DIPLOMADO DE PROFUNDIZACION CISCO
RESUMEN DE ACTIVIDADES COLABORATIVAS

ENTREGADO POR:
INGRID YALILE RODRIGUEZ

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA SISTEMAS
CEAD IBAGUE-TOLIMA
2018

DIPLOMADO DE PROFUNDIZACION CISCO
RESUMEN DE ACTIVIDADES COLABORATIVAS

ENTREGADO POR:

INGRID YALILE RODRIGUEZ

TUTOR:
NILSON ALBEIRO FERREIRA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA SISTEMAS
CEAD IBAGUE-TOLIMA
2018

INTRODUCCION

Mediante la realización del presente trabajo colaborativo se pretende realizar una conceptualización general de las temáticas desarrolladas en las dos unidades trabajadas, (Introducción a las Redes y Principios básicos de routing y switching) Fundamentos de Networking, del Diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integradas lan / wan), a la vez que se desarrollan una serie de actividades prácticas mediante la herramienta de simulación Packet Tracer según sea requerido. Las temáticas a tratar en este momento de evaluación corresponden a, Exploración de la red, Configuración de un sistema operativo de red, Protocolos y comunicaciones de red, Acceso a la red, Ethernet y finalmente, Capa de red.

Cabe destacar la importancia de reconocer el funcionamiento de las redes computacionales su aplicabilidad de acuerdo a las necesidades o parámetros, elección de mejor topología de red, de acuerdo a lo requisitos de solicitud, ya sea WAN o LAN. Sin lugar a duda el aprendizaje sobre configuración de Routers, Switch, Servidores y demás componentes de una red, por medio de comandos, el conocer la diferentes capas de del modelo OSI y TCP/IP, el Subnetting para poder realizar la segmentación de la red de acuerdo al direccionamiento IP y demás conocimientos que se adquieren por medio de este diplomado de CISCO se consideran de suma importancia para el desarrollo integral de nuestra formación como futuros ingenieros de Sistemas.

A continuación se presenta un resumen de las actividades realizadas de los procesos de configuración de dispositivos de Networking acorde con las indicaciones establecidas en cada una de las tareas.

OBJETIVOS.

Objetivos General:

- Evidenciar las actividades realizadas durante el proceso de formación del Diplomado en Cisco

Objetivos Específicos:

- Conceptualizar la temática planteada en las dos unidades del curso de profundización.
- Aplicar dichas temáticas en cada uno de los ejercicios propuestos.
- Utilizar la herramienta de simulación Packet Tracer de acuerdo a requisitos establecidos.

DESARROLLO DE LA ACTIVIDAD.

DESARROLLO DE ALGUNAS DE LAS TAREAS PRÁCTICAS PROPUESTAS EN LA UNIDAD 1

Ejercicio 2.4.1.2 Packet Tracer - Skills Integration Challenge Instructions

Packet Tracer: Reto de habilidades de integración

Tabla dedireccionamiento

Dispositivo	Interfaz	DirecciónIP	Máscara de subred
[[S1Name]]	VLAN1	[[S1Add]]	255.255.255.0
[[S2Name]]	VLAN1	[[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 demuestresu habilidadparaconfigurarunaLANpequeña.Sustareasincluyenlaconfiguracióñdeparámetrosinicialesen dosswitchesmedianteCiscoIOSylaconfiguracióñdeparámetrosdedireccióñIPendispositivoshostpara proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en unared

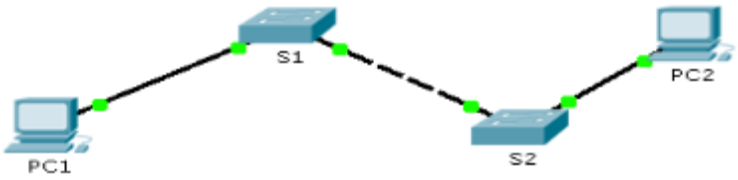
conectada por cable y conalimentación.

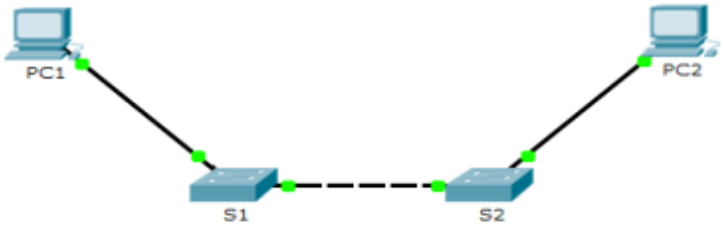
Requisitos

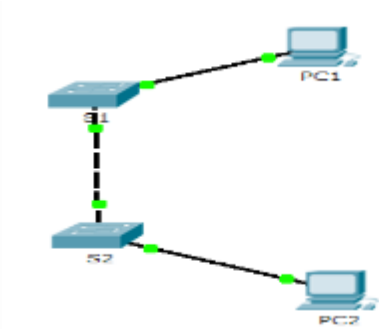
- Use una conexión de consola para acceder a cada switch.
- Nombre los switches **[[S1Name]]** y **[[S2Name]]**.
- Use la contraseña **[[LinePW]]** para todas las líneas.
- Use la contraseña secreta **[[SecretPW]]**.
- Encripte todas las contraseñas de texto no cifrado.
- Incluya la palabra **warning** (advertencia) en el mensaje del día (MOTD).
- Configure el direccionamiento para todos los dispositivos de acuerdo con la tabla de direccionamiento.
- Guarde las configuraciones.
- Verifique la conectividad entre todos los dispositivos.

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

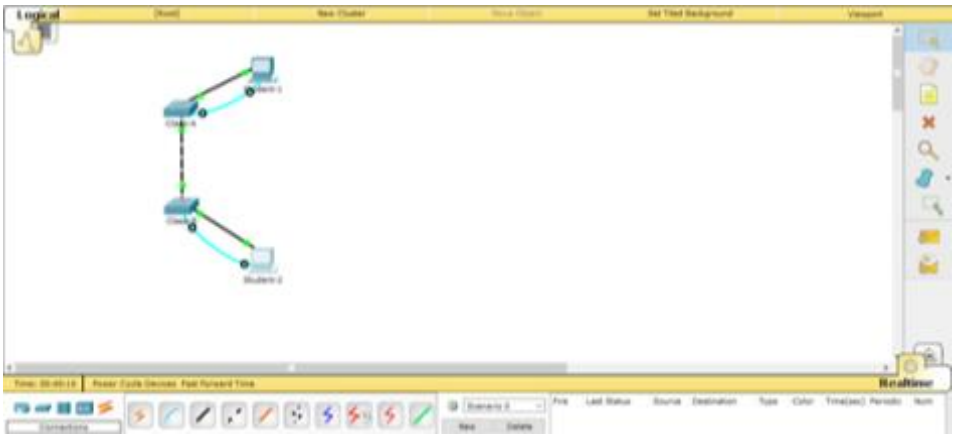
Índice de isomorfos: [[indexNames]][[indexPWs]][[indexAdds]][[indexTopos]]



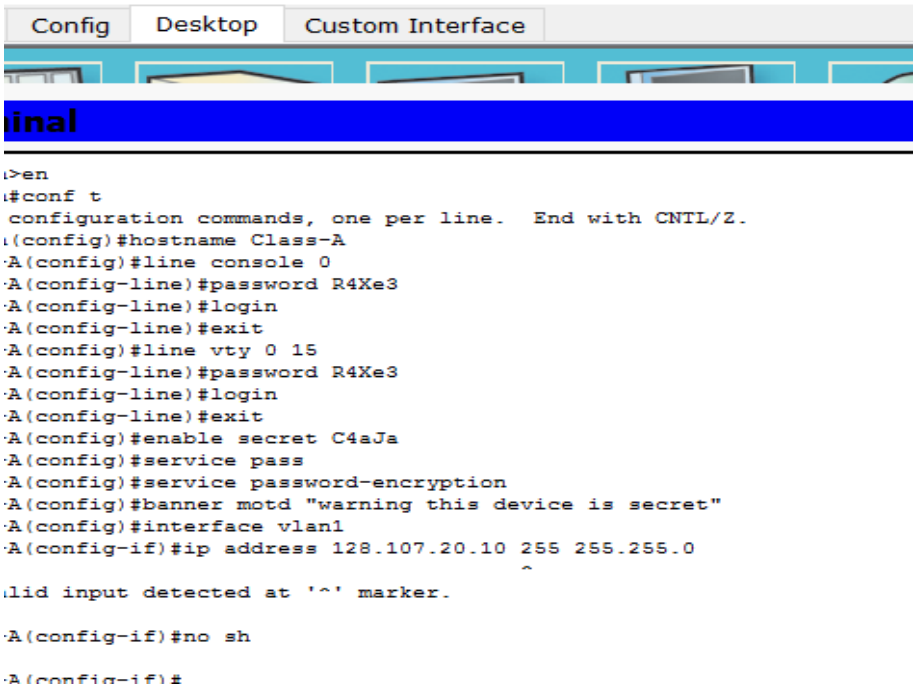


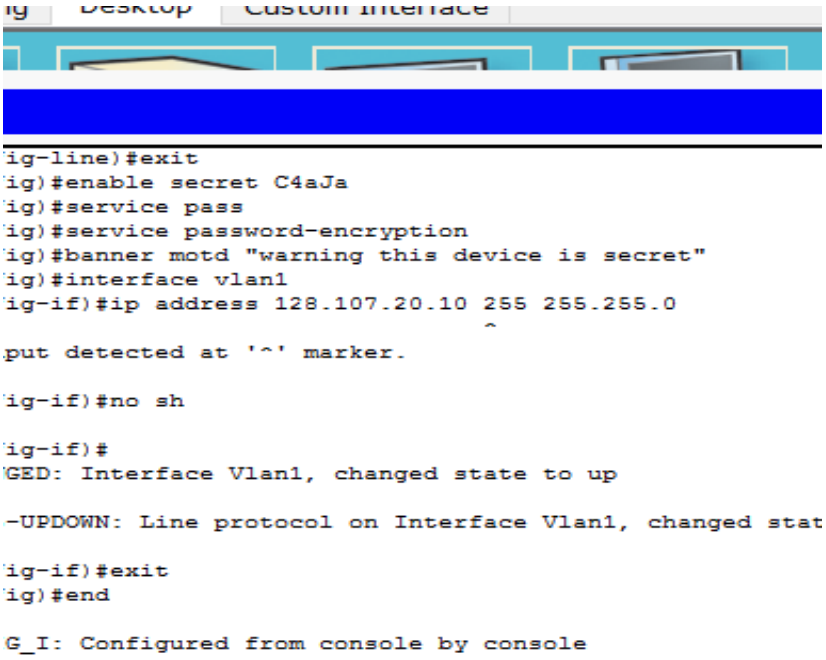


Solución: Primero realizamos la Conexión por la consola a los terminales

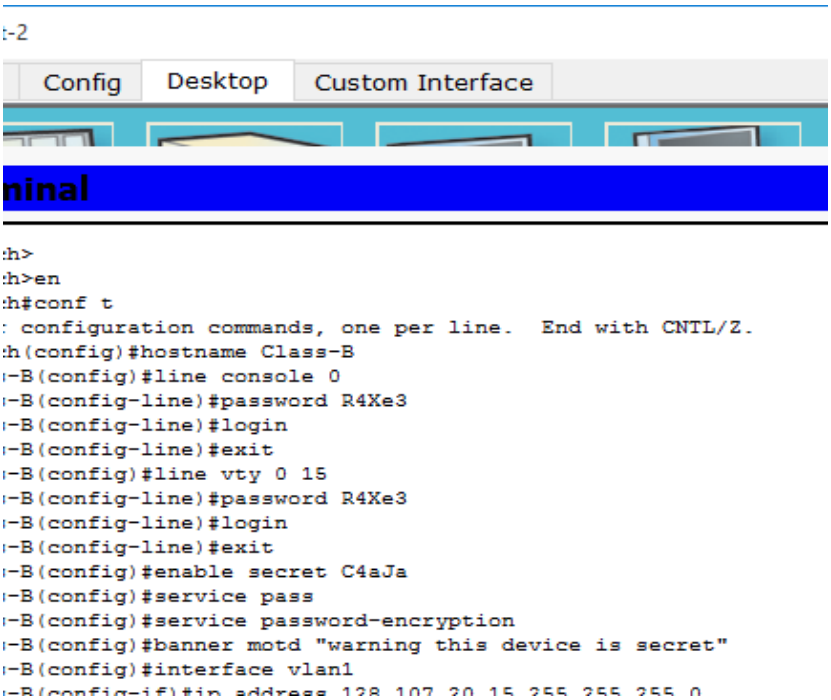


Luego configuramos el switch Class –A, realizamos todo el proceso iniciando por config t, le colocamos nombre como Class-A

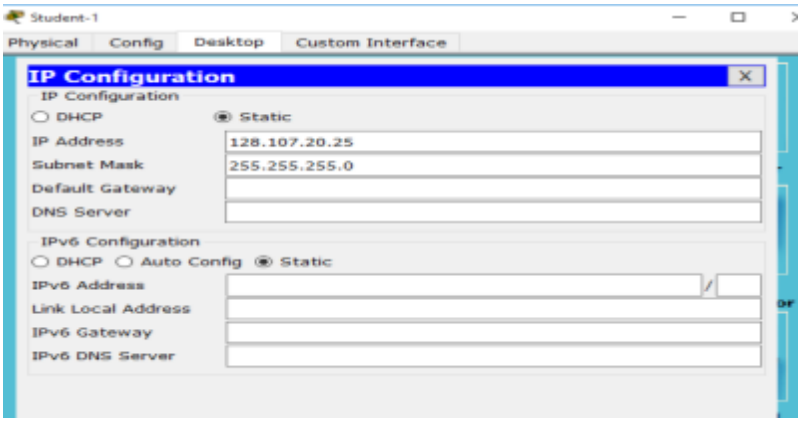


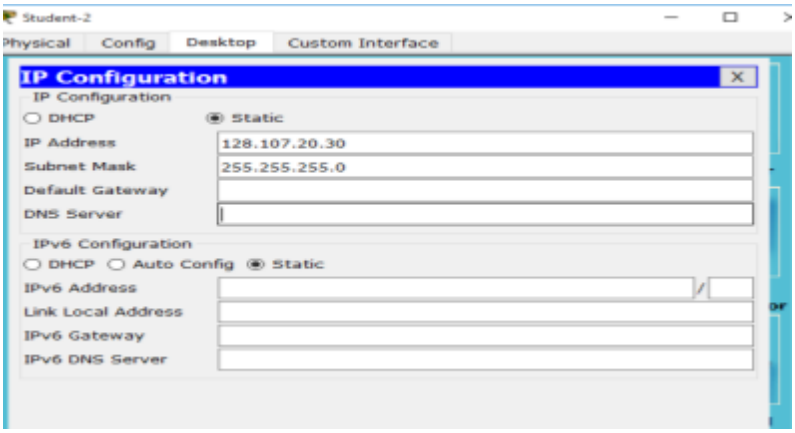


Luego de configurar el switch class – A, continuamos con el mismo procedimiento y configuramos a Switch Class-B

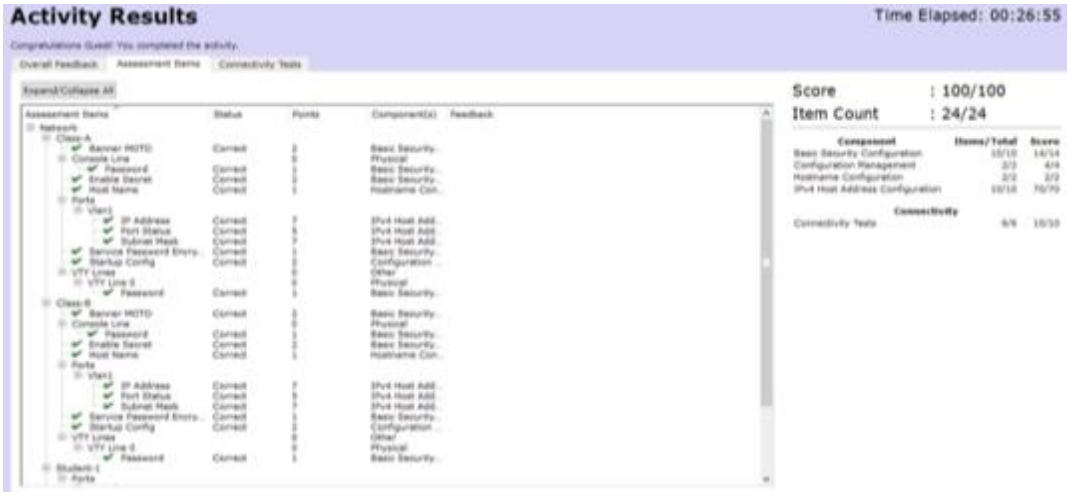


Para continuar Configuramos los terminales y les añadimos una ip.





Al realizar las respectivas configuraciones y conexiones, vamos a rectificar cuáles son sus resultados

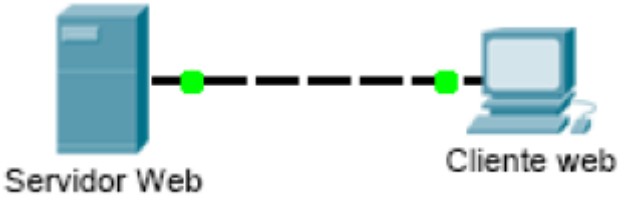


Como nos muestra la tabla, aparece la configuración que realizamos anteriormente, nos muestra los nombres, que cada ítem

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

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

Topología



Objetivos

Parte 1: Examinar el tráfico Web HTTP
Parte 2: Mostrar elementos de la suite de protocolos TCP/IP
Información básica

Esta actividad de simulación tiene como objetivo proporcionar una base para comprender la suite de protocolos TCP/IP y la relación con el modelo OSI. El modo de simulación le permite ver el contenido de los datos que se envían a través de la red en cada capa.

A medida que los datos se desplazan por la red, se dividen en partes más pequeñas y se identifican de modo que las piezas se puedan volver a unir cuando lleguen al destino. A cada pieza se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data units]) y se la asocia a una capa específica de los modelos TCP/IP y OSI. El modo de simulación de Packet Tracer le permite ver cada una de las capas y la PDU asociada. Los siguientes pasos guían al usuario a través del proceso de solicitud de una página Web desde un servidor Web mediante la aplicación de explorador Web disponible en una PC cliente.

Aunque gran parte de la información mostrada se analizará en mayor detalle más adelante, esta es una oportunidad de explorar la funcionalidad de Packet Tracer y de ver el proceso de encapsulación.

Parte 1: Examinar el tráfico Web HTTP

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

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

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

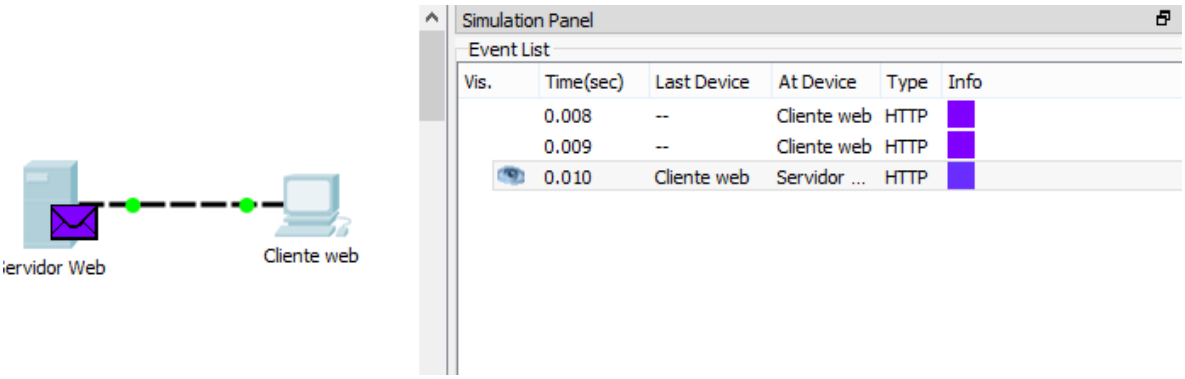
a. Haga clic en el ícono del modo **Simulation** (Simulación) para cambiar del modo **Realtime** (Tiempo real) al modo **Simulation**.
b. Seleccione **HTTP** de **Event List Filters** (Filtros de lista de eventos).

1) Es posible que HTTP ya sea el único evento visible. Haga clic en **Edit Filters** (Editar filtros) para mostrar los eventos visibles disponibles. Alterne la casilla de verificación **Show All/None** (Mostrar todo/ninguno) y observe cómo las casillas de verificación se desactivan y se activan, o viceversa, según el estado actual. 2) Haga clic en la casilla de verificación **Show all/None** (Mostrar todo/ninguno) hasta que se desactiven todas las casillas y luego seleccione **HTTP**. Haga clic en cualquier lugar fuera del cuadro **Edit Filters** (Editar filtros) para ocultarlo. Los eventos visibles ahora deben mostrar solo HTTP.

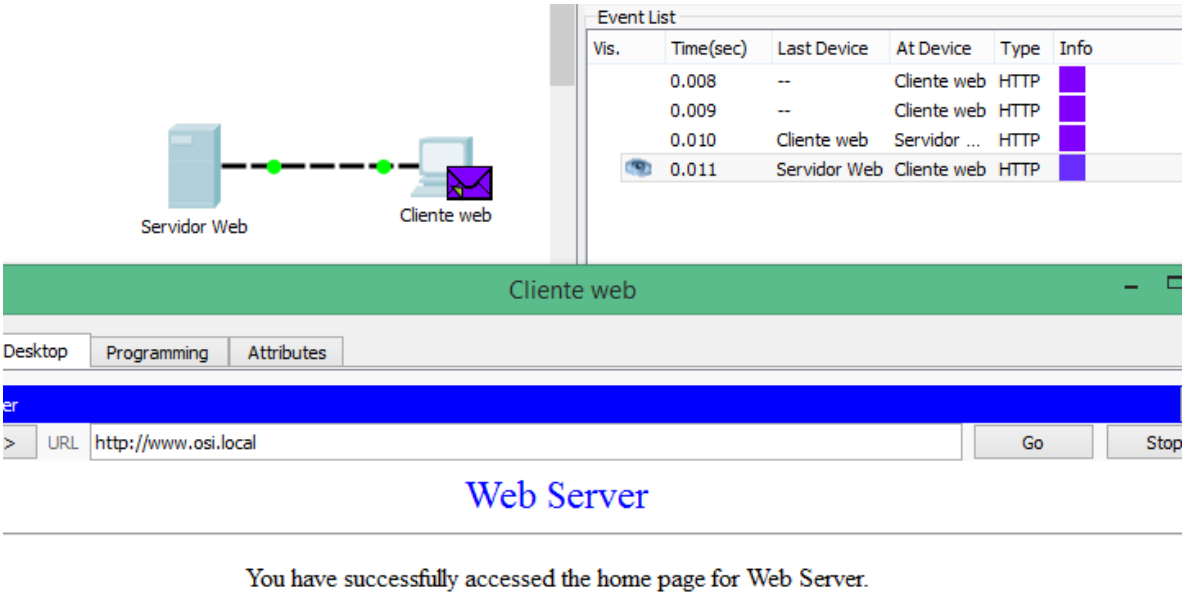
Paso 2: Genere tráfico web (HTTP).

El panel de simulación actualmente está vacío. En la parte superior de Event List (Lista de eventos) dentro del panel de simulación, se indican seis columnas. A medida que se genera y se revisa el tráfico, aparecen los eventos en la lista. La columna **Info** (Información) se utiliza para examinar el contenido de un evento determinado.
Nota: el servidor Web y el cliente Web se muestran en el panel de la izquierda. Se puede ajustar el tamaño de los paneles manteniendo el mouse junto a la barra de desplazamiento y arrastrando a la izquierda o a la derecha cuando aparece la flecha de dos puntas.
a. Haga clic en **Web Client** (Cliente Web) en el panel del extremo izquierdo.
b. Haga clic en la ficha **Desktop** (Escritorio) y luego en el ícono **Web Browser** (Explorador Web) para abrirlo.
c. En el campo de dirección URL, introduzca **www.osi.local** y haga clic en **Go** (Ir).

Debido a que el tiempo en el modo de simulación se desencadena por eventos, debe usar el botón **Capture/Forward** (Capturar/avanzar) para mostrar los eventos de red.
d. Haga clic en **Capture/Forward** cuatro veces. Debe haber cuatro eventos en la lista de eventos.



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

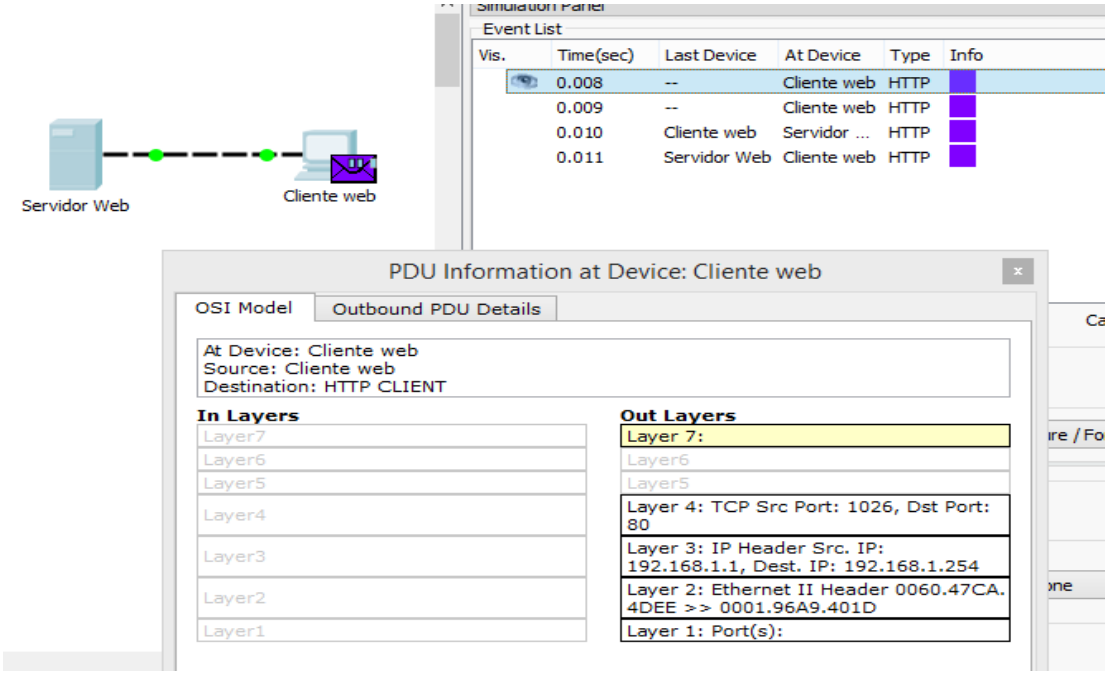


El servidor Web devolvió la página Web.

Paso 3: Explorar el contenido del paquete HTTP a. Haga clic en el primer cuadro coloreado debajo de la columna **Event List** >**Info** (Lista de eventos > Información). Quizá sea necesario expandir el **panel de simulación** o usar la barra de desplazamiento que se encuentra directamente debajo de la **lista de eventos**.

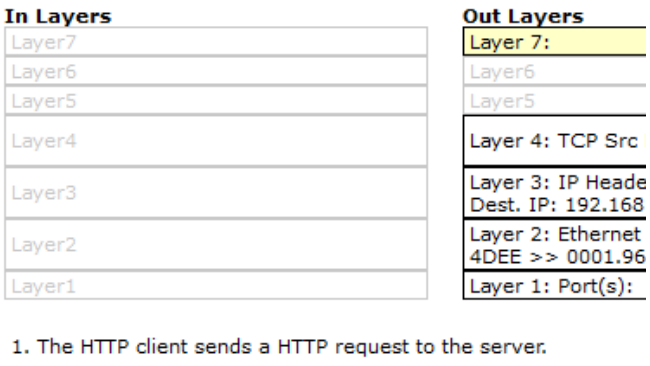
Se muestra la ventana **PDU Information at Device: Web Client** (Información de PDU en dispositivo: cliente Web). En esta ventana, solo hay dos fichas, **OSI Model** (Modelo OSI) y **Outbound PDU Details** (Detalles de PDU saliente), debido a que este es el inicio de la transmisión. A medida que se analizan más eventos, se

muestran tres fichas, ya que se agrega la ficha **Inbound PDU Details** (Detalles de PDU entrante). Cuando un evento es el último evento del stream de tráfico, solo se muestran las fichas **OSI Model** e **Inbound PDU Details**.



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

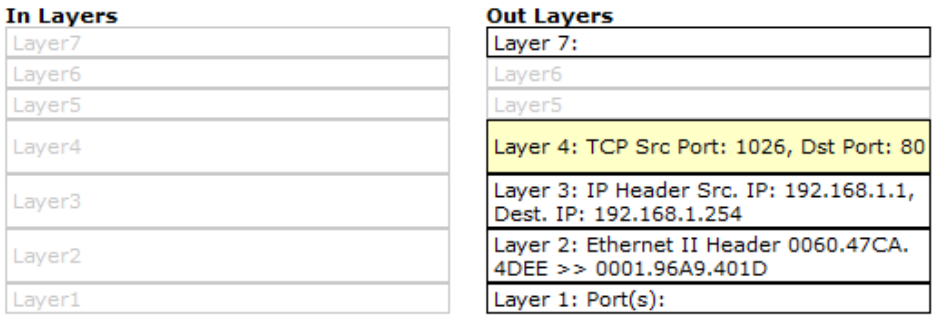
¿Cuál es el texto que se muestra junto a la etiqueta **Layer 7**? The HTTP client send a HTP request to the server



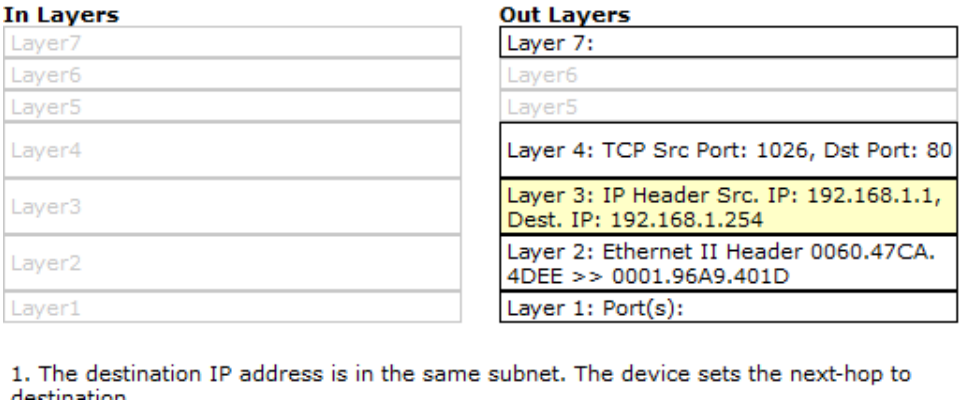
¿Qué información se indica en los pasos numerados directamente debajo de los cuadros **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida)?

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

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

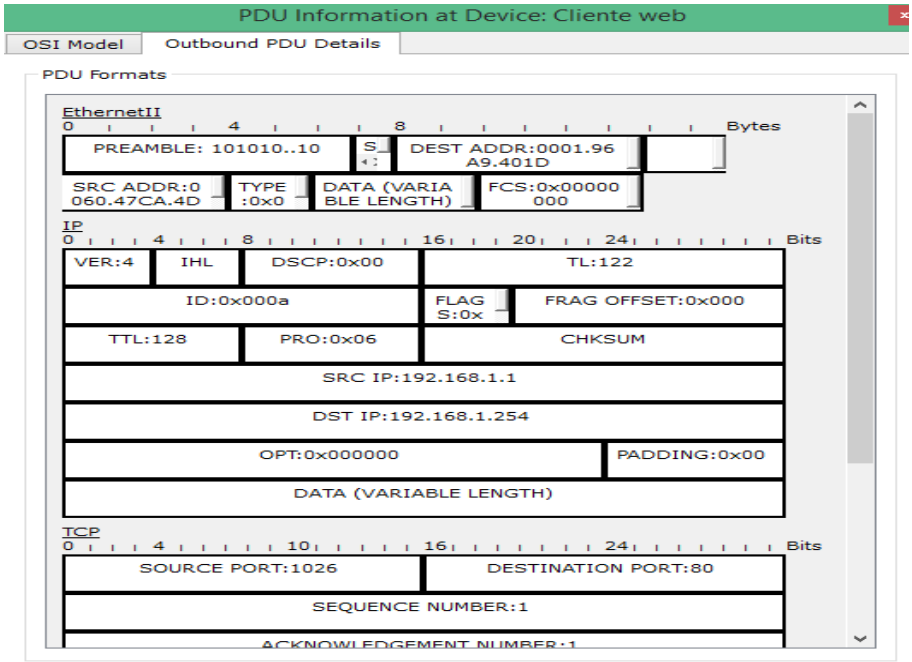
El encabezado Ethernet II de capa 2 y las direcciones MAC de entrada y salida.

In Layers	Out Layers
Layer7	Layer 7:
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1026, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254
Layer2	Layer 2: Ethernet II Header 0060.47CA.4DEE >> 0001.96A9.401D
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.

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

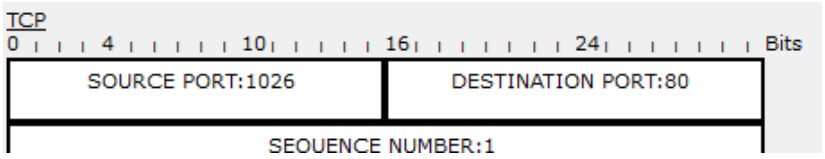
La información que se indica debajo de **PDU Details** (Detalles de PDU) refleja las capas dentro del modelo TCP/IP.
Nota: la información que se indica en la sección **Ethernet II** proporciona información aun más detallada que la que se indica en Layer 2 (Capa 2) en la ficha **OSI Model**. **Outbound 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**? Ethernet II , IP, TP y HTTP REQUEST

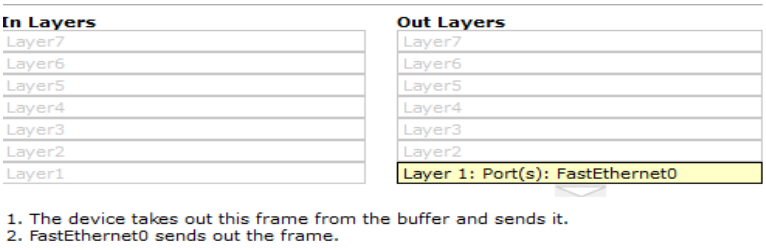
¿Con qué capa se relaciona? SRC IP (IP DE ORIG.) y DST IP (IP DE DEST.) en la capa 3
¿Cuál es la información frecuente que se indica en la sección **TCP** de **PDU Details** comparada con la información que se indica en la ficha **OSI Model**, y con qué capa se relaciona?

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



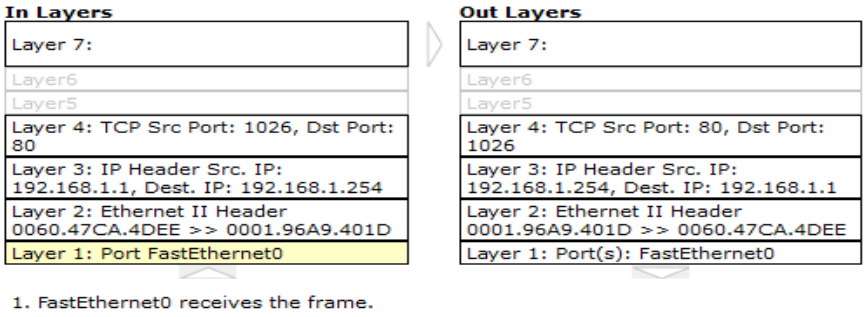
¿Cuál es el **host** que se indica en la sección **HTTP** de **PDU Details**? ¿Con qué capa se relacionaría esta información en la ficha **OSI Model**? www.osi.local, capa 7

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.



Avance al siguiente cuadro **Info** (Información) de HTTP dentro de la **lista de eventos** y haga clic en el cuadro coloreado. Esta ventana contiene las columnas **In Layers** (Capas de entrada) y **Out Layers** (Capas de salida). Observe la dirección de la flecha que está directamente debajo de la columna **In Layers**; esta apunta hacia arriba, lo que indica la dirección en la que se transfiere la información. Desplácese por estas capas y tome nota de los elementos vistos anteriormente. En la parte superior de la

columna, la flecha apunta hacia la derecha. Esto indica que el servidor ahora envía la información de regreso al cliente.

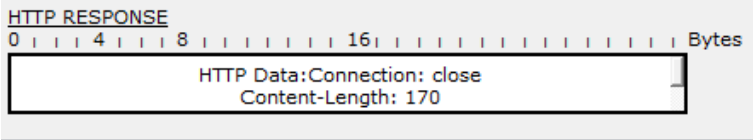


Compare la información que se muestra en la columna **In Layers** con la de la columna **Out Layers**: ¿cuáles son las diferencias principales?

Se intercambiaron los puertos de origen y destino, las direcciones IP de origen y destino, y las direcciones MAC.

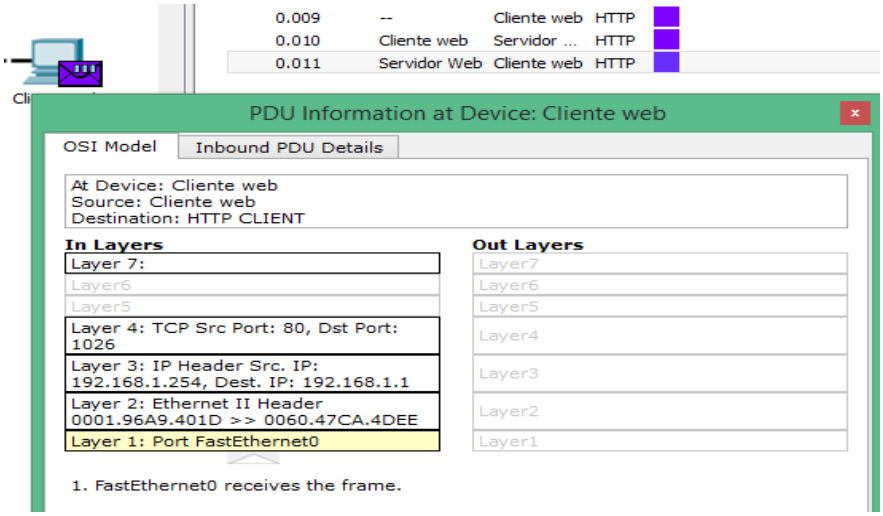
i. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). Desplácese hasta la sección **HTTP**.

¿Cuál es la primera línea del mensaje HTTP que se muestra? 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.

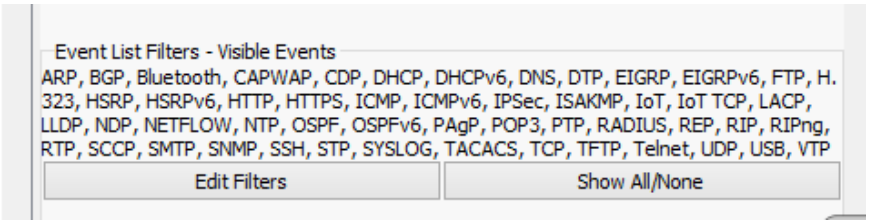


Parte 2: Mostrar elementos de la suite de protocolos TCP/IP
En la parte 2 de esta actividad, utilizará el modo de simulación de Packet Tracer para ver y examinar algunos de los otros protocolos que componen la suite TCP/IP.

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).

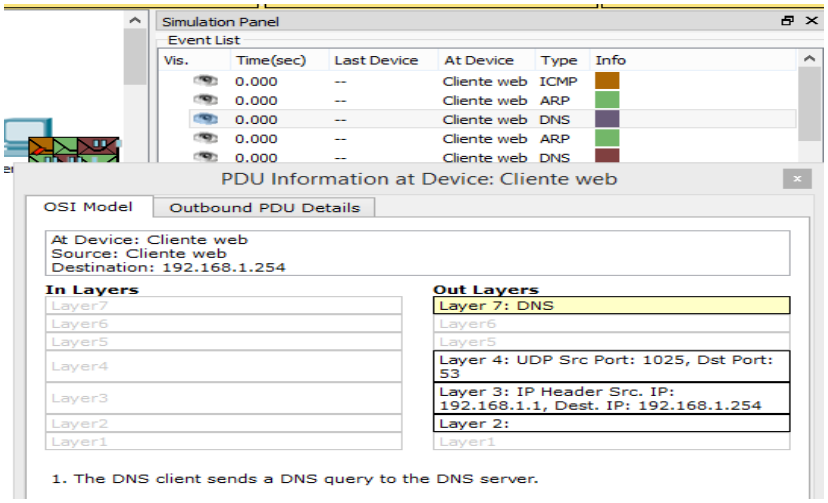
¿Qué tipos de eventos adicionales se muestran?



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

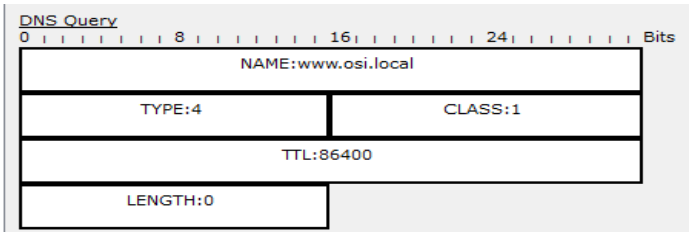
c. Haga clic en el primer evento de DNS en la columna **Info**. Examine las fichas **OSI Model** y **PDU Detail**, y observe el proceso de encapsulación. Al observar la ficha **OSI Model** con el cuadro **Layer 7** resaltado, se incluye una descripción de lo que ocurre,

inmediatamente debajo de **In Layers** y **Out Layers**: ("1. The DNS client sends a DNS query to the DNS server." ["El cliente DNS envía una consulta DNS al servidor DNS"]). Esta información es muy útil para ayudarlo a comprender qué ocurre durante el proceso de comunicación.



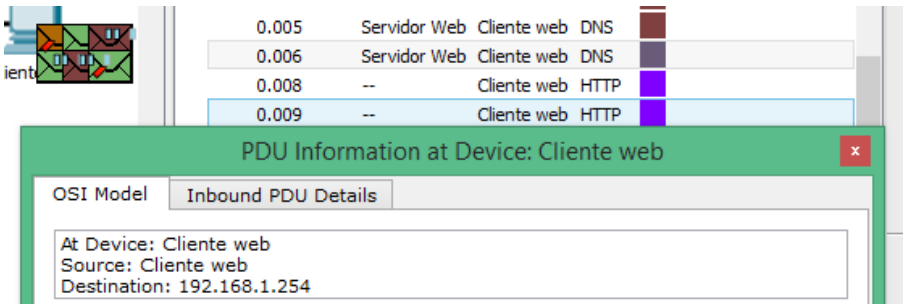
d. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿Qué información se indica en **NAME**: (NOMBRE:) en la sección DNS QUERY (CONSULTA DNS)?

www.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.

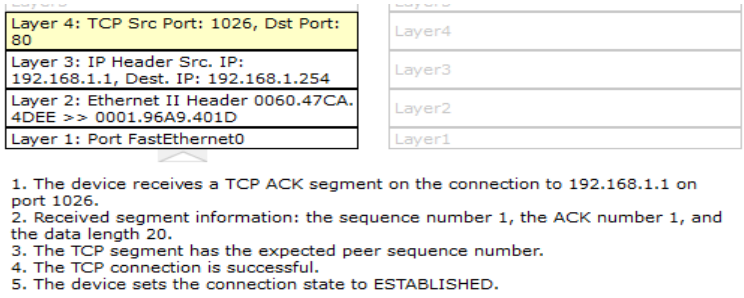


¿Cuál es el valor que se indica junto a **ADDRESS**: (DIRECCIÓN:) en la sección DNS ANSWER (RESPUESTA DE DNS) de **Inbound PDU Details**?

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).

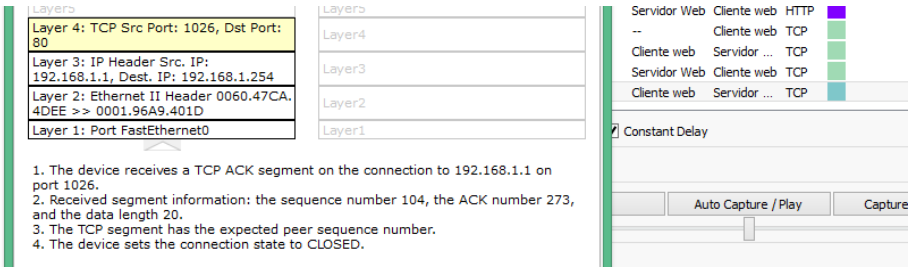


El protocolo TCP administra la conexión y la desconexión del canal de comunicación, además de tener otras responsabilidades. Este evento específico muestra que SE ESTABLECIÓ el canal de comunicación.

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)?

Conexión CLOSED (cerrada)

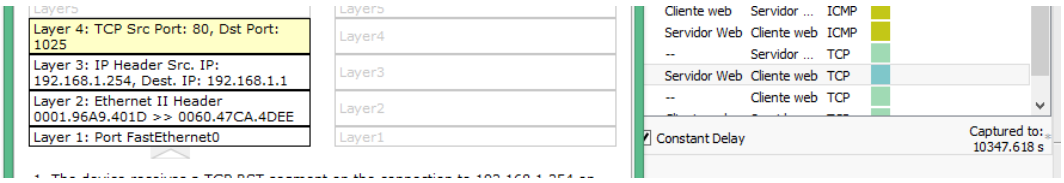


Desafío

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

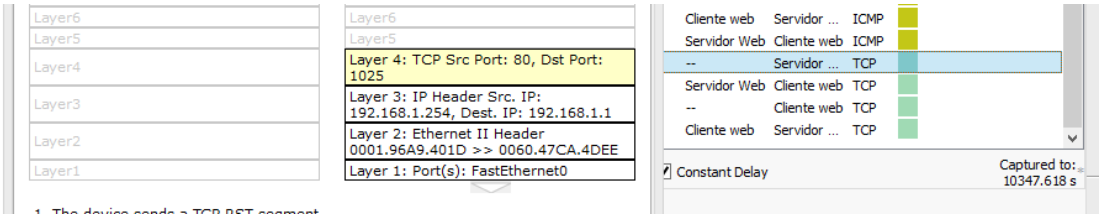
Sobre la base de la información que se analizó durante la captura de Packet Tracer, ¿qué número de puerto escucha el **servidor Web** para detectar la solicitud Web?

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



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

La primera PDU DNS que solicita el cliente Web muestra que el puerto de destino de capa 4 es el puerto 1025.



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

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

Topología

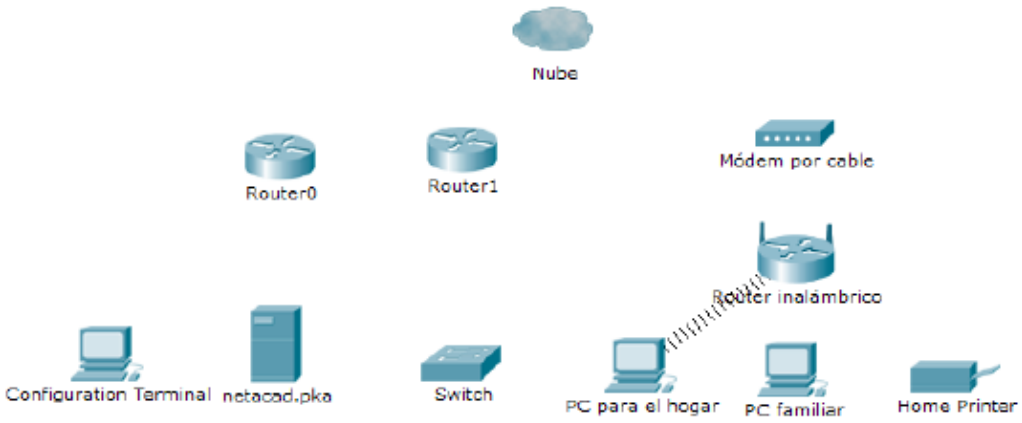


Tabla de direccionamiento

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

Objetivos

- **Parte 1: Conectarse a la nube**
- **Parte 2: Conectar el Router0**
- **Parte 3: Conectar los dispositivos restantes**
- **Parte 4: Verificar las conexiones**
- **Parte 5: Examinar la topología física**

Información básica

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

Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0

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

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

Paso 2: Conectar la nube al módem por cable

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

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

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

Paso 2: Conectar el Router0 a netacad.pka

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

Paso 3: Conectar el Router0 a la terminal de configuración

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

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

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

Paso 2: Conectar el módem por cable al router inalámbrico

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

Paso 3: Conectar el router inalámbrico a la PC familiar
Elija el cable adecuado para conectar la **interfaz Ethernet 1 del router inalámbrico** a la **PC familiar**.
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka a. Abra el símbolo del sistema de la **PC familiar** y haga ping a **netacad.pka**.
b. Abra el **explorador Web** e introduzca dirección Web **http://netacad.pka**.

Paso 2: Hacer ping al switch desde la PC doméstica

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

Paso 3: Abrir el Router0 desde la terminal de configuración a. Abra la **terminal** de la **terminal de configuración** y acepte la configuración predeterminada.
b. Presione **Entrar** para ver el símbolo del sistema del **Router0**.
c. Escriba **show ip interface brief** para ver el estado de las interfaces.

Parte 5: Examinar la topología física

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

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

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

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

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

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

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

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

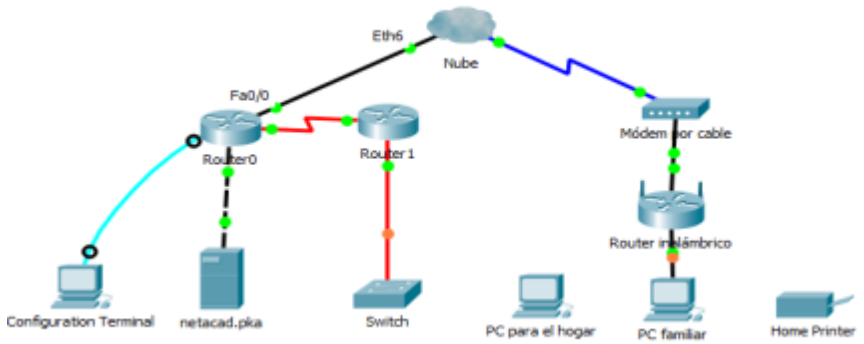
Paso 4: Examinar la red doméstica l. ¿Por qué hay una malla ovalada que cubre la red doméstica? Representa el alcance de la red inalámbrica.

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

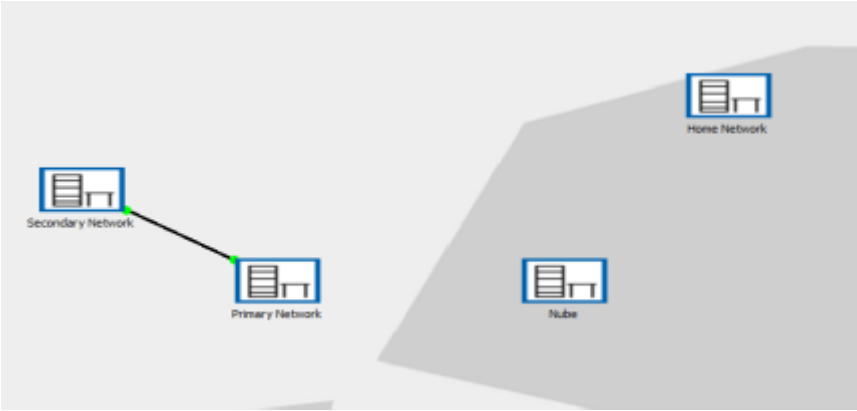
a. Haga clic en la ficha **Logical Workspace** (Área de trabajo lógica) para volver a la topología lógica.

DESARROLLO

Primer Cluster



Segundo Cluster



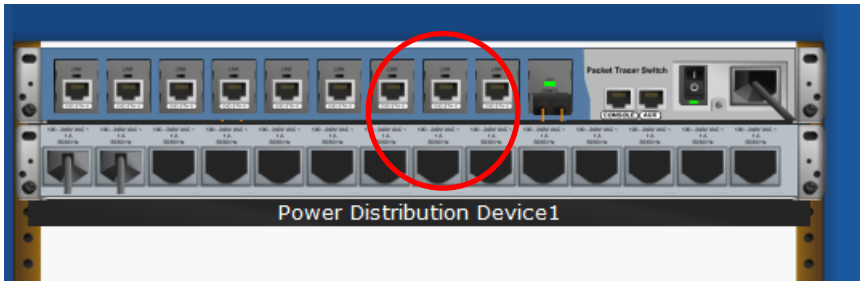
Paso 2: Examinar la red principal h. Haga clic en el ícono **Primary Network** (Red principal). Mantenga el puntero del mouse sobre los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del bastidor azul?

Cable de Terminal de configuración

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

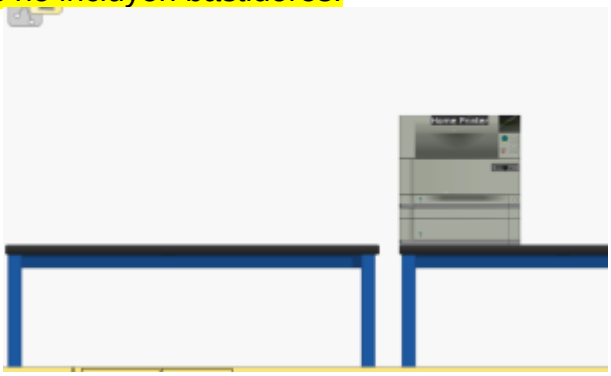
Paso 3: Examinar la red secundaria j. Haga clic en el ícono **Secondary Network** (Red secundaria). Mantenga el puntero del mouse sobre los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo?

