ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRESENTADO POR:

VIANNEY FAVIAN MARIÑO JULIO
ALBERTO DOMINGO CANTILLO
FAVIAN ALBERTO CAAMAÑO
IVAN DARIO CORREA
JOHAN LEONEL ALTAMIRANDA VALERA

GRUPO COLABORATIVO: 203092A_1

TUTOR:
NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
COLOMBIA
SEPTIEMBRE 2017

INTRODUCCIÓN

Durante la realización de esta actividad, se da solución al paso 1 mediante una actividad colaborativa en donde aprendimos la importancia, características, implementación de las redes para él envío de paquetes así como su configuración básica identificando fallas para lograr un conocimiento que nos permita profundizar y ponernos a la vanguardia del que proponen las redes en la actualidad y nuestro entorno profesional.

Hablar de un mundo interconectado en este siglo hace referencia al poder hacer uso de las tecnologías de información para transmitir al menos en lo que respecta a la tierra mensajes que pueden verse gracias a la velocidad de la luz prácticamente al instante en otro lugar remoto de la tierra independientemente de los aspectos de nivel sobre mar o región latitudinal. El modo y técnica para lograrlo se debe al uso de equipos interconectados que funcionan por medio del modelo OSI, a su vez en forma de capas desde las que se cuentan visible para nosotros la capa física (switch y router principalmente) y las demás seis capas que la conforman y entendibles para quienes trabajan en la manipulación, configuración, instalación y/o mantenimiento de dichos equipos pero a nivel de enlace de datos, de red, de trasporte, sesión, presentación y aplicación; por medio de protocolos, estándares de calidad en la formulación de software especializado para el control y trasmisión y contando con el grado de formación técnica que amerita dicho campo tanto desde la ingeniería de telecomunicaciones, de Sistemas y electrónica. Comprendiendo así, que el mundo intercomunicado en el cual nos hallamos es producto de la intervención constante de personas que tras lo dicho comprenden en estudio la dinámica de las redes de comunicaciones, es que se plasma este primer trabajo practico el cual abre las puertas a una serie de cuatro trabajos símiles en busca de la formación adecuada de los dispositivos utilizados en la composición de dichas redes de interconexión.

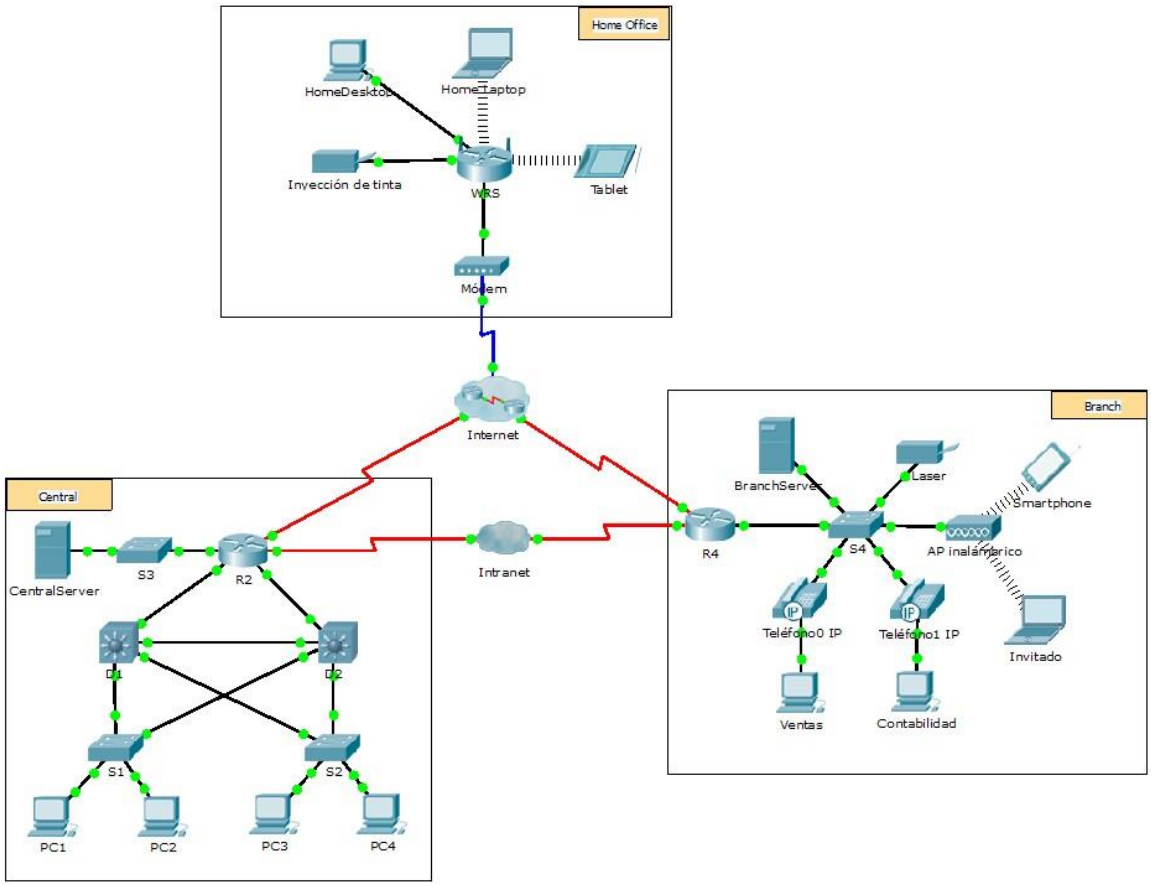
De este modo el siguiente trabajo expone evidencia correspondiente a las temáticas iniciales que abren las puertas a conceptos de redes, configuración de equipos a través del software packet tracer, tomando como referencia una serie de pasos en sentido creciente apuntando a la consolidación de saberes propios relacionados al mundo de las redes de telecomunicaciones. Aquí púes se exponen 16 ejercicios de formación en los temas de cableado, puertos de conexión, dispositivos centrados en el switch y el router, describiendo en la medida de su desarrollo comandos y resultados esperados para cada una de las actividades propuestas en la guía de trabajo del Diplomado de profundización en CISCO (Redes LAN y WAN). Conforme a ello se realizan la conexión de una PCs a un switches mediante consola, verificando su configuración predeterminada y acceso al modo privilegiado, estableciendo los nombres del host y las direcciones IP entre switches , donde un dispositivo se comunica a través de varias redes, utilizando una dirección IP, mascara de subred y un Gateway (puerta de enlace) para enviar un paquete a un dispositivo en otra red, finalizando este informe con la configuración del router el cual tiene como función en la red de direccionar adecuadamente la información que procede de esta y/o validar la que proceda de redes externas.

Por parte del equipo de trabajo que presenta este trabajo no resta sino invitar a que la revisión de este sea conforme a los requerimientos solicitados previamente y que responda a los criterios formadores de CISCO, tanto a nivel de competencias como de apropiación de conceptos y contenidos estudiados para esta unidad número uno del diplomado; muchas gracias y bienvenido.

LABORATORIOS	ESTUDIANTE
1.2.4.4 Packet Tracer - Representing the Network Instructions IG.pdf	IVAN CORREA
2.1.4.8 Packet Tracer - Navigating the IOS Instructions IG.pdf	JOHAN LEONEL ALTAMIRANDA VALERA
2.2.3.3 Packet Tracer - Configuring Initial Switch Settings Instructions IG.pdf	VIANNEY FAVIAN MARIÑO
2.3.2.5 Packet Tracer - Implementing Basic Connectivity	VIANNEY FAVIAN MARIÑO
2.4.1.2 Packet Tracer - Skills Integration Challenge	JOHAN LEONEL ALTAMIRANDA VALERA
3.2.4.6 Packet Tracer - Investigating the TCP-IP and OSI Models in Action	FAVIAN ALBERTO CAAMAÑO
3.3.3.3 Packet Tracer - Explore a Network	JOHAN LEONEL ALTAMIRANDA VALERA
4.2.4.5 Packet Tracer - Connecting a Wired and Wireless LAN	IVAN CORREA
5.1.4.4 Packet Tracer - Identify MAC and IP Addresses	FAVIAN ALBERTO CAAMAÑO
5.2.1.7 Packet Tracer - Examine the ARP Table	JOHAN LEONEL ALTAMIRANDA VALERA
5.3.3.5 Packet Tracer - Configure Layer 3 Switches	VIANNEY FAVIAN MARIÑO
6.3.1.10 Packet Tracer - Exploring Internetworking Devices	FAVIAN ALBERTO CAAMAÑO
6.4.1.2 Packet Tracer - Configure Initial Router Settings	IVAN CORREA
6.4.3.3 Packet Tracer - Connect a Router to a LAN	JOHAN LEONEL ALTAMIRANDA VALERA
6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues	VIANNEY FAVIAN MARIÑO
6.5.1.2 Packet Tracer Skills Integration Challenge	IVAN CORREA

1.2.4.4 Packet Tracer - Representing the Network Instructions IG

Topología



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

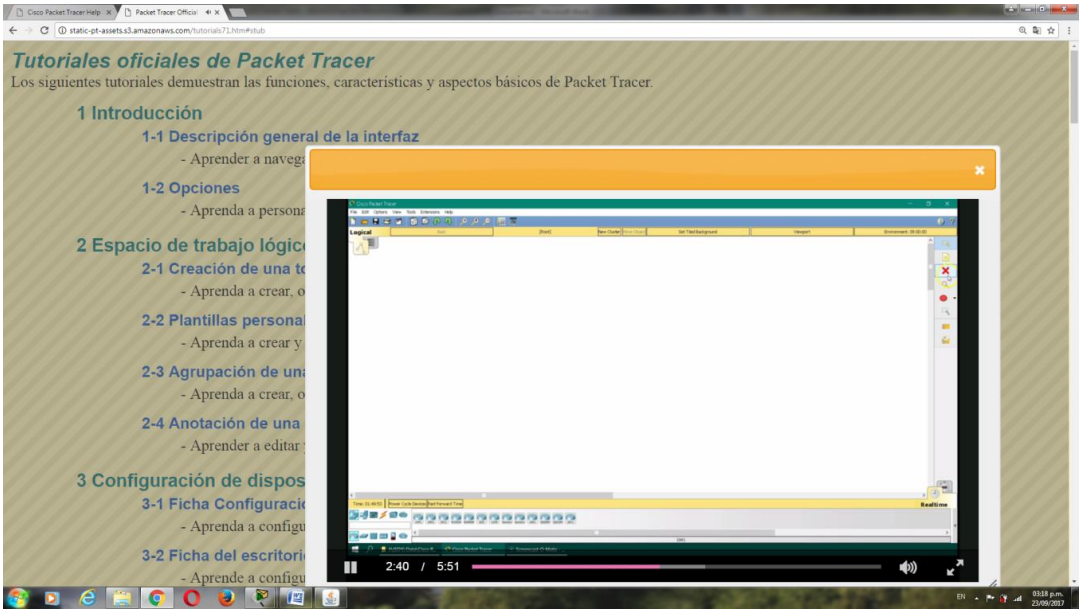
a. Acceda a las páginas de ayuda de Packet Tracer de dos maneras:

1) Haga clic en el ícono de signo de interrogación que está en la esquina superior derecha de la barra de herramientas del menú.

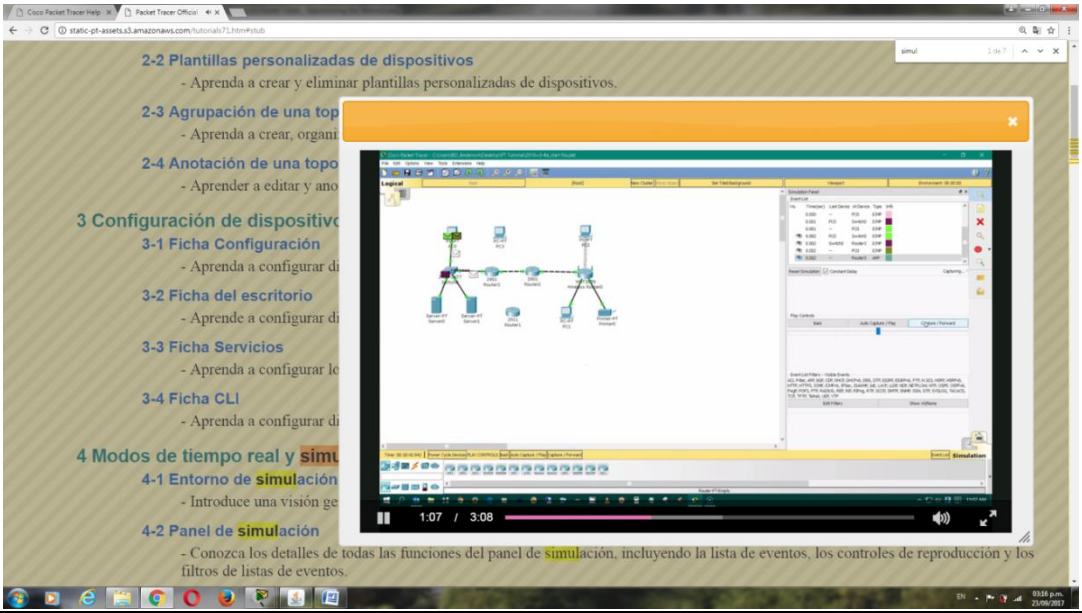
2) Haga clic en el menú Help (Ayuda) y, a continuación, seleccione Contents (Contenido).

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)?

Se puede seleccionar entre las opciones DHCP o Static y en esta ultima realizar la configuración de la dirección IP.

También en la opción Static se puede configurar la máscara de subred, el Gateway y el DNS.

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

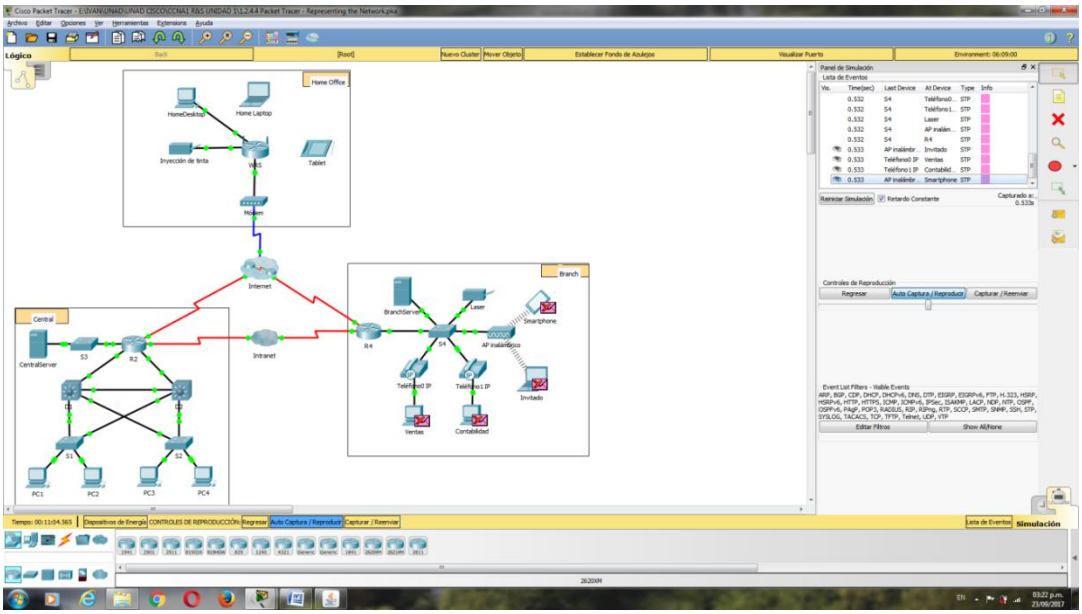
a. Busque la palabra Realtime (Tiempo real) en la esquina inferior derecha de la interfaz de Packet Tracer. En el modo de tiempo real, la red siempre funciona como una red real, ya sea que trabaje en la red o no. La configuración se realiza en tiempo real, y la red responde prácticamente en tiempo real.

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.

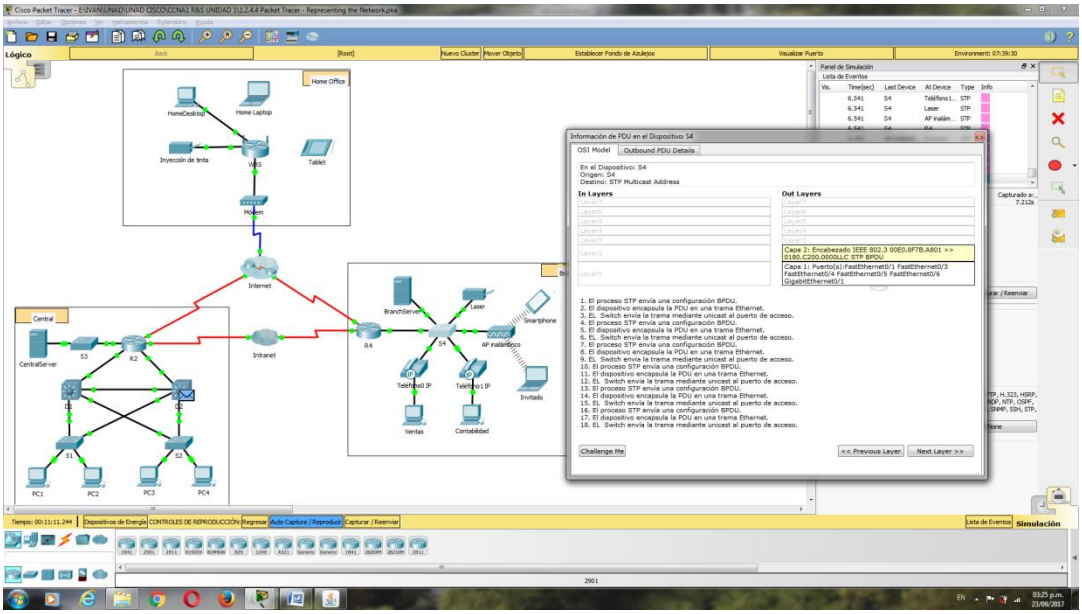
e. Haga clic en Capture / Forward (Capturar/avanzar) para avanzar en la simulación. Haga clic en este botón algunas veces más para ver el efecto.



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:

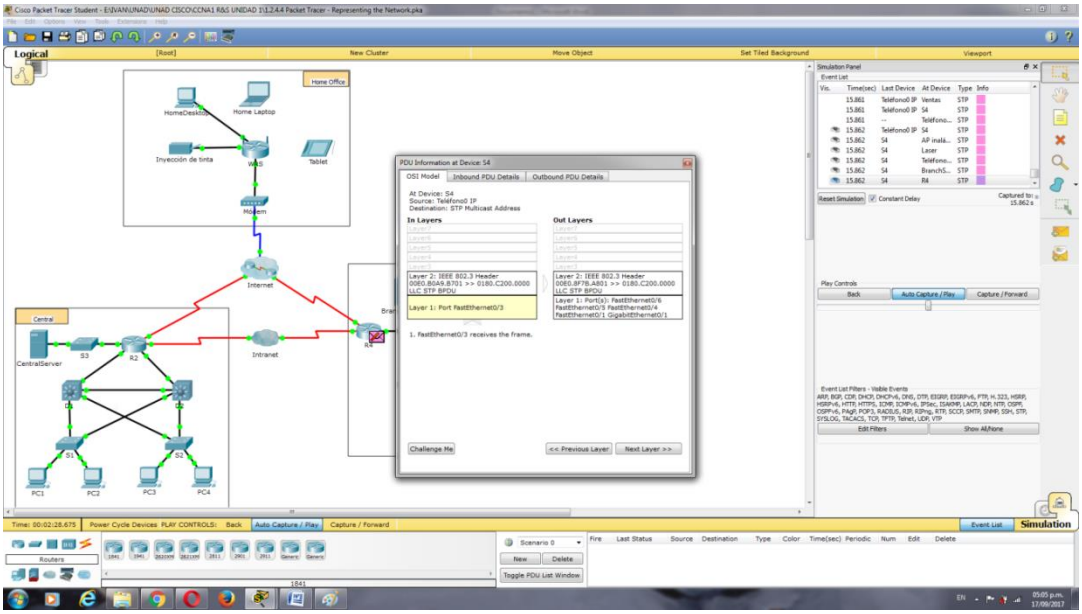
- En la ficha OSI Model (Modelo OSI), ¿cuántas In Layers (Capas de entrada) y Out Layers (Capas de salida) tienen información?

Se tiene información de las capas 1 y 2.



- 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?

  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?

  No se identifica cambios.

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

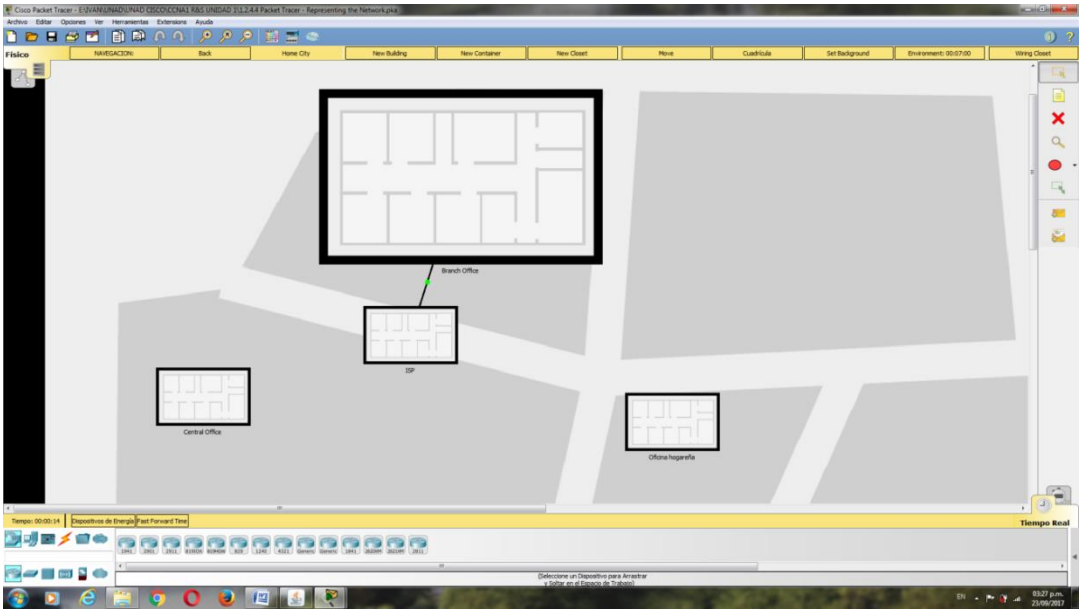
a. Busque la palabra Logical (Lógico) en la esquina superior izquierda de la interfaz de Packet Tracer. Actualmente se encuentra en el área de trabajo Logical, donde pasará la mayor parte del tiempo de creación, configuración, investigación y resolución de problemas de redes.

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.

Switch, router, hubs, dispositivos inalámbricos, emulación 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)?
Hay 13.

d. Sin contar las dos nubes, ¿cuántos íconos de la topología representan dispositivos intermediarios (varias conexiones conducen a ellos)?
Hay 11.

e. ¿Cuántos de esos dispositivos intermediarios son routers? Nota: el dispositivo Linksys es un router.
Hay 5.

f. ¿Cuántos dispositivos finales no son computadoras de escritorio?
Son 8.

g. ¿Cuántos tipos diferentes de conexiones de medios se utilizan en esta topología de red?
Se utilizan 4.

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.

Porque no se realizan de manera física.

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

En el mundo real las computadoras tanto portátiles como de escritorio si pueden funcionar como servidores, el cliente utiliza los recursos de otra máquina, el servidor es el que brinda servicios y recursos.

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.
Enrutar, dar conectividad, brindar seguridad.

Paso 3: Comparar redes LAN y WAN

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

Una LAN es la unión de varios equipos dentro de una misma red con un alcance mínimo, se utilizan para compartir archivos y recursos. Ejemplo de un red LAN es una oficina, una casa o redes pequeñas que no requieren de muchos recursos.

Una red WAN o red amplia, se puede decir que es la red de redes, esta se puede extender a nivel mundial. Un ejemplo de esta es el Internet.

b. ¿Cuántas WAN ve en la red de Packet Tracer? Se logran identificar dos, Internet e Intranet.

c. ¿Cuántas LAN ve? 3 LAN.

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 es la red de redes, es el sistema de comunicación mas usado y de mayor beneficio a nivel mundial, tiene la capacidad de brindar entretenimiento, de comunicarnos, de enseñar y dar trabajo.
Es el invento con mayor utilidad de la historia y aun está en proceso de expansión teniendo en cuenta los grandes beneficios que ofrece actualmente.

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

f. ¿Cuáles son algunas de las formas más comunes que utilizan las empresas para conectarse a Internet en su área?
DSL, cable, satelital, conexión móvil (MiFi).

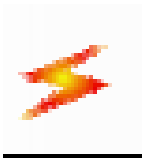
2.1.4.8 Packet Tracer - Navigating the IOS Instructions IG
Packet Tracer: Navegación de IOS

Objetivos
Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda
Parte 2: Exploración de los modos EXEC
Parte 3: Configuración del comando clock

Información básica
En esta actividad, practicará las habilidades necesarias para navegar Cisco IOS, incluidos distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando clock.

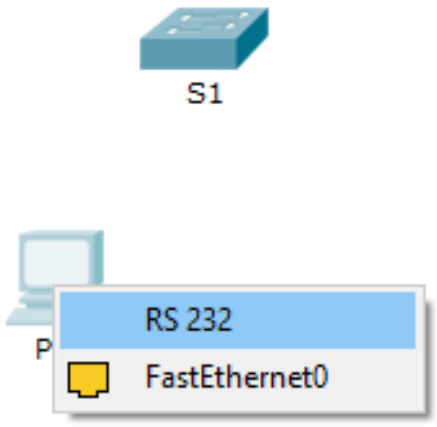
Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda
En la parte 1 de esta actividad, conectará una PC a un switch mediante una conexión de consola e investigará diferentes modos de comando y características de ayuda.

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

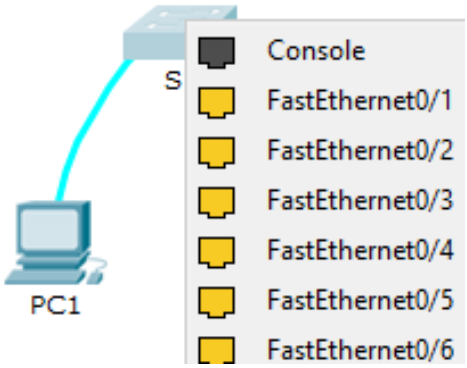


Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

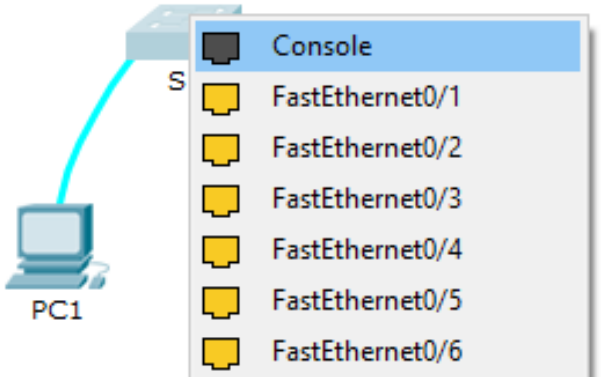
Haga clic en PC1. Aparece una ventana que muestra una opción para una conexión RS-232.

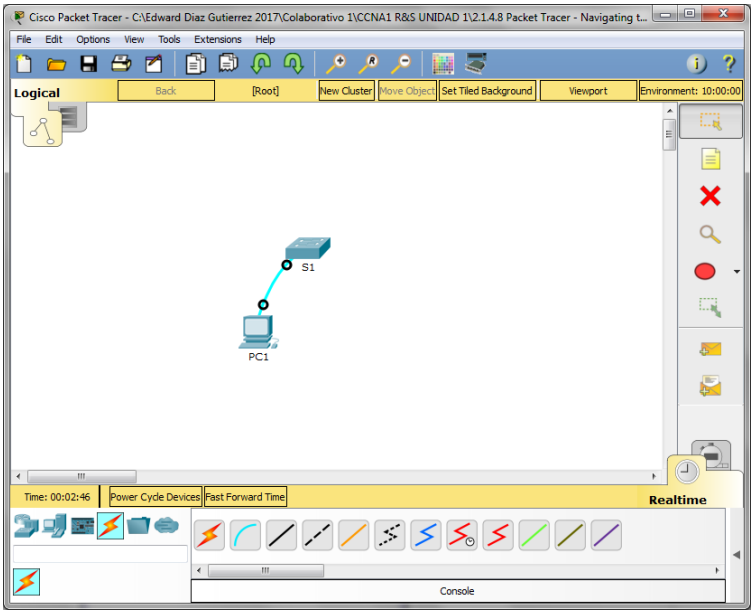


Arrastre el otro extremo de la conexión de consola al switch S1 y haga clic en el switch para abrir la lista de conexiones.

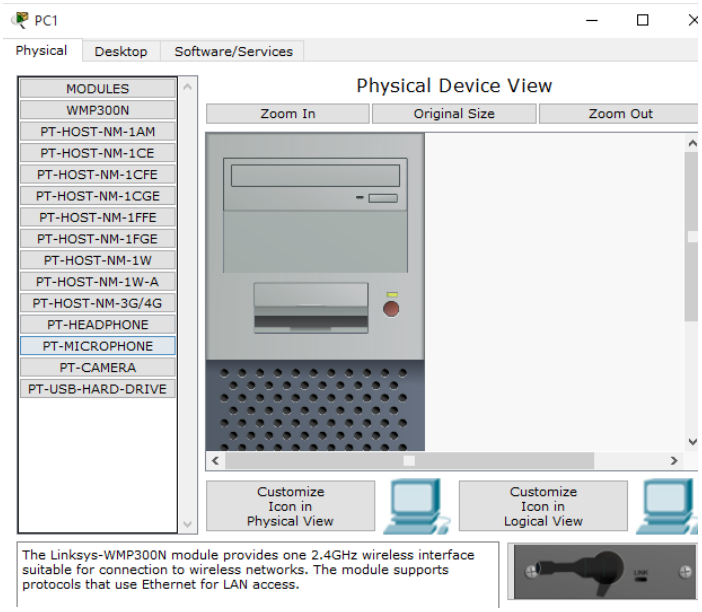


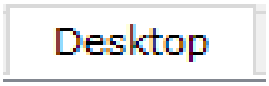
Seleccione el puerto de consola para completar la conexión.



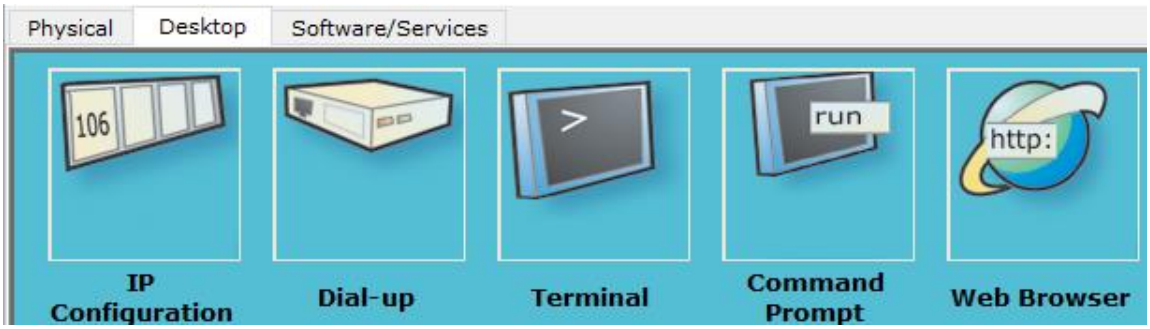


Paso 2: Establezca una sesión de terminal con el S1.
Haga clic en PC1 y después en la ficha Desktop (Escritorio).

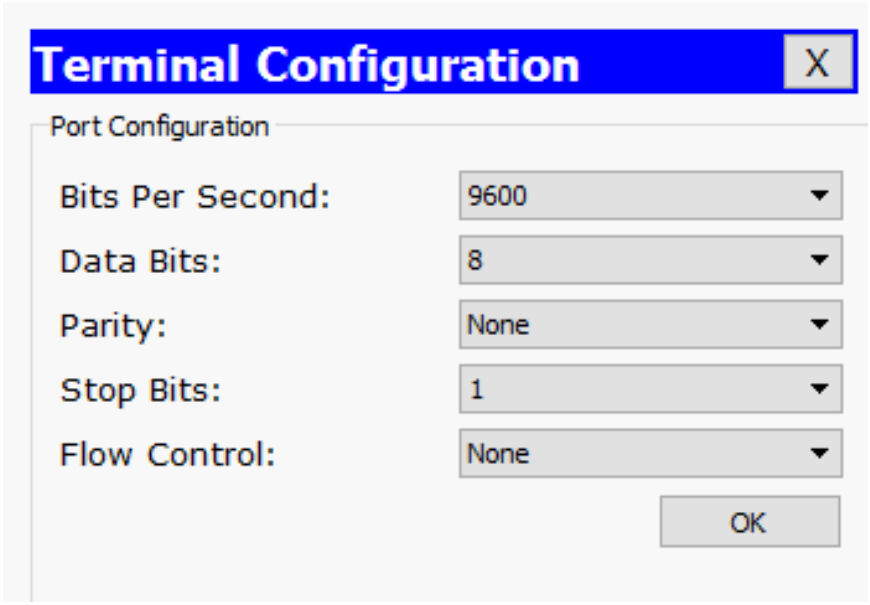




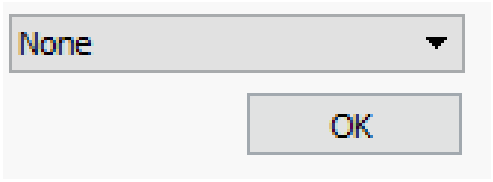
Haga clic en el ícono de la aplicación Terminal. Verifique que la configuración predeterminada de Port Configuration (Configuración del puerto) sea la correcta.



¿Cuál es el parámetro de bits por segundo? 9600



Haga clic en OK (Aceptar).



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.

```
Cisco IOS Software, C2960 Software (C2960-LANBAS
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!
```

¿Cuál es la petición de entrada que aparece en la pantalla? S1>

```
Press RETURN to get started!



S1>
```

Paso 3: Examine la ayuda de IOS.

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>?
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
```

¿Qué comando comienza con la letra “C”? conectar

```
connect      Open a terminal connection
```

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

S1> t?
¿Qué comandos se muestran? telnet terminal traceroute

```
S1>t?
telnet   terminal   traceroute
```

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

S1> te?

¿Qué comandos se muestran? telnet terminal

```
S1>te?
telnet   terminal
```

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

Parte 2: Exploración de los modos EXEC
En la parte 2 de esta actividad, debe cambiar al modo EXEC privilegiado y emitir comandos adicionales.

Paso 1: Ingrese al modo EXEC privilegiado.

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

```
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
```

¿Qué información de la que se muestra describe el comando enable? Active los comandos privilegiados.

```
enable      Turn on privileged commands
```

Escriba en y presione la tecla Tabulación.

S1> en<Tab>

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

```
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?

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

```
S1>te
S1>te
```

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

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

```
S1>ena
S1>enable
S1#
```

Cuando se le solicite, escriba el signo de interrogación (?).
S1# ?

```
S1#?
Exec commands:
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
 --More--
```

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
```

Aparecen 5: clear clock configure connect copy

Paso 2: Ingresar en el modo de configuración global

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

```
S1#conf
S1#configure
```

¿Cuál es el mensaje que se muestra?

```
S1#configure
Configuring from terminal, memory, or network [terminal]?
```

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

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

```
S1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

¿En qué cambia la petición de entrada? S1(config)#

```
S1(config)#
```

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(config)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#en
S1#enable
S1#con
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
```

Parte 3: Configuración del comando clock

Paso 1: Utilizar el comando clock

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>ena
S1>enable
S1#sho
S1#show clo
S1#show clock
*1:28:28.363 UTC Mon Mar 1 1993
S1#
```

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

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

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

S1# clock<ENTER>
¿Qué información aparece en pantalla? % Incomplete command.

```
S1#clock
% Incomplete command.
S1#
```

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? set Configura la hora y la fecha

```
S1#clock ?
  set  Set the time and date
```

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

```
S1#clock se
S1#clock set ?
```

¿Qué información se solicita? hh:mm:ss Hora actual

```
S1#clock se
S1#clock set ?
  hh:mm:ss  Current Time
S1#clock set
```

¿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? % Incomplete command

```
S1#clock set
% Incomplete command.
S1#
```

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:

```
S1#clock set 15:00:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
S1#clock set 15:00:00
```

<1-31> Day of the month
MONTH Month of the year

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

```
S1#show clock
*3:9:26.923 UTC Mon Mar 1 1993
S1#clock set 15:00:00 31 Jan 2035
S1#show clock
*15:0:3.530 UTC Wed Jan 31 2035
S1#
```

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

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.

```
S1#show clock
*3:9:26.923 UTC Mon Mar 1 1993
S1#clock set 15:00:00 31 Jan 2035
S1#show clock
*15:0:3.530 UTC Wed Jan 31 2035
S1#
```

Emita el siguiente comando y registre los mensajes:

S1# cl

¿Qué información se devolvió? % Ambiguous command: “cl”

```
S1#cl
% Ambiguous command:  "cl"
```

S1# clock

¿Qué información se devolvió? % Incomplete command.

```
S1# clock
% Incomplete command.
```

S1# clock set 25:00:00

¿Qué información se devolvió?

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

S1#clock set 25:00:00
^

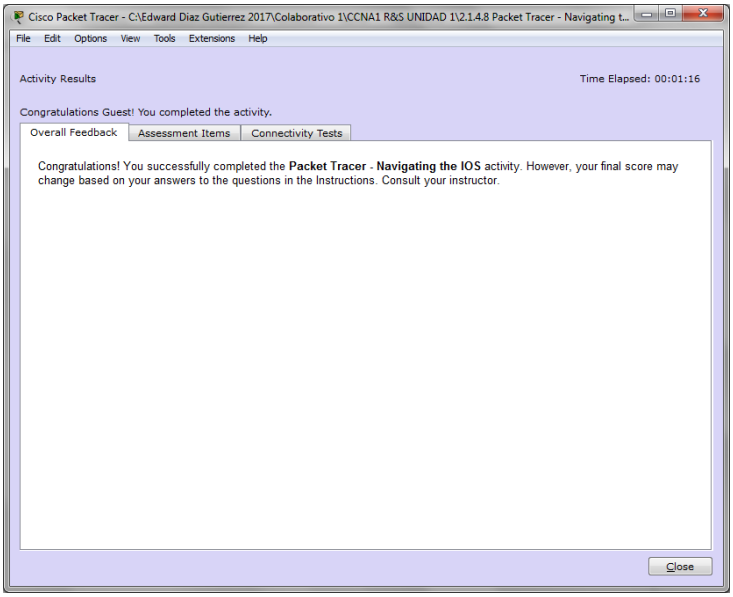
% Invalid input detected at '^' marker.

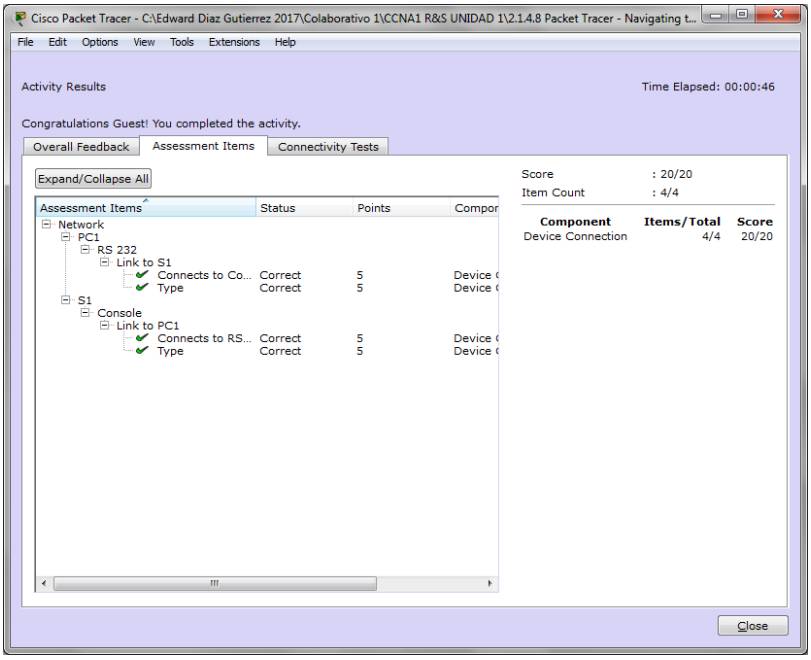
S1# clock set 15:00:00 32

¿Qué información se devolvió?

