Cisco Networking Academy®

Mind Wide Open™

Trabajo colaborativo 2

Ariel Otalora Ramirez -1079409358
Claudia Yoana Otalvaro Garces – 1111198435
Edinson Moreno
Sandra Liliana Martinez Castellanos - 1030523393
Yeison Daniel Parra Medina - 1049634007
Grupo 203092_52

Tutor
Nilson Albeiro Ferreira Manzanares

Universidad Nacional Abierta y a Distancia – UNAD
Diplomado de Profundizacion CISCO (Diseño e Implementacion de Soluciones Integradas LAN/WAN)
Semestre B 2017

Introduccion

En las comunicaciones TCP y UDP lo que se busca es generr trafico de red, en este caso en modo de simulacion en Packet Tracer al igual que examinar la funcionalidad de los protocolos TCP y UDP, cuando se investiga el trafico unicast, broadcast y multicast, lo que se esta examinando es el comportamiento de los mismos, siendo la matoria del trafico de red unicast, se tiene que recordar que la direccion de destino en el encabezado del aquete IP es la direccion IP de la interfaz del router remoto.

Cuando se realizan las configuraciones de direcciones IPv6 se tiene en cuenta que estas se realizan en los routers, servidores y en los clientes, asi mismo se debe probar y verificar la conectividad a la red, por otro lado se hara verificacion del direccionamiento IPv4 en IPv6 probando la conectividad mediante el comando ping y descubrir su ruta mediante su rastreo para probar las rutas.

En cuanto a la resolucion de problemas de direccionamiento IPv4 e IPv6 lo que se hara la verificacion detallada del soporte tecnico, en donde se consideraran las causas probables de la falla, proponer una solucion para resolver el problema, implementar el plan y verificar que esa solucion dada haya resuelto el problema, de igual manera se evidencia las habilidades de integracion en cuanto a configuracion de direccionamiento IPv4 e IPv6 y su verificacion en cuanto a conectividad.

En la situacion de division de subredes se realiza el diseño de un esquema de direccionamiento IP, y el direccionamiento IP a los dispositivos de red al igual que la verificacion a la conctividad, en la cual cada LAN de la red necesita espacio suficiente para alojar, como minimo 15 direcciones para los dispositivos finales, el switch y el router, en lo que es el diseño e implementacion de un esquema de direccionamiento VSLM se examinara los requisitos de la red, posteriormente se diseña el esquema de direccionamiento VSLM y finalmente las asignaciones de direcciones IP a los dispositivos y la verificacion de la conectividad.

Aviendo trabajado en el punto anterior se hace revision y trabajo en la implemetacion de un esquema de direccionamiento IPv6 dividido en subredes, para ello sedetermina las subredes y el esquema de direccionamiento IPv6 al igual que la configuracion en los routers, los pc y su verificacion, poniendo en practica las habilidades de integracion.

En la configuracion de servidores web y de correo electronico, se configurara los servicios HTTP y de correo electronico mediante el simulador de Packet Tracer, verificando los servicios web, en cuanto a los servidores de DHCP y servidores DNS se configurara y verificara el direccionamiento IP estatico y el direccionamiento DHCP, asi mismo se configurara un servidor de DNS para que se le asigne direcciones IP a los nombres de sitios web.

Los servidores FTP seran configurados para la utilizacion de los servicios FTP para transferir archivos entre los clientes y el servidor, por otro lado se manejara la funcion multiusuario de Packet Tracer, en la cual se establecera una conexión multiusuario local en otra instancia de Packet Tracer, a la cual se le

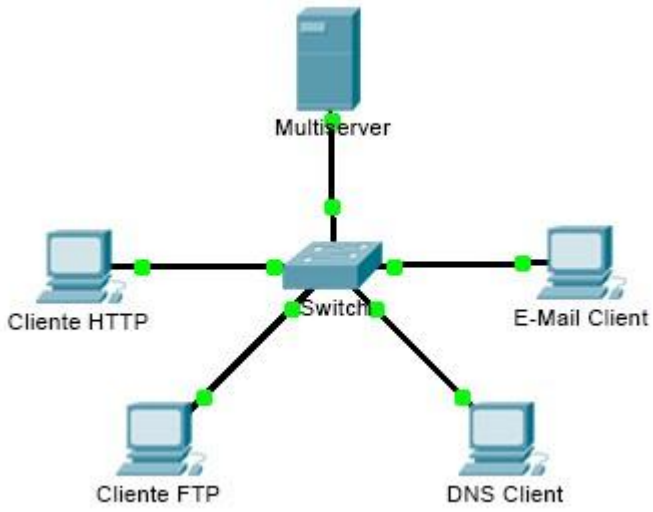
verificara la conectividad, tambien se maneja la implementacion de servicios, en esta implementacion se estara en dos partes una del lado del servidor y la otra del lado del cliente, en la que esta del lado del servidor implementa y verifica los servicios, y el que esta del lado del cliente configura y verifica el acceso a los servicios.

Hay que probar la conectividad con tracerouter, la cual se hara de extremo a extremo con el comando tracert y comparar con el comando tracerouter en un router, esta resolucion de problemas de cnectividad de red se lleva a cabo utilizando comandos para rastrear la ruta de origen a destino, tambien se hace uso de los comandos show para analisis de los resultados.

En cuanto a la realizacion de copias de seguridad de archivos de configuracion, lo que se realiza como primer medida es establecer la conectividad al servidor TFTP, en seguida es transferir l aconfiguracion del servidor y finalmente las copias de seguridad de la cnfiguracion y de IOS en el servidor FTFP, para finalizar se verificara las habilidades de integracion.

7.3.1.2 Comunicaciones TCP y UDP

Topología



Objetivos

Parte 1: Generar tráfico de red en modo de simulación

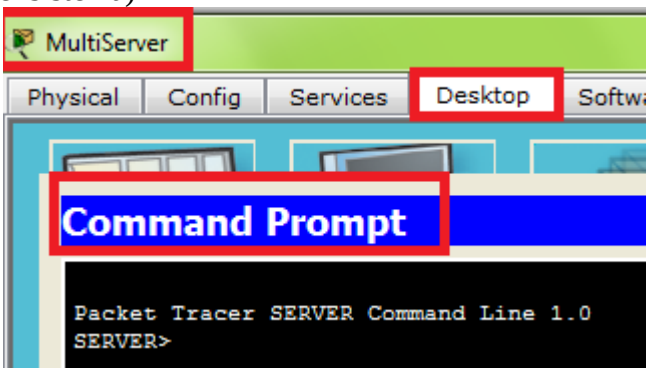
Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

Parte 1: Generar tráfico de red en modo de simulación

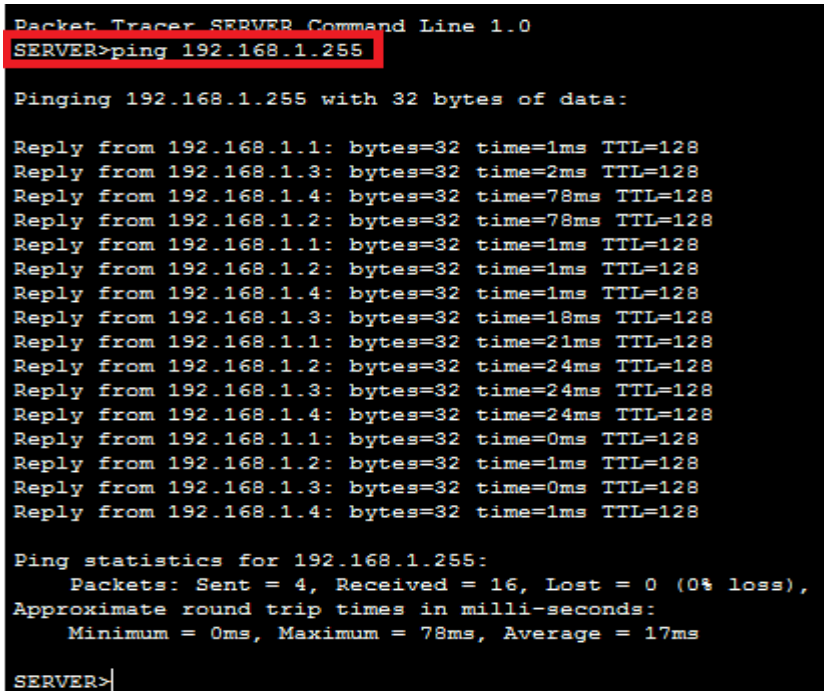
Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)

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

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



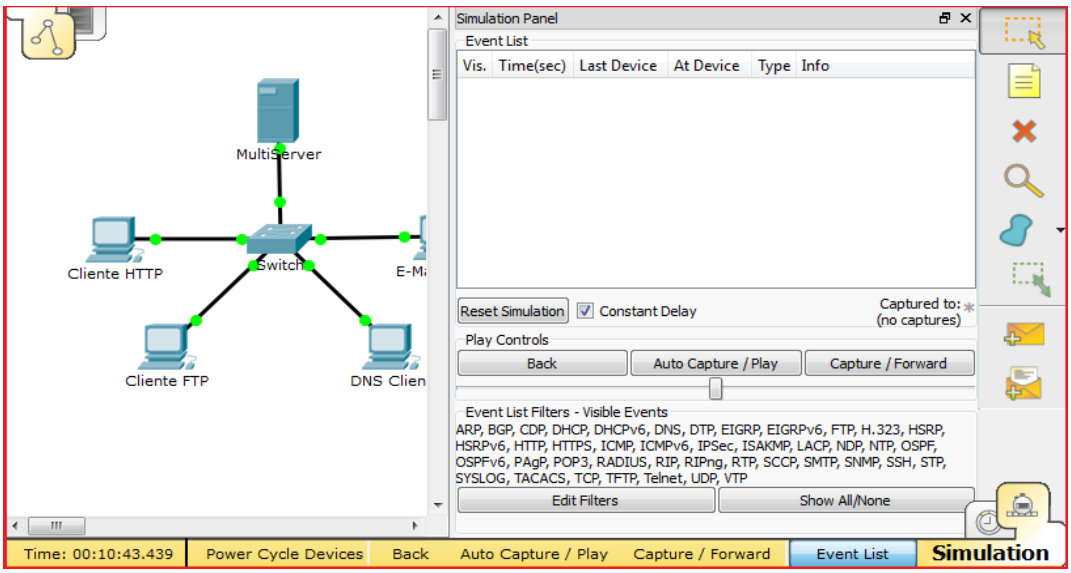
b. Introduzca el comando **ping 192.168.1.255**. Esto toma unos segundos, ya que todos los dispositivos en la red responden a **MultiServer**.



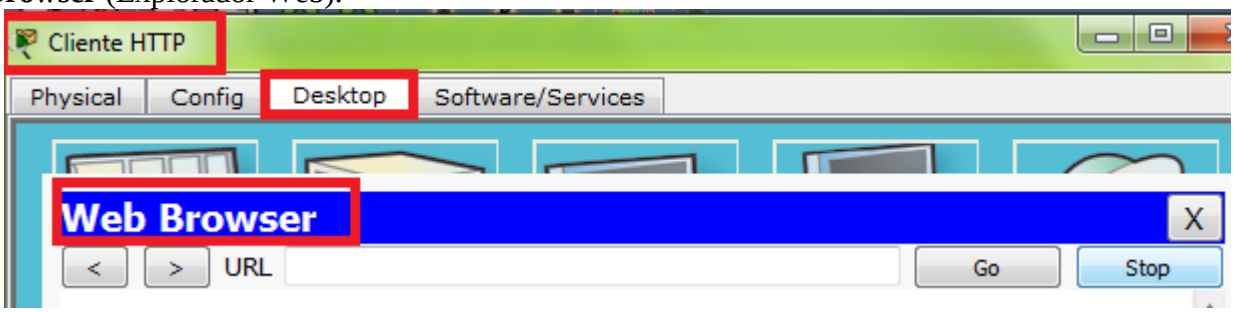
c. Cierre la ventana de **MultiServer**.

Paso 2: Genere tráfico web (HTTP).

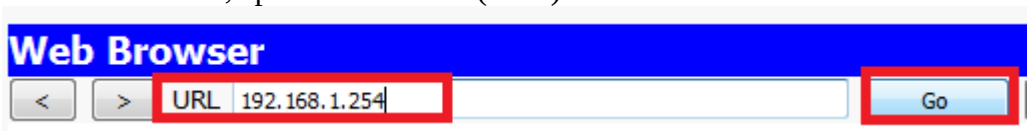
a. Cambie a modo de simulación.



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).

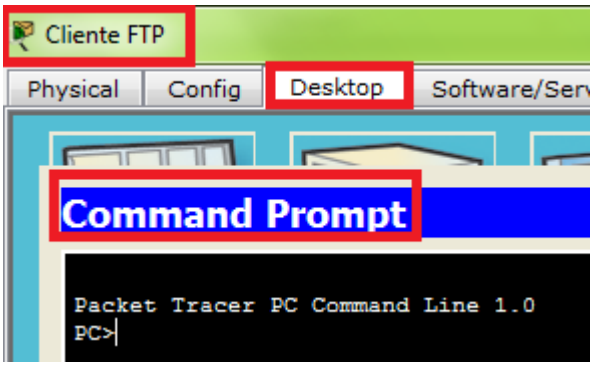


Después de dar Go

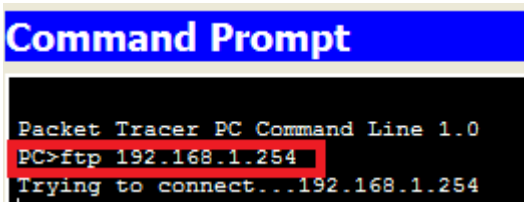
d. Minimice (pero no cierre) la ventana de configuración de **HTTP Client**.

Paso 3: Generar tráfico FTP

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



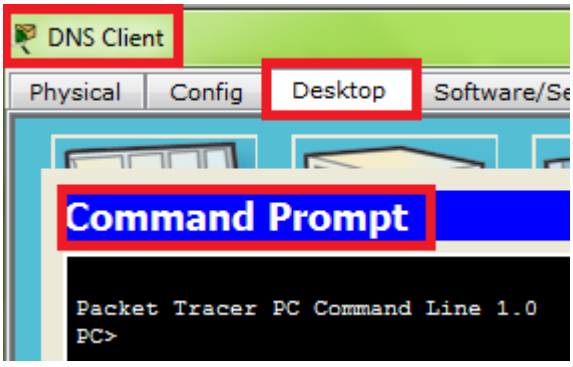
b. Introduzca el comando **ftp 192.168.1.254**. En la ventana de simulación, aparecerán PDU.



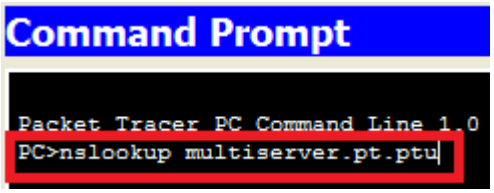
c. Minimice (pero no cierre) la ventana de configuración de **FTP Client**.

Paso 4:
Generar tráfico DNS

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



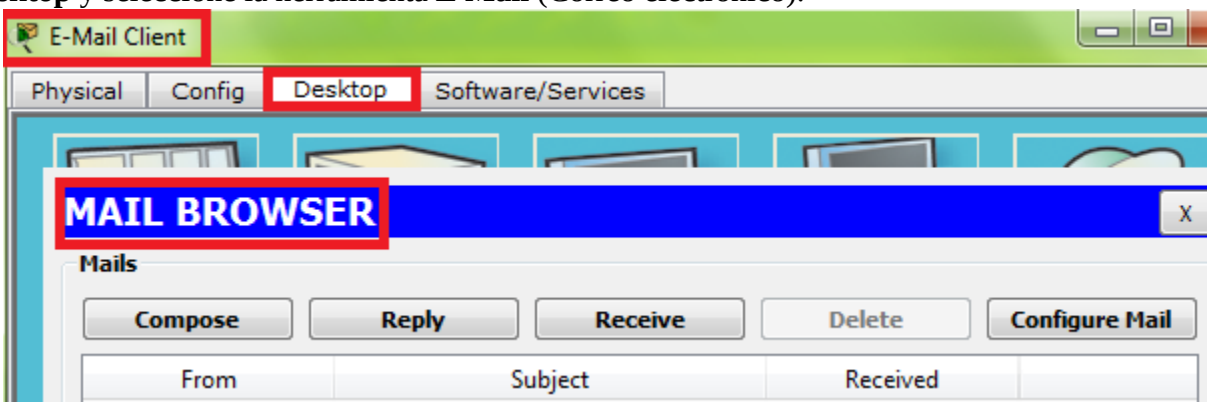
b. Introduzca el comando **nslookup multiserver.pt.ptu**. En la ventana de simulación, aparecerá una PDU.



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

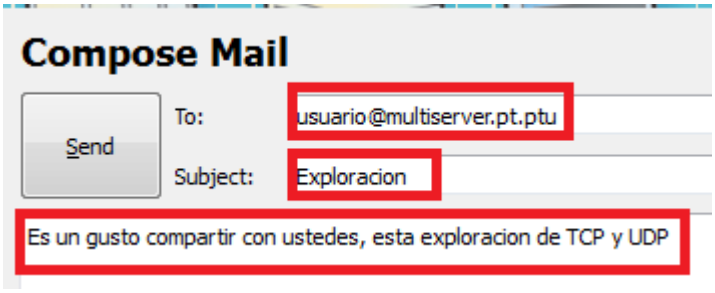
Paso 5: Generar tráfico de correo electrónico

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).

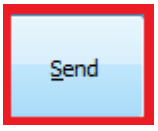


b. Haga clic en **Compose** (Redactar) e introduzca la siguiente información:

1) **To:** (Para:) usuario@multiserver.pt.ptu.
2) **Subject:** (Asunto:) personalice el campo de asunto.
3) E-Mail Body: (Cuerpo del correo electrónico:) personalice el correo electrónico.



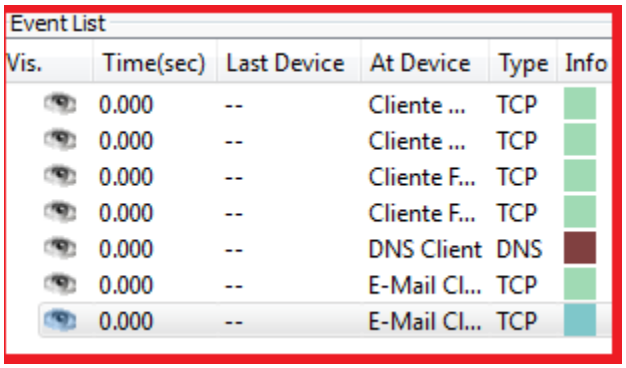
c. Haga clic en **Send** (Enviar).



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.

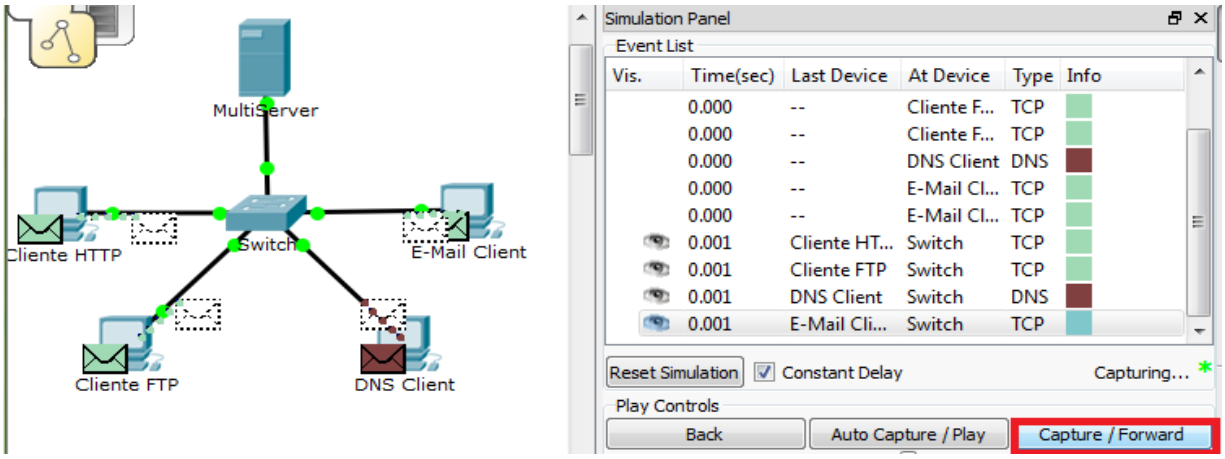


Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

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

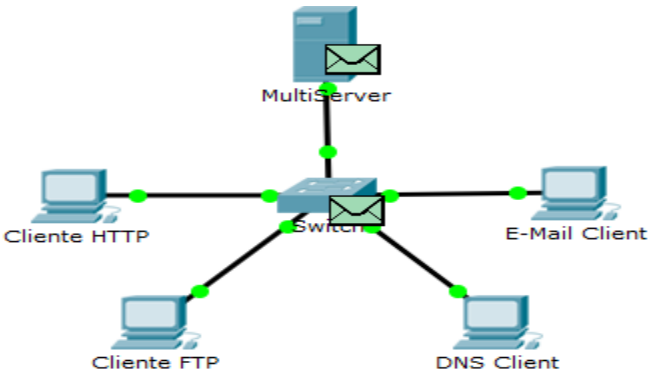
Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

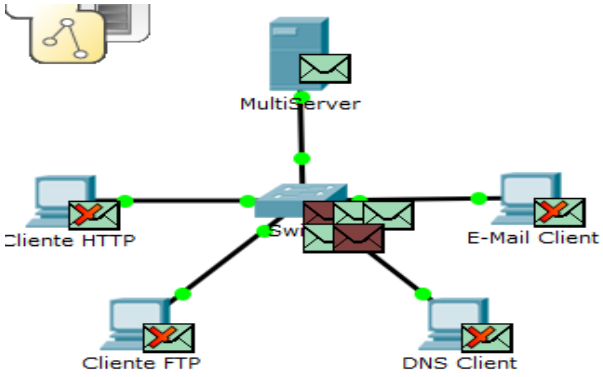
a. Haga clic en **Capture/Forward** (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.

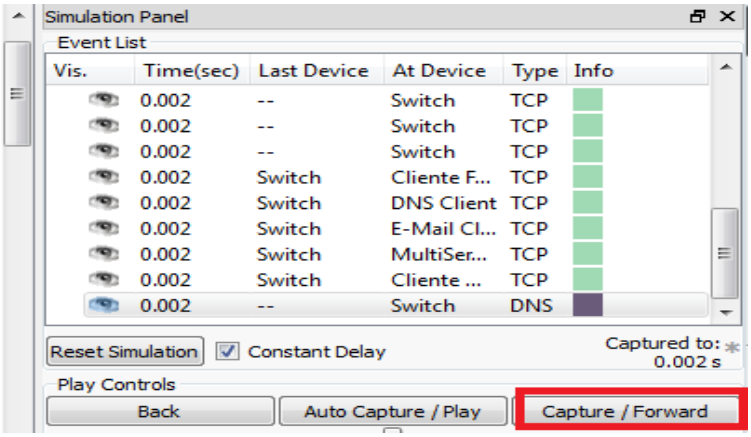


b. Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?

Según lo que se observa en la simulación las PDU están almacenados en al Switch

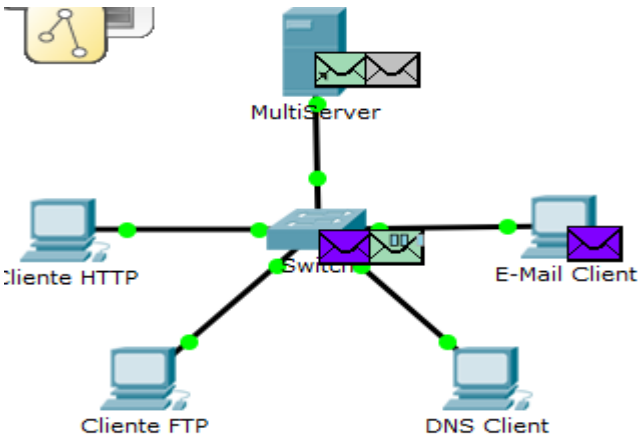






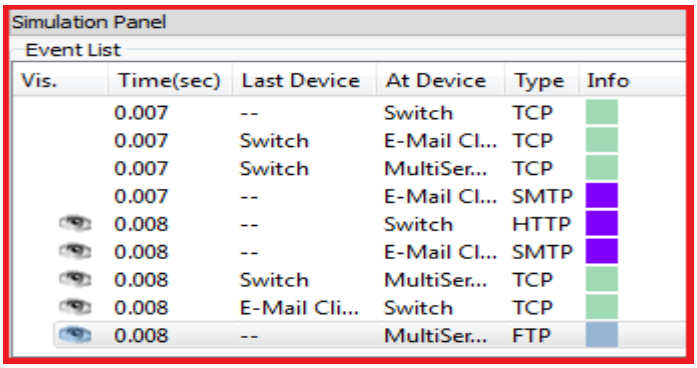
c. Haga clic en **Capture/Forward** seis veces. Todos los clientes deberían haber recibido una respuesta. Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado. ¿Cómo se denomina este proceso?

Multiplexación

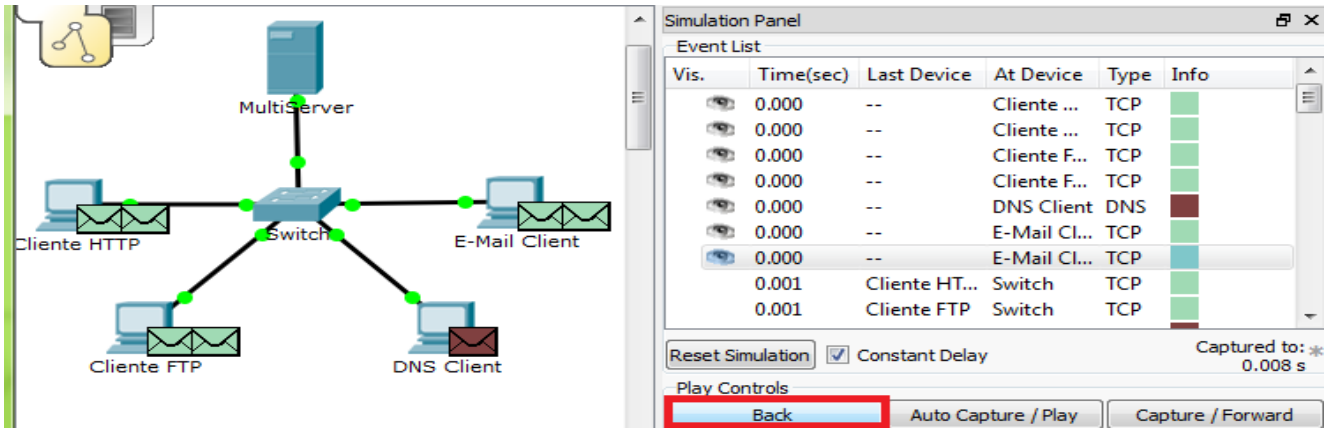


d. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?

Estos representan diferentes protocolos, como se muestra a continuación



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



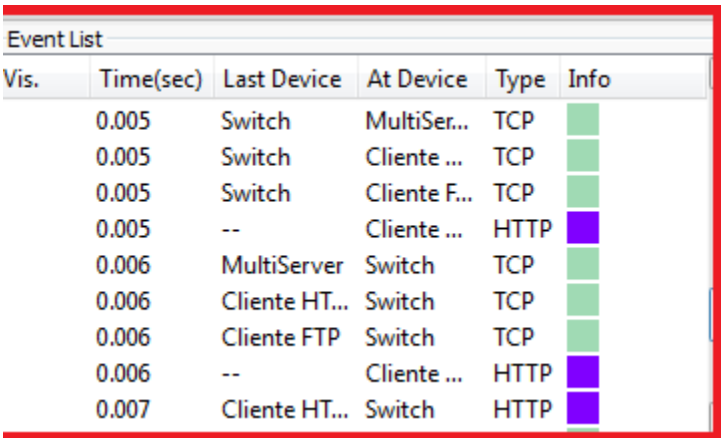
Nota: no haga clic en **Reset Simulation** (Restablecer simulación) en ningún momento durante esta actividad; si lo hace, deberá repetir los pasos de la parte 1.

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

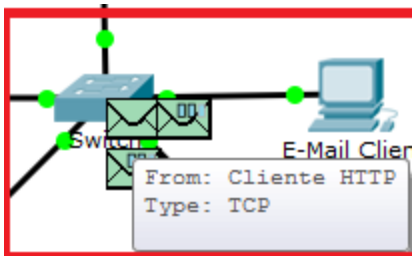
a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**:

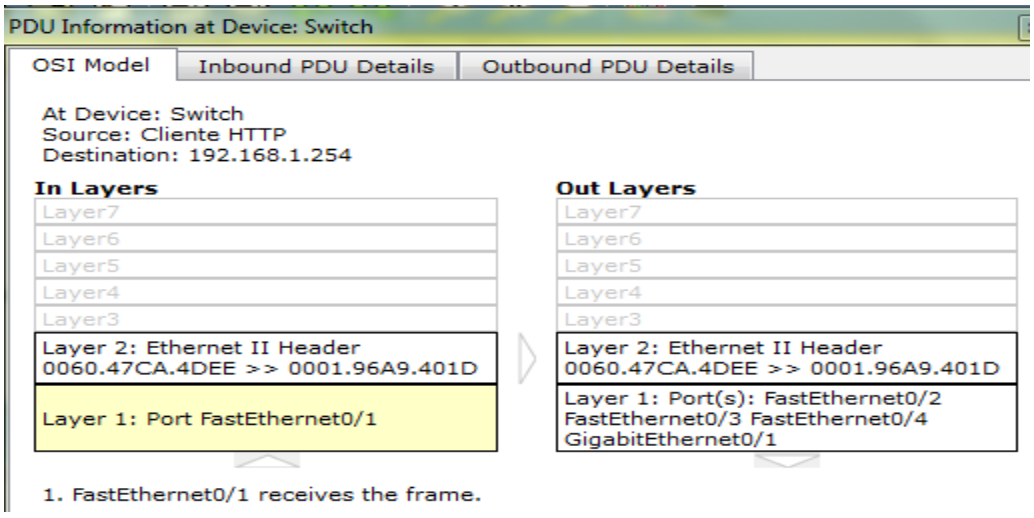
1) Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrartodos/ninguno).

2) 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**.



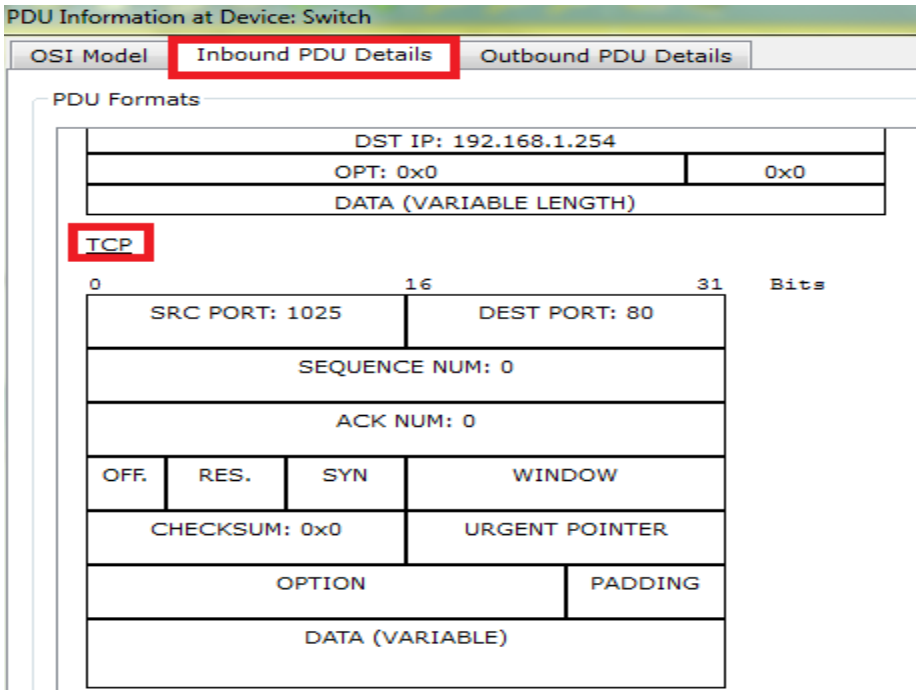
b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en **HTTP Client**. Haga clic en el sobre de PDU para abrirlo.





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

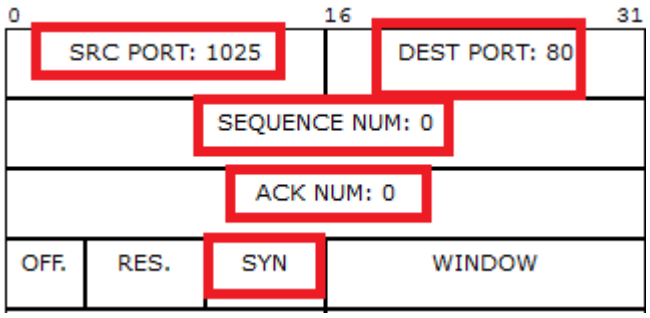
¿Cómo se rotula la sección? TCP



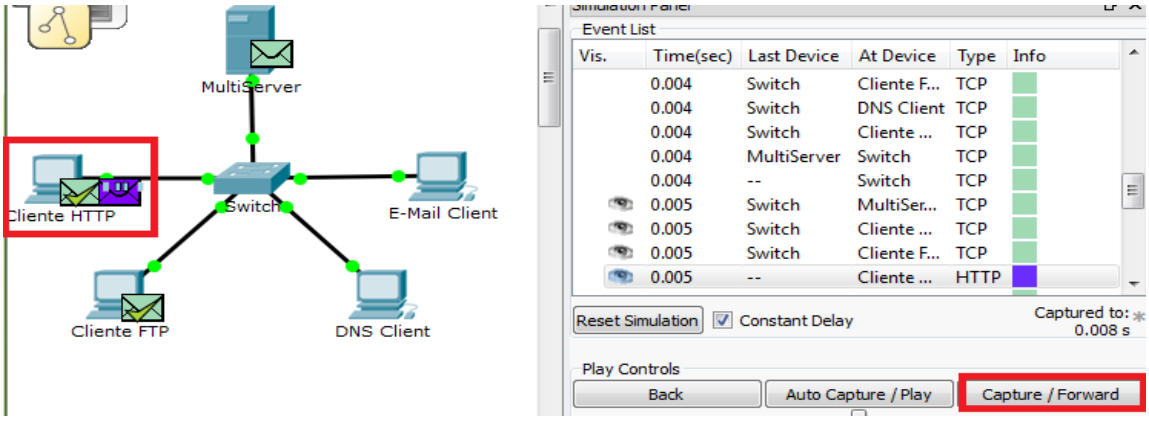
¿Estas comunicaciones se consideran confiables? Si

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 – 80 – 0 – 0 - SYN

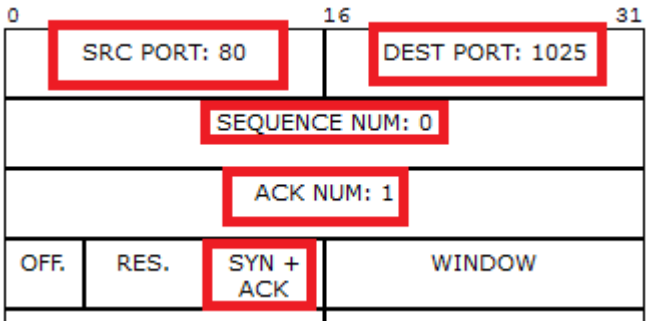


e. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **HTTP Client** con una marca de verificación.

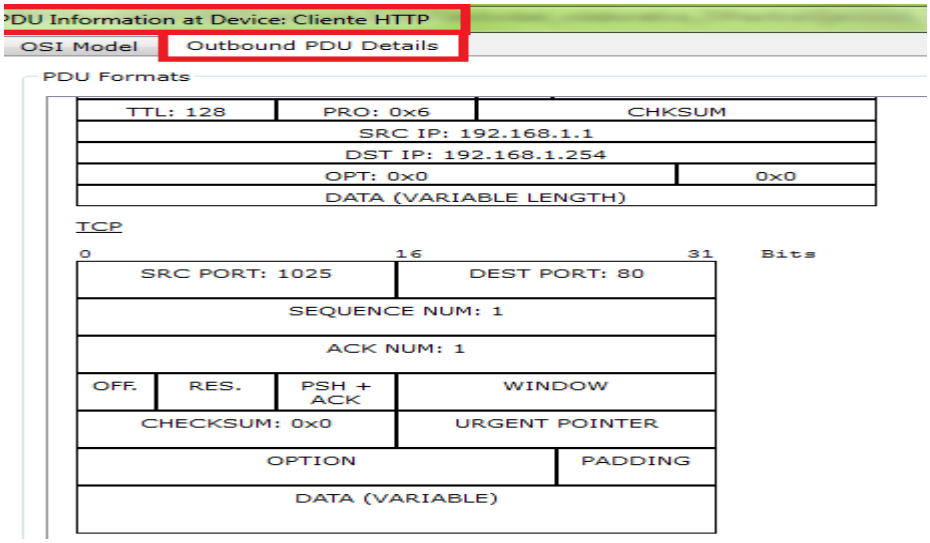


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

En este momento se invierten los puertos de origen y de destino, 80, 1025, 0, 1 y 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).



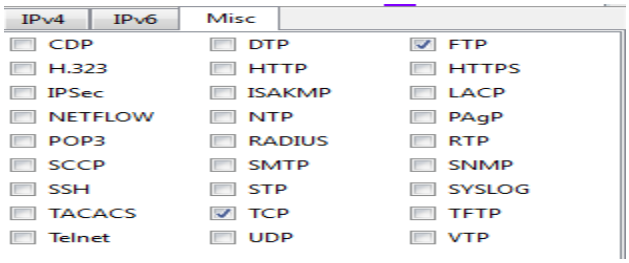
h. ¿Qué información se indica ahora en la sección TCP? ¿En qué se diferencian los números de puerto y de secuencia respecto de las dos PDU anteriores?

Aquí los puertos de origen y de destino están invertidos 1025, 80, 1, 1 PSH+ACK y el número de secuencia y el de acuse de recibo es 1

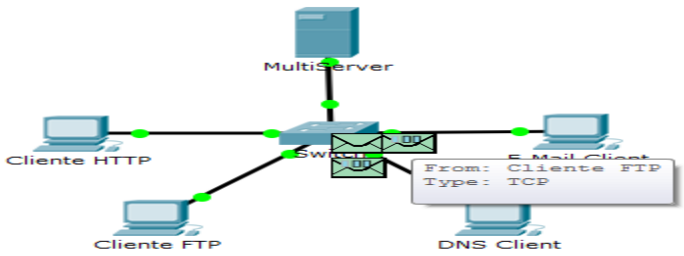
i. Haga clic en **Back** hasta que se restablezca la simulación

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

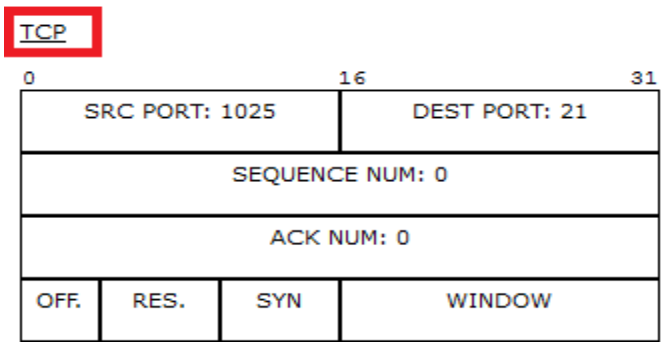
a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **FTP** y **TCP**.



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.



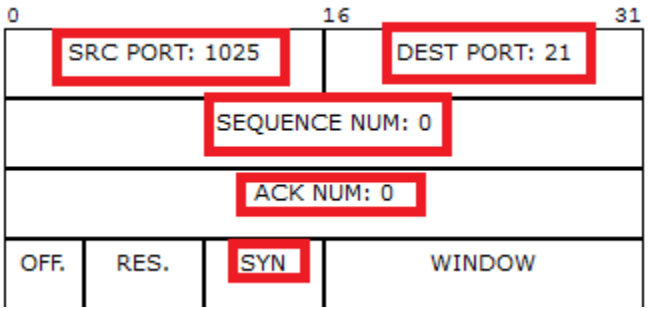
c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección? TCP



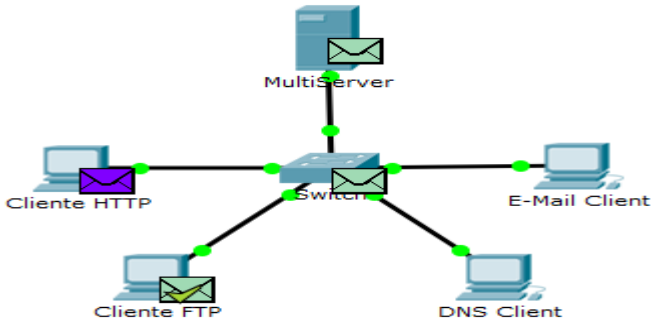
¿Estas comunicaciones se consideran confiables? Si

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

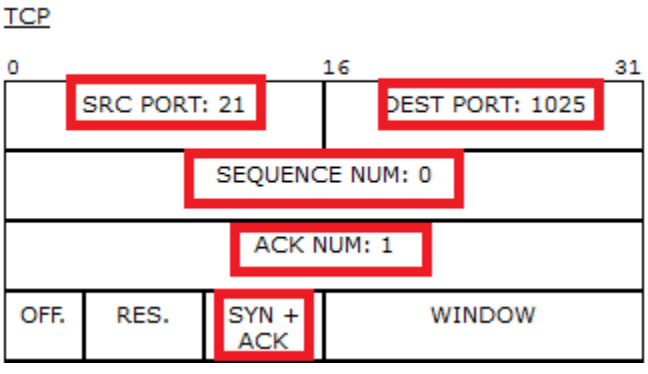


d. Cierre la PDU y haga clic en **Capture/Forward** hasta que una PDU vuelva a **FTP Client** con una marca de verificación.



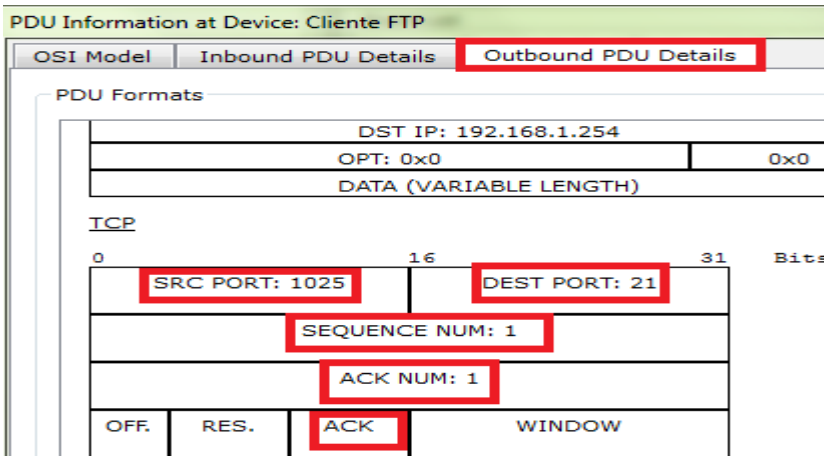
f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

En este momento se invierten los puertos de origen y de destino, 21, 1025, 0, 1 SYN+ACK y el número de acuse de recibido es 1

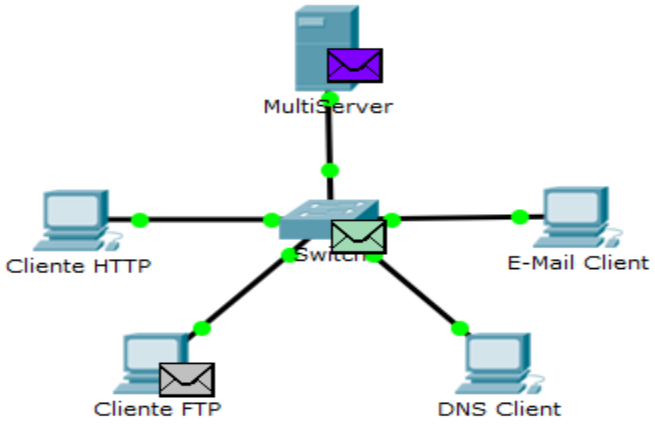


g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

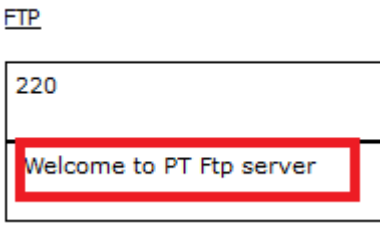
Se vuelven a invertir los puertos de origen y de destino, 1025, 21, 1, 1. ACK y los números de secuencia y de acuse de recibido son 1



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.



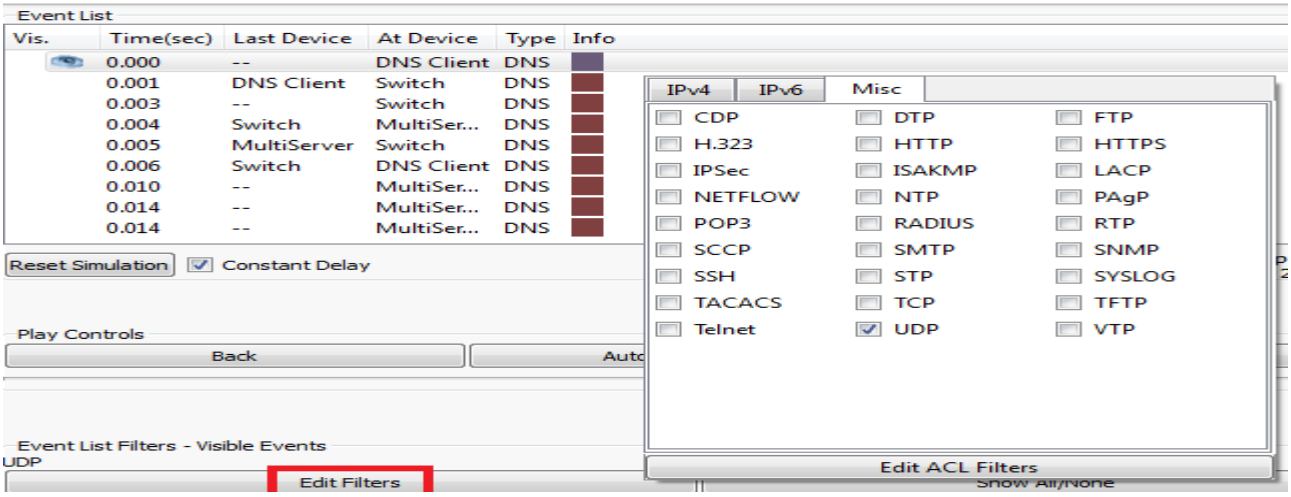
i. Abra la PDU y seleccione **Inbound PDU Details**. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?



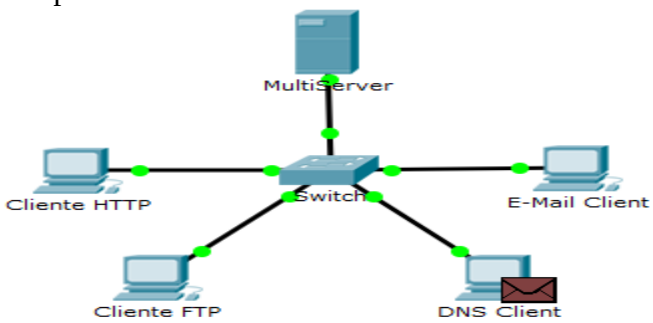
j. Haga clic en **Back** hasta que se restablezca la simulación.

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

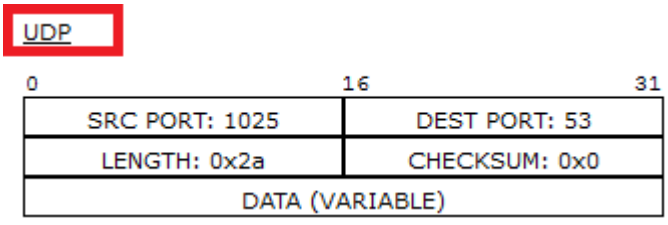
a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestren **DNS** y **UDP**.



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



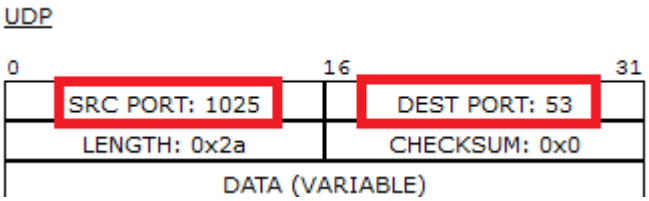
c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Cómo se rotula la sección? UDP



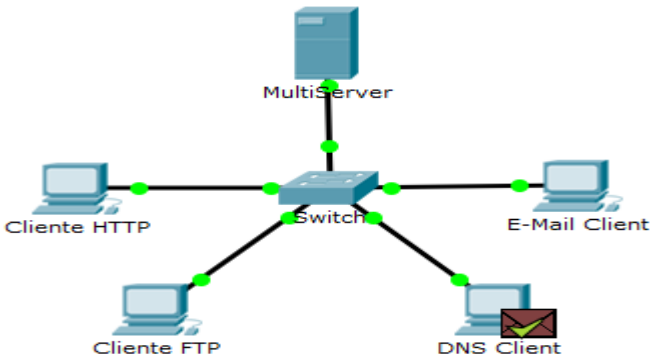
¿Estas comunicaciones se consideran confiables? No

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, no hay números de secuencia ni de acuse porque UDP no necesita establecer una conexión confiable

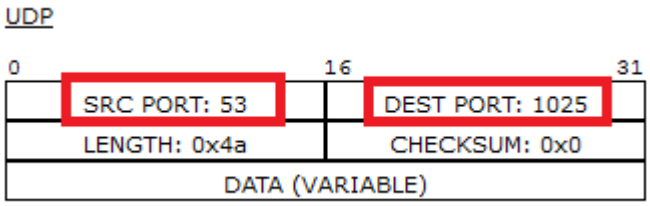


e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.



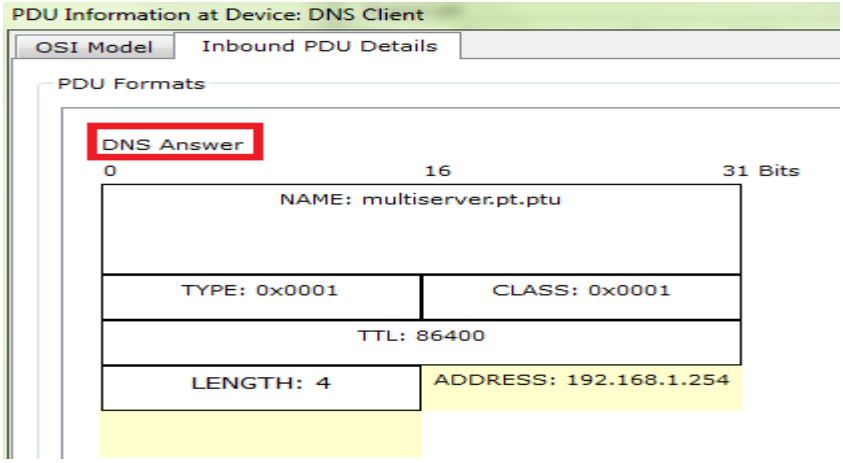
f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?

Los números de origen y de destino están invertidos, 52, 1025



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

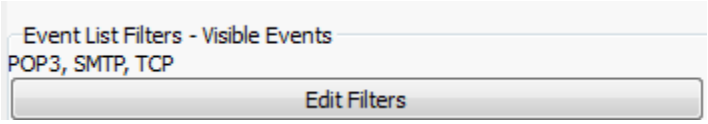
DNS Answer



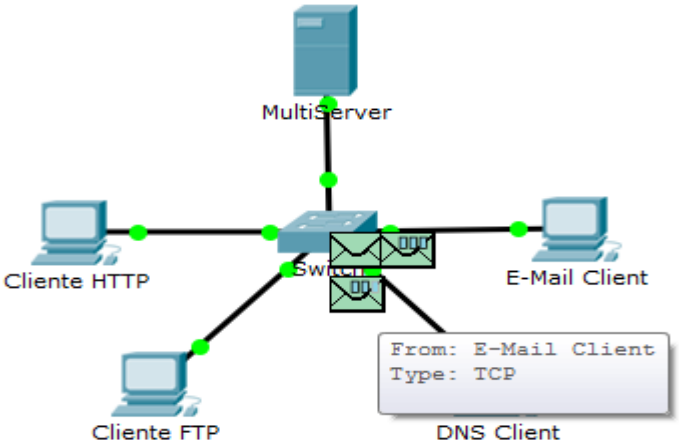
h. Haga clic en **Back** hasta que se restablezca la simulación.

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

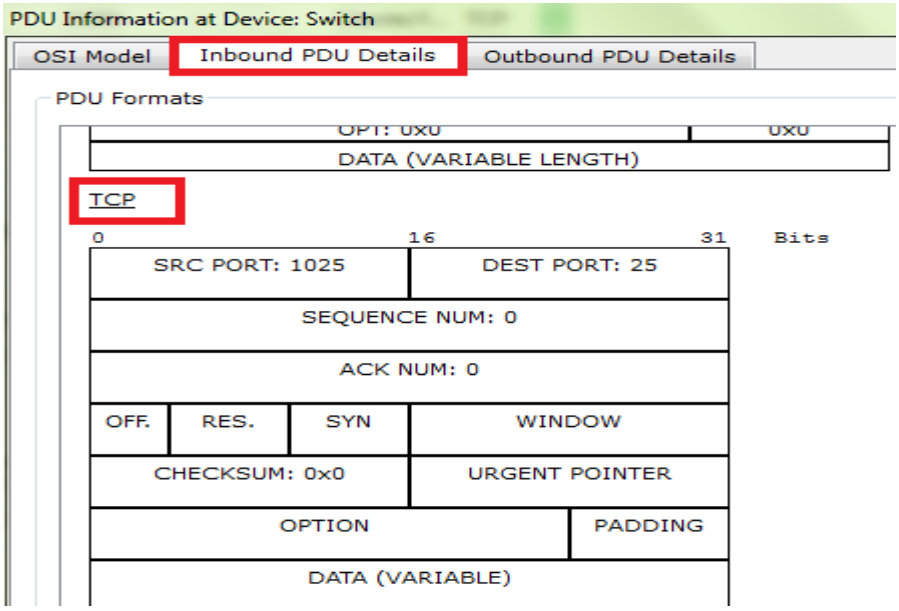
a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP** y **TCP**.



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.

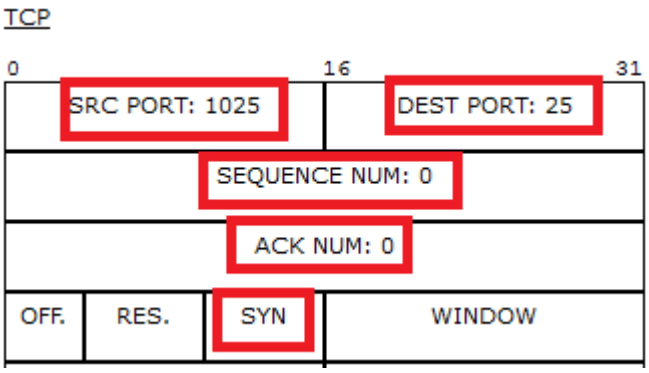


c. Haga clic en la ficha **Inbound PDU Details** (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico?
TCP



¿Estas comunicaciones se consideran confiables? Si

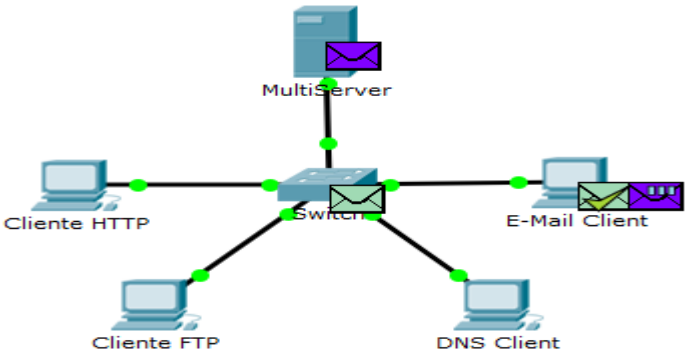
d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO).



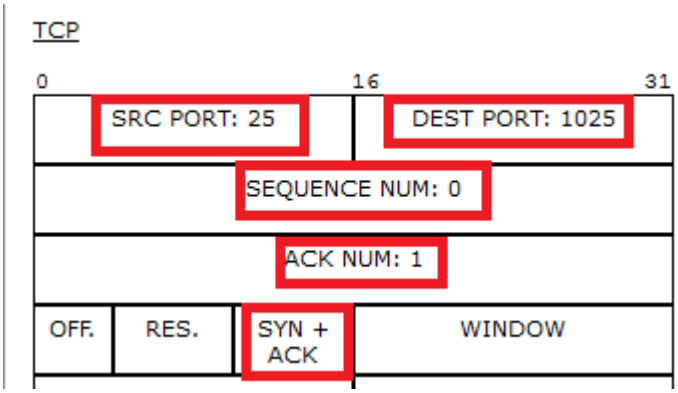
¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?

2025, 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.

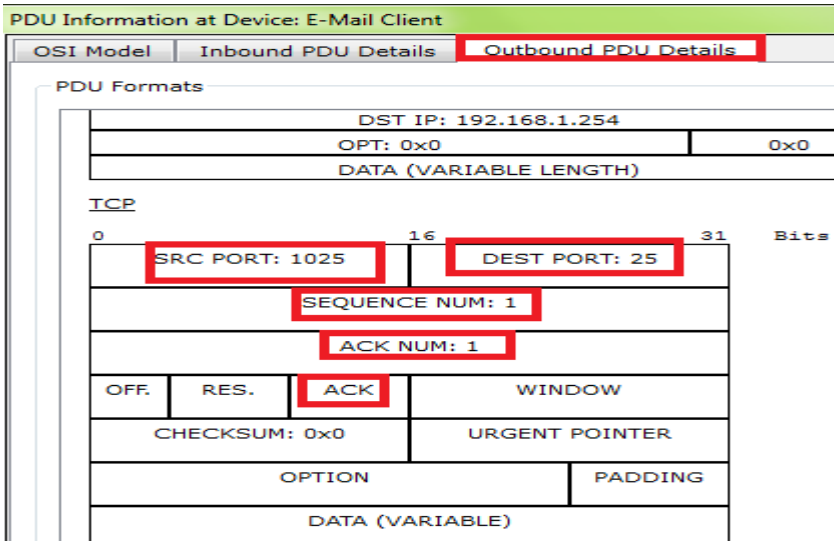


f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?
Se invierten los puertos de origen y de destino, 25 1025, 0, 1. SYN+ACK y el número de acuse de recibido es 1

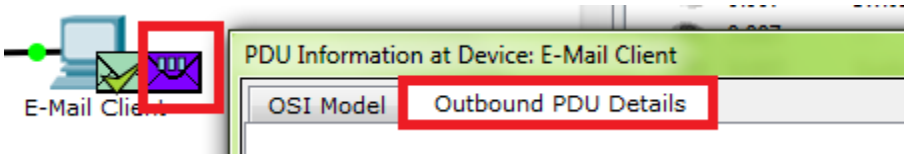


g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

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

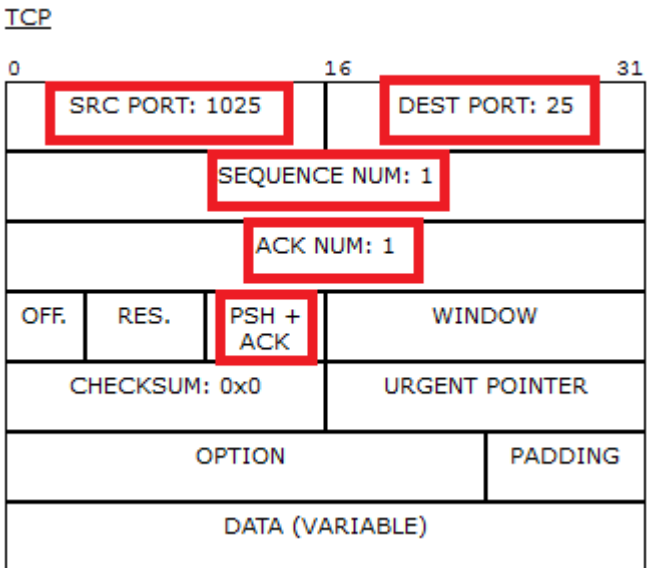


h. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y seleccione **Outbound PDU Details** (Detalles de PDU saliente).



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

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



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

SMTP. POP3

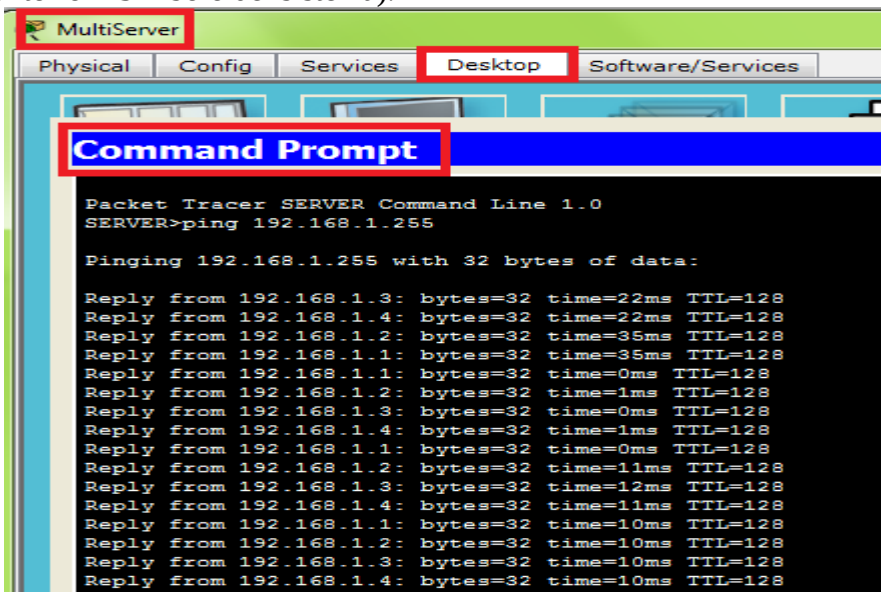
k. Haga clic en **Back** hasta que se restablezca la simulación

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?
Se podrán ver los puertos 21, 25 y 80

c. ¿En qué estados están las sesiones?
Los posibles estados incluyen: Closed, Established, Last_ACK

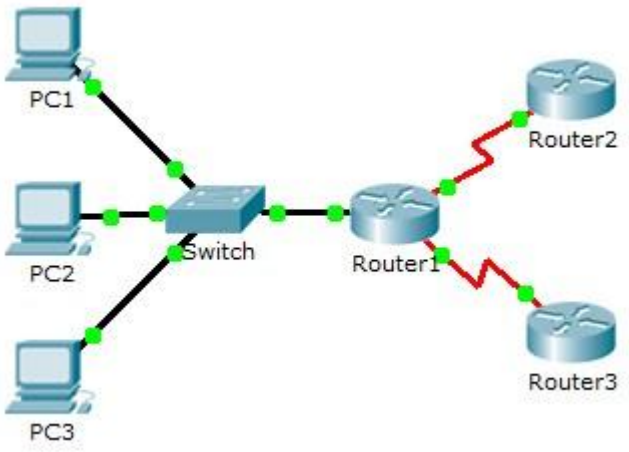
d. Repita el comando **netstat** varias veces hasta que vea solo una sola sesión con el estado ESTABLISHED. ¿Para qué servicio aún está abierta la conexión? FTP

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

El programa no deja avanzar más

8.1.3.8 Exploration of TCP and UDP Multicast Traffic

Topología



Objetivos

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

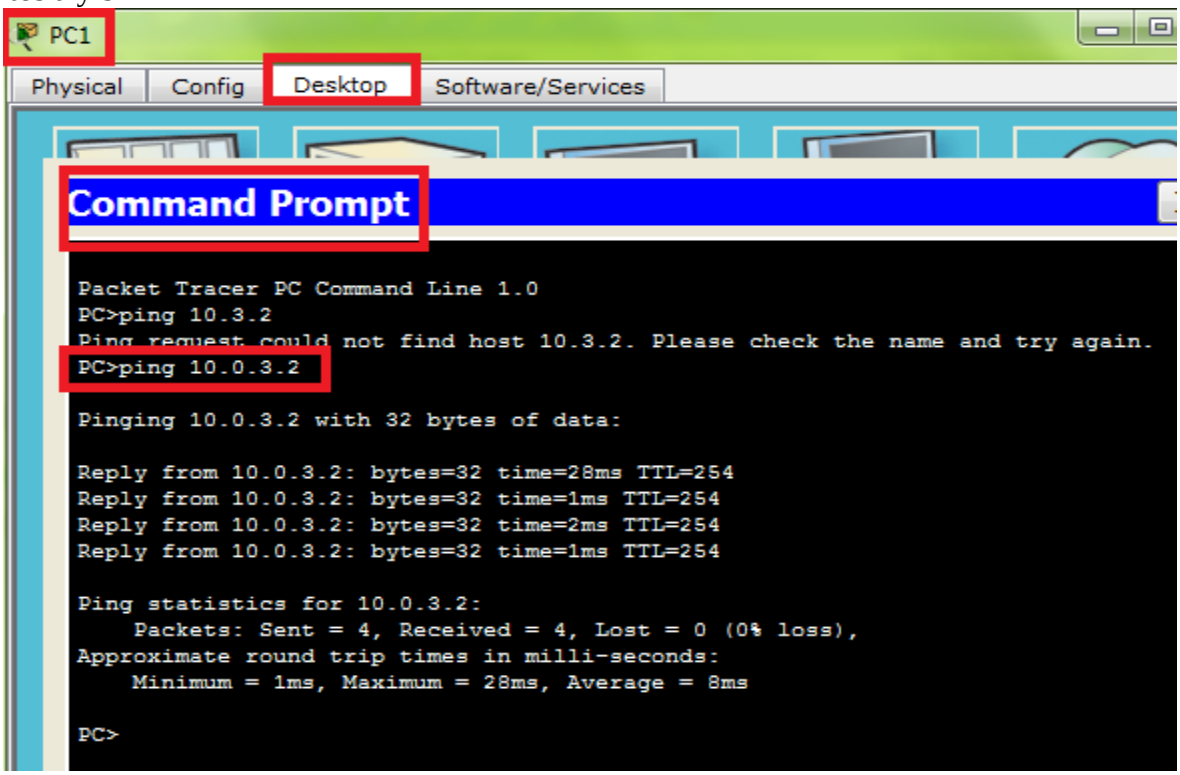
Parte 1: Generar tráfico de unicast

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.

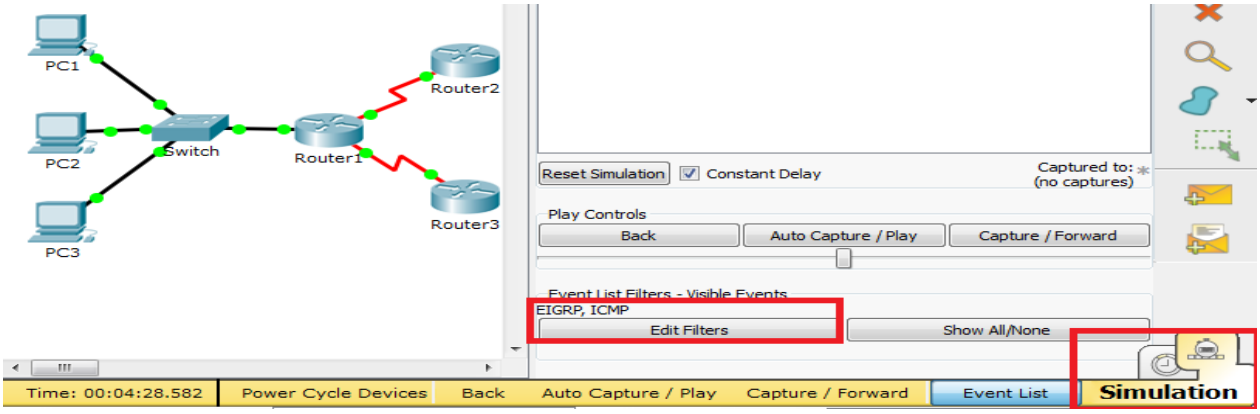
Puntos a y b



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**.

```
PC>ping 10.0.3.2

Pinging 10.0.3.2 with 32 bytes of data:
```

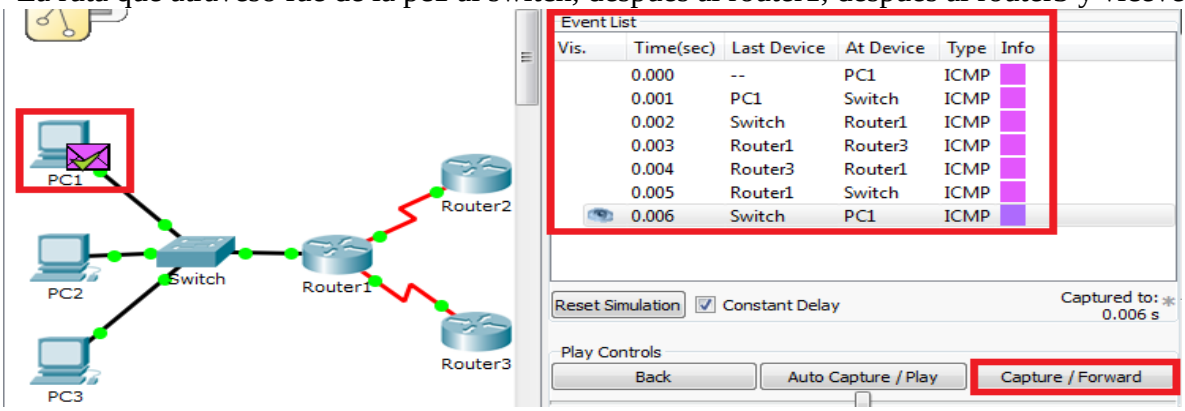
Paso 3: Examinar el tráfico de unicast

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?

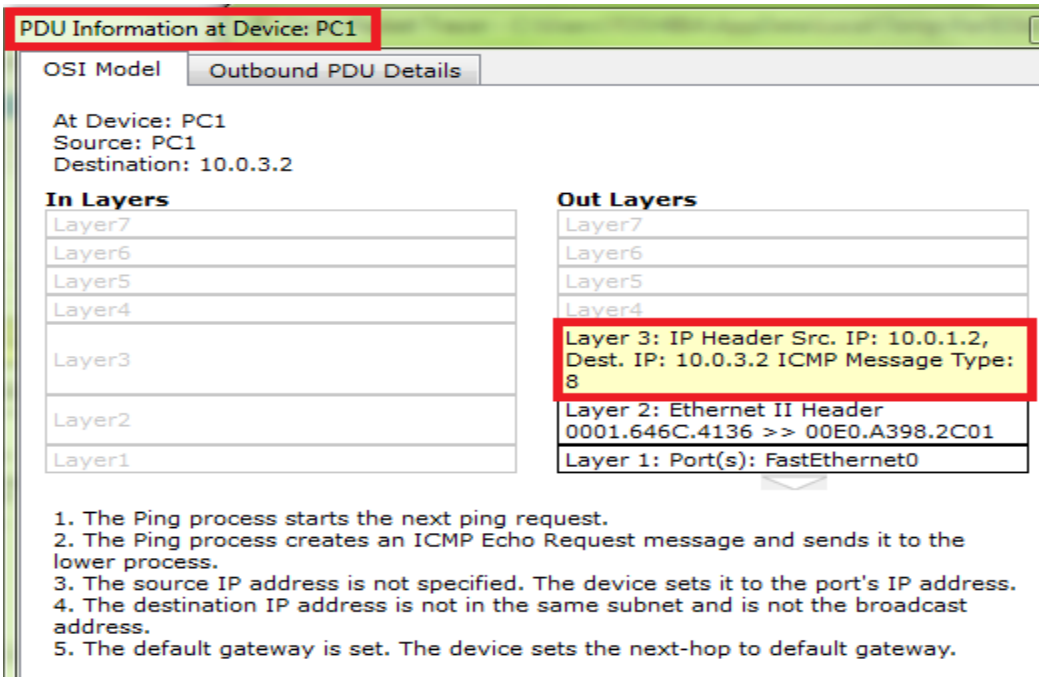
La ruta que atravesó fue de la pc1 al switch, después al router1, después al router3 y viceversa



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?

Comienza en la capa 3, porque esta específicamente relacionada con IP y 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?

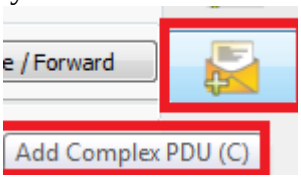
Según lo que se observa en cada uno de los eventos, las direcciones IP de origen y destino se intercambian y el mensaje o tipo de mensaje ahora es 0

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.



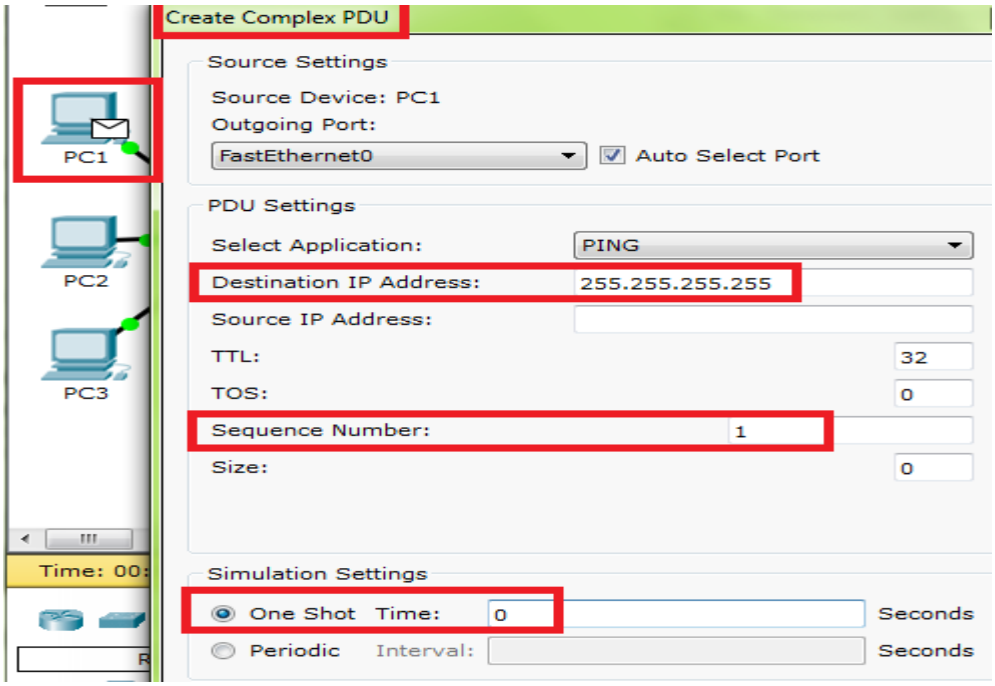
b. Pase el cursor del mouse sobre la topología, y el puntero cambiará por un sobre con un signo más (+).

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:

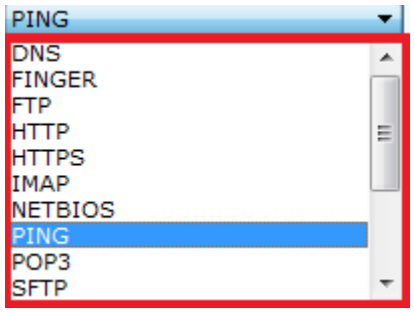
- Dirección IP de destino: **255.255.255.255** (dirección de broadcast)

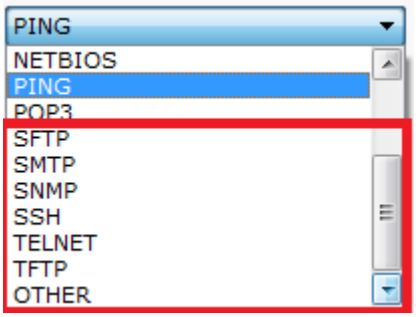
- Número de secuencia: 1
- Tiempo de intento único: **0**

Pasos de b y c

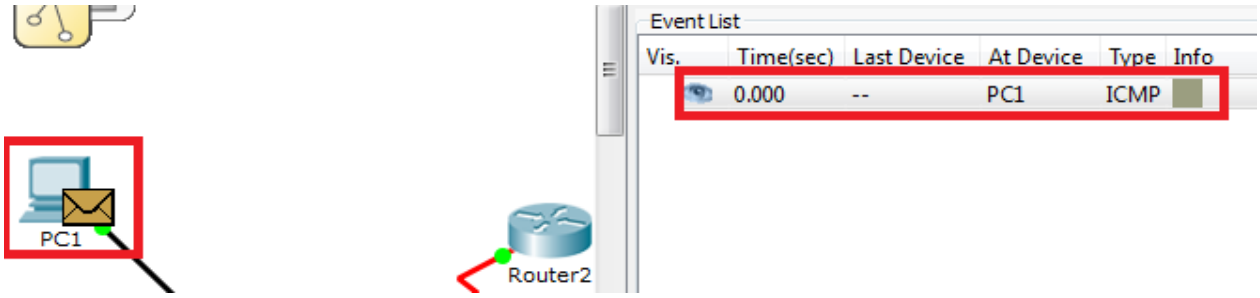


Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

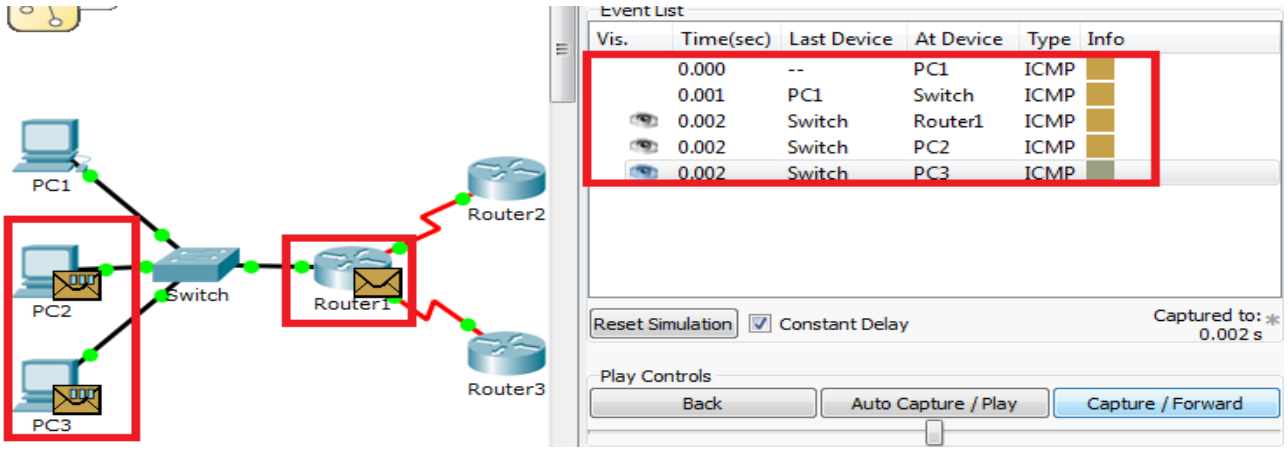




d. Haga clic en **Create PDU** (Crear PDU). Este paquete de broadcast de prueba ahora aparece en **Simulation Panel Event List** .También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para la Situación 0.

