Diplomado De Profundización Cisco
(Diseño E Implementación De Soluciones Integradas Lan / Wan)

Director

Juan Carlos Vesga
Ingeniero Telecomunicaciones

Sabemos Muy Poco, Y Sin Embargo Es Sorprendente Que Sepamos Tanto, Y Es Todavía Más Sorprendente Que Tan Poco Conocimiento Nos Dé Tanto Poder. Bertrand Russell

Universidad Nacional Abierta Y A Distancia (Unad)
Facultad De Ciencias Básicas, Tecnología E Ingeniería
Curso: 203092A_363
Bogotá
2017

Diplomado De Profundización Cisco
(Diseño E Implementación De Soluciones Integradas Lan / Wan)

Integrante:

Iván Darío Medrano

Grupo: 203092_39

Sabemos Muy Poco, Y Sin Embargo Es Sorprendente Que Sepamos Tanto, Y Es Todavía Más Sorprendente Que Tan Poco Conocimiento Nos Dé Tanto Poder. Bertrand Russell

Universidad Nacional Abierta Y A Distancia (Unad)
Facultad De Ciencias Básicas, Tecnología E Ingeniería
Curso: 203092A_363
Bogotá
2017

Tabla de Contenido

Contenido

GLOSARIO

Switch: Es un dispositivo para diseñar y resolver errores de rendimiento en la red, maneja el mejoramiento de ancho de banda.

LAN: Red de área local, se conectan múltiples dispositivos, la conexión es por cable o por ondas. Los equipos conectados en la red LAN son nodos y se pueden comunicar entre sí.

WAN: Red de área extensa, está distribuida geográficamente para intercomunicar múltiples redes de área local.

IP: Identifica la manera lógica de la interfaz de una red, lo usan los equipos de cómputo, impresoras, tabletas, celulares entre otros.

DSL: Es una línea de abonado digital se usa en servicios de telecomunicaciones distribuidos, mediante el cableado cobre, como la línea telefónica convencional.

Resumen:

El presente trabajo fue desarrollado para adquirir conocimientos y habilidades en el diplomado de profundización cisco. El primer módulo vamos a implementar una red de computadores, para analizar el funcionamiento de una red y sus diferentes funcionalidades, se trabaja dos tipos de redes (LAN, WAN), adicional se explica cómo se realiza la configuración de la placa, componentes físicos y las aplicaciones para detección de errores en la red. Esto se realiza mediante el programa CISCO PACKET TRACER.

Introducción

Una red de computadoras tiene dos o más dispositivos vinculados con el propósito de compartir información y recursos. Este módulo proporciona al alumno una descripción general respecto a cómo funcionan las redes y a cómo comparten servicios. Los tipos de redes que se detallan en este módulo incluyen peer-to-peer, cliente/servidor, red de área local (LAN) y red de área amplia (WAN). Además, se explica la diferencia entre una red por circuitos conmutados y por paquetes conmutados, así como la topología o la forma en la cual se configura la red. El alumno aprenderá cómo agregar la placa de interfaz de red, los componentes físicos de una red, y las importantes utilidades que se utilizan en la detección de problemas.

Objetivos

Objetivo General

La construcción del trabajo a través de redes, con un enfoque ganar en el que las relaciones tienen una óptica de largo plazo.

Objetivo Especifico

- Instalar y configurar switches y routers de Cisco en interconexiones de redes multiprotocolo que utilizan interfaces LAN y WAN
- Proporcionar servicio de Nivel 1 de solución de problemas
- Mejorar el rendimiento y la seguridad de la red
- Llevar a cabo tareas de nivel de entrada en la planificación, diseño, instalación, operación y solución de problemas de Redes Ethernet TCP / IP.

TRABAJO COLABORATIVO FASE 1

1.2.4.4 Packet Tracer - Representing The Network Instructions Ig

Parte 1: Descripción General Del Programa Packet Tracer

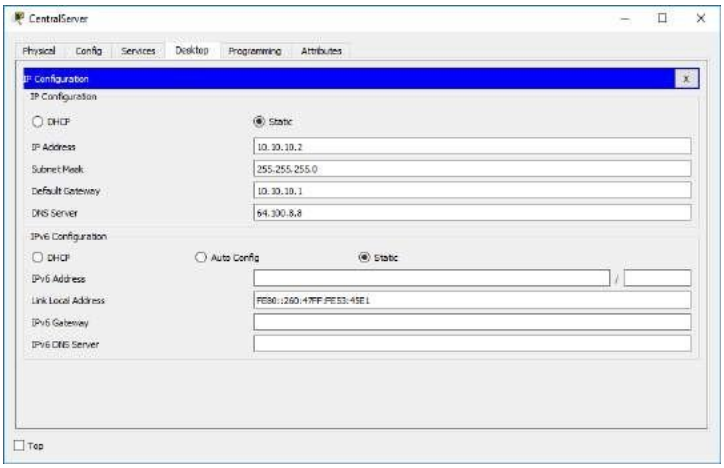
Paso 1C

Busque el tutorial "Configuring Devices Using the Desktop Tab" (Configuración de dispositivos mediante la ficha Desktop [Escritorio]). Mire la primera parte para responder la siguiente pregunta: ¿Qué información se puede configurar en la ventana IP Configuration (Configuración IP)? Puede elegir DHCP o Static (Estático) y configurar la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS.

Respuesta:

En esta ventana se puede configurar las interfaces de los dispositivos como los son equipos de escritorio, portátiles, tablets etc, tanto IPV4 e IPV6 por DHCP o de manera estática.

- IP ADDRESS.
- SUBNET MESK.
- DEFAULT GATEWAY.
- DNS SERVER.



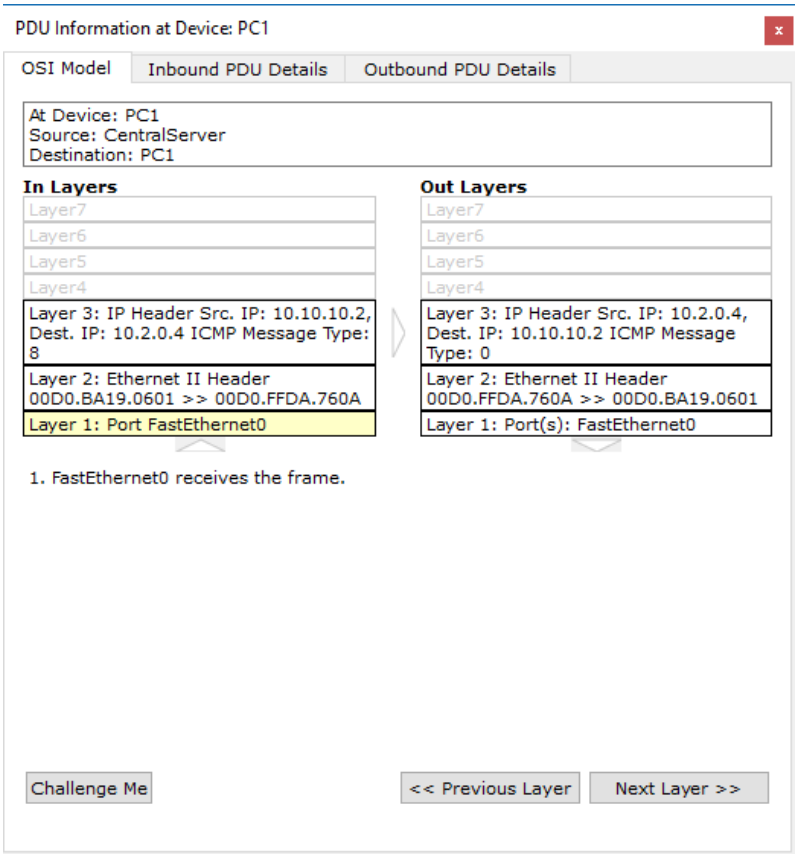
Paso 2F

f. En la topología de la red a la izquierda, haga clic en cualquiera de los sobres en un dispositivo intermediario e investigue qué hay dentro. En el curso de sus estudios de CCNA, aprenderá el significado la mayor parte del contenido de estos sobres. Por el momento, intente responder las siguientes preguntas:

- En la ficha OSI Model (Modelo OSI), ¿cuántas In Layers (Capas de entrada) y Out Layers (Capas de salida) tienen información? Las respuestas varían según la capa del dispositivo.

Respuesta:

In Layers: Tiene las Capas 1,2,3 de Entrada.
Out Layers: Tiene las Capas 1,2,3 de Salida.



- En las fichas Inbound PDU Details (Detalles de la PDU de entrada) y Outbound PDU Details (Detalles de la PDU de salida), ¿cuáles son los encabezados de las secciones principales? Las respuestas varían, pero algunas respuestas probables son Ethernet 802.3, LLC, STP BPDU, etcétera.

Inbound Pdu Details

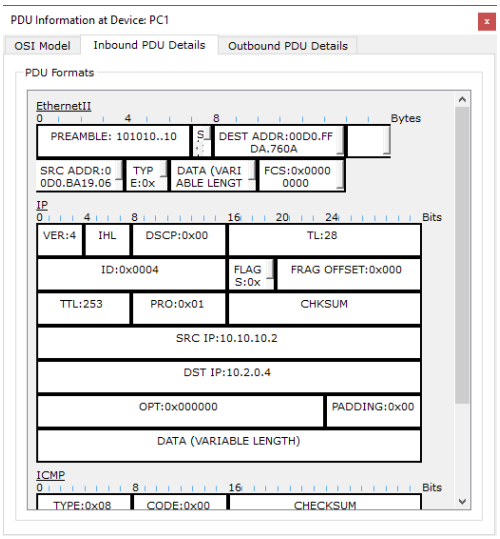
- Ethernet II
- IP
- ICMP
- Variable Size PDU

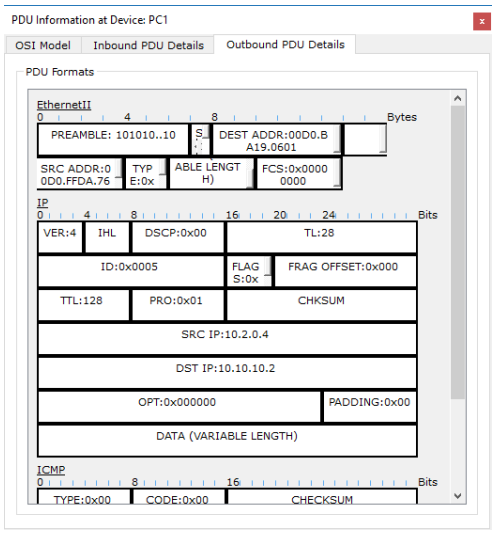
Outbound Pdu Details

- Ethernet II
- IP

- ICMP
- Variable Size PDU

- Alterne entre las fichas Inbound PDU Details y Outbound PDU Details. ¿Observa cambios en la información? Si es así, ¿qué es lo que cambia? Las respuestas varían, pero las direcciones de origen o destino de la capa de enlace de datos cambian. También pueden cambiar otros datos, según el paquete que haya abierto el estudiante.





Respuesta:

Las cabeceras son las mismas, pero dentro de cada cabecera principal cambia la información como los son las direcciones de origen y de destino.

Parte 2: Exploración de LAN, WAN e Internet

Paso 1: Identificar los componentes comunes de una red según se los representa en Packet Tracer

a. Enumere las categorías de los dispositivos intermediarios.

Respuesta:

- Routers.
- Switches.
- Hubs.
- Dispositivos inalámbricos.
- Emulación de WAN.
- Seguridad.

b. Sin ingresar en la nube de Internet o de intranet, ¿cuántos íconos de la topología representan dispositivos terminales (solo una conexión conduce a ellos)?

Respuesta:

c. Sin contar las dos nubes, ¿cuántos íconos de la topología representan dispositivos intermediarios (varias conexiones conducen a ellos)?
Respuesta:

d. ¿Cuántos de esos dispositivos intermediarios son routers? Nota: el dispositivo Linksys es un router.
Respuesta:

e. ¿Cuántos dispositivos finales no son computadoras de escritorio?
Respuesta:

f. ¿Cuántos tipos diferentes de conexiones de medios se utilizan en esta topología de red?
Respuesta:

g. ¿Por qué no hay un ícono de conexión para la tecnología inalámbrica en la categoría Connections?
Respuesta: El técnico de red no realiza las conexiones inalámbricas físicamente. En cambio, los dispositivos se encargan de negociar la conexión y de activar el enlace físico.

Paso 2: Explicar La Finalidad De Los Dispositivos

a. En Packet Tracer, el dispositivo Server-PT puede funcionar como servidor. Las computadoras de escritorio y portátiles no pueden funcionar como servidores. ¿Esto sucede en el mundo real?
Respuesta: No. Según lo que estudió hasta ahora, explique el modelo cliente-servidor. En las redes modernas, un host puede actuar como un cliente, un servidor o ambos. El software instalado en el host determina qué función tiene en la red. Los servidores son hosts que tienen instalado software que les permite proporcionar información y servicios, como correo electrónico o páginas Web, a otros hosts en la red.

Los clientes son hosts que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida. Sin embargo, un cliente también se puede configurar como servidor simplemente al instalar software de servidor.

b. Enumere, al menos, dos funciones de los dispositivos intermediarios.

Respuesta: Regenerar y retransmitir señales de datos; mantener información sobre qué rutas existen a través de la red y de la internetwork; notificar a otros dispositivos de los errores y las fallas de comunicación; direccionar datos a través de rutas

Alternativas cuando hay una falla de enlace; clasificar y direccionar mensajes según las prioridades de QoS; permitir o denegar el flujo de datos según la configuración de seguridad.

c. Enumere, al menos, dos criterios para elegir un tipo de medio de red.

Respuesta: La distancia en la cual el medio puede transportar exitosamente una señal. El ambiente en el cual se instalará el medio La cantidad de datos y la velocidad a la que se deben transmitir El costo de los medios y de la instalación.

Paso 3: Comparar Redes Lan Y Wan

a. Explique la diferencia entre una LAN y una WAN, y dé ejemplos de cada una.

Respuesta:

- Las redes LAN proporcionan acceso a los usuarios finales en una pequeña área geográfica. Una oficina doméstica o un campus son ejemplos de redes LAN.
- Las redes WAN proporcionan acceso a los usuarios en un área geográfica extensa a través de grandes distancias, que pueden ir de pocos a miles de kilómetros. Una red de área metropolitana e Internet son ejemplos de redes WAN. La intranet de una compañía también puede conectar varios sitios remotos mediante una WAN.

b. ¿Cuántas WAN ve en la red de Packet Tracer?

Respuesta:

Hay dos:

- La WAN de Internet
- La de intranet.

c. ¿Cuántas LAN ve?

Respuesta:

Hay tres, que se identifican fácilmente porque cada una tiene un límite y una etiqueta.

d. En esta red de Packet Tracer, Internet está simplificada en gran medida y no representa ni la estructura ni la forma de Internet propiamente dicha. Describa Internet brevemente. Internet se utiliza sobre todo cuando necesitamos comunicarnos con un recurso en otra red. Internet es una malla global de redes interconectadas (internetworks).

d. ¿Cuáles son algunas de las formas más comunes que utiliza un usuario doméstico para conectarse a Internet?

Respuesta:

- Cable
- DSL
- Dial-Up
- Datos móviles y satélites.

e. ¿Cuáles son algunas de las formas más comunes que utilizan las empresas para conectarse a Internet en su área?

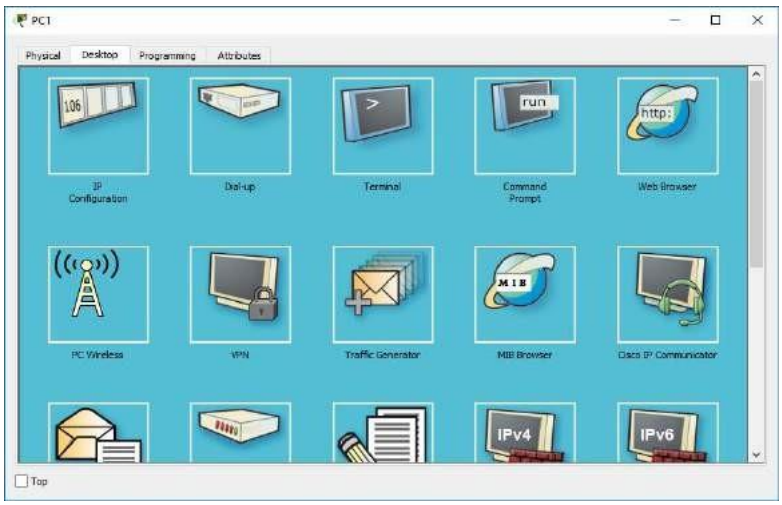
Respuesta:

- Línea arrendada dedicada
- Metro-E
- DSL
- Cable
- Satélite.

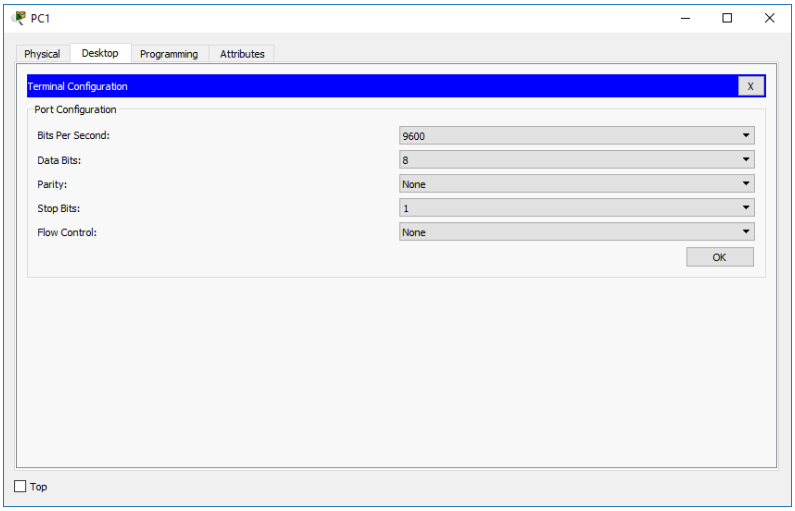
2.1.4.8 Packet Tracer - Navigating the IOS Instructions IG

Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda

a. Haga clic en PC1 y después en la ficha Desktop (Escritorio).



b. Haga clic en **OK** (Aceptar).



Paso 3: Examine la ayuda de IOS.

a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina Modo EXEC del usuario y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

   S1> ?

b. ¿Qué comando comienza con la letra "C"? conectar.

   S1>c?

   Connect

c. En la petición de entrada, escriba t, seguido de un signo de interrogación (?).

   S1> t?

d. ¿Qué comandos se muestran? telnet terminal traceroute

   S1>t?

   telnet terminal traceroute

e. En la petición de entrada, escriba te, seguido de un signo de interrogación (?).

   S1> te?

d. ¿Qué comandos se muestran? telnet terminal

   S1>te?

   telnet terminal

Este tipo de ayuda se conoce como ayuda contextual, ya que proporciona más información a medida que se amplían los comandos.

Parte 2: Exploración de los modos EXEC

En la parte 2 de esta actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Ingrese al modo EXEC privilegiado.

a. En la petición de entrada, escriba el signo de interrogación (?).
S1> ?

```
S1>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
S1>
```

b. ¿Qué información de la que se muestra describe el comando enable?

Respuesta: Activa los comandos privilegiados.

c. Escriba en y presione la tecla Tabulación.

S1> en<Tab>

d. ¿Qué se muestra después de presionar la tecla Tabulación? Enable

Respuesta: Esto se denomina completar un comando o completar la tabulación. Cuando se escribe parte de un comando, la tecla Tabulación se puede utilizar para completar el comando parcial. Si los caracteres que se escriben son suficientes para formar un comando único, como en el caso del comando enable, se muestra la parte restante.

e. ¿Qué ocurriría si escribiera te<Tabulación> en la petición de entrada?

Respuesta: "te" no proporciona suficientes caracteres para formar un comando único; por lo tanto, los caracteres continuarán apareciendo, y se le solicitará al usuario que introduzca más caracteres para formar el comando único. Hay más de un comando que comienza con las letras "te".

f. Introduzca el comando enable y presione tecla Entrar. ¿En qué cambia la petición de entrada?

Respuesta: Cambia de S1> a S1#, que indica el modo EXEC privilegiado.

g. Cuando se le solicite, escriba el signo de interrogación (?).

S1# ? Antes había un comando que comenzaba con la letra "C" en el modo EXEC del usuario. ¿Cuántos comandos se muestran ahora que está activo el modo EXEC privilegiado? (Sugerencia: ¿puede escribir c? para que aparezcan solo los comandos que comienzan con la letra "C").

Respuesta: S1#c?
Clear clock configure connect copy

Paso 2: Ingresar en el modo de configuración global

a. Cuando se está en el modo EXEC privilegiado, uno de los comandos que comienzan con la letra "C" es configure. Escriba el comando completo o la cantidad de caracteres suficiente para formar el comando único; presione la tecla <Tabulación> para emitir el comando y, a continuación, la tecla <Entrar>. S1# configure

b. ¿Cuál es el mensaje que se muestra?

Respuesta: Configuring from terminal, memory, or network [terminal]? (Configurando desde terminal, memoria o red [terminal]?)

c. Presione la tecla <Entrar> para aceptar el parámetro predeterminado [terminal] entre corchetes. ¿En qué cambia la petición de entrada?

Respuesta: S1(config)#

Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock

a. Utilice el comando clock para explorar en más detalle la ayuda y la sintaxis de comandos. Escriba show clock en la petición de entrada de EXEC privilegiado.

S1# show clock

b. ¿**Qué información aparece en pantalla? ¿Cuál es el año que se muestra?**

Respuesta: UTC Mon Mar 1 1993 (UTC lun 1 de marzo de 1993), precedido por las horas, los minutos y segundos desde que el dispositivo se inició. El año es 1993.

c. Utilice la ayuda contextual y el comando clock para establecer la hora del switch en la hora actual. Introduzca el comando clock y presione tecla Entrar.

S1# clock<ENTER>

d. **¿Qué información aparece en pantalla?**

Respuesta: % Incomplete command.

e. El IOS devuelve el mensaje % Incomplete command (% comando incompleto), que indica que el comando clock necesita otros parámetros. Cuando se necesita más información, se puede proporcionar ayuda escribiendo un espacio después del comando y el signo de interrogación (?). S1# clock ?

f. **¿Qué información aparece en pantalla?**

Respuesta: set Configura la hora y la fecha

g. Configure el reloj con el comando clock set. Continúe utilizando este comando paso por paso. S1# clock set ?

h. **¿Qué información se solicita? hh:mm:ss Hora actual ¿Qué información se habría mostrado si solo se hubiera ingresado el comando clock set y no se hubiera solicitado ayuda con el signo de interrogación?**

Respuesta: % Incomplete command

Paso 2: Explorar los mensajes adicionales del comando

a. Emita el siguiente comando y registre los mensajes: S1# cl ¿Qué información se devolvió?

Respuesta: % Ambiguous command: "cl" S1# clock

b. ¿**Qué información se devolvió?**

Respuesta: % Incomplete command. S1# clock set 25:00:00

c. ¿Qué información se devolvió?

Respuesta: S1#clock set 25:00:00 ^% Invalid input detected at '^' marker. S1# clock set 15:00:00 32

d. ¿Qué información se devolvió?

Respuesta: S1#clock set 15:00:00 32^% Invalid input detected at '^' marker.

3.2.4.6 Packet Tracer - Investigating the TCP-IP and OSI Models in Action Instructions IG

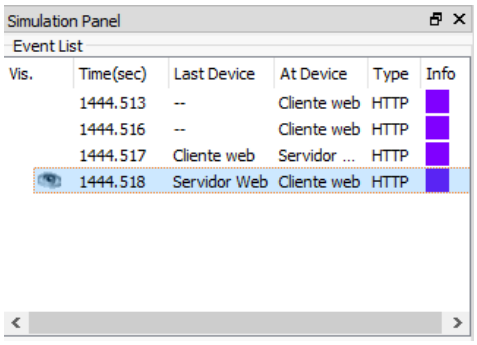
Parte 1: Examinar el tráfico Web HTTP

Paso 2: Genere tráfico web (HTTP).

El panel de simulación actualmente está vacío. En la parte superior de Event List (Lista de eventos) dentro del panel de simulación, se indican seis columnas. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna Info (Información) se utiliza para examinar el contenido de un evento determinado.

Nota: el servidor Web y el cliente Web se muestran en el panel de la izquierda. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha cuando aparece la flecha de dos puntas.

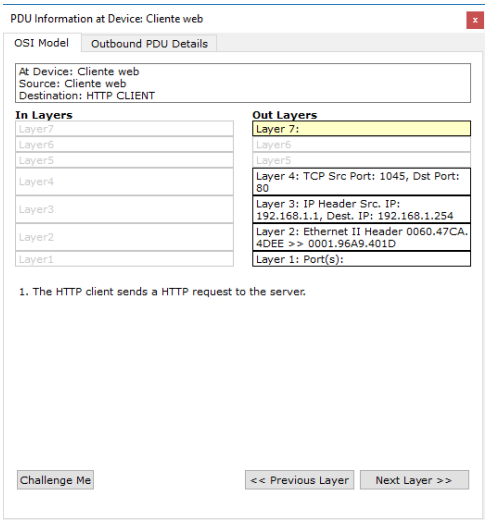
d. Haga clic en Capture/Forward cuatro veces. Debe haber cuatro eventos en la lista de eventos.



Observe la página del explorador Web del cliente Web. ¿Cambió algo? El servidor Web devolvió la página Web.

Paso 3: Explorar el contenido del paquete HTTP

b. Asegúrese de que esté seleccionada la ficha OSI Model. En la columna Out Layers (Capas de salida), asegúrese de que el cuadro Layer 7 (Capa 7) esté resaltado.



¿Cuál es el texto que se muestra junto a la etiqueta Layer 7?

Respuesta: HTTP

¿Qué información se indica en los pasos numerados directamente debajo de los cuadros In Layers (Capas de entrada) y Out Layers (Capas de salida)?

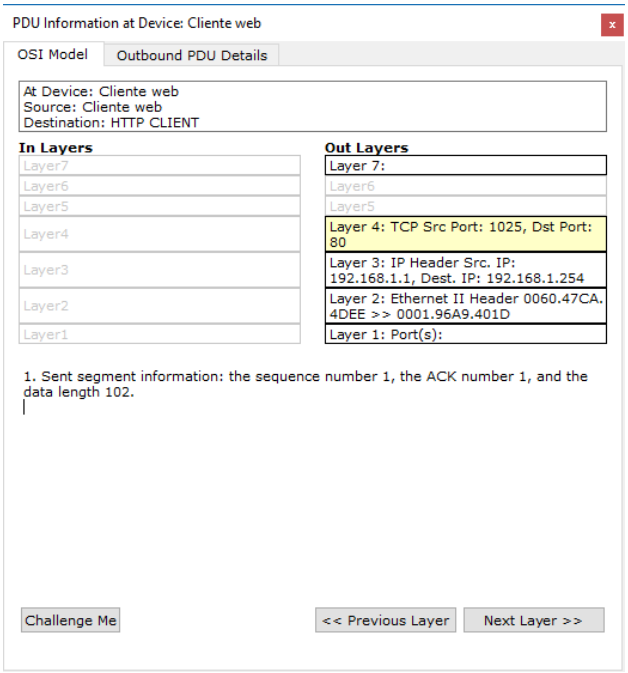
Respuesta:

"1. The HTTP client sends a HTTP request to the server." ("El cliente HTTP envía una solicitud de HTTP al servidor").

c. Haga clic en Next Layer (Capa siguiente). Layer 4 (Capa 4) debe estar resaltado. ¿Cuál es el valor de Dst Port (Puerto de dest?)?

Respuesta:

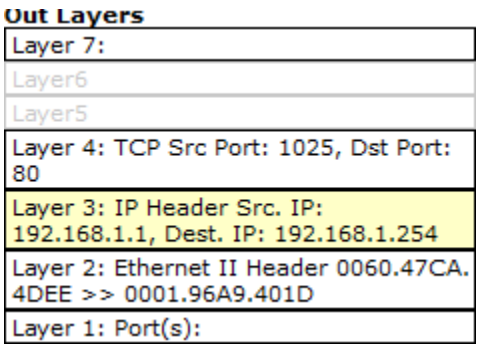
80



d. Haga clic en Next Layer (Capa siguiente). Layer 3 (Capa 3) debe estar resaltado. ¿Cuál es valor de Dest. IP (IP de dest.)?

Respuesta:

192.168.1.254

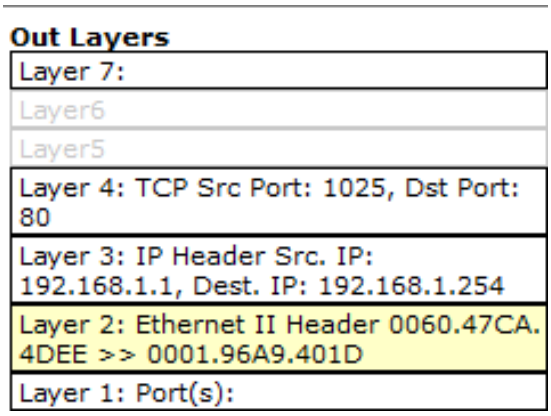


e. Haga clic en Next Layer (Capa siguiente). ¿Qué información se muestra en esta capa?

Respuesta:

El encabezado

Ethernet II de capa 2 y las direcciones MAC de entrada y salida.



f. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente).

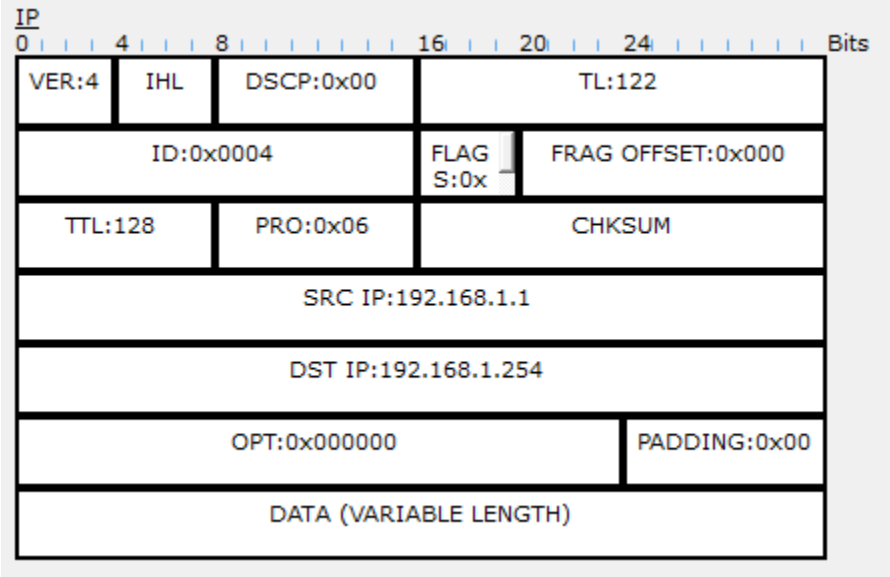
La información que se indica debajo de PDU Details (Detalles de PDU) refleja las capas dentro del modelo TCP/IP.

Nota: la información que se indica en la sección Ethernet II proporciona información aun más detallada que la que se indica en Layer 2 (Capa 2) en la ficha OSI Model. Outbound PDU Details (Detalles de PDU saliente) proporciona información más descriptiva y detallada. Los valores de DEST MAC (MAC DE DEST.) y de SRC MAC (MAC DE ORIGEN) en la sección Ethernet II de PDU Details (Detalles de PDU) aparecen en la ficha OSI Model, en Layer 2, pero no se los identifica como tales.

¿Cuál es la información frecuente que se indica en la sección IP de PDU Details comparada con la información que se indica en la ficha OSI Model? ¿Con qué capa se relaciona?

