DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN / WAN)

LABORATORIOS UNIDAD 2
CISCO CCNA 1

Teder Alberto Gamarra Martínez

Código: 1.103. 172.345

Diplomado en Cisco presentado como requisito para optar al título profesional en Ingeniería de Sistemas

PhD. Juan Carlos Vesga Ferreira

Asesor

Universidad Nacional Abierta y a Distancia - UNAD Escuela de Ciencias Básicas y Tecnologías de la Información- ECBTI

Diplomado en Cisco 2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

AGRADECIMIENTOS

Agradecerle primero que todo a Dios por haberme guiado y acompañado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Gracias a mis padres Isaac Gamarra y Margith Martinez, por apoyarme en todo el proceso de formacion, por los valores que me han inculcado, por haberme dado la oportunidad de tener una excelente educacion a lo largo de mi vida.

Por ultimo agradecer al cuerpo de Docentes UNAD quienes me apoyaron en el proceso académico para no rendirme y seguir hasta el final.

"Un sueño no se hace realidad atreves de magia, conlleva sudor, determinación y trabajo duro"

Contenido

INTRODUCCION

El presente trabajo corresponde al desarrollo de una serie de actividades correspondientes al Momento II del curso de profundización de Cisco (diseño e implementación de soluciones integradas LAN/WAN), en el cual se demuestran las destrezas adquiridas luego del estudio de los capítulos de la unidad 2.

Las actividades y áreas de conocimientos que se desarrollan a lo largo de este trabajo giran alrededor del modelo OSI y direccionamiento IP, donde se emula y se practica mediante el software Packet Tracer diferentes funcionalidades sobre temas como la capa de transporte, asignación de direcciones IP, subredes, capa de aplicación y soluciones de red.

Se contó con la participación de los integrantes que actualmente están realizando el curso y se seleccionaron las mejores respuestas que se adjuntan en el actual documento.

OBJETIVOS

OBJETIVO GENERAL:

Realizar las actividades de trasferencia de la Unidad 2, Modelo OSI y direccionamiento IP, del diplomado en redes Cisco, diseño e implementación de soluciones integradas LAN/WAN para comprender conceptos de redes tales como capa de transporte, capa de aplicación, direccionamiento IP, subredes, entre otros, mediante prácticas diseñadas para ser desarrolladas con el software Packet Tracer.

OBJETIVOS ESPECIFICOS:

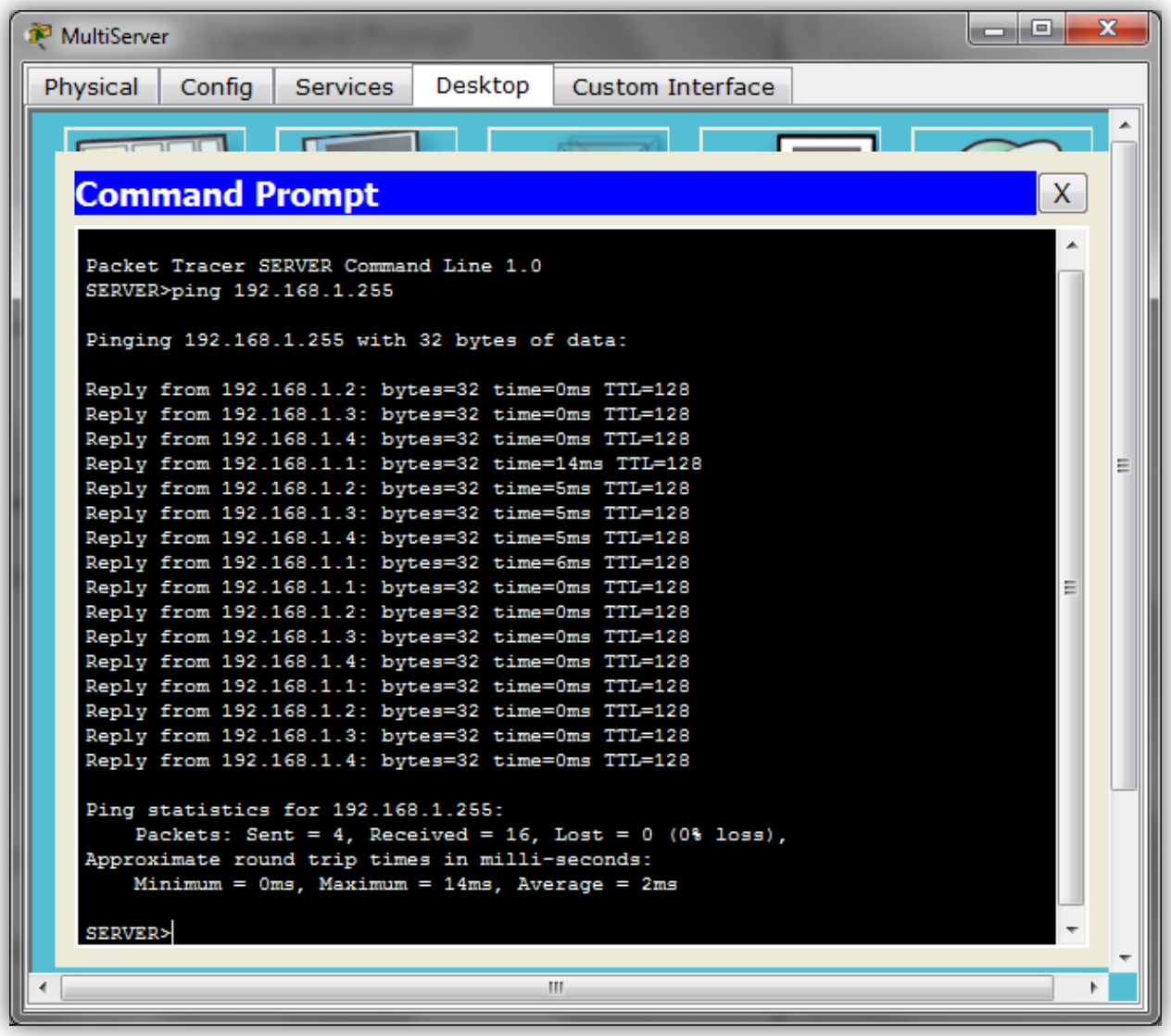
- Desarrollo de los laboratorios de la unidad 2 con el fin de desarrollar nuestras destrezas en la materia.
- Diferenciar entre los diferentes TCP Y UDP y simularlos dentro de Packet Tracer.
- Aprender todo lo relacionado sobre el direccionamiento IPV4 como IPV6.
- Realizar ejercicios de subeneteo aplicando VLSM.
- Desarrollar ejercicios empleando el protocolo FTP para transferir archivos.
- Aplicar el comando SHOW.

DESARROLLO DE LA ACTIVIDAD

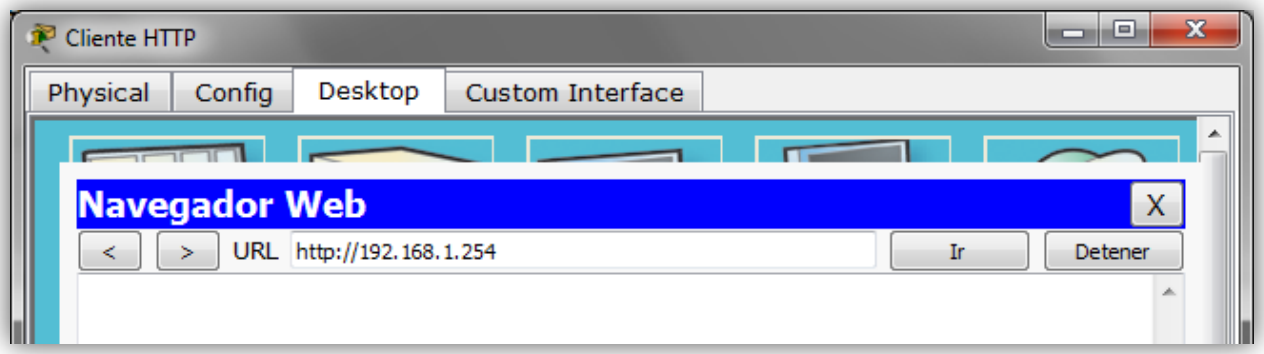
Laboratorio 7.3.1.2

Parte 1: Generar tráfico de red en modo de simulación.

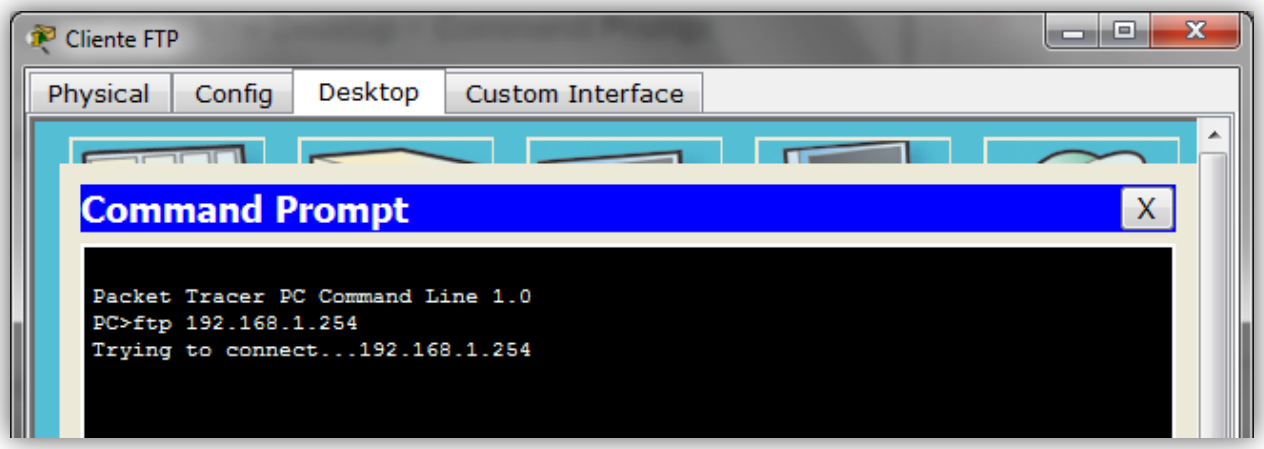
- Paso 1: Generar tráfico para completar las tablas del protocolo de resolución de direcciones (ARP)



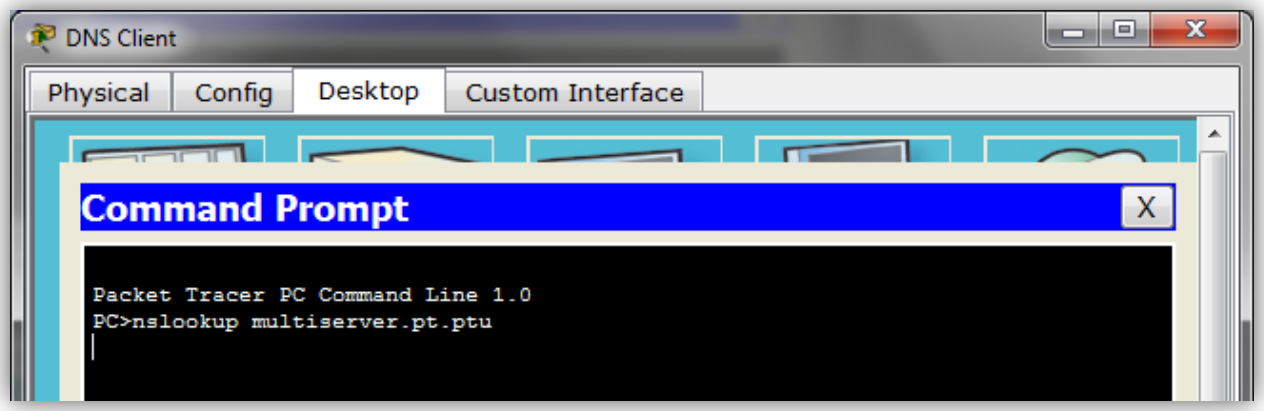
- Paso 2: Genere tráfico web (HTTP).

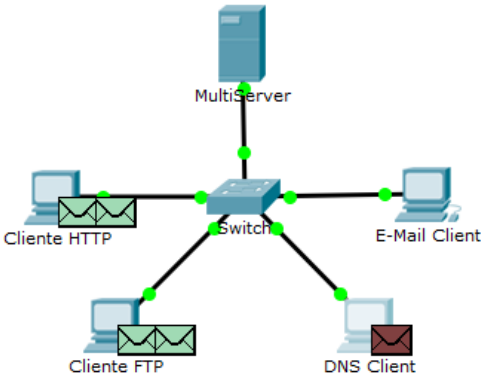


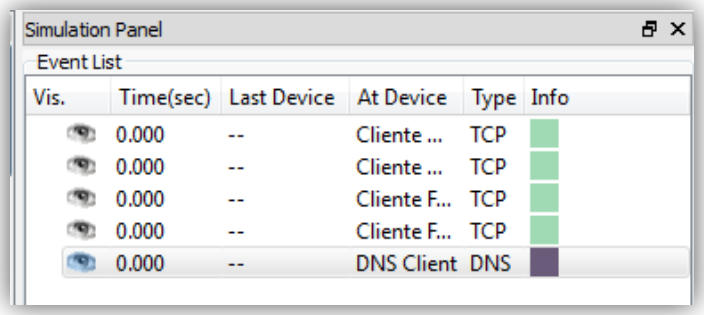
- Paso 3: Generar tráfico FTP



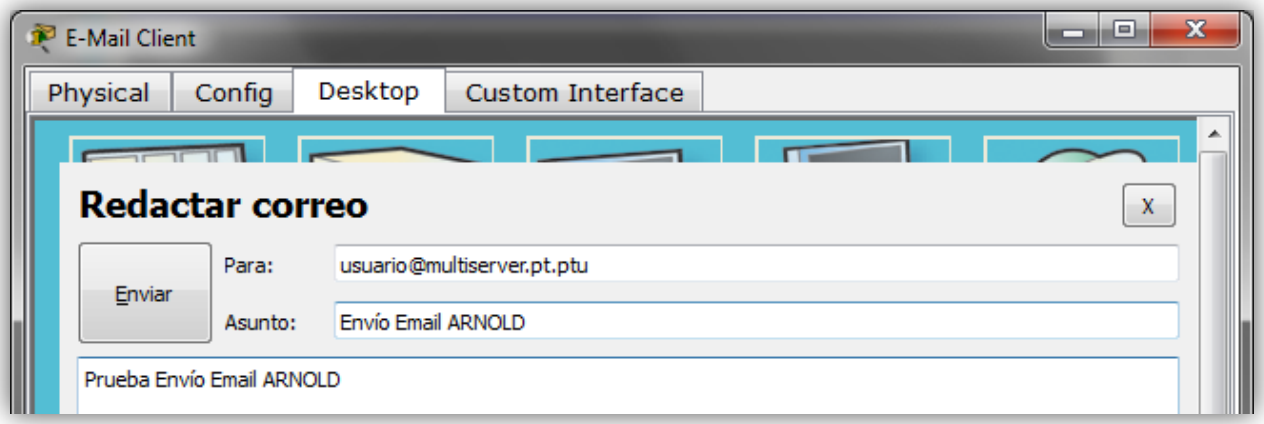
- Paso 4: Generar tráfico DNS
-



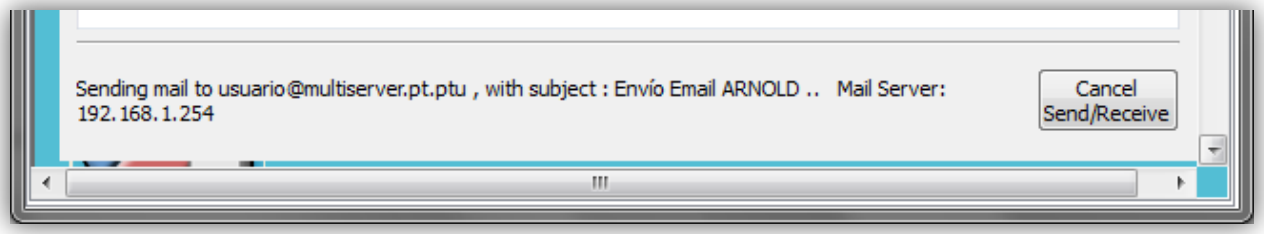




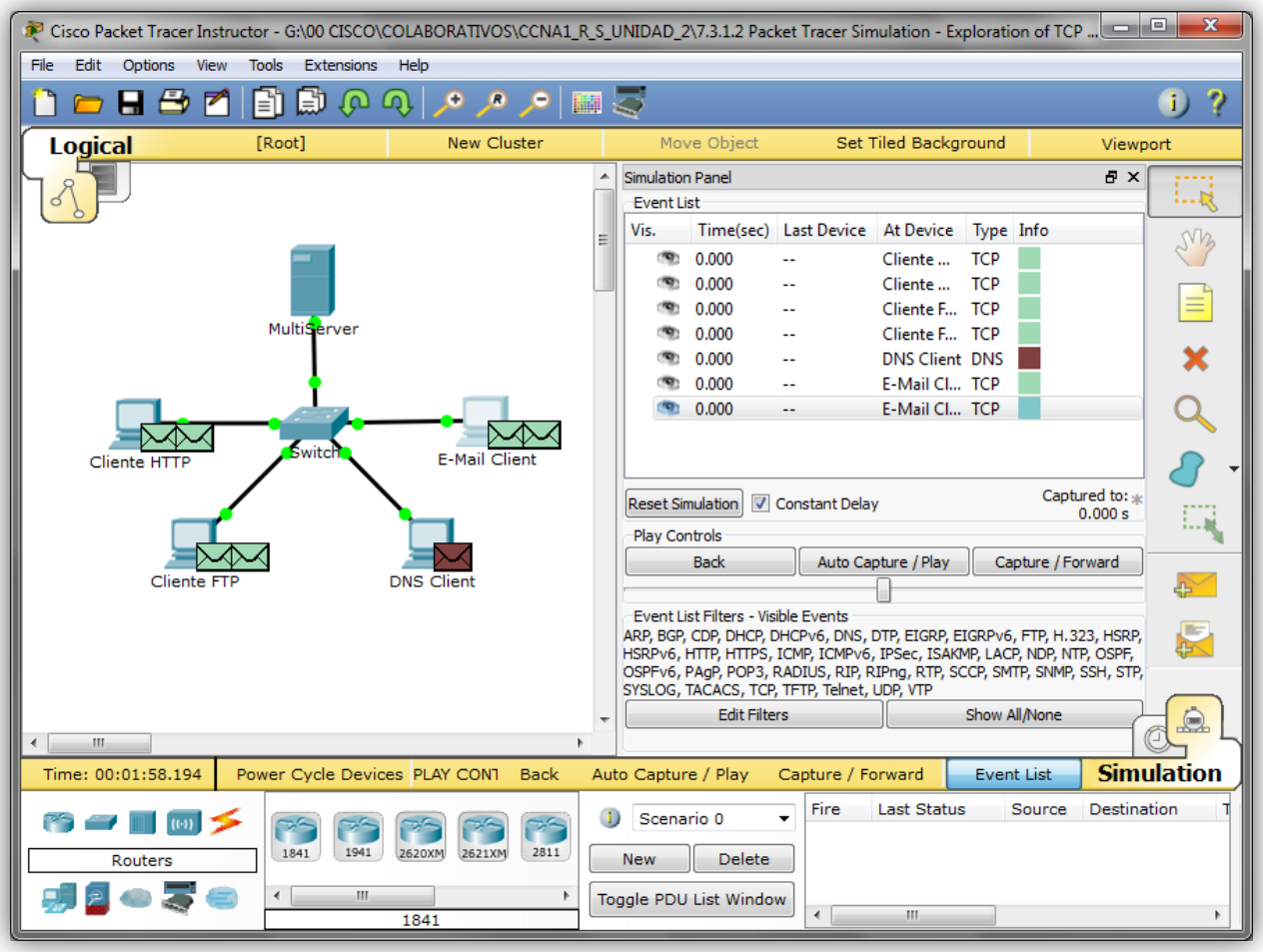
- Paso 5: Generar tráfico de correo electrónico



Después de Enviar



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

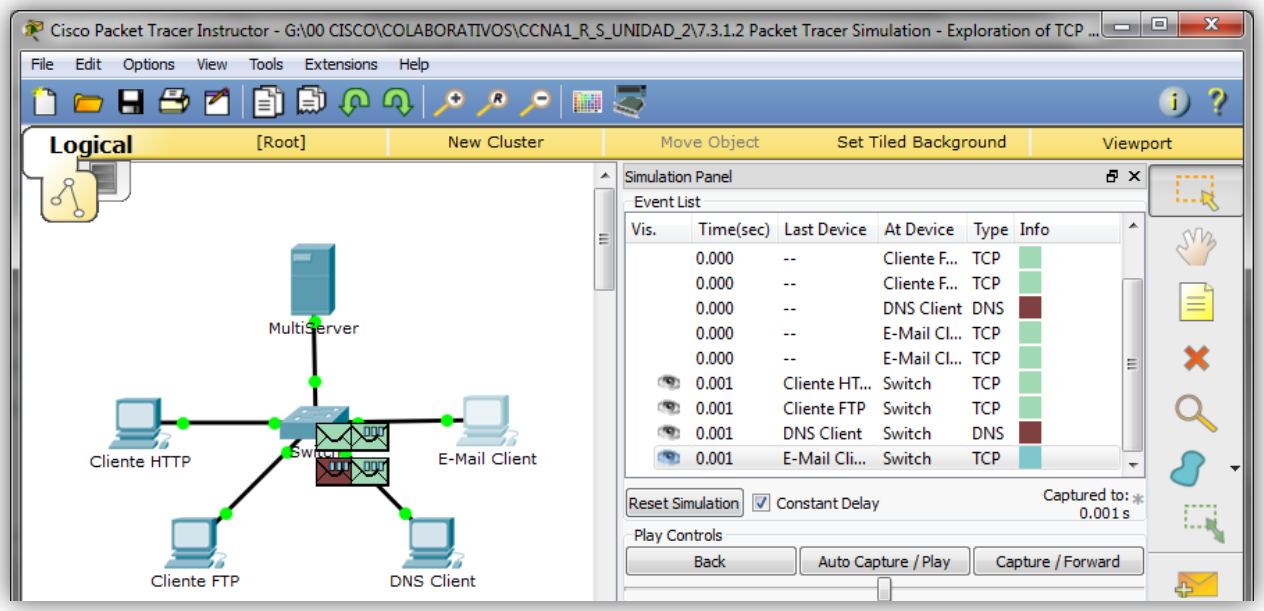


Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

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

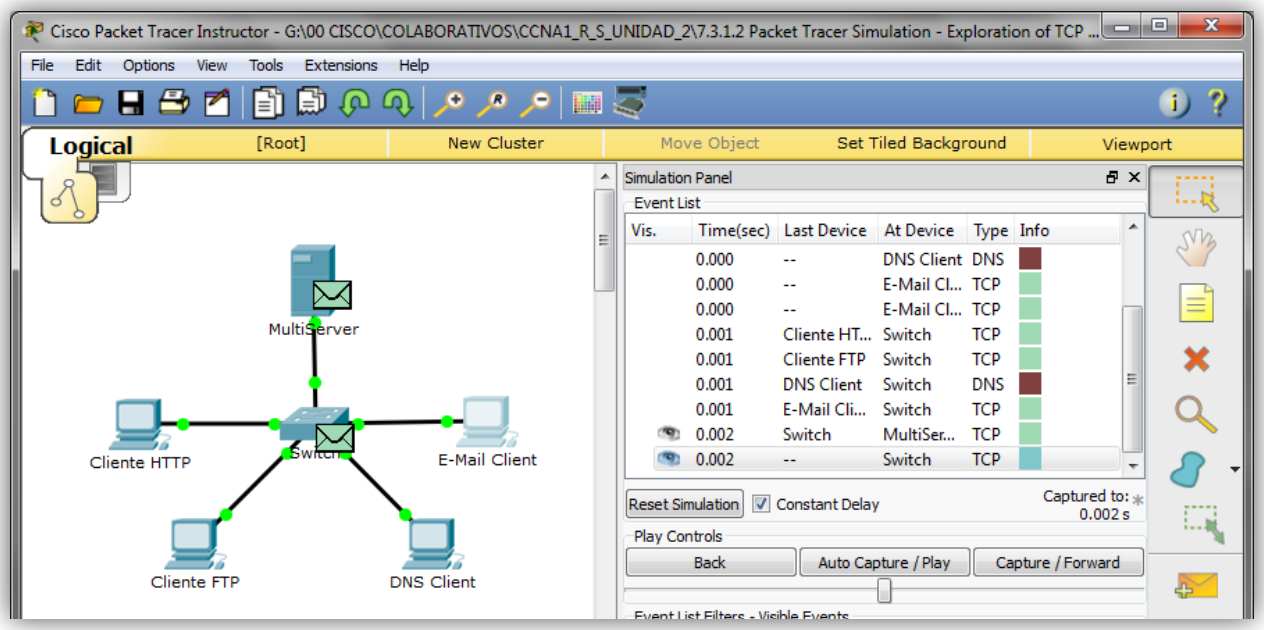
Ahora utilizará los botones **Capture/Forward** (Capturar/avanzar) y **Back** (Atrás) del panel de simulación.

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

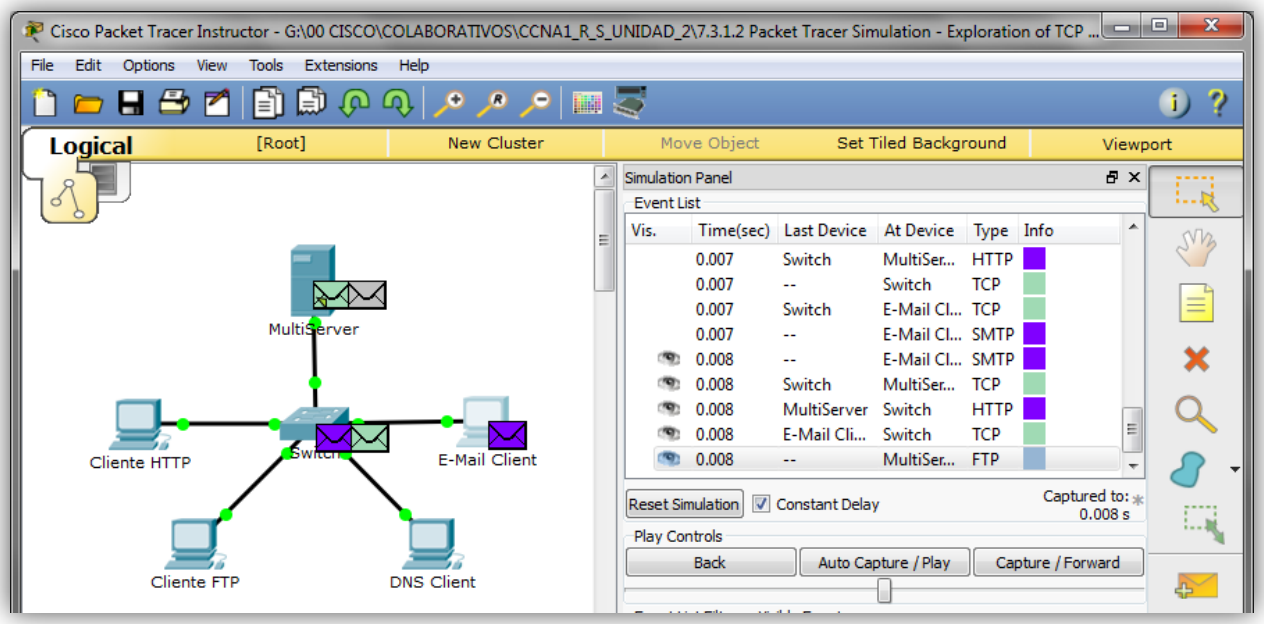


b. Haga clic en **Capture/Forward** nuevamente. Algunas de las PDU desaparecen. ¿Qué cree que ocurrió?

Están almacenadas en el switch.



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.



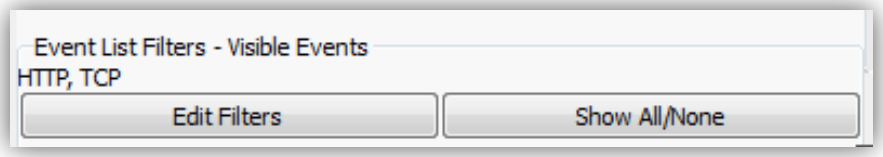
d. En la lista de eventos en el panel superior derecho de la ventana de simulación aparecen una variedad de PDU. ¿Por qué hay tantos colores diferentes?
Representan diferentes protocolos.

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

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

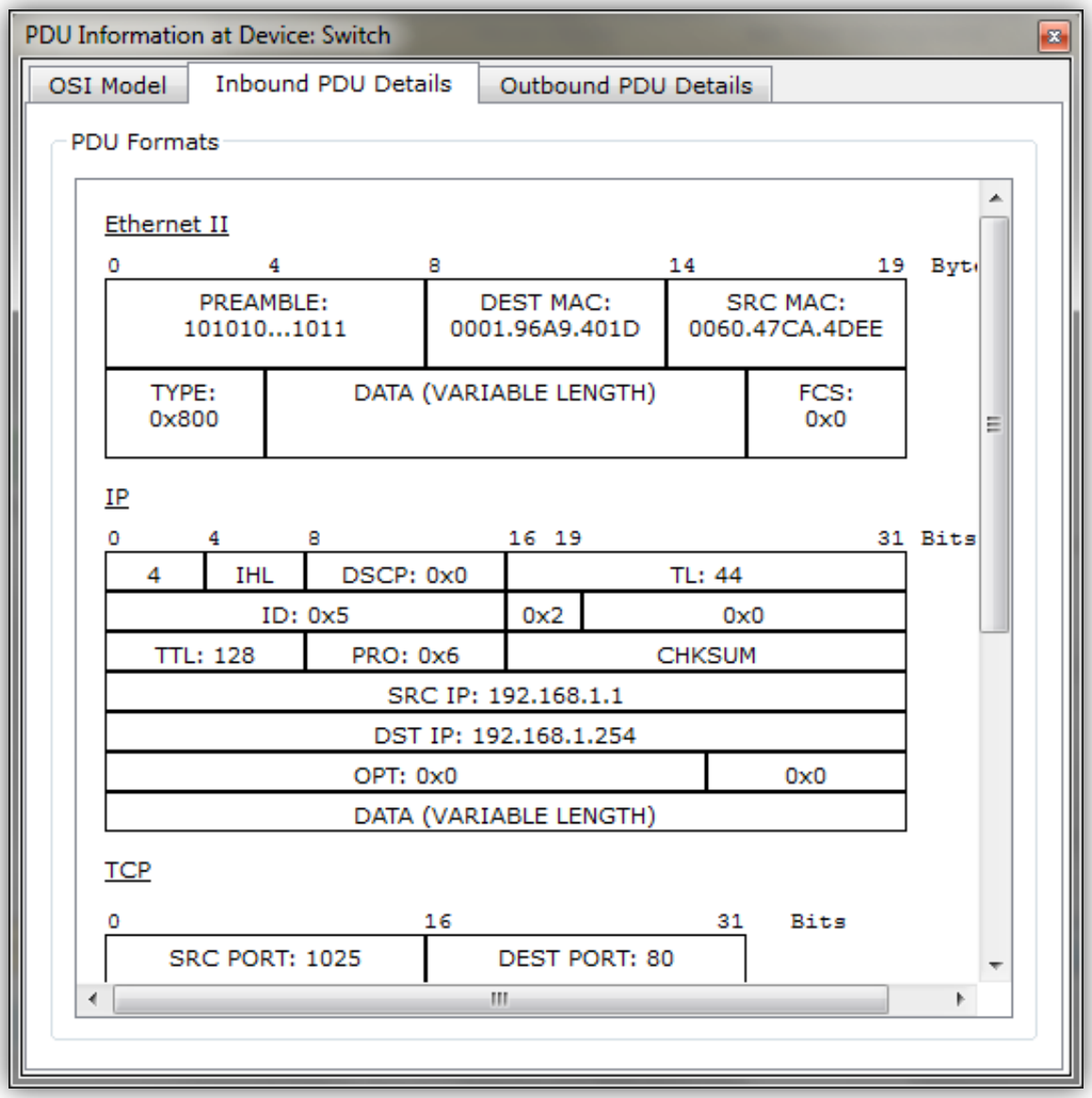
a. Filtre el tráfico que se muestra actualmente para que solo se muestren las PDU de **HTTP** y **TCP**: 1) Haga clic en **Edit Filters** (Editar filtros) y cambie el estado de la casilla de verificación **Show All/None** (Mostrar todos/ninguno).