Los cables de fibra vienen en pares, uno para transmitir y otro para recibir.



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

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



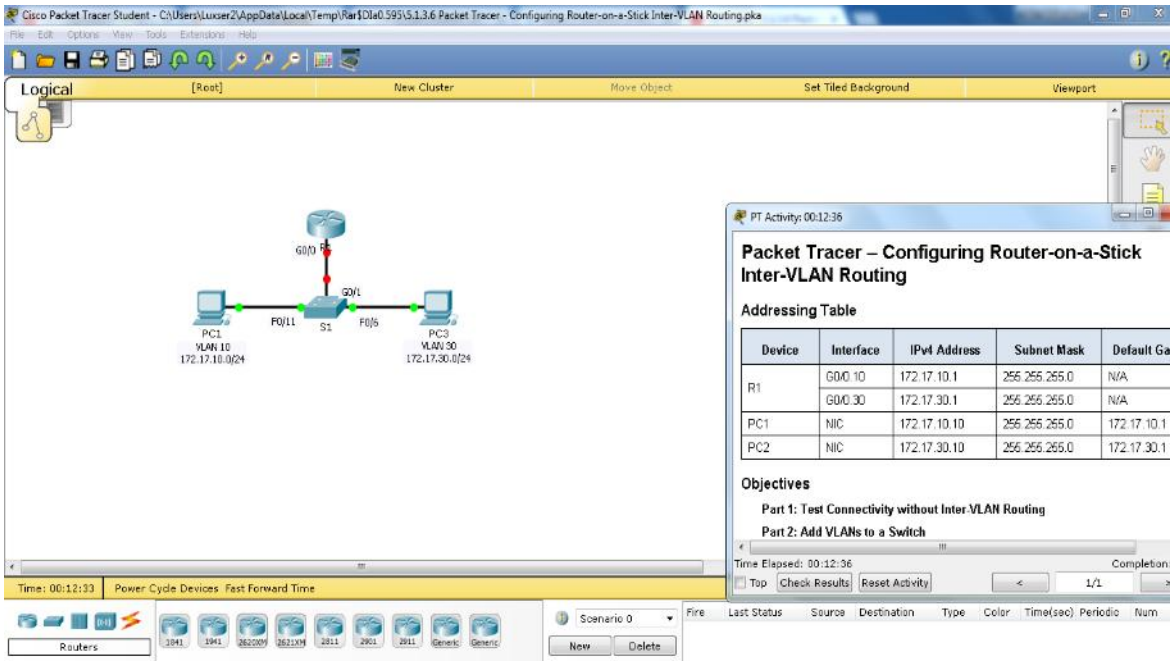
5.1.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing Instructions IG.

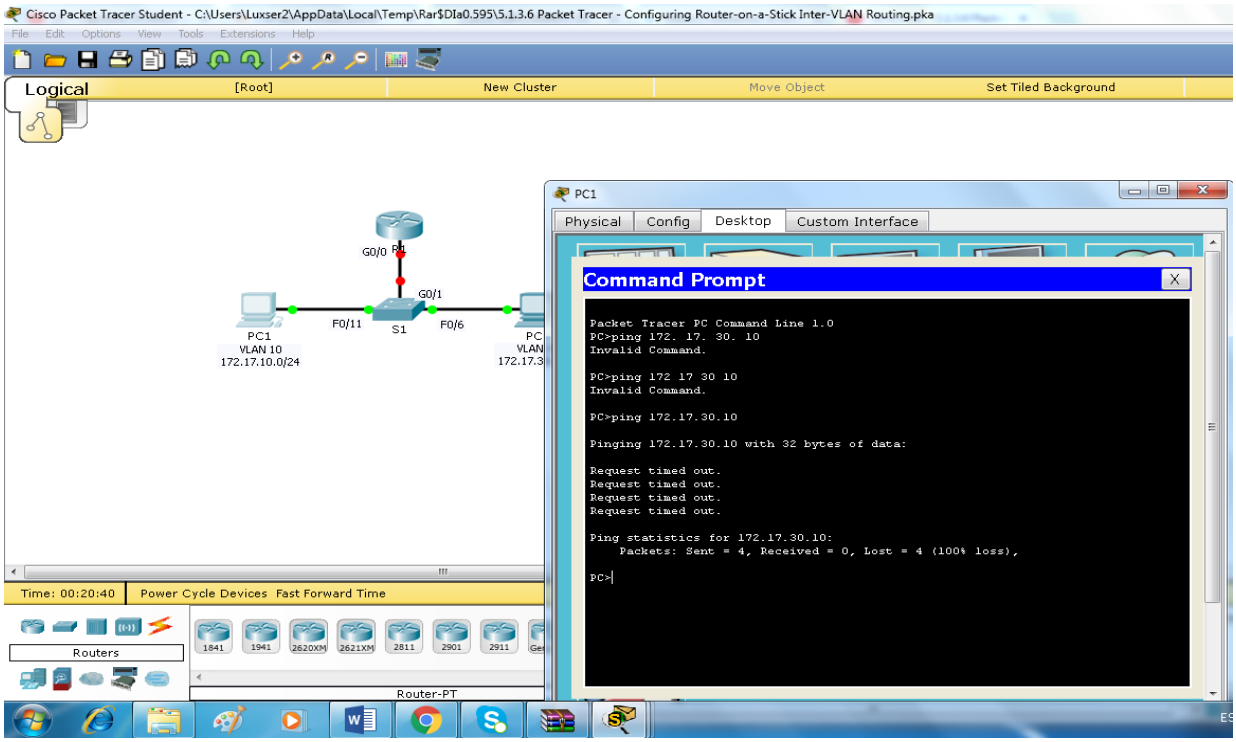
Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	N/A
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Part 1: Test Connectivity Without Inter-VLAN Routing
Step 1: Ping between PC1 and PC3.

Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs are on separate networks and **R1** is not configured, the ping fails.

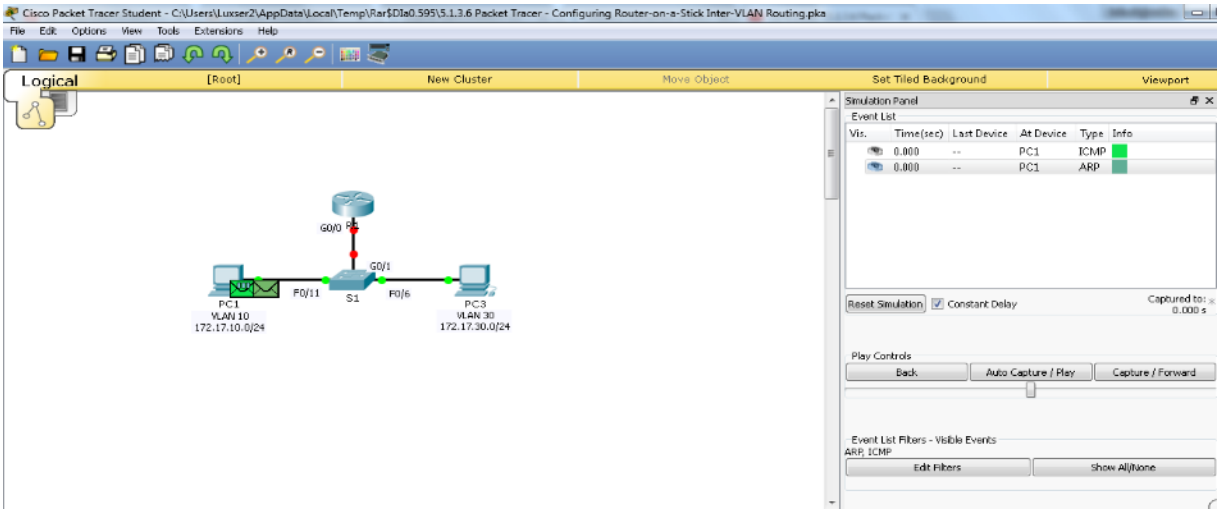


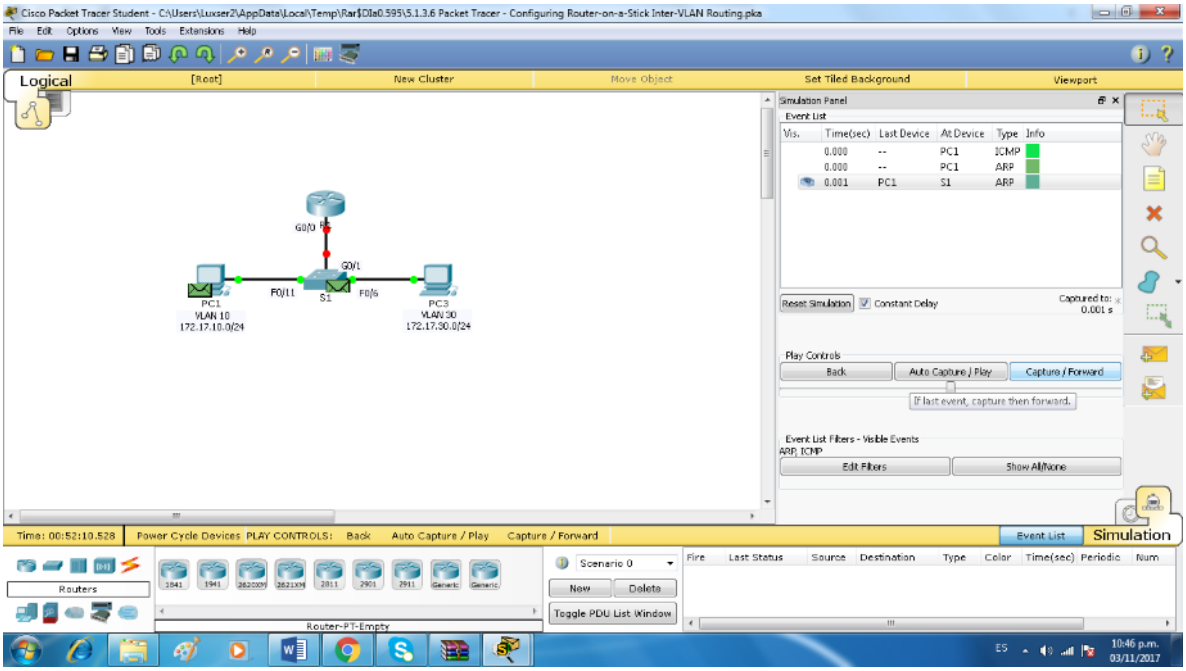


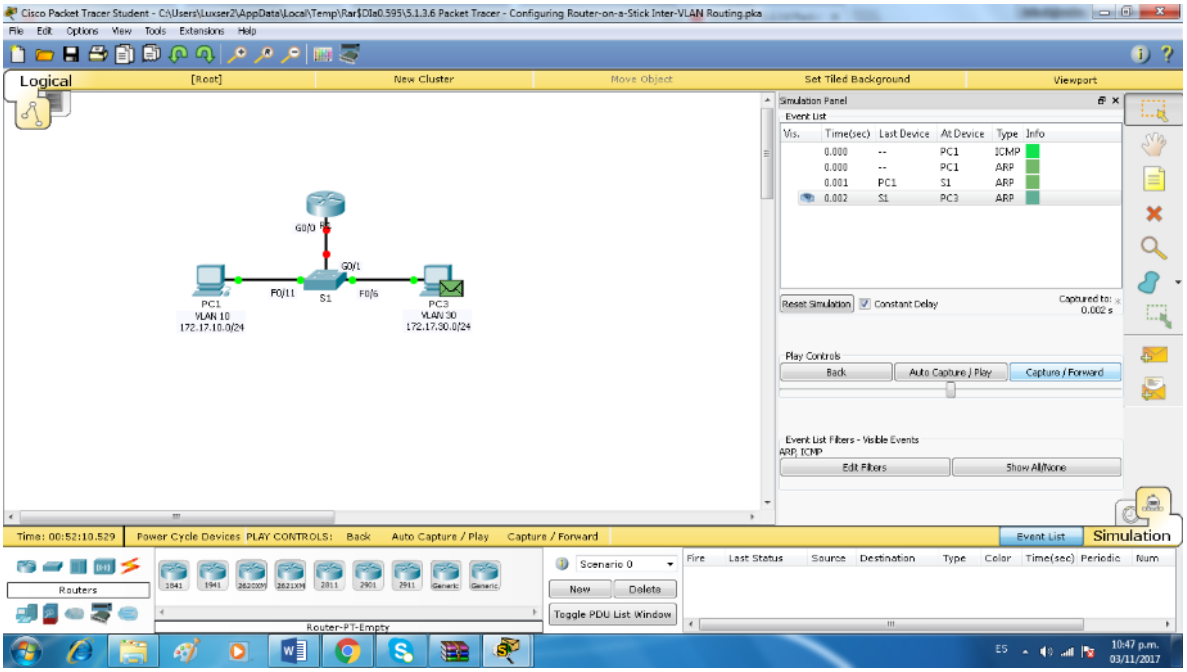
Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

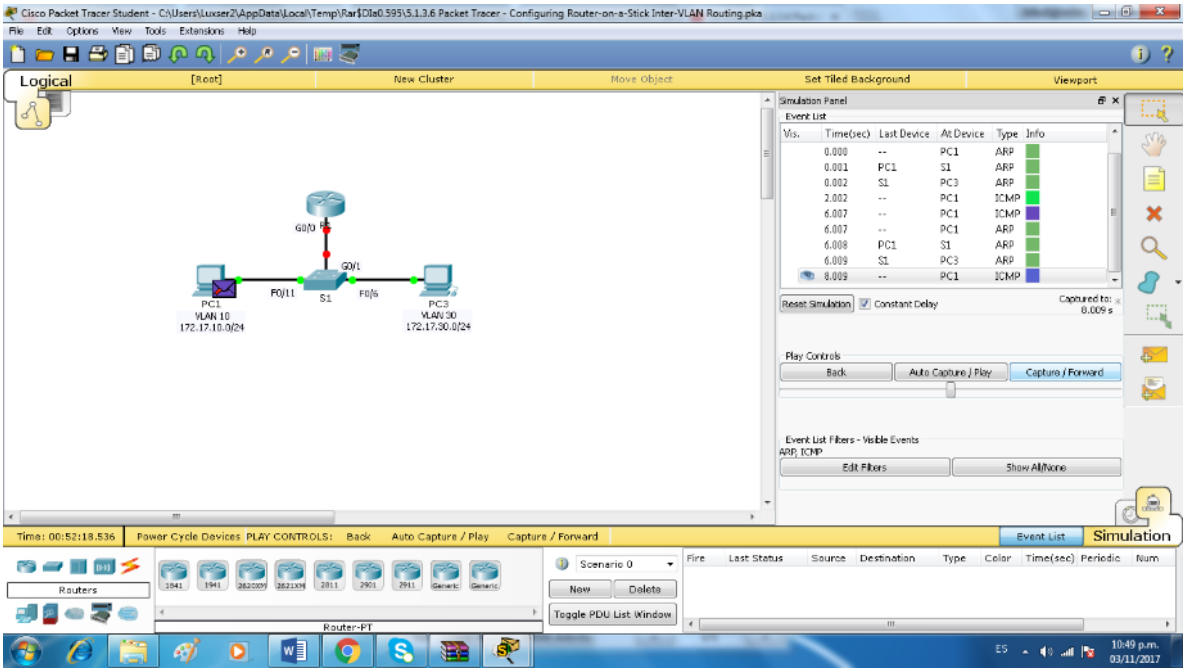
b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why?







What process failed and why?



Ha fallado porque la PC1 está en una red distinta a la PC2

Part 2: Add VLANs to a Switch

Step 1: Create VLANs on S1.

Return to **Realtime** mode and create VLAN 10 and VLAN 30 on **S1**.

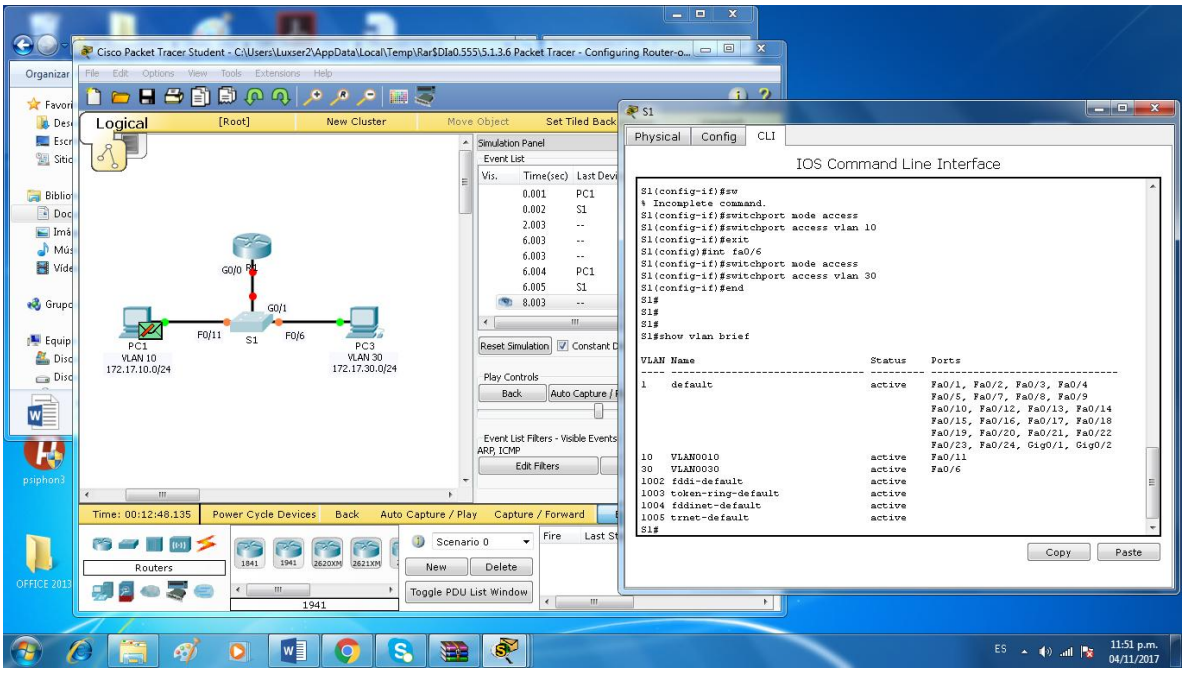
Step 2: Assign VLANs to ports.

a. Configure interface F0/6 and F0/11 as access ports and assign VLANs.

- Assign **PC1** to VLAN 10.
- Assign **PC3** to VLAN 30.

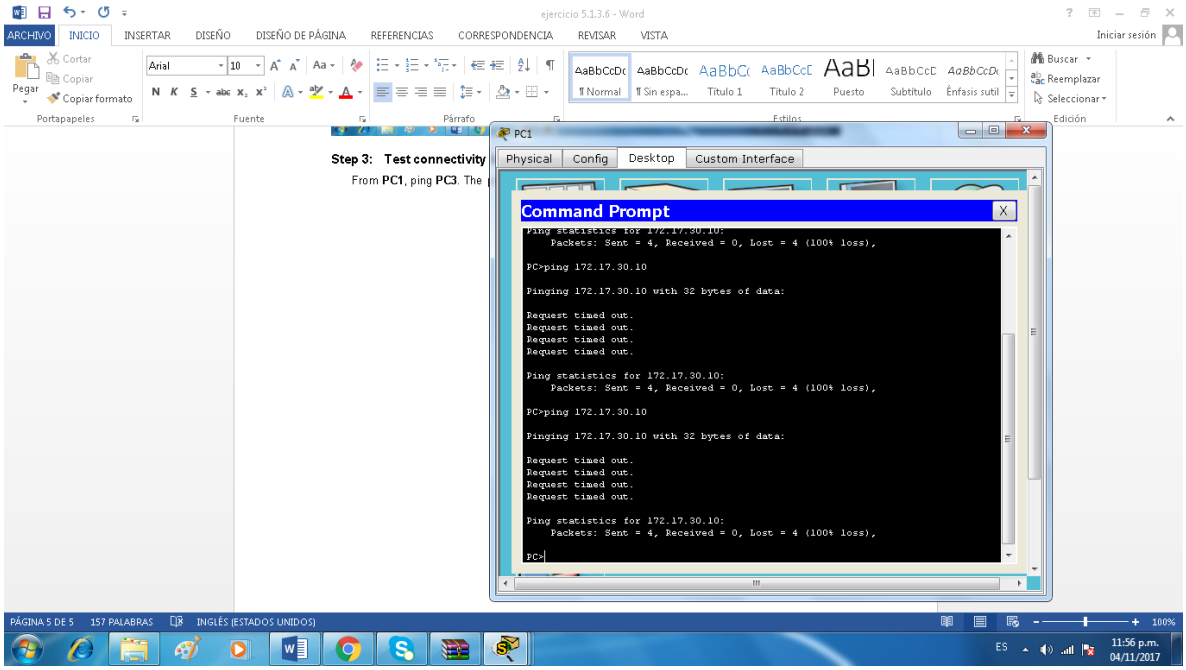
b. Issue the **show vlan brief** command to verify VLAN configuration.

S1# **show vlan brief**



Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful?



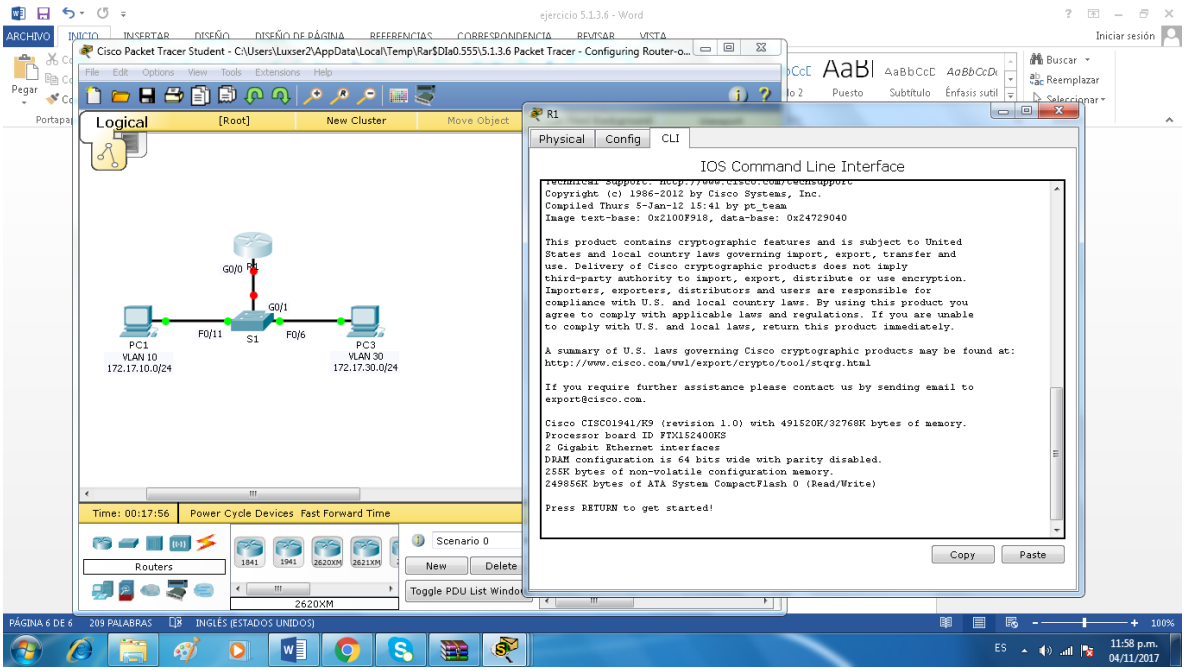
Part 3: Configure Subinterfaces

Step 1: Configure subinterfaces on R1 using the 802.1Q encapsulation.

a. Create the subinterface G0/0.10.

- Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.
- Refer to the **Address Table** and assign the correct IP address to the subinterface.

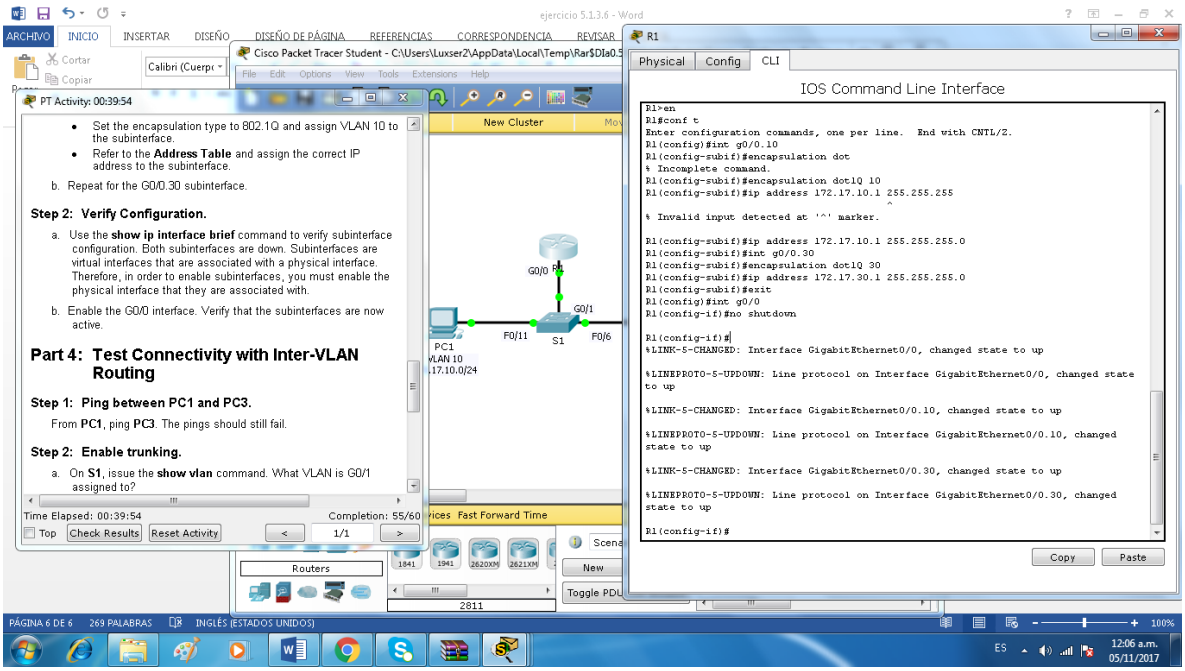
b. Repeat for the G0/0.30 subinterface.



Step 2: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

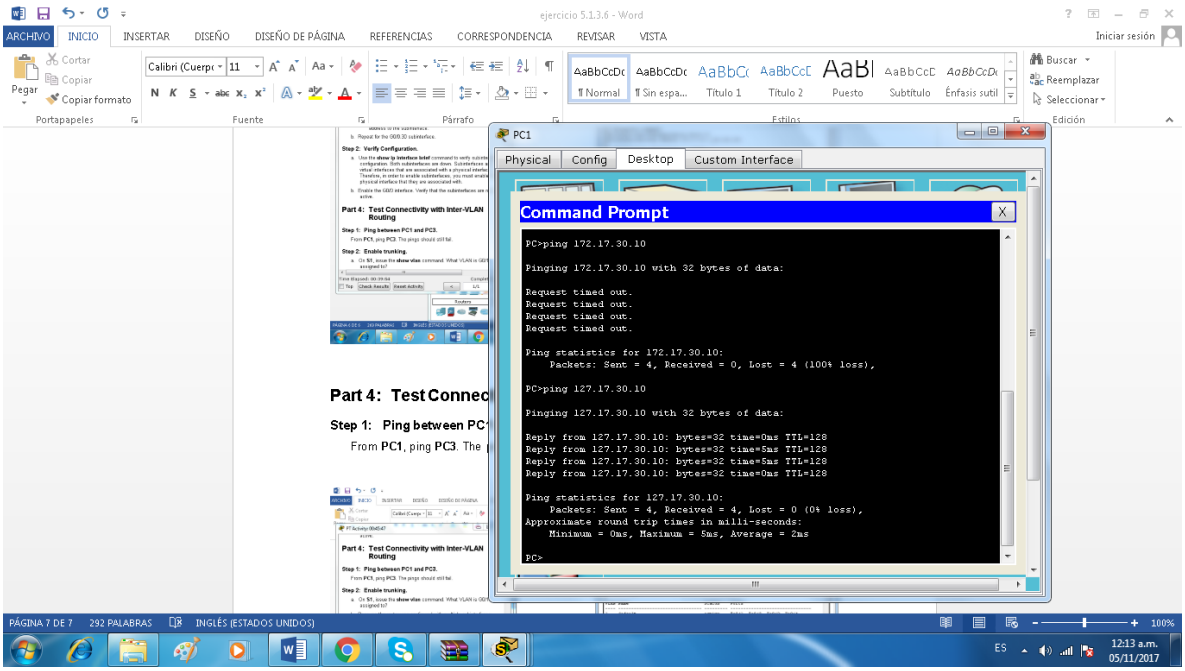
b. Enable the G0/0 interface. Verify that the subinterfaces are now active.



Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

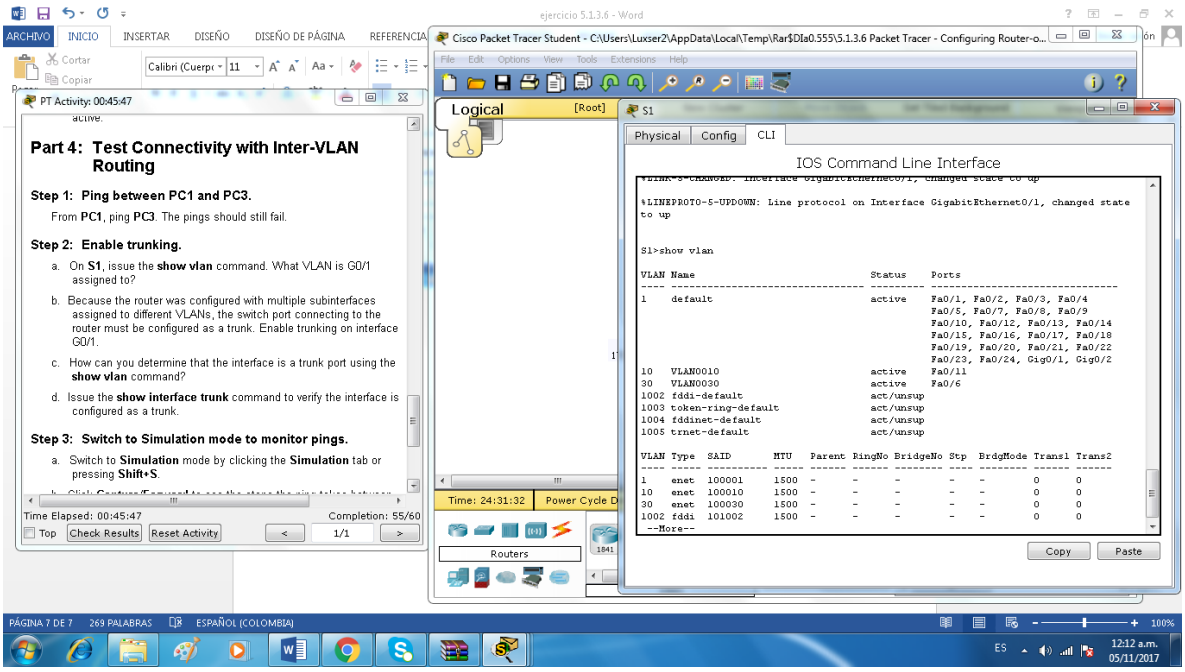
From **PC1**, ping **PC3**. The pings should still fail.

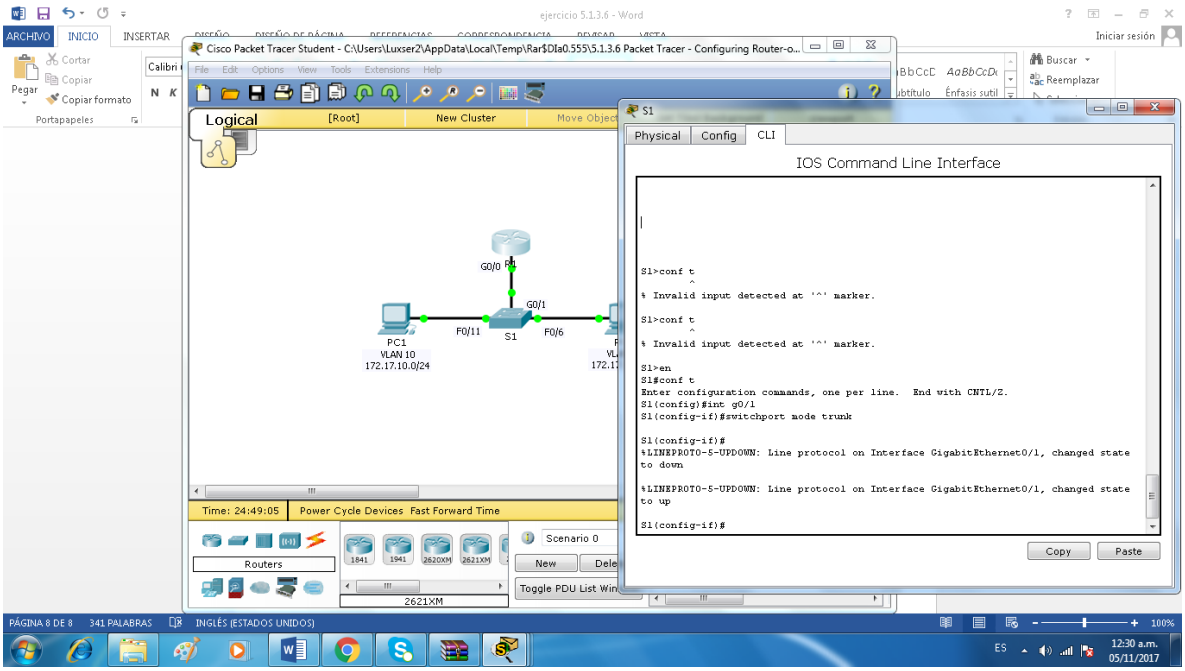


tep 2: Enable trunking.

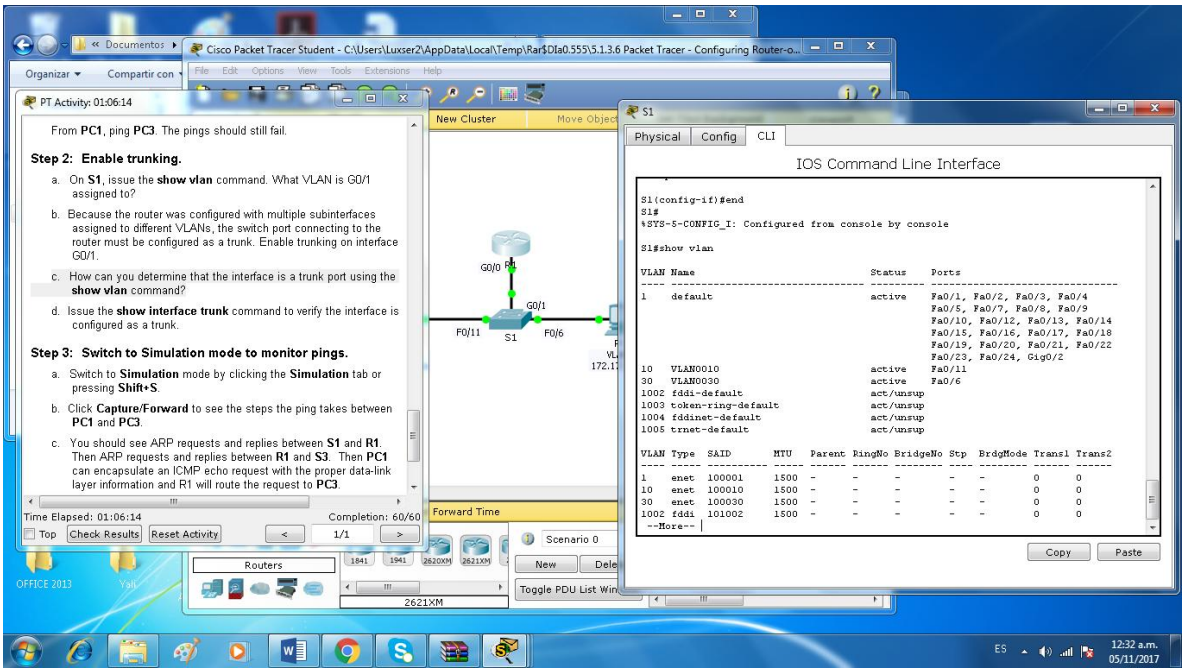
a. On **S1**, issue the **show vlan** command. What VLAN is G0/1 assigned to?

b. Because the router was configured with multiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk. Enable trunking on interface G0/1.

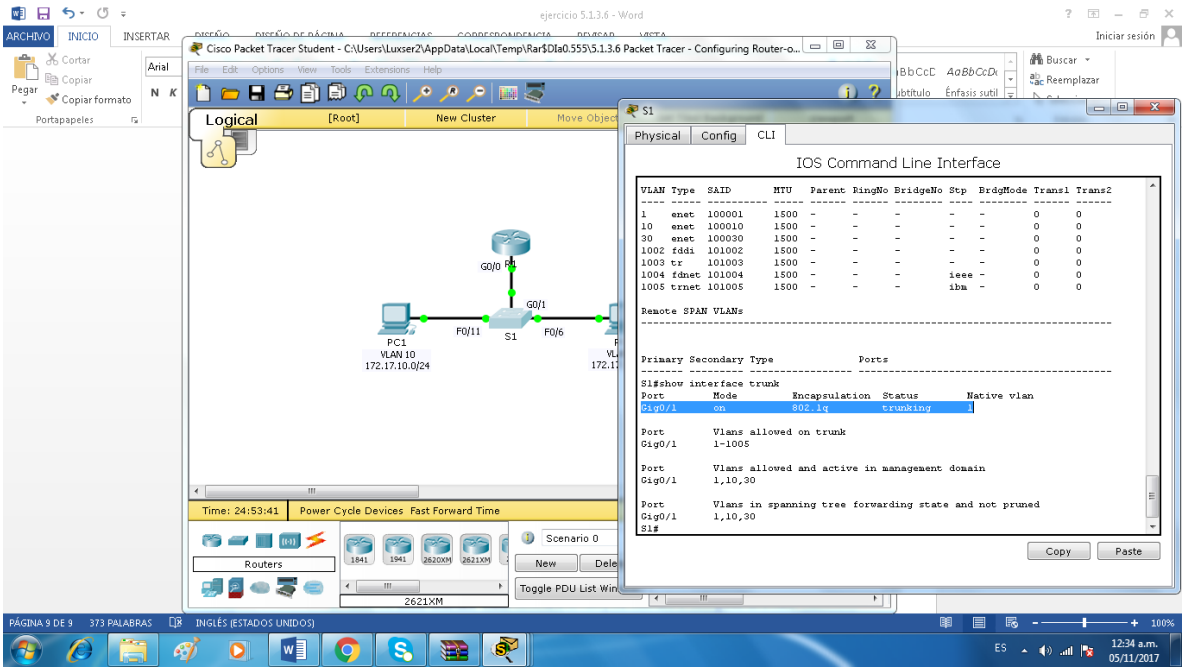


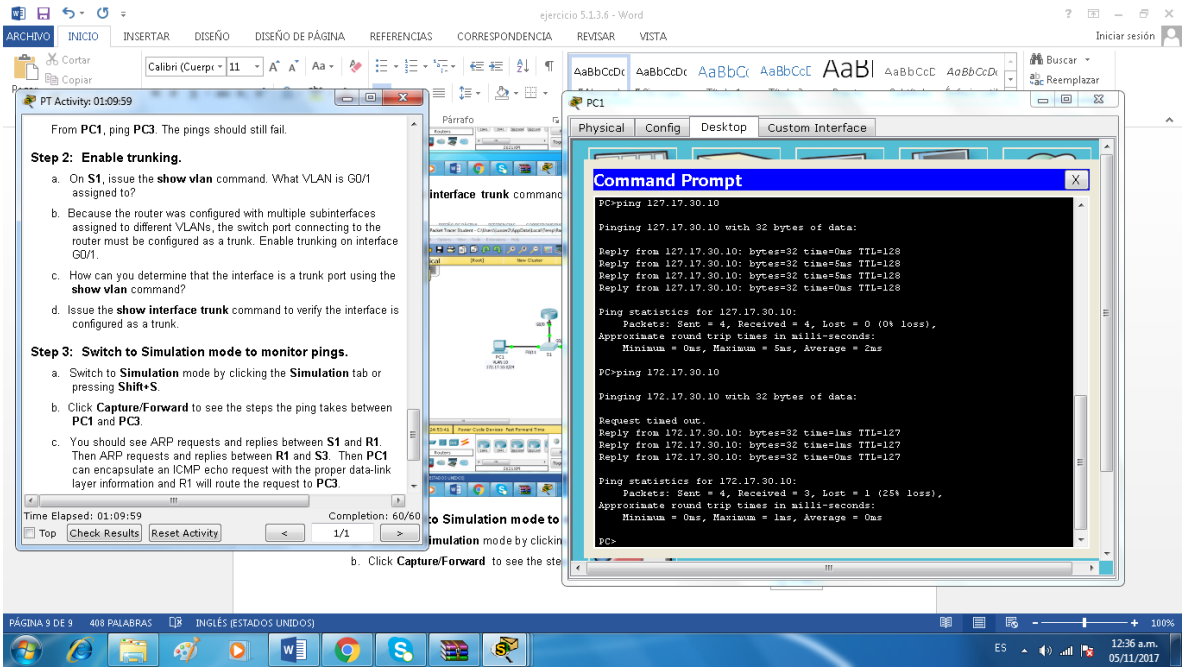


c. How can you determine that the interface is a trunk port using the**show vlan** command?



d. Issue the **show interface trunk** command to verify the interface is configured as a trunk.

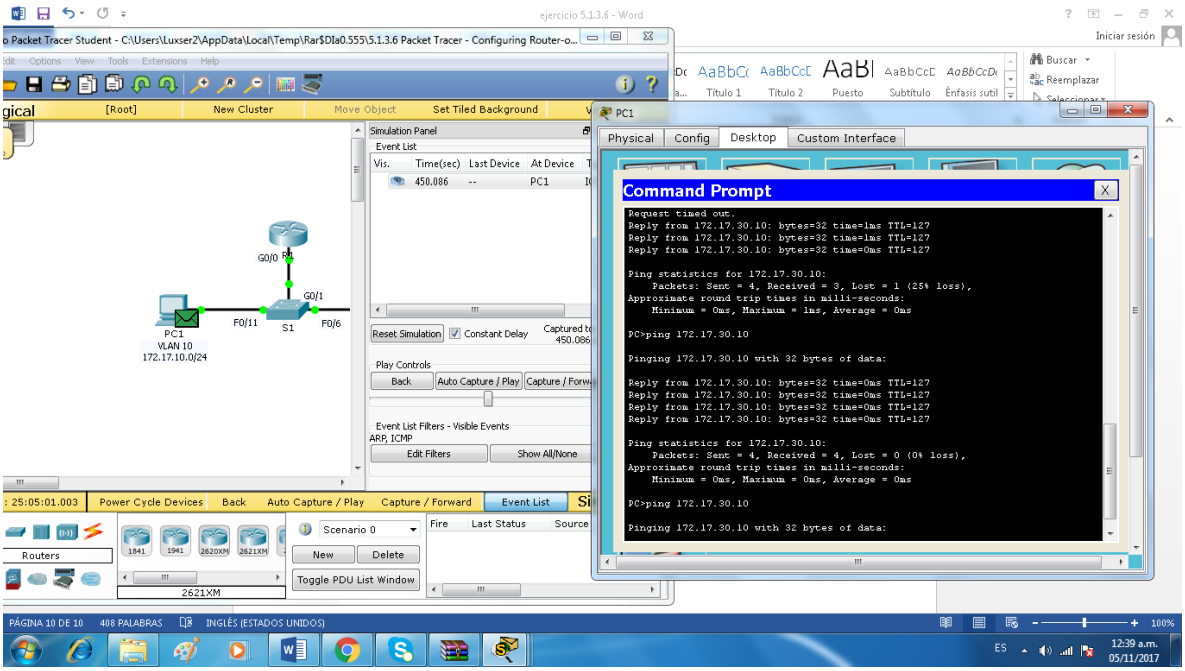


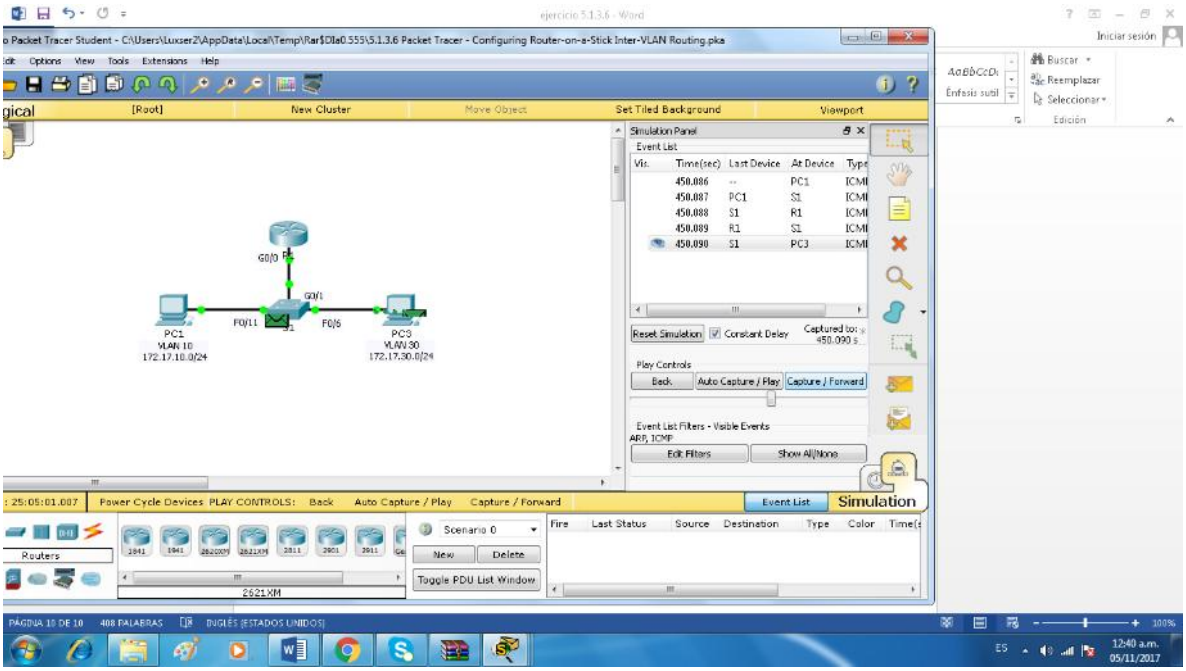


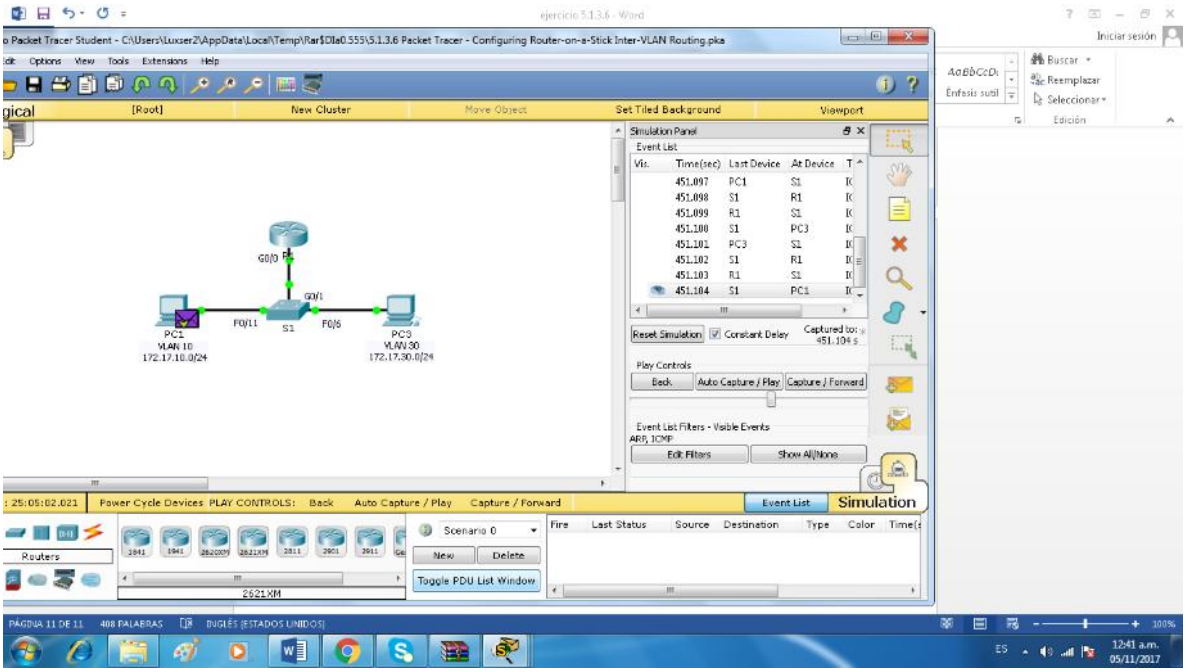
Step 3: Switch to Simulation mode to monitor pings.

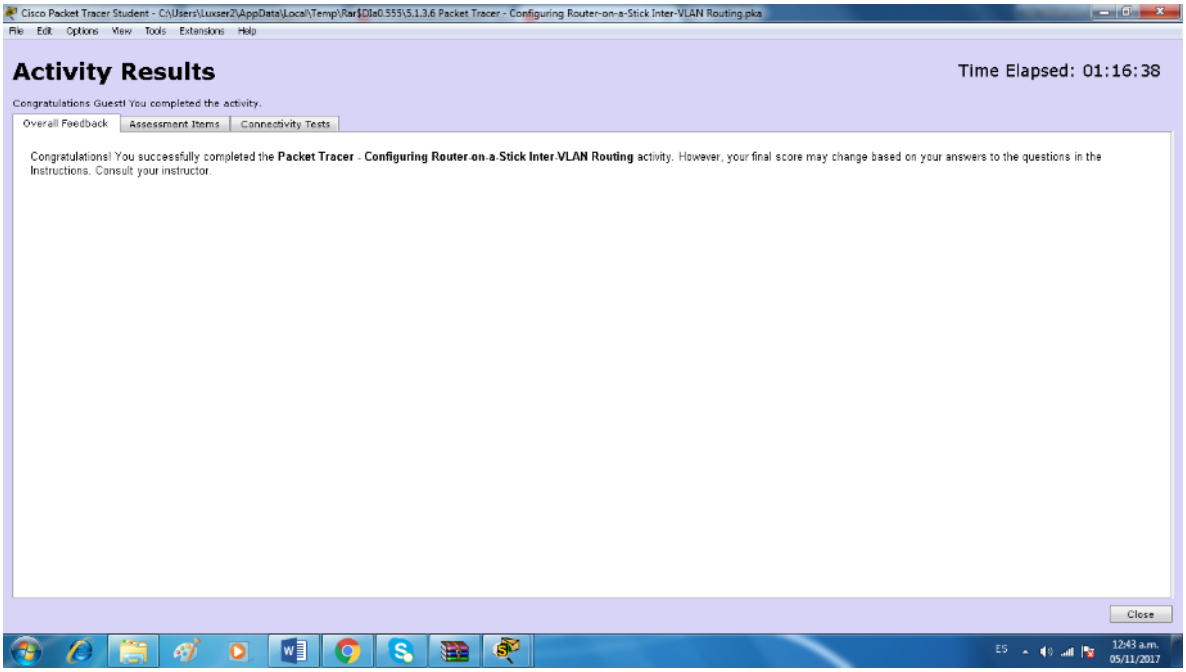
a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between**PC1** and **PC3**.