Respuesta:

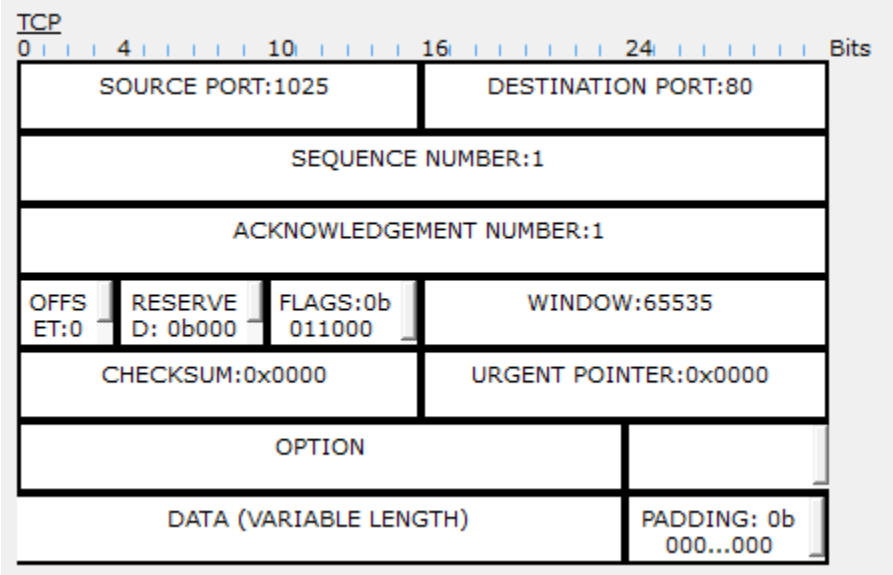
SRC IP (IP DE ORIG.) y DST IP (IP DE DEST.) en la capa 3



¿Cuál es la información frecuente que se indica en la sección TCP de PDU Details comparada con la información que se indica en la ficha OSI Model, y con qué capa se relaciona?

Respuesta:

SRC PORT (PUERTO DE ORIG.) y DEST PORT (PUERTO DE DEST.) en la capa 4



¿Cuál es el host que se indica en la sección HTTP de PDU Details? ¿Con qué capa se relacionaría esta información en la ficha OSI Model?

Respuesta:

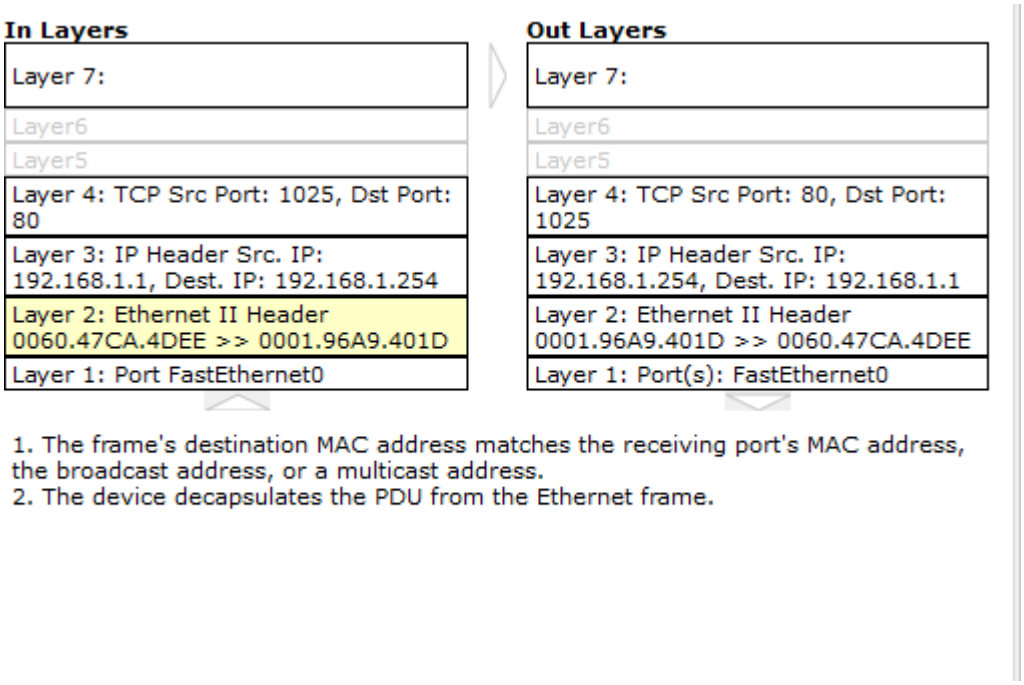
www.osi.local, capa 7.

h. Avance al siguiente cuadro Info (Información) de HTTP dentro de la lista de eventos y haga clic en el cuadro coloreado. Esta ventana contiene las columnas In Layers (Capas de entrada) y Out Layers (Capas de salida). Observe la dirección de la flecha que está

directamente debajo de la columna In Layers; esta apunta hacia arriba, lo que indica la dirección en la que se transfiere la información. Desplácese por estas capas y tome nota de los elementos vistos anteriormente. En la parte superior de la columna, la flecha apunta hacia la derecha. Esto indica que el servidor ahora envía la información de regreso al cliente.

Compare la información que se muestra en la columna In Layers con la de la columna Out Layers:

¿cuáles son las diferencias principales?
Respuesta:
Se intercambiaron los puertos de origen y destino, las direcciones IP de origen y destino, y las direcciones MAC.



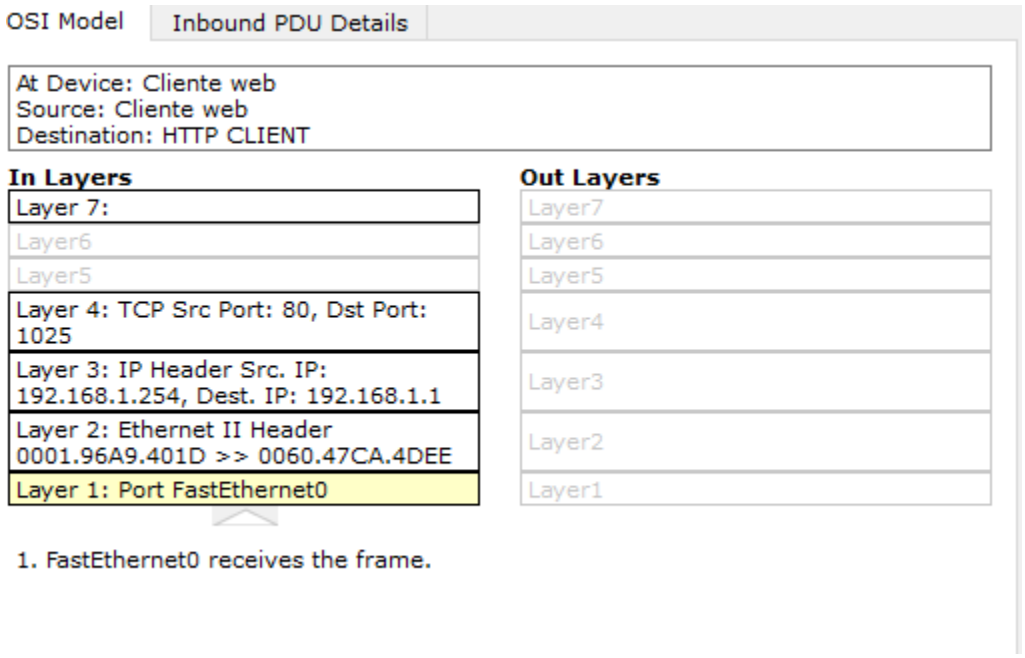
i. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente). Desplácese hasta la sección HTTP.

¿Cuál es la primera línea del mensaje HTTP que se muestra?
Respuesta:
HTTP/1.1 200 OK: esto significa que la solicitud se realizó correctamente y que se entregó la página desde el servidor.

j. Haga clic en el último cuadro coloreado de la columna Info. ¿Cuántas fichas se muestran con este evento y por qué?

Respuesta:

Solo dos, una para OSI Model y una para Inbound PDU Details, ya que este es el dispositivo receptor.



Parte 2: Mostrar Elementos De La Suite De Protocolos TCP/IP

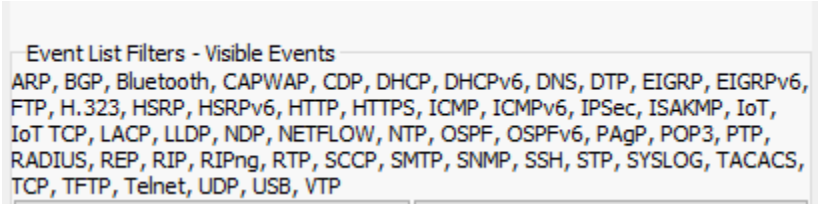
Paso 1: Ver Eventos Adicionales

b. En la sección Event List Filters > Visible Events (Filtros de lista de eventos > Eventos visibles), haga clic en Show All (Mostrar todo).

¿Qué tipos de eventos adicionales se muestran? Según si se produjo alguna comunicación antes de iniciar la simulación original, ahora debe haber entradas para ARP, DNS, TCP y HTTP. Es posible que no se puedan mostrar las entradas de ARP, según lo que haya hecho el estudiante antes de pasar al modo de simulación. Si la actividad se inicia desde cero, se muestran todas esas.

Respuesta:

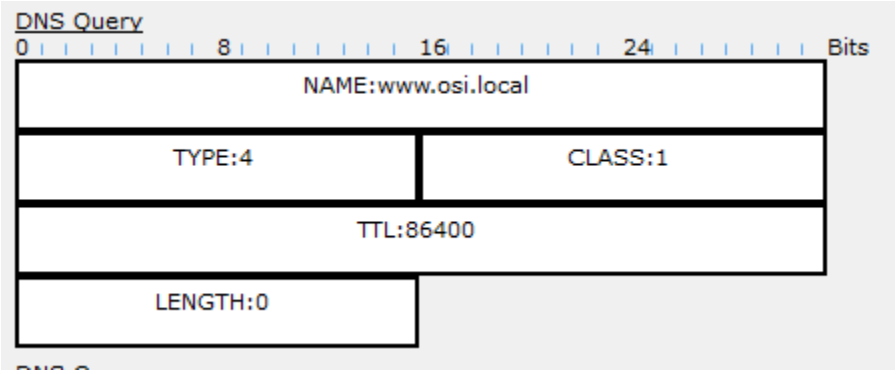
Estas entradas adicionales cumplen diversas funciones dentro de la suite TCP/IP. Si el protocolo de resolución de direcciones (ARP) está incluido, busca direcciones MAC. El protocolo DNS es responsable de convertir un nombre (por ejemplo, www.osi.local) a una dirección IP. Los eventos de TCP adicionales son responsables de la conexión, del acuerdo de los parámetros de comunicación y de la desconexión de las sesiones de comunicación entre los dispositivos. Estos protocolos se mencionaron anteriormente y se analizarán en más detalle a medida que avance el curso. Actualmente, hay más de 35 protocolos (tipos de evento) posibles para capturar en Packet Tracer.



d. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente). ¿Qué información se indica en NAME: (NOMBRE:) en la sección DNS QUERY (CONSULTA DNS)?

Respuesta:

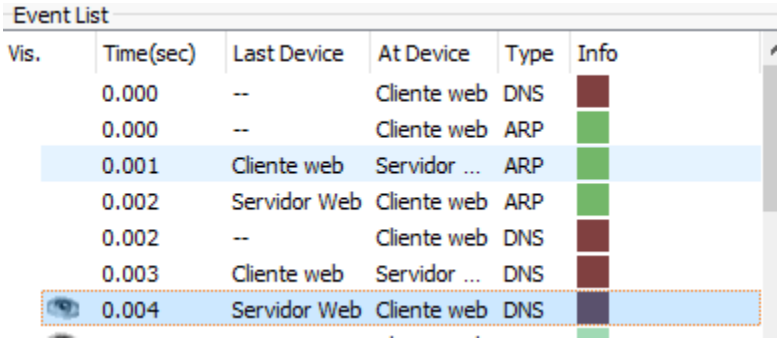
www.osi.local



e. Haga clic en el último cuadro coloreado Info de DNS en la lista de eventos. ¿Qué dispositivo se muestra?

Respuesta:

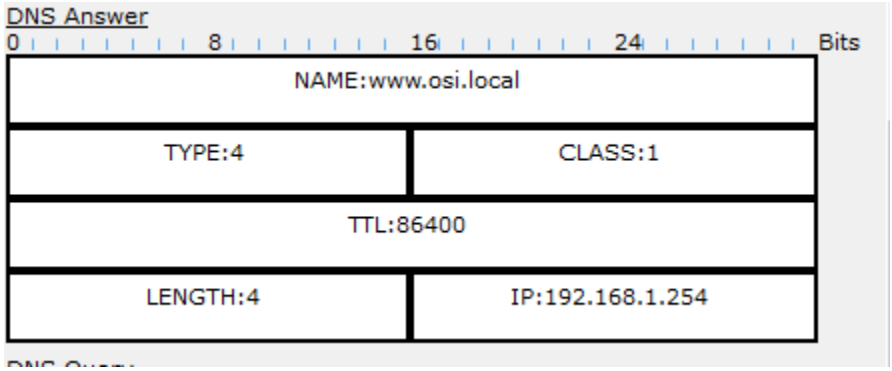
El cliente Web.



¿Cuál es el valor que se indica junto a ADDRESS: (DIRECCIÓN:) en la sección DNS ANSWER (RESPUESTA DE DNS) de Inbound PDU Details?

Respuesta:

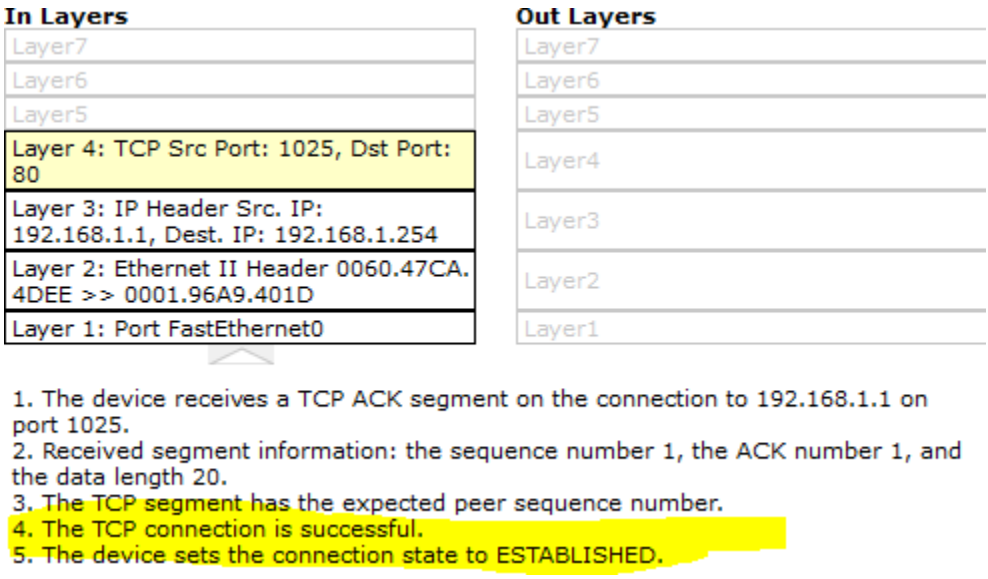
192.168.1.254, la dirección del servidor Web.



f. Busque el primer evento de HTTP en la lista y haga clic en el cuadro coloreado del evento de TCP que le sigue inmediatamente a este evento. Resalte Layer 4 (Capa 4) en la ficha OSI Model (Modelo OSI). En la lista numerada que está directamente debajo de In Layers y Out Layers, ¿cuál es la información que se muestra en los elementos 4 y 5?

Respuesta:

4. La conexión TCP se realizó correctamente. 5. El dispositivo establece el estado de la conexión en ESTABLISHED (ESTABLECIDA).



El protocolo TCP administra la conexión y la desconexión del canal de comunicación, además de tener otras responsabilidades. Este evento específico muestra que SE ESTABLECIÓ el canal de comunicación.

g. Haga clic en el último evento de TCP. Resalte Layer 4 (Capa 4) en la ficha OSI Model (Modelo OSI).

Examine los pasos que se indican directamente a continuación de In Layers y Out Layers.

¿Cuál es el propósito de este evento, según la información proporcionada en el último elemento de la lista (debe ser el elemento 4)?

Respuesta:

CERRAR la conexión.

DESAFÍO

En esta simulación, se proporcionó un ejemplo de una sesión Web entre un cliente y un servidor en una red de área local (LAN). El cliente realiza solicitudes de servicios específicos que se ejecutan en el servidor. Se debe configurar el servidor para que escuche puertos específicos y detecte una solicitud de cliente. (Sugerencia: observe Layer 4 [Capa 4] en la ficha OSI Model para obtener información del puerto).

Sobre la base de la información que se analizó durante la captura de Packet Tracer, ¿qué número de puerto escucha el servidor Web para detectar la solicitud Web?

Respuesta:

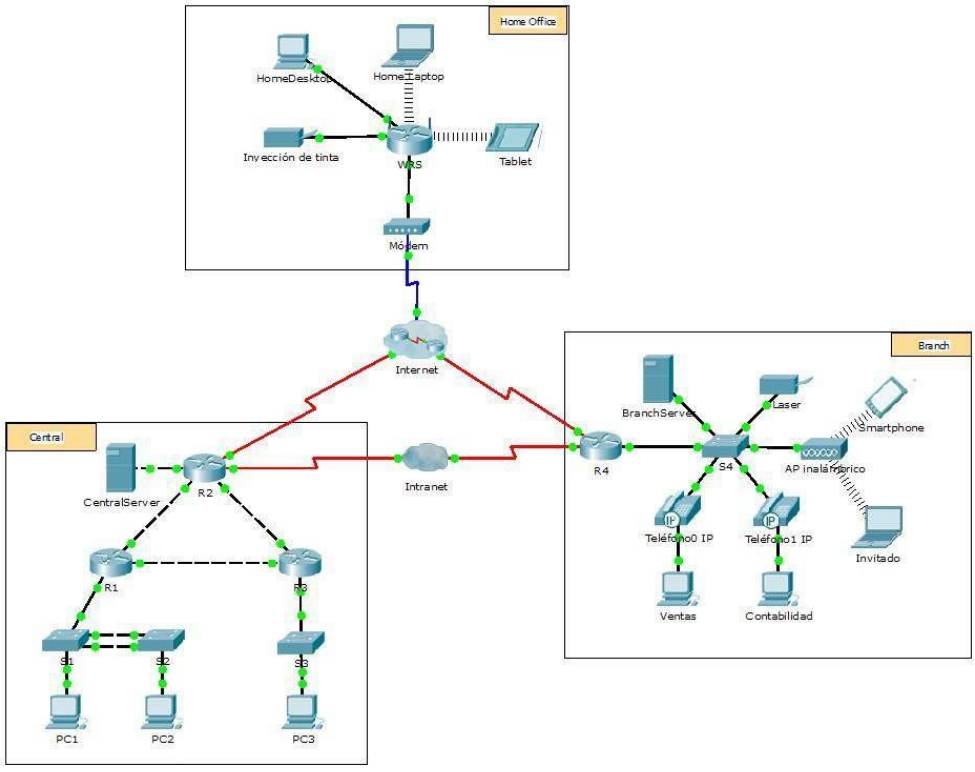
La primera PDU HTTP que solicita el cliente Web muestra el puerto 80 en el puerto DST (DESTINO) de capa 4.

¿Qué puerto escucha el servidor Web para detectar una solicitud de DNS?

Respuesta:

La primera PDU DNS que solicita el cliente Web muestra que el puerto de destino de capa 4 es el puerto 53.

3.3.3.3 Packet Tracer - Explore a Network Instructions IG



Parte 1: Examinar El Tráfico De Internetwork En La Sucursal

En la parte 1 de esta actividad, utilizará el modo de simulación para generar tráfico Web y examinar el protocolo

HTTP junto con otros protocolos necesarios para las comunicaciones.

Paso 1: Cambiar del modo de tiempo real al modo de simulación

a. Haga clic en el ícono del modo Simulation (Simulación) para cambiar del modo Realtime (Tiempo real) al modo Simulation.
b. Verifique que ARP, DNS, HTTP y TCP estén seleccionados en Event List Filters (Filtros de lista de eventos).
c. Mueva completamente hacia la derecha la barra deslizable que se encuentra debajo de los botones Play Controls (Controles de reproducción), Back, Auto Capture/Play, Capture/Forward (Retroceder, Captura/Reproducción automática,Capturar/avanzar).

Paso 2: Generar Tráfico Mediante Un Explorador Web

El panel de simulación actualmente está vacío. En Event List (Lista de eventos), en la parte superior del panel de simulación, hay seis columnas en el encabezado. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna Info (Información) se utiliza para examinar el contenido de un evento determinado.

Nota: la topología se muestra en el panel de la izquierda del panel de simulación. Utilice las barras de desplazamiento para incorporar la ubicación Branch al panel, en caso necesario. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha.

A. Haga clic en Sales PC (PC de ventas) en el panel del extremo izquierdo.
B. Haga clic en la ficha Desktop (Escritorio) y luego en el ícono Web Browser (Explorador Web) para abrirlo.
C. En el campo de dirección URL, introduzca http://branchserver.pt.pta y haga clic en Go (Ir). Observe la lista de eventos en el panel de simulación. ¿Cuál es el primer tipo

de evento que se indica? La solicitud de DNS de la dirección IP de branchserver.pt.pta.

D. Haga clic en el cuadro de información de DNS. En Out Layers (Capas de salida), se indica DNS para la capa 7. La capa 4 utiliza UDP para comunicarse con el servidor DNS en el puerto 53 (Dst Port: [Pto. de destino:]). Se indica tanto la dirección IP de origen como la de destino. ¿Qué información falta para comunicarse con el servidor DNS?

E. Haga clic en Auto Capture/Play. En aproximadamente 45 segundos, aparece una ventana en la que se indica la finalización de la simulación actual. Haga clic en el botón View Previous Events (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista y observe la cantidad de eventos de ARP. Observe la columna Device (Dispositivo) en la lista de eventos: ¿cuántos de los dispositivos en la ubicación Branch atraviesa la solicitud de ARP? Todos los dispositivos recibieron una solicitud de ARP.

F. Desplácese por los eventos en la lista hasta la serie de eventos de DNS. Seleccione el evento de DNS para el que se indica BranchServer en At Device (En el dispositivo). Haga clic en el cuadro de la columna Info. ¿Qué se puede determinar seleccionando la capa 7 en OSI Model (Modelo OSI)? (Consulte los resultados que se muestran directamente debajo de In Layers [Capas de entrada]).

El servidor DNS recibe una consulta DNS. La consulta del nombre se resuelve de forma local.

G. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente). Desplácese hasta la parte inferior de la ventana y ubique la sección DNS Answer (Respuesta de DNS). ¿Cuál es la dirección que se muestra?
172.16.0.3, la dirección de Branchserver.

H. Los eventos siguientes son eventos de TCP que permiten que se establezca un canal de comunicación. En el dispositivo Sales, seleccione el último evento de TCP anterior al evento de HTTP. Haga clic en el cuadro coloreado Info para ver la información de

PDU. Resalte Layer 4 (Capa 4) en la columna In Layers. Observe el elemento 6 en la lista que se encuentra directamente debajo de la columna In Layers: ¿cuál es el estado de la conexión?

Establecido

I. Los eventos siguientes son eventos de HTTP. Seleccione cualquiera de los eventos de HTTP en un dispositivo intermediario (teléfono IP o switch). ¿Cuántas capas están activas en uno de estos dispositivos y por qué?

Dos capas, porque son dispositivos de capa 2.

J. Seleccione el último evento de HTTP en Sales PC. Seleccione la capa superior en la ficha OSI Model. ¿Cuál es el resultado que se indica debajo de la columna In Layers?

El cliente HTTP recibe una respuesta de HTTP del servidor. Muestra la página en el explorador Web.

Parte 2: Examinar El Tráfico De Internetwork A La Central

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para ver y examinar cómo se administra el tráfico que sale de la red local.

Paso 1: Configurar la captura de tráfico hacia el servidor Web de la central

A. Cierre todas las ventanas de información de PDU abiertas.
B. Haga clic en la opción Reset Simulation (Restablecer simulación), que se encuentra cerca del centro del panel de simulación.
C. Escriba http://centralserver.pt.pta en el explorador Web de Sales PC.
D. Haga clic en Auto Capture/Play (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en View Previous Events (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es DNS y que no hay entradas de ARP antes de comunicarse con Branchserver. Según lo aprendido hasta ahora, ¿a qué se debe esto? Sales PC ya conoce la dirección MAC del servidor DNS.
E. Haga clic en el último evento de DNS en la columna Info. Seleccione Layer 7 (Capa 7) en la ficha OSI Model.

Al observar la información proporcionada, ¿qué se puede determinar sobre los resultados de DNS? El servidor DNS pudo resolver el nombre de dominio para centralserver.pt.pta.

F. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante). Desplácese hasta la sección DNS ANSWER (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta? 10.10.10.2.

G. Los eventos siguientes son eventos de ARP. Haga clic en el cuadro coloreado Info del último evento de ARP. Haga clic en la ficha Inbound PDU Details y observe la dirección MAC. Sobre la base de la información en la sección de ARP, ¿qué dispositivo proporciona la respuesta de ARP? El router R4, el dispositivo de gateway.

H. Los eventos siguientes son eventos de TCP, que nuevamente se preparan para establecer un canal de comunicación. Busque el primer evento de HTTP en Event List. Haga clic en el cuadro coloreado del evento de HTTP. Resalte Layer 2 (Capa 2) en la ficha OSI Model. ¿Qué se puede determinar sobre la dirección MAC de destino? Es la dirección MAC del router R4.

I. Haga clic en el evento de HTTP en el dispositivo R4. Observe que la capa 2 contiene un encabezado de Ethernet II. Haga clic en el evento de HTTP en el dispositivo Intranet. ¿Cuál es la capa 2 que se indica en este dispositivo? Frame Relay FRAME RELAY.

Observe que solo hay dos capas activas, en oposición a lo que sucede cuando se atraviesa el router. Esta es una conexión WAN, y se analizará en otro curso.

Parte 3: Examinar el tráfico de Internet desde la sucursal

En La Parte 3 De Esta Actividad, Borrará Los Eventos Y Comenzará Una Nueva Solicitud Web Que Usará Internet.

Paso 1: Configurar la captura de tráfico hacia un servidor Web de Internet

A. Cierre todas las ventanas de información de PDU abiertas.

B. Haga clic en la opción Reset Simulation, que se encuentra cerca del centro del panel de simulación. Escriba http://www.netacad.pta en el explorador Web de Sales PC.

C. Haga clic en Auto Capture/Play (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en View Previous Events (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es DNS. ¿Qué advierte sobre la cantidad de eventos de DNS?
Hay muchos más eventos de DNS. Dado que la entrada de DNS no es local, se reenvía hacia un servidor en Internet.

D. Observe algunos de los dispositivos a través de los que se transfieren los eventos de DNS en el camino hacia un servidor DNS. ¿Dónde se encuentran estos dispositivos?
En la nube de Internet. Se debe mostrar a los estudiantes que esos dispositivos se pueden ver haciendo clic en la nube y luego en el enlace Back (Atrás) para regresar.

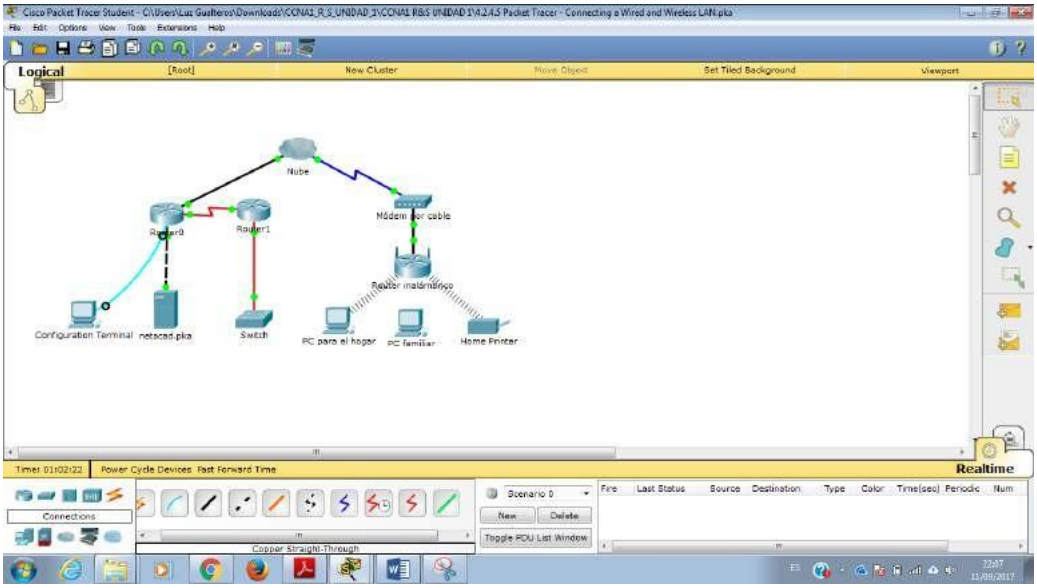
E. Haga clic en el último evento de DNS. Haga clic en la ficha Inbound PDU Details y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para www.netacad.pta? 216.146.46.11

F. Cuando los routers mueven el evento de HTTP a través de la red, hay tres capas activas en In Layers y Out Layers en la ficha OSI Model. Sobre la base de esa información, ¿cuántos routers se atraviesan?
Hay tres routers (ISP-Tier3a, ISP-Tier3b y R4); sin embargo, hay cuatro eventos de HTTP que los atraviesan

G. Haga clic en el evento de TCP anterior al último evento de HTTP. Según la información que se muestra, ¿cuál es el propósito de este evento? Cerrar la conexión TCP a 216.146.46.11.

H. Se indican varios eventos más de TCP. Ubique el evento de TCP donde se indique IP Phone (Teléfono IP) para Last Device (Último dispositivo) y Sales para At Device. Haga clic en el cuadro coloreado Info y seleccione Layer 4 en la ficha OSI Model. Según la información del resultado, ¿cómo se configuró el estado de la conexión? Cierre

4.2.4.5 Packet Tracer - Connecting a Wired and Wireless LAN Instructions IG



Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0 a. En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las **conexiones** disponibles.

b. Elija el cable adecuado para conectar la **interfaz Fa0/0 del Router0** a la **interfaz Eth6 de la nube**. La **nube** es un tipo de switch, de modo que debe usar una conexión por **cable de cobre de conexión directa**. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar la nube al módem por cable

Elija el cable adecuado para conectar la **interfaz Coax7 de la nube** al **Puerto0 del módem**.
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

Elija el cable adecuado para conectar la **interfaz Ser0/0/0 del Router0** a la **interfaz Ser0/0 del Router1**. Use uno de los cables **seriales** disponibles.
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar el Router0 a netacad.pka

Elija el cable adecuado para conectar la **interfaz Fa0/1 del Router0** a la **interfaz Fa0 de netacad.pka**. Los routers y las PC tradicionalmente utilizan los mismos cables para transmitir (1 y 2) y recibir (3 y 6). El cable adecuado que se debe elegir consta de cables cruzados. Si bien muchas NIC ahora pueden detectar automáticamente qué par se utiliza para transmitir y recibir, el **Router0** y **netacad.pka** no tienen NIC con detección automática.
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 3: Conectar el Router0 a la terminal de configuración

Elija el cable adecuado para conectar la **consola** del **Router0** a la **terminal de configuración RS232**. Este cable no proporciona acceso a la red a la **terminal de configuración**, pero le permite configurar el **Router0** a través de su terminal.
Si conectó el cable correcto, las luces de enlace del cable cambian a color negro.

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

Elija el cable adecuado para conectar la **interfaz Fa1/0 del Router1** a la **interfaz Fa0/1 del switch**.
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde. Deje que transcurran unos segundos para que la luz cambie de color ámbar a verde.

