DIPLOMADO DE PROFUNDIZACIÓN CISCO
UNIDAD 2 – MODELO OSI Y DIRECCIONAMIENTO IP
PASO 3: ACTIVIDAD COLABORATIVA 2

Edgar Yessid Ladino Abril COD. 1015412504
Carlos Manuel Mesa Méndez COD. 98632570
Juan David Rodríguez Gómez COD. 1019047577
Juan Camilo Bejarano Alarcón COD. 1019010161
Luis Fernando Quimbayo Calderon COD. 93134684

Grupo 203092_38

Presentado a

ING. JUAN CARLOS VESGA
Director del Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS – ECBTI
Noviembre de 2018

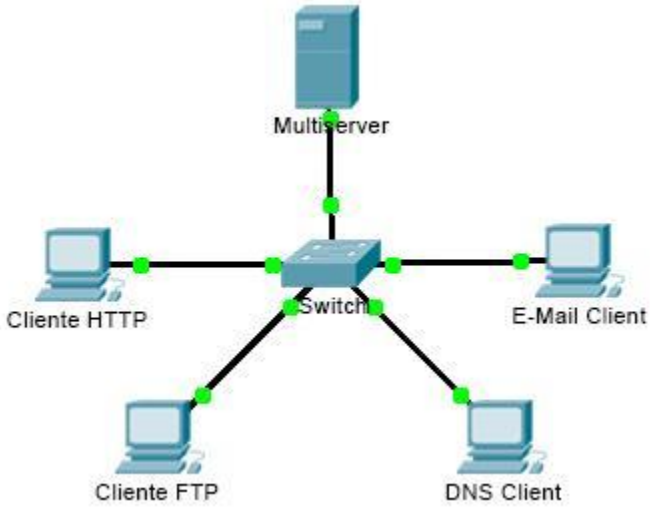
INTRODUCCIÓN

En el desarrollo del presente trabajo se pondrán en práctica los temas estudiados en la unidad dos del diplomado de profundización CISCO, en total se desarrollarán 22 ejercicios utilizando el simulador de red Packet Tracer.

Se identificarán y solucionarán problemas propios de las sub-redes y direccionamiento IP mediante el uso adecuado de estrategias basadas en comandos y estadísticas del IOS, con el cual se pretende fortalecer el desarrollo de competencias en el área de las redes orientadas al enrutamiento avanzado.

Ejercicio 7.3.1.2: Comunicaciones TCP y UDP

Topología



Objetivos

Parte 1: Generar tráfico de red en modo de simulación

Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Información básica

El objetivo de esta actividad de simulación es proporcionar una base para comprender en detalle los protocolos TCP y UDP. El modo de simulación permite ver la funcionalidad de los diferentes protocolos.

A medida que los datos se trasladan por la red, se dividen en partes más pequeñas y se identifican de forma tal que se puedan volver a juntar. A cada una de estas partes se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data unit]) y se la asocia a una capa específica. El modo de simulación de Packet Tracer le permite al usuario ver cada uno de los protocolos y las PDU asociadas. Los pasos que se detallan a continuación guían al usuario en el proceso de solicitud de servicios mediante diversas aplicaciones disponibles en una PC cliente.

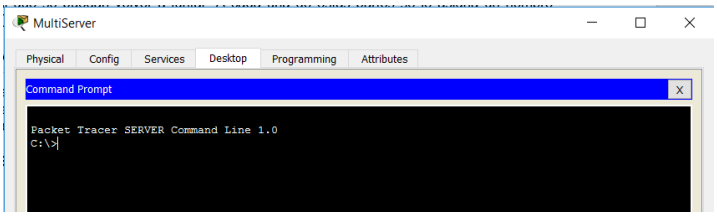
Esta actividad proporciona la oportunidad de explorar la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función que cumplen los números de puerto para determinar qué aplicación local solicita o envía los datos.

Parte 1: Generar tráfico de red en modo de simulación

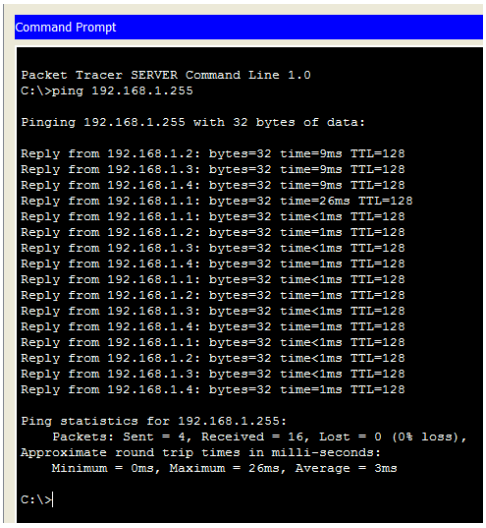
Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

Para reducir la cantidad de tráfico de red que se ve en la simulación, realice lo siguiente:

- Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).



- Introduzca el comando **ping 192.168.1.255**. Esto toma unos segundos, ya que todos los dispositivos en la red responden a **MultiServer**.

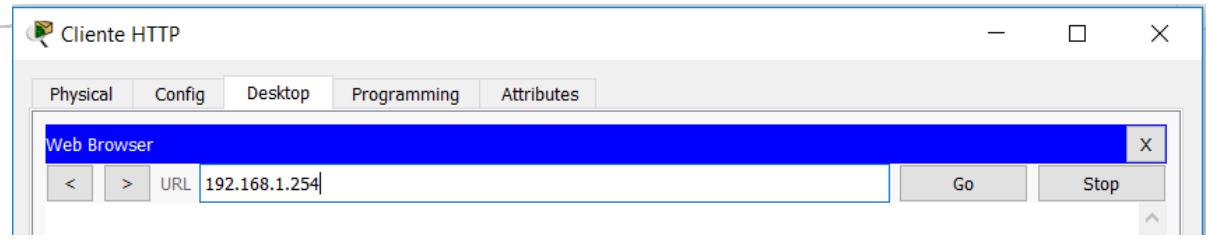


- Cierre la ventana de **MultiServer**.

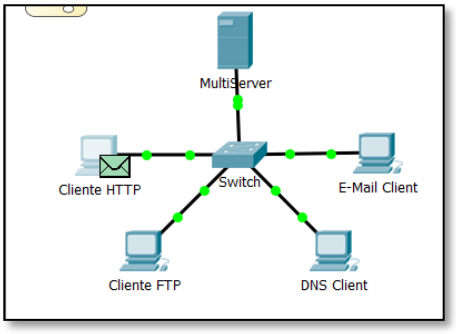
Paso 2: Genere tráfico web (HTTP).

a. Cambie a modo de simulación.

b. Haga clic en **HTTP Client** (Cliente HTTP) y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Explorador Web).



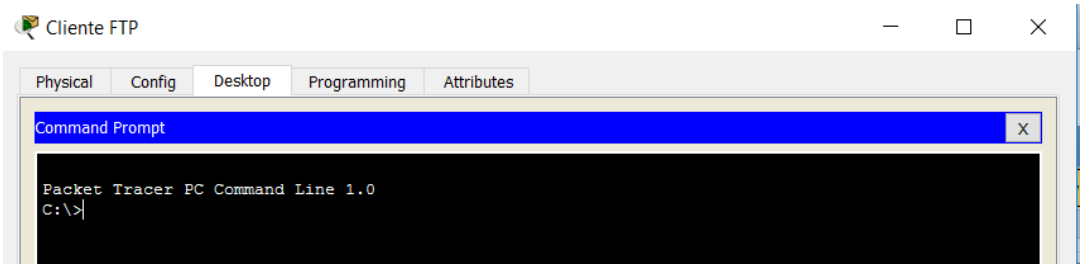
c. En el campo de dirección URL, introduzca **192.168.1.254** y haga clic en **Go** (Ir). En la ventana de simulación, aparecerán sobres (PDU).



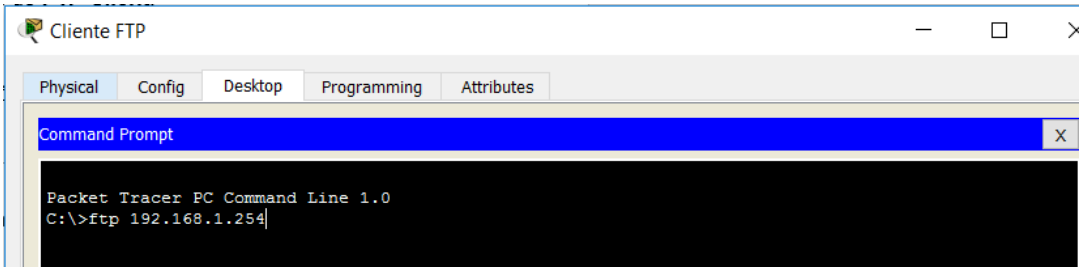
d. Minimice (pero no cierre) la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP

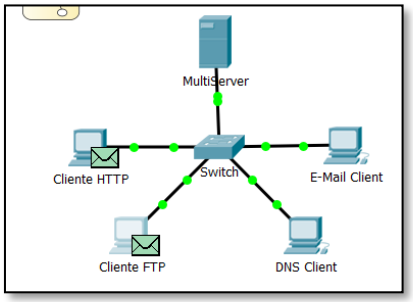
a. Haga clic en **FTP Client** (Cliente FTP) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.



b. Introduzca el comando **ftp 192.168.1.254**. En la ventana de simulación, aparecerán PDU.

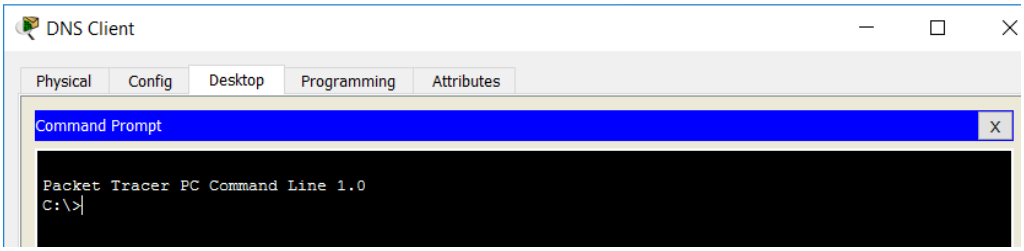


c. Minimice (pero no cierre) la ventana de configuración de **FTP Client**.

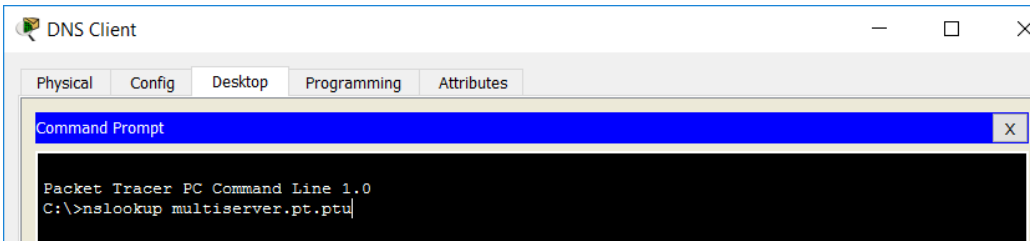


Paso 4: Generar tráfico DNS

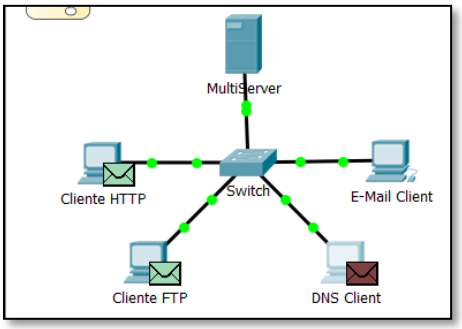
a. Haga clic en **DNS Client** (Cliente DNS) y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.



b. Introduzca el comando **nslookup multiserver.pt.ptu**. En la ventana de simulación, aparecerá una PDU.

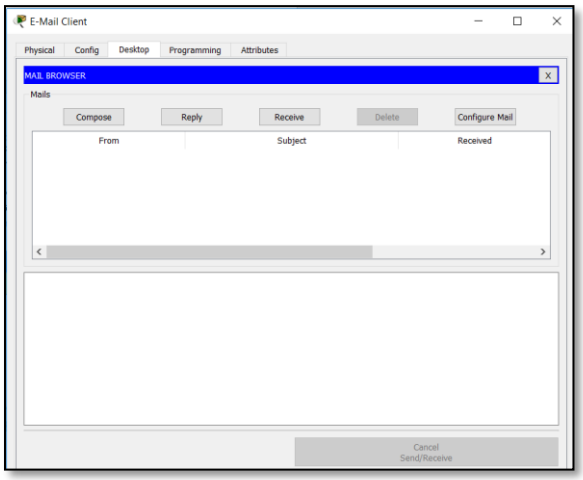


c. Minimice (pero no cierre) la ventana de configuración de **DNS Client**.



Paso 5: Generar tráfico de correo electrónico

a. Haga clic en **E-Mail Client** (Cliente de correo electrónico) y, a continuación, haga clic en la ficha **Desktop** y seleccione la herramienta **E Mail** (Correo electrónico).

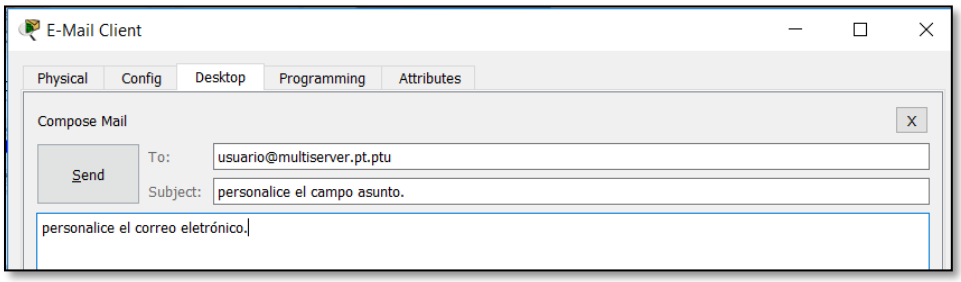


b. Haga clic en **Compose** (Redactar) e introduzca la siguiente información:

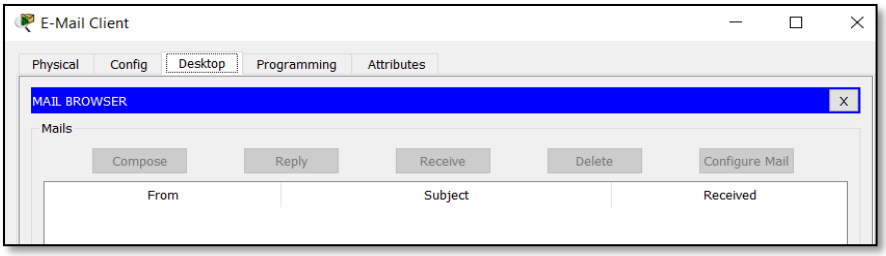
To: (Para:) usuario@multiserver.pt.ptu.

Subject: (Asunto:) personalice el campo de asunto.

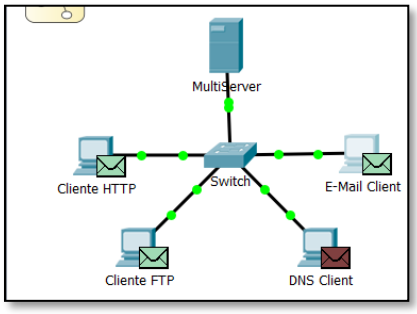
E-Mail Body: (Cuerpo del correo electrónico:) personalice el correo electrónico.



c. Haga clic en **Send** (Enviar).

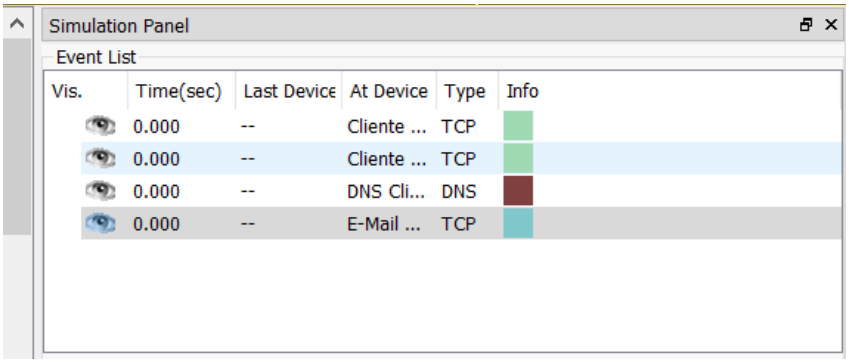


d. Minimice (pero no cierre) la ventana de configuración de **E-Mail Client**.



Paso 6: Verifique que se haya generado tráfico y que esté preparado para la simulación.

Cada equipo cliente debe tener PDU enumeradas en el panel de simulación.

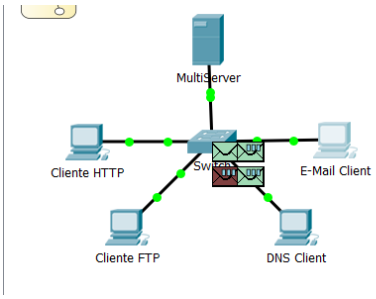


Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

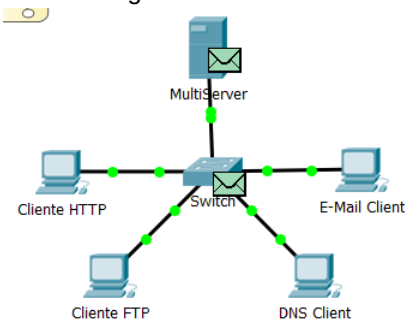
Paso 1: Examinar la multiplexación a medida que el tráfico cruza la red

Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

a. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.

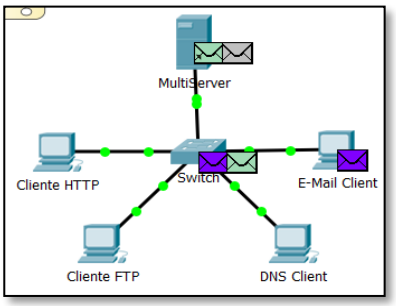


b. Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?



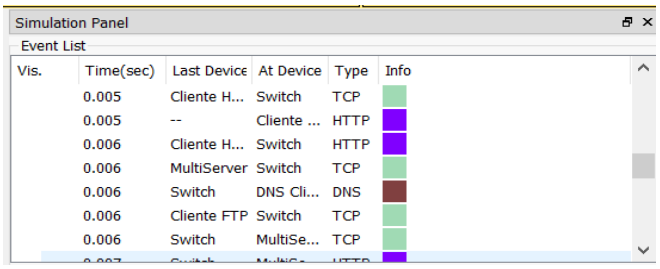
Están almacenadas en el switch

b. Haga clic en **Capture/Forward** seis veces. Todos los clientes deberían haber recibido una respuesta. Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado. ¿Cómo se denomina este proceso?



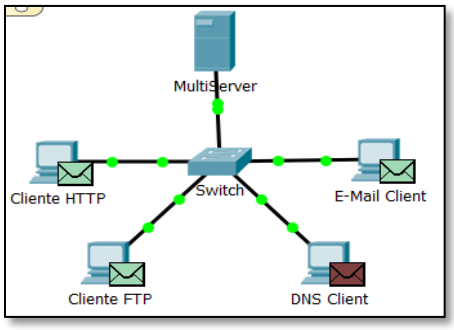
Multiplexación.

c. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?



Representan diferentes protocolos.

d. Haga clic en **Back** ocho veces. Esto restablecerá la simulación.

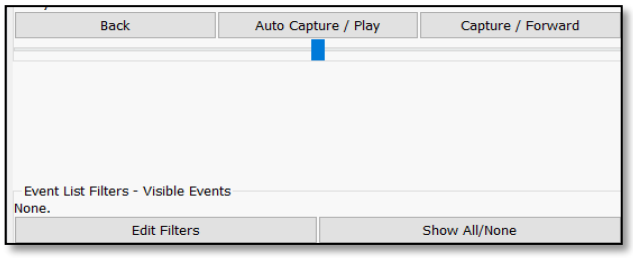


NOTA: no haga clic en **Reset Simulation** (Restablecer simulación) en ningún momento durante esta actividad; si lo hace, deberá repetir los pasos de la parte 1.

Paso 2: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor

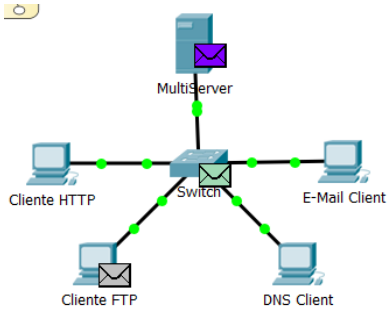
a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**:

Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrar todos/ninguno).

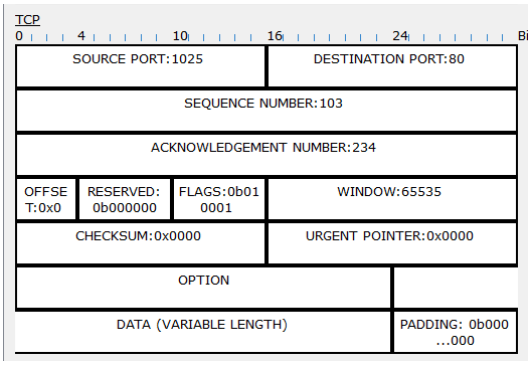


Seleccione **HTTP** y **TCP**. Haga clic en cualquier lugar fuera del cuadro Edit Filters (Editar filtros) para ocultarlo. En Visible Events (Eventos visibles), ahora solo se deberían mostrar las PDU de **HTTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en **HTTP Client**. Haga clic en el sobre de PDU para abrirlo.



c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

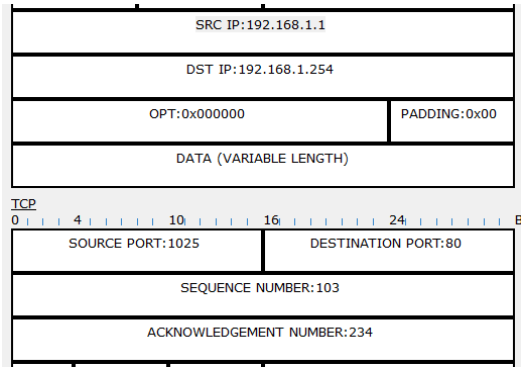


TCP

¿Estas comunicaciones se consideran confiables?

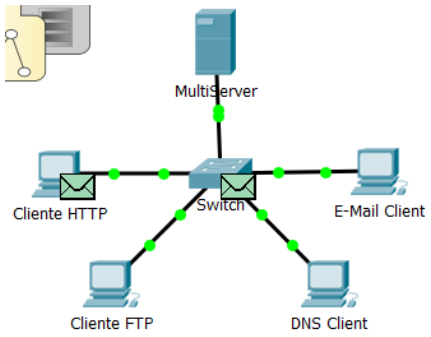
Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).

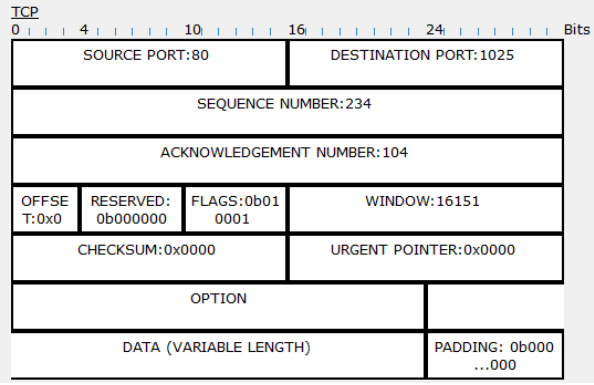


¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** Ventana)?
1025 (puede ser diferente), 80, 0, 0 SYN

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **HTTP Client** con una marca de verificación.

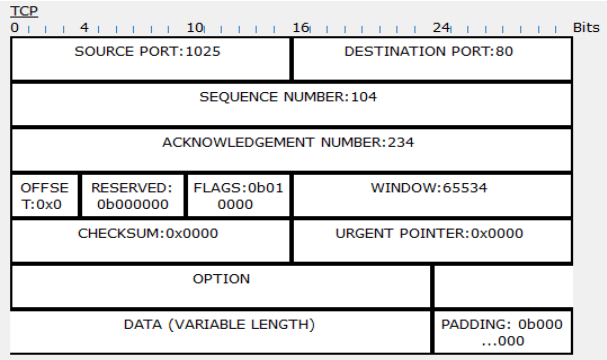


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?



80, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1. SYN cambió por SYN+ACK.

g. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación HTTP. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).



h. ¿Qué información se indica ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?

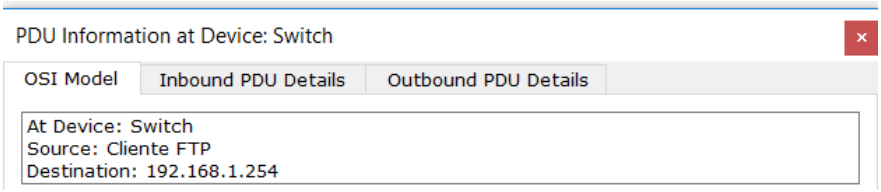
1025, 80, 1, 1. PSH+ACK: los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de acuse de recibo son 1.

i. Haga clic en **Back** hasta que se restablezca la simulación.

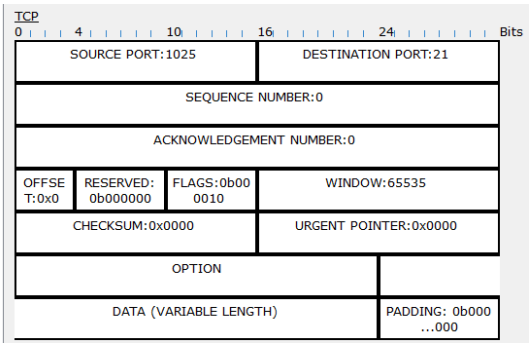
Paso 3: Examine el tráfico FTP cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **FTP Client**. Haga clic en el sobre de PDU para abrirlo.



c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

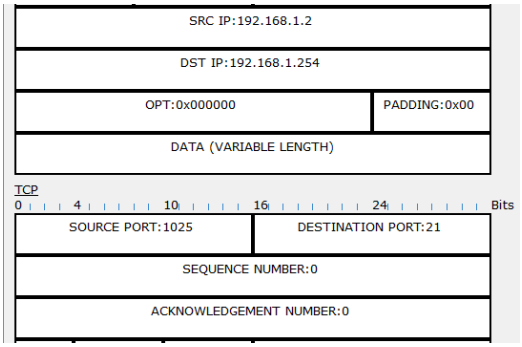


TCP

¿Estas comunicaciones se consideran confiables?

Sí.

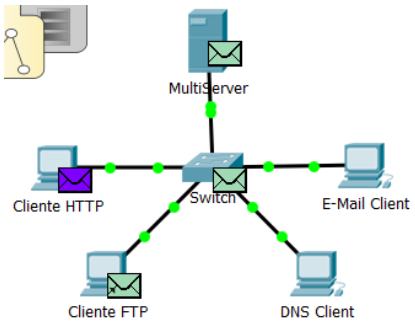
d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).



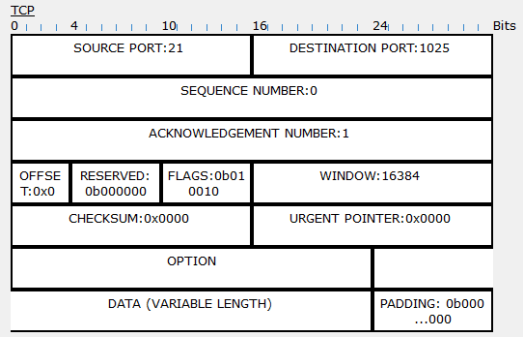
¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

1025, 21, 0, 0. SYN

e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.

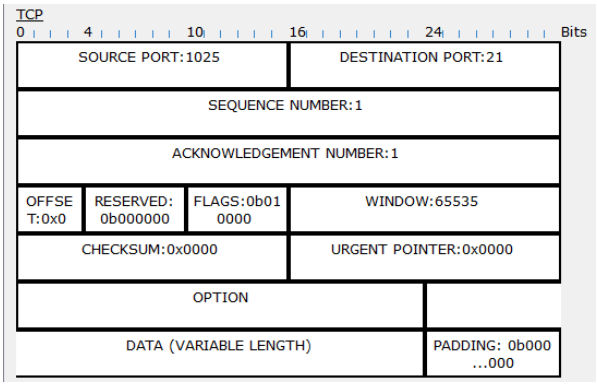


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?



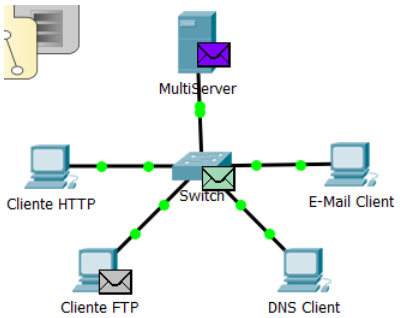
21, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

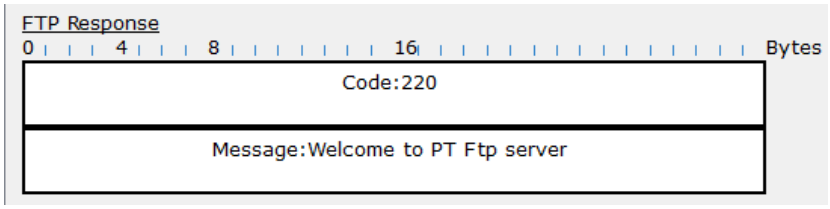


1025, 21, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

h. Cierre la PDU y haga clic en **Capture/Forward** hasta que una segunda PDU vuelva a **FTP Client**. La PDU es de un color diferente.



i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?



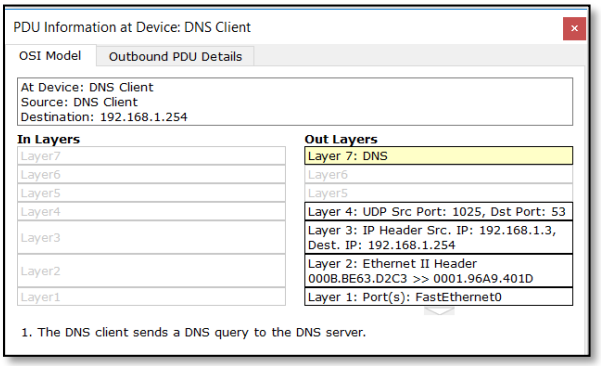
Puede decir “Username ok, need password” (Nombre de usuario correcto, se necesita contraseña) o “Welcome to PT Ftp server” (Bienvenido al servidor FTP de PT).

j. Haga clic en **Back** hasta que se restablezca la simulación.

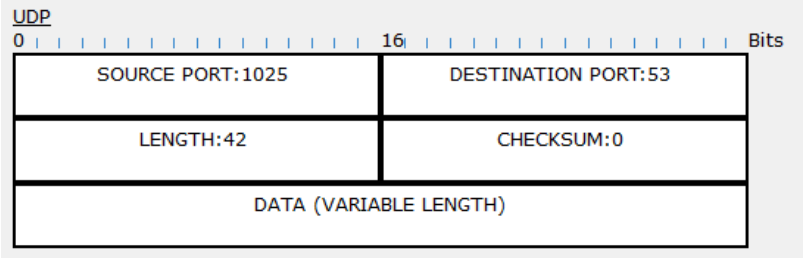
Paso 4: Examine el tráfico DNS cuando los clientes se comunican con el servidor.

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS** y **UDP**.

b. Haga clic en el sobre de PDU para abrirlo.



c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección?

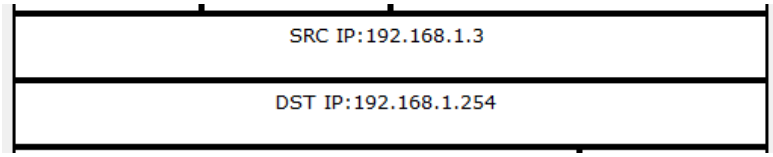


UDP

¿Estas comunicaciones se consideran confiables?

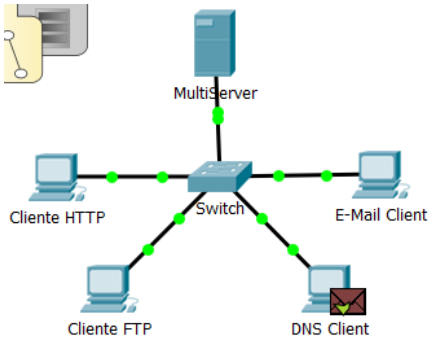
No

d. Registre los valores de **SRC PORT** (Puerto de origen) y **DEST PORT** (Puerto de destino). ¿Por qué no hay números de secuencia ni de acuse de recibo?

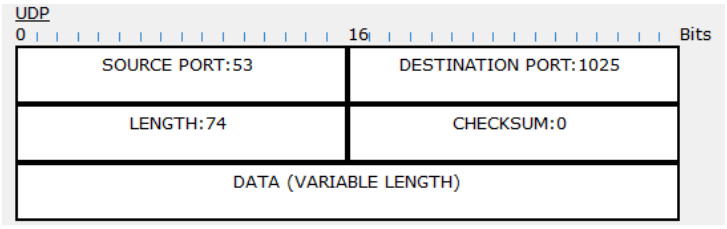


1025, 53. Porque UDP no necesita establecer una conexión confiable.

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.

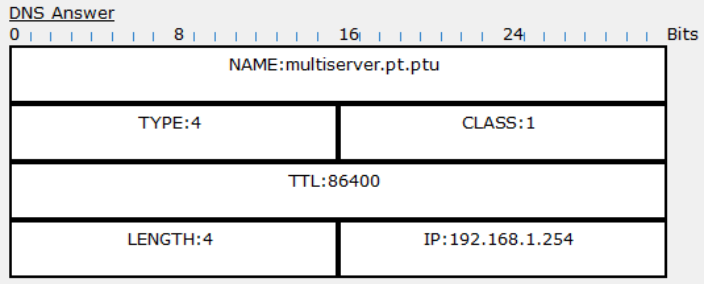


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?



53, 1025. Los puertos de origen y destino están invertidos.

g. ¿Cómo se llama la última sección de la **PDU**?



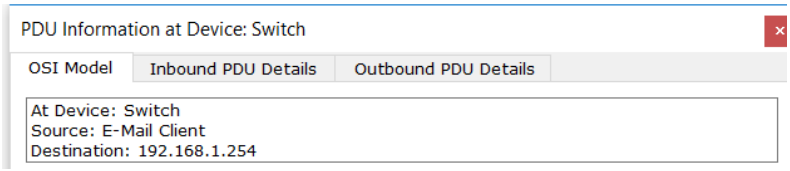
DNS ANSWER

h. Haga clic en **Back** hasta que se restablezca la simulación.

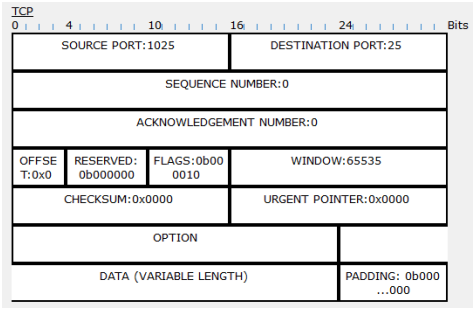
Paso 5: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor

a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP** y **TCP**.

b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **E-mail Client**. Haga clic en el sobre de PDU para abrirlo.



c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico?

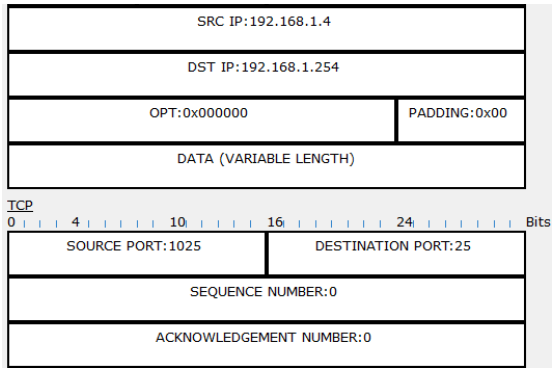


TCP

¿Estas comunicaciones se consideran confiables?

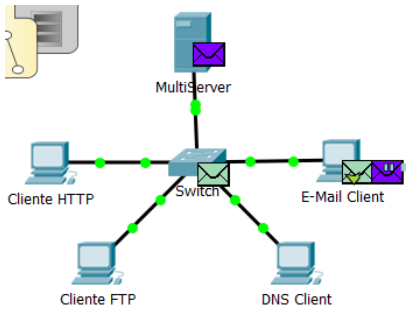
Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).

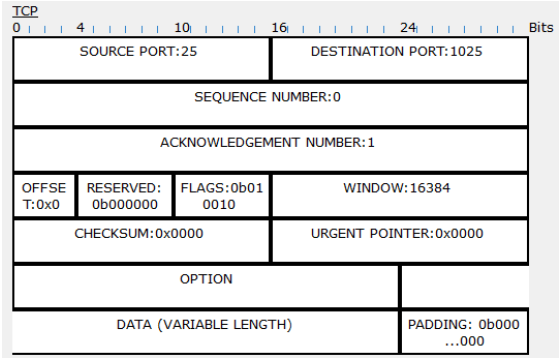


¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?
1025, 25, 0, 0. SYN

e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva a **E-Mail Client** con una marca de verificación.

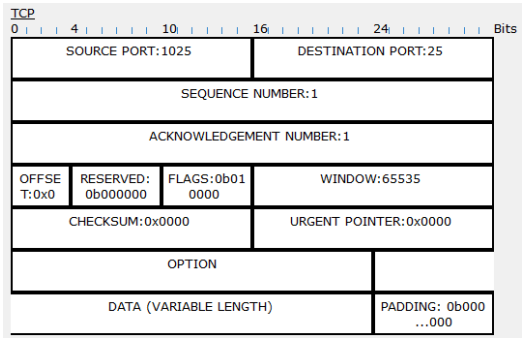


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?



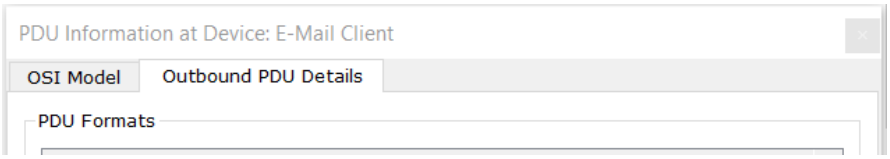
25, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.

g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?



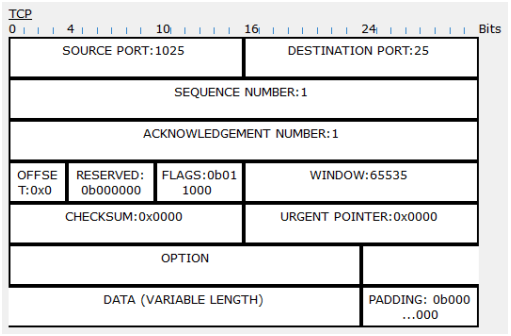
1025, 25, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1. ACK

h. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y selecciones Outbound PDU Details (Detalles de PDU saliente)



i. ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos **PDU** anteriores?

j.



1025, 25, 1, 1. PSH+ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.

k. ¿Qué protocolo de correo electrónico se relaciona con el puerto TCP 25? ¿Qué protocolo se relaciona con el puerto TCP 110?

SMTP. POP3.

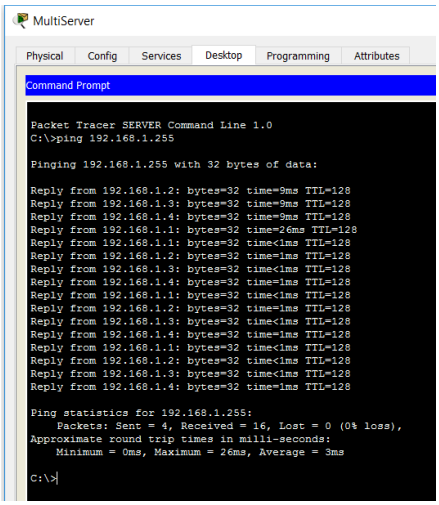
l. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 6: Examinar el uso de números de puerto del servidor

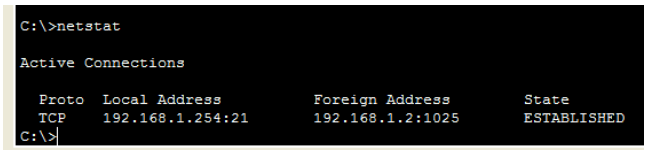
a. Para ver las sesiones TCP activas, siga estos pasos en una secuencia rápida:

1) Pase nuevamente al modo **Realtime** (Tiempo real).

2) Haga clic en **Multiserver** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).



b. Introduzca el comando **netstat**. ¿Qué protocolos se indican en la columna izquierda?
TCP



¿Qué números de puerto utiliza el servidor?
Las respuestas varían, pero los estudiantes pueden ver los tres: 21, 25 y 80. Definitivamente deben ver el puerto 21.

c. ¿En qué estados están las sesiones?

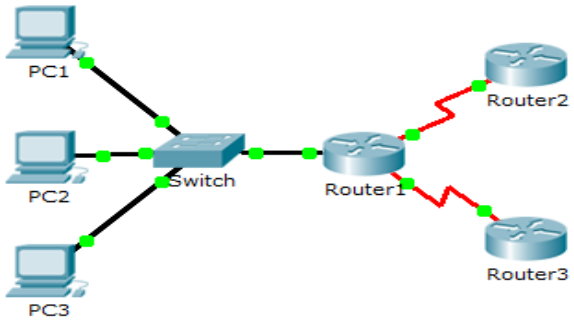
La respuesta varía. Entre los posibles estados se incluyen CLOSED (Cerrada), ESTABLISHED (Establecida), LAST_ACK (Último acuse de recibo).

d. Repita el comando **netstat** varias veces hasta que vea solo una sola sesión con el estado ESTABLISHED. ¿Para qué servicio aún está abierta la conexión? FTP

¿Por qué esta sesión no se cierra como las otras tres? (Sugerencia: revise los clientes minimizados)
El servidor está esperando una contraseña del cliente.

Ejercicio 8.1.3.8: Investigación del tráfico unicast, broadcast y multicast

Topología



Objetivos

Parte 1: Generar tráfico de unicast
Parte 2: Generar tráfico de broadcast
Parte 3: Investigar el tráfico de multicast

Información básica/situación

En esta actividad, se examina el comportamiento de unicast, broadcast y multicast. La mayoría del tráfico de una red es unicast. Cuando una PC envía una solicitud de eco ICMP a un router remoto, la dirección de origen en el encabezado del paquete IP es la dirección IP de la PC emisora. La dirección de destino en el encabezado del paquete IP es la dirección IP de la interfaz del router remoto. El paquete se envía sólo al destino deseado.

Mediante el comando **ping** o la característica Add Complex PDU (Agregar PDU compleja) de Packet Tracer, puede hacer ping directamente a las direcciones de broadcast para ver el tráfico de broadcast.

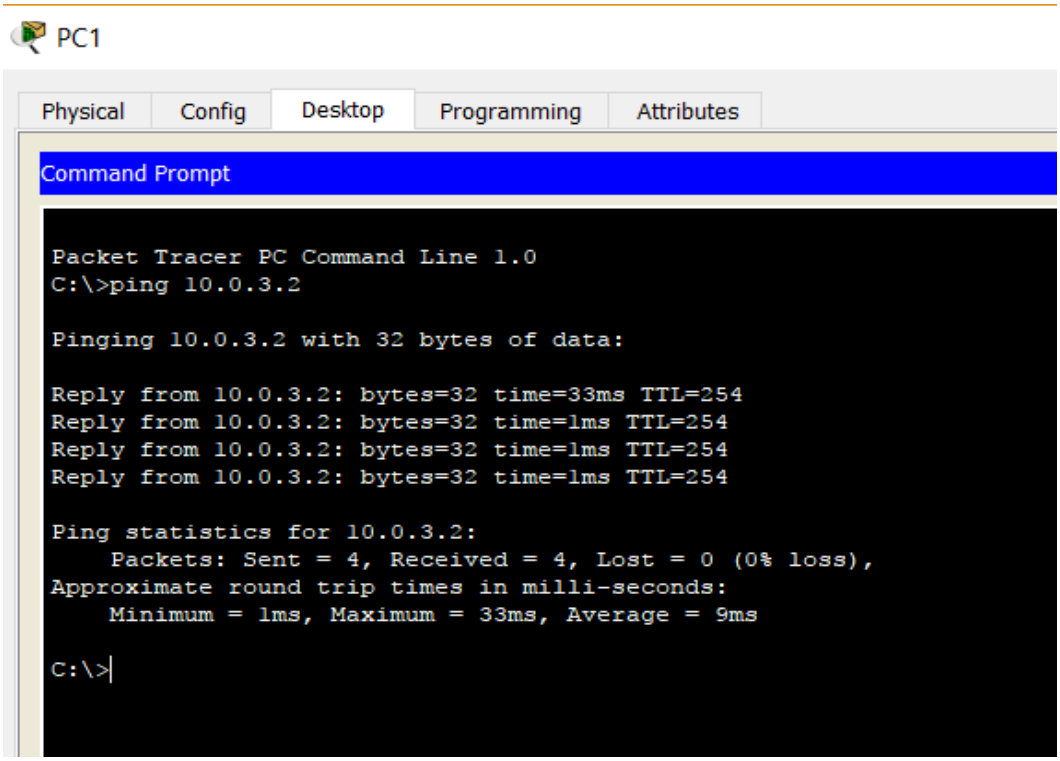
Para el tráfico de multicast, consultará el tráfico de EIGRP. Los routers Cisco utilizan EIGRP para intercambiar información de enrutamiento entre routers. Los routers que utilizan EIGRP envían paquetes a la dirección multicast 224.0.0.10, que representa el grupo de routers EIGRP. Si bien estos paquetes son recibidos por otros dispositivos, todos los dispositivos (excepto los routers EIGRP) los descartan en la capa 3, sin requerir otro procesamiento.

Parte 1: Generar tráfico de unicast

Paso 1: Utilizar el comando ping para generar tráfico

a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

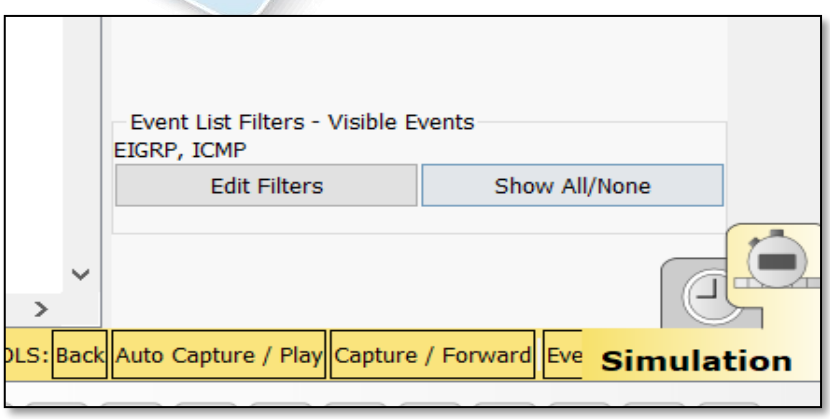
b. Introduzca el comando **ping 10.0.3.2**. El ping debe tener éxito.



Paso 2: Ingrese al modo de simulación.

a. Haga clic en la ficha **Simulation** (Simulación) para ingresar al modo de simulación.

b. Haga clic en **Edit Filters** (Editar filtros) y verifique que solo los eventos ICMP y EIGRP estén seleccionados.

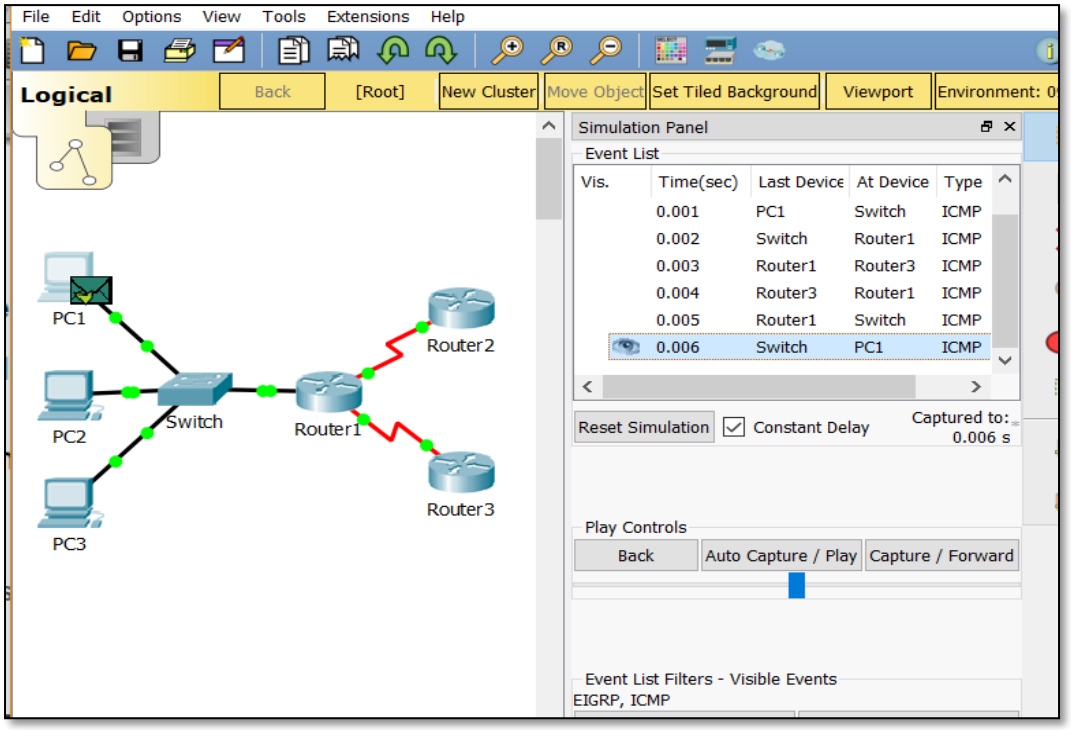


c. Haga clic en **PC1** e introduzca el comando **ping 10.0.3.2**.

Paso 3: Examinar el tráfico de unicast

La PDU en la **PC1** es una solicitud de eco de ICMP dirigida a la interfaz serial en el **Router3**.

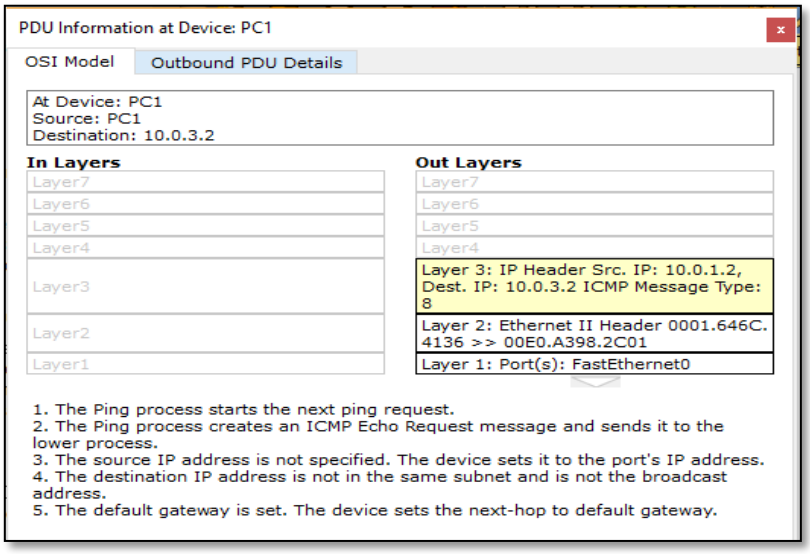
a. Haga clic en **Capture/Forward** (Capturar/avanzar) varias veces y observe mientras se envía la solicitud de eco al **Router3** y la respuesta de eco se envía a la **PC1**. Deténgase cuando la primera respuesta de eco llegue a la PC1.



¿Qué dispositivos atravesó el paquete con la transmisión de unicast?

R/A: Los dispositivos que atravesó el paquee con la transmisión unicast fueron de host PC1 al Switch, posteriormente del Switch al Router1, luego del Router1 al Router3 y por último se devolvió por los mismos dispositivos.

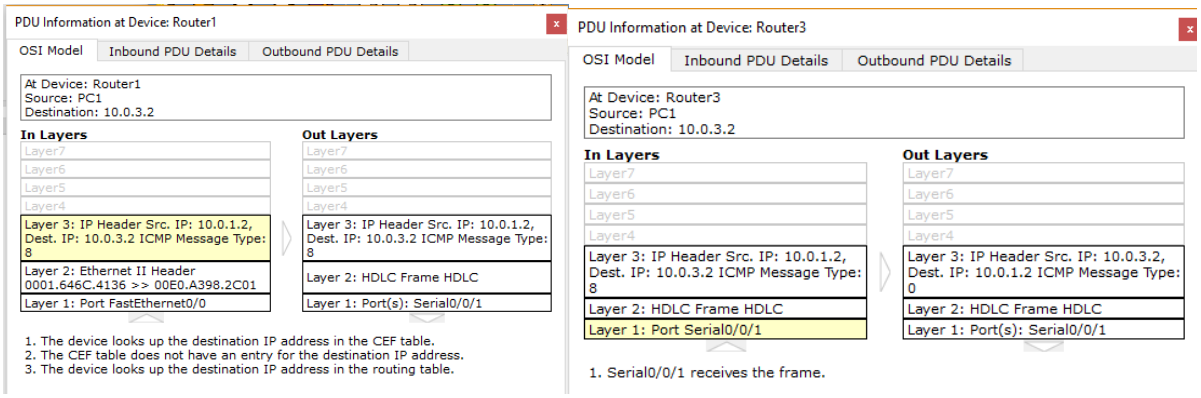
b. En la sección Simulation Panel Event List (Lista de eventos del panel de simulación), la última columna incluye un cuadro de color que proporciona acceso a información detallada sobre un evento. Haga clic en el cuadro de color de la última columna para obtener el primer evento. Se abre la ventana PDU Information (Información de PDU).

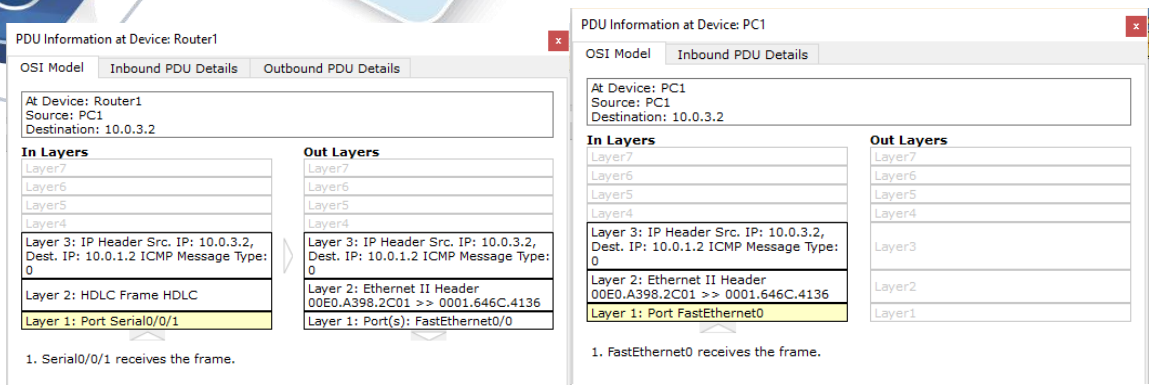


¿En qué capa comienza esta transmisión y por qué?

R/A: La transmisión comienza en la capa 3, debido a que está relacionada con IP e ICMP

c. Examine la información de la Capa 3 para todos los eventos. Observe que las direcciones IP de origen y de destino son direcciones unicast que hacen referencia a la PC1 y a la interfaz serial del Router3





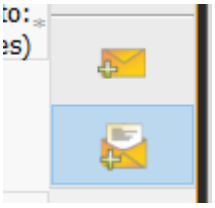
¿Cuáles son los dos cambios que ocurren en la capa 3 cuando un paquete llega al Router3?
R/A: los dos cambios que ocurres es el intercambio de las direcciones IP de origen y destino, por otra parte, el tipo de mensaje de ICMP cambia de 8 a 0.

d. Haga clic en **Reset Simulation** (Restablecer simulación).

Parte 2: Generar tráfico de broadcast

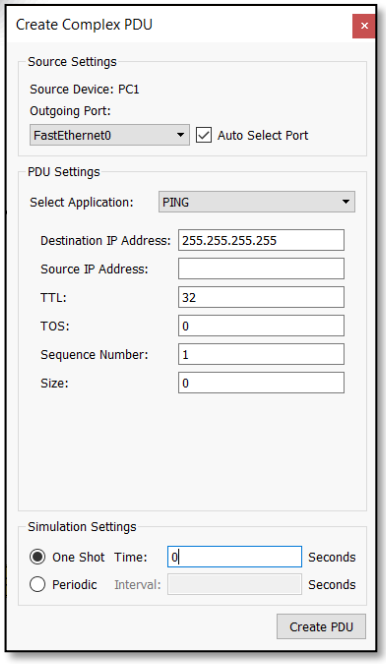
Paso 1: Agregar una PDU compleja

a. Haga clic en **Add Complex PDU** (Agregar una PDU compleja). Este ícono se ubica en la barra de herramientas de la derecha y muestra un sobre abierto.

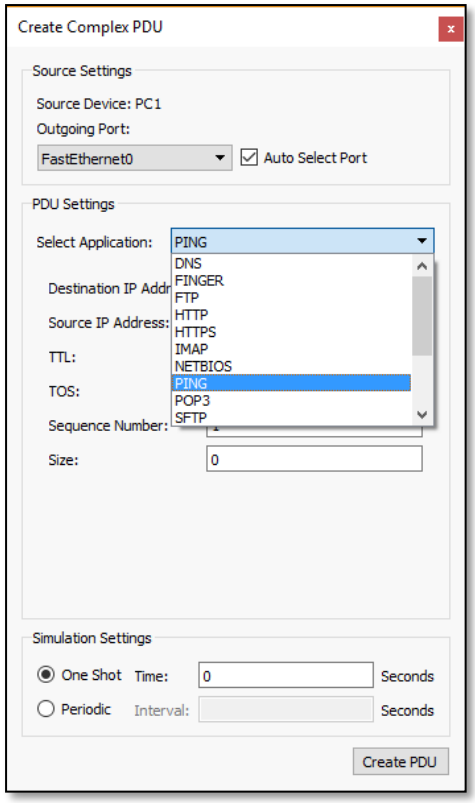


b. Pase el cursor del mouse sobre la topología, y el puntero cambiará por un sobre con un signo más (+). c. Haga clic en **PC1** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de
diálogo **Create Complex PDU** (Crear una PDU compleja). Introduzca los siguientes valores:

- Dirección IP de destino: **255.255.255.255** (dirección de broadcast)
- Número de secuencia: 1
- Tiempo de intento único: **0**



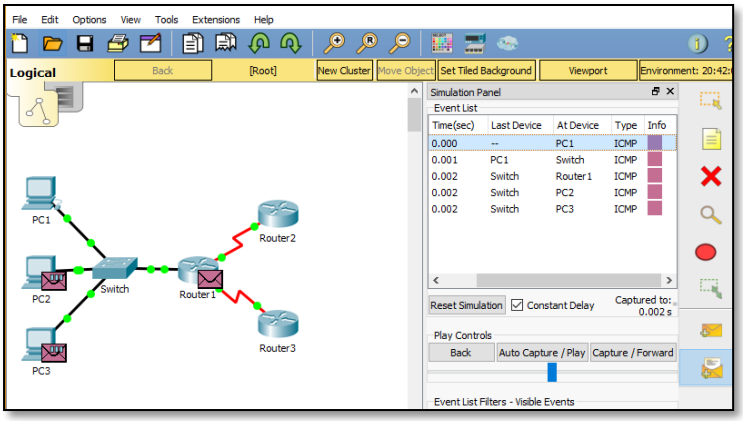
Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

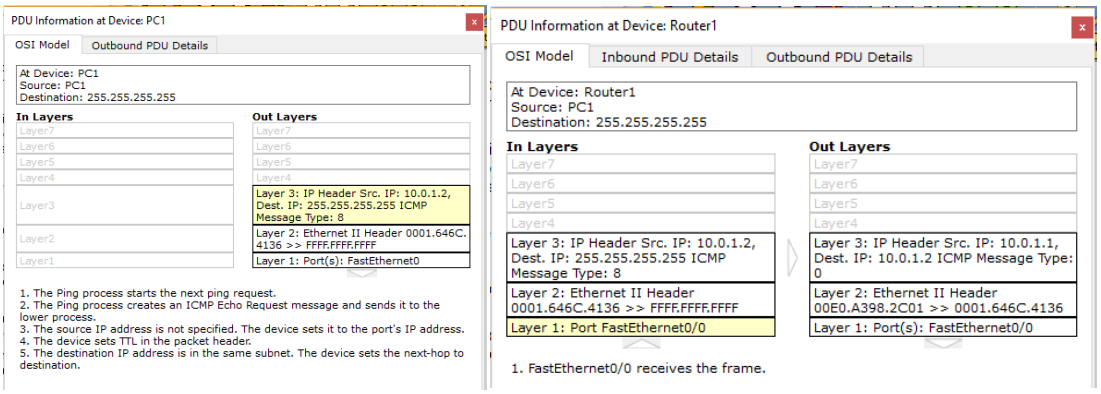


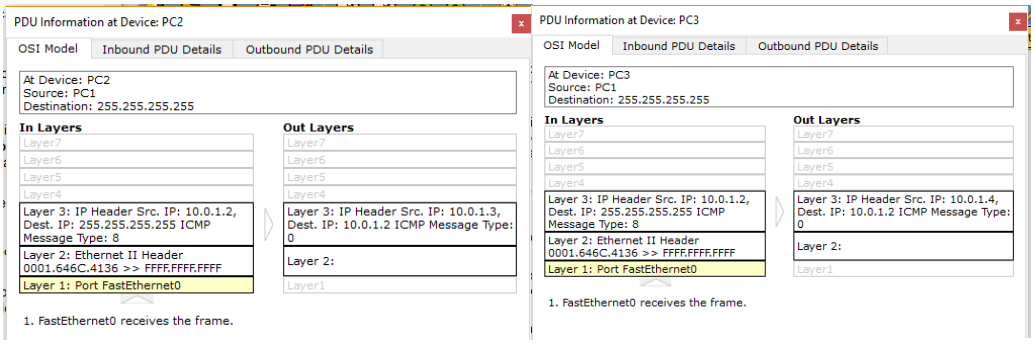
R/A: las otras aplicaciones disponibles para utilizar son: DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, entre otras.

d. Haga clic en **Create PDU** (Crear PDU). Este paquete de broadcast de prueba ahora aparece en **Simulation Panel Event List** .También aparece en la ventana PDU List (Lista de PDU). Es la primera
PDU para la Situación 0.

e. Haga clic en **Capture/Forward** dos veces. Este paquete se envía al switch y después se transmite por broadcast a la **PC2**, la **PC3**, y el **Router1**. Examine la información de la Capa 3 para todos los eventos. Observe que la dirección IP de destino es 255.255.255.255, que es la dirección IP de broadcast que configuró cuando creó la PDU compleja.





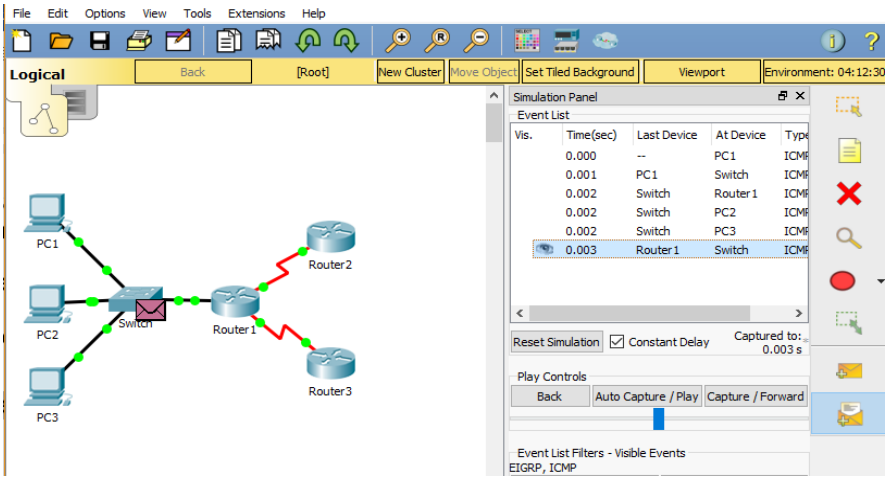


Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

R/A: De acuerdo a lo observado, la PDU se convierte en un UNICAST que contesta a la PC1

f. Haga clic en **Capture/Forward** nuevamente. ¿La PDU de broadcast se reenvía en algún momento al Router2 o al Router3? ¿Por qué?

R/A: La PDU de broadcast no se reenvía ni al Router2 ni al Router3, debido a que éste se realiza dentro de la red local.

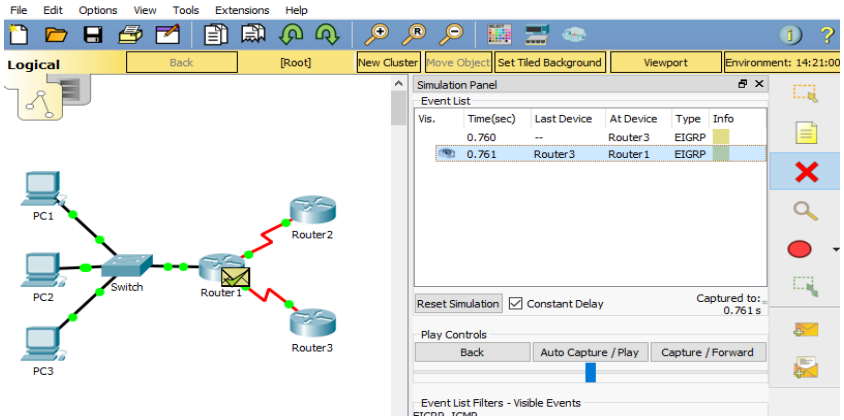


g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en **Delete** (Eliminar) debajo de **Scenario 0** (Situación 0).

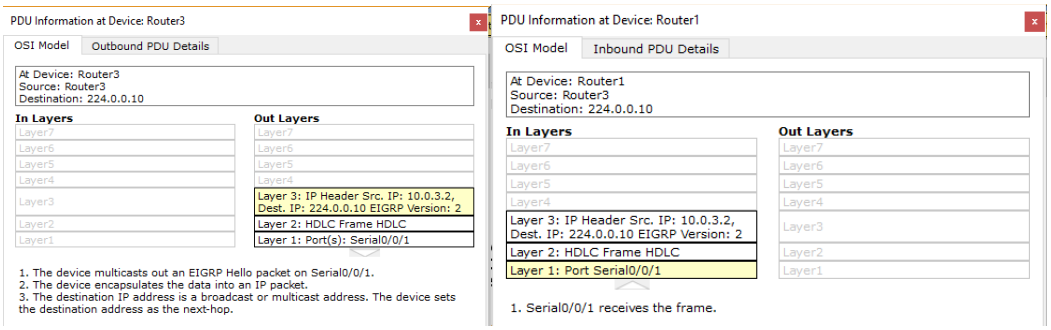
Parte 3: Investigar el tráfico de multicast

Paso 1: Examinar el tráfico que generan los protocolos de enrutamiento

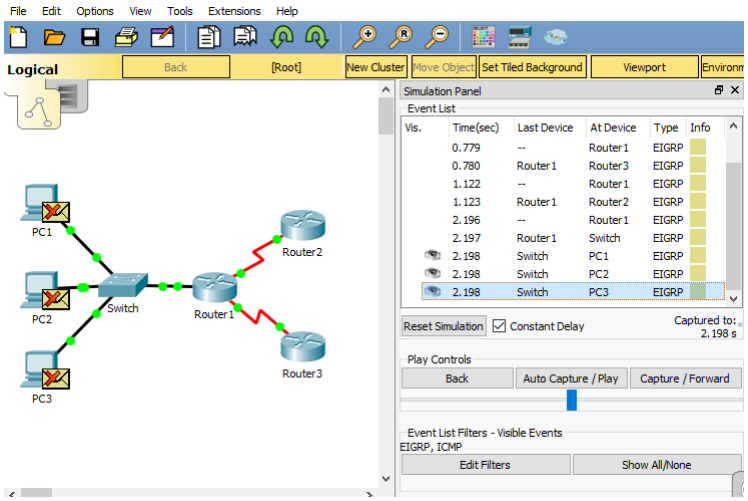
a. Haga clic en **Capture/Forward** (Capturar/avanzar). Los paquetes EIGRP están en el Router1 a la espera de que se los transmita por multicast a través de cada interfaz.



b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en **Capture/Forward**. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes a las PC.



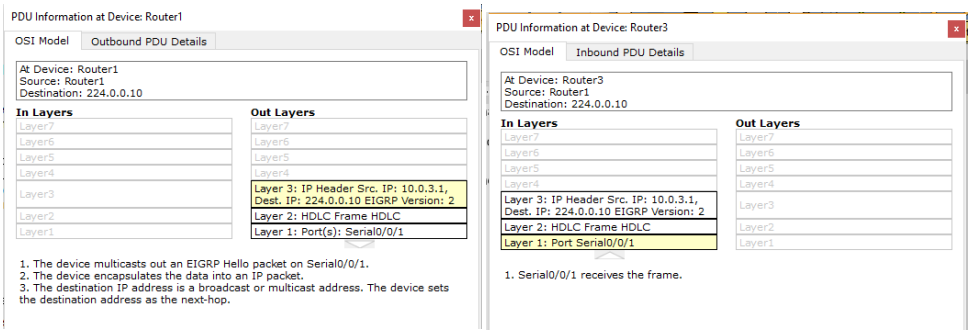
b. Haga clic en **Capture/Forward** hasta que vea que el paquete EIGRP llega a las PC.

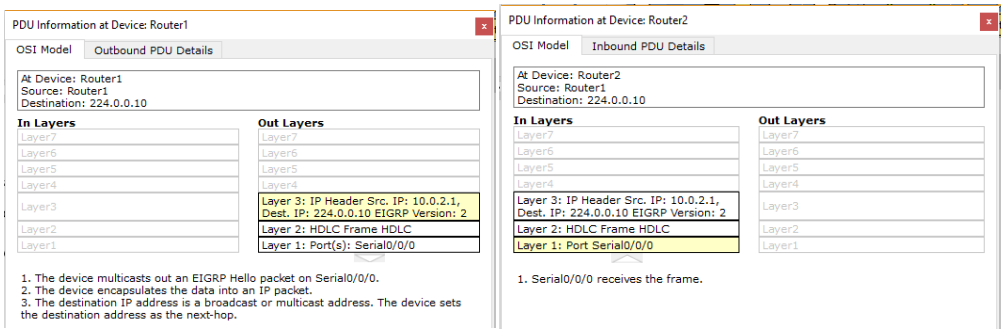


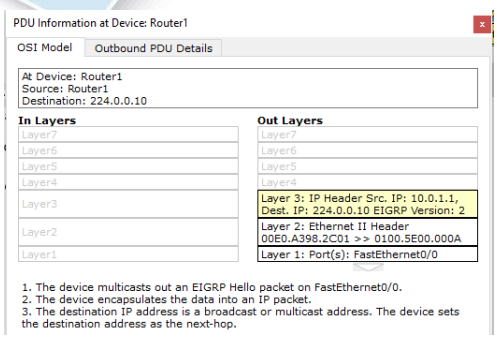
¿Qué hacen los hosts con los paquetes?