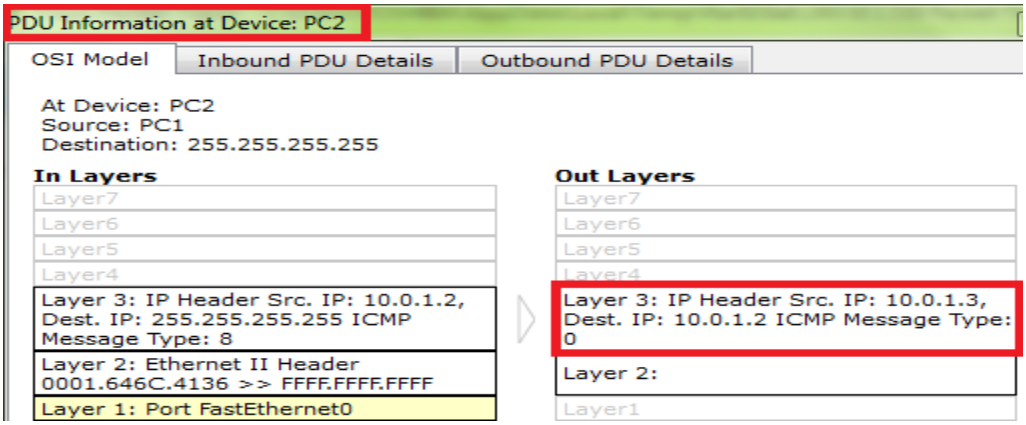


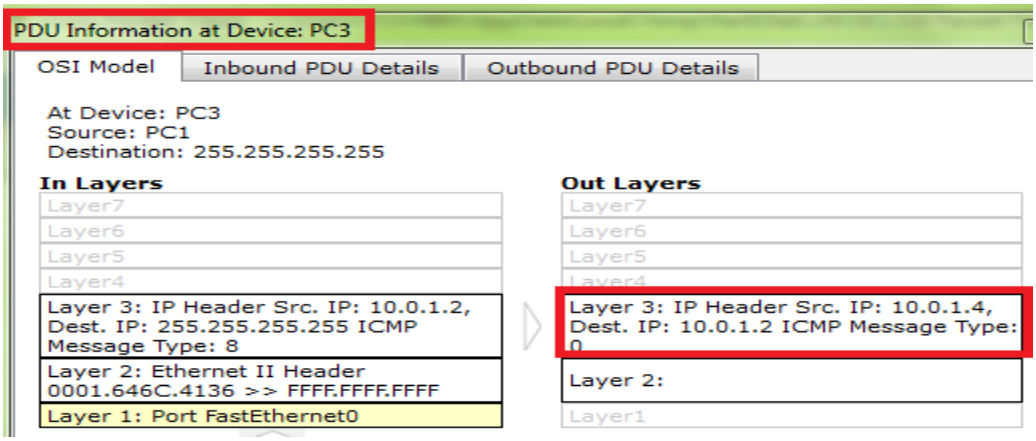
e. Haga clic en **Capture/Forward** dos veces. Este paquete se envía al switch y después se transmite por broadcast a la **PC2**, la **PC3**, y el **Router1**. Examine la información de la Capa 3 para todos los eventos. Observe que la dirección IP de destino es 255.255.255.255, que es la dirección IP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

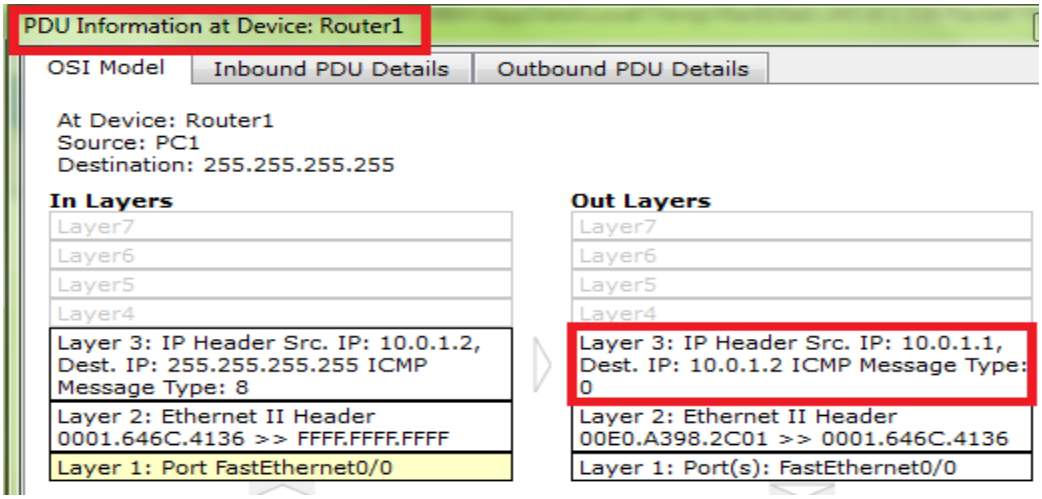


Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

La PDU se convierte en un unicast que contesta a la PC1

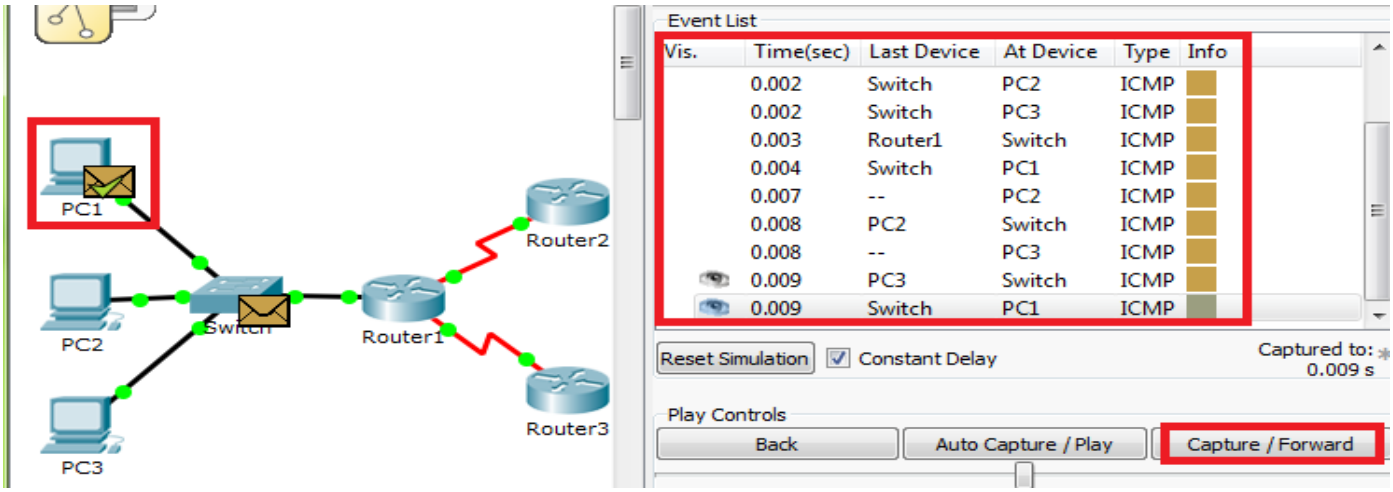






f. Haga clic en **Capture/Forward** nuevamente. ¿La PDU de broadcast se reenvía en algún momento al Router2 o al Router3? ¿Por qué?

No. El broadcast debe permanecer dentro de la red local, a menos que el router este establecido para reenviar

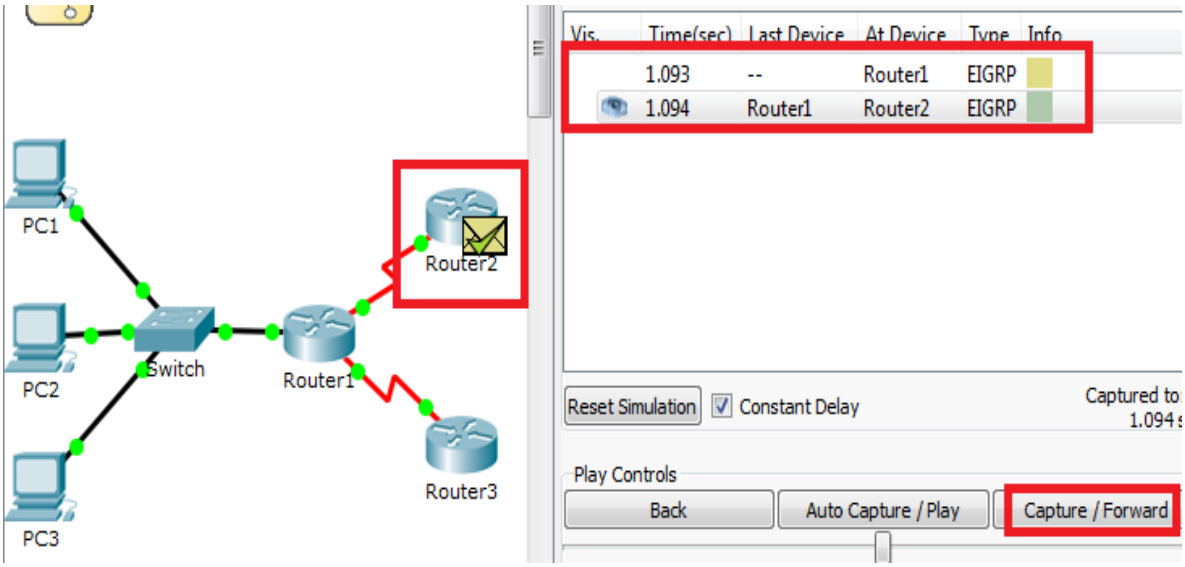


g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en **Delete** (Eliminar) debajo de **Scenario 0** (Situación 0).

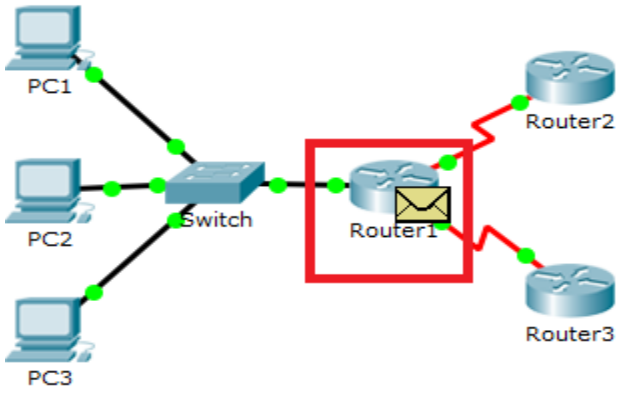
Parte 3: Investigar el tráfico de multicast

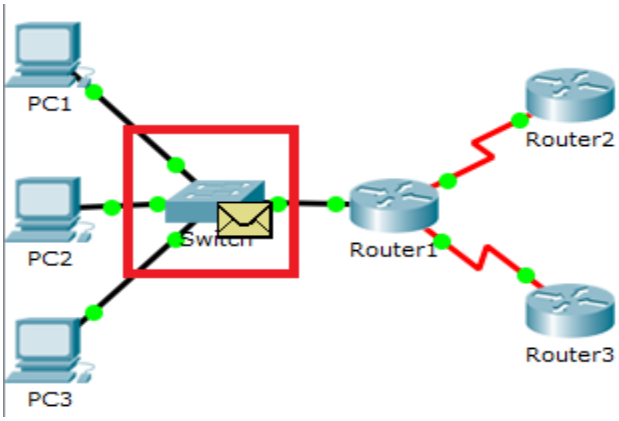
Paso 1: Examinar el tráfico que generan los protocolos de enrutamiento

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.



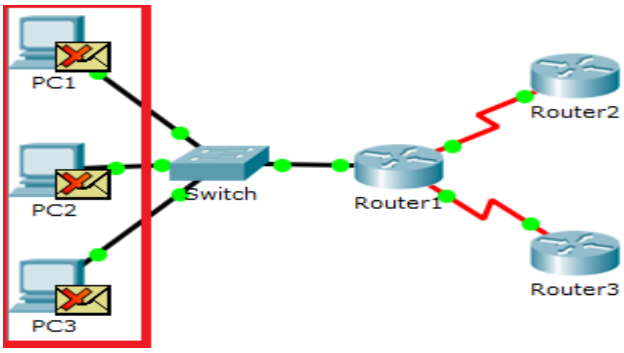
b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en **Capture/Forward**. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes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





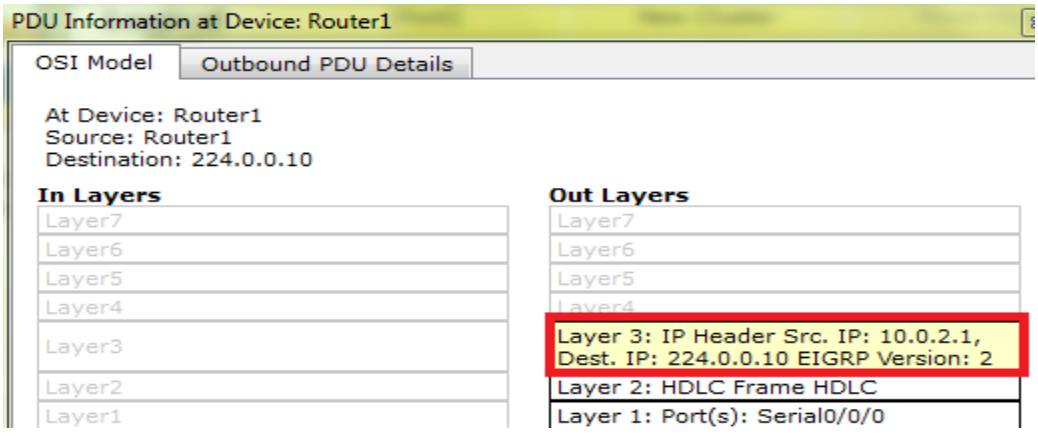
c. Haga clic en **Capture/Forward** hasta que vea que el paquete EIGRP llega a las PC. ¿Qué hacen los hosts con los paquetes?

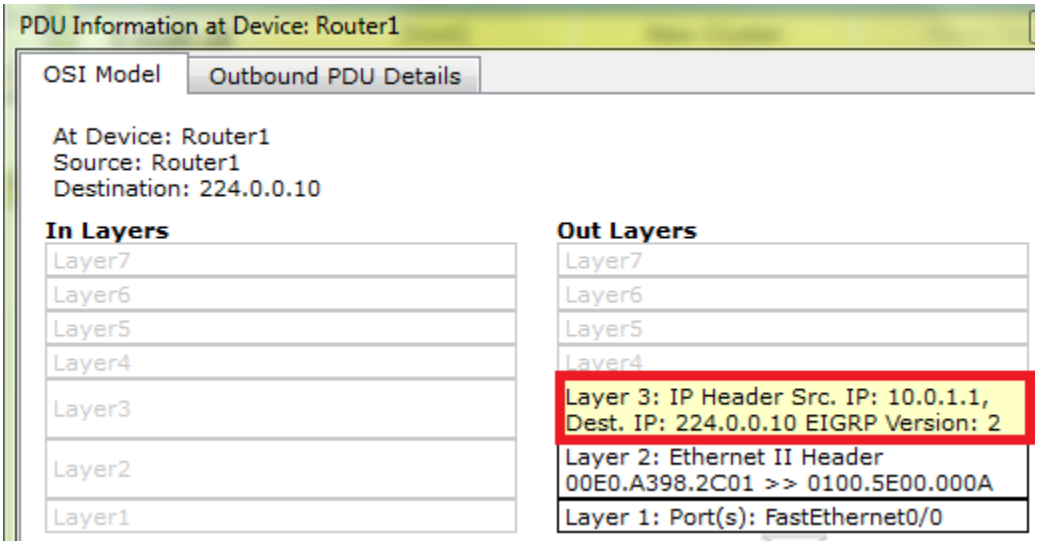
Los host rechazan y descartan los paquetes



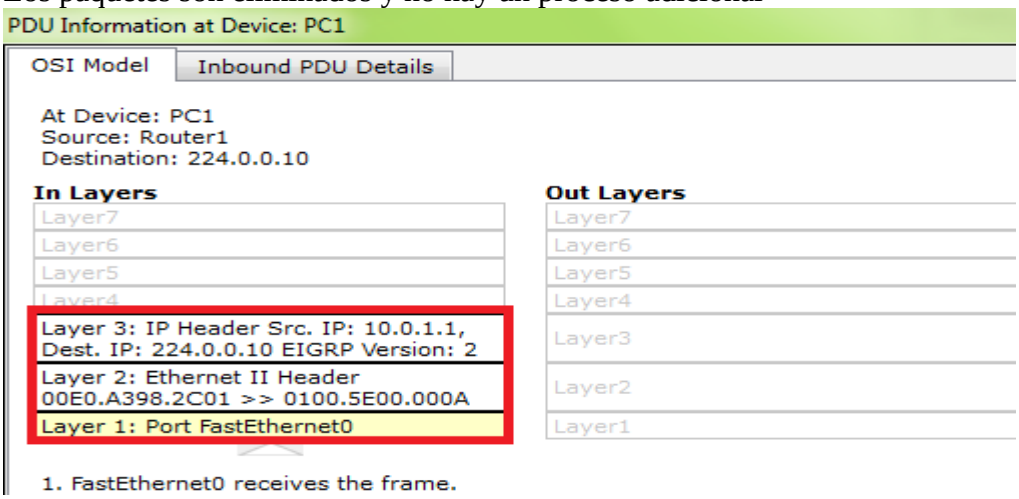
Examine la información de las capas 3 y 4 para todos los eventos EIGRP. ¿Cuál es la dirección de destino de cada uno de los paquetes?

224.0.0.10, la dirección IP del multicast para el protocolo de enrutamiento es EIGR





h. Haga clic en uno de los paquetes entregados a una de las PC. ¿Qué sucede con esos paquetes?
Los paquetes son eliminados y no hay un proceso adicional



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

Los paquetes unicast, se mueven atreves de la red destinado a un dispositivo especifico, el broadcast e envía a cada dispositivo en la red de área local y el multicast se envía a todos los dispositivos, cabe aclarar que solo se procesan aquellos que forman parte del grupo multicas

8.2.5.3 Configuring IPv6 Addressing Instruction IG

Configuración de direccionamiento IPv6

Topología

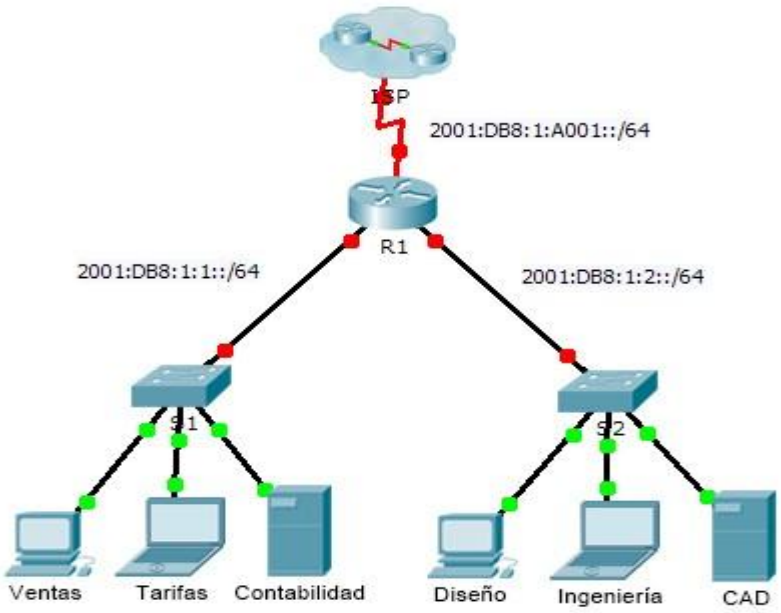


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
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

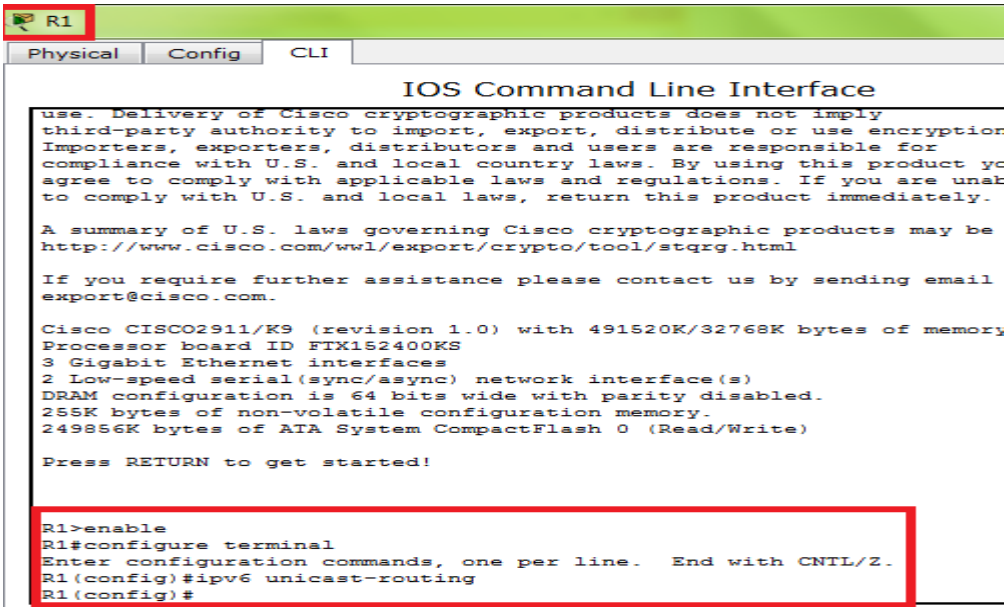
Parte 4: Probar y verificar la conectividad de red

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

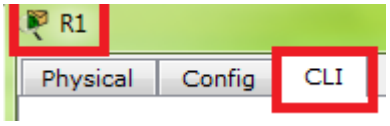
a. Introduzca el comando de configuración global ipv6 unicast-routing. Este comando se debe configurar para habilitar el router para que reenvíe paquetes IPv6. Este comando se analizará en otro semestre.

R1 (config)# ipv6 unicast-routing



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.

```
R1>enable
```

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

```
R1(config)#interface g0/0
R1(config-if)#
```

d. Configure la dirección IPv6 con el siguiente comando:

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

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

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

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

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

f. Active la interfaz.

```
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
```

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.

En esta evidencia se muestran los 3 puntos anteriores, a, b, c

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

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.

En esta evidencia se muestran los 3 puntos anteriores, a, b, c

```
R1(config-if)#interface 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 shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R1(config-if)#
```

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).

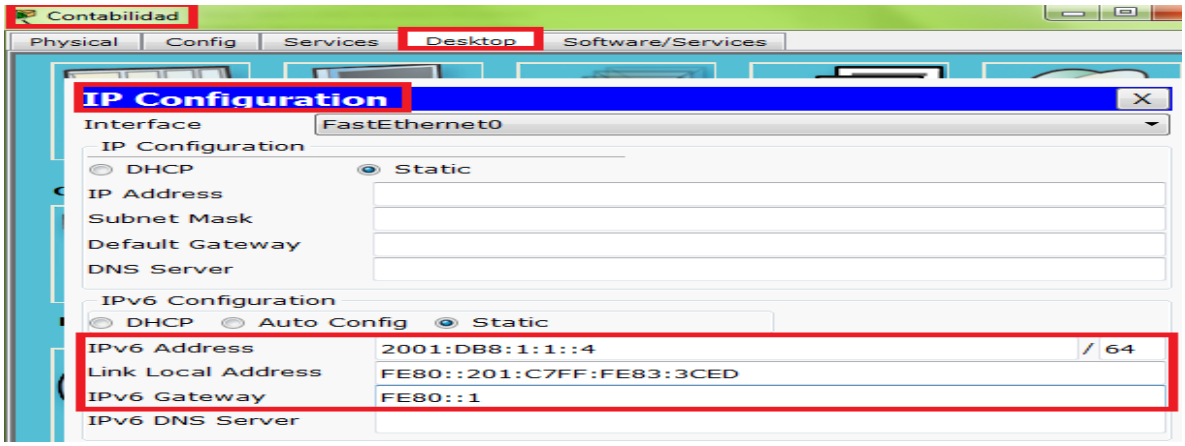
b. Establezca la **dirección IPv6 2001:DB8:1:1::4** con el

prefijo **/64**.

c. Configure el gateway IPv6 en la dirección link-local,

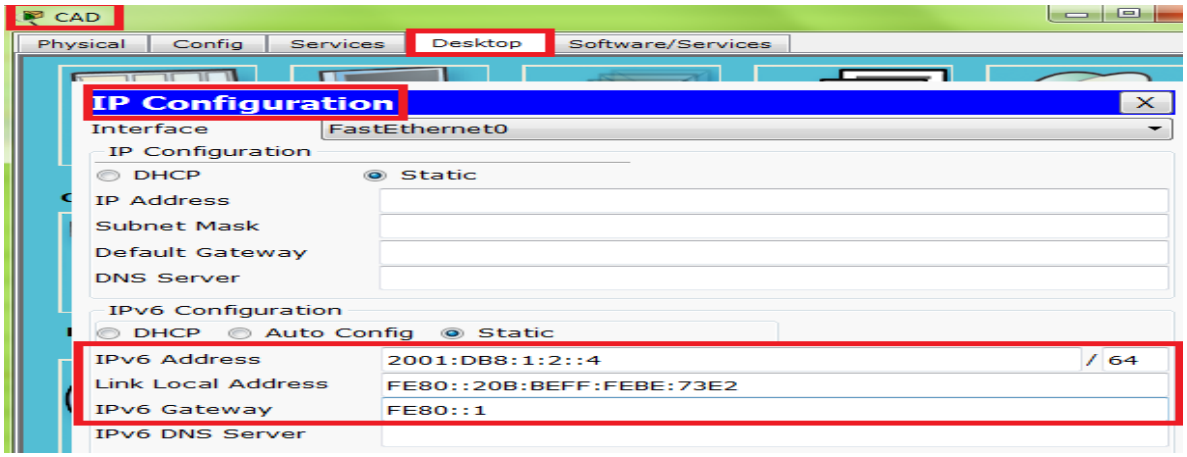
FE80::1.

En esta evidencia se muestran los 3 puntos anteriores, a, b, c



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

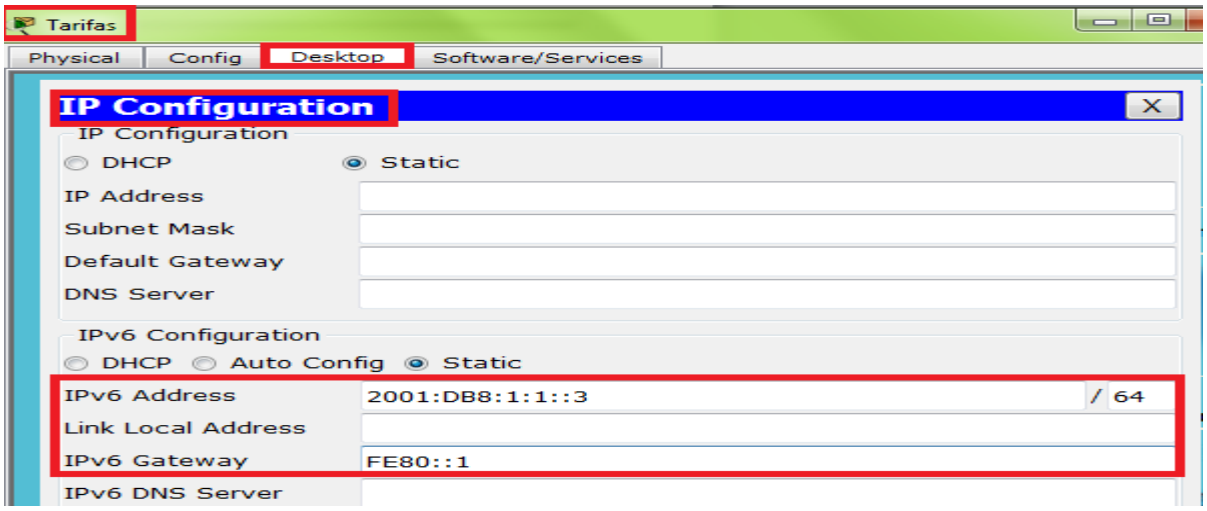
a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:1::3** con el

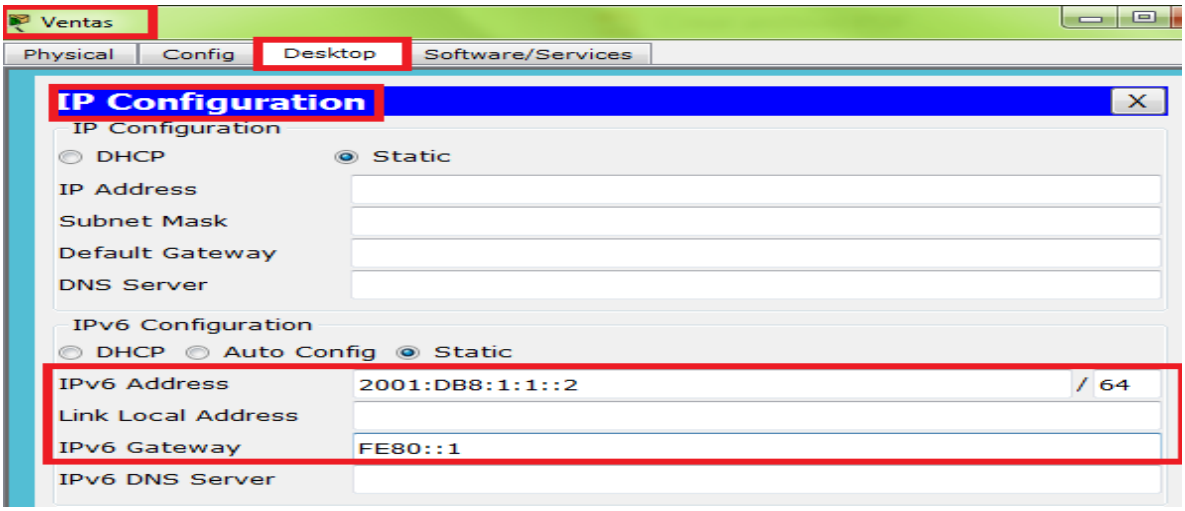
prefijo **/64**.

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

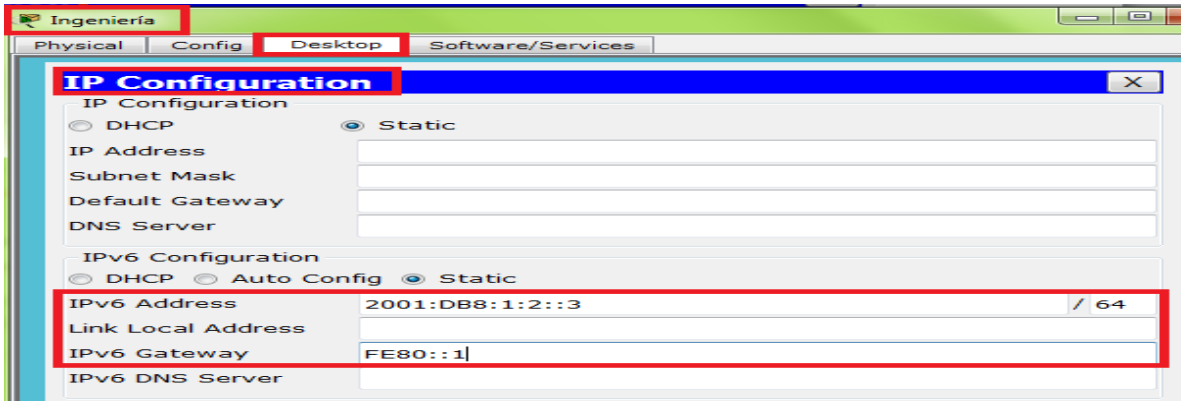
a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

b. Establezca la **dirección IPv6 2001:DB8:1:2::3** con el

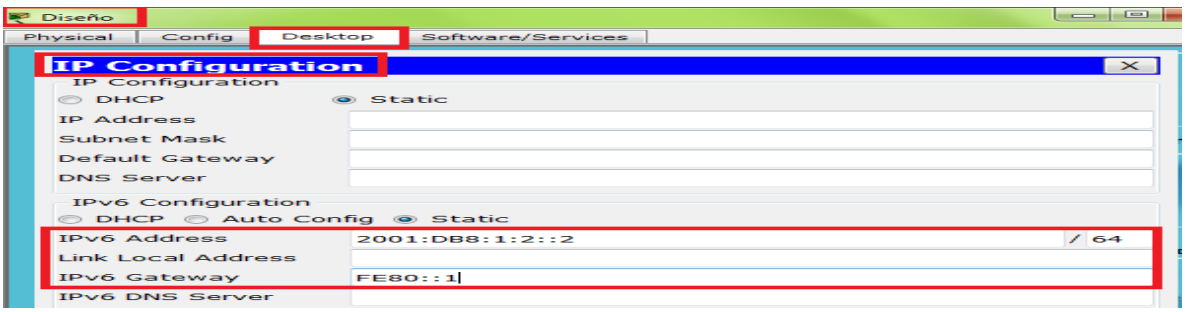
prefijo **/64**.

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.

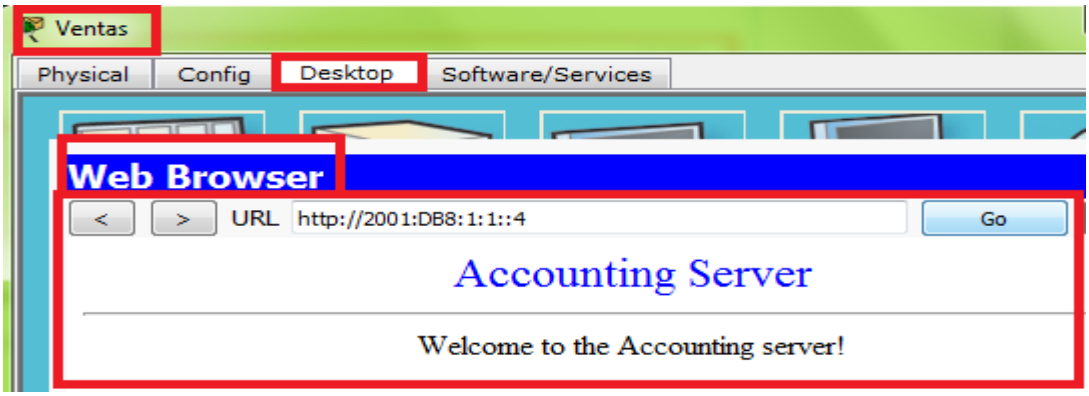


Parte 4: Probar y verificar la conectividad de la red

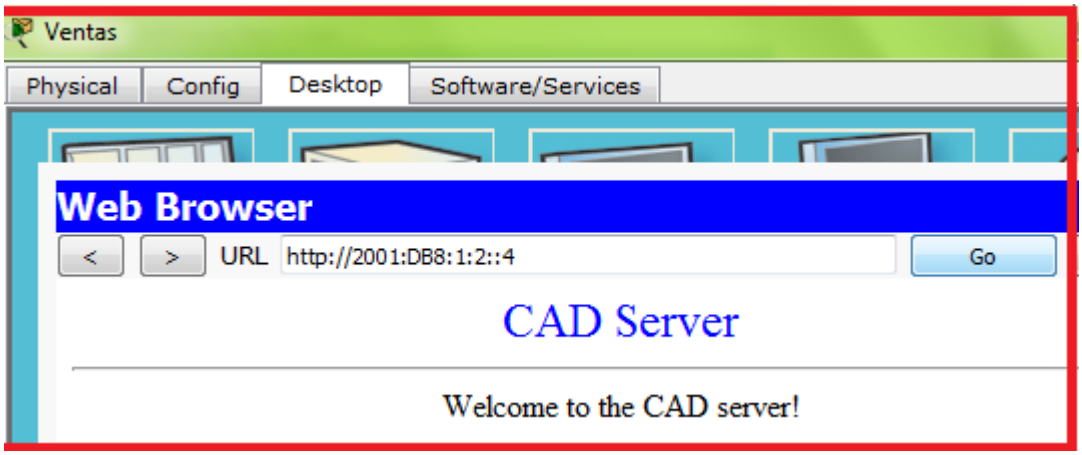
Paso 1: Abrir las páginas Web del servidor de los clientes

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.

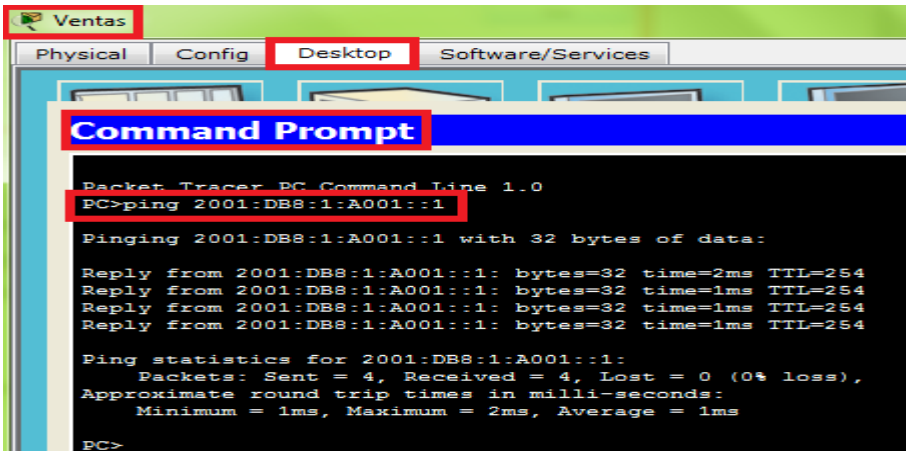
Paso 2: Hacer ping al ISP

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

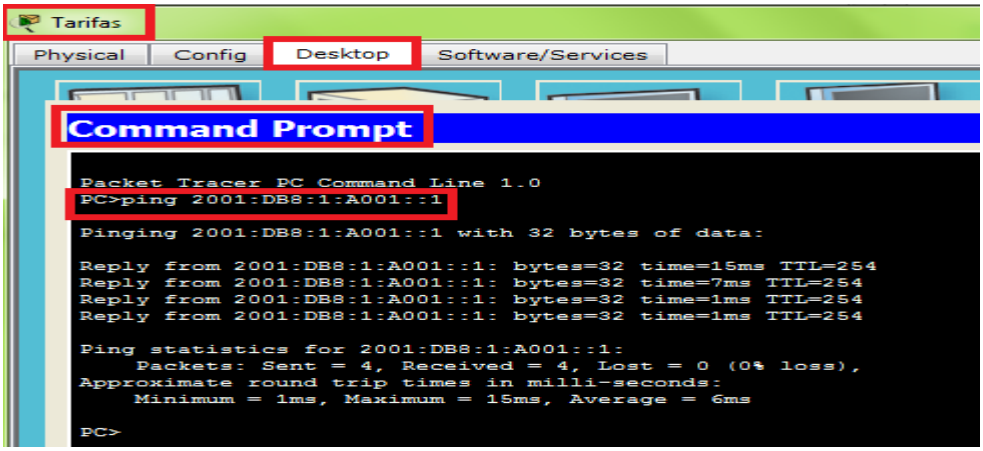
b. Haga clic en la ficha **Desktop** > **Command Prompt** (Símbolo del sistema).

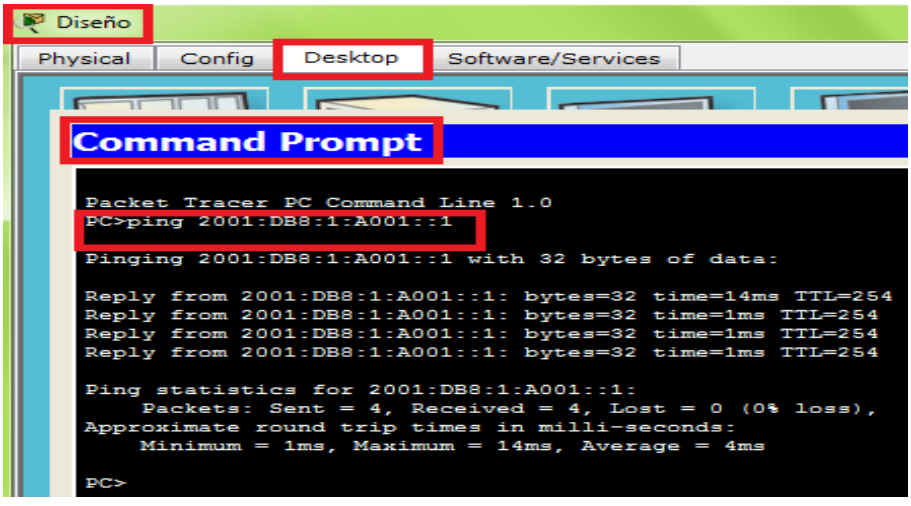
c. Pruebe la conectividad al ISP con el siguiente comando:

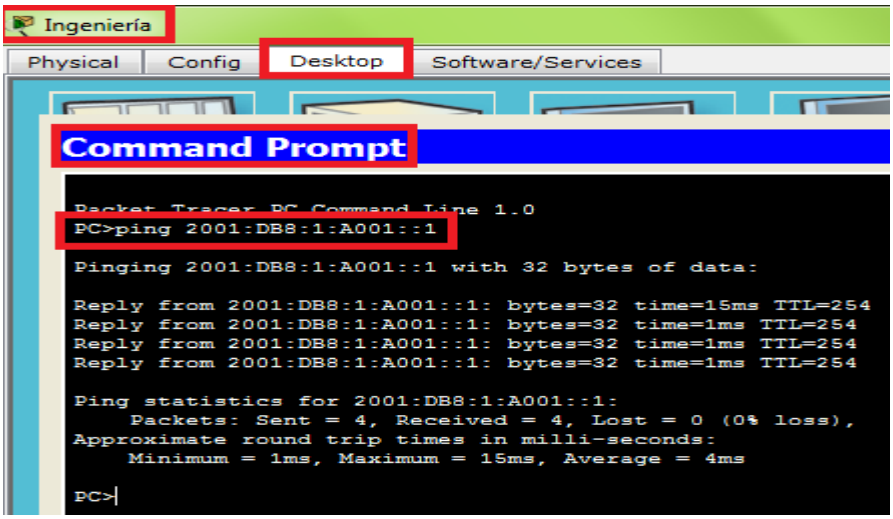
PC> **ping 2001:DB8:1:A001::1**



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






Ingeniería
Physical
Config
Desktop
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>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=15ms 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
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 = 15ms, Average = 4ms
PC>

8.3.2.5 Verifying IPv4 and IPv6 Addressing Instruction IG

Verificación del direccionamiento IPv4 e IPv6

Topología

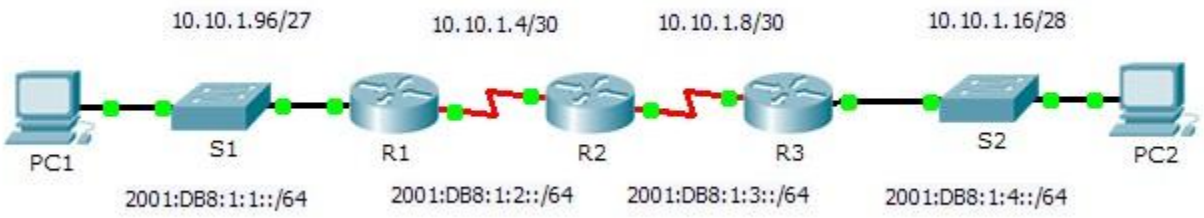


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4 / Dirección/Prefijo IPv6	Máscara de	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

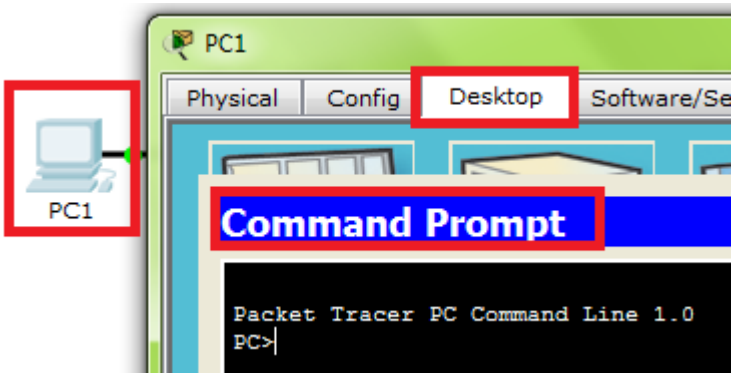
Parte 2: Probar la conectividad mediante el comando ping

Parte 3: Descubrir la ruta mediante su rastreo

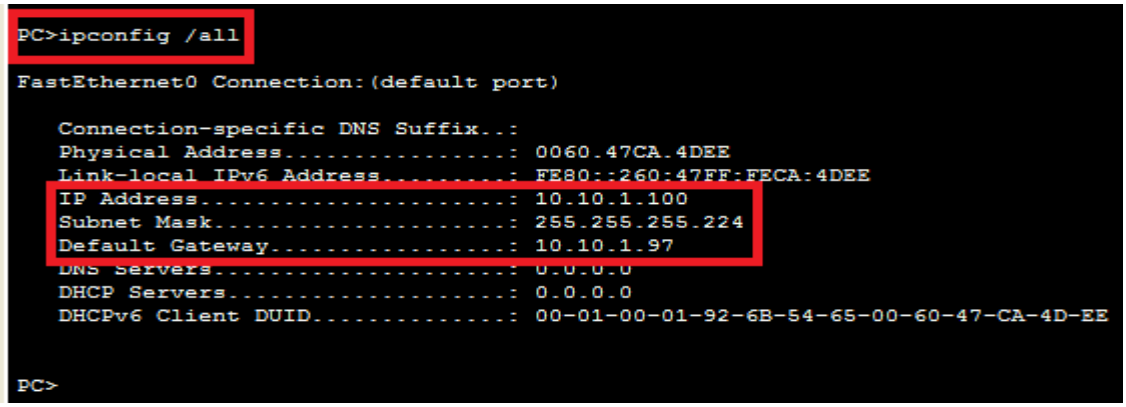
Parte 1: Completar la documentación de la tabla de direccionamiento

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

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

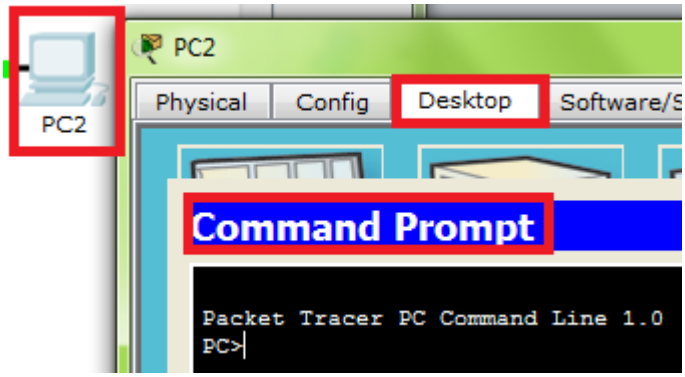


b. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.



Dispositivo	interfaz	Dirección IP	Mascara de Subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
PC2	NIC			

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



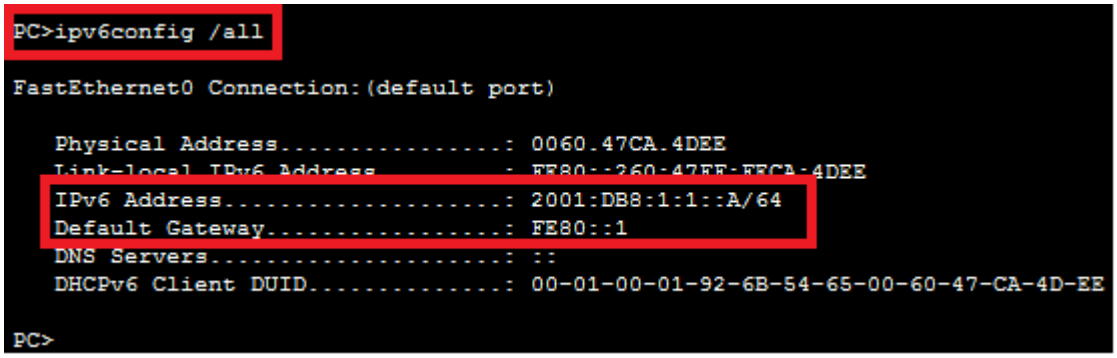
d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

```
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0060.7034.6930
   Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
   IP Address.....................: 10.10.1.20
   Subnet Mask.....................: 255.255.255.240
   Default Gateway.....................: 10.10.1.17
   DNS Servers.....................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID.....................: 00-01-00-01-CC-0A-6C-9A-00-60-70-34-69-30


PC>
```

Dispositivo	interfaz	Dirección IP	Mascara de Subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
PC1	NIC	10.10.1.100	255.255.255.224	10.10.1.97
PC2	NIC	10.10.1.20	255.255.255.240	10.10.1.17

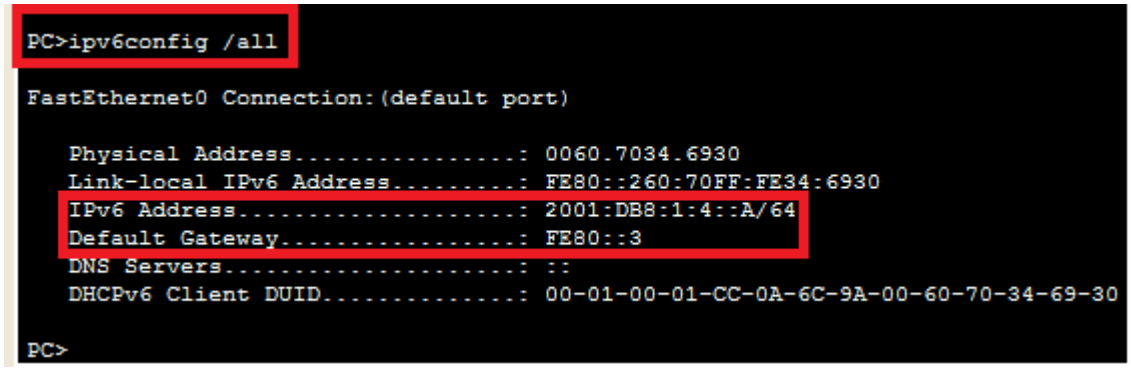
Paso 2: Usar el comando ipv6config para verificar el direccionamiento IPv6

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.



Dispositivo	interfaz	Dirección IP	Mascara de Subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
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

a. 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.



Dispositivo	interfaz	Dirección IP	Mascara de Subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
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

Parte 2: Probar la conectividad mediante el comando ping

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

a. Desde la **PC1**, haga ping a la dirección IPv4 de la **PC2**.

```
PC>ping 10.10.1.20

Pinging 10.10.1.20 with 32 bytes of data:

Request timed out.
Reply from 10.10.1.20: bytes=32 time=12ms TTL=125
Reply from 10.10.1.20: bytes=32 time=11ms TTL=125
Reply from 10.10.1.20: bytes=32 time=11ms TTL=125

Ping statistics for 10.10.1.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms

PC>
```

¿El resultado fue satisfactorio? Si

b. Desde la **PC2**, haga ping a la dirección IPv4 de la **PC1**.

```
PC>ping 10.10.1.100

Pinging 10.10.1.100 with 32 bytes of data:

Reply from 10.10.1.100: bytes=32 time=15ms TTL=125
Reply from 10.10.1.100: bytes=32 time=13ms TTL=125
Reply from 10.10.1.100: bytes=32 time=13ms TTL=125
Reply from 10.10.1.100: bytes=32 time=13ms TTL=125

Ping statistics for 10.10.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 15ms, Average = 13ms

PC>
```

¿El resultado fue satisfactorio? Si

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

a. Desde la **PC1**, haga ping a la dirección IPv6 de la **PC2**.

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

Pinging 2001:DB8:1:4::A with 32 bytes of data:

Reply from 2001:DB8:1:4::A: bytes=32 time=75ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=25ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=13ms TTL=125

Ping statistics for 2001:DB8:1:4::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 75ms, Average = 31ms

PC>
```

¿El resultado fue satisfactorio? Si

b. Desde la **PC2**, haga ping a la dirección IPv6 de la **PC1**.

```
PC>ping 2001:DB8:1:1::A

Pinging 2001:DB8:1:1::A with 32 bytes of data:

Reply from 2001:DB8:1:1::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=14ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=12ms TTL=125

Ping statistics for 2001:DB8:1:1::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 12ms

PC>
```

¿El resultado fue satisfactorio? Si

Parte 3: Descubrir la ruta mediante su rastreo

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

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

PC> **tracert 10.10.1.20**

```
PC>tracert 10.10.1.20

Tracing route to 10.10.1.20 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.1.97
  2    0 ms      0 ms      1 ms      10.10.1.5
  3    11 ms     11 ms     11 ms     10.10.1.10
  4    12 ms     12 ms     13 ms     10.10.1.20

Trace complete.

PC>
```

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

```
10.10.1.97
10.10.1.5
10.10.1.10
10.10.1.20
```

¿Con qué interfaces se asocian las cuatro direcciones?

G0/0 del R1, S0/0/0 en el R2, S0/0/1 en el R3, y NIC de la PC2

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

```
PC>tracert 10.10.1.100

Tracing route to 10.10.1.100 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.1.17
  2    1 ms      1 ms      0 ms      10.10.1.9
  3    10 ms     10 ms     1 ms      10.10.1.6
  4    13 ms     10 ms     11 ms     10.10.1.100

Trace complete.

PC>
```

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

```
10.10.1.17
10.10.1.9
10.10.1.6
10.10.1.100
```

¿Con qué interfaces se asocian las cuatro direcciones?
G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, y NIC de la PC1

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

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

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

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

Tracing route to 2001:DB8:1:4::A over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      2001:DB8:1:1::1
  2    0 ms      0 ms      0 ms      2001:DB8:1:2::1
  3    10 ms     1 ms      1 ms      2001:DB8:1:3::2
  4    11 ms     15 ms     14 ms     2001:DB8:1:4::A

Trace complete.

PC>
```

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

```
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?

G0/0 del R1, S/0/0/0 del R2, S0/0/1 del R3, y NIC de la PC2

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

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

Tracing route to 2001:DB8:1:1::A over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      2001:DB8:1:4::1
  2    3 ms      0 ms      3 ms      2001:DB8:1:3::1
  3    10 ms     11 ms     1 ms      2001:DB8:1:2::2
  4    12 ms     14 ms     14 ms     2001:DB8:1:1::A

Trace complete.

PC>
```

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

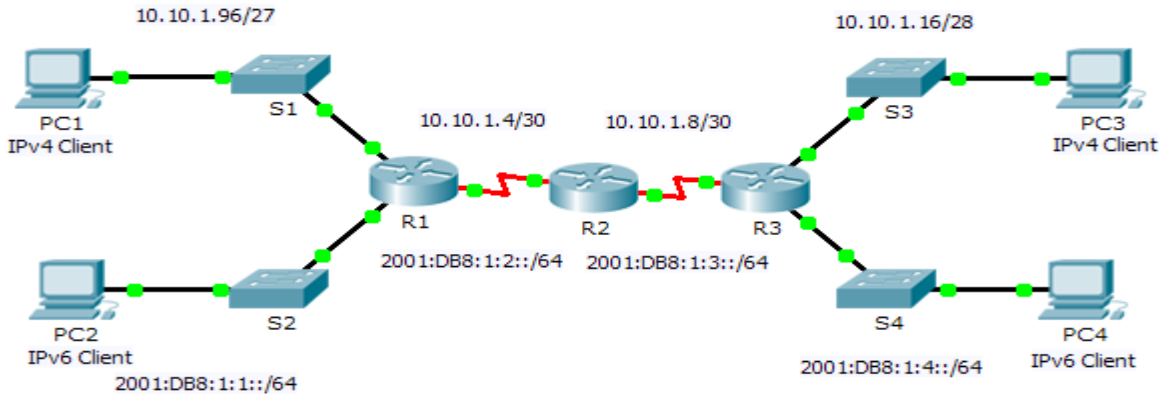
```
2001:DB8:1:4::1
2001:DB8:1:3::1
2001:DB8:1:2::2
2001:DB8:1:1::A
```

¿Con qué interfaces se asocian las cuatro direcciones?

Ga0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, y NIC de la PC1

8.3.2.6 Pinging Tracing to Test the Path

Packet Tracer: Ping y rastreo para probar rutas



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::2

Objetivos

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

Situación

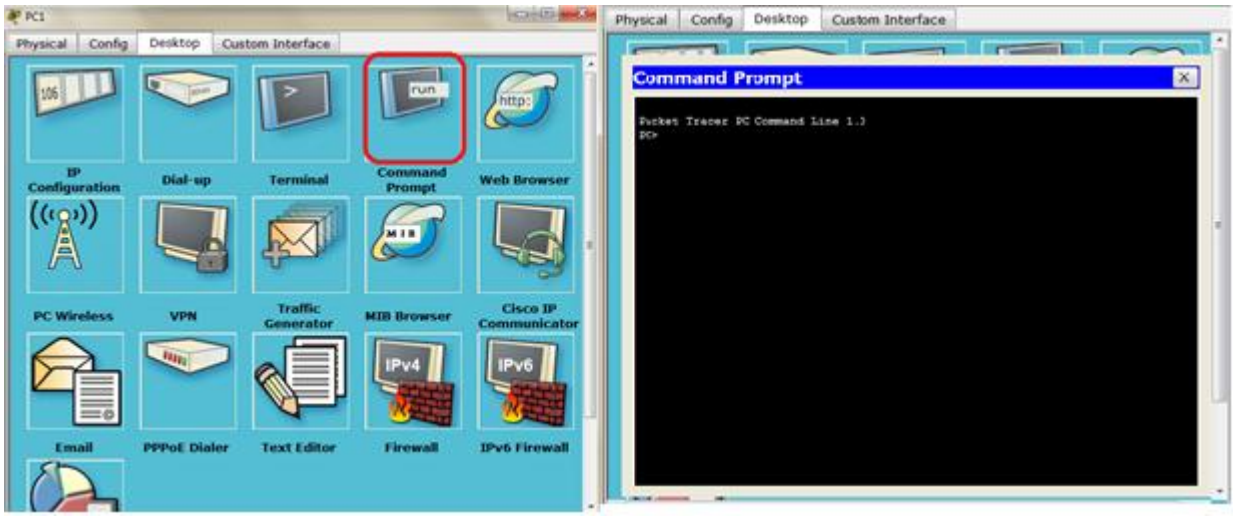
En esta actividad, hay problemas de conectividad. Además de recopilar y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad.

Nota: la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es **class**.

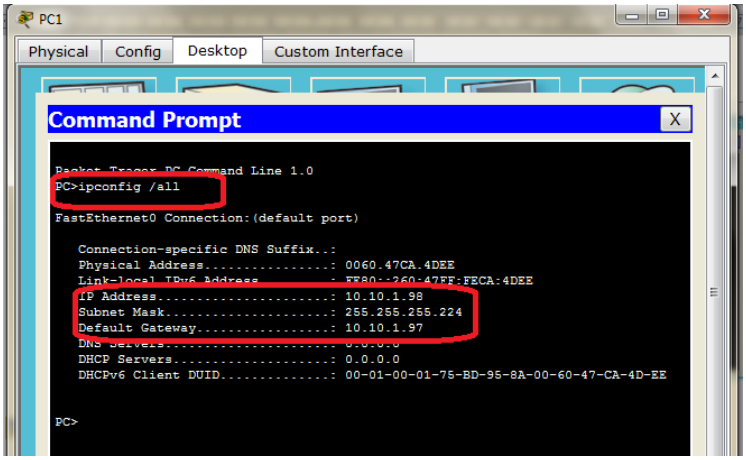
Parte 1: Probar y restaurar la conectividad IPv4

Paso 1: Usar los comandos ipconfig y ping para verificar la conectividad

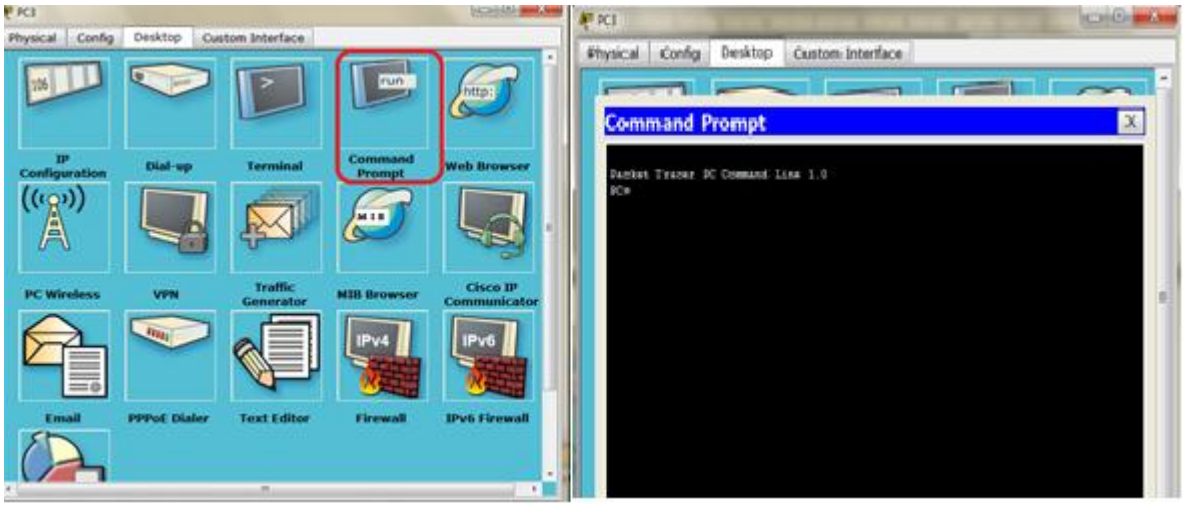
a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).



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

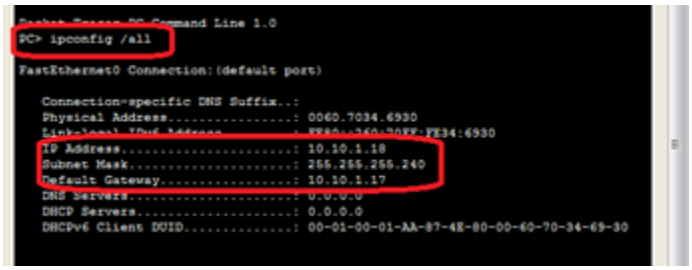


c. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

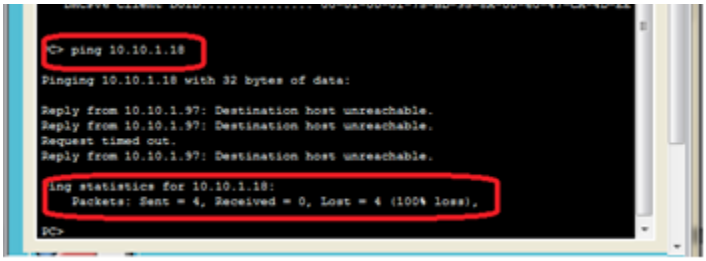


d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

Dispositivo	Interfaz	Dirección IPv4	Mascara de subred	Gateway predeterminado
		Dirección/ prefijo IPv6		
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17



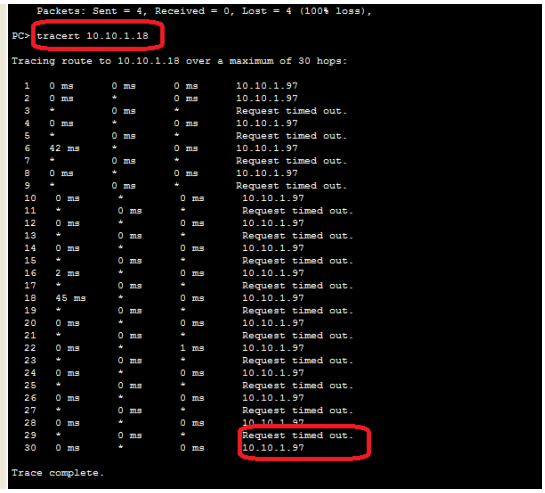
e. Pruebe la conectividad entre la **PC1** y la **PC3**. El ping debe fallar.



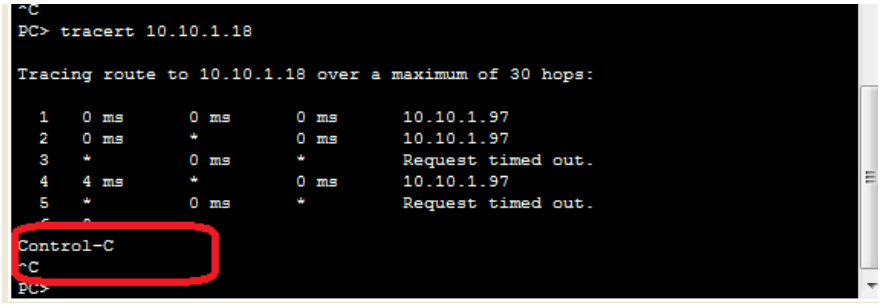
Paso 2: Localice el origen de la falla de conectividad.

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

RTA: 10.10.1.97

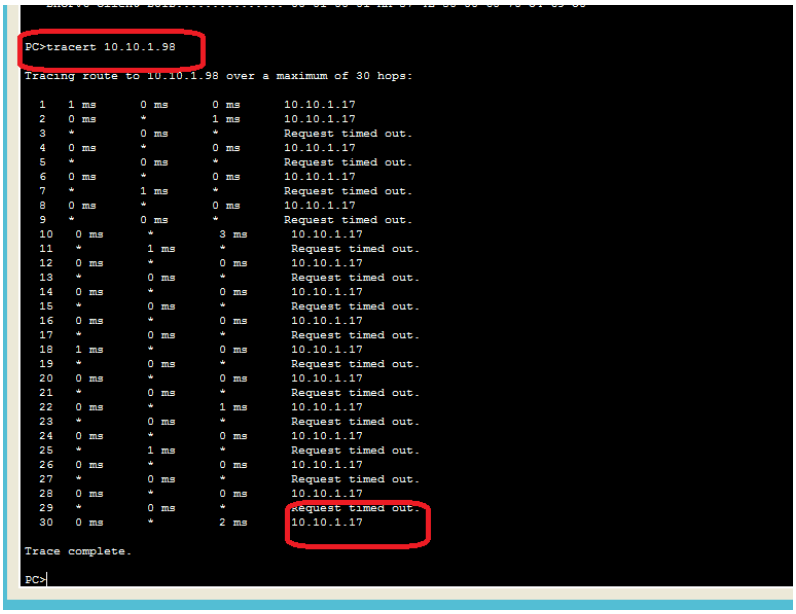


b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl+C** para detener el rastreo antes de los 30 intentos.

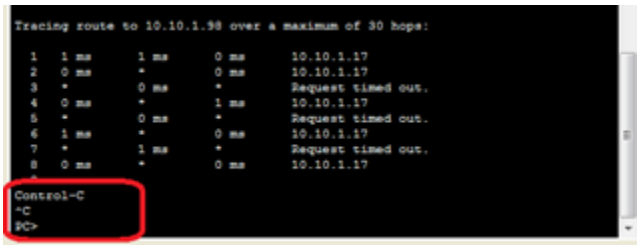


c. Desde la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**. ¿Cuál es la última dirección IPv4 correcta que alcanzó?

RTA: 10.10.1.17



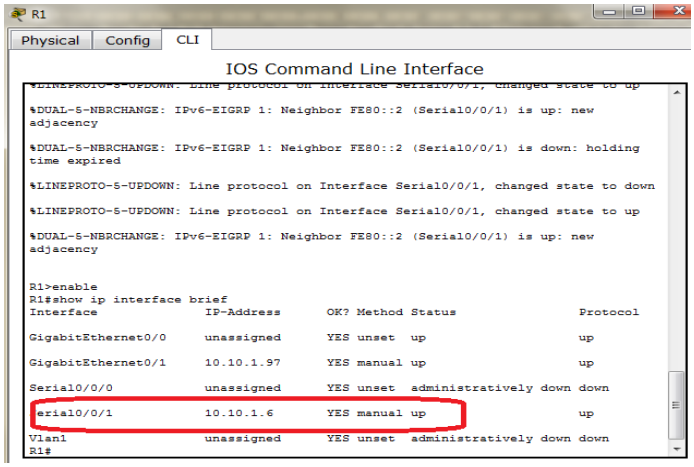
d. Introduzca **Ctrl+C** para detener el rastreo.



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

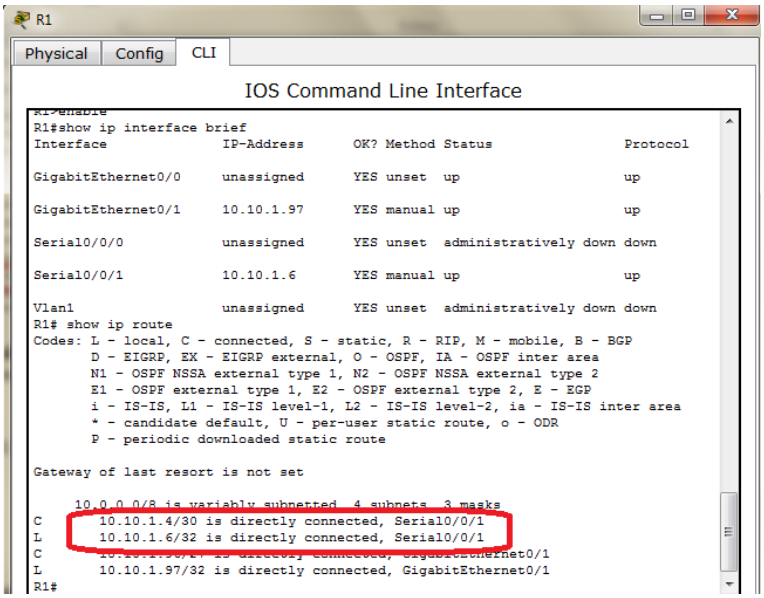
f. Introduzca el comando **show ip interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv4 en el router. Una se debió haber registrado en el paso 2a. ¿Cuál es la otra?

RTA: 10.10.1.6



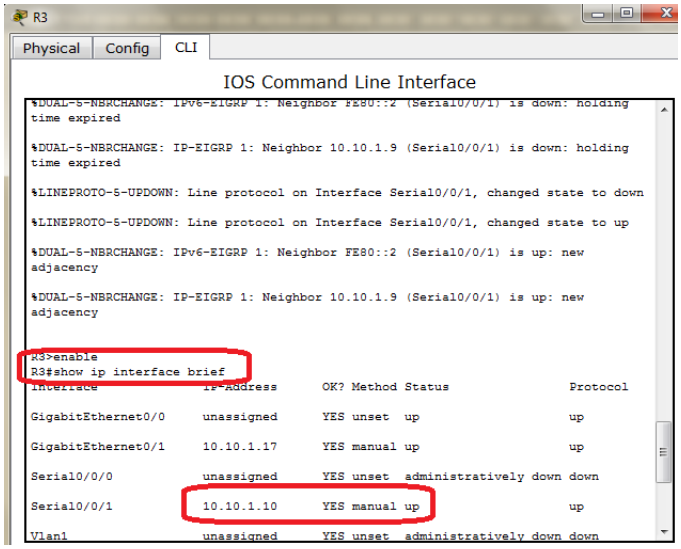
g. Introduzca el comando **show ip route** para obtener una lista de las redes a las que está conectado el router. Observe que hay dos redes conectadas a la interfaz **Serial0/0/1**. ¿Cuáles son?

RTA: 10.10.1.4/30, 10.10.1.6/32

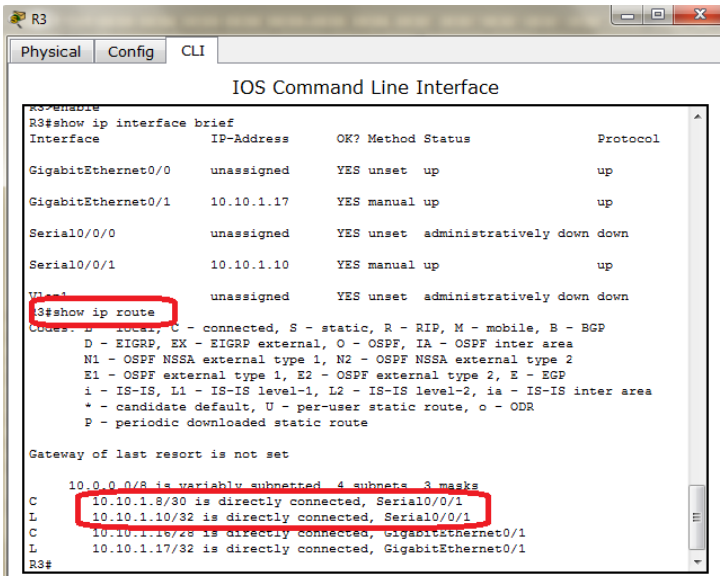


h. Repita los pasos 2e a 2g con el **R3** y escriba las respuestas aquí.

RTA: Dirección IPv4 10.10.1.10



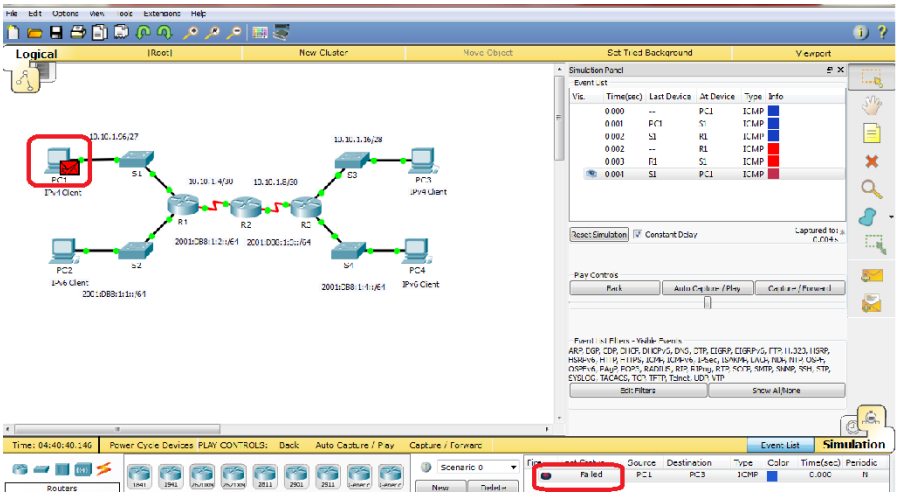
RTA: Redes conectadas a la interfaz serial 10/0/1 10.10.1.8/30, 10.10.1.10/32



Observe cómo cambia la interfaz serial para el R3.

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

RTA: Podemos observar que muestra error al momento en que llega la R1 y devuelve el mensaje con la respuesta fallida ya que en el paso del R1 al R2 podemos estar teniendo el error.



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?

RTA: La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP diferente.

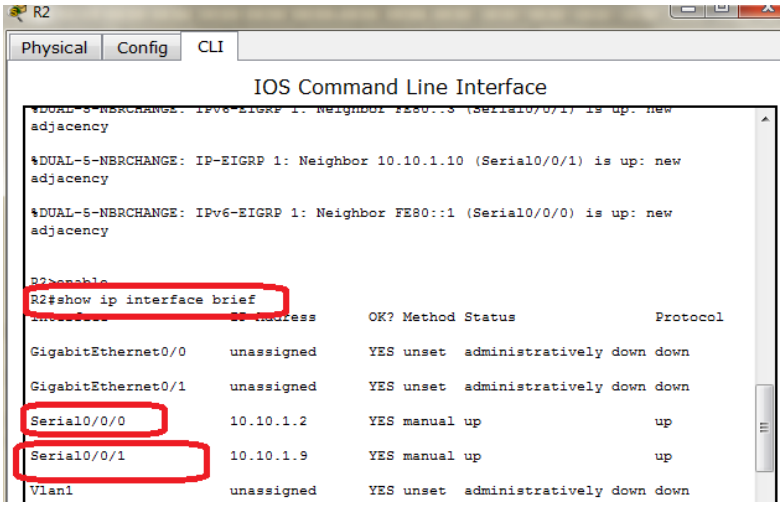
b. ¿Qué solución propondría para corregir el problema?

RTA: es necesario realizar la configuración 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.

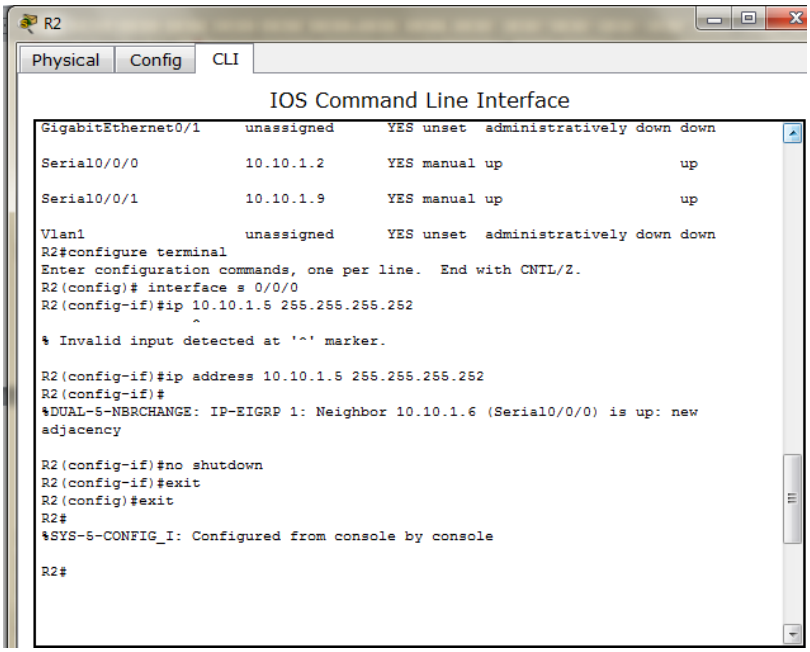
Se ingresa al R2 por CLI entramos al modo exec y al modo privilegiado
Verificamos las interfaces seriales que posee el R2



Procedemos a configurar la IP 10.10.1.5 introduciendo los siguientes comandos:

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface s 0/0/0
R2(config-if)#ip address 10.10.1.5 255.255.255.252
R2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.1.6 (Serial0/0/0) is up: new adjacency

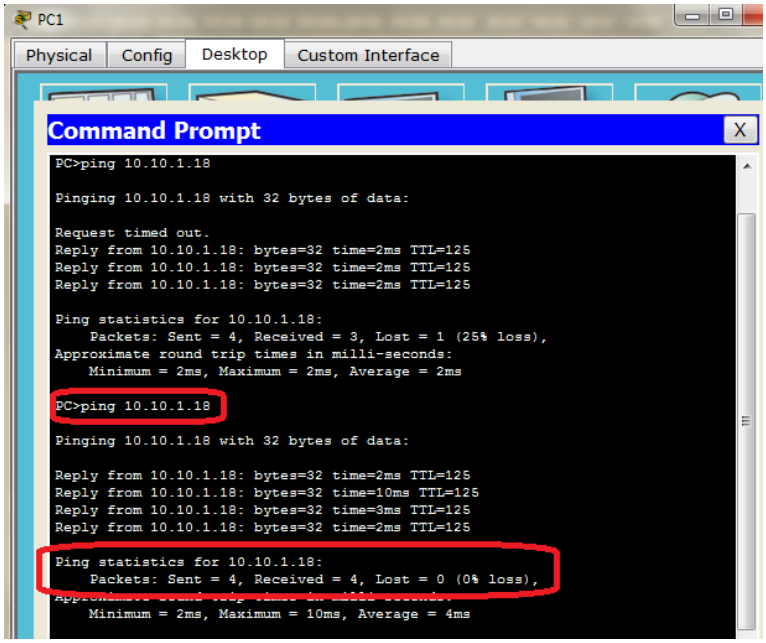
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit



Procedemos a realizar el ping desde PC1 al PC3 con el fin de verificar la conexión.

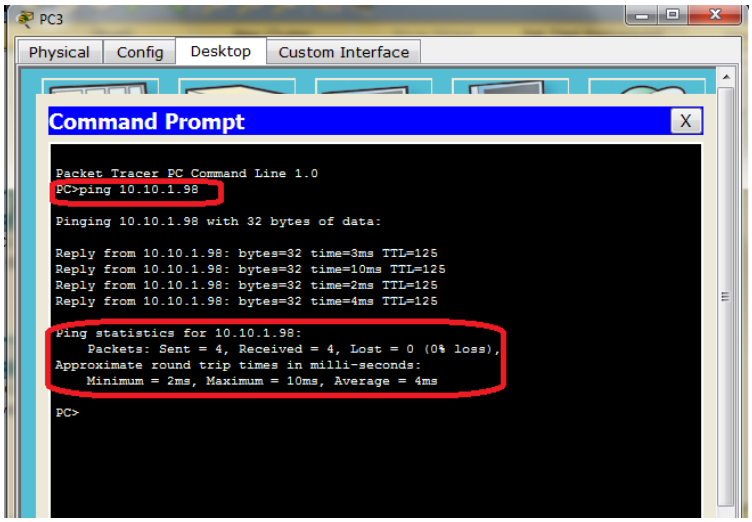
Paso 5: Verifique que la conectividad esté restaurada.

a. Desde la **PC1**, pruebe la conectividad a la **PC3**.



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

RTA: claro

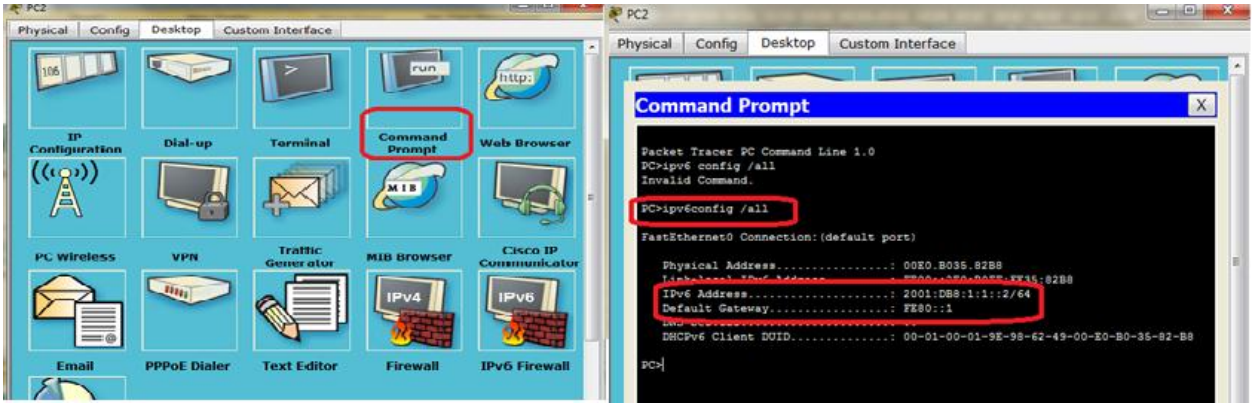


Parte 2: Probar y restaurar la conectividad IPv6

Paso 1: Usar los comandos ipv6config y ping para verificar la conectividad

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

b. 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.



c. Haga clic en **PC4** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt**.

d. 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.

