TRABAJO COLABORATIVO 1

DIPLOMADO DE PROFUNDIZACION CCNA1
SOLUCIONES INTEGRADAS LAN-WAN

GRUPO 31

CARLOS ARTURO VALDERRAMA
CC. 16189709
YONATAN PEREA
CC. 1121868054
FERNAND BOLIVAR CALDERON
CC. 86044420
SARY YANIA VASQUEZ
CC.
GERMAN RICARDO SANCHEZ
CC.

TUTOR

ING. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI

SEPTIEMBRE 2017

INTRODUCCION

Este informe se presenta el desarrollo de los laboratorios propuestos según la guía de actividades, en las cuales se obtienen conocimientos y destrezas en los siguientes temas:

- Exploración de la red
- Configuración de un sistema operativo de red
- Protocolos y comunicaciones de red
- Acceso a la red
- Ethernet
- Capa de red

Además se presentan los archivos de simulación trabajados en el desarrollo de los laboratorios, para lo cual se trabajo con el programa de cisco Packet Tracer. Dentro del desarrollo de las actividades se explora el entorno de trabajo en packet tracer, simulación en tiempo real y paso a paso de cada uno de los diseños trabajados, se cumple con la exploración de redes LAN y WAN mediante la programación de cada uno de sus componentes especialmente la programación del IOS de los switch y de los Reuters.
Así mismo se revisa y practica el proceso de conexión para el envío y recepción de la información.

Contenido de Practicas.

- 1.2.4.4 Packet Tracer: Representación de la red
- 2.1.4.8 Packet Tracer: Navegación de IOS
- 2.2.3.3 Packet Tracer: Configuración de los parámetros iniciales del switch
- 2.3.2.5 Packet Tracer: Implementación de conectividad básica
- 2.4.1.2 Packet Tracer: Reto de habilidades de integración
- 3.3.3.3 Packet Tracer: Exploración de una red
- 3.2.4.6 Packet Tracer: Investigación de los modelos TCP/IP y OSI en acción
- 4.2.4.5 Packet Tracer: Conexión de una LAN por cable y una LAN inalámbrica
- 5.1.4.4 Packet Tracer: Identificación de direcciones MAC y direcciones IP
- 5.2.1.7 Packet Tracer: Revisión de la tabla ARP
- 5.3.3.5 Packet Tracer: Configuración de switches de capa 3
- 6.3.1.10 Packet Tracer: Exploración de dispositivos de internetworking
- 6.4.1.2 Packet Tracer: Configuración inicial del router
- 6.4.3.3 Packet Tracer: Conexión de un router a una LAN
- 6.4.3.4 Packet Tracer: Resolución de problemas del gateway predeterminado
- 6.5.1.2 Packet Tracer: Reto de habilidades de integración

PRACTICA 1.2.4.4 Packet Tracer: Representación de la red

Objetivos
Parte 1: Descripción general del programa Packet Tracer
Parte 2: Exploración de LAN, WAN e Internet

Información básica
Packet Tracer es un programa de software flexible y divertido para llevar a casa que lo ayudará con sus estudios de Cisco Certified Network Associate (CCNA). Packet Tracer le permite experimentar con comportamientos de red, armar modelos de red y preguntarse "¿qué pasaría si...?". En esta actividad, explorará una red relativamente compleja que pone de relieve algunas de las características de Packet Tracer. Al hacerlo, aprenderá cómo acceder a la función de Ayuda y a los tutoriales. También aprenderá cómo alternar entre diversos modos y espacios de trabajo. Finalmente, explorará la forma en que Packet Tracer sirve como herramienta de creación de modelos para representaciones de red.
Nota: no es importante que comprenda todo lo que vea y haga en esta actividad. Explore la red por su cuenta con libertad. Si desea hacerlo de forma más sistemática, siga estos pasos. Responda las preguntas lo mejor que pueda.

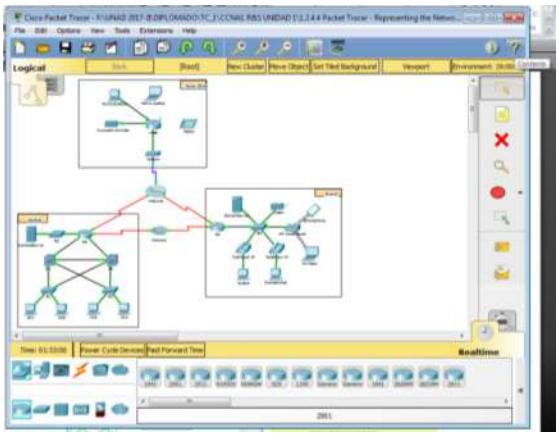
Parte 1: Descripción general del programa Packet Tracer
El tamaño de la red es mayor que la mayoría de las redes con las que trabajará en este curso (si bien verá esta topología a menudo en sus estudios de Networking Academy). Es posible que deba ajustar el tamaño de la ventana de Packet Tracer para ver la red completa. De ser necesario, puede utilizar las herramientas Acercar y Alejar para ajustar el tamaño de la ventana de Packet Tracer.

Paso 1: Acceder a las páginas de ayuda, a videos de tutoriales y a los recursos en línea de Packet Tracer

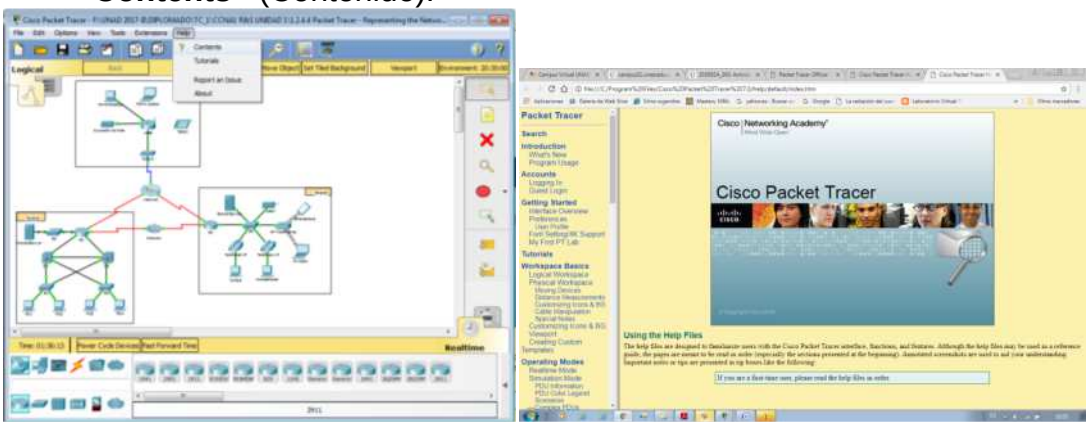
a. Acceda a las páginas de ayuda de Packet Tracer de dos maneras:

1) Haga clic en el ícono de signo de interrogación que está en la esquina superior

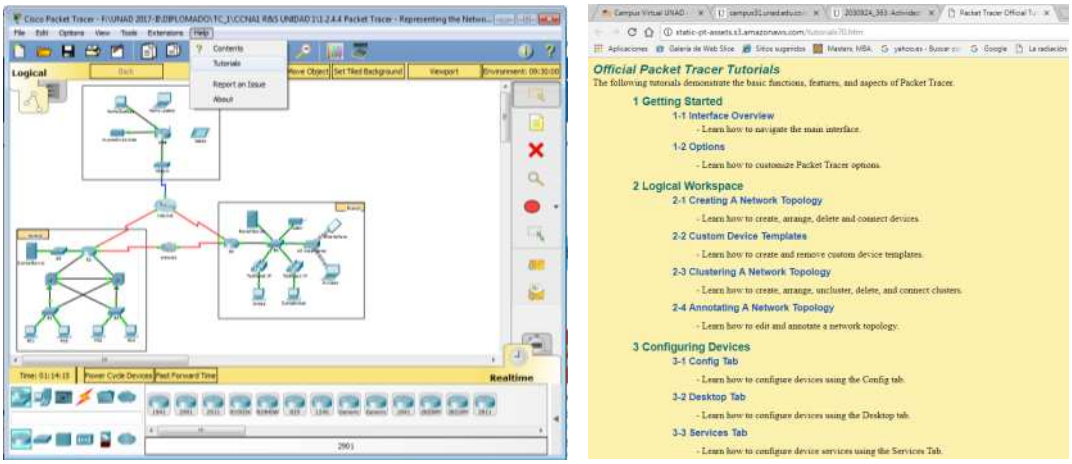
derecha de la barra de herramientas del menú.



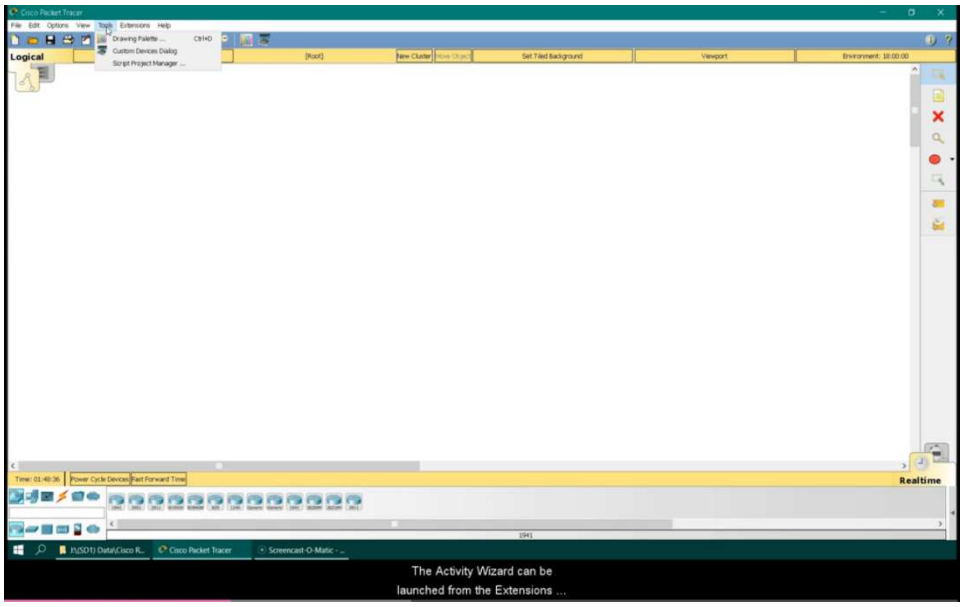
2) Haga clic en el menú **Help** (Ayuda) y, a continuación, seleccione **Contents** (Contenido).



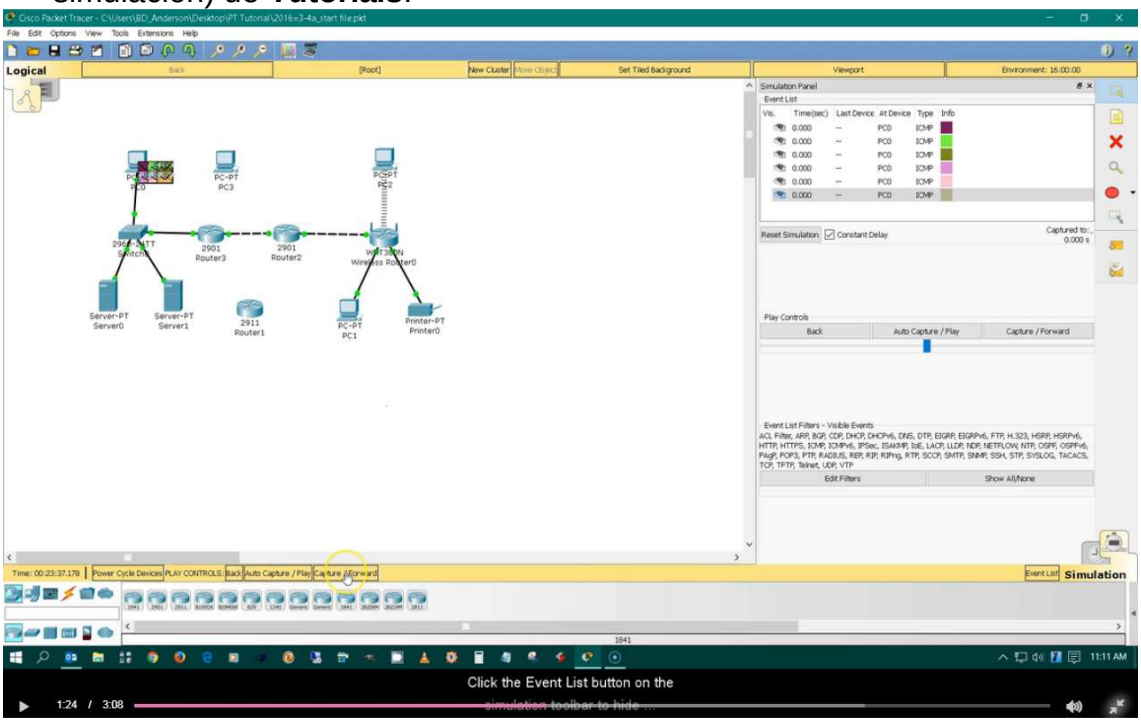
b. Acceda a los videos de tutoriales de Packet Tracer haciendo clic en **Help** > **Tutorials** (Tutoriales). Estos videos son una demostración visual de la información que se encuentra en las páginas de **ayuda** y diversos aspectos del programa de software Packet Tracer. Antes de continuar con esta actividad, debe familiarizarse con la interfaz y el modo de simulación de Packet Tracer.



1) Vea el video **Interface Overview** (Descripción general de la interfaz) en la sección **Getting Started** (Introducción) de Tutorials.



2) Vea el video **Simulation Environment** (Entorno de simulación) en la sección **Realtime and Simulation Modes** (Modos de tiempo real y de simulación) de **Tutorials**.

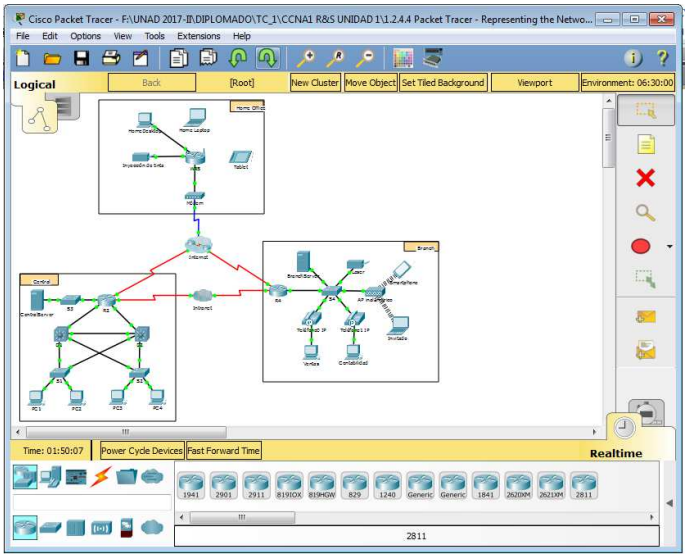


c. Busque el tutorial “Configuring Devices Using the Desktop Tab” (Configuración de dispositivos mediante la ficha Desktop [Escritorio]). Mire la primera parte para responder la siguiente pregunta: ¿Qué información se puede configurar en la ventana IP Configuration (Configuración IP)?

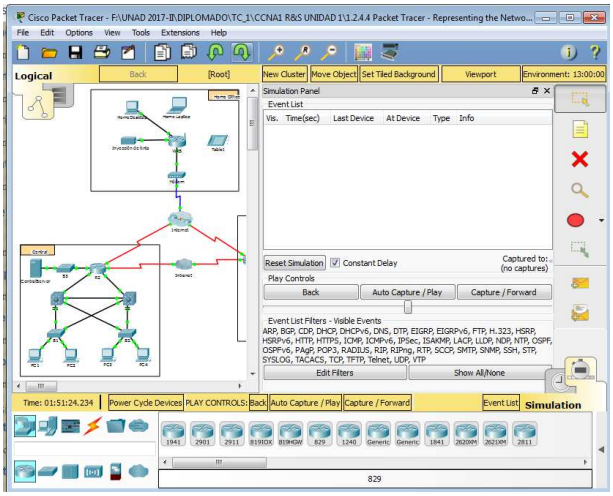
RTA: Podemos elegir entre DHCP o Static y configurar la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS.

Paso 2: Alternar entre los modos de tiempo real y de simulación

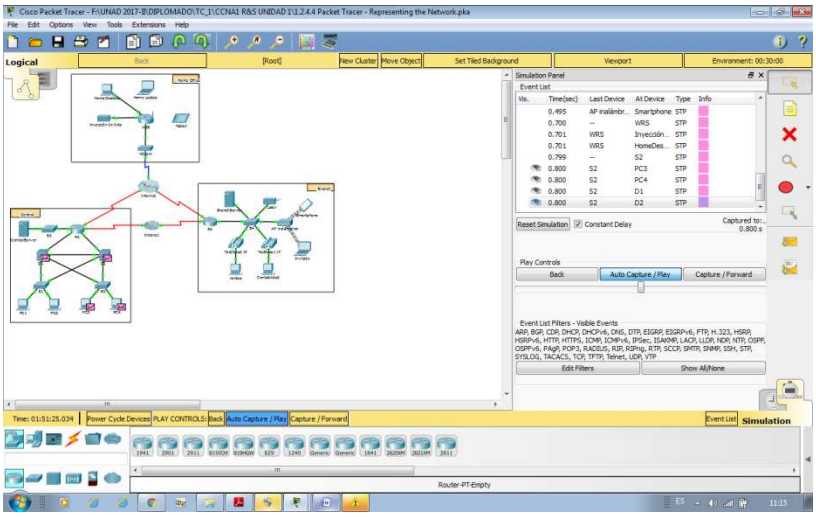
a. Busque la palabra **Realtime** (Tiempo real) en la esquina inferior derecha de la interfaz de Packet Tracer. En el modo de tiempo real, la red siempre funciona como una red real, ya sea que trabaje en la red o no. La configuración se realiza en tiempo real, y la red responde prácticamente en tiempo real.



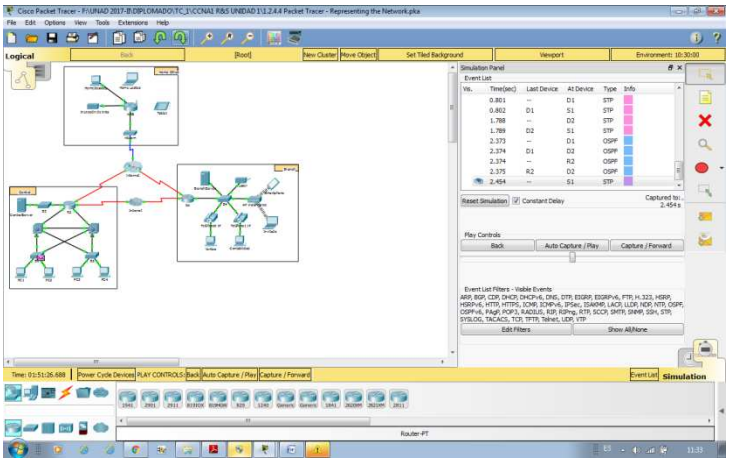
b. Haga clic en la ficha que está justo detrás de la ficha **Realtime** para cambiar al modo **Simulation** (Simulación). En el modo de simulación, puede ver la red en funcionamiento a menor velocidad, lo que le permite observar las rutas por las que viajan los datos e inspeccionar los paquetes de datos en detalle.



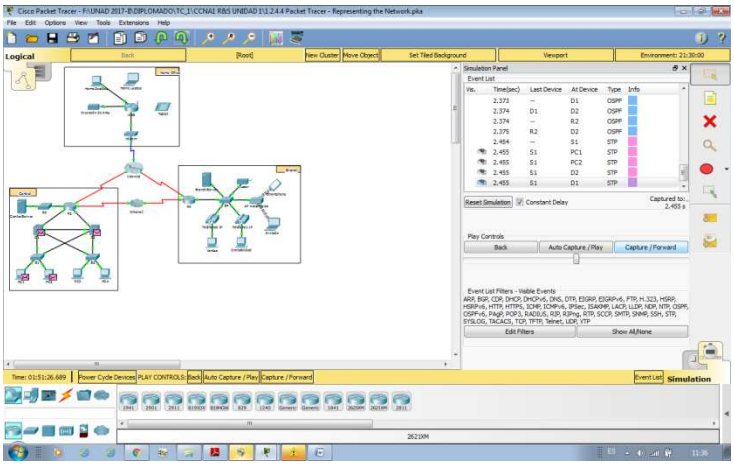
c. En el panel de simulación, haga clic en **Auto Capture / Play** (Captura/reproducción automática). Ahora debería ver los paquetes de datos, que se representan con sobres de diversos colores, que viajan entre los dispositivos.



d. Haga clic en **Auto Capture / Play** nuevamente para pausar la simulación.



e. Haga clic en **Capture / Forward** (Capturar/avanzar) para avanzar en la simulación. Haga clic en este botón algunas veces más para ver el efecto.



RTA: se realiza la simulación paso a paso de forma manual.

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:

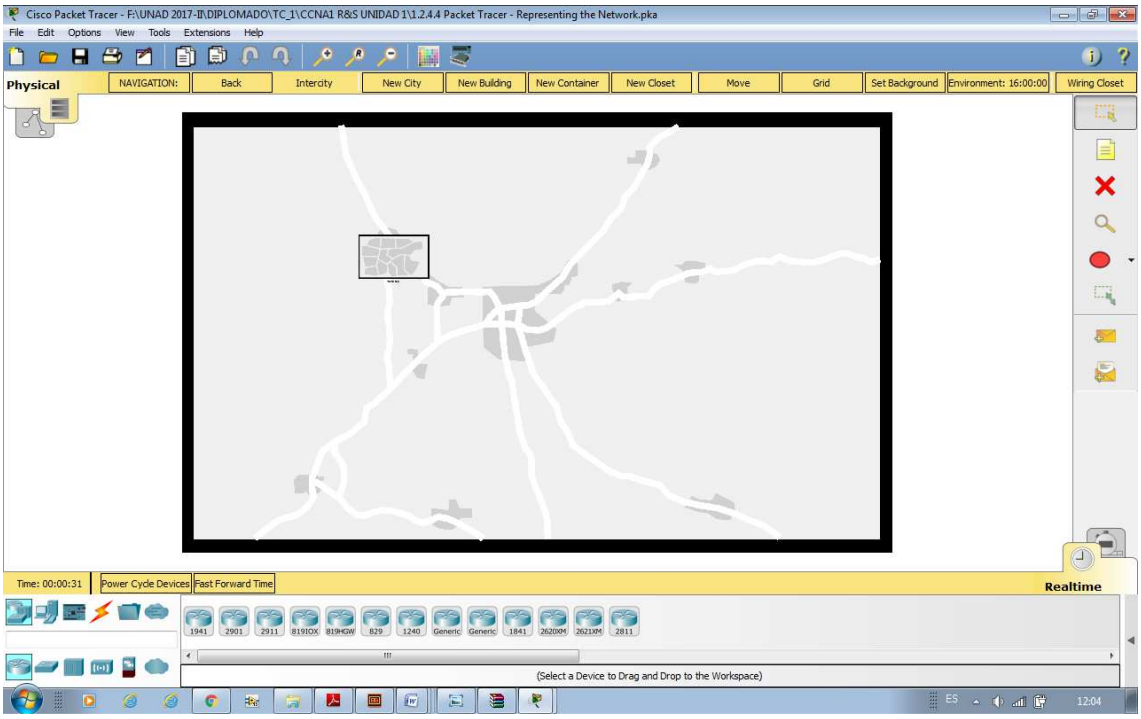
- En la **ficha OSI Model** (Modelo OSI), ¿cuántas **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida) tienen información?
Las respuestas varían según la capa del dispositivo.

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?
Los encabezados pueden ser Ethernet 802.3, LLC, STP BPDU.
- 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 direcciones de origen o destino de la capa de enlace de datos cambian.
g. Haga clic en el botón de alternancia arriba de **Simulation** en la esquina inferior derecha para volver al modo **Realtime**.

Paso 3: Alternar entre las vistas Logical y Physical

a. Busque la palabra **Logical** (Lógico) en la esquina superior izquierda de la interfaz de Packet Tracer. Actualmente se encuentra en el área de trabajo **Logical**, donde pasará la mayor parte del tiempo de creación, configuración, investigación y resolución de problemas de redes.

Nota: si bien puede agregar un mapa geográfico como imagen de fondo para el área de trabajo **Logical**, generalmente no tiene ninguna relación con la ubicación física real de los dispositivos.
b. Haga clic en la ficha que está debajo **Logical** para pasar al área de trabajo **Physical** (Físico). El propósito del área de trabajo **Physical** es darle una dimensión física a la topología lógica de la red. Le da una idea de la escala y la ubicación (cómo se vería la red en un entorno real).
c. Durante sus estudios en CCNA, utilizará esta área de trabajo de manera ocasional. Por el momento, solo debe saber que ese espacio está allí, disponible para que lo utilice. Para obtener más información sobre el área de trabajo Physical, consulte los archivos de ayuda y los videos de tutoriales.
d. Haga clic en el botón de alternancia ubicado debajo de **Physical** en la esquina superior derecha para volver al área de trabajo **Logical**.



Parte 2: Exploración de LAN, WAN e Internet
El modelo de red en esta actividad incluye muchas de las tecnologías que llegará a dominar en sus estudios en CCNA y representa una versión simplificada de la forma en que podría verse una red de pequeña o mediana empresa. Explore la red por su cuenta con libertad. Cuando esté listo, siga estos pasos y responda las preguntas.

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

a. La barra de herramientas de íconos tiene diferentes categorías de componentes de red. Debería ver las categorías que corresponden a los dispositivos intermediarios, los dispositivos finales y los medios. La categoría **Connections** (Conexiones, cuyo ícono es un rayo) representa los medios de red que admite Packet Tracer. También hay una categoría llamada **End Devices** (Dispositivos finales) y dos categorías específicas de Packet Tracer: **Custom Made Devices** (Dispositivos personalizados) y **Multiuser Connection** (Conexión multiusuario).

b. Enumere las categorías de los dispositivos intermediarios.
Las categorias son Routers, switches, hubs, dispositivos inalámbricos y emulación de WAN.

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

13 iconos

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

11 iconos

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

5 son router

f. ¿Cuántos dispositivos finales **no** son computadoras de escritorio?

8 no son computadoras

g. ¿Cuántos tipos diferentes de conexiones de medios se utilizan en esta topología de red?

4 tipos

h. ¿Por qué no hay un ícono de conexión para la tecnología inalámbrica en la categoría Connections?

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?

En el mundo real esto no sucede.

Según lo que estudió hasta ahora, explique el modelo cliente-servidor.

En las redes modernas, un hosts pueden 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.

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.

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.

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?

Hay dos: la WAN de Internet y la de intranet.

c. ¿Cuántas LAN ve?

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).

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

Las formas pueden ser cable, DSL, dial-up, datos móviles y satélite.

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

Las formas son: Línea arrendada dedicada, Metro-E, DSL, cable, satélite.

PRACTICA 2.1.4.8
Packet Tracer Navigating the IOS Instructions IG

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

En la parte 1 de esta actividad, conectará una PC a un switch mediante una conexión de consola e investigará diferentes modos de comando y características de ayuda.

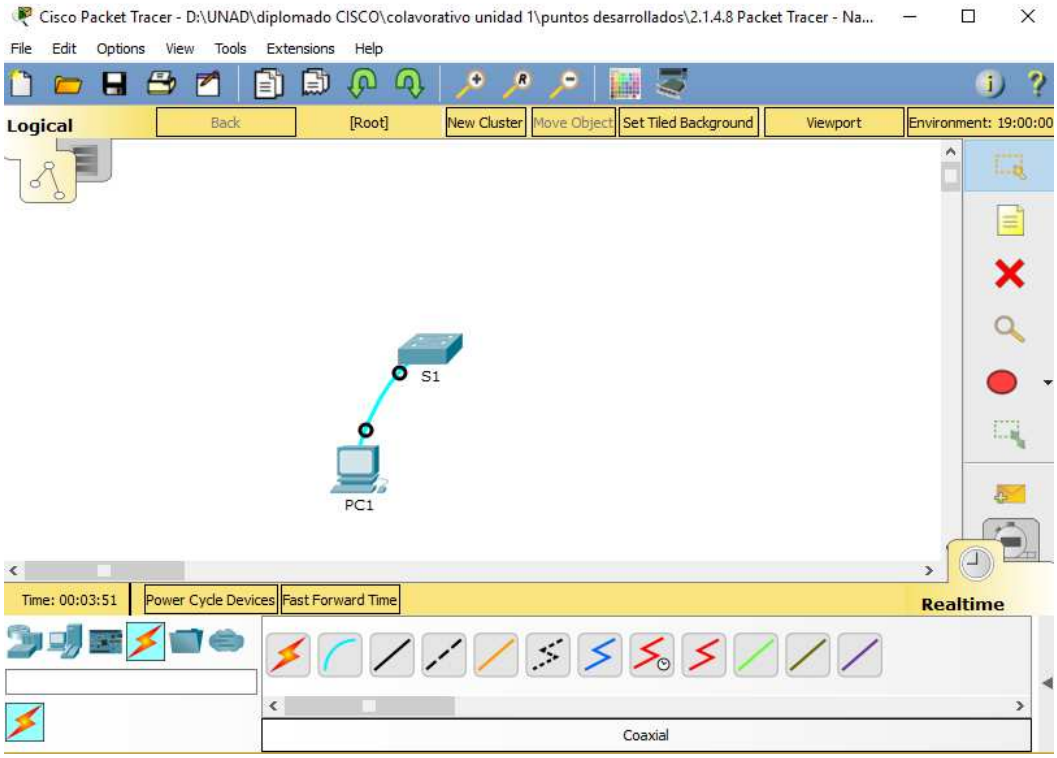
Paso 1: La conexión de la PC1 a S1 requiere un cable de consola. a. Haga clic en el ícono **Connections** (Conexiones), similar a un rayo, en la esquina inferior izquierda de la ventana de Packet Tracer.

b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

c. Haga clic en **PC1**. Aparece una ventana que muestra una opción para una conexión RS-232.

d. Arrastre el otro extremo de la conexión de consola al switch S1 y haga clic en el switch para abrir la lista de conexiones.

e. Seleccione el puerto de consola para completar la conexión.

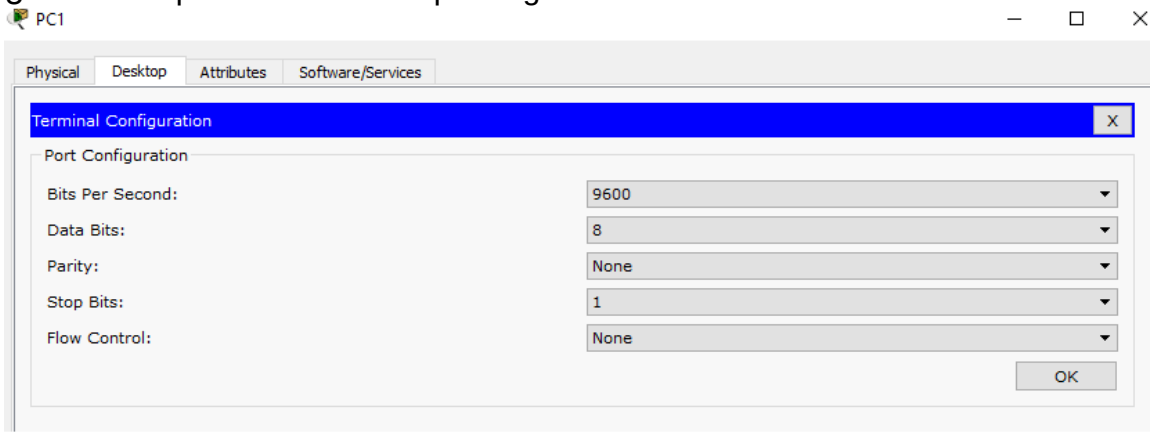


Paso 2: Establezca una sesión de terminal con el S1.

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

b. Haga clic en el ícono de la aplicación **Terminal**. Verifique que la configuración predeterminada de Port Configuration (Configuración del puerto) sea la correcta.

¿Cuál es el parámetro de bits por segundo? 9600



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

d. La pantalla que aparece puede mostrar varios mensajes. En alguna parte de la pantalla tiene que haber un mensaje que diga Press RETURN to get started! (Presione REGRESAR para comenzar) . Presione **Entrar**.

¿Cuál es la petición de entrada que aparece en la pantalla?

Paso 3: Explore 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> **?**

¿Qué comando comienza con la letra “C”?

Aparece el comando ***connect***

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

S1> **t?**

¿Qué comandos se muestran?

Aparece los comandos ***telnet terminal traceroute***

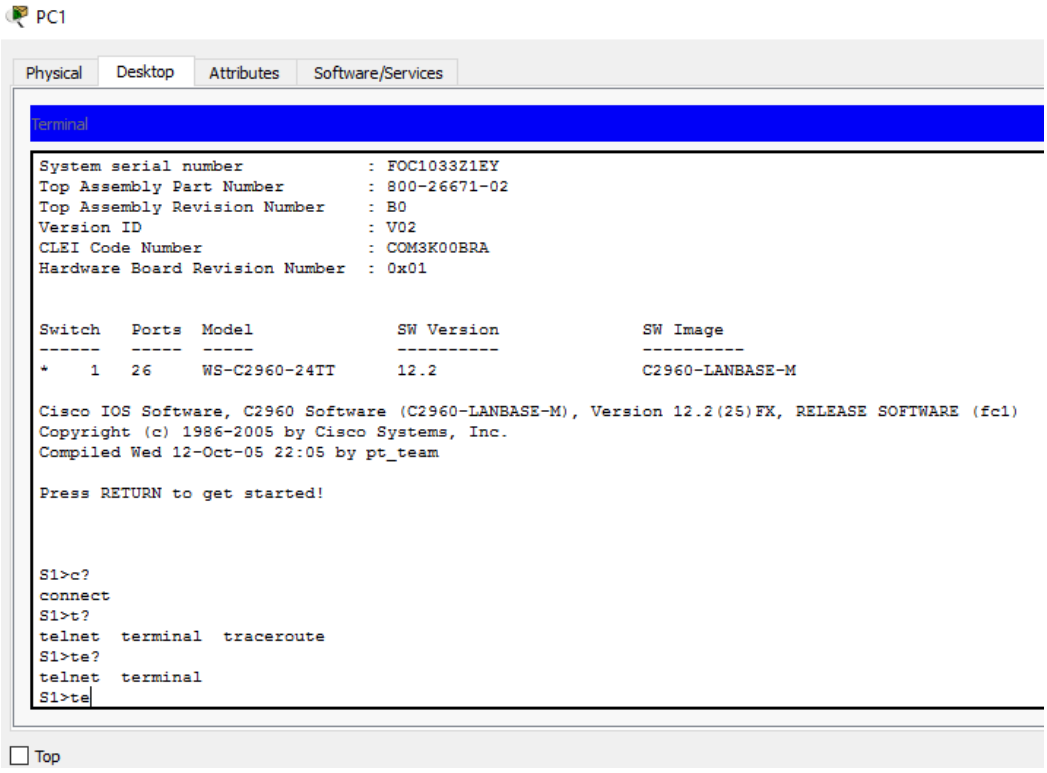
c. En la petición de entrada, escriba **te**, seguido de un signo de interrogación (**?**).

S1> **te?**

¿Qué comandos se muestran?

Aparece los comandos ***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: Entre al modo EXEC privilegiado.

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

S1> **?**

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

```
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>
```

Top

b. Escriba **en** y presione la tecla **Tabulación**.

S1> **en<Tabulación>**

¿Qué se muestra después de presionar la tecla **Tabulación**?

```
S1>en
S1>enable
```

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.

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

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

d. 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”).

```
S1#c?
clear  clock  configure  connect  copy
S1#c
```

Paso 2: Entre al 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, **<Entrar>**.

S1# **configure**

¿Cuál es el mensaje que se muestra?

b. Presione la tecla **<Entrar>** para aceptar el parámetro predeterminado**[terminal]** entre corchetes.

¿En qué cambia la petición de entrada?

c. Esto se denomina “modo de configuración global”. Este modo se analizará en más detalle en las próximas actividades y prácticas de laboratorio. Por el momento, escriba **end**, **exit** o **Ctrl-Z** para volver al modo EXEC privilegiado.

S1(config)# **exit**

S1#

```
S1#c?
clear  clock  configure  connect  copy
S1#conf
S1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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**

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

```
S1#show clock
*0:45:43.246 UTC Mon Mar 1 1993
S1#
```

b. 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<Entrar>**

¿Qué información aparece en pantalla?

c. 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 ?**

   ¿Qué información aparece en pantalla?

d. Configure el reloj con el comando **clock set**. Continúe utilizando este comando paso por paso.

   S1# **clock set ?**

   ¿Qué información se solicita?

   ¿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?

e. Según la información solicitada al emitir el comando **clock set ?**, introduzca la hora 3:00 p. m. con el formato de 24 horas, 15:00:00. Revise si se necesitan otros parámetros.

   S1# **clock set 15:00:00 ?**

   El resultado devuelve la solicitud de más información:

   <1-31> Day of the month

   MONTH Mes del año

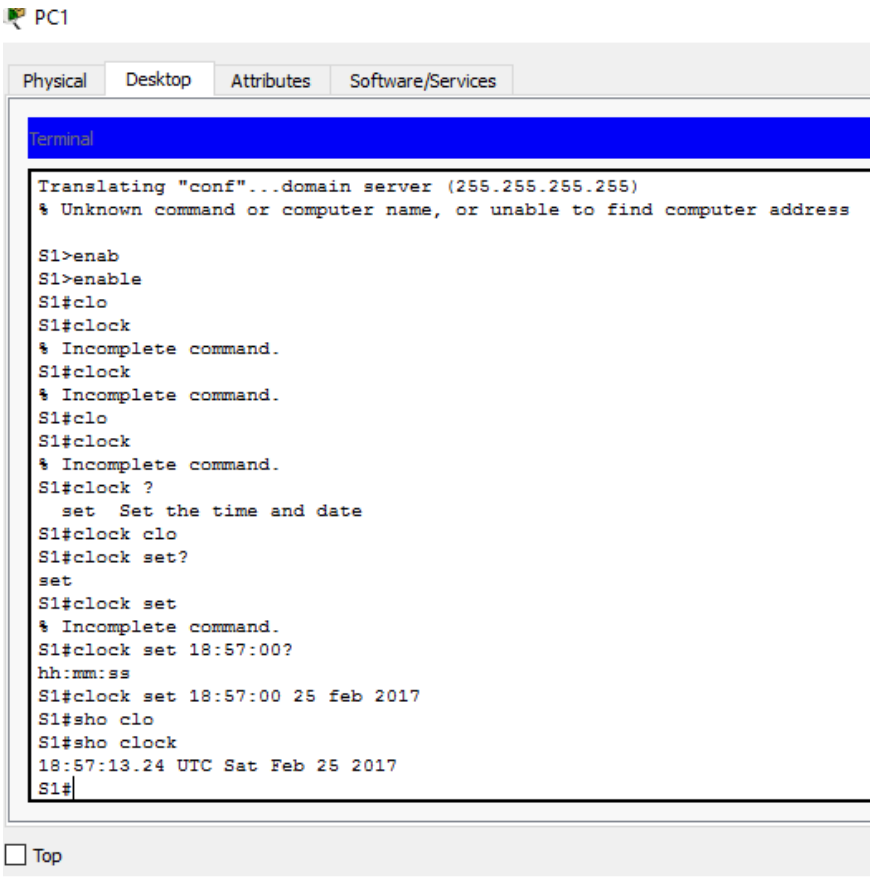
f. Intente establecer la fecha en 01/31/2035 con el formato solicitado. Es posible que para completar el proceso deba solicitar más ayuda mediante la ayuda contextual. Cuando termine, emita el comando **show clock** para mostrar la configuración del reloj. El resultado del comando debe mostrar lo siguiente:

   S1# **show clock**

   *15:0:4.869 UTC Tue Jan 31 2035

g. Si no pudo lograrlo, pruebe con el siguiente comando para obtener el resultado anterior:

   S1# **clock set 15:00:00 31 Jan 2035**



Paso 2: Explorar los mensajes adicionales del comando.

a. El IOS proporciona diversos resultados para los comandos incorrectos o incompletos, como se vio en secciones anteriores. Continúe utilizando el comando **clock** para explorar los mensajes adicionales con los que se puede encontrar mientras aprende a utilizar el IOS.

b. Emita el siguiente comando y registre los mensajes:

S1# **cl**

¿Qué información se devolvió?

S1# **clock**

¿Qué información se devolvió?

S1# **clock set 25:00:00**

¿Qué información se devolvió?

S1# **clock set 15:00:00 32**

¿Qué información se devolvió?

PC1

Physical | Desktop | Attributes | Software/Services

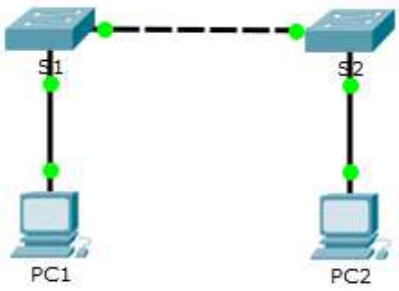
Terminal

```
S1>enable
S1#cl
% Ambiguous command: "cl"
S1#cl
S1#cloc
S1#clock
% Incomplete command.
S1#cloc
S1#clock set 25:00:00
                ^
% Invalid input detected at '^' marker.

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

PRACTICA 2.2.3.3

Packet Tracer: Configuración de los parámetros iniciales del switch

Topología



Objetivos

Parte 1: Verificar la configuración predeterminada del switch
Parte 2: Establecer una configuración básica del switch
Parte 3: Configurar un título de MOTD
Parte 4: Guardar los archivos de configuración en la NVRAM
Parte 5: Configurar el S2

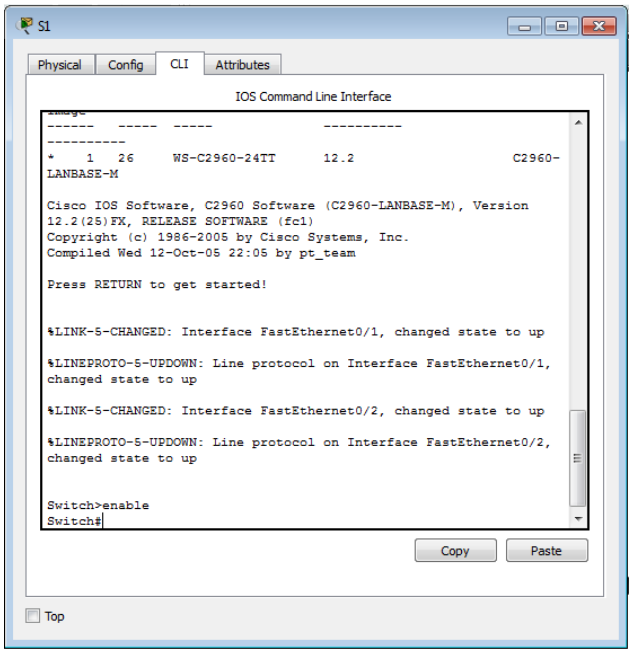
Información básica

En esta actividad, realizará configuraciones básicas del switch. Protegerá el acceso a la interfaz de línea de comandos (CLI, command-line interface) y a los puertos de la consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También aprenderá cómo configurar mensajes para los usuarios

que inician sesión en el switch. Estos avisos también se utilizan para advertir a usuarios no autorizados que el acceso está prohibido.

Parte 1: Verificar la configuración predeterminada del switch
Paso 1: Entre al modo privilegiado.

Puede acceder a todos los comandos del switch en el modo 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.
El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene el acceso a los modos de comando restantes.
a. Haga clic en **S1** y, a continuación, en la ficha **CLI**. Presione **<Entrar>**.
b. Ingrese al modo EXEC privilegiado introduciendo el comando **enable**:
Switch> **enable**
Switch#
Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

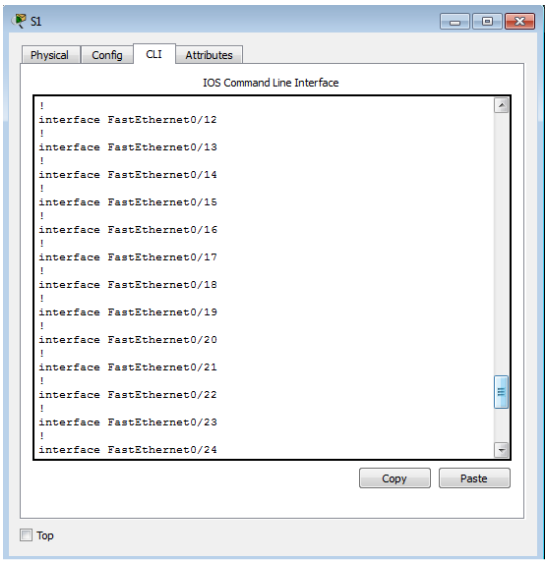


Paso 2: Examine la configuración actual del switch.

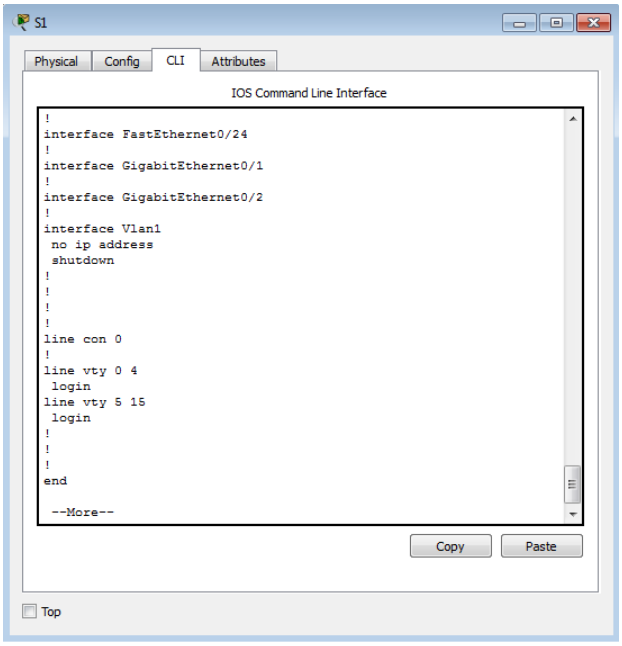
a. Ingrese el comando **show running-config**.

Switch# **show running-config**
b. Responda las siguientes preguntas:

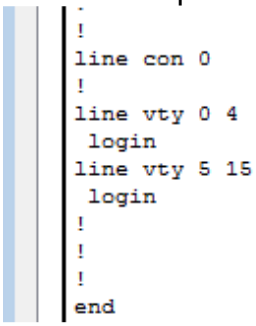
¿Cuántas interfaces FastEthernet tiene el switch? Rta: 24



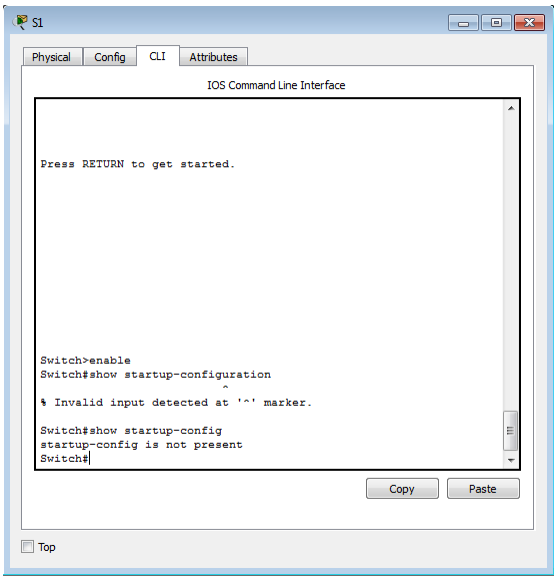
¿Cuántas interfaces Gigabit Ethernet tiene el switch? Rta: 2, IEEE 802.3



¿Cuál es el rango de valores que se muestra para las líneas vty? Rta: 0 -15



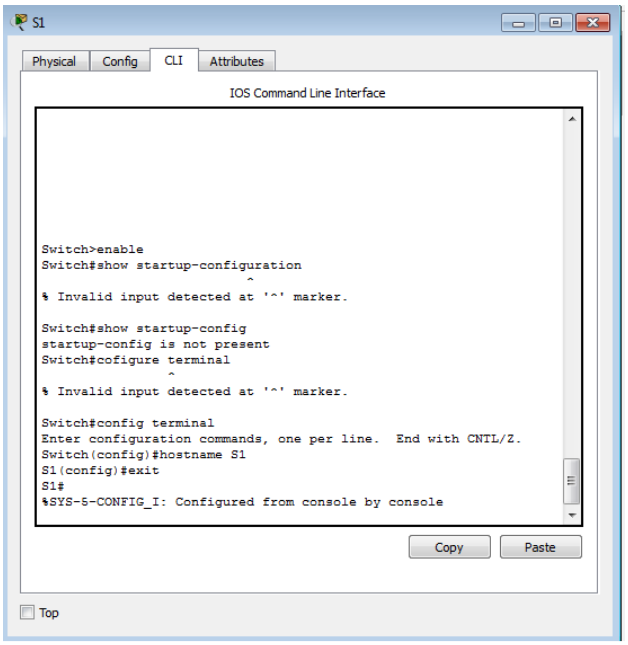
¿Qué comando muestra el contenido actual de la memoria de acceso aleatorio no volátil (NVRAM)? show startup-config



¿Por qué el switch responde con startup-config is not present?
Rta: Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.

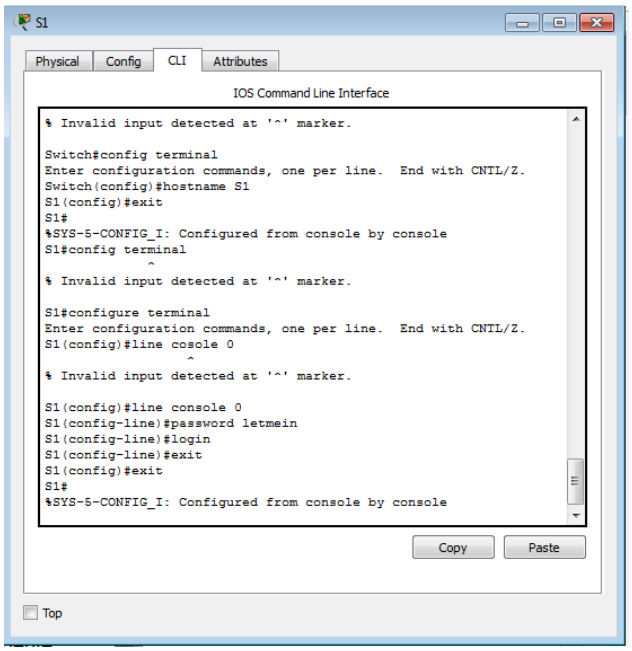
Parte 2: Crear una configuración básica del switch
Paso 1: Asignar un nombre a un switch

Para configurar los parámetros de un switch, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el switch.
Switch# **config terminal**
Switch(config)# **hostname S1**
S1(config)# **exit**
S1#



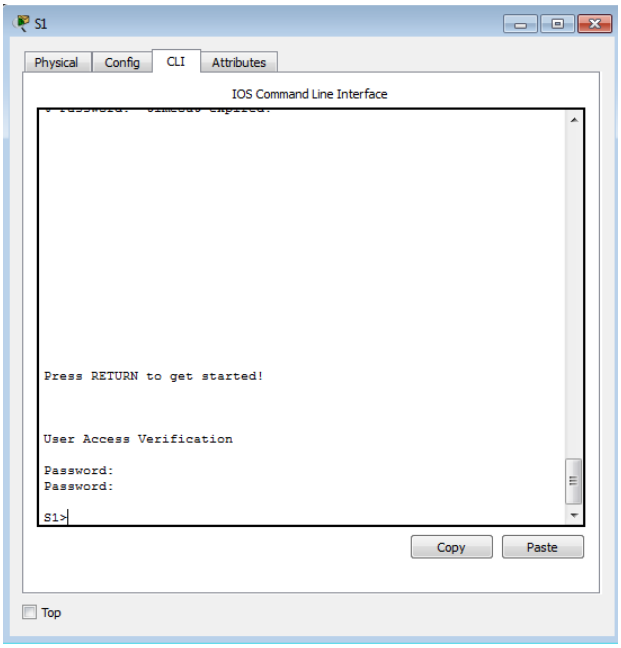
Paso 2: Proporcionar un acceso seguro a la línea de consola

Para proporcionar un acceso seguro a la línea de la consola, acceda al modo config-line y establezca la contraseña de consola en **letmein**.
S1# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **line console 0**
S1(config-line)# **password letmein**
S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#



¿Por qué se requiere el comando **login**?
Rta:En el control de seguridad de contraseña para que este proceso sea efectivo se requiere los comandos **login** y **password**.

Paso 3: Verifique que el acceso a la consola sea seguro.
Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.
S1# **exit**
Switch con0 is now available
Press RETURN to get started.
User Access Verification
Password:
S1>



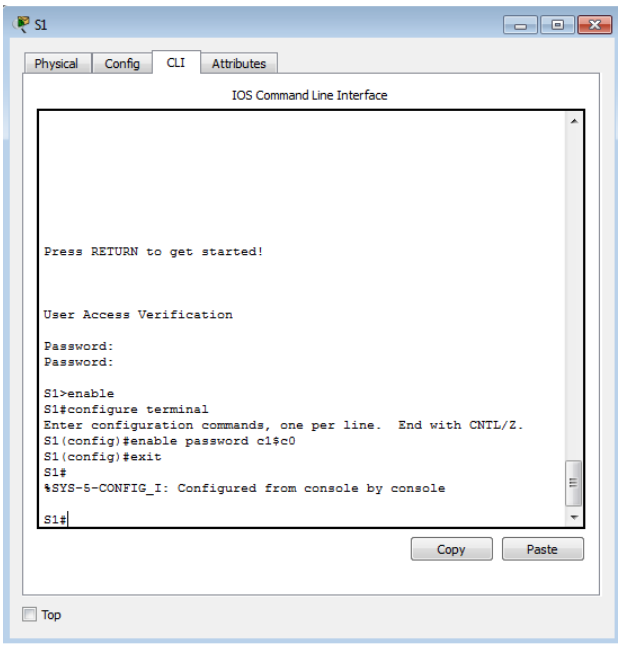
Nota: si el switch no le pidió una contraseña, entonces no se configuró el parámetro **login** en el paso 2.

Paso 4: Proporcionar un acceso seguro al modo privilegiado

Establezca la contraseña de **enable** en **c1$c0**. Esta contraseña protege el acceso al modo privilegiado.

Nota: el **0** en **c1$c0** es un cero, no una O mayúscula. Esta contraseña no calificará como correcta hasta que se la encriptado tal como se indica en el paso 8.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#



Paso 5: Verificar que el acceso al modo privilegiado sea seguro

a. Introduzca el comando **exit** nuevamente para cerrar la sesión del switch.

b. Presione **<Entrar>**; a continuación, se le pedirá que introduzca una contraseña:

User Access Verification
Password:

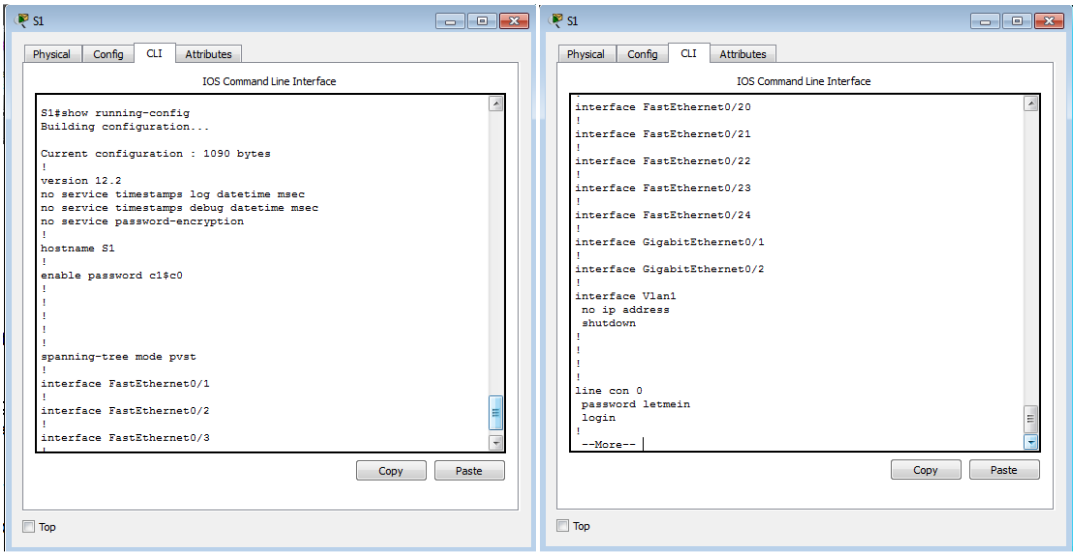
c. La primera contraseña es la contraseña de consola que configuró para **line con 0**. Introduzca esta contraseña para volver al modo EXEC del usuario.

d. Introduzca el comando para acceder al modo privilegiado.

e. Introduzca la segunda contraseña que configuró para proteger el modo EXEC privilegiado.

f. Para verificar la configuración, examine el contenido del archivo de configuración en ejecución:

S1# **show running-configuration**
Observe que las contraseñas de consola y de enable son de texto no cifrado. Esto podría presentar un riesgo para la seguridad si alguien está viendo lo que hace.

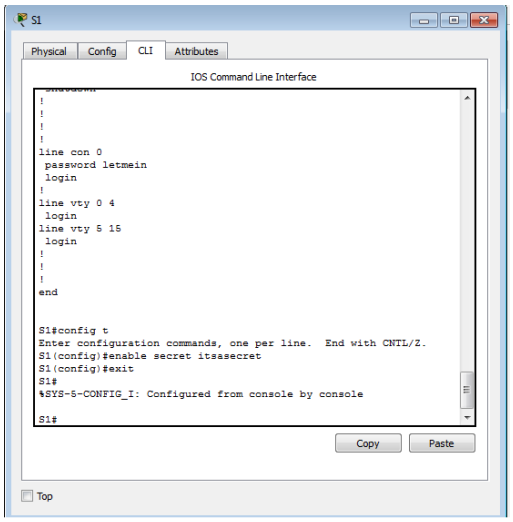


Paso 6: Configure una contraseña encriptada para proporcionar un acceso seguro al modo privilegiado.

La **contraseña de enable** se debe reemplazar por una nueva contraseña secreta encriptada mediante el comando **enable secret**. Establezca la contraseña secreta de enable en **itsasecret**.

S1# **config t**
S1(config)# **enable secret itsasecret**

S1(config)# **exit**
S1#



Nota: la contraseña **secreta de enable** sobrescribe la contraseña de **enable**. Si ambas están configuradas en el switch, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado.

Paso 7: Verificar si la contraseña secreta de enable se agregó al archivo de configuración

a. Introduzca el comando **show running-configuration** nuevamente para verificar si la nueva contraseña **secreta de enable** está configurada.

Nota: puede abreviar el comando **show running-configuration** de la siguiente manera:

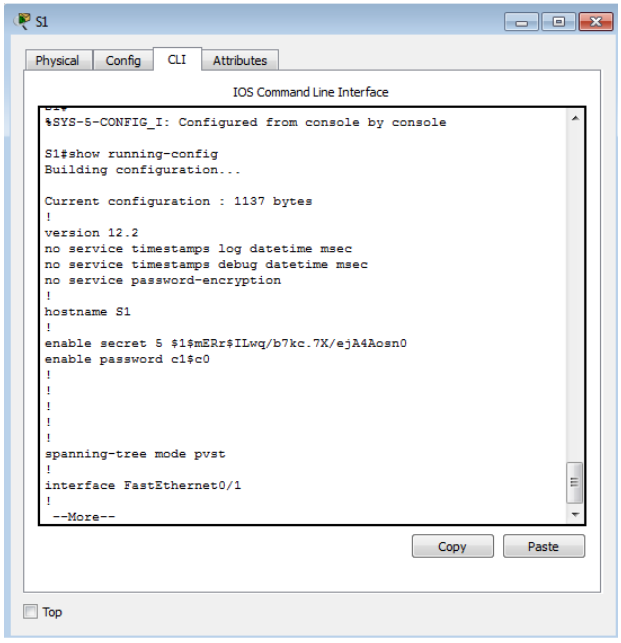
S1# **show run**

b. ¿Qué se muestra como contraseña **secreta de enable**?

Rta: 1mERr$ILwq/b7kc.7X/ejA4Aosn0

c. ¿Por qué la contraseña **secreta de enable** se ve diferente de lo que se configuró?

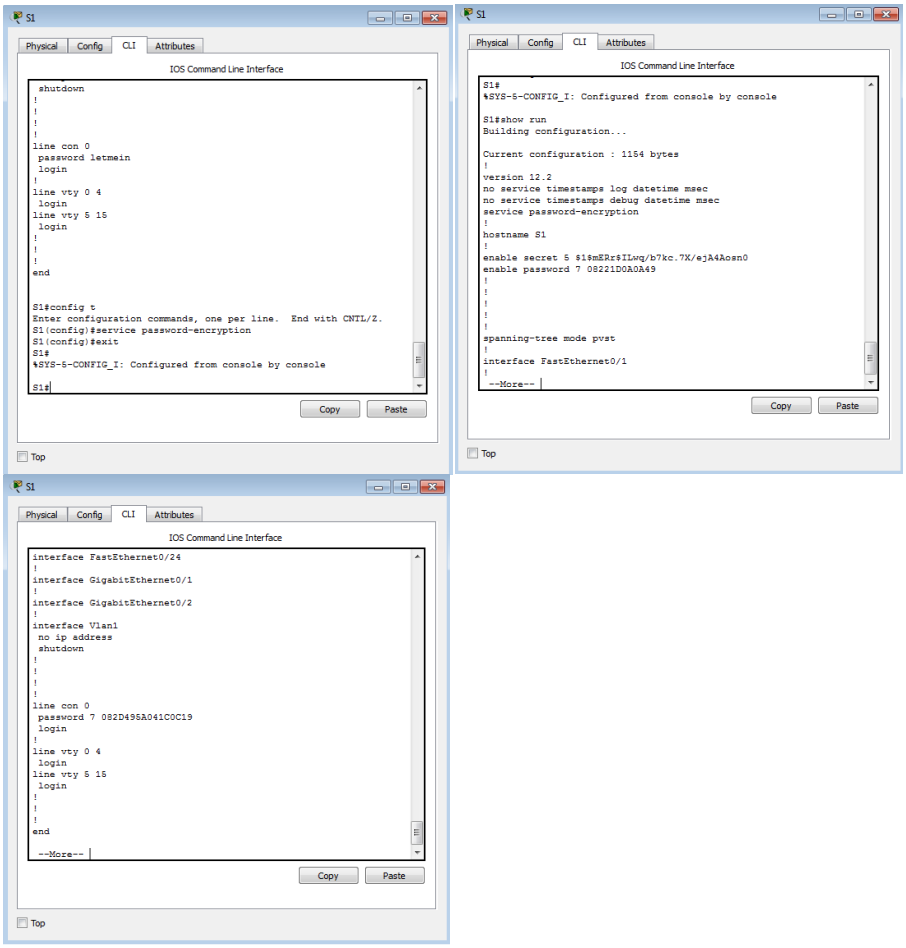
Se encripto la contraseña enable secret, mientras que la contraseña de enable aparece no cifrado.



