras consultar la resolución del ejercicio.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew
ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:43FF:FE84:A978
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.2.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ipconfig /renew

```

Observamos las IP del departamento de finanzas:

Device Name: Finance 1		Device Model: PC-PT	
Port	Link	IP Address	IPv6 Address
FastEthernet0	Up	192.168.2.2/24	<not set>
Bluetooth	Down	<not set>	<not set>
		MAC Address	
		00D0.972C.9DA6	
		00E0.F7A1.7EBA	
Gateway: 192.168.2.1			
DNS Server: <not set>			
Line Number: <not set>			
Physical Location: Intercity > Home City > Corporate Office > Finance 1			

Device Name:	Finance 2			
Device Model:	PC-PT			
Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.2.3/24	<not set>	0001.4384.A978
Bluetooth	Down	<not set>	<not set>	00D0.587C.80D8
Gateway: 192.168.1.1				
DNS Server: <not set>				
Line Number: <not set>				
Physical Location: Intercity > Home City > Corporate Office > Finance 2				

## Información de Configuración de los Dispositivos Finance

### 1. Finance 1:

- Dirección IP: 192.168.2.2
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada (Gateway): 192.168.2.1

### 2. Finance 2:

- Dirección IP: 192.168.2.3
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada (Gateway): 192.168.1.1

## Determinación de la Red IPv4 Asignada

Ambos dispositivos en la red de finanzas tienen direcciones IP que pertenecen a la subred 192.168.2.0/24. La máscara de subred 255.255.255.0 confirma que se trata de una red /24, es decir, que la red tiene 256 direcciones posibles (de 192.168.2.0 a 192.168.2.255).

Por tanto, la red IPv4 asignada a la red de finanzas es:

- **192.168.2.0/24**

**192.168.2.0/24**

¿Qué red IPv4 se asigna a la red de ventas?

Sales 1

Config Desktop Programming

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::260:70FF:FE0C:83C3
IPv4 Address.....: ::1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
192.168.1.1

Bluetooth Connection:
Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
0.0.0.0

C:\>ipconfig /renew

IP Address.....: 192.168.3.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.1
DNS Server.....: 0.0.0.0

C:\>
```

Sales 2

Config Desktop Programming

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2
Ping request could not find host 192.168.2. Please check the name and try again.
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ipconfig /renew

IP Address.....: 192.168.3.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.3.1
DNS Server.....: 0.0.0.0

C:\>
```

Device Name:	Sales 1		
Device Model:	PC-PT		
Port	Link	IP Address	IPv6 Address
FastEthernet0	Up	192.168.3.2/24	<not set>
Bluetooth	Down	<not set>	<not set>
Gateway:	192.168.3.1		
DNS Server:	<not set>		
Line Number:	<not set>		
Physical Location:	Intercity > Home City > Corporate Office > Sales 1		

```

Device Name: Sales 2
Device Model: PC-PT

Port      Link   IP Address          IPv6 Address           MAC Address
FastEthernet0 Up     192.168.3.3/24 <not set>            00E0.8FA9.B373
Bluetooth Down  <not set>          <not set>            0060.3E34.25EC

Gateway: 192.168.3.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Sales 2

```

**192.168.3.0/24**

### Parte 3: Observar el flujo de tráfico en la red enrutada.

En esta parte, observará cómo el tráfico ahora fluye a través de una red enrutada.

#### Paso 1: Haga ping a Sales 1 de Sales 2.

- Vuelva al **símbolo del sistema** de Sales 2 y verifique que su caché ARP esté vacía. Si no es así, elimine las entradas.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2
Ping request could not find host 192.168.2. Please check the name and try again.
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ipconfig /renew

    IP Address.....: 192.168.3.3
    Subnet Mask....: 255.255.255.0
    Default Gateway.: 192.168.3.1
    DNS Server.....: 0.0.0.0

C:\>arp -a
No ARP Entries Found
C:\>

```

- Cambie a modo de **simulación**.
- Haga ping a **Sales 1** de Sales 2.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.2
Ping request could not find host 192.168.2. Please check the name and try again.
C:>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:>ipconfig /renew

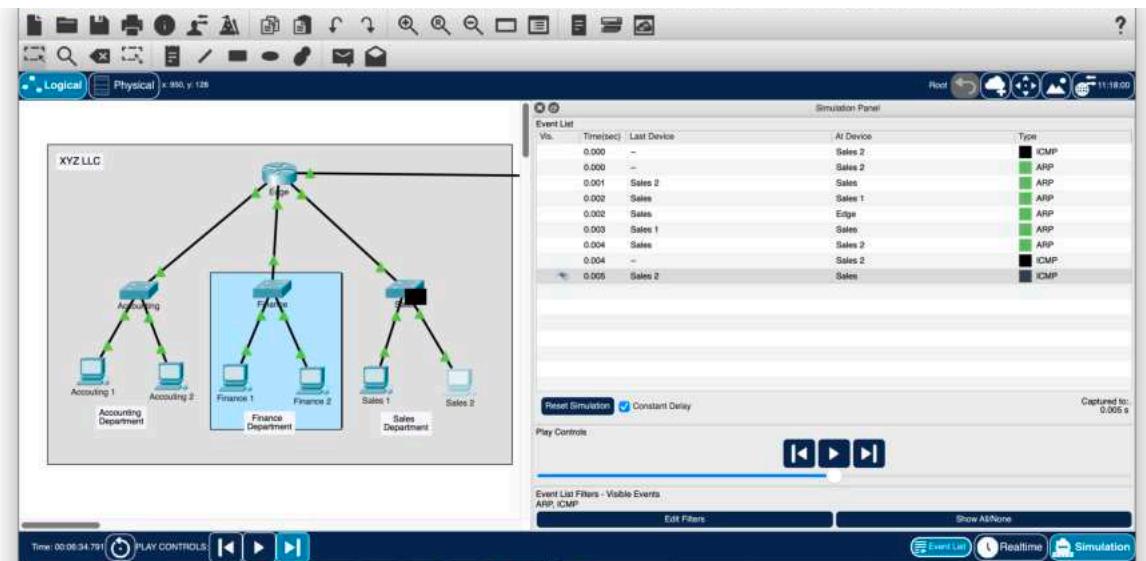
IP Address.....: 192.168.3.3
Subnet Mask.....: 255.255.255.0
Default Gateway...: 192.168.3.1
DNS Server.....: 0.0.0.0

C:>arp -a
No ARP Entries Found
C:>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

```

- d. Utilice el botón **Capture then Forward** para pasar las PDU por la red. Observe cómo el mensaje de solicitud ARP fluye a través de la red esta vez.



### ¿Qué dispositivos reciben las transmisiones ARP esta vez?

En esta ocasión solo Sales 1 y el Router reciben las transmisiones ARP.

**Solo las Sales 1 y la interfaz del router que está conectada a la red del departamento de ventas procesan la PDU.**

### Paso 2: Haga ping a otros hosts.

Repita esta demostración haciendo ping a otros hosts y al servidor de Internet. Observe el flujo de las PDU de solicitud de ARP.

Se ha quedado colgado.

**¿Cuál es el beneficio de utilizar múltiples redes IPv4, o subredes, dentro de una empresa?**

**Un beneficio importante de usar varias redes IP es la contención del tráfico dentro de partes relevantes de la red sin afectar innecesariamente el rendimiento en partes irrelevantes de la red.**

**Nota:** La topología de red que se usa en la actividad es solo para fines de demostración. Si bien es posible que una red empresarial real pueda utilizar un router de esta manera, existen topologías más óptimas que logran estos resultados. Aprenderá sobre otros enfoques de diseño en cursos de redes posteriores.

Component	Items/Total	Score
ip	3/4	3/4
Physical	2/2	2/2

Tal y como se comentó en el foro, este ejercicio no actualiza los resultados de renovación de IP cuando efectivamente se observa que se ha renovado exitosamente.

## Tarea 6: Crear una LAN (apartado 14.3.4 del curso)

### Packet Tracer: Crear una LAN

#### Tabla de direccionamiento

Dispositivo	Interfaz / puerto	Dirección IPv4	Máscara de subred
PC Admin	NIC	DHCP	N/D

Dispositivo	Interfaz / puerto	Dirección IPv4	Máscara de subred
PC de Administrador	NIC	DHCP	N/D
Impresora	NIC	192.168.1.100	255.255.255.0
www. Cisco.pt	NIC	209.165.200.225	No disponible

## Objetivos

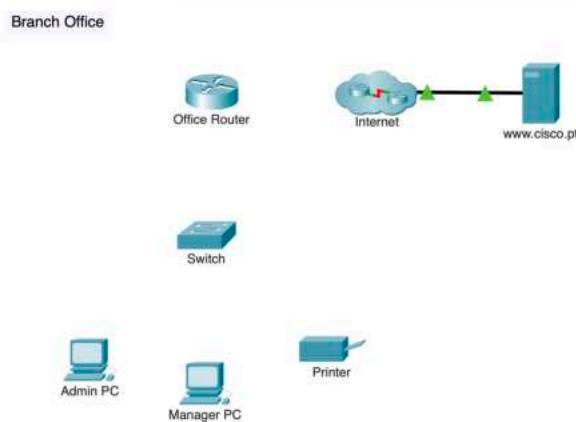
- Conectar dispositivos de red y hosts
- Configurar dispositivos con direccionamiento IPv4
- Verificar la configuración y la conectividad del dispositivo final
- Utilizar los comandos de red para ver la información del host

## Aspectos básicos/Situación

Se está abriendo una nueva sucursal y se le ha pedido que configure la LAN. Los dispositivos de red ya están configurados, pero debe conectarlos junto con los hosts. También debe configurar el direccionamiento IPv4 en los dispositivos finales y verificar que puedan alcanzar los recursos locales y remotos.

## Instrucciones

### Parte 1: Conectar dispositivos de red y hosts



### Paso 1: Encienda los dispositivos finales y el router de oficina.

- a. Haga clic en cada dispositivo y abra su pestaña Physical (Física). **Nota:** No hay ningún interruptor de alimentación en el modelo de switch utilizado en esta actividad.
- b. Localice el interruptor de alimentación para cada dispositivo en la ventana Vista de dispositivo físico.

- c. Haga clic en el interruptor de alimentación para encender el dispositivo. Debería ver una luz verde cerca del interruptor de alimentación para indicar que el dispositivo está encendido.



## Paso 2: Conectar los dispositivos finales.

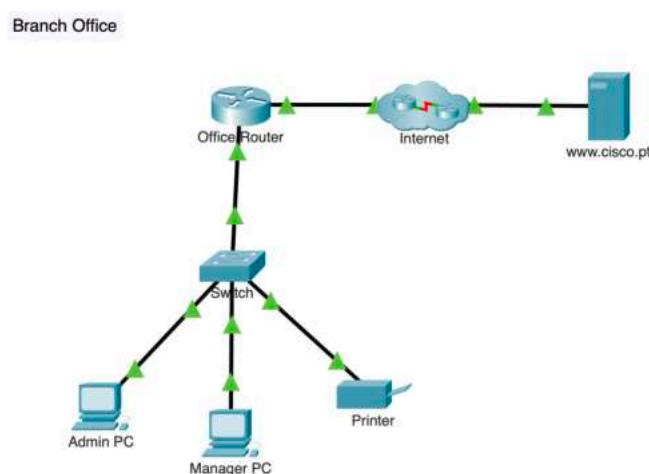
Utilice la tabla y las instrucciones para conectar los dispositivos de red y los hosts para crear la red física.

### Tabla de conexiones

Dispositivo	Interfaz / puerto	Conectado dispositivo	al	Interfaz de conexión / Puerto
Office Router (Enrutador de oficina)	G0/0	ISP1		G0/0
Office Router (Enrutador de oficina)	G0/1	Switch		G0/1
PC Admin	NIC (F / 0)	Switch		F0/1
PC de Administrador	NIC (F / 0)	Switch		F0/2
Impresora	NIC (F / 0)	Switch		F0/24

**Nota:** En la tabla anterior, las interfaces designadas con **G** son interfaces GigabitEthernet. Las interfaces que se designan con **F** son interfaces FastEthernet.

- Conecte los dispositivos de red según la información de la **tabla de conexiones** mediante cables directos de cobre Ethernet. Para la conexión de Internet a Office Router, seleccione el dispositivo y el puerto de los menús desplegables que aparecen cuando hace clic en la nube con la herramienta de conexiones seleccionada.
- Conecte las dos PC y la impresora al switch de oficina según la información de la tabla de conexiones. Utilice cables directos de cobre.
- Debería ver luces de enlace verdes en todas las conexiones después de un breve retraso.



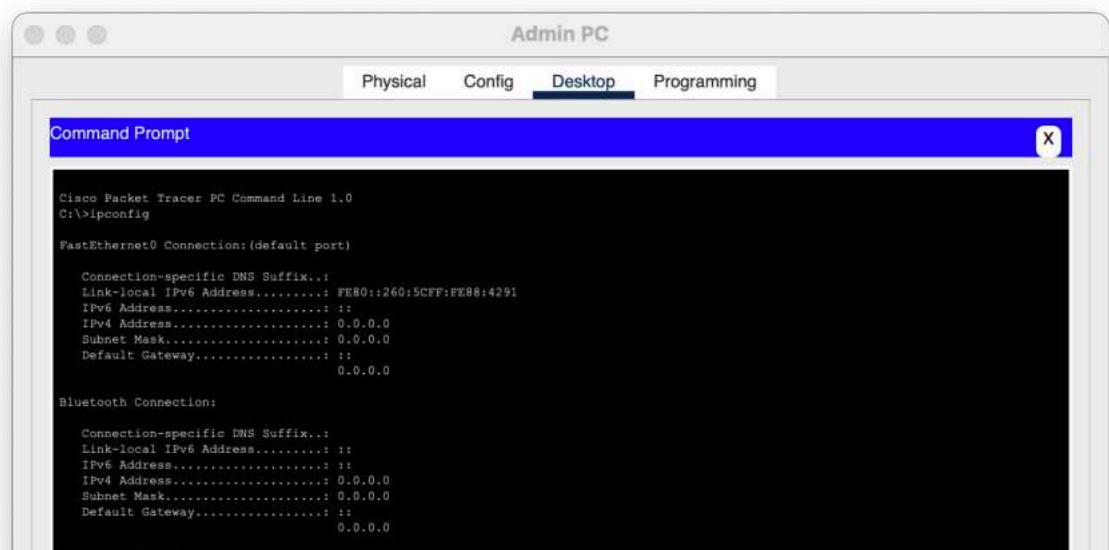
## Parte 2: Configurar dispositivos con direccionamiento IPv4

### Paso 1: Configure los hosts con información de direccionamiento.

- Las PC de Admin y Manager deben recibir la información de direccionamiento IP de DHCP. Office Router se ha configurado para proporcionar direcciones IP a los hosts en la LAN de la sucursal. Haga clic en las PC y vaya a las fichas de escritorio en cada PC. Abra la aplicación de configuración de IP y configure las PC para recibir sus direcciones IP dinámicamente.

- Admin PC:

Lo primero que vamos a hacer es comprobar el estado inicial del que partimos, para ello, el “command prompt” del desktop y hacemos un “ipconfig”.



The screenshot shows the Cisco Packet Tracer interface. At the top, there's a menu bar with "Physical", "Config", "Desktop" (which is highlighted in blue), and "Programming". Below the menu is a title bar for a window titled "Command Prompt". The main area of the window contains the output of the "ipconfig" command. The output shows two network connections: "FastEthernet0 Connection:(default port)" and "Bluetooth Connection:". For the FastEthernet0 connection, it lists the following information:  
Connection-specific DNS Suffix.:  
Link-local IPv6 Address.....: FE80::260:5CFF:FE88:4291  
IPv6 Address.....: ::  
IPv4 Address.....: 0.0.0.0  
Subnet Mask.....: 0.0.0.0  
Default Gateway.....: ::  
0.0.0.0  
For the Bluetooth connection, it lists:  
Connection-specific DNS Suffix.:  
Link-local IPv6 Address.....: ::  
IPv6 Address.....: ::  
IPv4 Address.....: 0.0.0.0  
Subnet Mask.....: 0.0.0.0  
Default Gateway.....: ::  
0.0.0.0

Actualmente la Admin PC no tiene una dirección IPv4 asignada. Esto es lo esperado si aún no se ha configurado el DHCP o si la PC no ha solicitado una dirección IP. En el caso de que tuviera una IP asignada podríamos proceder con los comandos “ipconfig /release” y “ipconfig /renew” para obtener una dirección IP, donde:

- ipconfig /release
- Este comando libera la dirección IP actual de la PC.
- Esencialmente, la PC "olvida" su dirección IP actual y la pone a disposición para que otra máquina la pueda usar
- ipconfig /renew
- Este comando solicita una nueva dirección IP del servidor DHCP.
- La PC envía una solicitud al servidor DHCP (en este caso, el router configurado como servidor DHCP) para obtener una nueva dirección IP.

En este caso, al no tener una IP asignada podemos proceder a renovar la IP directamente y posteriormente verificamos los cambios con “ipconfig”.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: FE80::260:5CFF:FE88:4291
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: ::1
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

C:\>ipconfig /renew

IP Address.....:: 192.168.1.2
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: 192.168.1.1
DNS Server.....:: 209.165.200.225

C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: FE80::260:5CFF:FE88:4291
IPv6 Address.....:: ::1
IPv4 Address.....:: 192.168.1.2
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: ::1
192.168.1.1

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: ::1
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

C:\>

```

Top

- Manager PC: repetimos los pasos para este PC.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: FE80::20A:41FF:FE36:3912
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: ::1
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

C:\>ipconfig /renew

IP Address.....:: 192.168.1.3
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: 192.168.1.1
DNS Server.....:: 209.165.200.225

C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: FE80::20A:41FF:FE36:3912
IPv6 Address.....:: ::1
IPv4 Address.....:: 192.168.1.3
Subnet Mask.....:: 255.255.255.0
Default Gateway.....:: ::1
192.168.1.1

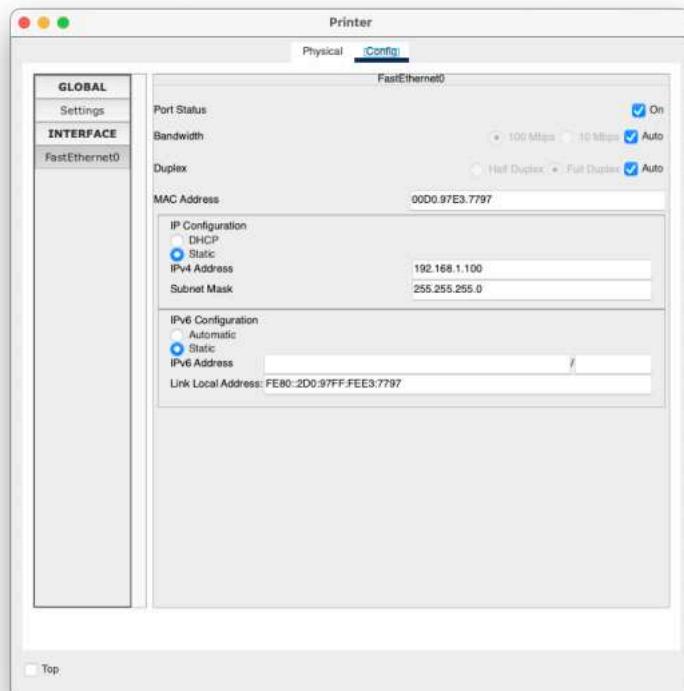
Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....:: ::1
IPv6 Address.....:: ::1
IPv4 Address.....:: 0.0.0.0
Subnet Mask.....:: 0.0.0.0
Default Gateway.....:: ::1
0.0.0.0