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



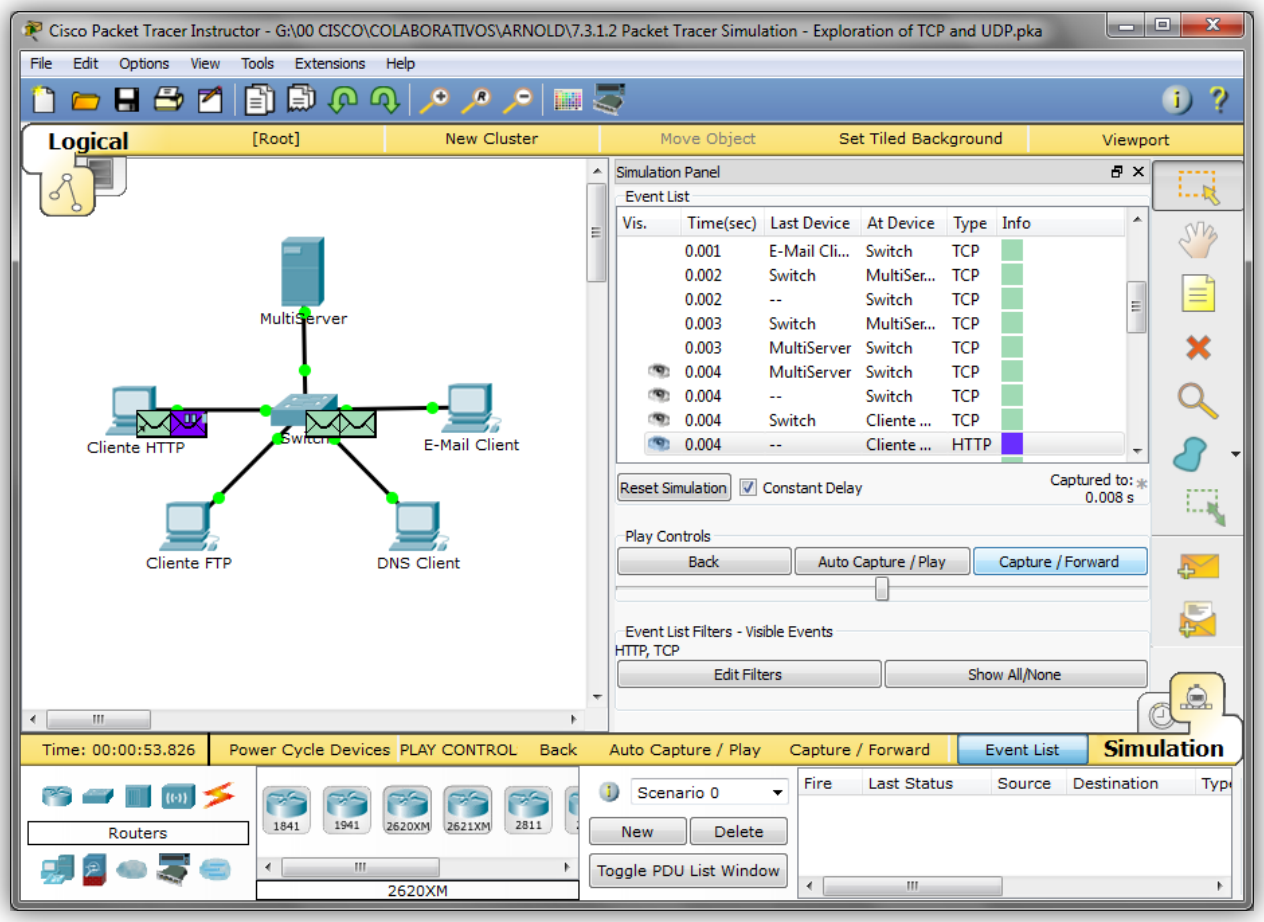
¿Estas comunicaciones se consideran confiables?
Sí.

d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?
1025, 80, 0, 0 SYN

TCP

0	16	31 Bits
SRC PORT: 1025	DEST PORT: 80	
SEQUENCE NUM: 0		
ACK NUM: 0		

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



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

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

TCP

0		16		31	Bits
SRC PORT: 80			DEST PORT: 1025		
SEQUENCE NUM: 0					
ACK NUM: 1					
OFF.	RES.	SYN + ACK	WINDOW		

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

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

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

TCP

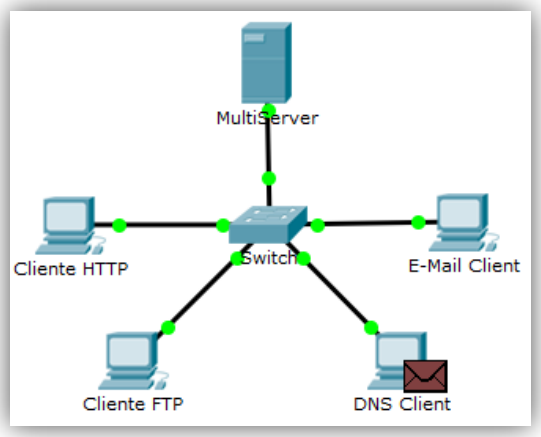
0		16		31	Bits
SRC PORT: 1025			DEST PORT: 80		
SEQUENCE NUM: 1					
ACK NUM: 1					
OFF.	RES.	PSH + ACK	WINDOW		

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

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

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

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



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

¿Estas comunicaciones se consideran confiables?
No

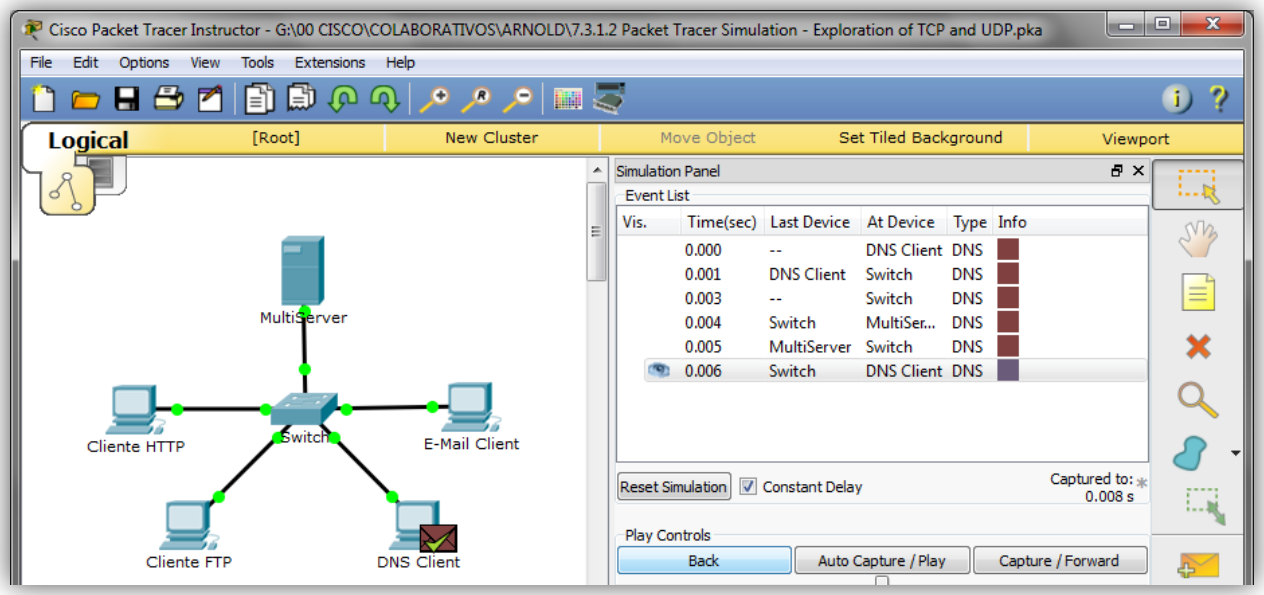
d. Registre los valores de **SRC PORT** (Puerto de origen) y **DEST PORT** (Puerto de destino). ¿Por qué no hay números de secuencia ni de acuse de recibo?

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

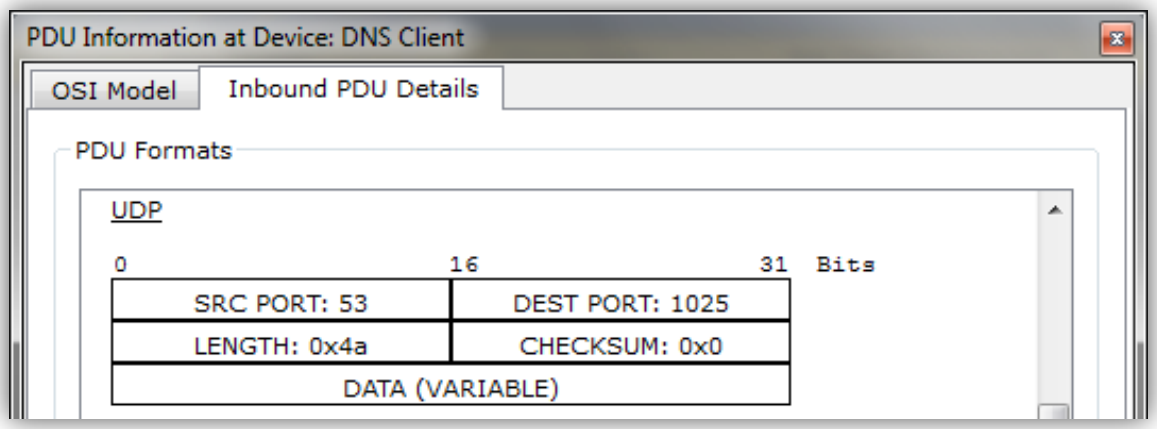
UDP

0	16	31 Bits
SRC PORT: 1025	DEST PORT: 53	
LENGTH: 0x2a	CHECKSUM: 0x0	
DATA (VARIABLE)		

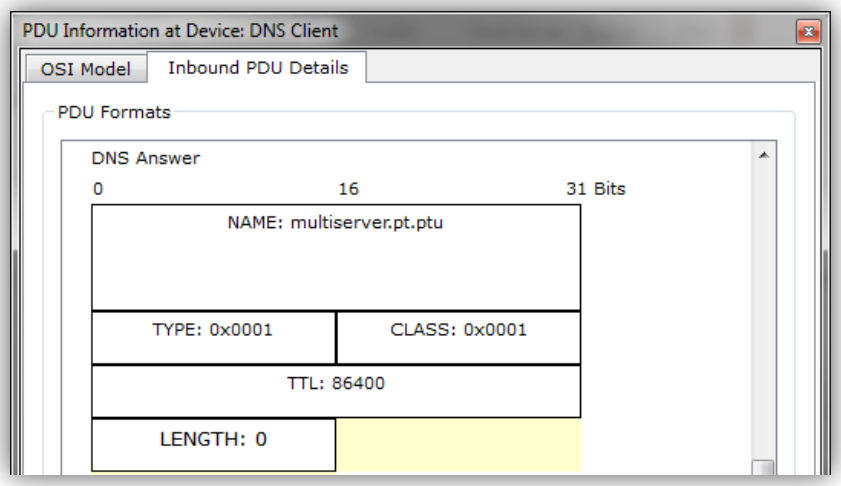
e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva al **cliente DNS** con una marca de verificación.



f. Haga clic en el sobre de PDU y seleccione **Inbound PDU Details**. ¿En qué cambiaron los números de puerto y de secuencia?
53, 1025. Los puertos de origen y destino están invertidos.



g. ¿Cómo se llama la última sección de la **PDU**?
DNS ANSWER (Respuesta DNS)

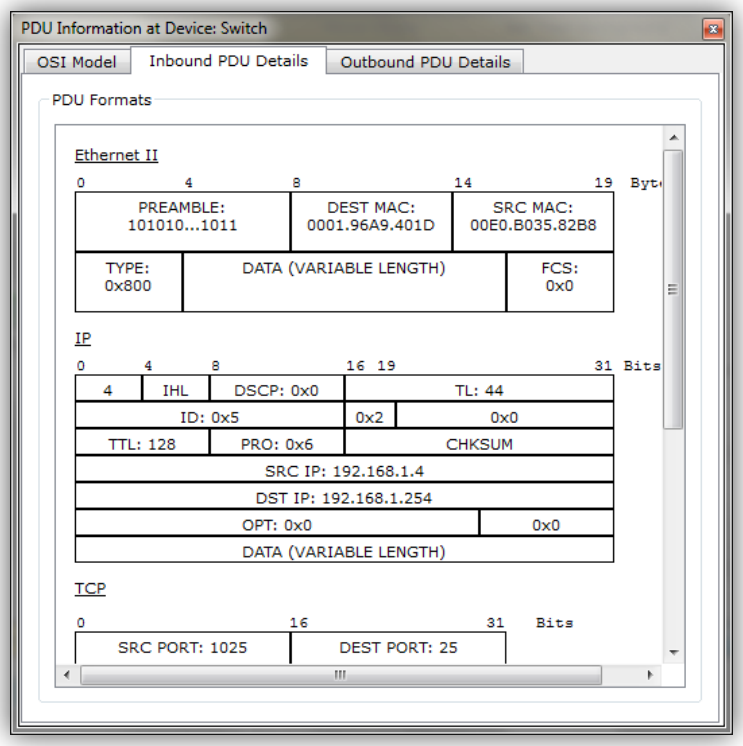


h. Haga clic en **Back** hasta que se restablezca la simulación.

Paso 5: Examinar el tráfico de correo electrónico cuando los clientes se comunican con el servidor a. En el panel de simulación, modifique las opciones de **Edit Filters** para que solo se muestre **POP3, SMTP** y **TCP**.

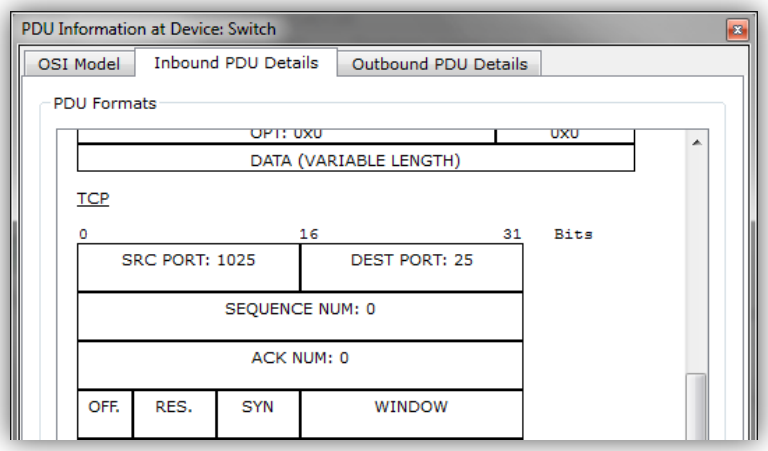
b. Haga clic en **Capture/Forward** (Capturar/avanzar). Pase el cursor sobre cada PDU hasta que encuentre una que se origine en **E-mail Client**. Haga clic en el sobre de PDU para abrirlo.

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

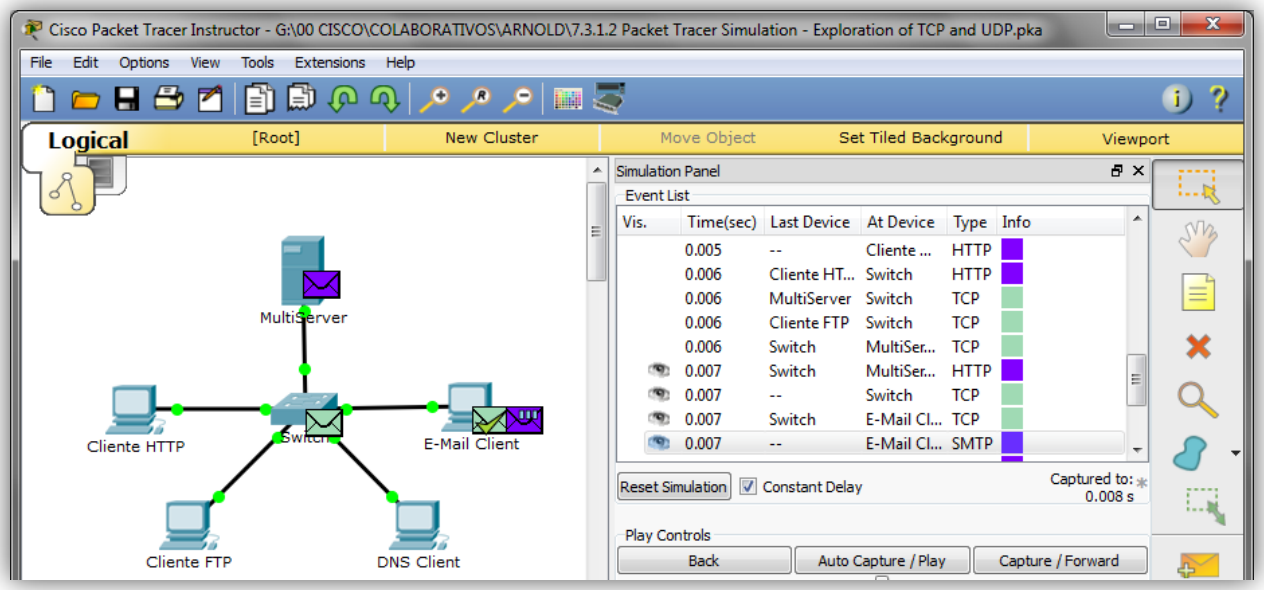


¿Estas comunicaciones se consideran confiables?
Sí.

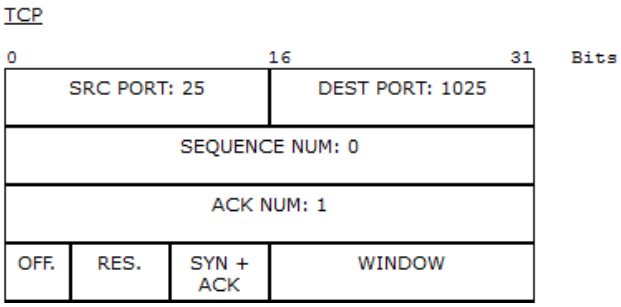
d. Registre los valores de **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** y **ACK NUM** (PUERTO DE ORIGEN, PUERTO DE DESTINO, NÚMERO DE SECUENCIA y NÚMERO DE ACUSE DE RECIBO). ¿Qué está escrito en el campo que se encuentra a la izquierda del campo **WINDOW** (Ventana)?
1025, 25, 0, 0. SYN



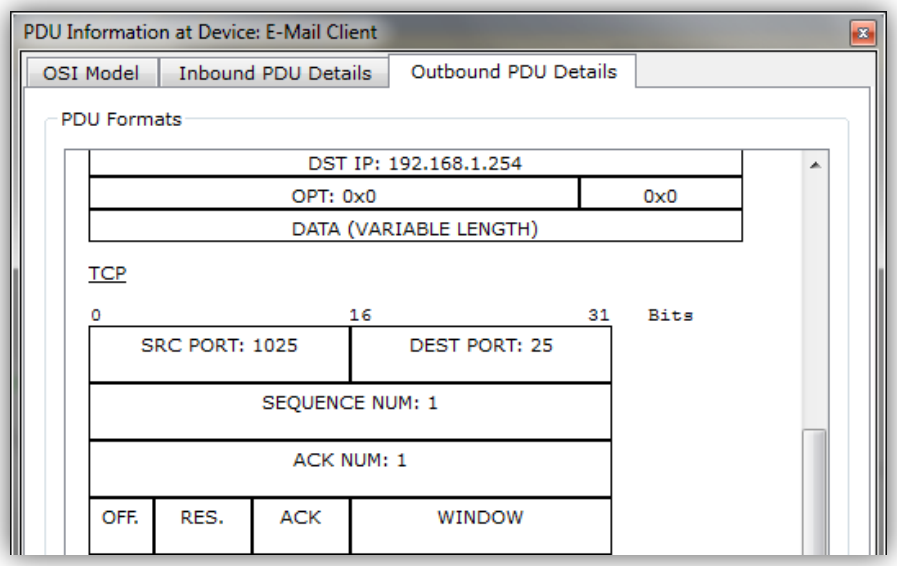
e. Cierre la **PDU** y haga clic en **Capture/Forward** hasta que una PDU vuelva a **E-Mail Client** con una marca de verificación.



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

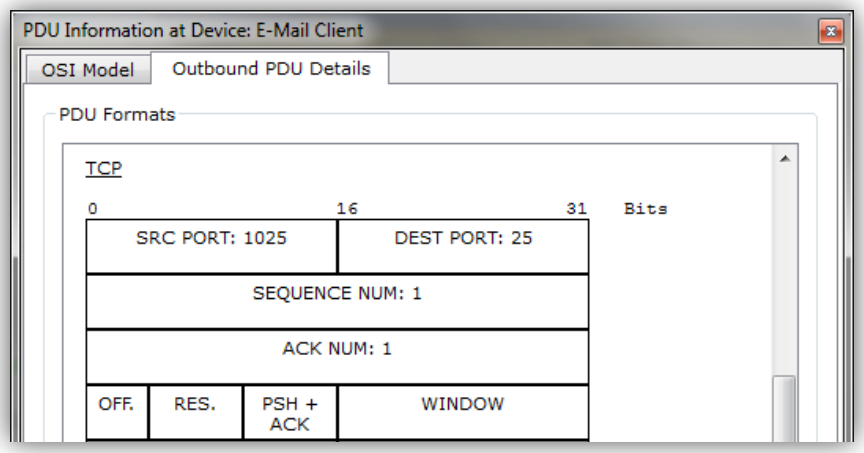


g. Haga clic en la ficha **Outbound PDU Details** (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?
1025, 25, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1. ACK



h. Hay otra **PDU** de un color diferente, que **HTTP Client** preparó para enviar a **MultiServer**. Este es el comienzo de la comunicación de correo electrónico. Haga clic en este segundo sobre de PDU y 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?
1025, 25, 1, 1. PSH+ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.



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.

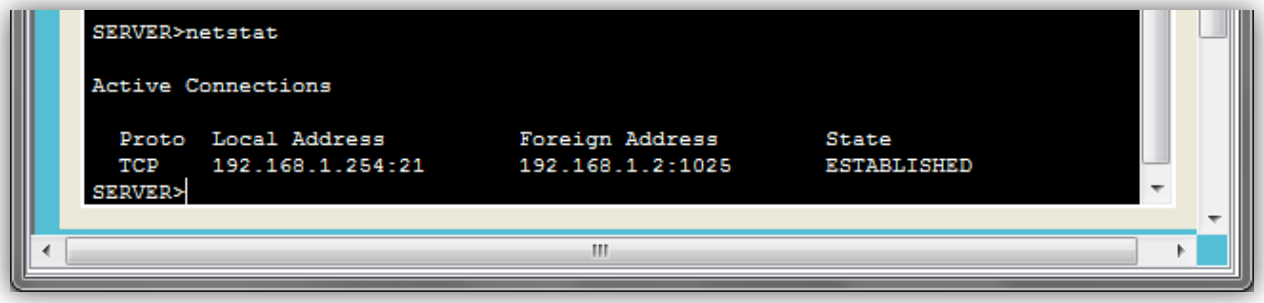
Paso 6: Examinar el uso de números de puerto del servidor

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



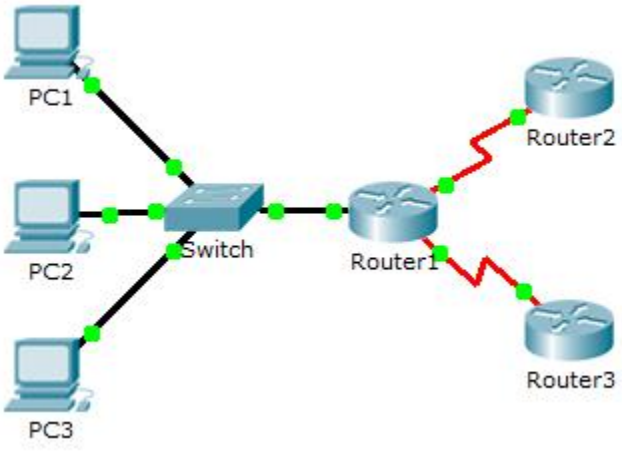
¿Qué números de puerto utiliza el servidor? Las respuestas varían, pero los estudiantes pueden ver los tres: 21, 25 y 80. Definitivamente deben ver el puerto 21.

c. ¿En qué estados están las sesiones?
ESTABLISHED (Establecida)

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

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

Laboratorio 8.1.3.8



Packet Tracer: investigación del tráfico unidifusión, difusión y multidifusión

Objetivos

Parte 1: Generar tráfico de unicast

Parte 2: Generar tráfico de broadcast

Parte 3: Investigar el tráfico de multicast

Información básica/situación

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

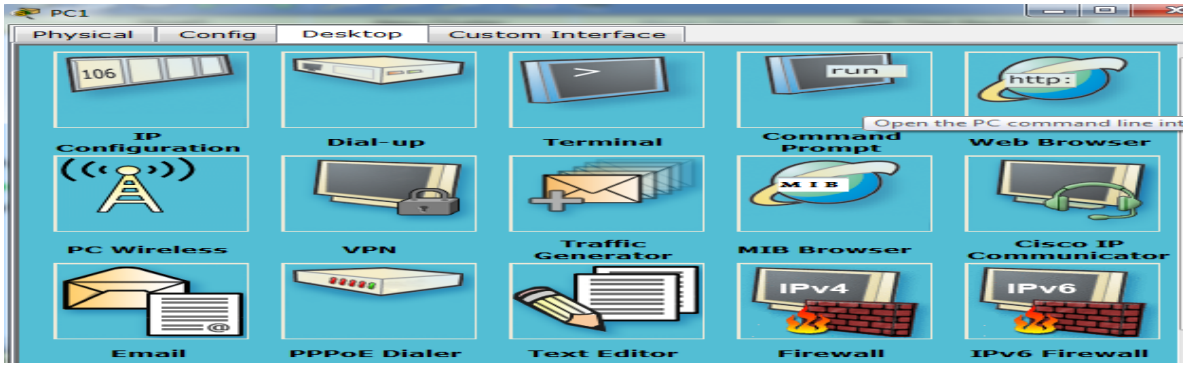
Mediante el comando **ping** o la característica Add Complex PDU (Agregar PDU compleja) de Packet Tracer, puede hacer ping directamente a las direcciones de broadcast para ver el tráfico de broadcast.

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

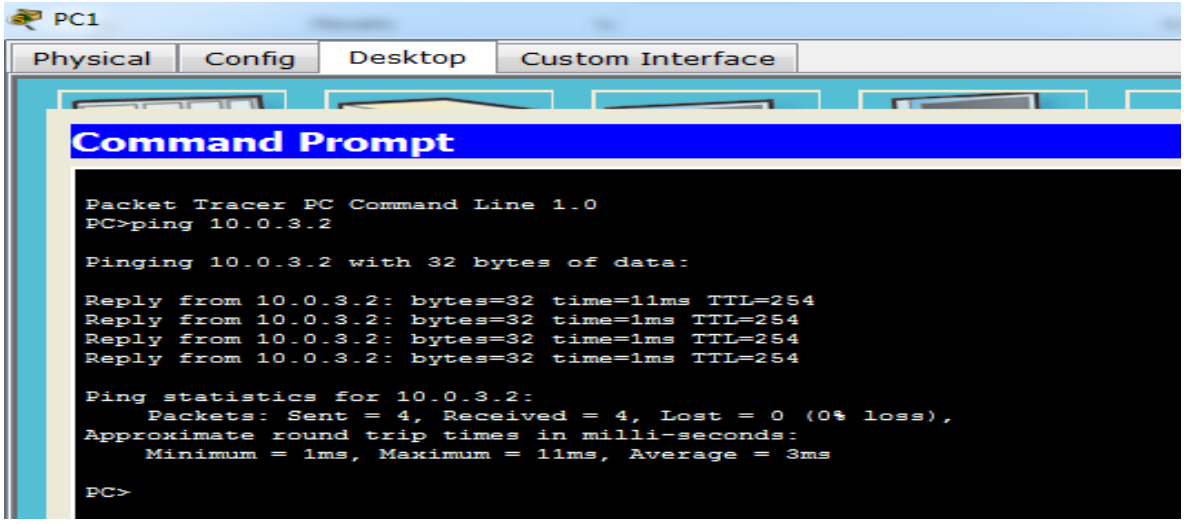
Parte 1: Generar tráfico de unicast

Paso 1: Utilizar el comando ping para generar tráfico.

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

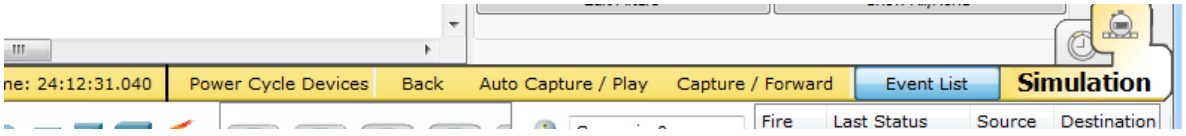


b. Introduzca el comando **ping 10.0.3.2**. El ping debe tener éxito.



Paso 2: Ingresar al modo de simulación.

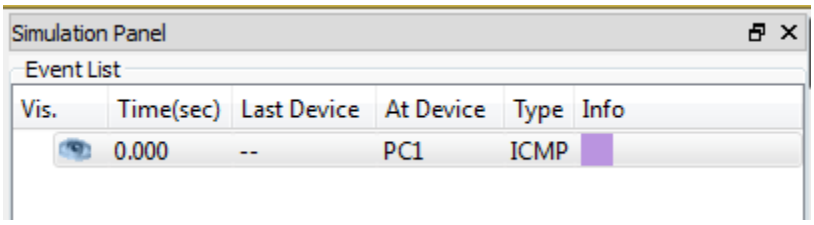
a. Haga clic en la ficha **Simulation** (Simulación) para ingresar al modo de simulación.



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** .