Paso 8: Encriptar las contraseñas de consola y de enable

Como pudo observar en el paso 7, la contraseña **secreta de enable** estaba encriptada, pero las contraseñas de **enable** y de **consola** aún estaban en texto no cifrado. Ahora encriptaremos estas contraseñas de texto no cifrado con el comando **service password-encryption**.
S1# **config t**
S1(config)# **service password-encryption**
S1(config)# **exit**

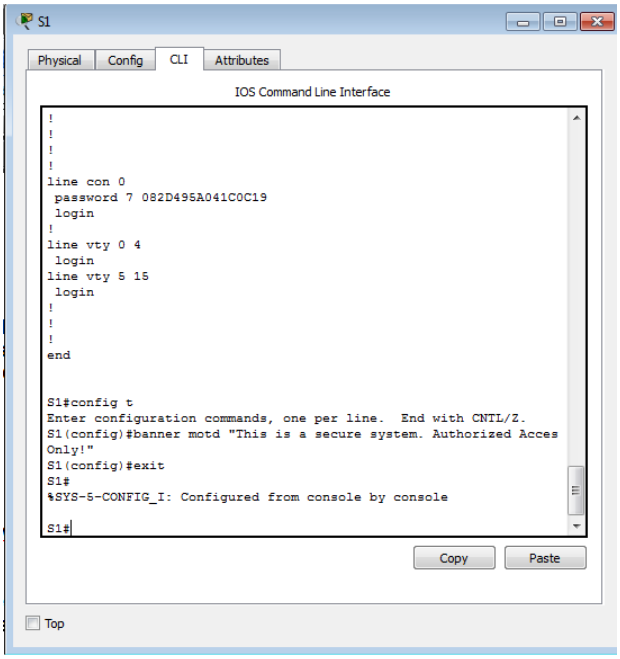
Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma encriptada en el archivo de configuración? Explique por qué.
El comando service password-encryption encripta todas las contraseñas es la función específica de este comando, tanto las actuales como las contraseñas futuras que puedan añadirse.



Parte 3: Configurar un título de MOTD
Paso 1: Configurar un mensaje del día (MOTD).

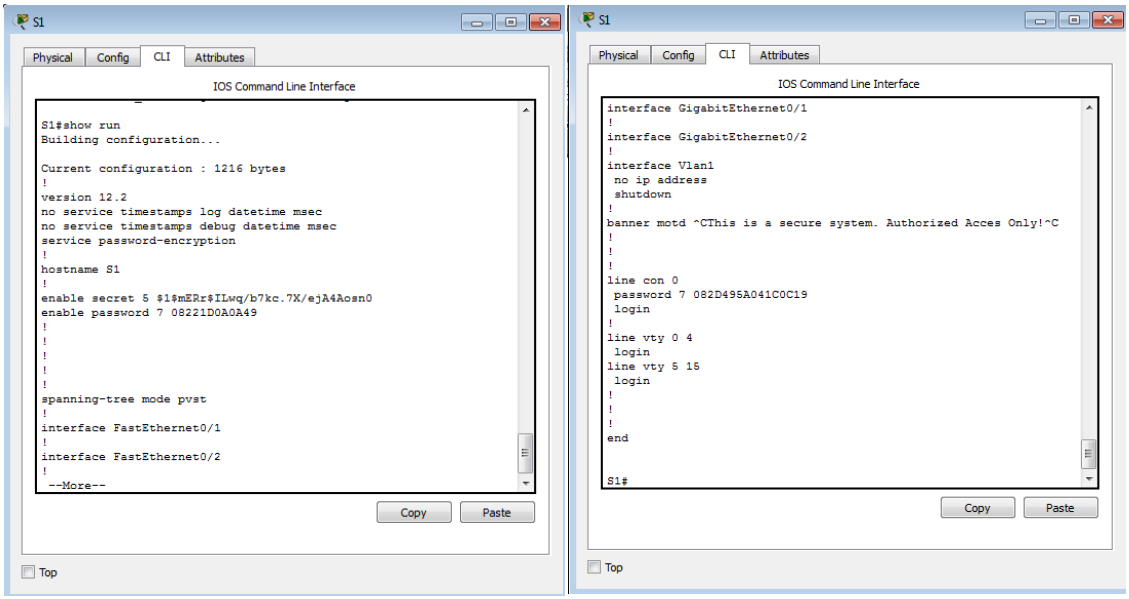
El conjunto de comandos IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se denominan “mensajes del día” o “mensajes

MOTD". Encierre el texto del mensaje entre comillas o utilice un delimitador diferente de cualquier carácter que aparece en la cadena de MOTD.
S1# **config t**
S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#



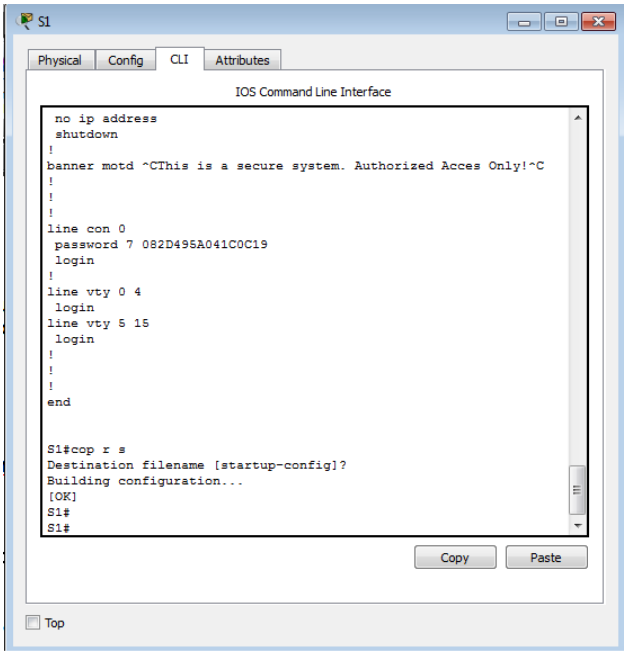
¿Cuándo se muestra este mensaje?
Rta: El mensaje se muestra cuando alguien no autorizado trata de acceder al switch a través del puerto de consola.
¿Por qué todos los switches deben tener un mensaje MOTD?
Rta: Debe tener el mensaje para advertir a los usuarios no autorizados que el acceso está prohibido o no está permitido, 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).

Parte 4: Guardar los archivos de configuración en la NVRAM
Paso 1: Verificar que la configuración sea precisa mediante el comando show run



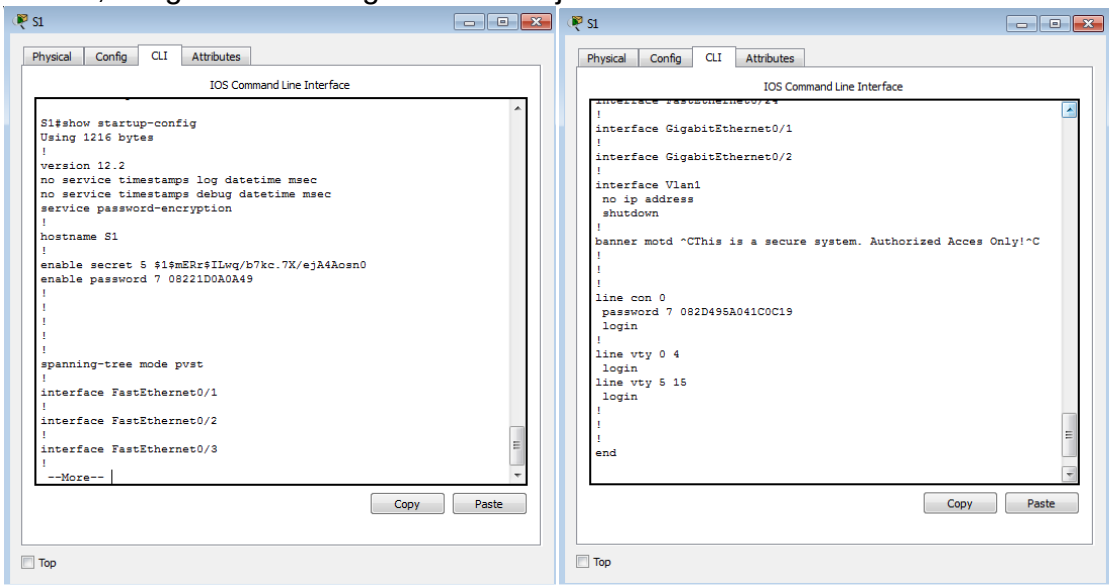
Paso 2: Guardar el archivo de configuración

Usted ha completado la configuración básica del switch. 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.
S1# **copy running-config startup-config**
Destination filename [startup-config]?**[Enter]**
Building configuration...
[OK]
¿Cuál es la versión abreviada más corta del comando **copy running-config startup-config**?
Rta: **cop r s**



Paso 3: Examinar el archivo de configuración de inicio

¿Qué comando muestra el contenido de la NVRAM? **show startup-config**
¿Todos los cambios realizados están grabados en el archivo?
Rta: Sí, es igual a la configuración en ejecución.

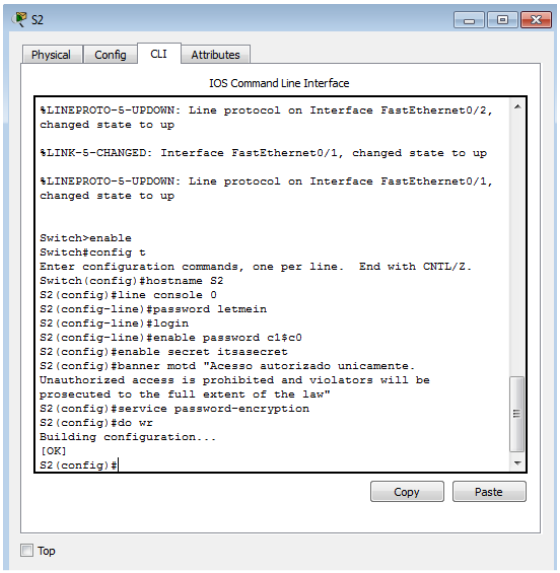


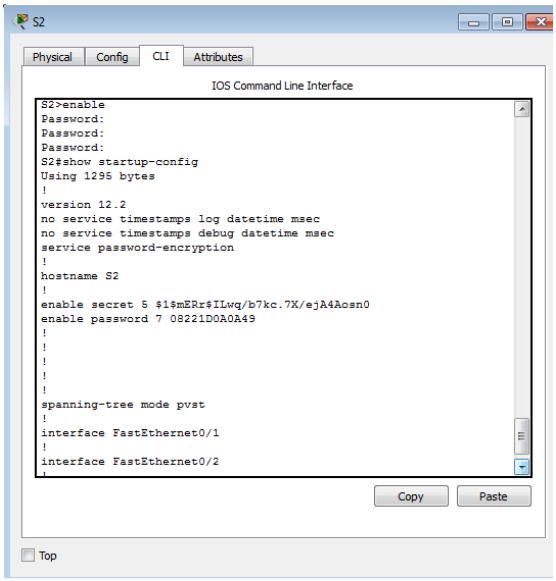
Parte 5: Configurar S2
Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.
Configure el S2 con los siguientes parámetros:
a. Nombre del dispositivo: **S2**
b. Proteja el acceso a la consola con la contraseña **letmein**.
c. Configure la contraseña **c1$c0** para enable y la contraseña secreta de enable, **itsasecret**.
d. Configure el siguiente mensaje para aquellas personas que inician sesión en el switch:

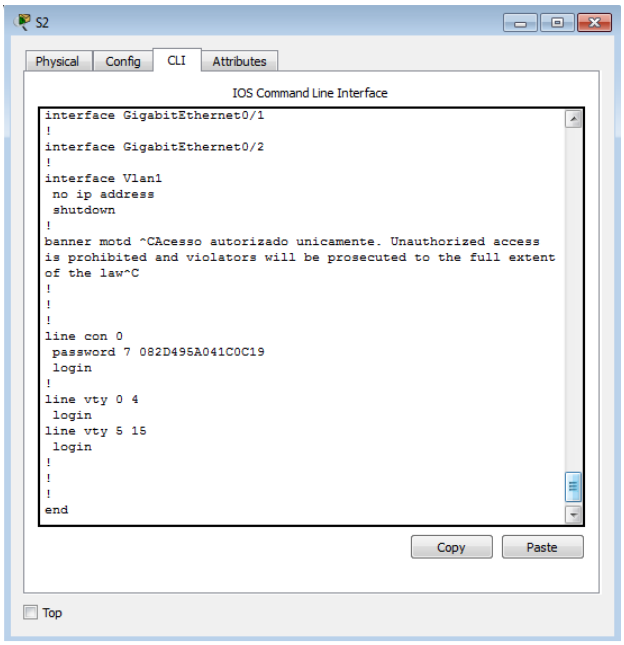
Acceso autorizado únicamente. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.
e. Encripte todas las contraseñas de texto no cifrado.
f. Asegúrese de que la configuración sea correcta.
g. Guarde el archivo de configuración para evitar perderlo si el switch se apaga.

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#enable password c1$c0
S2(config)#enable secret itsasecret

S2(config)#banner motd $any text here$
S2(config)#service password-encryption
S2(config)#do wr







PRACTICA 2.3.2.5

Packet Tracer: Implementación de conectividad básica

Topología

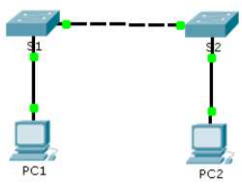


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Objetivos
Parte 1: Realizar una configuración básica en S1 y S2
Paso 2: Configurar la PC
Parte 3: Configurar la interfaz de administración de switches

Información básica
En esta actividad, primero realizará configuraciones básicas del switch. A continuación, implementará conectividad básica mediante la configuración del direccionamiento IP en switches y PC. Cuando haya finalizado la configuración del direccionamiento IP, utilizará diversos comandos **show** para revisar las configuraciones y utilizará el comando **ping** para verificar la conectividad básica entre los dispositivos.

Parte 1: Realizar una configuración básica en el S1 y el S2
Complete los siguientes pasos en el S1 y el S2.
Paso 1: Configurar un nombre de host en el S1
a. Haga clic en **S1** y, a continuación, haga clic en la ficha **CLI**.
b. Introduzca el comando correcto para configurar el nombre de host **S1**.

Paso 2: Configurar las contraseñas de consola y del modo EXEC privilegiado
a. Use **cisco** para la contraseña de consola.
b. Use **class** para la contraseña del modo EXEC privilegiado.

Paso 3: Verificar la configuración de contraseñas para el S1

¿Cómo puede verificar que ambas contraseñas se hayan configurado correctamente?
Una vez que salga del modo EXEC del usuario, el switch le solicitará una contraseña para acceder a la interfaz de consola y le solicitará una contraseña por segunda vez para acceder al modo EXEC privilegiado. También puede usar el comando **show run** para ver las contraseñas.

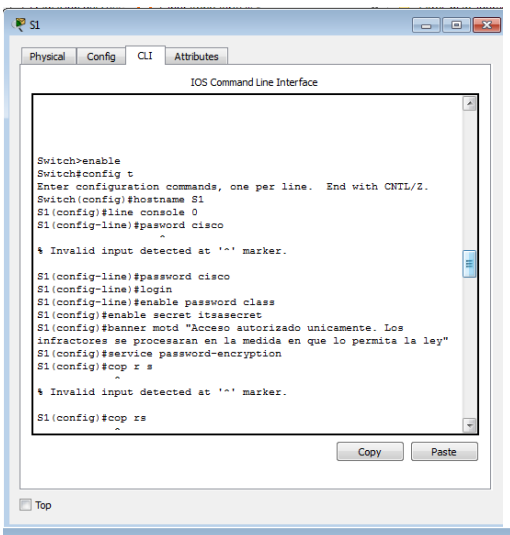
Paso 4: Configurar un mensaje del día (MOTD).

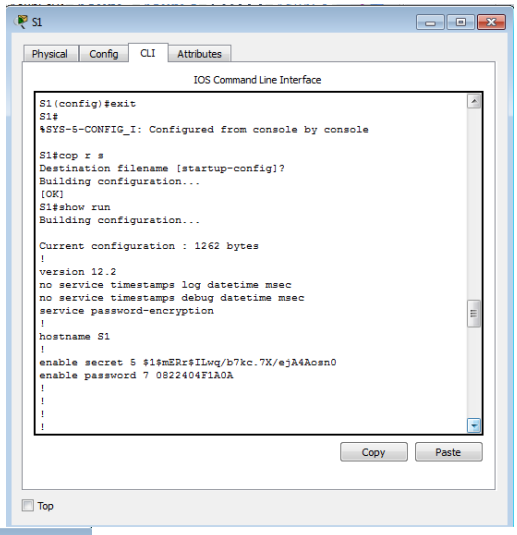
Utilice un texto de aviso adecuado para advertir contra el acceso no autorizado. El siguiente texto es un ejemplo:

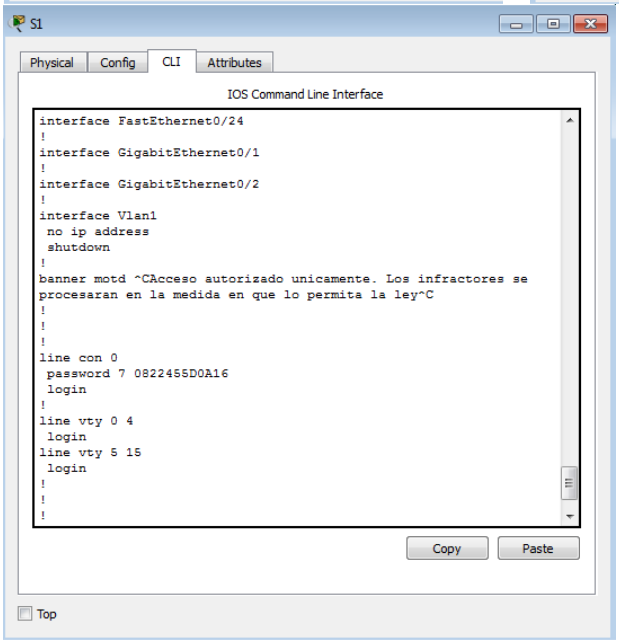
Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley.

Paso 5: Guarde el archivo de configuración en la NVRAM.

¿Qué comando emite para realizar este paso?
S1(config)#exit (or end)
S1#copy run start





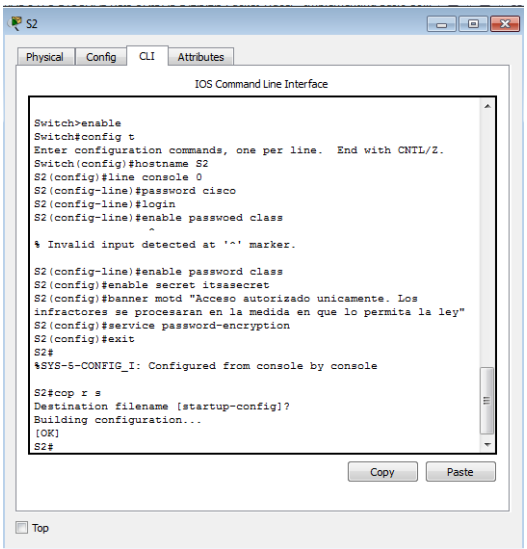


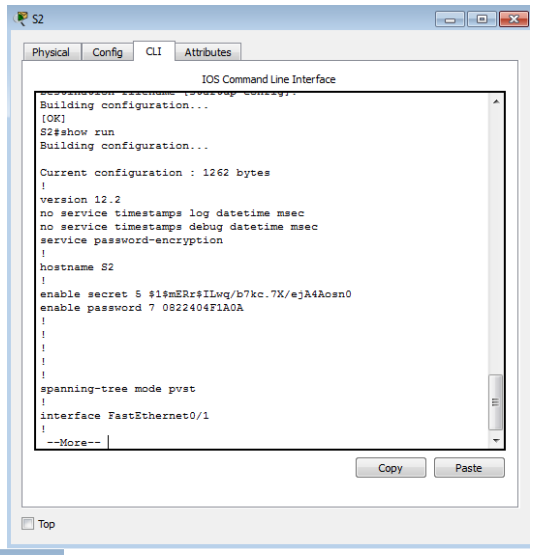
- Configuration del switch S1

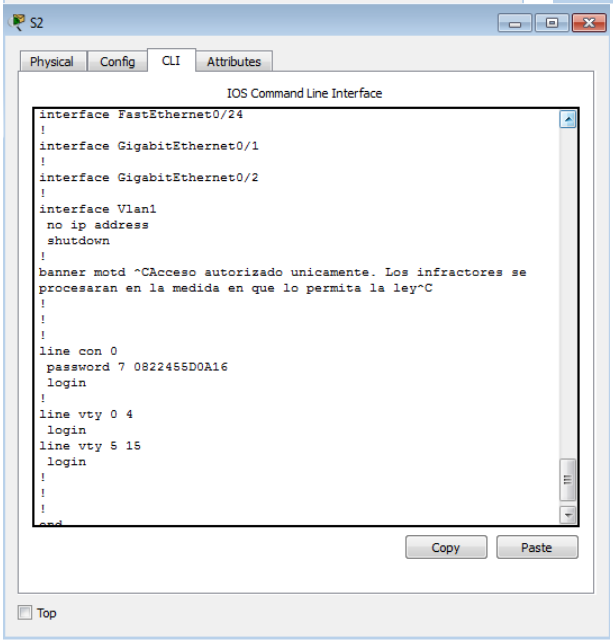
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login

S1(config-line)#enable password class
S1(config)#enable secret itsasecret
S1(config)#banner motd “**Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley”**
S1(config)#service password-encryption
S1(config)#exit
S1# cop r s

Paso 6: Repetir los pasos 1 a 5 para el S2







- Configuración del switch S2

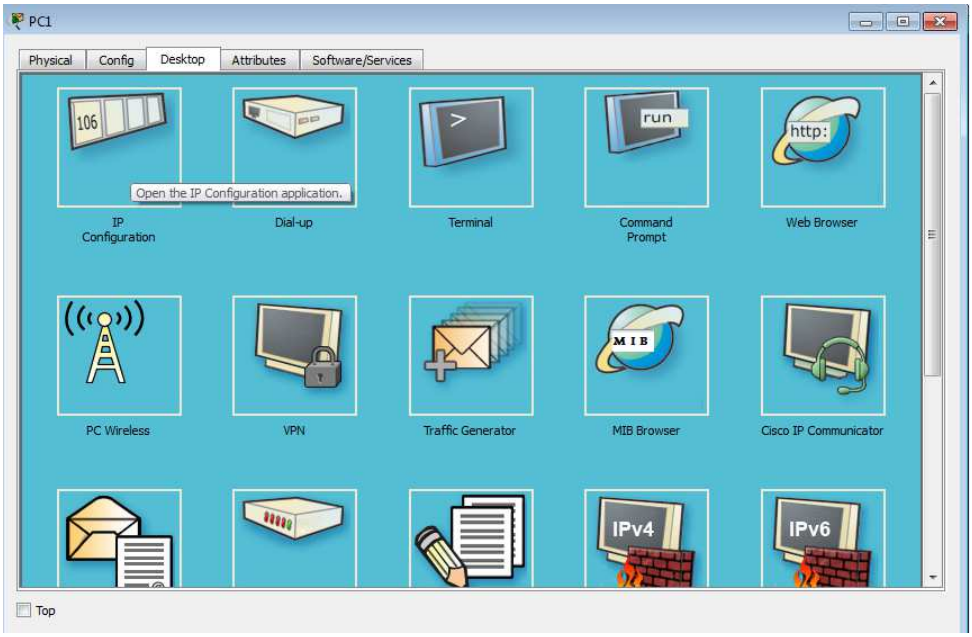
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0

S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#enable password class
S2(config)#enable secret itsasecret
S2(config)#banner motd “**Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley”**
S2(config)#service password-encryption
S2(config)#exit
S2# cop r s

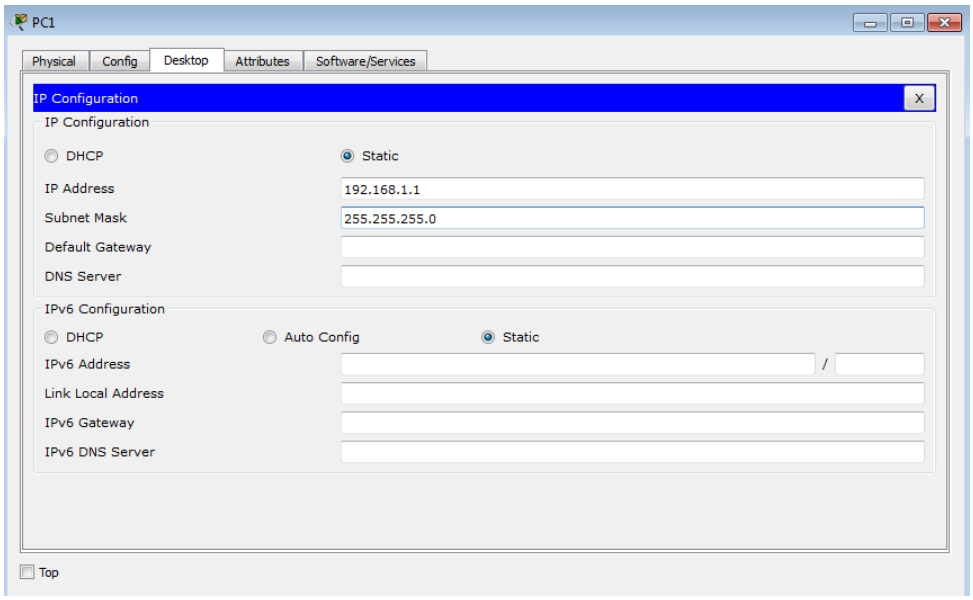
Parte 2: Configurar las PC
Configure la PC1 y la PC2 con direcciones IP.

Paso 1: Configurar ambas PC con direcciones IP

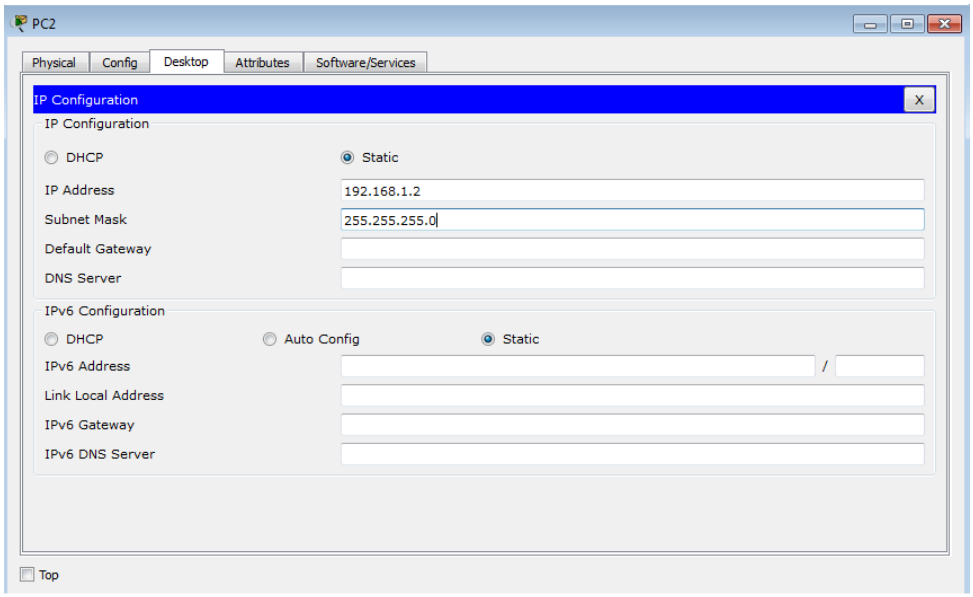
a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).



b. Haga clic en **IP Configuration** (Configuración de IP). En la **tabla de direccionamiento** anterior, puede ver que la dirección IP para la PC1 es 192.168.1.1 y la máscara de subred es 255.255.255.0. Introduzca esta información para la PC1 en la ventana **IP Configuration**.



c. Repita los pasos 1a y 1b para la PC2.



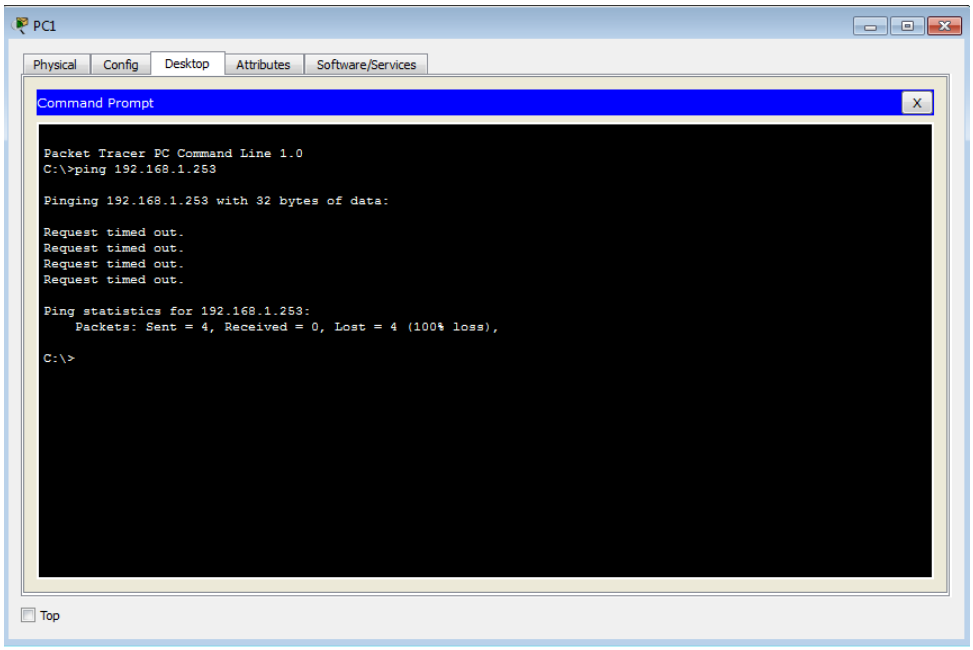
Paso 2: Probar la conectividad a los switches

a. Haga clic en **PC1**. Cierre la ventana **IP Configuration** si todavía está abierta. En la ficha **Desktop**, haga clic en **Command Prompt** (Símbolo del sistema). .

b. Escriba el comando **ping** y la dirección IP para el S1 y presione **Entrar**.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**



¿Tuvo éxito? Rta. No
¿Por qué o por qué no?
Rta. Los switches no están configurados todavía con la dirección IP

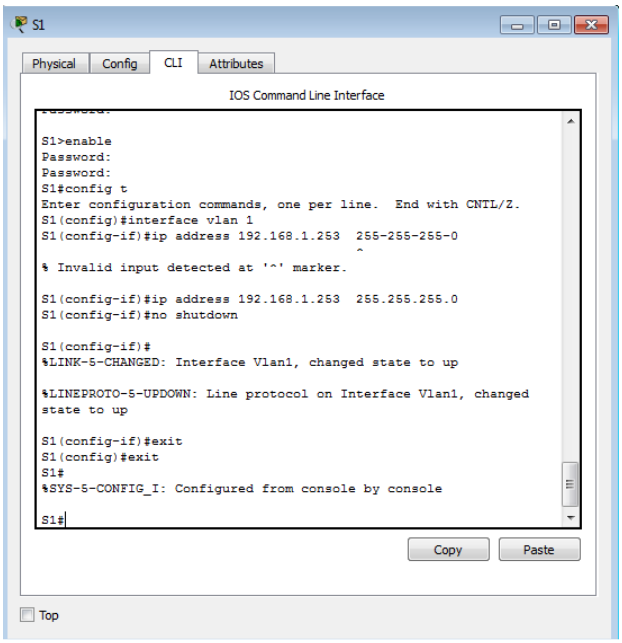
Parte 3: Configurar la interfaz de administración de switches

Configure el S1 y el S2 con una dirección IP.

Paso 1: Configurar el S1 con una dirección IP

Los switches se pueden usar como dispositivos Plug and Play, lo que significa que no es necesario configurarlos para que funcionen. Los switches reenvían información desde un puerto hacia otro sobre la base de direcciones de control de acceso al medio (MAC). Por lo tanto, ¿para qué lo configuraríamos con una dirección IP?
Para conectarse de forma remota a un switch, es necesario asignarle una dirección IP. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1.
Use los siguientes comandos para configurar el S1 con una dirección IP.

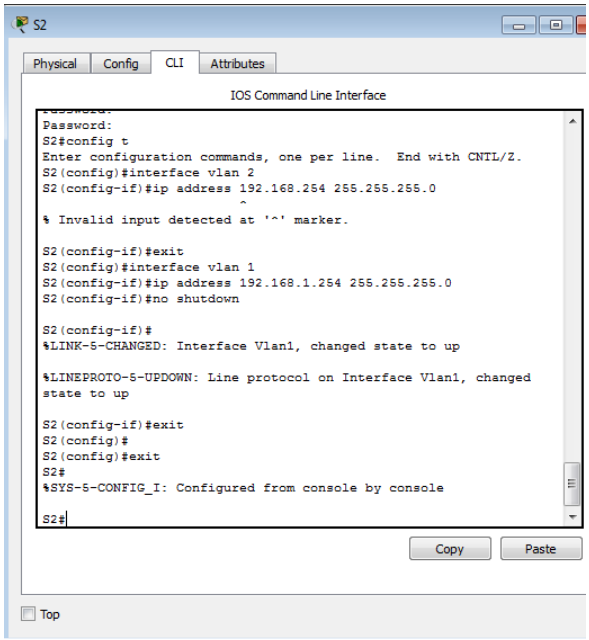
S1 #**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.253 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# **exit**
S1#



¿Por qué debe introducir el comando **no shutdown**? El comando **no shutdown** habilita administrativamente el estado activo de la interfaz.

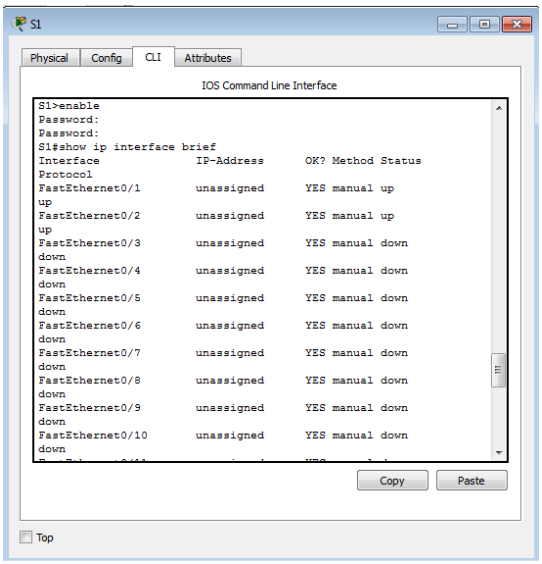
Paso 2: Configurar el S2 con una dirección IP

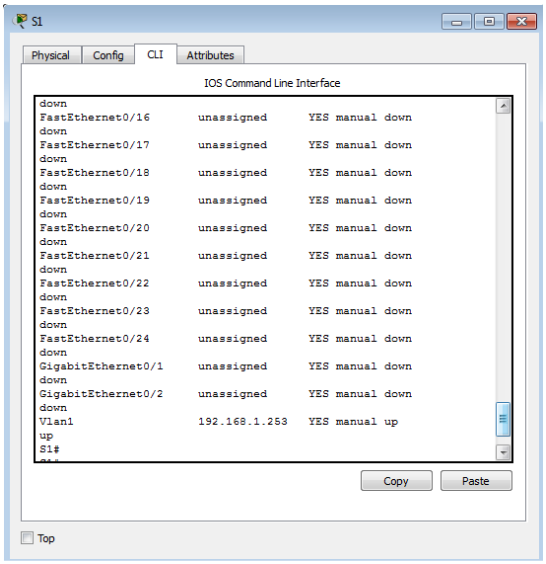
Use la información de la tabla de direccionamiento para configurar el S2 con una dirección IP.

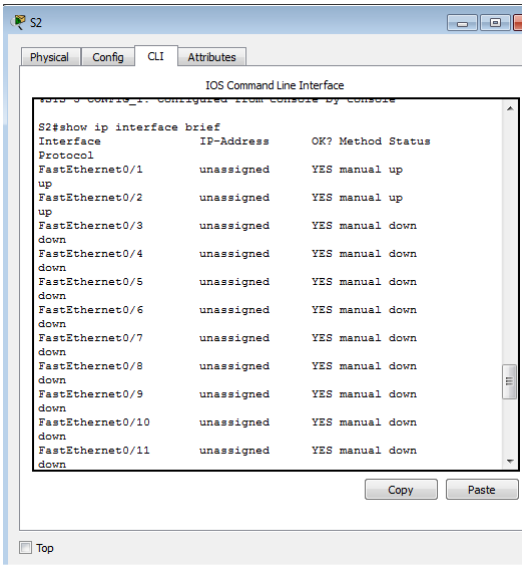


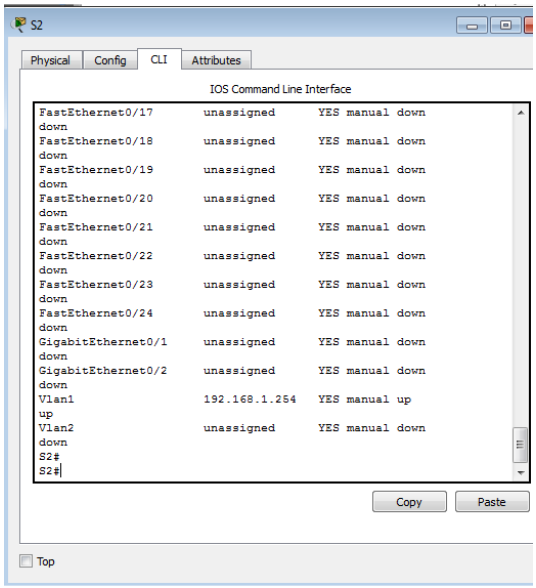
Paso 3: Verificar la configuración de direcciones IP en el S1 y el S2

Use el comando **show ip interface brief** para ver la dirección IP y el estado de todos los puertos y las interfaces del switch. También puede utilizar el comando **show running-config**.



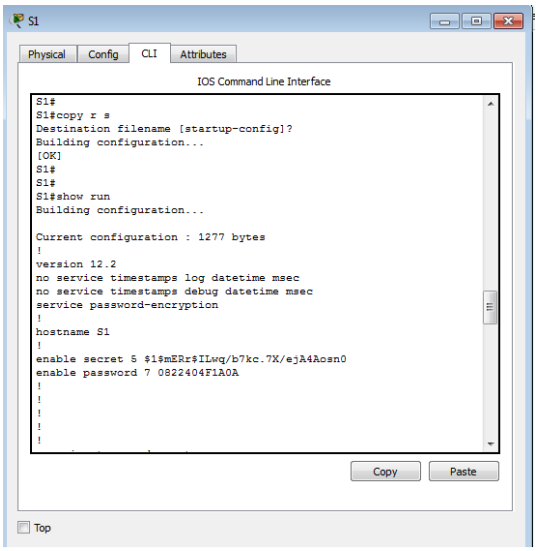


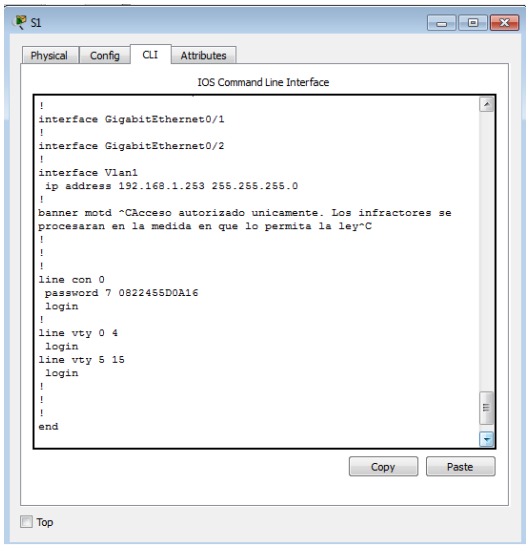


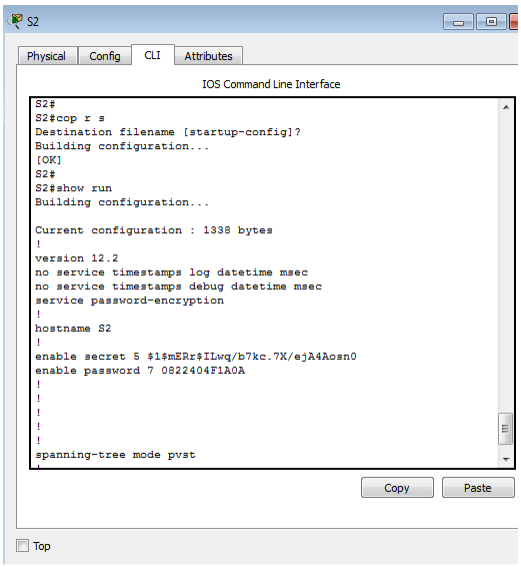


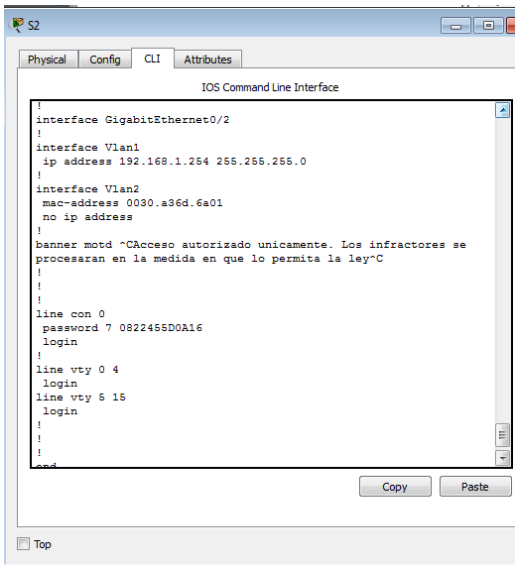
Paso 4: Guardar la configuración para el S1 y el S2 en la NVRAM

¿Qué comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM?
copy run start





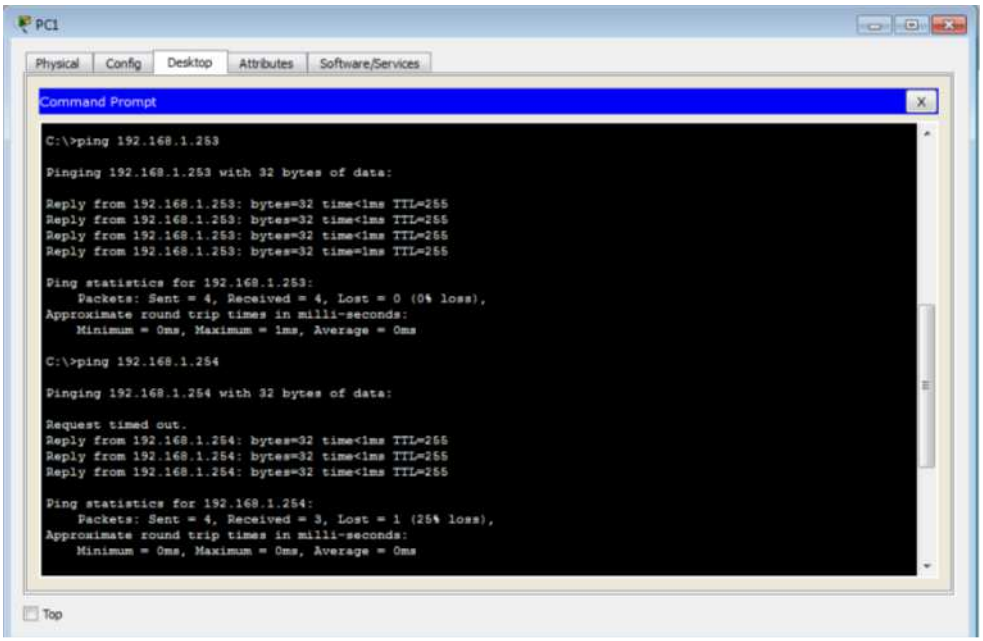


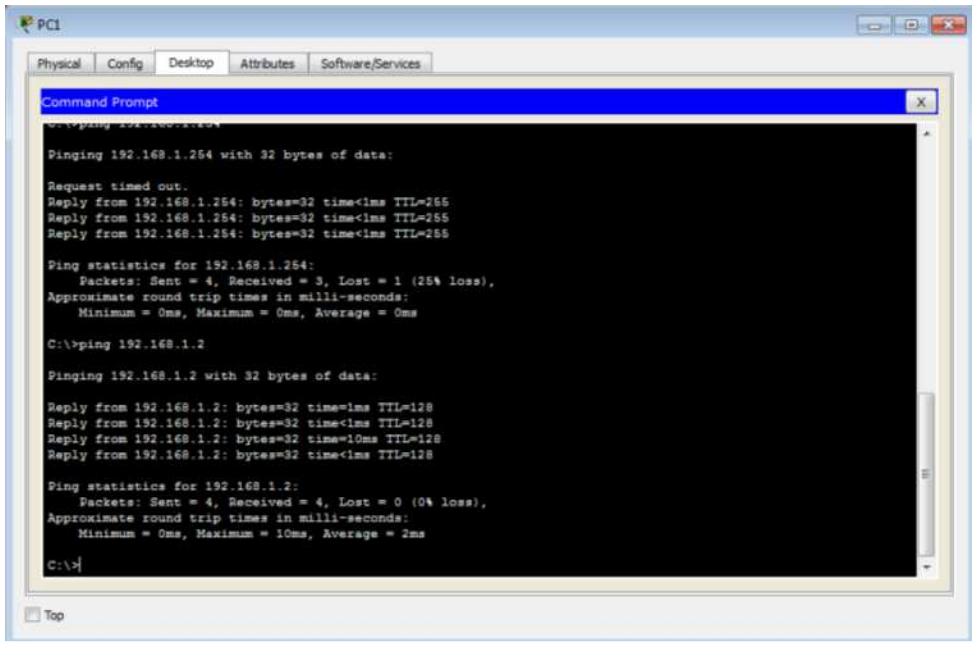


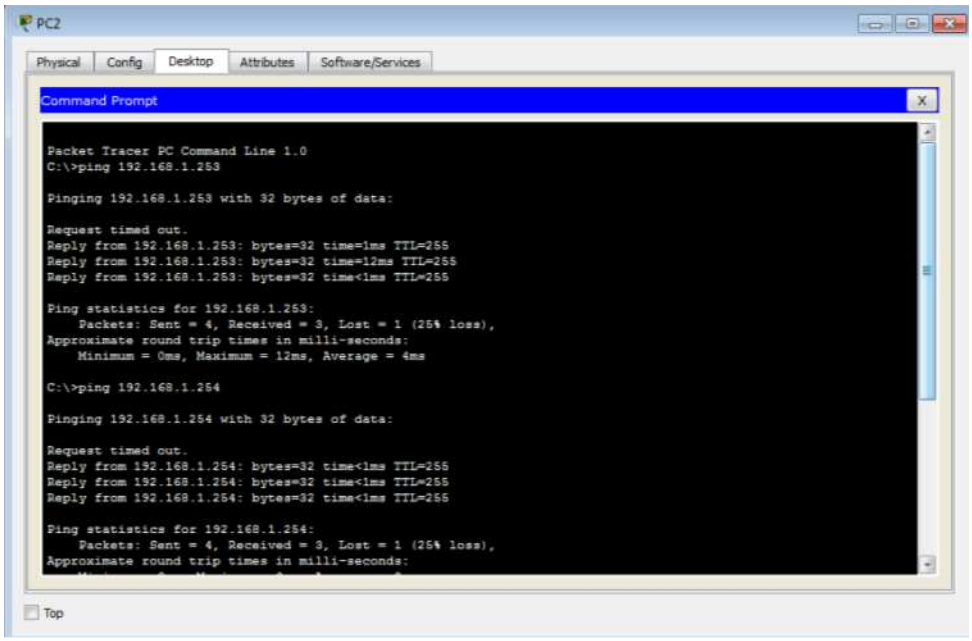
Paso 5: Verificar la conectividad de la red

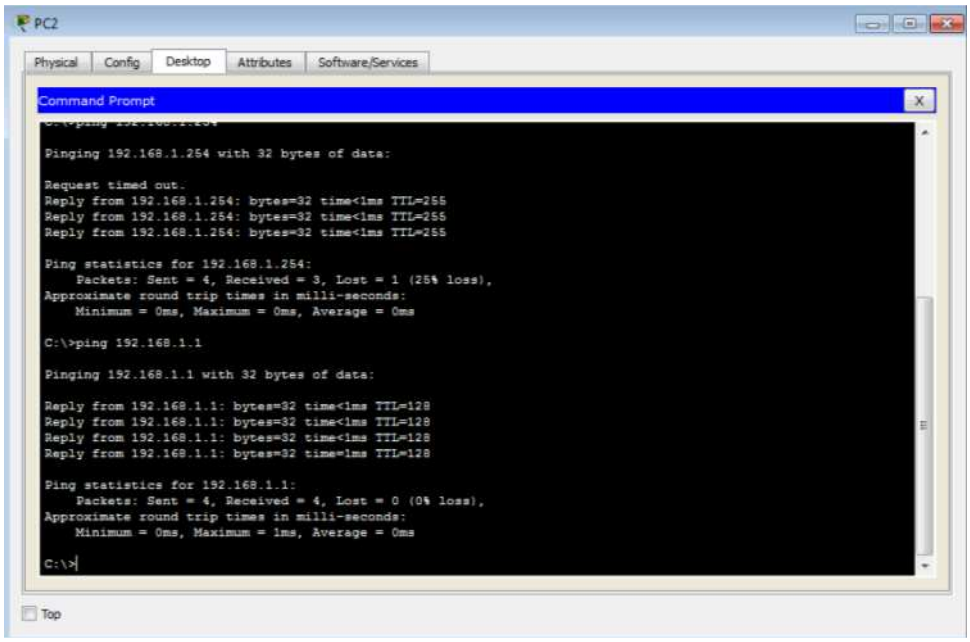
La conectividad de red se puede verificar mediante el comando **ping**. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Haga ping a la dirección IP del S1 y el S2 desde la PC1 y la PC2.

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** (Escritorio).
b. Haga clic en **Command Prompt**.
c. Haga ping a la dirección IP de la PC2.
d. Haga ping a la dirección IP del S1.
e. Haga ping a la dirección IP del S2.


PC1
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
C:\>ping 192.168.1.253
Pinging 192.168.1.253 with 32 bytes of data:
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.253:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.254:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Top

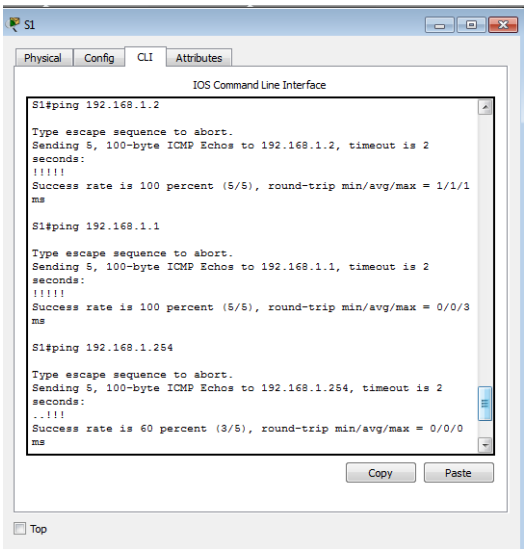

PC1
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.254:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>
Top

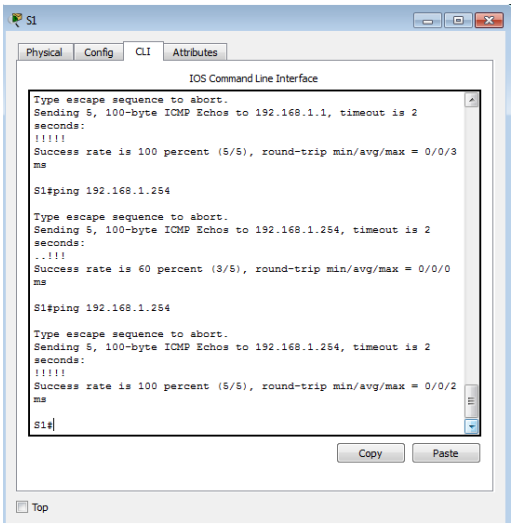


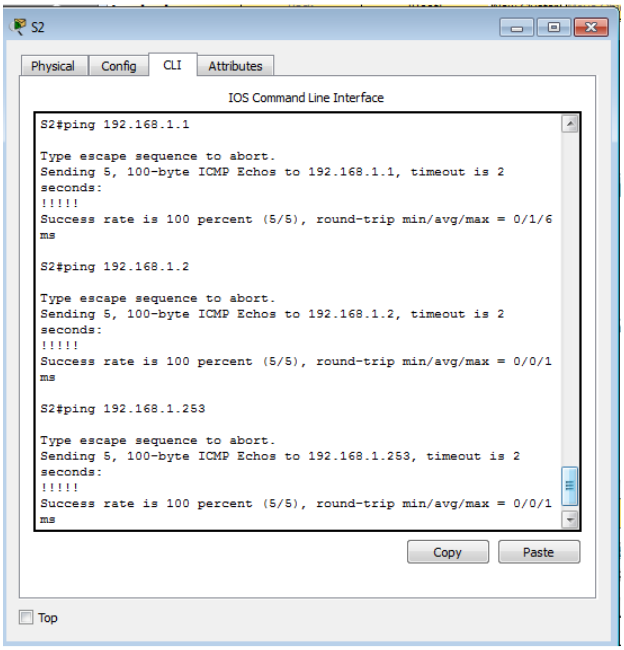


Nota: también puede usar el mismo comando **ping** en la CLI del switch y en la PC2.

Todos los ping deben tener éxito. Si el resultado del primer ping es 80%, vuelva a intentarlo; ahora debería ser 100%. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede hacer ping a ninguno de los dispositivos, vuelva a revisar la configuración para detectar errores.


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
S1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
S1#ping 192.168.1.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
Copy
Paste
Top


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
S1#ping 192.168.1.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
S1#ping 192.168.1.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S1#
Copy
Paste
Top


S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
S2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/6 ms
S2#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S2#ping 192.168.1.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.253, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
Copy
Paste
Top

PRACTICA 2.4.1.2
Packet Tracer: Reto de habilidades de integración

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
[[S1Name]]	VLAN 1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	[[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Objetivos

a. Configurar los nombres de host y las direcciones IP en dos switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).

b. Usar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones de los dispositivos.

c. Utilizar los comandos de IOS para guardar la configuración en ejecución.

d. Configurar dos dispositivos host con direcciones IP.

e. Verificar la conectividad entre los dos dispositivos finales de PC.

Situación

Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante Cisco IOS y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

Requisitos

1) Use una conexión de consola para acceder a cada switch.

2) Nombre los switches **[[S1Name]]** y **[[S2Name]]**.

3) Use la contraseña **[[LinePW]]** para todas las líneas.

4) Use la contraseña secreta **[[SecretPW]]**.

5) Encripte todas las contraseñas de texto no cifrado.

6) Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).

7) Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.

8) Guarde las configuraciones.

9) Verifique la conectividad entre todos los dispositivos.

Packet Tracer: Reto de habilidades de integración

Nota: haga clic en **Check Results** (Verificar resultados) para ver su progreso. Haga clic en **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Si hace clic en esto antes de completar la actividad, se perderán todas las configuraciones.