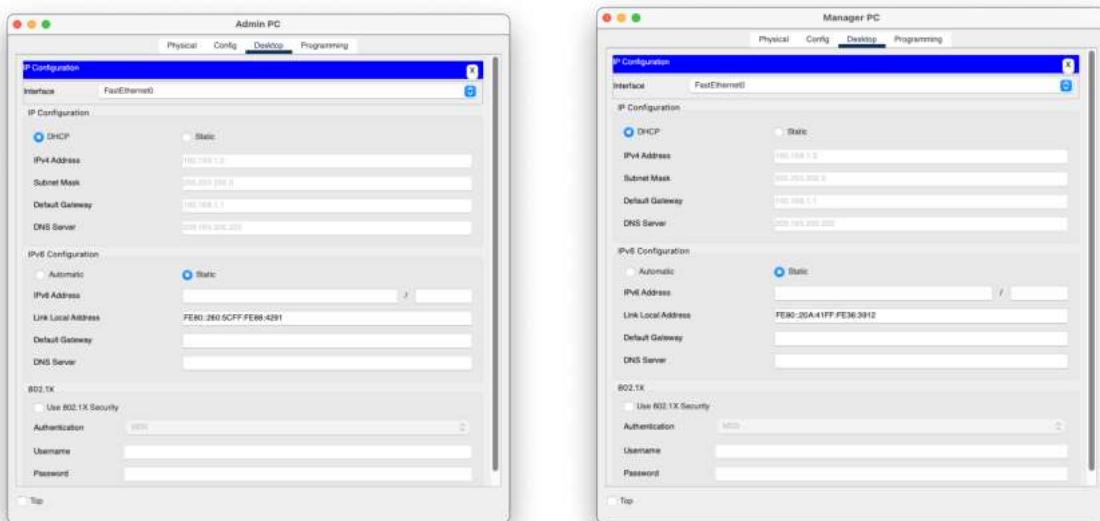
C:\>

```

- b. Las impresoras y los servidores a menudo se configuran manualmente con direccionamiento porque otros dispositivos en la red están configurados para acceder a ellos mediante direcciones IP. La configuración manual con una dirección estática garantizará que las direcciones IP de estos dispositivos no cambien.
- 1) Haga clic en la impresora y abra la pestaña Configuración.
  - 2) Haga clic en la interfaz FastEthernet0 en el panel izquierdo.
  - 3) Ingrese la información de direccionamiento de la tabla de direccionamiento.



- c. Dado que las dos computadoras se encuentran en la misma red, las direcciones IPv4 serán similares, las máscaras de subred y las puertas de enlace predeterminadas serán idénticas también.



**¿Por qué cree que las direcciones IPv4 son diferentes, pero las máscaras de subred y los gateways predeterminados son los mismos?**

Las direcciones IPv4, las máscaras de subred y las puertas de enlace predeterminadas juegan roles distintos pero complementarios en la configuración de una red.

## Direcciones IPv4 Diferentes

### 1. Identificación Única de Dispositivos:

- Cada dispositivo en una red debe tener una dirección IPv4 única para que pueda ser identificado de manera individual. Esto evita conflictos de direcciones IP y permite que cada dispositivo pueda ser encontrado y comunicado dentro de la red.

### 2. Asignación por DHCP:

- En esta red, las PC están configuradas para recibir sus direcciones IP de manera dinámica a través de DHCP. El servidor DHCP (en este caso, el router) asigna direcciones IP únicas a cada dispositivo dentro de un rango específico. Esto garantiza que no haya dos dispositivos con la misma dirección IP.

## Máscaras de Subred y Gateways Predeterminados Iguales

### 1. Máscara de Subred:

- La máscara de subred determina qué parte de la dirección IP identifica la red y qué parte identifica al host dentro de esa red.
- En una red local, todos los dispositivos deben tener la misma máscara de subred para que puedan comunicarse entre sí. Por ejemplo, una máscara de subred de 255.255.255.0 indica que los primeros tres octetos de la dirección IP son la parte de la red, y el último octeto identifica al dispositivo.

### 2. Puerta de Enlace Predeterminada (Default Gateway):

- La puerta de enlace predeterminada es la dirección IP del router que conecta la red local con otras redes, incluidas las redes externas como Internet.
- Todos los dispositivos en la red local utilizan la misma puerta de enlace predeterminada para enviar tráfico fuera de su red local. Esto es porque todas las comunicaciones que necesitan salir de la red local pasan a través del router.
- **Direcciones IPv4 Diferentes:** Cada dispositivo necesita una dirección IP única para evitar conflictos y permitir una comunicación adecuada dentro de la red.
- **Máscaras de Subred y Gateways Predeterminados Iguales:** Todos los dispositivos en la misma red comparten la misma máscara de subred para facilitar la comunicación interna y la misma puerta de enlace predeterminada para el tráfico externo.

Teniendo la siguiente configuración en la red:

- **PC Admin:**

- Dirección IP: 192.168.1.2 (asignada por DHCP)
- Máscara de Subred: 255.255.255.0
- Puerta de Enlace Predeterminada: 192.168.1.1

- **PC Manager:**
  - Dirección IP: 192.168.1.3 (asignada por DHCP)
  - Máscara de Subred: 255.255.255.0
  - Puerta de Enlace Predeterminada: 192.168.1.1
- **Impresora:**
  - Dirección IP: 192.168.1.100 (estática)
  - Máscara de Subred: 255.255.255.0
  - Puerta de Enlace Predeterminada: 192.168.1.1

En este caso, aunque las direcciones IP son diferentes, la máscara de subred y la puerta de enlace predeterminada son las mismas, permitiendo que todos los dispositivos se comuniquen correctamente dentro de la misma red y con otras redes a través del router.

### **Máscara de Subred**

Una máscara de subred es una herramienta utilizada en redes para dividir una dirección IP en dos partes: la parte de la red y la parte del host (o dispositivo). La máscara de subred se representa en formato de dirección IP y determina qué porción de la dirección IP total es para la red y qué porción es para los dispositivos dentro de esa red.

- **Máscara de Subred:** Determina cuántos bits de la dirección IP son para la parte de la red y cuántos son para la parte del host.
- **255.255.255.0:** Indica que los primeros 24 bits (tres octetos) son la parte de la red y el último octeto (8 bits) es para identificar dispositivos únicos dentro de esa red.

### **Ejemplos de Máscaras de Subred**

- *Máscara de Subred: 255.255.255.0*

#### **En binario:**

255	-> 11111111
255	-> 11111111
255	-> 11111111
0	-> 00000000

#### **Máscara de subred completa en binario:**

11111111.11111111.11111111.00000000

#### **Número de bits de red: 24 bits**

#### **Número de bits de host: 8 bits**

Esto permite 256 direcciones posibles ( $2^8$ ), con 254 direcciones de host utilizables (restando las direcciones de red y de broadcast).

- *Máscara de Subred: 255.255.255.128*

**En binario:**

255 -> 11111111  
255 -> 11111111  
255 -> 11111111  
128 -> 10000000

**Máscara de subred completa en binario:**

11111111.11111111.11111111.10000000

**Número de bits de red: 25 bits**

**Número de bits de host: 7 bits**

Esto permite 128 direcciones posibles ( $2^7$ ), con 126 direcciones de host utilizables (restando las direcciones de red y de broadcast).

- *Máscara de Subred: 255.255.255.192*

**En binario:**

255 -> 11111111  
255 -> 11111111  
255 -> 11111111  
192 -> 11000000

**Máscara de subred completa en binario:**

11111111.11111111.11111111.11000000

**Número de bits de red: 26 bits**

**Número de bits de host: 6 bits**

Esto permite 64 direcciones posibles ( $2^6$ ), con 62 direcciones de host utilizables.

- *Máscara de Subred: 255.255.255.224*

**En binario:**

255 -> 11111111  
255 -> 11111111  
255 -> 11111111  
224 -> 11100000

### Máscara de subred completa en binario:

11111111.11111111.11111111.11100000

### Número de bits de red: 27 bits

### Número de bits de host: 5 bits

Esto permite 32 direcciones posibles ( $2^5$ ), con 30 direcciones de host utilizables.

### CIDR Notation (Notación CIDR)

Además de la notación decimal separada por puntos, las máscaras de subred también se pueden representar en notación CIDR (Classless Inter-Domain Routing). En esta notación, se especifica la cantidad de bits utilizados para la parte de la red.

Por ejemplo:

- 255.255.255.0 se representa como /24.
- 255.255.255.128 se representa como /25.
- 255.255.255.192 se representa como /26.
- 255.255.255.224 se representa como /27.

Por tanto, podemos resumir toda esta información de la siguiente manera.

1. **Máscara de subred 255.255.255.0:**
  - **Binario:** 11111111.11111111.11111111.00000000
  - **CIDR:** /24
  - **Hosts:** 254 utilizables
2. **Máscara de subred 255.255.255.128:**
  - **Binario:** 11111111.11111111.11111111.10000000
  - **CIDR:** /25
  - **Hosts:** 126 utilizables
3. **Máscara de subred 255.255.255.192:**
  - **Binario:** 11111111.11111111.11111111.11000000
  - **CIDR:** /26
  - **Hosts:** 62 utilizables
4. **Máscara de subred 255.255.255.224:**
  - **Binario:** 11111111.11111111.11111111.11100000
  - **CIDR:** /27

- **Hosts:** 30 utilizables

### **Por qué Usar Máscaras Intermedias**

El uso de diferentes valores de máscara de subred permite a los administradores de red crear subredes de diferentes tamaños para optimizar el uso de direcciones IP y mejorar la eficiencia de la red. En redes grandes, esto es crucial para manejar adecuadamente la asignación de direcciones IP y reducir el desperdicio de espacio de direcciones.

**Las respuestas pueden variar. Cada dispositivo de la red debe tener un identificador exclusivo. La dirección IPv4 constituye un modo de identificar de manera exclusiva cada dispositivo o host de red. La puerta de enlace predeterminada representa la forma de comunicarse con los dispositivos que NO están en la red local.**

La impresora no requiere una puerta de enlace predeterminada porque solo los hosts podrán acceder a ella en la red local. Sin embargo, si necesita configurarlo con una puerta de enlace predeterminada, **¿qué valor utilizará la impresora? ¿Cómo puede determinar esto a partir de los otros dispositivos en la red?**

En una red local, todos los dispositivos, incluidas las impresoras, generalmente usan la misma puerta de enlace predeterminada para enrutar el tráfico fuera de la red local. La puerta de enlace predeterminada es la dirección IP del router o dispositivo que conecta la red local a otras redes, incluidas las redes externas como Internet.

Para determinar la puerta de enlace predeterminada que debe configurarse en la impresora, usaremos la misma de otros dispositivos en la misma red, como las PC de Admin y Manager. Dado que todas las máquinas en una red local generalmente usan la misma puerta de enlace predeterminada, revisamos las capturas anteriores en las que se detalla esta información y comprobamos que la dirección sería esta: 192.168.1.1.

**Puede determinar el valor de la puerta de enlace predeterminada que se utilizará observando los valores con los que DHCP ha configurado las PC o determinando la dirección IP de la interfaz Ethernet del enrutador de oficina que está conectada a la LAN de la sucursal.**

### **Parte 3: Verificar la configuración y la conectividad del dispositivo final**

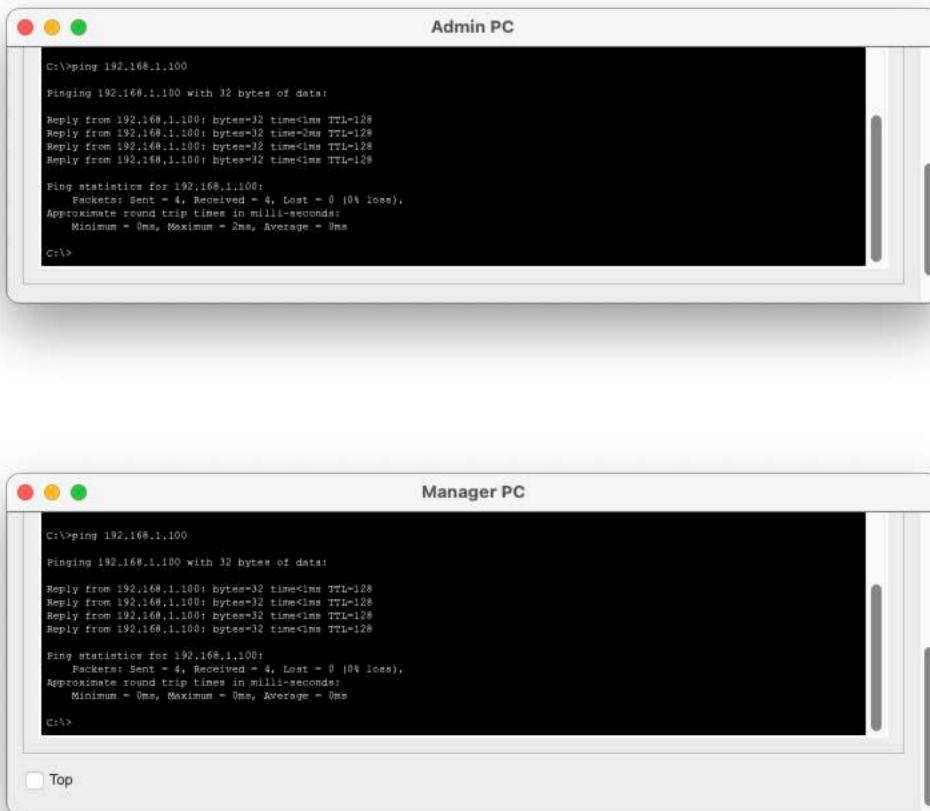
#### **Paso 1: Verificar la conectividad entre las dos PC.**

- a. Vaya a los escritorios de las PC y compruebe la configuración de direccionamiento IP. Debería ver que las PC han recibido dinámicamente direcciones IP en la red 192.168.1.0 255.255.255.0. También debería ver que han recibido direcciones para la configuración de la puerta de enlace predeterminada y del servidor DNS.

En las capturas anteriores se podía verificar que efectivamente esto es así ya se han asignado como efectivamente se indica.

- b. Desde el símbolo del sistema en Admin PC, haga ping a la dirección IP de la impresora. Repita este proceso para Manager PC. Debería ver pings exitosos para cada uno. Esto

verifica que las PC y la impresora estén encendidas, conectadas y direccionadas correctamente.



```
C:\>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>

C:\>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

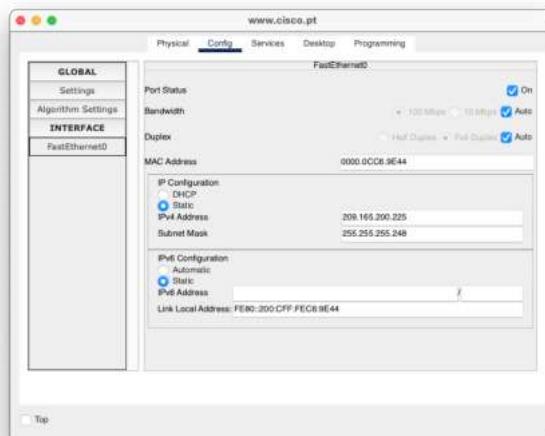
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

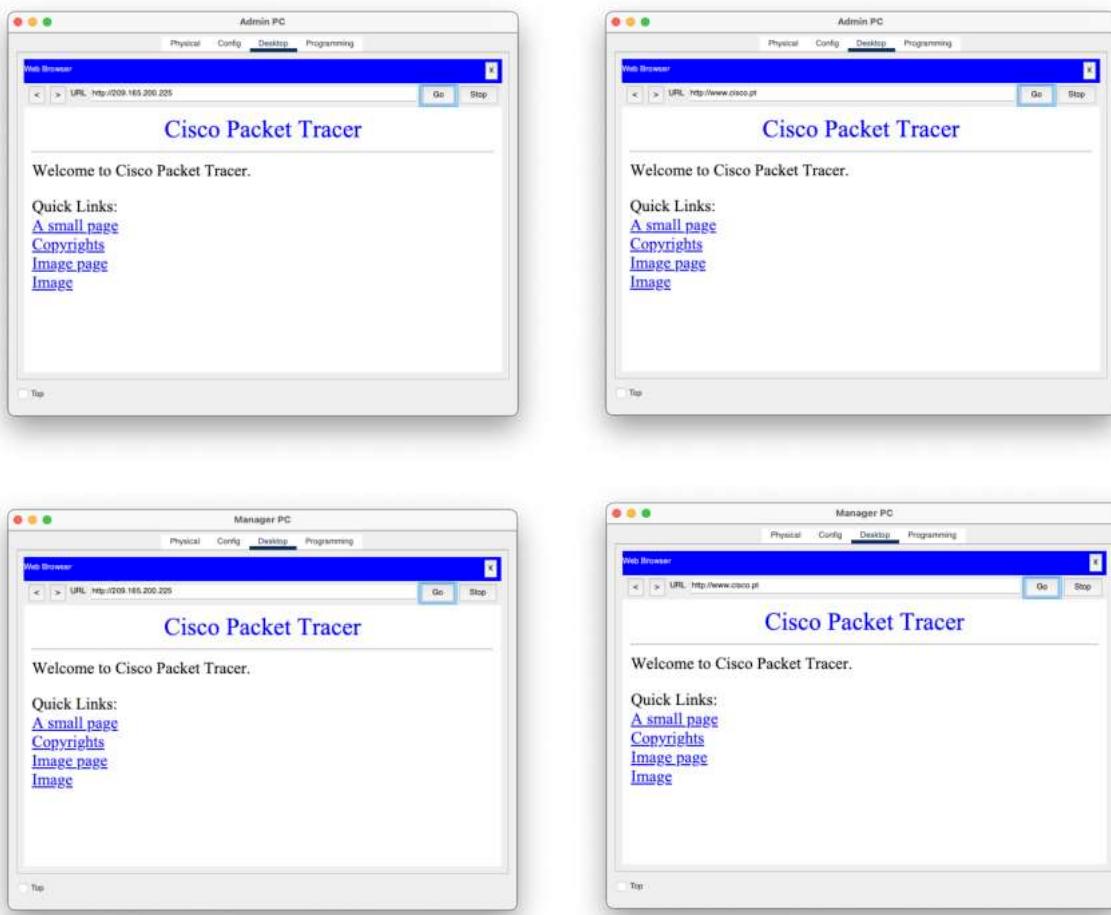
C:\>
```

Efectivamente, comprobamos que los ping son exitosos en cada uno de ellos.

## Paso 2: Verificar la conectividad hacia internet.

Desde el escritorio de las PC, abra el navegador web. Ingrese la dirección IP del servidor de Internet para mostrar la página web. Repita el proceso pero conéctese con la URL del servidor.





Comprobamos que podemos conectarnos exitosamente tanto por dirección IP como por URL, esto significa que no hay problemas de conexión y que la configuración de red está funcionando correctamente. El servidor DNS está resolviendo los nombres de dominio correctamente y los dispositivos están configurados adecuadamente.

**Si puede conectarse por la dirección IP, pero no por la URL, ¿cuál cree que es la causa de este problema?**

Si puedes conectarte por dirección IP pero no por URL, la causa más probable es un problema con la resolución DNS.

Algunas razones por las que se podría haber tenido problemas si la configuración no fuera correcta:

- **Problemas de Configuración DNS:** Si los servidores DNS no están configurados correctamente, no se podrá resolver la URL a una dirección IP.
- **Caché DNS Corrupta:** Entradas corruptas en la caché DNS pueden causar problemas de resolución de nombres.
- **Entradas Incorrectas en el Archivo de Hosts:** Entradas incorrectas en el archivo de hosts pueden redirigir URLs a direcciones IP equivocadas.
- **Problemas de Red o Firewall:** Configuraciones de red o firewall que bloqueen el tráfico DNS pueden impedir la resolución de nombres de dominio.

**Dado que el DNS se utiliza para resolver las URL en direcciones IP, puede adivinar con seguridad que no se puede acceder al servidor DNS. Esto puede deberse a un problema de conectividad de red o a que falta o es incorrecta la dirección del servidor DNS configurada en los hosts.**

## 1. Parte 4: Utilizar los comandos de red para ver la información del host

Los comandos de red disponibles desde el símbolo del sistema en las PC son muy similares a los disponibles en Windows. En esta parte de la actividad, utilizará **ipconfig** y **tracert** para obtener más información sobre la LAN.

### Paso 1: Use comando ipconfig.

El comando **ipconfig** muestra detalles sobre el direccionamiento configurado en un host.

Abra un símbolo del sistema en una de las PC, ingrese el comando **ipconfig** y tome nota de la información que se devuelve. Ahora ingrese el comando **ipconfig /all**. ¿Qué información adicional se muestra?