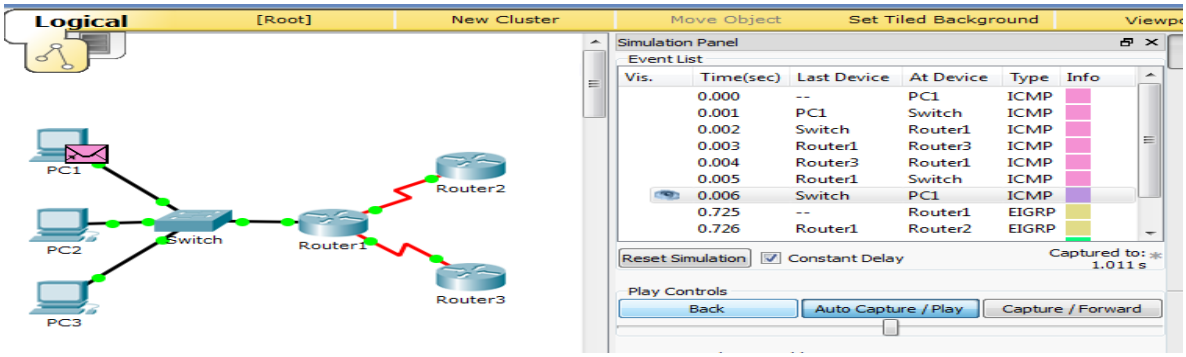
```
PC>ping 10.0.3.2

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.

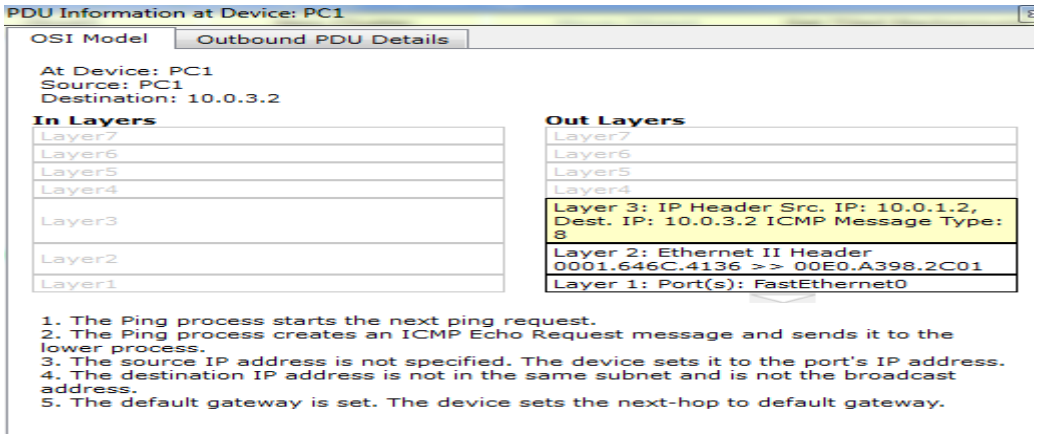


¿Qué dispositivos atravesó el paquete con la transmisión de unicast?

R/: De la PC1 al Switch1, después al Router1 y, finalmente, 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 abrirá la ventana Información de la PDU.

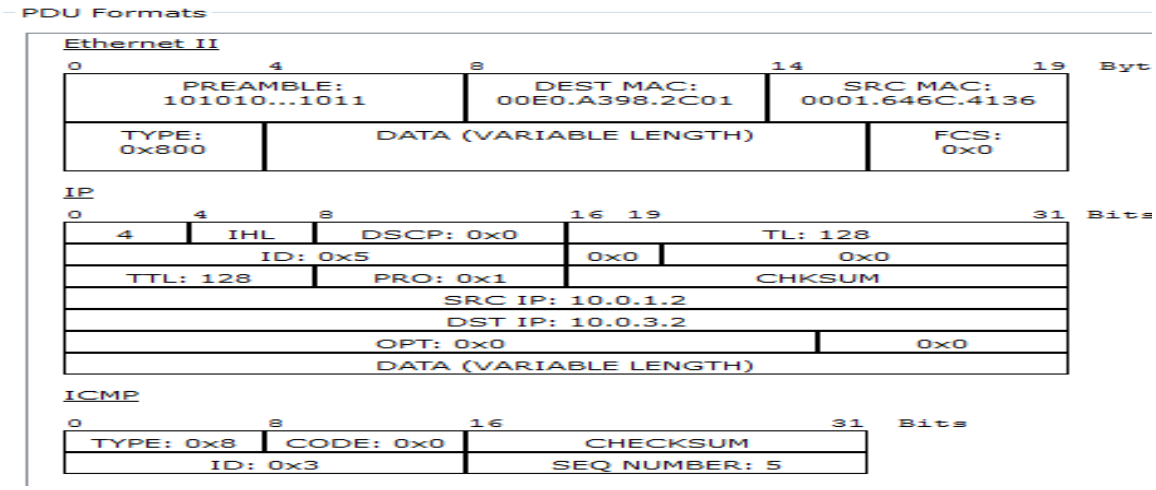


¿En qué capa comienza esta transmisión y por qué?

R/: En la capa 3, porque está específicamente relacionada con IP e ICMP.

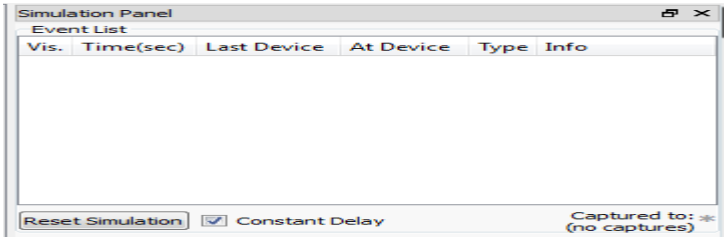
c. Examine la información de la Capa 3 para todos los eventos. Observe que las direcciones IP de origen y de destino son direcciones unicast que hacen referencia a la PC1 y a la interfaz serial del Router3.

¿Cuáles son los dos cambios que ocurren en la capa 3 cuando un paquete llega al Router3?



R/: Las direcciones IP de origen y destino se intercambian, y el tipo de mensaje ICMP ahora es 0.

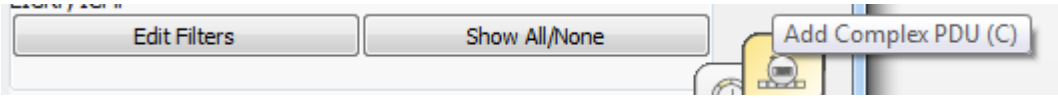
c. Haga clic en **Reset Simulation** (Restablecer simulación).



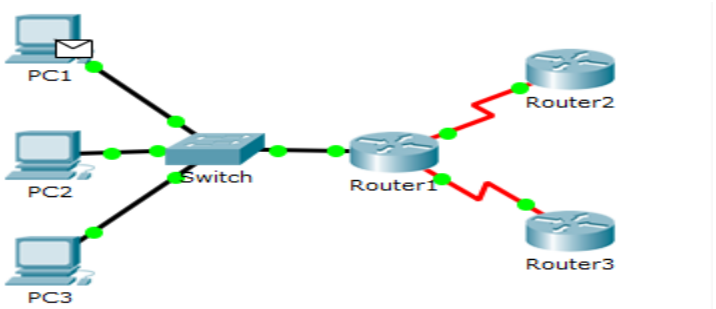
Parte 2: Generar tráfico de broadcast

Paso 1: Agregar una PDU compleja.

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



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



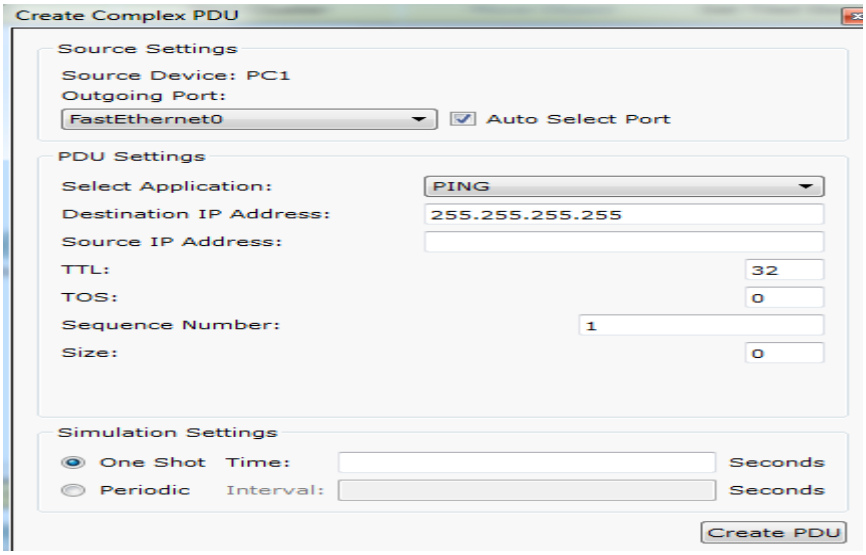
c. Haga clic en **PC1** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de diálogo **Create Complex PDU** (Crear una PDU compleja). Introduzca los siguientes valores:

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

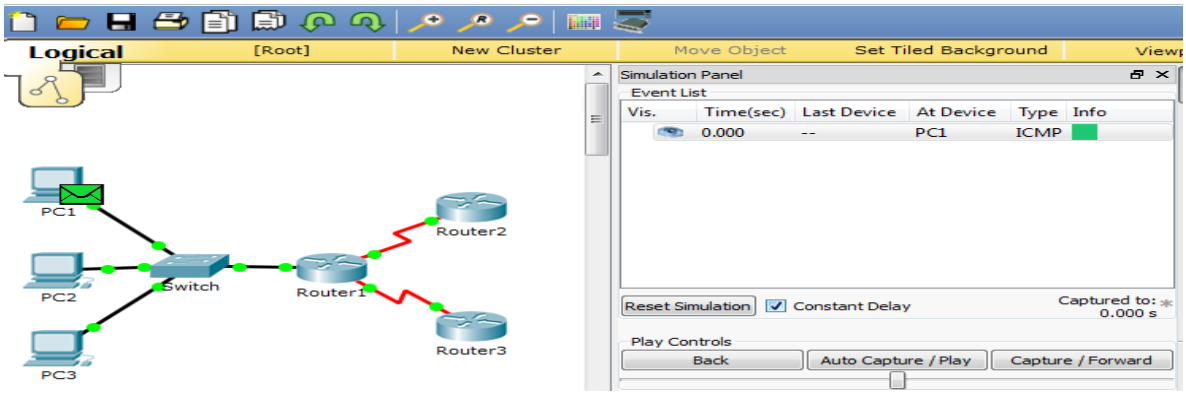
Dentro de la configuración de la PDU, el valor predeterminado para **Select Application** (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

R/: DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH,

TELNET, TFTP y OTHER.

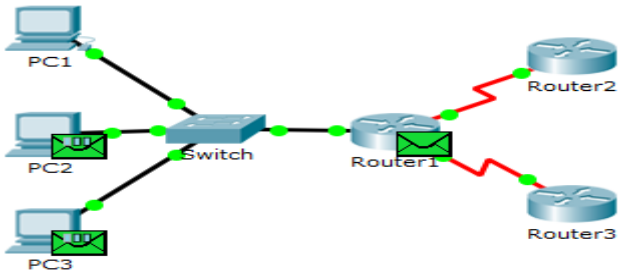


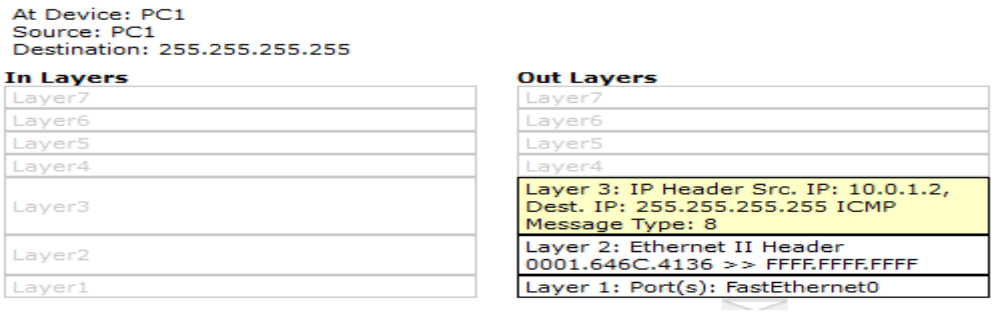
c. Haga clic en **Create PDU** (Crear PDU). Este paquete de difusión de prueba ahora aparece en **lista de eventos del panel de simulación.** También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para la Situación 0.



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

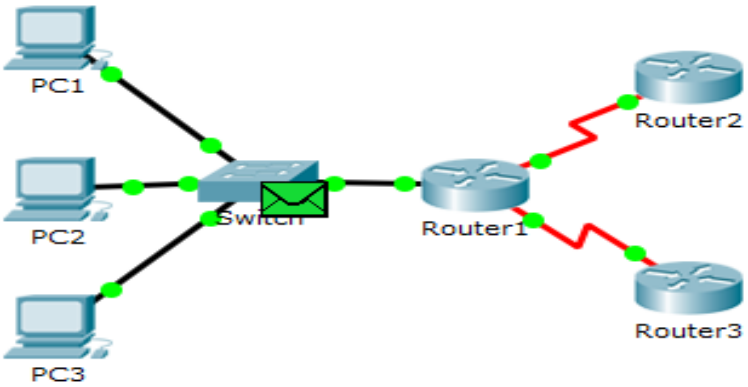
Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?





R/: La PDU se convierte en un unicast que contesta a la PC1.

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



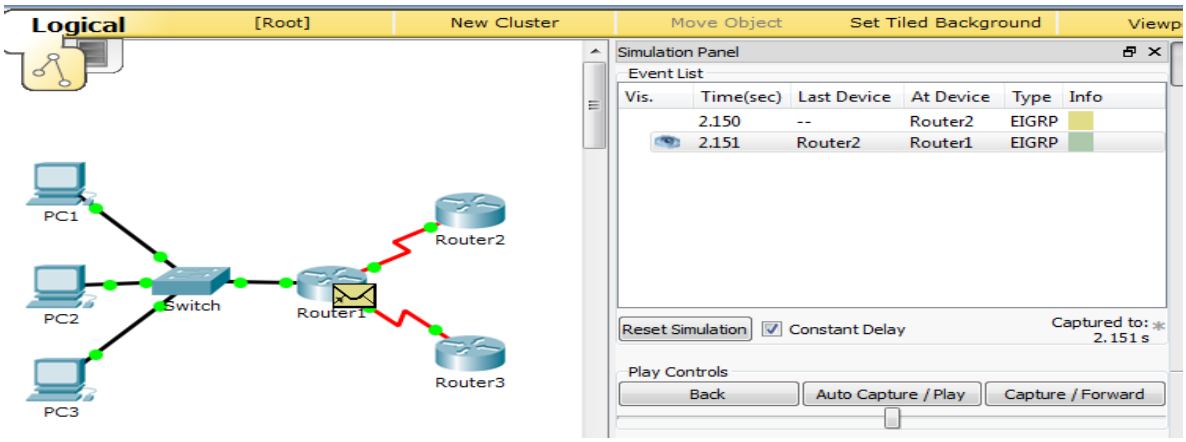
R/: No. El broadcast limitado debe permanecer dentro de la red local, a menos que el router esté establecido para reenviar.

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).

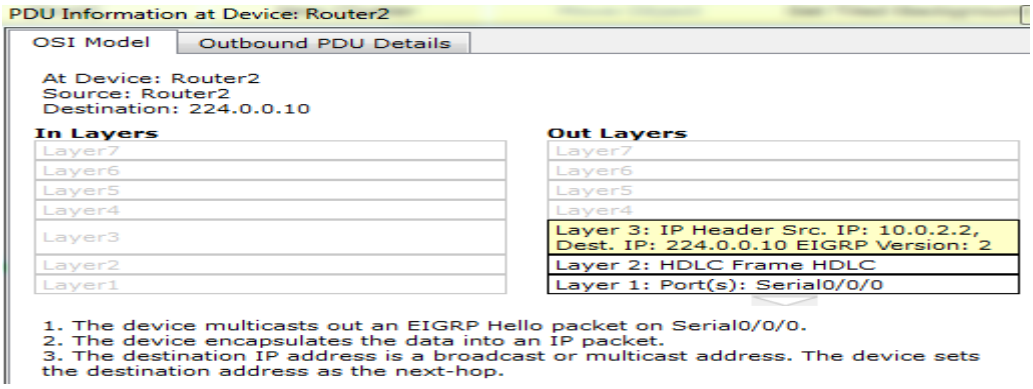
Parte 3: Investigar el tráfico de multicast

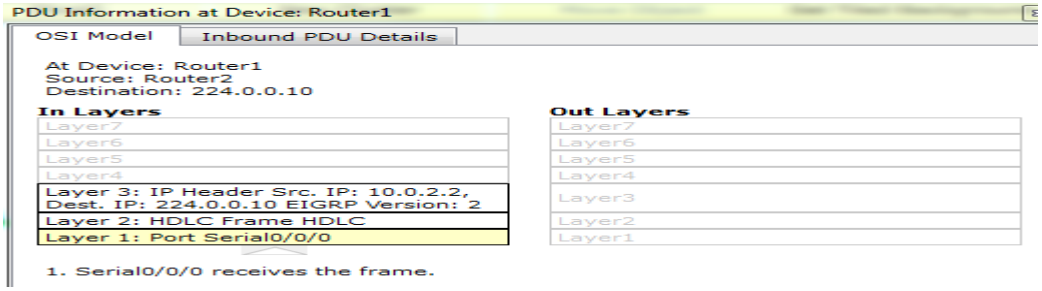
Paso 1: Examinar el tráfico que generan los protocolos de enrutamiento

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.

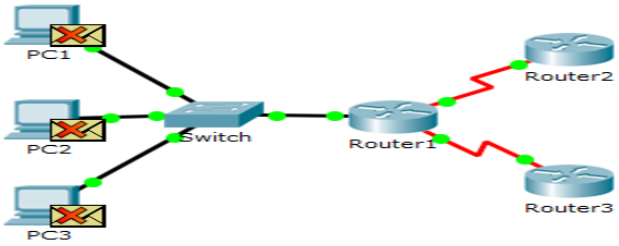


b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en **Capture/Forward**. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes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





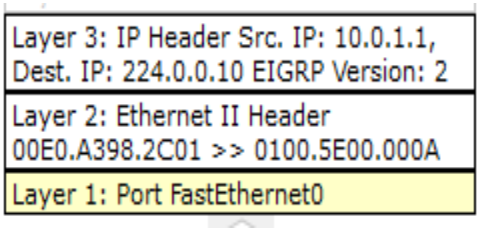
c. Haga clic en **Capture/Forward** hasta que vea que el paquete EIGRP llega a las PC.



¿Qué hacen los hosts con los paquetes?

R/: Los hosts 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?

R/: 224.0.0.10, la dirección IP de multicast para el protocolo de enrutamiento EIGRP.

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

R/: Los paquetes se descartan y no se realiza ningún procesamiento adicional.

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

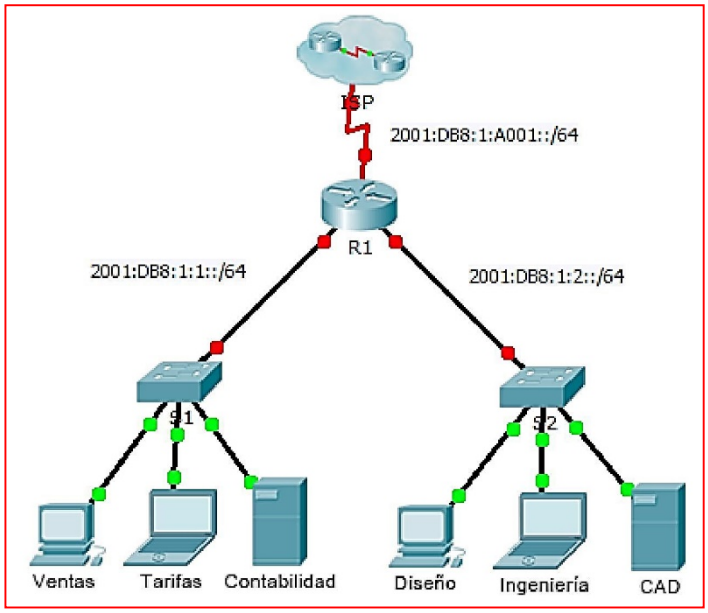
R/: El paquete unicast atraviesa la red destinado a un dispositivo específico, el broadcast se envía a cada dispositivo en la red de área local y el multicast se envía a todos los dispositivos, pero solo lo procesan aquellos que forman parte del grupo multicast.

Laboratorio 8.2.5.3

Packet Tracer: Configuración de direccionamiento IPv6 (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



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

Tabla de direccionamiento

Objetivos

- ✓ Parte 1: Configurar el direccionamiento IPv6 en el router
- ✓ Parte 2: Configurar el direccionamiento IPv6 en los servidores
- ✓ Parte 3: Configurar el direccionamiento IPv6 en los clientes
- ✓ Parte 4: Probar y verificar la conectividad de red

Información básica

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

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

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

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

```
R1>enable
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#
```

Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

a. Haga clic en **R1** y, a continuación, haga clic en la ficha **CLI**. Presione **Entrar**.

b. Ingrese al modo EXEC privilegiado.

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

```
R1(config)#
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)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
```

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

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

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#
```

f. Active la interfaz.

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

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.

```
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#
```

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

```
R1(config-if)#
R1(config-if)#ipv6 address 2001:DB8:1:2::1/64
```

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

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

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.

```
R1(config)#
R1(config)#interface s0/0/0
```

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

```
R1(config)#interface serial0/0/0
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
```

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

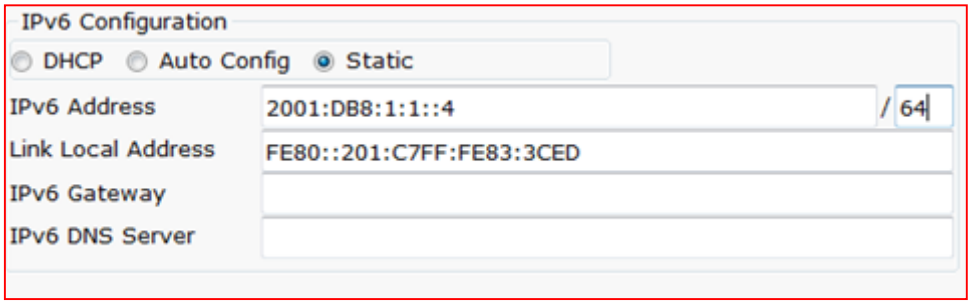
```
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
```

Parte 2: Configurar el direccionamiento IPv6 en los servidores

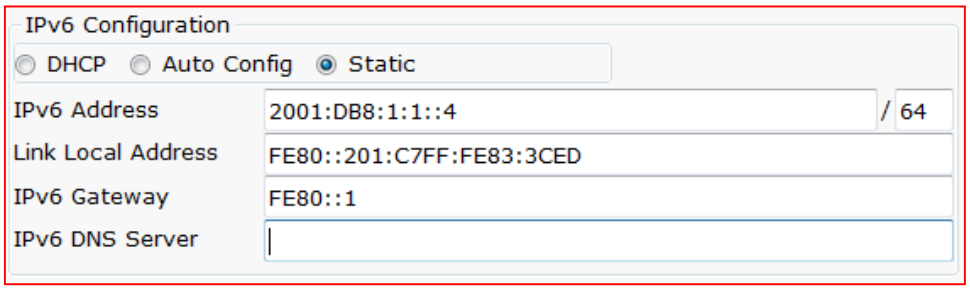
Paso 1: Configurar el direccionamiento IPv6 en el servidor de contabilidad

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**.

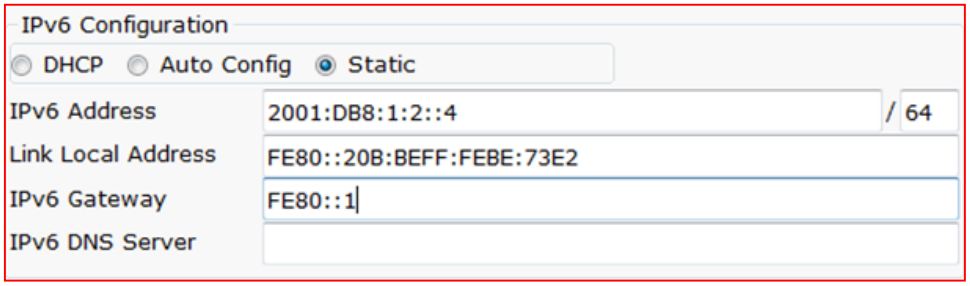


c. Configure el **gateway IPv6** en la dirección link-local, **FE80::1**.



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.



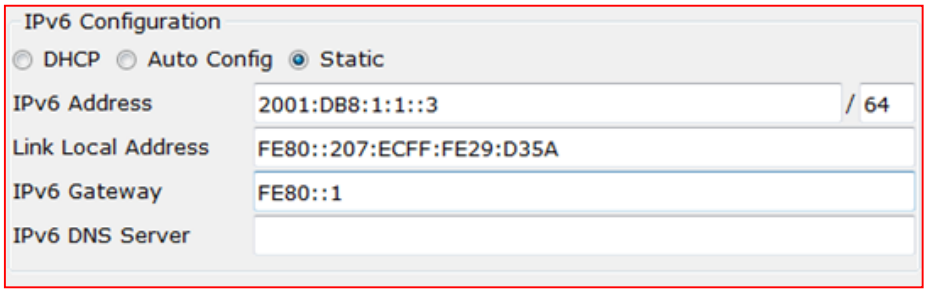
Parte 3: Configurar el direccionamiento IPv6 en los clientes

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

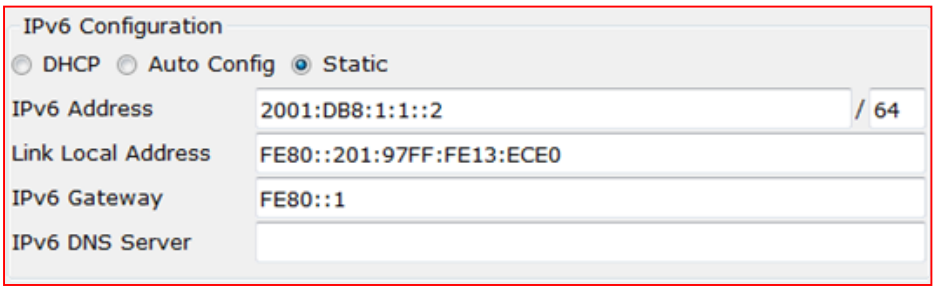
a. Haga clic en **Billing** (Facturación) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

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.

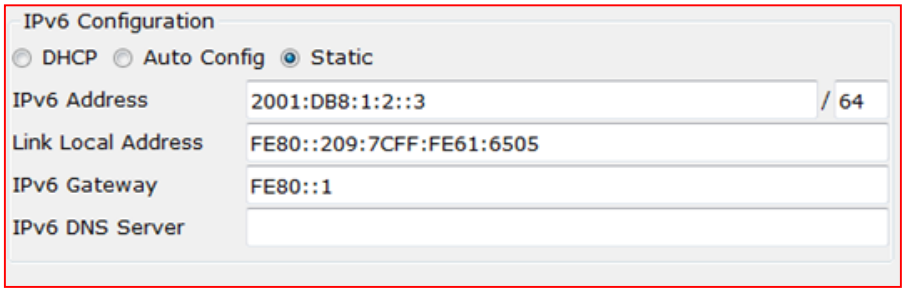


Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

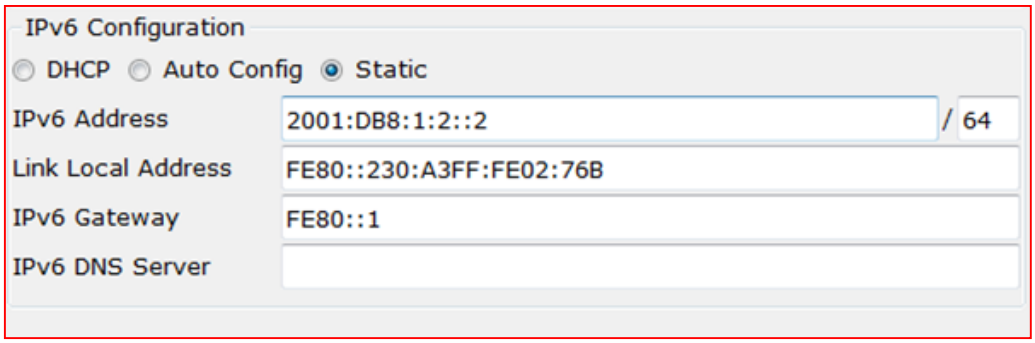
a. Haga clic en **Engineering** (Ingeniería) y, a continuación, seleccione la ficha **Desktop** seguida de **IP Configuration**.

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.

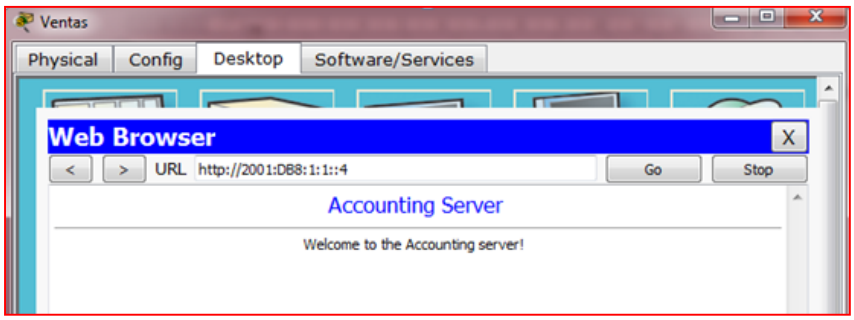


Parte 4: Probar y verificar la conectividad de la red

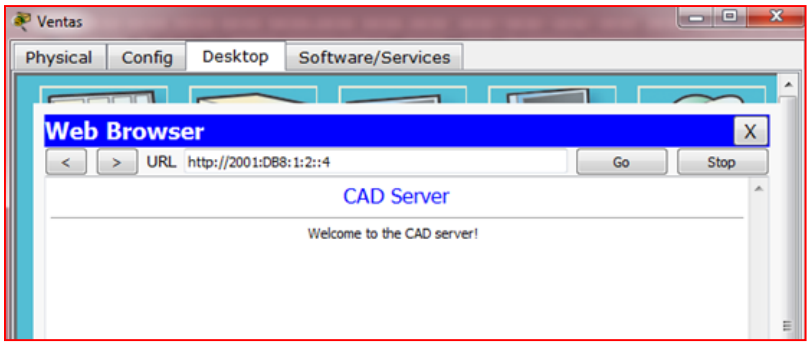
Paso 1: Abrir las páginas Web del servidor de los clientes

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

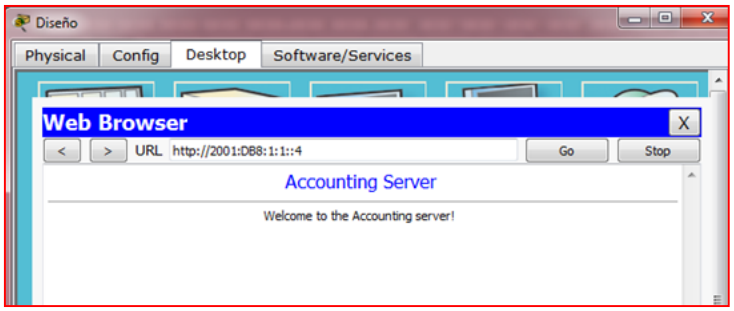
b. Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.

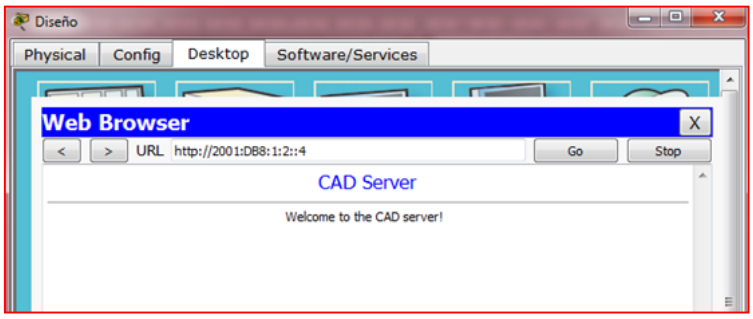


e. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.



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:

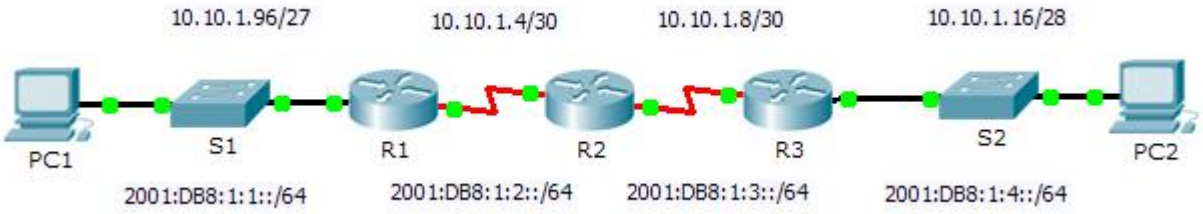
```
PC> ping 2001:DB8:1:A001::1
```

```
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>
```

```
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=2ms 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 = 2ms, Average = 1ms

PC>
```

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

Laboratorio 8.3.2.5



Packet Tracer: Verificación del direccionamiento IPv4 e IPv6

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
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

os

Objetivos

Parte 1: Completar la documentación de la tabla de direccionamiento

Parte 2: Probar la conectividad mediante el comando ping

Parte 3: Descubrir la ruta mediante su rastreo

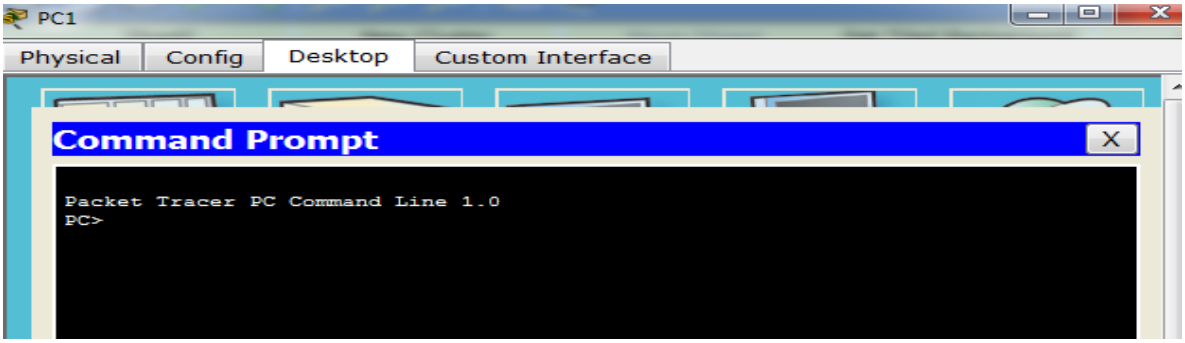
Información básica

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

Parte 1: Completar la documentación de la tabla de direccionamiento

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

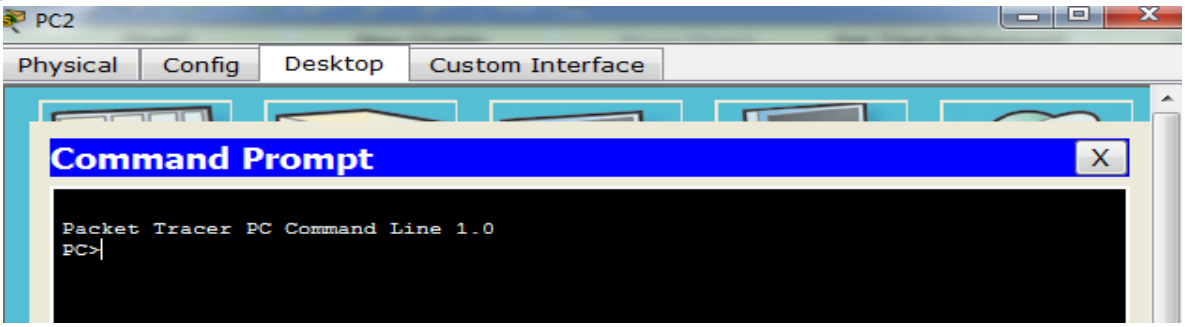
a. Haga clic en **PC1** y, a continuación, haga clic en la ficha **Desktop** > **Command Prompt** (Escritorio > Símbolo del sistema).



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.

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0060.47CA.4DEE
   Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
   IP Address.....................: 10.10.1.100
   Subnet Mask.....................: 255.255.255.224
   Default Gateway.....................: 10.10.1.97
   DNS Servers.....................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-7C-91-2A-62-00-60-47-CA-4D-EE


PC>
```

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.....................: 00-01-00-01-12-D6-A8-D7-00-60-70-34-69-30


PC>
```

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.

```
PC>ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.....................: 0060.47CA.4DEE
   Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
   IPv6 Address.....................: 2001:DB8:1:1::A/64
   Default Gateway.....................: FE80::1
   DNS Servers.....................: ::
   DHCPv6 Client DUID.....................: 00-01-00-01-7C-91-2A-62-00-60-47-CA-4D-EE

PC>
```

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

```
PC>ipv6config /all

FastEthernet0 Connection:(default port)

   Physical Address.....................: 0060.7034.6930
   Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
   IPv6 Address.....................: 2001:DB8:1:4::A/64
   Default Gateway.....................: FE80::3
   DNS Servers.....................: ::
   DHCPv6 Client DUID.....................: 00-01-00-01-12-D6-A8-D7-00-60-70-34-69-30

PC>
```

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**. ¿El resultado fue satisfactorio?

```
PC>ping 10.10.1.20

Pinging 10.10.1.20 with 32 bytes of data:

Reply from 10.10.1.20: bytes=32 time=12ms TTL=125
Reply from 10.10.1.20: bytes=32 time=13ms TTL=125
Reply from 10.10.1.20: bytes=32 time=13ms TTL=125
Reply from 10.10.1.20: bytes=32 time=13ms TTL=125

Ping statistics for 10.10.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms

PC>
```

R/: Sí

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

```
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=13ms TTL=125
Reply from 10.10.1.100: bytes=32 time=11ms TTL=125
Reply from 10.10.1.100: bytes=32 time=12ms TTL=125
Reply from 10.10.1.100: bytes=32 time=11ms 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 = 11ms, Maximum = 13ms, Average = 11ms

PC>
```

R/: Sí

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

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

Satisfactorio?

```
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=23ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=12ms 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 = 11ms, Maximum = 23ms, Average = 14ms

PC>
```

R/: Sí

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

```
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=12ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:1::A: bytes=32 time=10ms 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 = 10ms, Maximum = 12ms, Average = 11ms

PC>
```

R/: Sí

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      1 ms      1 ms      10.10.1.5
  3    8 ms      1 ms      2 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?

R/: 10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20

¿Con qué interfaces se asocian las cuatro direcciones?

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

c. 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    0 ms      0 ms      0 ms      10.10.1.17
  2    1 ms      1 ms      0 ms      10.10.1.9
  3    0 ms      2 ms      1 ms      10.10.1.6
  4    11 ms     12 ms     1 ms      10.10.1.100

Trace complete.

PC>
```

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

R/: 10.10.1.17, 10.10.1.9, 10.10.1.6, 10.10.1.100

¿Con qué interfaces se asocian las cuatro direcciones?

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

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

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

Trace complete.

PC>
```

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

R/: 2001:DB8:1:1::1, 2001:DB8:1:2::1,2001:DB8:1:3::2, 2001:DB8:1:4::A

¿Con qué interfaces se asocian las cuatro direcciones?