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

S1#
```

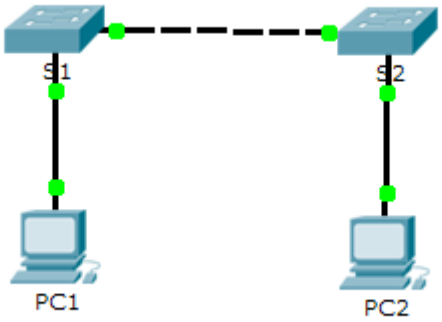
S1#clock set 15:00:00 32
^
% Invalid input detected at '^' marker.




Cisco Packet Tracer - C:\Edward Diaz Gutierrez 2017\Colaborativo 1\CCNA1 R&S UNIDAD 1\2.1.4.8 Packet Tracer - Navigating t...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:00:46
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Compor
Network
PC1
RS 232
Link to S1
Connects to Co...
Correct
5
Device
Type
Correct
5
Device
S1
Console
Link to PC1
Connects to RS...
Correct
5
Device
Type
Correct
5
Device
Score : 20/20
Item Count : 4/4
Component
Items/Total
Score
Device Connection
4/4
20/20
Close

2.2.3.3 Packet Tracer: Configuración de los parámetros iniciales del switch

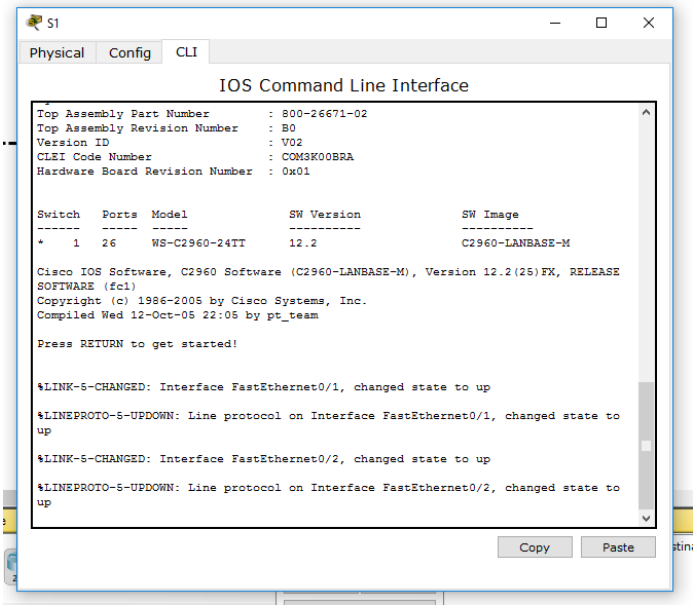
Topología



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.

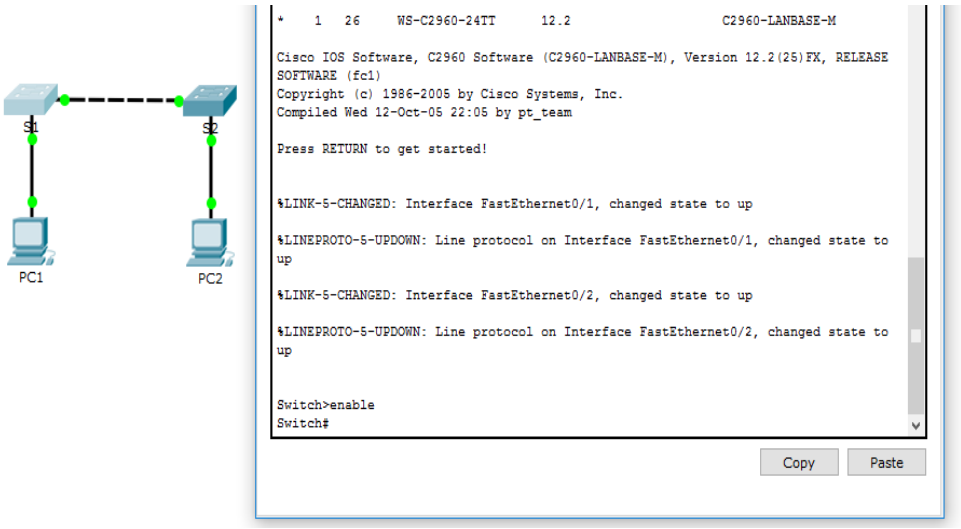
Parte 1: Verificar la configuración predeterminada del switch

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.
Haga clic en S1 y, a continuación, en la ficha CLI. Presione <Entrar>.



b. Ingrese al modo EXEC privilegiado introduciendo el comando enable:

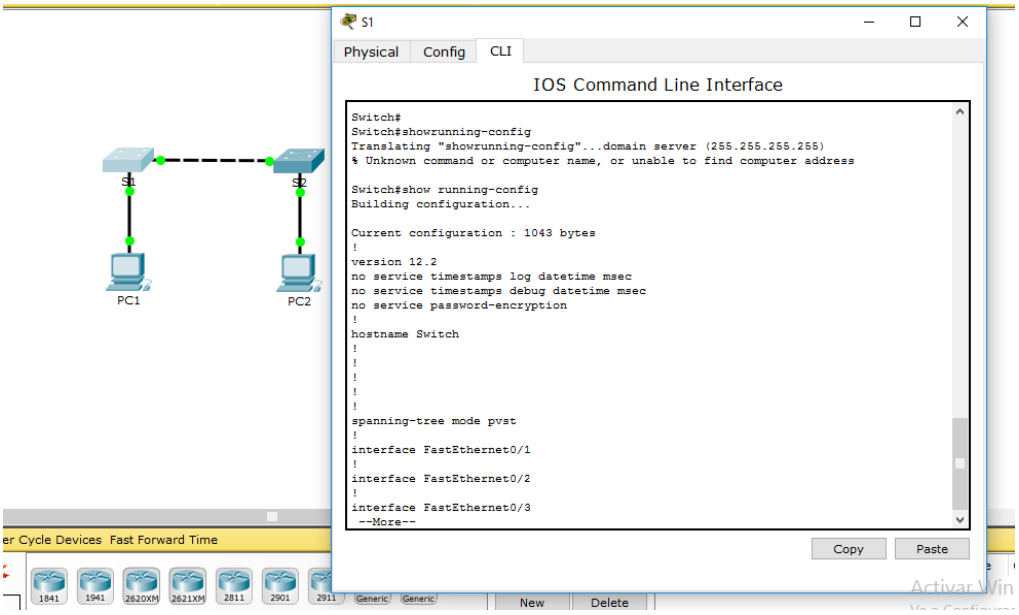
Switch> enable
Switch#
Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.



Paso 2: Examine la configuración actual del switch.

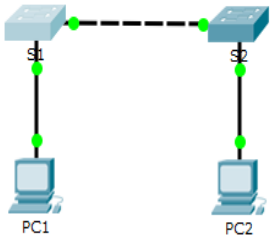
a. Ingrese el comando show running-config.

Switch# show running-config

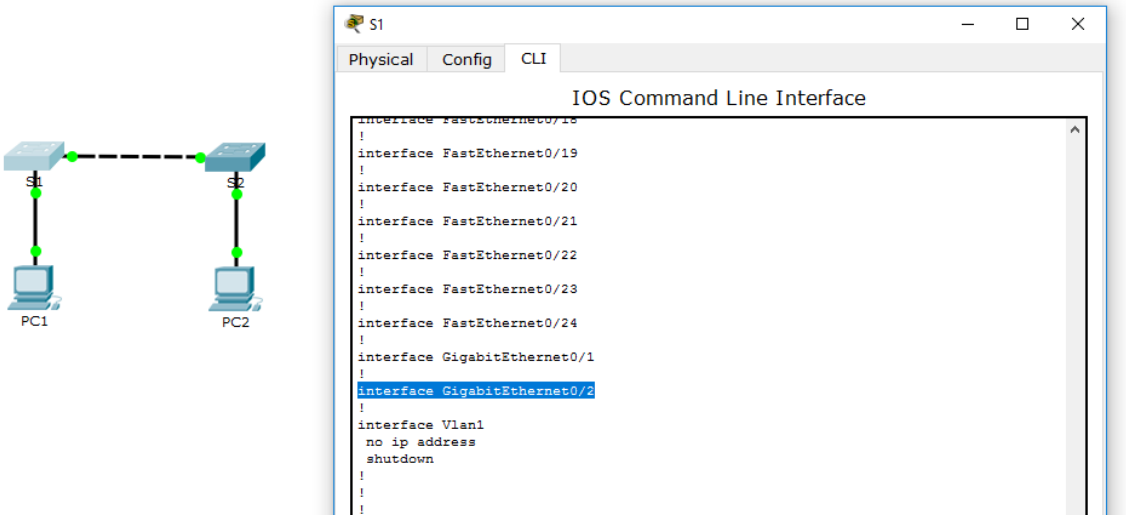


b. Responda las siguientes preguntas:

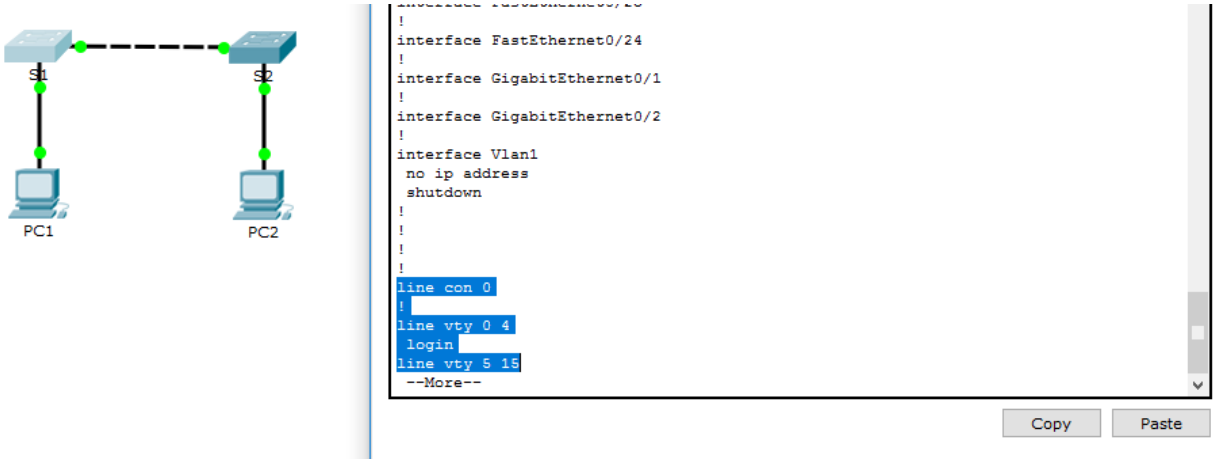
¿Cuántas interfaces FastEthernet tiene el switch? 24



¿Cuántas interfaces Gigabit Ethernet tiene el switch? 2

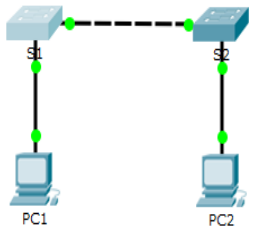


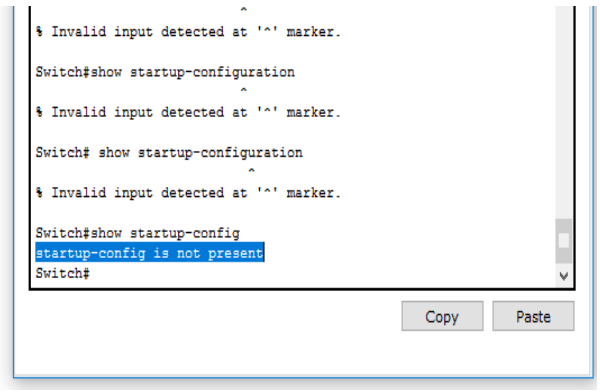
¿Cuál es el rango de valores que se muestra para las líneas vty? 0 -15



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

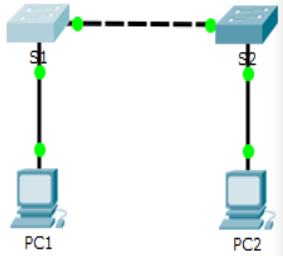
¿Por qué el switch responde con startup-config is not present? Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.

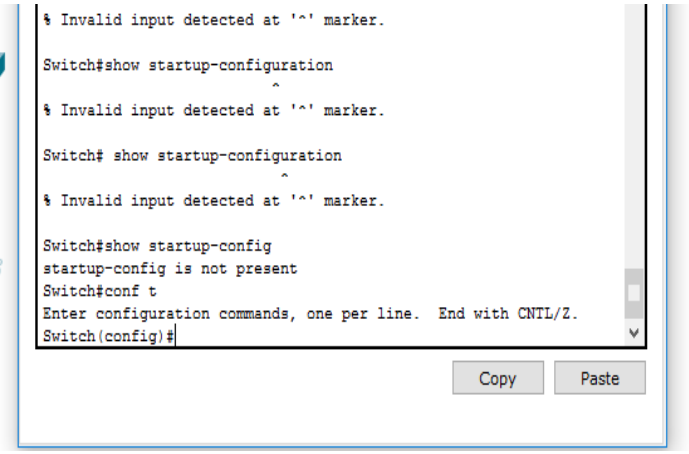




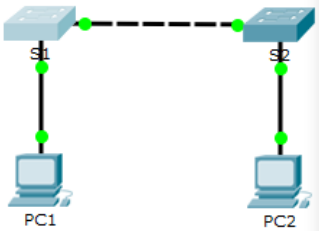
Parte 2: Crear una configuración básica del switch

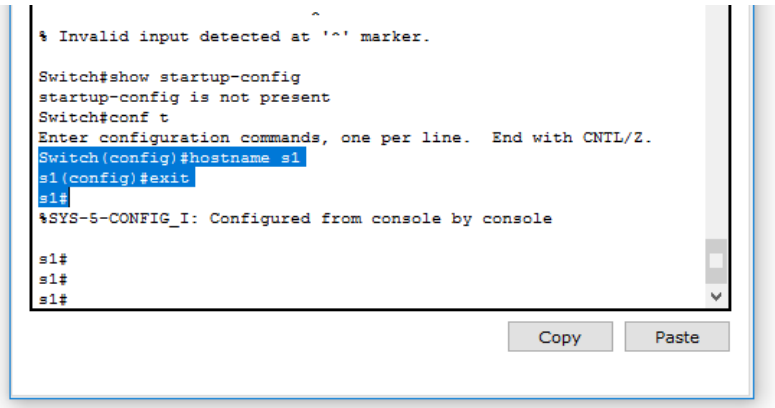
Paso 1: Asignar un nombre a un switch
Para configurar los parámetros de un switch, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el switch.
Switch# configure terminal



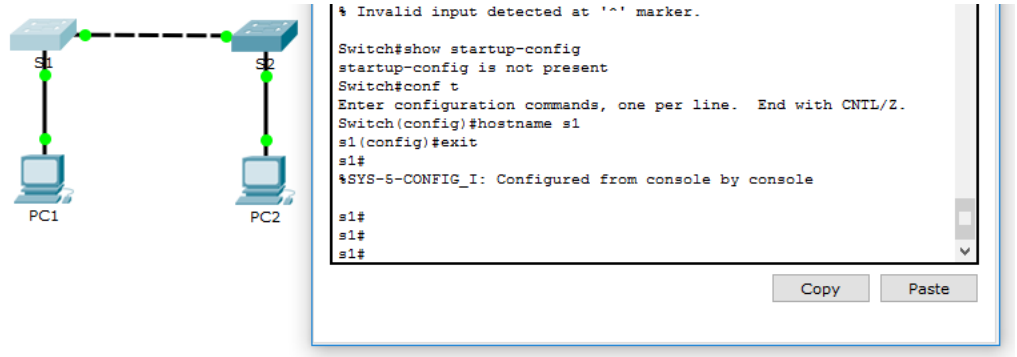


Switch(config)# hostname S1



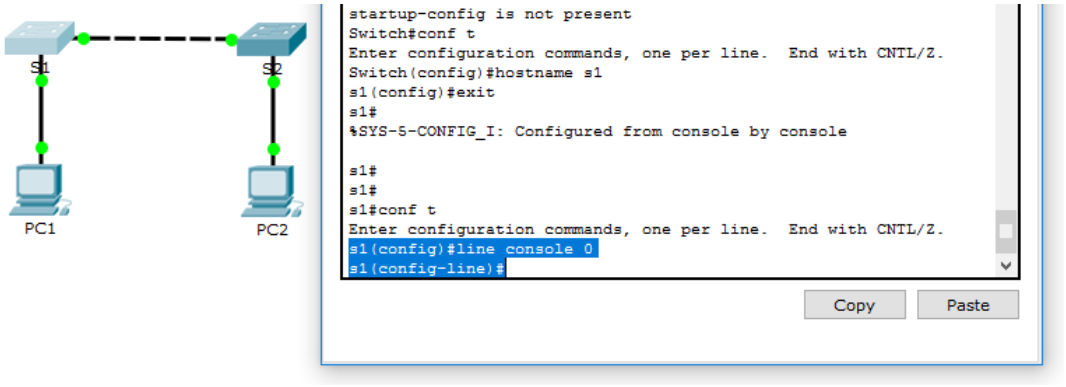


S1(config)# exit

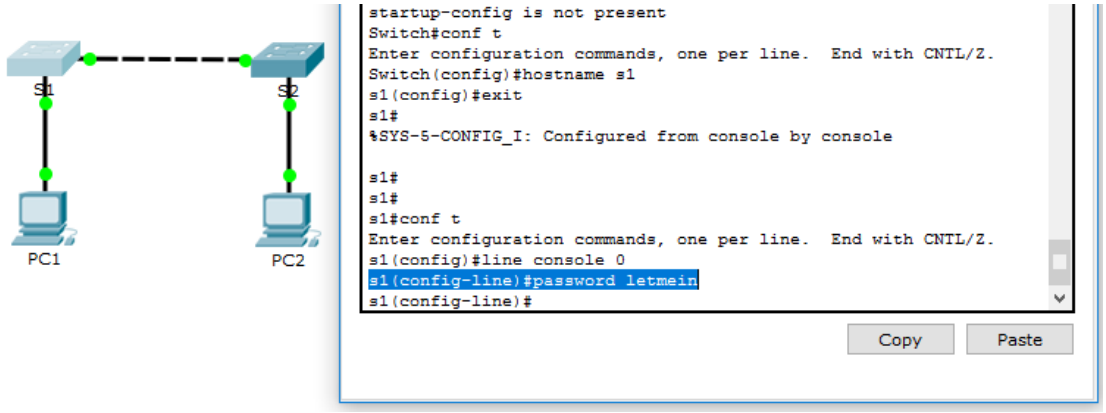


S1#

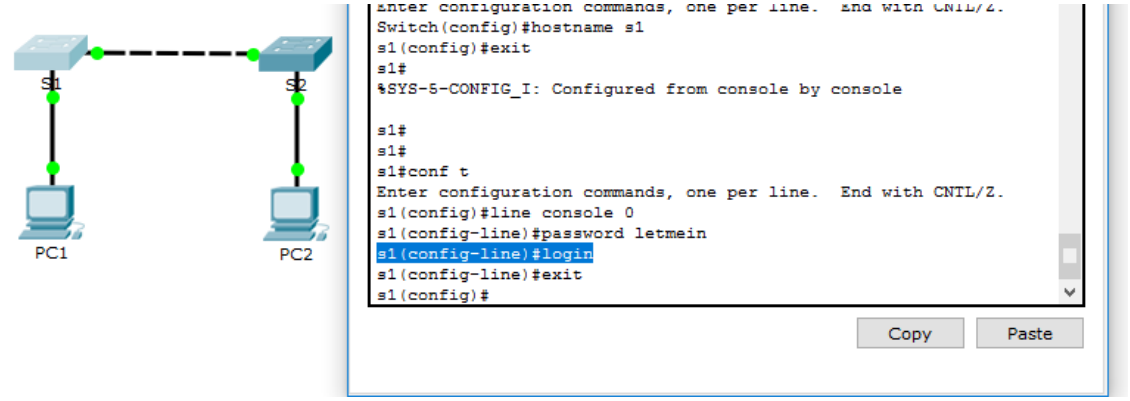
Paso 2: Proporcionar un acceso seguro a la línea de consola
Para proporcionar un acceso seguro a la línea de la consola, acceda al modo config-line y establezca la contraseña de consola en letmein.
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. S1(config)# line console 0



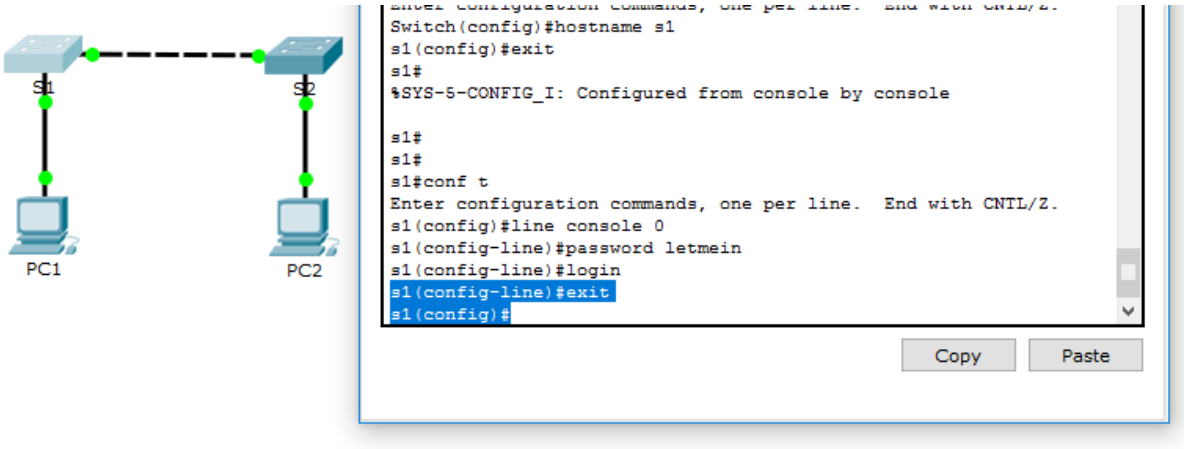
S1(config-line)# password letmein



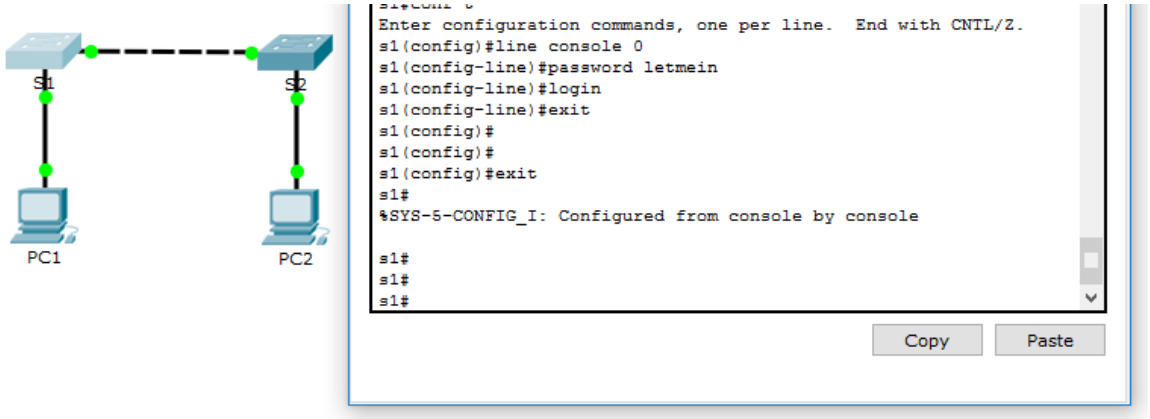
S1(config-line)# login



S1(config-line)# exit



S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console S1#

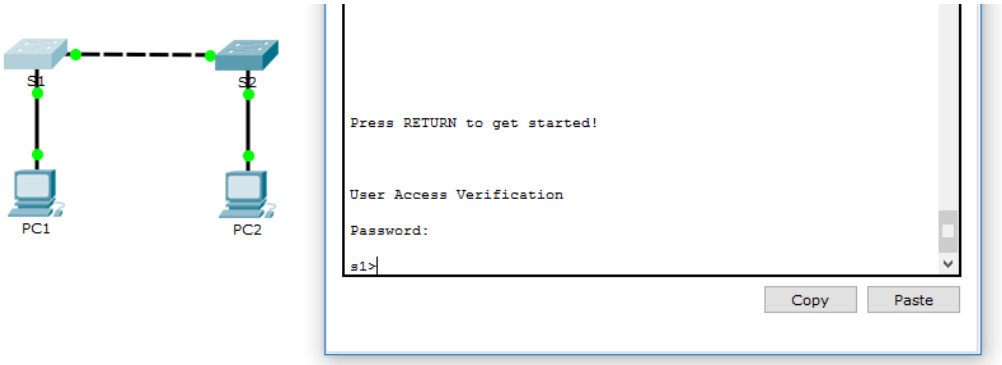


¿Por qué se requiere el comando login? Para que el proceso de control de contraseñas funcione, se necesitan los comandos login y password.

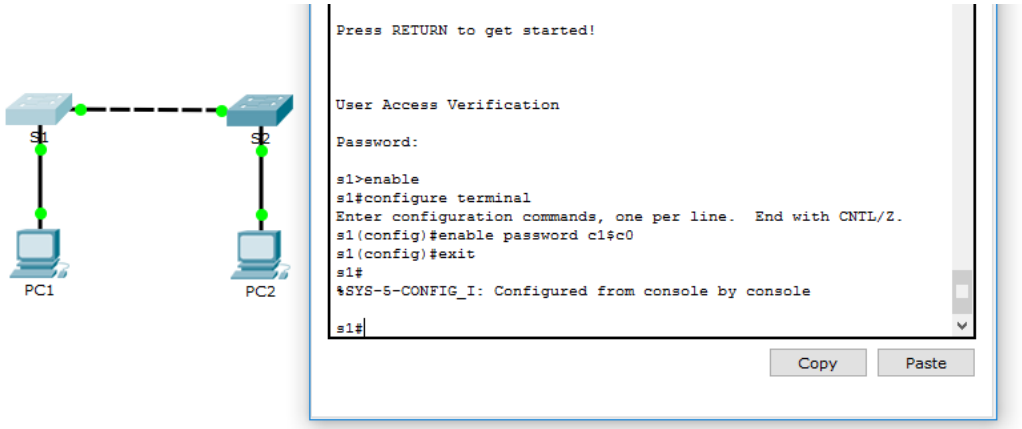
Paso 3: Verifique que el acceso a la consola sea seguro.
Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.
S1# exit
Switch con0 is now available Press RETURN to get started.

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 "letmein"



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 encripte 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.

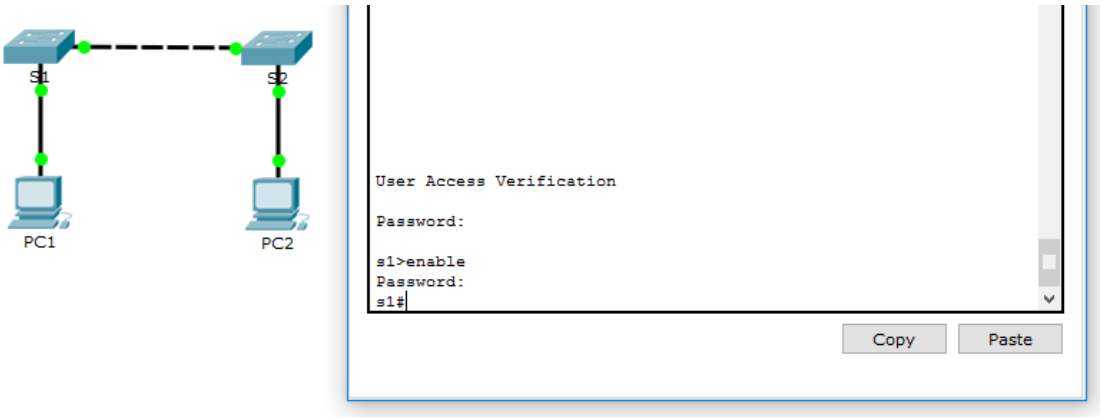
b. Presione <Entrar>; a continuación, se le pedirá que introduzca una contraseña:

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.

“letmein”

d. Introduzca el comando para acceder al modo privilegiado.

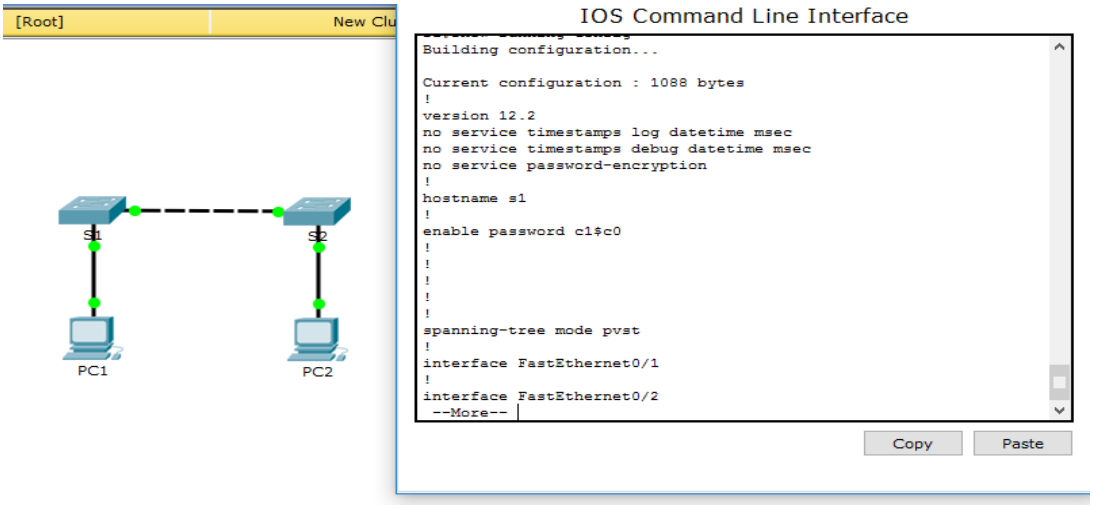


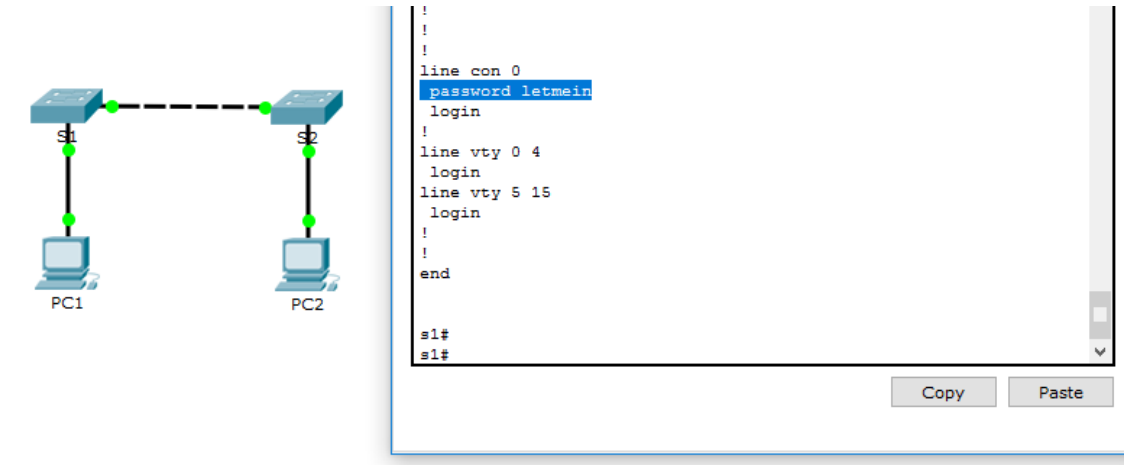
e. Introduzca la segunda contraseña que configuró para proteger el modo EXEC privilegiado.

c1$c0

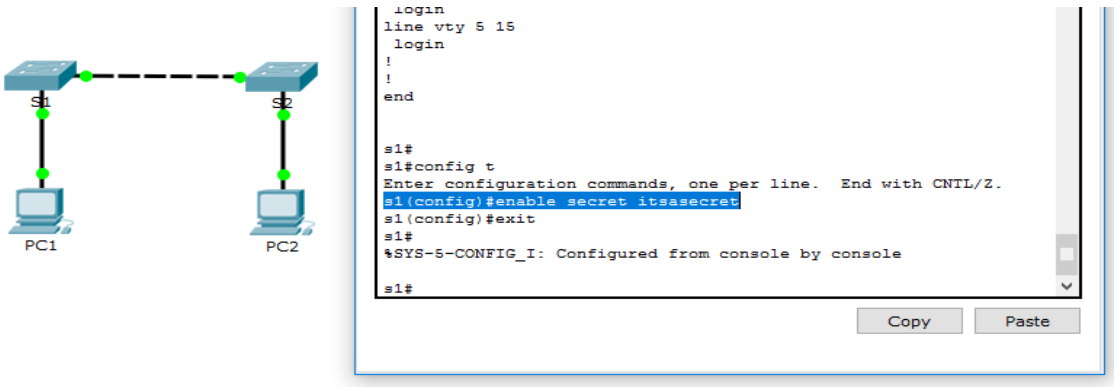
f. Para verificar la configuración, examine el contenido del archivo de configuración en ejecución:

S1# show running-config





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.

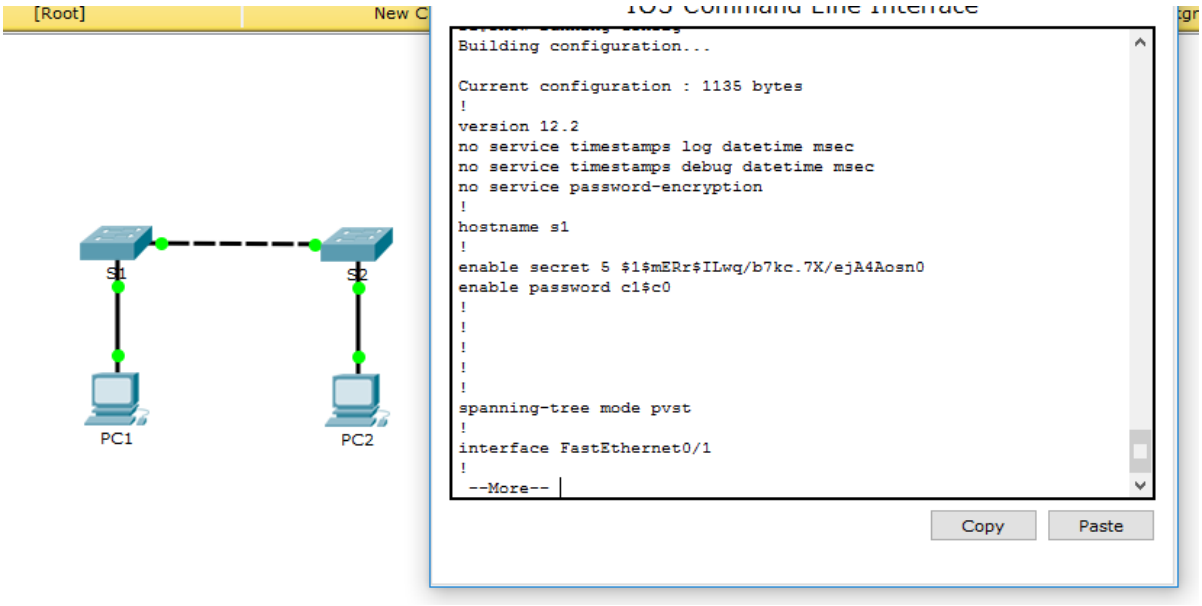
Paso 7: Verificar si la contraseña secreta de enable se agregó al archivo de configuración

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? 1mERr$ILwq/b7kc.7X/ejA4Aosn0



c. ¿Por qué la contraseña secreta de enable se ve diferente de lo que se configuró? El comando enable secret se muestra encriptado, mientras que la contraseña de enable aparece en texto no cifrado.

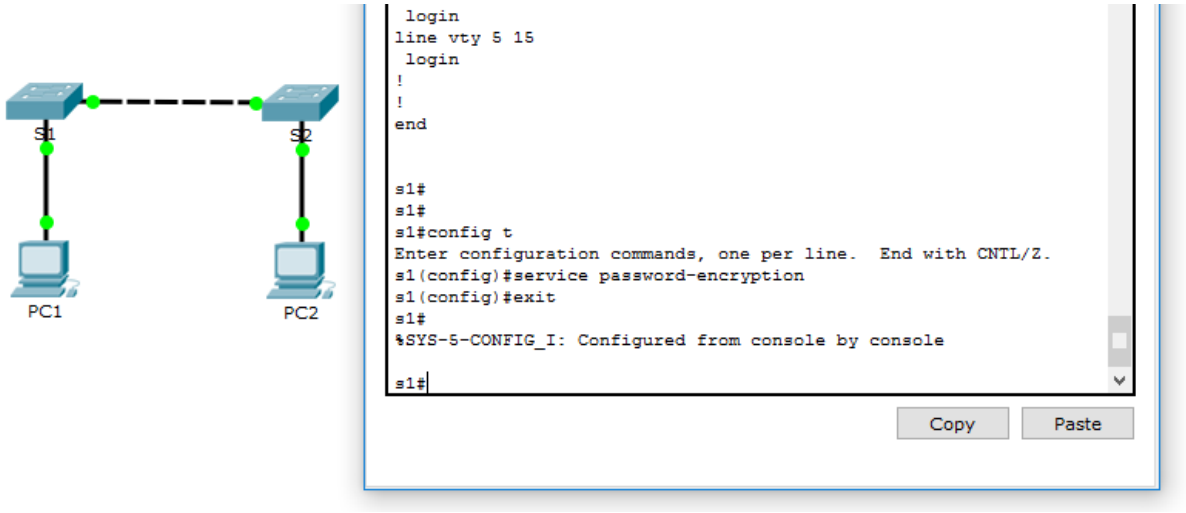
Paso 8: Encriptar las contraseñas de consola y de enable

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

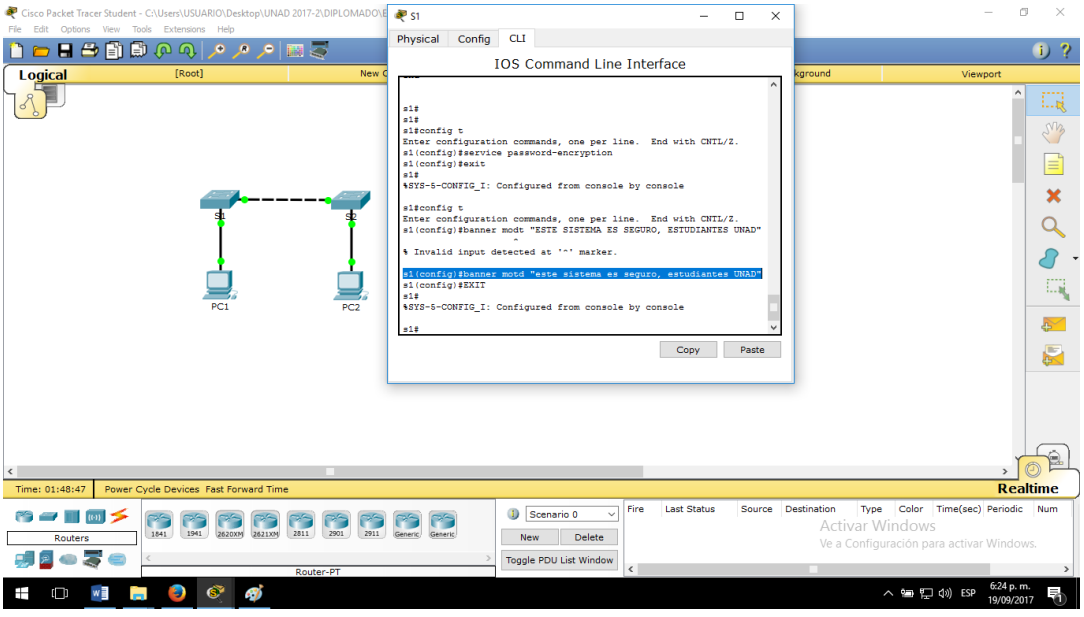


Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma encriptada en el archivo de configuración? Explique por qué. El comando service password-encryption encripta todas las contraseñas actuales y futuras.

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!"

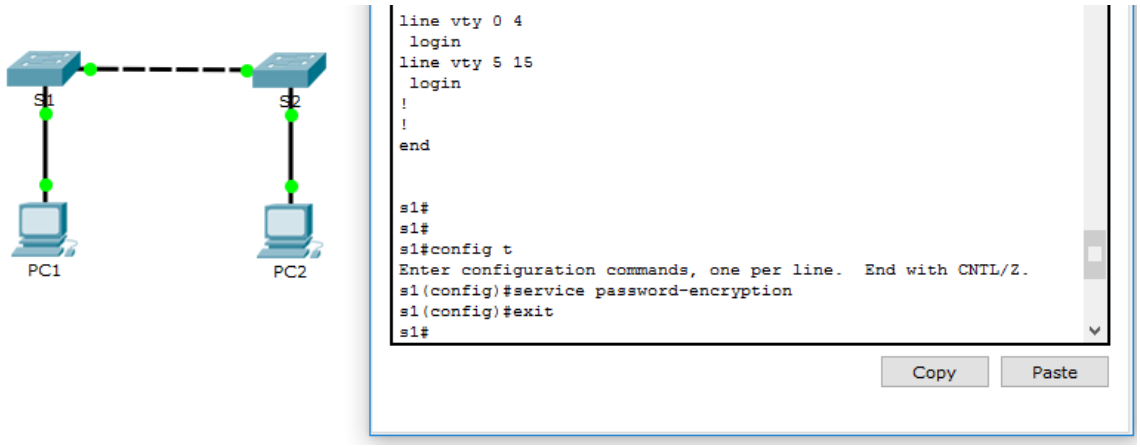
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#



¿Cuándo se muestra este mensaje? El mensaje se muestra cuando alguien accede al switch a través del puerto de consola.

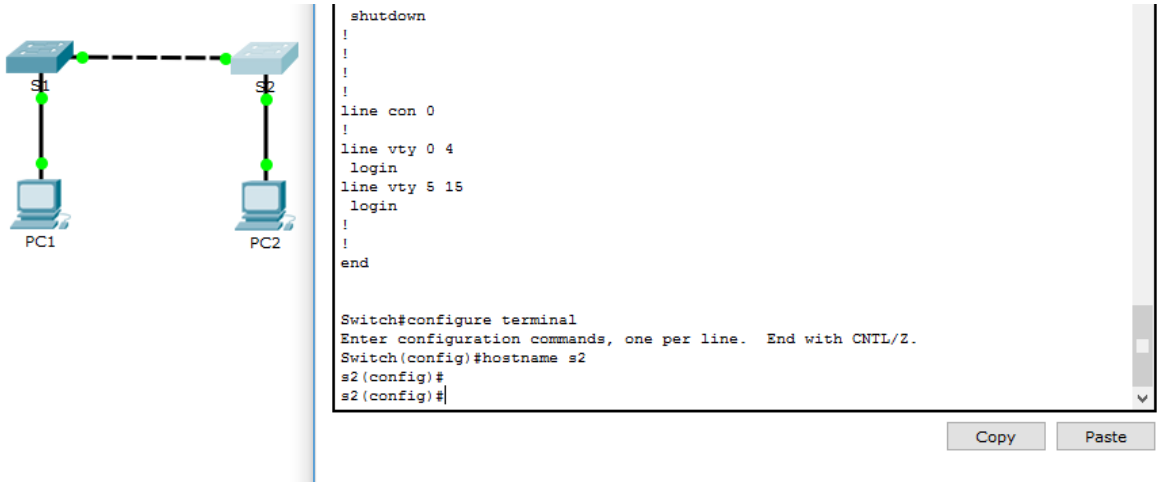
¿Por qué todos los switches deben tener un mensaje MOTD? Cada switch debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).

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? cop r s

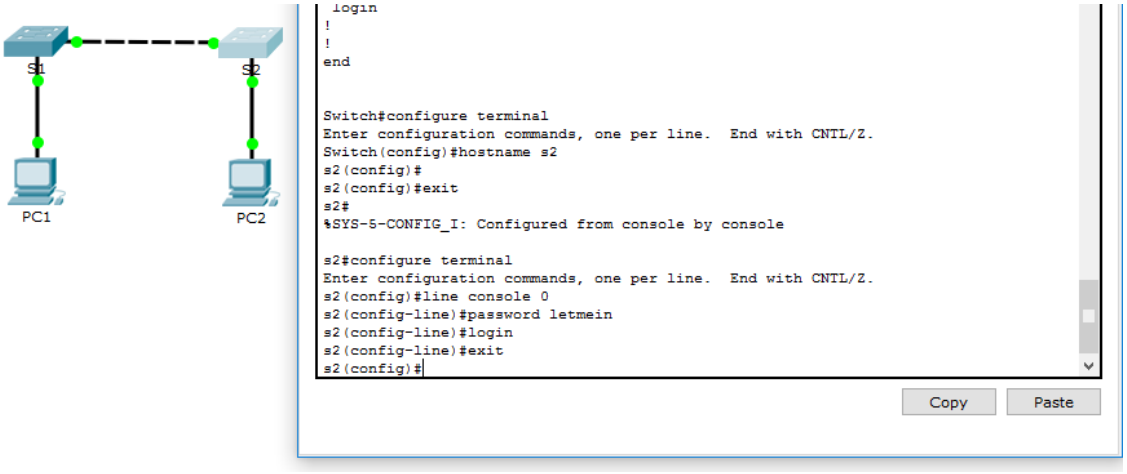


Paso 3: Examinar el archivo de configuración de inicio
¿Qué comando muestra el contenido de la NVRAM? show startup-configuration
¿Todos los cambios realizados están grabados en el archivo? Sí, es igual a la configuración en ejecución.

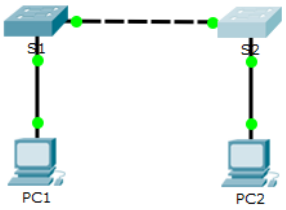
Parte 5: Configurar S2
Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.
Configure el S2 con los siguientes parámetros:
a. Nombre del dispositivo: S2



b. Proteja el acceso a la consola con la contraseña letmein.

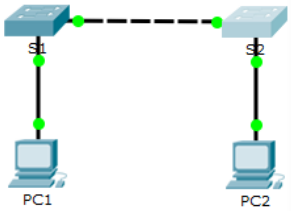


c. Configure la contraseña c1$c0 para enable y la contraseña secreta de enable, itsasecret.




```
s2(config)#line console 0
s2(config-line)#password letmein
s2(config-line)#login
s2(config-line)#exit
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#
s2#enale
Translating "enale"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

s2#enable
s2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#enable password c1$c0
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#
```

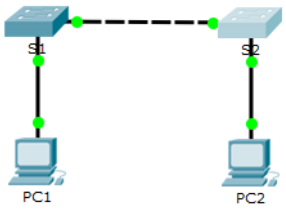
Copy Paste




```
s2#enable
s2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#enable password c1$c0
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#enable secret itsasecret
          ^
% Invalid input detected at '^' marker.

s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#enable secret itsasecret
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#
```

Copy Paste

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.




```
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end


s2#
s2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
s2(config)#banner motd "acceso autorizado unicamente. Unauthorized access is
prohibited and violators will be prosecuted to the full extent of the law."
s2(config)#exit
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#
```

Copy Paste

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.

2.3.2.5 Packet Tracer: Implementación de conectividad básica

Topología

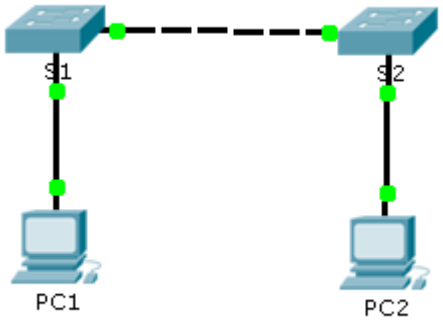


Tabla de direccionamiento

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

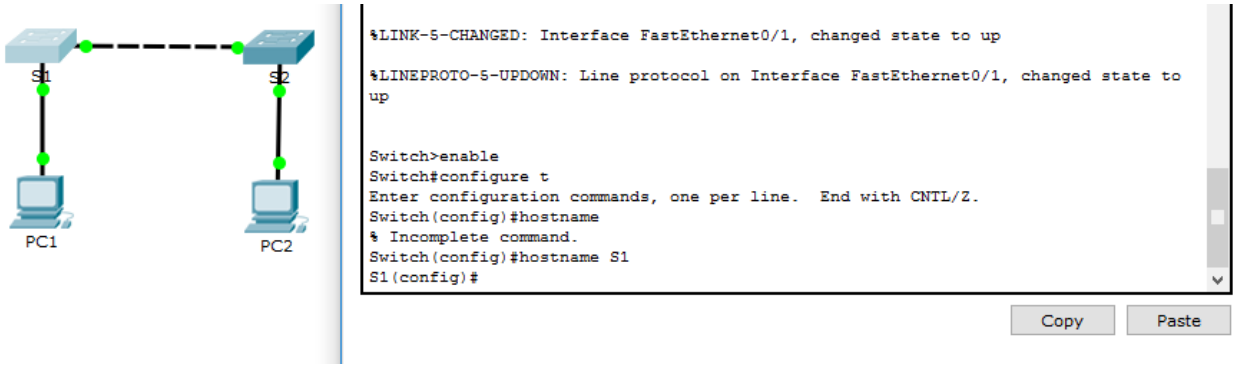
Objetivos
Parte 1: Realizar una configuración básica en S1 y S2 Paso 2: Configurar la PC
Parte 3: Configurar la interfaz de administración de switches

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.

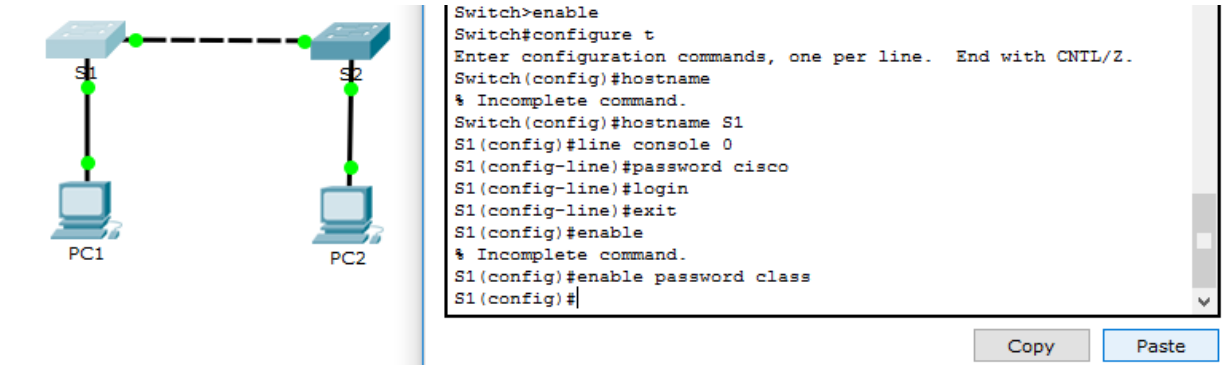
b. Introduzca el comando correcto para configurar el nombre de host S1.



Paso 2: Configurar las contraseñas de consola y del modo EXEC privilegiado

a. Use cisco para la contraseña de consola.

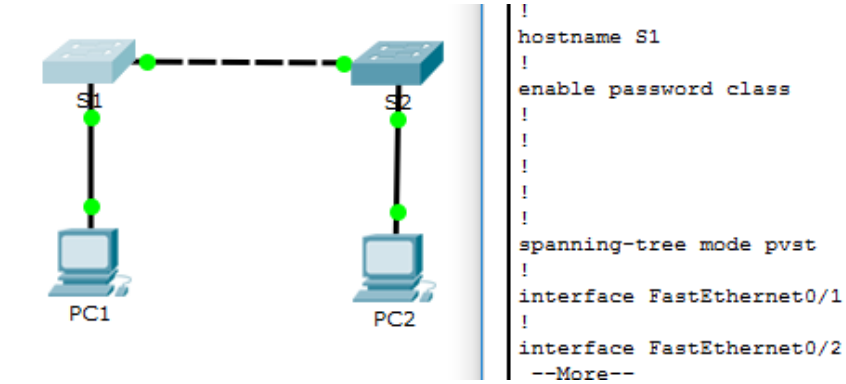
b. Use class para la contraseña del modo EXEC privilegiado.

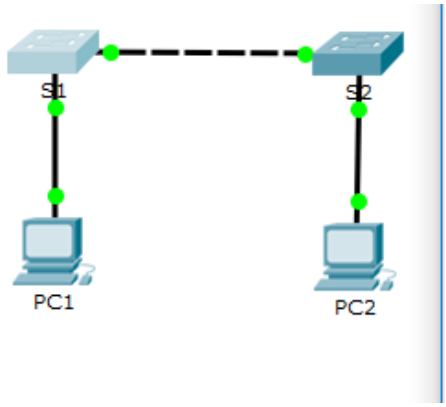


Paso 3: Verificar la configuración de contraseñas para el S1

¿Cómo puede verificar que ambas contraseñas se hayan configurado correctamente?

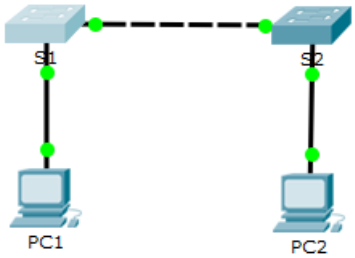
Una vez que salga del modo EXEC del usuario, el switch le solicitará una contraseña para acceder a la interfaz de consola y le solicitará una contraseña por segunda vez para acceder al modo EXEC privilegiado. También puede usar el comando show run para ver las contraseñas.






```
!
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
 --More--
```

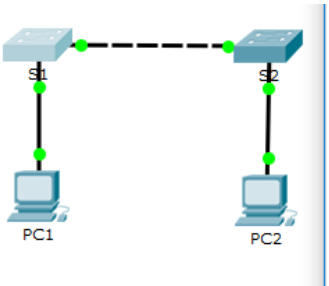
Paso 4: Configurar un mensaje del día (MOTD).
Utilice un texto de aviso adecuado para advertir contra el acceso no autorizado. El siguiente texto es un ejemplo: Acceso autorizado únicamente. Los infractores se procesarán en la medida en que lo permita la ley.




```
% Invalid input detected at '^' marker.

S1#enable
S1#banner motd "Acceso autorizado unicamente.Los infractores se
procesaran en la medida que lo permita la ley."
                ^
% Invalid input detected at '^' marker.

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "Acceso autorizado unicamente.Los
infractores se procesaran en la medida que lo permita la ley."
S1(config)#
```

Copy Paste

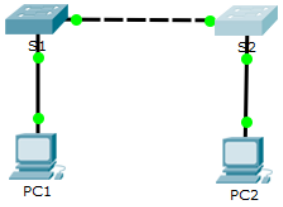
Paso 5: Guarde el archivo de configuración en la NVRAM.
¿Qué comando emite para realizar este paso?
S1(config)#exit (or end)
S1#copy run start




```
% Invalid input detected at '^' marker.

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "Acceso autorizado unicamente.Los
infractores se procesaran en la medida que lo permita la ley."
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Copy Paste

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



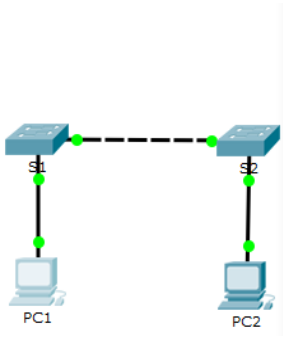

```
up


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)#exit
S2(config)#enable password class
S2(config)#banner motd "Acceso autorizado unicamente.Los infractores se procesaran
en la medida en que lo permita la ley."
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

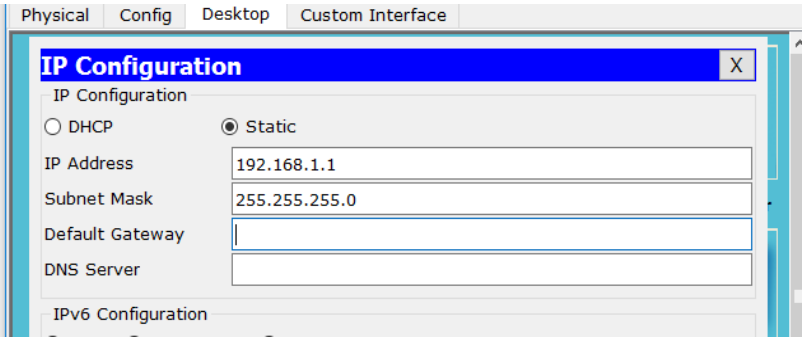
Parte 2: Configurar las PC
Configure la PC1 y la PC2 con direcciones IP.

Paso 1: Configurar ambas PC con direcciones IP

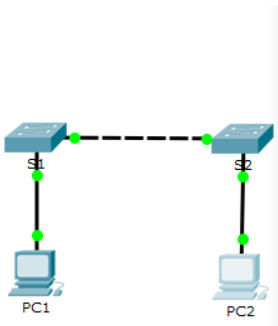
a. Haga clic en PC1 y, a continuación, haga clic en la ficha Desktop (Escritorio).

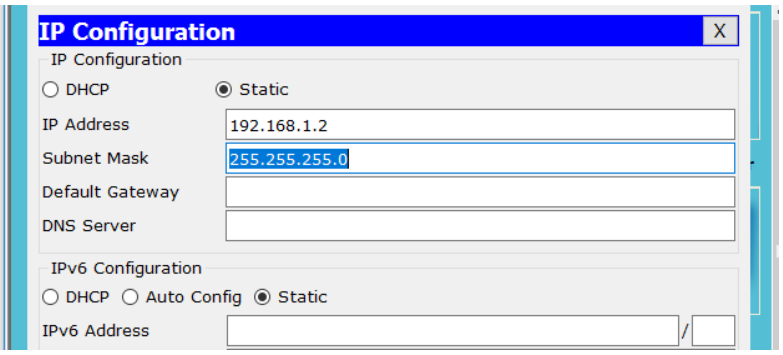
b. Haga clic en IP Configuration (Configuración de IP). En la tabla de direccionamiento anterior, puede ver que la dirección IP para la PC1 es 192.168.1.1 y la máscara de subred es 255.255.255.0. Introduzca esta información para la PC1 en la ventana IP Configuration.





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



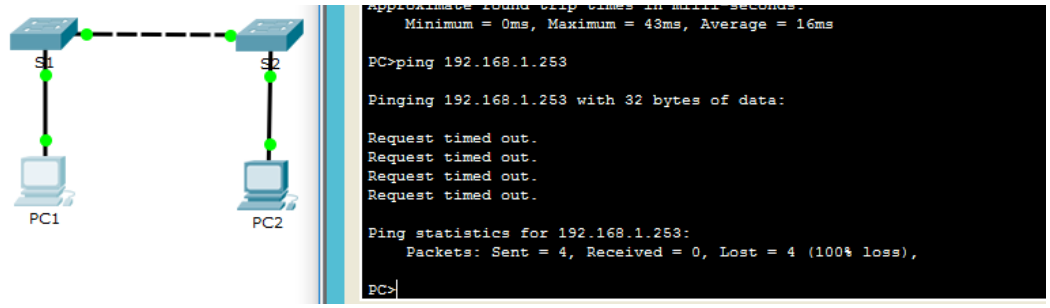


Paso 2: Probar la conectividad a los switches

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? ¿Por qué o por qué no?

No debería realizarse correctamente, porque los switches no están configurados con una 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

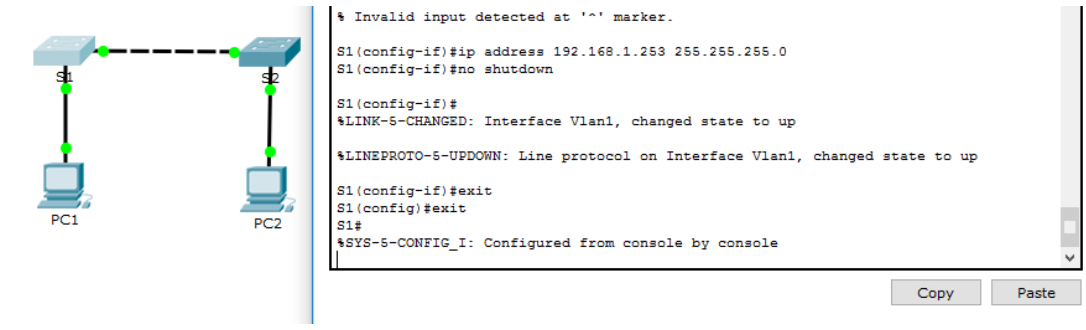
S1(config-if)# ip address 192.168.1.253 255.255.255.0

S1(config-if)# no shutdown

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#

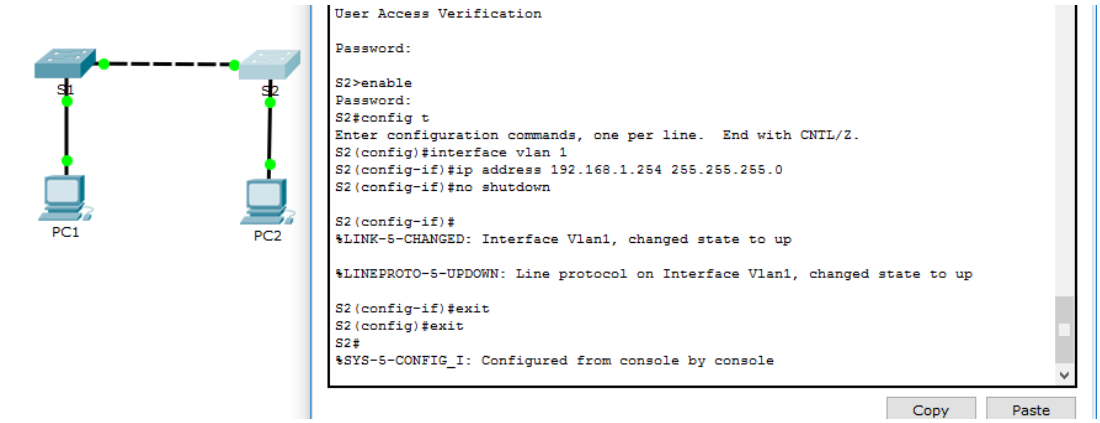
S1(config-if)# exit

S1#

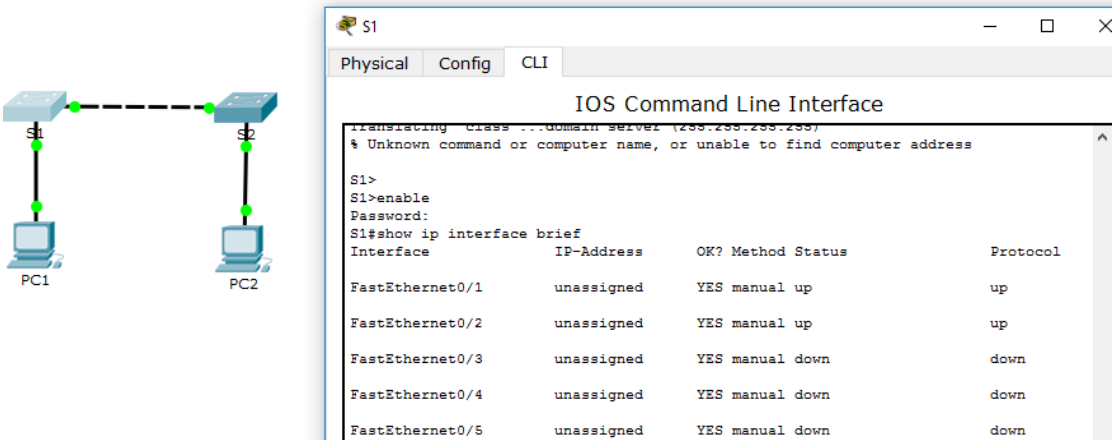


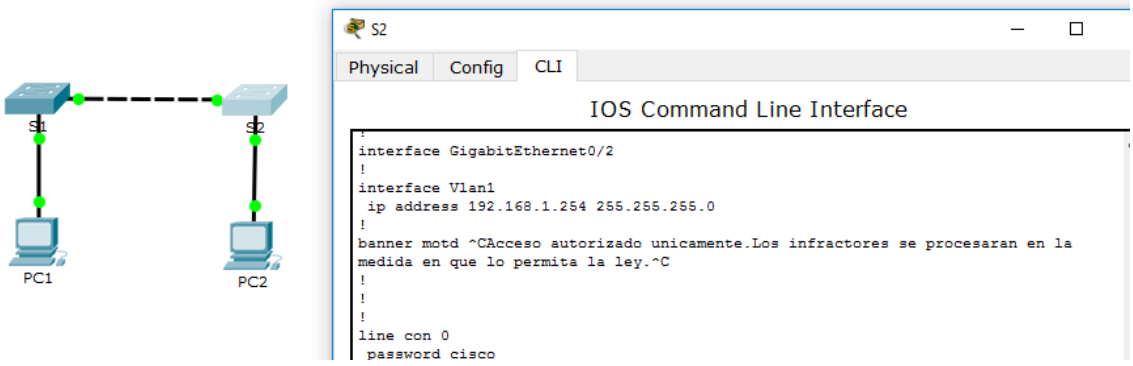
¿Por qué debe introducir el comando no shutdown? El comando no shutdown habilita administrativamente el estado activo de la interfaz.

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.

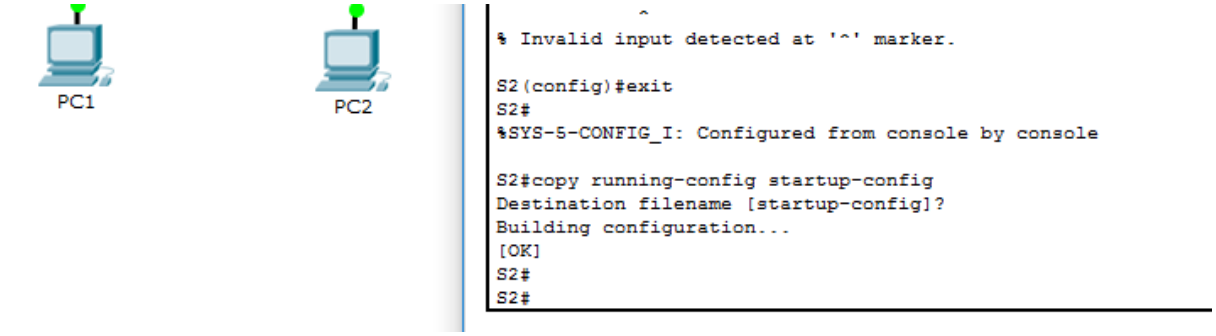


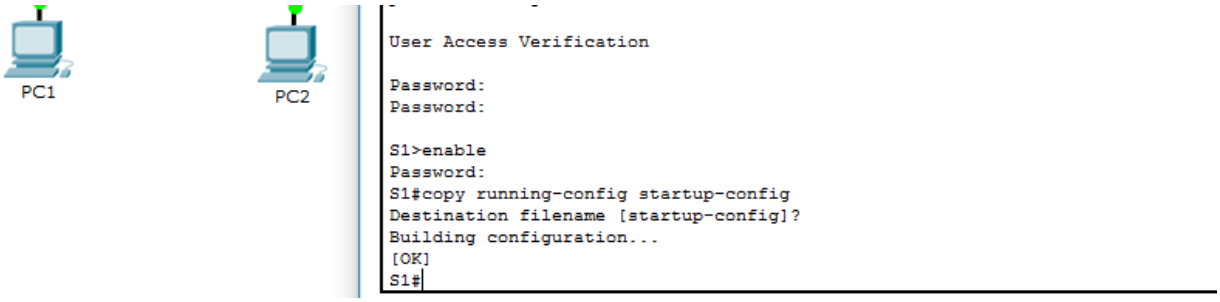
Paso 3: Verificar la configuración de direcciones IP en el S1 y el S2
Use el comando show ip interface brief para ver la dirección IP y el estado de todos los puertos y las interfaces del switch. También puede utilizar el comando show running-config.





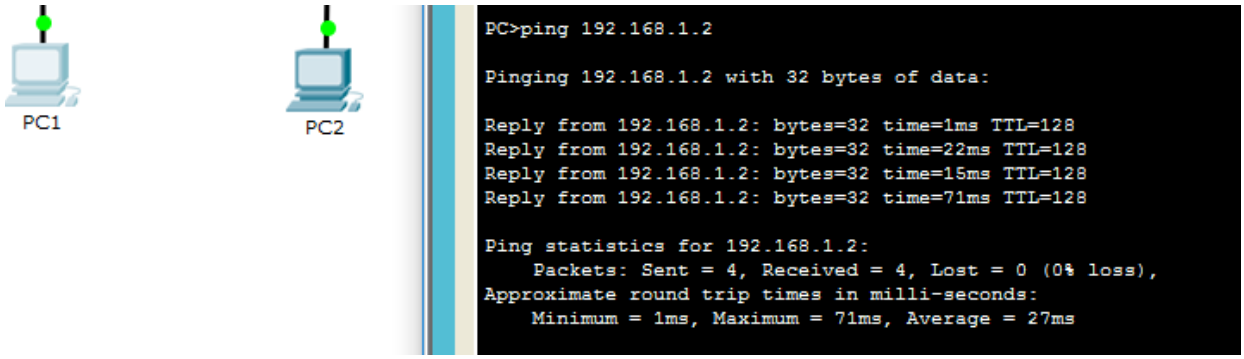
Paso 4: Guardar la configuración para el S1 y el S2 en la NVRAM
¿Qué comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM?
copy run start



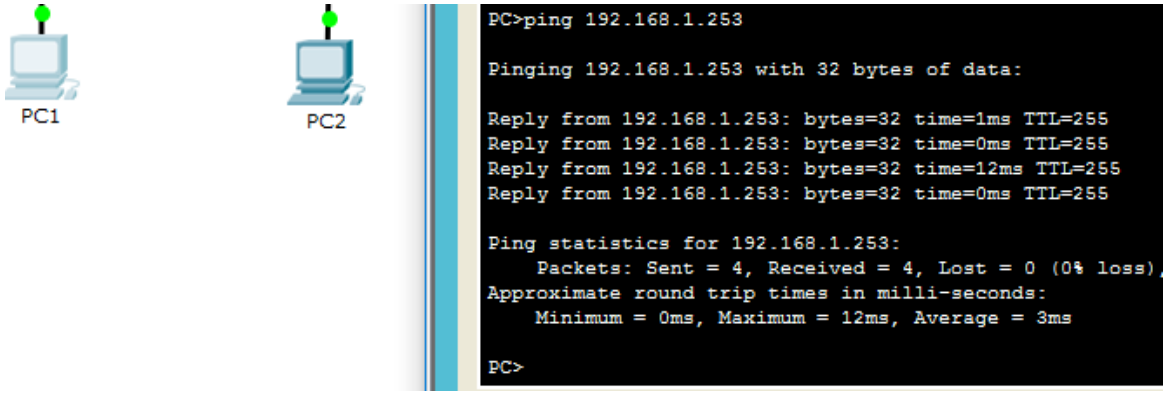


Paso 5: Verificar la conectividad de la red
La conectividad de red se puede verificar mediante el comando ping. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Haga ping a la dirección IP del S1 y el S2 desde la PC1 y la PC2.

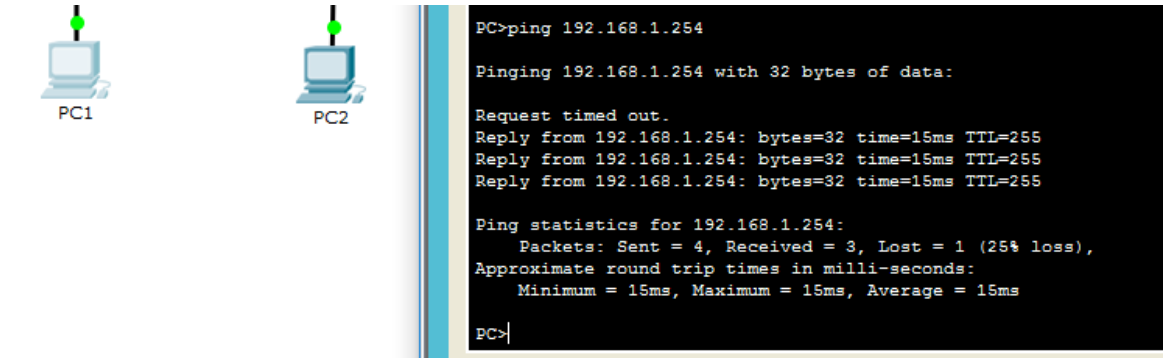
a. Haga clic en PC1 y, a continuación, haga clic en la ficha Desktop (Escritorio).
b. Haga clic en Command Prompt.
c. Haga ping a la dirección IP de la PC2.



d. Haga ping a la dirección IP del S1.



e. Haga ping a la dirección IP del S2.



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.

2.4.1.2 Packet Tracer: Reto de habilidades de integración

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
Class-A	VLAN 1	10.10.10.100	255.255.255.0
Class-B	VLAN 1	10.10.10.150	255.255.255.0
Student-1	NIC	10.10.10.4	255.255.255.0
Student-2	NIC	10.10.10.5	255.255.255.0

Objetivos

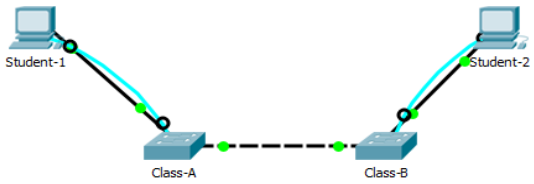
- Configurar los nombres de host y las direcciones IP en dos switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Usar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones de los dispositivos.
- Utilizar los comandos de IOS para guardar la configuración en ejecución.
- Configurar dos dispositivos host con direcciones IP.
- Verificar la conectividad entre los dos dispositivos finales de PC.

Situación

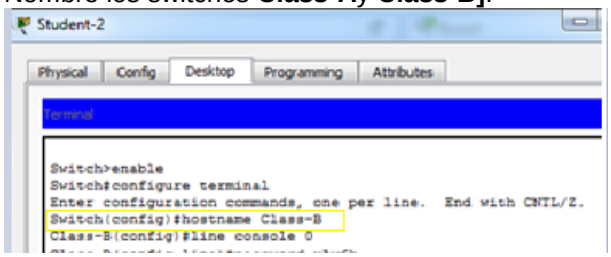
Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante Cisco IOS y la configuración de parámetros de dirección IP en dispositivos 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

- Use una conexión de consola para acceder a cada switch.

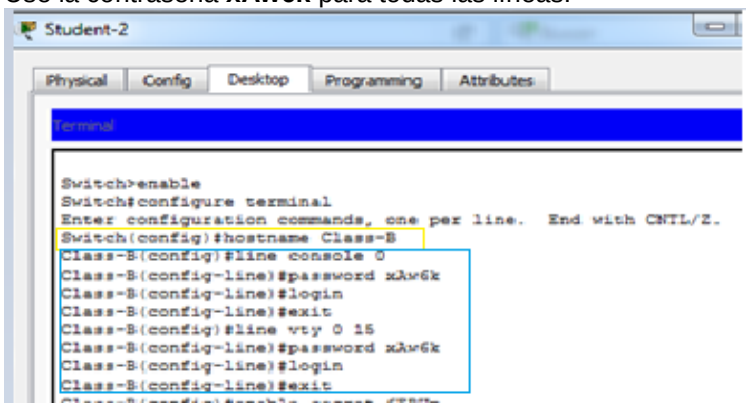


- Nombre los switches **Class-A**y **Class-B]**.