```
C:\>ipconfig
FastEthernet0 Connection:(default pmtu)
  Connection-specific DNS Suffix: .
  Link-local IPv6 Address . . . . . : FE80::E70A:41FF%FE36:3912
  IPv4 Address . . . . . : 192.168.1.3
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
Bluetooth Connection:
  Connection-specific DNS Suffix: .
  Link-local IPv6 Address . . . . . : FE80::210A:41FF%PM36:3912
  IPv4 Address . . . . . : 192.168.1.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
C:\>ipconfig /all
FastEthernet0 Connection:(default pmtu)
  Connection-specific DNS Suffix: .
  Physical Address . . . . . : 00B4:4138:3912
  Link-local IPv6 Address . . . . . : FE80::20B4:41FF%FE36:3912
  IPv4 Address . . . . . : 192.168.1.3
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
  DHCP Servers . . . . . : 192.168.1.1
  DHCPv4 TAID . . . . . : 00-01-00-01-25-3a-3a-31-00-0a-41-3d-39-12
  DNS Servers . . . . . : 192.168.200.225
Bluetooth Connection:
  Connection-specific DNS Suffix: .
  Physical Address . . . . . : 00B0:0927:6E77
  Link-local IPv6 Address . . . . . : FE80::20B0:0927%PM36:6E77
  IPv4 Address . . . . . : 192.168.1.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.0
  DHCP Servers . . . . . : 192.168.1.0
  DHCPv4 TAID . . . . . : 00-01-00-01-25-3a-3a-31-00-0a-41-3d-39-12
  DNS Servers . . . . . : 192.168.200.225
```

La información adicional que obtenemos, tanto en FastEthernet0 Connection como Bluetooth Connection:

- Physical Address
- DHCP Servers

- DHCPv6 IAID (Identity Association Identifier): Un identificador utilizado para distinguir entre diferentes direcciones IPv6 asignadas al mismo cliente.
- DHCPv6 Client DUID (DHCP Unique Identifier): Un identificador único para clientes DHCPv6.
- DNS Servers

El término IAID (Identity Association Identifier) es parte del protocolo DHCPv6 y se utiliza para identificar de manera única una dirección IP asignada a una interfaz específica en un cliente DHCPv6.

#### **IAID (Identity Association Identifier):**

- Es un identificador de 32 bits que se utiliza en DHCPv6 para identificar de manera única una “asociación de identidad” (Identity Association) entre un cliente DHCPv6 y una dirección IPv6 específica.
- Cada interfaz de red en un dispositivo tiene su propio IAID único, lo que permite que un cliente DHCPv6 distinga entre diferentes direcciones IPv6 que puede tener asignadas.

#### **Uso del IAID**

El IAID se combina con el DUID (DHCP Unique Identifier) para formar un identificador único que DHCPv6 utiliza para gestionar las direcciones y otras configuraciones asignadas a los clientes.

**Ipconfig /all muestra información sobre la dirección física (MAC) de la NIC. También muestra las direcciones de los servidores DHCP y DNS. En Windows, se muestran muchos detalles adicionales. Escriba ipconfig /all en el símbolo del sistema de una PC para ver toda la información que Windows muestra con este comando.**

#### **Paso 2: Utilizar el comando tracert.**

El comando **tracert** utiliza ICMP para devolver información sobre los routers que se pasan a medida que los paquetes pasan de la PC de origen al destino.

Rastree hasta un destino remoto yendo a una de las PC e ingresando **tracert** seguido de la URL del servidor web.

```

C:\>
C:\>
C:\>
C:\>tracert www.cisco.com
Tracing route to 209.165.200.225 over a maximum of 30 hops:
 1  0 ms      0 ms      0 ms    192.168.1.1
 2  0 ms      0 ms      0 ms    209.165.200.233
 3  0 ms      0 ms      0 ms    209.165.200.225
Trace complete.