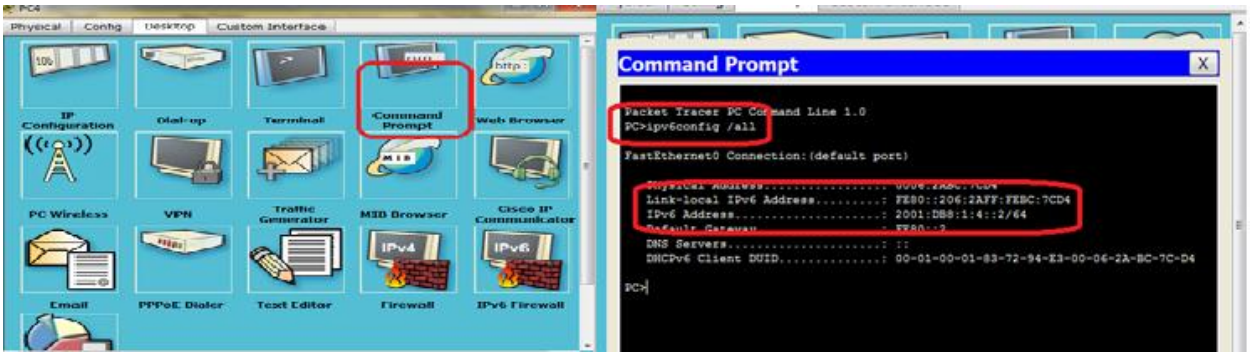
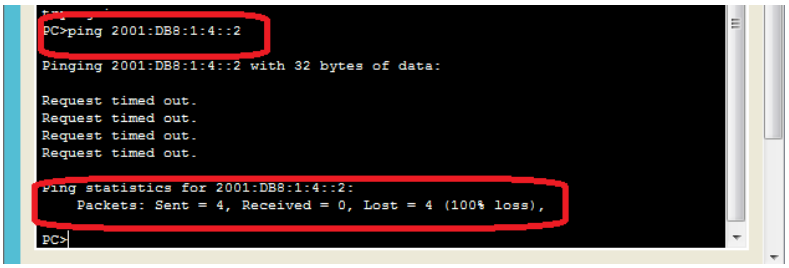


Tabla direccionamiento PC2 Y PC4

Dispositivo	interfaz	Dirección IPv4	Mascara de subred	Gateway predeterminado
		Dirección/ prefijo IPv6		
PC2	NIC	2001:DB8:1:1::2/64		FE80::1
PC4	NIC	2001:DB8:1:4::2/64		FE80::2

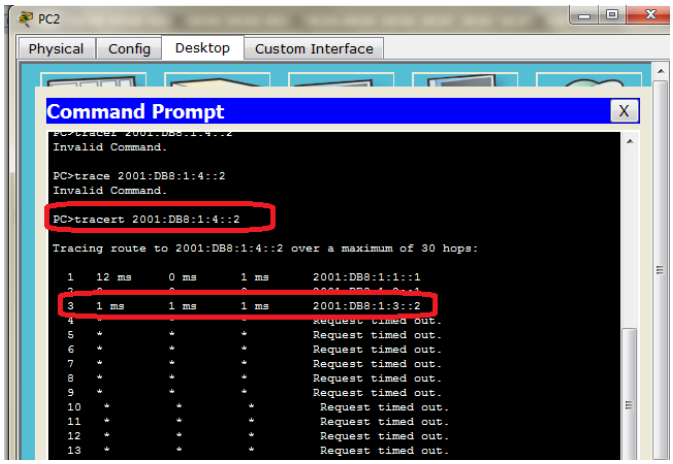
e. Pruebe la conectividad entre la **PC2** y la **PC4**. El ping debe fallar.



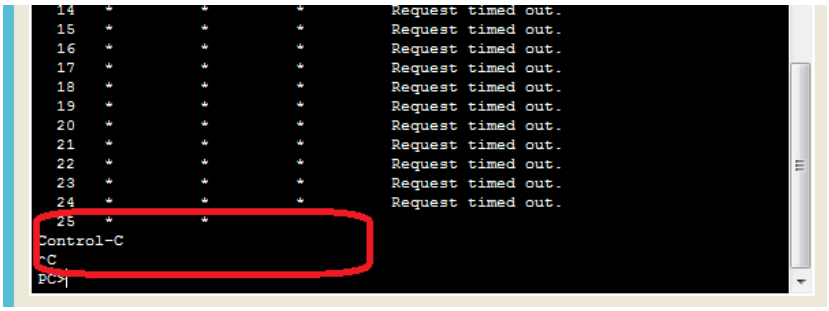
Paso 2: Localice el origen de la falla de conectividad.

a. Desde la **PC2**, introduzca el comando necesario para rastrear la ruta a la **PC4**. ¿Cuál es la última dirección IPv6 correcta que se alcanzó?

RTA: 2001:DB8:1:3::2

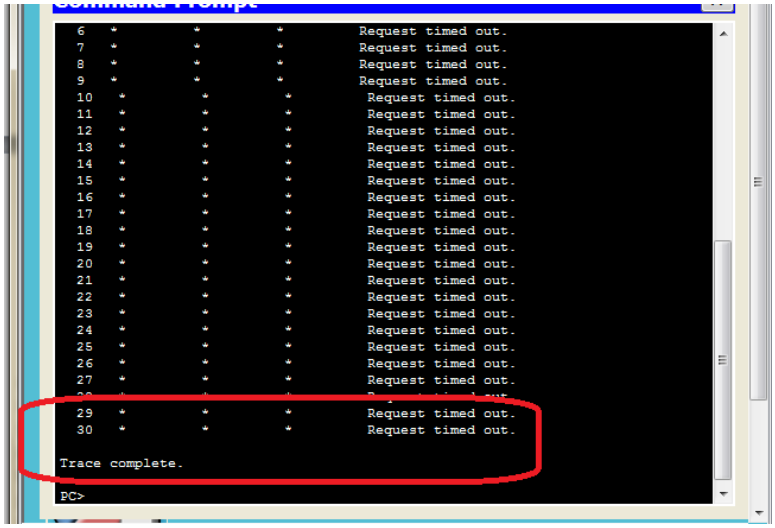


b. El rastreo finalmente terminará después de 30 intentos. Introduzca **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

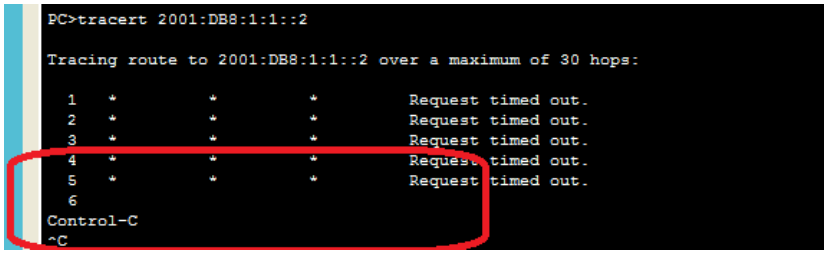


c. Desde la **PC4**, introduzca el comando necesario para rastrear la ruta a la **PC2**. ¿Cuál es la última dirección IPv6 correcta que se alcanzó?

RTA: No se alcanzó ninguna dirección IPv6.

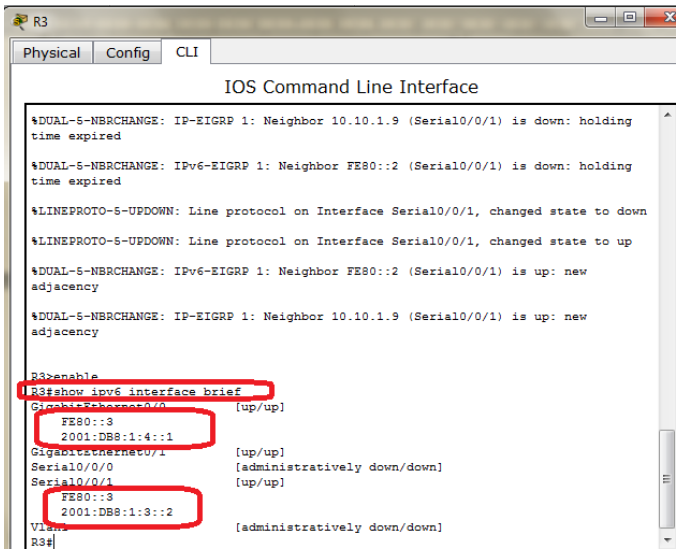


d. Introduzca **Ctrl**+**C** para detener el rastreo.

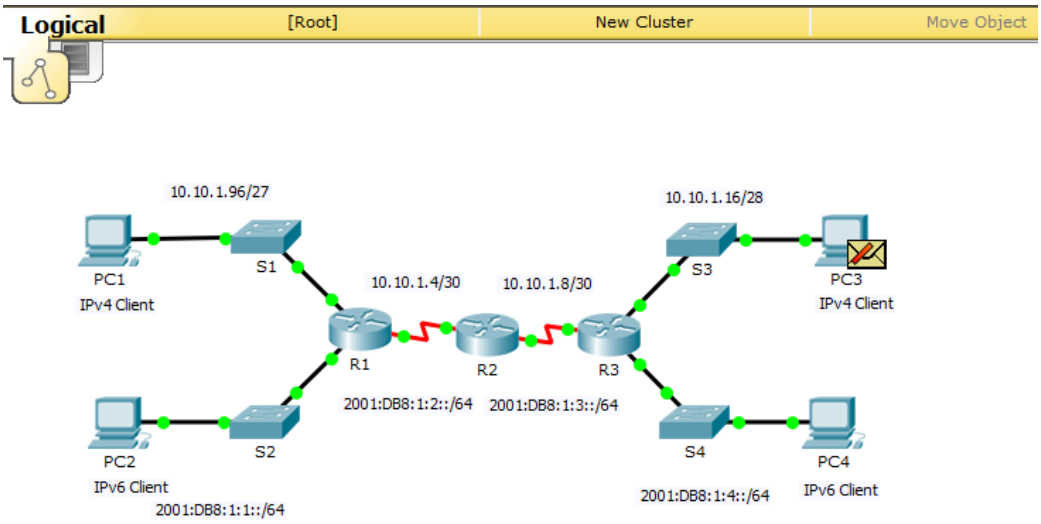


e. Haga clic en **R3** y, a continuación, haga clic en la ficha **CLI**. Presione **ENTRAR** e inicie sesión en el router.

f. Introduzca el comando **show ipv6 interface brief** para obtener una lista de las interfaces y su estado. Hay dos direcciones IPv6 en el router. Una debe coincidir con la dirección de gateway registrada en el paso 1d. ¿Hay alguna discrepancia?



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

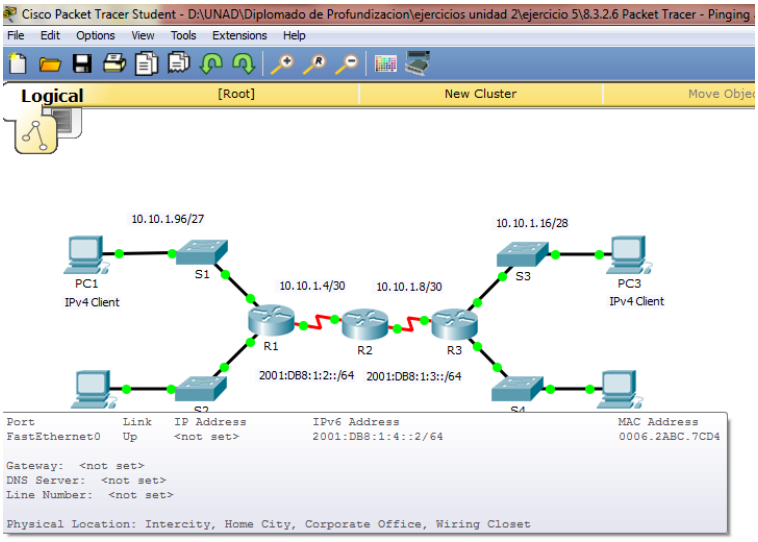


Al realizar las pruebas en la simulación se muestra que el PDU va por toda la red sin tener un correcto direccionamiento haciendo que la prueba tenga como resultado fallido

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?

RTA: La PC4 utiliza una configuración incorrecta.



b. ¿Qué solución propondría para corregir el problema?

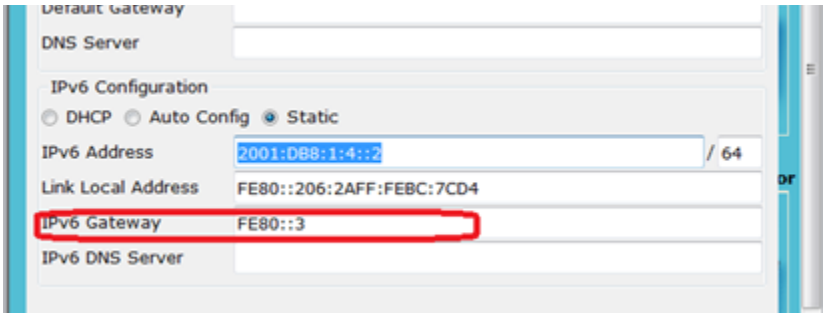
RTA: Configurar la PC4 con la dirección de gateway predeterminado correcta: FE80::3.

Paso 4: Implemente el plan.
Implemente la solución que propuso en el paso 3b.

Haga clic en PC4, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

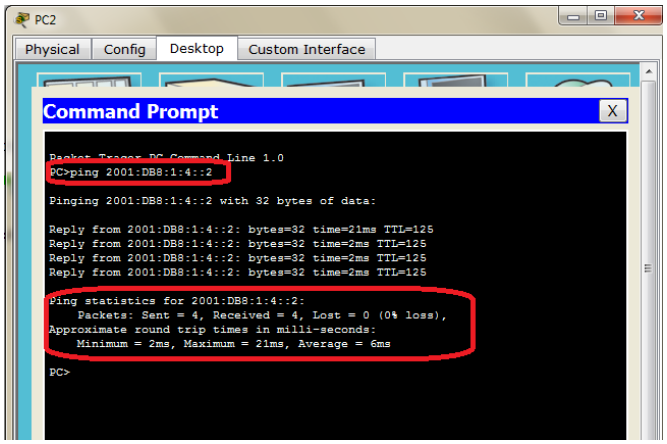
Establezca la dirección IPv6 2001:DB8:1:4::2 con el prefijo /64.

Configure el gateway IPv6 en este caso FE80::3 ya que es allí donde se encuentra el error.



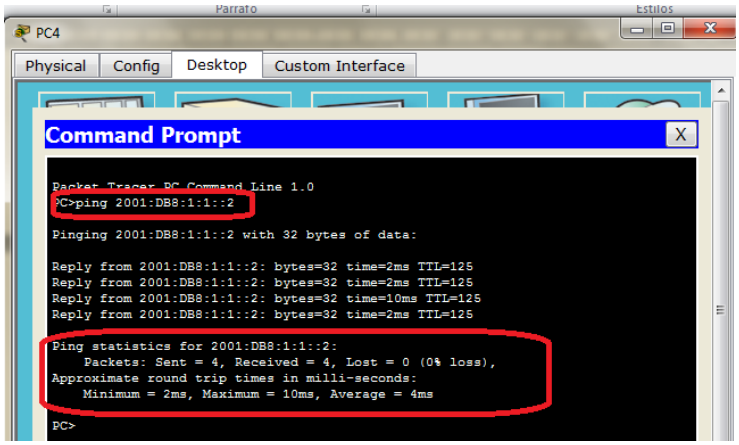
Paso 5: Verifique que la conectividad esté restaurada.

a. Desde la **PC2**, pruebe la conectividad a la **PC4**.



b. Desde la **PC4**, pruebe la conectividad a la **PC2**. ¿Se resolvió el problema?

RTA: Sí


Párrafo
Estilos
PC4
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:1:1::2
Pinging 2001:DB8:1:1::2 with 32 bytes of data:
Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Ping statistics for 2001:DB8:1:1::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 10ms, Average = 4ms
PC>

8.3.2.8 Troubleshooting Ipv4 and IPv6 Addressing Instructions IG

Packet Tracer: Resolución de problemas de direccionamiento IPv4 e IPv6

Topología

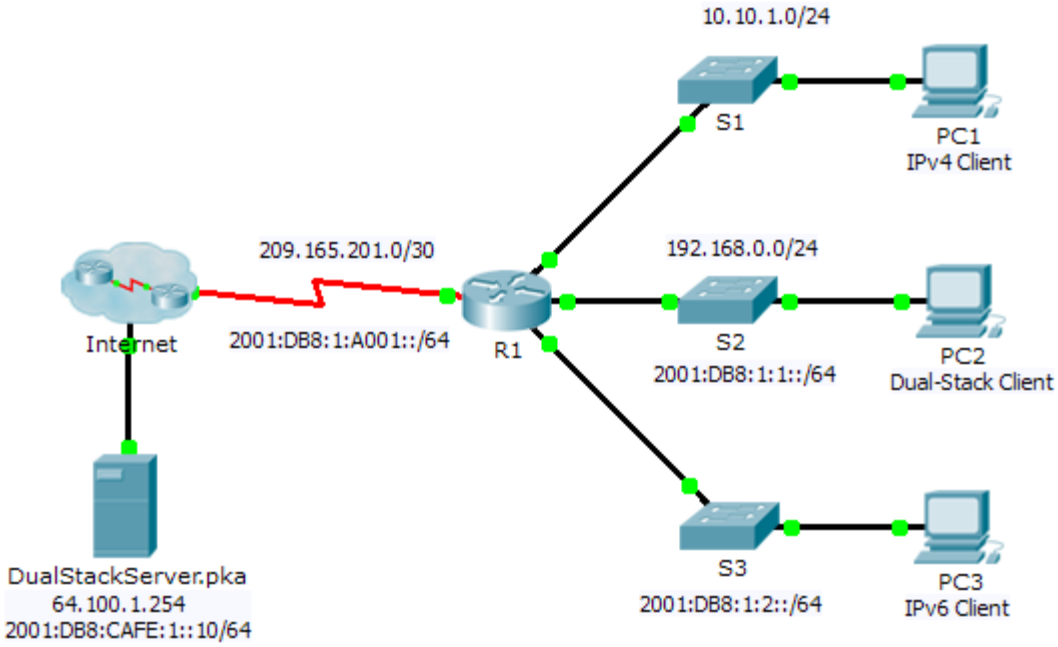


Tabla de direccionamiento

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

Dual-stack Servidor	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.

a. 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.

b. 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.

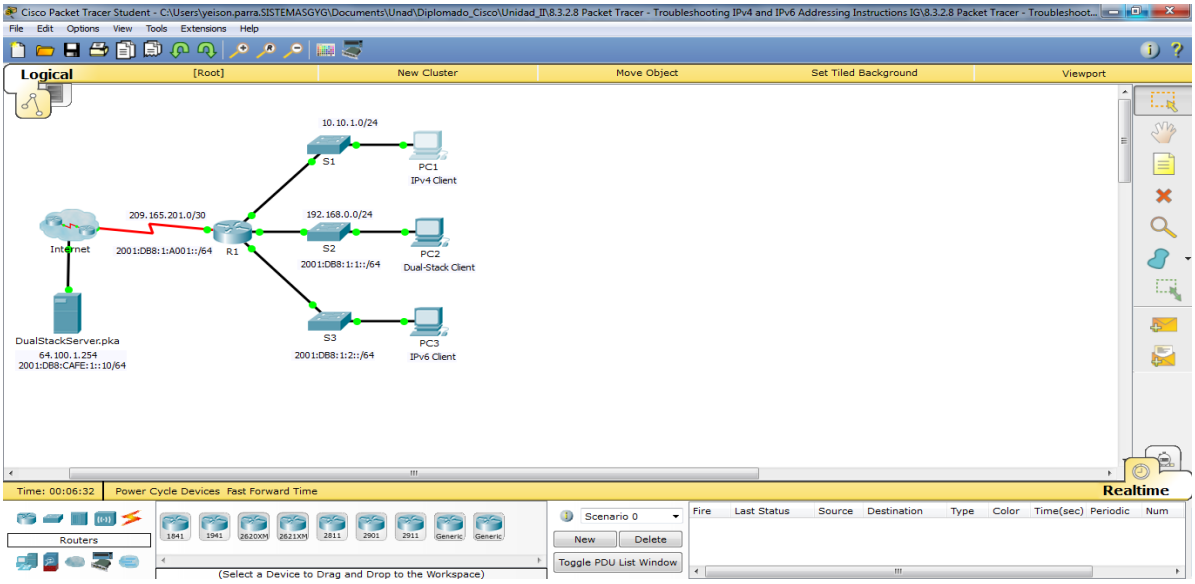
Paso 5: Verificar que la solución haya resuelto el problema.

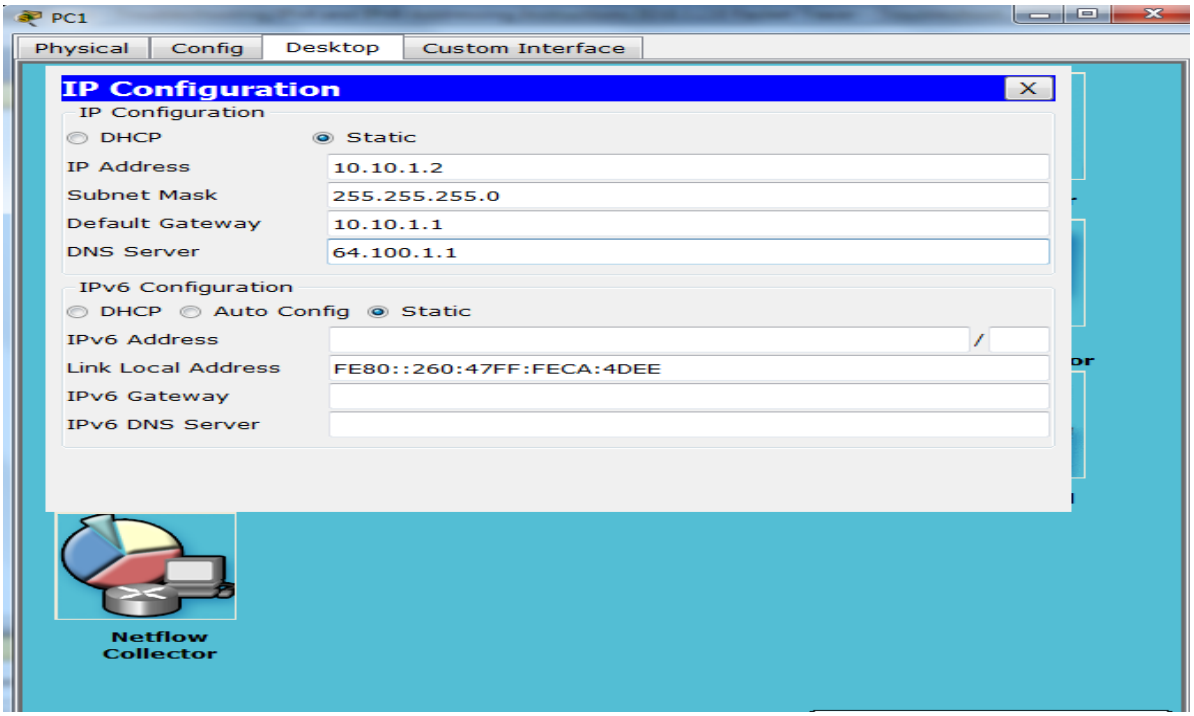
a. Repita las pruebas de la solicitud de soporte técnico. ¿Se solucionó el problema?

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

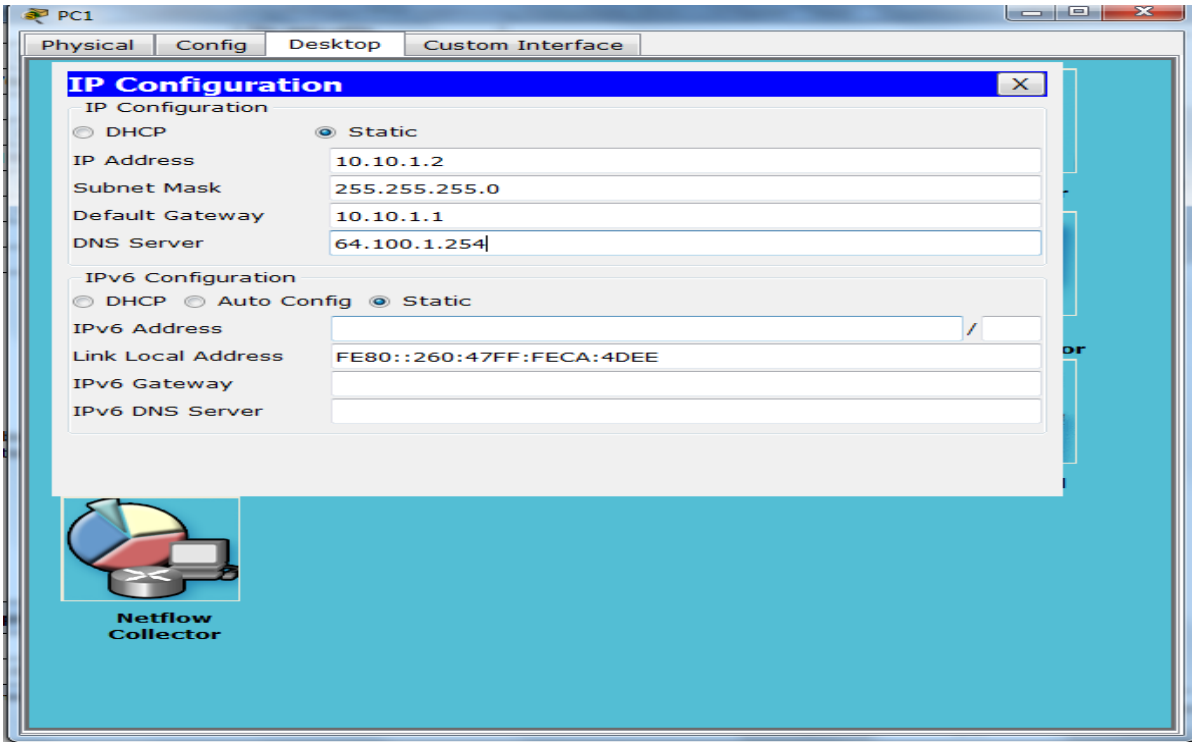
Paso 6: Documentar la solución.

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





Se cambia al DNS del servidor:



Parte 2: Resolver el segundo 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.

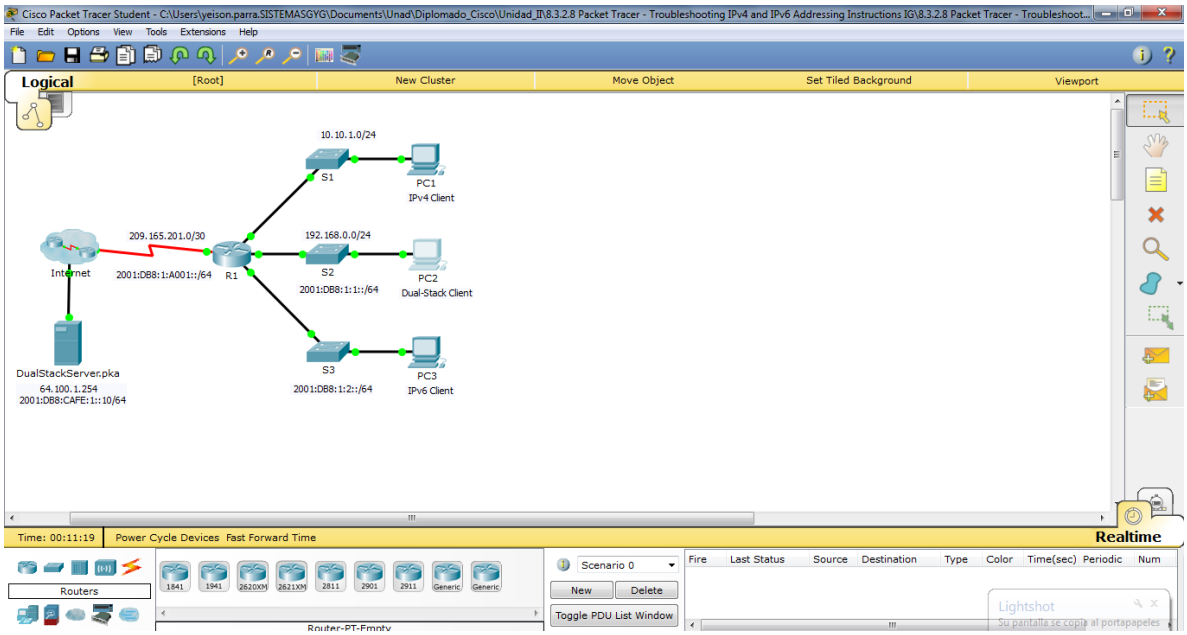
El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

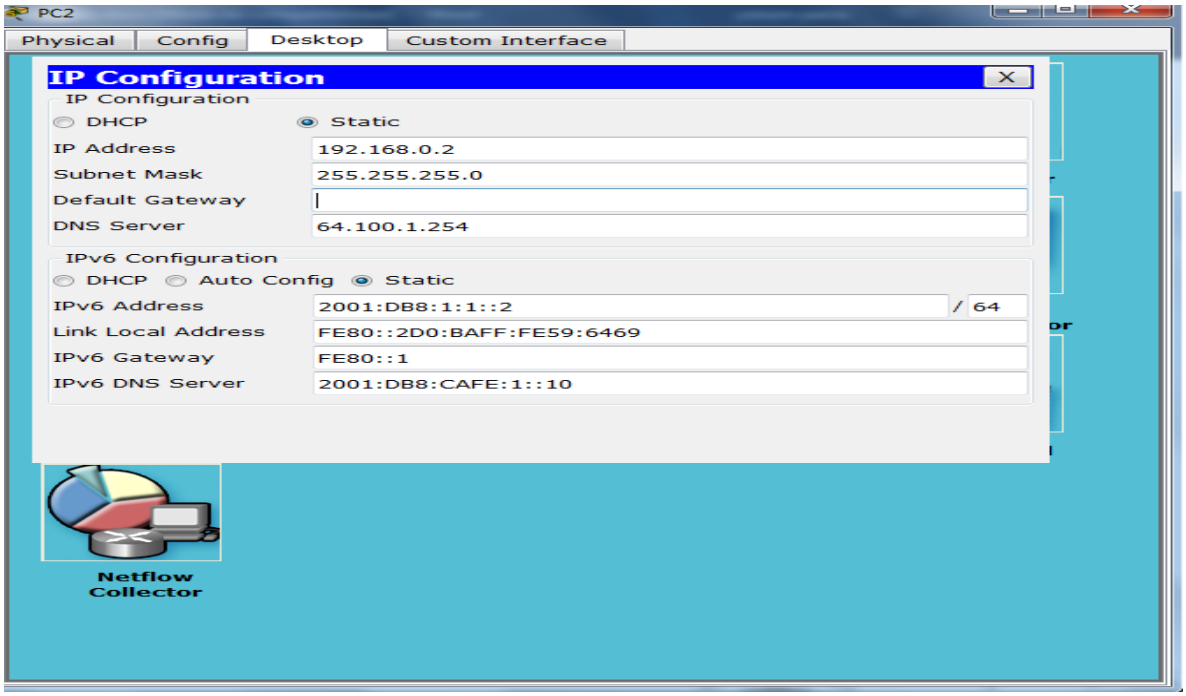
Solicitud de soporte técnico	
Identificador de cliente: PC2	
Problema: No puede acceder al servicio FTP de 2001:DB8:CAFE:1:10.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza**ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway 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.





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.

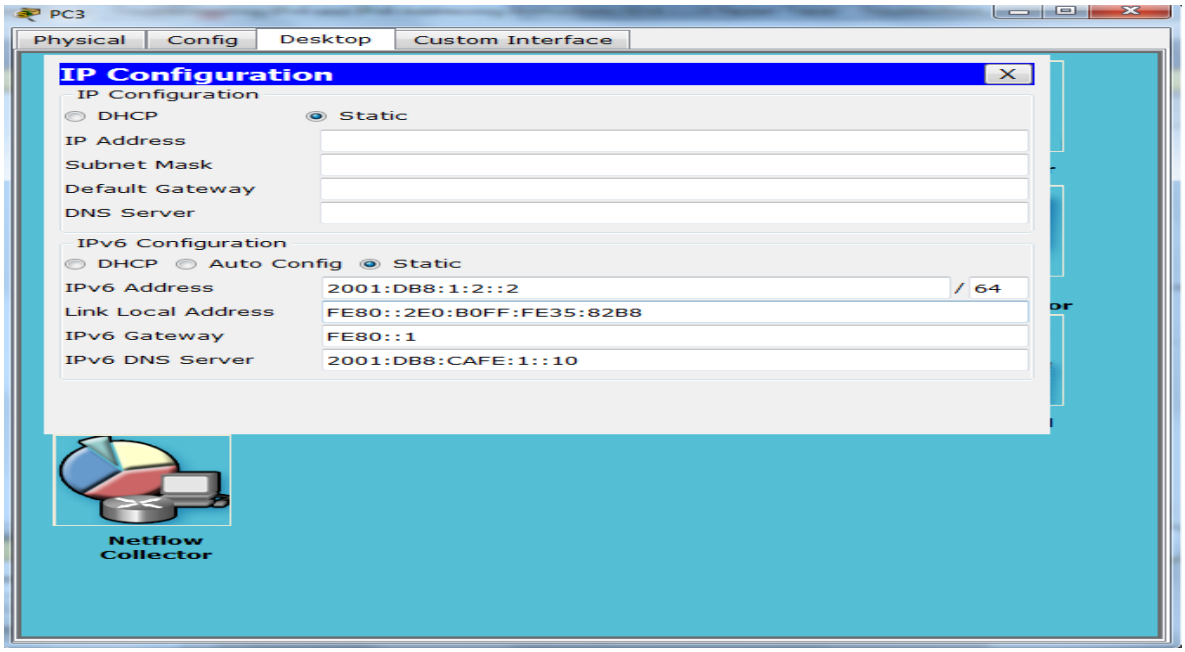
El soporte técnico recopiló la siguiente información del usuario por vía telefónica. Verifique que sea correcto.

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.	

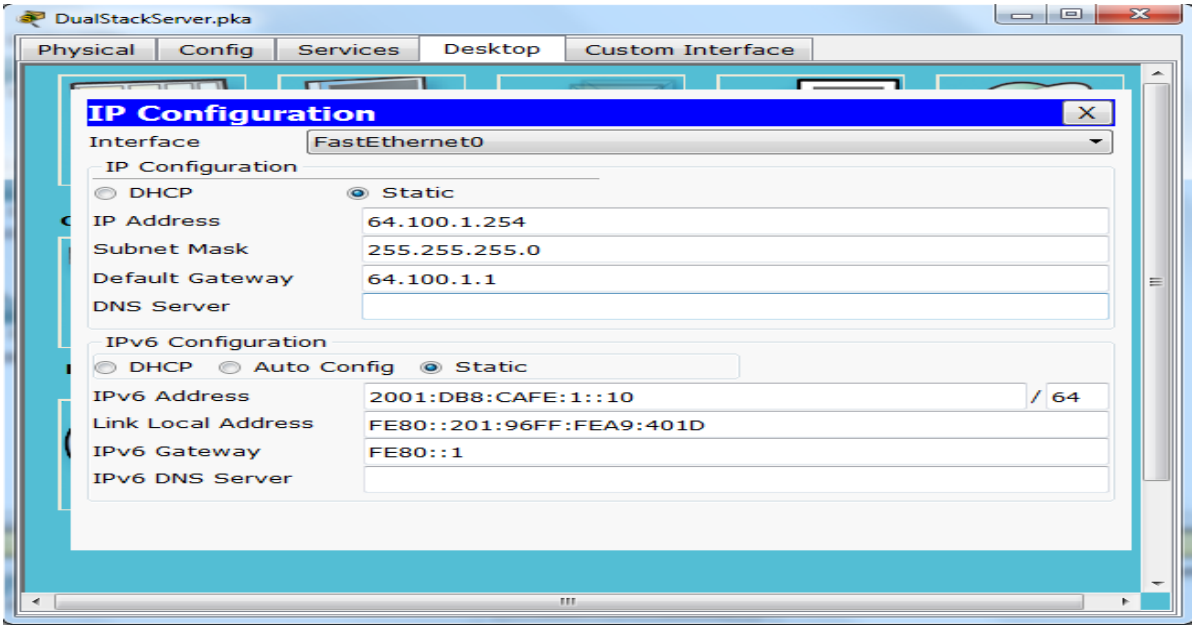
Paso 2: Realizar los pasos 2 a 5 de la parte 1 para abordar este problema.

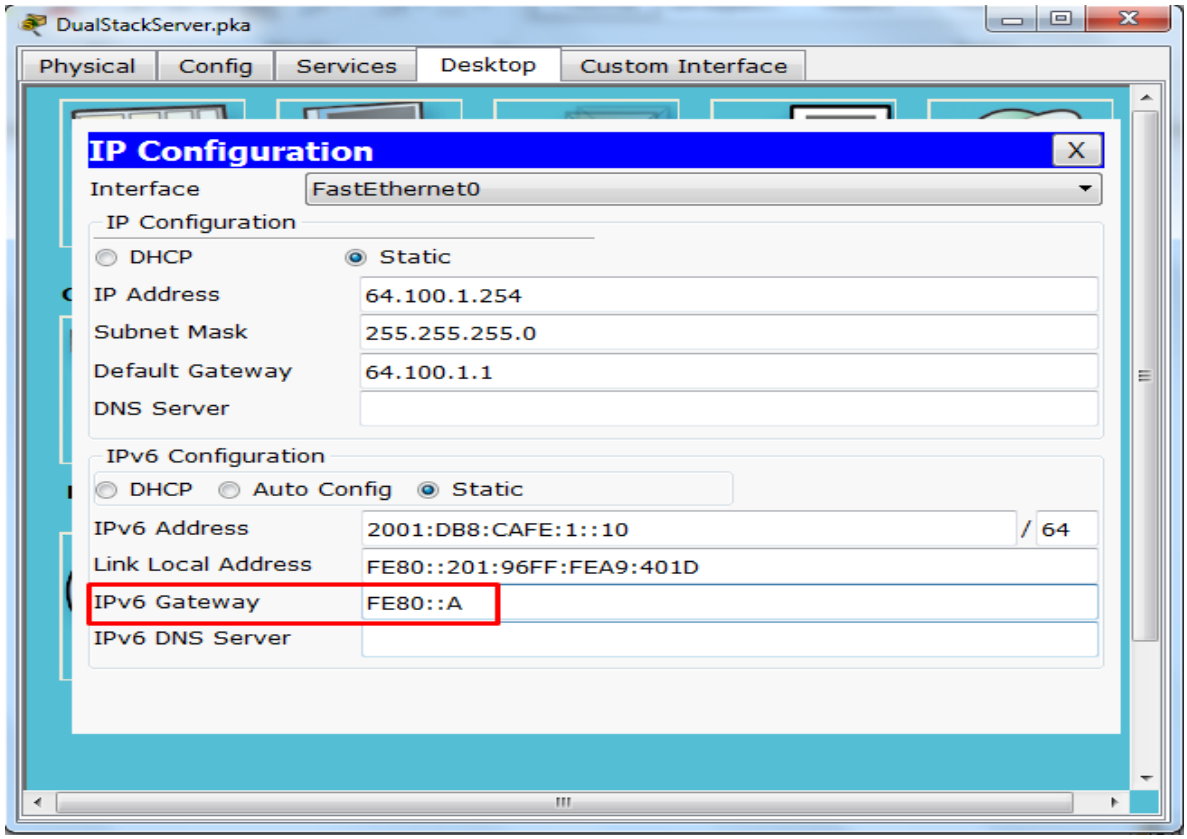
Paso 3: Documentar la solución.

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


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:1:2::2
/ 64
Link Local Address
FE80::2E0:B0FF:FE35:82B8
IPv6 Gateway
FE80::1
IPv6 DNS Server
2001:DB8:CAFE:1::10
Netflow Collector

Servidor:


DualStackServer.pka
Physical
Config
Services
Desktop
Custom Interface
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
64.100.1.254
Subnet Mask
255.255.255.0
Default Gateway
64.100.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:CAFE:1::10
/ 64
Link Local Address
FE80::201:96FF:FEA9:401D
IPv6 Gateway
FE80::1
IPv6 DNS Server


DualStackServer.pka
Physical
Config
Services
Desktop
Custom Interface
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
64.100.1.254
Subnet Mask
255.255.255.0
Default Gateway
64.100.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:CAFE:1::10
/ 64
Link Local Address
FE80::201:96FF:FEA9:401D
IPv6 Gateway
FE80::A
IPv6 DNS Server

8.4.1.2 Skills Integration Challenge Instructions IG

Packet Tracer: Reto de habilidades de integración

Tabla de direccionamiento

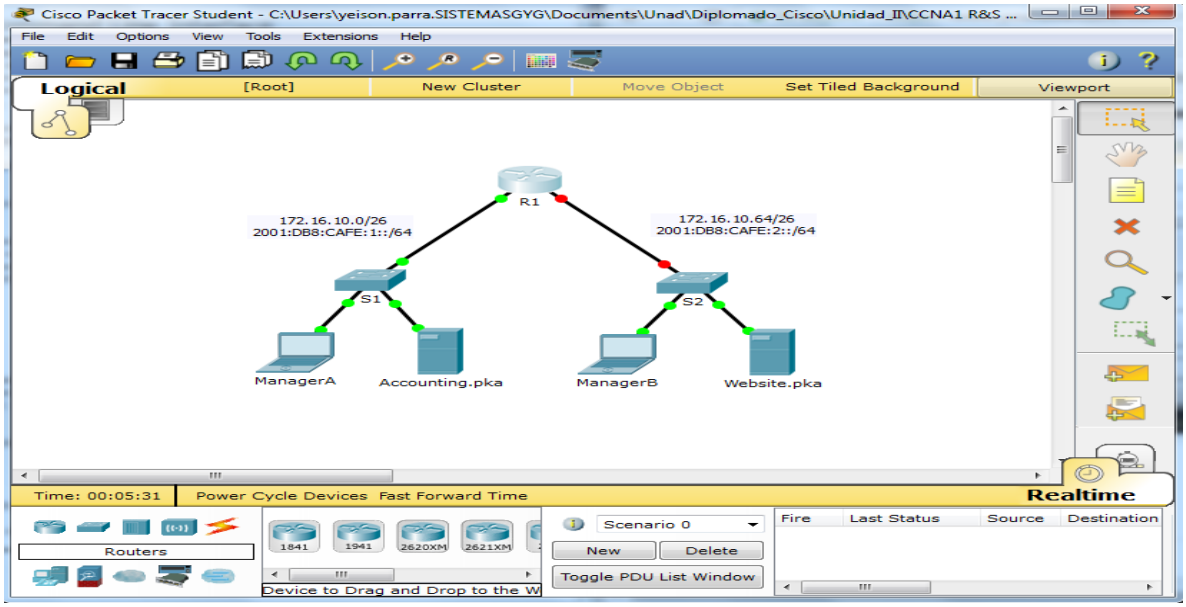
Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
R1	G0/0	172.16.10.1	255.255.255.192	No aplicable
		2001:DB8:CAFE:1::1/64		No aplicable
	G0/1	172.16.10.65	255.255.255.192	No aplicable
		2001:DB8:CAFE:2::1/64		No aplicable
	Link-local	FE80::1		No 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

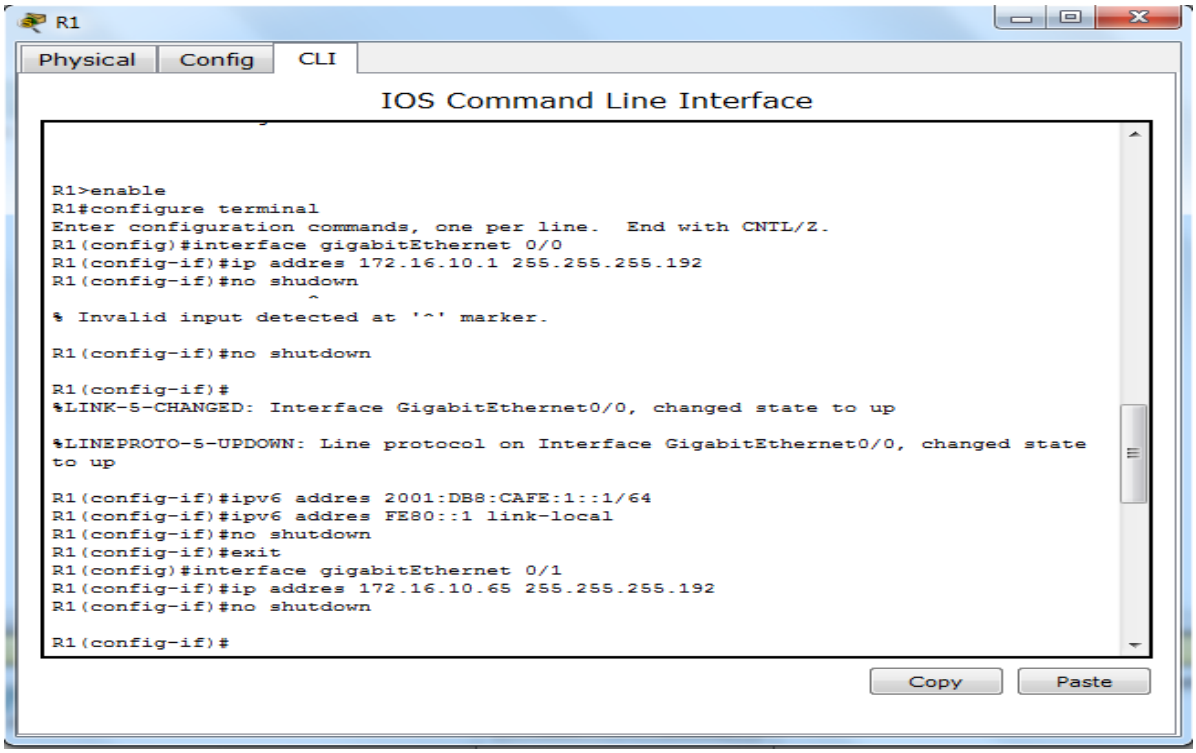
Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el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

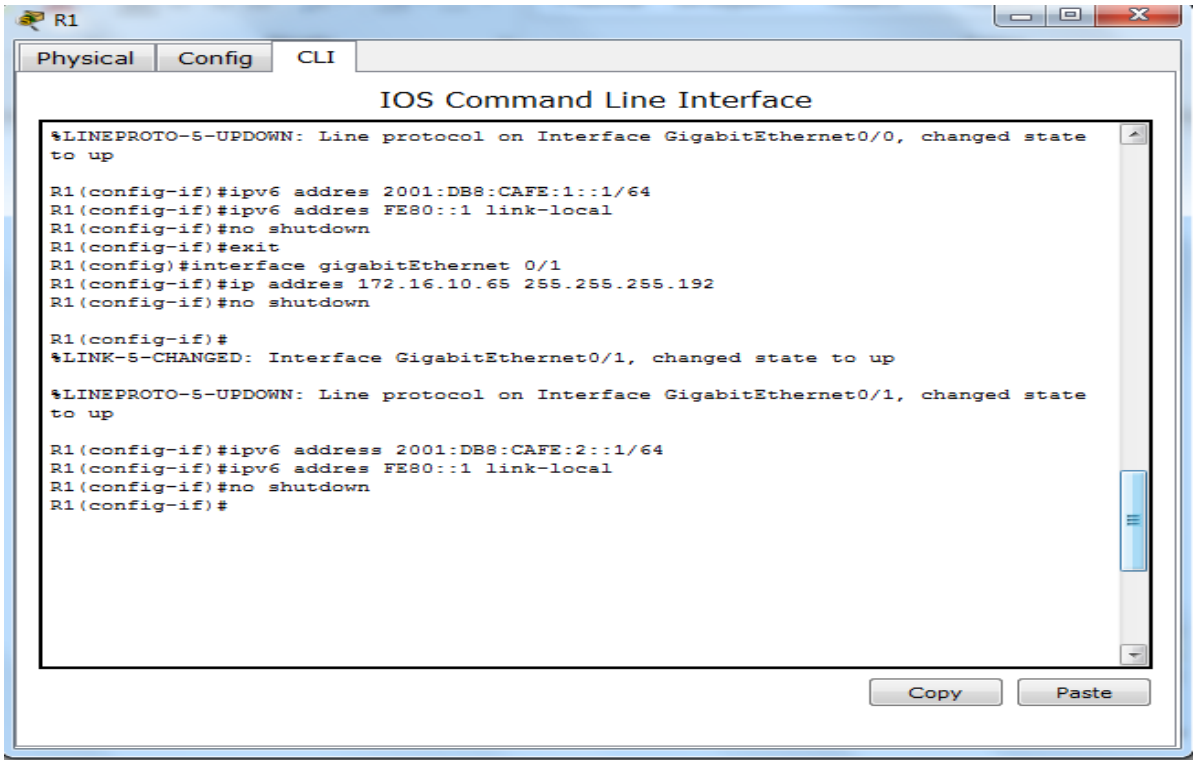
Requisitos

- Complete el registro de la **tabla de direccionamiento**.

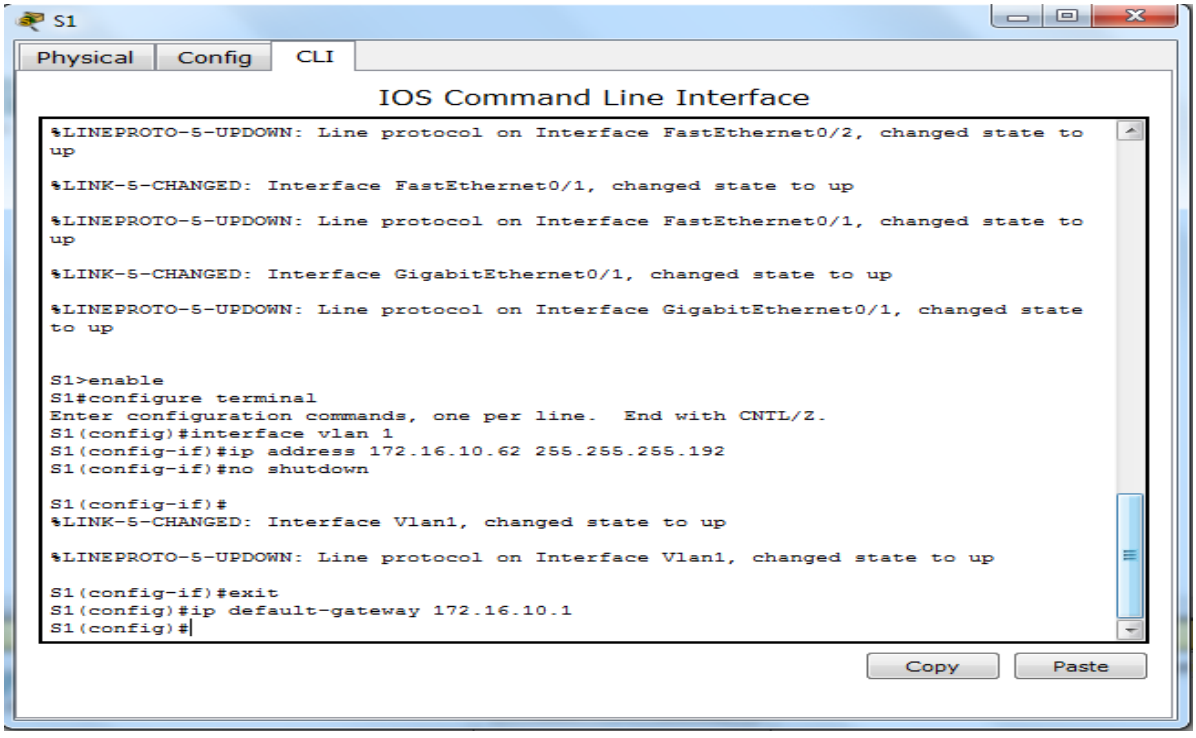


- Configure direccionamiento IPv4 e IPv6 en el **R1**.

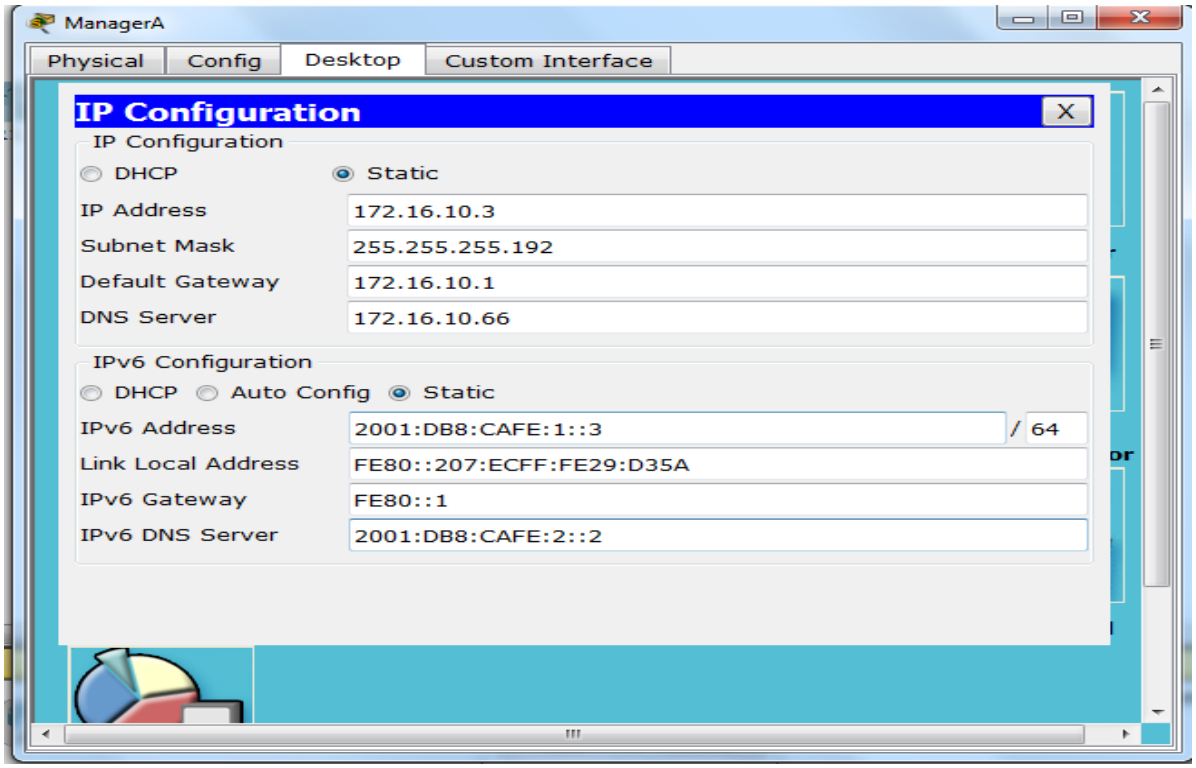


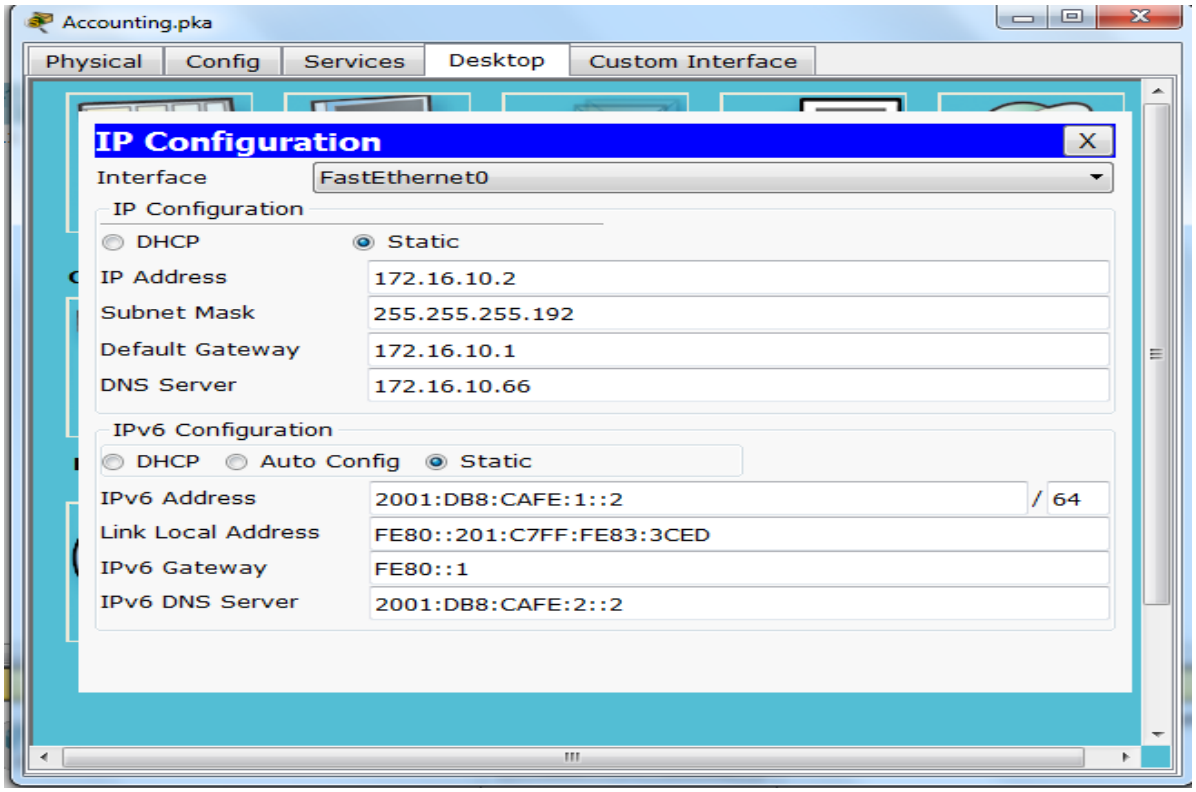


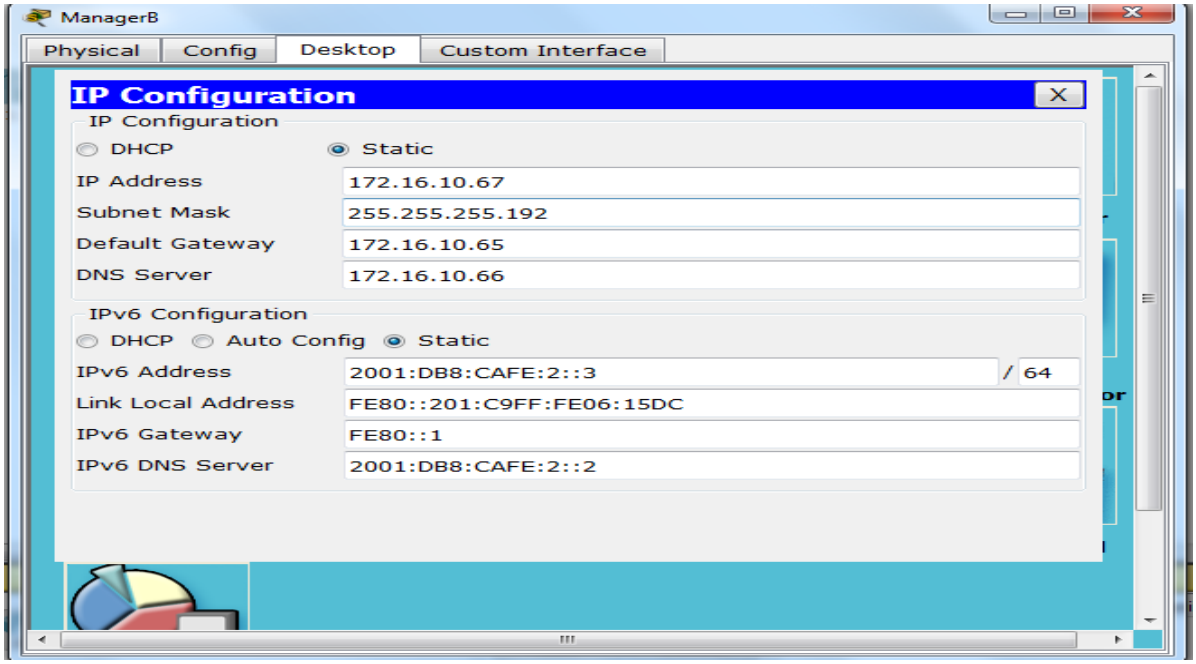
· Configure direccionamiento IPv4 en el **S1**. El **S2** ya está configurado.

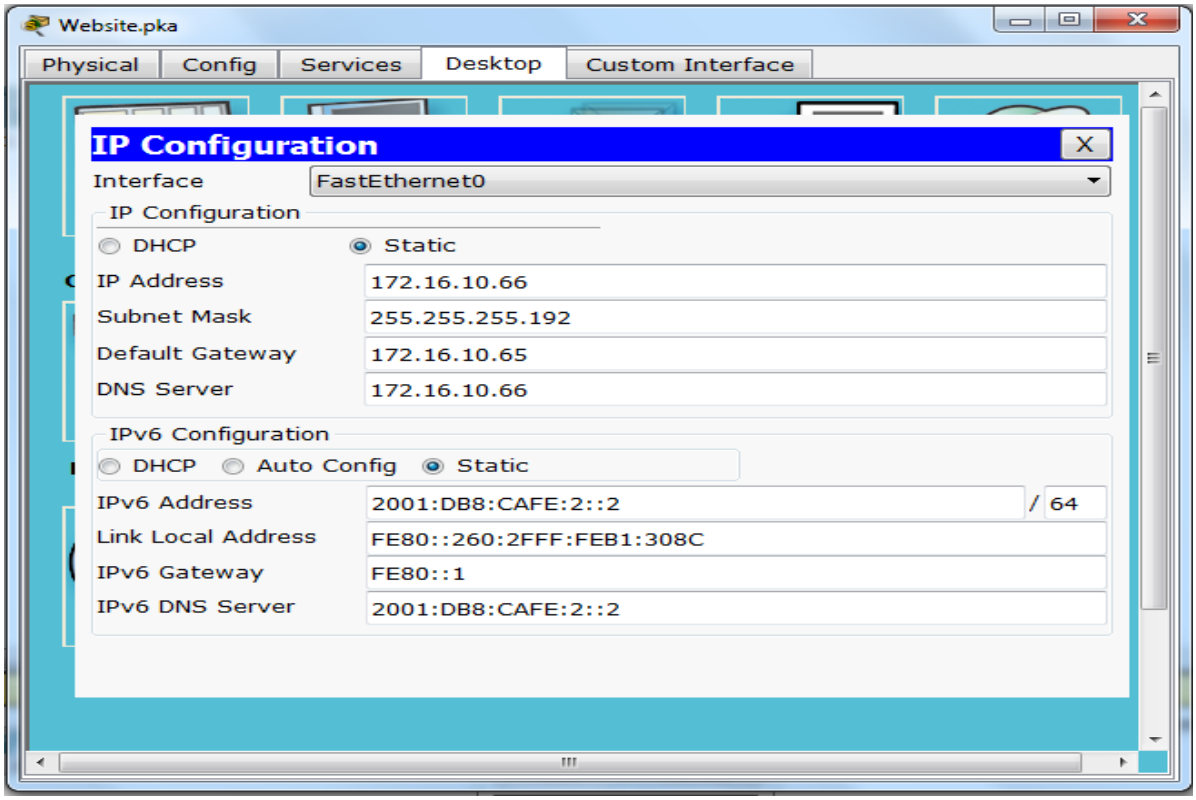


· Configure direccionamiento IPv4 e IPv6 en **ManagerA**. El resto de los clientes ya están configurados.

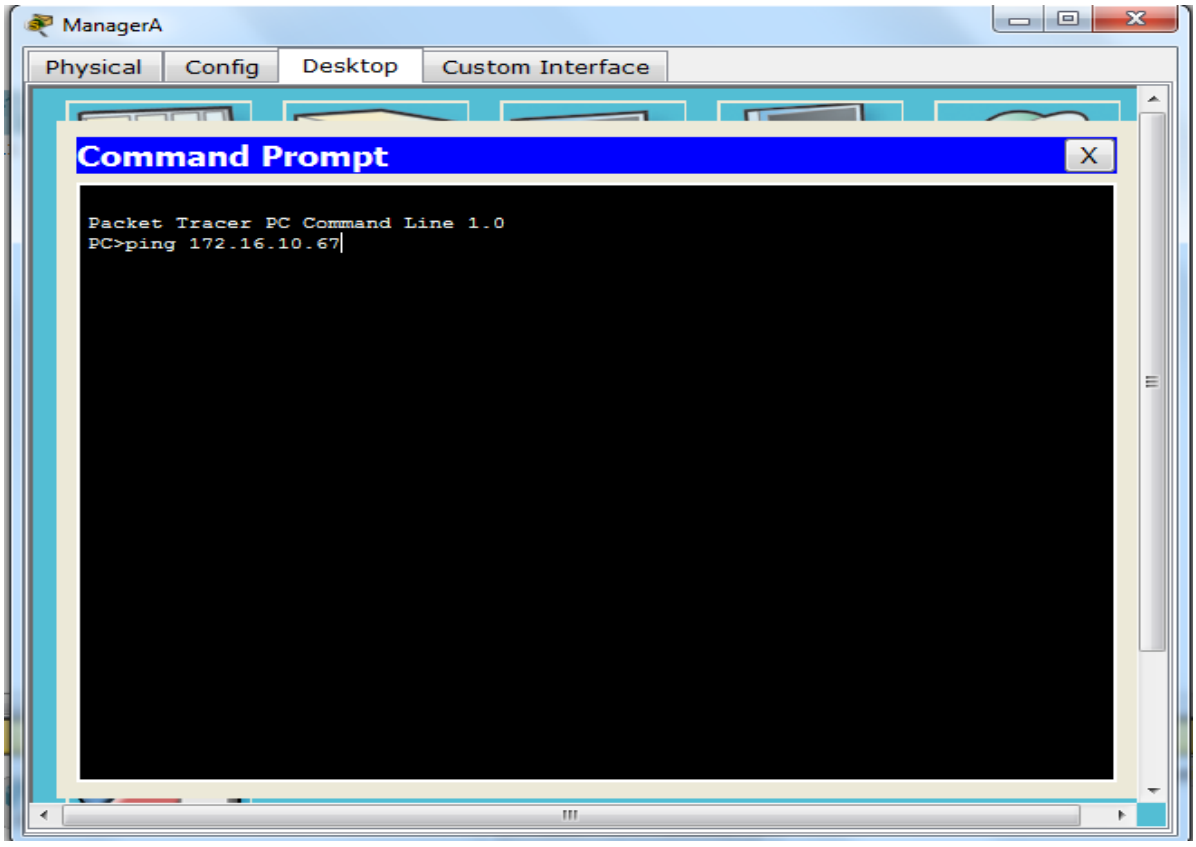


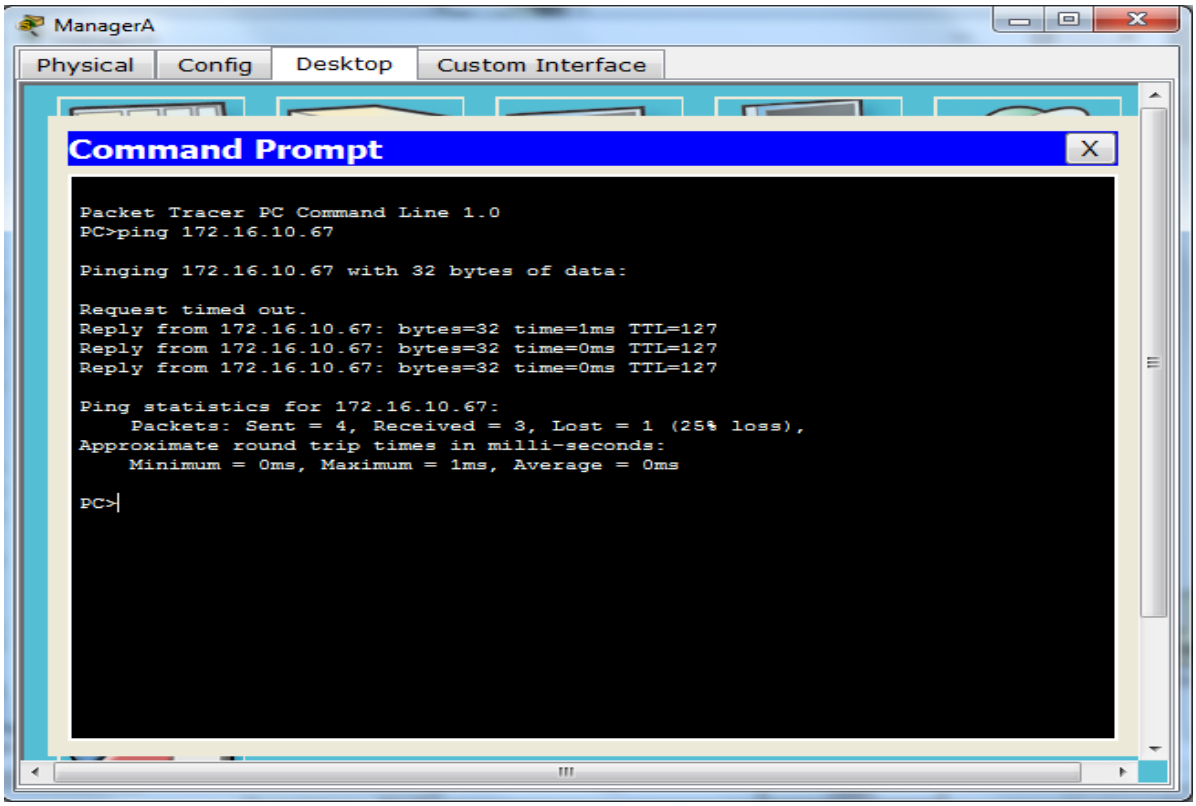






· Verifique la conectividad. Todos los clientes deben poder hacerse ping entre sí y acceder a los sitios Web en **Accounting.pka** y **Website.pka**.


ManagerA
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.10.67


ManagerA
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 172.16.10.67
Pinging 172.16.10.67 with 32 bytes of data:
Request timed out.
Reply from 172.16.10.67: bytes=32 time=1ms TTL=127
Reply from 172.16.10.67: bytes=32 time=0ms TTL=127
Reply from 172.16.10.67: bytes=32 time=0ms TTL=127
Ping statistics for 172.16.10.67:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>

9.1.4.6 Subnetting Scenario 1 Instructions IG

Packet Tracer: Situación de división en subredes 1

Topología

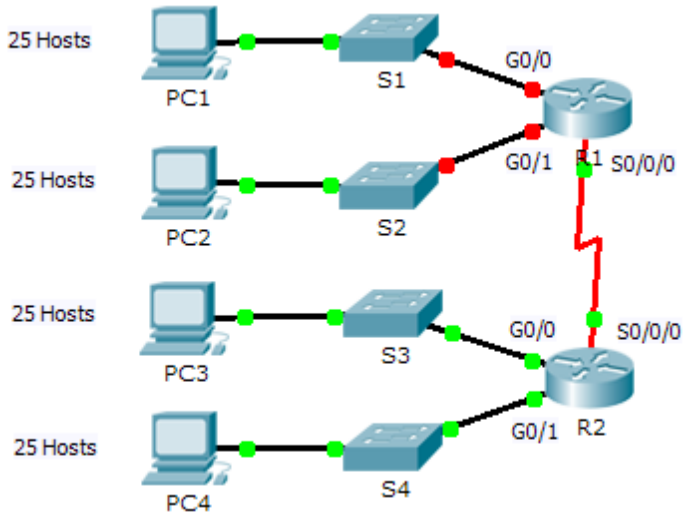


Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.100.1	255.255.255.224	No aplicable
	G0/1	192.168.100.33	255.255.255.224	No aplicable
	S0/0/0	192.168.100.129	255.255.255.224	No aplicable
R2	G0/0	192.168.100.65	255.255.255.224	No aplicable
	G0/1	192.168.100.97	255.255.255.224	No aplicable
	S0/0/0	192.168.100.158	255.255.255.224	No aplicable
S1	VLAN 1	192.168.100.2	255.255.255.224	192.168.100.1

S2	VLAN 1	192.168.100.34	255.255.255.224	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.224	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.224	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.224	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.224	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.224	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.224	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?

Rta: son necesarias 5 subredes

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

Rta: se toma prestados 3 bits admitir la cantidad de subredes en la tabla de topología.

c. ¿Cuántas subredes se crean?

Rta: se crean 8 subredes

d. ¿Cuántos hosts utilizables se crean por subred?

Rta: se crean 30 hosts utilizables por subred

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.

Numero de subred	**Dirección de subred**	**Primera dirección de host utilizable**	**Ultima dirección de host utilizable**	**Dirección bradcast**
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

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:
Rta: 192.168.100.0 /27

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

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.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.100.1	255.255.255.224	No aplicable
	G0/1	192.168.100.33	255.255.255.224	No aplicable
	S0/0/0	192.168.100.129	255.255.255.224	No aplicable

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

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R2	G0/0	192.168.100.65	255.255.255.224	No aplicable
	G0/1	192.168.100.97	255.255.255.224	No aplicable
	S0/0/0	192.168.100.158	255.255.255.224	No aplicable

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

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
S1	VLAN 1	192.168.100.2	255.255.255.224	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.224	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.224	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.224	192.168.100.97

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

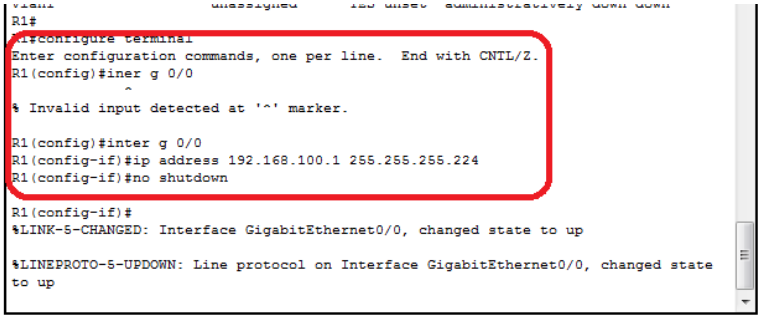
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
PC1	NIC	192.168.100.30	255.255.255.224	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.224	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.224	192.168.100.65

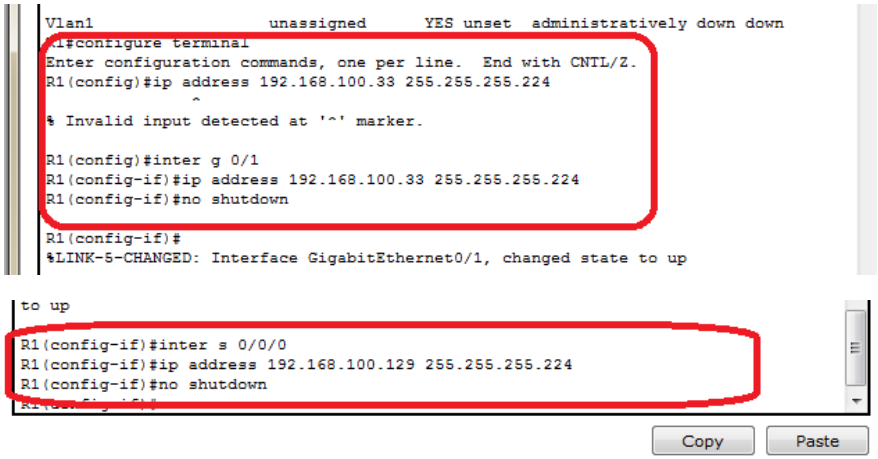
PC4	NIC	192.168.100.126	255.255.255.224	192.168.100.97

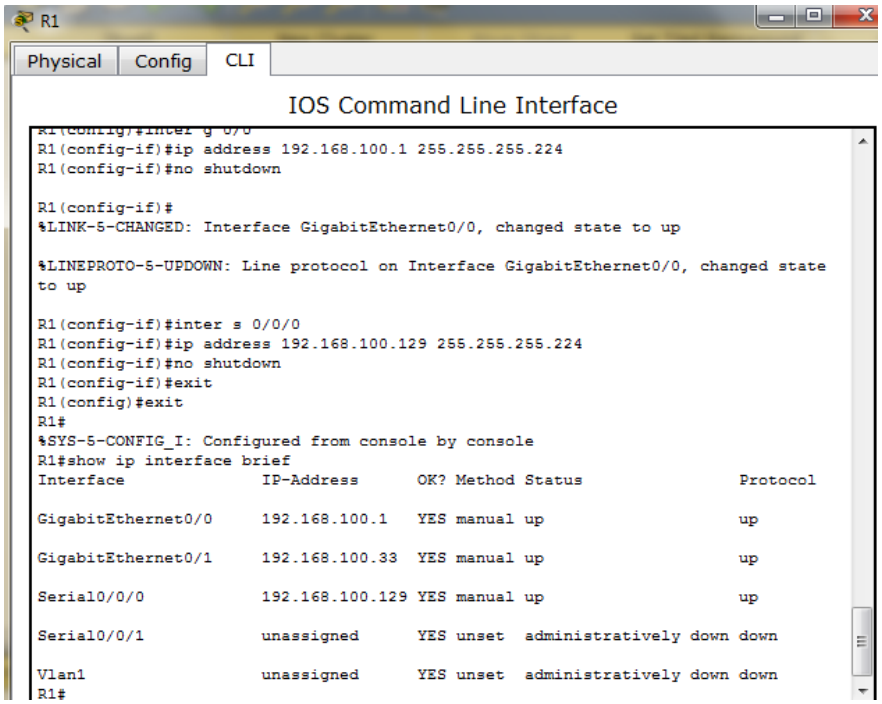
Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

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

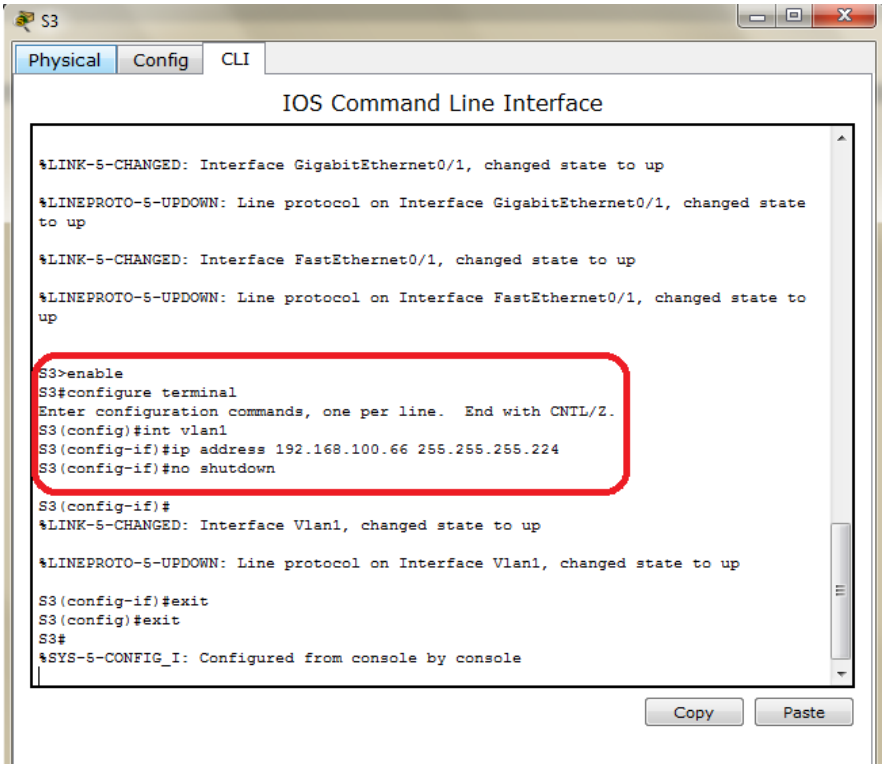
Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1



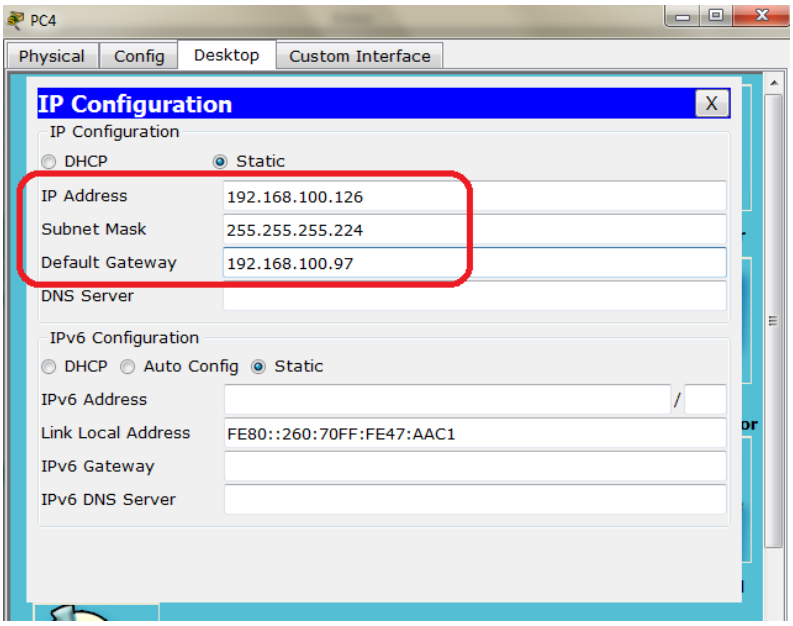




Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

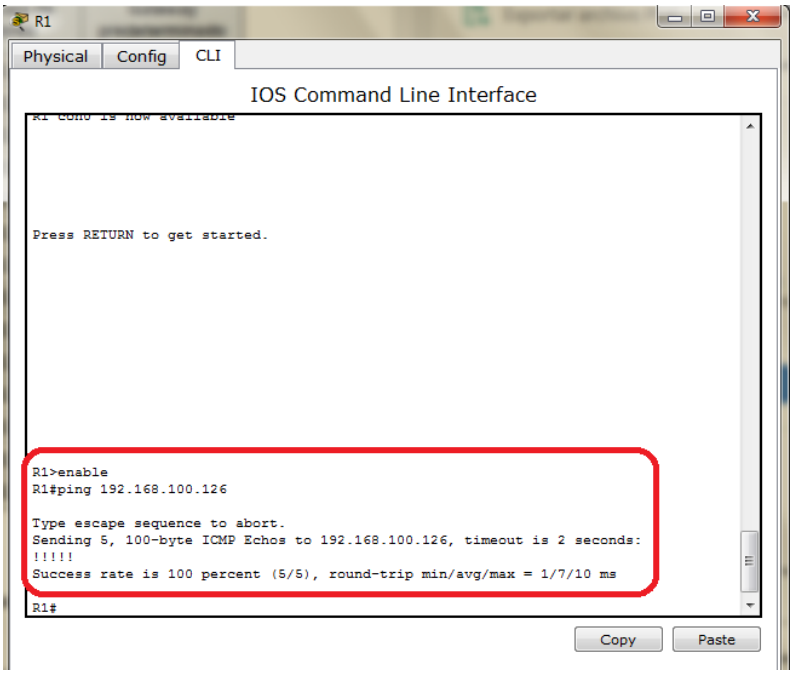


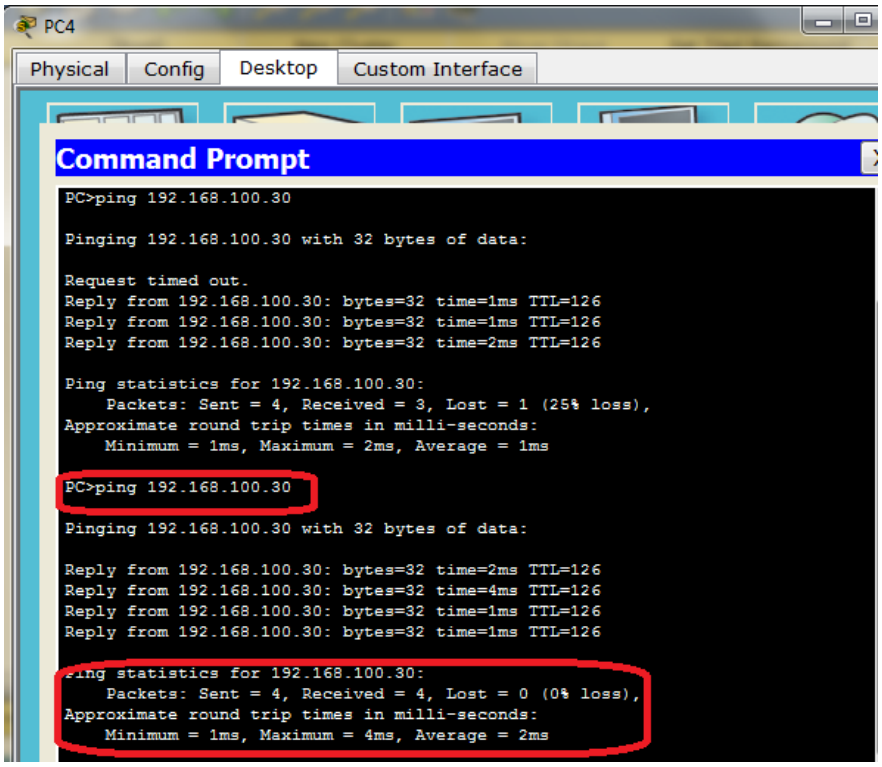
Paso 3: Configure el direccionamiento IP en PC4, incluido el gateway predeterminado.