Paso 2: Conectar el módem por cable al router inalámbrico

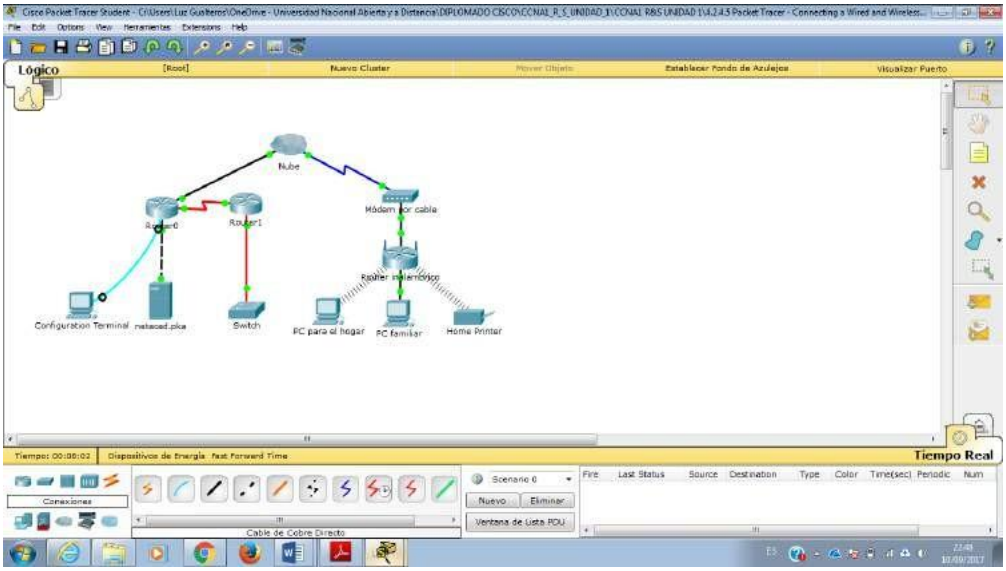
Elija el cable adecuado para conectar el **Puerto1** del **módem** al puerto de **Internet del router inalámbrico**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde. **Packet Tracer: conexión de una red LAN cableada e inalámbrica**

Paso 3: Conectar el router inalámbrico a la PC familiar

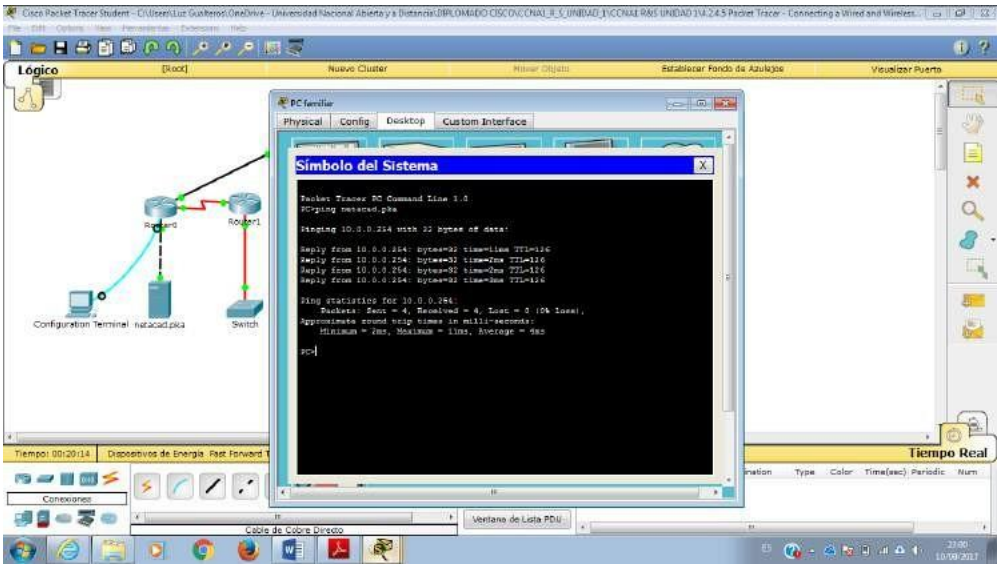
Elija el cable adecuado para conectar la **interfaz Ethernet 1 del router inalámbrico** a la **PC familiar**.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

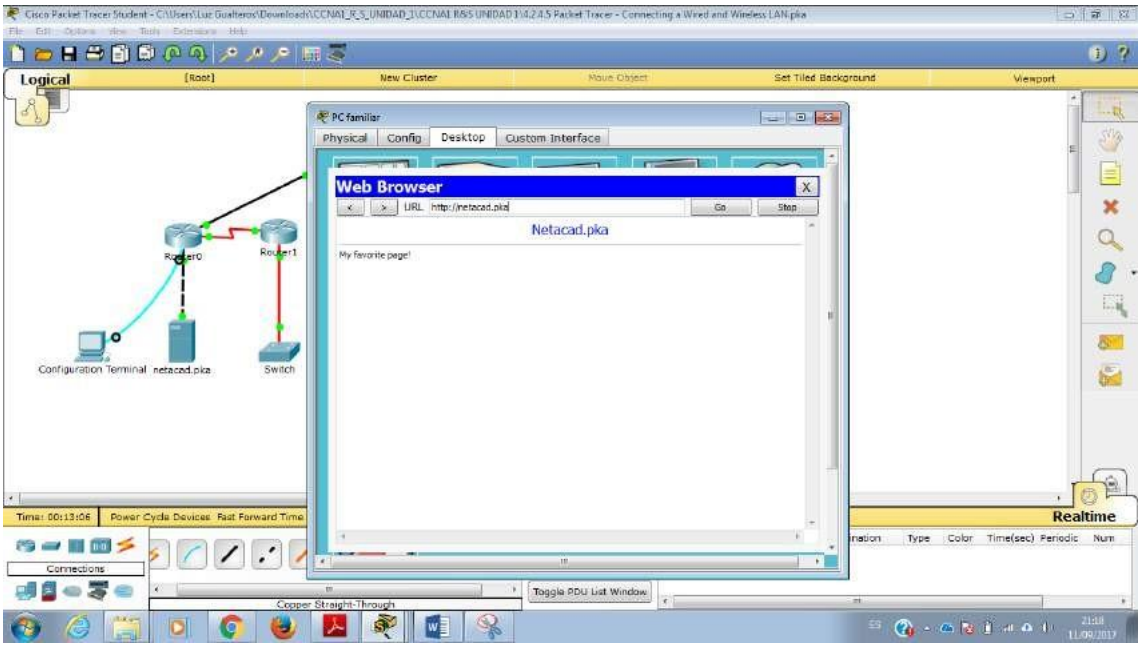


Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka a. Abra el símbolo del sistema de la **PC familiar** y haga ping a **netacad.pka**.

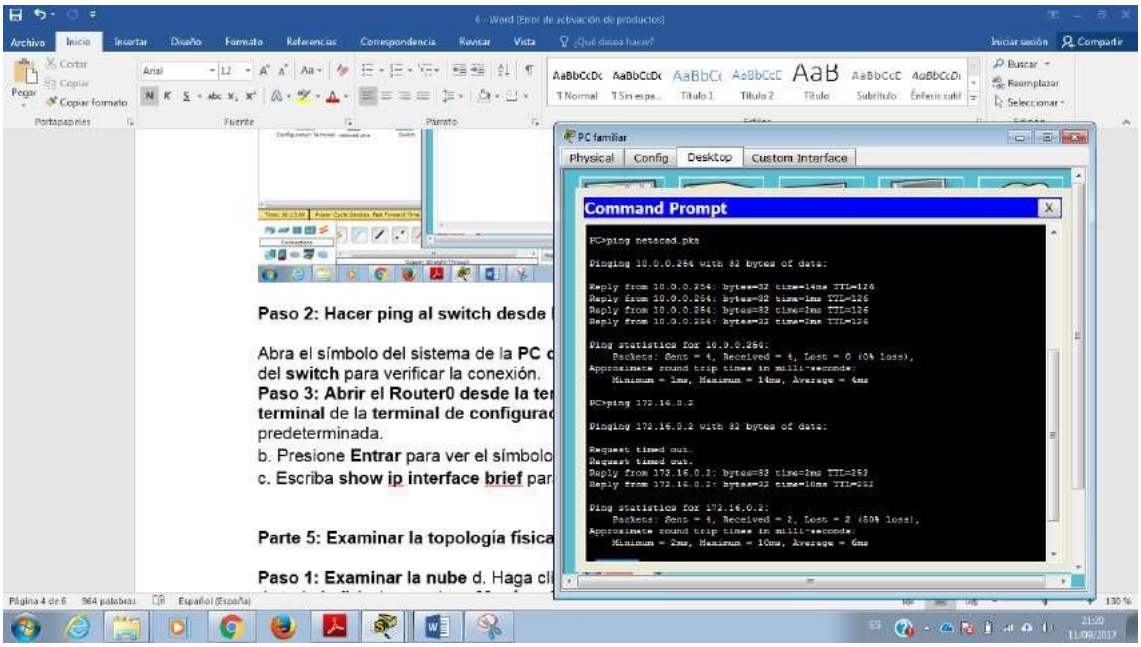


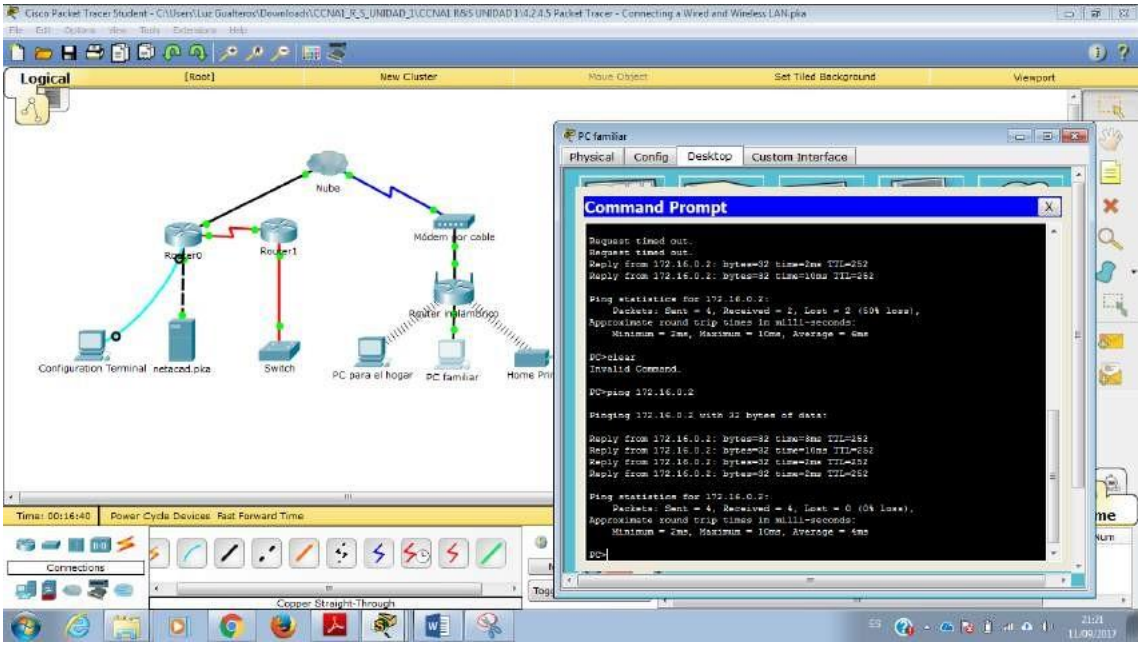
b. Abra el **explorador Web** e introduzca dirección Web **http://netacad.pka**.



Paso 2: Hacer ping al switch desde la PC doméstica

Abra el símbolo del sistema de la **PC doméstica** y haga ping a la dirección IP del **switch** para verificar la conexión.

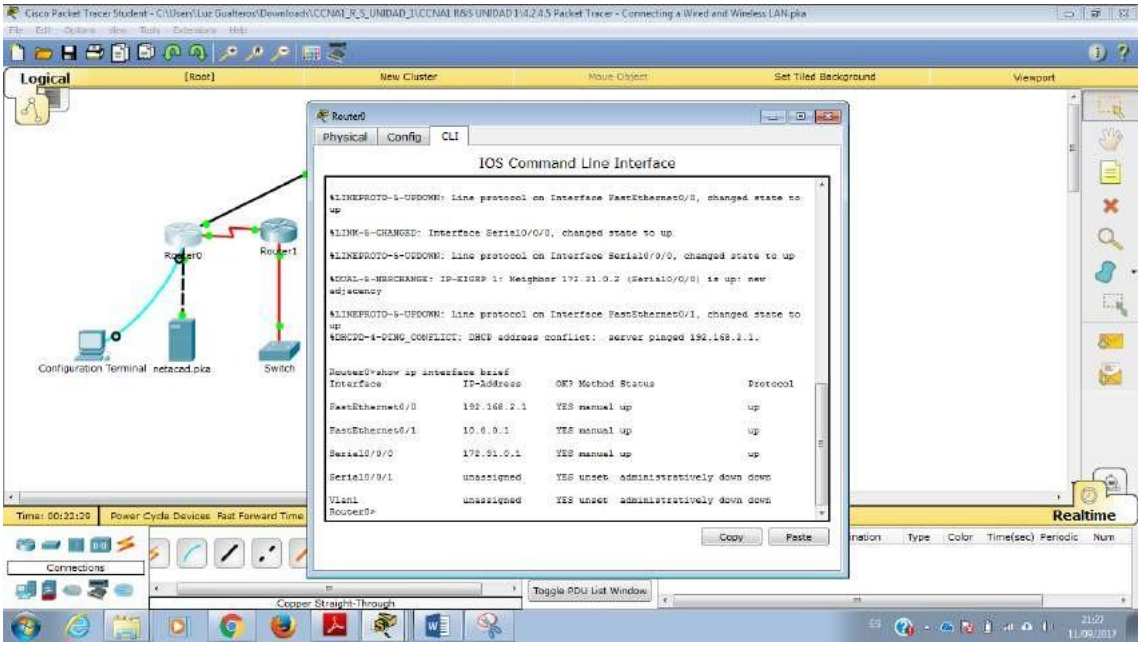




Paso 3: Abrir el Router0 desde la terminal de configuración a. Abra la **terminal** de la **terminal de configuración** y acepte la configuración predeterminada.

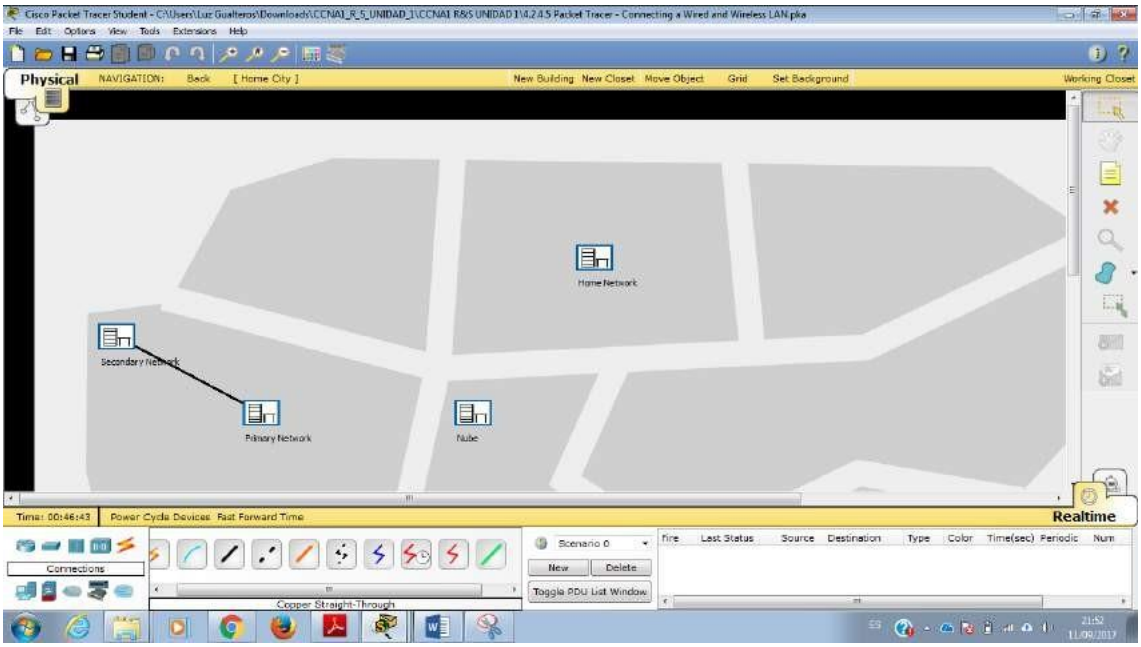
b. Presione **Entrar** para ver el símbolo del sistema del **Router0**.

c. Escriba **show ip interface brief** para ver el estado de las interfaces.

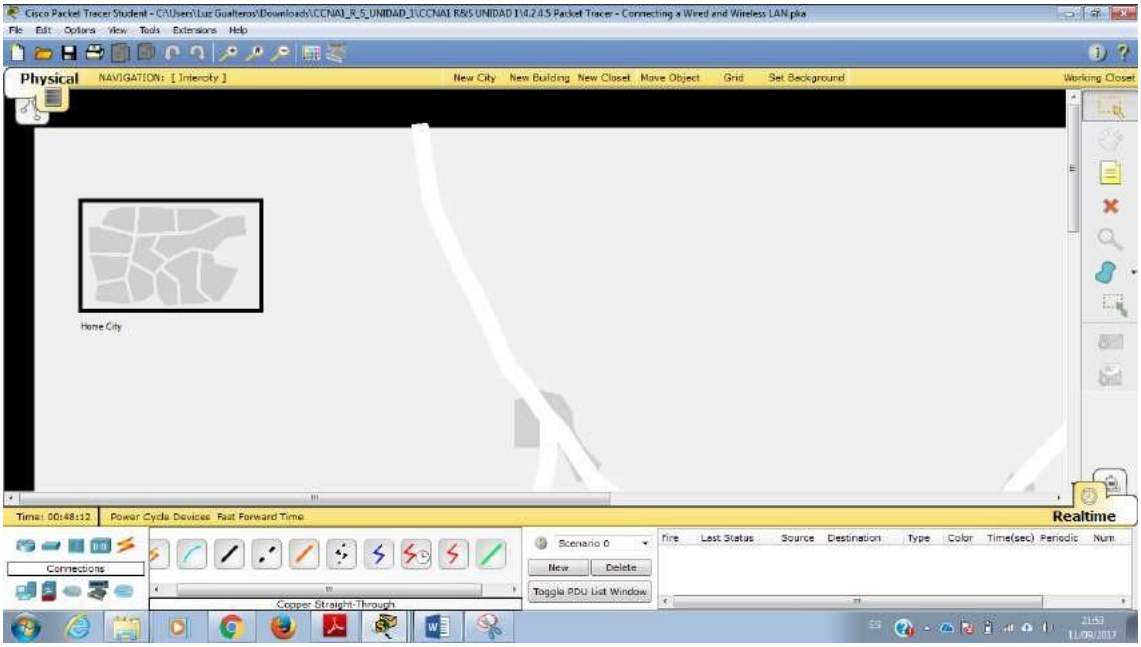


Parte 5: Examinar la topología física

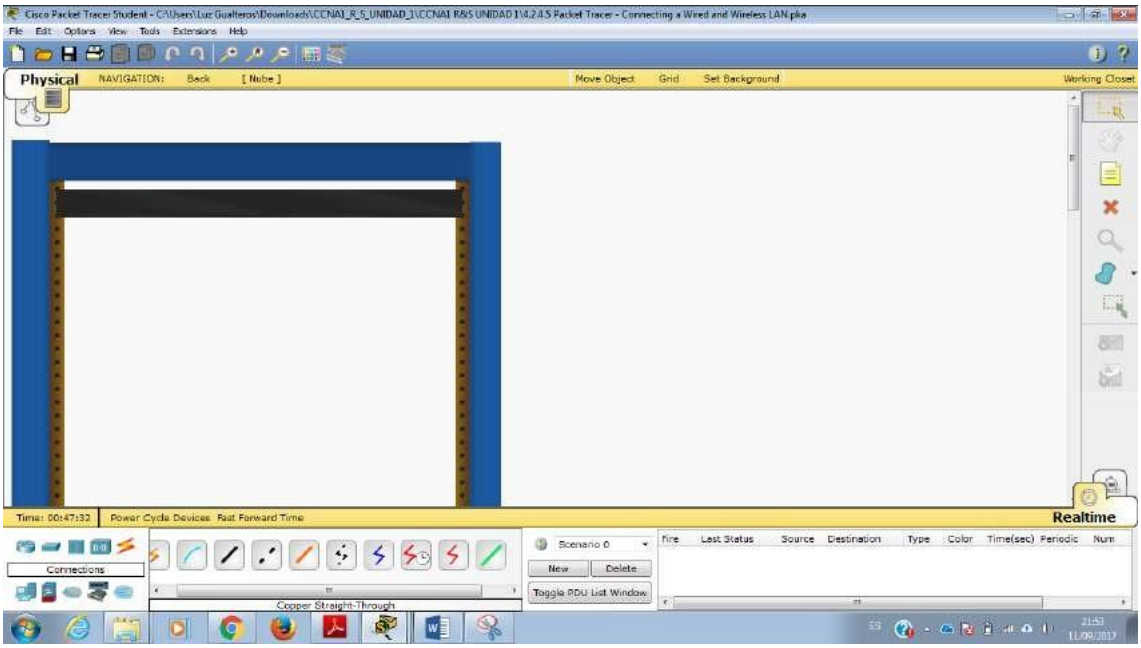
Paso 1: Examinar la nube d. Haga clic en la ficha **Physical Workspace** (Área de trabajo física) o presione **Mayús** + **P** y **Mayús** + **L** para alternar entre las áreas de trabajo lógicas y físicas.



e. Haga clic en el ícono **Home City** (Ciudad de residencia).



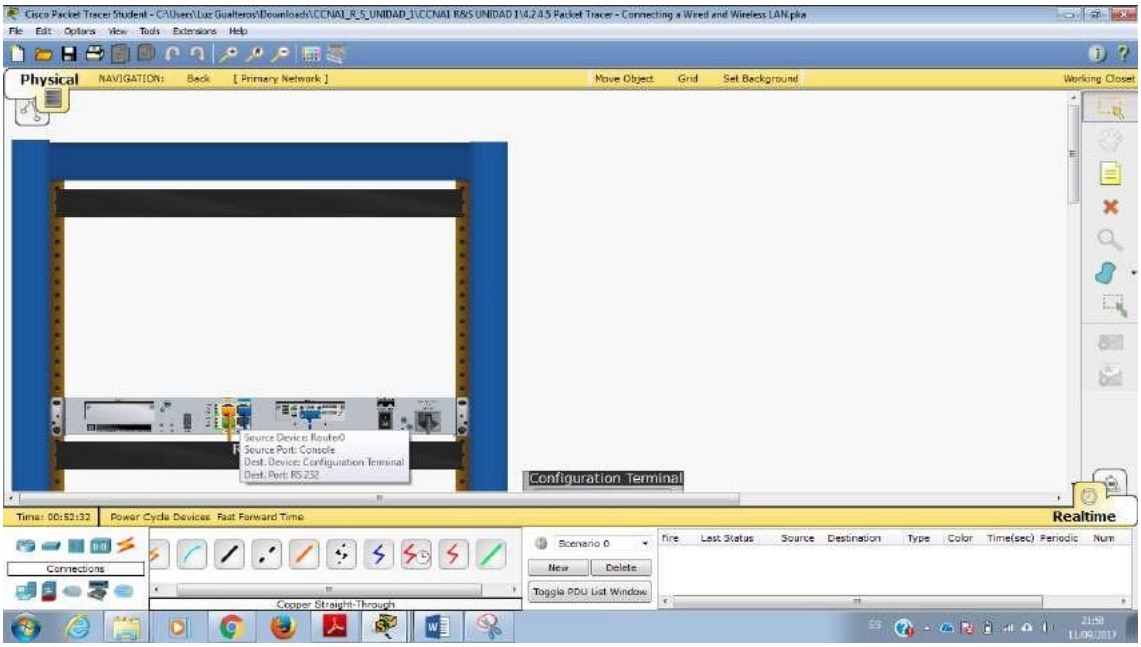
f. Haga clic en el ícono **Cloud** (Nube). ¿Cuántos cables están conectados al switch en el bastidor azul? 2

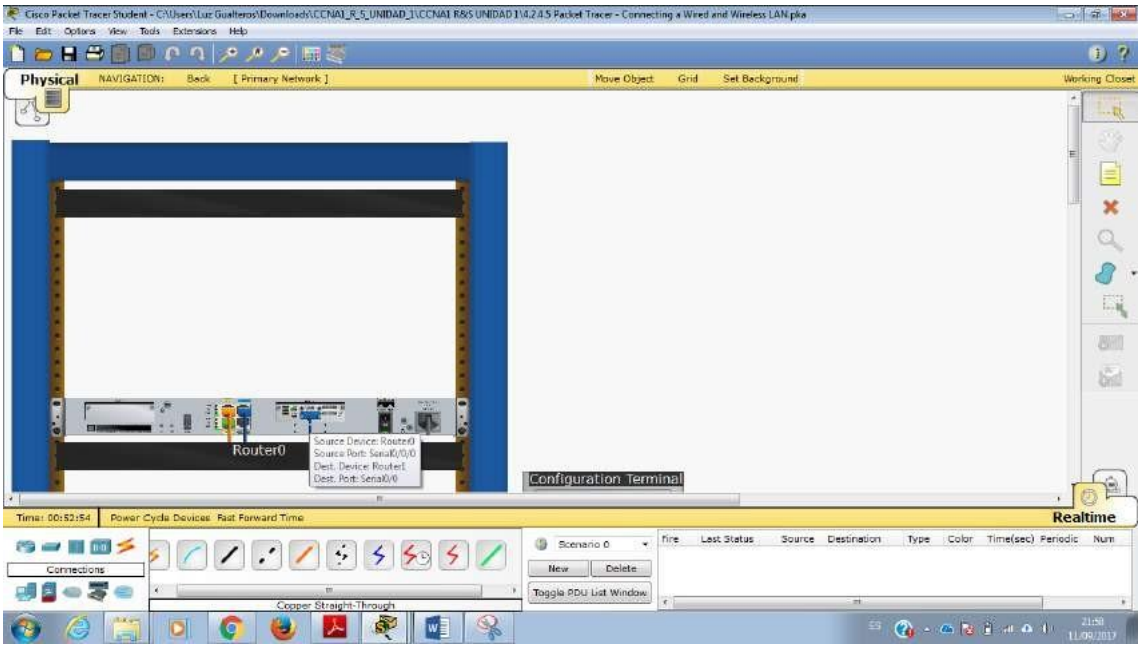


g. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

Paso 2: Examinar la red principal h. Haga clic en el ícono **Primary Network** (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul? Terminal de configuración

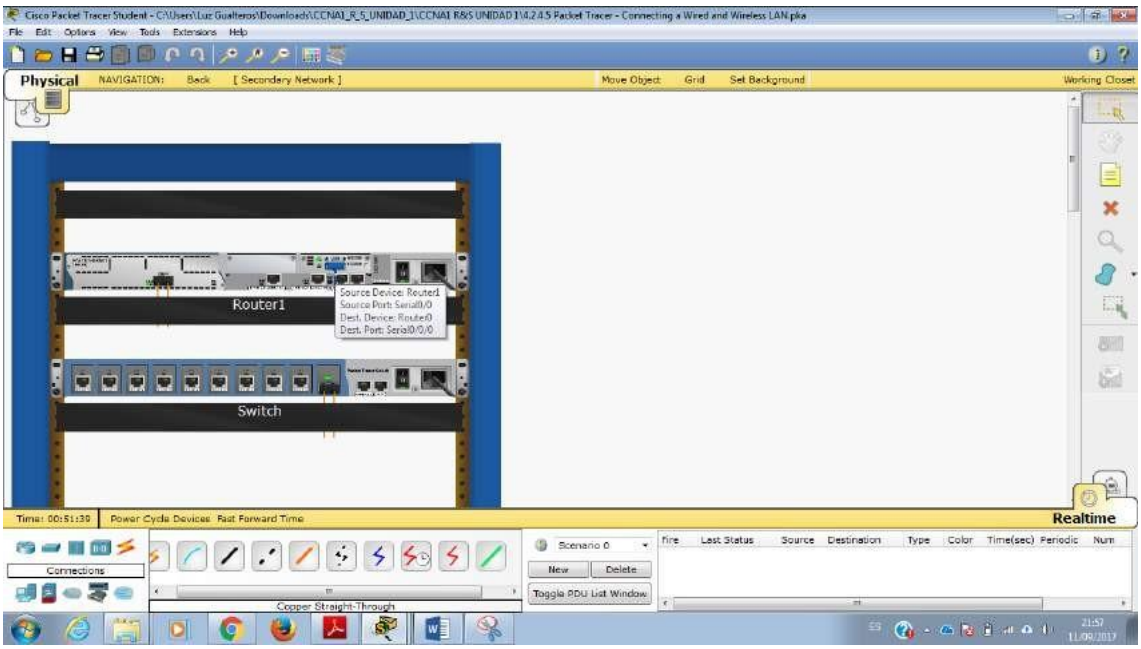
i. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

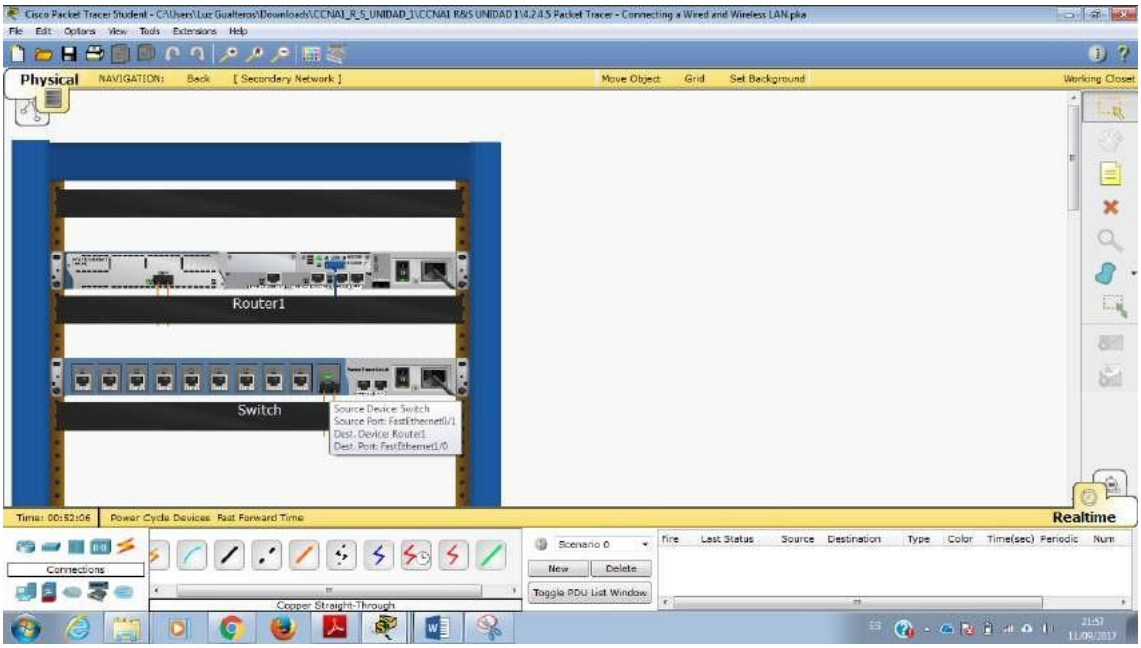


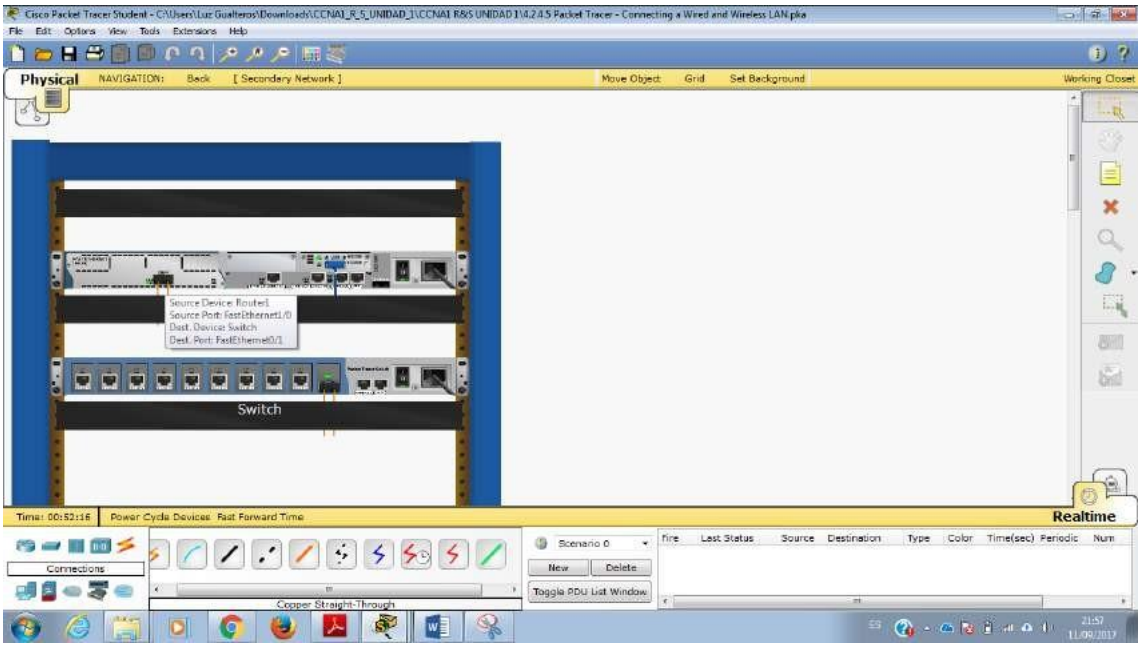


Paso 3: Examinar la red secundaria j. Haga clic en el ícono **Secondary Network** (Red secundaria). Mantenga el puntero del mouse sobre los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo? Los cables de fibra vienen en pares, uno para transmitir y otro para recibir.

k. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).