Command Prompt
Request timed out.
Reply from 172.17.30.10: bytes=32 time=1ms TTL=127
Reply from 172.17.30.10: bytes=32 time=1ms TTL=127
Reply from 172.17.30.10: bytes=32 time=0ms TTL=127
Ping statistics for 172.17.30.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 172.17.30.10
Pinging 172.17.30.10 with 32 bytes of data:
Reply from 172.17.30.10: bytes=32 time=0ms TTL=127
Reply from 172.17.30.10: bytes=32 time=0ms TTL=127
Reply from 172.17.30.10: bytes=32 time=0ms TTL=127
Reply from 172.17.30.10: bytes=32 time=0ms TTL=127
Ping statistics for 172.17.30.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 172.17.30.10
Pinging 172.17.30.10 with 32 bytes of data:



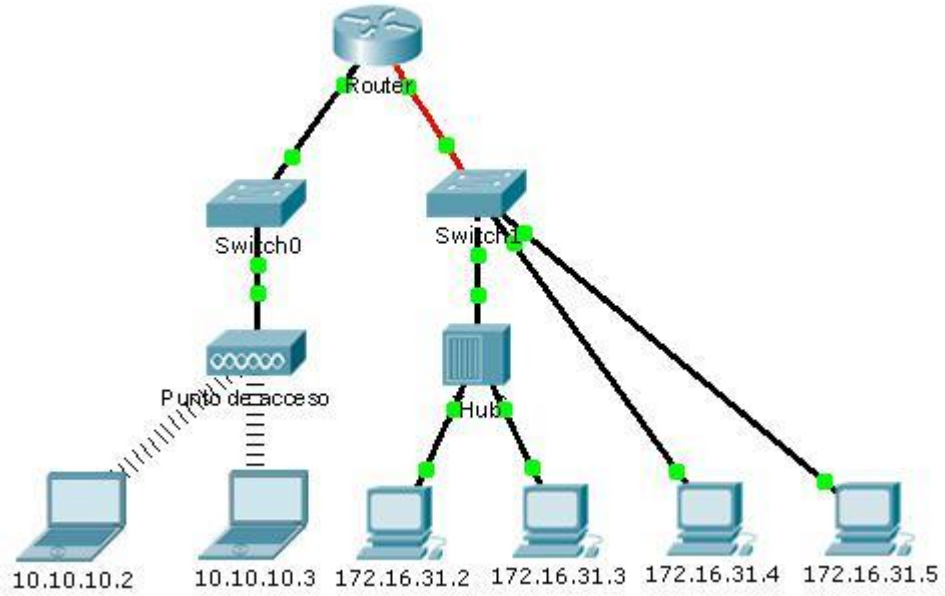




Ejercicio 5.1.4.4 Packet Tracer - Identify MAC and IP Addresses Instructions

Packet Tracer: Identificación de direcciones MAC y direcciones IP

Topología



Objetivos

Parte 1: Recopilar información de la PDU

Parte 2: Preguntas de reflexión

Información básica

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

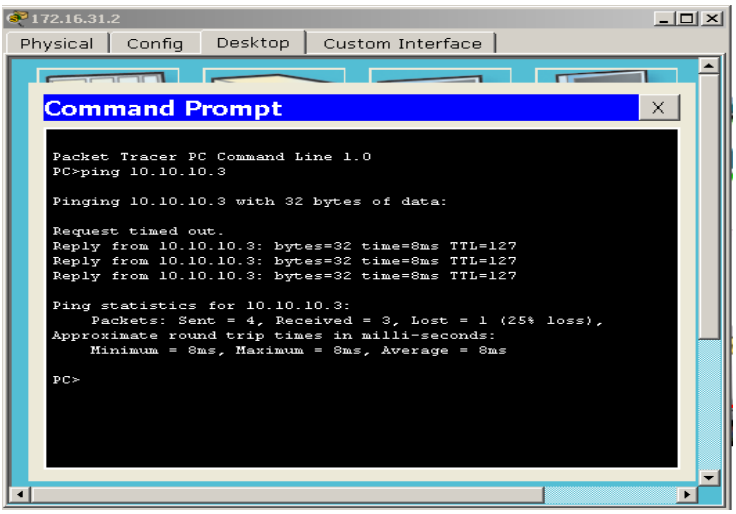
Parte 1: Recopilar información de la PDU

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

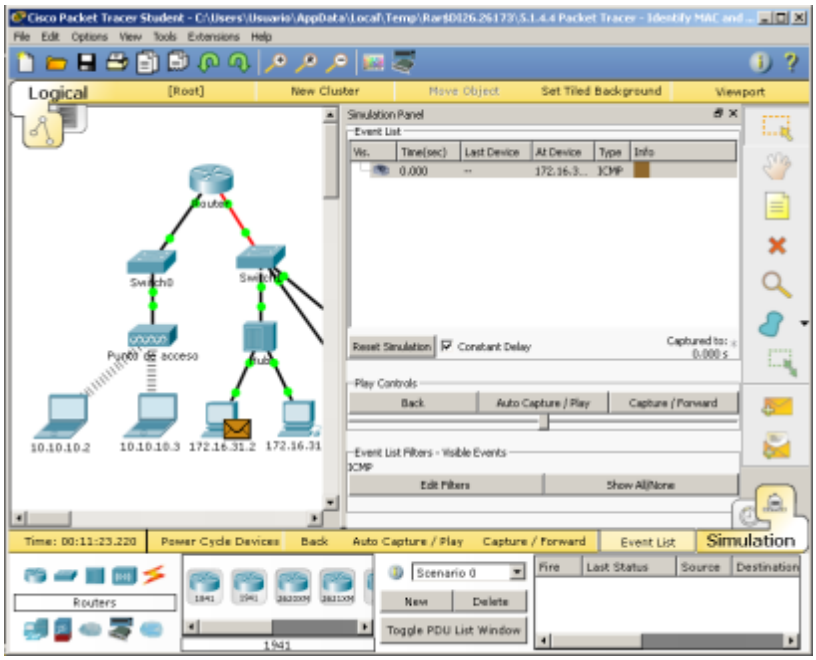
Paso 1: Recopilar información de la PDU mientras un paquete se transfiere de 172.16.31.2 a 10.10.10.3

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

b. Introduzca el comando **ping 10.10.10.3**.



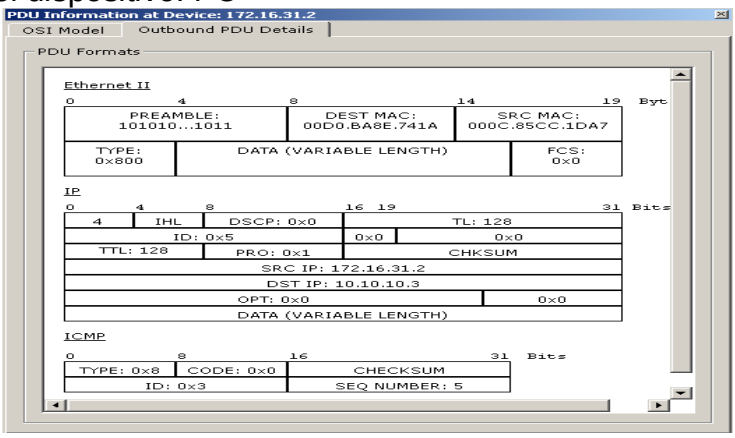
c. Cambie al modo de simulación y repita el comando **ping 10.10.10.3**. Aparece una PDU junto a **172.16.31.2**.



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

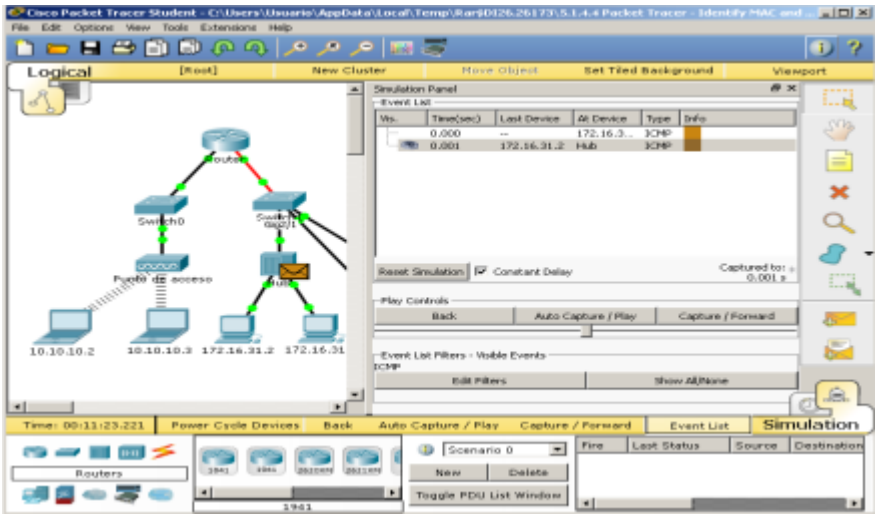
- Dirección MAC de destino: 00D0:BA8E:741A
- Dirección MAC de origen: 000C:85CC:1DA7
- Dirección IP de origen: 172.16.31.2
- Dirección IP de destino: 10.10.10.3

- En el dispositivo: PC



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

Se mueve el PDU al siguiente dispositivo.



Se verifica los valores del PDU en cada uno de los dispositivos mientras se hace el recorrido hasta llegar al final y se recolpilan los datos en la siguiente tabla.

Formato

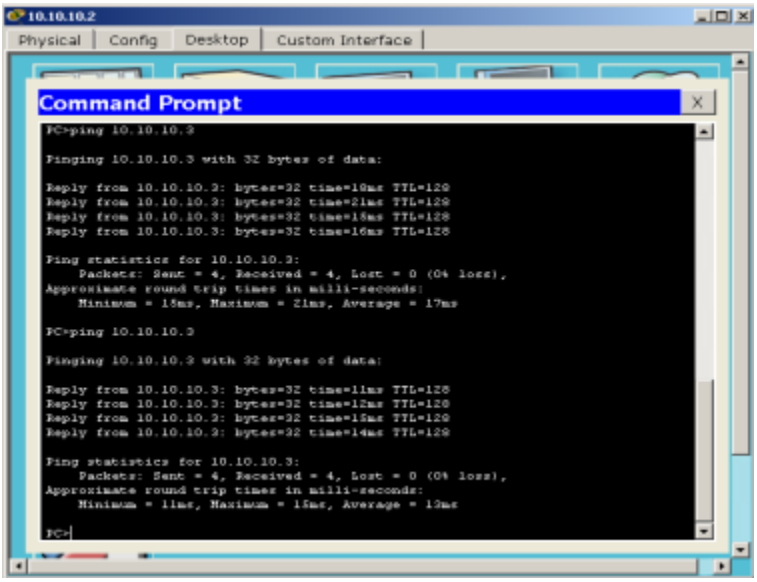
Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de	**172.16.31.2**	00D0:BA8E:	000C:85CC:	172.16.31.2	10.10.10.3

172.16.31.2 a 10.10.10.3		741A	1DA7		
	Hub	00D0:BA8E: 741A	000C:85CC: 1DA7	172.16.31.2	10.10.10.3
	Switch1	00D0:BA8E: 741A	000C:85CC: 1DA7	172.16.31.2	10.10.10.3
	Router	0060:4706:5 72B	00D0:588C: 2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:5 72B	00D0:588C: 2401	172.16.31.2	10.10.10.3
	Punto de acceso	0060.4706.5 72B	00D0.588C. 2401	172.16.31.2	10.10.10.3
	10.10.10.3	0060:4706:5 72B	00D0:588C: 2401	172.16.31.2	10.10.10.3

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

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

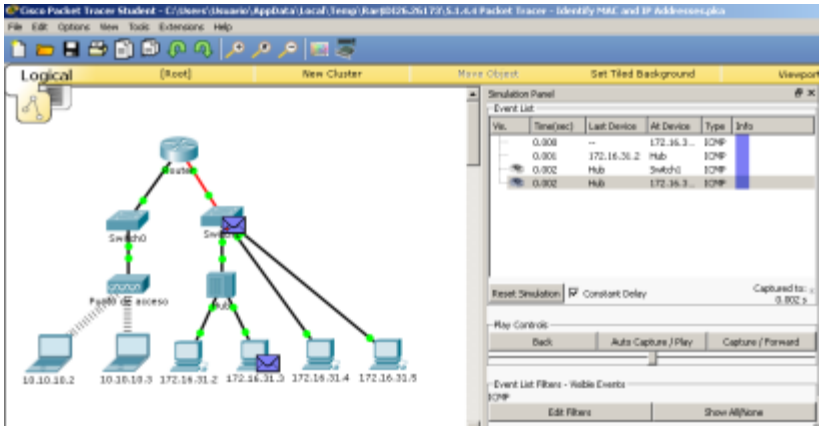
- **Ping de 10.10.10.2 a 10.10.10.3**



Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 10.10.10.2 a 10.10.10.3	**10.10.10.2**	0060.4706.5 72B	0060.2F84.4 AB6	10.10.10.2	10.10.10.3
	Punto de acceso	0060.4706.5 72B	0060.2F84.4 AB6	10.10.10.2	10.10.10.3
	10.10.10.3	0060.4706.5 72B	0060.2F84.4 AB6	10.10.10.3	10.10.10.2

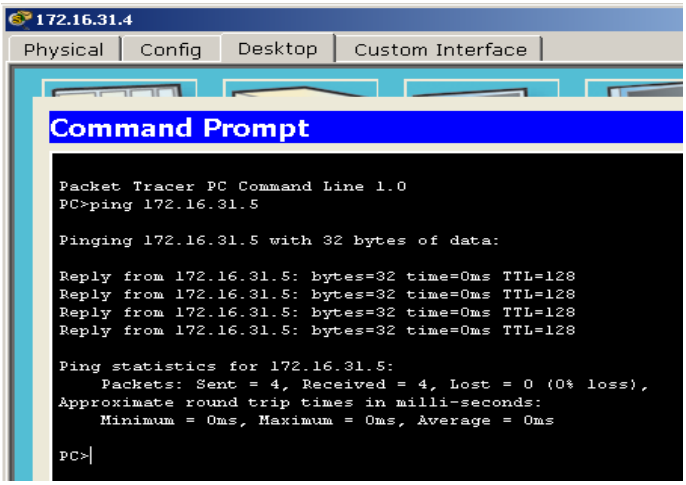
- **Ping de 172.16.31.2 a 172.16.31.3**

```
PC>
PC>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time=0ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms 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 = 0ms, Average = 0ms

PC>
```

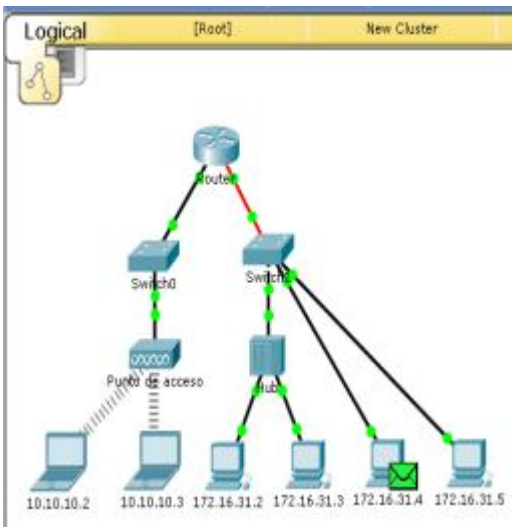


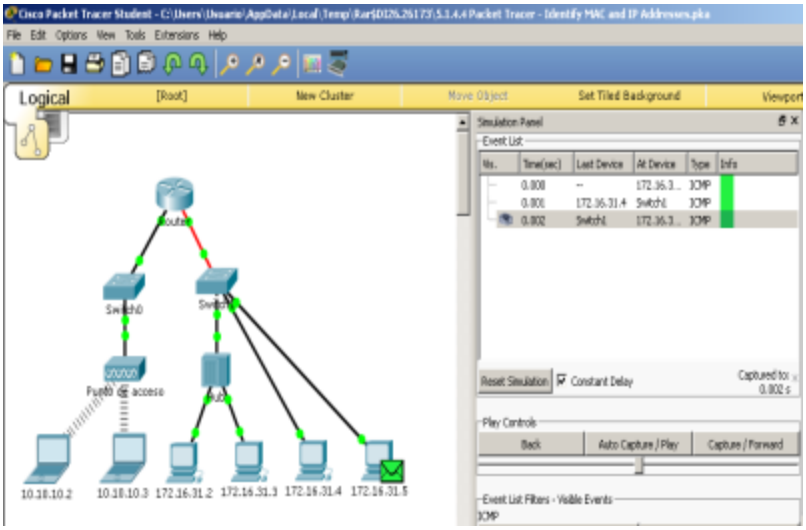
Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.2 a 172.16.31.3	**172.16.31.2**	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3
	Hub	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3
	172.16.13.3	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2

- **Ping de 172.16.31.4 a 172.16.31.5**

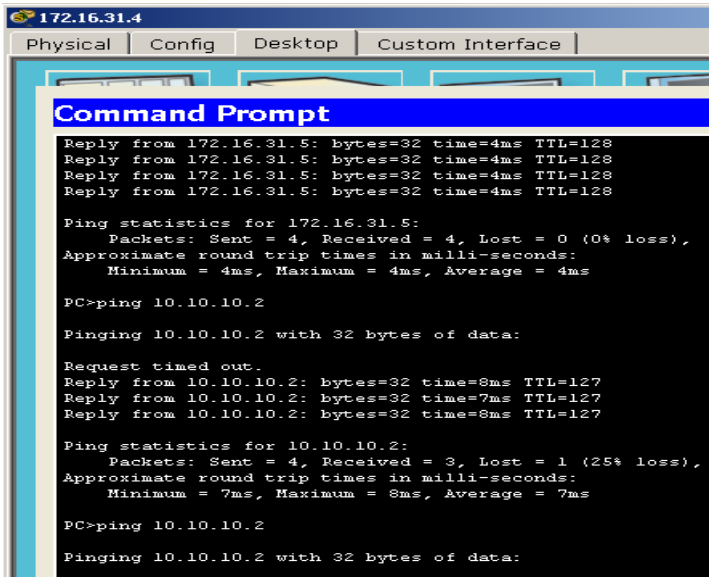


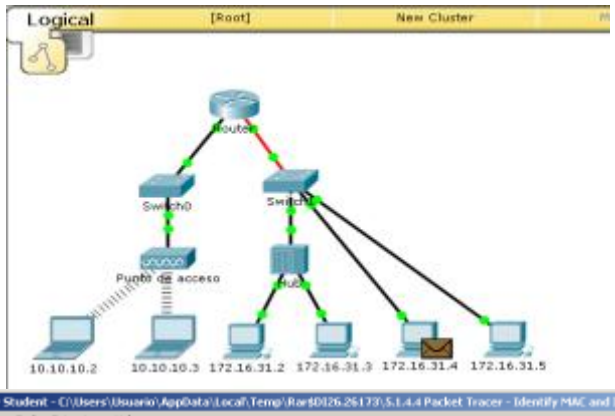
Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.4 a 172.16.31.5	**172.16.31.4**	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5
	Switch1	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5
	172.16.31.5	000C.CF0B.BC80	00D0.D311.C788	172.16.31.5	172.16.31.4

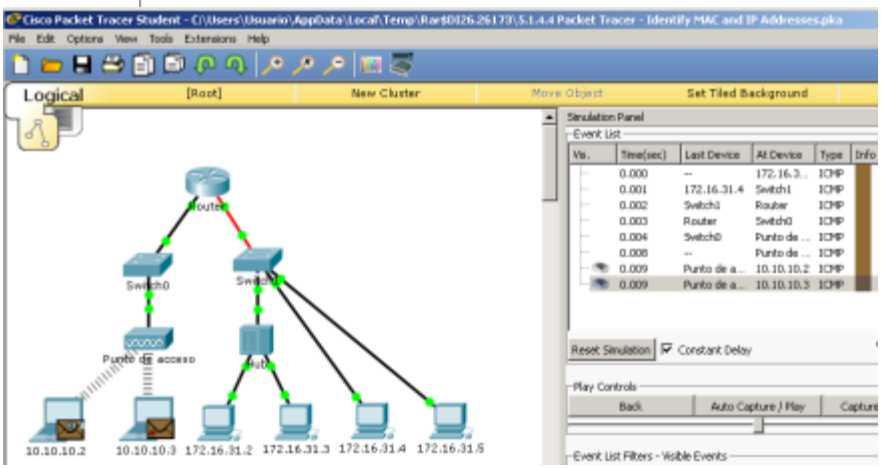




- **Ping de 172.16.31.4 a 10.10.10.2**



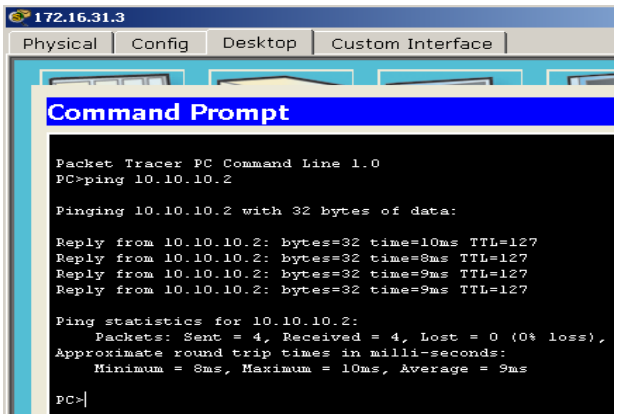


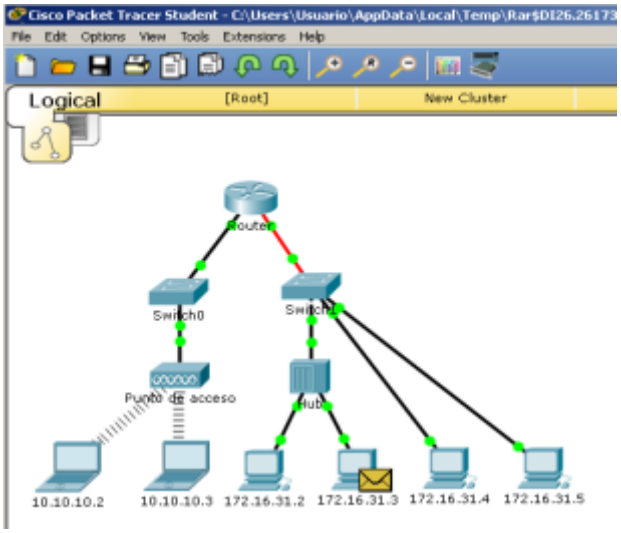


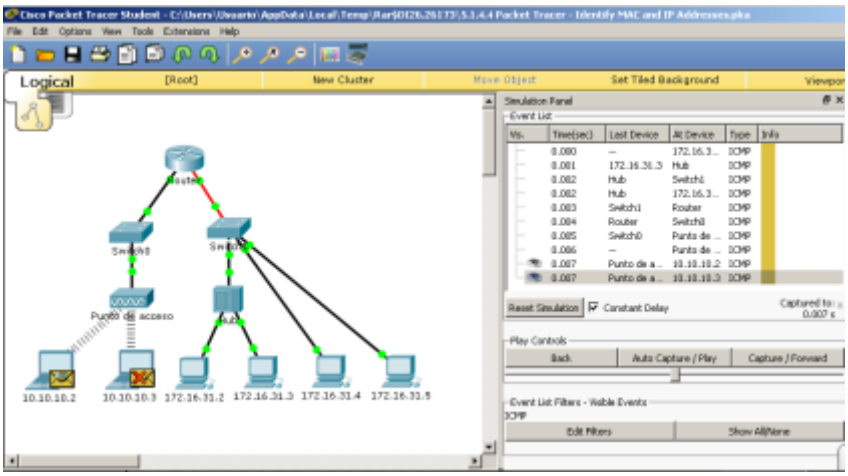
Prueba	En dispositivo	Dirección MAC	Src MAC	Src IPv4	Dest IPv4
Ping de 172.16.31.4 a 10.10.10.2	**172.16.31.4**	00D0.BA8E.741A	000C.CF0B.BC80	172.16.31.4	10.10.10.2
	Switch1	00D0.BA8E.	000C.CF0B.	172.16.31.4	10.10.10.2

		741A	BC80		
	Router	0060.2F84.4AB6	00D0.588C.2401	172.16.31.4	10.10.10.2
	Switch0	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Punto de acceso	0060.4706.572B	00D0.588C.2401	172.16.31.2	10.10.10.3
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.4

- **Ping de 172.16.31.3 a 10.10.10.2**







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

Parte 2: Preguntas de reflexión

Responda las siguientes preguntas relacionadas con la información reunida:

1. ¿Se utilizaron diferentes tipos de cables para conectar los dispositivos?
R/ Si de cobre y de fibra.

2. ¿Los cables cambiaron el manejo de la PDU de alguna forma?
R/ No

3. ¿El **hub** perdió la información que se le entregó?
R/ No

4. ¿Qué hace el **hub** con las direcciones MAC y las direcciones IP?
R/Nada

5. ¿El **punto de acceso inalámbrico** hizo algo con la información que se le entregó?
R/ Si lo volvió a empaquetar según el estándar inalámbrico 802.11

6. ¿Se perdió alguna dirección MAC o IP durante la transferencia inalámbrica?
R/ No
7. ¿Cuál fue la capa OSI más alta que utilizaron el **hub** y el **punto de acceso**?
R/ Capa 1

8. ¿El **hub** o el **punto de acceso** reprodujeron en algún momento una PDU rechazada con una "X" de color rojo?
R/ Si

9. Al examinar la ficha **PDU Details** (Detalles de PDU), ¿qué dirección MAC aparecía primero, la de origen o la de destino?
R/ La de destino

10. ¿Por qué las direcciones MAC aparecen en este orden?
R/ Porque de esta forma el Switch puede empezar a reenviar una trama a una dirección MAC conocida, más rápido.

11. ¿Había un patrón para el direccionamiento MAC en la simulación?
R/ No

12. ¿Los switches reprodujeron en algún momento una PDU rechazada con una "X" de color rojo?
R/Únicamente cuando tomaban rutas no especificadas.

13. Cada vez que se enviaba la PDU entre las redes 10 y 172, había un punto donde las direcciones MAC cambiaban repentinamente. ¿Dónde ocurrió eso?
R/ En el router

14. ¿Qué dispositivo utiliza las direcciones MAC que comienzan con 00D0?
R/ Switch, hub

15. ¿A qué dispositivos pertenecen las otras direcciones MAC?
R/ Al emisor y al receptor.

16. ¿Las direcciones IPv4 de envío y recepción cambian en alguna de las PDU?
R/ No

17. Si sigue la respuesta a un ping, a veces denominado *pong*, ¿las direcciones IPv4 de envío y recepción cambian?
R/ Si

18. ¿Cuál es el patrón para el direccionamiento IPv4 en esta simulación?
R/ Cada puerto de router requiere un conjunto de direcciones que no se superpongan.

19. ¿Por qué es necesario asignar diferentes redes IP a los diferentes puertos de un router?
R/Porque la función de un router es precisamente interconectar diferentes redes ip.

20. Si esta simulación fuera configurada con IPv6 en vez de IPv4, ¿cuál sería la diferencia?
R/ Las direcciones IPv4 se reemplazarían con las direcciones IPv6, lo demás sería igual.

Ejercicio 5.2.1.7 Packet Tracer - Examine the ARP Table Instructions

Packet Tracer: Revisión de la tabla ARP

Topología

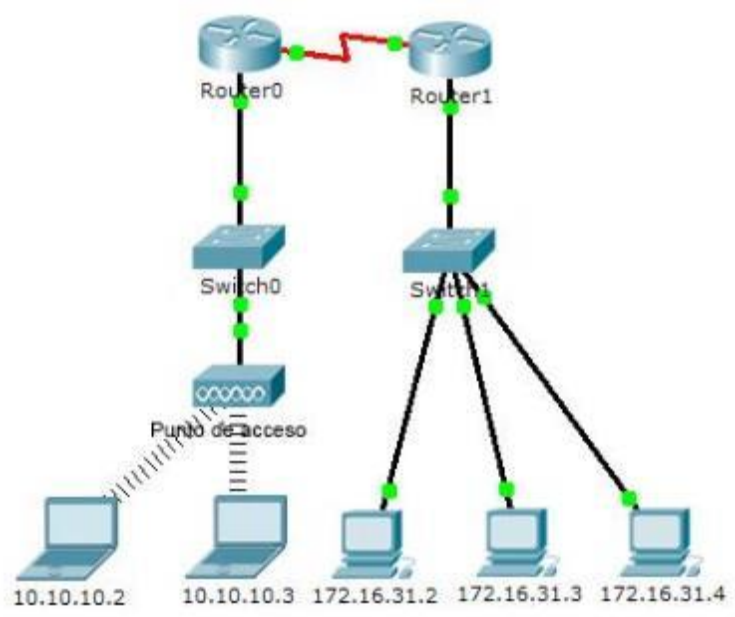


Tabla de direccionamiento

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

10.10.10.2.	Inalámbrico	0060.2F84.4AB6	Fa0/2
10.10.10.3	Inalámbrico	0060.4706.572B	Fa0/2
172.16.31.2	Fa0	000C.85CC.1DA7	Fa0/1
172.16.31.3	Fa0	0060.7036.2849	Fa0/2
172.16.31.4	Gig0	0002.1640.8D75	Fa0/3

Objetivos

Parte 1: Examinar una solicitud de ARP

Parte 2: Examinar una tabla de direcciones MAC del switch

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Información básica

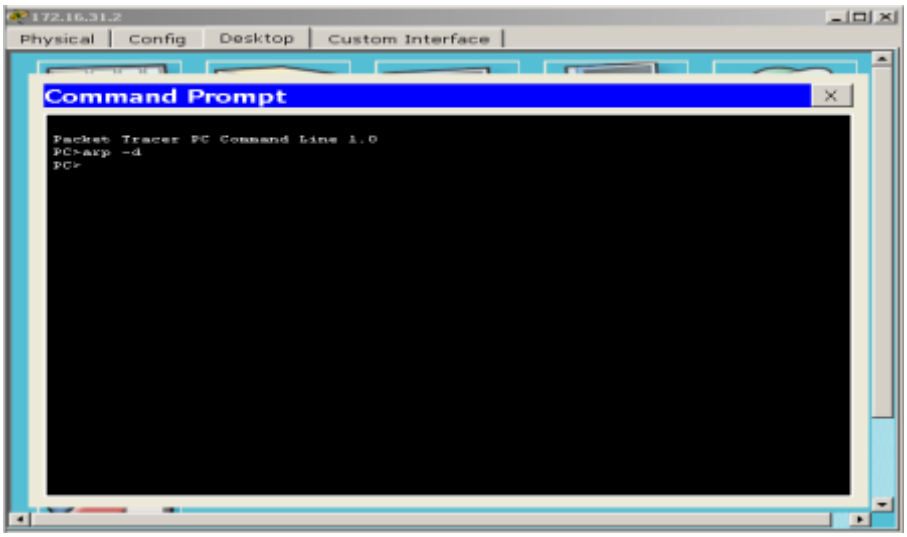
Esta actividad está optimizada para la visualización de PDU. Los dispositivos ya están configurados. Recopilará información de PDU en el modo de simulación y responderá una serie de preguntas sobre los datos que obtenga.

Parte 1: Examinar una solicitud de ARP

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

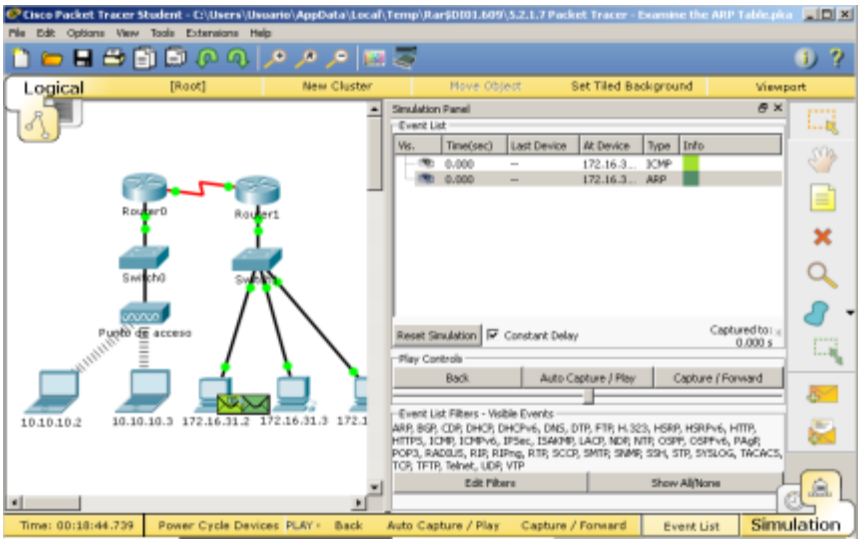
b Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

c Introduzca el comando **arp -d** para borrar la tabla ARP.
Se realiza paso a y paso b. Ingresamos al equipo 132.16.31.2, y se ejecuta el comando **arp –d** para borrar tabla arp anterior.



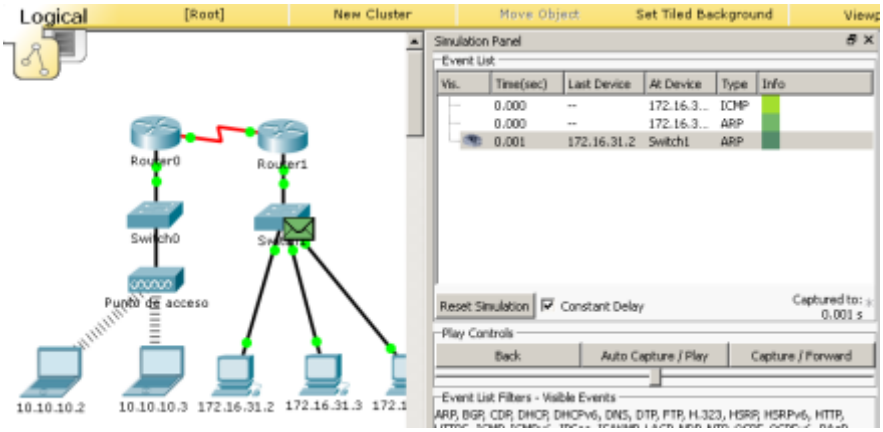
d Ingrese al modo **Simulation** (Simulación) e introduzca el comando **ping 172.16.31.3**. Se generan dos PDU. El comando **ping** no puede completar el paquete ICMP sin conocer la dirección MAC del destino. Por lo tanto, la PC envía una trama de broadcast de ARP para hallar la dirección MAC del destino.

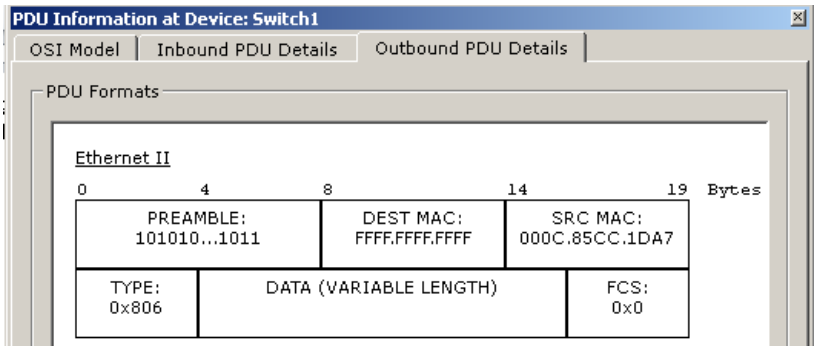
//Se ingresa al modo simulación y en la consola abierta anteriormente ejecutamos el comando **ping 172.16.31.3** como se indica en el documento base**. //**



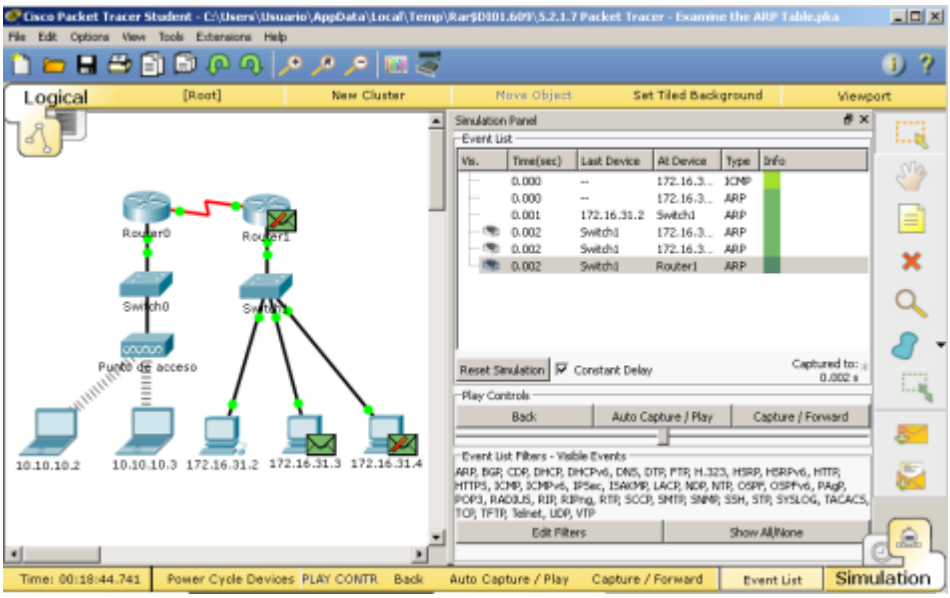
e Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. La PDU ARP mueve el **Switch1**, mientras que la PDU ICMP desaparece y espera la respuesta de ARP. Abra la PDU y registre la dirección MAC de destino. ¿Esta dirección se indica en la tabla anterior? **R/ No.**

//Direccion MAC de destino: FFFF.FFFF.FFFF //





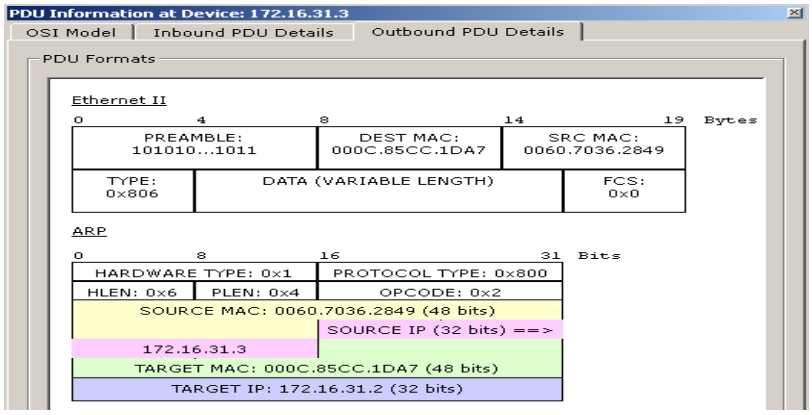
f Haga clic en **Capture/Forward** (Capturar/avanzar) para mover la PDU al siguiente dispositivo. ¿Cuántas copias de la PDU realizó el **Switch1**? **R/ 3**



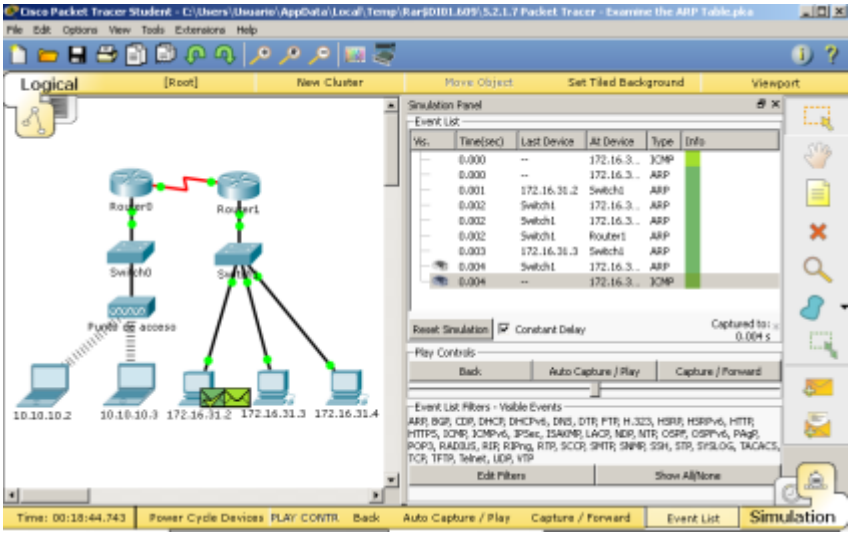
g ¿Cuál es la dirección IP del dispositivo que aceptó la PDU? **R/ 172.16.31.3**

h Abra la PDU y examine la capa 2. ¿Qué sucedió con las direcciones MAC de origen y destino?

R/ La dirección MAC de origen corresponde en esta instancia a la **0060.7036.2849** no identificada anteriormente sino que se especificada como **FFFF.FFFF.FFFF.** y la dirección MAC de destino pasa a ser la **000C.85CC.1DA7** identificada en la operación anterior como dirección MAC de origen, dado que en este punto el PDU inicia su viaje de regreso en estado de respuesta.

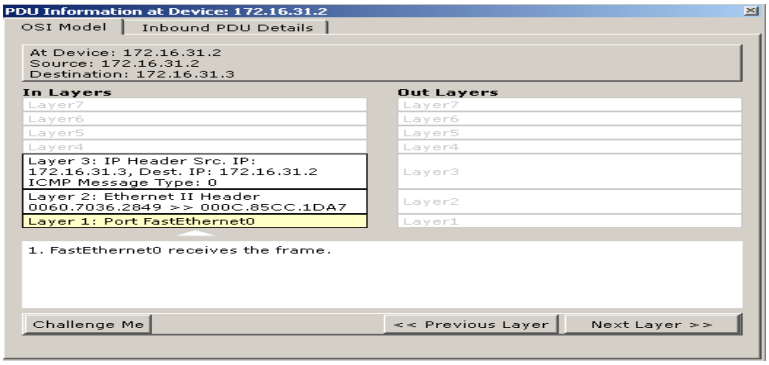


i Haga clic en **Capture/Forward** hasta que la PDU regrese a **172.16.31.2**. ¿Cuántas copias de la PDU realizó el switch durante la respuesta de ARP? **R/ 1 PDU**



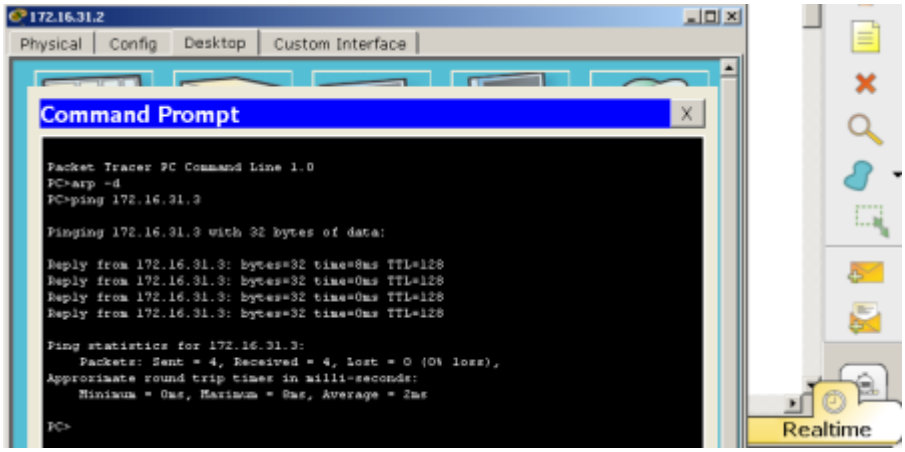
Paso 2: Revisar la tabla ARP

e. 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? **R/ Si coinciden.**

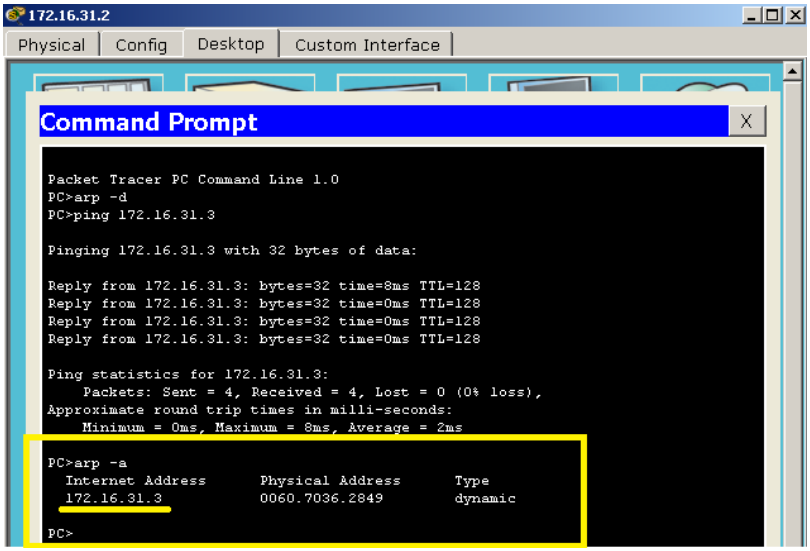


f. Vuelva a cambiar al modo **Realtime** (Tiempo real), y el ping se completa.

Ping completado



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

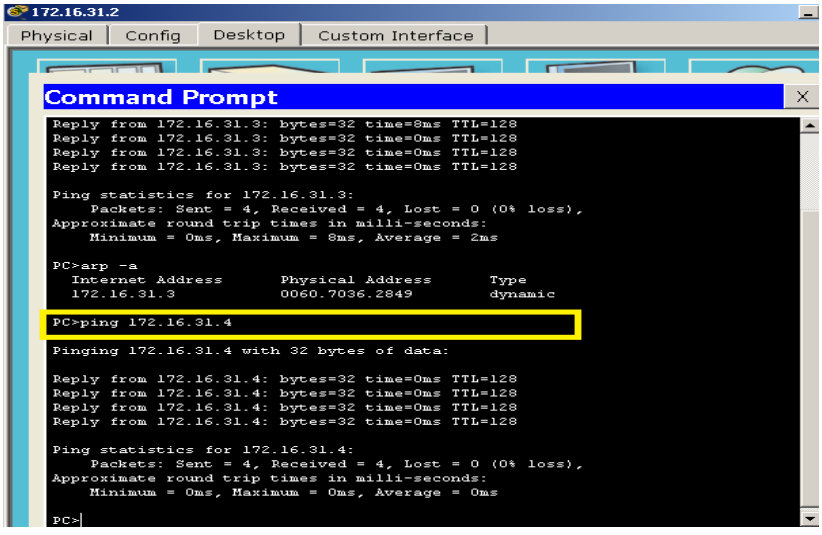


h. En general, ¿cuándo emite un dispositivo final una solicitud de ARP? **R/ Cuando no es conocida la dirección MAC del receptor.**

Parte 2: Examinar una tabla de direcciones MAC del switch

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

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



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

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

R/ Fueron enviadas 4 respuestas y recibidas las mismas 4 como se logra evidenciar en la imagen a continuación.

```
PC>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time=25ms TTL=128
Reply from 10.10.10.3: bytes=32 time=14ms TTL=128
Reply from 10.10.10.3: bytes=32 time=16ms TTL=128
Reply from 10.10.10.3: bytes=32 time=16ms TTL=128

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 25ms, Average = 17ms

PC>
```

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

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

R/Si corresponde, a continuación lo podemos evidenciar.

```
          Mac Address Table
-------------------------------------------

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

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

- 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?

R/Si corresponde, también podemos evidenciarlo a continuación.

```
          Mac Address Table
-------------------------------------------

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

   1    0001.6458.2501    DYNAMIC     Gig0/1
Switch0>
```

- ¿Por qué hay dos direcciones MAC asociadas a un puerto**?**

R/Es permitido que varias direcciones MAC se conecten a un mismo puerto eso dependen de la configuración. Y para este caso ambos

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

Parte 3: Examinar el proceso de ARP en comunicaciones remotas

Paso 1: Generar tráfico para producir tráfico ARP

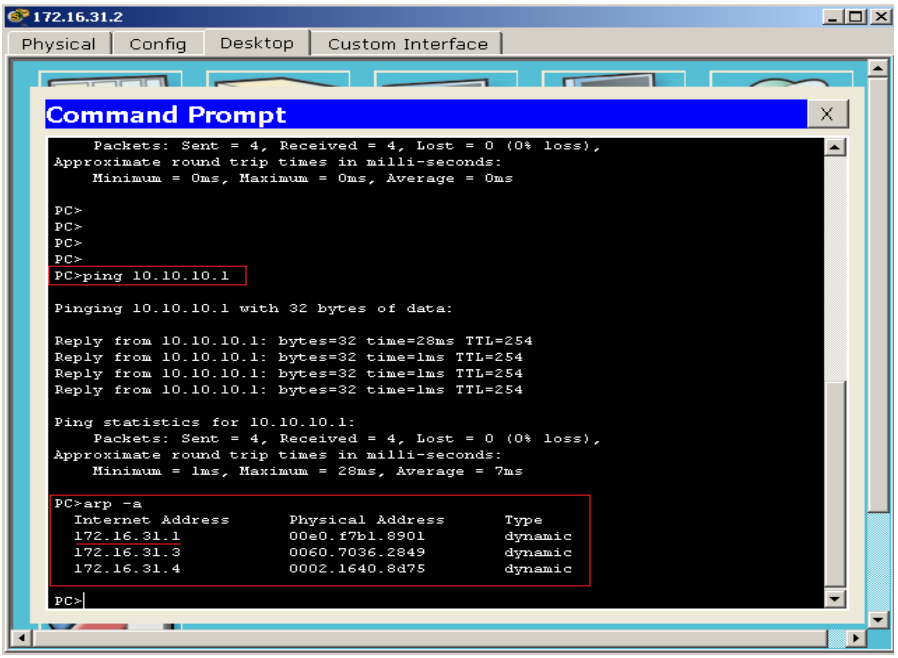
7. Haga clic en **172.16.31.2** y abra el **símbolo del sistema**.

8. Introduzca el comando **ping 10.10.10.1**.

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

R/ 172.16.31.1

Se realizan los encisos a, b y c. Como se puede evidenciar en la imagen, estamos desde la pc con ip 172.16.21.2 y se realiza un ping a la 10.10.10.1 a lo que se genera una respuesta positiva de comunicación entre los dispositivos. A continuación con el comando arp –a verificamos las direcciones registradas en la tabla ARP.

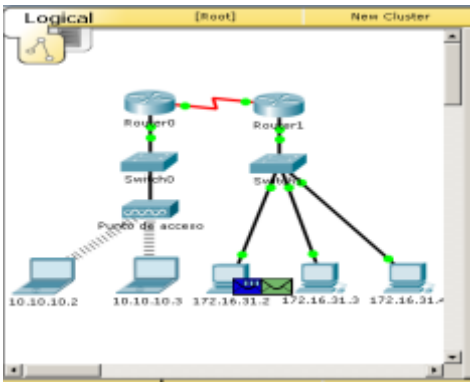


10. Introduzca el comando **arp -d** para borrar la tabla ARP y volver a cambiar al modo de **simulación**.

// se realiza el proceso/

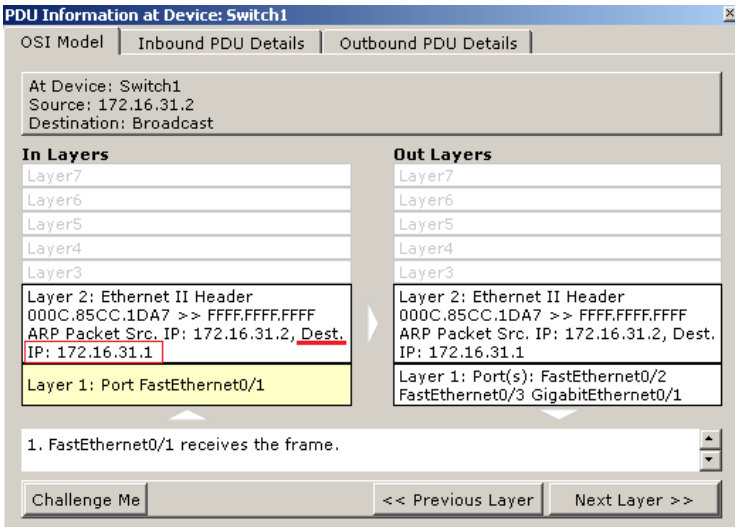
11. Repita el ping a 10.10.10.1. ¿Cuántas PDU aparecen?

R/ Aparecen 2 PDU, se puede evidenciar en la siguiente imagen.



12. 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?

R/ Tal como se muestra en la imagen podemos observar que la IP de destino de la solicitud de ARP corresponde a la 172.16.31.1



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

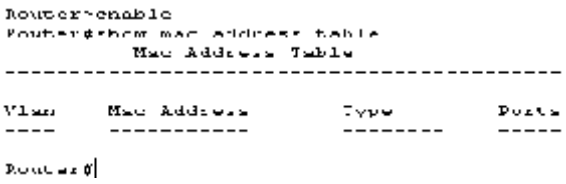
Porque la dirección de Gateway de interfaz de router se almacena en la configuración IPv4 de los host. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de Gateway.

Paso 2: Examinar la tabla ARP en el Router1

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

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

Como se nuestra a continuación no aparece ninguna dirección MAC en la tabla. Dado que el comando show mac-address-table no corresponde a un comando asignado al router sino a los switch para permitir visulizar información correspondiente a las direcciones MAC que figuran en el informe de tabla ARP.



23. Introduzca el comando **show arp**. ¿Figura una entrada para **172.16.31.2**? **R/ Si figura la entrada a la que se hace mención.**

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.31.1             -   00E0.F7B1.8901  ARPA   GigabitEthernet0/0
Internet  172.16.31.2            52   000C.85CC.1DA7  ARPA   GigabitEthernet0/0
Router#
```

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

R/ Excede el tiempo de espera.

6.2.2.5 Lab - Configuring IPv4 Static and Default Routes

Práctica de laboratorio: configuración de rutas estáticas y predeterminadas IPv4

Ingrid yalile Rodriguez

Topología

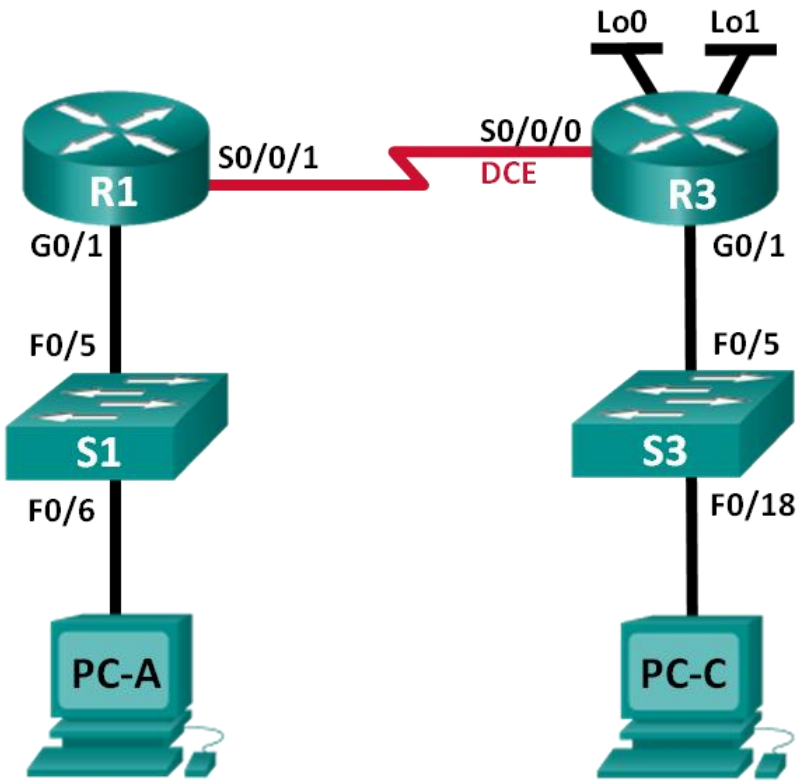


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los parámetros básicos de los dispositivos y verificar la conectividad

Parte 3: configurar rutas estáticas

- Configurar una ruta estática recursiva.
- Configurar una ruta estática conectada directamente.
- Configurar y eliminar rutas estáticas.