R/A: Los hosts rechazan y descartan los paquetes recibidos

Examine la información de las capas 3 y 4 para todos los eventos EIGRP.



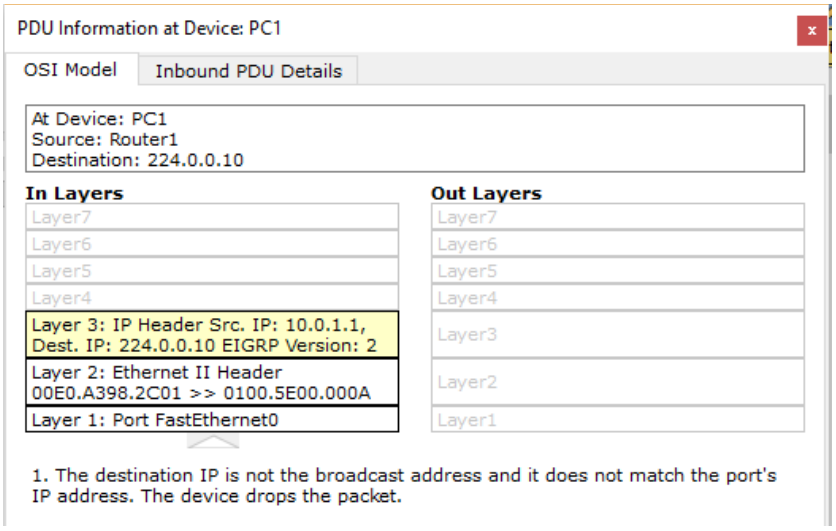




¿Cuál es la dirección de destino de cada uno de los paquetes?

R/A: Se observa que la dirección de destino de cada uno de los paquetes es la 224.0.0.10, la cual corresponde a la dirección IP de multicast para el protocolo EIGRP

d. Haga clic en uno de los paquetes entregados a una de las PC. ¿Qué sucede con esos paquetes?



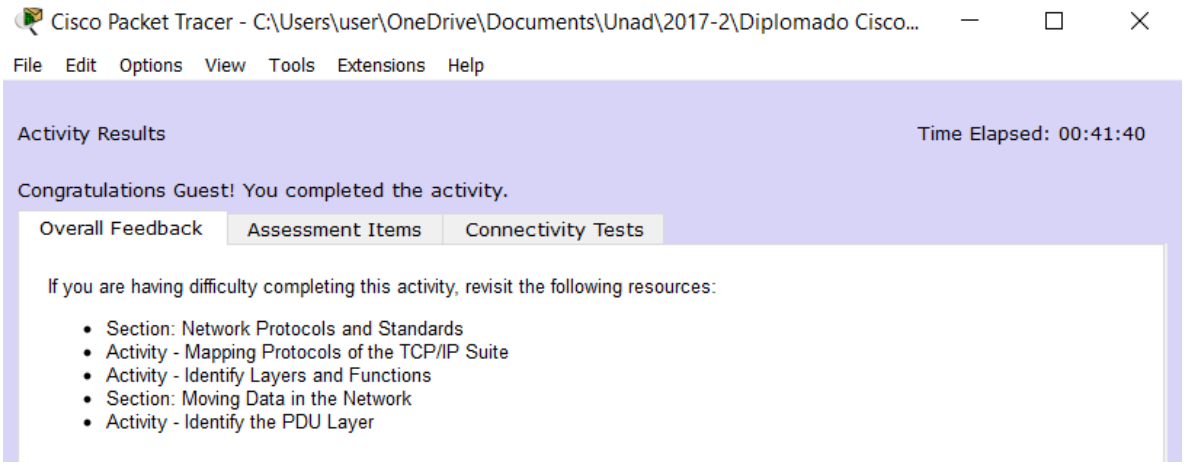
R/A: Se observa que los paquetes se descartan por lo tanto no se realiza ningún procesamiento adicional

Según el tráfico que generan los tres tipos de paquetes IP, ¿cuáles son las principales diferencias en la entrega?

R/A: Las principales diferencias en la entrega, de acuerdo al tráfico generado por los tres tipos de paquetes IP son:

- El paquete unicast atraviesa la red debiso a que está destinado a un dispositivo específico.
- El paquete broadcast se envía a cada dispositivo en la red de área local
- El paquete multicast se envía a todos los dispositivos (tanto de la red local como no local) pero éstos son procesados únicamente por los dispositivos que forman parte del grupo multicast, es decir los router

REULTADOS:



Ejercicio 8.2.5.3: Configuración de direccionamiento IPv6

Topología

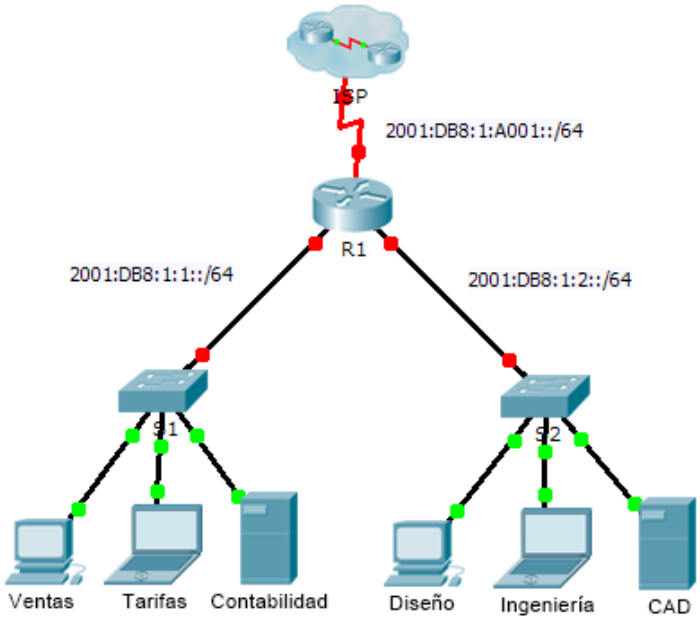


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminad
R1	G0/0	2001:DB8:1:1::1/64	No aplicable
	G0/1	2001:DB8:1:2::1/64	No aplicable
	S0/0/0	2001:DB8:1:A001::2/64	No aplicable
	Link-local	FE80::1	No aplicable
Ventas	NIC	2001:DB8:1:1::2/64	FE80::1
Tarifas	NIC	2001:DB8:1:1::3/64	FE80::1
Contabilidad	NIC	2001:DB8:1:1::4/64	FE80::1
Diseño	NIC	2001:DB8:1:2::2/64	FE80::1
Ingeniería	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objetivos

Parte 1: Configurar el direccionamiento IPv6 en el router

Parte 2: Configurar el direccionamiento IPv6 en los servidores.

Parte 3: Configurar el direccionamiento IPv6 en los clientes Parte 4: Probar y verificar la conectividad de red

Información básica

En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación de las direcciones IPv6.

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

a. Introduzca el comando de configuración global ipv6 unicast-routing. Este comando se debe configurar para habilitar el router para que reenvíe paquetes IPv6. Este comando se analizará en otro semestre.

```
R1(config)# ipv6 unicast-routing
```

```
R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#
```

Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

a. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **Entrar**. b. Ingrese al modo EXEC privilegiado.

c. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/0.

d. Configure la dirección IPv6 con el siguiente comando:

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

e. Configure la dirección IPv6 link-local con el siguiente comando:

```
R1(config-if)# ipv6 address FE80::1 link-local
```

f. Active la interfaz.

```
R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
```

Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/1.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta. c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

```
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:1:2::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

Paso 4: Configurar el direccionamiento IPv6 en Serial0/0/0

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para Serial0/0/0.

b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.

c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

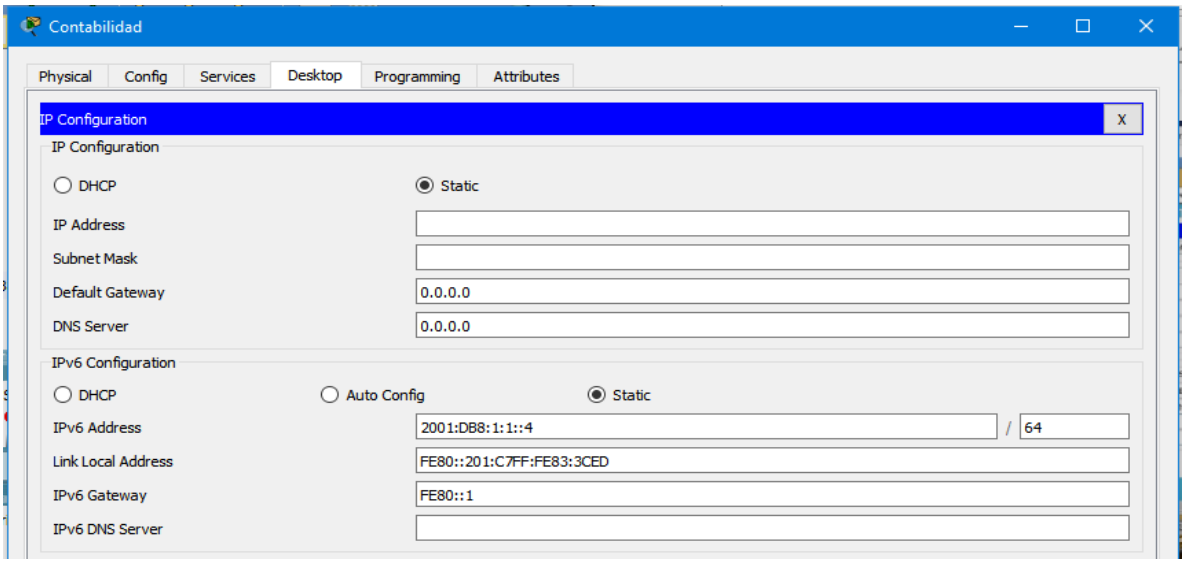
```
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:1:A001::2/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
 R1(config-if)#
 %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

Parte 2: Configurar el direccionamiento IPv6 en los servidores

Paso 1: Configurar el direccionamiento IPv6 en el servidor de contabilidad

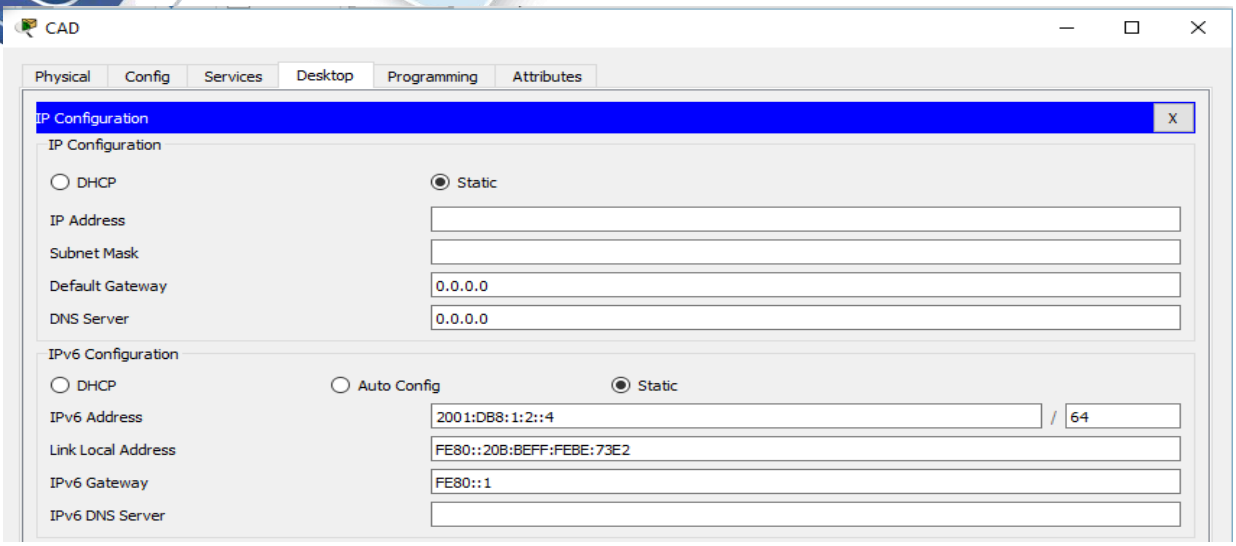
a. Haga clic en **Accounting** (Contabilidad) y, a continuación, en la ficha **Desktop** > **IP Configuration**
(Escritorio > Configuración de IP).

c. Establezca la **dirección IPv6 2001:DB8:1:1::4** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



Paso 2: Configurar el direccionamiento IPv6 en el servidor CAD

Repita los pasos 1a a 1c para el servidor **CAD**. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

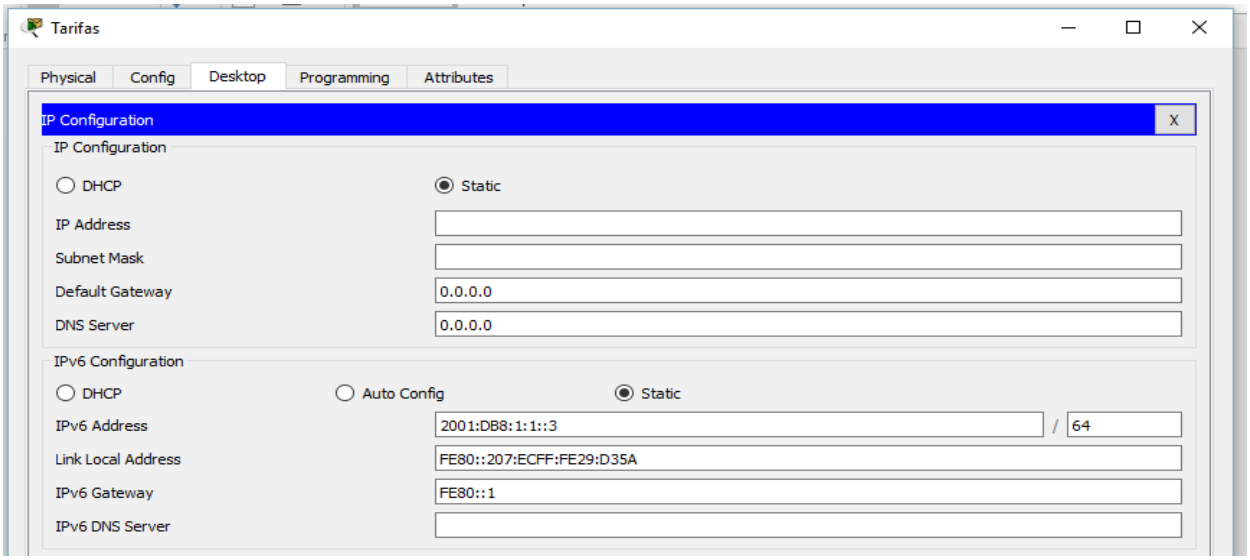


Parte 3: Configurar el direccionamiento IPv6 en los clientes

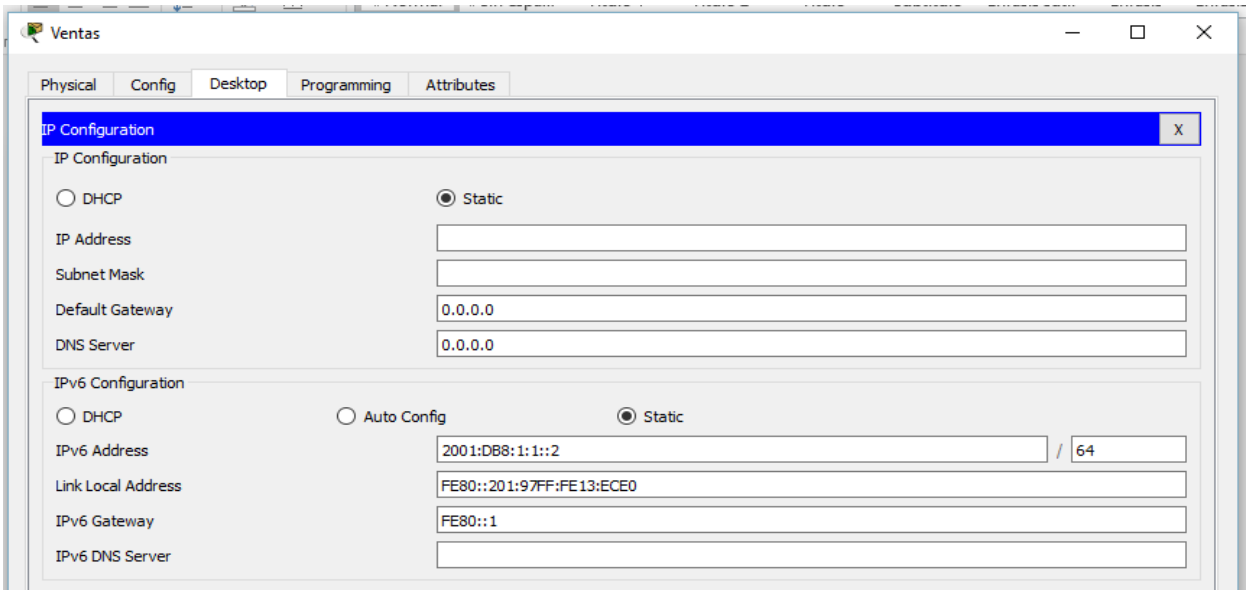
Paso 1: Configurar el direccionamiento IPv6 en los clientes de ventas y facturación

a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

c. Establezca la **dirección IPv6 2001:DB8:1:1::3** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



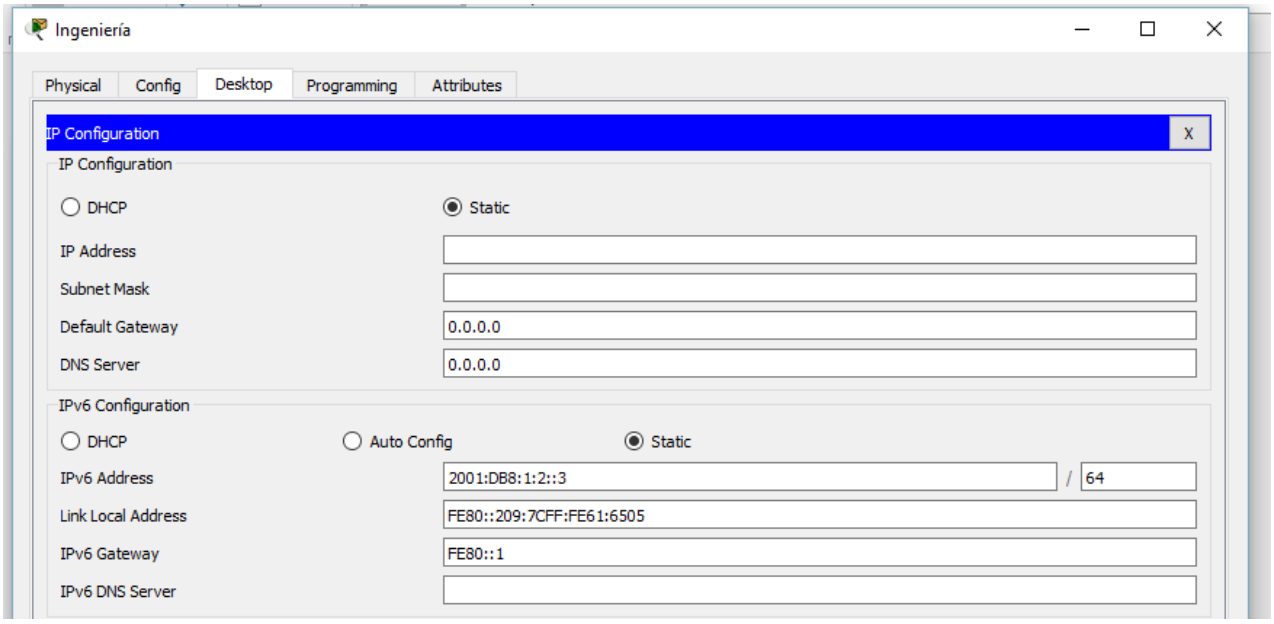
d. Repita los pasos 1a a 1c para **Sales** (Ventas). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.



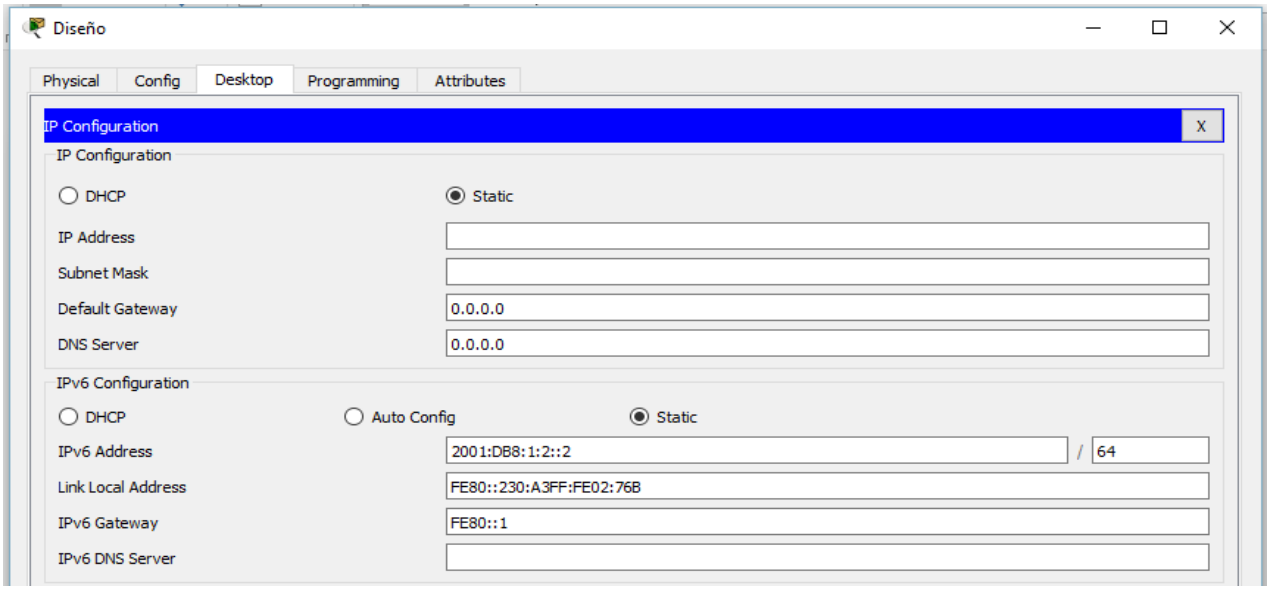
Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:2::3** con el prefijo **/64**. c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



d. Repita los pasos 1a a 1c para **Design** (Diseño). Consulte la **tabla de direccionamiento** para obtener la dirección IPv6.

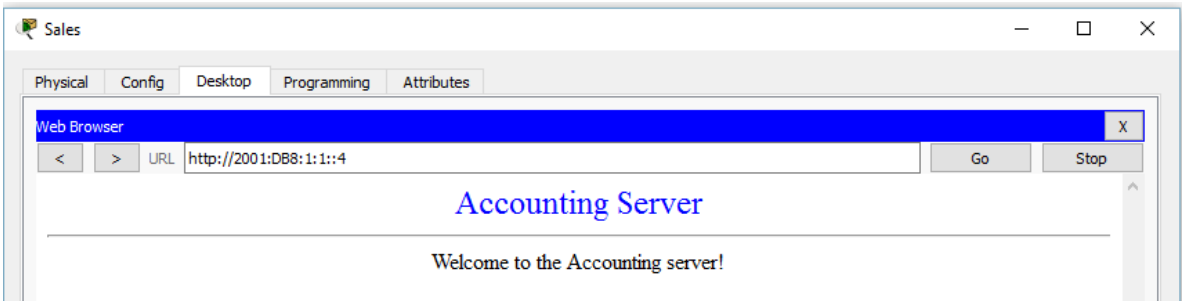


Parte 4: Probar y verificar la conectividad de la red

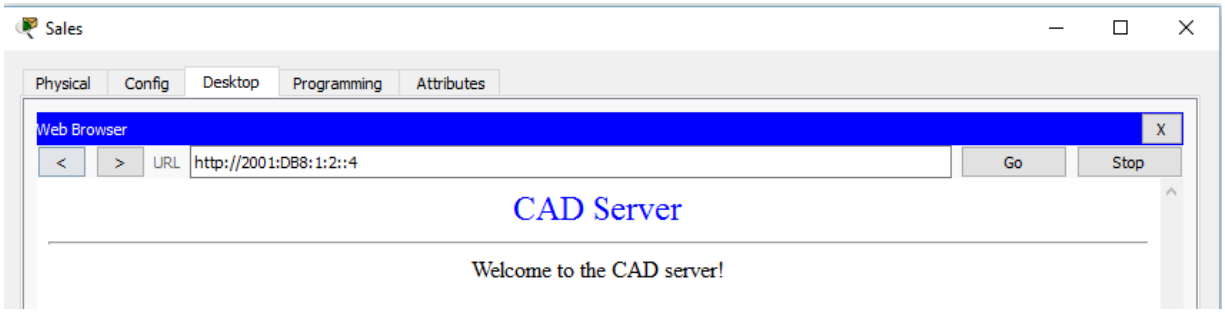
Paso 1: Abrir las páginas Web del servidor de los clientes

a. Haga clic en **Sales** y, a continuación, en la ficha **Desktop**. Si es necesario, cierre la ventana **IP Configuration**.

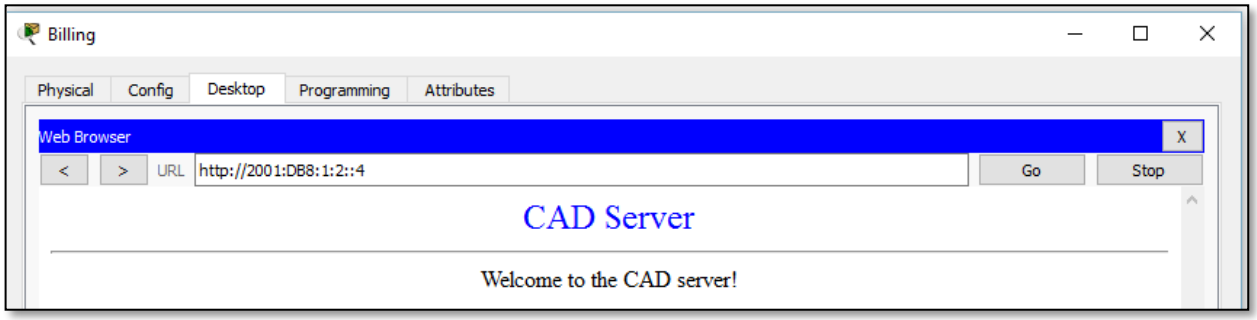
b. Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.

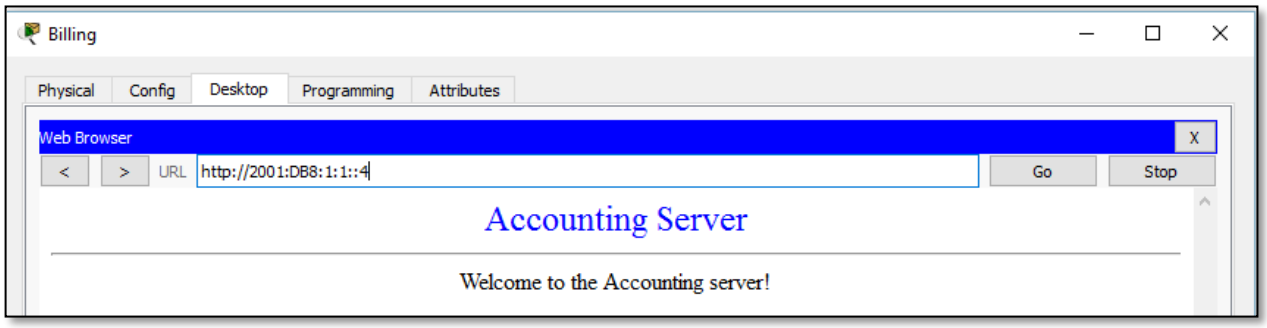


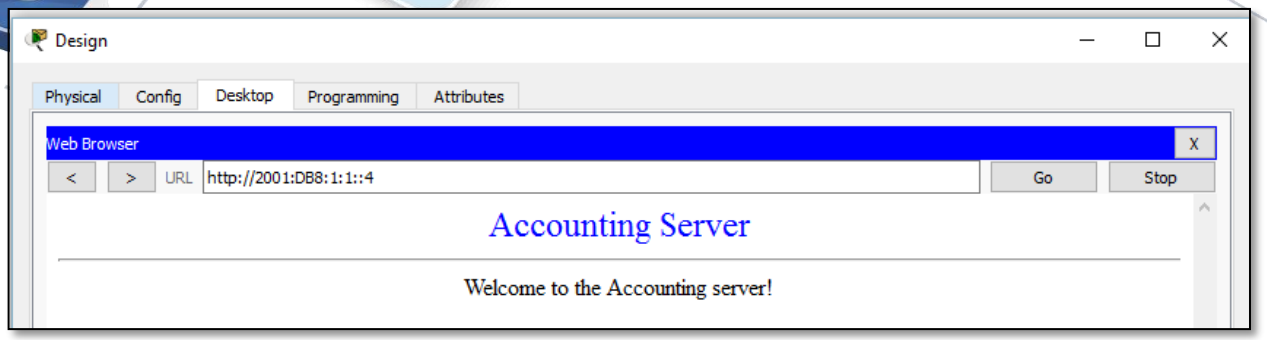
c. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.

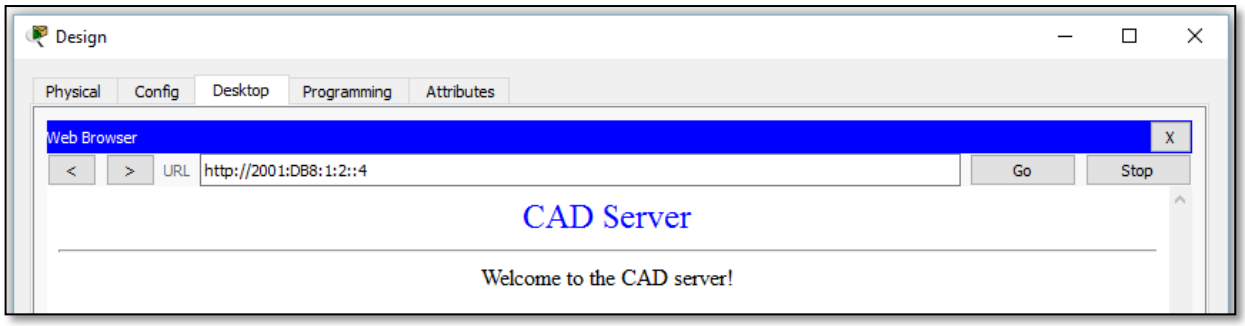


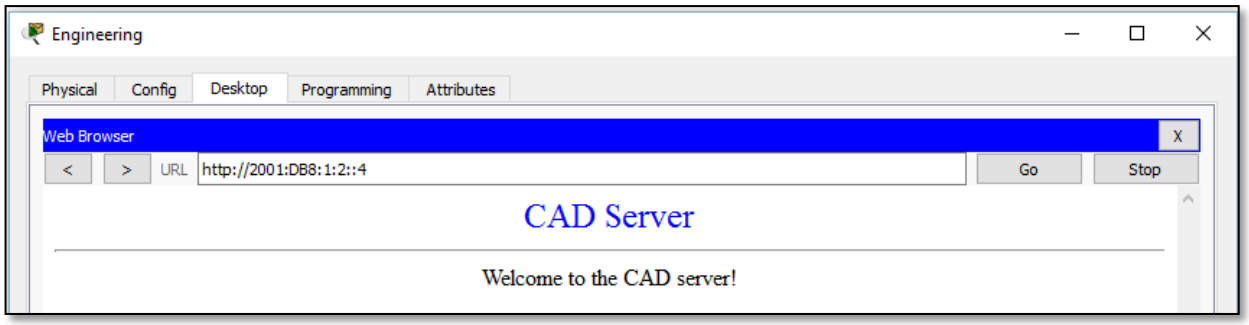
d. Repita los pasos 1a a 1d para el resto de los clientes.

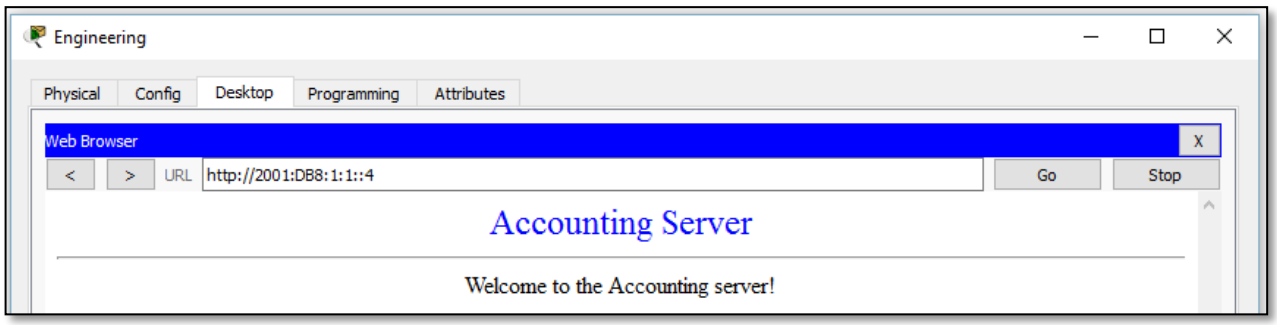





Design
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://2001:DB8:1:1::4
Go
Stop
Accounting Server
Welcome to the Accounting server!


Design
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://2001:DB8:1:2::4
Go
Stop
CAD Server
Welcome to the CAD server!


Engineering
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://2001:DB8:1:2::4
Go
Stop
CAD Server
Welcome to the CAD server!

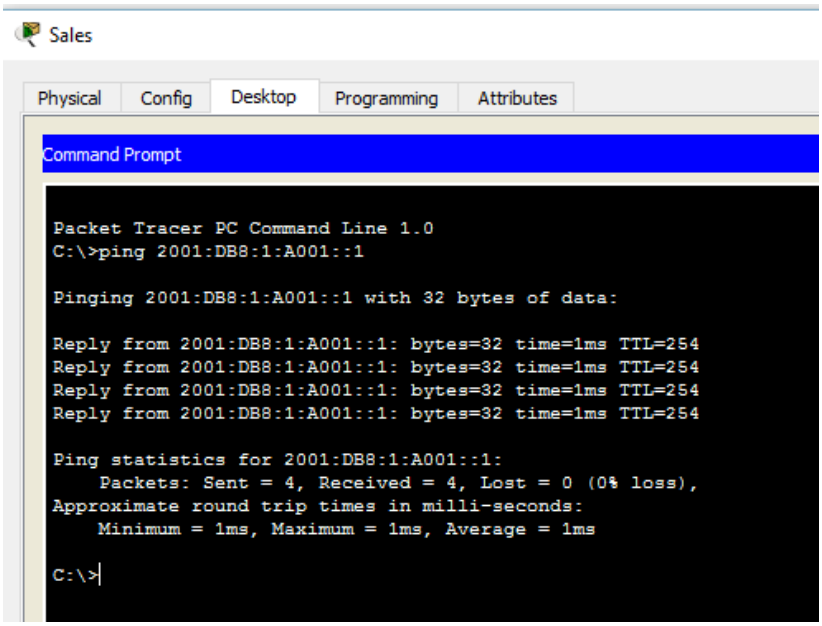

Engineering
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://2001:DB8:1:1::4
Go
Stop
Accounting Server
Welcome to the Accounting server!

Paso 2: Hacer ping al ISP

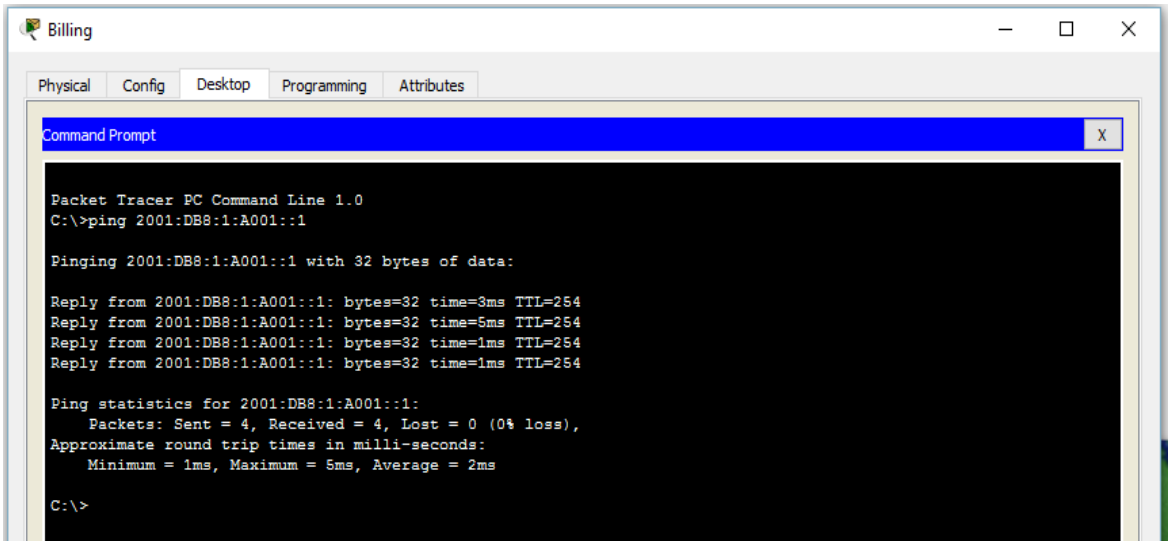
a. Abra una ventana de configuración de cualquier equipo cliente haciendo clic en el ícono.

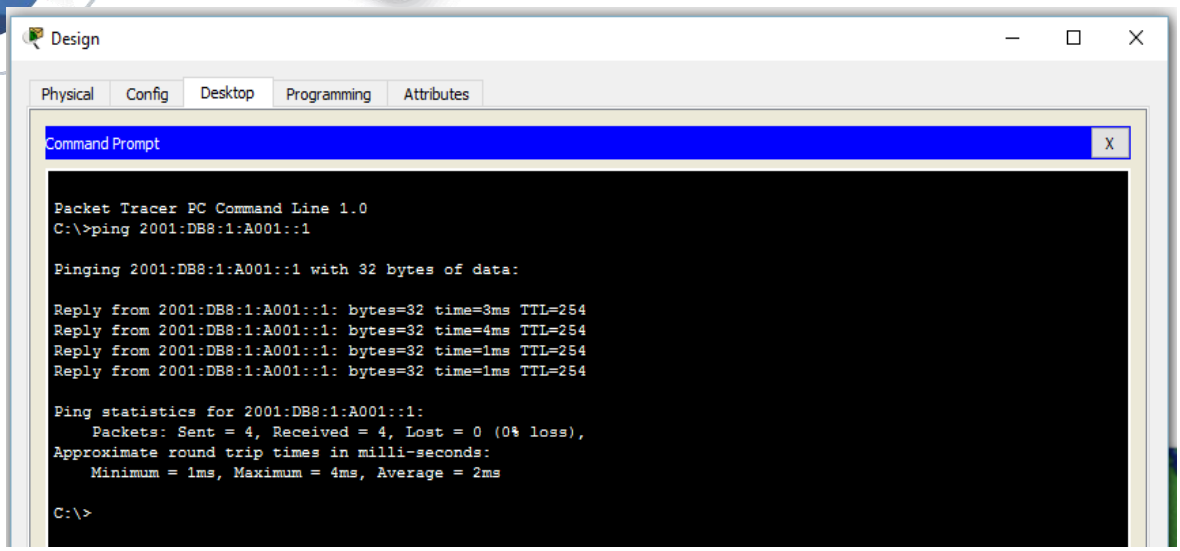
b. Haga clic en la ficha **Desktop** > **Command Prompt** (Símbolo del sistema).

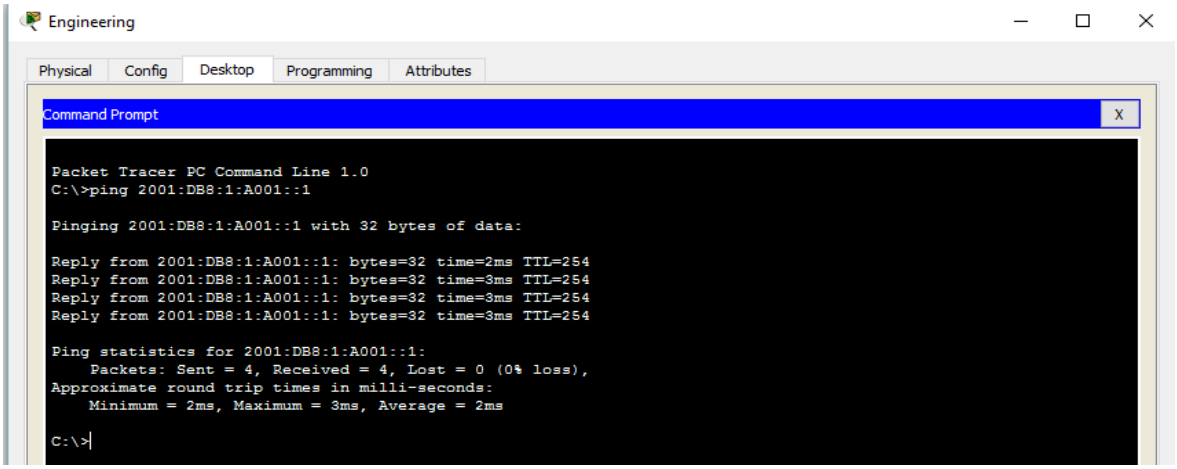
c. Pruebe la conectividad al ISP con el siguiente comando:
PC> **ping 2001:DB8:1:A001::1**



d. Repita el comando **ping** con otros clientes hasta que se haya verificado la conectividad completa.




Design
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1
Pinging 2001:DB8:1:A001::1 with 32 bytes of data:
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=4ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Ping statistics for 2001:DB8:1:A001::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 2ms
C:\>


Engineering
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:A001::1
Pinging 2001:DB8:1:A001::1 with 32 bytes of data:
Reply from 2001:DB8:1:A001::1: bytes=32 time=2ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=3ms TTL=254
Ping statistics for 2001:DB8:1:A001::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>

Ejercicio 8.3.2.5: Verificación del direccionamiento IPv4 e IPv6

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4 / Dirección/Prefijo IPv6	Máscara de subred	Gateway predeterminado
R1	G0/0	10.10.1.97	255.255.255.224	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
	Link-local	FE80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
	Link-local	FE80::2		No aplicable
R3	G0/0	10.10.1.17	255.255.255.240	No aplicable
		2001:DB8:1:4::1/64		No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
	Link-local	FE80::3		No aplicable
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
		2001:DB8:1:1::A/64		FE80::1
PC2	NIC	10.10.1.20	255.255.255.240	10.10.1.17
		2001:DB8:1:4::A/64		FE80::3

Objetivos

Parte 1: Completar la documentación de la tabla de direccionamiento

Parte 2: Probar la conectividad mediante el comando ping

Parte 3: Descubrir la ruta mediante su rastreo

Información básica

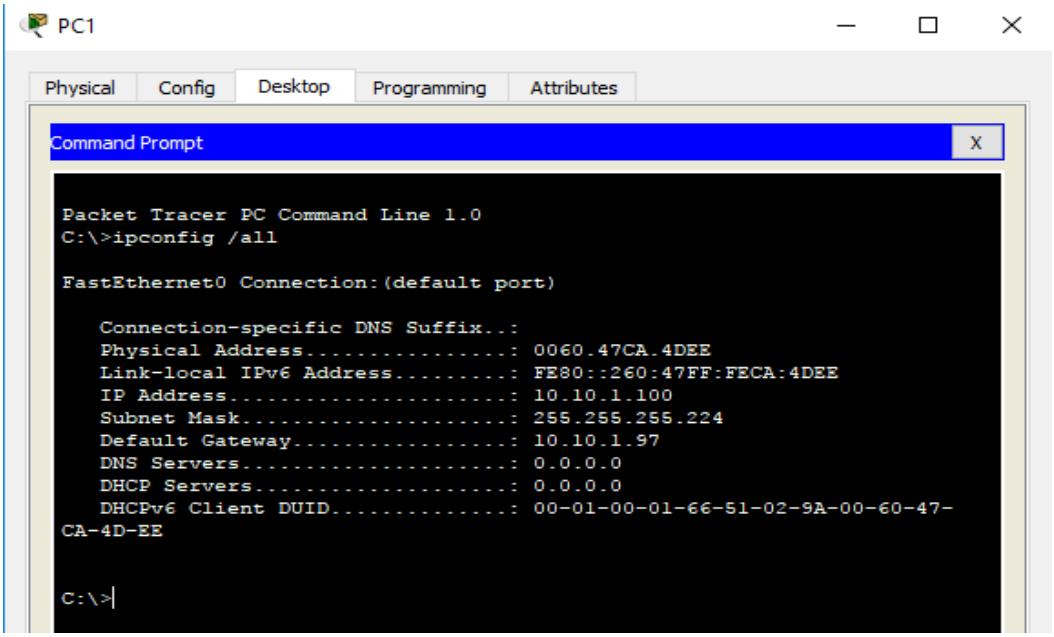
La técnica dual- stack permite que IPv4 e IPv6 coexistan en la misma red. En esta actividad, investigará la implementación de una técnica dual-stack incluidos la documentación de la configuración de IPv4 e IPv6 para dispositivos finales, la prueba de conectividad para IPv4 e IPv6 mediante el comando **ping** y el rastreo de la ruta de extremo a extremo para IPv4 e IPv6.

Parte 1: Completar la documentación de la tabla de direccionamiento

Paso 1: Usar el comando ipconfig para verificar el direccionamiento IPv4

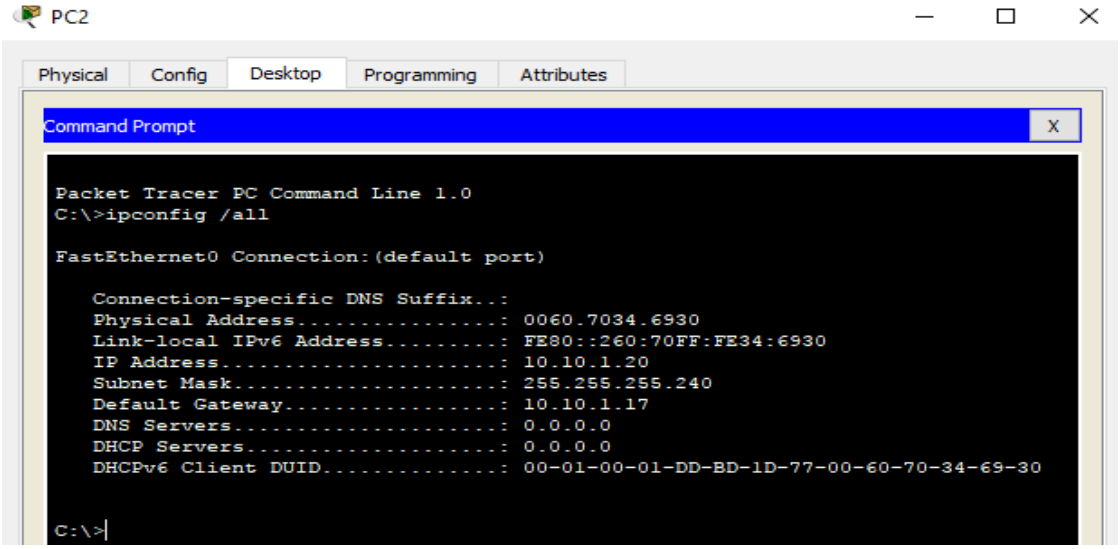
- Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

- Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.



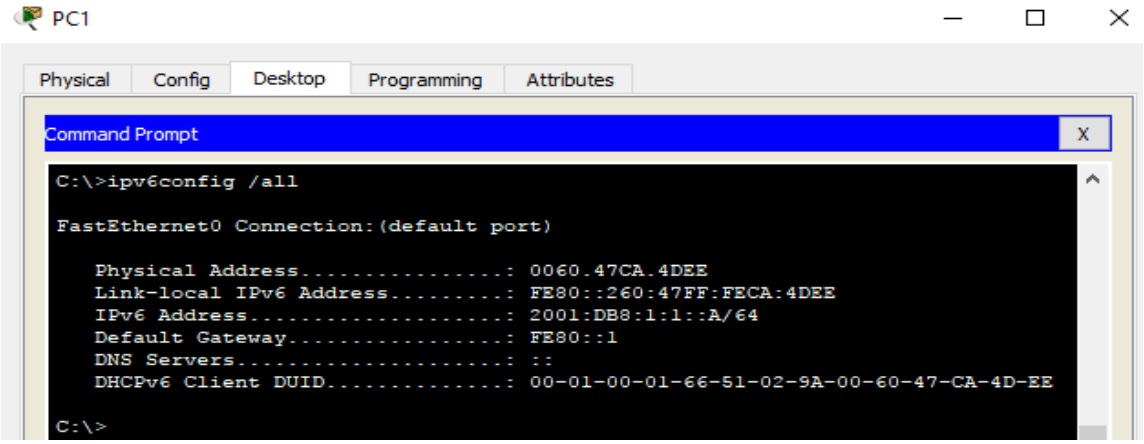
- Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

- Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

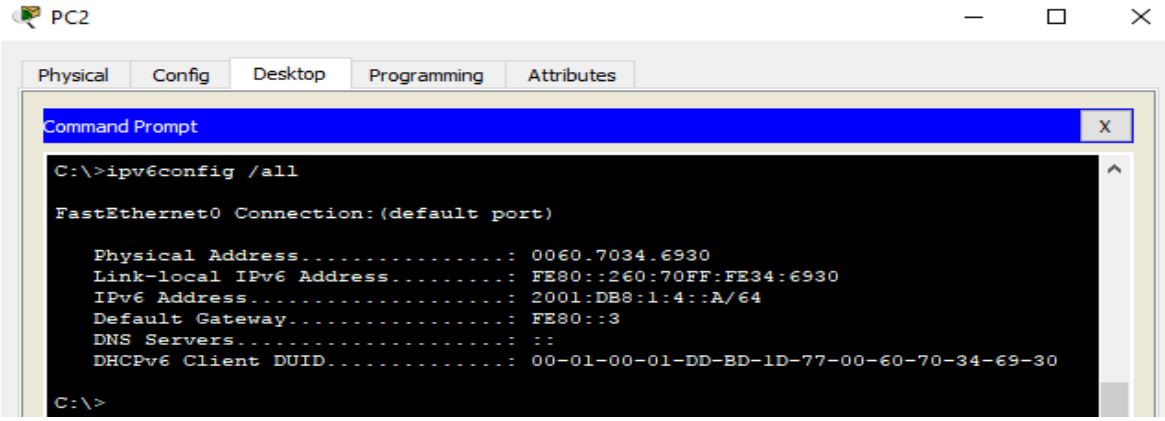


Paso 2: Usar el comando ipv6config para verificar el direccionamiento IPv6

a. En la **PC1**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.



b. En la **PC2**, introduzca el comando **ipv6config /all** para recopilar la información de IPv6. Complete la **tabla de direccionamiento** con la dirección IPv6, el prefijo de subred y el gateway predeterminado.

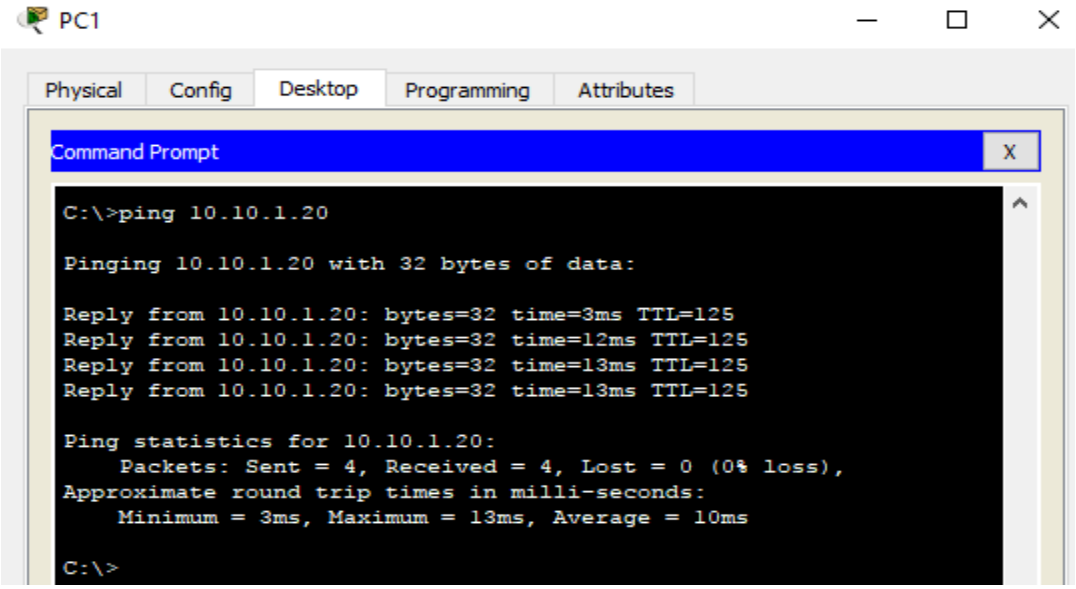


Parte 2: Probar la conectividad mediante el comando ping

Paso 1: Usar el comando ping para verificar la conectividad IPv4

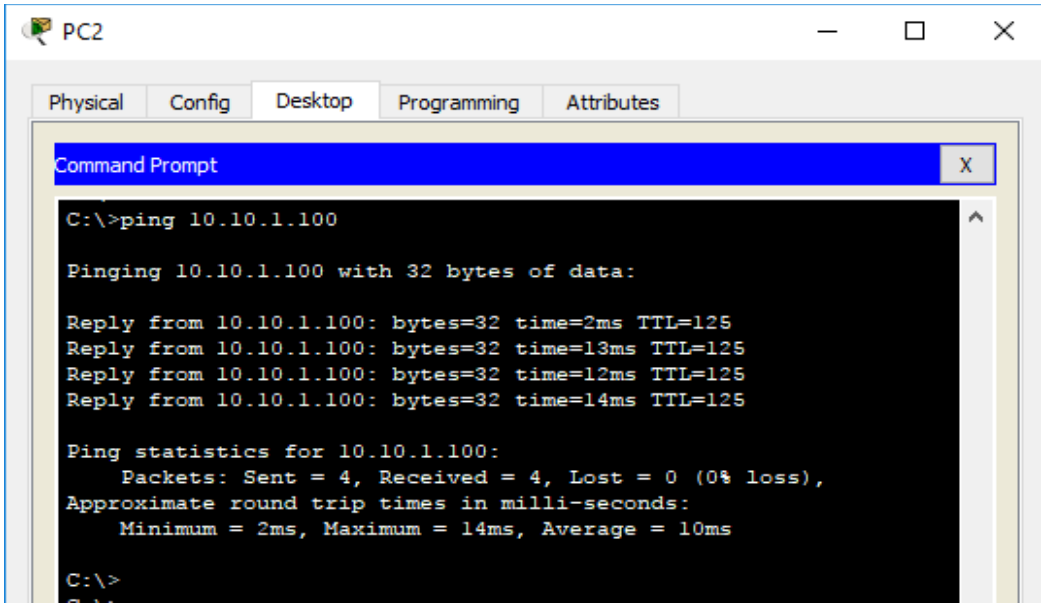
e. Desde la **PC1**, haga ping a la dirección IPv4 de la **PC2**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



f. Desde la **PC2**, haga ping a la dirección IPv4 de la **PC1**. ¿El resultado fue satisfactorio?

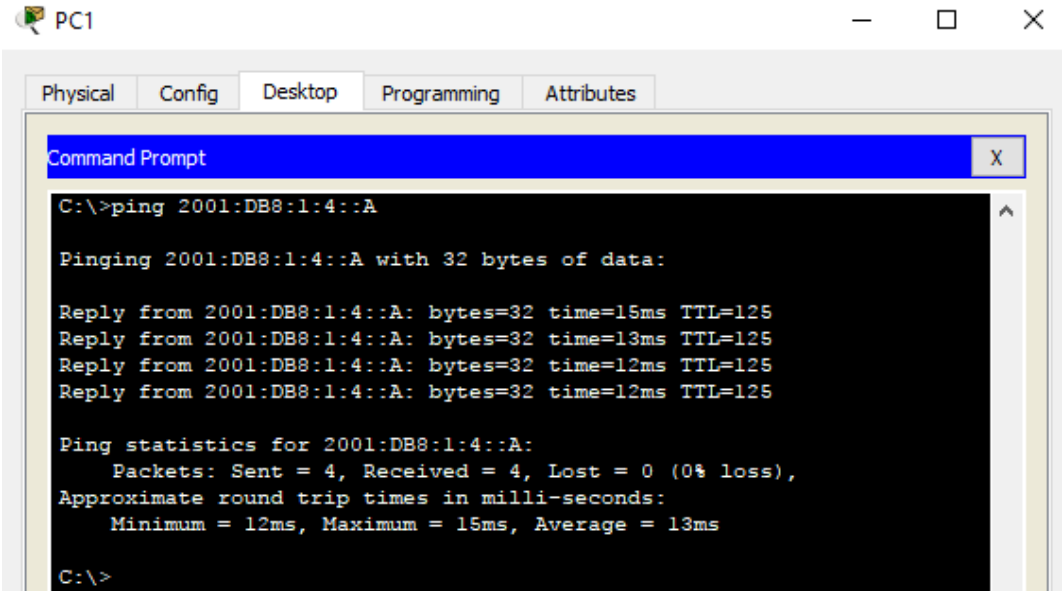
R: Si es satisfactorio



Paso 2: Usar el comando ping para verificar la conectividad IPv6

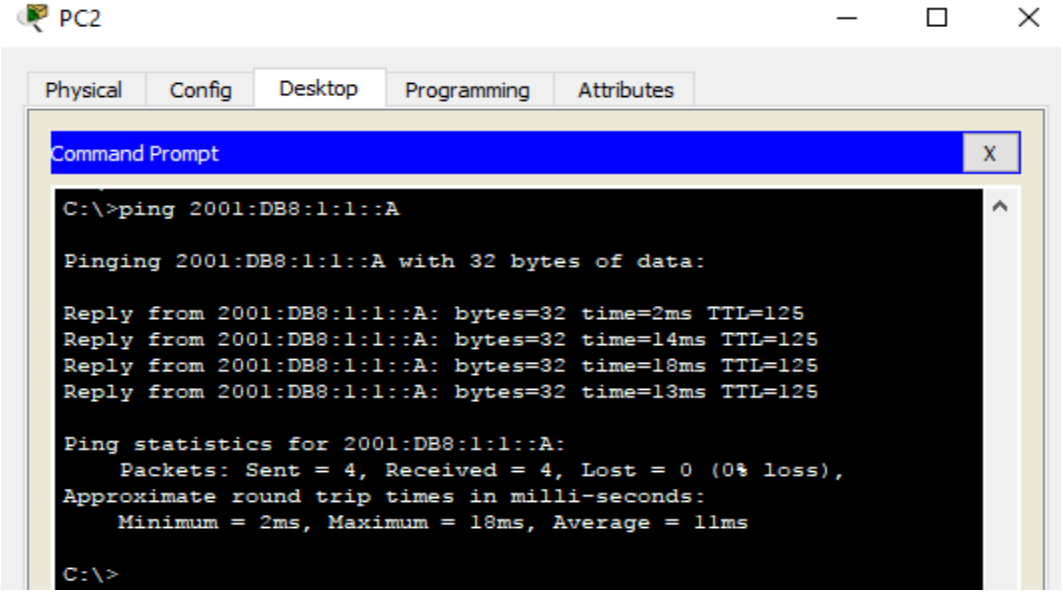
d. Desde la **PC1**, haga ping a la dirección IPv6 de la **PC2**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



e. Desde la **PC2**, haga ping a la dirección IPv6 de la **PC1**. ¿El resultado fue satisfactorio?

R: Si es satisfactorio



Parte 3: Descubrir la ruta mediante su rastreo

Paso 1: Usar el comando tracert para descubrir la ruta IPv4

d. Desde la **PC1**, rastree la ruta a la **PC2**.

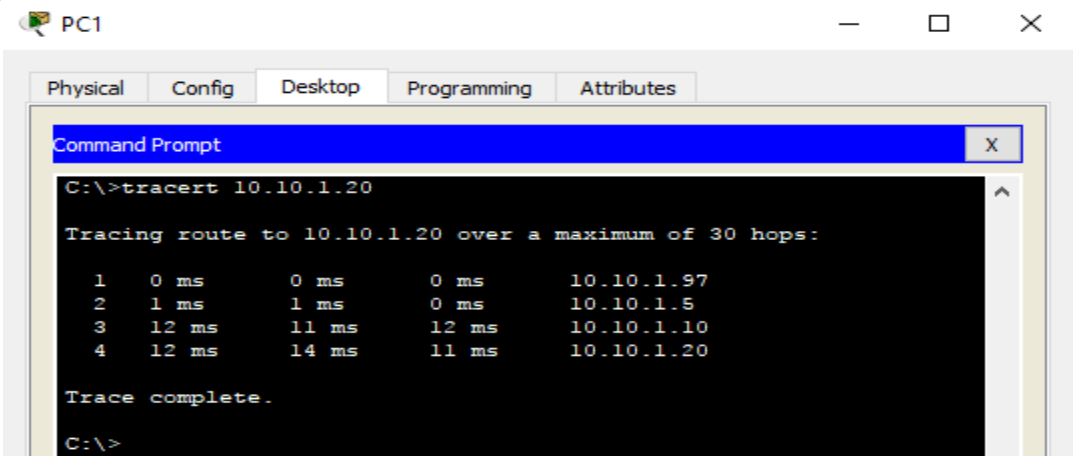
```
PC> tracert 10.10.1.20
```

¿Qué direcciones se encontraron a lo largo de la ruta?

R: 10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20

¿Con qué interfaces se asocian las cuatro direcciones?

R: G0/0 del R1, S0/0/0 en el R2, S0/0/01 en el R3, NIC de la PC2

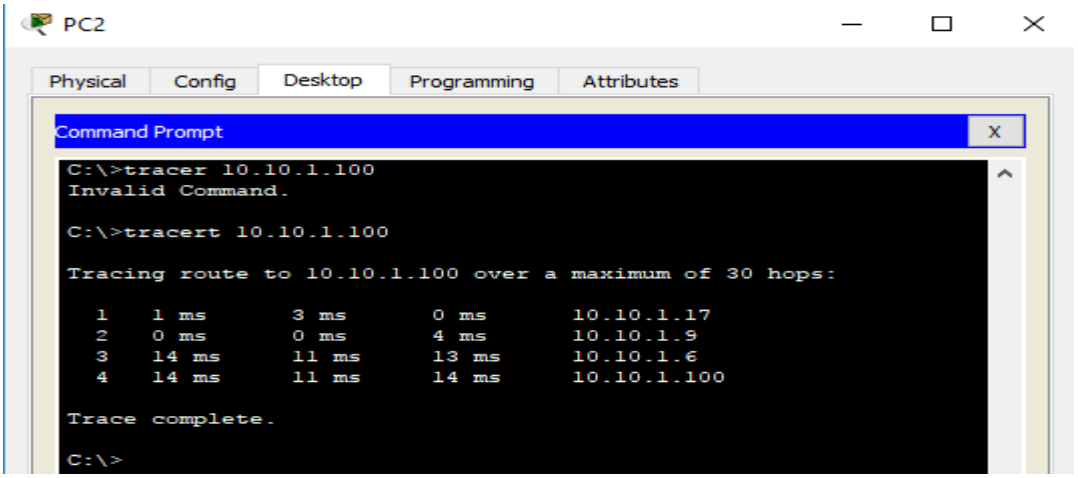


e. Desde la **PC2**, rastree la ruta a la **PC1**.

¿Qué direcciones se encontraron a lo largo de la ruta?
R: 10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100

¿Con qué interfaces se asocian las cuatro direcciones?

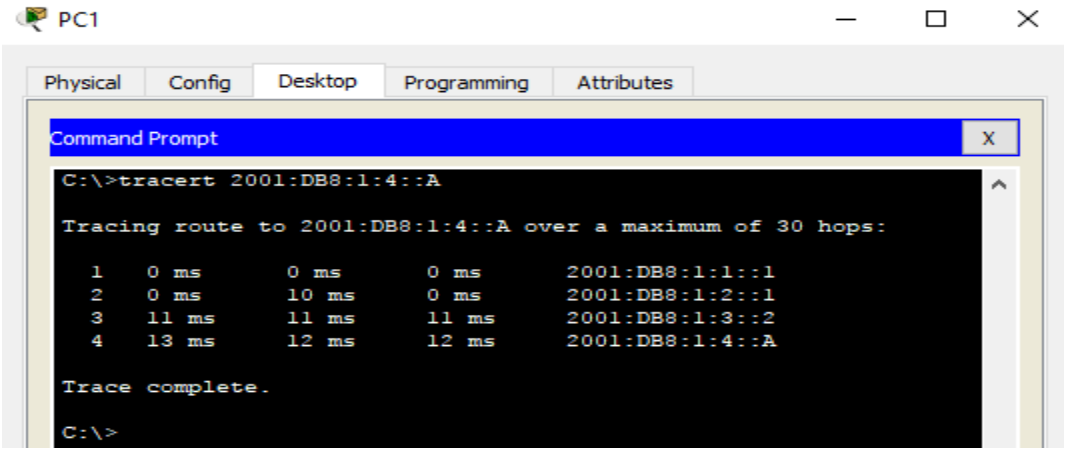
R: G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1



Paso 2: Usar el comando tracert para descubrir la ruta IPv6

e. Desde la **PC1**, rastree la ruta a la dirección IPv6 de la **PC2**.

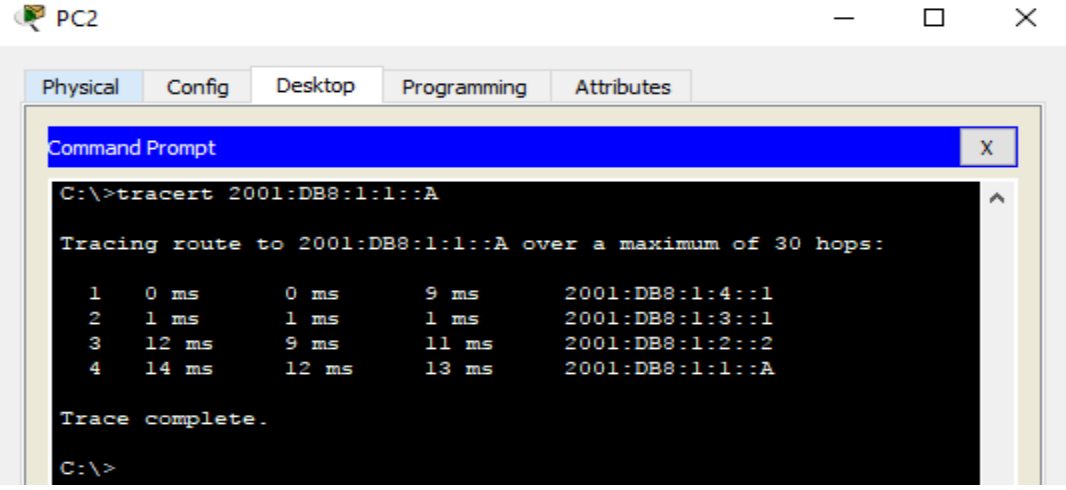
```
PC> tracert 2001:DB8:1:4::A
```



¿Qué direcciones se encontraron a lo largo de la ruta?
R: 2001:DB8:1:1::1, 2001:DB8:1:2::1, 2001:DB8:1:3::2, 2001:DB8:1:4::A

¿Con qué interfaces se asocian las cuatro direcciones?
R: G0/0 del R1, S0/0/0 del R2, S0/0/1 del R3, NIC de la PC2

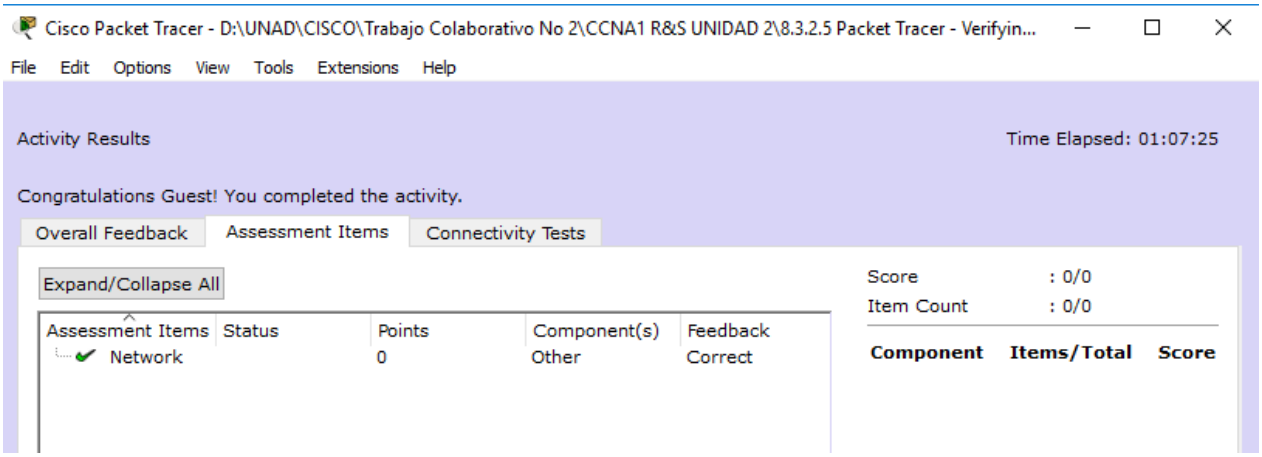
f. Desde la **PC2**, rastree la ruta a la dirección IPv6 de la **PC1**.