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**.




PC4
Physical
Config
Desktop
Custom Interface
Command Prompt
PC>ping 192.168.100.30
Pinging 192.168.100.30 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.30: bytes=32 time=1ms TTL=126
Reply from 192.168.100.30: bytes=32 time=1ms TTL=126
Reply from 192.168.100.30: bytes=32 time=2ms TTL=126
Ping statistics for 192.168.100.30:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>ping 192.168.100.30
Pinging 192.168.100.30 with 32 bytes of data:
Reply from 192.168.100.30: bytes=32 time=2ms TTL=126
Reply from 192.168.100.30: bytes=32 time=4ms TTL=126
Reply from 192.168.100.30: bytes=32 time=1ms TTL=126
Reply from 192.168.100.30: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.100.30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 2ms

9.1.4.7 Subnetting Scenario 2 Instructions IG

Packet Tracer: Situación de división en subredes 2

Topología

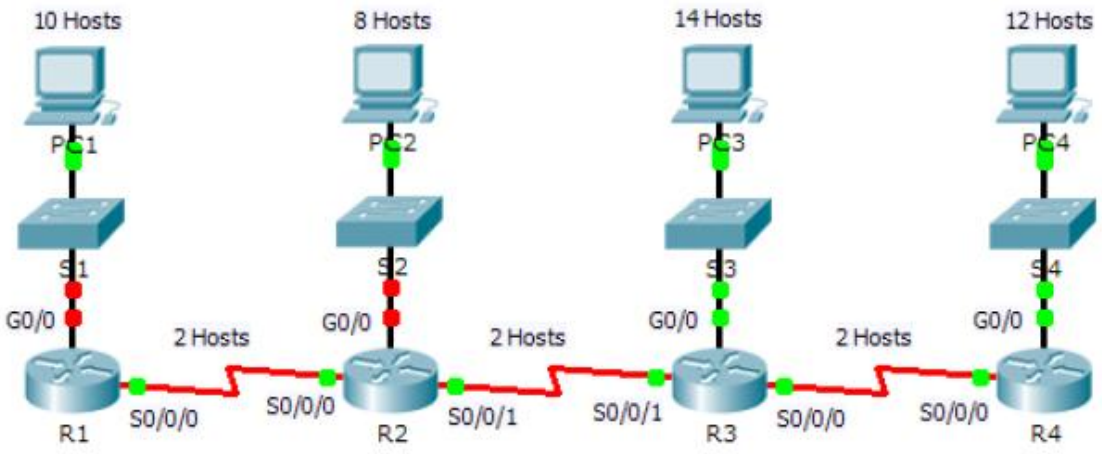


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0			No aplicable
	S0/0/0			No aplicable
R2	G0/0			No aplicable
	S0/0/0			No aplicable
	S0/0/1			No aplicable
R3	G0/0			No aplicable
	S0/0/0			No aplicable
	S0/0/1			No aplicable
R4	G0/0			No aplicable
	S0/0/0			No aplicable
S1	VLAN 1			
S2	VLAN 1			

S3	VLAN 1			
S4	VLAN 1			
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			

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? 7

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

c. ¿Cuántas subredes se crean? 16 subredes

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

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

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

Red 0: 172. 31 . 1 . 0 0 0 0 0 0 0 0

Red 1: 172. 31 . 1 . 0 0 0 1 0 0 0 0

Red 2: 172. 31 . 1 . 0 0 1 0 0 0 0 0

Red 3: 172. 31 . 1 . 0 0 1 1 0 0 0 0

Red 4: 172. 31 . 1 . 0 1 0 0 0 0 0 0

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

11111111.11111111.11111111. 11110000

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	172.31.1.0/28	172.31.1.1/28	172.31.1.14/28	172.16.1.15/28
1	172.31.1.16/28	172.31.1.17/28	172.31.1.30/28	172.16.1.31/28
2	172.31.1.32/28	172.31.1.33/28	172.31.1.46/28	172.16.1.47/28
3	172.31.1.48/28	172.31.1.49/28	172.31.1.62/28	172.16.1.63/28
4	172.31.1.64/28	172.31.1.65/28	172.31.1.78/28	172.16.1.79/28
5	172.31.1.80/28	172.31.1.81/28	172.31.1.94/28	172.16.1.95/28
6	172.31.1.96/28	172.31.1.97/28	172.31.1.110/28	172.16.1.111/28

7	172.31.1.112/28	172.31.1.113/28	172.31.1.126/28	172.16.1.27/28
8	172.31.1.128/28	172.31.1.129/28	172.31.1.142/28	172.16.1.143/28
9	172.31.1.144/28	172.31.1.145/28	172.31.1.158/28	172.16.1.159/28
10	172.31.1.160/28	172.31.1.161/28	172.31.1.174/28	172.16.1.175/28
11	172.31.1.176/28	172.31.1.177/28	172.31.1.190/28	172.16.1.191/28
12	172.31.1.192/28	172.31.1.193/28	172.31.1.206/28	172.16.1.207/28
13	172.31.1.208/28	172.31.1.209/28	172.31.1.222/28	172.16.1.223/28
14	172.31.1.224/28	172.31.1.225/28	172.31.1.238/28	172.16.1.239/28
15	172.31.1.240/28	172.31.1.241/28	172.31.1.254/28	172.16.1.255/28

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.

a. Asigne la subred 0 a la LAN de R1.

b. Asigne la subred 1 a la LAN de R2.

c. Asigne la subred 2 a la LAN de R3.

d. Asigne la subred 3 a la LAN de R4.

e. Asigne la subred 4 al enlace entre

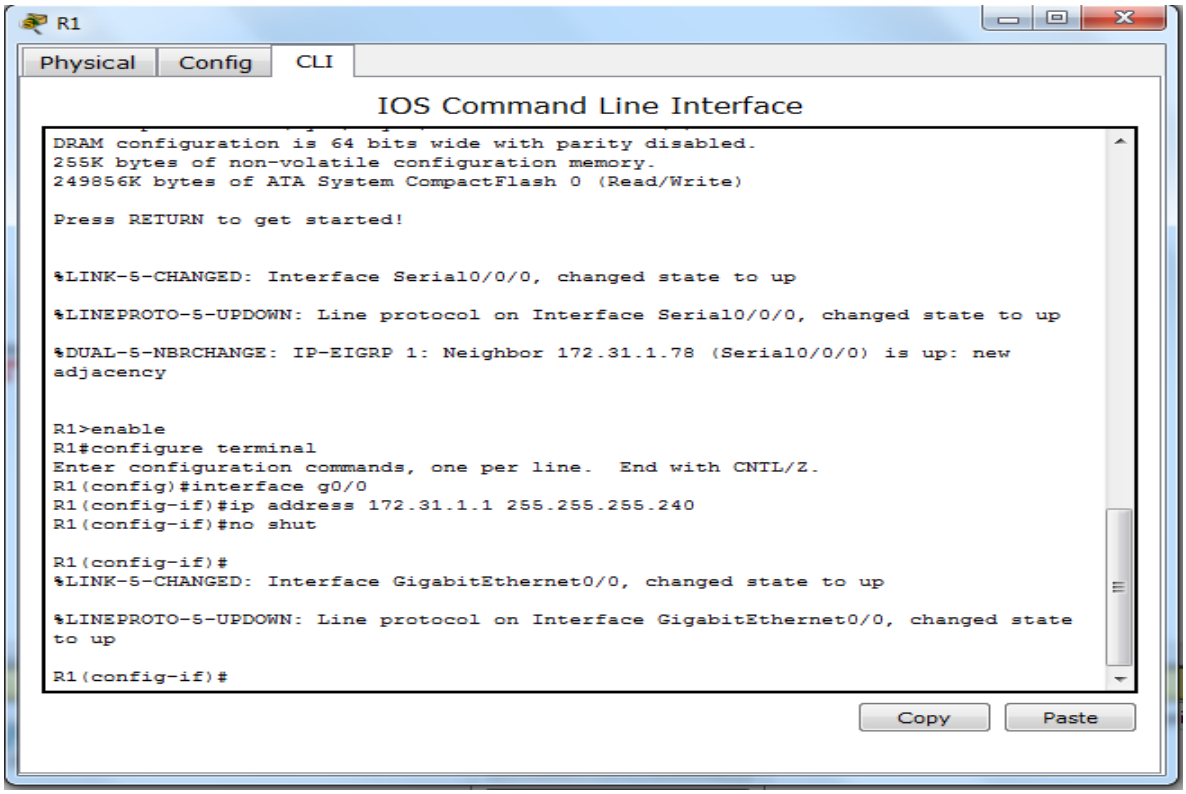
f. Asigne la subred 5 al enlace entre

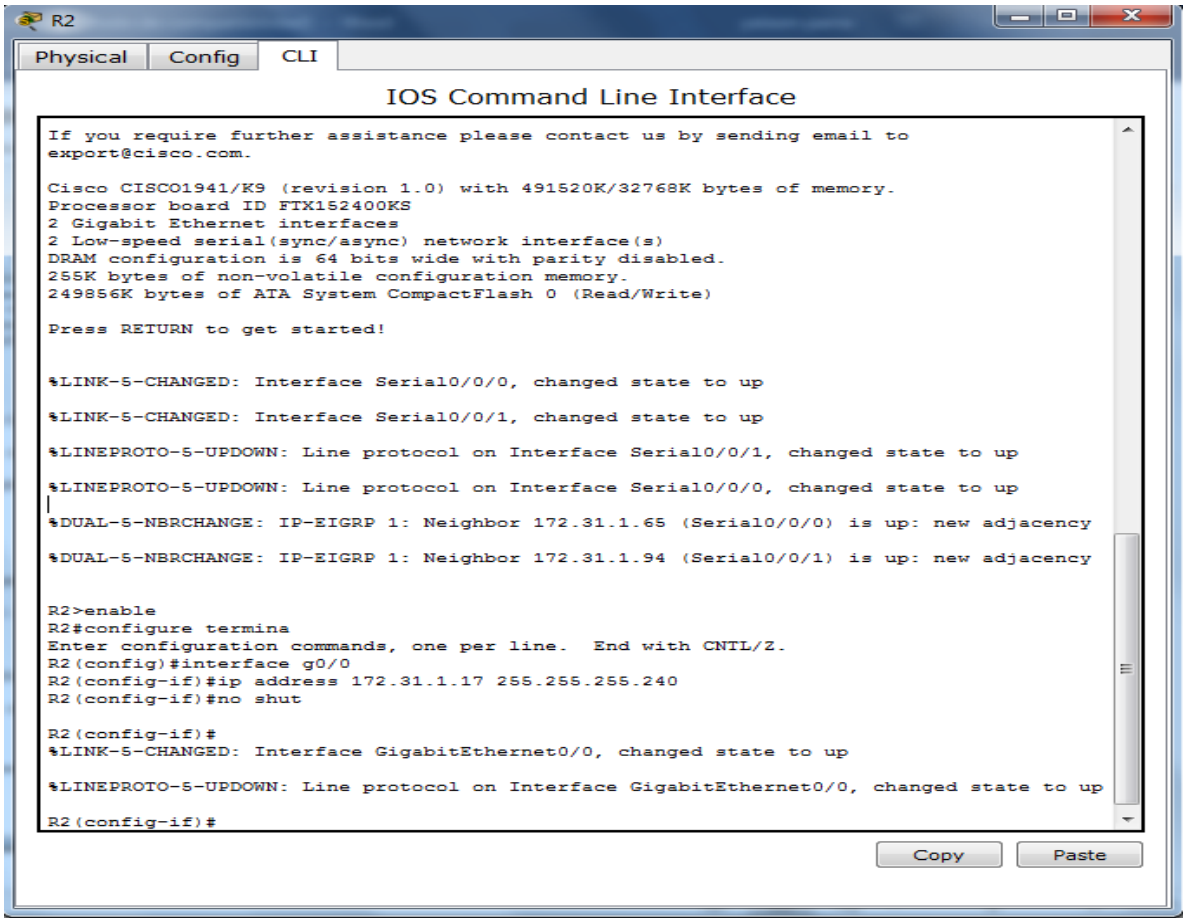
g. Asigne la subred 6 al enlace entre

Paso 3: Documente el esquema de direccionamiento.

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

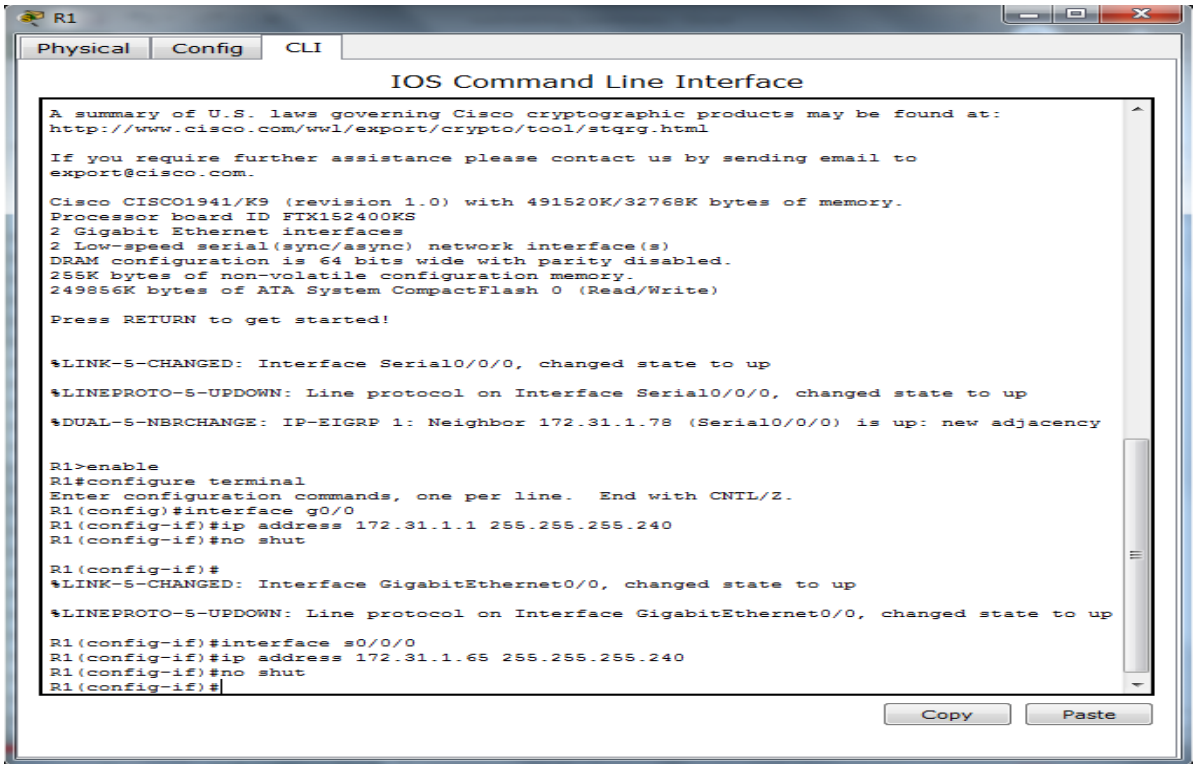
a. Asigne las primeras direcciones IP utilizables a los routers para cada uno de los enlaces LAN.

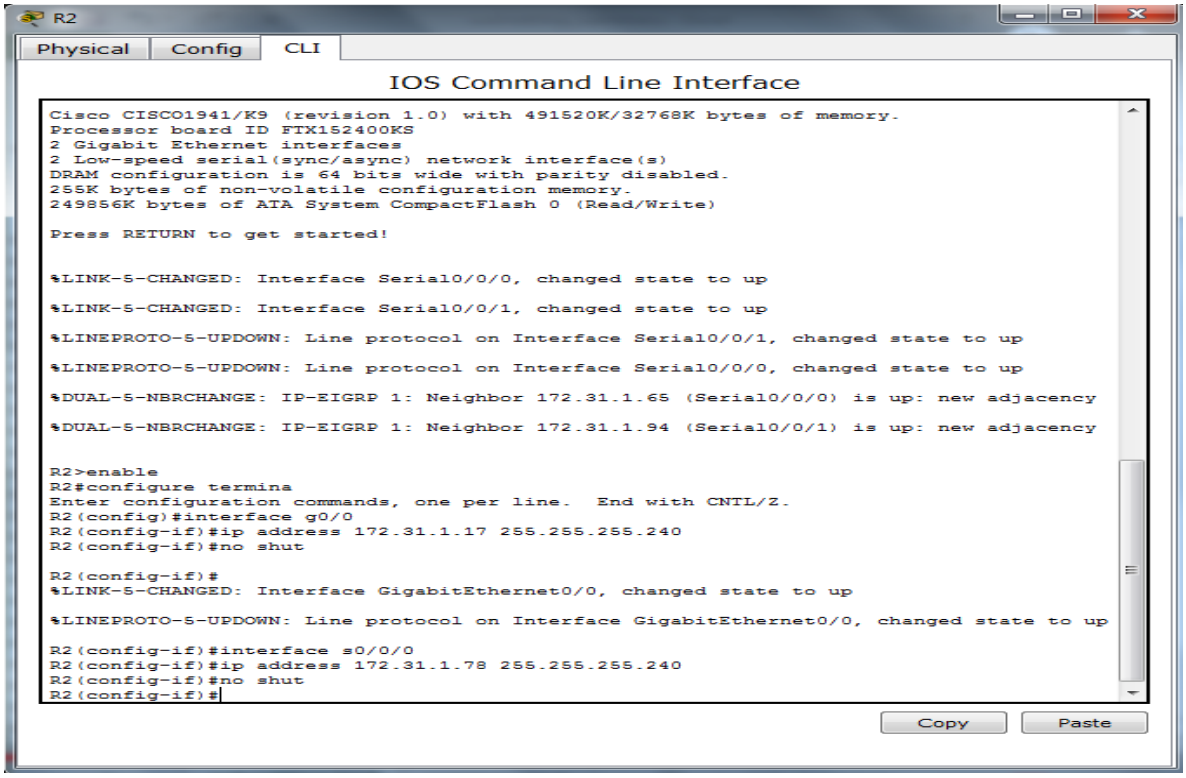

R1
Physical
Config
CLI
IOS Command Line Interface
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.1.78 (Serial0/0/0) is up: new adjacency
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ip address 172.31.1.1 255.255.255.240
R1(config-if)#no shut
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)#
Copy
Paste


R2
Physical
Config
CLI
IOS Command Line Interface
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.1.65 (Serial0/0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.31.1.94 (Serial0/0/1) is up: new adjacency
R2>enable
R2#configure termina
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)#
Copy
Paste

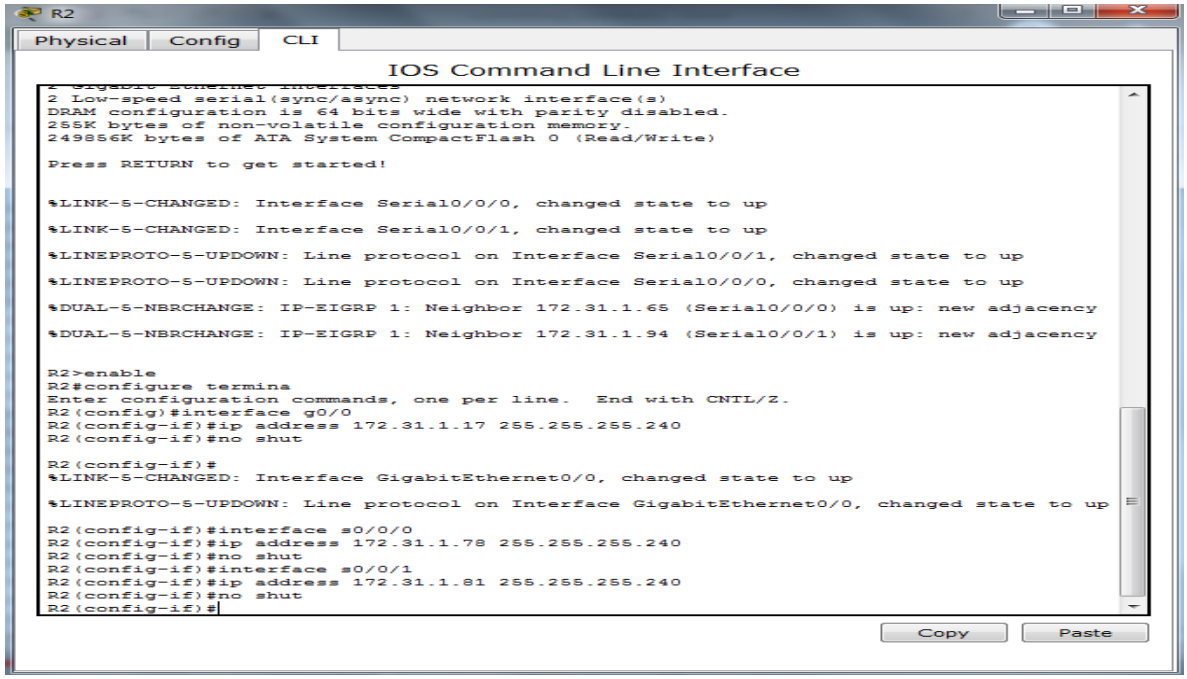
b. Utilice el siguiente método para asignar las direcciones IP de los enlaces WAN:

- 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.



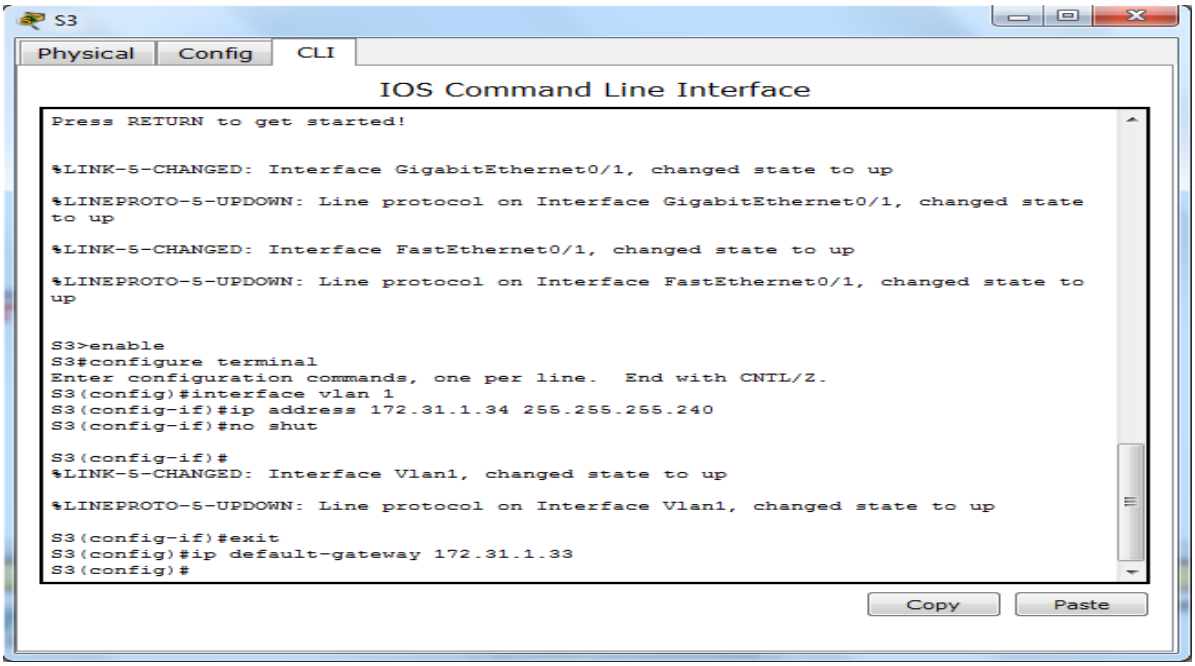


- Para el enlace WAN entre el R2 y el R3, asigne la primera dirección IP utilizable al R2 y la última dirección IP utilizable al R3.

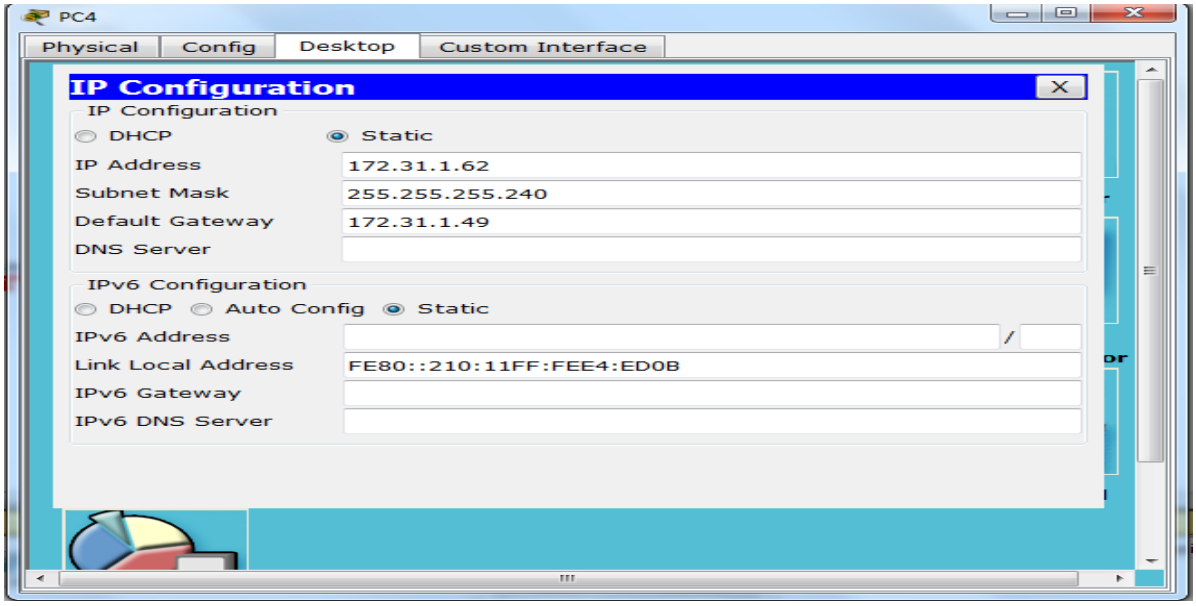


  - Para el enlace WAN entre el R3 y el R4, asigne la primera dirección IP utilizable al R3 y la última dirección IP utilizable al R4.

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



d. 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.

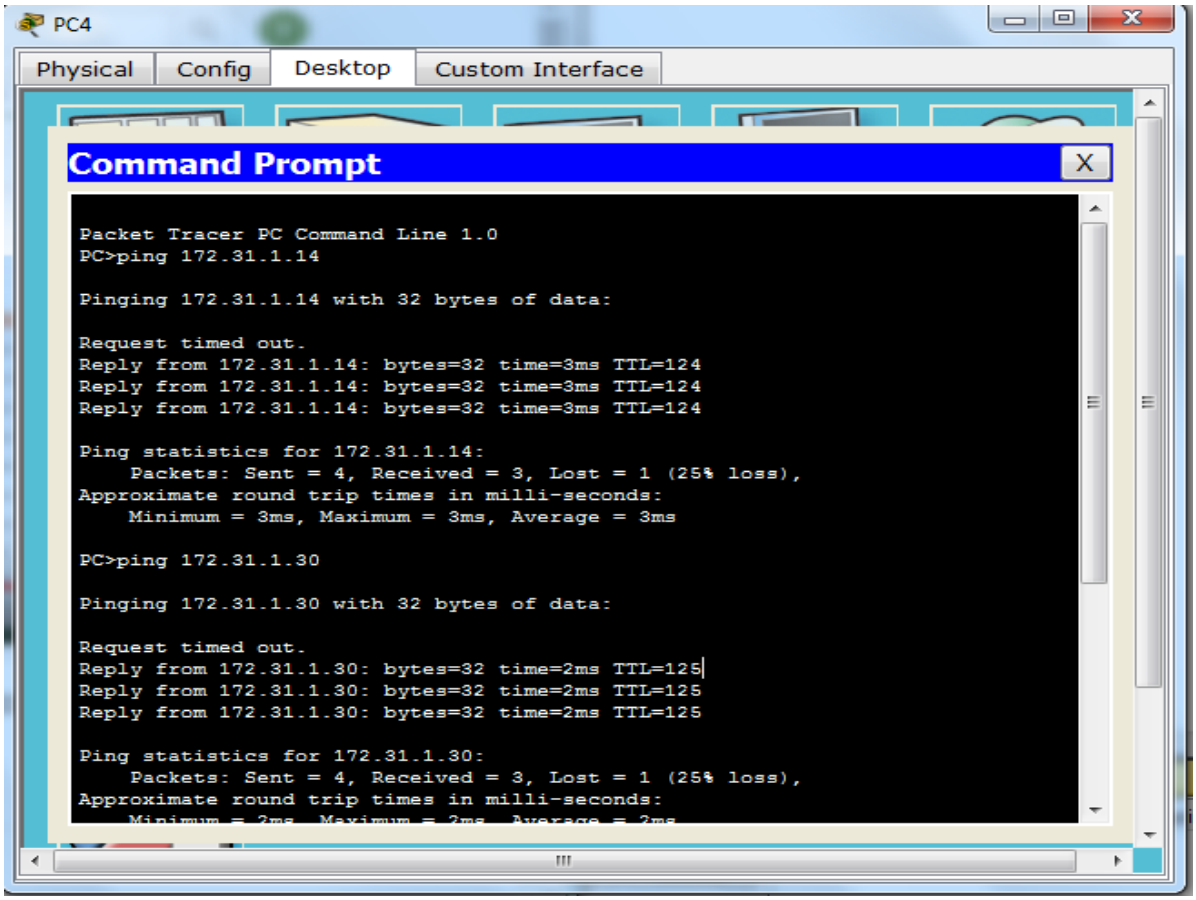
Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1 y el R2

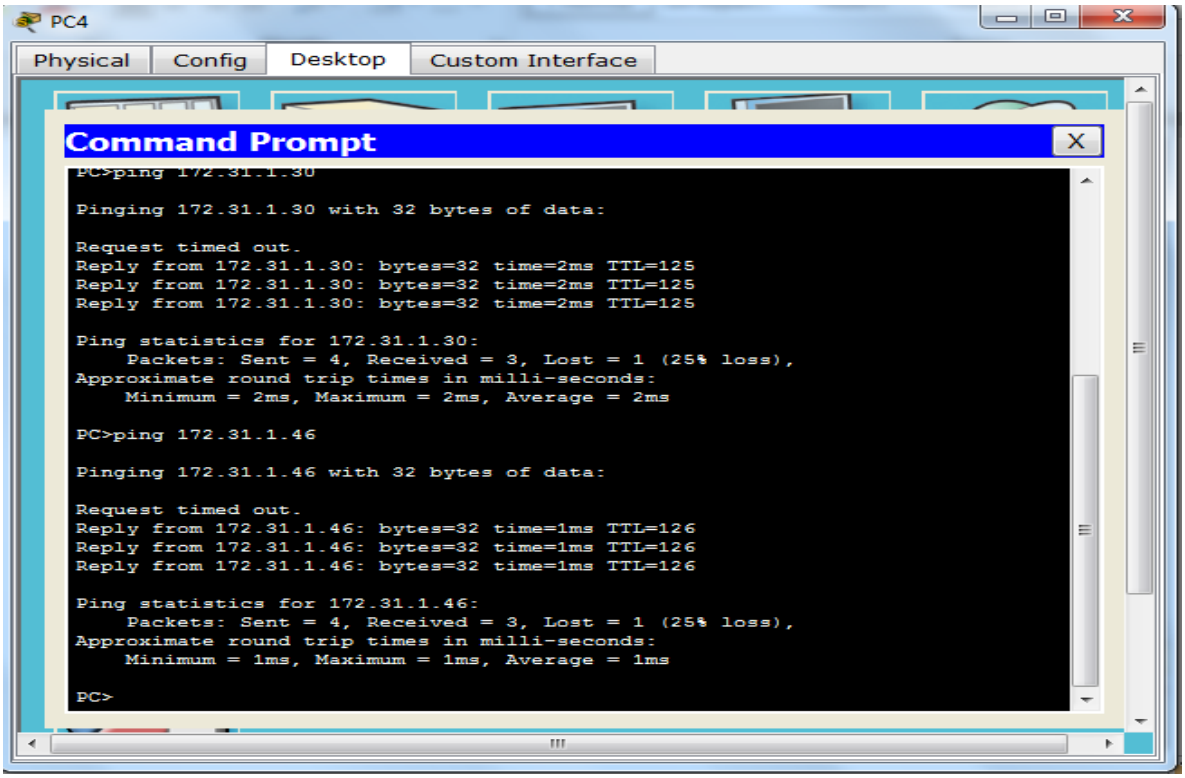
Paso 2: Configure el direccionamiento IP en S3, incluido el gateway predeterminado.

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

Paso 4: Verificar 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**.


PC4
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 172.31.1.14
Pinging 172.31.1.14 with 32 bytes of data:
Request timed out.
Reply from 172.31.1.14: bytes=32 time=3ms TTL=124
Reply from 172.31.1.14: bytes=32 time=3ms TTL=124
Reply from 172.31.1.14: bytes=32 time=3ms TTL=124
Ping statistics for 172.31.1.14:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 3ms, Average = 3ms
PC>ping 172.31.1.30
Pinging 172.31.1.30 with 32 bytes of data:
Request timed out.
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Ping statistics for 172.31.1.30:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:


PC4
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 172.31.1.30
Pinging 172.31.1.30 with 32 bytes of data:
Request timed out.
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Reply from 172.31.1.30: bytes=32 time=2ms TTL=125
Ping statistics for 172.31.1.30:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms
PC>ping 172.31.1.46
Pinging 172.31.1.46 with 32 bytes of data:
Request timed out.
Reply from 172.31.1.46: bytes=32 time=1ms TTL=126
Reply from 172.31.1.46: bytes=32 time=1ms TTL=126
Reply from 172.31.1.46: bytes=32 time=1ms TTL=126
Ping statistics for 172.31.1.46:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
PC>

9.2.1.5 Designing and Implementing a VLSM Addressing Scheme Instruct IG

Packet Tracer: diseño e implementación de un esquema de direccionamiento VLSM

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Building1	G0/0	192.168.72.129	255.255.255.240	No aplicable
	G0/1	192.168.72.97	255.255.255.224	No aplicable
	S0/0/0	192.168.72.145	255.255.255.252	No aplicable
Building2	G0/0	192.168.72.65	255.255.255.224	No aplicable
	G0/1	192.168.72.1	255.255.255.192	No aplicable
	S0/0/0	192.168.72.146	255.255.255.252	No aplicable
ASW-1	VLAN 1	192.168.72.130	255.255.255.240	192.168.72.129
ASW-2	VLAN 1	192.168.72.98	255.255.255.224	192.168.72.97
ASW-3	VLAN 1	192.168.72.66	255.255.255.224	192.168.72.65
ASW-4	VLAN 1	192.168.72.2	255.255.255.192	192.168.72.1
Host-A	NIC	192.168.72.142	255.255.255.240	192.168.72.129
Host-B	NIC	192.168.72.126	255.255.255.224	192.168.72.97
Host-C	NIC	192.168.72.94	255.255.255.224	192.168.72.65
Host-D	NIC	192.168.72.62	255.255.255.192	192.168.72.1

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

Parte 1: examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias.

Dividirá la dirección de red 192.168.72.0/24 en subredes. La red tiene los siguientes requisitos:

- La LAN de **ASW-1** requerirá **7** direcciones IP de host.
- La LAN de **ASW-2** requerirá **15** direcciones IP de host.
- La LAN de **ASW-3** requerirá **29** direcciones IP de host.
- La LAN de **ASW-4** requerirá **58** direcciones IP de host.

¿Cuántas subredes se necesitan en la topología de la red?

Respuesta: 5 Sudredes.

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 **ASW-1**?

   - 255.255.255.240

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

   - Desde la 192.168.72.129 hasta la 192.168.72.142

b. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **ASW-2**?

   - 255.255.255.224

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

   - Desde la 192.168.72.97 hasta la 192.168.72.126

c. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **ASW-3**?

   - 255.255.255.224

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

   - Desde la 192.168.72.65 hasta la 192.168.72.94

d. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **ASW-4**?

   - 255.255.255.192

   ¿Cuántas direcciones de host utilizables admitirá esta subred?

   - Desde la 192.168.72.1 hasta la 192.168.72.62

e. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para la conexión entre **Building1** y**Building2**?

   - 255.255.255.252

Parte 2: diseñar el esquema de direccionamiento VLSM

Paso 1: Dividir la red 192.168.72.0/24 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 **Building1** y **Building2**.

Paso 2: Registrar las subredes VLSM.

Complete la **tabla de subredes** con las descripciones de las subred (p. ej., LAN de ASW-1), 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.

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Dirección de broadcast
ASW-4	58	192.168.72.0/26	192.168.72.1	192.168.72.63
ASW-3	29	192.168.72.64/27	192.168.72.65	192.168.72.95
ASW-2	15	192.168.72.96/27	192.168.72.97	192.168.72.127
ASW-1	7	192.168.72.128/28	192.168.72.129	192.168.72.143
Enlace WAN	2	192.168.72.144/30	192.168.72.145	192.168.72.147

Paso 3: Documente el esquema de direccionamiento.

a. Asigne las primeras direcciones IP utilizables a **Building1** para los dos enlaces LAN y el enlace WAN.

b. Asigne las primeras direcciones IP utilizables a **Building2** 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.

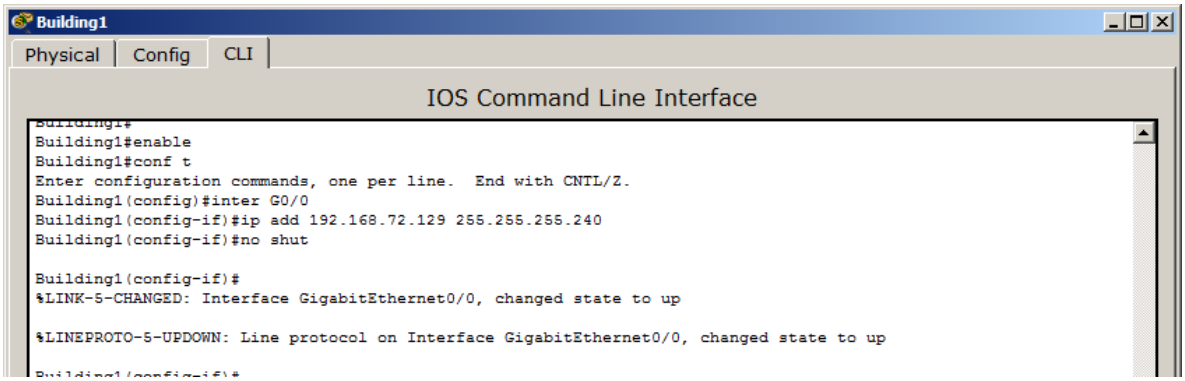
d. Asigne las últimas direcciones IP utilizables a los hosts.

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

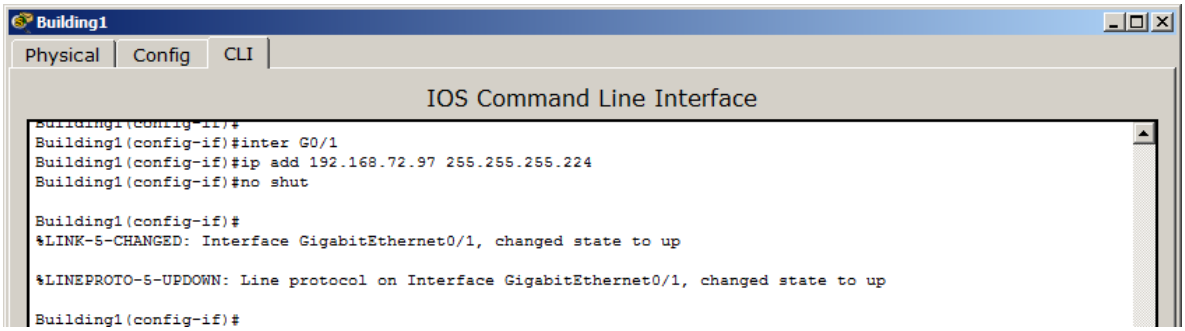
La mayor parte del direccionamiento IP ya está configurado en esta red. Implemente los siguientes pasos para realizar la configuración de direccionamiento.

Paso 1: Configurar el direccionamiento IP en las interfaces LAN de Building1

G0/0

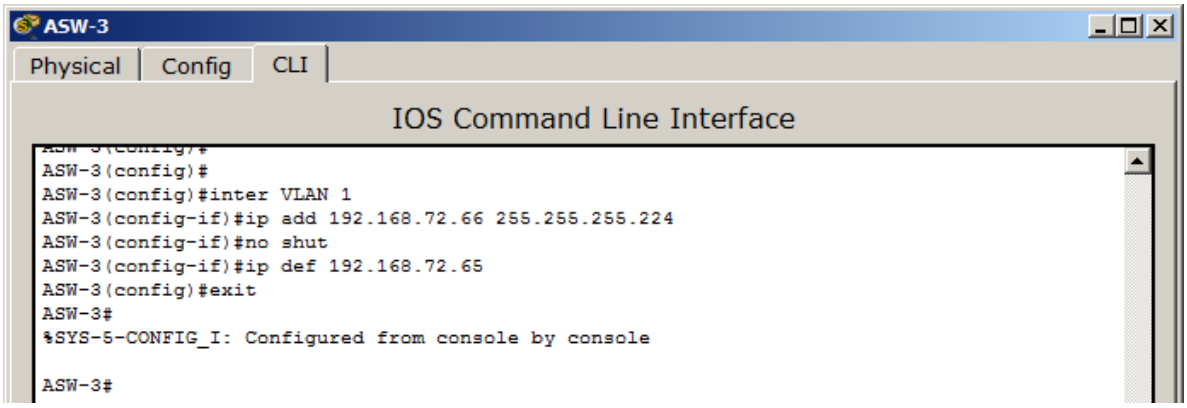


G0/1

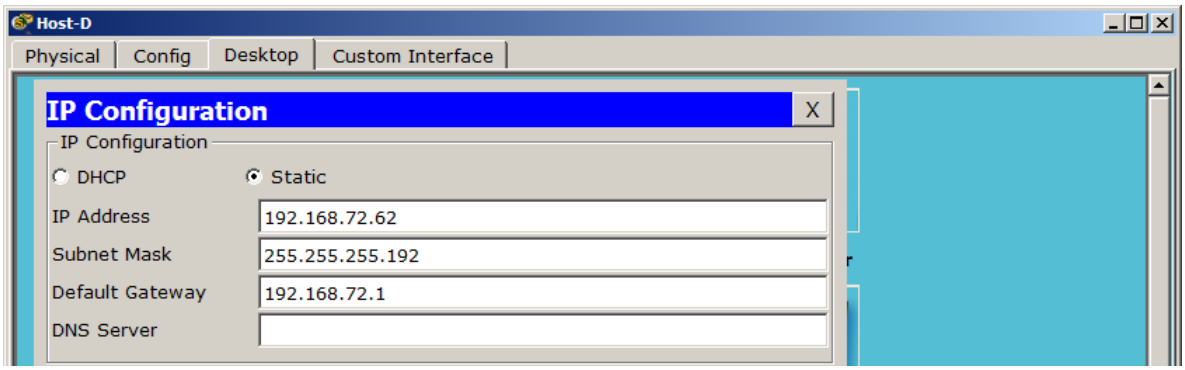


Paso 2: Configurar el direccionamiento IP en ASW-3, incluido el gateway predeterminado

VLAN 1



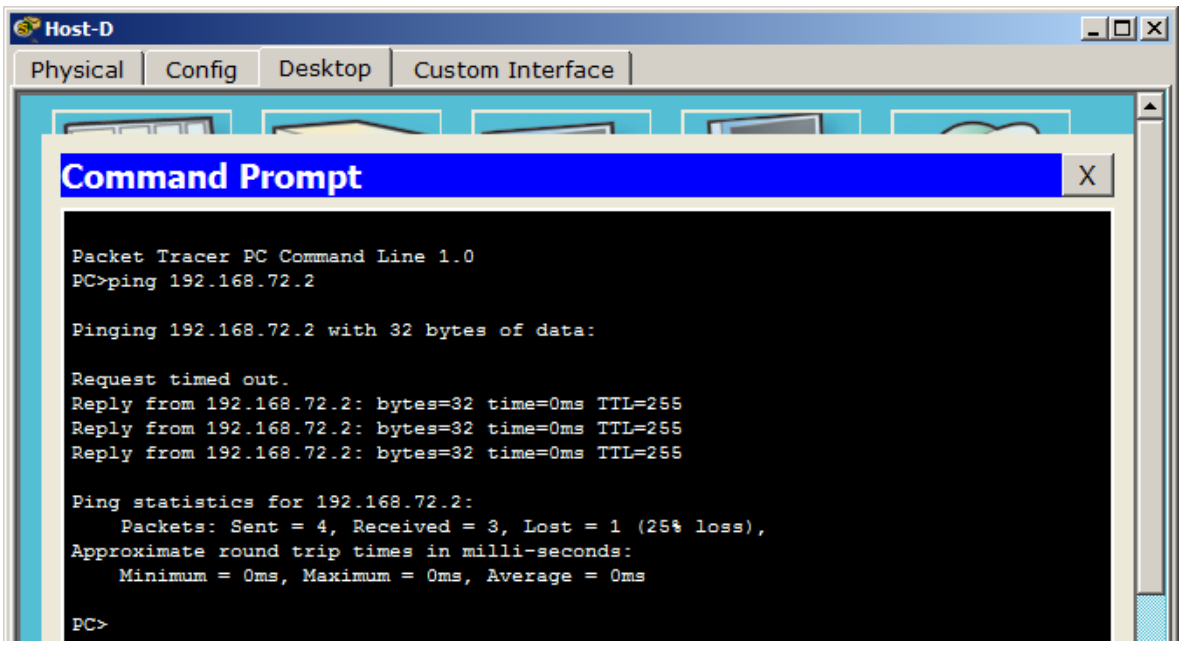
Paso 3: Configurar el direccionamiento IP en Host-D, incluido el gateway predeterminado

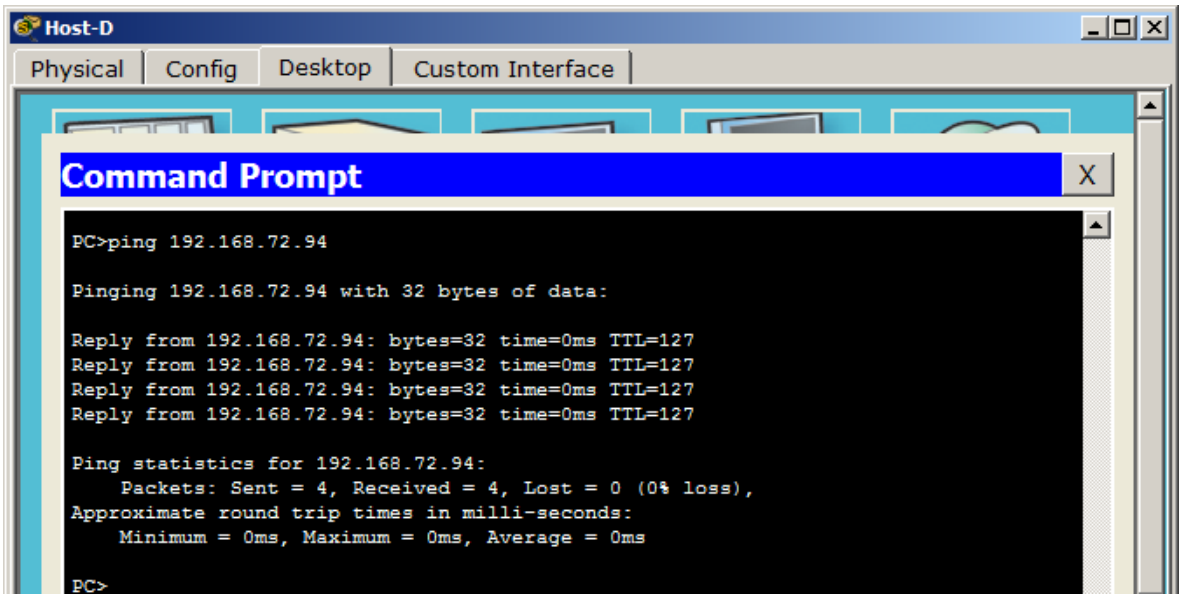


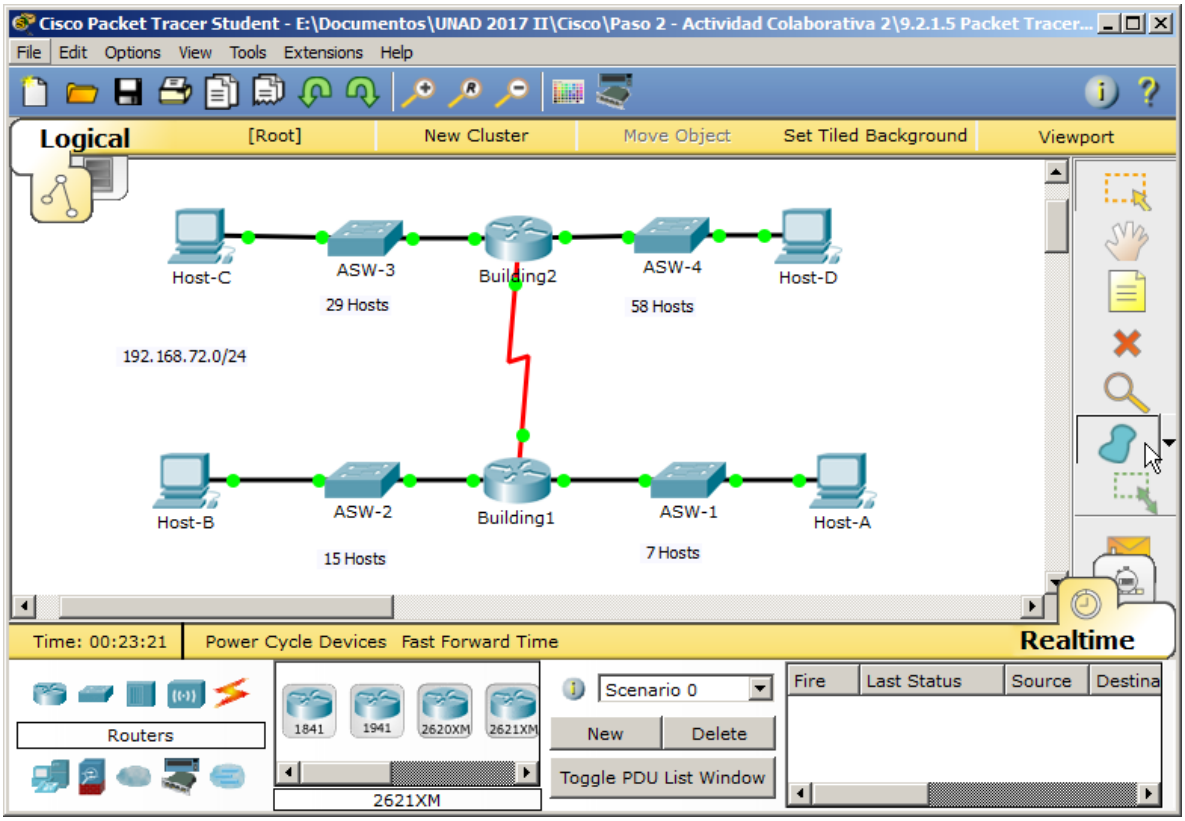
Paso 4: Verificar la conectividad.

Solo puede verificar la conectividad desde Building1, ASW-3 y Host-D. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

- Host-D




Host-D
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.72.94
Pinging 192.168.72.94 with 32 bytes of data:
Reply from 192.168.72.94: bytes=32 time=0ms TTL=127
Reply from 192.168.72.94: bytes=32 time=0ms TTL=127
Reply from 192.168.72.94: bytes=32 time=0ms TTL=127
Reply from 192.168.72.94: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.72.94:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>


Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 2 - Actividad Colaborativa 2\9.2.1.5 Packet Tracer...
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Host-C
ASW-3
29 Hosts
Building2
ASW-4
58 Hosts
Host-D
192.168.72.0/24
Host-B
ASW-2
15 Hosts
Building1
ASW-1
7 Hosts
Host-A
Time: 00:23:21
Power Cycle Devices
Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2621XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destina

9.3.1.4 Implementing a Subnetted IPv6 Addressing Scheme Instructions IG

Packet Tracer: Implementación de un esquema de direccionamiento IPv6 dividido en subredes

Topología

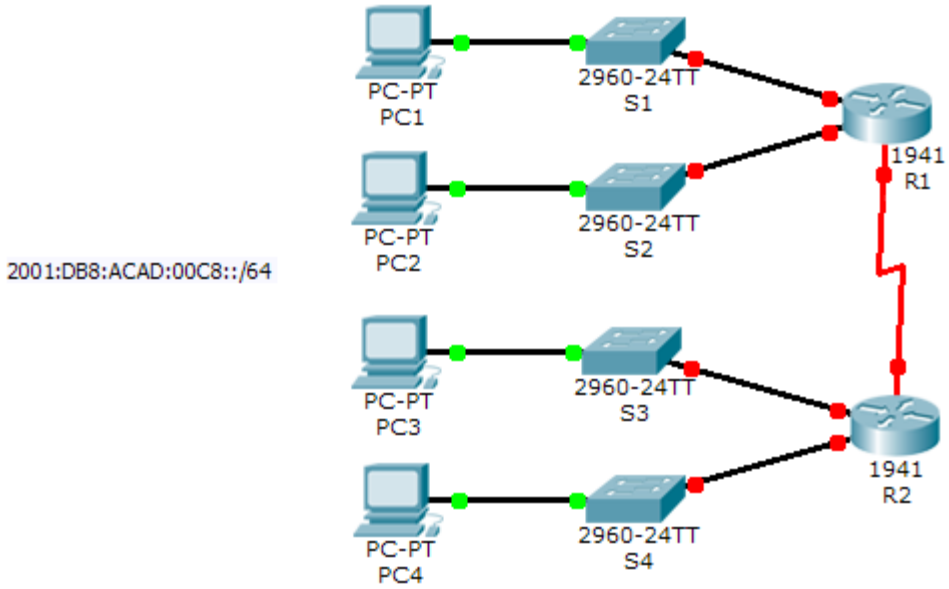


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Link-Local
R1	G0/0		FE80::1
	G0/1		FE80::1
	S0/0/0		FE80::1
R2	G0/0		FE80::2
	G0/1		FE80::2
	S0/0/0		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.

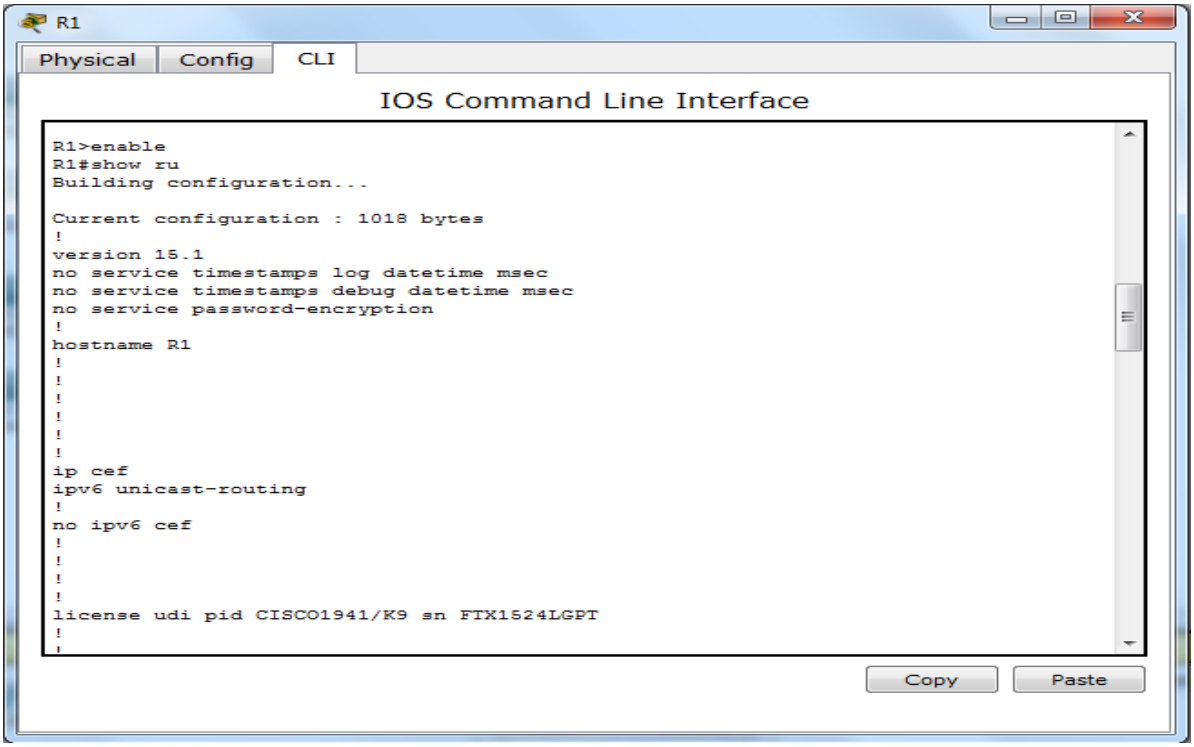
Comience con la subred IPv6 2001:DB:ACAD:00C8::/64 y asígnela a la LAN del R1 conectada a GigabitEthernet 0/0, como se muestra en la **tabla de subredes**. Para el resto de las subredes IPv6, incremente la dirección de la subred 2001:DB:ACAD:00C8::/64 de a 1 y complete la **tabla de subredes** con las direcciones de la subred IPv6.

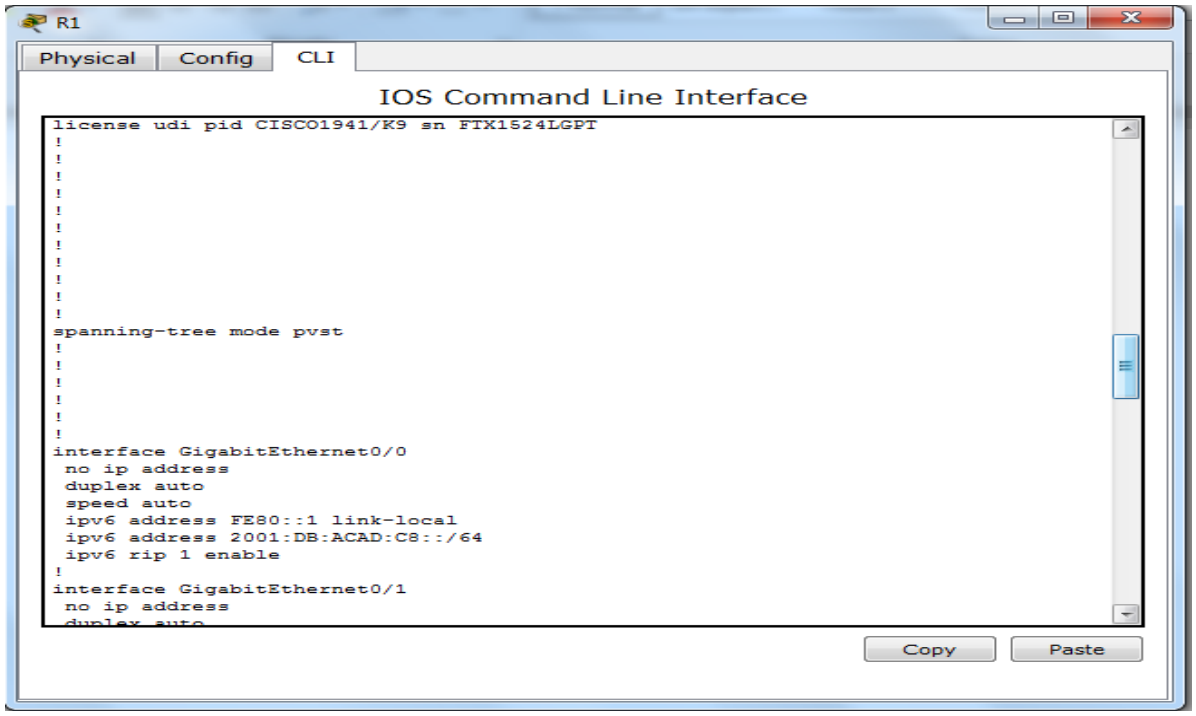
Tabla de subredes

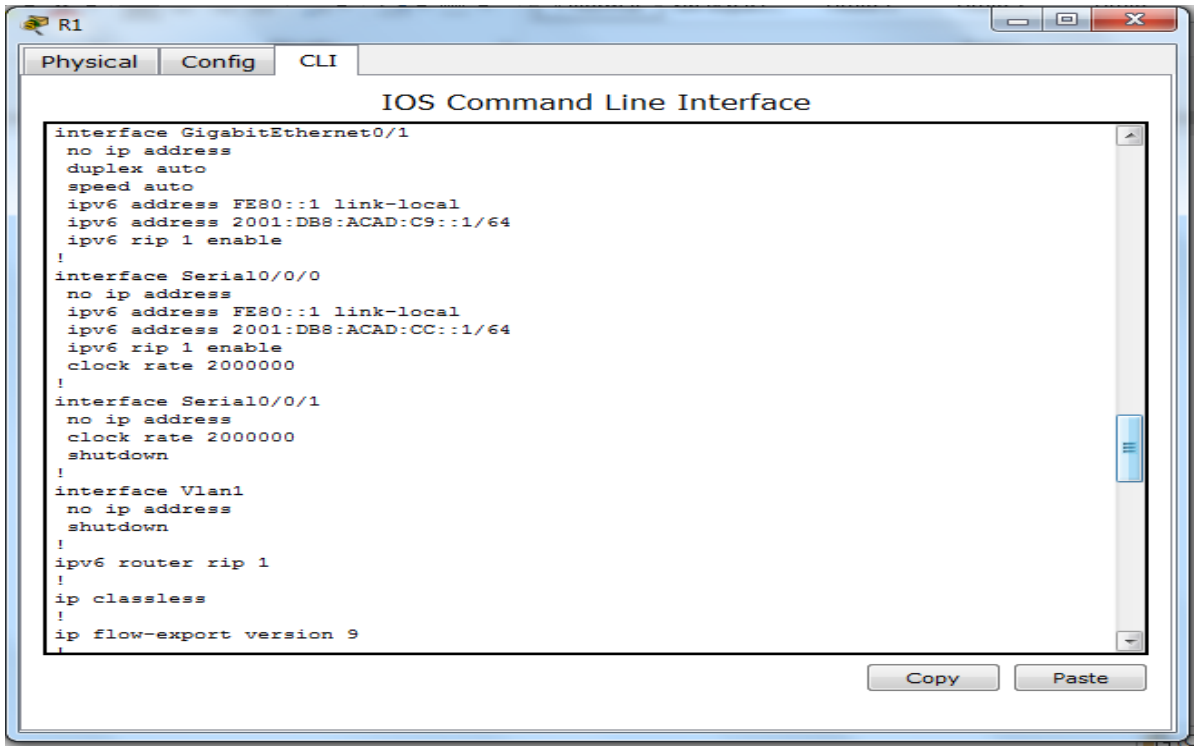
Descripción de la subred	Dirección de subred
R1 G0/0 LAN	2001:DB8:ACAD:00C8::1/64
R1 G0/1 LAN	2001:DB8:ACAD:00C9::1/64
R2 G0/0 LAN	2001:DB8:ACAD:00CA::2/64
R2 G0/1 LAN	2001:DB8:ACAD:00CB::2/64
Enlace WAN	2001:DB8:ACAD:00CC::

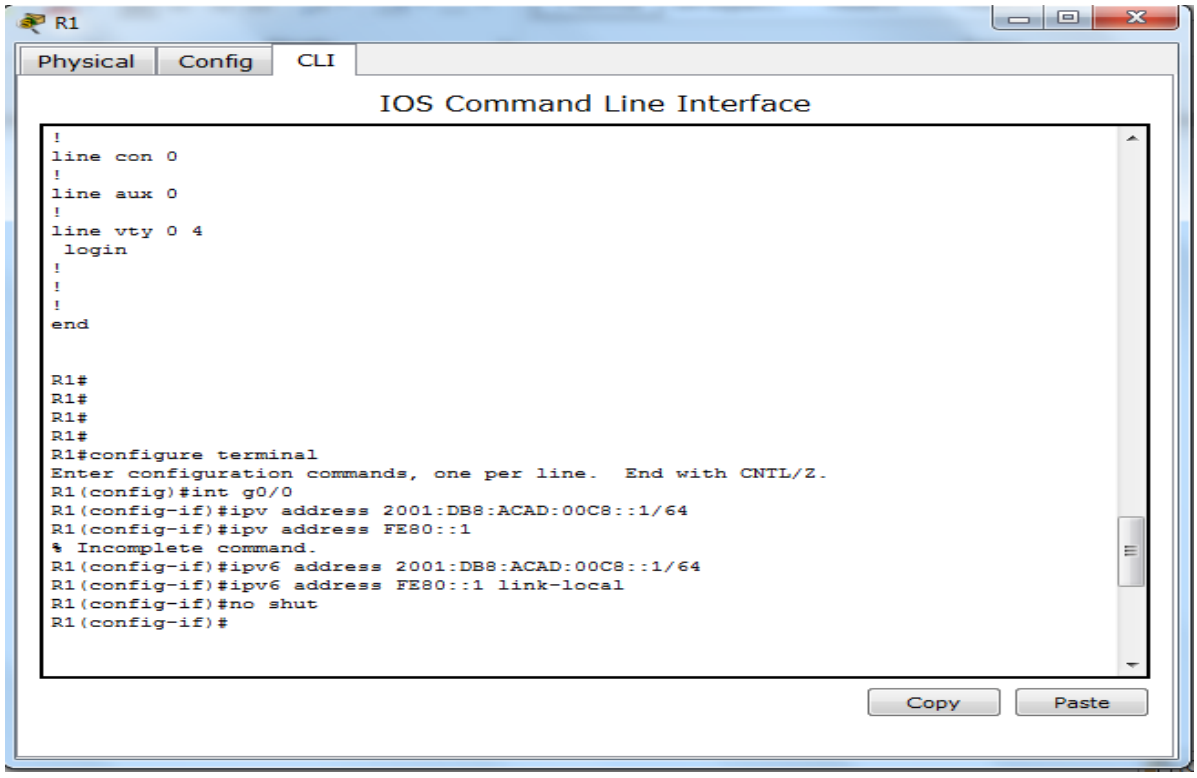
Paso 2: Asignar el direccionamiento IPv6 a los routers.

a. Asigne las primeras direcciones IPv6 al R1 para los dos enlaces LAN y el enlace WAN.

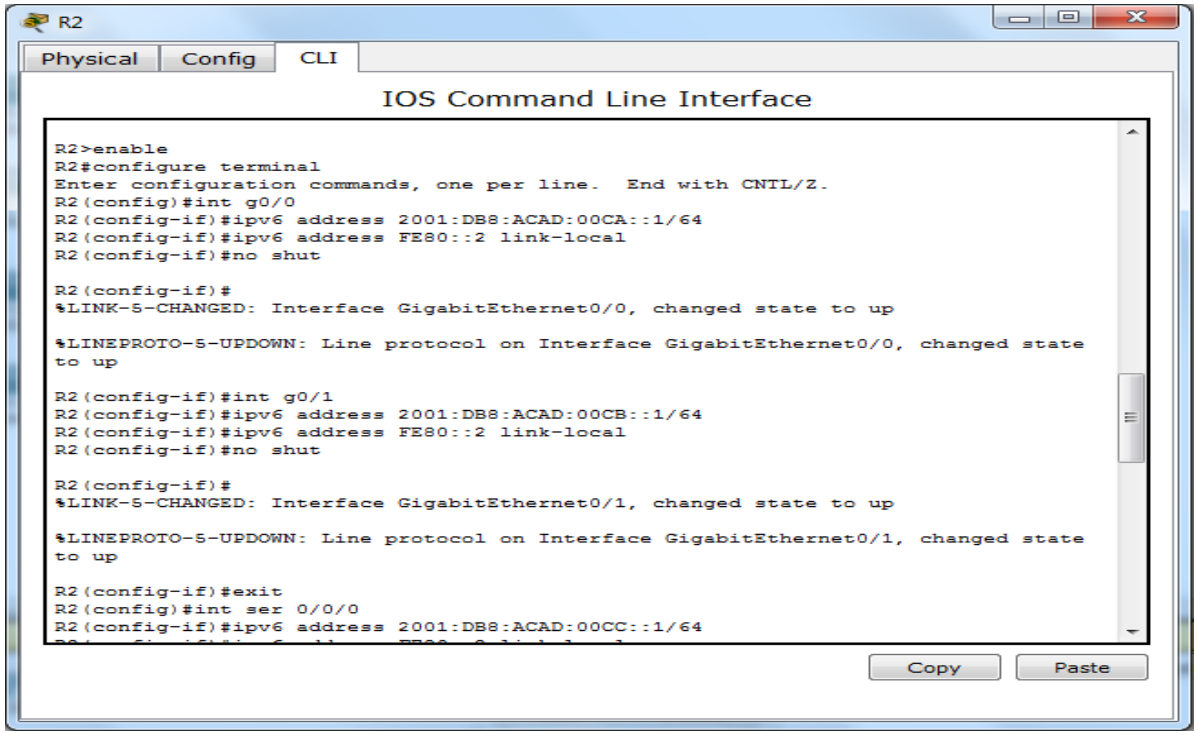


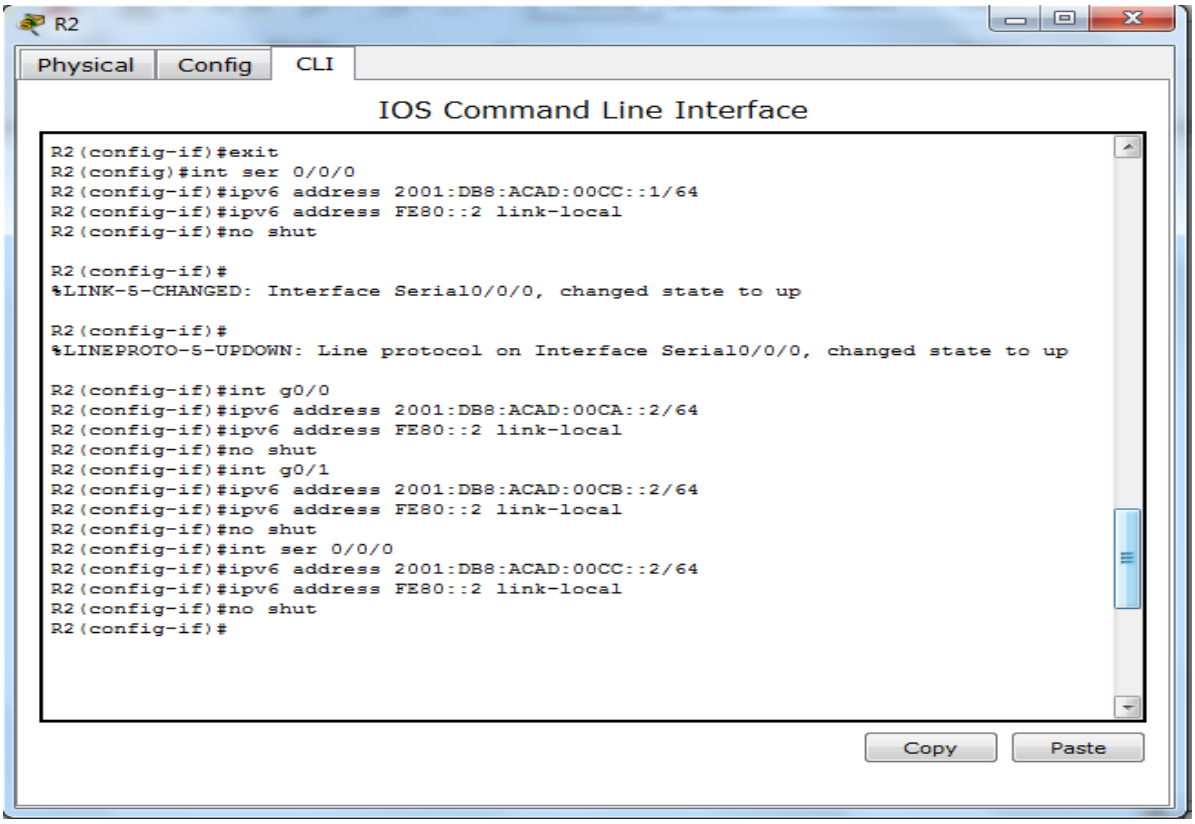

R1
Physical
Config
CLI
IOS Command Line Interface
license udi pid CISCO1941/K9 sn FTX1524LGPT
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB:ACAD:C8::/64
 ipv6 rip 1 enable
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
Copy
Paste


R1
Physical
Config
CLI
IOS Command Line Interface
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:C9::1/64
 ipv6 rip 1 enable
!
interface Serial0/0/0
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:CC::1/64
 ipv6 rip 1 enable
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ipv6 router rip 1
!
ip classless
!
ip flow-export version 9
Copy
Paste



b. Asigne las primeras direcciones IPv6 al R2 para las dos LAN. Asigne la segunda dirección IPv6 para el enlace WAN.





c. Registre el esquema de direccionamiento IPv6 en la **tabla de direccionamiento**.

Dispositivo	Interfaz	Dirección IPv6	Link-Local
R1	G0/0	2001:DB8:ACAD:00C8::1/64	FE80::1
	G0/1	2001:DB8:ACAD:00C9::1/64	FE80::1
	S0/0/0	2001:DB8:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB8:ACAD:00CA::2/64	FE80::2
	G0/1	2001:DB8:ACAD:00CB::2/64	FE80::2
	S0/0/0	2001:DB8:ACAD:00CC::2/64	FE80::2
PC1	NIC	Configuración automática	
PC2	NIC	Configuración automática	
PC3	NIC	Configuración automática	
PC4	NIC	Configuración automática	

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

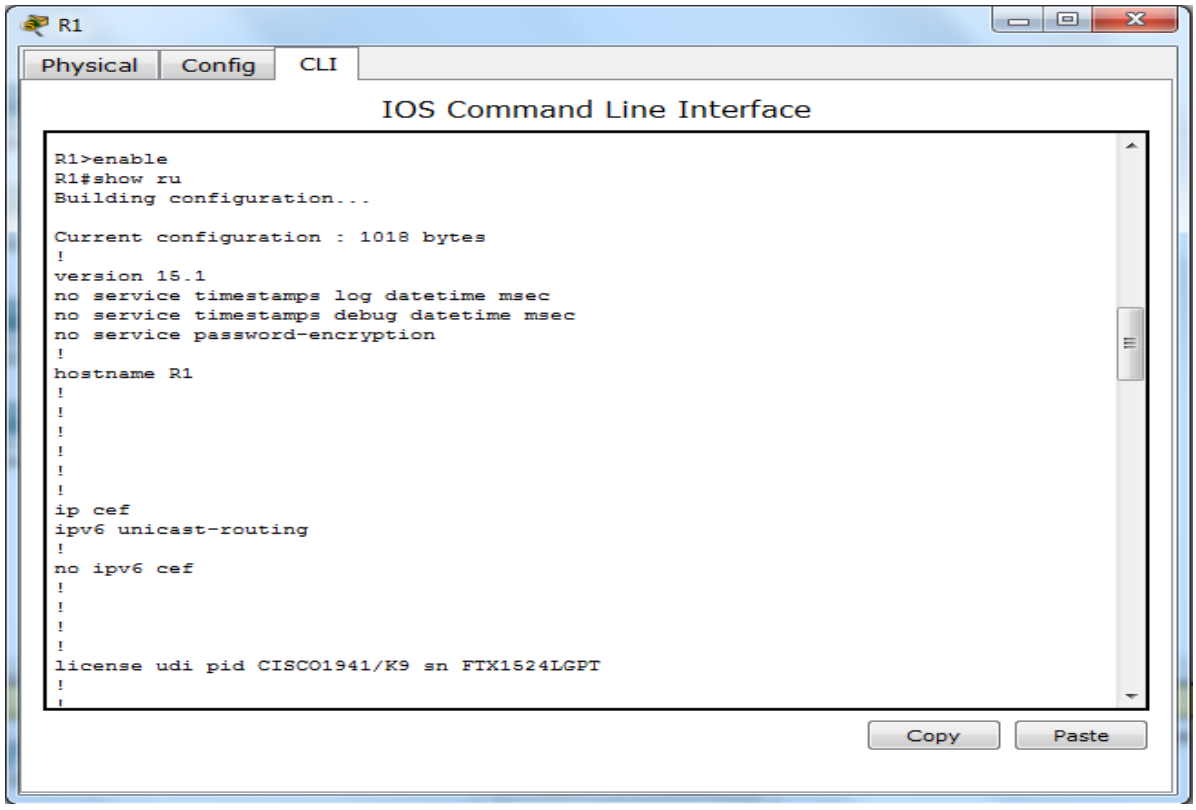
Paso 1: Configurar el direccionamiento IPv6 en los routers.