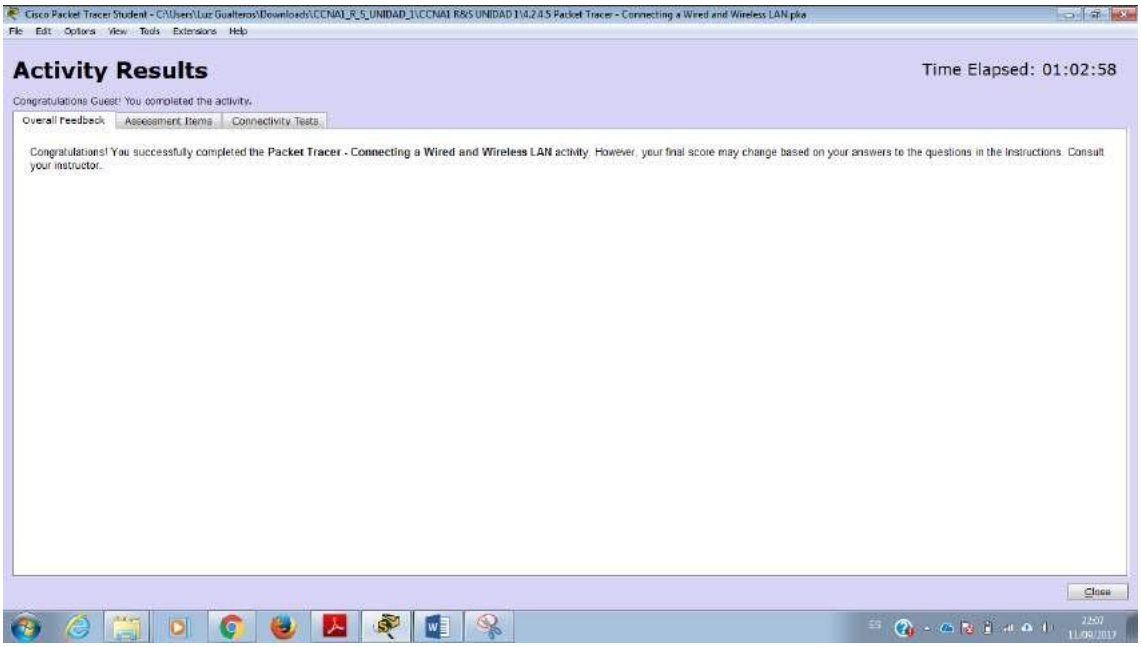


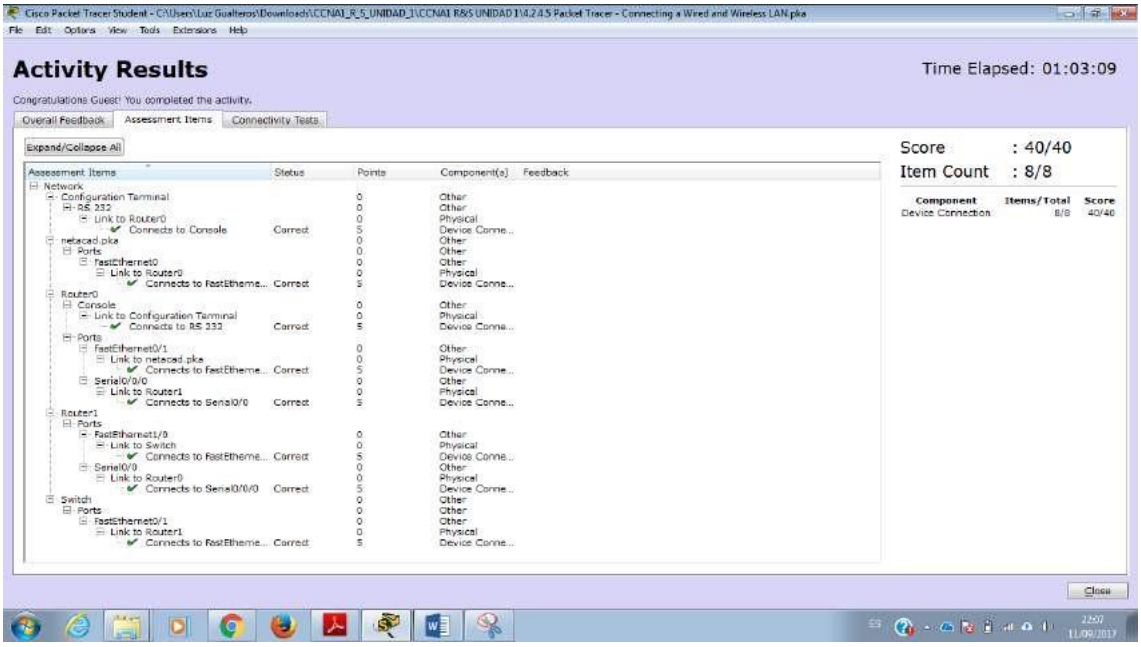


Paso 4: Examinar la red doméstica l. ¿Por qué hay una malla ovalada que cubre la red doméstica? Representa el alcance de la red inalámbrica.

m. Haga clic en el ícono **Home Network** (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo? Por lo general, las redes domésticas no incluyen bastidores.

a. Haga clic en la ficha **Logical Workspace** (Área de trabajo lógica) para volver a la topología lógica.





5.1.4.4 Packet Tracer - Identify MAC and IP Addresses Instructions IG

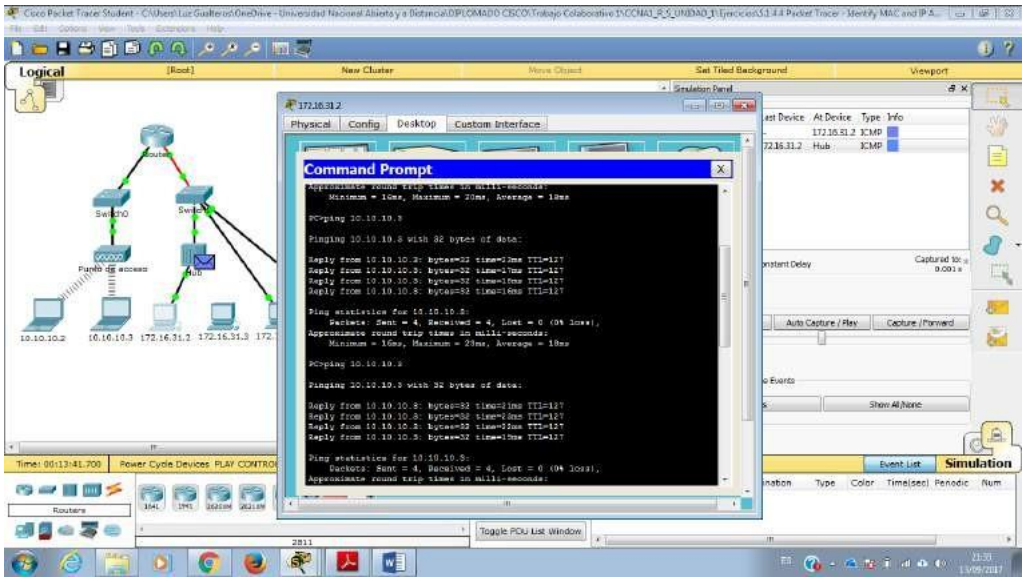
Parte 1: Recopilar información de la PDU

Nota: revise las preguntas de reflexión de la parte 2 antes de continuar con la parte 1. Le darán una idea de los tipos de información que debe recopilar.

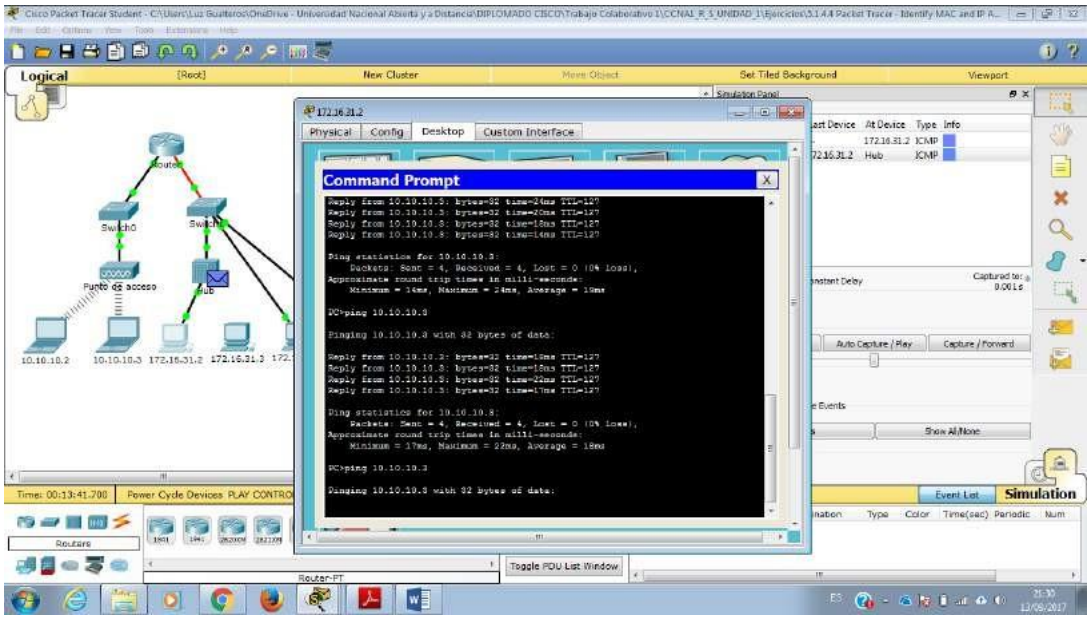
Paso 1: Recopilar información de la PDU mientras un paquete se transfiere de 172.16.31.2 a 10.10.10.3

a. Haga clic en 172.16.31.2 y abra el símbolo del sistema.

b. Introduzca el comando ping 10.10.10.3.

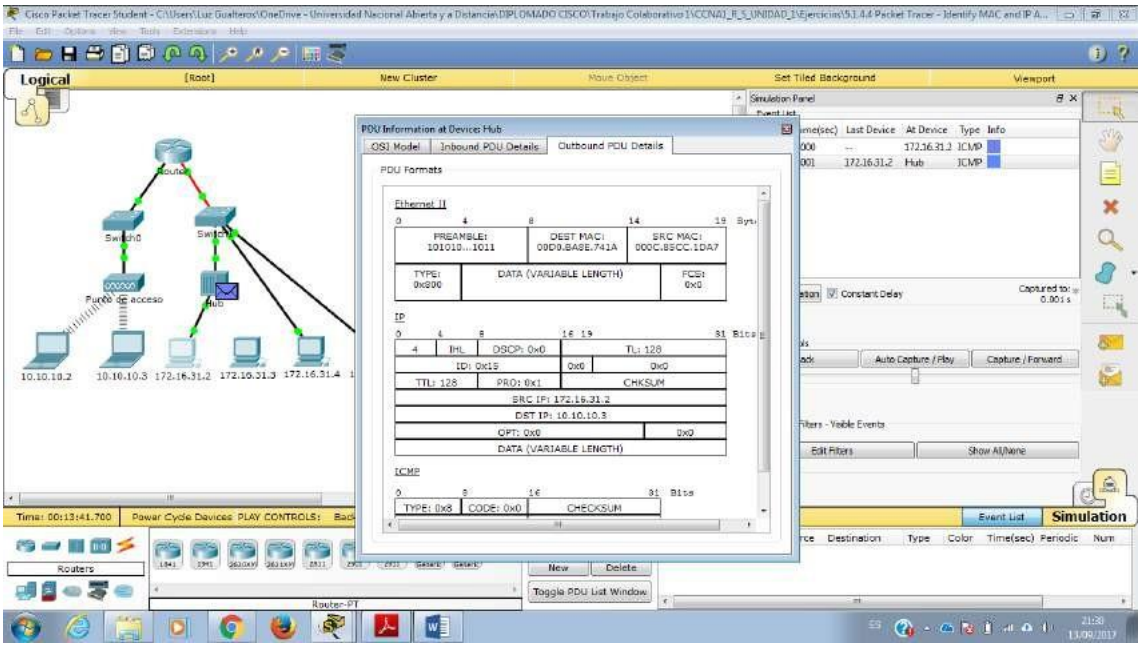


c. Cambie al modo de simulación y repita el comando ping 10.10.10.3. Aparece una PDU junto a 172.16.31.2.

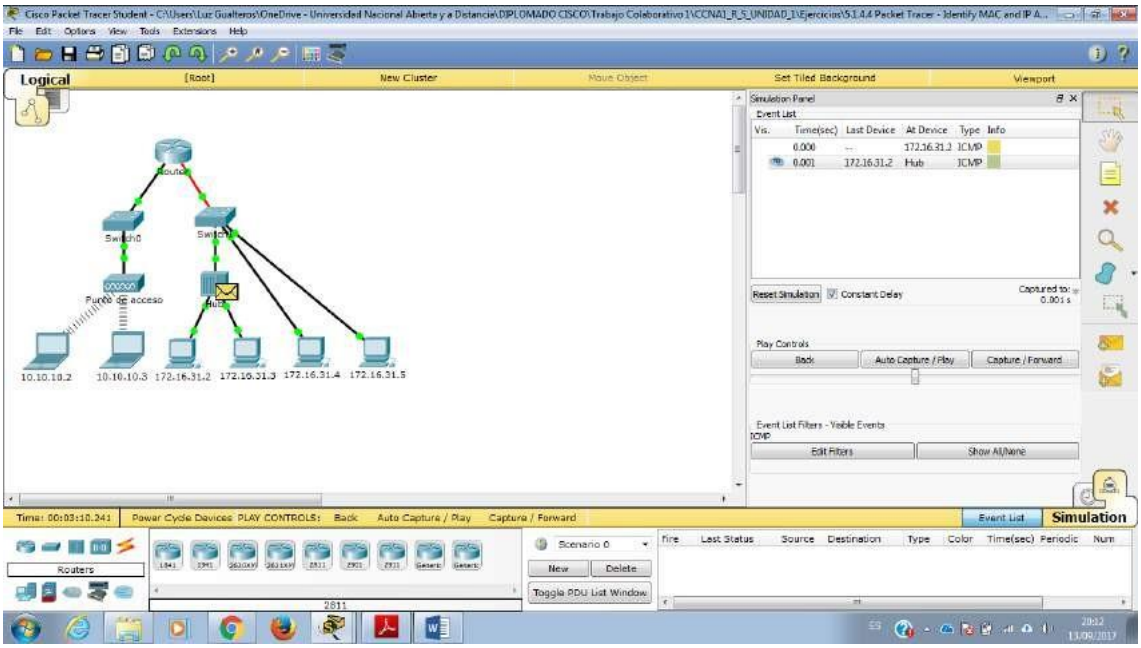


d. Haga clic en la PDU y observe la siguiente información en la ficha Outbound PDU Layer (Capa de PDU saliente):

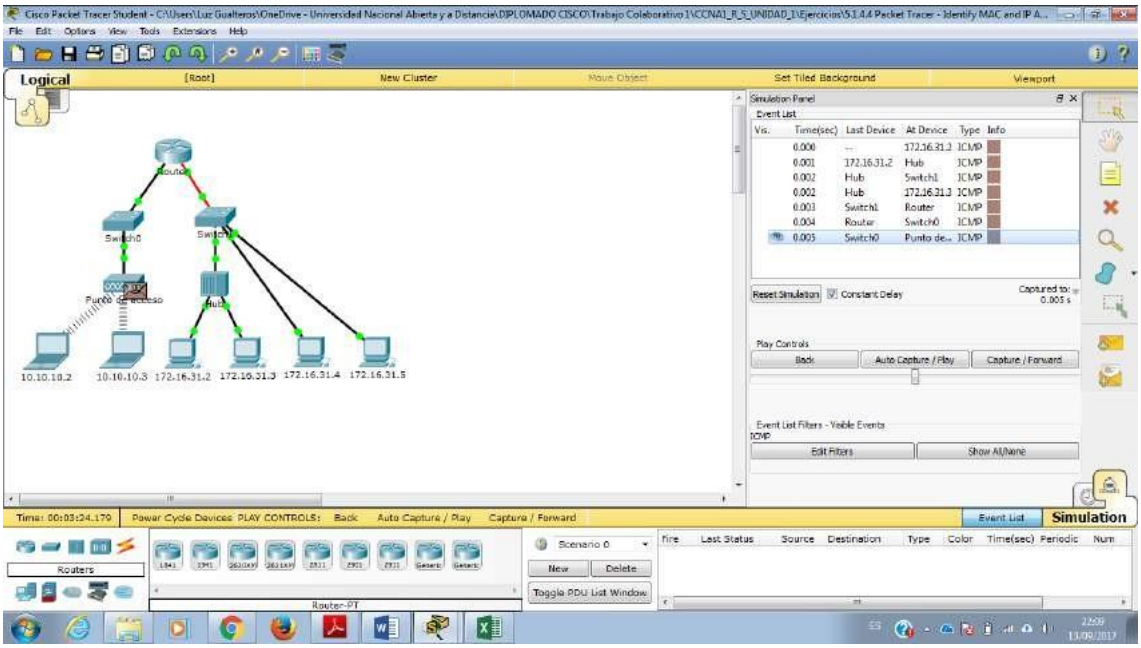
• Dirección MAC de destino: 00D0:BA8E:741A
• Dirección MAC de origen: 000C:85CC:1DA7
• Dirección IP de origen: 172.16.31.2
• Dirección IP de destino: 10.10.10.3
• En el dispositivo: PC



e. Haga clic en Capture/Forward (Capturar/reenviar) para mover la PDU al siguiente dispositivo. Recopile la misma información del paso 1d. Repita este proceso hasta que la PDU llegue al destino. Registre la información que recopiló de la PDU en una hoja de cálculo con un formato como el de la tabla que se muestra a continuación:



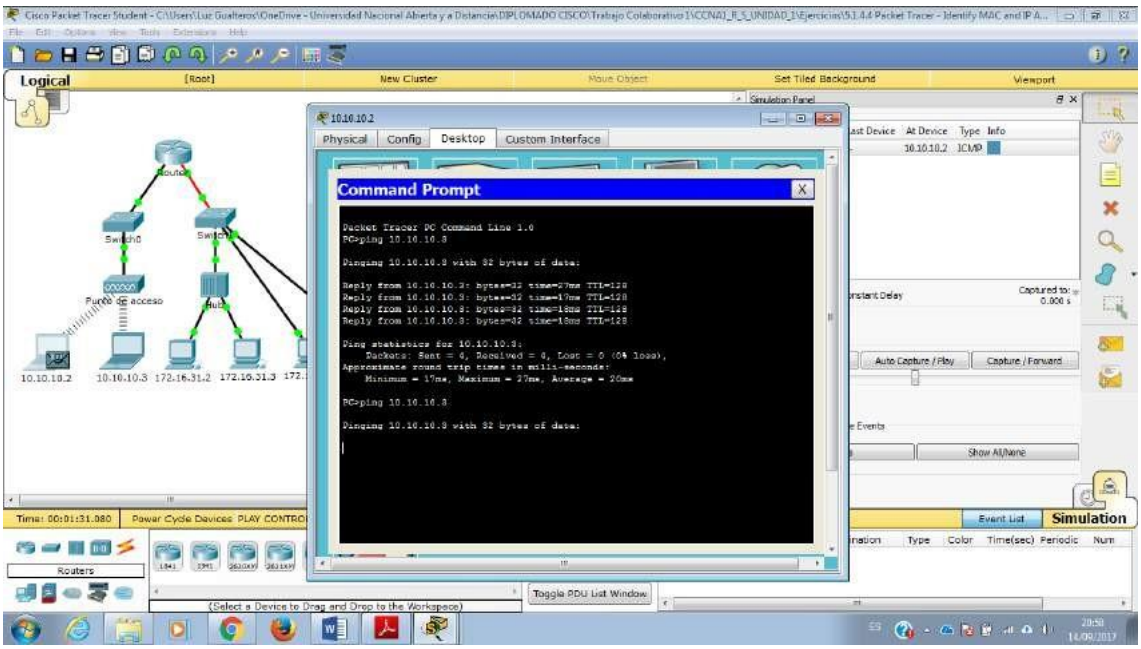
Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
ping de 172.16.31.2 a 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	00D0:BA8E:741A	00D0:BA8E:741A	172.16.31.2	10.10.10.3
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Punto de acceso				
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3



Paso 2: Recopilar información adicional de la PDU de otros pings

Repita el proceso del paso 1 y recopile información para las pruebas siguientes:

• Ping de 10.10.10.2 a 10.10.10.3



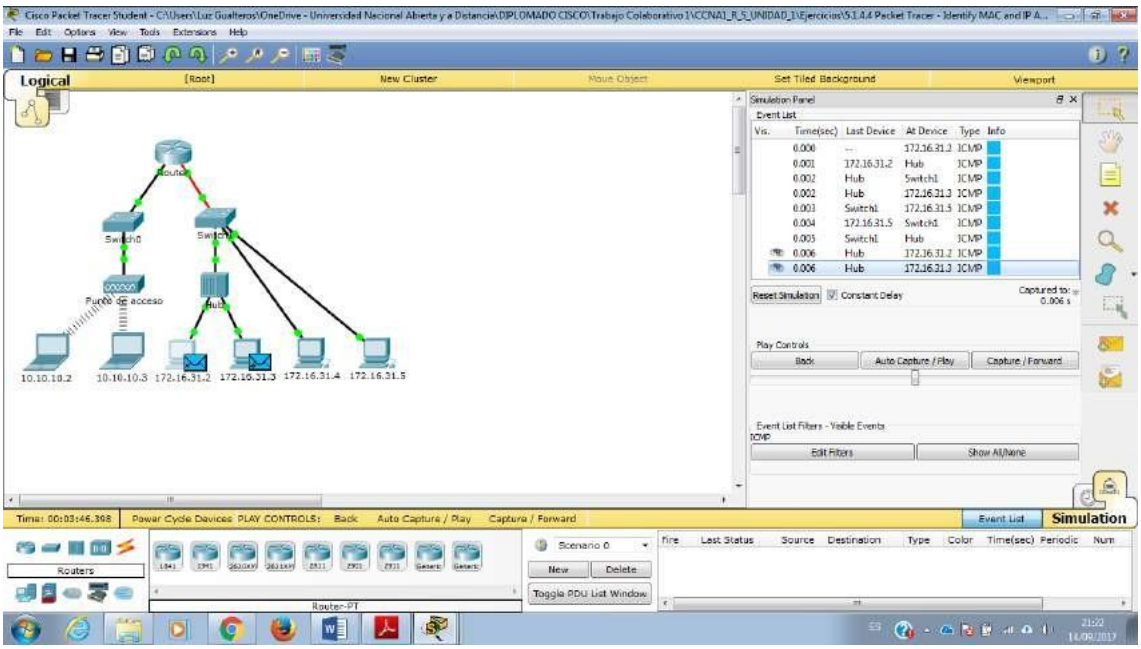
Está generando el ping, pero no va a pasar de ahí porque no tiene para donde circular.

• Ping de 172.16.31.2 a 172.16.31.3

• Ping de 172.16.31.4 a 172.16.31.5

• Ping de 172.16.31.4 a 10.10.10.2

• Ping de 172.16.31.3 a 10.10.10.2



5.2.1.7 *Packet Tracer - Examine the ARP Table Instructions IG*

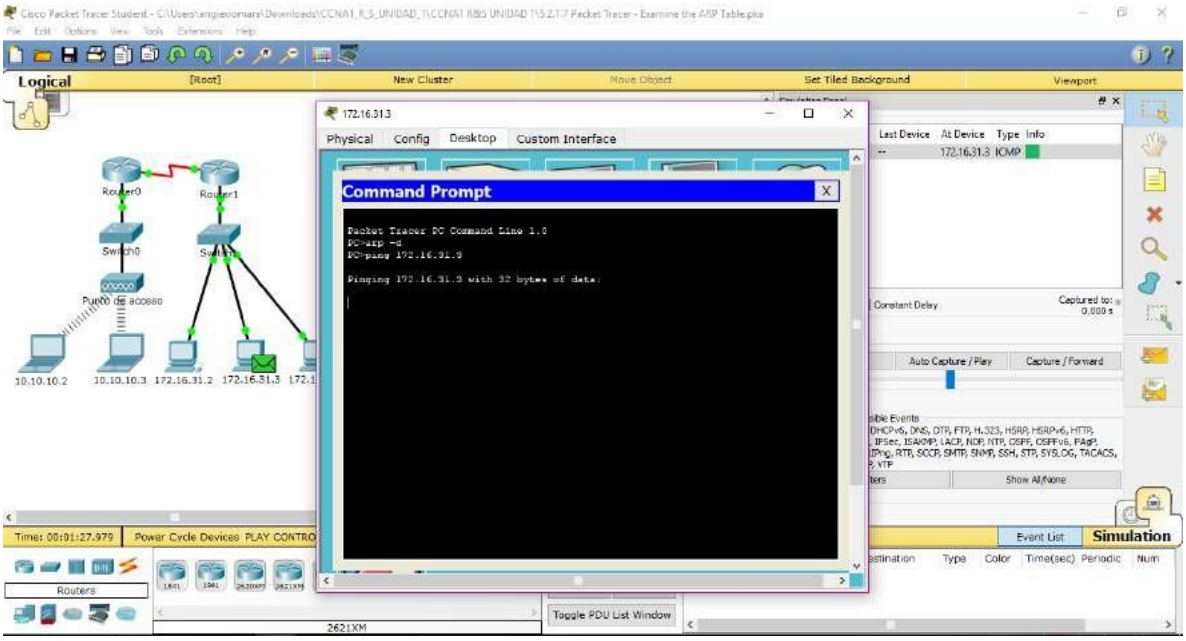
Parte 1: Examinar una solicitud de ARP

Paso 1: Generar solicitudes de ARP haciendo ping a 172.16.31.3 desde 172.16.31.2

a. Haga clic en 172.16.31.2 y abra el símbolo del sistema.

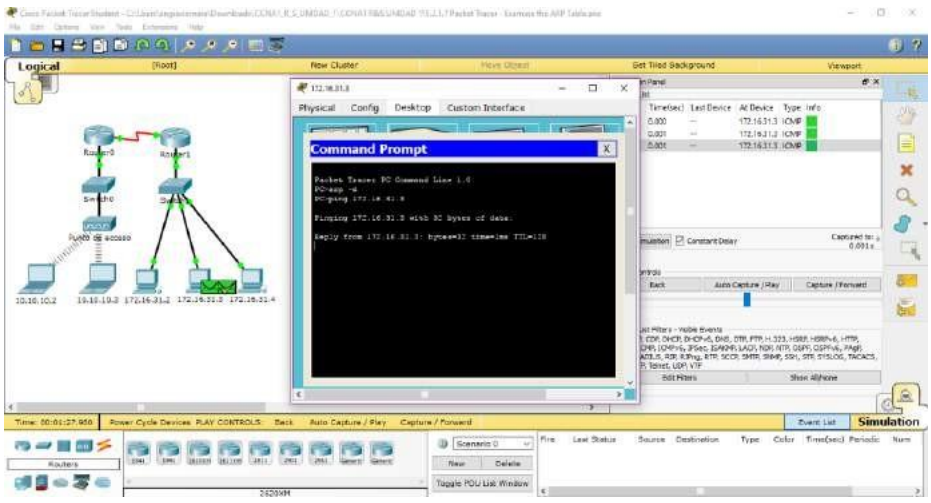
b. Introduzca el comando arp -d para borrar la tabla ARP.

c. Ingrese al modo Simulation (Simulación) e introduzca el comando ping 172.16.31.3. Se generan dos PDU. El comando ping no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.



d. Haga clic en Capture/Forward (Capturar/avanzar) una vez. La PDU ARP mueve el Switch1, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior?

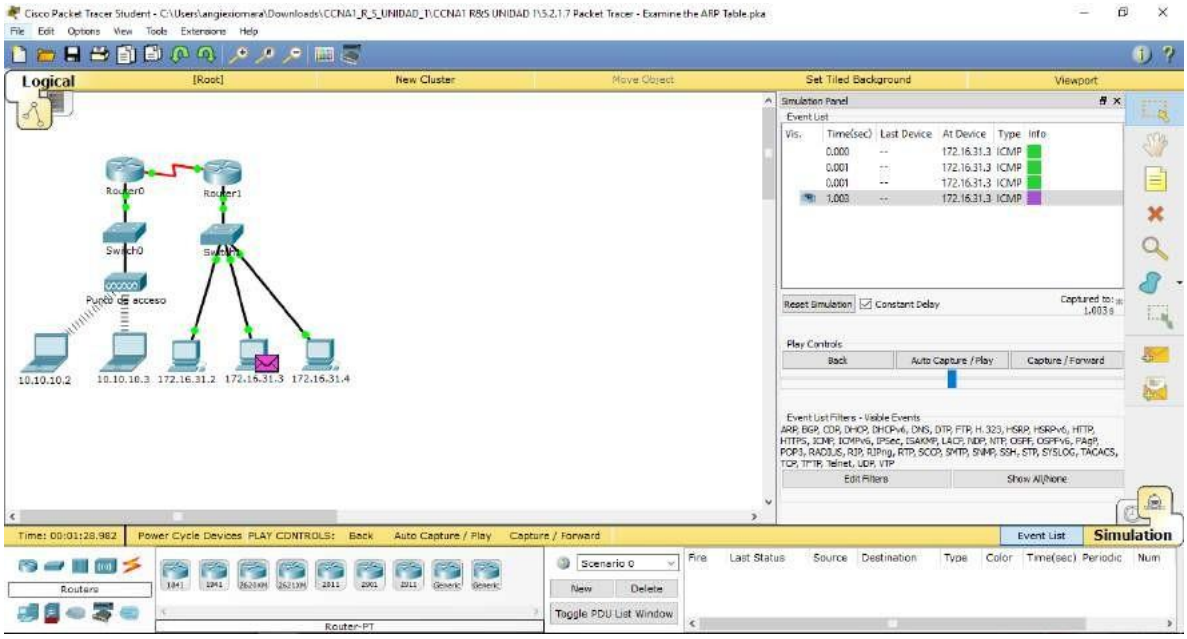
Rta No



e. Haga clic en Capture/Forward (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el Switch1?

