CONSOLIDADO INFORME FINAL
TRABAJO COLABORATIVO N°1
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)
GRUPOS: 203092A_363

INTEGRANTES:

RAFAEL VICENTE CASTILLO
CÓD: 1065597142
KATIA TAYSE ESCOBAR
CÓD:
VIVIANA HOYOS
CÓD: 1120866279
GERMAN MONTENEGRO
CÓD:1065993707
LEIDY PEÑALOZA ALMANZA
CÓD: 1121329070

TUTOR:

NILSON ALBEIRO FERREIRA MANZANARES
DOCENTE OCASIONAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA FACULTAD BASICA DE INGENIERIA Y TECNOLOGIA SEPTIEMBRE DE 2017

INTRODUCCION

Las redes de datos en la actualidad se han convertido en un aspecto muy importante de las vidas de todos los seres humanos, es por este motivo que existen grupos especializados en desarrollar estándares, normas y protocolos que contribuyan al avance de esta ciencia. Uno de los aspectos importantes es el desarrollo de protocolos de enrutamiento que permitan mayor confiabilidad y rapidez, ya que en la actualidad la velocidad de transmisión y comunicación es muy importante.

La tarea de diseñar una red puede ser una tarea fascinante e implica mucho más que simplemente conectar dos computadoras entre sí. Una red requiere muchas funciones para que sea confiable, escalable y fácil de administrar. Para diseñar redes confiables, fáciles de administrar, y escalables, los diseñadores de red deben darse cuenta de que cada uno de los componentes principales de una red tiene requisitos de diseño específicos.

Para todo aquel que esté involucrado en el mundo de las redes es una necesidad comprender el funcionamiento de todos los dispositivos físicos y de todas las tecnologías que comprenden una red, es por ello que la realización de este trabajo ayuda a su aprendiz a introducirse en el mundo de las redes, desde la apariencia de una red básica hasta la configuración de cada uno de los dispositivos que en ella intervienen.

DESARROLLO DE LAS ACTIVIDADES PROPUESTAS

- **RAFAEL CASTILLO**

1. **EJERCICIO 1.2.4.4**
2. **EJERCICIO 3.2.46**
3. **EJERCICIO 5.3.3.**
4. **EJERCICIO 6.5.1.2**

- **VIVIANO HOYOS**

5. **EJERCICIO 2.1.4.8**
6. **EJERCICIO 3.3.3.3**
7. **EJERCICIO 6.3.1.10**

- **LEIDY PEÑALOZA**

8. **EJERCICIO 2.2.3.3**
9. **EJERCICIO 4.2.4.5**
10. **EJERCICIO 6.4.1.2**

- **KIARA ESCOBAR**

11. **EJERCICIO 2.3.2.5**
12. **EJERCICIO 5.1.4.4**
13. **EJERCICIO 6.4.3.3**

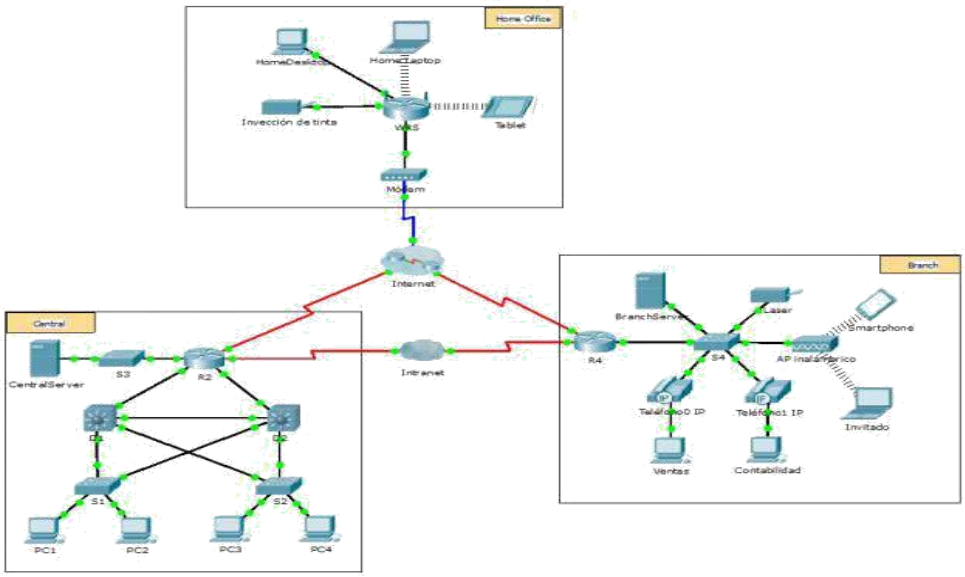
- **GERMAN MONTENEGRO**

14. **EJERCICIO 2.4.1.2**
15. **EJERCICIO 5.2.1.7**
16. **EJERCICIO 6.4.3.4**
17. **5. EJERCICIO 2.1.4.8**

1.2.4.4 **Packet Tracer: representación de la red**

Packet Tracer: Representación de la red

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).

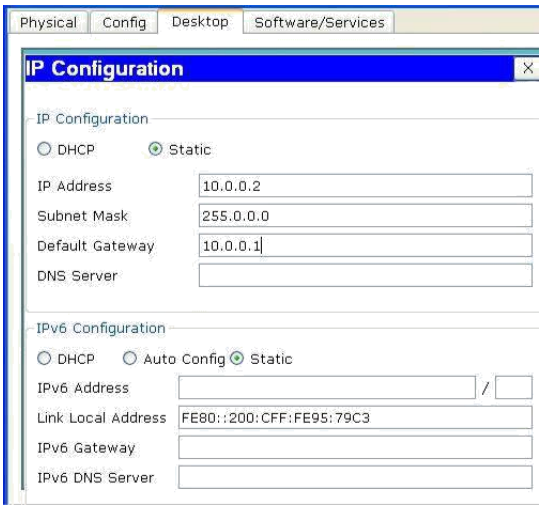
b. Acceda a los videos de tutoriales de Packet Tracer haciendo clic en Help > Tutorials (Tutoriales). Estos videos son una demostración visual de la información que se encuentra en las páginas de ayuda y diversos aspectos del programa de software Packet Tracer. Antes de continuar con esta actividad,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

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)?

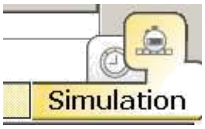
Puede elegir DHCP o Static (Estático) y configurar la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS.



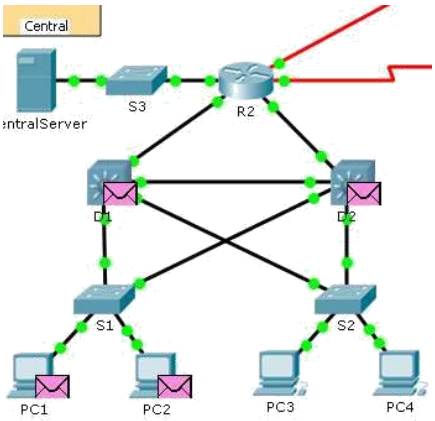
Paso 2: Alternar entre los modos Realtime y Simulation.

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.

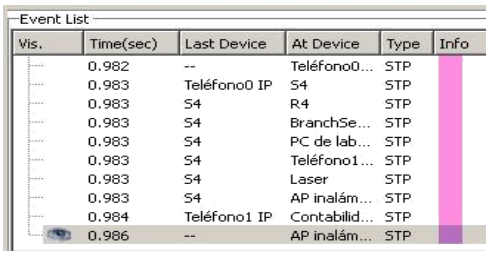
b. Haga clic en la ficha que está justo detrás de la fichaRealtime para cambiar al modo Simulation (Simulación). En el modo de simulación, puede ver la red en funcionamiento a menor velocidad, lo que le permite observar las rutas por las que viajan los datos e inspeccionar los paquetes de datos en detalle.



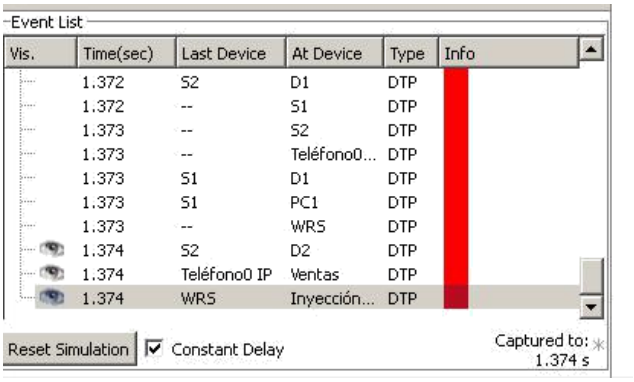
c. En el panel de simulación, haga clic en Auto Capture / Play(Captura/reproducción automática). Ahora debería ver los paquetes de datos, que se representan con sobres de diversos colores, que viajan entre los dispositivos.



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



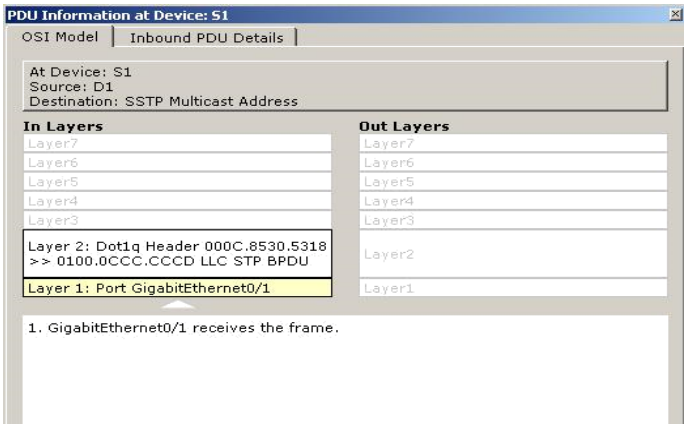
e. Haga clic en Capture / Forward (Capturar/avanzar) para avanzar en la simulación. Haga clic en este botón algunas veces más para ver el efecto.



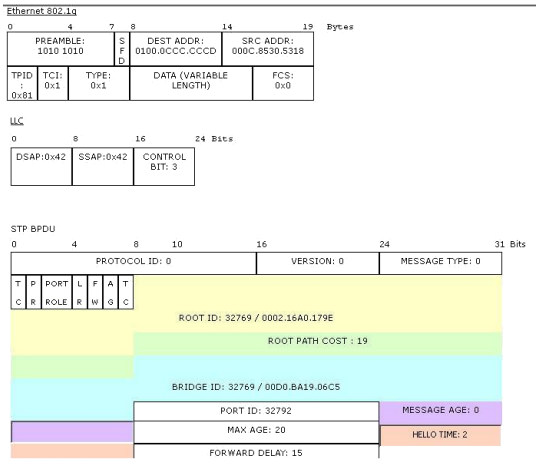
f. En la topología de la red a la izquierda, haga clic en cualquiera de los sobres en un dispositivo intermediario e investigue qué hay dentro. En el curso de sus estudios de CCNA, aprenderá el significado la mayor parte del contenido de estos sobres. Por el momento, intente responder las siguientes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

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

En este caso en el dispositivo S1 dos layer 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?

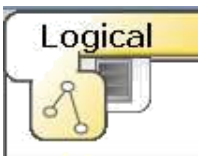


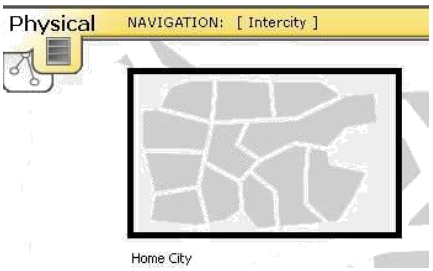
- Alterne entre las fichas Inbound PDU Details yOutbound PDU Details. ¿Observa cambios en la información? Si es así, ¿qué es lo que cambia?

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.





b. 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.

c. 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).

d. 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.

e. d. Haga clic en el botón de alternancia ubicado debajo dePhysical 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.

1. Routers,
2. switches,
3. hubs,
4. dispositivos inalámbricos
5. emulación de WAN.

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

13

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

11

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

5

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

8

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

4

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

La conexión se realiza por negociación entre dispositivos inhalambricos.

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?

Dentro del estudio del curso se ha visto no puede suceder esto, según la teoría de cliente-servidor, porque un host puede actuar como un cliente, un servidor o ambos.

El programa que contienen los dispositivos determina qué función tiene en la red.

Los servidores son hosts que tienen instalado programa que le da poder de proporcionar información y servicios.

Los clientes son hosts que tienen instalado un programa que les permite solicitar información al servidor y mostrar la información obtenida.

Un cliente puede hacer las funciones de un servidor siempre y cuando se configure para tal función.

31655

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

1. Notificar a otros dispositivos de los errores y las fallas de comunicación;
2. Direccionar datos a través de rutas alternativas cuando hay una falla de enlace;
3. 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.

1. La distancia en la cual el medio puede transportar exitosa mente una señal.
2. Zona en la cual funcionaran los dispositivos.
3. Velocidad que se requiere para hacer la conexión de red sabiendo los costos que acarean.

Paso 3: Comparar redes LAN y WAN

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

Las redes LAN (Local Network Area) dan acceso a los usuarios finales en una pequeña área geográfica. Por ejemplo, una microempresa, una red de escuela, una planta de producción.

Las redes WAN proporcionan acceso a los usuarios en un área geográfica extensa a través de grandes distancias muy extensas. Por ejemplo, metropolitano e Internet son ejemplos de redes WAN.

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

Son dos la WAN de Internet y la de intranet.

c. ¿Cuántas LAN ve?

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

d. En esta red de Packet Tracer, Internet está simplificada en gran medida y no representa ni la estructura ni la forma de Internet propiamente dicha. Describa Internet breve mente.

Internet se utiliza sobre todo cuando necesitamos comunicarnos con un recurso en otra red que está a gran distancia.

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

Cable, DSL, dial-up, datos móviles y satélite.

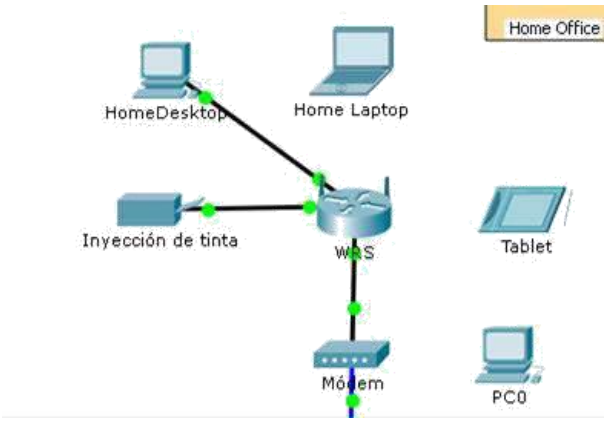
f. ¿Cuáles son algunas de las formas más comunes que utilizan las empresas para conectarse a Internet en su área?

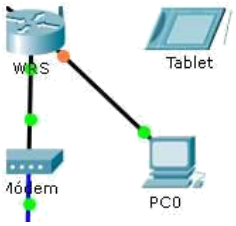
Línea arrendada dedicada, Metro-E, DSL, cable, satélite.

Desafío

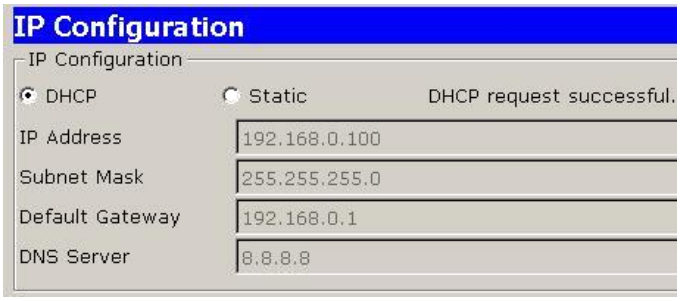
Ahora que tuvo la oportunidad de explorar la red representada en esta actividad de Packet Tracer, es posible que haya adquirido algunas habilidades que quiera poner en práctica o tal vez desee tener la oportunidad de analizar esta red en mayor detalle. Teniendo en cuenta que la mayor parte de lo que ve y experimenta en Packet Tracer supera su nivel de habilidad en este momento, los siguientes son algunos desafíos que tal vez quiera probar. No se preocupe si no puede completarlos todos. Muy pronto se convertirá en un usuario y diseñador de redes experto en Packet Tracer.

- Agregue un dispositivo final a la topología y conéctelo a una de las LAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para enviar datos a otros usuarios finales? ¿Puede proporcionar la información? ¿Hay alguna manera de verificar que conectó correctamente el dispositivo?

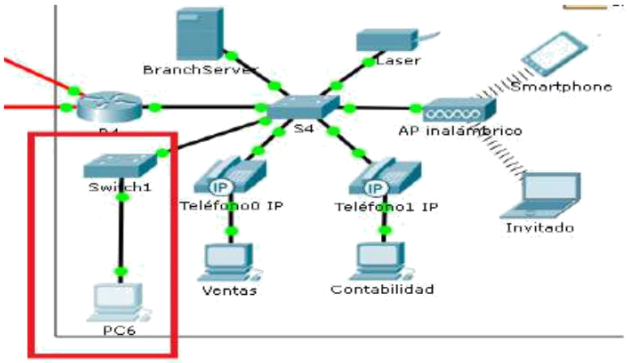




Ahora el direccionamiento IP:



- Agregue un nuevo dispositivo intermediario a una de las redes y conéctelo a uno de las LAN o WAN con una conexión de medios. ¿Qué otra cosa necesita este dispositivo para funcionar como intermediario de otros dispositivos en la red?



- Abra una nueva instancia de Packet Tracer. Cree una nueva red con, al menos, dos redes LAN conectadas mediante una WAN. Conecte todos los dispositivos. Investigue la actividad de Packet Tracer original para ver qué más necesita hacer para que la nueva red esté en condiciones de funcionamiento. Registre sus comentarios y guarde el archivo de Packet Tracer. Tal vez desee volver a acceder a la red cuando domine algunas habilidades más.

3.2.4.6 Packet Tracer Investigating the TCP – IP and OSI Models in Action

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.

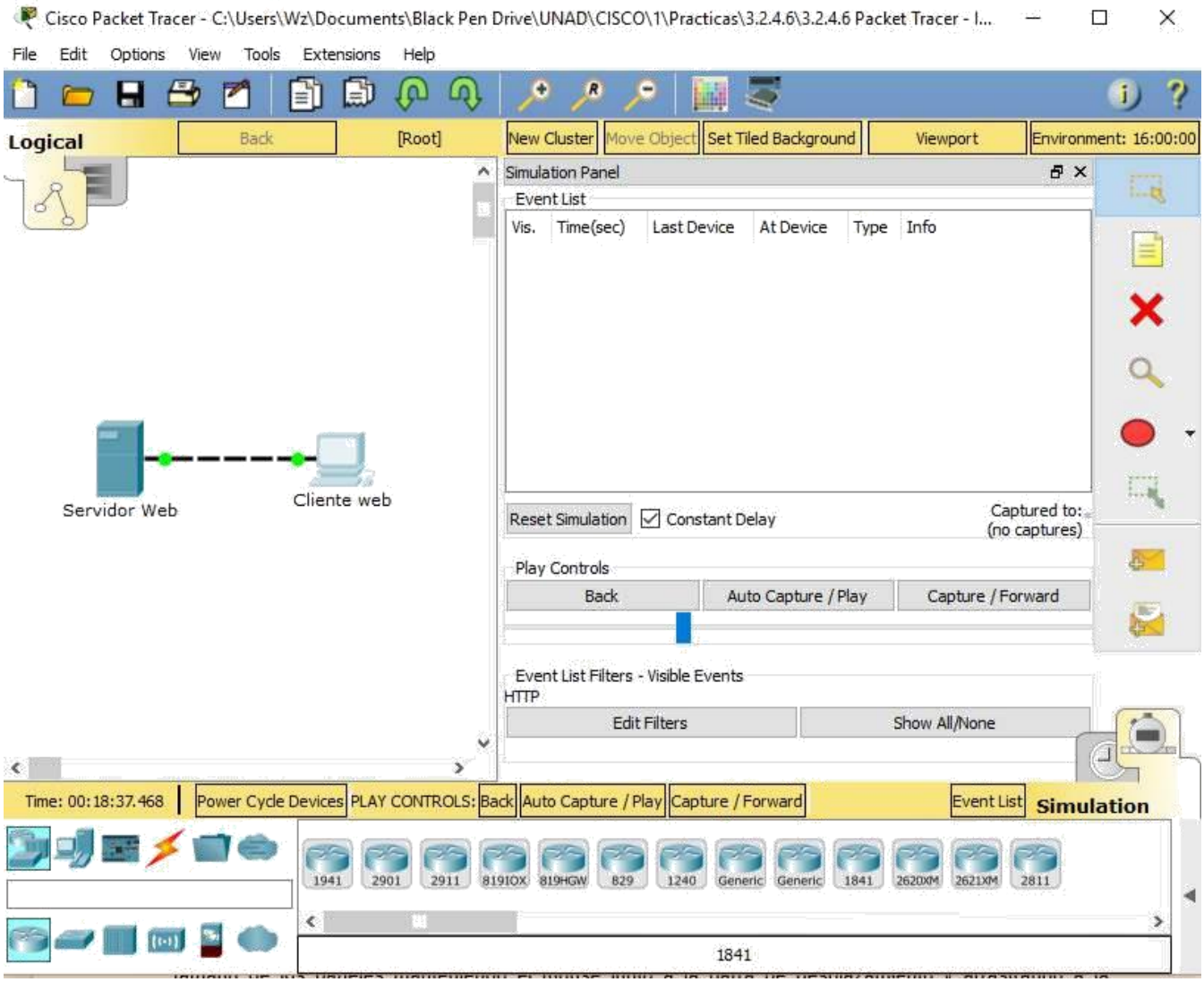
En la esquina inferior derecha de la interfaz de Packet Tracer, hay fichas que permiten alternar entre el modo **Realtime** (Tiempo real) y **Simulation** (Simulación). PT siempre se inicia en el modo **Realtime**, en el que los protocolos de red operan con intervalos realistas. Sin embargo, una excelente 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).

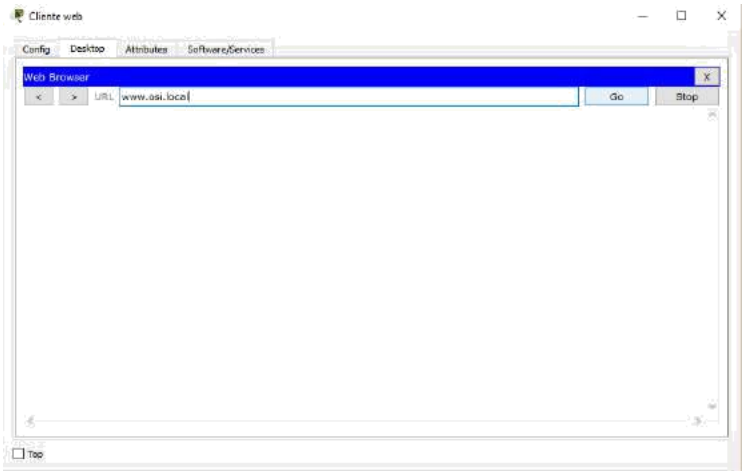
El panel de simulación actualmente está vacío. En la parte superior de Event List (Lista de eventos) dentro del panel de simulación, se indican seis columnas. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el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

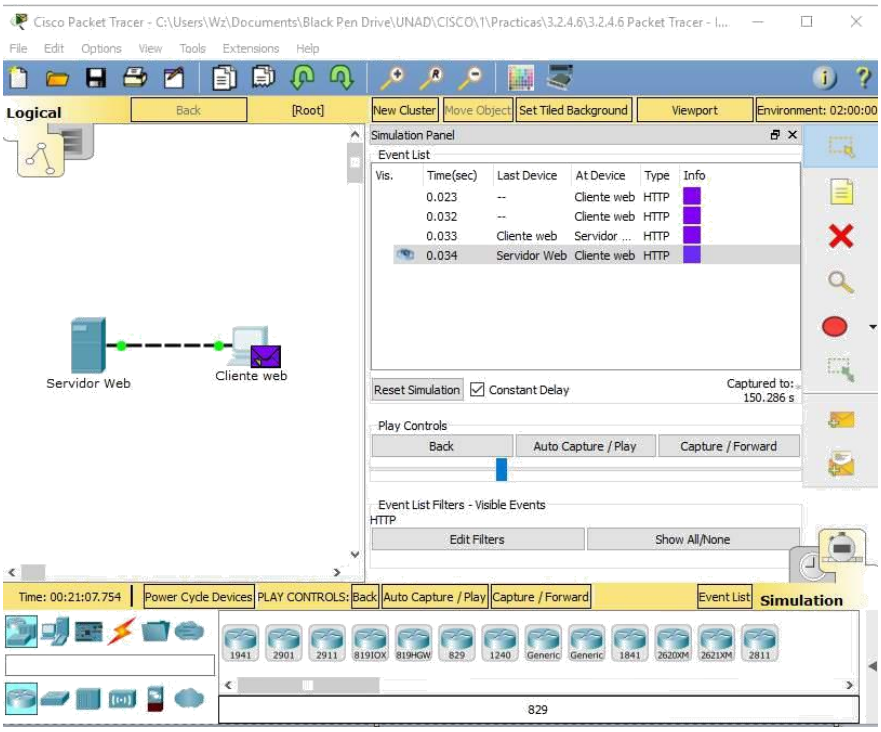
a. Haga clic en **Web Client** (Cliente Web) en el panel del extremo izquierdo.

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).

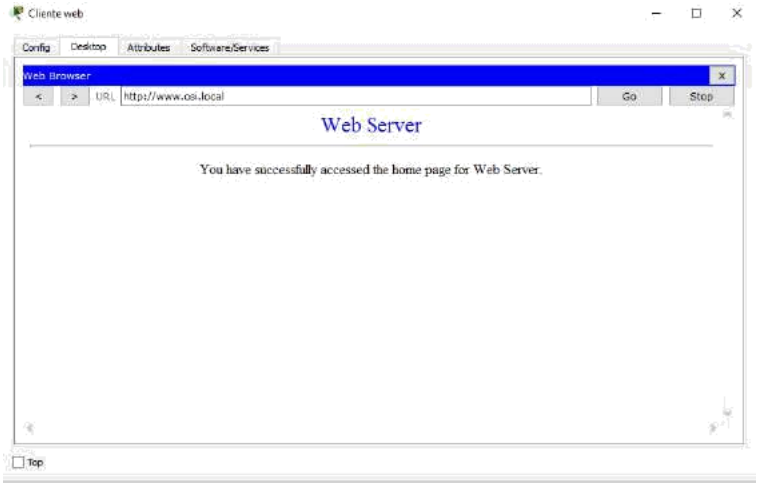


Debido a que el tiempo en el modo de simulación se desencadena por eventos, debe usar el botón **Capture/Forward** (Capturar/avanzar) para mostrar los eventos de red.