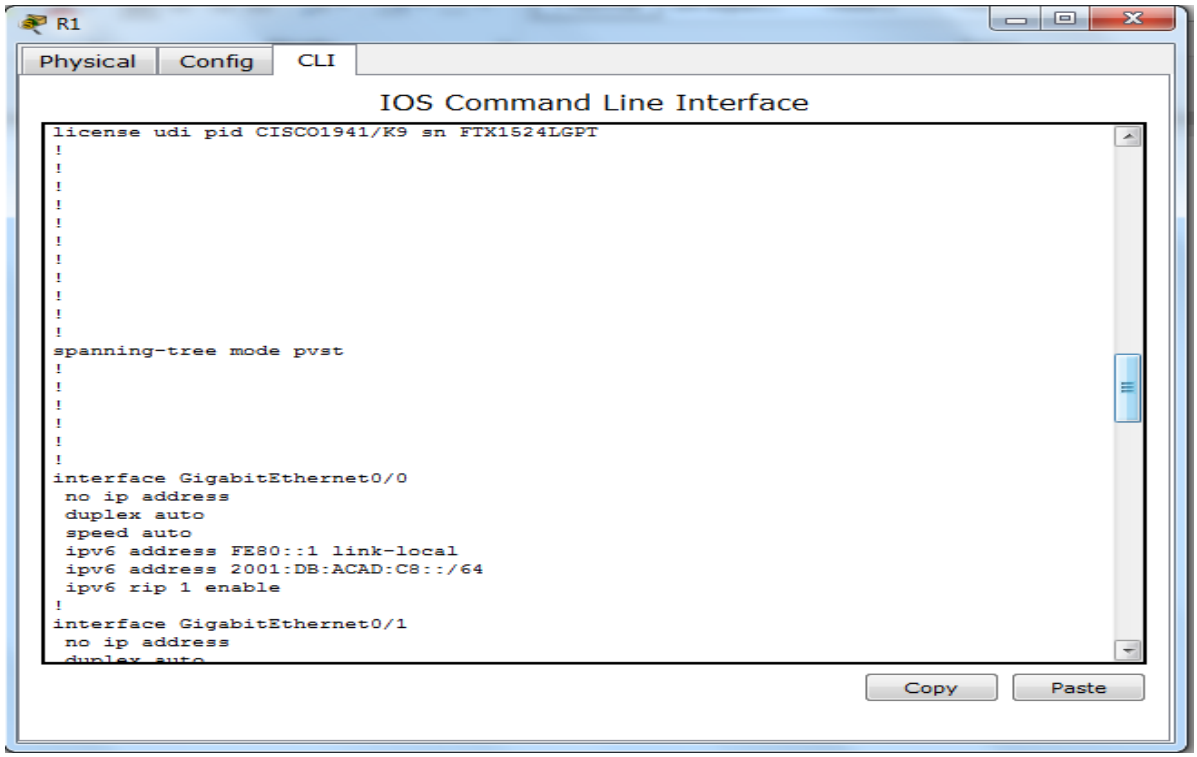
Nota: esta red ya está configurada con algunos comandos de IPv6 que se abordan en un curso posterior. En este punto de sus estudios, solo necesita saber cómo configurar la dirección IPv6 en una interfaz.

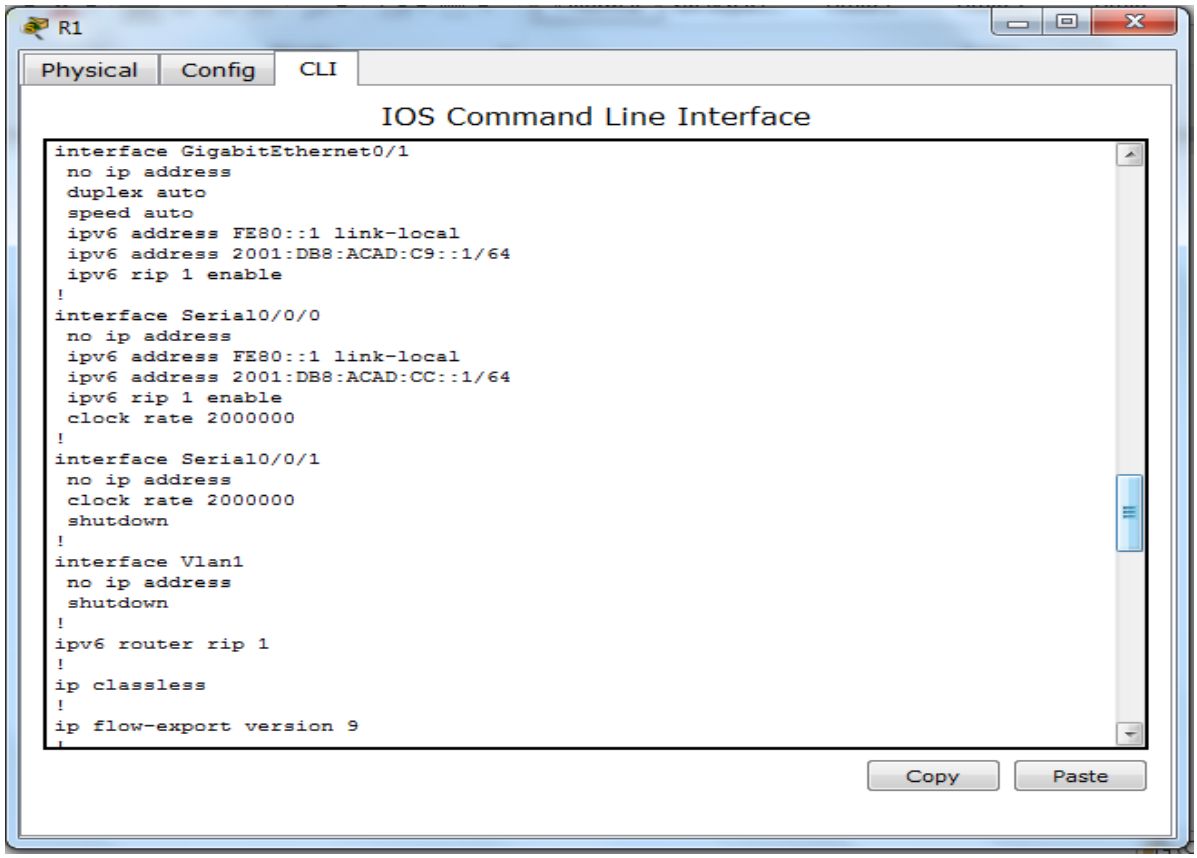
Configure el R1 y el R2 con las direcciones IPv6 que especificó en la **tabla de direccionamiento** y active las interfaces.

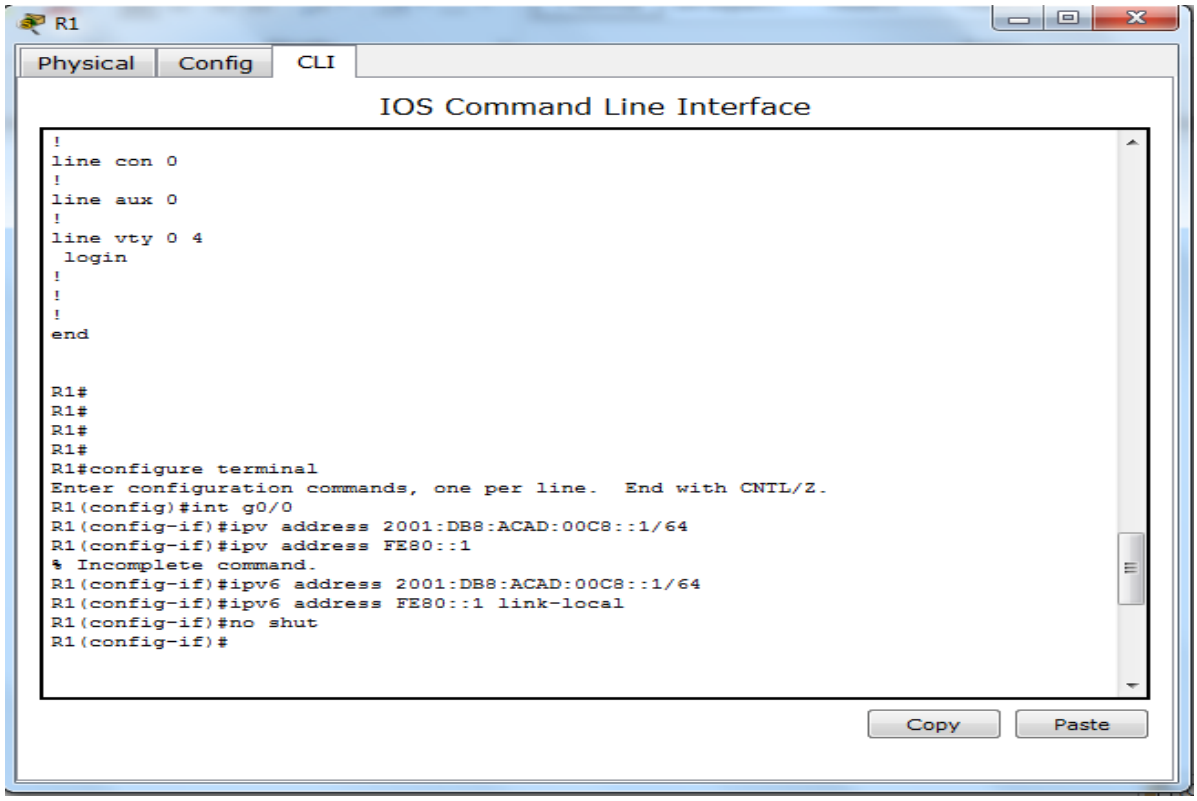
Router(config-if)# **ipv6 address** *ipv6-address/prefix*

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

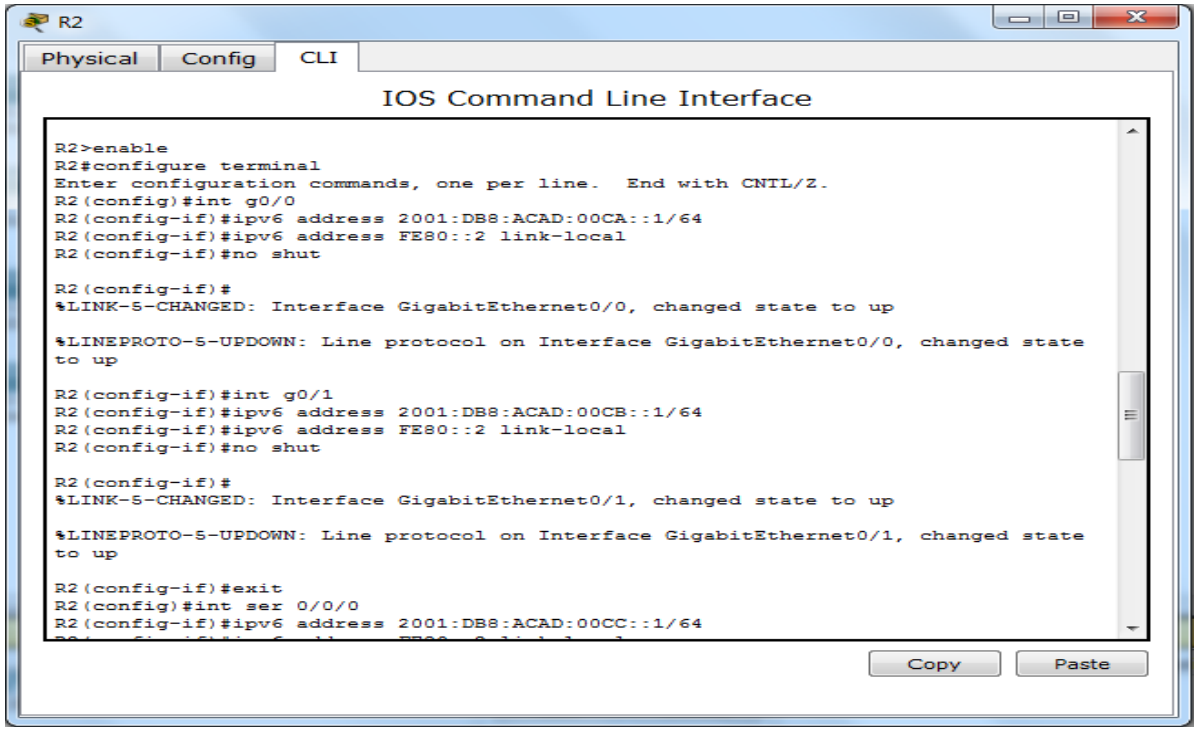


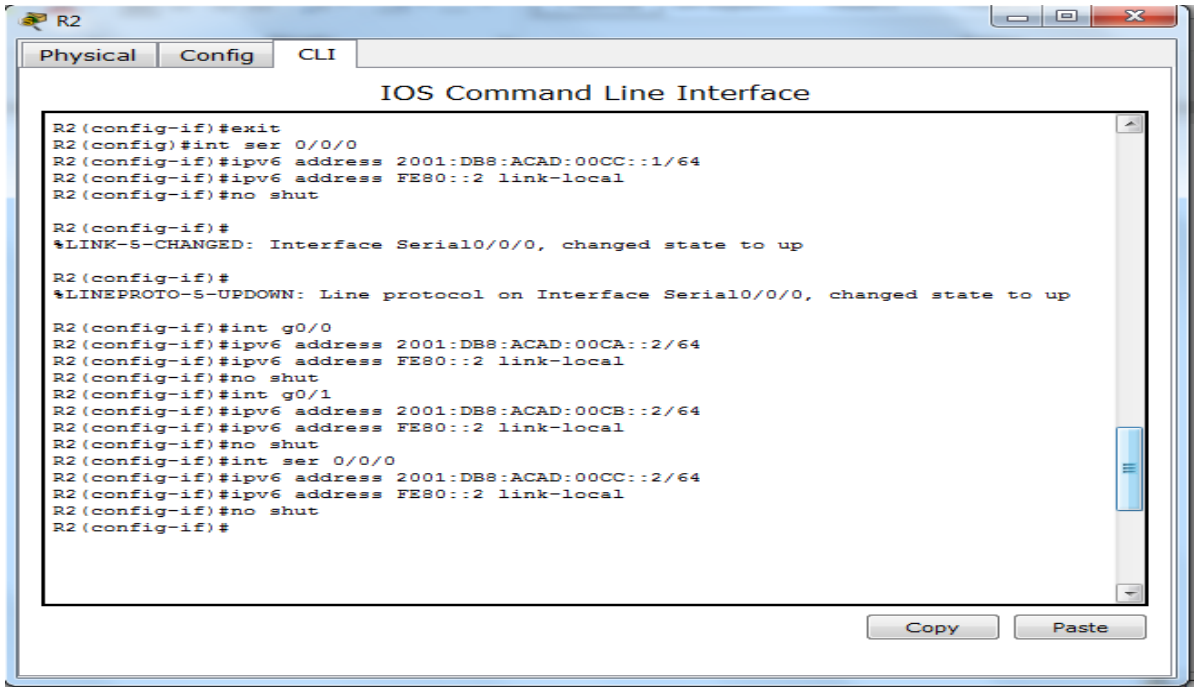

R1
Physical
Config
CLI
IOS Command Line Interface
license udi pid CISCO1941/K9 sn FTX1524LGPT
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB:ACAD:C8::/64
 ipv6 rip 1 enable
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
Copy
Paste


R1
Physical
Config
CLI
IOS Command Line Interface
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:C9::1/64
 ipv6 rip 1 enable
!
interface Serial0/0/0
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:CC::1/64
 ipv6 rip 1 enable
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ipv6 router rip 1
!
ip classless
!
ip flow-export version 9
Copy
Paste


R1
Physical
Config
CLI
IOS Command Line Interface
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
R1#
R1#
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#ipv address 2001:DB8:ACAD:00C8::1/64
R1(config-if)#ipv address FE80::1
% Incomplete command.
R1(config-if)#ipv6 address 2001:DB8:ACAD:00C8::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut
R1(config-if)#
Copy
Paste

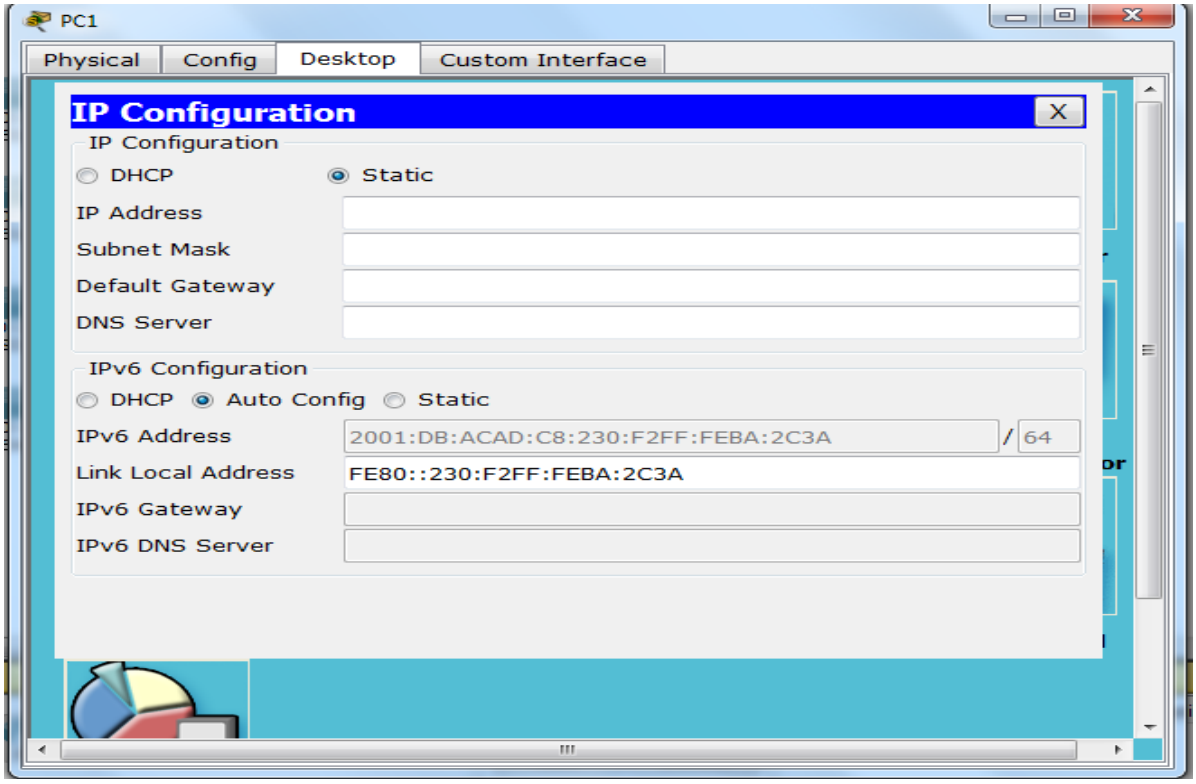
R2

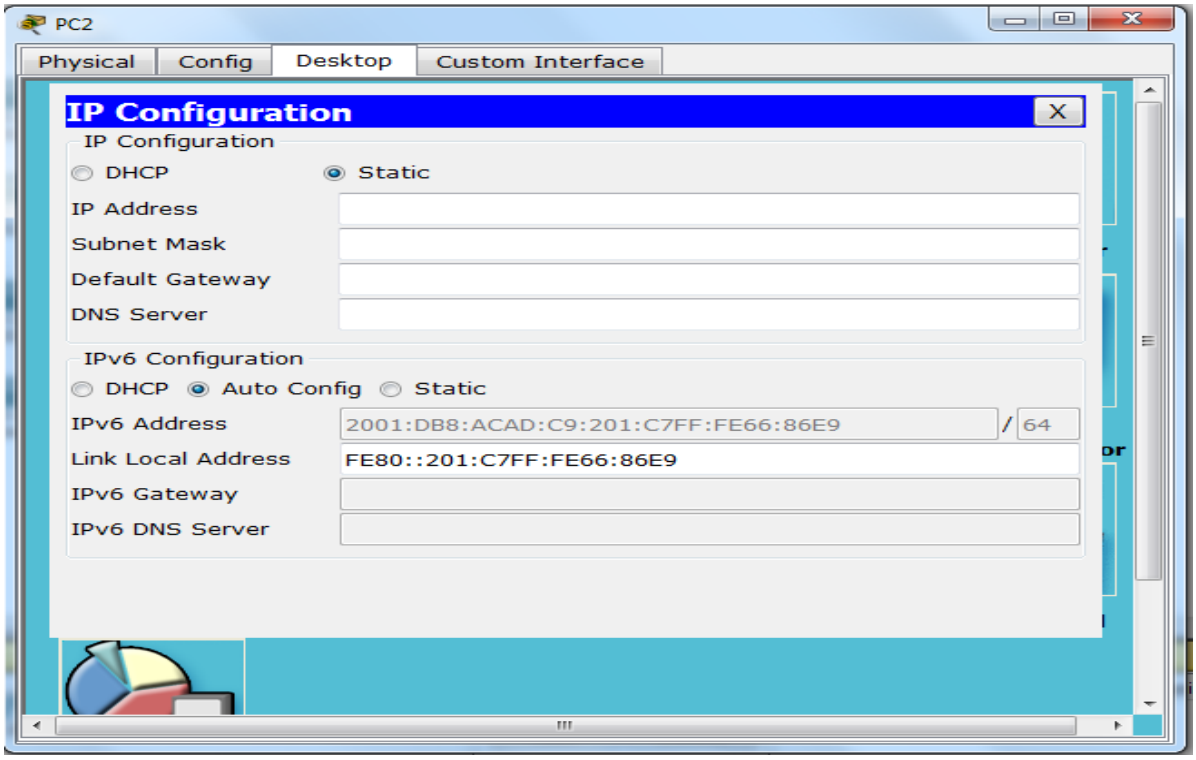

R2
Physical
Config
CLI
IOS Command Line Interface
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CA::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#int g0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CB::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shut
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)#exit
R2(config)#int ser 0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:00CC::1/64
Copy
Paste

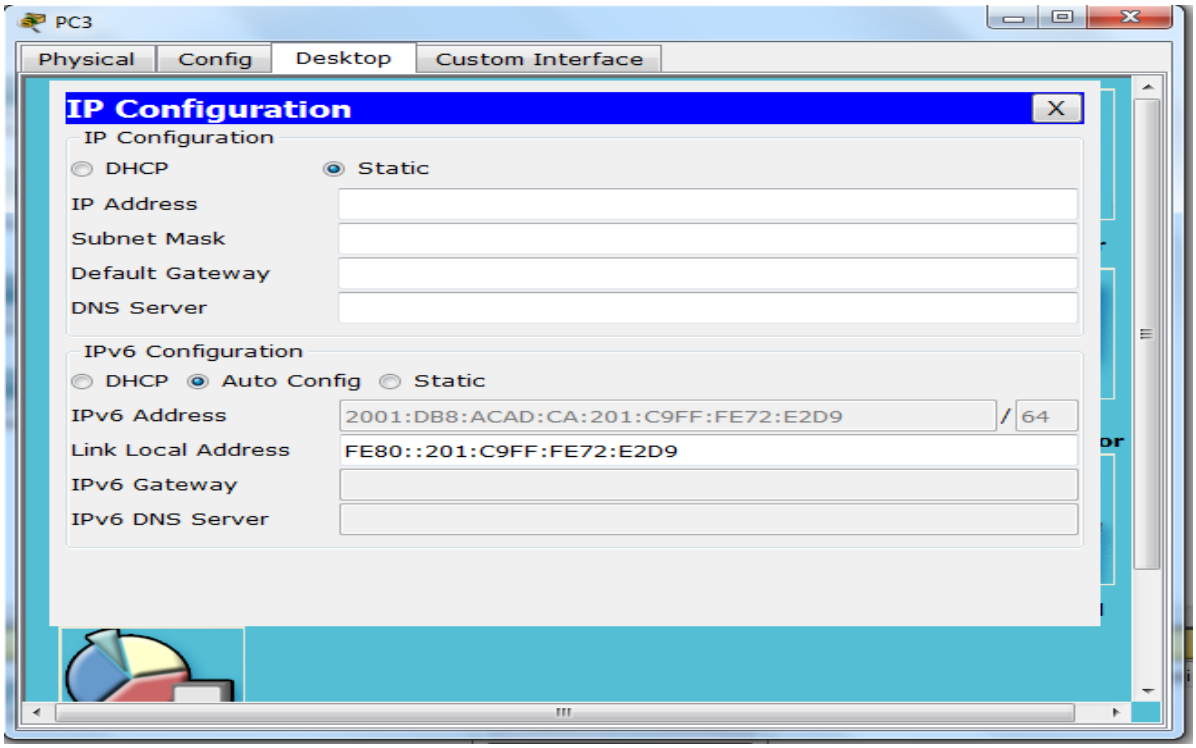


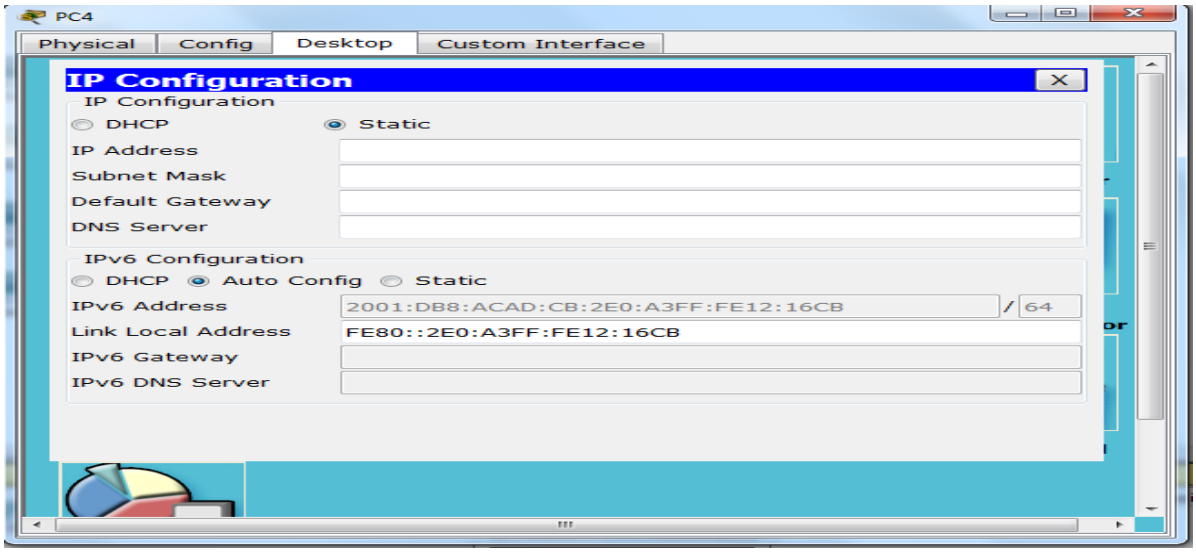
Paso 2: Configurar las PC para que reciban el direccionamiento IPv6 automáticamente

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



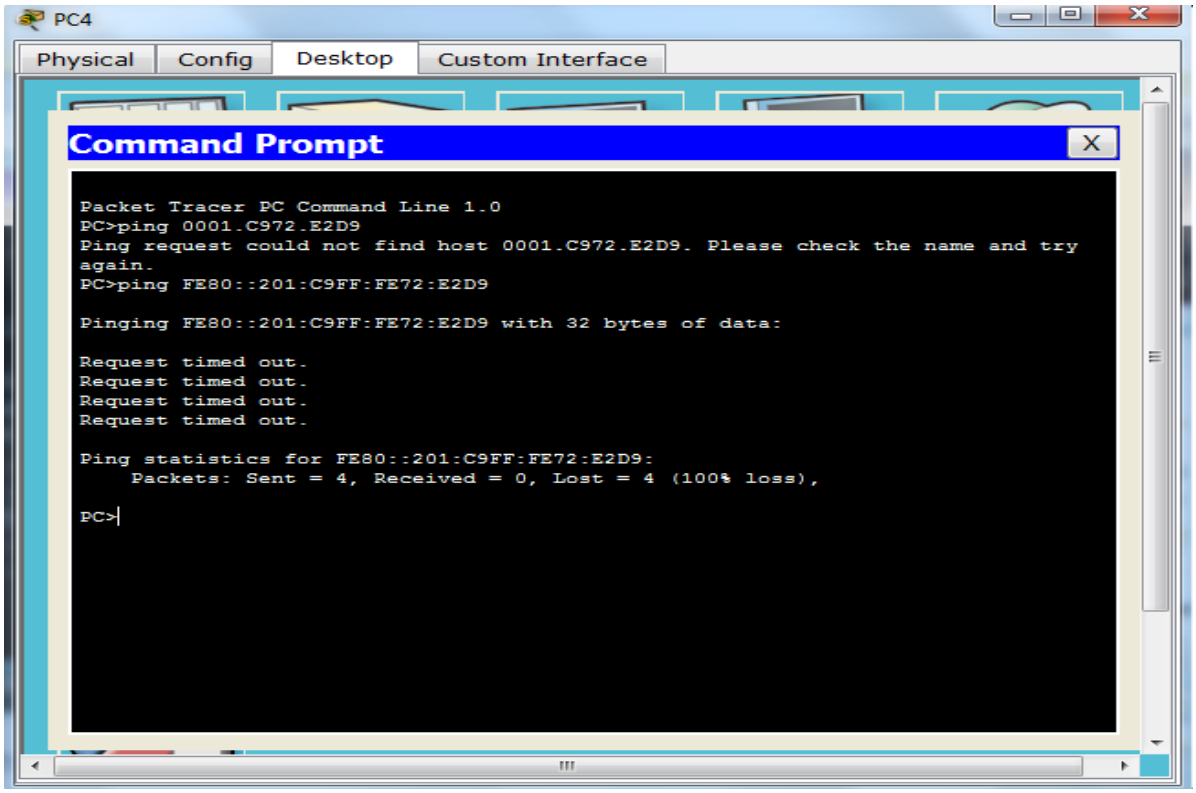

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:C9:201:C7FF:FE66:86E9
/ 64
Link Local Address
FE80::201:C7FF:FE66:86E9
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address
Subnet Mask
Default Gateway
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
2001:DB8:ACAD:CA:201:C9FF:FE72:E2D9
/ 64
Link Local Address
FE80::201:C9FF:FE72:E2D9
IPv6 Gateway
IPv6 DNS Server



Paso 3: Probar la conectividad entre las PC.

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



9.4.1.2 Skills Integration Challenge Instructions IG

Packet Tracer: Reto de habilidades de integración

Topología

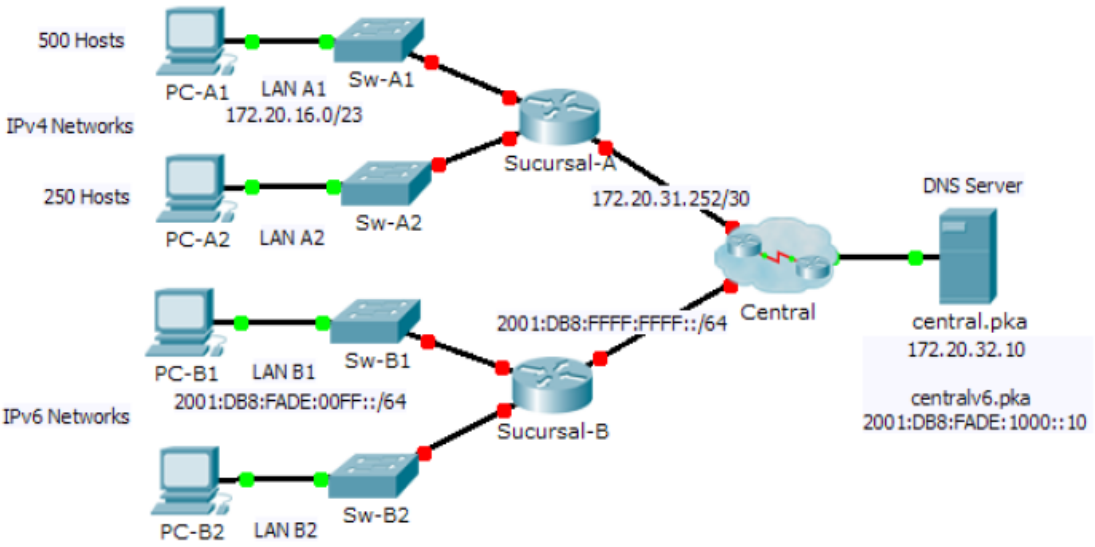


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
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	172.20.31.254	255.255.255.252	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	172.20.17.254	255.255.254.0	172.20.16.1
PC-A2	NIC	172.20.18.254	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

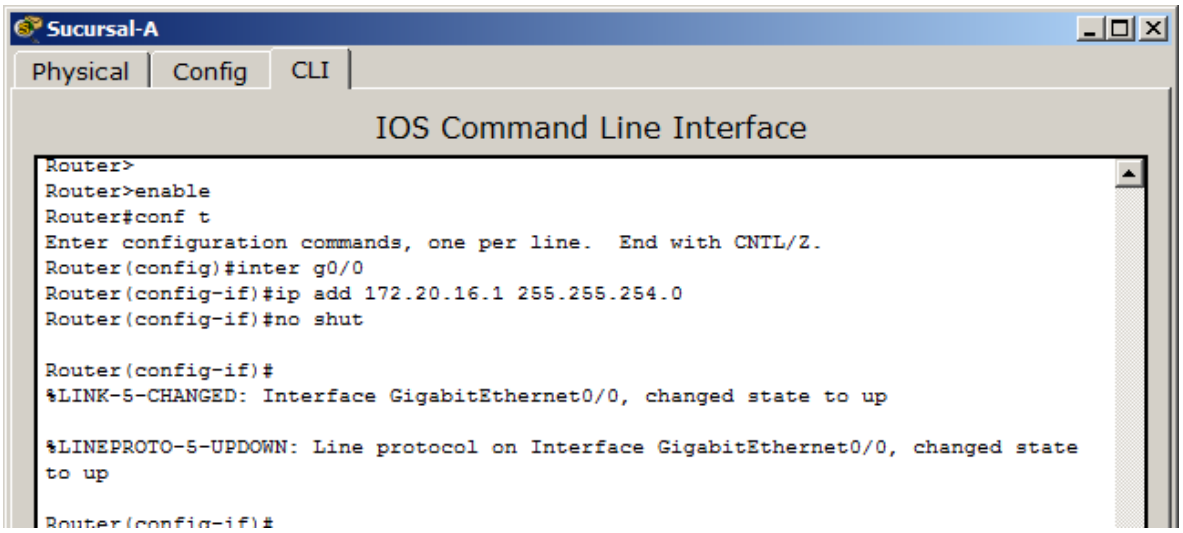
Como técnico de redes familiarizado con implementaciones de direccionamiento IPv4 e IPv6, ya está preparado para tomar una infraestructura de red existente y aplicar sus conocimientos y habilidades a finalizar la configuración. En esta actividad, el administrador de red ya configuró algunos comandos 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.

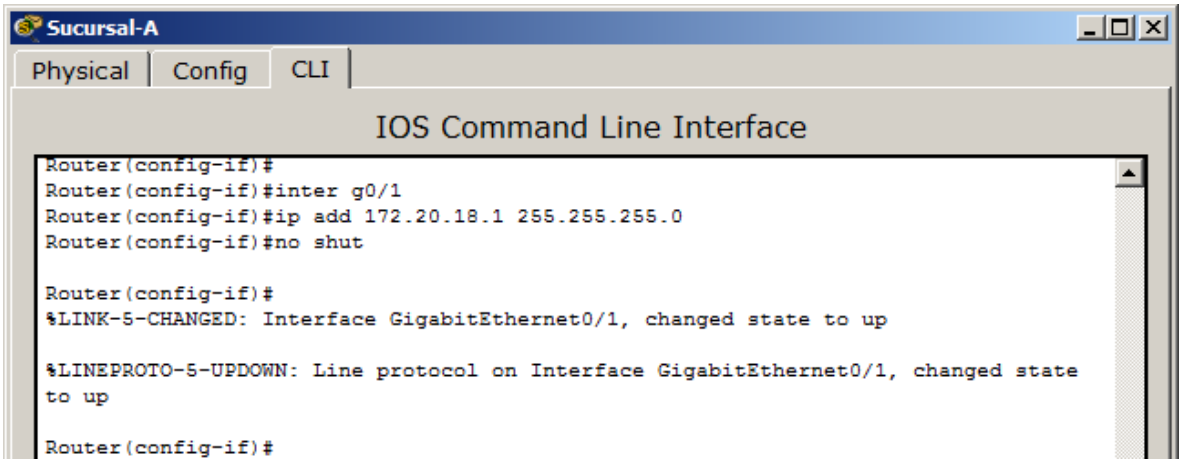
Requisitos

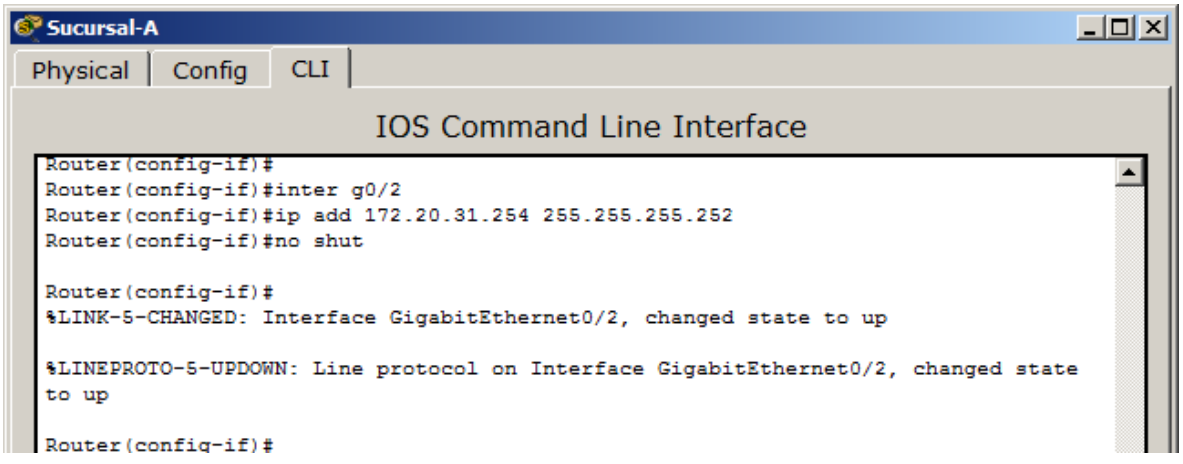
- Configure los parámetros iniciales en **Sucursal-A** y **Sucursal-B**, incluidos el nombre de host, el aviso, las líneas y las contraseñas. Utilice **cisco** como contraseña de EXEC del usuario y **class** como contraseña de EXEC privilegiado. Encripte todas las contraseñas.

- 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.

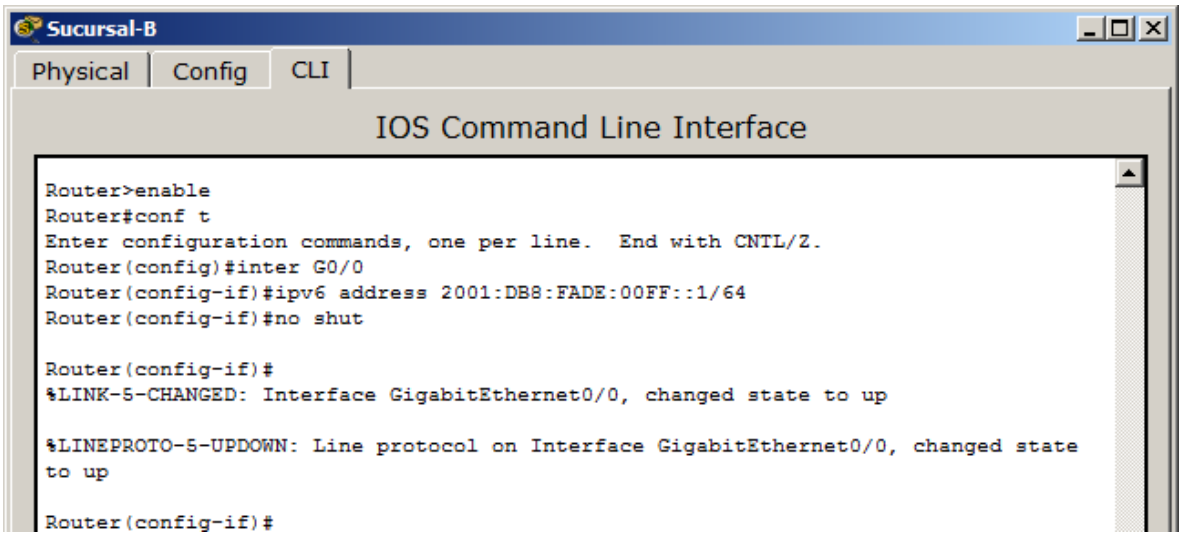
Sucursal-A

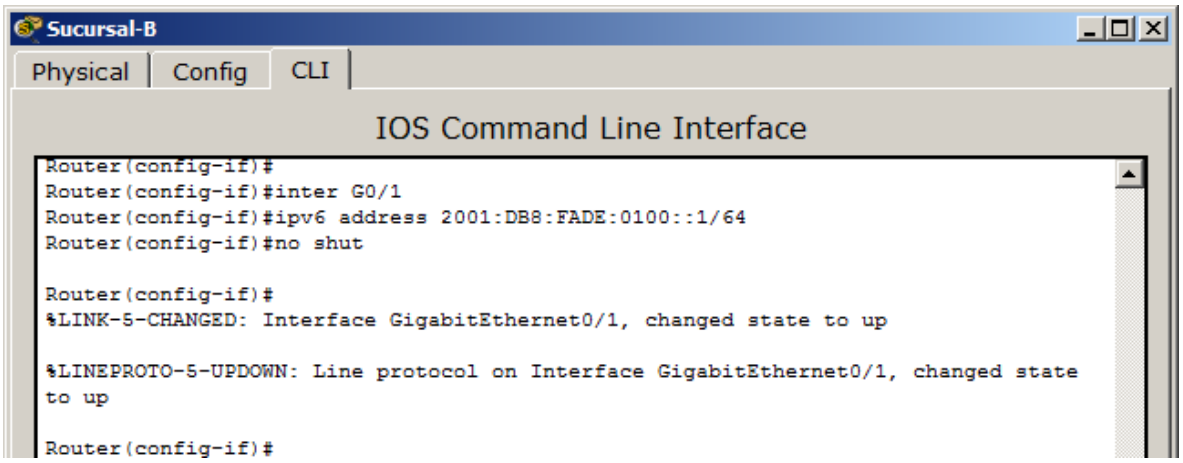

Sucursal-A
Physical
Config
CLI
IOS Command Line Interface
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter g0/0
Router(config-if)#ip add 172.20.16.1 255.255.254.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

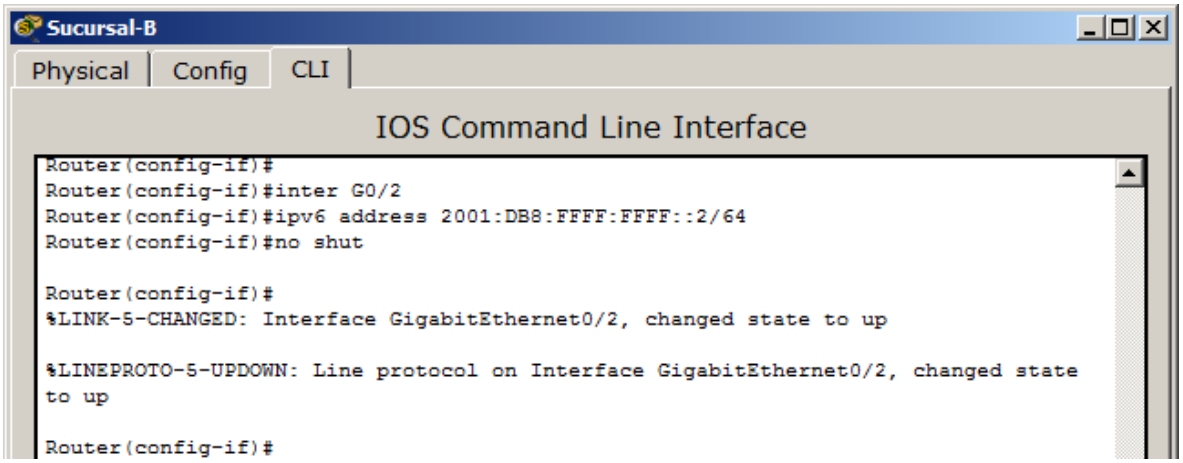

Sucursal-A
Physical
Config
CLI
IOS Command Line Interface
Router(config-if)#
Router(config-if)#inter g0/1
Router(config-if)#ip add 172.20.18.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to up
Router(config-if)#


Sucursal-A
Physical
Config
CLI
IOS Command Line Interface
Router(config-if)#
Router(config-if)#inter g0/2
Router(config-if)#ip add 172.20.31.254 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state
to up

Sucursal-B

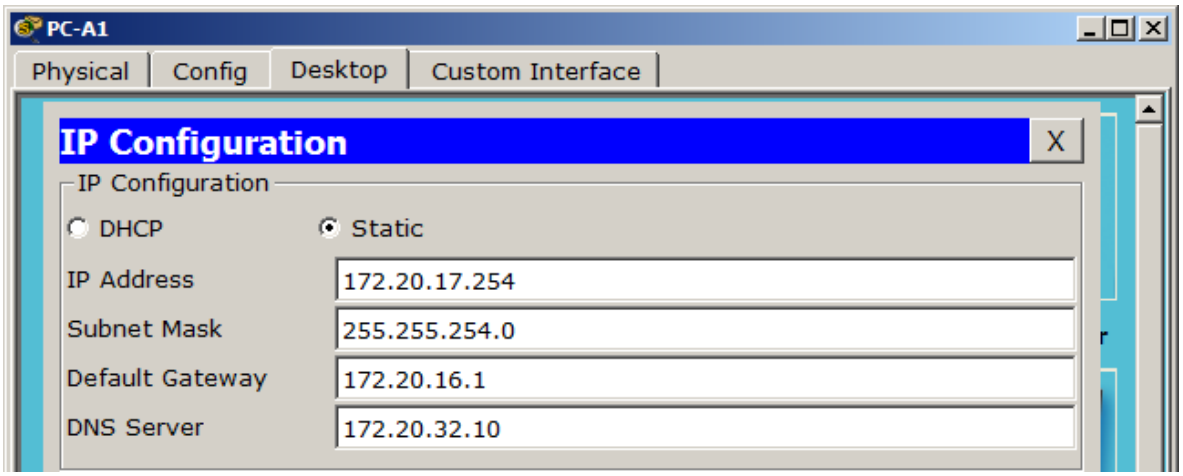




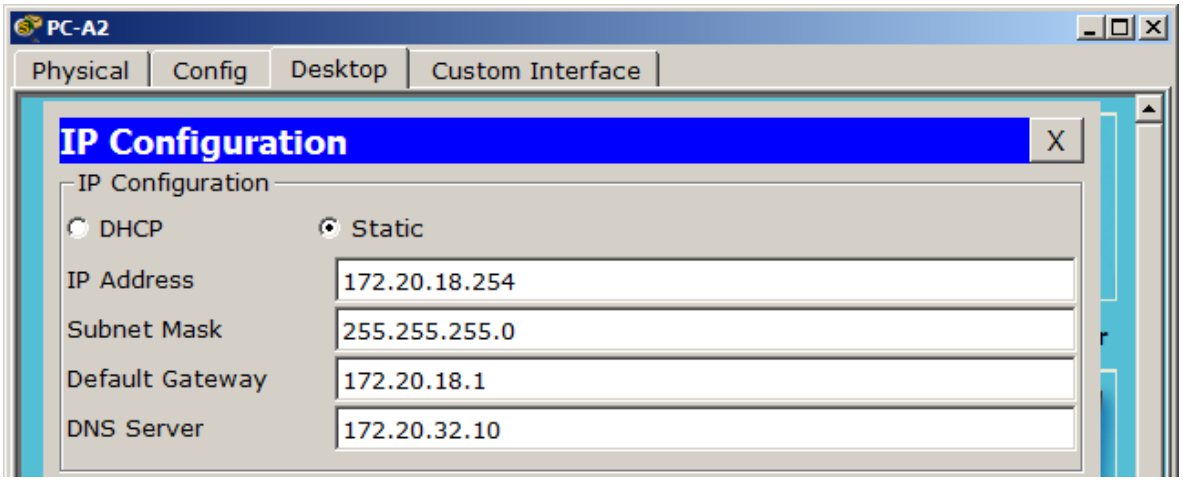


- Para las redes IPv4, asigne la última dirección IPv4 a las PC.
- Para las redes IPv6, asigne la 16.ª dirección IPv6 a las PC.

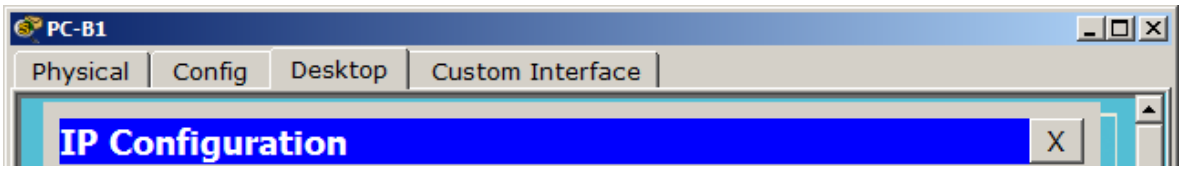
PC-A1

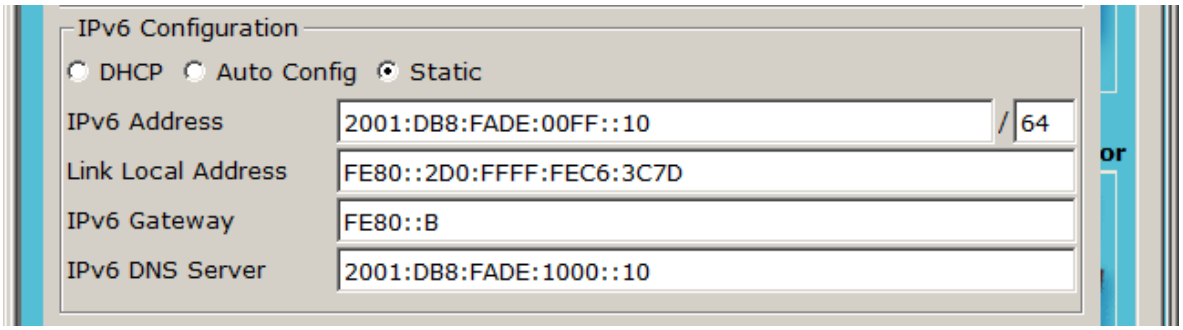


PC-A2

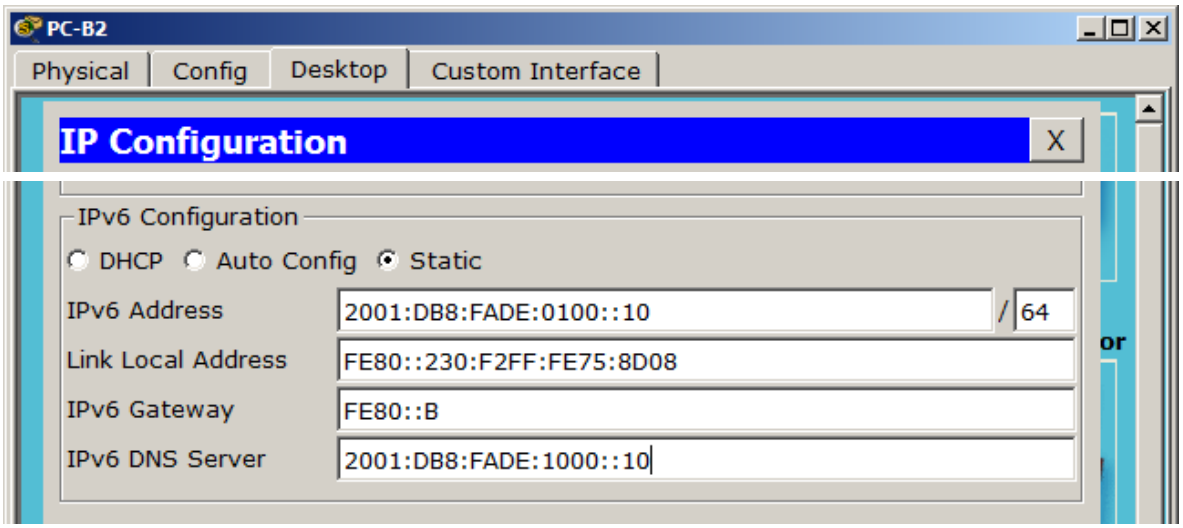


PC-B1

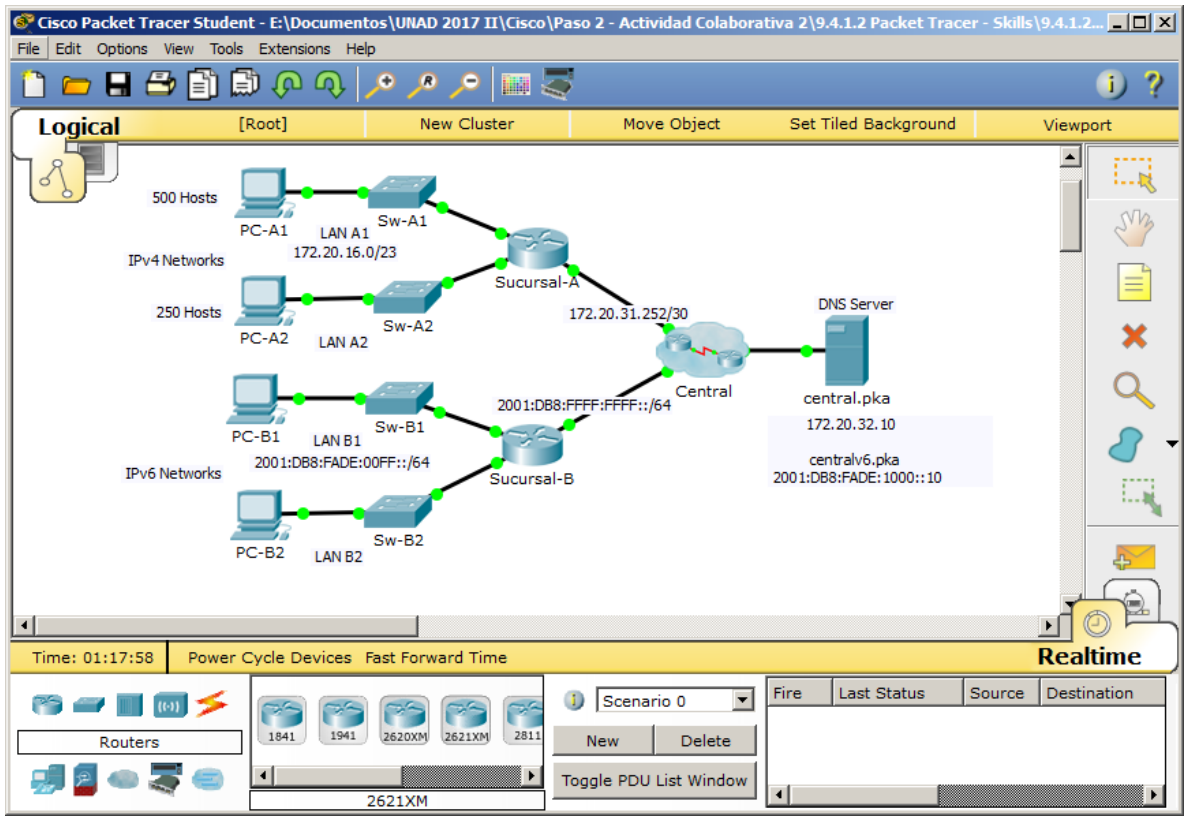




PC-B2



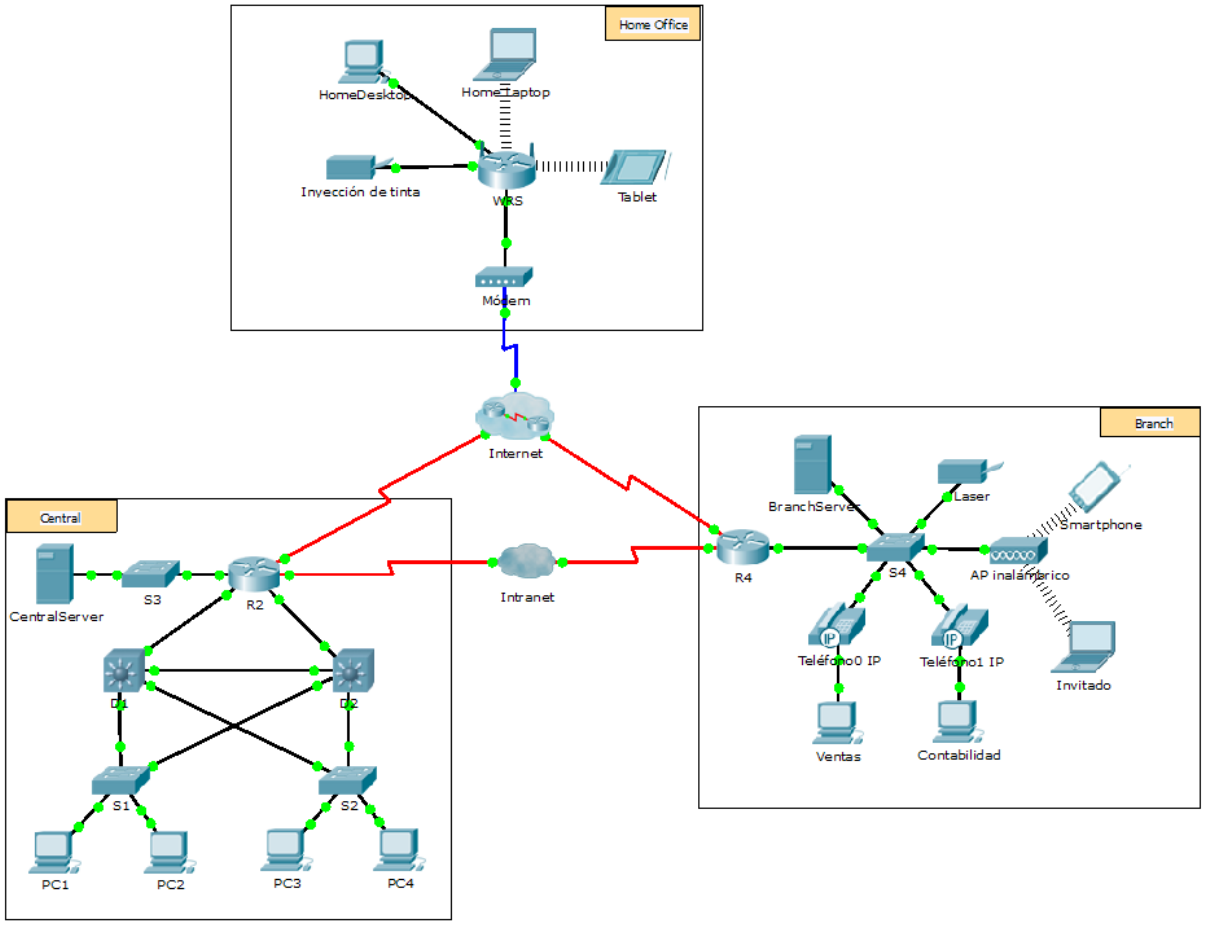
- Configure el direccionamiento de los routers según los registros. Incluya una descripción adecuada para cada interfaz del router. **Sucursal-B** utiliza FE80::B como dirección link-local.
- Configure el direccionamiento de las PC según los registros. Las direcciones del servidor DNS para IPv4 e IPv6 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**.


Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 2 - Actividad Colaborativa 2\9.4.1.2 Packet Tracer - Skills\9.4.1.2...
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
500 Hosts
PC-A1
LAN A1
Sw-A1
172.20.16.0/23
IPv4 Networks
Sucursal-A
250 Hosts
PC-A2
LAN A2
Sw-A2
172.20.31.252/30
DNS Server
Central
central.pka
172.20.32.10
centralv6.pka
2001:DB8:FADE:1000::10
2001:DB8:FFFF:FFFF::/64
PC-B1
LAN B1
Sw-B1
2001:DB8:FADE:00FF::/64
IPv6 Networks
Sucursal-B
PC-B2
LAN B2
Sw-B2
Time: 01:17:58
Power Cycle Devices
Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2811
2621XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

10.2.1.8 Web and Email Instructions IG

Packet Tracer: 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

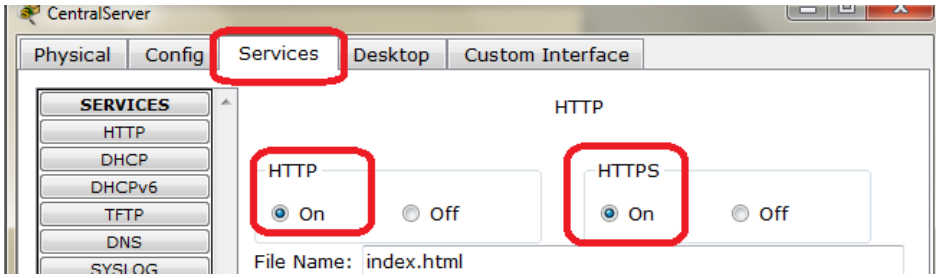
En esta actividad, configurará los servicios HTTP y de correo electrónico mediante el servidor simulado de Packet Tracer. Luego, configurará clientes para que accedan a los servicios HTTP y de correo electrónico.

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).

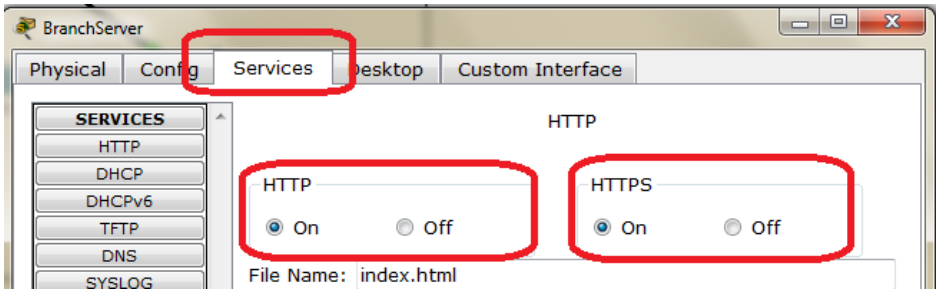


c. Optativo: personalice el código HTML.

```
<html>
<center><font size='+2' color='red'>Central
Server</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new
opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='image.jpg'>Image</a>
</html>
```

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

Haga clic en **On** (Activar) para habilitar HTTP y HTTP seguro (HTTPS).



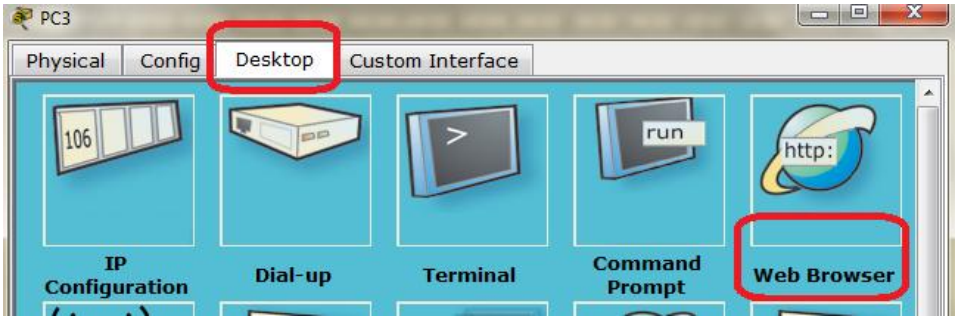
Optativo: personalice el código HTML.

```
<html>
<center><font size='+2' color='blue'>Branch
Server</font></center>
<hr>Welcome to Packet Tracer, the best thing since.....
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
</html>
```

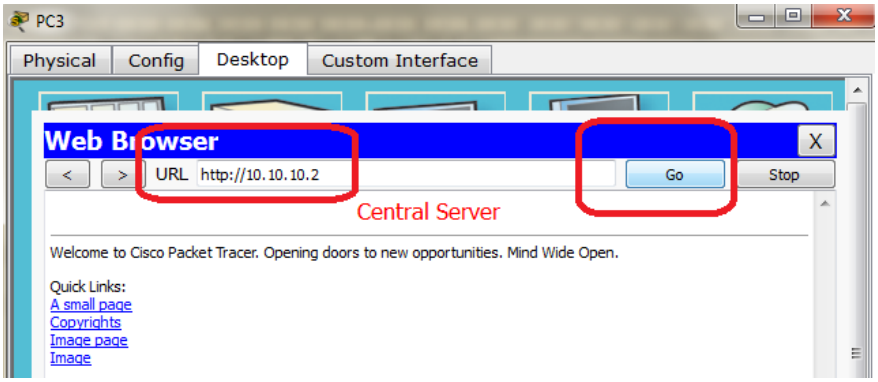
Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web

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

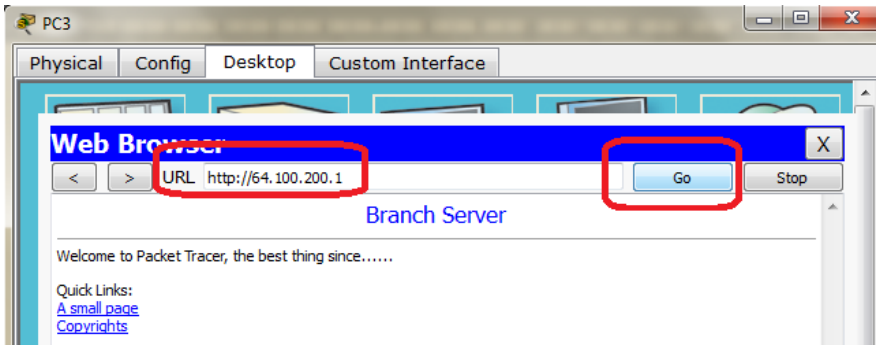
a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **Web Browser** (Escritorio > Explorador Web).



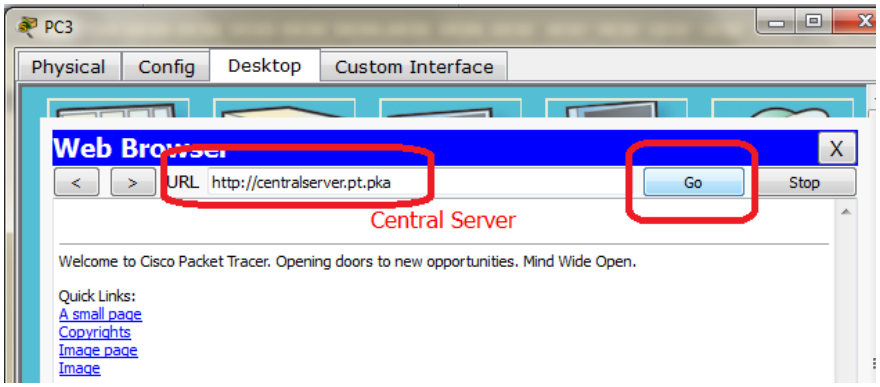
b. En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.



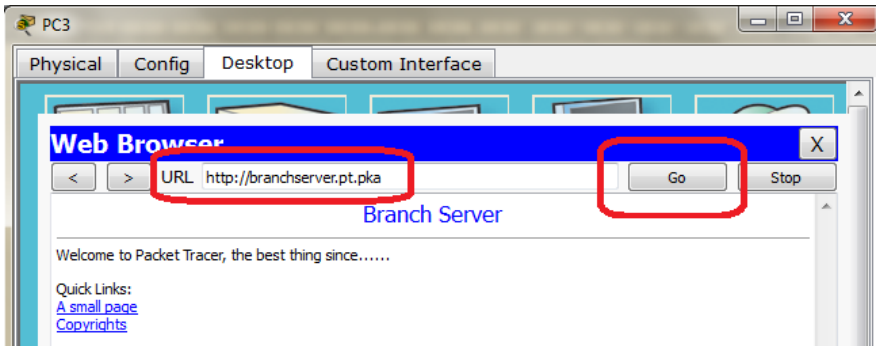
c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



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**.



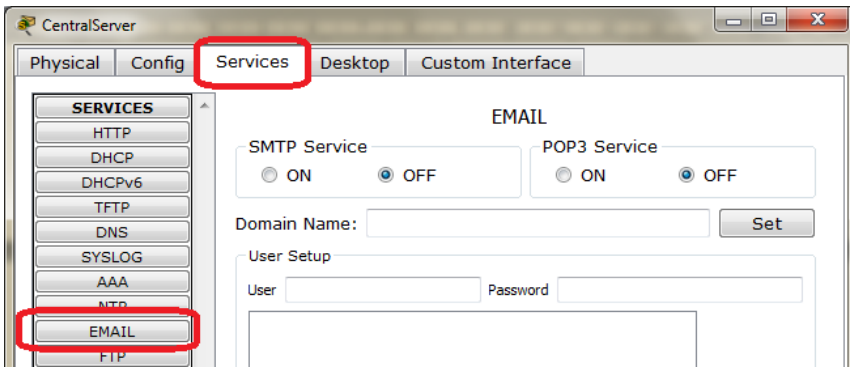
f. ¿Qué protocolo traduce los nombres **centralserver.pt.pka** y **branchserver.pt.pka** por direcciones IP?

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

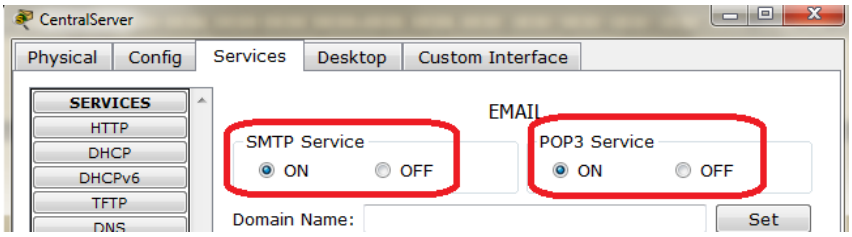
Parte 2: Configurar y verificar los servicios de correo electrónico en los servidores

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

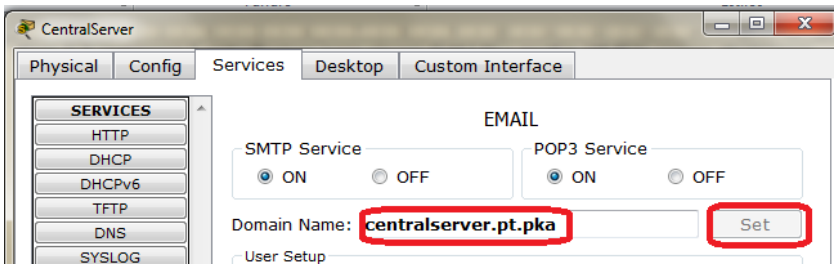
a. Haga clic en **CentralServer** y, a continuación, seleccione la ficha **Config**, seguida del botón **EMAIL** (Correo electrónico).



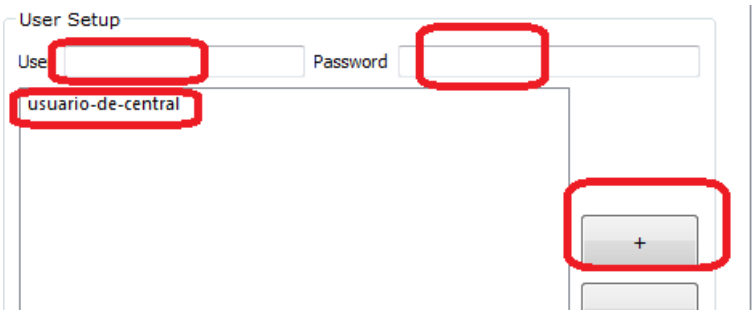
b. Haga clic en **On** para habilitar SMTP y POP3.



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

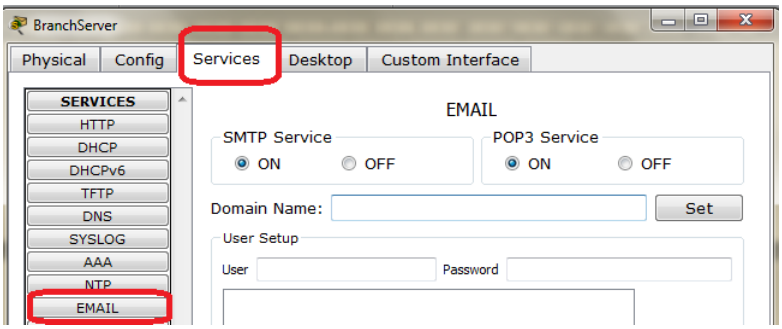


d. Cree un usuario denominado **usuario-de-central** con la contraseña **cisco**. Haga clic en + para agregar el usuario.

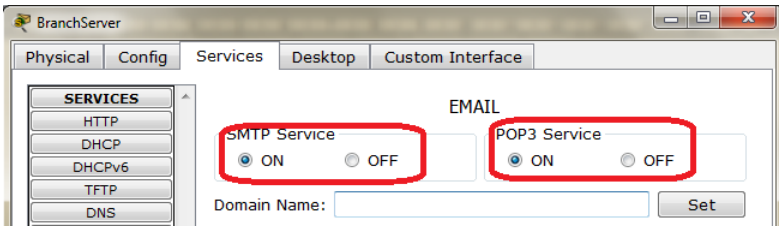


Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

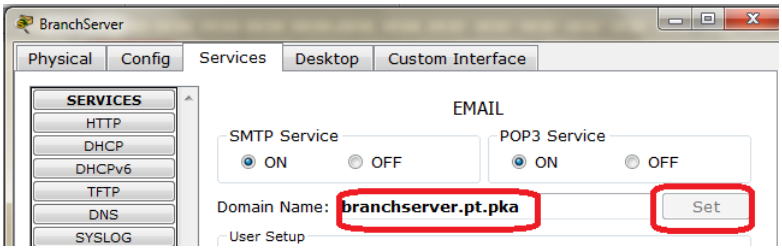
a. Haga clic en **BranchServer** y, a continuación, haga clic en la ficha **Config** > **EMAIL**.



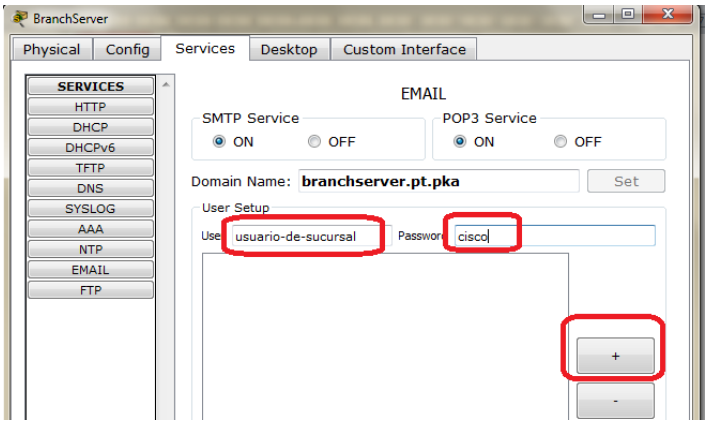
b. Haga clic en **On** para habilitar SMTP y POP3**.**



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

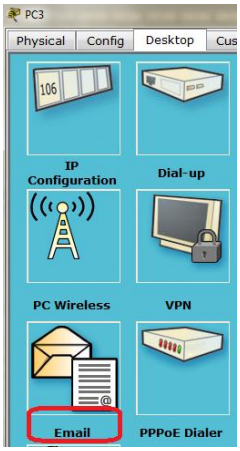


d. Cree un usuario denominado **usuario-de-sucursal** con la contraseña **cisco**. Haga clic en **+** para agregar el usuario.



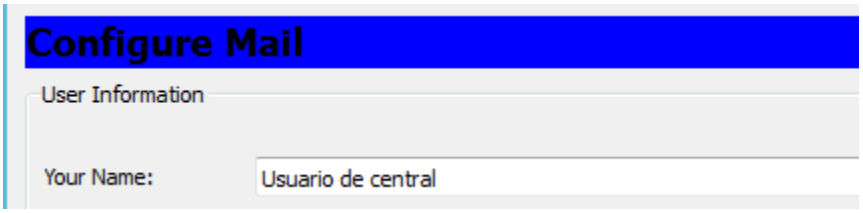
Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

a. Haga clic en **PC3** y, a continuación, haga clic en la ficha **Desktop** > **E Mail** (Correo electrónico).

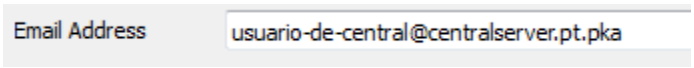


b. Introduzca los siguientes valores en los campos correspondientes:

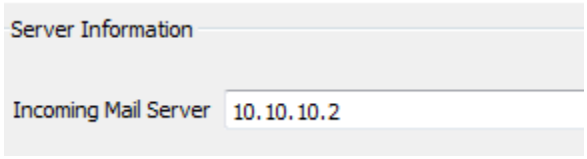
1) Your Name (Su nombre): **Usuario de central**



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

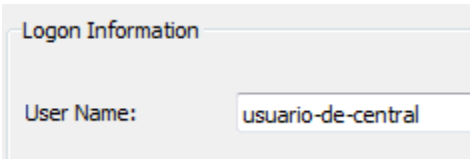


3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**



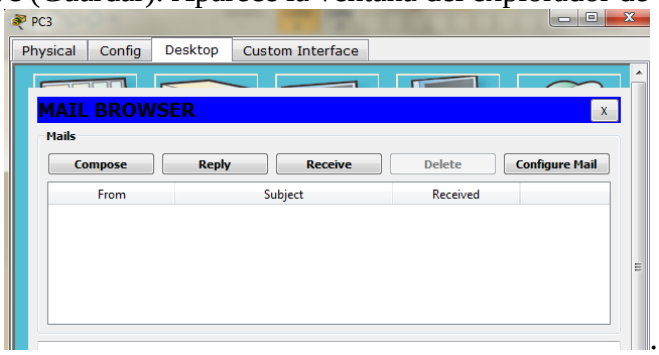
4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**

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

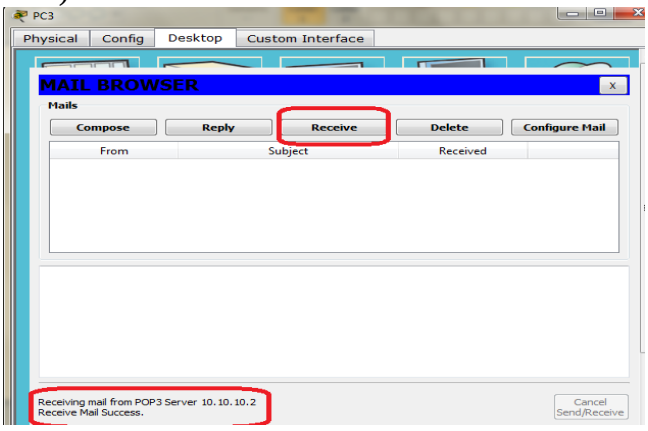


6) Password (Contraseña): **cisco**

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).

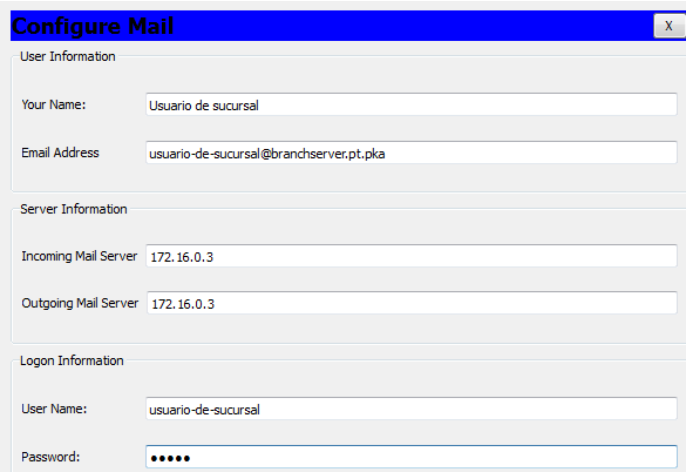


Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

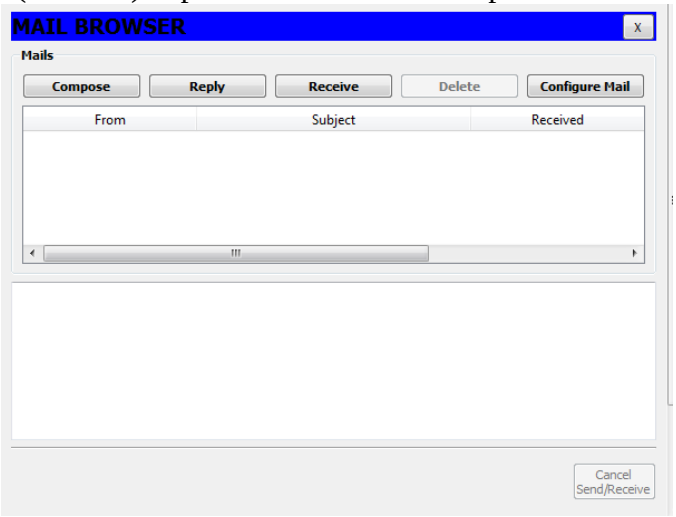
a. Haga clic en **Sales** (Ventas) y, a continuación, haga clic en la ficha **Desktop** > **E Mail**.

b. Introduzca los siguientes valores en los campos correspondientes:

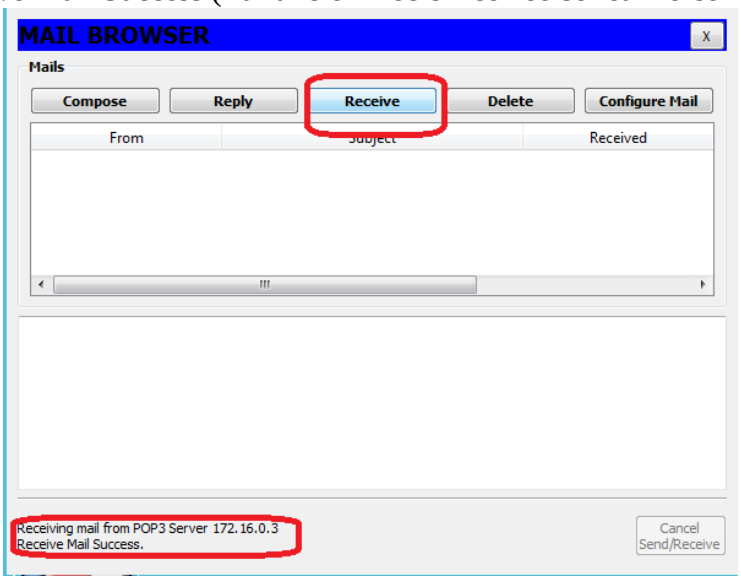
1) Your Name (Su nombre): **Usuario de sucursal**
2) Email Address (Dirección de correo electrónico): **usuario-de-sucursal@branchserver.pt.pka**
3) Incoming Mail Server (Servidor de correo entrante): **172.16.0.3**
4) Outgoing Mail Server (Servidor de correo saliente): **172.16.0.3**
5) User Name (Nombre 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).