¿Qué direcciones se encontraron a lo largo de la ruta?
R: 2001:DB8:1:4::1, 2001:DB8:1:3::1, 2001:DB8:1:2::2, 2001:DB8:1:1::A

¿Con qué interfaces se asocian las cuatro direcciones?
R: Ga0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1

Ítems Resueltos



Ejercicio 8.3.2.6: Ping y rastreo para probar rutas

Topología

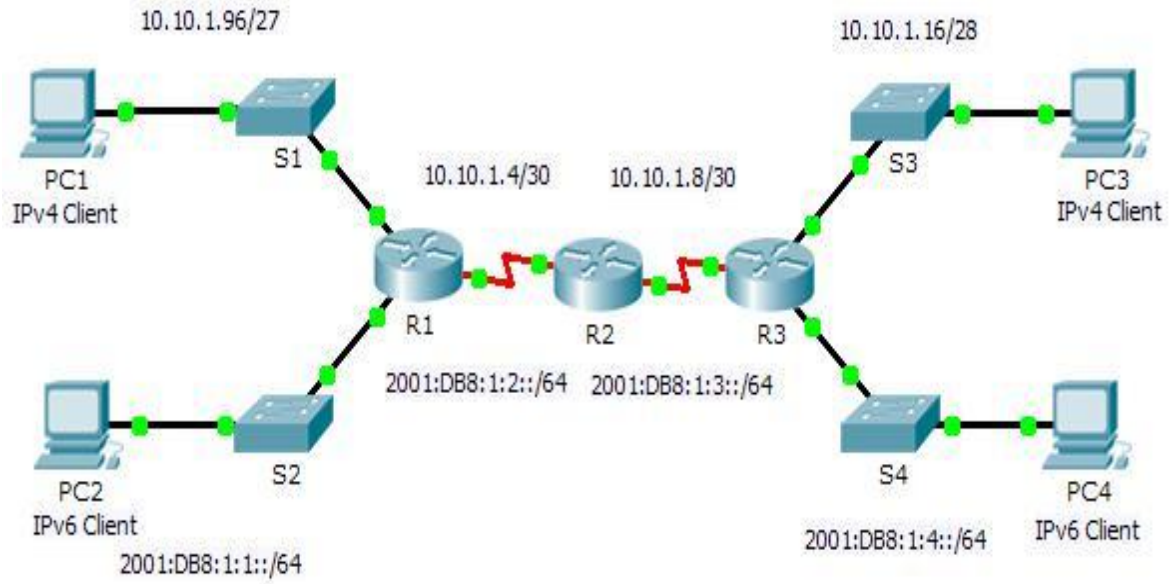


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	2001:DB8:1:1::1/64		No aplicable
	G0/1	10.10.1.97	255.255.255.224	No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:DB8:1:2::2/64		No aplicable
	Link-local	FE80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:DB8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:DB8:1:3::1/64		No aplicable
	Link-local	FE80::2		No aplicable
R3	G0/0	2001:DB8:1:4::1/64		No aplicable
	G0/1	10.10.1.17	255.255.255.240	No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:DB8:1:3::2/64		No aplicable
	Link-local	FE80::3		No aplicable
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:DB8:1:1::2/64		FE80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:DB8:1:4::2/64		FE80::1

Objetivos

Parte 1: Probar y restaurar la conectividad IPv4
Parte 2: Probar y restaurar la conectividad IPv6

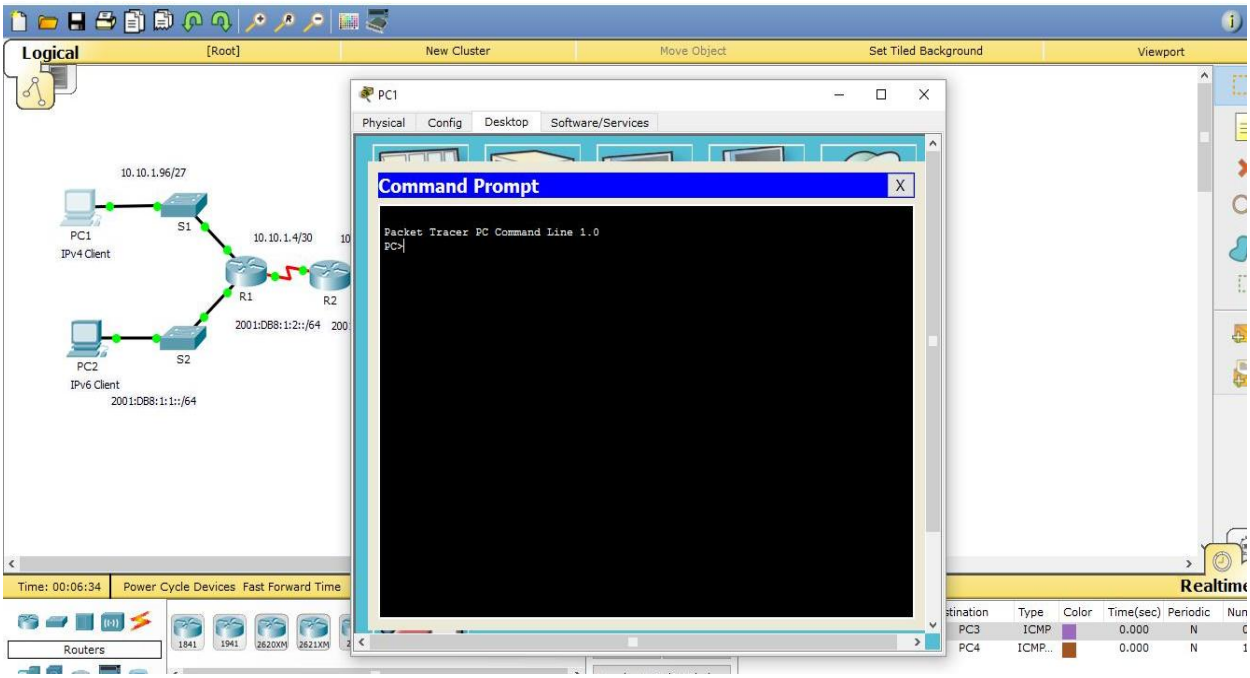
Situación

En esta actividad, hay problemas de conectividad. Además de recopilar y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad. **Nota:** la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

Packet Tracer: uso de herramientas de ping y rastreo para probar la ruta

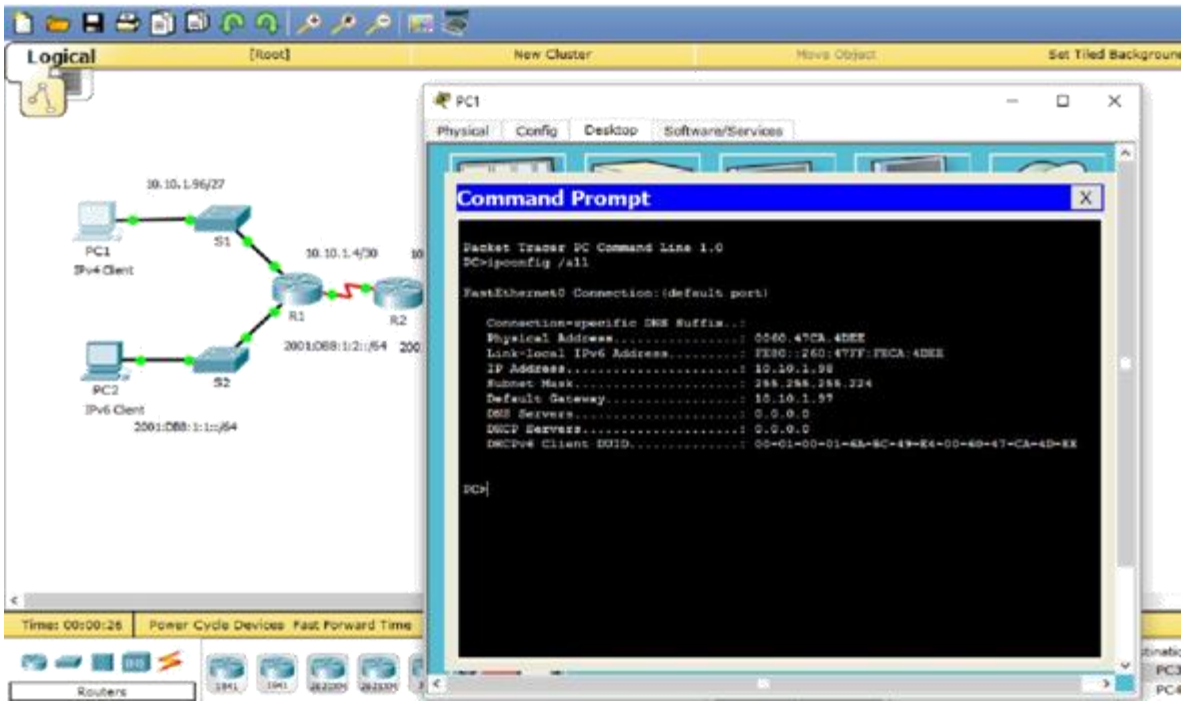
Parte 1: Probar y restaurar la conectividad IPv4

Paso 1: Usar los comandos ipconfig y ping para verificar la conectividad a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).

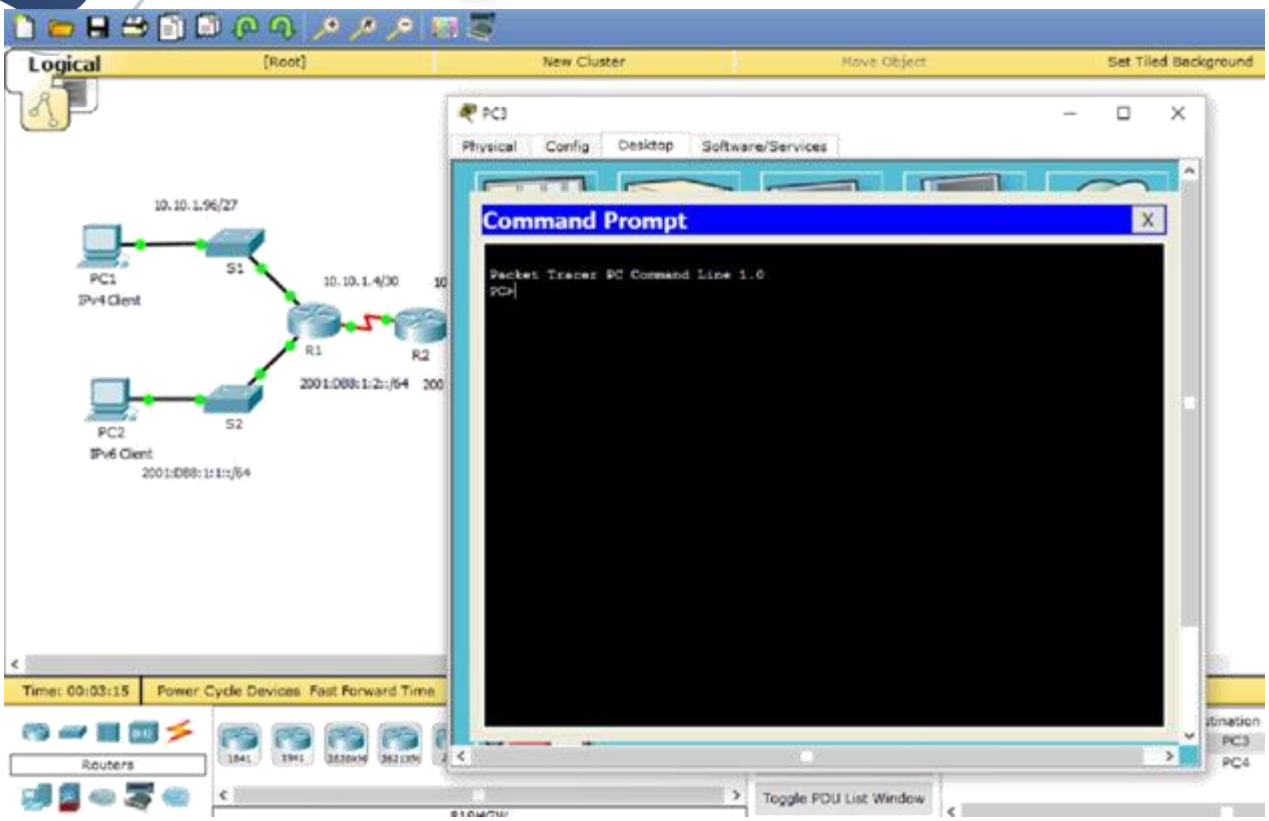


b. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de reccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

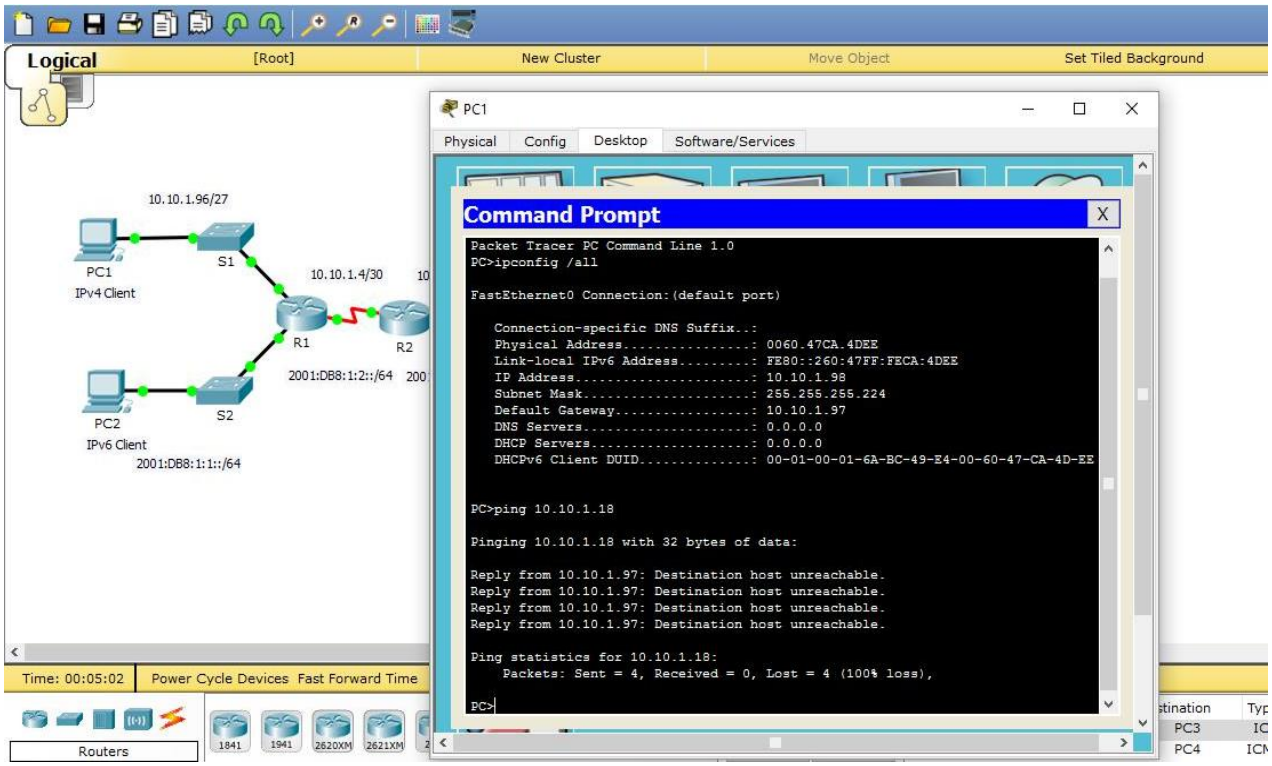
c. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**



d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

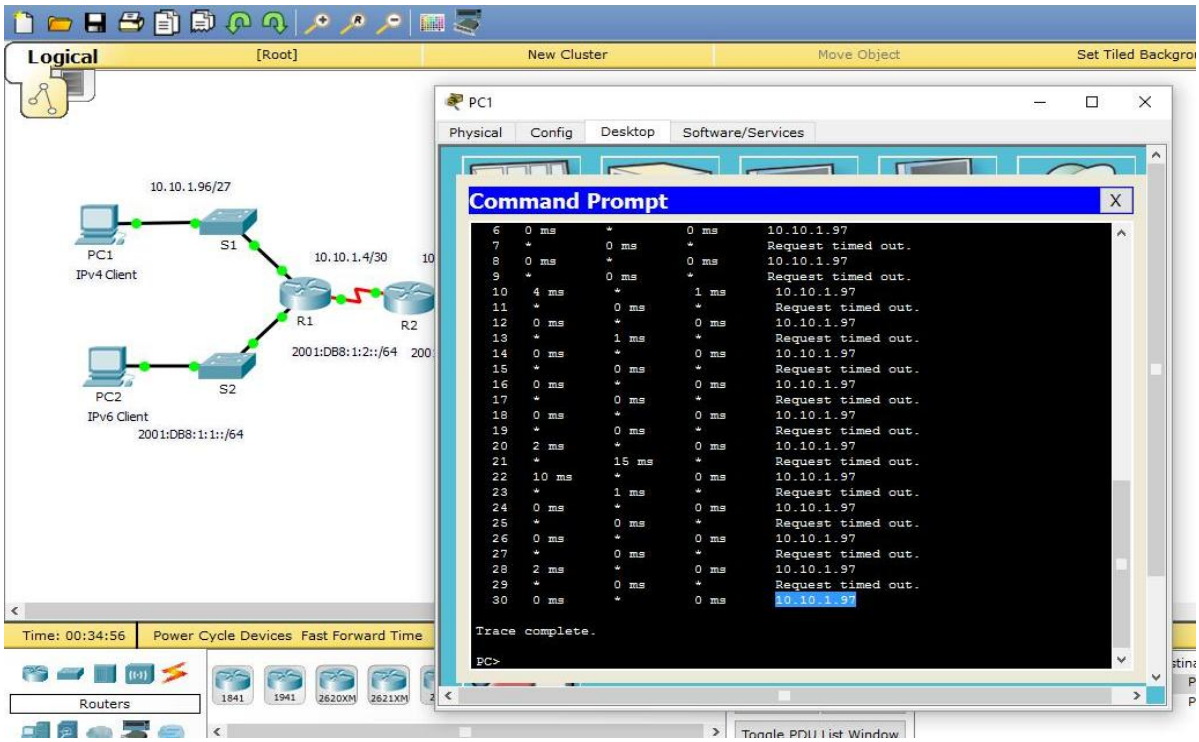


d. Pruebe la conectividad entre la **PC1** y la **PC3**. El ping debe fallar.

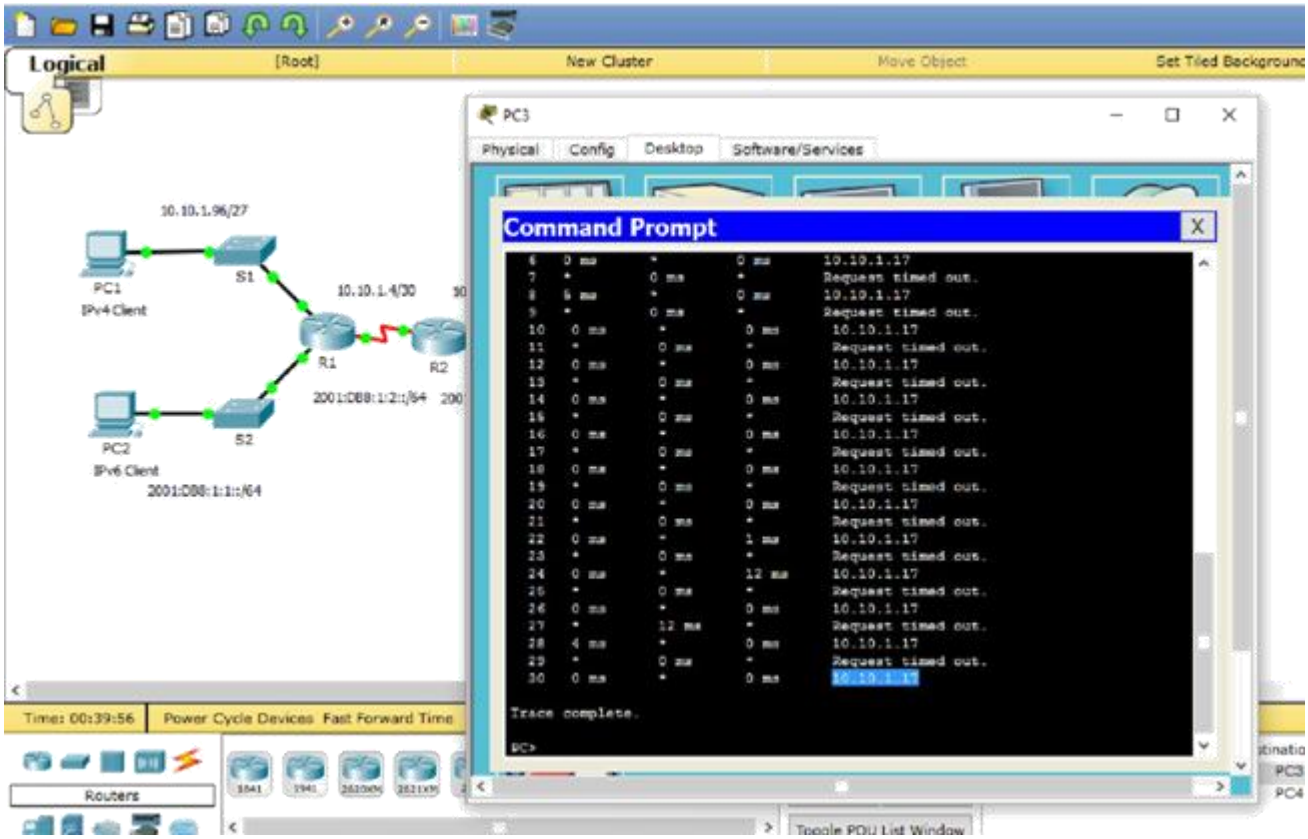


Paso 2: Localice el origen de la falla de conectividad.

a. Desde la **PC1**, introduzca el comando necesario para rastrear la ruta a la **PC3**. ¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.97



b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.



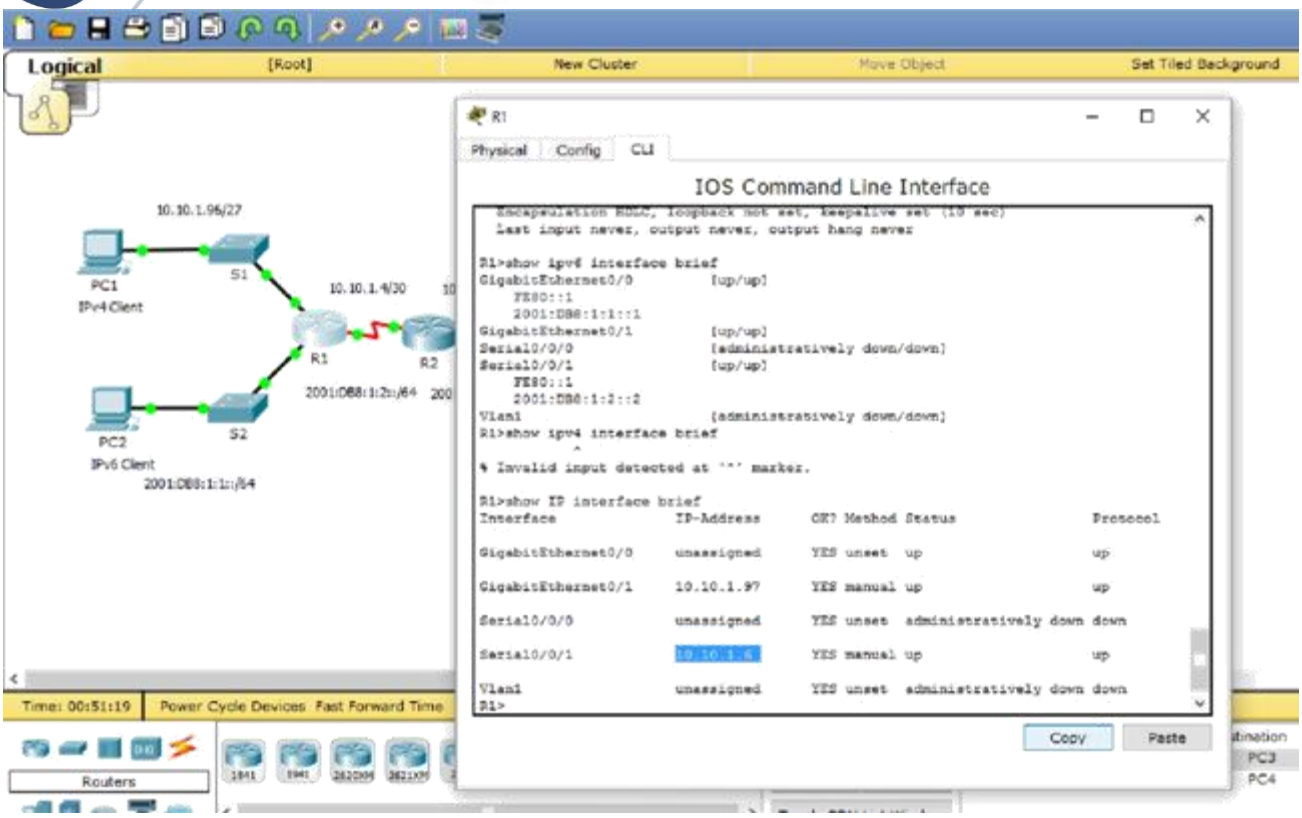
c. Desde la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**. ¿Cuál es la última

d. dirección IPv4 correcta que alcanzó? 10.10.1.17

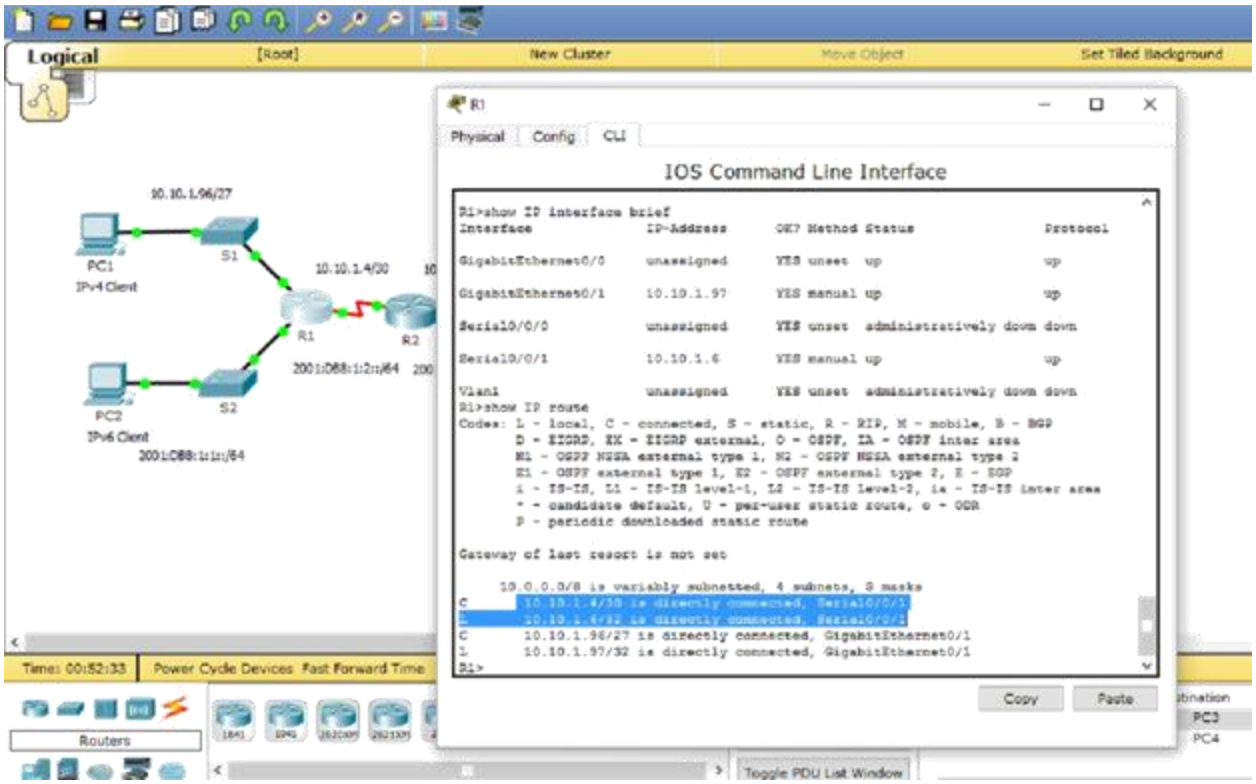
e. Introduzca **Ctrl**+**C** para detener el rastreo.

f. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **ENTRAR** e inicie sesión en el router.

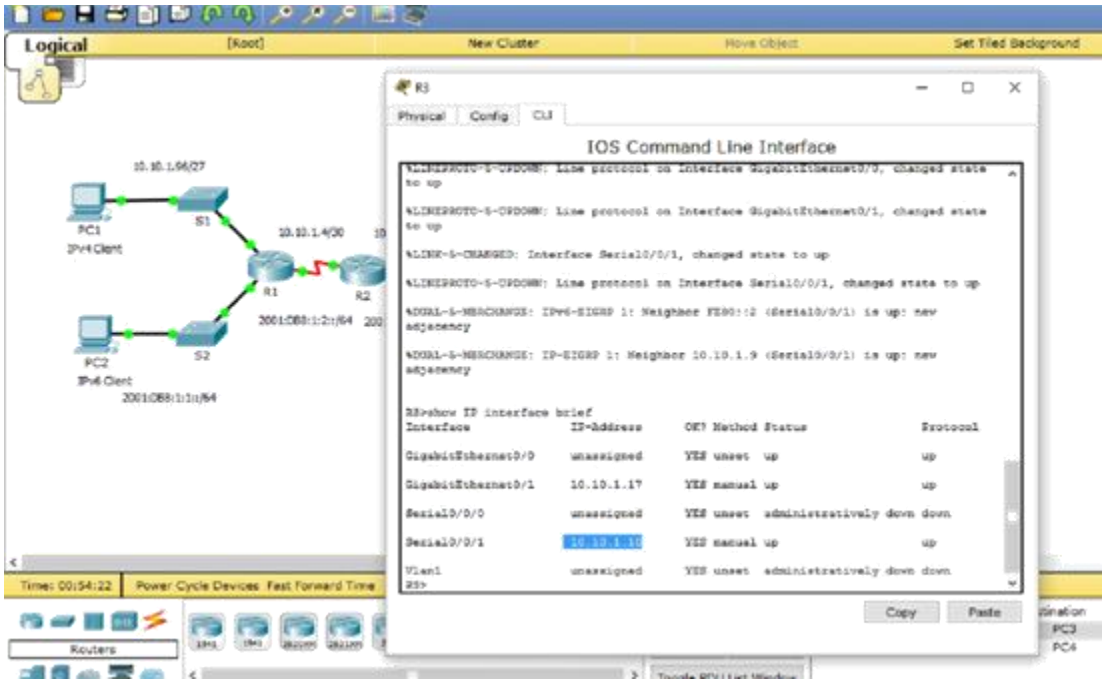
g. Introduzca el comando **show ip interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv4 en el router. Una se debió haber registrado en el paso 2a. ¿Cuál es la otra? 10.10.1.6

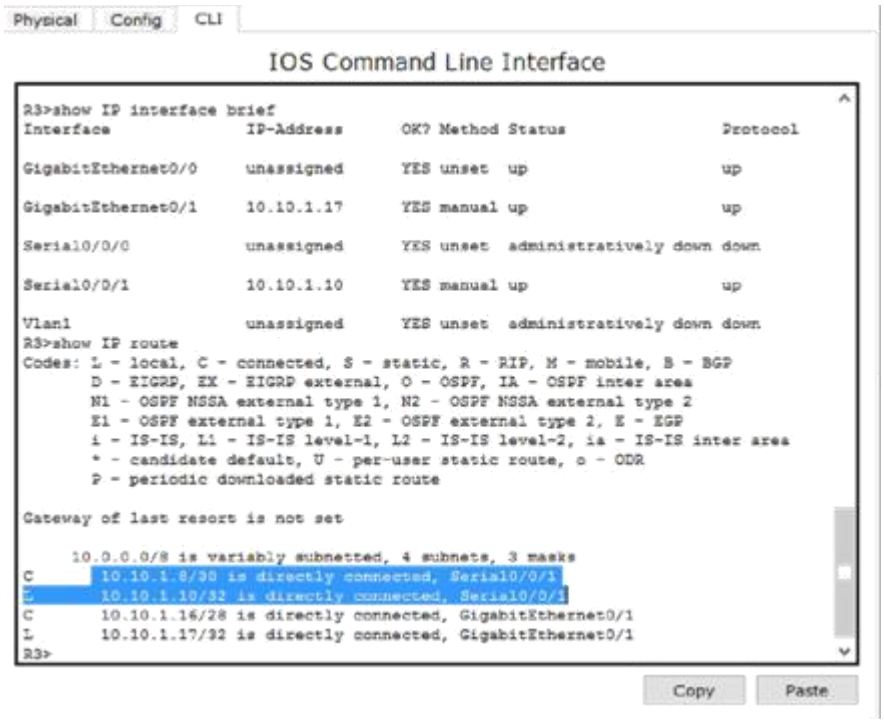


g. Introduzca el comando **show ip route** para obtener una lista de las redes a las que está conectado el router. Observe que hay dos redes conectadas a la interfaz **Serial0/0/1**. ¿Cuáles son? 10.10.1.6/32, 10.10.1.4/30



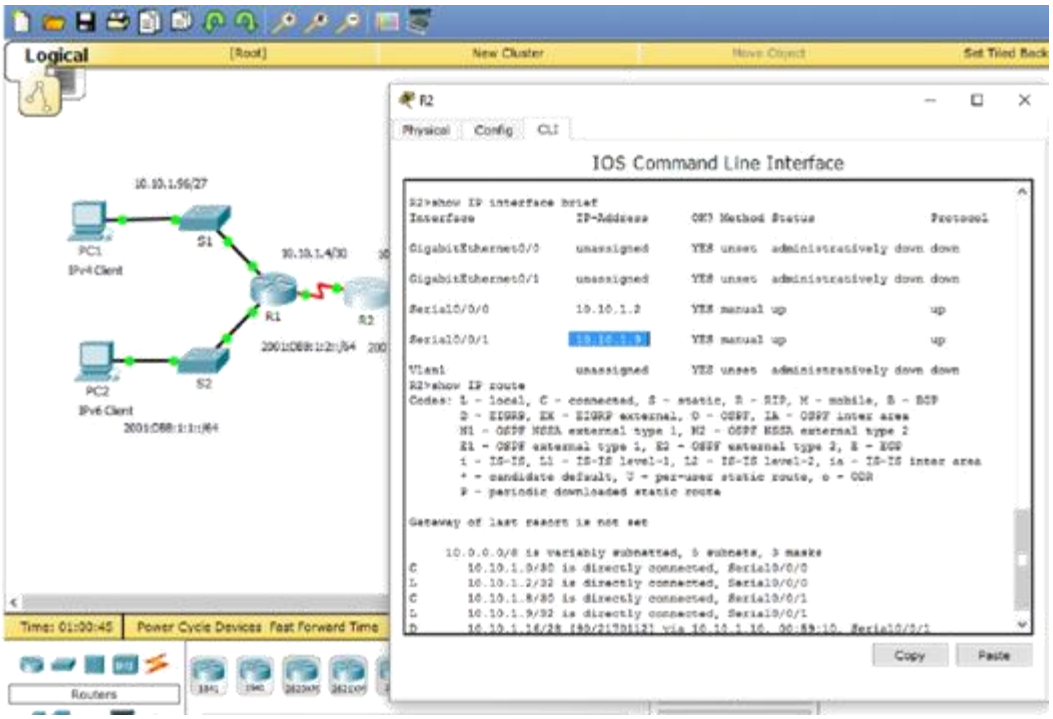
h. Repita los pasos 2e a 2g con el **R3** y escriba las respuestas aquí. 10.10.1.10, 10.10.1.8/30, 10.10.1.10/32





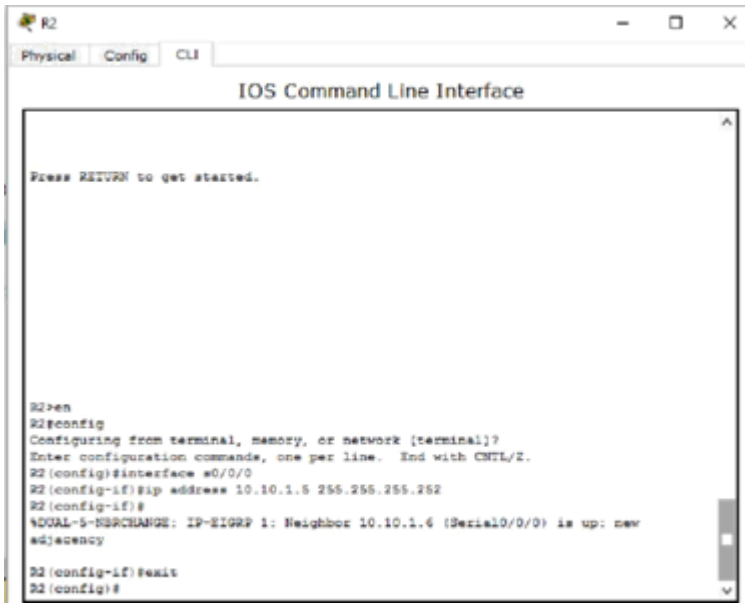
Observe cómo cambia la interfaz serial para el R3.

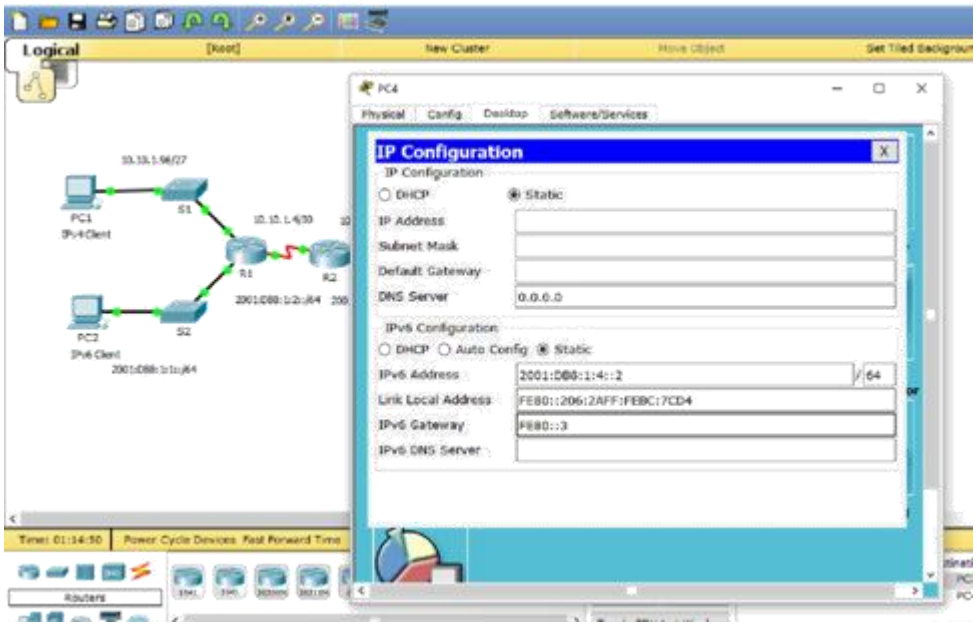
h. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.



Paso 3: Proponga una solución para resolver el problema. a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error?
La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.

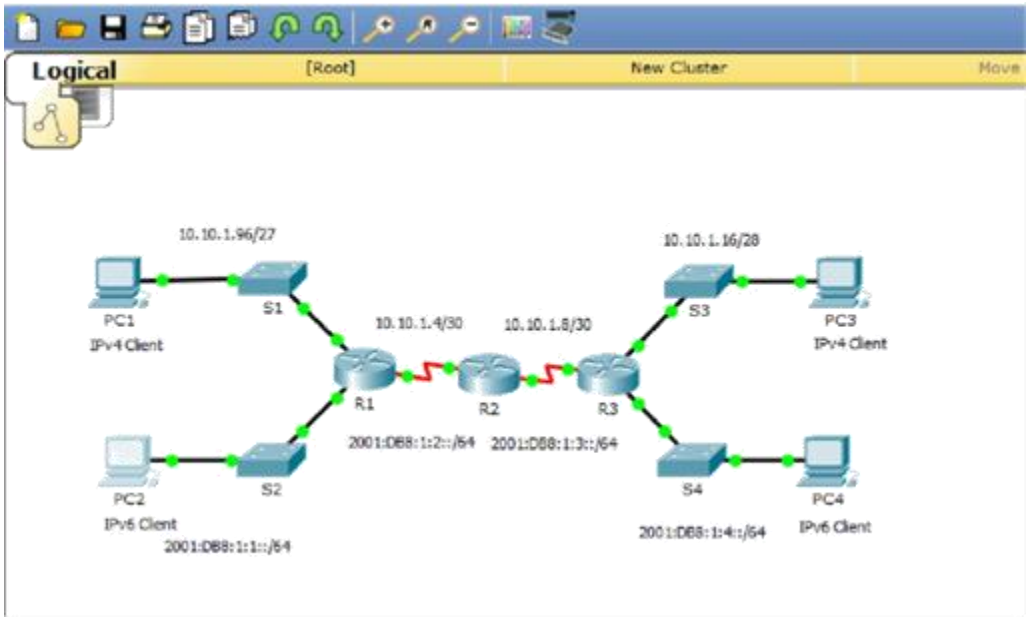
b. ¿Qué solución propondría para corregir el problema? Configurar la dirección IP correcta en la interfaz Serial 0/0/0 del R2 (10.10.1.5).





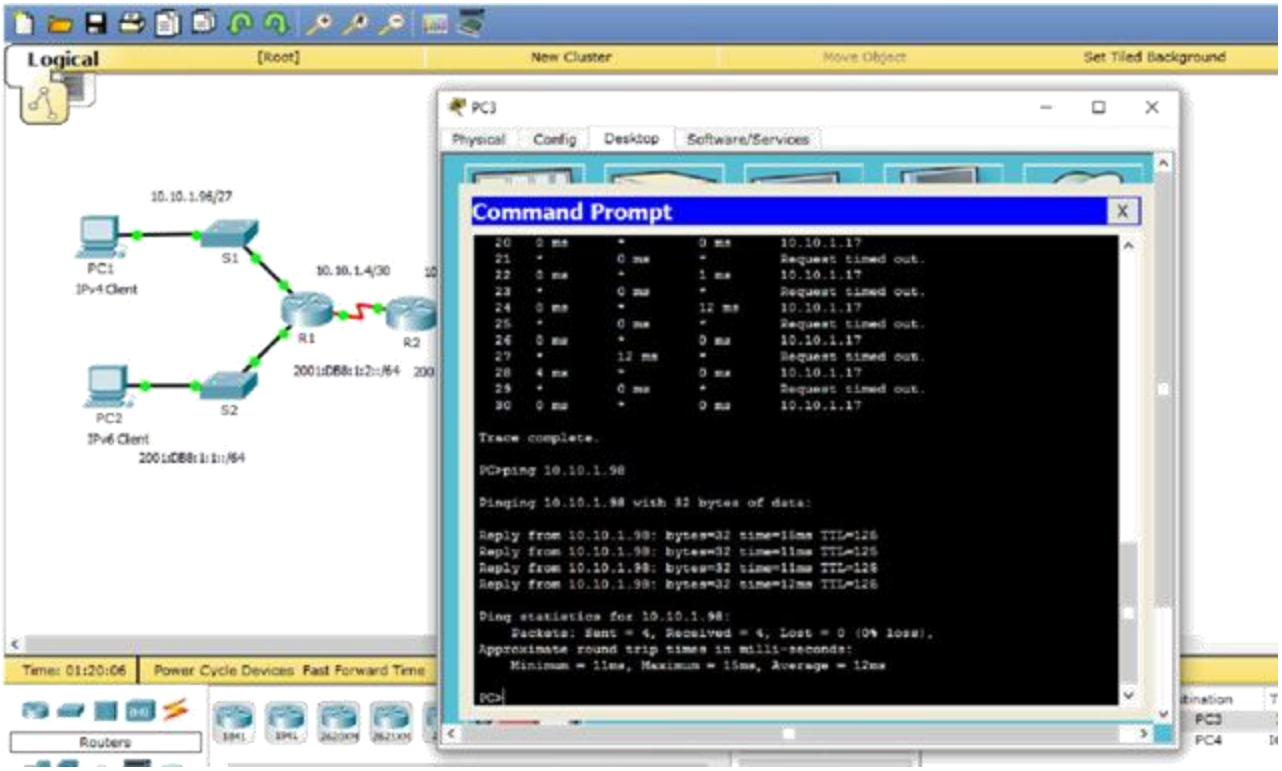
Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

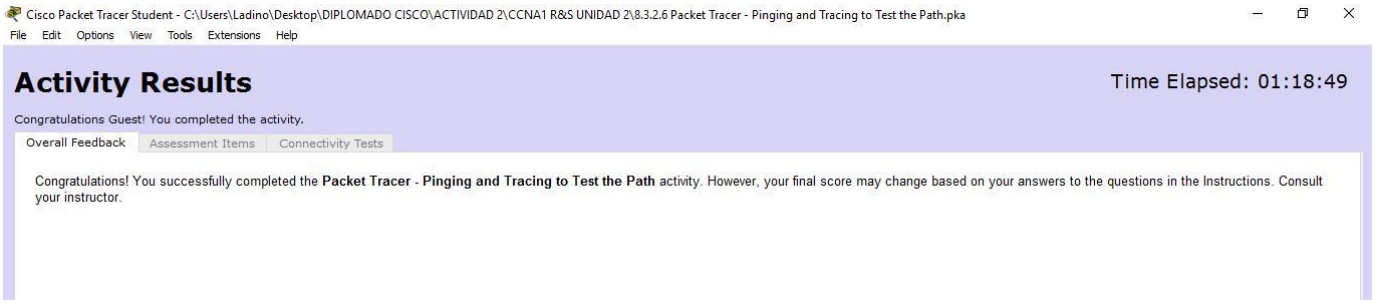


Paso 5: Verifique que la conectividad esté restaurada. a. Desde la **PC1**, pruebe la conectividad a la **PC3**.

b. Desde la **PC3**, pruebe la conectividad a la **PC1**. ¿Se resolvió el problema? Sí



Paso 6: Documentar la solución.



Ejercicio 8.3.2.8: Resolución de problemas de direccionamiento IPv4 e IPv6

Topología

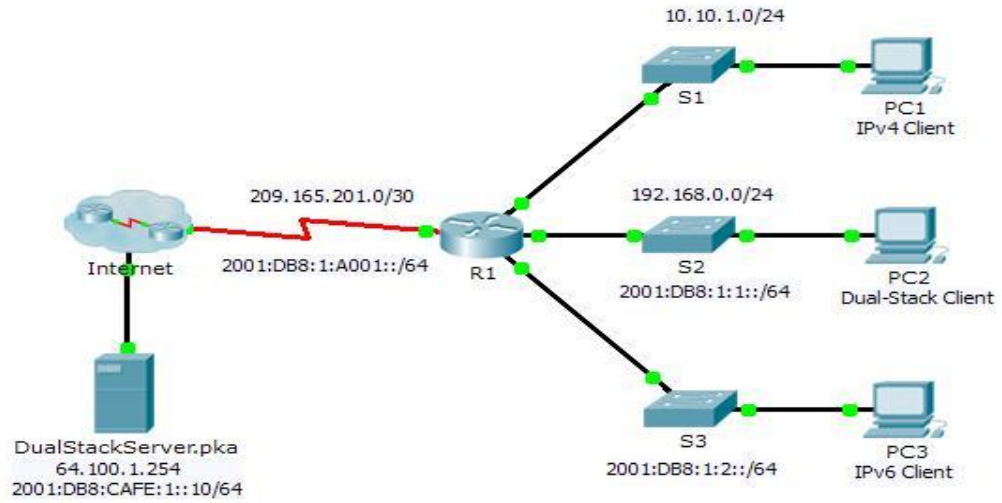


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	10.10.1.1	255.255.255.0	No aplicable
	Ga0/1	192.168.0.1	255.255.255.0	No aplicable
		2001:DB8:1:1::1/64		No aplicable
	G0/2	2001:DB8:1:2::1/64		No aplicable
	S0/0/0	209.165.201.2	255.255.255.252	No aplicable
		2001:DB8:1:A001::2/64		No aplicable
	Link-local	FE80::1		No aplicable
Servidor dual-stack	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1

		2001:DB8:1:1::2/64	FE80::1
PC3	NIC	2001:DB8:1:2::2/64	FE80::1

Objetivos

Parte 1: Resolver el primer problema

Parte 2: Resolver el segundo problema

Parte 3: Resolver el tercer problema

Situación

Usted es un técnico de red que trabaja para una compañía que decidió migrar de IPv4 a IPv6. Mientras tanto, debe admitir ambos protocolos (dual-stack). Tres compañeros de trabajo llamaron al soporte técnico para resolver algunos problemas, pero no recibieron suficiente asistencia. El soporte técnico le elevó el problema a usted, un técnico de soporte de nivel 2. Su trabajo es localizar el origen de los problemas e implementar las soluciones adecuadas.

Parte 1: Resolver el primer problema

Un cliente que usa la **PC1** se queja de que no puede acceder a la página Web **dualstackserver.pka**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico

Identificador de cliente: PC1

Problema: No puede acceder a la página Web dualstackserver.pka.

Información detallada sobre el problema

Prueba: ¿Tiene la PC una dirección IP cuando se utiliza **ipconfig**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando **ping**?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando **tracert**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el servidor mediante **nslookup**?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Considerar las causas probables de la falla

- Observe las pruebas que se realizaron. De ser posible, analice con sus colegas técnicos de red (compañeros de curso) las situaciones que podrían ser la causa de este problema.
- Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

Haga una lista de factores que se podrían cambiar para solucionar este problema. Comience con la solución que tenga más posibilidades de funcionar.

Paso 4: Implemente el plan.

Pruebe la solución más probable de la lista. Si ya se probó, pase a la siguiente solución.

Paso 5: Verificar que la solución haya resuelto el problema

i. Repita las pruebas de la solicitud de soporte técnico. ¿Se solucionó el problema?

j. Si el problema persiste, revierta el cambio en caso de no estar seguro de que sea correcto y vuelva al paso 4.

Paso 6: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.
La dirección DNS IPv4 de la PC1 es incorrecta.

Parte 2: Resolver el segundo el problema

Un cliente que usa la PC2 se queja de que no puede acceder a los archivos ubicados en **DualStackServer.pka** en 2001:DB8:CAFE:1::10.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico

Identificador de cliente: PC2

Problema: No puede acceder al servicio FTP de 2001:DB8:CAFE:1:10.

Información detallada sobre el problema

Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza **ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando **ping**?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando **tracert**?	No
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.
La dirección de gateway IPv6 de DualStackServer.pka es incorrecta

Parte 3: Resolver el tercer problema

Un cliente que usa la **PC1** se queja de que no se puede comunicar con la **PC2**.

Paso 1: Verificar una solicitud detallada de soporte técnico.

El soporte técnico recopiló la siguiente información del usuario por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC3	
Problema: No se puede comunicar con la PC2.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IP cuando se utiliza **ipconfig**?	Sí
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza **ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv4 mediante **ping**?	No
Prueba: ¿Puede la PC ponerse en contacto con su gateway IPv6 mediante **ping**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv4 mediante **tracert**?	No
Prueba: ¿Puede la PC ponerse en contacto con el cliente IPv6 mediante **tracert**?	Sí
Resolución: Elevar al soporte de nivel 2.	

Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

Paso 3: Documentar la solución.

Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.

La dirección de gateway IPv4 de la PC2 es incorrecta.

Ejercicio 8.4.1.2: Reto de habilidades de integración.

Topología

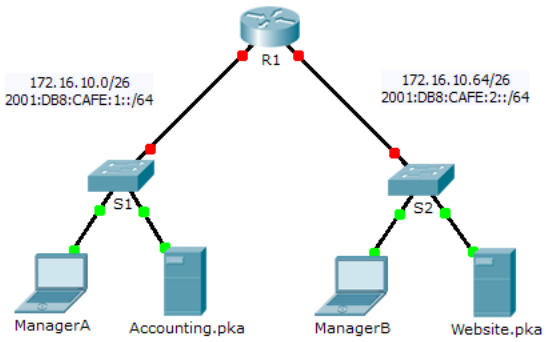


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4 / Dirección/Prefijo IPv6	Máscara de	Gateway predeterminado
R1	G0/0	172.16.10.1	255.255.255.192	No aplicable
		2001:DB8:CAFE:1::1/64		No aplicable
	G0/1	172.16.10.65	255.255.255.192	No aplicable
		2001:DB8:CAFE:2::1/64		No aplicable
	Link-local	FE80::1		No aplicable
S1	VLAN1	172.16.10.62	255.255.255.192	172.16.10.1
S2	VLAN1	172.16.10.126	255.255.255.192	172.16.10.65
ManagerA	NIC	172.16.10.3	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::3/64		FE80::1
Accounting.pka	NIC	172.16.10.2	255.255.255.192	172.16.10.1
		2001:DB8:CAFE:1::2/64		FE80::1
ManagerB	NIC	172.16.10.67	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::3/64		FE80::1
Website.pka	NIC	172.16.10.66	255.255.255.192	172.16.10.65
		2001:DB8:CAFE:2::2/64		FE80::1

Situación

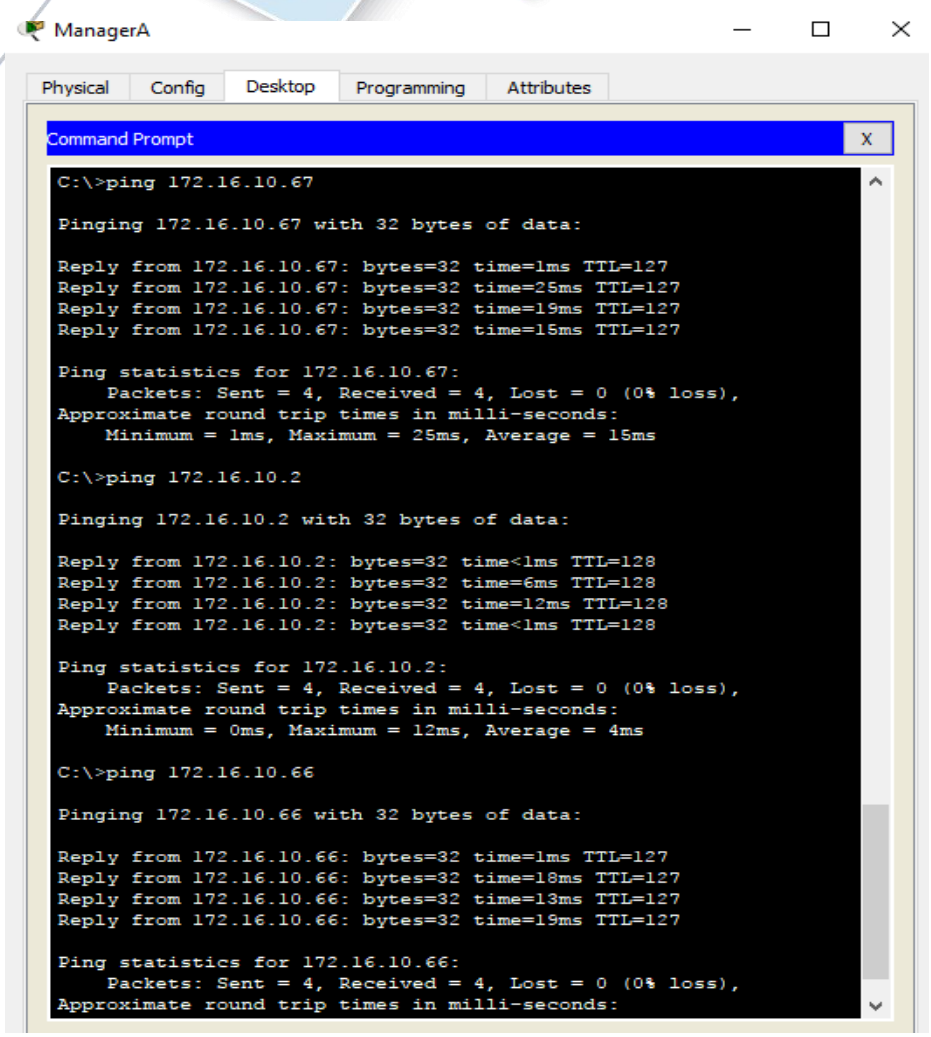
Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el resto del esquema de direccionamiento de acuerdo con la tabla de direccionamiento abreviada y verificar la conectividad.

Requisitos

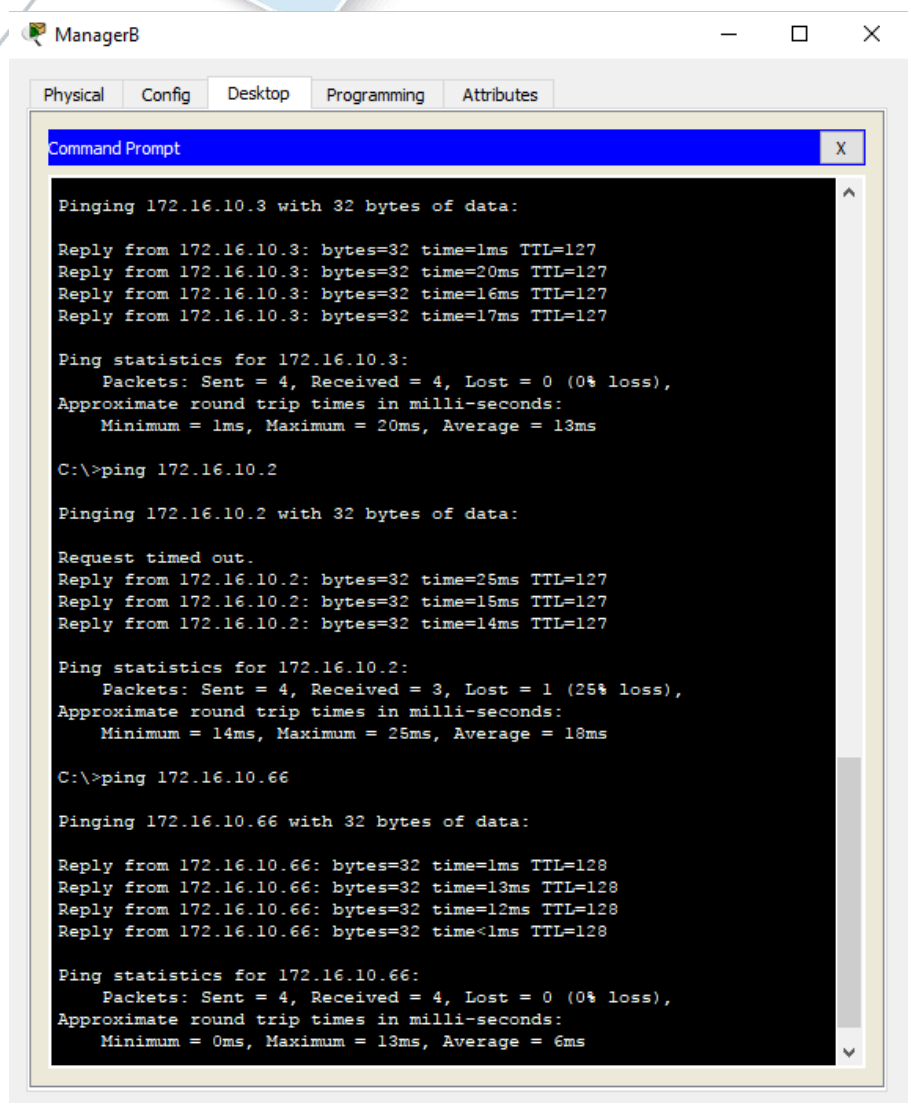
- Complete el registro de la **tabla de direccionamiento**.
- Configure direccionamiento IPv4 e IPv6 en el **R1**.
- Configure direccionamiento IPv4 en el **S1**. El **S2** ya está configurado.
- Configure direccionamiento IPv4 e IPv6 en **ManagerA**. El resto de los clientes ya están configurados.
- Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios Web en **Accounting.pka** y **Website.pka**.

Verificación de conectividad:

- Ping desde ManagerA hacia ManagerB (172.16.10.67), Accounting.pka (172.16.10.2) y Website.pka (172.16.10.66):

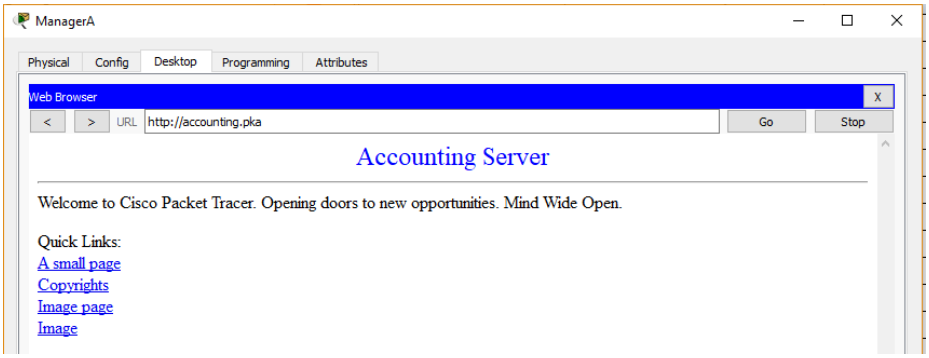


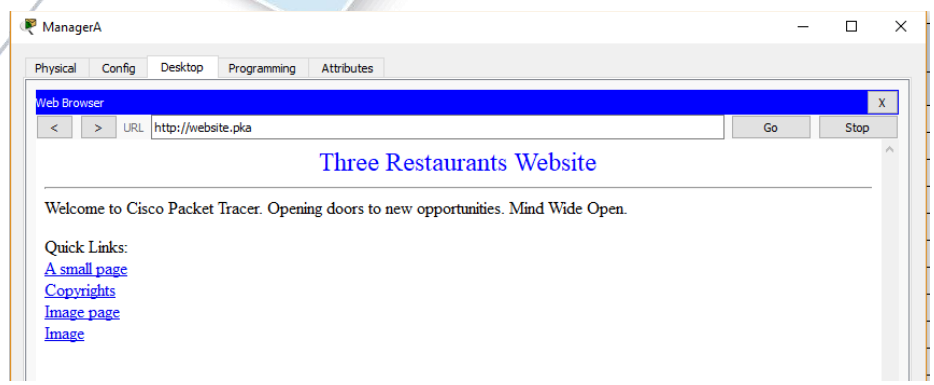
- Ping desde ManagerB hacia ManagerA (172.16.10.3), Accounting.pka (172.16.10.2) y Website.pka (172.16.10.66):



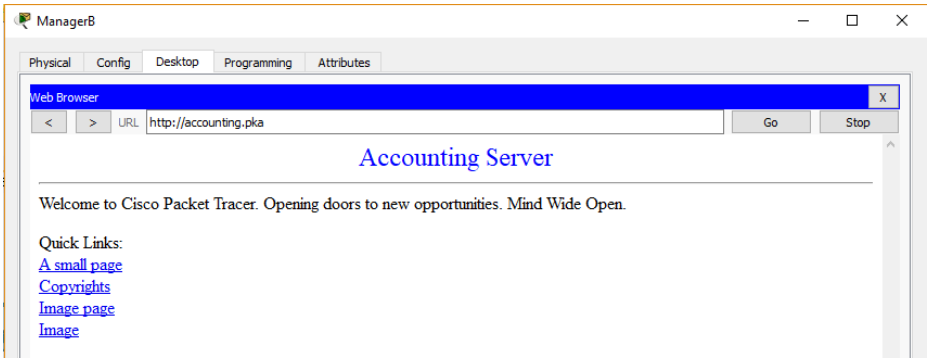
Accediendo a los sitios Web:

- Desde ManagerA

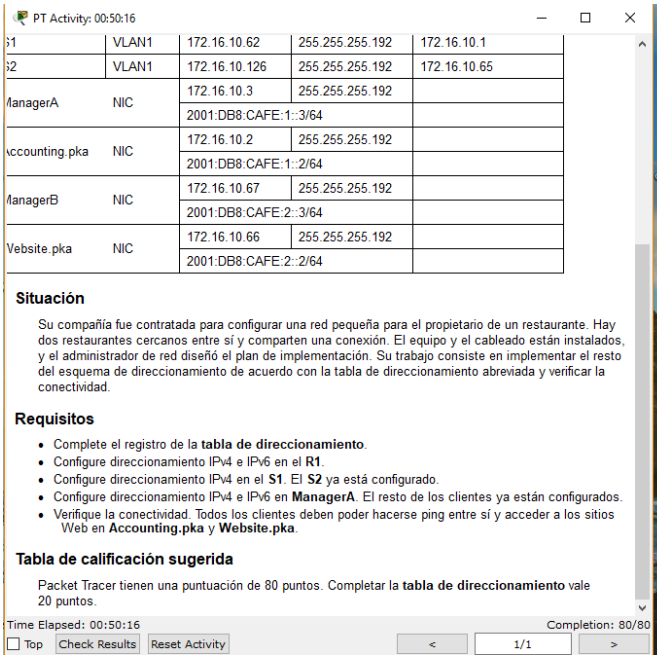


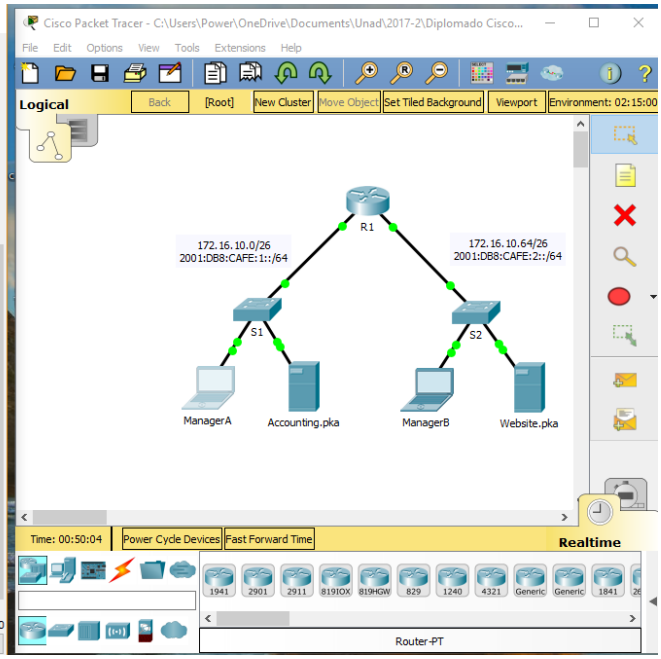


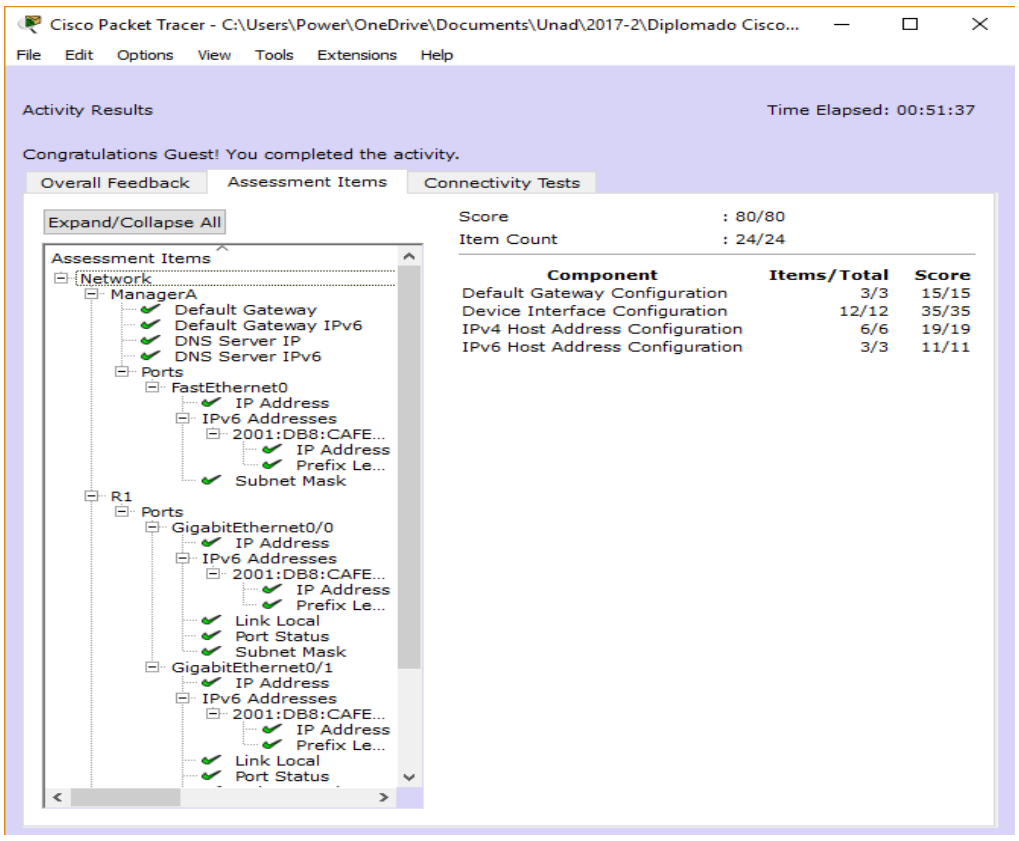
- Desde ManagerB



Resultados:


PT Activity: 00:50:16
VLAN1 172.16.10.62 255.255.255.192 172.16.10.1
VLAN1 172.16.10.126 255.255.255.192 172.16.10.65
NIC 172.16.10.3 255.255.255.192
2001:DB8:CAFE:1::3/64
NIC 172.16.10.2 255.255.255.192
2001:DB8:CAFE:1::2/64
NIC 172.16.10.67 255.255.255.192
2001:DB8:CAFE:2::3/64
NIC 172.16.10.66 255.255.255.192
2001:DB8:CAFE:2::2/64
Situación
Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el resto del esquema de direccionamiento de acuerdo con la tabla de direccionamiento abreviada y verificar la conectividad.
Requisitos
Complete el registro de la tabla de direccionamiento.
Configure direccionamiento IPv4 e IPv6 en el R1.
Configure direccionamiento IPv4 en el S1. El S2 ya está configurado.
Configure direccionamiento IPv4 e IPv6 en ManagerA. El resto de los clientes ya están configurados.
Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios Web en Accounting.pka y Website.pka.
Tabla de calificación sugerida
Packet Tracer tienen una puntuación de 80 puntos. Completar la tabla de direccionamiento vale 20 puntos.
Time Elapsed: 00:50:16
Completion: 80/80
Top
Check Results
Reset Activity
1/1


Cisco Packet Tracer - C:\Users\Power\OneDrive\Documents\Unad\2017-2\Diplomado Cisco...
Logical
R1
172.16.10.0/26
2001:DB8:CAFE:1::/64
172.16.10.64/26
2001:DB8:CAFE:2::/64
S1
S2
ManagerA
Accounting.pka
ManagerB
Website.pka
Time: 00:50:04
Power Cycle Devices
Fast Forward Time
Realtime
Router-PT


Cisco Packet Tracer - C:\Users\Power\OneDrive\Documents\Unad\2017-2\Diplomado Cisco...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:51:37
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Network
ManagerA
Default Gateway
Default Gateway IPv6
DNS Server IP
DNS Server IPv6
Ports
FastEthernet0
IP Address
IPv6 Addresses
2001:DB8:CAFE...
IP Address
Prefix Le...
Subnet Mask
R1
Ports
GigabitEthernet0/0
IP Address
IPv6 Addresses
2001:DB8:CAFE...
IP Address
Prefix Le...
Link Local
Port Status
Subnet Mask
GigabitEthernet0/1
IP Address
IPv6 Addresses
2001:DB8:CAFE...
IP Address
Prefix Le...
Link Local
Port Status
Score : 80/80
Item Count : 24/24
Component Items/Total Score
Default Gateway Configuration 3/3 15/15
Device Interface Configuration 12/12 35/35
IPv4 Host Address Configuration 6/6 19/19
IPv6 Host Address Configuration 3/3 11/11

Ejercicio 9.4.1.6: Situación de división en subredes 1.