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?

R/ 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)?

- **Layer 7: HTTP** = "1. The HTTP client sends a HTTP request to the server." ("El cliente HTTP envía una solicitud de HTTP al servidor")
- **Layer 4 TCP Src Port: 1034, Dst Port: 80** = 1. Sent segment information: the sequence number 1, the ACK number 1, and the data length 102. (Información del segmento enviado: el número de secuencia 1, el número ACK, y la longitud del dato 102)
- **Layer 3 IP Headers Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254** = 1. The destination IP address is in the same subnet. The device sets the next-hop to destination.

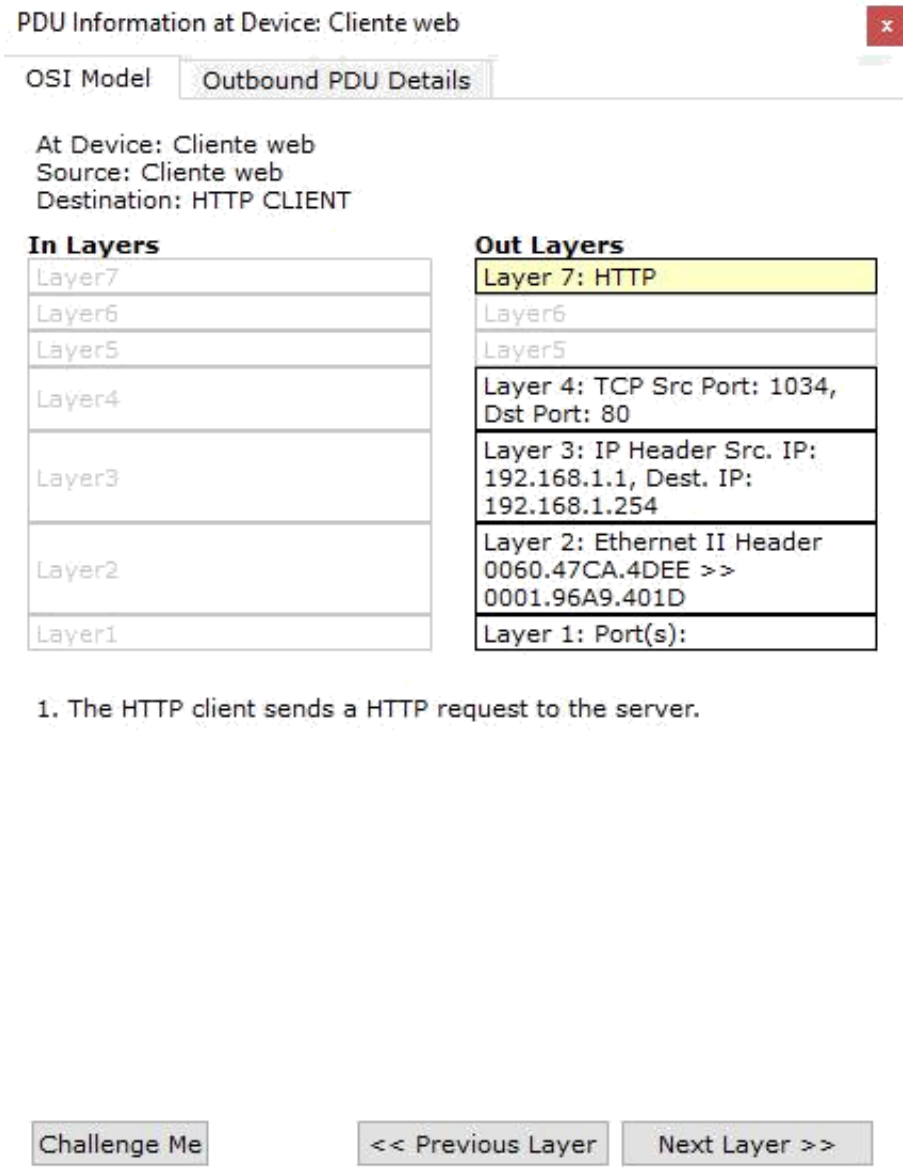
(La dirección IP de destino está en la misma subred. El dispositivo establece el next-hop al destino.)

- **Layer 2: Ethernet II Header 0060.47CA.4DEE>>0001.96A9.401D** = 1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table. (El siguiente next-hop dirección IP es una unicast. El proceso ARP mira la tabla ARP.)
- **Layer 1: Port(s): =** 1. The port FastEthernet0 is sending another frame at this time. The device buffers the frame to be sent later. (El Puerto FastEthernet0 está enviando otra trama al mismo tiempo. El dispositivo almaceno la trama para enviarla más tarde.)

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.

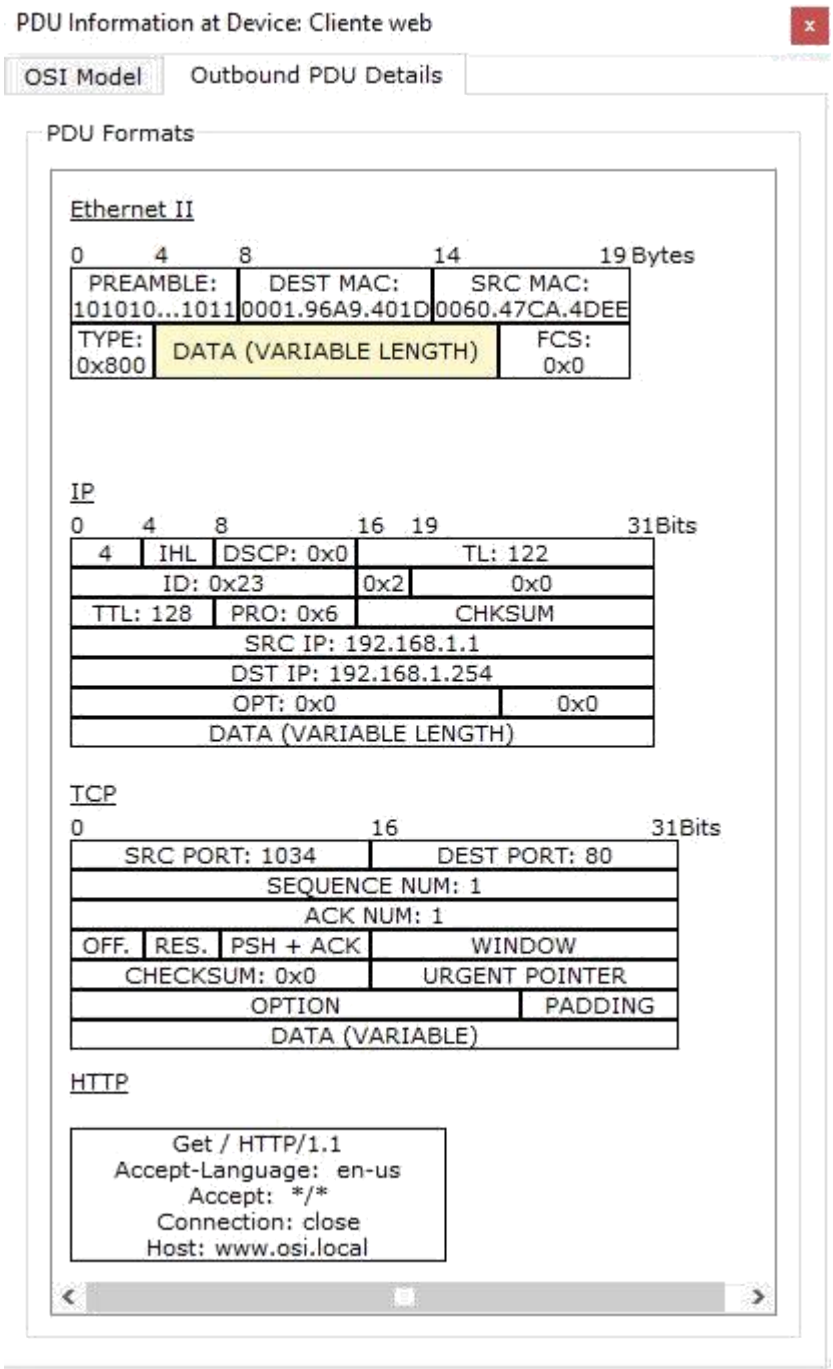


c. Haga clic en **Next Layer** (Capa siguiente). Layer 4 (Capa 4) debe estar resaltado. ¿Cuál es el valor de **Dst Port** (Puerto de dest.)? 80

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.

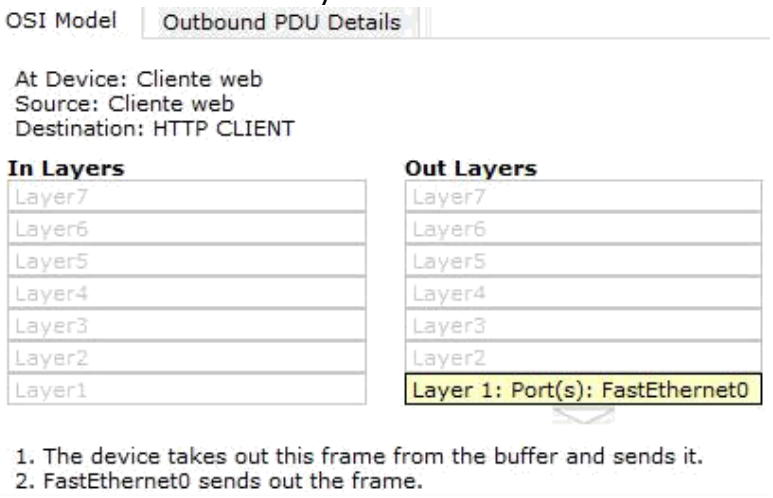
Nota: la información que se indica en la sección **Ethernet II** proporciona información aun más detallada que la que se indica en Layer 2 (Capa 2) en la ficha **OSI Model**. **Outbound PDU Details** (Detalles de PDU saliente) proporciona información más descriptiva y detallada. Los valores de **DEST 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.) y DST IP (IP DE DEST.) en la capa 3

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

In Layers

Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D	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.
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254	1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
Layer 4: TCP Src Port: 1034, Dst Port: 80	1. The device receives a TCP PUSH+ACK segment on the connection to 192.168.1.1 on port 1034. 2. Received segment information: the sequence number 1, the ACK number 1, and the data length 102. 3. The TCP segment has the expected peer sequence number. 4. TCP processes payload data. 5. TCP reassembles all data segments and passes to the upper layer.
Layer 7: HTTP	1. The server receives a HTTP request.

Out Layers

Layer 7: HTTP	1. The server sends back a HTTP reply to the client.
Layer 4: TCP Src Port: 80, Dst Port: 1034	1. Sent segment information: the sequence number 1, the ACK number 103, and the data length 272.
Layer 3: IP Header Src. IP: 192.168.1.254, Dest. IP: 192.168.1.1	1. The destination IP address is in the same subnet. The device sets the next-hop to destination.
Layer 2: Ethernet II Header 0001.96A9.401D >> 0060.47CA.4DEE	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.
Layer 1: Port(s): FastEthernet0	1. FastEthernet0 sends out the frame.

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 IP de origen y destino, y las direcciones MAC.

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

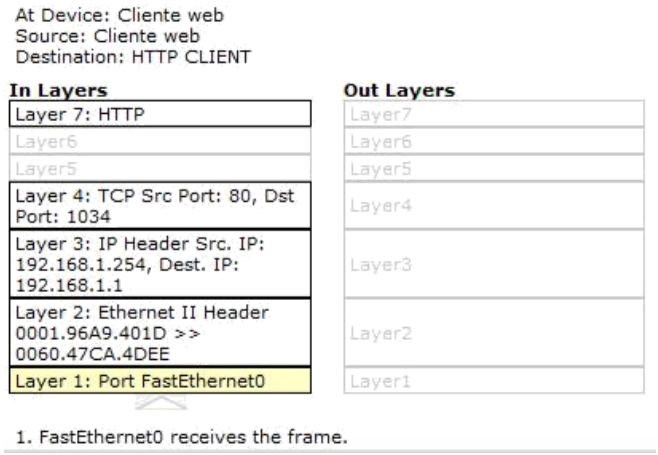
HTTP

HTTP/1.1 200 OK
Connection: close
Content-Length: 170
Content-Type: text/html
Server: PT-Server/5.2
HTTP DATA..

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

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

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



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

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

Paso 1: Ver eventos adicionales

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

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

¿Qué tipos de eventos adicionales se muestran? Se ven ARP, DNS, TCP y HTTP

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.

PDU Information at Device: Cliente web

OSI Model | Outbound PDU Details

PDU Formats

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 57		
ID: 0x1			0x0	0x0	
TTL: 128	PRO: 0x11		CHKSUM		
SRC IP: 192.168.1.1					
DST IP: 192.168.1.254					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

UDP

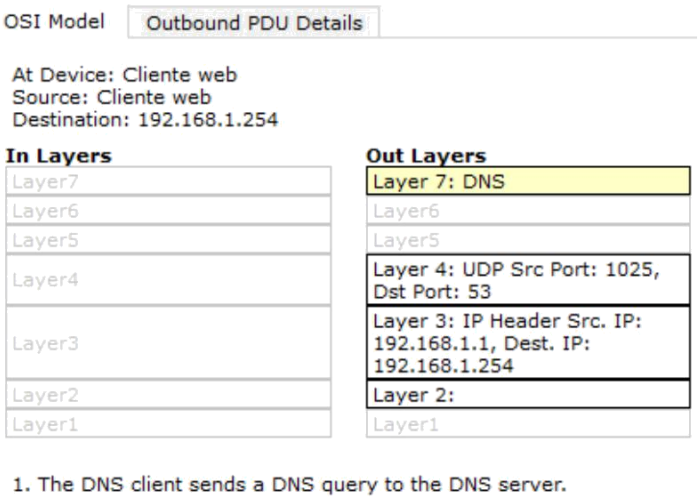
0	16	31 Bits
SRC PORT: 1025	DEST PORT: 53	
LENGTH: 0x25	CHECKSUM: 0x0	
DATA (VARIABLE)		

DNS Header

0 1	5	8 9	12	15 Bits
ID				
	OPCODE	AA TC RD RA	Z	RCODE
QDCOUNT: 1				
ANCOUNT: 0				
NSCOUNT: 0				
ARCOUNT: 0				

DNS Query

0	16	31 Bits
NAME: www.osi.local		
TYPE: 0x0001	CLASS: 0x0001	



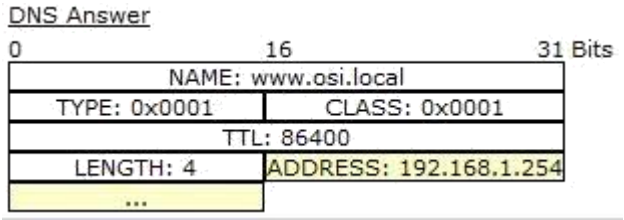
d. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿Qué información se indica en **NAME**: (NOMBRE:) en la sección DNS QUERY (CONSULTA DNS)?

www.osi.local

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**?

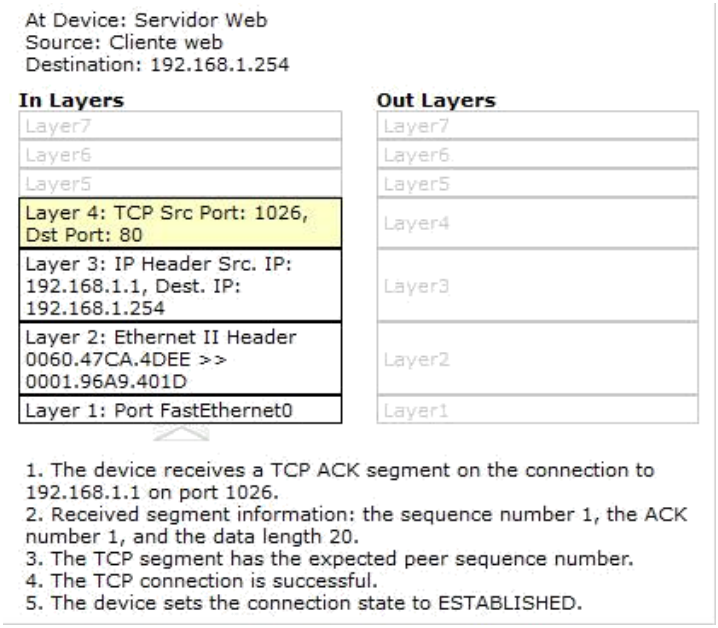
192.168.1.254, la dirección del servidor Web.



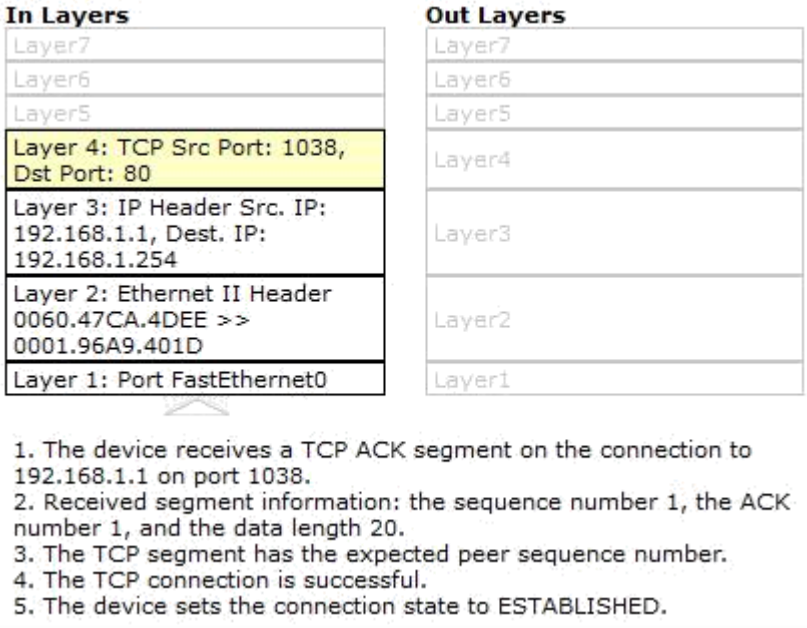
f. Busque el primer evento de **HTTP** en la lista y haga clic en el cuadro coloreado del evento de **TCP** que le sigue inmediatamente a este evento. Resalte **Layer 4** (Capa 4) en la ficha **OSI Model** (Modelo OSI). En la lista numerada que está directamente debajo de **In Layers** y **Out Layers**,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

```
Layer 4: TCP Src Port: 1038,
Dst Port: 80
```

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.

```
Layer 4: UDP Src Port: 1025,
Dst Port: 53
```

5.3.3.5 Configuración de Switches de Capa 3

Topología

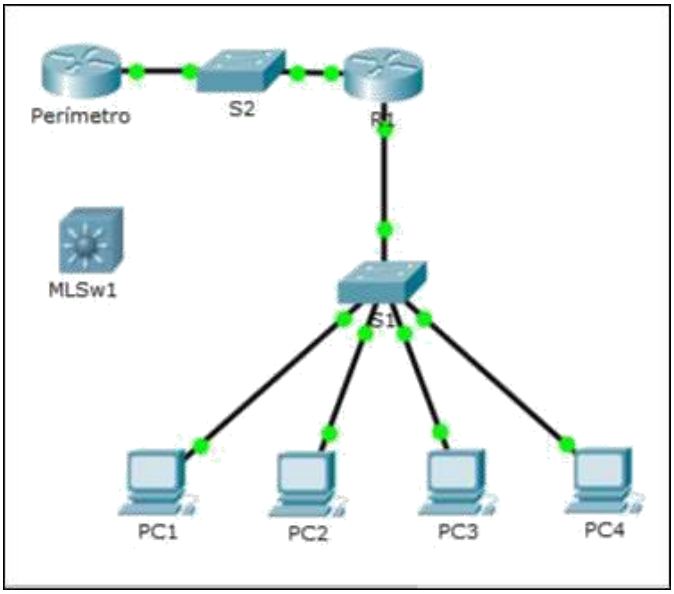


Tabla de direccionamiento

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

Objetivos

Parte 1: Documentar la configuración actual de la red

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

Situación

El administrador de red reemplaza el router y el switch actuales por un nuevo switch de capa 3. Como técnico de red, su trabajo consiste en configurar el switch y ponerlo en funcionamiento. Trabajará después del horario laboral para minimizar los inconvenientes para la empresa.

Parte 1: Documentar la configuración actual de la red

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.

```
Router#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 172.16.31.1/24
  Broadcast address is 255.255.255.255
```

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

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

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

a. Haga clic en **MLSw1** y, a continuación, en la ficha **CLI**.

b. Ingrese al modo de configuración de interfaz para **GigabitEthernet 0/1**.

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

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

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface g0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.0.2 255.255.255.0
Switch(config-if)#no shutdown
```

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(config)#interface vlan 1
Switch(config-if)#ip address 172.16.31.1 255.255.255.0
Switch(config-if)#no shutdown

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

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

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

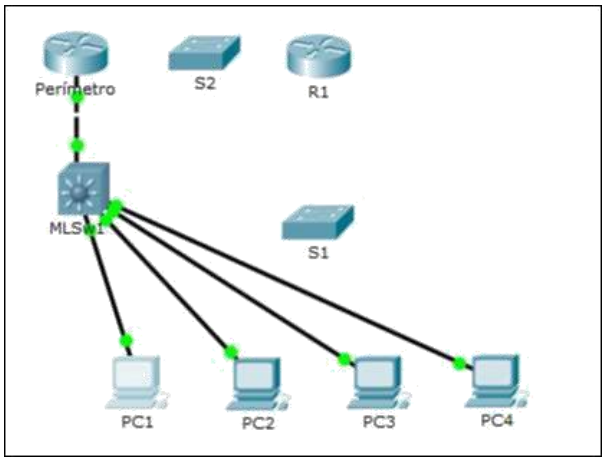
Paso 2: Implementar el nuevo switch multicapa y verificar que la conectividad esté restaurada

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**.

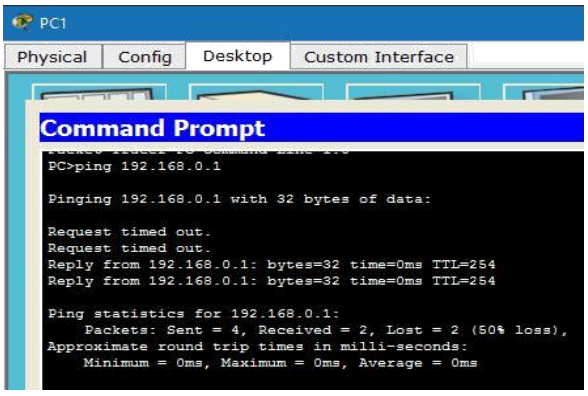


d. Verifique que todas las PC puedan hacer ping a **Edge** en 192.168.0.1.

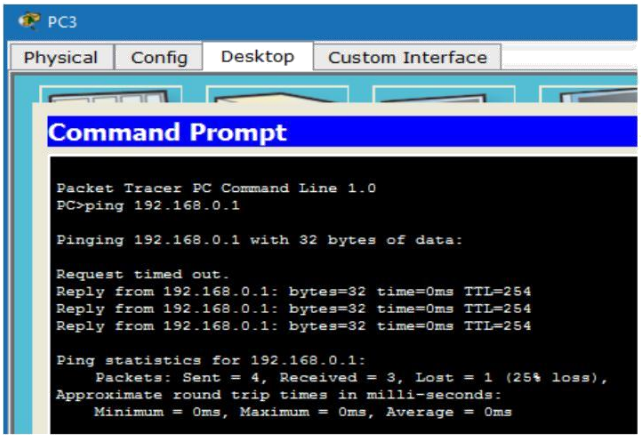
PC1

```
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=0ms TTL=254
Reply from 192.168.0.1: bytes=32 time=3ms TTL=254
Reply from 192.168.0.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

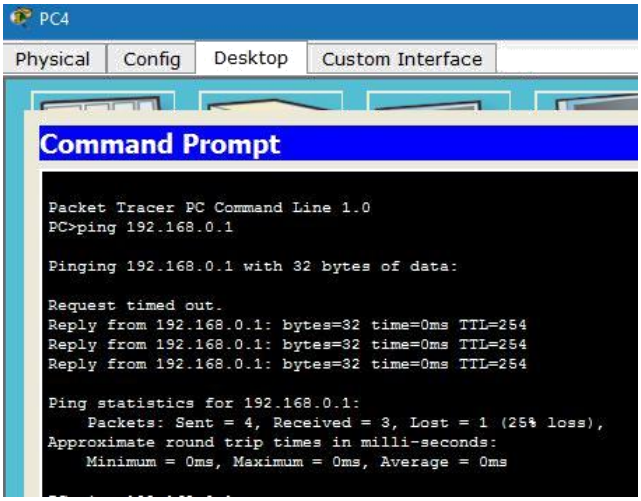
PC2



PC3



PC4



6.5.1.2 Packet Tracer Skills Integration Challenge Instructions IG

Packet Tracer: Reto de habilidades de integración

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado

College	G0/0	172.14.5.1	255.255.255.0	No aplicable
	G0/1	172.14.10.1	255.255.255.0	No aplicable
Class-A	VLAN 1	172.14.5.35	255.255.255.0	[[R1G0Add]]
Class-B	VLAN 1	172.14.10.35	255.255.255.0	[[R1G1Add]]
Student-1	NIC	172.14.5.50	255.255.255.0	[[R1G0Add]]
Student-2	NIC	172.14.5.60	255.255.255.0	[[R1G0Add]]
Student-3	NIC	172.14.10.50	255.255.255.0	[[R1G1Add]]
Student-4	NIC	172.14.10.60	255.255.255.0	[[R1G1Add]]

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.