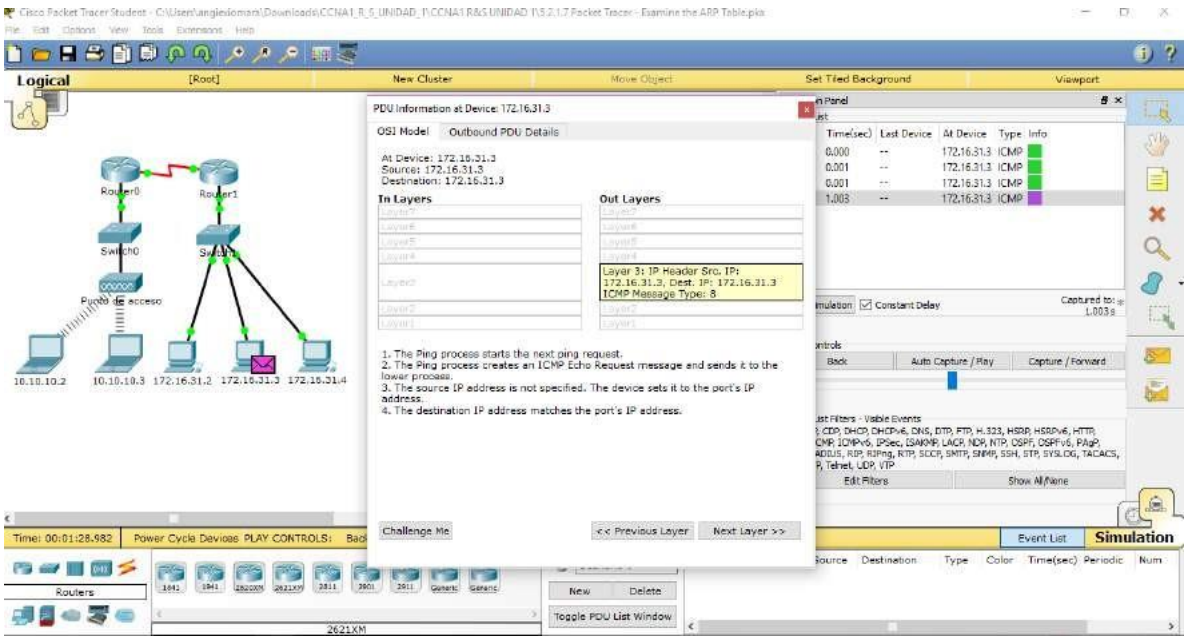
Rta 3

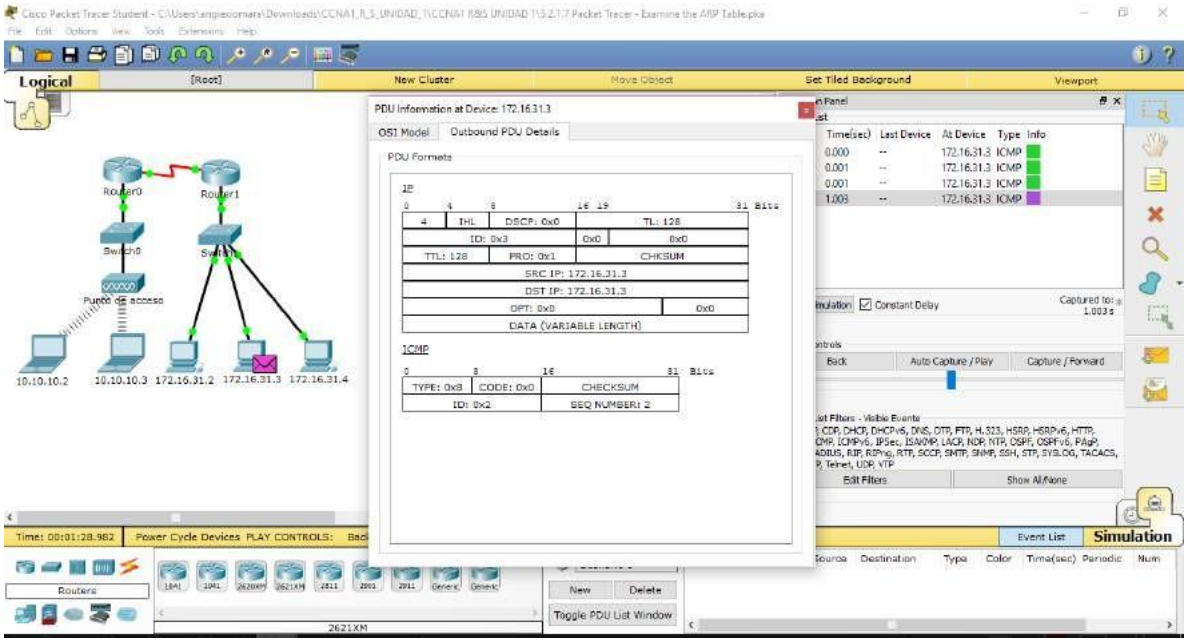
f. ¿Cuál es la dirección IP del dispositivo que aceptó la PDU? 172.16.31.3



g. Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino? El origen se transformó en el destino, FFFF.FFFF.FFFF se convirtió en la dirección MAC de

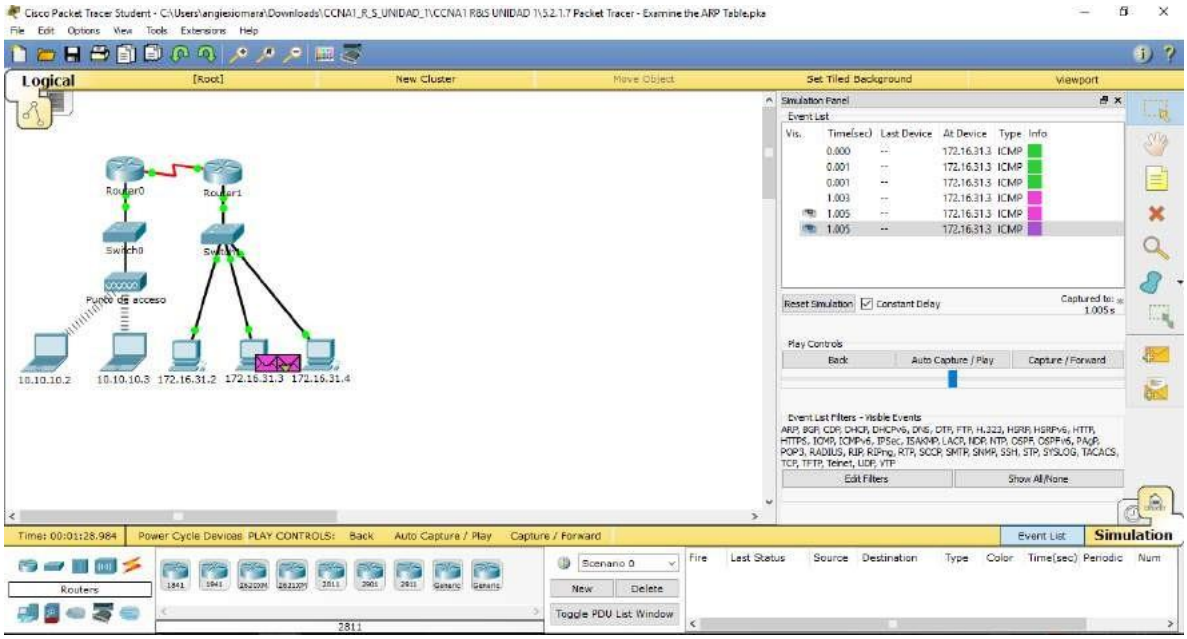
Rta 172.16.31.3.





h. Haga clic en Capture/Forward hasta que la PDU regrese a 172.16.31.2. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP?

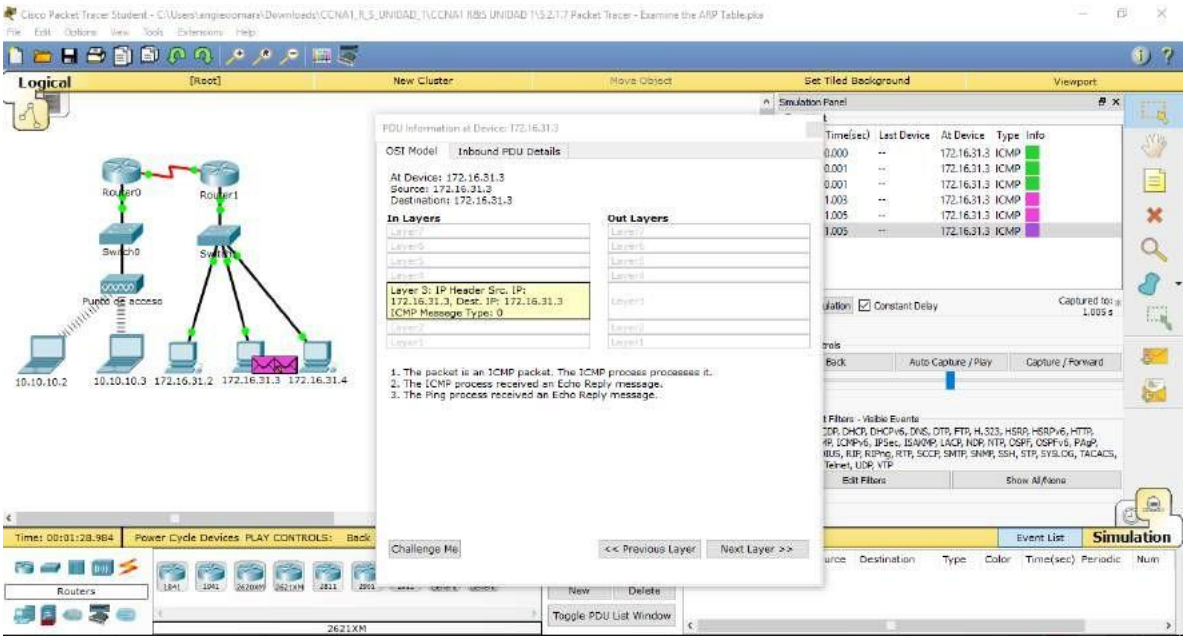
Rta 1

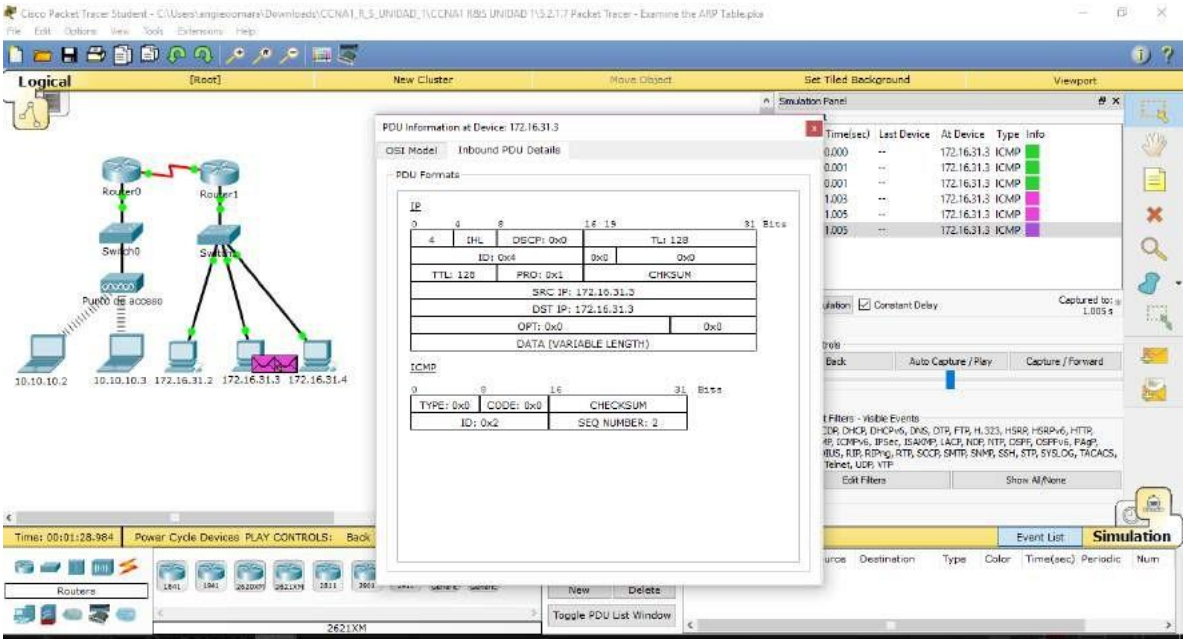


Paso 2: Revisar la tabla ARP

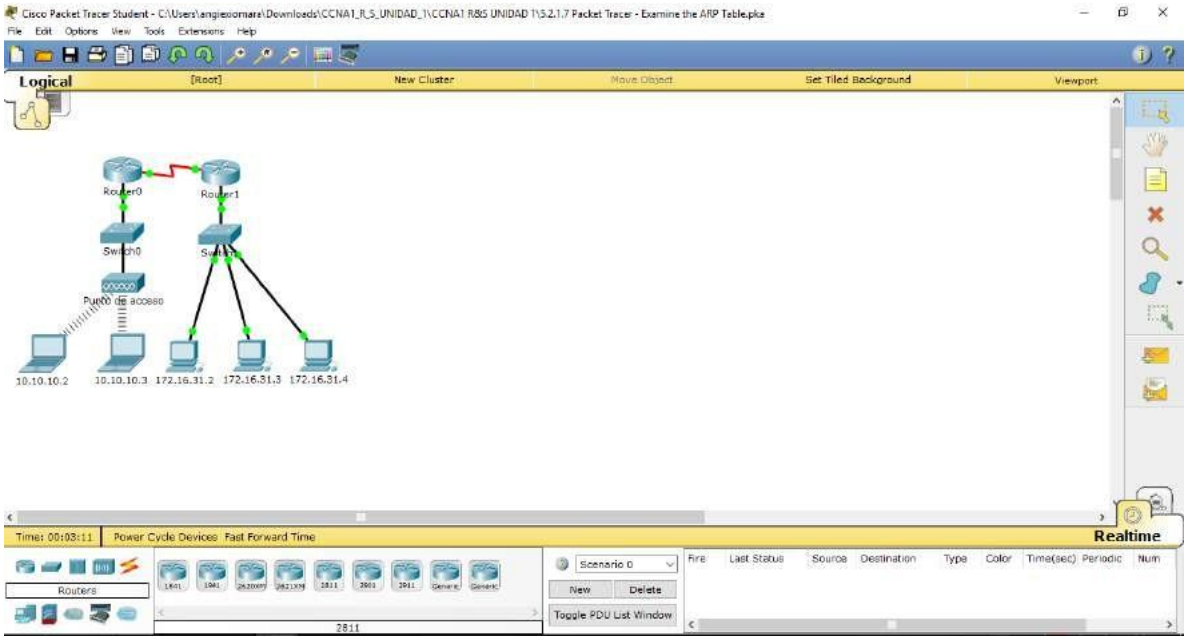
a. Observe que vuelve a aparecer el paquete ICMP. Abra la PDU y revise las direcciones MAC. ¿Las direcciones MAC de origen y destino coinciden con sus direcciones IP?

Rta Sí





b. Vuelva a cambiar al modo Realtime (Tiempo real), y el ping se completa.



c. Haga clic en 172.16.31.2 e introduzca el comando arp -a. ¿A qué dirección IP corresponde la entrada de la dirección MAC?

Rta 172.16.31.3

d. En general, ¿cuándo emite un dispositivo final una solicitud de ARP?

Rta Cuando no conoce la dirección MAC del receptor.

Parte 2:Examinar una tabla de direcciones MAC del switch

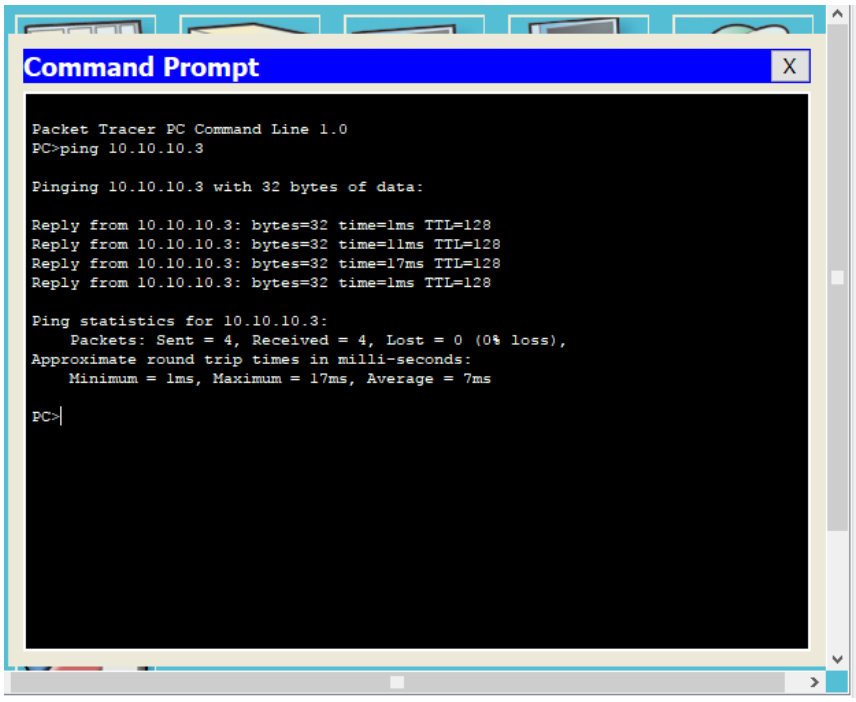
Paso 1: Generar tráfico adicional para completar la tabla de direcciones MAC del switch

a. En **172.16.31.2**, introduzca el comando **ping 172.16.31.4**.

b. Haga clic en **10.10.10.2** y abra el **símbolo del sistema**.

c. Introduzca el comando **ping 10.10.10.3**. ¿Cuántas respuestas se enviaron y se recibieron?

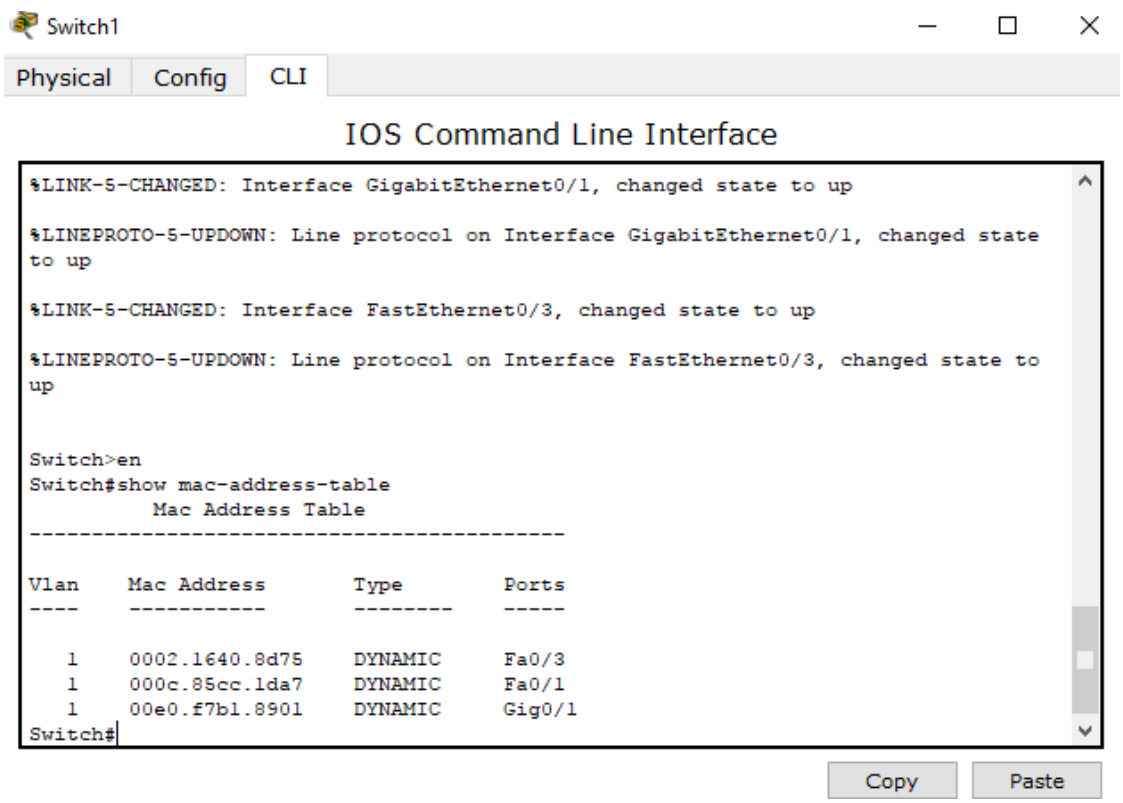
Rta: Se enviaron cuatro y se recibieron cuatro.



Paso 2: Examinar la tabla de direcciones MAC en los switches

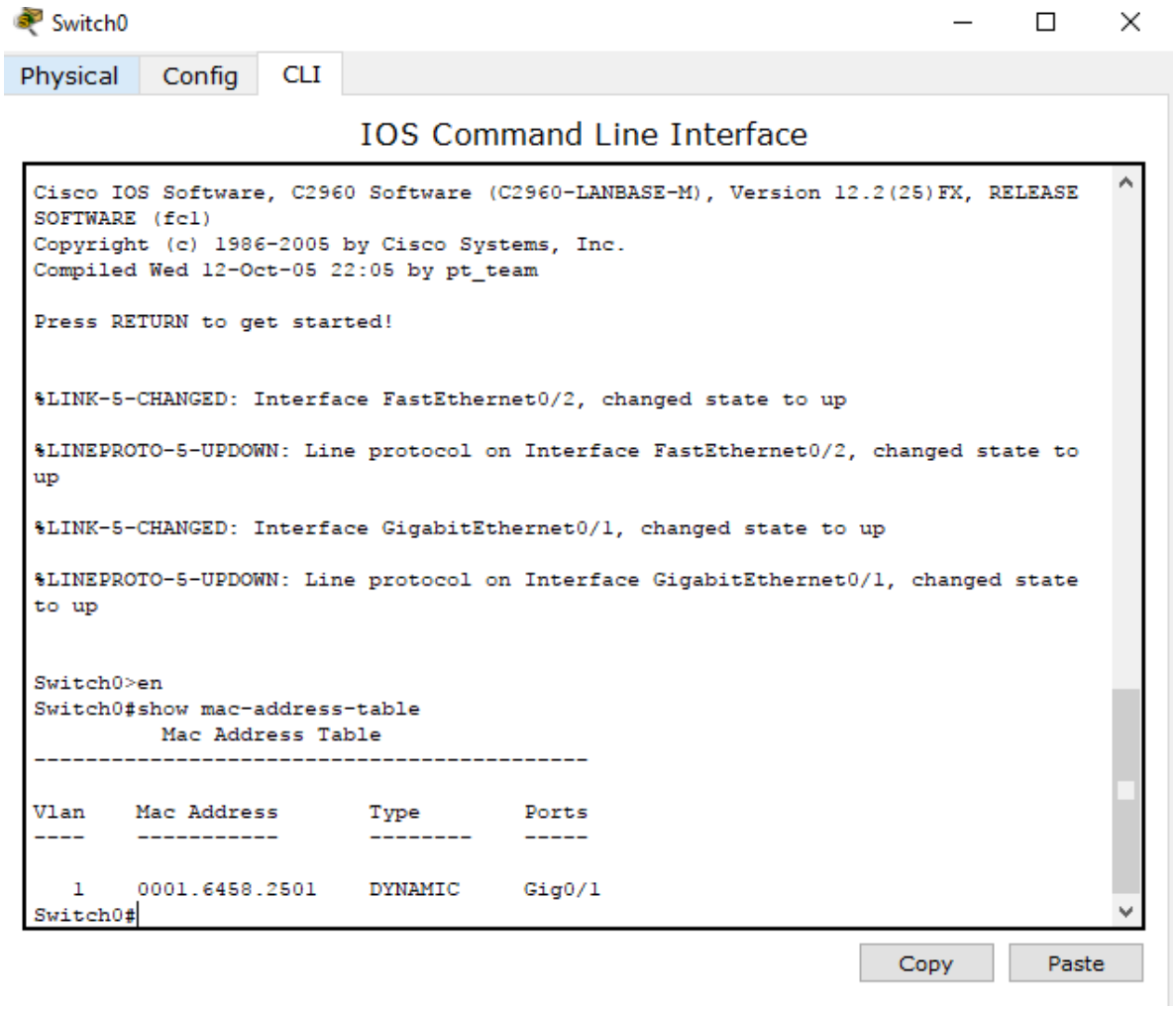
a. Haga clic en Switch1 y, a continuación, en la ficha CLI. Introduzca el comando show mac-address-table. ¿Las entradas corresponden a las de la tabla anterior?

Rta Sí



b. Haga clic en Switch0 y, a continuación, en la ficha CLI. Introduzca el comando show mac-address-table. ¿Las entradas corresponden a las de la tabla anterior?

Rta Sí



c. ¿Por qué hay dos direcciones MAC asociadas a un puerto?

Rta Porque ambos dispositivos se conectan a un puerto a través del punto de acceso.

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

a. Haga clic en 172.16.31.2 y abra el símbolo del sistema.

b. Introduzca el comando ping 10.10.10.1.

c. Escriba arp -a. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP?

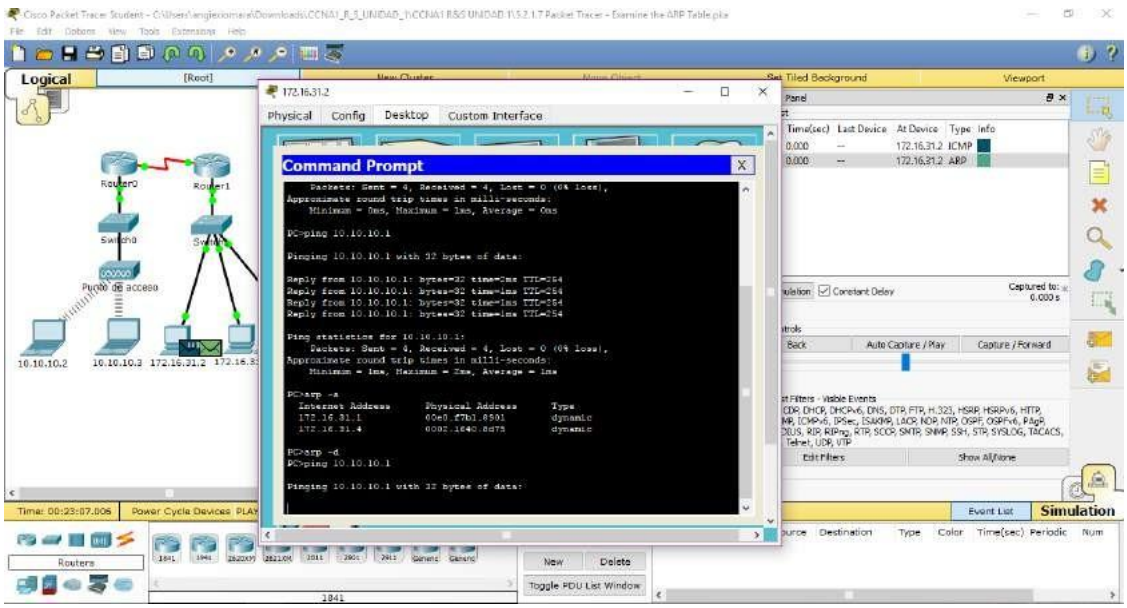
Rta 172.16.31.1

```
Command Prompt

Reply from 172.16.31.4: bytes=32 time=0ms TTL=128
Reply from 172.16.31.4: bytes=32 time=0ms TTL=128
Reply from 172.16.31.4: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.31.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=2ms TTL=254
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>arp -a
  Internet Address      Physical Address      Type
  172.16.31.1           00e0.f7b1.8901        dynamic
  172.16.31.4           0002.1640.8d75        dynamic

PC>
```

d. Introduzca el comando arp -d para borrar la tabla ARP y volver a cambiar al modo de simulación.

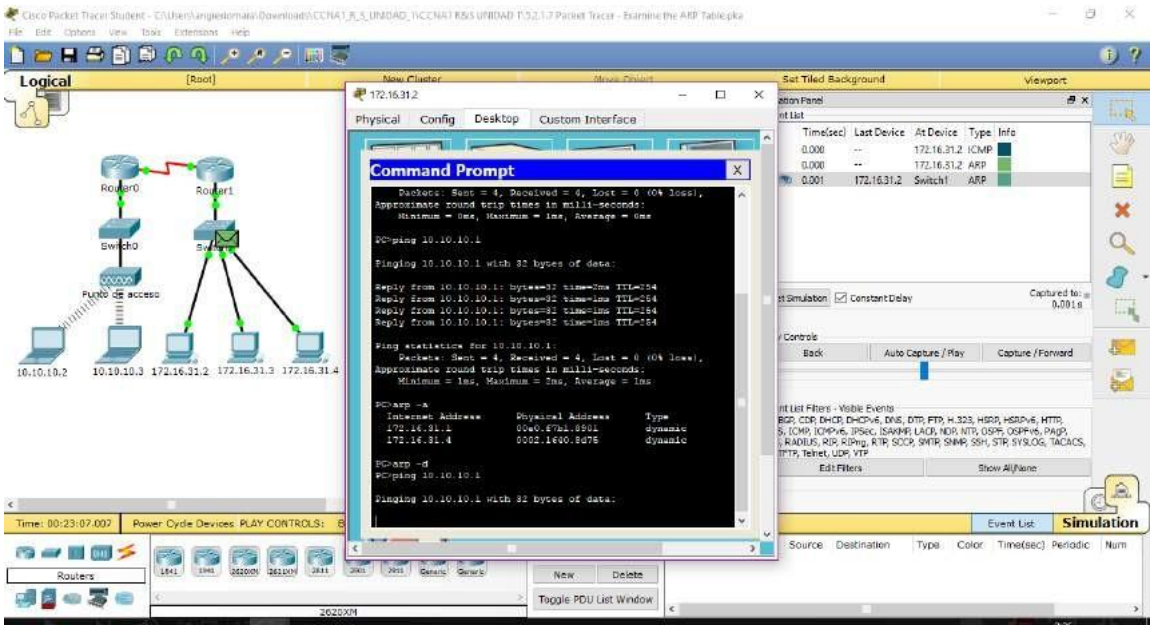
e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen?

Rta 2



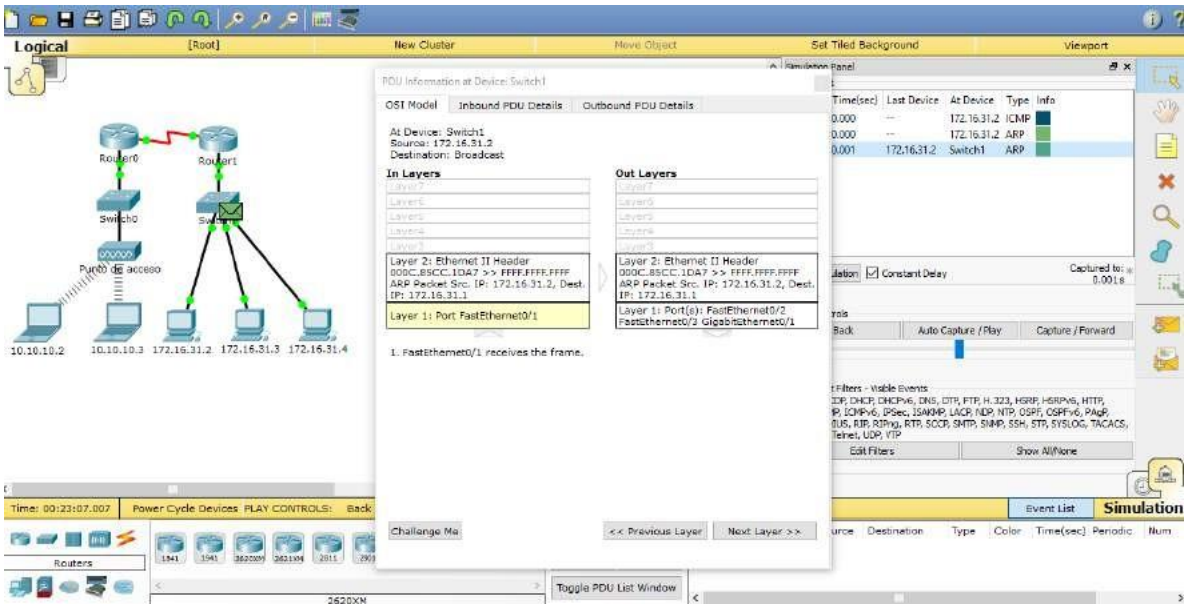
f. Haga clic en Capture/Forward (Capturar/avanzar). Haga clic en la PDU que ahora se encuentra en el Switch1. ¿Cuál es la dirección IP de destino de la solicitud de ARP?