Parte 4: configurar y verificar una ruta predeterminada

Información básica/situación

Un router utiliza una tabla de enrutamiento para determinar a dónde enviar los paquetes. La tabla de routing consta de un conjunto de rutas que describen el gateway o la interfaz que el router usa para llegar a una red especificada. Inicialmente, la tabla de routing contiene solo redes conectadas directamente. Para comunicarse con redes distantes, se deben especificar las rutas, que deben agregarse a la tabla de routing.

En esta práctica de laboratorio, configurará manualmente una ruta estática a una red distante especificada sobre la base de una dirección IP del siguiente salto o una interfaz de salida. También configurará una ruta estática predeterminada. Una ruta predeterminada es un tipo de ruta estática que especifica el gateway que se va a utilizar cuando la tabla de routing no incluye una ruta para la red de destino.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

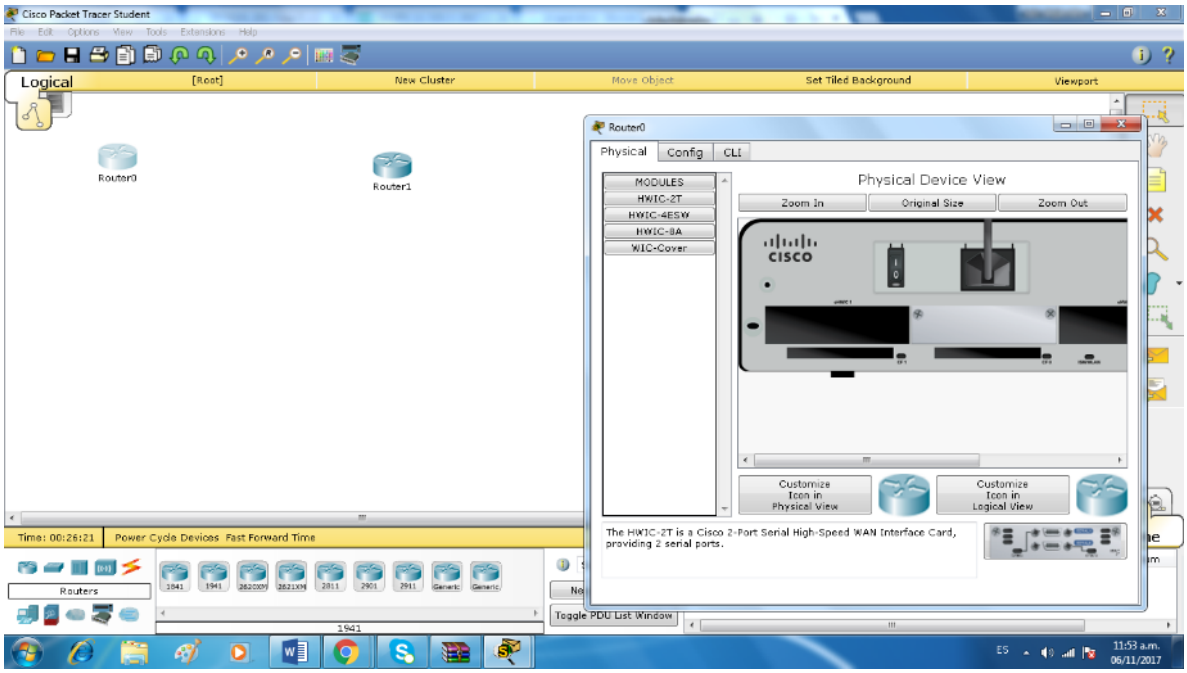
Recursosnecesarios

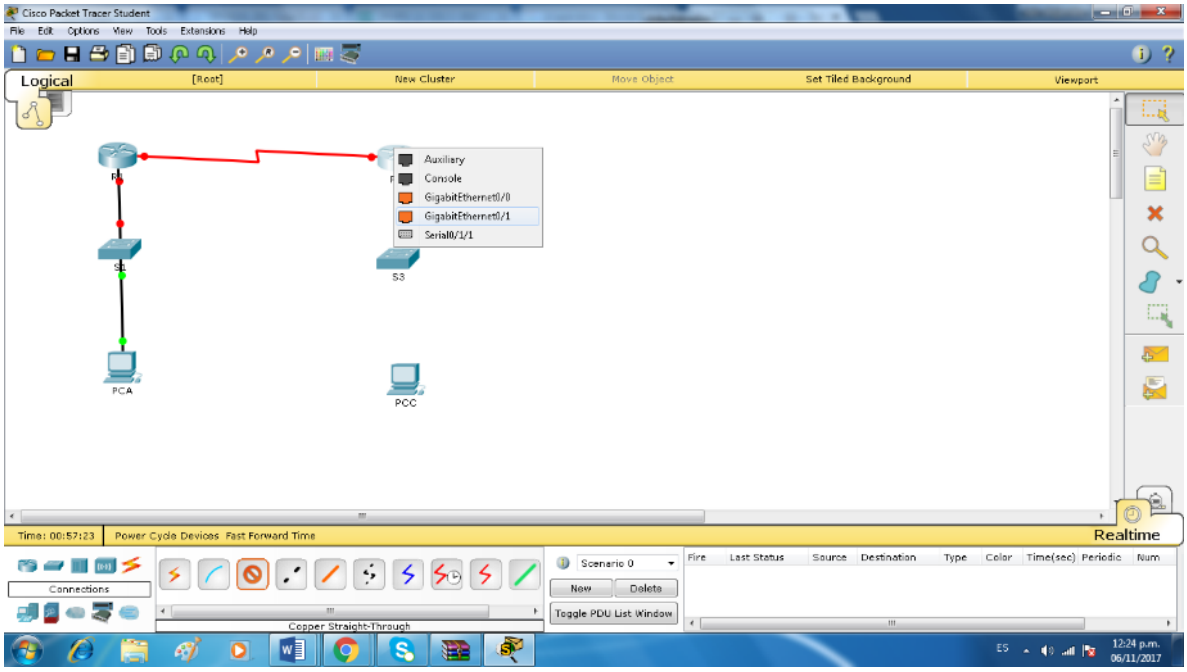
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1. establecer la topología e inicializar los dispositivos

Paso 1. realizar el cableado de red tal como se muestra en la topología.

Paso 2. inicializar y volver a cargar el router y el switch.

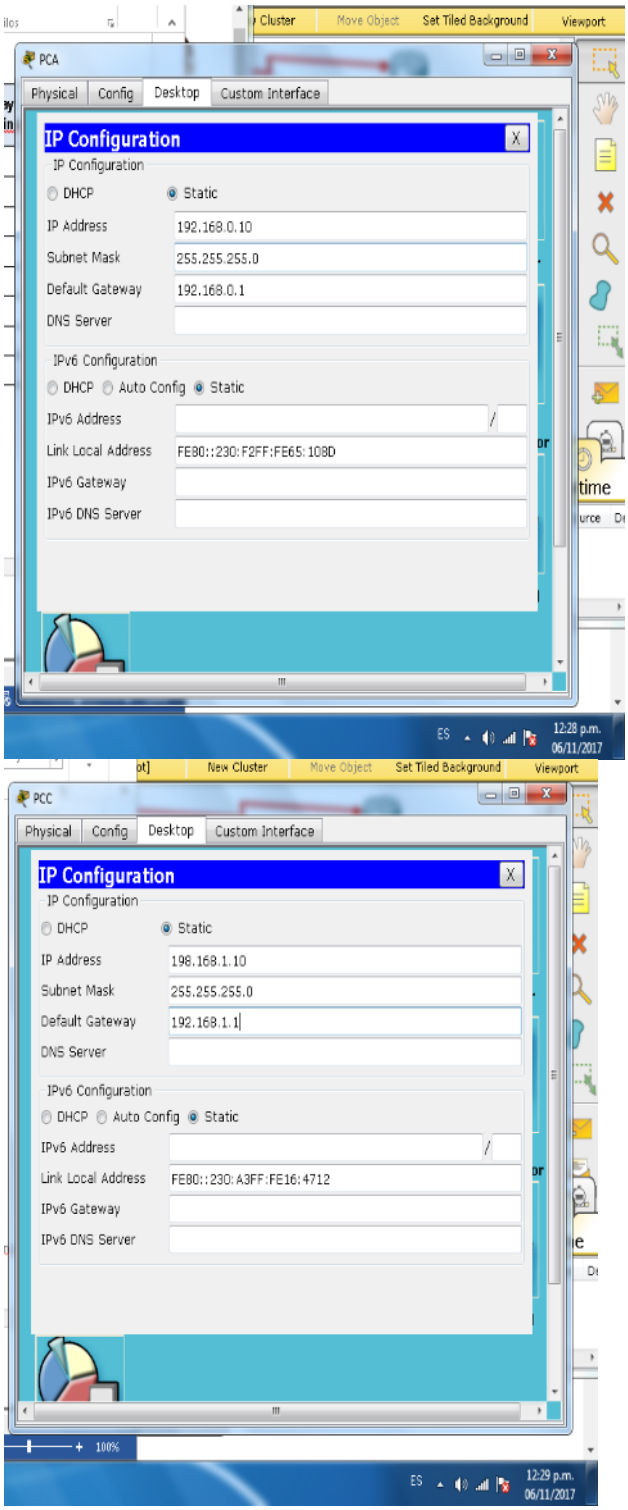




Parte 2. configurar los parámetros básicos de los dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos, como las direcciones IP de interfaz, el acceso a dispositivos y las contraseñas. Verificará la conectividad LAN e identificará las rutas que se indican en las tablas de routing del R1 y el R3.

Paso 1. Configure las interfaces de la PC.



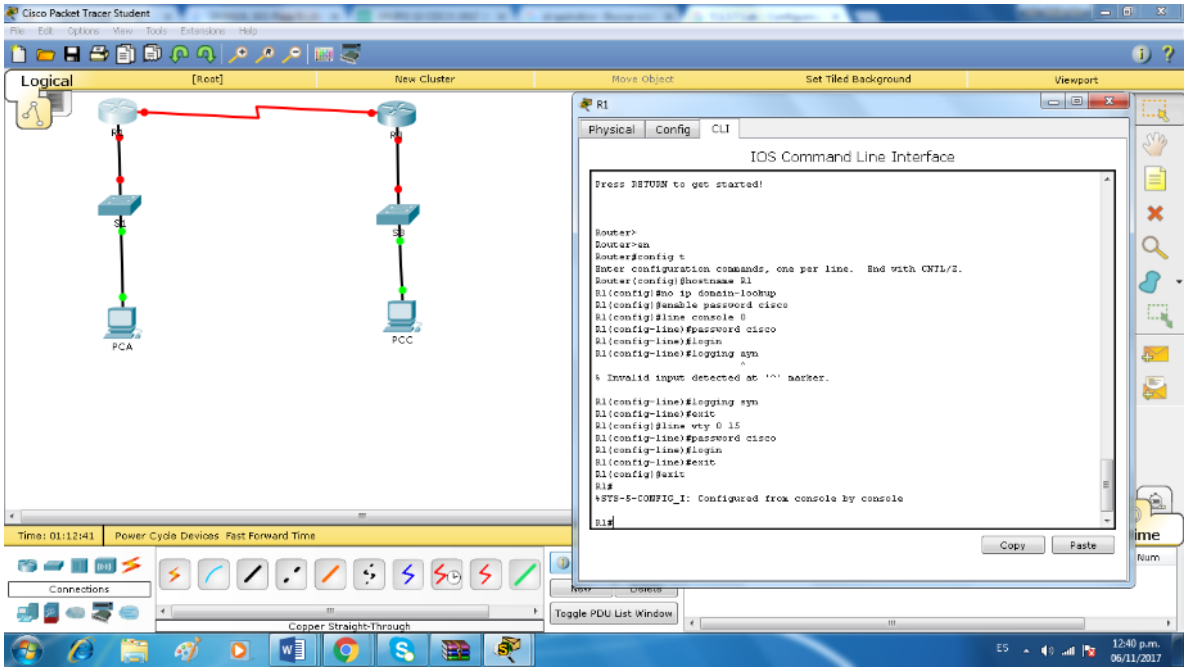
Paso 2. configurar los parámetros básicos en los routers.

a. Configure los nombres de los dispositivos, como se muestra en la topología y en la tabla de direccionamiento.

b. Desactive la búsqueda del DNS.

c. Asigne**class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.

d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

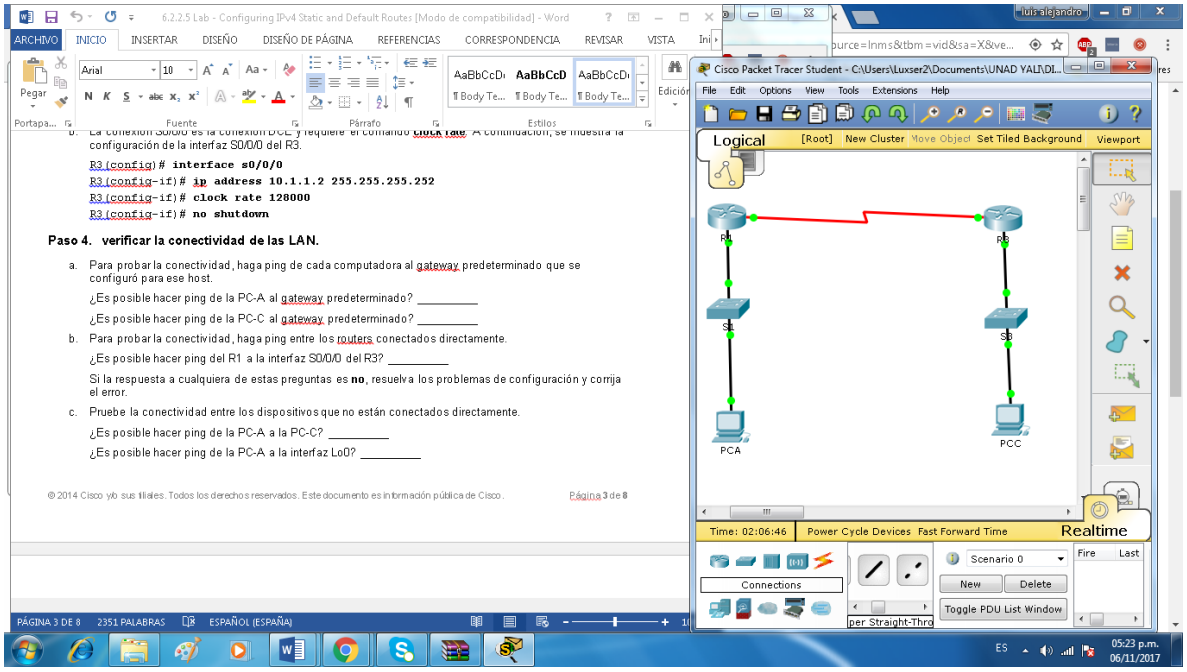
e. 

Paso 3. configurar los parámetros IP en los routers.

a. Configure las interfaces del R1 y el R3 con direcciones IP según la tabla de direccionamiento.

b. La conexión S0/0/0 es la conexión DCE y requiere el comando **clockrate**. A continuación, se muestra la configuración de la interfaz S0/0/0 del R3.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```



Paso 4. verificar la conectividad de las LAN.

a. Para probar la conectividad, haga ping de cada computadora al gateway predeterminado que se configuró para ese host.

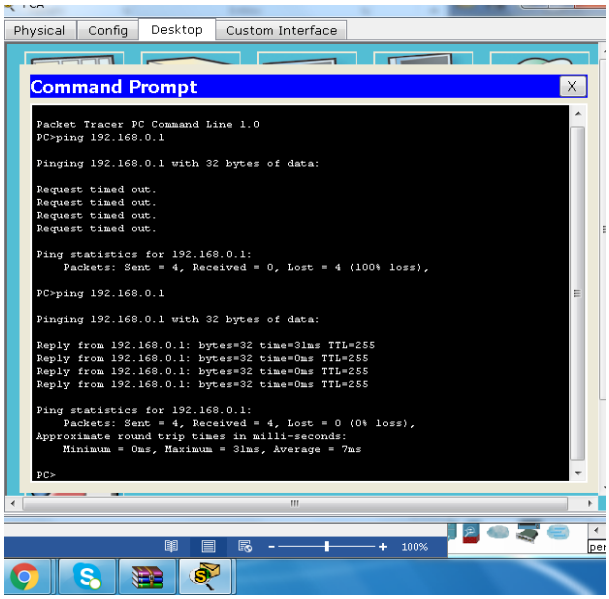
¿Es posible hacer ping de la PC-A al gateway predeterminado? __si_____

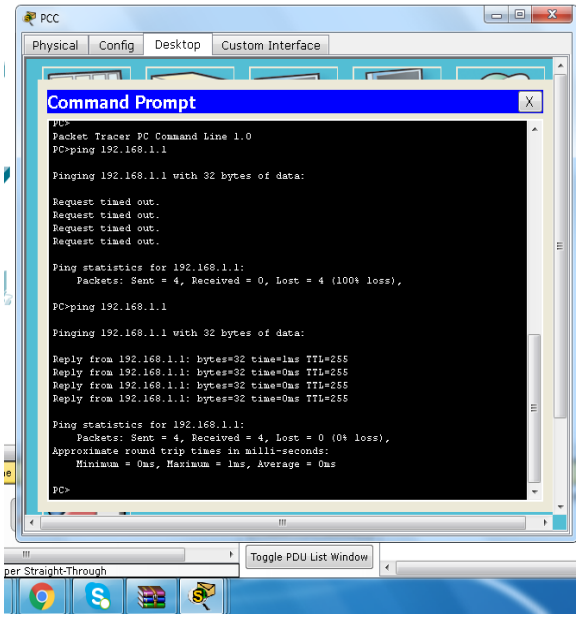
¿Es posible hacer ping de la PC-C al gateway predeterminado? ___si____

b. Para probar la conectividad, haga ping entre los routers conectados directamente.

¿Es posible hacer ping del R1 a la interfaz S0/0/0 del R3? ___si_____

Si la respuesta a cualquiera de estas preguntas es **no**, resuelva los problemas de configuración y corrija el error.





c. Pruebe la conectividad entre los dispositivos que no están conectados directamente.

¿Es posible hacer ping de la PC-A a la PC-C? __no_____

¿Es posible hacer ping de la PC-A a la interfaz Lo0? __no___

¿Es posible hacer ping de la PC-A a la interfaz Lo1? __no_____

¿Los pings eran correctos? ¿Por qué o por qué no?

____**porque no se está configurada la conexión entre estos dispositivos**._____

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

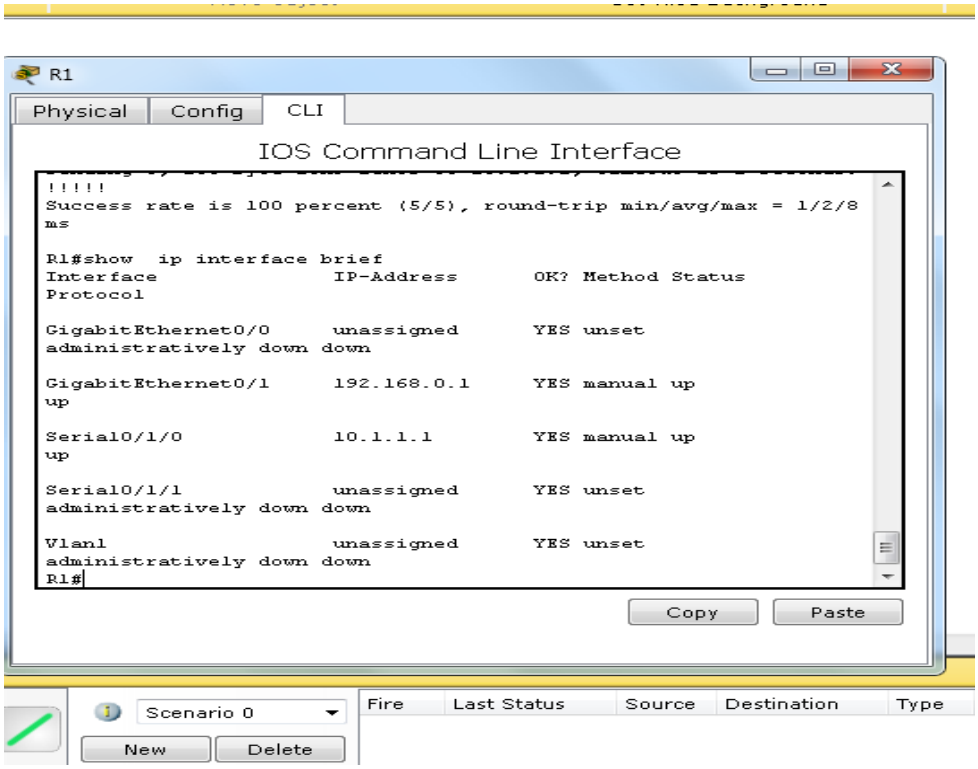
Paso 5. reunirinformación.

a. Revise el estado de las interfaces en el R1 con el comando **show ip interface brief**.

¿Cuántas interfaces están activadas en el R1? ___2___

b. Revise el estado de las interfaces en el R3.

¿Cuántas interfaces están activadas en el R3? __4__



c. Vea la información de la tabla de routing del R1 con el comando **show iproute**.

¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la **tabla de routing del R1?**

192.168.1.1
209.165.200.225
198.133.219.1

_____

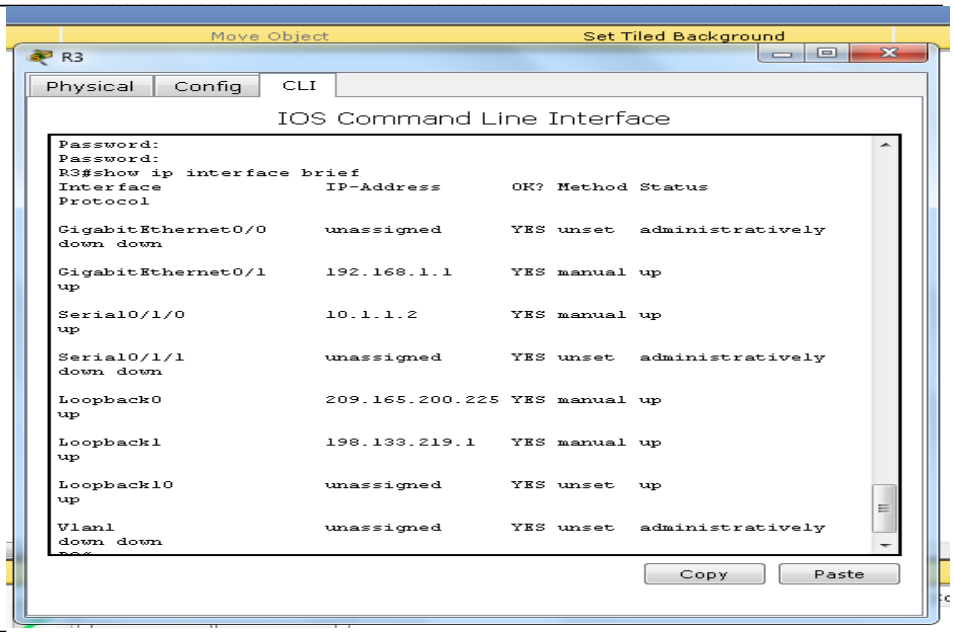
d. Vea la información de la tabla de routing para el R3.

¿Qué redes están presentes en la tabla de direccionamiento de esta práctica de laboratorio, pero no en la tabla de routing del R3?

_____**192.168.0.0**_____

¿Por qué ninguna de las redes está presente en las tablas de enrutamiento para cada uno de los routers?

Porque los Routers solo conocen la red que se conectó directamente a ellos._____



_____

Parte 3. Configure las rutas estáticas.

En la parte 3, empleará varias formas de implementar rutas estáticas y predeterminadas, confirmará si las rutas se agregaron a las tablas de routing del R1 y el R3, y verificará la conectividad sobre la base de las rutas introducidas.

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Paso 1. Configure una ruta estática recursiva.

Con una ruta estática recursiva, se especifica la dirección IP del siguiente salto. Debido a que solo se especifica la IP de siguiente salto, el router tiene que hacer varias búsquedas en la tabla de routing antes de reenviar paquetes. Para configurar rutas estáticas recursivas, utilice la siguiente sintaxis:

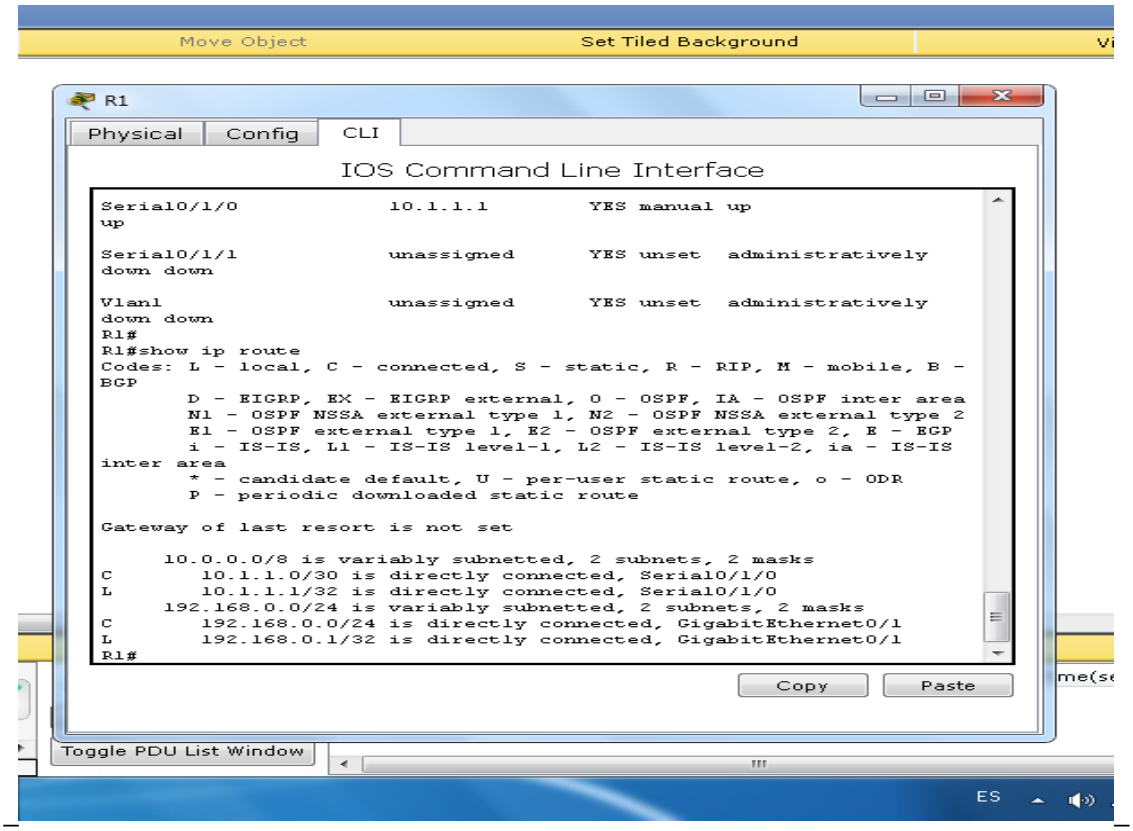
```
Router(config)# iproute dirección-redmáscara-subreddirección-ip
```

a. En el router R1, configure una ruta estática a la red 192.168.1.0 utilizando la dirección IP de la interfaz serial 0/0/0 del R3 como la dirección de siguiente salto. En el espacio proporcionado, escriba el comando que utilizó.

_R1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2_____

b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

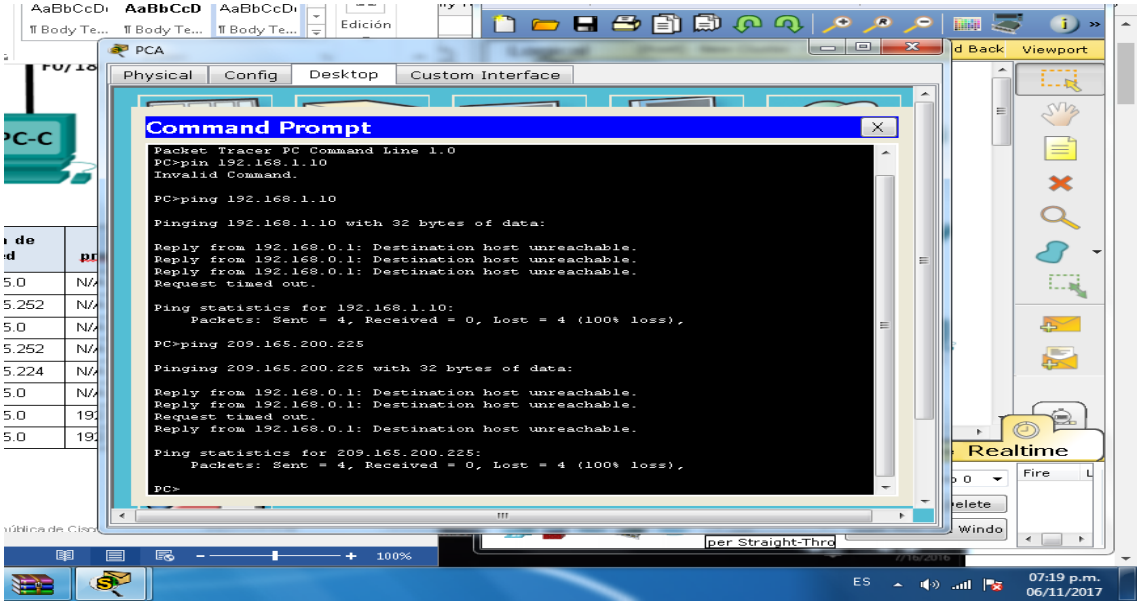
¿Cómo se indica esta ruta nueva en la tabla de routing?



_____

¿Es posible hacer ping del host PC-A host a al host PC-C? _no_____

Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, este ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 192.168.0.0 en la tabla de routing.



Paso 2. configurar una ruta estática conectada directamente.

Con una ruta estática conectada directamente, se especifica el parámetro *interfaz-salida*, que permite que el router resuelva una decisión de reenvío con una sola búsqueda. En general, una ruta estática conectada directamente se utiliza con una interfaz serial punto a punto. Para configurar rutas estáticas conectadas directamente con una interfaz de salida especificada, utilice la siguiente sintaxis:

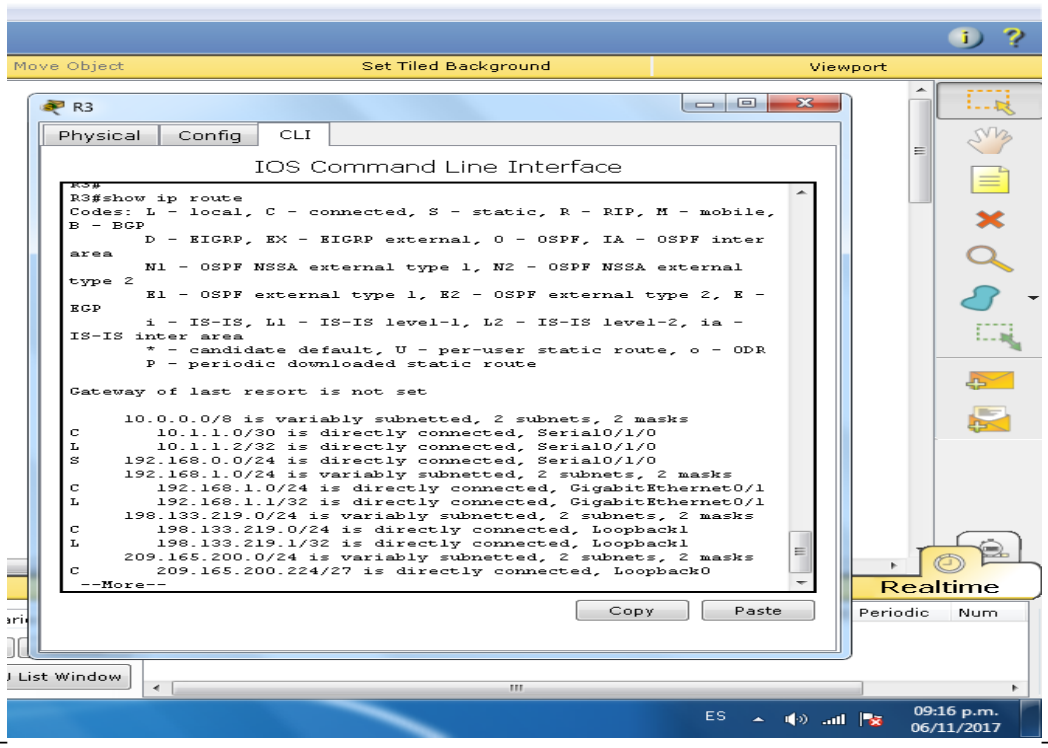
```
Router(config)# iproute dirección-redmáscara-subredinterfaz-salida
```

a. En el router R3, configure una ruta estática a la red 192.168.0.0 con la interfaz S0/0/0 como la interfaz de salida. En el espacio proporcionado, escriba el comando que utilizó.

_R3(config)#ip route 192.168.0.0 255.255.255.0 s0/1/0_____

b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?



_____
_____
__

c. ¿Es posible hacer ping del host PC-A host a al host PC-C? si

Este ping debe tener éxito.

Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

Paso 3. configurar una ruta estática.

a. En el router R1, configure una ruta estática a la red 198.133.219.0 utilizando una de las opciones de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)#ip route 198.133.219.0 255.255.255.0 10.1.1.2

R1(config)#ip route 198.133.219.0 255.255.255.0 s0/1/0

_____

b. En el router R1, configure una ruta estática a la red 209.165.200.224 en el R3 utilizando la otra opción de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

_____R1(config)#ip route 209.165.200.224 255.255.255.224 s0/1/0_____

R1(config)#ip route 209.165.200.224 255.255.255.224 10.1.1.2

c. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?

_____
_____

d. ¿Es posible hacer ping del host PC-A a la dirección 198.133.219.1 del R1? sii__

Este ping debe tener éxito.

Paso 4. Elimine las rutas estáticas de las direcciones de loopback.

a. En el R1, utilice el comando **no** para eliminar las rutas estáticas de las dos direcciones de loopback de la tabla de routing. En el espacio proporcionado, escriba los comandos que utilizó.

_#no ip route 209.165.200.224 255.255.255.224s0/1/0

_noip route 198.133.219.0 255.255.255.0 10.1.1.2

b. Observe la tabla de routing para verificar si se eliminaron las rutas.

¿Cuántas rutas de red se indican en la tabla de routing del R1? 3 ___

¿El gateway de último recurso está establecido? _no_____

Parte 4. configurar y verificar una ruta predeterminada

En la parte 4, implementará una ruta predeterminada, confirmará si la ruta se agregó a la tabla de routing y verificará la conectividad sobre la base de la ruta introducida.

Una ruta predeterminada identifica el gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática predeterminada es una ruta estática con 0.0.0.0 como dirección IP y máscara de subred de destino. Comúnmente, esta ruta se denomina "ruta de cuádruple cero".

En una ruta predeterminada, se puede especificar la dirección IP del siguiente salto o la interfaz de salida. Para configurar una ruta estática predeterminada, utilice la siguiente sintaxis:

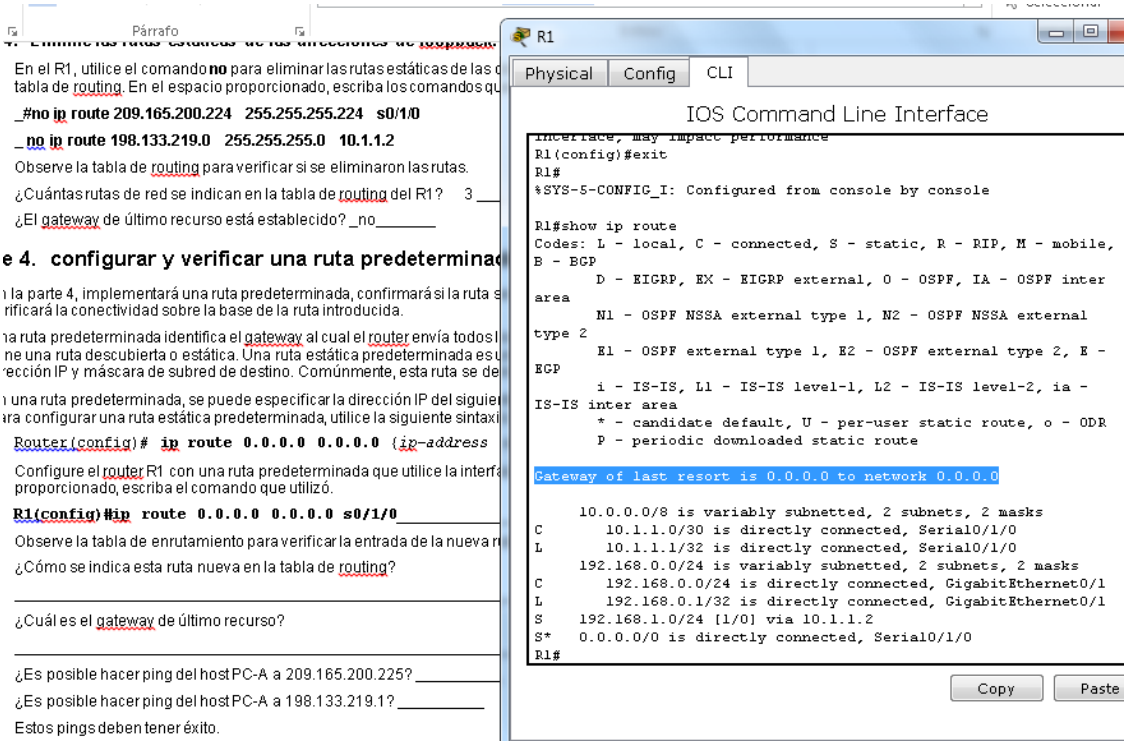
```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

a. Configure el router R1 con una ruta predeterminada que utilice la interfaz de salida S0/0/1. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0_____

b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

¿Cómo se indica esta ruta nueva en la tabla de routing?



En el R1, utilice el comando **no** para eliminar las rutas estáticas de las
tabla de routing. En el espacio proporcionado, escriba los comandos qu

_#no ip route 209.165.200.224 255.255.255.224 s0/1/0

_ no ip route 198.133.219.0 255.255.255.0 10.1.1.2

Observe la tabla de routing para verificar si se eliminaron las rutas.

¿Cuántas rutas de red se indican en la tabla de routing del R1? 3 ___

¿El gateway de último recurso está establecido? _no_____

e 4. configurar y verificar una ruta predeterminad

la parte 4, implementará una ruta predeterminada, confirmará si la ruta s
rificará la conectividad sobre la base de la ruta introducida.

na ruta predeterminada identifica el gateway al cual el router envía todos l
ne una ruta descubierta o estática. Una ruta estática predeterminada es u
rección IP y máscara de subred de destino. Comúnmente, esta ruta se de

una ruta predeterminada, se puede especificar la dirección IP del siguie
ara configurar una ruta estática predeterminada, utilice la siguiente sintaxi

Router(config)# **ip route 0.0.0.0 0.0.0.0** *{ip-address*

Configure el router R1 con una ruta predeterminada que utilice la interf
proporcionado, escriba el comando que utilizó.

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0_____

Observe la tabla de enrutamiento para verificar la entrada de la nueva r

¿Cómo se indica esta ruta nueva en la tabla de routing?

_____

¿Cuál es el gateway de último recurso?

_____

¿Es posible hacer ping del host PC-A a 209.165.200.225? _____

¿Es posible hacer ping del host PC-A a 198.133.219.1? _____

Estos pings deben tener éxito.

R1

Physical | Config | CLI

IOS Command Line Interface

```
Interface, may impact performance
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.1/32 is directly connected, Serial0/1/0
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.2
S*   0.0.0.0/0 is directly connected, Serial0/1/0
R1#
```

Copy Paste

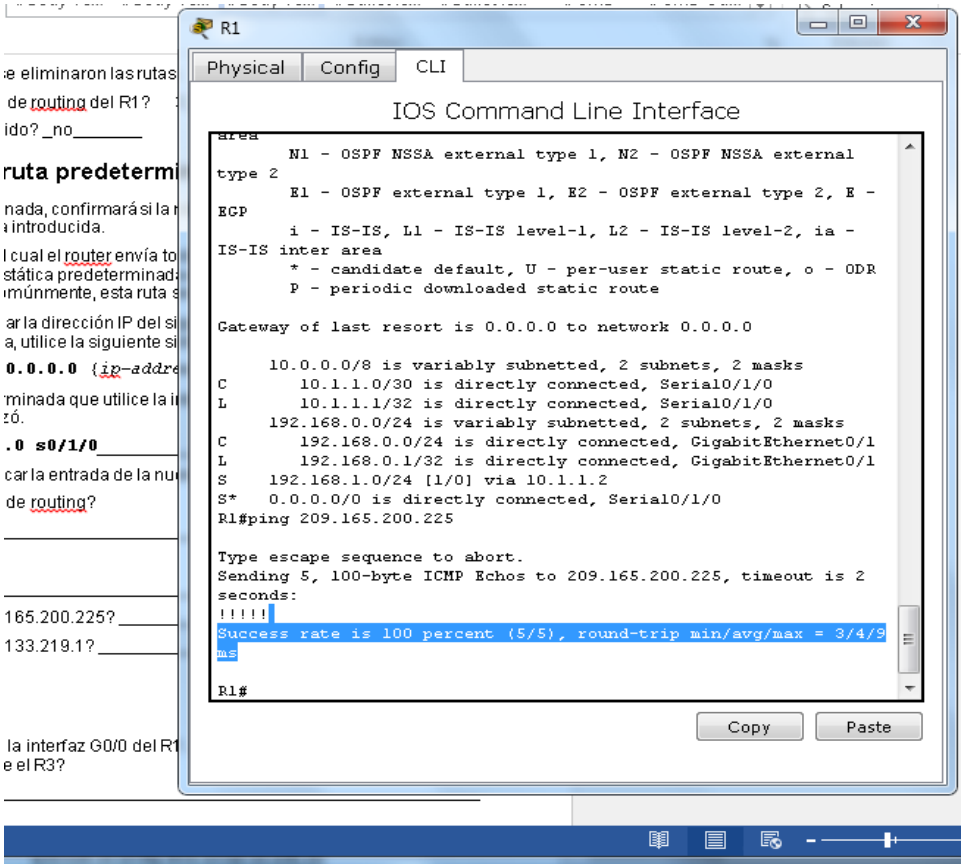
¿Cuál es el gateway de último recurso?

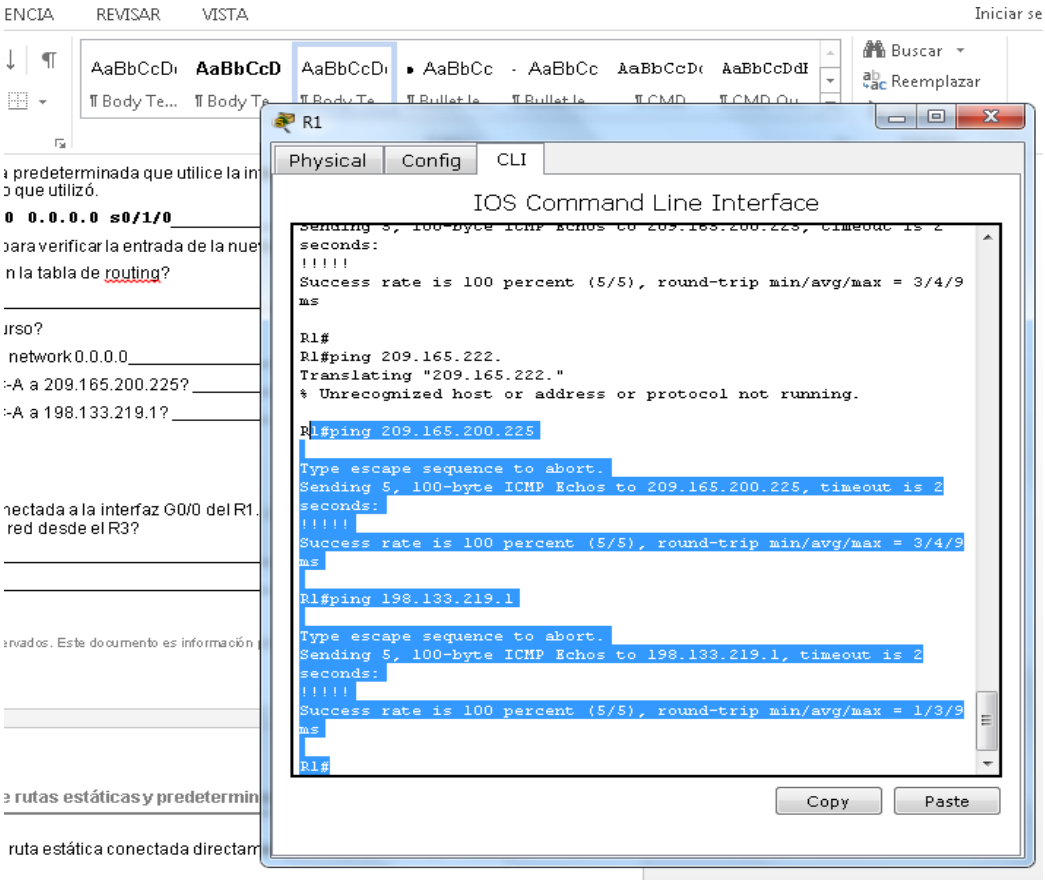
Gateway of last resort is 0.0.0.0 to network 0.0.0.0_____

c. ¿Es posible hacer ping del host PC-A a 209.165.200.225? ___si__

d. ¿Es posible hacer ping del host PC-A a 198.133.219.1? _si___

Estos pings deben tener éxito.


R1
Physical
Config
CLI
IOS Command Line Interface
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/1/0
L 10.1.1.1/32 is directly connected, Serial0/1/0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/1
L 192.168.0.1/32 is directly connected, GigabitEthernet0/1
S 192.168.1.0/24 [1/0] via 10.1.1.2
S* 0.0.0.0/0 is directly connected, Serial0/1/0
R1#ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/9 ms
R1#
Copy
Paste



Reflexión

1. Una nueva red 192.168.3.0/24 está conectada a la interfaz G0/0 del R1. ¿Qué comandos podrían utilizarse para configurar una ruta estática a esa red desde el R3?

   _192.168.3.0 255.255.255.0 10.1.1.1 – 192.163.3.0 s0/0/0/_____

   _____

   _____

2. ¿Ofrece alguna ventaja configurar una ruta estática conectada directamente, en vez de una ruta estática?

   Porque permite que la tabla del routing resuelva la interfaz de salida en una sola ussqueda y no que sean dos.

   _____

   _____

3. ¿Por qué es importante configurar una ruta predeterminada en un router?

   Para direccionar los paquetes dirigidos a las redes que no están explícitamente enumeradas en la tabla de

ruteo. _____
_____

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.

Apéndice A: comandos de configuración para las partes 2, 3 y 4

Los comandos que se indican en el apéndice A sirven exclusivamente como referencia. Este apéndice no incluye todos los comandos específicos que se necesitan para completar esta práctica de laboratorio.

Configuración básica de los dispositivos

Configure los parámetros IP en el router.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Configuraciones de rutas estáticas

Configure una ruta estática recursiva.

```
R1(config)# iproute 192.168.1.0 255.255.255.0 10.1.1.2
```

Configure una ruta estática conectada directamente.

```
R3(config)# iproute 192.168.0.0 255.255.255.0 s0/0/0
```

Elimine lasrutas estáticas.

```
R1(config)# no iproute 209.165.200.224 255.255.255.224 serial0/0/1
```

o

```
R1(config)# no iproute 209.165.200.224 255.255.255.224 10.1.1.2
```

o

```
R1(config)# no iproute 209.165.200.224 255.255.255.224
```

Configuración de rutas predeterminadas

R1(config)# iproute 0.0.0.0 0.0.0.0 s0/0/1

Ejercicio 6.3.1.10 Packet Tracer - Exploring Internetworking Devices Instructions

Packet Tracer: Exploración de dispositivos de internetworking

Topología

Objetivos

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

Parte 2: Seleccionar los módulos correctos para la conectividad

Parte 3: Conectar los dispositivos

Información básica

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

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

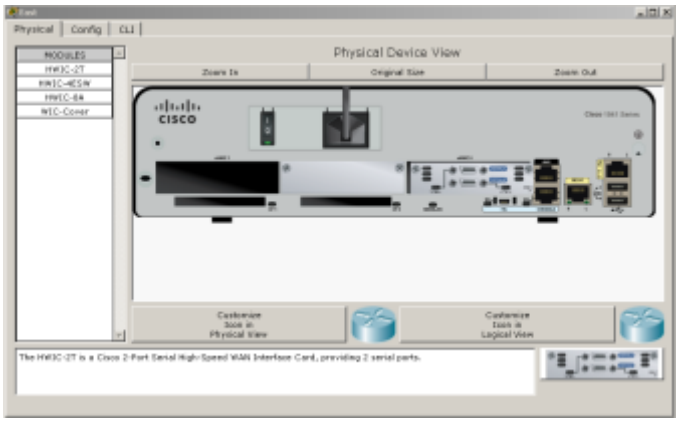
Parte 1: Identificar las características físicas de los dispositivos de internetworking

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

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

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

//..Realizado.../



l ¿Qué puertos de administración se encuentran disponibles?
R/ Los puertos auxiliar y de consola

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

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

R/ Hay dos interfaces LAN (GigabitEthernet 0/0, y GigabitEthernet 0/1) y dos interfaces WAN (seria 0/0/0; serial 0/0/1)

j. 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**

```
East>enable
East#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Serial0/0/0            unassigned      YES unset  down                  down

Serial0/0/1            unassigned      YES unset  down                  down

Vlan1                  unassigned      YES unset  administratively down down
East#
```

k. 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 gigabitethernet 0/0
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is CN Gigabit Ethernet, address is 0001.4274.a401 (bia 0001.4274.a401)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
 --More--
```

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

¿Cuál es el ancho de banda predeterminado de esta interfaz? **R/1544 kbit**

```
East>show interface serial 0/0/0
Serial0/0/0 is down, line protocol is down (disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
```

Nota: los procesos de enrutamiento usan el ancho de banda en las interfaces seriales para determinar elmejor 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.

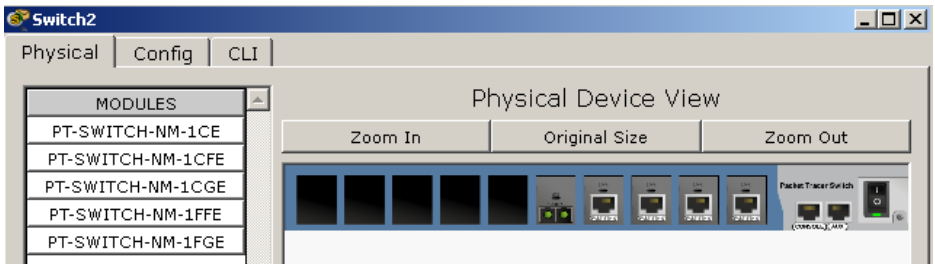
Paso 3: Identificar las ranuras de expansión de módulos en los switches

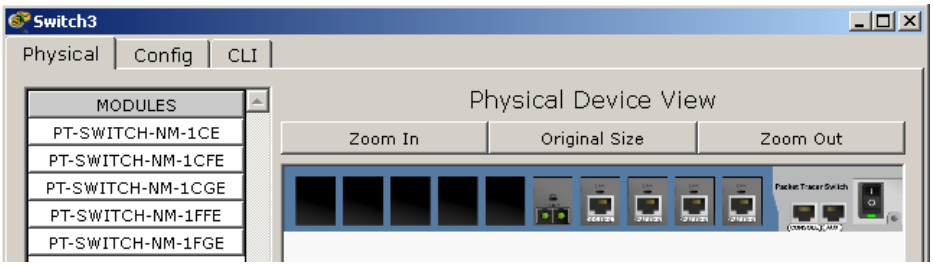
i. ¿Cuántas ranuras de expansión se encuentran disponibles para agregar más módulos al router **East**?

R/1

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

R/ Cada uno tiene cinco ranuras disponibles como se puede apreciar en la siguiente imagen.





Parte 2: Seleccionar los módulos correctos para la conectividad

Paso 1: Determinar qué módulos proporcionan la conectividad requerida

• 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.