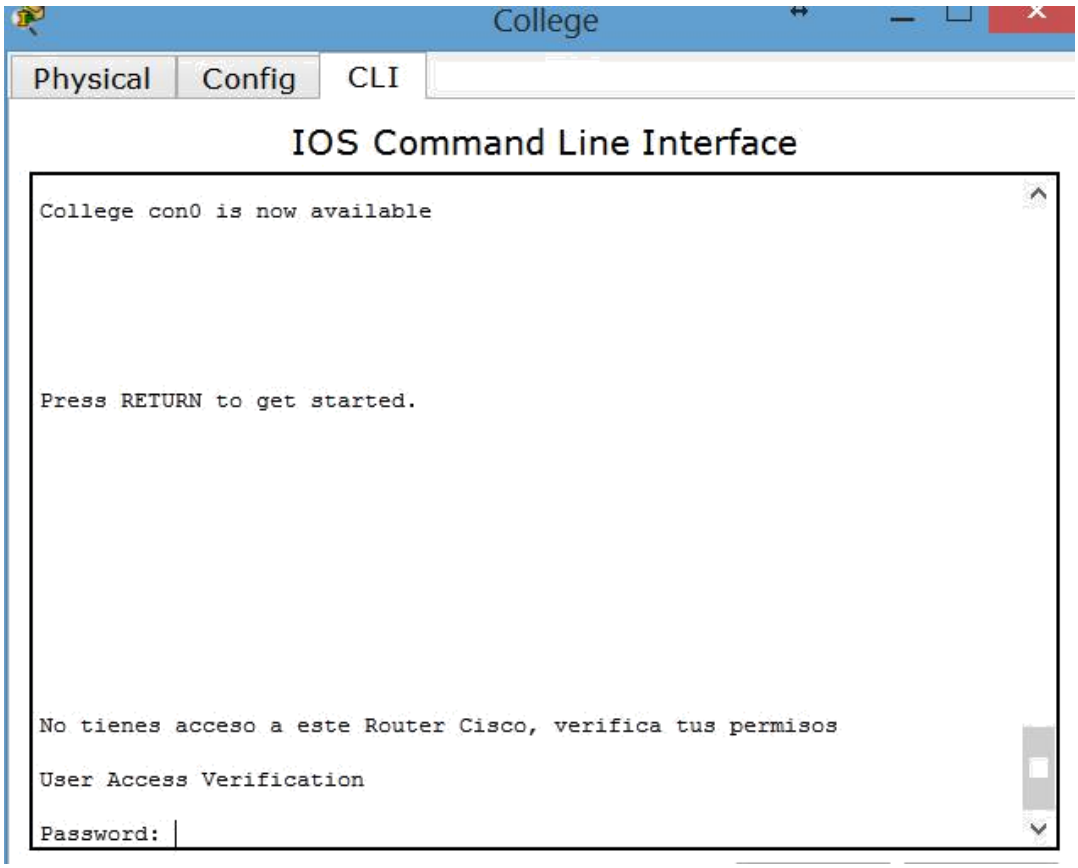
Requisitos

- Proporcione la información que falta en la tabla de direccionamiento.
- Asigne el nombre **[[R1Name]]** al router y **[[S2Name]]** al segundo switch. No podrá acceder a

[[S1Name]].

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

- Utilice **class** como contraseña de EXEC privilegiado.
- Encripte todas las contraseñas de texto no cifrado.
- Configure un aviso apropiado.

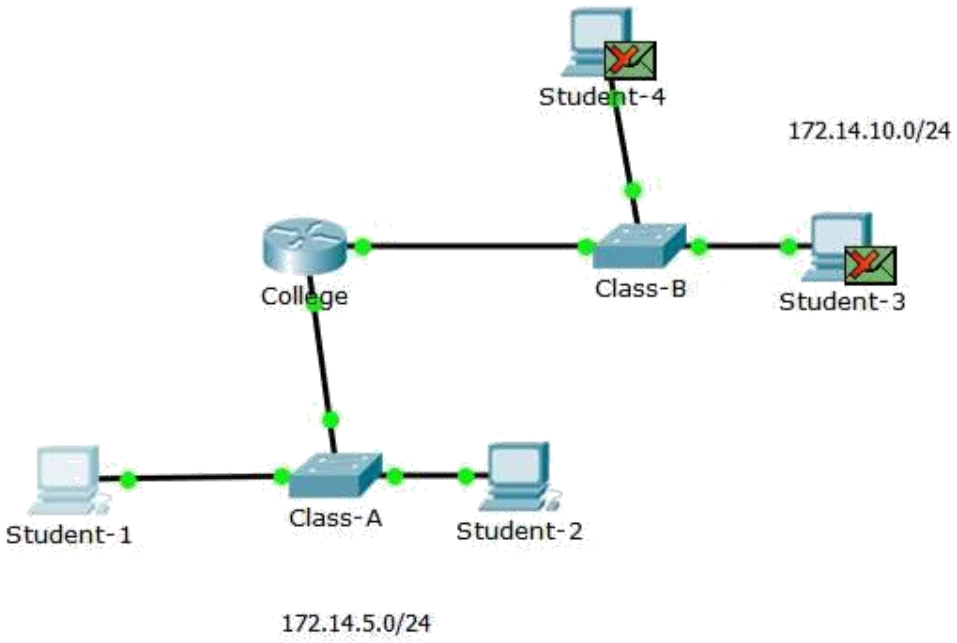


- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Registre las interfaces con descripciones, incluida la interfaz VLAN 1 de **[[S2Name]]**.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos. Todos los dispositivos deben poder hacerse ping entre sí.
- Resuelva cualquier problema y regístrelo.

Al realizar PING al PC 172.14.10.60 se presentó una falla

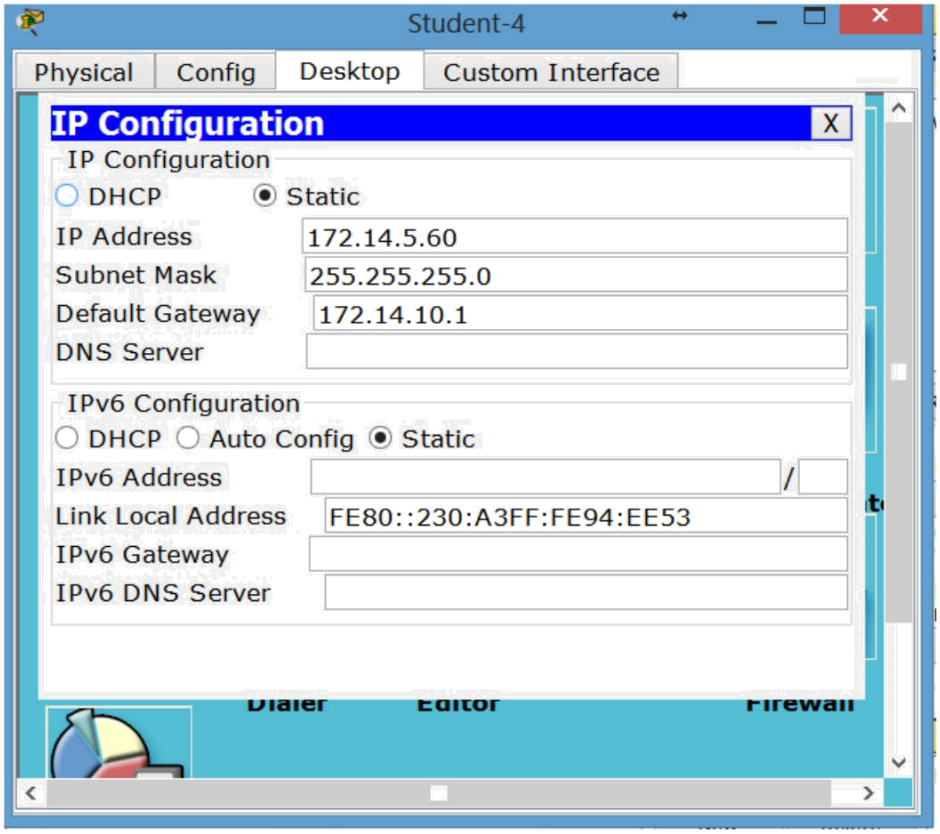
```
PC>ping 172.14.10.60

Pinging 172.14.10.60 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.14.10.60:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Se pasó a modo simulación para observar como viajan los paquetes y en donde está el error

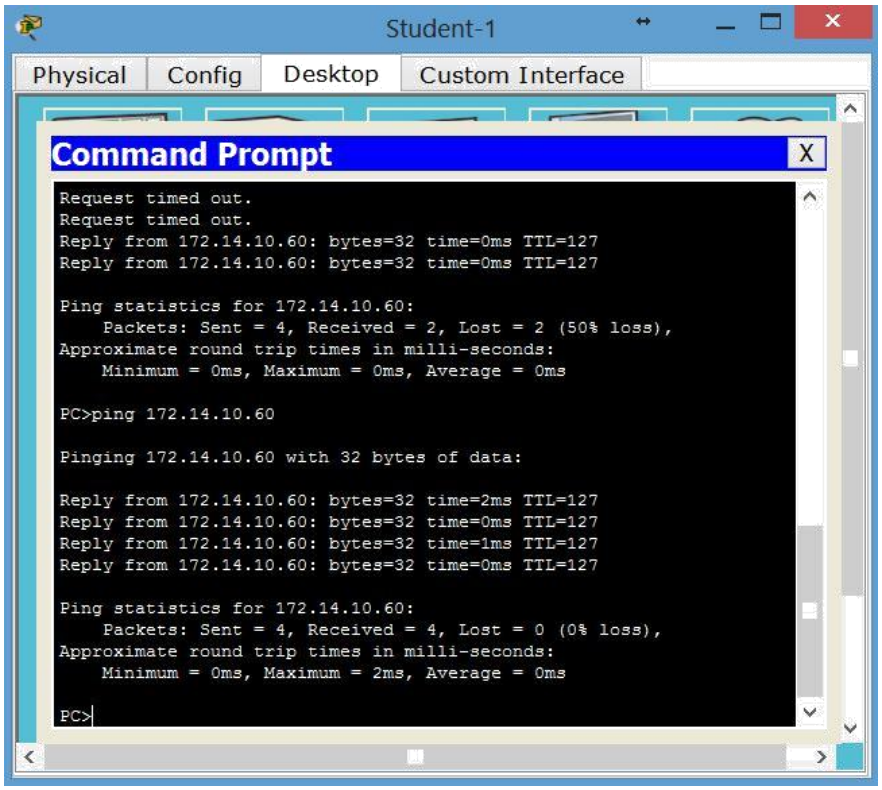


Se observa que la falla esta en la VLAN

Al investigar un poco nos damos cuenta que la dirección IP del equipo Student-4 está mal asignada, ya que debería de ser 172.14.10.60 y está 172.14.5.60



Al cambiar ya el PING funciona correctamente



- 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: [[indexNames]][[indexAdds]][[indexTopos]]

Esta actividad está configurada con un error que el estudiante deberá corregir para obtener la mayor puntuación. La dirección IP en [[PC4Name]] está en la subred incorrecta y no coincide con la dirección IP en la tabla de direccionamiento. Las respuestas correctas dependen de la situación que el alumno recibió para trabajar. La contraseña para acceder al asistente de la actividad es **PT_ccna5**.

2.1.4.8 Packet Tracer: Navegación de IOS.

Topología

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**.

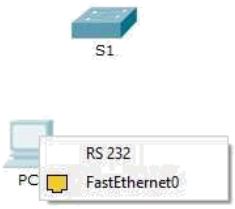
Parte 1: Conexiones básicas, acceso a la CLI y exploración de ayuda
En la parte 1 de esta actividad, conectará una PC a un switch mediante una conexión de consola e investigará diferentes modos de comando y características de ayuda.

Paso 1: La conexión de la PC1 a S1 requiere un cable de consola.

a. Haga clic en el ícono **Connections** (Conexiones), similar a un rayo, en la esquina inferior izquierda de la ventana de Packet Tracer.

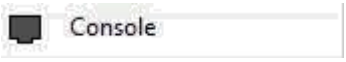
b. Haga clic en el cable de consola celeste para seleccionarlo. El puntero del mouse cambia a lo que parece ser un conector con un cable que cuelga de él.

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



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

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

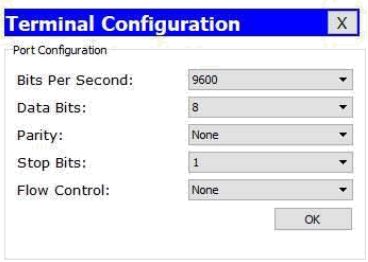


Paso 2: Establezca una sesión de terminal con el S1.

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

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

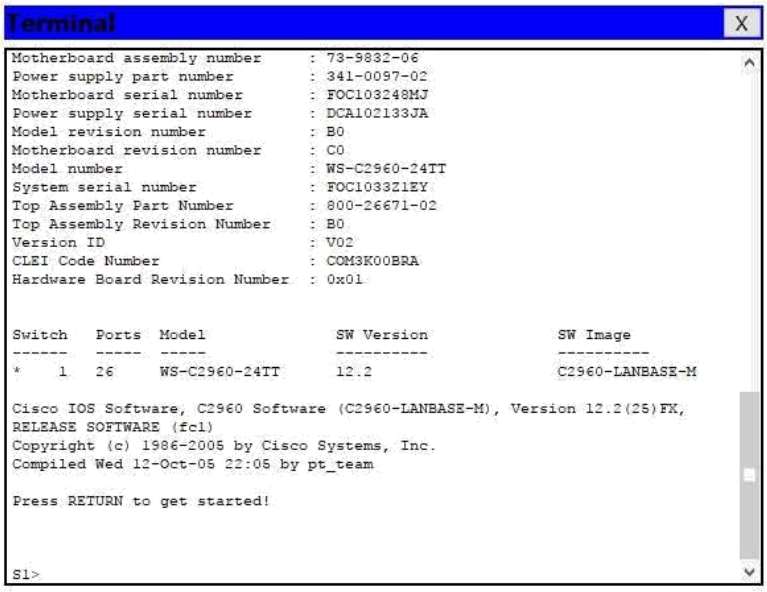
¿Cuál es el parámetro de bits por segundo?



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

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

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



Paso 3: Examine la ayuda de IOS. a. El IOS puede proporcionar ayuda para los comandos según el nivel al que se accede. La petición de entrada que se muestra actualmente se denomina **Modo EXEC del usuario** y el dispositivo está esperando un comando. La forma más básica de solicitar ayuda es escribir un signo de interrogación (?) en la petición de entrada para mostrar una lista de comandos.

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

¿Qué comando comienza con la letra "C"?

```
connect     Open a terminal connection
```

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

¿Qué comandos se muestran?

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

En la petición de entrada, escriba **te**, seguido de un signo de interrogación (**?**).
¿Qué comandos se muestran?

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

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

Parte 2: Exploración de los modos EXEC

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

Paso 1: Ingrese al modo EXEC privilegiado.

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

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

```
enable      Turn on privileged commands
```

b. Escriba **en** y presione la tecla **Tabulación**
¿Qué se muestra después de presionar la tecla **Tabulación**?

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

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

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

Al no ser un comando único, este no proporciona información suficiente por lo tanto el comando seguirá repitiéndose hasta que el usuario introduzca el nombre del comando completo.

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

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

```
S1>enable
S1#
```

d. Cuando se le solicite, escriba el signo de interrogación (**?**).
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
```

Paso 2: Ingresar en el modo de configuración global

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

¿Cuál es el mensaje que se muestra?

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

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

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

Parte 3: Configuración del comando clock
Paso 1: Utilizar el comando clock

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

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

```
S1#show clock
*1:12:22.944 UTC Mon Mar 1 1993
```

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

¿Qué información aparece en pantalla?

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

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

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

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

paso. ¿Qué información se solicita?

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

¿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?

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

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

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
```

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

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

```
S1#clock set 15:00:00 31 jan 2035
S1#show clock
*15:0:9.943 UTC Wed Jan 31 2035
S1#
```

Paso 2: Explorar los mensajes adicionales del comando

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

b. Emita el siguiente comando y registre los mensajes:

S1# **cl**

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

S1# **clock**

¿Qué información se devolvió?

```
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.
```

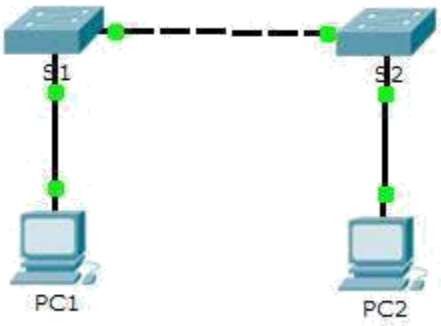
S1# **clock set 15:00:00 32**

¿Qué información se devolvió?

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

8. EJERCICIO 2.2.3.3

Packet Tracer: Configuración de los parámetros iniciales del switch Topología



Objetivos

Parte 1: Verificar la configuración predeterminada del switch

Parte 2: Establecer una configuración básica del switch

Parte 3: Configurar un título de MOTD

Parte 4: Guardar los archivos de configuración en la NVRAM

Parte 5: Configurar el S2

Información básica

En esta actividad, realizará configuraciones básicas del switch. Protegerá el acceso a la interfaz de línea de comandos (CLI, command-line interface) y a los puertos de la consola mediante contraseñas encriptadas
y contraseñas de texto no cifrado. También aprenderá cómo configurar mensajes para los usuarios que inician sesión en el switch. Estos avisos también se utilizan para advertir a usuarios no autorizados que el acceso está prohibido.

Parte 1: Verificar la configuración predeterminada del switch

Paso 1: Entre al modo privilegiado.

Puede acceder a todos los comandos del switch en el modo privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros

operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como el comando **configure** a través del cual se obtiene el acceso a los modos de comando restantes.

a. Haga clic en **S1** y, a continuación, en la ficha **CLI**. Presione **<Entrar>**.
b. Ingrese al modo EXEC privilegiado introduciendo el comando **enable**:

Packet Tracer: Configuración de los parámetros iniciales del switch

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**

```
Switch>enable
Switch#show
Switch#show r
Switch#show running-config
Building configuration...

Current configuration : 1043 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
```

```
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
```

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
        end
```

b. Responda las siguientes preguntas:

¿cuantas interfaces FastEthernet tiene el switch?

R. 24

¿cuantas interfaces Gigabit Ethernet tiene el switch?

R: 2

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

R: 0 -15

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

R: show startup-configuration

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

R: Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM

. Actualmente se encuentra solo en RAM.

Parte 2: 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#

```
S1#CONF
S1#CONFigure TER
S1#CONFigure TERminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line
S1(config)#line c
S1(config)#line console 0
S1(config-line)#pas
S1(config-line)#password letmein
S1(config-line)#login
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Packet Tracer: Configuración de los parámetros iniciales del switch

Paso 3: Verifique que el acceso a la consola sea seguro.

Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.

S1# **exit**

Switch con0 is now
available Press RETURN
to get started.

User Access
Verification
Password:

S1>

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

Paso 4: Proporcionar un acceso seguro al modo privilegiado

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

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

```
S1>ena
S1>enable
S1#conf
S1#configure ter
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ena
S1(config)#enable pas
S1(config)#enable password c1$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

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

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

   User Access
   Verification
   Password:

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

d. Introduzca el comando para acceder al modo privilegiado.

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

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

   S1# **show running-configuration**

S1#show
S1#show run
S1#show running-config
Building configuration...

Current configuration : 1088 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec

```
no service password-encryption
!
hostname S1
!
enable password c1$c0
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
```

```
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password letmein
login
!
line vty 0 4
login
line vty 5 15
login
!
!
end

        S1#
```

Observe que las contraseñas de consola y de enable son de texto no cifrado. Esto podría presentar un riesgo para la seguridad si alguien está viendo lo que hace.

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

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

de enable en **itsasecret**.

S1# **config t**

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

Packet Tracer: Configuración de los parámetros iniciales del switch

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**

```
Password:
S1#
S1#sho
S1#show r
S1#show running-config
Building configuration...

Current configuration : 1135 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
!
```

```
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
```

```
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password letmein
login
!
line vty 0 4
login
line vty 5 15
login
!
!
end
```

S1#

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

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

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

R: El commando 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?

R: 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?

R: 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).

Packet Tracer: Configuración de los parámetros iniciales del switch

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**?

R: **cop r s**

Paso 3: Examinar el archivo de configuración de inicio

¿Qué comando muestra el contenido de la NVRAM?

R: **show startup-configuration**

¿Todos los cambios realizados están grabados en el archivo?

R: Sí, es igual a la configuración en ejecución.

Parte 5: Configurar S2

Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.

Configure el S2 con los siguientes parámetros:

a. Nombre del dispositivo: **S2**

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

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

d. Configure el siguiente mensaje para aquellas personas que inician sesión en el switch:

   Acceso autorizado únicamente. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

e. Encripte todas las contraseñas de texto no cifrado.

f. Asegúrese de que la configuración sea correcta.

g. Guarde el archivo de configuración para evitar perderlo si el switch se apaga.

```
Switch>ena
ble
Switch#con
fig t
Enter configuration commands,one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console0 S2(config-
line)#password letmein S2(config-
line)#login S2(config-line)#enable
password c1$c0 S2(config)#enable
secret itsasecret
```

S2(config)#banner motd $any text here$

S2(config)#service password-encryption

S2(config)#do wr

S2#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption !

hostname S2
!
enable secret 5
1mERr$ILwq/b7kc.7X/ejA4Aosn0 enable
password 7 08221D0A0A49 !
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^CAcceso no autorizado^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
```

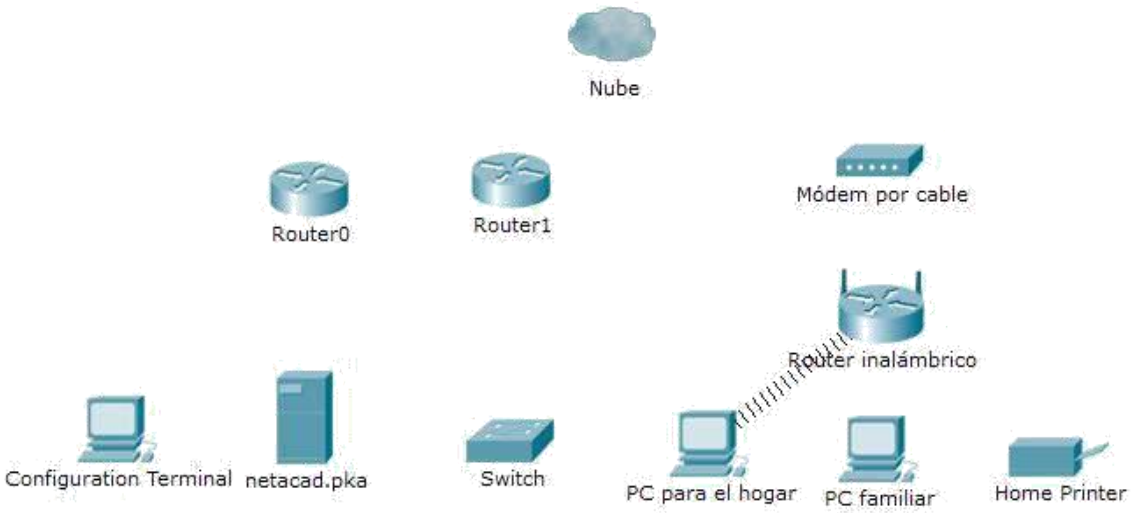
!
end

S2#

9. EJERCICIO 4.2.4.5

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

Topología



Packet Tracer: conexión de una red LAN cableada e inalámbrica 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

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

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

Paso 2: Conectar la nube al módem por cable

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

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

Elija el cable adecuado para conectar la **interfaz Ser0/0/0 del Router0** a la **interfaz Ser0/0 del Router1**. Use uno de los cables **seriales** disponibles.

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

Paso 2: Conectar el Router0 a netacad.pka

Elija el cable adecuado para conectar la **interfaz Fa0/1 del Router0** a la **interfaz Fa0 de netacad.pka**. Los routers y las PC tradicionalmente utilizan los mismos cables para transmitir (1 y 2) y recibir (3 y 6). El cable adecuado que se debe elegir

consta de cables cruzados. Si bien muchas NIC ahora pueden detectar automáticamente qué par se utiliza para transmitir y recibir, el **Router0** y **netacad.pka** no tienen NIC con detección automática.

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

Paso 3: Conectar el Router0 a la terminal de configuración

Elija el cable adecuado para conectar la **consola** del **Router0** a la **terminal de configuración RS232**. Este cable no proporciona acceso a la red a la **terminal de configuración**, pero le permite configurar el **Router0** a través de su terminal.

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

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

Elija el cable adecuado para conectar la **interfaz Fa1/0 del Router1** a la **interfaz Fa0/1 del switch**.

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

Deje que transcurran unos segundos para que la luz cambie de color ámbar a verde.

Paso 2: Conectar el módem por cable al router inalámbrico

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

Packet Tracer: conexión de una red LAN cableada e inalámbrica

Paso 3: Conectar el router inalámbrico a la PC familiar

Elija el cable adecuado para conectar la **interfaz Ethernet 1 del router inalámbrico** a la **PC familiar**. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka

c. Abra el símbolo del sistema de la **PC familiar** y haga ping a **netacad.pka**.

d. 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

g. Abra la **terminal** de la **terminal de configuración** y acepte la configuración predeterminada.

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

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

Parte 5: Examinar la topología física

Paso 1: Examinar la nube

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

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

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

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

Paso 2: Examinar la red principal

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

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

Paso 3: Examinar la red secundaria

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

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

Packet Tracer: conexión de una red LAN cableada e inalámbrica

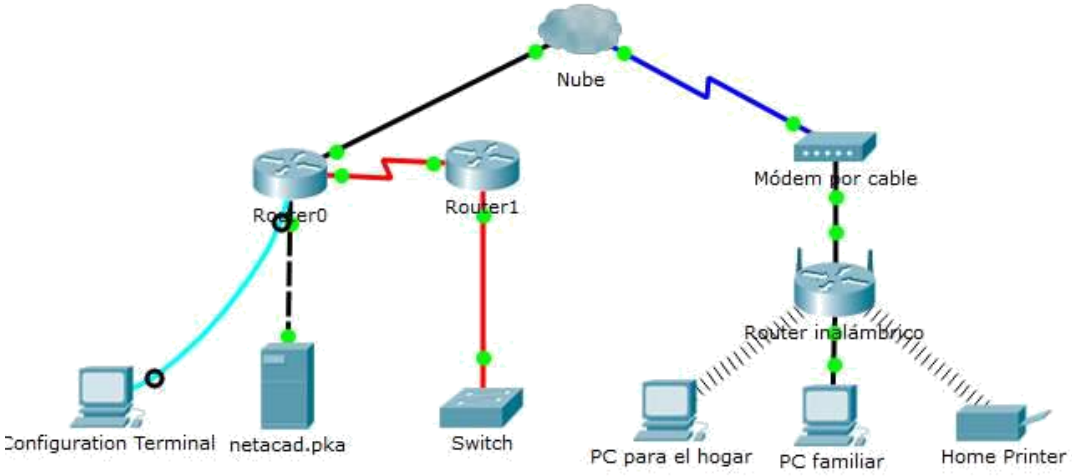
Paso 4: Examinar la red doméstica

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

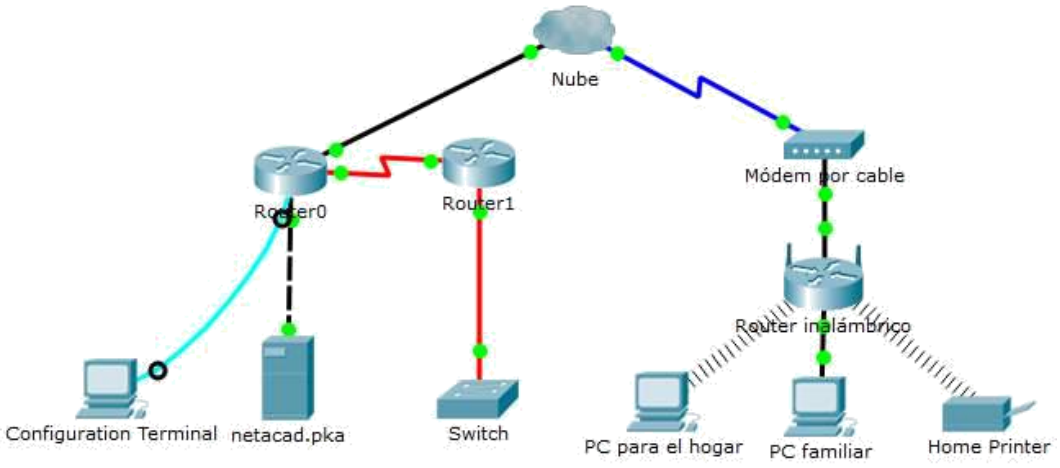
m. Haga clic en el ícono **Home Network** (Red doméstica). ¿Por qué no hay ningún bastidor para contener el equipo?
R: Por lo general, las redes domésticas no incluyen bastidores.

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

EVIDENCIAS



FUNCIONAMIENTO



DU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router0	Switch	ICMP		0.000	N	0	(edit)	
	Successful	PC par...	Home Printer	ICMP		0.000	N	1	(edit)	
	Successful	Switch	netacad.pka	ICMP		0.000	N	2	(edit)	

10. EJERCICIO 6.4.1.2

Packet Tracer: Configuración inicial del router

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

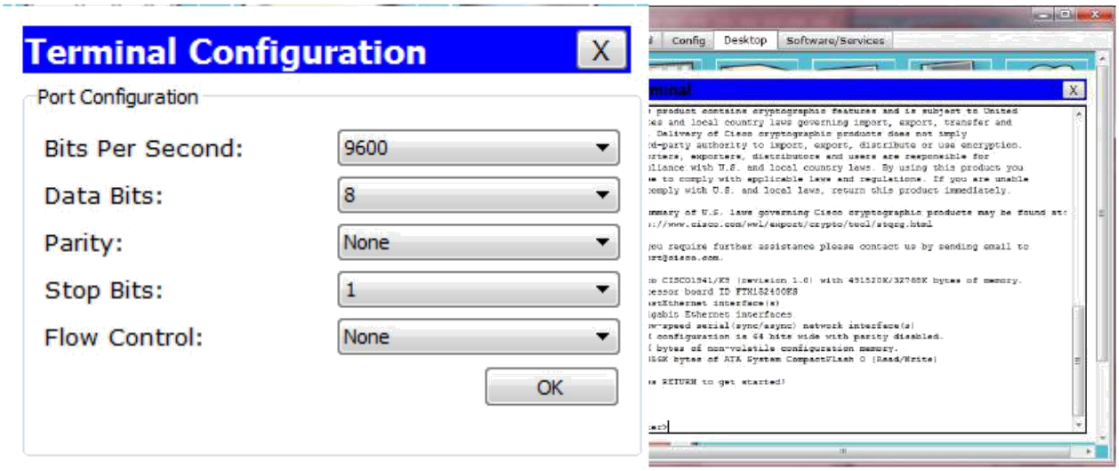
a. Elija un cable de **consola** de las conexiones disponibles.

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? R: Router

d. ¿Cuántas interfaces Fast Ethernet tiene el router?
R: 4