R/: G0/0 del R1, S0/0/0 del R2, S0/0/1 del R3, NIC de la PC2

c. 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    0 ms      1 ms      0 ms      2001:DB8:1:3::1
  3    2 ms      1 ms      1 ms      2001:DB8:1:2::2
  4    12 ms     17 ms     11 ms     2001:DB8:1:1::A

Trace complete.

PC>
```

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

R/: 2001:DB8:1:4::1, 2001:DB8:1:3::1, 2001:DB8:1:2::2, 2001:DB8:1:1::A

¿Con qué interfaces se asocian las cuatro direcciones?

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

Laboratorio 8.3.2.6

Packet Tracer: Ping y rastreo para probar rutas (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

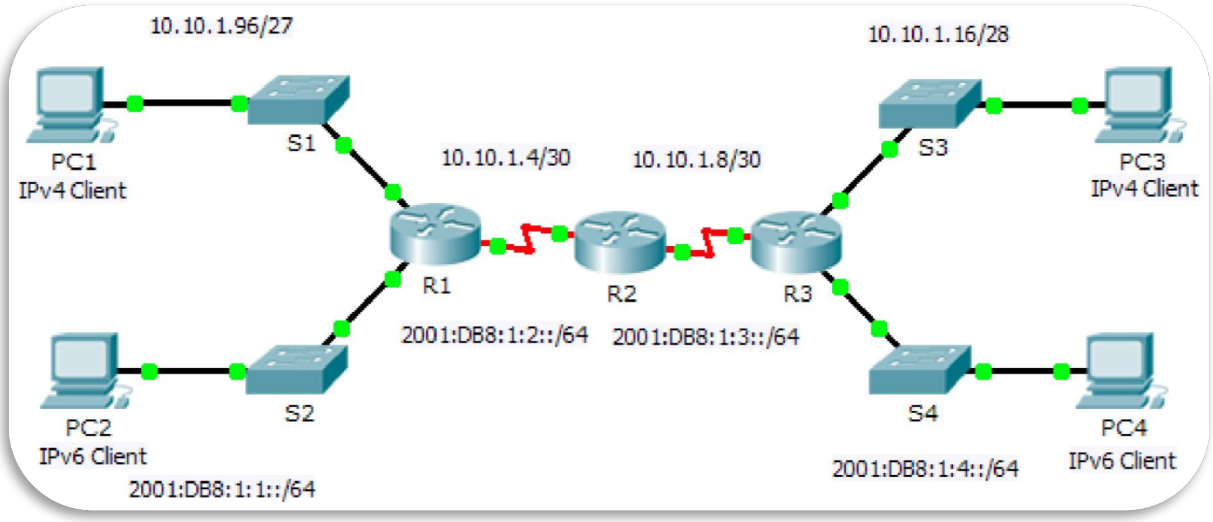


Tabla de direccionamiento

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

Objetivos

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

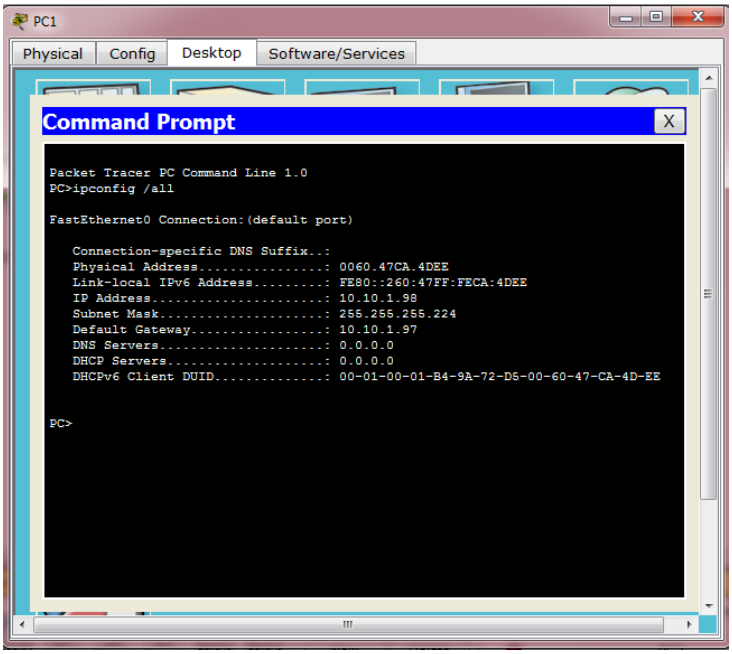
Situación

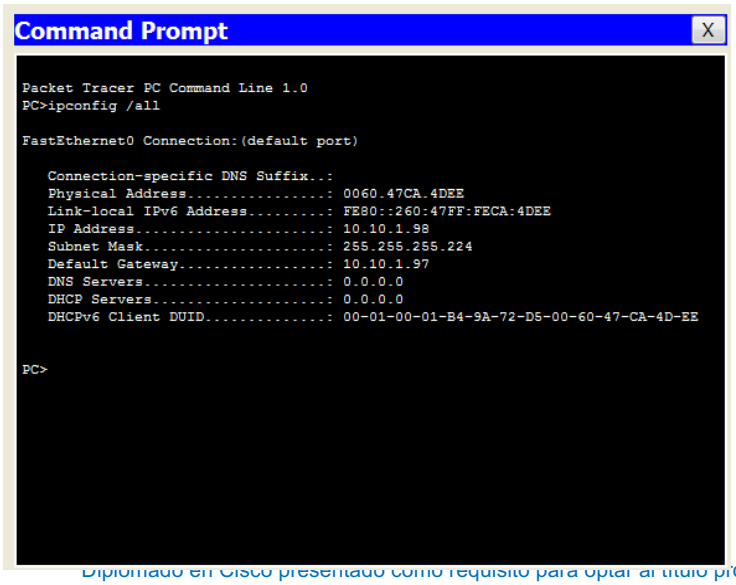
En esta actividad, hay problemas de conectividad. Además de recopilar y registrar información acerca de la red, localizará los problemas e implementará soluciones razonables para restaurar la conectividad. **Nota:** la contraseña de EXEC del usuario es **cisco**. La contraseña de EXEC privilegiado es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

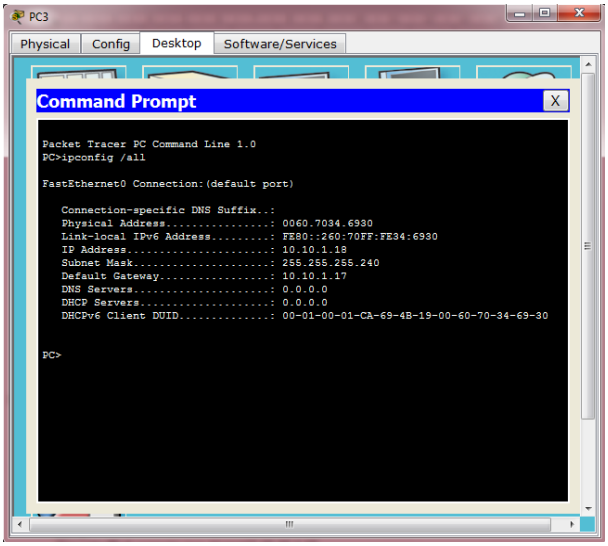


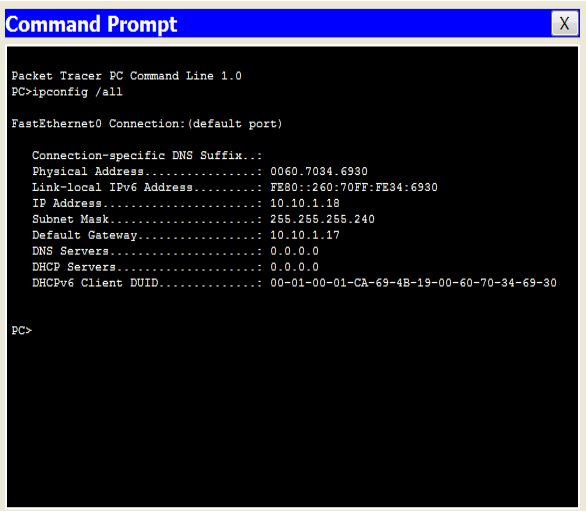


```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0060.47CA.4DEE
Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
IP Address.....: 10.10.1.98
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 10.10.1.97
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-B4-9A-72-D5-00-60-47-CA-4D-EE

PC>
```

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

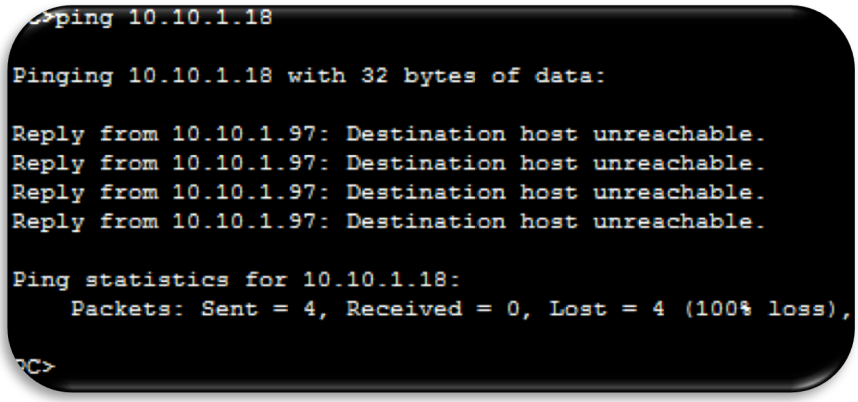
d. Introduzca el comando **ipconfig /all** para recopilar la información de IPv4. Complete la **tabla de direccionamiento** con la dirección IPv4, la máscara de subred y el gateway predeterminado.

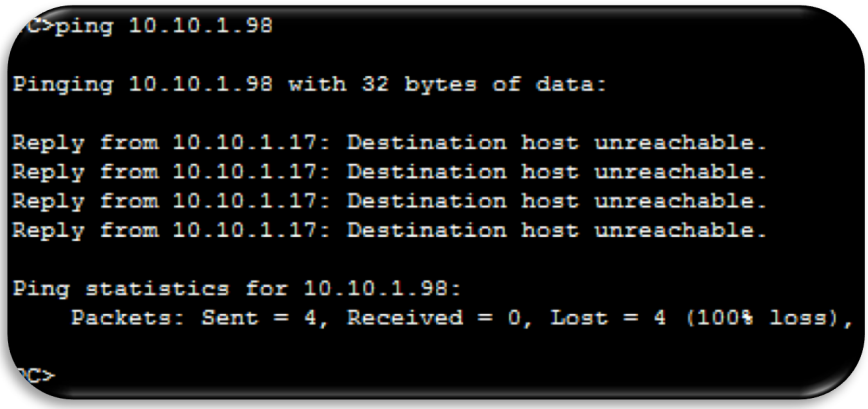




```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0060.7034.6930
Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
IP Address.....: 10.10.1.18
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-CA-69-4B-19-00-60-70-34-69-30

PC>
```

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






```
PC>ping 10.10.1.18
```

Pinging 10.10.1.18 with 32 bytes of data:

Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.

Ping statistics for 10.10.1.18:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

PC>ping 10.10.1.98

Pinging 10.10.1.98 with 32 bytes of data:

Reply from 10.10.1.17: Destination host unreachable.
Reply from 10.10.1.17: Destination host unreachable.
Reply from 10.10.1.17: Destination host unreachable.
Reply from 10.10.1.17: Destination host unreachable.

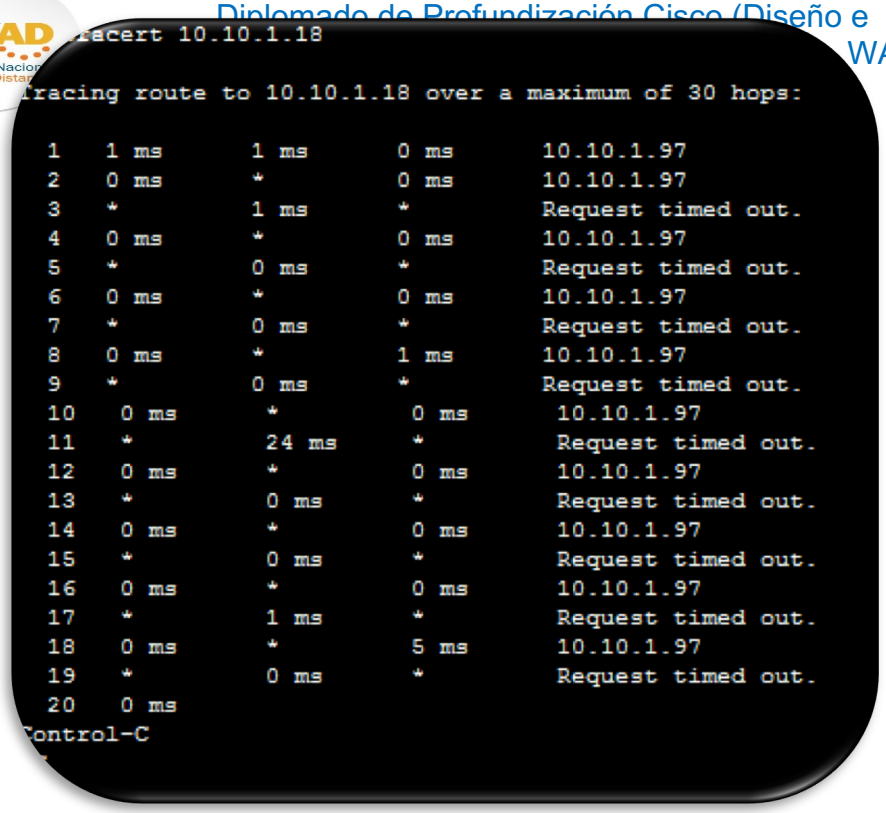
Ping statistics for 10.10.1.98:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

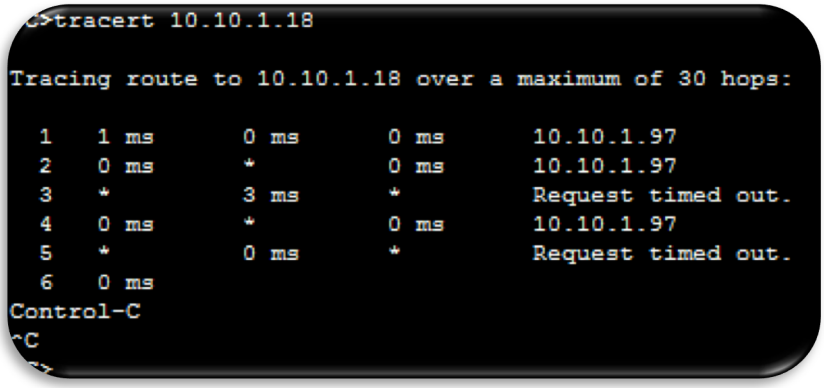
PC>

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

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

```
C>tracert 10.10.1.18

Tracing route to 10.10.1.18 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.1.97
  2    0 ms      *         0 ms      10.10.1.97
  3    *         0 ms      *         Request timed out.
  4    0 ms      *         0 ms      10.10.1.97
  5    *         0 ms      *         Request timed out.
  6    1 ms      *         0 ms      10.10.1.97
  7    *         1 ms      *         Request timed out.
  8    0 ms
Control-C
^C
```





PC>tracert 10.10.1.18

Tracing route to 10.10.1.18 over a maximum of 30 hops:

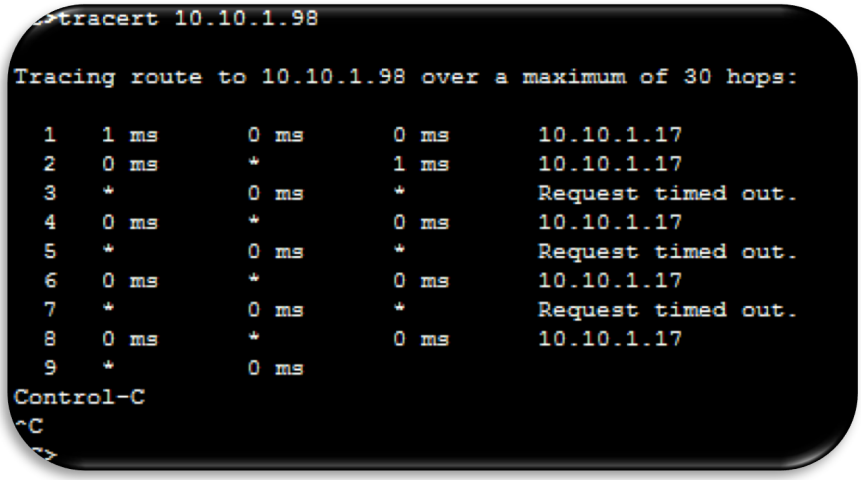
1 1 ms 1 ms 0 ms 10.10.1.97
2 0 ms * 0 ms 10.10.1.97
3 * 1 ms * Request timed out.
4 0 ms * 0 ms 10.10.1.97
5 * 0 ms * Request timed out.
6 0 ms * 0 ms 10.10.1.97
7 * 0 ms * Request timed out.
8 0 ms * 1 ms 10.10.1.97

```
 9 * 0 ms * Request timed out.
10 0 ms * 0 ms 10.10.1.97
11 * 24 ms * Request timed out.
12 0 ms * 0 ms 10.10.1.97
13 * 0 ms * Request timed out.
14 0 ms * 0 ms 10.10.1.97
15 * 0 ms * Request timed out.
16 0 ms * 0 ms 10.10.1.97
17 * 1 ms * Request timed out.
18 0 ms * 5 ms 10.10.1.97
19 * 0 ms * Request timed out.
20 0 ms
Control-C
^C
PC>
```

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? 10.10.1.17

```
acert 10.10.1.98

racing route to 10.10.1.98 over a maximum of 30 hops:

 1    4 ms     0 ms     0 ms     10.10.1.17
 2    0 ms     *        0 ms     10.10.1.17
 3    *        0 ms     *        Request timed out.
 4    1 ms     *        0 ms     10.10.1.17
 5    *        0 ms     *        Request timed out.
 6    0 ms     *        1 ms     10.10.1.17
 7    *        0 ms     *        Request timed out.
 8    0 ms     *        1 ms     10.10.1.17
 9    *        0 ms     *        Request timed out.
10    0 ms     *        0 ms     10.10.1.17
11    *        1 ms     *        Request timed out.
12    0 ms     *        0 ms     10.10.1.17
13    *        0 ms     *        Request timed out.
14    0 ms     *        0 ms     10.10.1.17
15    *        0 ms     *        Request timed out.
16    0 ms     *        0 ms     10.10.1.17
17    *        0 ms     *        Request timed out.
18    0 ms     *        0 ms     10.10.1.17
19    *        0 ms     *        Request timed out.
20    0 ms     *        0 ms     10.10.1.17
21    *        0 ms     *        Request timed out.
22    0 ms     *        0 ms     10.10.1.17
23    *        0 ms     *        Request timed out.
24    0 ms     *        0 ms     10.10.1.17
25    *        0 ms     *        Request timed out.
26    0 ms     *        1 ms     10.10.1.17
27    *        0 ms     *        Request timed out.
28    0 ms     *        0 ms     10.10.1.17
29    *        0 ms     *        Request timed out.
30    0 ms     *        0 ms     10.10.1.17

race complete.
```



PC>tracert 10.10.1.98

Tracing route to 10.10.1.98 over a maximum of 30 hops:

1 4 ms 0 ms 0 ms 10.10.1.17

2 0 ms * 0 ms 10.10.1.17

3 * 0 ms * Request timed out.

4 1 ms * 0 ms 10.10.1.17

5 * 0 ms * Request timed out.

6 0 ms * 1 ms 10.10.1.17

7 * 0 ms * Request timed out.

8 0 ms * 1 ms 10.10.1.17

9 * 0 ms * Request timed out.

10 0 ms * 0 ms 10.10.1.17

11 * 1 ms * Request timed out.

12 0 ms * 0 ms 10.10.1.17

13 * 0 ms * Request timed out.

14 0 ms * 0 ms 10.10.1.17

15 * 0 ms * Request timed out.

16 0 ms * 0 ms 10.10.1.17

17 * 0 ms * Request timed out.

18 0 ms * 0 ms 10.10.1.17

19 * 0 ms * Request timed out.

20 0 ms * 0 ms 10.10.1.17

21 * 0 ms * Request timed out.

22 0 ms * 0 ms 10.10.1.17

23 * 0 ms * Request timed out.

24 0 ms * 0 ms 10.10.1.17

25 * 0 ms * Request timed out.

26 0 ms * 1 ms 10.10.1.17

27 * 0 ms * Request timed out.

28 0 ms * 0 ms 10.10.1.17

29 * 0 ms * Request timed out.

30 0 ms * 0 ms 10.10.1.17

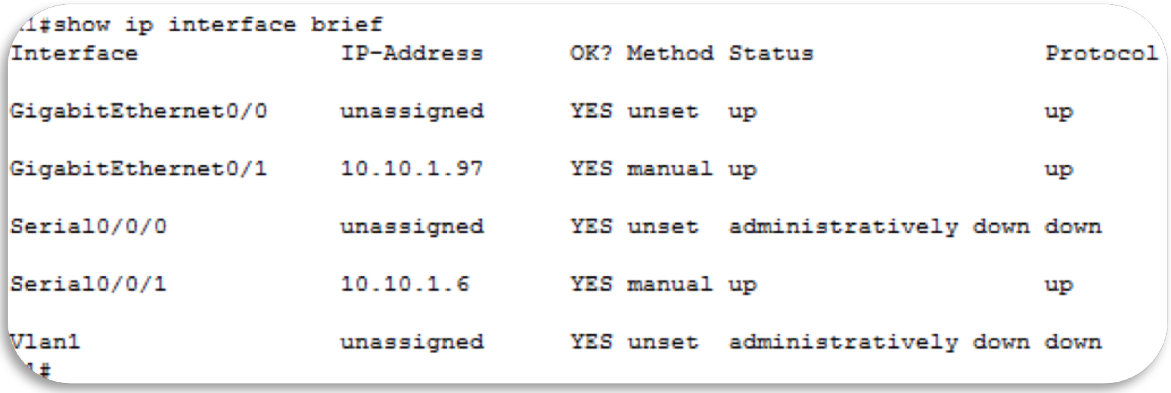
Trace complete.

PC>

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? 10.10.1.6



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

GigabitEthernet0/0     unassigned      YES unset  up                    up

GigabitEthernet0/1     10.10.1.97      YES manual up                    up

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            10.10.1.6       YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
1#
```

R1#show ip interface brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES unset up up

GigabitEthernet0/1 10.10.1.97 YES manual up up

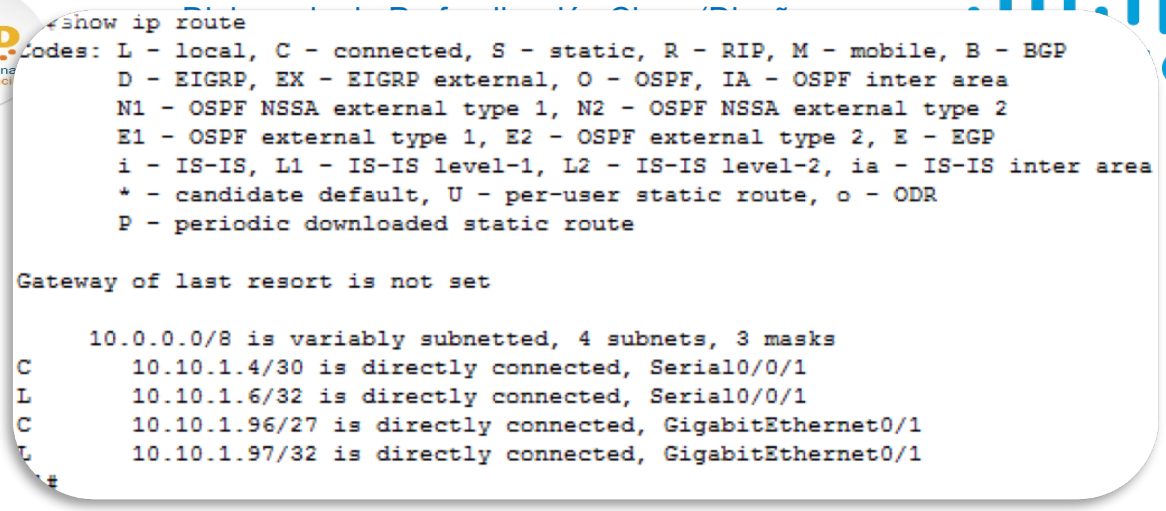
Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.10.1.6 YES manual up up

Vlan1 unassigned YES unset administratively down down

R1#

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



R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks

C 10.10.1.4/30 is directly connected, Serial0/0/1

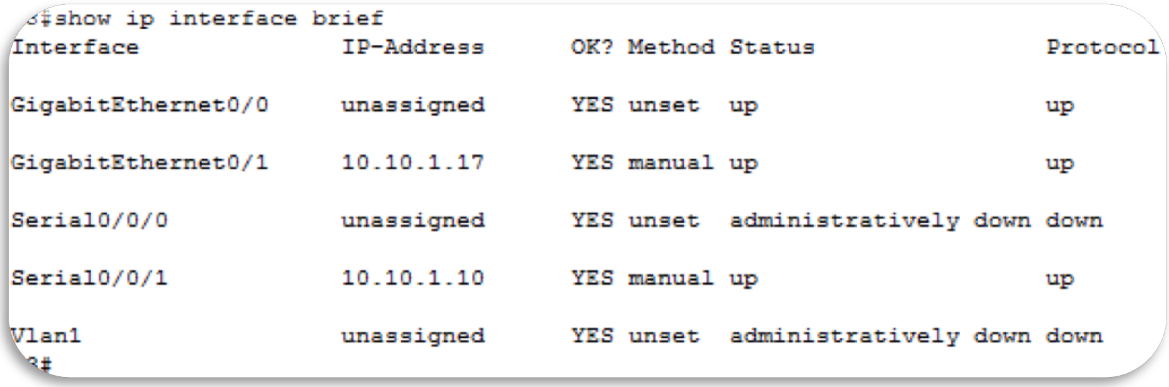
L 10.10.1.6/32 is directly connected, Serial0/0/1

C 10.10.1.96/27 is directly connected, GigabitEthernet0/1

L 10.10.1.97/32 is directly connected, GigabitEthernet0/1

R1#

h. Repita los pasos 2e a 2g con el **R3** y escriba las respuestas aquí. 10.10.1.10, 10.10.1.8/30, 10.10.1.10/32 Observe cómo cambia la interfaz serial para el R3.



```
3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     10.10.1.17      YES manual up                    up
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            10.10.1.10      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
3#
```

R3#show ip interface brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES unset up up

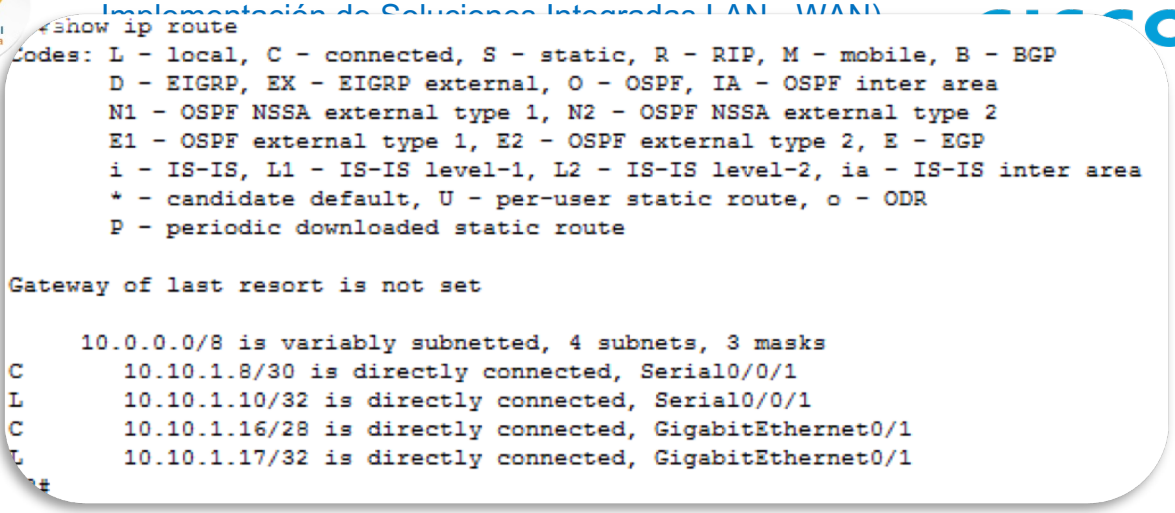
GigabitEthernet0/1 10.10.1.17 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.10.1.10 YES manual up up

Vlan1 unassigned YES unset administratively down down

R3#



```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.1.8/30 is directly connected, Serial0/0/1
L       10.10.1.10/32 is directly connected, Serial0/0/1
C       10.10.1.16/28 is directly connected, GigabitEthernet0/1
L       10.10.1.17/32 is directly connected, GigabitEthernet0/1
R3#
```

R3#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks

C 10.10.1.8/30 is directly connected, Serial0/0/1

L 10.10.1.10/32 is directly connected, Serial0/0/1

C 10.10.1.16/28 is directly connected, GigabitEthernet0/1

L 10.10.1.17/32 is directly connected, GigabitEthernet0/1

R3#

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

```
2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.10.1.2       YES manual up                    up
Serial0/0/1            10.10.1.9       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
2#
```

R2#show ip interface brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset administratively down down

Serial0/0/0 10.10.1.2 YES manual up up

Serial0/0/1 10.10.1.9 YES manual up up

Vlan1 unassigned YES unset administratively down down

R2#

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.10.1.0/30 is directly connected, Serial0/0/0
L       10.10.1.2/32 is directly connected, Serial0/0/0
C       10.10.1.8/30 is directly connected, Serial0/0/1
L       10.10.1.9/32 is directly connected, Serial0/0/1
O       10.10.1.16/28 [90/2170112] via 10.10.1.10, 01:12:37, Serial0/0/1
#
```

R2#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks

C 10.10.1.0/30 is directly connected, Serial0/0/0

L 10.10.1.2/32 is directly connected, Serial0/0/0

C 10.10.1.8/30 is directly connected, Serial0/0/1

L 10.10.1.9/32 is directly connected, Serial0/0/1

D 10.10.1.16/28 [90/2170112] via 10.10.1.10, 01:12:37, Serial0/0/1

R2#

Paso 3: Proponga una solución para resolver el problema.

a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error? La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.
b. ¿Qué solución propondría para corregir el problema? Configurar la dirección IP correcta en la interfaz Serial 0/0/0 del R2 (10.10.1.5).

```
R2(config)#
R2(config)#interface s0/0/0
R2(config-if)#ip addres 10.10.1.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#
```

R2(config)#
R2(config)#interface s0/0/0
R2(config-if)#ip addres 10.10.1.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#

Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada.

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

```
C>ping 10.10.1.18

Pinging 10.10.1.18 with 32 bytes of data:

Reply from 10.10.1.18: bytes=32 time=3ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

PC>ping 10.10.1.18

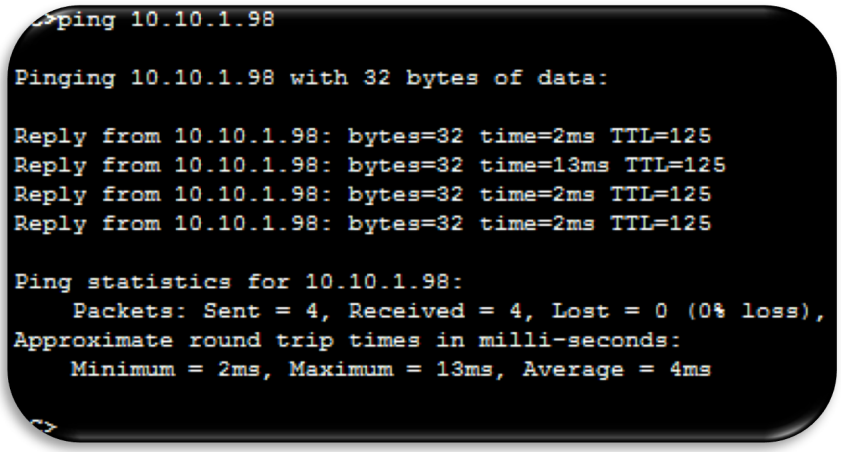
Pinging 10.10.1.18 with 32 bytes of data:

Reply from 10.10.1.18: bytes=32 time=3ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.18:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>

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



PC>ping 10.10.1.98

Pinging 10.10.1.98 with 32 bytes of data:

Reply from 10.10.1.98: bytes=32 time=2ms TTL=125
Reply from 10.10.1.98: bytes=32 time=13ms TTL=125
Reply from 10.10.1.98: bytes=32 time=2ms TTL=125
Reply from 10.10.1.98: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.98:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 4ms

PC>

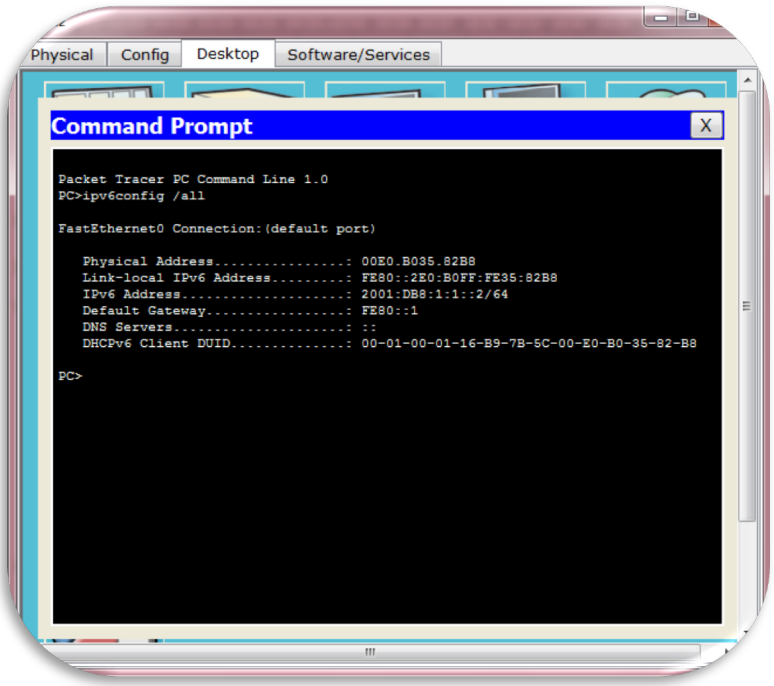
Paso 6: Documentar la solución.