C:\>

```

Top

**¿Cuántos enruteadores se pasan en el camino hacia el destino? ¿Cómo se identifican esos routers?**

- **Número de Enruteadores Pasados:**
  - El destino final (209.165.200.225) no se cuenta como un enruteador intermedio; por lo tanto, solo se cuentan los enruteadores pasados.
  - El número de enruteadores pasados es **2**.
- **Identificación de los Enruteadores:**
  - Los enruteadores se identifican mediante las direcciones IP de las interfaces entrantes en los routers.
  - Primer enruteador: 192.168.1.1
  - Segundo enruteador: 209.165.200.233

Por tanto, podemos concluir,

- **Número de enruteadores pasados: 2**
- **Identificación de los enruteadores:**
  - Primer enruteador: 192.168.1.1
  - Segundo enruteador: 209.165.200.233

**Dos. Se identifican mediante las direcciones IP de las interfaces entrantes en los routers.**

**¿Dónde se encuentra el segundo router?**

**Primer Salto:** 192.168.1.1

- Este es típicamente el router de la red local, probablemente el gateway de tu red local.

**Segundo Salto:** 209.165.200.233

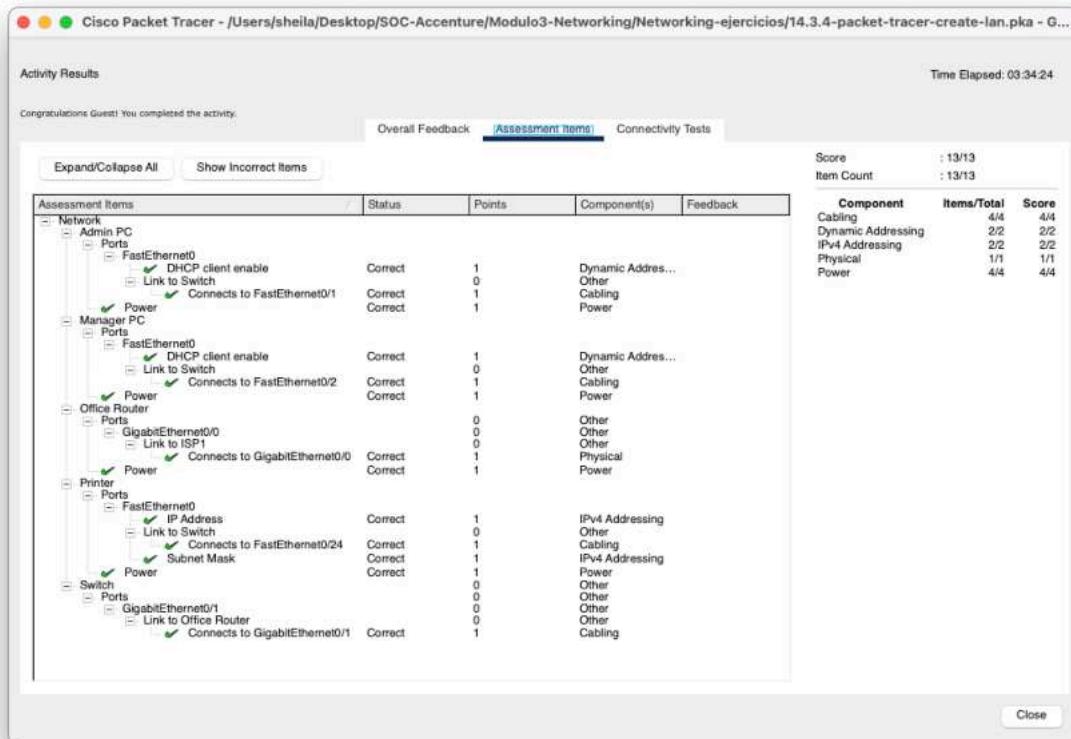
- Este es el segundo router, que puede estar en la red del ISP (Proveedor de Servicios de Internet) o en una red intermedia. No está directamente bajo nuestro control ni en la red local, sino en la red del ISP o en otra parte de la infraestructura de internet.

**Está en la nube de internet.**

## Reflexión

Considere una oficina pequeña que tenga una LAN similar a la que ha creado aquí. **¿Cuál es el mayor desafío de las instalaciones para configurar la red en una nueva ubicación?**

**La infraestructura de cableado físico.** La oficina debe estar cableada y tener salidas de comunicación para todos los dispositivos. Además, las salidas deben estar en ubicaciones convenientes. Además, las salidas deben conectarse a una ubicación central donde se encuentren el switch y el router. El cableado físico puede presentar muchos problemas al crear una nueva ubicación de oficina.



## Tarea 7: La Interacción del Cliente (apartado 16.1.5. del curso)

### Packet Tracer: La interacción con los clientes

#### Objetivos

Observar la interacción de los clientes entre el servidor y la PC.

#### Aspectos básicos/situación

Los clientes, como las PC de escritorio, solicitan servicios a los servidores. El entorno de laboratorio, que usa PC y servidores físicos, admite una gama completa de servicios. En un ambiente simulado, la cantidad de servicios es limitada. Packet Tracer permite agregar

servidores de red simulados que soportan DHCP, DNS, HTTP y TFTP. Packet Tracer también soporta la adición de PC simuladas que pueden solicitar dichos servicios. Esta actividad usa una red simple que consiste en una PC conectada directamente a un servidor configurado para prestar servicios de DNS, además de alojar una página web mediante un servidor HTTP. Esta actividad rastreará el flujo de tráfico que se produce cuando se solicita una página web, cómo se resuelve la dirección IP de la página web y cómo se entrega esta.

Antes de empezar con el ejercicio, vamos a recordar brevemente que significan cada uno de estos conceptos:

- **DHCP (Dynamic Host Configuration Protocol):** Es un protocolo de red que asigna automáticamente direcciones IP y otros parámetros de configuración a los dispositivos en una red. Esto facilita la conexión de nuevos dispositivos sin necesidad de configurarlos manualmente.
- **DNS (Domain Name System):** Es un sistema que traduce nombres de dominio fáciles de recordar (como [www.example.com](http://www.example.com)) en direcciones IP numéricas (como 192.0.2.1) que son utilizadas por los dispositivos para identificar y comunicarse entre sí en la red.
- **HTTP (Hypertext Transfer Protocol):** Es un protocolo utilizado para la transferencia de páginas web en la World Wide Web. Permite la comunicación entre un navegador web (cliente) y un servidor web para solicitar y entregar contenido como texto, imágenes, y otros recursos multimedia.
- **TFTP (Trivial File Transfer Protocol):** Es un protocolo de transferencia de archivos sencillo y menos robusto que FTP. Se utiliza principalmente para transferir pequeños archivos de configuración o bootstrapping entre dispositivos en una red. No proporciona autenticación ni encriptación.

## InSTRUCCIONES

### Parte 1: Ingrese al modo de simulación.

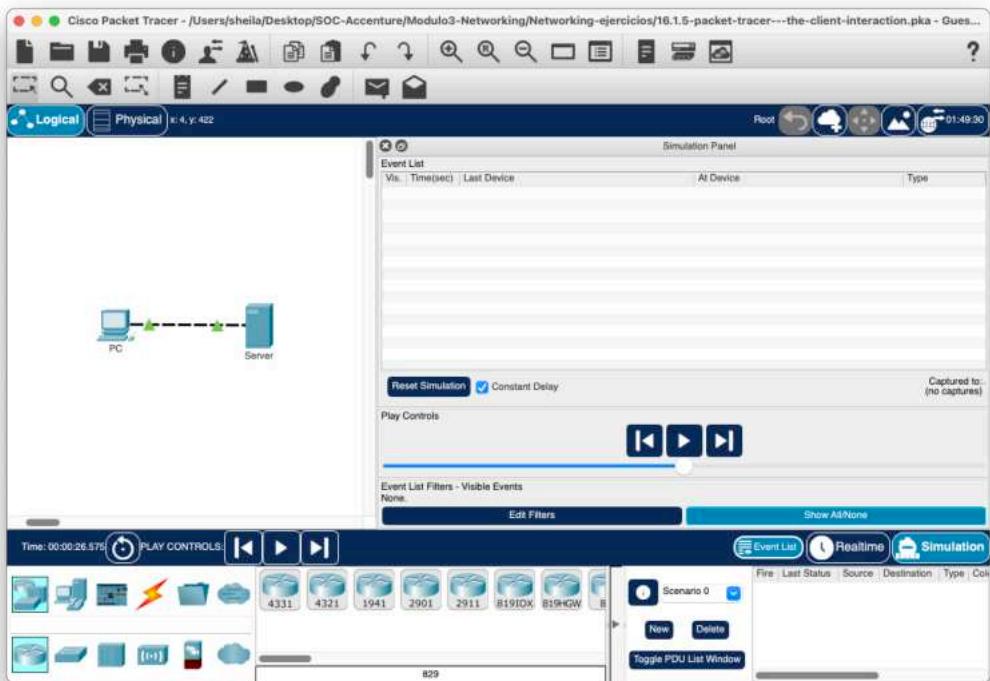
Cuando se inicia el Packet Tracer, éste presenta una vista lógica de la red en el modo de tiempo real.

Haga clic en **Simulation Mode** para ingresar al modo de simulación. El icono del modo de simulación se encuentra en la parte inferior derecha del área de trabajo lógico.

### Parte 2: Establezca filtros para la lista de eventos.

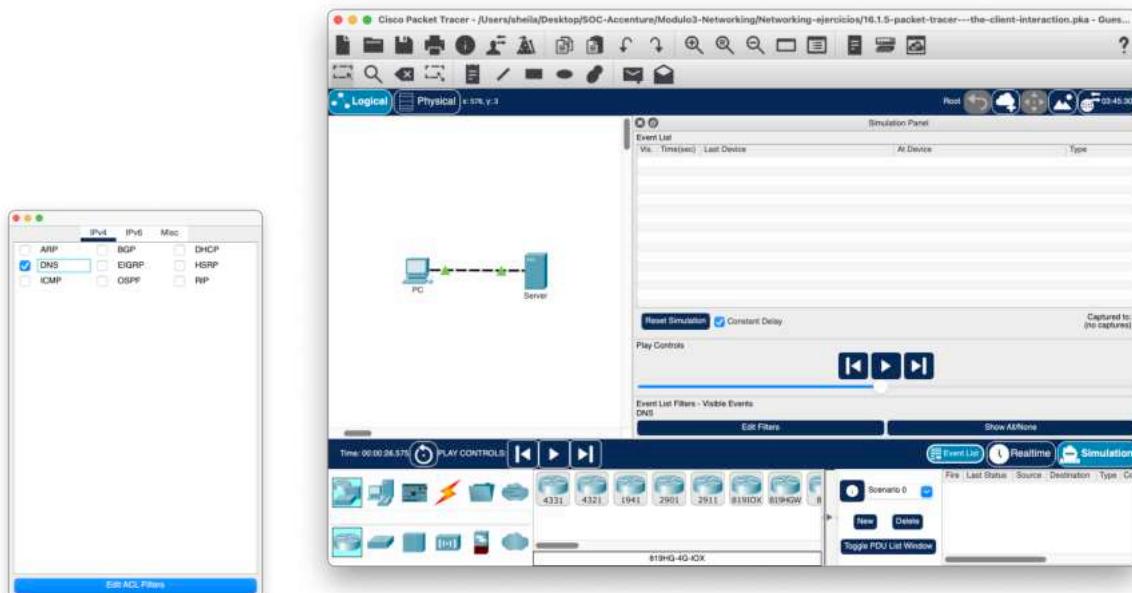
En el modo de simulación, la opción predeterminada es capturar todos los eventos. Usará filtros para capturar solamente eventos DNS y HTTP.

- a. En la sección **Event List Filters** (Filtros de la lista de eventos), haga clic en **Show All/None** (Mostrar todos/ninguno) para borrar todas las marcas.



Observamos que se han borrado.

- Haga clic en **Edit Filters** (Editar filtros). En la ficha IPv4, seleccione **DNS**. En la ficha Misc, seleccione **HTTP**. Cierre la ventana cuando haya terminado. **Event List Filters** muestra DNS y HTTP como los únicos eventos visibles.

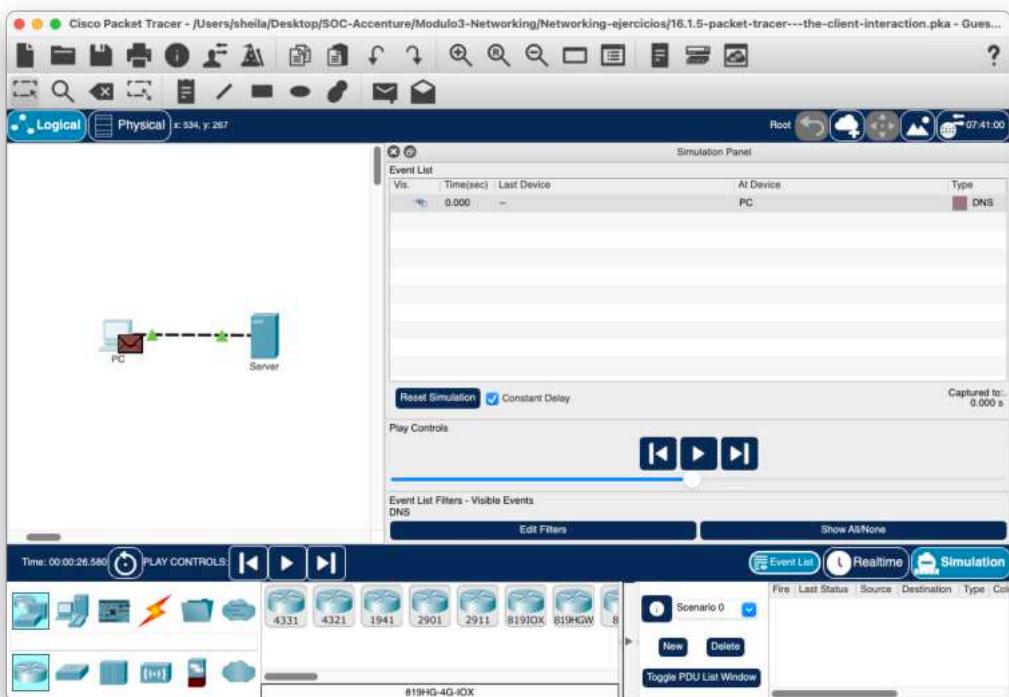
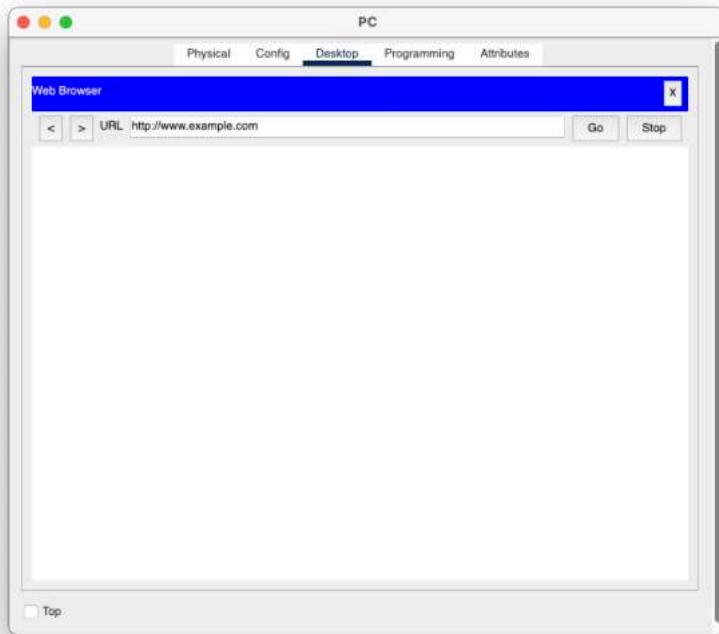


Ahora aparece en los Event List Filters: DNS.

### Parte 3: Solicite una página web desde la PC.

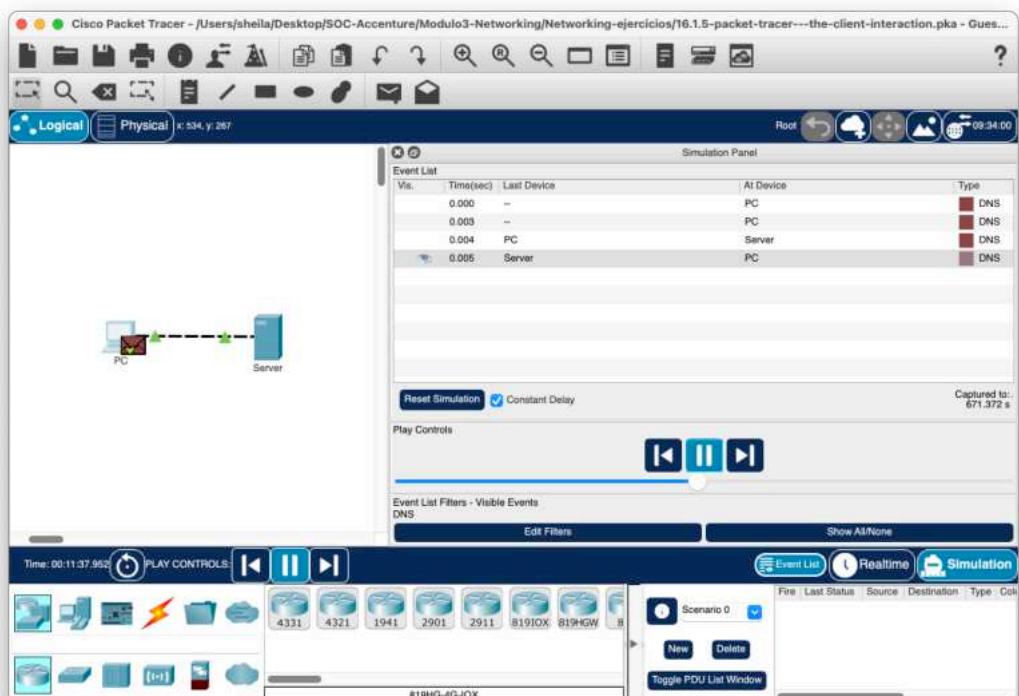
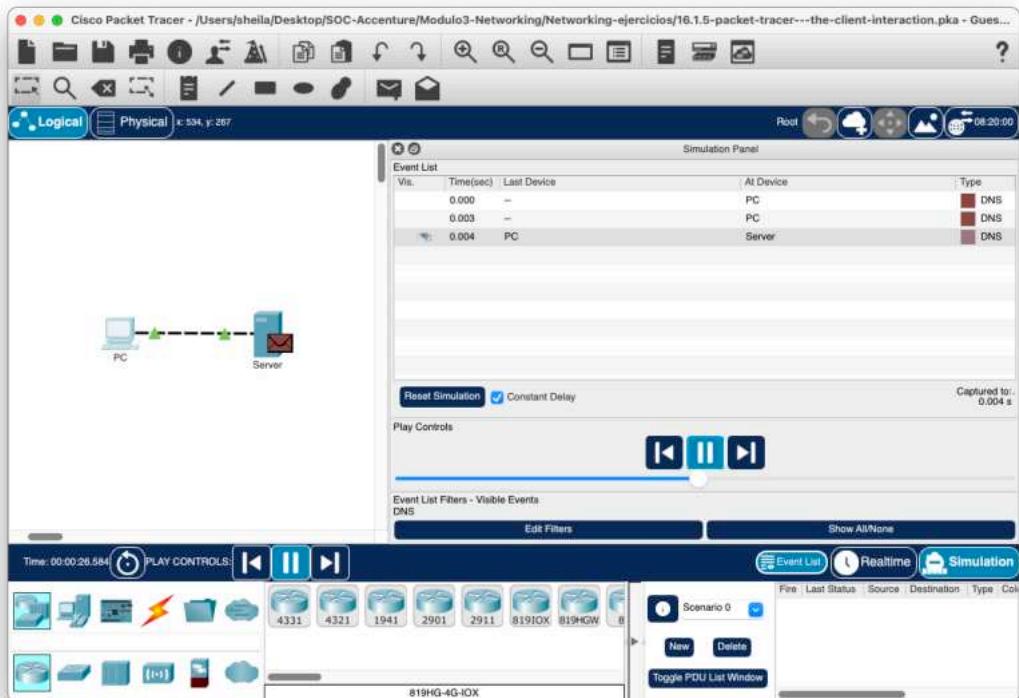
Abrirá un navegador web simulado en la PC y solicitará una página web al servidor.

- a. Haga clic en **PC**. Haga clic en la ficha **Desktop** (Escritorio) y en **Web Browser** (Navegador web).
- b. Se abrirá un navegador web simulado. Escriba **www.ejemplo.com** en el cuadro de la URL y haga clic en el botón **Go** (Ir) a la derecha. Minimice la ventana de la PC.



## Parte 4: Ejecute la simulación.

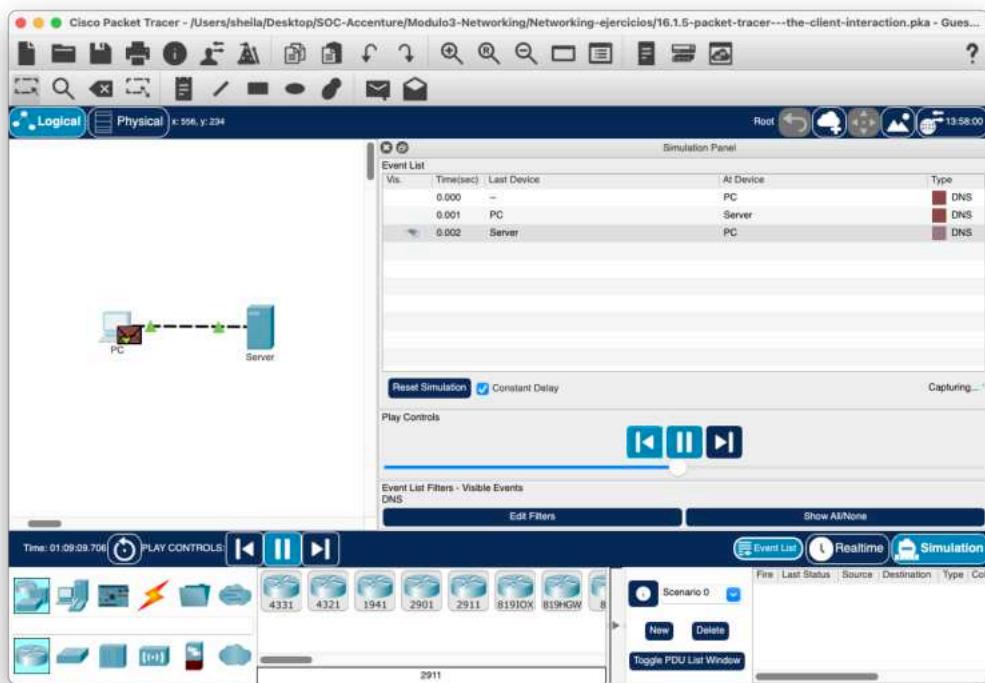
- En la sección **Play Controls** (Controles de reproducción) del **Simulation Panel** (Panel de simulación), haga clic en **Play** (Reproducir). Se anima el intercambio entre la PC y el servidor, y se agregan eventos a **Event List** (Lista de eventos).



Estos eventos representan la solicitud de la PC de resolver la URL en una dirección IP, el suministro del servidor de la dirección IP, la solicitud de la página web por parte de la PC, el envío de la página web por parte del servidor en dos segmentos y la confirmación de la PC de que recibió la página web.

- b. Haga clic en **View Previous Event** (Ver evento anterior) para continuar cuando el búfer esté lleno.

Seleccionamos el paso previo y vuelve a continuar.



#### Parte 5: Acceda a una PDU específica.

- a. Restaure la ventana de la PC simulada. Observe que se muestra una página web en el navegador web. Minimice la ventana de navegador simulado.



Efectivamente, ahora si podemos ver la web.

- b. En la sección **Simulation Panel Event List** (Lista de eventos del panel de simulación), la última columna contiene un cuadro coloreado que brinda acceso a información detallada sobre un evento. Haga clic en el cuadro coloreado en la primera fila del primer evento. Se abre la ventana **PDU Information** (Información de la PDU).

The screenshot displays two windows from Cisco Packet Tracer:

- PDU Information at Device: PC**: This window shows the configuration of the device (At Device: PC, Source: PC, Destination: 192.168.1.2) and a list of layers (In Layers and Out Layers). It also contains a note: "1. The DNS client sends an A DNS query to the DNS server." At the bottom are buttons for "Challenge Me", "<< Previous Layer", and "Next Layer >>".
- PDU Formats**: This window is titled "PDU Information at Device: PC" and "OSI Model: Outbound PDU Details". It displays the structure of an outbound PDU across multiple layers:
  - Ethernet II**: Shows fields like PREAMBLE (101010...), DEST ADDR (0001.97AB.0AEA), and FCS (0x00000000).
  - IP**: Shows fields like VER (4), IHL (5), DSCH (0x00), TTL (128), PRO (0x11), and CHKSUM.
  - UDP**: Shows fields like SOURCE PORT (1026), DESTINATION PORT (53), LENGTH (0x0027), and CHECKSUM.
  - DNS Header**: Shows fields like Transaction ID (0x610c), OPCODE (0x1), RD (1), Z (0), RCODE (0x0), QDCOUNT (1), ANCOUNT (0), NSCOUNT (0), and ARCOUNT (0).
  - DNS Query**: Shows fields like NAME (NAME (VARIABLE LENGTH): www.example.com), TYPE (1), CLASS (1), and TTL (86400).

Vamos a detallar las dos pestañas en cuestión y su relevancia para la tarea:

## PDU Information at Device: PC

### *OSI Model*

Esta pestaña detalla cómo se procesan los datos a través de las diferentes capas del modelo OSI.

1. **Layer 7: DNS**
  - Esta capa representa la capa de aplicación, y en este caso, el servicio DNS está involucrado.
2. **Layer 4: UDP**
  - Aquí se muestra el puerto de origen (1026) y el puerto de destino (53), que es el puerto estándar para DNS.
3. **Layer 3: IP**
  - Proporciona la dirección IP de origen (192.168.1.1) y la dirección IP de destino (192.168.1.2).
4. **Layer 2: Ethernet II**
  - Muestra las direcciones MAC de origen (00D0.FF57.B11A) y destino (0001.97AB.OAEA).
5. **Layer 1: Physical**
  - Esta capa describe los medios físicos utilizados para la transmisión de datos (cables, ondas de radio, etc.). Aunque los detalles específicos de la capa física no siempre se muestran en estas ventanas de información, es importante recordar que esta capa es responsable de la transmisión real de los bits a través del medio de red.

### *Outbound PDU Details*

Esta pestaña proporciona una vista detallada de los datos de la PDU saliente desde la perspectiva de cada capa.

#### **Proceso:**

1. **Ethernet II:**
  - La capa de enlace de datos incluye las direcciones MAC de origen y destino. El tipo de protocolo es IP (0x0800).
2. **IP:**
  - La capa de red incluye información sobre la versión del protocolo, longitud del encabezado, servicios diferenciados, longitud total del paquete, identificación, fragmentación, TTL, protocolo (UDP en este caso), checksum de encabezado, y las direcciones IP de origen y destino.
3. **UDP:**
  - La capa de transporte muestra los puertos de origen y destino, la longitud del datagrama UDP, y un checksum.

**4. DNS Header:**

- La capa de aplicación para DNS incluye el ID de transacción, el opcode para una consulta estándar, las flags que indican una consulta recursiva, y los conteos de registros de pregunta, respuesta, autoridad y adicionales.

**5. DNS Query:**

- Detalles específicos de la consulta DNS, incluyendo el nombre del dominio ([www.example.com](http://www.example.com)), el tipo de registro (A), la clase (IN), TTL, y la longitud.

**Flujo de Datos:**

- El PC envía una consulta DNS encapsulada en un paquete UDP que a su vez está encapsulado en un paquete IP, y finalmente en un frame Ethernet.
- La consulta DNS se dirige al servidor DNS en la dirección IP 192.168.1.2, solicitando la dirección IP correspondiente al dominio [www.example.com](http://www.example.com).

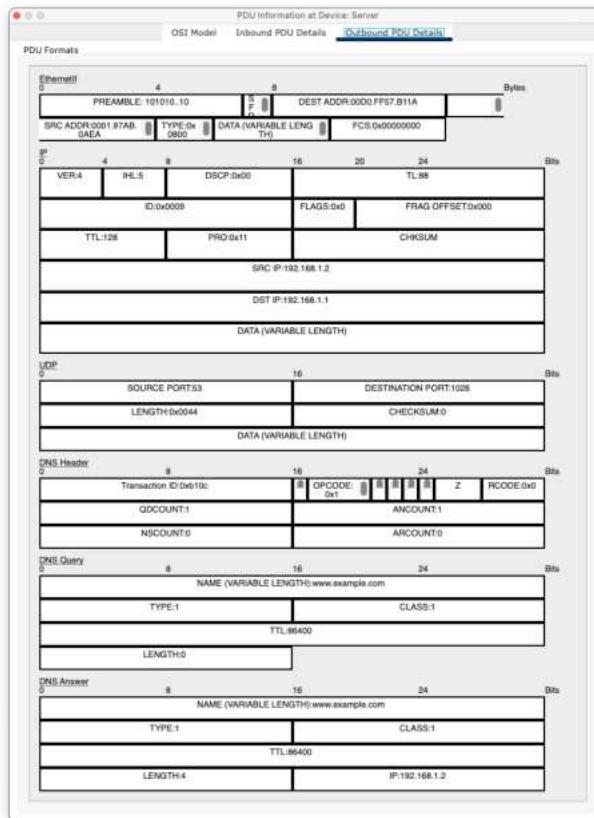
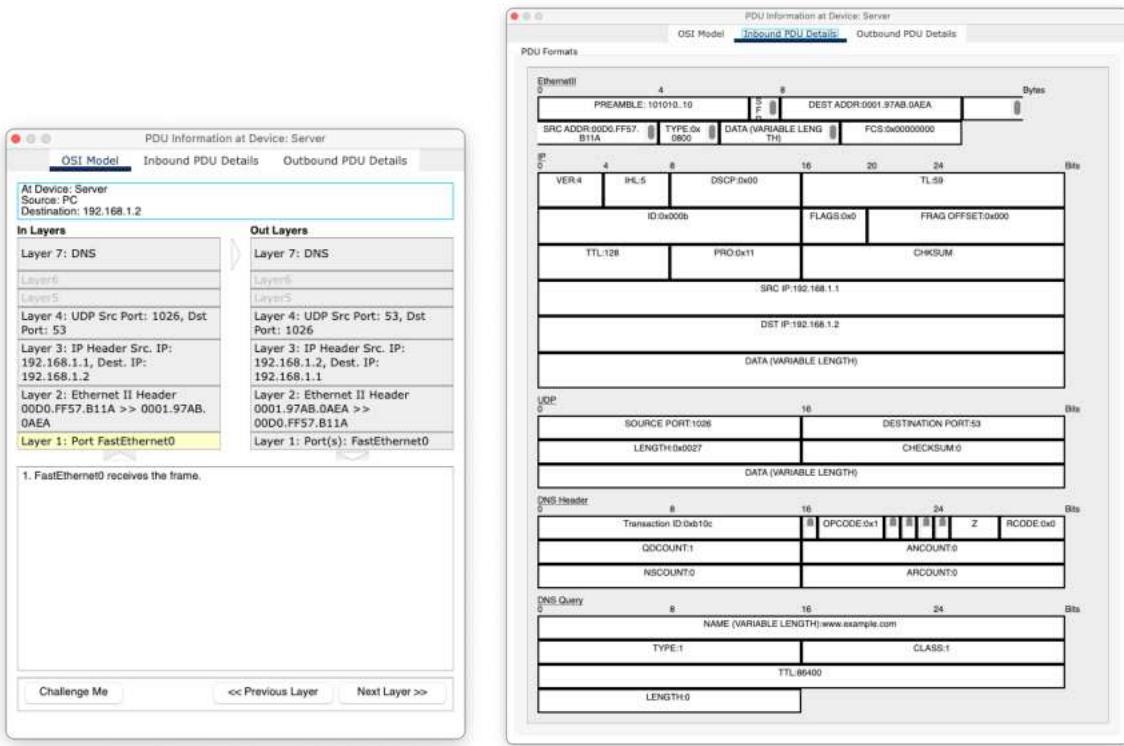
Este análisis detalla cómo se encapsulan y se transmiten los datos desde la capa de aplicación hasta la capa física en el modelo OSI, y cómo cada capa añade su propio encabezado y/o trailer para garantizar la correcta entrega de los datos.

**Parte 6: Examine el contenido de la ventana PDU Information (Información de la PDU).**

La primera ficha en la ventana PDU Information (Información de PDU) contiene información sobre la PDU entrante y/o saliente en relación con el modelo OSI. Haga clic en **Next Layer >>** (Próxima capa) varias veces para recorrer las capas entrantes y salientes, y lea la descripción del cuadro debajo de las capas para obtener una descripción general de cómo funciona el intercambio.

Examine la información de PDU de los otros eventos para obtener una descripción general de todo el proceso de intercambio.

Segundo evento de la lista:



Este evento refleja la recepción de la solicitud DNS enviada por el PC al servidor. Vamos a revisar la información detallada de la PDU en este evento.

### Detalles de la PDU:

*PDU Information at Device: Server*

Pestaña “OSI Model”:

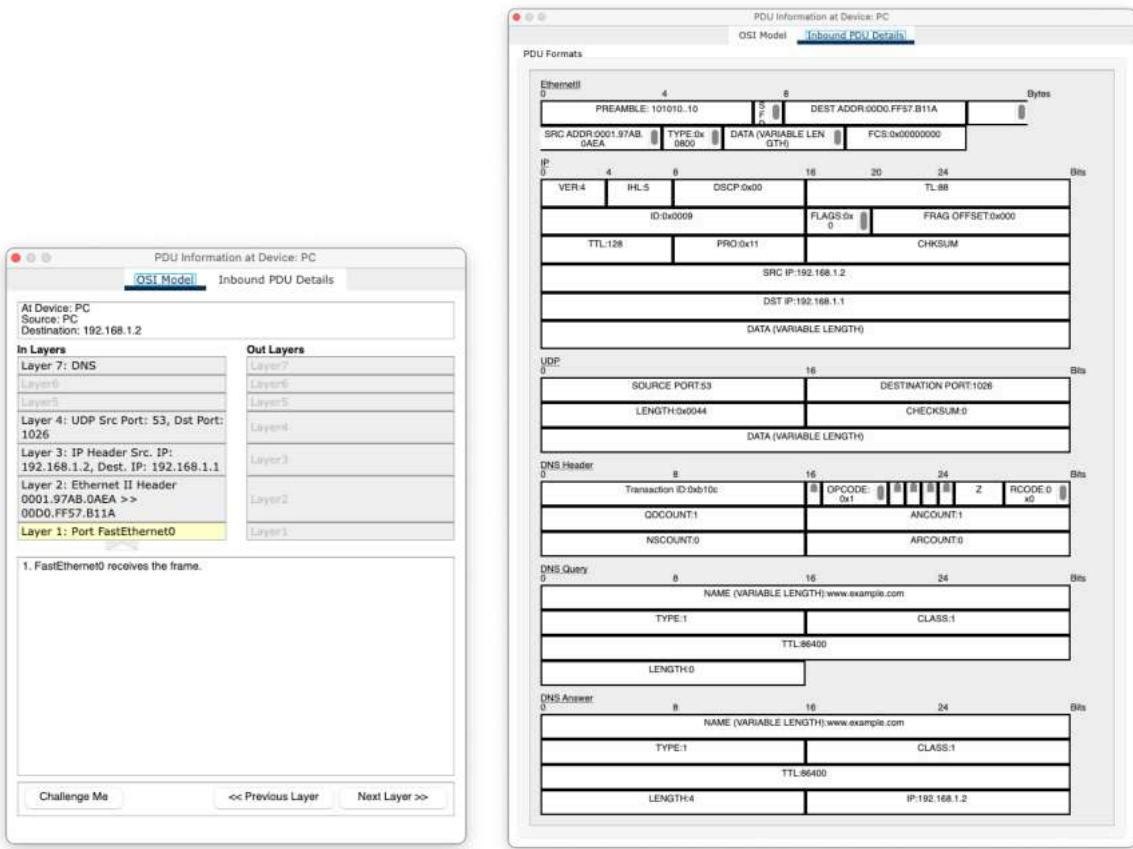
- **In Layers (Capas Entrantes):**
  - **Layer 7: DNS:** El servidor recibe una consulta DNS.
  - **Layer 4: UDP:** Puerto de origen 1026, puerto de destino 53.
  - **Layer 3: IP:** Dirección IP de origen 192.168.1.1, dirección IP de destino 192.168.1.2.
  - **Layer 2: Ethernet II:** Dirección MAC de origen 00D0.FF57.B11A, dirección MAC de destino 0001.97AB.0AEA.
- **Out Layers (Capas Salientes):**
  - **Layer 7: DNS:** El servidor envía una respuesta DNS.
  - **Layer 4: UDP:** Puerto de origen 53, puerto de destino 1026.
  - **Layer 3: IP:** Dirección IP de origen 192.168.1.2, dirección IP de destino 192.168.1.1.
  - **Layer 2: Ethernet II:** Dirección MAC de origen 0001.97AB.0AEA, dirección MAC de destino 00D0.FF57.B11A.

El servidor recibe la consulta DNS, la procesa y prepara una respuesta. Esta respuesta viaja de vuelta a la PC siguiendo el mismo camino pero en sentido inverso.

**Descripción General del Proceso:**

1. **Solicitud DNS de la PC:** La PC envía una consulta DNS al servidor.
2. **Recepción de la Consulta en el Servidor:** El servidor recibe la consulta DNS a través de las capas Ethernet II, IP, UDP, y finalmente DNS.
3. **Procesamiento y Respuesta DNS del Servidor:** El servidor procesa la consulta, forma una respuesta DNS con la dirección IP correspondiente al dominio solicitado, y encapsula esta respuesta a través de las capas DNS, UDP, IP, y Ethernet II.
4. **Respuesta DNS de Vuelta a la PC:** La respuesta se envía de vuelta a la PC siguiendo el mismo camino en sentido inverso.

Tercer y último evento de la lista:

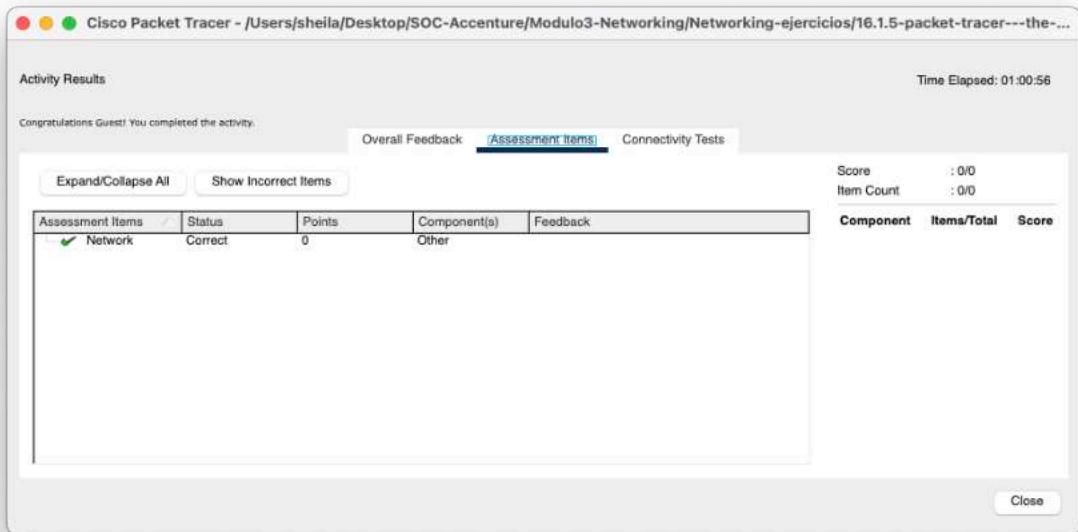


### PDU Information at Device: PC

Pestaña “OSI Model”:

- **In Layers (Capas Entrantes):**
  - **Layer 7: DNS:** La PC recibe una respuesta DNS.
  - **Layer 4: UDP:** Puerto de origen 53, puerto de destino 1026.
  - **Layer 3: IP:** Dirección IP de origen 192.168.1.2, dirección IP de destino 192.168.1.1.
  - **Layer 2: Ethernet II:** Dirección MAC de origen 0001.97AB.0AEA, dirección MAC de destino 00D0.FF57.B11A.
  - **Layer 1: Physical:** Interfaz FastEthernet0 recibe el frame.

La PC recibe la respuesta DNS del servidor, desencapsulando los datos desde la capa 2 (Ethernet II) hasta la capa 7 (DNS), donde se utiliza la dirección IP proporcionada.

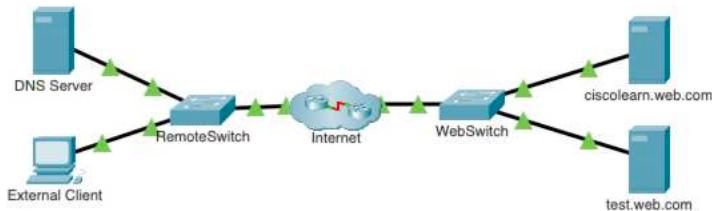


## Tarea 8: Observar solicitudes Web (apartado 16.4.3. del curso)

### Packet Tracer: Observar las solicitudes web

#### Objetivos

Ver el tráfico cliente y servidor enviado desde una PC a un servidor Web al solicitar servicios Web.



#### Instrucciones

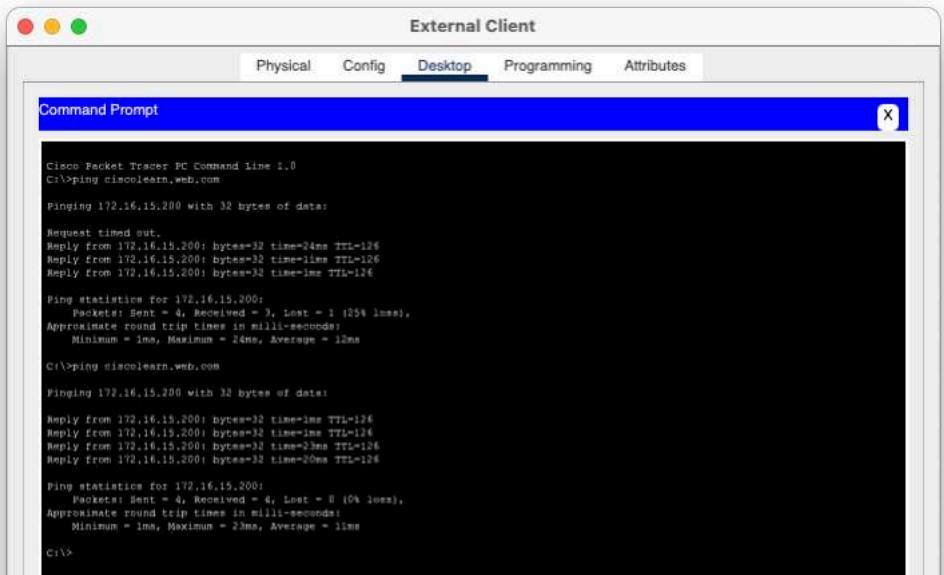
##### Parte 1: Verificar la conectividad al servidor Web.

- Haga clic en External Client (Cliente externo) y acceda a **Command Prompt** (Línea de comandos) desde la ficha **Desktop** (Escritorio).
- Use el comando **ping** para comunicarse con la URL **ciscolearn.web.com**.

**PC> ping ciscolearn.web.com**

Observe la dirección IP que aparece en el resultado del ping. Esta dirección se obtiene del servidor DNS y se resuelve como el nombre de dominio ciscolearn.web.com. Todo el tráfico reenviado a través de una red usar información de dirección IP de origen y destino.

- c. Cierre la ventana de la línea de comandos pero deje la ventana del escritorio del cliente externo abierta.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping ciscolearn.web.com

Pinging 172.16.15.200 with 32 bytes of data:
Request timed out.
Reply from 172.16.15.200: bytes=32 time=24ms TTL=126
Reply from 172.16.15.200: bytes=32 time=11ms TTL=126
Reply from 172.16.15.200: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.15.200:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 12ms

C:\>ping ciscolearn.web.com

Pinging 172.16.15.200 with 32 bytes of data:
Reply from 172.16.15.200: bytes=32 time=1ms TTL=126
Reply from 172.16.15.200: bytes=32 time=1ms TTL=126
Reply from 172.16.15.200: bytes=32 time=23ms TTL=126
Reply from 172.16.15.200: bytes=32 time=20ms TTL=126

Ping statistics for 172.16.15.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 23ms, Average = 11ms

C:\>
```