```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Class-A
```

- Use la contraseña **xAw6k** para todas las líneas.



```
Class-A(config)#line console 0
Class-A(config-line)#password 6EBUp
Class-A(config-line)#login
Class-A(config-line)#exit
Class-A(config)#line vty 0 15
Class-A(config-line)#password 6EBUp
Class-A(config-line)#login
Class-A(config-line)#exit
```

- Use la contraseña secreta **6EBUp**.
- Encripte todas las contraseñas de texto no cifrado.
- Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).

```
Class-B(config)#enable secret 6EBUp
Class-B(config)#service password-encryption
Class-B(config)#banner motd #warning#
Class-B(config)#interface vlan 1
```

```
Class-A(config)#enable secret 6EBUp
Class-A(config)#service password-encryption
Class-A(config)#banner motd # Warning#
```

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

```
Class-B(config)#interface vlan 1
Class-B(config-if)#ip address 10.10.10.100 255.255.255.0
Class-B(config-if)#interface vlan 1
Class-B(config-if)#ip address 10.10.10.150 255.255.255.0
Class-B(config-if)#no shutdow

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up

Class-B(config-if)#end
```

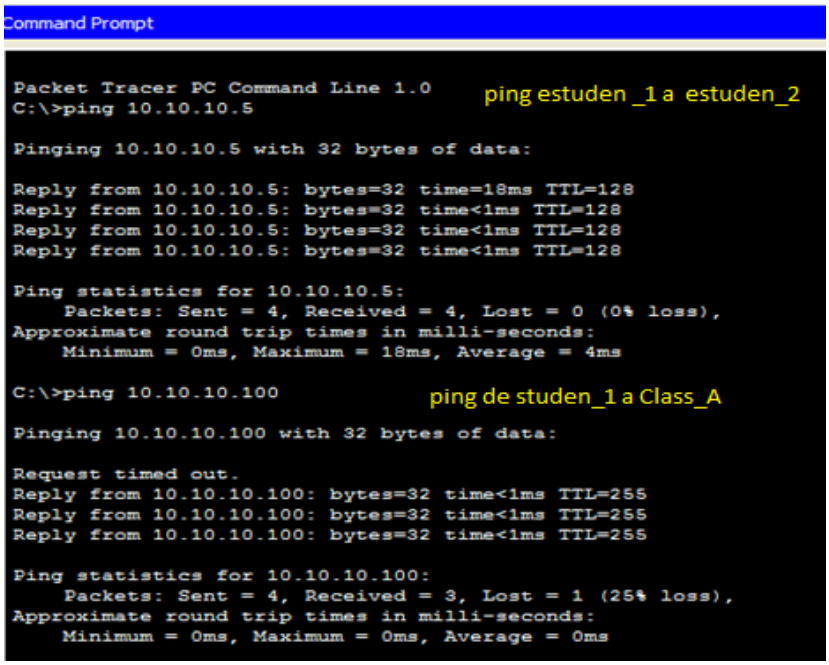
```
Class-A(config)#interface vlan 1
Class-A(config-if)#ip address 10.10.10.100 255.255.255.0
Class-A(config-if)#no shutdow

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Class-A(config-if)#end
Class-A#
```

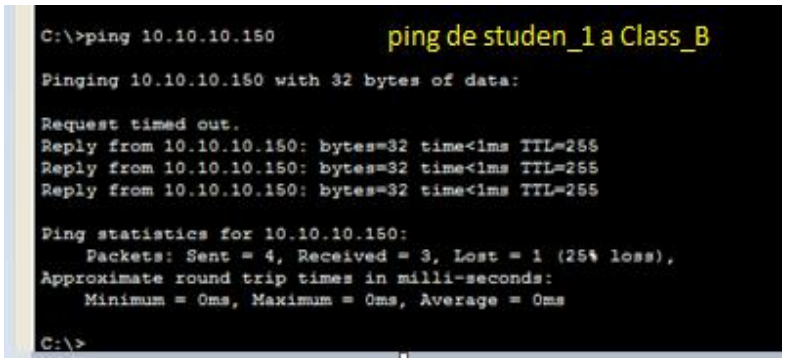
- Guarde las configuraciones.

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

```
Class-A#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Class-A#
```

Verifique la conectividad entre todos los dispositivos.


Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.5
ping estuden _1 a estuden_2
Pinging 10.10.10.5 with 32 bytes of data:
Reply from 10.10.10.5: bytes=32 time=18ms TTL=128
Reply from 10.10.10.5: bytes=32 time<1ms TTL=128
Reply from 10.10.10.5: bytes=32 time<1ms TTL=128
Reply from 10.10.10.5: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 18ms, Average = 4ms
C:\>ping 10.10.10.100
ping de studen_1 a Class_A
Pinging 10.10.10.100 with 32 bytes of data:
Request timed out.
Reply from 10.10.10.100: bytes=32 time<1ms TTL=255
Reply from 10.10.10.100: bytes=32 time<1ms TTL=255
Reply from 10.10.10.100: bytes=32 time<1ms TTL=255
Ping statistics for 10.10.10.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms


C:\>ping 10.10.10.150
ping de studen_1 a Class_B
Pinging 10.10.10.150 with 32 bytes of data:
Request timed out.
Reply from 10.10.10.150: bytes=32 time<1ms TTL=255
Reply from 10.10.10.150: bytes=32 time<1ms TTL=255
Reply from 10.10.10.150: bytes=32 time<1ms TTL=255
Ping statistics for 10.10.10.150:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

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.

Notas para el instructor

La siguiente información se incluye solo en la versión para el instructor.

En esta actividad, se utilizan variables que se generan aleatoriamente cada vez que se abre la actividad o se hace clic en el botón de Reset Activity. Si bien en las tablas que se encuentran a continuación se muestra la asignación de nombres de dispositivos a esquemas de direcciones específicos, los nombres y las direcciones no se corresponden de manera exclusiva. Por ejemplo, un estudiante podría obtener los nombres de dispositivos presentados en la situación 1 con el direccionamiento que se muestra en la situación 2. Además, el estudiante recibirá una de tres versiones de la topología.

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

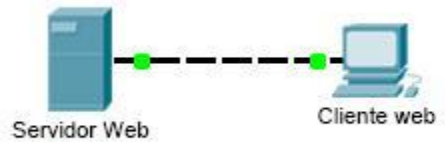
Escenario 3

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

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.

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

b. Seleccione HTTP de Event List Filters (Filtros de lista de eventos).

1) 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.

2) 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).

Packet Tracer: investigación de los modelos TCP/IP y OSI en acción

¿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

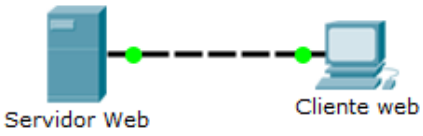
En esta simulación, se proporcionó un ejemplo de una sesión Web entre un cliente y un servidor en una red de área local (LAN). El cliente realiza solicitudes de servicios específicos que se ejecutan en el servidor. Se debe configurar el servidor para que escuche puertos específicos y detecte una solicitud de cliente.

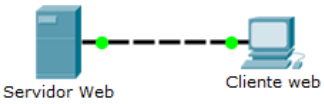
(Sugerencia: observe Layer 4 [Capa 4] en la ficha OSI Model para obtener información del puerto).

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.

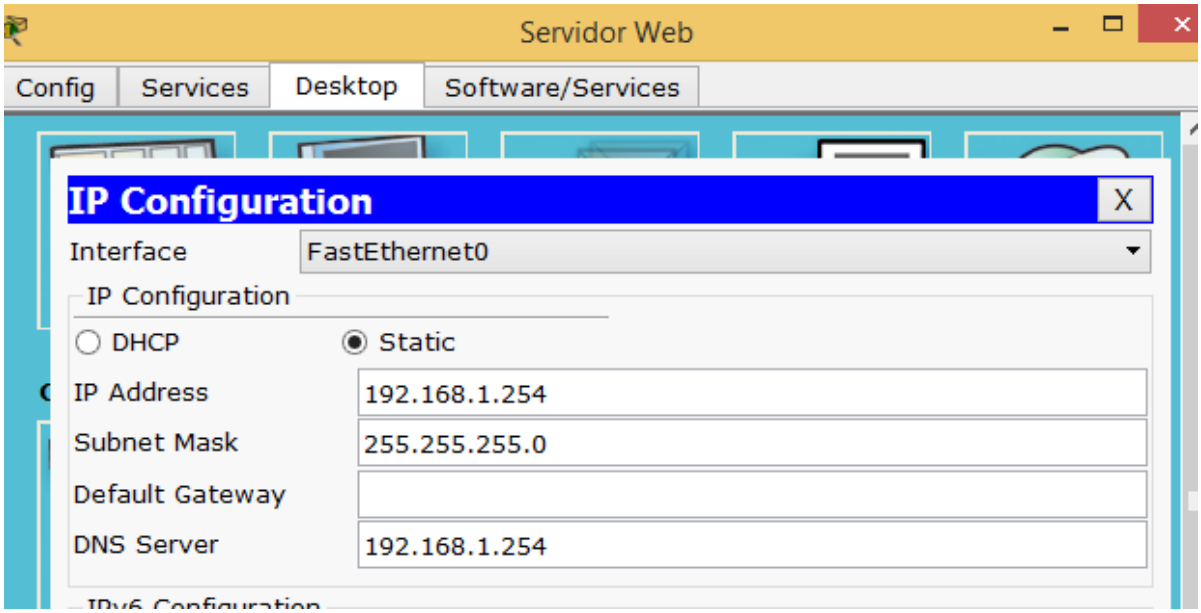
EVIDENCIAS

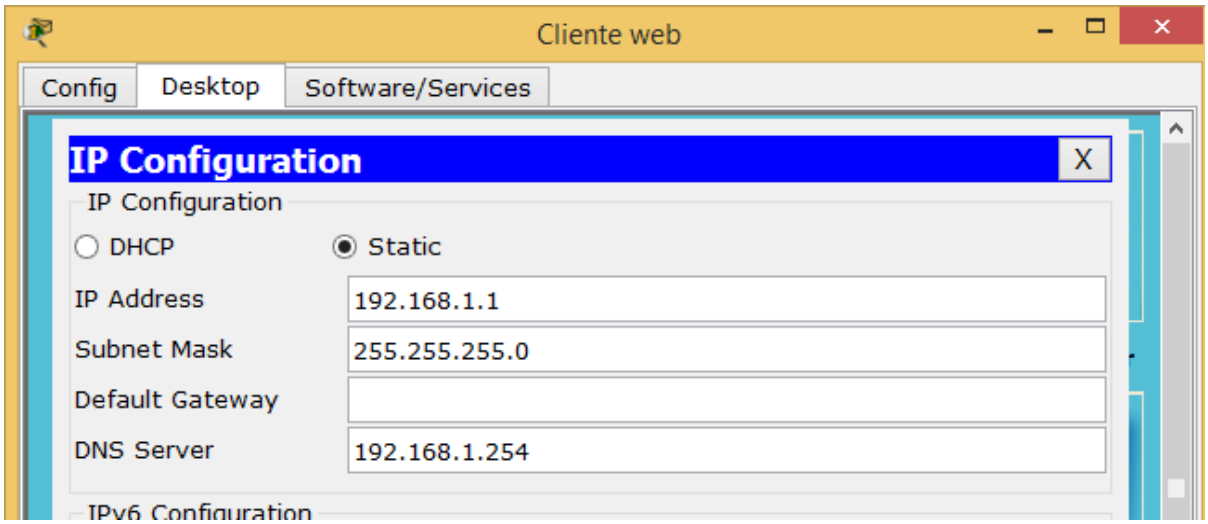




DU List Window

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)	

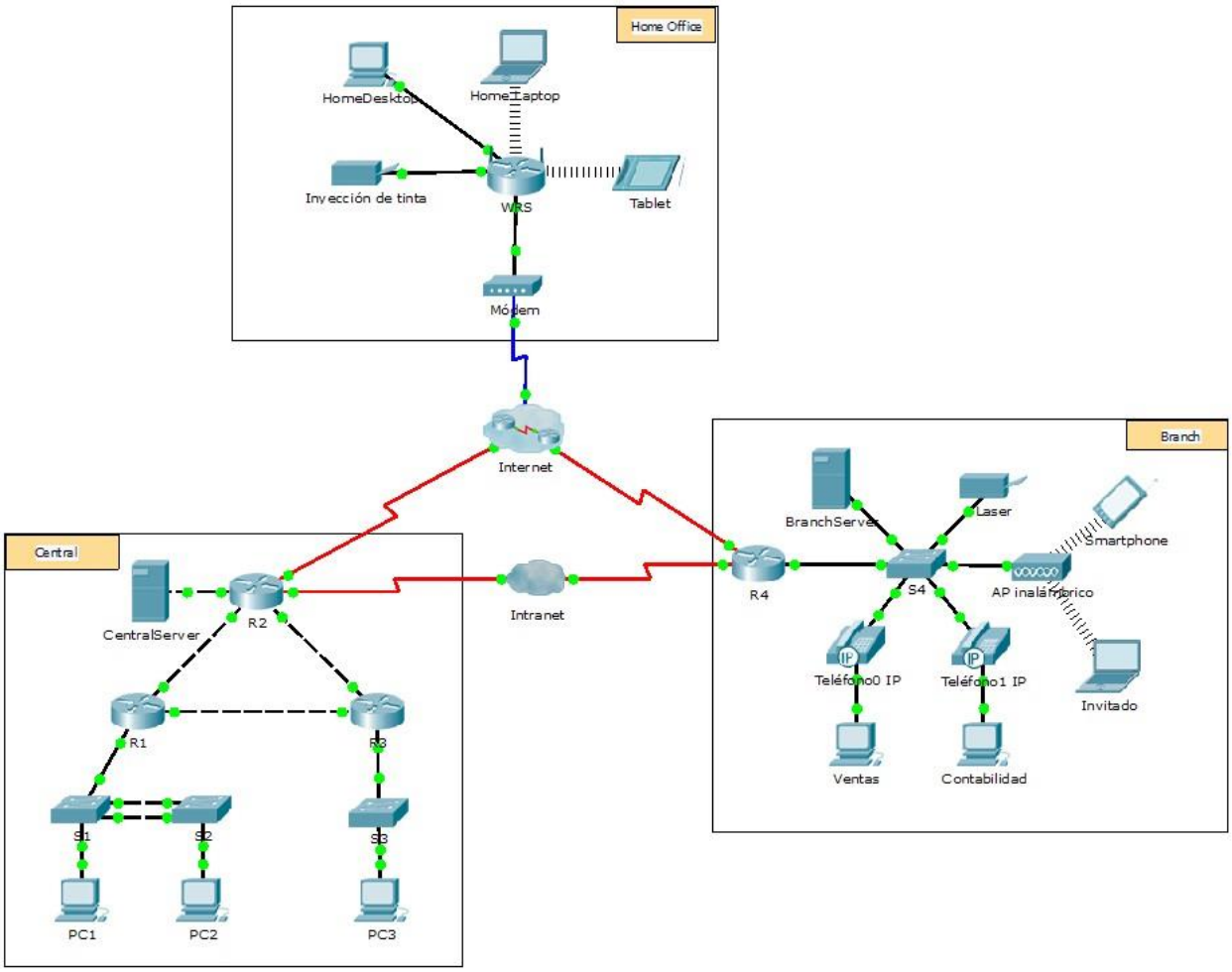

Servidor Web
Config
Services
Desktop
Software/Services
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.254
Subnet Mask
255.255.255.0
Default Gateway
DNS Server
192.168.1.254


Cliente web
Config
Desktop
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
DNS Server
192.168.1.254

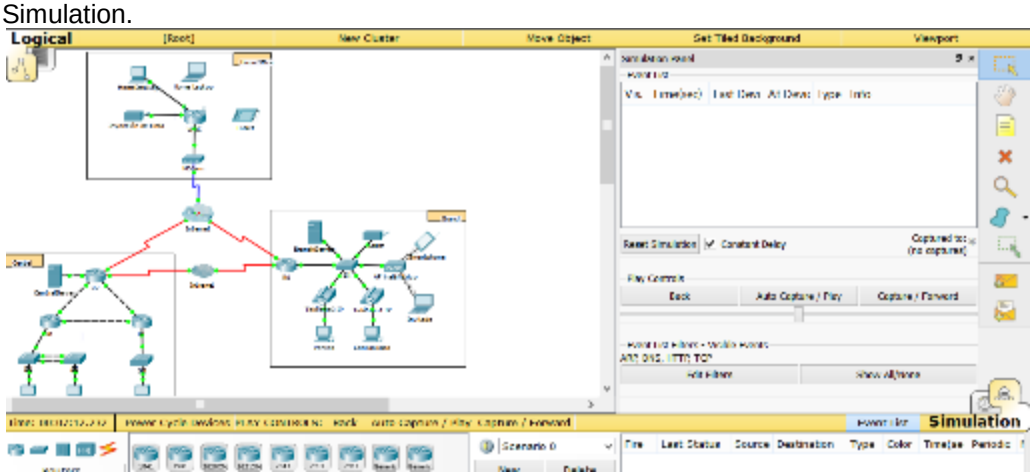
3.3.3.3 Packet Tracer - Explore a Network Instructions IG

Packet Tracer: Exploración de una red

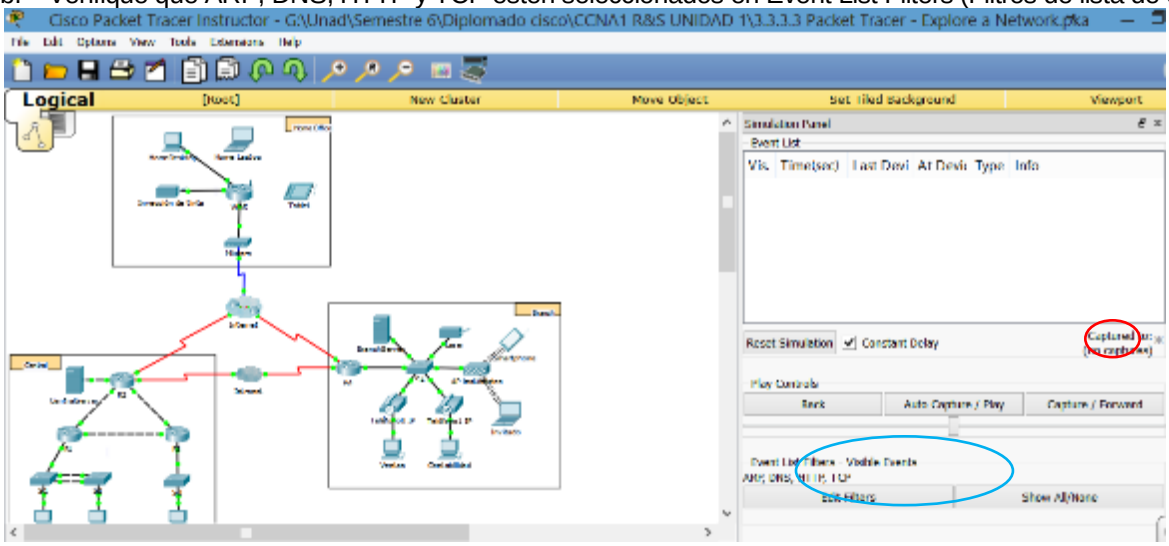
En esta actividad, se utiliza una topología compleja y un dominio del nivel superior ficticio (.pta) para evitar conflictos con la nomenclatura para Internet. Dado que PT no reenvía las solicitudes de DNS, se crearon las mismas entradas en cada servidor DNS para que el tráfico DNS pueda seguir siendo 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).



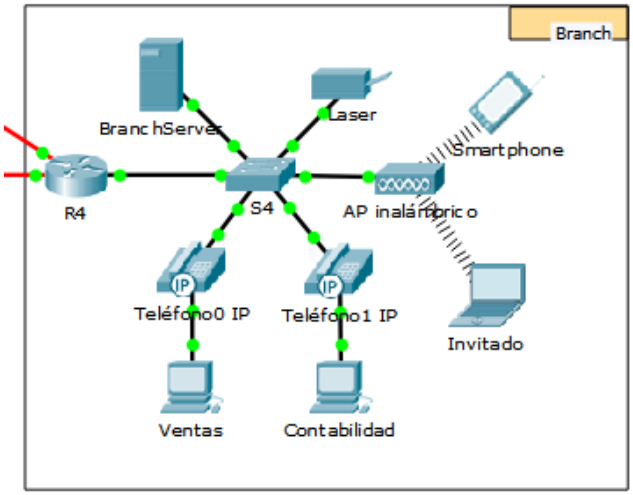
c. Mueva completamente hacia la derecha la barra deslizable que se encuentra debajo de los botones Play Controls (Controles de reproducción), Back, Auto Capture/Play, Capture/Forward (Retroceder, Captura/Reproducción automática, Capturar/avanzar).

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.

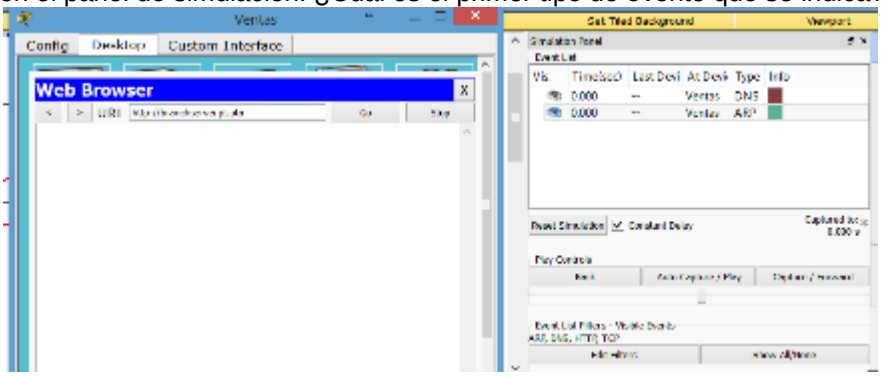
Nota: la topología se muestra en el panel de la izquierda del panel de simulación. Utilice las barras de desplazamiento para incorporar la ubicación Branch al panel, en caso necesario. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la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

Haga clic en Sales PC (PC de ventas) en el panel del extremo izquierdo.



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?

OSI Model | Outbound PDU Details

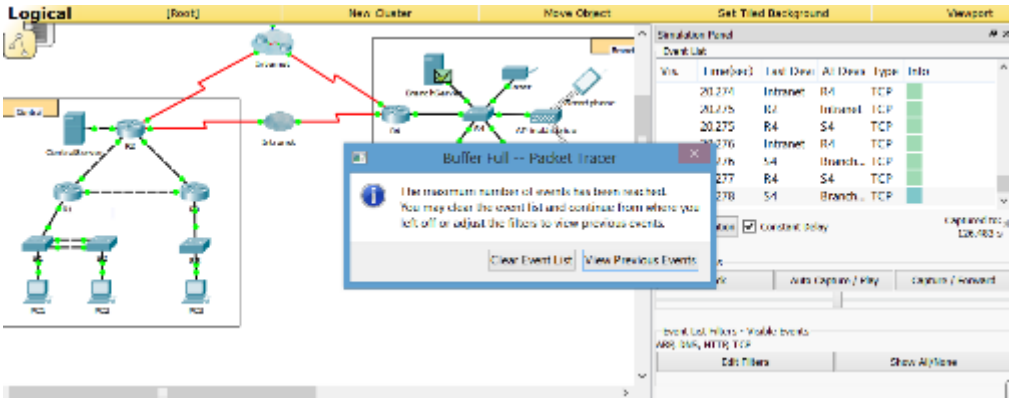
At Device: Ventas
Source: Ventas
Destination: 172.16.0.3

In Layers	Out Layers
Layer7	Layer 7: DNS
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 1025, Dst Port: 53
Layer3	Layer 3: IP Header Src. IP: 172.16.0.6, Dest. IP: 172.16.0.3
Layer2	Layer 2:
Layer1	Layer1

1. The DNS client sends a DNS query to the DNS server

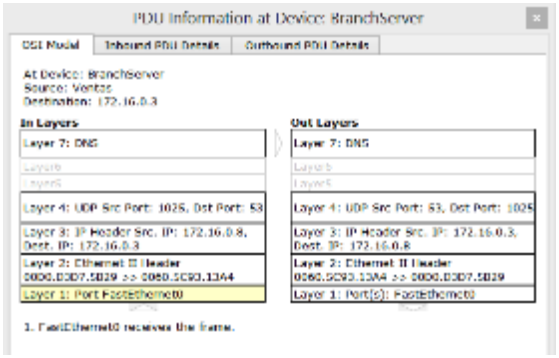
La información de capa 2, específicamente la dirección MAC de destino.

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



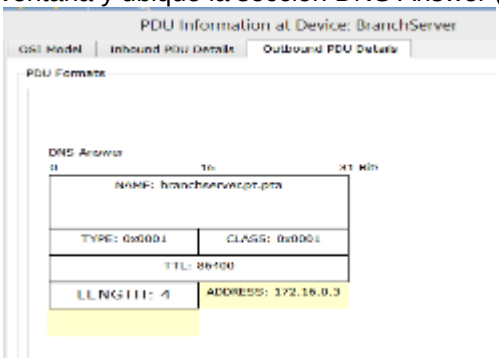
16 Dispositivos
Todos los dispositivos recibieron una solicitud de ARP.

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]).



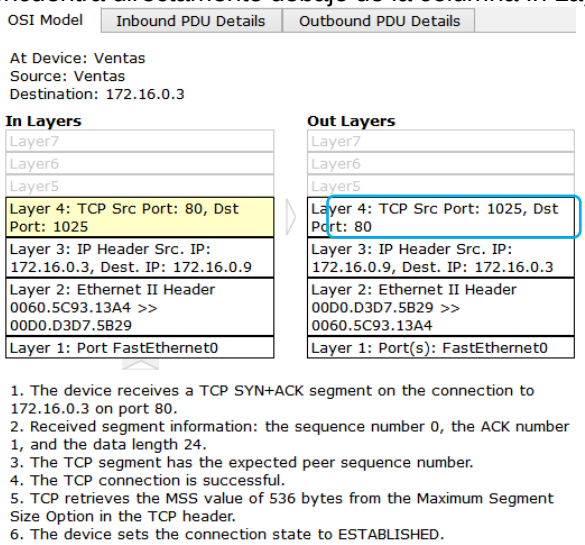
El servidor DNS recibe una consulta DNS. La consulta del nombre se resuelve de forma local.

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?

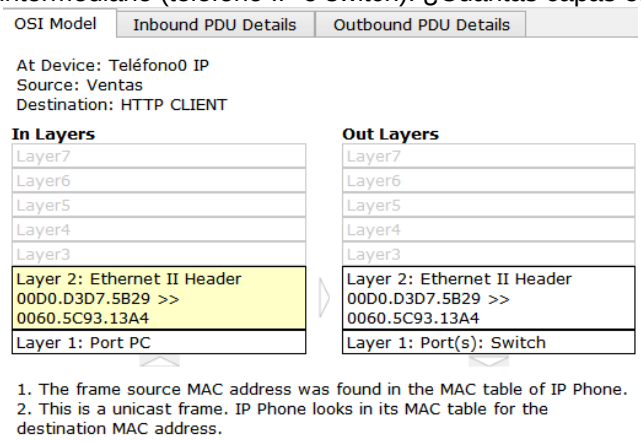


172.16.0.3, la dirección de Branchserver.

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? R//ESTABLISHED

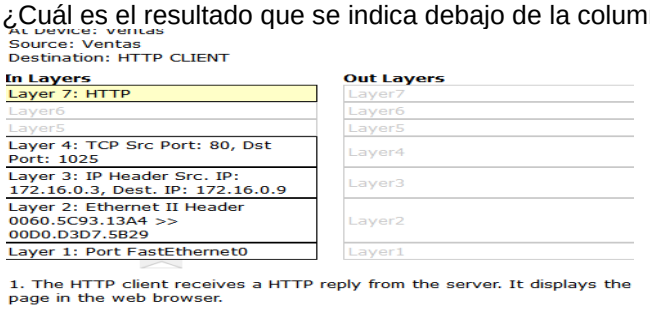


Los eventos siguientes son eventos de HTTP. Seleccione cualquiera de los eventos de HTTP en un dispositivo intermediario (teléfono IP o switch). ¿Cuántas capas están activas en uno de estos dispositivos y por qué?



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.

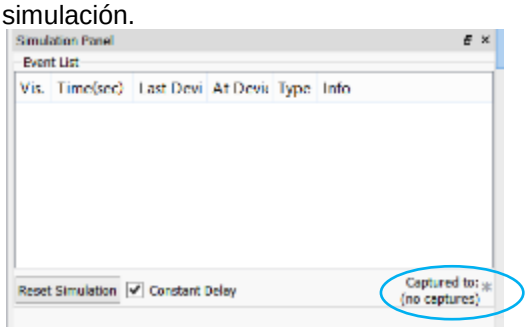
Parte 2: Examinar el tráfico de internetwork a la central

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.

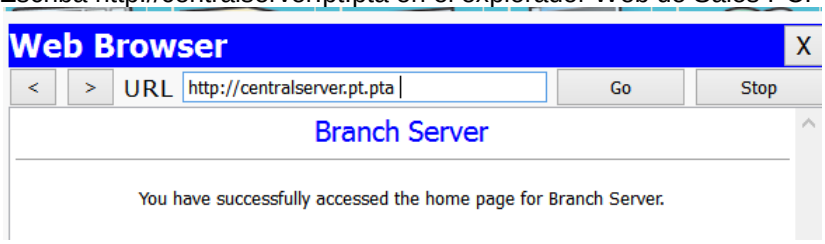
Paso 1: Configurar la captura de tráfico hacia el servidor Web de la central

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

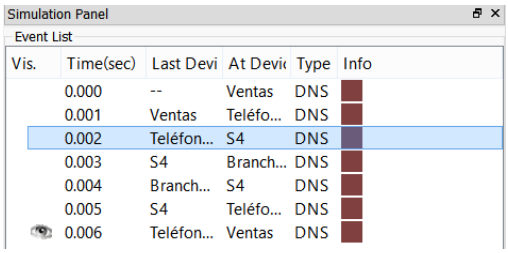
Haga clic en la opción Reset Simulation (Restablecer simulación), que se encuentra cerca del centro del panel de simulación.



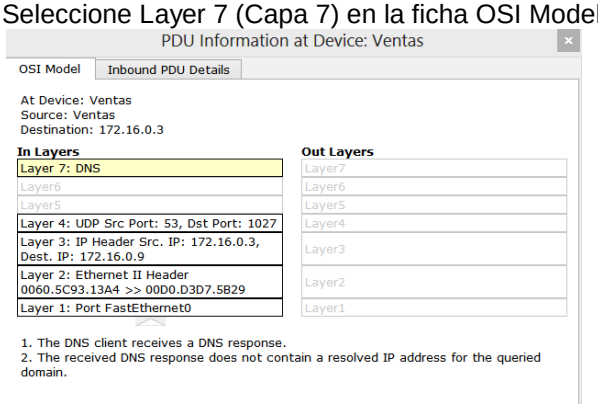
Escriba http://centralserver.pt.pta en el explorador Web de Sales PC.



Haga clic en Auto Capture/Play (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en View Previous Events (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es DNS y que no hay entradas de ARP antes de comunicarse con Branchserver. Según lo aprendido hasta ahora, ¿a qué se debe esto?

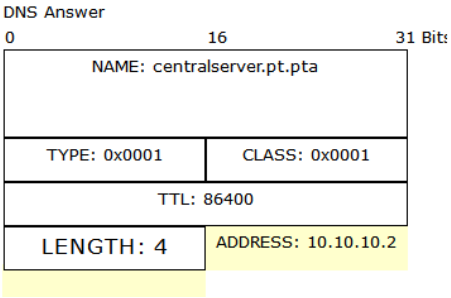


Sales PC ya conoce la dirección MAC del servidor DNS.Haga clic en el último evento de DNS en la columna Info. Seleccione Layer 7 (Capa 7) en la ficha OSI Model.



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.

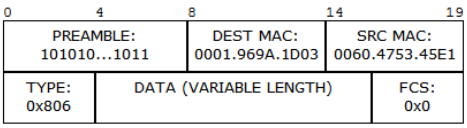
f. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante). Desplácese hasta la sección



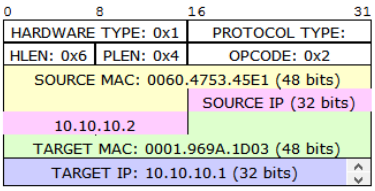
DNS ANSWER (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta?
10.10.10.2.

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?

Ethernet II

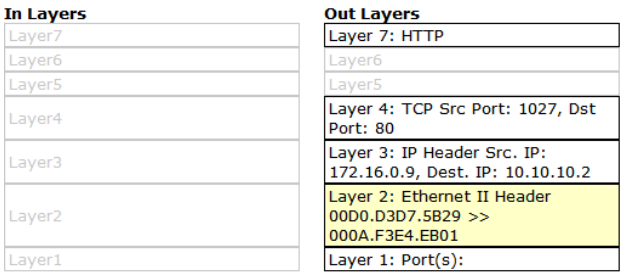


ARP



El router R4, el dispositivo de gateway.

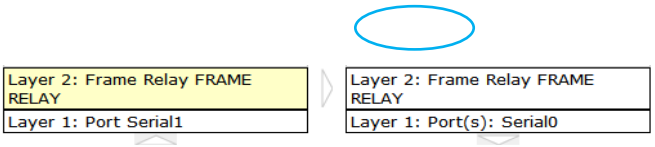
Los eventos siguientes son eventos de TCP, que nuevamente se preparan para establecer un canal de comunicación. Busque el primer evento de HTTP en Event List. Haga clic en el cuadro coloreado del evento de HTTP. Resalte Layer 2 (Capa 2) en la ficha OSI Model. ¿Qué se puede determinar sobre la dirección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



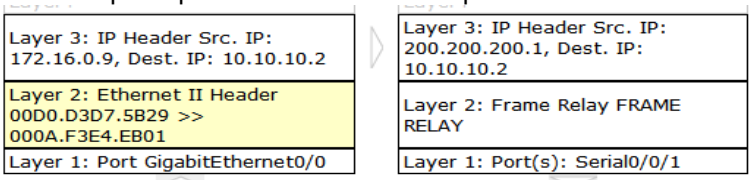
1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

Es la dirección MAC del router R4.

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?

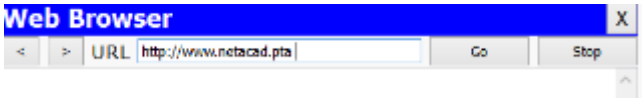


1. The cloud looks up the DLCI number on the frame for the connected sublink.

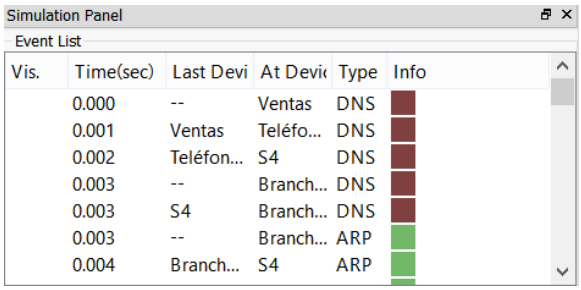


1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.

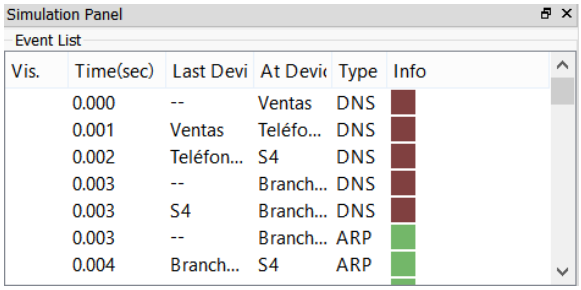
Frame Relay FRAME RELAY.
Observe que solo hay dos capas activas, en oposición a lo que sucede cuando se atraviesa el router. Esta es una conexión WAN, y se analizará en otro curso.
Parte 3: Examinar el tráfico de Internet desde la sucursal
En la parte 3 de esta actividad, borrará los eventos y comenzará una nueva solicitud Web que usará Internet.
Paso 1: Configurar la captura de tráfico hacia un servidor Web de Internet
a. Cierre todas las ventanas de información de PDU abiertas.
b. Haga clic en la opción Reset Simulation, que se encuentra cerca del centro del panel de simulación.
Escriba http://www.netacad.pta en el explorador Web de Sales PC.



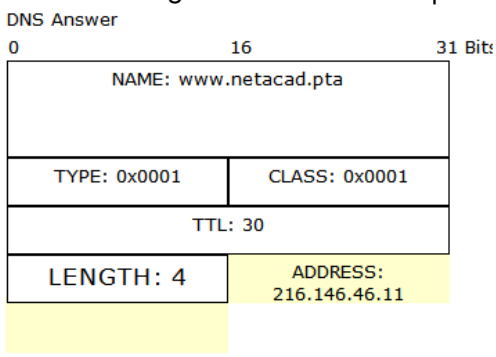
c. Haga clic en Auto Capture/Play (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en View Previous Events (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe que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



Hay muchos más eventos de DNS. Dado que la entrada de DNS no es local, se reenvía hacia un servidor en Internet.
d. Observe algunos de los dispositivos a través de los que se transfieren los eventos de DNS en el camino hacia un servidor DNS. ¿Dónde se encuentran estos dispositivos? En la nube de Internet. Se debe mostrar a los estudiantes que esos dispositivos se pueden ver haciendo clic en la nube y luego en el enlace Back (Atrás) para regresar.



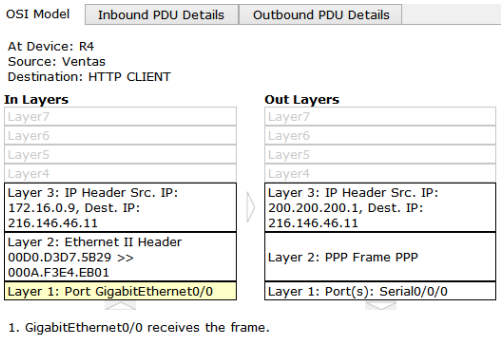
e. Haga clic en el último evento de DNS. Haga clic en la ficha Inbound PDU Details y desplácese hasta la última sección DNS Answer. ¿Cuál es la dirección que se indica para **www.netacad.pta**?

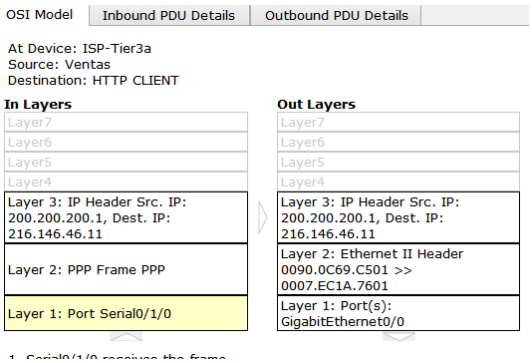


216.146.46.11

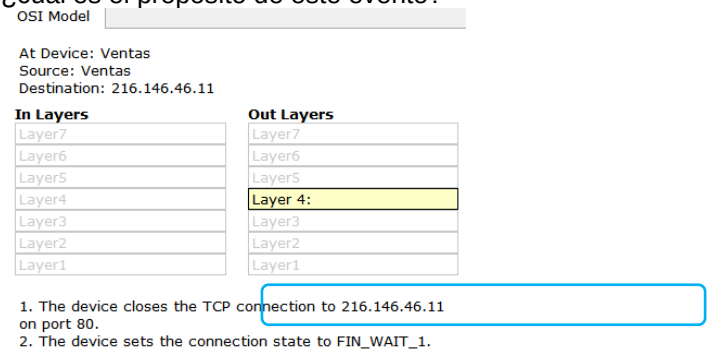
f. Cuando los routers mueven el evento de HTTP a través de la red, hay tres capas activas en In Layers y Out Layers en la ficha OSI Model. Sobre la base de esa información, ¿cuántos routers se atraviesan?

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



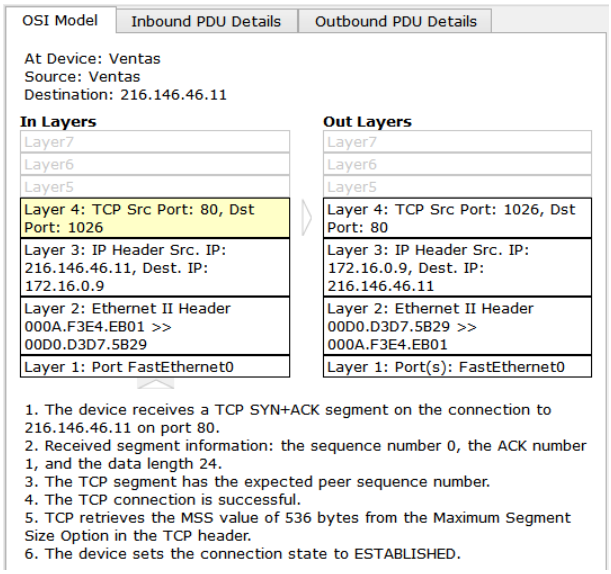


g. Haga clic en el evento de TCP anterior al último evento de HTTP. Según la información que se muestra, ¿cuál es el propósito de este evento?



Cerrar la conexión TCP a 216.146.46.11.

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


OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Ventas
Source: Ventas
Destination: 216.146.46.11
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1026
Layer 3: IP Header Src. IP: 216.146.46.11, Dest. IP: 172.16.0.9
Layer 2: Ethernet II Header 000A.F3E4.EB01 >> 00D0.D3D7.5B29
Layer 1: Port FastEthernet0
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 1026, Dst Port: 80
Layer 3: IP Header Src. IP: 172.16.0.9, Dest. IP: 216.146.46.11
Layer 2: Ethernet II Header 00D0.D3D7.5B29 >> 000A.F3E4.EB01
Layer 1: Port(s): FastEthernet0
1. The device receives a TCP SYN+ACK segment on the connection to 216.146.46.11 on port 80.
2. Received segment information: the sequence number 0, the ACK number 1, and the data length 24.
3. The TCP segment has the expected peer sequence number.
4. The TCP connection is successful.
5. TCP retrieves the MSS value of 536 bytes from the Maximum Segment Size Option in the TCP header.
6. The device sets the connection state to ESTABLISHED.

4.2.4.5 Packet Tracer: Conexión de una LAN por cable y una LAN inalámbrica

Topología

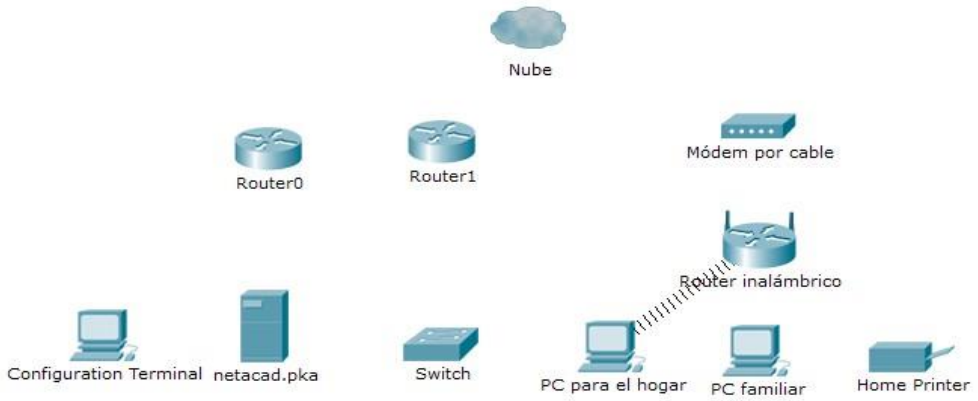


Tabla de direccionamiento

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

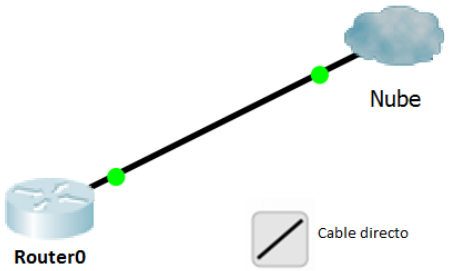
Al trabajar en Packet Tracer (un entorno de laboratorio o un contexto empresarial), debe saber cómo seleccionar el cable adecuado y cómo conectar correctamente los dispositivos. En esta actividad se analizarán configuraciones de dispositivos en el Packet Tracer, se seleccionarán los cables adecuados 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

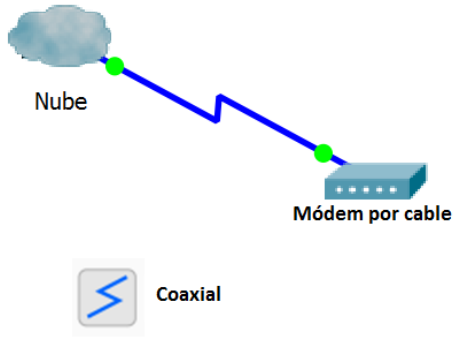
a. En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las conexiones disponibles.

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.

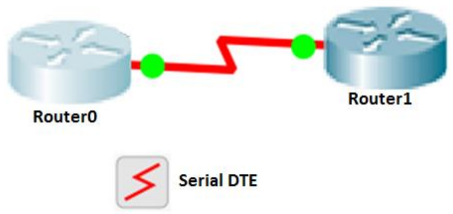


Parte 2: Conectar el Router0

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.

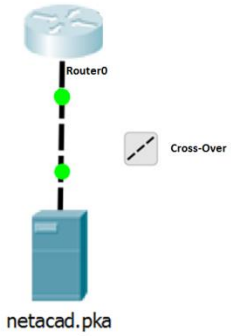
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.



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.

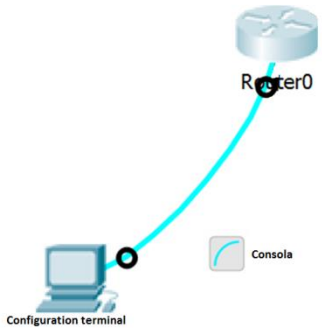
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.



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

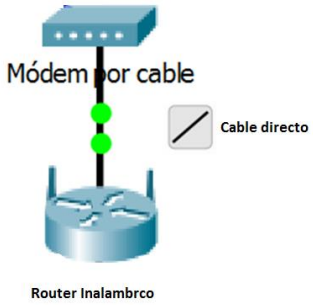
Paso 1: Conectar el Router1 al switch

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.

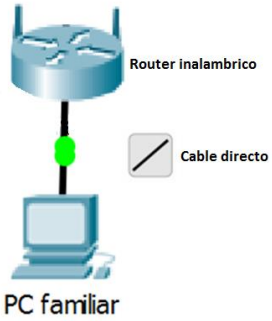
Paso 2: Conectar el módem por cable al router inalámbrico

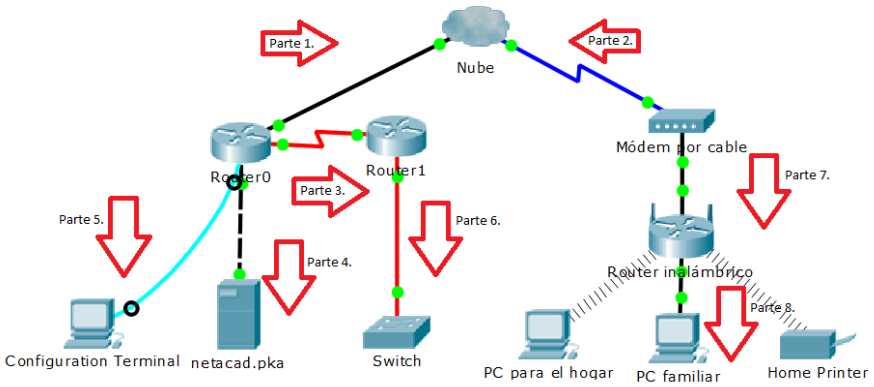
Elija el cable adecuado para conectar el Puerto1 del módem al puerto de Internet del router inalámbrico. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.



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.

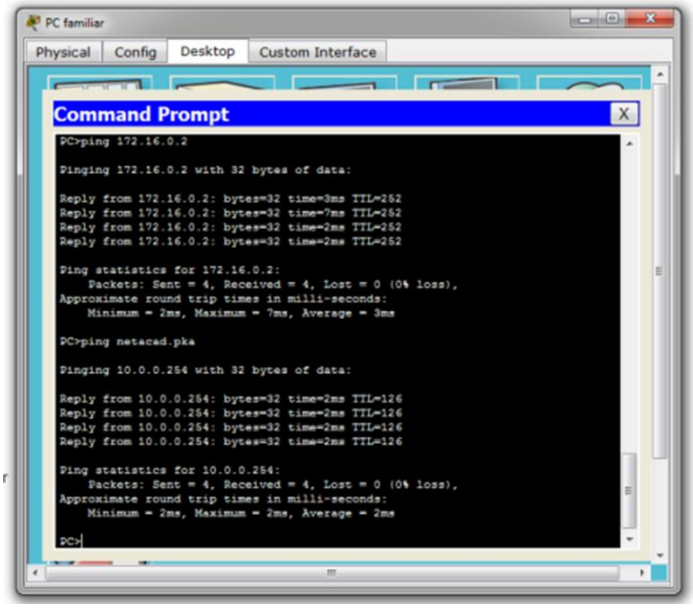




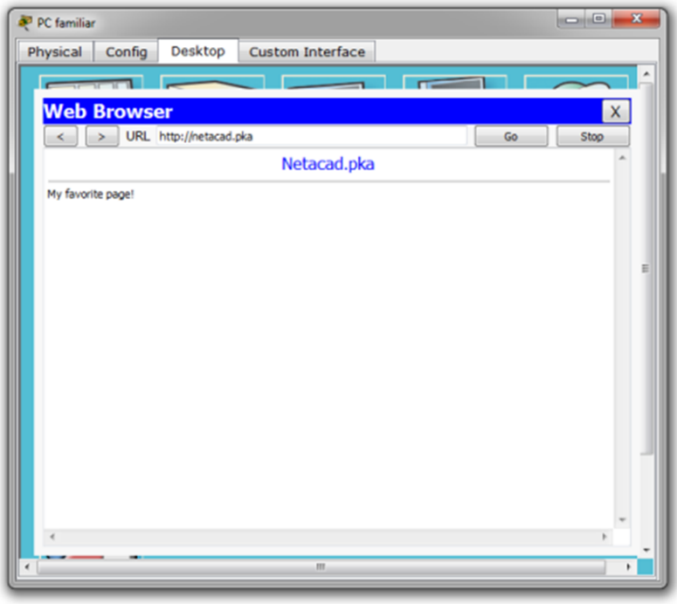
Parte 4: Verificar las conexiones

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.

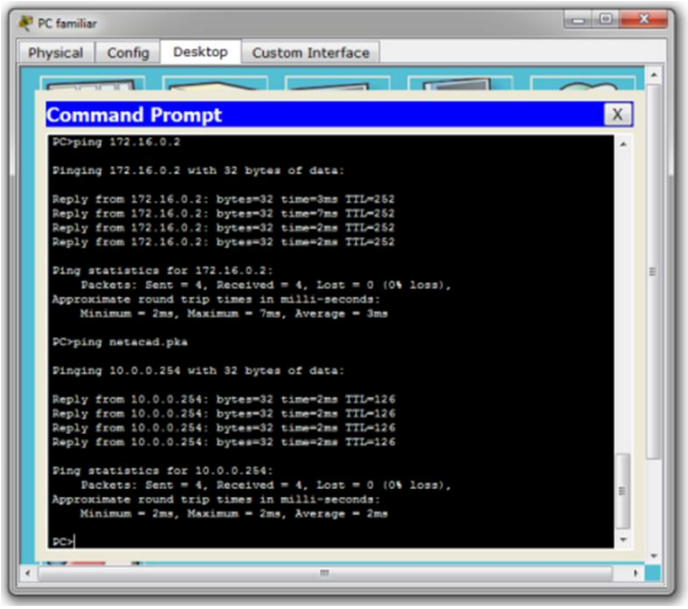


b. Abra el explorador Web e introduzca dirección Web http://netacad.pka.



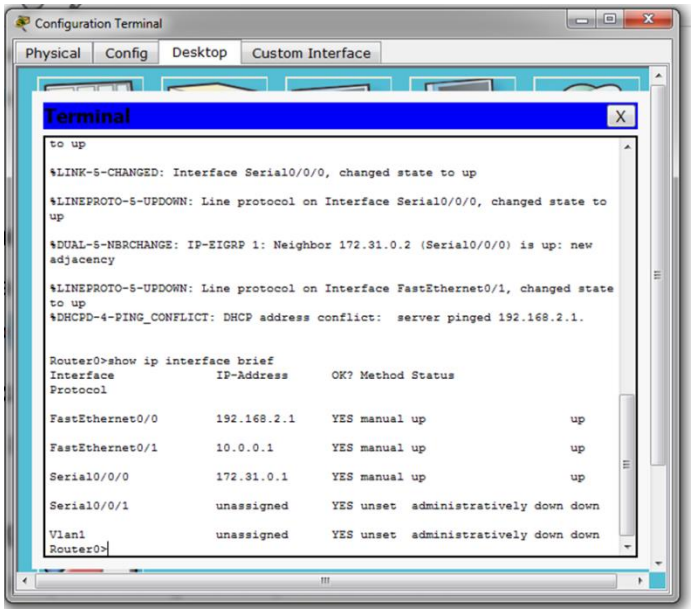
Paso 2: Hacer ping al switch desde la PC doméstica

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



Paso 3: Abrir el Router0 desde la terminal de configuración

a. Abra la terminal de la terminal de configuración y acepte la configuración predeterminada.
b. Presione Entrar para ver el símbolo del sistema del Router0.
c. Escriba show ip interface brief para ver el estado de las interfaces.



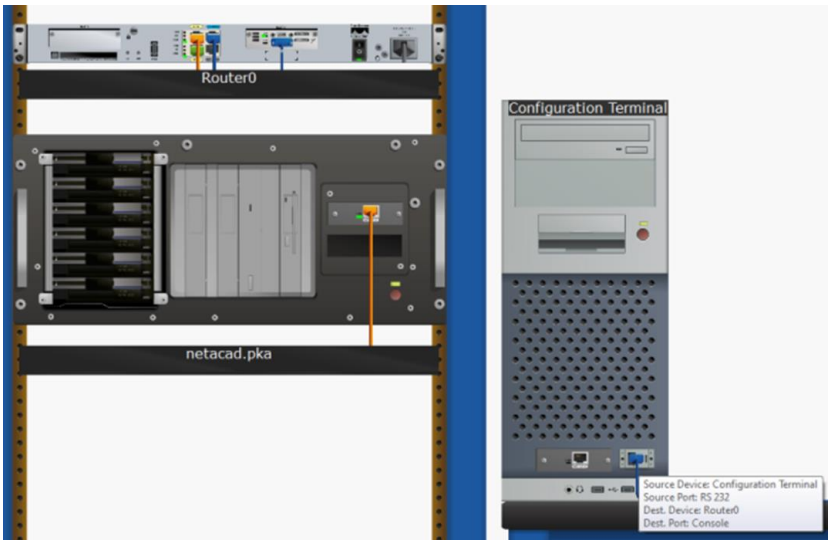
Parte 5: Examinar la topología física

Paso 1: Examinar la nube

d. Haga clic en la ficha Physical Workspace (Área de trabajo física) o presione Mayús + P y Mayús + L para alternar entre las áreas de trabajo lógicas y físicas.
e. Haga clic en el ícono Home City (Ciudad de residencia).
f. Haga clic en el ícono Cloud (Nube). ¿Cuántos cables están conectados al switch en el bastidor azul?
R// 2.
g. Haga clic en Back (Atrás) para volver a Home City (Ciudad de residencia).

Paso 2: Examinar la red principal

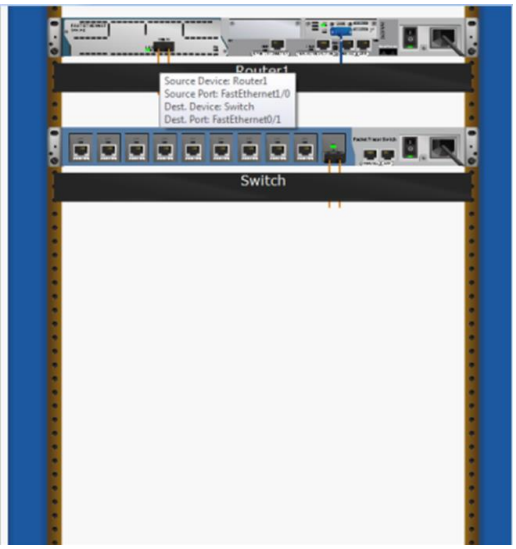
h. Haga clic en el ícono Primary Network (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul? La terminal de configuración.



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 están en pares una para transmisión y el otro para la recepción de la información.



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?

Distancia máxima red inalámbrica.

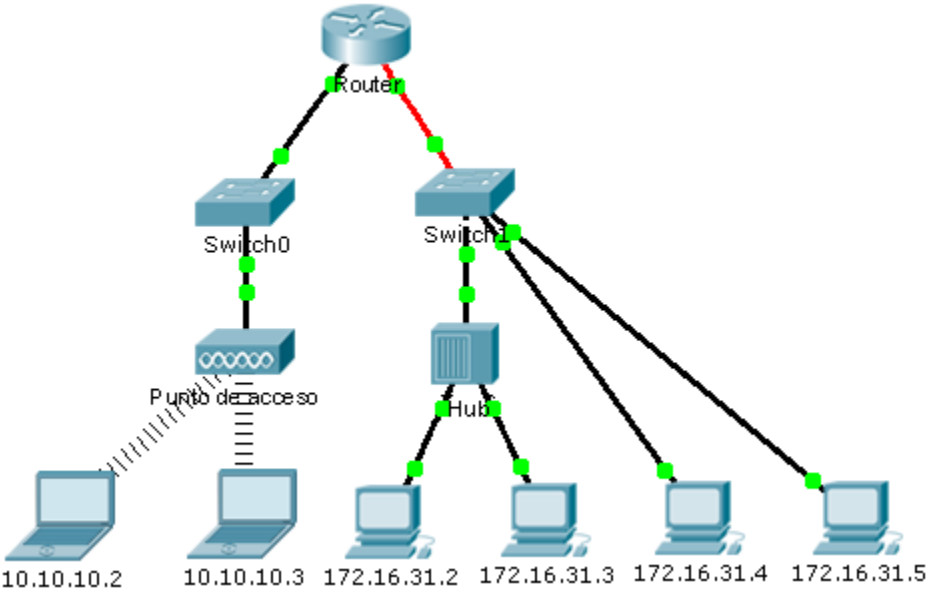
m. Haga clic en el ícono Home Network (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo?

Las redes domésticas no siempre llevan bastidores.

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

5.1.4.4 Packet Tracer: 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.

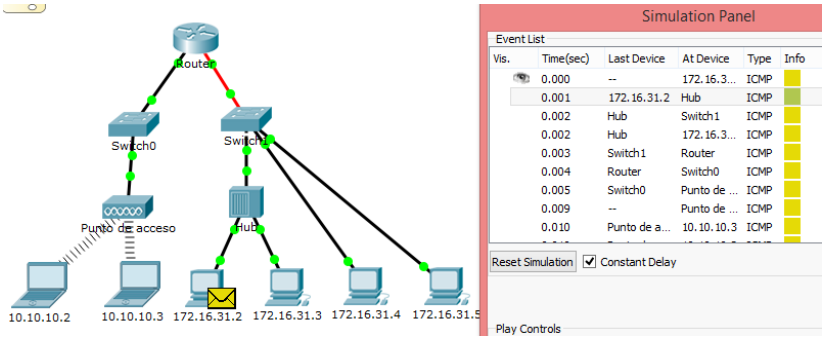
Parte 1: Recopilar información de la PDU
Nota: revise las preguntas de reflexión de la parte 2 antes de continuar con la parte 1. Le darán una idea de los tipos de información que debe recopilar.

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:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time=1ms TTL=127
Reply from 10.10.10.3: bytes=32 time<1ms TTL=127
Reply from 10.10.10.3: bytes=32 time=23ms TTL=127
Reply from 10.10.10.3: bytes=32 time=12ms TTL=127

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 23ms, Average = 9ms
```