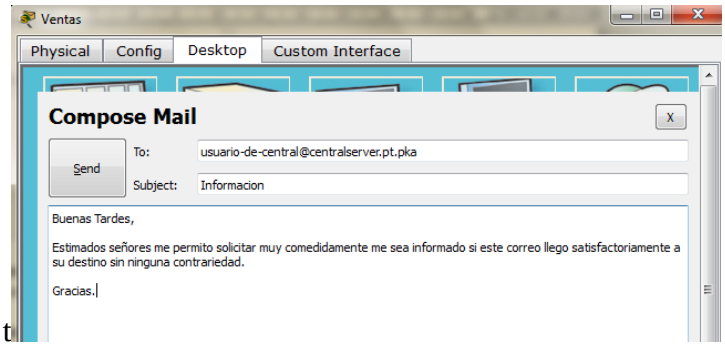
e. Esta actividad debe completarse en un 100%. No cierre la ventana de configuración de Sales ni la ventana del explorador de correo.

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

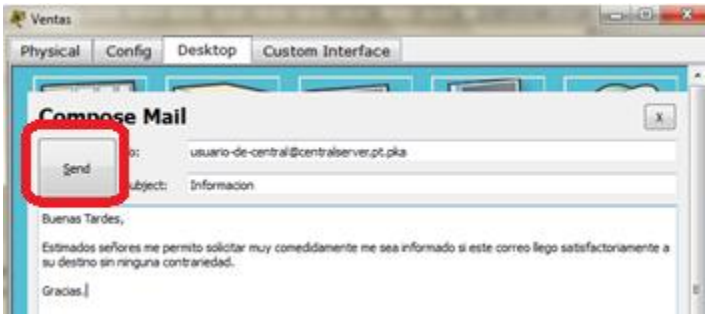
a. Desde la ventana del **explorador de correo** de **Sales**, haga clic en **Compose** (Redactar).

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.*

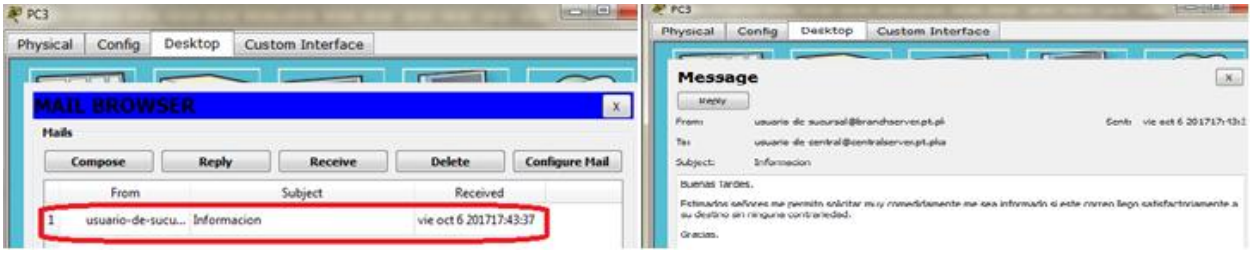


c. Haga clic en **Send** (Enviar)

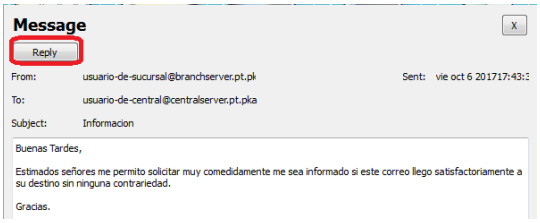


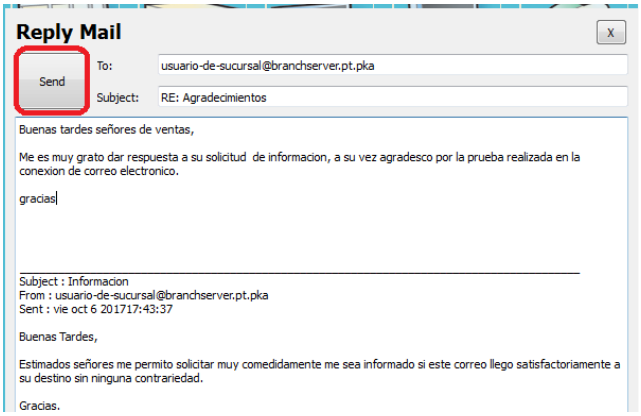
d. Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

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

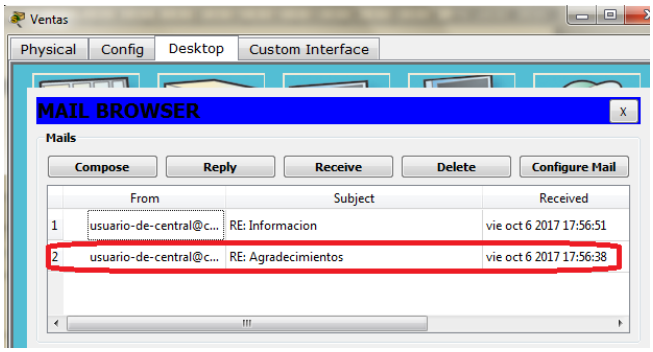


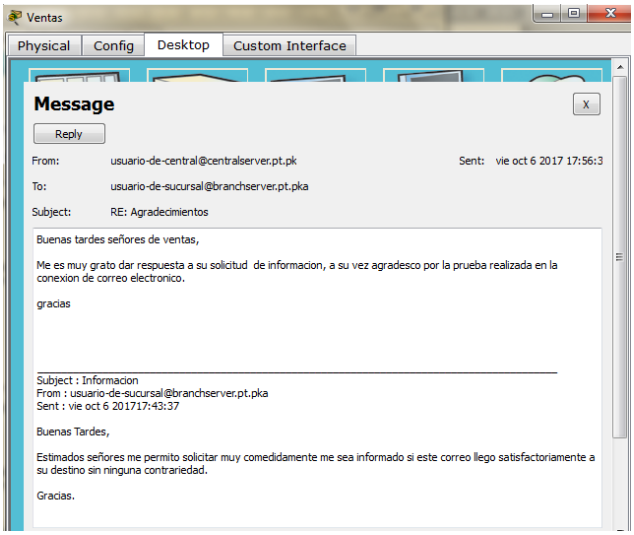
f. Haga clic en **Reply** (Responder), personalice una respuesta y haga clic en **Send**.





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

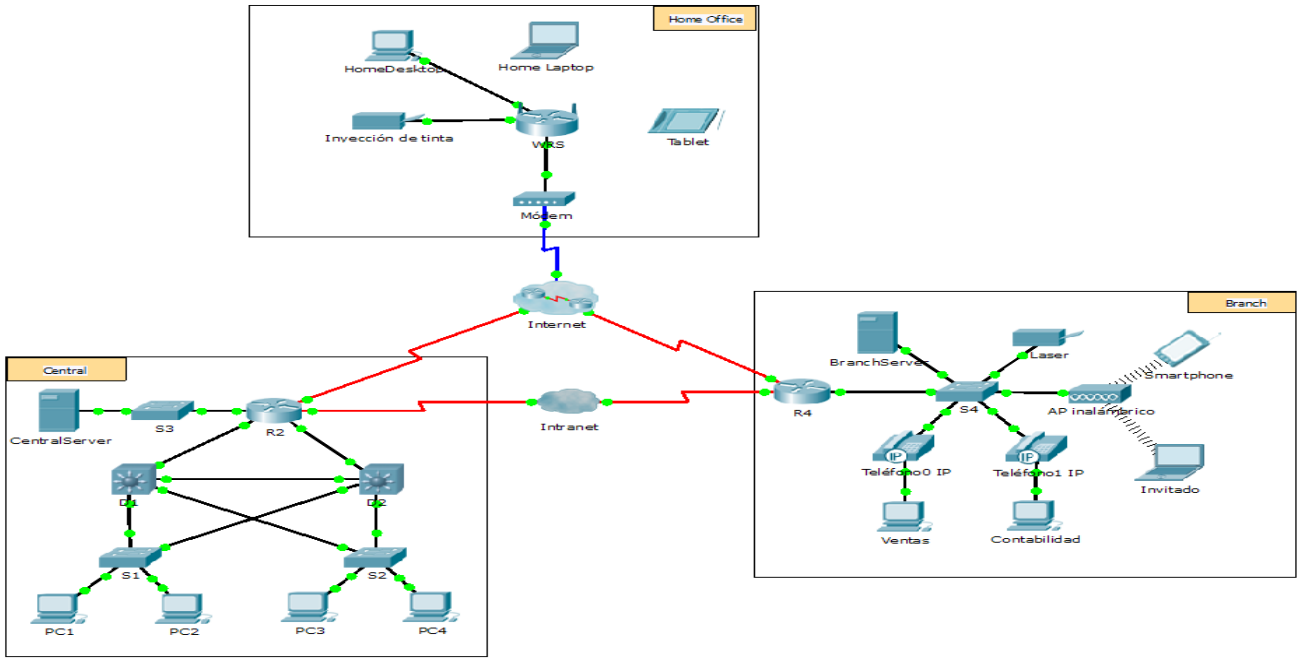

Ventas
Physical
Config
Desktop
Custom Interface
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
usuario-de-central@c...
RE: Informacion
vie oct 6 2017 17:56:51
2
usuario-de-central@c...
RE: Agradecimientos
vie oct 6 2017 17:56:38


Ventas
Physical
Config
Desktop
Custom Interface
Message
X
Reply
From:
usuario-de-central@centralserver.pt.pk
Sent:
vie oct 6 2017 17:56:3
To:
usuario-de-sucursal@branchserver.pt.pka
Subject:
RE: Agradecimientos
Buenas tardes señores de ventas,
Me es muy grato dar respuesta a su solicitud de informacion, a su vez agradesco por la prueba realizada en la conexion de correo electronico.
gracias
Subject : Informacion
From : usuario-de-sucursal@branchserver.pt.pka
Sent : vie oct 6 201717:43:37
Buenas Tardes,
Estimados señores me permito solicitar muy comedidamente me sea informado si este correo llego satisfactoriamente a su destino sin ninguna contrariedad.
Gracias.

10.2.2.8 DNS and DHCP Instructions IG

Packet Tracer: Servidores de DHCP y Servidores DNS

Topología



Objetivos

Parte 1: Configurar el direccionamiento IPv4 estático
Parte 2: Configurar y verificar los registros DNS

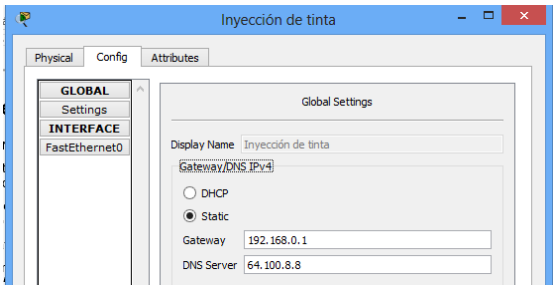
Parte 1: Configurar el direccionamiento IPv4 estático

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).

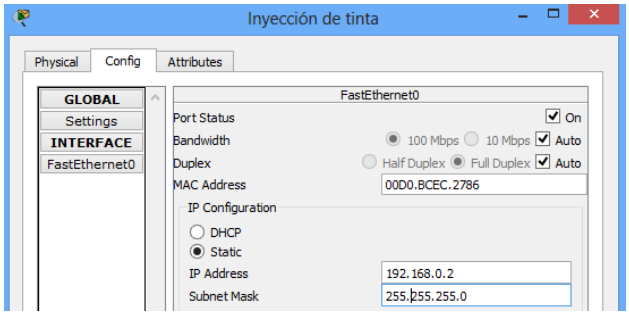
a. Haga clic en **Inkjet** (Inyección de tinta) y, a continuación, haga clic en la ficha **Config**, en la que se muestran los parámetros de Global Settings (Configuración global).

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



c. 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**.

d. Cierre la ventana Inkjet.



Paso 2: Configurar WRS para que proporcione servicios de DHCP.

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

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

1) Cambie la Dirección IP a **192.168.0.1**.

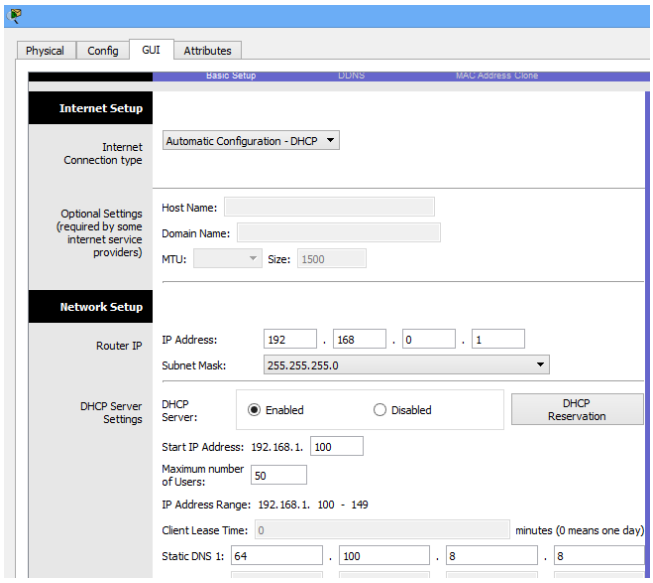
2) Establezca la máscara de subred **255.255.255.0**.

3) Habilite el servidor de DHCP.

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

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

c. 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**.

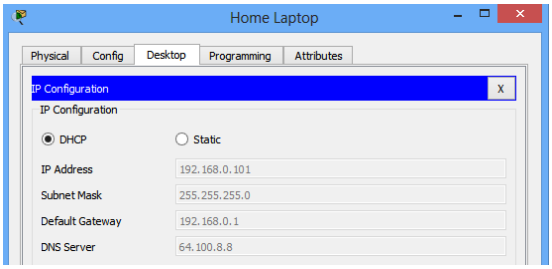
a. Haga clic en **Home Laptop** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration** (Escritorio > Configuración de IP).

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** .

Adicional a estos pasos hay que verificar que la pc portátil tenga conexión wifi para que así pueda obtener el direccionamiento dhcp

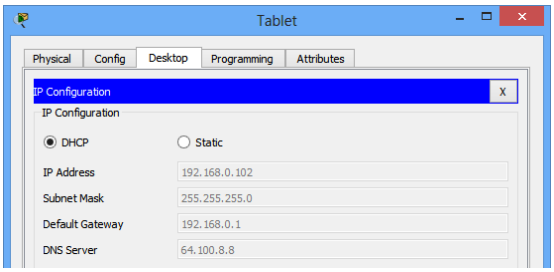


Paso 4: Solicitar direccionamiento DHCP para la tablet PC.

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.

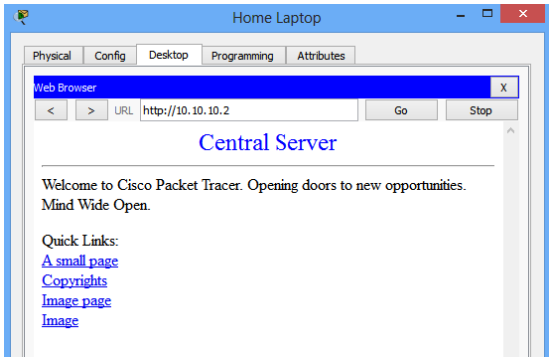
c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.

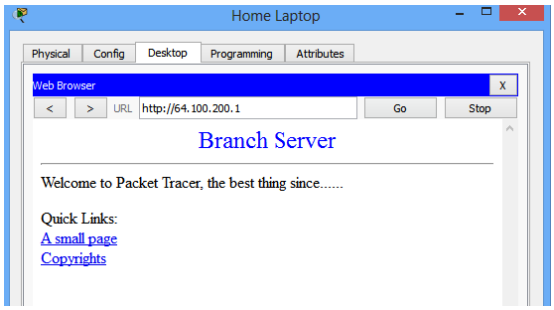


Paso 5: Probar el acceso a sitios Web.

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.

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.

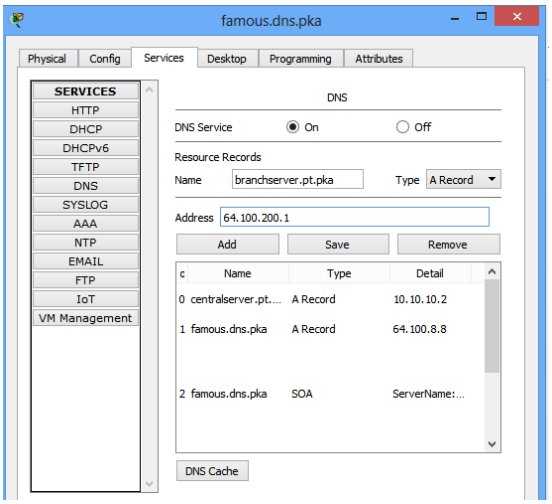
b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config** > **DNS**.

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**.



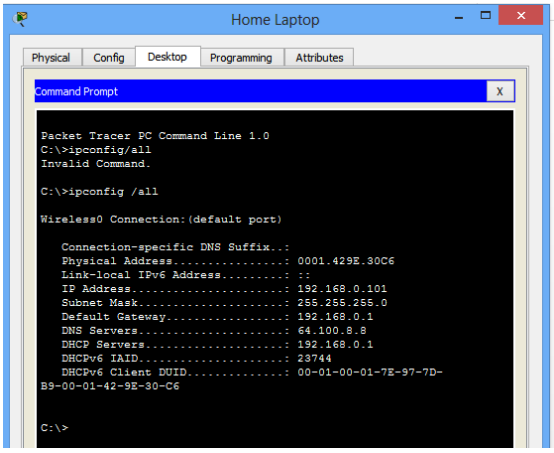
Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

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**.

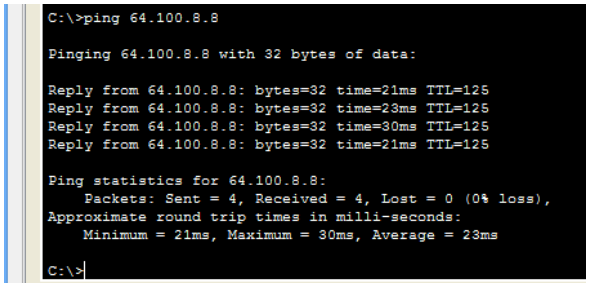
b. Si el explorador Web está abierto, ciérrelo y seleccione **Command Prompt** (Símbolo del sistema).

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

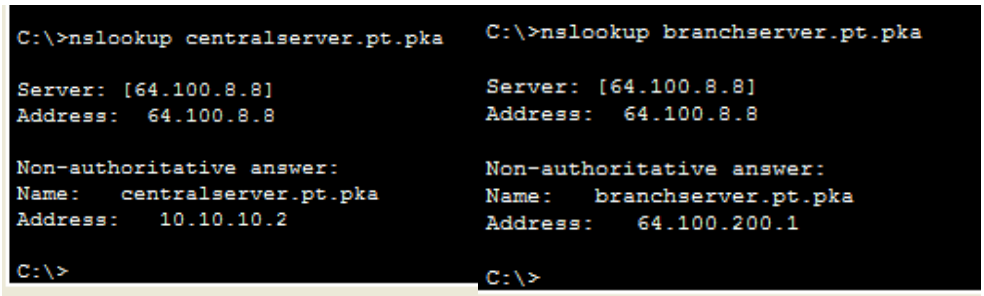


d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.

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.

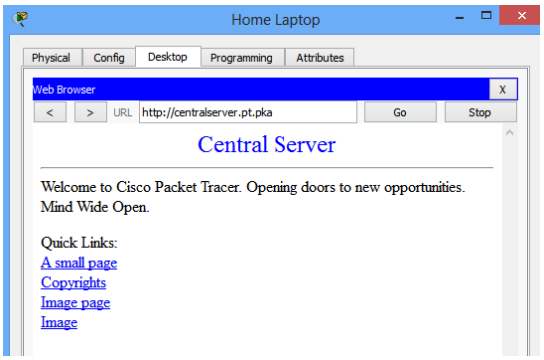


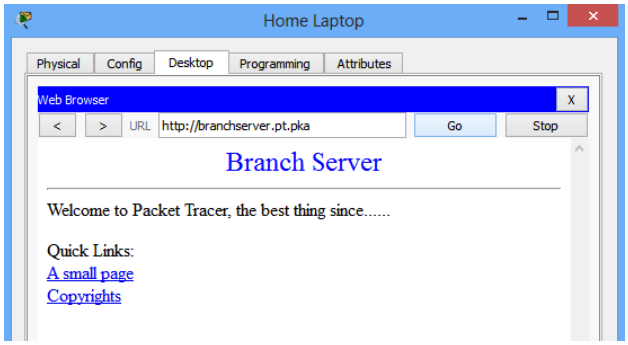
e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos **nslookup centralserver.pt.pka** y . Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.



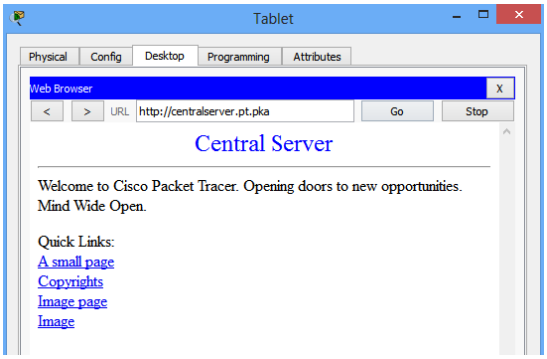
f. Cierre la ventana Command Prompt y haga clic en **Web Browser**. Verifique que **Home Laptop** o **Tablet** puedan acceder ahora a las páginas Web de **CentralServer** y **BranchServer**.

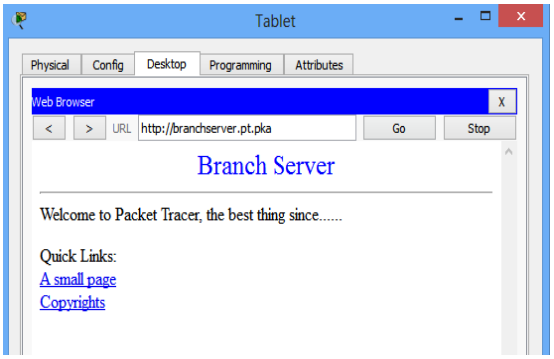
Desde home laptop





Desde tablet

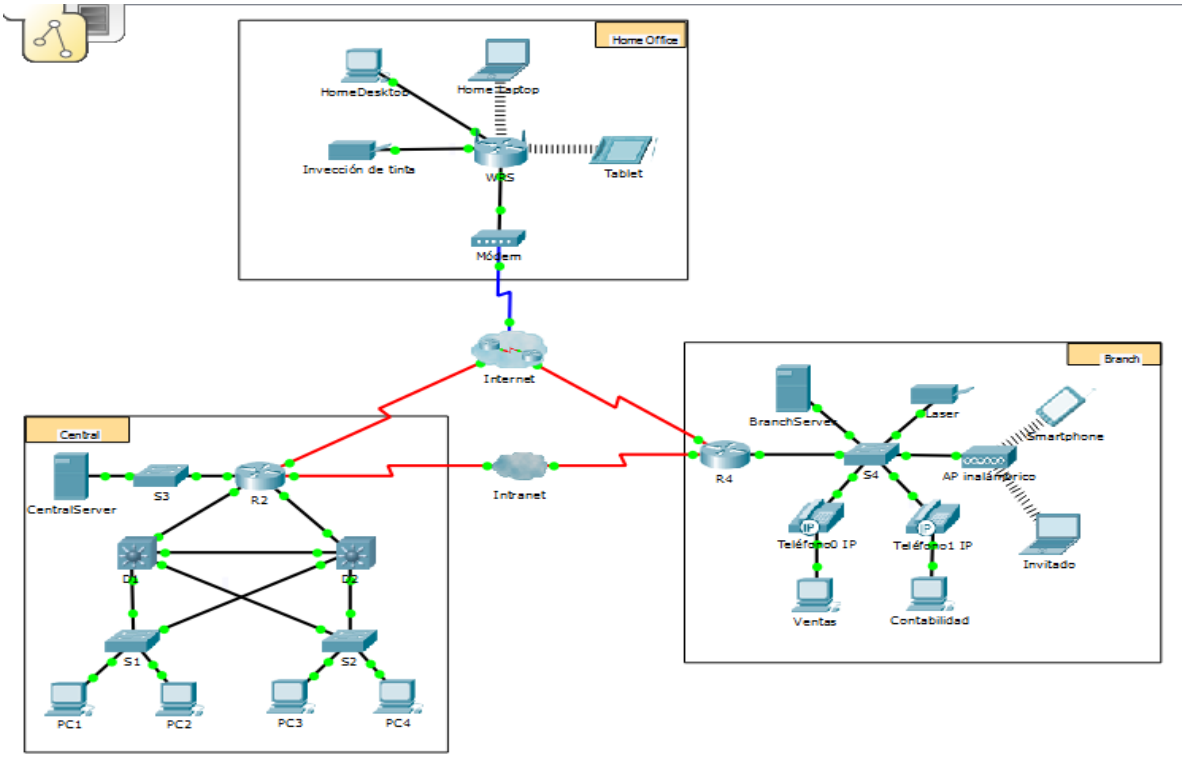




10.2.3.2 FTP Instructions IG

Packet Tracer: Servidores FTP

Topología



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

Parte 1: Configurar servicios FTP en los servidores

Paso 1: Configurar el servicio FTP en CentralServer.

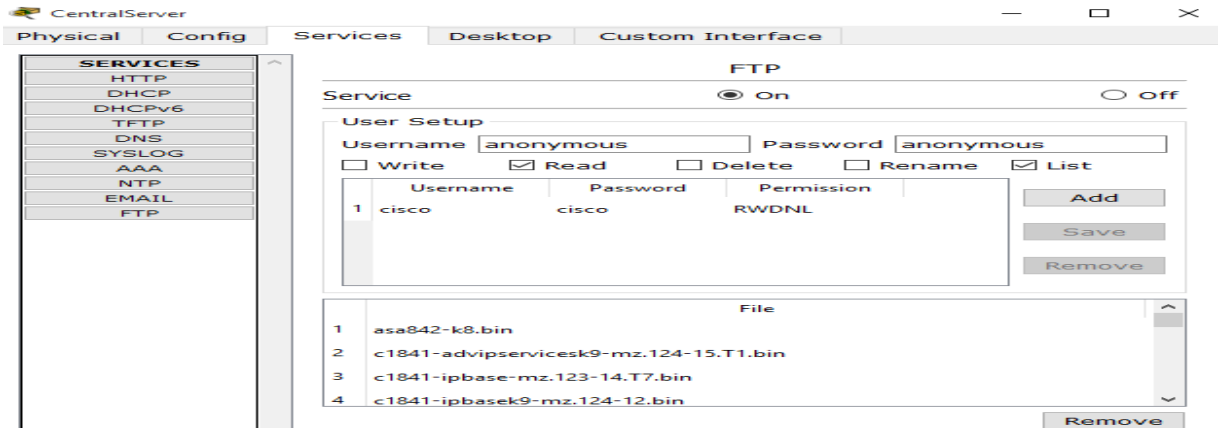
a. Haga clic en **CentralServer** > ficha **Config** > **FTP**.

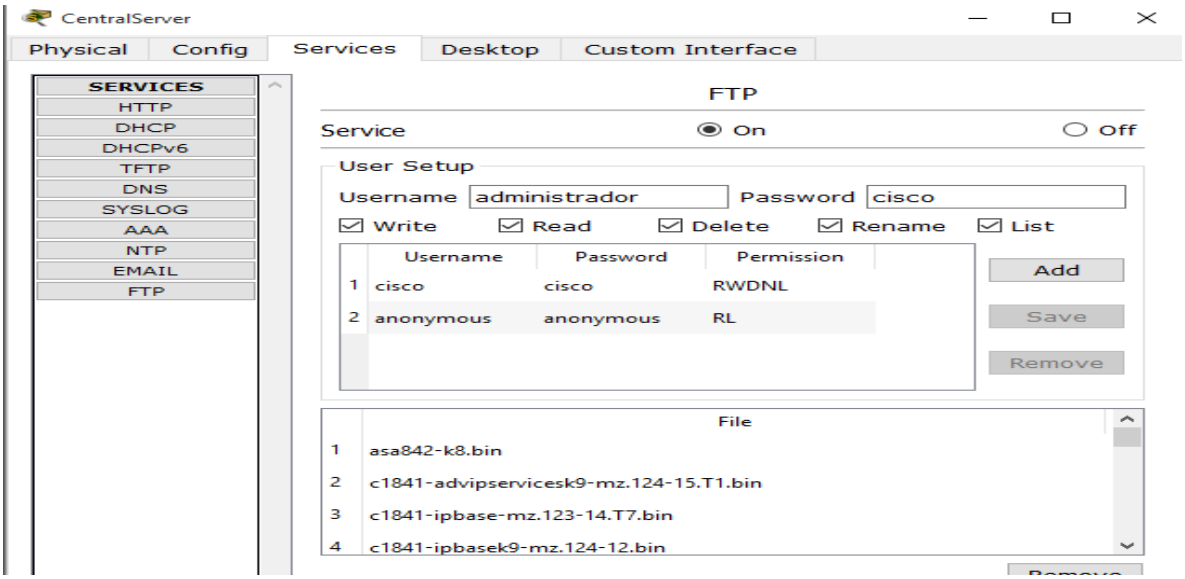
b. Haga clic en **On** (Activar) para habilitar el servicio FTP.

c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario.

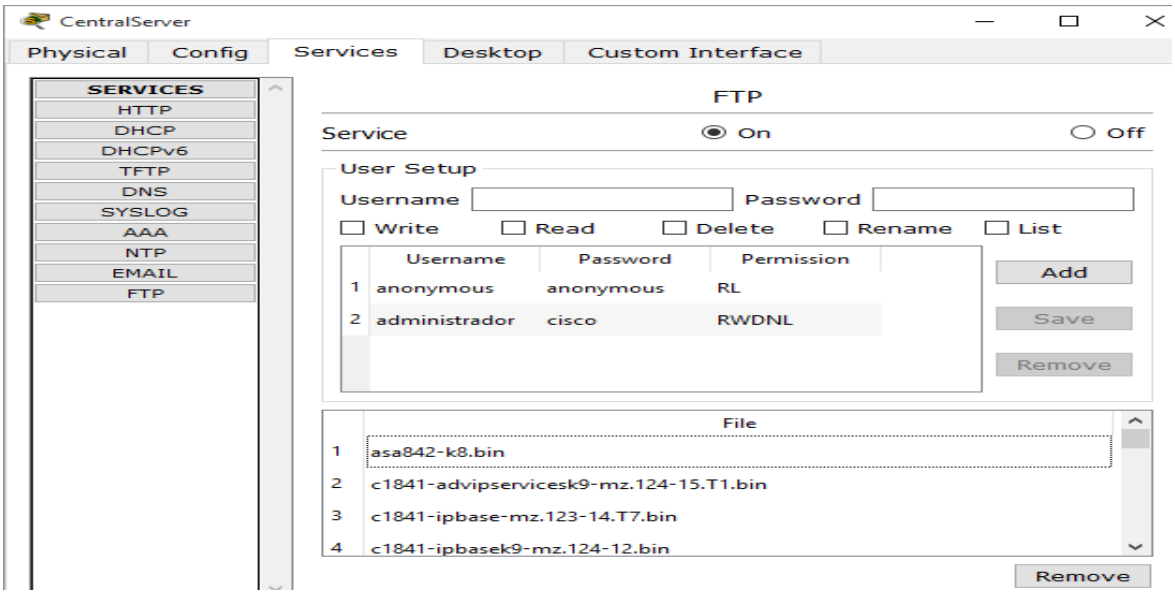
Haga clic en el botón **+** para agregar la cuenta:

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

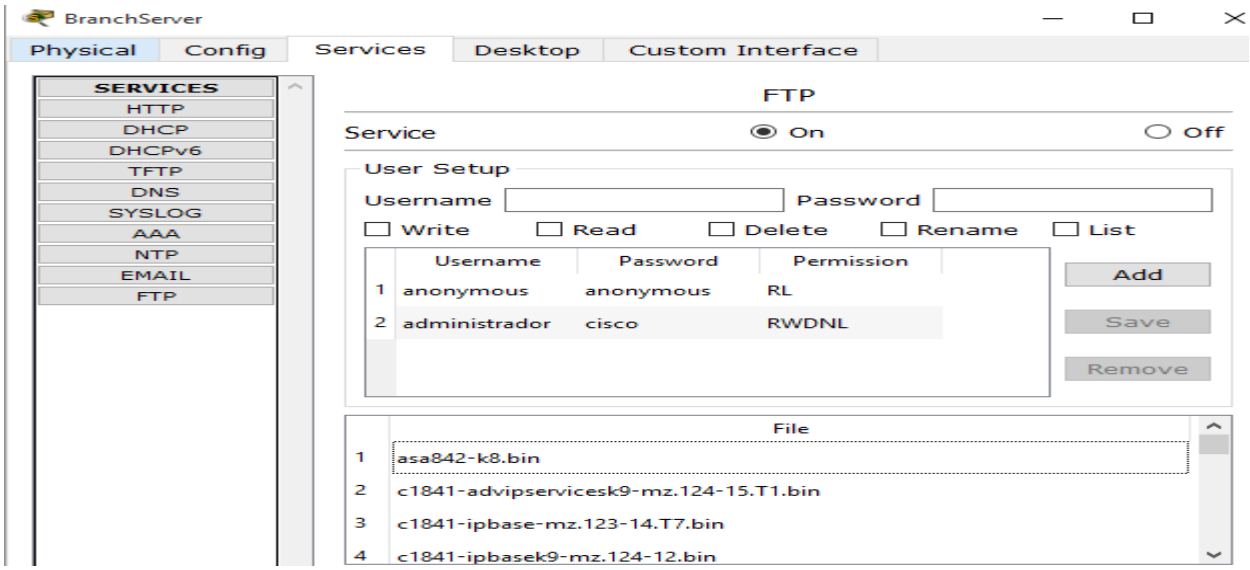




d. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón **-** para eliminarla. Cierre la ventana de configuración de la CentralServer.



Paso 2: Configurar el servicio FTP en BranchServer.
Repita el paso 1 en **BranchServer**.



Parte 2: Subir un archivo al servidor FTP

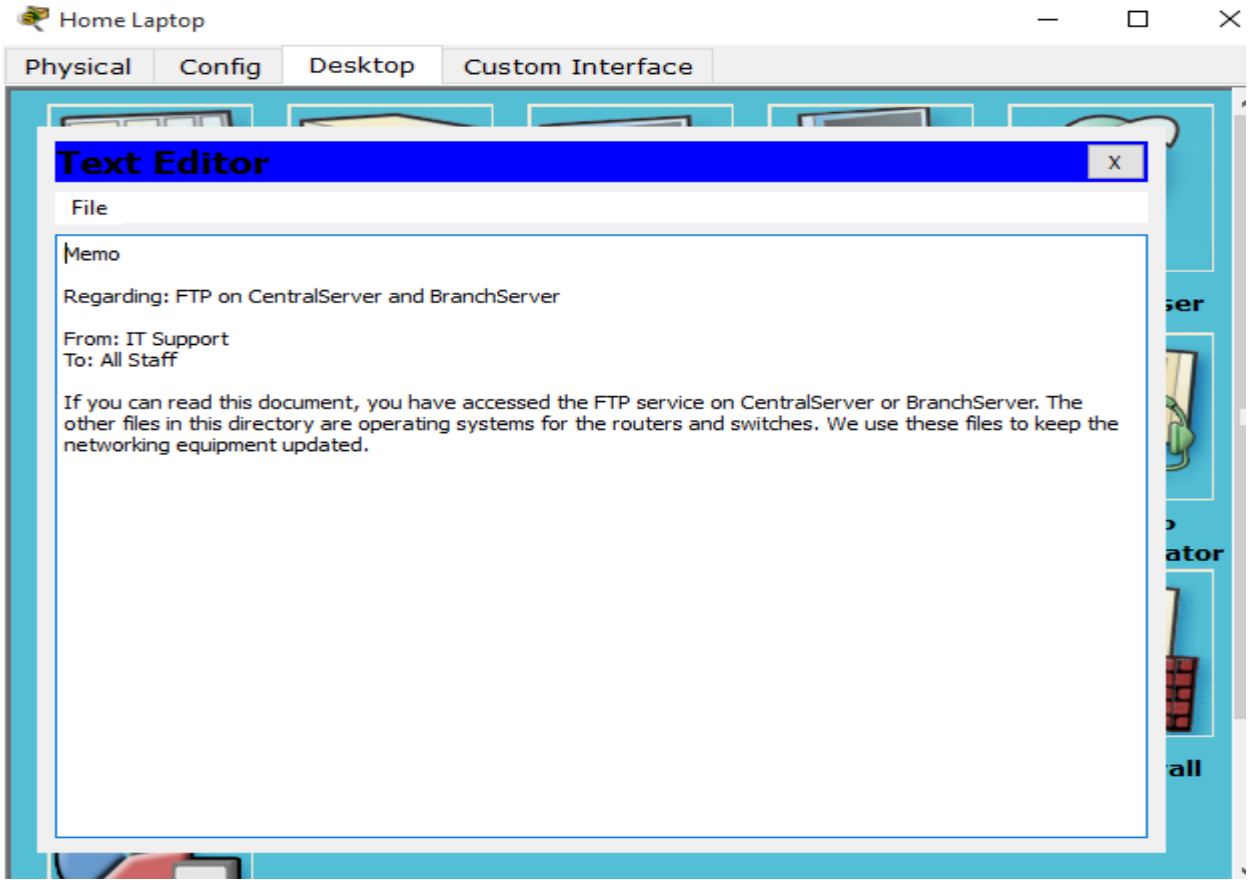
Paso 1: Transferir el archivo README.txt de la computadora portátil doméstica a CentralServer

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.

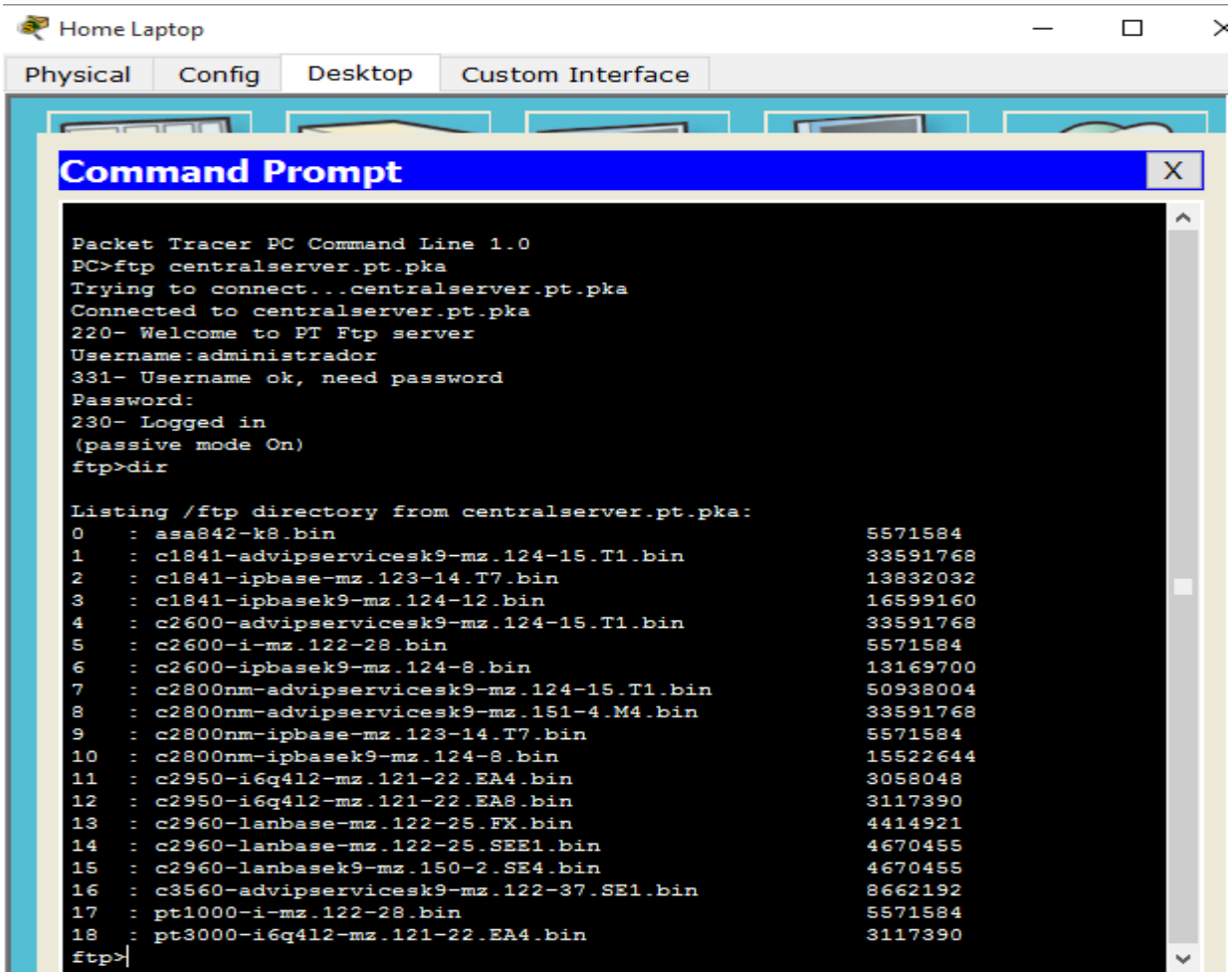


c. En la ficha **Desktop**, abra la ventana del símbolo del sistema y siga estos pasos:
1) Escriba **ftp centralserver.pt.pka** . Espere algunos segundos mientras se conecta el cliente.

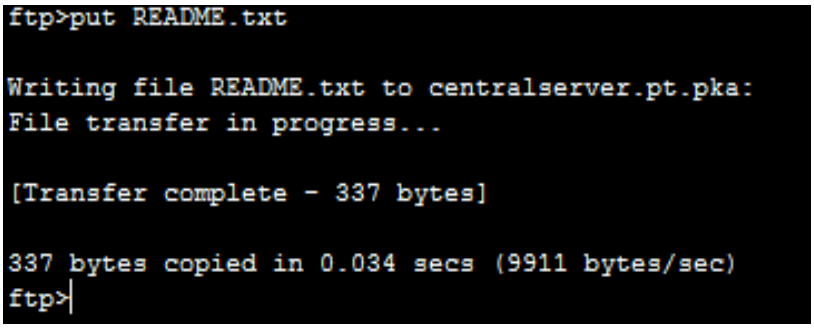
Nota: dado que Packet Tracer es una simulación, FTP puede tardar hasta 30 segundos en conectarse la primera vez.

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

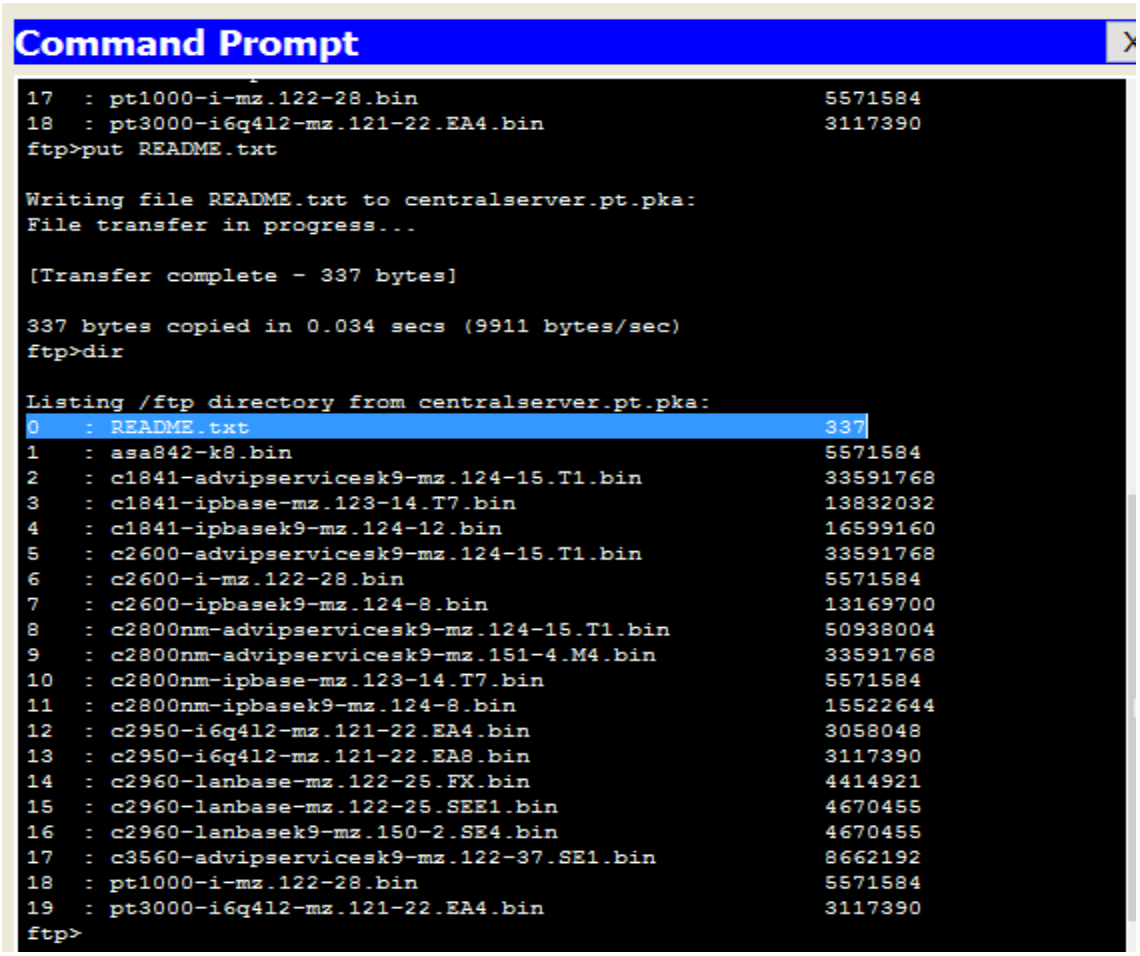
3) La petición de entrada cambia a ftp>. Enumere el contenido del directorio escribiendo **dir.** Se muestra el directorio de archivos en **CentralServer** .



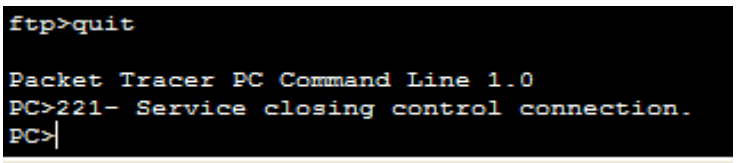
4) Transfiera el archivo README.txt: en la petición de entrada ftp>, escriba **put README.txt**. El archivo README.txt se transfiere de la computadora portátil doméstica a **CentralServer**.



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.

```
PC>ftp branchserver.pt.pka
Trying to connect...branchserver.pt.pka
Connected to branchserver.pt.pka
220- Welcome to PT Ftp server
Username:administrador
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from branchserver.pt.pka:
0    : asa842-k8.bin                                  5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin         33591768
2    : c1841-ipbase-mz.123-14.T7.bin                  13832032
3    : c1841-ipbasek9-mz.124-12.bin                   16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin         33591768
5    : c2600-i-mz.122-28.bin                          5571584
6    : c2600-ipbasek9-mz.124-8.bin                    13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin       50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin        33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin                5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                  15522644
11   : c2950-i6q4l2-mz.121-22.EA4.bin                 3058048
12   : c2950-i6q4l2-mz.121-22.EA8.bin                 3117390
13   : c2960-lanbase-mz.122-25.FX.bin                 4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin               4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin               4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin        8662192
17   : pt1000-i-mz.122-28.bin                         5571584
18   : pt3000-i6q4l2-mz.121-22.EA4.bin                3117390
```

```
ftp>put README.txt

Writing file README.txt to branchserver.pt.pka:
File transfer in progress...

[Transfer complete - 337 bytes]

337 bytes copied in 0.03 secs (11233 bytes/sec)
ftp>dir

Listing /ftp directory from branchserver.pt.pka:
0    : README.txt                                     337
1    : asa842-k8.bin                                  5571584
2    : c1841-advipservicesk9-mz.124-15.T1.bin         33591768
3    : c1841-ipbase-mz.123-14.T7.bin                  13832032
4    : c1841-ipbasek9-mz.124-12.bin                   16599160
5    : c2600-advipservicesk9-mz.124-15.T1.bin         33591768
6    : c2600-i-mz.122-28.bin                          5571584
7    : c2600-ipbasek9-mz.124-8.bin                    13169700
8    : c2800nm-advipservicesk9-mz.124-15.T1.bin       50938004
9    : c2800nm-advipservicesk9-mz.151-4.M4.bin        33591768
10   : c2800nm-ipbase-mz.123-14.T7.bin                5571584
11   : c2800nm-ipbasek9-mz.124-8.bin                  15522644
12   : c2950-i6q4l2-mz.121-22.EA4.bin                 3058048
13   : c2950-i6q4l2-mz.121-22.EA8.bin                 3117390
14   : c2960-lanbase-mz.122-25.FX.bin                 4414921
15   : c2960-lanbase-mz.122-25.SEE1.bin               4670455
16   : c2960-lanbasek9-mz.150-2.SE4.bin               4670455
17   : c3560-advipservicesk9-mz.122-37.SE1.bin        8662192
18   : pt1000-i-mz.122-28.bin                         5571584
19   : pt3000-i6q4l2-mz.121-22.EA4.bin                3117390
ftp>
```

Parte 3: Descargar un archivo del servidor FTP

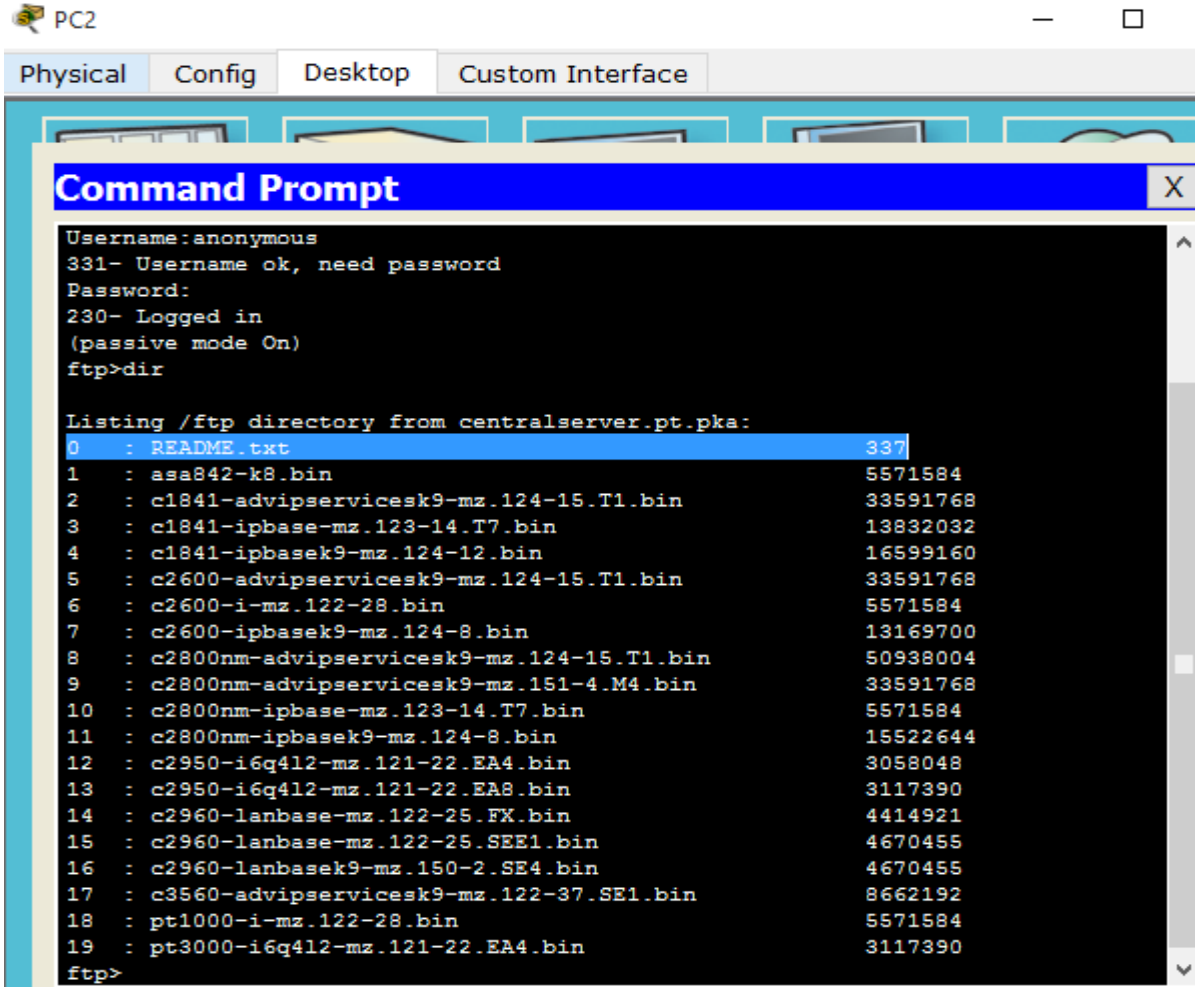
Paso 1: Transferir README.txt de CentralServer a la PC2

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:

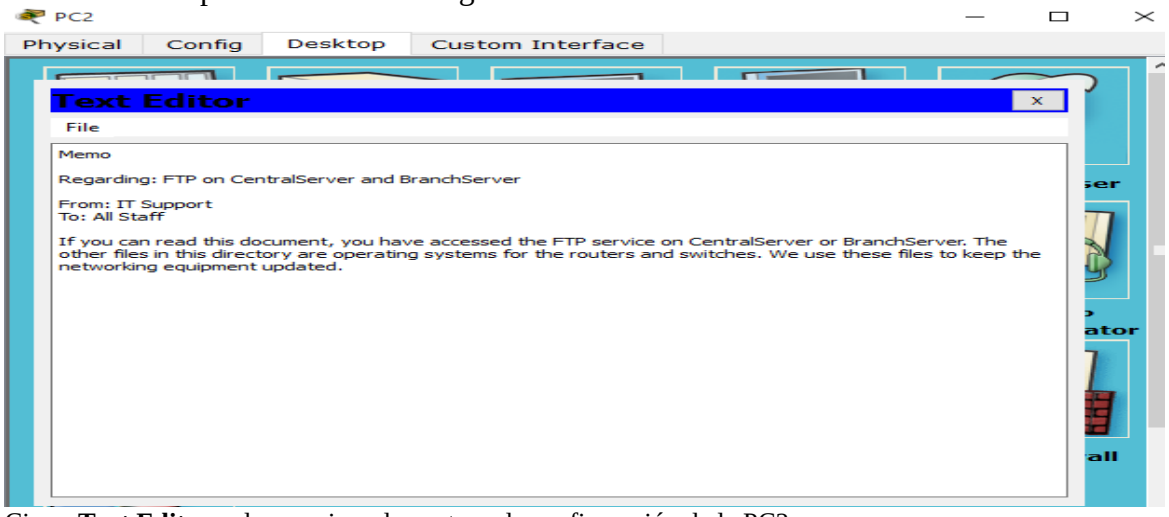
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...
%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or Permission denied)
(550-Requested action not taken. permission denied).

```
ftp>get README.txt

Reading file README.txt from centralserver.pt.pka:
File transfer in progress...

[Transfer complete - 337 bytes]

337 bytes copied in 0 secs
ftp>put sampleFile.txt

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).

ftp>
```

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.

```
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>dir

 Volume in drive C has no label.
 Volume Serial Number is 5E12-4AF3
 Directory of C:\
  12/31/1969  19:0 PM       337                 README.txt
  2/7/2106    1:28 PM       26                  sampleFile.txt
                            363 bytes           2 File(s)
PC>
```

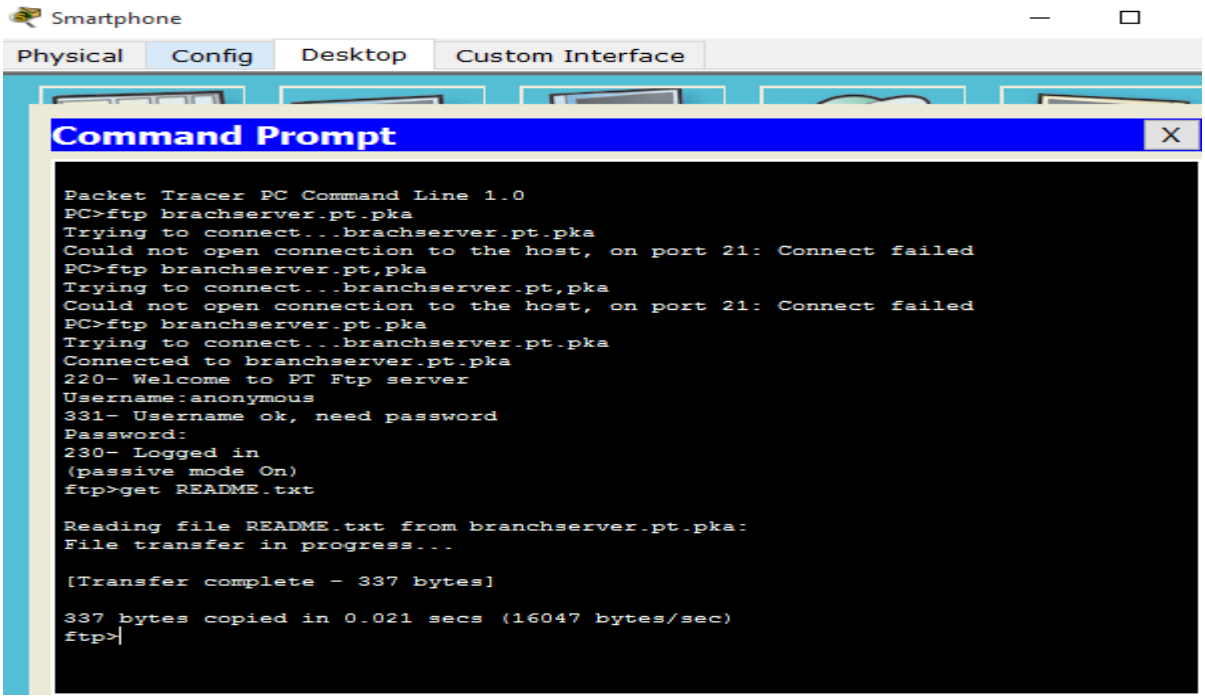
8) Cierre la ventana de línea de comandos.
b. En la ficha **Desktop**, abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.



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**.



10.4.1.2 Multiuser – Tutorial Instructions IG

Función multiusario de Packet Tracer: Tutorial

Topología

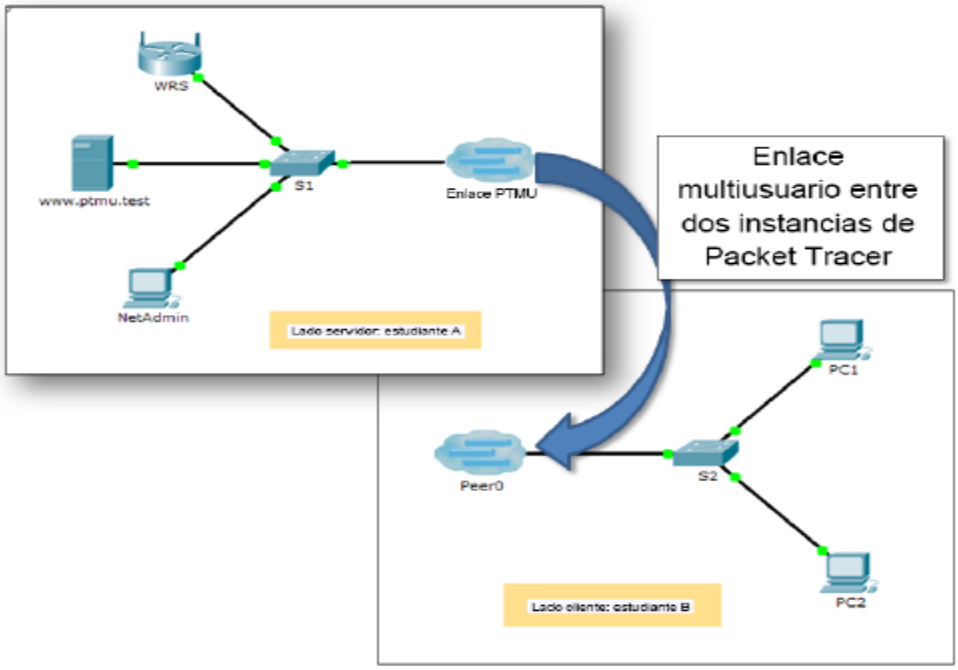


Tabla de direccionamiento

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

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

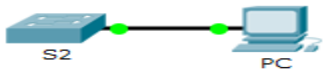
Paso 1: Seleccionar un compañero y determinar el rol para cada estudiante

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.

Server Side - Student A

- 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.**



Client Side - Student B

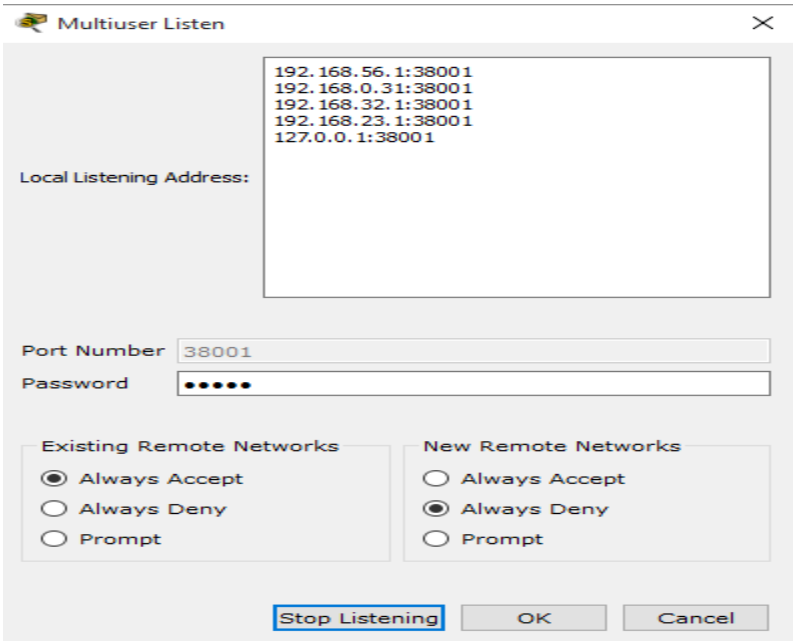
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso2 : Jugador del lado servidor: configurar el lado servidor del enlace PTMU

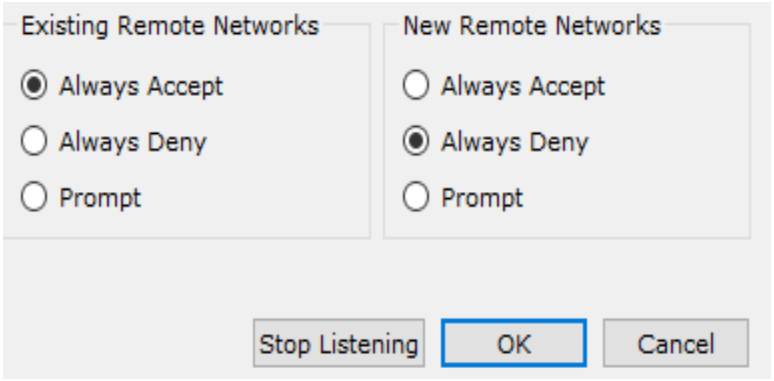
El jugador del lado cliente debe contar con la dirección IP, el número de puerto y la contraseña utilizados por el jugador del lado servidor para poder crear una conexión con el jugador del lado servidor.

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).



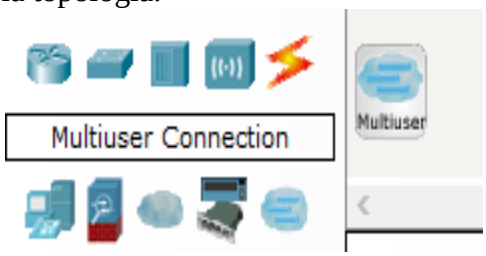
2) Tiene dos Local Listening Addresses (Direcciones de escucha locales). Si se indican más de dos direcciones, utilice solo las primeras dos. La primera es la dirección IP real de la máquina local del jugador del lado servidor. Es la dirección IP que utiliza su PC para enviar y recibir datos. La otra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

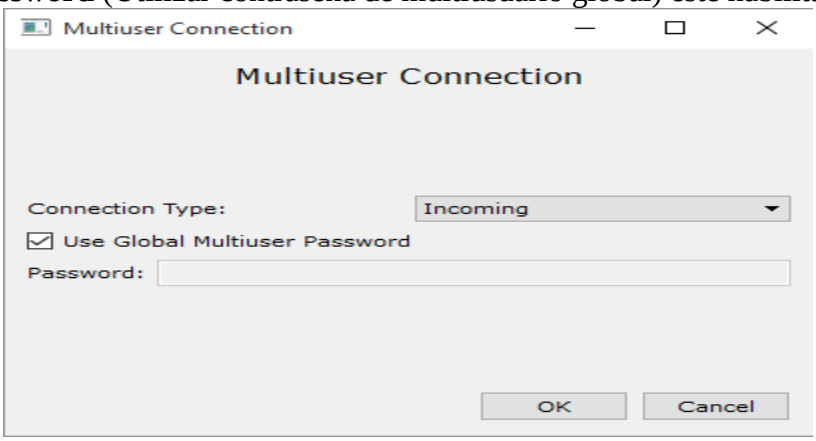
8) Haga clic en **OK** (Aceptar).

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.



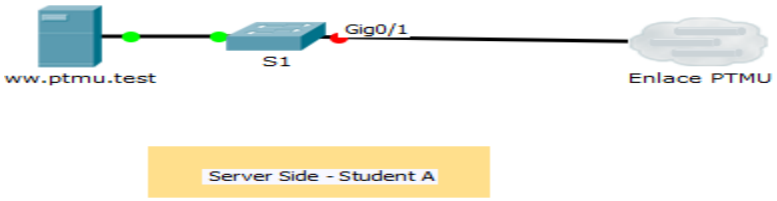
c. Haga clic en el nombre **Peer0** y cámbielo por **Enlace PTMU** (distingue mayúsculas de minúsculas).

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).

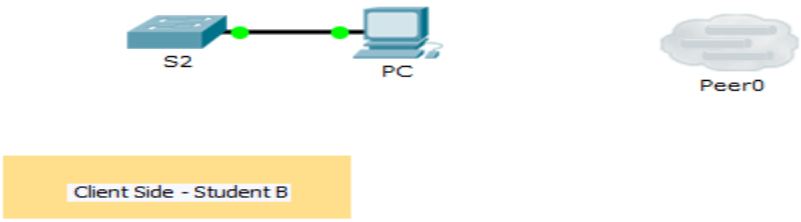


Paso 3: Jugador del lado cliente: configurar el lado cliente del enlace PTMU

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

Dirección IP: 192.168.56.1
Número de puerto: 38001
Contraseña (**cisco**, de manera predeterminada) cisco

b. El jugador del lado cliente debe agregar una **red remota** a la topología mediante las siguientes instrucciones: haga clic en el ícono **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).

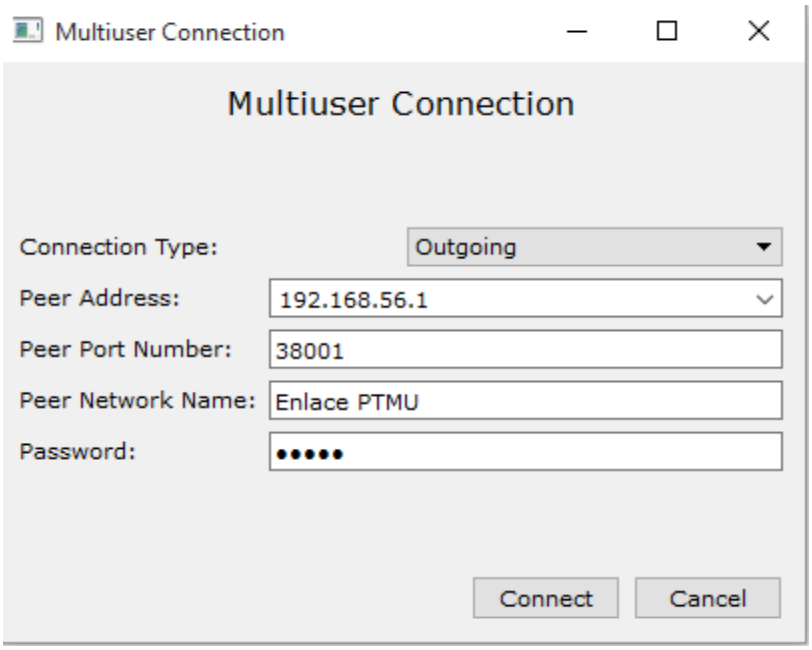
1) En el campo Peer Address (Dirección del punto), introduzca la dirección IP del lado servidor que registró en el paso 3a.

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.

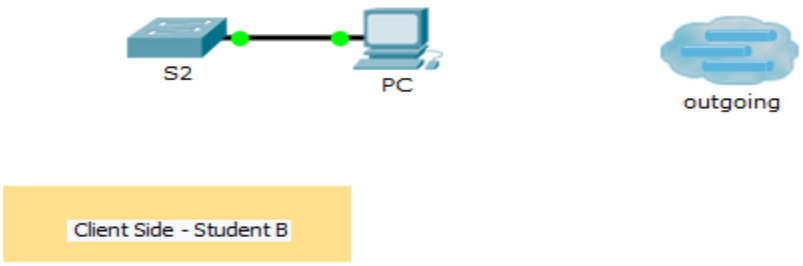
3) En el campo Peer Network Name (Nombre de red del punto), introduzca **Enlace PTMU**. Este campo distingue mayúsculas de minúsculas.

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

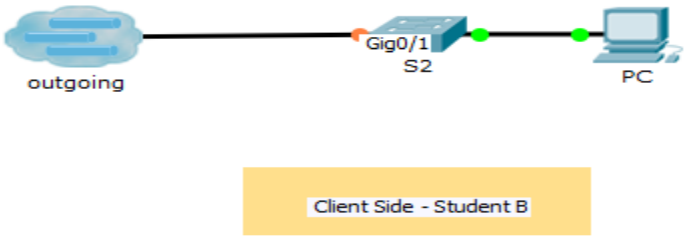
5) Haga clic en **Connect** (Conectar).



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

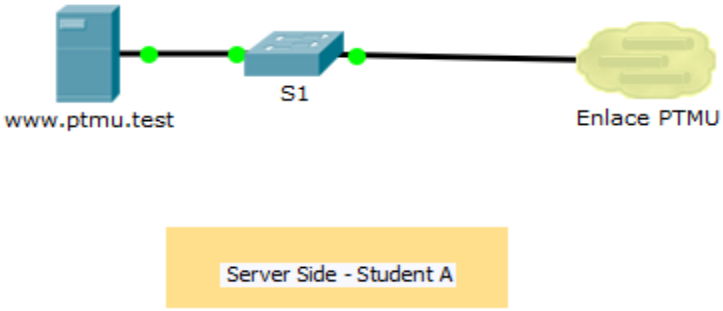


e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).
f. Haga clic en el **S2** y elija la conexión **GigabitEthernet0/1**. A continuación, haga clic en **Peer0** > **Link 0 (S1 GigabitEthernet 0/1)**.



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

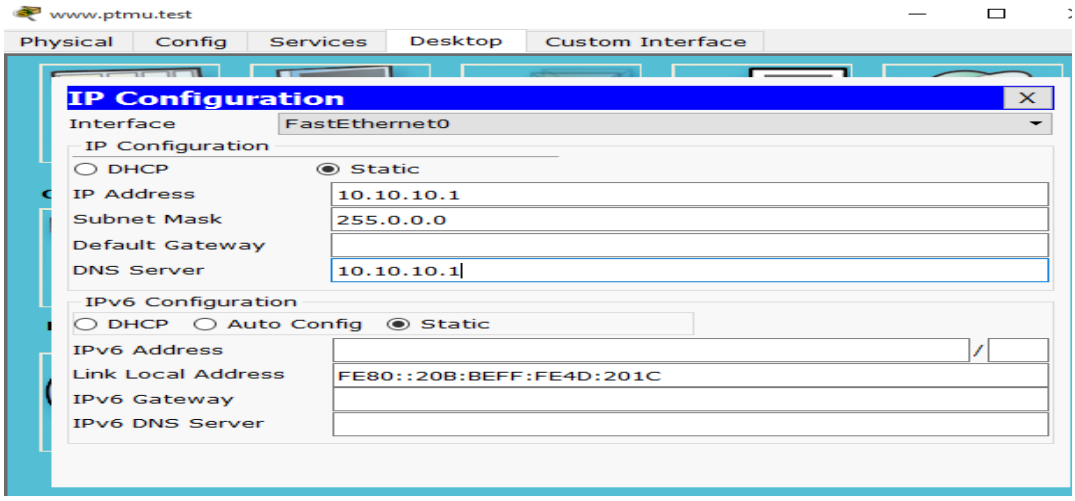
enlace entre el switch y la nube pasa de color ámbar a verde. El enlace de multiusuario está establecido y listo para probar.



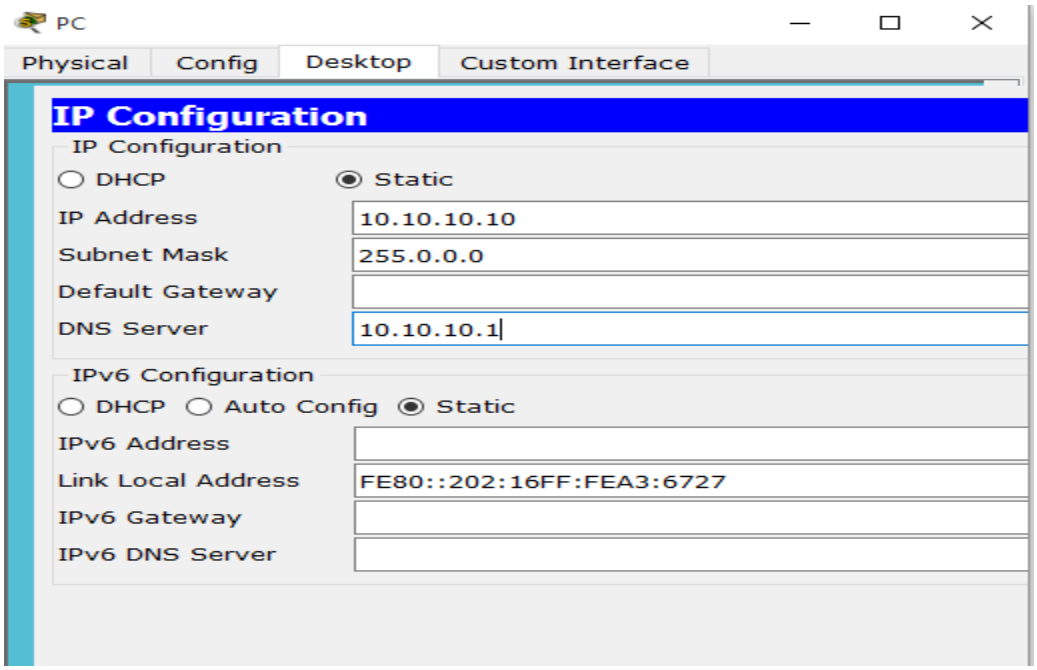
Parte 2: Verificar la conectividad a través de una conexión multiusuario local

Paso 1: Configurar el direccionamiento IP

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

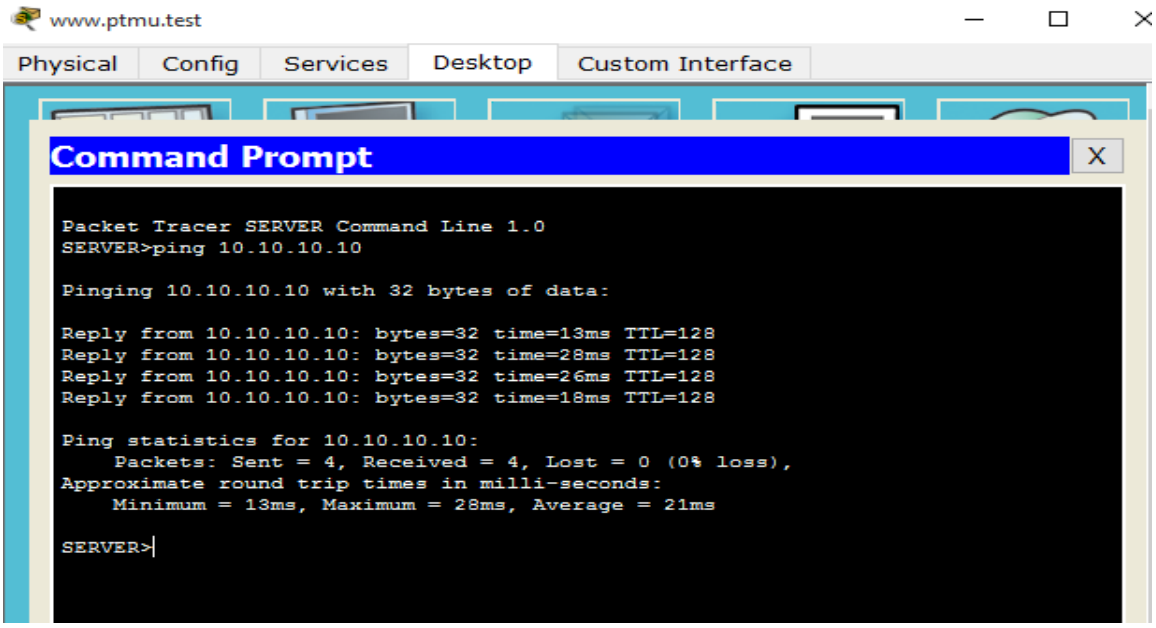


b. El jugador del lado cliente configura la PC con la dirección IP **10.10.10.10**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.