```
interface FastEthernet0/1/0
 switchport mode access
 shutdown
!
interface FastEthernet0/1/1
 switchport mode access
 shutdown
!
interface FastEthernet0/1/2
 switchport mode access
 shutdown
!
interface FastEthernet0/1/3
 switchport mode access
 shutdown
```

e. ¿Cuántas interfaces Gigabit Ethernet tiene el router?

R: 2

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
```

f. ¿Cuántas interfaces seriales tiene el router?

R: 2

```
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
```

g. ¿Cuál es el rango de valores que se muestra para las líneas vty?

R: 0 – 4

```
line vty 0 4
 login
!
```

h. Muestre el contenido actual de la NVRAM.
Router# **show startup-config**
startup-config is not present

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

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

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

Parte 2: Configurar y verificar la configuración inicial del router

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

Paso 1: Configurar los parámetros iniciales de R1

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

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

b. Utilice las siguientes contraseñas:

1) Consola: **letmein**
2) EXEC privilegiado, sin encriptar: **cisco**
3) EXEC privilegiado, encriptado: **itsasecret**

```
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#enable password cisco
R1(config)#enable secret itsasecret
R1(config)#
```

R1(config)#

R1(config)#line console 0

R1(config-line)#password letmein

R1(config-line)#login

R1(config-line)#enable password cisco

R1(config)#enable secret itsasecret

R1(config)#

c. Encripte todas las contraseñas de texto no cifrado.}

```
R1(config)#
R1(config)#service password-encryption
R1(config)#
```

R1(config)#

R1(config)#service password-

encryption R1(config)#

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

```
R1(config)#banner motd &
Enter TEXT message.  End with the character '&'.
Unauthorized access is strictly prohibited (El acceso no
autorizado queda terminantemente prohibido).
&
```

R1(config)#banner motd &

Enter TEXT message. End with the character '&'.

Unauthorized access is strictly prohibited (El acceso

no autorizado queda terminantemente prohibido). &

R1(config)#

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

Paso 2: Verificar los parámetros iniciales de R1

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

R:show running-config

b. Salga de la sesión de consola actual hasta que vea el siguiente mensaje:
R1 con0 is now available

Press RETURN to get started.

c. Presione **Entrar**; debería ver el siguiente mensaje:
Unauthorized access is strictly

prohibited. User Access Verification

Password:

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

R: Cada router debe tener un mensaje para advertir a los usuarios no autorizados que el acceso está prohibido, pero también se puede utilizar para enviar mensajes al personal y a los técnicos de red (por ejemplo, sobre cierres inminentes del sistema o a quién contactar para obtener acceso).

Si no se le pide una contraseña, ¿qué comando de la línea de consola se olvidó de configurar? R1(config-line)# **login**

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

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

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

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

Parte 3: Guardar el archivo de configuración en ejecución

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

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

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

R: copy running-config startup-config

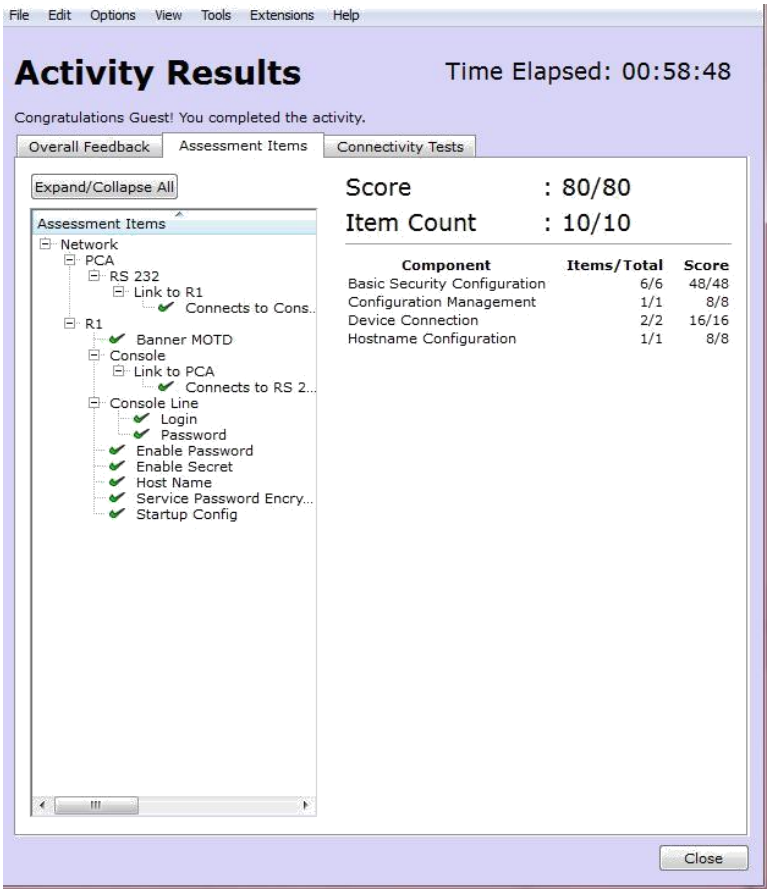
¿Cuál es la versión más corta e inequívoca de este comando?

R: copy r s

¿Qué comando muestra el contenido de la NVRAM?

R: show startup-configuration or show start

c. 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? 3

```
R1#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

R1#show flash

System flash directory:

File Length Name/status

3 33591768 c1900-universalk9-mz.SPA.151-4.M4.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

[33847587 bytes used, 221896413 available, 255744000 total]

249856K bytes of processor board System flash (Read/Write)

¿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?

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

b. Utilice los siguientes comandos para guardar el archivo de configuración de inicio en la memoria flash:
R1# **copy startup-config flash**
Destination filename [startup-config]

```
R1#copy startup-config flash
Destination filename [startup-config]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

1237 bytes copied in 0.416 secs (2973 bytes/sec)
R1#
```

R1#

R1#copy startup-config flash

Destination filename [startup-config]?

%Warning:There is a file already existing with this name

Do you want to over write? [confirm]

1237 bytes copied in 0.416 secs (2973 bytes/sec)

R1#

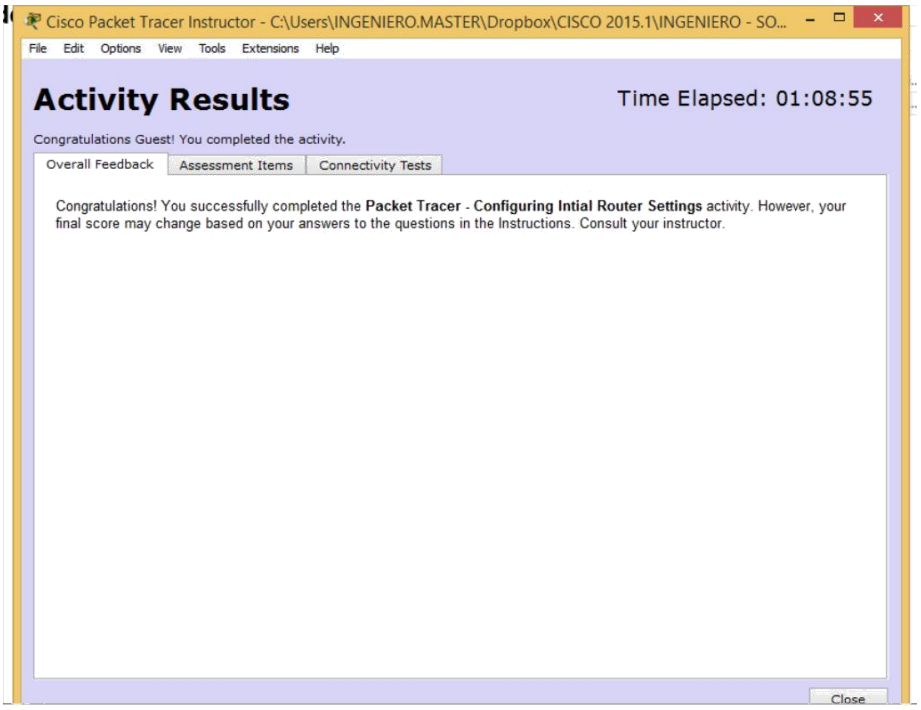
El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione **Entrar**; de lo contrario, escriba un nombre adecuado y presione la tecla **Entrar**.

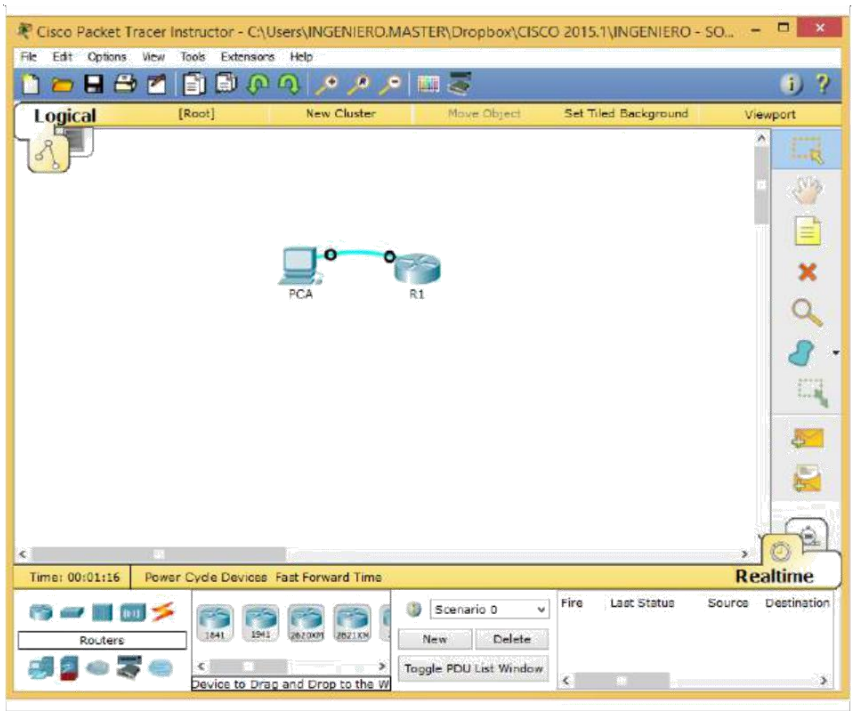
c. Utilice el comando **show flash** para verificar que el archivo de configuración de inicio esté almacenado en la memoria flash.

```
R1#show flash

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

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

EVIDENCIAS


Cisco Packet Tracer Instructor - C:\Users\INGENIERO.MASTER\Dropbox\CISCO 2015.1\INGENIERO - SO...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:08:55
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the Packet Tracer - Configuring Intial Router Settings activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.
Close


Cisco Packet Tracer Instructor - C:\Users\INGENIERO.MASTER\Dropbox\CISCO 2015.1\INGENIERO - SO...
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PCA
R1
Time: 00:01:16
Power Cycle Devices
Fast Forward Time
Realtime
Routers
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

EJERCICIOS 5.2.1.7

Topología

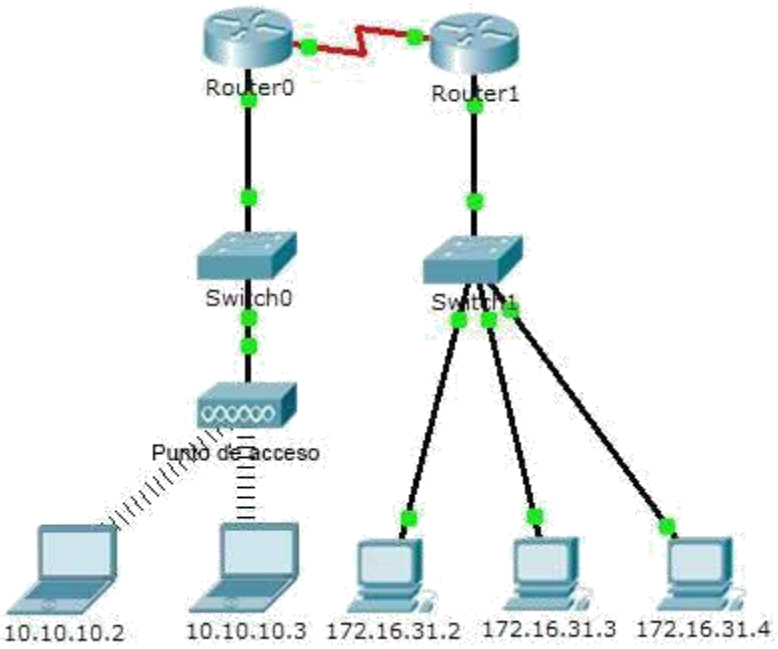


Tabla de direccionamiento

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

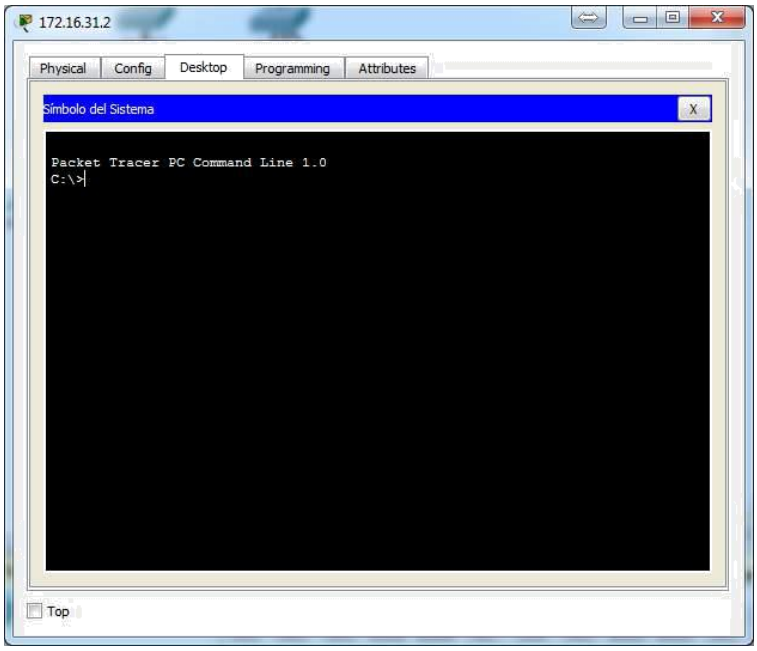
Información básica

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.

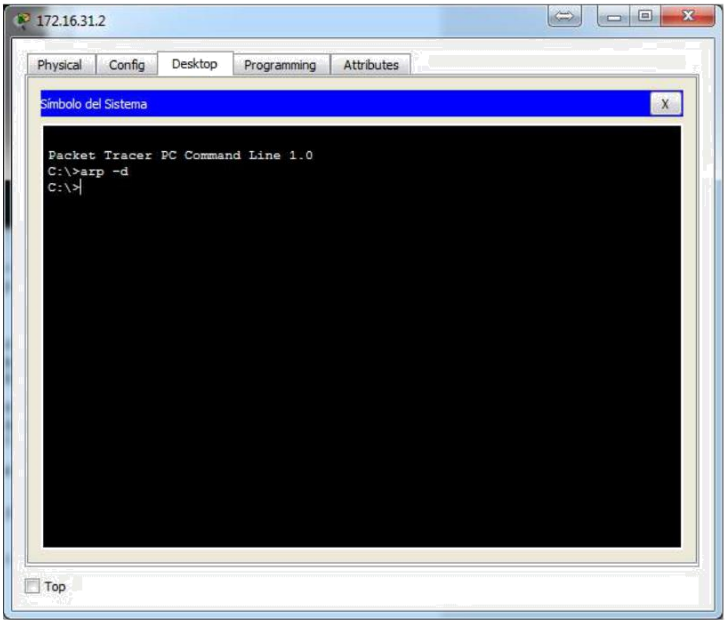
Parte 1: Examinar una solicitud de ARP

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

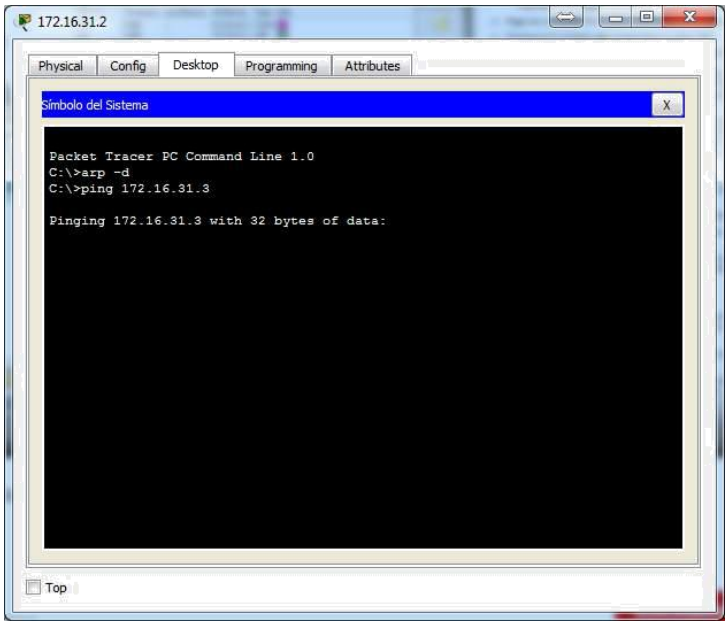
a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

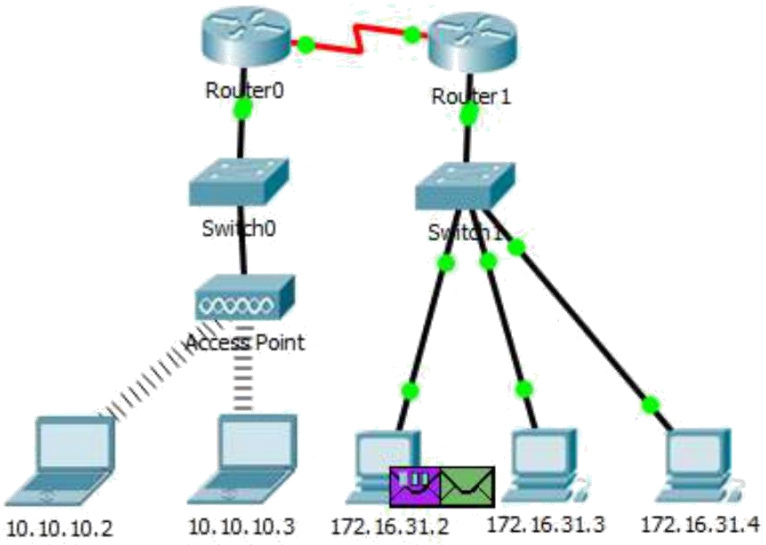


b. Introduzca el comando **arp -d** para borrar la tabla ARP.

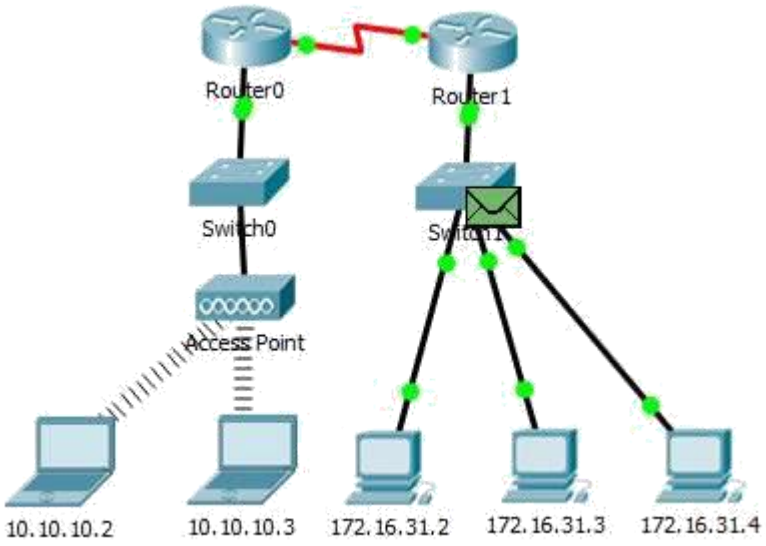


c. Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3**. Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.

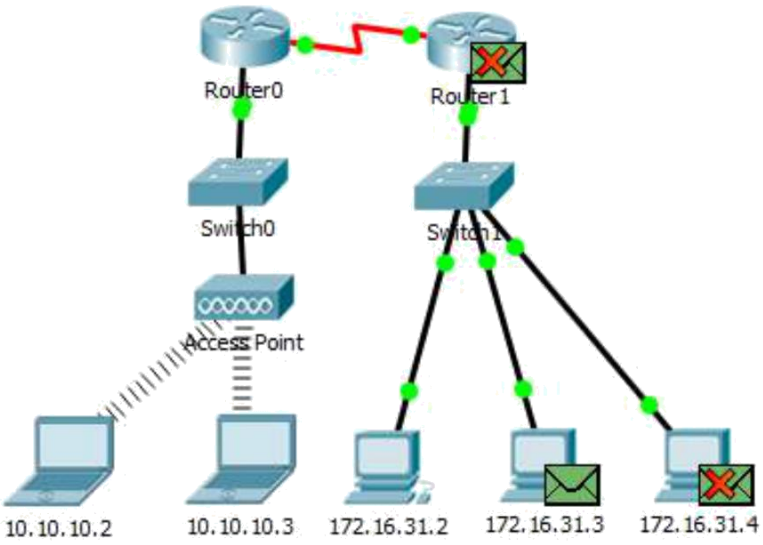




d. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. La PDU ARP mueve el **Switch1**, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior?NO



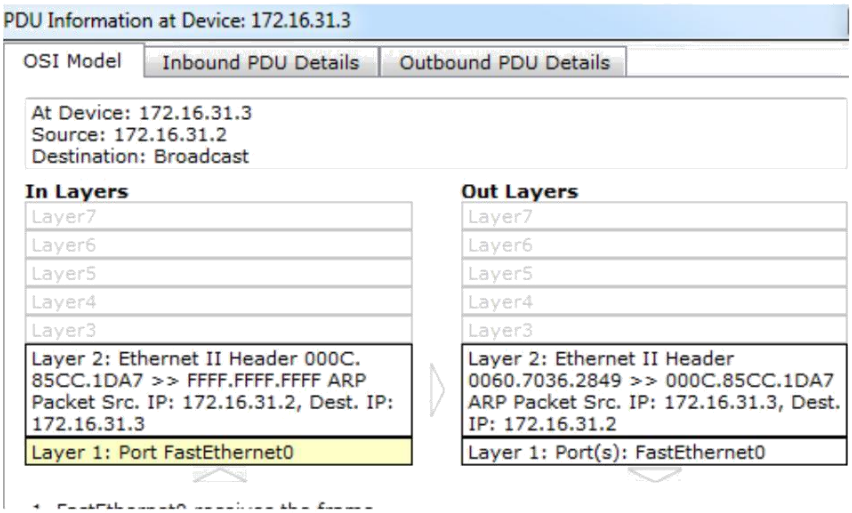
e. Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**? 3



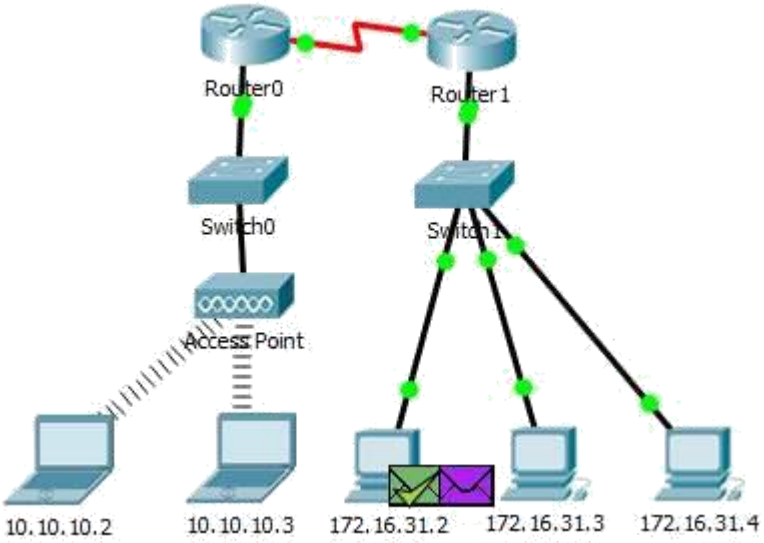
f. ¿Cuál es la dirección IP del dispositivo que aceptó la PDU? 172.16.31.3

```
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=7ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms 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 = 4ms, Maximum = 7ms, Average = 4ms

C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0060.7036.2849        dynamic

C:\>
```

g. Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino? El origen se transformó en el destino, FFFF.FFFF.FFFF se convirtió en la dirección MAC de 172.16.31.3.