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:

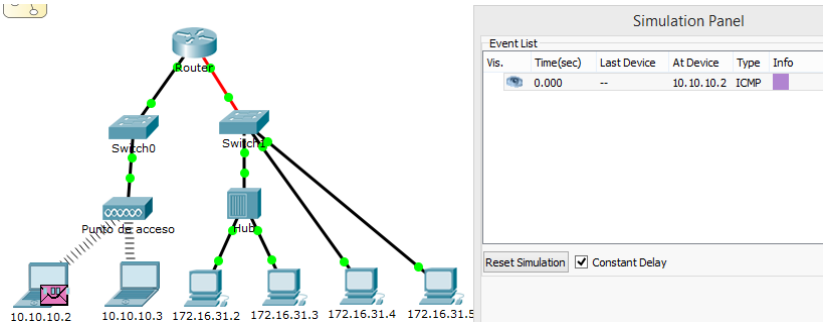
Formato de hoja de cálculo de ejemplo

Prueba	En dispositivo	Dest MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 10.10.10.3	172.16.31.2	00D0:BA8E:	000C:85CC:1	172.16.31.	10.10.10.
	Hub	00D0:BA8E:	000C:85CC:1	172.16.31.	10.10.10.
	Switch1	00D0:BA8E:	000C:85CC:1	172.16.31.	--
	Router	0060:4706:5	00D0:588C:24	172.16.31.	10.10.10.
	Switch0	0060:4706:5	00D0:588C:24	172.16.31.	--
	Punto de acceso	--	--	--	--
	10.10.10.3	0060:4706:5	00D0:588C:24	172.16.31.	10.10.10.

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

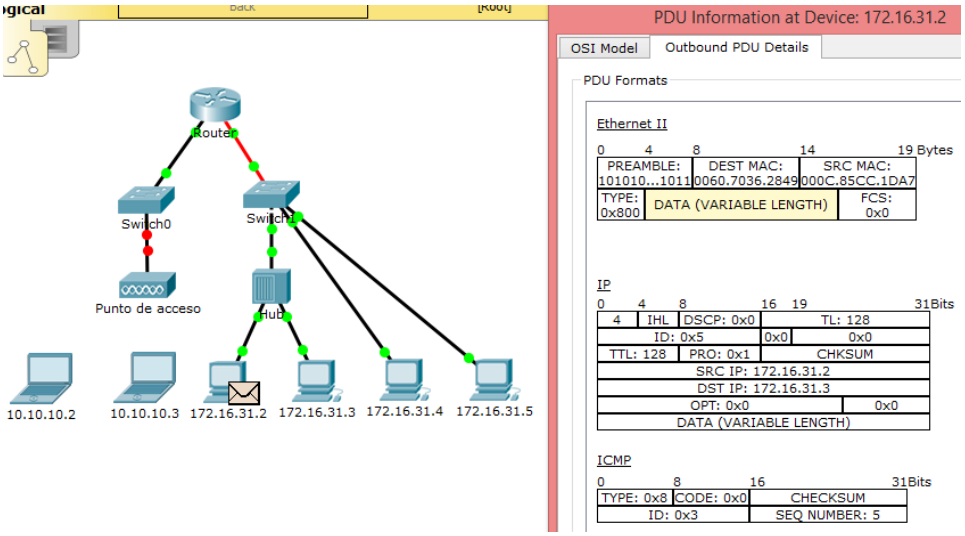
```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time=32ms TTL=128
Reply from 10.10.10.3: bytes=32 time=17ms TTL=128
Reply from 10.10.10.3: bytes=32 time=9ms TTL=128
Reply from 10.10.10.3: bytes=32 time=16ms TTL=128

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 32ms, Average = 18ms

C:\>
```



Prueba	En dispositivo	Dest MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 10.10.10.2 a 10.10.10.3	10.10.10.2			10.10.10.2	10.10.10.3
	Punto de acceso			10.10.10.2	10.10.10.3
	Switch0	0060.4706.572B	0060.2F84.4AB6	10.10.10.2	10.10.10.3
	Punto de acccceso			10.10.10.2	10.10.10.3
	10.10.10.3			10.10.10.3	10.10.10.2
	Punto de acceso	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

- Ping de 172.16.31.4 a 172.16.31.5

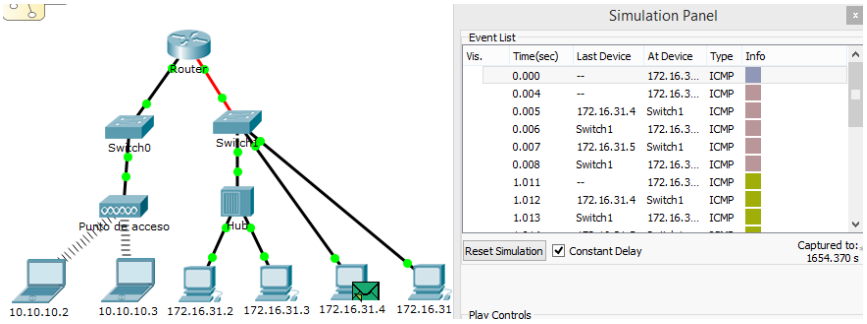
```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time=1ms TTL=128
Reply from 172.16.31.3: bytes=32 time=1ms TTL=128
Reply from 172.16.31.3: bytes=32 time<1ms TTL=128
Reply from 172.16.31.3: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.31.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



Prueba	En dispositivo	Dest 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
	172.16.31.3	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2

- Ping de 172.16.31.4 a 10.10.10.2

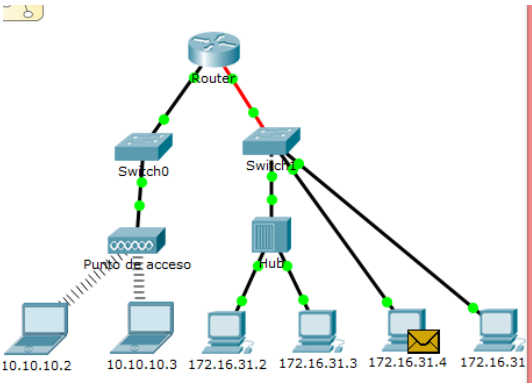
```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.31.5

Pinging 172.16.31.5 with 32 bytes of data:

Reply from 172.16.31.5: bytes=32 time<1ms TTL=128
Reply from 172.16.31.5: bytes=32 time<1ms TTL=128
Reply from 172.16.31.5: bytes=32 time<1ms TTL=128
Reply from 172.16.31.5: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

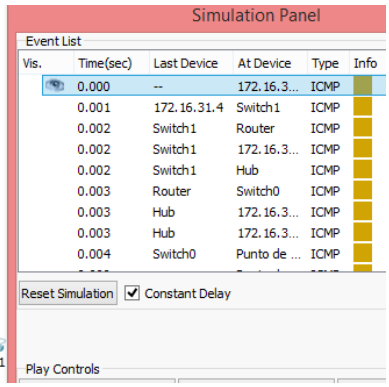


Prueba	En dispositivo	Dest MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.4 a 172.16.31.5	172.16.31.4			172.16.31.4	172.16.31.5
	Switch1	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5
	172.16.31.5	000C.CF0B.BC80	00D0.D311.C788	172.16.31.5	172.16.31.4

- Ping de 172.16.31.3 a 10.10.10.2

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=17ms TTL=127
Reply from 10.10.10.2: bytes=32 time=14ms TTL=127
Reply from 10.10.10.2: bytes=32 time=16ms TTL=127
Reply from 10.10.10.2: bytes=32 time=20ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 20ms, Average = 16ms
```

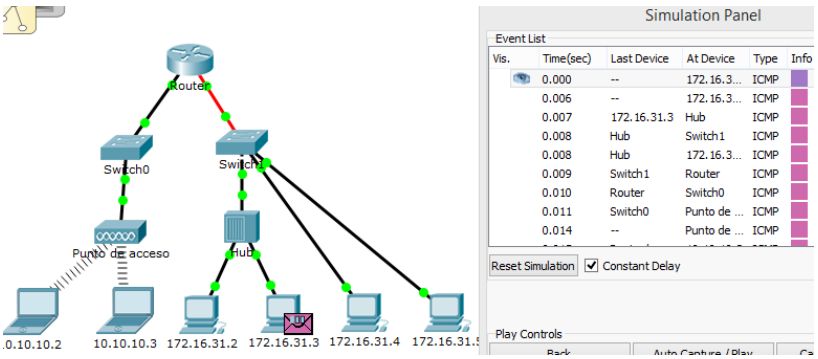




Prueba	En dispositivo	Dest MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.4 a 10.10.10.2	172.16.31.4	00D0.BA8E.741A	000C.CF0B.BC80	172.16.31.4	10.10.10.2
	Switch1	00D0.BA8E.741A	000C.CF0B.BC80	172.16.31.4	10.10.10.2
	Router	0060.2F84.4AB6	00D0.588C.2401	172.16.31.4	10.10.10.2
	Switch0	0060.2F84.4AB6	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

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=23ms TTL=127
Reply from 10.10.10.2: bytes=32 time=18ms TTL=127
Reply from 10.10.10.2: bytes=32 time=16ms TTL=127
Reply from 10.10.10.2: bytes=32 time=18ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 23ms, Average = 18ms

C:\>
```



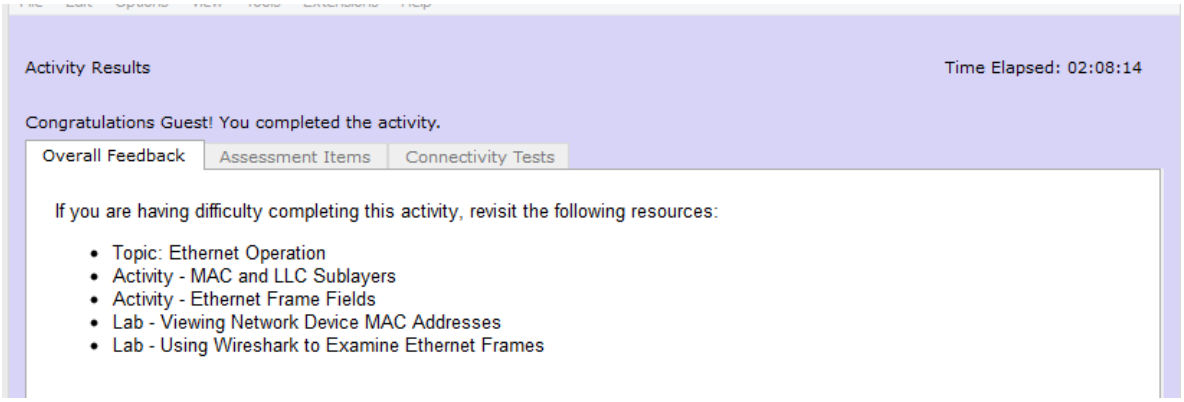
Prueba	En dispositivo	Dest MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.3 a 10.10.10.2	172.16.31.3	00D0.BA8E.741A	0060.7036.2849	172.16.31.3	10.10.10.2
	Hub	00D0.BA8E.741A	0060.7036.2849	172.16.31.3	10.10.10.2
	Switch1	00D0.BA8E.741A	0060.7036.2849	172.16.31.3	10.10.10.2
	Router	0060.2F84.4AB6	00D0.588C.2401	172.16.31.3	10.10.10.2
	Switch0	0060.2F84.4AB6	00D0.588C.2401	172.16.31.3	10.10.10.2
	Punto de acceso				
	10.10.10.2			10.10.10.2	172.16.31.3

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? Sí, 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? Sí. 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? 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.

Resultados de la actividad



5.2.1.7 Packet Tracer: Revisión de la tabla ARP

Topología

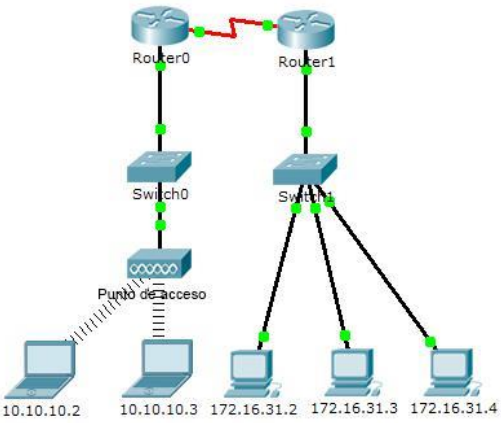


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	No aplicable	No aplicable
Router1	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

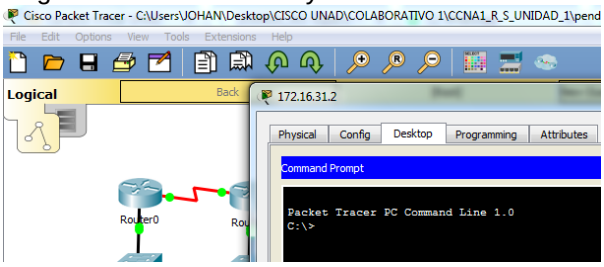
Información básica

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.

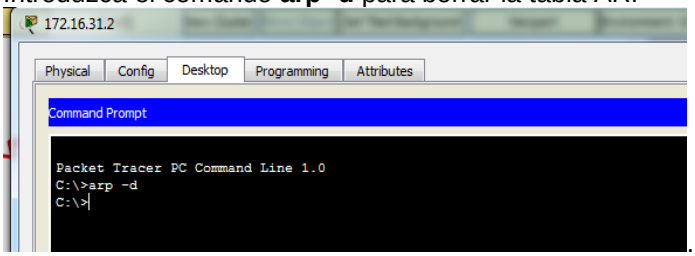
Parte 1: Examinar una solicitud de ARP

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

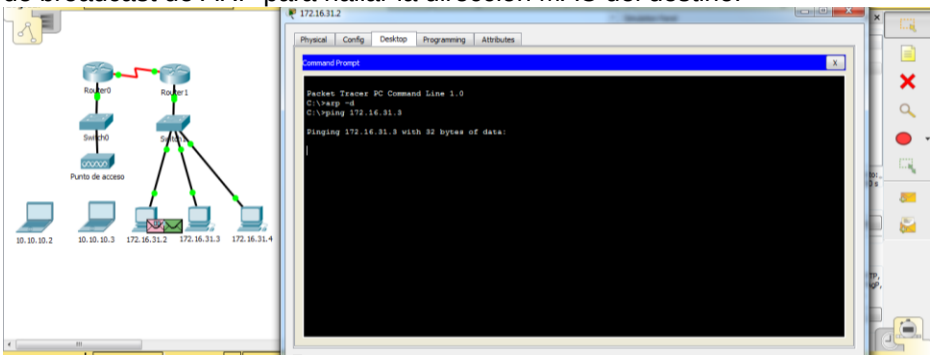
Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.



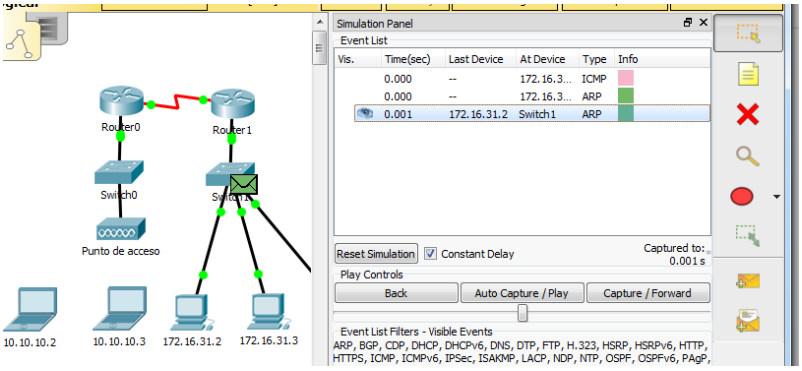
Introduzca el comando **arp -d** para borrar la tabla ARP



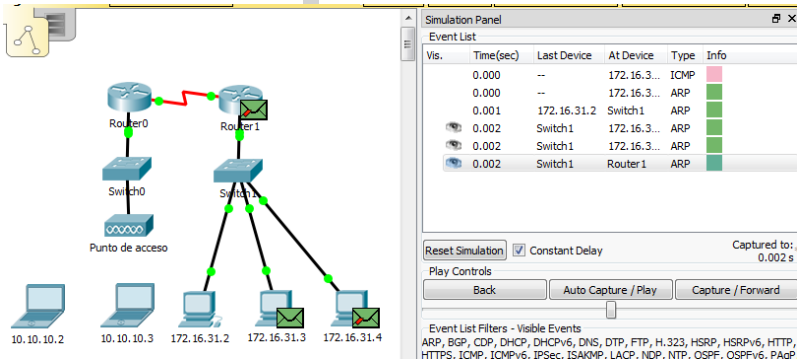
Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3**. Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.



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

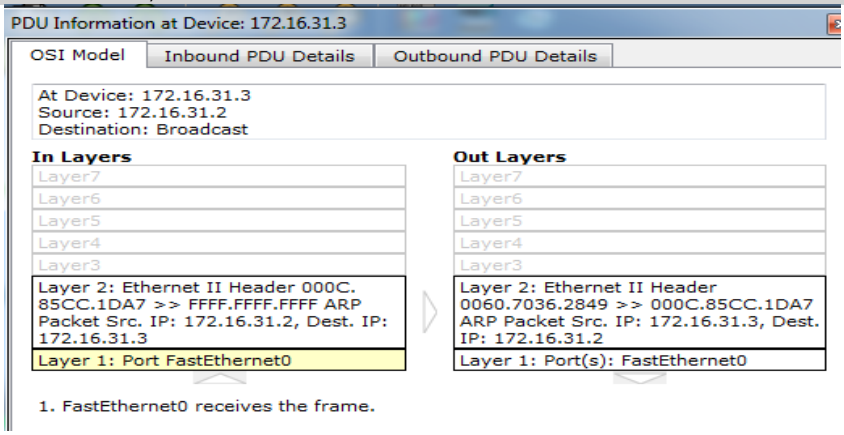


Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**? 3

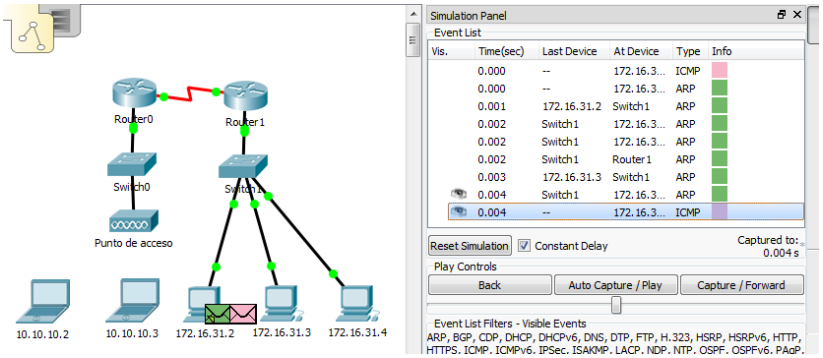


¿Cuál es la dirección IP del dispositivo que aceptó la PDU? 172.16.31.3

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.

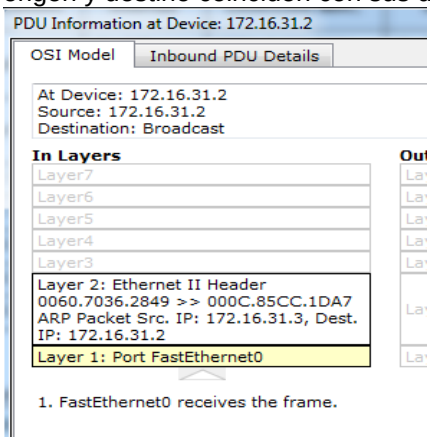


Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP? 1

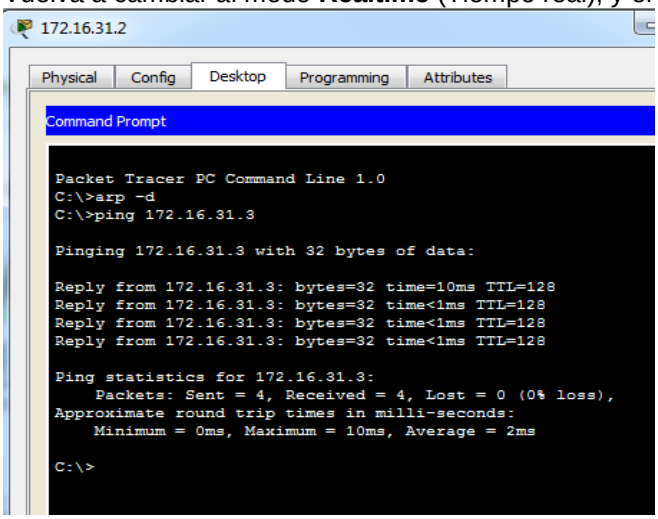

Router0
Router1
Switch0
Switch1
Punto de acceso
10.10.10.2
10.10.10.3
172.16.31.2
172.16.31.3
172.16.31.4
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- 172.16.3... ICMP
0.000 -- 172.16.3... ARP
0.001 172.16.31.2 Switch1 ARP
0.002 Switch1 172.16.3... ARP
0.002 Switch1 172.16.3... ARP
0.002 Switch1 Router1 ARP
0.003 172.16.31.3 Switch1 ARP
0.004 Switch1 172.16.3... ARP
0.004 -- 172.16.3... ICMP
Reset Simulation
Constant Delay
Captured to: 0.004 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NTP, OSPF, OSPFv6, PAgP,

Paso 2: Revisar la tabla ARP

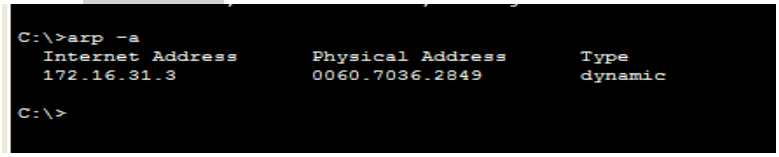
Observe que vuelve a aparecer el paquete ICMP. Abra la PDU y revise las direcciones MAC. ¿Las direcciones MAC de origen y destino coinciden con sus direcciones IP? Sí



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



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



En general, ¿cuándo emite un dispositivo final una solicitud de ARP? Cuando no conoce la dirección MAC del receptor.

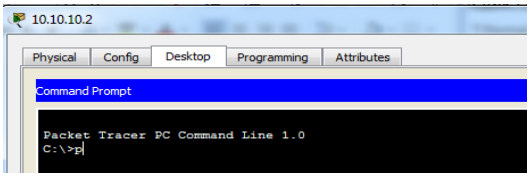
Parte 2: Examinar una tabla de direcciones MAC del switch

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

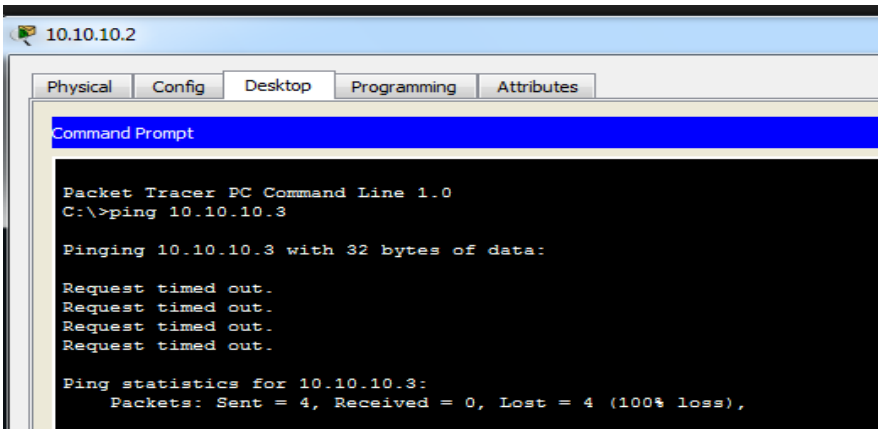
En **172.16.31.2**, introduzca el comando **ping 172.16.31.4**.

```
Pinging 172.16.31.4 with 32 bytes of data:

Reply from 172.16.31.4: bytes=32 time=12ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

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



Introduzca el comando **ping 10.10.10.3**. ¿Cuántas respuestas se enviaron y se recibieron? Se enviaron cuatro y se perdieron 4 cuatro no hay conexión configurada.



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

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>show mac-address-table
          Mac Address Table
-------------------------------------------

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

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

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	No aplicable	No aplicable
Router1	Gig0/0	00E0.F7B1.8901	Gig0/1
	Se0/0/0	No aplicable	No aplicable

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>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.6458.2501      DYNAMIC       Gig0/1
Switch0>
```

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección MAC	Interfaz del switch
Router0	Gig0/0	0001.6458.2501	Gig0/1
	Se0/0/0	No aplicable	No aplicable
Router1	Gig0/0	00E0.F7B1.8901	Gig0/1
	Se0/0/0	No aplicable	No aplicable

¿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

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

Introduzca el comando **ping 10.10.10.1**.

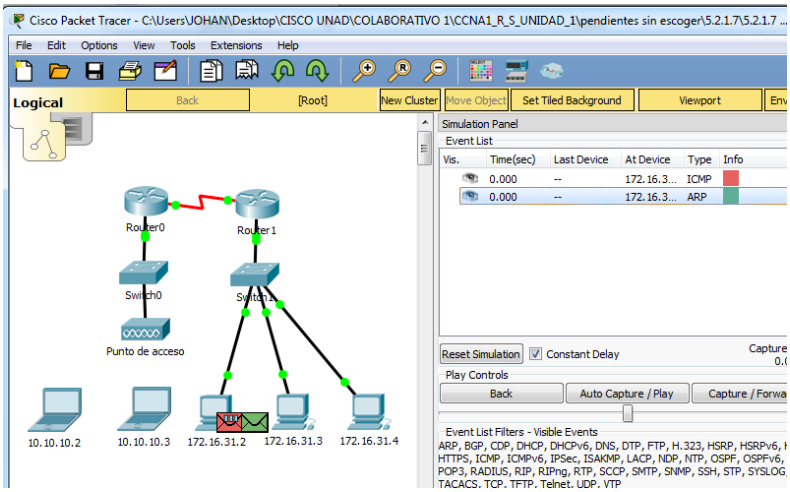
```
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=13ms 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=2ms 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 = 13ms, Average = 4ms
```

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

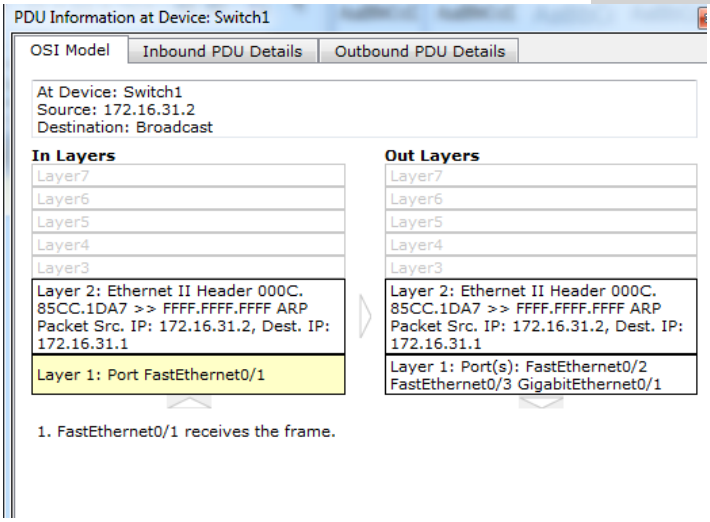
```
Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 4ms

C:\>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
```

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

Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen? 2



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



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 para determinar una dirección MAC para la interfaz del router que sirve de gateway.

Paso 2: Examinar la tabla ARP en el Router1

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

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>ena
Router#show mac-address-table
          Mac Address Table
-------------------------------------------

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

Router#
```

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             8   000C.85CC.1DA7  ARPA
GigabitEthernet0/0
Router#
```

¿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.

5.3.3.5 Packet Tracer - Configure Layer 3 Switches

Topología

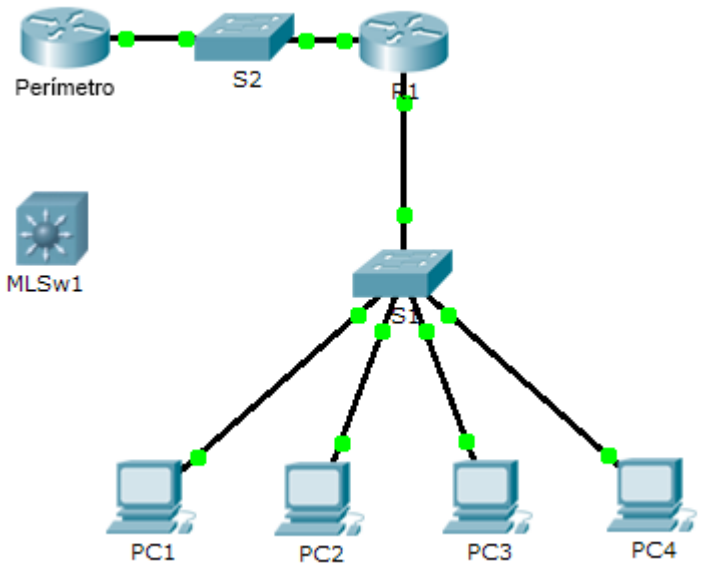


Tabla de direccionamiento

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

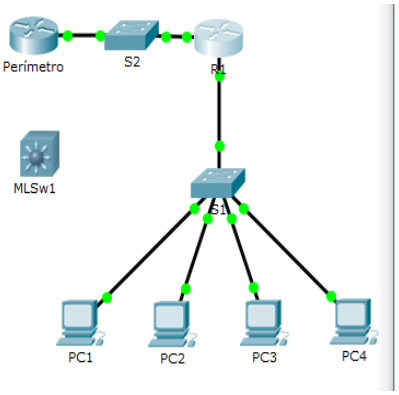
Nota: por lo general, un router de producción tendría muchas más configuraciones que simplemente el direccionamiento IP de las interfaces. Sin embargo, para agilizar esta actividad, se configuró solo el direccionamiento IP de interfaces en **R1**.

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**.

d.




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

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


Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.16.31.1     YES manual up                    up
GigabitEthernet0/1     192.168.0.2     YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

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**.

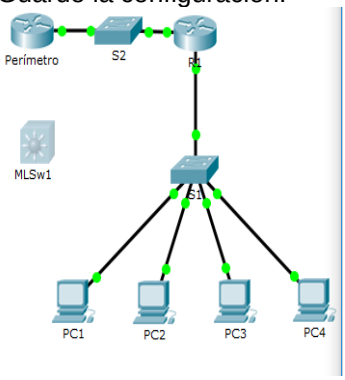
c. Cambie el puerto al modo de enrutamiento introduciendo el comando **no switchport**.

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.



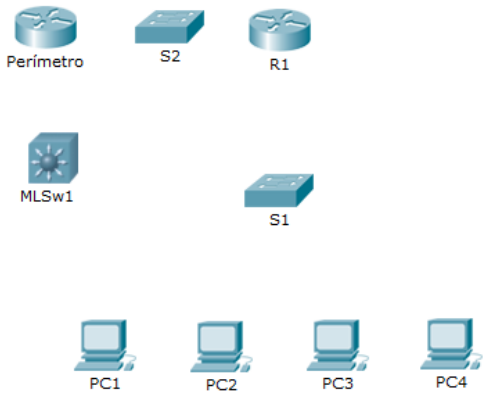

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.0.2 255.255.255.0
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to down
Switch(config-if)#
Switch(config-if)#int vlan 1
Switch(config-if)#ip address 172.16.31.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

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

Nota: por lo general, los siguientes pasos se llevarían a cabo después del horario laboral o cuando el tráfico en la red de producción está en su volumen más bajo. Para minimizar el tiempo de inactividad, el nuevo equipo debe estar totalmente configurado y listo para implementar.

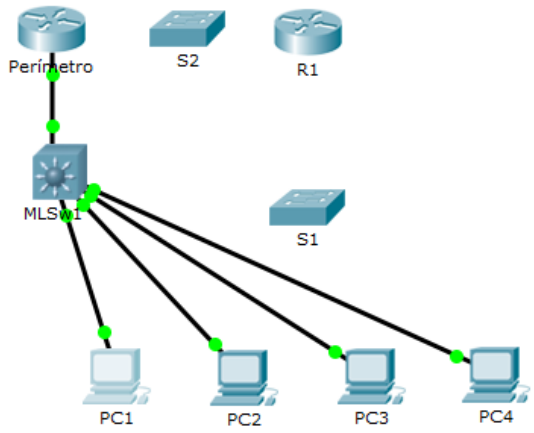
a. Haga clic en un área vacía de la pantalla para anular la selección de todos los dispositivos.

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



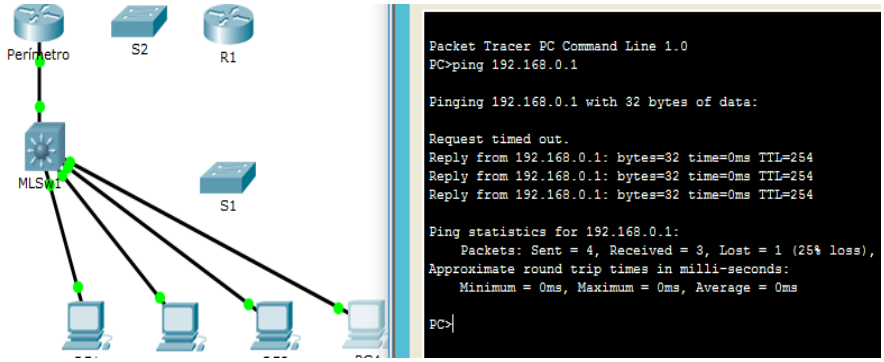
c. Seleccione los cables adecuados para completar lo siguiente:

- Conectar MLSw1 GigabitEthernet 0/1 a Edge GigabitEthernet 0/0.
- Conectar las PC a los puertos Fast Ethernet en **MLSw1**.



-

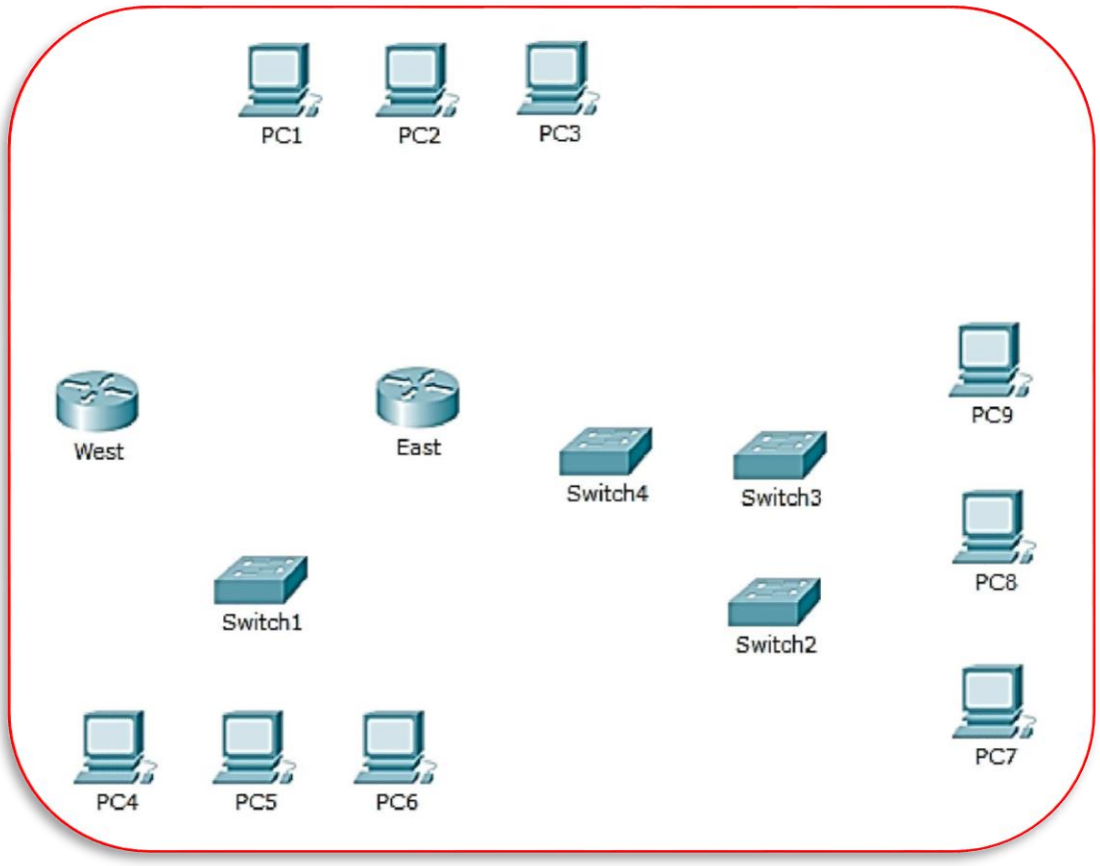
d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.



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

6.3.1.10 Packet Tracer: Exploración de dispositivos de internetworking

Topología



Objetivos

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

Información básica

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

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

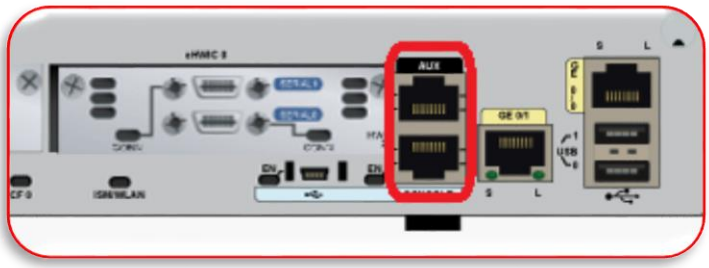
Parte 1: Identificar las características físicas de los dispositivos de internetworking

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

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

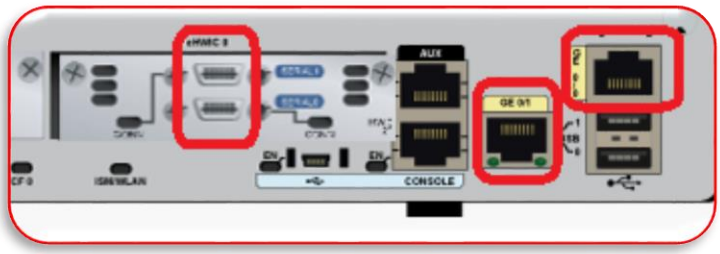
b. Acerque el elemento y expanda la ventana para ver todo el router.

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



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

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



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

East> **show ip interface brief**

```
East>show ip interface brief
Interface IP-Address OK? Method                 Status   Protocol
GigabitEthernet0/0 unassigned      YES unset administratively down down
GigabitEthernet0/1 unassigned      YES unset administratively down down
Serial0/0/0        unassigned      YES unset down down
```

Serial0/0/1 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

East>

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

c. Introduzca los siguientes comandos:

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

East>show interface g0/0

GigabitEthernet0/0 is administratively down, line protocol is down (disabled)

Hardware is CN Gigabit Ethernet, address is 0001.4274.a401 (bia 0001.4274.a401)

MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full-duplex, 100Mb/s, media type is RJ45

output flow-control is unsupported, input flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00,

Last input 00:00:08, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0 (size/max/drops); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 watchdog, 1017 multicast, 0 pause input

0 input packets with dribble condition detected

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 2 interface resets

0 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

East>

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

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

East>show interface s0/0/0

Serial0/0/0 is down, line protocol is down (disabled)

Hardware is HD64570

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

Last input never, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0 (size/max/drops); Total output drops: 0

Queueing strategy: weighted fair

Output queue: 0/1000/64/0 (size/max total/threshold/drops)

Conversations 0/0/256 (active/max active/max total)

Reserved Conversations 0/0 (allocated/max allocated)

Available Bandwidth 1158 kilobits/sec

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 output buffer failures, 0 output buffers swapped out

0 carrier transitions

DCD=down DSR=down DTR=down RTS=down CTS=down

East>

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

1544 Kbit

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

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

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

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

Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

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

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

Módulo HWIC-4ESW

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

c. 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.

West>show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

West>

Parte 3: Conectar los dispositivos

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

a. Seleccione el tipo de cable adecuado.

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

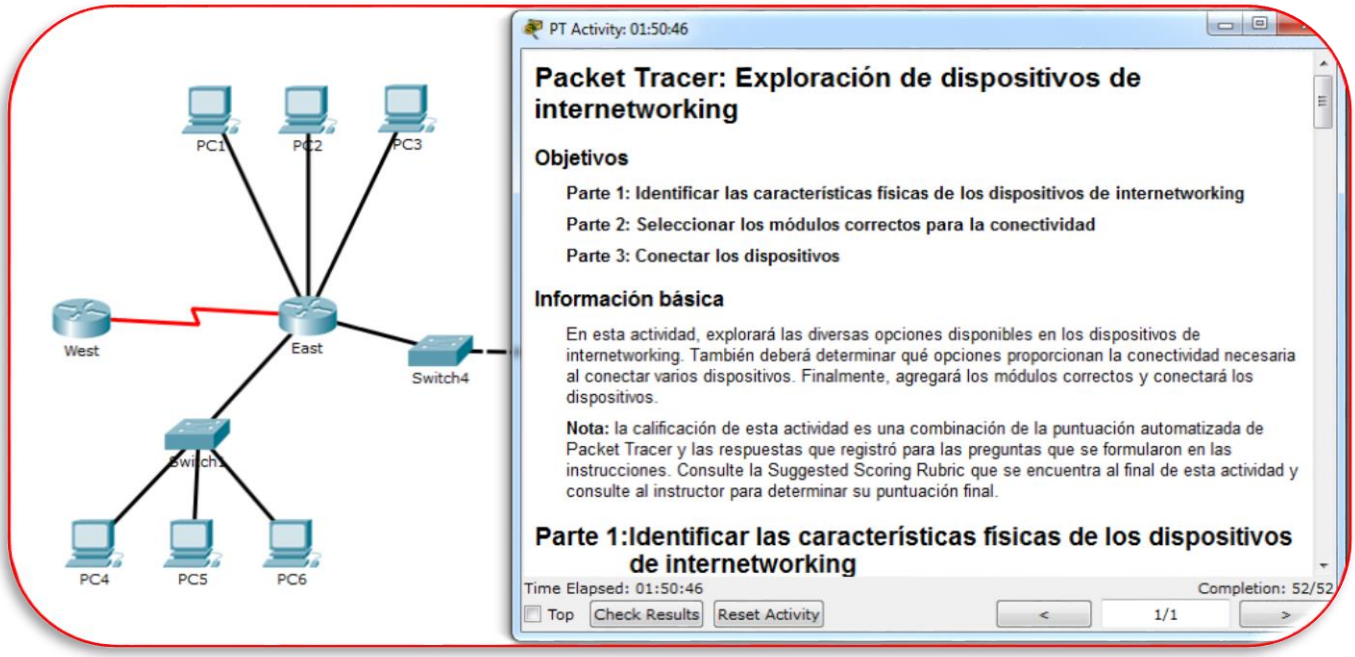
c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.