Topología

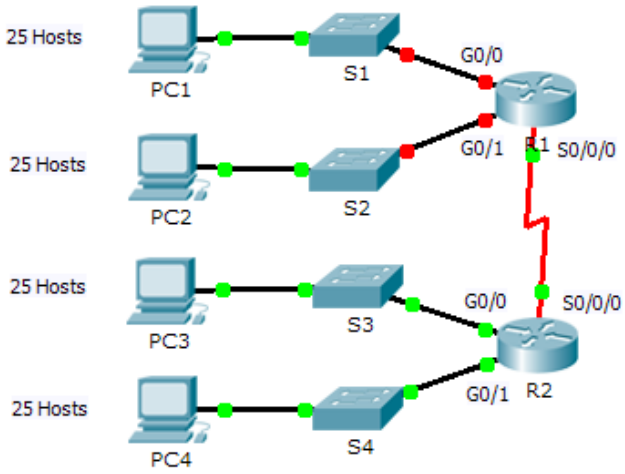


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de	Gateway predeterminad
R1	G0/0	192.168.100.1	255.255.255.22	No aplicable
	G0/1	192.168.100.33	255.255.255.22	No aplicable
	S0/0/0	192.168.100.129	255.255.255.22	No aplicable
R2	G0/0	192.168.100.65	255.255.255.22	No aplicable
	G0/1	192.168.100.97	255.255.255.22	No aplicable
	S0/0/0	192.168.100.158	255.255.255.22	No aplicable
S1	VLAN 1	192.168.100.2	255.255.255.22	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.22	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.22	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.22	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.22	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.22	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.22	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.22	192.168.100.97

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 192.168.100.0/24 para que cree una subred y proporcione el direccionamiento IP para la red que se muestra en la topología. Cada LAN de la red necesita espacio suficiente para alojar, como mínimo, 25 direcciones para dispositivos finales, el switch y el router. La conexión entre las redes R1 y R2 requiere una dirección IP para cada extremo del enlace.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida en subredes la red 192.168.100.0/24 en la cantidad adecuada de subredes.

a. Según la topología, ¿cuántas subredes se necesitan?
5 subredes

b. ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología?
3 bit

c. ¿Cuántas subredes se crean?
8 subredes

e. ¿Cuántos hosts utilizables se crean por subred?

30 host

Nota: si su respuesta es menor que los 25 hosts requeridos, tomó prestados demasiados bits. e. Calcule el valor binario para las primeras cinco subredes. La primera subred ya se muestra.

```
Net 0: 192. 168. 100.  0   0   0   0   0   0   0   0

Net 1: 192. 168. 100. ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 192. 168. 100.  0   0   1   0   0   0   0   0

Net 2: 192. 168. 100. ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 192. 168. 100.  0   1   0   0   0   0   0   0
```

Net 3: 192. 168. 100. ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 192. 168. 100. 0 1 1 0 0 0 0 0

Net 4: 192. 168. 100. ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 192. 168. 100. 1 0 0 0 0 0 0 0

f. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1 1 1 0 0 0 0 0
255. 255. 255. _____
255. 255. 255. 224

g. Complete la **tabla de subredes** con el valor decimal de todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas.

Tabla de subredes

Número de	Dirección de	Primera dirección de host	Última dirección de host utilizable	Dirección de
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255
8				
9				
10				

Paso 2: Asigne las subredes a la red que se muestra en la topología.

a. Asigne la subred 0 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R1: 192.168.100.0 /27

```
R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ip address 192.168.100.1 255.255.255.224
R1(config-if)#no shut
```

b. Asigne la subred 1 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R1: 192.168.100.32 /27

```
R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.100.33 255.255.255.224
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R1(config-if)#int s0/0/0
R1(config-if)#ip address 192.168.100.129 255.255.255.252
R1(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.100.158 (Serial0/0/0) is down: interface down

R1(config-if)#no shut
```

c. Asigne la subred 2 a la LAN conectada a la interfaz GigabitEthernet 0/0 del R2: 192.168.100.64 /27

d. Asigne la subred 3 a la LAN conectada a la interfaz GigabitEthernet 0/1 del R2: 192.168.100.96 /27

e. Asigne la subred 4 al enlace WAN entre el R1 y el R2: 192.168.100.128 /27

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

a. Asigne las primeras direcciones IP utilizables al R1 para los dos enlaces LAN y el enlace WAN.

ok

b. Asigne las primeras direcciones IP utilizables al R2 para los enlaces LAN. Asigne la última dirección IP
utilizable para el enlace WAN.

ok

d. Asigne las segundas direcciones IP utilizables a los switches.

Al switch 3

```
S3>enable
S3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int vlan 1
S3(config-if)#ip address 192.168.100.66 255.255.255.224
S3(config-if)#no shut

S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S3(config-if)#exit
```

e. Asigne las últimas direcciones IP utilizables a los hosts.

Ok

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

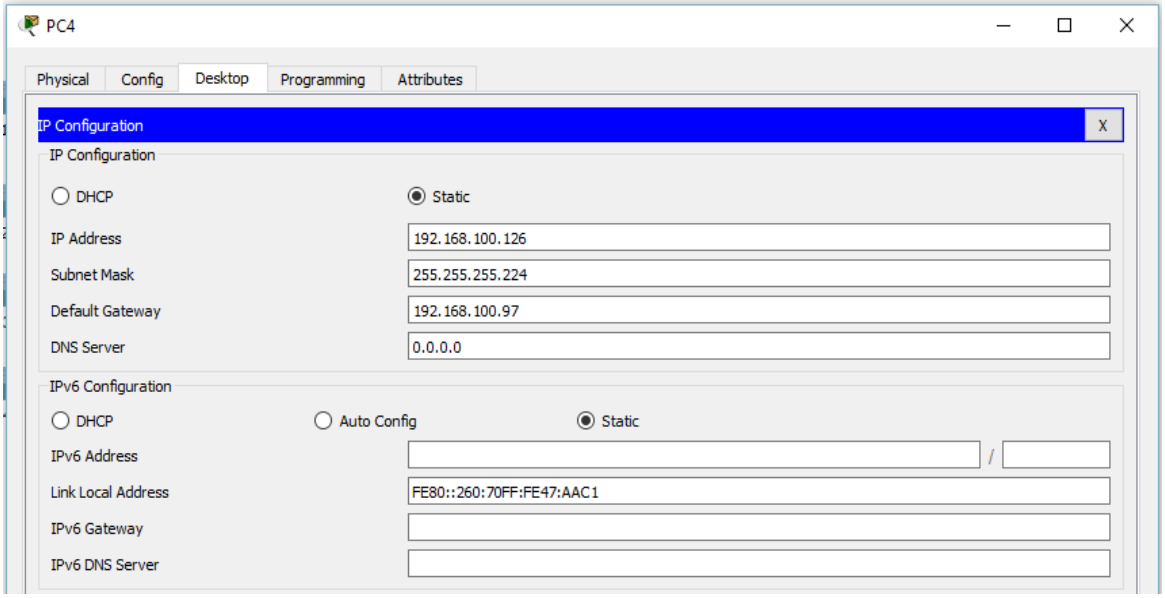
Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1

Ok

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

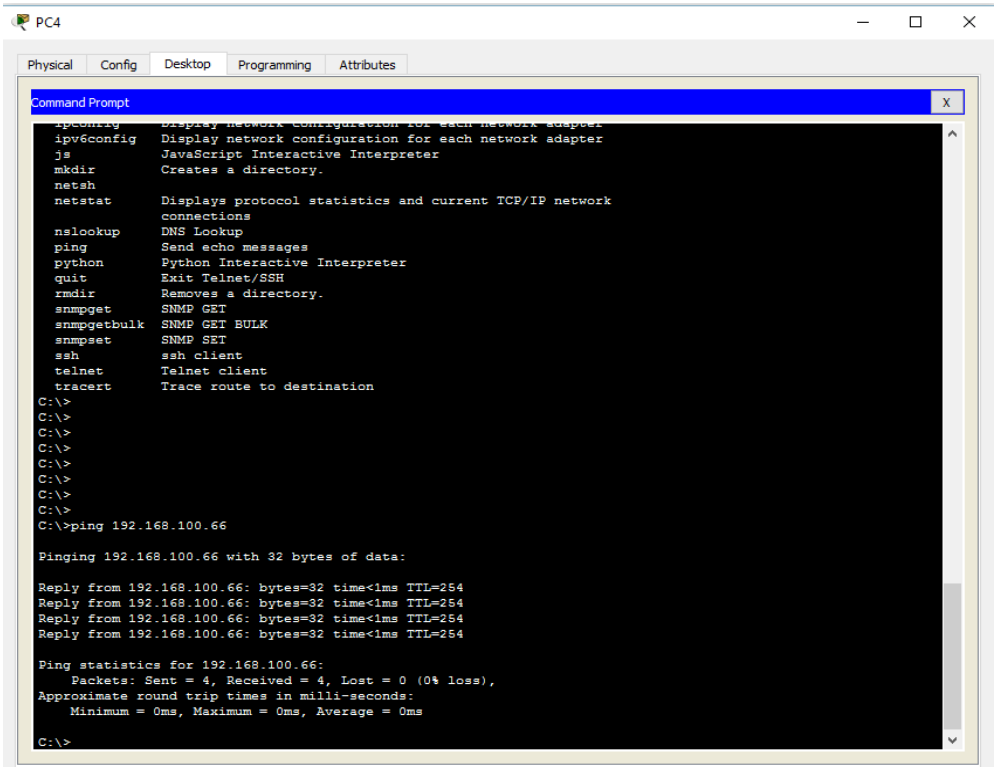
```
S3(config)#ip default-gateway
% Incomplete command.
S3(config)#ip default-gateway 192.168.100.65
S3(config)#
```

Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.



Ejercicio 9.1.4.7: Situación de división en subredes 2.

Topología

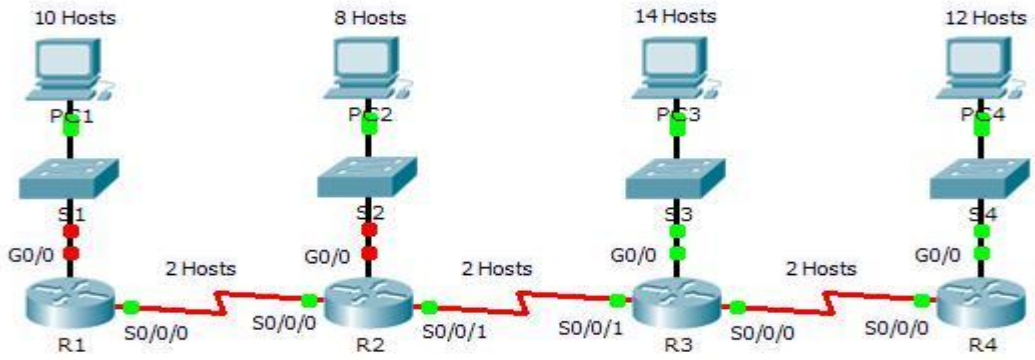


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.1.1	255.255.255.240	No aplicable
	S0/0/0	172.31.1.65	255.255.255.240	No aplicable
R2	G0/0	172.31.1.17	255.255.255.240	No aplicable
	S0/0/0	172.31.1.78	255.255.255.240	No aplicable
	S0/0/1	172.31.1.81	255.255.255.240	No aplicable
R3	G0/0	172.31.1.33	255.255.255.240	No aplicable
	S0/0/0	172.31.1.97	255.255.255.240	No aplicable
	S0/0/1	172.31.1.94	255.255.255.240	No aplicable
R4	G0/0	172.31.1.49	255.255.255.240	No aplicable
	S0/0/0	172.31.1.110	255.255.255.240	No aplicable
S1	VLAN 1	172.31.1.2	255.255.255.240	172.31.1.1
S2	VLAN 1	172.31.1.18	255.255.255.240	172.31.1.17
S3	VLAN 1	172.31.1.34	255.255.255.240	172.31.1.33
S4	VLAN 1	172.31.1.50	255.255.255.240	172.31.1.49
PC1	NIC	172.31.1.14	255.255.255.240	172.31.1.1

		172.31.1.30	255.255.255.240	172.31.1.17
PC3	NIC	172.31.1.46	255.255.255.240	172.31.1.33
PC4	NIC	172.31.1.62	255.255.255.240	172.31.1.49

Objetivos

Parte 1: Diseñar un esquema de direccionamiento IP

Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

Situación

En esta actividad, se le asigna la dirección de red 172.31.1.0 /24 para que la divida en subredes y proporcione direccionamiento IP para la red que se muestra en la topología. Las direcciones de host requeridas para cada enlace WAN y LAN se muestran en la topología.

Parte 1: Diseñar un esquema de direccionamiento IP

Paso 1: Divida la red 172.31.1.0/24 en subredes de acuerdo con la cantidad máxima de hosts que requiere la subred más extensa.

a. Según la topología, ¿cuántas subredes se necesitan?
R: 7

b. ¿Cuántos bits se deben tomar prestados para admitir la cantidad de subredes en la tabla de topología?
R: 4

c. ¿Cuántas subredes se crean?
R: 16

d. ¿Cuántas direcciones de host utilizables se crean por subred?
R: 14

e. **Nota:** si su respuesta es menor que el máximo de 14 hosts que requiere la LAN del R3, tomó prestados demasiados bits.

f. Calcule el valor binario para las primeras cinco subredes. La subred cero ya se muestra.

```
Net 0: 172 .  31 . 1 .   0   0   0   0   0   0   0   0

Net 1: 172 .  31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 1: 172 .  31 . 1 .   0   0   0   1   0   0   0   0
```

```
Net 2: 172 .  31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 2: 172 .  31 . 1 .   0   0   1   0   0   0   0   0

Net 3: 172  . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 3: 172  . 31 . 1 .   0   0   1   1   0   0   0   0

Net 4: 172  . 31 . 1 . ___ ___ ___ ___ ___ ___ ___ ___
Net 4: 172  . 31 . 1 .   0   1   0   0   0   0   0   0
```

k. Calcule el valor binario y el valor decimal de la nueva máscara de subred.

```
 11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.111111111. 1   1   1   1   0   0   0   0

    255  .   255  .   255  . ______
    255  .   255  .   255  . 240
```

g. Complete la **tabla de subredes** con todas las subredes disponibles, la primera y la última dirección de host utilizable y la dirección de broadcast. La primera subred ya se completó. Repita hasta que todas las direcciones estén en la lista.

Nota: es posible que no necesite utilizar todas las filas

Tabla de subredes

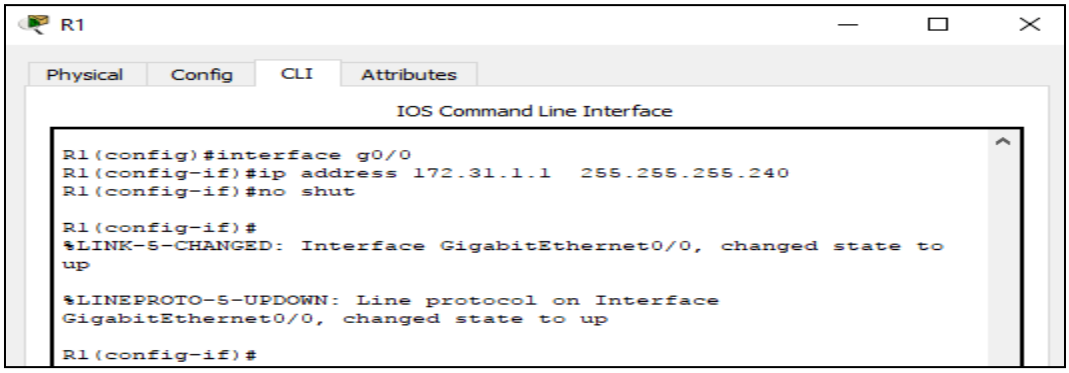
Número de subred	IP de subred	Primera IP de host utilizable	Última IP de host utilizable	Dirección de broadcast
0	172.31.1.0	172.31.1.1	172.31.1.14	172.16.1.15
1	172.31.1.16	172.31.1.17	172.31.1.30	172.31.1.31
2	172.31.1.32	172.31.1.33	172.31.1.46	172.31.1.47
3	172.31.1.48	172.31.1.49	172.31.1.62	172.31.1.63
4	172.31.1.64	172.31.1.65	172.31.1.78	172.31.1.79
5	172.31.1.80	172.31.1.81	172.31.1.94	172.31.1.95
6	172.31.1.96	172.31.1.97	172.31.1.110	172.31.1.111
7	172.31.1.112	172.31.1.113	172.31.1.126	172.31.1.127
8	172.31.1.128	172.31.1.129	172.31.1.142	172.31.1.143
9	172.31.1.144	172.31.1.145	172.31.1.158	172.31.1.159

10	172.31.1.160	172.31.1.161	172.31.1.174	172.31.1.175
11	172.31.1.176	172.31.1.177	172.31.1.190	172.31.1.191
12	172.31.1.192	172.31.1.193	172.31.1.206	172.31.1.207
13	172.31.1.208	172.31.1.209	172.31.1.222	172.31.1.223
14	172.31.1.224	172.31.1.225	172.31.1.238	172.31.1.239
15	172.31.1.240	172.31.1.241	172.31.1.254	172.31.1.255

Paso 2: Asigne las subredes a la red que se muestra en la topología.

Cuando asigne las subredes, tenga en cuenta que es necesario el enrutamiento para permitir que la información se envíe a través de la red.

f. Asigne la subred 0 a la LAN del R1:



g. Asigne la subred 1 a la LAN del R2:

```
R2>enable
R2#configure termi
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0
R2(config-if)#ip address 172.31.1.17 255.255.255.240
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

R2(config-if)#

h. Asigne la subred 2 a la LAN del R3
Ya ha sido asignada

i. Asigne la subred 3 a la LAN del R4:
Ya ha sido asignada

j. Asigne la subred 4 al enlace entre el R1 y el R2:
Ya ha sido asignada

```
R1>enable
R1#show run
Building configuration...

hostname R1
!
interface Serial0/0/0
ip address 172.31.1.65 255.255.255.240
clock rate 64000
!
end
```

R1#

k. Asigne la subred 5 al enlace entre el R2 y el R3:
Ya ha sido asignada

```
R2>enable
R2#show run
Building configuration...
interface Serial0/0/1
ip address 172.31.1.81 255.255.255.240
clock rate 2000000
!
end
```

R2#

l. Asigne la subred 6 al enlace entre el R3 y el R4:
Ya ha sido asignada

Paso 3: Documente el esquema de direccionamiento.

Complete la **tabla de direccionamiento** con las siguientes pautas:

f. Asigne las primeras direcciones IP utilizables a los routers para cada uno de los enlaces LAN.

g. Utilice el siguiente método para asignar las direcciones IP de los enlaces WAN:

Para el enlace WAN entre el R1 y el R2, asigne la primera dirección IP utilizable al R1 y la última dirección IP utilizable al R2.
Ya ha sido asignada

Para el enlace WAN entre el R2 y el R3, asigne la primera dirección IP utilizable al R2 y la última dirección IP utilizable al R3.
Ya ha sido asignada

Para el enlace WAN entre el R3 y el R4, asigne la primera dirección IP utilizable al R3 y la última dirección IP utilizable al R4.
Ya ha sido asignada

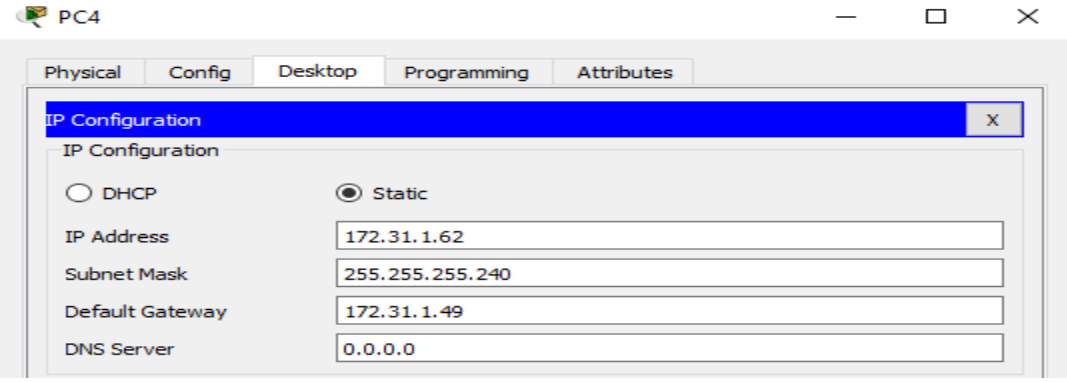
g. Asigne las segundas direcciones IP utilizables a los switches.

```
S3>enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface vlan 1
S3(config-if)#ip address 172.31.1.34 255.255.255.240
S3(config-if)#no shut

S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S3(config-if)#

Los demás switches ya han sido configurados

h. Asigne las últimas direcciones IP utilizables a los hosts.



Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1 y el R2

```
R1#show run
Building configuration...

Current configuration : 797 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
interface GigabitEthernet0/0
ip address 172.31.1.1 255.255.255.240
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.31.1.65 255.255.255.240
clock rate 64000
!
end
```

```
R1#
```

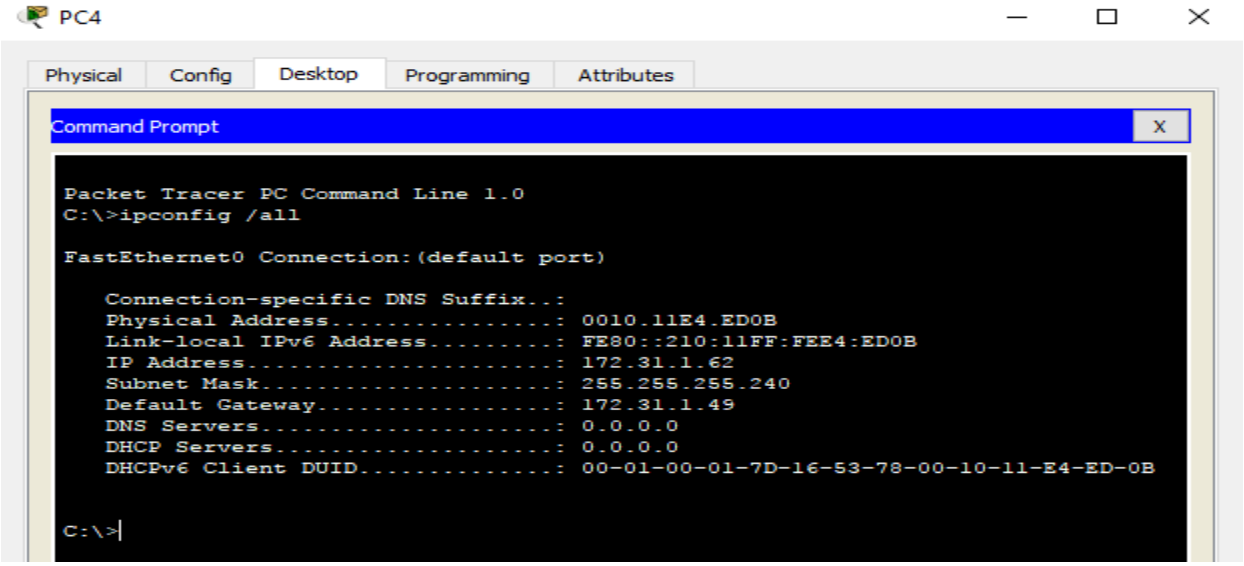
```
R2>enable
R2#show run
Building configuration...

Current configuration : 805 bytes
!
!
interface GigabitEthernet0/0
ip address 172.31.1.17 255.255.255.240
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.31.1.78 255.255.255.240
!
interface Serial0/0/1
ip address 172.31.1.81 255.255.255.240
clock rate 2000000
!
!
end

R2#
```

Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

```
S3#show run
Building configuration...

Current configuration : 1120 bytes
!
hostname S3
!
!
interface Vlan1
ip address 172.31.1.34 255.255.255.240
!
```

```
ip default-gateway 172.31.1.33
!
end

S3#
```

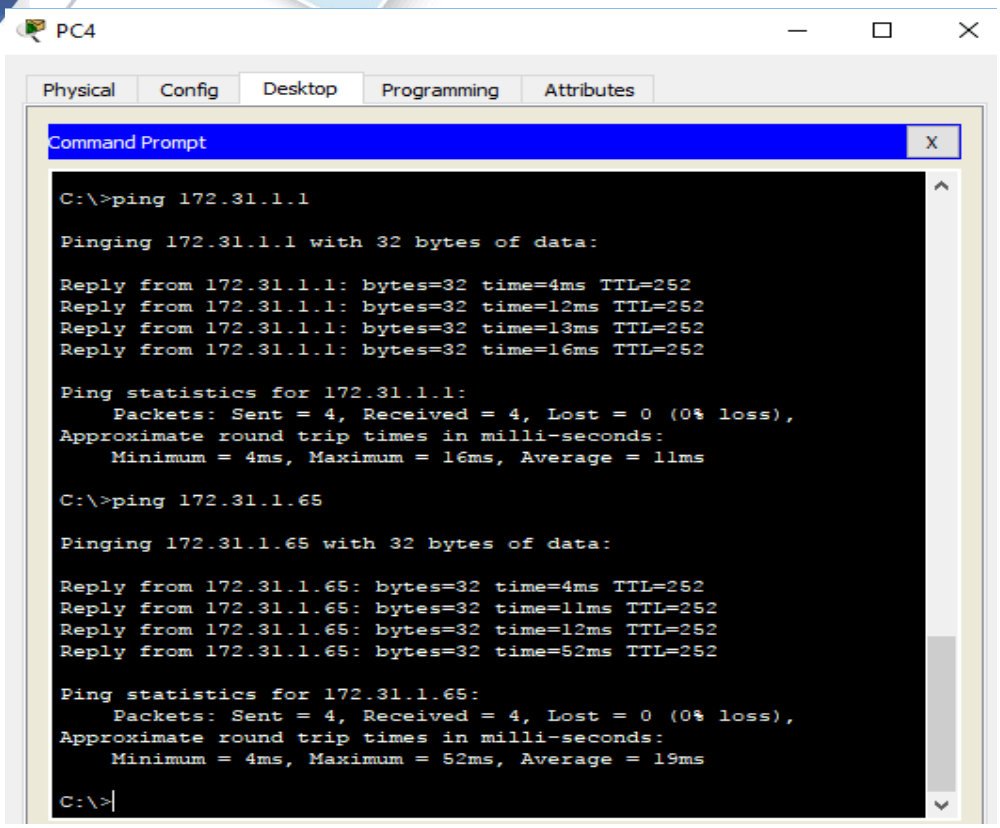
Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde el R1, el R2, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Ping desde el PC4 a R1



Ping desde el PC4 a R2

C:\>ping 172.31.1.17

Pinging 172.31.1.17 with 32 bytes of data:

Reply from 172.31.1.17: bytes=32 time=2ms TTL=253
Reply from 172.31.1.17: bytes=32 time=12ms TTL=253
Reply from 172.31.1.17: bytes=32 time=10ms TTL=253
Reply from 172.31.1.17: bytes=32 time=13ms TTL=253

Ping statistics for 172.31.1.17:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 9ms

C:\>ping 172.31.1.78

Pinging 172.31.1.78 with 32 bytes of data:

Reply from 172.31.1.78: bytes=32 time=3ms TTL=253

Reply from 172.31.1.78: bytes=32 time=19ms TTL=253
Reply from 172.31.1.78: bytes=32 time=11ms TTL=253
Reply from 172.31.1.78: bytes=32 time=13ms TTL=253

Ping statistics for 172.31.1.78:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 19ms, Average = 11ms

C:\>ping 172.31.1.81

Pinging 172.31.1.81 with 32 bytes of data:

Reply from 172.31.1.81: bytes=32 time=3ms TTL=253
Reply from 172.31.1.81: bytes=32 time=12ms TTL=253
Reply from 172.31.1.81: bytes=32 time=13ms TTL=253
Reply from 172.31.1.81: bytes=32 time=12ms TTL=253

Ping statistics for 172.31.1.81:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 13ms, Average = 10ms

C:\>

Ping desde el PC4 a R2

C:\>ping 172.31.1.33

Pinging 172.31.1.33 with 32 bytes of data:

Reply from 172.31.1.33: bytes=32 time=2ms TTL=254
Reply from 172.31.1.33: bytes=32 time=1ms TTL=254
Reply from 172.31.1.33: bytes=32 time=10ms TTL=254
Reply from 172.31.1.33: bytes=32 time=1ms TTL=254

Ping statistics for 172.31.1.33:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>ping 172.31.1.97

Pinging 172.31.1.97 with 32 bytes of data:

Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254
Reply from 172.31.1.97: bytes=32 time=1ms TTL=254

Ping statistics for 172.31.1.97:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 172.31.1.94

Pinging 172.31.1.94 with 32 bytes of data:

Reply from 172.31.1.94: bytes=32 time=1ms TTL=254
Reply from 172.31.1.94: bytes=32 time=4ms TTL=254
Reply from 172.31.1.94: bytes=32 time=2ms TTL=254
Reply from 172.31.1.94: bytes=32 time=2ms TTL=254

Ping statistics for 172.31.1.94:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>

Ping PC4 a S1

C:\>ping 172.31.1.2

Pinging 172.31.1.2 with 32 bytes of data:

Reply from 172.31.1.2: bytes=32 time=3ms TTL=251
Reply from 172.31.1.2: bytes=32 time=16ms TTL=251
Reply from 172.31.1.2: bytes=32 time=14ms TTL=251
Reply from 172.31.1.2: bytes=32 time=15ms TTL=251

Ping statistics for 172.31.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 16ms, Average = 12ms

C:\>

Ping PC4 a S2

```
C:\>ping 172.31.1.18

Pinging 172.31.1.18 with 32 bytes of data:

Reply from 172.31.1.18: bytes=32 time=3ms TTL=252
Reply from 172.31.1.18: bytes=32 time=13ms TTL=252
Reply from 172.31.1.18: bytes=32 time=16ms TTL=252
Reply from 172.31.1.18: bytes=32 time=13ms TTL=252

Ping statistics for 172.31.1.18:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 16ms, Average = 11ms
C:\>
```

Ping PC4 a S3

```
C:\>ping 172.31.1.34

Pinging 172.31.1.34 with 32 bytes of data:

Reply from 172.31.1.34: bytes=32 time=2ms TTL=253
Reply from 172.31.1.34: bytes=32 time=13ms TTL=253
Reply from 172.31.1.34: bytes=32 time=10ms TTL=253
Reply from 172.31.1.34: bytes=32 time=13ms TTL=253

Ping statistics for 172.31.1.34:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 9ms
C:\>
```

Ping PC4 a PC1, PC2 y PC3

```
C:\>ping 172.31.1.14

Pinging 172.31.1.14 with 32 bytes of data:

Reply from 172.31.1.14: bytes=32 time=4ms TTL=124
Reply from 172.31.1.14: bytes=32 time=15ms TTL=124
Reply from 172.31.1.14: bytes=32 time=22ms TTL=124
```

Reply from 172.31.1.14: bytes=32 time=17ms TTL=124

Ping statistics for 172.31.1.14:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 22ms, Average = 14ms

C:\>ping 172.31.1.30

Pinging 172.31.1.30 with 32 bytes of data:

Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Reply from 172.31.1.30: bytes=32 time=13ms TTL=125
Reply from 172.31.1.30: bytes=32 time=12ms TTL=125
Reply from 172.31.1.30: bytes=32 time=12ms TTL=125

Ping statistics for 172.31.1.30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 9ms

C:\>ping 172.31.1.46

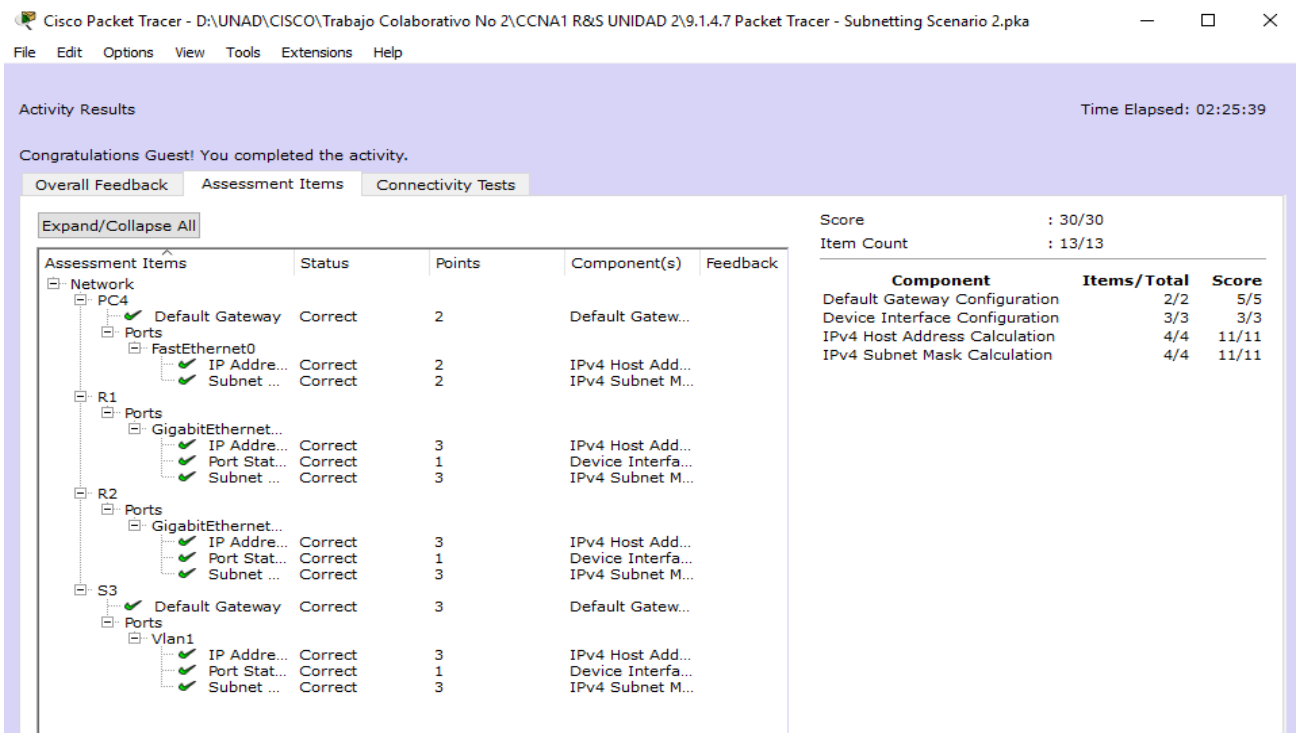
Pinging 172.31.1.46 with 32 bytes of data:

Reply from 172.31.1.46: bytes=32 time=2ms TTL=126
Reply from 172.31.1.46: bytes=32 time=11ms TTL=126
Reply from 172.31.1.46: bytes=32 time=14ms TTL=126
Reply from 172.31.1.46: bytes=32 time=21ms TTL=126

Ping statistics for 172.31.1.46:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 21ms, Average = 12ms

C:\>

Ítems Resueltos



Ejercicio 9.2.1.5: Diseño e implementación de un esquema de direccionamiento VSLM

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
[[R1Name]]	G0/0	[[R1G0Add]]	[[R1G0Sub]]	No aplicable
	G0/1	[[R1G1Add]]	[[R1G1Sub]]	No aplicable
	S0/0/0	[[R1S0Add]]	[[R1S0Sub]]	No aplicable
[[R2Name]]	G0/0	[[R2G0Add]]	[[R2G0Sub]]	No aplicable
	G0/1	[[R2G1Add]]	[[R2G1Sub]]	No aplicable
	S0/0/0	[[R2S0Add]]	[[R2S0Sub]]	No aplicable
[[S1Name]]	VLAN 1	[[S1Add]]	[[S1Sub]]	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]	[[S2Sub]]	[[R1G1Add]]
[[S3Name]]	VLAN 1	[[S3Add]]	[[S3Sub]]	[[R2G0Add]]
[[S4Name]]	VLAN 1	[[S4Add]]	[[S4Sub]]	[[R2G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]	[[PC1Sub]]	[[R1G0Add]]
[[PC2Name]]	NIC	[[PC2Add]]	[[PC2Sub]]	[[R1G1Add]]
[[PC3Name]]	NIC	[[PC3Add]]	[[PC3Sub]]	[[R2G0Add]]
[[PC4Name]]	NIC	[[PC4Add]]	[[PC4Sub]]	[[R2G1Add]]

Objetivos

Parte 1: Examinar los requisitos de la red
Parte 2: Diseñar el esquema de direccionamiento VLSM
Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

Información básica

En esta actividad, se le proporciona una dirección de red /24 para diseñar un esquema de direccionamiento VLSM. Sobre la base de un conjunto de requisitos, asignará subredes y direccionamiento, configurará los dispositivos y verificará la conectividad.

Parte 1: Examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias

Dividirá la dirección de red [[DisplayNet]] en subredes. La red tiene los siguientes requisitos:

- La LAN de **Room-114** requerirá **27** direcciones IP de host.
- La LAN de **Room-279** requerirá **25** direcciones IP de host.
- La LAN de **Room-312** requerirá **14** direcciones IP de host.
- La LAN de **Room-407** requerirá **8** direcciones IP de host.

¿Cuántas subredes se necesitan en la topología de la red?
R: 5

Paso 2: Determinar la información de máscara de subred para cada subred a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-114**?

¿Cuántas direcciones de host utilizables admitirá esta subred?
b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-279**?

¿Cuántas direcciones de host utilizables admitirá esta subred?
c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-312**?

¿Cuántas direcciones de host utilizables admitirá esta subred?
d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **Room-407**?

¿Cuántas direcciones de host utilizables admitirá esta subred?
e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para la conexión entre **Branch1** y **Branch2**?

Parte 2: Diseñar el esquema de direccionamiento VLSM

Paso 1: Dividir la red 172.31.103.0/24 según la cantidad de hosts por subred

a. Use la primera subred para la LAN más extensa.
b. Use la segunda subred para la segunda LAN más extensa.
c. Use la tercera subred para la tercera LAN más extensa.
d. Use la cuarta subred para la cuarta LAN más extensa.
e. Use la quinta subred para admitir la conexión entre **Branch1** y **Branch2**.

Paso 2: Registrar las subredes VLSM

Complete la **tabla de subredes** con las descripciones de las subred (p. ej., LAN de Room-114), la cantidad de hosts necesarios, la dirección de red para la subred, la primera dirección de host utilizable y la dirección de broadcast. Repita hasta que todas las direcciones estén en la lista.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Dirección de broadcast

Paso 3: Documente el esquema de direccionamiento.

a. Asigne las primeras direcciones IP utilizables a **Branch1** para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables a **Branch2** para los dos enlaces LAN. Asigne la última dirección IP utilizable para el enlace WAN.

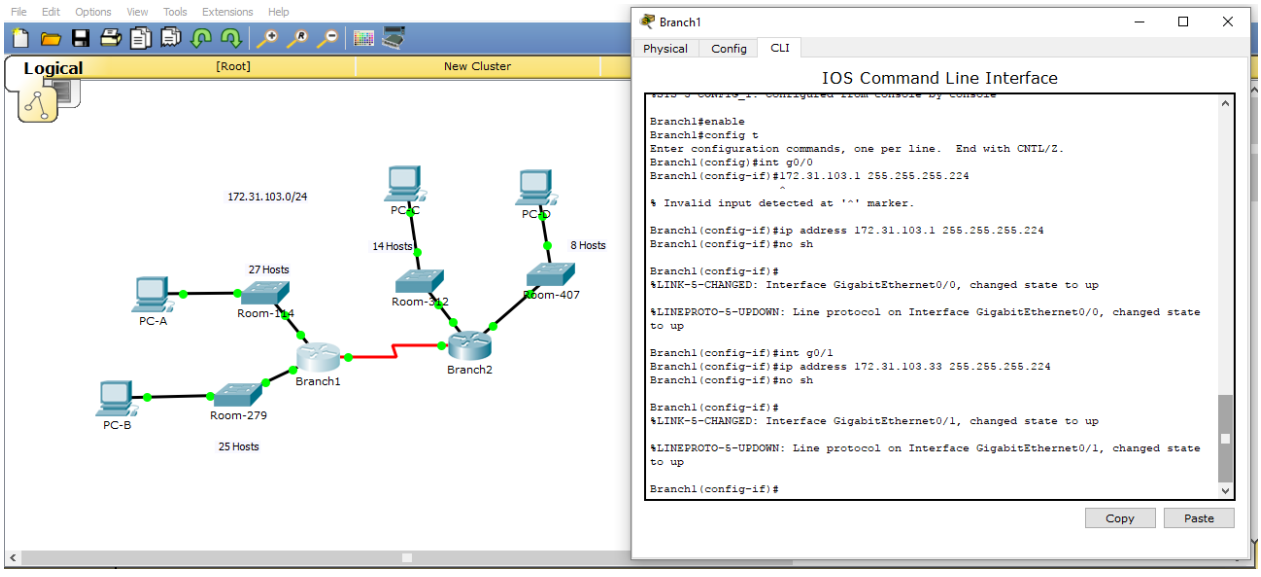
c. Asigne las segundas direcciones IP utilizables a los switches.

d. Asigne las últimas direcciones IP utilizables a los hosts.

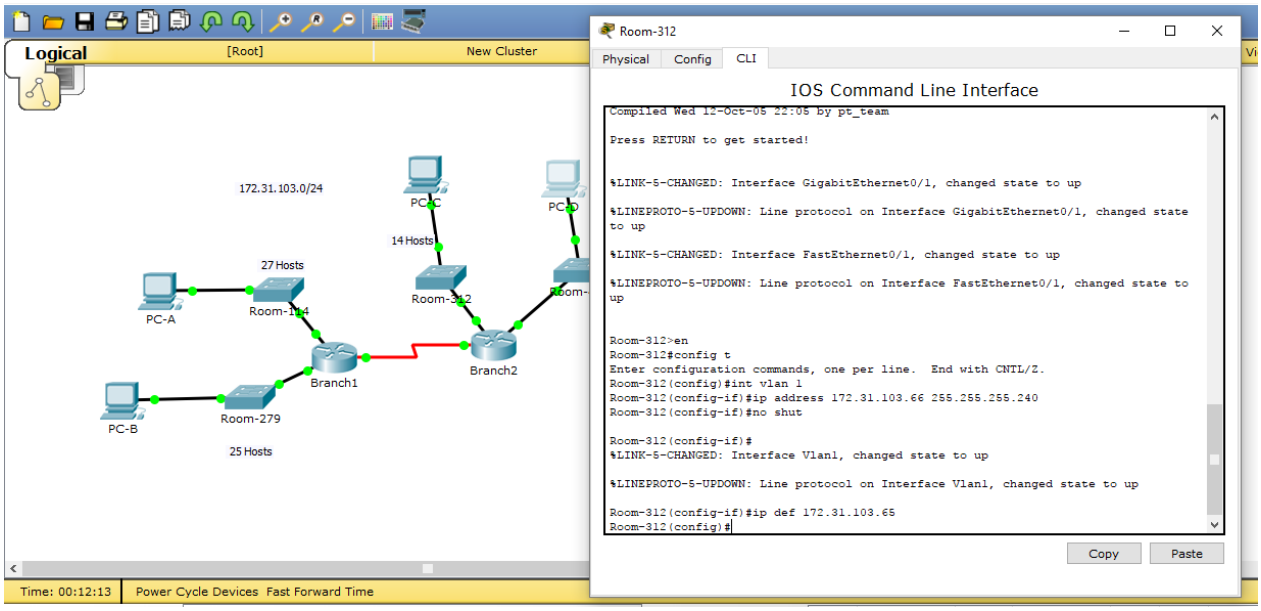
Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

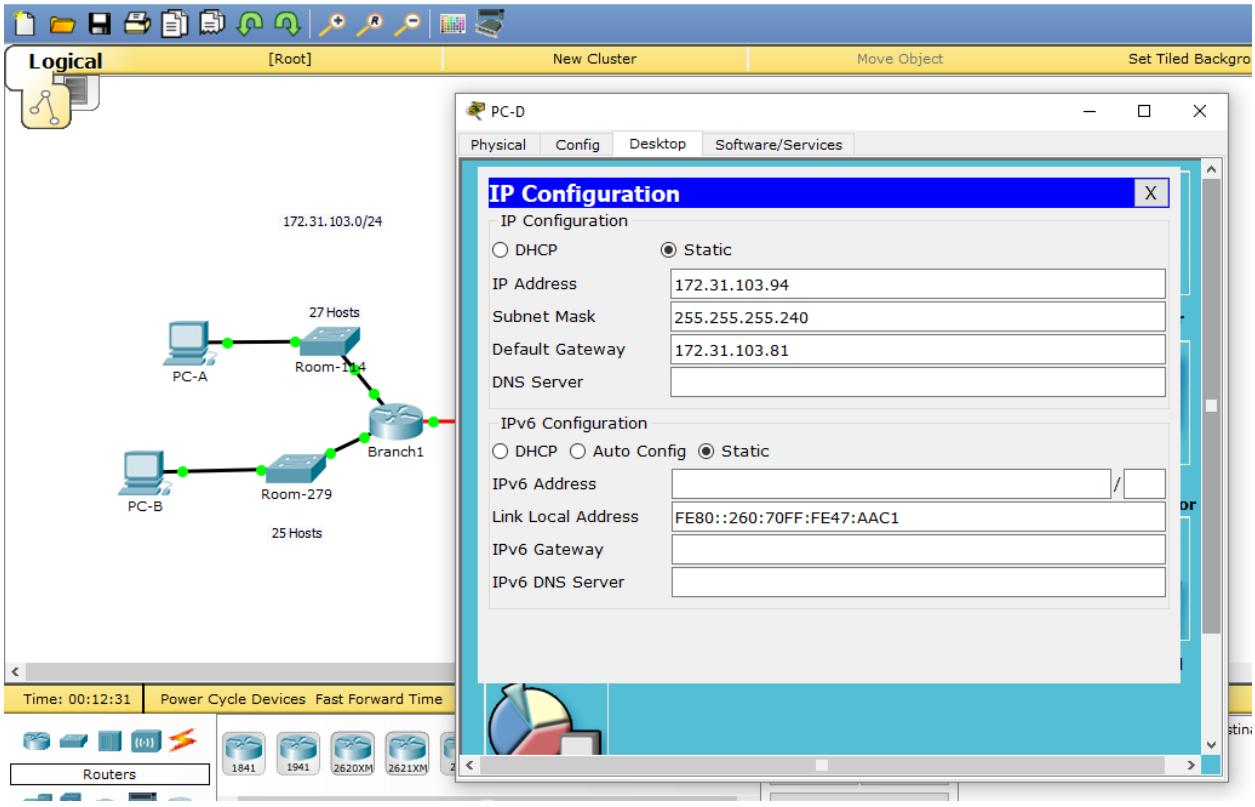
Paso 1: Configurar el direccionamiento IP en las interfaces LAN de [[R1Name]]



Paso 2: Configurar el direccionamiento IP en [[S3Name]], incluido el gateway predeterminado

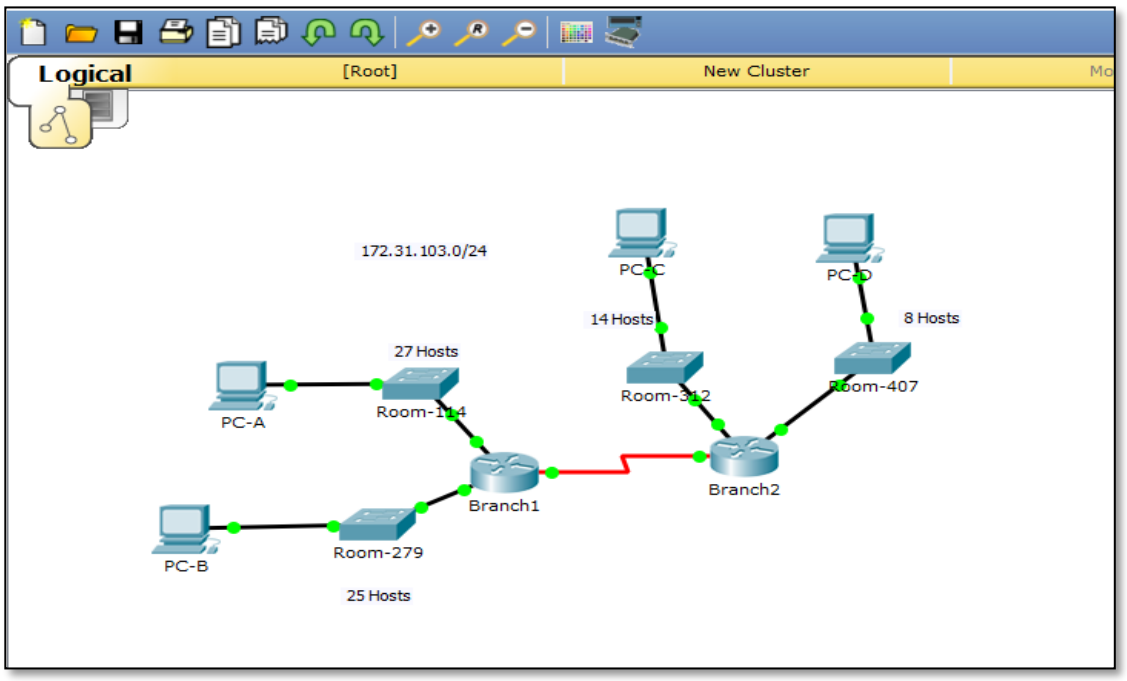


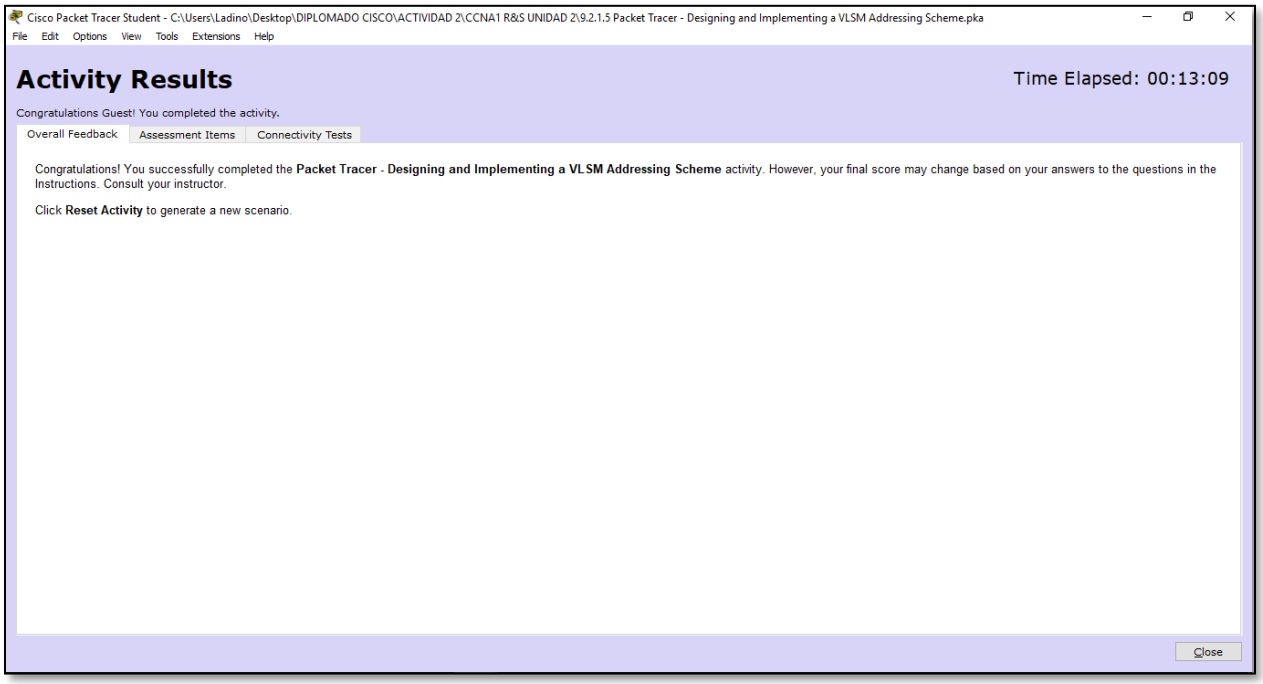
Paso 3: Configurar el direccionamiento IP en [[PC4Name]], incluido el gateway predeterminado



Paso 4: Verifique la conectividad.

Solo puede verificar la conectividad desde [[R1Name]], [[S3Name]] y [[PC4Name]]. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.





Ejercicio 9.3.1.4: Implementación de un esquema de direccionamiento IPv6 dividido en subredes

Topología

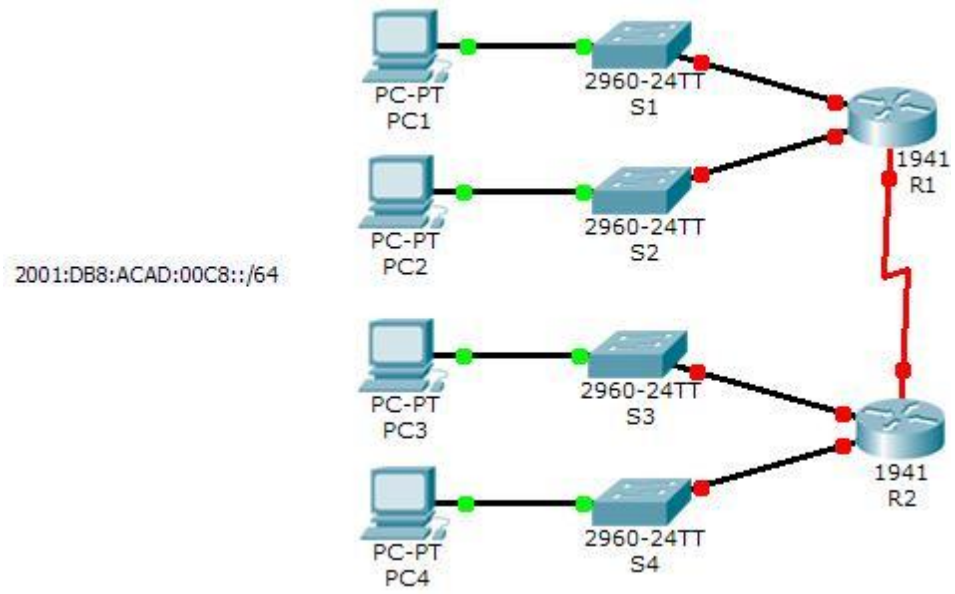


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Link-Local
R1	G0/0	2001:DB:ACAD:00C8::1/64	FE80::1
	G0/1	2001:DB:ACAD:00C9::1/64	FE80::1
	S0/0/0	2001:DB:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB:ACAD:00CA::1/64	FE80::2
	G0/1	2001:DB:ACAD:00CB::1/64	FE80::2
	S0/0/0	2001:DB:ACAD:00CC::2/64	FE80::2
PC1	NIC	Configuración automática	
PC2	NIC	Configuración automática	
PC3	NIC	Configuración automática	
PC4	NIC	Configuración automática	

Objetivos

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Situación

El administrador de red desea que asigne cinco subredes IPv6 /64 a la red que se muestra en la topología. Su tarea consiste determinar las subredes IPv6, asignar direcciones IPv6 a los routers y configurar las PC para que reciban automáticamente el direccionamiento IPv6. El último paso es verificar la conectividad entre los hosts IPv6.

Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6

Paso 1: Determinar la cantidad de subredes necesarias

Comience con la subred IPv6 2001:DB:ACAD:00C8::/64 y asígnela a la LAN del R1 conectada

a GigabitEthernet 0/0, como se muestra en la **tabla de subredes**. Para el resto de las subredes IPv6, incremente la dirección de la subred 2001:DB:ACAD:00C8::/64 de a 1 y complete la **tabla de subredes** con las direcciones de la subred IPv6.

Tabla de subredes

Descripción de la subred	Dirección de subred
R1 G0/0 LAN	2001:DB:ACAD:00C8::0/64
R1 G0/1 LAN	2001:DB:ACAD:00C9::0/64
R2 G0/0 LAN	2001:DB:ACAD:00CA::0/64
R2 G0/1 LAN	2001:DB:ACAD:00CB::0/64
Enlace WAN	2001:DB:ACAD:00CC::0/64

Paso 2: Asignar el direccionamiento IPv6 a los routers

- Asigne las primeras direcciones IPv6 al R1 para los dos enlaces LAN y el enlace WAN.
- Asigne las primeras direcciones IPv6 al R2 para las dos LAN. Asigne la segunda dirección IPv6 para el enlace WAN.
- Registre el esquema de direccionamiento IPv6 en la **tabla de direccionamiento**.

```
Press RETURN to get started!



R1>enable
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:00C8::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

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

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

```
R1(config-if)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:00C9::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

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

```
R1(config-if)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:00CC::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CA::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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

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

```
R2(config-if)#interface gigabitethernet 0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CB::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

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

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

```
R2(config-if)#interface serial 0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CC::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Paso 1: Configurar el direccionamiento IPv6 en los routers

Nota: esta red ya está configurada con algunos comandos de IPv6 que se abordan en un curso posterior. En este punto de sus estudios, solo necesita saber cómo configurar la dirección IPv6 en una interfaz.
Configure el R1 y el R2 con las direcciones IPv6 que especificó en la **tabla de direccionamiento** y active las interfaces.