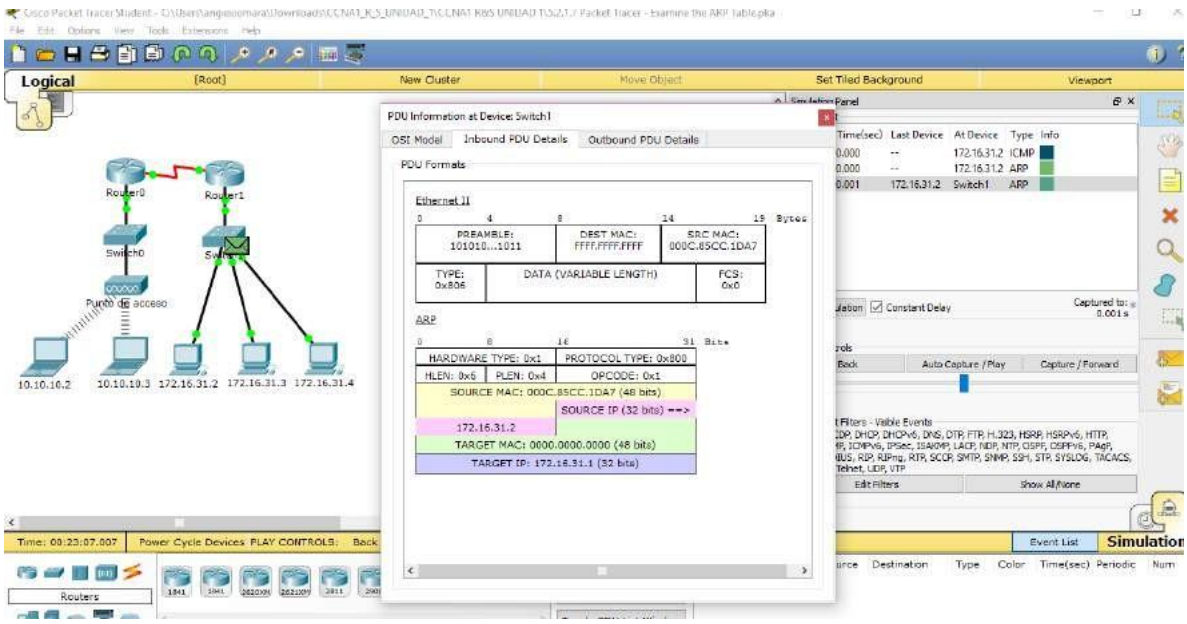
Rta 172.16.31.1



g. La dirección IP de destino no es 10.10.10.1. ¿Por qué?

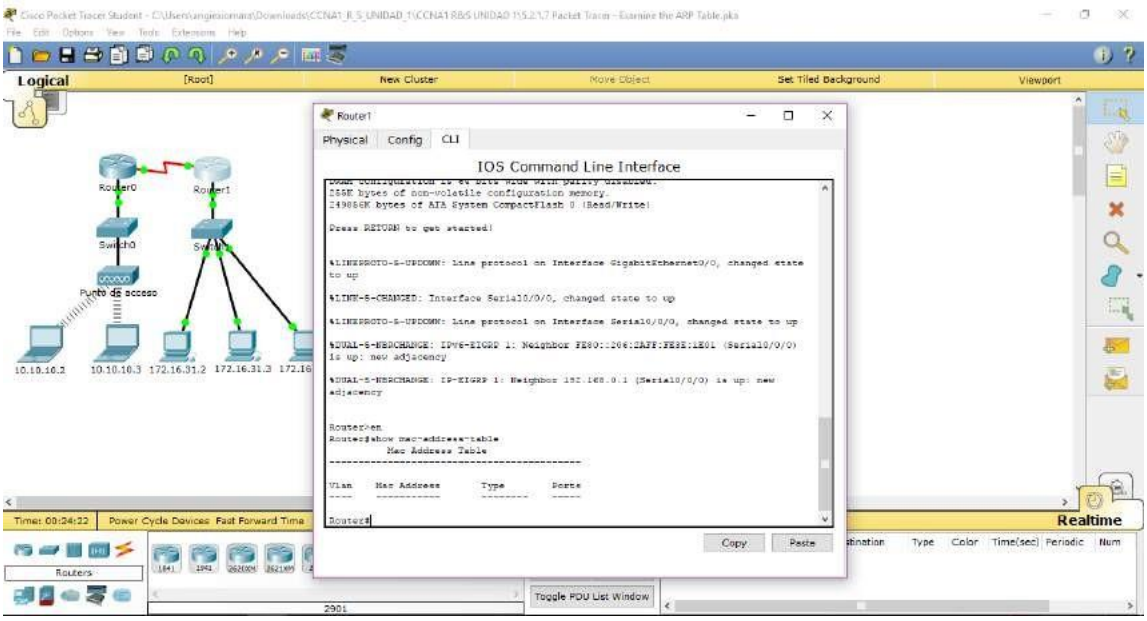
Rta La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.





Paso 2: Examinar la tabla ARP en el Router1

a. Cambie al modo Realtime. Haga clic en Router1 y, a continuación, en la ficha CLI.

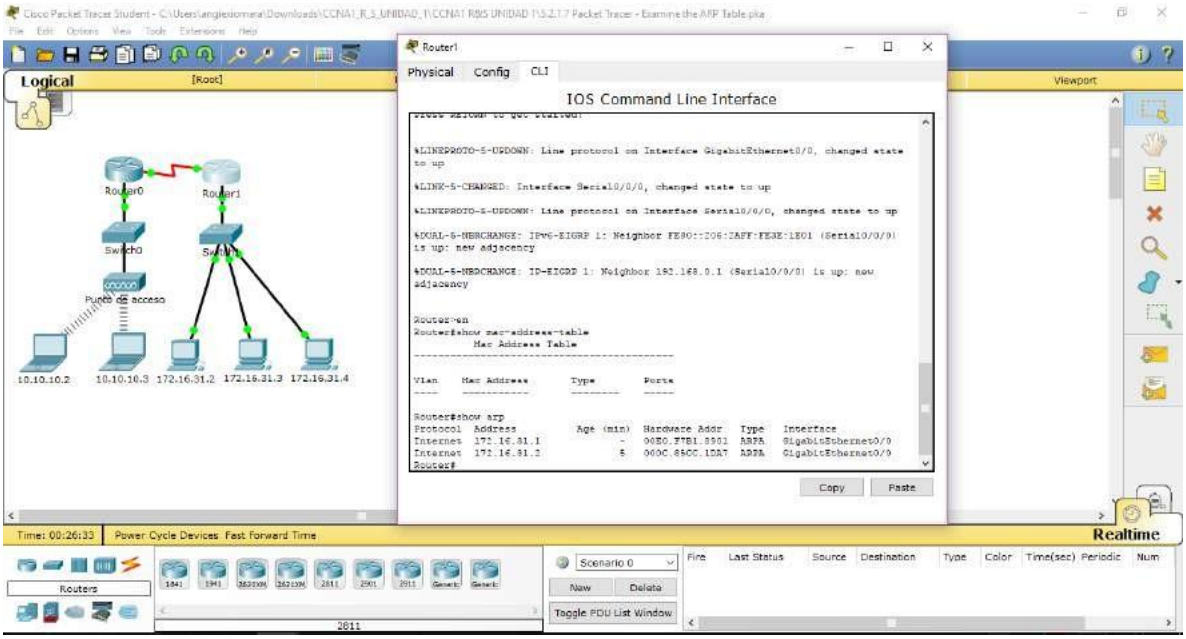


b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando show mac-address-table. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué?

Rta Ninguna, este comando significa algo totalmente distinto que el comando show mac address-table de un switch.

c. Introduzca el comando show arp. ¿Figura una entrada para 172.16.31.2?

Rta Sí



d. ¿Qué sucede con el primer ping en una situación en la que el router responde a la solicitud de ARP?

Rta Excede el tiempo de espera.

5.3.3.5 Packet Tracer - Configure Layer 3 Switches Instructions IG

Parte 1: Documentar la configuración actual de la red

Nota: por lo general, un router de producción tendría muchas más configuraciones que simplemente el direccionamiento IP de las interfaces. Sin embargo, para agilizar esta actividad, se configuró solo el direccionamiento IP de interfaces en R1.

a. Haga clic en R1 y, a continuación, haga clic en la ficha CLI.

b. Utilice los comandos disponibles para recopilar información sobre el direccionamiento de interfaces.

c. Registre la información en la tabla de direccionamiento.

```
Router>enable
Router#show run
Building configuration...

Current configuration : 903 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX152422VM
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet0/0
ip address 172.16.31.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.0.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
```

```
shutdown
!
interface Serial0/0/0
no ip address
encapsulation ppp
clock rate 2000000
shutdown
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
      end
```

Parte 2: Configurar, implementar y probar el nuevo switch multicapa

Paso 1: Configurar MLSw1 para utilizar el esquema de direccionamiento de R1

a. Haga clic en MLSw1 y, a continuación, en la ficha CLI.
b. Ingrese al modo de configuración de interfaz para GigabitEthernet 0/1.
c. Cambie el puerto al modo de enrutamiento introduciendo el comando no switchport.

d. Configure la dirección IP para que sea la misma que la dirección de R1 GigabitEthernet 0/1 y active el puerto.
e. Ingrese al modo de configuración de interfaz para interface VLAN1.
f. Configure la dirección IP para que sea la misma que la dirección de R1 GigabitEthernet 0/0 y active el puerto.
g. Guarde la configuración.

```
CLEI Code Number                 : COM1100ARC
Hardware Board Revision Number   : 0x01


Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C3560-24PS      12.2(37)SE1           C3560-ADVIPSERVICESK

Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

Press RETURN to get started!


Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.0.2 255.255.255.0
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to down
Switch(config-if)#no shutdown
Switch(config-if)#interface VLan1
Switch(config-if)#ip address 172.16.31.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
Switch#
```

Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

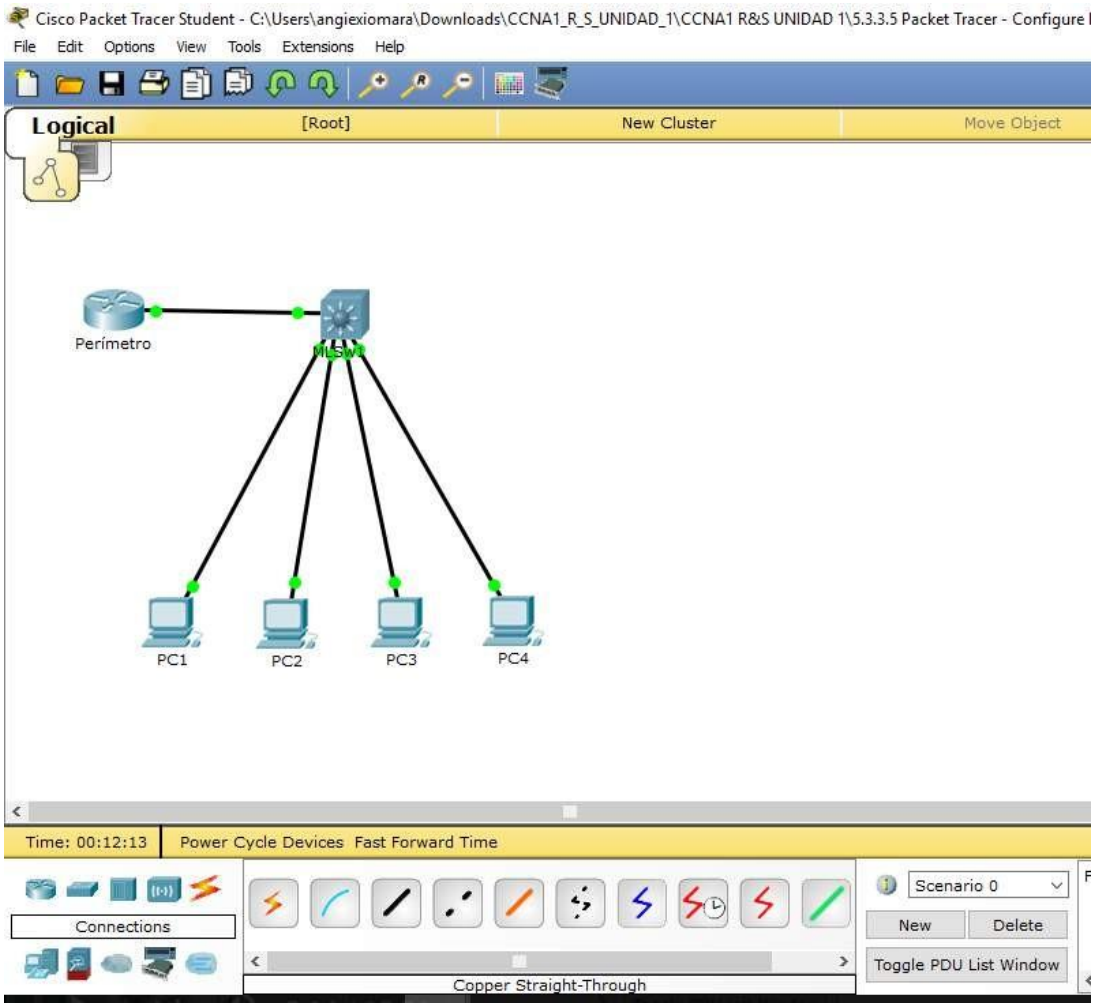
Nota: por lo general, los siguientes pasos se llevarían a cabo después del horario laboral o cuando el tráfico en la red de producción está en su volumen más bajo. Para minimizar el

tiempo de inactividad, el nuevo equipo debe estar totalmente configurado y listo para implementar.

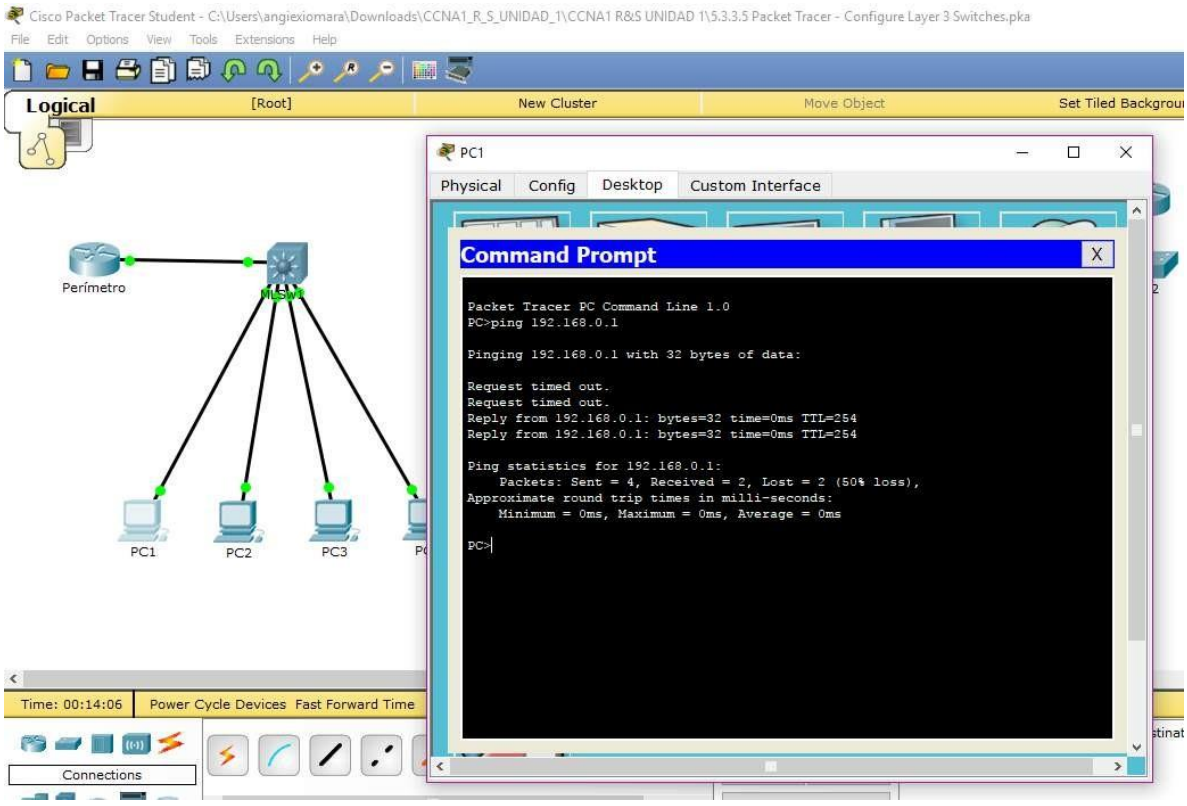
a. Haga clic en un área vacía de la pantalla para anular la selección de todos los dispositivos.

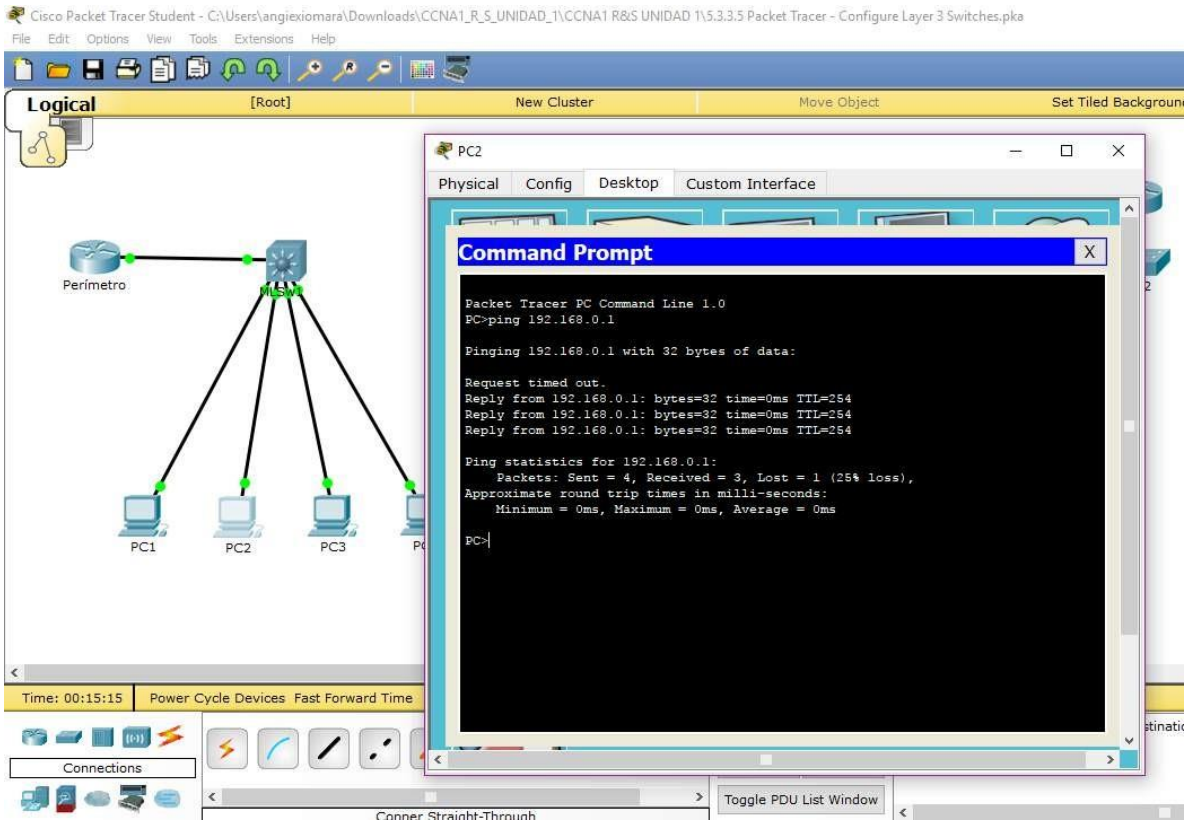
b. Use la herramienta Delete (Eliminar) para eliminar todas las conexiones o simplemente elimine R1, S1 y S2.

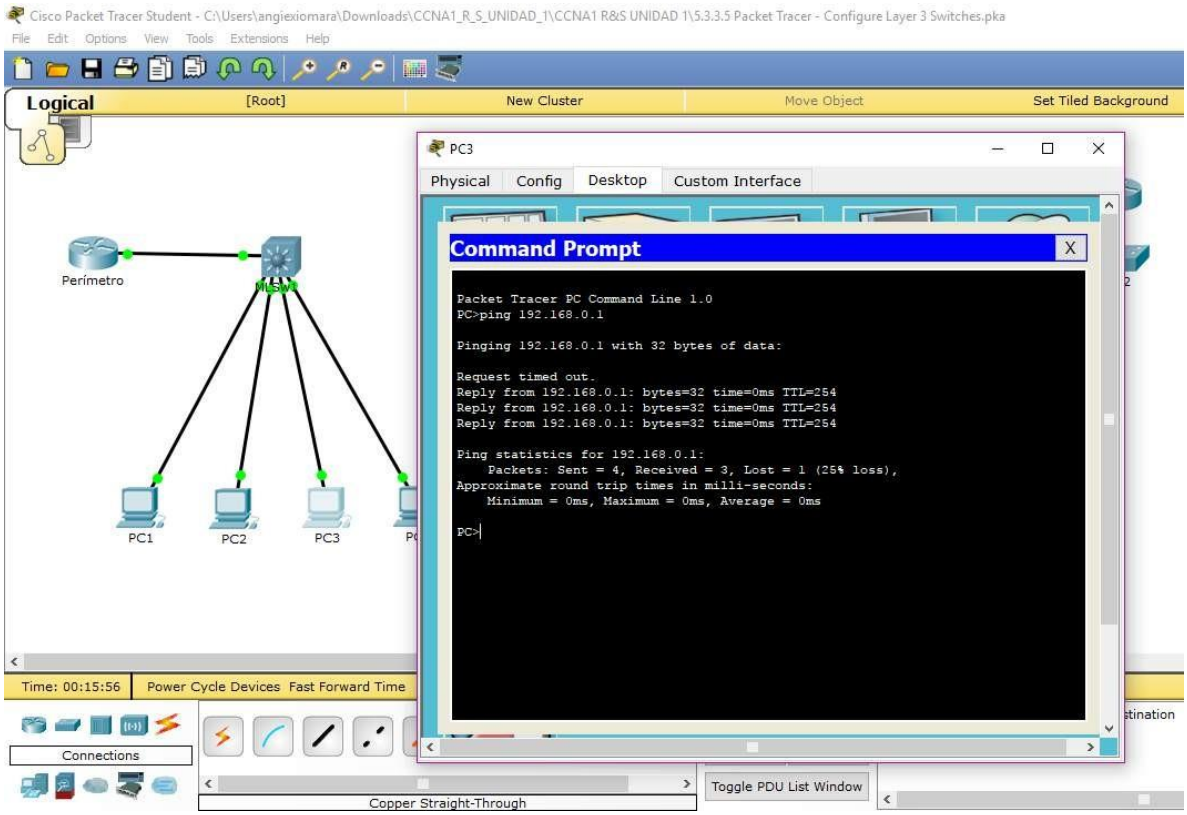
c. Seleccione los cables adecuados para completar lo siguiente: - Conectar MLSw1 GigabitEthernet 0/1 a Edge GigabitEthernet 0/0. - Conectar las PC a los puertos Fast Ethernet en MLSw1.

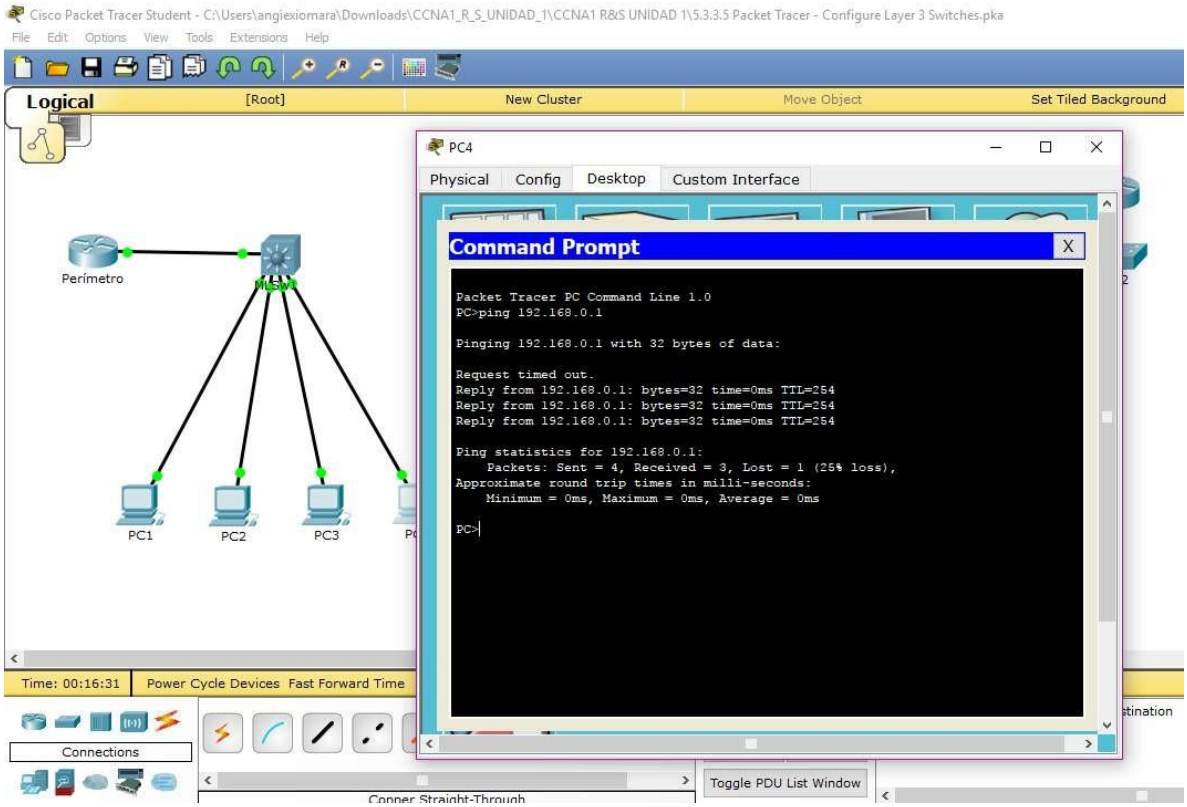


d. Verifique que todas las PC puedan hacer ping a Edge en 192.168.0.1. Nota: espere hasta que las luces de enlace anaranjadas cambien a color verde.


Cisco Packet Tracer Student - C:\Users\angiexiomara\Downloads\CCNA1_R_S_UNIDAD_1\CCNA1 R&S UNIDAD 1\5.3.3.5 Packet Tracer - Configure Layer 3 Switches.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Backgrou
Perímetro
MLS-3
PC1
PC2
PC3
Time: 00:14:06
Power Cycle Devices Fast Forward Time
Connections
PC1
Physical Config Desktop Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

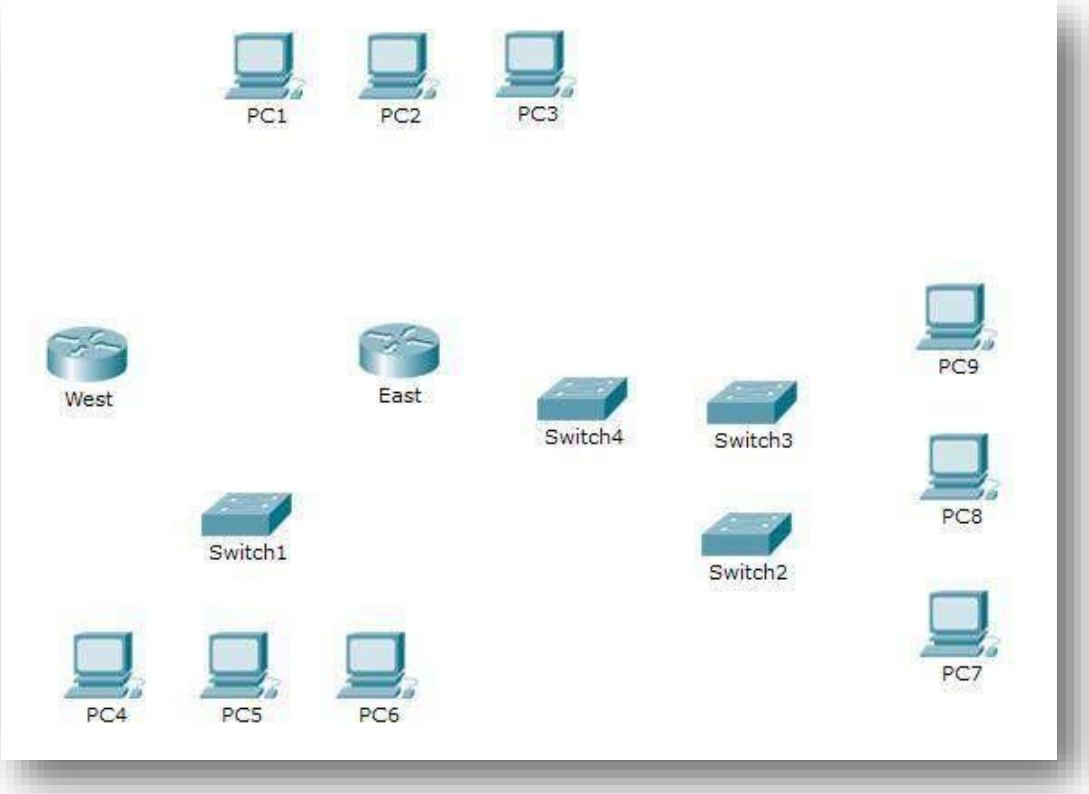

Cisco Packet Tracer Student - C:\Users\angiexiomara\Downloads\CCNA1_R_S_UNIDAD_1\CCNA1 R&S UNIDAD 1\5.3.3.5 Packet Tracer - Configure Layer 3 Switches.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Perímetro
MLS-3
PC1
PC2
PC3
Time: 00:15:15
Power Cycle Devices Fast Forward Time
Connections
Toggle PDU List Window
PC2
Physical Config Desktop Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>


Cisco Packet Tracer Student - C:\Users\angiexiomara\Downloads\CCNA1_R_S_UNIDAD_1\CCNA1 R&S UNIDAD 1\5.3.3.5 Packet Tracer - Configure Layer 3 Switches.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Perímetro
PC1
PC2
PC3
PC3
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>
Time: 00:15:56
Power Cycle Devices
Fast Forward Time
Connections
Copper Straight-Through
Toggle PDU List Window


Cisco Packet Tracer Student - C:\Users\angiexiomara\Downloads\CCNA1_R_S_UNIDAD_1\CCNA1 R&S UNIDAD 1\5.3.3.5 Packet Tracer - Configure Layer 3 Switches.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Perímetro
PC1
PC2
PC3
PC4
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>
Time: 00:16:31
Power Cycle Devices
Fast Forward Time
Connections
Toggle PDU List Window

6.3.1.10 Packet Tracer - Exploring Internetworking Devices Instructions IG

Topología



Objetivos

Parte 1: Identificar las características físicas de los dispositivos de internetworking
Parte 2: Seleccionar los módulos correctos para la conectividad
Parte 3: Conectar los dispositivos

Información básica

En esta actividad, explorará las diversas opciones disponibles en los dispositivos de internetworking. También deberá determinar qué opciones proporcionan la conectividad necesaria al conectar varios dispositivos. Finalmente, agregará los módulos correctos y conectará los dispositivos.

Nota: la calificación de esta actividad es una combinación de la puntuación automatizada de Packet Tracer y las respuestas que registró para las preguntas que se formularon en las instrucciones. Consulte la Tabla de calificación sugerida que se encuentra al final de esta actividad y consulte al instructor para determinar su puntuación final.