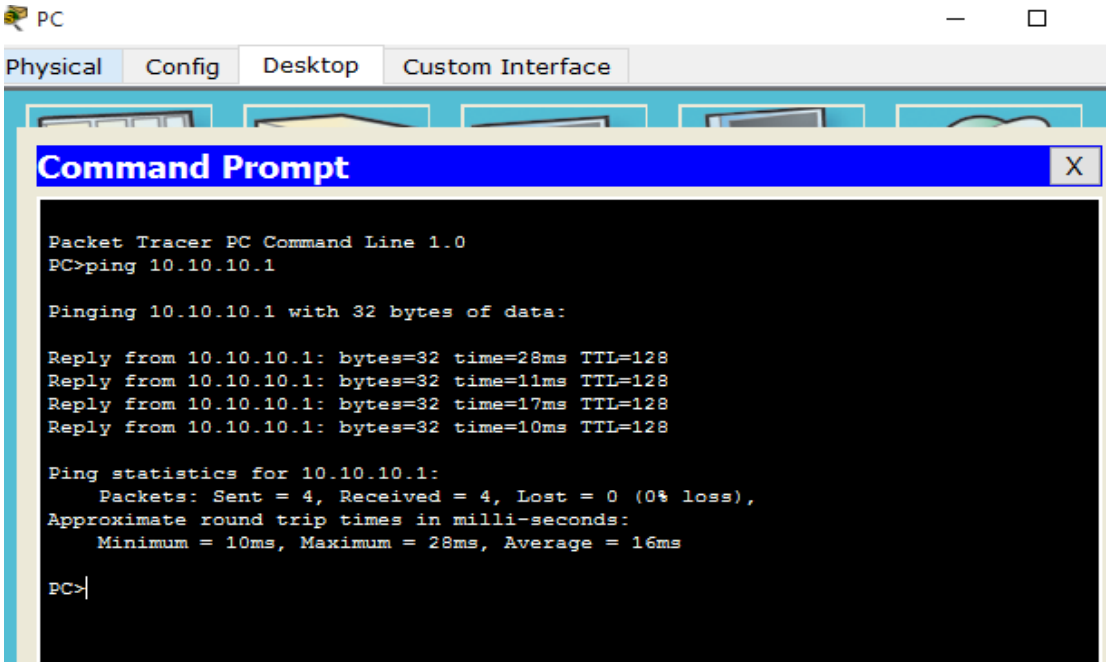


Paso 2: Verificar la conectividad y acceder a una página Web desde el lado servidor

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

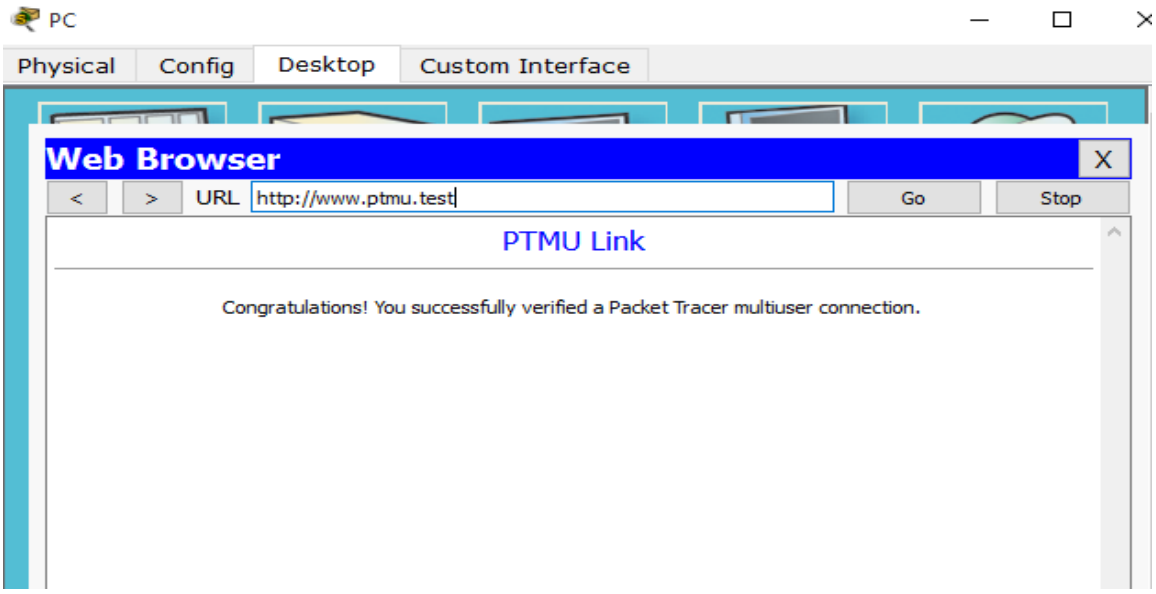


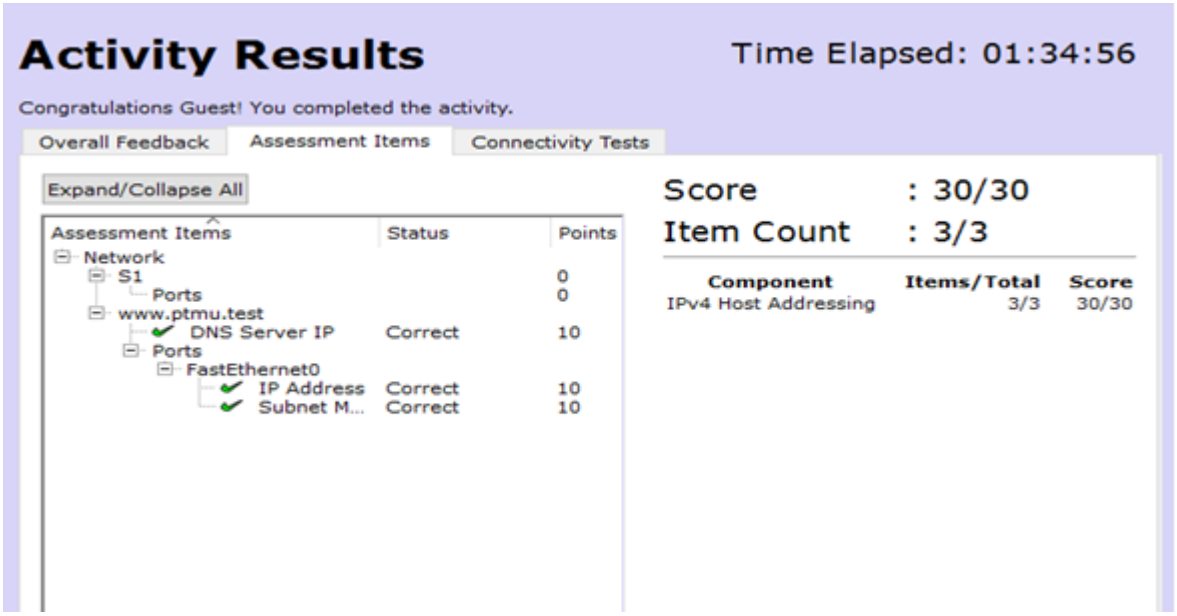
b. El jugador del lado cliente ahora debe poder hacer ping al servidor de **www.ptmu.test**.



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? **R=/**

Congratulations! You successfully verified a Packet Tracer multiuser connection (Felicidades. Verificó correctamente una conexión multiusuario de Packet Tracer)




Activity Results
Time Elapsed: 01:34:56
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Network
S1
0
Ports
0
www.ptmu.test
DNS Server IP
Correct
10
Ports
FastEthernet0
IP Address
Correct
10
Subnet M...
Correct
10
Score : 30/30
Item Count : 3/3
Component
Items/Total
Score
IPv4 Host Addressing
3/3
30/30

10.4.1.3 Multiuser – Implement Services Instructions IG

Multiusuario de Packet Tracer: Implementación de servicios (10.4.1.3)

Topología

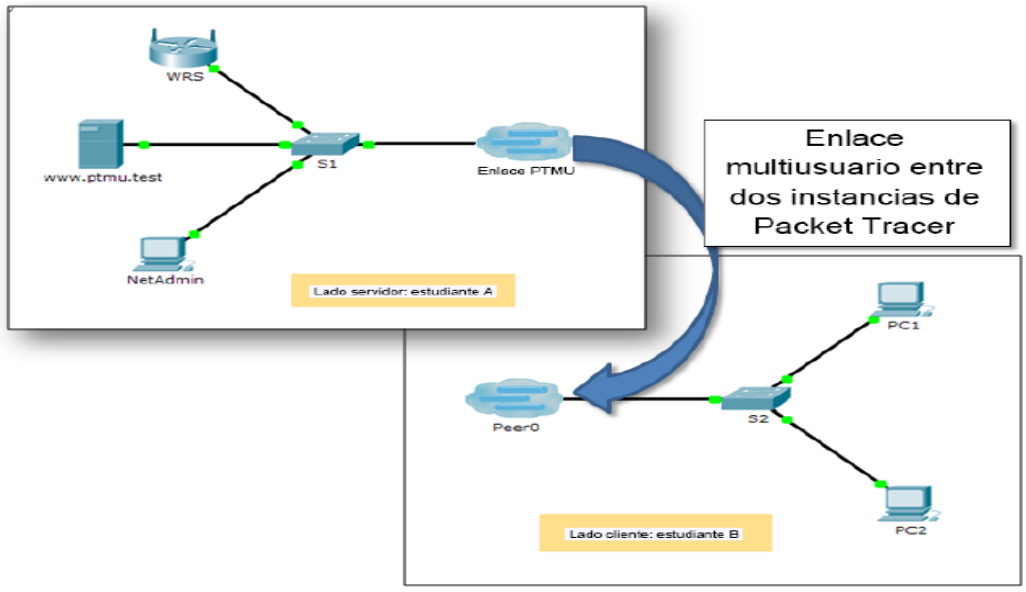


Tabla de direccionamiento

Dispositivo	Dirección IP	Máscara de subred
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.

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.

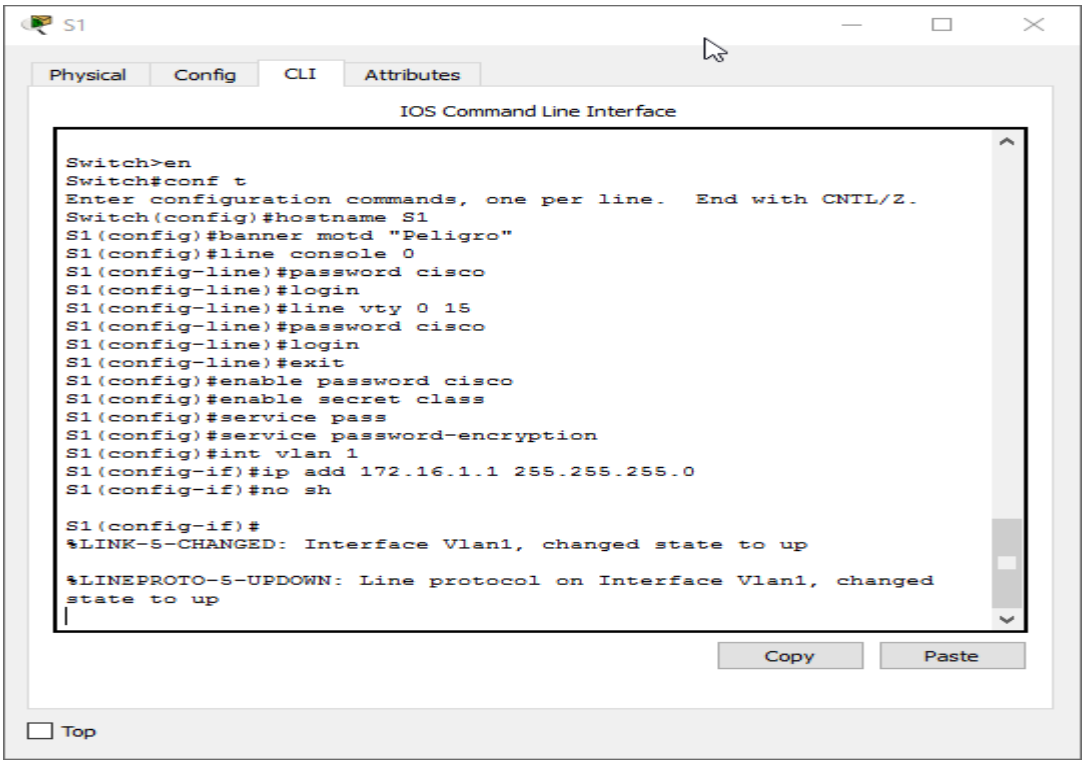
- El jugador del lado servidor abre el archivo **Packet Tracer Multiuser - Implement Services - Server Side.pka.**
- El jugador del lado cliente abre el archivo **Packet Tracer Multiuser - Implement Services - Client Side.pka.**

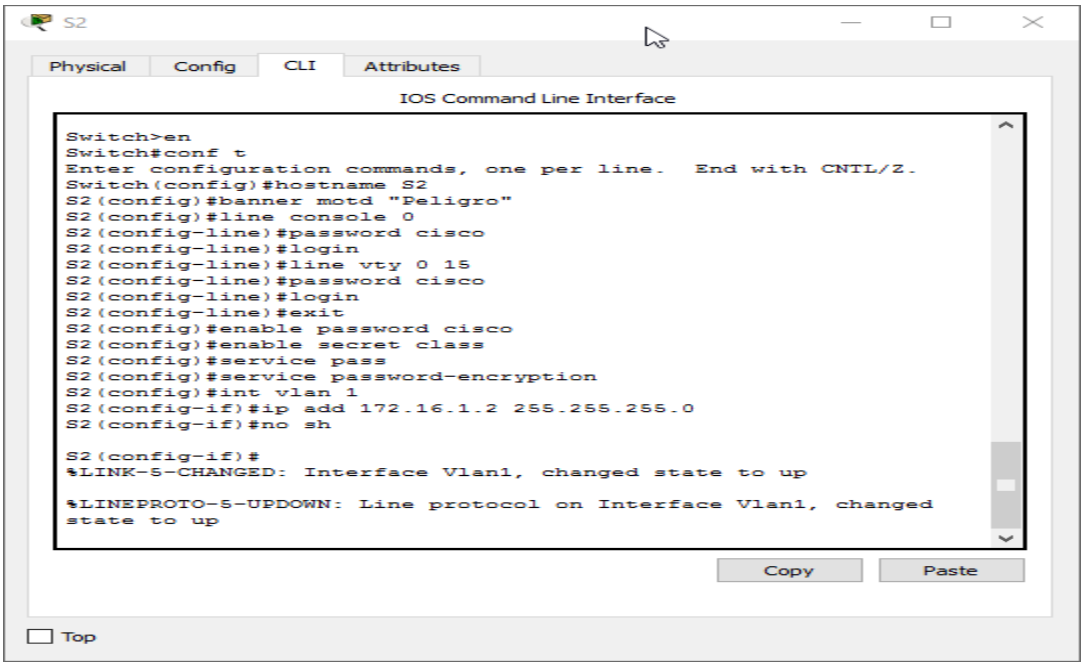
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

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 Addressing Table

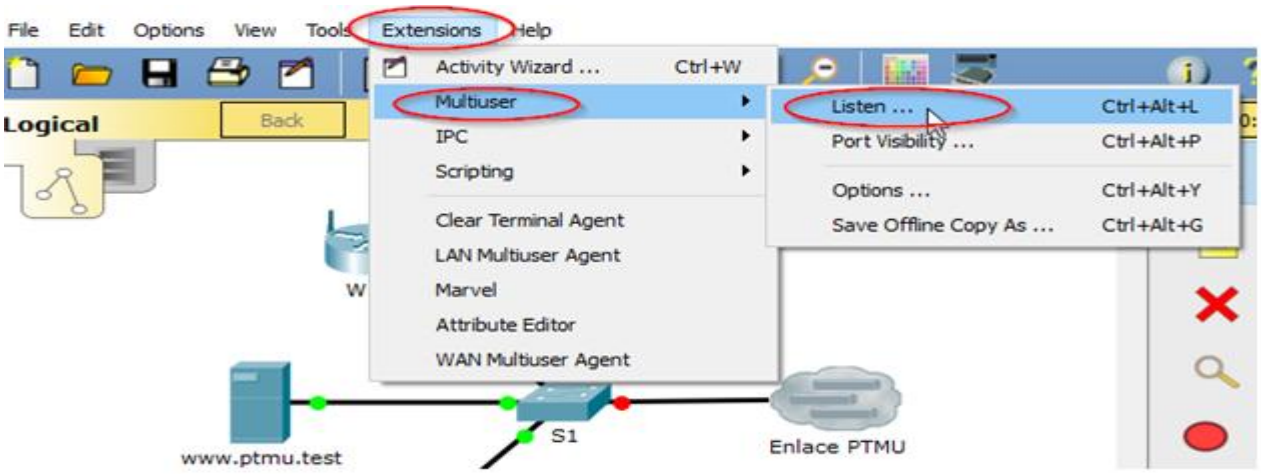


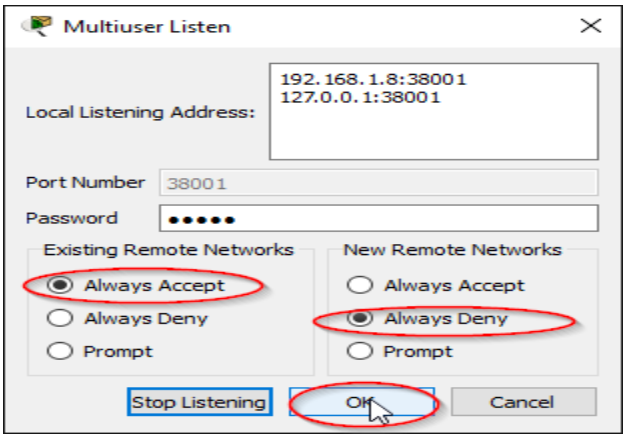


Paso 3: Jugador del lado servidor: Configurar el enlace PTMU y comunicar el direccionamiento

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:

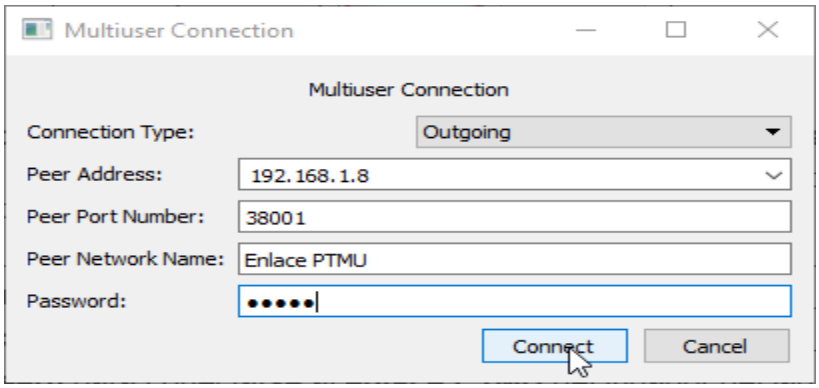
Dirección IP: 192.168.1.8

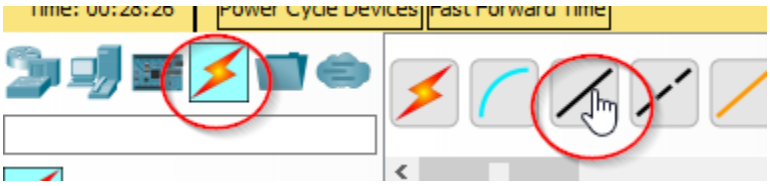
Número de puerto: 38001

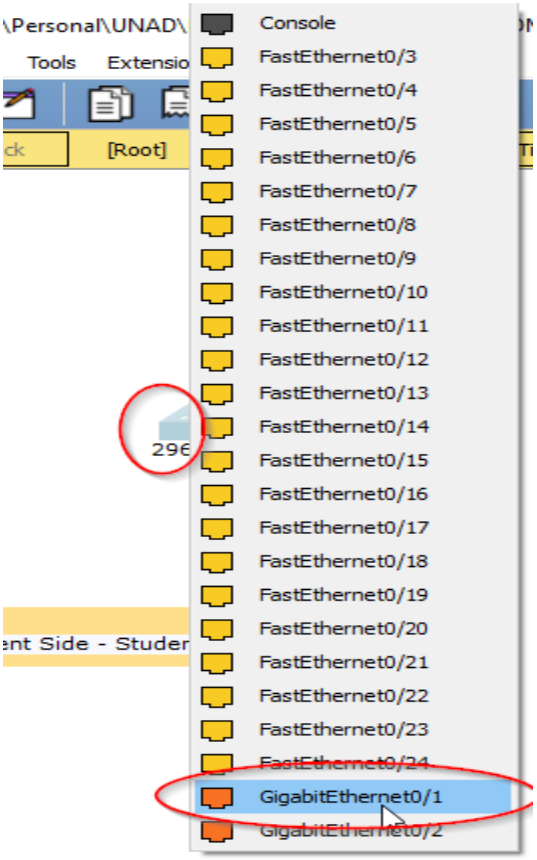
Contraseña (**cisco**, de manera predeterminada) cisco

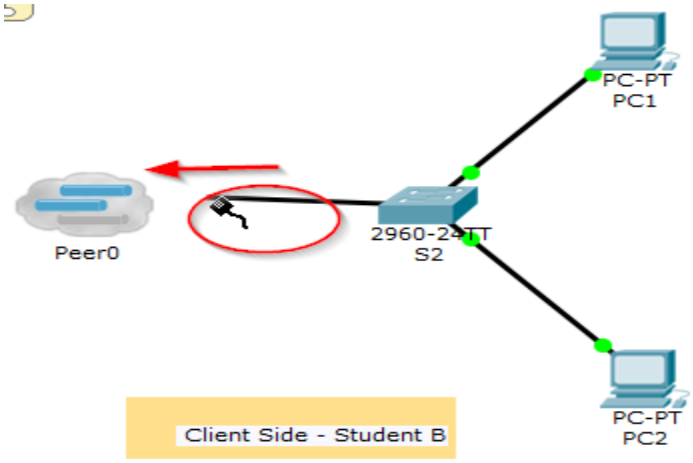
b. Configure **Peer0** para conectarse al **enlace PTMU** del jugador del lado servidor.

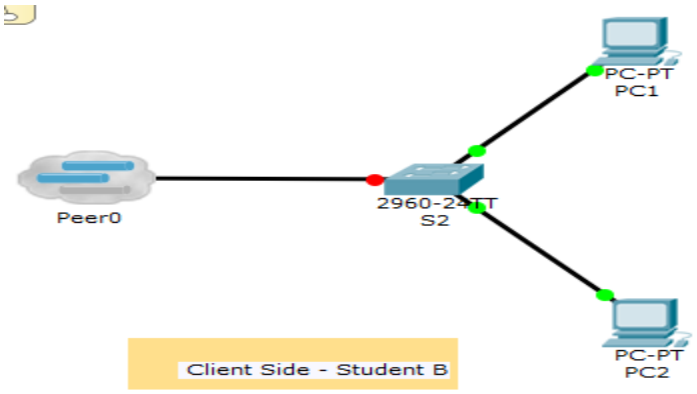
c. Conecte la **GigabitEthernet0/1** de **S2** al **Link0** en **Peer0**.





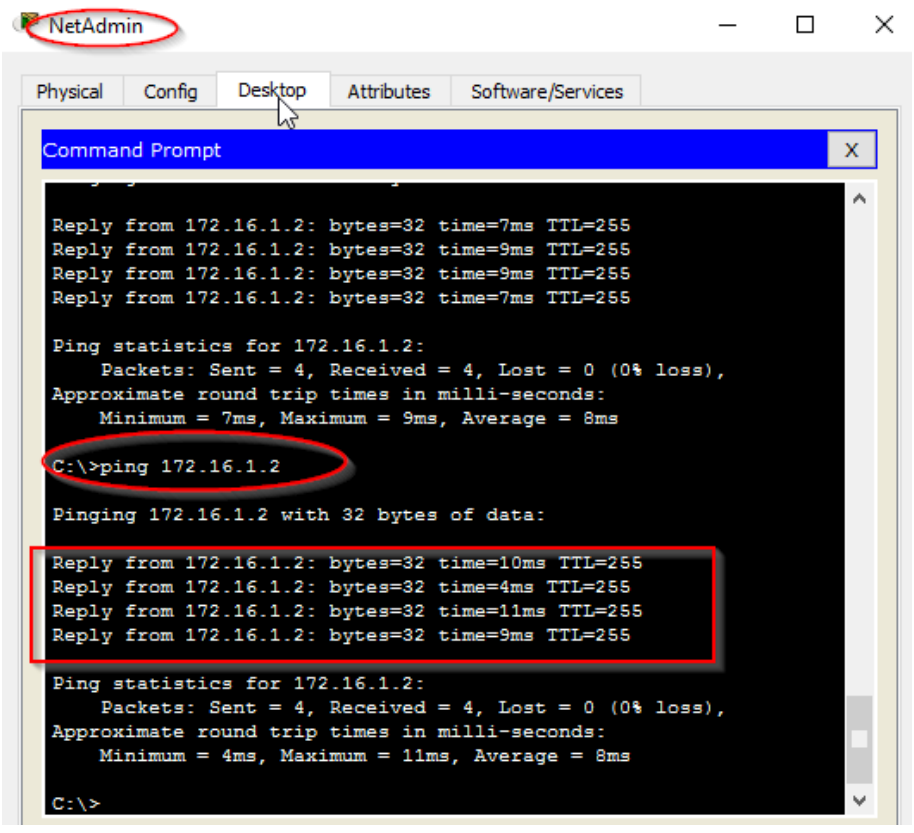

\Personal\UNAD\
Tools
Extensio
[Root]
Console
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
FastEthernet0/10
FastEthernet0/11
FastEthernet0/12
FastEthernet0/13
FastEthernet0/14
FastEthernet0/15
FastEthernet0/16
FastEthernet0/17
FastEthernet0/18
FastEthernet0/19
FastEthernet0/20
FastEthernet0/21
FastEthernet0/22
FastEthernet0/23
GigabitEthernet0/1


PC-PT
PC1
Peer0
2960-24TT
S2
PC-PT
PC2
Client Side - Student B

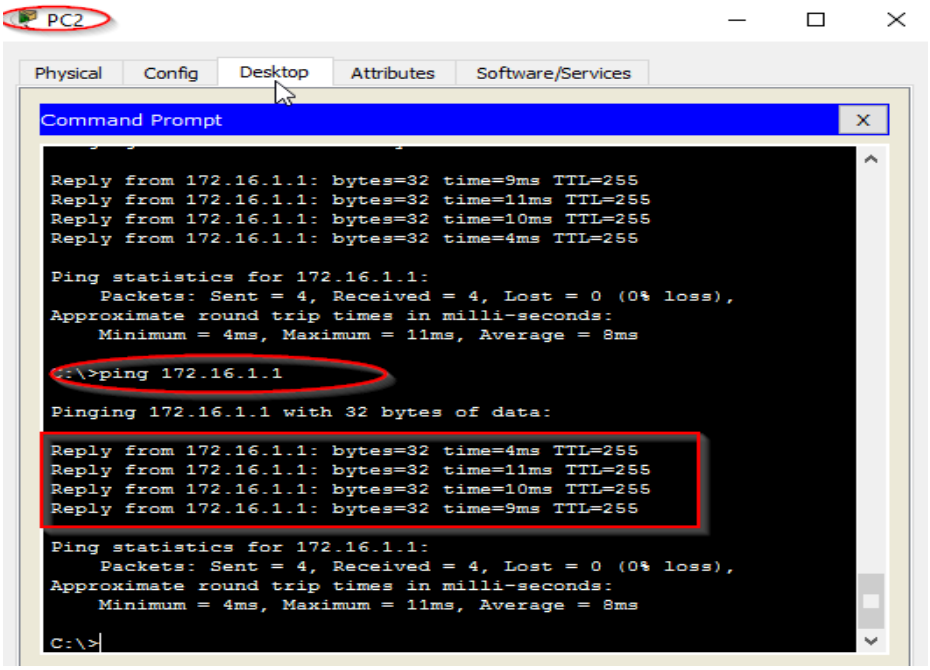


Paso 5: Verificar la conectividad a través de una conexión multiusuario local

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.

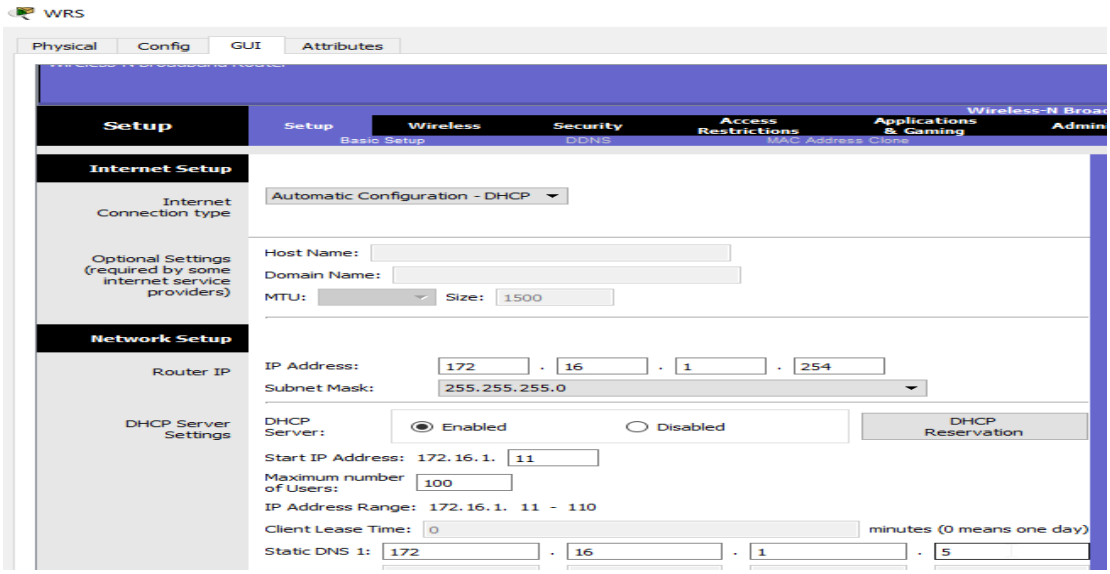


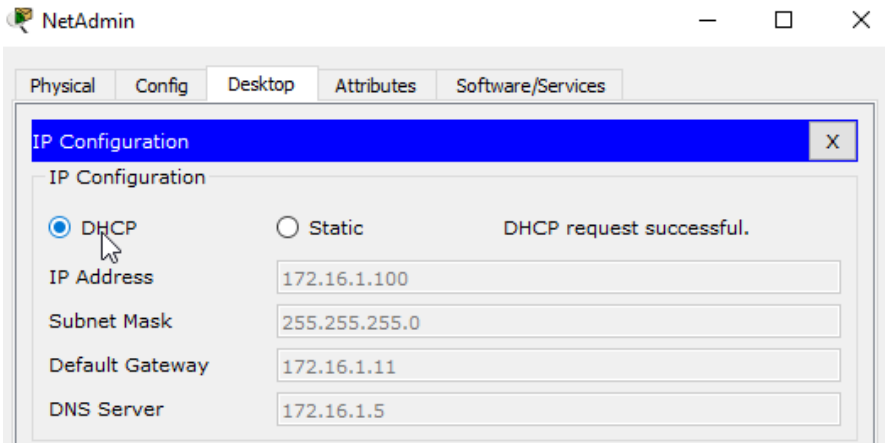
Parte 2: Jugador del lado servidor: Implementar y verificar servicios

Paso 1: Configurar WRS como servidor de DHCP

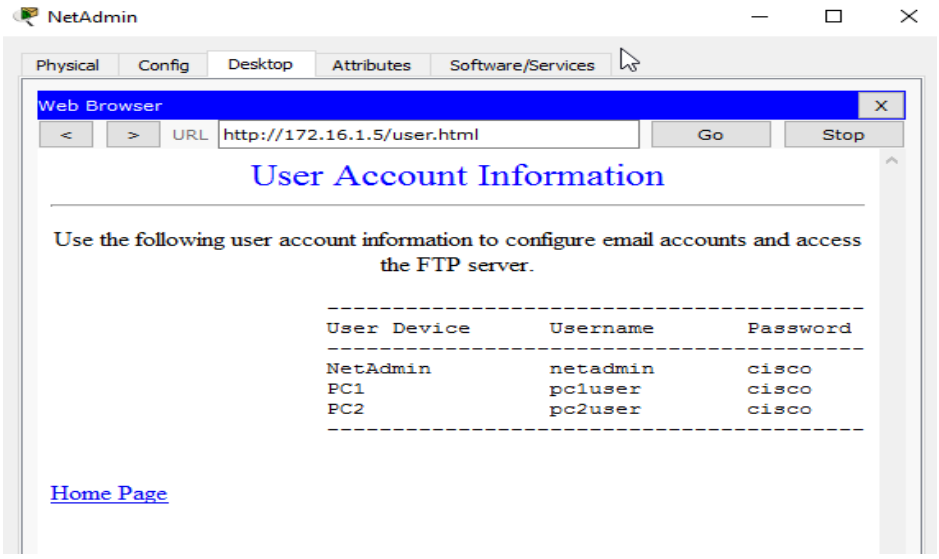
WRS proporciona servicios de DHCP. Establezca los siguientes parámetros para la configuración del servidor de DHCP:

- 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.


WRS
Physical
Config
GUI
Attributes
Setup
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Admin
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:
172 . 16 . 1 . 254
Subnet Mask:
255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address: 172.16.1. 11
Maximum number of Users:
100
IP Address Range: 172.16.1. 11 - 110
Client Lease Time:
0
minutes (0 means one day)
Static DNS 1:
172 . 16 . 1 . 5


NetAdmin
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
172.16.1.100
Subnet Mask
255.255.255.0
Default Gateway
172.16.1.11
DNS Server
172.16.1.5

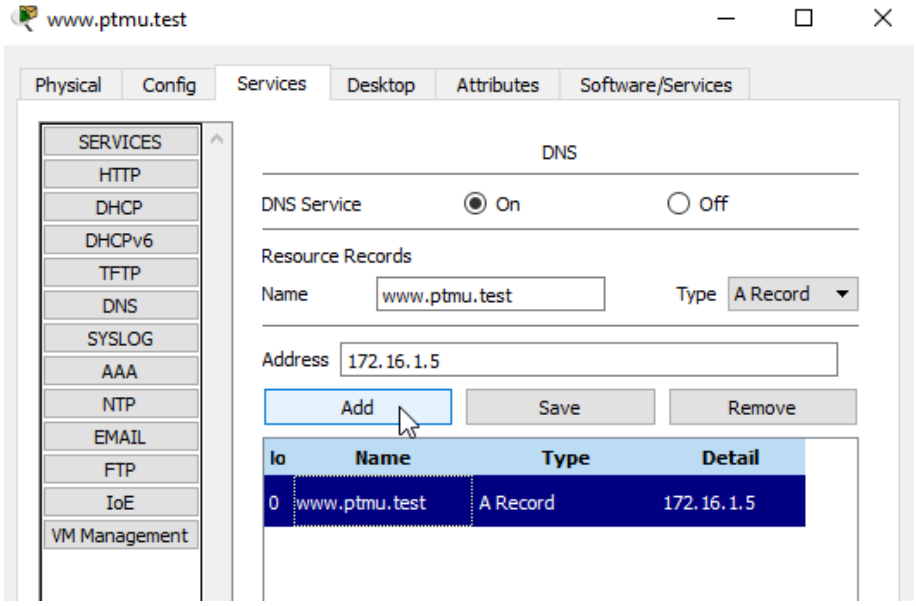

NetAdmin
Physical
Config
Desktop
Attributes
Software/Services
Web Browser
X
<
>
URL
http://172.16.1.5
Go
Stop
www.ptmu.test
Welcome to www.ptmu.test.
User Account Information



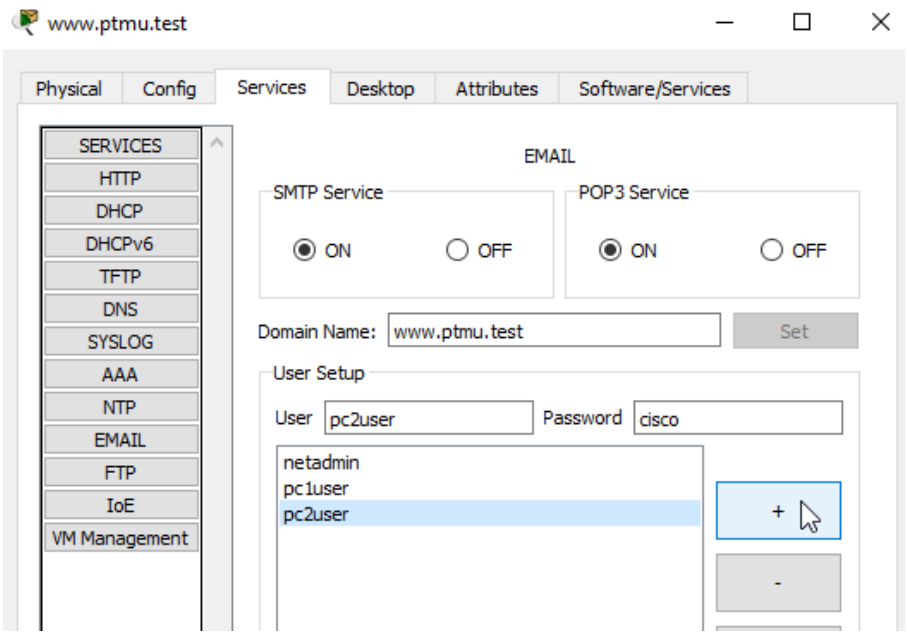
Paso 2: Configurar servicios en www.ptmu.test

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

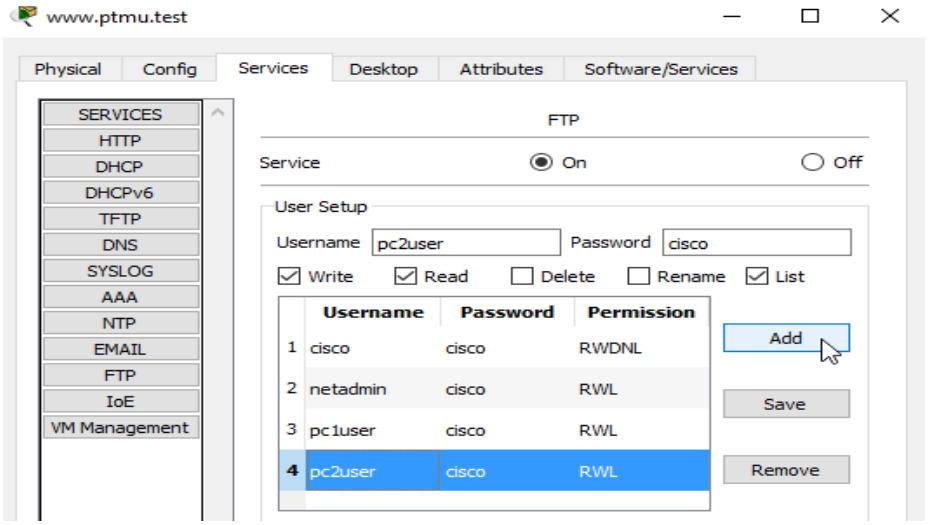
· Un registro DNS que asocie la dirección IP del servidor **www.ptmu.test** al nombre www.ptmu.test.



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



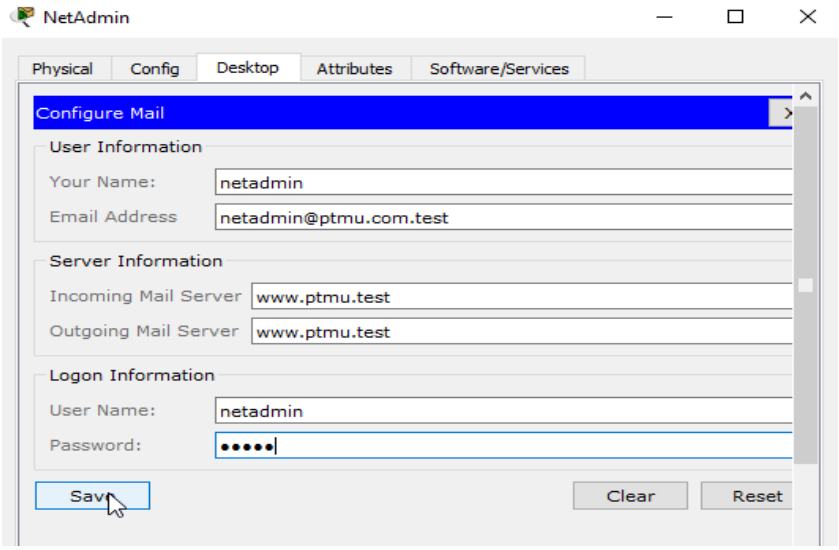
· Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.



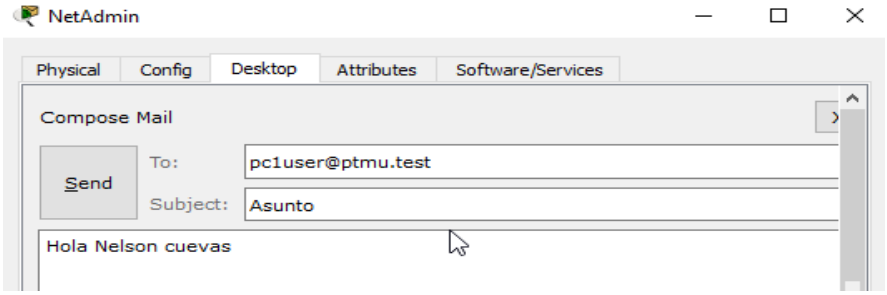
Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos

En **NetAdmin**, realice lo siguiente:

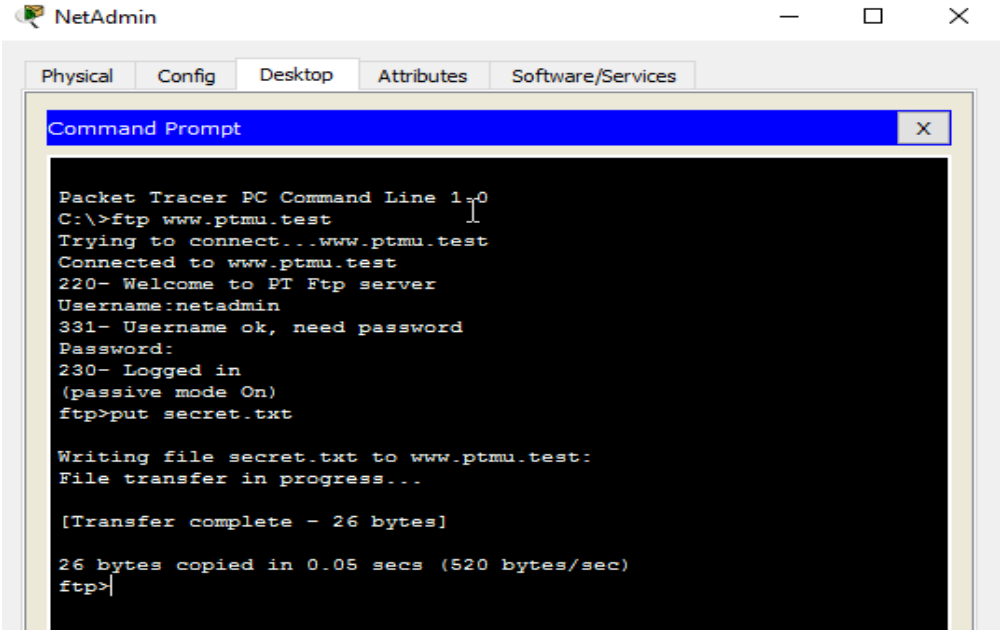
· Configure el cliente de correo electrónico para la cuenta de usuario de NetAdmin.

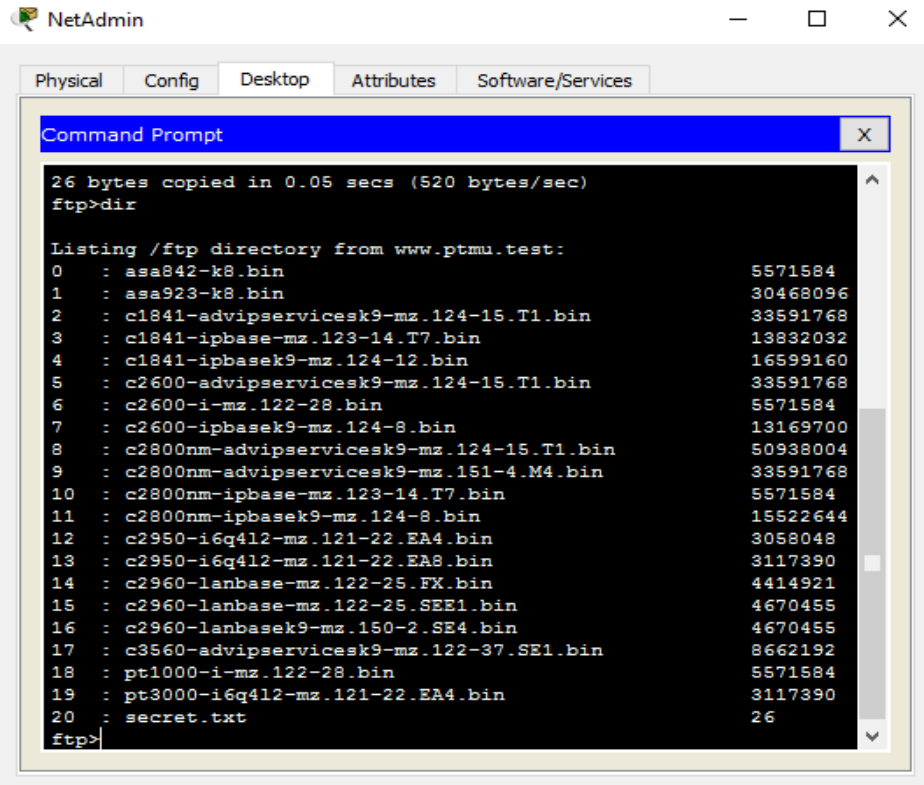


· Envíe un correo electrónico al usuario de la **PC1**.

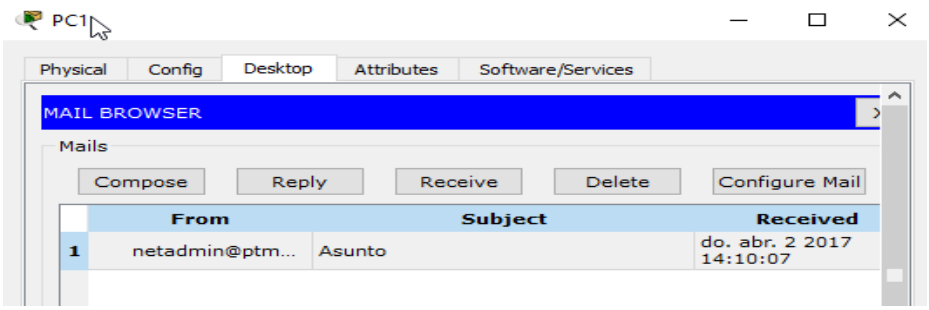


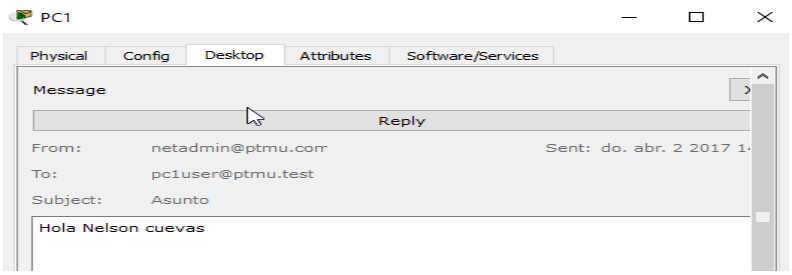
· Suba el archivo **secret.txt** al servidor FTP. No modifique el archivo.





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.



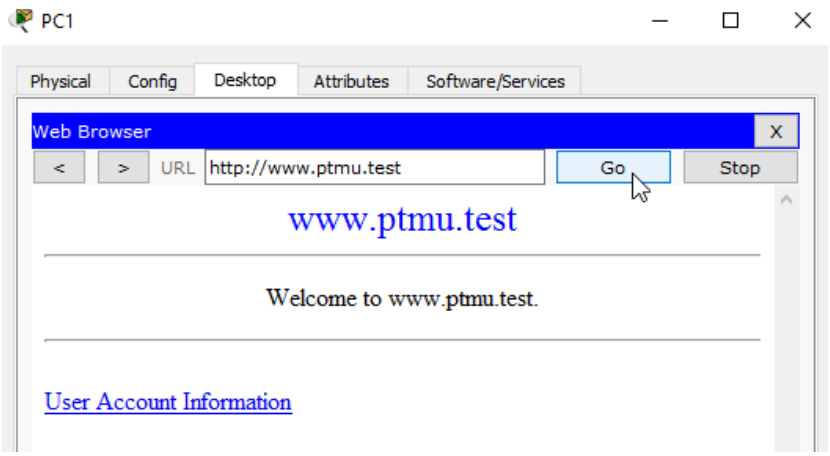


Parte 3: Jugador del lado cliente: Configurar y verificar el acceso a los servicios

Paso 1: Configurar y verificar el direccionamiento de las PC

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

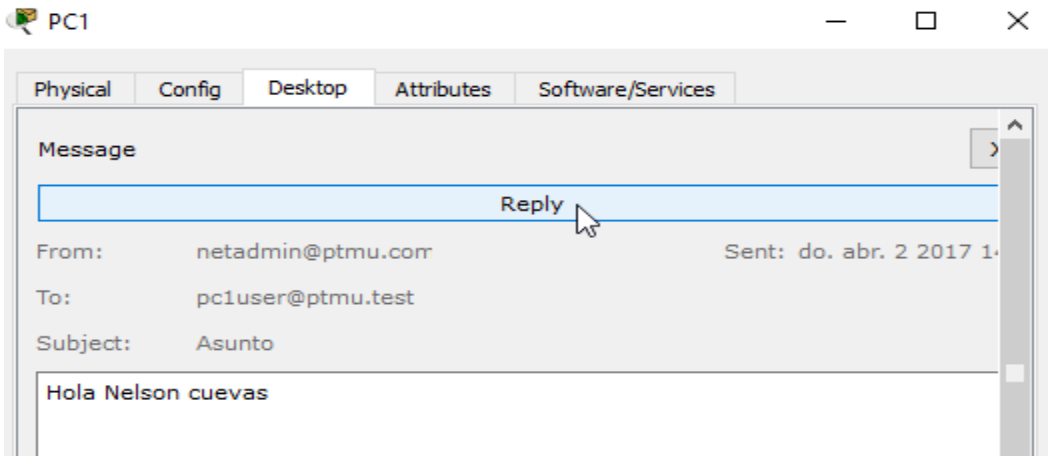
b. Las PC1 y PC2 deben poder acceder a la página Web **http://www.ptmu.test**.

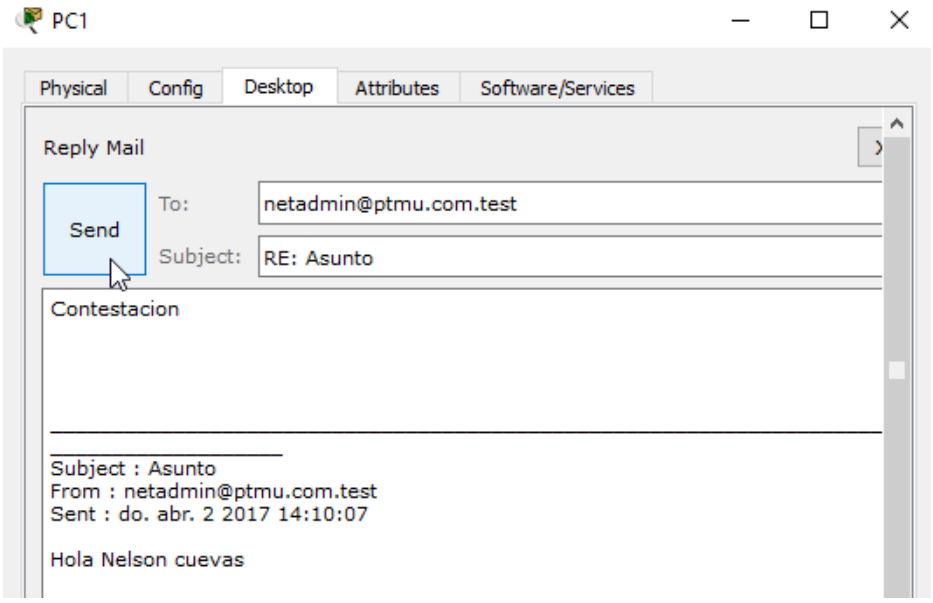


Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

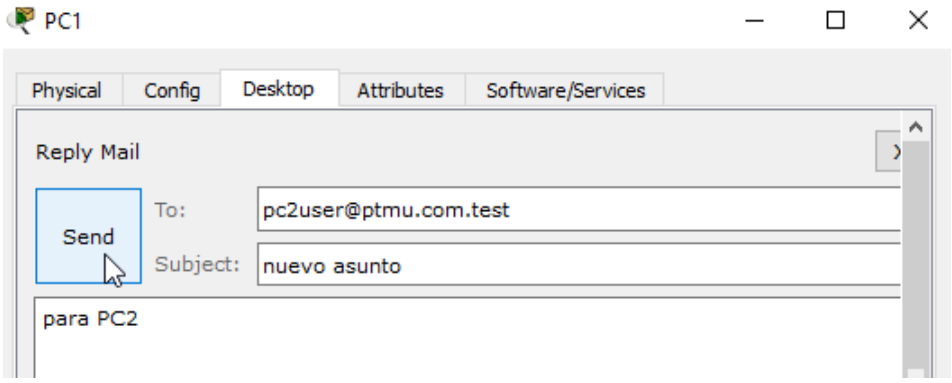
a. Configure las cuentas de correo electrónico según los requisitos que se indican en **www.ptmu.test/user.html**.

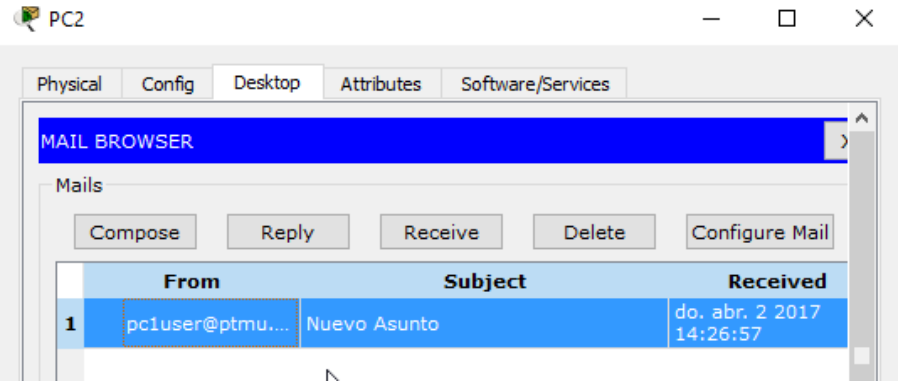
b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta.





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

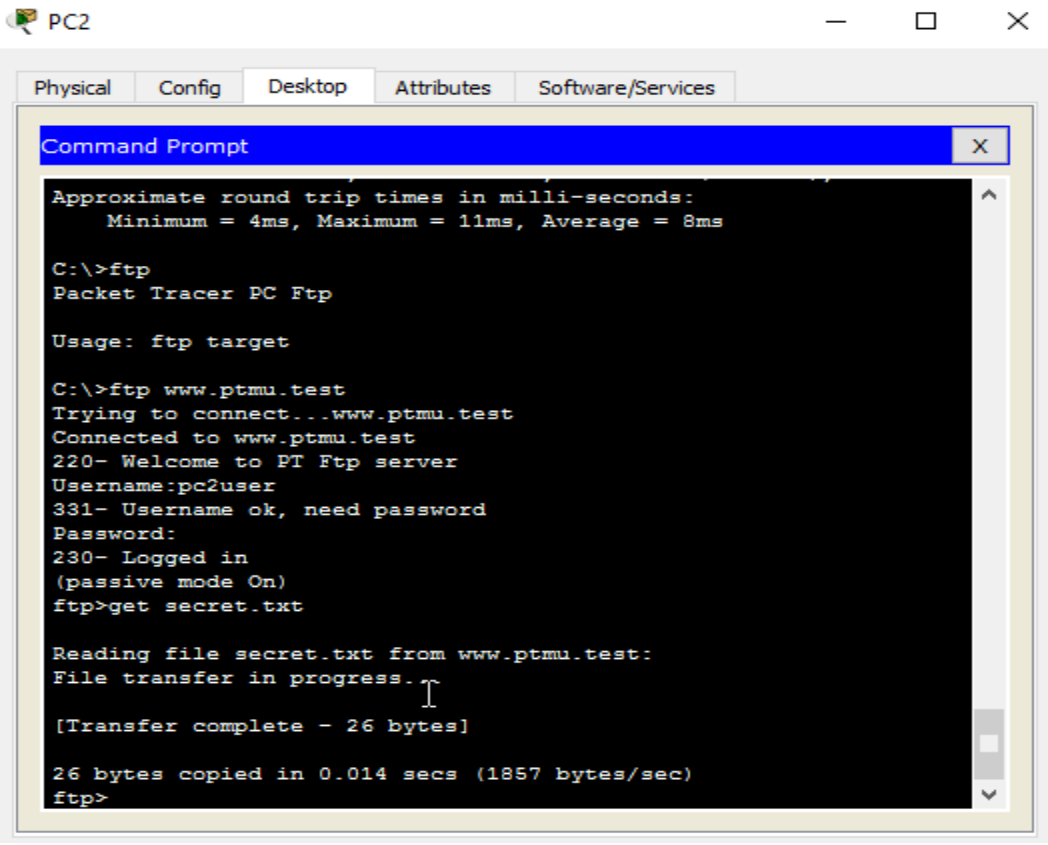




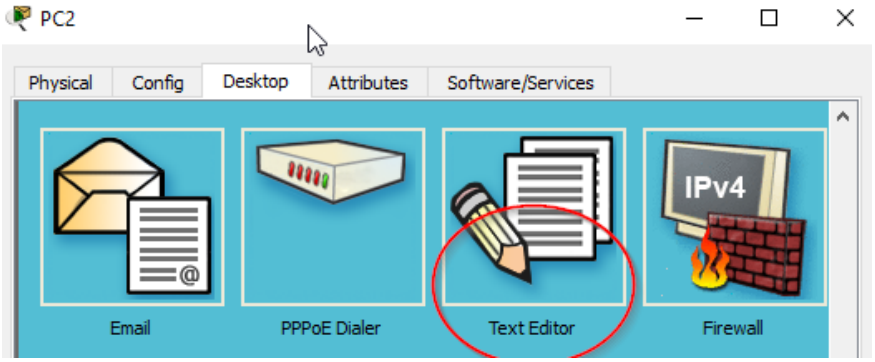
d. Verifique si la PC2 recibió un correo electrónico de la PC1.

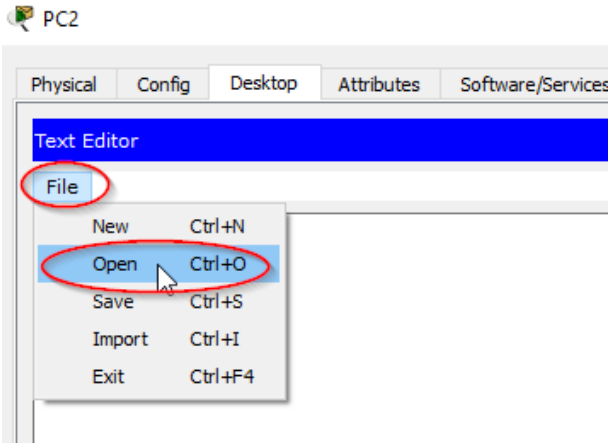
Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

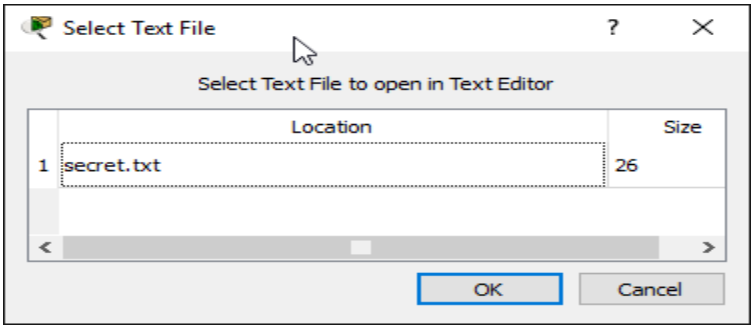
a. En la PC2, acceda al servidor FTP y descargue el archivo **secret.txt**.

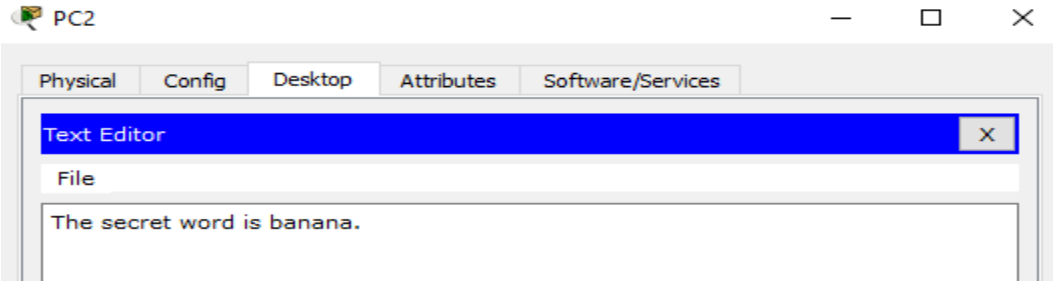


b. Abra el archivo **secret.txt**, solo cambie la palabra secreta por **apple** y suba el archivo.









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

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 03:04:23

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status
Network	
NetAdmin	
Default Gateway	Correct
DNS Server IP	Correct
Email Client	
Email User	
Email	Correct
Incoming Mail ...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Ports	
FastEthernet0	
DHCP client en...	Correct
IP Address	Correct
Subnet Mask	Correct
S1	
Banner MOTD	Correct
Console Line	
Password	Correct
Enable Secret	Correct
Host Name	Correct
Ports	
Vlan1	
IP Address	Correct
Port Status	Correct
Subnet Mask	Correct
VTY Lines	
VTY Line 0	
Password	Correct
WRS	
DHCP Server	
Pools	

Score : 43/43
Item Count : 43/43

Component	Items/Total	Score
Basic Security Configuration	5/5	5/5
Client DHCP Configuration	5/5	5/5
IPv4 Host Configuration	3/3	3/3
PT Client Configuration	5/5	5/5
PT Server Configuration	25/25	25/25

Close

File Edit Options View Tools Extensions Help

Activity Results

Time Elapsed: 00:26:57

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 ...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Ports	
FastEthernet0	
DHCP client en...	Correct
IP Address	Correct
Subnet Mask	Correct
PC2	
Default Gateway	Correct
DNS Server IP	Correct
Email Client	
Email User	
Email	Correct
Incoming Mail ...	Correct
Outgoing Mail S...	Correct
User Name	Correct
User Password	Correct
Files	
C Directory	
secret.txt	Correct
Desktop	
secret.txt	Correct
Ports	
FastEthernet0	

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

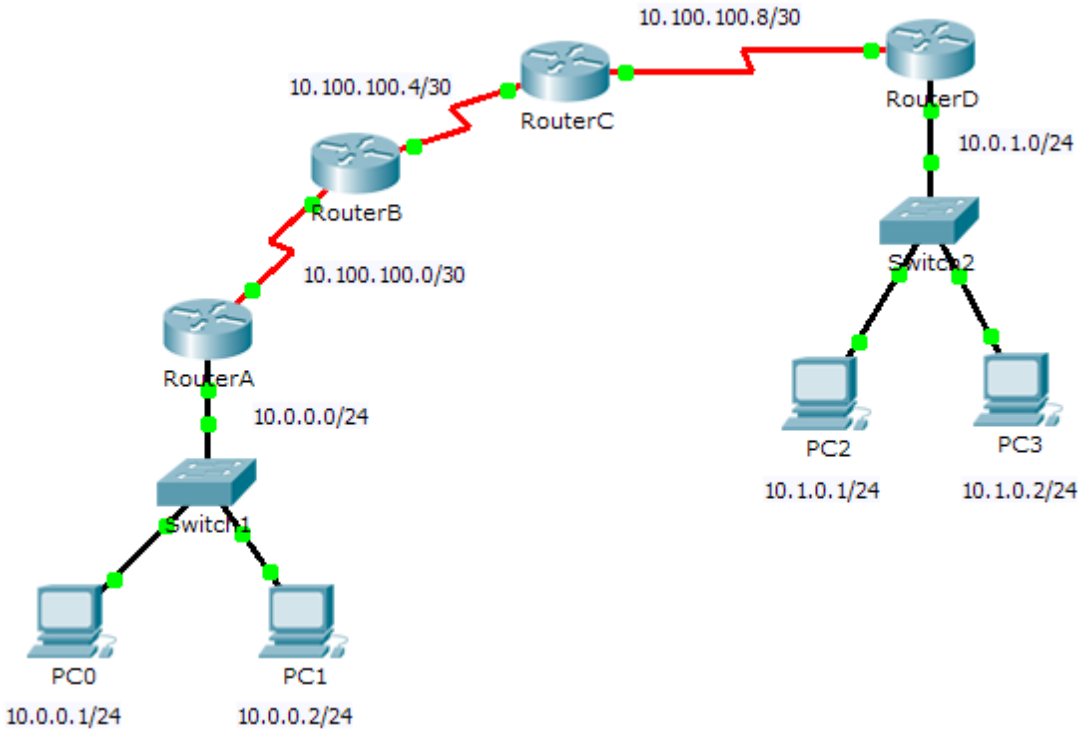
Close

11.3.2.2 Test Connectivity with Traceroute Instructions IG

Packet Tracer: Prueba de la conectividad con traceroute

.

Topología



Objetivos:

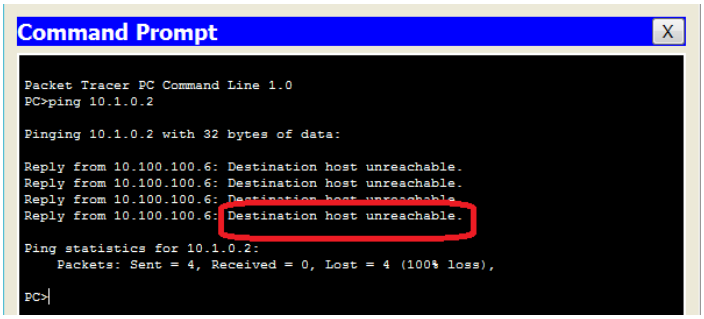
Parte 1: probar la conectividad de extremo a extremo con el comando tracert
Parte 2: comparar con el comando traceroute en un router

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

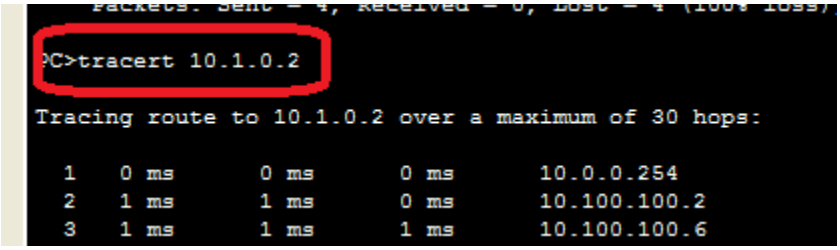
Haga clic en **PC1** y abra el **símbolo del sistema**. Haga ping a **PC3** en **10.1.0.2**. ¿Qué mensaje se muestra como resultado del ping?

RTA: Host de destino inalcanzable.



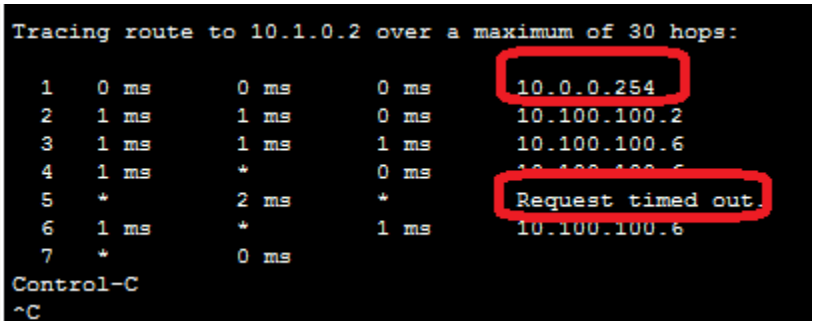
Paso 2: Rastrear la ruta de PC1 para determinar dónde falla la conectividad

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



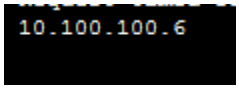
b. Cuando reciba el mensaje **Request timed out** (Tiempo de espera agotado), presione **Ctrl**+**C**. ¿Cuál fue la primera dirección IP indicada en el resultado del comando **tracert**?

RTA: 10.0.0.254, la dirección de gateway de la PC.



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

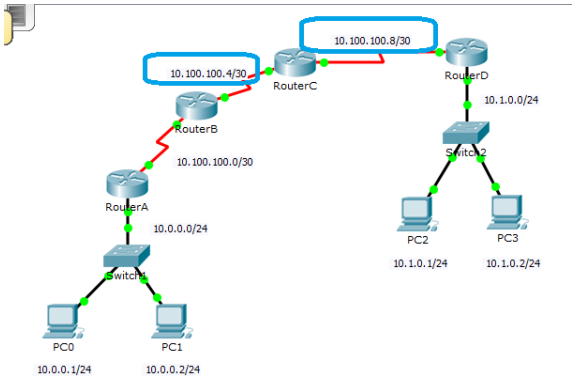
RTA: 10.100.100.6



Paso 3: Corregir el problema de red

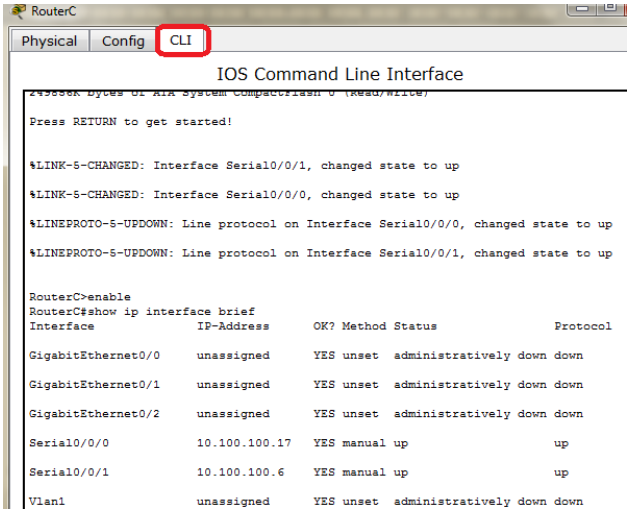
a. Compare la última dirección que se alcanzó con el comando **tracert** con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de falla. ¿Qué dispositivos tienen direcciones configuradas para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

RTA: El Router B y el Router C.



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

c. ¿Cuál es el estado de las interfaces?
RTA: 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?

RTA: La interfaz serial 0/0/0 tiene una dirección IP incorrecta según la topología.

```
RouterC#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

GigabitEthernet0/2     unassigned      YES unset  administratively down down

Serial0/0/0            10.100.100.17   YES manual up                    up

Serial0/0/1            10.100.100.6    YES manual up                    up
```

e. Realice los cambios necesarios para restaurar la conectividad, pero no modifique las subredes. ¿Cuál es la solución?

RTA: Cambiar la dirección IP de la S0/0/0 a 10.100.100.9/30

```
RouterC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterC(config)#interface s0/0/0
RouterC(config-if)#ip address 10.100.100.9 255.255.255.252
RouterC(config-if)#no shutdown
RouterC(config-if)#exit
RouterC(config)#exit
RouterC#
%SYS-5-CONFIG_I: Configured from console by console
```

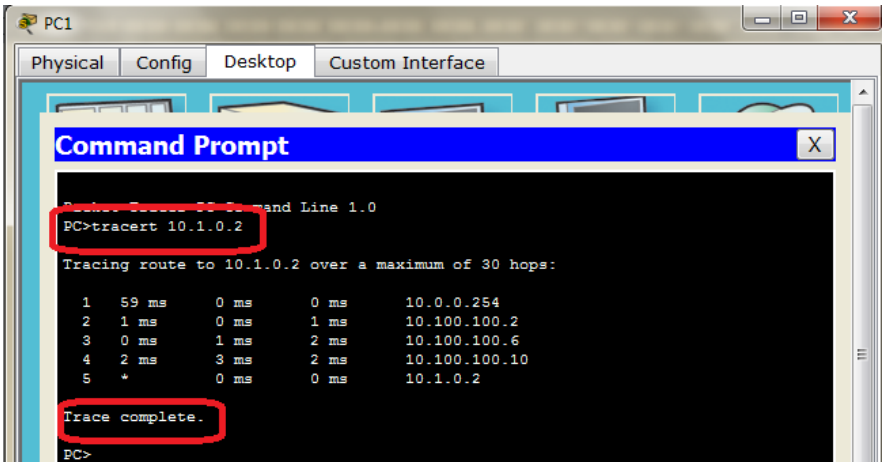
```
RouterC#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

GigabitEthernet0/2     unassigned      YES unset  administratively down down

Serial0/0/0            10.100.100.9    YES manual up                    up

Serial0/0/1            10.100.100.6    YES manual up                    up

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

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**.

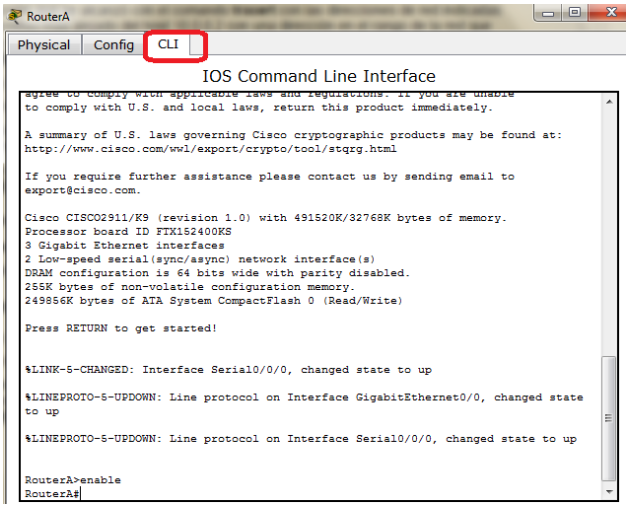
b. Observe el resultado del comando **tracert**. ¿El comando funcionó correctamente?

RTA: Sí nos muestra el mensaje trace complete



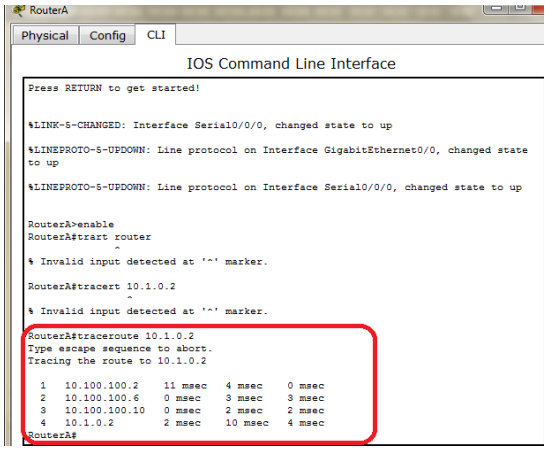
Parte 2: Comparar con el comando traceroute en un router

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



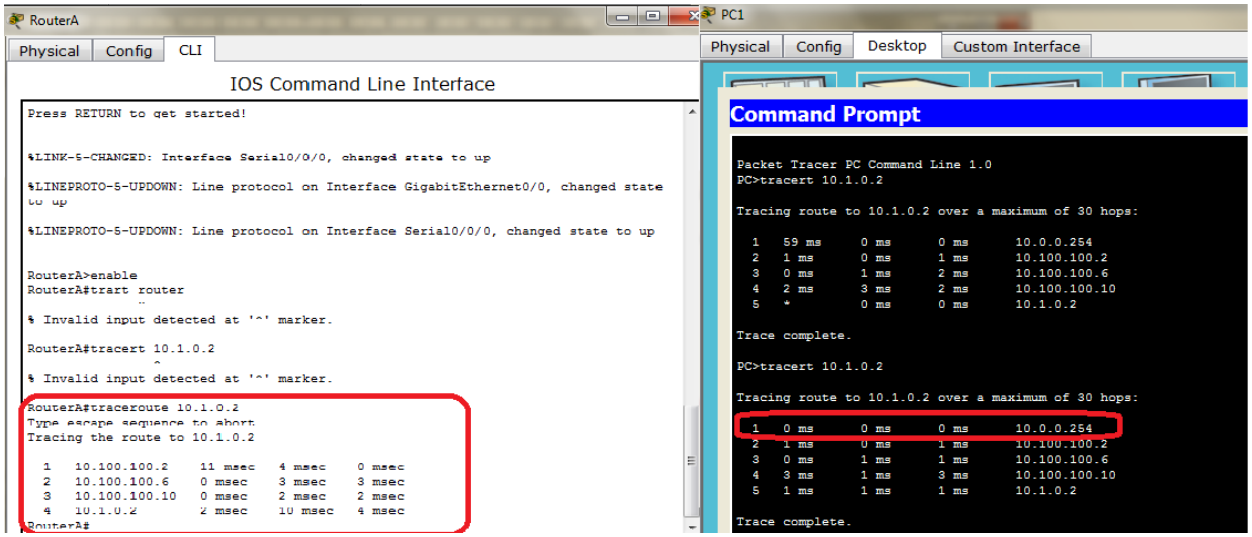
b. Introduzca el comando **traceroute 10.1.0.2**. ¿El comando se completó correctamente?

RTA: es correcto mostrando las diferentes direcciones ip hasta llegar al destino 10.1.0.2.



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?

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



11.3.3.4 Using Show Commands Instructions IG

Packet Tracer: Uso de los comandos show

Objetivos

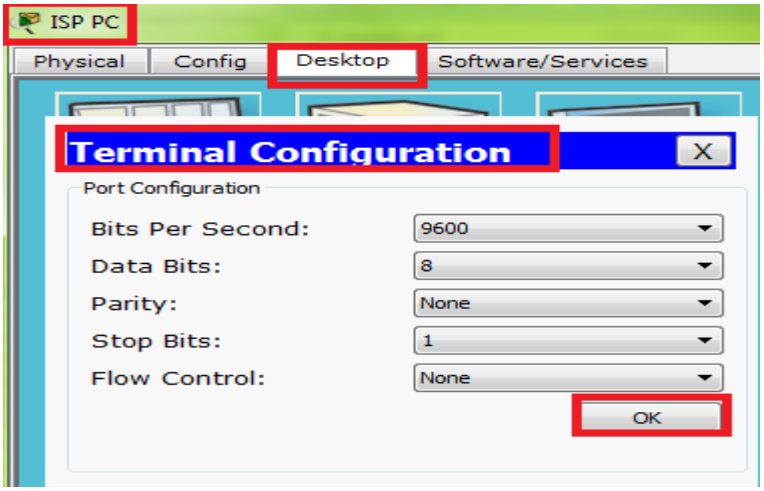
Parte 1: Analizar el resultado del comando show

Parte 2: Preguntas de reflexión

Parte 1: Analizar el resultado del comando show

Paso 1: Conectarse a ISPRouter

a. Haga clic en PC ISP y, a continuación, en la ficha Desktop (Escritorio), seguida de Terminal.



b. Ingrese al modo EXEC privilegiado.

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

show arp
show flash:
show ip route
show interfaces
show ip interface brief show protocols.
show users
show version

Parte 2: Preguntas de reflexión

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

   - Show ip route
   - show protocols

Terminal

```
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
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
```

```
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>
```

2. ¿Qué comandos proporcionan la dirección IP y la asignación de interfaces, pero no el prefijo de red?
   - Show ip interface brief

```
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>
```

3. ¿Qué comandos proporcionan el estado de las interfaces?
   - Show interfaces
   - Show ip interface brief

```
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
```

```
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
```

4. ¿Qué comandos proporcionan información sobre el IOS que se encuentra cargado en el router?
   - 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 26 minutes, 8 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
```

5. ¿Qué comandos proporcionan información sobre las direcciones de las interfaces del router?
   - show arp
   - show interfaces

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

6. ¿Qué comandos proporcionan información sobre la cantidad de memoria flash disponible?
   - Show version

```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:
```

7. ¿Qué comandos proporcionan información sobre las líneas que se utilizan para propósitos de control de dispositivos o de configuración?
   - 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>
```

8. ¿Qué comandos proporcionan estadísticas de tráfico de las interfaces del router?
   - show interfaces

```
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
```

9. ¿Qué comandos proporcionan información sobre las rutas disponibles para el tráfico de la red? 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>
```

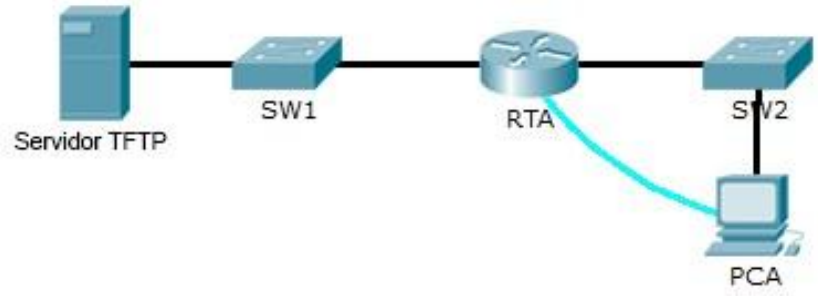
10. ¿Qué interfaces están activas actualmente en el router?
    Las interfaces actualmente activas son la GigabitEthernet 0/0, serial 0/0/1

```
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>
```

11.4.2.5 Backing UP Configuration Files Instructions IG

Packet Tracer: 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

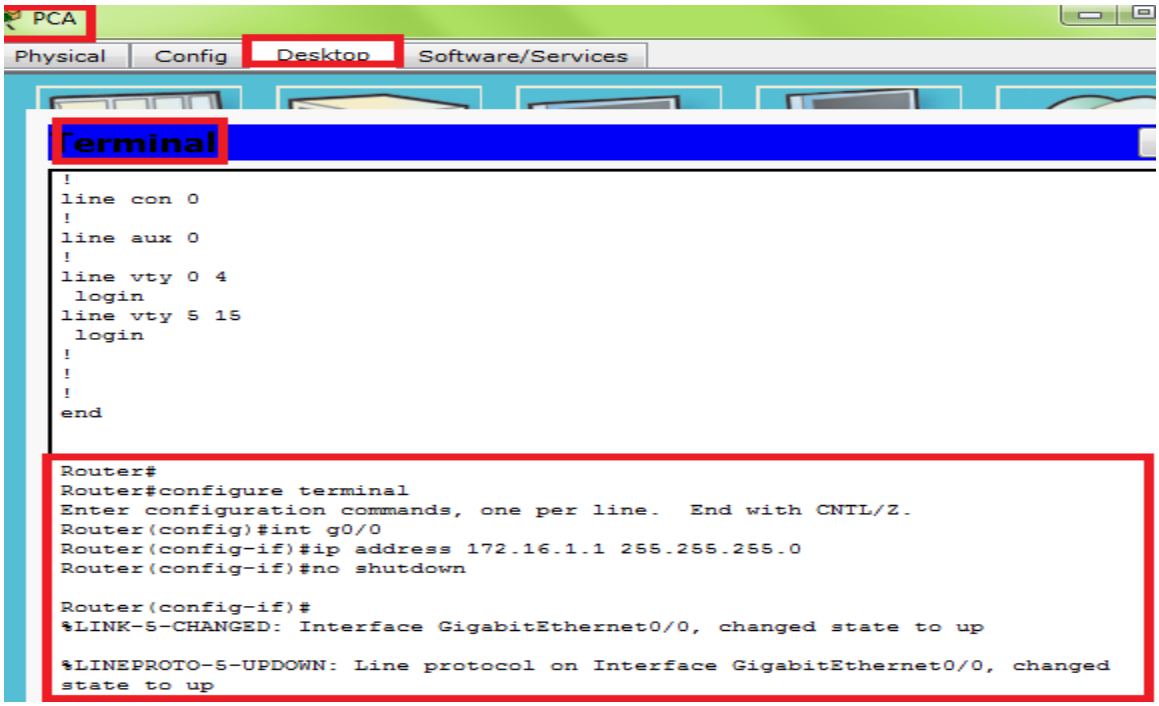
Parte 1: Establecer la conectividad al servidor TFTP

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

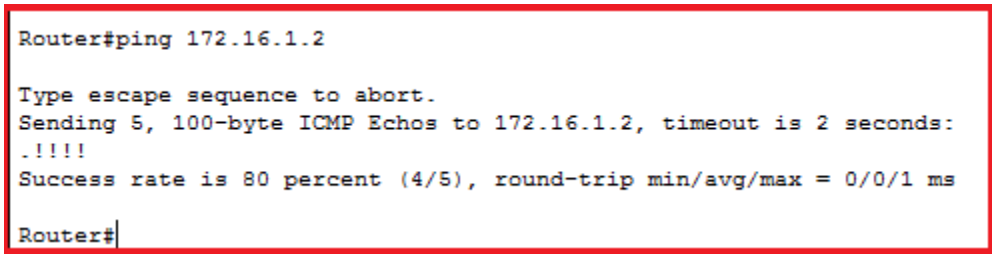
a. Haga clic en **PCA**, después en la ficha **Desktop** (Escritorio) y, a continuación, en **Terminal** para acceder a la línea de comandos **RTA**.