Índice de isomorfos:
[[indexNames]][[indexPWs]][[indexAdds]][[indexTopos]]

Escenario 1

Dispositivo	Interfaz	Dirección	Máscara de subred
Clase-A	VLAN 1	128.107.20.10	255.255.255.0
Clase-B	VLAN1	128.107.20.15	255.255.255.0
Estudiante 1	NIC	128.107.20.25	255.255.255.0
Estudiante 2	NIC	128.107.20.30	255.255.255.0

Escenario 2

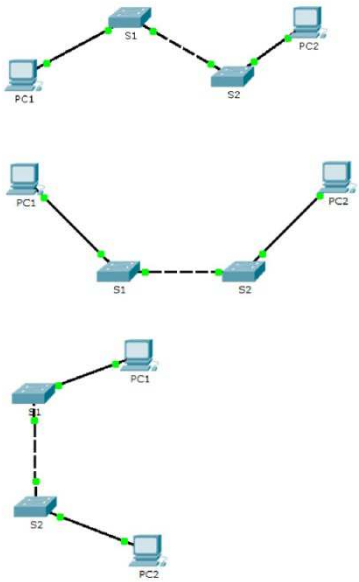
Dispositivo	Interfaz	Dirección	Máscara de subred
Aula 145	VLAN 1	172.16.5.35	255.255.255.0
Aula 146	VLAN 1	172.16.5.40	255.255.255.0
Gerente	NIC	172.16.5.50	255.255.255.0
Recepción	NIC	172.16.5.60	255.255.255.0

Escenario 3

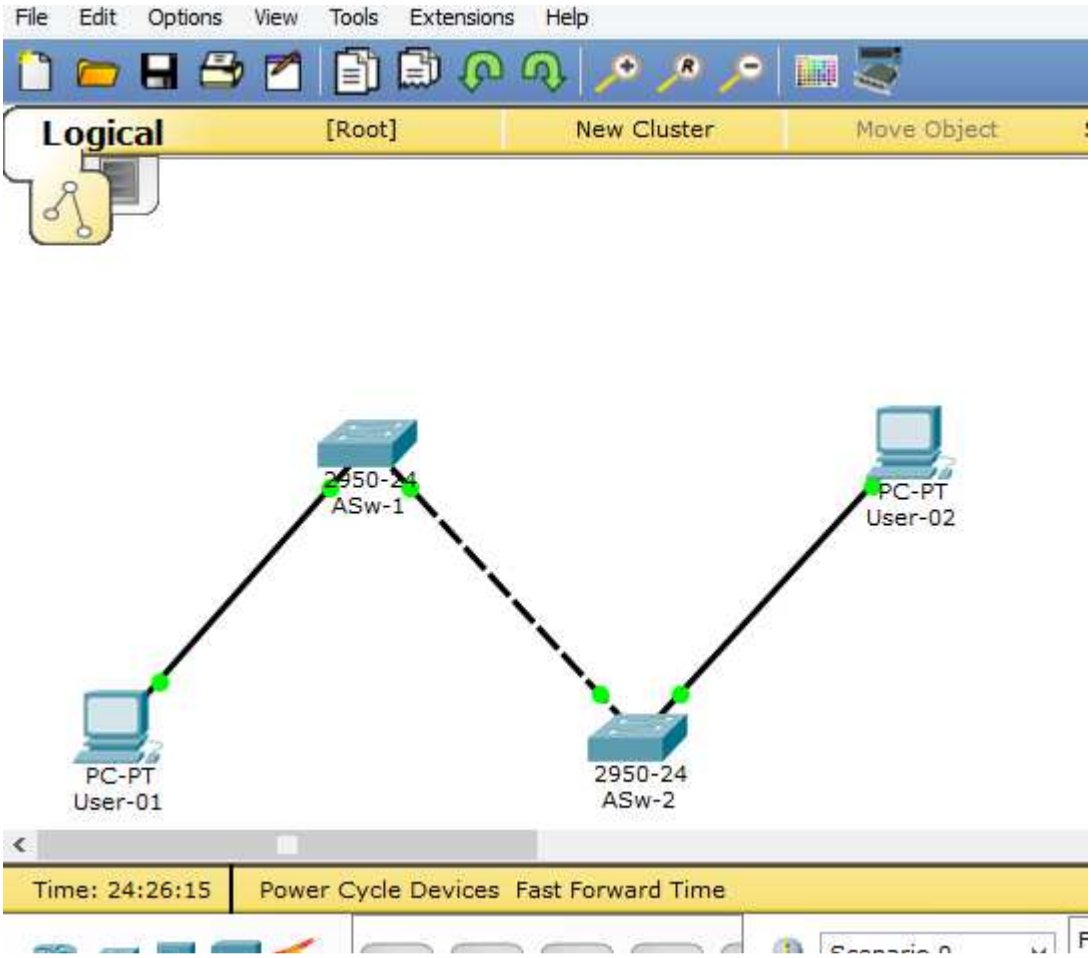
Dispositivo	Interfaz	Dirección	Máscara de subred
ASw-1	VLAN 1	10.10.10.100	255.255.255.0
ASw-2	VLAN 1	10.10.10.150	255.255.255.0
Usuario 01	NIC	10.10.10.4	255.255.255.0
Usuario 02	NIC	10.10.10.5	255.255.255.0

Packet Tracer: Reto de habilidades de integración

Isomorfos de la topología

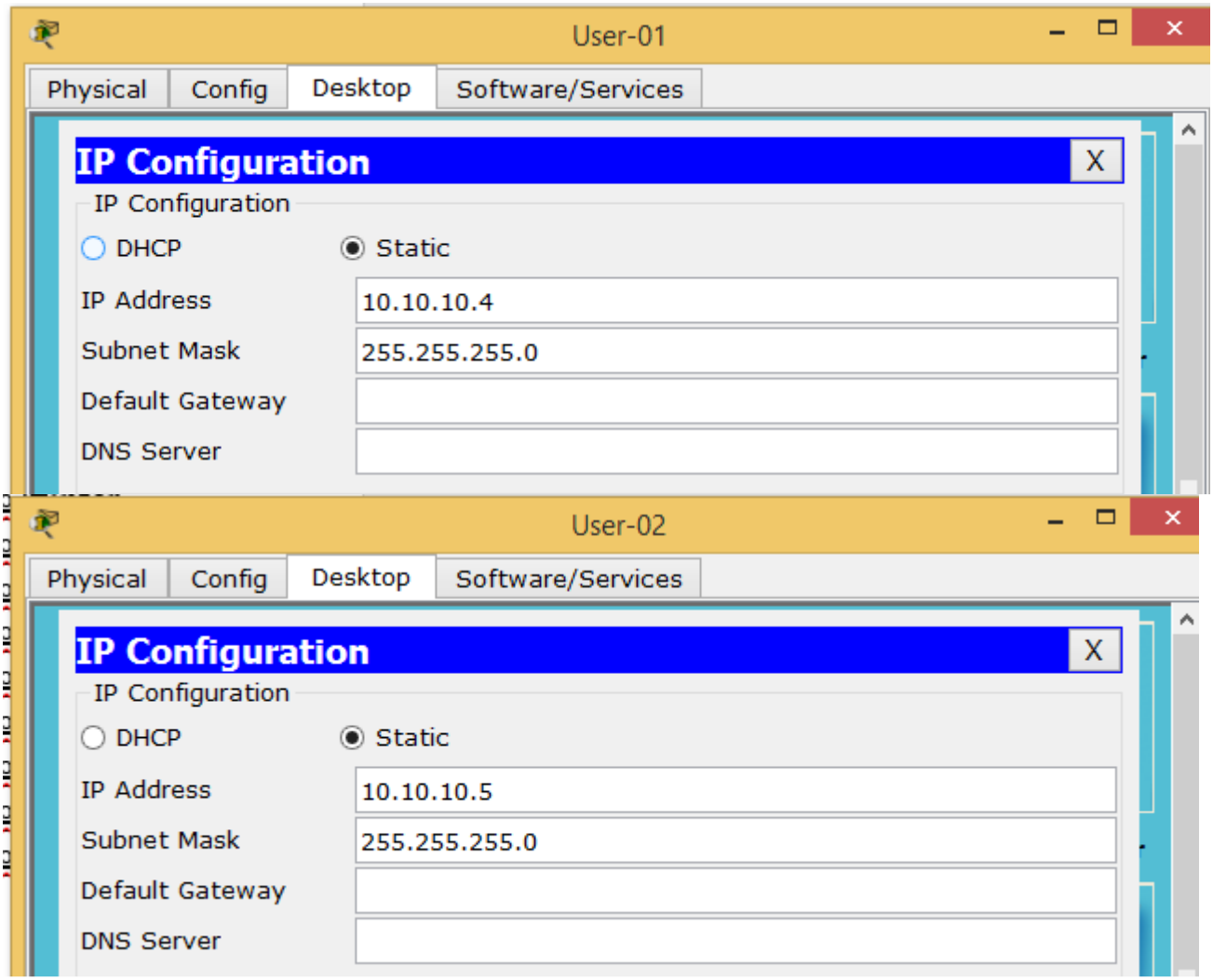


EVIDENCIAS



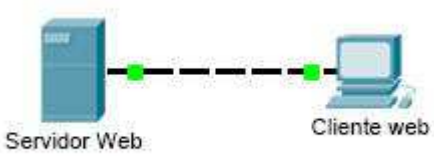

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname ASw-1
ASw-1(config)#line console 0
ASw-1(config-line)#password xAw6k
ASw-1(config-line)#exit
ASw-1(config)#enable secret 6EBUp
ASw-1(config)#banner motd "warning"
ASw-1(config)#interface vlan 1
ASw-1(config-if)#ip address 10.10.10.100 255.255.255.0
ASw-1(config-if)#no shutdown

Switch>enable
Switch#configure terminal
Switch(config)#hostname ASw-2
ASw-2(config)#line console 0
ASw-2(config-line)#password xAw6k
ASw-2(config-line)#exit
ASw-2(config)#enable secret 6EBUp
ASw-2(config)#banner motd "warning"
ASw-2(config)#interface vlan 1
ASw-2(config-if)#ip a
```

ASw-2(config-if)#ip address 10.10.10.150 255.255.255.0
ASw-2(config-if)#no shutdown .



PRACTICA 3.2.4.6
Packet Tracer: Investigación de los modelos TCP/IP y OSI en acción

Topología



Objetivos

Parte 1: Examinar el tráfico Web HTTP

Parte 2: Mostrar elementos de la suite de protocolos TCP/IP

Información básica

Esta actividad de simulación tiene como objetivo proporcionar una base para comprender la suite de protocolos TCP/IP y la relación con el modelo OSI. El modo de simulación le permite ver el contenido de los datos que se envían a través de la red en cada capa.
A medida que los datos se desplazan por la red, se dividen en partes más pequeñas y se identifican de modo que las piezas se puedan volver a unir cuando lleguen al destino. A cada pieza se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data units]) y se la asocia a una capa específica de los modelos TCP/IP y OSI. El modo de simulación de Packet Tracer le permite ver cada una de las capas y la PDU asociada. Los siguientes pasos guían al usuario a través del proceso de solicitud de una página Web desde un servidor Web mediante la aplicación de explorador Web disponible en una PC cliente.
Aunque gran parte de la información mostrada se analizará en mayor detalle más adelante, esta es una oportunidad de explorar la funcionalidad de Packet Tracer y de ver el proceso de encapsulación.

Parte 1: Examinar el tráfico Web HTTP

En la parte 1 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para generar tráfico Web y examinar HTTP.

Paso 1: Cambie del modo de tiempo real al modo de simulación.

En la esquina inferior derecha de la interfaz de Packet Tracer, hay fichas que permiten alternar entre el modo **Realtime** (Tiempo real) y **Simulation** (Simulación). PT siempre se inicia en el modo **Realtime**, en el que los protocolos de red operan con intervalos realistas. Sin embargo, una excelente característica de Packet Tracer permite que el usuario “detenga el tiempo” al cambiar al modo de simulación. En el modo de simulación, los paquetes se muestran como sobres animados, el tiempo se desencadena por eventos y el usuario puede avanzar por eventos de red.

f. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.

g. Seleccione **HTTP** de **Event List Filters** (Filtros de lista de eventos).
Packet Tracer: investigación de los modelos TCP/IP y OSI en acción

10) Es posible que HTTP ya sea el único evento visible. Haga clic en **Edit Filters** (Editar filtros) para mostrar los eventos visibles disponibles. Alterne la casilla de verificación **Show All/None** (Mostrar todo/ninguno) y observe cómo las casillas de verificación se desactivan y se activan, o viceversa, según el estado actual.

11) Haga clic en la casilla de verificación **Show all/None** (Mostrar todo/ninguno) hasta que se desactiven todas las casillas y luego

seleccione **HTTP**. Haga clic en cualquier lugar fuera del cuadro **Edit Filters** (Editar filtros) para ocultarlo. Los eventos visibles ahora deben mostrar solo 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.

a. Haga clic en **Web Client** (Cliente Web) 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 **www.osi.local** y haga clic en **Go** (Ir).

   Debido a que el tiempo en el modo de simulación se desencadena por eventos, debe usar el botón **Capture/Forward** (Capturar/avanzar) para mostrar los eventos de red.

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

a. Haga clic en el primer cuadro coloreado debajo de la columna **Event List** > **Info** (Lista de eventos > Información). Quizá sea necesario expandir el **panel de simulación** o usar la barra de desplazamiento que se encuentra directamente debajo de la **lista de eventos**.

   Se muestra la ventana **PDU Information at Device: Web Client** (Información de PDU en dispositivo: cliente Web). En esta ventana, solo hay dos fichas, **OSI Model** (Modelo OSI) y **Outbound PDU Details** (Detalles de PDU saliente), debido a que este es el inicio de la transmisión. A medida que se analizan más eventos, se muestran tres fichas, ya que se agrega la ficha **Inbound PDU Details** (Detalles de PDU entrante). Cuando un evento es el último evento del stream de

tráfico, solo se muestran las fichas **OSI Model** e **Inbound PDU Details**.

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**? 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)?

   “1. The HTTP client sends a HTTP request to the server.” (“El cliente HTTP envía una solicitud de HTTPal 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.)? 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.)? 192.168.1.254

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

   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?

   SRC IP (IP DE ORIG.) yDST 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?

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**?
www.osi.local, capa 7

g. Haga clic en el siguiente cuadro coloreado en la columna **Event List** > **Info** (Lista de eventos > Información). Solo la capa 1 está activa (sin atenuar). El dispositivo mueve la trama desde el búfer y la coloca en la red.

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?

Se intercambiaron los puertos de origen y destino, las direcciones IPde 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?

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?

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

En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer para ver y examinar algunos de los otros protocolos que componen la suite TCP/IP.

Paso 1: Ver eventos adicionales

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

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.

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.

c. Haga clic en el primer evento de DNS en la columna **Info**. Examine las fichas **OSI Model** y **PDU Detail**, y observe el proceso de encapsulación. Al observar la ficha **OSI Model** con el cuadro **Layer 7** resaltado, se incluye una descripción de lo que ocurre, inmediatamente debajo de **In Layers** y **Out Layers**: (“1. The DNS client sends a DNS query to the DNS server.” [“El cliente DNS envía una consulta DNS al servidor DNS”]). Esta información es muy útil para ayudarlo a comprender qué ocurre durante el proceso de comunicación.

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)?

www.osilocal

e. Haga clic en el último cuadro coloreado **Info** de DNS en la lista de

eventos. ¿Qué dispositivo se muestra?
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**?

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?

   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)? CERRAR la conexión.

Desafío

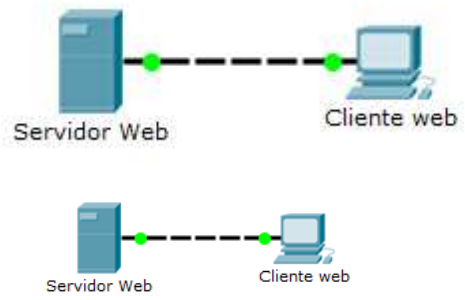
En esta simulación, se proporcionó un ejemplo de una sesión Web entre un cliente y un servidor en una red de área local (LAN). El cliente realiza solicitudes de servicios específicos que se ejecutan en el servidor. Se debe configurar el servidor para que escuche puertos específicos y detecte una solicitud 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? La primera PDU HTTP que solicita el cliente Web muestra el puerto 80 en el puerto DST (DESTINO) de capa 4.

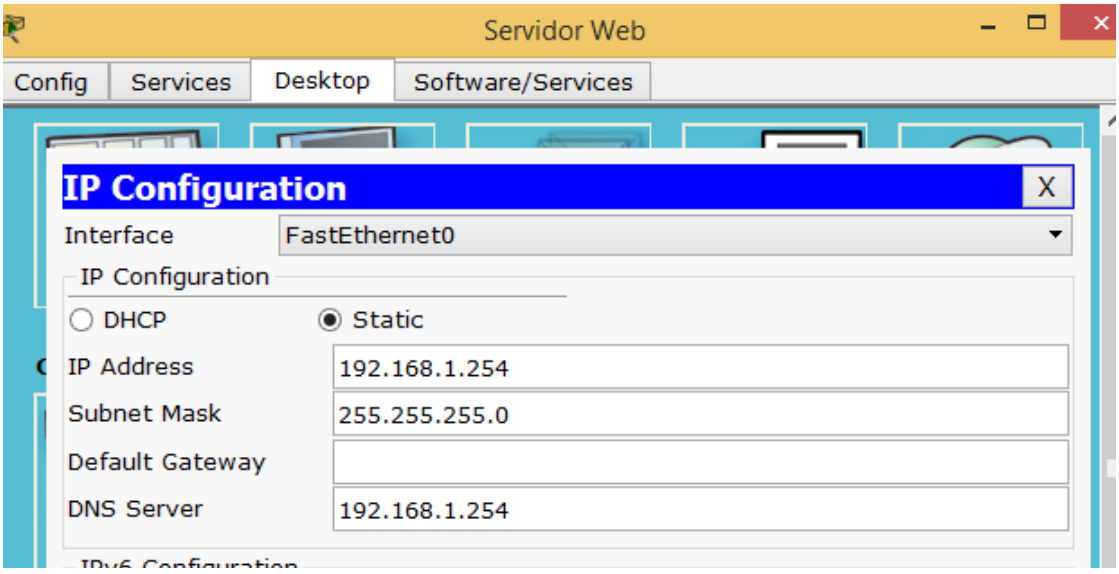
¿Qué puerto escucha el **servidor Web** para detectar una solicitud de DNS? La primera PDU DNS que solicita el cliente Web muestra que el puerto de destino de capa 4 es el puerto 53.

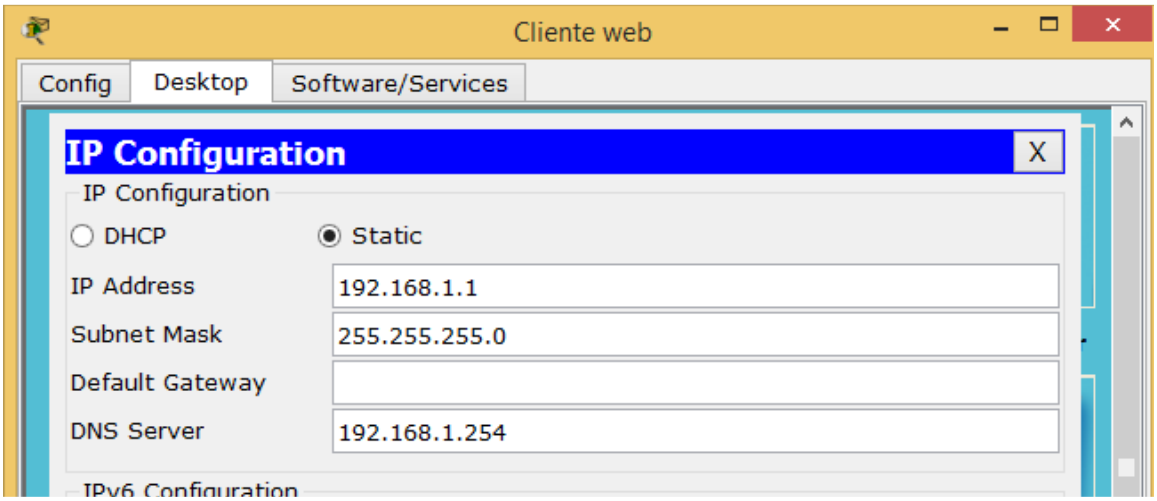
EVIDENCIAS



DU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Servid...	Cliente web	ICMP		0.000	N	0	(edit)	
	Successful	Servid...	Cliente web	ICMP		0.000	N	1	(edit)	

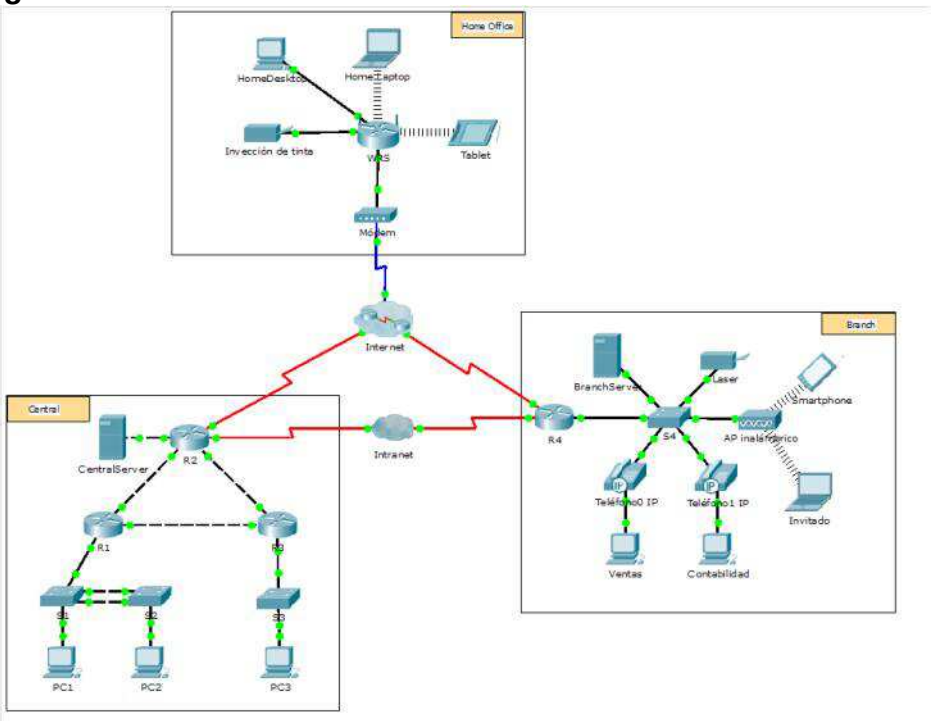




PRACTICA 3.3.3.3
Packet Tracer: Exploración de una red

En esta actividad, se utiliza una topología compleja y un dominio del nivel superior ficticio (.pta) para evitar conflictos con la nomenclatura para Internet. Dado que PT no reenvía las solicitudes de DNS, se crearon las mismas entradas en cada servidor DNS para que el tráfico DNS pueda seguir siendo local cuando es importante hacerlo. Para abordar el uso de direccionamiento privado RFC 1918, se utiliza NAT en la oficina doméstica y en la sucursal, a fin de evitar cualquier concepto erróneo.

Topología



Objetivos

Parte 1: Examinar el tráfico de internetwork en la sucursal
Parte 2: Examinar el tráfico de internetwork a la central
Parte 3: Examinar el tráfico de Internet desde la sucursal

Información básica

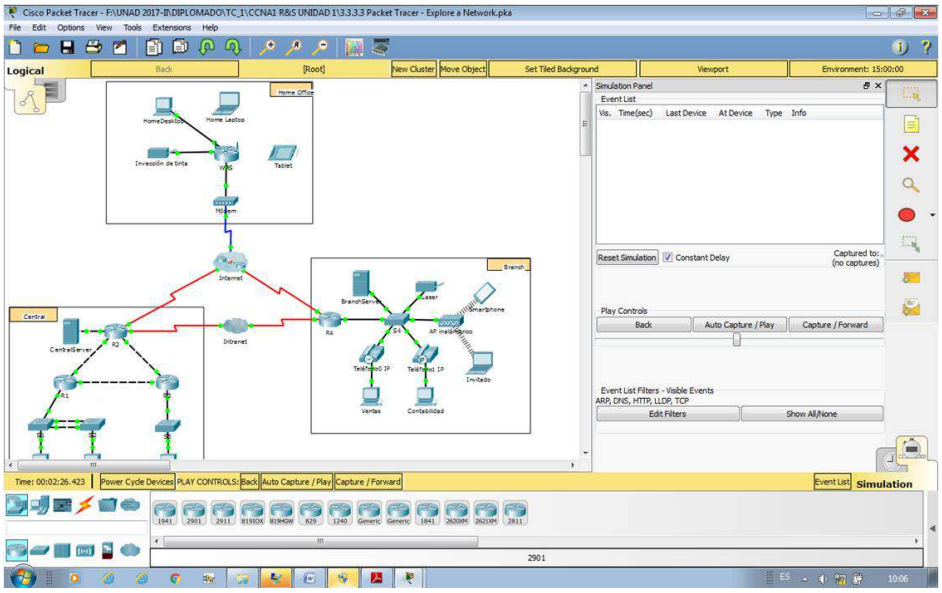
El objetivo de esta actividad de simulación es ayudarlo a comprender el flujo de tráfico y el contenido de los paquetes de datos a medida que atraviesan una red compleja. Las comunicaciones se examinarán en tres ubicaciones distintas que simulan redes comerciales y domésticas típicas.
Tómese unos minutos para analizar la topología que se muestra. La ubicación Central tiene tres routers y varias redes que posiblemente representen distintos edificios dentro de un campus. La ubicación Branch (Sucursal) tiene solo un router con una conexión a Internet y una conexión dedicada de red de área

extensa (WAN) a la ubicación Central. La Home Office (Oficina doméstica) utiliza una conexión de banda ancha con módem por cable para proporcionar acceso a Internet y a los recursos corporativos a través de Internet.
Los dispositivos en cada ubicación utilizan una combinación de direccionamiento estático y dinámico. Los dispositivos se configuran con gateways predeterminados y con información del Sistema de nombres de dominios (DNS), según corresponda.

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).

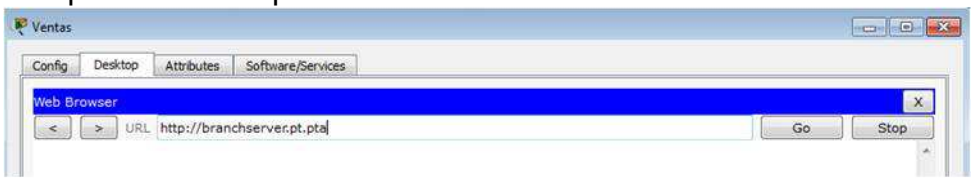


Paso 2: Generar tráfico mediante un explorador Web

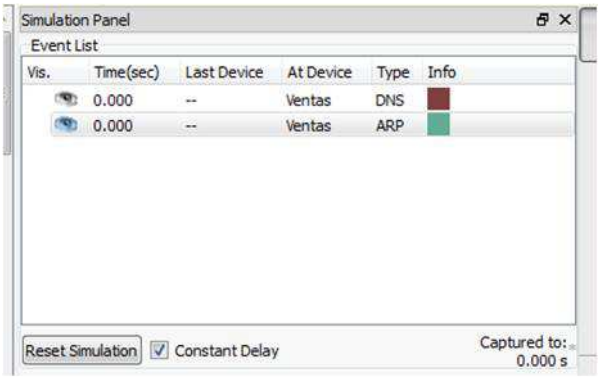
El panel de simulación actualmente está vacío. En Event List (Lista de eventos), en la parte superior del panel de simulación, hay seis columnas en el encabezado. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar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

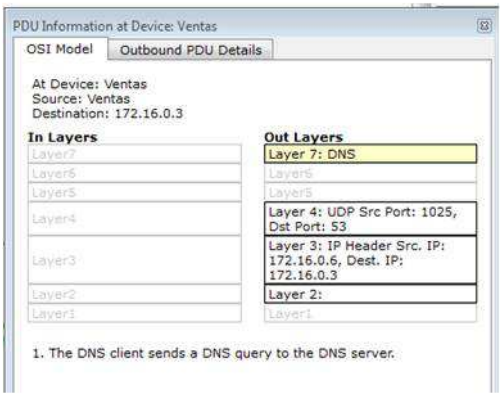
a. Haga clic en **Sales PC** (PC de ventas) en el panel del extremo izquierdo.
b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.
c. En el campo de dirección URL, introduzca **http://branchserver.pt.pta** y haga clic en **Go** (Ir). Observe 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.



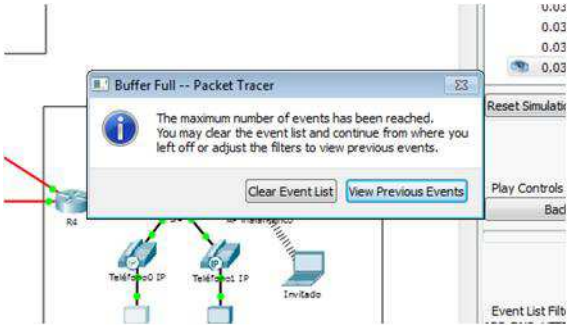
d. Haga clic en el cuadro de información de **DNS**. En **Out Layers** (Capas de salida), se indica DNS para la capa 7. La capa 4 utiliza UDP para comunicarse con el servidor DNS en el puerto 53 (**Dst Port:** [Pto. de destino:]). Se indica tanto la dirección IP de origen como la de destino. ¿Qué información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



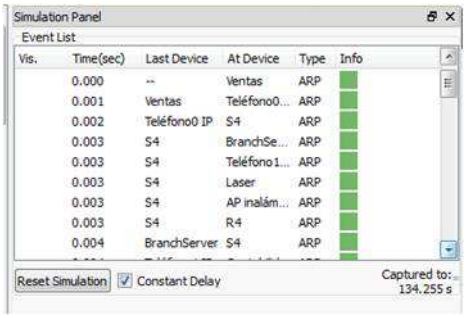
La información de capa 2, específicamente la dirección MAC de destino.

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

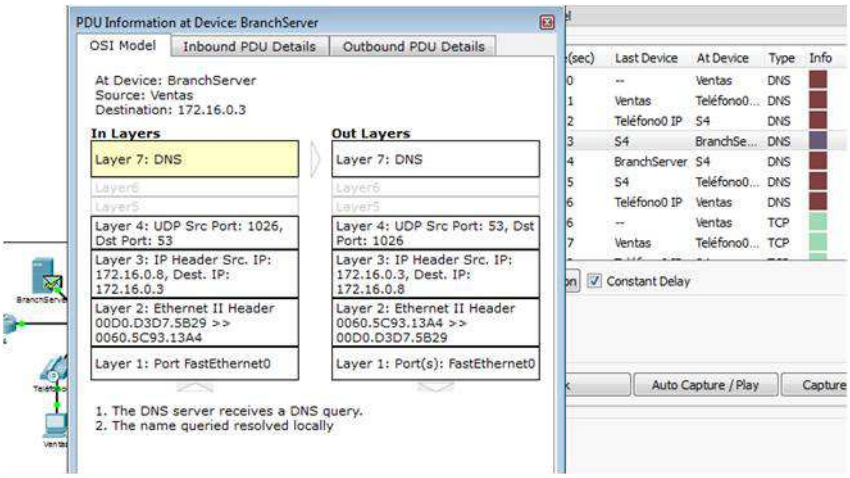
desplazarse hasta la parte superior de la lista y observe la cantidad de eventos de **ARP**. Observe la columna Device (Dispositivo) en la lista de eventos: ¿cuántos de los dispositivos en la ubicación Branch atraviesa la solicitud de **ARP**?



Todos los dispositivos recibieron una solicitud de ARP.

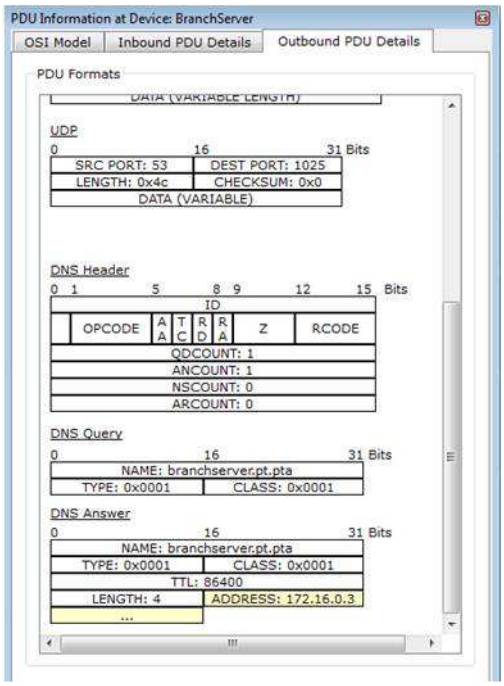


f. Desplácese por los eventos en la lista hasta la serie de eventos de **DNS**. Seleccione el evento de **DNS** para el que se indica **BranchServer** en At Device (En el dispositivo). Haga clic en el cuadro de la columna **Info**. ¿Qué se puede determinar seleccionando la capa 7 en **OSI Model** (Modelo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



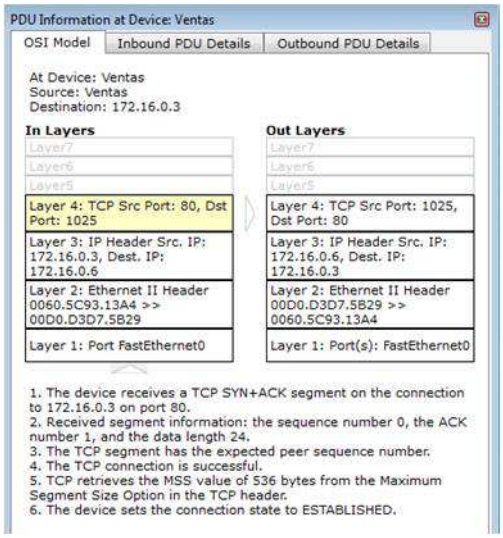
El servidor DNS recibe una consulta DNS. La consulta del nombre se resuelve de forma local.

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?



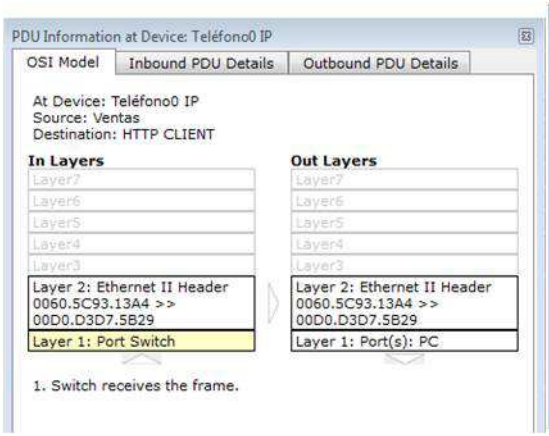
172.16.0.3, la dirección de Branchserver.

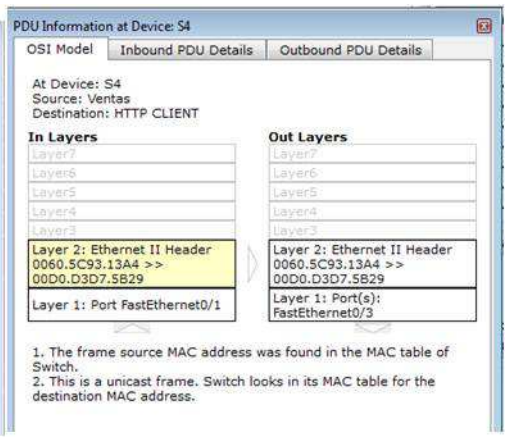
h. Los eventos siguientes son eventos de **TCP** que permiten que se establezca un canal de comunicación. En el dispositivo **Sales**, seleccione el último evento de **TCP** anterior al evento de **HTTP**. Haga clic en el cuadro coloreado Info para ver la información de PDU. Resalte Layer 4 (Capa 4) 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

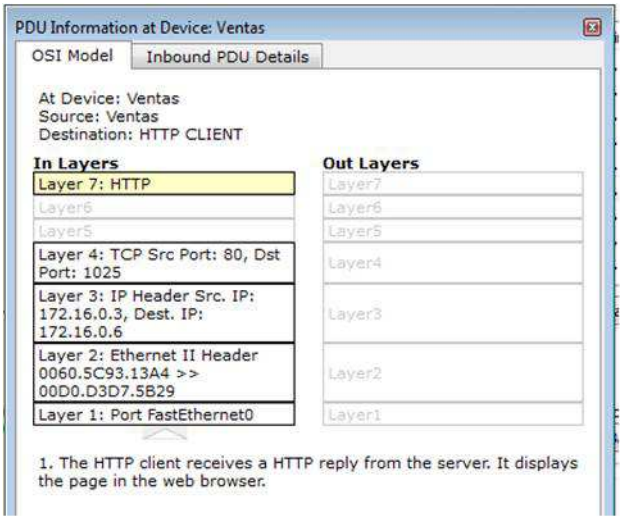
i. Los eventos siguientes son eventos de **HTTP**. Seleccione cualquiera de los eventos de **HTTP** en un dispositivo intermediario (teléfono IP o switch). ¿Cuántas capas están activas en uno de estos dispositivos y por qué?



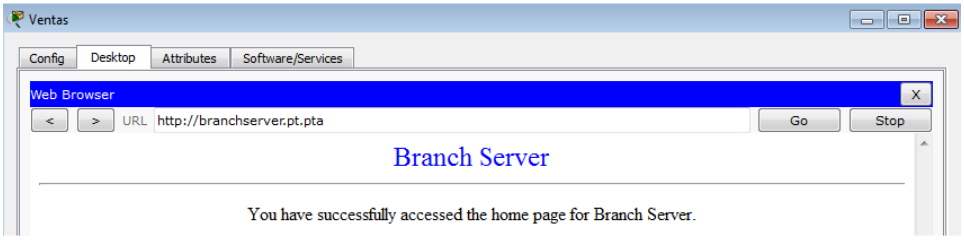


Dos capas, porque son dispositivos de capa 2.

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

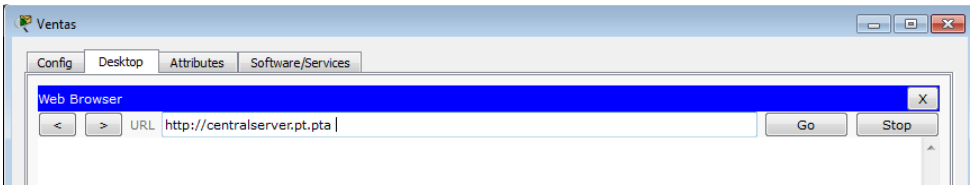
En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer (PT) para ver y examinar cómo se administra el tráfico que sale de la red local.

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

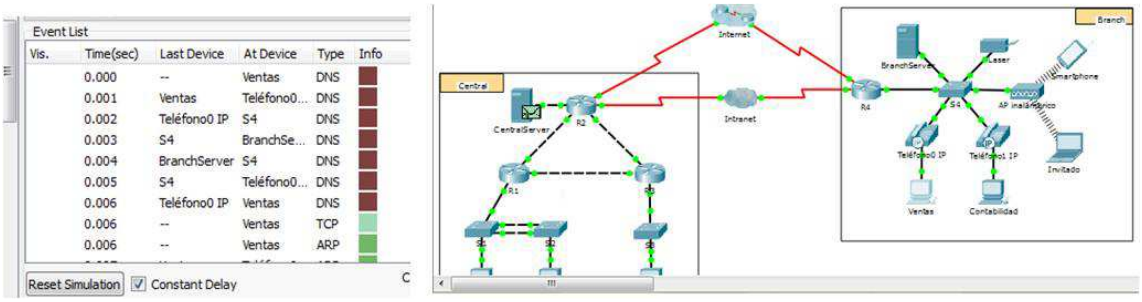
a. Cierre todas las ventanas de información de PDU abiertas.

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.

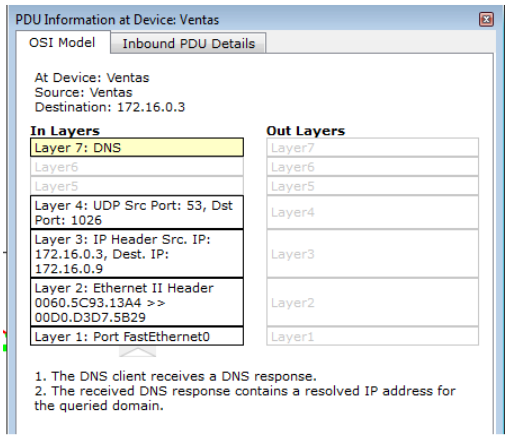


d. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe 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?



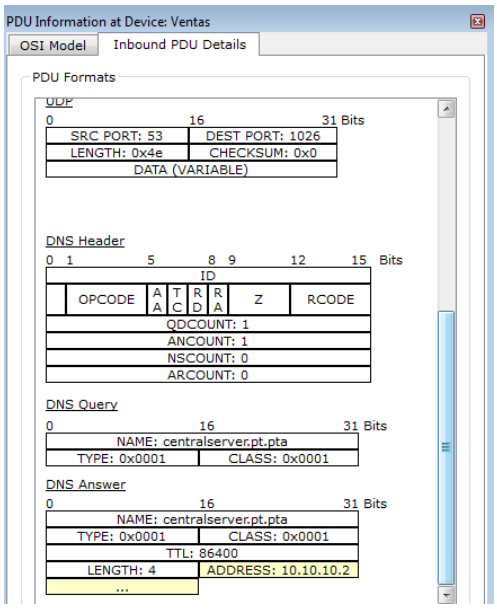
PC Ventas ya conoce la dirección MAC del servidor DNS.

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?

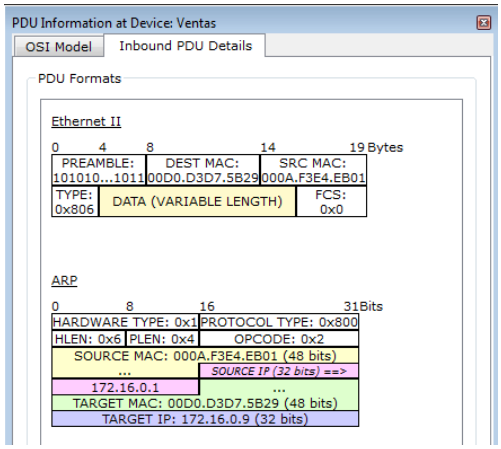


El servidor DNS pudo resolver el nombre de dominio para centralserver.pt.pta.

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.

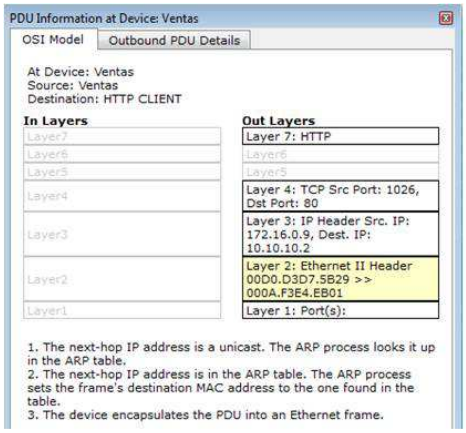


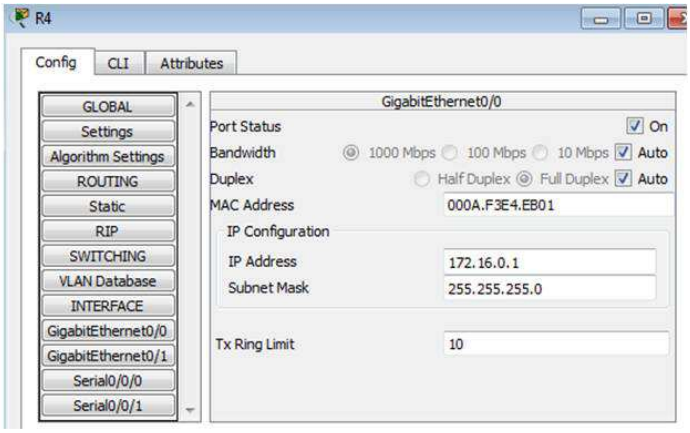
g. Los eventos siguientes son eventos de **ARP**. Haga clic en el cuadro coloreado Info del último evento de **ARP**. Haga clic en la ficha **Inbound PDU Details** y observe la dirección MAC. Sobre la base de la información en la sección de ARP, ¿qué dispositivo proporciona la respuesta de ARP?



El router R4, el dispositivo de Gateway.

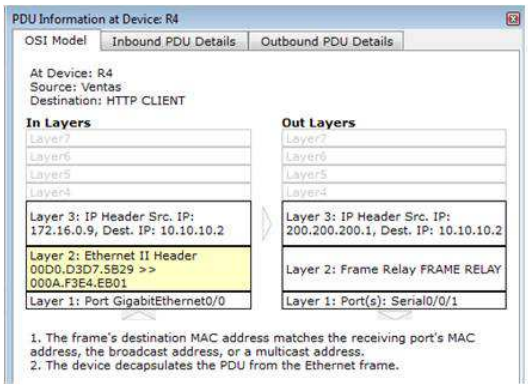
h. Los eventos siguientes son eventos de **TCP**, que nuevamente se preparan para establecer un canal de comunicación. Busque el primer evento de **HTTP** en Event List. Haga clic en el cuadro coloreado del evento de **HTTP**. Resalte Layer 2 (Capa 2) en la ficha **OSI Model**. ¿Qué se puede determinar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

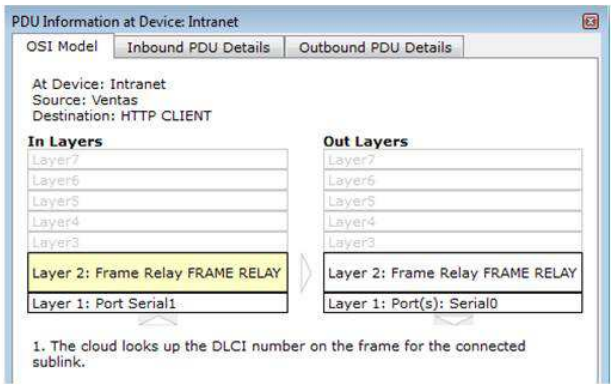




Es la dirección MAC del router R4.

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?





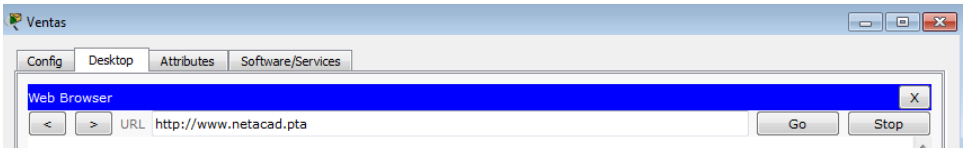
Frame Relay FRAME RELAY.

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.

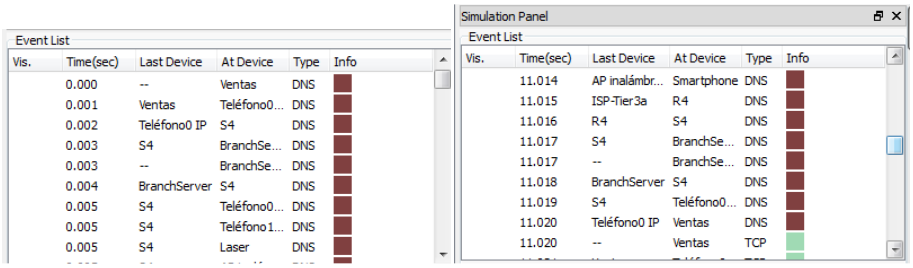
Parte 3: Examinar el tráfico de Internet desde la sucursal
En la parte 3 de esta actividad, borrará los eventos y comenzará una nueva solicitud Web que usará Internet.

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.

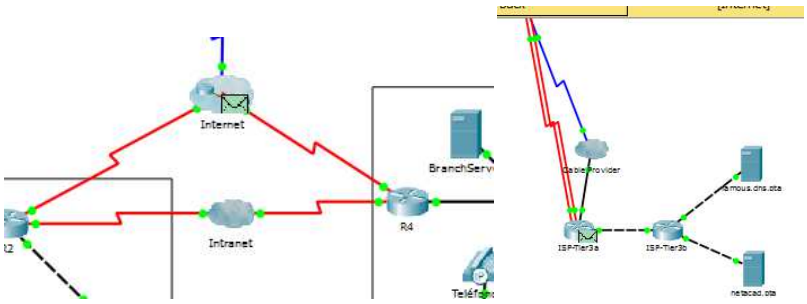


c. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS**. ¿Qué advierte sobre la cantidad de eventos de **DNS**?



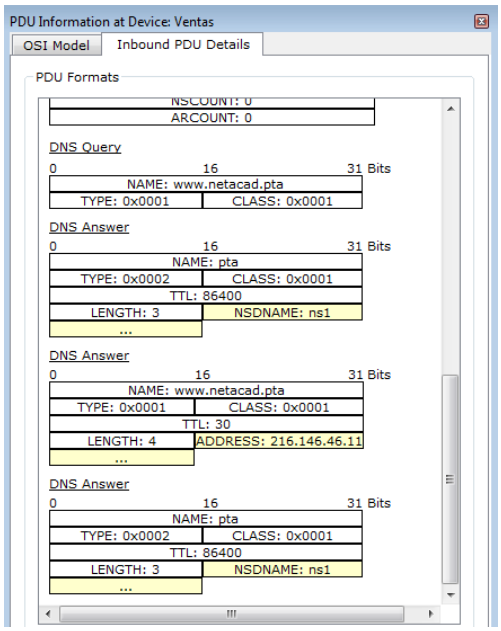
Hay muchos más eventos de DNS. Dado que la entrada de DNS no es local, se reenvía hacia un servidor en Internet.

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?

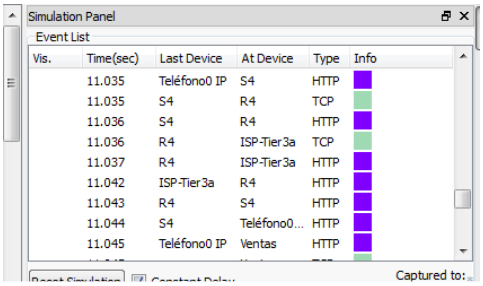


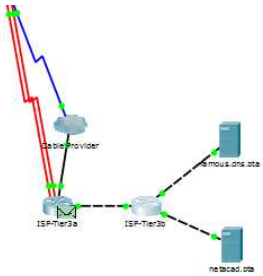
En la nube de Internet. Se debe mostrar a los estudiantes que esos dispositivos se pueden ver haciendo clic en la nube y luego en el enlace Back (Atrás) para regresar.

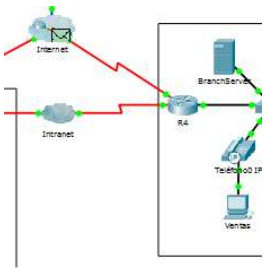
e. Haga clic en el último evento de **DNS**. Haga clic en la ficha **Inbound PDU Details** y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para **www.netacad.pta**? 216.146.46.11



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?

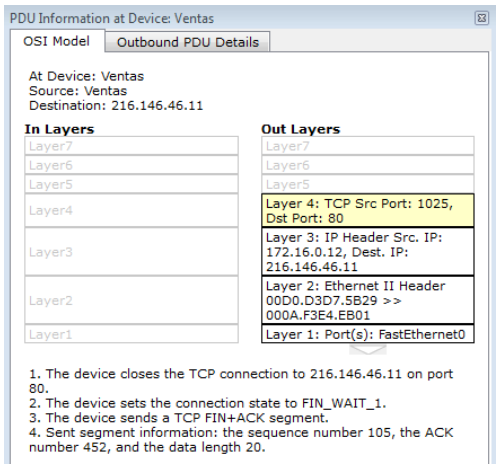




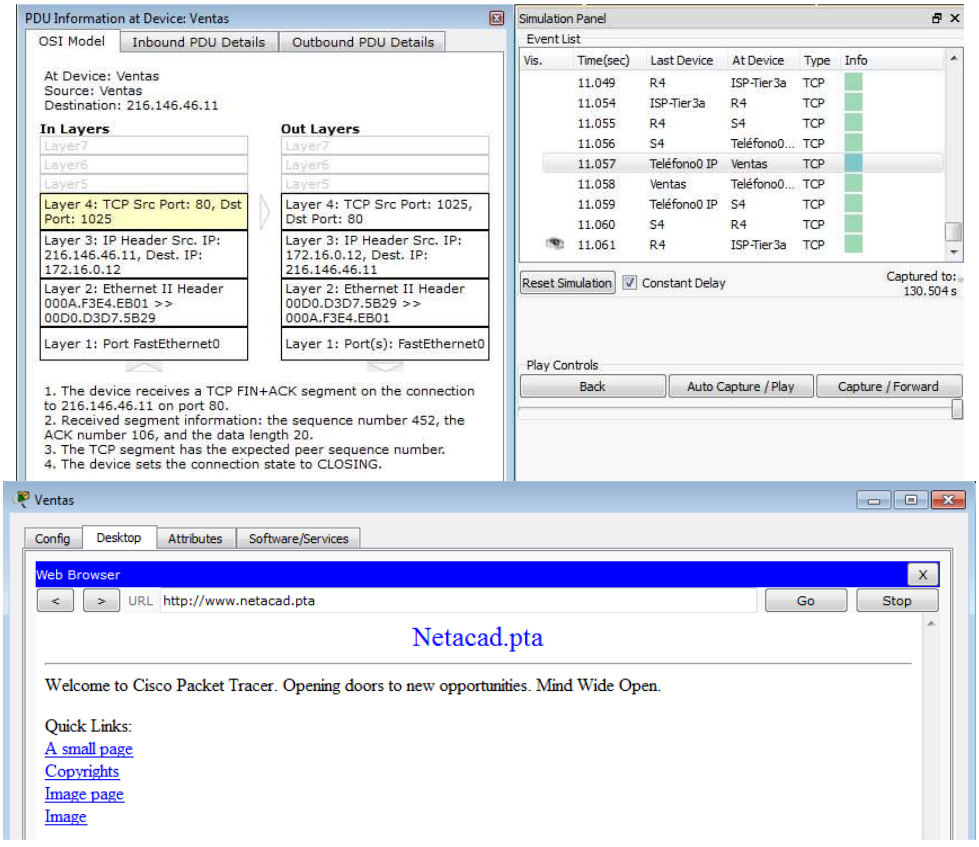


Hay tres routers (ISP-Tier3a, ISP-Tier3b y R4); sin embargo, hay cuatro eventos de HTTP que los atraviesan.

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? Cerrada



PRACTICA 4.2.4.5

Conexión de una LAN por cable y una LAN inalámbrica

Topología

Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IP	Conectar a
Nube	Eth6	No aplicable	Fa0/0
	Coax7	No aplicable	Port0
Módem por cable	Port0	No aplicable	Coax7
	Puerto1	No aplicable	Internet
Router0	Consola	No aplicable	RS232
	Fa0/0	192.168.2.1/24	Eth6
	Fa0/1	10.0.0.1/24	Fa0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	Fa1/0	172.16.0.1/24	Fa0/1
Router inalámbrico	Internet	192.168.2.2/24	Puerto 1
	Eth1	192.168.1.1	Fa0
PC familiar	Fa0	192.168.1.102	Eth1
Switch	Fa0/1	172.16.0.2	Fa1/0
Netacad.pka	Fa0	10.0.0.1	Fa0/1
Terminal de configuración	RS232	No aplicable	Consola

Objetivos

Parte 1: Conectarse a la nube
Parte 2: Conectar el Router0
Parte 3: Conectar los dispositivos restantes

Parte 4: Verificar las conexiones
Parte 5: Examinar la topología física

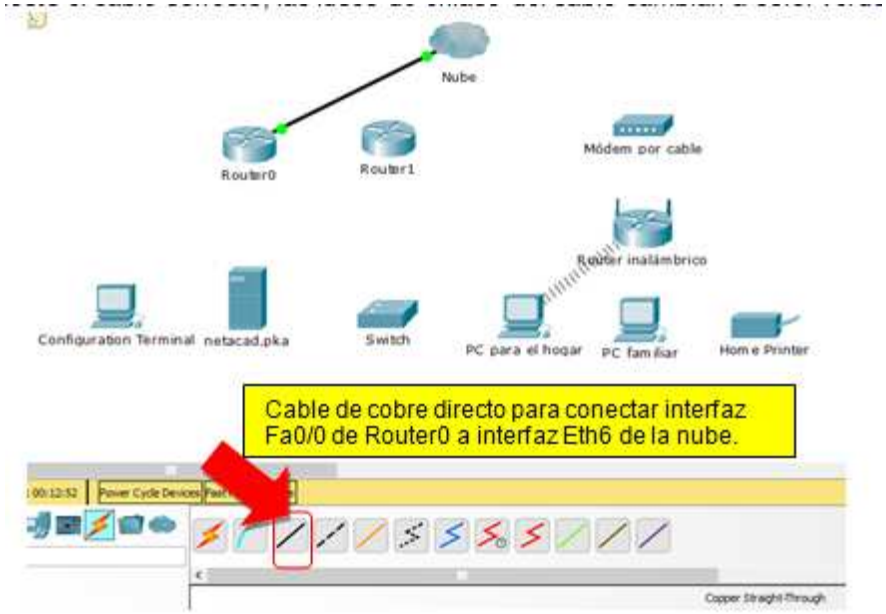
Información básica

Al trabajar en Packet Tracer (un entorno de laboratorio o un contexto empresarial), debe saber cómo seleccionar el cable adecuado y cómo conectar correctamente los dispositivos. En esta actividad se analizarán configuraciones de dispositivos en el Packet Tracer, se seleccionarán los cables adecuados según la configuración y se conectarán los dispositivos. Esta actividad también explorará la vista física de la red en el Packet Tracer.

Parte 1: Conectarse a la nube
Paso 1: Conectar la nube al Router0

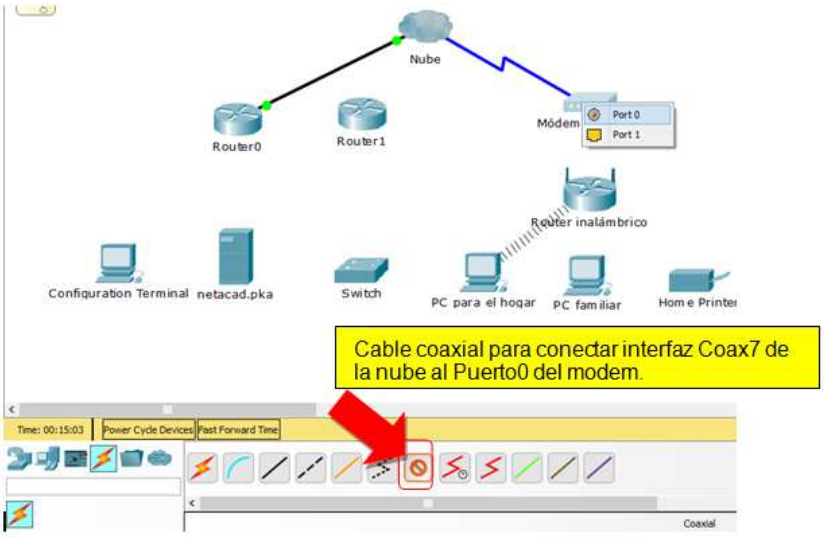
a. En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las **conexiones** disponibles.

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.



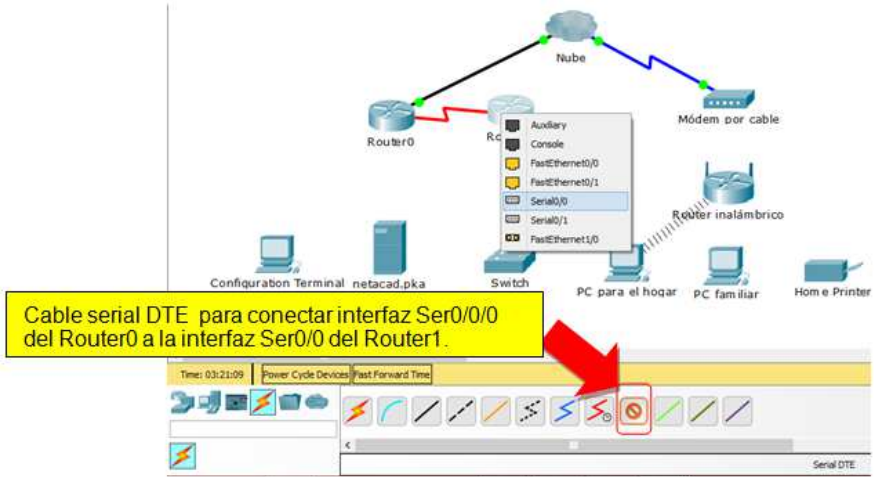
Paso 2: Conectar la nube al módem por cable

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.



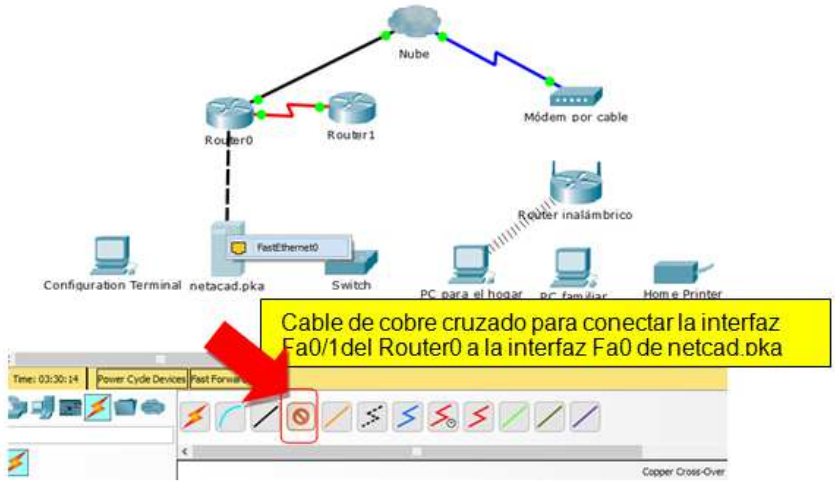
Parte 2: Conectar el Router0
Paso 1: Conectar el Router0 al Router1

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.



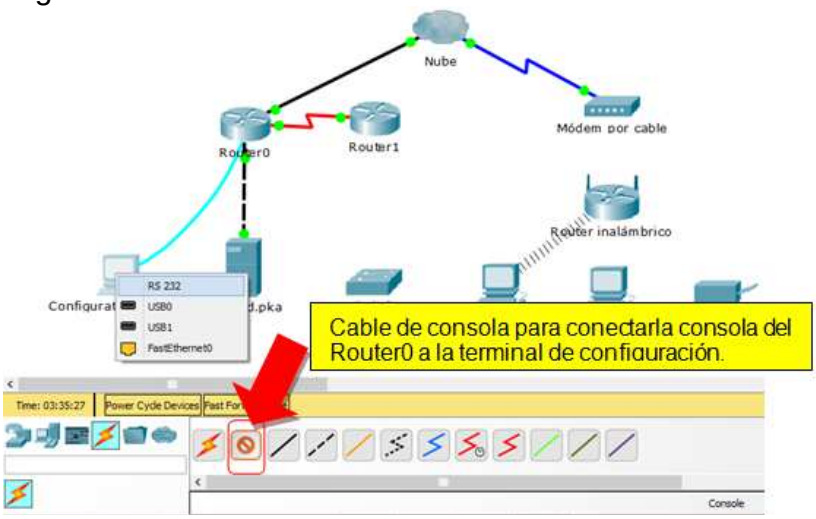
Paso 2: Conectar el Router0 a netacad.pka

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.



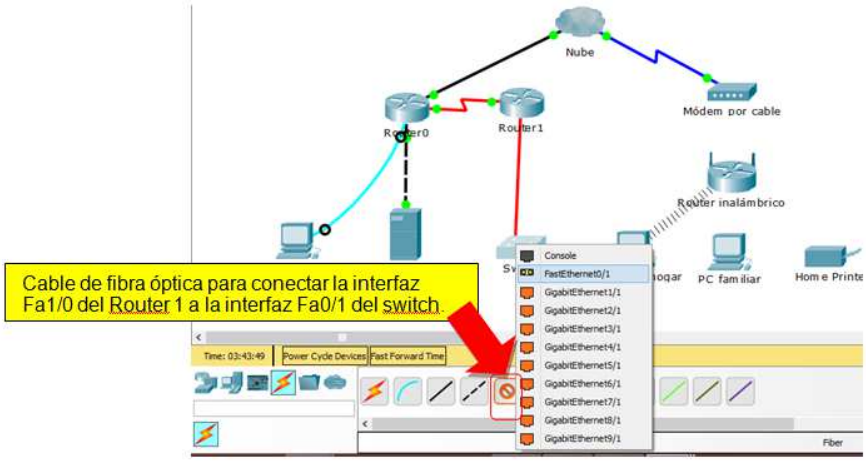
Paso 3: Conectar el Router0 a la terminal de configuración

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.



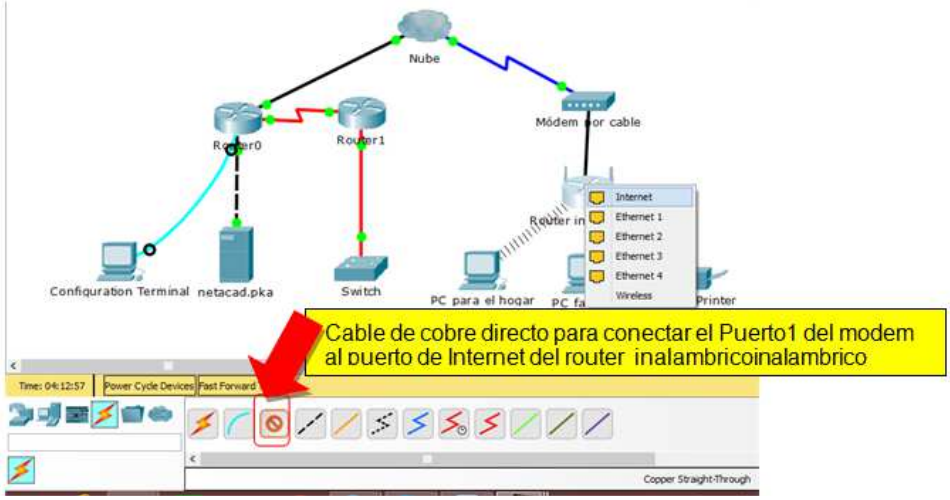
Parte 3: Conectar los dispositivos restantes
Paso 1: Conectar el Router1 al switch

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.

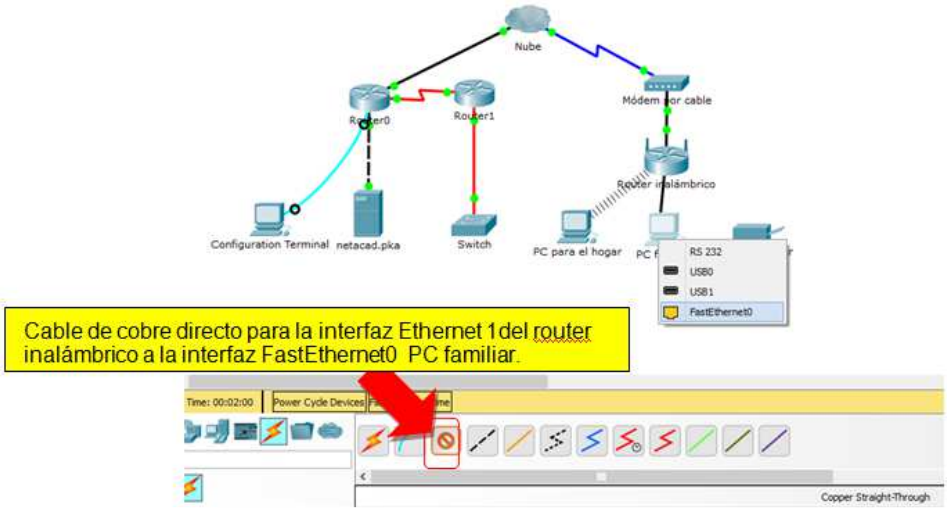


Paso 2: Conectar el módem por cable al router inalámbrico

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



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.



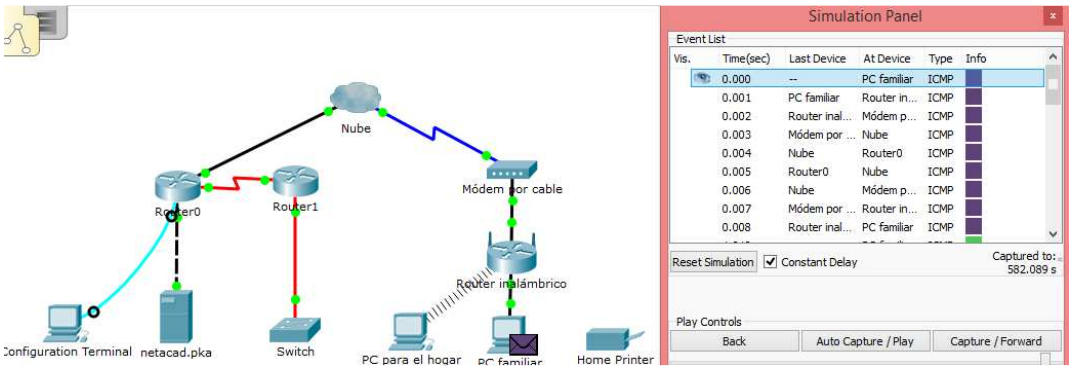
Parte 4: Verificar las conexiones

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**.