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 host**

• Haga clic en **Switch2**. ¿Qué módulo puede insertar para proporcionar una conexión óptica Gigabit al **Switch3**?

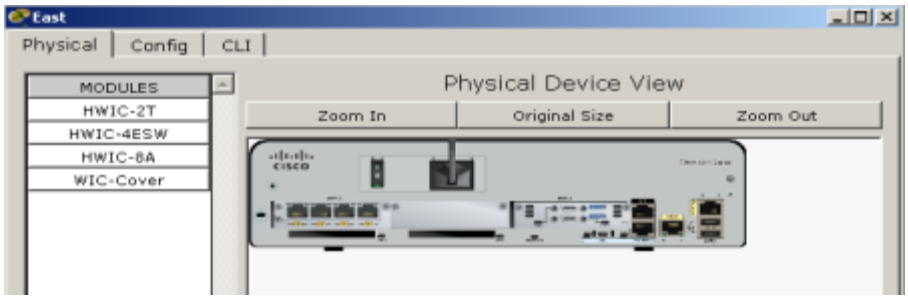
R/ El modulo que se puede insertar para proporcionar dicha conexión corresponde al PT-SWITCH-NM-1FGE, que cumple con los requisitos porque está disponible otro modulo para fibra óptica pero no es gigabit Ethernet sino Fast-Ethernet.

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**.

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

// Se procede a agregar el módulo **HWIC-4ESW** que cumple con los requisitos para conectar posteriormente los 3 pc. //



// Llevamos a cabo la verificación con el comando "**show ip interface brief"**. Podemos evidenciar que se agregaron los 4 puertos FastEternet //

```
East>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  down                  down
Serial0/0/1            unassigned      YES unset  down                  down
FastEthernet0/1/0      unassigned      YES unset  up                    down
FastEthernet0/1/1      unassigned      YES unset  up                    down
FastEthernet0/1/2      unassigned      YES unset  up                    down
FastEthernet0/1/3      unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  administratively down down
East>
```

14. 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**.

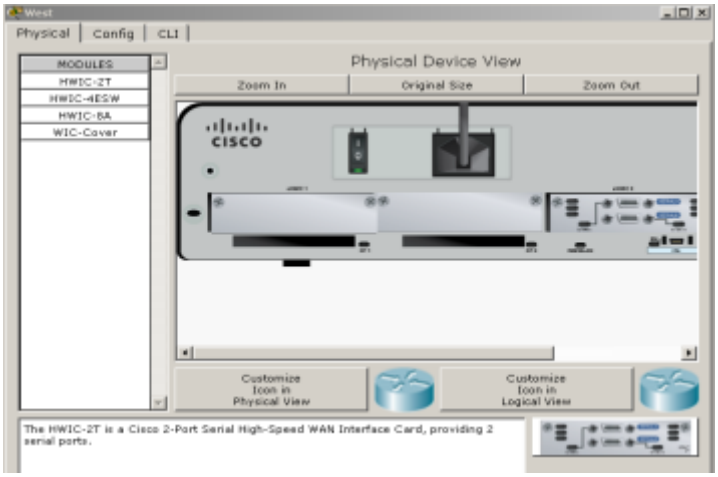
//Se procede a agregar el modulo **PT-SWITCH-NM-1FGE** y verificamos por CLI que ya se encuentre la interfaz. Se identifica como **GigabitEhernet 5/1**.//

```
Switch>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES manual down                  down

FastEthernet1/1        unassigned      YES manual down                  down

FastEthernet2/1        unassigned      YES manual down                  down

FastEthernet3/1        unassigned      YES manual down                  down

FastEthernet4/1        unassigned      YES manual down                  down

GigabitEthernet5/1     unassigned      YES manual down                  down

Vlan1                  unassigned      YES manual administratively down down
Switch>
```

15. Use el comando **show ip interface brief** para identificar la ranura en la que se colocó el módulo. ¿En qué ranura se insertó? **R/ GigabitEthernet5/1**

16. 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).

// Se adiciona el **módulo HWIC-2T** dado que el que se encuentra disponible y cumple con los requisitos solicitados//



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

// Verificamos mediante la utilización del comando show ip interface brief//

```
West>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
West>
```

Parte 3: Conectar los dispositivos

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

- Seleccione el tipo de cable adecuado.
- Haga clic en el primer dispositivo y seleccione la interfaz especificada.
- Haga clic en el segundo dispositivo y seleccione la interfaz especificada.
- Si conectó correctamente los dos dispositivos, verá que su puntuación aumenta.

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

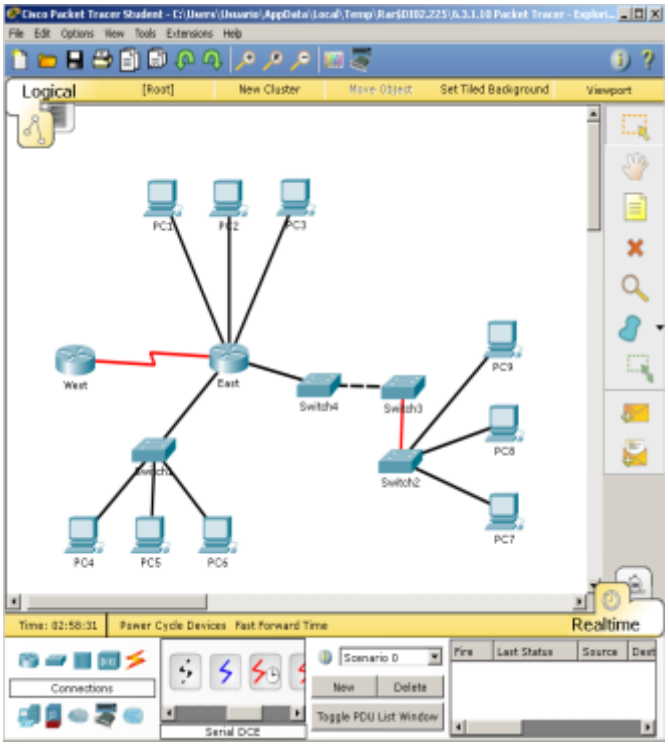
Nota: a los efectos de esta actividad, se deshabilitaron las luces de enlace. Los dispositivos no estánconfigurados con ningún direccionamiento IP, de modo que no puede probar la conectividad.

Dispositivo	Interfaz	Tipo de cable	Dispositivo	Interfaz
East	GigabitEthernet0/0	Cable de cobre de conexión directa	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Cable de cobre de conexión directa	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Cable de cobre de conexión directa	PC1	FastEthernet0
East	FastEthernet0/1/1	Cable de cobre de conexión directa	PC2	FastEthernet0
East	FastEthernet0/1/2	Cable de cobre de conexión directa	PC3	FastEthernet0
Switch1	FastEthernet0/1	Cable de cobre de conexión directa	PC4	FastEthernet0
Switch1	FastEthernet0/2	Cable de cobre de conexión directa	PC5	FastEthernet0

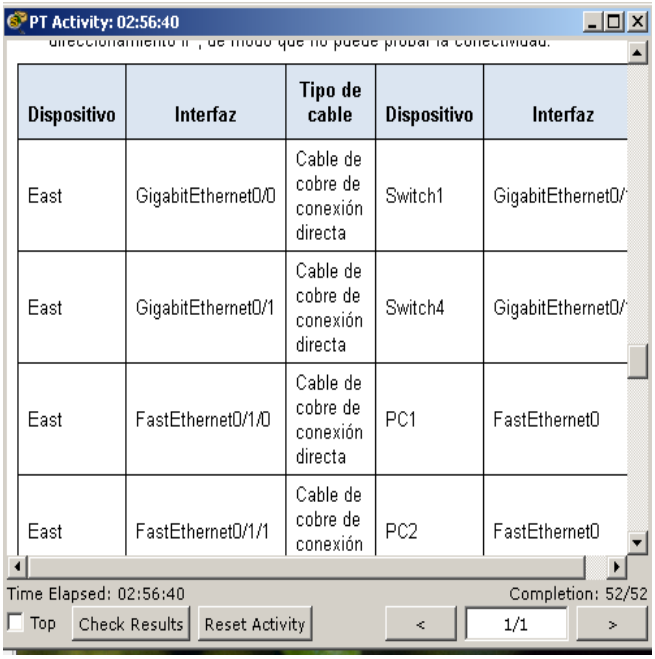
Switch1	**FastEthernet0/3**	**Cable de cobre de conexión directa**	**PC6**	**FastEthernet0**
Switch4	**GigabitEthernet0/2**	**Cross-Over de cobre**	**Switch3**	**GigabitEthernet3/1**
Switch3	**GigabitEthernet5/1**	**Fibra**	**Switch2**	**GigabitEthernet5/1**
Switch2	**FastEthernet0/1**	**Cable de cobre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

// Son realizadas todas y cada una de las conexiones especificadas en la tabla anterior//

CONEXIONES REALIZADAS



VERIFICACION DE COMPLETO 52/52



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

Ejercicio 6.4.1.2 Packet Tracer - Configure Initial Router Settings Instructions

Packet Tracer: configuración Inicial del Router

Topología

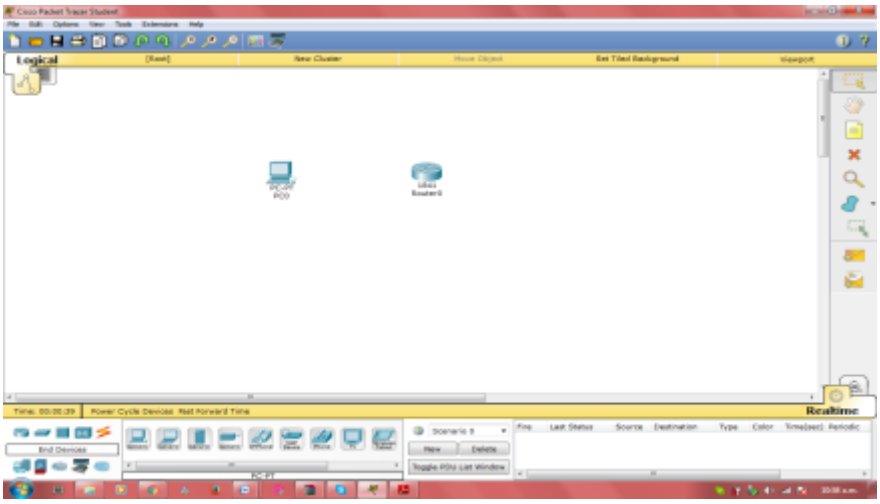
Objetivos

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

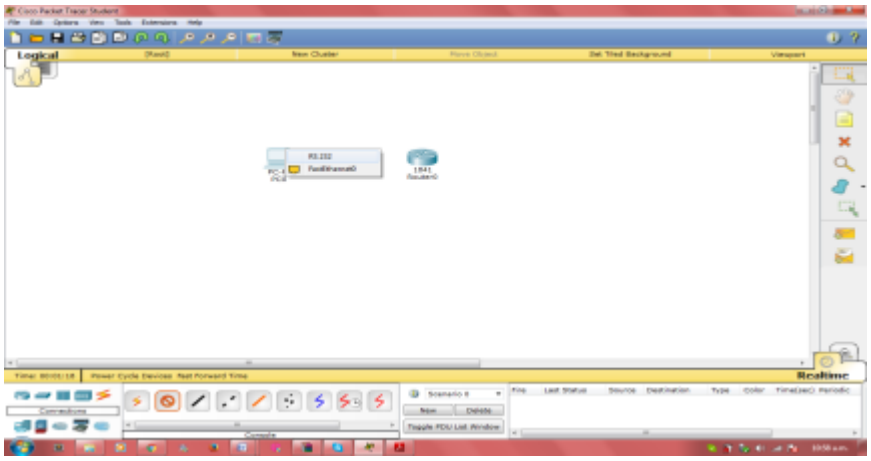
En esta actividad, configurará los parámetros básicos del router. Proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado. También configurará mensajes para los usuarios que inicien sesión en el router. Estos avisos también advierten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

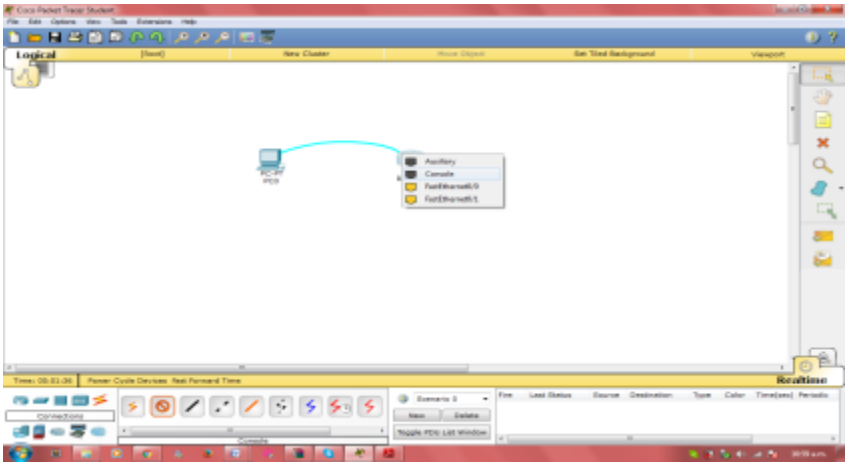
Parte 1: Verificar la configuración predeterminada del router
Paso 1: Establecer una conexión de consola al R1 a. Elija un cable de **consola** de las conexiones disponibles.

b. Haga clic en **PCA** y seleccione **RS 232**.
c. Haga clic en **R1** y seleccione **Console** (Consola).
d. Haga clic en **PCA** > ficha **Desktop** (Escritorio) >**Terminal**.
e. Haga clic en **OK** (Aceptar) y presione **Entrar**. Ahora puede configurar **R1**.



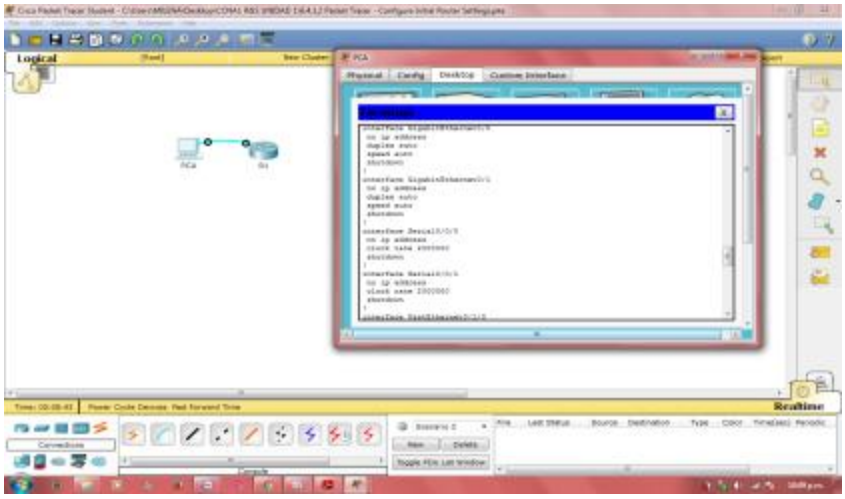
Seleccionamos un router y un pc y realizamos la conexión. Como se muestra a continuación.

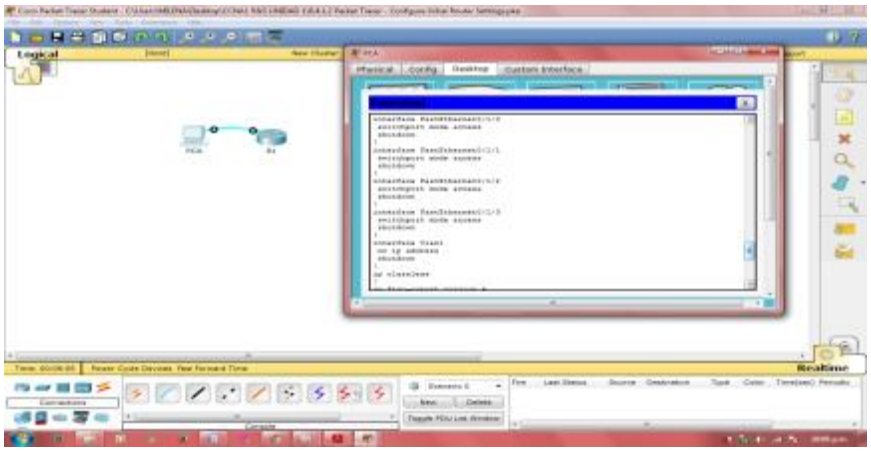




Responda las siguientes preguntas:

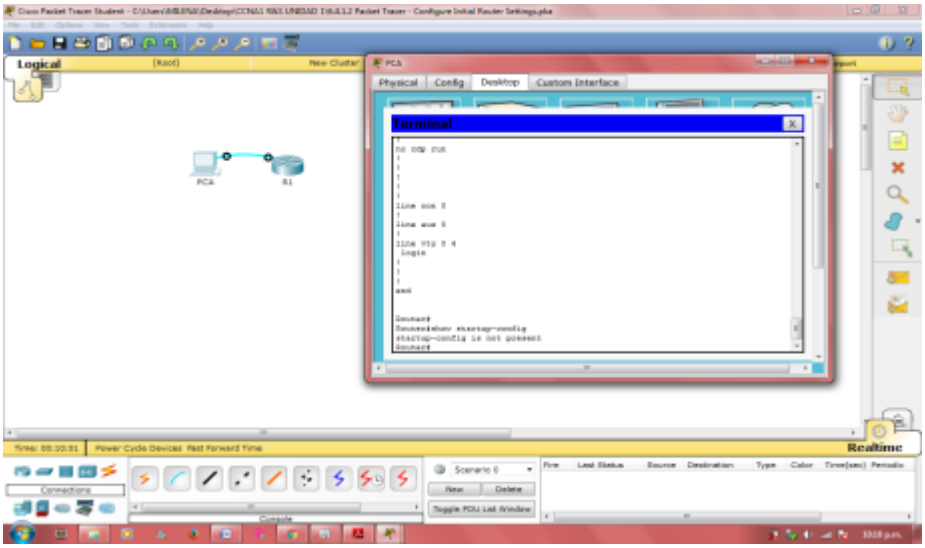
- **¿Cuál es el nombre de host del router?**
  R= Router
- **¿Cuántas interfaces Fast Ethernet tiene el router?**
  R=4
- **¿Cuántas interfaces Gigabit Ethernet tiene el router?**
  R=2
- **¿Cuántas interfaces seriales tiene el router?**
  R=2
- **¿Cuál es el rango de valores que se muestra para las líneas vty?**
  R= 0 – 4



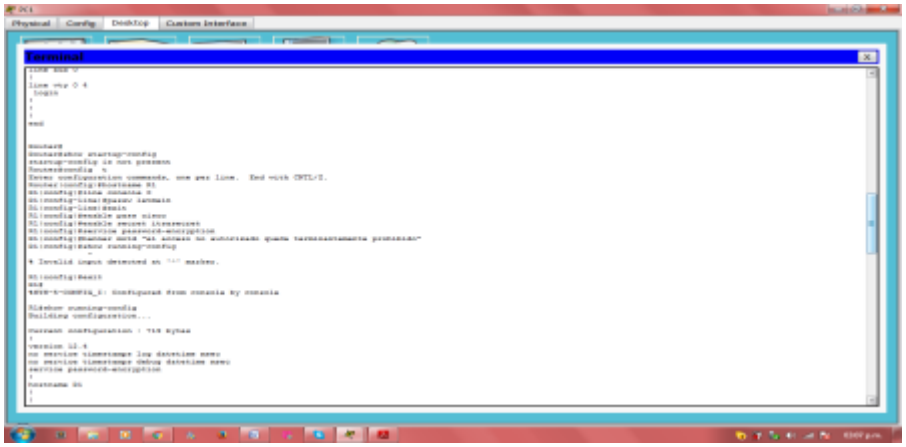


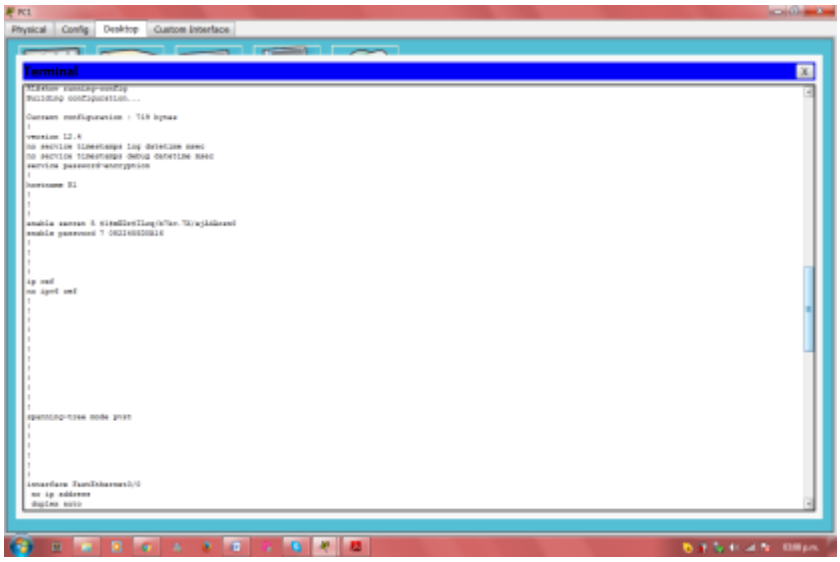
¿Por qué el router responde con el mensaje startup-config is not present?

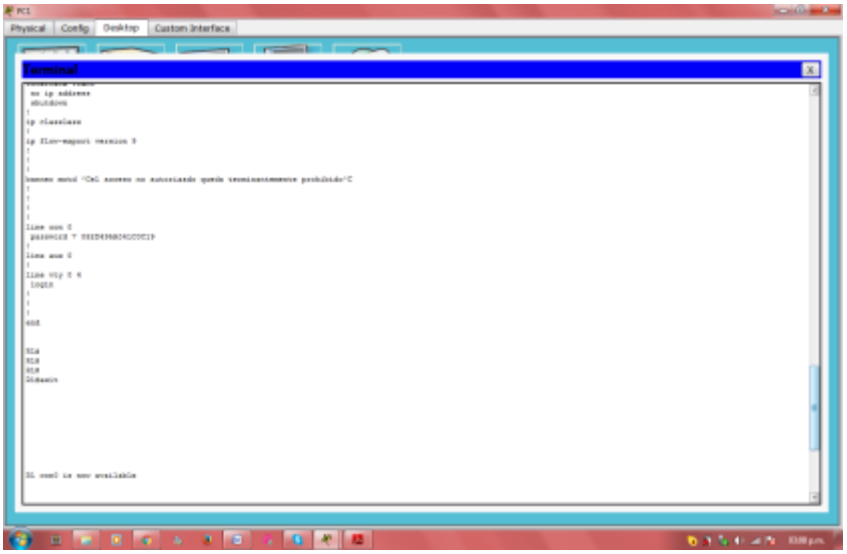
Este mensaje se muestra porque el archivo de configuración no se guardó en la NVRAM. Actualmente se encuentra solo en RAM.



PARTE 2: CONFIGURAR Y VERIFICAR LA CONFIGURACIÓN INICIAL DEL ROUTER

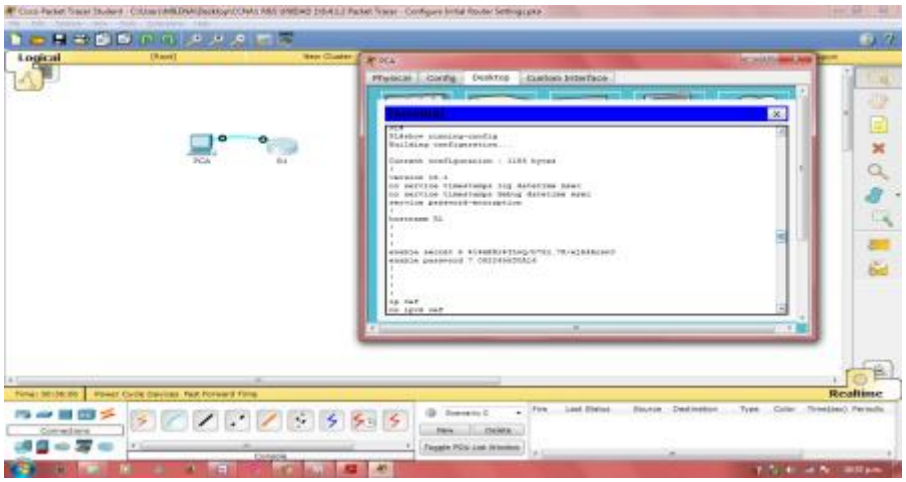


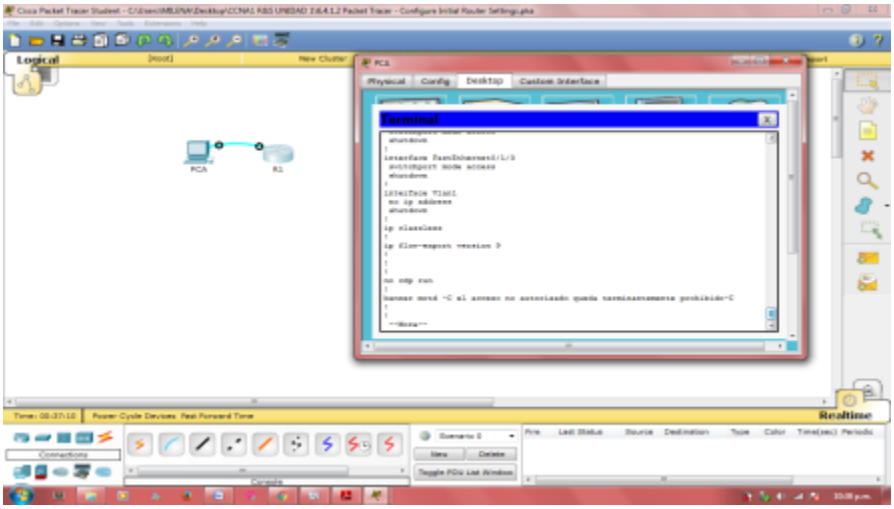




2: VERIFICAR LOS PARÁMETROS INICIALES DE R1

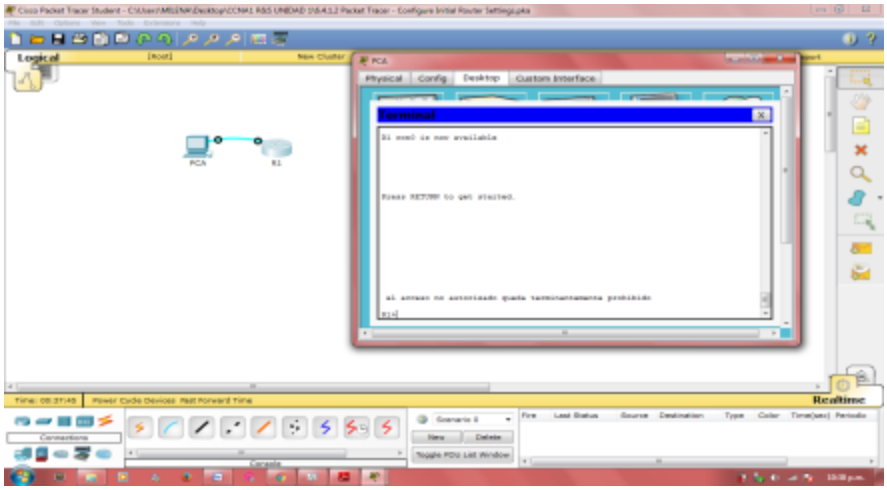
a. Para verificar los parámetros iniciales, observe la configuración de R1. ¿Qué comando utiliza? **show running-config**





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

R1 con0 is now available
Press RETURN to get started. **Packet Tracer: configuración inicial del router**
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)?

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**

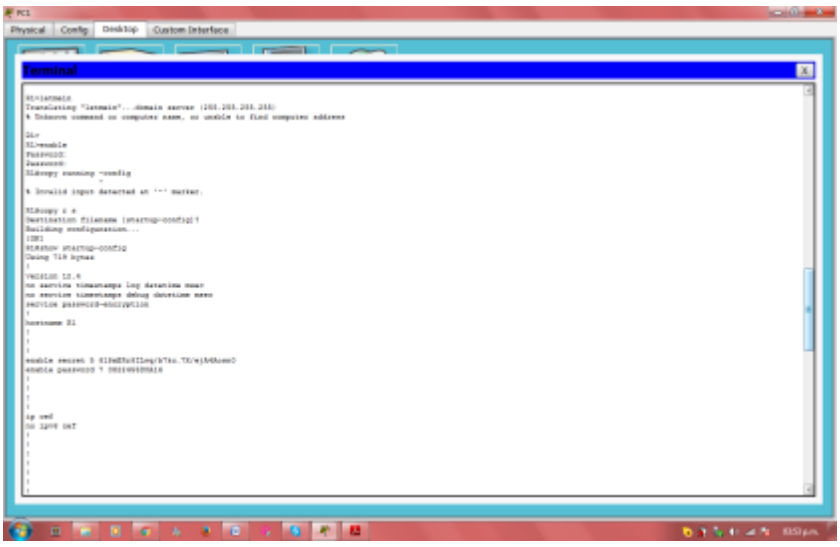
d. Introduzca las contraseñas necesarias para regresar al modo EXEC privilegiado.

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

La **contraseña secreta de enable** sobrescribe la contraseña de enable. Si ambas están configuradas en el router, debe introducir la contraseña **secreta de enable** para ingresar al modo EXEC privilegiado. Si configura más contraseñas en el router, ¿se muestran como texto no cifrado o en forma encriptada en el archivo de configuración? Explique. El comando service password-encryption encripta todas las contraseñas actuales y futuras

Parte 3: Guardar el archivo de configuración en ejecución
Paso 1: Guarde el archivo de configuración en la NVRAM. a. Configuró los parámetros iniciales de **R1**. Ahora realice una copia de seguridad del archivo de configuración en ejecución en la NVRAM para garantizar que no se pierdan los cambios realizados si el sistema se reinicia o se apaga.

¿Qué comando introdujo para guardar la configuración en la NVRAM? copy running-config startup-config
¿Cuál es la versión más corta e inequívoca de este comando? copy r s
¿Qué comando muestra el contenido de la NVRAM? show startup-configuration or show start
b. Verifique que todos los parámetros configurados estén registrados. Si no fuera así, analice el resultado y determine qué comandos no se introdujeron o se introdujeron incorrectamente. También puede hacer clic en **Check Results** (Verificar resultados) en la ventana de instrucción.



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

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

R1# **show flash**
¿Cuántos archivos hay almacenados actualmente en la memoria flash? 3

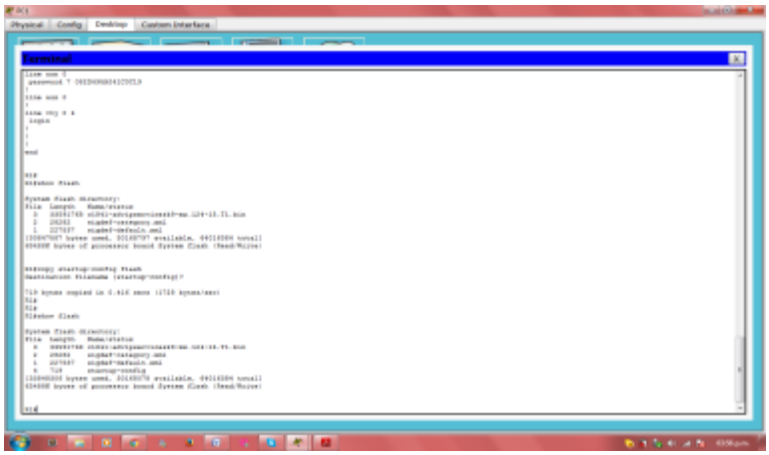
CUÁL DE ESTOS ARCHIVOS CREE QUE ES LA IMAGEN DE IOS? c1900-universalk9-mz.SPA.151-4.M4.bin
¿Por qué cree que este archivo es la imagen de IOS?
Las respuestas pueden variar, pero hay dos pistas: la longitud del archivo en comparación con otros y la extensión .bin al final del nombre de archivo.

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

R1# **copy startup-config flash**
Destination filename [startup-config]
El router le pide que almacene el archivo en la memoria flash con el nombre entre corchetes. Si la respuesta es afirmativa, presione **Entrar**; de lo contrario, escriba un nombre adecuado y presione la tecla **Entrar**.

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

c.



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

Packet Tracer: Conexión de un Router a una LAN

.

Topología

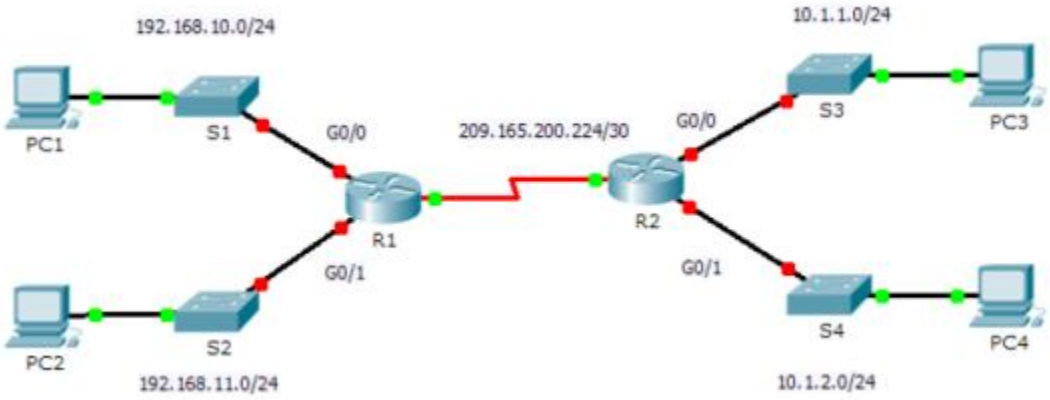


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	No aplicable
	G0/1	192.168.11.1	255.255.255.0	No aplicable
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	No aplicable
R2	G0/0	10.1.1.1	255.255.255.0	No aplicable
	G0/1	10.1.2.1	255.255.255.0	No aplicable
	S0/0/0	209.165.200.226	255.255.255.252	No aplicable
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Objetivos

Parte 1: Mostrar la información del router
Paso 2: Configurar las interfaces del router
Paso 3: Verificar la configuración

Información básica

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

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

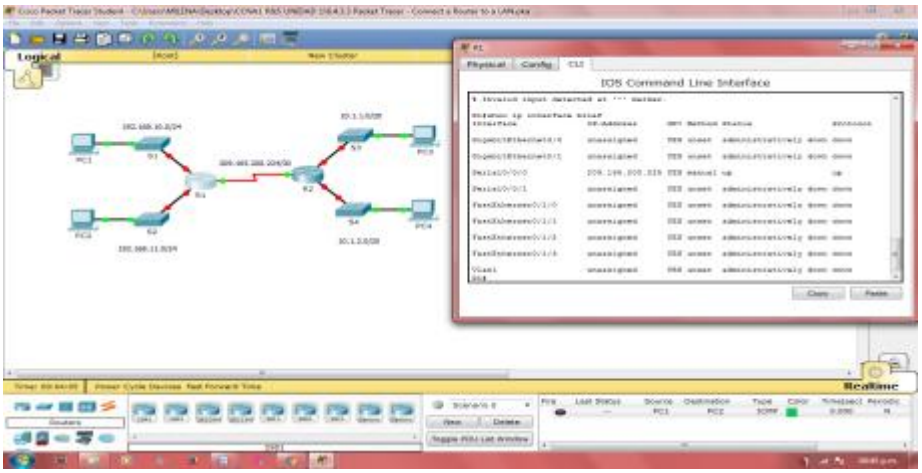
Parte 1: Mostrar la información del router

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

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

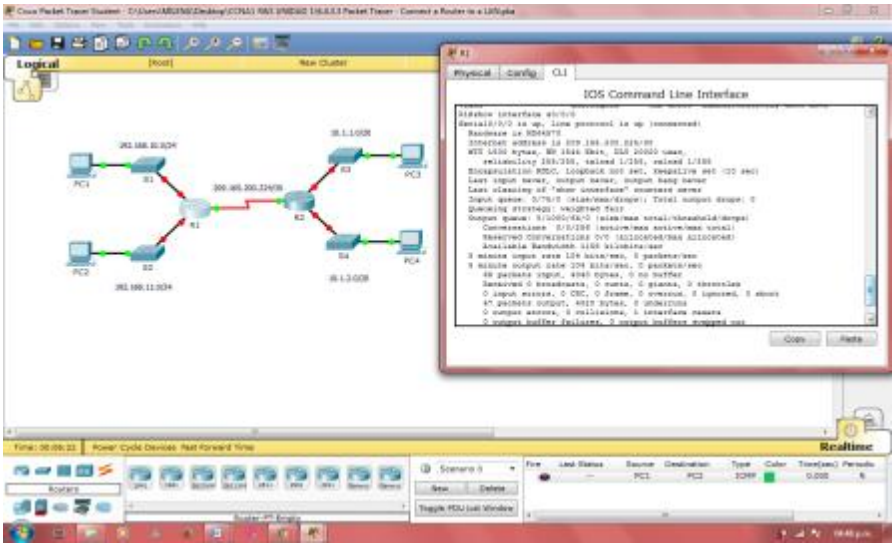
a. **¿Qué comando muestra las estadísticas para todas las interfaces configuradas en el router**?

R:/ show interfaces



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

R/: SHOW INTERFACE S0/0/0



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

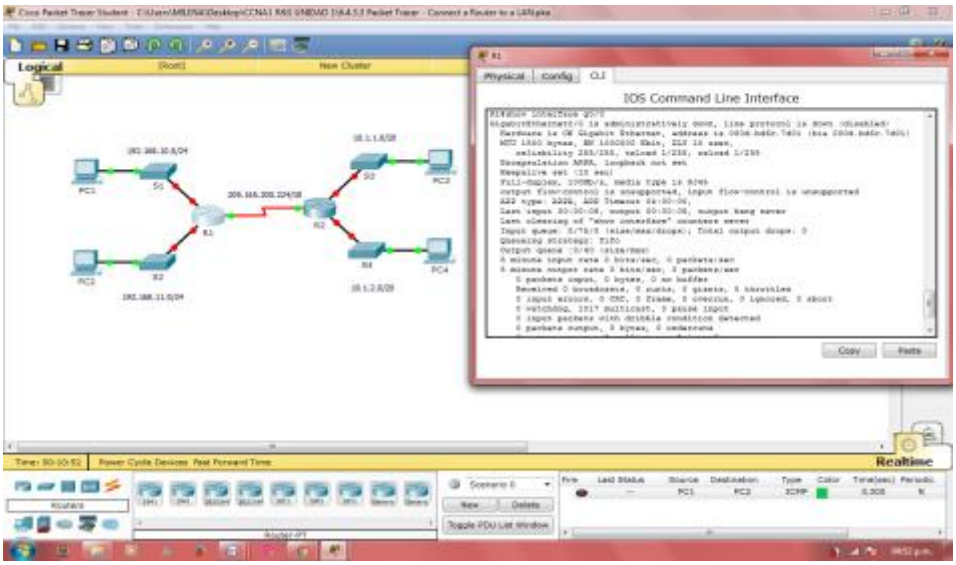
1) ¿Cuál es la dirección IP configurada en el R1?

R/: 209.165.200.225/30

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

BW 1544 kbit

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



1) ¿Cuál es la dirección IP en el R1?

No hay una dirección ip configurada en la interfaz gigabitethernet 0/0

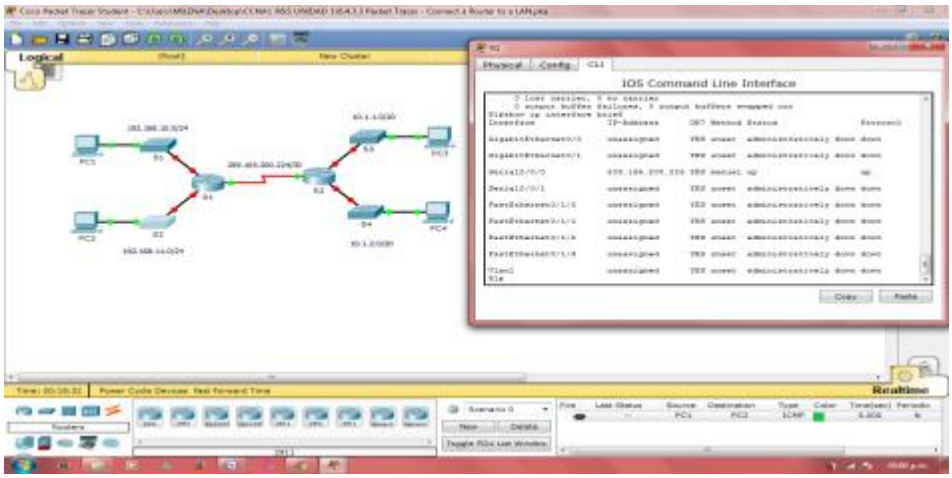
2) ¿Cuál es la dirección MAC de la interfaz GigabitEthernet 0/0?

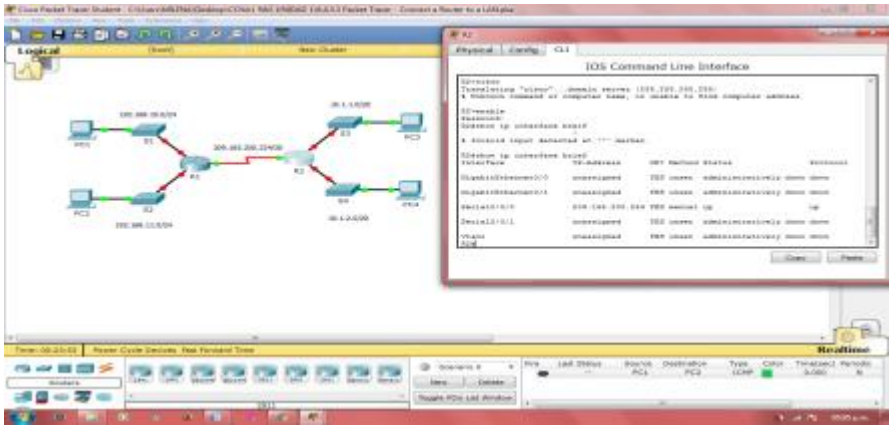
R/: 000d.bd6c.7d01

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

Bw 1000000 kbit

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





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

Show ip interface brief

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

1) ¿Cuántas interfaces seriales hay en R1 y R2?

R1: Muestra 2 la serial0/0/0 y la serial 0/0/1

R2: Muestra 2, la serial0/0/0 y la serial 0/0/1

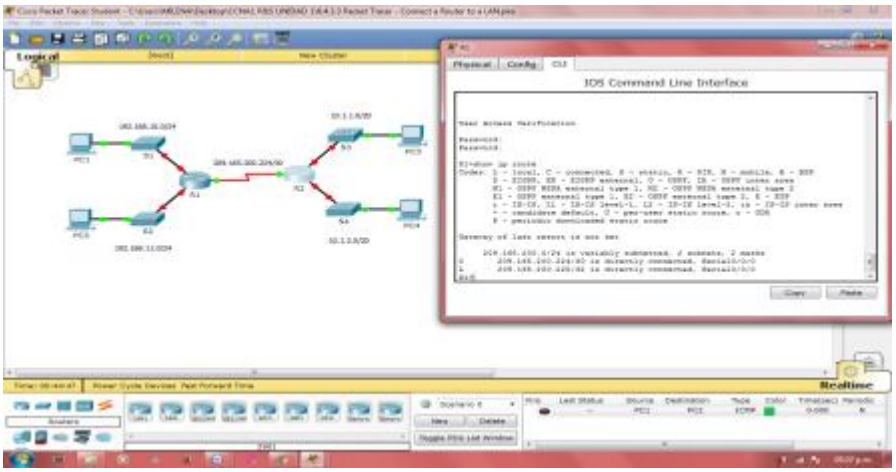
2) ¿Cuántas interfaces Ethernet hay en R1 y R2?

En el R1 hay 4 interfaces Ethernet y en el R2 no hay interfaces ethernet

4) ¿Son iguales todas las interfaces Ethernet en el R1? Si no es así, explique las diferencias.

Todas son diferentes, existen dos interfaces gigabit Ethernet y 4 interfaces fast Ethernet. Las primeras admiten velocidades de hasta 1 000 000 000 bits, y las interfaces fastEthernet admiten hasta 1 000 000 bits.

Paso 3: Mostrar la tabla de enrutamiento en el R1.



a. ¿Qué comando muestra el contenido de la tabla de enrutamiento?

R/: show ip route

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

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

R/: 1

2) ¿Qué ruta se indica?

R/: 209.165.200.0/30

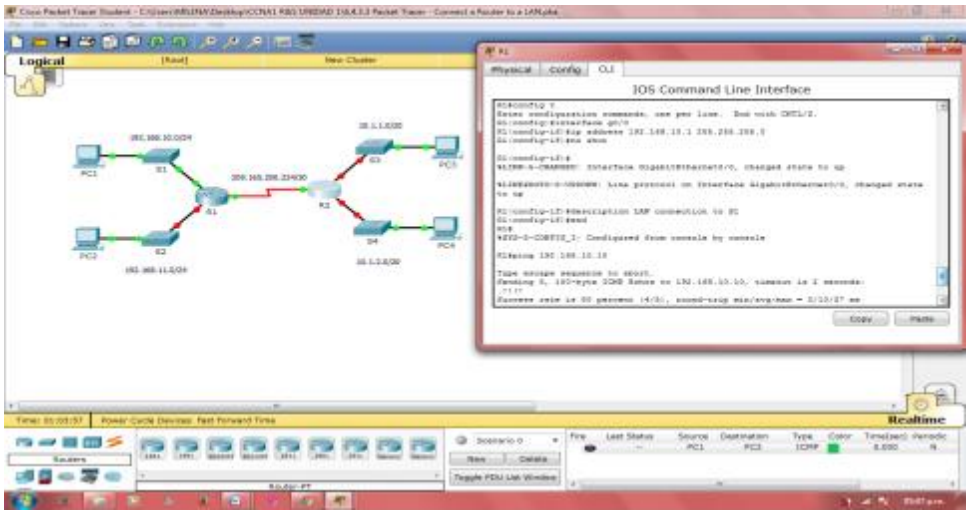
3) ¿Cómo administra el router un paquete destinado a una red que no se incluye en la tabla de enrutamiento?

Un router solo envía paquetes a redes indicada en la tabla de enrutamiento, si una red no aparece en la lista, el paquete se descarta.

Paso 2: Configurar las interfaces del router

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

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



R1(config)# **interface gigabitethernet 0/0**

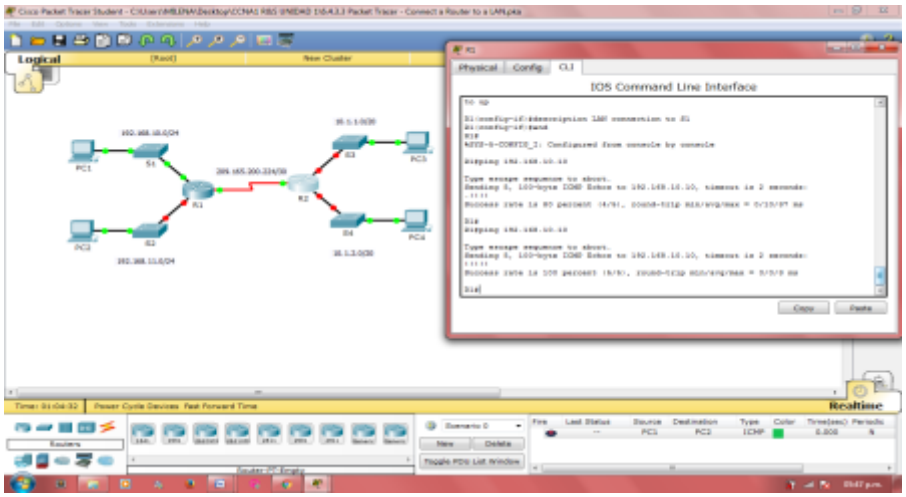
R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **no shutdown**

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

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

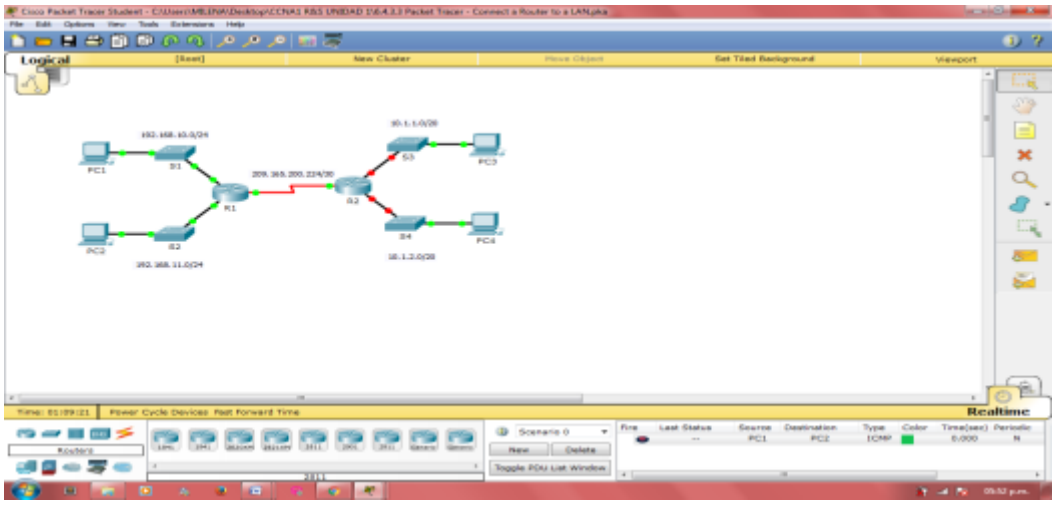


R1(config-if)# **description LAN connection to S1**

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

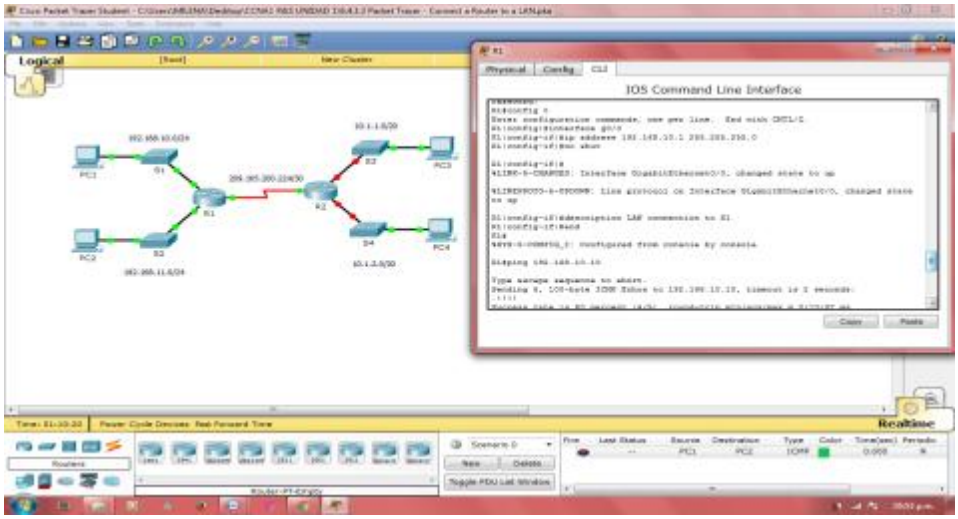
R1(config-if)# **end**
%SYS-5-CONFIG_I: Configured from console by console
R1# **ping 192.168.10.10**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms

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



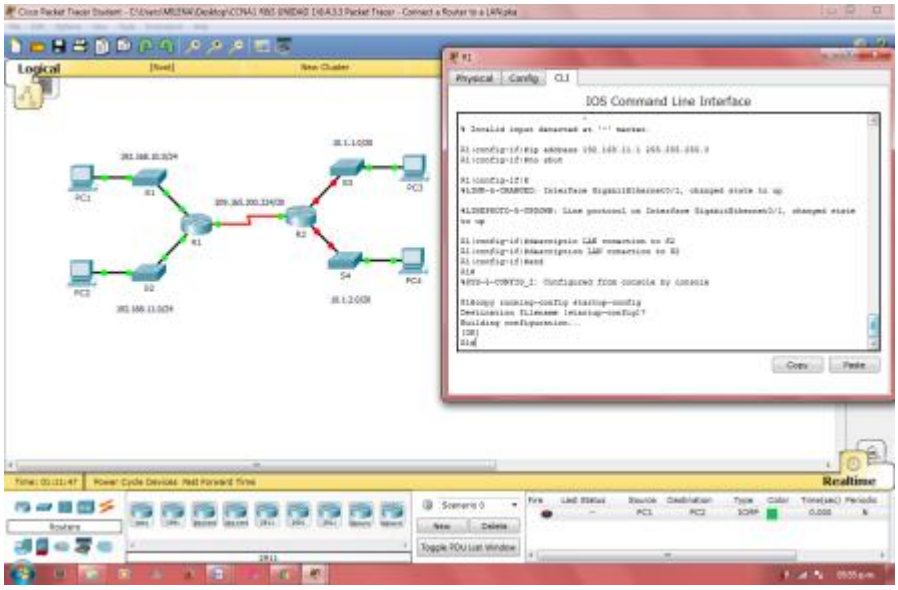
a. Utilice la información en la tabla de direccionamiento para finalizar la configuración de **R1** y **R2**. Para cada interfaz, realice lo siguiente:

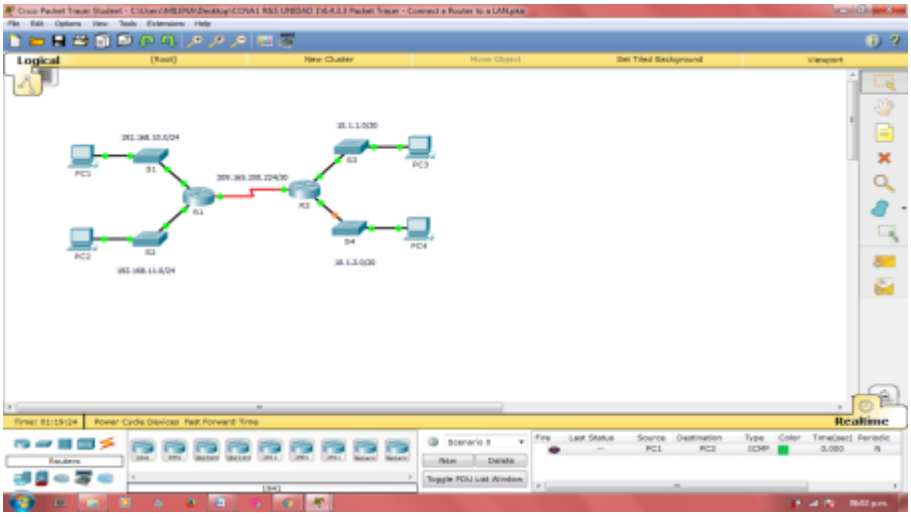
1) Introduzca la dirección IP y active la interfaz.