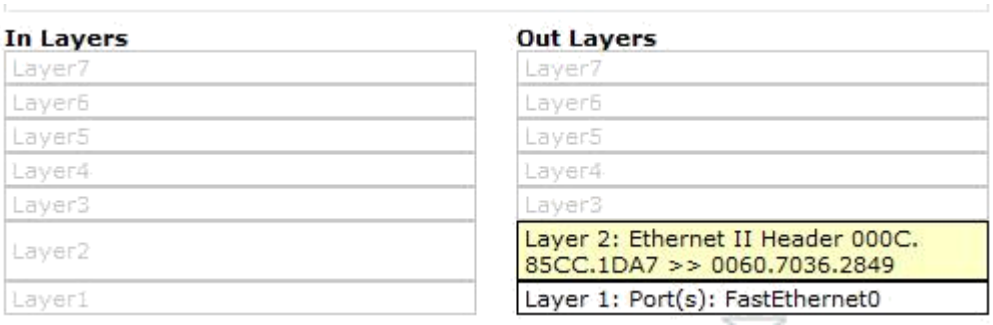


h. Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP? 1



Paso 2: Revisar la tabla ARP

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



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


```
C:\>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time=7ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms TTL=128
Reply from 172.16.31.3: bytes=32 time=4ms 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 = 4ms, Maximum = 7ms, Average = 4ms
```

c. Haga clic en **172.16.31.2** e introduzca el comando **arp -a**. ¿A qué dirección IP corresponde la entrada de la dirección MAC? 172.16.31.3

```
Packet Tracer PC Command Line 1.0
C:\>arp -d
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=11ms 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 = 11ms, Average = 2ms

C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0060.7036.2849        dynamic

C:\>
```

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

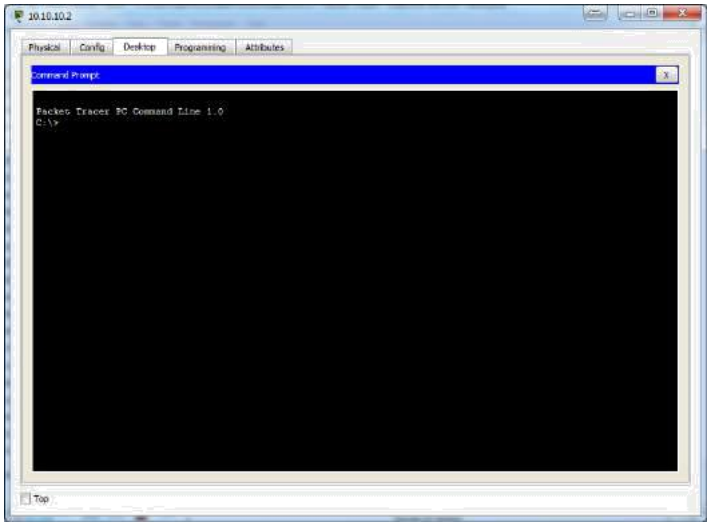
Parte 2: Examinar una tabla de direcciones MAC del switch

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

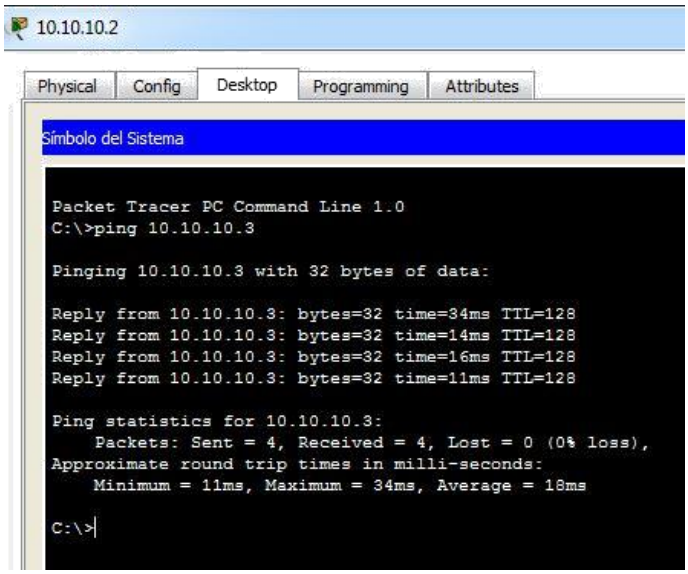
a. En **172.16.31.2**, introduzca el comando **ping 172.16.31.4**.

```
C:\>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=5ms 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 = 4ms

C:\>
```

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



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



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

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

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

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

   1    0002.1640.8d75    DYNAMIC     Fa0/3
   1    000c.85cc.1da7    DYNAMIC     Fa0/1
   1    0060.7036.2849    DYNAMIC     Fa0/2
   1    00e0.f7b1.8901    DYNAMIC     Gig0/1
Switch>
```

Si corresponden a la tabla anterior

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

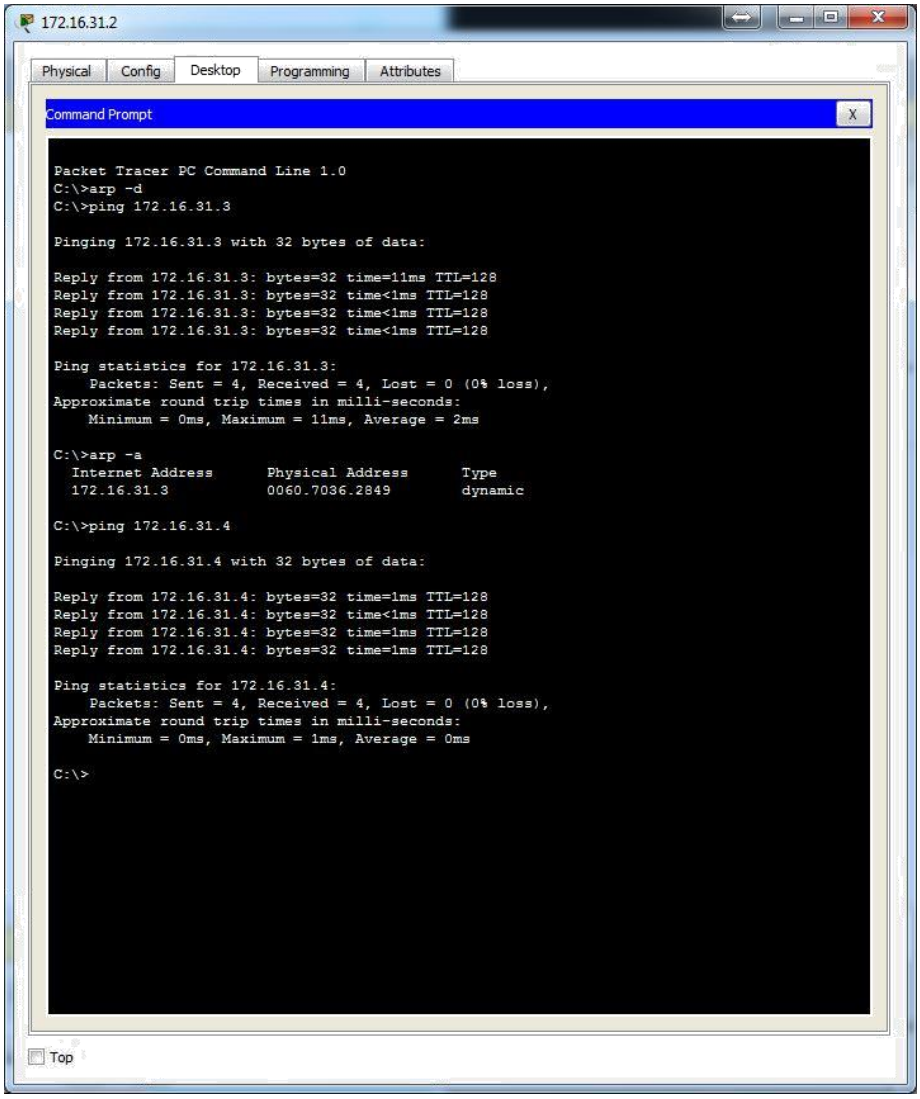
```
Switch0>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.6458.2501    DYNAMIC     Gig0/1
   1    0060.2f84.4ab6    DYNAMIC     Fa0/2
   1    0060.4706.572b    DYNAMIC     Fa0/2
Switch0>
```

c. ¿Por qué hay dos direcciones MAC asociadas a un puerto? Porque ambos dispositivos se conectan a un puerto a través del punto de acceso.

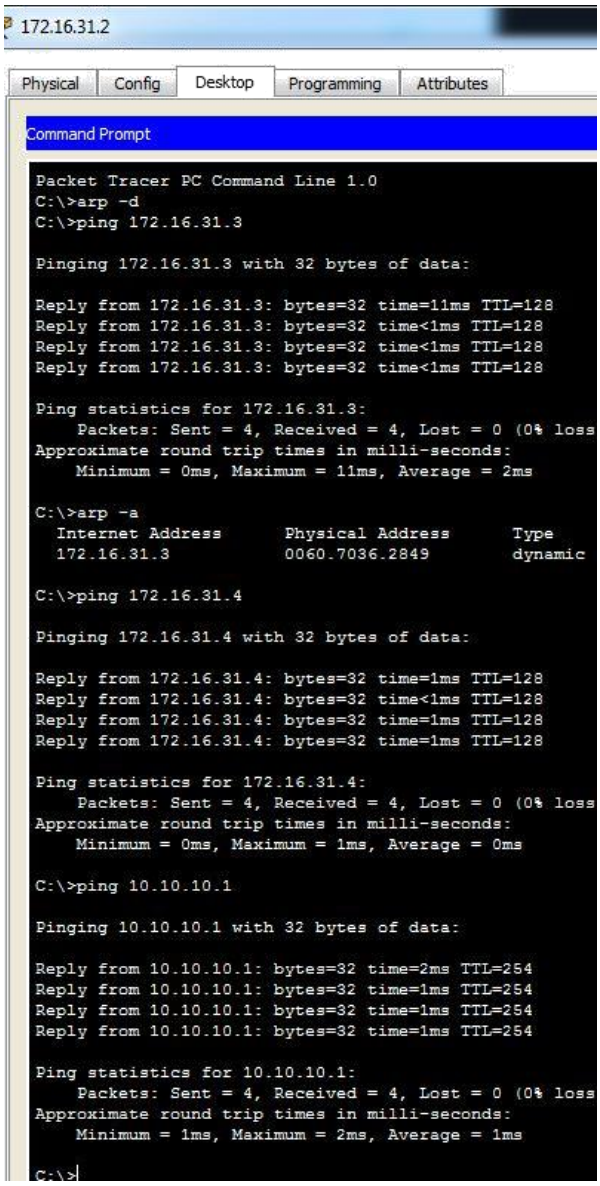
Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

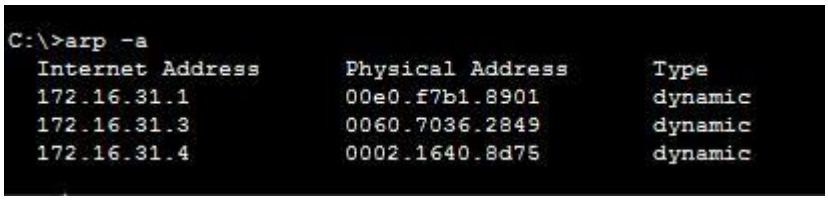
a. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.



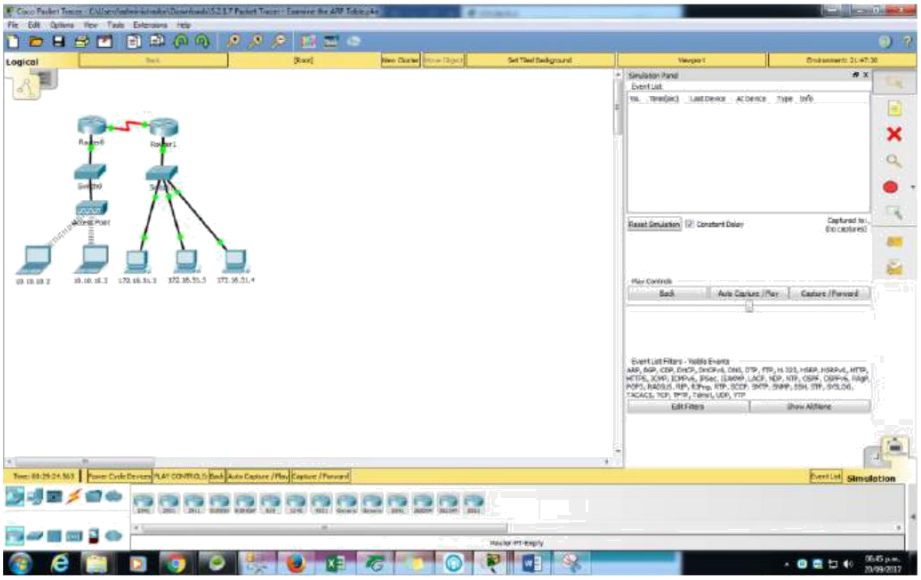
b. Introduzca el comando **ping 10.10.10.1**.



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



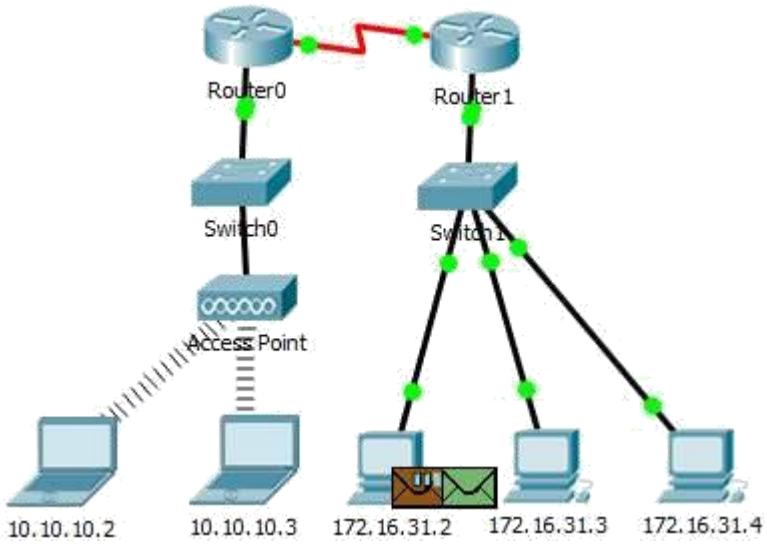
d. Introduzca el comando **arp -d** para borrar la tabla ARP y volver a cambiar al modo de **simulación**.

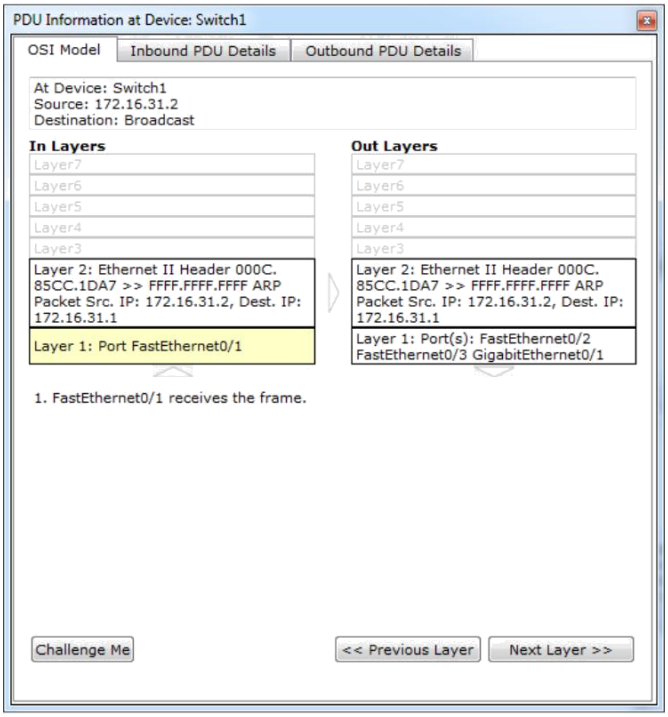


e. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen? 2

f.
```
C:\>arp -d
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
```

g. 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

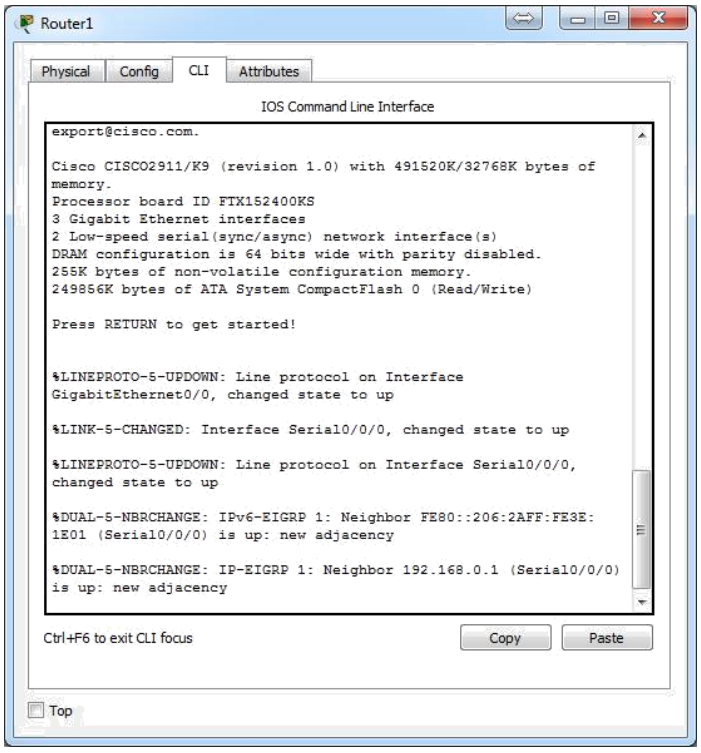




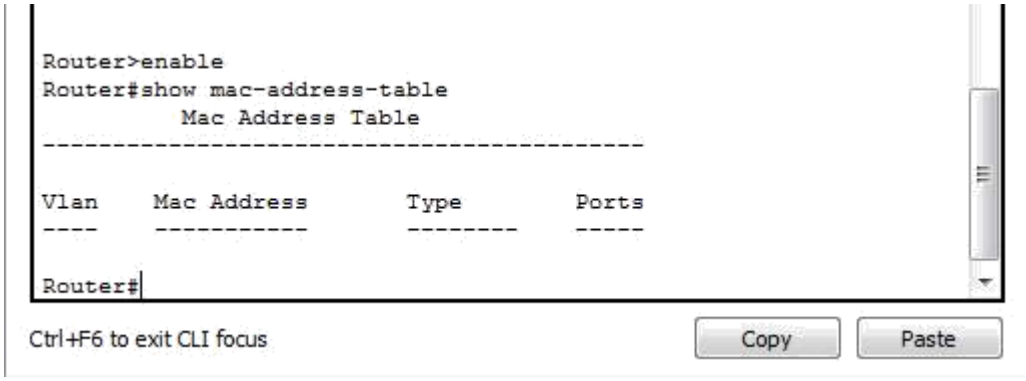
h. La dirección IP de destino no es 10.10.10.1. ¿Por qué? La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

Paso 2: Examinar la tabla ARP en el Router1

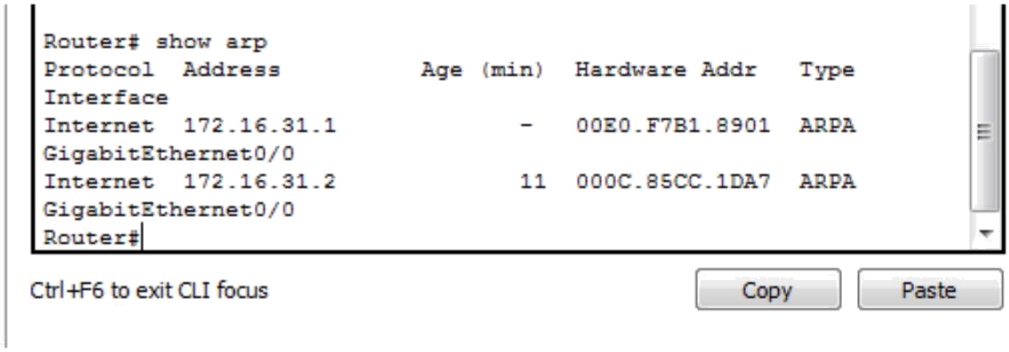
a. Cambie al modo **Realtime**. Haga clic en **Router1** y, a continuación, en la ficha **CLI**.



b. Ingrese al modo EXEC privilegiado y, a continuación, introduzca el comando **show mac-address-table**. ¿Cuántas direcciones MAC figuran en la tabla? ¿Por qué? Ninguna, este comando significa algo totalmente distinto que el comando show mac address-table de un switch.



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



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

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar una solicitud de ARP	Paso 1	10	
	Paso 2	15	
	Total de la parte 1	**25**	
Parte 2: Examinar una tabla de direcciones MAC del switch	Paso 1	5	
	Paso 2	20	
	Total de la parte 2	**25**	
Parte 3: Examinar el proceso de ARP en comunicaciones remotas	Paso 1	25	
	Paso 2	25	
	Total de la parte 3	**50**	
	Puntuación total	**100**	

EJERCICIO 6.4.3.4

Topología

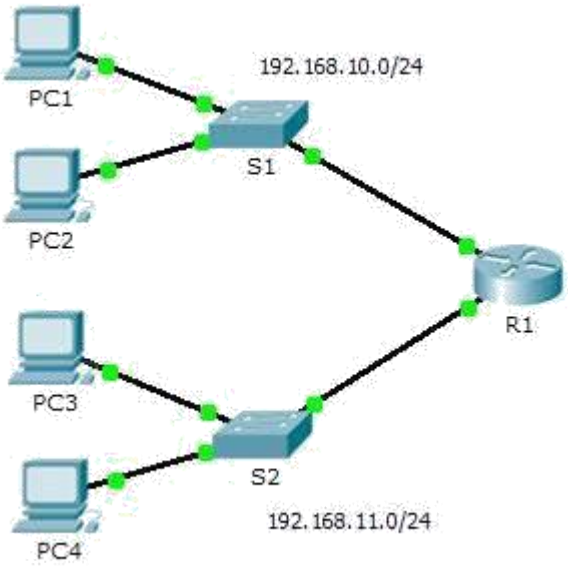


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Objetivos

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

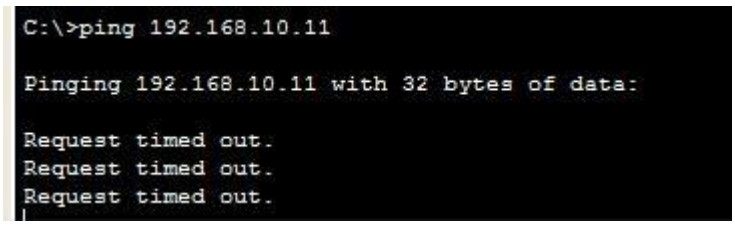
Parte 2: Implementar, verificar y documentar las soluciones

Información básica

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

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

   Lo primero que vamos a hacer es hacer ping entre los diferentes computadores para determinar si tenemos problemas de configuración.



   Revisamos y la ip se encuentra mal configurada

   Se le cambia la ip

   Se realizan de nuevo las pruebas

```
Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
```

Ya tenemos comunicación entre pc1 y pc2

Ahora verificamos la configuración del pc1 con sw1

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Después verificamos la comunicaion entre el pc1 y R1

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Realizo un ping del pc1 al pc4 y el equipo no responde

```
C:\>ping 192.168.11.11

Pinging 192.168.11.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.11.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Verificamos la información de pc4

Comparamos la dirección IP y está bien pero nos damos cuenta que la puerta de enlace esta incorrupta procedemos a corregirla