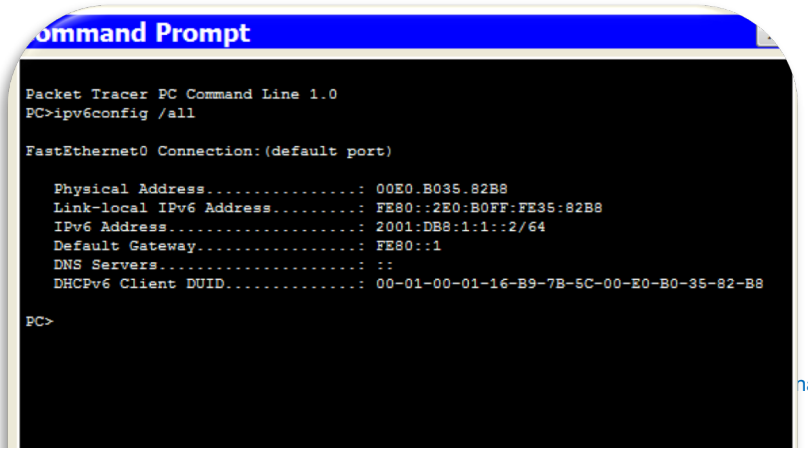
Parte 2: Probar y restaurar la conectividad IPv6

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.





PC>ipv6config /all

FastEthernet0 Connection:(default port)

Physical Address.....: 00E0.B035.82B8

Link-local IPv6 Address.....: FE80::2E0:B0FF:FE35:82B8

IPv6 Address.....: 2001:DB8:1:1::2/64

Default Gateway.....: FE80::1

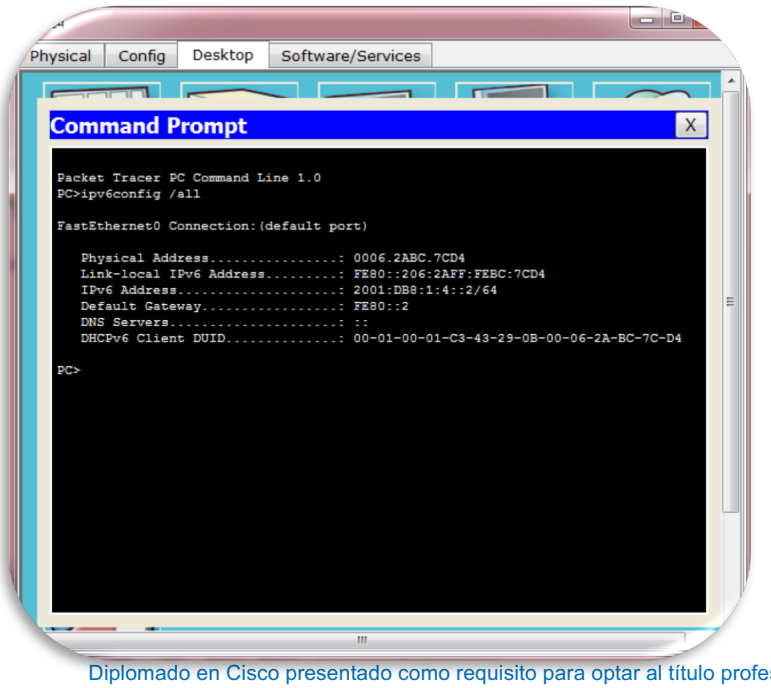
DNS Servers.....: ::

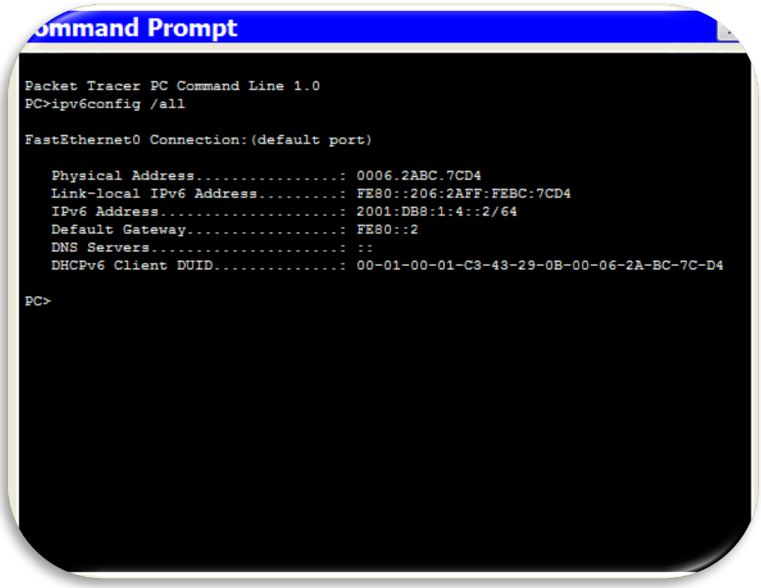
DHCPv6 Client DUID.....: 00-01-00-01-16-B9-7B-5C-00-E0-B0-35-82-B8

PC>

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.





PC>ipv6config /all

FastEthernet0 Connection:(default port)

Physical Address.....: 0006.2ABC.7CD4

Link-local IPv6 Address.....: FE80::206:2AFF:FEBC:7CD4

IPv6 Address.....: 2001:DB8:1:4::2/64

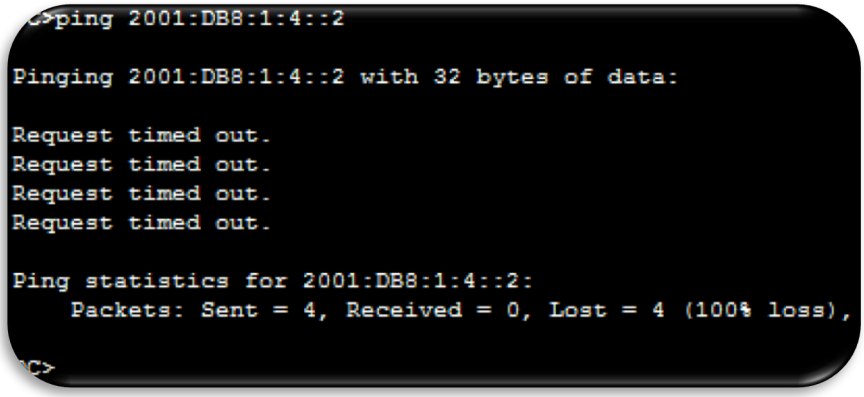
Default Gateway.....: FE80::2

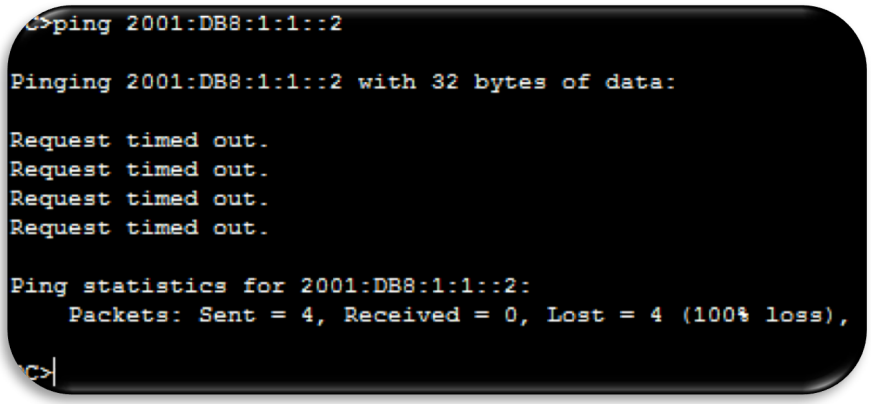
DNS Servers.....: ::

DHCPv6 Client DUID.....: 00-01-00-01-C3-43-29-0B-00-06-2A-BC-7C-D4

PC>

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





PC>ping 2001:DB8:1:4::2

Pinging 2001:DB8:1:4::2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 2001:DB8:1:4::2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

PC>ping 2001:DB8:1:1::2

Pinging 2001:DB8:1:1::2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

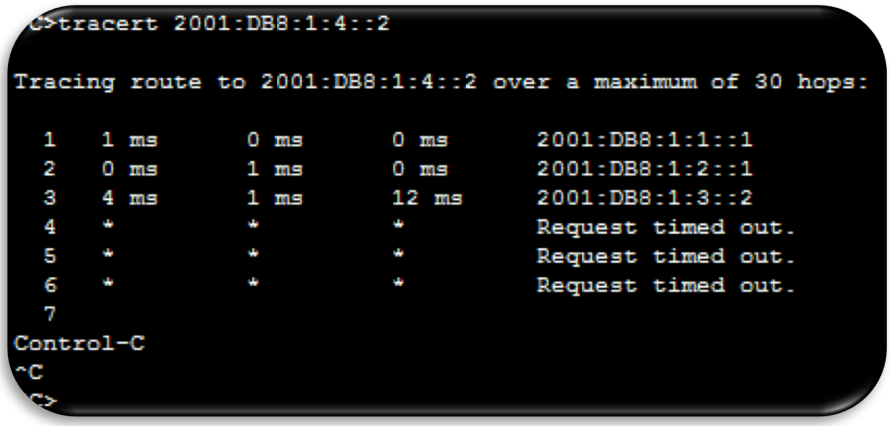
Ping statistics for 2001:DB8:1:1::2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

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? 2001:DB8:1:3::2



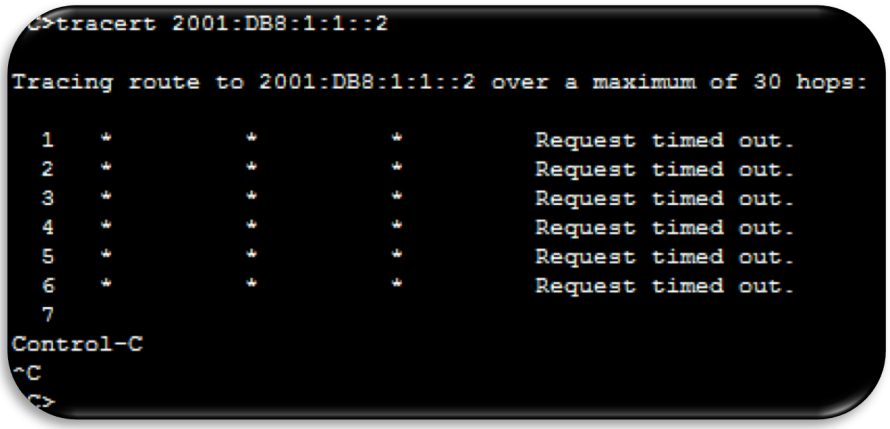
PC>tracert 2001:DB8:1:4::2

Tracing route to 2001:DB8:1:4::2 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 2001:DB8:1:1::1
2 0 ms 1 ms 0 ms 2001:DB8:1:2::1
3 4 ms 1 ms 12 ms 2001:DB8:1:3::2
4 * * * Request timed out.
5 * * * Request timed out.
6 * * * Request timed out.
7
Control-C
^C
PC>

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? No se alcanzó ninguna dirección IPv6.



```
PC>tracert 2001:DB8:1:1::2

Tracing route to 2001:DB8:1:1::2 over a maximum of 30 hops:

1 * * * Request timed out.
2 * * * Request timed out.
3 * * * Request timed out.
4 * * * Request timed out.
5 * * * Request timed out.
6 * * * Request timed out.
7
Control-C
^C
PC>
```

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? Sí

```
R3>show ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::3
    2001:DB8:1:4::1
GigabitEthernet0/1         [up/up]
Serial0/0/0                [administratively down/down]
Serial0/0/1                [up/up]
    FE80::3
    2001:DB8:1:3::2
Vlan1                      [administratively down/down]
R3>
```

```
R3>show ipv6 interface brief
GigabitEthernet0/0 [up/up]
FE80::3
2001:DB8:1:4::1
GigabitEthernet0/1 [up/up]
Serial0/0/0 [administratively down/down]
Serial0/0/1 [up/up]
FE80::3
2001:DB8:1:3::2
Vlan1 [administratively down/down]
R3>
```

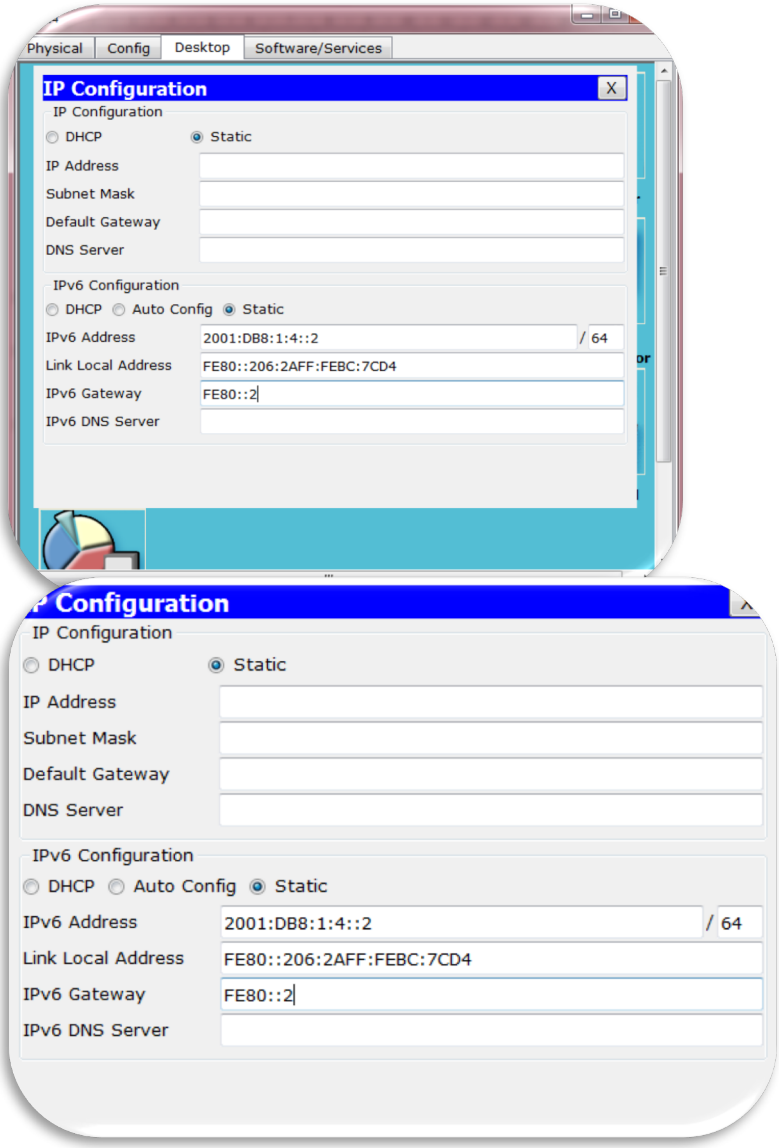
g. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

```
show ipv6 route
Ipv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
D   2001:DB8:1:1::/64 [90/2682112]
     via FE80::2, Serial0/0/1, receive
D   2001:DB8:1:2::/64 [90/2681856]
     via FE80::2, Serial0/0/1, receive
C   2001:DB8:1:3::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:1:3::2/128 [0/0]
     via Serial0/0/1, receive
C   2001:DB8:1:4::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:1:4::1/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

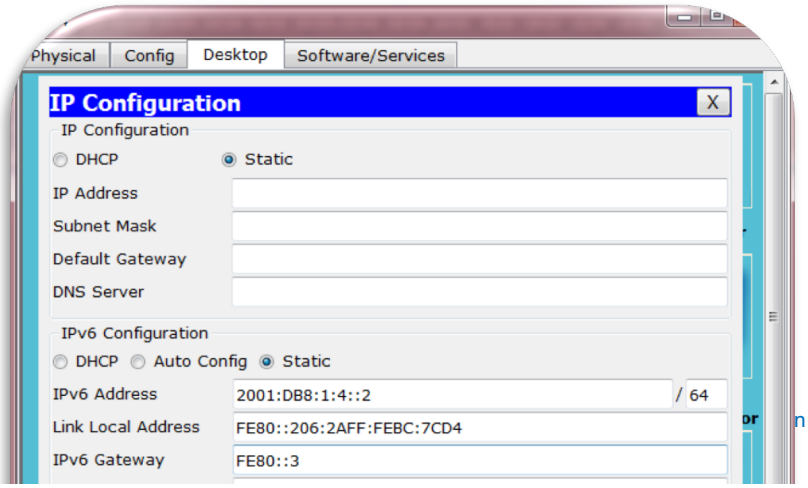
```
R3>show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
D 2001:DB8:1:1::/64 [90/2682112]
via FE80::2, Serial0/0/1, receive
D 2001:DB8:1:2::/64 [90/2681856]
via FE80::2, Serial0/0/1, receive
C 2001:DB8:1:3::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:1:3::2/128 [0/0]
via Serial0/0/1, receive
C 2001:DB8:1:4::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:1:4::1/128 [0/0]
via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
via Null0, receive
R3>
```

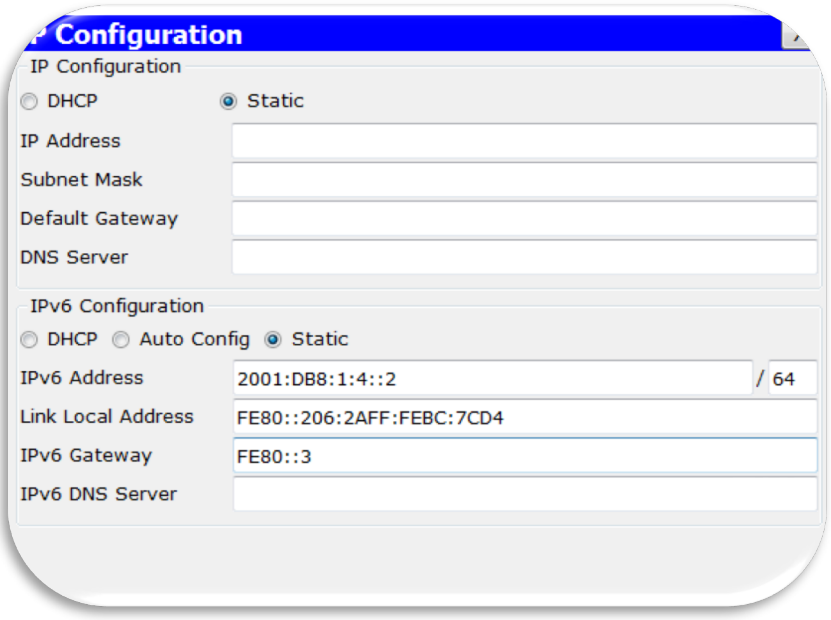
Paso 3: Proponga una solución para resolver el problema.

a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red. ¿Cuál es el error? La PC4 utiliza una configuración de gateway predeterminado incorrecta.



Este debe ser cambiado por:





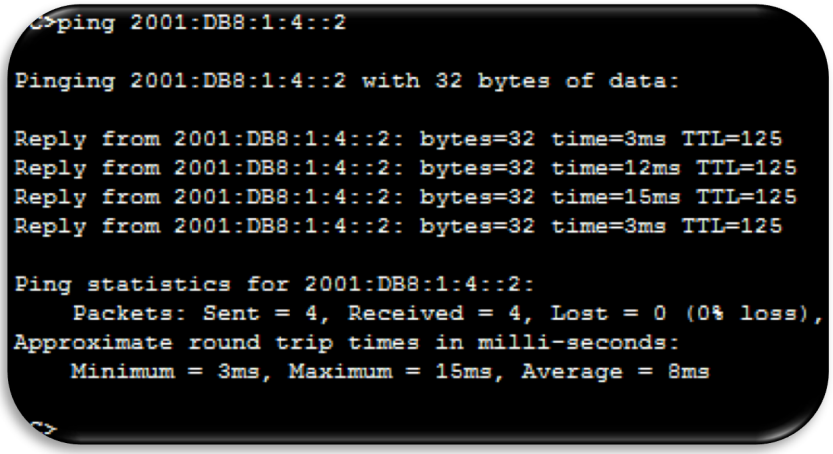
b. ¿Qué solución propondría para corregir el problema? Configurar la PC4 con la dirección de gateway predeterminado correcta: FE80::3.

Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

Paso 5: Verifique que la conectividad esté restaurada.

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



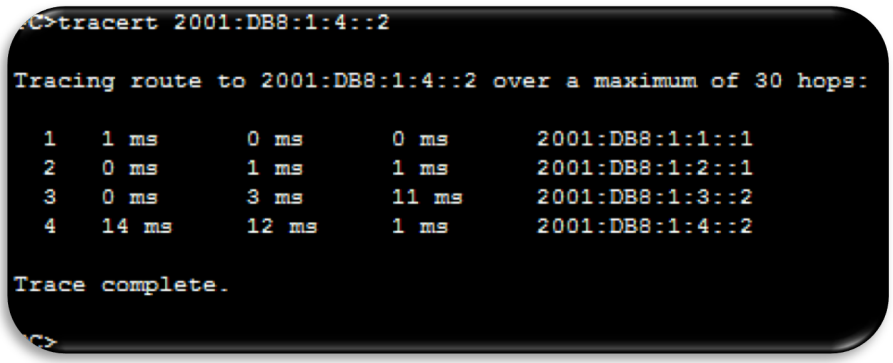
PC>ping 2001:DB8:1:4::2

Pinging 2001:DB8:1:4::2 with 32 bytes of data:

Reply from 2001:DB8:1:4::2: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=15ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=3ms TTL=125

Ping statistics for 2001:DB8:1:4::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 15ms, Average = 8ms

PC>



PC>tracert 2001:DB8:1:4::2

Tracing route to 2001:DB8:1:4::2 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 2001:DB8:1:1::1

2 0 ms 1 ms 1 ms 2001:DB8:1:2::1

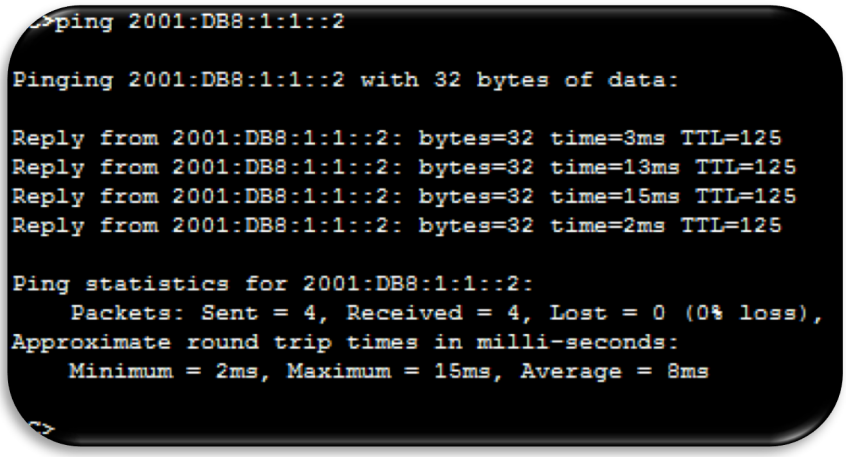
3 0 ms 3 ms 11 ms 2001:DB8:1:3::2

4 14 ms 12 ms 1 ms 2001:DB8:1:4::2

Trace complete.

PC>

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



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=3ms TTL=125

Reply from 2001:DB8:1:1::2: bytes=32 time=13ms TTL=125

Reply from 2001:DB8:1:1::2: bytes=32 time=15ms TTL=125

Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125

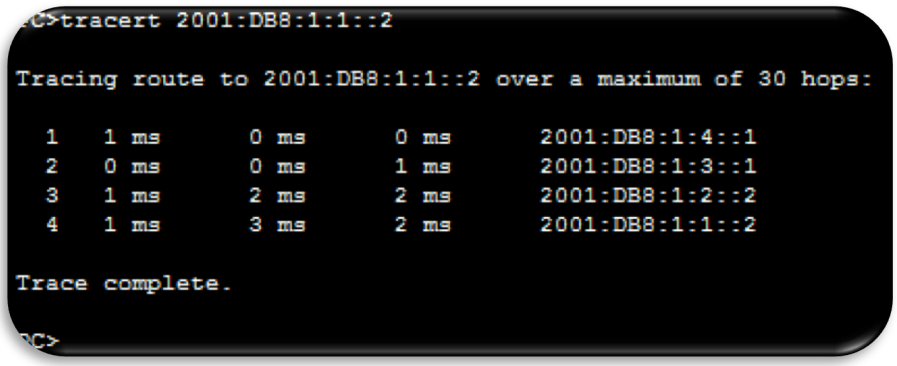
Ping statistics for 2001:DB8:1:1::2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 15ms, Average = 8ms

PC>



PC>tracert 2001:DB8:1:1::2

Tracing route to 2001:DB8:1:1::2 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 2001:DB8:1:4::1

2 0 ms 0 ms 1 ms 2001:DB8:1:3::1

3 1 ms 2 ms 2 ms 2001:DB8:1:2::2

4 1 ms 3 ms 2 ms 2001:DB8:1:1::2

Trace complete.

PC>

Paso 6: Documentar la solución.

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Probar y restaurar la conectividad entre la PC1 y la PC3	Paso 1b	5	
		5	
		5	
		5	
		5	
		5	
		5	
		5	
		5	
Total de la parte 1		**45**	
Parte 2: Probar y restaurar la conectividad entre la PC2 y la PC4	Paso 1b	5	
		5	
		5	
		5	
		5	
		5	
		5	
Total de la parte 2		**35**	
Puntuación de Packet Tracer		**20**	
Puntuación total		**100**	

Packet Tracer: Resolución de problemas de direccionamiento IPv4 e IPv6 (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

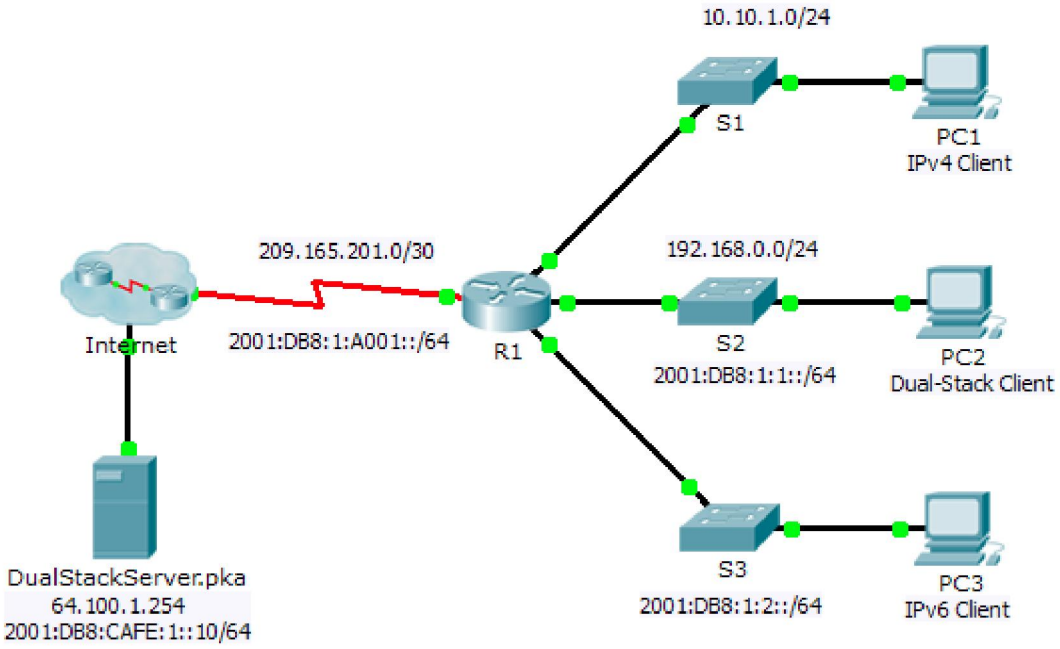


Tabla de direccionamiento

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
		192.168.0.1	255.255.255.0	No aplicable
	Se0/1			No aplicable

		2001:DB8:1:2::1/64		No aplicable
	s0/0/0	209.165.201.2	255.255.255.252	No aplicable
				No aplicable
		FE80::1		No aplicable
Servidor dual-stack	NIC	64.100.1.254	255.255.255.0	64.100.1.1
				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
				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

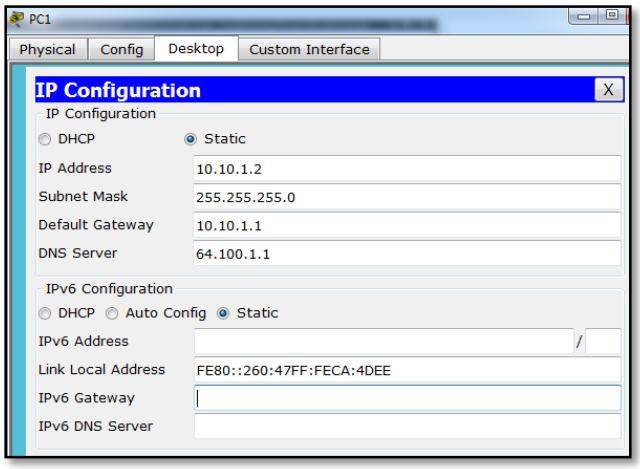
Un cliente que usa la **PC1** se queja de que no puede acceder a la página Web **dualstackserver.pka**.

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.	