```
Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=8ms TTL=254
Reply from 10.0.0.1: bytes=32 time=8ms TTL=254
Reply from 10.0.0.1: bytes=32 time=8ms TTL=254
Reply from 10.0.0.1: bytes=32 time=8ms TTL=254

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Se establece que la conexión del Pc familiar con netacad.pka es exitosa con 4 paquetes enviados y 4 recibidos



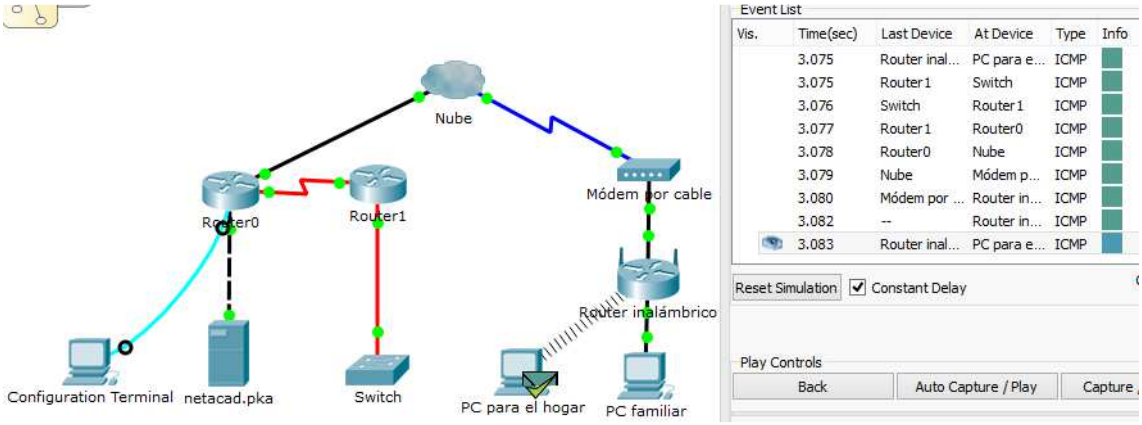
La ruta que debe seguir el paquete es router inalámbrico, modem por cable, nube y Router 0.

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.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=24ms TTL=252
Reply from 172.16.0.2: bytes=32 time=20ms TTL=252
Reply from 172.16.0.2: bytes=32 time=14ms TTL=252
Reply from 172.16.0.2: bytes=32 time=17ms TTL=252

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 24ms, Average = 18ms
```

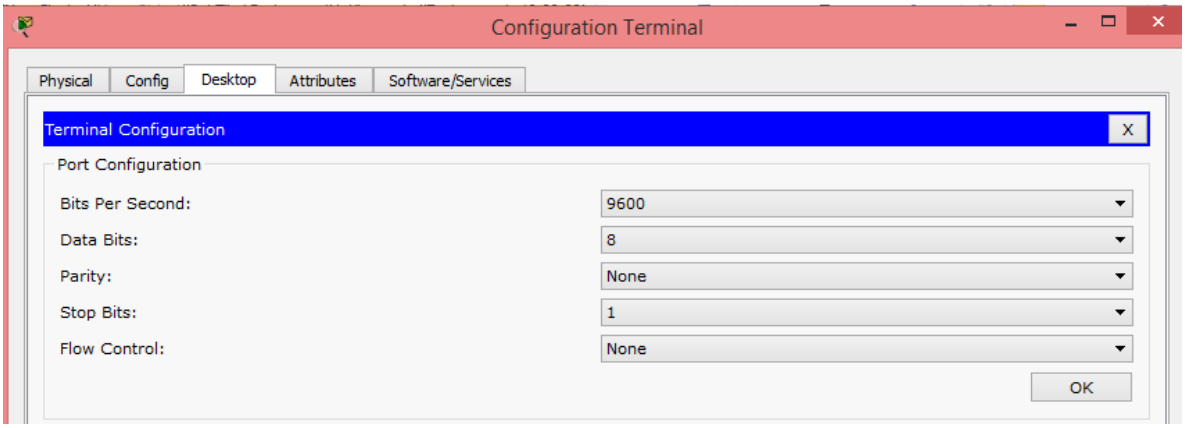
Se establece que la conexión del Pc para el hogar con el switch es exitosa con 4 paquetes enviados y 4 recibidos



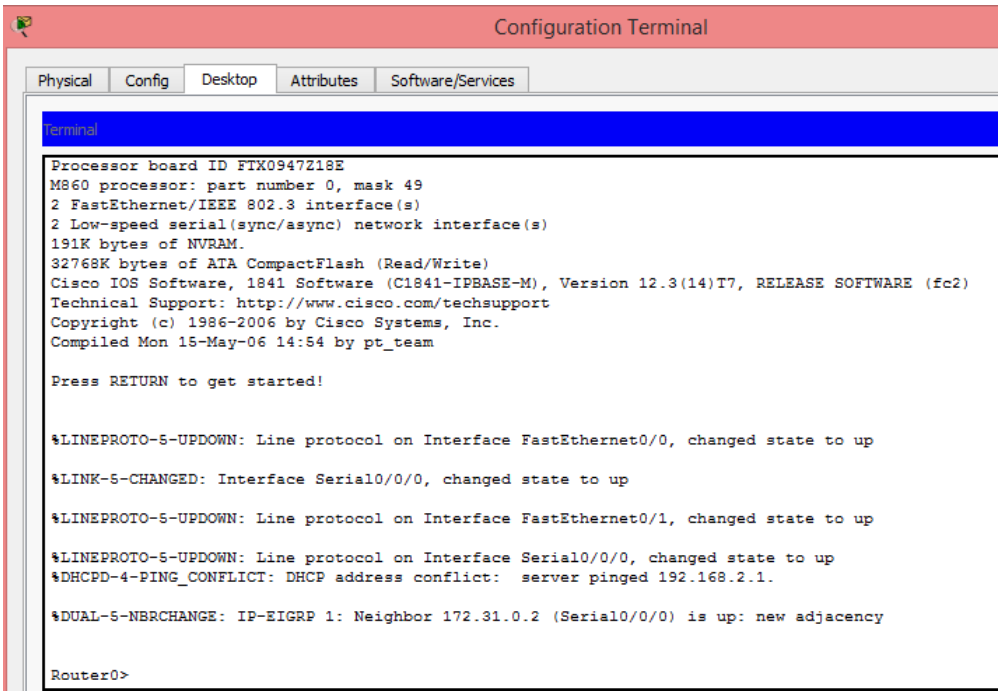
La ruta que debe seguir el paquete es: router inalámbrico, modem por cable, nube, Router 0, Router1 y switch.

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**.



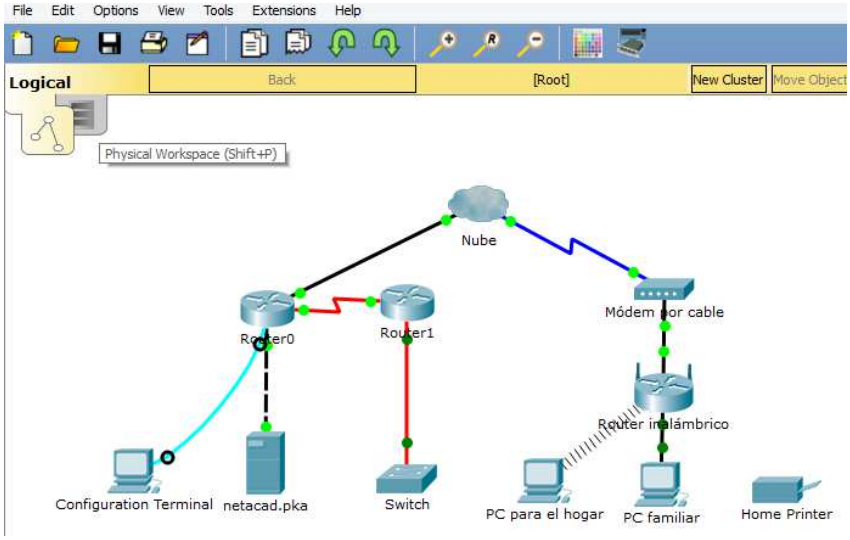
c. Escriba **show ip interface brief** para ver el estado de las interfaces.

```
Router0>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.2.1     YES manual up                    up
FastEthernet0/1        10.0.0.1        YES manual up                    up
Serial0/0/0            172.31.0.1      YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router0>
```

Parte 5: Examinar la topología física

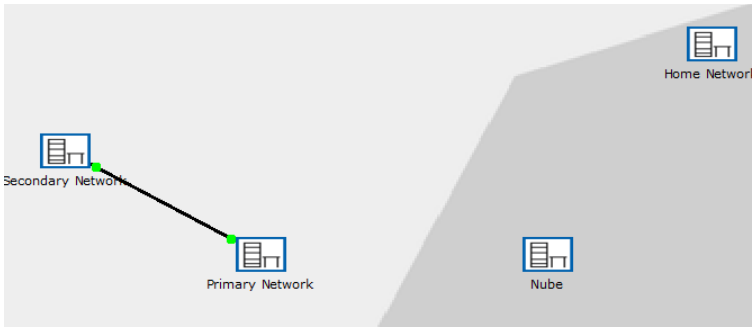
Paso 1: Examinar la nube

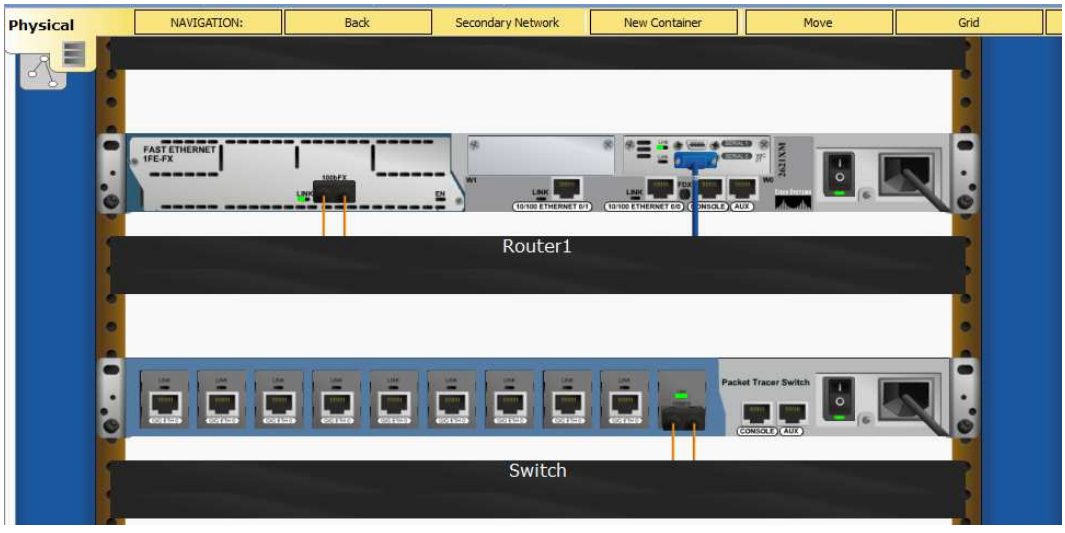
d. Haga clic en la ficha **Physical Workspace** (Área de trabajo física) o presione **Mayús** + **P** y **Mayús** + **L** para alternar entre las áreas de trabajo lógicas y físicas.



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

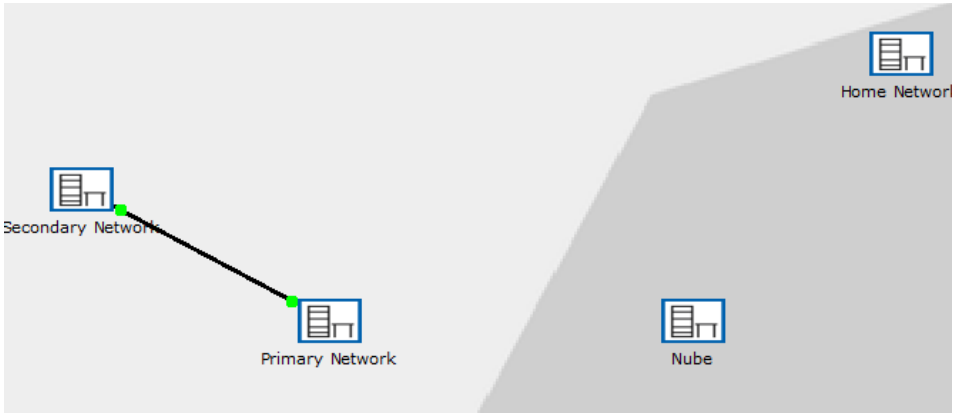




g. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

Paso 2: Examinar la red principal

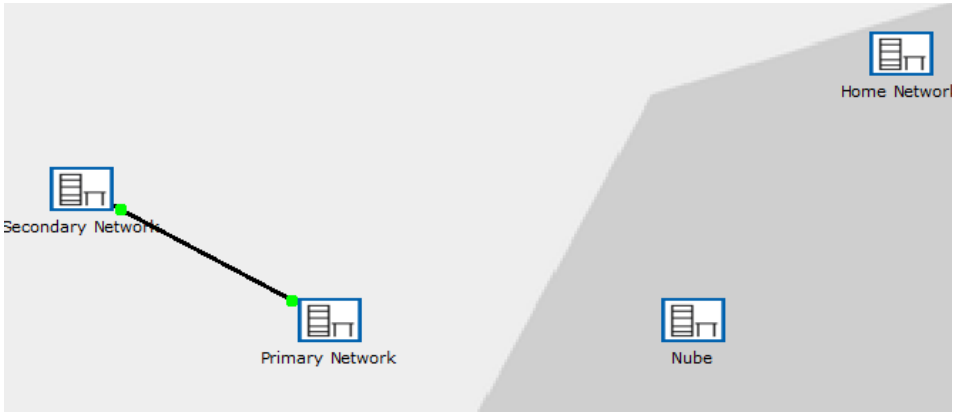
h. Haga clic en el ícono **Primary Network** (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul? Terminal de configuración

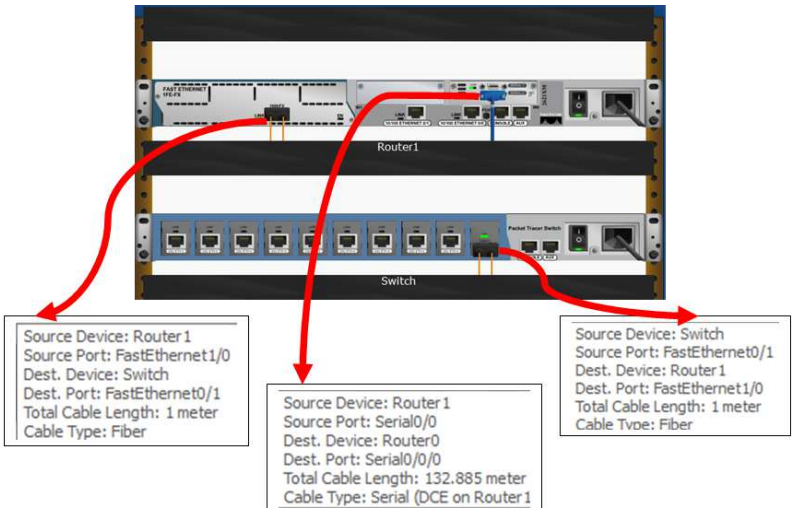


i. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

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.

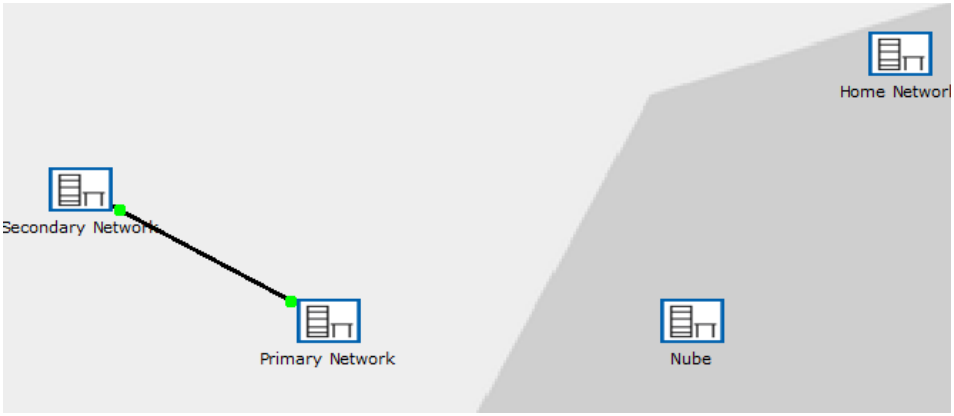




k. Haga clic en **Back** (Atrás) para volver a **Home City** (Ciudad de residencia).

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.

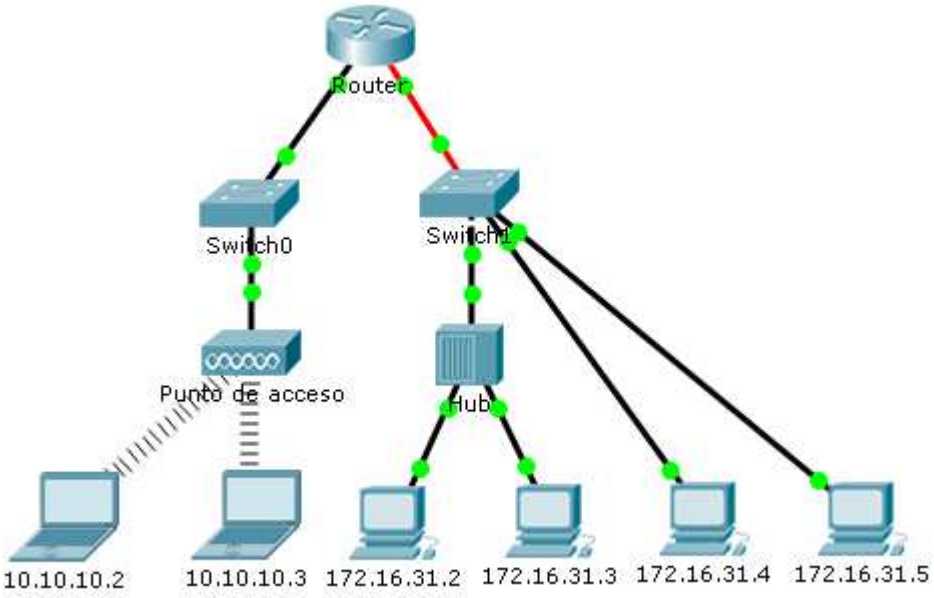


m. Haga clic en el ícono **Home Network** (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo? Por lo general, las redes domésticas no incluyen bastidores.

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

PRACTICA 5.1.4.4
Identificación de direcciones MAC y direcciones IP

Topología



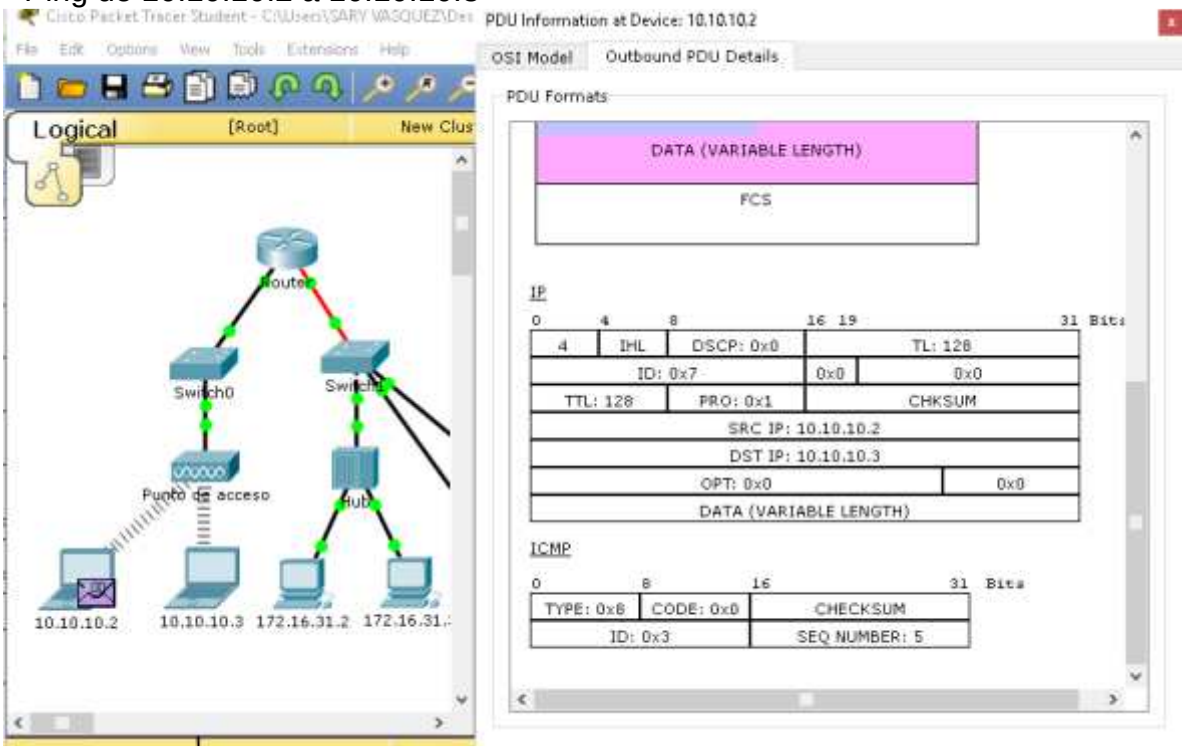
Objetivos
Parte 1: Recopilar información de la PDU
Parte 2: Preguntas de reflexión
Información básica Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.
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

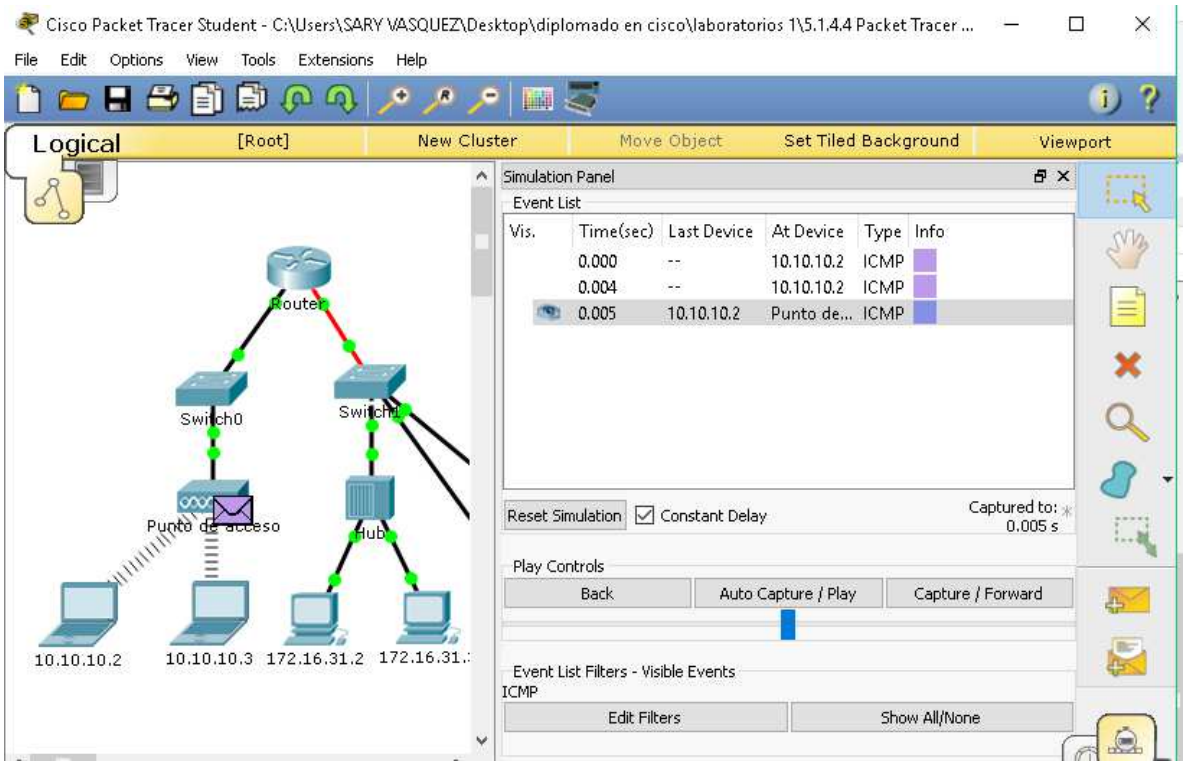
recopiló de la PDU en una hoja de cálculo con un formato como el de la tabla que se muestra a continuación:

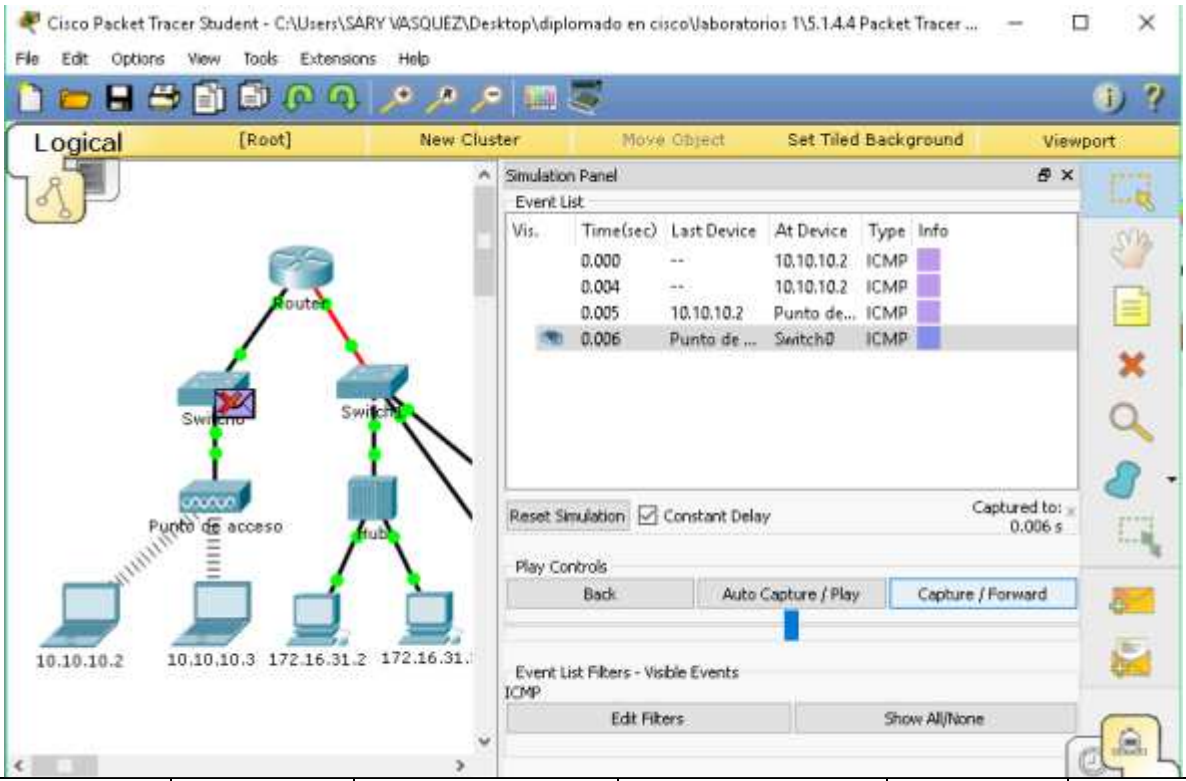
Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	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 ping Repita el proceso del paso 1 y recopile información para las pruebas siguientes:

• Ping de 10.10.10.2 a 10.10.10.3



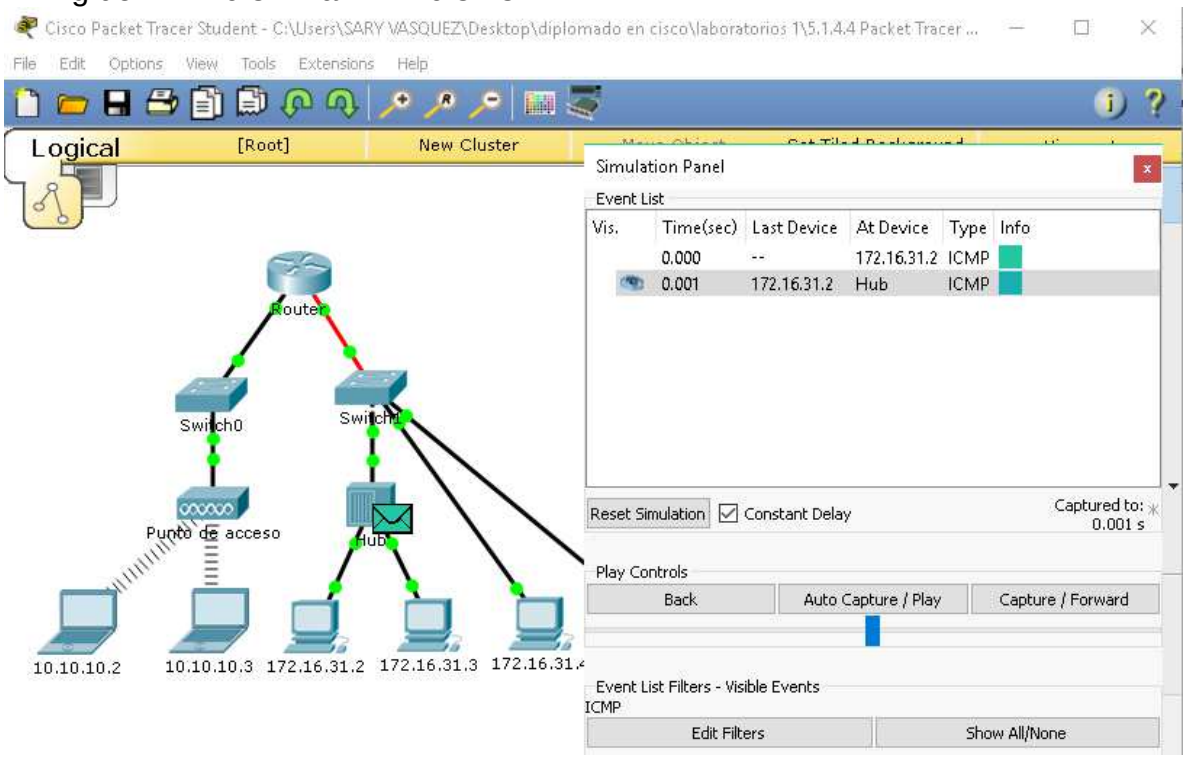


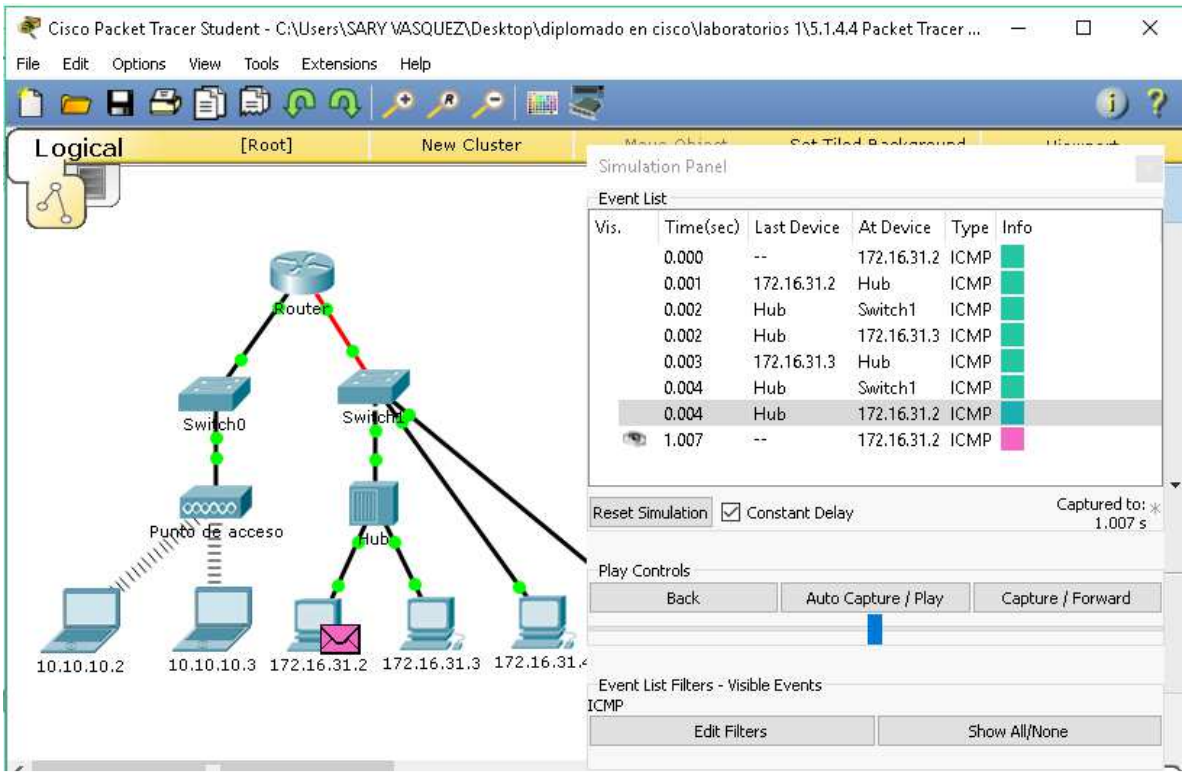


Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
	10.10.10.2	--	--	10.10.10.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	--	--	--	--

Ping de 10.10.10.2 a 10.10.10.3	Router	--	--	--	--
	Switch0	0060.4706.572B	0060.2F84.4AB6	10.10.10.2	10.10.10.3
	Punto De Acceso	0060.4706.572B	0060.2F84.4AB6	10.10.10.2	10.10.10.3
	10.10.10.3	--	--	10.10.10.3	10.10.10.2

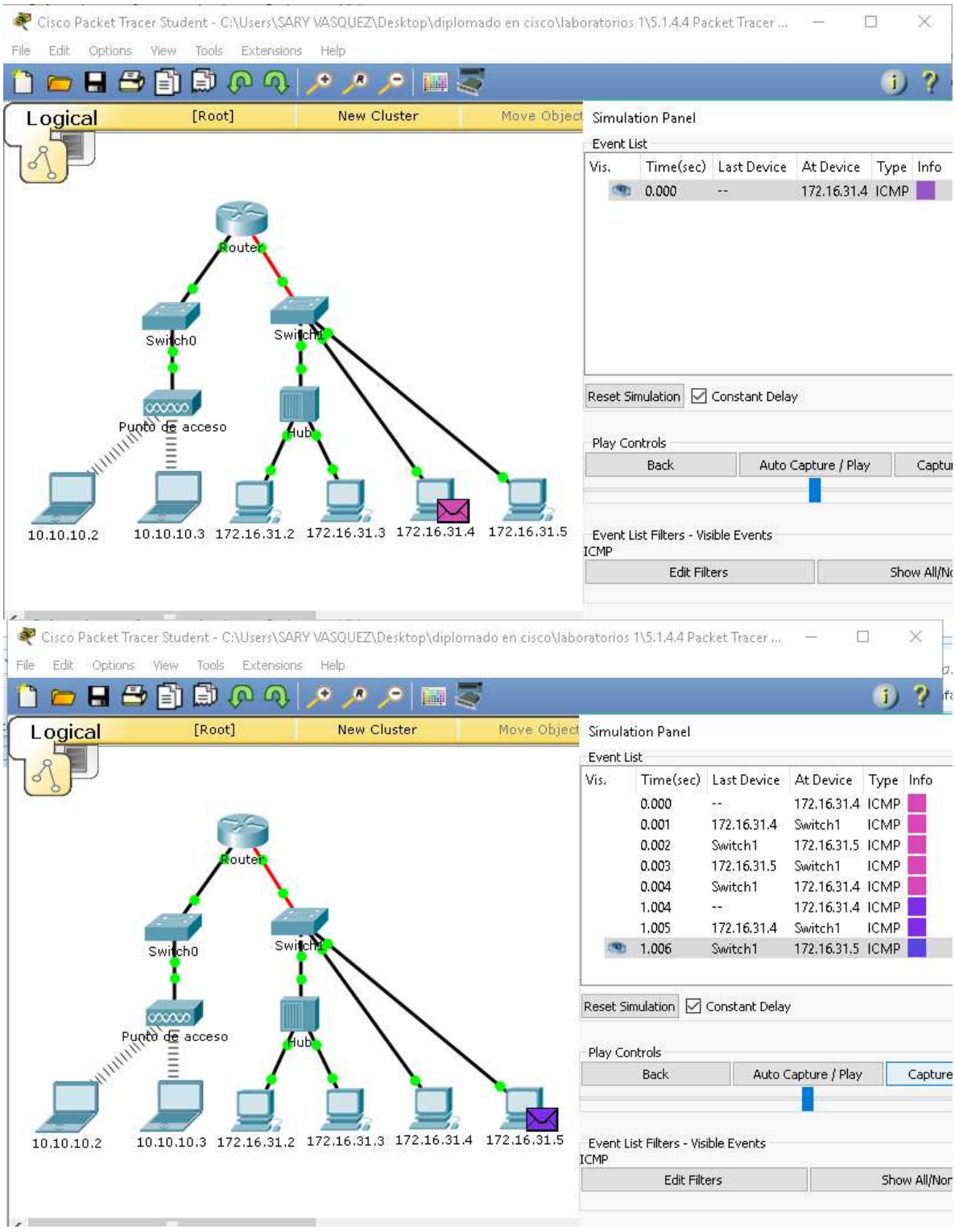
• Ping de 172.16.31.2 a 172.16.31.3





Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 172.16.31.3	172.16.31.2	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3
	Hub	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3
	Switch1	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3
	Router	--	--	--	--
	Switch0	--	--	--	--
	Punto De Acceso	--	--	--	--
	172.16.31.3	0060.7036.2849	000C.85CC.1DA7	172.16.31.3	172.16.31.2

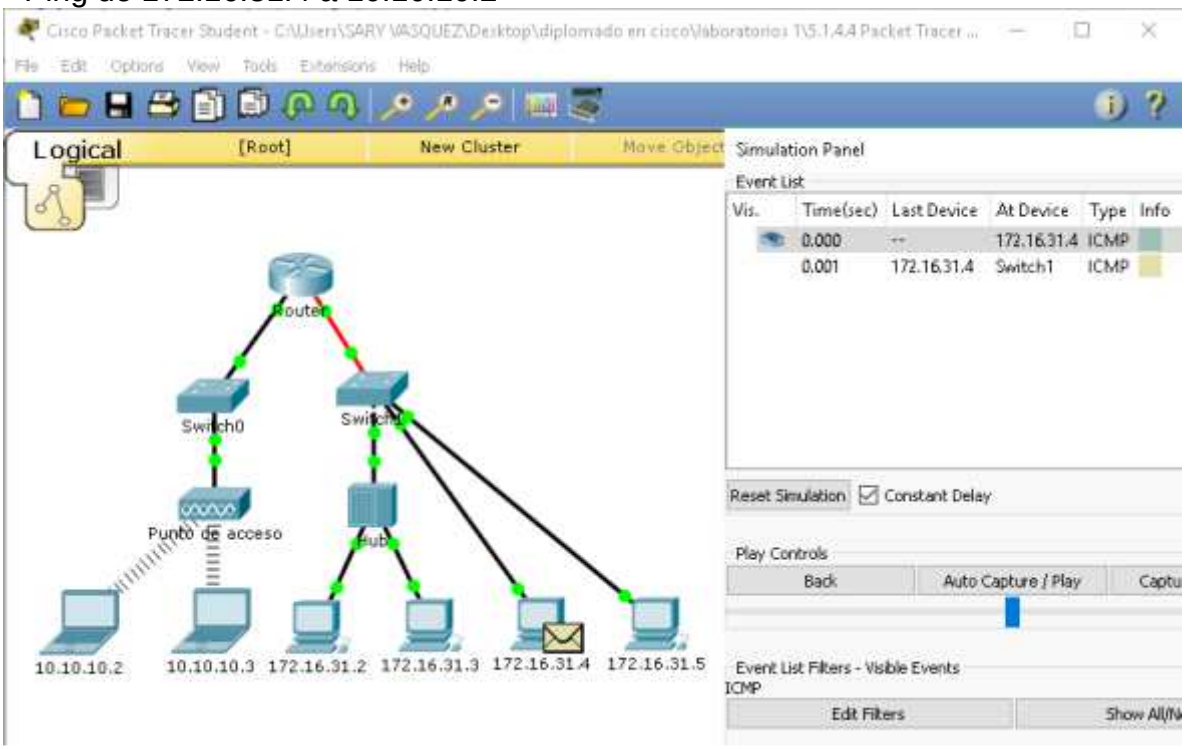
• Ping de 172.16.31.4 a 172.16.31.5

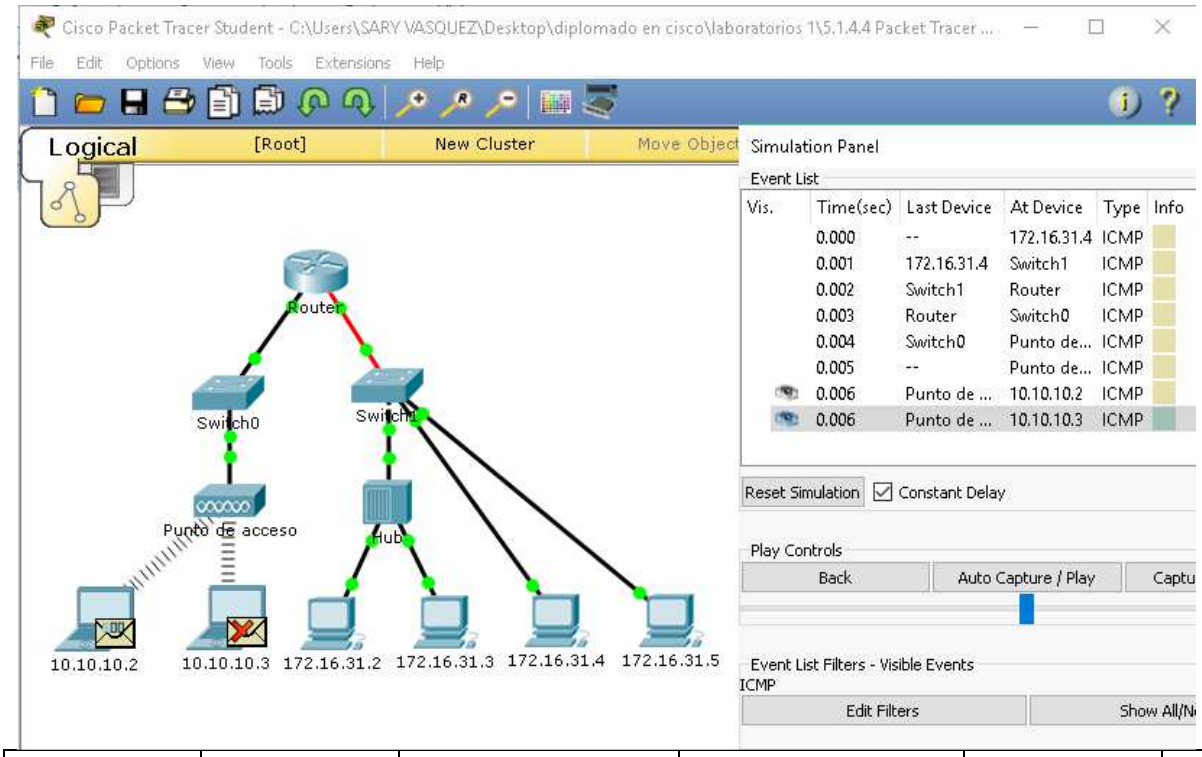


Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4

Ping de 172.16.31.4 a 172.16.31.5	172.16.31.4	--	--	172.16.31.4	172.16.31.5
	Hub	--	--	--	--
	Switch1	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5
	Router	--	--	--	--
	Switch0	--	--	--	--
	Punto De Acceso	--	--	--	--
	172.16.31.5	000C.CF0B.BC80	00D0.D311.C788	172.16.31.5	172.16.31.4

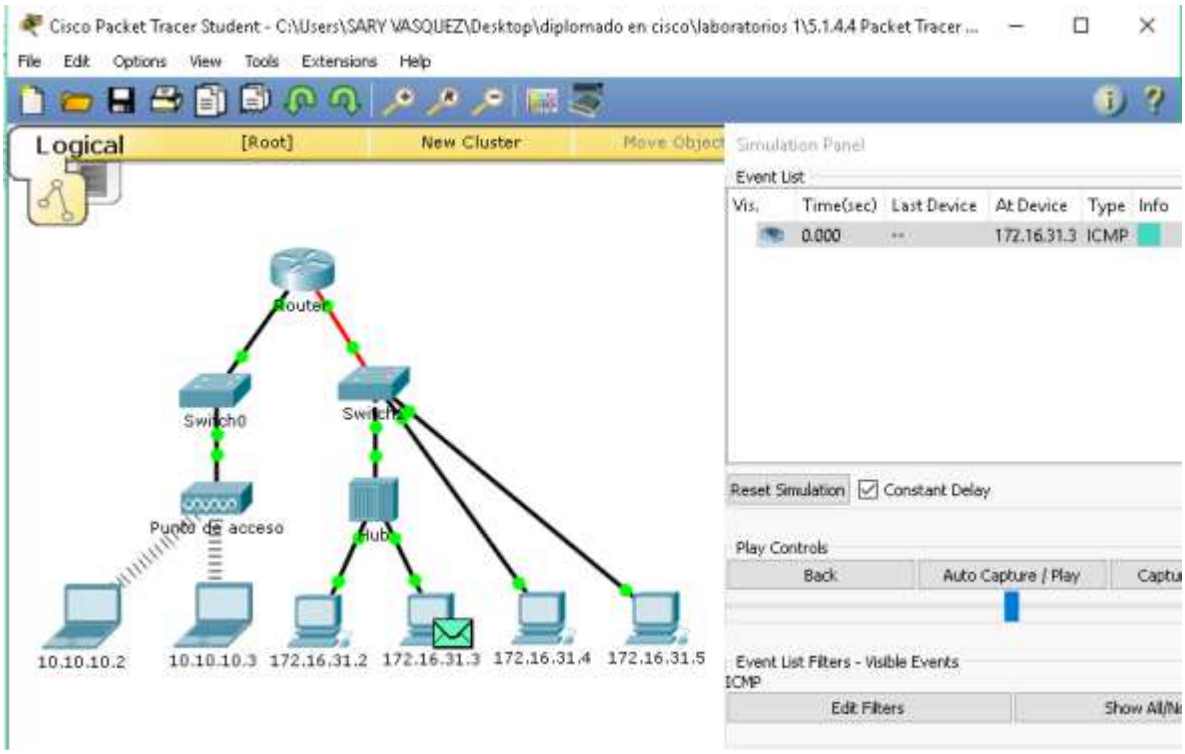
• Ping de 172.16.31.4 a 10.10.10.2

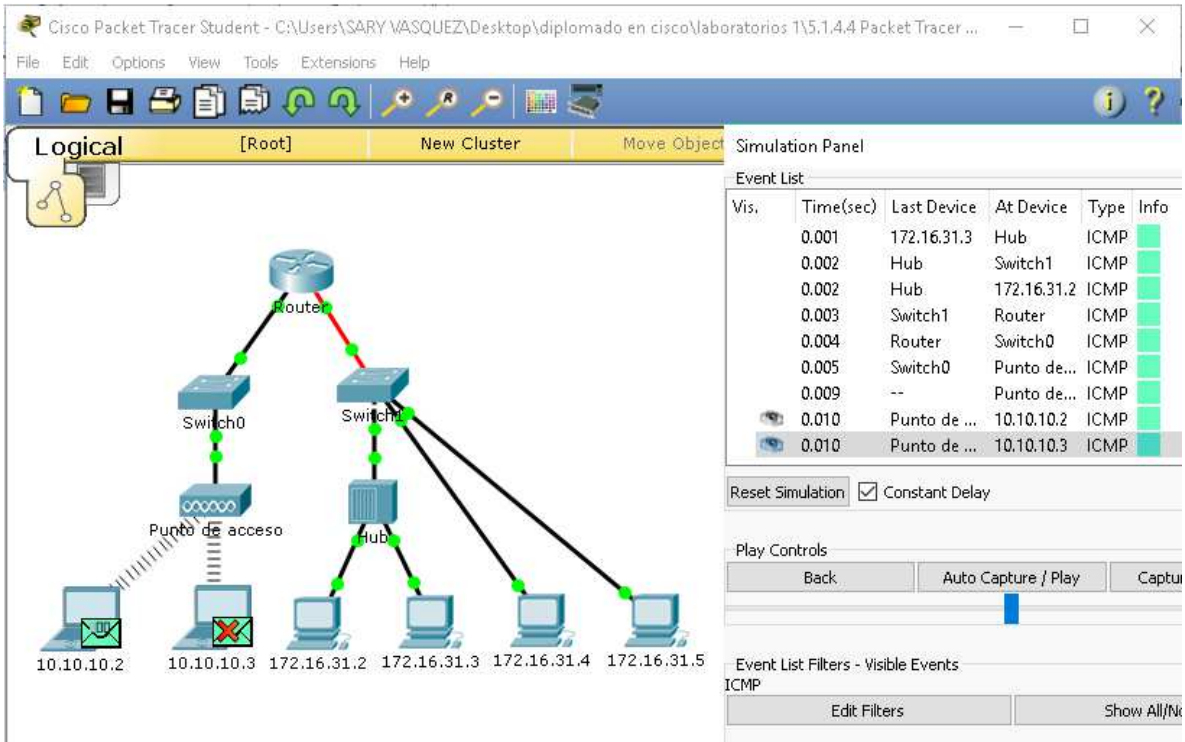




Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.4 a 10.10.10.2	172.16.31.4	--	--	172.16.31.4	10.10.10.2
	Hub	--	--	--	--
	Switch1	00D0.BA8E.741A	000C.CF0B.BC80	172.16.31.4	10.10.10.2
	Router	--	--	172.16.31.4	10.10.10.2
	Switch0	0060.2F84.4AB6	00D0.588C.2401	172.16.31.4	10.10.10.2
	Punto De Acceso	--	--	172.16.31.4	10.10.10.2
	10.10.10.2	--	--	10.10.10.2	172.16.31.4

- Ping de 172.16.31.3 a 10.10.10.2





Prueba	En Dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.3 a 10.10.10.2	172.16.31.3	00D0.BA8E.741A	0060.7036.2849	171.16.31.3	10.10.10.2
	Hub	00D0.BA8E.741A	0060.7036.2849	171.16.31.3	10.10.10.2
	Switch1	--	--	--	--
	Router	0060.2F84.4AB6	00D0.588C.2401	171.16.31.3	10.10.10.2

	Switch0	0060.2F84.4AB6	00D0.588C.2401	171.16.31.3	10.10.10.2
	Punto De Acceso	--	--	171.16.31.3	10.10.10.2
	10.10.10.2	--	--	10.10.10.2	171.16.31.3

Parte 2: Preguntas de reflexión

Responda las siguientes preguntas relacionadas con la información reunida:

1. ¿Se utilizaron diferentes tipos de cables para conectar los dispositivos? De cobre y de fibra.
2. ¿Los cables cambiaron el manejo de la PDU de alguna forma? No
3. ¿El hub perdió la información que se le entregó? No
4. ¿Qué hace el hub con las direcciones MAC y las direcciones IP? Nada.
5. ¿El punto de acceso inalámbrico hizo algo con la información que se le entregó? La volvió a empaquetar según el estándar inalámbrico 802.11.
6. ¿Se perdió alguna dirección MAC o IP durante la transferencia inalámbrica? No
7. ¿Cuál fue la capa OSI más alta que utilizaron el hub y el punto de acceso? Capa 1
8. ¿El hub o el punto de acceso reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? Sí
9. Al examinar la ficha PDU Details (Detalles de PDU), ¿que dirección MAC aparecía primero, la de origen o la de destino? Aparece la de destino
10. ¿Por qué las direcciones MAC aparecen en este orden? Si el destino aparece primero en la lista, un switch puede comenzar a reenviar una trama a una dirección MAC conocida más rápidamente.
11. ¿Había un patrón para el direccionamiento MAC en la simulación? No
12. ¿Los switches reprodujeron en algún momento una PDU rechazada con una “X” de color rojo? No
13. Cada vez que se enviaba la PDU entre las redes 10 y 172, había un punto donde las direcciones MAC cambiaban repentinamente. ¿Dónde ocurrió eso? En el router.
14. ¿Qué dispositivo utiliza las direcciones MAC que comienzan con 00D0? El router.
15. ¿A qué dispositivos pertenecen las otras direcciones MAC? Al emisor y al receptor.
16. ¿Las direcciones IPv4 de envío y recepción cambian en alguna de las PDU? No
17. Si sigue la respuesta a un ping, a veces denominado pong, ¿las direcciones IPv4 de envío y recepción cambian? Sí
18. ¿Cuál es el patrón para el direccionamiento IPv4 en esta simulación? Cada puerto de router requiere un conjunto de direcciones que no se superpongan.
19. ¿Por qué es necesario asignar diferentes redes IP a los diferentes puertos de un router? La función de un router es interconectar diferentes redes IP.
20. Si esta simulación fuera configurada con IPv6 en vez de IPv4, ¿cuál sería la diferencia? Las direcciones IPv4 se reemplazarían con direcciones IPv6, pero todo lo demás sería igual. Tabla

PRACTICA 5.2.1.7

Packet Tracer: Revisión de la tabla ARP

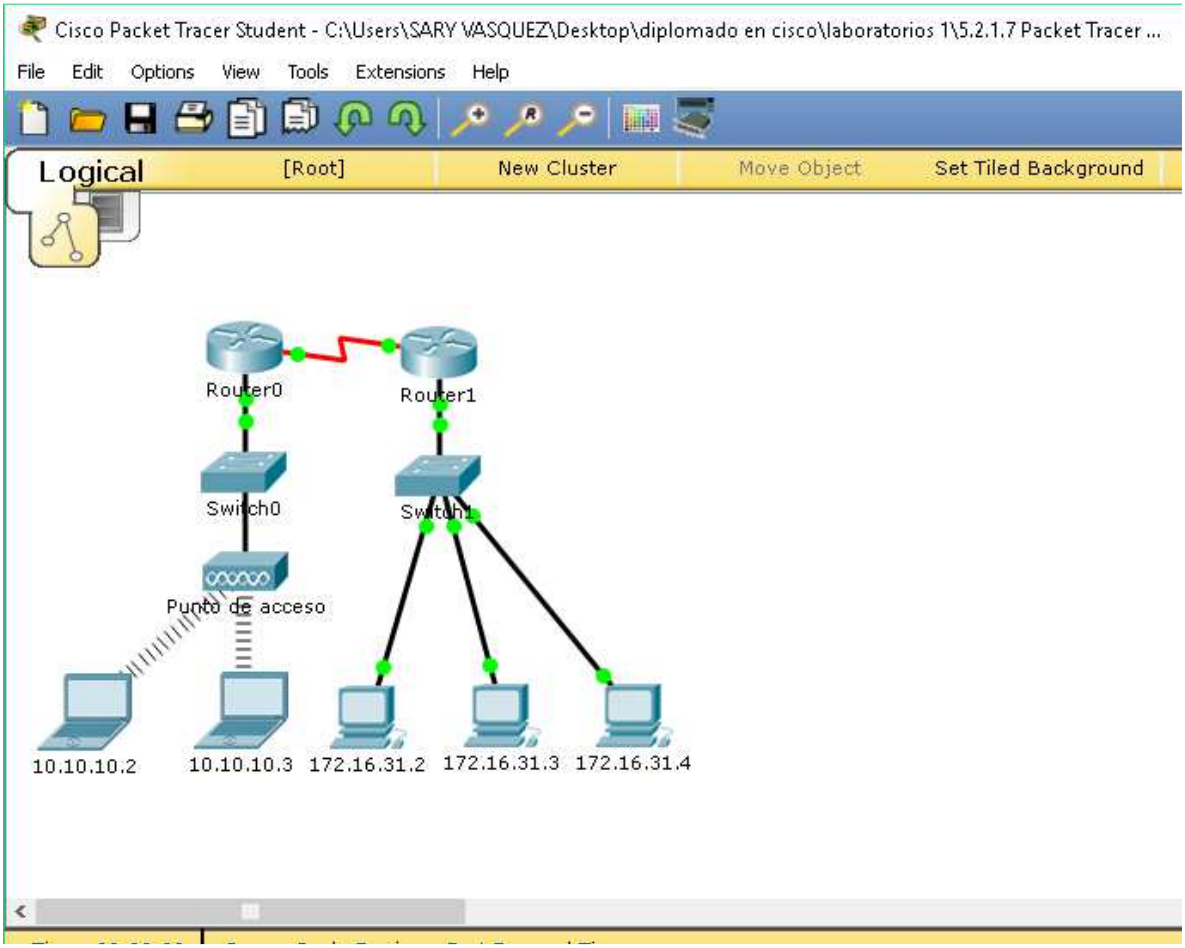


Tabla de direccionamiento

Dispositivo	**Interfaz**	**Dirección MAC**	**Interfaz del switch**
router 0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	No Aplicable	No aplicable
router 1	Gig0/0	00E0.F7B1.8901	Gig0/1
	Se0/0/0	No Aplicable	No aplicable
10.10.10.2	Inalámbrico	0060.2F84.4AB6	Fa0/2
10.10.10.3	Inalámbrico	0060.4706.572B	Fa0/2
172.16.31.2	Fa0	000C.85CC.1DA7	Fa0/1
172.16.31.3	Fa0	0060.7036.2849	Fa0/2
172.16.31.4	Gig0	0002.1640.8D75	Fa0/3

Objetivos

Parte 1: Examinar una solicitud de ARP

Parte 2: Examinar una tabla de direcciones MAC del switch

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

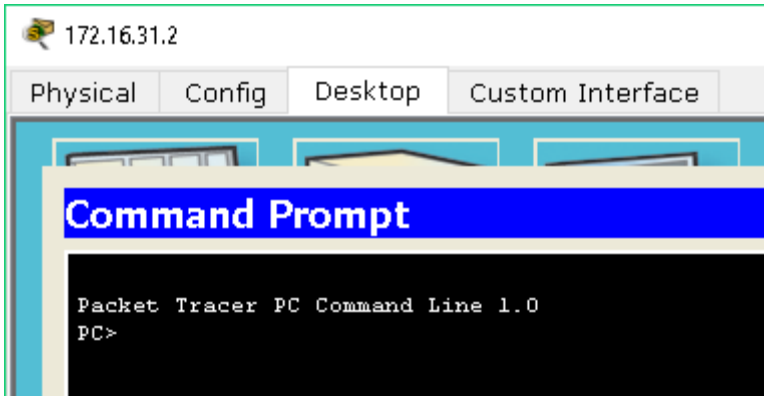
Información básica

Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

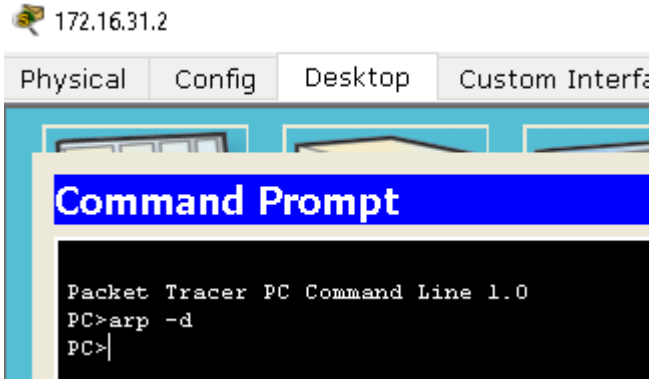
Parte 1: Examinar una solicitud de ARP

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

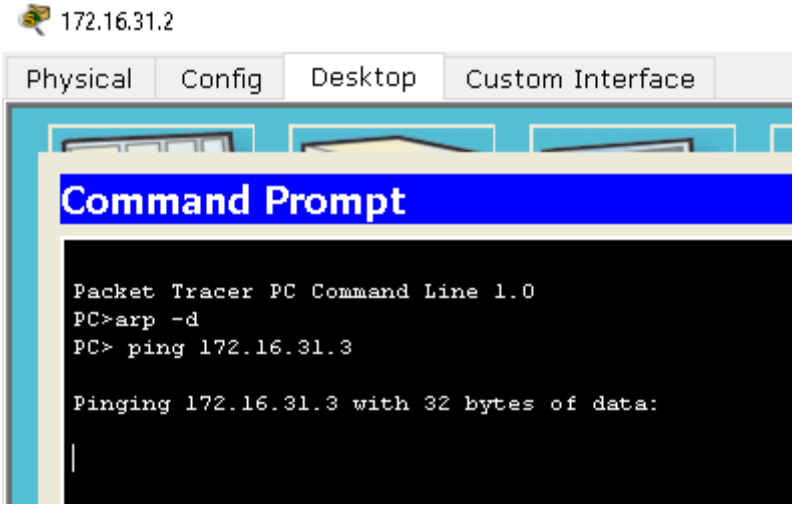
a. Haga clic en **172.16.31.2** y abra el símbolo del sistema.

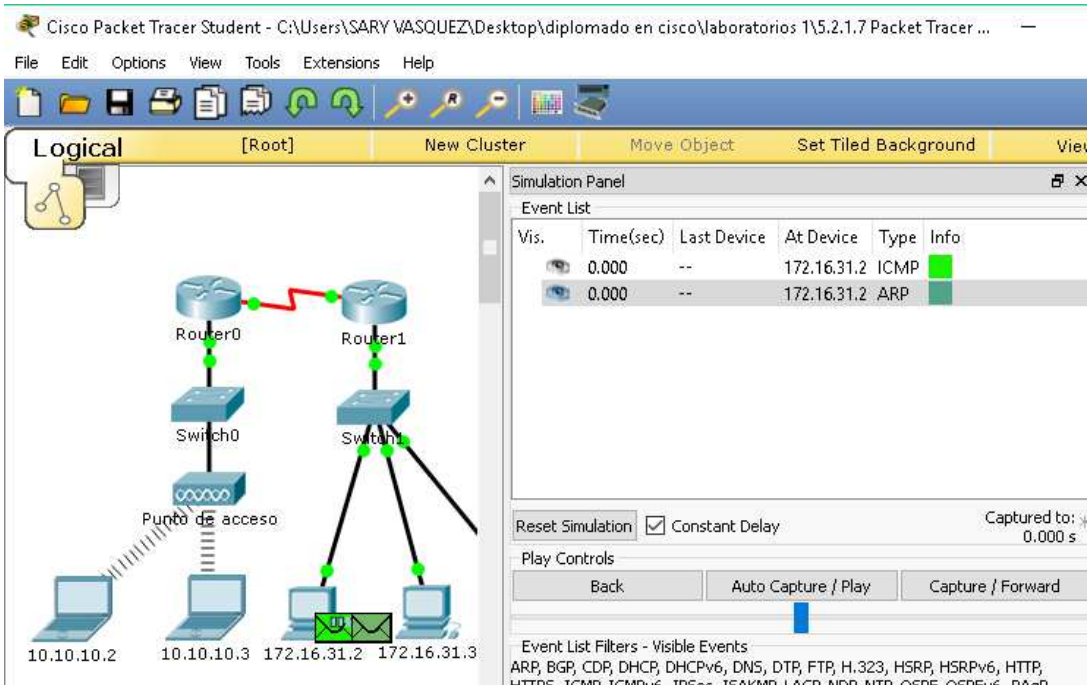


b. Introduzca el comando **arp -d** para borrar la tabla ARP.

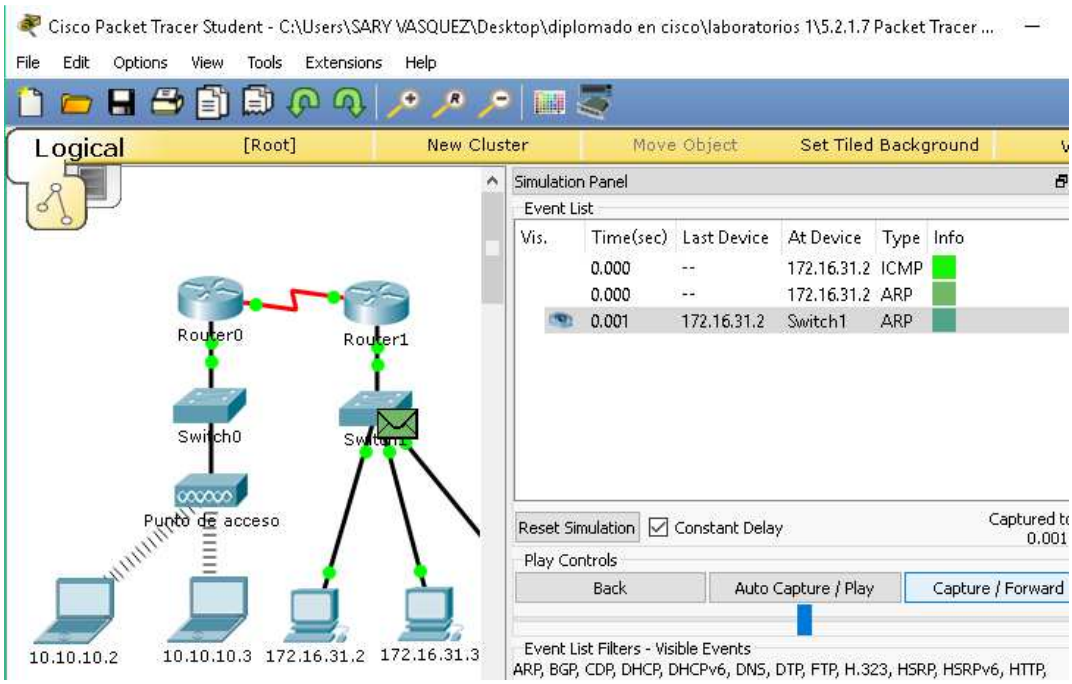


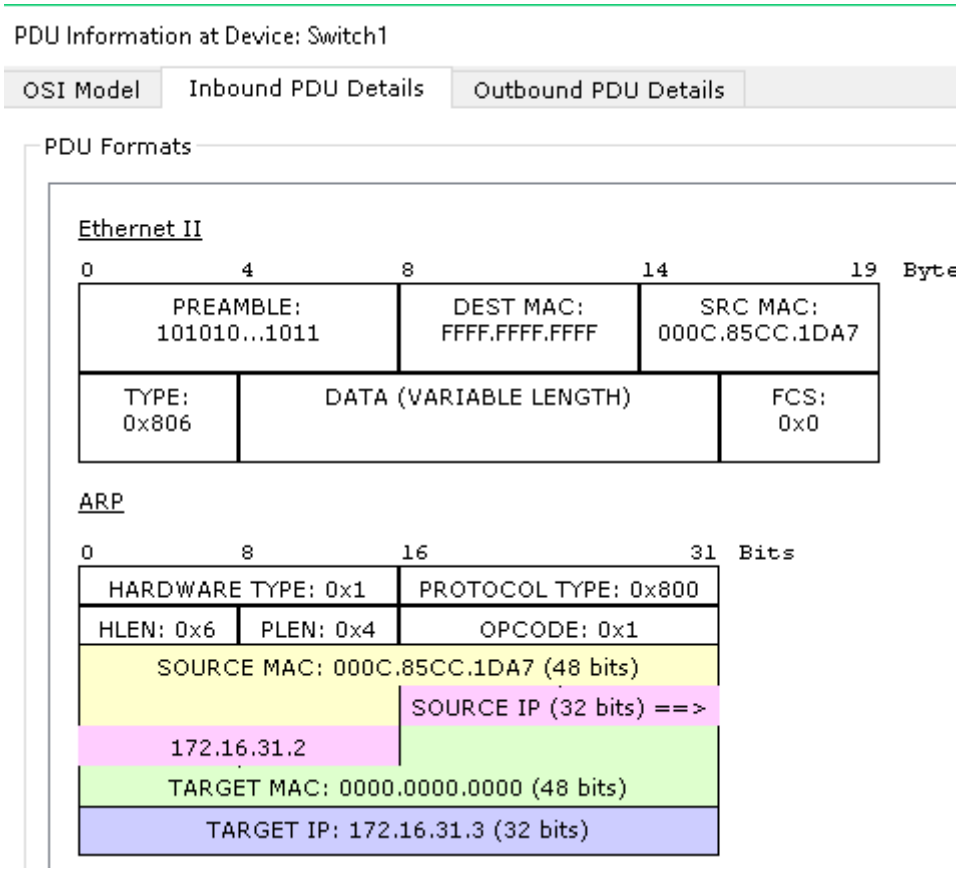
c. Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3.** Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.



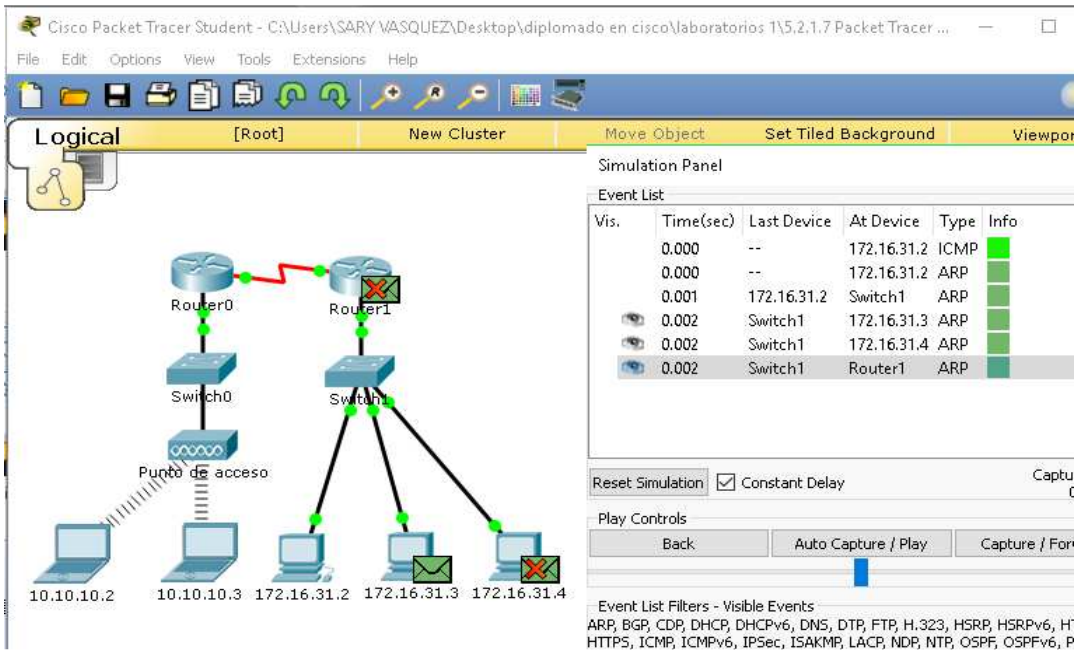


d. Haga clic en Capture/Forward (Capturar/avanzar) una vez. La PDU ARP mueve el Switch1, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior? No





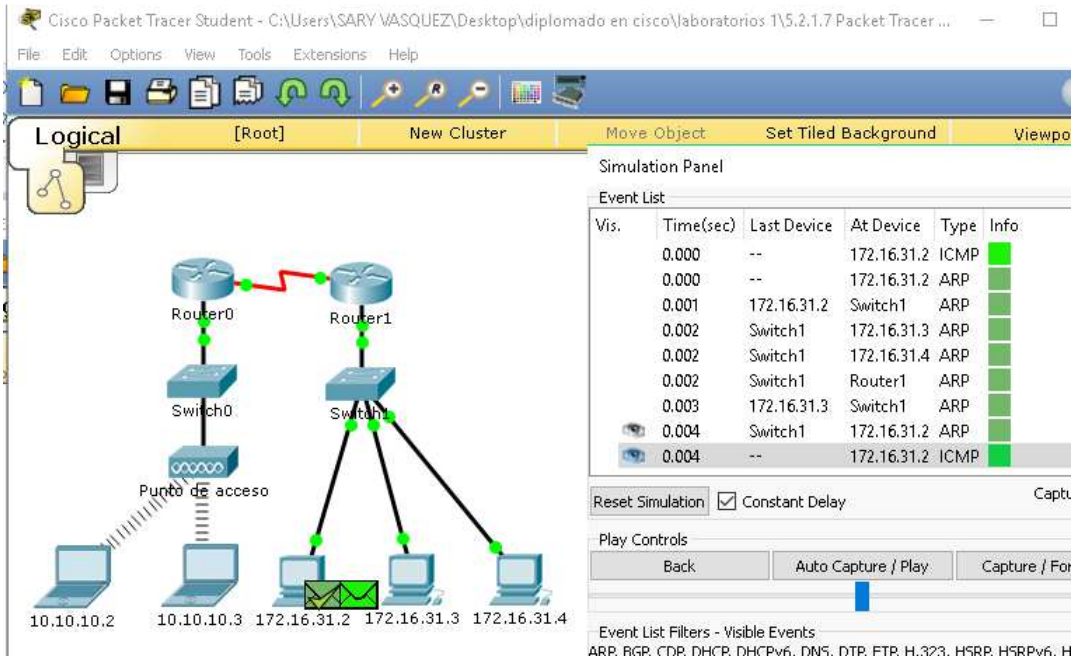
e. Haga clic en Capture/Forward (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el Switch1? 3



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 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? 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? 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? 172.16.31.3