```
Router(config-if)# ipv6 address ipv6-address/prefix
```

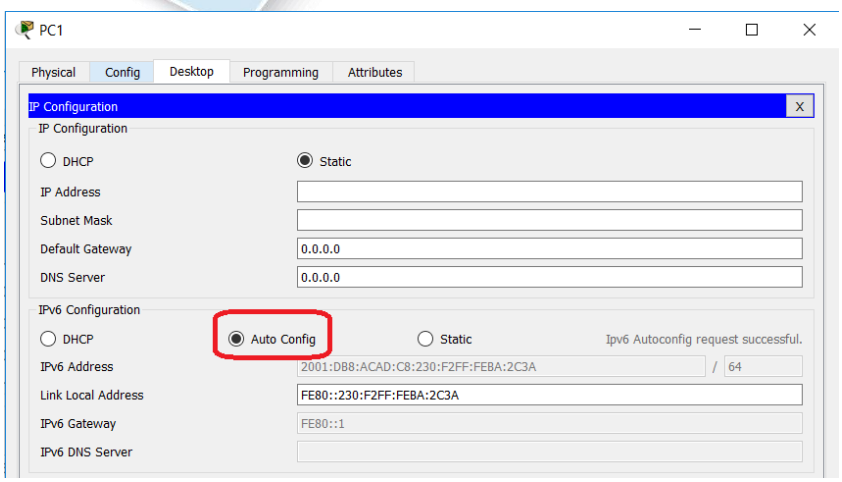
```
Router(config-if)# ipv6 address ipv6-link-local link-local
```

Paso 2: Configurar las PC para que reciban el direccionamiento IPv6 automáticamente

Configure las cuatro PC para que tengan configuración automática. Luego, cada una debe recibir automáticamente las direcciones IPv6 completas de los routers.

Paso 3: Verificar la conectividad entre las PC

Cada PC debe ser capaz de hacer ping a las otras PC y a los routers.



Ejercicio 9.4.1.2: Reto de habilidades de integración

Topología

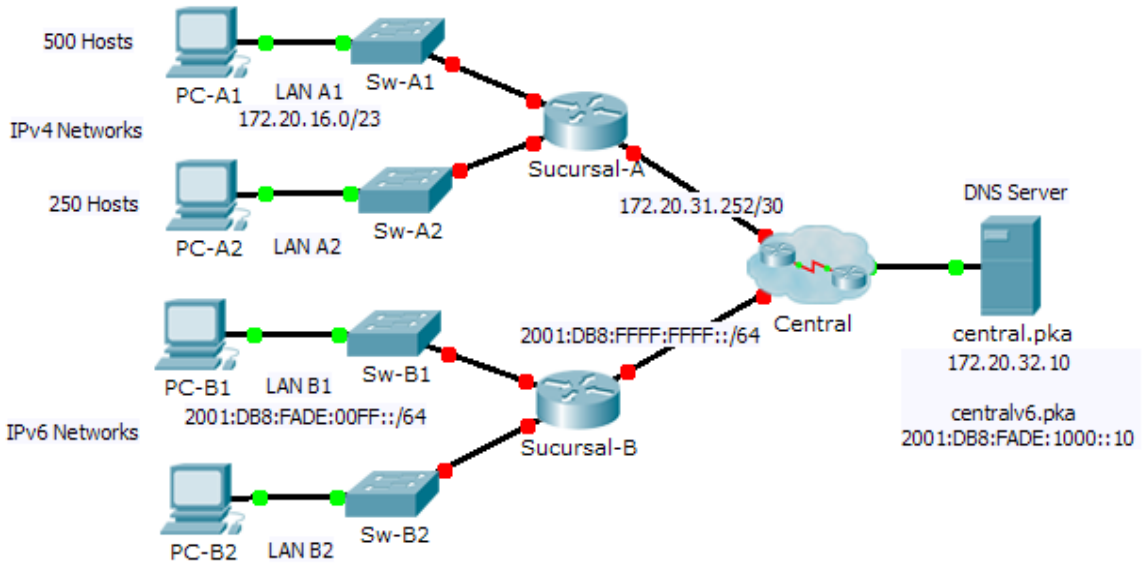


Tabla de direccionamiento: Resaltado en Amarillo se muestra las direcciones IP configuradas

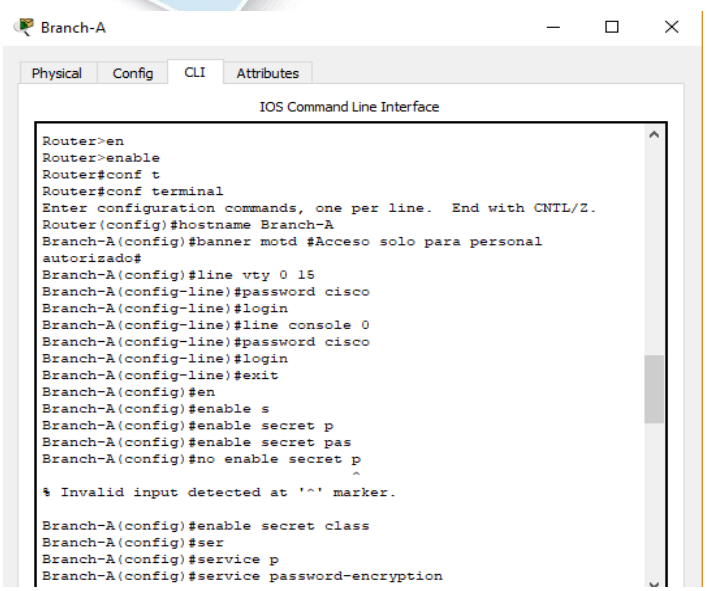
Dispositivo	Interfaz	Dirección/Prefijo IPv6	Máscara de	Gateway predeterminado
Sucursal-A	G0/0	172.20.16.1	255.255.254.0	No aplicable
	G0/1	172.20.18.1	255.255.255.0	No aplicable
	G0/2	172.20.31.25	255.255.255.25	No aplicable
Sucursal-B	G0/0	2001:DB8:FADE:00FF::1/64		No aplicable
	G0/1	2001:DB8:FADE:0100::1/64		No aplicable
	G0/2	2001:DB8:FFFF:FFFF::2/64		No aplicable
PC-A1	NIC	172.20.17.25	255.255.254.0	172.20.16.1
PC-A2	NIC	172.20.18.25	255.255.255.0	172.20.18.1
PC-B1	NIC	2001:DB8:FADE:00FF::10/64		FE80::B
PC-B2	NIC	2001:DB8:FADE:0100::10/64		FE80::B

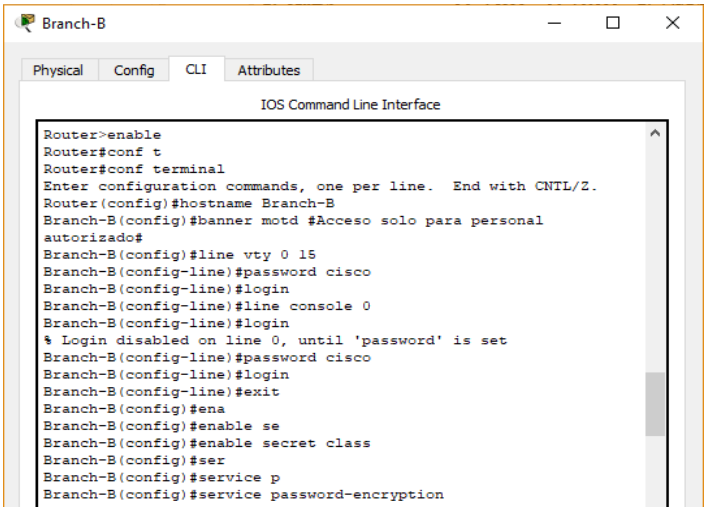
Situación

Como técnico de redes familiarizado con implementaciones de direccionamiento IPv4 e IPv6, ya está preparado para tomar una infraestructura de red existente y aplicar sus conocimientos y habilidades
a finalizar la configuración. En esta actividad, el administrador de red ya configuró algunos comandos en los routers. **No borre ni modifique esas configuraciones**. Su tarea consiste en completar el esquema de direccionamiento IPv4 e IPv6, implementar el direccionamiento IPv4 e IPv6 y verificar la conectividad.

Requisitos

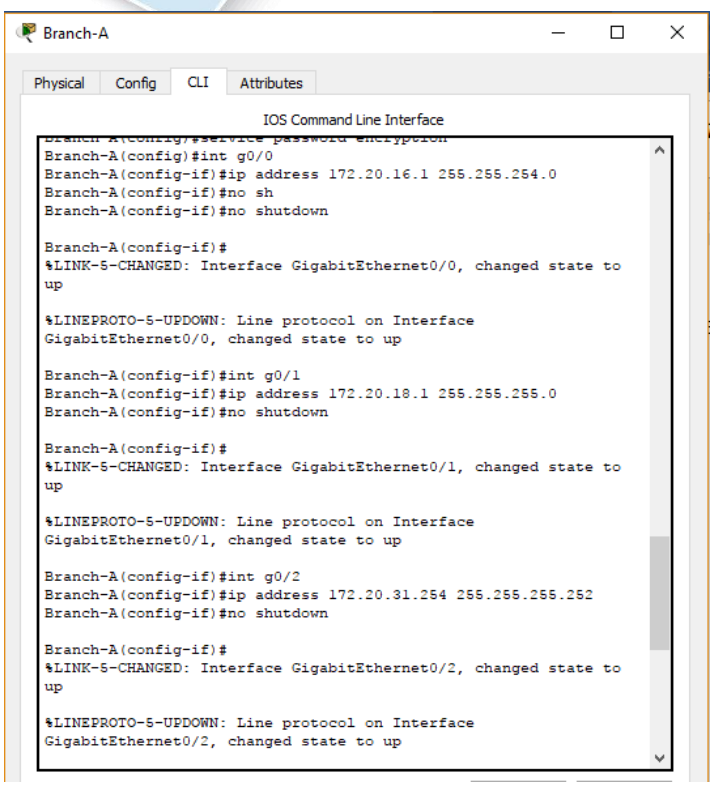
- Configure los parámetros iniciales en **Sucursal-A** y **Sucursal-B**, incluidos el nombre de host, el aviso, las líneas y las contraseñas. Utilice **cisco** como contraseña de EXEC del usuario y **class** como contraseña de EXEC privilegiado. Encripte todas las contraseñas.

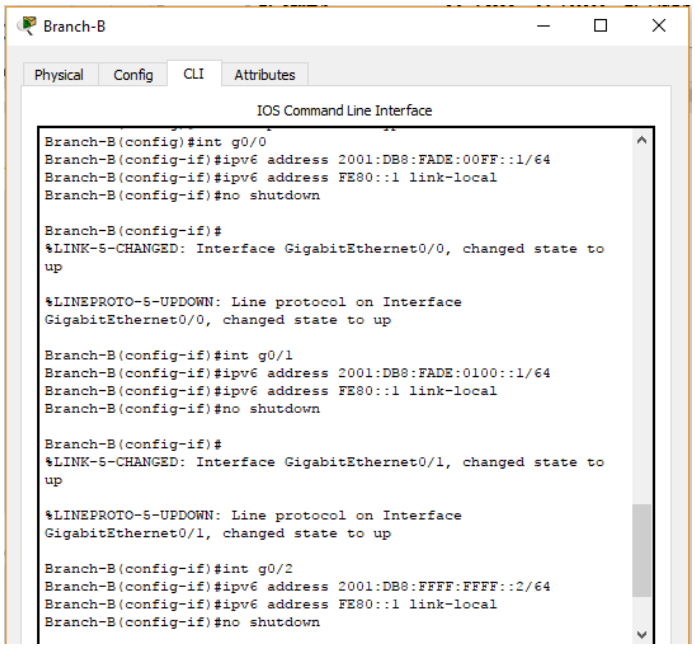




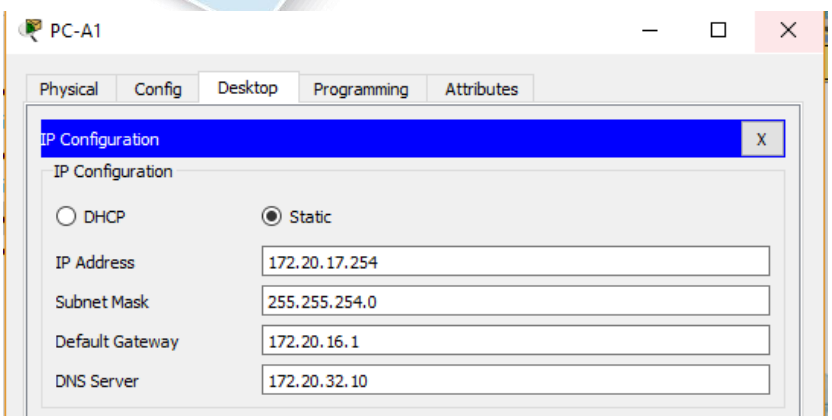
- LAN A1 utiliza la subred 172.20.16.0/23. Asigne la siguiente subred disponible a LAN A2 para admitir un máximo de 250 hosts.
- LAN B1 utiliza la subred 2001:DB8:FADE:00FF::/64. Asigne la siguiente subred disponible a la B2 de LAN.
- Termine de registrar el esquema de direccionamiento en la **tabla de direccionamiento** con las siguientes pautas:

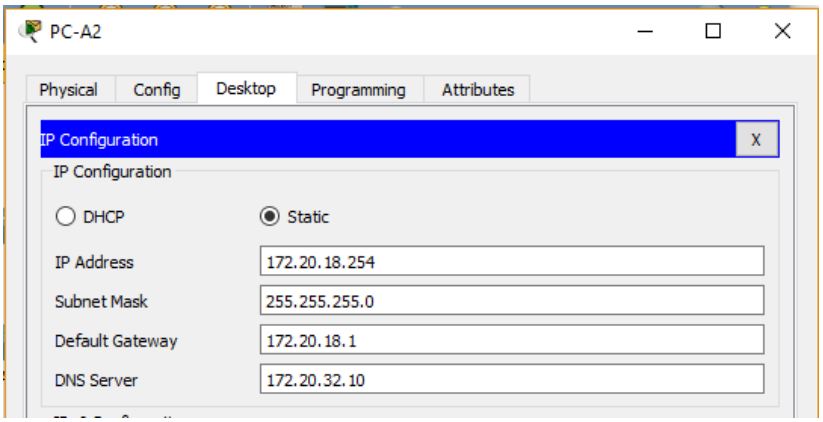
  - Asigne la primera dirección IP a la interfaz del router para LAN A1, LAN A2, LAN B1 y LAN B2.



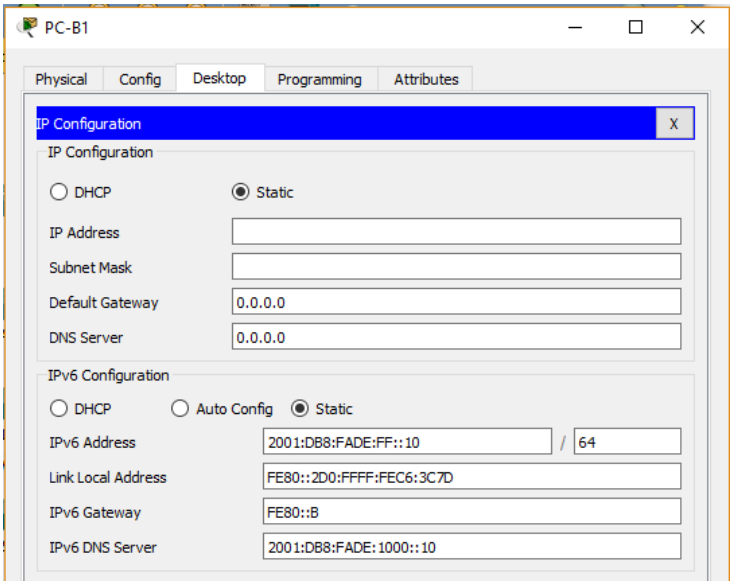


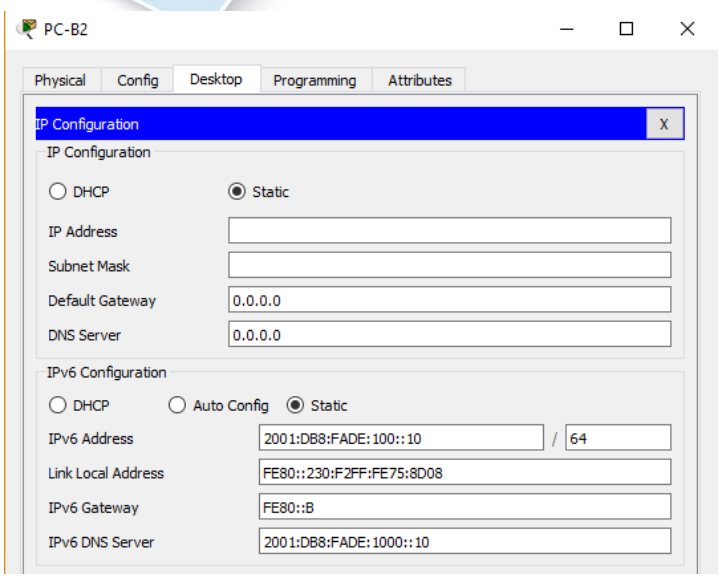
- Para las redes IPv4, asigne la última dirección IPv4 a las PC.



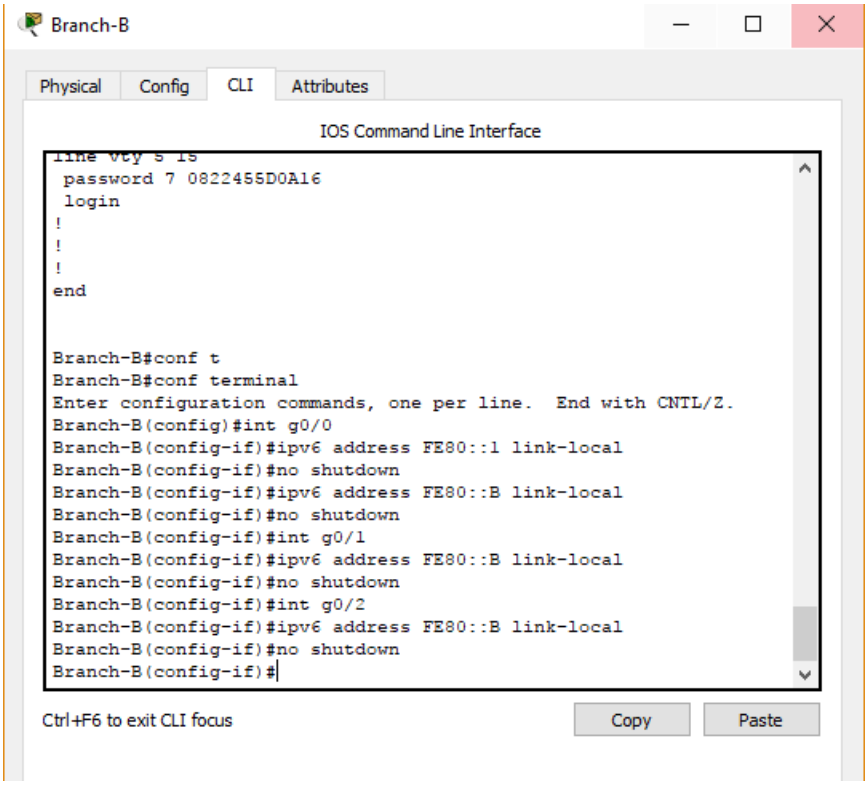


- Para las redes IPv6, asigne la 16.ª dirección IPv6 a las PC.



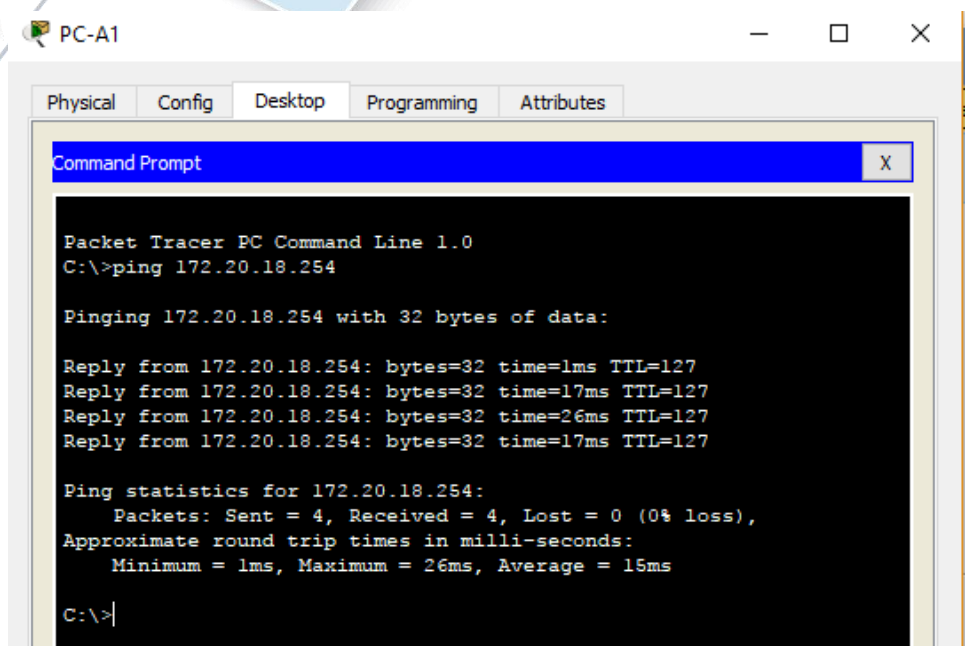


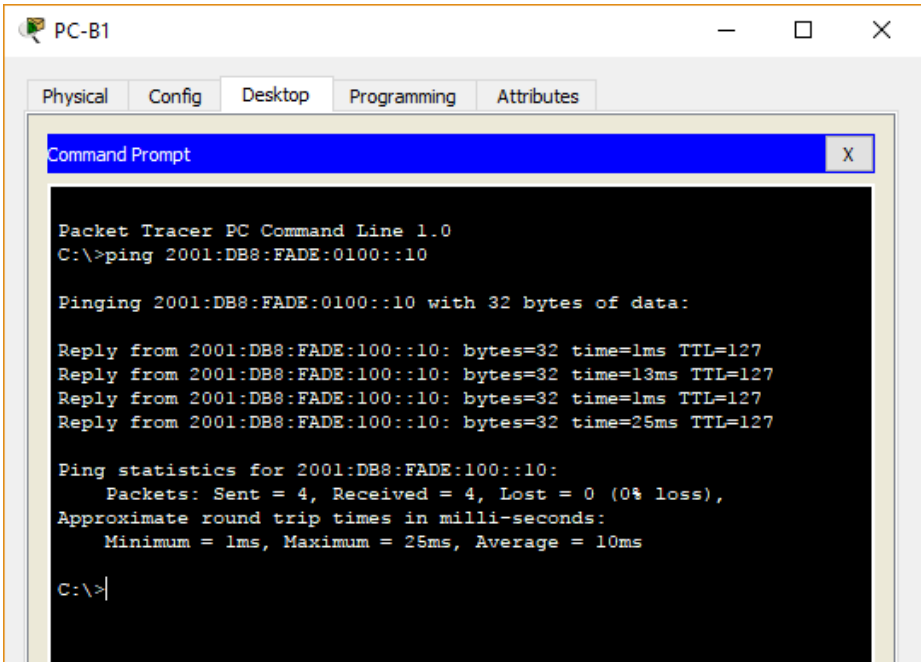
- Configure el direccionamiento de los routers según los registros. Incluya una descripción adecuada para cada interfaz del router. **Sucursal-B** utiliza FE80::B como dirección link-local.



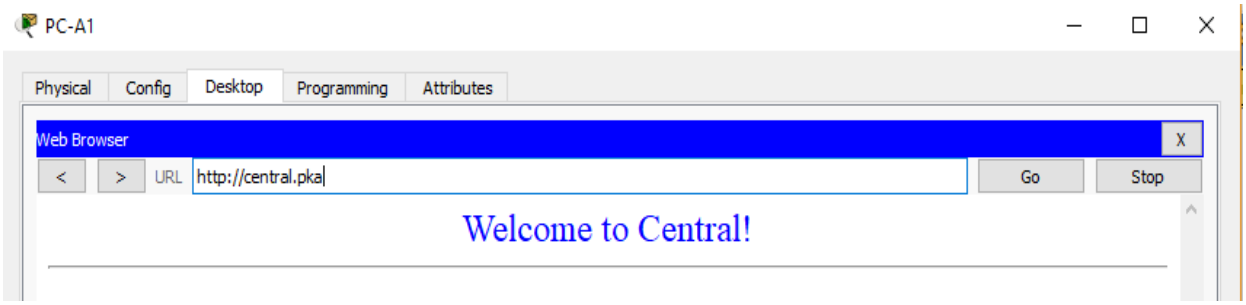
- Configure el direccionamiento de las PC según los registros. Las direcciones del servidor DNS para IPv4 e IPv6 se muestran en la topología.

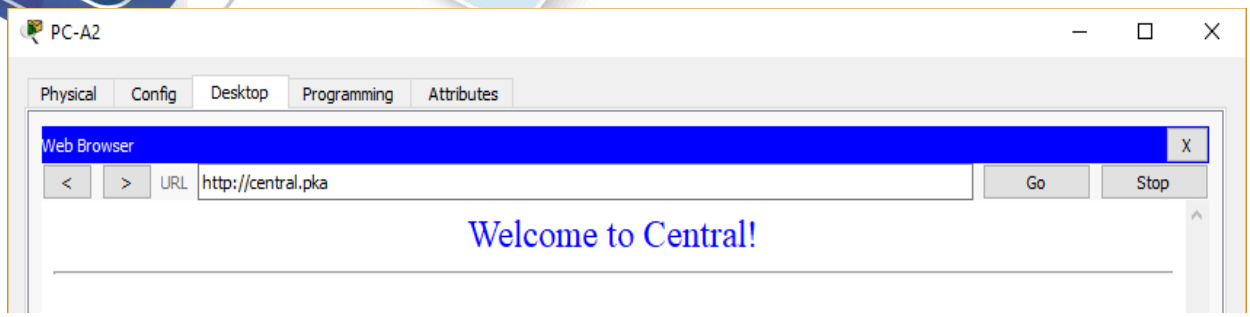
- Verifique la conectividad entre las PC IPv4 y entre las PC IPv6.



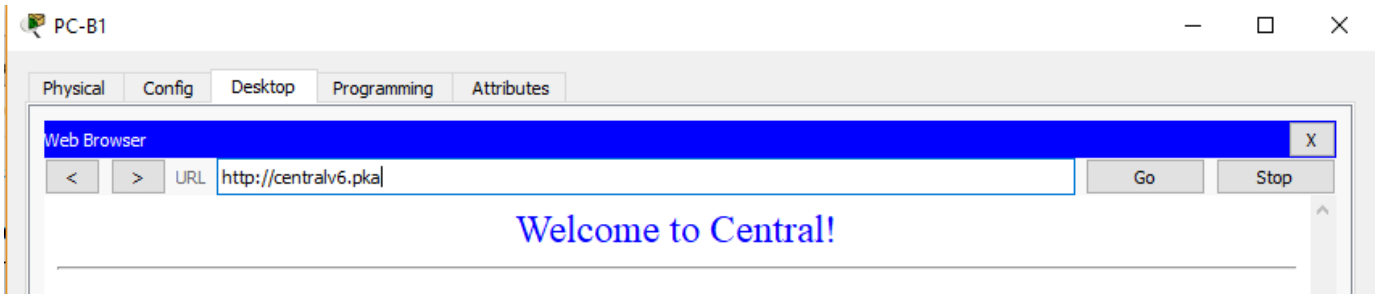


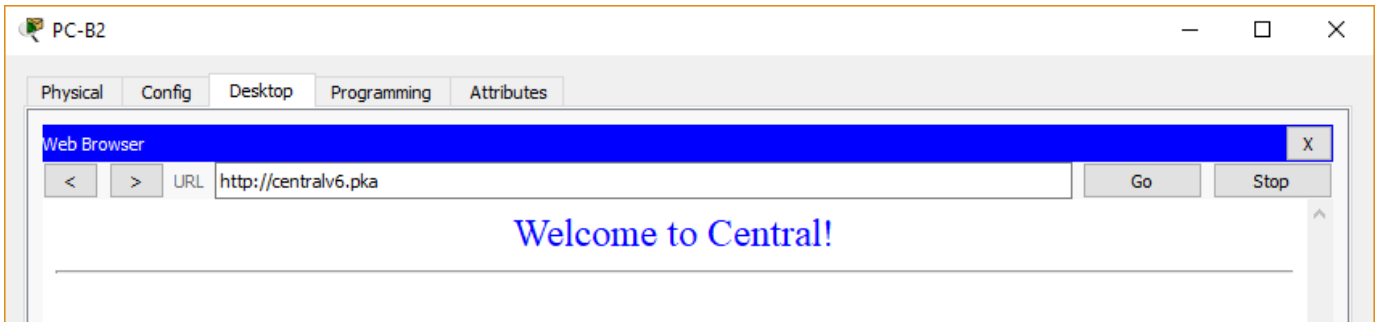
- Verifique que las PC IPv4 puedan acceder a la página Web en **central.pka**.



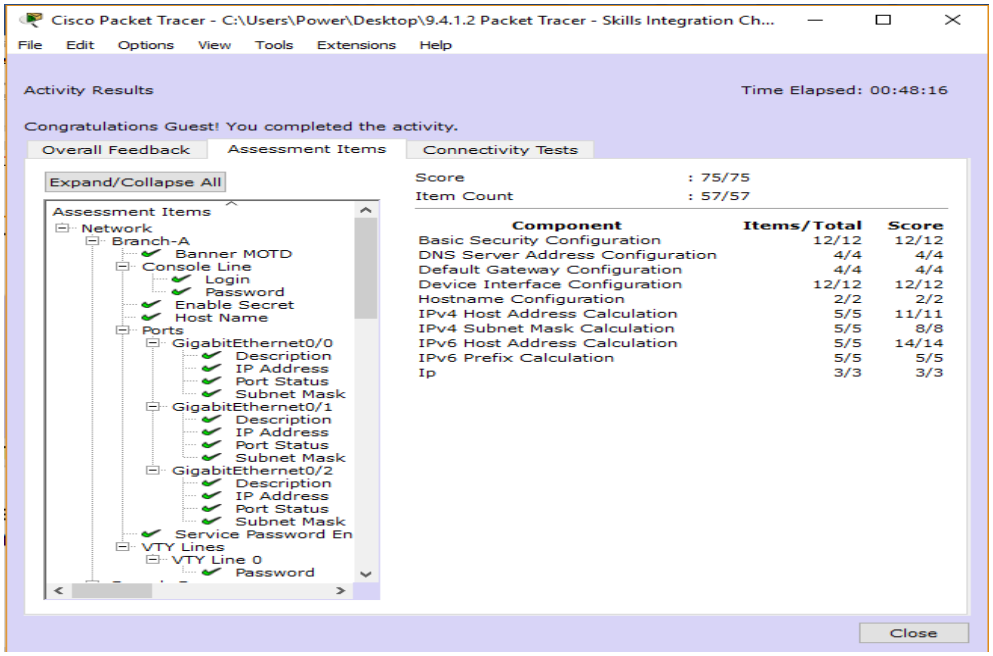


- Verifique que las PC IPv6 puedan acceder a la página Web en **centralv6.pka**.



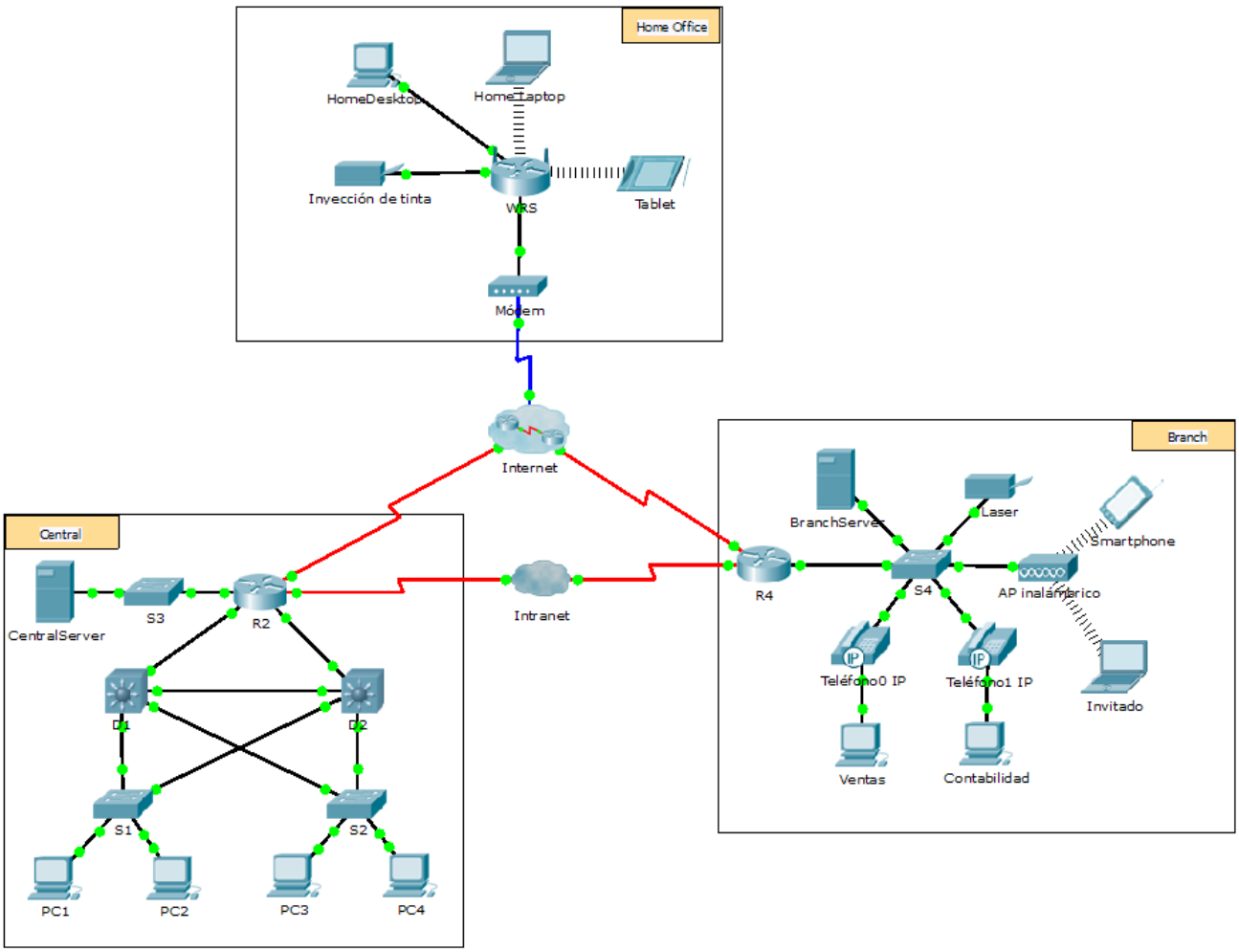


Resultados



Ejercicio 10.2.1.8: Servidores Web y de correo electrónico

Topología



Objetivos

Parte 1: Configurar y verificar los servicios Web

Parte 2: Configurar y verificar los servicios de correo electrónico

Información básica

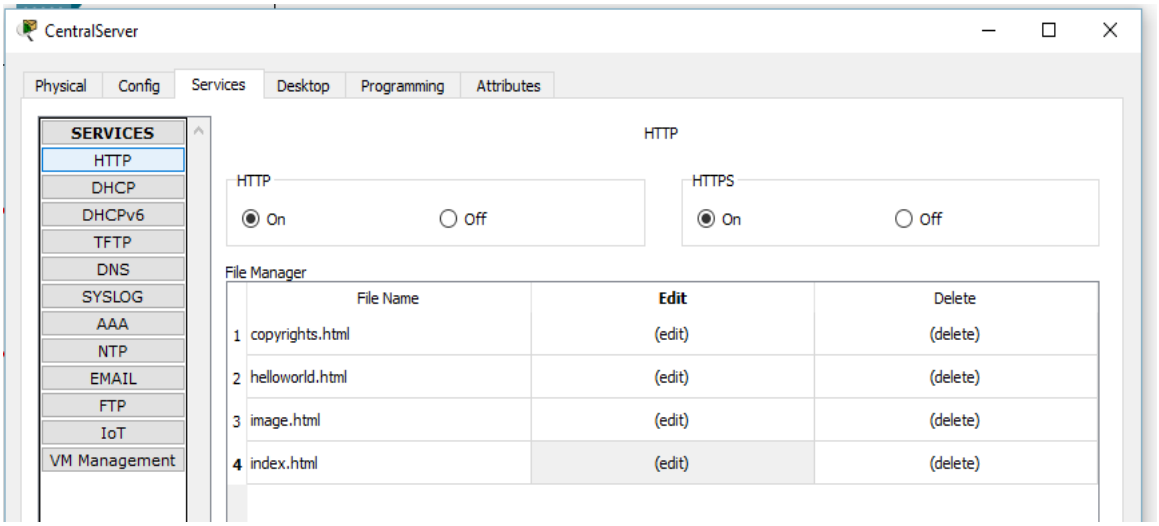
En esta actividad, configurará los servicios HTTP y de correo electrónico mediante el servidor simulado de
Packet Tracer. Luego, configurará clientes para que accedan a los servicios HTTP y de correo electrónico.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de
HTTP y de correo electrónico tiene sus propias instrucciones exclusivas de configuración e instalación.

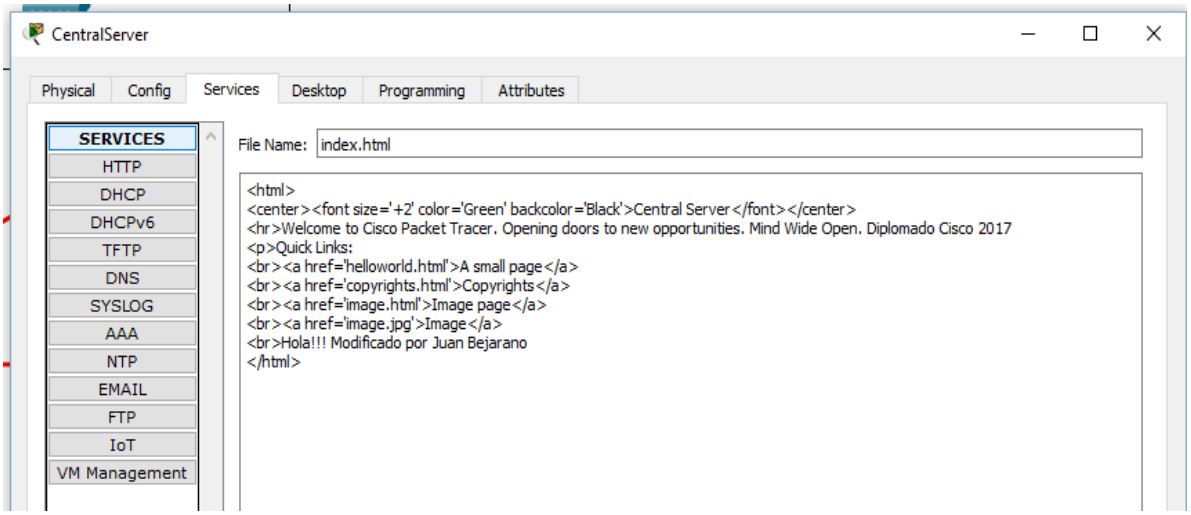
Parte 1: Configurar y verificar los servicios Web

Paso 1: Configurar servicios Web en CentralServer y BranchServer

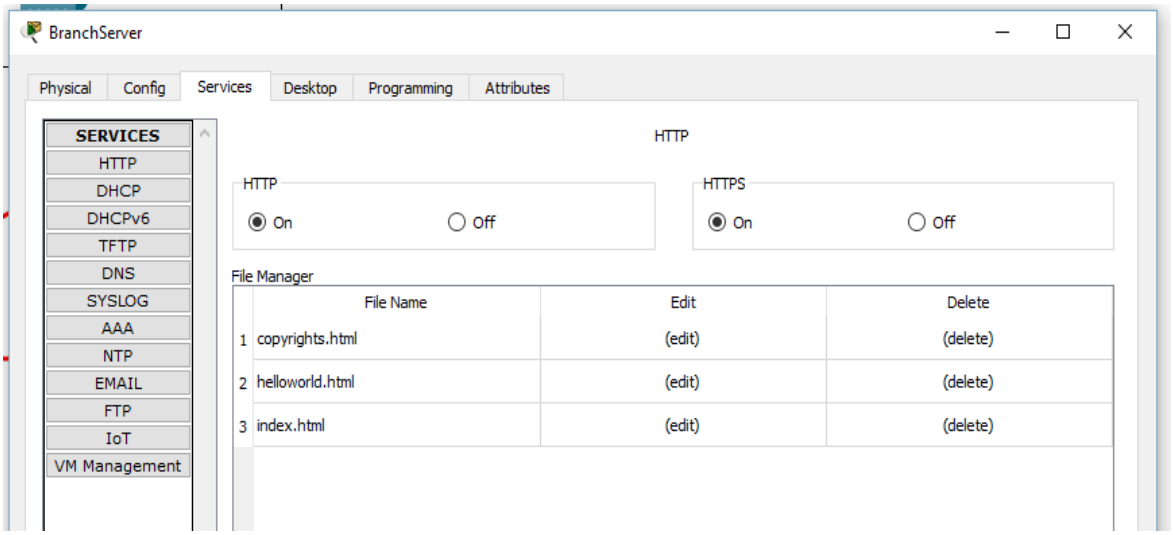
a. Haga clic en **CentralServer** y, a continuación, haga clic en la ficha **Config** > **HTTP**.
b. Haga clic en **On** (Activar) para habilitar HTTP y HTTP seguro (HTTPS).

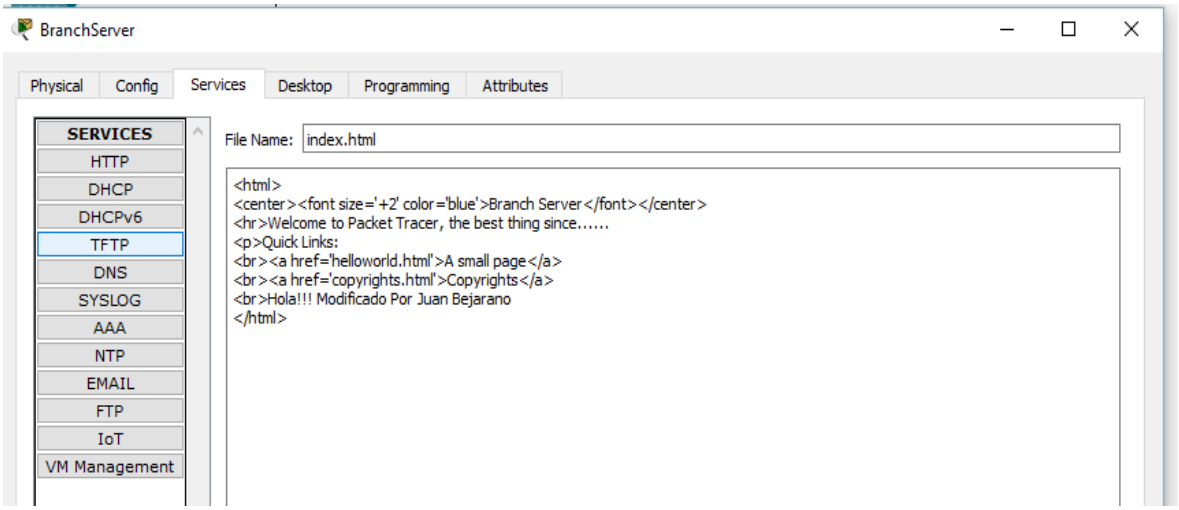


c. Optativo: personalice el código HTML.



d. Repita desde el paso 1a hasta el paso 1c en **BranchServer**.



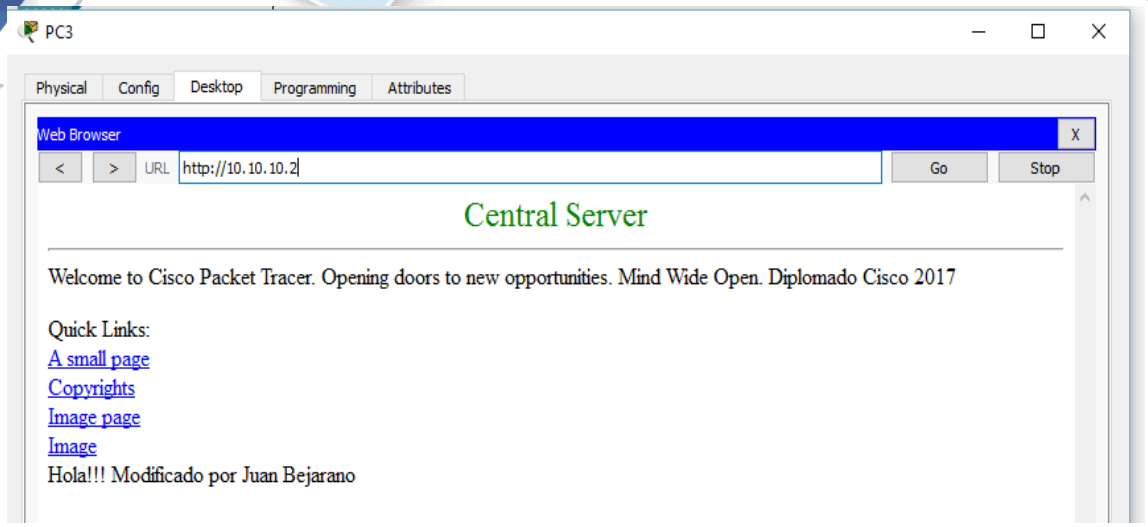


Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web

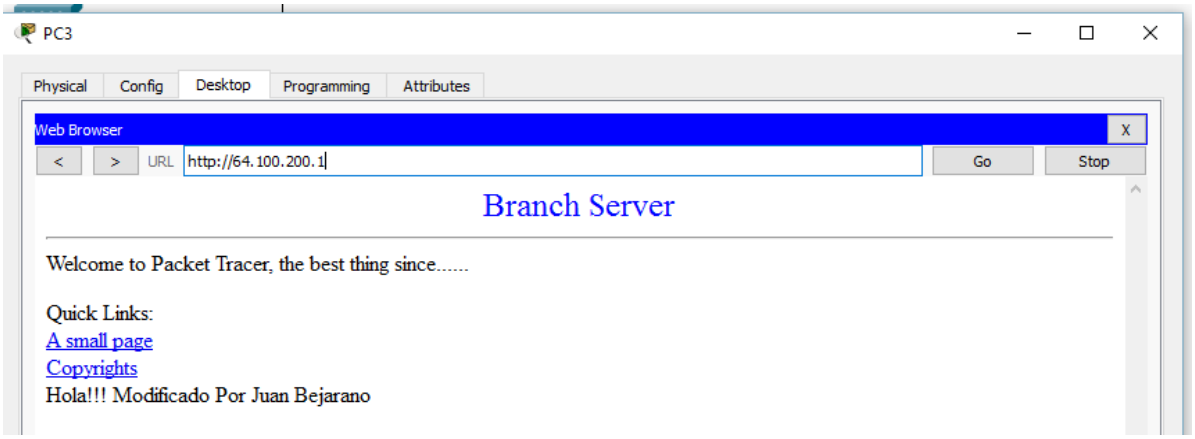
Existen muchos dispositivos terminales en esta red, pero para este paso, use **PC3**.

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Escritorio > Explorador Web).

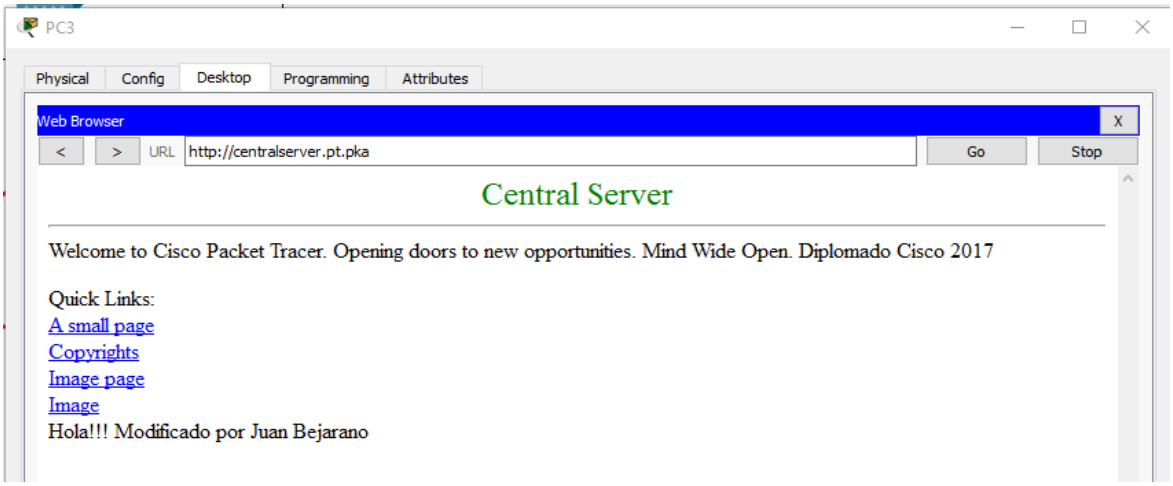
b. En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.



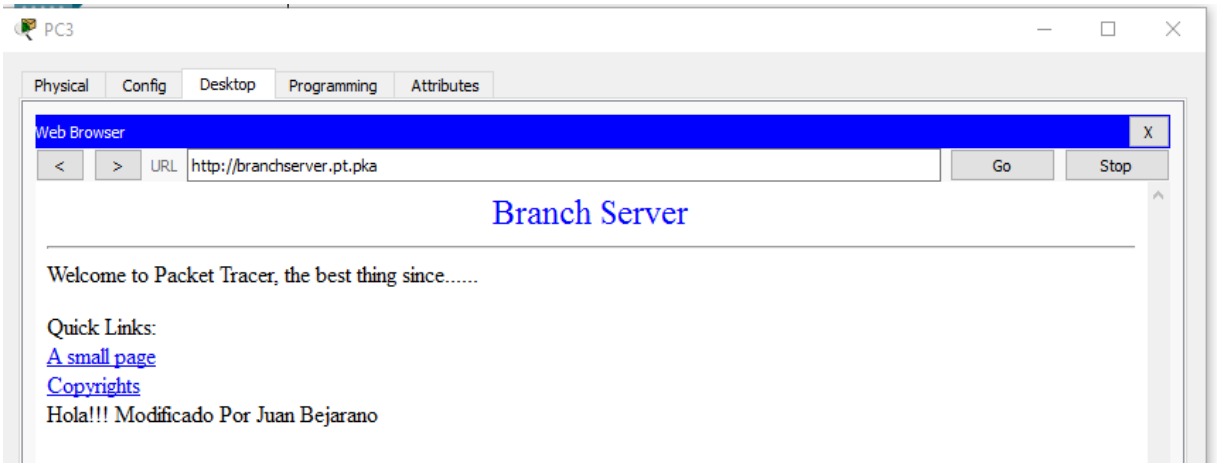
c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



d. En el cuadro de dirección URL, introduzca **centralserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **CentralServer**.



e. En el cuadro de dirección URL, introduzca **branchserver.pt.pka** y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



¿Qué protocolo traduce los nombres **centralserver.pt.pka** y **branchserver.pt.pka** por direcciones IP?

Servicio de nombres de dominios (DNS, Domain Name Service)

Parte 2: Configurar y verificar los servicios de correo electrónico en los servidores

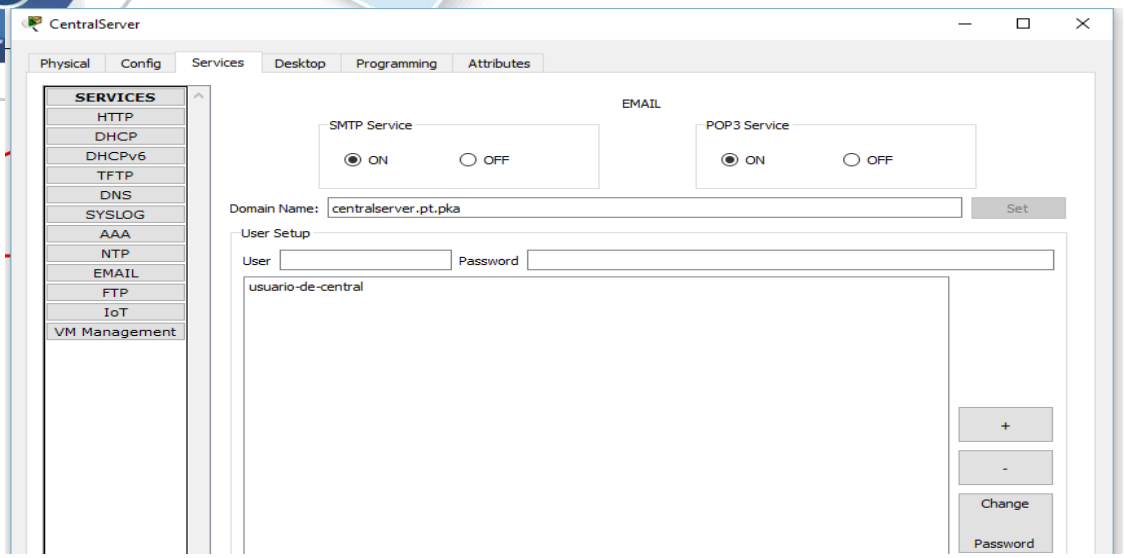
Paso 1: Configurar CentralServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **CentralServer** y, a continuación, seleccione la ficha **Config**, seguida del botón **EMAIL** (Correo electrónico).

b. Haga clic en **On** para habilitar SMTP y POP3.

c. Establezca el nombre de dominio **centralserver.pt.pka** y haga clic en **Set** (Establecer).

d. Cree un usuario denominado **usuario-de-central** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario

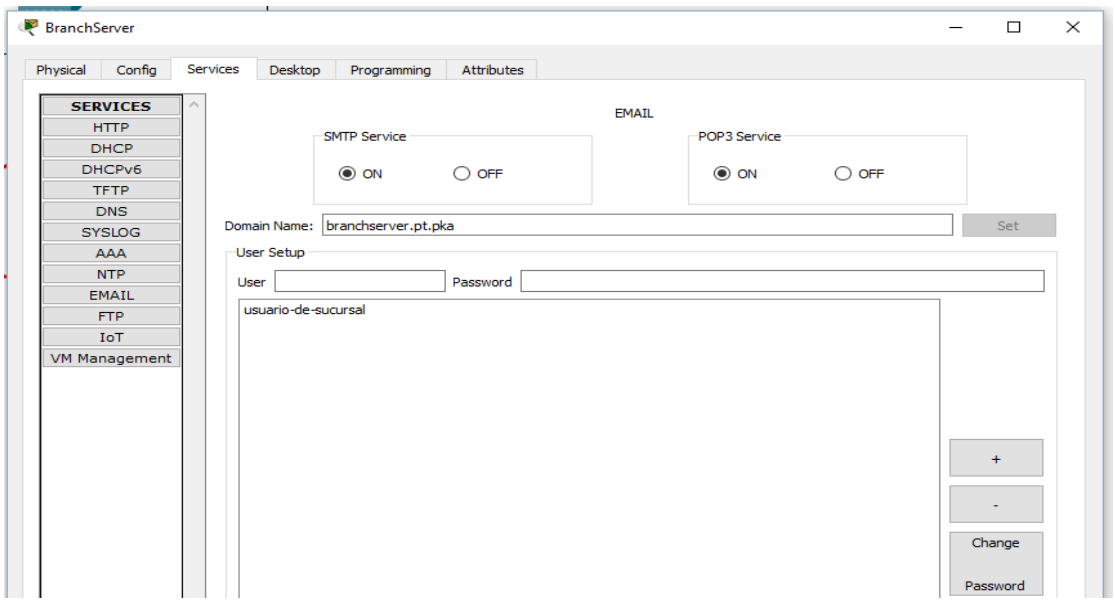


Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

a. Haga clic en **BranchServer** y, a continuación, haga clic en la ficha **Config** > **EMAIL**. b. Haga clic en **On** para habilitar SMTP y POP3**.**

c. Establezca el nombre de dominio **branchserver.pt.pka** y haga clic en **Set**.

d. Cree un usuario denominado **usuario-de-sucursal** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.



Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **E Mail** (Correo electrónico). b. Introduzca los siguientes valores en los campos correspondientes:

1) Your Name (Su nombre): **Usuario de central**

2) Email Address (Dirección de correo electrónico): **usuario-de-central@centralserver.pt.pka**

3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**

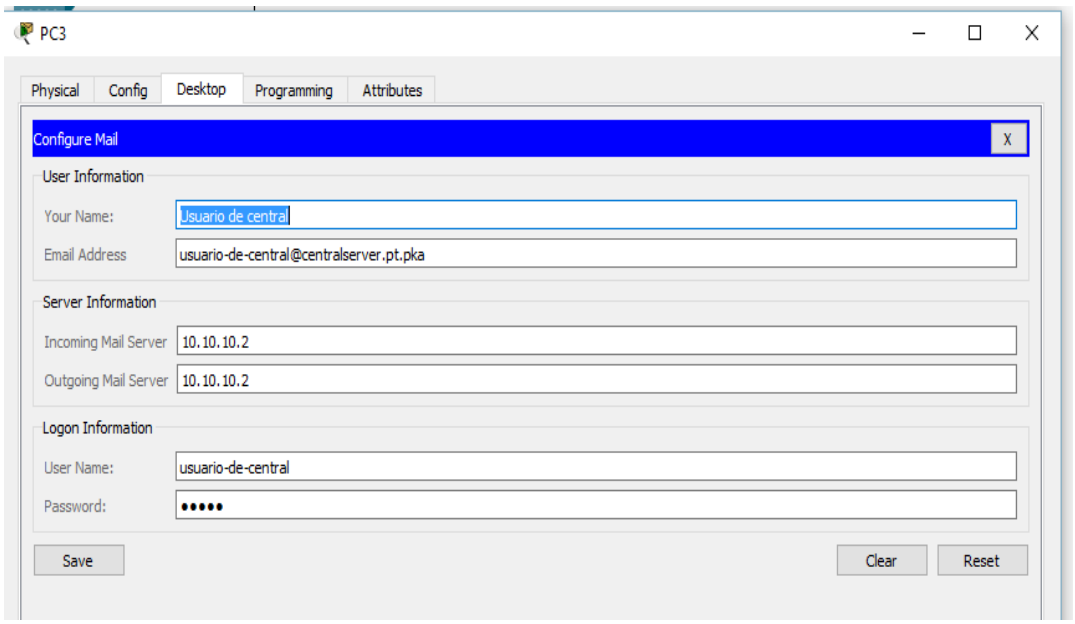
4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**

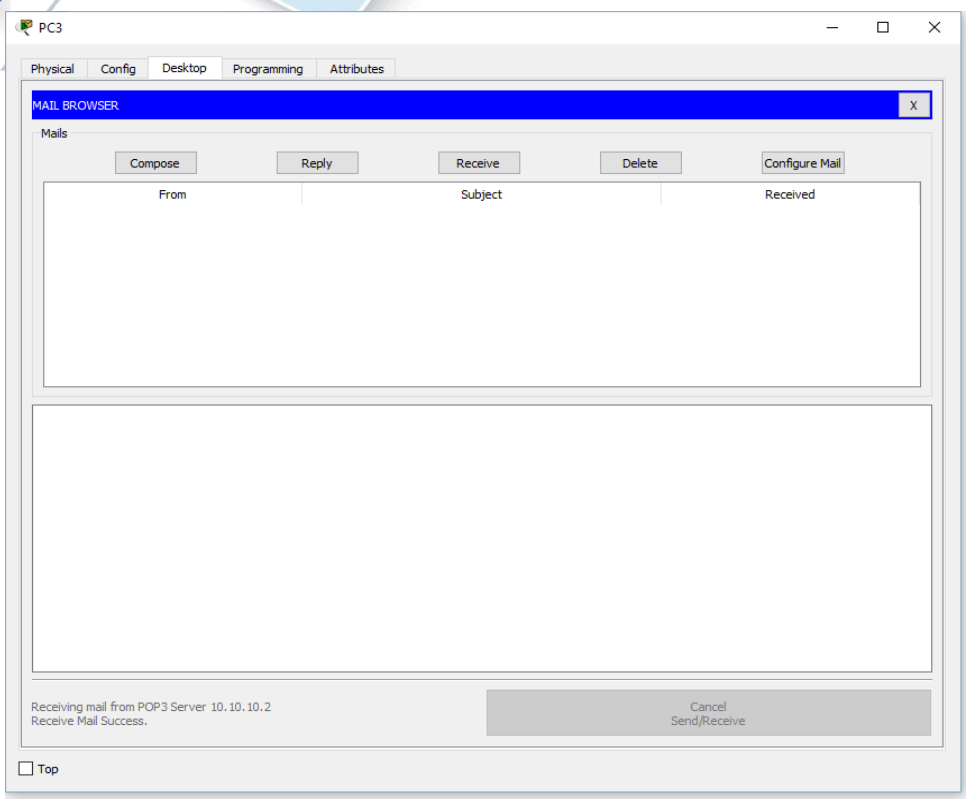
5) User Name (Nombre de usuario): **usuario-de-central**

6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.

d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).





Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

a. Haga clic en **Sales** (Ventas) y, a continuación, haga clic en la ficha **Desktop** > **E Mail**. b. Introduzca los siguientes valores en los campos correspondientes:

1) Your Name (Su nombre): **Usuario de sucursal**

2) Email Address (Dirección de correo electrónico): **usuario-de-sucursal@branchserver.pt.pka**

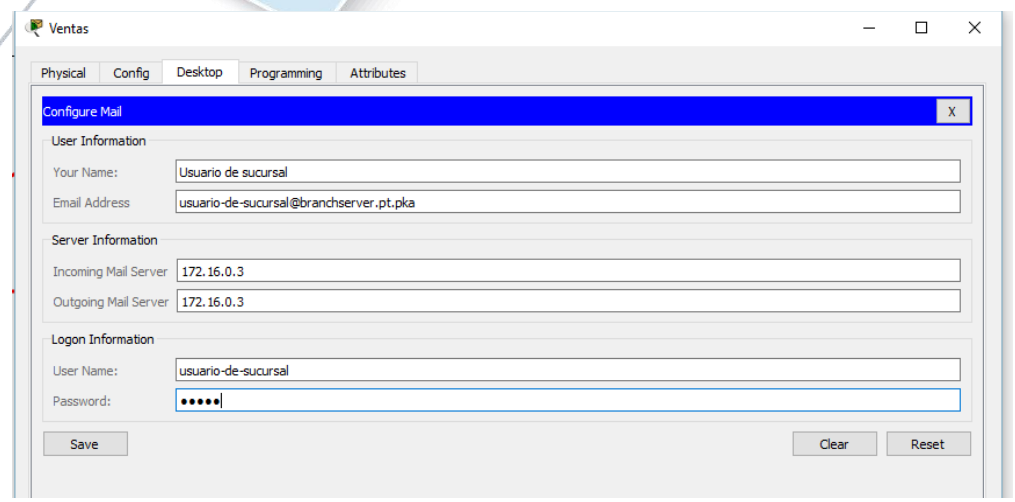
3) Incoming Mail Server (Servidor de correo entrante): **172.16.0.3**

4) Outgoing Mail Server (Servidor de correo saliente): **172.16.0.3**

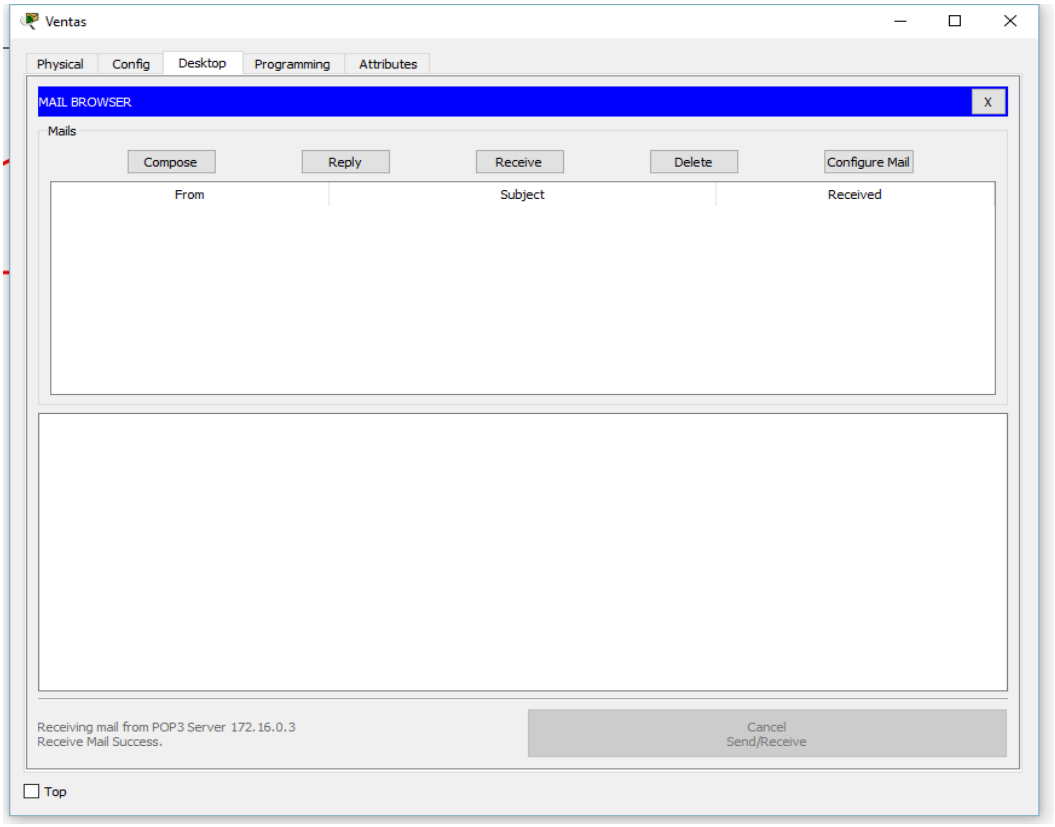
5) User Name (Nombre de usuario): **usuario-de-sucursal**

6) Password (Contraseña): **cisco**

c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.



d. Haga clic en **Receive** (Recibir). Si todo se configuró correctamente tanto en el cliente como en el servidor, la ventana del explorador de correo muestra la confirmación de mensaje `Receive Mail Success` (La función Recibir correo se realizó correctamente).



e. Esta actividad debe completarse en un 100%. No cierre la ventana de configuración de Sales ni la ventana del explorador de correo.

Paso 5: Envíe un correo electrónico desde el cliente Sales y el cliente PC3.

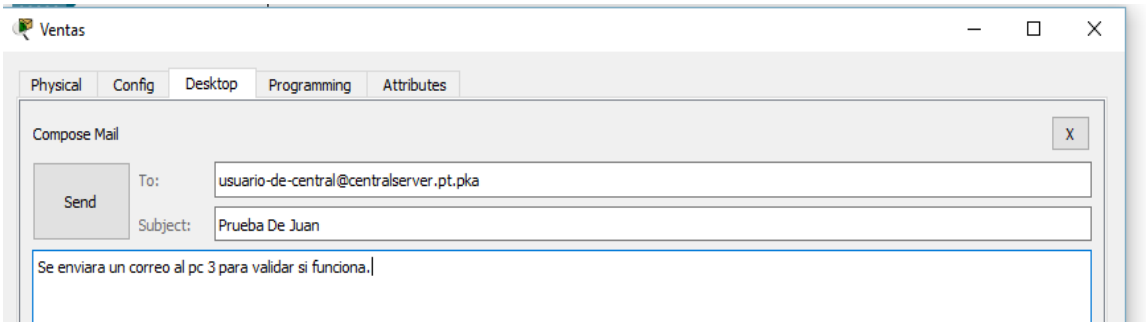
a. Desde la ventana del **explorador de correo** de **Sales**, haga clic en **Compose** (Redactar). b. Introduzca los siguientes valores en los campos correspondientes:

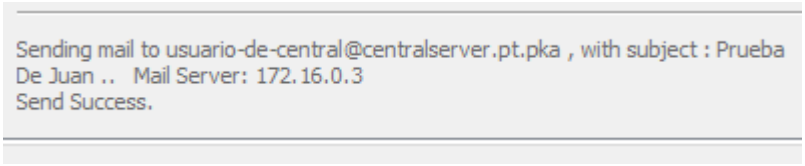
1) To (Para): **usuario-de-central@centralserver.pt.pka**

2) Subject (Asunto): *Personalice el asunto*.

3) **Email** body (Cuerpo del correo electrónico): *Personalice el correo electrónico*.

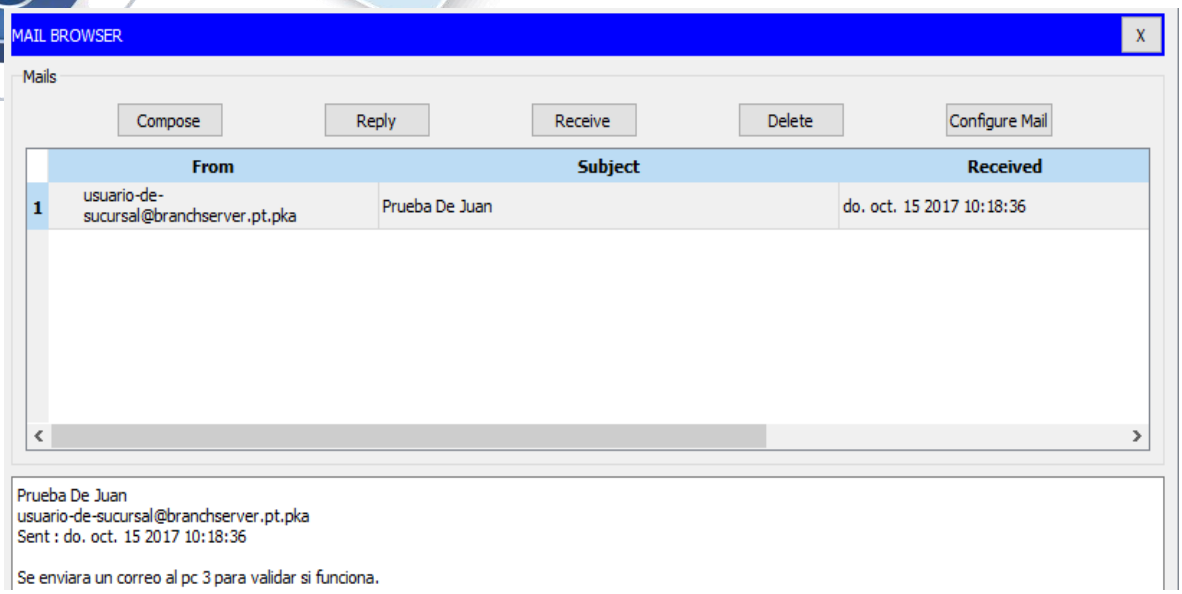
c. Haga clic en **Send** (Enviar).





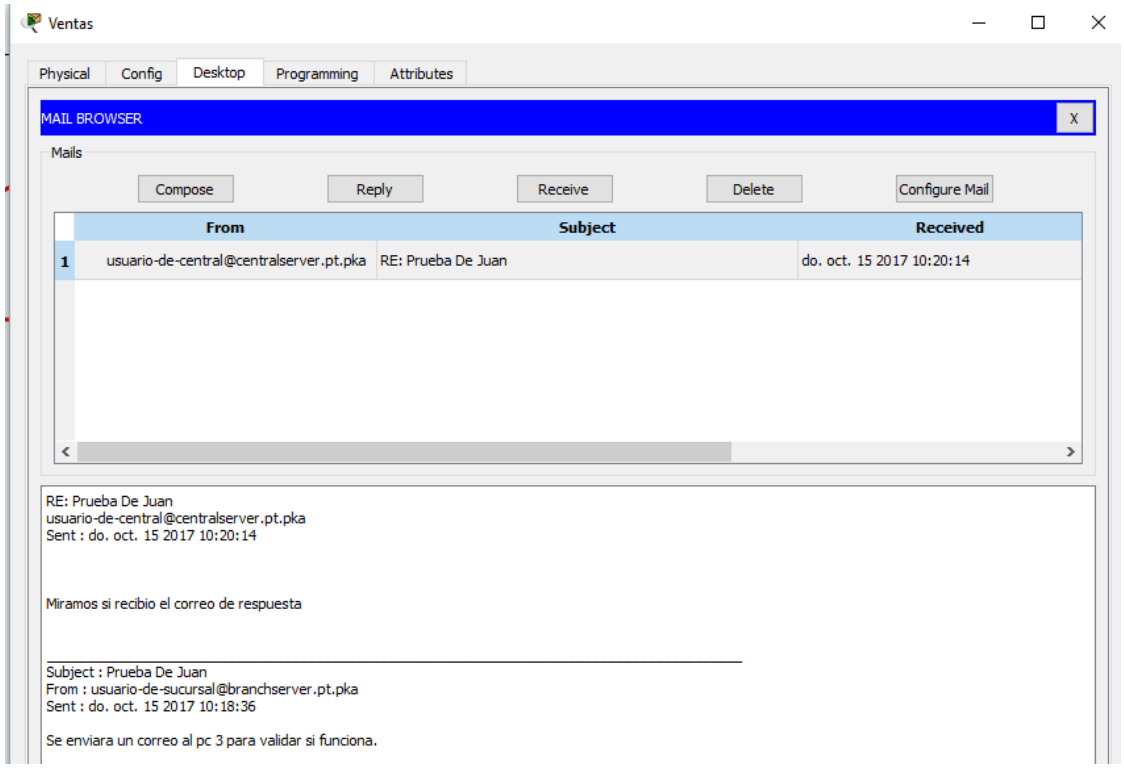
Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

Haga clic en **Receive** (Recibir). Aparece un correo electrónico proveniente de Sales. Haga doble clic en el correo electrónico.



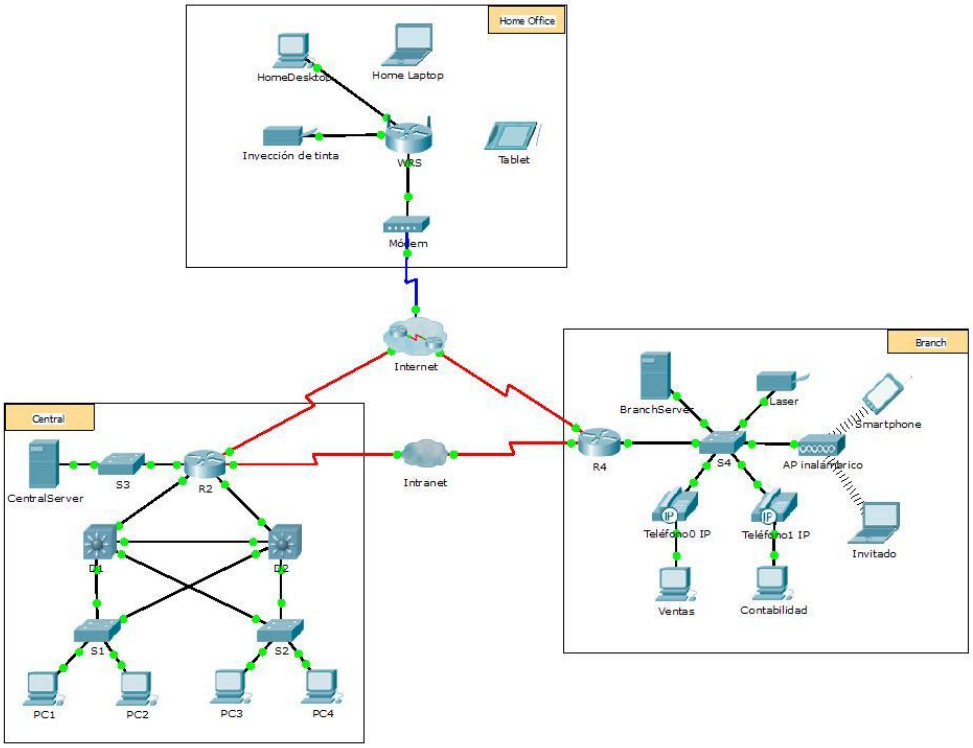
f. Haga clic en **Reply** (Responder), personalice una respuesta y haga clic en **Send**.

g. Verifique que **Sales** haya recibido la respuesta.



Ejercicio 10.2.2.8: Servidores de DHCP y servidores DNS

Topología



Objetivos

Parte 1: Configurar el direccionamiento IPv4 estático

Parte 2: Configurar y verificar los registros DNS

Información básica

En esta actividad, configurará y verificará el direccionamiento IP estático y el direccionamiento DHCP. A continuación, configurará un servidor DNS para que asigne direcciones IP a los nombres de sitios Web.

Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de DHCP y DNS tiene sus propias instrucciones exclusivas de configuración e instalación.

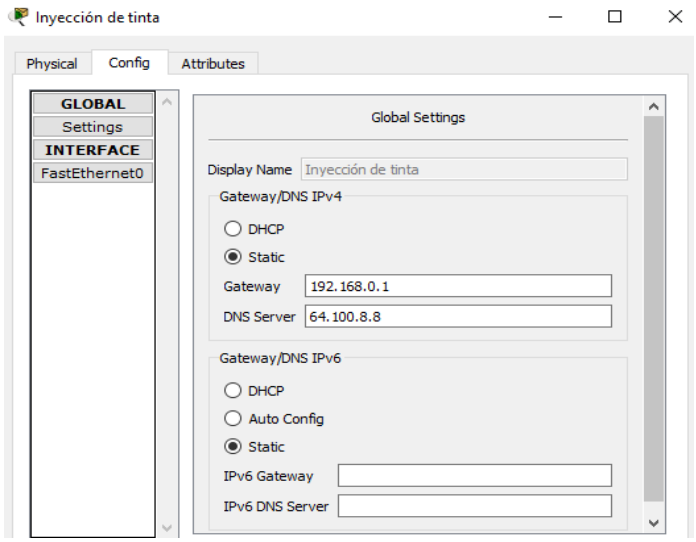
Parte 1: Configurar el direccionamiento IPv4 estático

Paso 1: Configurar la impresora de inyección de tinta con direccionamiento IPv4 estático

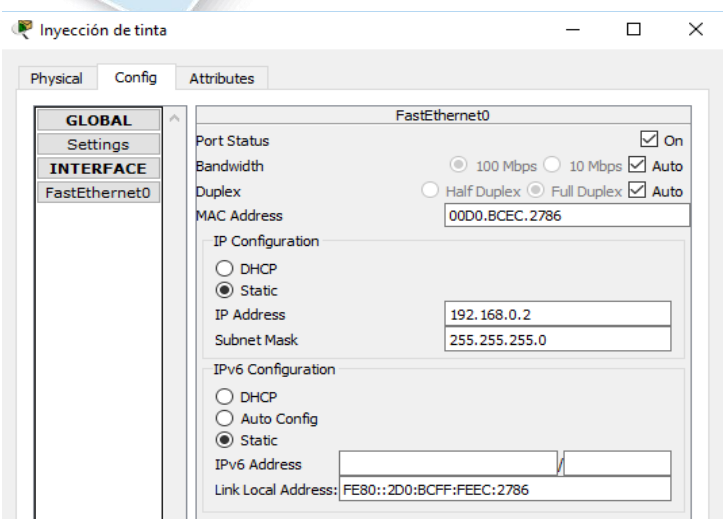
Las PC de oficinas domésticas necesitan conocer la dirección IPv4 de una impresora para enviarle información. Por lo tanto, la impresora debe utilizar una dirección IPv4 estática (invariable).

- Haga clic en **Inkjet** (Inyección de tinta) y, a continuación, haga clic en la ficha **Config**, en la que se muestran los parámetros de Global Settings (Configuración global).

- Asigne de manera estática la dirección de gateway **192.168.0.1** y la dirección de servidor DNS **64.100.8.8**.



Haga clic en **FastEthernet0** y asigne de manera estática la dirección IP **192.168.0.2** y la dirección de máscara de subred **255.255.255.0**.



- Cierre la ventana Inkjet.

Paso 2: Configurar WRS para que proporcione servicios de DHCP

l. Haga clic en **WRS** y, a continuación, haga clic en la ficha **GUI** y maximice la ventana.

m. Se muestra la ventana Basic Setup (Configuración básica) de manera predeterminada. Configure los siguientes parámetros en la sección Network Setup (Configuración de red):

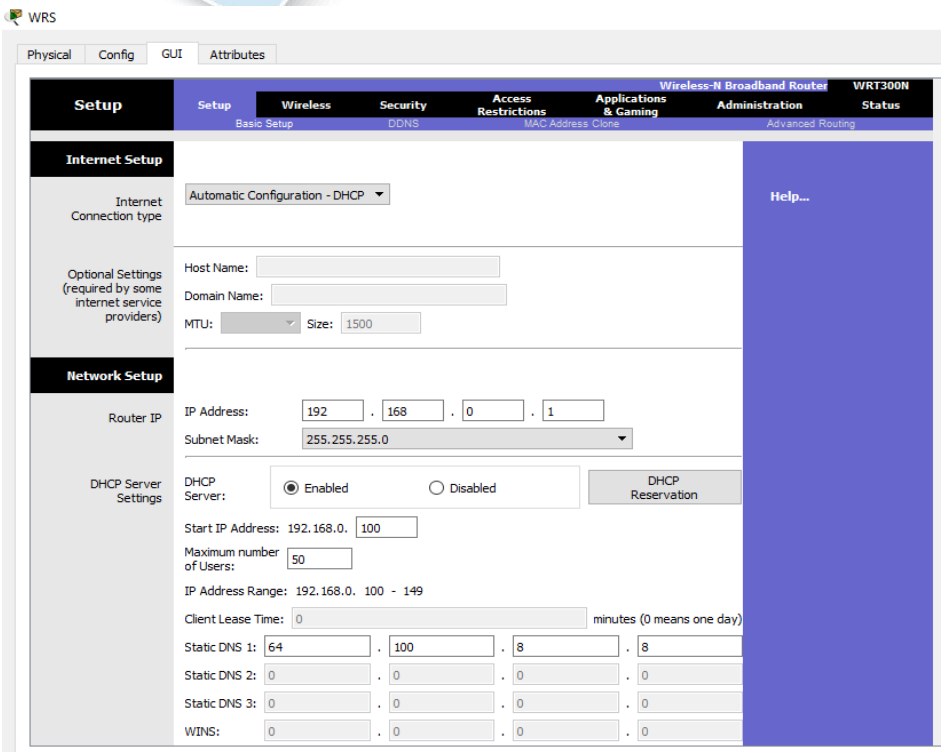
Cambie la Dirección IP a **192.168.0.1**.

Establezca la máscara de subred **255.255.255.0**.

Habilite el servidor de DHCP.

Establezca la dirección DNS estática 1 **64.100.8.8**.

Desplácese hasta la parte inferior y haga clic en **Save** (Guardar).



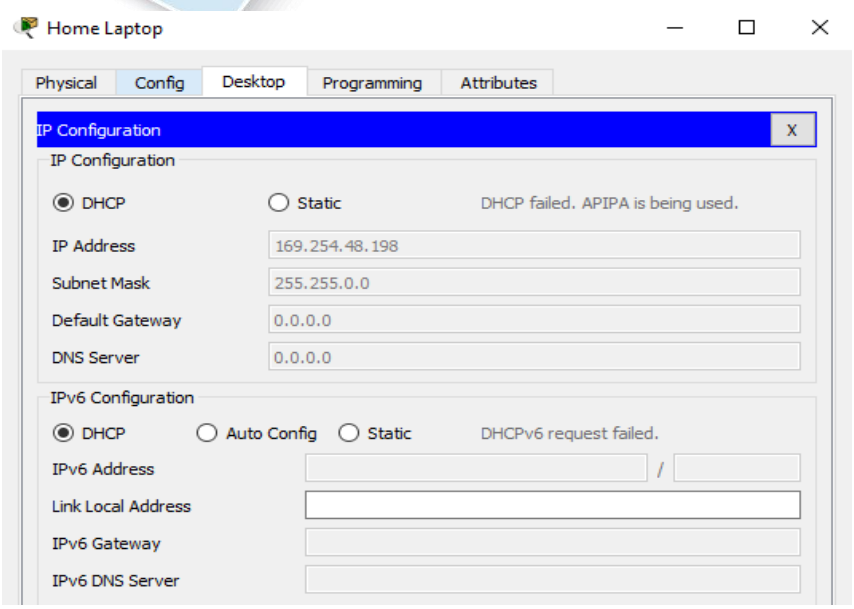
n. Cierre la ventana **WRS**.

Paso 3: Solicitar direccionamiento DHCP para la computadora portátil doméstica

Esta actividad se centra en la oficina doméstica. Los clientes que configurará con DHCP son **Home Laptop** (Computadora portátil doméstica) y **Tablet PC**.

a. Haga clic en **Home Laptop** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.



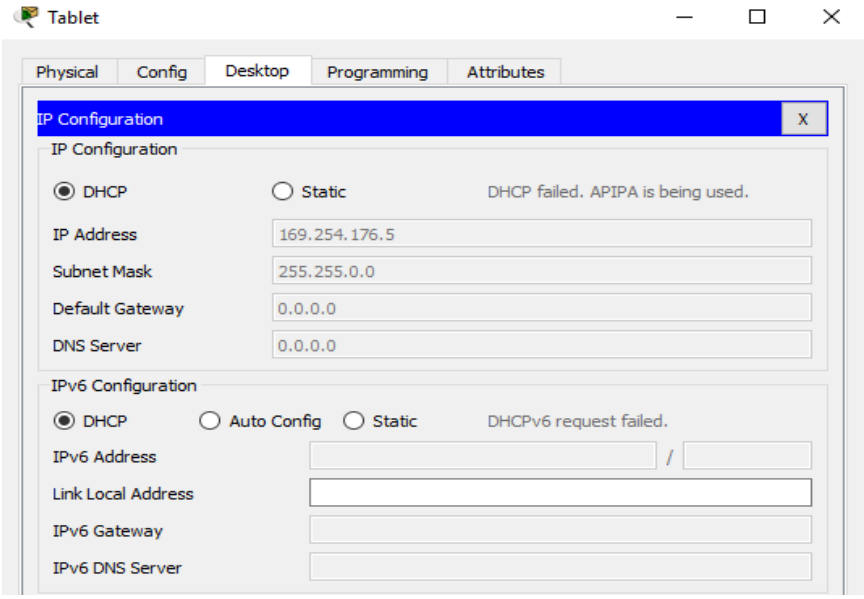
c. Ahora, **Home Laptop** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

d. Cierre la ventana IP Configuration y, a continuación, cierre la ventana **Home Laptop**.

Paso 4: Solicitar direccionamiento DHCP para la tablet PC

a. Haga clic en **Tablet** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration**.

b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.

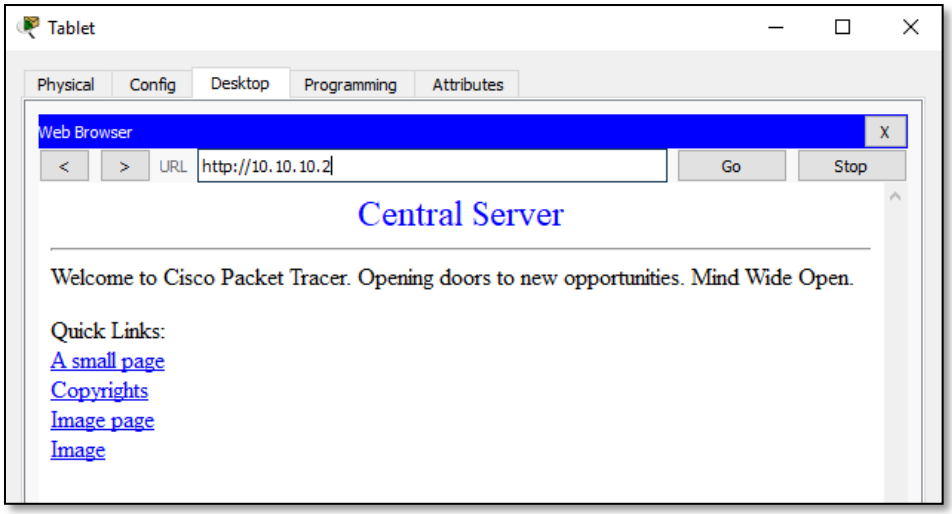


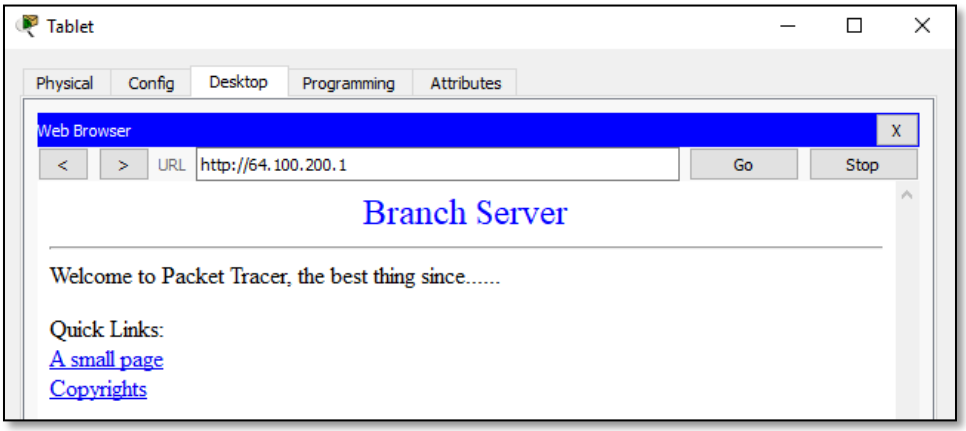
c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

Paso 5: Probar el acceso a sitios Web

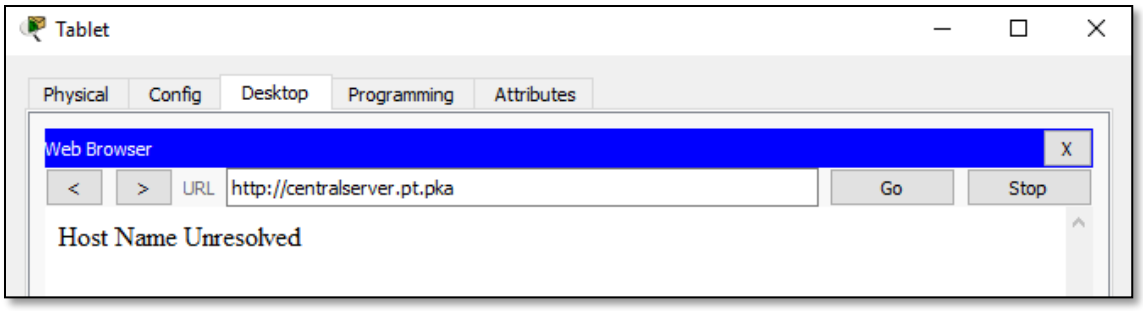
a. Cierre la ventana **IP Configuration** y, a continuación, haga clic en Web Browser (Explorador Web).

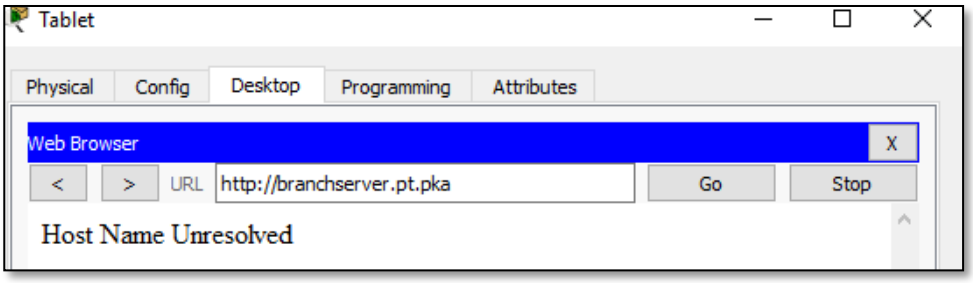
b. En el cuadro de dirección URL, escriba **10.10.10.2** (para el sitio Web de **CentralServer**) o **64.100.200.1** (para el sitio web de **BranchServer**) y haga clic en **Go** (Ir). Deben aparecer ambos sitios Web.





c. Vuelva a abrir el explorador Web. Pruebe los nombres para esos mismos sitios Web mediante la introducción de **centralserver.pt.pka** y **branchserver.pt.pka**. Haga clic en **Fast Forward Time** (Adelantar el tiempo) en la barra amarilla que se encuentra debajo de la topología, a fin de acelerar el proceso.
Con los nombres no genera conexión al sitio.



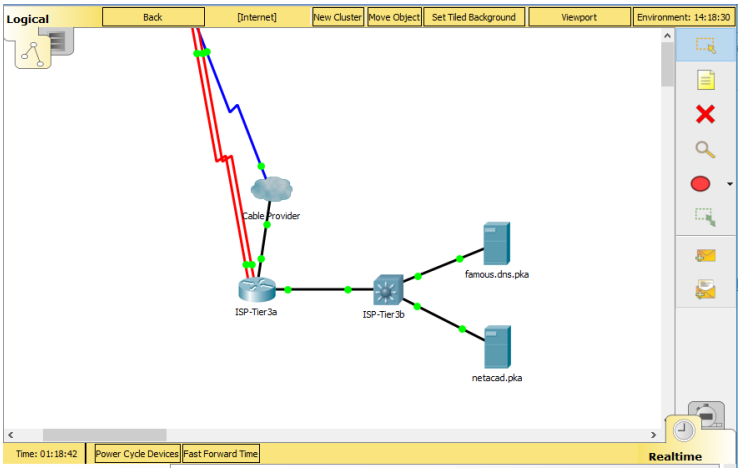


Parte 2: Configurar los registros en el servidor DNS

Paso 1: Configurar famous.dns.pka con registros para CentralServer y BranchServer.

En general, los registros DNS se realizan ante compañías, pero en esta actividad, usted controla el servidor **famous.dns.pka** en Internet.

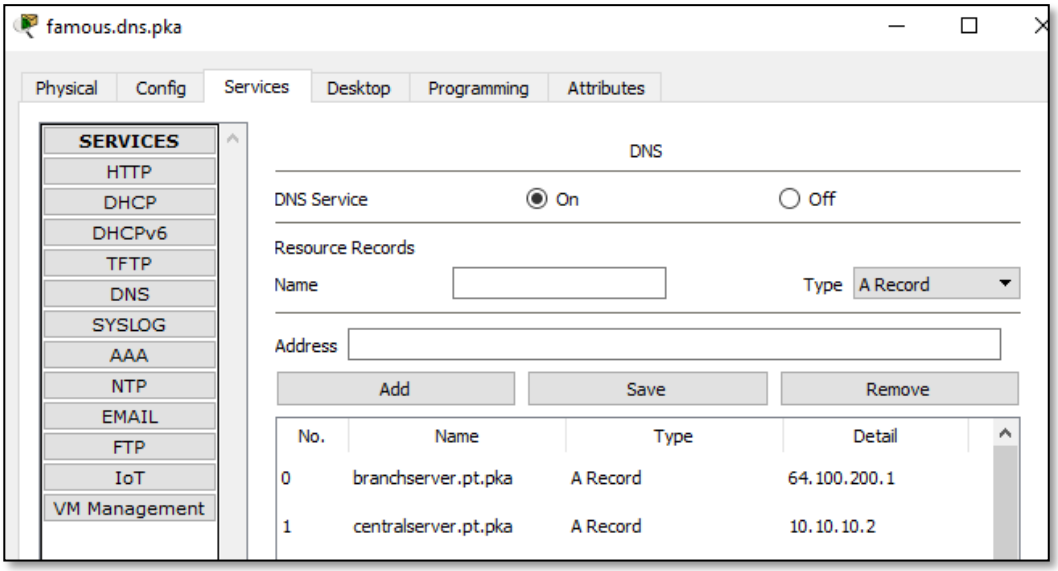
a. Haga clic en la nube de **Internet**. Se muestra una nueva red.



b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config** > **DNS**. c. Agregue los siguientes registros del recurso:

Nombre de registro del recurso	Dirección
centralserver.pt.pka	10.10.10.2.
branchserver.pt.pka	64.100.200.1

d. Cierre la ventana famous.dns.pka.



e. Haga clic en **Back** (Atrás) para salir de la nube de **Internet**.

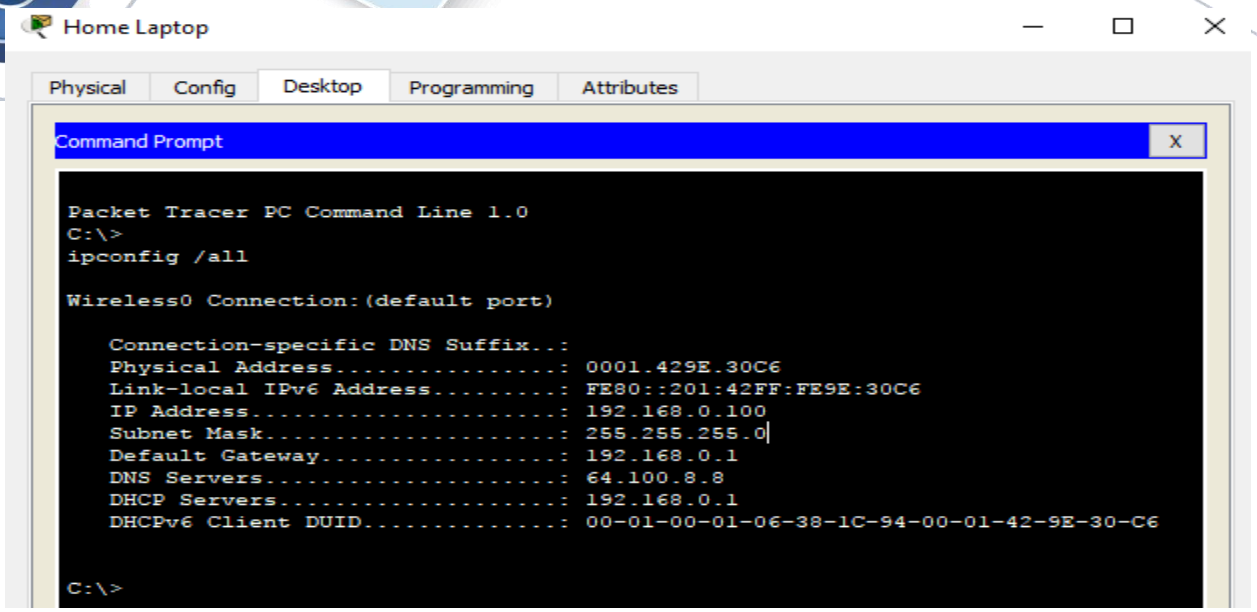
Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

Ahora que configuró los registros DNS, **Home Laptop** y **Tablet** deben ser capaces de acceder a los sitios Web mediante los nombres en lugar de las direcciones IP. Primero, compruebe que el cliente DNS funcione correctamente y, a continuación, verifique el acceso al sitio Web.

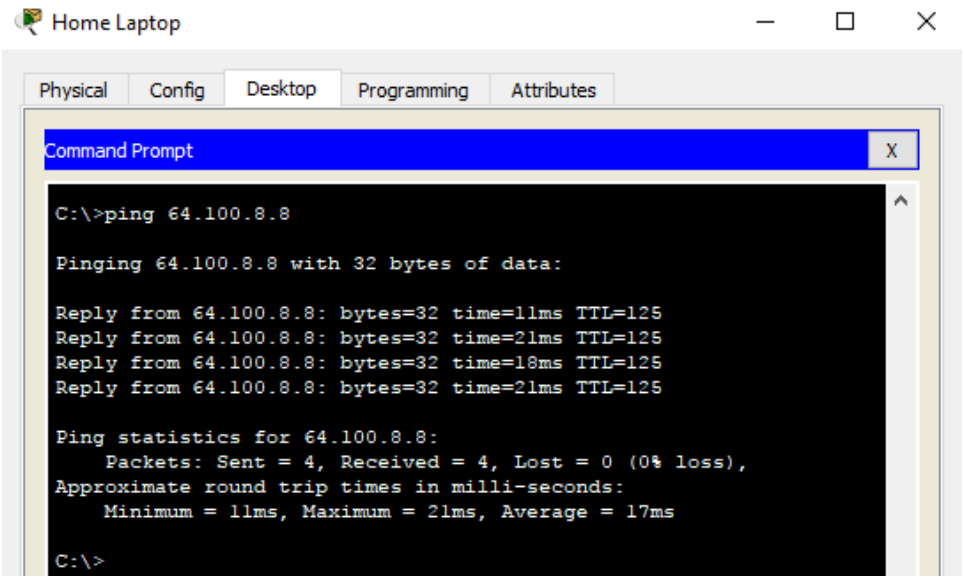
a. Haga clic en **Home Laptop** o **Tablet**.

b. Si el explorador Web está abierto, ciérrelo y seleccione **Command Prompt** (Símbolo del sistema).

c. Verifique el direccionamiento IPv4 mediante la introducción del comando **`ipconfig /all`**. Debe ver la dirección IP del servidor DNS.

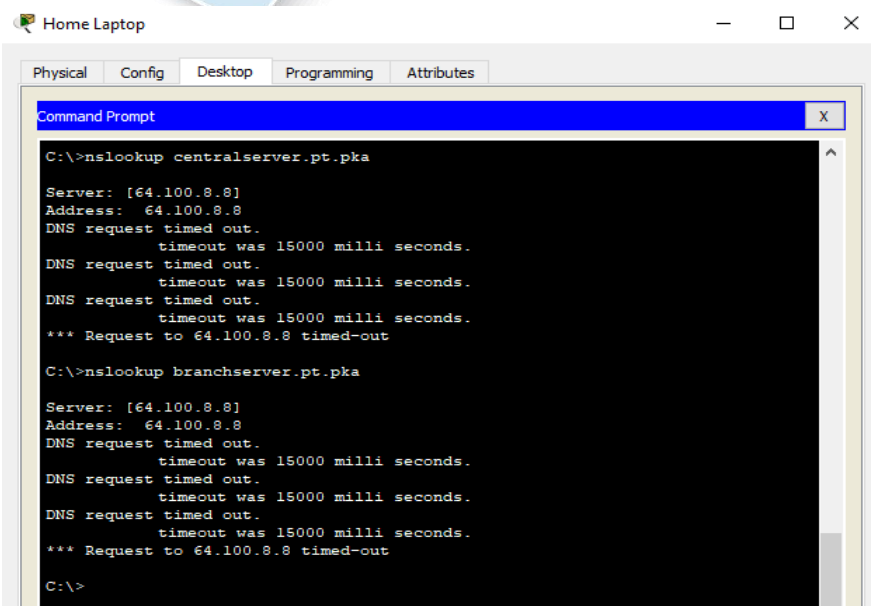


d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.

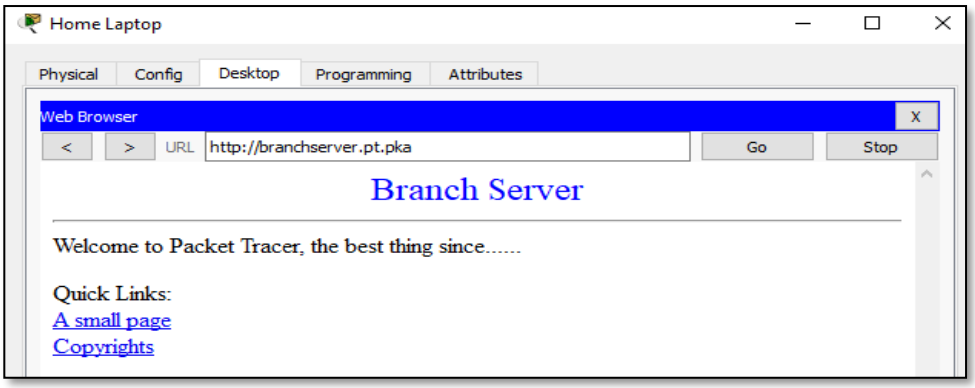


Nota: es posible que los primeros dos o tres pings fallen, ya que Packet Tracer simula los distintos procesos que deben ocurrir para que la conectividad a un recurso remoto sea correcta.

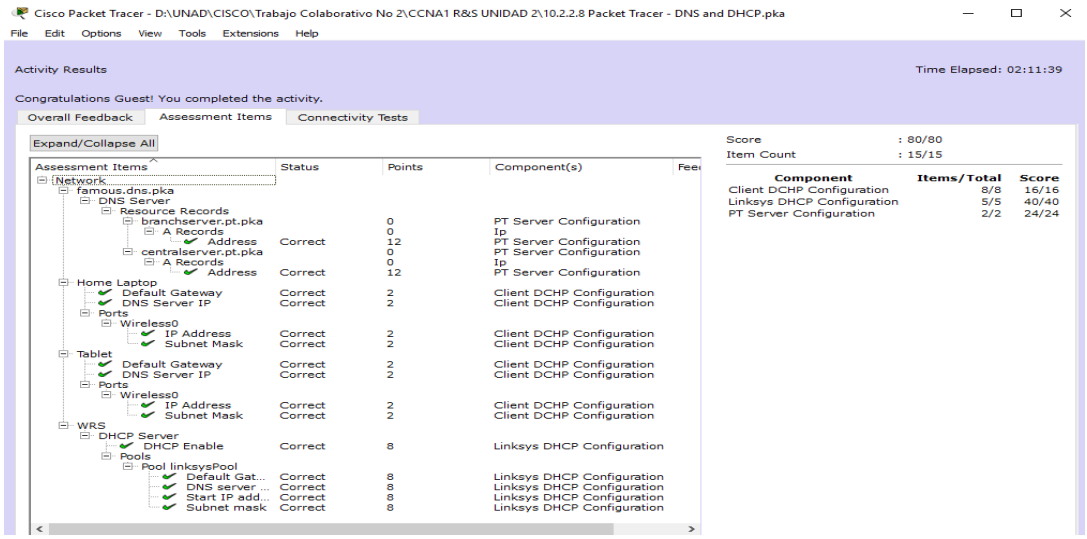
e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos **`nslookup centralserver.pt.pka`** y **`nslookup branchserver.pt.pka`**. Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.



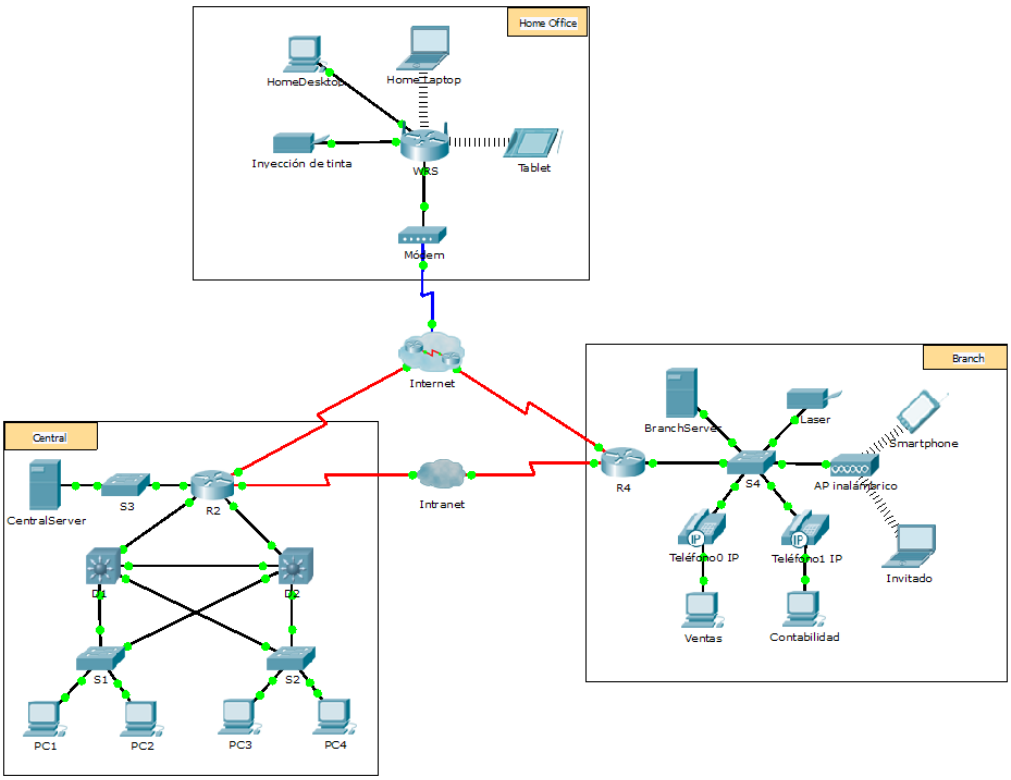
f. Cierre la ventana Command Prompt y haga clic en **Web Browser**. Verifique que **Home Laptop** o **Tablet** puedan acceder ahora a las páginas Web de **CentralServer** y **BranchServer**.



Ítems Desarrollados


Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\10.2.2.8 Packet Tracer - DNS and DHCP.pka
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 02:11:39
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Component(s)
Network
famous.dns.pka
DNS Server
Resource Records
branchserver.pt.pka
0
PT Server Configuration
A Records
0
Ip
Address
Correct
12
PT Server Configuration
centralserver.pt.pka
0
PT Server Configuration
A Records
0
Ip
Address
Correct
12
PT Server Configuration
Home Laptop
Default Gateway
Correct
2
Client DCHP Configuration
DNS Server IP
Correct
2
Client DCHP Configuration
Ports
Wireless0
IP Address
Correct
2
Client DCHP Configuration
Subnet Mask
Correct
2
Client DCHP Configuration
Tablet
Default Gateway
Correct
2
Client DCHP Configuration
DNS Server IP
Correct
2
Client DCHP Configuration
Ports
Wireless0
IP Address
Correct
2
Client DCHP Configuration
Subnet Mask
Correct
2
Client DCHP Configuration
WRS
DHCP Server
DHCP Enable
Correct
8
Linksys DHCP Configuration
Pools
Pool linksysPool
Default Gat...
Correct
8
Linksys DHCP Configuration
DNS server ...
Correct
8
Linksys DHCP Configuration
Start IP add...
Correct
8
Linksys DHCP Configuration
Subnet mask
Correct
8
Linksys DHCP Configuration
Score : 80/80
Item Count : 15/15
Component
Items/Total
Score
Client DCHP Configuration
8/8
16/16
Linksys DHCP Configuration
5/5
40/40
PT Server Configuration
2/2
24/24

Ejercicio 10.2.3.2: Servidores FTP



Objetivos

Parte 1: Configurar servicios FTP en los servidores
Parte 2: Subir un archivo al servidor FTP
Parte 3: Descargar un archivo del servidor FTP

Información básica

En esta actividad, configurará servicios FTP. Luego, utilizará los servicios FTP para transferir archivos entre los clientes y el servidor.

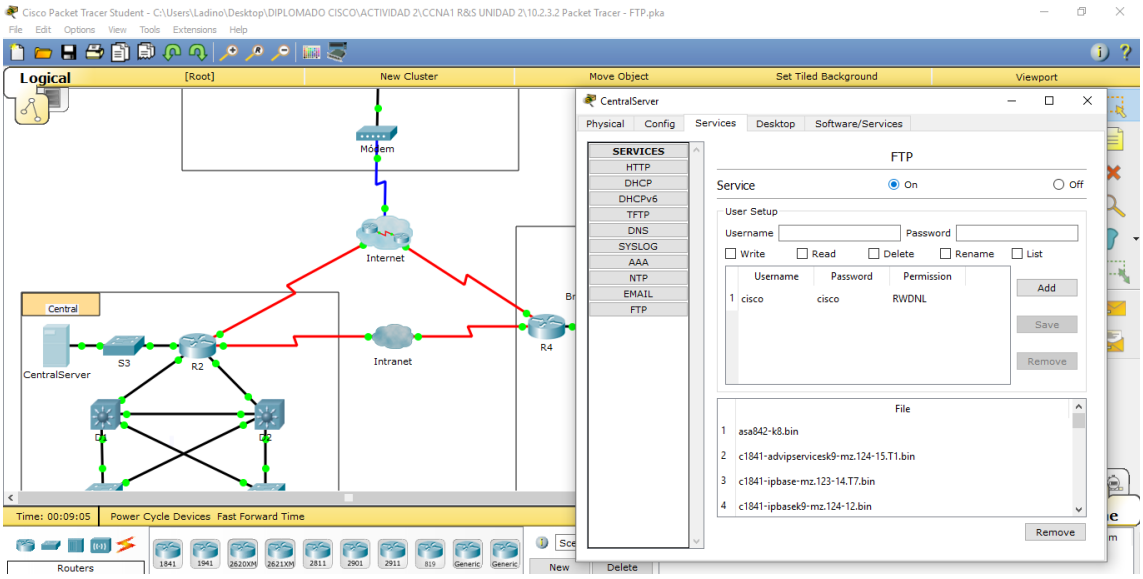
Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de servidor y cliente FTP tiene sus propias instrucciones exclusivas de configuración e instalación. La primera vez que intente conectarse a una dirección Web, Packet Tracer tardará varios

Parte 1: Configurar servicios FTP en los servidores

Paso 1: Configurar el servicio FTP en CentralServer

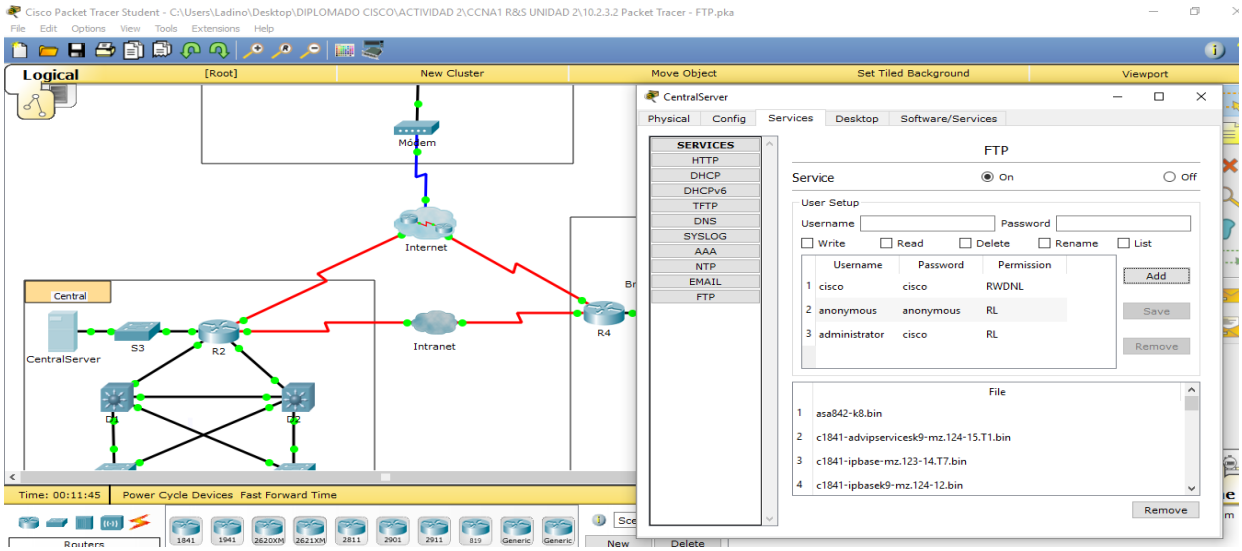
a. Haga clic en **CentralServer** > ficha **Config** > **FTP**.

b. Haga clic en **On** (Activar) para habilitar el servicio FTP.

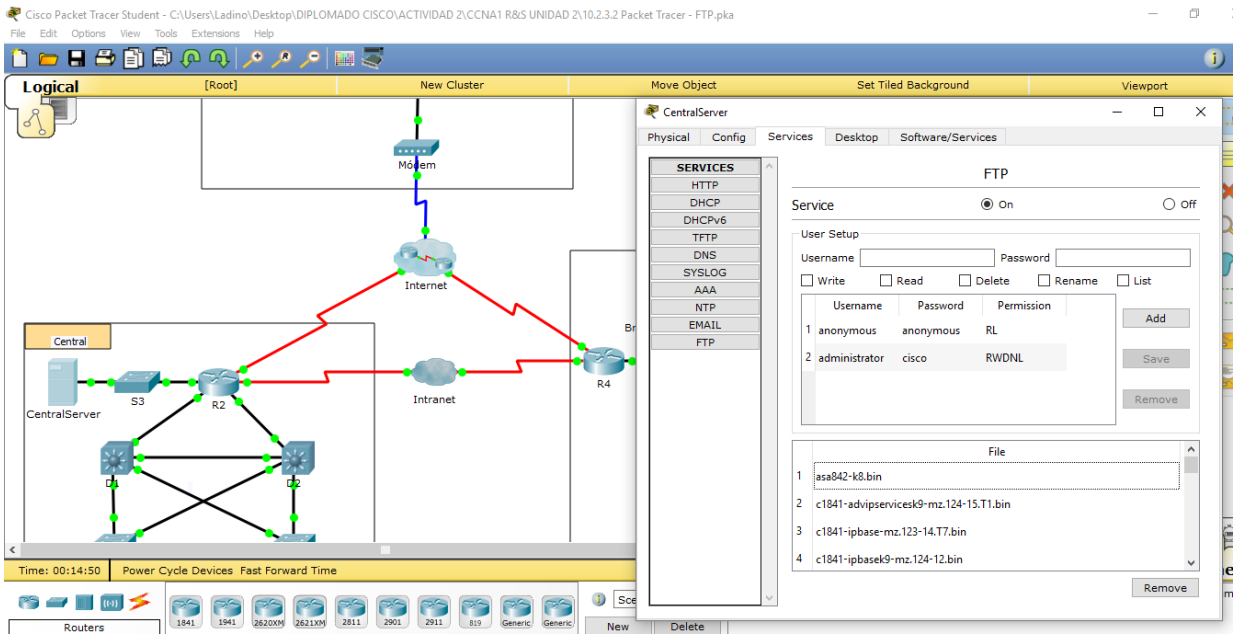


c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario. Haga clic en el botón **+** para agregar la cuenta:

Nombre de usuario	Contraseña	Permisos
anonymous	anonymous	limitado a **Read** (Lectura) y **List** (Lista)
administrator	cisco	permiso total

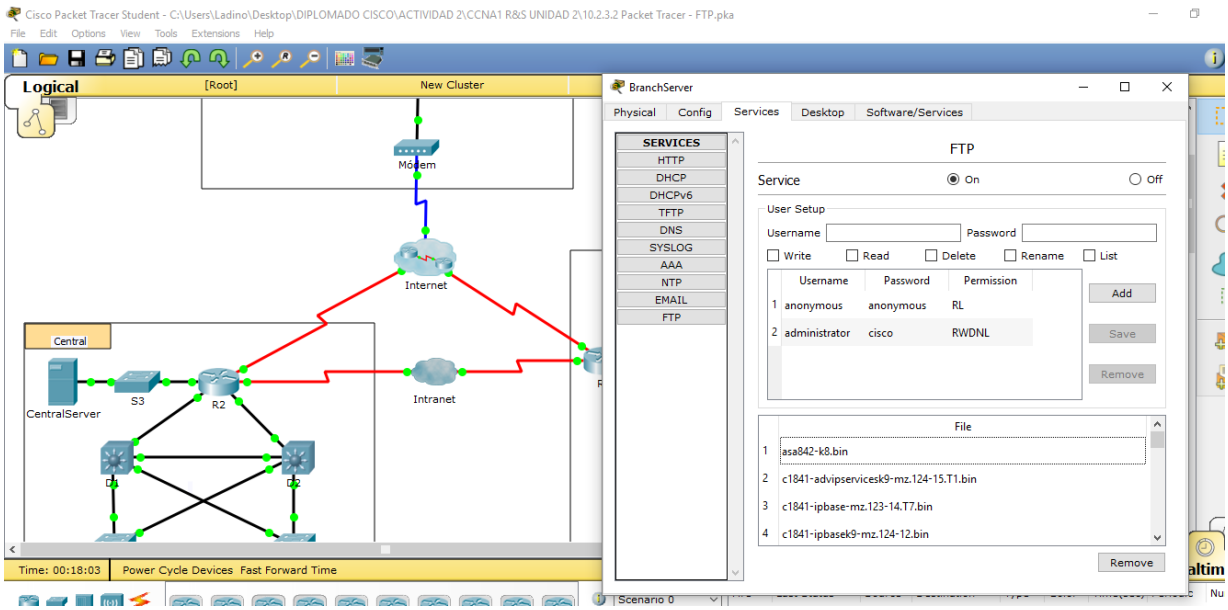


e. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón **-** para eliminarla. Cierre la ventana de configuración de la CentralServer.



Paso 2: Configurar el servicio FTP en BranchServer

Repita el paso 1 en **BranchServer**



Parte 2: Subir un archivo al servidor FTP

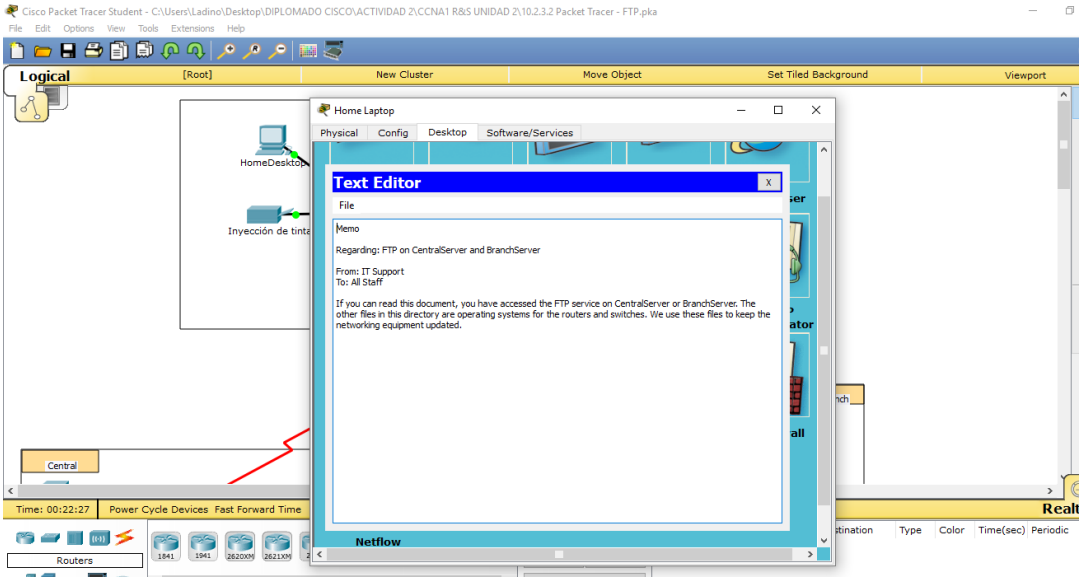
Paso 1: Transferir el archivo README.txt de la computadora portátil doméstica a CentralServer

Como administrador de red, debe colocar un aviso en los servidores FTP. El documento se creó en la computadora portátil doméstica y se debe subir a los servidores FTP.

a. Haga clic en **Home Laptop** (Computadora portátil doméstica) y, a continuación, haga clic en la ficha **Desktop** > **Text Editor** (Escritorio > Editor de texto).

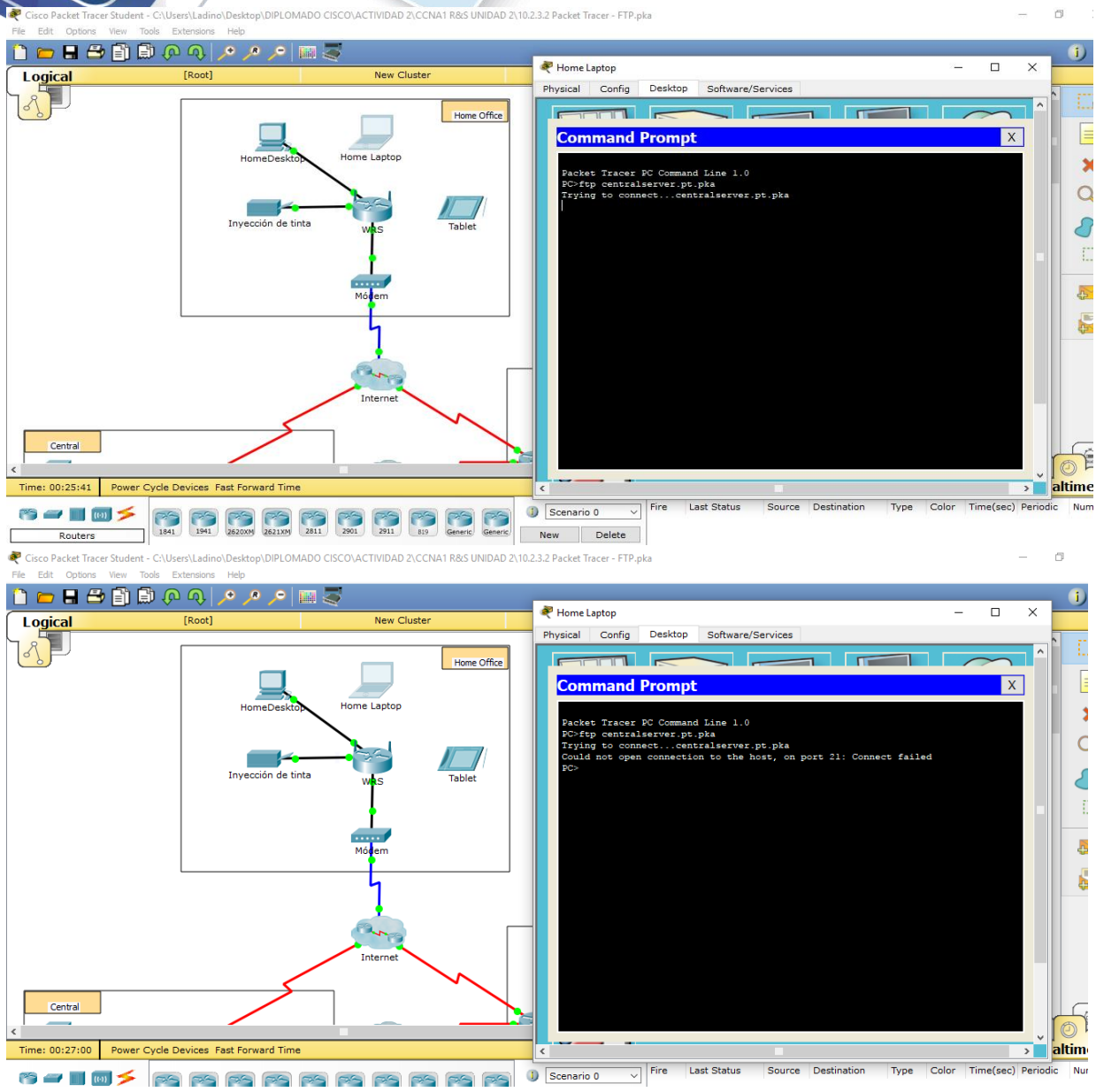
b. Abra el archivo **README.txt** y revíselo. Cierre **Text Editor** cuando haya terminado.

Nota: no modifique el archivo porque esto afecta la puntuación.

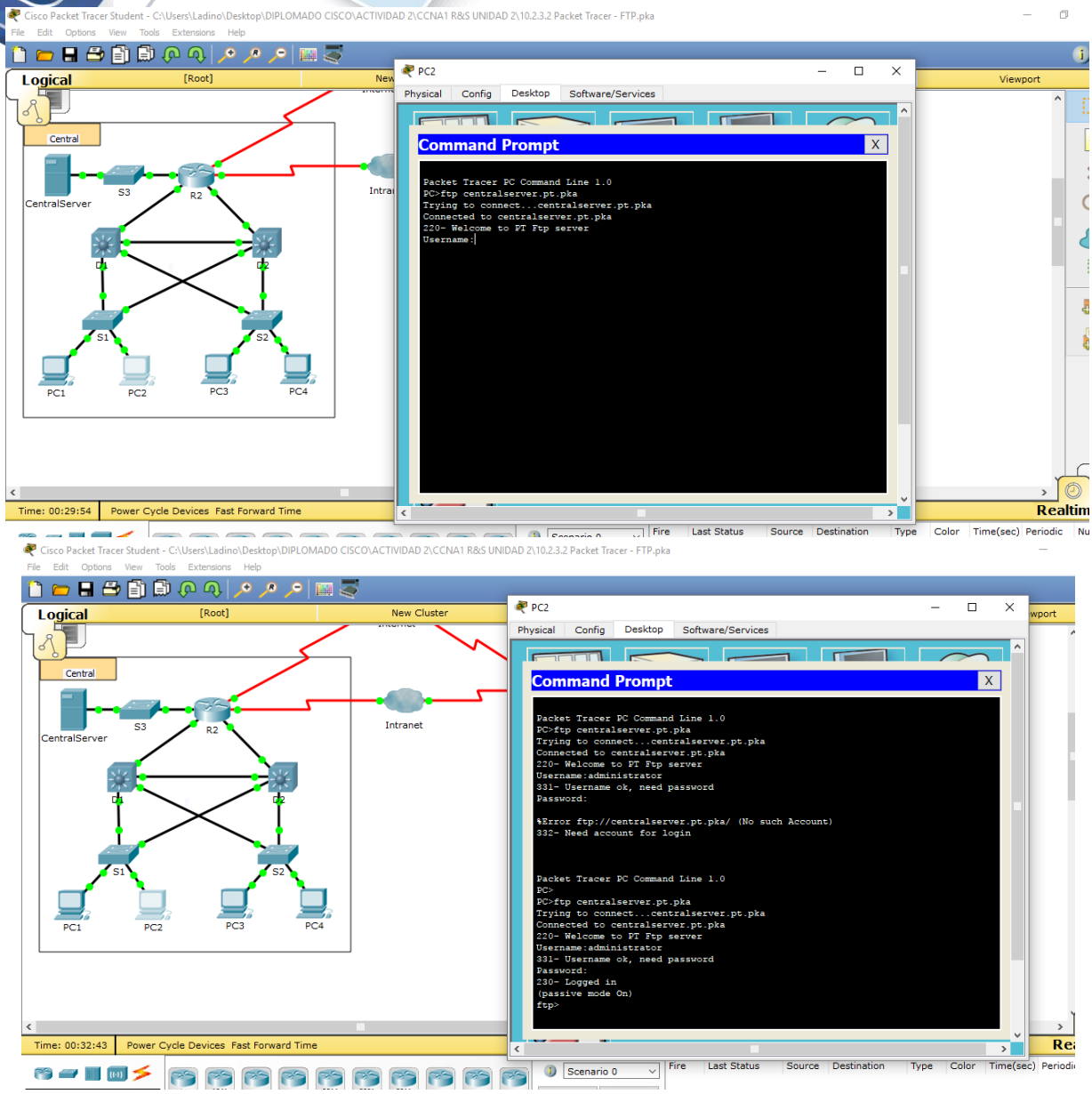


c. En la ficha **Desktop**, abra la ventana del símbolo del sistema y siga estos pasos: 1) Escriba **`ftp centralserver.pt.pka`**. Espere algunos segundos mientras se conecta el cliente.

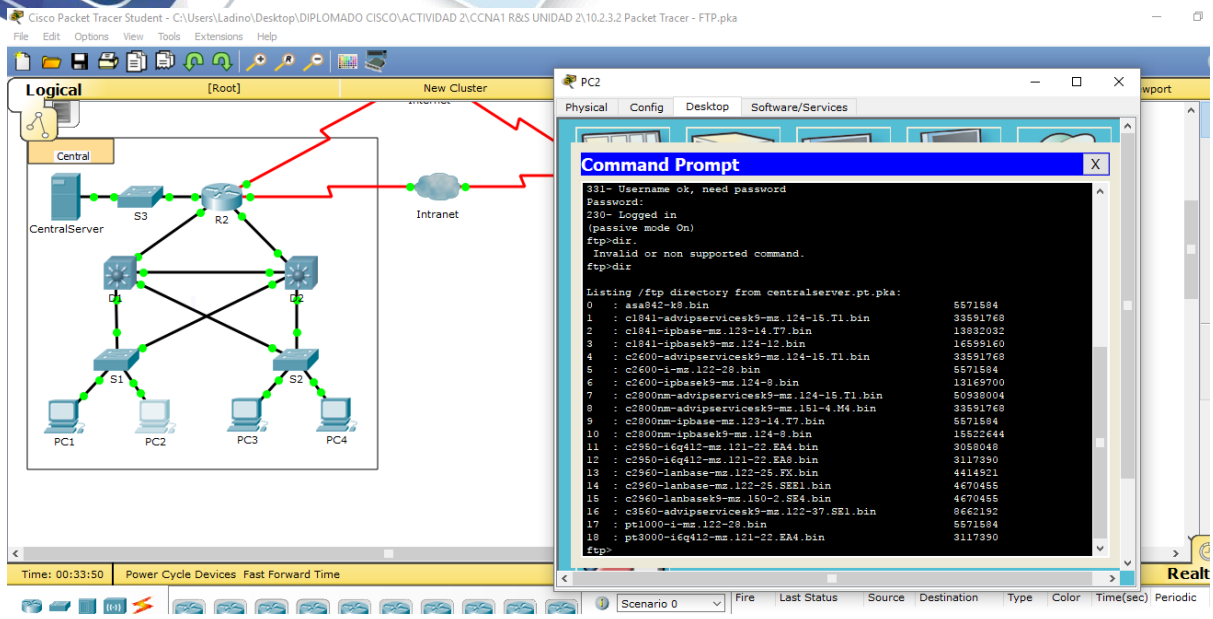
Nota: dado que Packet Tracer es una simulación, FTP puede tardar hasta 30 segundos en conectarse la primera vez.



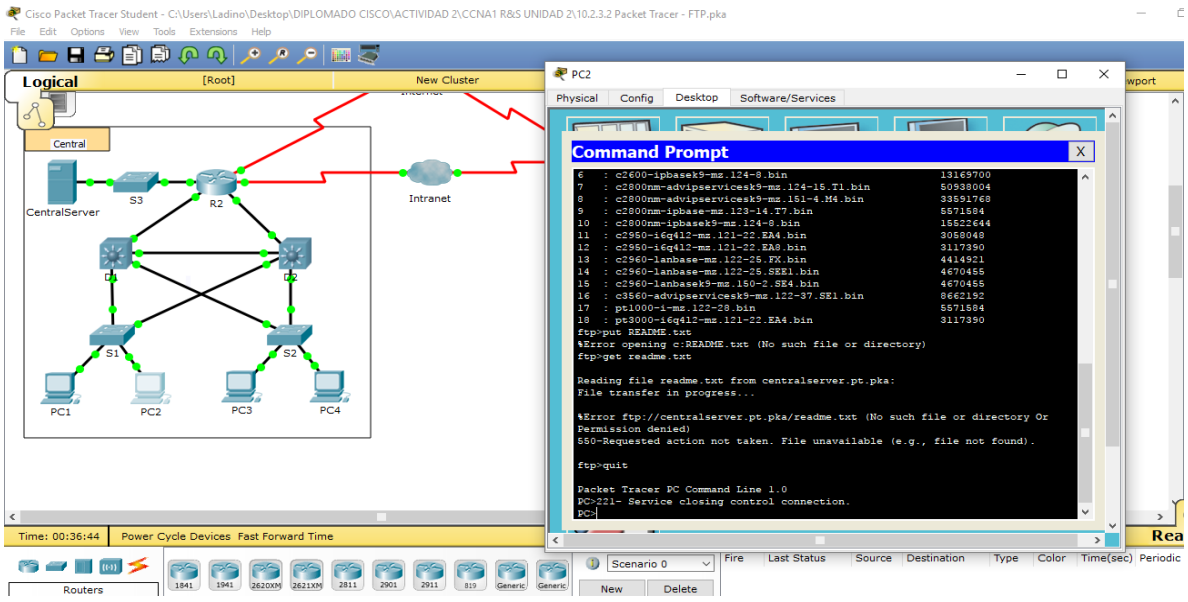
2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **administrator** (administrador).



3) La petición de entrada cambia a ftp>. Enumere el contenido del directorio escribiendo **dir.** Se muestra el directorio de archivos en **CentralServer**.



4) Transfiera el archivo README.txt: en la petición de entrada ftp>, escriba **put README.txt**. El archivo README.txt se transfiere de la computadora portátil doméstica a **CentralServer**.
5) Para verificar la transferencia del archivo, escriba **dir**. El archivo README.txt ahora figura en el directorio de archivos.
6) Cierre el cliente FTP escribiendo **quit**. La petición de entrada se revierte a PC>.



Paso 2: Transferir el archivo README.txt de la computadora portátil doméstica a BranchServer
a. Repita el paso 1c para transferir el archivo README.txt a **branchserver.pt.pka**.

b. Cierre las ventanas Command Prompt (Símbolo del sistema) y Home Laptop.

Parte 3: Descargar un archivo del servidor FTP

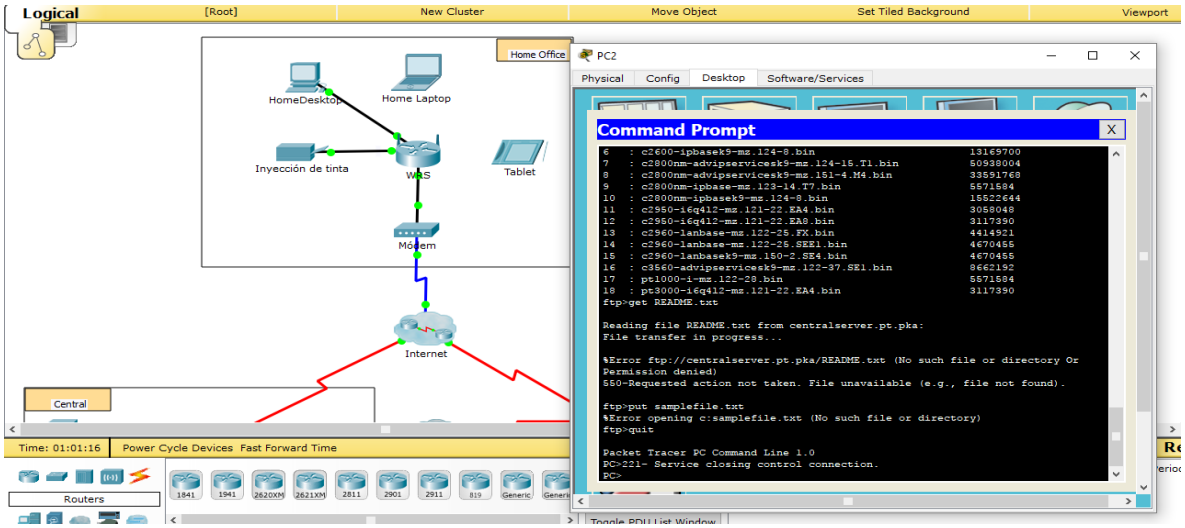
Paso 1: Transferir README.txt de CentralServer a la PC2 a. Haga clic en **PC2** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**. 1) Escriba **`ftp centralserver.pt.pka`**.

2) El servidor pide un nombre de usuario y una contraseña. Utilice las credenciales de la cuenta **anonymous** (anónimo)

3) La petición de entrada cambia a `ftp>`. Enumere el contenido del directorio escribiendo **`dir.`** El archivo README.txt figura en la parte superior de la lista del directorio.

4) Descargue el archivo README.txt: en la petición de entrada ftp>, escriba **`get README.txt`**. El archivo README.txt se transfiere a la **PC2**.

5) Verifique que la cuenta **anonymous** no tenga permiso para escribir archivos en **CentralServer** escribiendo **`put sampleFile.txt`**. Se muestra el siguiente mensaje de error:




```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...
%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

6) Cierre el cliente FTP escribiendo **`quit`**. La petición de entrada se revierte a `PC>`.

7) Para verificar la transferencia del archivo a la PC2, escriba **`dir`**. El archivo README.txt figura en el directorio.

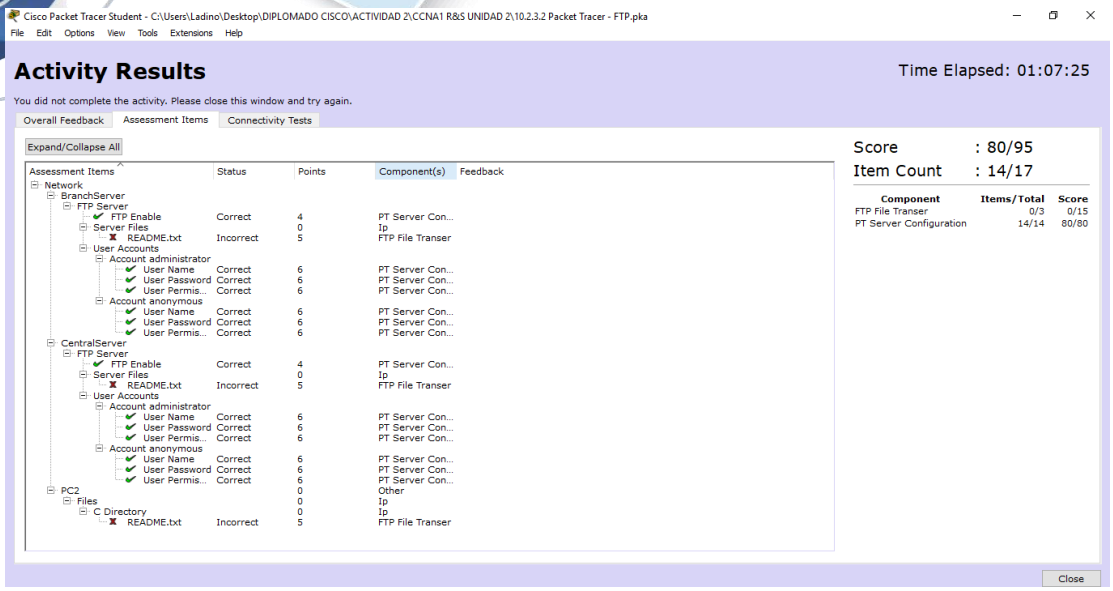
8) Cierre la ventana de línea de comandos.

b. En la ficha **Desktop**, abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.

c. Cierre **Text Editor** y, luego, cierre la ventana de configuración de la PC2.

Paso 2: Transferir el archivo README.txt de BranchServer al smartphone

Repita el paso 1 para **Smart Phone**, excepto la descarga del archivo README.txt desde **branchserver.pt.pka**.



Ejercicio 10.4.1.2: Función Multiusuario de Packet Tracer: Tutorial

Topología

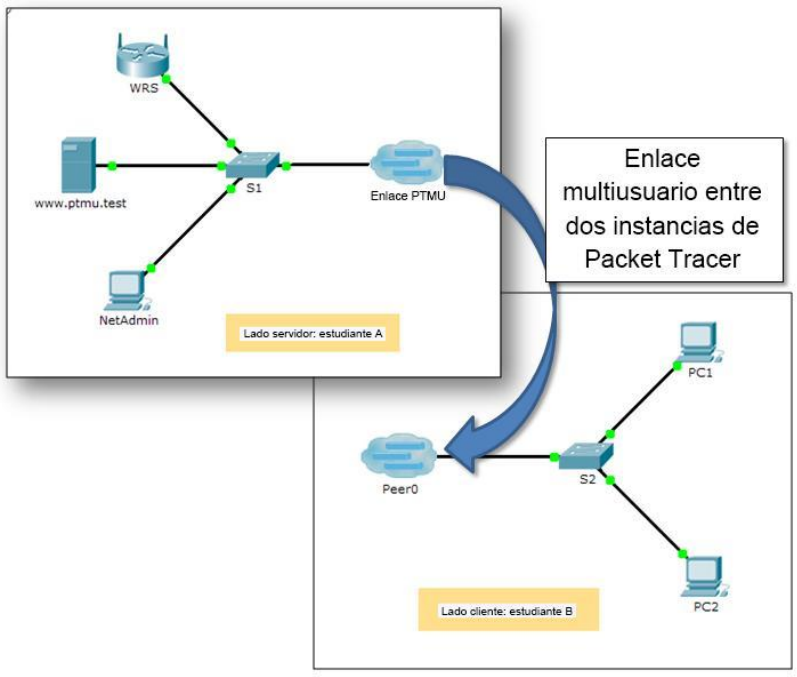


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred	Servidor DNS
www.ptmu.test	10.10.10.1	255.0.0.0	10.10.10.1
PC	10.10.10.10	255.0.0.0	10.10.10.1

Objetivos

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

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

Información básica

La característica Multiusuario de Packet Tracer permite varias conexiones punto a punto entre diversas instancias de Packet Tracer. Esta primera actividad de la función Multiusuario de Packet Tracer (PTMU, Packet Tracer Multiuser) es un tutorial rápido que muestra los pasos para establecer y verificar una conexión multiusuario a otra instancia de Packet Tracer dentro de la misma LAN. Idealmente, esta actividad está pensada para dos estudiantes. Sin embargo, también se puede realizar como actividad individual abriendo los dos archivos independientes para crear dos instancias distintas de Packet Tracer en su máquina local.

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

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

- 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 - Tutorial - Server Side.pka.**

  El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Tutorial - Client Side.pka.**

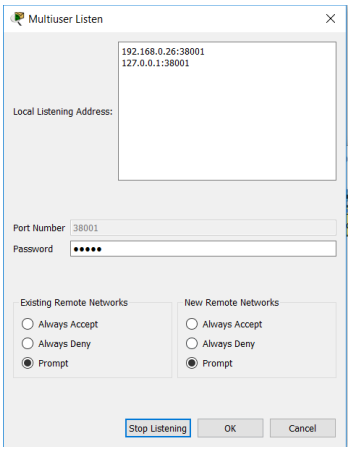
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

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

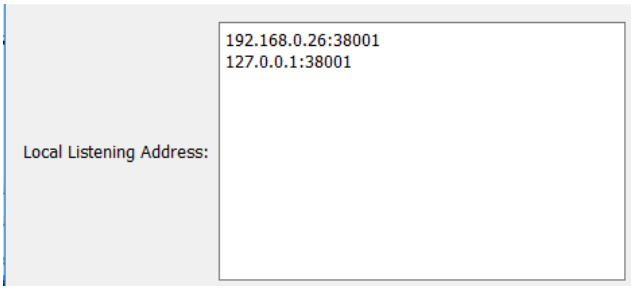
El jugador del lado cliente debe contar con la dirección IP, el número de puerto y la contraseña utilizados por el jugador del lado servidor para poder crear una conexión con el jugador del lado servidor.

a. Siga estos pasos para configurar Packet Tracer de manera de que esté preparado para recibir una conexión entrante:

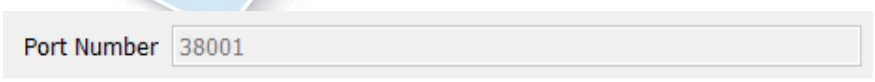
1) Haga clic en el menú **Extensions** (Extensiones), después en **Multiuser** (Multiusuario) y, finalmente, en **Listen** (Escuchar).



2) Tiene dos Local Listening Addresses (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.



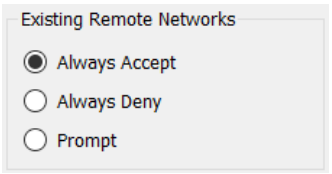
3) El número de puerto se indica junto a las direcciones IP y en el campo Port Number (Número de puerto). Si esta es la primera instancia de Packet Tracer que abrió en la PC, el número de puerto será 38000. Sin embargo, si hay varias instancias abiertas, el número aumenta de a uno por cada instancia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



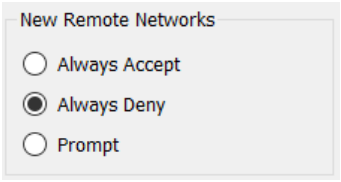
4) La contraseña está establecida en **cisco** de manera predeterminada. Puede cambiarla, pero no es necesario hacerlo para esta actividad.

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 Packet Tracer en el paso 3.

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

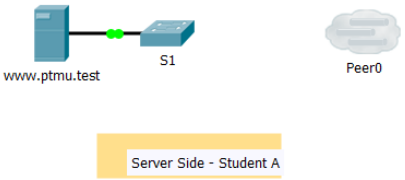


7) En la sección **New Remote Networks** (Nuevas redes remotas), confirme que el botón de opción **Always Deny** (Denegar siempre) esté habilitado. Esto evitará que el jugador del lado cliente cree un nuevo enlace no especificado en esta actividad.



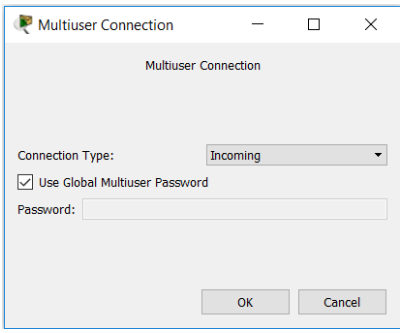
8) Haga clic en **OK** (Aceptar).

b. Haga clic en el ícono **Multiuser Connection** (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.



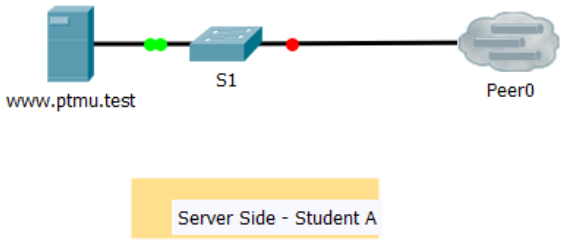
c. Haga clic en el nombre **Peer0** y cámbielo por **Enlace PTMU** (distingue mayúsculas de minúsculas).

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



e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-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).



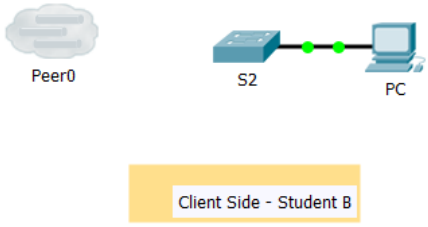
Paso 3: Jugador del lado cliente: configurar el lado cliente del enlace PTMU

a. Registre la siguiente información que le suministró el jugador del lado servidor:
Dirección IP: 192.168.90.26

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 **Multiuser Connection** (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.



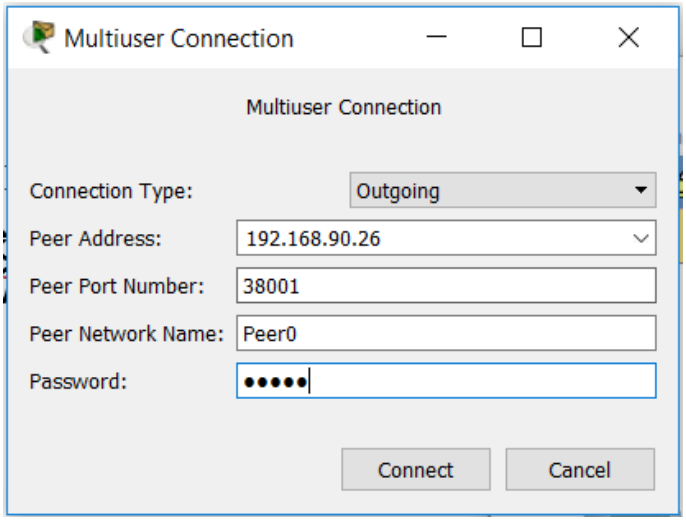
c. Haga clic en la nube de **Peer0** y cambie Connection Type por **Outgoing** (Saliente).

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.

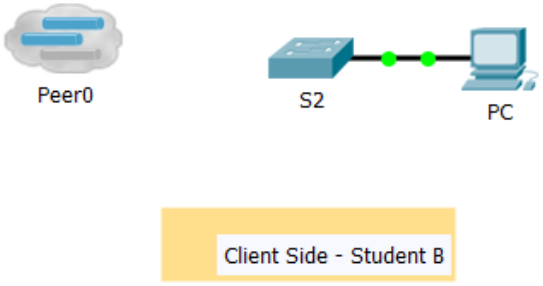
3) En el campo Peer Network Name (Nombre de red del punto), introduzca **Enlace PTMU**. Este campo distingue mayúsculas de minúsculas.

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



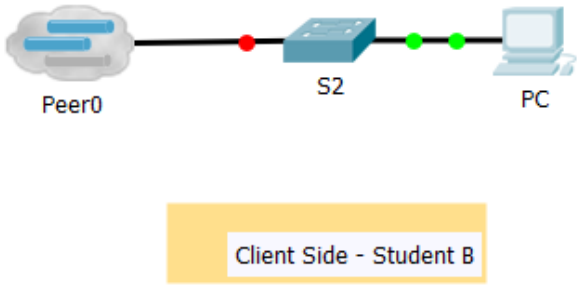
5) Haga clic en **Connect** (Conectar).

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

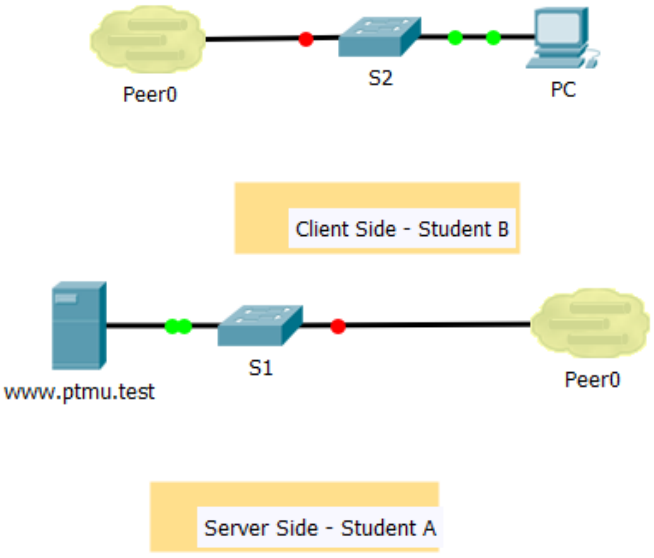


e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).

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.

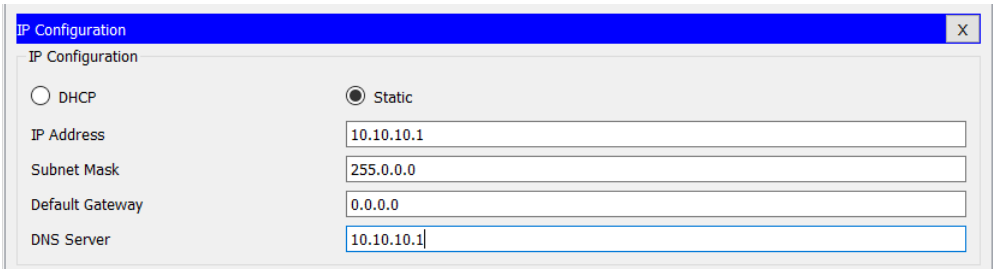


El enlace de multiusuario está establecido y listo para probar.

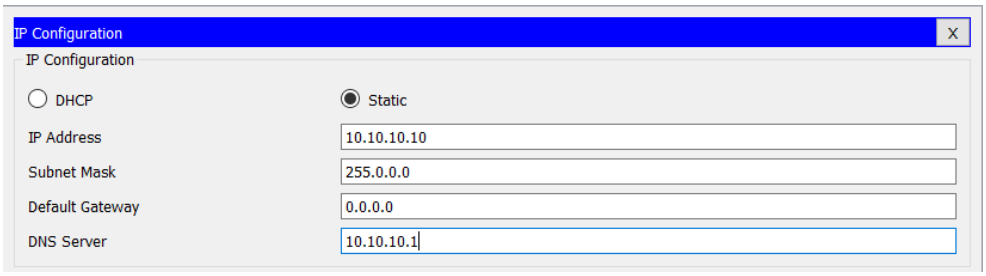
Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Paso 1: Configurar el direccionamiento IP

i. 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**.



j. 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 Packet Tracer 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 Packet Trac.

Ejercicio 10.4.1.3 Función Multiusuario de Packet Tracer: Implementación de servicios

Topología

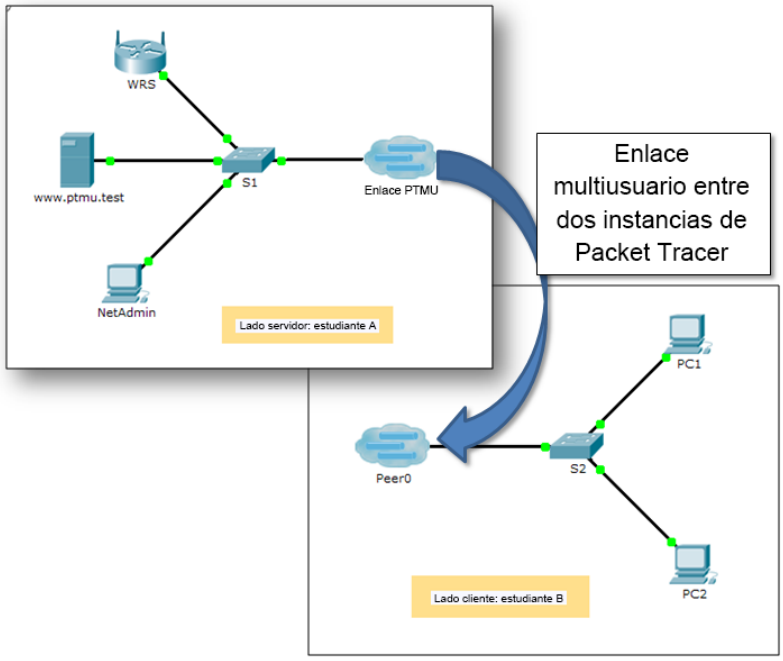


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de
Jugador del lado servidor		
WRS	172.16.1.254	255.255.255.0
S1	172.16.1.1	255.255.255.0
www.ptmu.test	172.16.1.5	255.255.255.0
NetAdmin	DHCP asignado	DHCP asignado
Jugador del lado cliente		
S2	172.16.1.2	255.255.255.0
PC1	DHCP asignado	DHCP asignado
PC2	DHCP asignado	DHCP asignado

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

Información básica

Nota: completar las actividades previas de este capítulo, incluida la actividad **Función Multiusuario de**
Packet Tracer: Tutorial, constituye un requisito previo.