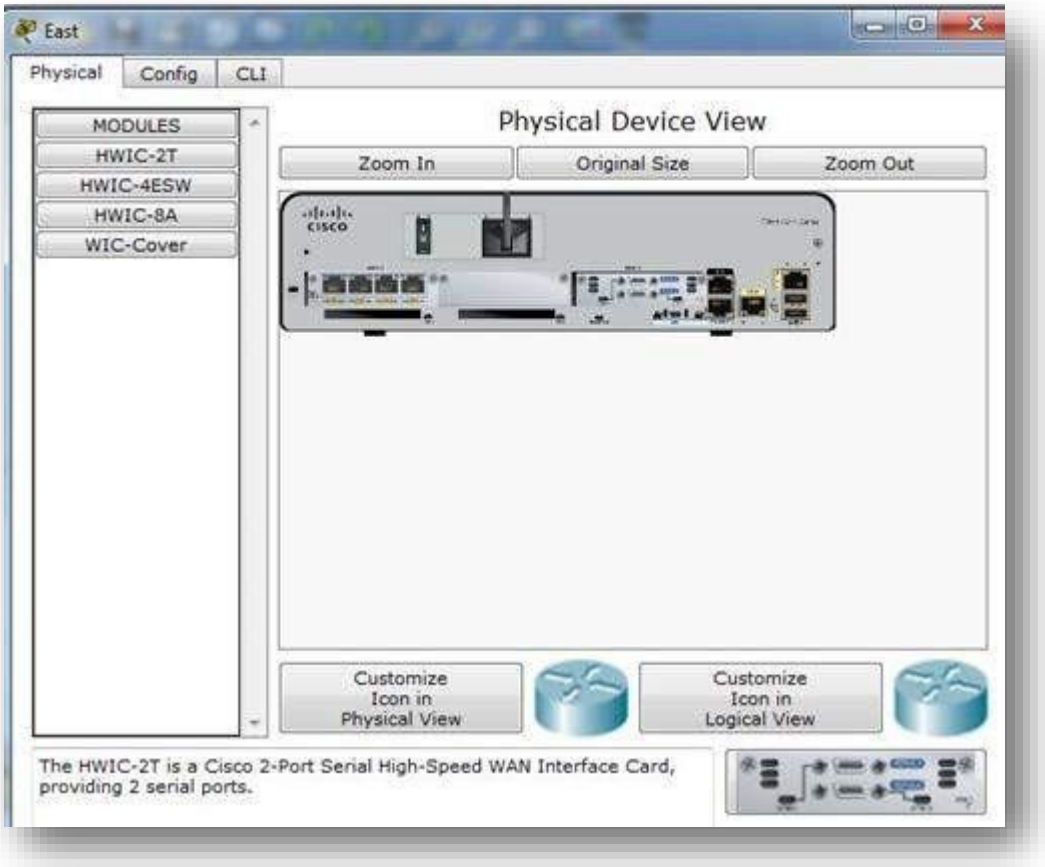
Parte 1: Identificar las características físicas de los dispositivos de internetworking

Paso 1: Identificar los puertos de administración de un router Cisco

a. Haga clic en el router **East** (Este). La ficha **Physical** (Capa física) debe estar activa.

b. Acerque el elemento y expanda la ventana para ver todo el router.

c. ¿Qué puertos de administración se encuentran disponibles? Los puertos auxiliar y de consola



Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay?

Hay dos interfaces WAN y dos interfaces Gigabit Ethernet.

b. Haga clic en la ficha **CLI** e introduzca los siguientes comandos:

East> **show ip interface brief**

El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican? 4

c. Introduzca los siguientes comandos:

East> **show interface gigabitethernet 0/0**

¿Cuál es el ancho de banda predeterminado de esta interfaz? 1 000 000 Kbit

East> ***show interface serial 0/0/0***

¿Cuál es el ancho de banda predeterminado de esta interfaz? 1544 Kbit

```
East>show interface serial 0/0/0
Serial0/0/0 is down, line protocol is down (disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

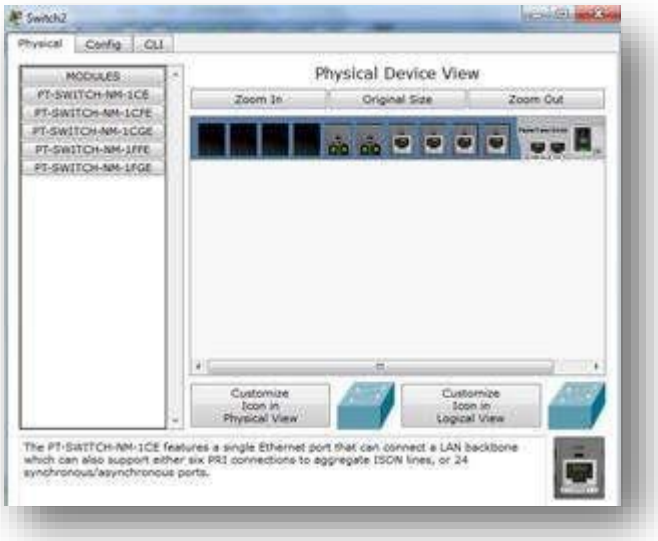
Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

Paso 3: Identificar las ranuras de expansión de módulos en los switches

a. ¿Cuántas ranuras de expansión se encuentran disponibles para agregar más módulos al router **East**? 1 ranura

b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles?

Cada uno tiene cinco ranuras disponibles.



Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

a. Haga clic en **East** y, a continuación, haga clic en la ficha **Physical**. En el lado izquierdo, debajo de la etiqueta **Modules** (Módulos), se ven las opciones disponibles para expandir las capacidades del router. Haga clic en cada módulo. Se muestra una imagen y una descripción en la parte inferior. Familiarícese con estas opciones.

1) Debe conectar las PC 1, 2 y 3 al router **East**, pero no cuenta con los fondos necesarios para adquirir un nuevo switch. ¿Qué módulo puede usar para conectar las tres PC al router **East**?

Módulo HWIC-4ESW

2) ¿Cuántos hosts puede conectar al router mediante este módulo?
4

b. Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**?
PT-SWITCH-NM-1FGE

Paso 2: Agregar los módulos correctos y encender los diapositivos

a. Haga clic en **East** e intente insertar el módulo adecuado del paso 1a.

c. Debe aparecer el mensaje Cannot add a module when the power is on (No se puede agregar un módulo cuando el dispositivo está encendido). Las interfaces para este modelo de router no son intercambiables en caliente. Se debe apagar el dispositivo. Haga clic en el interruptor de alimentación que se encuentra a la derecha del logotipo de Cisco para apagar **East**. Inserte el módulo adecuado del paso 1a. Cuando haya terminado, haga clic en el interruptor de alimentación para encender **East**.

Nota: si inserta el módulo incorrecto y debe quitarlo, arrastre el módulo hasta su imagen en la esquina inferior derecha y suelte el botón del mouse.

d. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

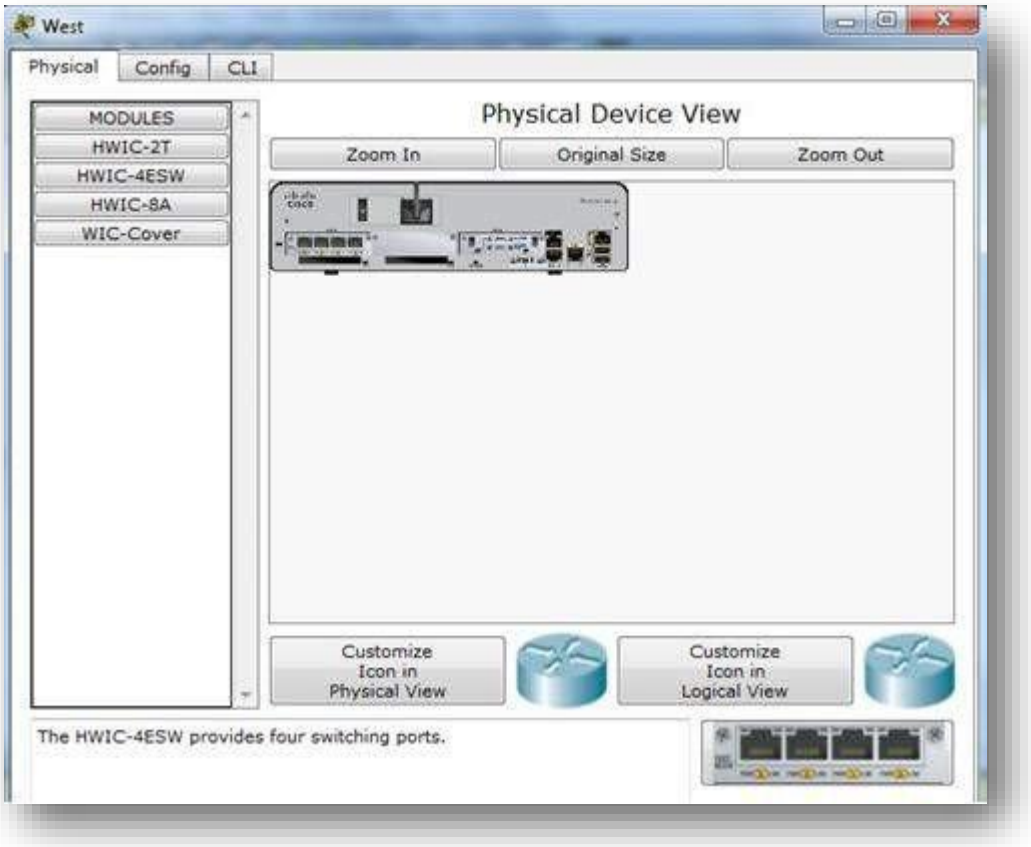
e. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo. ¿En qué ranura se insertó?

GigabitEthernet5/1

e. Haga clic en el router **West** (Oeste). La ficha **Physical** (Capa física) debe estar activa.

Instale el módulo adecuado que agregará una interfaz serial a la ranura para tarjetas de interfaz WAN de alta velocidad mejoradas (**EHWIC 0**) de la derecha. Puede cubrir las ranuras sin utilizar para evitar que ingrese polvo al router (optativo).

c. Use el comando adecuado para verificar que se hayan instalado las nuevas interfaces seriales.



Parte 3: Conectar los dispositivos

Esta puede ser la primera actividad que realiza en la que se le solicita conectar dispositivos. Si bien es posible que no conozca el propósito de los distintos tipos de cables, use la tabla que se encuentra a continuación y siga estas pautas para conectar correctamente todos los dispositivos:

a. Seleccione el tipo de cable adecuado.

b. Haga clic en el primer dispositivo y seleccione la interfaz especificada.

c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.

d. Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

Ejemplo: para conectar **East** al **Switch1**, seleccione el tipo de cable de **cobre de conexión directa**. Haga clic en **East** y elija **GigabitEthernet0/0**. Luego, haga clic en **Switch1** y elija **GigabitEthernet0/1**. Su puntuación ahora debe ser de 4/52.

Nota: a los efectos de esta actividad, se deshabilitaron las luces de enlace. Los dispositivos no están configurados con ningún direccionamiento IP, de modo que no puede probar la conectividad.

Dispositivo	**Interfaz**	**Tipo de cable**	**Dispositivo**	**Interfaz**
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0

Switch1	FastEthernet0/1	Cable de cobre de conexión directa	PC4	FastEthernet0
Switch1	FastEthernet0/2	Cable de cobre de conexión directa	PC5	FastEthernet0
Switch1	FastEthernet0/3	Cable de cobre de conexión directa	PC6	FastEthernet0
Switch4	GigabitEthernet0/2	Cross-Over de cobre	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fibra	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Cable de cobre de conexión directa	PC7	FastEthernet0
Switch2	FastEthernet1/1	Cable de cobre de conexión directa	PC8	FastEthernet0
Switch2	FastEthernet2/1	Cable de cobre de conexión directa	PC9	FastEthernet0
East	Serial0/0/0	DCE serial (conectar primero a East)	West	Serial0/0/0

6.4.1.2 Packet Tracer - Configure Initial Router Settings Instructions IG

Topología

Objetivos:

Parte 1: Verificar la configuración predeterminada del router
Parte 2: Configurar y verificar la configuración inicial del router
Parte 3: Guardar el archivo de configuración en ejecución

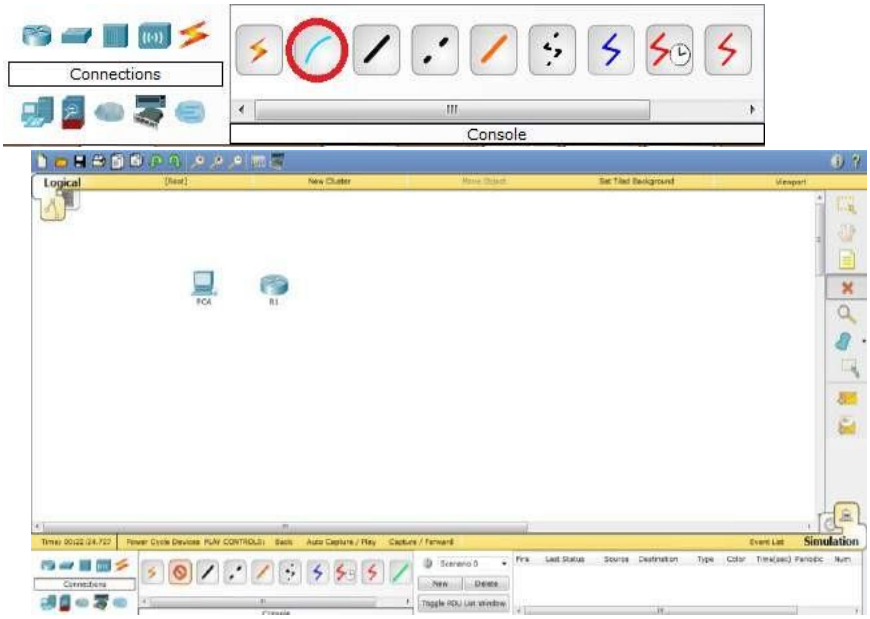
Información básica

En esta actividad, configurará los parámetros básicos del router. Proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También configurará mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten a los usuarios no autorizados que el acceso está prohibido. Finalmente, verificará y guardará la configuración en ejecución.

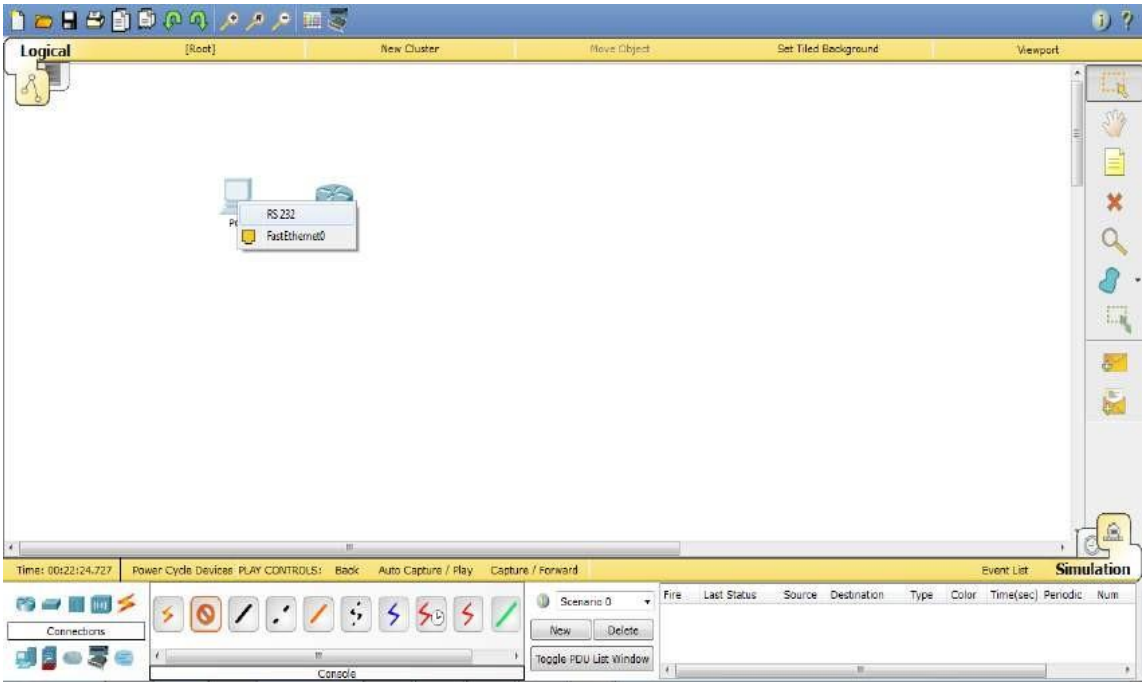
Parte 1: Verificar la configuración predeterminada del router

Paso 1: Establecer una conexión de consola al R1

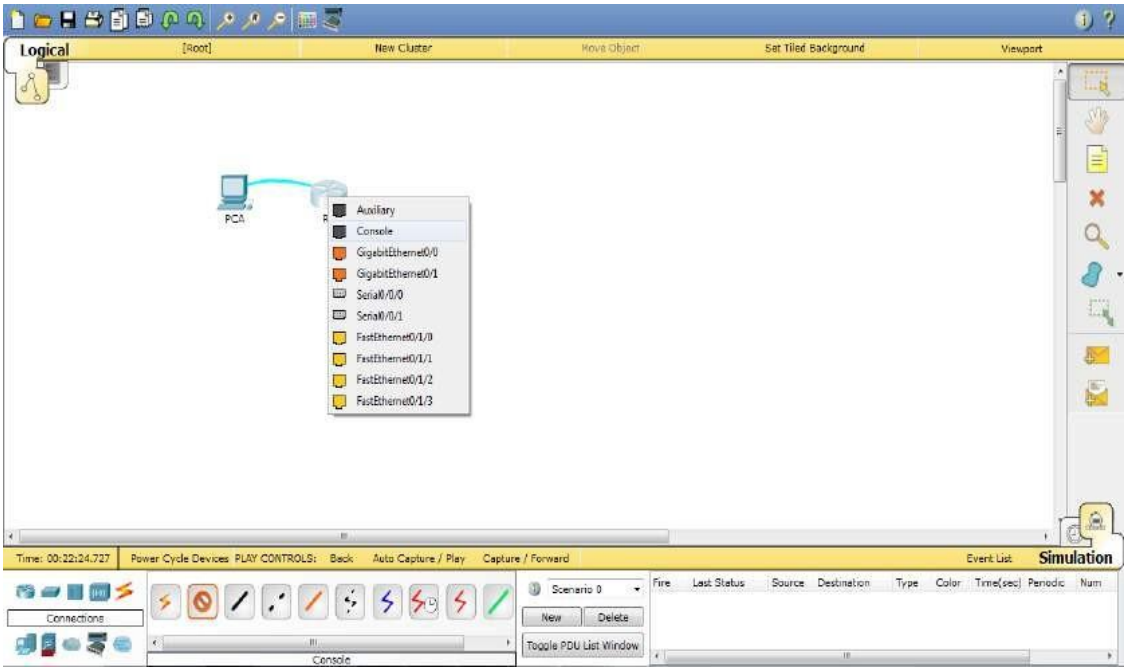
a. Elija un cable de consola de las conexiones disponibles.



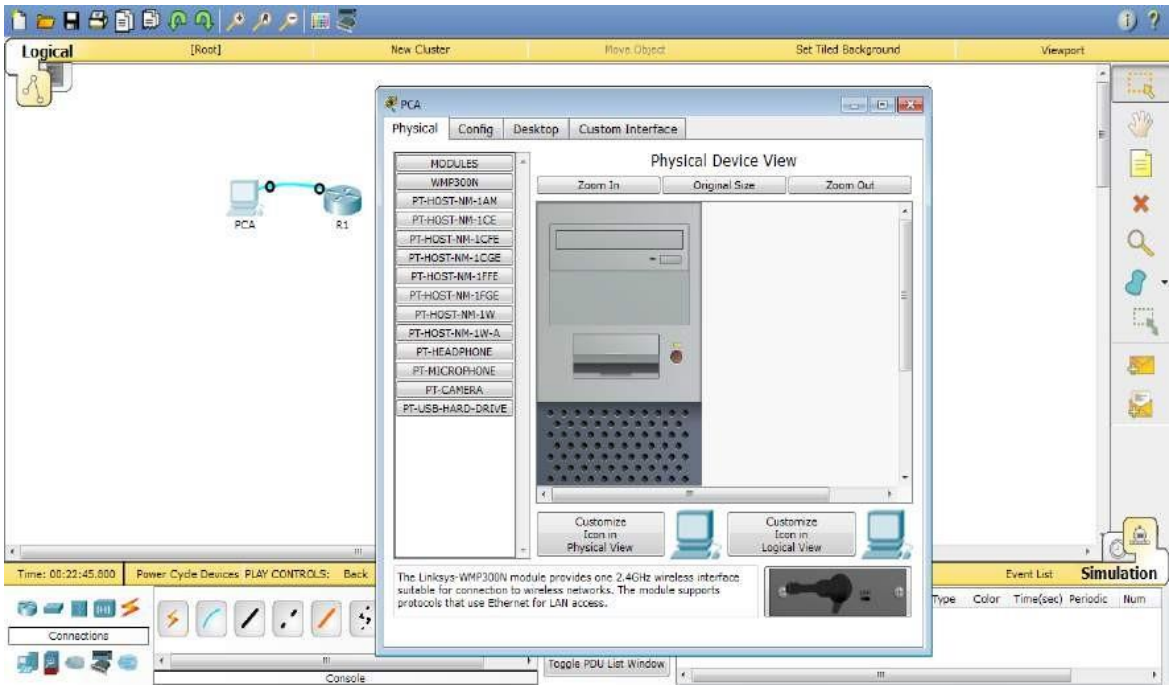
b. Haga clic en PCA y seleccione RS 232.

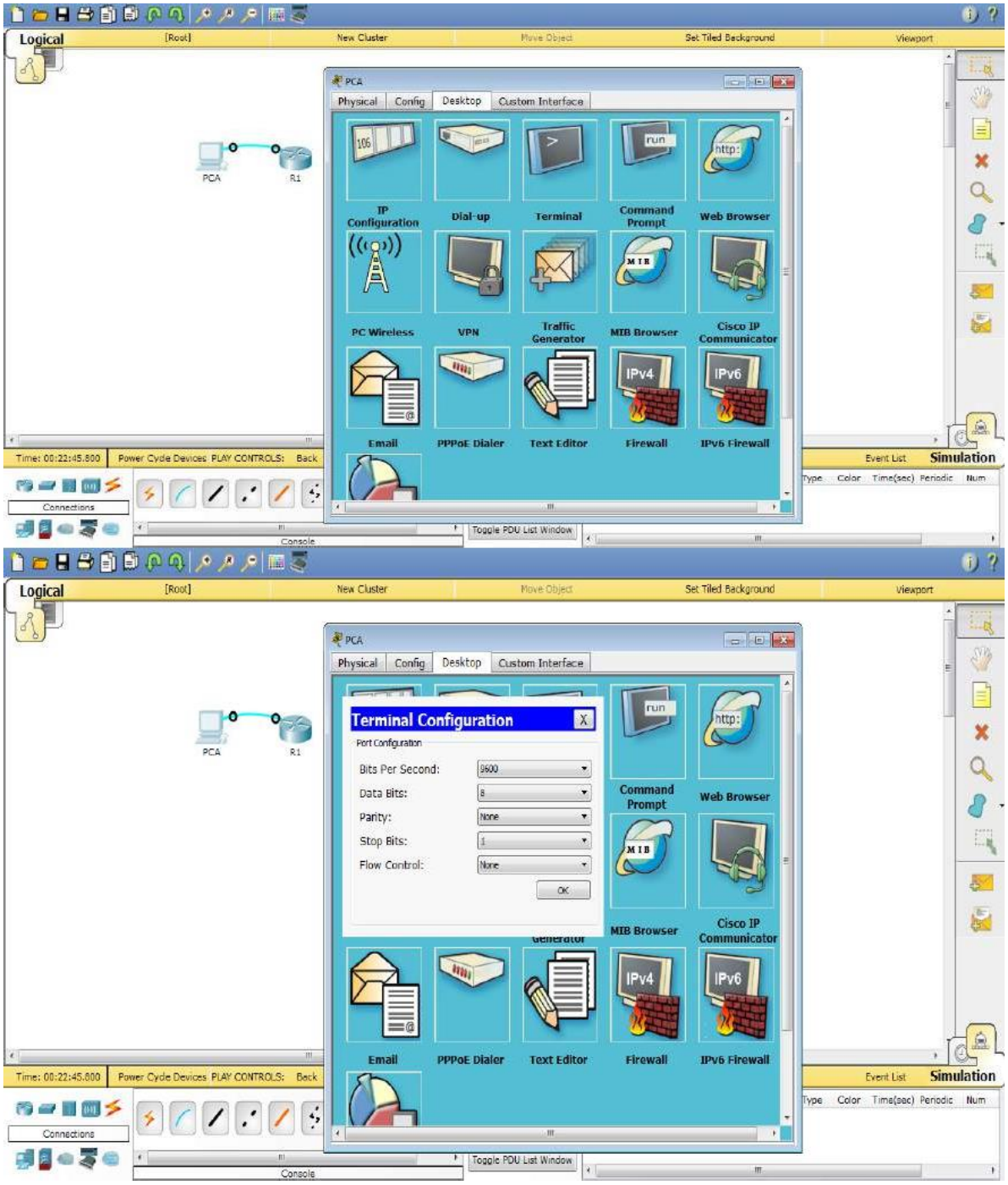


c. Haga clic en R1 y seleccione Console (Consola).

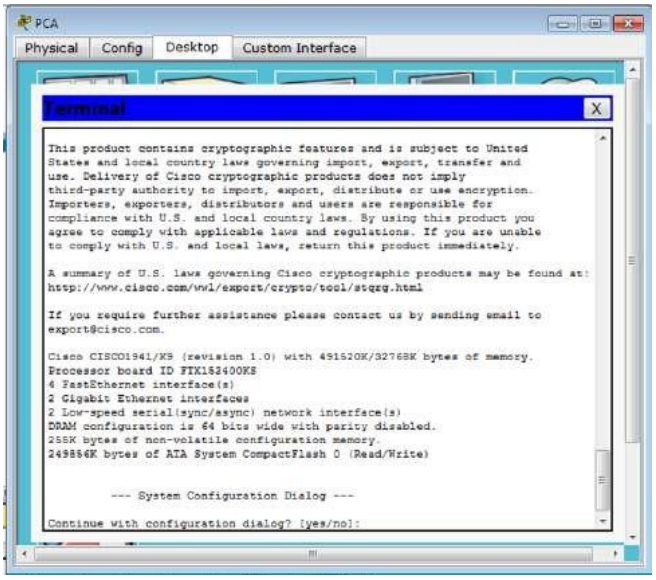


d. Haga clic en PCA > ficha Desktop (Escritorio) > Terminal.





e. Haga clic en OK (Aceptar) y presione Entrar. Ahora puede configurar R1.



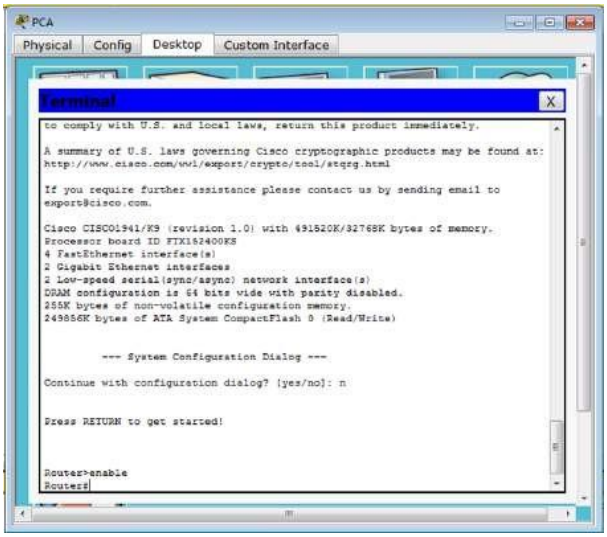
Paso 2: Ingresar al modo privilegiado y examinar la configuración actual

Puede acceder a todos los comandos del router en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

a. Introduzca el modo EXEC privilegiado introduciendo el comando enable.

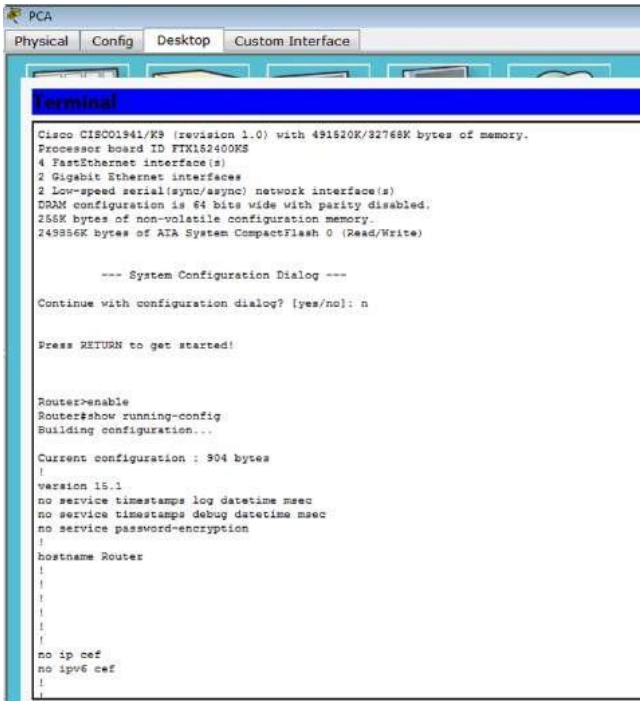
Router> **enable**
Router#

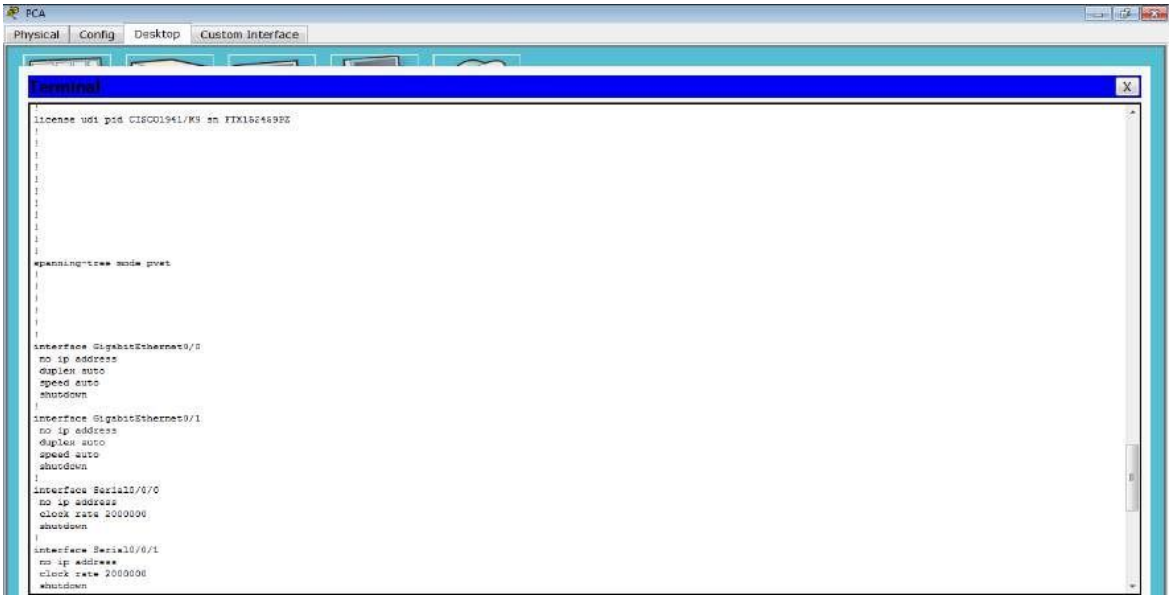
Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

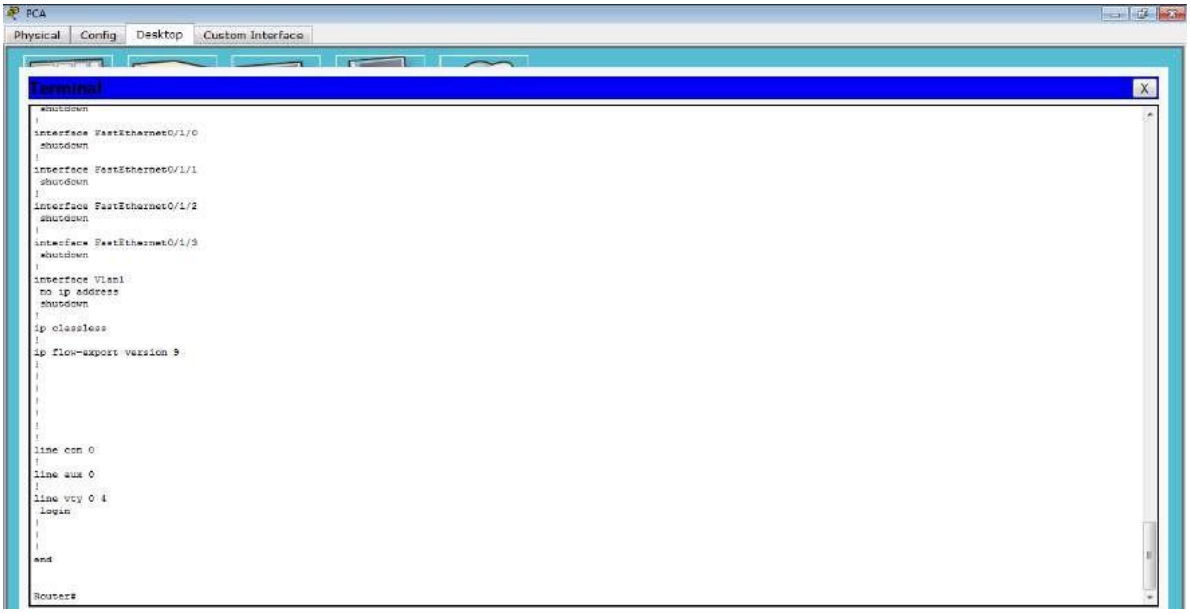


b. Introduzca el comando show running-config:

running-config:
Router# **show running-config**







c. Responda las siguientes preguntas:

¿Cuál es el nombre de host del router? R/ Router

¿Cuántas interfaces Fast Ethernet tiene el router? R/ 4

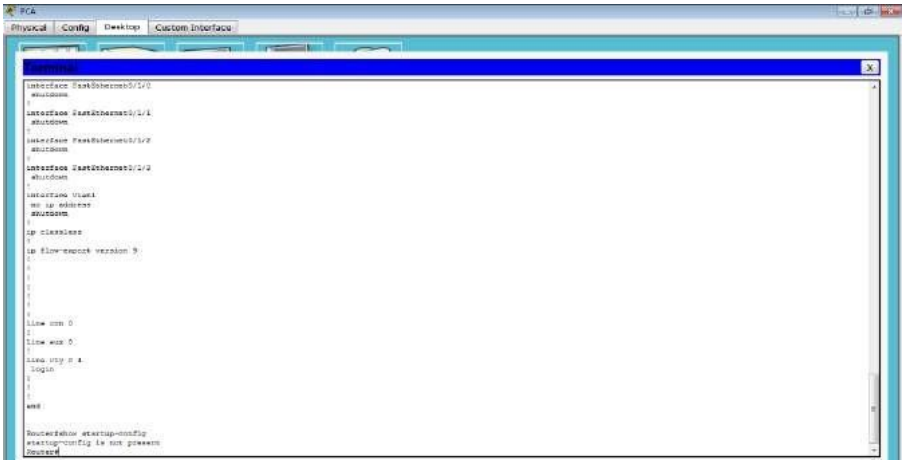
¿Cuántas interfaces Gigabit Ethernet tiene el router? R/ 2

¿Cuántas interfaces seriales tiene el router? R/ 2

¿Cuál es el rango de valores que se muestra para las líneas vty? R/ 0-4

d. Muestre el contenido actual de la NVRAM.

Router# show startup-config
Startup-config is not present



¿Por qué el router responde con el mensaje startup-config is not present?

R/ Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.

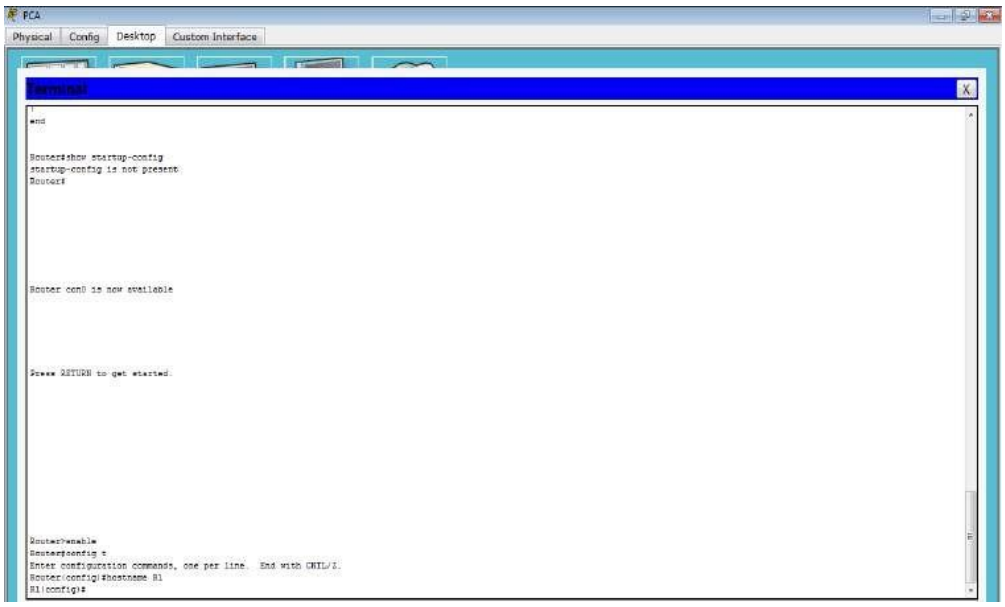
Parte 2: Configurar y verificar la configuración inicial del router

Para configurar los parámetros de un router, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el router.

Paso 1: Configurar los parámetros iniciales de R1

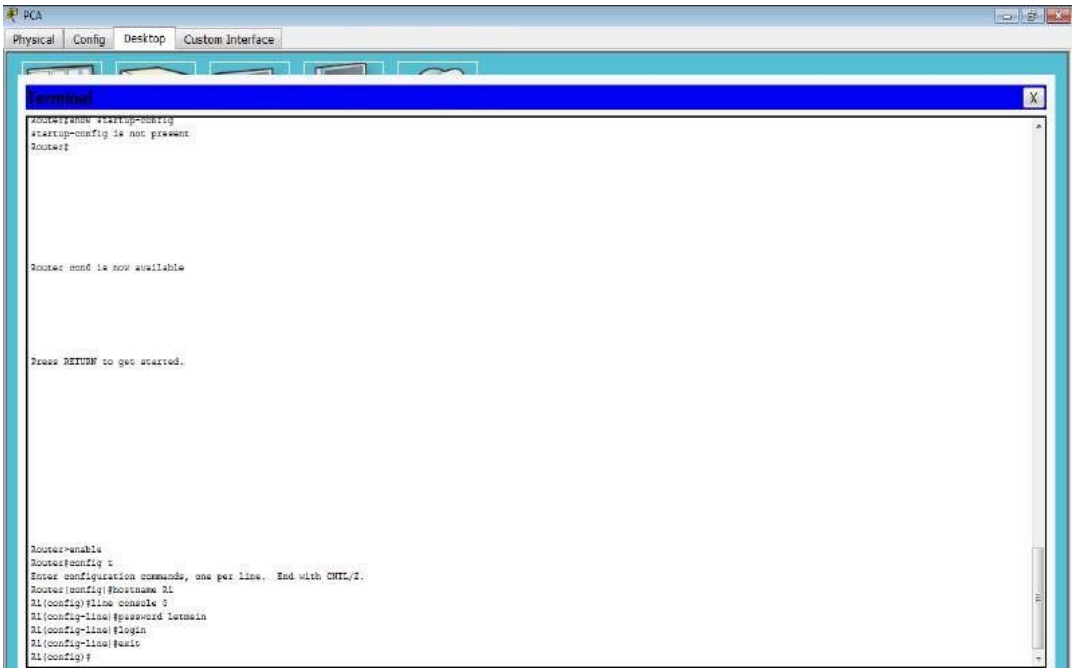
Nota: si tiene dificultad para recordar los comandos, consulte el contenido de este tema. Los comandos son los mismos que configuró en un switch.

a. Establezca R1 como nombre de host.

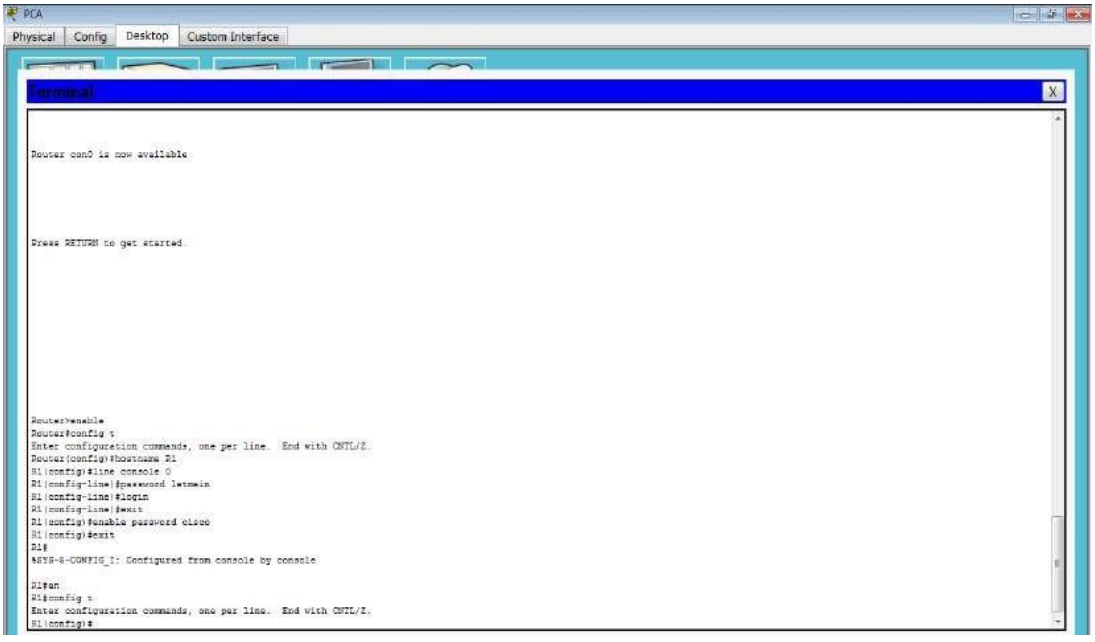


b. Utilice las siguientes contraseñas:

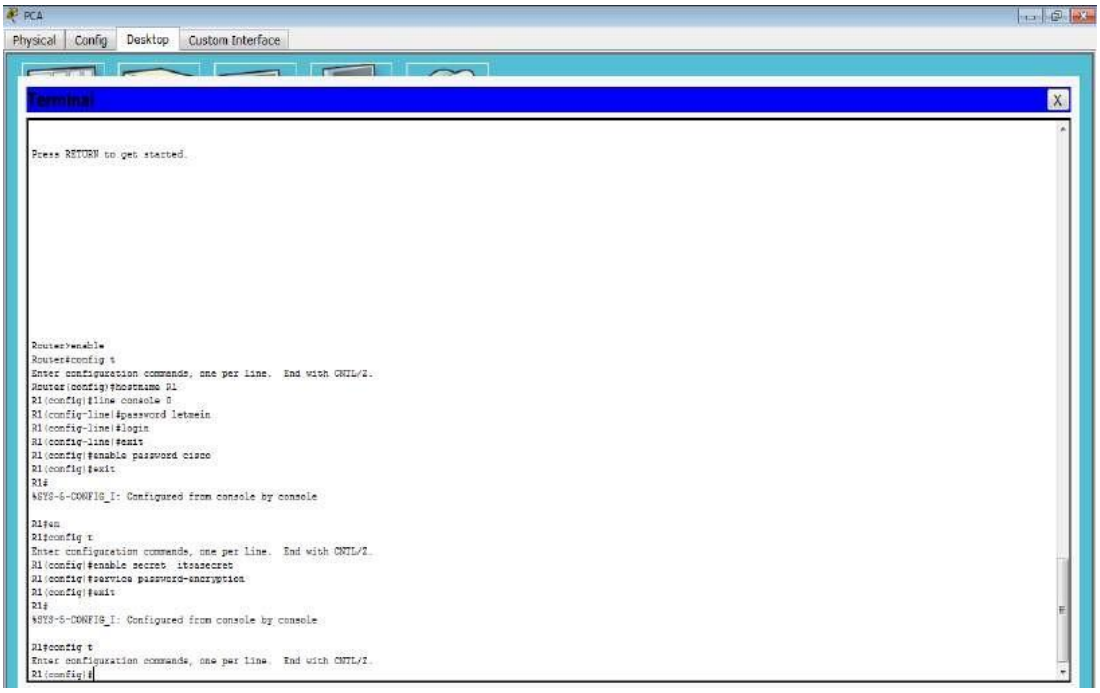
1) Consola: letmein



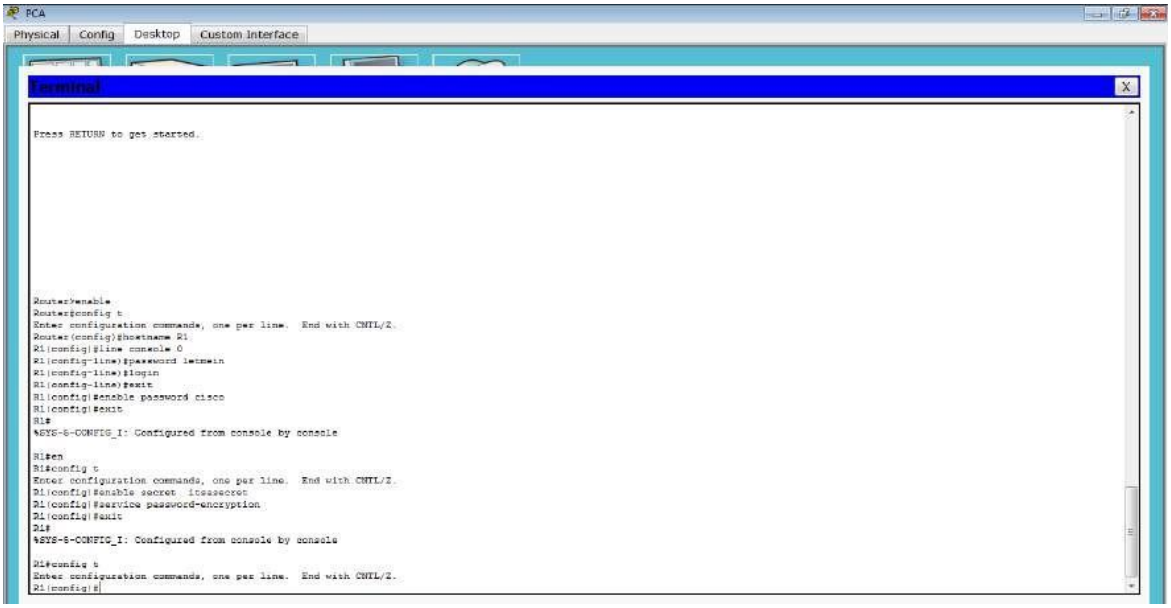
2) EXEC privilegiado, sin encriptar: cisco



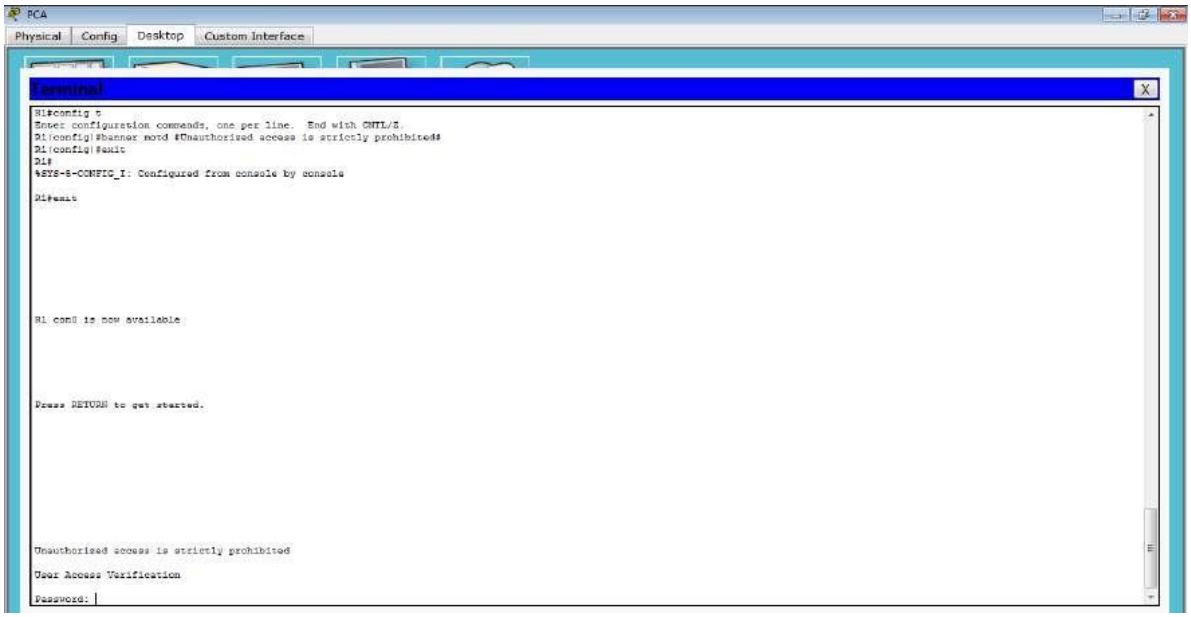
3) EXEC privilegiado, encriptado: itsasecret



c. Encripte todas las contraseñas de texto no cifrado.



d. Texto del mensaje del día: Unauthorized access is strictly prohibited (El acceso no autorizado queda terminantemente prohibido).



Paso 2: Verificar los parámetros iniciales de R1

a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza?

R/ show running-config

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:

R1 con0 is now available
Press RETURN to get started.

c. Presione Entrar; debería ver el siguiente mensaje:

Unauthorized access is strictly prohibited.
User Access Verification
Password:

(El acceso no autorizado queda terminantemente prohibido).

User Access Verification

Password:

¿Por qué todos los routers deben tener un mensaje del día (MOTD)?

R/ Cada router debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).
Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?

R/ R1 (config-line) # **login**

d. Introduzca las contraseñas necesarias para regresar al modo EXEC privilegiado.

¿Por qué la contraseña secreta de enable permitiría el acceso al modo EXEC privilegiado y la contraseña de enable dejaría de ser válida?

R/ La **contraseña secreta de enable** sobrescribe la contraseña de enable. Si ambas están configuradas en el router, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique.

R/ El comando service password-encryption encripta todas las contraseñas actuales y futuras.

Parte 3: Guardar el archivo de configuración en ejecución

Paso 1: Guarde el archivo de configuración en la NVRAM.

a. Configuró los parámetros iniciales de R1. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM?

R/ copy running-config startup-config

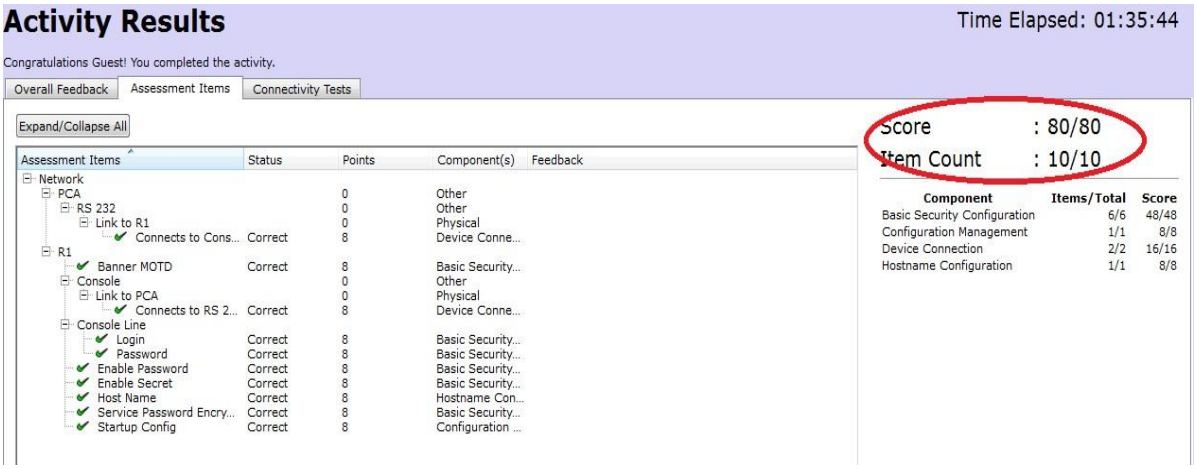
¿Cuál es la versión más corta e inequívoca de este comando?

R/ copy r s

¿Qué comando muestra el contenido de la NVRAM?

R/ show startup-configuration or show start

b. Verifique que todos los parámetros configurados estén registrados. Si no fuera así, analice el resultado y determine qué comandos no se introdujeron o se introdujeron incorrectamente. También puede hacer clic en Check Results (Verificar resultados) en la ventana de instrucción.



Paso 2: Puntos extra optativos: guarde el archivo de configuración de inicio en la memoria flash.

Aunque aprenderá más sobre la administración del almacenamiento flash de un router en los siguientes capítulos, le puede interesar saber ahora que puede guardar el archivo de configuración de inicio en la memoria flash como procedimiento de respaldo adicional. De manera predeterminada, el router seguirá cargando la configuración de inicio desde la NVRAM, pero si esta se daña, puede restablecer la configuración de inicio copiándola de la memoria flash.

Complete los siguientes pasos para guardar la configuración de inicio en la memoria flash.

a. Examine el contenido de la memoria flash mediante el comando show flash:

R1# show flash

¿Cuántos archivos hay almacenados actualmente en la memoria flash?

R/ 3

¿Cuál de estos archivos cree que es la imagen de IOS?

R/ c1900-universalk9-mz.SPA.151-4.M4.bin

¿Por qué cree que este archivo es la imagen de IOS?

R/ Las respuestas pueden variar, pero hay dos pistas: la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo.

b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

R1# **copy startup-config flash**
Destination filename [startup-config]