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

En estos pantallazos se encuentran los dos puntos anteriores, a y b



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**

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#

```
Router#copy tftp 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 0.002 secs (392500 bytes/sec)
RTA#
%SYS-5-CONFIG_I: Configured from console by console

RTA#
```

c. Emita el comando para visualizar la configuración actual. ¿Qué cambios se realizaron?

La configuración que fue almacenada en el servidor TFFP se cargó en el router

```
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.31.1.1 255.255.255.0
 duplex auto
 speed auto
 shutdown
```

d. Emita el comando **show** adecuado para mostrar el estado de la interfaz. ¿Todas las interfaces están activas?

Todas las interfaces no están activas, la interfaz Gi0/1 está inactiva administrativamente, de igual manera las todas las interfaces del router están desactivadas de manera predeterminada

```
RTA#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     172.16.1.1      YES manual up                    up

GigabitEthernet0/1     172.31.1.1      YES manual administratively down down

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

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

```
RTA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RTA(config)#int g0/1
RTA(config-if)#no shutdown

RTA(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

RTA(config-if)#
```

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.

```
RTA(config-if)#exit
RTA(config)#hostname RTA-1
RTA-1(config)#
```

b. Guarde la configuración en la NVRAM.

```
RTA-1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTA-1#
```

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>**

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

Writing running-config...!!
[OK - 849 bytes]

849 bytes copied in 0.001 secs (849000 bytes/sec)
RTA-1#
```

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

```
RTA-1#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)


RTA-1#
```

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>**

```
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)


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 4.019 secs (877580 bytes/sec)
RTA-1#
```

11.5.2.4 Configuring a Linksys Router IG

Packet Tracer: Configuración de un router Linksys

Topología

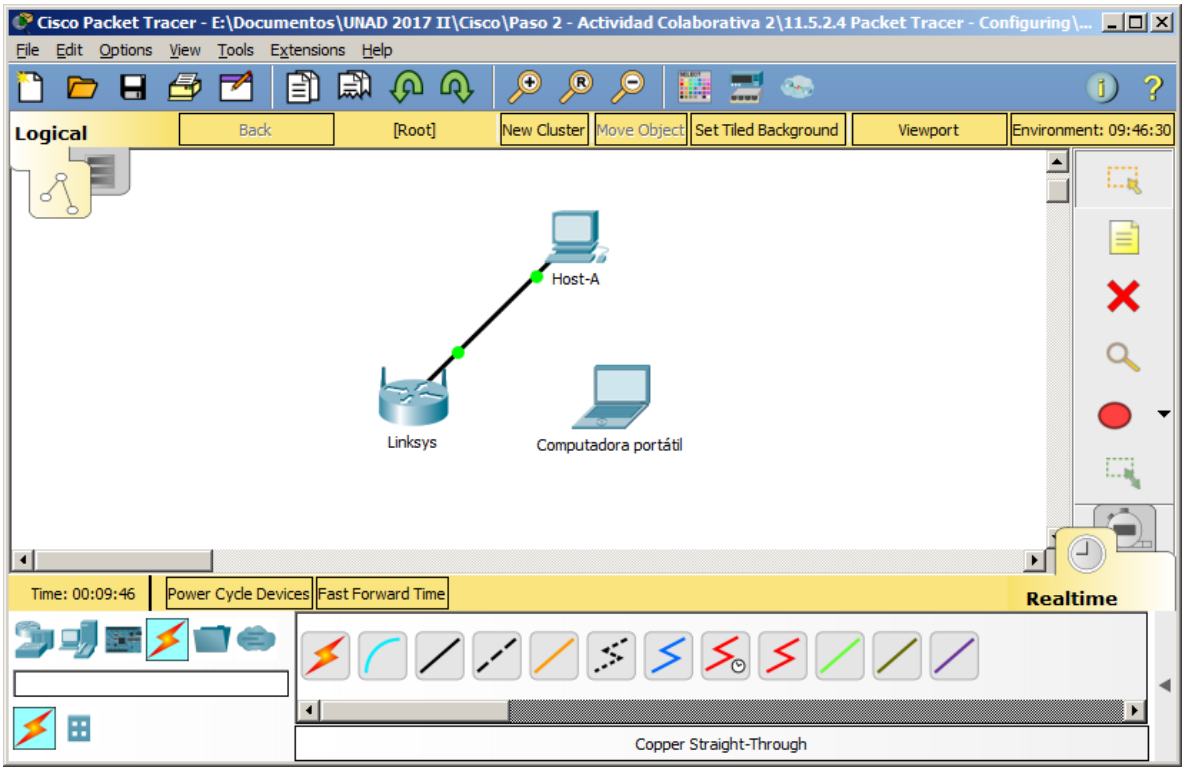
Objetivos

Parte 1: Conectar al router Linksys
Parte 2: Habilitar conectividad inalámbrica
Parte 3: Configurar y verificar el acceso al cliente inalámbrico

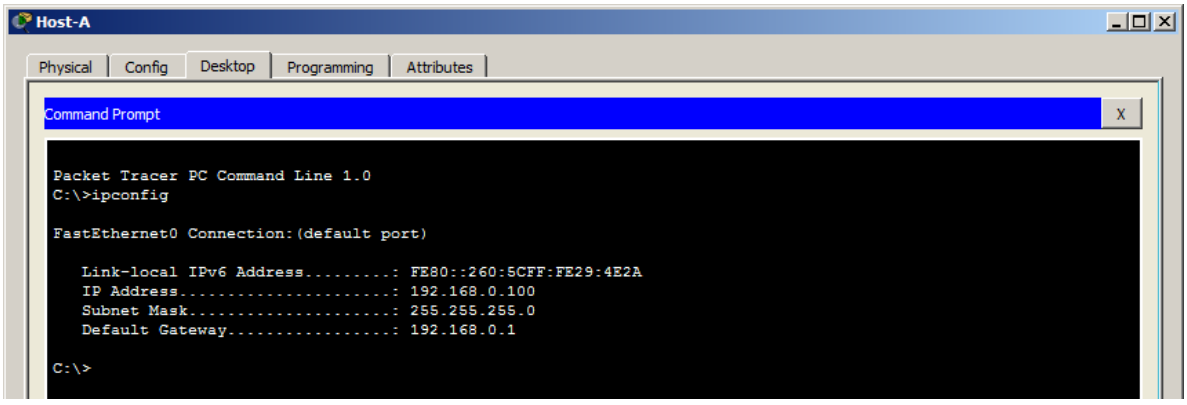
Parte 1: Conectar al router Linksys

Paso 1: Establecer y verificar la conectividad al router Linksys

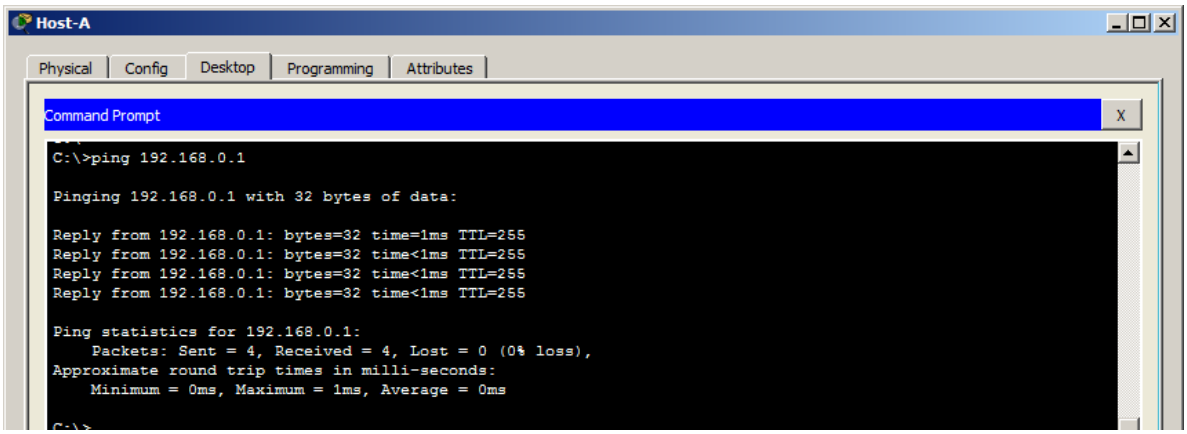
a. Conecte el cable adecuado del Host-A al puerto Ethernet 1 en Linksys.



b. 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.

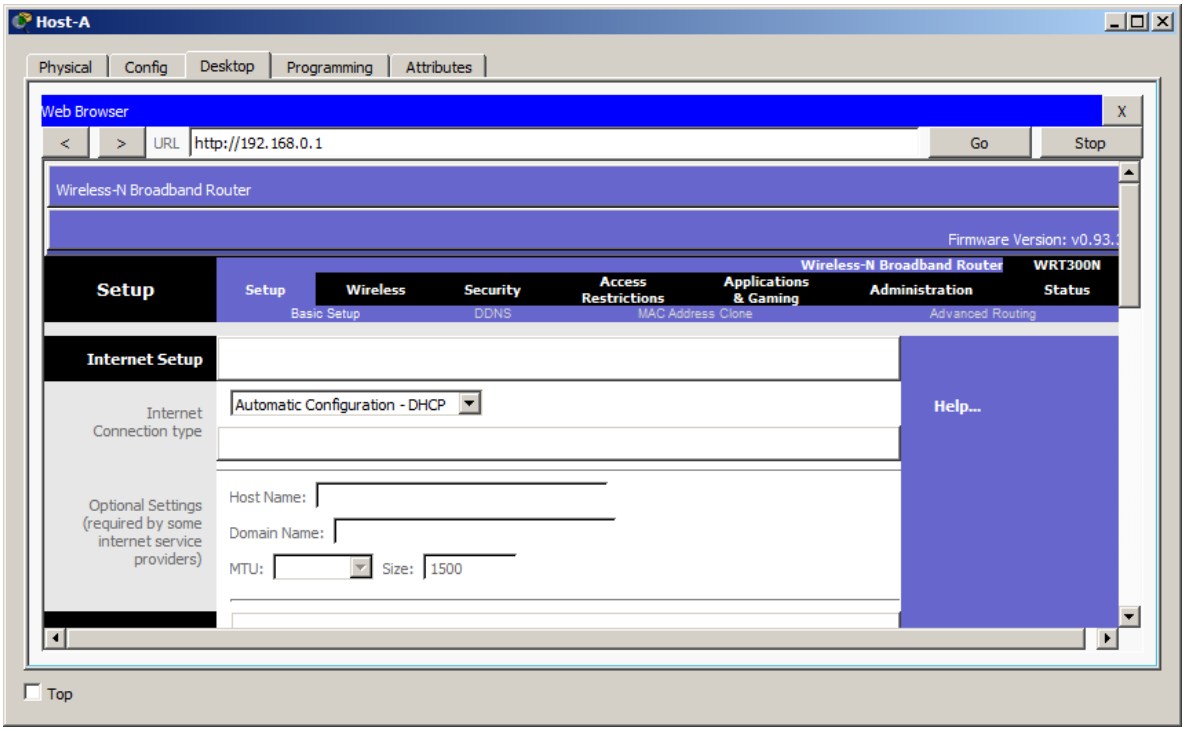


c. Introduzca el comando ping 192.168.0.1 para verificar que el Host-A pueda acceder al Gateway predeterminado.



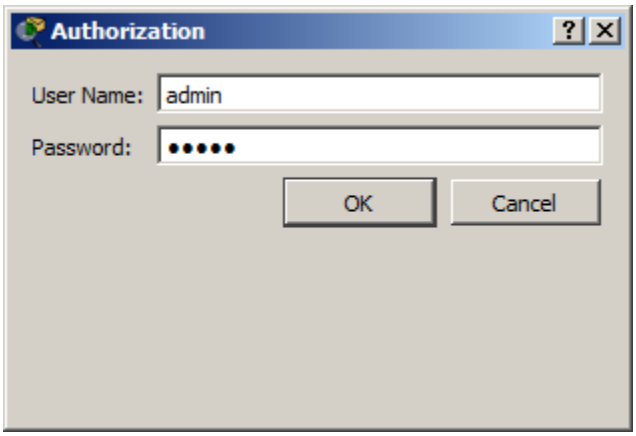
Paso 2: Acceda a la interfaz gráfica de usuario (GUI) de Linksys mediante un explorador Web.

a. 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.



b. 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).

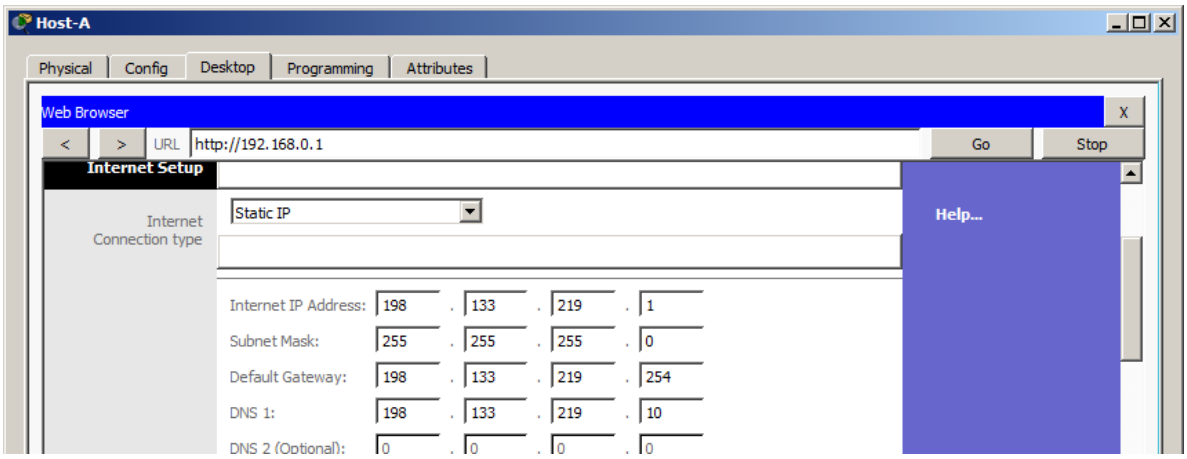


Parte 2: Habilitar conectividad inalámbrica

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:

- Dirección IP de Internet: 198.133.219.1
- Máscara de subred: 255.255.255.0
- Gateway predeterminado: 198.133.219.254
- DNS 1: 198.133.219.10



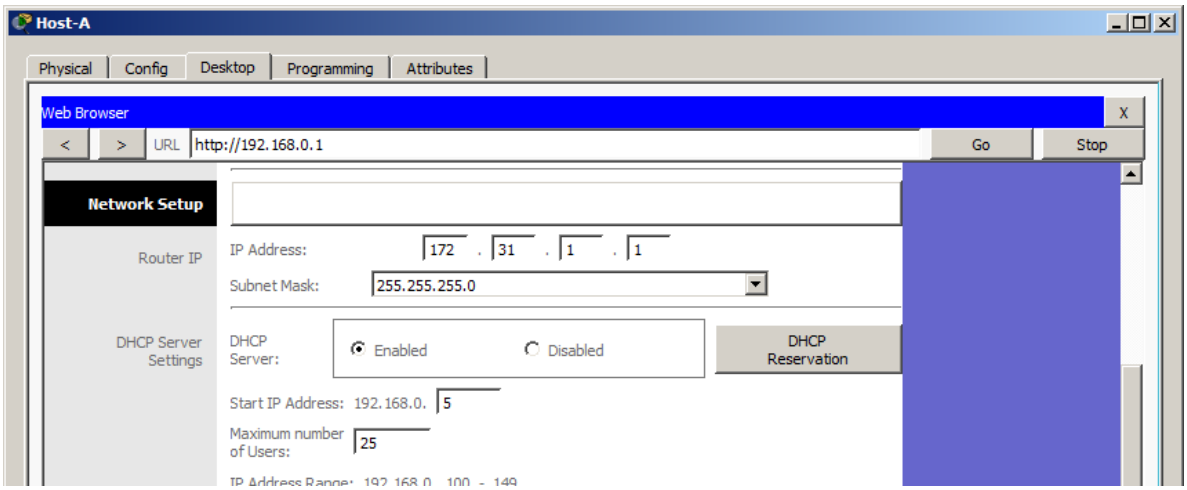
Paso 2: Configure los parámetros de red internos.

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

- Dirección IP: 172.31.1.1

- Máscara de subred: 255.255.255.224
- Dirección IP de inicio: introduzca 5 para el último octeto.
- Cantidad máxima de usuarios: 25

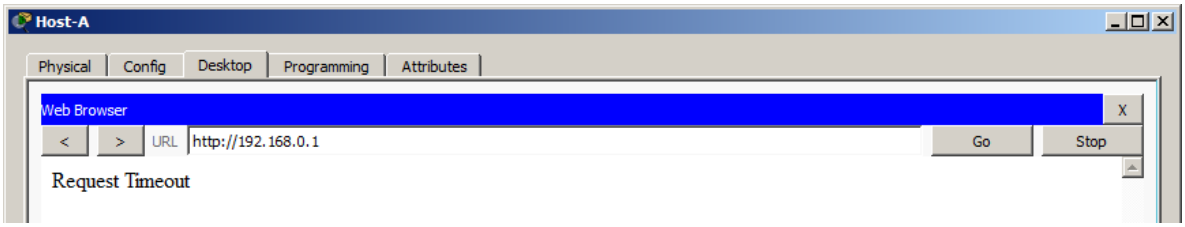
Nota: el rango de direcciones IP del pool de DHCP solo refleja los cambios una vez que hace clic en Save Settings.



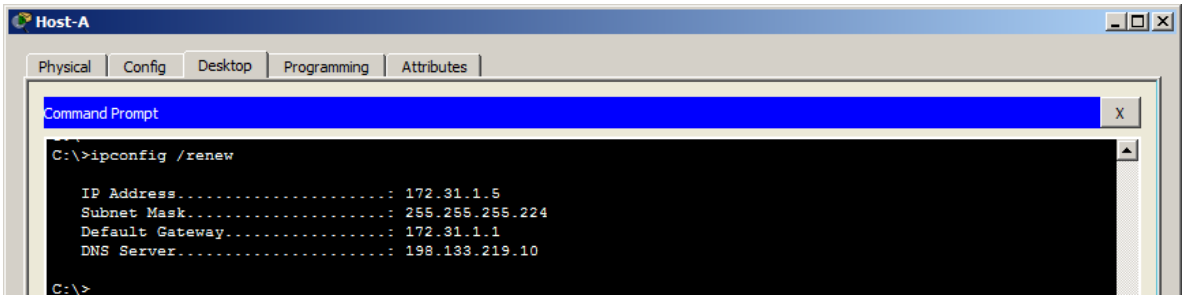
Paso 3: Guardar la configuración y volver a conectarse al router Linksys

a. 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.

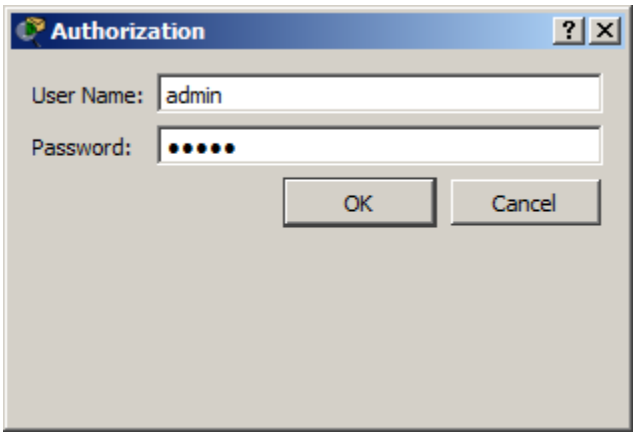
b. Cuando hace clic en Save Settings, se pierde la conexión. Esto ocurre porque cambió la dirección IP del router.

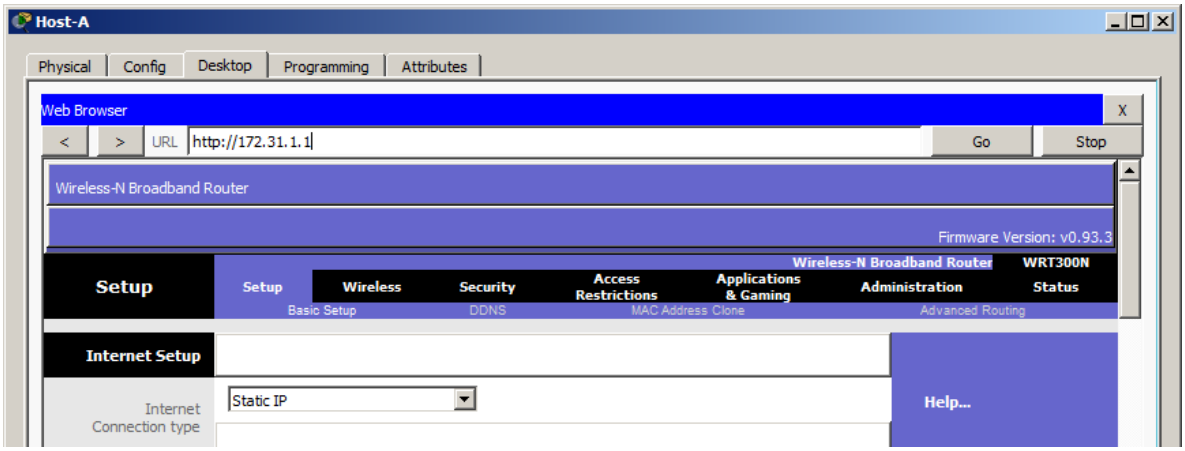


c. Regrese al símbolo del sistema del Host-A. Introduzca el comando ipconfig /renew para renovar la dirección IP.



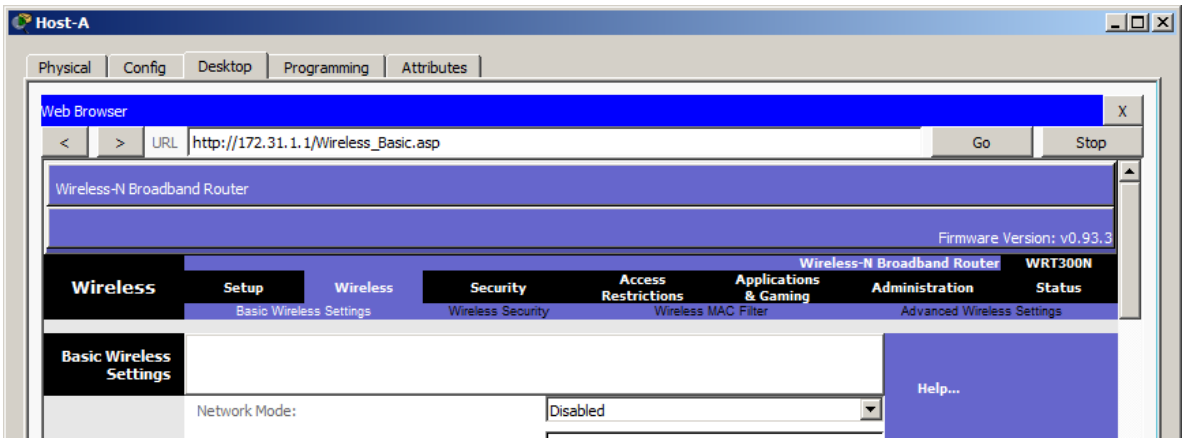
d. Utilice el explorador Web del Host-A para volver a conectarse al router Linksys. Deberá utilizar la nueva dirección de gateway predeterminado. Verifique la configuración de Internet Connection (Conexión a Internet) en la ficha Status (Estado). La configuración debe coincidir con los valores que configuró 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

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



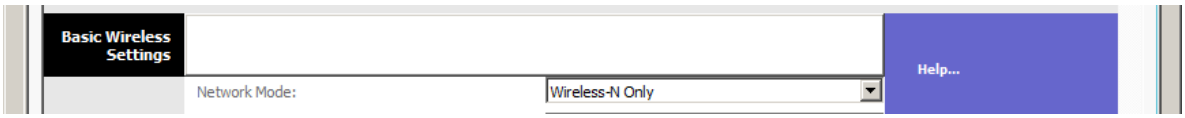
¿En qué caso elegiría la opción Disable (Deshabilitar)?

- Cuando no hay dispositivos inalámbricos.

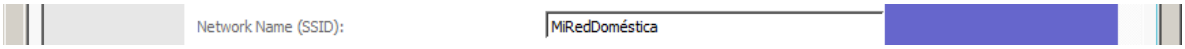
¿En qué caso elegiría la opción Mixed (Combinada)?

- Cuando hay dispositivos inalámbricos que constan de B, G o N.

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



c. Cambie el SSID a MiRedDoméstica.



¿Cuáles son dos características de un SSID?

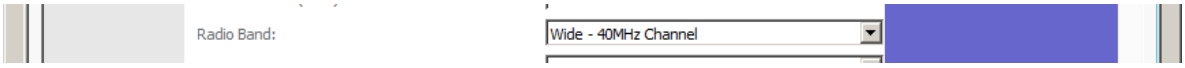
- Distingue mayúsculas de minúsculas y el nombre no puede exceder los 32 caracteres.

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.

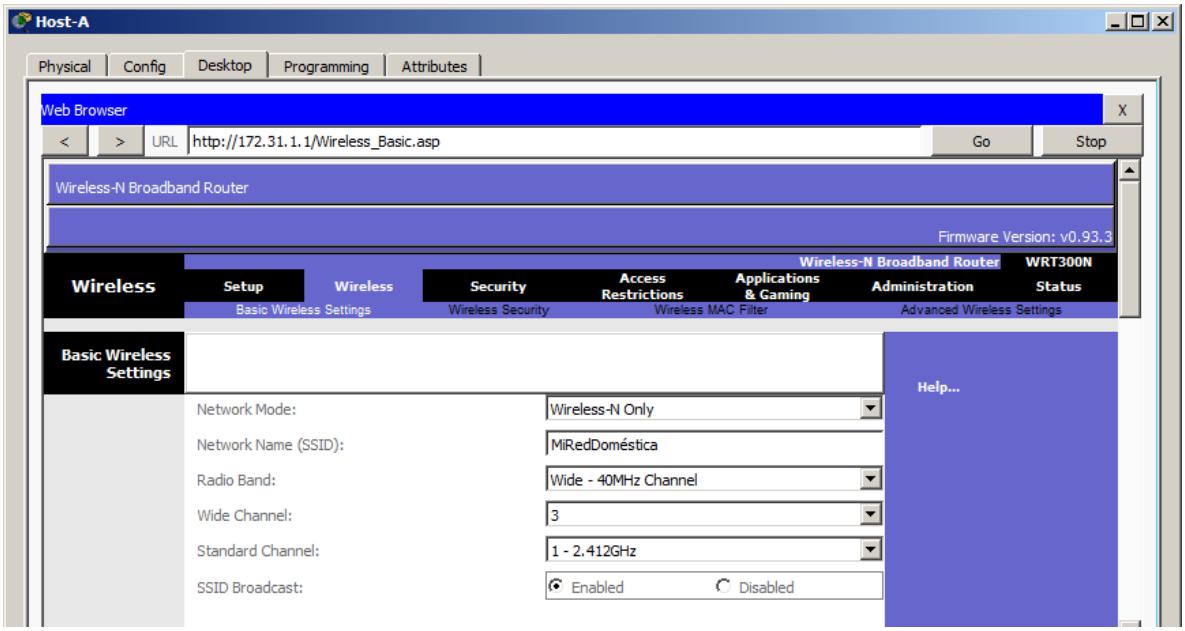
Si no se transmite el SSID de un punto de acceso, ¿cómo se conectan los dispositivos a este? El cliente debe estar configurado con el nombre, el cual debe estar bien escrito para que se lleve a cabo la conexión.

- El cliente debe tener configurado correctamente la contraseña y el nombre de la red inalámbrica.

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).



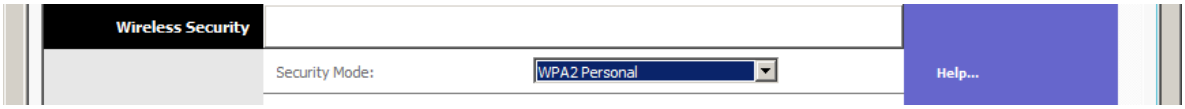
f. Haga clic en Save settings (Guardar configuración) y, a continuación, haga clic en Continue (Continuar).



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.

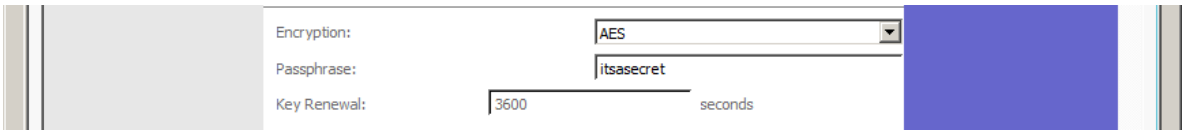
b. Configure el Security Mode (Modo de seguridad) en WPA2 Personal.



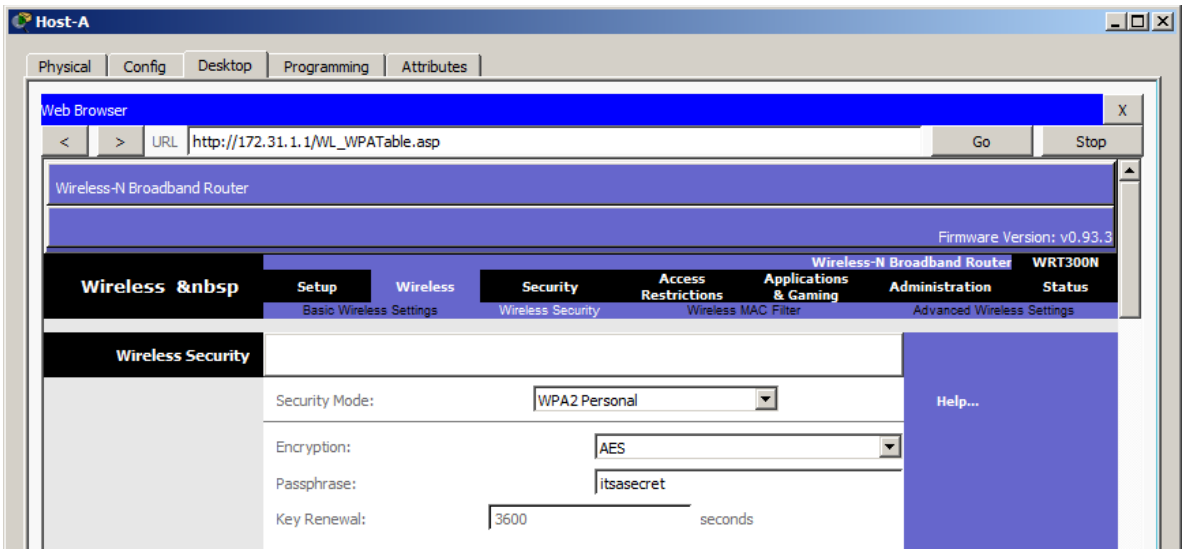
¿Cuál es la diferencia entre la opción Personal y la opción Enterprise (Empresa)?

- Enterprise usa un servidor Radius para autenticar a los usuarios, mientras que el modo Personal usa el router Linksys para autenticar usuarios.

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



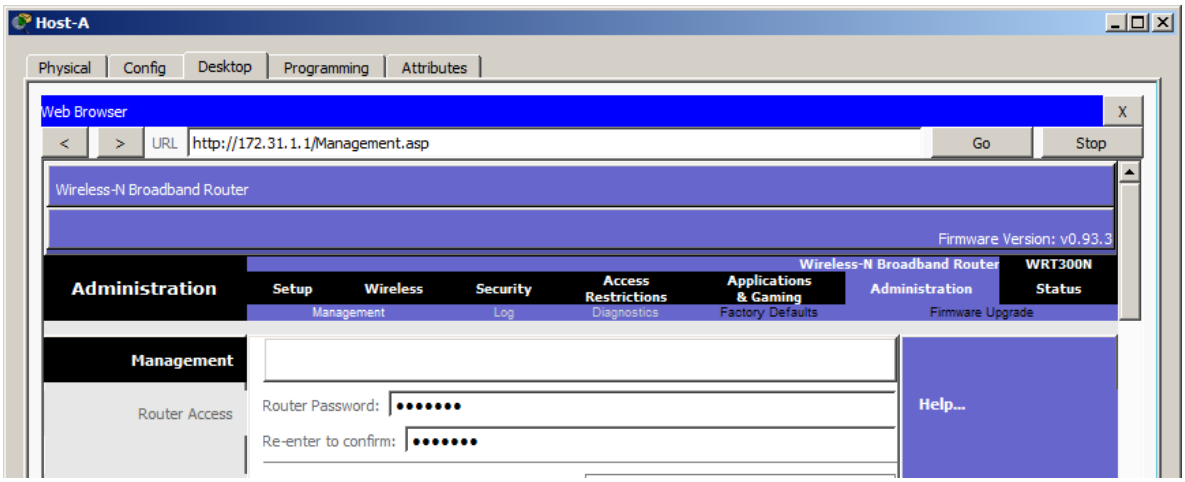
d. Haga clic en Save settings (Guardar configuración) y, a continuación, haga clic en Continue (Continuar).



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.

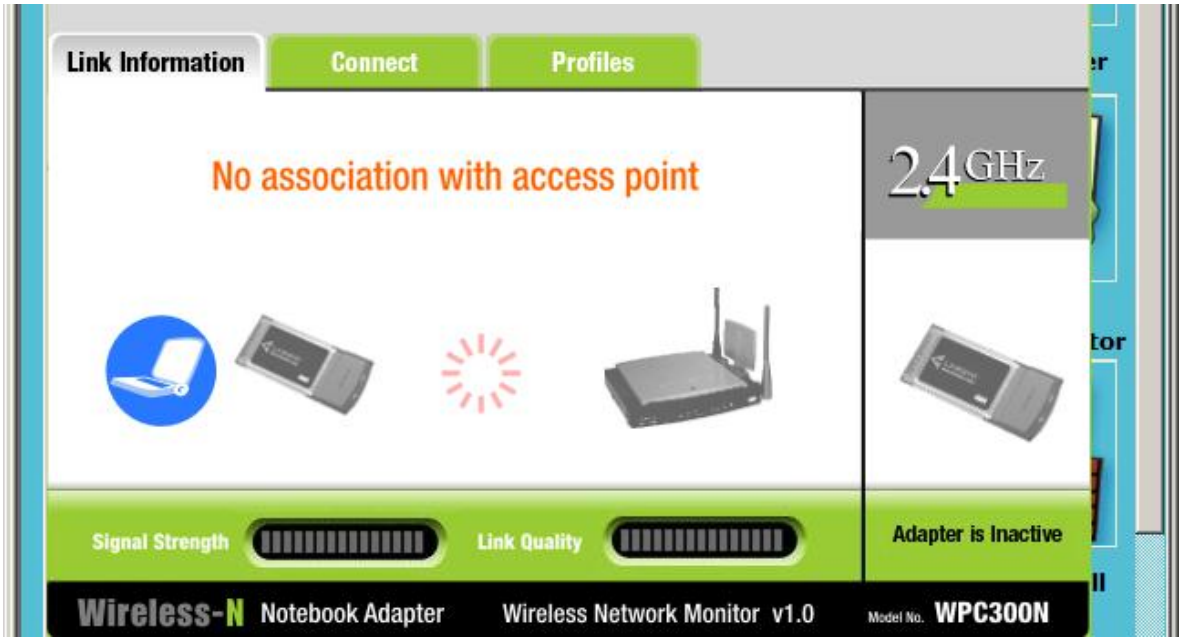
b. Haga clic en Save Settings. Introduzca el nombre de usuario admin y la nueva contraseña.



Parte 3: Configurar y verificar el acceso al cliente inalámbrico.

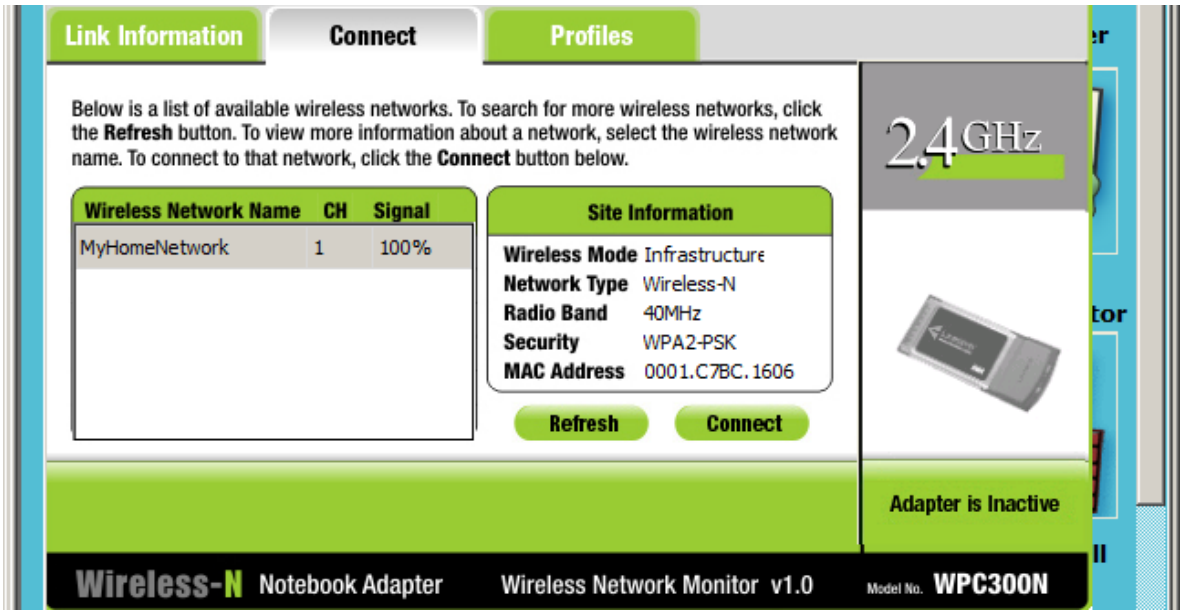
Paso 1: Configurar la computadora portátil para acceder a la red inalámbrica

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.



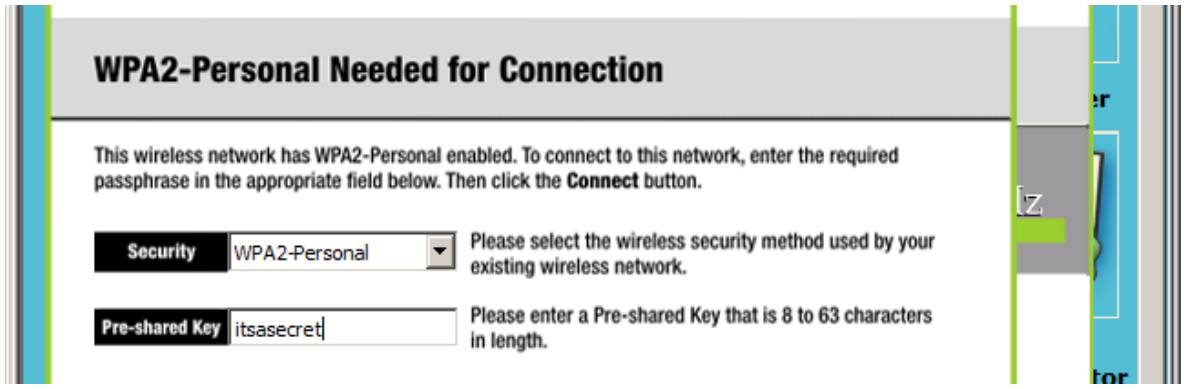
b. Haga clic en la ficha Connect (Conectar) y después en Refresh (Actualizar), si es necesario. Debería ver la red MiRedDoméstica indicada en Wireless Network Name (Nombre de red inalámbrica).

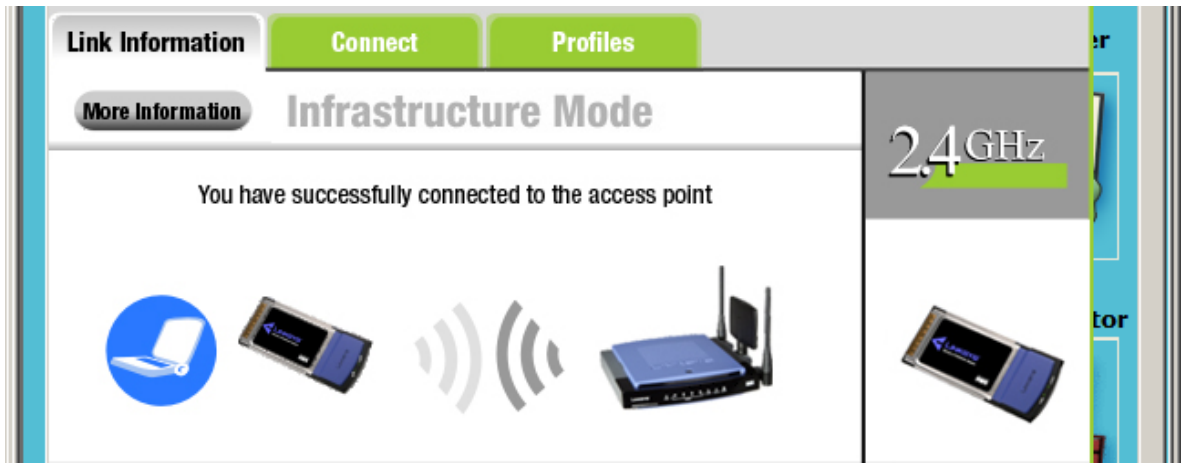
c. Haga clic en MiRedDoméstica y después en Connect.



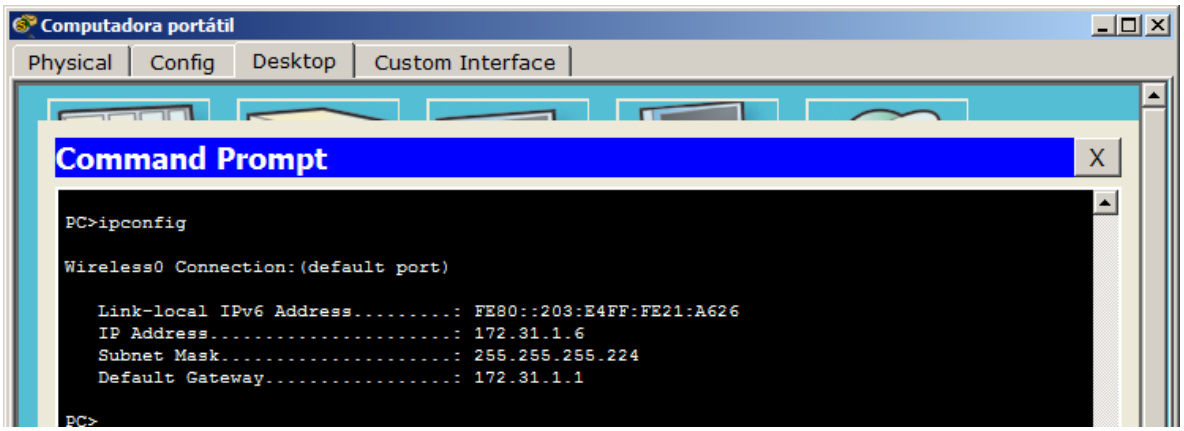
d. Ahora debería ver la red MiRedDoméstica. Haga clic en esta y después en Connect.

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.



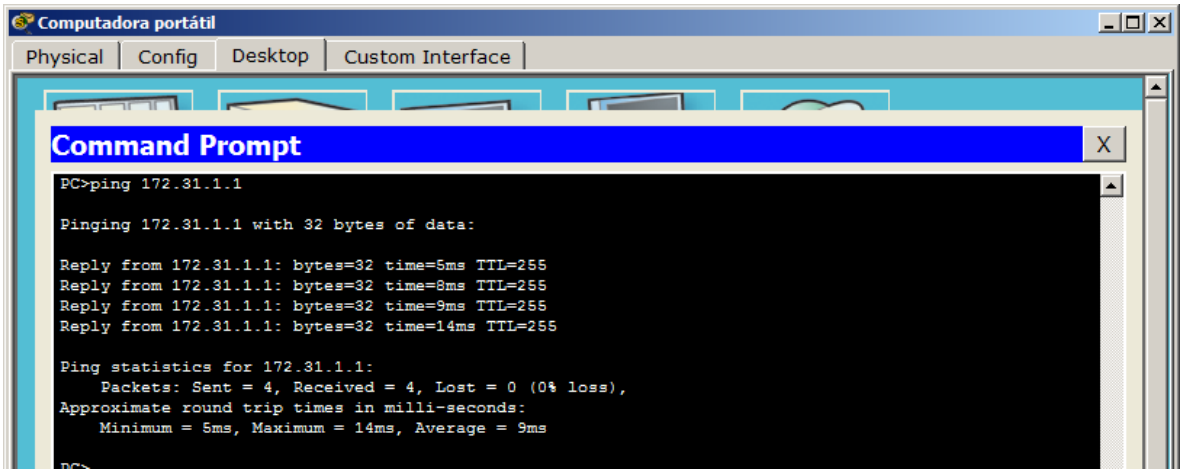


f. Cierre la GUI de Linksys y haga clic en Command Prompt (Símbolo del sistema). Introduzca el comando ipconfig para verificar si Laptop recibió el direccionamiento IP.

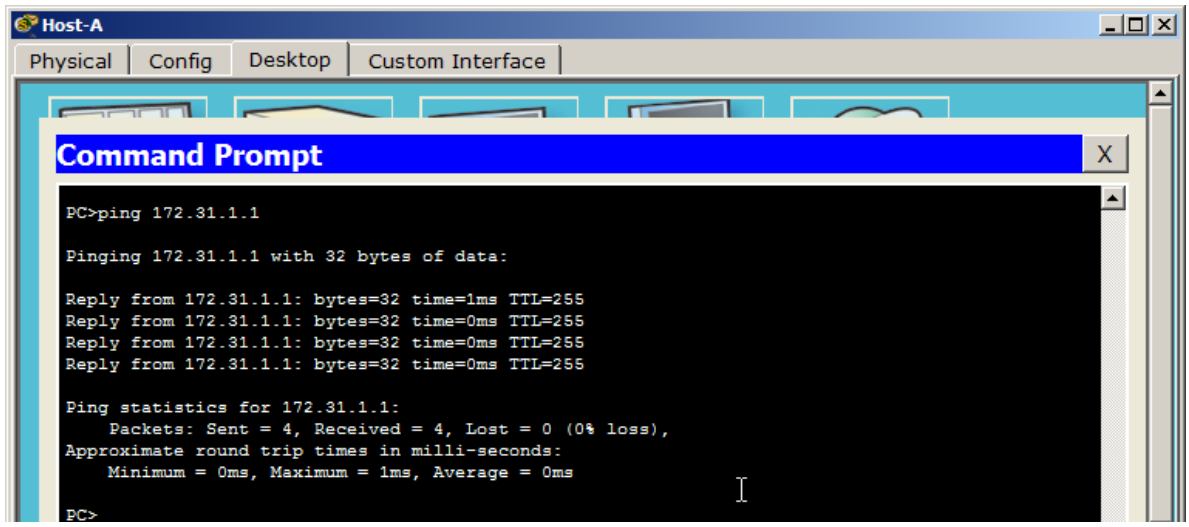


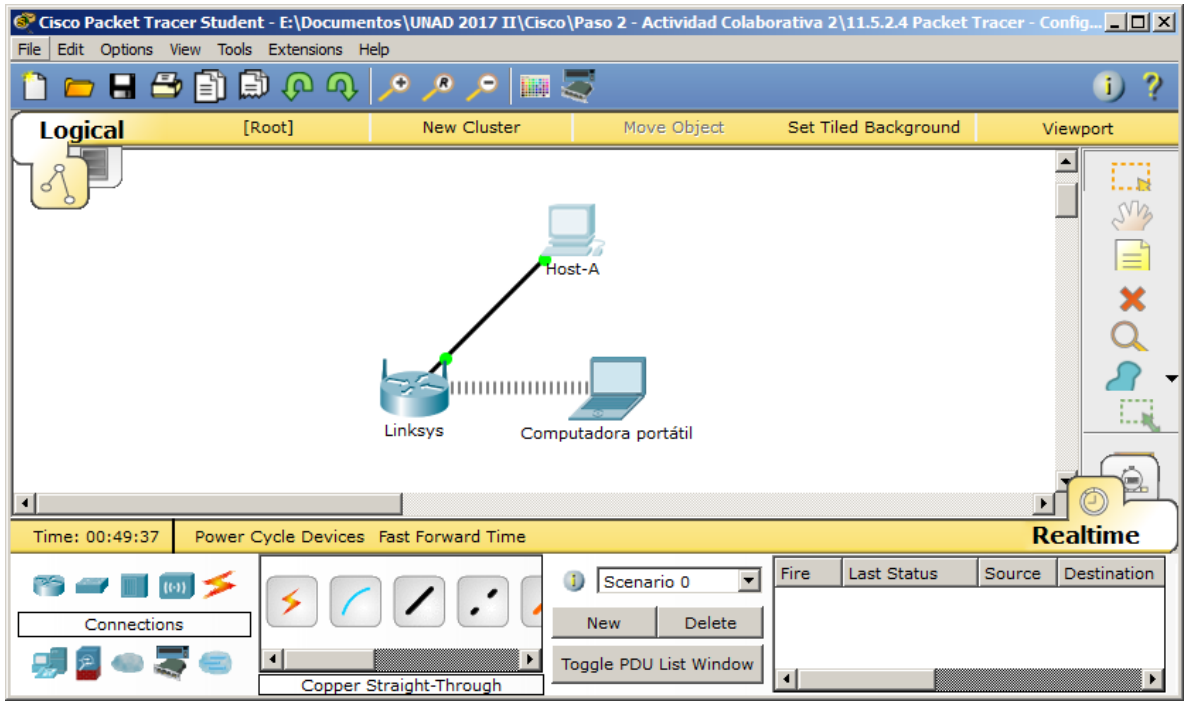
Paso 2: Verificar la conectividad entre la computadora portátil y el Host-A

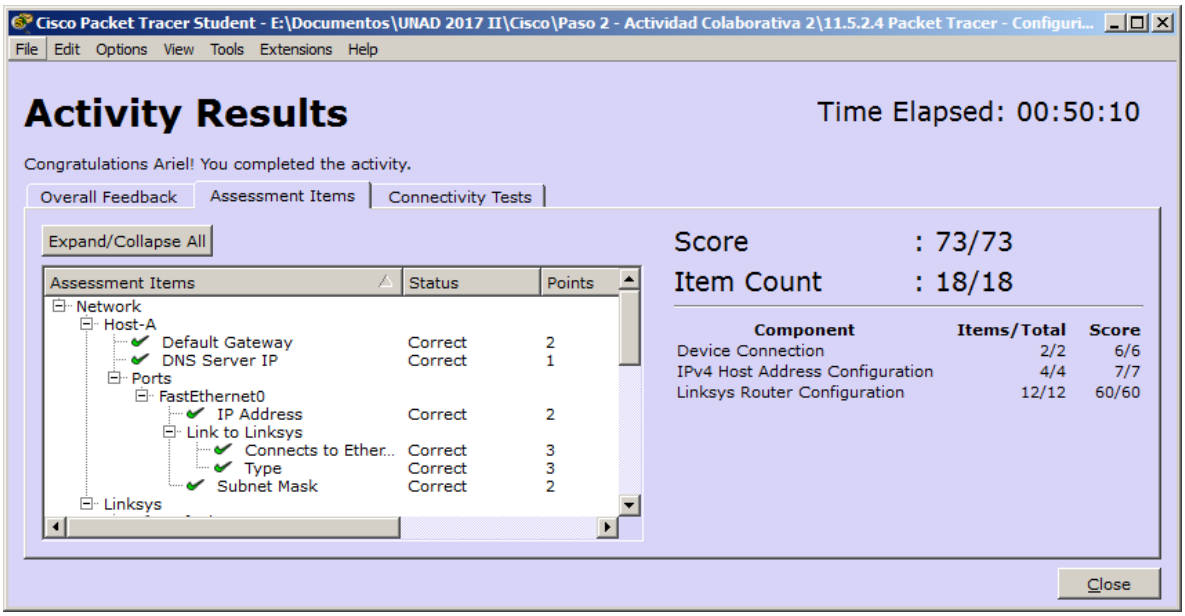
a. Haga ping al router Linksys desde la computadora portátil.



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


Host-A
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 172.31.1.1
Pinging 172.31.1.1 with 32 bytes of data:
Reply from 172.31.1.1: bytes=32 time=1ms TTL=255
Reply from 172.31.1.1: bytes=32 time=0ms TTL=255
Reply from 172.31.1.1: bytes=32 time=0ms TTL=255
Reply from 172.31.1.1: bytes=32 time=0ms TTL=255
Ping statistics for 172.31.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>


Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 2 - Actividad Colaborativa 2\11.5.2.4 Packet Tracer - Config...
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Host-A
Linksys
Computadora portátil
Time: 00:49:37
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination



Notas:

- Para poder completar la actividad un 73/73 fue necesario cambiar el nombre de la red por “MyHomeNetwork”
- Al abrir el archivo hay que conectar el computador portátil a la red para que se pueda tener la actividad desarrollada 73/73. Contraseña: **itsasecret**

11.6.1.2 Skills Integration Challenge Instructions IG

Reto de habilidades de integración

Topología

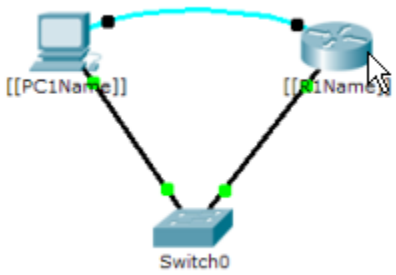


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Main	G0/0	192.168.10.1	255.255.255.0
NetAdmin	NIC	192.168.10.2	255.255.255.0

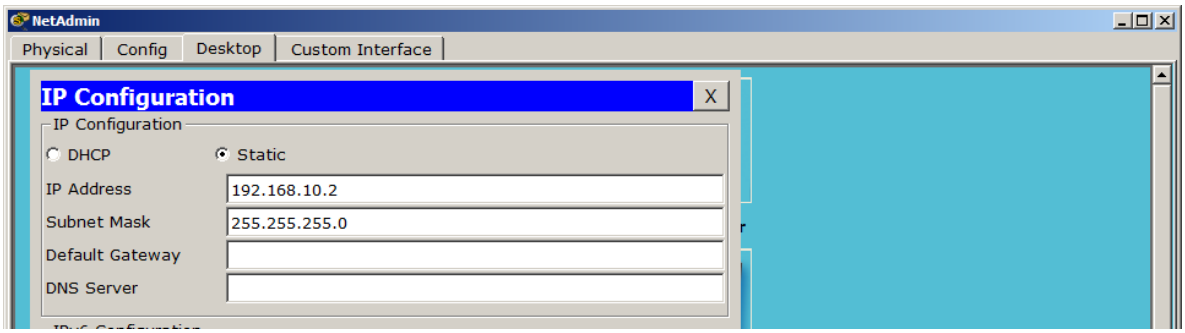
Situación

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.

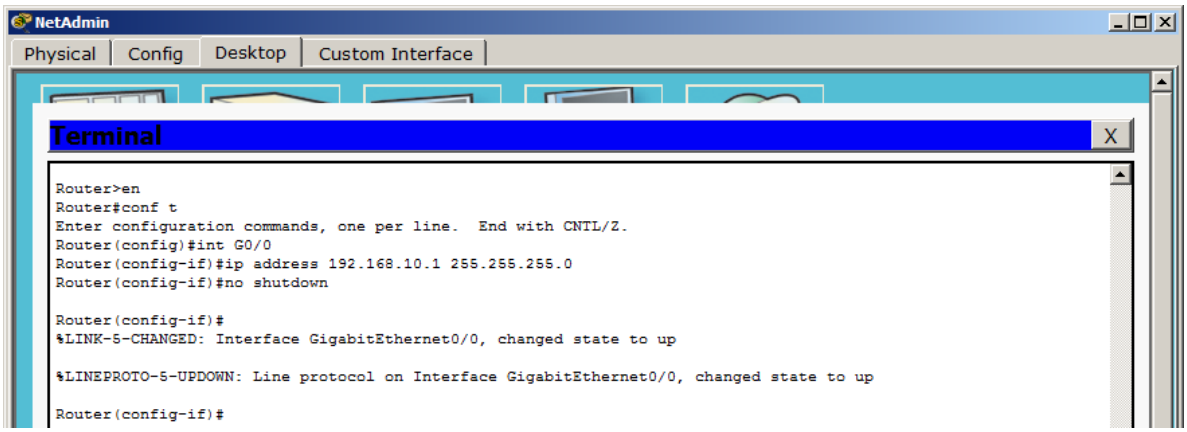
Requisitos

- Configure el direccionamiento IP en **NetAdmin** y **Main**.

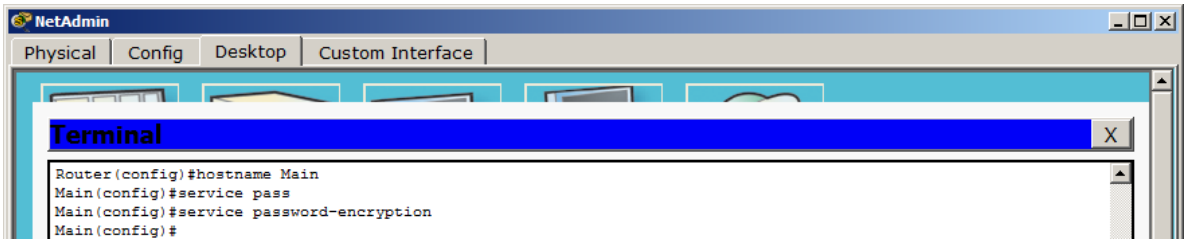
NetAdmin



Main

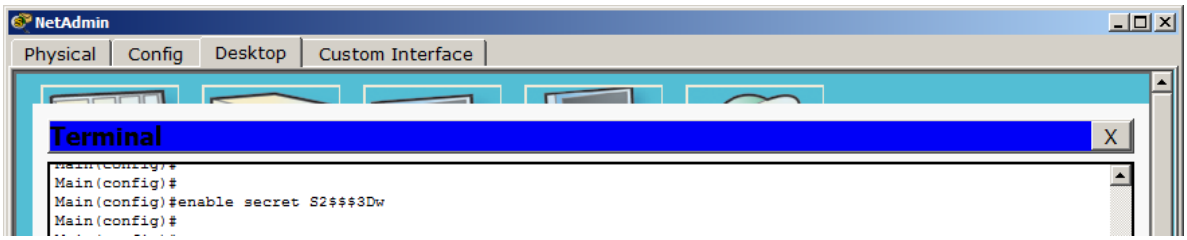


- Configure el nombre de host como **Main** y encripte todas las contraseñas de texto no cifrado.

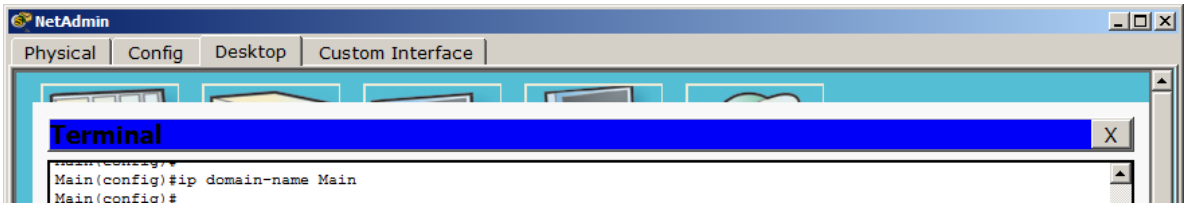


- Establezca la contraseña secreta segura que desee.

Contraseña: S2$$$3Dw

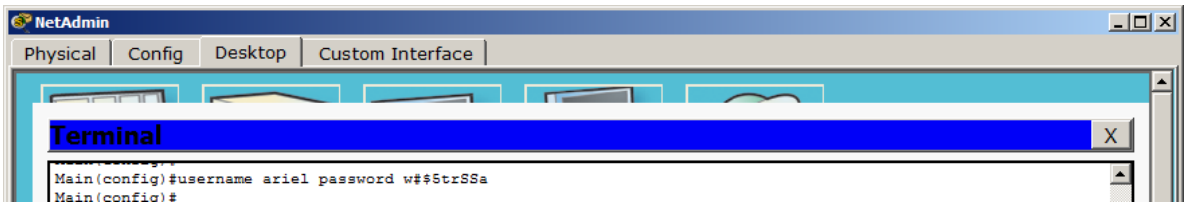


- Establezca el nombre de dominio en **Main** (distinguir mayúsculas de minúsculas).



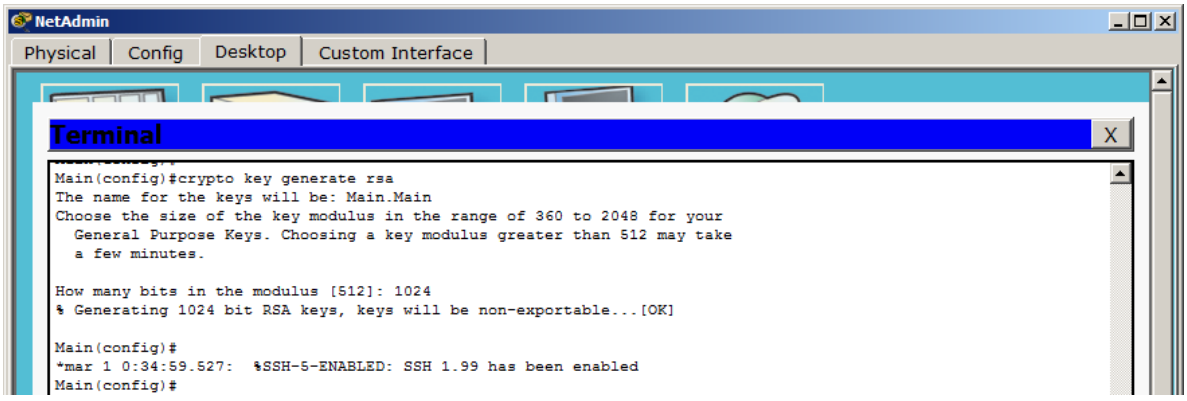
- Cree un usuario de su elección con una contraseña segura.

Usuario: ariel
Contraseña: w#$5trSSa

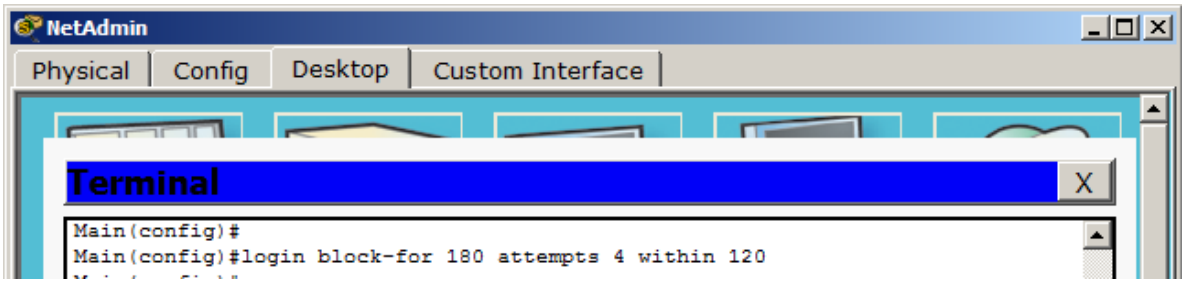


- Genere claves RSA de 1024 bits.

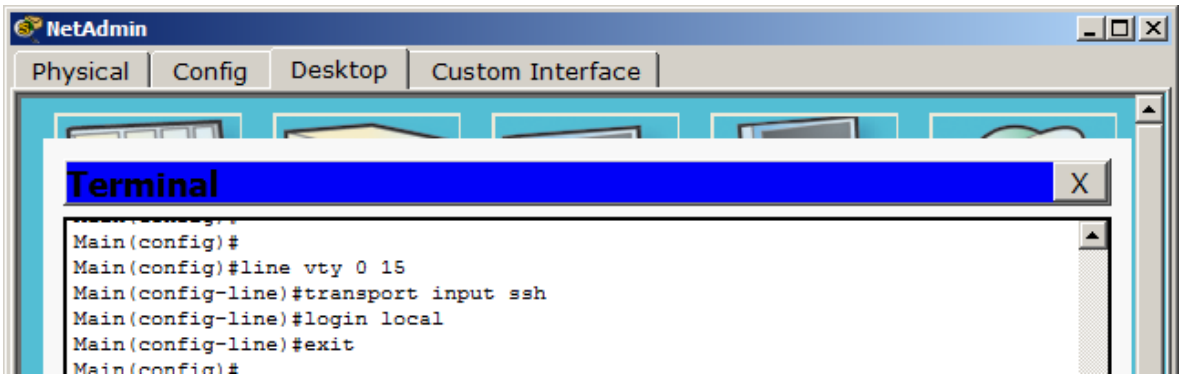
  Nota: en Packet Tracer, introduzca el comando **crypto key generate rsa** y presione tecla **Entrar** para continuar.



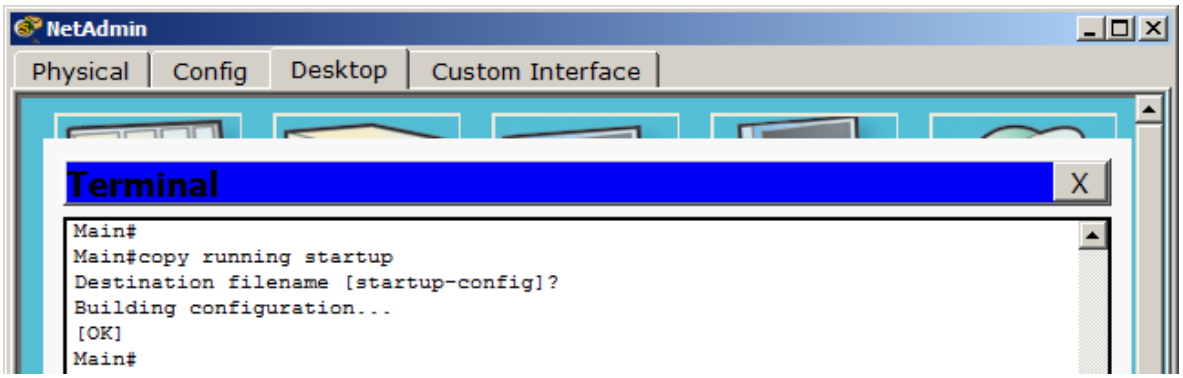
- Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un período de dos minutos.



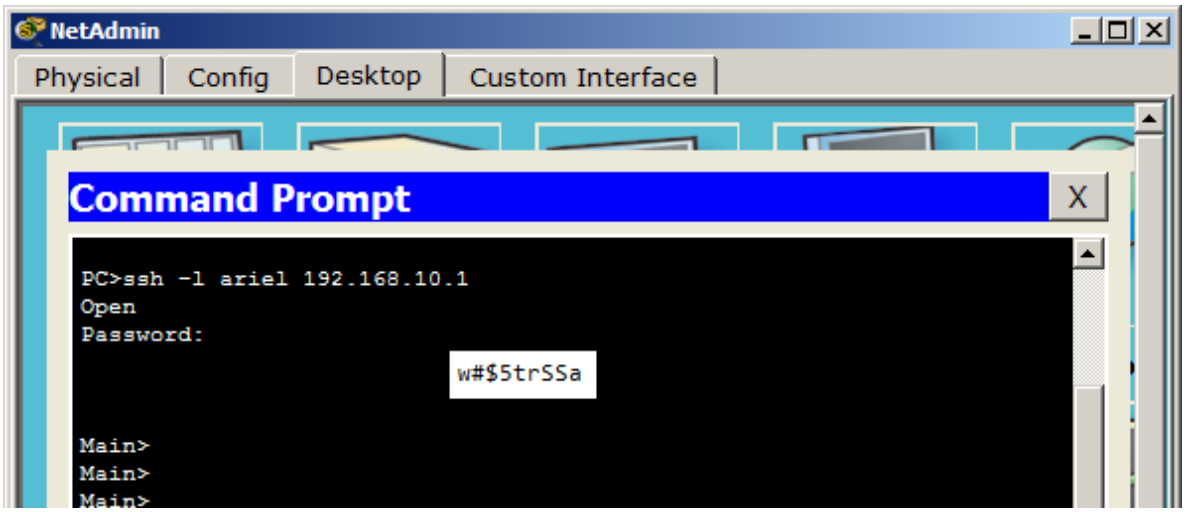
- Configure las líneas vty para el acceso por SSH y solicite los perfiles de usuarios locales.



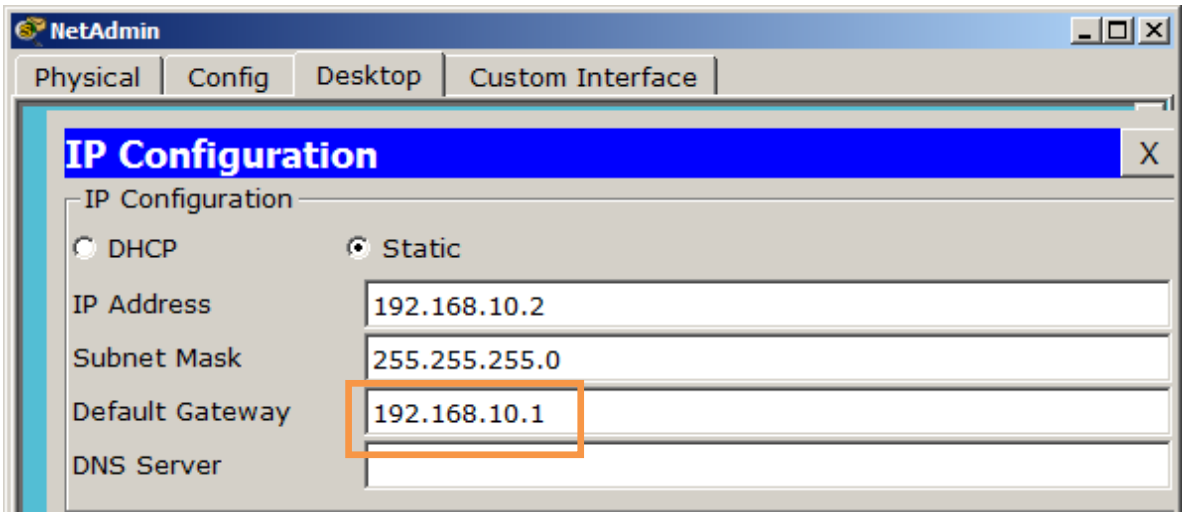
- Guardar la configuración en la NVRAM.

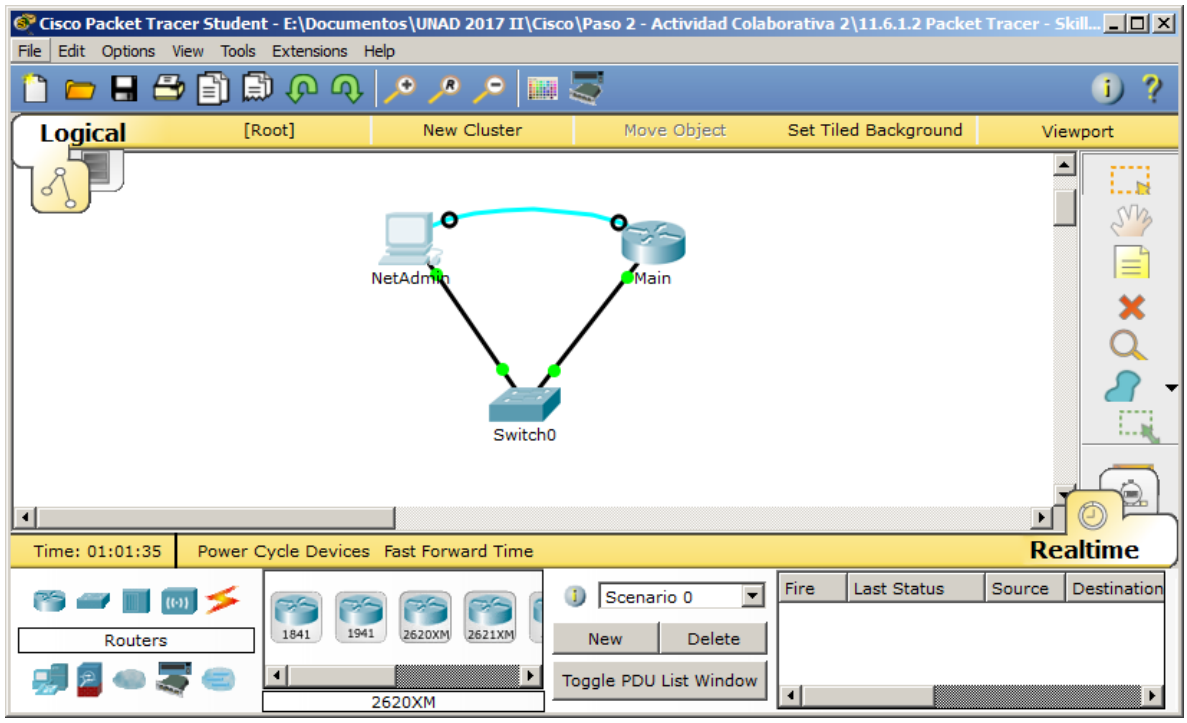


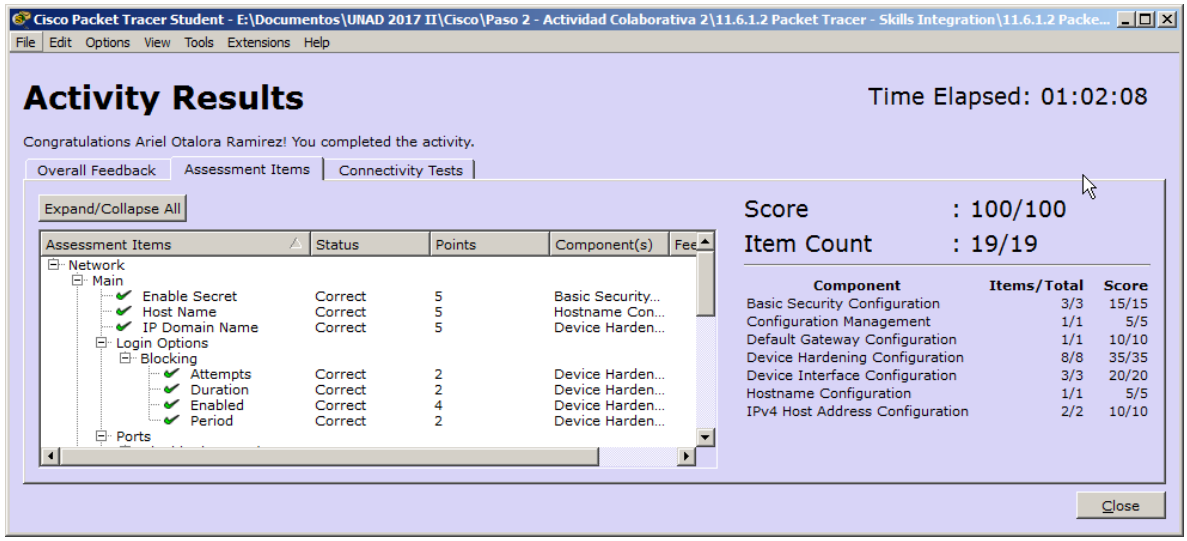
- Esté preparado para demostrar al instructor que estableció el acceso por SSH de **NetAdmin** a **Main**.

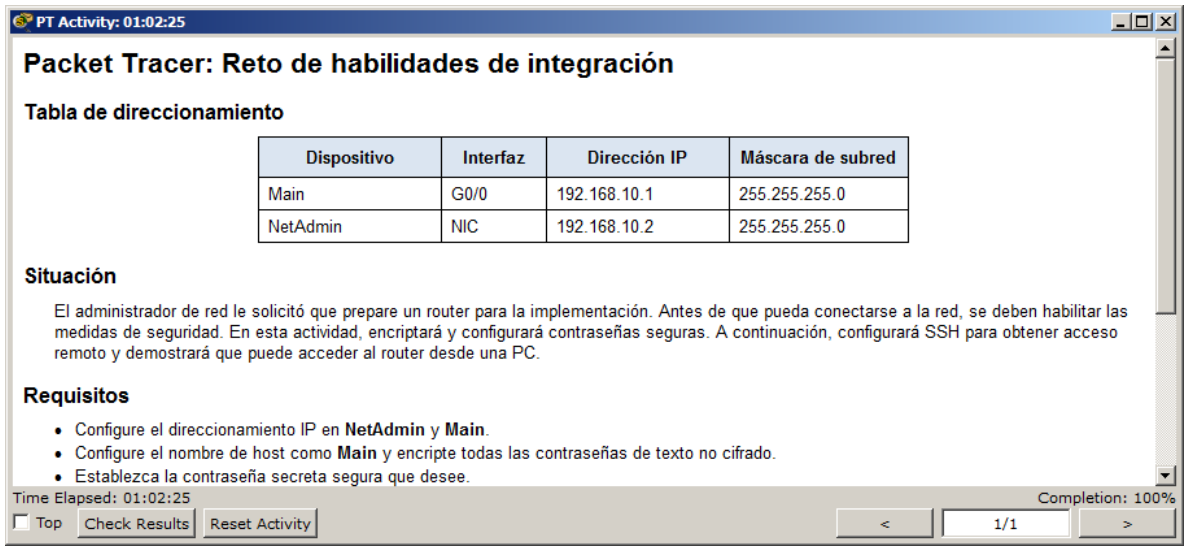


Puerta de enlace predeterminada:




Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 2 - Actividad Colaborativa 2\11.6.1.2 Packet Tracer - Skill...
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
NetAdmin
Main
Switch0
Time: 01:01:35
Power Cycle Devices
Fast Forward Time
Realtime
Routers
1841
1941
2620XM
2621XM
2620XM
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination


Cisco Packet Tracer Student - E:\Documentos\UNAD 2017 II\Cisco\Paso 2 - Actividad Colaborativa 2\11.6.1.2 Packet Tracer - Skills Integration\11.6.1.2 Packe...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:02:08
Congratulations Ariel Otalora Ramirez! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Component(s)
Network
Main
Enable Secret Correct 5 Basic Security...
Host Name Correct 5 Hostname Con...
IP Domain Name Correct 5 Device Harden...
Login Options
Blocking
Attempts Correct 2 Device Harden...
Duration Correct 2 Device Harden...
Enabled Correct 4 Device Harden...
Period Correct 2 Device Harden...
Ports
Score : 100/100
Item Count : 19/19
Component
Items/Total
Score
Basic Security Configuration 3/3 15/15
Configuration Management 1/1 5/5
Default Gateway Configuration 1/1 10/10
Device Hardening Configuration 8/8 35/35
Device Interface Configuration 3/3 20/20
Hostname Configuration 1/1 5/5
IPv4 Host Address Configuration 2/2 10/10
Close


PT Activity: 01:02:25
Packet Tracer: Reto de habilidades de integración
Tabla de direccionamiento
Dispositivo
Interfaz
Dirección IP
Máscara de subred
Main
G0/0
192.168.10.1
255.255.255.0
NetAdmin
NIC
192.168.10.2
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 NetAdmin y Main.
Configure el nombre de host como Main y encripte todas las contraseñas de texto no cifrado.
Establezca la contraseña secreta segura que desee.
Time Elapsed: 01:02:25
Completion: 100%
Top
Check Results
Reset Activity
<
1/1
>

Conclusiones

- Se genera tráfico de red y se examina la funcionalidad de los protocolos TCP y UDP
- Se analiza e investiga el tráfico de unicast, broadcast
- Con el Packet Tracer se configura y verifica el direccionamiento IPv4 e IPv6
- Con la utilización del ping para el rastreo y así probar las rutas que se le asignan a las topologías
- Se desarrollan los retos de habilidades de integración
- Se analiza y trabaja la división de subredes, al igual que la implementación del esquema de direccionamiento IPv6 dividido en subredes
- Se maneja la configuración de los servidores web, de correo electrónico, de DHCP, de DNS y FTP

Bibliografía

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). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

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

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