Verificamos realizando un ping del pc1 al pc4

```
C:\>ping 192.168.11.11

Pinging 192.168.11.11 with 32 bytes of data:

Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ahora realizamos un ping al pc3

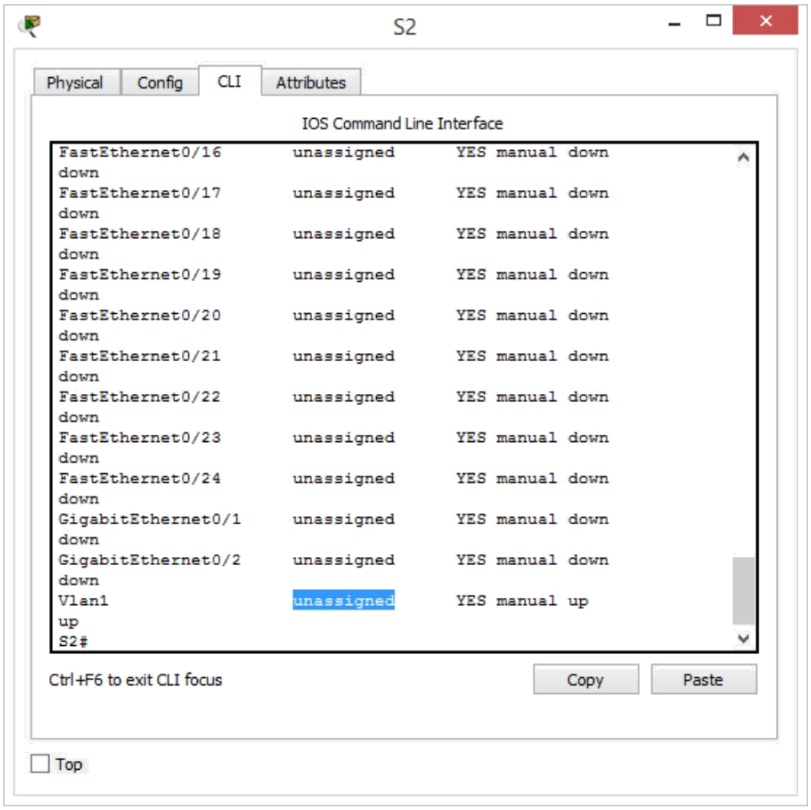
```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

El cual se realiza sin inconvenientes

Procedemos a verificar la coneccion entre el PC1 y S2haciendole ping a su dirección IP

```
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Como nos podemos dar cuenta no tienen comunicación asi que procedemos a mirar la configuración de S2

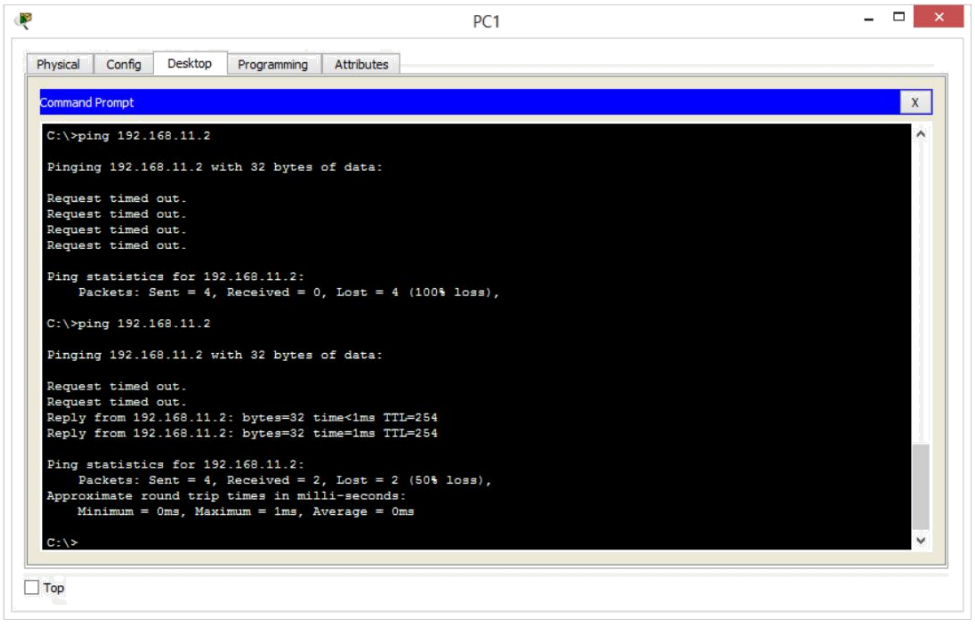



```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
ip default-gateway 192.168.11.1
!
```

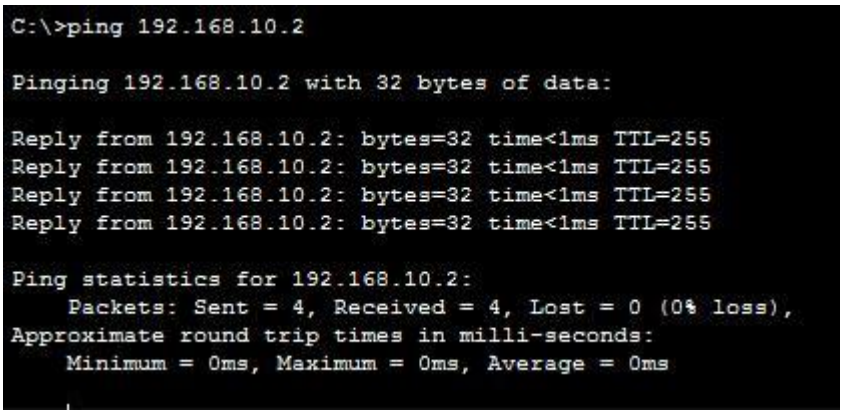
Nos damos cuneta que no tienemos una direecion asignada

```
S2#onfig t
         ^
% Invalid input detected at '^' marker.

S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.11.2 255.255.255.0
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

Le asignamos una dirección a S2 y realizamos las pruebas

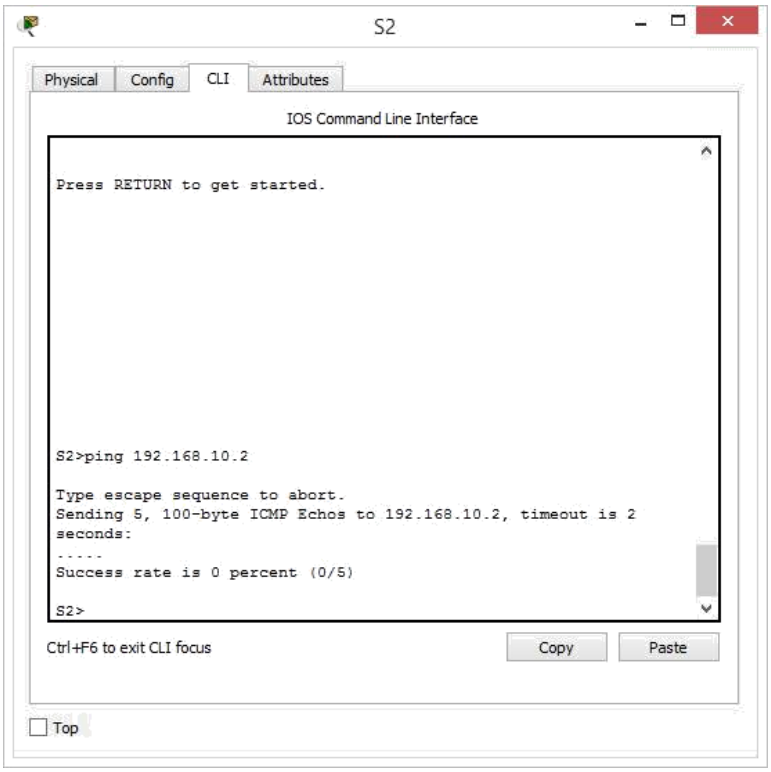


Como podemos ver ya tenemos comunicaion entre los dispositivos Ahora hacemos ping a S1



Y como podemos ver no tenemos inconvenientes

Ahroa vamos a revisar la comunicaion entre S2 y S1



Como podemos ver no tienen comunicación los dispositivos

Verificamos nuentro S2 par confirmar su dirección IP

```
down
GigabitEthernet0/2     unassigned      YES manual down
down
Vlan1                  192.168.11.2    YES manual up
up
S2>
```

Como esta bien configurado ingresamos al S1

```
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.10.2 255.255.255.0
!
 --More--
```

Y procedemos a colocarle la puerta de enlace para que puedan tener comunicaion los dispositvos

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.10.1
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Realizamos las pruebas para verificar la coneccion

```
S2>enable
S2#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1
ms
```

.

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**	si
PC1 a S1	si			si
PC1 a R1	si			si
PC1 a PC4	no	Puerta de enlace mal configurada	Se cambia la puerta de enlace	si
PC1 a PC3	si			si
PC1 a S2	no	Dirección IP no configurada	Se le configura la dirrecion IP	si
PC1 a S1	No	Puerta de enlace no configurada	Se le configura la puerta de enlace	si

EJERCICIO 2.4.1.2

Tabla de direccionamiento

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

Objetivos

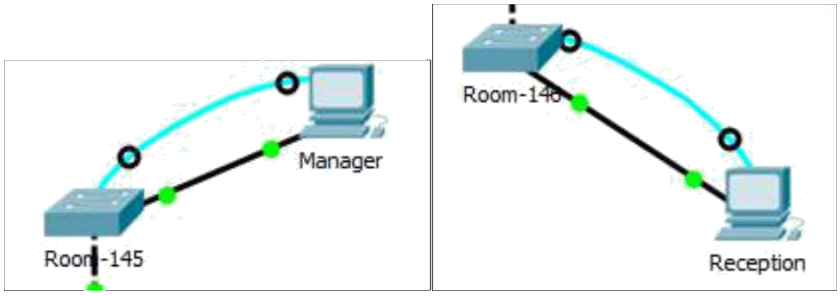
- Configurar los nombres de host y las direcciones IP en dos switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Usar los comandos de Cisco IOS para especificar o limitar el acceso a las configuraciones de los dispositivos.
- Utilizar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

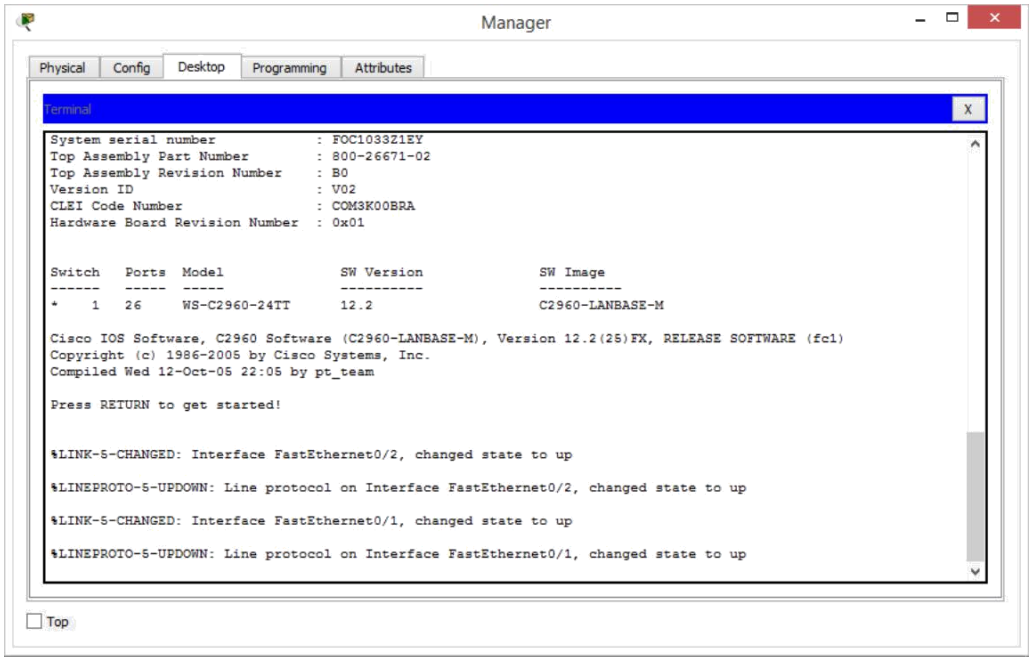
- Use una conexión de consola para acceder a cada switch.



- Nombre los switches **[[S1Name]]** y **[[S2Name]]**.

Para ingresar al switch lon primero que tenemos que hacer el ingresar al pc es desktop, terminal y presionamos el botón ok en la pantalla que aparece, para comenzar a configurar.

Los pantallazos se van a mostrar con el Room-145 pero se hace lo mismo con el Room-146




```
Switch>enable
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Room-145
Room-145(config)#
```

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

```
Room-145(config)#line console 0
Room-145(config-line)#pas
Room-145(config-line)#password R4Xe3
Room-145(config-line)#
```

- Use la contraseña secreta **[[SecretPW]]**.

```
Room-145(config)#enable secret C4aja
Room-145(config)#
```

- Encripte todas las contraseñas de texto no cifrado.
  - Room-145(config-line)#login
  - Room-145(config-line)#exit
  - Room-145(config)#
  - Room-145(config)#do show run
  - Building configuration...
  -

- Current configuration : 1182 bytes
- !
- version 12.2
- no service timestamps log datetime msec
- no service timestamps debug datetime msec
- no service password-encryption
- !
- hostname Room-145
- !
- enable secret 5 1mERr$7.2QH1ZQuchuwv7SrpgBm1
- !
- !
- !
- !
- !
- spanning-tree mode pvst
- spanning-tree extend system-id
- !
- interface FastEthernet0/1
- !
- interface FastEthernet0/2
- !
- interface FastEthernet0/3
- !
- interface FastEthernet0/4
- !
- interface FastEthernet0/5
- !
- interface FastEthernet0/6
- !
- interface FastEthernet0/7
- !
- interface FastEthernet0/8
- !
- interface FastEthernet0/9
- !
- interface FastEthernet0/10
- !
- interface FastEthernet0/11
- !
- interface FastEthernet0/12
- !
- interface FastEthernet0/13
- !
- interface FastEthernet0/14
- !
- interface FastEthernet0/15

- !
- interface FastEthernet0/16
- !
- interface FastEthernet0/17
- !
- interface FastEthernet0/18
- !
- interface FastEthernet0/19
- !
- interface FastEthernet0/20
- !
- interface FastEthernet0/21
- !
- interface FastEthernet0/22
- !
- interface FastEthernet0/23
- !
- interface FastEthernet0/24
- !
- interface GigabitEthernet0/1
- !
- interface GigabitEthernet0/2
- !
- interface Vlan1
- no ip address
- shutdown
- !
- !
- !
- !
- line con 0
- password R4Xe3
- login
- !
- line vty 0 4
- password R4Xe3
- login
- line vty 5 15
- password R4Xe3
- login
- !
- !
- !
- end
-
-
- Room-145(config)#se

- Room-145(config)#service pa
- Room-145(config)#service password-encryption
- Room-145(config)#do show run
- Building configuration...
-
- Current configuration : 1206 bytes
- !
- version 12.2
- no service timestamps log datetime msec
- no service timestamps debug datetime msec
- service password-encryption
- !
- hostname Room-145
- !
- enable secret 5 1mERr$7.2QH1ZQuchuwv7SrpgBm1
- !
- !
- !
- !
- !
- spanning-tree mode pvst
- spanning-tree extend system-id
- !
- interface FastEthernet0/1
- !
- interface FastEthernet0/2
- !
- interface FastEthernet0/3
- !
- interface FastEthernet0/4
- !
- interface FastEthernet0/5
- !
- interface FastEthernet0/6
- !
- interface FastEthernet0/7
- !
- interface FastEthernet0/8
- !
- interface FastEthernet0/9
- !
- interface FastEthernet0/10
- !
- interface FastEthernet0/11
- !
- interface FastEthernet0/12
- !

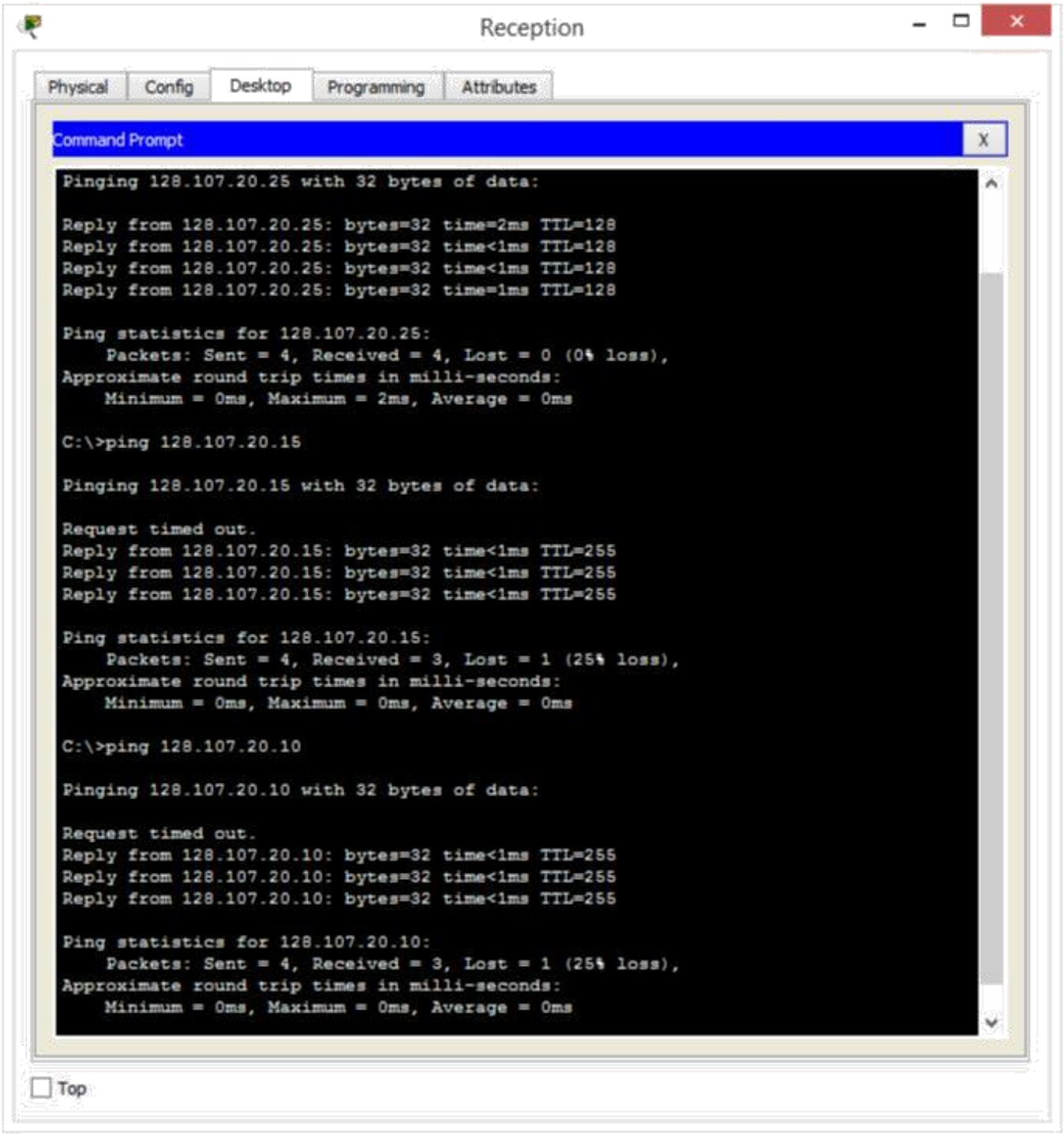
```
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password 7 081318760C4A
login
!
line vty 0 4
password 7 081318760C4A
login
line vty 5 15
password 7 081318760C4A
login
!
!
```

- !
- end

- Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).
  - Room-145(config)#ban
  - Room-145(config)#banner m
  - Room-145(config)#banner motd #
  - Enter TEXT message. End with the character '#'.
  - WARNING
  - #
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
  - Room-145(config)#int vlan 1
  - Room-145(config-if)#ip add
  - Room-145(config-if)#ip address 128.107.20.10 255.255.255.0
  - Room-145(config-if)#
- Guarde las configuraciones.
  - Room-145(config-if)#no shutdown
  -
  - Room-145(config-if)#
  - %LINK-5-CHANGED: Interface Vlan1, changed state to up
  -

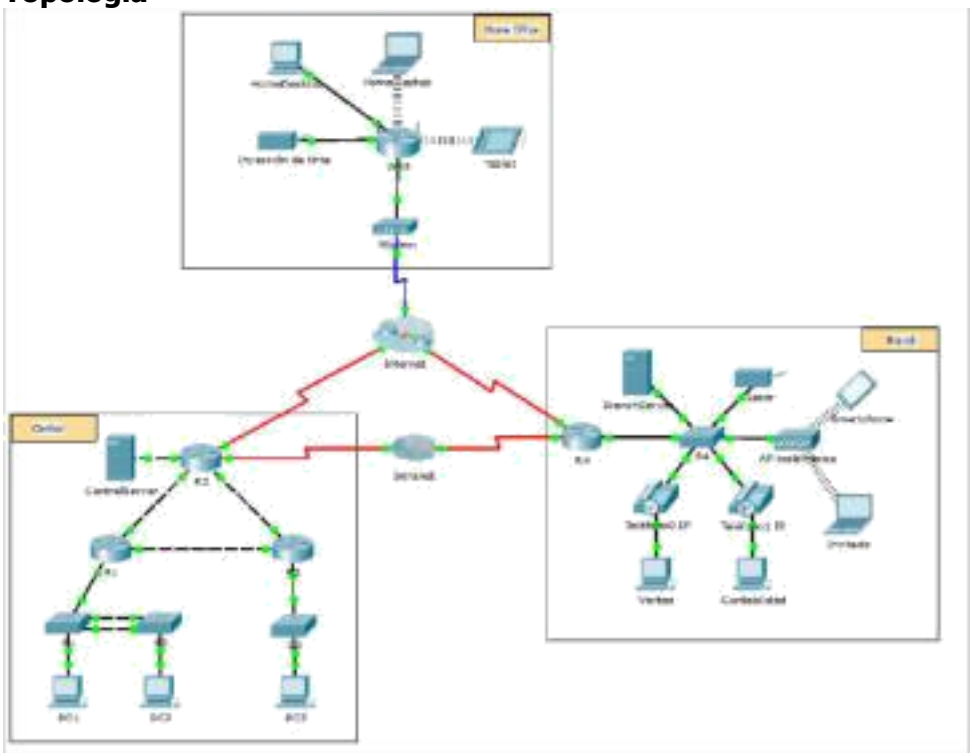
  •%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
- Verifique la conectividad entre todos los dispositivos.

  Se realiza un ping a todos los dispositivos para verificar la coneccion con los demás dispositivos.


Reception
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Pinging 128.107.20.25 with 32 bytes of data:
Reply from 128.107.20.25: bytes=32 time=2ms TTL=128
Reply from 128.107.20.25: bytes=32 time<1ms TTL=128
Reply from 128.107.20.25: bytes=32 time<1ms TTL=128
Reply from 128.107.20.25: bytes=32 time=1ms TTL=128
Ping statistics for 128.107.20.25:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>ping 128.107.20.15
Pinging 128.107.20.15 with 32 bytes of data:
Request timed out.
Reply from 128.107.20.15: bytes=32 time<1ms TTL=255
Reply from 128.107.20.15: bytes=32 time<1ms TTL=255
Reply from 128.107.20.15: bytes=32 time<1ms TTL=255
Ping statistics for 128.107.20.15:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 128.107.20.10
Pinging 128.107.20.10 with 32 bytes of data:
Request timed out.
Reply from 128.107.20.10: bytes=32 time<1ms TTL=255
Reply from 128.107.20.10: bytes=32 time<1ms TTL=255
Reply from 128.107.20.10: bytes=32 time<1ms TTL=255
Ping statistics for 128.107.20.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Top

Punto. 3.3.3.3

Topología

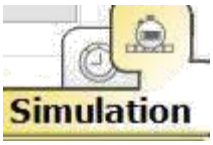


Objetivos
Parte 1: Examinar el tráfico de internetwork en la sucursal
Parte 2: Examinar el tráfico de internetwork a la central
Parte 3: Examinar el tráfico de Internet desde la sucursal

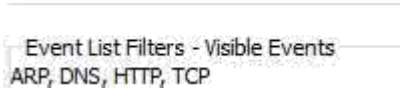
Información básica
El objetivo de esta actividad de simulación es ayudarlo a comprender el flujo de tráfico y el contenido de los paquetes de datos a medida que atraviesan una red compleja. Las comunicaciones se examinarán en tres ubicaciones distintas que simulan redes comerciales y domésticas típicas.
Tómese unos minutos para analizar la topología que se muestra. La ubicación Central tiene tres routers y varias redes que posiblemente representen distintos edificios dentro de un campus. La ubicación Branch (Sucursal) tiene solo un router con una conexión a Internet y una conexión dedicada de red de área extensa (WAN) a la ubicación Central. La Home Office (Oficina doméstica) utiliza una conexión de banda ancha con módem por cable para proporcionar acceso a Internet y a los recursos corporativos a través de Internet.
Los dispositivos en cada ubicación utilizan una combinación de direccionamiento estático y dinámico. Los dispositivos se configuran con gateways predeterminados y con información del Sistema de nombres de dominios (DNS), según corresponda.

Parte 1: Examinar el tráfico de internetwork en la sucursal
En la parte 1 de esta actividad, utilizará el modo de simulación para generar tráfico Web y examinar el protocolo HTTP junto con otros protocolos necesarios para las comunicaciones.

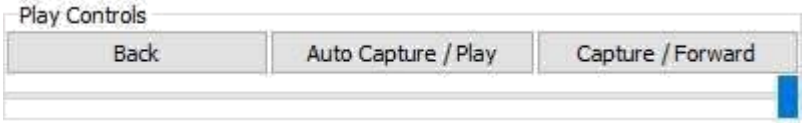
Paso 1: Cambiar del modo de tiempo real al modo de simulación a. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.



b. Verifique que **ARP, DNS, HTTP** y **TCP** estén seleccionados en **Event List Filters** (Filtros de lista de eventos).



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



Paso 2: Generar tráfico mediante un explorador Web
El panel de simulación actualmente está vacío. En Event List (Lista de eventos), en la parte superior del panel de simulación, hay seis columnas en el encabezado. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el contenido de un evento determinado.

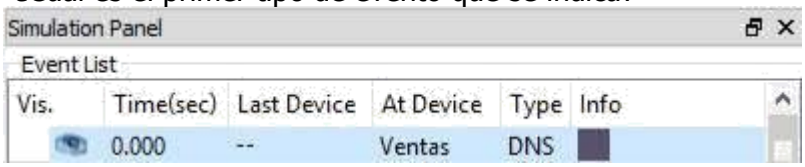
Nota: la topología se muestra en el panel de la izquierda del panel de simulación. Utilice las barras de desplazamiento para incorporar la ubicación Branch al panel, en caso necesario. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la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

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

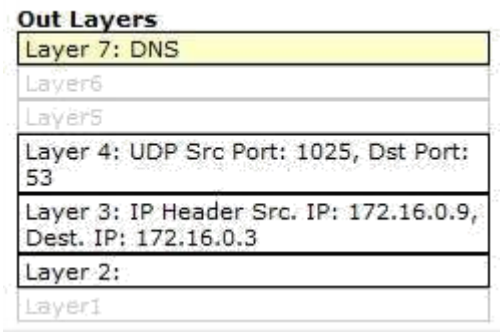
b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.

c. En el campo de dirección URL, introduzca **http://branchserver.pt.pta** y haga clic en **Go** (Ir).