```
PC> arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0060.7036.2849        dynamic

PC>
```

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

```
PC>ping 172.16.31.4

Pinging 172.16.31.4 with 32 bytes of data:

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

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? Se enviaron cuatro y se recibieron cuatro.

```
Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 34ms, Average = 21ms
```

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? Sí

```
Switch>enable
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00e0.f7b1.8901    DYNAMIC     Gig0/1
Switch#
```

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? Sí

```
Switch0>enable
Switch0#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6458.2501    DYNAMIC     Gig0/1
Switch0#
```

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

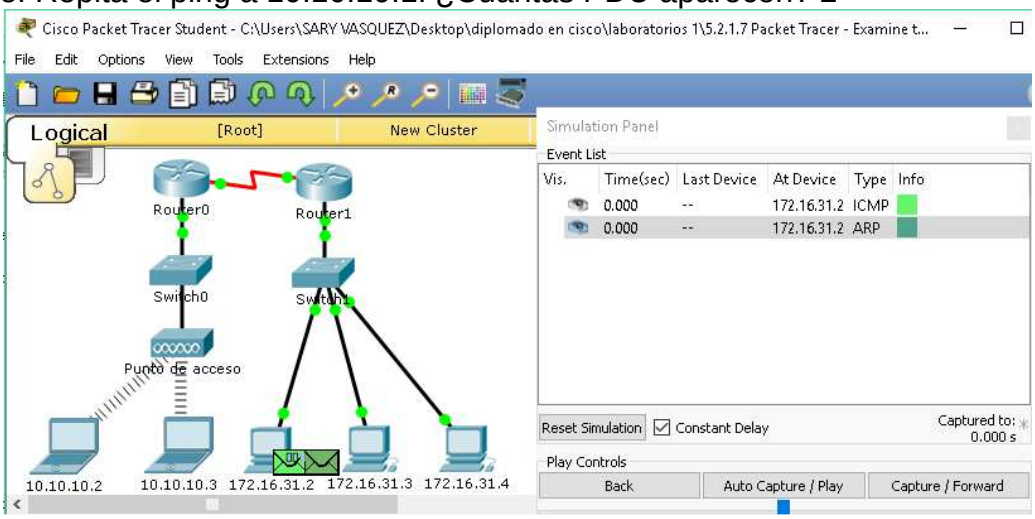
```
PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=44ms 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 = 44ms, Average = 11ms
```

c. Escriba arp -a. ¿Cuál es la dirección IP de la nueva entrada de la tabla ARP? 172.16.31.1

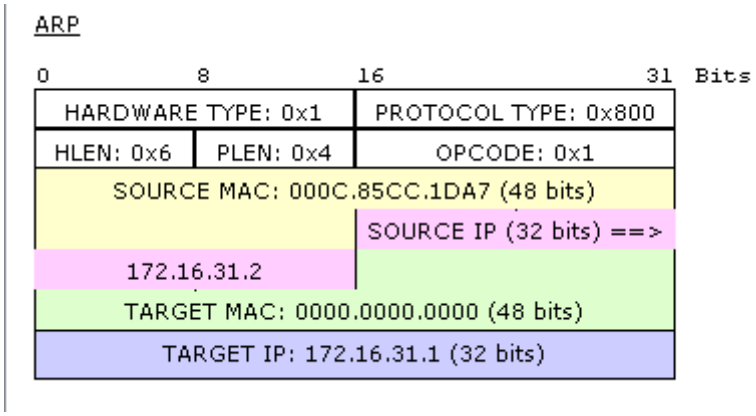
```
PC> arp -a
  Internet Address      Physical Address      Type
  172.16.31.1           00e0.f7b1.8901        dynamic
  172.16.31.3           0060.7036.2849        dynamic
  172.16.31.4           0002.1640.8d75        dynamic
```

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? 2



e. 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? 172.16.31.1



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

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

```
Router>enable
Router#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

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

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.31.1             -   00E0.F7B1.8901  ARPA   GigabitEthernet0/0
Internet  172.16.31.2            22   000C.85CC.1DA7  ARPA   GigabitEthernet0/0
```

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

PRACTICA 5.3.3.5
Packet Tracer: Configuración de switches de capa 3

Topología

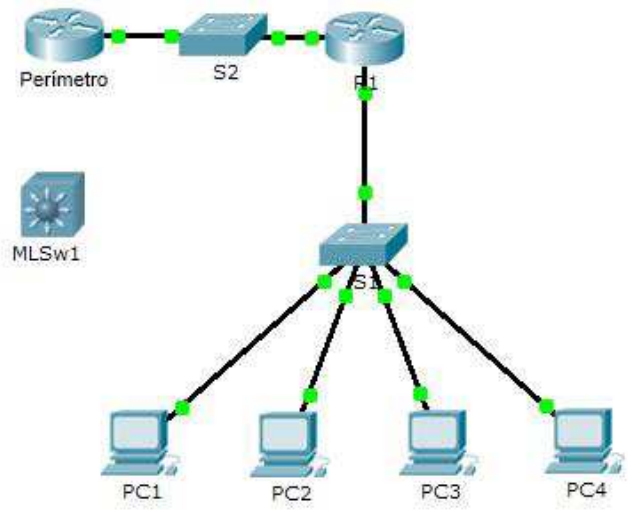


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0	172.16.31.1	255.255.255.0
	G0/1	192.168.0.2	255.255.255.0
MLSw1	G0/1	192.168.0.2	255.255.255.0
	VLAN 1	172.16.31.1	255.255.255.0

Objetivos

Parte 1: Documentar la configuración actual de la red

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

Situación

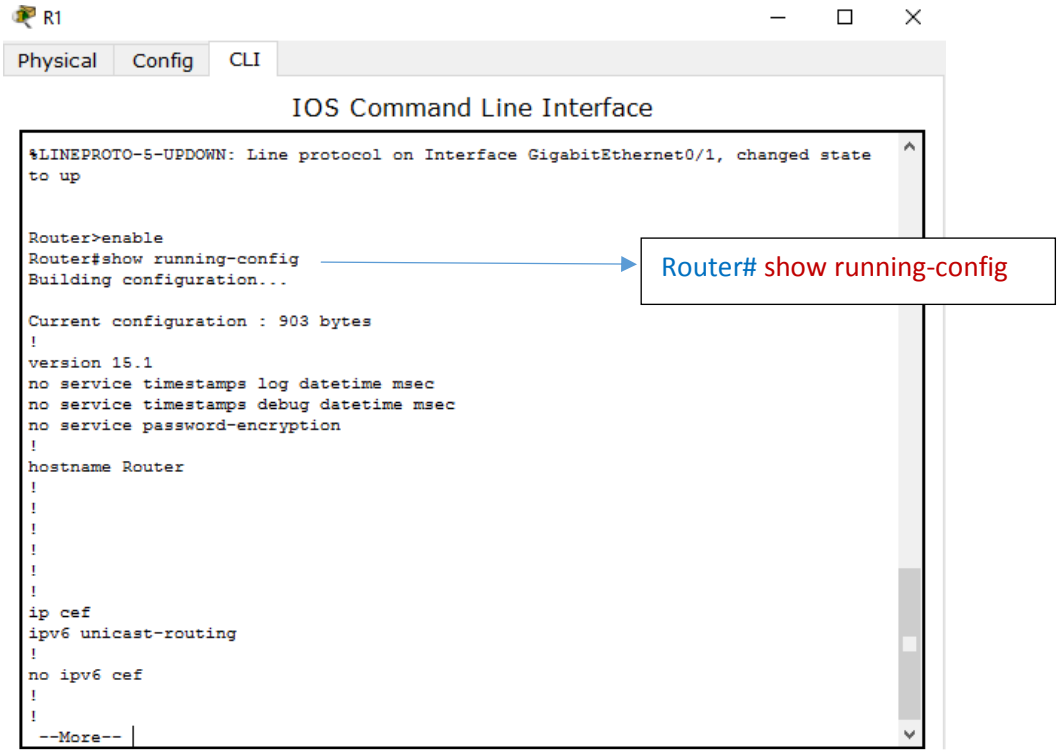
El administrador de red reemplaza el router y el switch actuales por un nuevo switch de capa 3. Como técnico de red, su trabajo consiste en configurar el switch y ponerlo en funcionamiento. Trabajará después del horario laboral para minimizar los inconvenientes para la empresa.
Nota: esta actividad comienza con una puntuación de 8/100, debido a que ya se calificaron las conexiones de los dispositivos para las PC. En la parte 2, eliminará y restaurará estas conexiones. La puntuación se incluye para verificar que haya restaurado correctamente las conexiones.

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

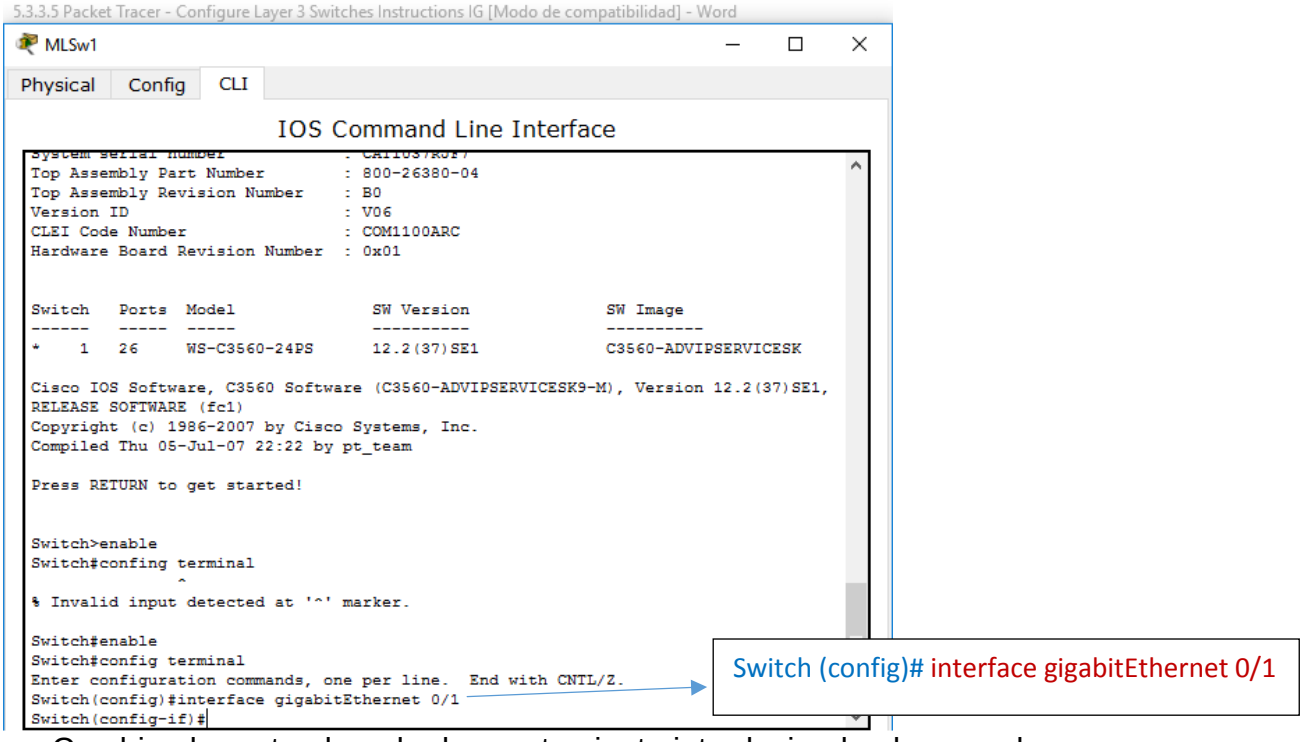


c. Registre la información en la **tabla de direccionamiento**.

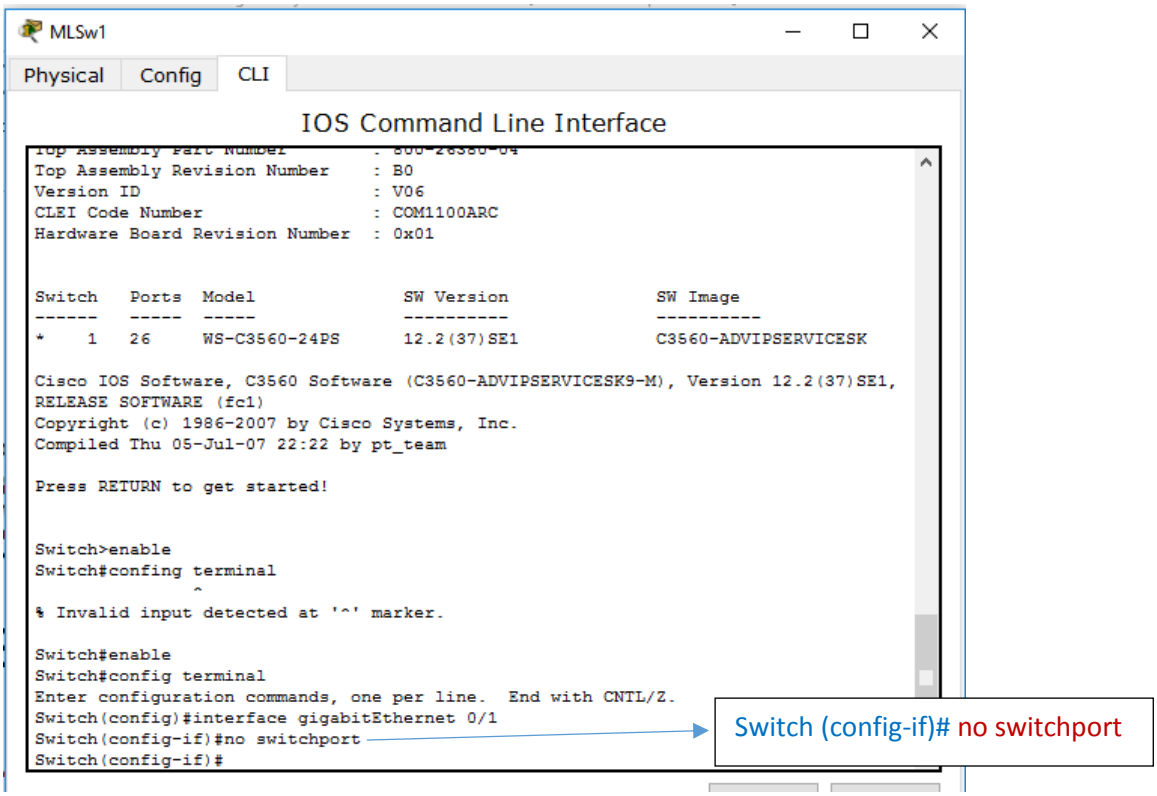
Parte 2: Configurar, implementar y probar el nuevo switch multicapa

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

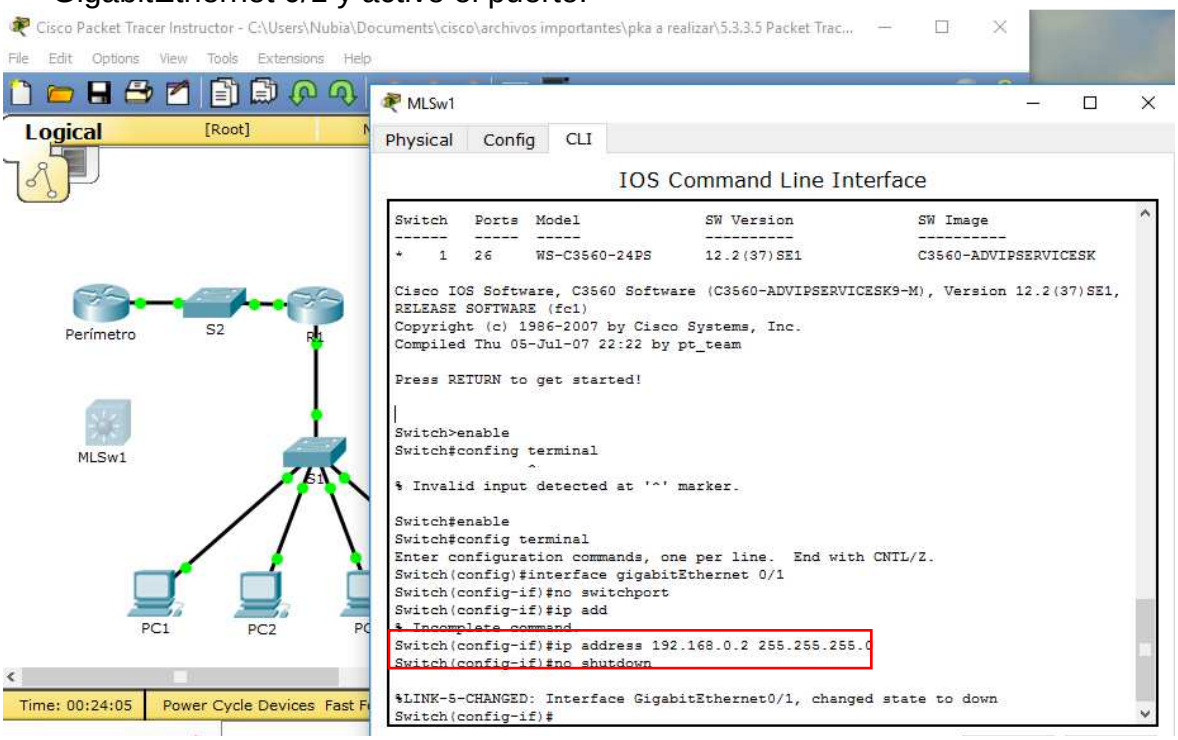
a. Haga clic en **MLSw1** y, a continuación, en la ficha **CLI**.
b. Ingrese al modo de configuración de interfaz para GigabitEthernet 0/1.



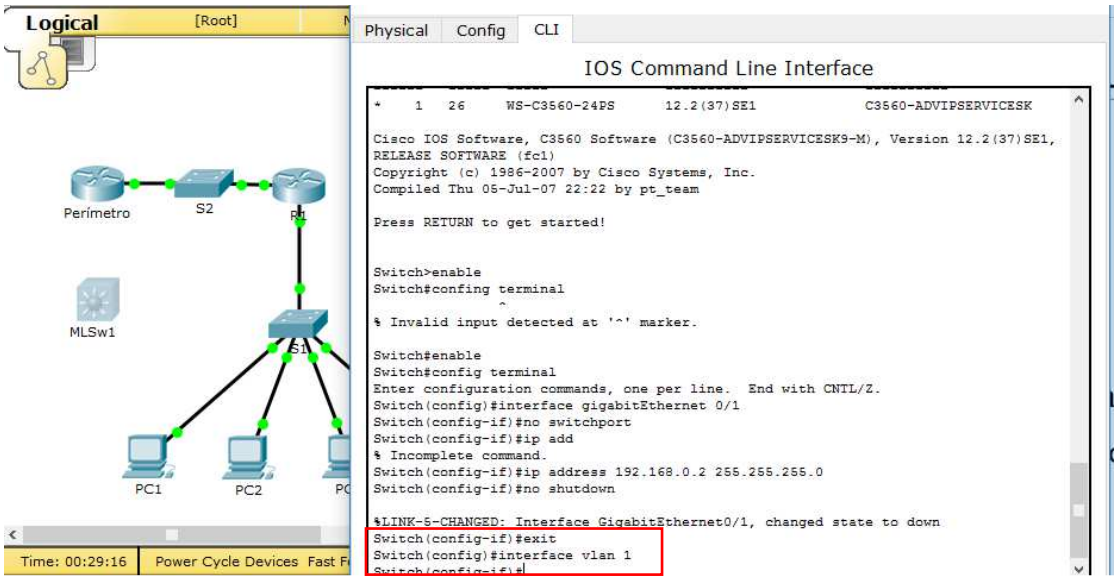
c. Cambie el puerto al modo de enrutamiento introduciendo el comando **no switchport**.



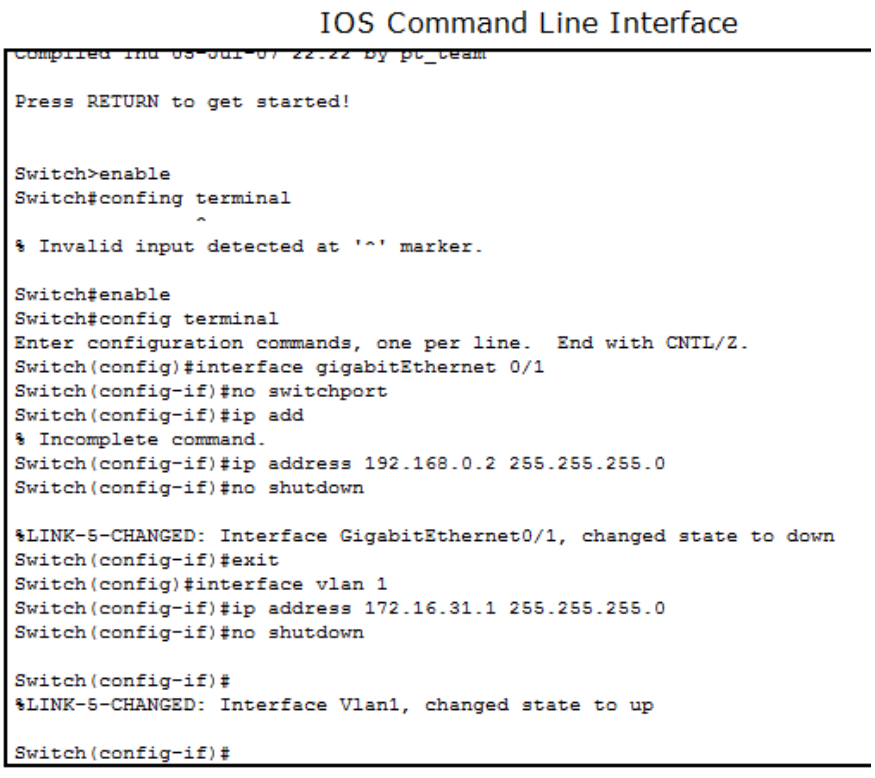
d. Configure la dirección IP para que sea la misma que la dirección de R1 GigabitEthernet 0/1 y active el puerto.



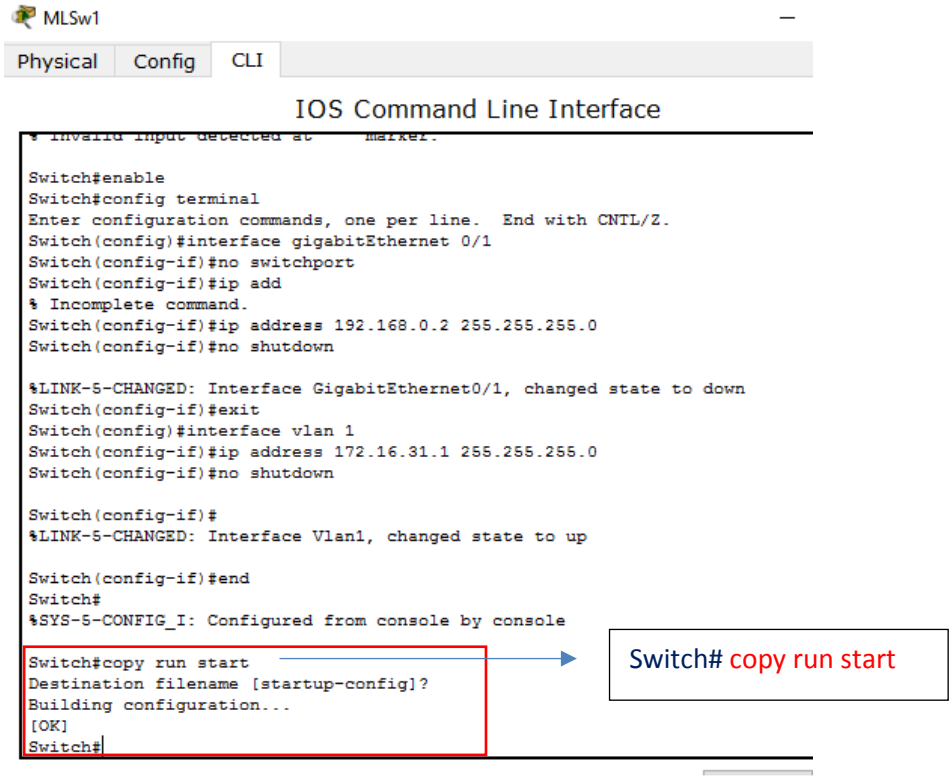
e. Ingrese al modo de configuración de interfaz para **interface VLAN1**.



f. Configure la dirección IP para que sea la misma que la dirección de **R1 GigabitEthernet 0/0** y active el puerto.



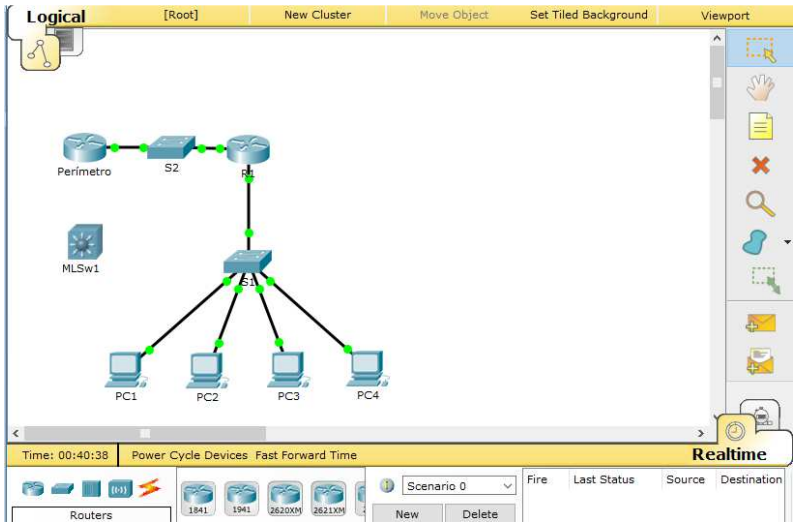
g. Guarde la configuración



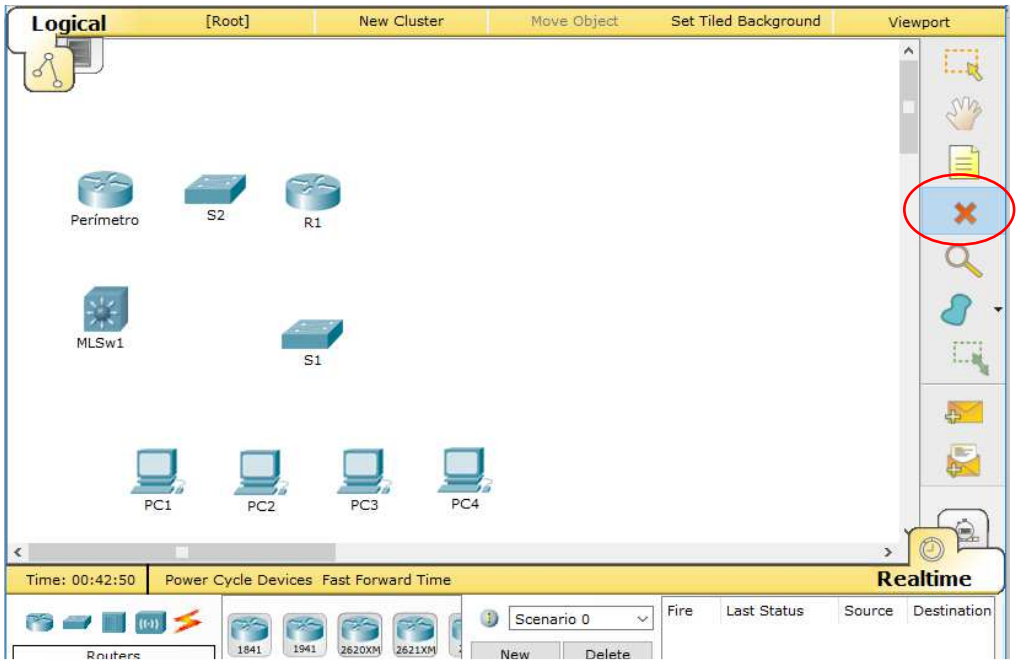
Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

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.

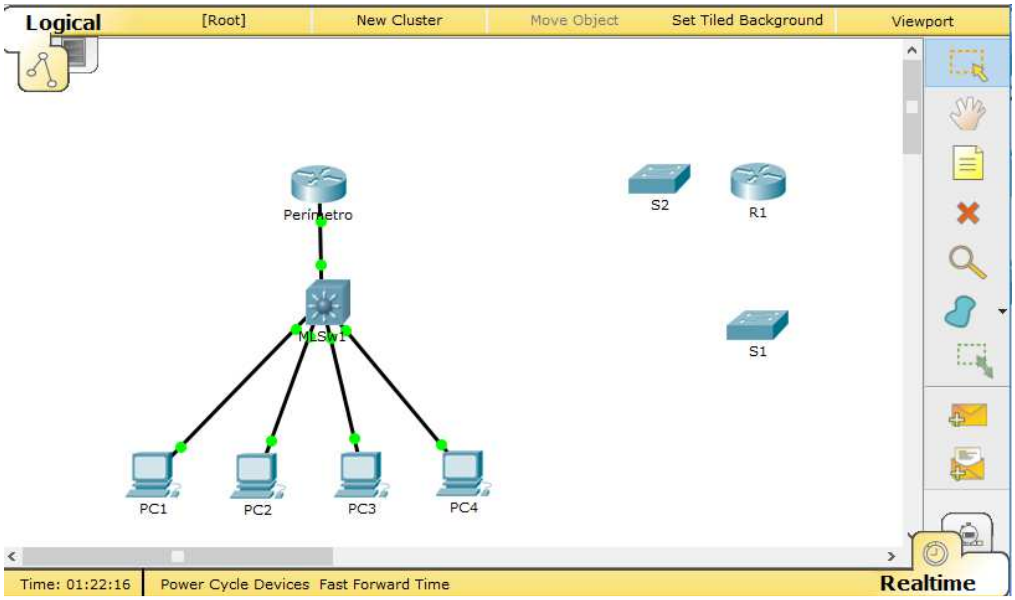


b. Use la herramienta **Delete** (Eliminar) para eliminar todas las conexiones o simplemente elimine **R1**, **S1** y **S2**.



c. Seleccione los cables adecuados para completar lo siguiente:

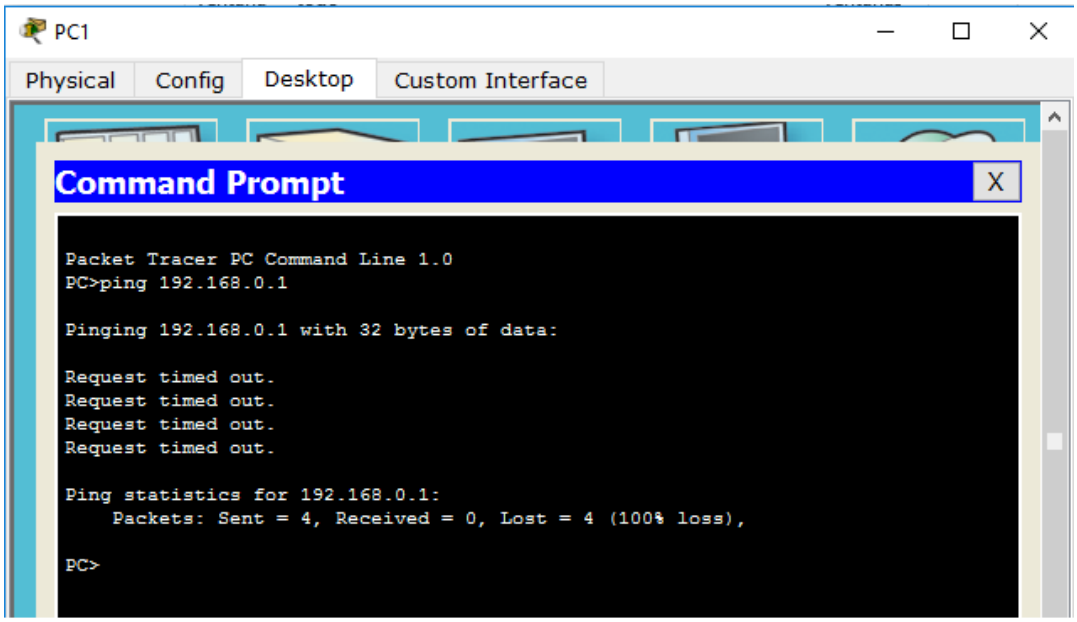
- Conectar **MLSw1 GigabitEthernet 0/1** a **Edge GigabitEthernet 0/0**.

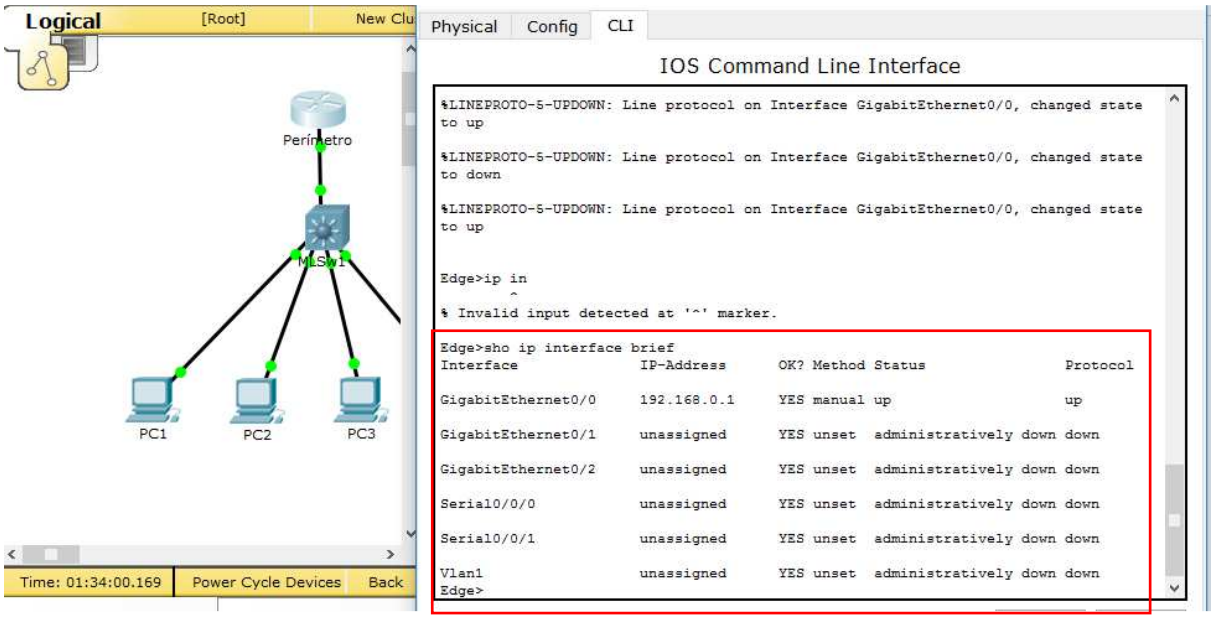


- Conectar las PC a los puertos Fast Ethernet en **MLSw1**.

d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.

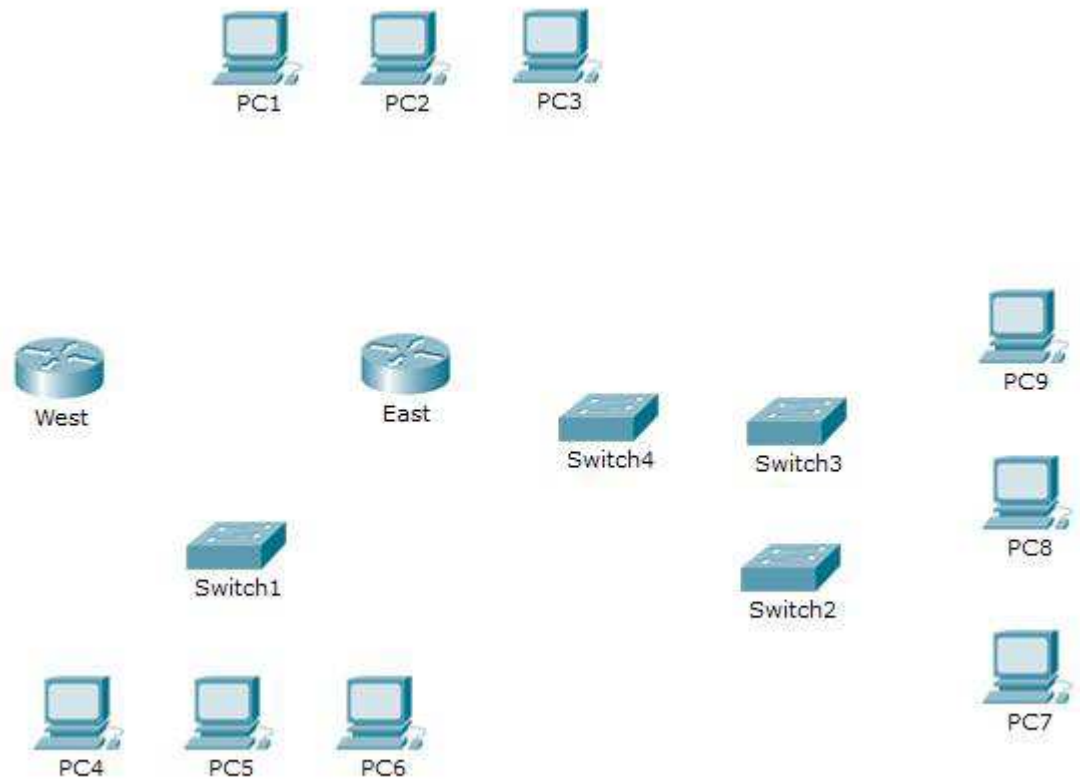
Nota: espere hasta que las luces de enlace anaranjadas cambien a color verde.



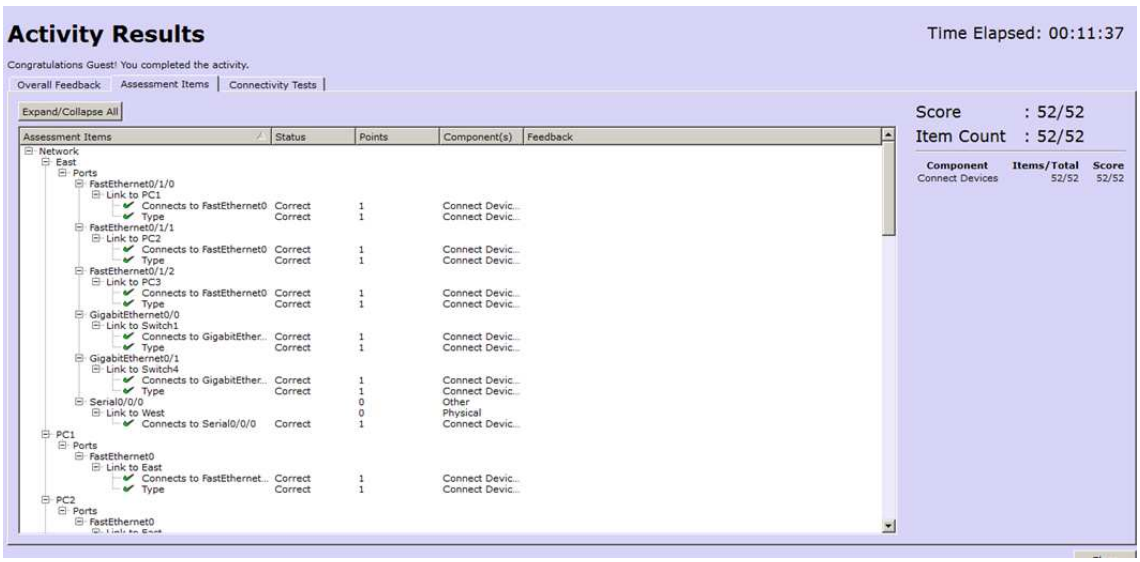


PRACTICA 6.3.1.0

Packet Tracer: Exploración de dispositivos de internetworking



Captura de Pantalla Solución del Laboratorio



Puntos del Laboratorio que necesitan muestra o demostración

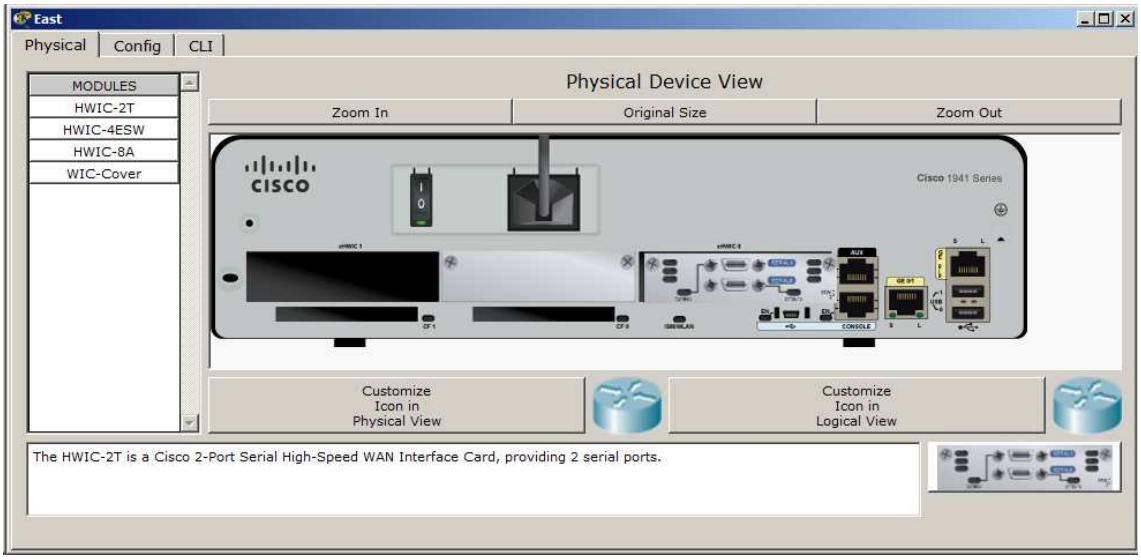
Parte 1: Identificar las características físicas de los dispositivos de internetworking

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? Auxiliar y consola



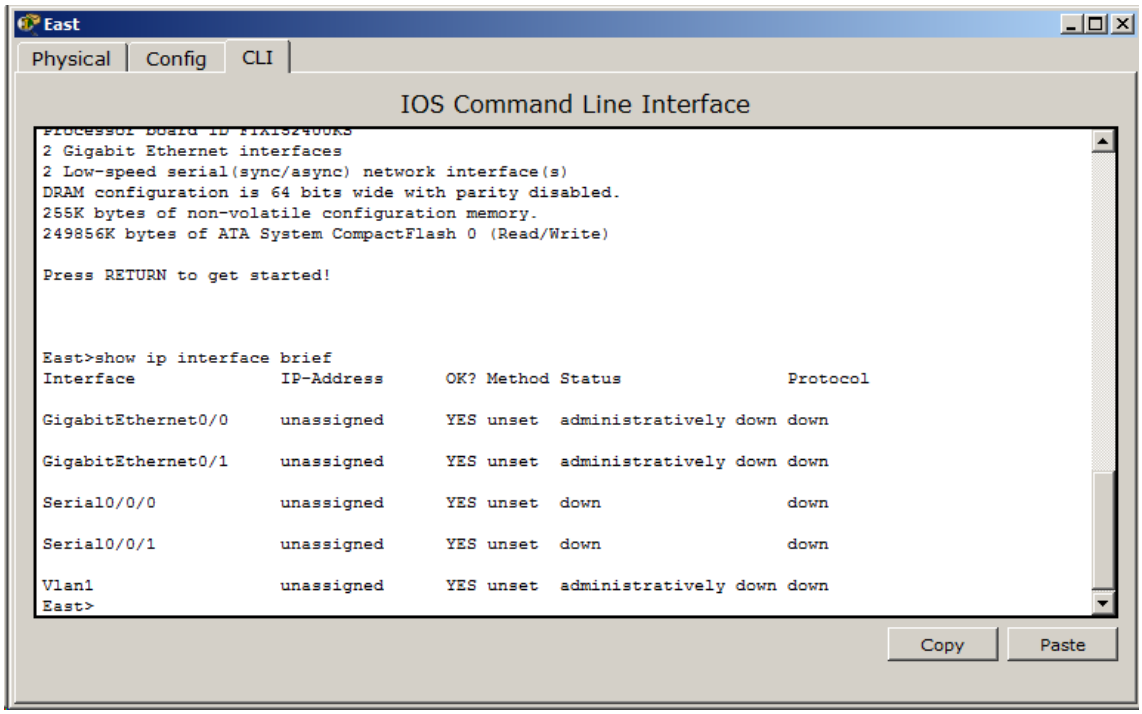
Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay?
2 Wan y 2 Gigabit

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

East> **show ip interface brief**

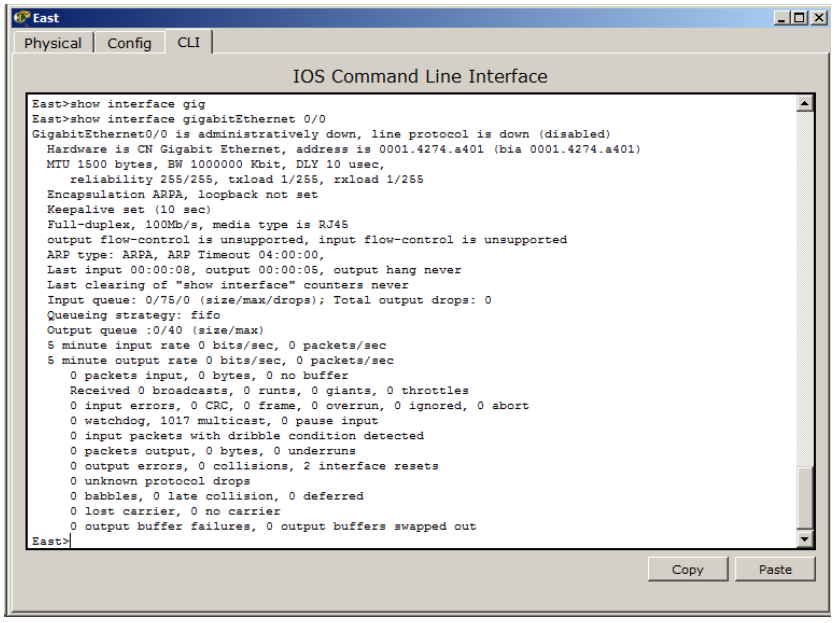
El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican?



c. Introduzca los siguientes comandos:

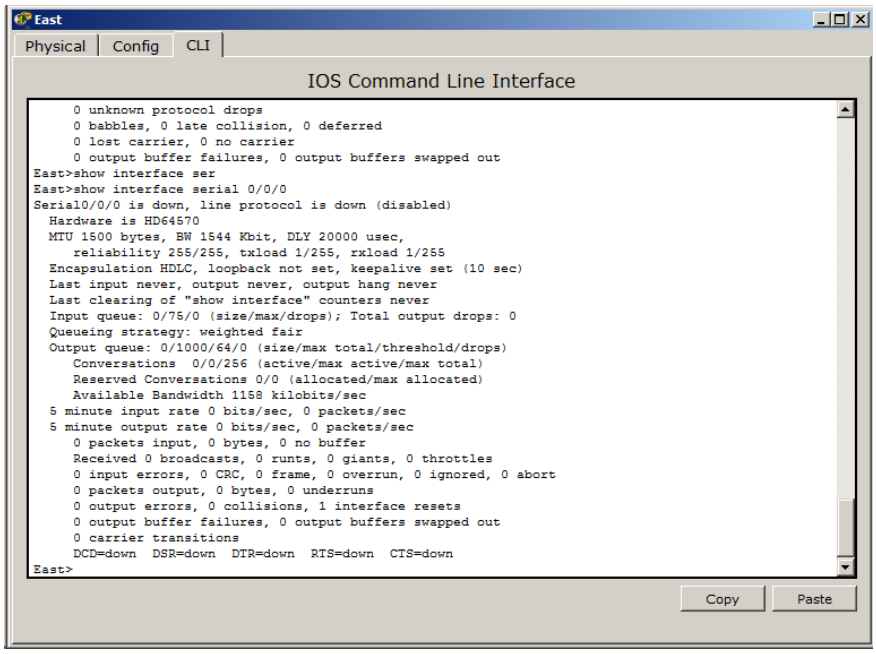
East> **show interface gigabitethernet 0/0**

¿Cuál es el ancho de banda predeterminado de esta interfaz?
1000000Kbit



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

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

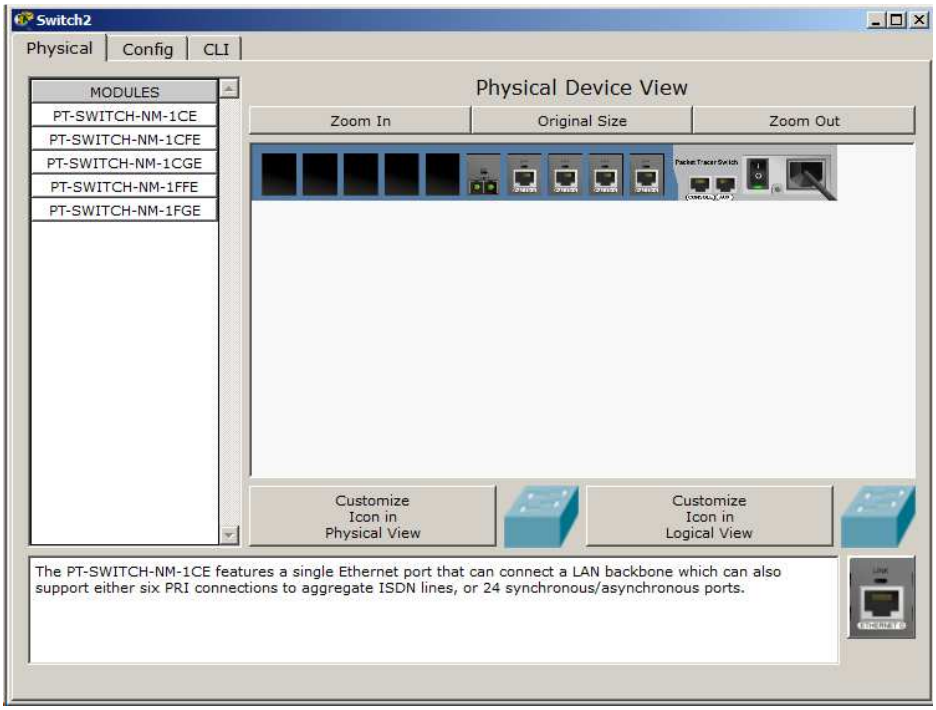


Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

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**?

b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles? 5 Ranuras



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**?

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 dispositivos

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

b. 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.