En esta actividad para varios usuarios, dos estudiantes (jugadores) cooperan para implementar y verificar servicios, incluso DHCP, HTTP, correo electrónico, DNS y FTP. El jugador del lado servidor implementará
y verificará servicios en un servidor. El jugador del lado cliente configurará dos clientes y verificará 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.**

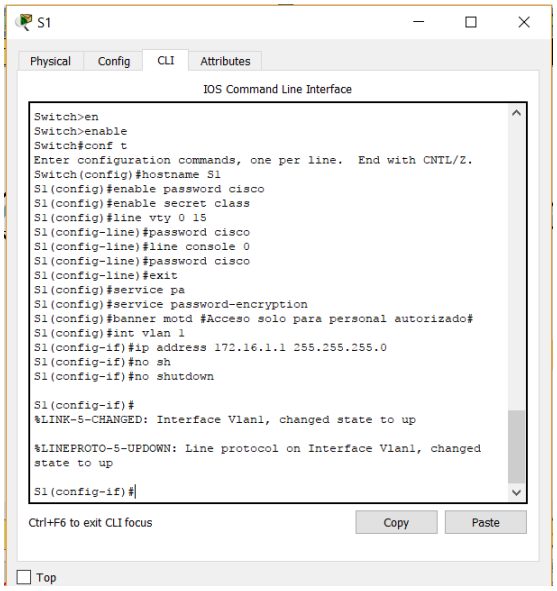
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los switches

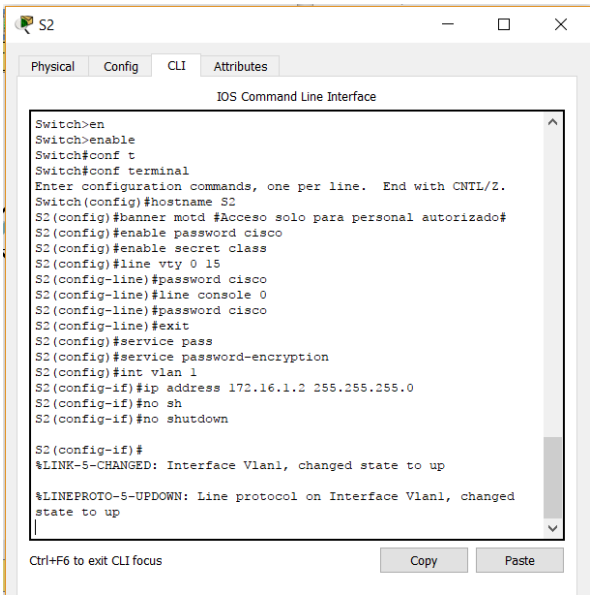
Cada jugador: configure su respectivo switch con los siguientes parámetros:

- Nombre de host que utilice el nombre para mostrar (**S1** o **S2**)
- Mensaje del día (MOTD) adecuado
- Contraseñas de modo EXEC privilegiado y de línea
- Direccionamiento IP correcto, según Tabla de direccionamiento

S1



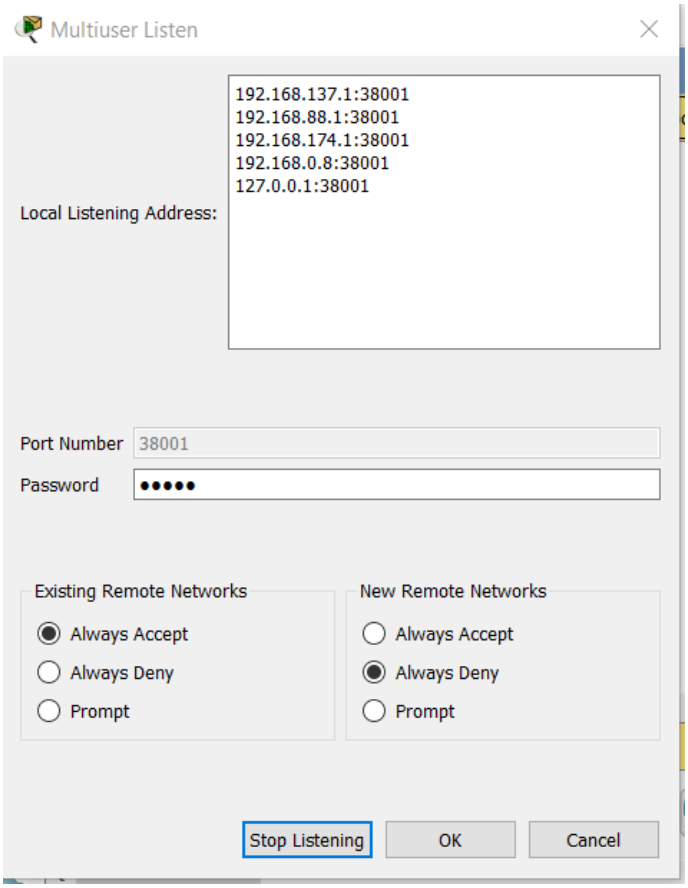
S2



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.

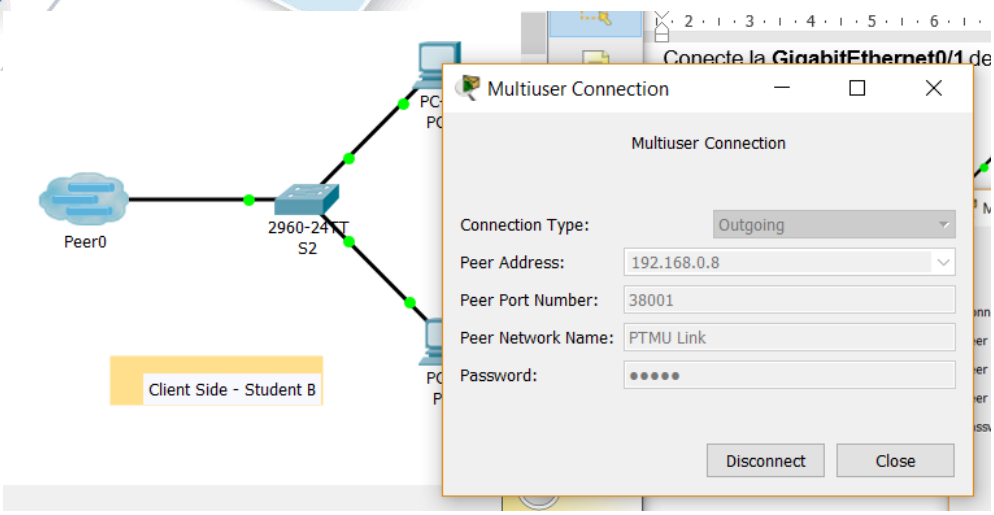


Paso 4: Jugador del lado cliente: Configurar la conexión multiusuario saliente

a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor: Dirección IP: 192.168.0.8
Número de puerto: 38001

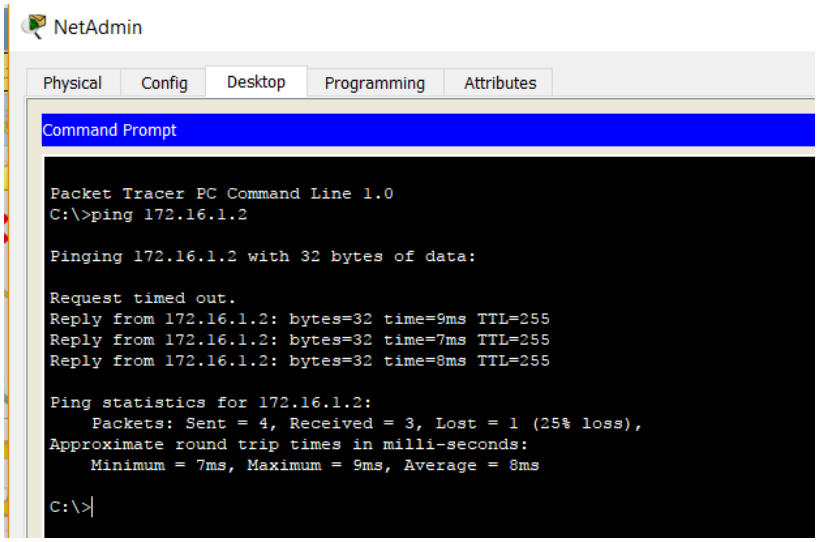
Contraseña (**cisco**, de manera predeterminada): cisco

b. Configure **Peer0** para conectarse al **enlace PTMU** del jugador del lado servidor. c. Conecte la **GigabitEthernet0/1** de **S2** al **Link0** en **Peer0**.

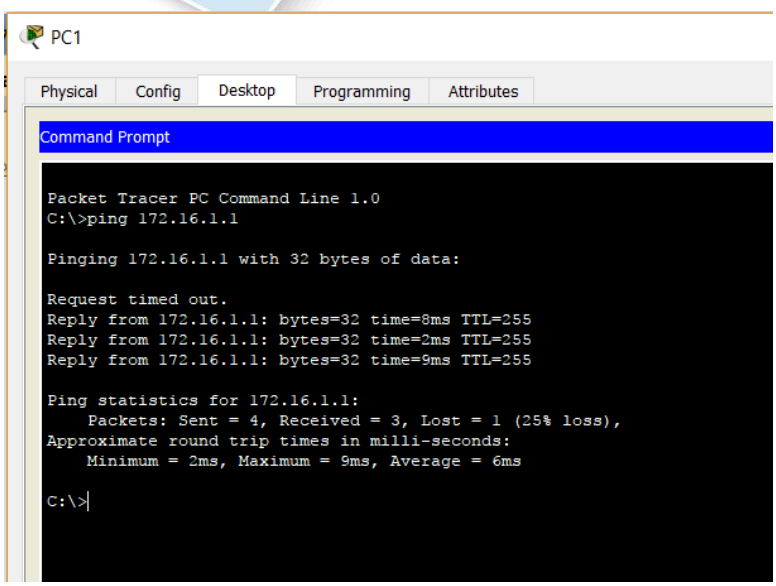


Paso 5: Verificar la conectividad a través de una conexión multiusuario local

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.

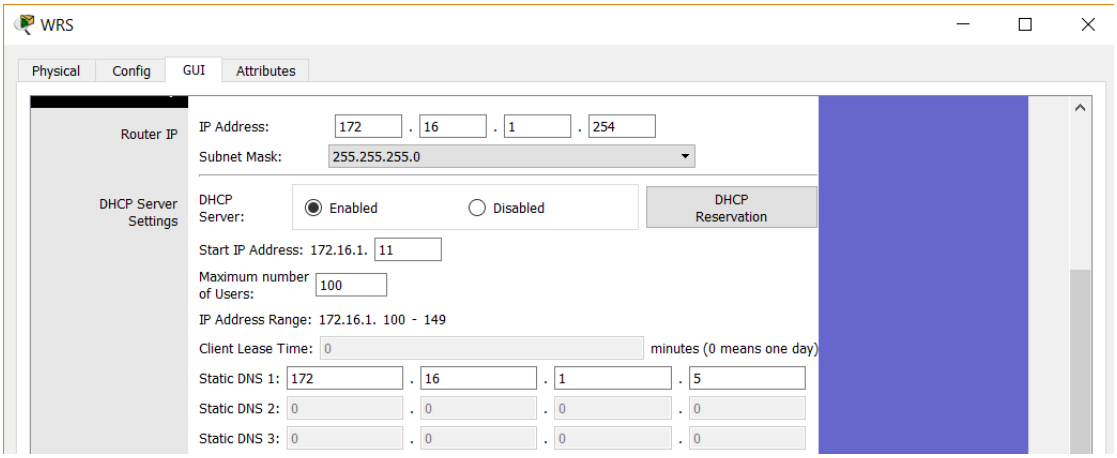


Parte 2: Jugador del lado servidor: Implementar y verificar servicios

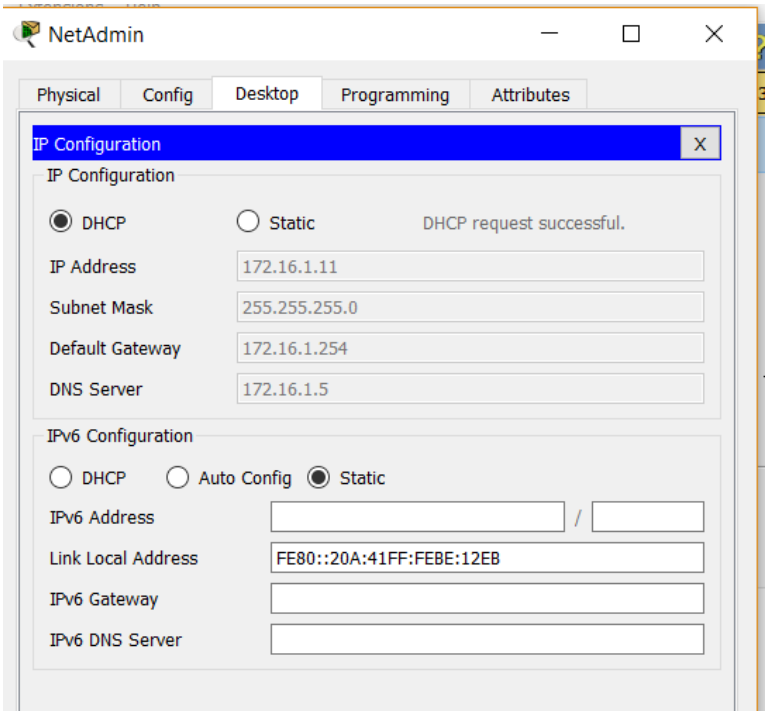
Paso 1: Configurar WRS como servidor de DHCP

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**.

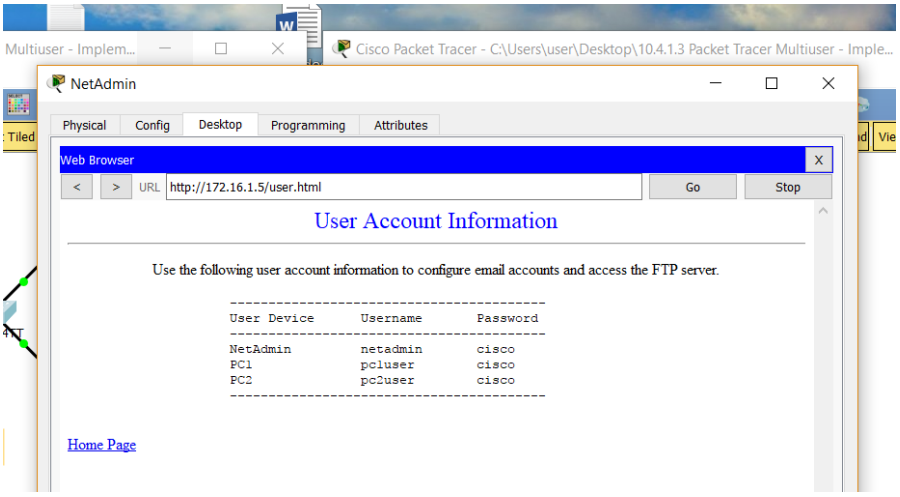


Verifique si **NetAdmin** recibió el direccionamiento IP mediante DHCP.



En **NetAdmin**, acceda a la página Web User Account Information (Información de cuenta de usuario) en

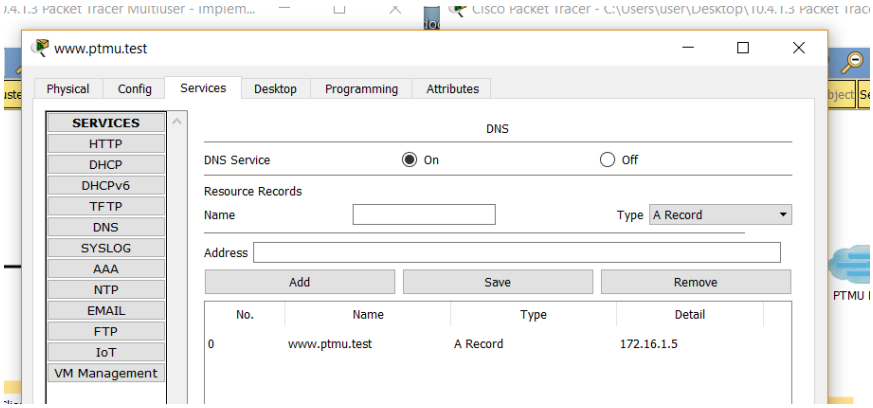
172.16.1.5. Utilizará esta información para configurar las cuentas de usuario en el paso 2.



Paso 2: Configurar servicios en www.ptmu.test

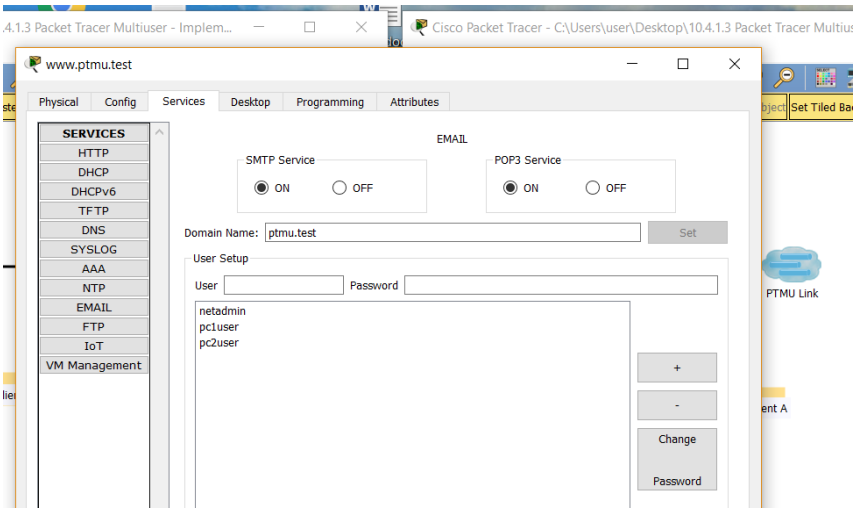
El servidor **www.ptmu.test** proporciona el resto de los servicios y se debe configurar con lo siguiente:

Un registro DNS que asocie la dirección IP del servidor **www.ptmu.test** al nombre www.ptmu.test.

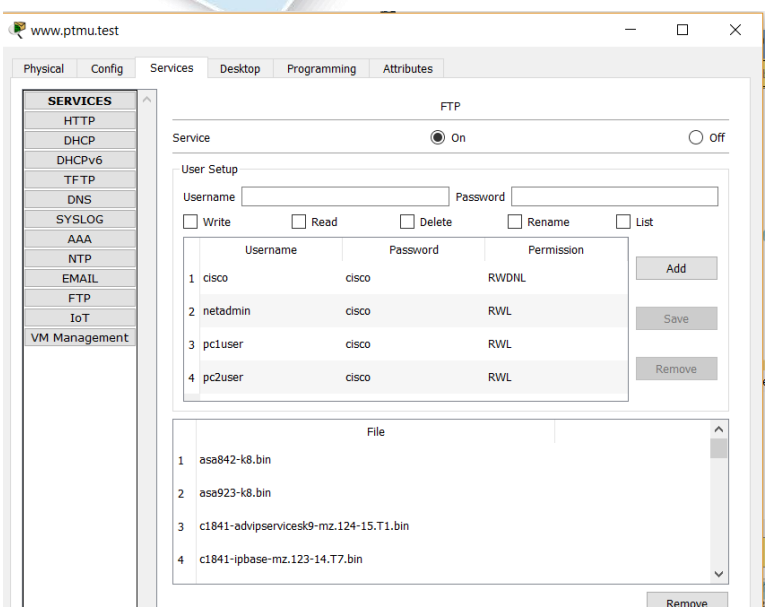


Cuentas de usuario y servicios de correo electrónico según la lista de usuarios. El nombre de dominio es

ptmu.test.



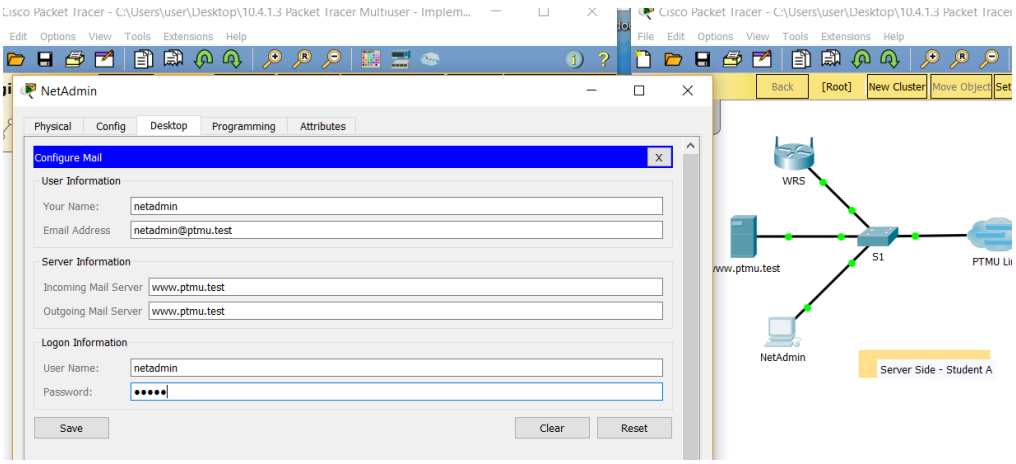
Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.



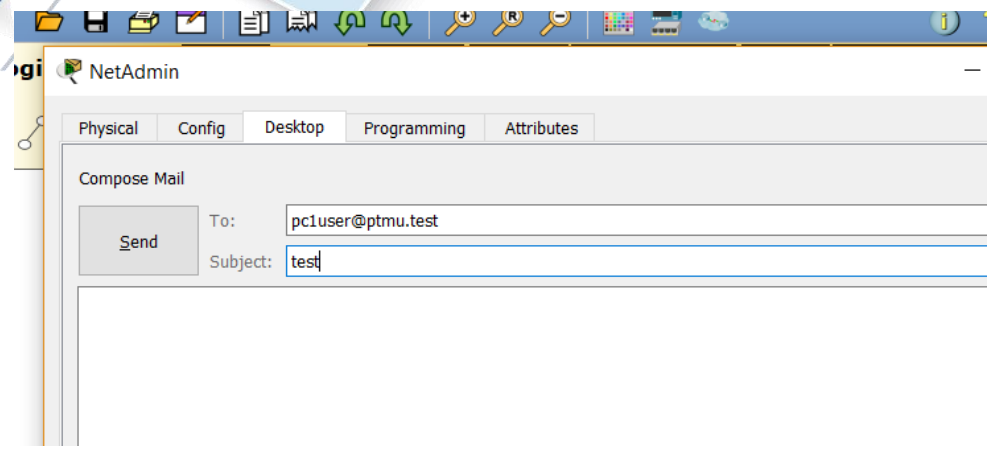
Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos

En **NetAdmin**, realice lo siguiente:

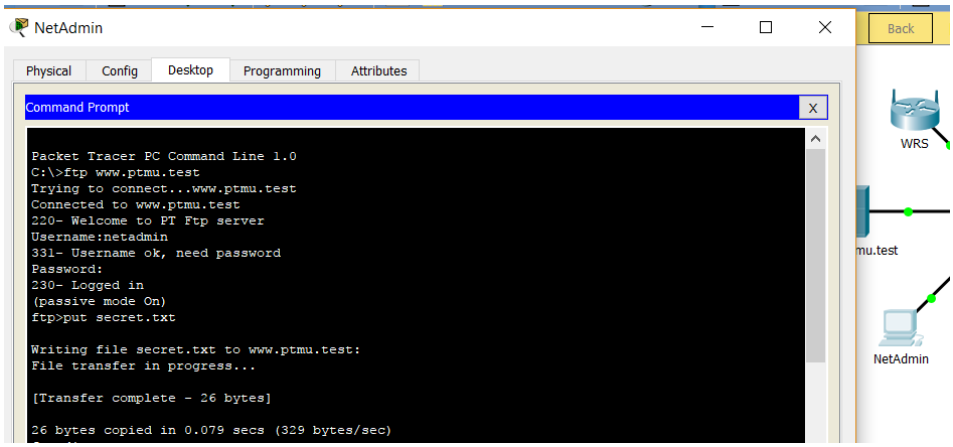
- Configure el cliente de correo electrónico para la cuenta de usuario de NetAdmin.

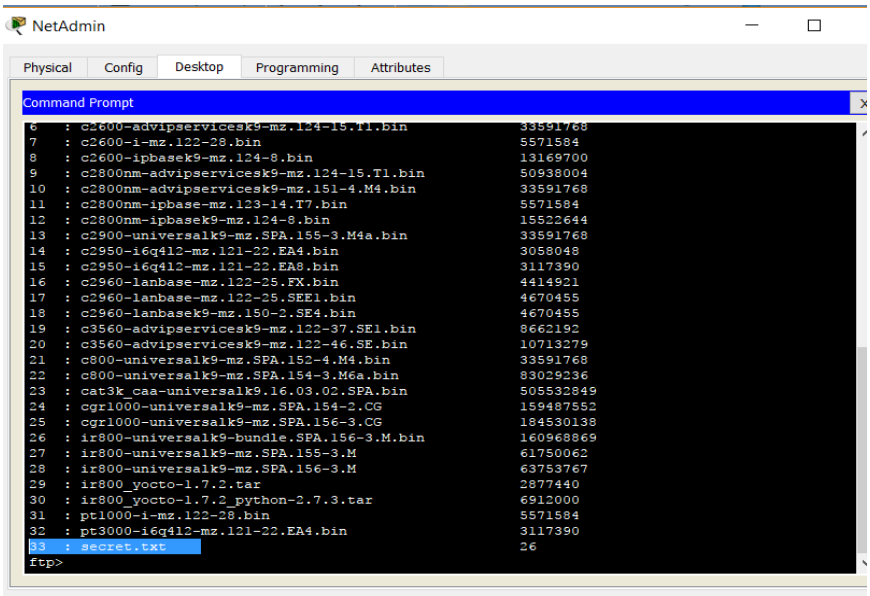


- Envíe un correo electrónico al usuario de la **PC1**.



Suba el archivo **secret.txt** al servidor FTP. No modifique el archivo.



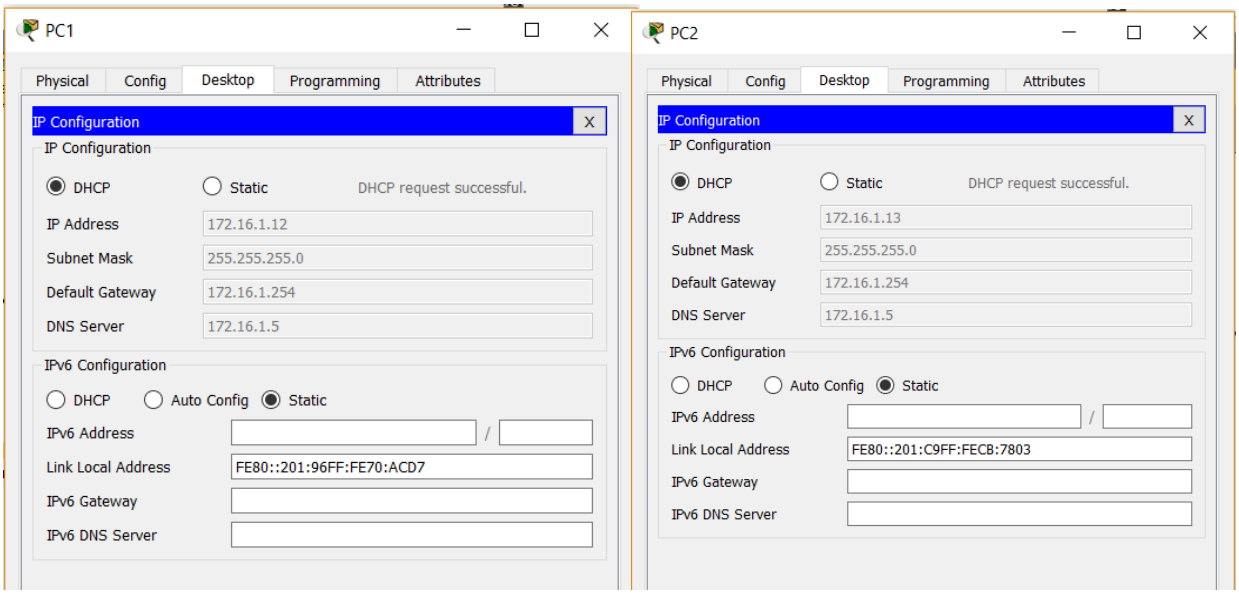


Nota: la puntuación para el jugador del lado servidor será de **43/44** hasta que el jugador del lado cliente descargue correctamente el archivo **secret.txt**, lo modifique y lo suba al servidor FTP **www.ptmu.test**.

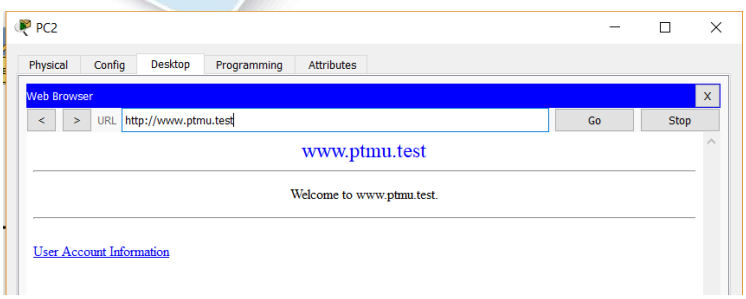
Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Paso 1: Configurar y verificar el direccionamiento de las PC

a. Configure la **PC1** y **la PC2** para obtener el direccionamiento automáticamente.

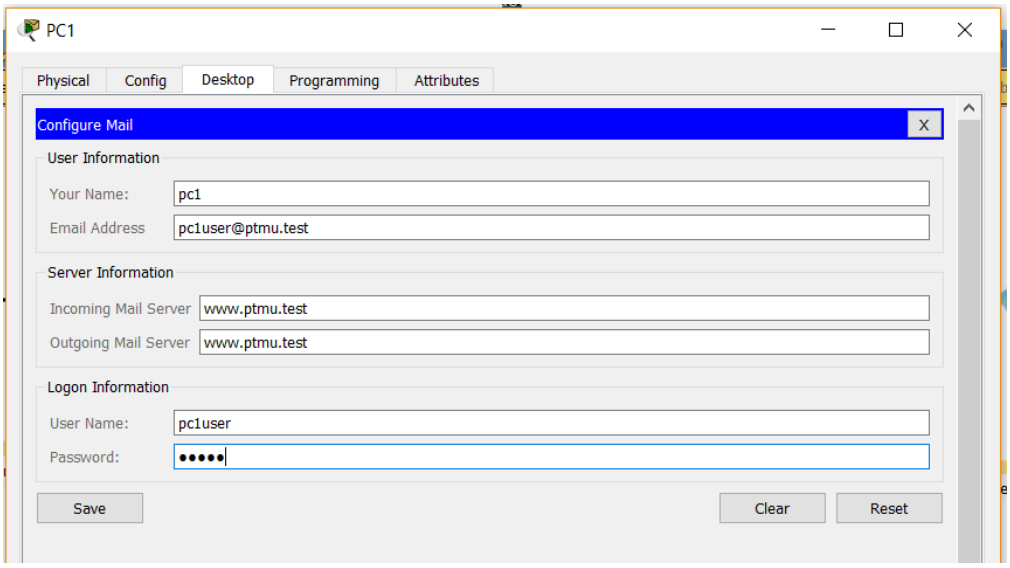


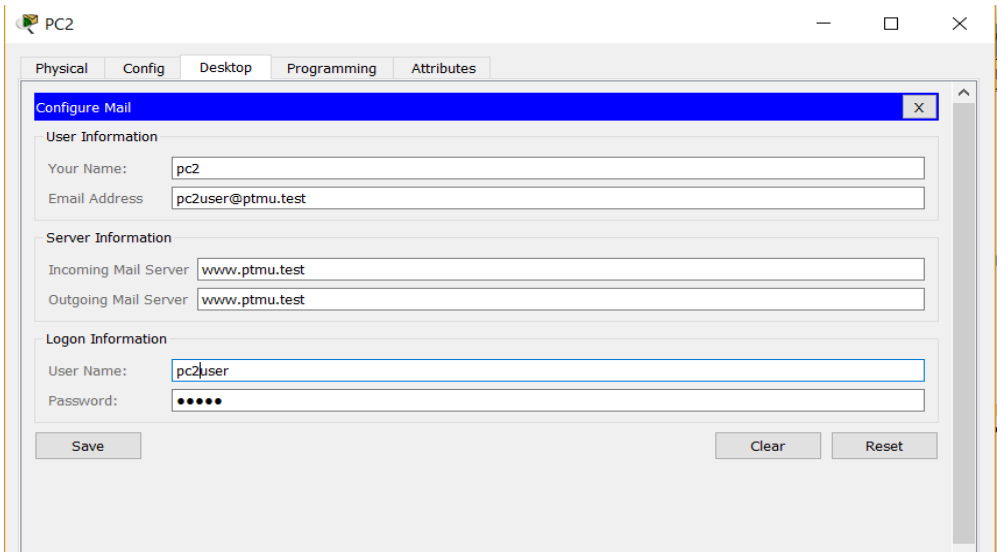
b. Las PC1 y PC2 deben poder acceder a la página Web **http://www.ptmu.test**.



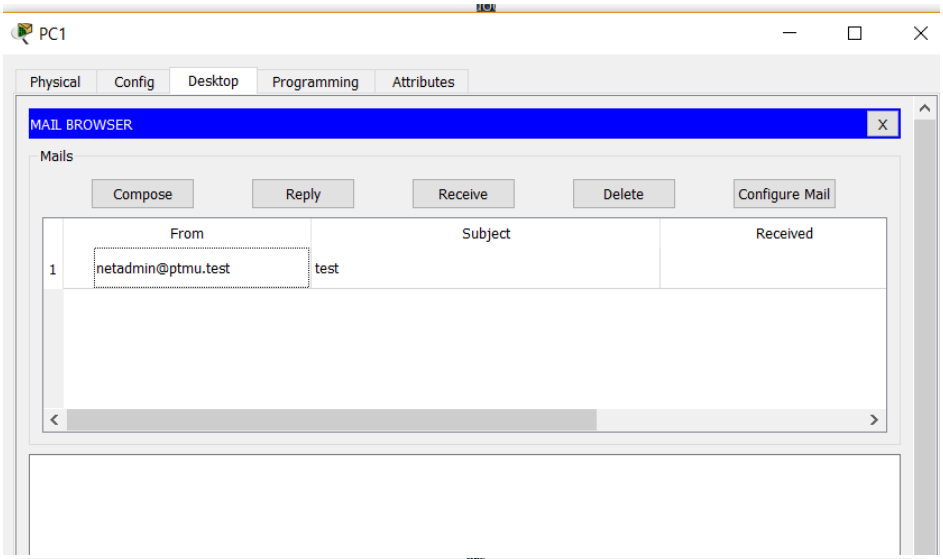
Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

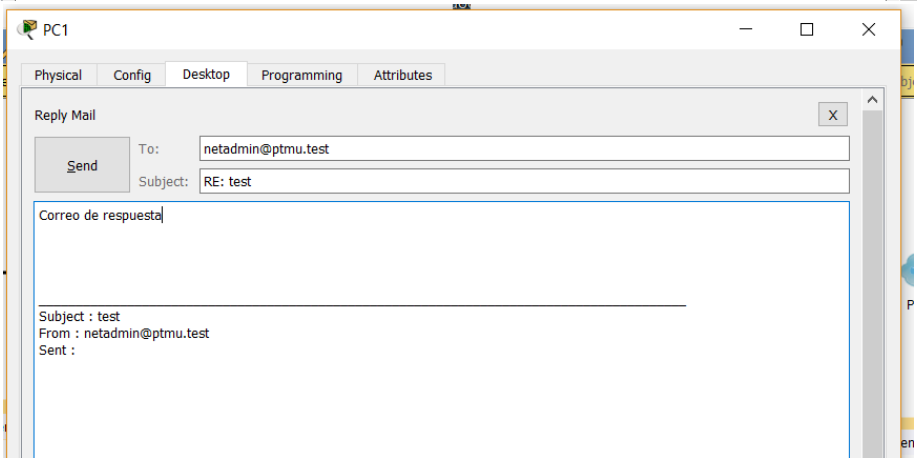
a. Configure las cuentas de correo electrónico según los requisitos que se indican en **www.ptmu.test/user.html**



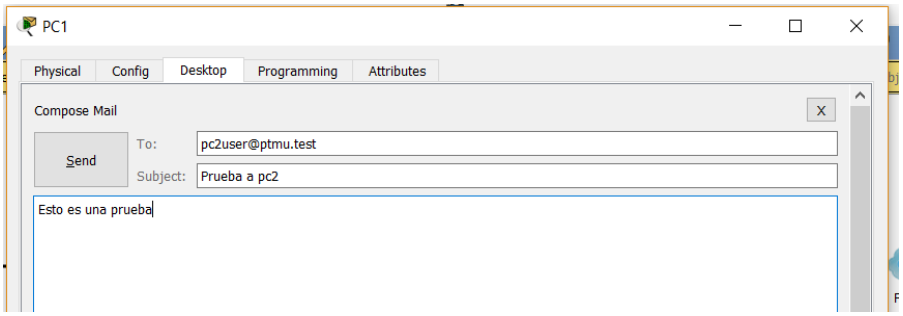


b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta.

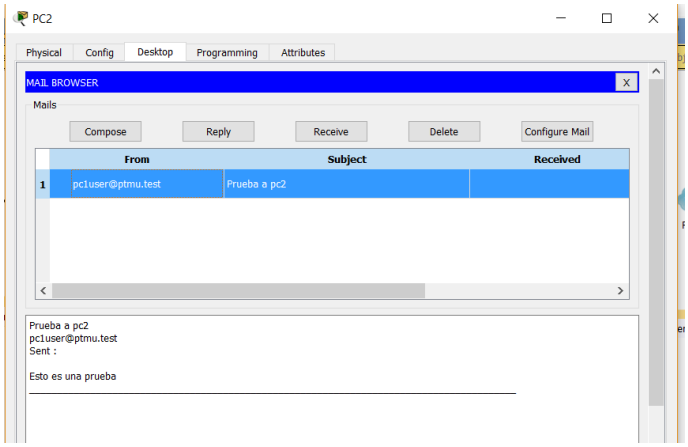




c. Envíe un correo electrónico de la PC1 a la PC2. **Nota:** la puntuación no cambiará.

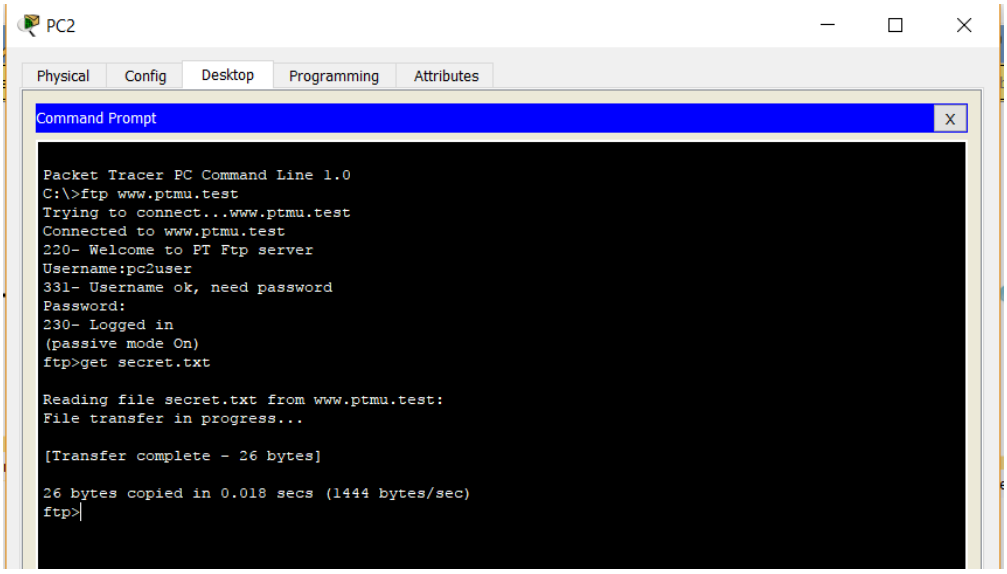


d. Verifique si la PC2 recibió un correo electrónico de la PC1.

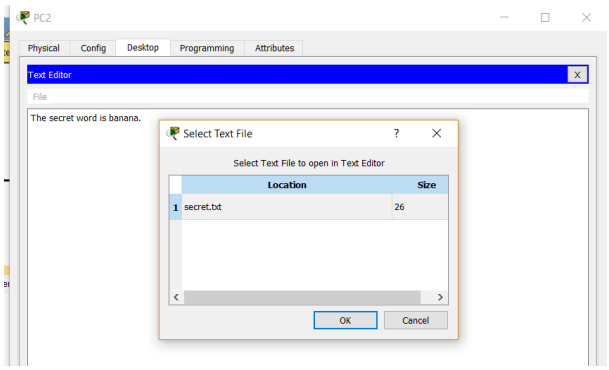


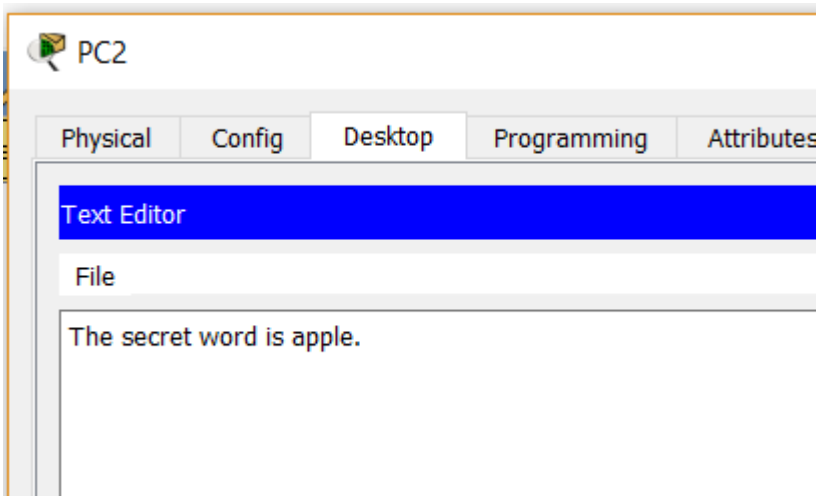
Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

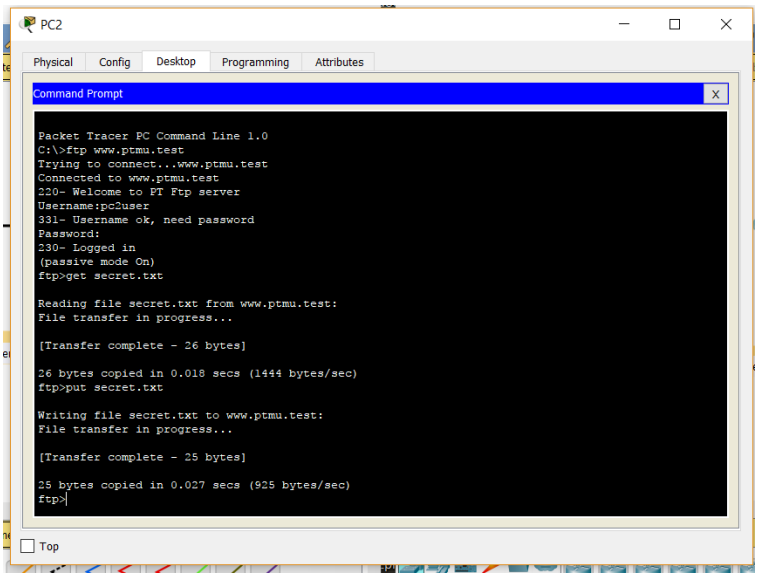
a. En la PC2, acceda al servidor FTP y descargue el archivo **secret.txt**.



b. Abra el archivo **secret.txt**, solo cambie la palabra secreta por **apple** y suba el archivo.



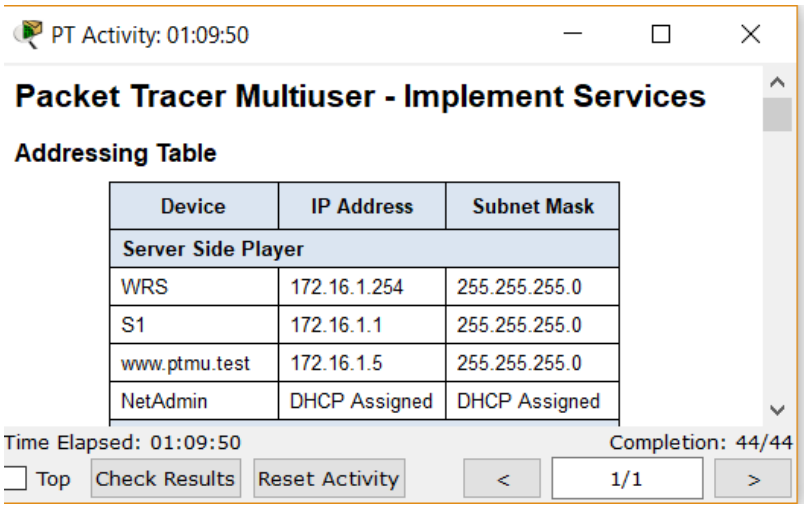


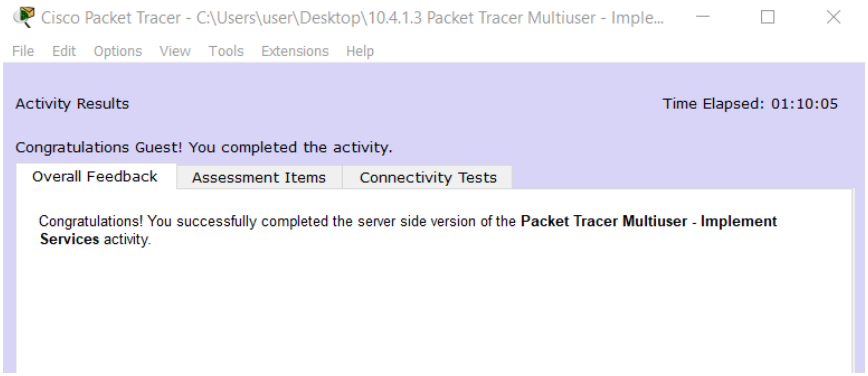


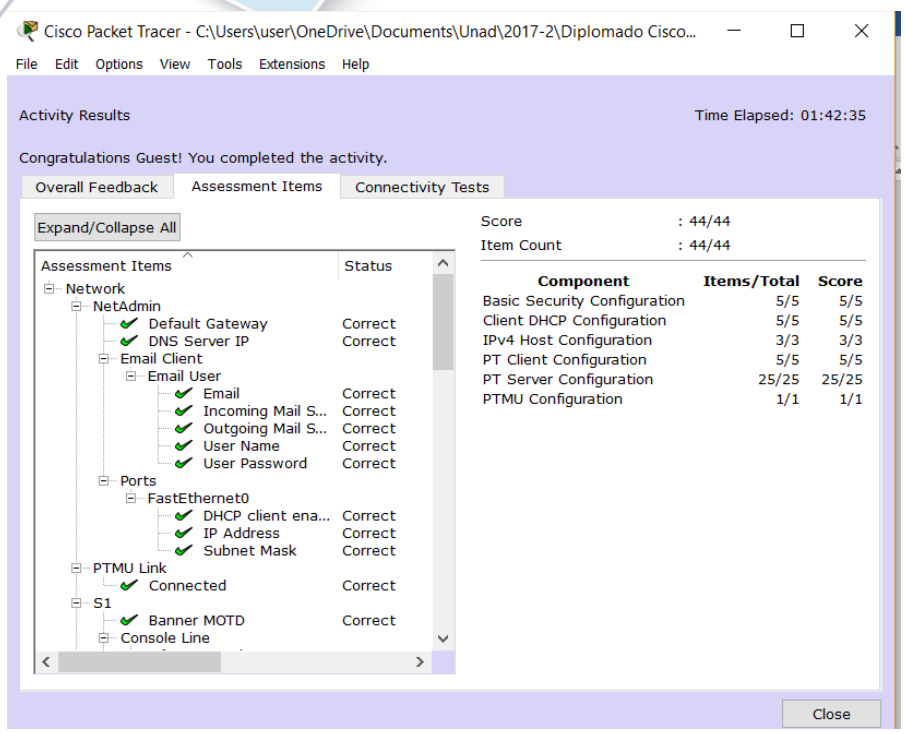
c. La puntuación del jugador del lado servidor debería ser **44/44** y la del jugador del lado cliente debería ser
33/33.

RESULTADOS:

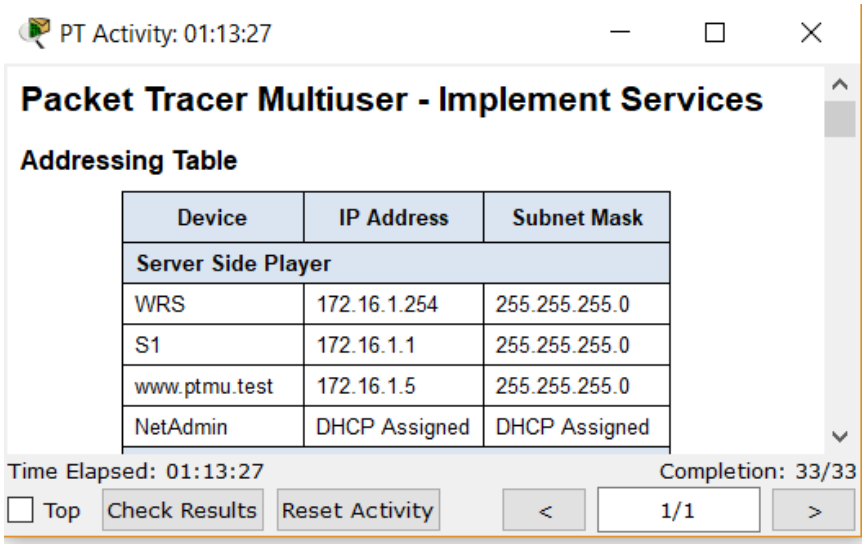
Lado del servidor:

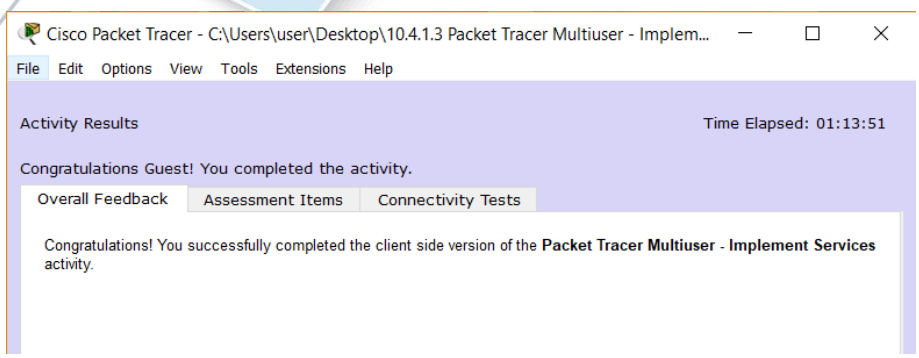


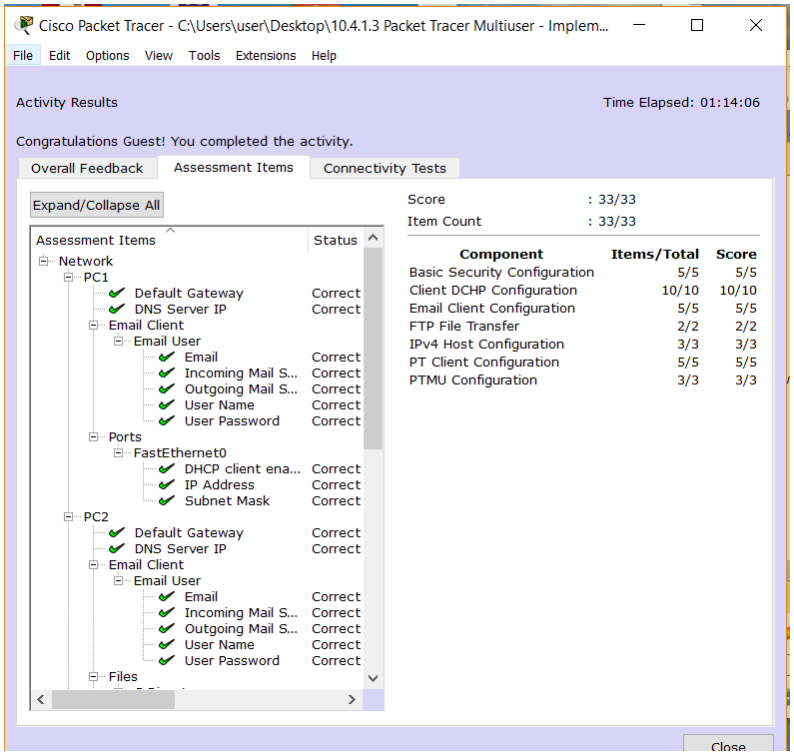




Lado del cliente:

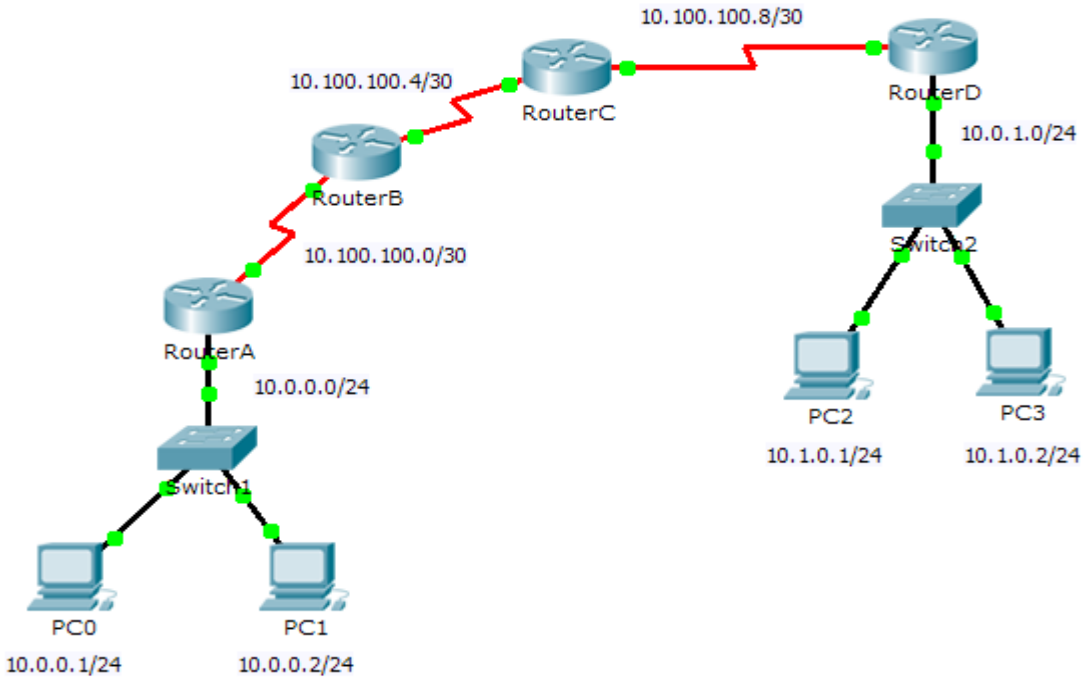



Cisco Packet Tracer - C:\Users\user\Desktop\10.4.1.3 Packet Tracer Multiuser - Implem...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:13:51
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the client side version of the Packet Tracer Multiuser - Implement Services activity.


Cisco Packet Tracer - C:\Users\user\Desktop\10.4.1.3 Packet Tracer Multiuser - Implem...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:14:06
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Network
PC1
Default Gateway Correct
DNS Server IP Correct
Email Client
Email User
Email Correct
Incoming Mail S... Correct
Outgoing Mail S... Correct
User Name Correct
User Password Correct
Ports
FastEthernet0
DHCP client ena... Correct
IP Address Correct
Subnet Mask Correct
PC2
Default Gateway Correct
DNS Server IP Correct
Email Client
Email User
Email Correct
Incoming Mail S... Correct
Outgoing Mail S... Correct
User Name Correct
User Password Correct
Files
Score : 33/33
Item Count : 33/33
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 3/3 3/3
Close

Ejercicio 11.3.2.2 Prueba de la conectividad con traceroute

Topología



Objetivos

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Parte 2: Comparar con el comando traceroute en un router

Información básica

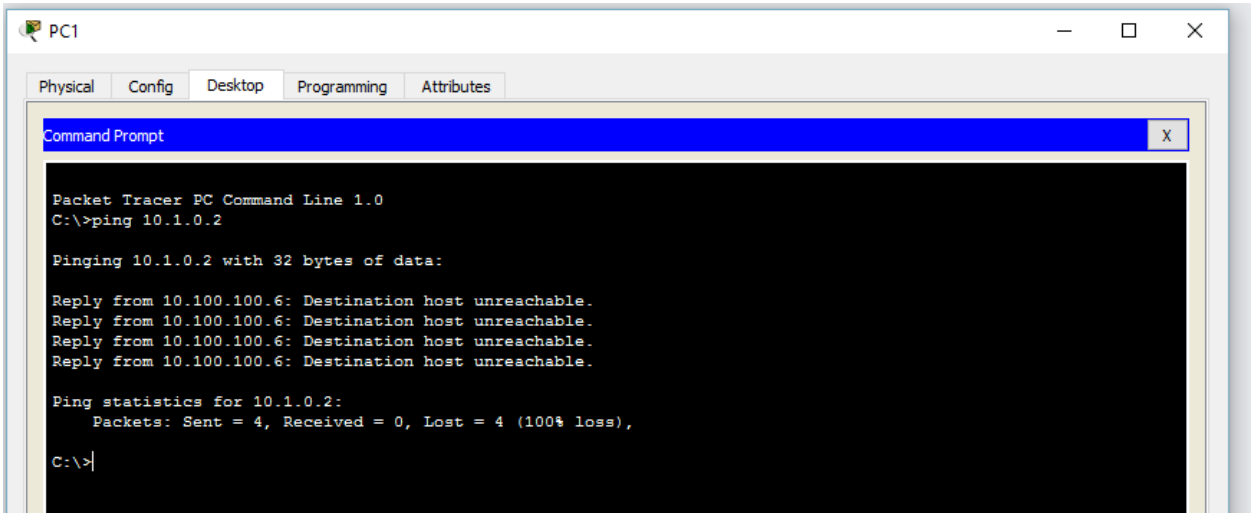
Esta actividad está diseñada para ayudarlo a llevar a cabo la resolución de problemas de conectividad de red utilizando comandos para rastrear la ruta de origen a destino. Debe examinar el resultado de **tracert** (el comando de Windows) y **traceroute** (el comando de IOS) mientras los paquetes atraviesan la red y determinar la causa de un problema de red. Una vez que se corrija el problema, utilice los comandos **tracert** y **traceroute** para verificar la finalización.

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Paso 1: Enviar un ping de un extremo al otro de la red

Haga clic en **PC1** y abra el **símbolo del sistema**. Haga ping a **PC3** en **10.1.0.2**. ¿Qué mensaje se muestra como resultado del ping?

Host de destino inalcanzable.



c. Observe los resultados del comando **tracert**. ¿Cuál es la última dirección que se alcanzó con el comando **tracert**?

10.100.100.6

Paso 3: Corregir el problema de red

a. Compare la última dirección que se alcanzó con el comando **tracert** con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de falla. ¿Qué dispositivos tienen direcciones configuradas para la red donde ocurrió la falla?

El RouterB y el RouterC.

b. Haga clic en **RouterC** y, a continuación, haga clic en la ficha **CLI**. c. ¿Cuál es el estado de las interfaces?
Parecen estar activas.

d. Compare las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo común?
La interfaz serial 0/0/0 tiene una dirección IP incorrecta según la topología.

e. Realice los cambios necesarios para restaurar la conectividad, pero no modifique las subredes. ¿Cuál es la solución?
Cambiar la dirección IP de la S0/0/0 a 10.100.100.9/30.

Paso 4: Verificar que la conectividad de extremo a extremo esté establecida

a. En el **símbolo del sistema de la PC1**, introduzca el comando **tracert 10.1.0.2**.

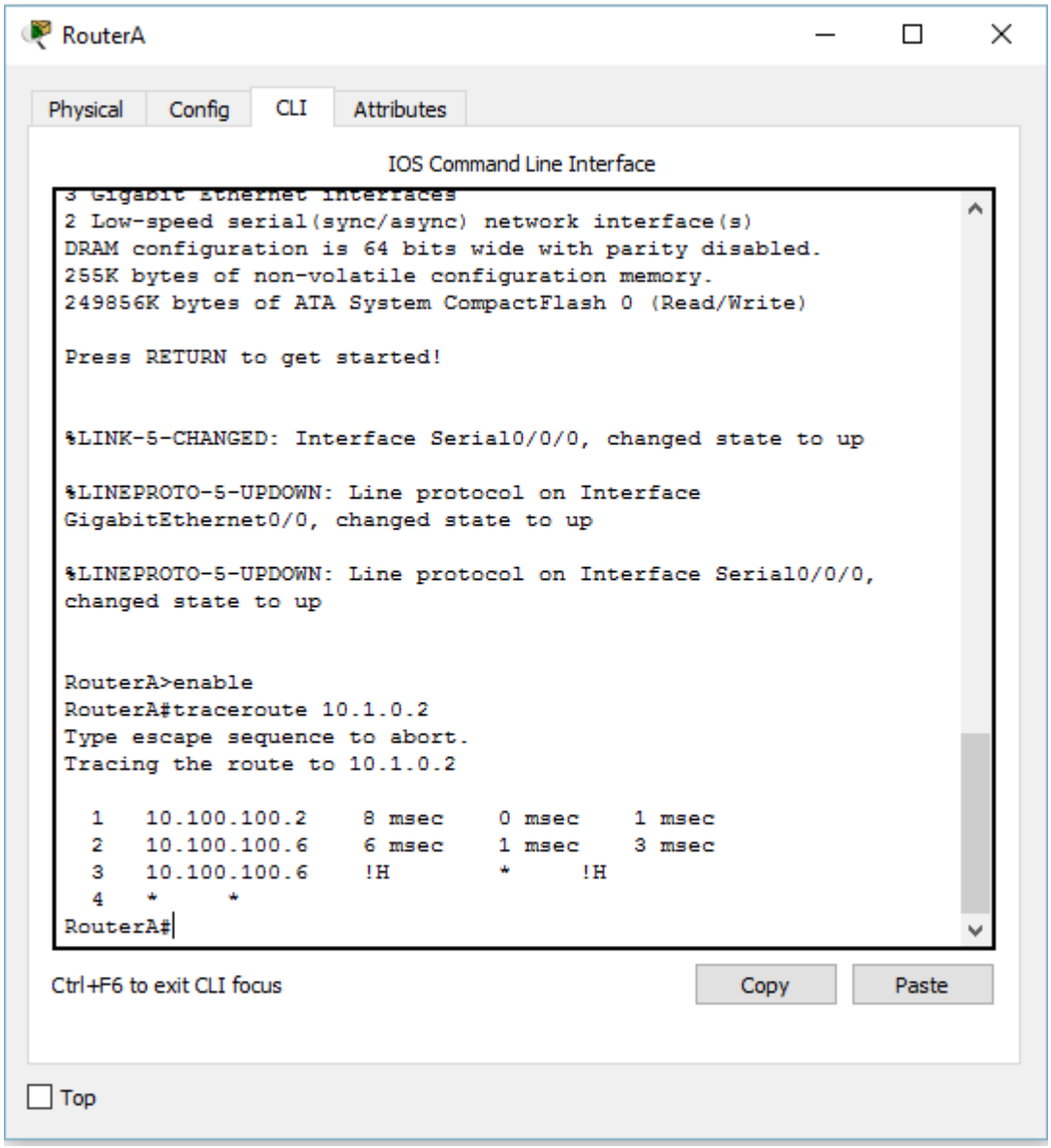
c. Observe el resultado del comando **tracert**. ¿El comando funcionó correctamente?

Sí

Parte 2: Comparar con el comando traceroute en un router

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

d. Introduzca el comando **traceroute 10.1.0.2**. ¿El comando se completó correctamente? Sí



c. Compare el resultado del comando **traceroute** del router con el del comando **tracert** de la PC. ¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió?