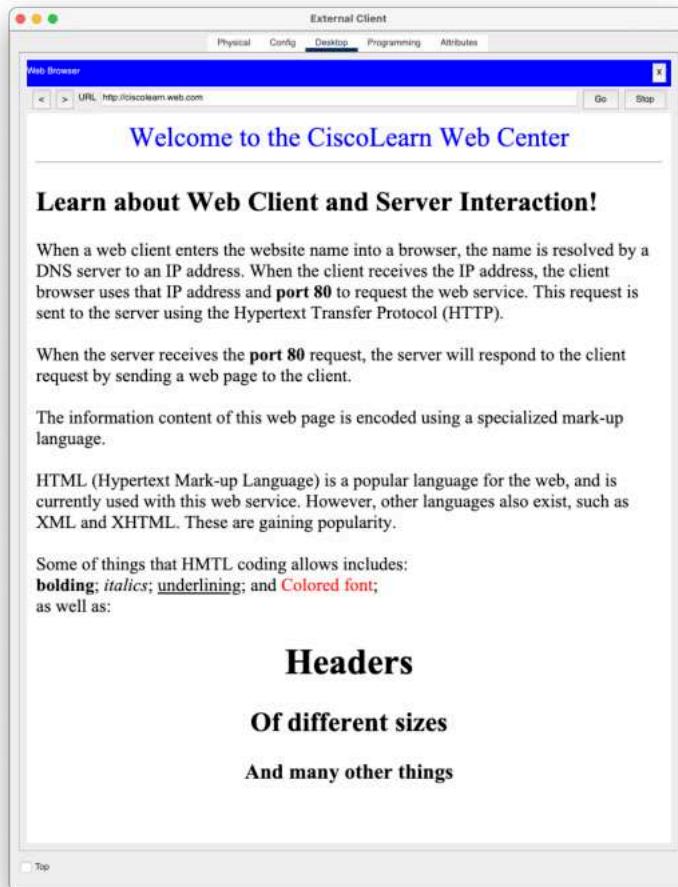
La dirección IP que aparece es 172.16.15.200.

## Parte 2: Conéctese con el servidor web.

- a. En la ventana del escritorio acceda al **Explorador Web**.
- b. En el cuadro de la URL escriba **ciscolearn.web.com**.

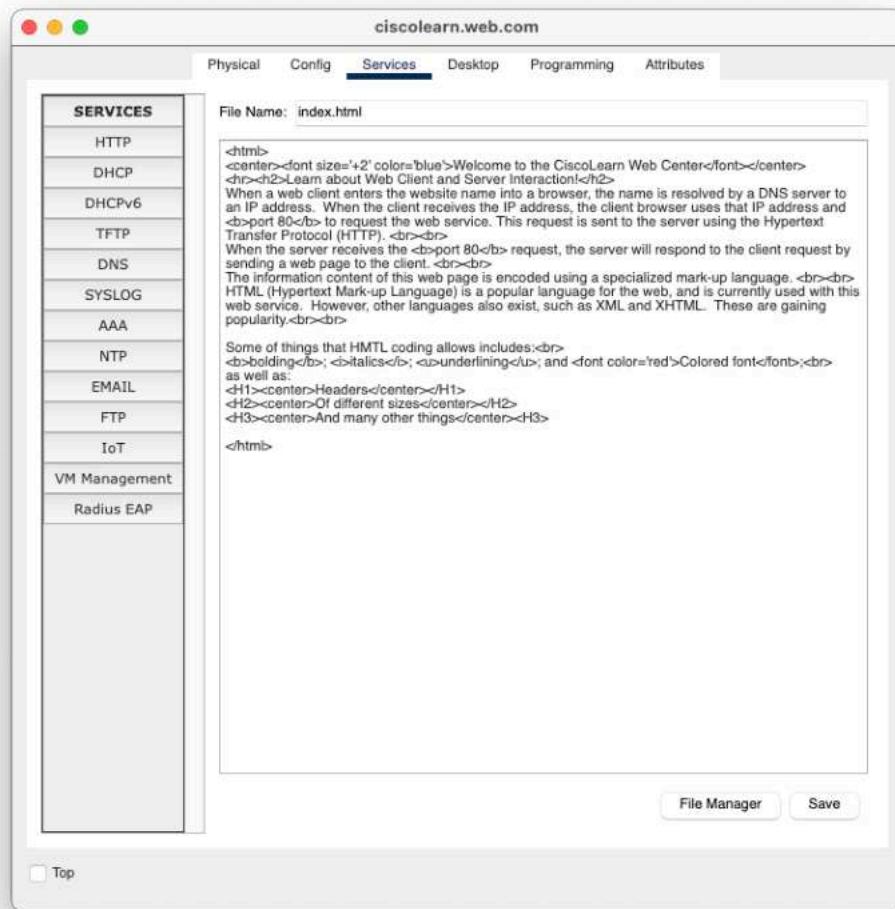
Asegúrese de leer la página Web que se muestra. Deje esta página abierta.

- c. Minimice la ventana del cliente externo, pero no la cierre.



### Parte 3: Vea el código HTML.

- Desde la topología lógica, haga clic en el servidor **ciscolearn.web.com**.
- Haga clic en la ficha **Services (Servicios)** > **HTTP**. Luego, junto al archivo **index.html**, haga clic en **(edit)** (editar).



- c. Compare el código de marcado HTML en el servidor que crea la página de visualización del navegador web en el cliente externo. Puede ser necesario volver a maximizar la ventana del cliente si se minimizó al abrir la ventana del servidor.
- d. Cierre la ventana del cliente externo y la del servidor Web.

## Comparación

Al comparar el contenido de la página web mostrada en el navegador con el código HTML del servidor, podemos ver que coinciden perfectamente. La estructura y el contenido de la página HTML generada por el servidor se reflejan exactamente en la página web mostrada al cliente.

### *Detalles específicos:*

1. **Título:** En el HTML del servidor, el título de la página es "Welcome to the CiscoLearn Web Center", que coincide con el encabezado de la página web mostrada en el cliente.
2. **Encabezado (h1):** El encabezado principal `<h1>` en el código HTML es "Welcome to the CiscoLearn Web Center", que también es el título visible en la página web del cliente.

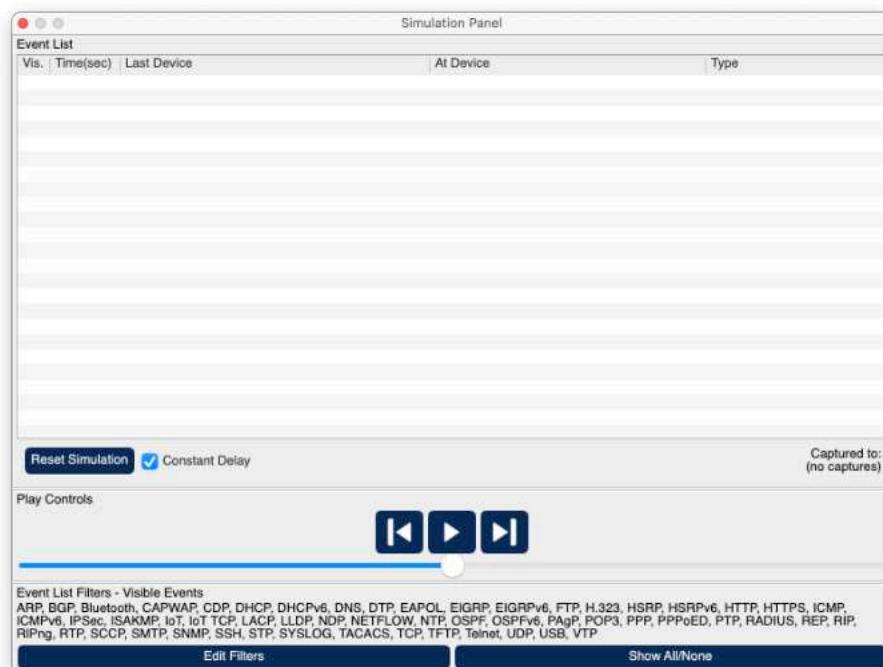
3. **Párrafos (p):** Todos los párrafos <p> en el HTML del servidor aparecen en el mismo orden y con el mismo contenido en la página web del cliente.
4. **Lista Desordenada (ul):** La lista de elementos dentro de <ul> en el servidor coincide con la lista mostrada en la página web del cliente.
5. **Encabezado Secundario (h2):** El encabezado secundario <h2> “Headers” aparece como se muestra en el cliente.
6. **Texto de Párrafo:** Los párrafos de texto, incluyendo “Of different sizes” y “And many other things”, están presentes tanto en el HTML del servidor como en la visualización del cliente.

La comparación confirma que la página web mostrada en el navegador del cliente refleja con precisión el código HTML alojado en el servidor. Todos los elementos y el contenido estructural del HTML en el servidor están presentes y se muestran correctamente en la página web del cliente.

#### **Parte 4: Observe el tráfico entre el cliente y el servidor Web.**

- a. Haga clic en la ficha Simulación de la esquina inferior derecha para acceder al modo **Simulación**.
- b. Haga doble clic en el Panel de simulación para desacoplarlo de la ventana de PT. Esto le permite mover el Panel de simulación para ver toda la topología de la red.

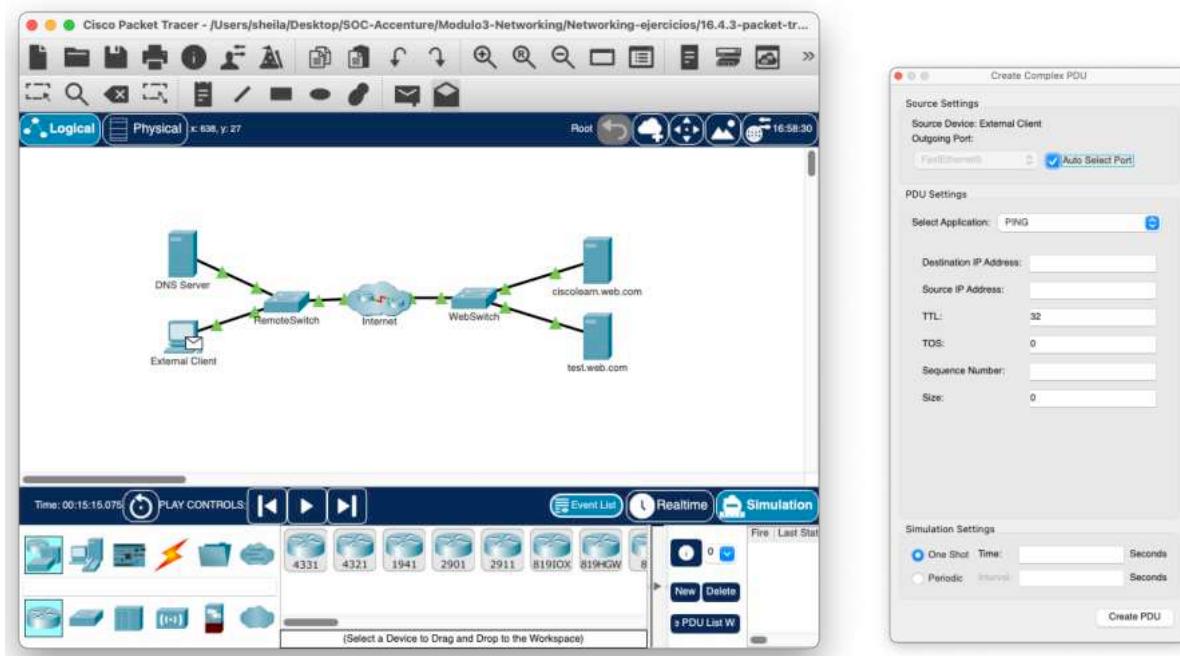
Panel de Simulación desacoplado del PT:



- c. Cree una PDU compleja en el modo Simulación para ver el tráfico.
- 1) En el **Simulation Panel** (Panel de simulación), seleccione **Edit Filters** (Editar filtros).
  - 2) Haga clic en la ficha Misc para verificar que solo estén marcadas las casillas TCP y HTTP.



- 3) Haga clic en el sobre abierto que está sobre el ícono del modo de simulación para agregar una PDU compleja.
- 4) Haga clic en **External Client** (Cliente externo) para especificarlo como origen. Se abre la ventana **Create Complex PDU** (Crear PDU compleja).

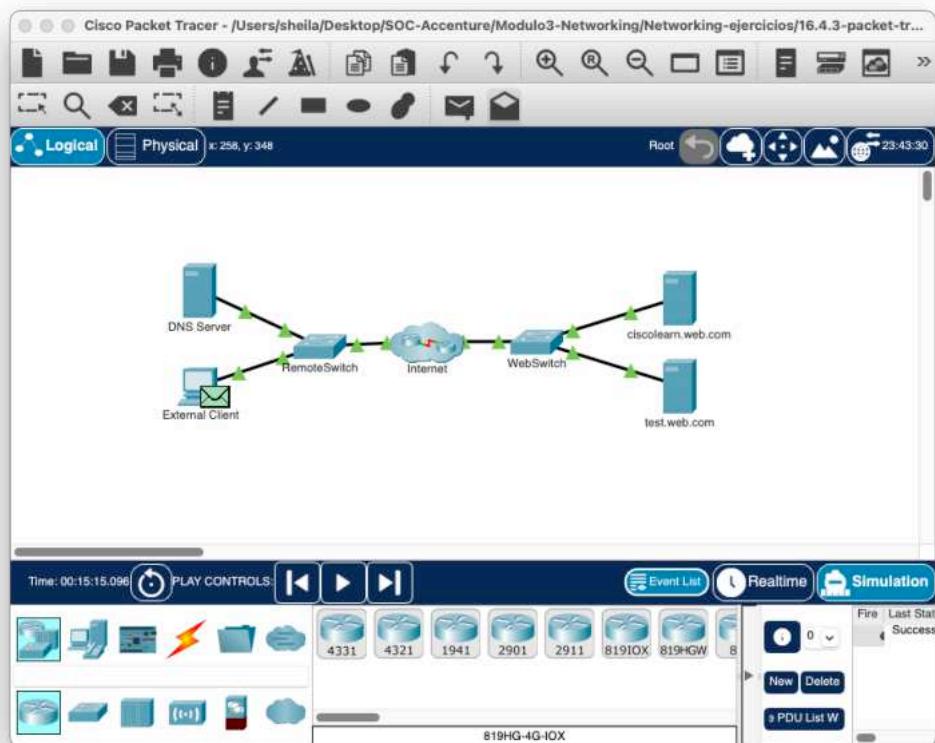


- d. Especifique la configuración de **Create Complex PDU** cambiando lo siguiente en la ventana de la PDU compleja:
  - 1) En PDU Settings (Configuración de PDU), Select Application (Seleccionar aplicación) debe ser **HTTP**.
  - 2) Haga clic en el servidor **ciscolearn.web.com** para configurarlo como dispositivo de destino. Observe que aparecerá la dirección IP del servidor web en el cuadro de destino dentro de la ventana de la PDU compleja.
  - 3) En Starting Source Port (Puerto de origen inicial), introduzca **1000**.

- 4) En Simulation Settings (Configuración de la simulación), seleccione Periodic Interval (Intervalo periódico) y escriba **120**.