Observe la lista de eventos en el panel de simulación.
¿Cuál es el primer tipo de evento que se indica?



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?

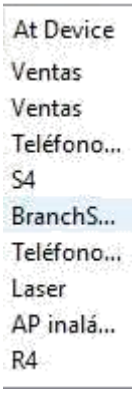
Layer 2:

La dirección MAC de destino.

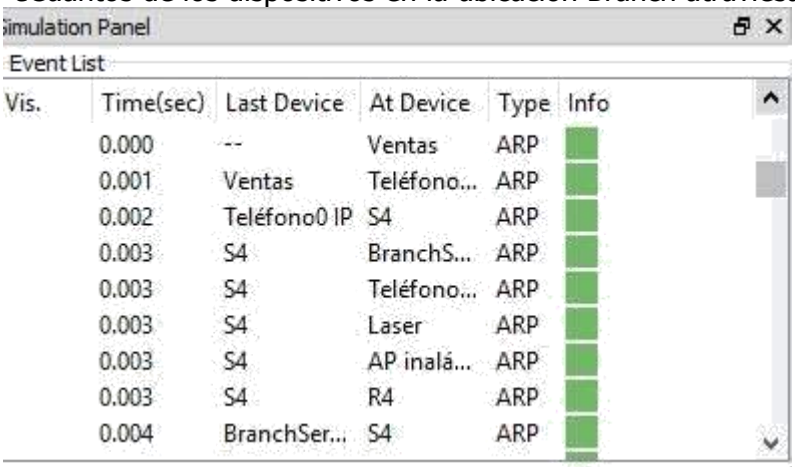
e. Haga clic en **Auto Capture/Play**.

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:

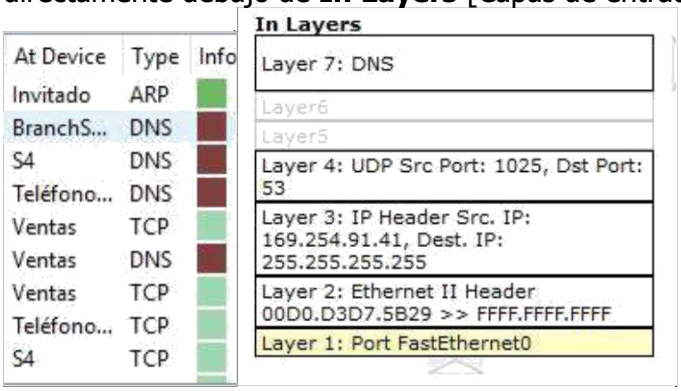


¿Cuántos de los dispositivos en la ubicación Branch atraviesa la solicitud de **ARP**?



Todos los dispositivos recibieron una solicitud de ARP.

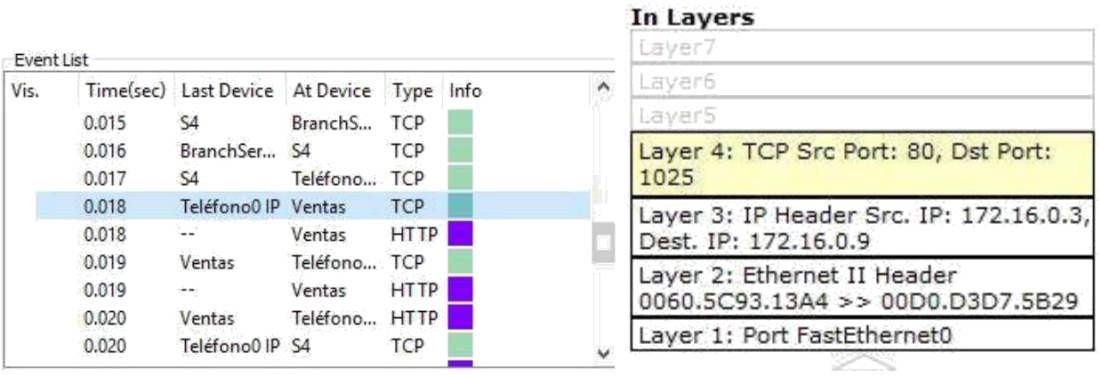
f. Desplácese por los eventos en la lista hasta la serie de eventos de **DNS**. Seleccione el evento de **DNS** para el que se indica **BranchServer** en At Device (En el dispositivo). Haga clic en el cuadro de la columna **Info**. ¿Qué se puede determinar seleccionando la capa 7 en **OSI Model** (Modelo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

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**:

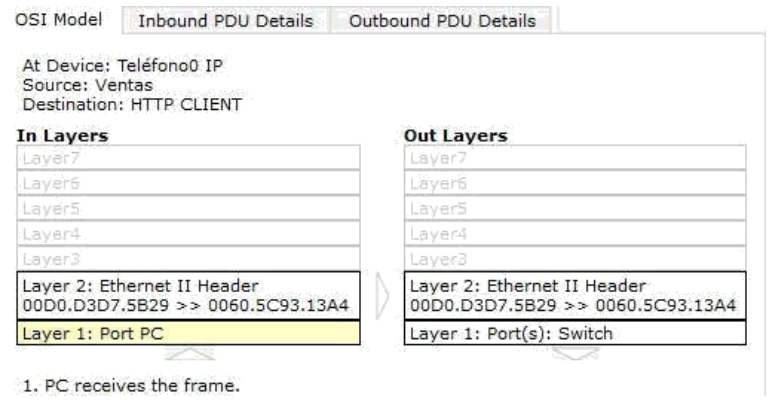


¿Cuál es el estado de la conexión?

1. The device receives a TCP SYN+ACK segment on the connection to 172.16.0.3 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.

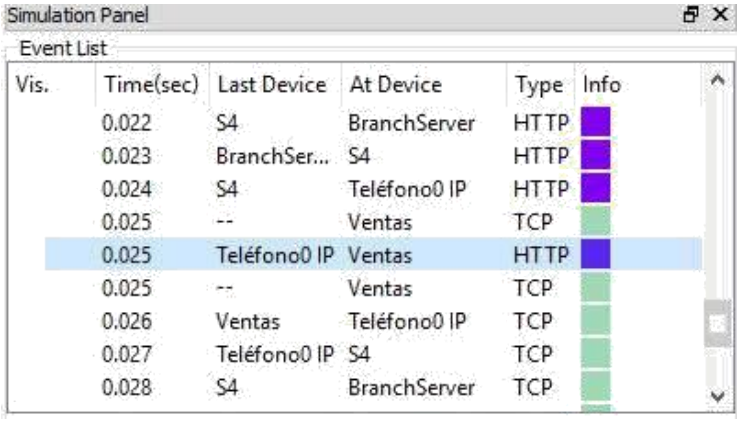
i. Los eventos siguientes son eventos de **HTTP**. Seleccione cualquiera de los eventos de **HTTP** en un dispositivo intermediario (teléfono IP o switch).

¿Cuántas capas están activas en uno de estos dispositivos y por qué?

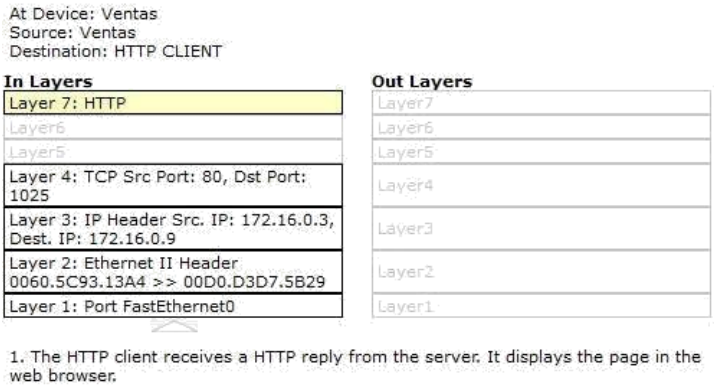


2 capas, porque son dispositivos de capa 2.

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**?



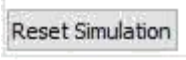
Parte 2: Examinar el tráfico de internetwork a la central

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

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

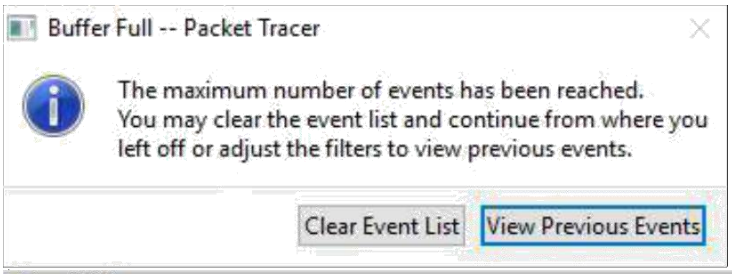
a. Cierre todas las ventanas de información de PDU abiertas.

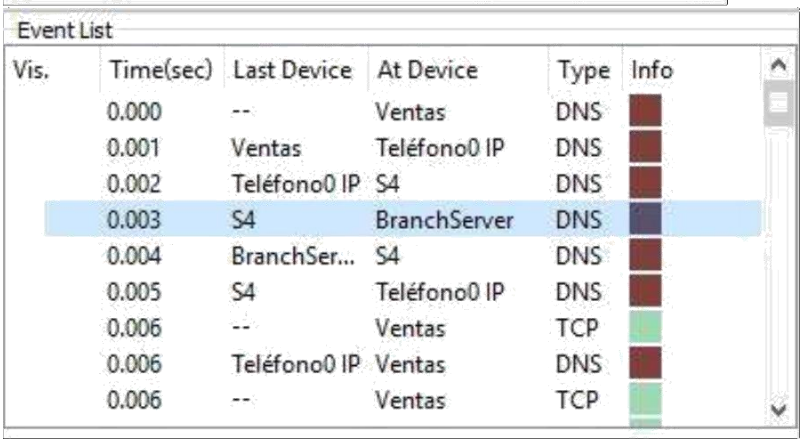
b. Haga clic en la opción **Reset Simulation** (Restablecer simulación), que se encuentra cerca del centro del panel de simulación.



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

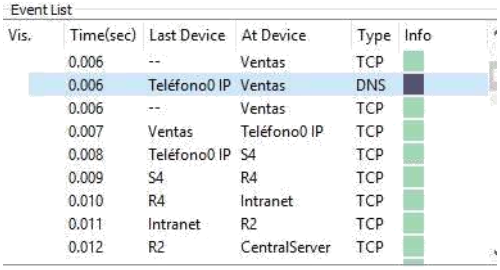
d. Haga clic en **Auto Capture/Play** (Captura/reproducción automática). En aproximadamente 75 segundos, aparece una ventana que indica la finalización de la simulación actual. Haga clic en **View Previous Events** (Ver eventos anteriores). Vuelva a desplazarse hasta la parte superior de la lista; observe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



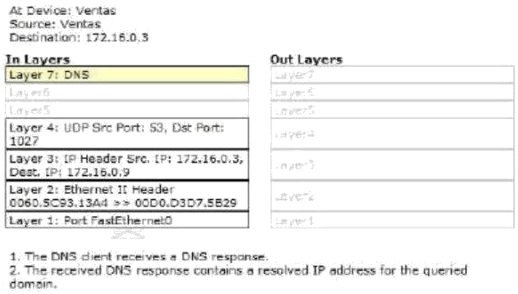


R// PC Ventas ya conoce la dirección MAC del servidor DNS.

e. Haga clic en el último evento de DNS en la columna **Info**. Seleccione **Layer 7** (Capa 7) en la ficha **OSI Model**.

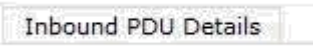


¿Qué se puede determinar sobre los resultados de DNS?

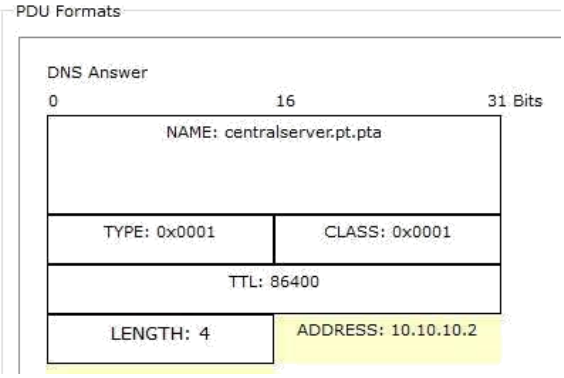


Que el servidor DNS pudo resolver el nombre de dominio para centralserver.pt.pta.

f. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante).

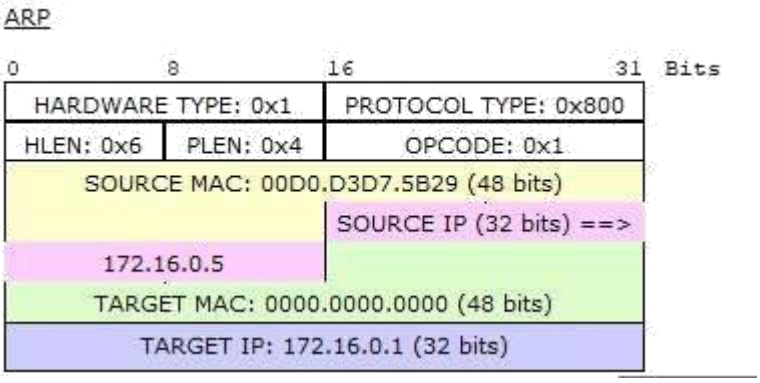


Desplácese hasta la sección **DNS ANSWER** (RESPUESTA DE DNS). ¿Cuál es la dirección que se indica para centralserver.pt.pta? 10.10.10.2.



R// 10.10.10.2

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



¿Qué dispositivo proporciona la respuesta de ARP?

R//El router R4, el dispositivo de gateway.

At Device	Type	Info
Ventas	DNS	
Ventas	ARP	
Teléfono0 IP	ARP	
S4	ARP	
BranchServer	ARP	
Teléfono1 IP	ARP	
Laser	ARP	
AP inalámb...	ARP	
R4	ARP	

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

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.016	R4	S4	TCP	
	0.017	S4	Teléfono...	TCP	
	0.018	Teléfono0 IP	Ventas	TCP	
	0.018	--	Ventas	HTTP	
	0.019	Ventas	Teléfono...	TCP	
	0.019	--	Ventas	HTTP	
	0.020	Ventas	Teléfono...	HTTP	
	0.020	Teléfono0 IP	S4	TCP	
	0.021	Teléfono0 IP	S4	HTTP	

PDU Information at Device: Ventas

OSI Model | Outbound PDU Details

At Device: Ventas
Source: Ventas
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1027, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 172.16.0.12, Dest. IP: 10.10.10.2
Layer2	Layer 2: Ethernet II Header 00D0.D3D7.5B29 >> 000A.F3E4.EB01
Layer1	Layer 1: Port(s):

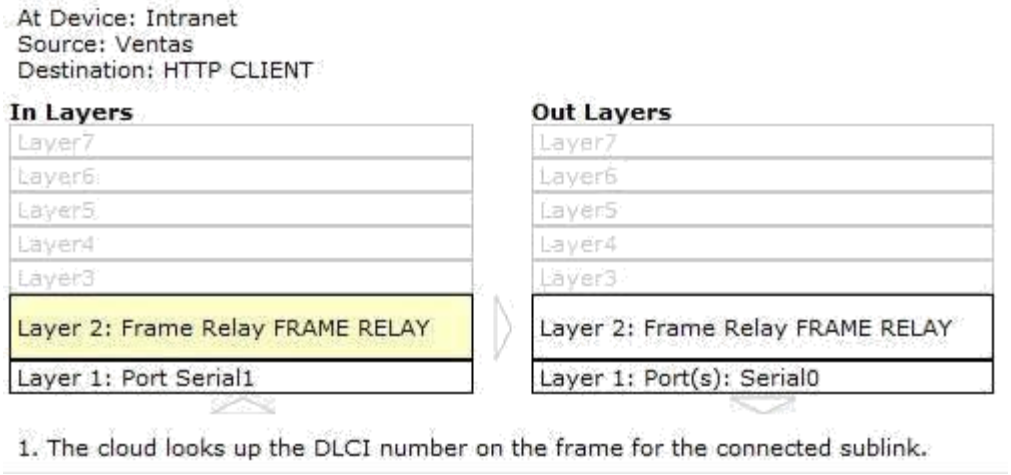
1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. The device encapsulates the PDU into an Ethernet frame.

¿Qué se puede determinar sobre la dirección MAC de destino?

R// tiene la misma dirección MAC del Router 4 (R4)

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

R// 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.

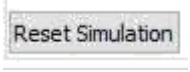
Parte 3: Examinar el tráfico de Internet desde la sucursal

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.

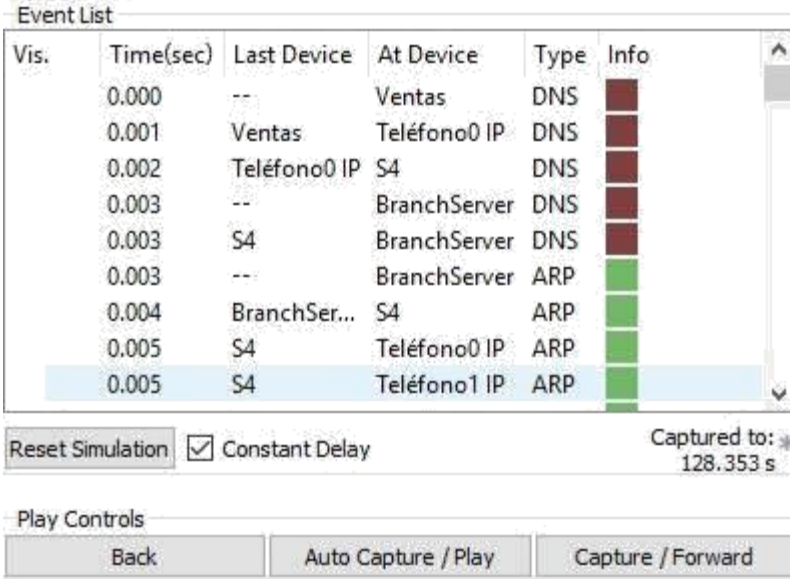


Escriba **http://www.netacad.pta** en el explorador Web de Sales PC.

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

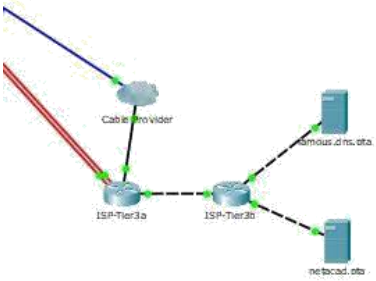
desplazarse hasta la parte superior de la lista; observe que la primera serie de eventos es **DNS**. ¿Qué advierte sobre la cantidad de eventos de **DNS**?

R// 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?

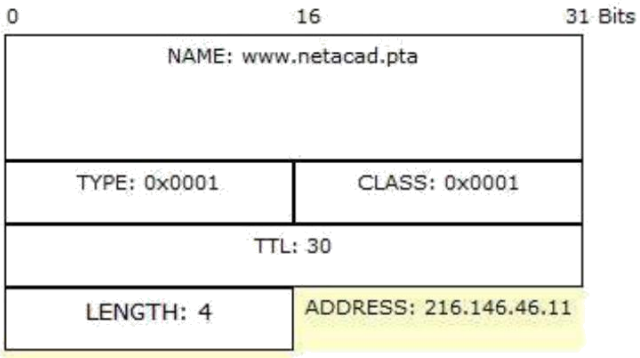
R// En la nube de Internet.



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**?

R// 216.146.46.11

DNS Answer



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?

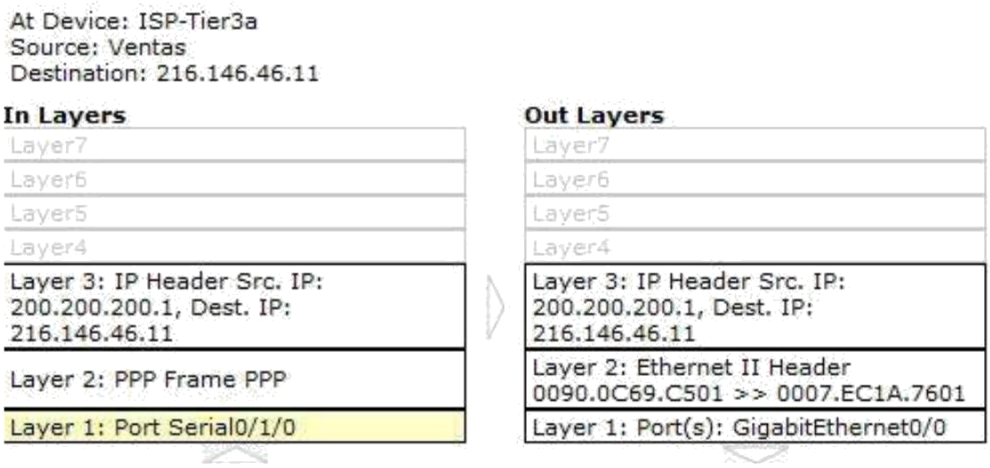
R// Hay tres routers (ISP-Tier3a, ISP-Tier3b y R4); sin embargo, hay cuatro eventos de HTTP que los atraviesan.

Event List

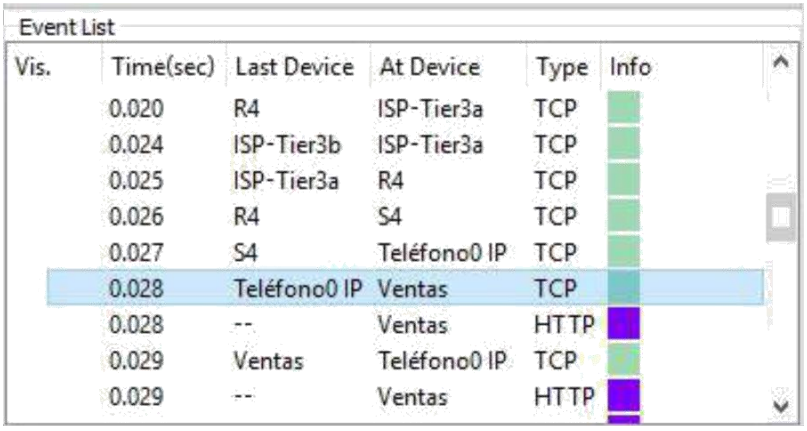
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.030	Ventas	Teléfono0 IP	HTTP	
	0.030	Teléfono0 IP	S4	TCP	
	0.031	Teléfono0 IP	S4	HTTP	
	0.031	S4	R4	TCP	
	0.032	S4	R4	HTTP	
	0.032	R4	ISP-Tier3a	TCP	
	0.033	R4	ISP-Tier3a	HTTP	
	0.037	ISP-Tier3b	ISP-Tier3a	HTTP	
	0.038	ISP-Tier3a	R4	HTTP	

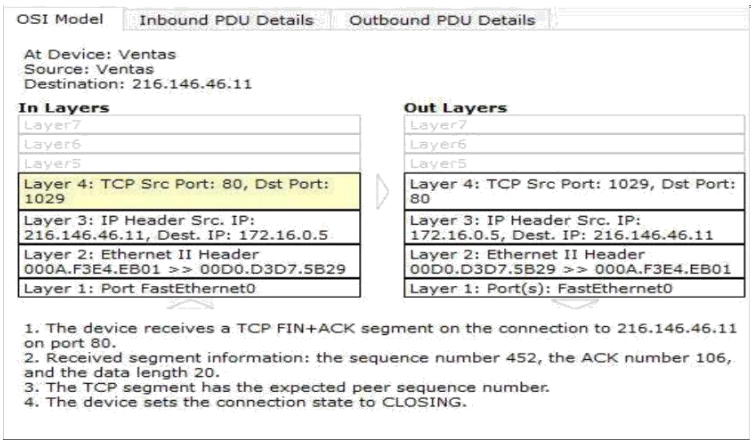
g. Haga clic en el evento de **TCP** anterior al último evento de **HTTP**. Según la información que se muestra, ¿cuál es el propósito de este evento?

R// 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?
R// CLOSING



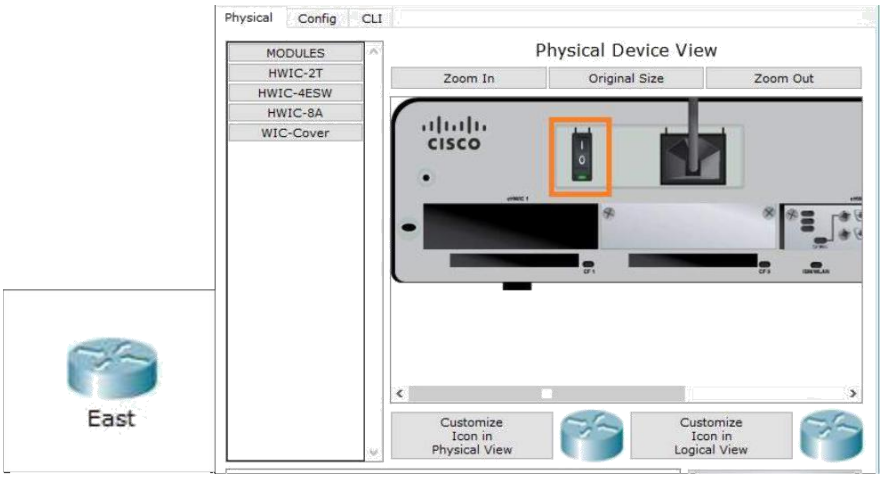


Punto. 6.3.1.10

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.

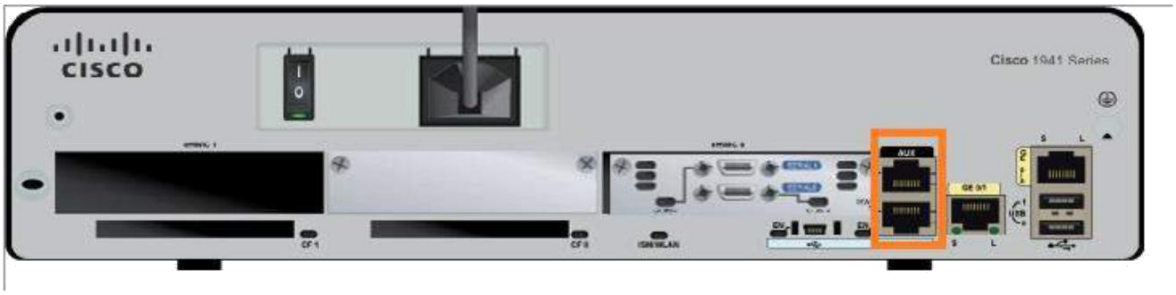


b. Acerque el elemento y expanda la ventana para ver todo el router.

c. ¿Qué puertos de administración se encuentran disponibles?