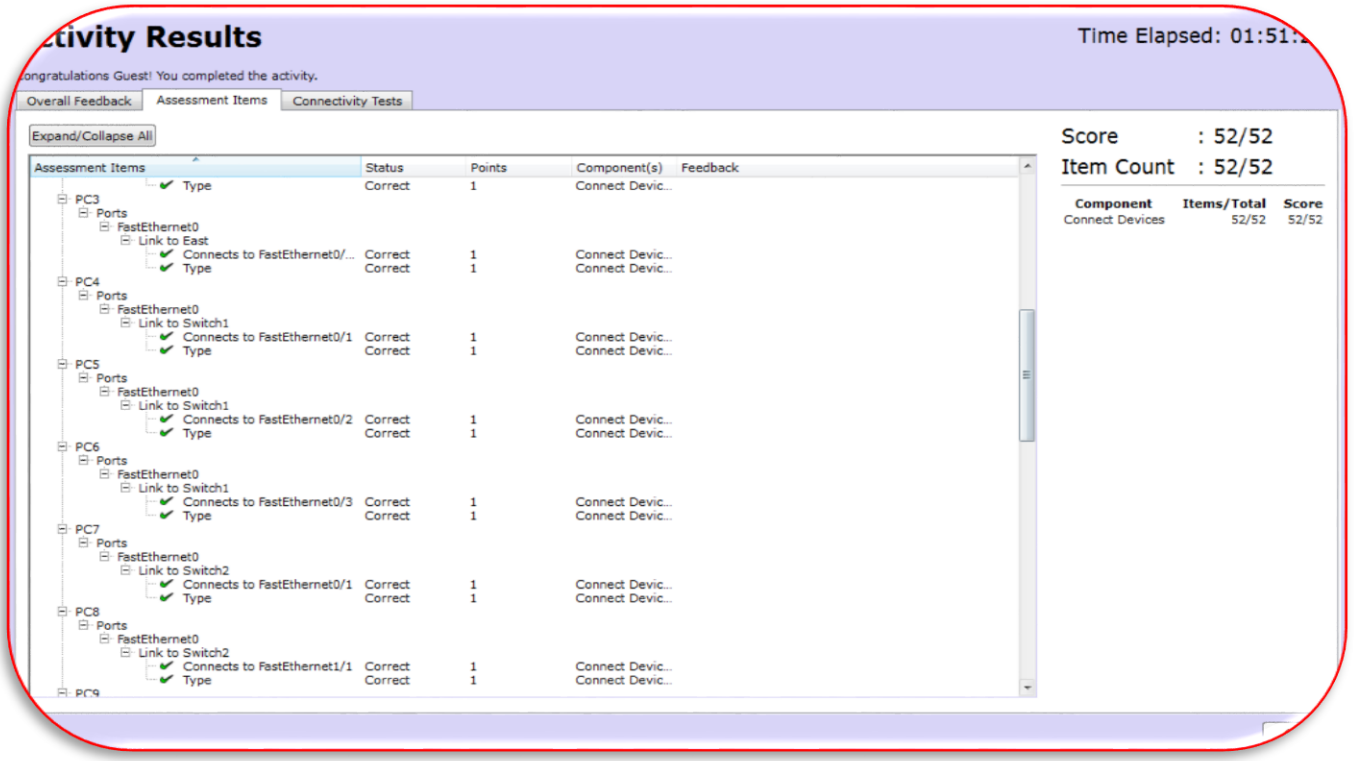
d. Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

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

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

Dispositivo	Interfaz	Tipo de cable	Dispositivo	Interfaz
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0
Switchl	FastEthernetO/1	Cable de cobre de conexión directa	PC4	FastEthernetO
Switchl	FastEthernetO/2	Cable de cobre de conexión directa	PC5	FastEthernetO
Switchl	FastEthernetO/3	Cable de cobre de conexión directa	PC6	FastEthernetO
Switch4	GigabitEthernetO/2	Cross-Over de cobre	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fibra	Switch2	GigabitEthernet5/1
Switch2	FastEthernetO/1	Cable de cobre de conexión directa	PC7	FastEthernetO
Switch2	FastEthernet1/1	Cable de cobre de conexión directa	PC8	FastEthernetO
Switch2	FastEthernet2/1	Cable de cobre de conexión directa	PC9	FastEthernetO
East	SerialO/0/0	DCE serial (conectar primero a	West	SerialO/O/O


PC1
PC2
PC3
West
East
Switch4
Switch1
PC4
PC5
PC6
PT Activity: 01:50:46
Packet Tracer: Exploración de dispositivos de internetworking
Objetivos
Parte 1: Identificar las características físicas de los dispositivos de internetworking
Parte 2: Seleccionar los módulos correctos para la conectividad
Parte 3: Conectar los dispositivos
Información básica
En esta actividad, explorará las diversas opciones disponibles en los dispositivos de internetworking. También deberá determinar qué opciones proporcionan la conectividad necesaria al conectar varios dispositivos. Finalmente, agregará los módulos correctos y conectará los dispositivos.
Nota: la calificación de esta actividad es una combinación de la puntuación automatizada de Packet Tracer y las respuestas que registró para las preguntas que se formularon en las instrucciones. Consulte la Suggested Scoring Rubric que se encuentra al final de esta actividad y consulte al instructor para determinar su puntuación final.
Parte 1:Identificar las características físicas de los dispositivos de internetworking
Time Elapsed: 01:50:46
Completion: 52/52
Top
Check Results
Reset Activity
<
1/1
>


tivity Results
Time Elapsed: 01:51:
ongratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Component(s)
Feedback
Score : 52/52
Item Count : 52/52
Component
Items/Total
Score
Connect Devices
52/52
52/52

6.4.1.2 Packet Tracer: 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

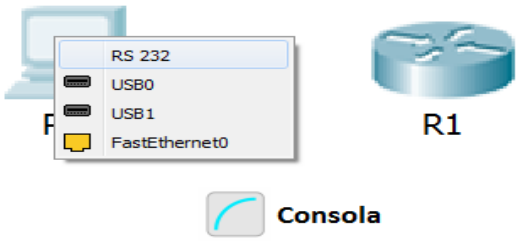
En esta actividad, configurará los parámetros básicos del router. Proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También configurará mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten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

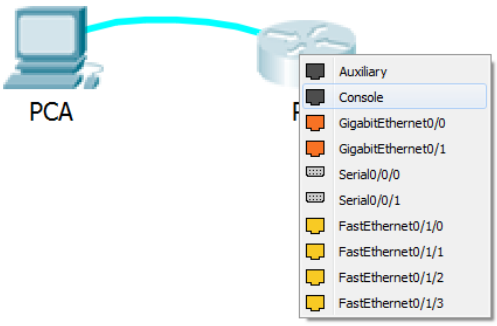
Paso 1: Establecer una conexión de consola al R1

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

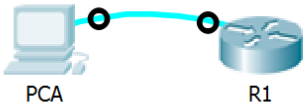
b. Haga clic en **PCA** y seleccione **RS 232**.

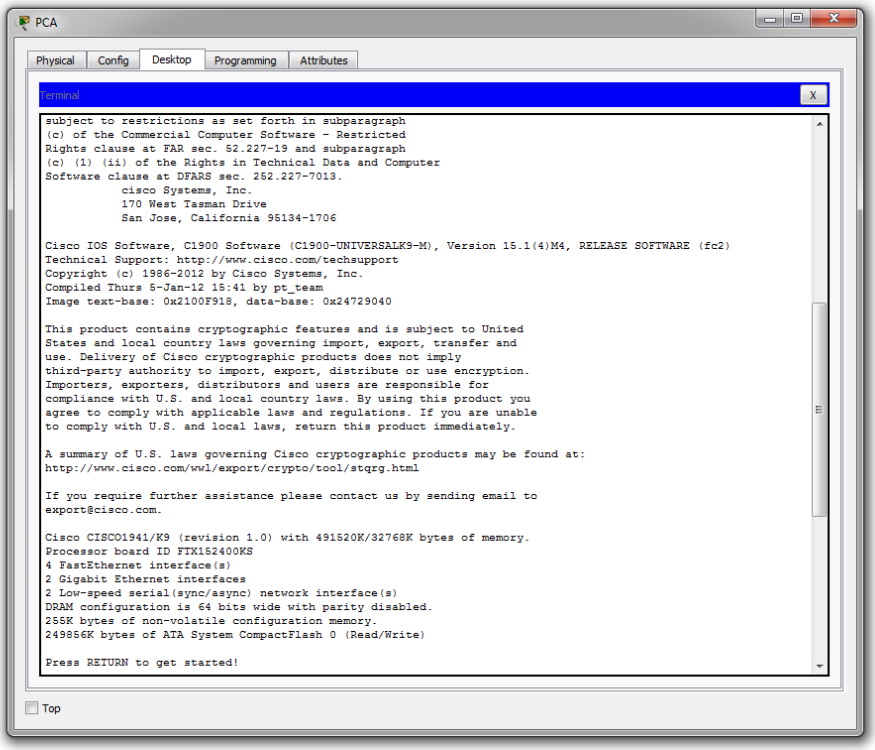


c. Haga clic en **R1** y seleccione **Console** (Consola).



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? Tiene 4

¿Cuántas interfaces Gigabit Ethernet tiene el router? Tiene 2 interfaces

¿Cuántas interfaces seriales tiene el router? Tiene 2 interfaces

¿Cuál es el rango de valores que se muestra para las líneas vty? De 0 a 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? La información se encuentra alojada en la RAM.

Parte 2: Configurar y verificar la configuración inicial del router

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

Paso 1: Configurar los parámetros iniciales de R1

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

a. Establezca **R1** como nombre de host. b.

Utilice las siguientes contraseñas:

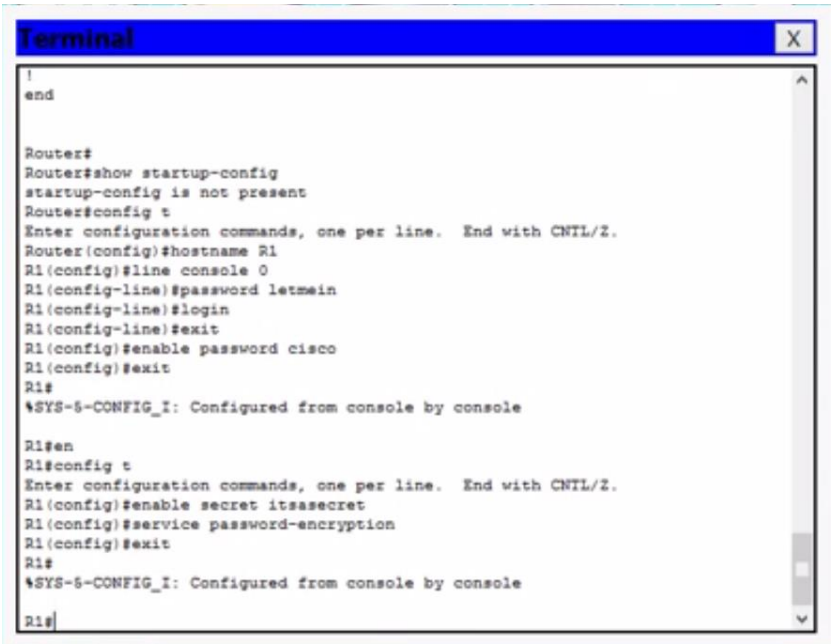
1) Consola: **letmein**

2) EXEC privilegiado, sin encriptar: **cisco**

3) EXEC privilegiado, encriptado: **itsasecret**

c. Encripte todas las contraseñas de texto no cifrado.

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



Paso 2: Verificar los parámetros iniciales de R1

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

¿Por qué todos los routers deben tener un mensaje del día (MOTD)? Son mensajes con fin informativo.

Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar?

login

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

¿Por qué la contraseña secreta de enable permitiría el acceso al modo EXEC privilegiado y la contraseña de enable dejaría de ser válida? Se remplaza la contraseña de enable. Para ingresar al modo EXEC privilegiado se debe introducir la contraseña secreta de enable.

Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique. service password-encryption encripta todas las contraseñas.

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 ?

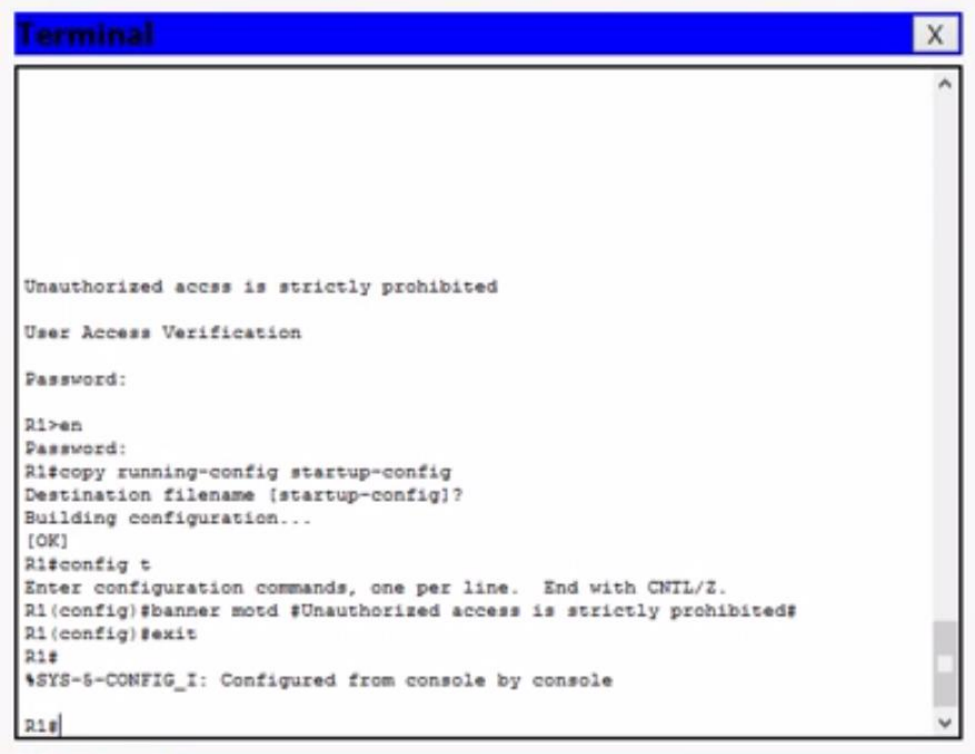
startup-config

copy running-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**

¿Cuántos archivos hay almacenados actualmente en la memoria flash? Hay 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? la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo.

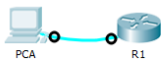
b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:

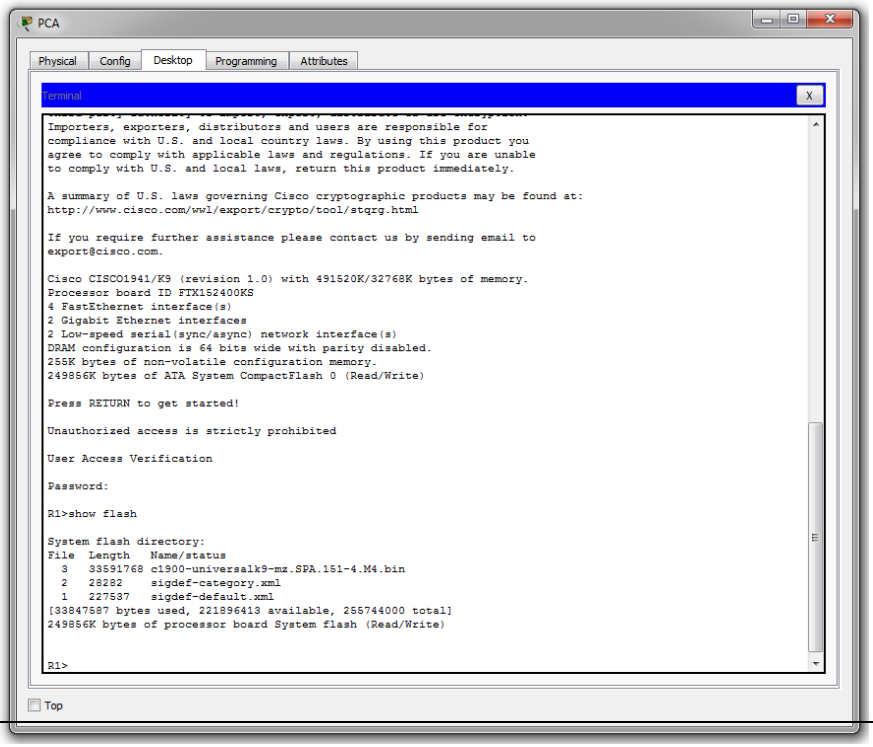
R1# **copy startup-config flash**

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.





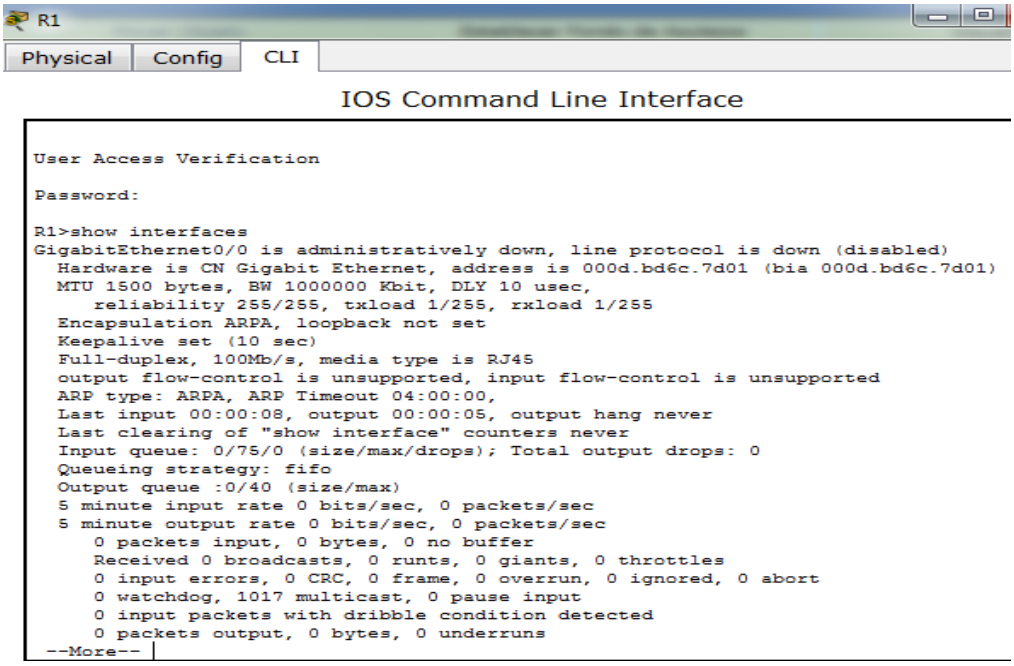
6.4.3.3 Packet Tracer - Connect a Router to a LAN

Parte 1: Mostrar la información del router

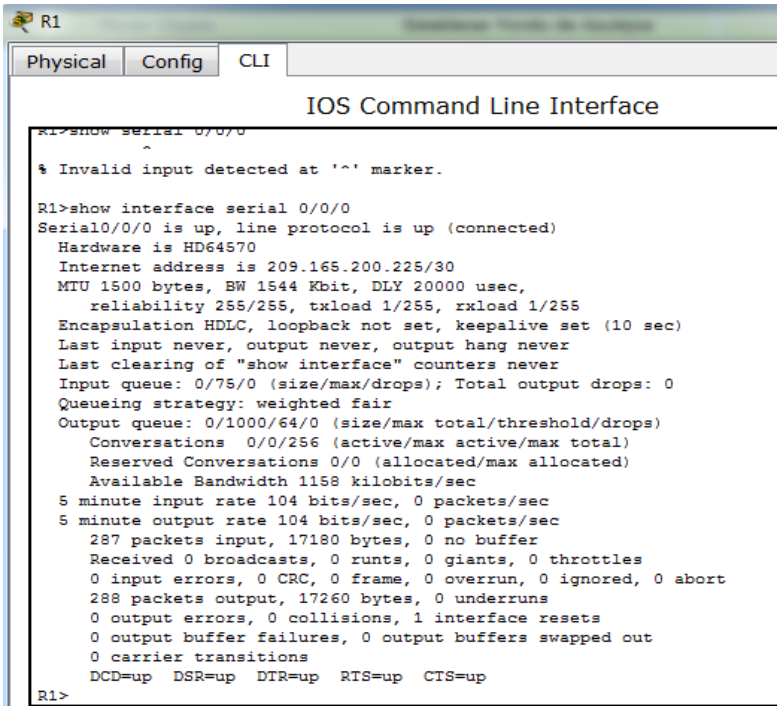
Paso 1: Mostrar la información de la interfaz en el R1.

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



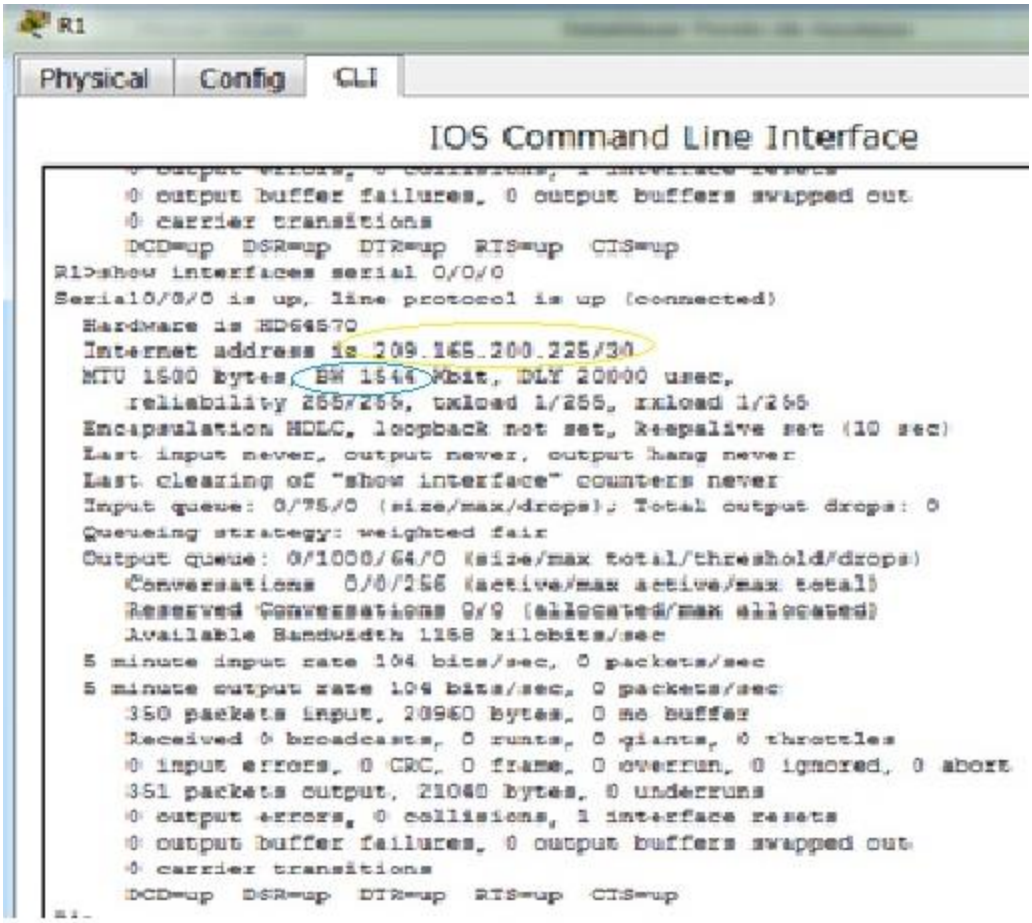
b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0? show interface serial 0/0/0



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

1) ¿Cuál es la dirección IP configurada en el R1? 209.165.200.225/30

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

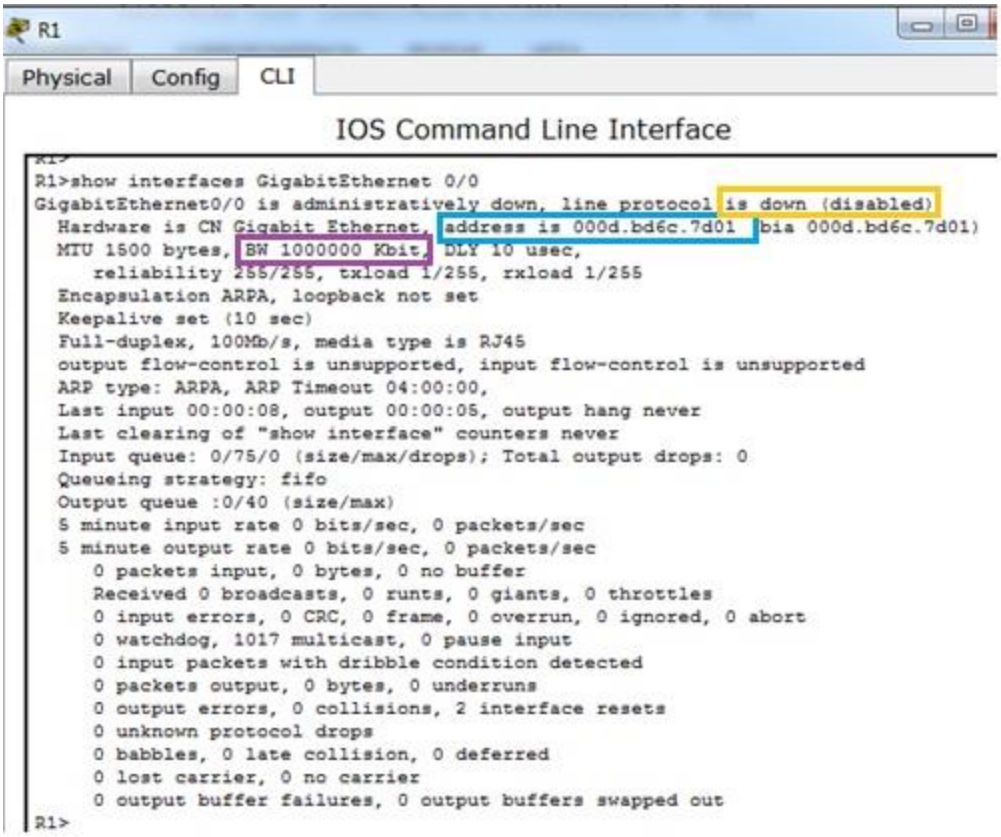


d. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:

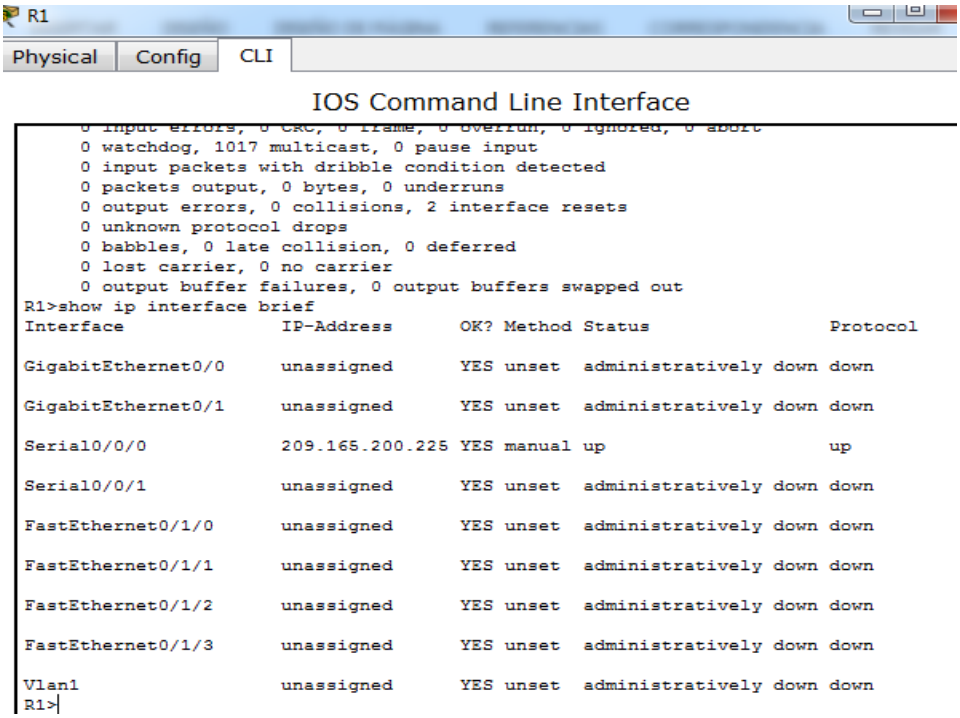
1) ¿Cuál es la dirección IP en el R1? No hay una dirección IP configurada en la interfaz GigabitEthernet 0/0.

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

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



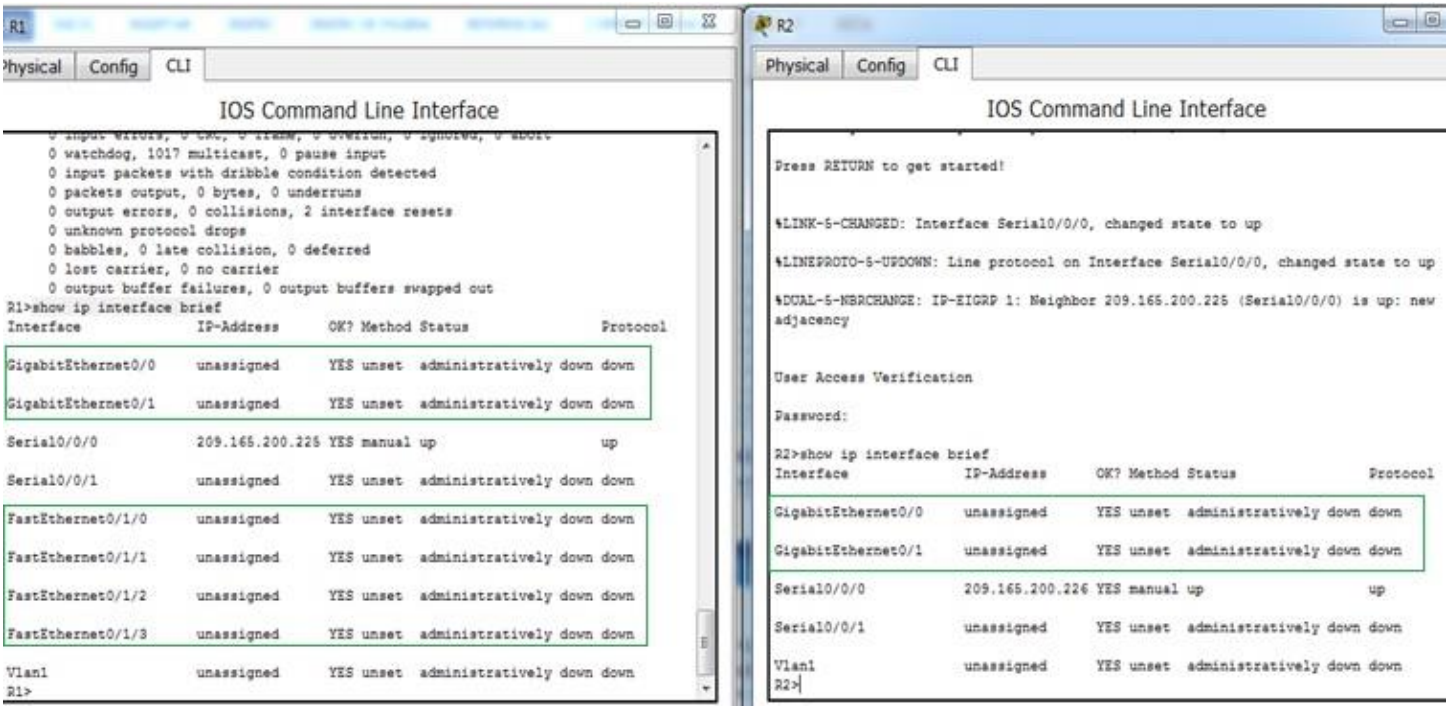
Paso 2: Mostrar una lista de resumen de las interfaces en el R1 a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas? show ip interface brief



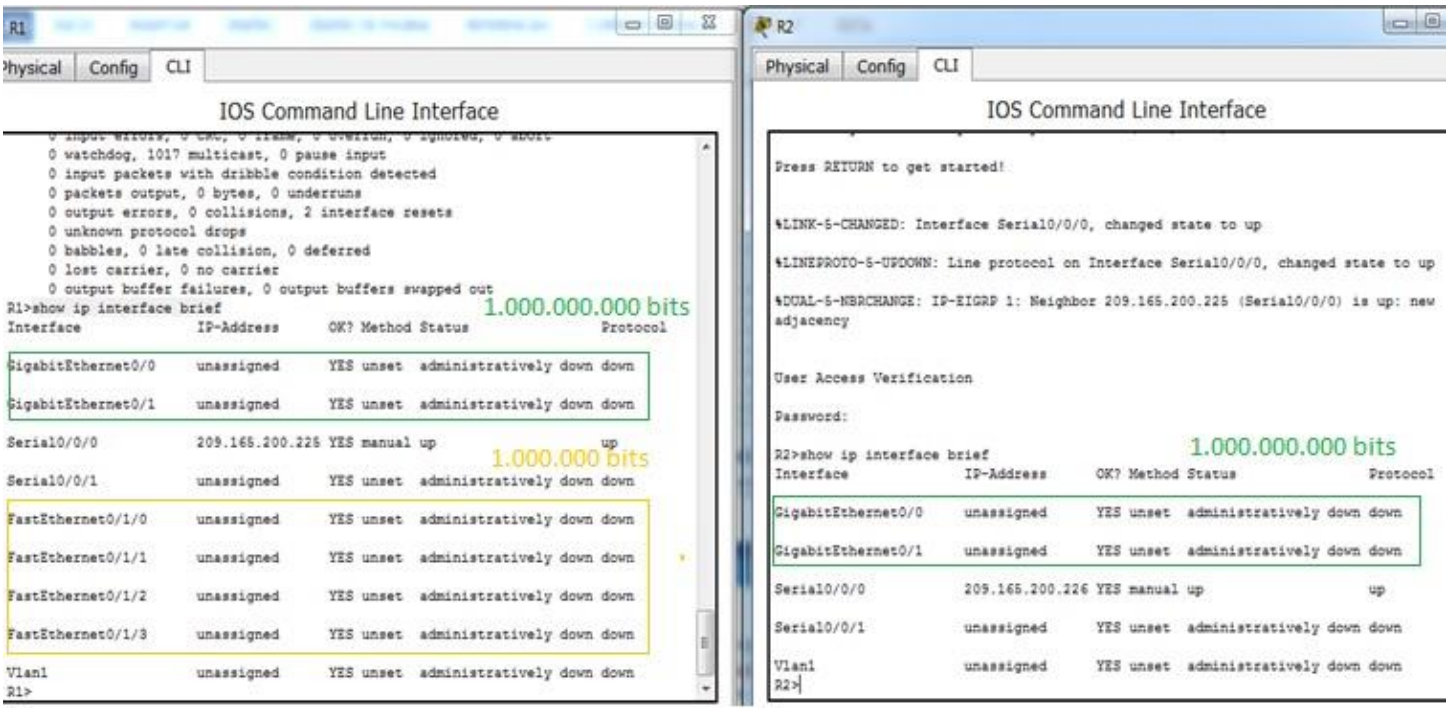
b. Introduzca el comando en cada router y responda las siguientes preguntas:

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

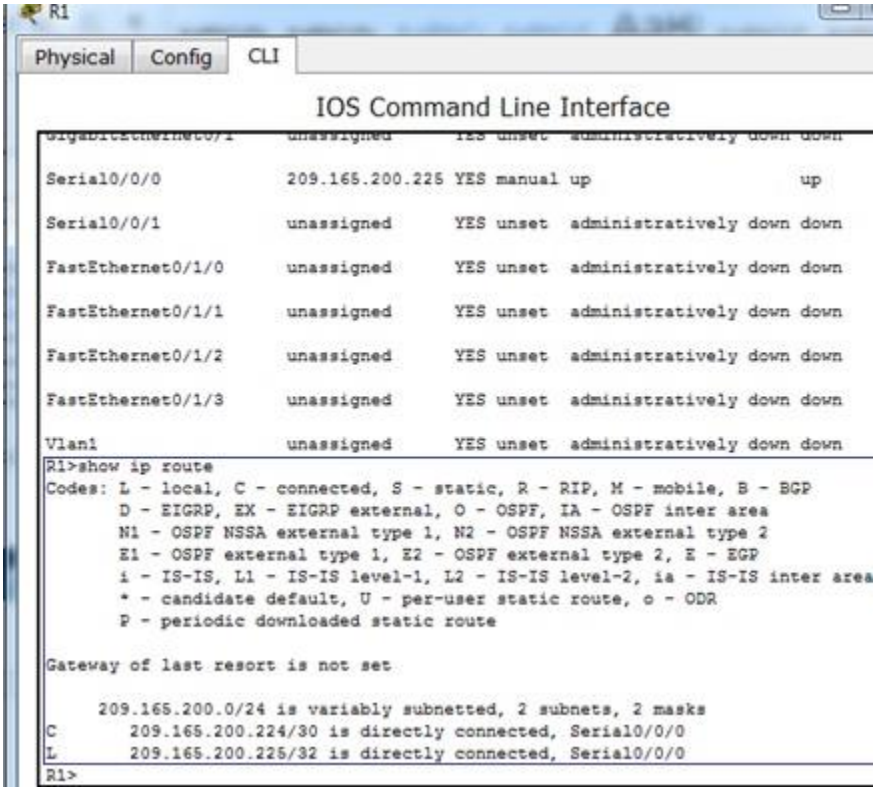
2) ¿Cuántas interfaces Ethernet hay en R1 y R2? R1 tiene seis interfaces Ethernet y R2 tiene dos interfaces Ethernet.



3) ¿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 a. ¿Qué comando muestra el contenido de la tabla de enrutamiento? show ip route

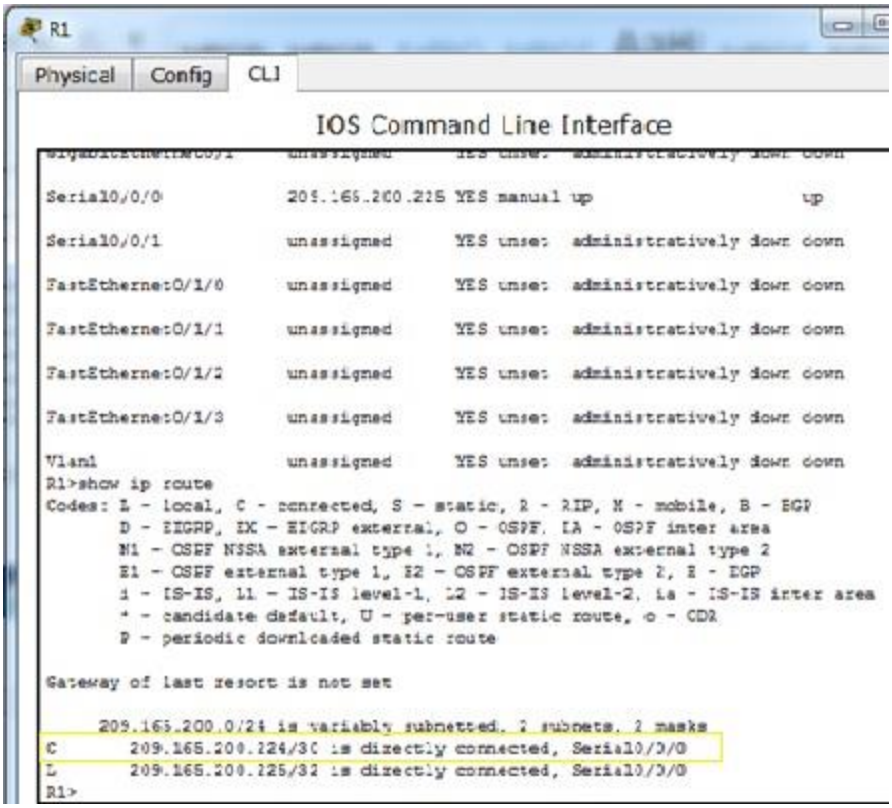


b. Introduzca el comando en el R1 y responda las siguientes preguntas:

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

2) ¿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:

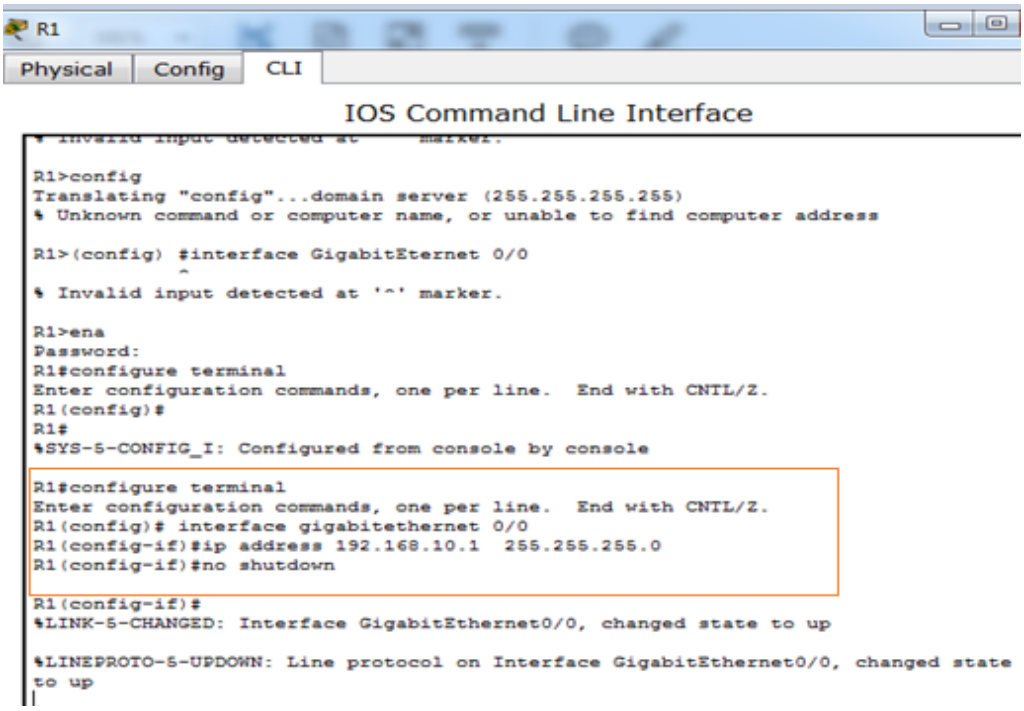
R1(config)# interface gigabitethernet 0/0

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



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

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

R1(config-if)# end

%SYS-5-CONFIG_I: Configured from console by console

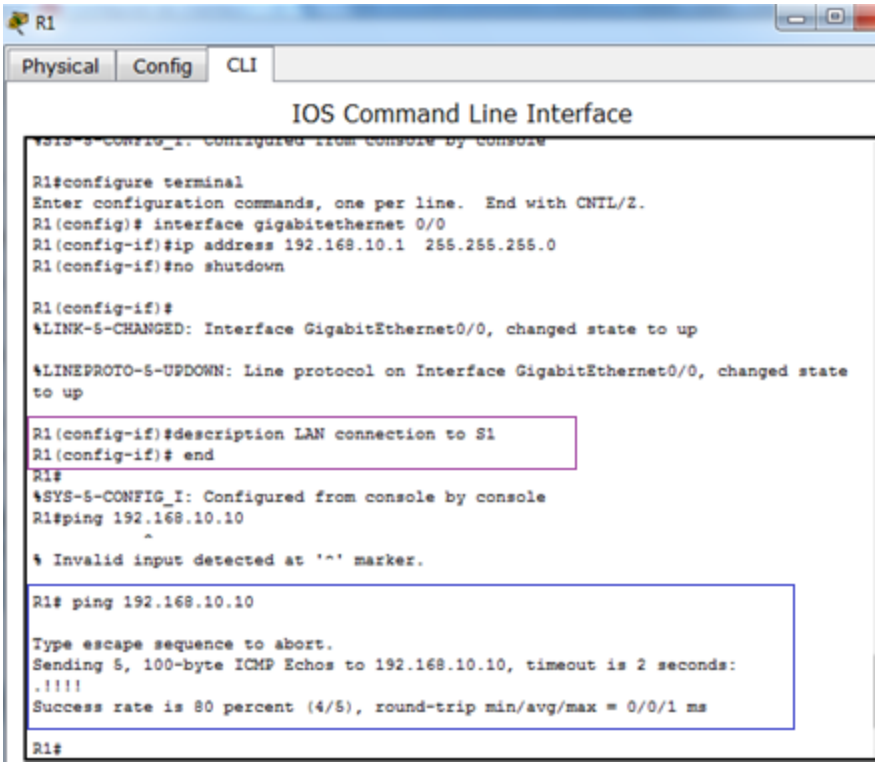
R1# ping 192.168.10.10

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



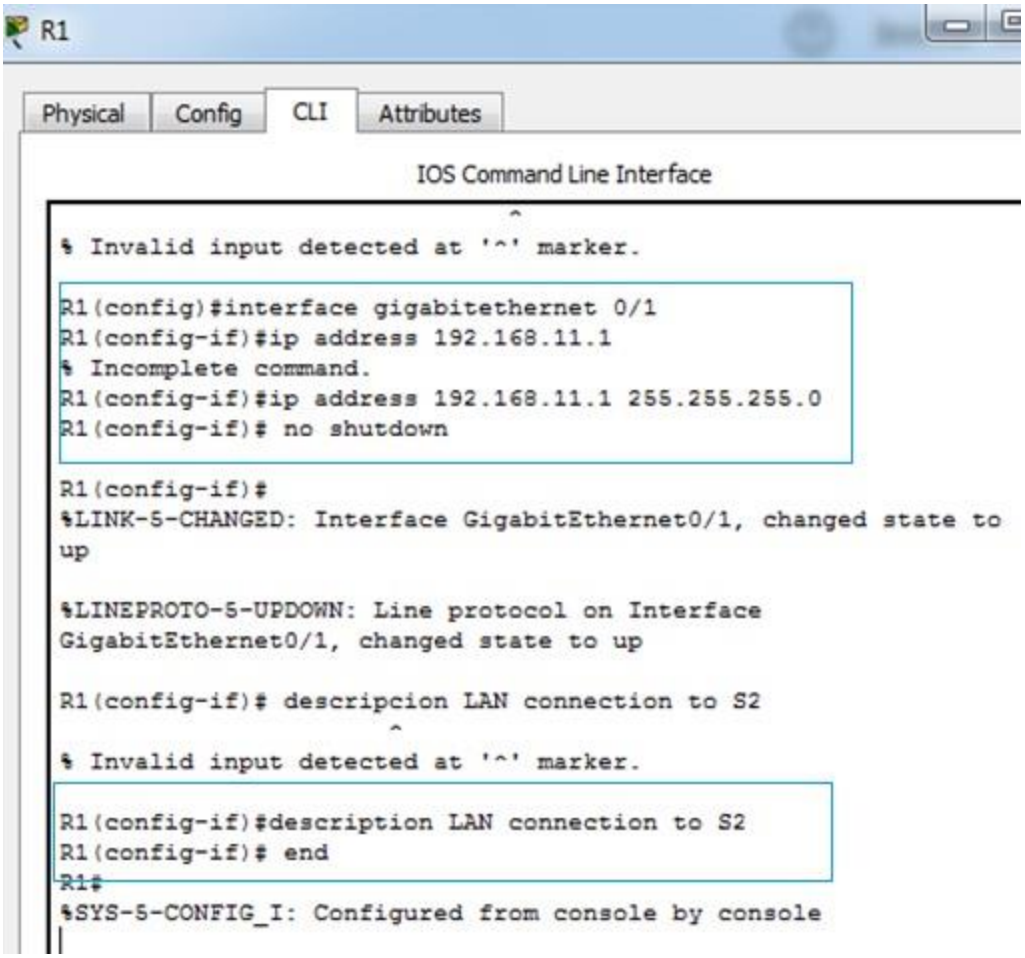
Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.

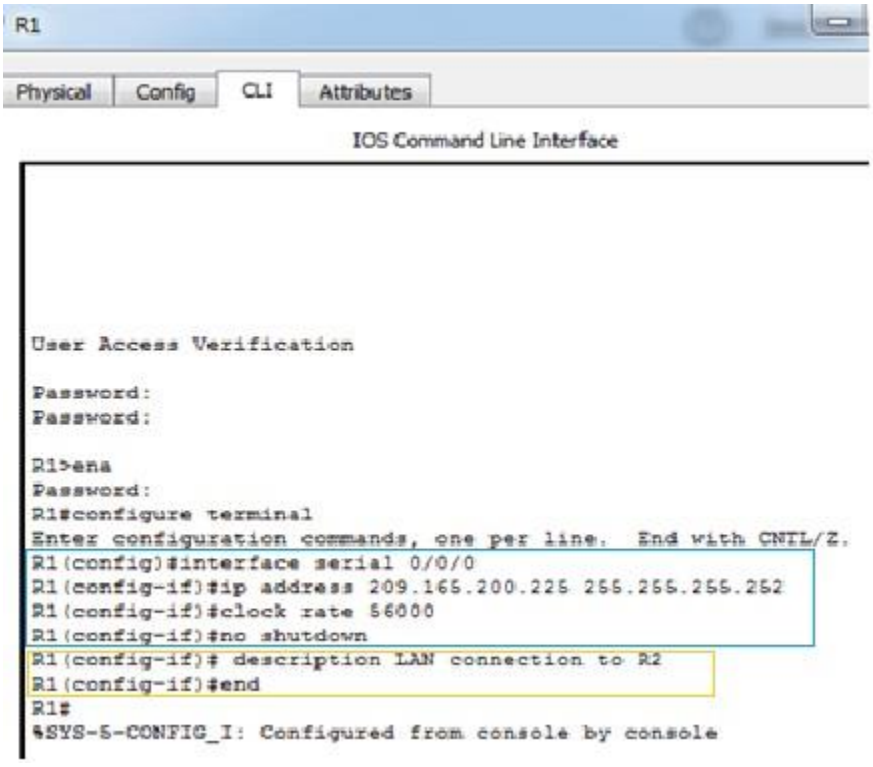
a. Utilice la información en la Addressing Table para finalizar la configuración de R1 y R2. Para cada interfaz, realice lo siguiente:

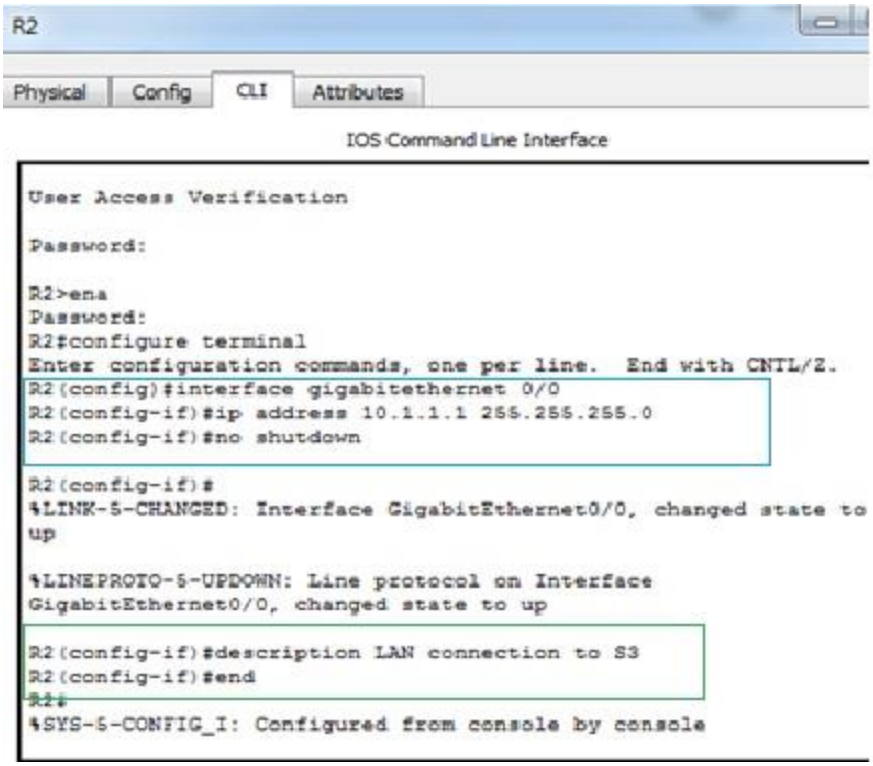
1) Introduzca la dirección IP y active la interfaz.