```
PC>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time=121ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 121ms, Average = 30ms

PC>
```

```
PC>nslookup dualstackserver.pka

Server:  [64.100.1.1]
Address:  64.100.1.1
DNS request timed out.
            timeout was 15000 milli seconds.
DNS request timed out.
            timeout was 15000 milli seconds.
DNS request timed out.
            timeout was 15000 milli seconds.
*** Request to 64.100.1.1 timed-out

PC>
```

Paso 2: Considerar las causas probables de la falla

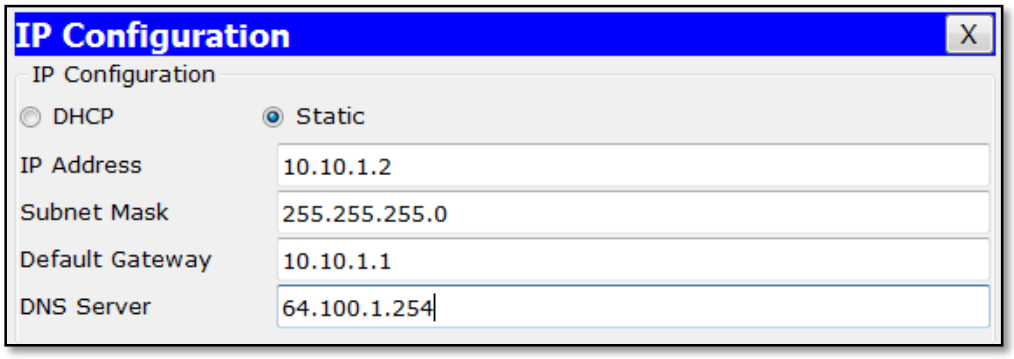
a. Observe las pruebas que se realizaron. De ser posible, analice con sus colegas técnicos de red
(compañeros de curso) las situaciones que podrían ser la causa de este problema.

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.

- Dirección configurada como DNS en el PC no es la correcta.

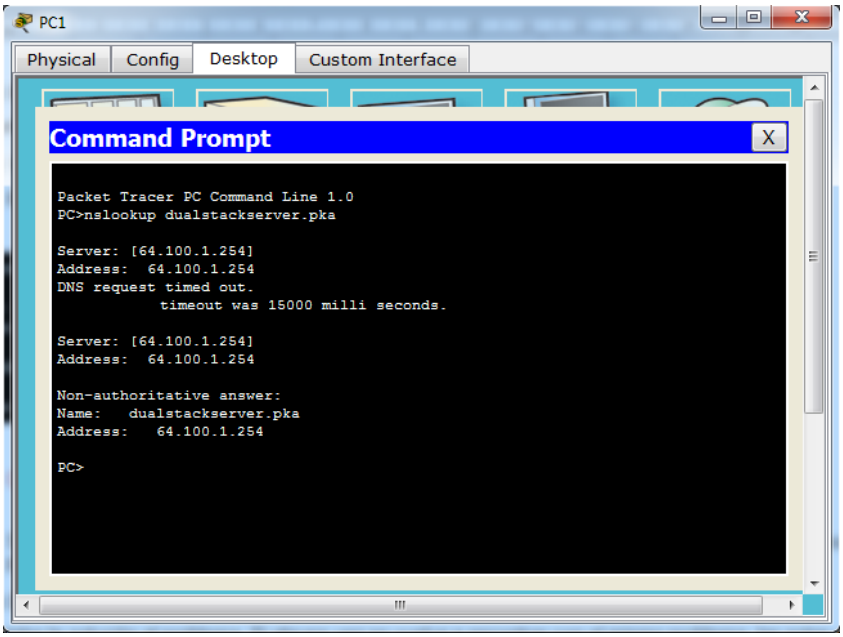


Paso 4: Implemente el plan.

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

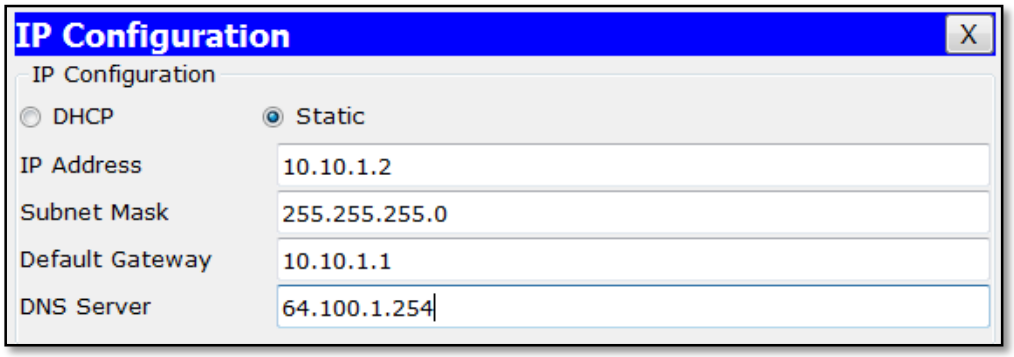
Paso 5: Verificar que la solución haya resuelto el problema

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



- Con el cambio hecho ya está funcionando.

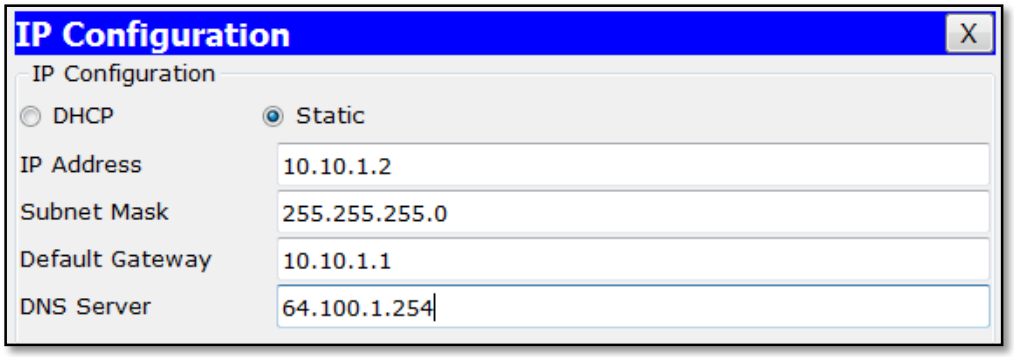
b. Si el problema persiste, revierta el cambio en caso de no estar seguro de que sea correcto y vuelva al paso 4.



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.

- La dirección DNS IPv4 de la PC1 es incorrecta.



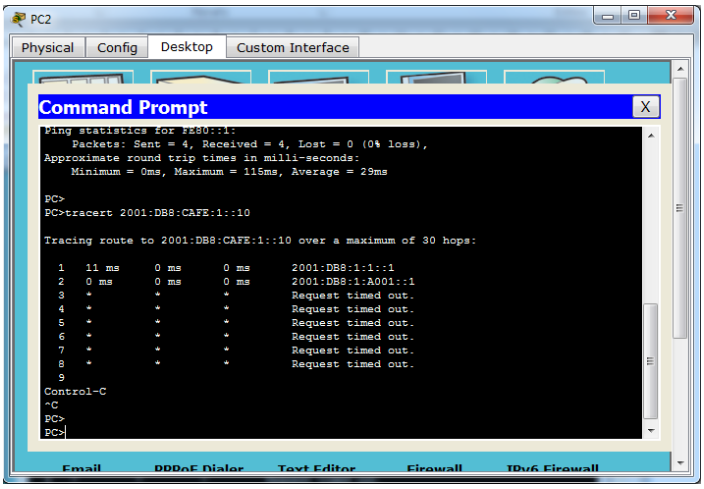
Parte 2: Resolver el segundo el problema

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

Paso 1: Verificar una solicitud detallada de soporte técnico.

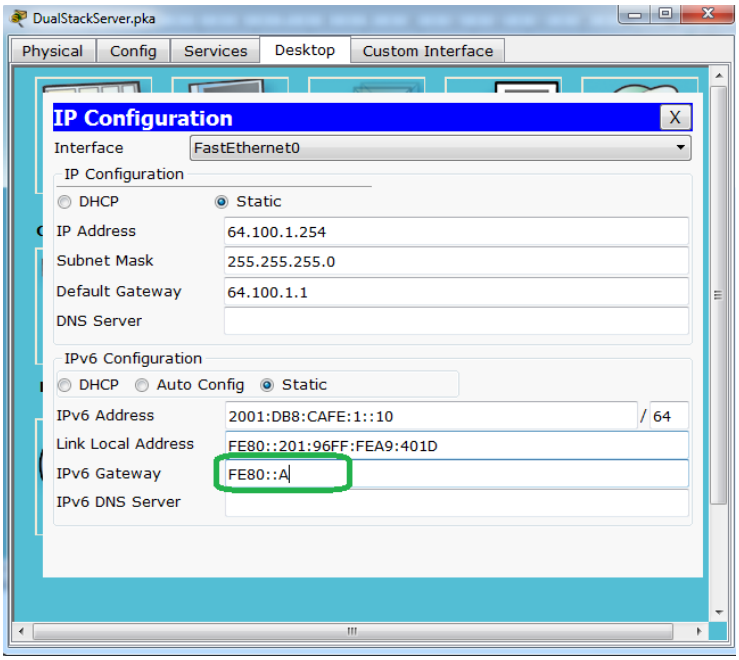
El soporte técnico recopiló la siguiente información del cliente por vía telefónica. Verifique que sea correcto.

Solicitud de soporte técnico	
Identificador de cliente: PC2	
Problema: No puede acceder al servicio FTP de 2001:DB8:CAFE:1:10.	
Información detallada sobre el problema	
Prueba: ¿Tiene la PC una dirección IPv6 cuando se utiliza **ipv6config**?	Sí
Prueba: ¿Puede la PC ponerse en contacto con el gateway usando **ping**?	Sí
Prueba: ¿Puede la PC contactar al servidor utilizando **tracert**?	No
Resolución: Elevar al soporte de nivel 2.	



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

- Cambiamos el Gateway del servidor.



Paso 3: Documentar la solución.

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

- La dirección de gateway IPv6 de DualStackServer.pka es incorrecta

```
PC>tracert 2001:DB8:CAFE:1::10

Tracing route to 2001:DB8:CAFE:1::10 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      2001:DB8:1:1::1
  2    1 ms      0 ms      1 ms      2001:DB8:1:A001::1
  3    0 ms      0 ms      4 ms      2001:DB8:CAFE:1::10

Trace complete.

PC>
```

Parte 3: Resolver el tercer problema

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

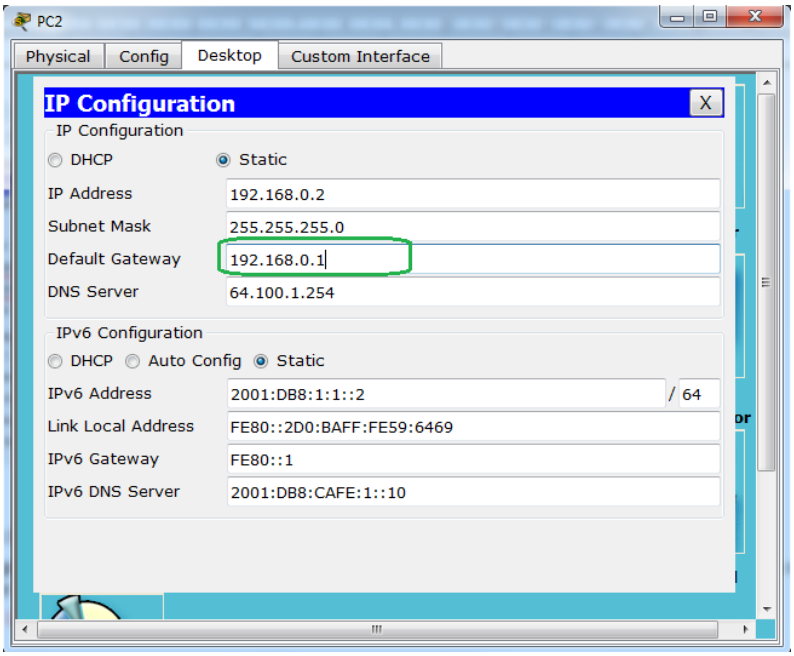
Paso 1: Verificar una solicitud detallada de soporte técnico.

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

Solicitud de soporte técnico	
Identificador de cliente: PC1	
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.	

```
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

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

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

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

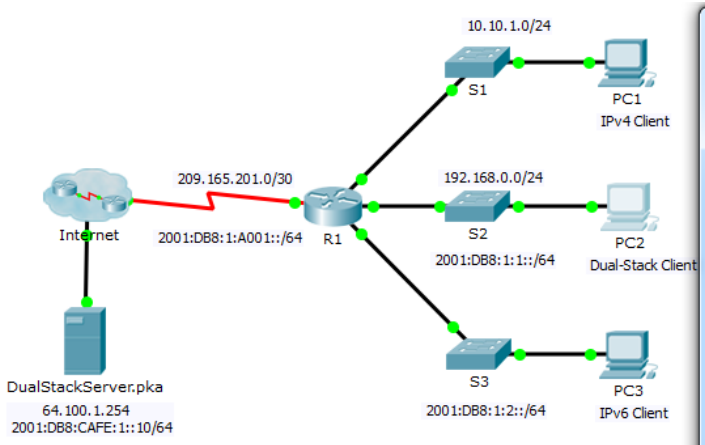


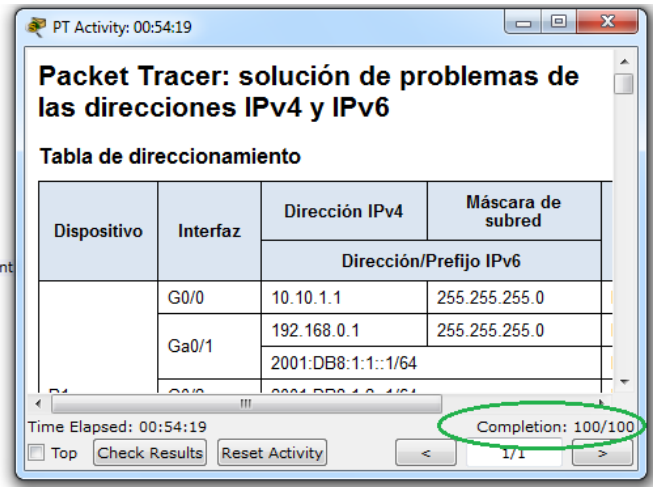
Paso 3: Documentar la solución.

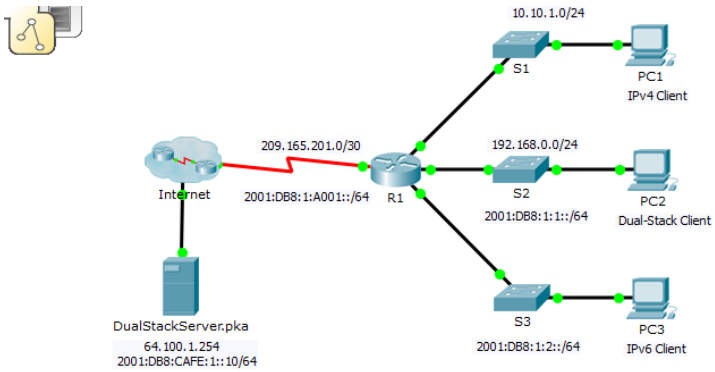
Registre la solución al problema. Si alguna vez se vuelve a encontrar con el mismo problema, las notas serán muy valiosas.

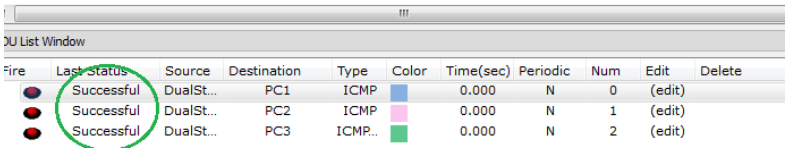
- La dirección de gateway IPv4 de la PC2 es incorrecta.

```
PC>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=1ms TTL=127
Reply from 192.168.0.2: bytes=32 time=1ms TTL=127
Reply from 192.168.0.2: bytes=32 time=0ms TTL=127
Reply from 192.168.0.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```









Packet Tracer: Reto de habilidades de integración (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

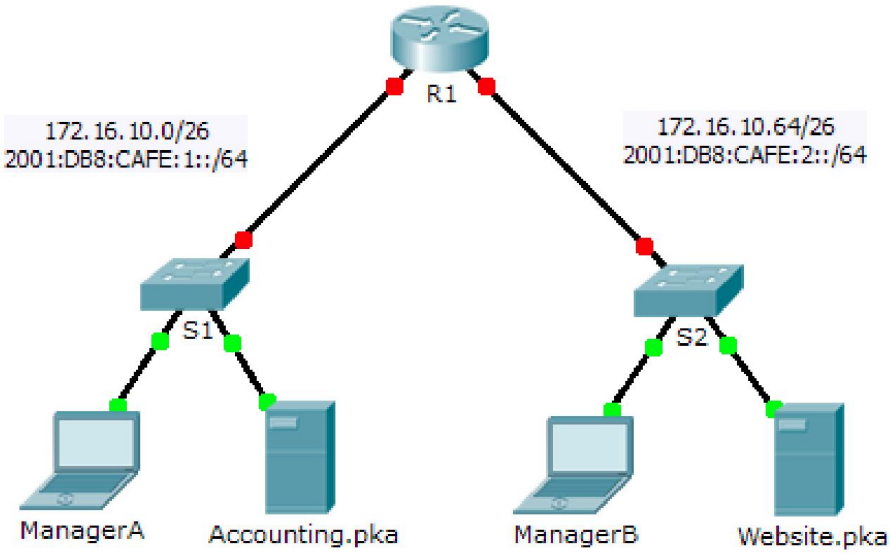


Tabla de direccionamiento

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

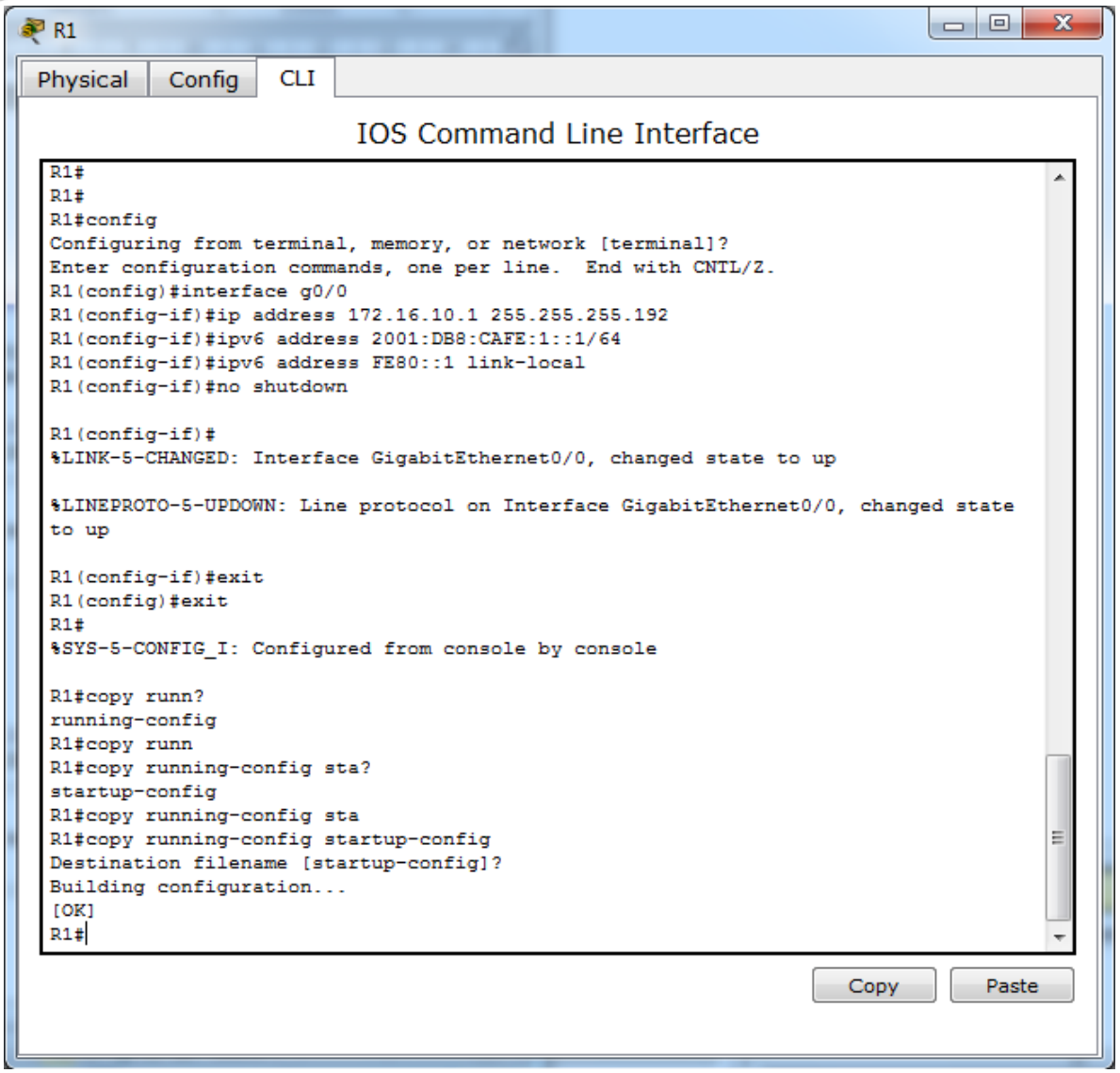
Su compañía fue contratada para configurar una red pequeña para el propietario de un restaurante. Hay dos restaurantes cercanos entre sí y comparten una conexión. El equipo y el cableado están instalados, y el administrador de red diseñó el plan de implementación. Su trabajo consiste en implementar el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

Requisitos

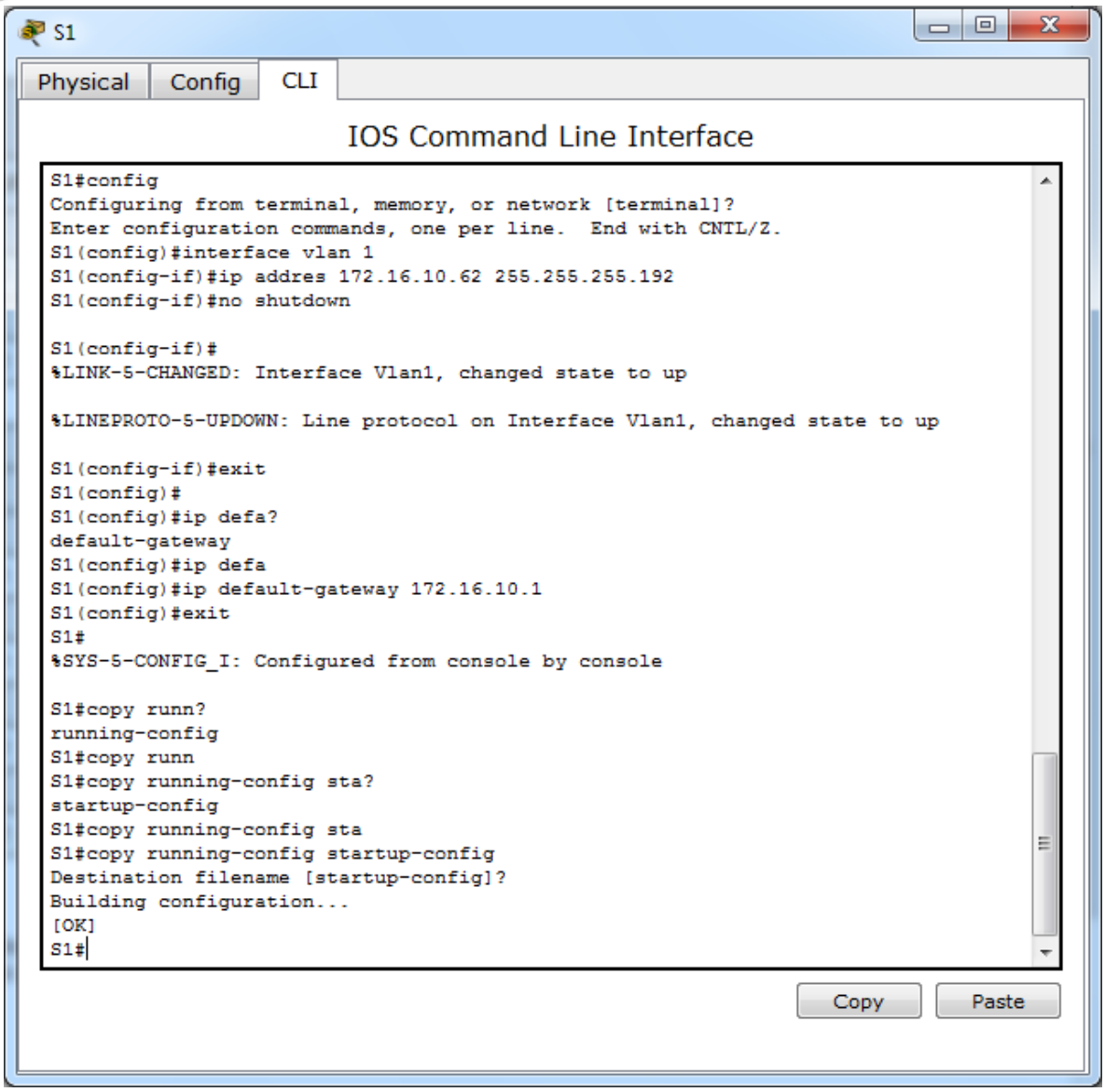
- Complete el registro de la **tabla de direccionamiento**.
- Configure direccionamiento IPv4 e IPv6 en el **R1**.

Con la información que hemos recolectado podemos completar la información de las tablas de direccionamiento.

- Procedemos a configurar el router R1.

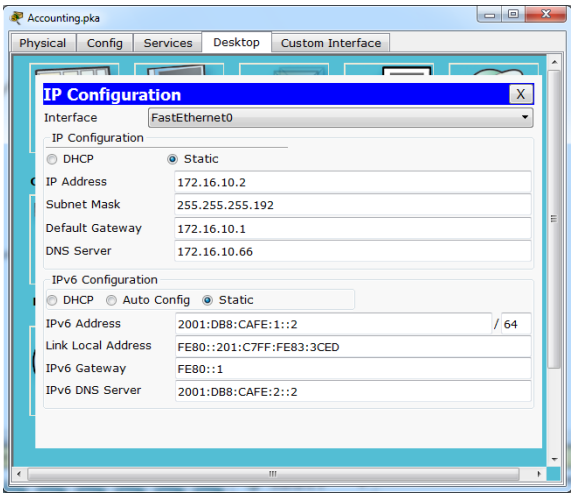


- Configure direccionamiento IPv4 en el **S1**. El **S2** ya está configurado.

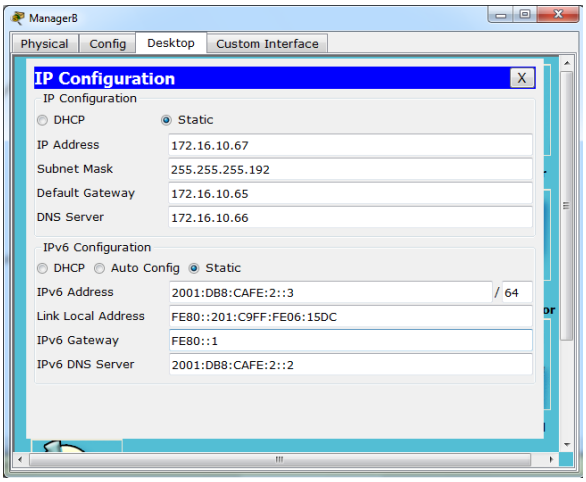


- Configure direccionamiento IPv4 e IPv6 en **ManagerA**. El resto de los clientes ya están configurados.

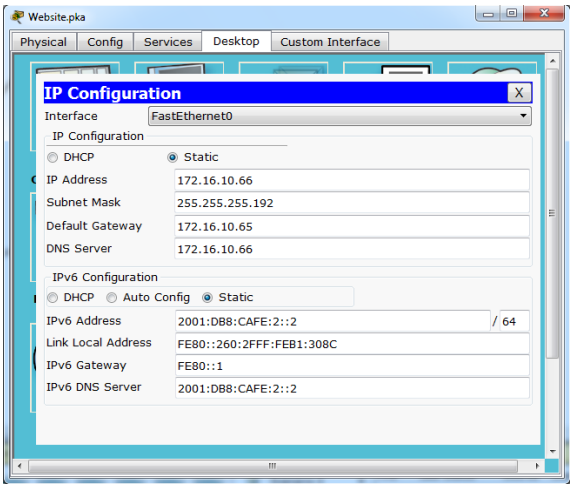
- **Accounting.pka**



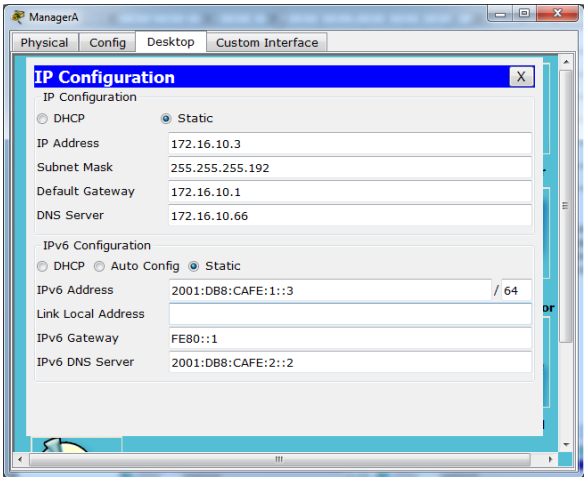
- **ManagerB**



- **Website.pka**



- Procedemos a configurar el PC ManagerA con la información de la tabla de direccionamiento.



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

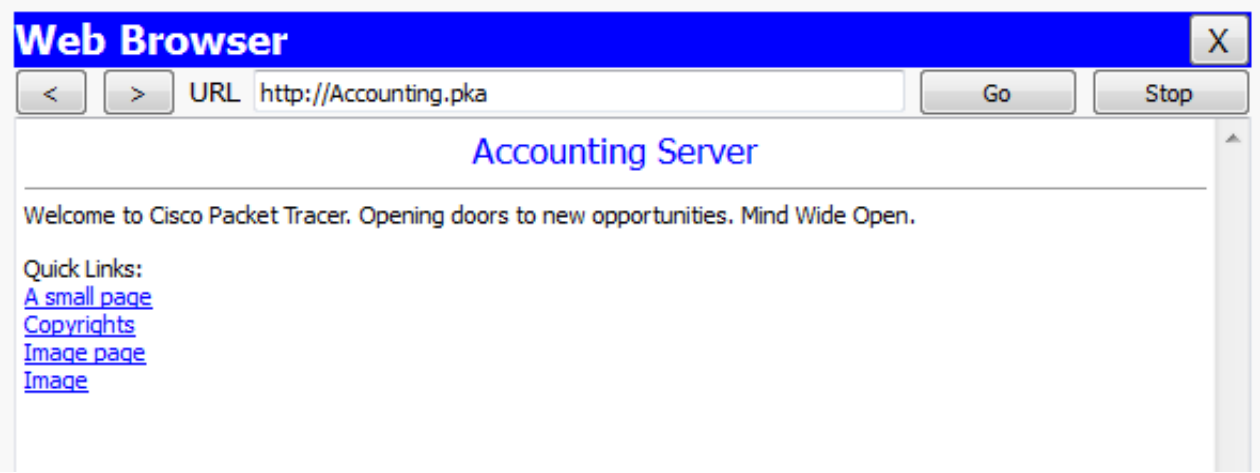
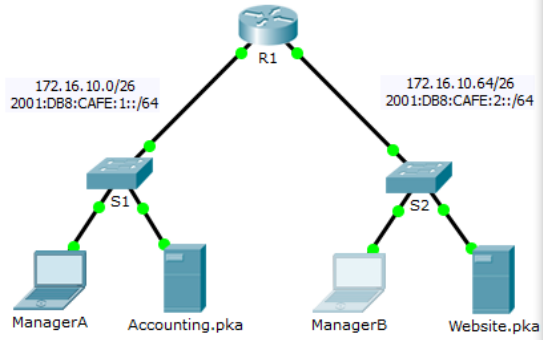


Tabla de calificación sugerida

Packet Tracer tienen una puntuación de 80 puntos. Completar la **tabla de direccionamiento** vale 20 puntos.



PT Activity: 00:52:58

Packet Tracer: Reto de habilidades de integración

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred
		Dirección/Prefijo IPv6	
	G0/0	172.16.10.1	255.255.255.192
		2001:DB8:CAFE:1::1/64	

Time Elapsed: 00:52:58 Completion: 80/80

Top | Check Results | Reset Activity | < | 1/1 | >

Activity Results

Time Elapsed: 00:59:54

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Default Gateway IPv6	Correct	5	Default Gatew...	
DNS Server IP	Correct	4	IPv4 Host Add...	
DNS Server IPv6	Correct	4	IPv6 Host Add...	
Ports				
FastEthernet0				
IP Address	Correct	5	IPv4 Host Add...	
IPv6 Addresses				
2001:DB8:CAFE:...				
IP Address	Correct	5	IPv6 Host Add...	
Prefix Len...	Correct	2	IPv6 Host Add...	
Subnet Mask	Correct	2	IPv4 Host Add...	
R1				
Ports				
GigabitEthernet0/0				
IP Address	Correct	5	Device Interfa...	
IPv6 Addresses				
2001:DB8:CAFE:...				
IP Address	Correct	5	Device Interfa...	
Prefix Len...	Correct	2	Device Interfa...	
Link Local	Correct	3	Device Interfa...	
Port Status	Correct	1	Device Interfa...	
Subnet Mask	Correct	2	Device Interfa...	
GigabitEthernet0/1				
IP Address	Correct	4	Device Interfa...	
IPv6 Addresses				
2001:DB8:CAFE:...				
IP Address	Correct	5	Device Interfa...	
Prefix Len...	Correct	2	Device Interfa...	
Link Local	Correct	3	Device Interfa...	
Port Status	Correct	1	Device Interfa...	
Subnet Mask	Correct	2	Device Interfa...	
S1				
Default Gateway	Correct	5	Default Gatew...	
Ports				
Vlan1				
IP Address	Correct	5	IPv4 Host Add...	
Port Status	Correct	1	IPv4 Host Add...	
Subnet Mask	Correct	2	IPv4 Host Add...	

Score : 80/80

Item Count : 24/24

Component	Items/Total	Score
Default Gateway Configuration	3/3	15/15
Device Interface Configuration	12/12	35/35
IPv4 Host Address Configuration	6/6	19/19
IPv6 Host Address Configuration	3/3	11/11

Close

Laboratorio 9.1.4.6

Packet Tracer: Situación de división en subredes 1 (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

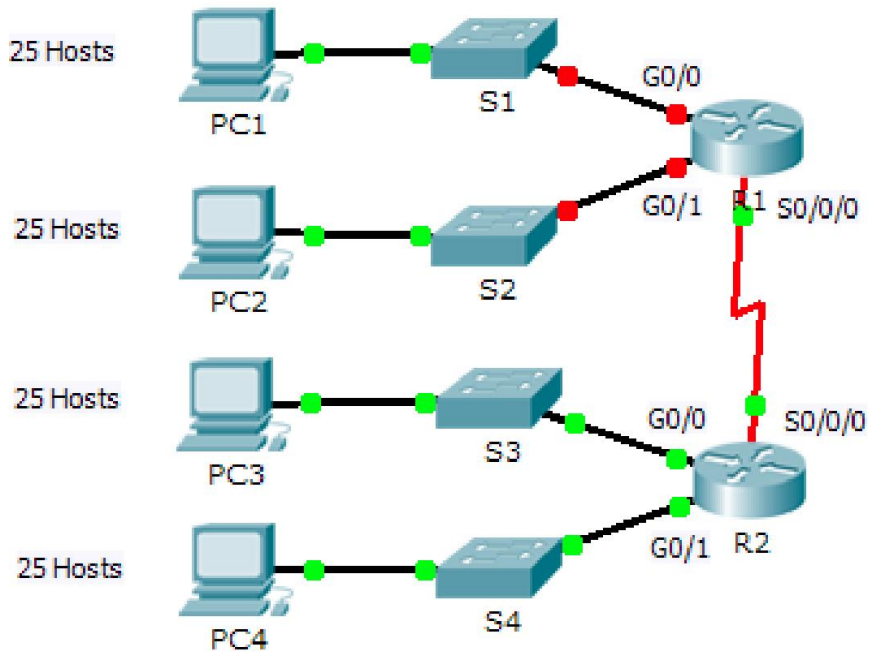


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de	Gateway
	G0/0	192.168.100.1	255.255.255.224	No aplicable

R1		192.168.100.33	255.255.255.224	No aplicable
		192.168.100.129	255.255.255.224	No aplicable
R2	G0/0	192.168.100.65	255.255.255.224	No aplicable
		192.168.100.97	255.255.255.224	No aplicable
		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?
   - 5

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

c. ¿Cuántas subredes se crean?

- 8

d. ¿Cuántos hosts utilizables se crean por subred?

- 30

Nota: si su respuesta es menor que los 25 hosts requeridos, tomó prestados demasiados bits.

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

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

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

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

Net 2: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

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

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

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

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

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

- Podemos encontrar muchas ayudas que nos facilitan este proceso de subneteo, entre ellas las que muestro a continuación:

1.

Network:	192.168.100.0/27	11000000.10101000.01100100.000 00000
HostMin:	192.168.100.1	11000000.10101000.01100100.000 00001
HostMax:	192.168.100.30	11000000.10101000.01100100.000 11110
Broadcast:	192.168.100.31	11000000.10101000.01100100.000 11111
Hosts/Net:	30	Class C, Private Internet

2.

Network:	192.168.100.32/27	11000000.10101000.01100100.001 00000

HostMin:	192.168.100.33	11000000.10101000.01100100.001 00001
HostMax:	192.168.100.62	11000000.10101000.01100100.001 11110
Broadcast:	192.168.100.63	11000000.10101000.01100100.001 11111
Hosts/Net:	30	Class C, Private Internet

3.

Network:	192.168.100.64/27	11000000.10101000.01100100.010 00000
HostMin:	192.168.100.65	11000000.10101000.01100100.010 00001
HostMax:	192.168.100.94	11000000.10101000.01100100.010 11110
Broadcast:	192.168.100.95	11000000.10101000.01100100.010 11111
Hosts/Net:	30	Class C, Private Internet

4.

Network:	192.168.100.96/27	11000000.10101000.01100100.011 00000
HostMin:	192.168.100.97	11000000.10101000.01100100.011 00001
HostMax:	192.168.100.126	11000000.10101000.01100100.011 11110
Broadcast:	192.168.100.127	11000000.10101000.01100100.011 11111
Hosts/Net:	30	Class C, Private Internet

5.

Network:	192.168.100.128/27	11000000.10101000.01100100.100 00000
HostMin:	192.168.100.129	11000000.10101000.01100100.100 00001
HostMax:	192.168.100.158	11000000.10101000.01100100.100 11110
Broadcast:	192.168.100.159	11000000.10101000.01100100.100 11111
Hosts/Net:	30	Class C, Private Internet

6.

Network:	192.168.100.160/27	11000000.10101000.01100100.101 00000
HostMin:	192.168.100.161	11000000.10101000.01100100.101 00001
HostMax:	192.168.100.190	11000000.10101000.01100100.101 11110
Broadcast:	192.168.100.191	11000000.10101000.01100100.101 11111
Hosts/Net:	30	Class C, Private Internet

7.

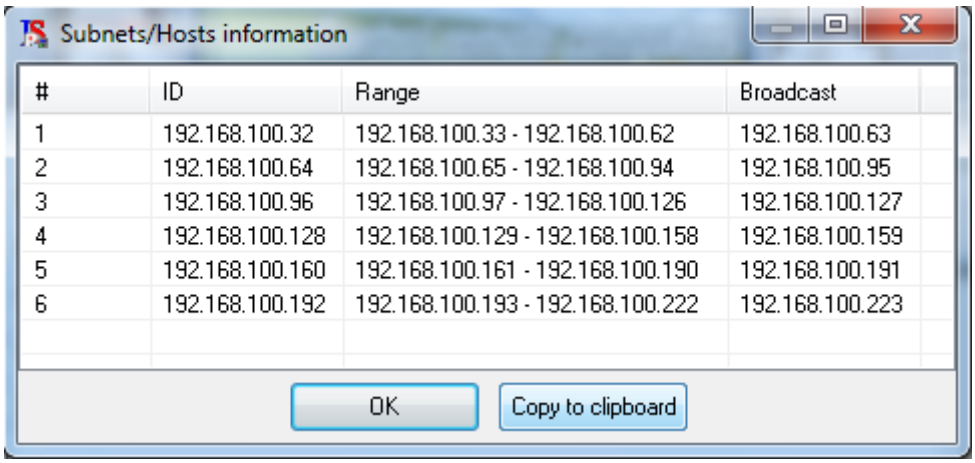
```
Network:    192.168.100.192/27   11000000.10101000.01100100.110 00000
HostMin:    192.168.100.193      11000000.10101000.01100100.110 00001
HostMax:    192.168.100.222      11000000.10101000.01100100.110 11110
Broadcast:  192.168.100.223      11000000.10101000.01100100.110 11111
Hosts/Net:  30                   Class C, Private Internet
```

8.