2) Configure una descripción apropiada.

b. Verifique las configuraciones de las interfaces.





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

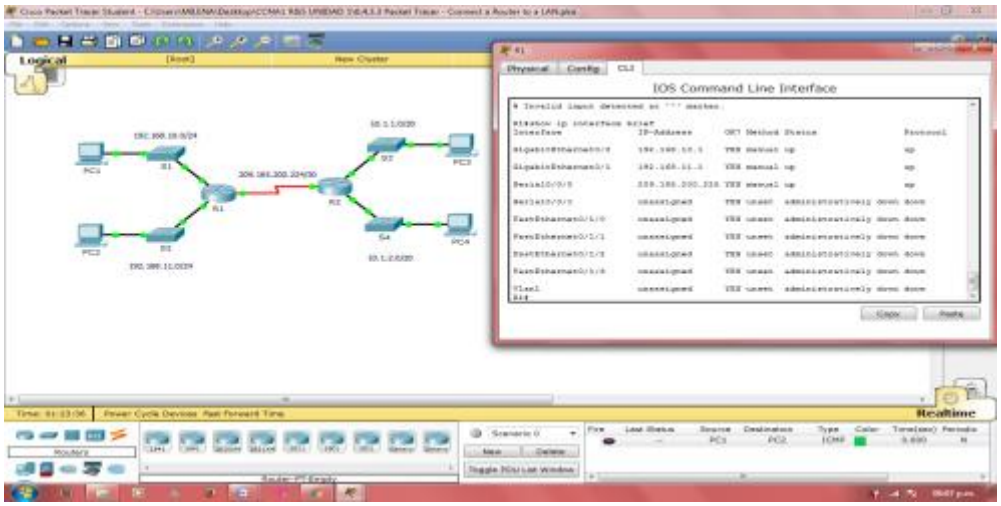
Guarde los archivos de configuración de ambos routers en la NVRAM. ¿Qué comando utilizó?

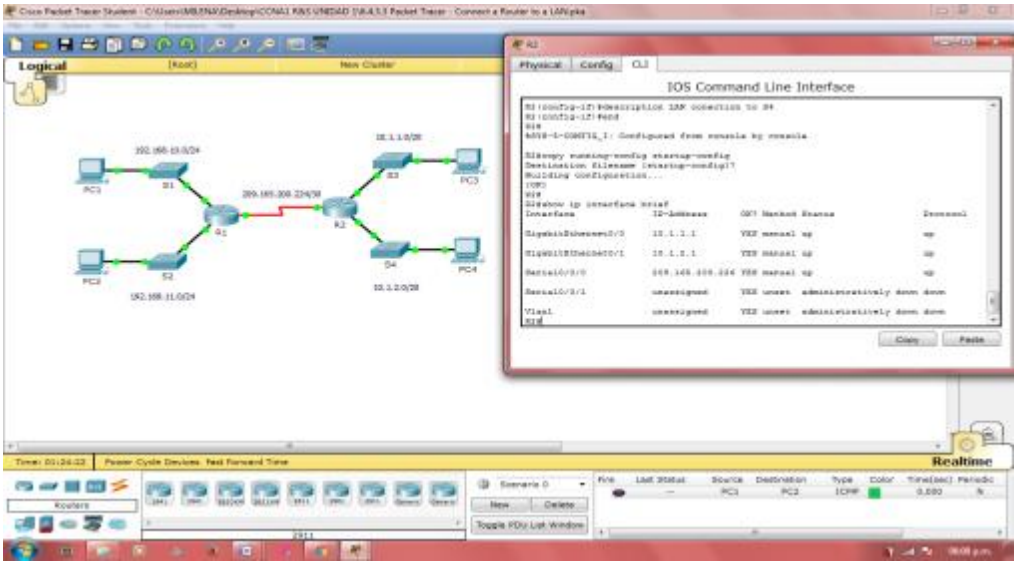
R/: Copy running-config startup-config

Paso 3: Verificar la configuración

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

a. Utilice el comando **show ip interface brief** en **R1** y **R2** para verificar rápidamente que las interfaces estén configuradas con la dirección IP correcta y estén activas.





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

GigabitEthernet0/0 192.168.10.1 YES manual up up
GigabitEthernet0/1 192.168.11.1 YES manual up up

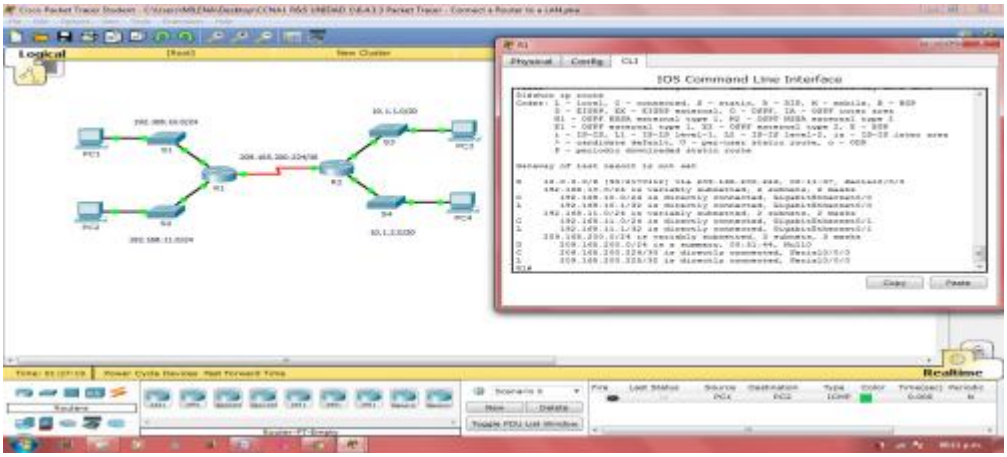
Serial0/0/0 209.165.200.225 YES manual up up

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

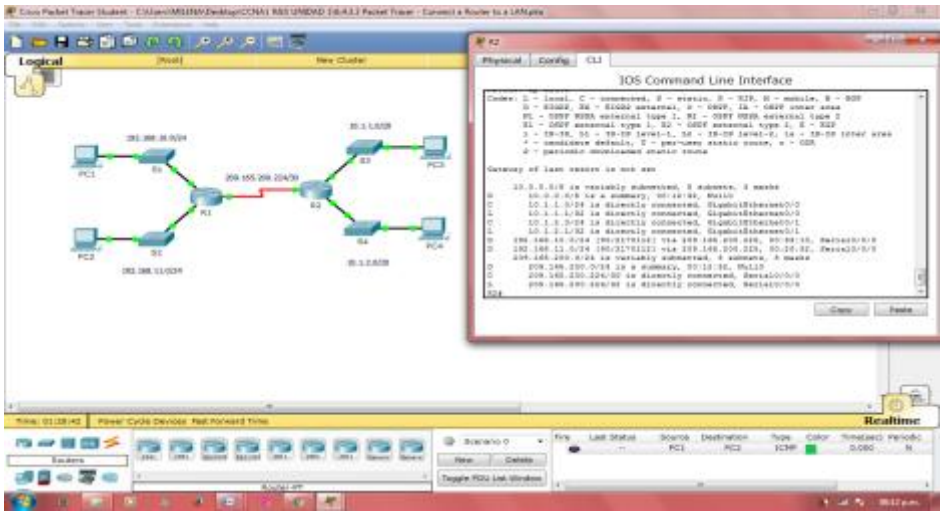
¿Qué comandos puede utilizar para verificar esta parte de la configuración?

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

R1



R2



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

R1: 3 rutas

R2: 3 rutas

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

R1:2

R2: 4

3) Si el router conoce todas las rutas en la red, la cantidad de rutas conectadas y de rutas descubiertas dinámicamente (EIGRP) debe ser

igual a la cantidad total de LAN y WAN. ¿Cuántas LAN y WAN hay en la topología?

R/: 5

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

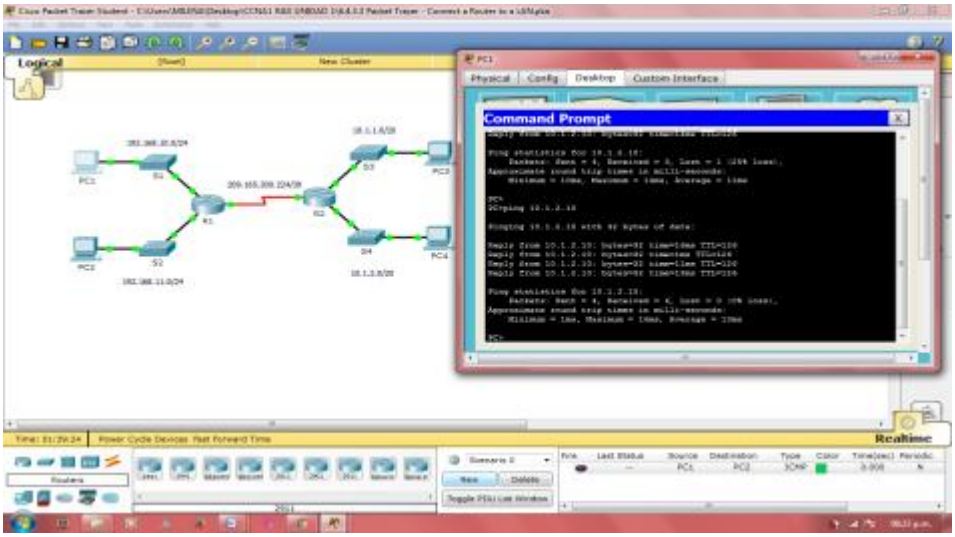
R/: SI

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

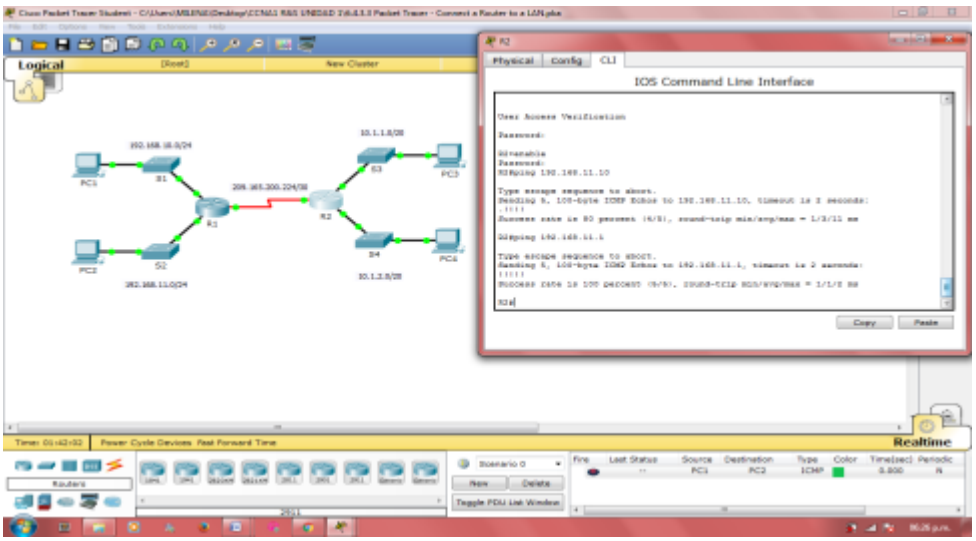
Paso 2: Probar la conectividad de extremo a extremo a través de la red

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

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



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

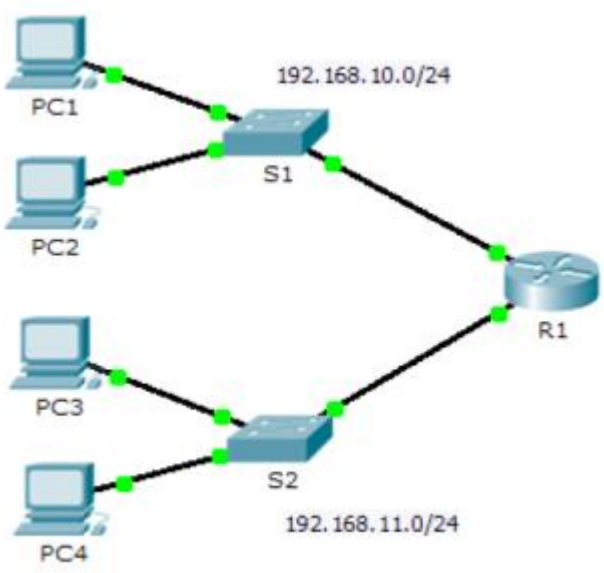


Nota: para simplificar esta actividad, los switches no están configurados, por lo que podrá hacerles ping

Ejercicio 6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues Instructions I

Packet Tracer: Resolución de Problemas de Gateway

Topología



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

Objetivos

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

Parte 2: Implementar, verificar y documentar las soluciones

Información básica

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

1) Verificar la documentación de la red y utilizar pruebas para descartar problemas.
2) Determinar cuál es la solución adecuada para un problema dado.
3) Implementar la solución.
4) Realizar pruebas para verificar que se haya resuelto el problema.
5) Documentar la solución.

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

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

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

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

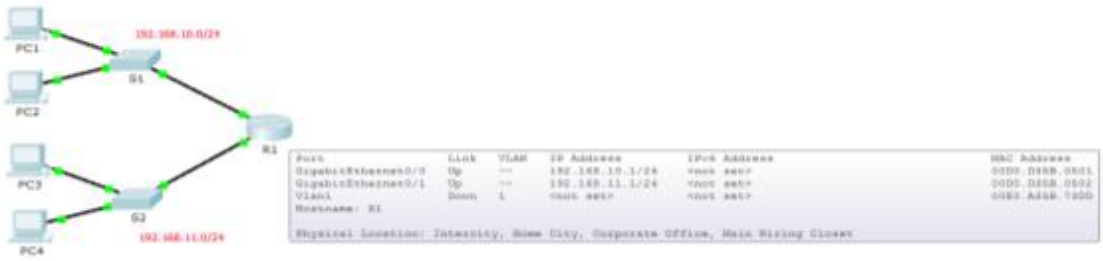
Paso 1: Verificar el registro de la red y descartar cualquier problema

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

R:/ La tabla de direccionamiento presenta falta de información tal como se ve en la imagen

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	
S2	VLAN 1	192.168.11.2	255.255.255.0	
PC1	NIC	192.168.10.10	255.255.255.0	
PC2	NIC	192.168.10.11	255.255.255.0	
PC3	NIC	192.168.11.10	255.255.255.0	
PC4	NIC	192.168.11.11	255.255.255.0	

Se procede a realizar las verificaciones
S1= 192.168.10.1
S2= 192.168.11.1



PC1
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::20D:BDFF:FE84:B6D1
IP Address.....: 192.168.11.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

PC 2
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::201:43FF:FEB0:4891
IP Address.....: 192.168.10.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

PC3
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::290:2BFF:FE65:7DCC
IP Address.....: 192.168.11.10

Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.11.1

PC4

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::201:64FF:FE94:E76B
IP Address.....: 192.168.11.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

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

b. Pruebe la conectividad a los dispositivos en la misma red. Al descartar y corregir Cualquier problema de acceso local, puede probar mejor la conectividad remota, con la seguridad de que la conectividad local está en funcionamiento.
Un plan de verificación puede ser tan simple como una lista de pruebas de conectividad. Use las siguientes pruebas para verificar la conectividad local y descartar cualquier problema de acceso. El primer problema ya se documentó, pero debe implementar y verificar la solución durante la parte 2.

Documentación de prueba y verificación

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

PC3 a PC4	Si	Ok	Ok	
PC3 a S2	No	falta configurar S2	Pendiente	
PC3 a R1	Si	Ok	Ok	
PC4 a S2	No	falta configurar S2	Pendiente	
PC4 a R1	Si	ok	ok	

c. Pruebe la conectividad a los dispositivos remotos (p. ej., de la PC1 a la PC4) y documente cualquier problema. Esto se conoce frecuentemente como *conectividad de extremo a extremo*. Esto significa que la política de red permite que todos los todos los dispositivos en una red tengan conectividad total.
Nota: es posible que aún no se pueda realizar la prueba de conectividad remota, dado que primero debe resolver los problemas de conectividad local. Una vez que solucione dichos problemas, vuelva a este paso y pruebe la conectividad entre redes.

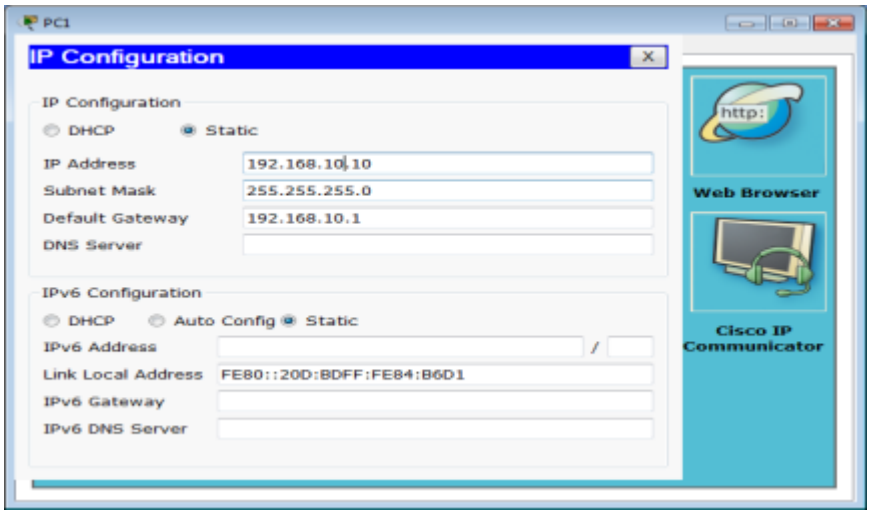
Parte 2: Implementar, verificar y documentar las soluciones

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

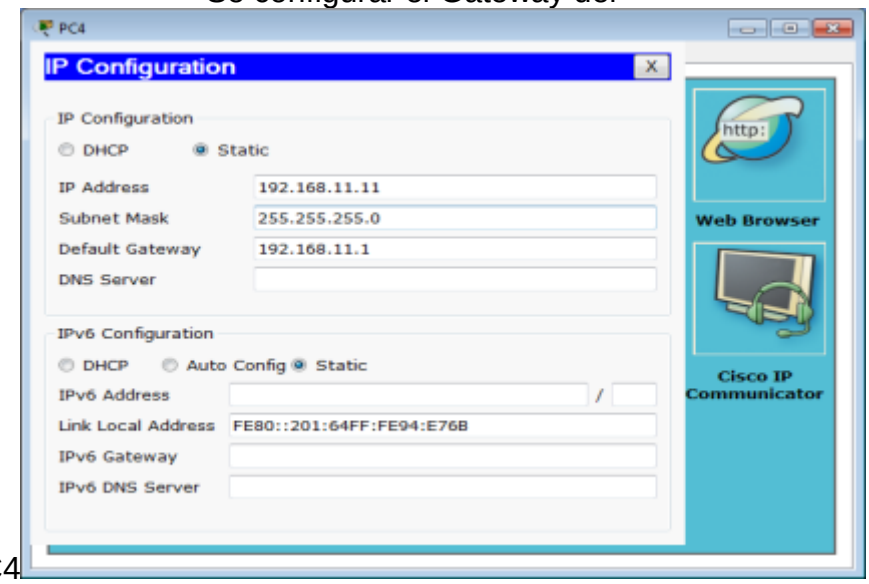
Paso 1: Implementar soluciones para abordar los problemas de conectividad

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

Se procede a configurar la ip del PC1

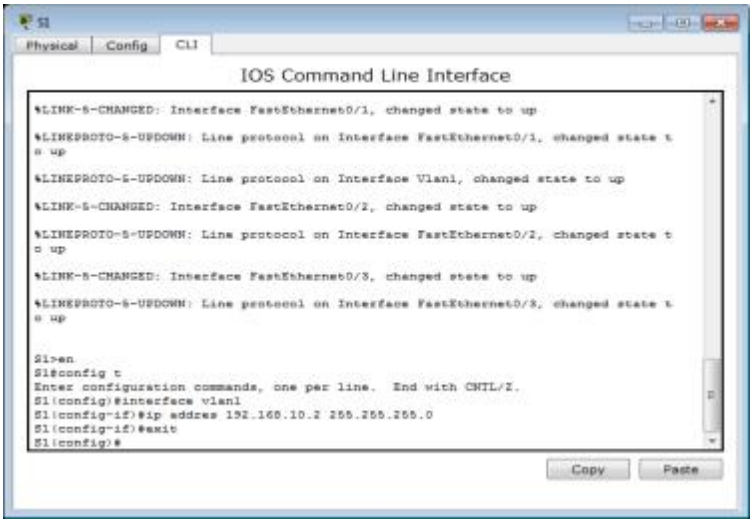


Se configurar el Gateway del

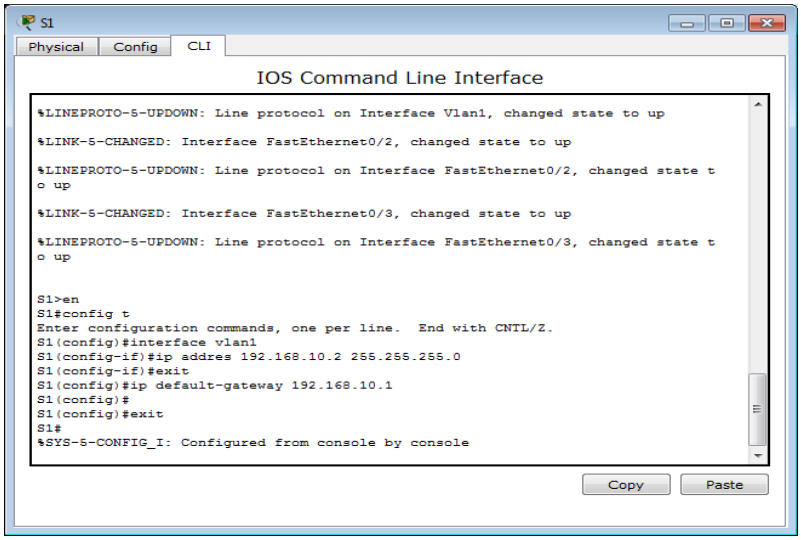


PC4

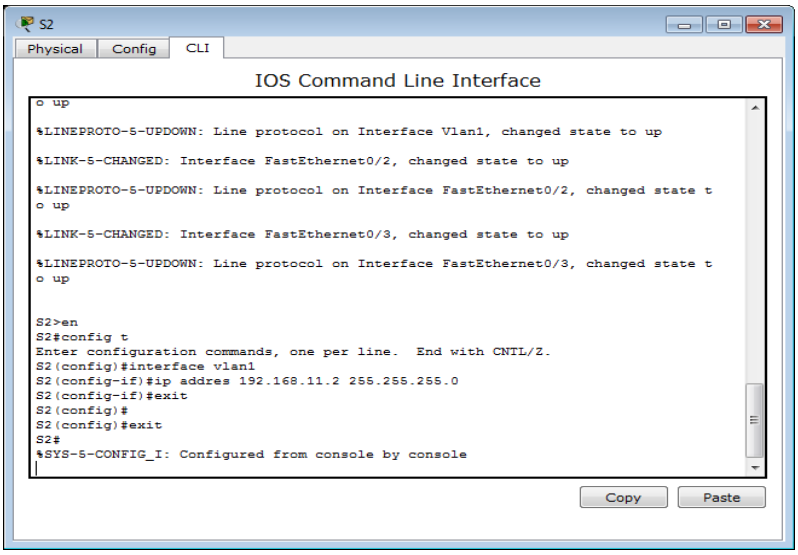
Se ingresa al Switch 1 y se configura la ip y la mascara de subnet



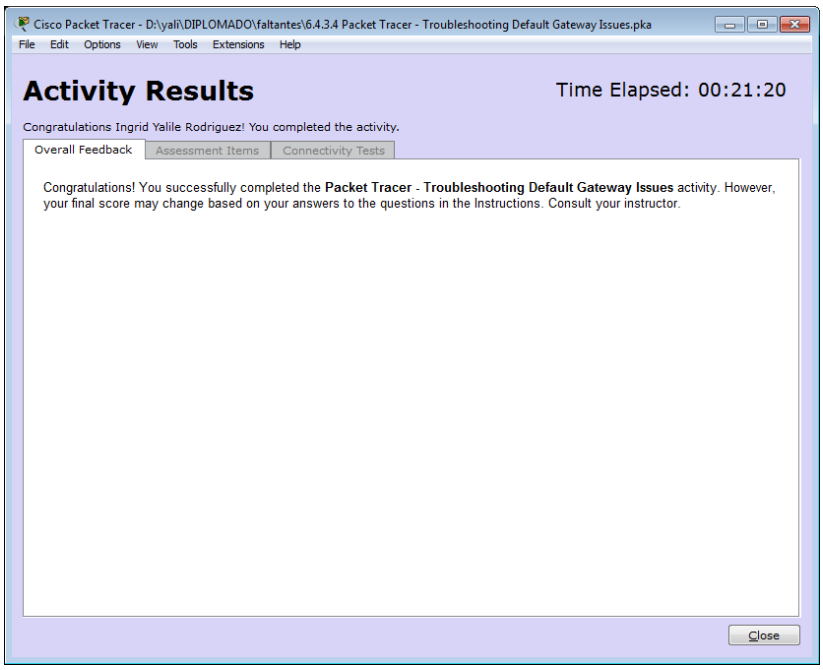
De la misma forma se configura el gateway



Se ingresa al Switch 2 y se configura la ip



Se da por terminada el problema



10.4.1.3 Packet Tracer Multiuser - Implement Services Instructions IG

Objetivos Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN. b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad. - El jugador del lado servidor abre el archivo Packet Tracer Multiuser - Implement Services - Server Side.pka. - El jugador del lado cliente abre el archivo Packet Tracer Multiuser - Implement Services - Client Side.pka.

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los switches

Cada jugador: configure su respectivo switch con los siguientes parámetros: Nombre de host que utilice el nombre para mostrar (S1 o S2) Mensaje del día (MOTD) adecuado Cortraseñas de modo EXEC privilegiado y de línea Direccionamiento IP correcto, según Tabla de direccionamiento

Paso 3: Jugador del lado servidor: Configurar el enlace PTMU y comunicar el direccionamiento

a. Complete los pasos necesarios para verificar que el enlace PTMU esté listo para recibir una conexión entrante. b. Comunique la información de configuración necesaria al jugador del lado cliente.

Paso 4: Jugador del lado cliente: Configurar la conexión multiusuario saliente

a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor: Dirección IP: _____ Número de puerto: _____ Contraseña (cisco, de manera predeterminada) _____ b. Configure Peer0 para conectarse al enlace PTMU del jugador del lado servidor. c. Conecte la GigabitEthernet0/1 de S2 al Link0 en Peer0.

Función Multiusuario de Packet Tracer: Implementación de servicios

Paso 5: Verificar la conectividad a través de una conexión multiusuario local

a. El jugador del lado servidor debe poder hacer ping al S2 en la instancia de Packet Tracer del jugador del lado cliente. b. El jugador del lado cliente debe poder hacer ping al S1 en la instancia de Packet Tracer del jugador del lado servidor.

Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Paso 1: Configurar WRS como servidor de DHCP

WRS proporciona servicios de DHCP. Establezca los siguientes parámetros para la configuración del servidor de DHCP: La dirección IP de inicio es 172.16.1.11. La cantidad máxima de usuarios es 100. El DNS 1 estático es 172.16.1.5. Verifique si NetAdmin recibió el direccionamiento IP mediante DHCP. En NetAdmin, acceda a la página Web User Account Information (Información de cuenta de usuario) en 172.16.1.5. Utilizará esta información para configurar las cuentas de usuario en el paso 2.

Paso 2: Configurar servicios en www.ptmu.test

El servidor www.ptmu.test proporciona el resto de los servicios y se debe configurar con lo siguiente: Un registro DNS que asocie la dirección IP del servidor www.ptmu.test al nombre www.ptmu.test. Cuentas de usuario y servicios de correo electrónico según la lista de usuarios. El nombre de dominio es ptmu.test. Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.

Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos

En NetAdmin, realice lo siguiente: Configure el cliente de correo electrónico para la cuenta de usuario de NetAdmin. Envíe un correo electrónico al usuario de la PC1. Suba el archivo secret.txt al servidor FTP. No modifique el archivo.

Nota: la puntuación para el jugador del lado servidor será de 43/44 hasta que el jugador del lado cliente descargue correctamente el archivo secret.txt, lo modifique y lo suba al servidor FTP www.ptmu.test.

Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Paso 1: Configurar y verificar el direccionamiento de las PC

a. Configure la PC1 y la PC2 para obtener el direccionamiento automáticamente. b. Las PC1 y PC2 deben poder acceder a la página Web http://www.ptmu.test.

Función Multiusuario de Packet Tracer: Implementación de servicios

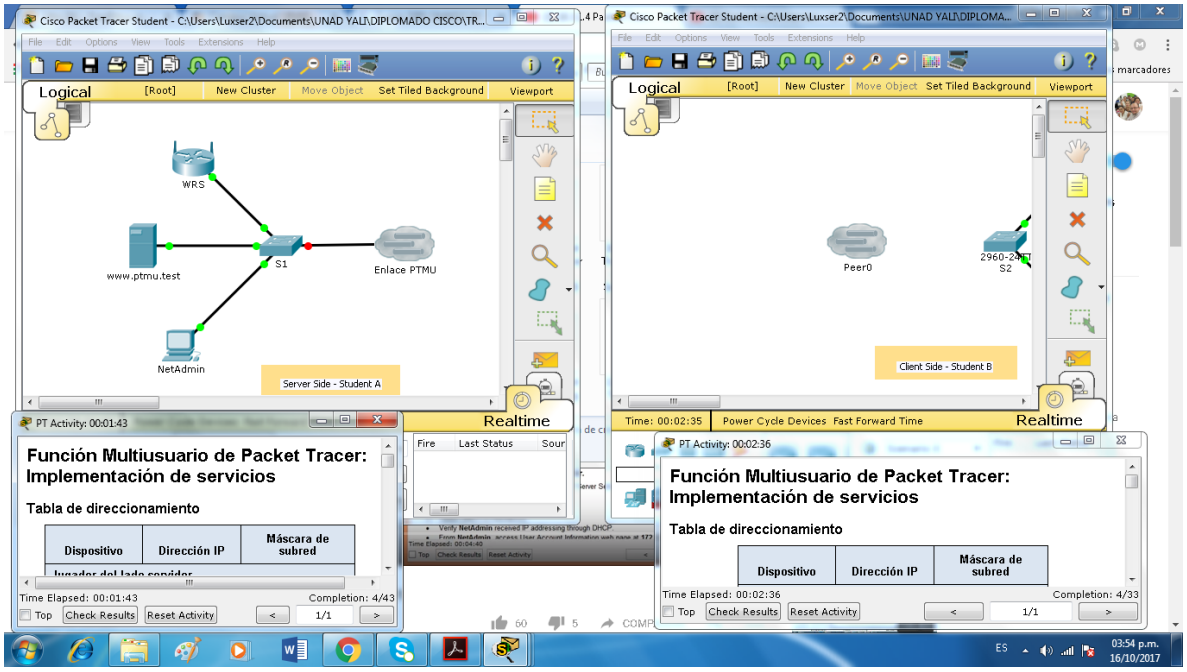
Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

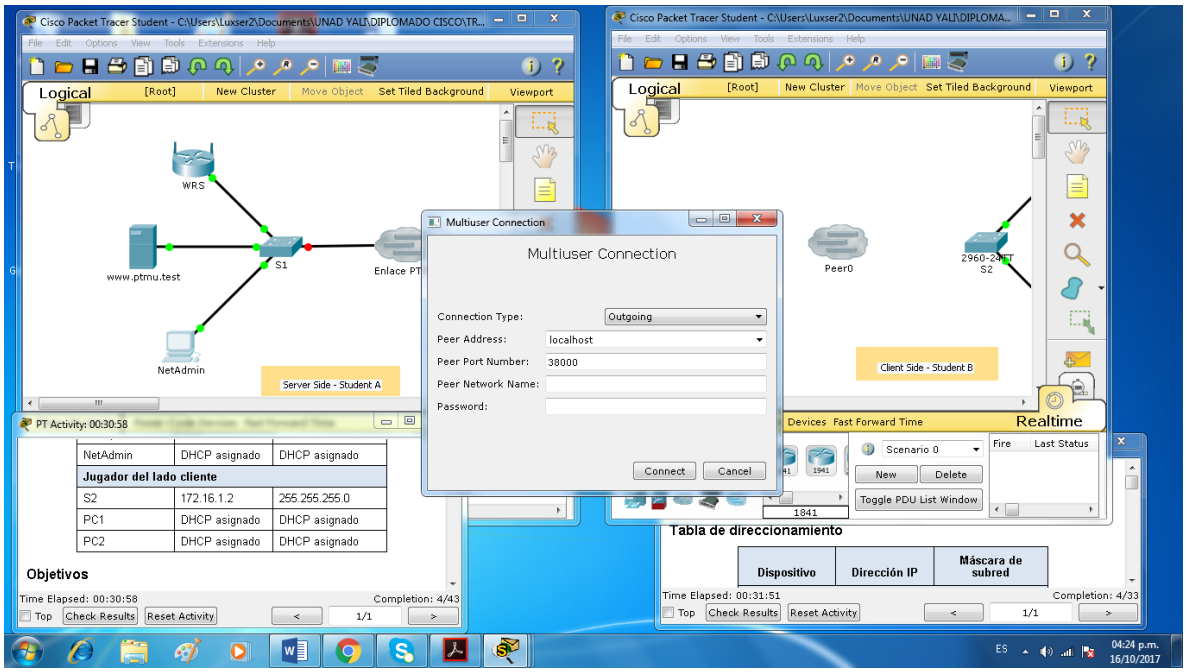
a. Configure las cuentas de correo electrónico según los requisitos que se indican en www.ptmu.test/user.html. b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta. c. Envíe un correo electrónico

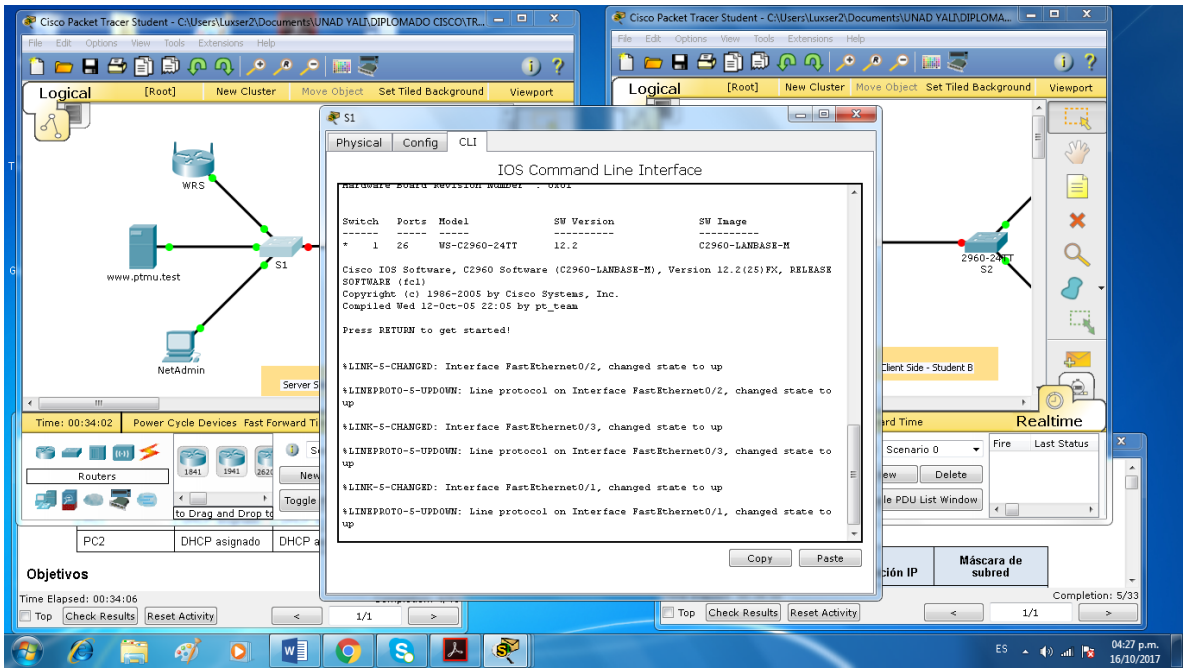
de la PC1 a la PC2. Nota: la puntuación no cambiará. d. Verifique si la PC2 recibió un correo electrónico de la PC1.

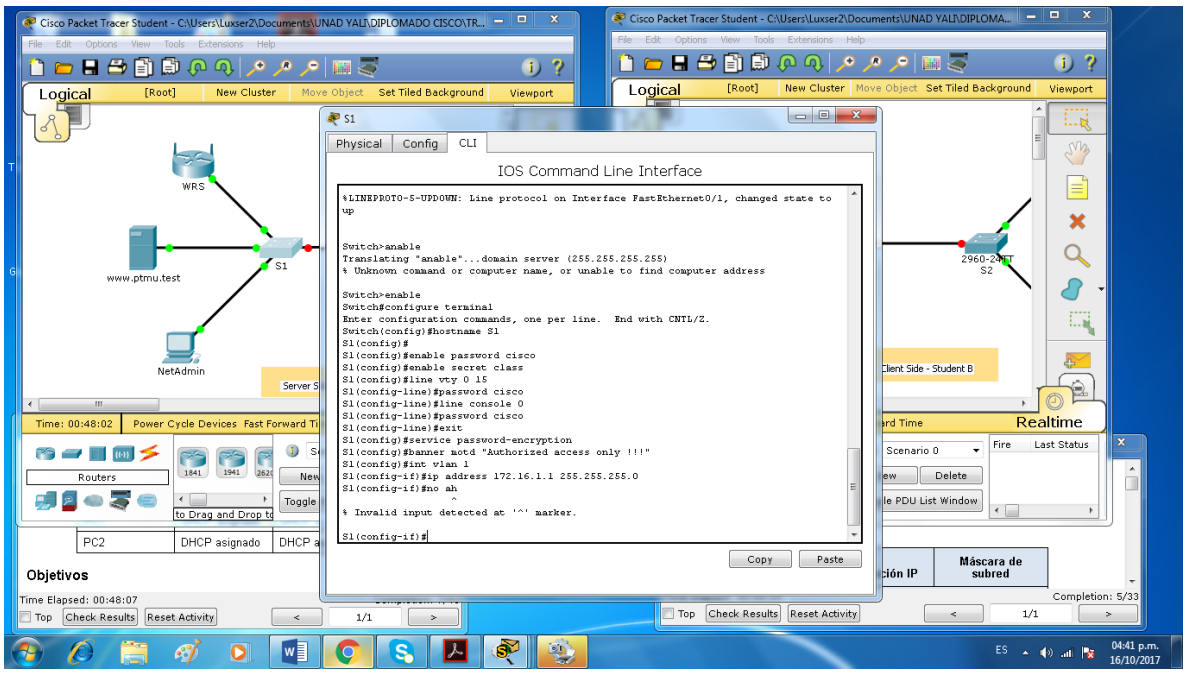
Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

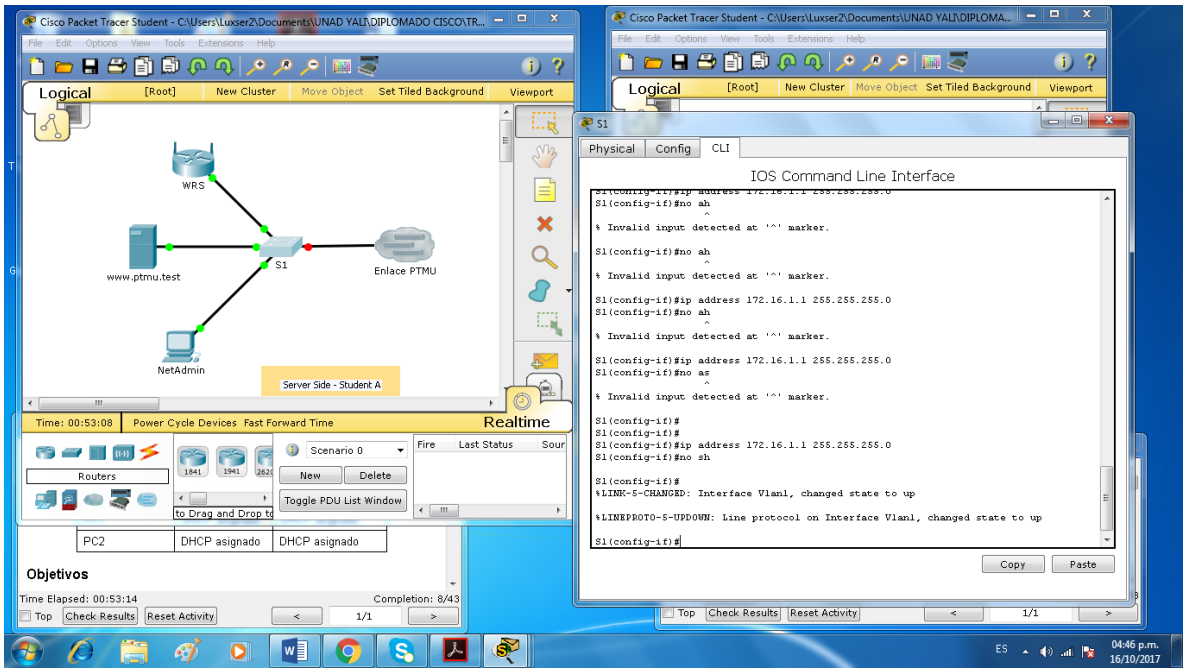
a. En la PC2, acceda al servidor FTP y descargue el archivo secret.txt. b. Abra el archivo secret.txt, solo cambie la palabra secreta por apple y suba el archivo. c. La puntuación del jugador del lado servidor debería ser 44/44 y la del jugador del lado cliente debería

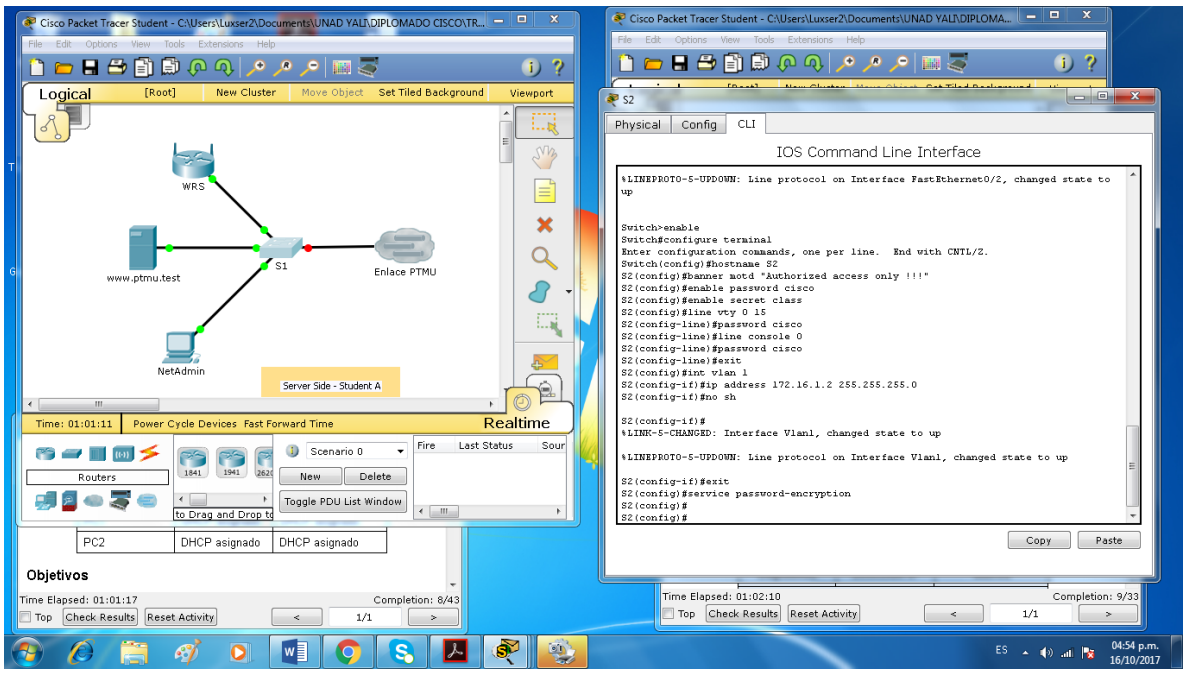


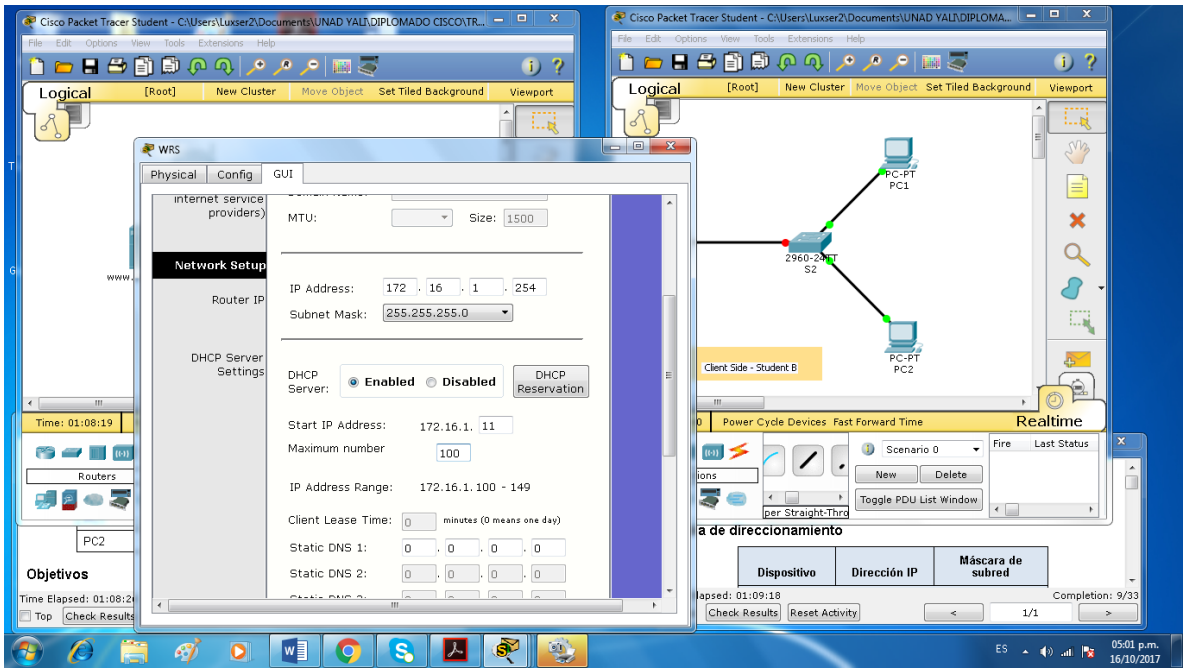


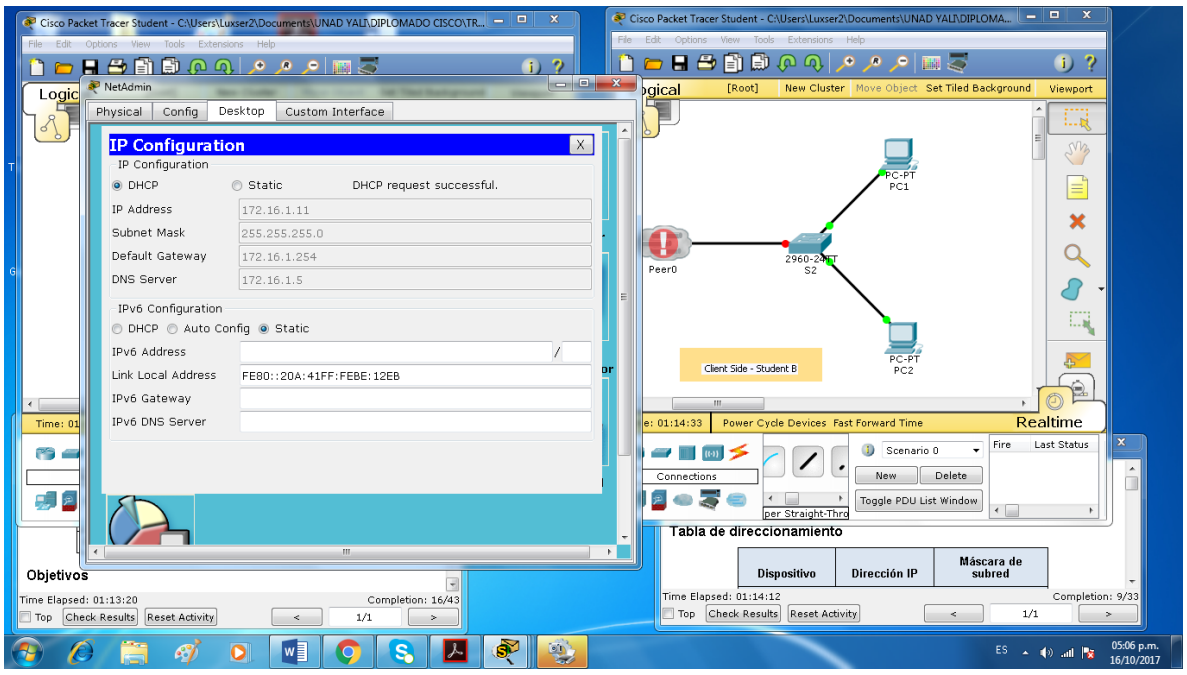

S1
Physical
Config
CLI
IOS Command Line Interface
Switch Ports Model SW Version SW Image
1 26 WS-C2960-24TT 12.2 C2960-LANBASE-M
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Copy
Paste
Logical
Realtime
Objetivos

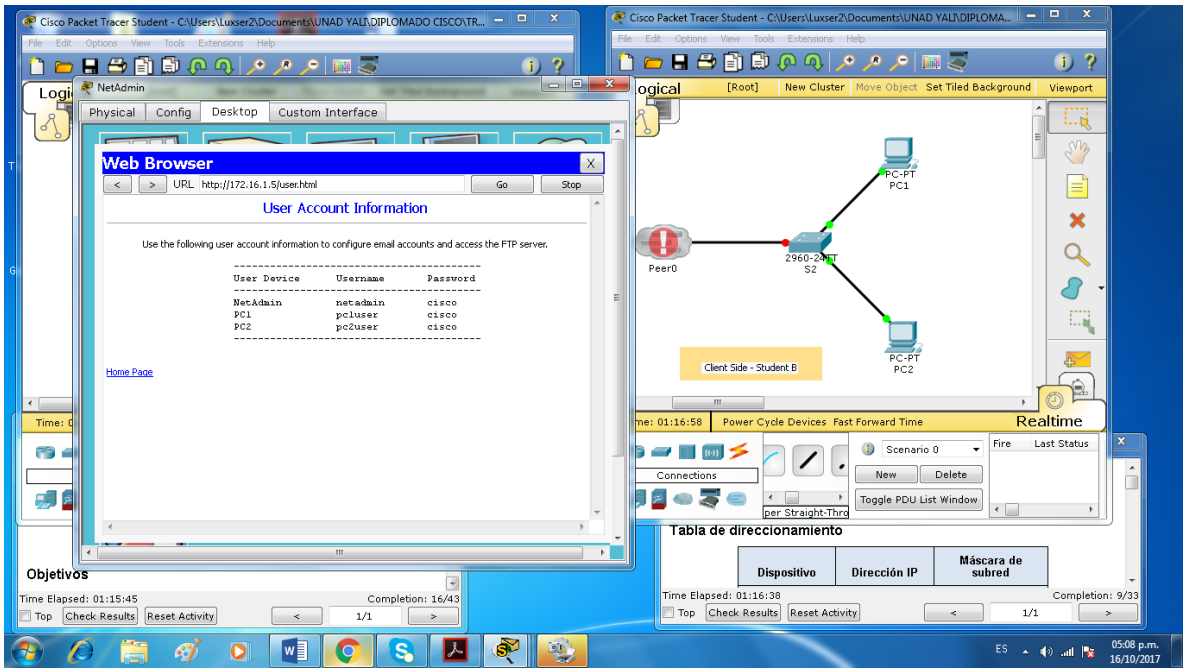

S1
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch>enable
Translating "enable"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
S1(config)#enable password cisco
S1(config)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#line console 0
S1(config-line)#password cisco
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Authorized access only !!!"
S1(config)#int vlan 1
S1(config-if)#ip address 172.16.1.1 255.255.255.0
S1(config-if)#no ah
% Invalid input detected at '^' marker.
S1(config-if)#
Copy
Paste
Logical
Realtime
Objetivos