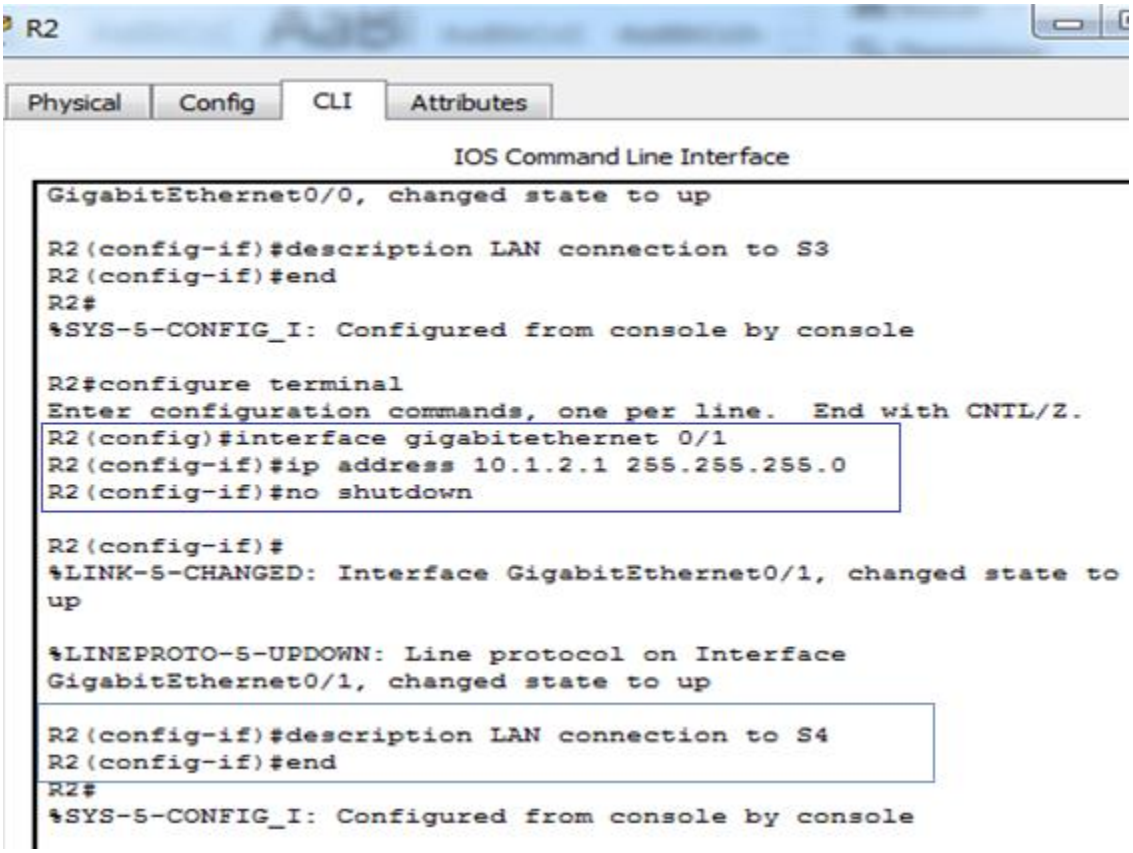
2) Configure una descripción apropiada.

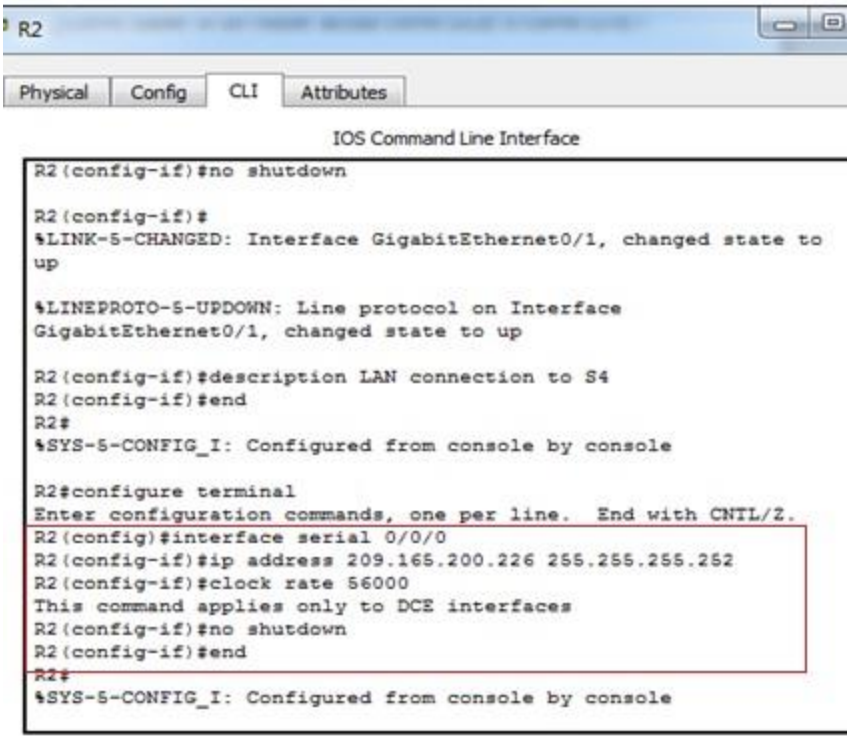
b. Verifique las configuraciones de las interfaces

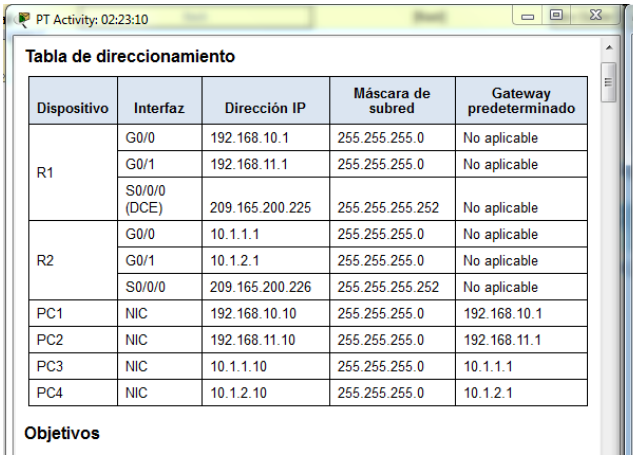

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.11.1
% Incomplete command.
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)# descripcion LAN connection to S2
% Invalid input detected at '^' marker.
R1(config-if)#description LAN connection to S2
R1(config-if)# end
R1#
%SYS-5-CONFIG_I: Configured from console by console


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
Password:
R1>ena
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.252
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
R1(config-if)# description LAN connection to R2
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

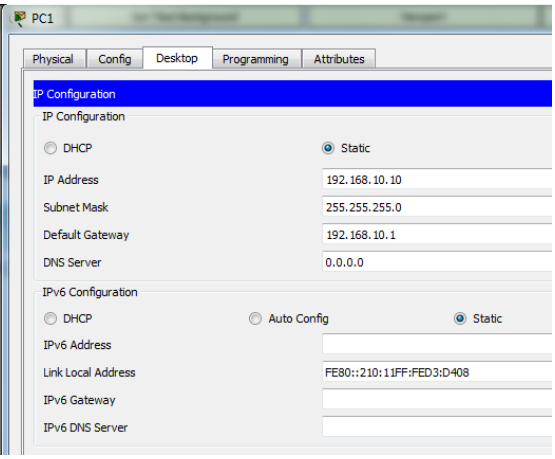

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
R2>ena
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ip address 10.1.1.1 255.255.255.0
R2(config-if)#no 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)#description LAN connection to S3
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

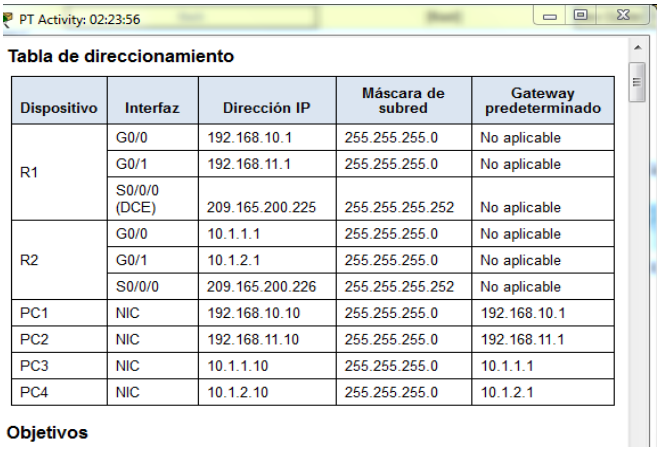

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
GigabitEthernet0/0, changed state to up
R2(config-if)#description LAN connection to S3
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitethernet 0/1
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)#description LAN connection to S4
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console



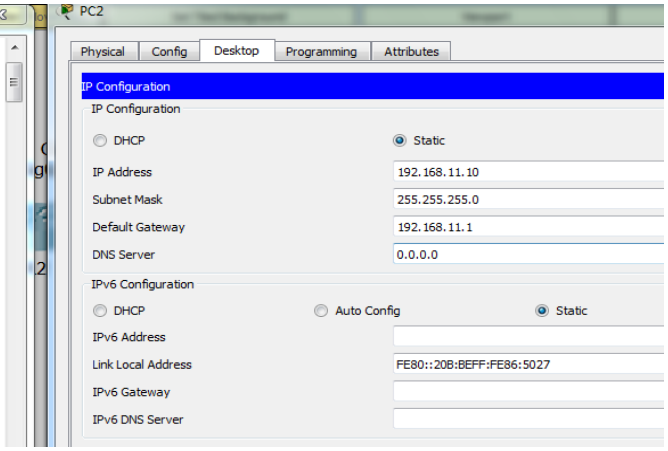


Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	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





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

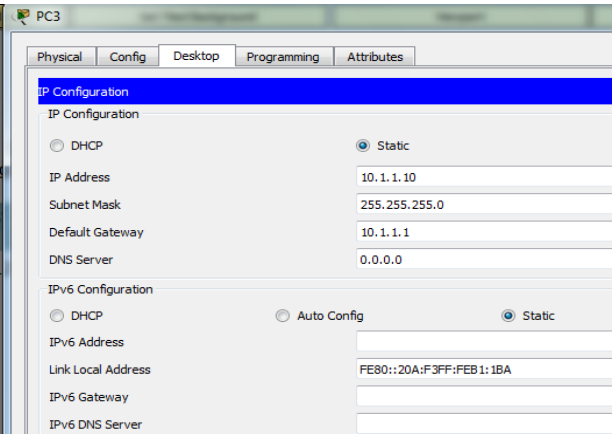


PT Activity: 02:24:33

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

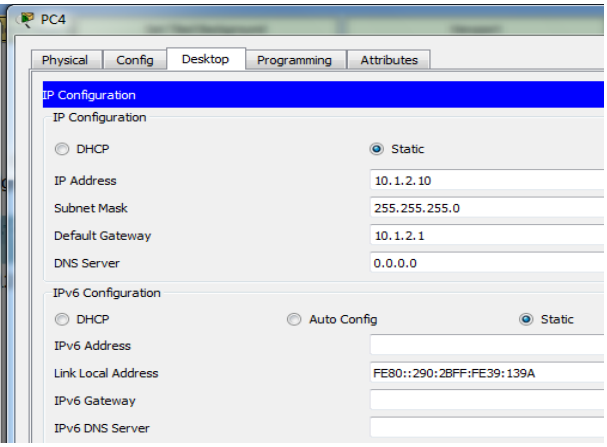
Objetivos

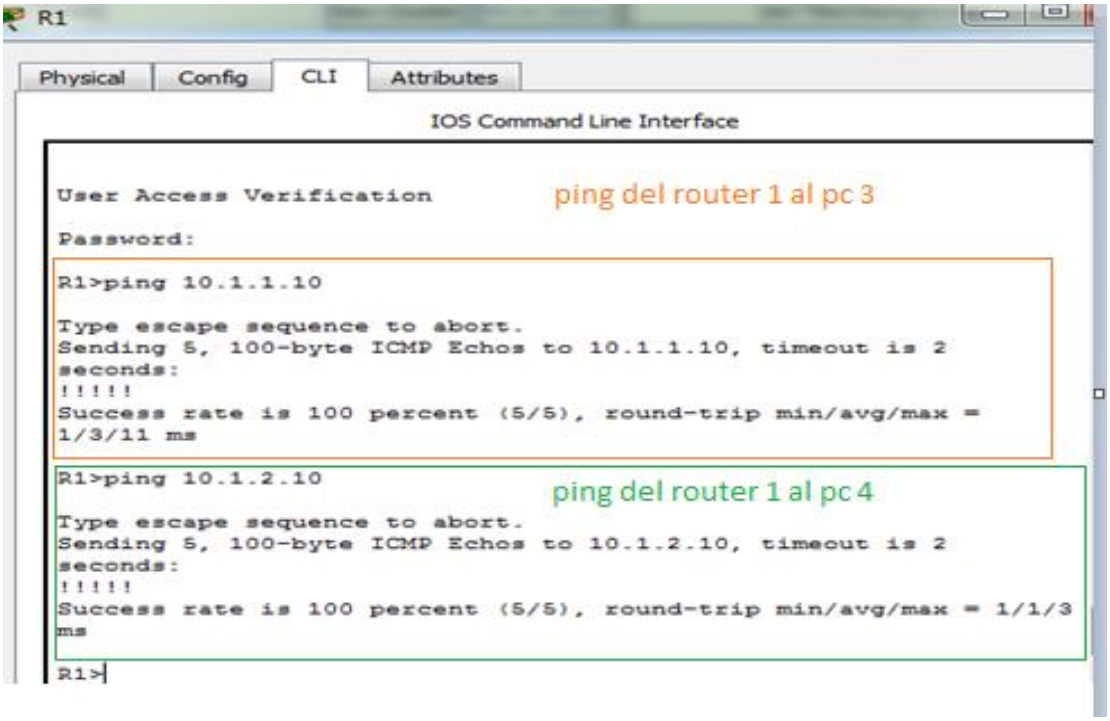


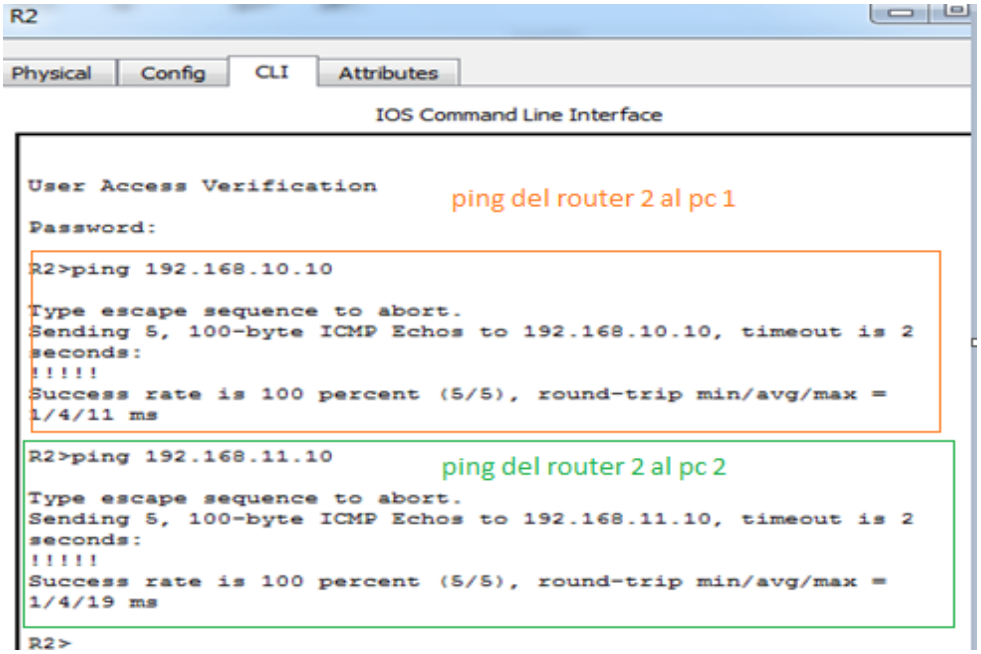
PT Activity: 02:25:16

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

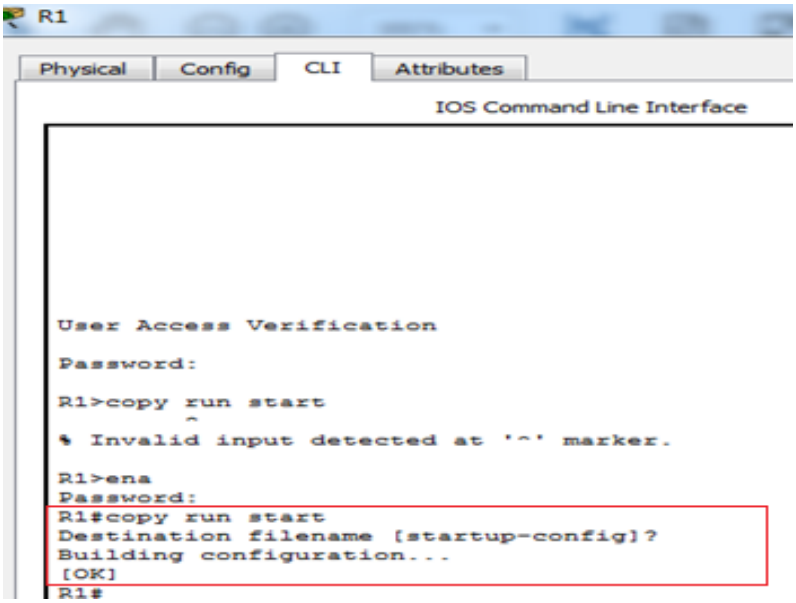


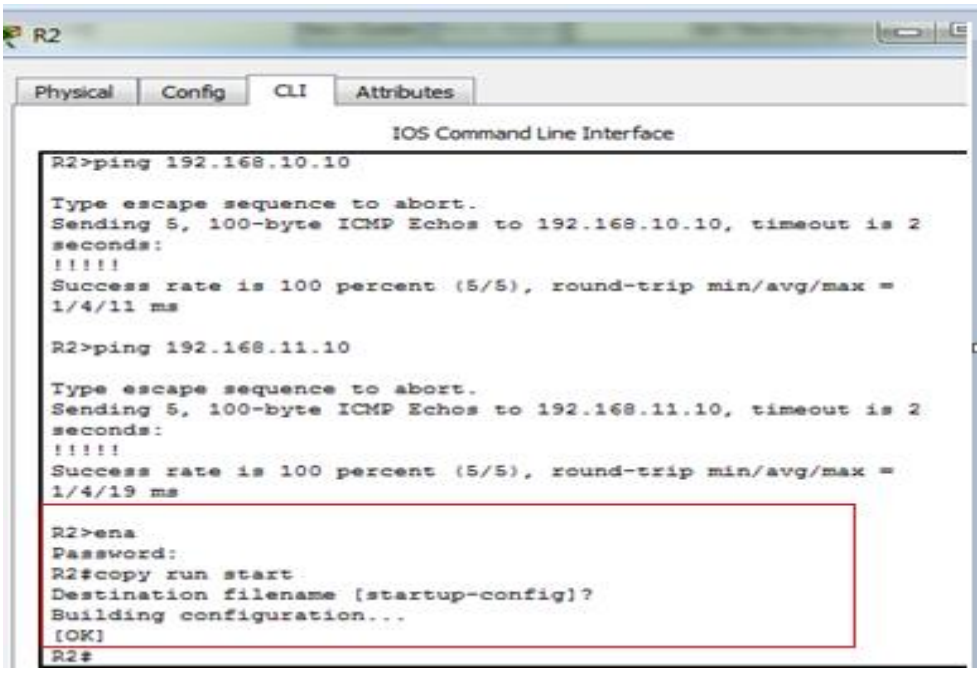




Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM

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

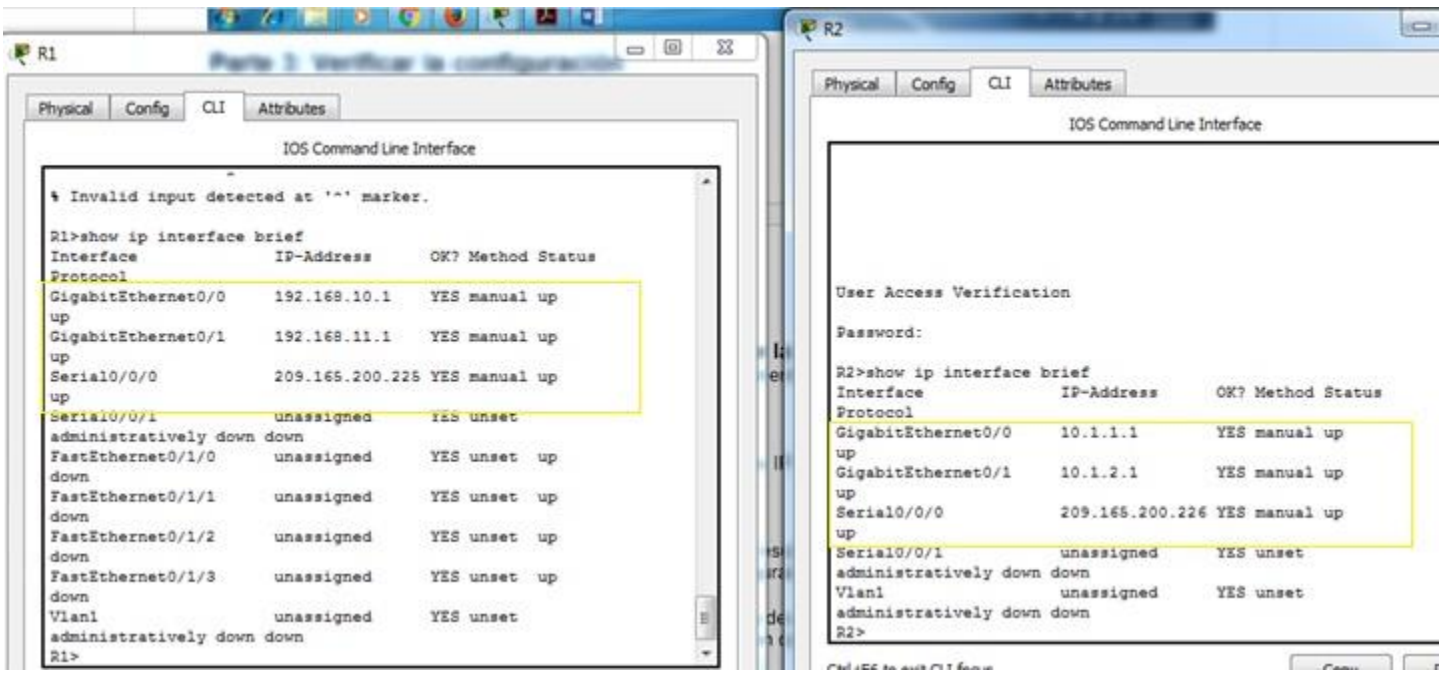




Parte 3: Verificar la configuración

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.

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

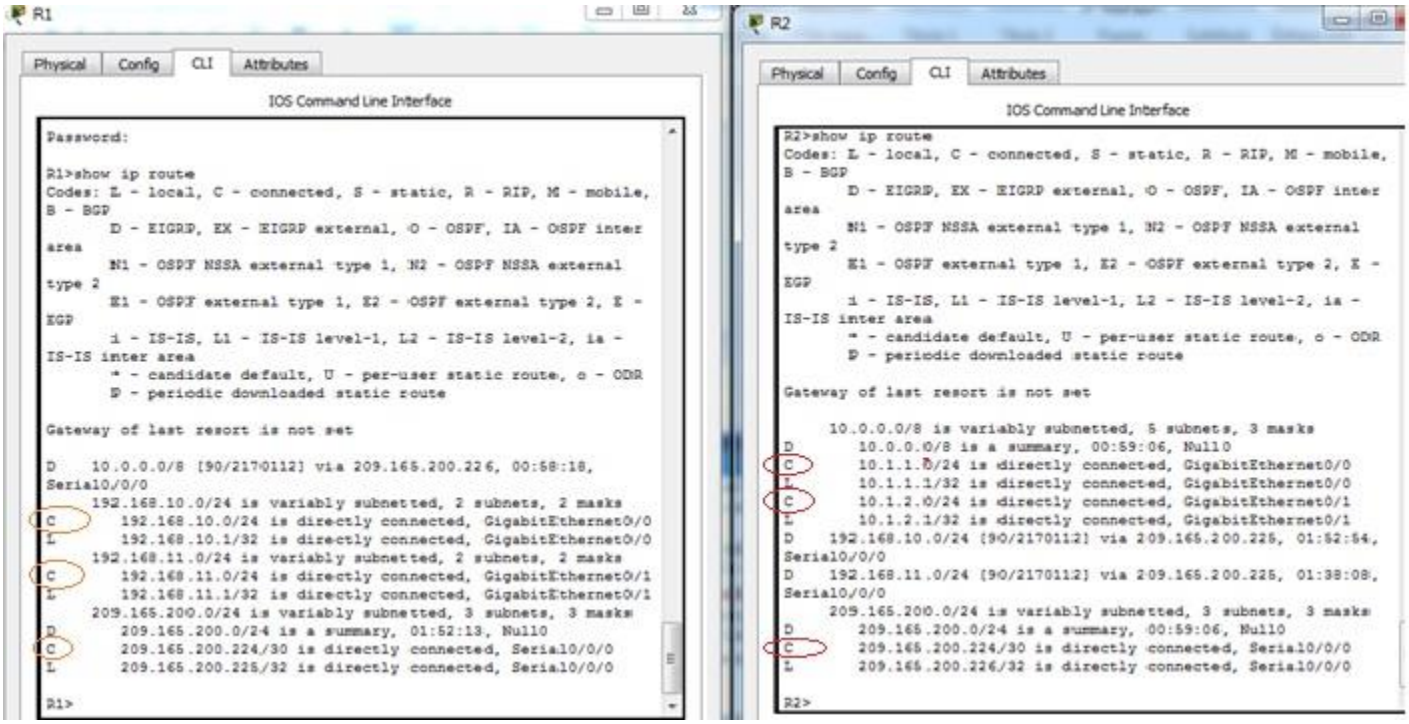


¿Qué parte de la configuración de la interfaz NO se muestra en el resultado del comando? La máscara de subred

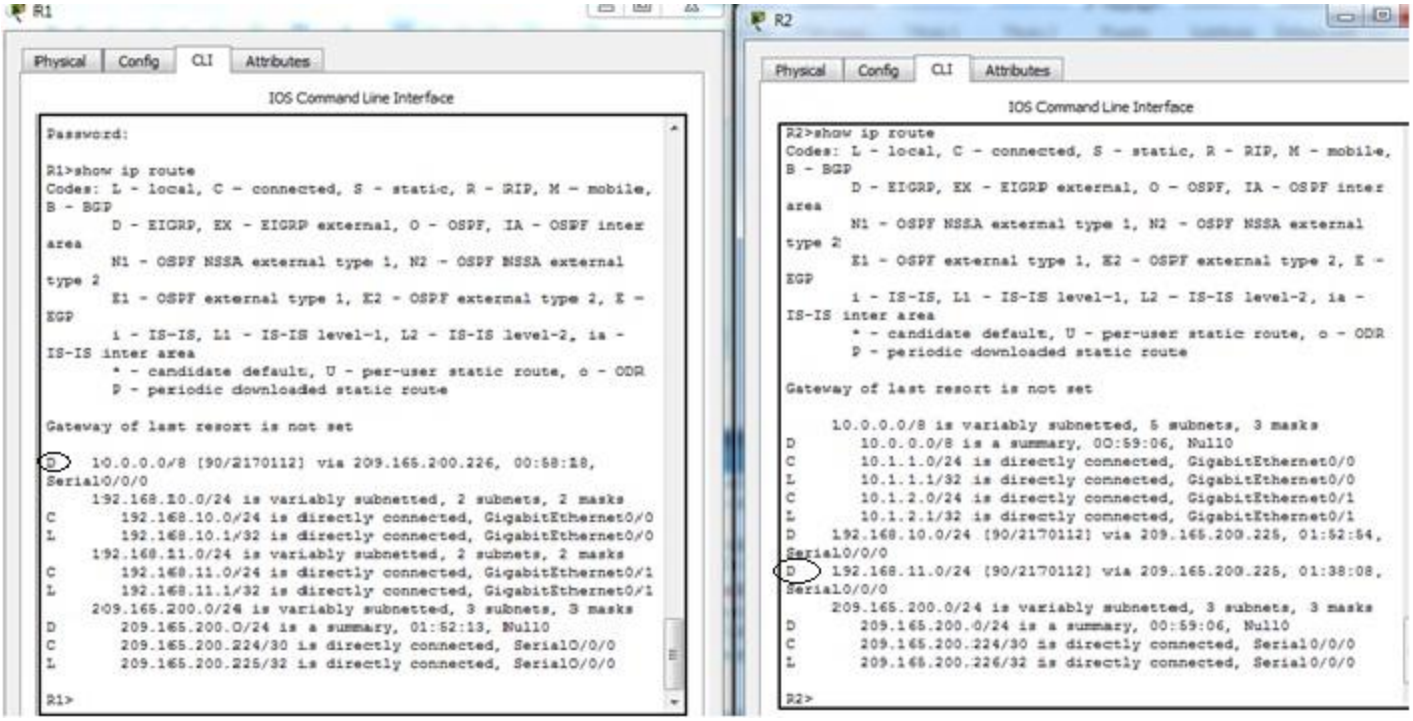
¿Qué comandos puede utilizar para verificar esta parte de la configuración? show run, show interfaces, show ip protocols

b. Utilice el comando show ip route en R1 y R2 para ver las tablas de enrutamiento actuales y responda las siguientes preguntas:

1) ¿Cuántas rutas conectadas (utilizan el código C) ve en cada router? 3

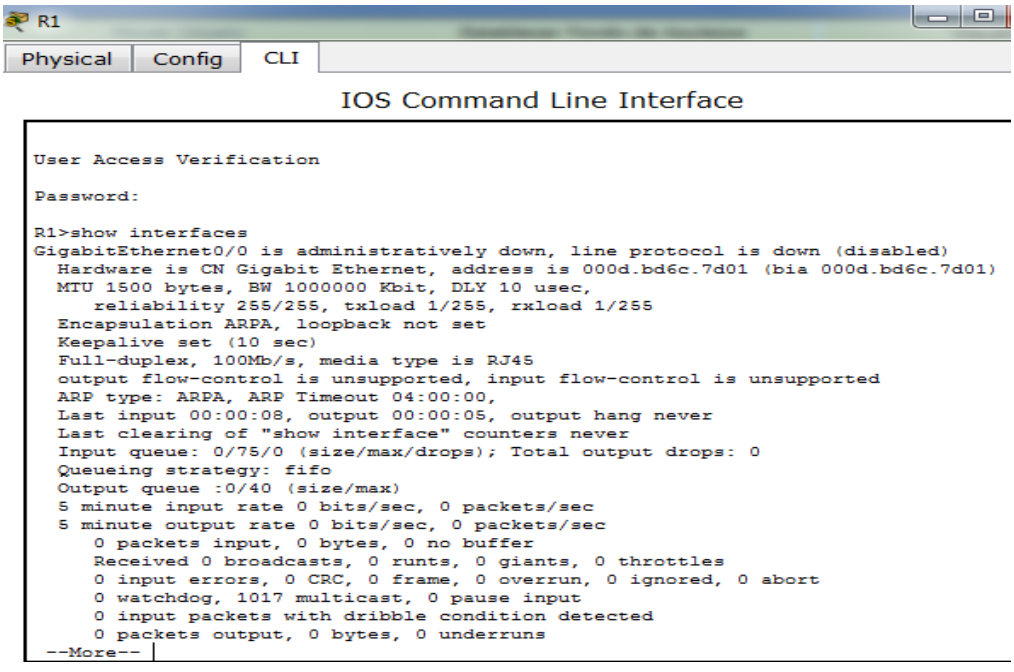


2) ¿Cuántas rutas EIGRP (utilizan el código D) ve en cada router? 2

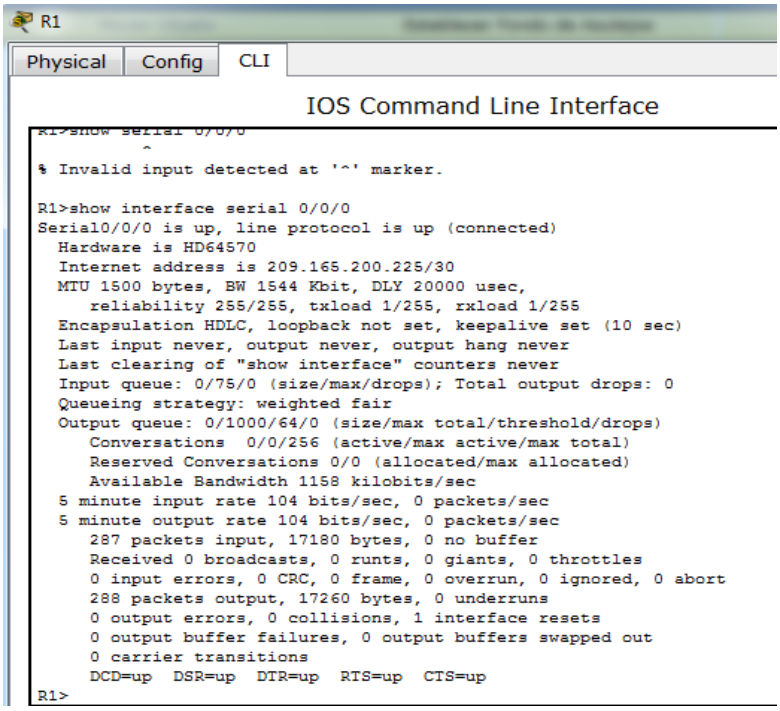


3) Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y Parte 1: Mostrar la información del router
Paso 1: Mostrar la información de la interfaz en el R1.

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

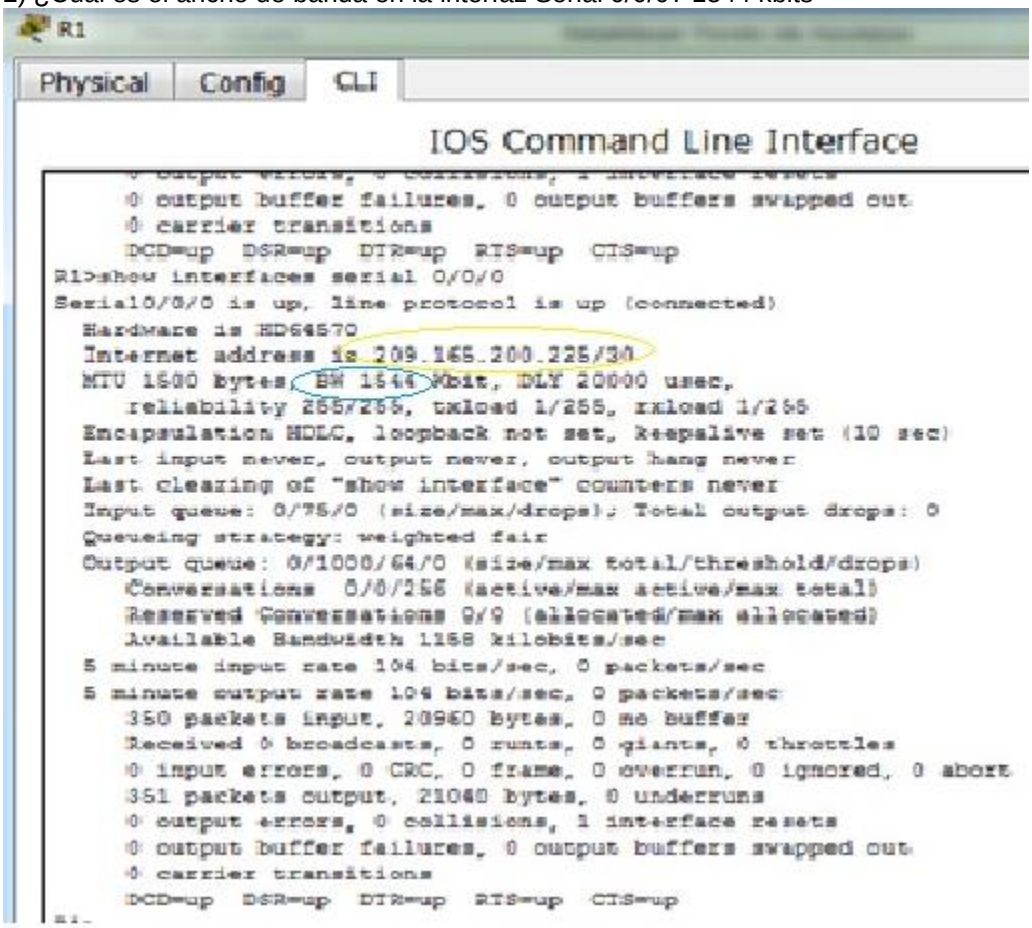


b. ¿Qué comando muestra solo la información de la interfaz Serial 0/0/0? show interface serial 0/0/0



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

1) ¿Cuál es la dirección IP configurada en el **R1**? 209.165.200.225/30
2) ¿Cuál es el ancho de banda en la interfaz Serial 0/0/0? 1544 kbits

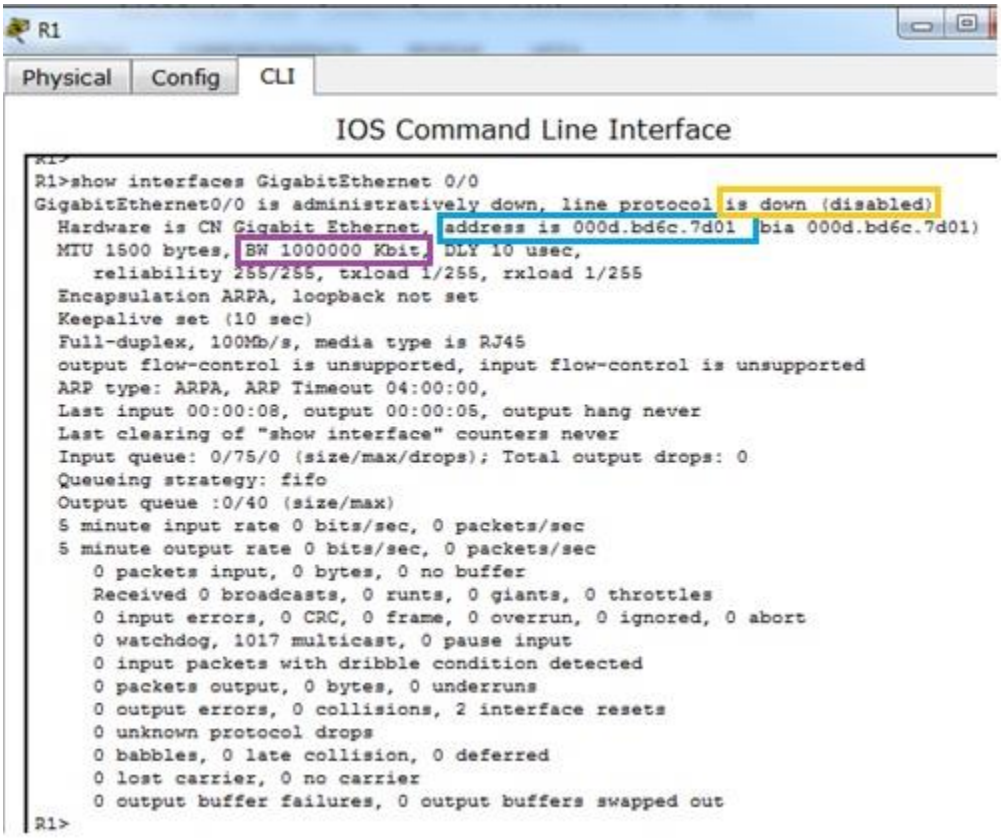


d. Introduzca el comando para visualizar las estadísticas de la interfaz GigabitEthernet 0/0 y responda las siguientes preguntas:

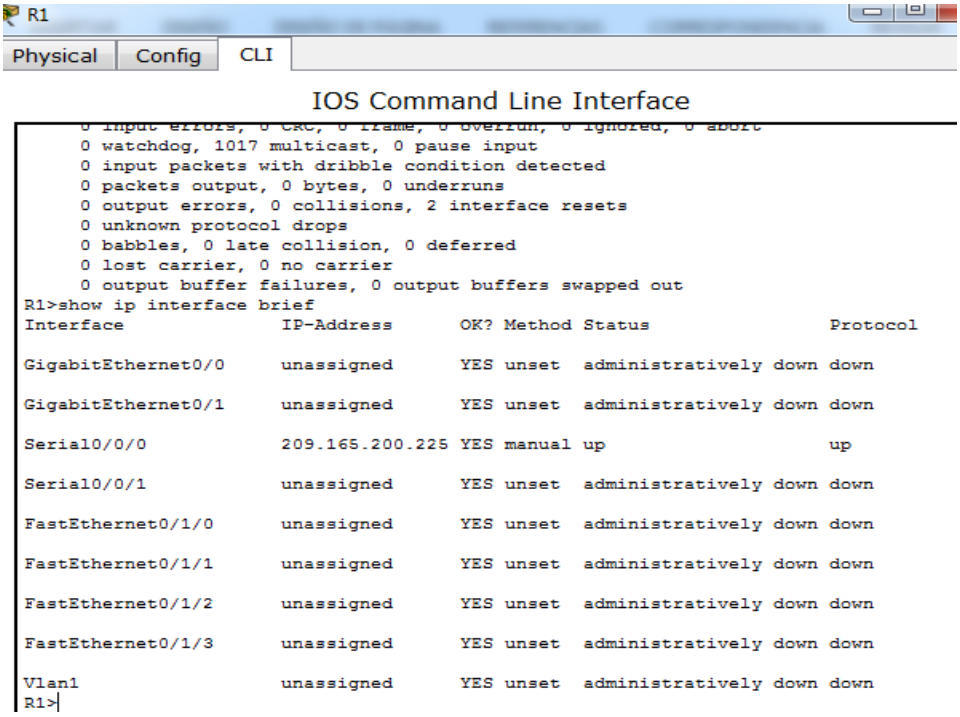
1) ¿Cuál es la dirección IP en el **R1**? No hay una dirección IP configurada en la interfaz GigabitEthernet 0/0.

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

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



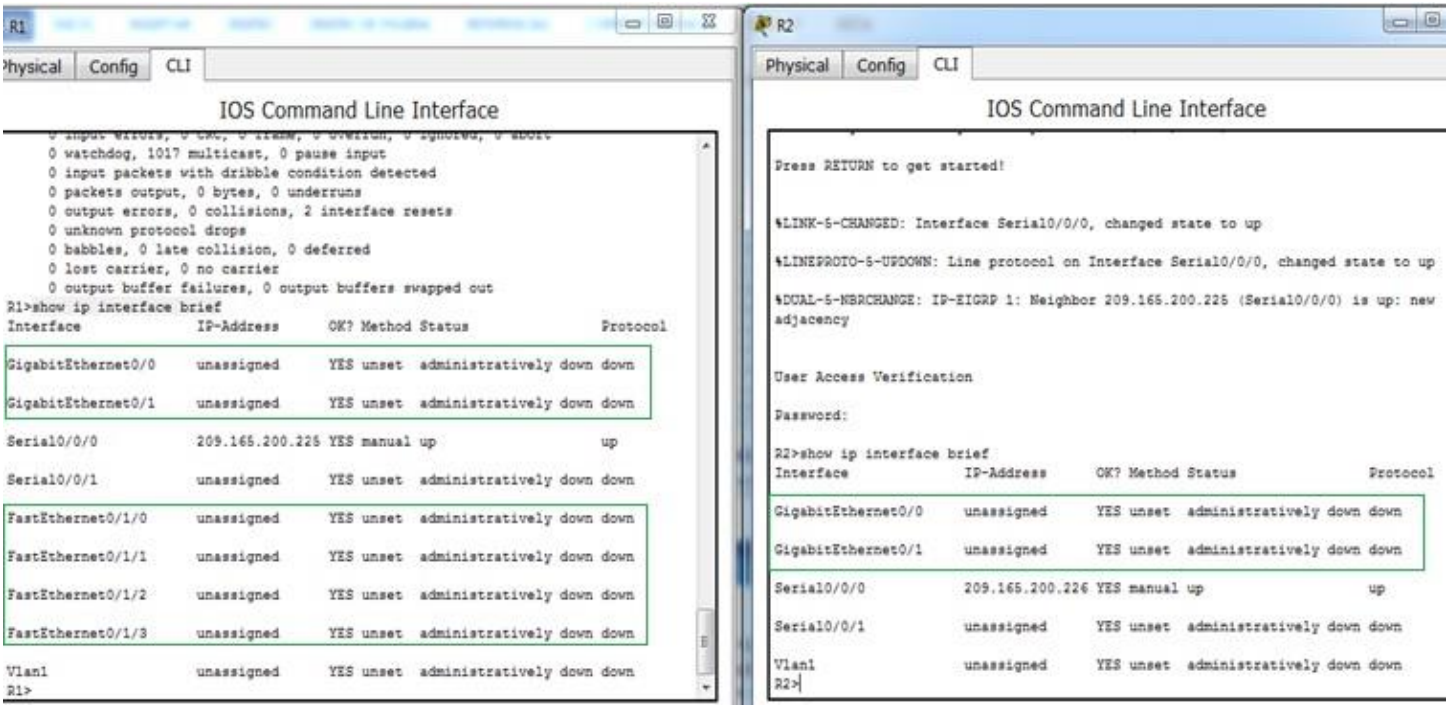
Paso 2: Mostrar una lista de resumen de las interfaces en el R1 a. ¿Qué comando muestra un breve resumen de las interfaces, los estados y las direcciones IP actualmente asignadas a ellas? show ip interface brief



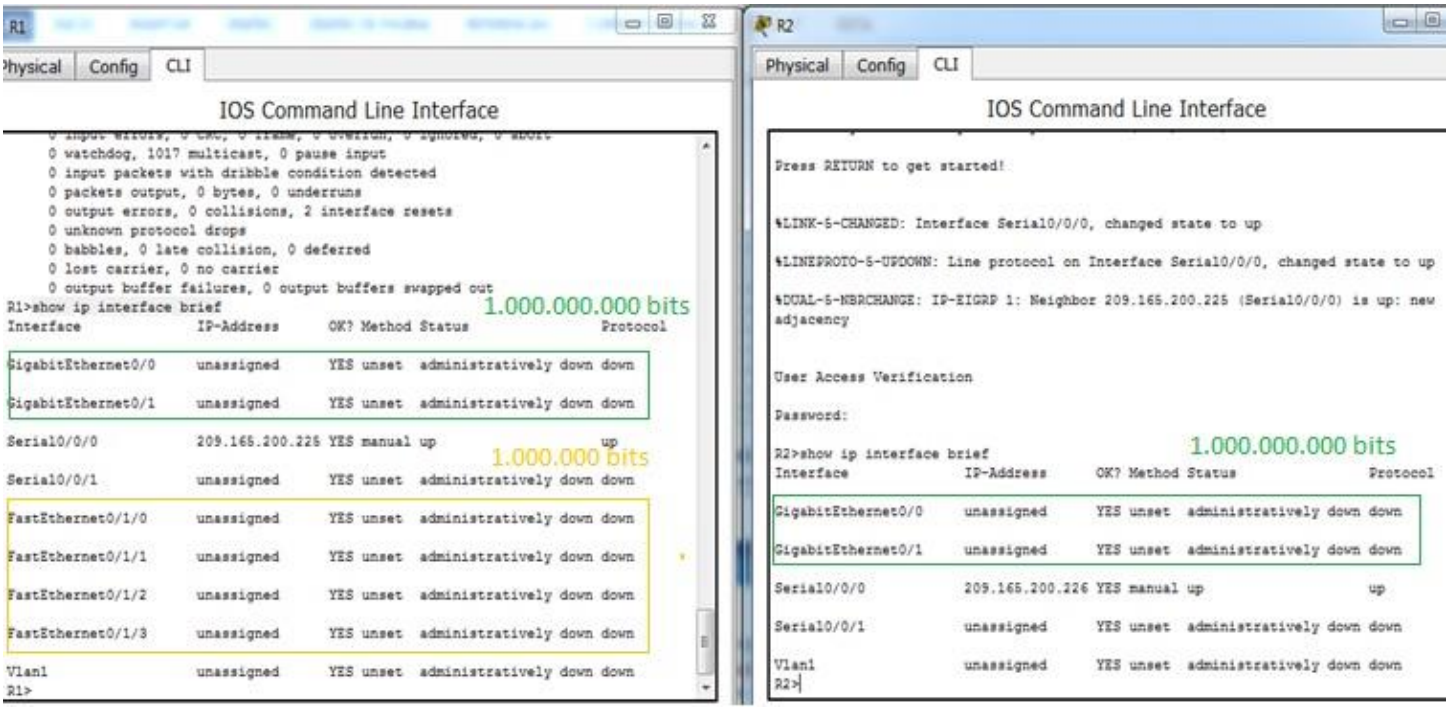
b. Introduzca el comando en cada router y responda las siguientes preguntas:

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

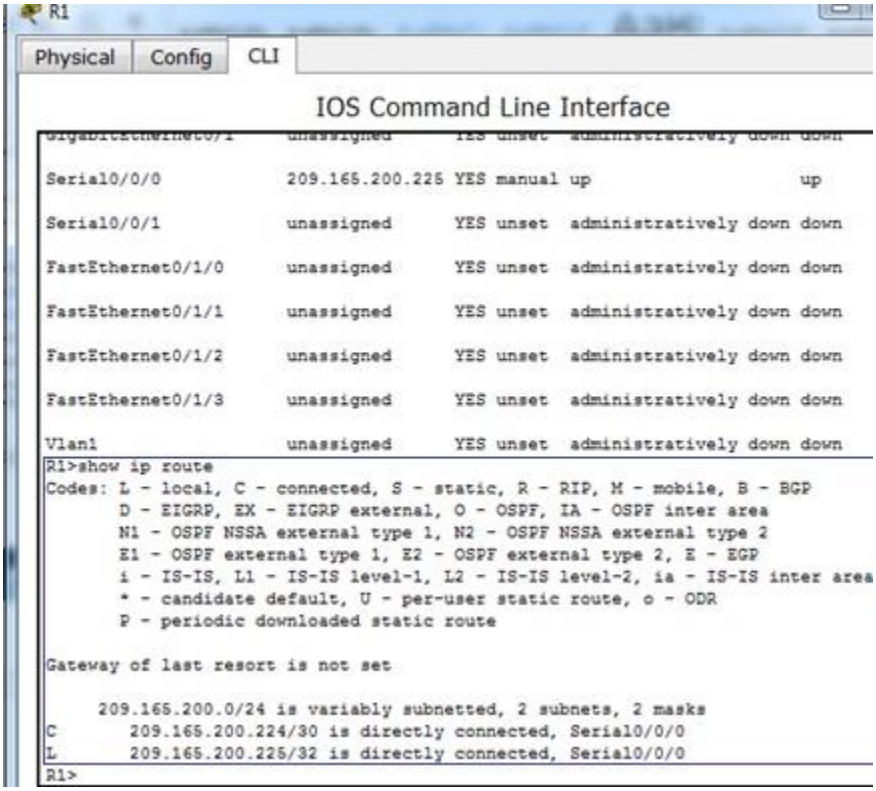
2) ¿Cuántas interfaces Ethernet hay en **R1** y **R2**? R1 tiene seis interfaces Ethernet y R2 tiene dos interfaces Ethernet.



3) ¿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 a. ¿Qué comando muestra el contenido de la tabla de enrutamiento? show ip route

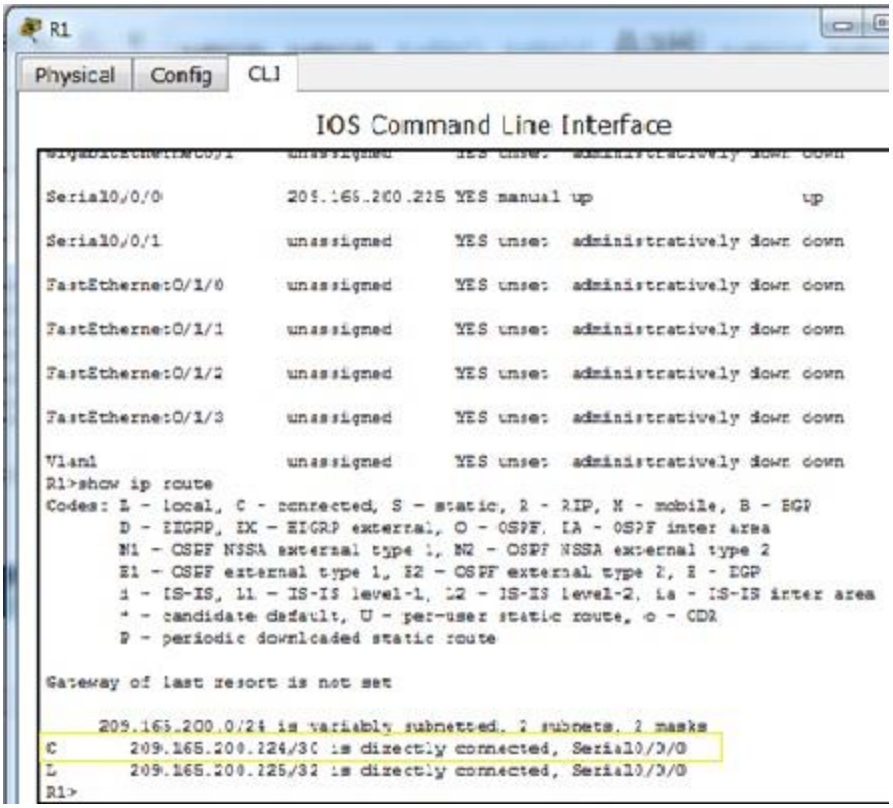


b. Introduzca el comando en el **R1** y responda las siguientes preguntas:

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

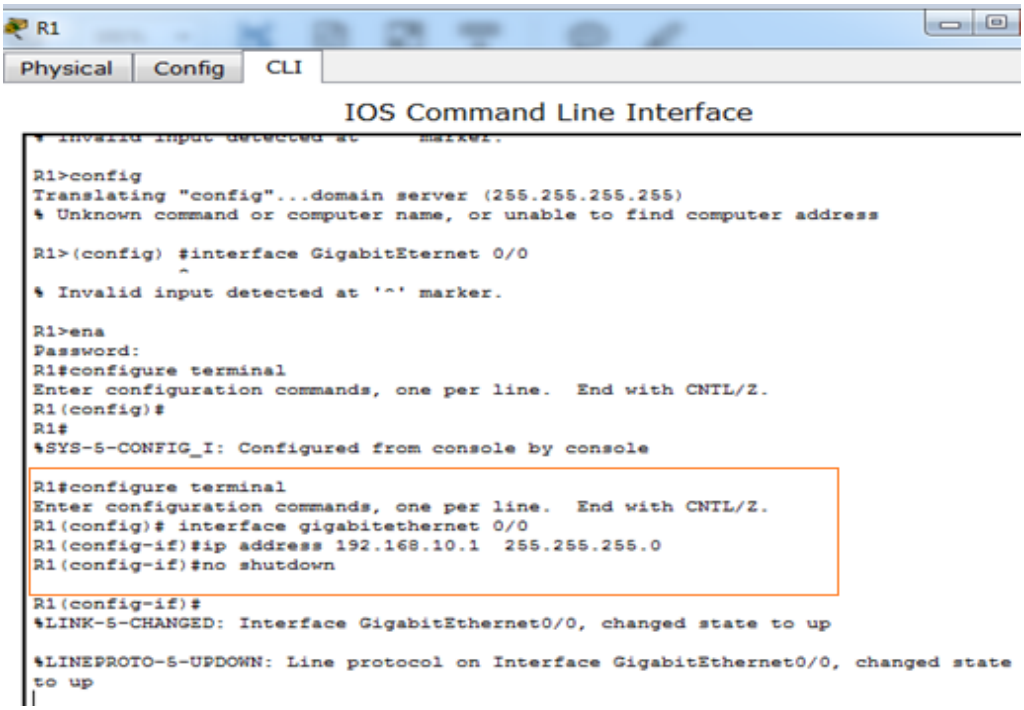
2) ¿Qué ruta se indica? 209.165.200.224/30

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.