- e. Cree la PDU, haga clic en la casilla **Create PDU** de la ventana **Create Complex PDU**.
- 1) Observe el flujo de tráfico haciendo clic en **Play** (Reproducir) en el panel de simulación. Para acelerar la animación utilice el control deslizante de reproducción. Cuando aparezca la ventana Buffer Full (Búfer lleno), haga clic en el botón **View Previous Events** (Ver eventos anteriores).
  - 2) Desplácese por la lista de eventos. Observe la cantidad de paquetes que viajaron desde el origen hacia el destino. HTTP es un protocolo TCP, por lo que requiere que se establezca una conexión y se acuse recibo de los paquetes. Esto aumenta considerablemente la cantidad de tráfico.



**Event List**

Vis.	Time(sec)	Last Device	At Device	Type
	0.001	External Client	RemoteSwitch	TCP
	0.002	RemoteSwitch	Remote	TCP
	0.004	Local	WebSwitch	TCP
	0.005	WebSwitch	test.web.com	TCP
	0.005	WebSwitch	ciscolearn.web.com	TCP
	0.006	ciscolearn.web.com	WebSwitch	TCP
	0.007	WebSwitch	Local	TCP
	0.009	Remote	RemoteSwitch	TCP
	0.010	RemoteSwitch	External Client	TCP
	0.010	--	External Client	TCP
	0.011	External Client	RemoteSwitch	TCP
	0.011	--	External Client	TCP
	0.012	External Client	RemoteSwitch	TCP
	0.012	RemoteSwitch	Remote	TCP
	0.013	RemoteSwitch	Remote	TCP
	0.014	Local	WebSwitch	TCP
	0.015	WebSwitch	WebSwitch	TCP
	0.015	Local	WebSwitch	TCP
	0.016	WebSwitch	ciscolearn.web.com	TCP
	0.016	WebSwitch	ciscolearn.web.com	TCP
	0.017	ciscolearn.web.com	WebSwitch	TCP
	0.018	WebSwitch	Local	TCP
	0.020	Remote	RemoteSwitch	TCP
	0.021	RemoteSwitch	External Client	TCP

Below the event list, there are buttons for "Reset Simulation" and "Constant Delay". A timestamp "Captured to: 0.021 s" is shown. The "Play Controls" section features buttons for step forward/backward and play/pause. At the bottom, there are "Edit Filters" and "Show All/None" buttons, along with a list of event filters: ARP, BGP, DHCP, DHCPv6, DNS, EIGRP, EIGRPv6, HSRP, HSRPv6, HTTP, ICMP, ICMPv6, NDP, OSPF, OSPFv6, RIP, RIPng, TCP.

## **Análisis de la PDU:**

### **1. Eventos TCP Listados:**

- La lista de eventos en la captura muestra múltiples intercambios de paquetes TCP entre diferentes dispositivos.
- Los dispositivos involucrados incluyen WebSwitch, RemoteSwitch, External Client, y ciscolearn.web.com.
- Cada línea en la lista representa un evento individual donde un paquete es enviado de un dispositivo a otro.

### **2. Cantidad de Paquetes:**

- La captura muestra que hay muchos eventos listados en un período de tiempo corto (menos de un segundo en algunos casos), lo que indica un tráfico bastante intenso.
- Esto es típico en las conexiones TCP debido a la naturaleza del protocolo que requiere el establecimiento de conexión, transferencia de datos, y confirmaciones.

### **3. Patrón de Comunicación:**

- Los paquetes están siendo enviados de External Client a ciscolearn.web.com y viceversa.
- También hay paquetes que pasan por WebSwitch y RemoteSwitch, indicando que estos dispositivos están en la ruta de la comunicación entre el cliente y el servidor.

### **4. Establecimiento de Conexión:**

- Se observa el intercambio inicial necesario para establecer una conexión TCP.

### **5. Tipos de Eventos:**

- Todos los eventos listados están etiquetados como TCP.

## **Descripción del Flujo de Tráfico**

### **1. Inicio del Tráfico:**

- El External Client inicia la conexión TCP con ciscolearn.web.com.
- El servidor responde, y la conexión se establece. Mediante el three handshake.

### **2. Transferencia de Datos:**

- Una vez establecida la conexión, el cliente envía solicitudes HTTP (a través de TCP) al servidor.
- El servidor responde con los datos solicitados (la página web), que son fragmentados en múltiples paquetes TCP.

### **3. Confirmaciones (ACKs):**

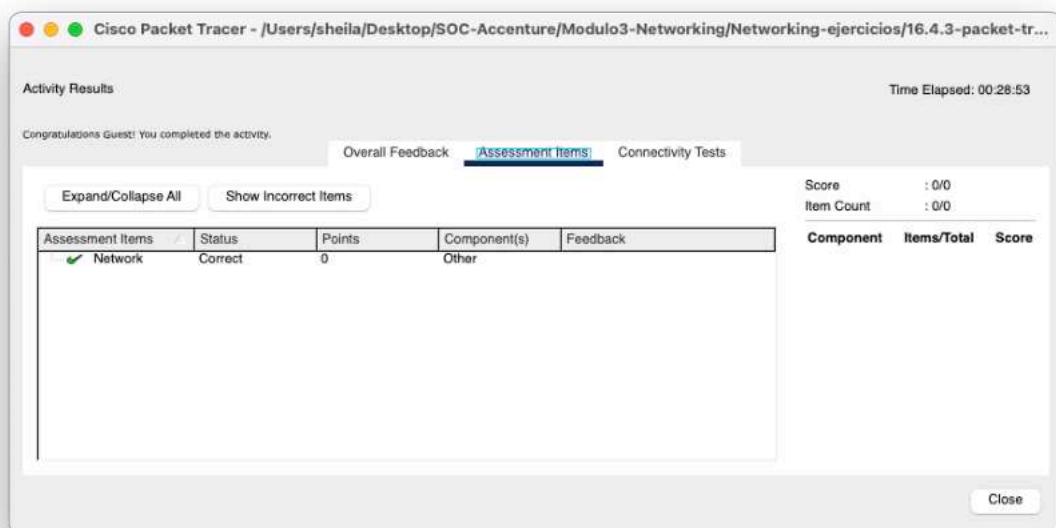
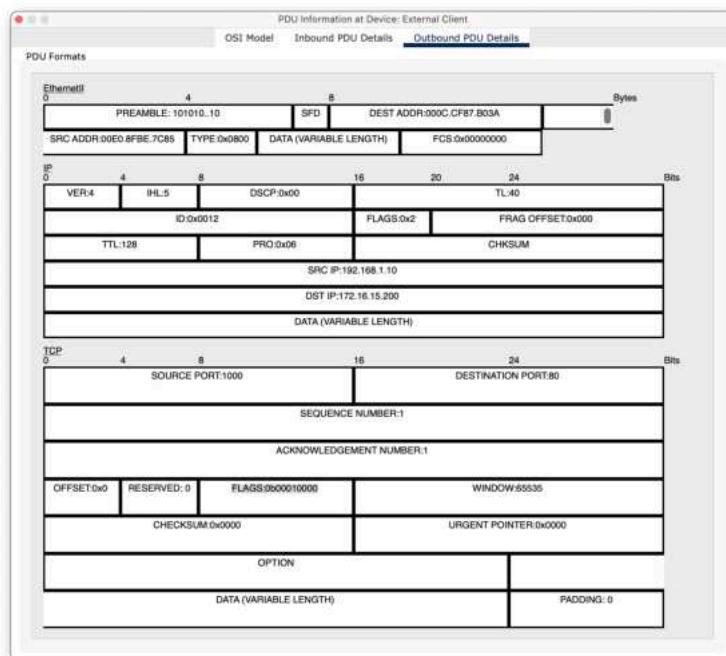
- Despues de la recepción de los datos, hay varios mensajes de confirmación (ACK) enviados de vuelta al servidor para asegurar que los paquetes fueron recibidos correctamente.
- Este proceso continúa para cada segmento de datos transferido.

### **4. Ruteo a través de Switches:**

- Los paquetes se están ruteando a través de WebSwitch y RemoteSwitch, que son puntos intermedios en la red.
- Esto es indicado por los eventos que muestran tráfico pasando por estos dispositivos antes de llegar a su destino final.

La captura de pantalla del panel de simulación muestra un tráfico típico de una comunicación HTTP sobre TCP, incluyendo el establecimiento de conexión, transferencia de datos y confirmaciones, con el tráfico pasando a través de varios switches en la red.

Por último, revisando los eventos de la PDU, encontramos uno de “ACK” para mostrar aquí.



## Tarea 9: Usar Servicios FTP (apartado 16.5.3. del curso)

### Packet Tracer: Utilizar Servicios FTP

#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
Servidor FTP (ftp.pka)	NIC	209.165.200.226	255.255.255.224

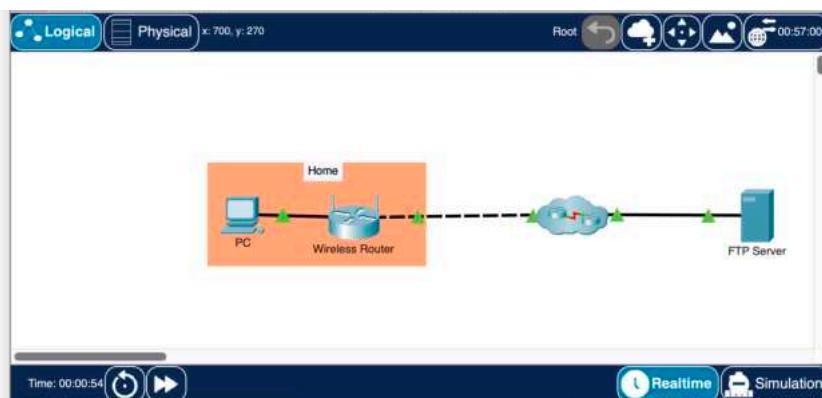
#### Objetivos

- Cargar un archivo al servidor FTP
- Descargar un archivo desde el servidor FTP

#### Aspectos básicos/Situación

El Protocolo de transferencia de archivos (FTP) es una aplicación comúnmente utilizada para transferir archivos entre clientes y servidores en la red. El servidor está configurado para ejecutar el servicio donde los clientes se conectan, inician sesión y transfieren archivos. FTP utiliza el puerto 21 como puerto de comando del servidor para crear la conexión. A continuación, FTP utiliza el puerto 20 para la transferencia de datos.

En esta actividad, cargará un archivo a un servidor FTP. También descargará un archivo desde un servidor FTP.



#### Instrucciones

##### Parte 1: Cargar un archivo al servidor FTP

En esta parte, encontrará el archivo **sampleFile.txt** y lo cargará en un servidor FTP.

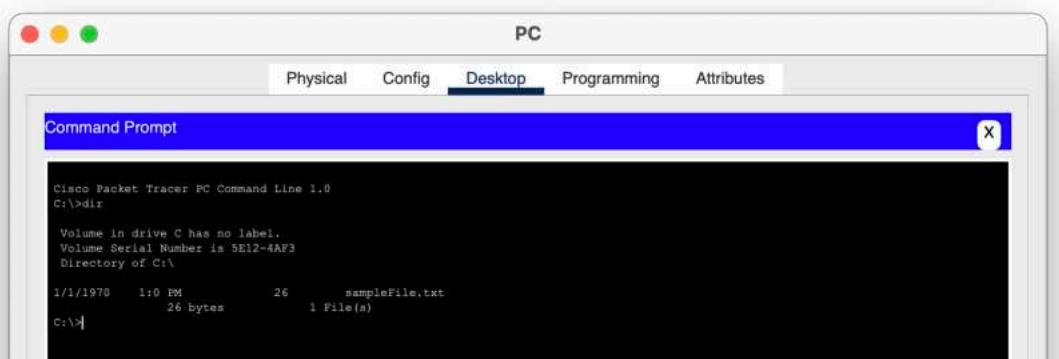
##### Paso 1: Ubique el archivo.

- Haga click en **PC-A**.
- Haga click en **Desktop(Escritorio)**

- c. Haga clic en **Símbolo del sistema**.
- d. En el indicador, haga clic en ? para listar los comandos disponibles.
- e. Ingrese **dir** para ver los archivos en la PC. Observe que hay un archivo **sampleFile.txt** en el directorio C:\

C:> **dir**

Volume in drive C has no label.  
 Volume Serial Number is 5E12-4AF3  
 Directory of C:\  
  
 12/31/1969 17:0 PM 26 sampleFile.txt  
 26 bytes 1 File (s)



```
Cisco Packet Tracer PC Command Line 1.0
C:>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

12/31/1969  1:0 PM           26      sampleFile.txt
               26 bytes      1 File(s)

C:>
```

## Paso 2: Conectarse al servidor FTP.

- a. FTP al servidor FTP en **209.165.200.226** o **ftp.pka**.

C:> **ftp 209.165.200.226**

Trying to connect...209.165.200.226

Connected to 209.165.200.226

- b. Ingrese el nombre de usuario **student** y la contraseña **class** para obtener acceso.

220- Welcome to PT Ftp Server

Username:**student**

331- Username ok, need password

Password:

230- Logged in

(passive mode On)

```

Cisco Packet Tracer PC Command Line 1.0
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3

Directory of C:\

1/1/1970   1:0 PM           26      sampleFile.txt
               26 bytes          1 File(s)

C:\>ftp 209.165.200.226
Trying to connect...209.165.200.226
Connected to 209.165.200.226
220- Welcome to PT Ftp server
Username:student
331- Username ok, need password
Password:
230- Logged in
      (passive mode On)
ftp>

```

### Paso 3: Cargar un archivo al servidor FTP

- a. Ingresar ? para ver los comandos disponibles en el cliente ftp.

```

ftp> ?
?
cd
delete
dir
get
help
passive
put
pwd
quit
rename

```

ftp>

- b. Introduzca **dir** para ver los archivos disponibles en el servidor.

ftp> **dir**

Listing /ftp directory from 192.168.1.3:

```

0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advpipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
<output omitted>

```

```

ftp>?
?
cd
delete
dir
get
help
passive
put
pwd
quit
rename
ftp>dir
Listing /ftp directory from 209.165.200.226:
0 : aa942-k8.bin 5571584
1 : aa923-k8.bin 30468096
2 : c1841-adviservicesk9-mz.124-15.t1.bin 33591760
3 : c1841-ipbase-mz.123-14.W7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591760
6 : c2600-adviservicesk9-mz.124-15.t1.bin 33591760
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-adviservicesk9-mz.124-15.t1.bin 50938004
10 : c2800nm-adviservicesk9-mz.151-4.M4.bin 33591760
11 : c2800nm-ipbase-mz.123-14.W7.bin 59715408
12 : c2800nm-ipbasek9-mz.124-8.bin 15595648
13 : c2960-universalk9-mz.SPA.155-3.M4a.bin 33591760
14 : c2950-16p12-mz.121-23.EA8.bin 3058048
15 : c2950-16p12-mz.121-22.EA8.bin 3117380
16 : c2960-lanbase-mz.122-35.FX.bin 4414921
17 : c2960-lanbase-mz.122-35.SE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-adviservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-adviservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_cnn-universalk9-16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487592
25 : cgr1000-universalk9-mz.SPA.156-1.CG 184530138
26 : ir800-universalk9+bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yoato-1.7.2.tar 2877446
30 : ir800_yoato-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-ieq412-mz.121-22.EA4.bin 3117380
ftp>

```

Top

c. Introduzca **put sampleFile.txt** para enviar el archivo al servidor.

**ftp> put sampleFile.txt**

Writing file sampleFile.txt to 209.165.200.226:

File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.08 secs (325 bytes/sec)

**ftp>**

d. Utilice el comando **dir** nuevamente para listar el contenido del servidor FTP y verificar que el archivo se haya cargado en el servidor FTP.

```

PC

Physical Config Desktop Programming Attributes

Command Prompt

ftp>put sampleFile.txt
Writing file sampleFile.txt to 209.165.200.226:
File transfer in progress...

[Transfer complete - 26 bytes]
26 bytes copied in 0.254 secs (102 bytes/sec)
ftp>dir
Listing /ftp directory from 209.165.200.226:
0 : ass840-kd.bin
1 : as5923-k8.bin
2 : c1841+advipservicesk9-mz.124-15.Tl.bin
3 : c1841-ipbase-mz.123-14.7T.bin
4 : c1841-ipbasek9-mz.124-12.bin
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin
6 : c2800-advipservicesk9-mz.124-15.Tl.bin
7 : c2800-1-mz.122-28.bin
8 : c2800-ipbasek9-mz.124-8.bin
9 : c2800nm-advipservicesk9-mz.124-15.Tl.bin
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin
11 : c2800nm-ipbase-mz.123-14.7T.bin
12 : c2800nm-ipbasek9-mz.124-8.bin
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin
14 : c2950-1Eq412-mz.121-22.EA8.bin
15 : c2950-1Eq412-mz.121-22.EA8.bin
16 : c2960-lanbase-mz.122-25.FX.bin
17 : c2960-lanbase-mz.122-25.EERI.bin
18 : c2960-lanbasek9-mz.150-2.S84.bin
19 : c3560+advipservicesk9-mz.122-37.S8L.bin
20 : c3560+advipservicesk9-mz.122-46.S8_.bin
21 : c800-universalk9-mz.SPA.152-4.M4.bin
22 : c800-universalk9-mz.SPA.154-3.M6a.bin
23 : cat3k_caa-universalk9.16.03.02.SPA.bin
24 : ogr1000-universalk9-mz.SPA.154-2.CG
25 : ogr1000-universalk9-mz.SPA.156-3.CG
26 : ir800-universalk9-bundle.SPA.156-3.M.bin
27 : ir800-universalk9-mz.SPA.155-3.M
28 : ir800-universalk9-mz.SPA.156-3.M
29 : ir800_yocto-1.7.2.tar
30 : ir800_yocto-1.7.2_python-2.7.3.tar
31 : pt1000-1-mz.122-28.bin
32 : pt3000-16q412-mz.121-22.EN4.bin
33 : sampleFile.txt
26
ftp>

```

## 2. Parte 2: Descargar un archivo desde el servidor FTP

También puede descargar un archivo desde un servidor FTP. En esta parte, cambiará el nombre del archivo **sampleFile.txt** y lo descargará del servidor FTP.

### Paso 1: Cambie el nombre del archivo a un servidor FTP.

- En el indicador **ftp>**, cambie el nombre del archivo **ampleFile.txt** a **sampleFile\_FTP.txt**.

```
ftp> rename sampleFile.txt sampleFile_FTP.txt
```

Renaming sampleFile.txt

```
ftp>
```

[OK Renamed file successfully from sampleFile.txt to sampleFile\_FTP.txt]

```
ftp>
```

- En el indicador **ftp>**, ingrese **dir** para verificar que se haya cambiado el nombre del archivo.

```

PC
Physical Config Desktop Programming Attributes

Command Prompt X

ftp>rename sampleFile.txt sampleFile_FTP.txt
Renaming sampleFile.txt

ftp>
[OK] Renamed file successfully from sampleFile.txt to sampleFile_FTP.txt
ftp>dir
Listing /ftp directory from 209.165.200.226:
0 : axa42-k8.bin 5571584
1 : axa923-k8.bin 30468096
2 : c1841-adviservicesk9-mz.124-15.Tl.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M&a.bin 33591768
6 : c2800-adviservicesk9-mz.124-15.Tl.bin 33591768
7 : c2800-i-mz.122-28.bin 5571584
8 : c2800-ipbasek9-mz.124-8.bin 13169700
9 : c2800m-adviservicesk9-mz.124-15.Tl.bin 50938004
10 : c2800m-adviservicesk9-mz.151-8.M&.bin 33591768
11 : c2800m-ipbase-mz.123-14.T7.bin 5571584
12 : c2800m-ipbasek9-mz.124-8.bin 15322644
13 : c2800-universalk9-mz.SPA.155-3.M&a.bin 33591768
14 : c2900-adviservicesk9-mz.124-20.ZM4.bin 3059148
15 : c2900-adviservicesk9-mz.121-25.ZAE.bin 3117952
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SREI.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SRA.bin 4670455
19 : c3560-adviservicesk9-mz.122-37.SEI.bin 8662192
20 : c3560-adviservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M&.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M&a.bin 83029236
23 : cat3k_csa-universalk9.16.03.02.BPA.bin 50532949
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487582
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ix800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ix800-universalk9-mz.SPA.155-3.M 61750062
28 : ix800-universalk9-mz.SPA.156-3.M 63753767
29 : ix800_yocto-1.7.2.tar 2877440
30 : ix800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-1-mz.122-28.bin 5571584
32 : pt3000-16g411-mz.121-22.ZA4.bin 3117390
33 : sampleFile_FTP.txt 26
ftp>
```

## Paso 2: Descargar el archivo desde el servidor FTP.

- Ingrese el comando **get sampleFile\_FTP.txt** para recuperar el archivo del servidor.