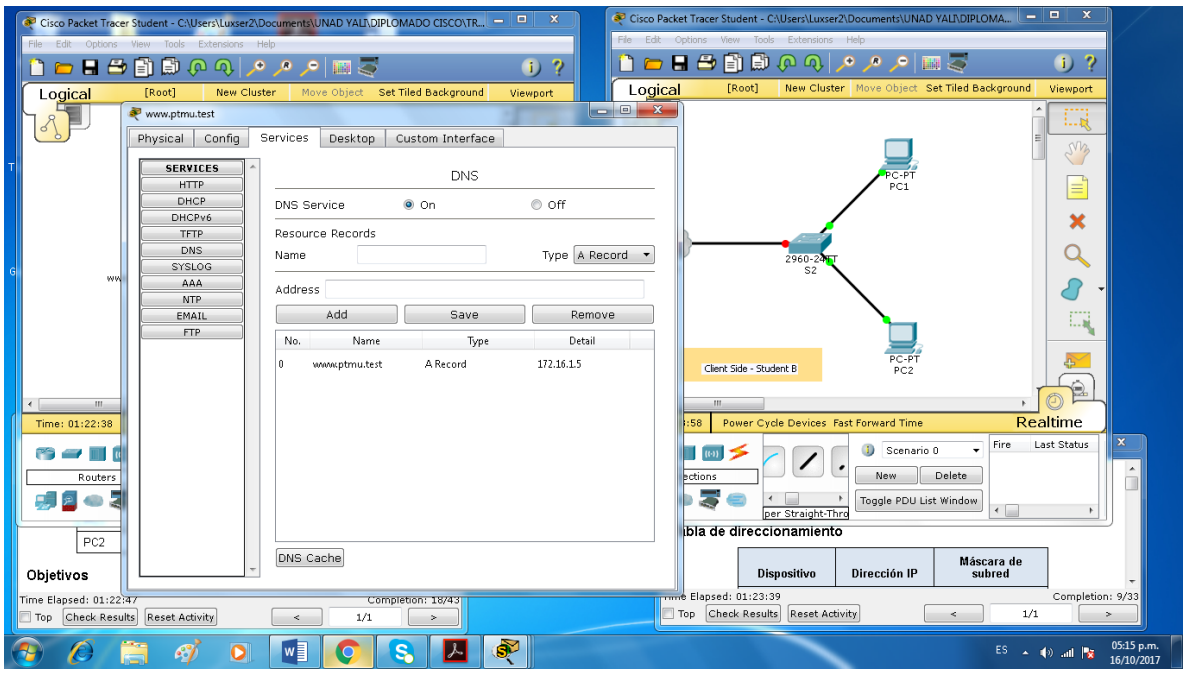

Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TR...
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
WRS
www.ptmu.test
S1
Enlace PTMU
NetAdmin
Server Side - Student A
Time: 00:53:08
Power Cycle Devices
Fast Forward Time
Realtime
Routers
Scenario 0
New
Delete
Toggle PDU List Window
PC2
DHCP asignado
DHCP asignado
Objetivos
Time Elapsed: 00:53:14
Completion: 8/43
Check Results
Reset Activity
S1
Physical
Config
CLI
IOS Command Line Interface
S1(config-if)#no ah
% Invalid input detected at '^' marker.
S1(config-if)#ip address 172.16.1.1 255.255.255.0
S1(config-if)#no as
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Copy
Paste
04:46 p.m.
16/10/2017

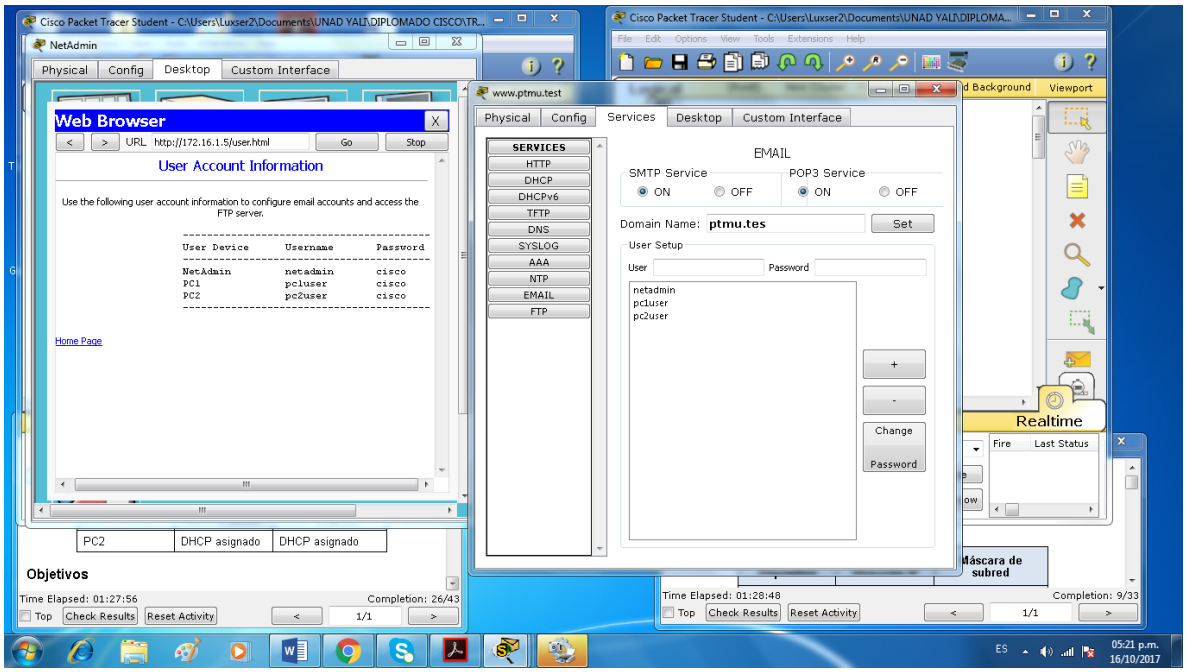

Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TR...
Logical
WRS
www.ptmu.test
S1
Enlace PTMU
NetAdmin
Server Side - Student A
Time: 01:01:11
Power Cycle Devices
Fast Forward Time
Realtime
Routers
Scenario 0
New
Delete
Toggle PDU List Window
PC2
DHCP asignado
DHCP asignado
Objetivos
Time Elapsed: 01:01:17
Completion: 8/43
Check Results
Reset Activity
S2
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#banner motd "Authorized access only !!!"
S2(config)#enable password cisco
S2(config)#enable secret class
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#line console 0
S2(config-line)#password cisco
S2(config-line)#exit
S2(config)#int vlan 1
S2(config-if)#ip address 172.16.1.2 255.255.255.0
S2(config-if)#no sh
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S2(config-if)#exit
S2(config)#service password-encryption
S2(config)#
S2(config)#
Copy
Paste
Time Elapsed: 01:02:10
Completion: 9/33
04:54 p.m.
16/10/2017

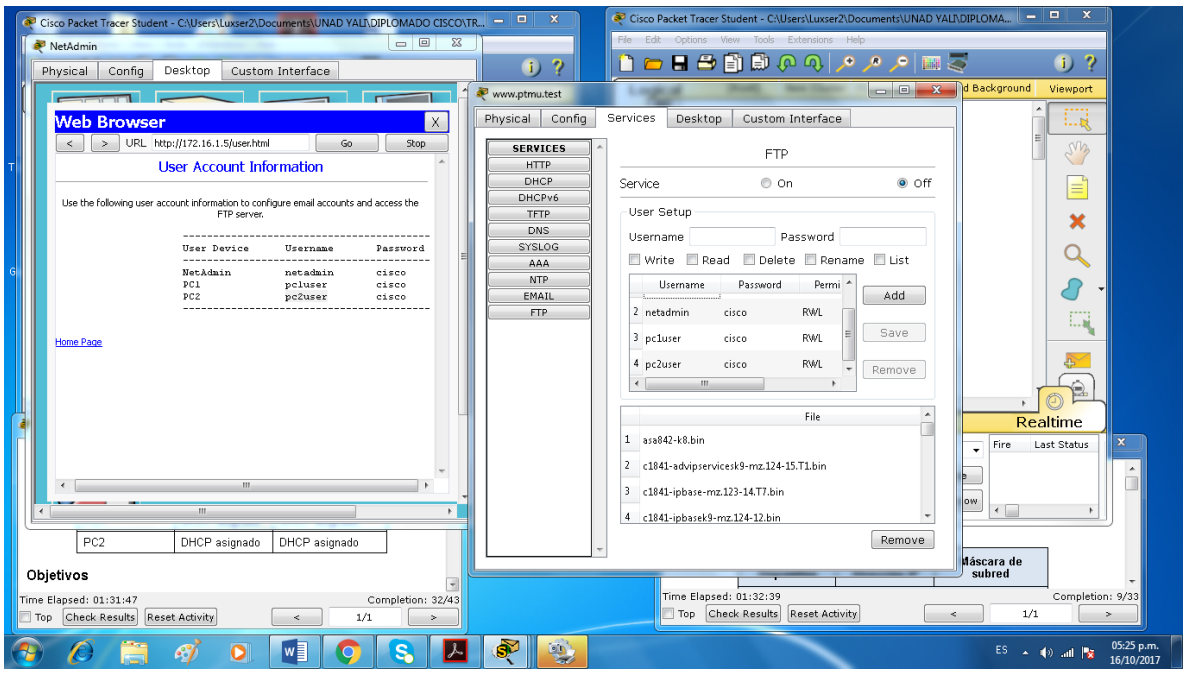

WRS
Physical
Config
GUI
Network Setup
Router IP
DHCP Server Settings
MTU:
Size:
1500
IP Address:
172 . 16 . 1 . 254
Subnet Mask:
255.255.255.0
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
172.16.1. 11
Maximum number
100
IP Address Range:
172.16.1.100 - 149
Client Lease Time:
minutes (0 means one day)
Static DNS 1:
Static DNS 2:
Logical
PC-PT PC1
2960-24TT S2
PC-PT PC2
Client Side - Student B
Realtime
Objetivos
Dispositivo
Dirección IP
Máscara de subred

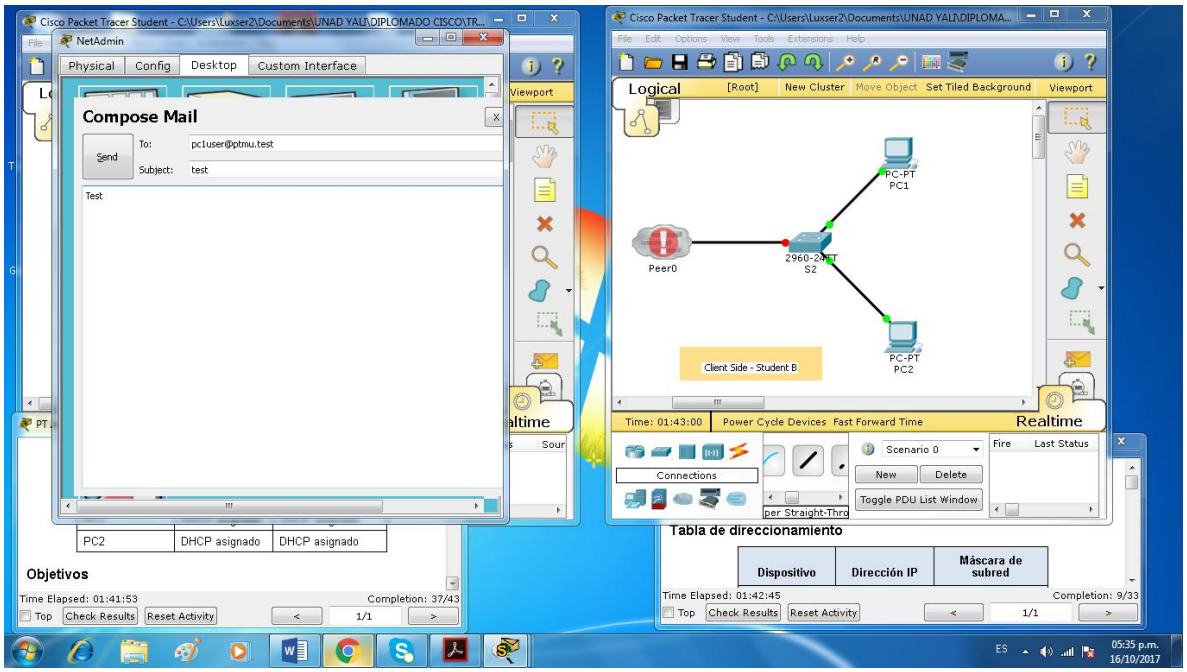

NetAdmin
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
172.16.1.11
Subnet Mask
255.255.255.0
Default Gateway
172.16.1.254
DNS Server
172.16.1.5
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FEBE:12EB
IPv6 Gateway
IPv6 DNS Server
Peer0
PC-PT PC1
2960-24TT S2
PC-PT PC2
Client Side - Student B
Realtime
Objetivos
Dispositivo
Dirección IP
Máscara de subred

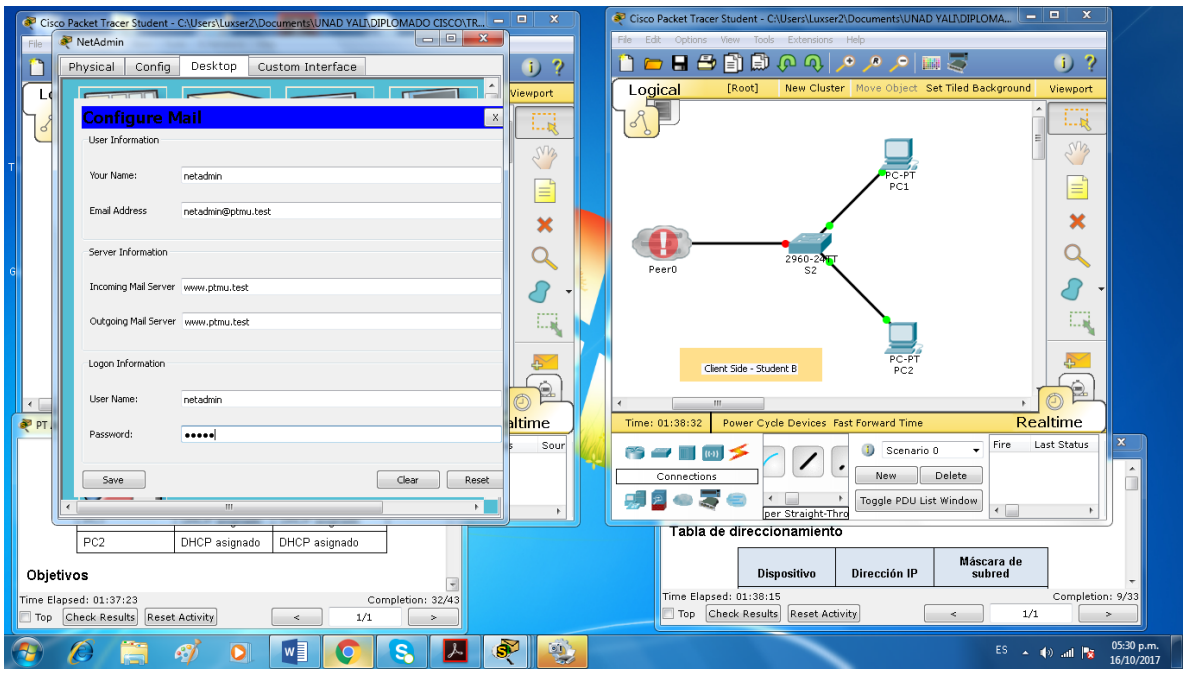

Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TR...
NetAdmin
Physical
Config
Desktop
Custom Interface
Web Browser
URL http://172.16.1.5/user.html
Go
Stop
User Account Information
Use the following user account information to configure email accounts and access the FTP server.
User Device Username Password
NetAdmin netadmin cisco
PC1 pc1user cisco
PC2 pc2user cisco
Home Page
Objetivos
Time Elapsed: 01:15:45
Completion: 16/43
Check Results
Reset Activity
Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMA...
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT PC1
Peer0
2960-24TT S2
PC-PT PC2
Client Side - Student B
Power Cycle Devices
Fast Forward Time
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Connections
Tabla de direccionamiento
Dispositivo
Dirección IP
Máscara de subred
Time Elapsed: 01:16:38
Completion: 9/33
ES
05:08 p.m.
16/10/2017


Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TR...
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
www.ptmu.test
Physical
Config
Services
Desktop
Custom Interface
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No. Name Type Detail
0 www.ptmu.test A Record 172.16.1.5
DNS Cache
PC-PT PC1
2960-24TT S2
PC-PT PC2
Client Side - Student B
Power Cycle Devices
Fast Forward Time
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Routers
PC2
Objetivos
Time: 01:22:38
Time Elapsed: 01:22:47
Completion: 18/43
Tabla de direccionamiento
Dispositivo
Dirección IP
Máscara de subred
Time Elapsed: 01:23:39
Completion: 9/33
ES
05:15 p.m.
16/10/2017

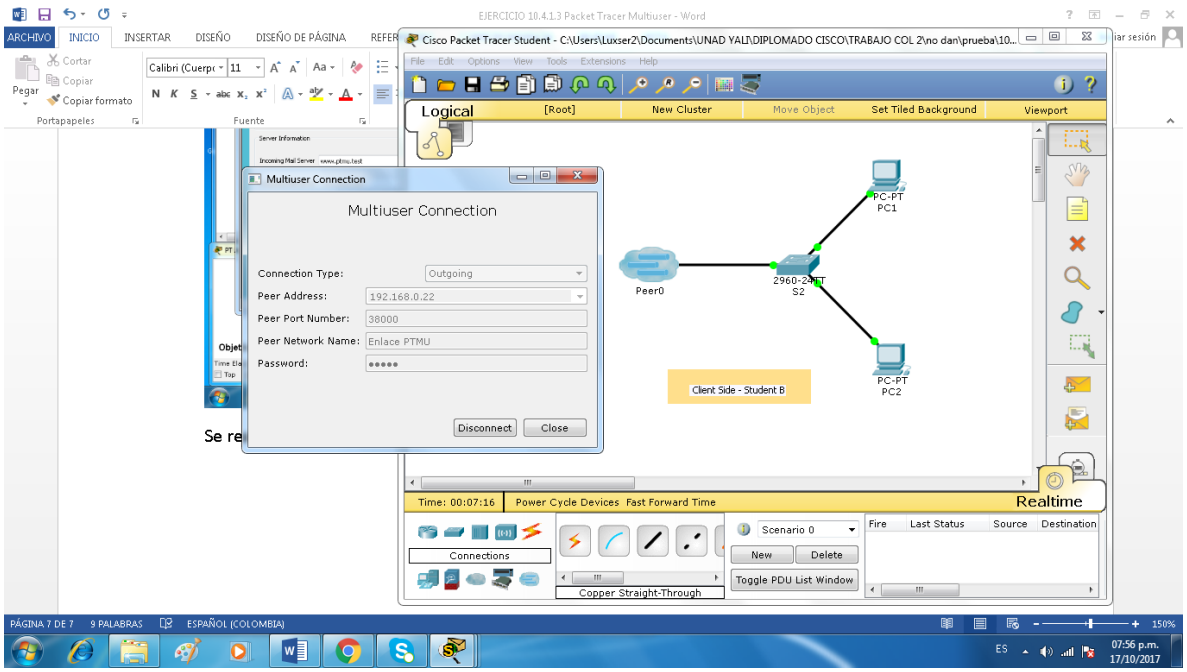

Web Browser
User Account Information
Use the following user account information to configure email accounts and access the FTP server.
User Device Username Password
NetAdmin netadmin cisco
PC1 pc1user cisco
PC2 pc2user cisco
Home Page
PC2 DHCP asignado DHCP asignado
Objetivos
Time Elapsed: 01:27:56
Completion: 26/43
EMAIL
SMTP Service
POP3 Service
Domain Name: ptmu.tes
Set
User Setup
netadmin
pc1user
pc2user
Change Password
Time Elapsed: 01:28:48
Completion: 9/33
Realtime

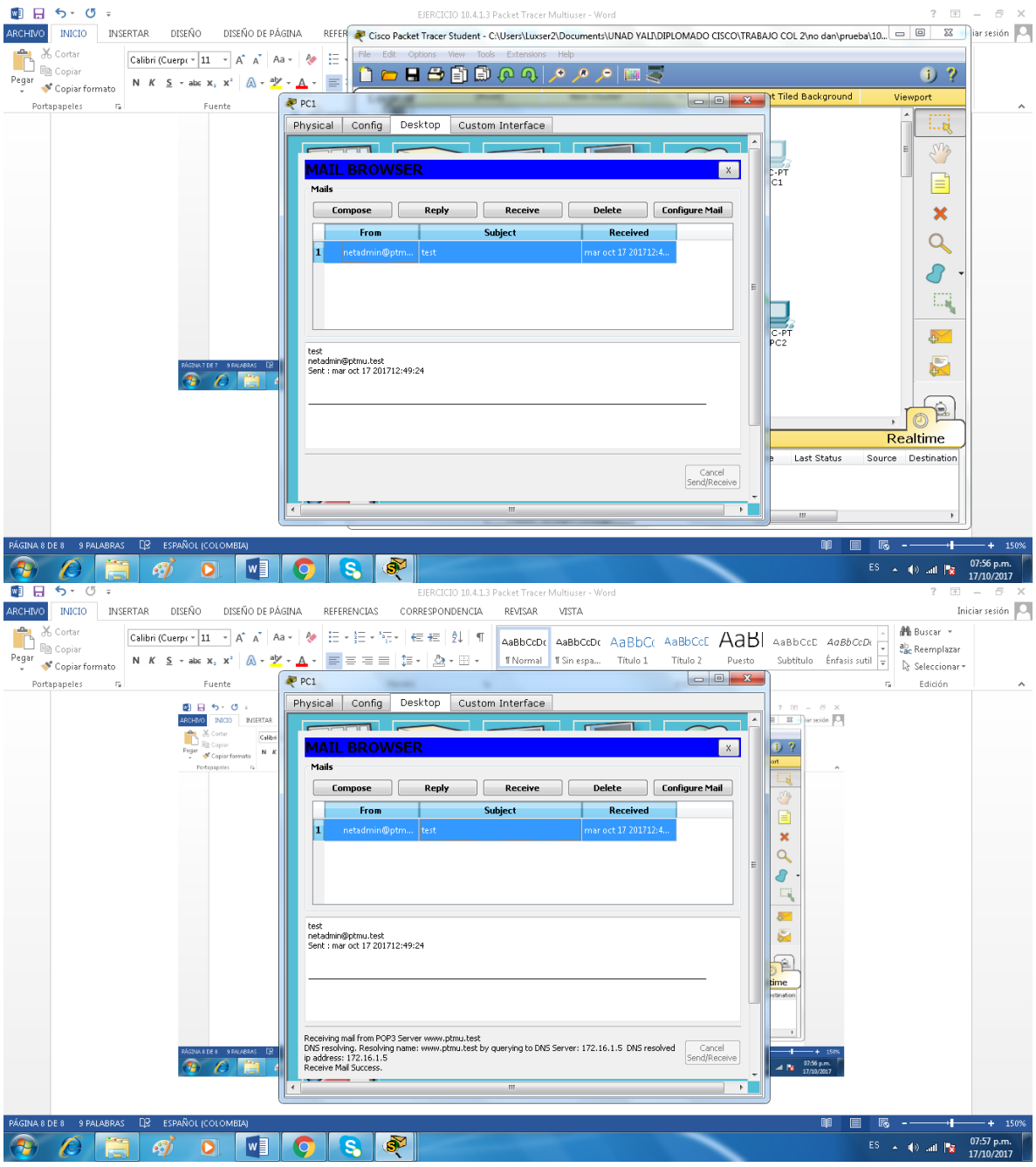

Web Browser
User Account Information
Use the following user account information to configure email accounts and access the FTP server.
User Device Username Password
NetAdmin netadmin cisco
PC1 pc1user cisco
PC2 pc2user cisco
Home Page
PC2 DHCP asignado DHCP asignado
Objetivos
Time Elapsed: 01:31:47
Completion: 32/43
FTP
Service On Off
User Setup
Username Password
Write Read Delete Rename List
Add
Save
Remove
asa842-k8.bin
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbase-mz.123-14.T7.bin
c1841-ipbasek9-mz.124-12.bin
Time Elapsed: 01:32:39
Completion: 9/33
Realtime

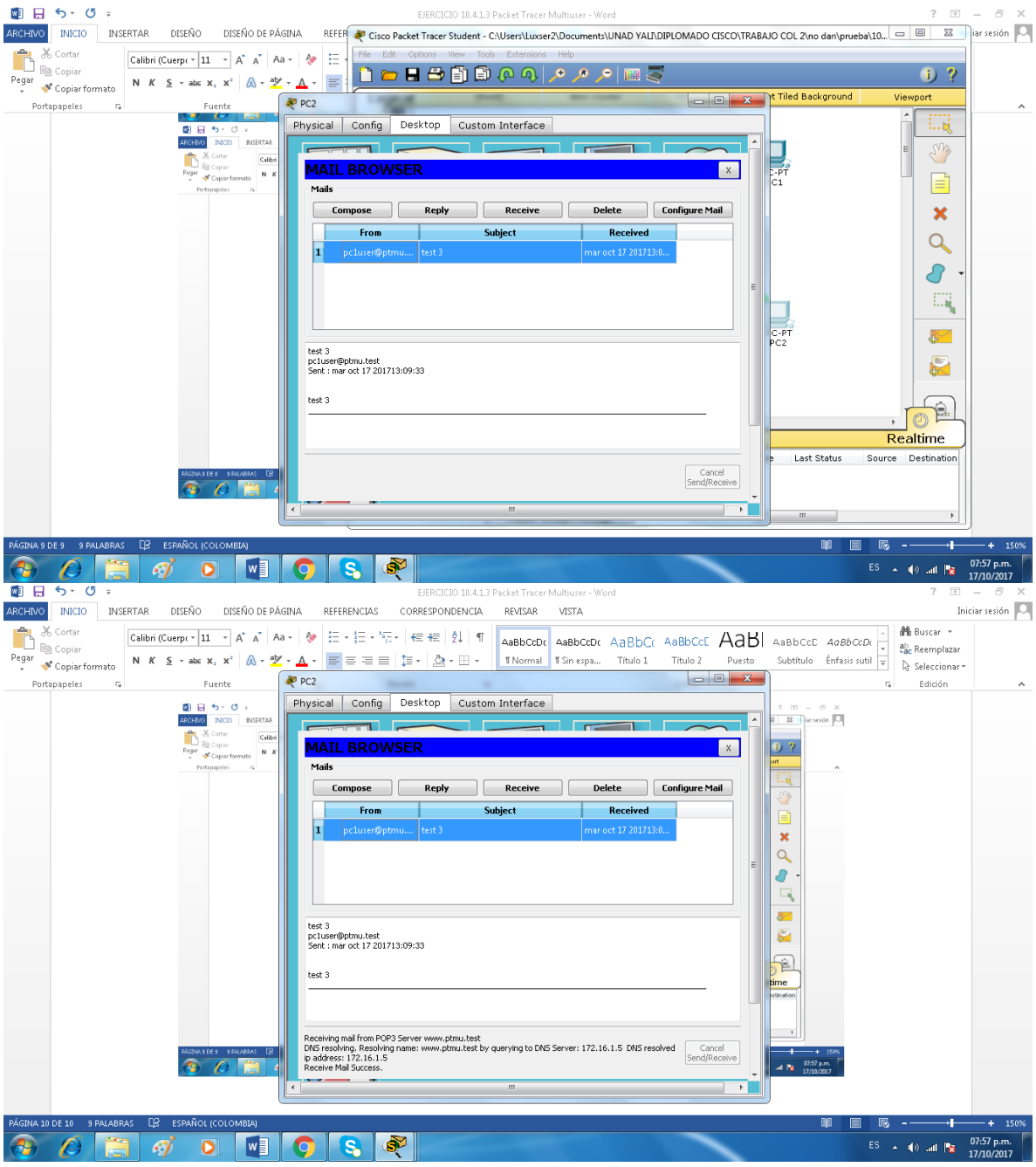


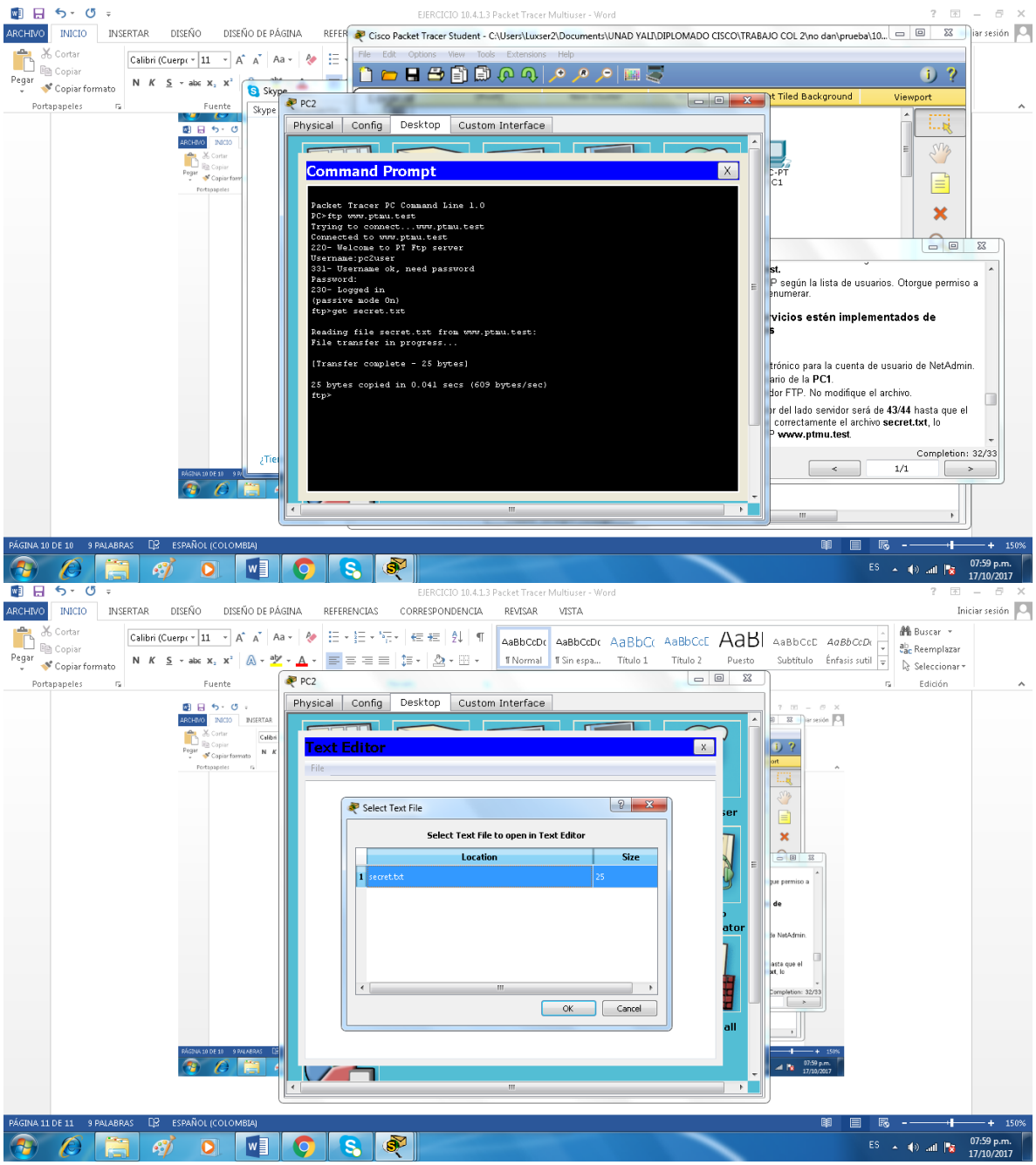


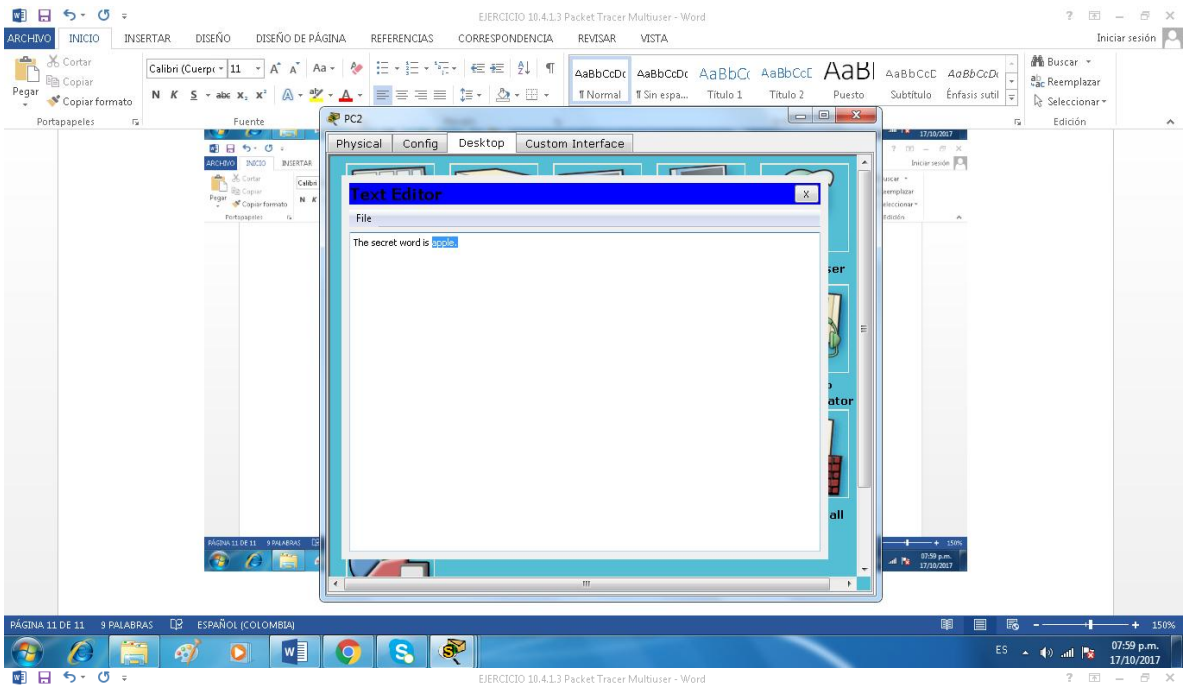
Se realiza la corrección de la conexión del Peer0

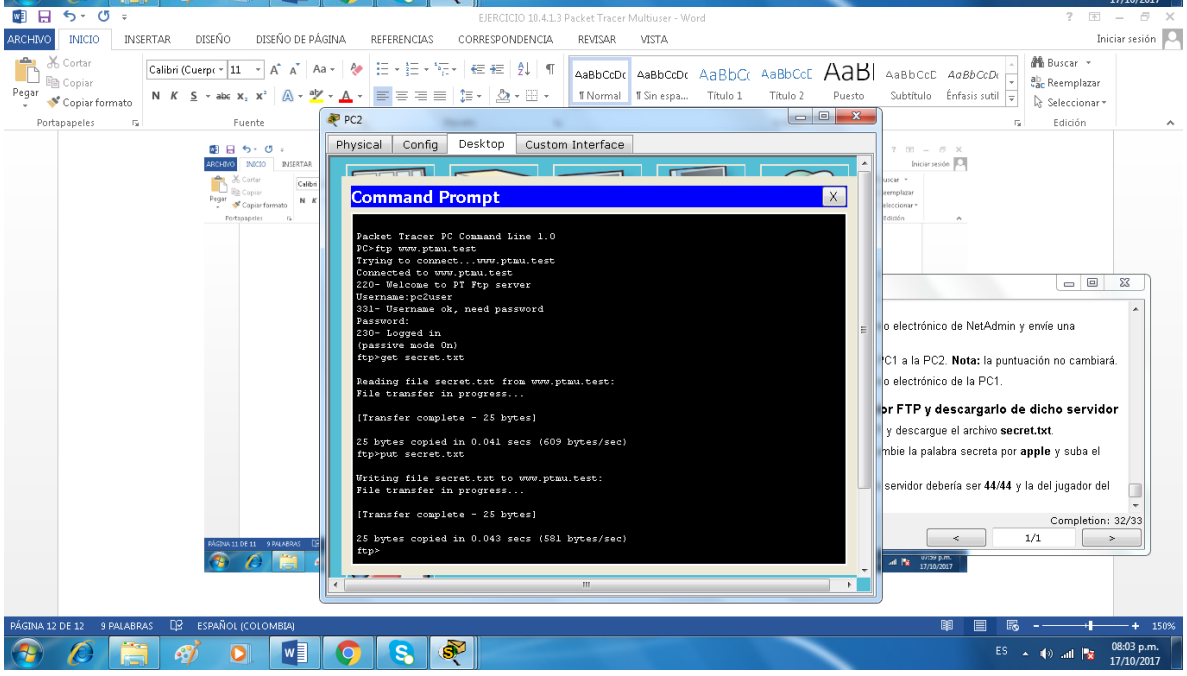

EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
ARCHIVO
INICIO
INSERTAR
DISEÑO
DISEÑO DE PÁGINA
Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TRABAJO COL 2\no dan\prueba\10...
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Multiuser Connection
Connection Type:
Outgoing
Peer Address:
192.168.0.22
Peer Port Number:
38000
Peer Network Name:
Enlace PTMU
Password:
Disconnect
Close
Peer0
2960-24TT
S2
PC-PT
PC1
PC-PT
PC2
Client Side - Student B
Time: 00:07:16
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
PÁGINA 7 DE 7
9 PALABRAS
ESPAÑOL (COLOMBIA)
150%
07:56 p.m.
17/10/2017

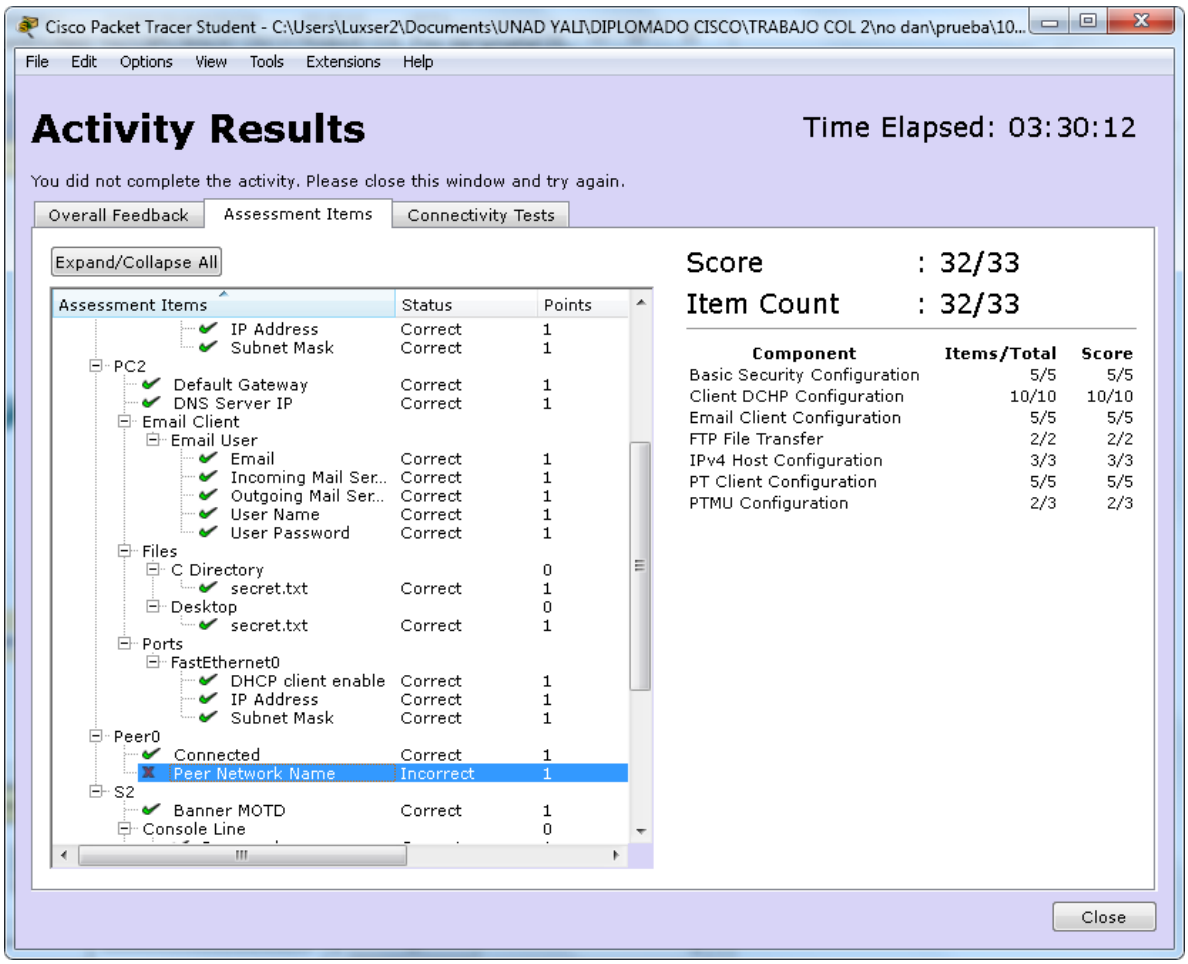

EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TRABAJO COL 2\no dan\prueba\10...
PC1
Physical
Config
Desktop
Custom Interface
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
netadmin@ptm...
test
mar oct 17 201712:4...
test
netadmin@ptmu.test
Sent : mar oct 17 201712:49:24
Cancel
Send/Receive
Realtime
Last Status
Source
Destination
PÁGINA 8 DE 8
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:56 p.m.
17/10/2017
Receiving mail from POP3 Server www.ptmu.test
DNS resolving. Resolving name: www.ptmu.test by querying to DNS Server: 172.16.1.5 DNS resolved ip address: 172.16.1.5
Receive Mail Success.
07:57 p.m.

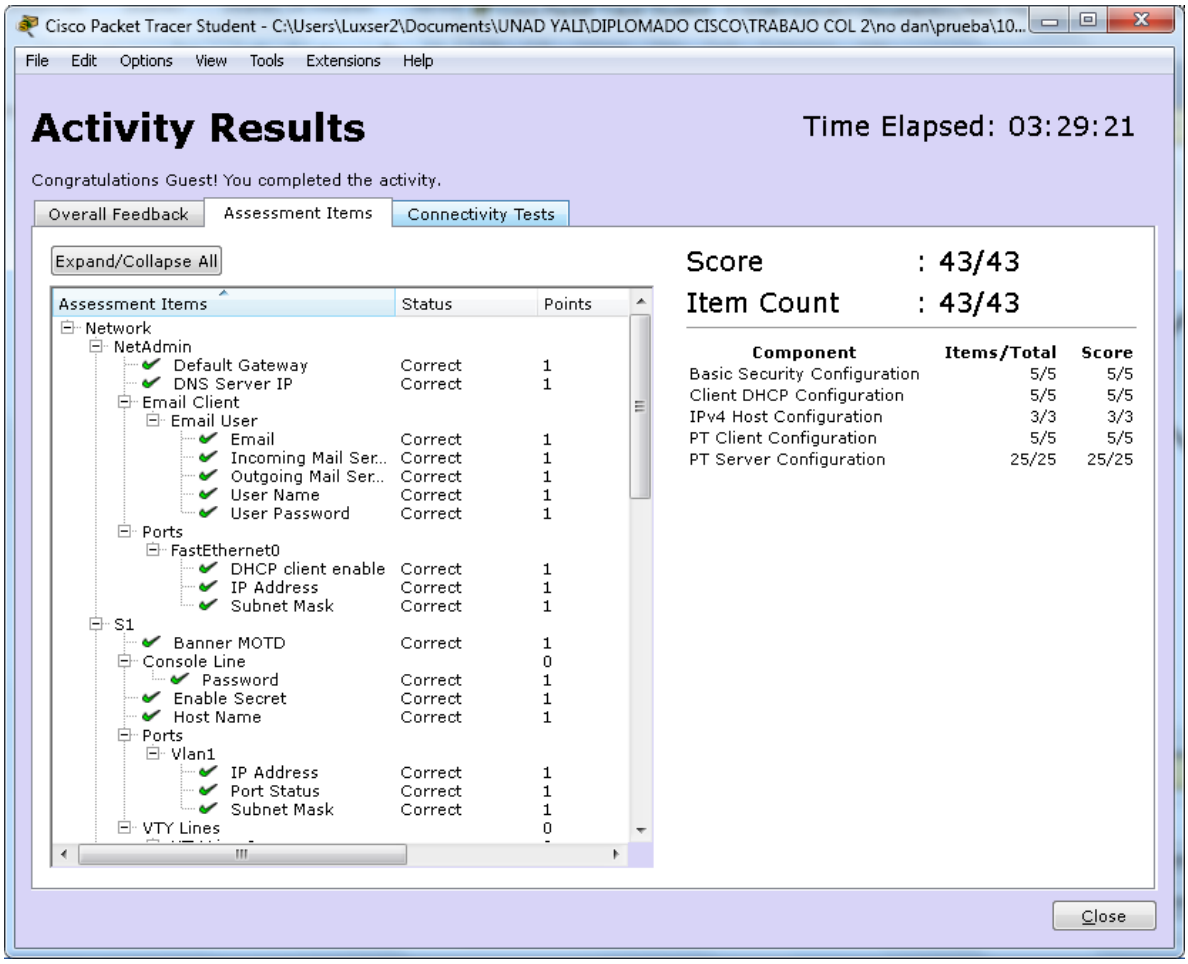

EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TRABAJO COL 2\no dan\prueba\10...
PC2
Physical
Config
Desktop
Custom Interface
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
pc1user@ptmu....
test 3
mar oct 17 201713:0...
test 3
pc1user@ptmu.test
Sent : mar oct 17 201713:09:33
test 3
Cancel
Send/Receive
Realtime
Last Status
Source
Destination
PÁGINA 9 DE 9
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:57 p.m.
17/10/2017
EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
PC2
Physical
Config
Desktop
Custom Interface
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
pc1user@ptmu....
test 3
mar oct 17 201713:0...
test 3
pc1user@ptmu.test
Sent : mar oct 17 201713:09:33
test 3
Receiving mail from POP3 Server www.ptmu.test
DNS resolving. Resolving name: www.ptmu.test by querying to DNS Server: 172.16.1.5 DNS resolved ip address: 172.16.1.5
Receive Mail Success.
Cancel
Send/Receive
PÁGINA 10 DE 10
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:57 p.m.
17/10/2017


EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TRABAJO COL 2\no dan\prueba\10...
PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ftp www.ptmu.test
Trying to connect...www.ptmu.test
Connected to www.ptmu.test
220- Welcome to PT Ftp server
Username:pc2user
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get secret.txt
Reading file secret.txt from www.ptmu.test:
File transfer in progress...
[Transfer complete - 25 bytes]
25 bytes copied in 0.041 secs (609 bytes/sec)
ftp>
Completion: 32/33
1/1
PÁGINA 10 DE 10
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:59 p.m.
17/10/2017
EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
PC2
Physical
Config
Desktop
Custom Interface
Text Editor
File
Select Text File
Select Text File to open in Text Editor
Location
Size
secret.txt
25
OK
Cancel
PÁGINA 11 DE 11
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:59 p.m.
17/10/2017


EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
PC2
Physical
Config
Desktop
Custom Interface
Text Editor
File
The secret word is apple.
PÁGINA 11 DE 11
9 PALABRAS
ESPAÑOL (COLOMBIA)
07:59 p.m.
17/10/2017


EJERCICIO 10.4.1.3 Packet Tracer Multiuser - Word
PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ftp www.ptmu.test
Trying to connect...www.ptmu.test
Connected to www.ptmu.test
220- Welcome to PT Ftp server
Username:pc2user
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get secret.txt
Reading file secret.txt from www.ptmu.test:
File transfer in progress...
[Transfer complete - 25 bytes]
25 bytes copied in 0.041 secs (609 bytes/sec)
ftp>put secret.txt
Writing file secret.txt to www.ptmu.test:
File transfer in progress...
[Transfer complete - 25 bytes]
25 bytes copied in 0.043 secs (581 bytes/sec)
ftp>
Completion: 32/33
PÁGINA 12 DE 12
9 PALABRAS
ESPAÑOL (COLOMBIA)
08:03 p.m.
17/10/2017


Cisco Packet Tracer Student - C:\Users\Luxser2\Documents\UNAD YALI\DIPLOMADO CISCO\TRABAJO COL 2\no dan\prueba\10...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 03:30:12
You did not complete the activity. Please close this window and try again.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
IP Address Correct 1
Subnet Mask Correct 1
PC2
Default Gateway Correct 1
DNS Server IP Correct 1
Email Client
Email User
Email Correct 1
Incoming Mail Ser.. Correct 1
Outgoing Mail Ser.. Correct 1
User Name Correct 1
User Password Correct 1
Files
C Directory 0
secret.txt Correct 1
Desktop 0
secret.txt Correct 1
Ports
FastEthernet0
DHCP client enable Correct 1
IP Address Correct 1
Subnet Mask Correct 1
Peer0
Connected Correct 1
Peer Network Name Incorrect 1
S2
Banner MOTD Correct 1
Console Line 0
Score : 32/33
Item Count : 32/33
Component Items/Total Score
Basic Security Configuration 5/5 5/5
Client DCHP Configuration 10/10 10/10
Email Client Configuration 5/5 5/5
FTP File Transfer 2/2 2/2
IPv4 Host Configuration 3/3 3/3
PT Client Configuration 5/5 5/5
PTMU Configuration 2/3 2/3
Close



9.2.1.11. PacketTracer: configuración de las ACL estándar designadas

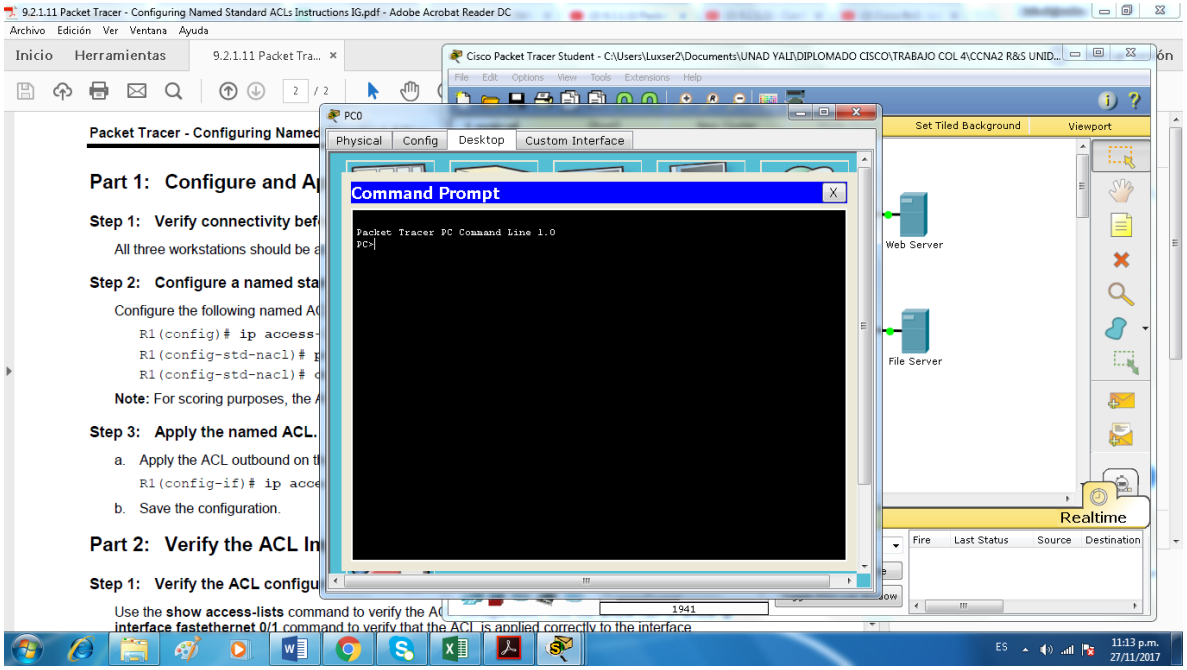
Objetivos

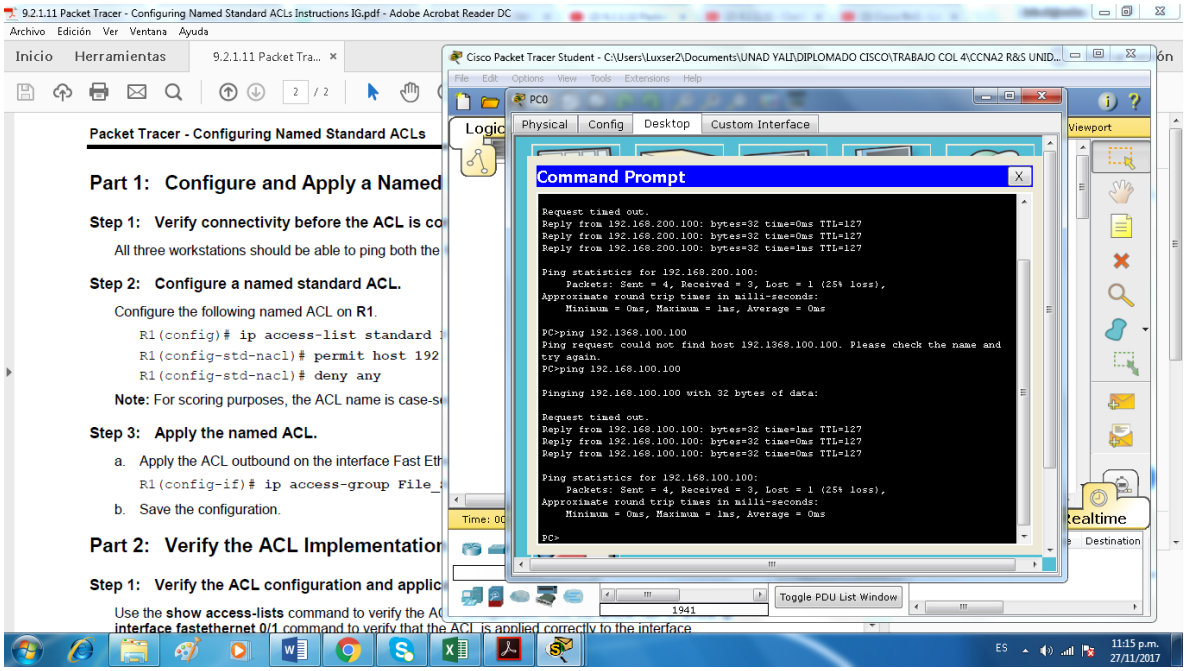
Parte 1: configurar y aplicar una ACL estándar designada

Parte 2: Verificar la implementación de ACL

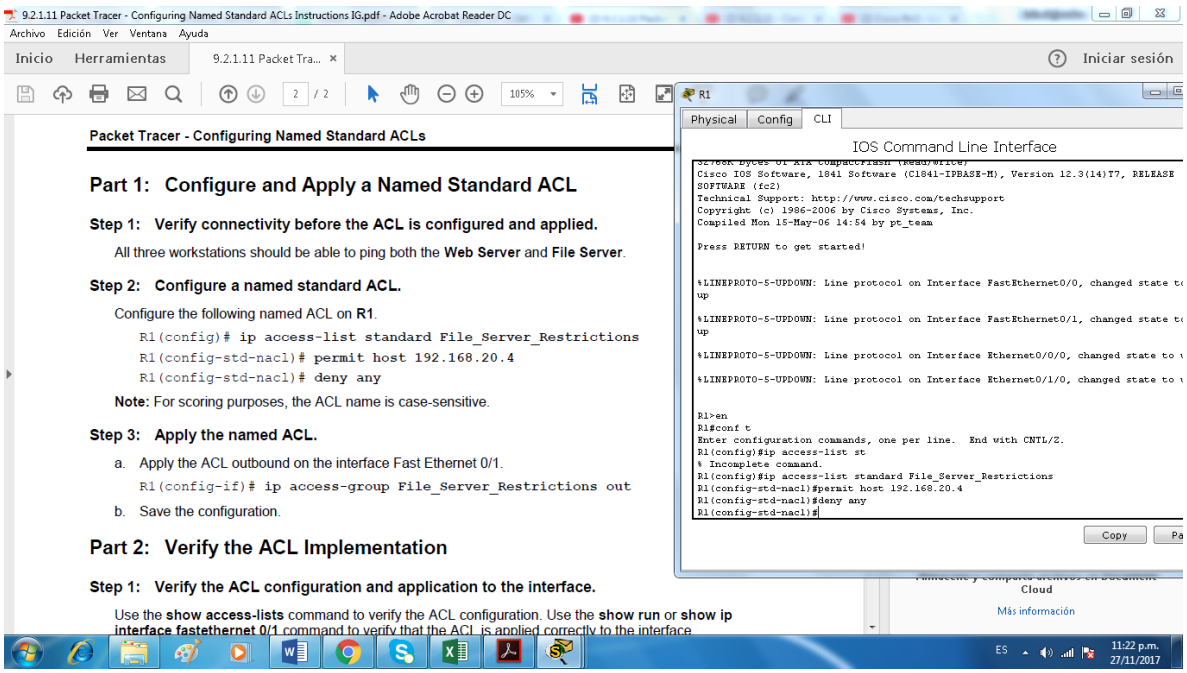
Parte 1: configurar y aplicar una ACL estándar designada

Paso 1: Verifique la conectividad antes de configurar y aplicar la ACL. Las tres estaciones de trabajo deberían poder hacer ping al servidor web y al servidor de archivos.