```
Network:    192.168.100.224/27   11000000.10101000.01100100.111 00000
HostMin:    192.168.100.225      11000000.10101000.01100100.111 00001
HostMax:    192.168.100.254      11000000.10101000.01100100.111 11110
Broadcast:  192.168.100.255      11000000.10101000.01100100.111 11111
Hosts/Net:  30                   Class C, Private Internet
```

Subnets: 8

Hosts: 240



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

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

255 . 255 . 255 . _____

255 . 255 . 255 . 224

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

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

Tabla de subredes

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

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

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

192.168.100.0 /27

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.
b. Asigne las primeras direcciones IP utilizables al R2 para los 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 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.

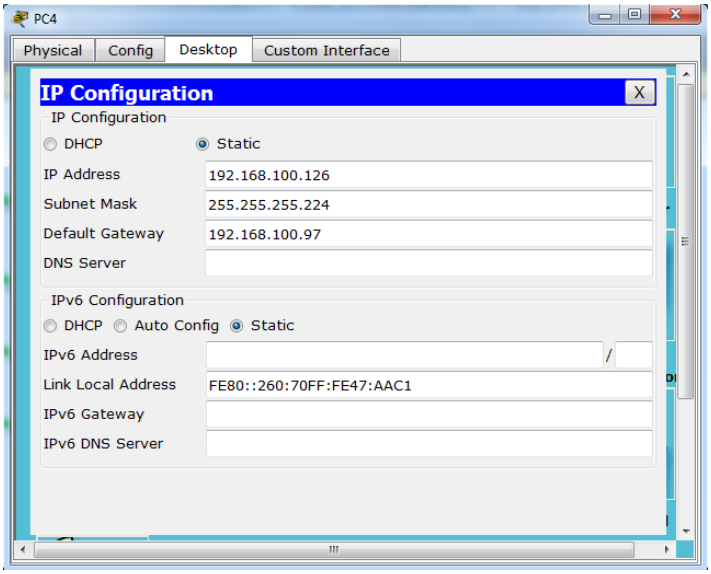
Paso 1: Configurar el direccionamiento IP en las interfaces LAN del R1

```
R1(config)#interface g0/0
R1(config-if)#ip addres 192.168.100.1 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface g0/1
R1(config-if)#ip addres 192.168.100.33 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip addres 192.168.100.129 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#do wr
```

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

```
S3(config)#int vlan 1
S3(config-if)#ip add
S3(config-if)#ip address 192.168.100.66 255.255.255.224
S3(config-if)#exit
S3(config)#ip de
S3(config)#ip default-gateway 192.168.100.65
```

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



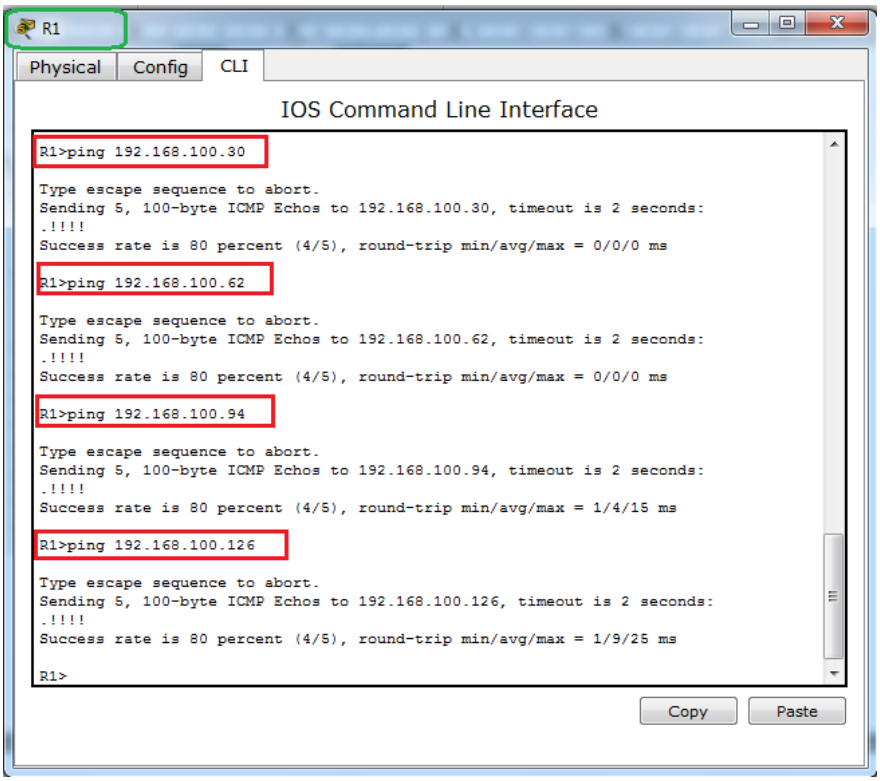
Paso 4: Verifique la conectividad.

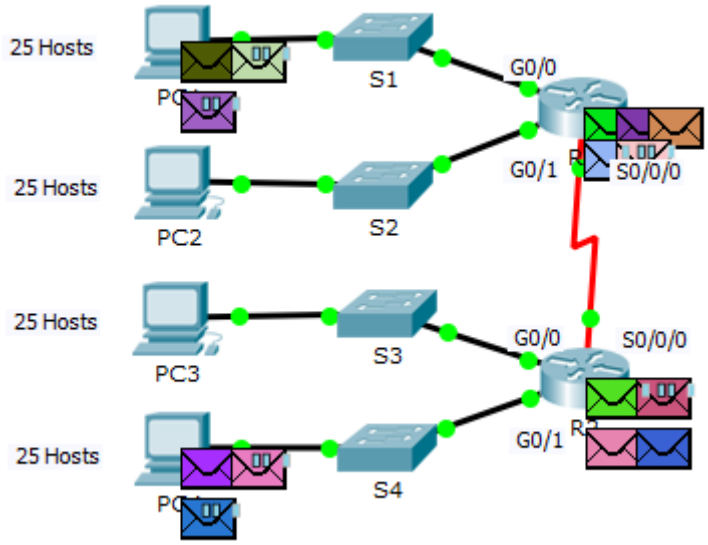
Solo puede verificar la conectividad desde el R1, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Diseñar un esquema de direccionamiento IP	Paso 1a	1	
		1	
		1	
		1	
		4	
		2	
Completar la tabla de subredes	Paso 1g	10	
Asignar subredes	Paso 2	10	
Documentar el direccionamiento	Paso 3	40	
Total de la parte 1		**70**	
	Puntuación de Packet Tracer	**30**	
	Puntuación total	**100**	


R1
Physical
Config
CLI
IOS Command Line Interface
R1>ping 192.168.100.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
R1>ping 192.168.100.62
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.62, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
R1>ping 192.168.100.94
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.94, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/4/15 ms
R1>ping 192.168.100.126
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.126, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/9/25 ms
R1>
Copy
Paste


25 Hosts
25 Hosts
PC2
25 Hosts
PC3
25 Hosts
S1
S2
S3
S4
G0/0
G0/1
S0/0/0
G0/0
G0/1
S0/0/0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC4	PC3	ICMP		0.000	N	0	(edit)	
	Successful	PC4	PC2	ICMP		0.000	N	1	(edit)	
	Successful	PC4	PC1	ICMP		0.000	N	2	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	3	(edit)	
	Successful	PC1	PC3	ICMP		0.000	N	4	(edit)	
	Successful	PC1	PC4	ICMP		0.000	N	5	(edit)	
	Successful	R1	PC1	ICMP		0.000	N	6	(edit)	
	Successful	R1	R1	ICMP		0.000	N	7	(edit)	
	Successful	R1	PC2	ICMP		0.000	N	8	(edit)	
	Successful	R1	PC3	ICMP		0.000	N	9	(edit)	
	Successful	R1	PC4	ICMP		0.000	N	10	(edit)	
	Successful	R2	PC1	ICMP		0.000	N	11	(edit)	
	Successful	R2	PC2	ICMP		0.000	N	12	(edit)	
	Successful	R2	PC3	ICMP		0.000	N	13	(edit)	
	Successful	R2	PC4	ICMP		0.000	N	14	(edit)	

Laboratorio 9.1.4.7

Packet Tracer: Situación de división en subredes 2 (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

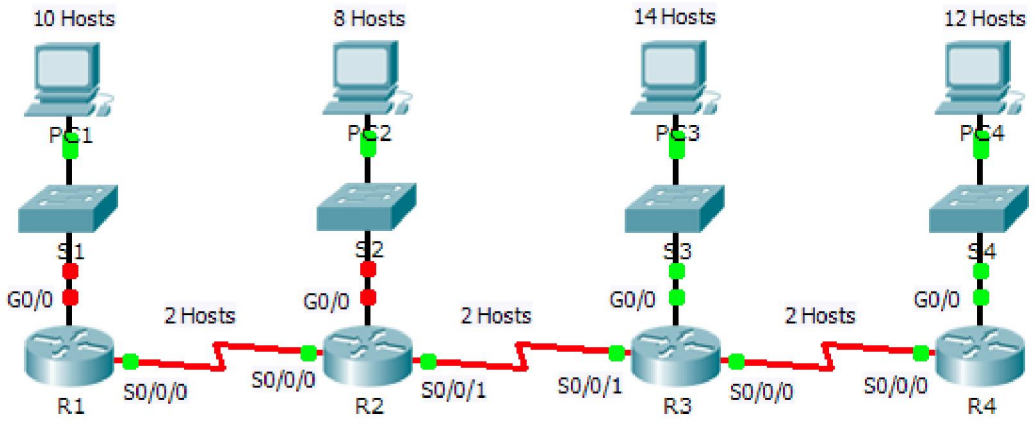


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.31.1.1	255.255.255.240	No aplicable
		172.31.1.65	255.255.255.240	No aplicable
R2	G0/0	172.31.1.17	255.255.255.240	No aplicable
		172.31.1.78	255.255.255.240	No aplicable
		172.31.1.81	255.255.255.240	No aplicable
R3	G0/0	172.31.1.33	255.255.255.240	No aplicable
		172.31.1.97	255.255.255.240	No aplicable
		172.31.1.94	255.255.255.240	No aplicable
R4	G0/0	172.31.1.49	255.255.255.240	No aplicable
		172.31.1.110	255.255.255.240	No aplicable
S1	VLAN 1	172.31.1.2	255.255.255.240	172.31.1.1
S2	VLAN 1	172.31.1.18	255.255.255.240	172.31.1.17
S3	VLAN 1	172.31.1.34	255.255.255.240	172.31.1.33
S4	VLAN 1	172.31.1.50	255.255.255.240	172.31.1.49
PC1	NIC	172.31.1.14	255.255.255.240	172.31.1.1
PC2	NIC	172.31.1.30	255.255.255.240	172.31.1.17
PC3	NIC	172.31.1.46	255.255.255.240	172.31.1.33
PC4	NIC	172.31.1.62	255.255.255.240	172.31.1.49

Objetivos

- Parte 1: Diseñar un esquema de direccionamiento IP
- Parte 2: Asignar direcciones IP a los dispositivos de red y verificar la conectividad

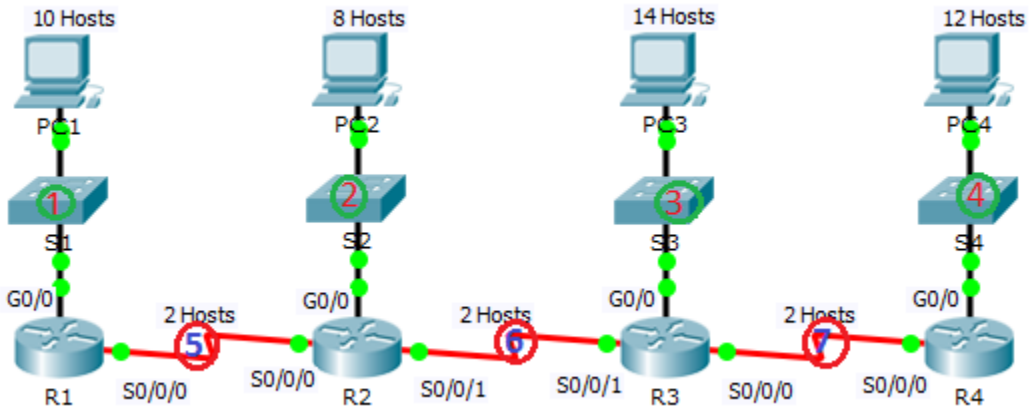
Situación

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

Parte 1: Diseñar un esquema de direccionamiento IP

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

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



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

c. ¿Cuántas subredes se crean? 16

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

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.

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

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

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

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

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

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

```
11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___
11111111.11111111.11111111.  1   1   1   1   0   0   0   0
   255   .   255   .   255   . ______
   255   .   255   .   255   .  240
```

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

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

Tabla de subredes

Número de subred	IP de subred	Primera IP de host utilizable	Última IP de host utilizable	Dirección de broadcast
0	172.31.1.0	172.31.1.1	172.31.1.14	172.16.1.15
1	172.31.1.16	172.31.1.17	172.31.1.30	172.31.1.31
2	172.31.1.32	172.31.1.33	172.31.1.46	172.31.1.47
3	172.31.1.48	172.31.1.49	172.31.1.62	172.31.1.63
4	172.31.1.64	172.31.1.65	172.31.1.78	172.31.1.79
5	172.31.1.80	172.31.1.81	172.31.1.94	172.31.1.95
6	172.31.1.96	172.31.1.97	172.31.1.110	172.31.1.111
7	172.31.1.112	172.31.1.113	172.31.1.126	172.31.1.127
8	172.31.1.128	172.31.1.129	172.31.1.142	172.31.1.143
9	172.31.1.144	172.31.1.145	172.31.1.158	172.31.1.159
10	172.31.1.160	172.31.1.161	172.31.1.174	172.31.1.175
11	172.31.1.176	172.31.1.177	172.31.1.190	172.31.1.191
12	172.31.1.192	172.31.1.193	172.31.1.206	172.31.1.207
13	172.31.1.208	172.31.1.209	172.31.1.222	172.31.1.223
14	172.31.1.224	172.31.1.225	172.31.1.238	172.31.1.239
15	172.31.1.240	172.31.1.241	172.31.1.254	172.31.1.255

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

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

a. Asigne la subred 0 a la LAN del R1: 172.31.1.0 /28

b. Asigne la subred 1 a la LAN del R2: 172.31.1.16/28

c. Asigne la subred 2 a la LAN del R3: 172.31.1.32/28

d. Asigne la subred 3 a la LAN del R4: 172.31.1.48/28

e. Asigne la subred 4 al enlace entre el R1 y el R2: 172.31.1.64/28

f. Asigne la subred 5 al enlace entre el R2 y el R3: 172.31.1.80/28

g. Asigne la subred 6 al enlace entre el R3 y el R4: 172.31.1.96/28

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.

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

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip addres 172.31.1.1 255.255.255.240
R1(config-if)#no shutdown
```

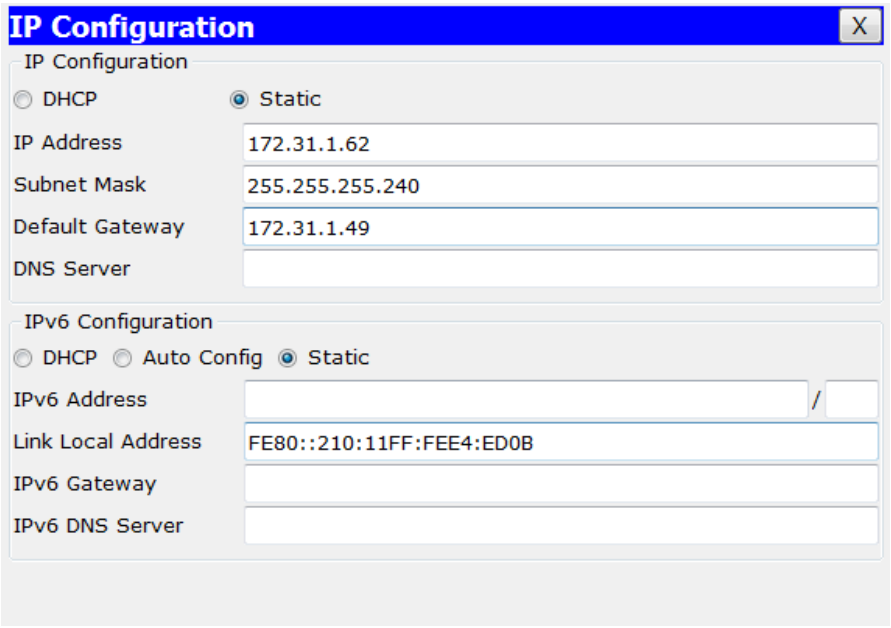
```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip addres 172.31.1.17 255.255.255.240
R2(config-if)#no shutdown
```

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

```
S3(config)#interface vlan 1
S3(config-if)#ip addres 172.31.1.34 255.255.255.240
S3(config-if)#no shutdown
```

```
S3(config)#ip default-gateway 172.31.1.33
S3(config)#
```

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

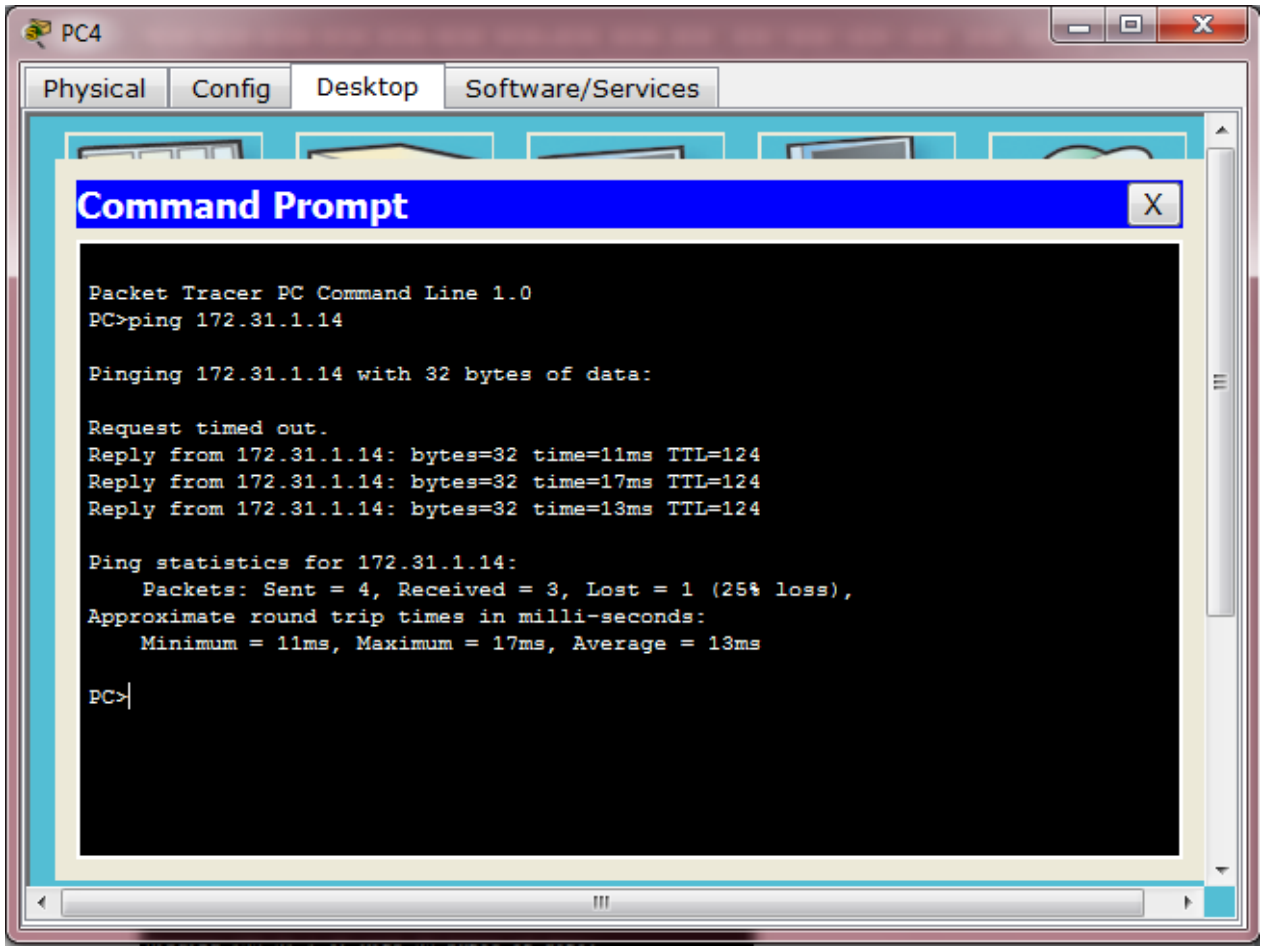


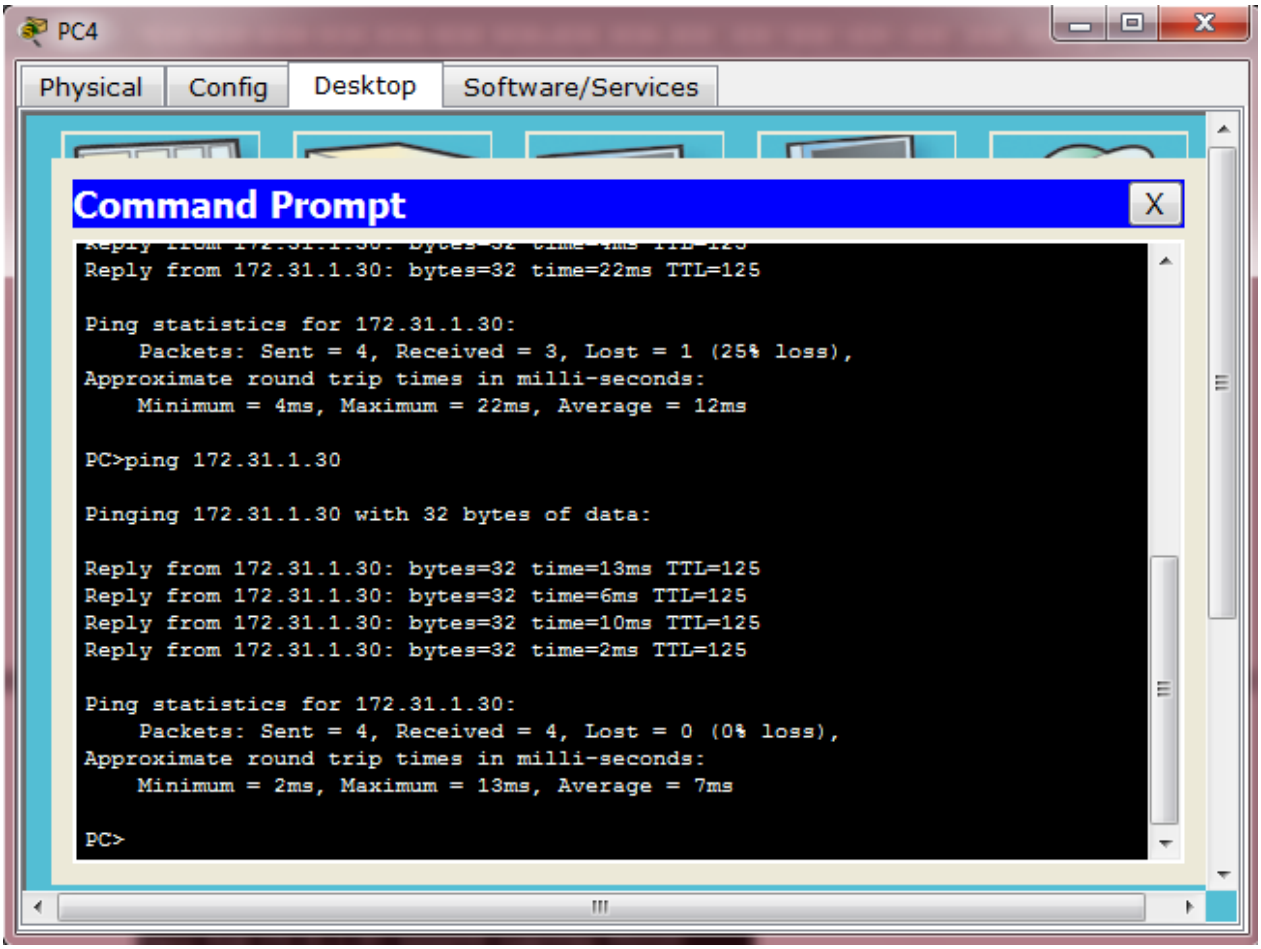
Paso 4: Verifique la conectividad.

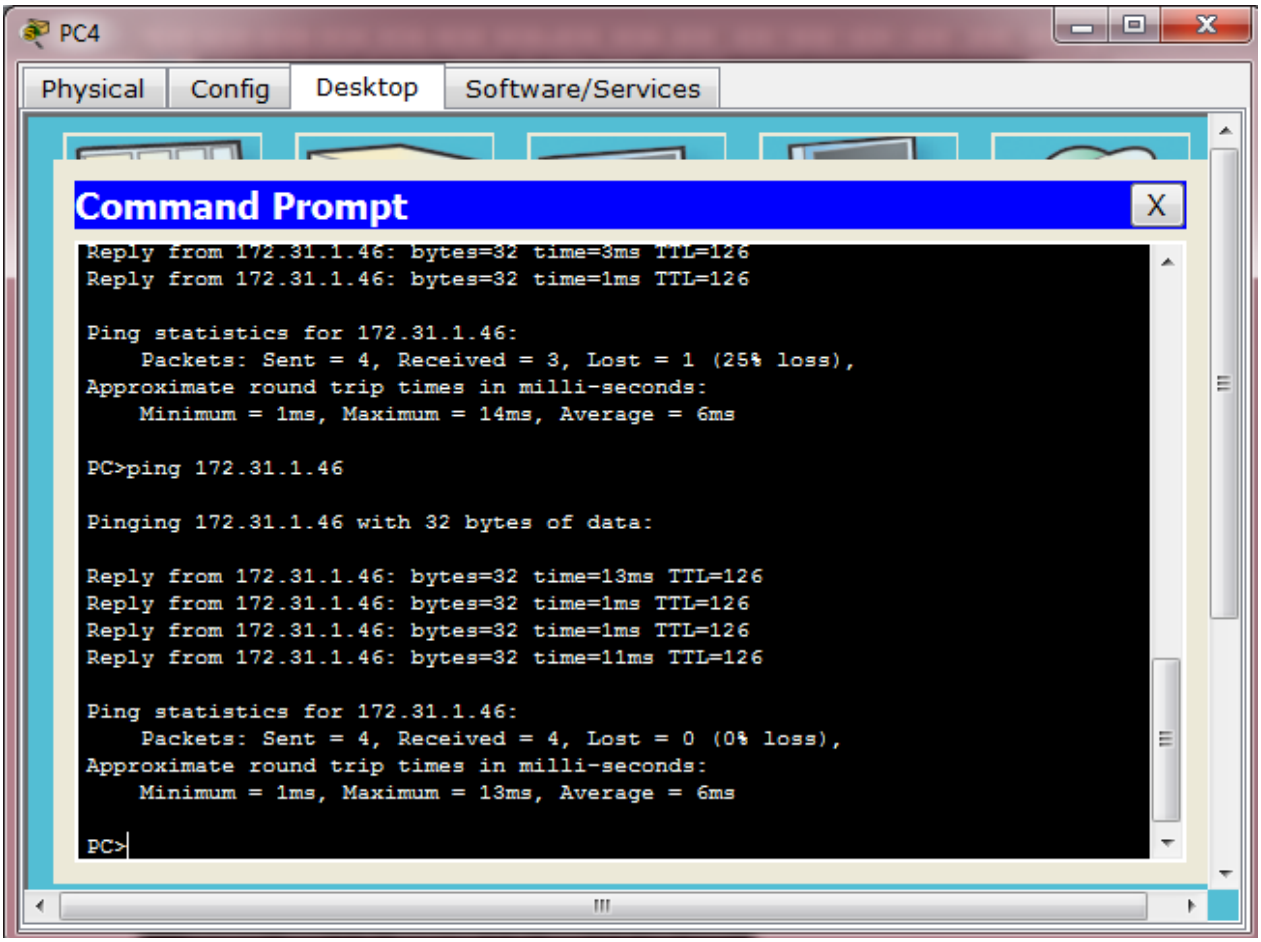
Solo puede verificar la conectividad desde el R1, el R2, el S3 y la PC4. Sin embargo, debería poder hacer ping a cada dirección IP incluida en la **tabla de direccionamiento**.

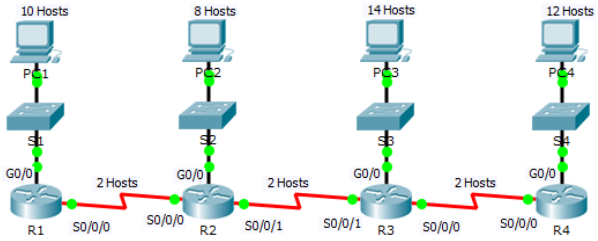
```
R1>ping 172.31.1.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.14, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/5/21 ms

R1>ping 172.31.1.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/5/11 ms

R1>ping 172.31.1.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.46, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 10/11/12 ms

R1>ping 172.31.1.62

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.62, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/8/14 ms

R1>
```

```
R2>ping 172.31.1.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/15 ms

R2>ping 172.31.1.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

R2>ping 172.31.1.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/16 ms

R2>ping 172.31.1.62

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.62, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/13/35 ms

R2>
```


PC4
Physical
Config
Desktop
Software/Services
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=11ms TTL=124
Reply from 172.31.1.14: bytes=32 time=17ms TTL=124
Reply from 172.31.1.14: bytes=32 time=13ms 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 = 11ms, Maximum = 17ms, Average = 13ms
PC>


PC4
Physical
Config
Desktop
Software/Services
Command Prompt
X
Reply from 172.31.1.30: bytes=32 time=22ms 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 = 4ms, Maximum = 22ms, Average = 12ms
PC>ping 172.31.1.30
Pinging 172.31.1.30 with 32 bytes of data:
Reply from 172.31.1.30: bytes=32 time=13ms TTL=125
Reply from 172.31.1.30: bytes=32 time=6ms TTL=125
Reply from 172.31.1.30: bytes=32 time=10ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 7ms
PC>


PC4
Physical
Config
Desktop
Software/Services
Command Prompt
X
Reply from 172.31.1.46: bytes=32 time=3ms 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 = 14ms, Average = 6ms
PC>ping 172.31.1.46
Pinging 172.31.1.46 with 32 bytes of data:
Reply from 172.31.1.46: bytes=32 time=13ms 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
Reply from 172.31.1.46: bytes=32 time=11ms TTL=126
Ping statistics for 172.31.1.46:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 13ms, Average = 6ms
PC>


10 Hosts
8 Hosts
14 Hosts
12 Hosts
PC1
PC2
PC3
PC4
S1
S2
S3
S4
G0/0
2 Hosts
S0/0/0
S0/0/1
R1
R2
R3
R4

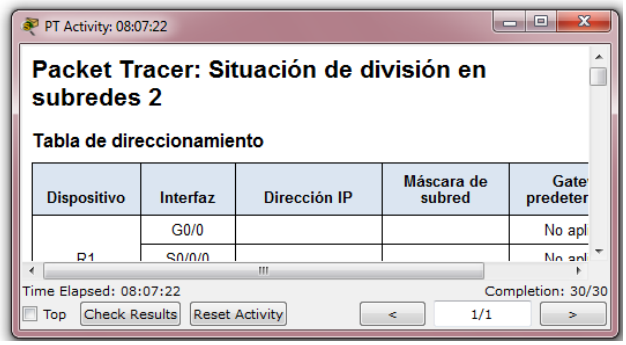

PT Activity: 08:07:22
Packet Tracer: Situación de división en subredes 2
Tabla de direccionamiento
Dispositivo
Interfaz
Dirección IP
Máscara de subred
Gate predeter
G0/0
No apl
Time Elapsed: 08:07:22
Completion: 30/30
Top
Check Results
Reset Activity
1/1

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Diseñar un esquema de direccionamiento IP	Paso 1a	1	
	Paso 1b	1	
	Paso 1c	1	
	Paso 1d	1	
	Paso 1e	4	
	Paso 1f	2	
Completar la tabla de subredes	Paso 1g	10	
Asignar subredes	Paso 2	10	
Documentar el direccionamiento	Paso 3	40	
Total de la parte 1		**70**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

- Práctica muy importante para nuestro desarrollo profesional, ahora entiendo con total seguridad cuál es el proceso que se sigue para encontrar cada uno de los elementos que hacen parte de las tablas de direccionamiento, comprendo la importancia de convertir una determinada dirección IP a su equivalente en binario ya que esta es la forma de encontrar las máscaras de subred, la dirección de red, broadcast, etc…..