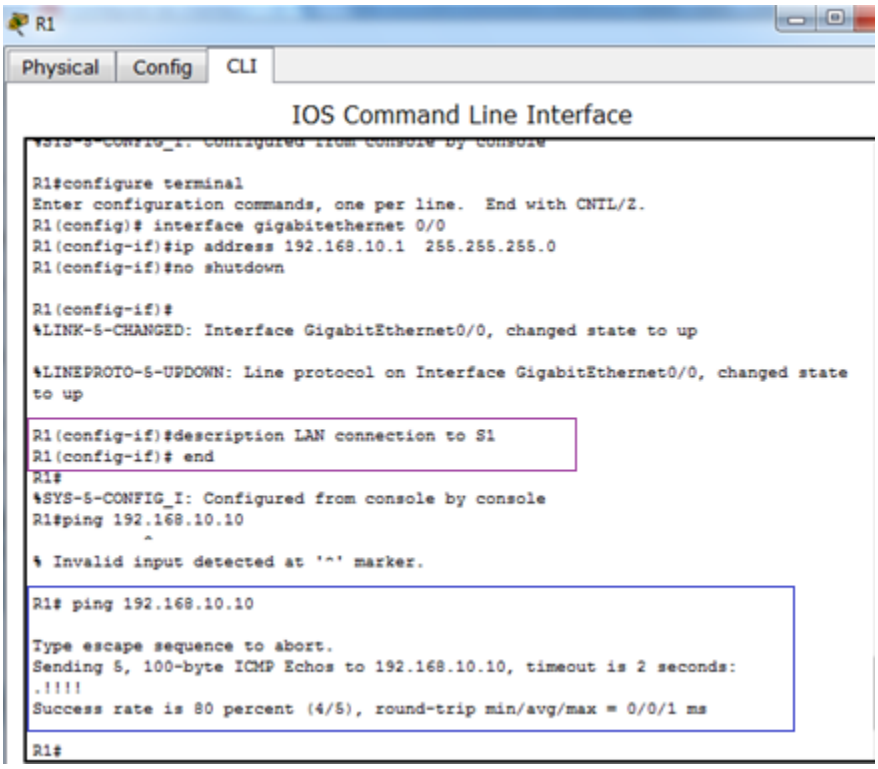
Parte 2: Configurar las interfaces del router
Paso 1: Configurar la interfaz GigabitEthernet 0/0 en el R1 a. Introduzca los siguientes comandos direccionar y activar la interfaz GigabitEthernet 0/0 en el **R1**:

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



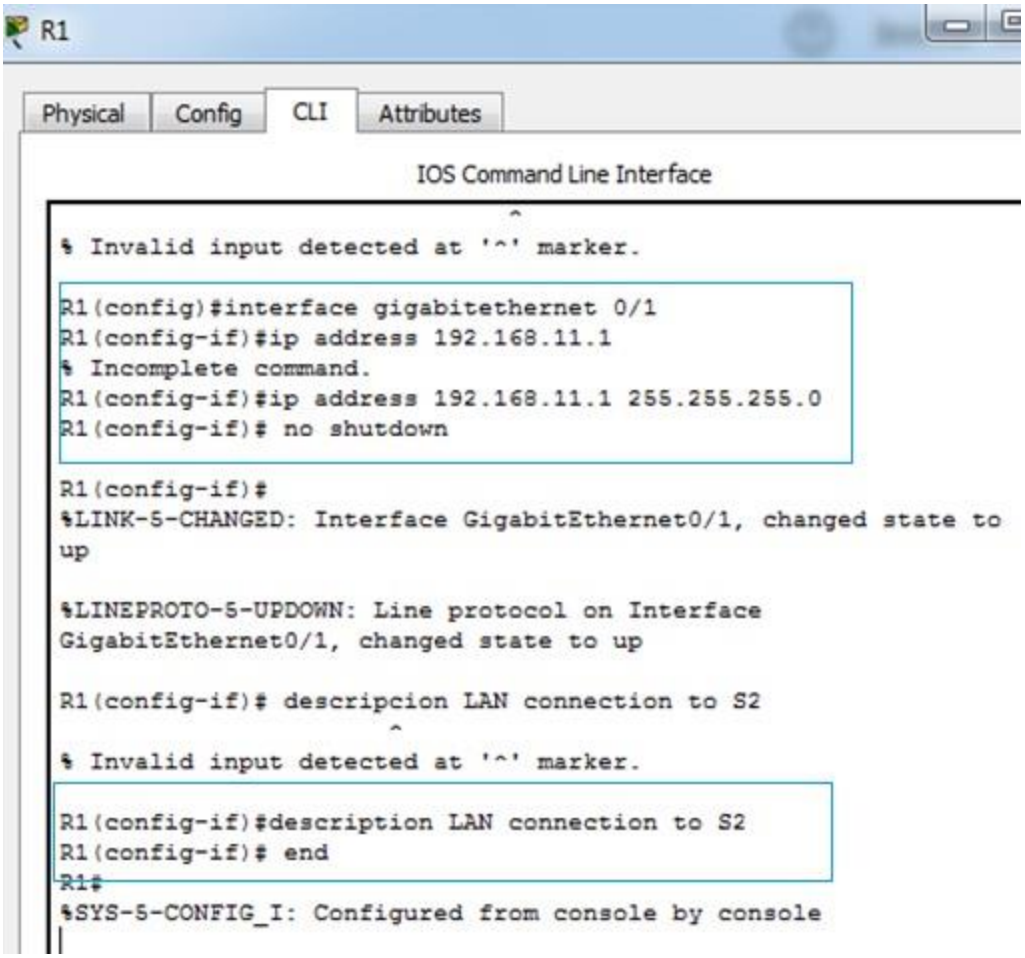
b. Es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. Configure una descripción de la interfaz que indique a qué dispositivo está conectada.
R1(config-if)# **description LAN connection to S1**
c. Ahora, el **R1** debe poder hacer ping a la PC1.

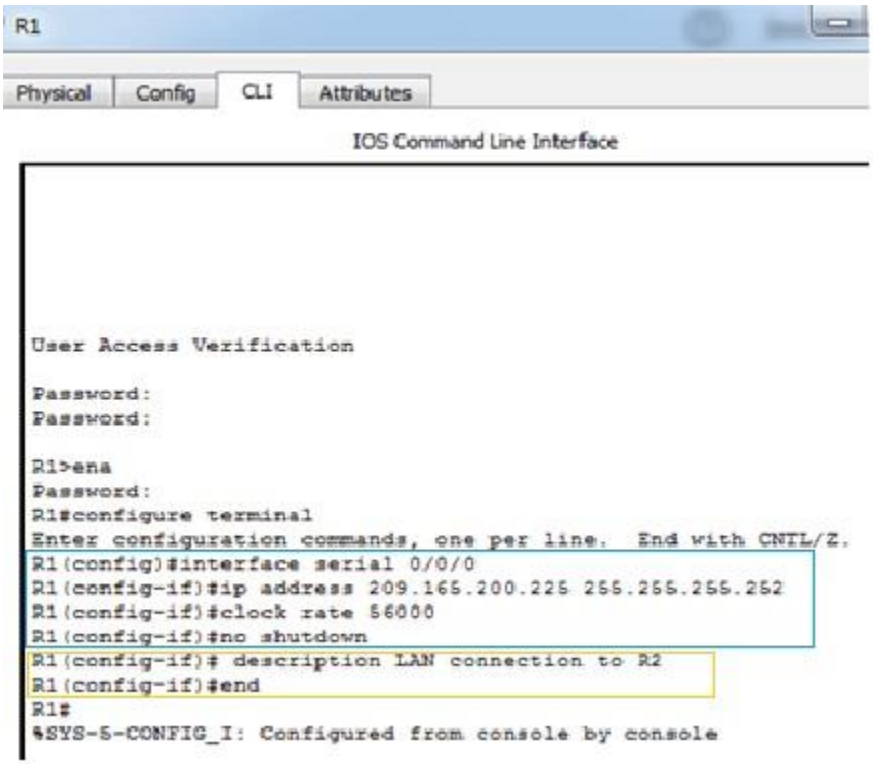
R1(config-if)# **end**
%SYS-5-CONFIG_I: Configured from console by console
R1# **ping 192.168.10.10**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

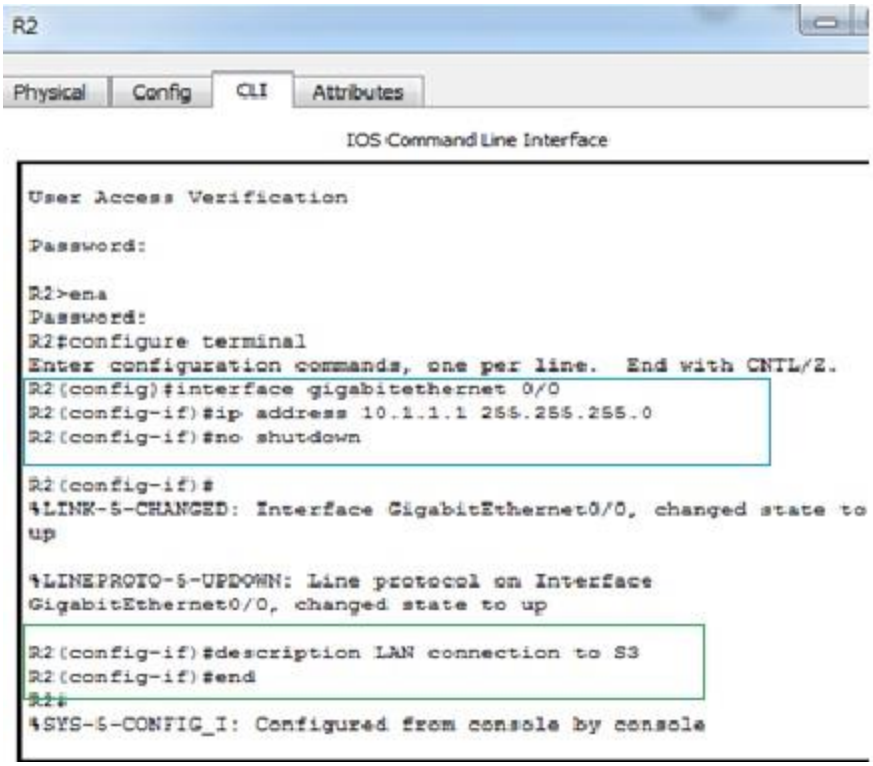


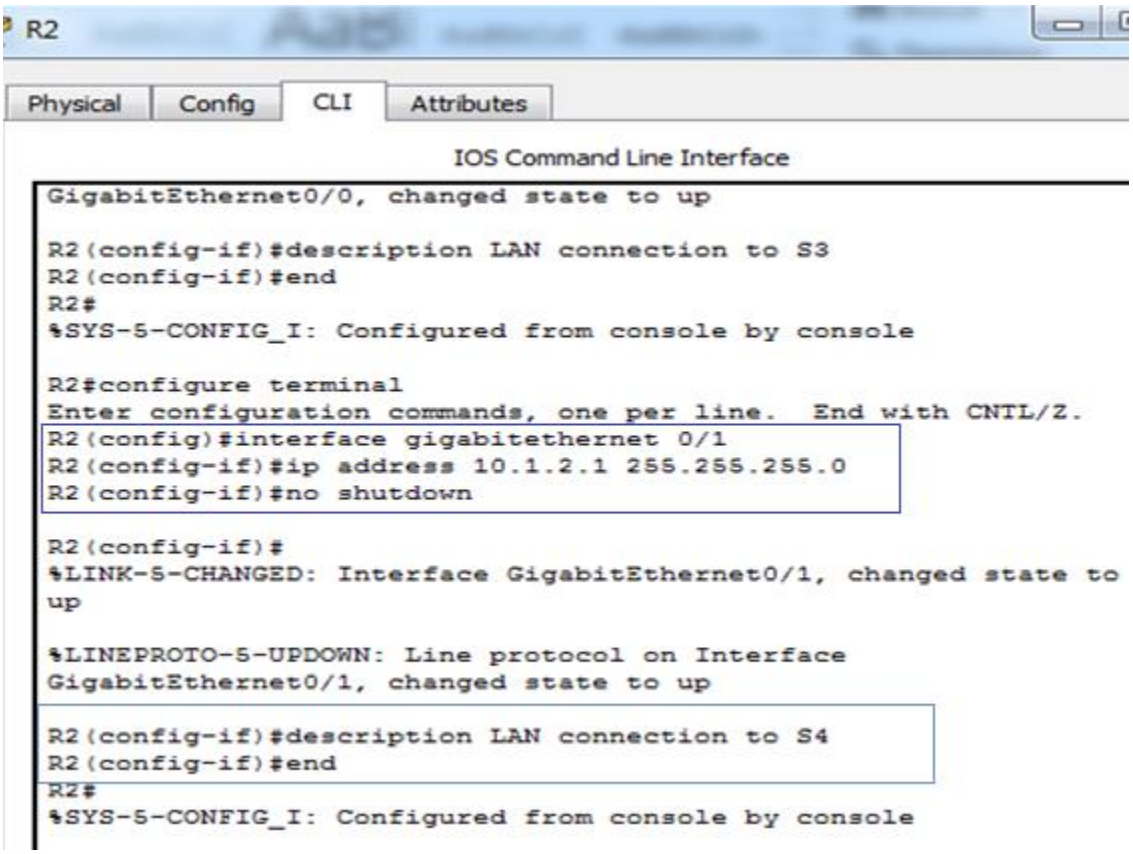
Paso 2: Configure las interfaces Gigabit Ethernet restantes en R1 y R2.
a. Utilice la información en la Addressing Table para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:
1) Introduzca la dirección IP y active la interfaz.
2) Configure una descripción apropiada.

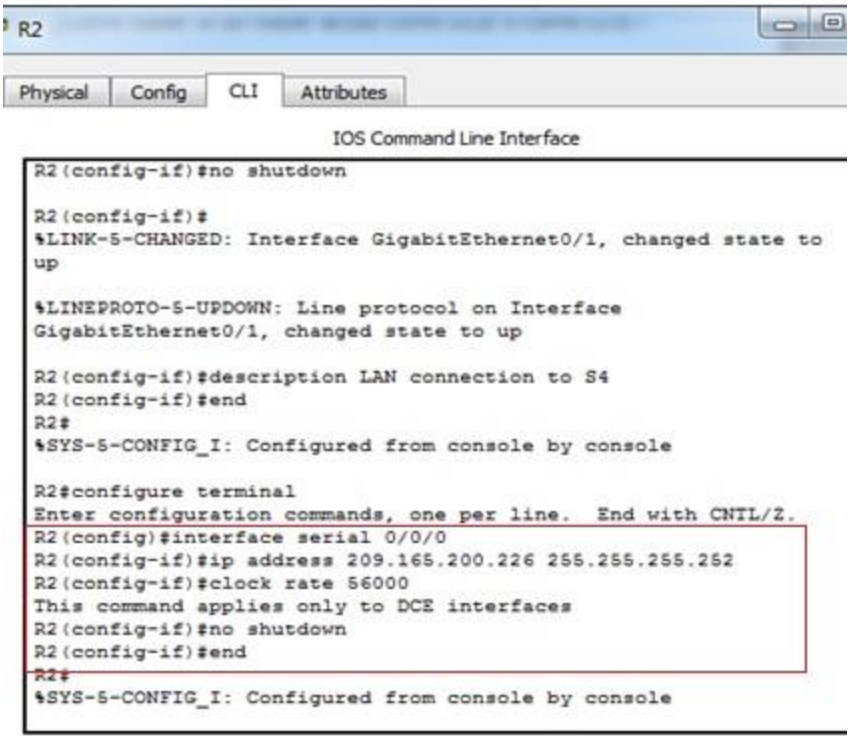
b. Verifique las configuraciones de las interfaces


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.11.1
% Incomplete command.
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(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
R1(config-if)# descripcion LAN connection to S2
% Invalid input detected at '^' marker.
R1(config-if)#description LAN connection to S2
R1(config-if)# end
R1#
%SYS-5-CONFIG_I: Configured from console by console


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
Password:
R1>ena
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.252
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
R1(config-if)# description LAN connection to R2
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
R2>ena
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#description LAN connection to S3
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
GigabitEthernet0/0, changed state to up
R2(config-if)#description LAN connection to S3
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitethernet 0/1
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)#description LAN connection to S4
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

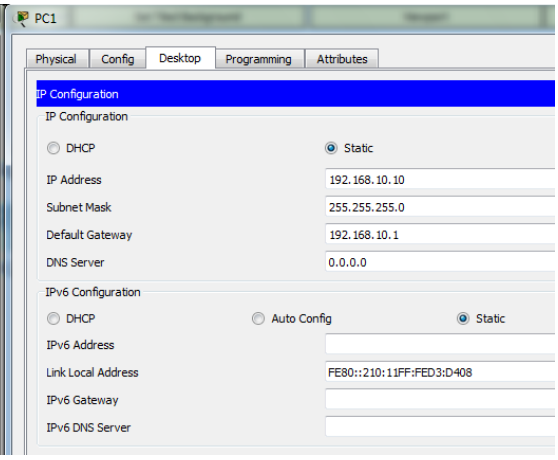


PT Activity: 02:23:10

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

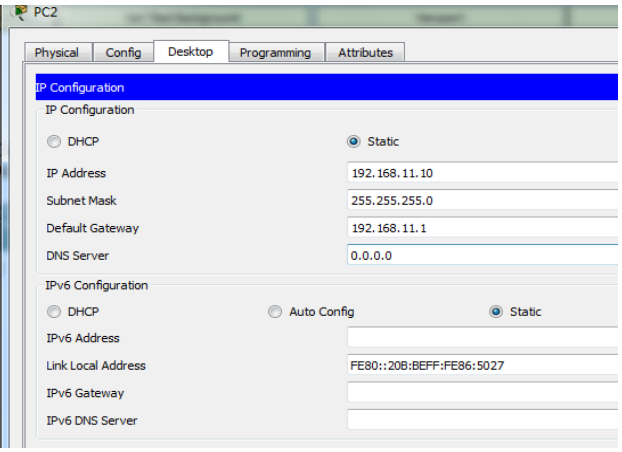


PT Activity: 02:23:56

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

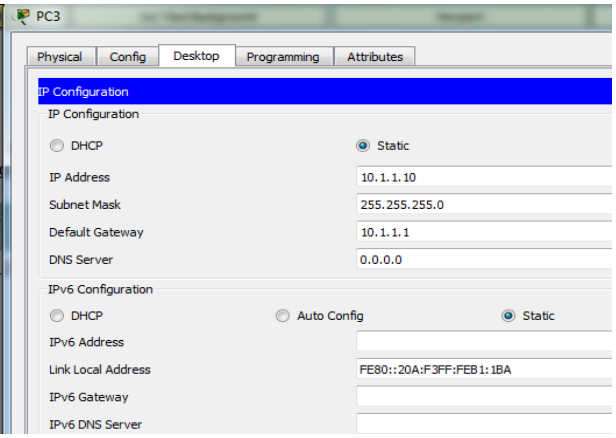


PT Activity: 02:24:33

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

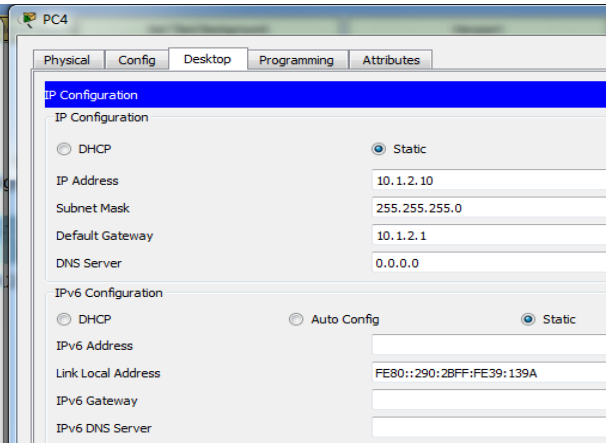
Objetivos

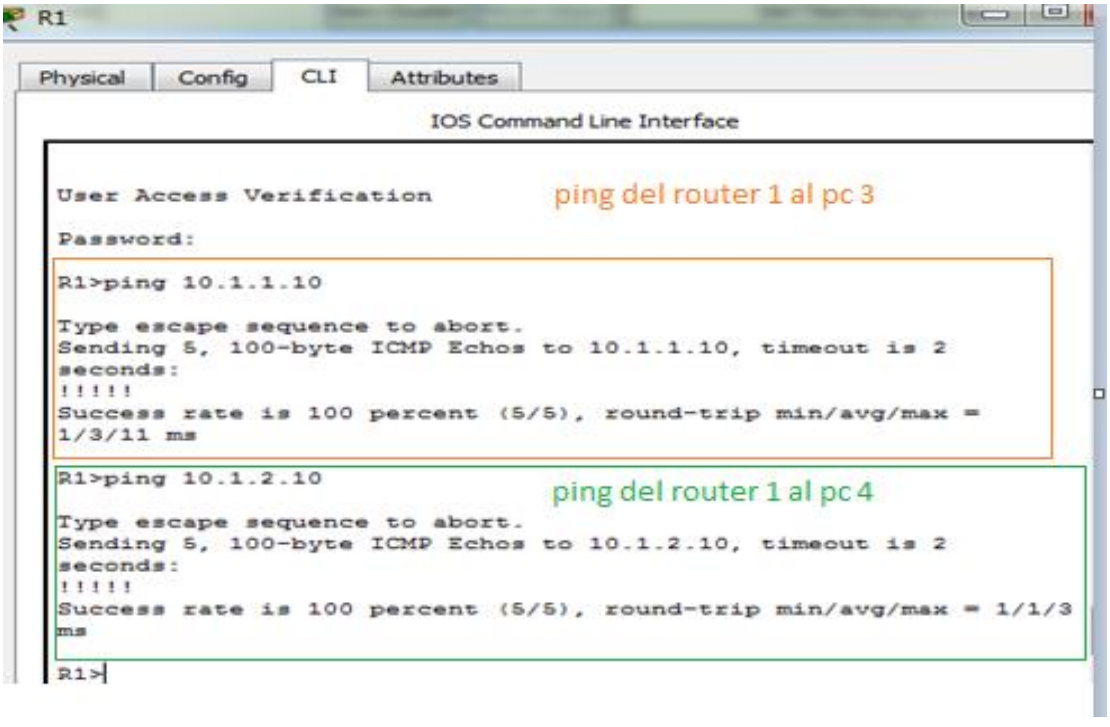


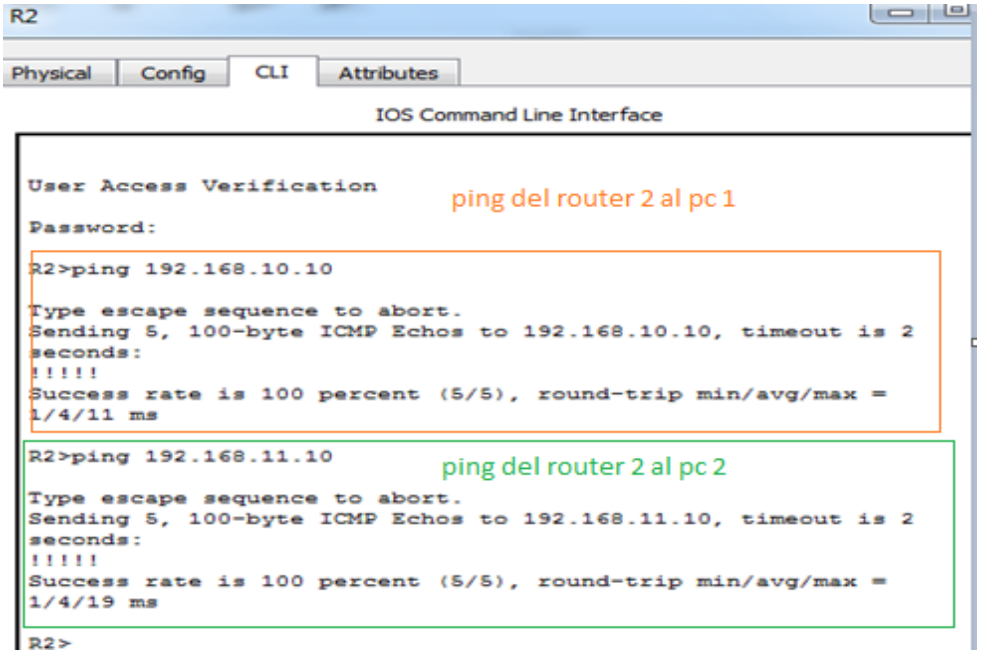
PT Activity: 02:25:16

Tabla de direccionamiento

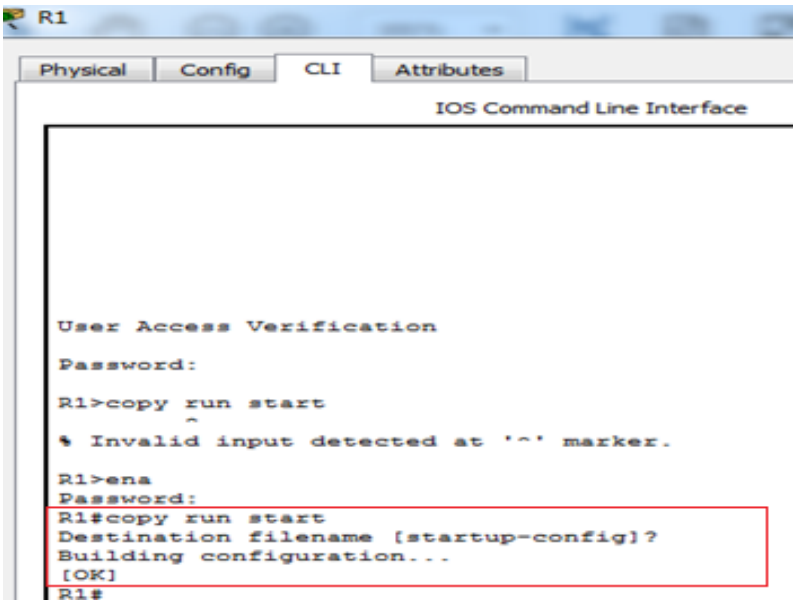
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	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

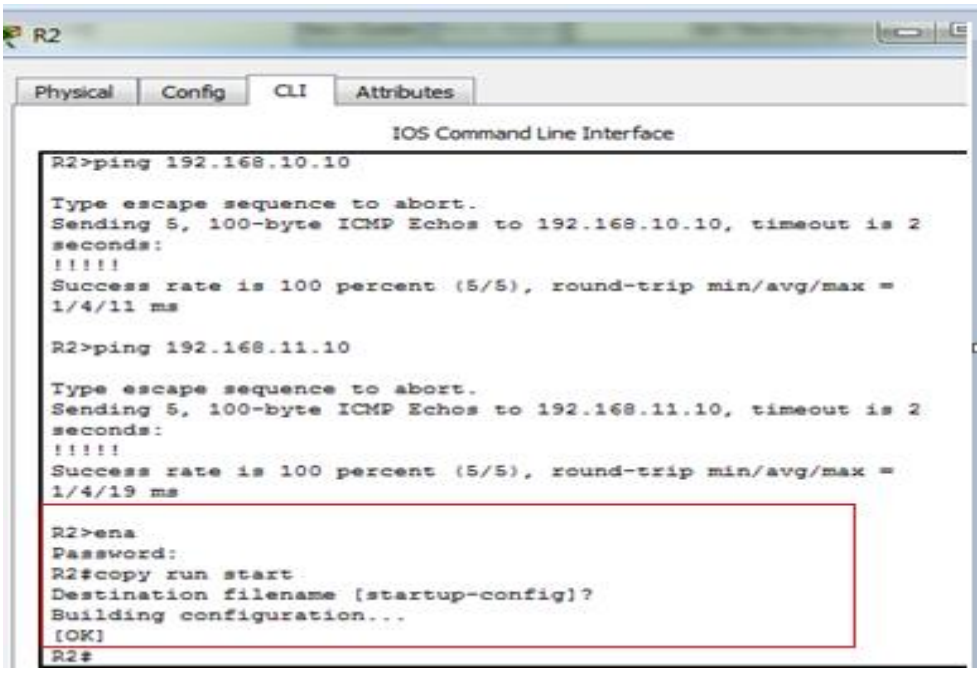






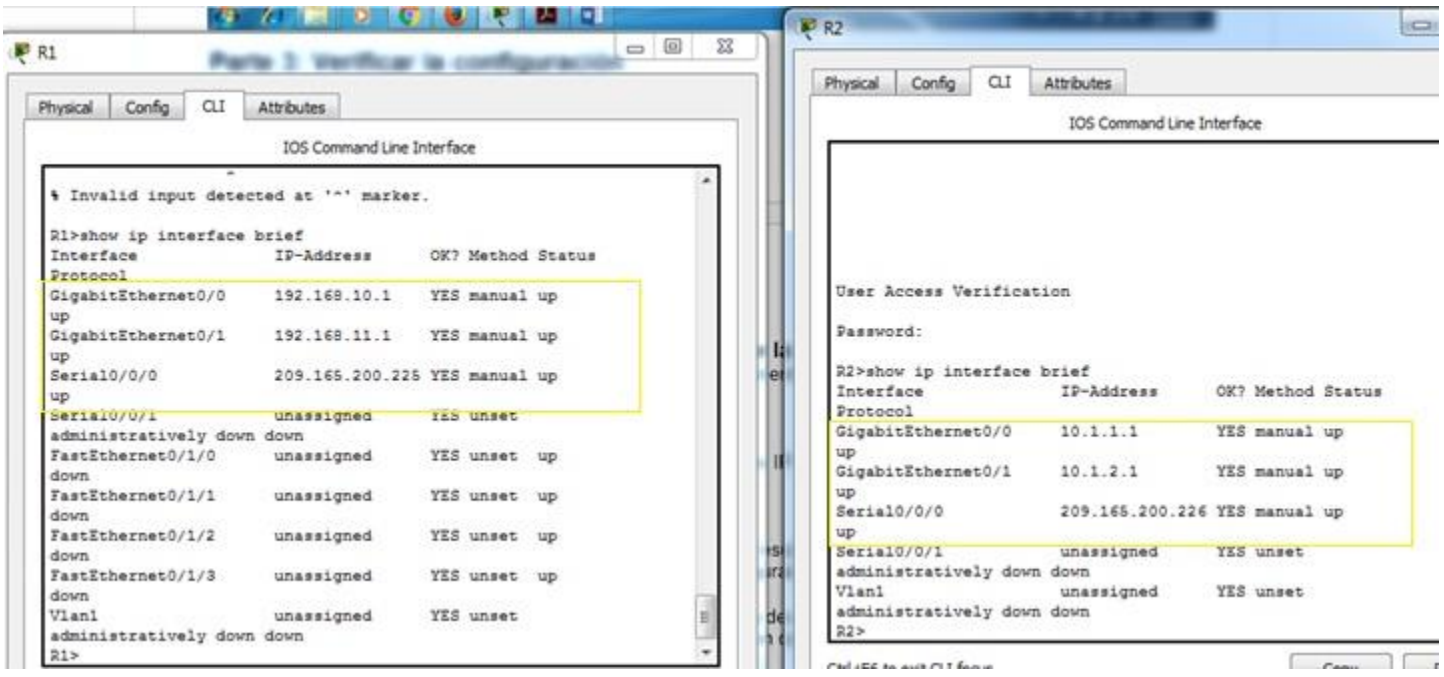
Paso 3: Realizar una copia de seguridad de las configuraciones en la NVRAM
Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó? copy run start





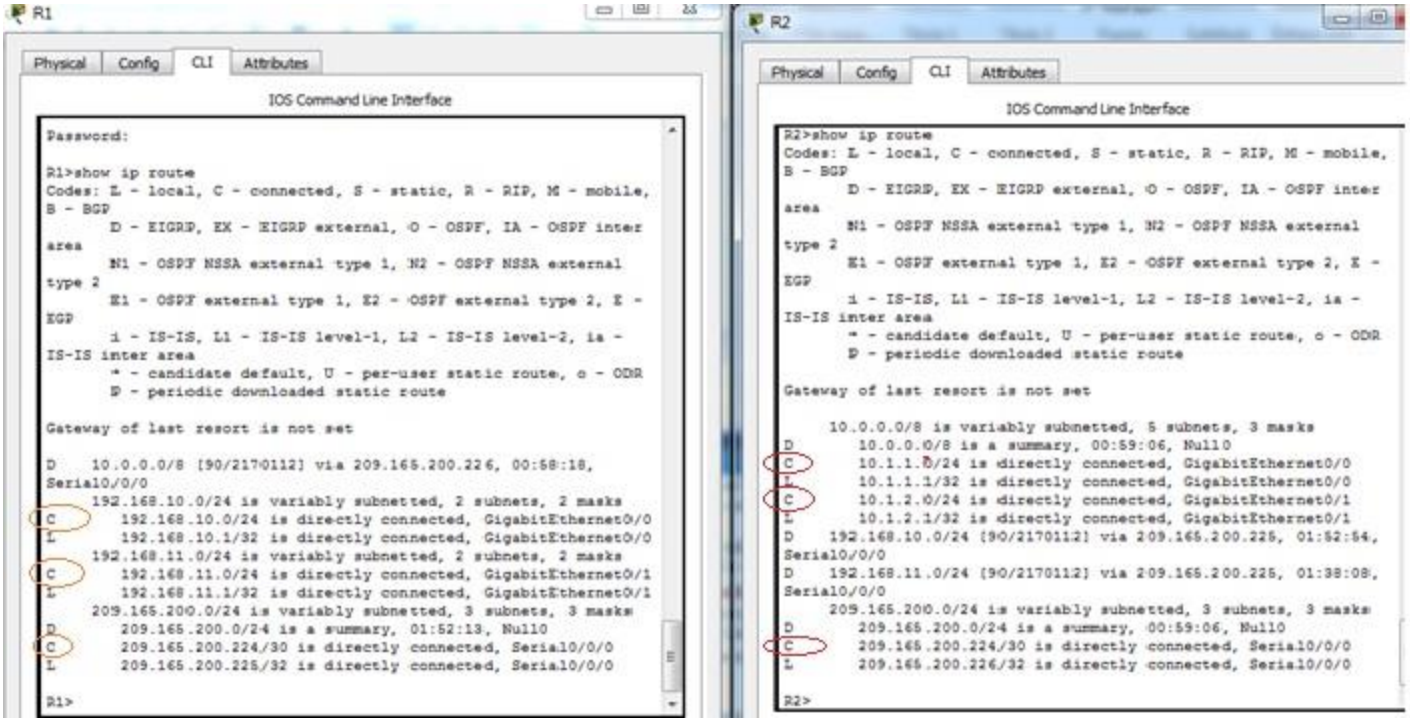
Parte 3: Verificar la configuración
Paso 1: Utilizar los comandos de verificación para revisar la configuración de la interfaz a. Utilice el comando **show ip interface brief** en **R1** y **R2** para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.

¿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:

1) ¿Cuántas rutas conectadas (utilizan el código **C**) ve en cada router? 3



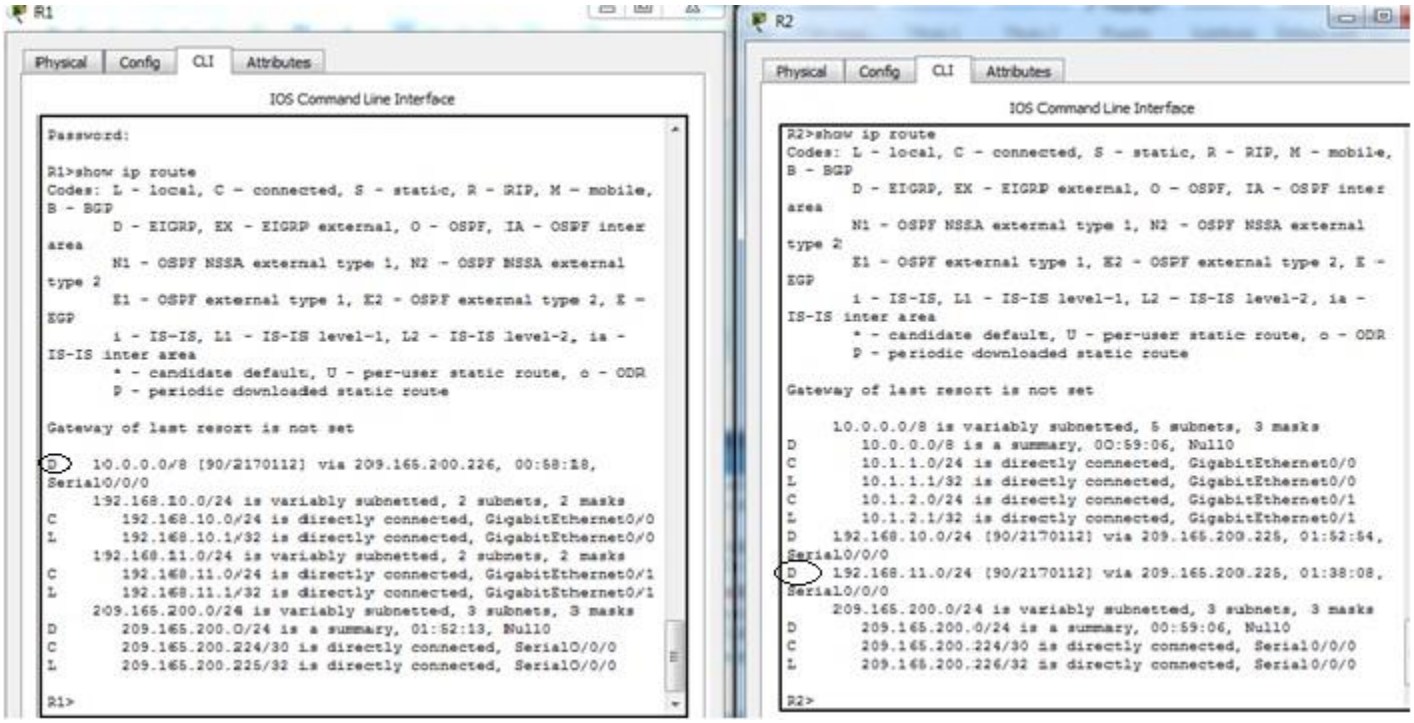
R1

```
Physical  Config  CLI  Attributes

IOS Command Line Interface

Password:

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

D    10.0.0.0/8 [90/2170112] via 209.165.200.226, 00:58:18,
Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 01:52:13, Null0
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>
```

R2

```
Physical  Config  CLI  Attributes

IOS Command Line Interface

R2>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

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:59:06, Null0
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
C       10.1.2.0/24 is directly connected, GigabitEthernet0/1
L       10.1.2.1/32 is directly connected, GigabitEthernet0/1
D    192.168.10.0/24 [90/2170112] via 209.165.200.225, 01:52:54,
Serial0/0/0
D    192.168.11.0/24 [90/2170112] via 209.165.200.225, 01:38:08,
Serial0/0/0
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 00:59:06, Null0
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.226/32 is directly connected, Serial0/0/0

R2>
```

2) ¿Cuántas rutas EIGRP (utilizan el código **D**) ve en cada router? 2



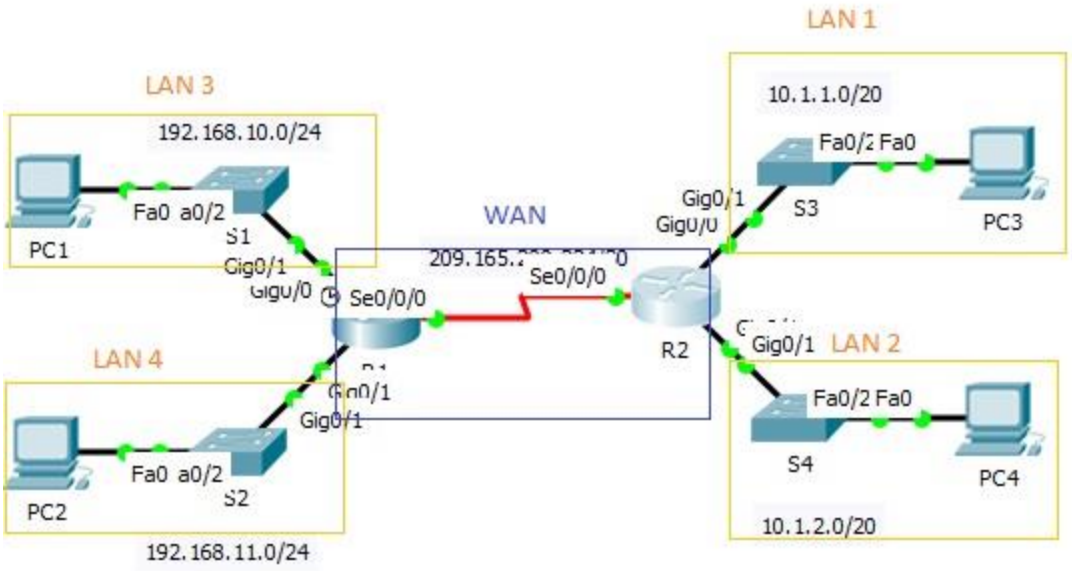
R1

```
Physical  Config  CLI  Attributes

IOS Command Line Interface

Password:

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

D    10.0.0.0/8 [90/2170112] via 209.165.200.226, 00:58:18,
Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 01:52:13, Null0
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>
```

R2

```
Physical  Config  CLI  Attributes

IOS Command Line Interface

R2>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

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:59:06, Null0
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
C       10.1.2.0/24 is directly connected, GigabitEthernet0/1
L       10.1.2.1/32 is directly connected, GigabitEthernet0/1
D    192.168.10.0/24 [90/2170112] via 209.165.200.225, 01:52:54,
Serial0/0/0
D    192.168.11.0/24 [90/2170112] via 209.165.200.225, 01:38:08,
Serial0/0/0
     209.165.200.0/24 is variably subnetted, 3 subnets, 3 masks
D       209.165.200.0/24 is a summary, 00:59:06, Null0
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.226/32 is directly connected, Serial0/0/0

R2>
```

3) 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



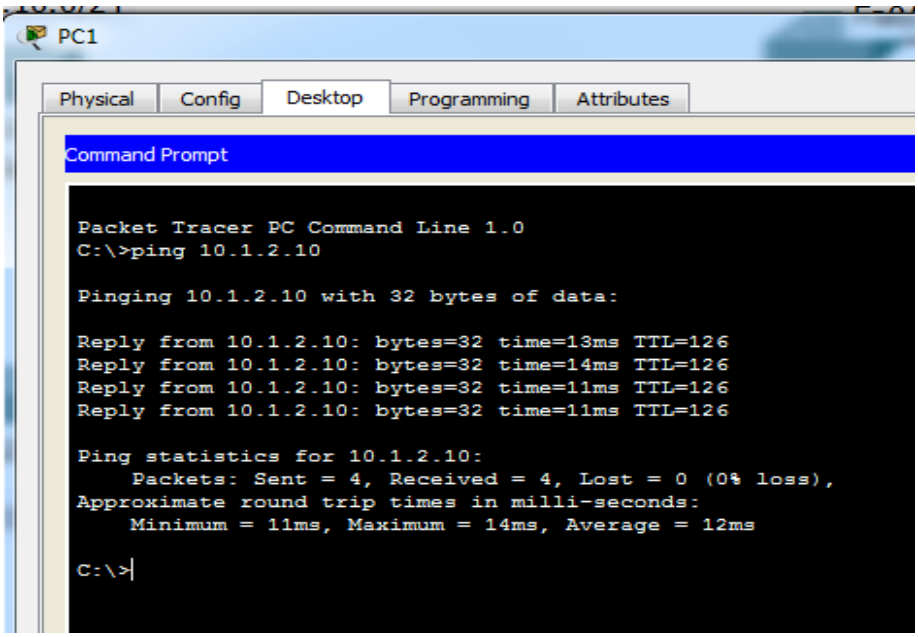
4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? sí

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

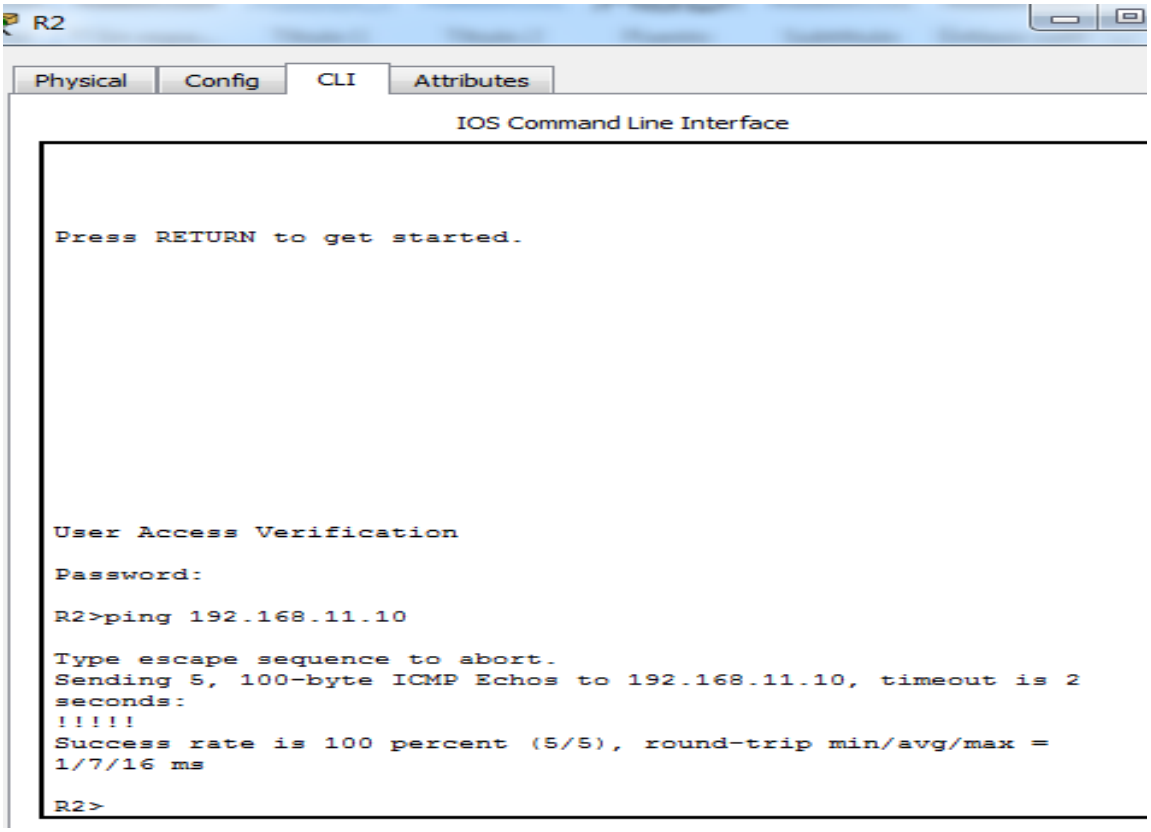
Paso 2: Probar la conectividad de extremo a extremo a través de la red

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:

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

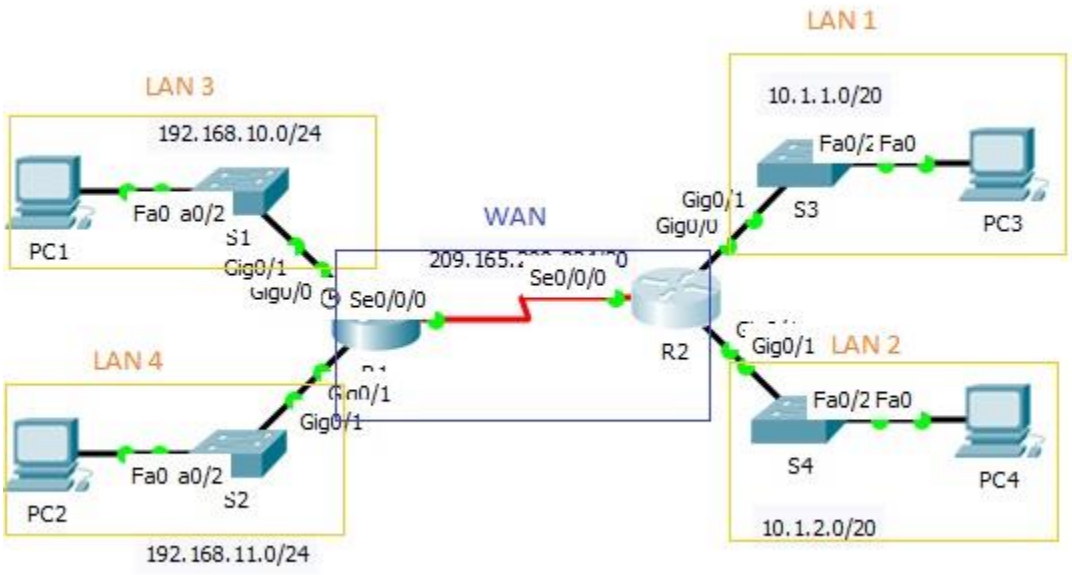


• Desde la línea de comandos en el R2, haga ping a la PC2.



Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping

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



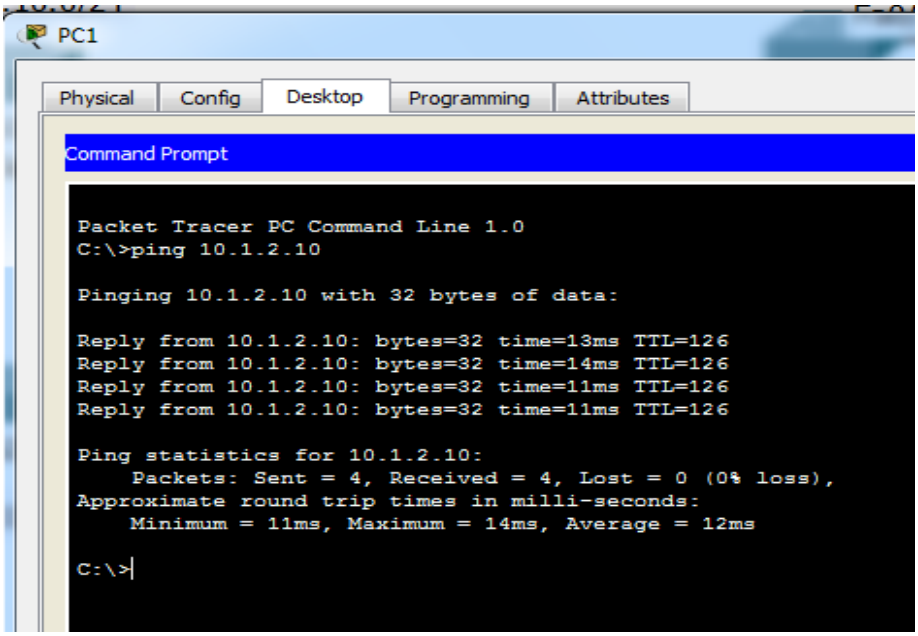
4) ¿Esta cantidad coincide con la cantidad de rutas C y D que se muestran en la tabla de enrutamiento? sí

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

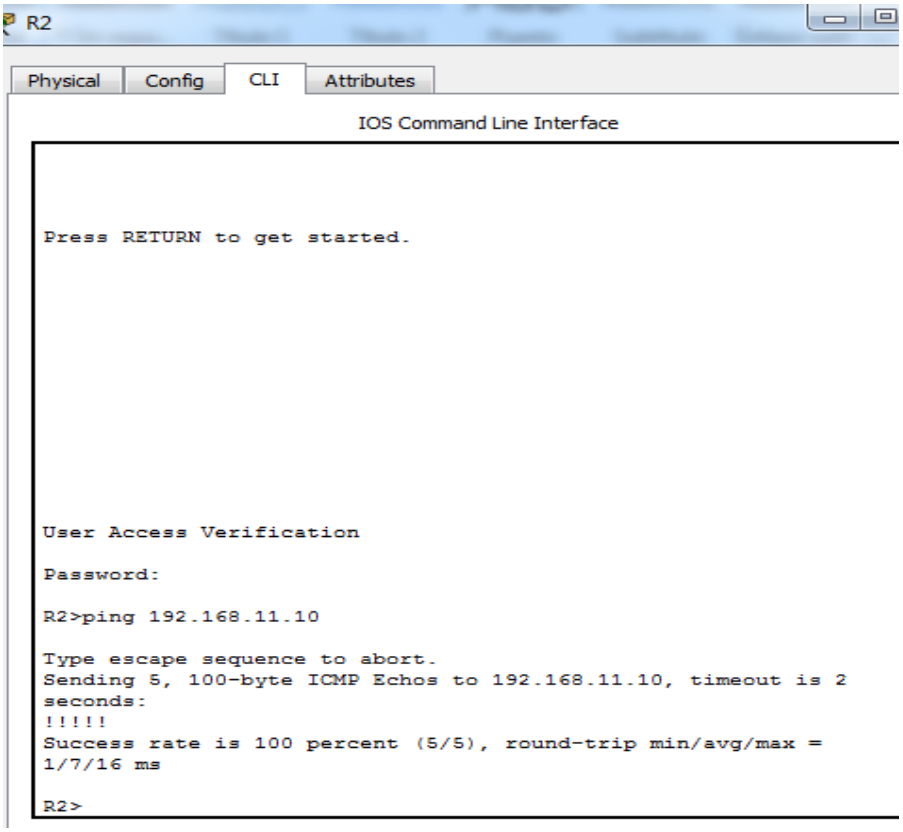
Paso 2: Probar la conectividad de extremo a extremo a través de la red

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:

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



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



Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping

6.4.3.4 Packet Tracer: Resolución de problemas del gateway predeterminado

Topología

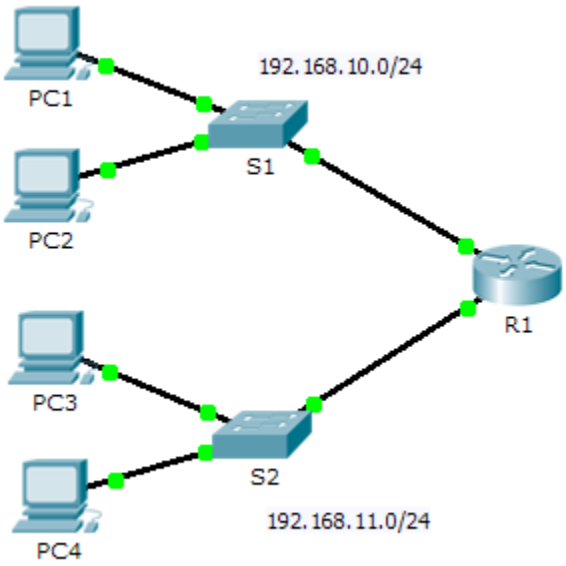


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No applicable
	G0/1	192.168.11.1	255.255.255.0	No applicable
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

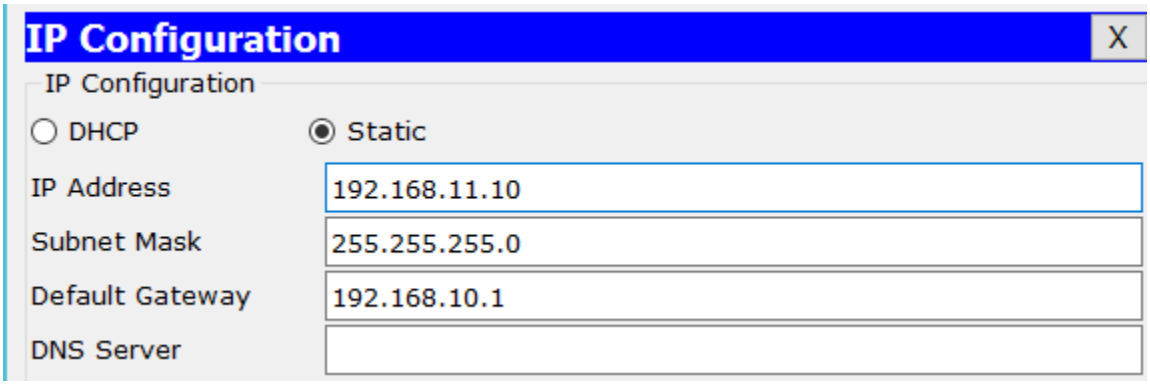
Para que un dispositivo se comunique a través de varias redes, debe estar configurado con una dirección IP, una máscara de subred y un gateway predeterminado. El gateway predeterminado se utiliza cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway 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.