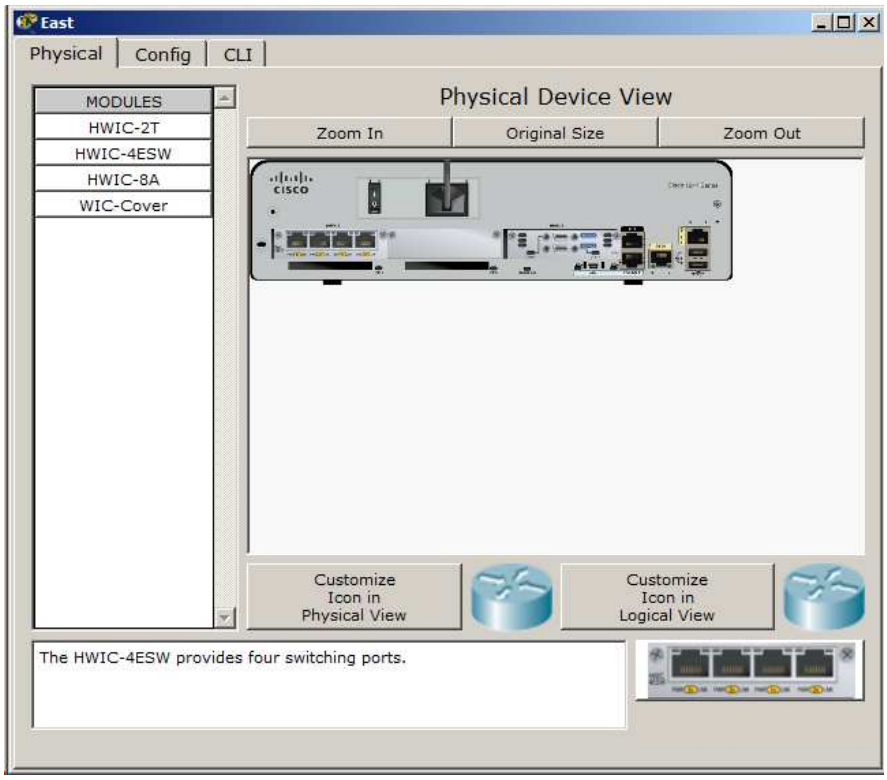
c. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

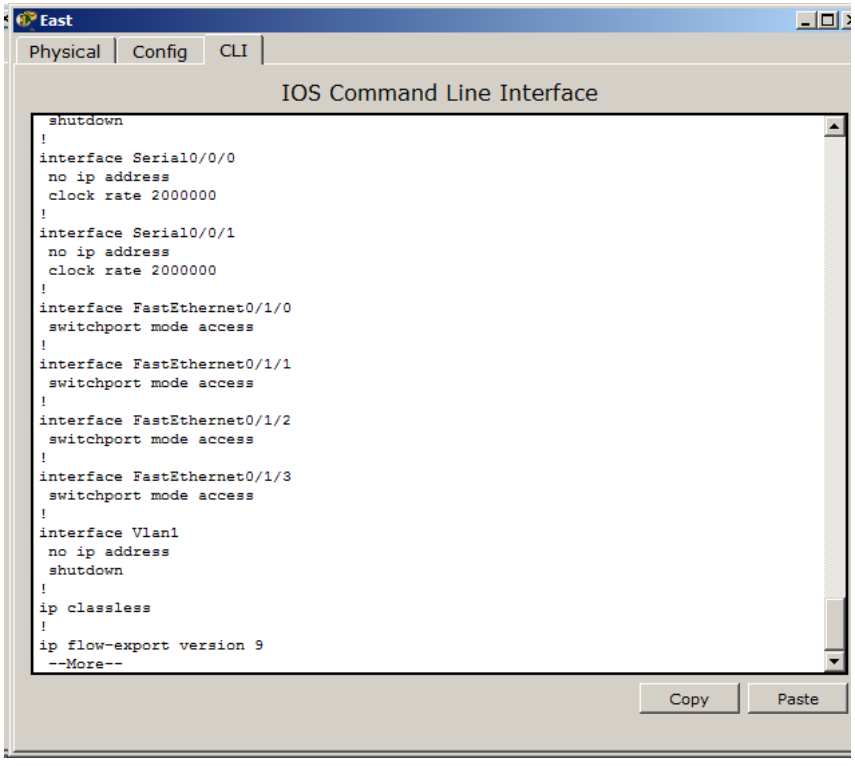
d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo.

¿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).

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





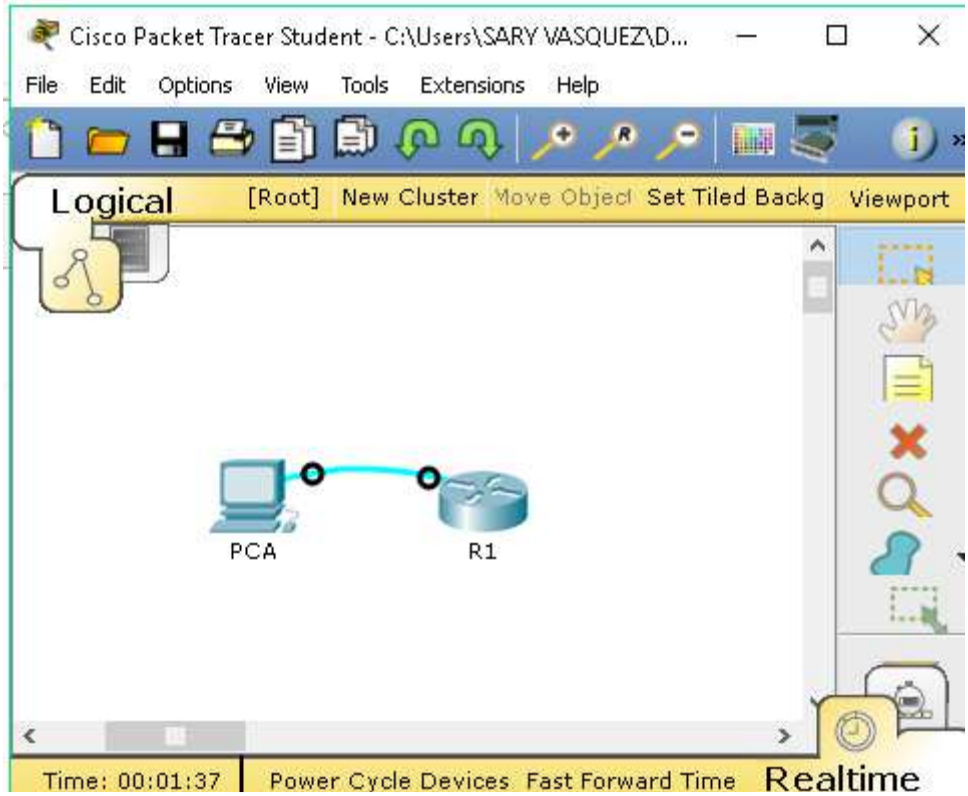
PRACTICA 6.4.1.2
Configuración inicial del Router
Topología

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.

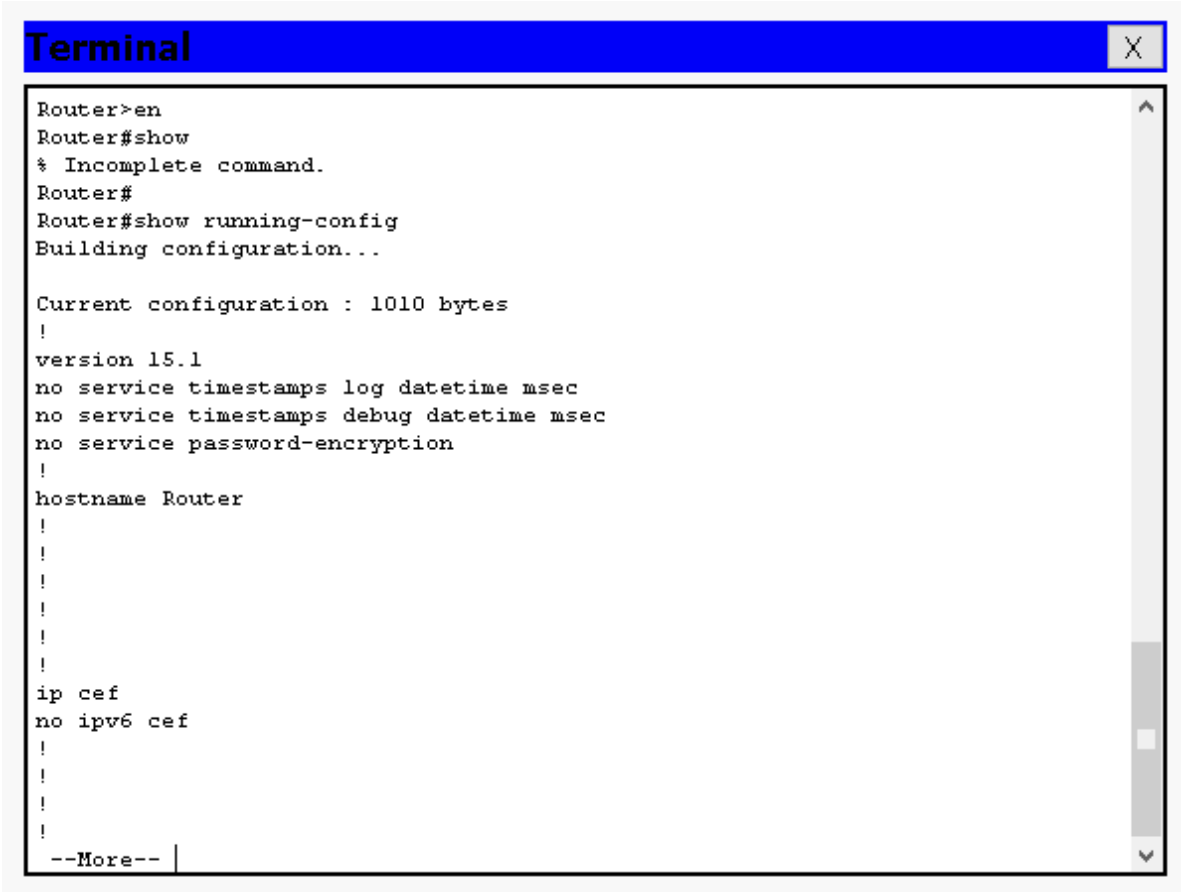
Router> enable

Router#

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

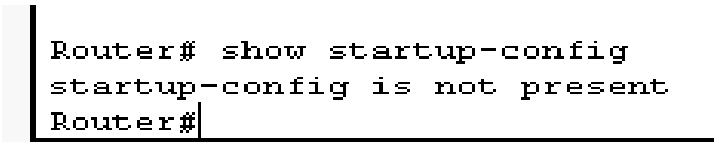
b. Introduzca el comando show running-config:

Router# show running-config



c. Responda las siguientes preguntas:
¿Cuál es el nombre de host del router? Router
¿Cuántas interfaces Fast Ethernet tiene el router? 4
¿Cuántas interfaces Gigabit Ethernet tiene el router? 2
¿Cuántas interfaces seriales tiene el router? 2
¿Cuál es el rango de valores que se muestra para las líneas vty? 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? 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.

```
Router# show startup-config
startup-config is not present
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

b. Utilice las siguientes contraseñas:
1) Consola: letmein
2) EXEC privilegiado, sin encriptar: cisco

```
Router# show startup-config
startup-config is not present
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable pas
% Incomplete command.
R1(config)#enable password cisco
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

3) EXEC privilegiado, encriptado: itsasecret

```
R1#en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret itsasecret
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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).

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd *Unauthorized access is strictly prohibited.*
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Nota: la actividad se configura con una expresión normal para que solo se detecte la palabra “access” en el comando banner motd del alumno.

Paso 2: Verificar los parámetros iniciales de R1

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

```
Press RETURN to get started!

Unauthorized access is strictly prohibited.

User Access Verification

Password: |
```

¿Por qué todos los routers deben tener un mensaje del día (MOTD)?
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?
R1(config-line)# login

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

```
 Unauthorized access is strictly prohibited

User Access Verification

Password:

R1>en
Password:
Password:
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

¿Por qué la contraseña secreta de enable permitiría el acceso al modo EXEC privilegiado y la contraseña de enable dejaría de ser válida? 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.
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? copy running-config startup-config
   ¿Cuál es la versión más corta e inequívoca de este comando? copy r s
   ¿Qué comando muestra el contenido de la NVRAM? 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

```
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
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

¿Cuántos archivos hay almacenados actualmente en la memoria flash?
3
¿Cuál de estos archivos cree que es la imagen de IOS? c1900-universalk9- mz.SPA.151-4.M4.bin
¿Por qué cree que este archivo es la imagen de IOS? 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]
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
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


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

1177 bytes copied in 0.416 secs (2829 bytes/sec)
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
  4   1177     startup-config
[33848764 bytes used, 221895236 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R1#
```

PRACTICA 6.4.3.3

Packet Tracer: Conexión de un router a una red LAN

Topología

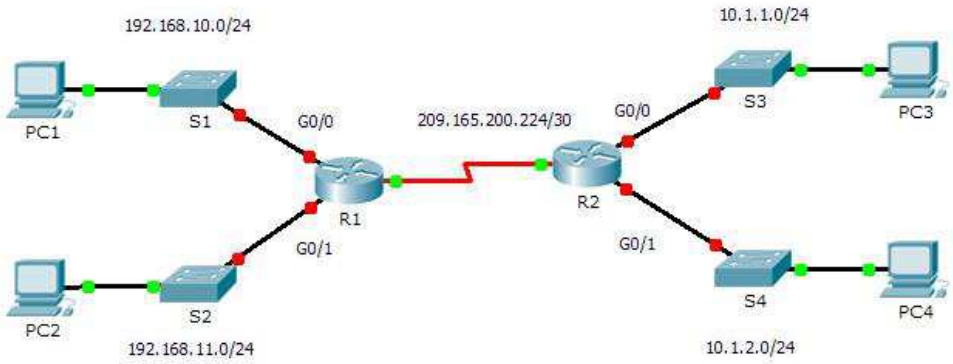


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara 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 (DCE)	209.165.200.225	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	192.168.11.10	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

Objetivos

Parte 1: Mostrar la información del router

Paso 2: Configurar las interfaces del router

Paso 3: Verificar la configuración

Información básica

En esta actividad, utilizará diversos comandos **show** para mostrar el estado actual del router. Después utilizará la Tabla de direccionamiento para configurar las interfaces Ethernet del router. Finalmente, utilizará comandos para verificar y probar las configuraciones.

Nota: los routers en esta actividad están parcialmente configurados. Algunas de las configuraciones no se incluyen en este curso, pero se proporcionan para ayudarlo a utilizar los comandos de verificación.

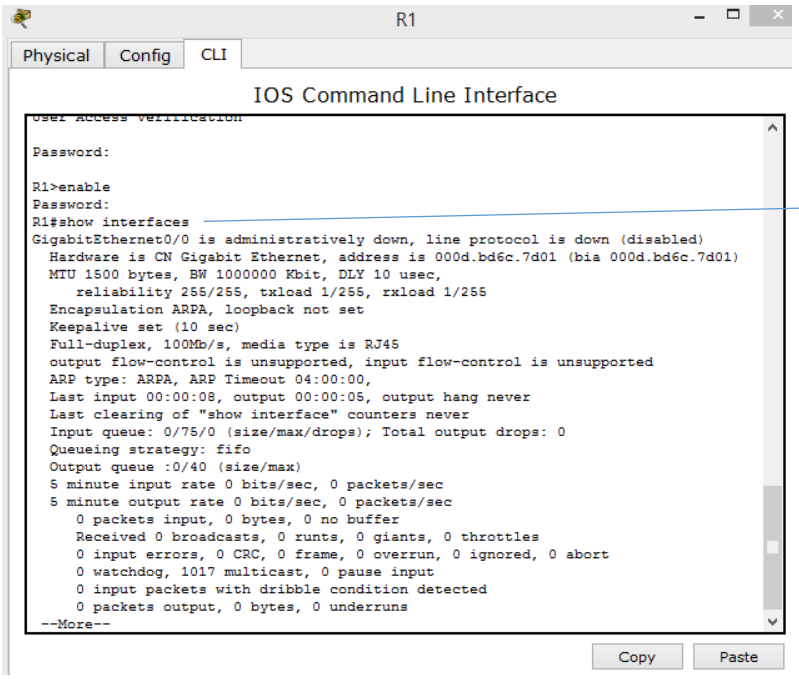
Parte 1: Mostrar la información del router

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**.

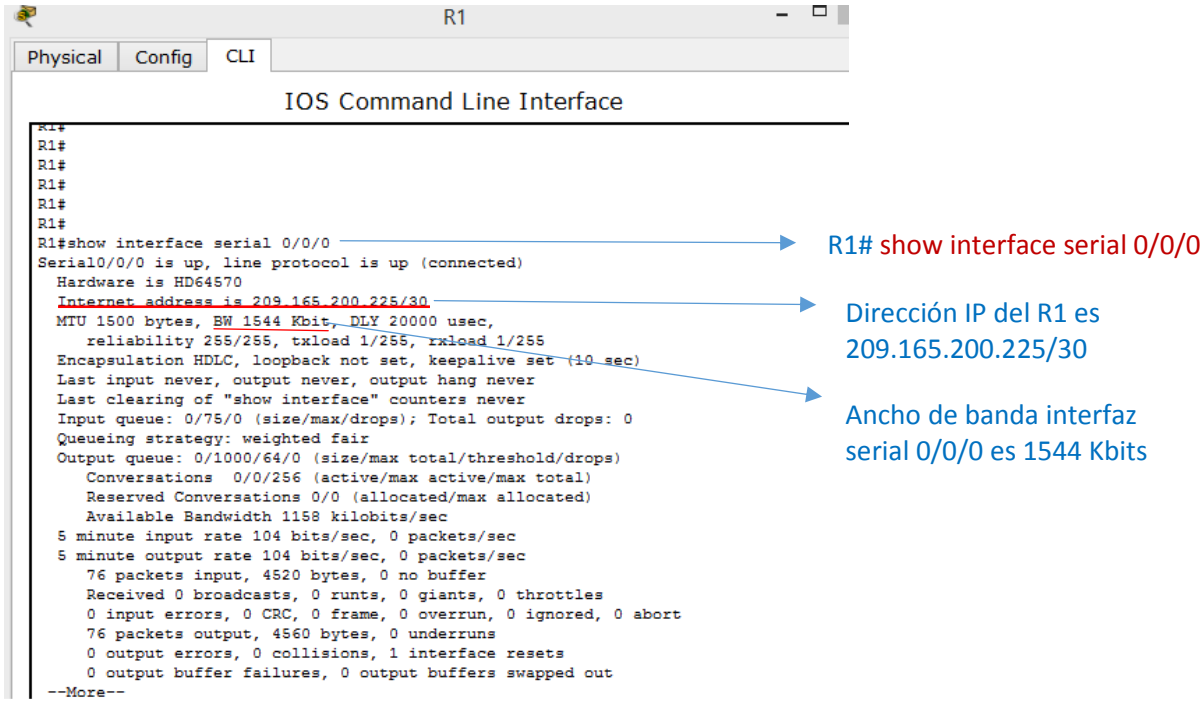
a. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router?

show interfaces



e. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0?

show interface serial 0/0/0

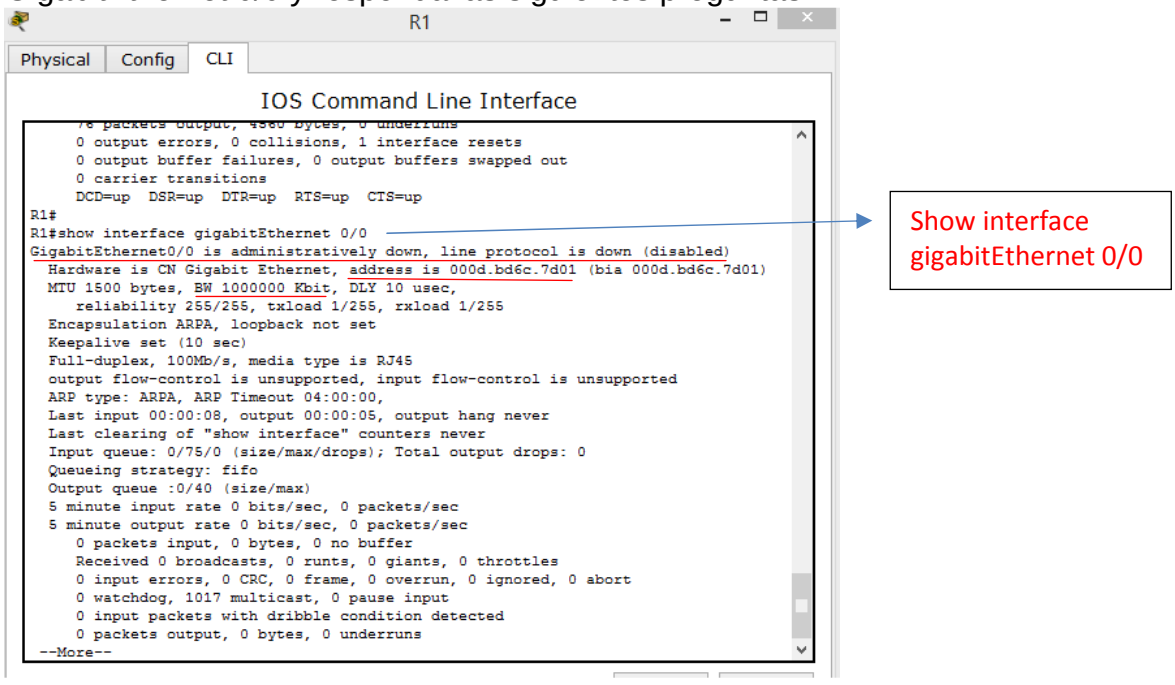


f. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

   a. ¿Cuál es la dirección IP configurada en el **R1**?
   209.165.200.225/30

   b. ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0? 1544 kbits

g. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:



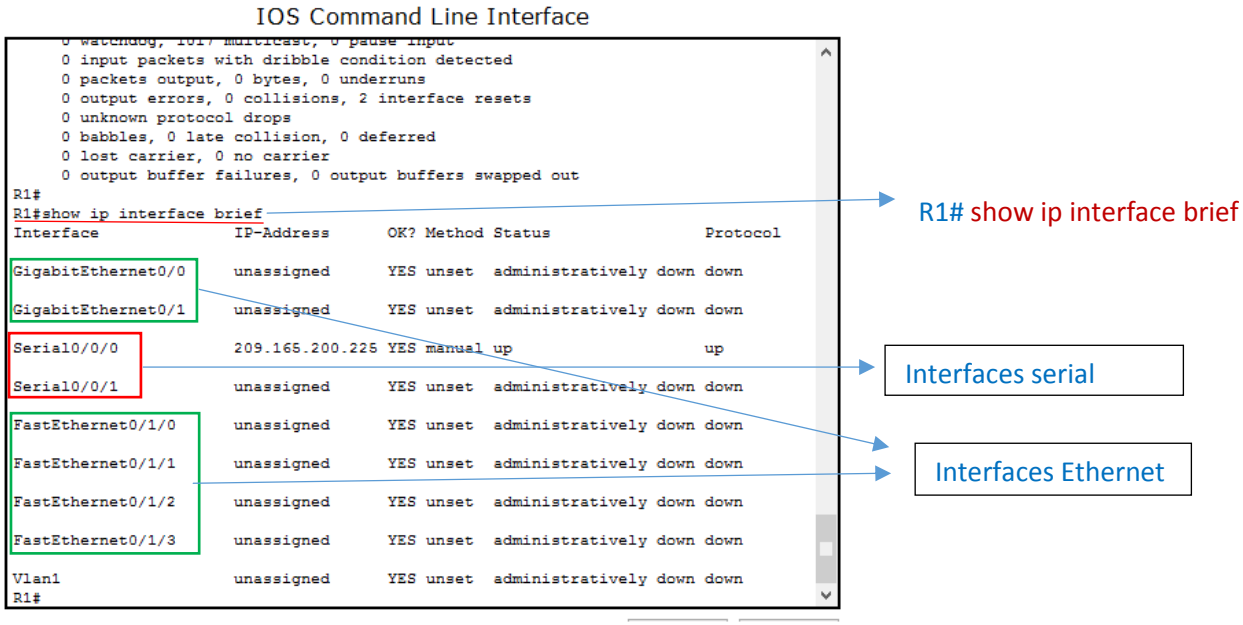
a. ¿Cuál es la dirección IP en el **R1**? No hay una dirección IP configurada en la interfaz GigabitEthernet 0/0.

b. ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0? 000d.bd6c.7d01

c. ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0? 1 000 000 kbits

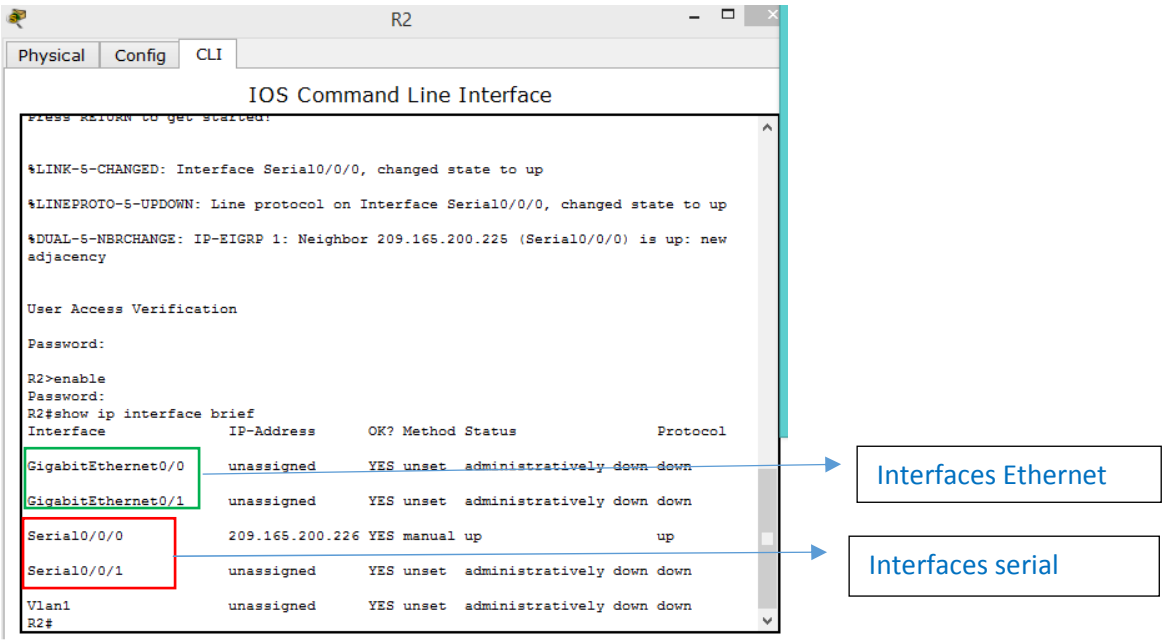
Paso 2: Mostrar una lista de resumen de las interfaces en el R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas? show ip interface brief



b. Introduzca el comando en cada router y responda las siguientes preguntas:

¿Cuántas interfaces seriales hay en **R1** y **R2**? Cada router tiene 2 interfaces seriales.



¿Cuántas interfaces Ethernet hay en **R1** y **R2**? R1 tiene seis interfaces Ethernet y R2 tiene dos interfaces Ethernet.

¿Son iguales todas las interfaces Ethernet en el **R1**? Si no es así, explique las diferencias. No lo son. Hay dos interfaces Gigabit Ethernet y cuatro interfaces Fast Ethernet. Las interfaces Gigabit Ethernet admiten velocidades de hasta 1 000 000 000 bits, y las interfaces Fast Ethernet admiten velocidades de hasta 1 000 000 bits.

Paso 3: Mostrar la tabla de enrutamiento en el R1

1. ¿Qué comando muestra el contenido de la tabla de enrutamiento? show ip route

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

2. Introduzca el comando en el **R1** y responda las siguientes preguntas:

a. ¿Cuántas rutas conectadas hay (utilizan el código C)? 1

b. ¿Qué ruta se indica? 209.165.200.224/30

3. ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento? Un router solo envía paquetes a redes

indicadas en la tabla de enrutamiento. Si una red no aparece en la lista, el paquete se descarta.

Parte 2: Configurar las interfaces del router

Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1

a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitet
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R1(config-if)#exit
R1(config)#
```

b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.

R1(config-if)# **description LAN connection to S1**

```
R1(config-if)#exit
R1(config)#interf
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#description LAN connection to S1
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

c. Ahora, el **R1** debe poder hacer ping a la PC1.

R1(config-if)# **end**
%SYS-5-CONFIG_I: Configured from console by
console R1# **ping 192.168.10.10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

```
R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/5/15 ms

R1#
```

Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

a. Utilice la información en la Addressing Table para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:

1. Introduzca la dirección IP y active la interfaz.
2. Configure una descripción apropiada.
3. Verifique las configuraciones de las interfaces.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config-if)#exit
R1(config)#int
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip address 10.1.1.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R2(config-if)#
```

```
R2(config-if)#exit
R2(config)#in
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#ip address 10.1.2.1
% Incomplete command.
R2(config-if)#ip address 10.1.2.1. 255.255.255.0
                                  ^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 10.1.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R2(config-if)#
```

```
R2(config-if)#exit
R2(config)#in
R2(config)#interface s
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#description LAN connection to S3
R2(config-if)#exit
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#description LAN connection to S4
R2(config-if)#exit
R2(config)#
```

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? copy run start

Parte 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.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         192.168.11.1    YES manual up                    up
Serial0/0/0                209.165.200.225 YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
FastEthernet0/1/0          unassigned      YES unset  administratively down down
FastEthernet0/1/1          unassigned      YES unset  administratively down down
FastEthernet0/1/2          unassigned      YES unset  administratively down down
FastEthernet0/1/3          unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
R1#
```

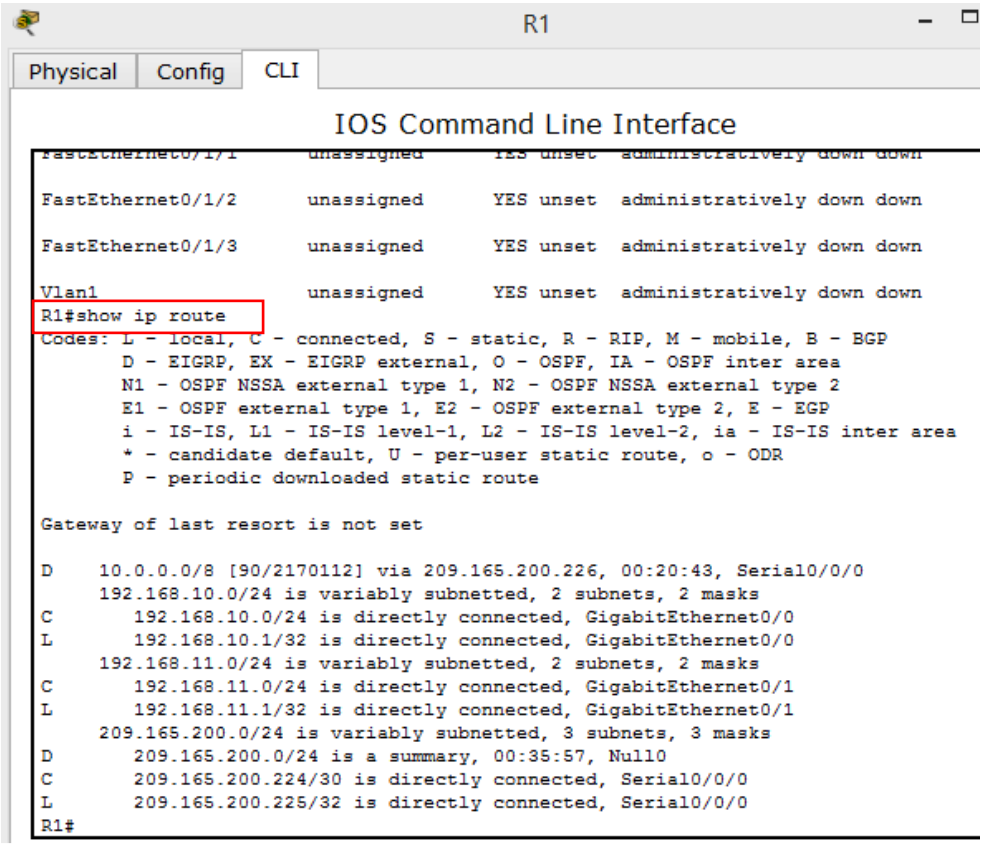
```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.1.1.1        YES manual up                    up
GigabitEthernet0/1         10.1.2.1        YES manual up                    up
Serial0/0/0                209.165.200.226 YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
R2#
```

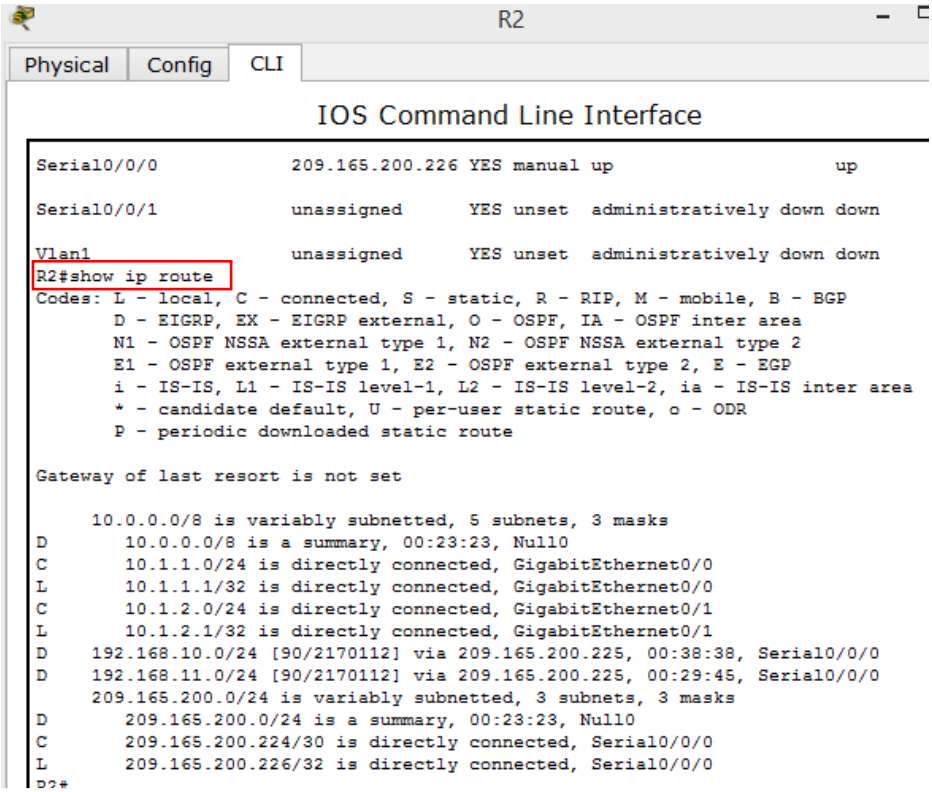
¿Cuántas interfaces en **R1** y **R2** están configuradas con direcciones IP y tienen el estado “up/up” (activa/activa)? Tres en cada router.

¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando? La máscara de subred

¿Qué comandos puede utilizar para verificar esta parte de la configuración?
show run, show interfaces, show ip protocols

b. 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? 3

¿Cuántas rutas EIGRP (utilizan el código **D**) ve en cada router? 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? 5

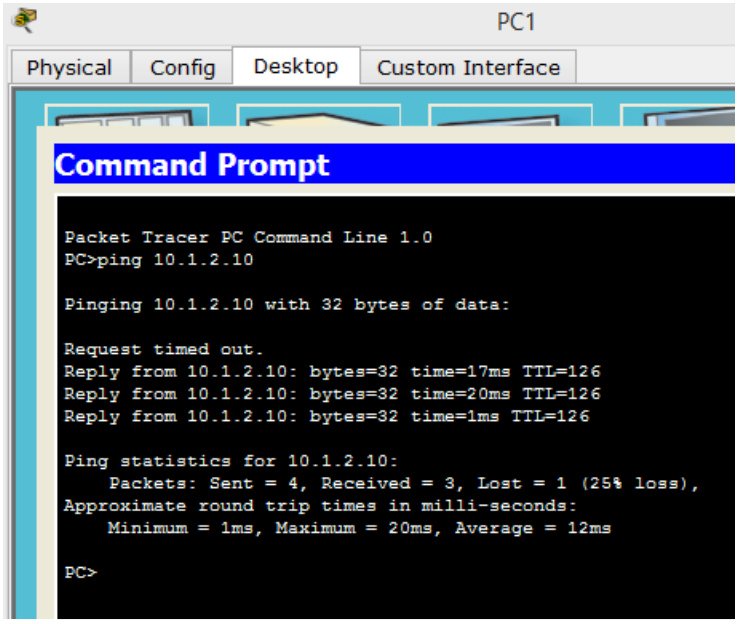
¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? sí

Nota: si su respuesta es “no”, falta una configuración necesaria. Revise los pasos de la parte 2.

Paso 2: Probar la conectividad de extremo a extremo a través de la red

Ahora debería poder hacer ping desde cualquier PC a cualquier otra PC en la red. Además, debería poder hacer ping a las interfaces activas de los routers. Por ejemplo, las siguientes pruebas deberían realizarse correctamente:

a. Desde la línea de comandos en la PC1, haga ping a la PC4.



b. Desde la línea de comandos en el R2, haga ping a la PC2.

```
R2#ping 192.168.11.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/13/18 ms

R2#
```

PRACTICA 6.4.3.4: Packet Tracer: Resolución de problemas del gateway predeterminado

Topología

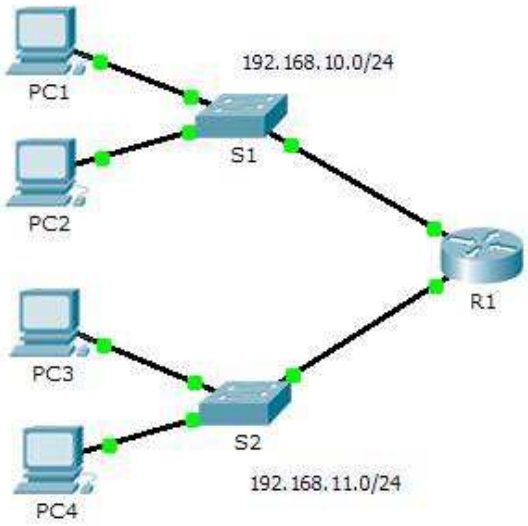


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara 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
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Objetivos

Parte 1: Verificar el registro de la red y descartar problemas

Parte 2: Implementar, verificar y documentar las soluciones

Información básica

Para que un dispositivo se comunique a través de varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se utiliza cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local a la que el host está conectado. En esta actividad, terminará de documentar la red. A continuación, verificará la documentación de la red mediante la puesta a prueba de la conectividad de extremo a extremo y la resolución de problemas. El método de resolución de problemas que utilizará consta de los siguientes pasos:

1. Verificar la documentación de la red y utilizar pruebas para descartar problemas.

2. Determinar cuál es la solución adecuada para un problema dado.

3. Implementar la solución.

4. Realizar pruebas para verificar que se haya resuelto el problema.

5. Documentar la solución.

A lo largo de sus estudios de CCNA, encontrará distintas descripciones del método de resolución de problemas, así como distintas formas de probar y documentar problemas y soluciones. Esto es intencional. No existe un estándar o una plantilla establecida para la resolución de problemas. Cada organización desarrolla procesos y estándares de documentación exclusivos (incluso si ese proceso consiste en no tener ninguno). No obstante, todas las metodologías de resolución de problemas eficaces generalmente incluyen los pasos anteriores.

> **Nota:** si usted es experto en la configuración de gateway predeterminado, es posible que esta actividad parezca más compleja de lo debido. Lo más probable es que pueda descubrir y solucionar todos los problemas de conectividad más rápido que si siguiera estos procedimientos. No obstante, a medida que avance con sus estudios, las redes y los problemas que encuentre serán cada vez más complejos. En tales situaciones, la única forma eficaz de descartar y resolver problemas es aplicar un enfoque metódico como el que se usa en esta actividad.

Parte 1: Verificar el registro de la red y descartar problemas

En la parte 1 de esta actividad, completará la documentación y realizará pruebas de conectividad para detectar problemas. Además, determinará la solución adecuada y la implementará en la parte 2.

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

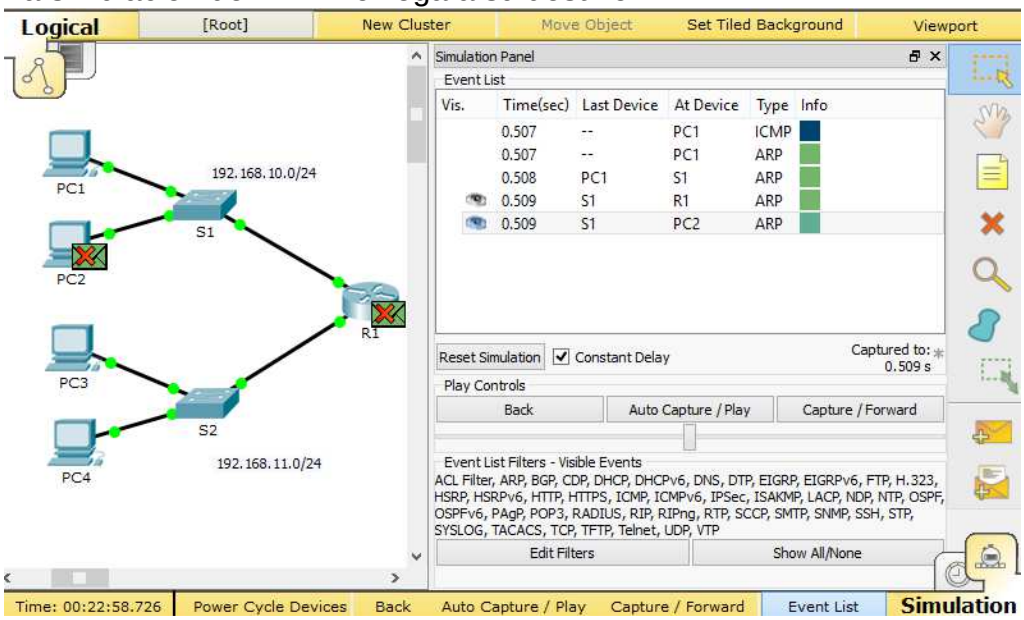
Prueba	¿Se realizó Correctamente?	Problemas	Solución	Verificado
PC1 a PC2	**No**	**Dirección IP en la PC1 está incorrecta**	**Cambiar la dirección IP de la PC1 a 192.168.10.10**	Si
PC1 a PC4	no	Se revisaron las configuraciones IP y se encontró que el PC4 tiene configurado un gateway predeterminado incorrecto	corregir el Gateway 192.168.1.1 por 192.168.11.1	Si
Configuración del S1	no	Se revisó la configuración con el comando Show running-config y se encontró que no tiene el Gateway configurado.	Realizar la configuración del Gateway con el comando ip default-gateway y la dirección 192.168.10.1	Si
Configuración del S2	no	Se revisó la configuración con el comando show running	Configurar la dirección IP del S2, según la tabla de direccionamiento	si

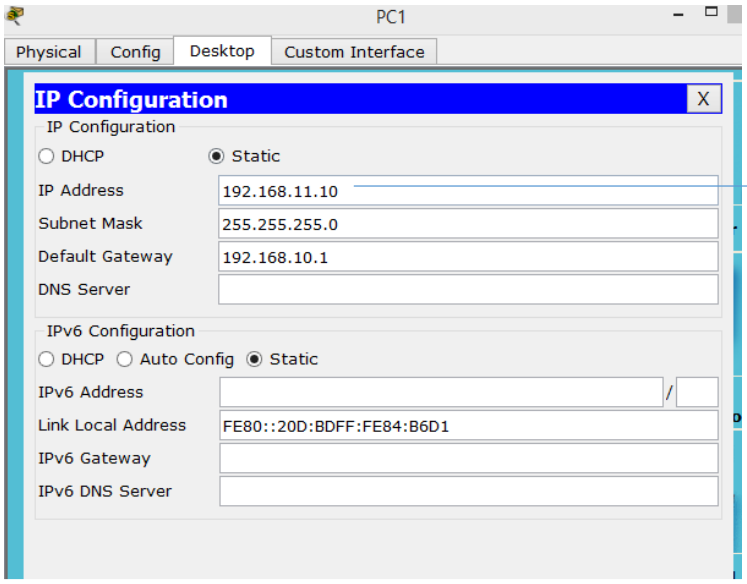
		config y se encontró que no tiene la dirección IP		

c. 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.

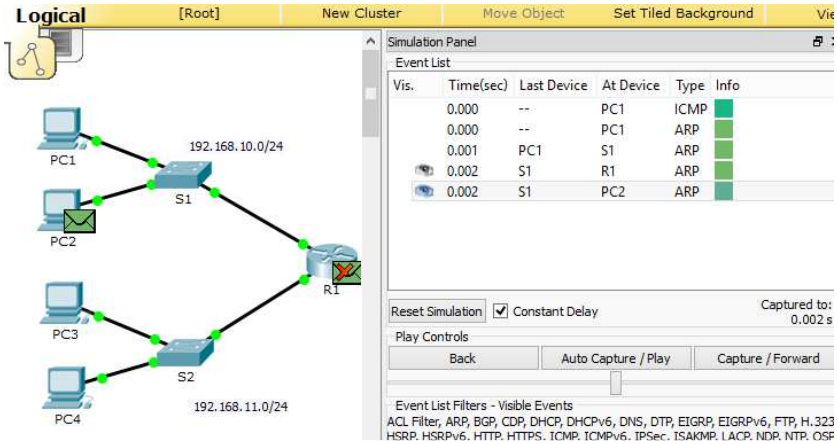
   Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

Prueba PC1 a PC2:
La simulación del PDA no llega a su destino





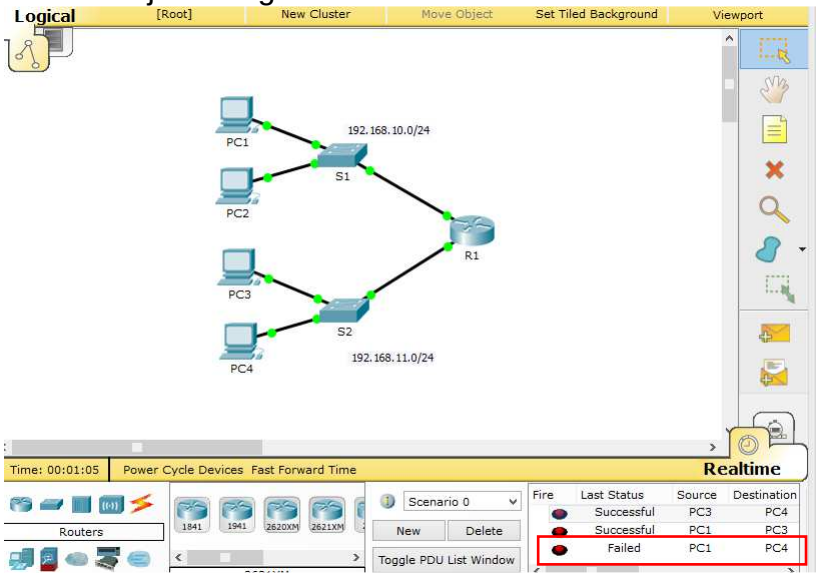
Se corrigió la dirección IP por 192.168.10.10

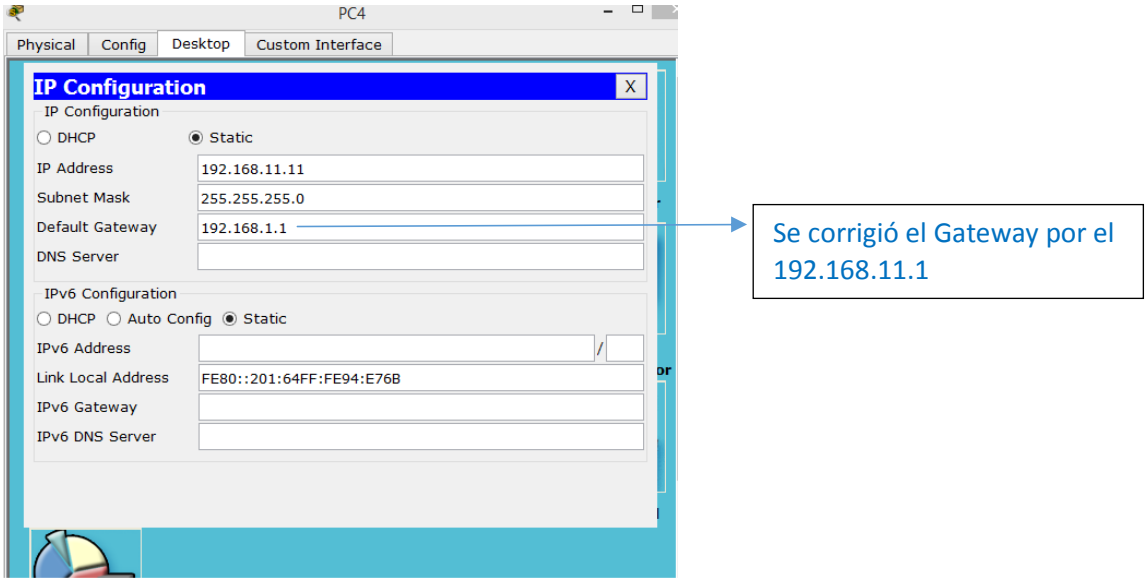


Simulación exitosa.

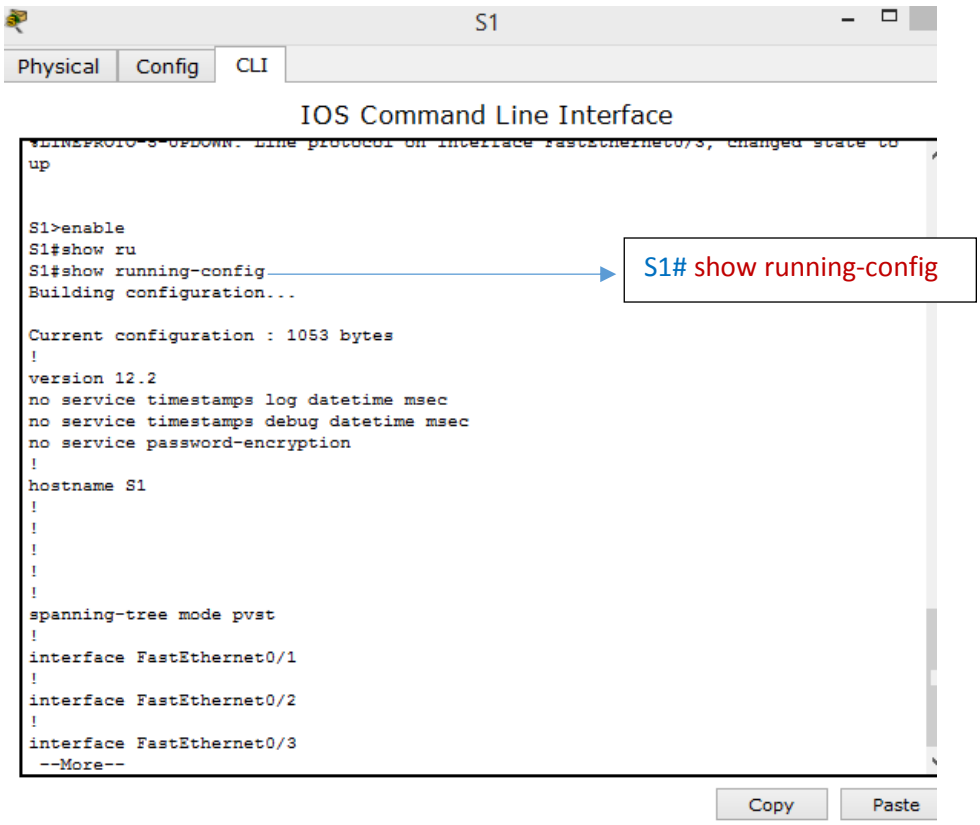
Prueba PC1 a PC4:

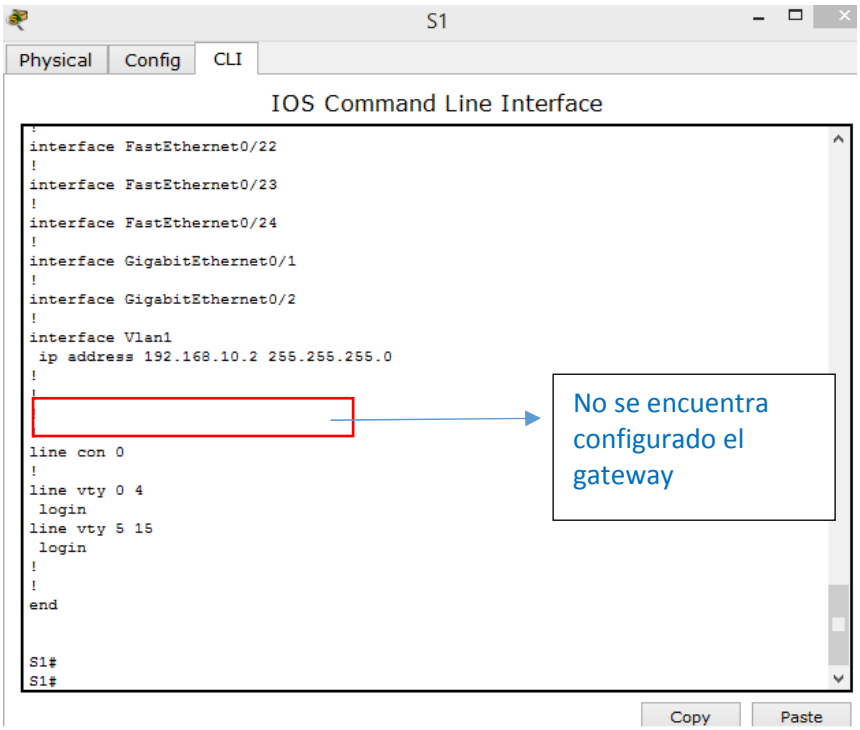
El mensaje no llega a su destino

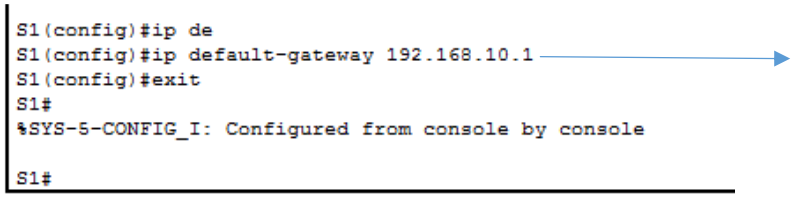




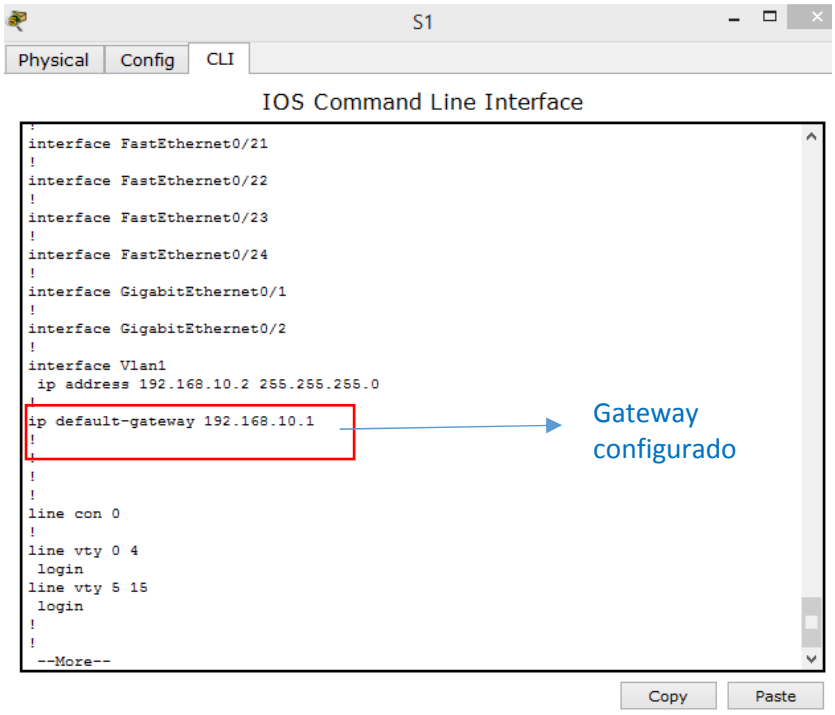
Prueba al dispositivo S1:



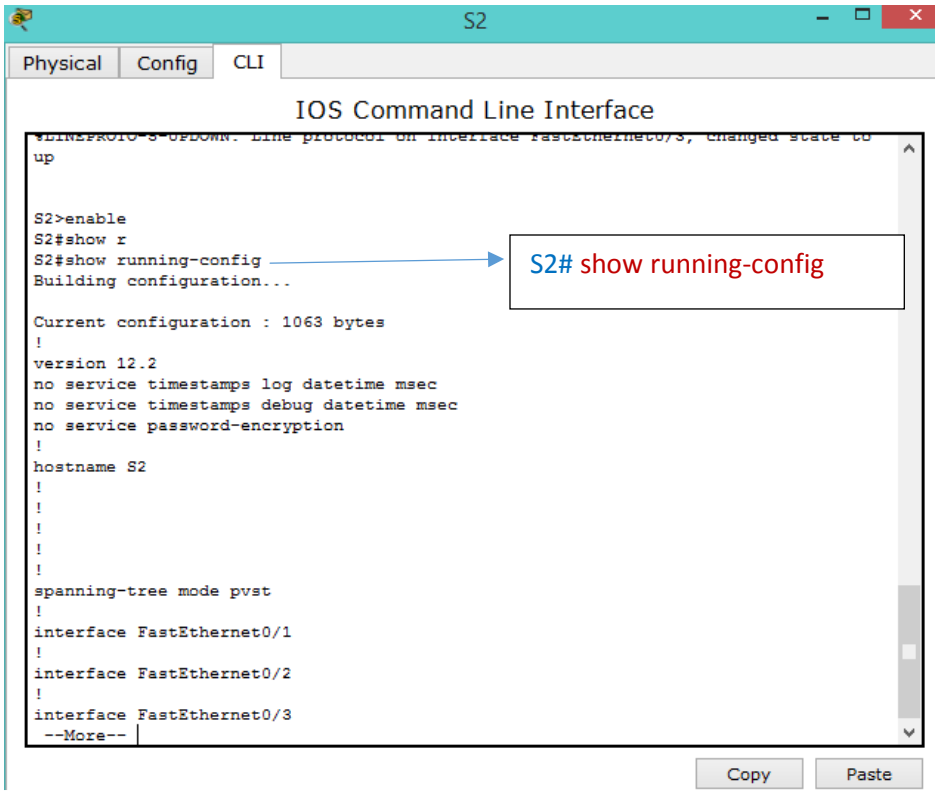


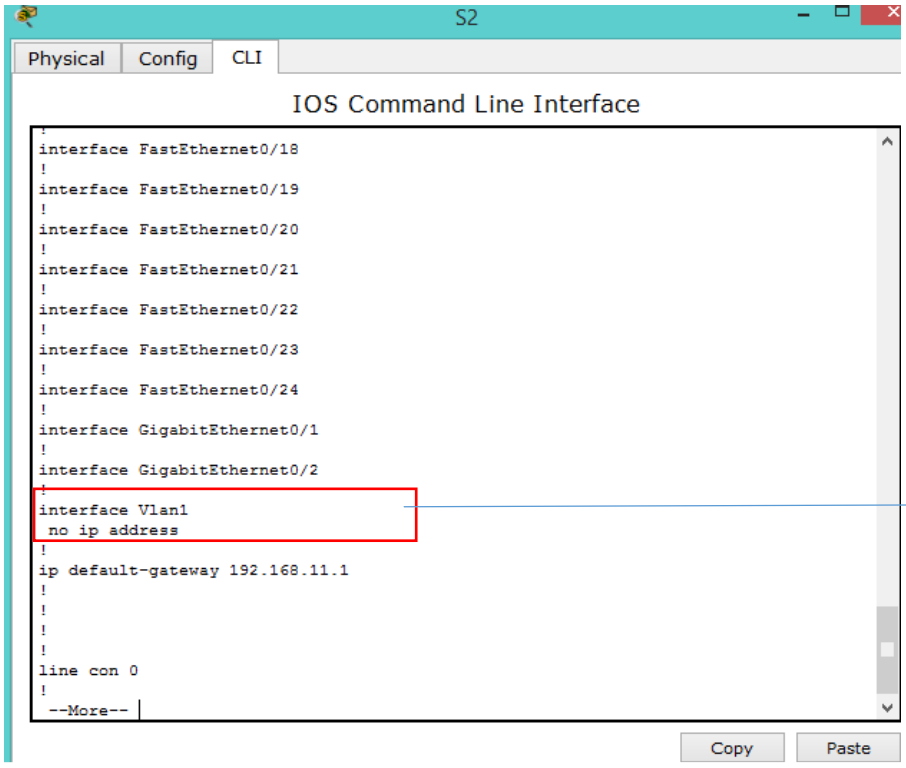


Se configura el Gateway con el comando.
S1(config)# Ip default-gateway 192.168.10.1

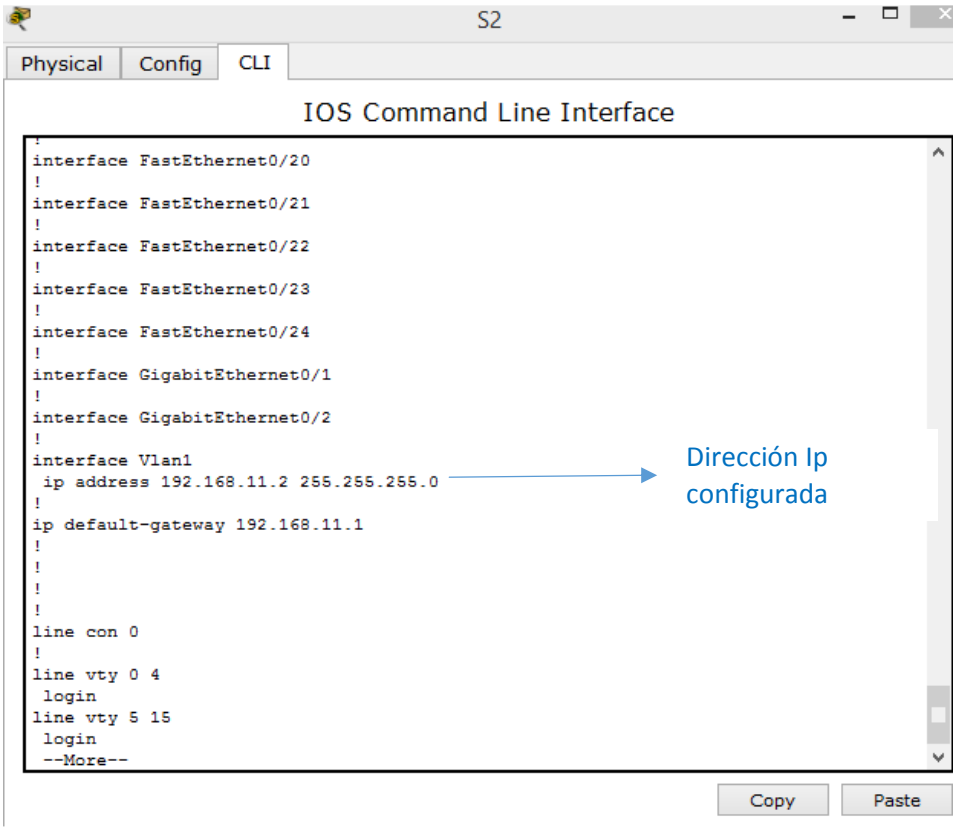


Prueba al dispositivo S2:

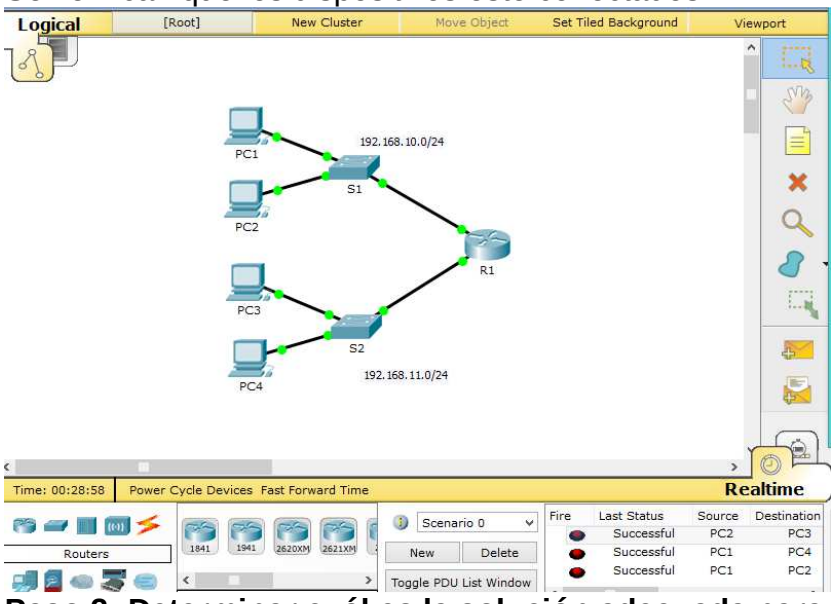

S2
Physical
Config
CLI
IOS Command Line Interface
up
S2>enable
S2#show r
S2#show running-config
Building configuration...
Current configuration : 1063 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
--More--
Copy
Paste
S2# show running-config


S2
Physical
Config
CLI
IOS Command Line Interface
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
!
ip default-gateway 192.168.11.1
!
!
!
!
line con 0
!
--More--
Copy
Paste
No se encuentra la dirección IP

```
S2(config)#interface Vlan 1
S2(config-if)#ip address 192.168.11.2 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```



Se verifican que los dispositivos este conectados



Paso 2: Determinar cuál es la solución adecuada para el problema

a. Con sus conocimientos sobre la forma en que operan las redes y sus aptitudes para configurar dispositivos, busque la causa del problema. Por ejemplo, el S1 no es la causa del problema de conectividad entre la PC1 y la PC2. Las luces de enlace son de color verde, y ninguna configuración en el S1 provocaría que no pase el tráfico entre la PC1 y la PC2. Por lo tanto, el problema debe de estar en la PC1, en la PC2 o en ambas.
b. verifique el direccionamiento del dispositivo para asegurarse de que coincida con el registro de la red. Por ejemplo, la dirección IP para la PC1 es incorrecta, como se verificó con el comando **ipconfig**.
c. Sugiera una solución con la que usted crea que se resolverá el problema y documéntela. Por ejemplo, cambiar la dirección IP de la PC1 para que coincida con la documentación.

Nota: por lo general, hay más de una solución. Sin embargo, una práctica recomendada de resolución de problemas es implementar de a una solución por vez. Implementar más de una solución podría presentar problemas adicionales en una situación más compleja.

Parte 2: Implementar, verificar y documentar las soluciones

En la parte 2 de esta actividad, implementará las soluciones que identificó en la parte 1. Luego, verificará si la solución funcionó. Es posible que deba volver a la parte 1 para terminar de descartar todos los problemas.

Paso 1: Implementar soluciones para abordar los problemas de conectividad

Consulte la documentación en la parte 1. Elija el primer problema e implemente la solución que sugirió. Por ejemplo, corrija la dirección IP en la PC1.

Paso 2: Verificar si ahora el problema está resuelto

a. Verifique si la solución que propuso solucionó el problema realizando la prueba que usó para identificarlo. Por ejemplo, ¿la PC1 puede ahora hacer ping a la PC2?

b. Si el problema se resolvió, indíquelo en la documentación. Por ejemplo, en la tabla anterior, con colocar una simple marca de verificación en la columna “Verificado” sería suficiente.

Paso 3: Verificar si se resolvieron todos los problemas

a. Si todavía tiene un problema pendiente con una solución que aún no se implementó, vuelva al paso 1 de la parte 2.

b. Si se solucionaron todos los problemas actuales, ¿también solucionó todos los problemas de conectividad remota (por ejemplo, que la PC1 pueda hacer ping a la PC4)? Si la respuesta es negativa, vuelva al paso 1c de la parte 1 para probar la conectividad remota.

PRACTICA 6.5.1.2
Packet Tracer: Reto de habilidades de integración

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
College	G0/0	172.14.5.1	255.255.255.0	No aplicable
	G0/1	172.14.10.1	255.255.255.0	No aplicable
Class-A	VLAN 1	172.14.5.35	255.255.255.0	172.14.5.1
Class-B	VLAN 1	172.14.10.35	255.255.255.0	172.14.10.1
Student-1	NIC	172.14.5.50	255.255.255.0	172.14.5.1
Student-2	NIC	172.14.5.60	255.255.255.0	172.14.5.1
Student-3	NIC	172.14.10.50	255.255.255.0	172.14.10.1
Student-4	NIC	172.14.10.60	255.255.255.0	172.14.10.1

Objetivos

- Terminar el registro de la red.
- Realizar la configuración básica de dispositivos en un router y un switch.
- Verificar la conectividad y resolver cualquier problema.

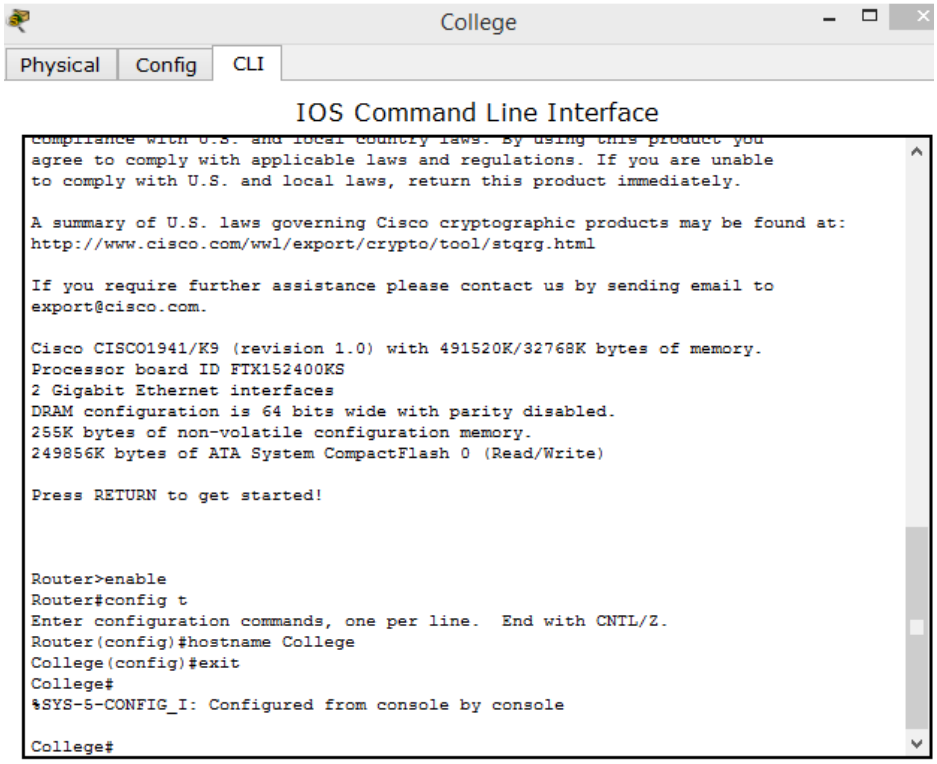
Situación

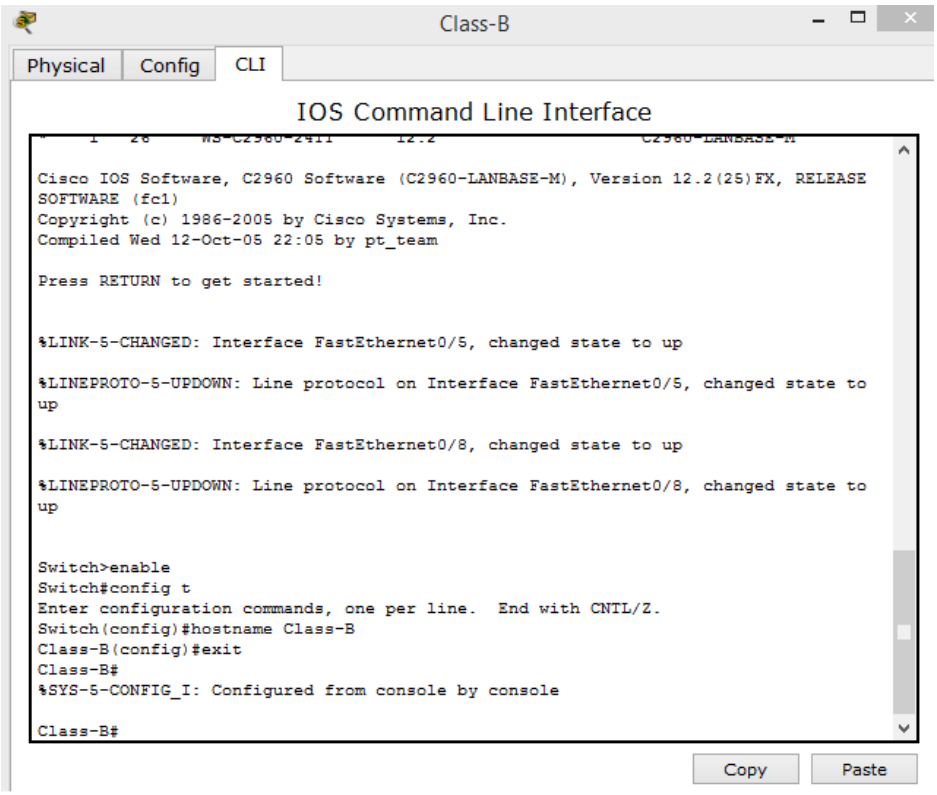
La administradora de la red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración básica de un router y un switch utilizando Cisco IOS. Luego, verificará la configuración realizada por usted, así como la configuración de los dispositivos existentes, probando la conectividad de extremo a extremo.

Nota: después de completar esta actividad, puede elegir hacer clic en el botón **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Entre los aspectos variables se incluyen los nombres de dispositivo, los esquemas de direccionamiento IP y la topología.

Requisitos

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre **College** al router y **Class-B** al segundo switch. No podrá acceder a **Class-A.**





- Utilice **cisco** como contraseña de EXEC del usuario para todas las líneas.

```
College>enable
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#line console 0
College(config-line)#password cisco
College(config-line)#login
College(config-line)#line vty 0 4
College(config-line)#password cisco
College(config-line)#login
College(config-line)#exit
College(config)#
```

```
Class-B>enable
Class-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-B(config)#line console 0
Class-B(config-line)#password cisco
Class-B(config-line)#login
Class-B(config-line)#line vty 0 4
Class-B(config-line)#pa
Class-B(config-line)#password cisco
Class-B(config-line)#login
Class-B(config-line)#exit
Class-B(config)#
```

- Utilice **class** como contraseña de EXEC privilegiado.

```
College(config-line)#exit
College(config)#enable secret class
College(config)#exit
College#
%SYS-5-CONFIG_I: Configured from console by console

College#
```

```
Class-B(config-line)#exit
Class-B(config)#enable secret class
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#
```

- Encripte todas las contraseñas de texto no cifrado.

```
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#service password-
College(config)#service password-encryption
College(config)#banner motd "warnning"
College(config)#
```

Comando de encriptación de contraseñas

- Configure un aviso apropiado.

```
Class-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-B(config)#serv
Class-B(config)#service pass
Class-B(config)#service password-encryption
Class-B(config)#bann
Class-B(config)#banner motd "warnning"
Class-B(config)#
```

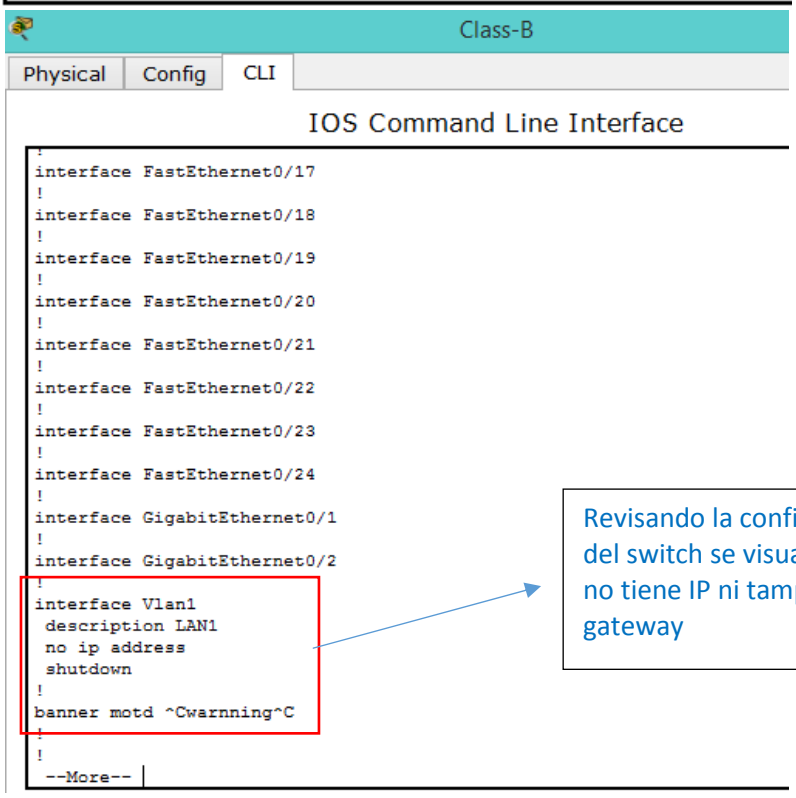
Mensaje MOTD

- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.

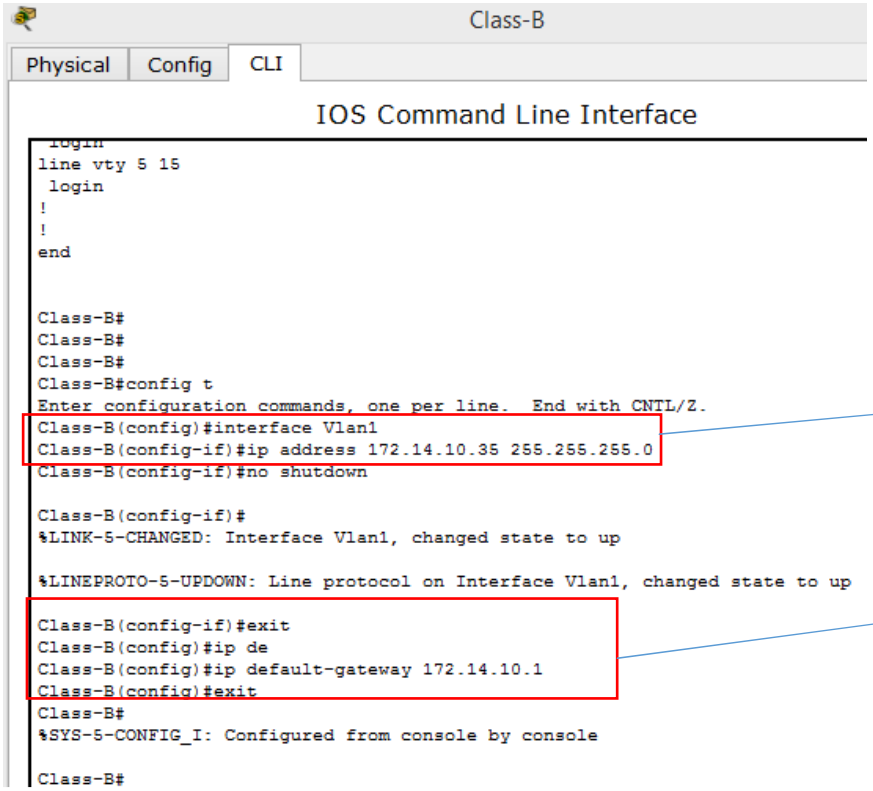
```
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#interface G0/1
College(config-if)#ip addre
College(config-if)#ip address 172.14.10.1 255.255.255.0
College(config-if)#no shutdown

College(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

College(config-if)#
```

- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **Class-B**.

```
Class-B(config)#interface Vlan 1
Class-B(config-if)#des
Class-B(config-if)#description LAN1
Class-B(config-if)#exit
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#
```

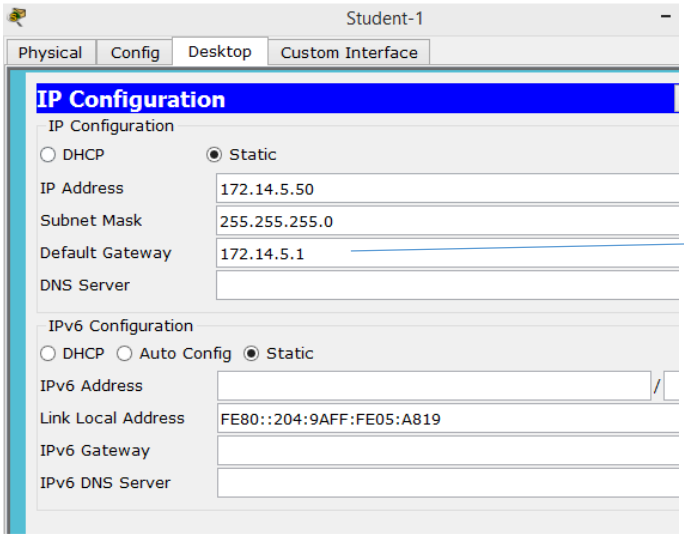


Revisando la configuración del switch se visualiza que no tiene IP ni tampoco gateway



Se configuro la dirección IP:
Ip address 172.14.10.35
255.255.255.0

Se asignó el Gateway al Switch: Class-B
Ip default-gateway
172.14.10.1

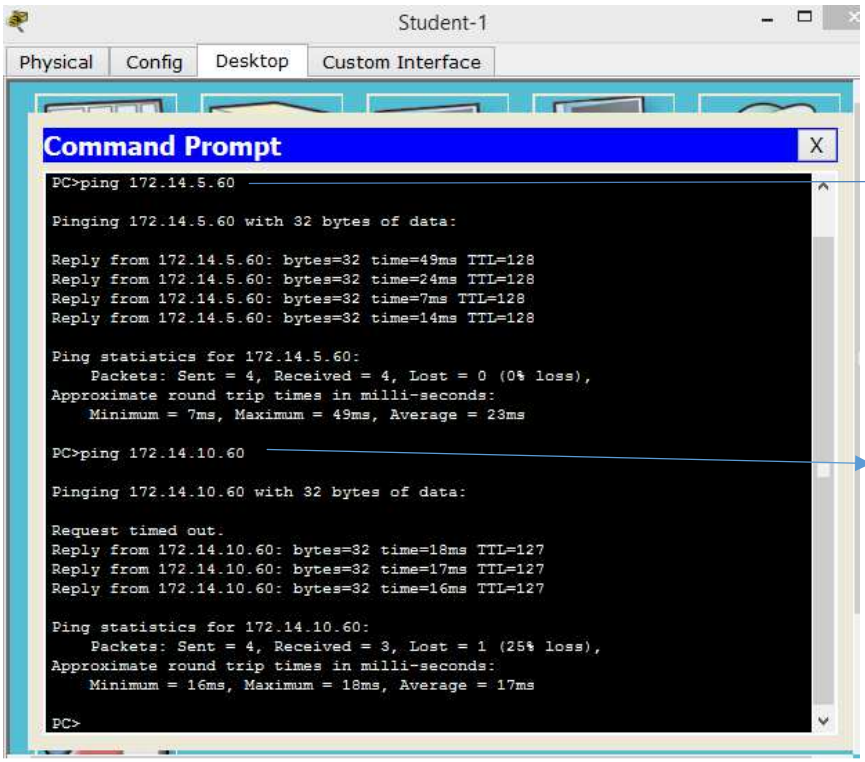


Se asignaron a cada uno de los PC los Gateway correspondiente

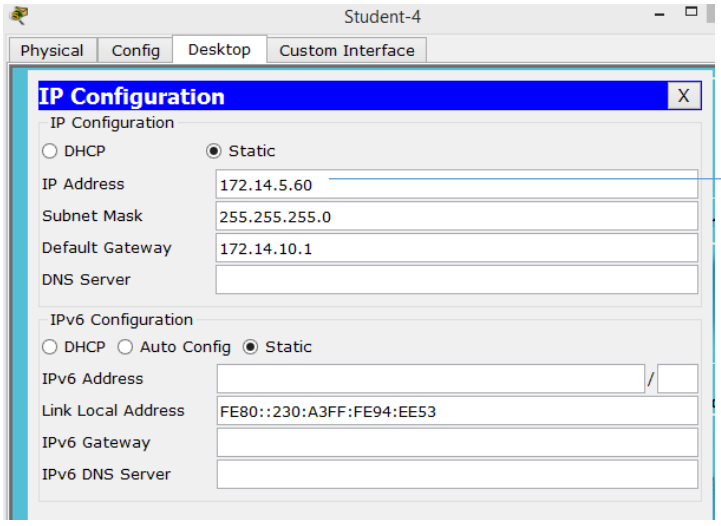
- Guarde las configuraciones.

```
Class-B#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
Class-B#
```

- Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.



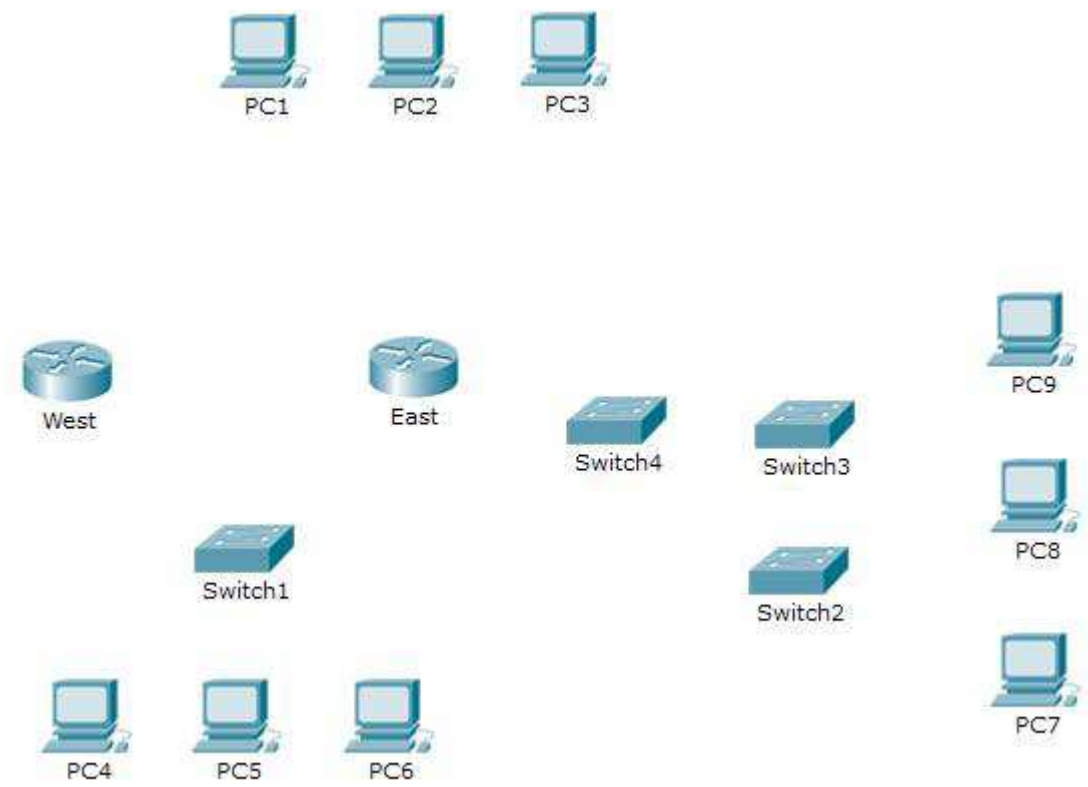
- Resuelva cualquier problema y regístrelo.



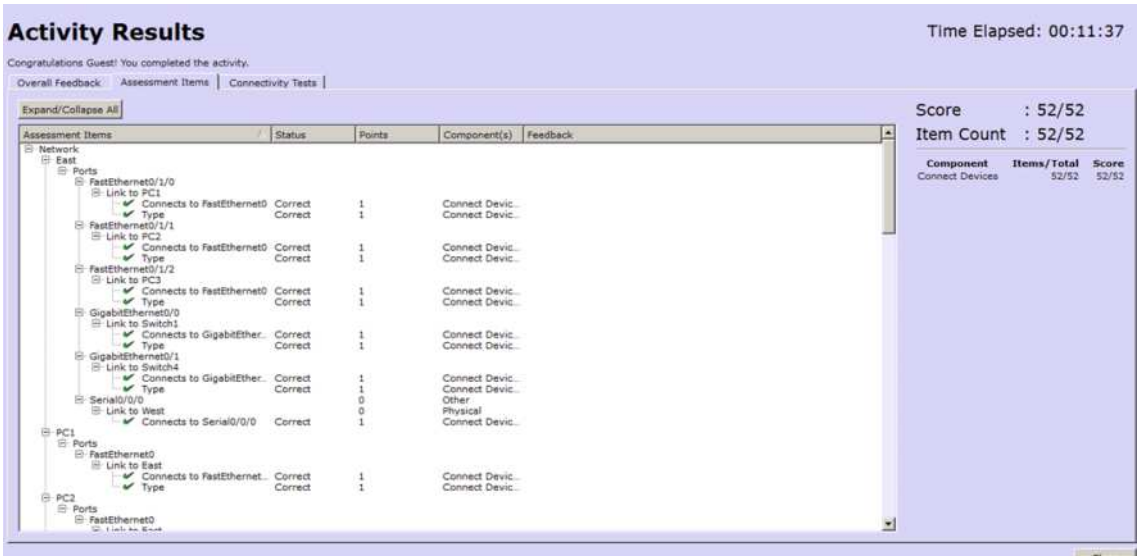
- Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo.

PRACTICA 6.3.1.0

Packet Tracer: Exploración de dispositivos de internetworking



Captura de Pantalla Solución del Laboratorio



Puntos del Laboratorio que necesitan muestra o demostración

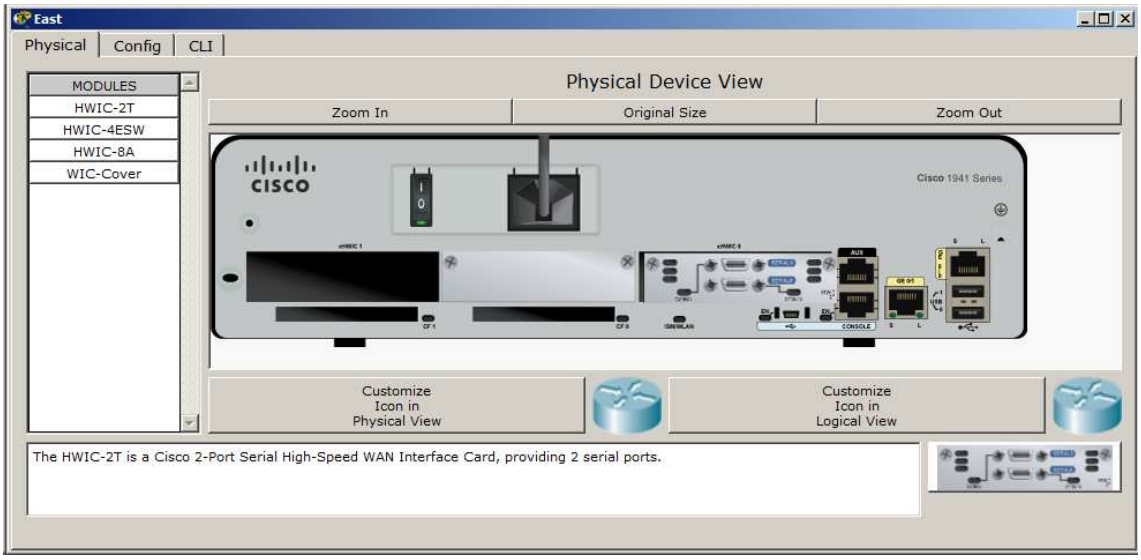
Parte 1: Identificar las características físicas de los dispositivos de internetworking

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? Auxiliar y consola



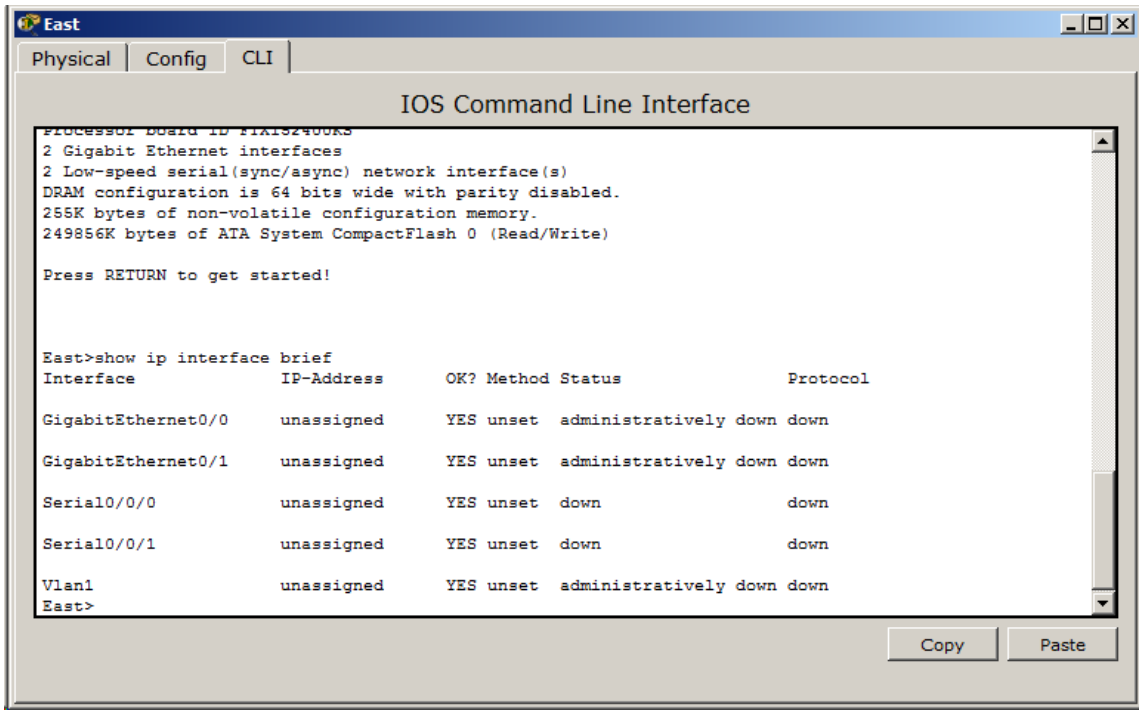
Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

a. ¿Qué interfaces LAN y WAN se encuentran disponibles en el router **East** y cuántas hay?
2 Wan y 2 Gigabit

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

East> **show ip interface brief**

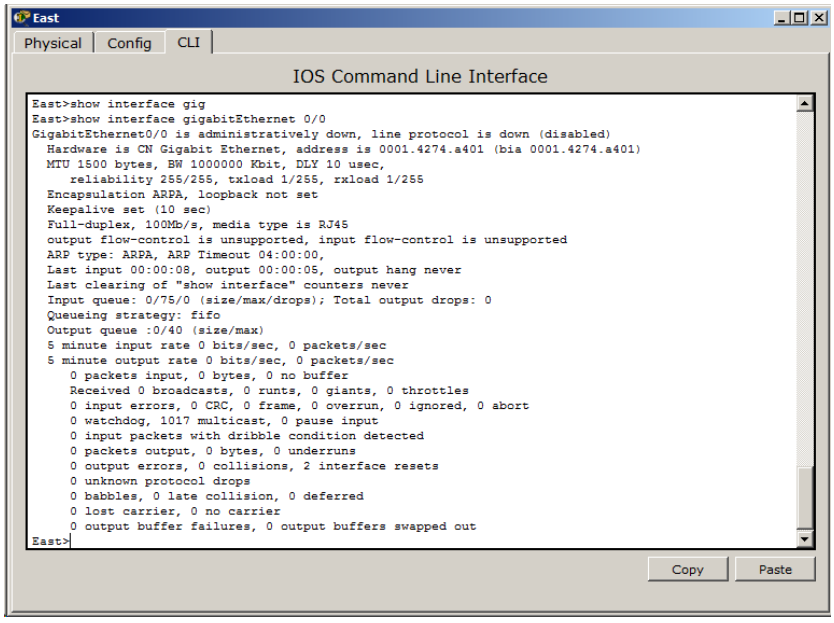
El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican?



c. Introduzca los siguientes comandos:

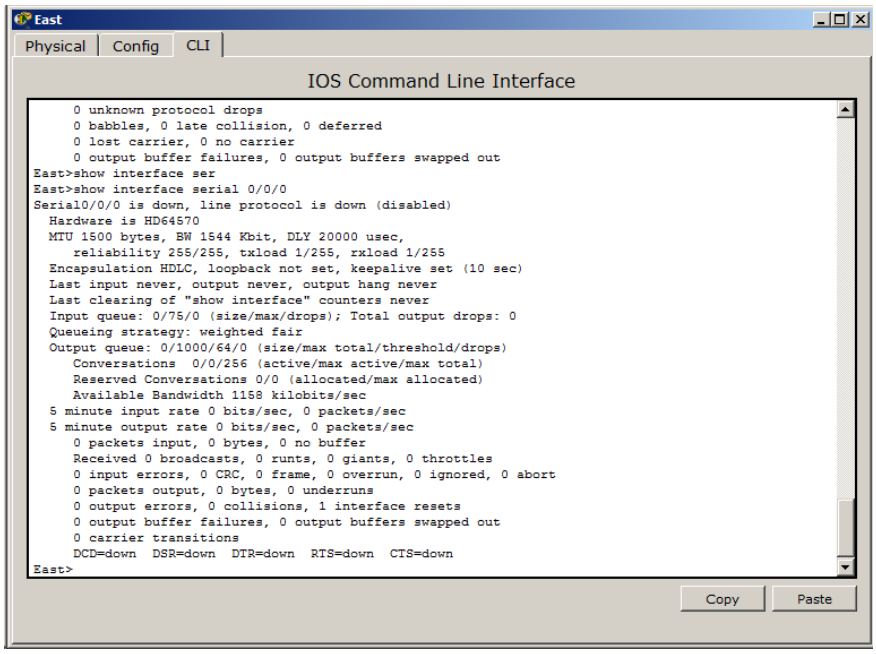
East> **show interface gigabitethernet 0/0**

¿Cuál es el ancho de banda predeterminado de esta interfaz?
1000000Kbit



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

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

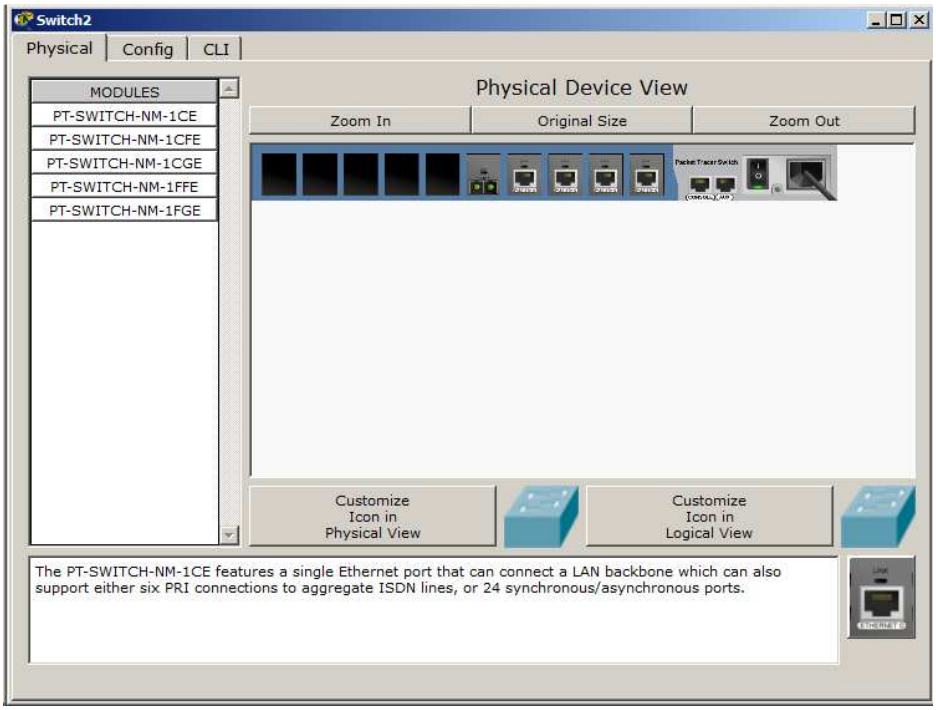


Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

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**?

b. Haga clic en **Switch2** o **Switch3** .¿Cuántas ranuras de expansión están disponibles? 5 Ranuras



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**?

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 dispositivos

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

b. 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.

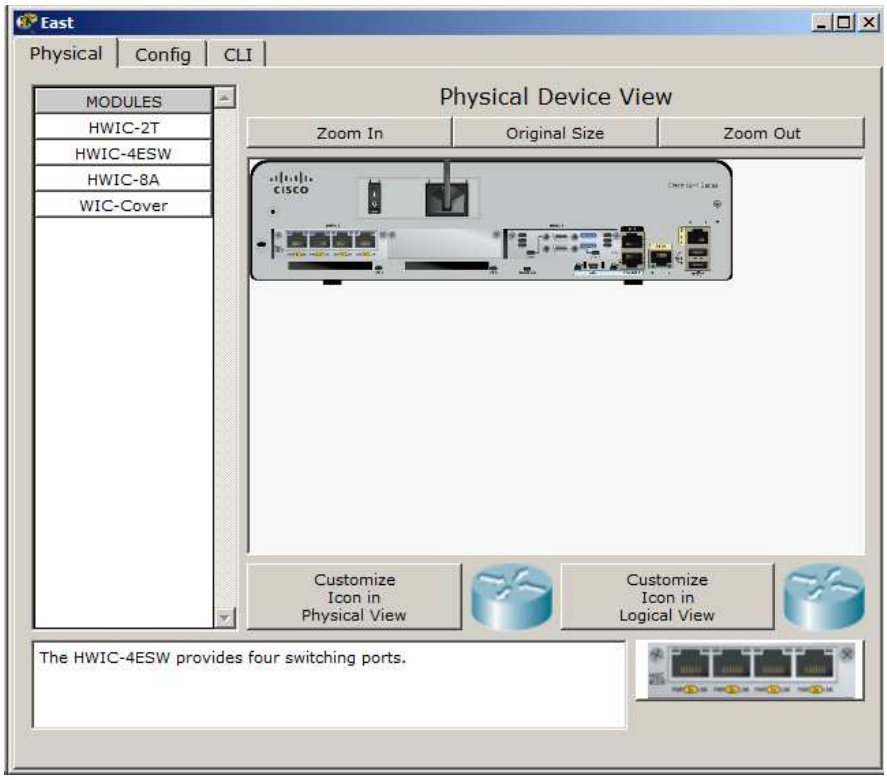
c. Mediante el mismo procedimiento, inserte los módulos correctos del paso 1b en la ranura vacía más alejada que se encuentra a la derecha en el **Switch2** y el **Switch3**.

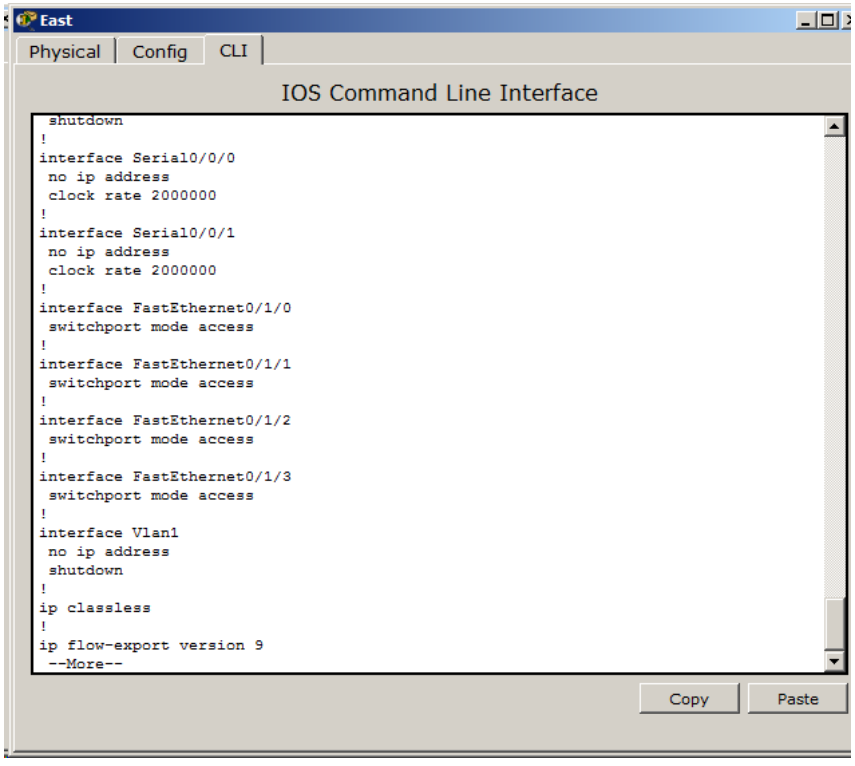
d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo.

¿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).

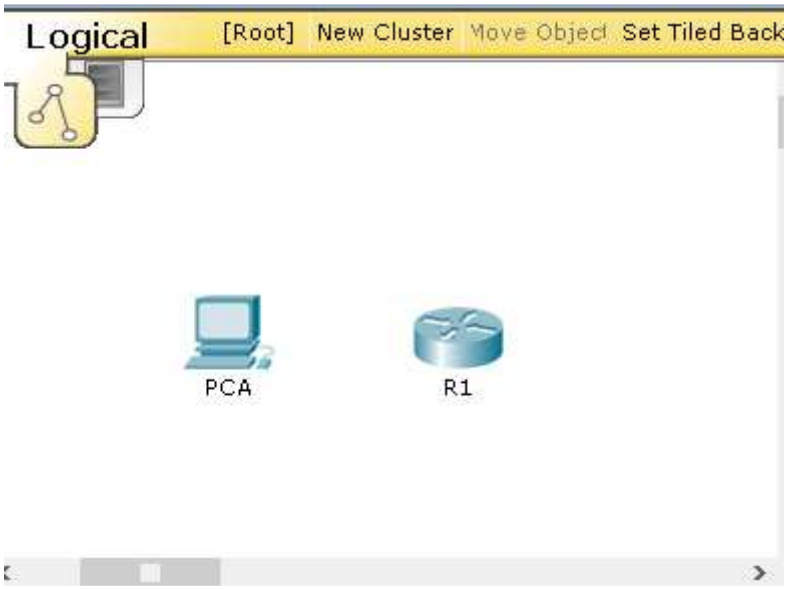
f. Use el comando adecuado para verificar que se hayan instalado las nuevas interfaces seriales.



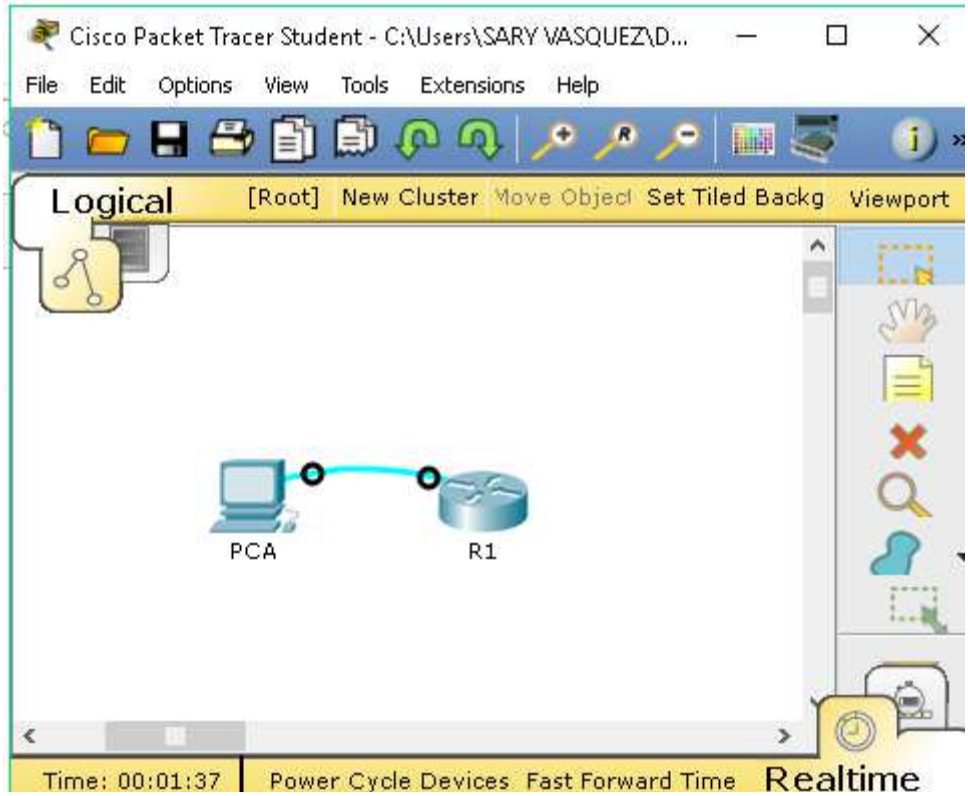


PRACTICA 6.4.1.2
Configuración inicial del Router

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.

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

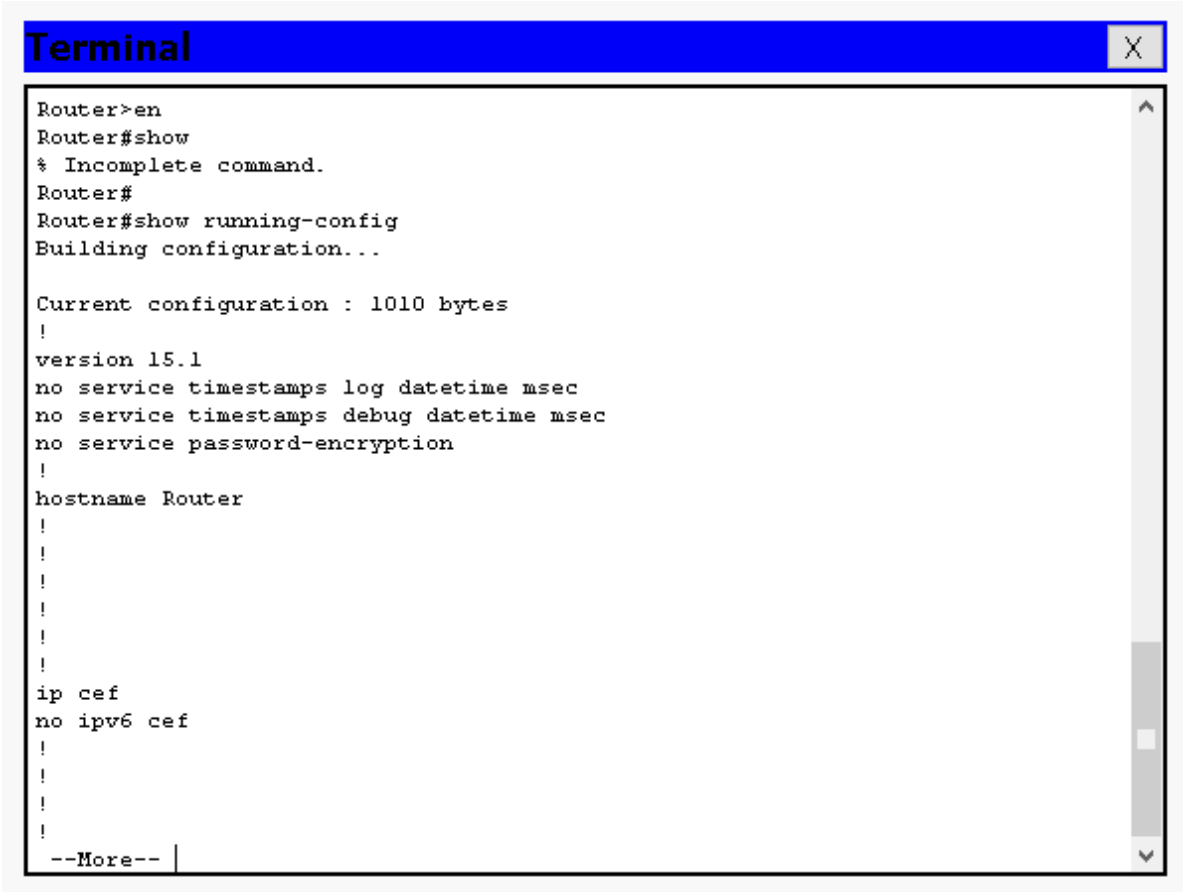
Router> enable

Router#

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

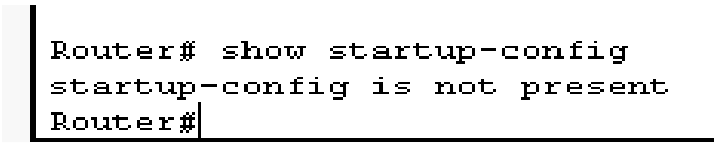
f. Introduzca el comando show running-config:

Router# show running-config



g. Responda las siguientes preguntas:
¿Cuál es el nombre de host del router? Router
¿Cuántas interfaces Fast Ethernet tiene el router? 4
¿Cuántas interfaces Gigabit Ethernet tiene el router? 2
¿Cuántas interfaces seriales tiene el router? 2
¿Cuál es el rango de valores que se muestra para las líneas vty? 0 - 4

h. 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? 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.

b. Establezca R1 como nombre de host.

```
Router# show startup-config
startup-config is not present
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

b. Utilice las siguientes contraseñas:
1) Consola: letmein
2) EXEC privilegiado, sin encriptar: cisco

```
Router# show startup-config
startup-config is not present
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable pas
% Incomplete command.
R1(config)#enable password cisco
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

3) EXEC privilegiado, encriptado: itsasecret

```
R1#en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret itsasecret
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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).

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd *Unauthorized access is strictly prohibited.*
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Nota: la actividad se configura con una expresión normal para que solo se detecte la palabra “access” en el comando banner motd del alumno.

Paso 2: Verificar los parámetros iniciales de R1

e. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza? show running-config

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

R1 con0 is now available
Press RETURN to get started.

g. Presione Entrar; debería ver el siguiente mensaje:

Unauthorized access is strictly prohibited.
User Access Verification
Password:

```
Press RETURN to get started!

Unauthorized access is strictly prohibited.

User Access Verification

Password: |
```

¿Por qué todos los routers deben tener un mensaje del día (MOTD)?
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?
R1(config-line)# login

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

```
 Unauthorized access is strictly prohibited

User Access Verification

Password:

R1>en
Password:
Password:
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

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

c. 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? copy running-config startup-config
   ¿Cuál es la versión más corta e inequívoca de este comando? copy r s
   ¿Qué comando muestra el contenido de la NVRAM? show startup-configuration or show start
d. 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.

d. Examine el contenido de la memoria flash mediante el comando show flash:
R1# show 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
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

¿Cuántos archivos hay almacenados actualmente en la memoria flash?
3
¿Cuál de estos archivos cree que es la imagen de IOS? c1900-universalk9- mz.SPA.151-4.M4.bin
¿Por qué cree que este archivo es la imagen de IOS? 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.

e. 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]
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.
f. 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
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


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

1177 bytes copied in 0.416 secs (2829 bytes/sec)
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
  4   1177     startup-config
[33848764 bytes used, 221895236 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


R1#
```

PRACTICA 6.4.3.3

Packet Tracer: Conexión de un router a una red LAN

Topología

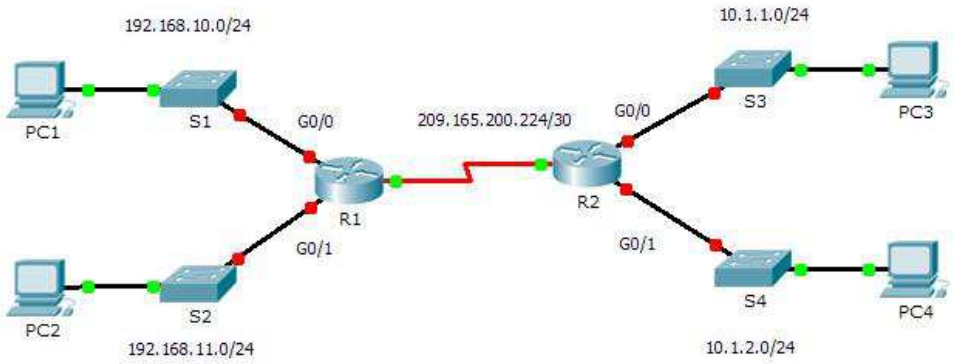


Tabla de direccionamiento

Dispositiv	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminad

o				o
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 (DCE)	209.165.200.225	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	192.168.11.10	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

Objetivos

Parte 1: Mostrar la información del router

Paso 2: Configurar las interfaces del router

Paso 3: Verificar la configuración

Información básica

En esta actividad, utilizará diversos comandos **show** para mostrar el estado actual del router. Después utilizará la Tabla de direccionamiento para configurar las interfaces Ethernet del router. Finalmente, utilizará comandos para verificar y probar las configuraciones.

Nota: los routers en esta actividad están parcialmente configurados. Algunas de las configuraciones no se incluyen en este curso, pero se proporcionan para ayudarlo a utilizar los comandos de verificación.

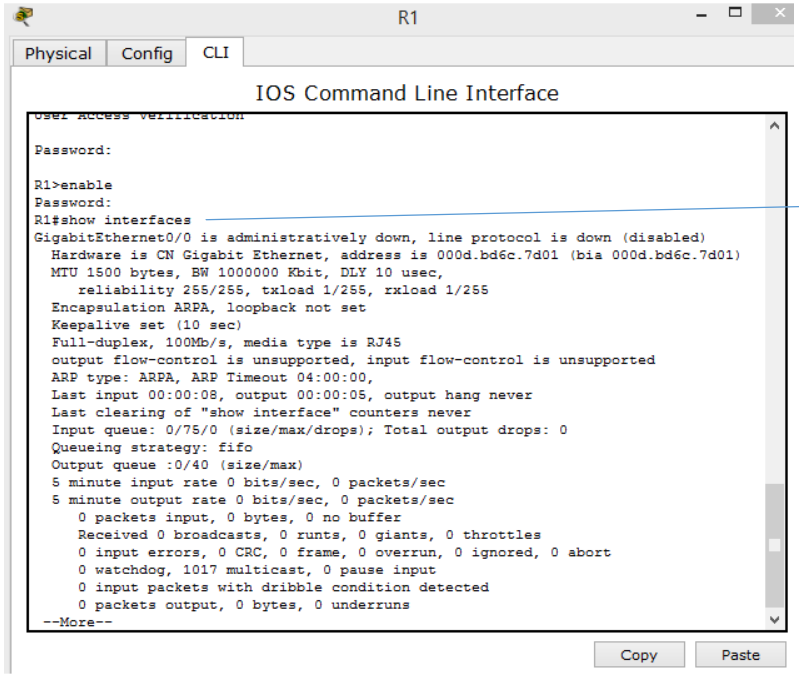
Parte 1: Mostrar la información del router

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**.

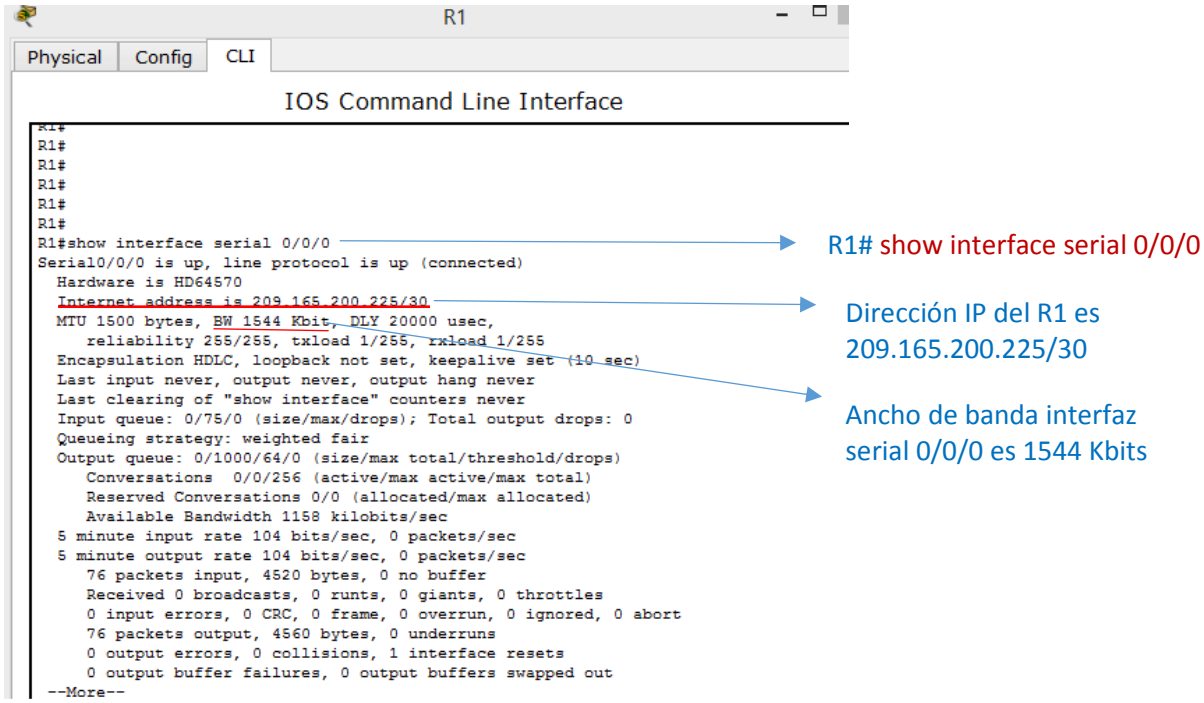
b. ¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router?

show interfaces



h. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0?

show interface serial 0/0/0

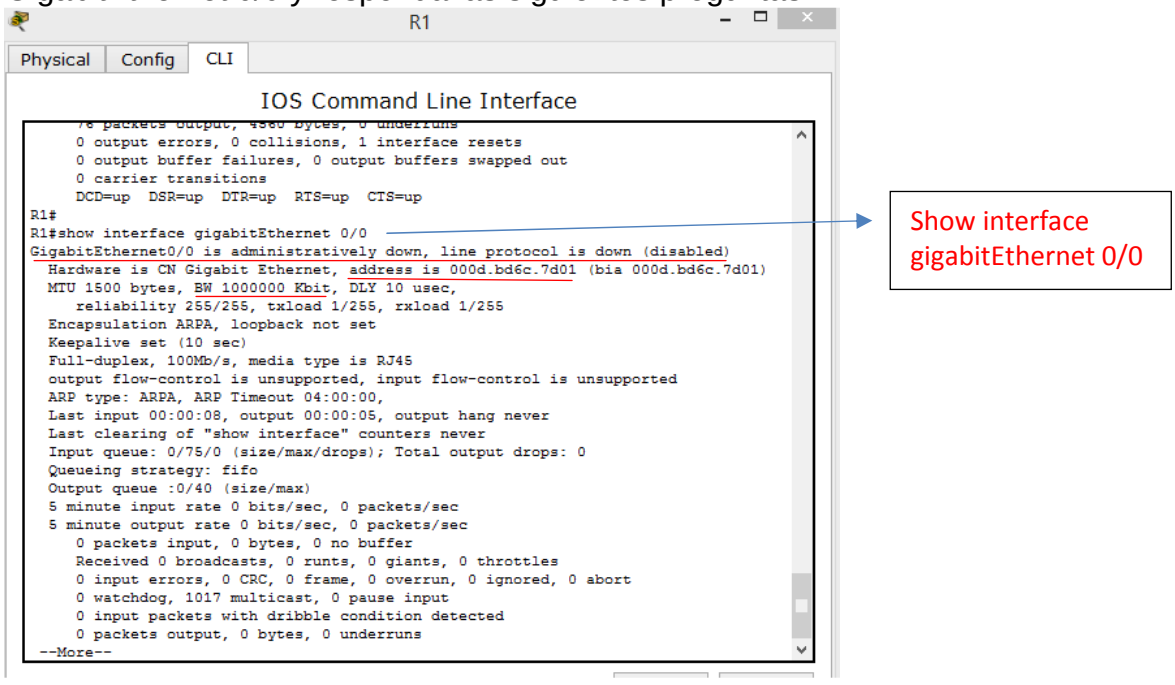


i. Introduzca el comando para visualizar las estadísticas de la interfaz Serial 0/0/0 en el R1 y responda las siguientes preguntas:

   a. ¿Cuál es la dirección IP configurada en el **R1**?
   209.165.200.225/30

   b. ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0? 1544 kbits

j. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:



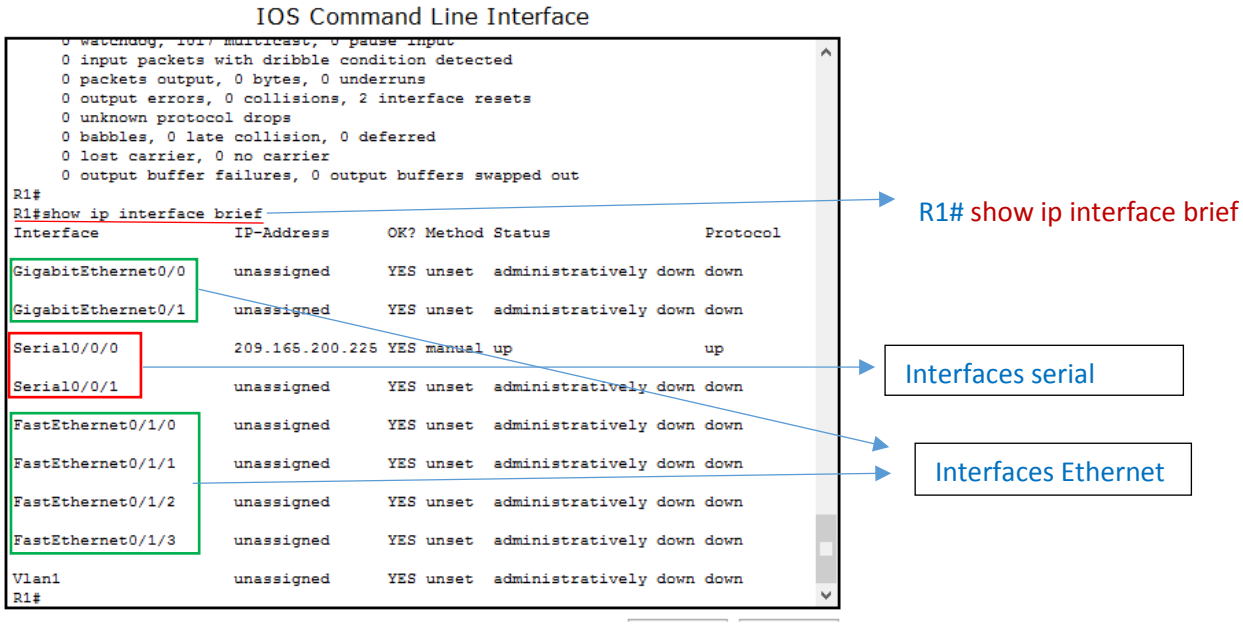
a. ¿Cuál es la dirección IP en el **R1**? No hay una dirección IP configurada en la interfaz GigabitEthernet 0/0.

b. ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0? 000d.bd6c.7d01

c. ¿Cuál es el ancho de banda en la interfaz GigabitEthernet 0/0? 1 000 000 kbits

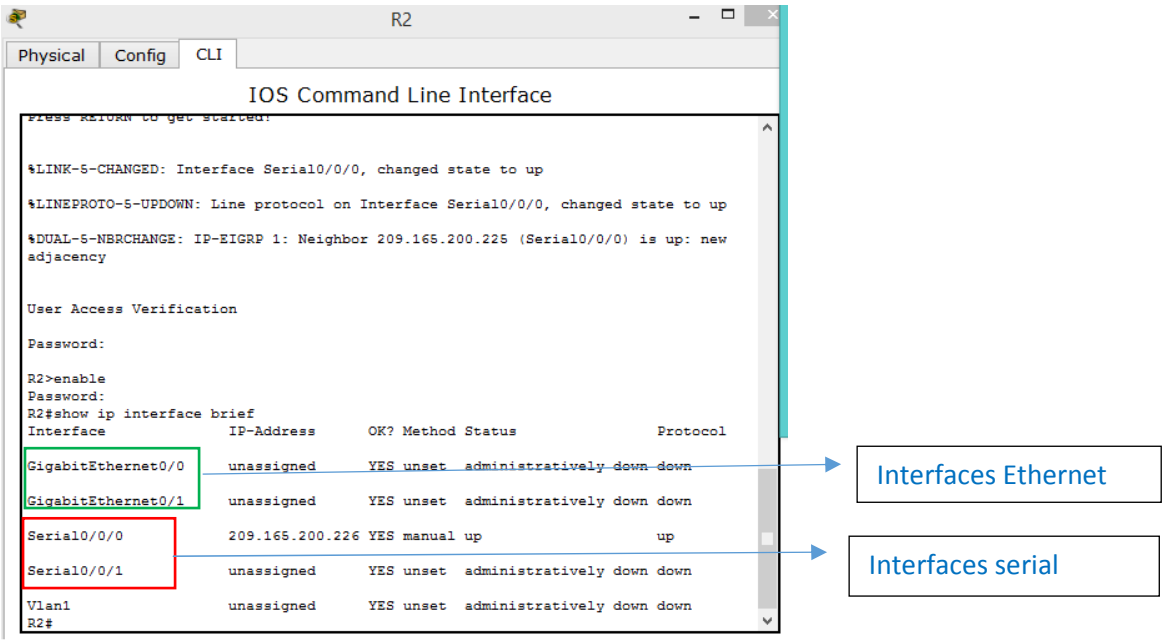
Paso 2: Mostrar una lista de resumen de las interfaces en el R1

a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas? show ip interface brief



b. Introduzca el comando en cada router y responda las siguientes preguntas:

¿Cuántas interfaces seriales hay en **R1** y **R2**? Cada router tiene 2 interfaces seriales.