**ftp> get sampleFile\_FTP.txt**

Reading file sample File\_FTP.txt from 209.165.200.226:

File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.013 secs (2000 bytes/sec)

**ftp>**

- Ingrese **quit** para salir del cliente FTP cuando haya terminado.
- Mostrar de nuevo el contenido del directorio en el PC para ver el archivo de imagen desde el servidor FTP.

```

PC

ftp>get sampleFile_FTP.txt
Reading file sampleFile_FTP.txt from 209.165.200.226:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0 secs
ftp>quit

221- Service closing control connection.
C:\>dir

Volume in drive C has no label,
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970  1:0 PM           26      sampleFile.txt
1/1/1970  1:0 PM           26      sampleFile_FTP.txt
                           52 bytes   2 File(s)

C:\>

```

Top

### Paso 3: Eliminar el archivo del servidor FTP.

- Inicie sesión en el servidor FTP nuevamente para eliminar el archivo **sampleFile\_FTP.txt**.
- Ingrese el comando para eliminar el archivo **sampleFile\_FTP.txt** del servidor.

¿Qué comando utilizó para eliminar el archivo del servidor FTP?

**ftp> delete sampleFile\_FTP.txt**

- Ingrese **quit** para salir del cliente FTP cuando haya terminado.

```

PC

Physical Config Desktop Programming Attributes

Command Prompt X

ftp>delete sampleFile_FTP.txt
Deleting file sampleFile_FTP.txt from 209.165.200.226: ftp>
[Deleted sampleFile_FTP.txt successfully]
ftp>dir

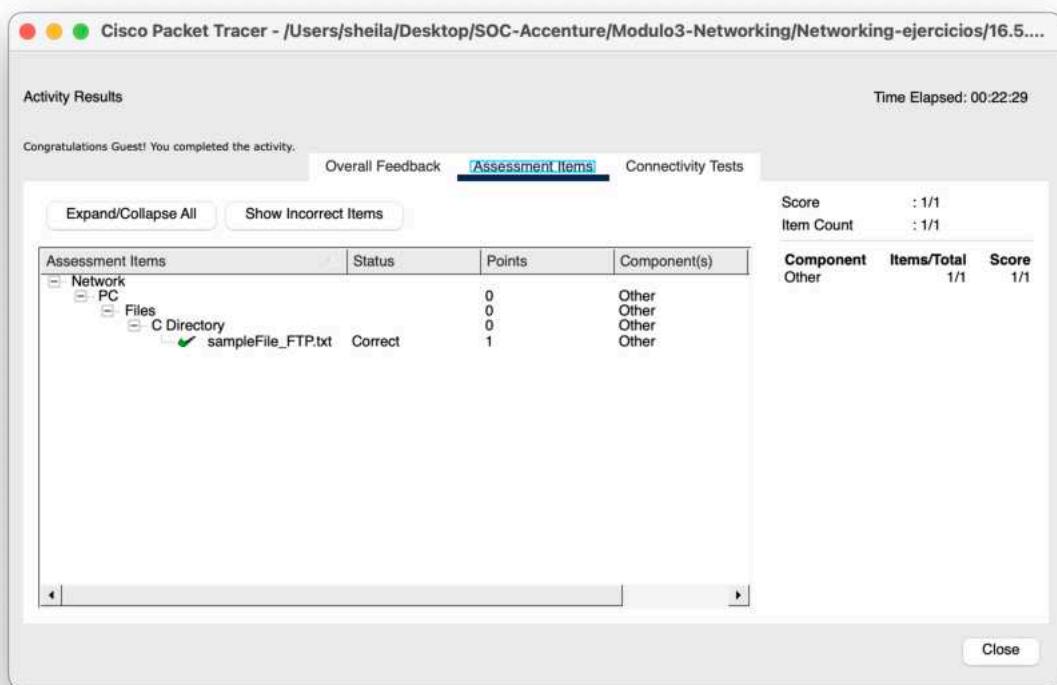
Listing /ftp directory from 209.165.200.226:
0 : aa842-k8.bin                               5571594
1 : aa823-k8.bin                               30468096
2 : c1841-adviservicesk9-mz.124-15.71.bin    33591768
3 : c1841-ipbase-nz.123-14.77.bin             13832032
4 : c1841-ipbasek9-mz.124-17.bin              16599160
5 : c1900-universalk9-mz.BPA.155-3.M4a.bin    33591768
6 : c2600-adviservicesk9-mz.124-15.71.bin    33591768
7 : c2800m-adviservicesk9-mz.124-15.71.bin    8571594
8 : c2800m-adviservicesk9-mz.124-15.71.bin    13163700
9 : c2800m-adviservicesk9-mz.124-15.71.bin    50398004
10 : c2800m-adviservicesk9-mz.151-4.M4.bin     33591768
11 : c2800m-ipbase-nz.123-14.77.bin            5571594
12 : c2800m-ipbasek9-mz.124-8.bin              15522644
13 : c2900-universalk9-mz.BPA.155-3.M4a.bin    33591768
14 : c2950-16q412-nz.121-22.EA4.bin            3058048
15 : c2950-16q412-nz.121-22.RA8.bin            3117390
16 : c2960-lanbase-mz.122-25.FX.bin            4424921
17 : c2960-lanbase-mz.122-25.RR61.bin          4470455
18 : c2960-lanbasek9-mz.122-25.RR61.bin        4470455
19 : c3500-adviservicesk9-mz.122-31.SFL.bin    84621355
20 : c3500-adviservicesk9-mz.122-46.SE.bin     10713278
21 : c800-universalk9-mz.BPA.152-4.M4.bin     33591768
22 : s800-universalk9-mz.BPA.154-3.M6.bin     83029236
23 : csm100-csa-universalk9.16.03.02.BPA.bin   505932819
24 : cgr1000-universalk9-mz.BPA.154-2.CG      159487552
25 : cgr1000-universalk9-mz.BPA.156-2.CG      184530138
26 : ir800-universalk9-bundlew.BPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.BPA.155-3.M          61750062
28 : ir800-universalk9-mz.BPA.156-3.M          63753767
29 : ir800-youngster-tar.BPA.155-3.M          2819000
30 : ir800-zipcode-1.7.2-python-2.7.3.tar     6912000
31 : pt1000-1-nz.122-28.his                   5571594
32 : pt1000-16q412-mz.121-22.EA4.bin          3117390

ftp>quit

221- Service closing control connection.
C:\>
```

Top

Se ha usado el comando “dir” para comprobar que efectivamente el archivo había sido borrado.



## Tarea 10: Uso de Telnet y SSH (apartado 16.6.4 del curso)

### Packet Tracer: uso de Telnet y SSH

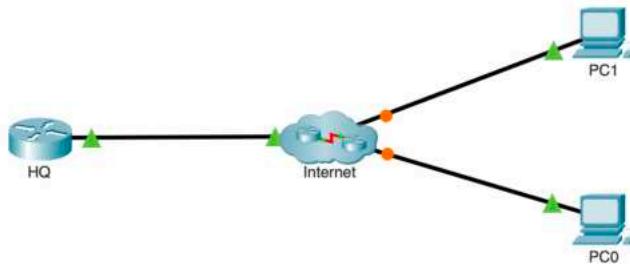
#### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
SEDE CENTRAL (HQ)	G0/0/1	64.100.1.1	255.255.255.0
PC0	NIC	DHCP	
PC1	NIC	DHCP	

#### Objetivos

En esta actividad, establecerá una conexión remota a un enrutador utilizando Telnet y SSH.

- Verifique la conectividad
- Acceder a un dispositivo remoto



## Instrucciones

### Parte 1: Verificar la conectividad

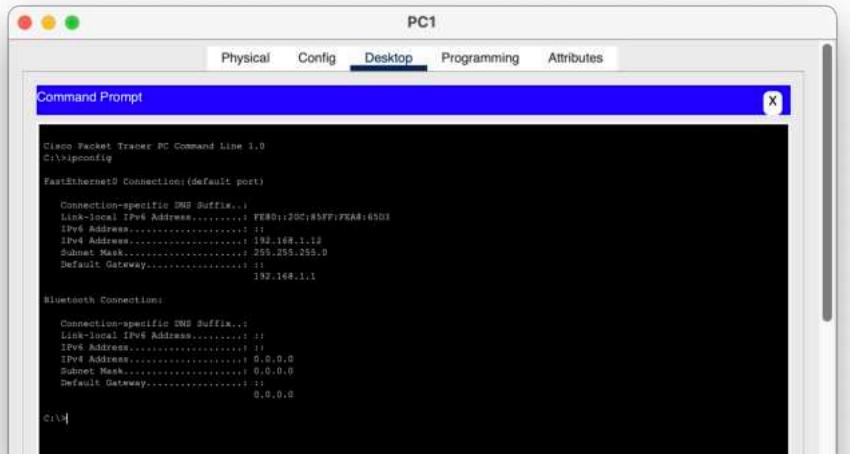
En esta parte, verificará que la PC tenga direccionamiento IP y pueda hacer ping al router remoto.

#### Paso 1: Verificar la dirección IP en una PC.

- Desde una PC, haga clic en **Desktop** (Escritorio). Haga clic en **Símbolo del sistema**.
- En el indicador, verifique que la PC tenga una dirección IP de DHCP.

¿Qué comando utilizó para verificar la dirección IP de DHCP?

**ipconfig**



#### Paso 2: Verifique la conectividad a la sede central (HQ).

Verifique que pueda hacer ping al enrutador en HQ con la dirección IP que figura en la tabla de direccionamiento.

```

C:\>ping 64.100.1.1

Pinging 64.100.1.1 with 32 bytes of data:
Request timed out.
Reply from 64.100.1.1: bytes=32 time<1ms TTL=253
Reply from 64.100.1.1: bytes=32 time<1ms TTL=253
Reply from 64.100.1.1: bytes=32 time<1ms TTL=253

Ping statistics for 64.100.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

## Parte 2: Acceder a un dispositivo remoto

En esta parte, intentará establecer una conexión remota mediante Telnet y SSH.

### Paso 1: Telnet a la sede central (HQ).

En el indicador, ingrese el comando **telnet 64.100.1.1**.

¿Tuvo éxito? ¿Cuál fue la salida?

```

C:\>telnet 64.100.1.1
Trying 64.100.1.1 ...Open
[Connection to 64.100.1.1 closed by foreign host]
C:\>

```

No.			
C:>	telnet		64.100.1.1
Trying	64.100.1.1		...Open
<b>[Connection to 64.100.1.1 closed by foreign host]</b>			

### Paso 2: SSH a HQ.

El enrutador está configurado correctamente para no permitir el acceso inseguro a Telnet. Debe usar SSH.

En el indicador, ingrese el comando **ssh -l admin 64.100.1.1**. Introduzca la contraseña **class** cuando corresponda.

C:> **ssh -l admin 64.100.1.1**

Password:

¿Qué aparece después de acceder al enrutador con éxito a través de SSH?

HQ#

C:\>ssh -l admin 64.100.1.1  
Password:  
% Password: timeout expired!  
% Login invalid  
[Connection to 64.100.1.1 closed by foreign host]  
C:\>ssh -l admin 64.100.1.1  
Password:  
% Login invalid  
Password:  
% Login invalid  
Password:  
HQ#

Congratulations Guest! You completed the activity.

Activity Results

Time Elapsed: 00:16:16

Overall Feedback    **Assessment Items**    Connectivity Tests

Expand/Collapse All    Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PC1				
Files				
C Directory				
sampleFile_FTP.txt	Correct	1	Other	

Score : 1/1  
Item Count : 1/1

Component	Items/Total	Score
Other	1/1	1/1

**Close**

## Tarea 11: Usar el Comando ipconfig (apartado 17.1.3 del curso)

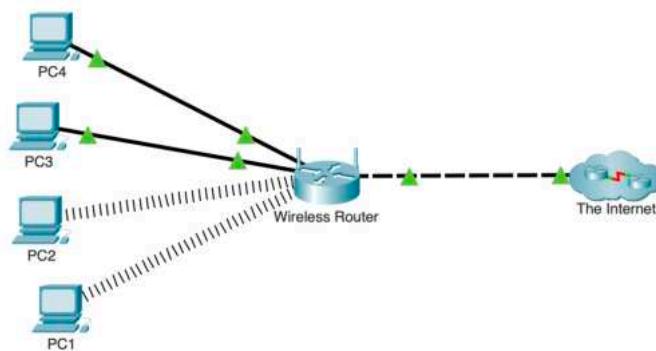
### Packet Tracer: Usar el comando ipconfig

#### Objetivos

- Usar el comando **ipconfig** para identificar configuraciones incorrectas en una PC.

## Aspectos básicos/Situación

El propietario de una pequeña empresa no puede conectarse a Internet desde una de las cuatro PC de la oficina. Todas las PC están configuradas con direcciones IP estáticas que usan la red 192.168.1.0 /24. Las PC deben poder acceder al servidor web [www.cisco.pka](http://www.cisco.pka). Use el comando **ipconfig /all** para identificar qué PC está configurada incorrectamente.



## Instrucciones

### Parte 1: Verificar las configuraciones

- Acceda al **símbolo del sistema** en cada PC y escriba el comando **ipconfig /all** en el indicador.

The screenshot shows a "Command Prompt" window with a blue title bar and a white body. The title bar has the text "PC1" and several tabs: "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". The window contains the following text:

```
C:\>ipconfig /all

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

Wlaness0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0090.210A.70A5
Link-local IPv6 Address....: FE80::210A:70A5%1
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.101
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DHCP Server.....: 192.168.1.1
DHCPv6 IID.....: 11940
DHCPv6 Client DUID.....: 00-01-00-01-D2-06-CD-3B-00-90-21-0A-70-A5
DNS Servers.....: 192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0001.97D4.61E3
Link-local IPv6 Address....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
DHCP Server.....: 0.0.0.0
DHCPv6 IID.....: 11940
DHCPv6 Client DUID.....: 00-01-00-01-D2-06-CD-3B-00-90-21-0A-70-A5
DNS Servers.....: 192.15.2.5

C:\>
```

PC2

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

Wireless0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0004:9ADD:3D59
Link-local IPv6 Address.....: FE80::204:9AFF:FE00:3D59
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.10.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAIID.....: 11728
DHCPv6 Client DUID.....: 00-01-00-01-00-B3-73-B0-00-04-9A-DD-3D-59
DNS Servers.....: ::1
192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 00E0:8F85:1B46
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAIID.....: 11728
DHCPv6 Client DUID.....: 00-01-00-01-00-B3-73-B0-00-04-9A-DD-3D-59
DNS Servers.....: ::1
192.15.2.5

C:\>
```

PC3

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0000:0CB5:0933
Link-local IPv6 Address.....: FE80::200:CF7:FE00:933
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.103
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAIID.....: 11728
DHCPv6 Client DUID.....: 00-01-00-01-39-E4-AB-C2-00-00-0C-B5-09-33
DNS Servers.....: ::1
192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 00E0:8F85:1B46
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAIID.....: 11728
DHCPv6 Client DUID.....: 00-01-00-01-39-E4-AB-C2-00-00-0C-B5-09-33
DNS Servers.....: ::1
192.15.2.5

C:\>
```

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0050:0FCE:6C67
Link-local IPv6 Address....: FE80::250:FF:FECE:6C67
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.104
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                           192.168.1.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IID.....: 
DHCPv6 Client DUID.....: 00-01-00-01-4C-67-1C-24-00-50-0F-C6-0C-67
DNS Servers.....: ::
                           192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0001:C743:D6E4
Link-local IPv6 Address....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                           0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IID.....: 
DHCPv6 Client DUID.....: 00-01-00-01-4C-67-1C-24-00-50-0F-C6-0C-67
DNS Servers.....: ::
                           192.15.2.5

C:\>

```

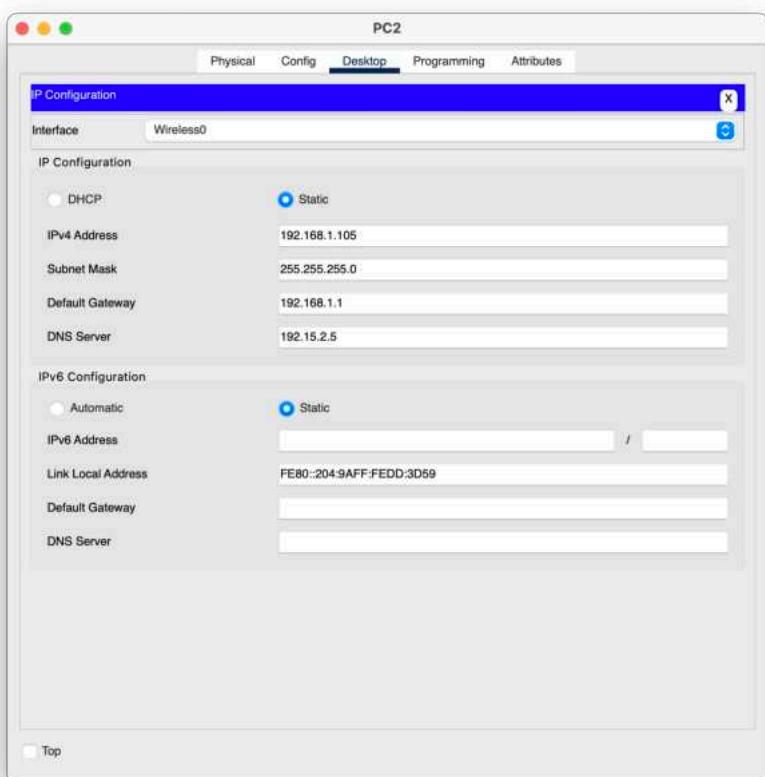
- Examine la configuración de dirección IP, máscara de subred y puerta de enlace predeterminada en cada PC. Asegúrese de registrar esta configuración IP para cada PC a fin de identificar si alguna de ellas está configurada incorrectamente.

De la información proporcionada por ipconfig, observamos que el PC2 tiene una configuración incorrecta. Su dirección IPv4 es 192.168.10.102, no pertenece a la red 192.168.1.0/24. Debería estar en la forma 192.168.1.x (donde x es un número único dentro del rango 2-254 que no esté en uso) para estar en la misma red que las demás PC y poder acceder a Internet.

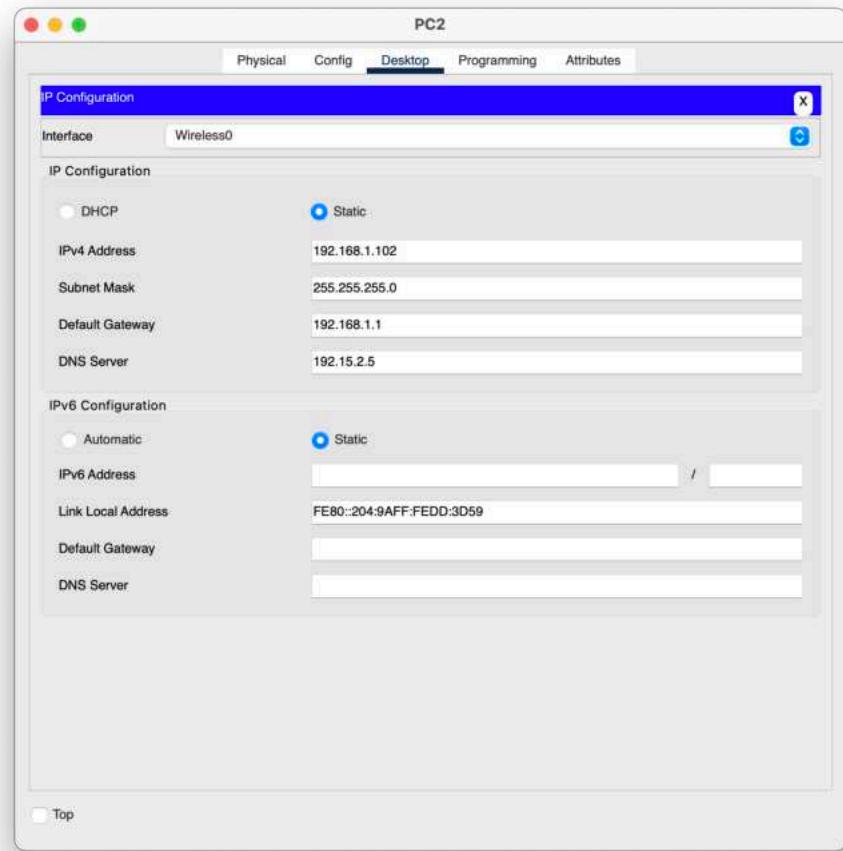
## Parte 2: Corregir configuraciones incorrectas

- Seleccione la PC que está configurada incorrectamente.
- Haga clic en la ficha **Desktop** (Escritorio) > **IP Configuration** (Configuración IP) para corregir la configuración.