R//

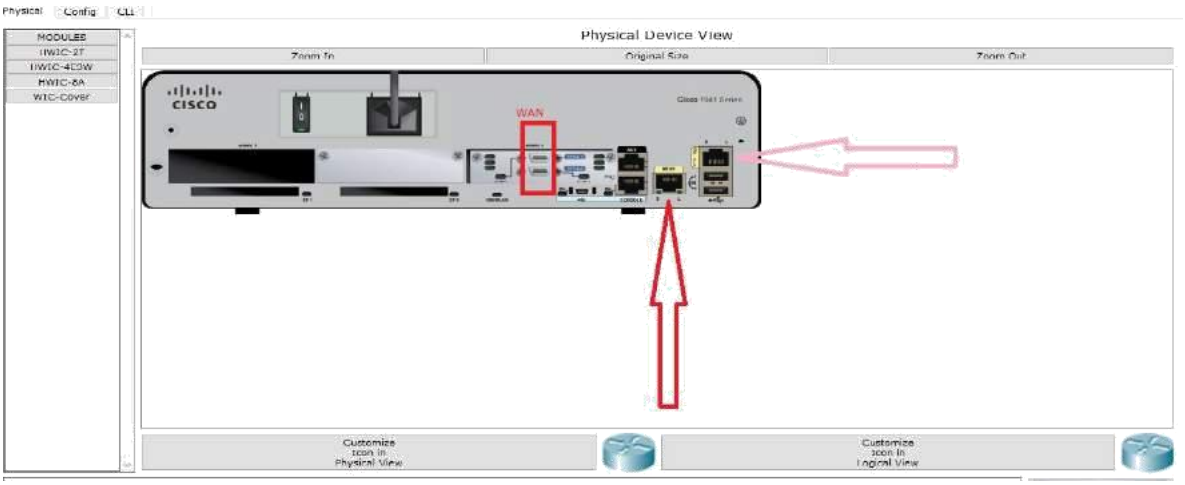
Consola y auxiliar.



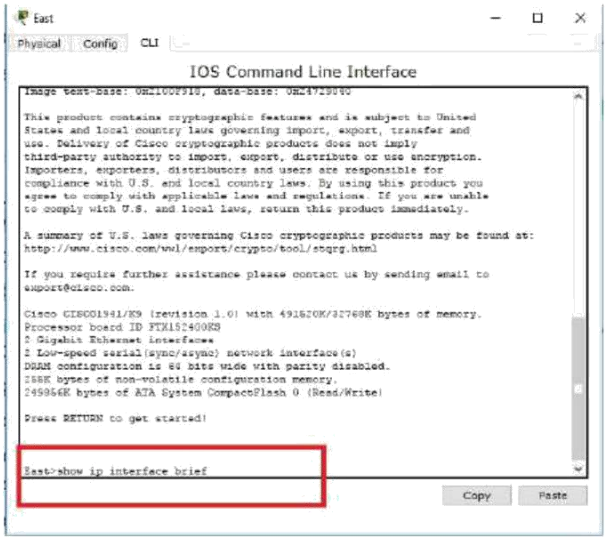
Paso 2: Identificar las interfaces LAN y WAN de un router Cisco

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

R// 1 interface Wan de dos puertos y 2 Gigabit Ethernet.

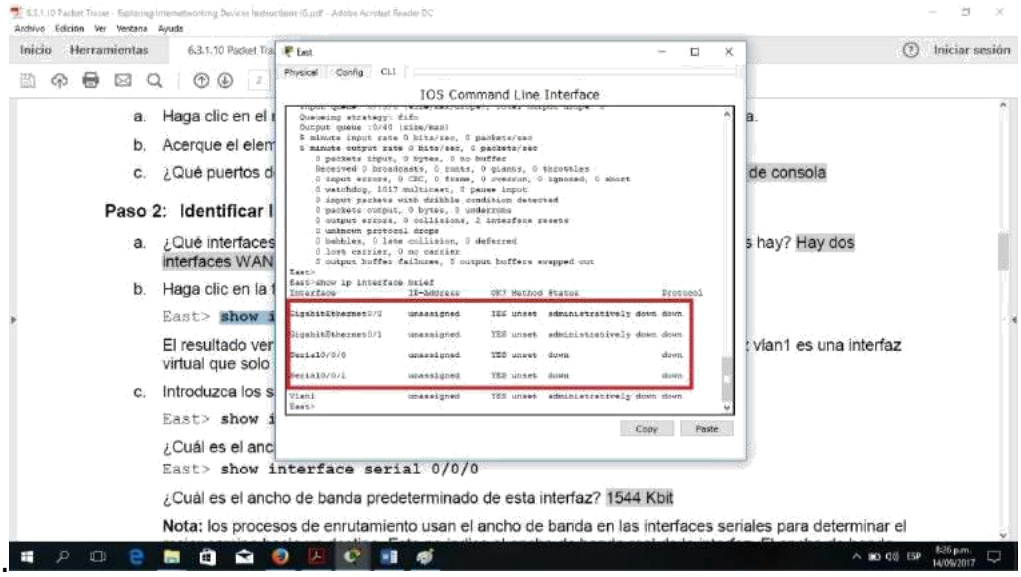


Haga clic en la ficha **CLI** e introduzca los siguientes comandos:
East> **show ip interface brief**



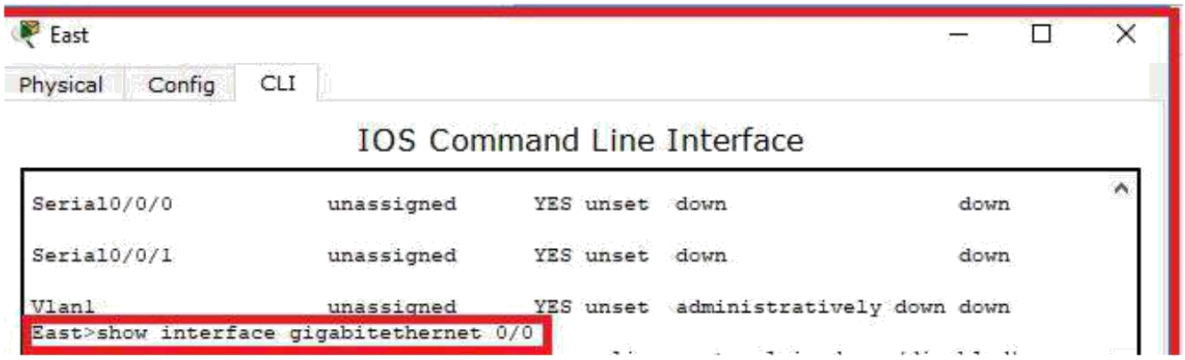
El resultado verifica la cantidad correcta de interfaces y su designación. La interfaz vlan1 es una interfaz virtual que solo existe en el software. ¿Cuántas interfaces físicas se indican?

R// 4.



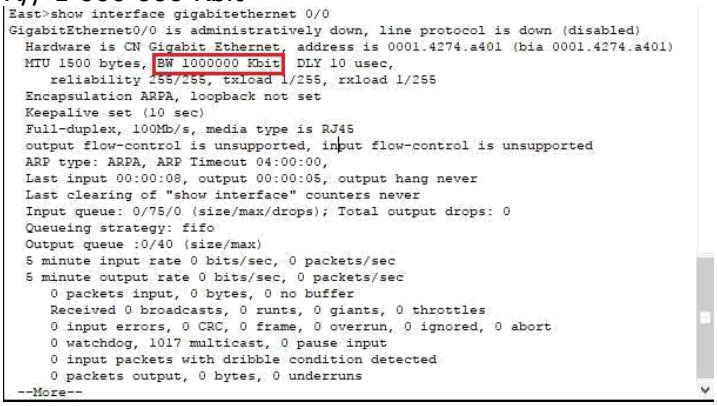
b. Introduzca los siguientes comandos:

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

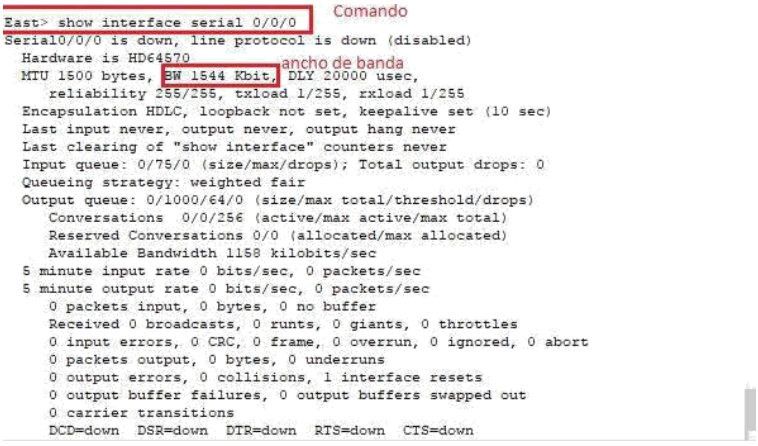


¿Cuál es el ancho de banda predeterminado de esta interfaz?

R// 1 000 000 Kbit



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



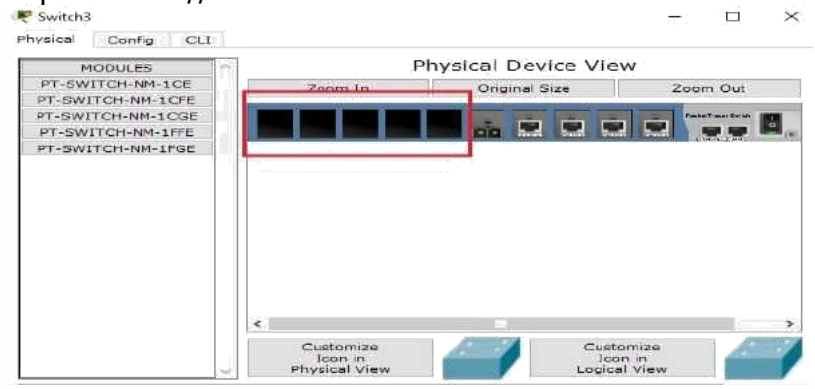
Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar el mejor camino hacia un destino. Esto no indica el ancho de banda real de la interfaz. El ancho de banda real se negocia con un proveedor de servicios.

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**?

R// una. (1)

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



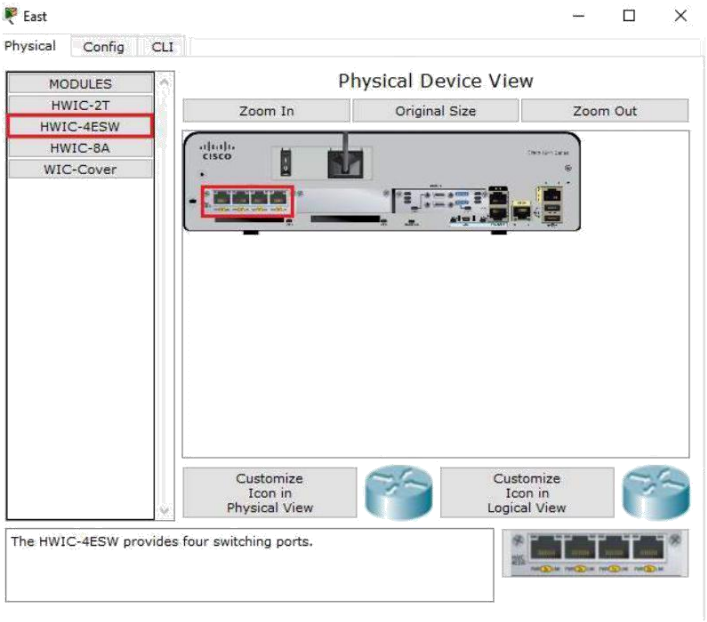
Parte 2: Seleccionar los módulos correctos para la conectividad
Paso 1: Determinar qué módulos proporcionan la conectividad requerida

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

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

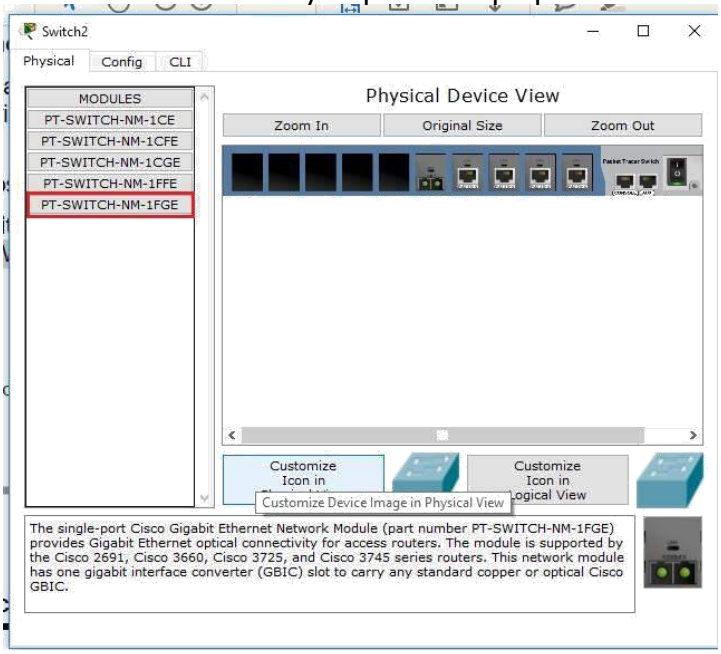
b. Debe conectar las PC 1, 2 y 3 al router **East**, pero no cuenta con los fondos necesarios para adquirir un nuevo switch. ¿Qué módulo puede usar para conectar las tres PC al router **East**?

R//
Módulo HWIC-4ESW



¿Cuántos hosts puede conectar al router mediante este módulo?
R// 4.

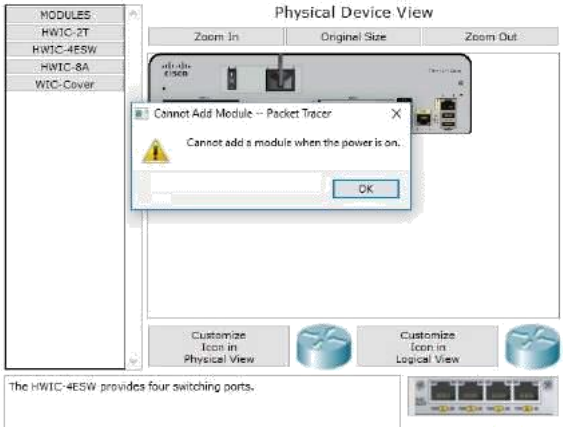
Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**?
R//
PT-SWITCH-NM-1FGE ya que este proporciona conectividad óptica Gigabits Ethernet.



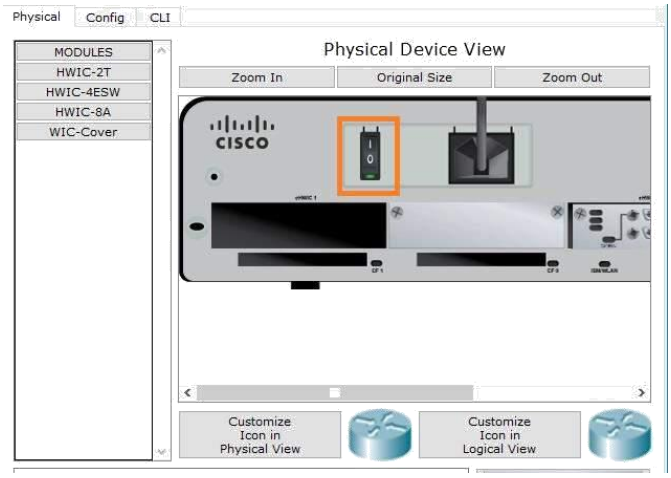
Paso 2: Agregar los módulos correctos y encender los dispositivos

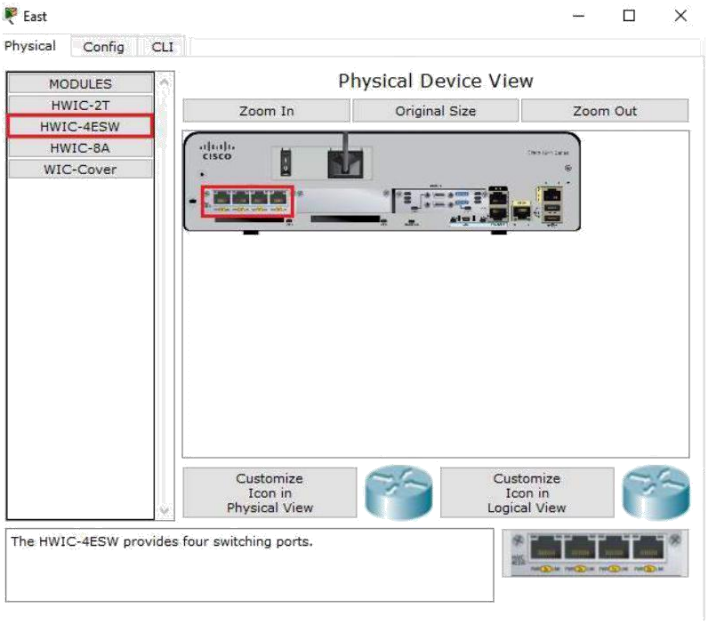
a. Haga clic en **East** e intente insertar el módulo adecuado del paso 1a.

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**.



Apagamos.

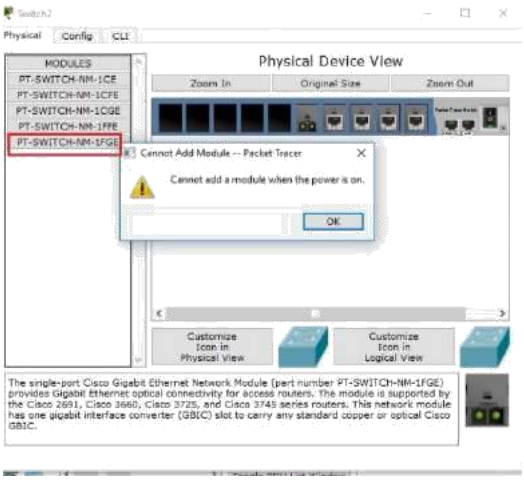




Nota: si inserta el módulo incorrecto y debe quitarlo, arrastre el módulo hasta su imagen en la esquina inferior derecha y suelte el botón del mouse.

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**.

R// Switch2.

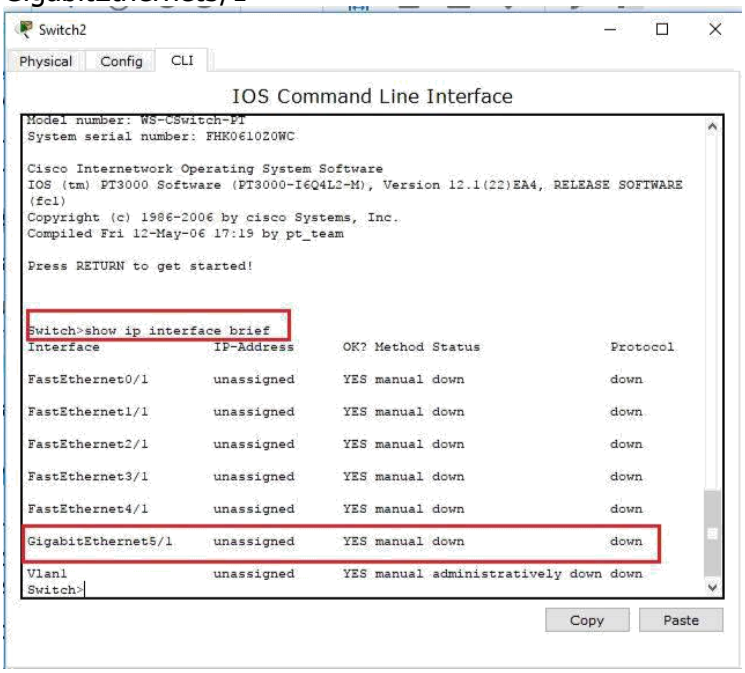


Agregado.

R// Switch 3.

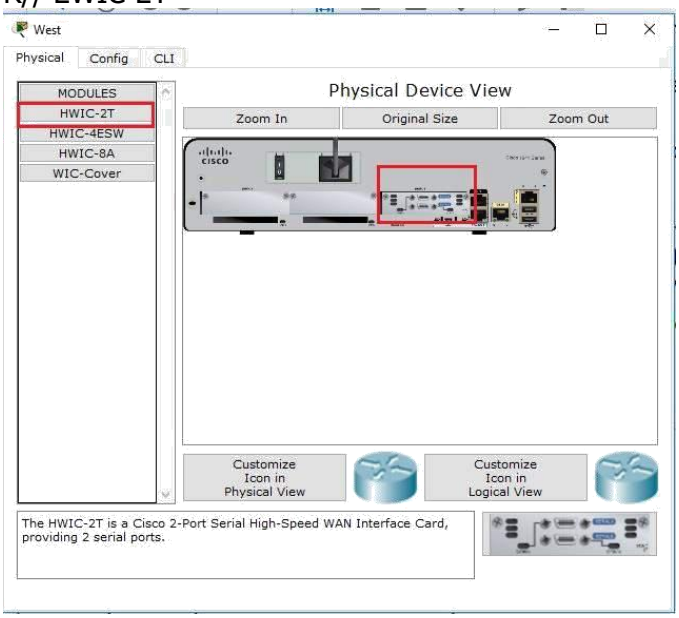
d. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo. ¿En qué ranura se insertó?

GigabitEthernet5/1

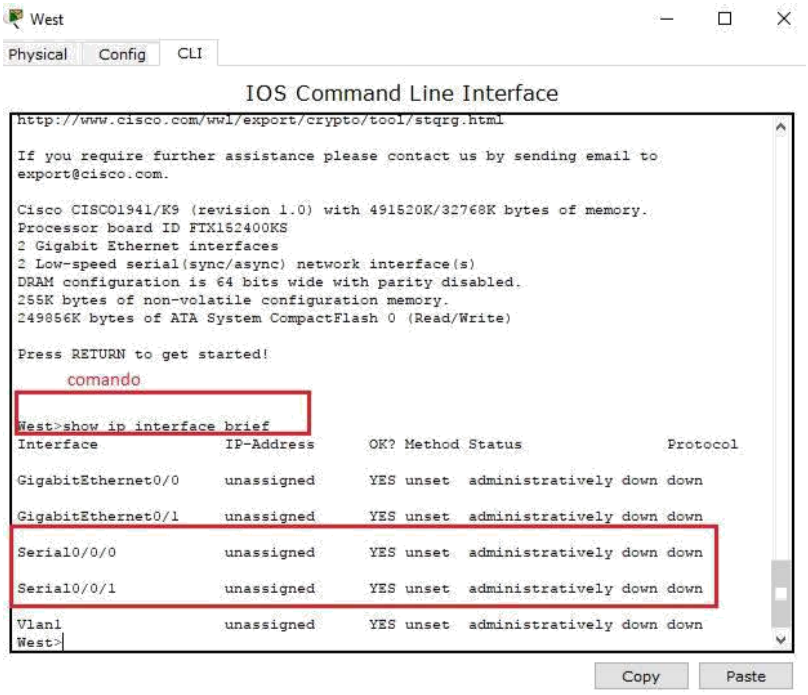


e. Haga clic en el router **West** (Oeste). La ficha **Physical** (Capa física) debe estar activa. Instale el módulo adecuado que agregará una interfaz serial a la ranura para tarjetas de interfaz WAN de alta velocidad mejoradas (**EHWIC 0**) de la derecha. Puede cubrir las ranuras sin utilizar para evitar que ingrese polvo al router (optativo).

R// EWIC-2T



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

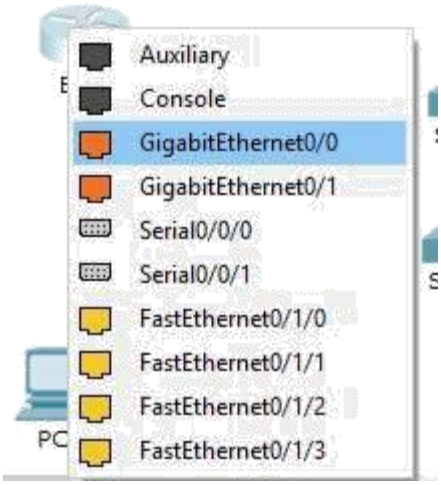


Parte 3: Conectar los dispositivos

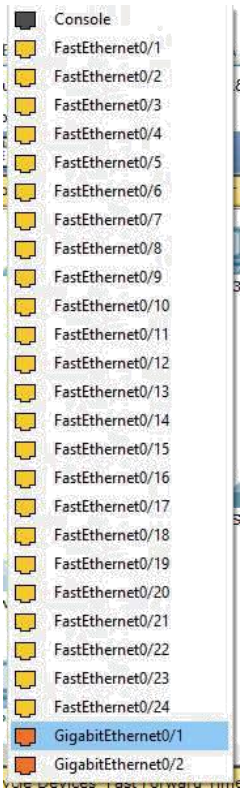
Esta puede ser la primera actividad que realiza en la que se le solicita conectar dispositivos. Si bien es posible que no conozca el propósito de los distintos tipos de cables, use la tabla que se encuentra a continuación y siga estas pautas para conectar correctamente todos los dispositivos:
a. Seleccione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

R// conexión de EAST y Switch 1

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



c. Haga clic en el segundo dispositivo y seleccione la interfaz especificada.
SWITCH 1



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

CONCLUSIONES

- Se sabe de los dispositivos básicos LAN, la respectiva configuración, gestión de una red de datos.

- Con la elaboración de este documento, se comprende cómo se transmiten los datos a través de los medios físicos de transmisión como medios guiados y no guiados, identificando cuales se deben utilizar en un caso determinado.

- El diseño de red se ha vuelto cada vez más difícil a pesar de los avances que se han logrado a nivel del rendimiento de los equipos y las capacidades de los medios. El uso de distintos tipos de medios y de las LAN que se interconectan con otras redes agrega complejidad al entorno de red. Los buenos diseños de red permiten mejorar el rendimiento y reducir las dificultades asociadas con el crecimiento y la evolución de la red.

BIBLIOGRAFÍA

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-courseassets.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#6.0.1.1

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: https://cdn2.hubspot.net/hub/280690/file270025813-pdf//ICND1.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de: http://gonda.nic.in/swangonda/pdf/ccna1.pdf