El router tiene una dirección IP menos, porque el próximo dispositivo que utilizará en la ruta será el RouterB

Ejercicio 11.3.3.4 Uso de los comandos show

Objetivos

Parte 1: Analizar el resultado del comando show

Parte 2: Preguntas de reflexión

Información básica

Esta actividad está diseñada para reforzar el uso de los **show** del router. No debe realizar comandos configuraciones, sino examinar el resultado de **show**.
diversos comandos

Parte 1: Analizar el resultado del comando show

Paso 1: Conectarse a ISPRouter

- Haga clic en **PC ISP** y, a continuación, en la ficha **Desktop** (Escritorio), seguida de **Terminal**.
- Ingrese al modo EXEC privilegiado.

```
ISPRouter>enable
ISPRouter#
```

- Use los siguientes comandos **show** para contestar las preguntas de reflexión en la parte 2:

`show arp`

```
ISPRouter#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  209.165.201.1           -   0030.F275.CE01  ARPA   GigabitEthernet0/0
ISPRouter#
```

`show flash:`

```
ISPRouter#show flash:

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


ISPRouter#
```

show ip route

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

Gateway of last resort is not set

     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Serial0/0/1
L       209.165.200.226/32 is directly connected, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/27 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0

ISPRouter#
```

show interfaces

```
ISPRouter#
ISPRouter#show interfaces
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0030.f275.ce01 (bia
0030.f275.ce01)
  Internet address is 209.165.201.1/27
  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
 --More--
```

show ip interface brief

```
ISPRouter#
ISPRouter#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     209.165.201.1   YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            209.165.200.226 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
ISPRouter#
```

show protocols

```
ISPRouter#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 209.165.201.1/27
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is administratively down, line protocol is down
Serial0/0/1 is up, line protocol is up
  Internet address is 209.165.200.226/27
Vlan1 is administratively down, line protocol is down
ISPRouter#
```

show users

```
ISPRouter#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
ISPRouter#
```

show version

```
ISPRouter#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 20 minutes, 13 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
 --More--
```

Parte 2: Preguntas de reflexión

o. ¿Qué comandos proporcionarían la dirección IP, el prefijo de red y la interfaz?

R: Los comandos son:

Show ip route

Show interfaces

Show protocols

p. ¿Qué comandos proporcionan la dirección IP y la asignación de interfaces, pero no el prefijo de red?

R: show ip interface brief

q. ¿Qué comandos proporcionan el estado de las interfaces?

R: Los comandos son:

Show interfaces

Show ip interface brief.

r. ¿Qué comandos proporcionan información sobre el IOS que se encuentra cargado en el router?

R: Los comandos son:

Show flash, show version.

s. ¿Qué comandos proporcionan información sobre las direcciones de las interfaces del router?
R: Los comandos son:
Show arp
Show interfaces

t. ¿Qué comandos proporcionan información sobre la cantidad de memoria flash disponible?
R: show version

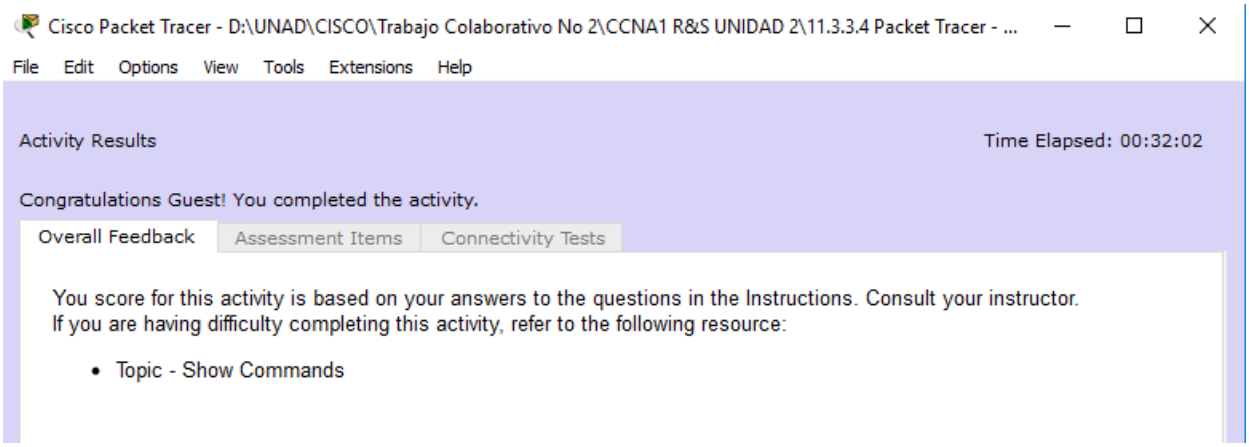
u. ¿Qué comandos proporcionan información sobre las líneas que se utilizan para propósitos de control de dispositivos o de configuración?
R: Show users

v. ¿Qué comandos proporcionan estadísticas de tráfico de las interfaces del router?
R: show interfaces

h. ¿Qué comandos proporcionan información sobre las rutas disponibles para el tráfico de la red?
R: show ip route

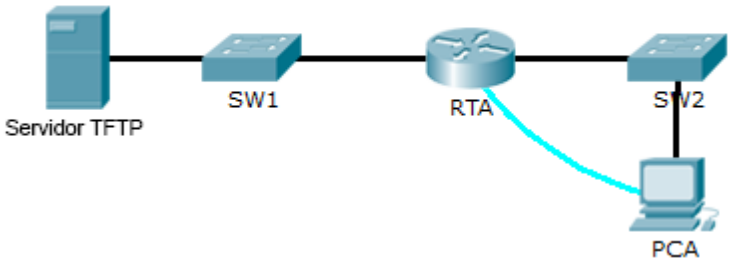
i. ¿Qué interfaces están activas actualmente en el router?
R: GigabitEthernet 0/0, Serial 0/0/1.

Ítems Resueltos



Ejercicio 11.4.2.5 Realización de copias de seguridad de archivos de configuración

Topología



Objetivos

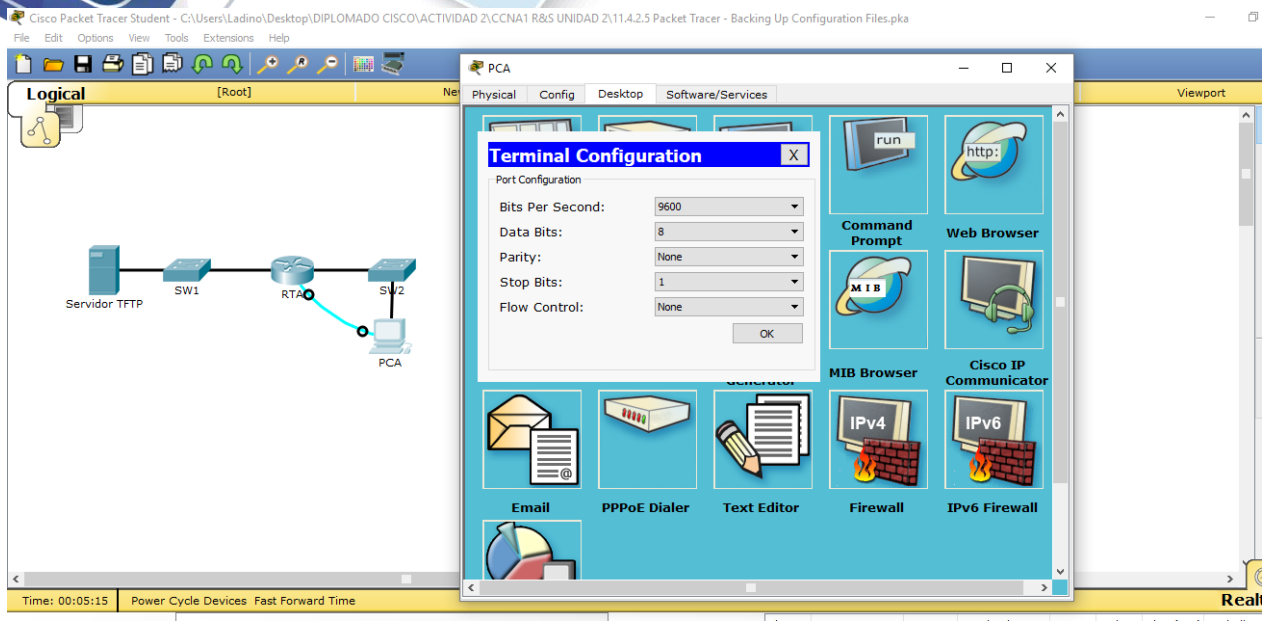
Parte 1: Establecer la conectividad al servidor TFTP
Parte 2: Transferir la configuración del servidor TFTP
Parte 3: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP
Información básica/Situación

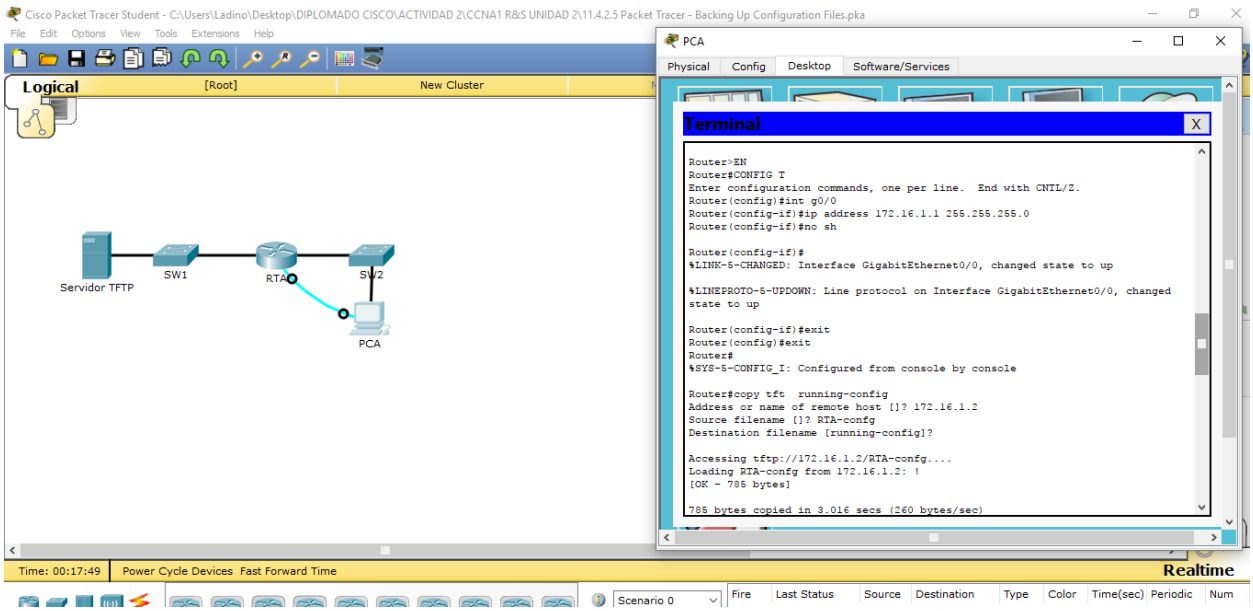
Esta actividad está diseñada para mostrar cómo restaurar una configuración a partir de una copia de seguridad y, luego, realizar una nueva copia de seguridad. Debido a una falla del equipo, se colocó un router nuevo. Afortunadamente, los archivos de configuración de respaldo se guardaron en un servidor de protocolo TFTP (Trivial File Transfer Protocol, protocolo trivial de transferencia de archivos). Debe restaurar los archivos del servidor TFTP para que el router vuelva a estar en línea con el menor tiempo de inactividad posible.

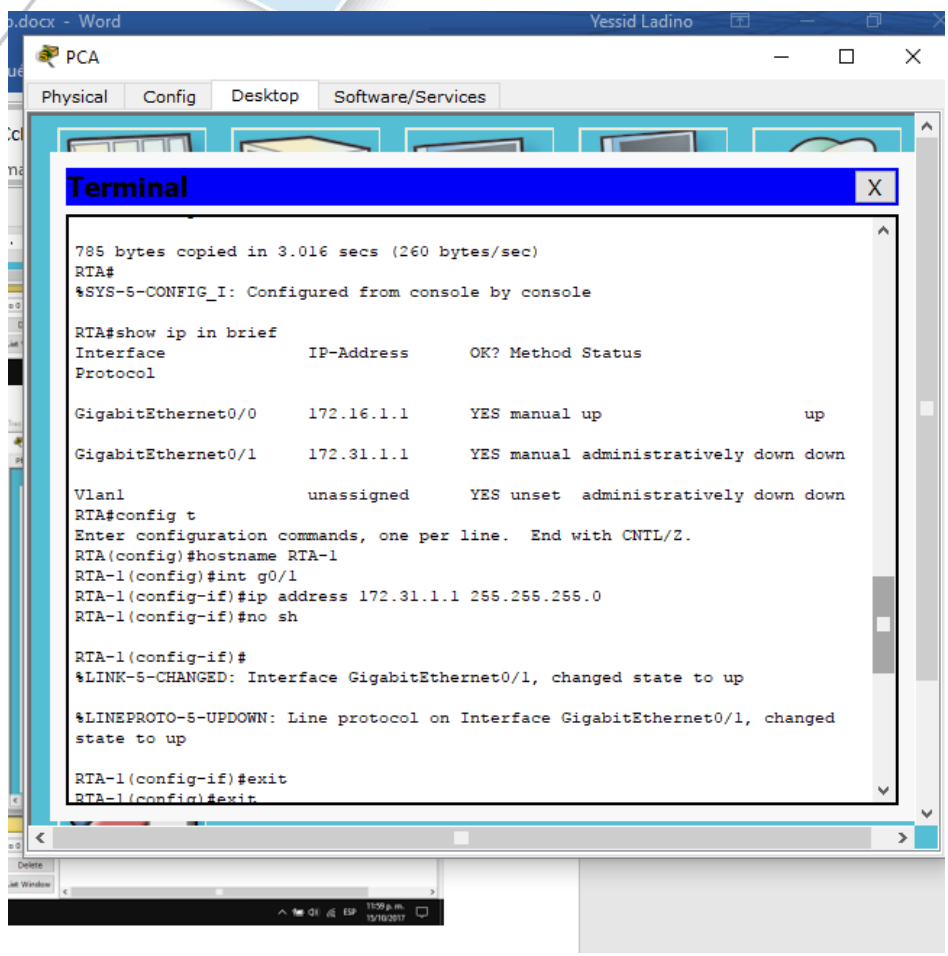
Parte 1: Establecer la conectividad al servidor TFTP

Nota: debido a que es un router nuevo, la configuración inicial se realizará mediante una conexión de consola al router.

a. Haga clic en **PCA**, después en la ficha **Desktop** (Escritorio) y, a continuación, en **Terminal** para acceder a la línea de comandos **RTA**.


Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\11.4.2.5 Packet Tracer - Backing Up Configuration Files.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
Viewport
Servidor TFTP
SW1
RTA
SW2
PCA
Time: 00:05:15
Power Cycle Devices Fast Forward Time
PCA
Physical Config Desktop Software/Services
Terminal Configuration
Port Configuration
Bits Per Second: 9600
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None
OK
run
Command Prompt
http:
Web Browser
MIB
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
IPv4
Firewall
IPv6
IPv6 Firewall


Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\11.4.2.5 Packet Tracer - Backing Up Configuration Files.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Servidor TFTP
SW1
RTA
SW2
PCA
Time: 00:17:49
Power Cycle Devices Fast Forward Time
Realtime
Scenario 0
Fire Last Status Source Destination Type Color Time(sec) Periodic Num
PCA
Physical Config Desktop Software/Services
Terminal
Router>EN
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 172.16.1.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy tft running-config
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-confg
Destination filename [running-config]?
Accessing tftp://172.16.1.2/RTA-confg....
Loading RTA-confg from 172.16.1.2: !
[OK - 785 bytes]
785 bytes copied in 3.016 secs (260 bytes/sec)



b. Configure y active la interfaz **Gigabit Ethernet 0/0**. La dirección IP debe coincidir con el gateway predeterminado para el **servidor TFTP**.

c. Pruebe la conectividad al **servidor TFTP**. Si es necesario, lleve a cabo la resolución de problemas.

Parte 2: Transferir la configuración del servidor TFTP

a. Emita el siguiente comando desde el modo EXEC privilegiado:

```
Router# copy tftp running-config
Address or name of remote host []? 172.16.1.2 Packet Tracer: Realización de copias de seguridad de archivos de configuración
```


Source filename []? **RTA-confg**
Destination filename [running-config]? **<cr>**

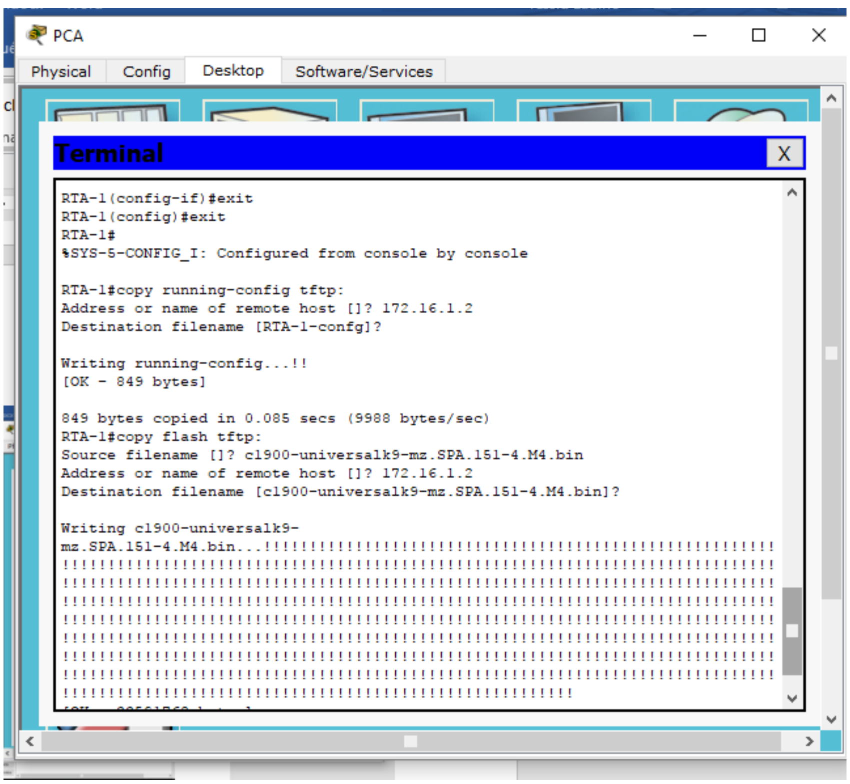
El router debe devolver lo siguiente:

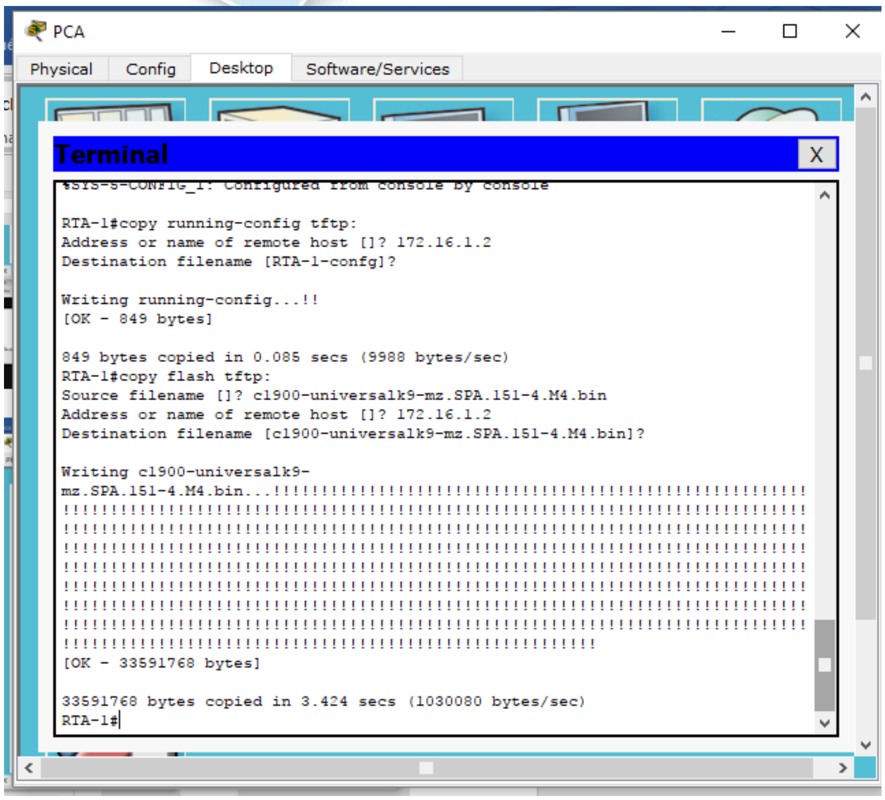
```
Accessing tftp://172.16.1.2/RTA-confg...
Loading RTA-confg from 172.16.1.2: !
[OK - 785 bytes]
785 bytes copied in 0 secs
RTA#
%SYS-5-CONFIG_I: Configured from console by console
RTA#
```

b. Emita el comando para visualizar la configuración actual. ¿Qué cambios se realizaron? La configuración almacenada en el servidor TFTP se cargó en el router.

c. Emita el comando **show** adecuado para mostrar el estado de la interfaz. ¿Todas las interfaces están activas? No, la interfaz Gi0/1 está inactiva administrativamente. Todas las interfaces del router están desactivadas de manera predeterminada.

d. Corrija cualquier problema relacionado con las interfaces y pruebe la conectividad.





Parte 3: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP

a. Cambie el nombre de host **RTA** a **RTA-1**.

b. Guarde la configuración en la NVRAM.

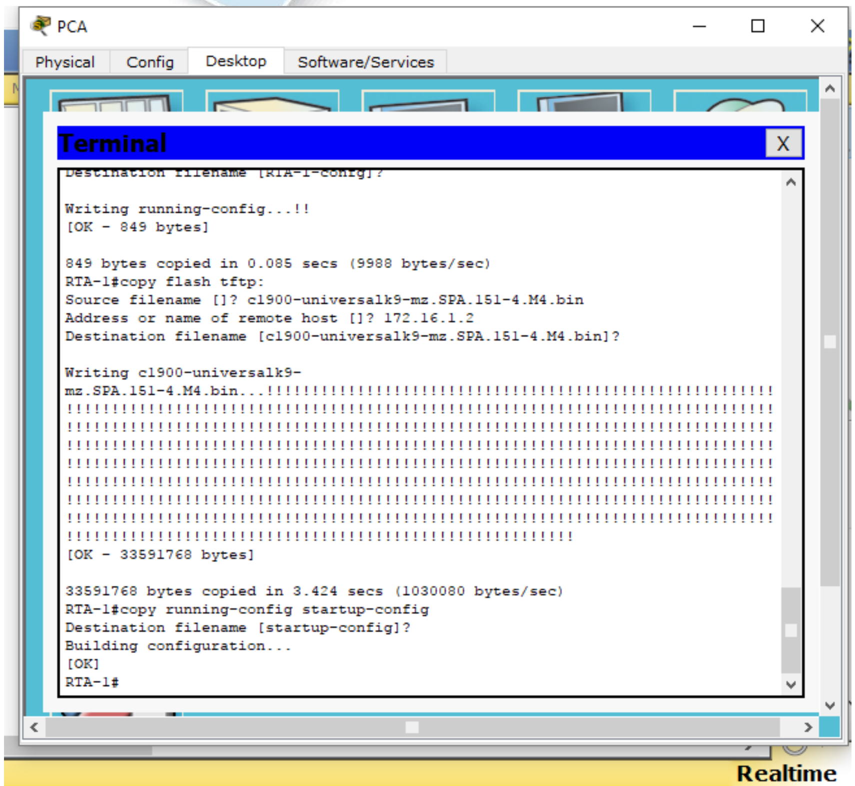
c. Copie la configuración al **servidor TFTP** con el comando **copy**:

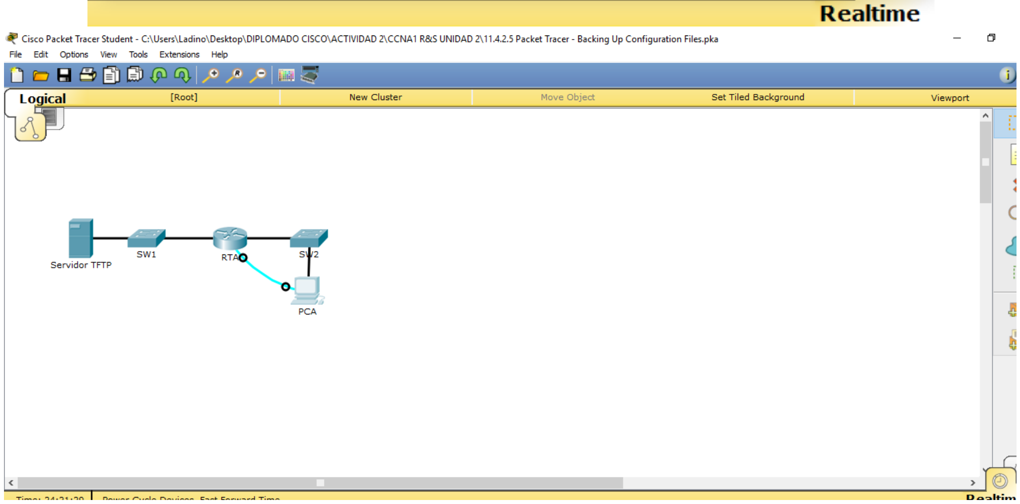
```
RTA-1# copy running-config tftp:
Address or name of remote host []? 172.16.1.2
Destination filename [RTA-1-confg]? <cr>
```

d. Emita el comando para mostrar los archivos ubicados en la memoria flash.

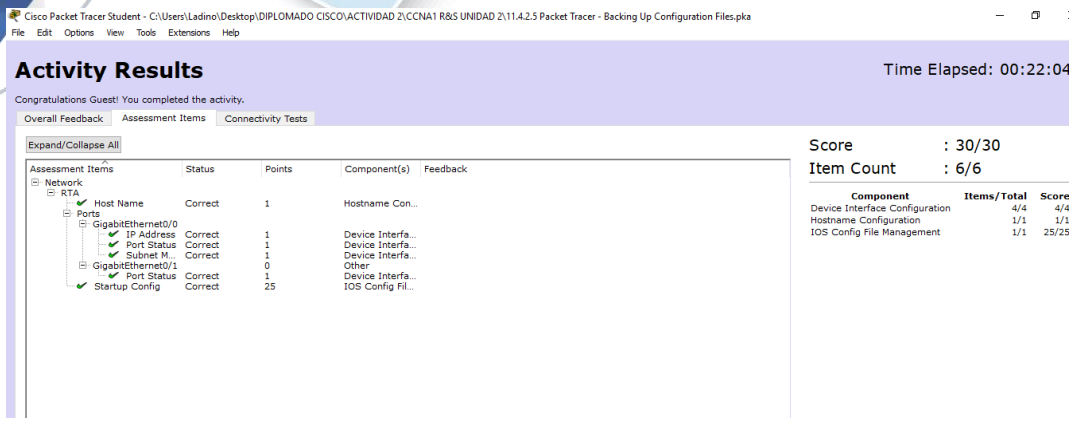
e. Copie el IOS que está en la memoria flash al **servidor TFTP** con el siguiente comando:

```
RTA-1# copy flash tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? <cr>
```


PCA
Physical
Config
Desktop
Software/Services
Terminal
Writing running-config...!!
[OK - 849 bytes]
849 bytes copied in 0.085 secs (9988 bytes/sec)
RTA-1#copy flash tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?
Writing c1900-universalk9-
mz.SPA.151-4.M4.bin...!!
!!
!!
!!
!!
!!
!!
!!
!!!
[OK - 33591768 bytes]
33591768 bytes copied in 3.424 secs (1030080 bytes/sec)
RTA-1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTA-1#
Realtime


Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\11.4.2.5 Packet Tracer - Backing Up Configuration Files.pka
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Servidor TFTP
SW1
RTA
SW2
PCA


Cisco Packet Tracer Student - C:\Users\Ladino\Desktop\DIPLOMADO CISCO\ACTIVIDAD 2\CCNA1 R&S UNIDAD 2\11.4.2.5 Packet Tracer - Backing Up Configuration Files.pka
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:21:57
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the Packet Tracer - Backing Up Configuration Files activity.



Ejercicio 11.5.2.4: Configuración de un router Linksys

Topología

Objetivos

Parte 1: Conectar al router Linksys

Parte 2: Habilitar conectividad inalámbrica

Parte 3: Configurar y verificar el acceso al cliente inalámbrico

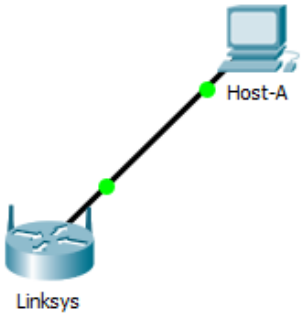
Información básica

En esta actividad, configurará un router inalámbrico Linksys, lo que permite el acceso remoto a los clientes inalámbricos así como conectividad con seguridad WPA.

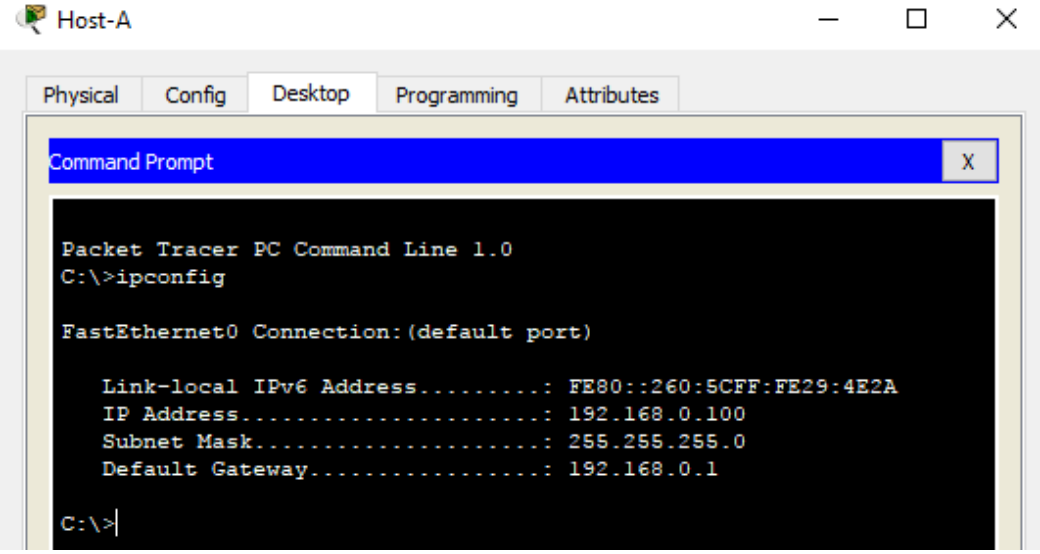
Parte 1: Conectar al router Linksys

Paso 1: Establecer y verificar la conectividad al router Linksys

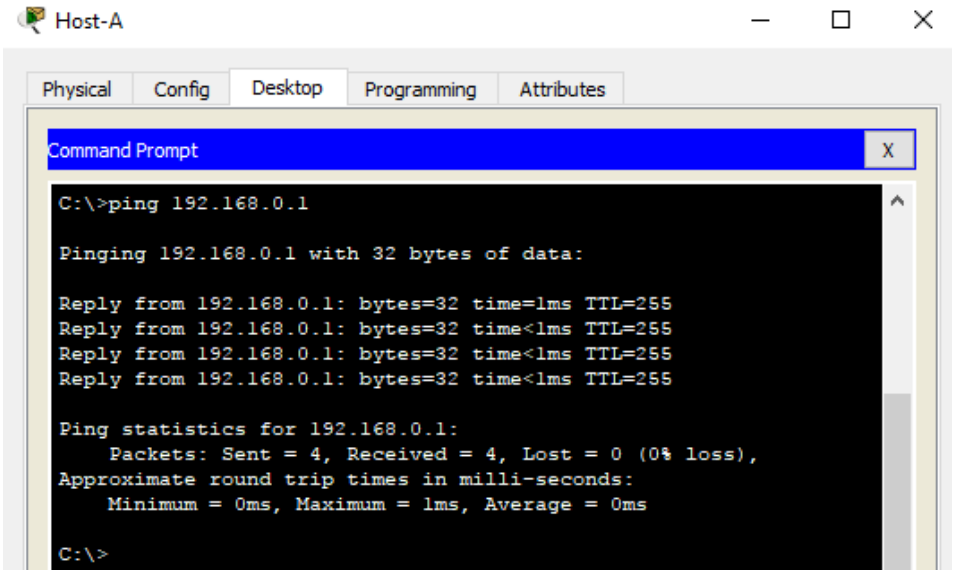
- Conecte el cable adecuado del **Host-A** al puerto Ethernet 1 en **Linksys**.



- Espere a que la luz de enlace se vuelva de color verde. A continuación, abra el símbolo del sistema para el **Host-A**. Utilice el comando **ipconfig** para verificar la información de direccionamiento IP del **Host recibido**.



- Introduzca el comando **ping 192.168.0.1** para verificar que el **Host-A** pueda acceder al gateway predeterminado.

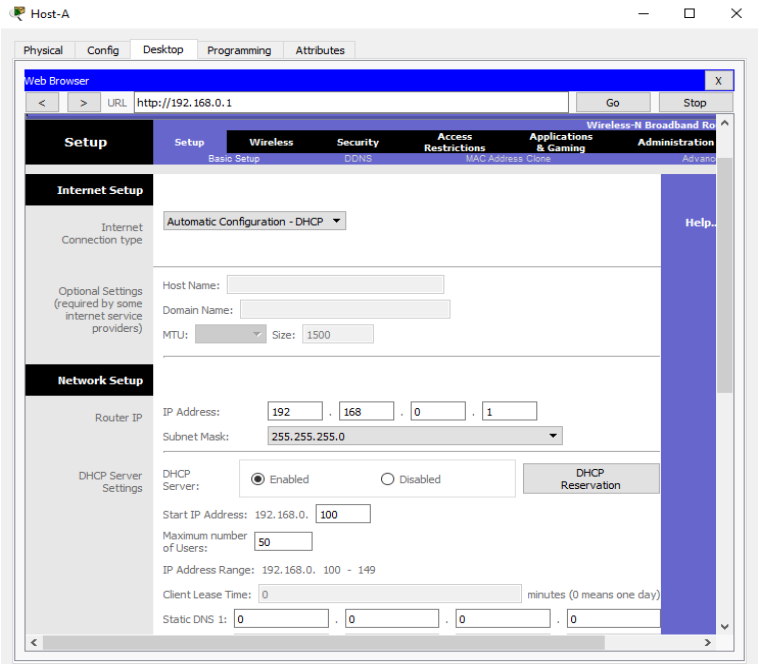


Paso 2: Acceda a la interfaz gráfica de usuario (GUI) de Linksys mediante un explorador Web.

w. Para configurar el router **Linksys** con la GUI, debe acceder a este mediante el explorador Web del **Host-A**. Abra el explorador Web y escriba la dirección de gateway predeterminado en el campo de dirección URL para acceder a **Linksys**.

x. Introduzca **admin** como nombre de usuario y contraseña predeterminados para acceder al router **Linksys**.

Nota: no podrá ver el cambio en la puntuación al configurar el router **Linksys** hasta que haya hecho clic en **Save Settings** (Guardar configuración).


Host-A
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://192.168.0.1
Go
Stop
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Basic Setup
DDNS
MAC Address Clone
Internet Setup
Internet Connection type
Automatic Configuration - DHCP
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size:
1500
Network Setup
Router IP
IP Address:
192
168
0
1
Subnet Mask:
255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
192.168.0.
100
Maximum number of Users:
50
IP Address Range:
192.168.0.
100
149
Client Lease Time:
minutes (0 means one day)
Static DNS 1:
Help

Parte 2: Habilitar conectividad inalámbrica

Paso 1: Configure el router Linksys para que tenga conectividad a Internet.

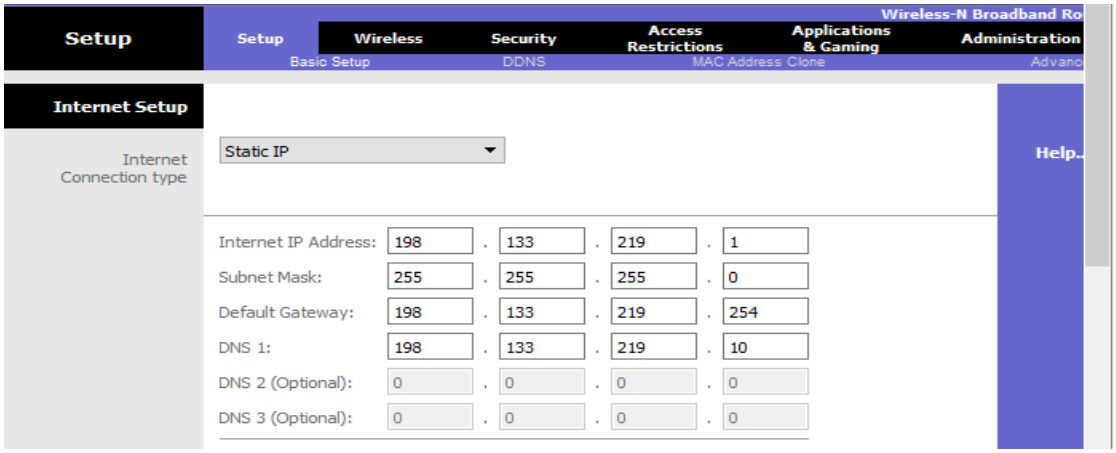
En esta situación no hay conectividad a Internet, pero de todas formas configurará los parámetros para la interfaz con conexión a Internet. Para **Internet Connection Type** (Tipo de conexión a Internet), elija **Static IP** (IP estática) en la lista desplegable. A continuación, introduzca la siguiente información de IP estática:

j. Dirección IP de Internet: **198.133.219.1**

k. Máscara de subred: **255.255.255.0**

l. Gateway predeterminado: **198.133.219.254**

m. DNS 1: **198.133.219.10**



Paso 2: Configure los parámetros de red internos.

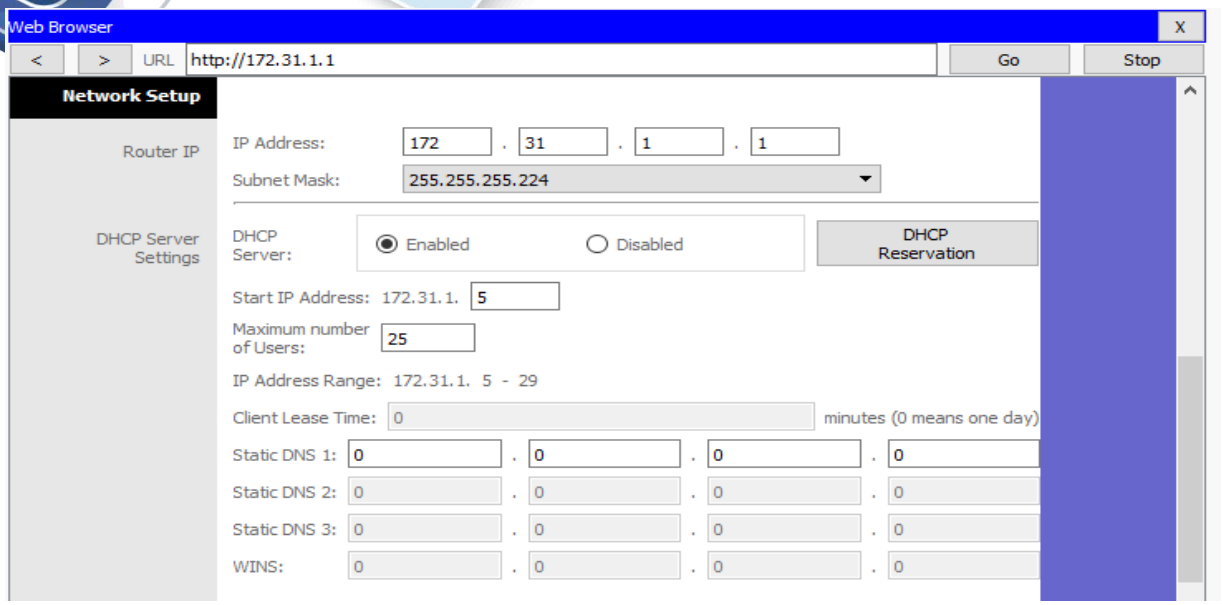
Desplácese hasta la sección **Network Setup** (Configuración de red) y configure la siguiente información:

m. Dirección IP: **172.31.1.1**

n. Máscara de subred: **255.255.255.224**

o. Dirección IP de inicio: introduzca **5** para el último octeto.

p. Cantidad máxima de usuarios: **25**



Nota: el rango de direcciones IP del pool de DHCP solo refleja los cambios una vez que hace clic en
Save Settings.

Paso 3: Guardar la configuración y volver a conectarse al router Linksys

h. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**. Si pasa de una ficha a otra sin guardar la configuración, esta se perderá.

i. Cuando hace clic en **Save Settings**, se pierde la conexión. Esto ocurre porque cambió la dirección IP del router.

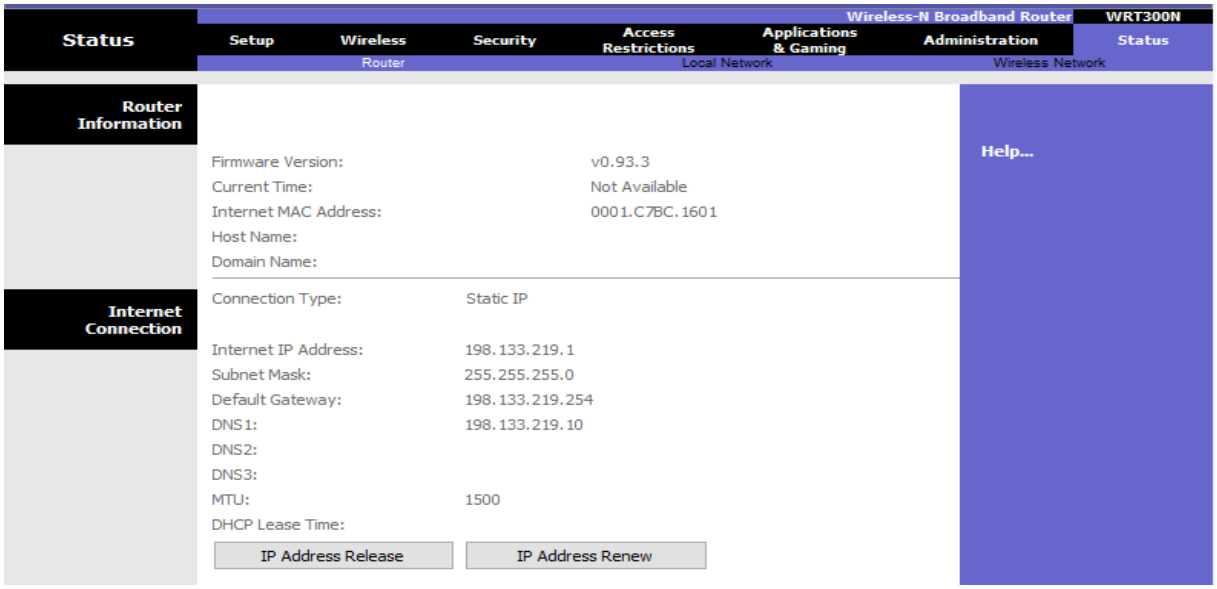
j. Regrese al símbolo del sistema del **Host-A**. Introduzca el comando **ipconfig /renew** para renovar la dirección IP.

```
C:\>ipconfig /renew

IP Address.....: 172.31.1.5
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 172.31.1.1
DNS Server.....: 198.133.219.10

C:\>
```

k. Utilice el explorador Web del **Host-A** para volver a conectarse al router **Linksys**. Deberá utilizar la nueva dirección de gateway predeterminado. Verifique la configuración de **Internet**

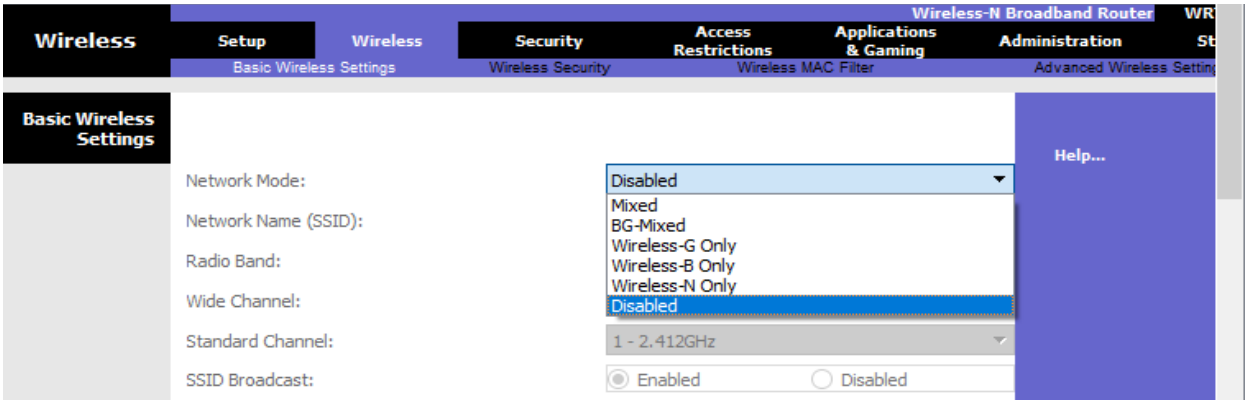
Connection (Conexión

a Internet) en la ficha **Status** (Estado). La configuración debe coincidir con los valores que configuró en el paso 1 de la parte 2. Si no coinciden, repita los pasos 1 y 2 de la parte 2.



Paso 4: Configurar la conectividad inalámbrica de los dispositivos inalámbricos

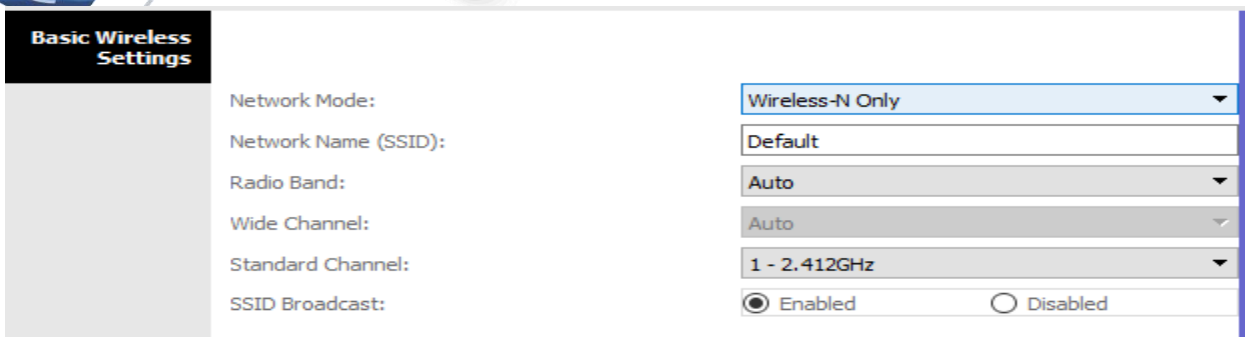
k. Haga clic en la ficha **Wireless** (Conexión inalámbrica) e investigue las opciones de la lista desplegable de **Network Mode** (Modo de red).



¿En qué caso elegiría la opción **Disable** (Deshabilitar)?
R: Cuando no haya dispositivos inalámbricos.

¿En qué caso elegiría la opción **Mixed** (Combinada)?
R: Cuando hay dispositivos inalámbricos que constan de B, G o N.

l. Configure el modo de red en **Wireless-N Only** (Solo Wireless-N).



m. Cambie el SSID a **MiRedDoméstica.**

¿Cuáles son dos características de un SSID?
R: Distingue mayúsculas de minúsculas y el nombre no puede exceder los 32 caracteres.

d. Cuando un cliente inalámbrico busca redes inalámbricas en el área, este detecta cualquier transmisión del SSID. Las transmisiones del SSID están habilitadas de manera predeterminada.

Si no se transmite el SSID de un punto de acceso, ¿cómo se conectan los dispositivos a este?
R: El cliente debe estar configurado con el nombre, el cual debe estar escrito correctamente para que se lleve a cabo la conexión.

e. Para obtener el mejor rendimiento de una red que utiliza Wireless-N, configure la banda de radio en **Wide-40MHz** (40 MHz de ancho).

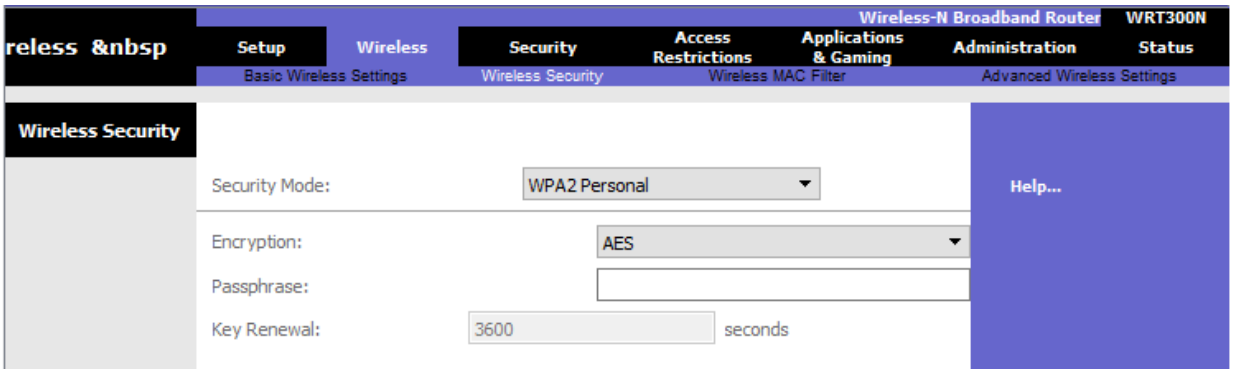
f. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 5: Configure la seguridad inalámbrica de modo que los clientes deban autenticarse para

poder conectarse a la red inalámbrica.

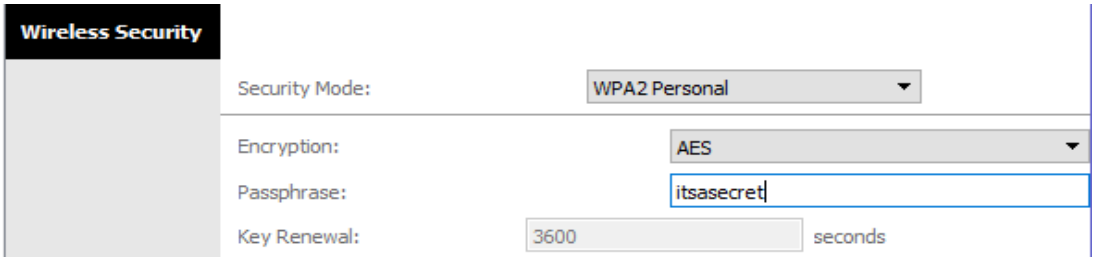
a. Haga clic en la opción **Wireless Security** (Seguridad inalámbrica) en la ficha **Wireless**.

b. Configure el **Security Mode** (Modo de seguridad) en **WPA2 Personal**.



¿Cuál es la diferencia entre la opción Personal y la opción Enterprise (Empresa)?
R: La opción Enterprise utiliza un servidor Radius para autenticar a los usuarios, mientras que el modo Personal utiliza el router Linksys para autenticar los usuarios.

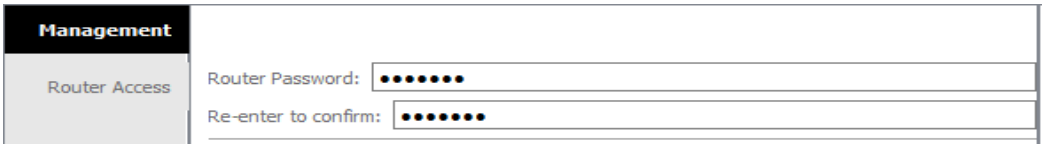
c. Deje el modo de encriptación en AES y establezca la frase de contraseña **itsasecret**.



d. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue** (Continuar).

Paso 6: Cambie la contraseña predeterminada para acceder a la configuración del router Linksys.

a. Siempre debe cambiar la contraseña predeterminada. Haga clic en la ficha **Administration** (Administración) y cambie la contraseña de **Router Access** (Acceso al router) por **letmein**.



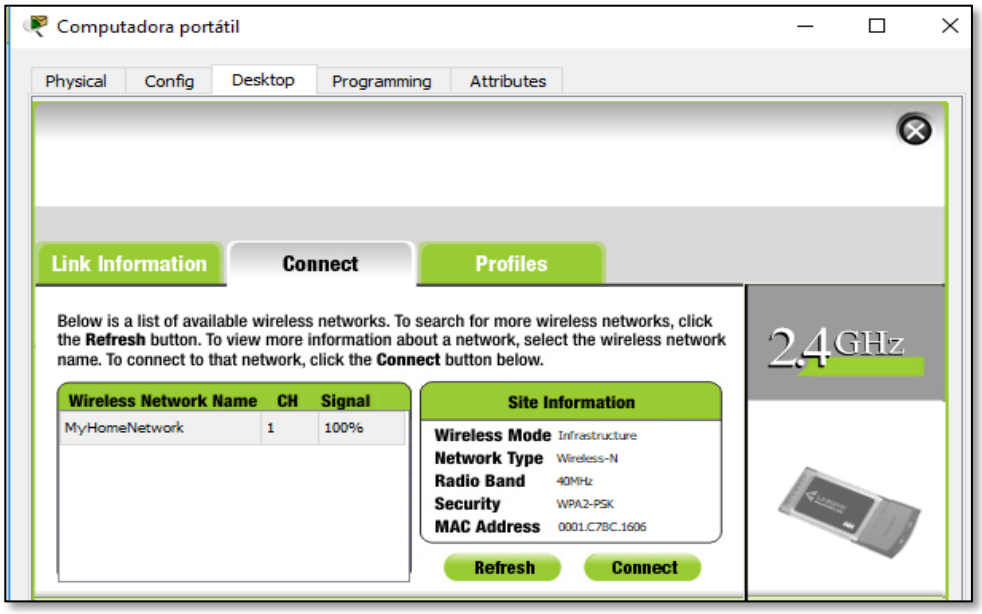
b. Haga clic en **Save Settings**. Introduzca el nombre de usuario **admin** y la nueva contraseña.

Parte 3: Configurar y verificar el acceso al cliente inalámbrico

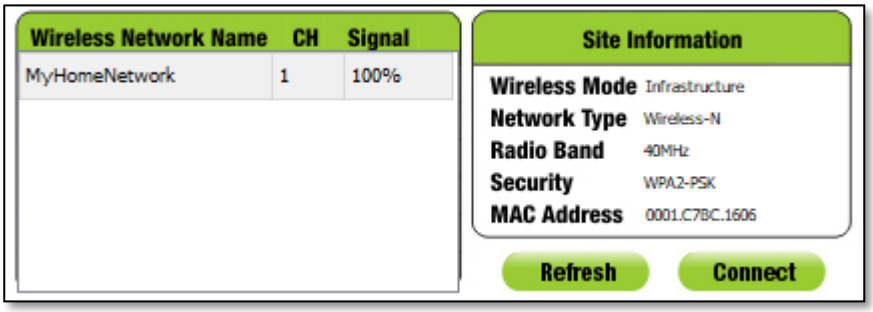
Paso 1: Configurar la computadora portátil para acceder a la red inalámbrica

a. Haga clic en **Laptop** (Computadora portátil) y después en **Desktop** > **PC Wireless** (PC inalámbrica). La ventana que se abre es la GUI de Linksys del cliente.

b. Haga clic en la ficha **Connect** (Conectar) y después en **Refresh** (Actualizar), si es necesario. Debería ver la red **MiRedDoméstica** indicada en Wireless Network Name (Nombre de red inalámbrica).

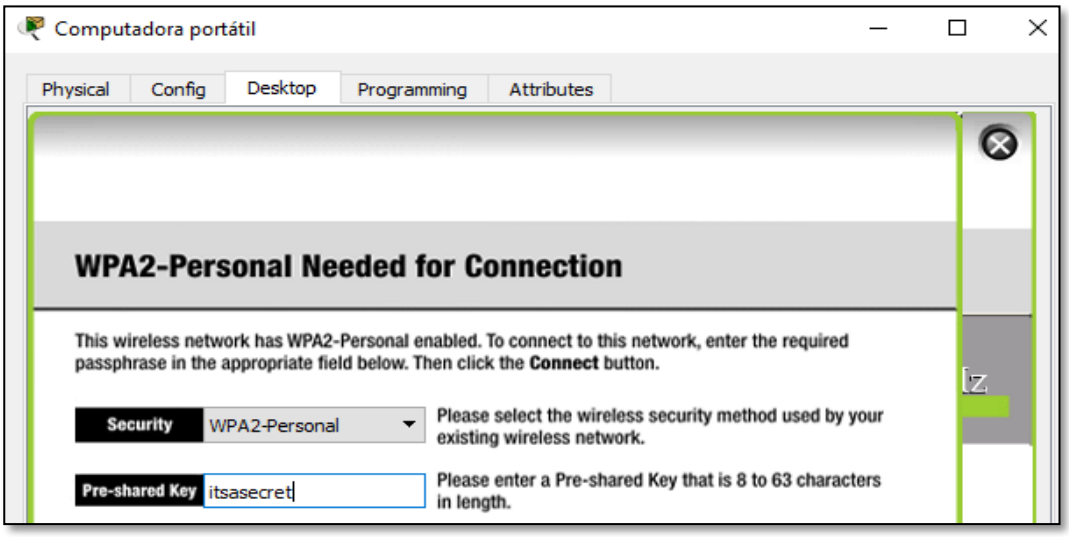


c. Haga clic en **MiRedDoméstica** y después en **Connect**.

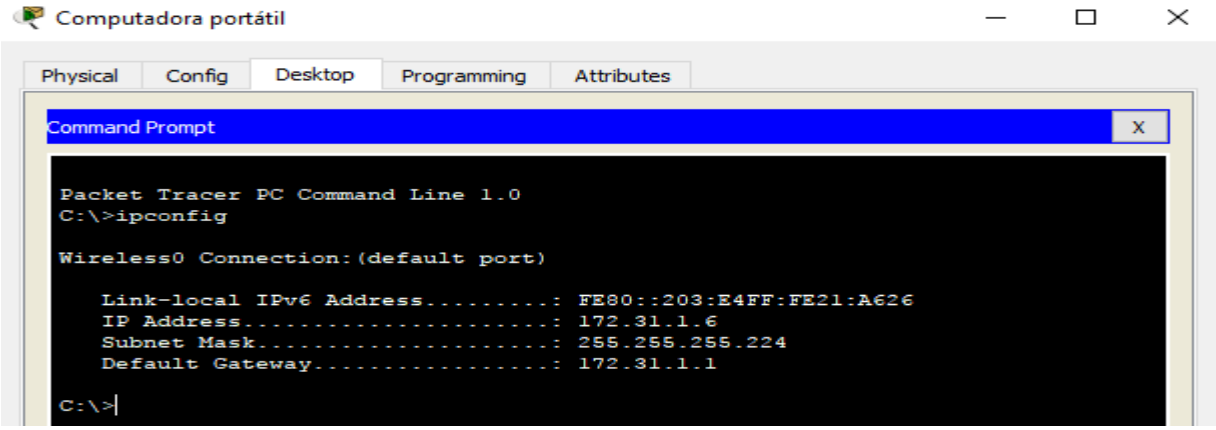


d. Ahora debería ver la red **MiRedDoméstica**. Haga clic en esta y después en **Connect**.

e. La **Pre-shared Key** (Clave previamente compartida) es la contraseña que configuró en el paso 5c de la parte 2. Introduzca la contraseña y haga clic en **Connect**.

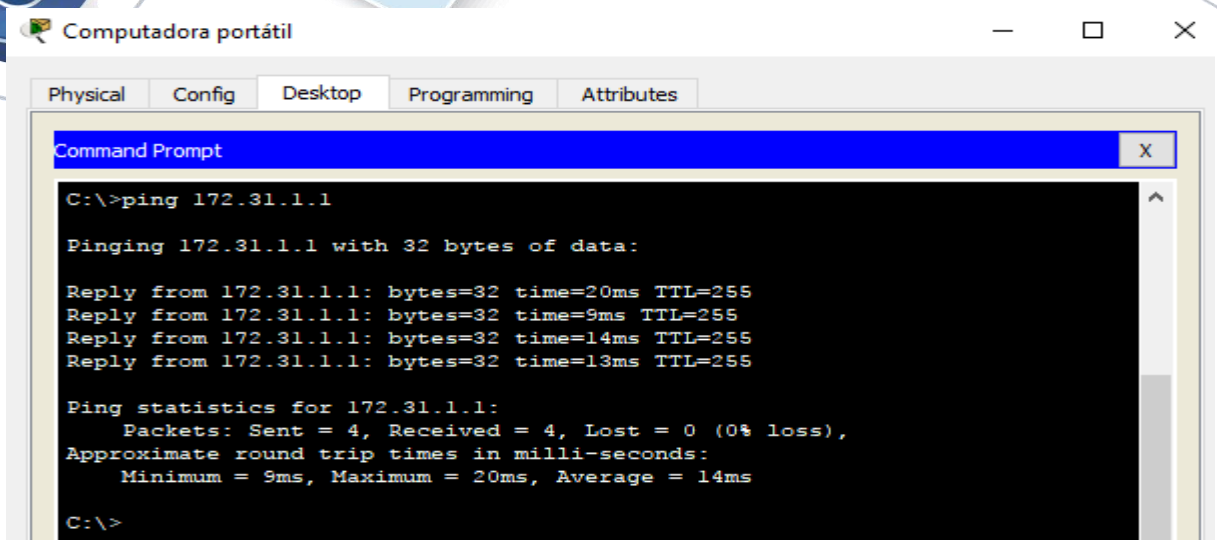


f. Cierre la GUI de Linksys y haga clic en **Command Prompt** (Símbolo del sistema). Introduzca el comando **ipconfig** para verificar si **Laptop** recibió el direccionamiento IP.

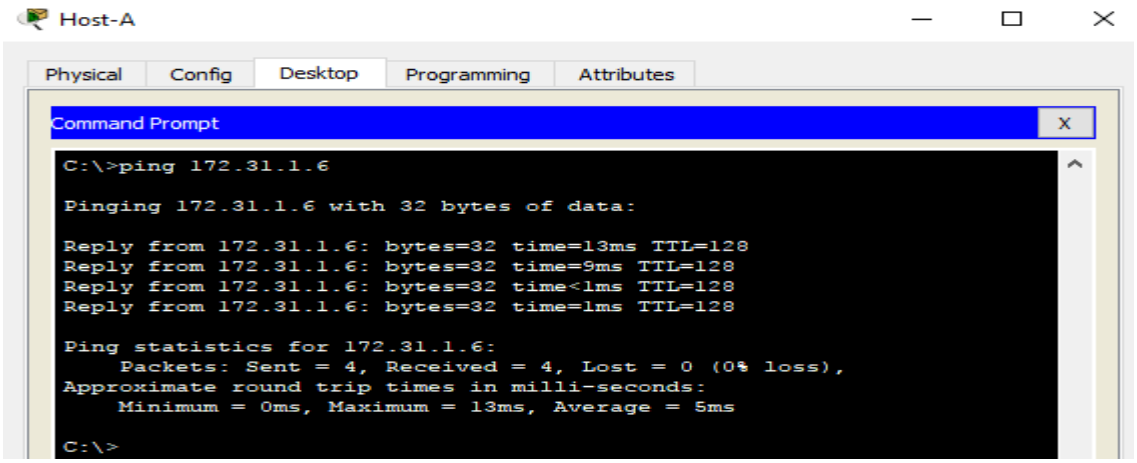


Paso 2: Verificar la conectividad entre la computadora portátil y el Host-A

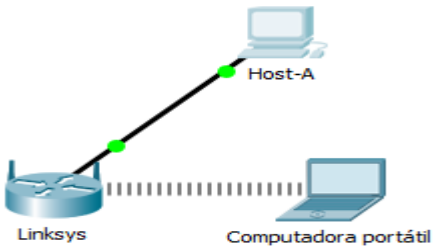
a. Haga ping al router **Linksys** desde la **computadora portátil**.

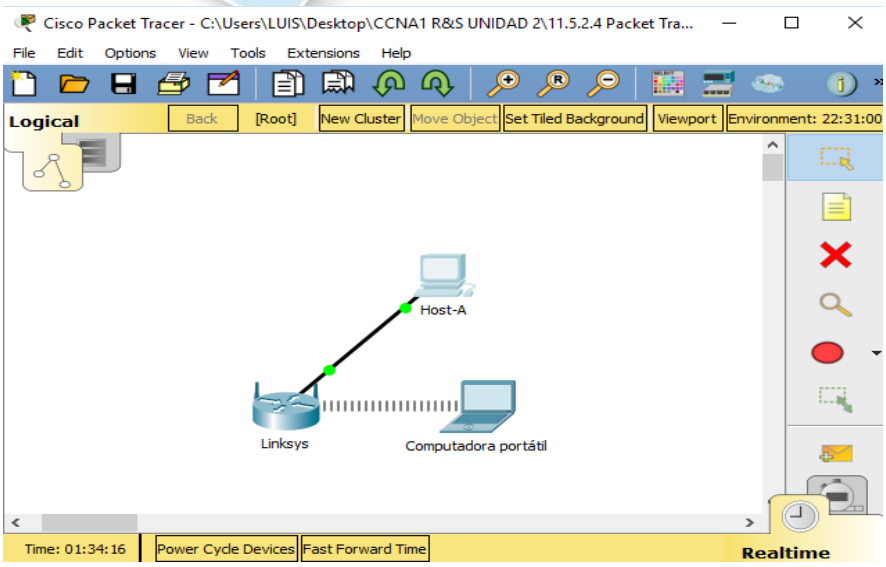


b. Haga ping desde el **Host-A** a la **computadora portátil.**



Conexión Red final





Ejercicio 11.6.1.2: Reto de habilidades de integración

Topología

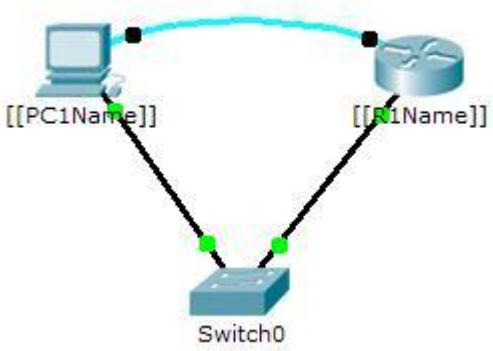


Tabla de direccionamiento

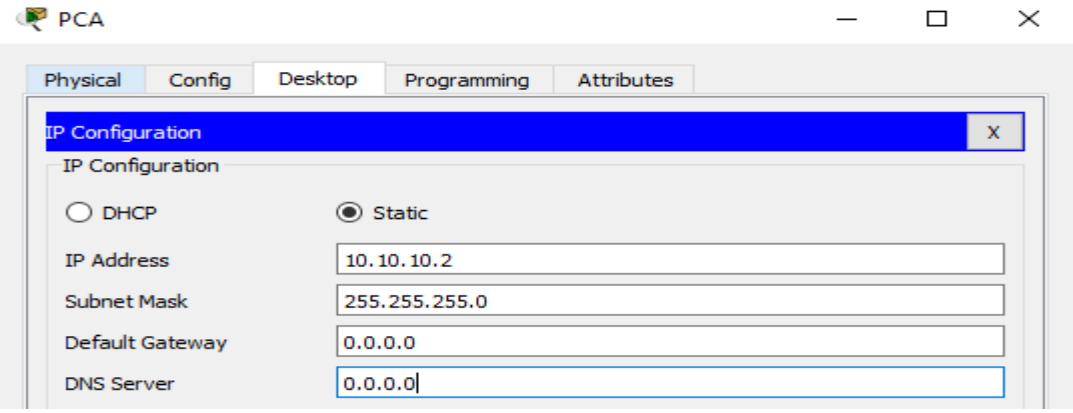
Dispositivo	Interfaz	Dirección IP	Máscara de subred
RTA	G0/0	10.10.10.1	255.255.255.0
PCA	NIC	10.10.10.2	255.255.255.0

Situación

El administrador de red le solicitó que prepare un router para la implementación. Antes de que pueda conectarse a la red, se deben habilitar las medidas de seguridad. En esta actividad, encriptará y configurará contraseñas seguras. A continuación, configurará SSH para obtener acceso remoto y demostrará que puede acceder al router desde una PC.

Requisitos

- Configure el direccionamiento IP en **PCA** y **RTA**.




```
Router>enable
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shut

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

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

Router(config-if)#

- Configure el nombre de host como **RTA** y encripte todas las contraseñas de texto no cifrado.

```
Router(config-if)#exit
Router(config)#hostname RTA
RTA(config)#service password-encryption
RTA(config)#
```

- Establezca la contraseña secreta segura que desee.

```
RTA(config)#enable secret Ci$coLetmein
RTA(config)#
```

- Establezca el nombre de dominio en **RTA** (distinguir mayúsculas de minúsculas).
  `RTA(config)#` **`ip domain-name RTA1`**

```
RTA(config)#ip domain-name RTA
RTA(config)#
```

- Cree un usuario de su elección con una contraseña segura.
  `RTA` `(config)#` **`user Luis password Ci$co001`**

```
RTA(config)#user Luis password Ci$co001
RTA(config)#
```

- Genere claves RSA de 1024 bits.

  Nota: en Packet Tracer, introduzca el comando **crypto key generate rsa** y presione tecla **Entrar** para continuar.

`RTA(config)#` **`crypto key generate rsa`**

```
RTA(config)#crypto key generate rsa
The name for the keys will be: RTA.RTA
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RTA(config)#
```

y. Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.

`[[R1Name]](config)#` **`login block-for 180 attempts 4 within 120`**

```
RTA(config)#login block-for 180 attempts 4 within 120
*mar. 1 1:18:40.588:  %SSH-5-ENABLED: SSH 1.99 has been enabled
RTA(config)#
```

z. Configure las líneas vty para el acceso por SSH y solicite los perfiles de usuarios locales.

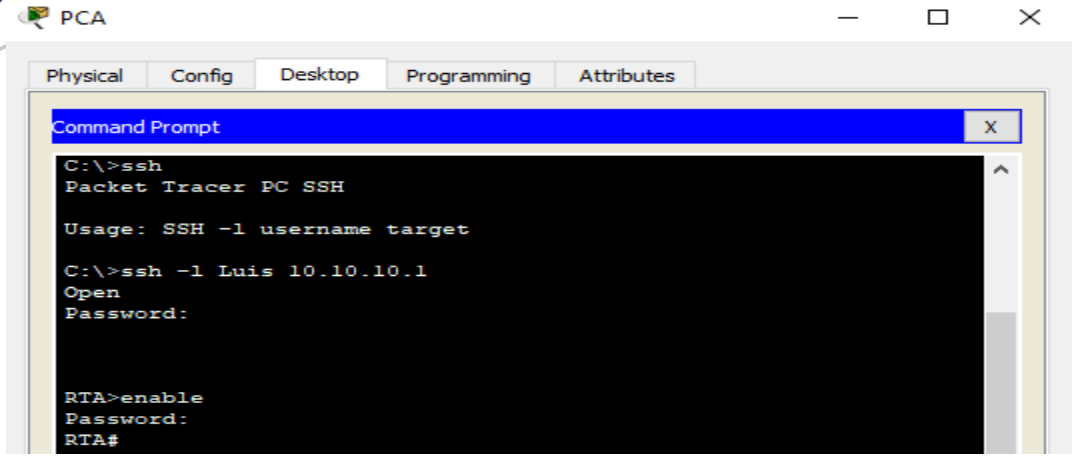
```
RTA(config)#line vty 0 15
RTA(config-line)#transport input ssh
RTA(config-line)#login local
RTA(config-line)#
```

aa. Guardar la configuración en la NVRAM.

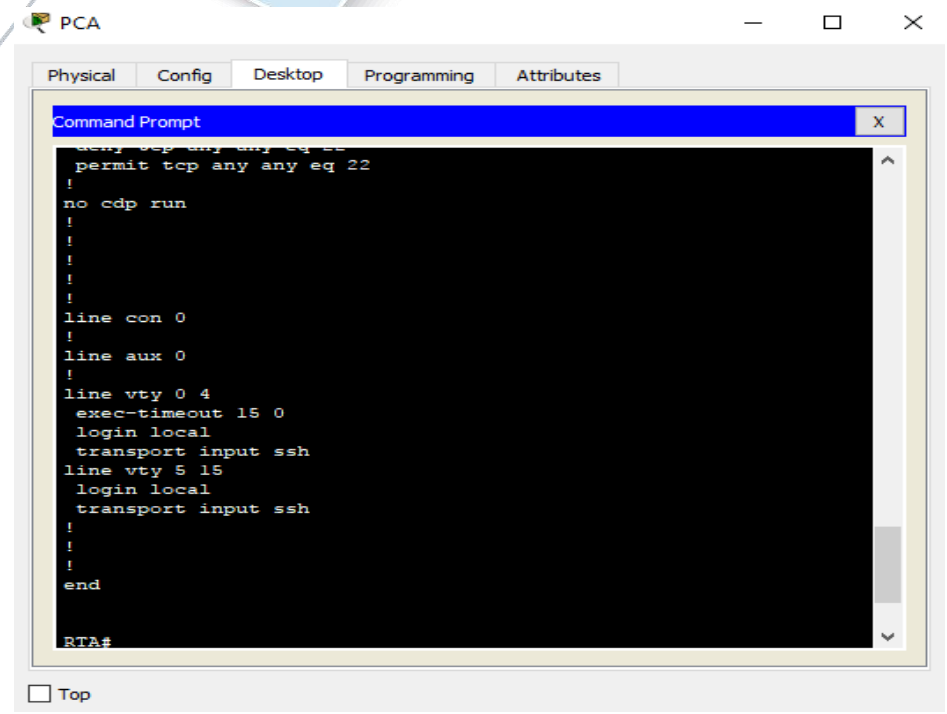
```
RTA#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
RTA#
```

bb. Esté preparado para demostrar al instructor que estableció el acceso por SSH de **PCA a RTA.**

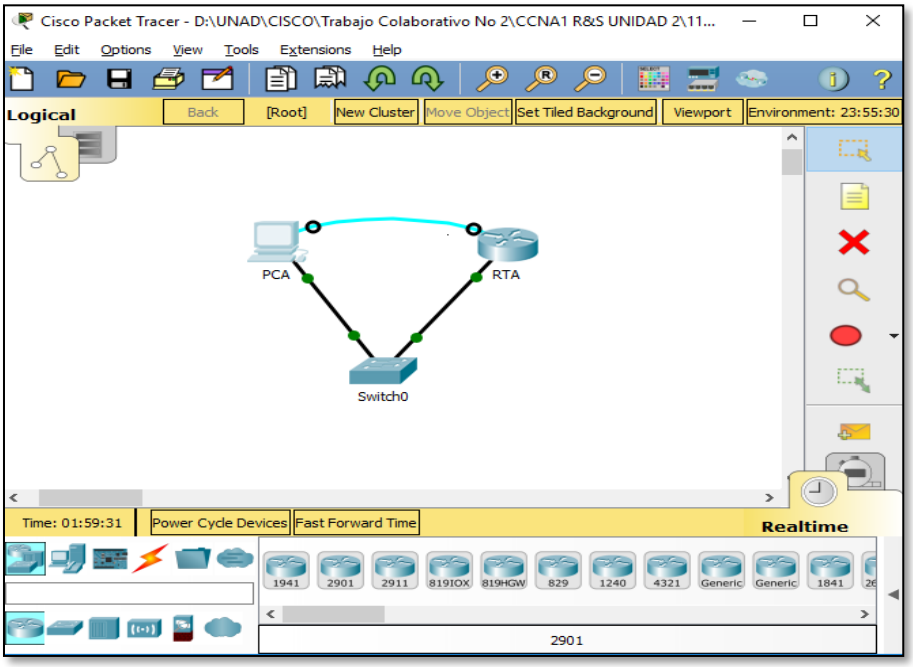
ID:10




```
RTA#show running
Building configuration...

Current configuration : 1211 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RTA
!
login block-for 180 attempts 4 within 120
!
enable secret 5 $1$mERr$oYgkCAl1OOcOAKSkOlk2D.
!
ip cef
no ipv6 cef
!
username Luis password 7 0802450A0A16554743
username any_Luis password 7 08204257363A0C5311044F547A7A
```


PCA
Physical
Config
Desktop
Programming
Attributes
Command Prompt
permit tcp any any eq 22
!
no cdp run
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
exec-timeout 15 0
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
end
RTA#
Top

Red final


Cisco Packet Tracer - D:\UNAD\CISCO\Trabajo Colaborativo No 2\CCNA1 R&S UNIDAD 2\11...
File
Edit
Options
View
Tools
Extensions
Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 23:55:30
PCA
RTA
Switch0
Time: 01:59:31
Power Cycle Devices
Fast Forward Time
Realtime
1941
2901
2911
819IOX
819HGW
829
1240
4321
Generic
Generic
1841
2901

CONCLUSIONES

Al haber concluido el desarrollo del presente trabajo se pudo establecer la importancia de los conocimientos adquiridos en los temas estudiados en la unidad dos, en total se desarrollaron 22 ejercicios utilizando el simulador de red Packet Tracer.

Se lograron identificarán y solucionar los problemas de las sub-redes y del direccionamiento IP mediante el uso adecuado de las estrategias basadas en comandos y estadísticas del IOS, con el cual se logró fortalecer el desarrollo de las competencias en el área de las redes orientadas al enrutamiento avanzado.

REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-ssets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-course-ssets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://static-course-ssets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3