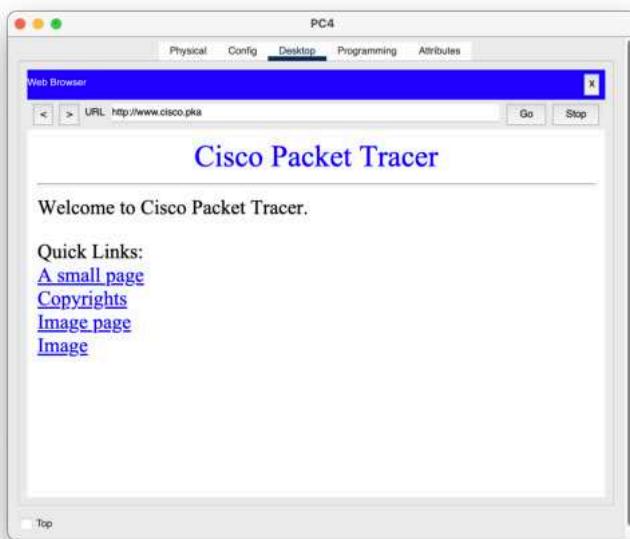
Cambiamos la IP por 192.168.1.105 y probamos la conectividad intentando acceder a la web.

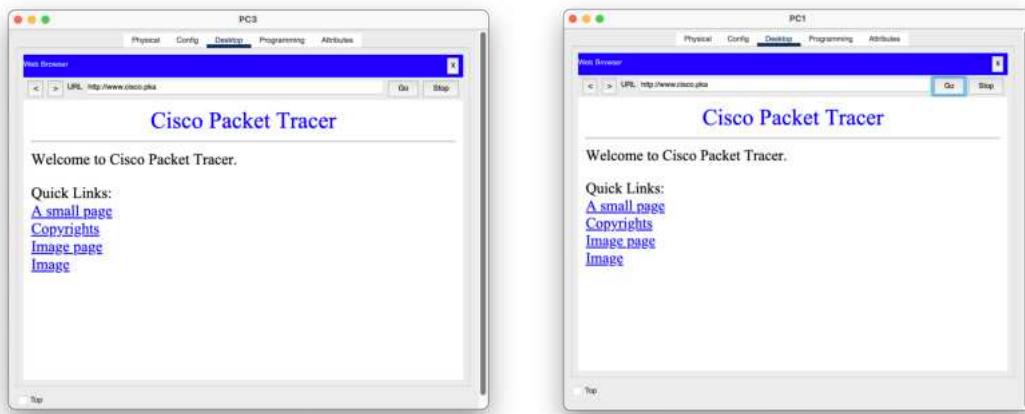


La IP que se ha elegido, el ejercicio no la acepta, a pesar de que hay conexión a internet. Por tanto, se ha vuelto a cambiar y ahora si ha resultado el ejercicio completo.

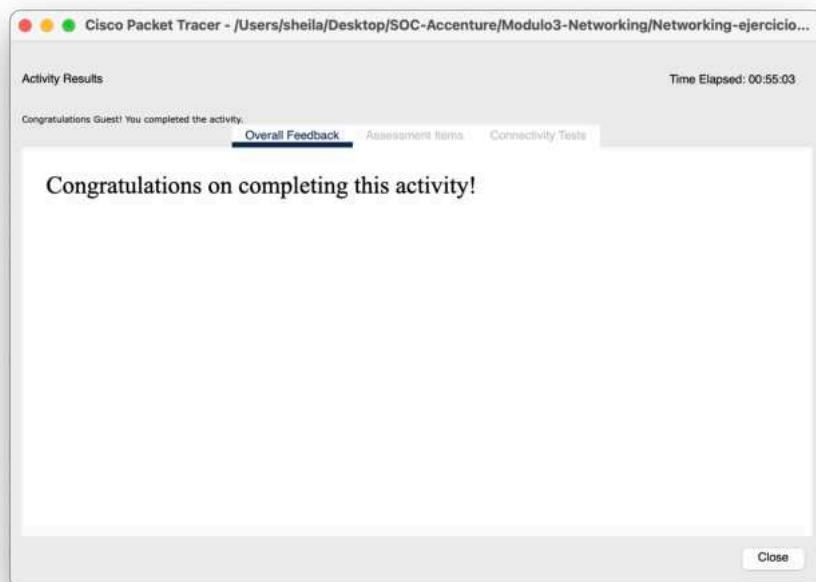


Comprobamos del mismo modo que los demás PC tienen conexión a internet y el problema está resuelto.





En esta ocasión el acceso a “Assessment Items” no está accesible como puede verse en la captura.



## Tarea 12: Usar el Comando ping (apartado 17.1.6. del curso)

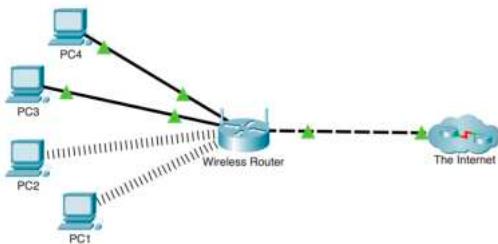
### **Packet Tracer: Usar el comando ping**

#### **Objetivos**

Usar el comando **ping** para identificar configuraciones incorrectas en una PC.

#### **Aspectos básicos/situación**

El dueño de una pequeña empresa descubre que algunos usuarios no pueden acceder a un sitio web. Todas las PC están configuradas con direcciones IP estáticas. Use el comando **ping** para identificar el problema.

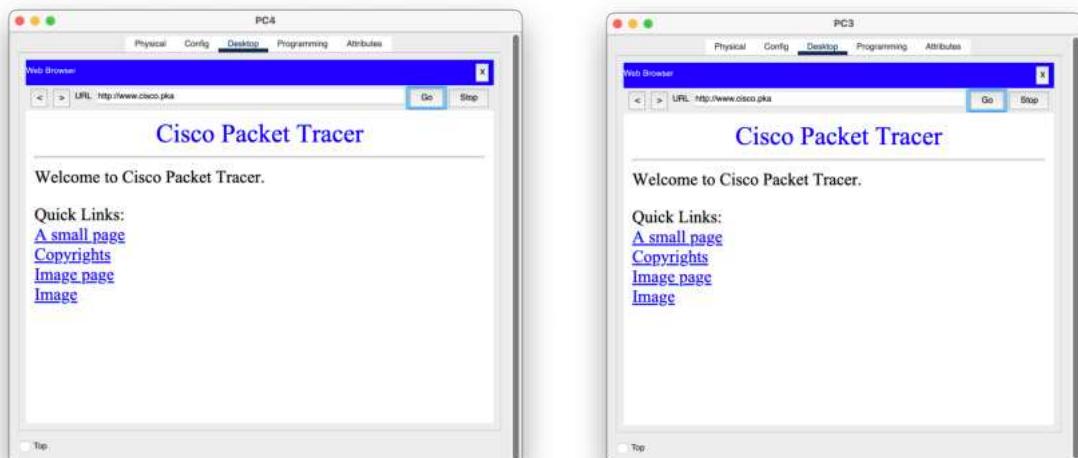


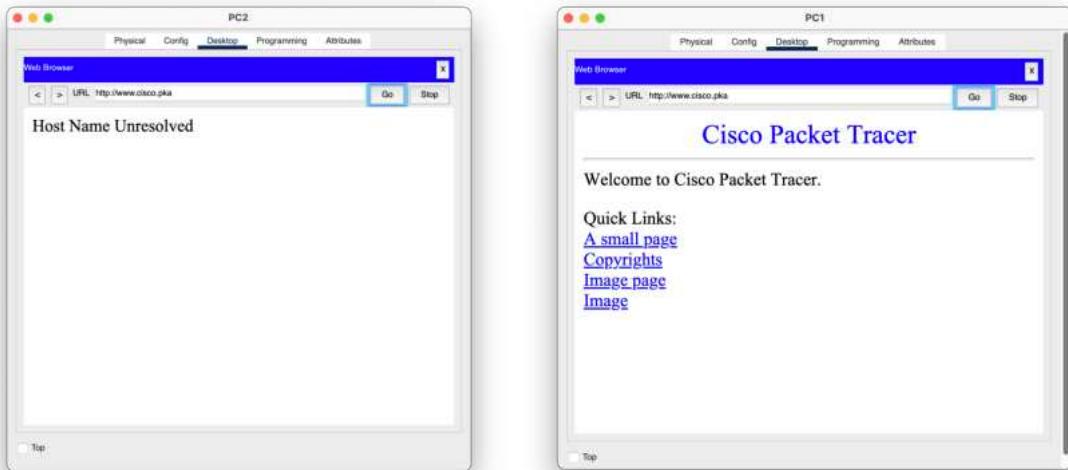
## Instrucciones

### Parte 1: Verificar la conectividad

Acceda a la ficha **Desktop** (Escritorio) > **Web Browser** (Navegador web) de cada PC e introduzca la URL **www.cisco.pka**. Identifique las PC que no se pueden conectar con el servidor Web.

**Nota:** Todos los dispositivos requieren un tiempo para realizar el proceso de arranque. Deje pasar hasta un minuto para recibir una respuesta de la Web.



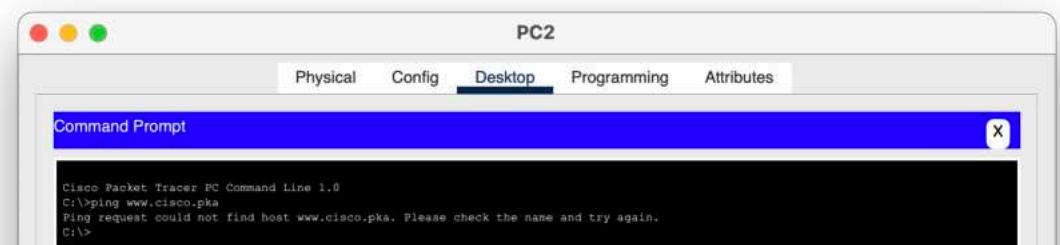


¿Cuáles PC tienen problemas para conectarse al servidor Web?

### PC2

#### Parte 2: Hacer ping al servidor web desde la PC con problemas de conectividad.

- En la PC, acceda a **Command Prompt** (Línea de comandos) desde la pestaña **Desktop** (Escritorio).
- Cuando se le solicite, ingrese **ping [www.cisco.pka](http://www.cisco.pka)**.



¿Obtuvo una respuesta al ping? ¿Qué dirección IP se muestra en la respuesta, en caso de existir alguna?

**No hubo respuesta. No se mostró ninguna dirección IP en el mensaje.**

#### Parte 3: Hacer ping al servidor web desde las PC configuradas correctamente.

- En la PC, acceda a **Command Prompt** (Línea de comandos) desde la pestaña **Desktop** (Escritorio).
- Cuando se le solicite, ingrese **ping [www.cisco.pka](http://www.cisco.pka)**.

**PC1**

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.cisco.pka

Pinging 192.15.2.10 with 32 bytes of data:
Reply from 192.15.2.10: bytes=32 time=11ms TTL=127
Reply from 192.15.2.10: bytes=32 time=28ms TTL=127
Reply from 192.15.2.10: bytes=32 time=27ms TTL=127
Reply from 192.15.2.10: bytes=32 time=23ms TTL=127

Ping statistics for 192.15.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 28ms, Average = 22ms

C:\>
```

**PC3**

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.cisco.pka

Pinging 192.15.2.10 with 32 bytes of data:
Reply from 192.15.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.15.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**PC4**

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.cisco.pka

Pinging 192.15.2.10 with 32 bytes of data:
Reply from 192.15.2.10: bytes=32 time<1ms TTL=127
Reply from 192.15.2.10: bytes=32 time<1ms TTL=127
Reply from 192.15.2.10: bytes=32 time=18ms TTL=127
Reply from 192.15.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.15.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>
```

¿El ping produjo una respuesta? ¿Qué dirección IP se devolvió, si la hay?

**La respuesta se devolvió con 192.15.2.10 como dirección IP para www.cisco.pka.**

#### **Parte 4: Hacer ping a la dirección IP del servidor web desde la PC con problemas de conectividad.**

- a. En la PC, acceda a **Command Prompt** (Línea de comandos) desde la pestaña **Desktop** (Escritorio).
- b. Intente llegar a la dirección IP del servidor web con el comando **ping**.

```
Cisco Packet Tracer PC Command Line 1.0
C:\ping www.cisco.pka
Ping request could not find host www.cisco.pka. Please check the name and try again.
C:\ping 192.15.2.10

Pinging 192.15.2.10 with 32 bytes of data:
Reply from 192.15.2.10: bytes=32 time=40ms TTL=127
Reply from 192.15.2.10: bytes=32 time=29ms TTL=127
Reply from 192.15.2.10: bytes=32 time=27ms TTL=127
Reply from 192.15.2.10: bytes=32 time=26ms TTL=127

Ping statistics for 192.15.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 40ms, Average = 30ms

C:\>
```

¿El **ping** produjo una respuesta? De ser así, entonces la PC puede comunicarse con el servidor Web a través de la dirección IP, pero no a través del nombre de dominio. Esto puede indicar un problema en la configuración del servidor DNS en la PC.

#### **Parte 5: Comparar la información del servidor DNS en las PC.**

- a. Acceda al **Command Prompt** (Línea de comandos) de las PC sin ningún problema.
- b. Con el comando **ipconfig /all**, examine la configuración del servidor DNS en las PC sin ningún problema.

PC1

```
C:\>ipconfig /all

Wireless0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0000.974E.7EDA
Link-local IPv6 Address....: FE80::2D0:97FF:FE4E:7EDA
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.101
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
DHCP Servers.....: 192.168.1.1
DHCPv6 IAID.....: 23360
DHCPv6 Client DUID.....: 00-01-00-01-E3-BA-E3-98-00-00-97-4E-7E-DA
DNS Servers.....: ::1
                                         192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0000.5864.0DC0
Link-local IPv6 Address....: ::1
IPv6 Address.....: ::0.0.0
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
                                         0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....: 23360
DHCPv6 Client DUID.....: 00-01-00-01-E3-BA-E3-98-00-00-97-4E-7E-DA
DNS Servers.....: ::1
                                         192.15.2.5

c:\>
```

Top

PC3

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0000.0CB5.0933
Link-local IPv6 Address....: FE80::200:CF:FEB5:933
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.103
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
                                         192.168.1.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....: 23360
DHCPv6 Client DUID.....: 00-01-00-01-97-79-52-BB-00-00-0C-B5-09-33
DNS Servers.....: ::1
                                         192.15.2.5

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0001.6498.0289
Link-local IPv6 Address....: ::1
```

Top

```

C:\>ipconfig /all

FastEthernet0 Connection:(default port)
  Connection-specific DNS Suffix...:
  Physical Address.....: 0050.0FC6.0C67
  Link-local IPv6 Address.....: FE80::250:FF:FE6C:6C67
  IPv6 Address.....: ::1
  IPv4 Address.....: 192.168.1.104
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: 192.168.1.1
  DHCP Servers.....: 0.0.0.0
  DHCPv6 IAID.....: 
  DHCPv6 Client DUID.....: 00-01-00-01-C5-35-19-58-00-50-0F-C6-0C-67
  DNS Servers.....: ::1
                                192.15.2.5

Bluetooth Connection:
  Connection-specific DNS Suffix...:
  Physical Address.....: 0004.9A57.598D
  Link-local IPv6 Address.....: ::

C:\>

```

- c. Acceda al **Command Prompt** (Línea de comandos) de las PC con problemas de conectividad.
- d. Con el comando **ipconfig /all**, examine la configuración del servidor DNS en las PC con problemas de conectividad. ¿Coinciden las dos configuraciones?

```

C:\>ipconfig /all

Wireless0 Connection:(default port)
  Connection-specific DNS Suffix...:
  Physical Address.....: 000A.416D.E046
  Link-local IPv6 Address.....: FE80::20A:41FF:FE6D:E046
  IPv6 Address.....: ::1
  IPv4 Address.....: 192.168.1.102
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: 192.168.1.1
  DHCP Servers.....: 192.168.1.1
  DHCPv6 IAID.....: 23377
  DHCPv6 Client DUID.....: 00-01-00-01-43-D0-D7-DE-00-0A-41-6D-E0-46
  DNS Servers.....: ::1
                                191.15.2.5

Bluetooth Connection:
  Connection-specific DNS Suffix...:
  Physical Address.....: 0000.97B4.9CAA
  Link-local IPv6 Address.....: ::1
  IPv6 Address.....: ::1
  IPv4 Address.....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: 0.0.0.0
  DHCP Servers.....: 0.0.0.0
  DHCPv6 IAID.....: 23377
  DHCPv6 Client DUID.....: 00-01-00-01-43-D0-D7-DE-00-0A-41-6D-E0-46
  DNS Servers.....: ::1
                                191.15.2.5

C:\>

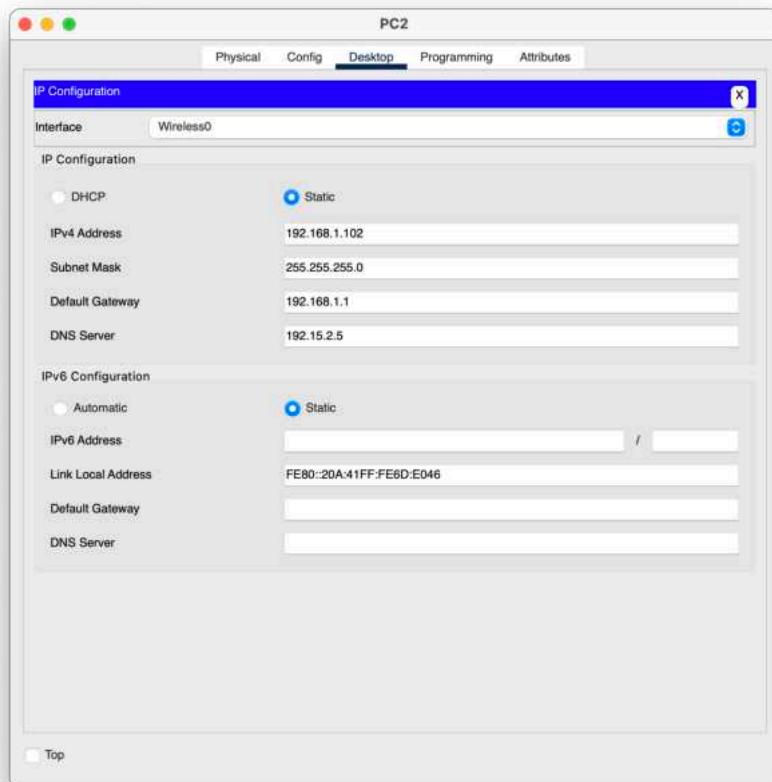
```

No coinciden, la DNS del PC2 es distinta, 191.15.2.5 a diferencia de las demás que es 192.15.2.5.

## Parte 6: Realizar los cambios de configuración necesarios en las PC.

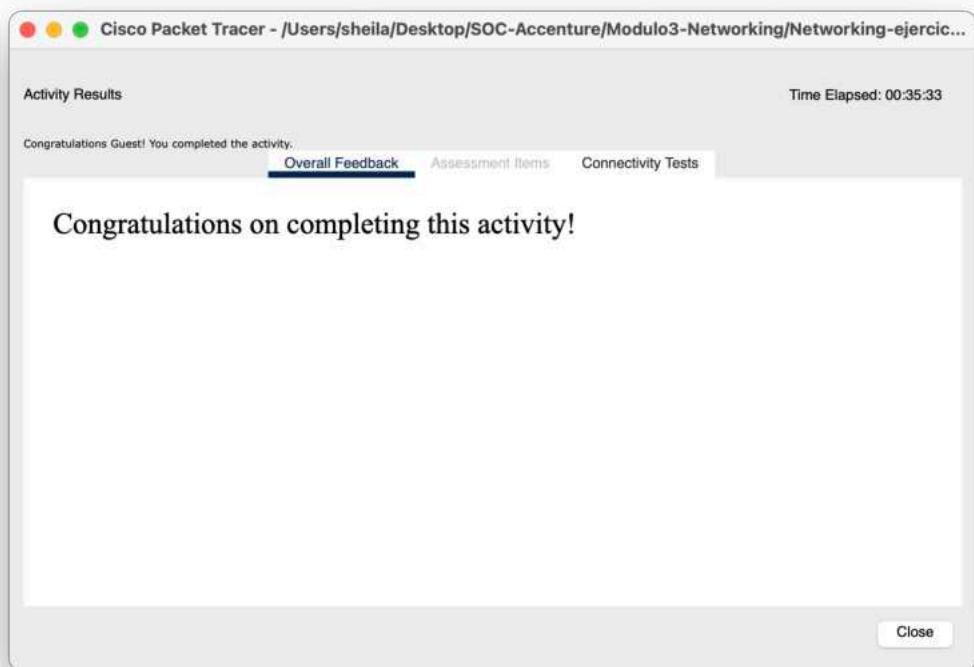
- Navegue a la pestaña **Desktop** (Escritorio) de las PC con problemas y haga los cambios de configuración necesarios en **IP Configuration** (Configuración IP).

Cambiamos la DNS.



- Mediante el **Web Browser** (Navegador web) dentro de la ficha **Desktop** (Escritorio), conéctese con **www.cisco.pka** para verificar que los cambios de configuración hayan resuelto el problema.





De nuevo el acceso a Assessment Items no es posible.