PC1

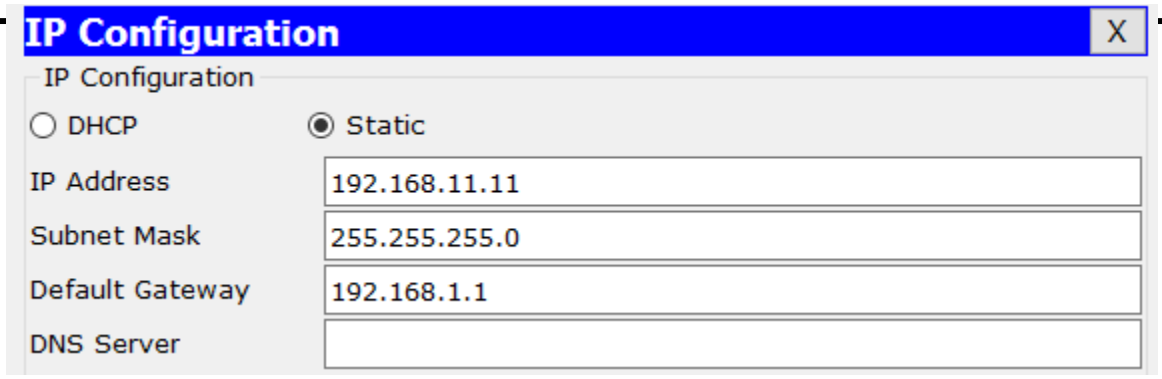


SE CAMBIA IP POR 192.168.10.10

PC2 SE ENCUENTRA CORRECTO

PC3 SE ENCUENTRA CORRECTO

PC4

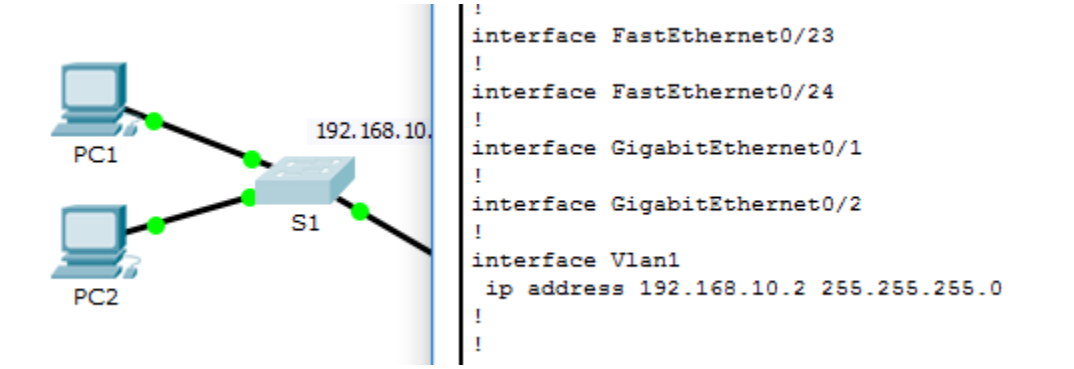


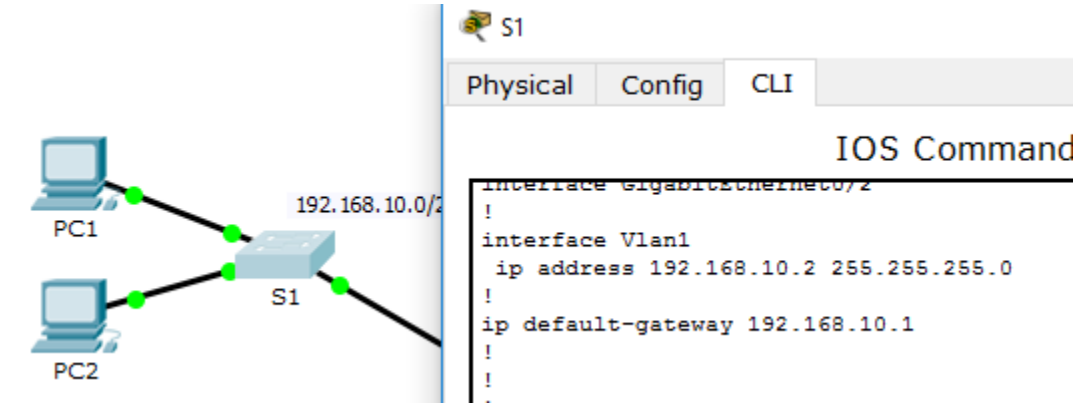
SE CAMBIA PUERTA DE ENLACE POR 192.168.1.1

VERIFICANDO S1

NO TIENE PUERTA DE ENLACE

LA CONFIGURAMOS CON IP DEFAULT-GATEWAY 192.168.10.1

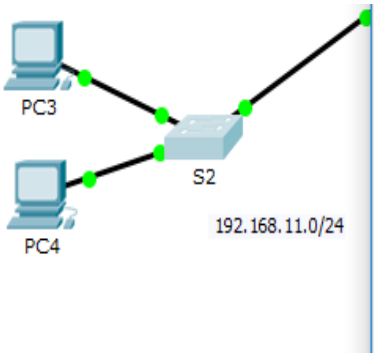




VERIFICANDO S2

NO TIENE INTERFACE VLAN

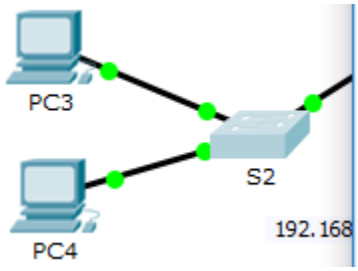
LA CONFIGURAMOS




```
S2>ENABLE
S2#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#INTERFACE VLAN 1
S2(config-if)#IP ADDRESS 192.168.11.2 255.255.255.0
S2(config-if)#
```

Copy Paste

VERIFICAMOS CON SHOW RUNNING-CONFIG




```
interface Vlan1
 ip address 192.168.11.2 255.255.255.0
!
ip default-gateway 192.168.11.1
!
!
!
!
line con 0
```

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

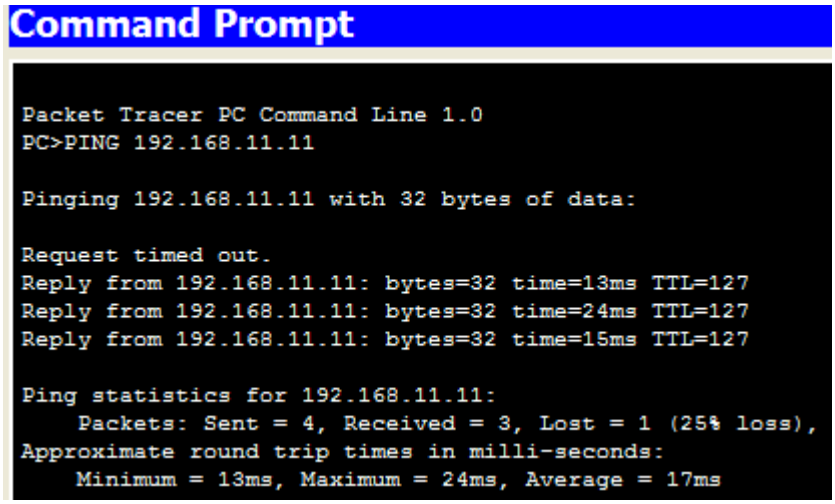
Prueba	¿Se realizó correctamente?	Problemas	Solución	Verificado
PC1 a PC2	**No**	**Dirección IP en la PC1**	**Cambiar la dirección IP de la PC1**	
PC1 a S1				
PC1 a R1				

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

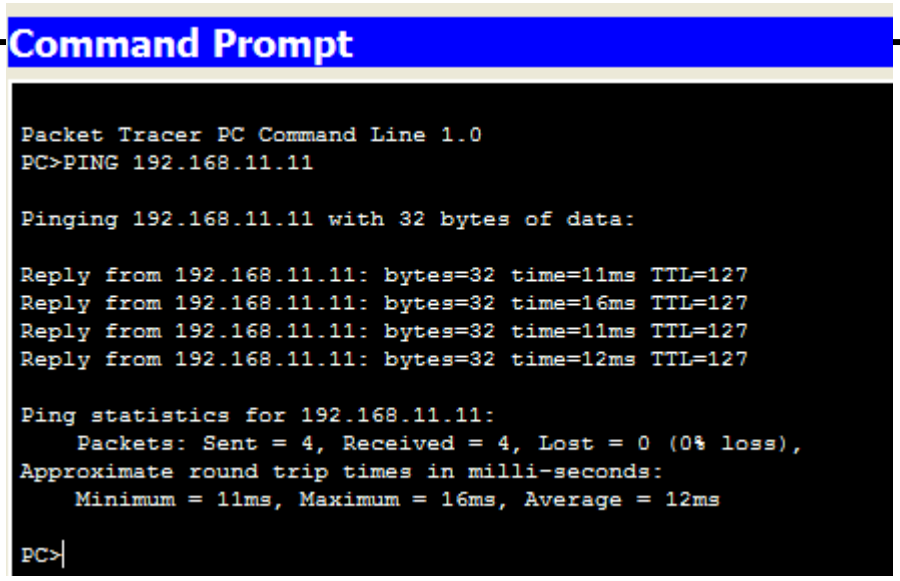
c. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y documente cualquier problema. Esto se conoce frecuentemente como *conectividad de extremo a extremo*. Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad total.

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.

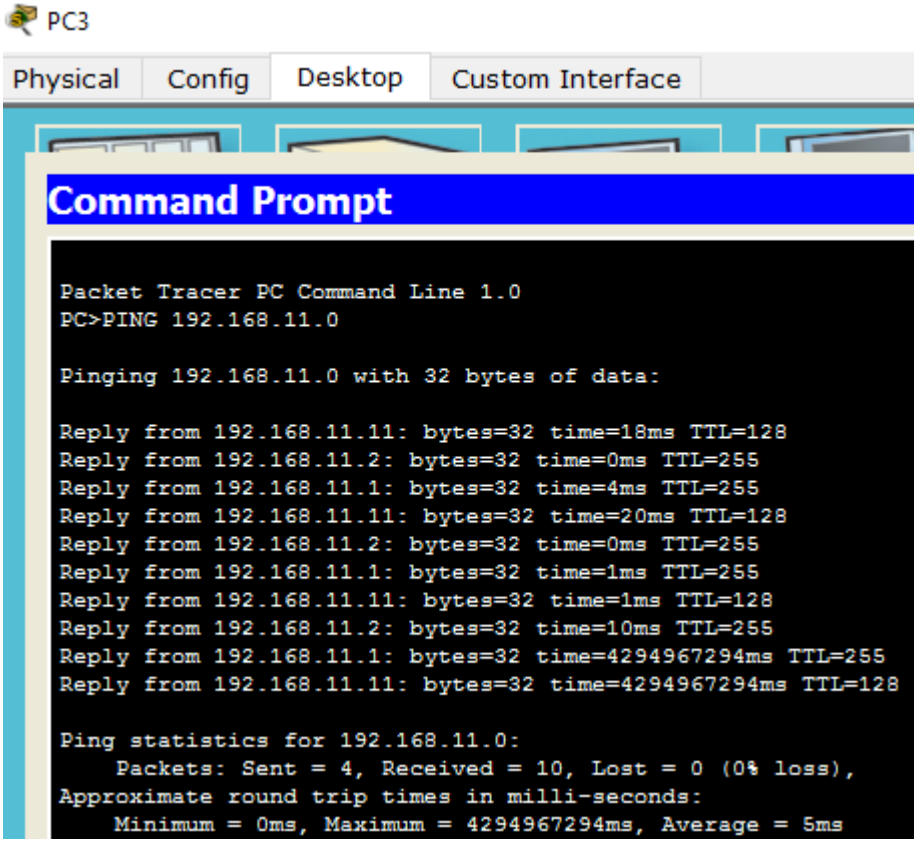
PING DE PC1 A PC4



PING DE PC2 A PC4



DE PC3 A S1



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 documentela. 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.

Problemas

- La PC1 no puede hacer ping a la PC2, porque la PC1 tiene una dirección IP que no pertenece a la red a la que está conectada.
- Los dispositivos no pueden hacer ping al S2, y el S2 no puede hacer ping a ningún dispositivo porque le falta una dirección IP.
- Los dispositivos remotos no pueden hacer ping a la PC4, porque la PC4 tiene configurado un gateway predeterminado incorrecto.

Los dispositivos remotos no pueden hacer ping al S1, porque le falta la configuración de gateway predeterminado

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	10.10.10.1	255.255.255.0	No aplicable
	G0/1	10.10.11.1	255.255.255.0	No aplicable
Class-A	VLAN 1	10.10.10.100	255.255.255.0	
Class-B	VLAN 1	10.10.11.100	255.255.255.0	
Student-1	NIC	10.10.10.101	255.255.255.0	
Student-2	NIC	10.10.10.102	255.255.255.0	
Student-3	NIC	10.10.11.101	255.255.255.0	
Student-4	NIC	10.10.11.102	255.255.255.0	

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.

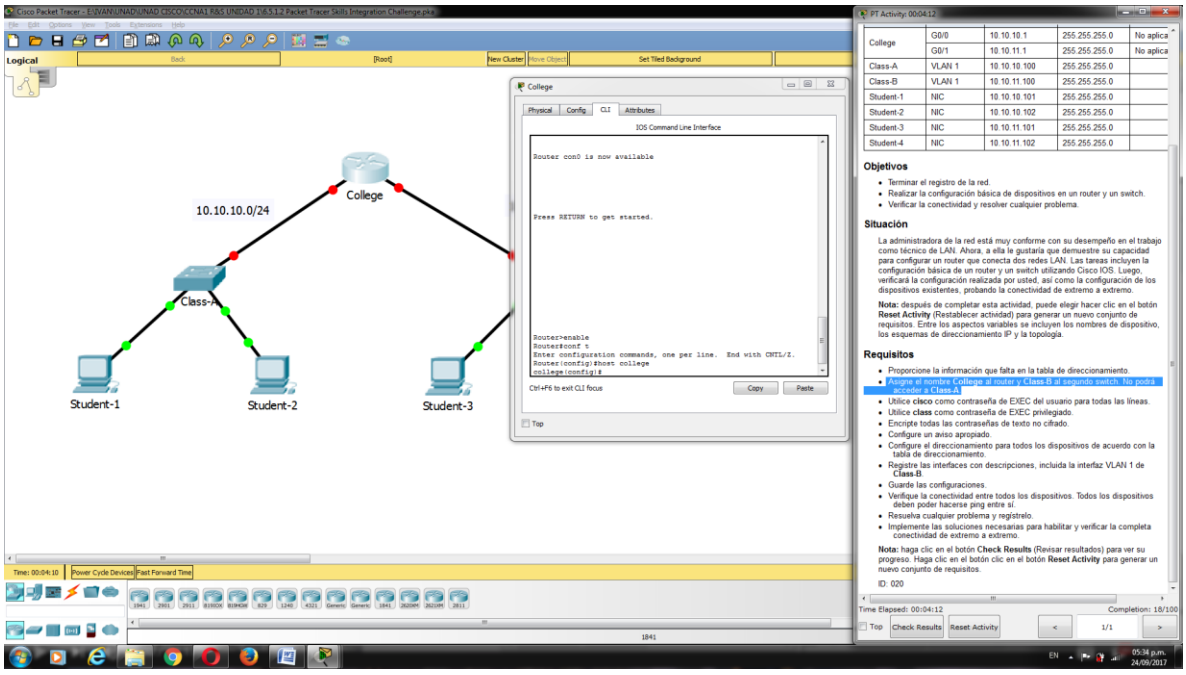
Situación

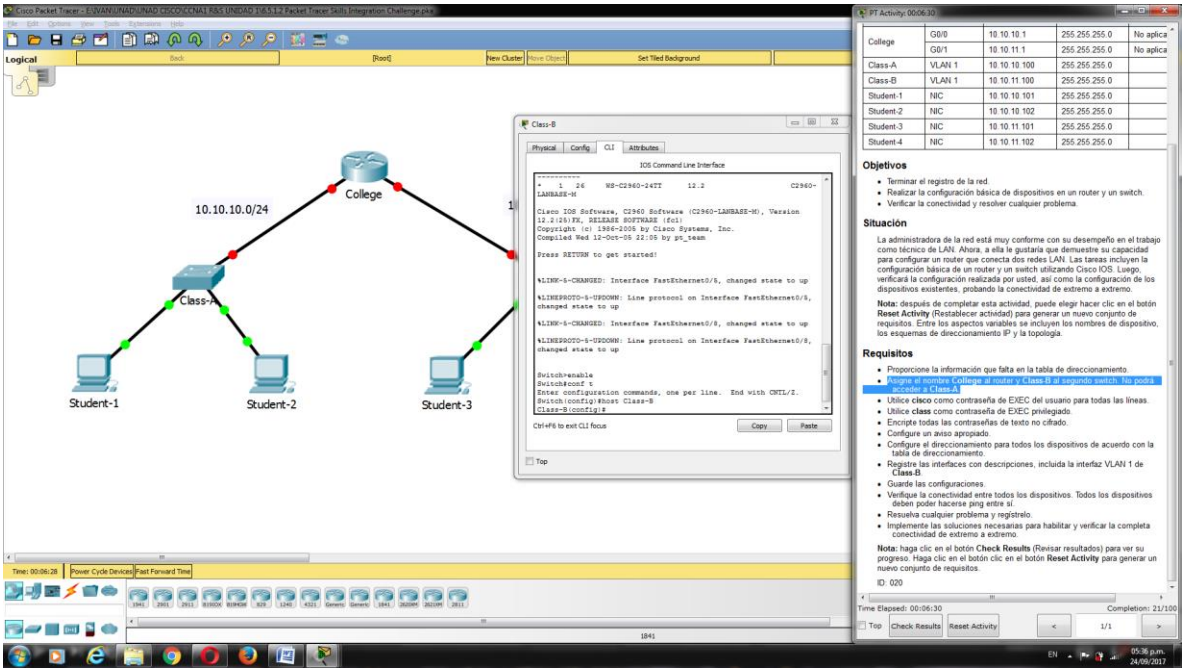
La administradora de la red está muy conforme con su desempeño en el trabajo como técnico de LAN. Ahora, a ella le gustaría que demuestre su capacidad para configurar un router que conecta dos redes LAN. Las tareas incluyen la configuración básica de un router y un switch utilizando Cisco IOS. Luego,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

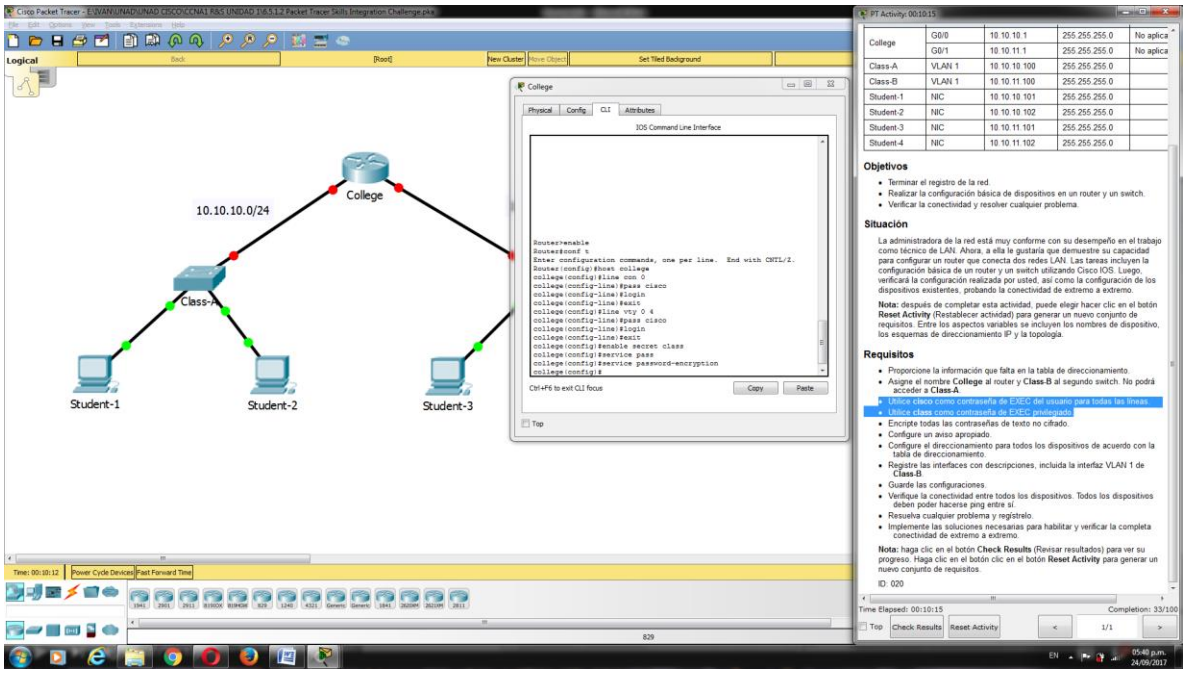
Requisitos

- 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.**

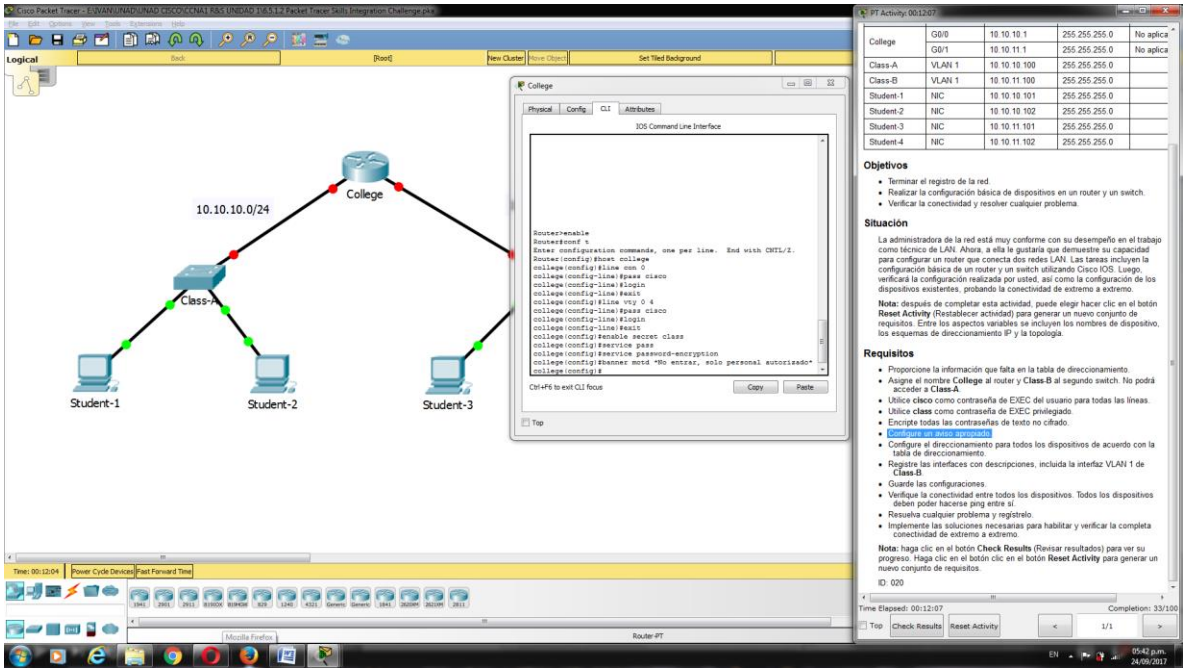




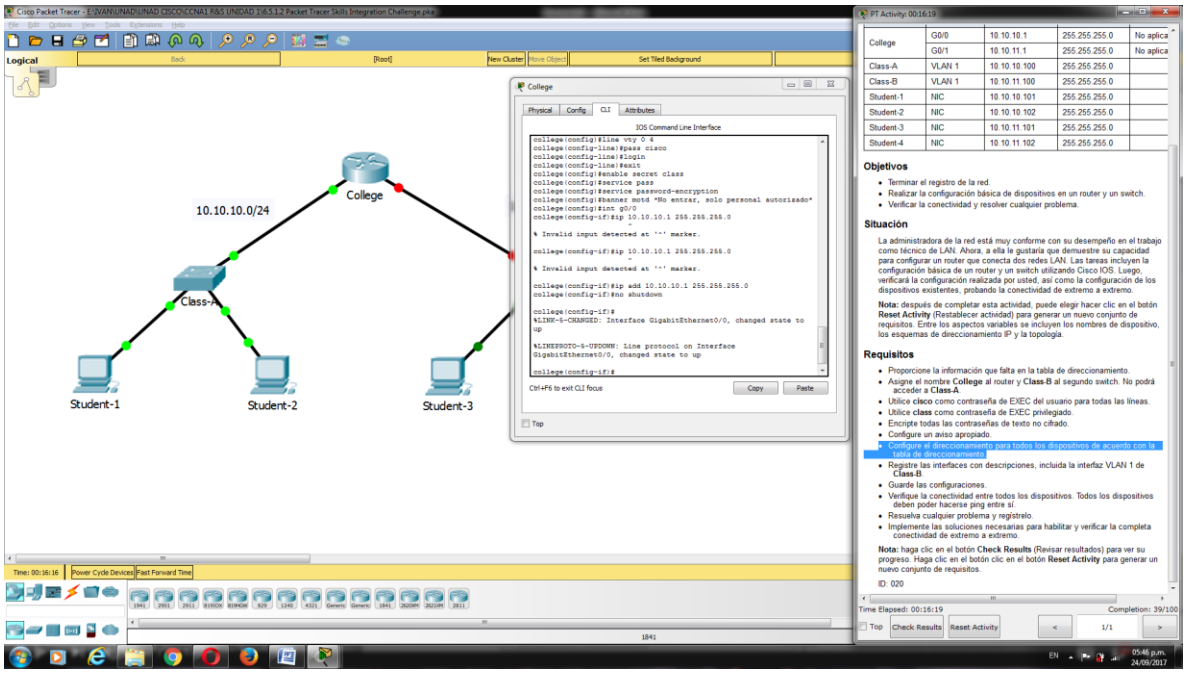
- Utilice **cisco** como contraseña de EXEC del usuario para todas las líneas.
- Utilice **class** como contraseña de EXEC privilegiado.
- Encripte todas las contraseñas de texto no cifrado.

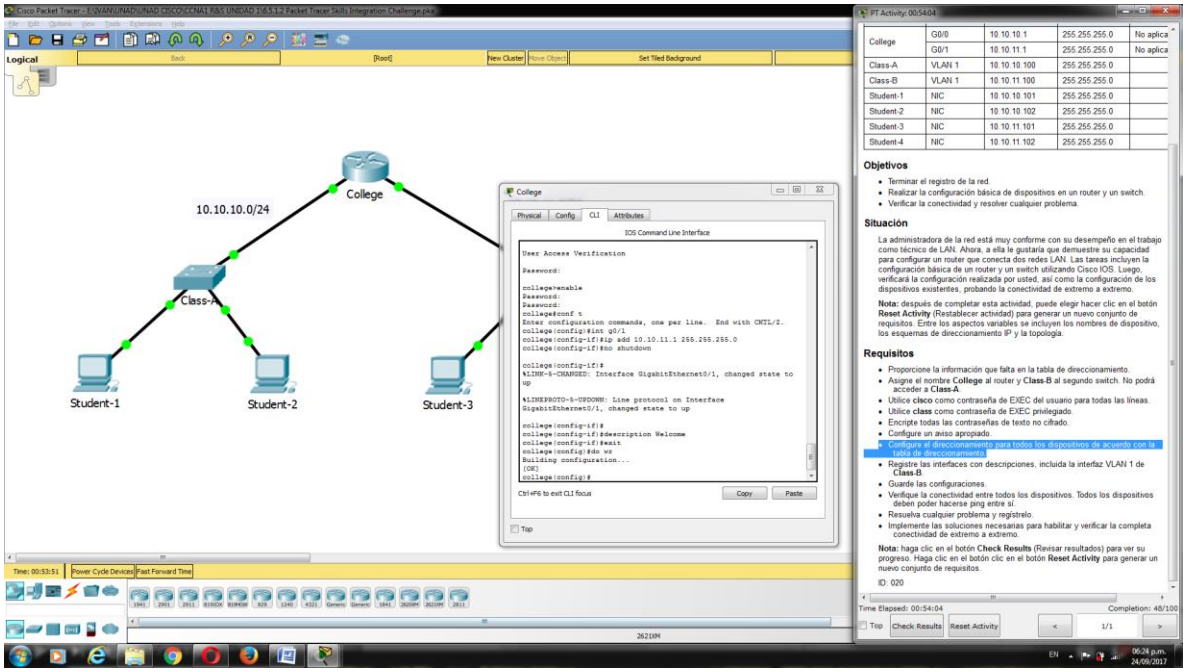


- Configure un aviso apropiado.

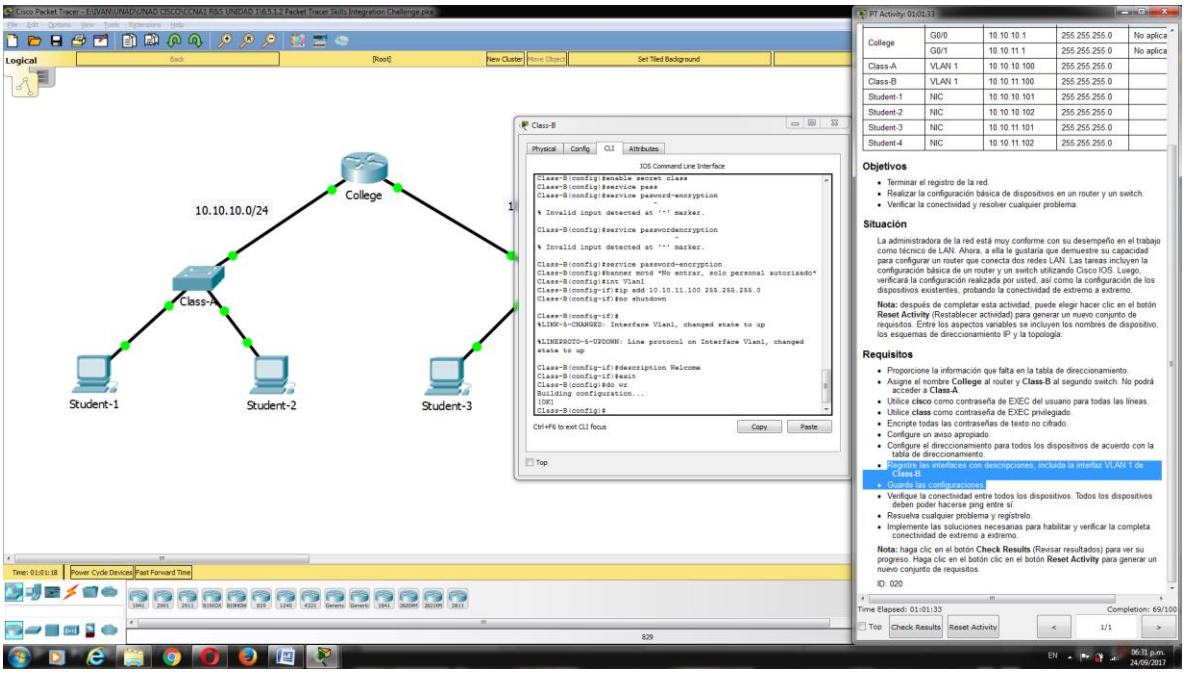


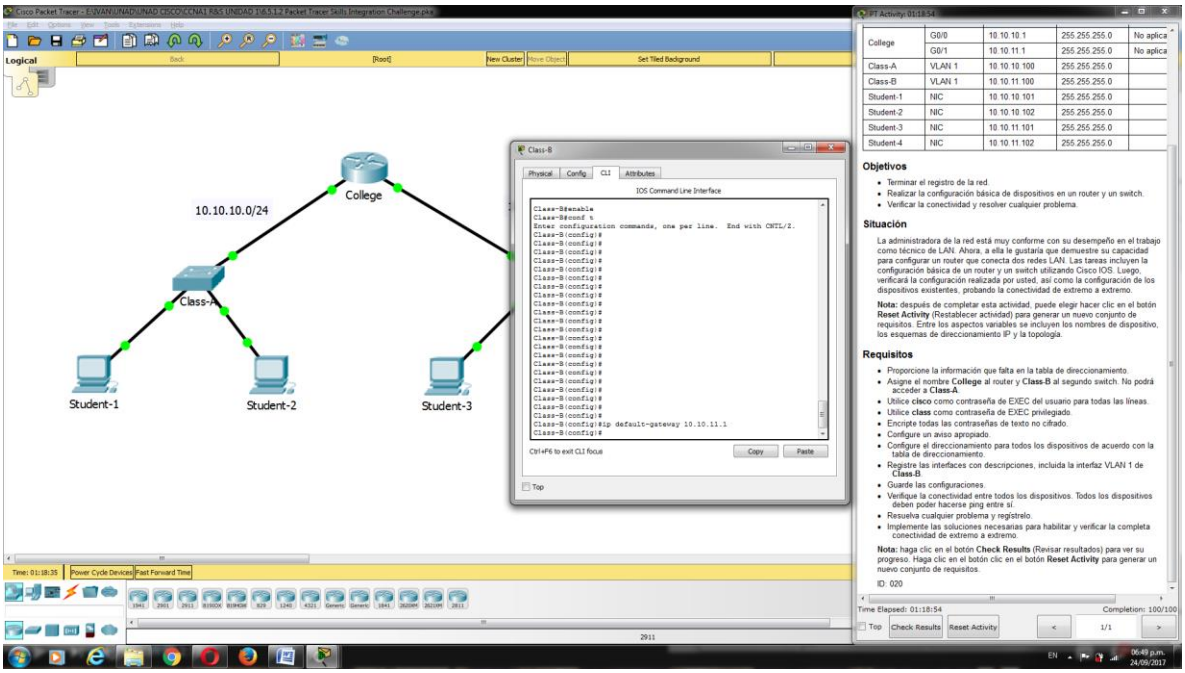
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.



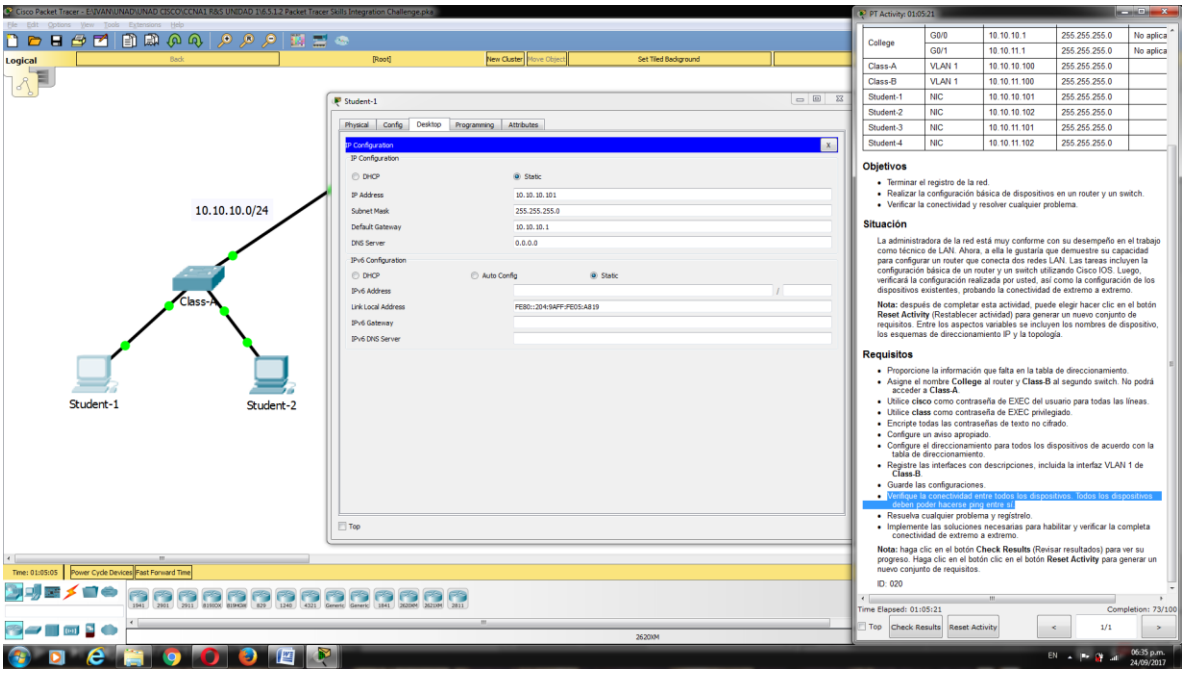


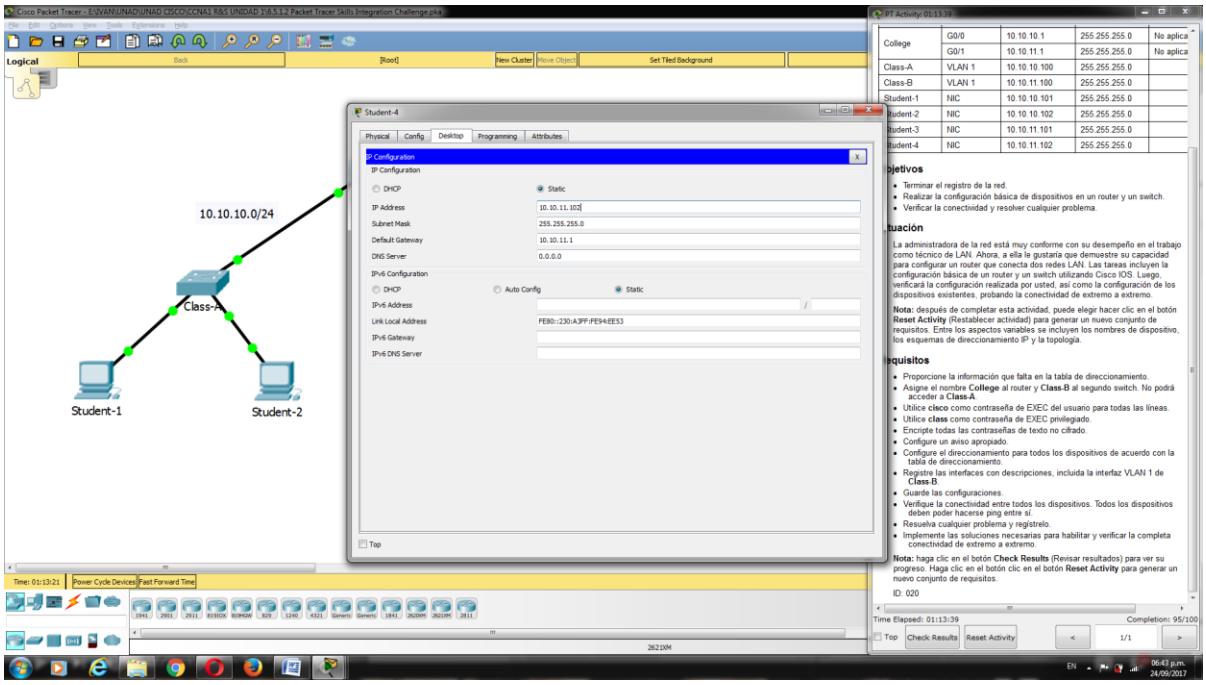
- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **Class-B**.
- Guarde las configuraciones.

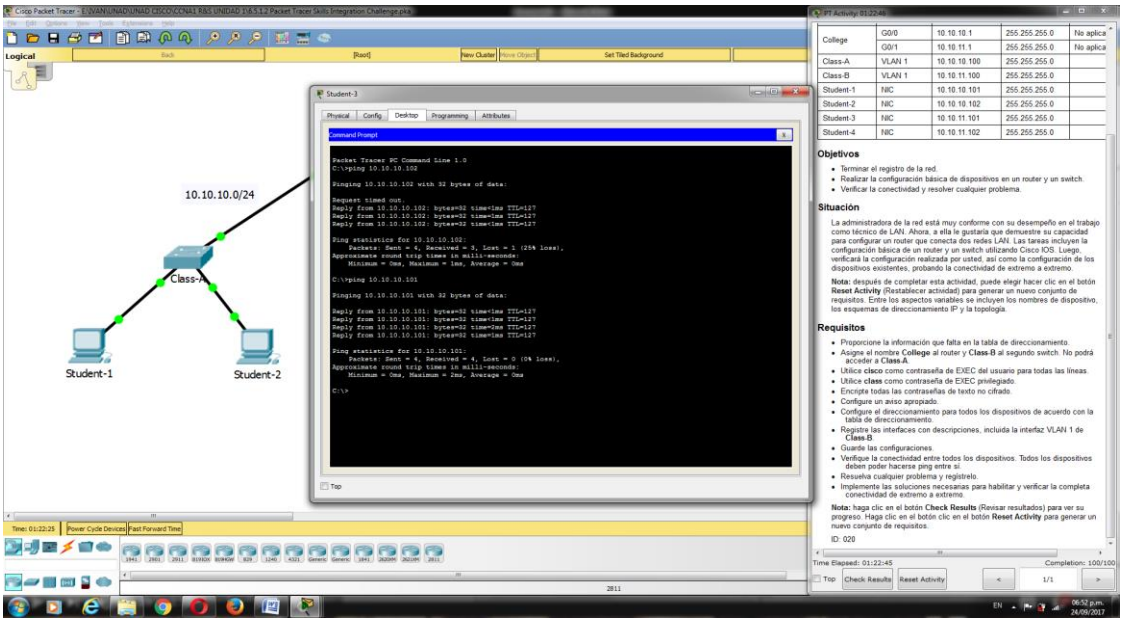


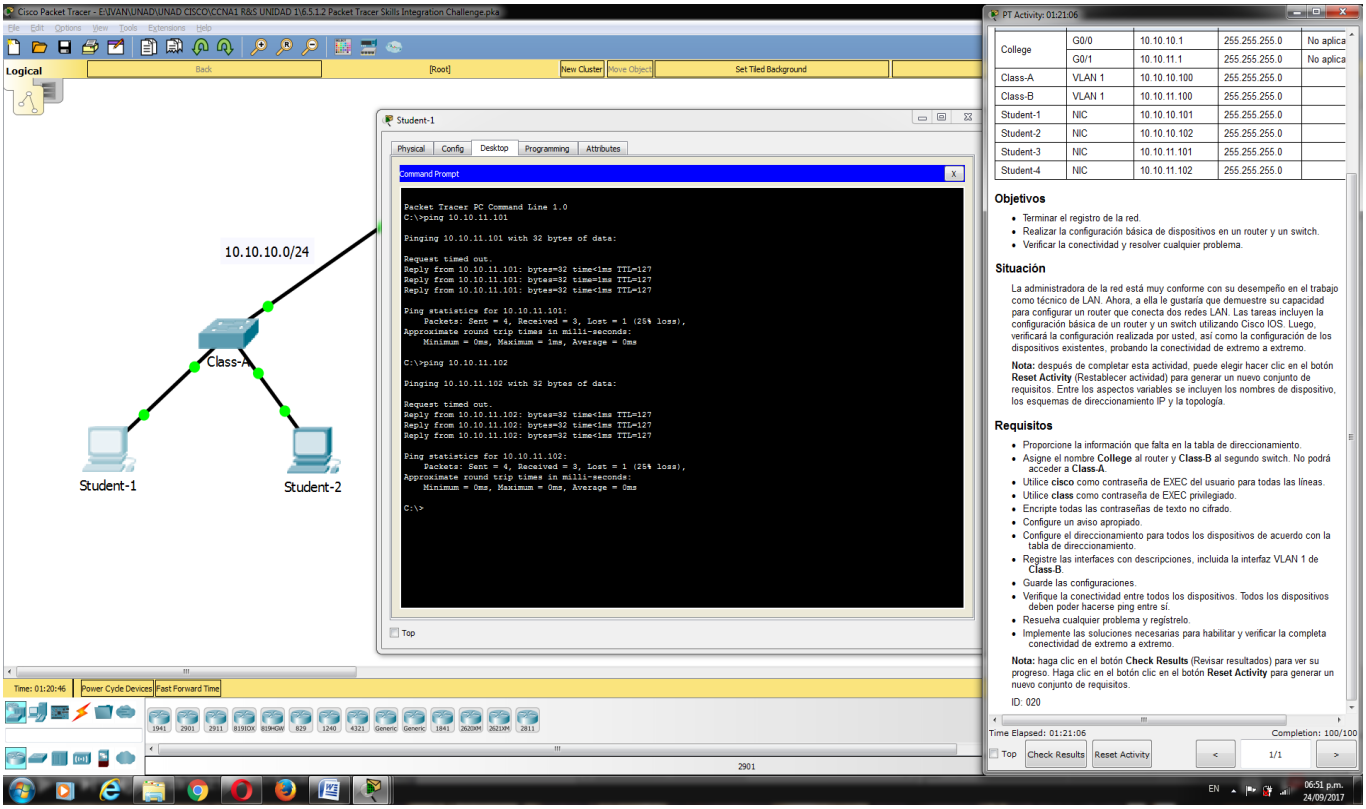


Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.


Cisco Packet Tracer - E:\IVAN\UNAD\UNAD CISCO\CCNA1 R&S UNIDAD 1\v5.1.2 Packet Tracer Skills Integration Challenge.pka
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
10.10.10.0/24
Class-A
Student-1
Student-2
Student-1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
DHCP
Static
IP Address
10.10.10.101
Subnet Mask
255.255.255.0
Default Gateway
10.10.10.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::204:9AFF:FE05:AB19
IPv6 Gateway
IPv6 DNS Server
Top
PT Activity: 01:05:21
College
G0/0
10.10.10.1
255.255.255.0
No aplica
G0/1
10.10.11.1
255.255.255.0
No aplica
Class-A
VLAN 1
10.10.10.100
255.255.255.0
Class-B
VLAN 1
10.10.11.100
255.255.255.0
Student-1
NIC
10.10.10.101
255.255.255.0
Student-2
NIC
10.10.10.102
255.255.255.0
Student-3
NIC
10.10.11.101
255.255.255.0
Student-4
NIC
10.10.11.102
255.255.255.0
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.
Utilice class como contraseña de EXEC privilegiado.
Encripte todas las contraseñas de texto no cifrado.
Configure un aviso apropiado.
Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de Class-B.
Guarde las configuraciones.
Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
Resuelva cualquier problema y regístrelo.
Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo.
Nota: haga clic en el botón Check Results (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón Reset Activity para generar un nuevo conjunto de requisitos.
ID: 020
Time Elapsed: 01:05:21
Completion: 73/100
Check Results
Reset Activity
1/1
Time: 01:05:05
Power Cycle Devices
Fast Forward Time
2620XM
06:35 p.m.
24/09/2017


Cisco Packet Tracer - E:\IVAN\UNAD\UNAD CISCO\CCNA1 R&S UNIDAD 1\v5.1.2 Packet Tracer Skills Integration Challenge.pka
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
10.10.10.0/24
Class-A
Student-1
Student-2
Student-4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
DHCP
Static
IP Address
10.10.11.102
Subnet Mask
255.255.255.0
Default Gateway
10.10.11.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::230:A3FF:FE94:EE53
IPv6 Gateway
IPv6 DNS Server
Top
PT Activity: 01:13:39
College
G0/0
10.10.10.1
255.255.255.0
No aplica
G0/1
10.10.11.1
255.255.255.0
No aplica
Class-A
VLAN 1
10.10.10.100
255.255.255.0
Class-B
VLAN 1
10.10.11.100
255.255.255.0
Student-1
NIC
10.10.10.101
255.255.255.0
Student-2
NIC
10.10.10.102
255.255.255.0
Student-3
NIC
10.10.11.101
255.255.255.0
Student-4
NIC
10.10.11.102
255.255.255.0
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.
Utilice class como contraseña de EXEC privilegiado.
Encripte todas las contraseñas de texto no cifrado.
Configure un aviso apropiado.
Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de Class-B.
Guarde las configuraciones.
Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
Resuelva cualquier problema y regístrelo.
Implemente las soluciones necesarias para habilitar y verificar la completa conectividad de extremo a extremo.
Nota: haga clic en el botón Check Results (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón Reset Activity para generar un nuevo conjunto de requisitos.
ID: 020
Time Elapsed: 01:13:39
Completion: 95/100
Check Results
Reset Activity
1/1
Time: 01:13:21
Power Cycle Devices
Fast Forward Time
2621XM
06:43 p.m.
24/09/2017





- Resuelva cualquier problema y regístrelo. Se corrige dirección IP del equipo estudiante 4 el cual no estaba correctamente configurado.Se colocó la dirección IP correcta y la puerta de enlace que le corresponde.

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

Conectividad correcta de extremo a extremo, con la corrección realizada.

Nota: haga clic en el botón **Check Results** (Revisar resultados) para ver su progreso. Haga clic en el botón clic en el botón **Reset Activity** para generar un nuevo conjunto de requisitos.

CONCLUSIONES

El uso adecuado del software Packet Tracer, permite la exploración de redes LAN y WAN conforme a los conceptos Internet en tanto permite una solución directa en el uso y simulación de escenarios de formación de redes, el concepto en este sentido se basa en la formación gradual de la materia, basados en el uso de términos relacionados con la implementación de la normativa OSI, desprendiéndose de esto una familiarización de componentes que en su puesta en marcha nos prepara para el campo real de configuración de tales dispositivos.

La interfaz de línea de comandos (CLI) permite que como técnicos de redes podamos manipular la configuración de los diferentes dispositivos LAN tanto de manera directa como inalámbrica, permite a los operadores conectar una consola ASCII al controlador LAN inalámbrico de Cisco y configurar el controlador y sus puntos de acceso asociados, así pues el lograr una configuración de conexiones básicas, por medio de dicha interfaz, determina una mayor posibilidad de exploración de ayudas tanto del modo normal o desde privilegiado (EXEC). La Configuración del switch y del router no difieren más que aspectos de redireccionamiento y determinación de puertas de enlace para el caso de router, lo cual facilita en gran medida la asociación de los comandos utilizados para las configuraciones comunes las cuales e guardan en la NVRAM, pudiendo controlar el acceso por medio de mensajes de advertencia desde el comando MOTD y expedición de información por pantalla de IP, máscaras y gateway por medio de las diferentes opciones que permite el comando SHOW.

Cuando revisamos el tráfico de una red para identificar las características físicas de los dispositivos de que hacen parte de esta notamos que los dispositivos como router y un switch desempeñan una labor especifica en el flujo de la información que transita por la red cableada o inalámbrica según el caso de donde destacamos que para que un técnico implemente políticas de Calidad de Servicio en los routers, es preciso asegurar que los dispositivos estén adecuadamente configurados en las redes, entonces la configuración de los enlaces y en los patrones del tráfico ayudaran significativamente a que de la mano de los switch los datos viajen y sean recibidos de manera adecuada por los usuarios de destino siendo allí donde la selección de los módulos correctos para la conectividad de dispositivos dará por sentado una red tanto segura como viable pudiendo aun hacer mantenimiento a estas siendo que se es capaz de gestionar los registro de la red y configuración básica de dispositivos en un router y un switch y así dar resolución de cualquier problema que se presente en redes reales, puesto que los estándares de configuración por lo general apuntan a la aplicación de comandos para su funcionamiento.

Se pudo lograr la comprobación de la conectividad de los equipos y encontrar los datos faltantes en los ejercicios que ameritaron revisión implementando claves de seguridad y la encriptación de las mismas, pudiendo identificar el entorno de línea de comando (CLI), incluyendo el ingreso por el modo EXEC para el ingreso a los modos de configuración tanto global como privilegiado, así mismo la configuración de comandos como lo es Clock (hora), además de la identificación mediante la ejecución url en un web browser como se realiza el proceso de envío y solicitud de paquetes ARP, DNS, HTTP y TCP los cuales viajan a través de los diferentes equipos activos que se encuentran en la red para así desplegarnos en la ventana de un explorador la información solicitada.

REFERENCIAS BIBLIOGRAFIAS

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

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

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

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

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

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.