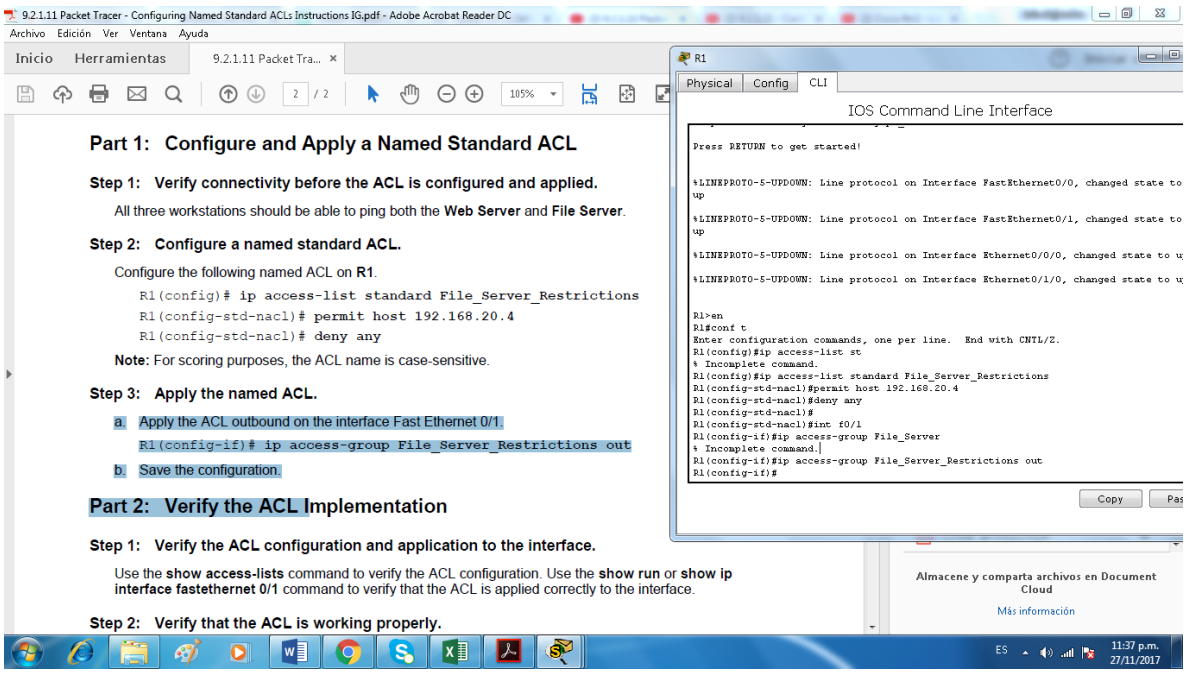


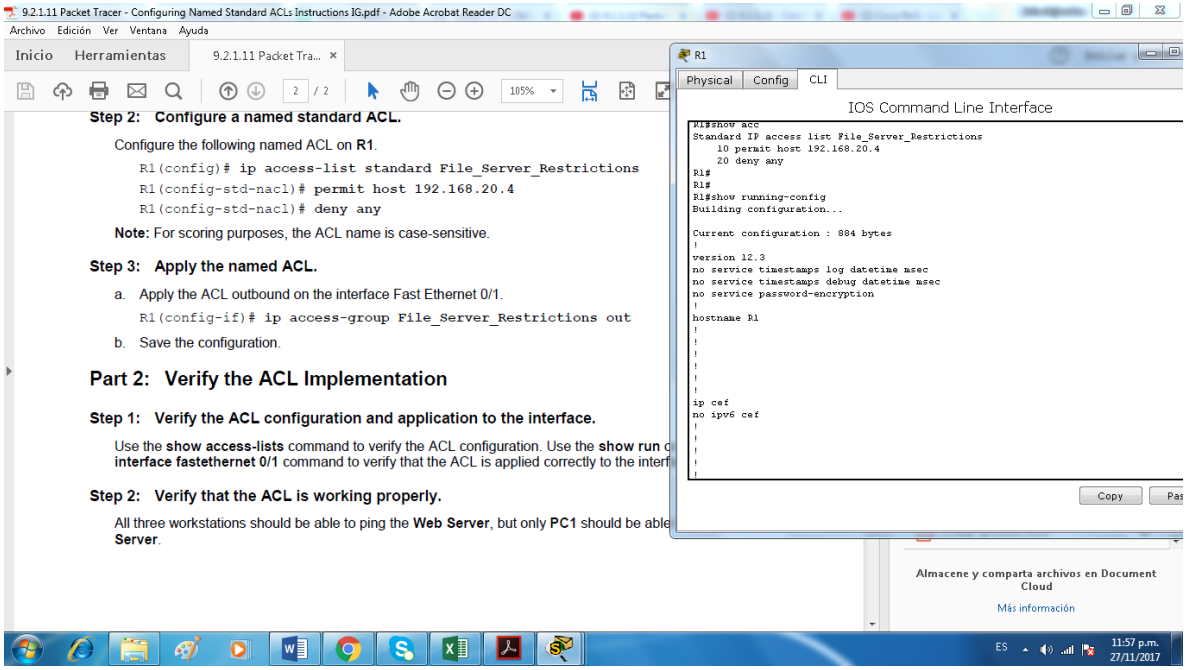
Paso 2: configure una ACL estándar nombrada. Configure la siguiente ACL nombrada en R1.



Paso 3: aplique la ACL nombrada.

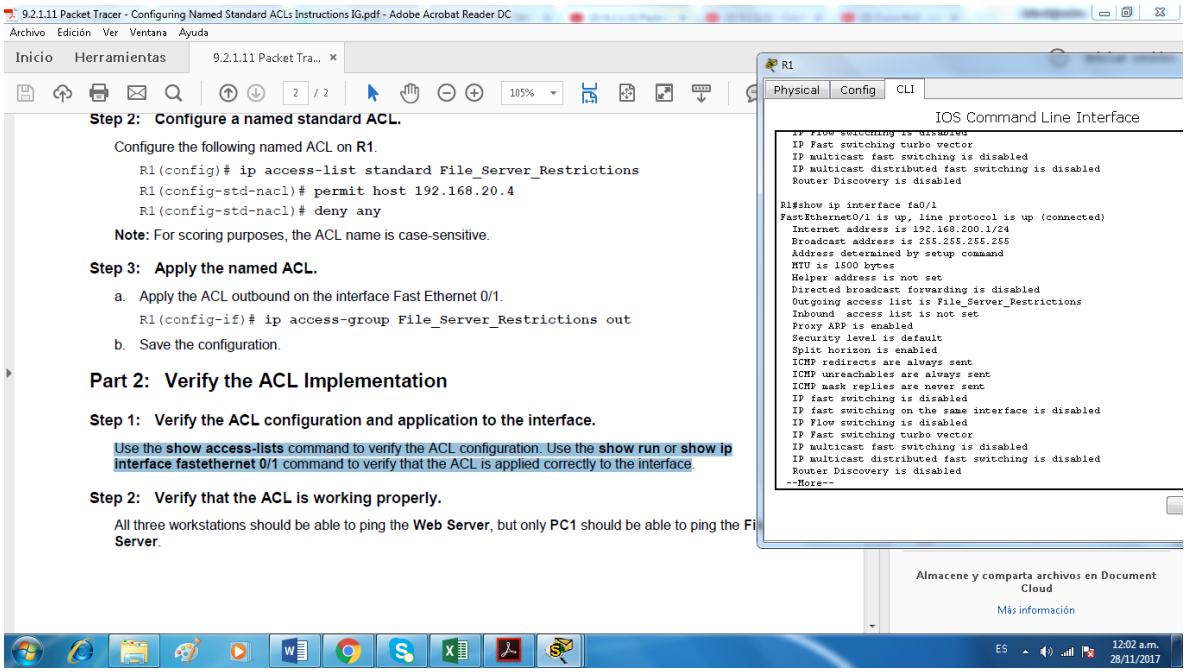
a. Aplicar la ACL saliente en la interfaz Fast Ethernet 0/1. R1 (config-if) # ip access-group File_Server_Restrictions out

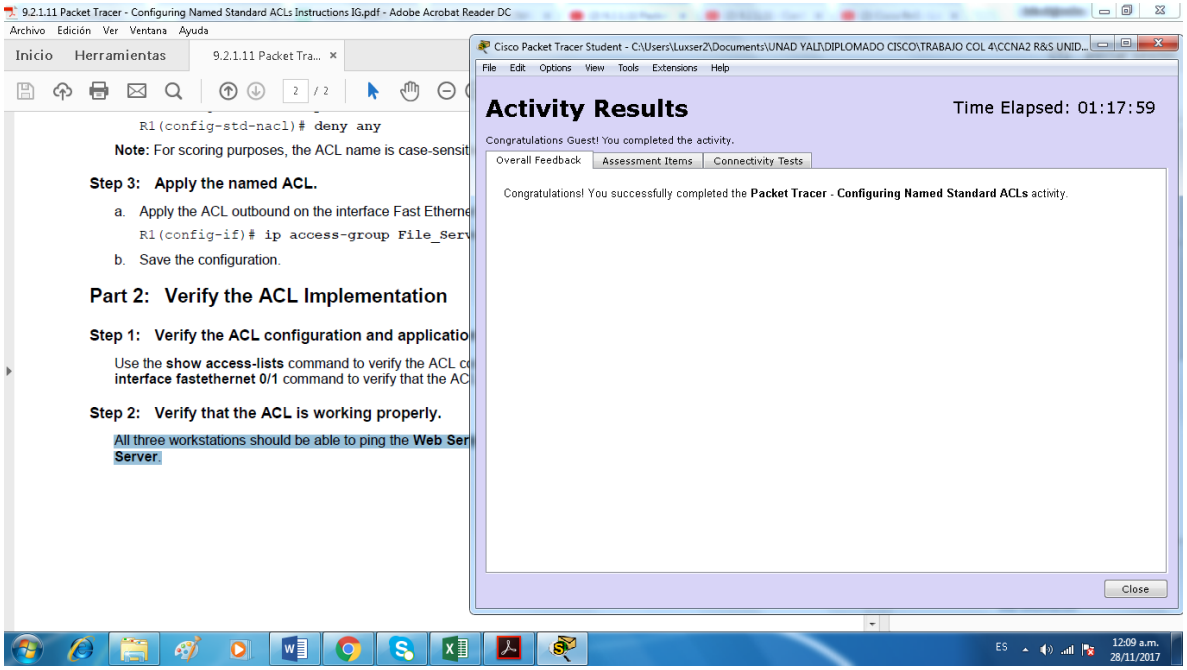




Parte 2: Verificar la implementación de ACL

Paso 1: Verifique la configuración de ACL y la aplicación a la interfaz.
Use el comando show access-lists para verificar la configuración de ACL. Utilice el comando show run o show ip interface fastethernet 0/1 para verificar que la ACL se aplique correctamente a la interfaz.





Función Multiusuario de PacketTracer: Tutorial

Objetivos

Parte 1: Establecer una conexión multiusuario local en otra instancia de PacketTracer

Parte 2: Verificar la conectividad a través de una conexión multiusuario local.

Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.

b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.

- El jugador del lado servidor abre el archivo **PacketTracerMultiuser - Tutorial - Server Side.pka.**

- El jugador del lado cliente abre el archivo **PacketTracerMultiuser - Tutorial - ClientSide.pka.**

Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar

Paso 2: Jugador del lado servidor: configurar el lado servidor del enlace PTMU

El jugador del lado cliente debe contar con la dirección IP, el número de puerto y la contraseña utilizados por el jugador del lado servidor para poder crear una conexión con el jugador del lado servidor.
a. Siga estos pasos para configurar PacketTracer de manera de que esté preparado para recibir una conexión entrante:
1) Haga clic en el menú **Extensions**(Extensiones), después en **Multiuser**(Multiusuario) y, finalmente, en **Listen** (Escuchar).

2) Tiene dos Local ListeningAddresses (Direcciones de escucha locales). Si se indican más de dos direcciones, utilice solo las primeras dos. La primera es la dirección IP real de la máquina local del jugador del lado servidor. Es la dirección IP que utiliza su PC para enviar y recibir datos. La otra dirección IP (127.0.0.1) solamente se puede utilizar para comunicaciones dentro del entorno de su propia PC.

3) El número de puerto se indica junto a las direcciones IP y en el campo Port Number (Número de puerto). Si esta es la primera instancia de PacketTracer que abrió en la PC, el número de puerto será 38000. Sin embargo, si hay varias instancias abiertas, el número aumenta de a uno por cada instancia (38001, 38002, etcétera). El número de puerto es necesario para que el jugador del lado cliente configure la conexión multiusuario.

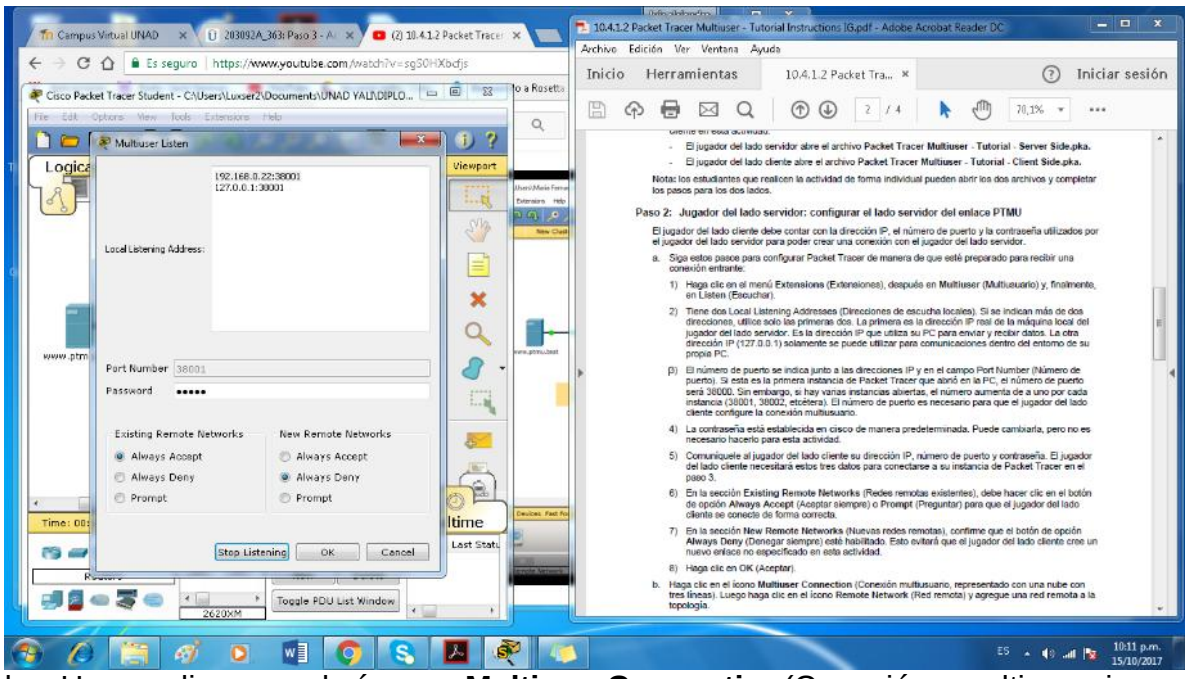
4) La contraseña está establecida en **cisco** de manera predeterminada. Puede cambiarla, pero no es necesario hacerlo para esta actividad.

5) Comuníquele al jugador del lado cliente su dirección IP, número de puerto y contraseña. El jugador del lado cliente necesitará estos tres datos para conectarse a su instancia de PacketTracer en el paso 3.

6) En la sección **ExistingRemote Networks** (Redes remotas existentes), debe hacer clic en el botón de opción **AlwaysAccept**(Aceptar siempre) o **Prompt**(Preguntar) para que el jugador del lado cliente se conecte de forma correcta.

7) En la sección **New Remote Networks** (Nuevas redes remotas), confirme que el botón de opción **AlwaysDeny**(Denegar siempre) esté habilitado. Esto evitará que el jugador del lado cliente cree un nuevo enlace no especificado en esta actividad.

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

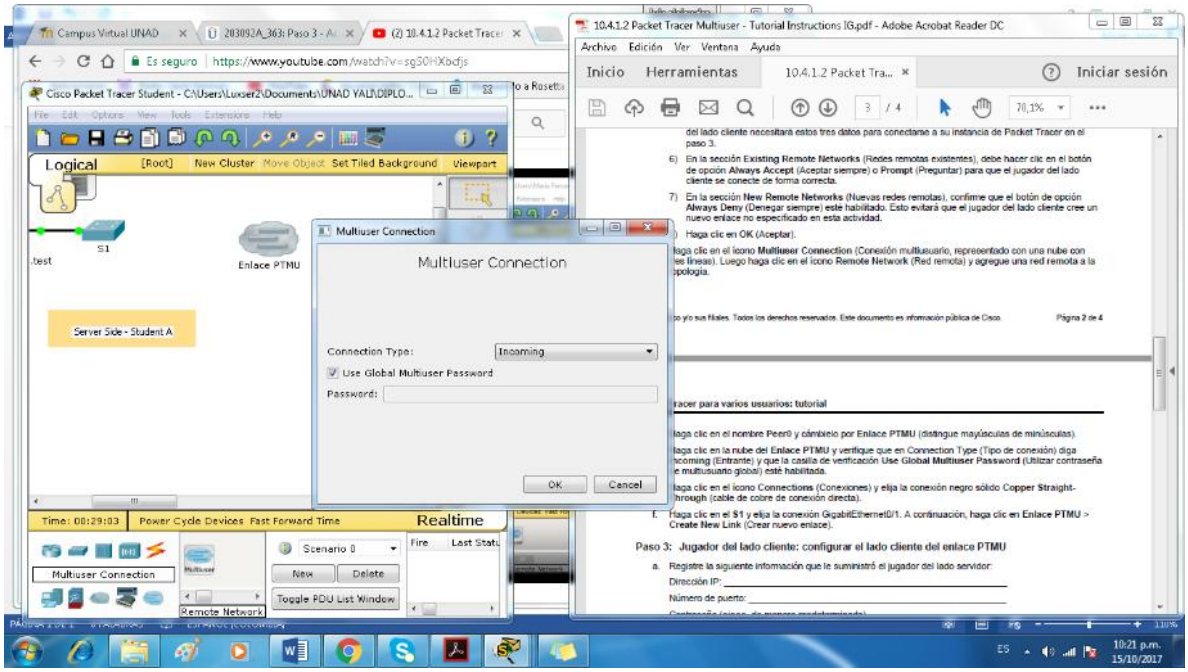


b. Haga clic en el ícono **MultiuserConnection**(Conexión multiusuario, representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

PacketTracer para varios usuarios: tutorial

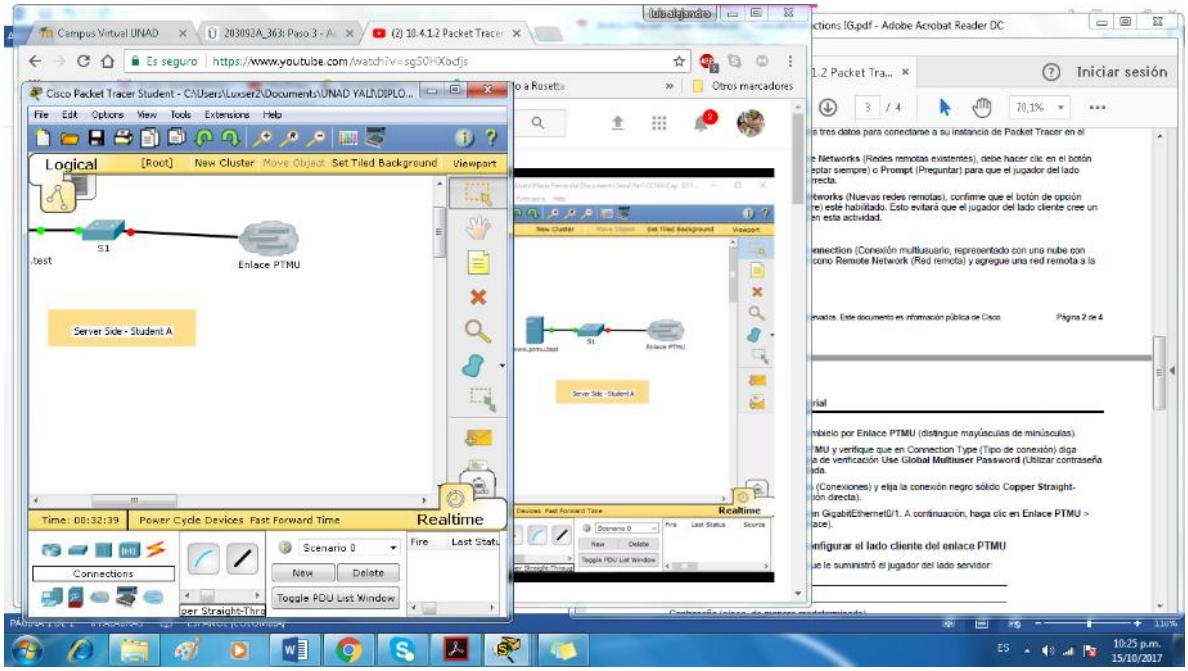
c. Haga clic en el nombre **Peer0** y cámbielo por **Enlace PTMU** (distingue mayúsculas de minúsculas).

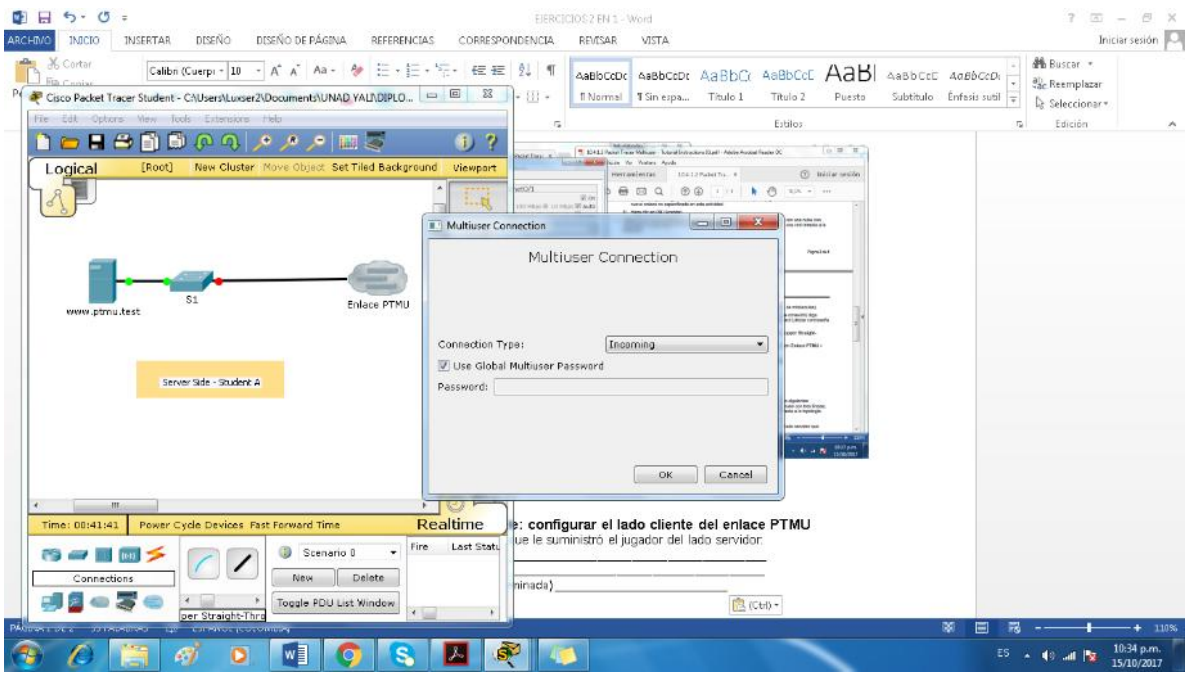
d. Haga clic en la nube del **Enlace PTMU** y verifique que en ConnectionType (Tipo de conexión) diga **Incoming**(Entrante) y que la casilla de verificación **Use Global MultiuserPassword**(Utilizar contraseña de multiusuario global) esté habilitada.



e. Haga clic en el ícono **Connections**(Conexiones) y elija la conexión negro sólido **CopperStraight- Through**(cable de cobre de conexión directa).

f. Haga clic en el **S1** y elija la conexión GigabitEthernet0/1. A continuación, haga clic en **Enlace PTMU** >**Create New Link** (Crear nuevo enlace).



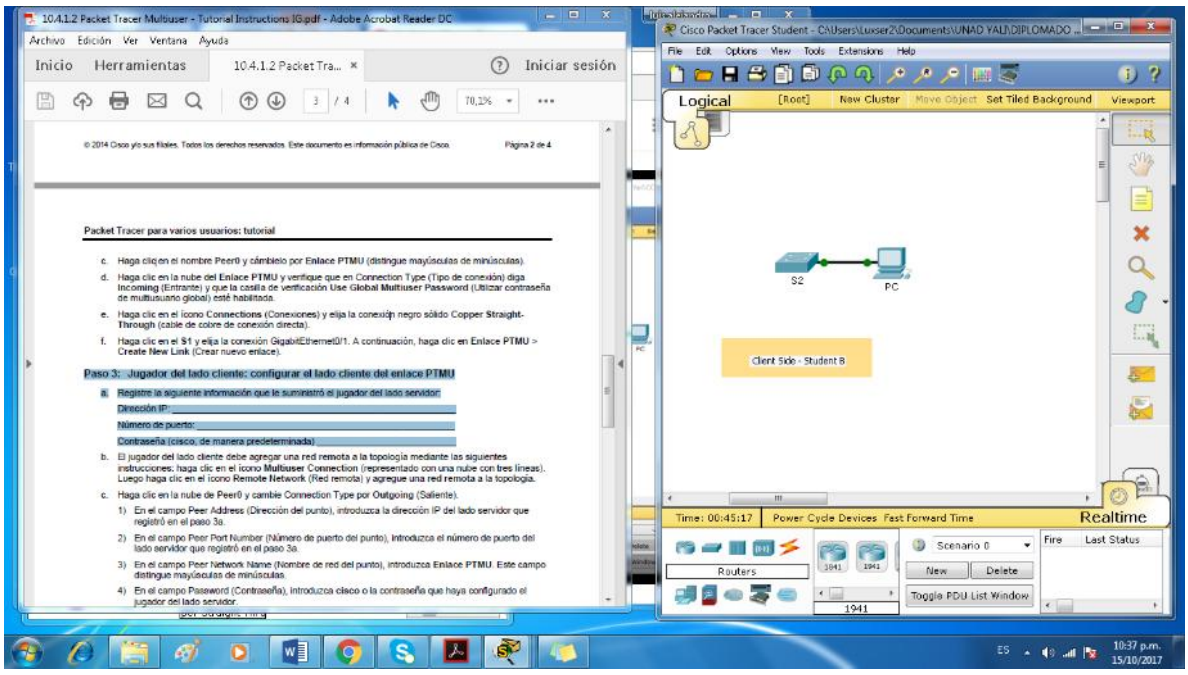


Paso 3: Jugador del lado cliente: configurar el lado cliente del enlace PTMU

a. Registre la siguiente información que le suministró el jugador del lado servidor:

Dirección IP: _____192.168.0.22

127.0.0.1_____
Número de puerto: __38001_____
Contraseña (**cisco**, de manera predeterminada) ____cisco_____



b. El jugador del lado cliente debe agregar una **red remota** a la topología mediante las siguientes instrucciones: haga clic en el ícono **MultiuserConnection**(representado con una nube con tres líneas). Luego haga clic en el ícono **Remote Network** (Red remota) y agregue una **red remota** a la topología.

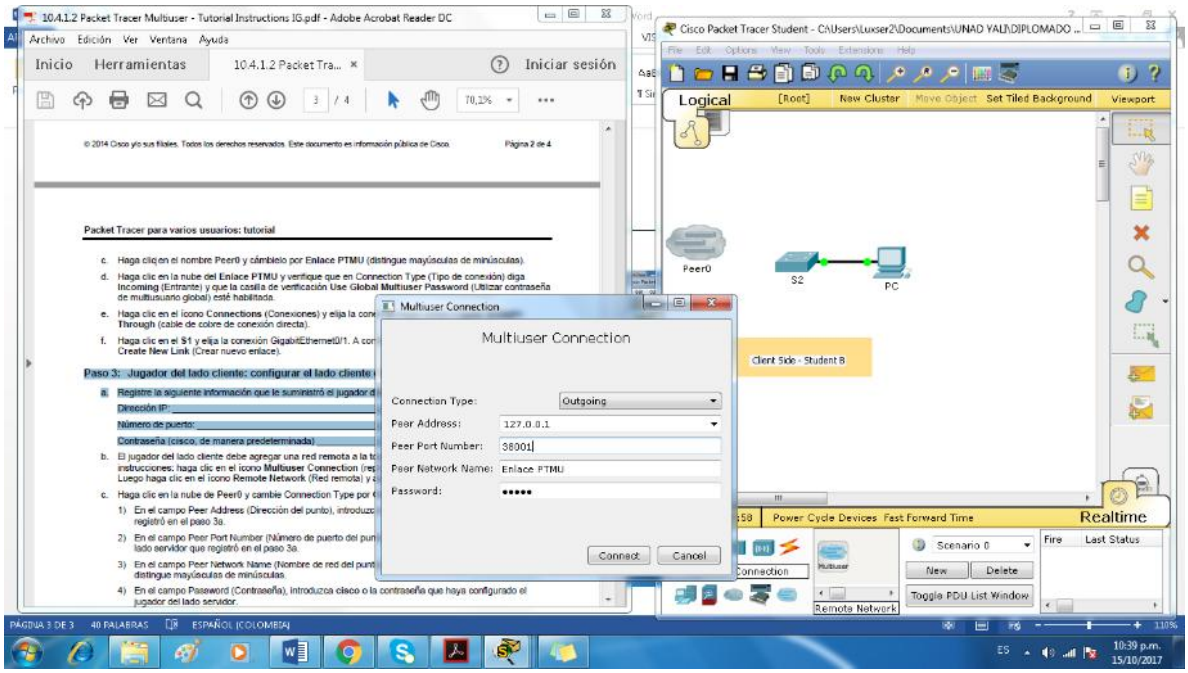
c. Haga clic en la nube de **Peer0** y cambie ConnectionType por **Outgoing**(Saliente).

1) En el campo Peer Address (Dirección del punto), introduzca la dirección IP del lado servidor que registró en el paso 3a.

2) En el campo Peer Port Number (Número de puerto del punto), introduzca el número de puerto del lado servidor que registró en el paso 3a.

3) En el campo Peer Network Name (Nombre de red del punto), introduzca **Enlace PTMU**. Este campo distingue mayúsculas de minúsculas.

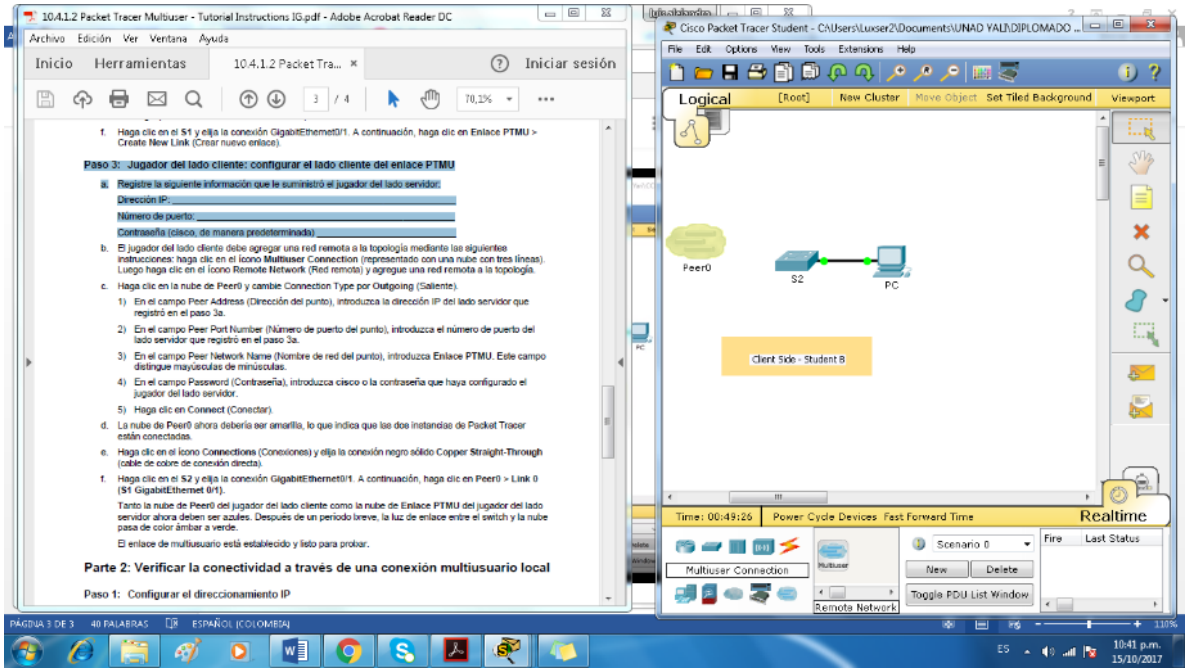
4) En el campo Password (Contraseña), introduzca **cisco** o la contraseña que haya configurado el jugador del lado servidor.



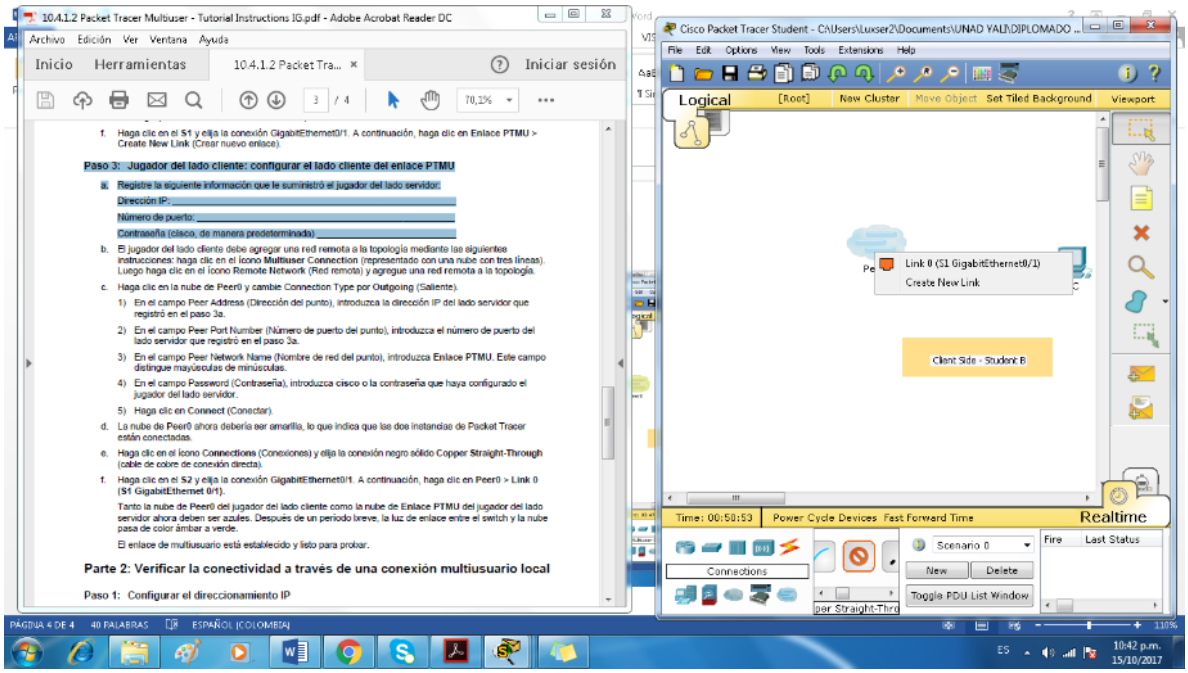
5) Haga clic en **Connect**(Conectar).

d. La nube de **Peer0** ahora debería ser amarilla, lo que indica que las dos instancias de PacketTracer están conectadas.

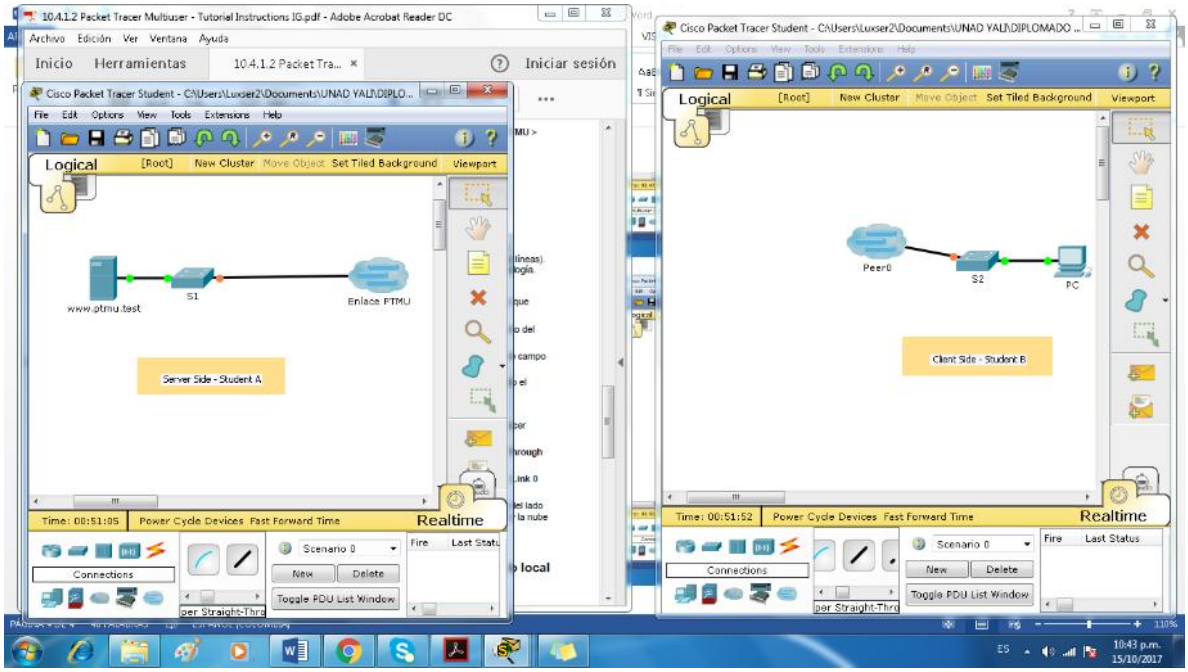
e. Haga clic en el ícono **Connections**(Conexiones) y elija la conexión negro sólido **CopperStraight-Through**(cable de cobre de conexión directa).



f. Haga clic en el **S2** y elija la conexión **GigabitEthernet0/1**. A continuación, haga clic en **Peer0** >**Link 0 (S1 GigabitEthernet 0/1)**.



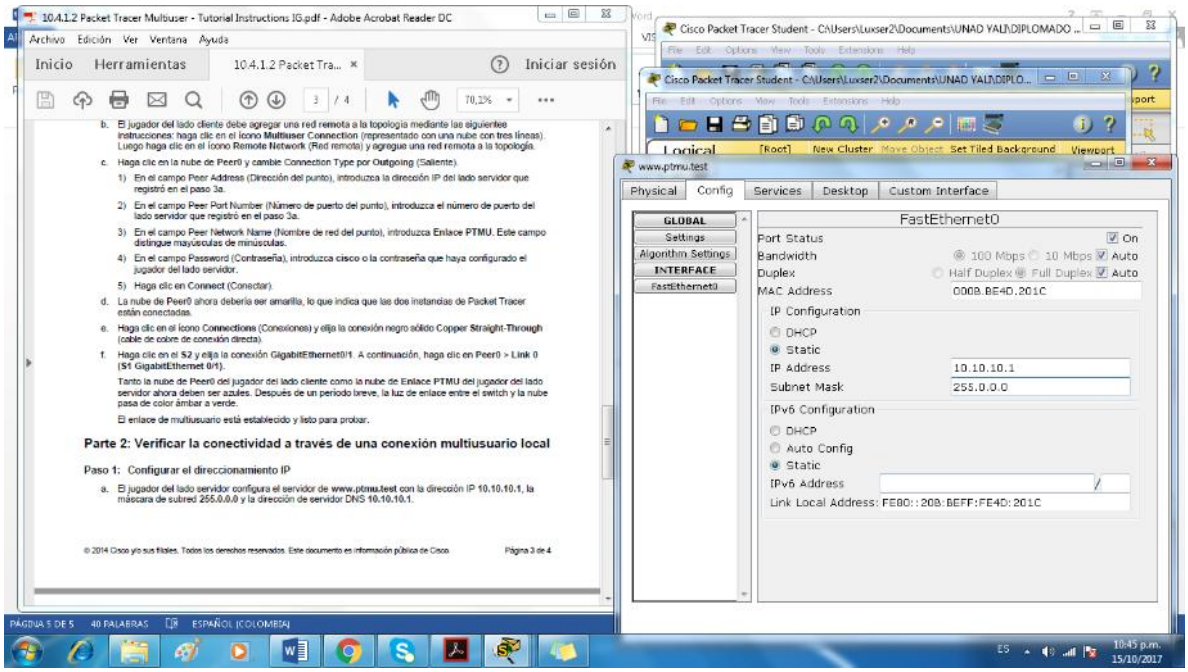
Tanto la nube de **Peer0** del jugador del lado cliente como la nube de **Enlace PTMU** del jugador del lado servidor ahora deben ser azules. Después de un período breve, la luz de enlace entre el switch y la nube pasa de color ámbar a verde.
El enlace de multiusuario está establecido y listo para probar.



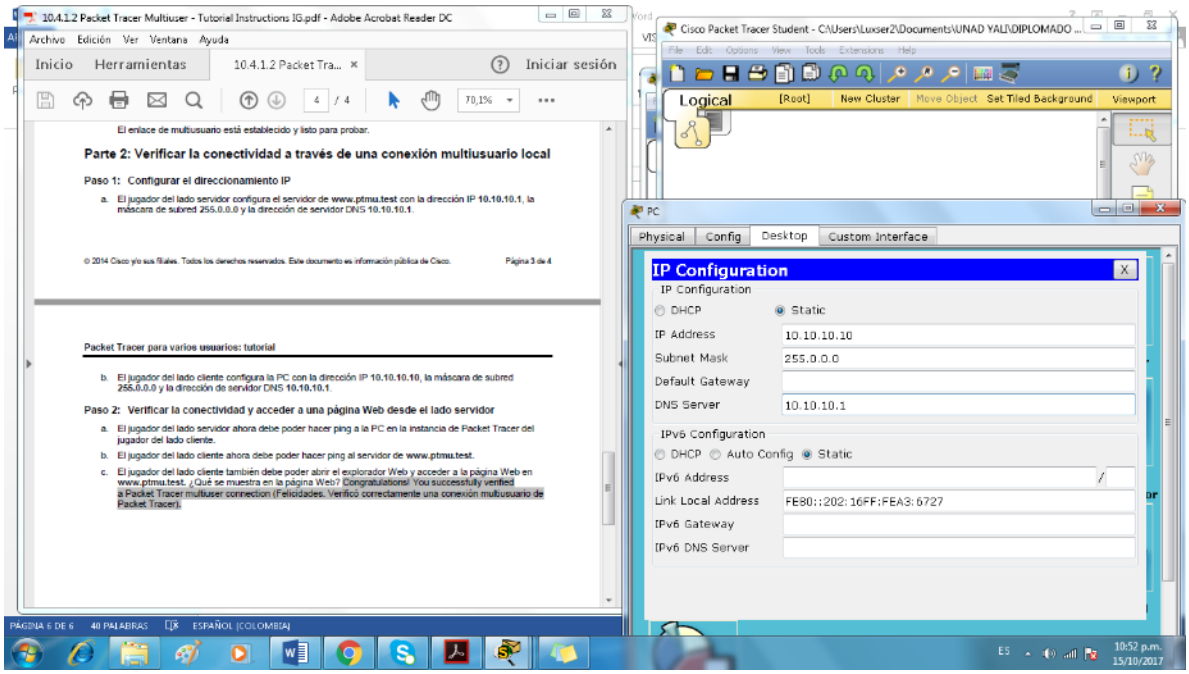
Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Paso 1: Configurar el direccionamiento IP

a. El jugador del lado servidor configura el servidor de **www.ptmu.test** con la dirección IP **10.10.10.1**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.



b. El jugador del lado cliente configura la PC con la dirección IP **10.10.10.10**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.

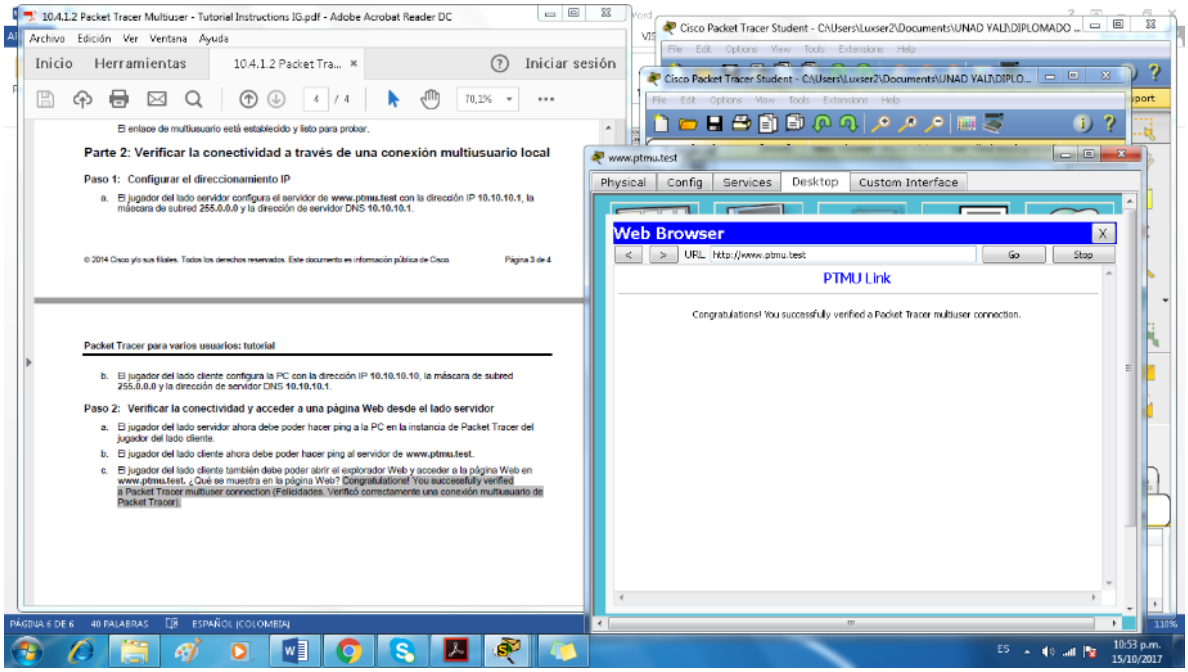


Paso 2: Verificar la conectividad y acceder a una página Web desde el lado servidor

a. El jugador del lado servidor ahora debe poder hacer ping a la PC en la instancia de PacketTracer del jugador del lado cliente.

b. El jugador del lado cliente ahora debe poder hacer ping al servidor de **www.ptmu.test**.

c. El jugador del lado cliente también debe poder abrir el explorador Web y acceder a la página Web en **www.ptmu.test.** ¿Qué se muestra en la página Web? Congratulations! You successfully verified a Packet Tracer multiuser connection (Felicidades. Verificó correctamente una conexión multiusuario de PacketTracer).



CONCLUSIONES

En los trabajos de las dos unidades de manera general nos permitió conocer y desarrollar cada una de las temática, resaltar la importancia que tienen las redes a nivel global y en cada ámbito específico. Se desarrollan las competencias básicas que nos permiten llevar a cabo los procesos de configuración y administración de dispositivos de Networking mediante el estudio de los modelos OSI, la arquitectura TCP/IP además, del uso de recursos y herramientas en función de los protocolos y servicios. De manera específica se desarrolló lo siguiente:

- Desarrollamos actividades de representación de red, que incluían exploración, conexión y configuración de dispositivos.
- Revisión de procesos de configuración de un sistema operativo de red e identificación de su funcionalidad y propósito.
- Identificación de los protocolos y comunicaciones de red.
- Exploración de las propiedades físicas y lógicas de los dispositivos de red.

BIBLIOGRAFIA

Routing and Switching: Introducción a las redes (Introduction to Networks) CISCO.
Routing y switching de CCNA: Principios básicos de routing y switching CISCO.

CISCO. (2014). Exploración de la red. Fundamentos de Networking.
CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de
CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado
CISCO. (2014). Acceso a la red. Fundamentos de Networking.
CISCO. (2014). Ethernet. Fundamentos de Networking.
CISCO. (2014). Capa de red. Fundamentos de Networking.
UNAD (2014). Diseño y configuración de redes con Packet Tracer [OVA].