```
R1#
R1#copy startup-config flash
Destination filename [startup-config]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
1237 bytes copied in 0.416 secs (2973 bytes/sec)
R1#
```

El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione Entrar; de lo contrario, escriba un nombre adecuado y presione la tecla Entrar.

c. Utilice el comando show flash para verificar que el archivo de configuración de inicio esté almacenado en la memoria flash.

```
R1#show flash
System flash directory:
File Length Name/status
3 33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
5 1237 startup-config
[33848824 bytes used, 221895176 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

6.4.3.3 Packet Tracer - Connect a Router to a LAN Instructions IG

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0	209.168.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	No aplicable
	S0/0/0	209.165.200.226	255.255.255.252	No aplicable
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.11	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Parte 1: Mostrar La Información Del Router

Paso 1: Mostrar La Información De La Interfaz En El R1.

Nota: haga clic en un dispositivo y, a continuación, en la ficha CLI para acceder a la línea de comandos directamente. La contraseña de consola es cisco. La contraseña de EXEC privilegiado es class.

a. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router?
   El comando es show interfaces
b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0?
   El comando es show interface serial 0/0/0
c. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

1) ¿Cuál es la dirección IP configurada en el R1?
   La direccion configurada del router es 209.165.200.225/30
2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0?
   El ancho de banda de la interfaz 0/0/0/ es 1544 Kbit
   Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:
   1) ¿Cuál es la dirección IP en el R1?
      Al ejecutar el comando show interface G0/0 no registra configurada ninguna IP

a. ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0?

Registra la dirección MAC address is 000d.bd6c.7d01

2) ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0?
   El ancho de banda es de 1000000 Kbits

Paso 2: Mostrar Una Lista De Resumen De Las Interfaces En El R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas?
   El comando es show ip interface brief
b. Introduzca el comando en cada router y responda las siguientes preguntas:

a. ¿Cuántas interfaces seriales hay en R1 y R2?
   Cada uno de los routers tiene dos interfaces seriales
b. ¿Cuántas interfaces Ethernet hay en R1 y R2?
   El R1 se evidencia que tiene 6 interfaces Ethernet y el R2 tiene 2 interfaces de Ethernet
c. ¿Son iguales todas las interfaces Ethernet en el R1? Si no es así, explique las diferencias.
   No es correcto ya que la diferencia esta en que las 2 Gigabit Ethernet de R1 generan ancho de banda de 1000000Kbits en cambio las 4 Fast Ethernet son de 1000 Kbits.

Paso 3: Mostrar La Tabla De Enrutamiento En El R1.

a. ¿Qué comando muestra el contenido de la tabla de enrutamiento?
   El comando es show ip route
b. Introduzca el comando en el R1 y responda las siguientes preguntas:
   ¿Cuántas rutas conectadas hay (utilizan el código C)?
   Están conectadas 1
   ¿Qué ruta se indica?
   209.165.200.224/30 is directly connected, Serial0/0/0

¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento?
Solo lo envía paquetes a redes que se encuentran incluidas en la tabla de enrutamiento en caso que no esté ahí el paquete es descartado.

Paso 3: Realizar Una Copia De Seguridad De Las Configuraciones En La NVRAM

Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó?

Se utiliza el comando copy run start

Paso 3: Verificar la configuración

Paso 1: Utilizar los comandos de verificación para revisar la configuración de la interfaz

a. Utilice el comando show ip interface brief en R1 y R2 para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.
   ¿Cuántas interfaces en R1 y R2 están configuradas con direcciones IP y tienen el estado "up/up" (activa/activa)?
   Hay 3 en cada router
b. ¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando?
   La máscara de subred
c. ¿Qué comandos puede utilizar para verificar esta parte de la configuración?
   Se puede emplear show interfaces, show run y show ip protocols.
d. Utilice el comando show ip route en R1 y R2 para ver las tablas de enrutamiento actuales y responda las siguientes preguntas:
   ¿Cuántas rutas conectadas (utilizan el código C) ve en cada router? Hay 3
   ¿Cuántas rutas EIGRP (utilizan el código D) ve en cada router? Hay 2
   Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y de rutas descubiertas dinámicamente (EIGRP) debe ser igual a la cantidad total de LAN y WAN.
   ¿Cuántas LAN y WAN hay en la topología? Hay 5
   ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? Es correcto.
   Nota: si su respuesta es "no", falta una configuración necesaria. Revise los pasos de la parte 2.

6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues Instructions IG

Paso 1: Verificar El Registro De La Red Y Descartar Cualquier Problema

a. Para que pueda probar una red con eficacia, debe contar con la documentación completa. Observe que falta determinada información en la tabla de direccionamiento. Complete la tabla de direccionamiento con la información de gateway predeterminado que falta para los switches y las PC.

b. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local está en funcionamiento.

Un plan de verificación puede ser tan simple como una lista de pruebas de conectividad. Use las siguientes pruebas para verificar la conectividad local y descartar cualquier problema de acceso. El primer problema ya se documentó, pero debe implementar y verificar la solución durante la parte 2.

Documentación de prueba y verificación

Prueba	¿Se realiza correctamente?	Problemas	Solución	Verificado
PC1 a PC2	NO	Dirección IP errada PC1	Se coloca correcta 192.168.10.10	
PC1 a S1	NO	Dirección IP errada PC1	Se coloca correcta 192.168.10.10	
PC1 a R1	NO	Dirección IP errada PC1	Se coloca correcta 192.168.10.10	
PC1 a PC3	NO	Dirección IP errada PC1	Se coloca correcta 192.168.10.10	
PC1 a PC4	NO	El switch S2 no está asociada a la VLAN1 y PC4 no tenía configurado el Gateway	Se adiciona S2 a VLAN1 192.168.11.2 y Gateway 192.168.11.1	
PC2 a PC1	NO	Dirección IP errada PC1	Se coloca correcta 192.168.10.10	
PC2 a S1	SI			
PC2 a R1	SI			
PC2 a PC3	SI			
PC2 a PC4	SI			
PC3 a PC4	NO	El switch S2 no está asociada a la VLAN1	Se adiciona S2 a VLAN1 192.168.11.2	
PC3 a S2	NO	El switch S2 no está asociada a la VLAN1	Se adiciona S2 a VLAN1 192.168.11.2	
PC3 a R1	SI			
PC3 a PC1	NO	El switch S2 no está asociada a la VLAN1	Se adiciona S2 a VLAN1 192.168.11.2	
PC3 a PC2	SI			
PC4 a PC3	SI			
PC4 a S2	NO	Dirección IP Gateway errada PC4	Se coloca correcta 192.168.11.1	
PC4 a R1	SI			
PC4 a PC1	NO	Dirección IP Gateway errada PC4	Se coloca correcta 192.168.11.1	

PC4 a PC2	NO	Dirección IP Gateway errada PC4	Se coloca correcta 192.168.11.1	

Nota: esta tabla es un ejemplo; debe crear su propio documento. Puede usar lápiz y papel para dibujar una tabla, o puede utilizar un editor de texto o una hoja de cálculo. Consulte al instructor si necesita más orientación.

d. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y documente cualquier problema. Esto se conoce frecuentemente como conectividad de extremo a extremo. Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad total.

Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

6.5.1.2 Packet Tracer Skills Integration Challenge Instructions IG

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway predeterminado
RTA	G0/0	172.14.5.1	255.255.255.0	No aplicable
	G0/1	172.14.10.1	255.255.255.0	No aplicable
ASw-1	VLAN 1	172.14.5.35	255.255.255.0	172.14.5.1
ASw-2	VLAN 1	172.14.10.35	255.255.255.0	172.14.10.1
User-01	NIC	172.14.5.50	255.255.255.0	172.14.5.1
User-02	NIC	172.14.5.60	255.255.255.0	172.14.5.1
User-03	NIC	172.14.10.50	255.255.255.0	172.14.10.1
User-04	NIC	172.14.10.60	255.255.255.0	172.14.10.1

Requisitos

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre [[R1Name]] al router y [[S2Name]] al segundo switch. No podrá acceder a [[S1Name]].
- Utilice cisco como contraseña de EXEC del usuario para todas las líneas.
- Utilice class como contraseña de EXEC privilegiado.
- Encripte todas las contraseñas de texto no cifrado.
- Configure un aviso apropiado.
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de [[S2Name]].
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
- Resuelva cualquier problema y regístrelo
- Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo

Conclusiones

He podido conocer y comprender como realizar una configuración básica de computadores en una red LAN usando el emulador "CISCO PACKET TRACER", siendo un tipo de red que se limita a un área relativamente pequeña tal como un cuarto, un edificio, una nave, o un avión; mediante dicho emulador pude simular una conexión de computadores con su respectiva configuración, la cual después de haber conocido el programa a fondo pude desarrollar hasta comprobaciones y verificaciones las cuales me permiten saber el estado correcto de la conexión.

El emulador "CISCO PACKET TRACER" destinado a la simulación de conexión de computadores en una red, me permitió conocer más a fondo las configuraciones, maneras, formas en las que se realiza y posteriormente aplicar dichos conocimientos en la práctica al momento de la creación y manipulación de una red en este caso una red de datos LAN.

Recomendaciones

- Es necesario que el estudiante o practicante, sepa a fondo el tema de las conexiones de redes, debido a que si se realiza una conexión de datos incorrecta a ningún momento se va a poder establecer contacto entre las mismas, causando una pérdida de tiempo, dinero, etc.

- Tanto el emulador como la simulación de la red deben estar bien instalados, configurados, además de digitar bien los comandos, para que se ejecuten correctamente, cumplan las funciones programadas, de esta manera la red rendirá y cumplirá cada paso de la programación correspondiente sin ningún problema.

Bibliografía

- ✓ Cisco Networking Academy Obtenido De: Https://Www.Netacad.Com/Es/
- ✓ Instalación De Cisco Parker Trace, Recatado De: Https://Www.Youtube.Com/Watch?V=F8tytcaetw0
- ✓ Instalación de redes LAN Y WAN (2014) obtenido de: http://repository.unad.edu.co/bitstream/10596/1625/1/1057577725.pdf