¿Cuántas interfaces Ethernet hay en **R1** y **R2**? R1 tiene seis interfaces Ethernet y R2 tiene dos interfaces Ethernet.

¿Son iguales todas las interfaces Ethernet en el **R1**? Si no es así, explique las diferencias. No lo son. Hay dos interfaces Gigabit Ethernet y cuatro interfaces Fast Ethernet. Las interfaces Gigabit Ethernet admiten velocidades de hasta 1 000 000 000 bits, y las interfaces Fast Ethernet admiten velocidades de hasta 1 000 000 bits.

Paso 3: Mostrar la tabla de enrutamiento en el R1

1. ¿Qué comando muestra el contenido de la tabla de enrutamiento? show ip route

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

2. Introduzca el comando en el **R1** y responda las siguientes preguntas:

a. ¿Cuántas rutas conectadas hay (utilizan el código C)? 1

b. ¿Qué ruta se indica? 209.165.200.224/30

3. ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento? Un router solo envía paquetes a redes

indicadas en la tabla de enrutamiento. Si una red no aparece en la lista, el paquete se descarta.

Parte 2: Configurar las interfaces del router

Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1

a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitet
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R1(config-if)#exit
R1(config)#
```

b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.

R1(config-if)# **description LAN connection to S1**

```
R1(config-if)#exit
R1(config)#interf
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#description LAN connection to S1
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

c. Ahora, el **R1** debe poder hacer ping a la PC1.

R1(config-if)# **end**
%SYS-5-CONFIG_I: Configured from console by
console R1# **ping 192.168.10.10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

```
R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/5/15 ms

R1#
```

Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

a. Utilice la información en la Addressing Table para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:

4. Introduzca la dirección IP y active la interfaz.

5. Configure una descripción apropiada.

6. Verifique las configuraciones de las interfaces.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config-if)#exit
R1(config)#int
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip address 10.1.1.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

R2(config-if)#
```

```
R2(config-if)#exit
R2(config)#in
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#ip address 10.1.2.1
% Incomplete command.
R2(config-if)#ip address 10.1.2.1. 255.255.255.0
                                  ^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 10.1.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

R2(config-if)#
```

```
R2(config-if)#exit
R2(config)#in
R2(config)#interface s
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#description LAN connection to S3
R2(config-if)#exit
R2(config)#interface g
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#description LAN connection to S4
R2(config-if)#exit
R2(config)#
```

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? copy run start

Parte 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.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         192.168.11.1    YES manual up                    up
Serial0/0/0                209.165.200.225 YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
FastEthernet0/1/0          unassigned      YES unset  administratively down down
FastEthernet0/1/1          unassigned      YES unset  administratively down down
FastEthernet0/1/2          unassigned      YES unset  administratively down down
FastEthernet0/1/3          unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
R1#
```

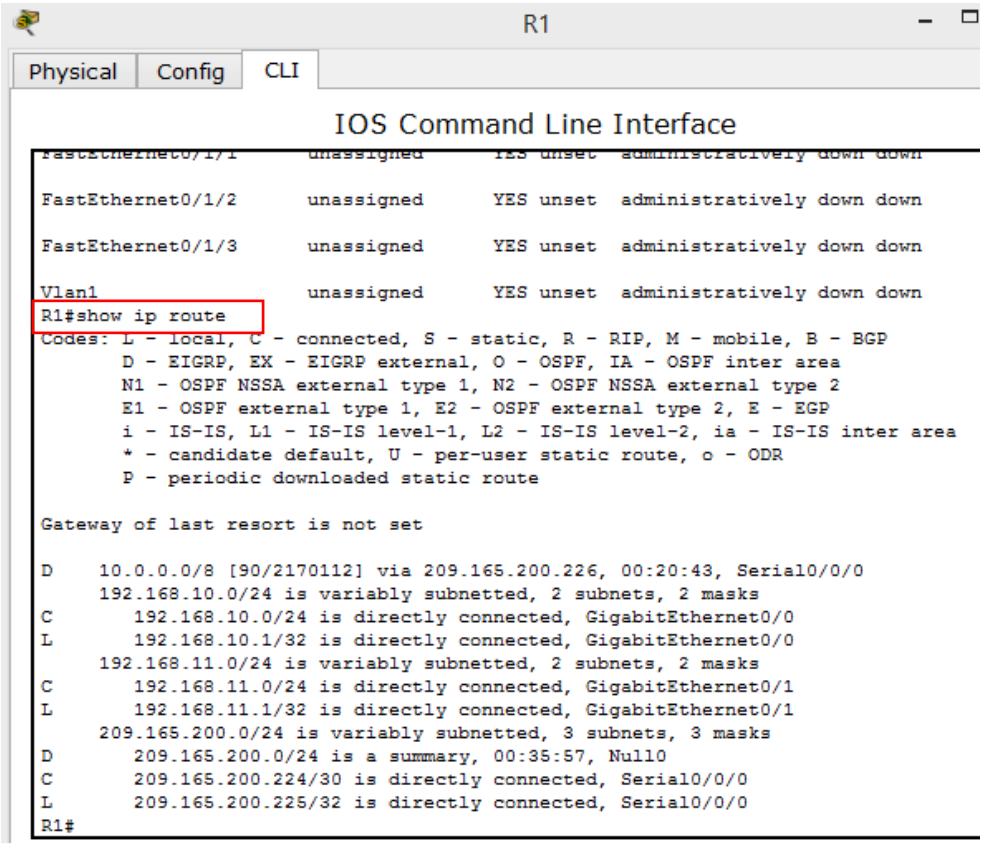
```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.1.1.1        YES manual up                    up
GigabitEthernet0/1         10.1.2.1        YES manual up                    up
Serial0/0/0                209.165.200.226 YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  administratively down down
R2#
```

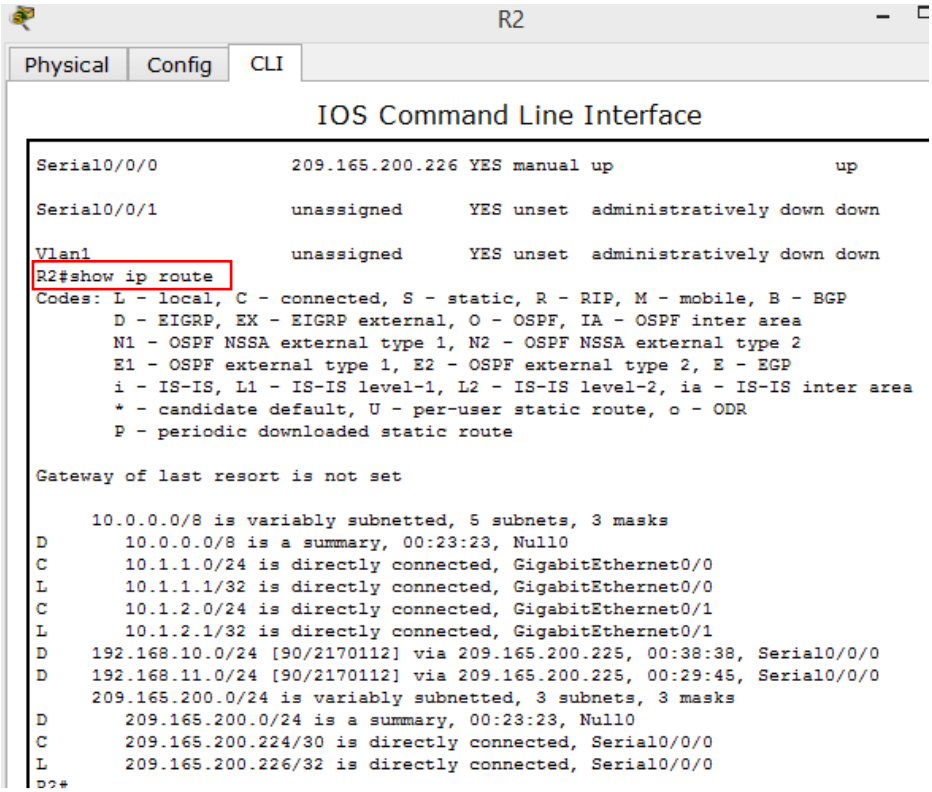
¿Cuántas interfaces en **R1** y **R2** están configuradas con direcciones IP y tienen el estado “up/up” (activa/activa)? Tres en cada router.

¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando? La máscara de subred

¿Qué comandos puede utilizar para verificar esta parte de la configuración?
show run, show interfaces, show ip protocols

b. 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? 3

¿Cuántas rutas EIGRP (utilizan el código **D**) ve en cada router? 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? 5

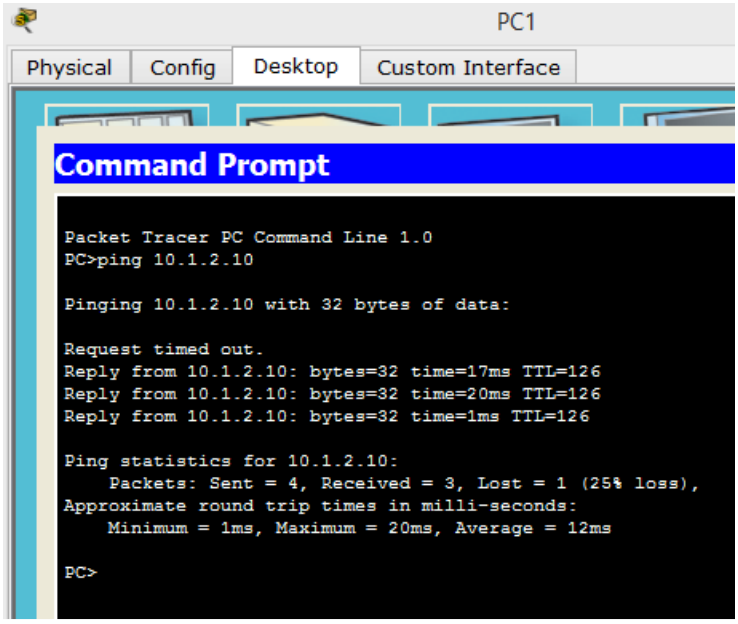
¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? sí

Nota: si su respuesta es “no”, falta una configuración necesaria. Revise los pasos de la parte 2.

Paso 2: Probar la conectividad de extremo a extremo a través de la red

Ahora debería poder hacer ping desde cualquier PC a cualquier otra PC en la red. Además, debería poder hacer ping a las interfaces activas de los routers. Por ejemplo, las siguientes pruebas deberían realizarse correctamente:

c. Desde la línea de comandos en la PC1, haga ping a la PC4.



d. Desde la línea de comandos en el R2, haga ping a la PC2.

```
R2#ping 192.168.11.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/13/18 ms

R2#
```

6.4.3.4: Packet Tracer: Resolución de problemas del gateway predeterminado

Topología

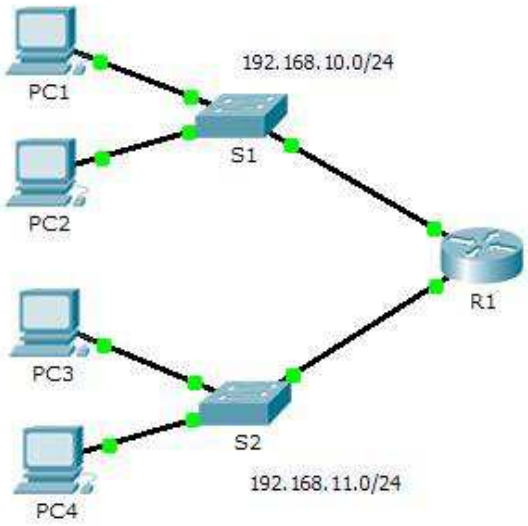


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara 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
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Objetivos

Parte 1: Verificar el registro de la red y descartar problemas

Parte 2: Implementar, verificar y documentar las soluciones

Información básica

Para que un dispositivo se comunique a través de varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se utiliza cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local a la que el host está conectado. En esta actividad, terminará de documentar la red. A continuación, verificará la documentación de la red mediante la puesta a prueba de la conectividad de extremo a extremo y la resolución de problemas. El método de resolución de problemas que utilizará consta de los siguientes pasos:

6. Verificar la documentación de la red y utilizar pruebas para descartar problemas.
7. Determinar cuál es la solución adecuada para un problema dado.
8. Implementar la solución.
9. Realizar pruebas para verificar que se haya resuelto el problema.
10. Documentar la solución.

A lo largo de sus estudios de CCNA, encontrará distintas descripciones del método de resolución de problemas, así como distintas formas de probar y documentar problemas y soluciones. Esto es intencional. No existe un estándar o una plantilla establecida para la resolución de problemas. Cada organización desarrolla procesos y estándares de documentación exclusivos (incluso si ese proceso consiste en no tener ninguno). No obstante, todas las metodologías de resolución de problemas eficaces generalmente incluyen los pasos anteriores.

> **Nota:** si usted es experto en la configuración de gateway predeterminado, es posible que esta actividad parezca más compleja de lo debido. Lo más probable es que pueda descubrir y solucionar todos los problemas de conectividad más rápido que si siguiera estos procedimientos. No obstante, a medida que avance con sus estudios, las redes y los problemas que encuentre serán cada vez más complejos. En tales situaciones, la única forma eficaz de descartar y resolver problemas es aplicar un enfoque metódico como el que se usa en esta actividad.

Parte 1: Verificar el registro de la red y descartar problemas

En la parte 1 de esta actividad, completará la documentación y realizará pruebas de conectividad para detectar problemas. Además, determinará la solución adecuada y la implementará en la parte 2.

Paso 1: Verificar el registro de la red y descartar cualquier problema

d. 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.

e. 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

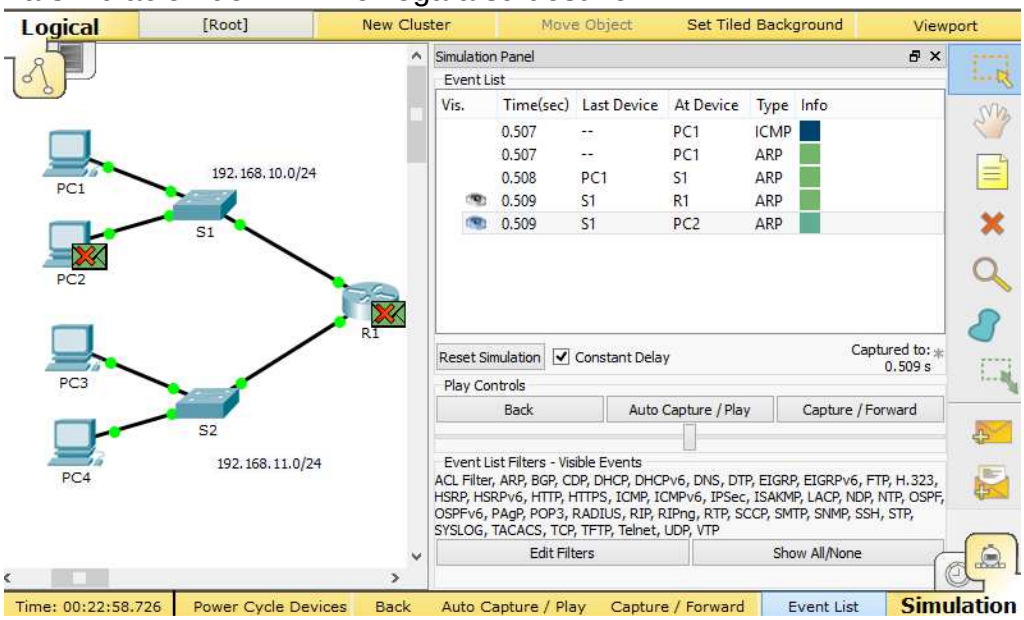
Prueba	¿Se realizó Correctamente?	Problemas	Solución	Verificado
PC1 a PC2	**No**	**Dirección IP en la PC1 está incorrecta**	**Cambiar la dirección IP de la PC1 a 192.168.10.10**	Si
PC1 a PC4	no	Se revisaron las configuraciones IP y se encontró que el PC4 tiene configurado un gateway predeterminado incorrecto	corregir el Gateway 192.168.1.1 por 192.168.11.1	Si
Configuración del S1	no	Se revisó la configuración con el comando Show running-config y se encontró que no tiene el Gateway configurado.	Realizar la configuración del Gateway con el comando ip default-gateway y la dirección 192.168.10.1	Si

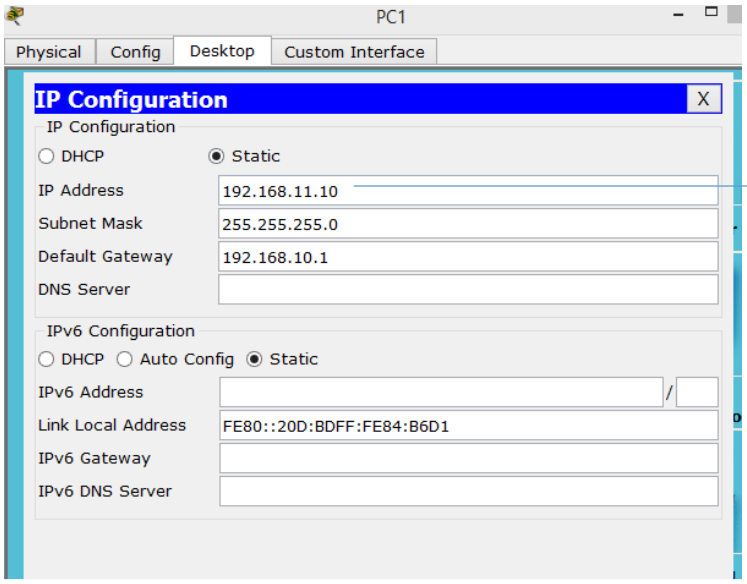
Configuración del S2	no	Se revisó la configuración con el comando show running config y se encontró que no tiene la dirección IP	Configurar la dirección IP del S2, según la tabla de direccionamiento	si

f. 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.

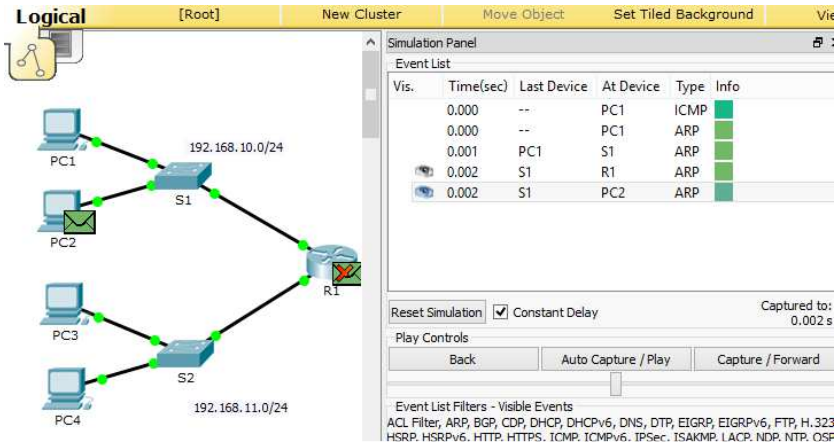
Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

Prueba PC1 a PC2:
La simulación del PDA no llega a su destino





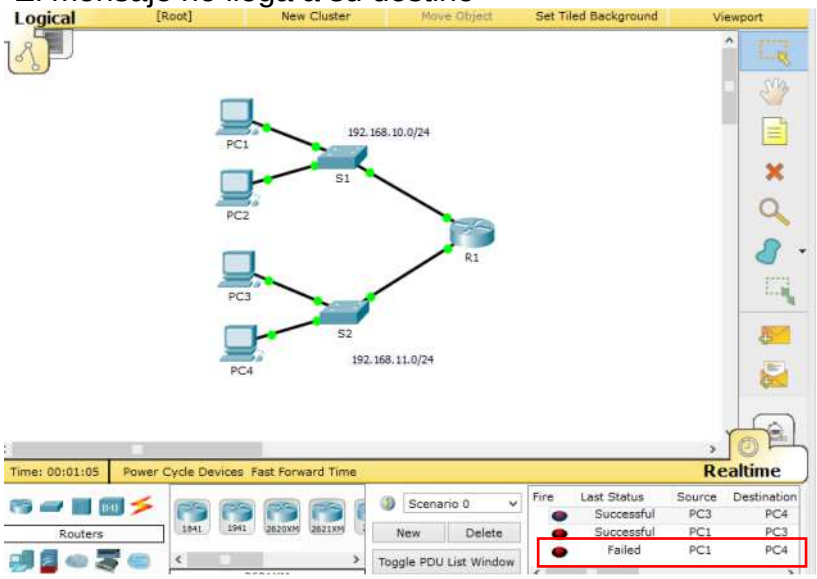
Se corrigió la dirección IP por 192.168.10.10

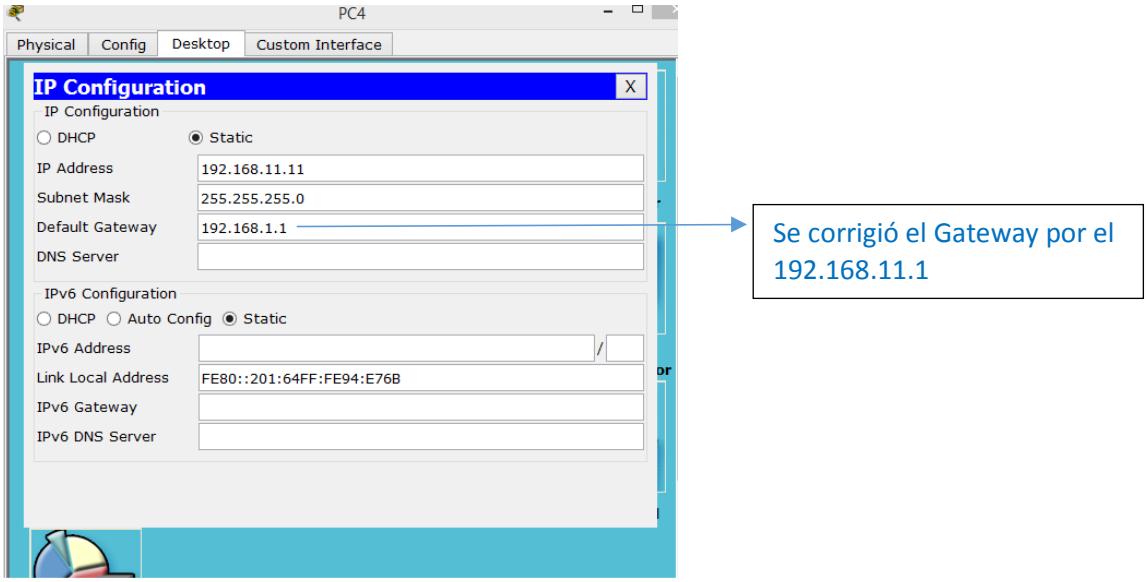


Simulación exitosa.

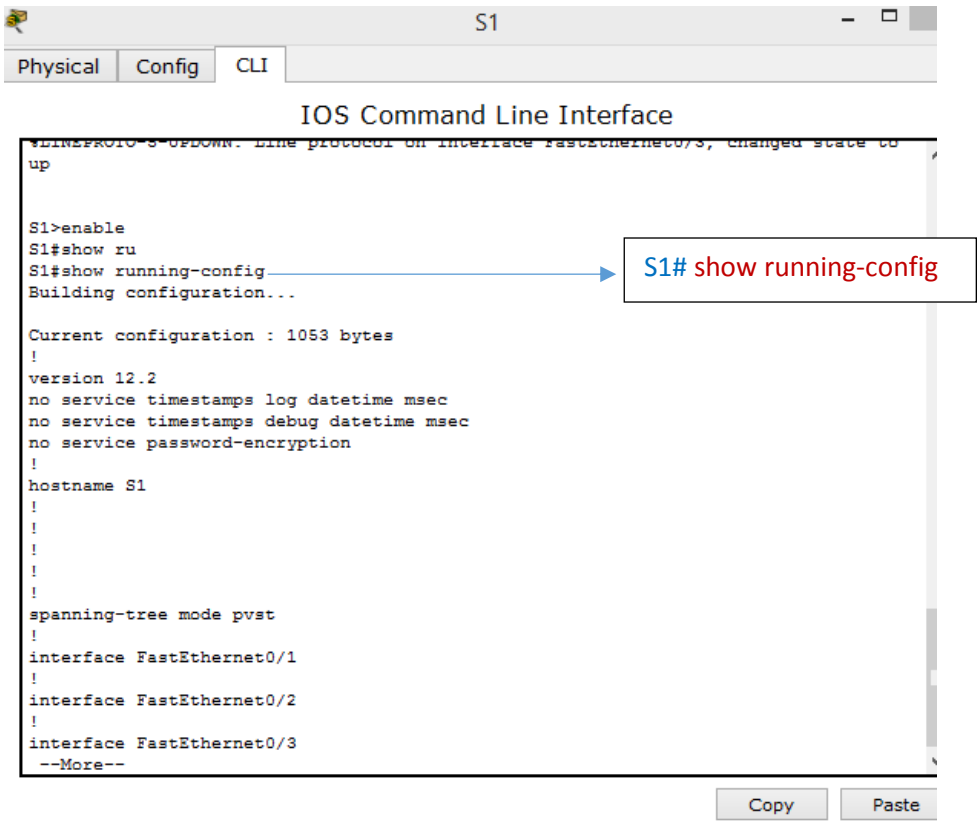
Prueba PC1 a PC4:

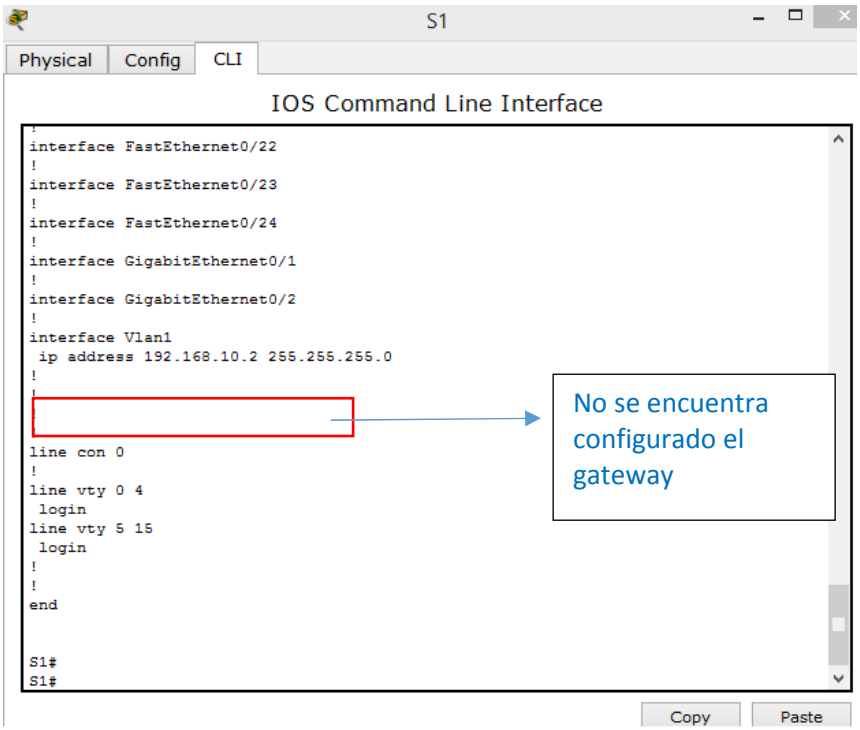
El mensaje no llega a su destino

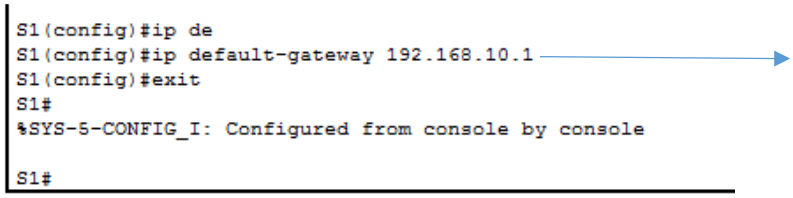




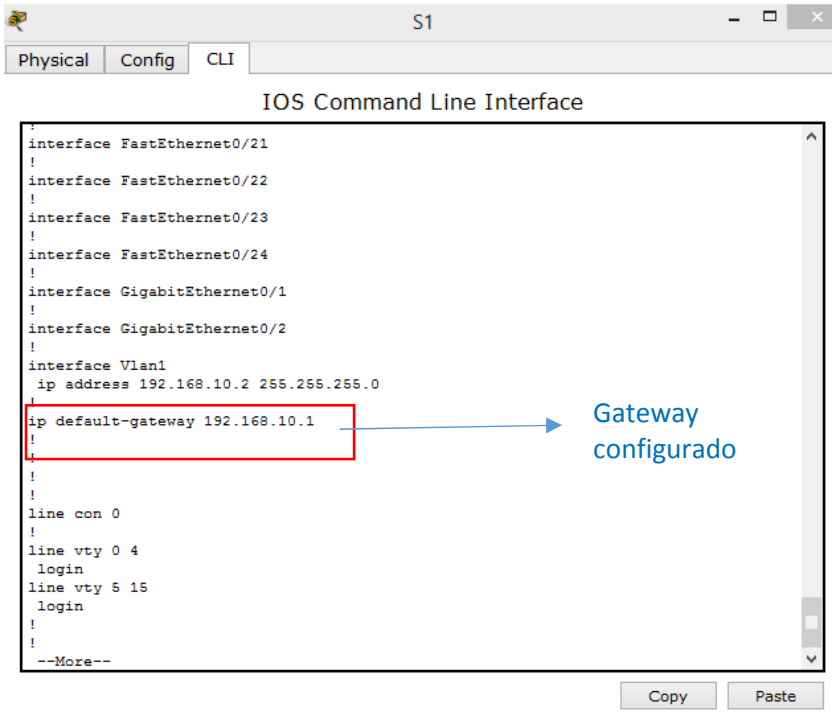
Prueba al dispositivo S1:



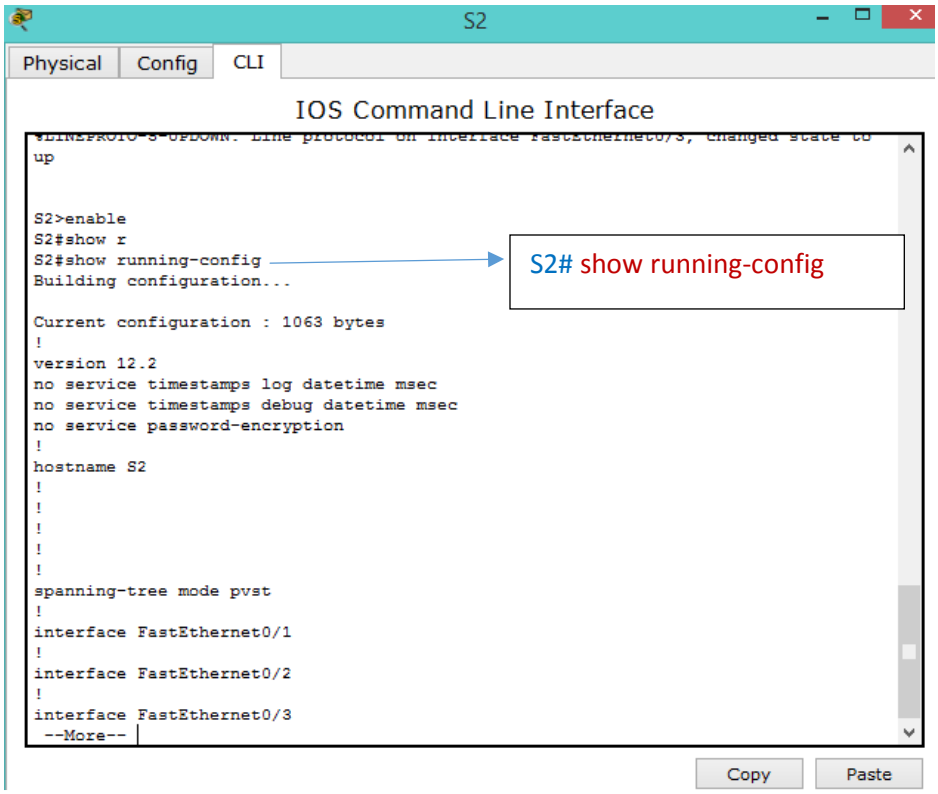


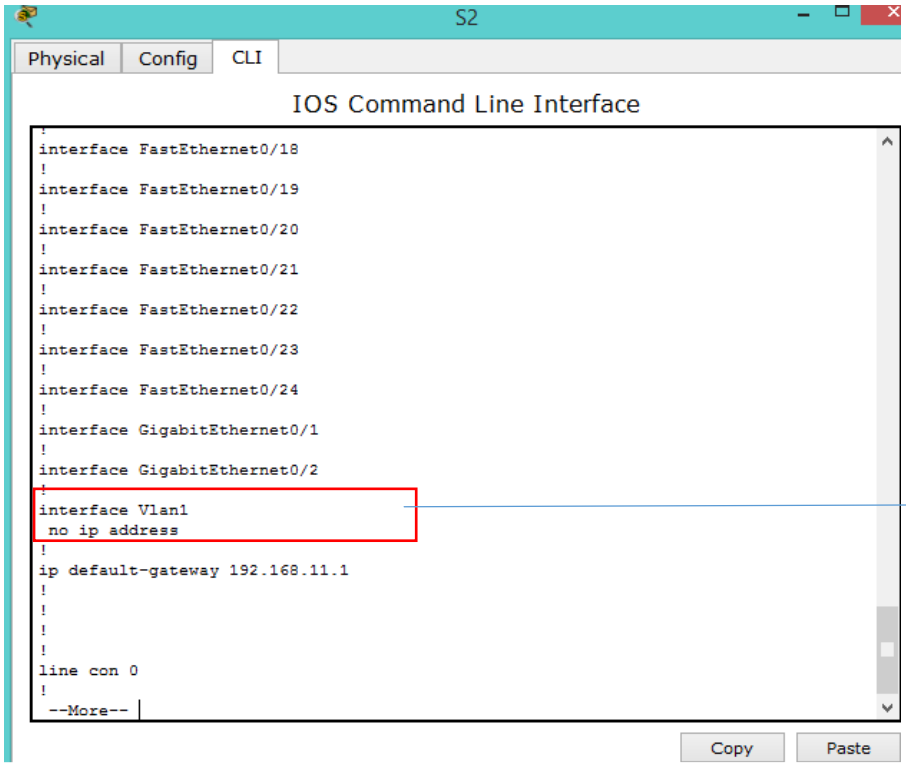


Se configura el Gateway con el comando.
S1(config)# Ip default-gateway 192.168.10.1

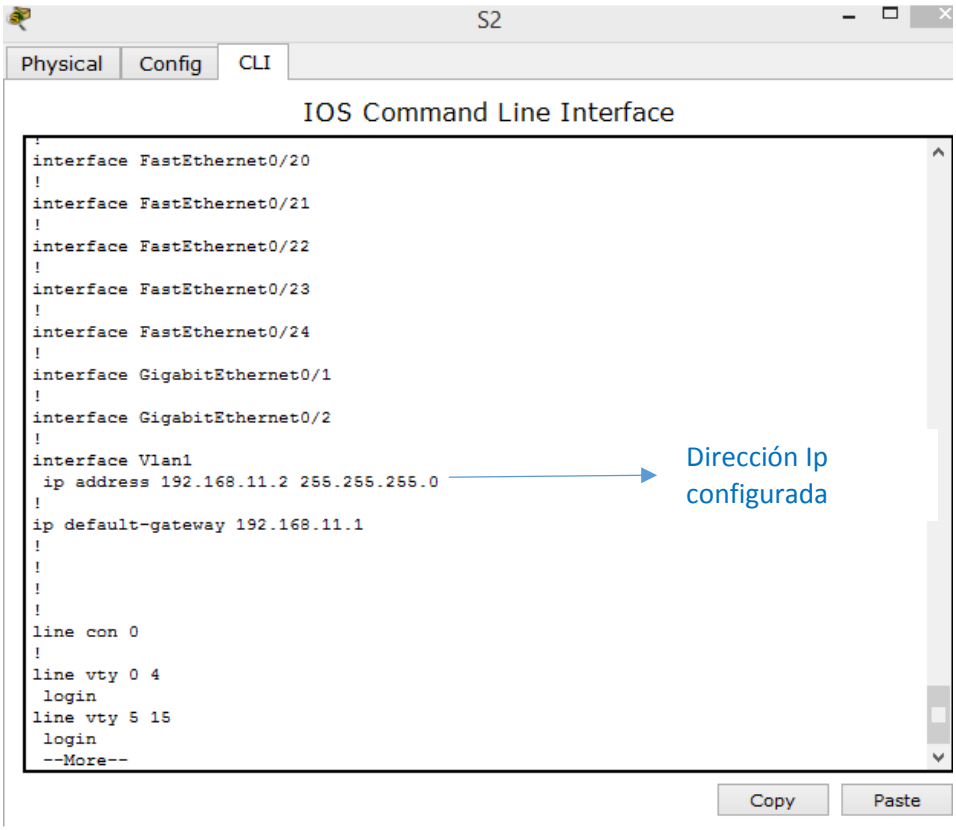


Prueba al dispositivo S2:

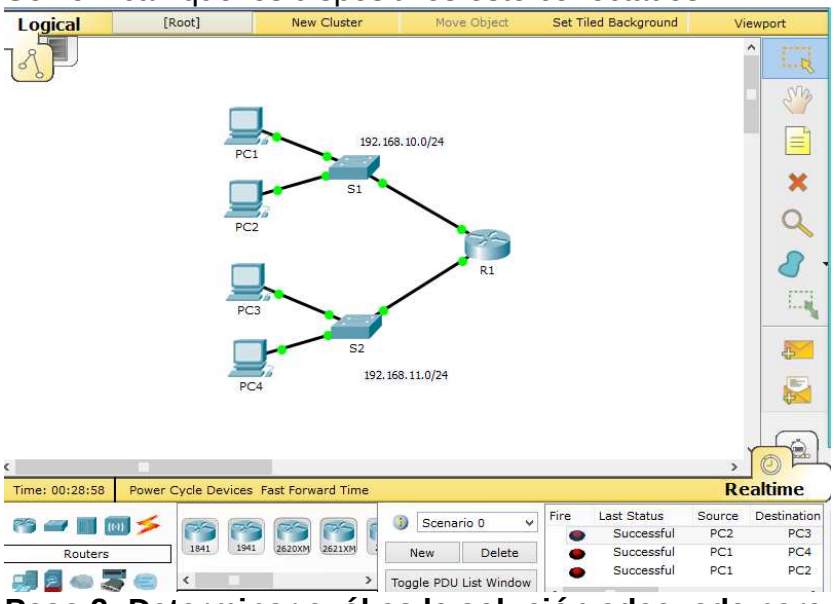

S2
Physical
Config
CLI
IOS Command Line Interface
up
S2>enable
S2#show r
S2#show running-config
Building configuration...
Current configuration : 1063 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
--More--
Copy
Paste
S2# show running-config


S2
Physical
Config
CLI
IOS Command Line Interface
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
!
ip default-gateway 192.168.11.1
!
!
!
!
line con 0
!
--More--
Copy
Paste
No se encuentra la dirección IP

```
S2(config)#interface Vlan 1
S2(config-if)#ip address 192.168.11.2 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```



Se verifican que los dispositivos este conectados



Paso 2: Determinar cuál es la solución adecuada para el problema

d. Con sus conocimientos sobre la forma en que operan las redes y sus aptitudes para configurar dispositivos, busque la causa del problema. Por ejemplo, el S1 no es la causa del problema de conectividad entre la PC1 y la PC2. Las luces de enlace son de color verde, y ninguna configuración en el S1 provocaría que no pase el tráfico entre la PC1 y la PC2. Por lo tanto, el problema debe de estar en la PC1, en la PC2 o en ambas.
e. verifique el direccionamiento del dispositivo para asegurarse de que coincida con el registro de la red. Por ejemplo, la dirección IP para la PC1 es incorrecta, como se verificó con el comando **ipconfig**.
f. Sugiera una solución con la que usted crea que se resolverá el problema y documéntela. Por ejemplo, cambiar la dirección IP de la PC1 para que coincida con la documentación.

Nota: por lo general, hay más de una solución. Sin embargo, una práctica recomendada de resolución de problemas es implementar de a una solución por vez. Implementar más de una solución podría presentar problemas adicionales en una situación más compleja.

Parte 2: Implementar, verificar y documentar las soluciones

En la parte 2 de esta actividad, implementará las soluciones que identificó en la parte 1. Luego, verificará si la solución funcionó. Es posible que deba volver a la parte 1 para terminar de descartar todos los problemas.

Paso 1: Implementar soluciones para abordar los problemas de conectividad

Consulte la documentación en la parte 1. Elija el primer problema e implemente la solución que sugirió. Por ejemplo, corrija la dirección IP en la PC1.

Paso 2: Verificar si ahora el problema está resuelto

c. Verifique si la solución que propuso solucionó el problema realizando la prueba que usó para identificarlo. Por ejemplo, ¿la PC1 puede ahora hacer ping a la PC2?

d. Si el problema se resolvió, indíquelo en la documentación. Por ejemplo, en la tabla anterior, con colocar una simple marca de verificación en la columna “Verificado” sería suficiente.

Paso 3: Verificar si se resolvieron todos los problemas

c. Si todavía tiene un problema pendiente con una solución que aún no se implementó, vuelva al paso 1 de la parte 2.

d. Si se solucionaron todos los problemas actuales, ¿también solucionó todos los problemas de conectividad remota (por ejemplo, que la PC1 pueda hacer ping a la PC4)? Si la respuesta es negativa, vuelva al paso 1c de la parte 1 para probar la conectividad remota.

Resultado de la actividad 6.4.3.4

PRACTICA 6.5.1.2
Packet Tracer: Reto de habilidades de integración

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
College	G0/0	172.14.5.1	255.255.255.0	No aplicable
	G0/1	172.14.10.1	255.255.255.0	No aplicable
Class-A	VLAN 1	172.14.5.35	255.255.255.0	172.14.5.1
Class-B	VLAN 1	172.14.10.35	255.255.255.0	172.14.10.1
Student-1	NIC	172.14.5.50	255.255.255.0	172.14.5.1
Student-2	NIC	172.14.5.60	255.255.255.0	172.14.5.1
Student-3	NIC	172.14.10.50	255.255.255.0	172.14.10.1
Student-4	NIC	172.14.10.60	255.255.255.0	172.14.10.1

Objetivos

- Terminar el registro de la red.
- Realizar la configuración básica de dispositivos en un router y un switch.
- Verificar la conectividad y resolver cualquier problema.

Situación

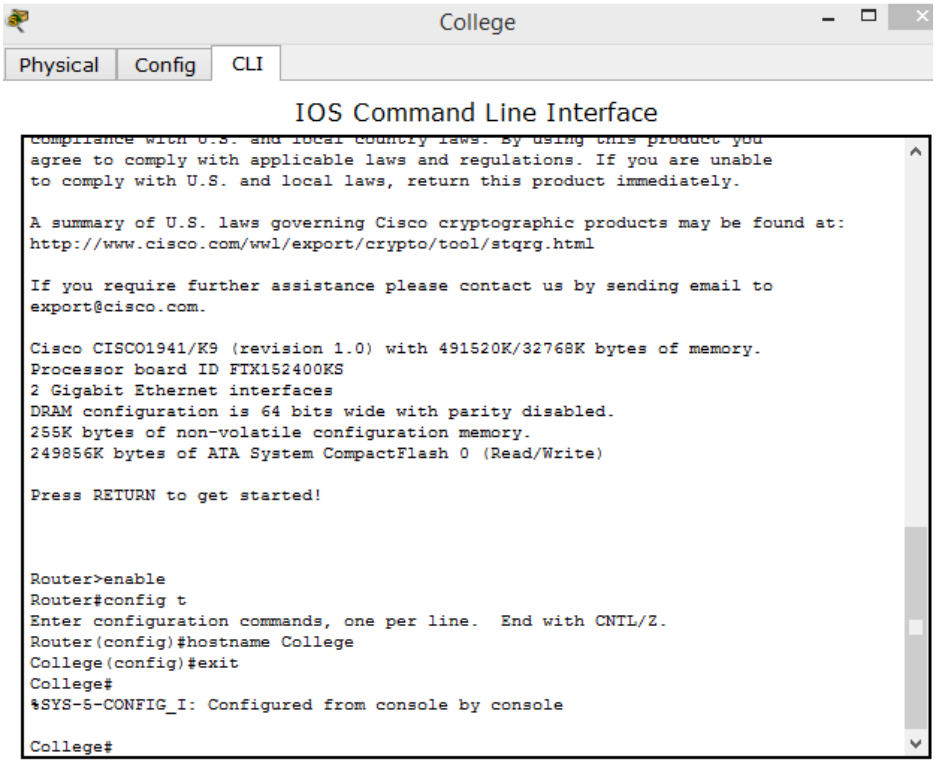
La administradora de la red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su

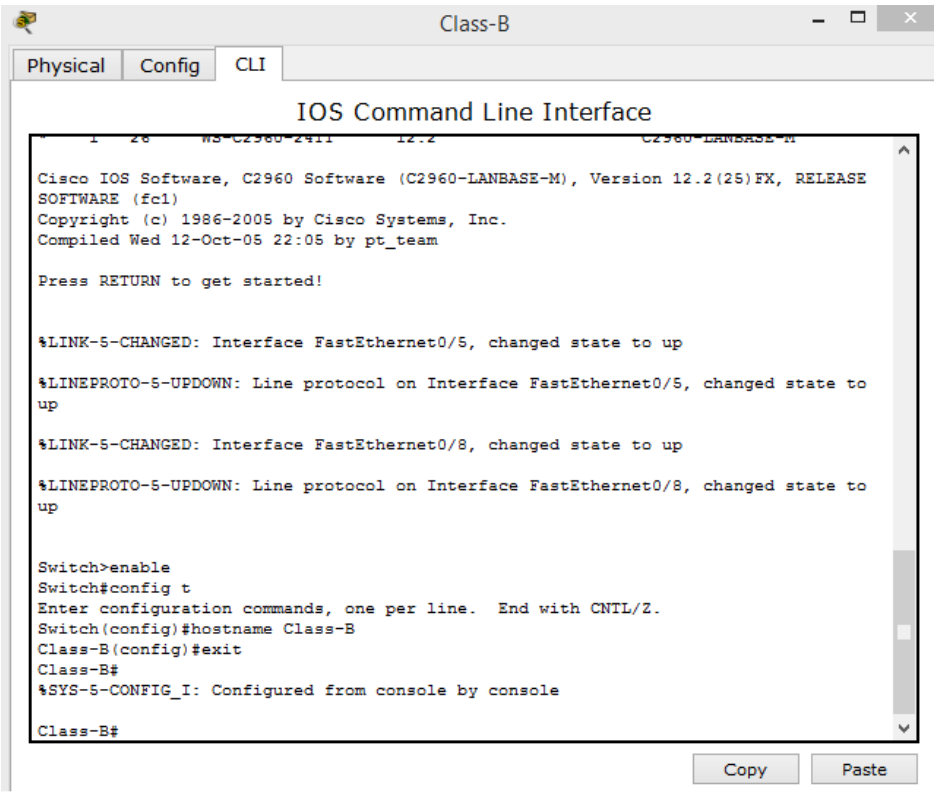
capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración básica de un router y un switch utilizando Cisco IOS. Luego, verificará la configuración realizada por usted, así como la configuración de los dispositivos existentes, probando la conectividad de extremo a extremo.

> **Nota:** después de completar esta actividad, puede elegir hacer clic en el botón **Reset Activity** (Restablecer actividad) para generar un nuevo conjunto de requisitos. Entre los aspectos variables se incluyen los nombres de dispositivo, los esquemas de direccionamiento IP y la topología.

Requisitos

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre **College** al router y **Class-B** al segundo switch. No podrá acceder a **Class-A.**





- Utilice **cisco** como contraseña de EXEC del usuario para todas las líneas.

```
College>enable
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#line console 0
College(config-line)#password cisco
College(config-line)#login
College(config-line)#line vty 0 4
College(config-line)#password cisco
College(config-line)#login
College(config-line)#exit
College(config)#
```

```
Class-B>enable
Class-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-B(config)#line console 0
Class-B(config-line)#password cisco
Class-B(config-line)#login
Class-B(config-line)#line vty 0 4
Class-B(config-line)#pa
Class-B(config-line)#password cisco
Class-B(config-line)#login
Class-B(config-line)#exit
Class-B(config)#
```

- Utilice **class** como contraseña de EXEC privilegiado.

```
College(config-line)#exit
College(config)#enable secret class
College(config)#exit
College#
%SYS-5-CONFIG_I: Configured from console by console

College#
```

```
Class-B(config-line)#exit
Class-B(config)#enable secret class
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#
```

- Encripte todas las contraseñas de texto no cifrado.

```
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#service password-
College(config)#service password-encryption
College(config)#banner motd "warnning"
College(config)#
```

Comando de encriptación de contraseñas

- Configure un aviso apropiado.

```
Class-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Class-B(config)#serv
Class-B(config)#service pass
Class-B(config)#service password-encryption
Class-B(config)#bann
Class-B(config)#banner motd "warnning"
Class-B(config)#
```

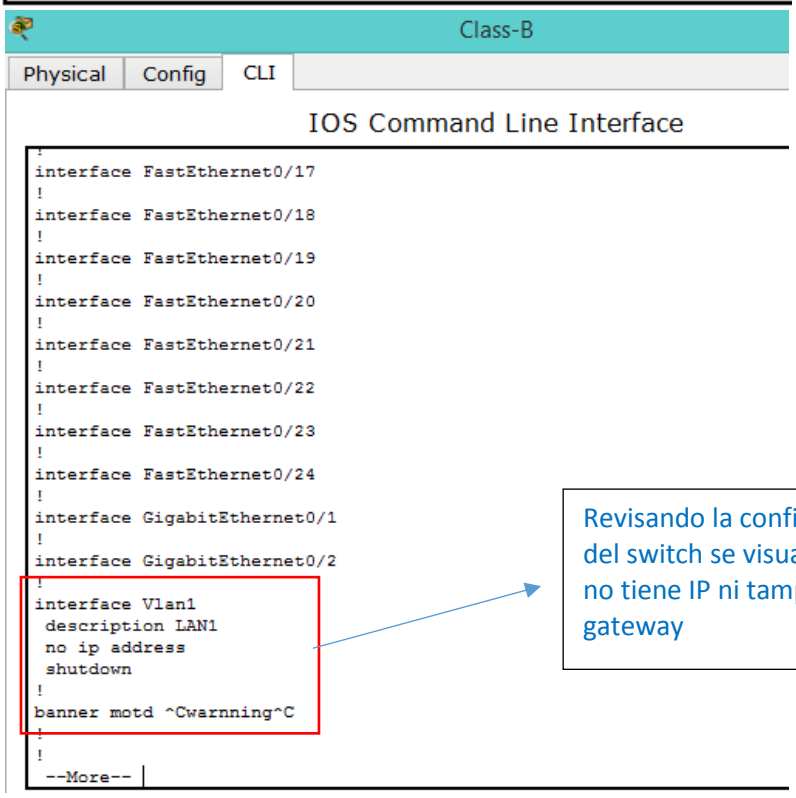
Mensaje MOTD

- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.

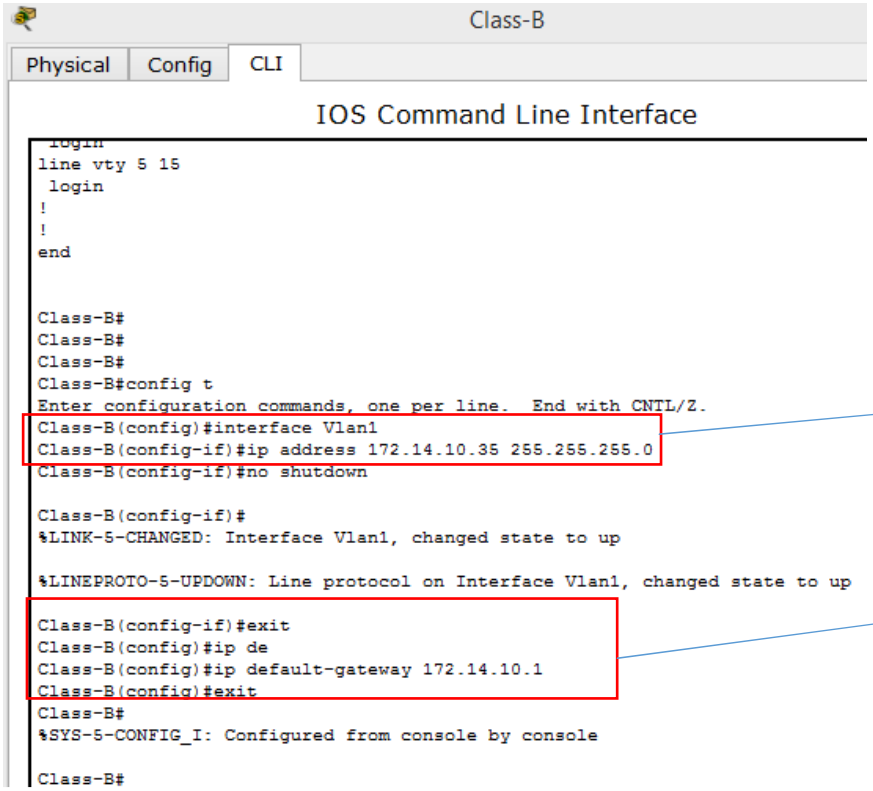
```
College#config t
Enter configuration commands, one per line.  End with CNTL/Z.
College(config)#interface G0/1
College(config-if)#ip addre
College(config-if)#ip address 172.14.10.1 255.255.255.0
College(config-if)#no shutdown

College(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up

College(config-if)#
```

- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **Class-B**.

```
Class-B(config)#interface Vlan 1
Class-B(config-if)#des
Class-B(config-if)#description LAN1
Class-B(config-if)#exit
Class-B(config)#exit
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#
```

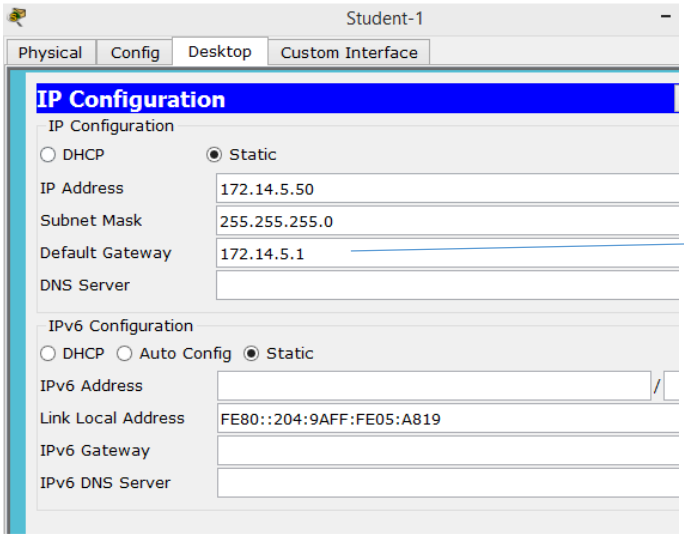


Revisando la configuración del switch se visualiza que no tiene IP ni tampoco gateway



Se configuro la dirección IP:
Ip address 172.14.10.35
255.255.255.0

Se asignó el Gateway al Switch: Class-B
Ip default-gateway
172.14.10.1

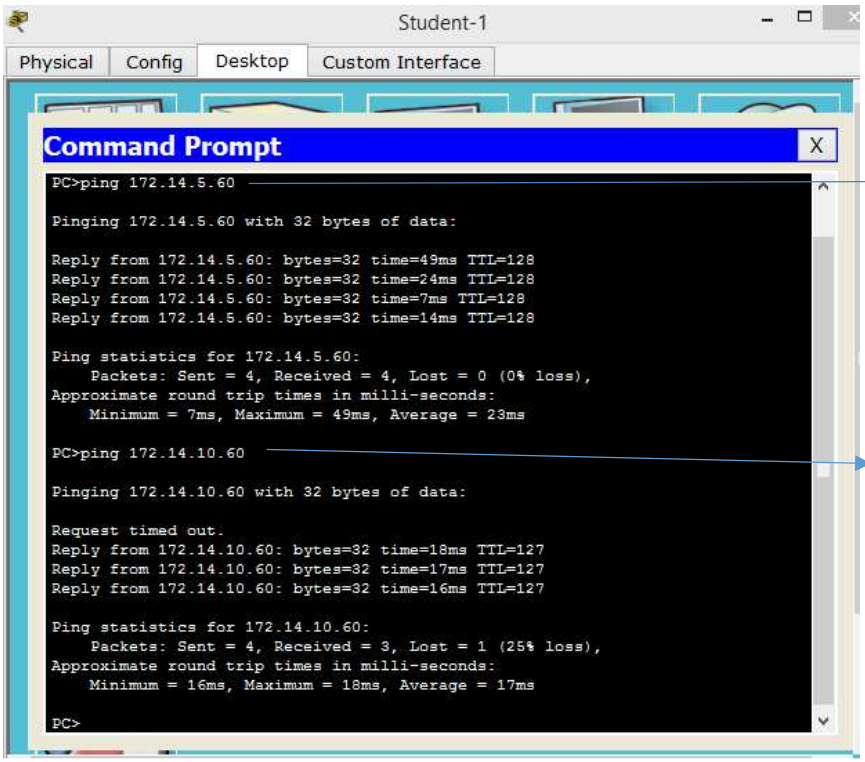


Se asignaron a cada uno de los PC los Gateway correspondiente

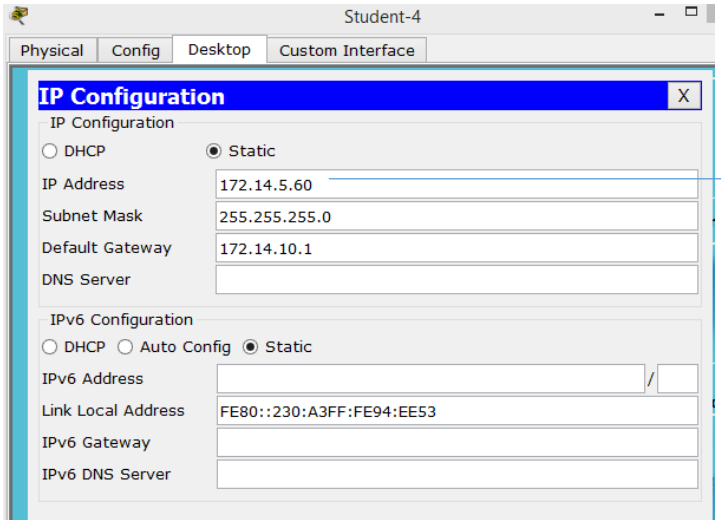
- Guarde las configuraciones.

```
Class-B#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
Class-B#
```

- 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 y Comentarios

Cisco ofrece una gran cantidad de dispositivos de internetworking, conocerlos y saber cómo interconectarlos es fundamental para hacer una correcta instalación de cualquier Red.
Y gracias a la posibilidad de agregar módulos a los dispositivos Cisco las posibilidades se incrementan pudiendo solventar casi cualquier situación problema que se presente.
Las indicaciones de la Guía fueron bastante claras, al inicio parece agobiante pero después de prácticas es bastante sencillo y se nota la facilidad de uso de los dispositivos modulares de Cisco.

Bibliografía.

Temática: Exploración de la red
CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

Temática: Configuración de un sistema operativo de red
CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

Temática: Protocolos y comunicaciones de red
CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

Temática: Acceso a la red
CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

Temática: Ethernet
CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

Temática: Capa de red
CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1