Laboratorio 9.2.1.5

Packet Tracer: Diseño e implementación de un esquema de direccionamiento VSLM (versión para el instructor)..

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Recibirá una de tres topologías posibles.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Building1	G0/0	172.31.103.1	255.255.255.224	No aplicable
		172.31.103.33	255.255.255.224	No aplicable
		172.31.103.97	255.255.255.252	No aplicable
Building2	G0/0	172.31.103.65	255.255.255.240	No aplicable
		172.31.103.81	255.255.255.240	No aplicable
		172.31.103.98	255.255.255.252	No aplicable
ASW-1	VLAN 1	172.31.103.2	255.255.255.224	172.31.103.1
ASW-2	VLAN 1	172.31.103.34	255.255.255.224	172.31.103.33
ASW-3	VLAN 1	172.31.103.66	255.255.255.240	172.31.103.65
ASW-4	VLAN 1	172.31.103.82	255.255.255.240	172.31.103.81
Host-A	NIC	172.31.103.30	255.255.255.224	172.31.103.1
Host-B	NIC	172.31.103.62	255.255.255.224	172.31.103.33
Host-C	NIC	172.31.103.78	255.255.255.240	172.31.103.65
Host-D	NIC	172.31.103.94	255.255.255.240	172.31.103.81

Objetivos

- Parte 1: Examinar los requisitos de la red

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

Información básica

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

Parte 1: Examinar los requisitos de la red

Paso 1: Determinar la cantidad de subredes necesarias

Dividirá la dirección de red **172.31.103.0/24** en subredes. La red tiene los siguientes requisitos:

- La LAN de **ASW-1** requerirá **27** direcciones IP de host.
- La LAN de **ASW-2** requerirá **25** direcciones IP de host.
- La LAN de **ASW-3** requerirá **14** direcciones IP de host.
- La LAN de **ASW-4** requerirá **8** direcciones IP de host.

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

5

Paso 2: Determinar la información de máscara de subred para cada subred

a. ¿Qué máscara de subred admitirá la cantidad de direcciones IP requeridas para **ASW-1**?

255.255.255.224

¿Cuántas direcciones de host utilizables admitirá esta subred?

30

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?

30

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

255.255.255.240

¿Cuántas direcciones de host utilizables admitirá esta subred?

14

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

255.255.255.240

¿Cuántas direcciones de host utilizables admitirá esta subred?

14.

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

255.255.255.252 - 2 direcciones.

Parte 2: Diseñar el esquema de direccionamiento VLSM

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

a. Use la primera subred para la LAN más extensa.
172.31.103.0/27 - 255.255.255.224

b. Use la segunda subred para la segunda LAN más extensa.

172.31.103.32/27 - 255.255.255.224

c. Use la tercera subred para la tercera LAN más extensa.

172.31.103.64/28 - 255.255.255.240

d. Use la cuarta subred para la cuarta LAN más extensa.

172.31.103.80/28 - 255.255.255.240

e. Use la quinta subred para admitir la conexión entre **Building1** y **Building2**

172.31.103.96/30 - 255.255.255.252

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

Nota: las respuestas correctas para esta tabla varían según la situación recibida. Consulte las notas para el instructor que se encuentran al final de estas instrucciones para obtener más información. El formato que se usa aquí sigue el utilizado por el estudiante en **Diseño e implementación de un esquema de direccionamiento VLSM**.

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Dirección de broadcast
Host-A	27	172.31.103.0/27	172.31.103.1	172.31.103.31
Host-B	25	172.31.103.32/27	172.31.103.33	172.31.103.63
Host-C	14	172.31.103.64/28	172.31.103.65	172.31.103.79
Host-D	8	172.31.103.80/28	172.31.103.81	172.31.103.95
Enlace WAN	2	172.31.103.96/30	172.31.103.97	172.31.103.99

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.

G0/0: 172.31.103.1 - 255.255.255.224
G0/1: 172.31.103.33 - 255.255.255.224
SO/0/0: 172.31.103.97 - 255.255.255.252

b. Asigne las primeras direcciones IP utilizables a **Building2** para los dos enlaces LAN. Asigne la última
dirección IP utilizable para el enlace WAN.

G0/0: 172.31.103.65 - 255.255.255.240
G0/1: 172.31.103.81 - 255.255.255.240
SO/0/0: 172.31.103.98 - 255.255.255.252

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

ASW-1: 172.31.103.2 - 255.255.255.224
ASW-2: 172.31.103.34 - 255.255.255.224
ASW-3: 172.31.103.66 - 255.255.255.240
ASW-4: 172.31.103.82 - 255.255.255.240

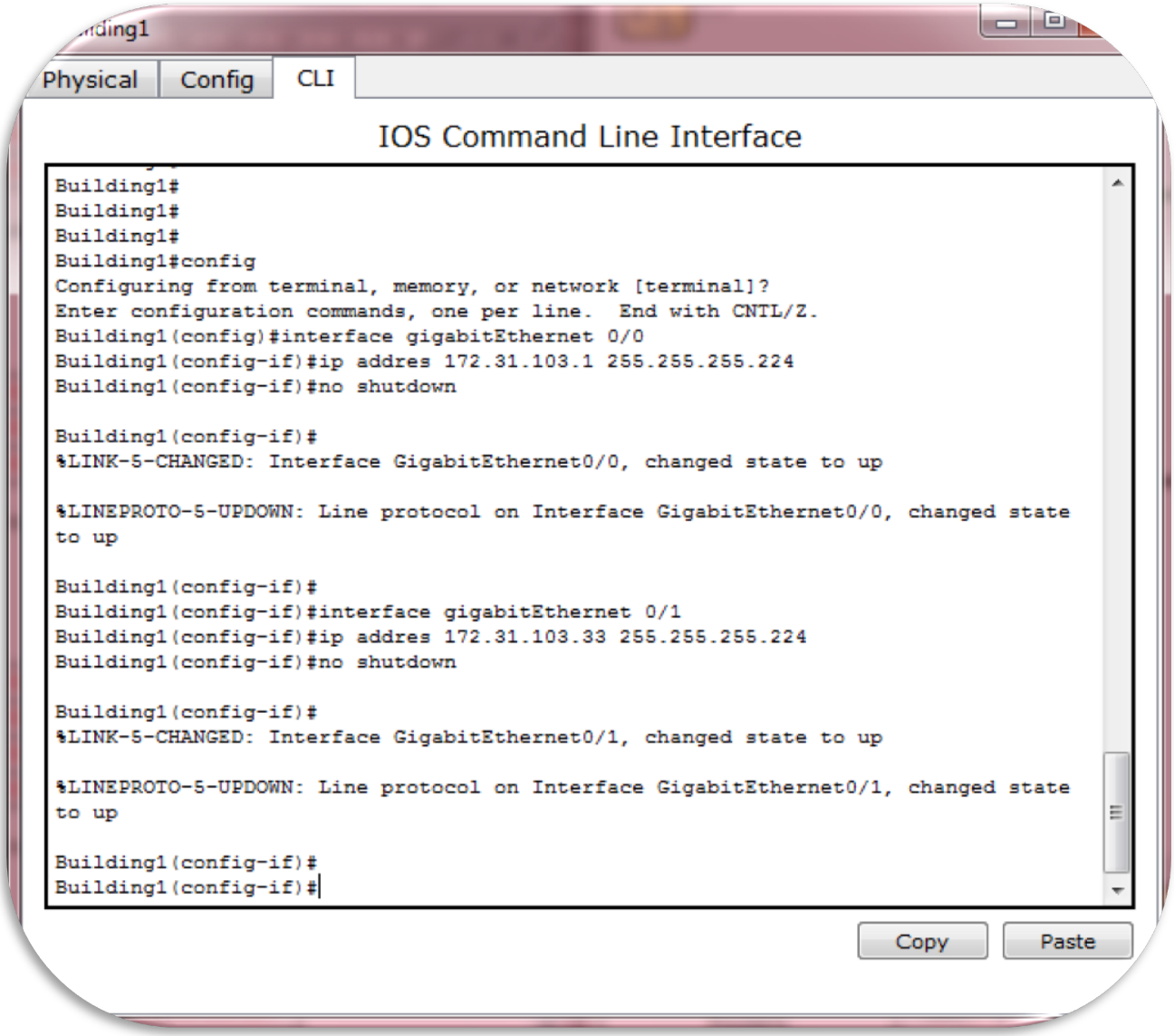
d. Asigne las últimas direcciones IP utilizables a los hosts.

Host-A: 172.31.103.30 - 255.255.255.224
Host-B: 172.31.103.62 - 255.255.255.224
Host-C: 172.31.103.78 - 255.255.255.240
Host-D: 172.31.103.94 - 255.255.255.240

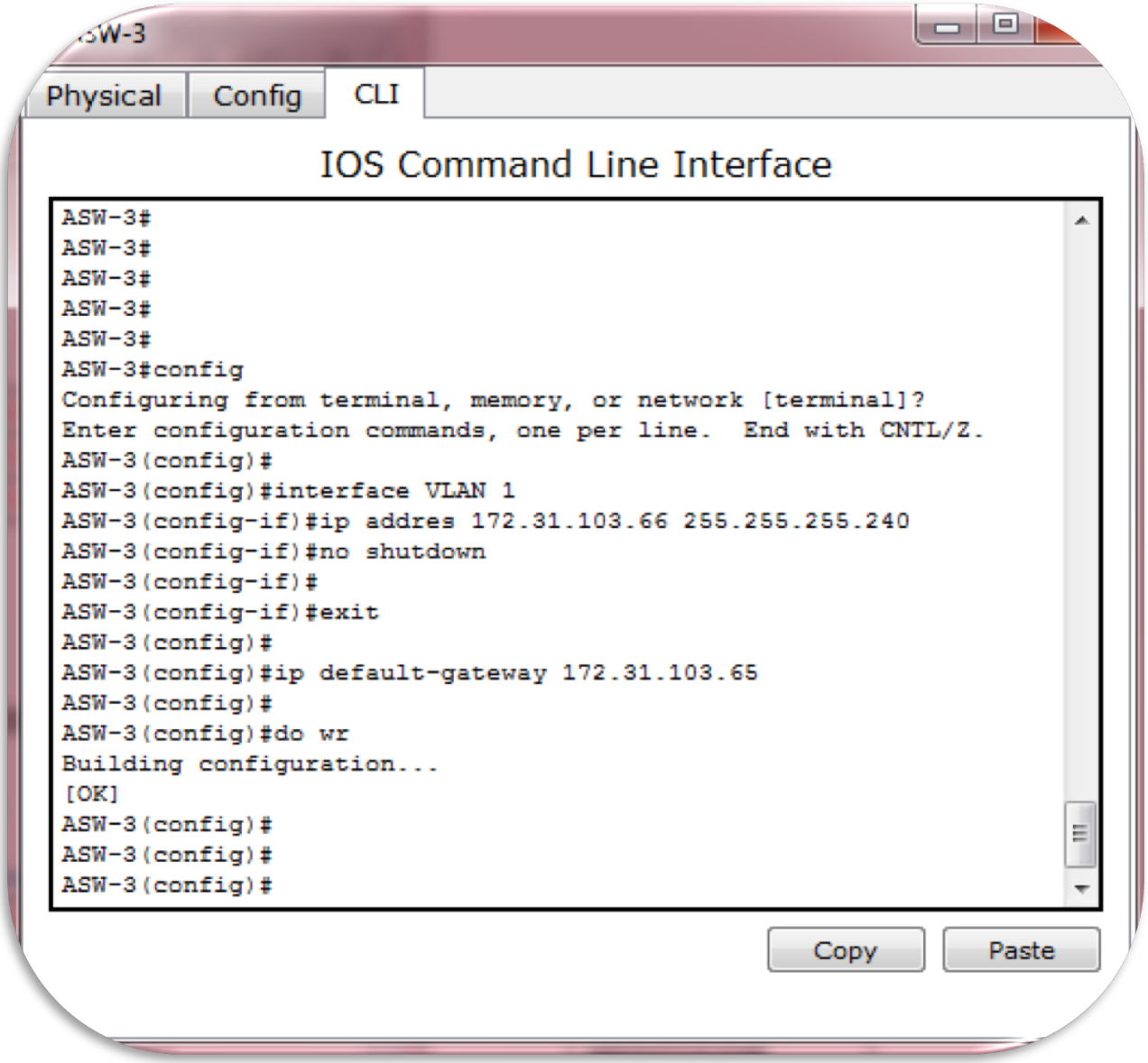
Parte 3: Asignar direcciones IP a los dispositivos y verificar la conectividad

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

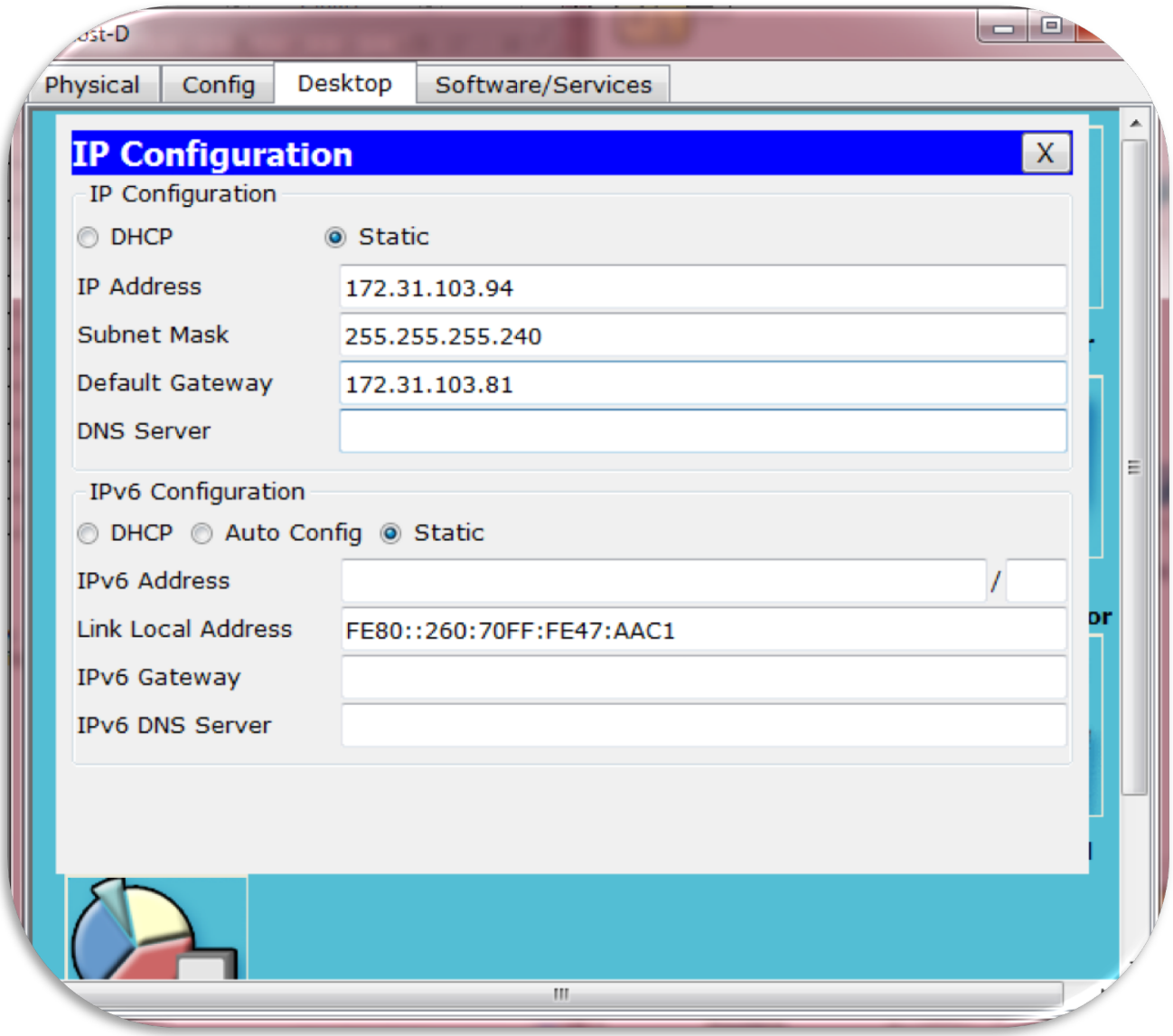
Paso 1: Configurar el direccionamiento IP en las interfaces LAN de **Building1**



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



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



Paso 4: Verifique 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**.

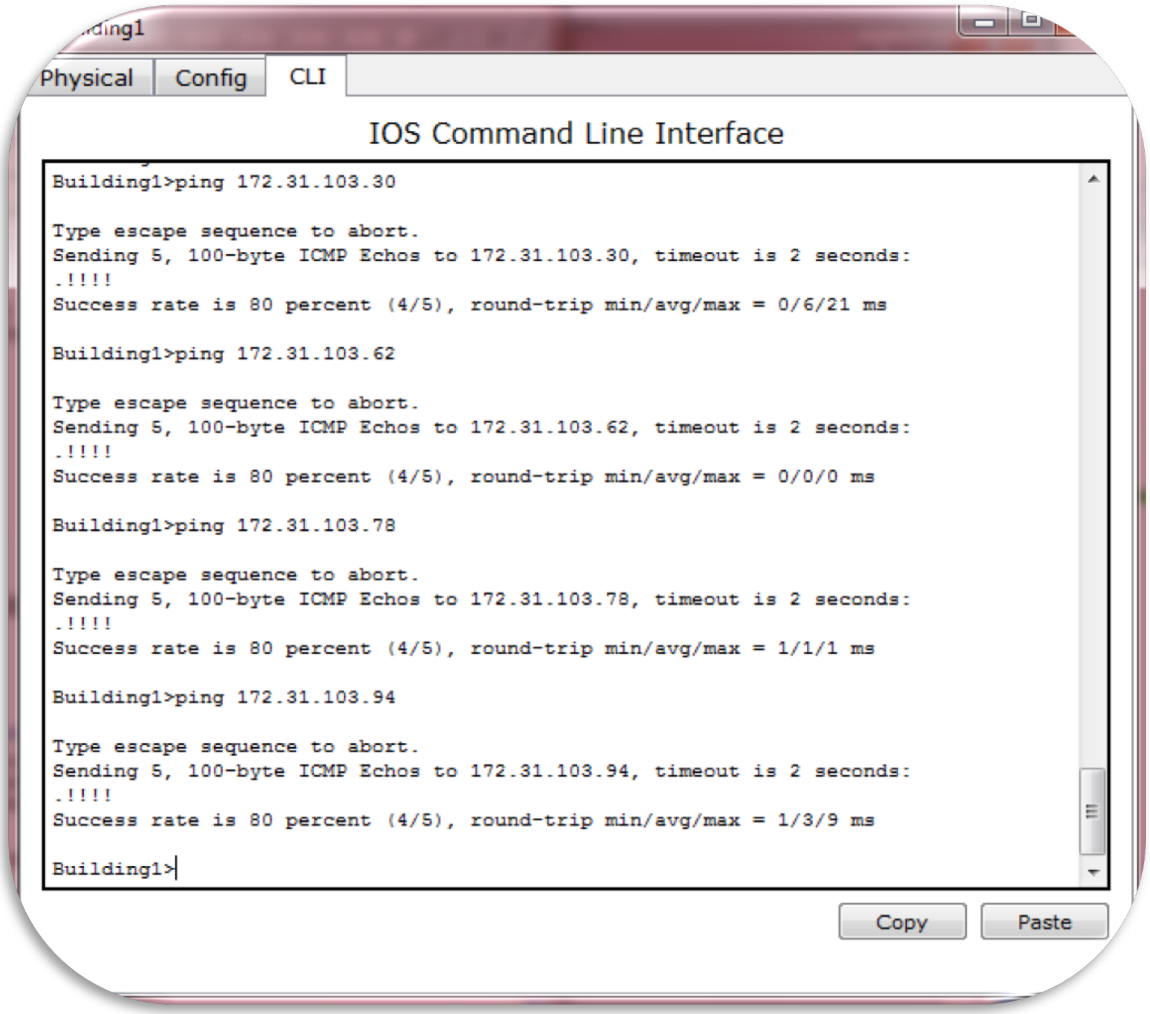

Physical
Config
CLI
IOS Command Line Interface
Building1>ping 172.31.103.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.103.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/6/21 ms
Building1>ping 172.31.103.62
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.103.62, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
Building1>ping 172.31.103.78
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.103.78, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Building1>ping 172.31.103.94
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.103.94, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/9 ms
Building1>
Copy
Paste

Tabla de calificación sugerida

Nota: la mayoría de los puntos se asignan para diseñar y documentar el esquema de direccionamiento. La implementación de las direcciones en Packet Tracer es de mínima consideración.

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Examinar los requisitos de la red	Paso 1	1	
		4	
Total de la parte 1		**5**	
Parte 2: Diseñar el esquema de direccionamiento VLSM			
Completar la tabla de subredes		25	
Documentar el direccionamiento		40	
Total de la parte 2		**65**	
Puntuación de Packet Tracer		**30**	
Puntuación total		**100**	

ID: 100

Notas para el instructor:

Las siguientes tablas de direccionamiento representan las tres situaciones de direccionamiento posibles que puede recibir el estudiante. Observe que la columna Dispositivo es independiente del esquema de direccionamiento. Por ejemplo, un estudiante podría recibir los nombres de dispositivos de la situación 1 y el esquema de direccionamiento de la situación 3. Además, las tres topologías posibles también son independientes de los nombres de los dispositivos y del esquema de direccionamiento (haga clic en Reset [Restablecer] en la actividad para ver las distintas topologías). Por lo tanto, en esta actividad se utilizan tres variables independientes con tres valores posibles cada una, con lo que se obtiene un total de 27 combinaciones posibles. (3 nombres de dispositivos x 3 esquemas de direccionamiento x 3 topologías = 27 isomorfos).

Situación 1: Dirección de red 10.11.48.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN Host-D	60	10.11.48.0/26	10.11.48.1	10.11.48.62	10.11.48.63
LAN Host-B	30	10.11.48.64/27	10.11.48.65	10.11.48.94	10.11.48.95
LAN Host-A	14	10.11.48.96/28	10.11.48.97	10.11.48.110	10.11.48.111
LAN Host-C	6	10.11.48.112/29	10.11.48.113	10.11.48.118	10.11.48.119
Enlace WAN	2	10.11.48.120/30	10.11.48.121	10.11.48.122	10.11.48.123

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Edificiol	GO/0	10.11.48.97	255.255.255.240	No aplicable
		10.11.48.65	255.255.255.224	No aplicable
		10.11.48.121	255.255.255.252	No aplicable
Edificio2	GO/0	10.11.48.113	255.255.255.248	No aplicable
		10.11.48.1	255.255.255.192	No aplicable
		10.11.48.122	255.255.255.252	No aplicable
ASW1	VLAN 1	10.11.48.98	255.255.255.240	10.11.48.97
ASW2	VLAN 1	10.11.48.66	255.255.255.224	10.11.48.65
ASW3	VLAN 1	10.11.48.114	255.255.255.248	10.11.48.113
ASW4	VLAN 1	10.11.48.2	255.255.255.192	10.11.48.1
Host A	NIC	10.11.48.110	255.255.255.240	10.11.48.97
Host B	NIC	10.11.48.94	255.255.255.224	10.11.48.65
Host C	NIC	10.11.48.118	255.255.255.248	10.11.48.113
Host D	NIC	10.11.48.62	255.255.255.192	10.11.48.1

Edificio 1

```
en
conf t int g0/0
ip add 10.11.48.97 255.255.255.240 no shut int g0/1
ip add 10.11.48.65 255.255.255.224 no shut ASW3
en
conf t
int vlan 1
ip add 10.11.48.114 255.255.255.248
no shut
ip def 10.11.48.113
```

ASW3

```
en
conf t
int vlan 1
ip add 10.11.48.114 255.255.255.248
no shut
ip def 10.11.48.113
```

Situación 2: Dirección de red 172.31.103.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
PC-A LAN	27	172.31.103.0/27	172.31.103.1	172.31.103.30	172.31.103.31
PC-B LAN	25	172.31.103.32/27	172.31.103.33	172.31.103.62	172.31.103.63
PC-C LAN	14	172.31.103.64/28	172.31.103.65	172.31.103.78	172.31.103.79
PC-D LAN	8	172.31.103.80/28	172.31.103.81	172.31.103.94	172.31.103.95
Enlace WAN	2	172.31.103.96/30	172.31.103.97	172.31.103.98	172.31.103.99

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Branchl	G0/0	172.31.103.1	255.255.255.224	No aplicable
		172.31.103.33	255.255.255.224	No aplicable
		172.31.103.97	255.255.255.252	No aplicable
Branch2	G0/0	172.31.103.65	255.255.255.240	No aplicable
		172.31.103.81	255.255.255.240	No aplicable
		172.31.103.98	255.255.255.252	No aplicable
Sala 114	VLAN 1	172.31.103.2	255.255.255.224	172.31.103.1
Sala 279	VLAN 1	172.31.103.34	255.255.255.224	172.31.103.33
Sala 312	VLAN 1	172.31.103.66	255.255.255.240	172.31.103.65
Sala 407	VLAN 1	172.31.103.82	255.255.255.240	172.31.103.81
PC-A	NIC	172.31.103.30	255.255.255.224	172.31.103.1
PC-B	NIC	172.31.103.62	255.255.255.224	172.31.103.33
PC-C	NIC	172.31.103.78	255.255.255.240	172.31.103.65
PC-D	NIC	172.31.103.94	255.255.255.240	172.31.103.81

Sucursal 1

```
en
conf t
```

int g0/0

ip add 172.31.103.1 255.255.255.224

no shut

int g0/1

ip add 172.31.103.33 255.255.255.224 no shut Sala 312 en

conf t int vlan 1

ip add 172.31.103.66 255.255.255.240 no shut ip def 172.31.103.65

Sala 312

en

conf t

int vlan 1

ip add 172.31.103.66 255.255.255.240

no shut

ip def 172.31.103.65

Situación 3: Dirección de red 192.168.72.0/24

Tabla de subredes

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN User-4	58	192.168.72.0/26	192.168.72.1	192.168.72.62	192.168.72.63
LAN User-3	29	192.168.72.64/27	192.168.72.65	192.168.72.94	192.168.72.95
LAN User-2	15	192.168.72.96/27	192.168.72.97	192.168.72.126	192.168.72.127
LAN User-1	7	192.168.72.128/28	192.168.72.129	192.168.72.142	192.168.72.143
Enlace WAN	2	192.168.72.144/30	192.168.72.145	192.168.72.146	192.168.72.147

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
Sitio remoto 1	G0/0	192.168.72.129	255.255.255.240	No aplicable
		192.168.72.97	255.255.255.224	No aplicable
		192.168.72.145	255.255.255.252	No aplicable
Sitio remoto 2	G0/0	192.168.72.65	255.255.255.224	No aplicable
	G0/1	192.168.72.1	255.255.255.192	No aplicable
	SO/0/0	192.168.72.146	255.255.255.252	No aplicable
Sw1	VLAN 1	192.168.72.130	255.255.255.240	192.168.72.129
Sw2	VLAN 1	192.168.72.98	255.255.255.224	192.168.72.97
Sw3	VLAN 1	192.168.72.66	255.255.255.224	192.168.72.65
Sw4	VLAN 1	192.168.72.2	255.255.255.192	192.168.72.1
Usuario 1	NIC	192.168.72.142	255.255.255.240	192.168.72.129
Usuario 2	NIC	192.168.72.126	255.255.255.224	192.168.72.97
Usuario 3	NIC	192.168.72.94	255.255.255.224	192.168.72.65
Usuario 4	NIC	192.168.72.62	255.255.255.192	192.168.72.1

Sitio remoto 1

```
en
conf t
```

```
int g0/0
ip add 192.168.72.129 255.255.255.240
no shut
int g0/1
ip add 192.168.72.97 255.255.255.224 no shut Sw-3
en
conf t
int vlan 1
ip add 192.168.72.66 255.255.255.224
no shut
ip def 192.168.72.65
```

Sw-3

```
en
conf t
int vlan 1
ip add 192.168.72.66 255.255.255.224
no shut
ip def 192.168.72.65
```

Laboratorio 9.3.1.4

Packet Tracer: Implementación de un esquema de direccionamiento IPv6 dividido en subredes (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

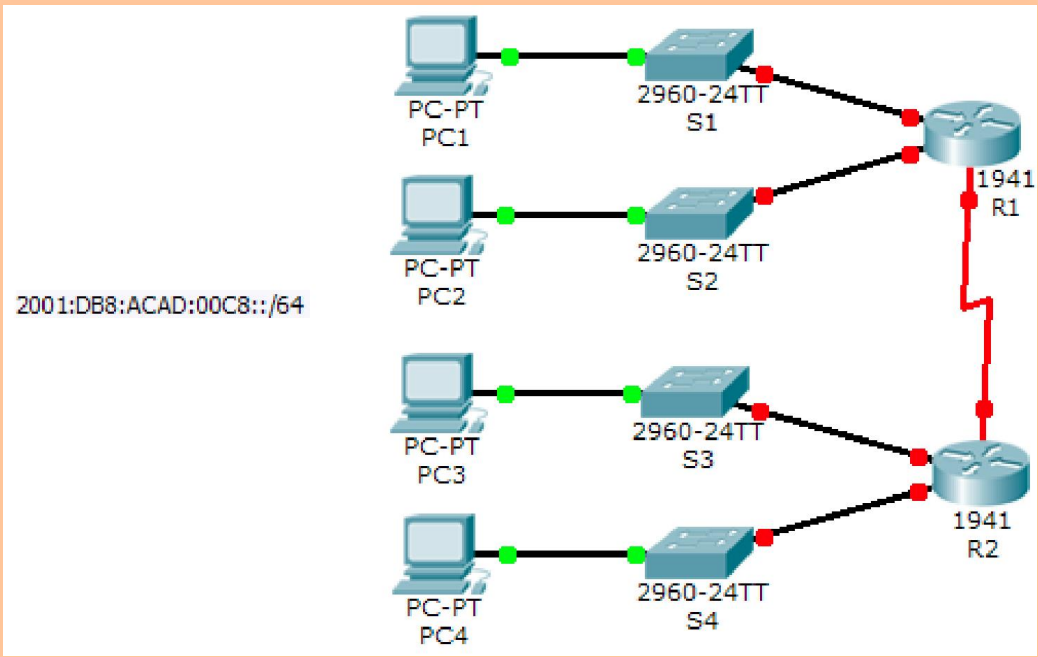


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Link-Local

R1	G0/0	2001:DB8:ACAD:00C8::1/64	FE80::1
		2001:DB8:ACAD:00C9::1/64	FE80::1
		2001:DB8:ACAD:00CC::1/64	FE80::1
R2	G0/0	2001:DB8:ACAD:00CA::1/64	FE80::2
		2001:DB8:ACAD:00CB::1/64	FE80::2
		2001:DB8:ACAD:00CC::2/64	FE80::2
PC1	NIC	Configuración automática	
PC2	NIC	Configuración automática	
PC3	NIC	Configuración automática	
PC4	NIC	Configuración automática	

Objetivos

- Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6
- Parte 2: Configurar el direccionamiento IPv6 en los routers y las PC, y verificar la conectividad

Situación

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

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

Paso 1: Determinar la cantidad de subredes necesarias

Comience con la subred IPv6 2001:DB8: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:DB8: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::0/64
R1 G0/1 LAN	2001:DB8:ACAD:00C9::0/64
R2 G0/0 LAN	2001:DB8:ACAD:00CA::0/64
R2 G0/1 LAN	2001:DB8:ACAD:00CB::0/64
Enlace WAN	2001:DB8:ACAD:00CC::0/64

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.

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**.

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
```

- **Configuración router 1.**

```
R1(config)#interface g0/0
R1(config-if)#ipv6 addres 2001:DB8:ACAD:00C8::1/64
R1(config-if)#ipv6 addres fe80::1 link-local
R1(config-if)#no shutdown

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

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

R1(config-if)#interface g0/1
R1(config-if)#ipv6 addres 2001:DB8:ACAD:00C9::1/64
R1(config-if)#ipv6 addres fe80::1 link-local
R1(config-if)#no shutdown

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

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

R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 addres 2001:DB8:ACAD:00CC::1/64
R1(config-if)#ipv6 addres fe80::1 link-local
R1(config-if)#no shutdown

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

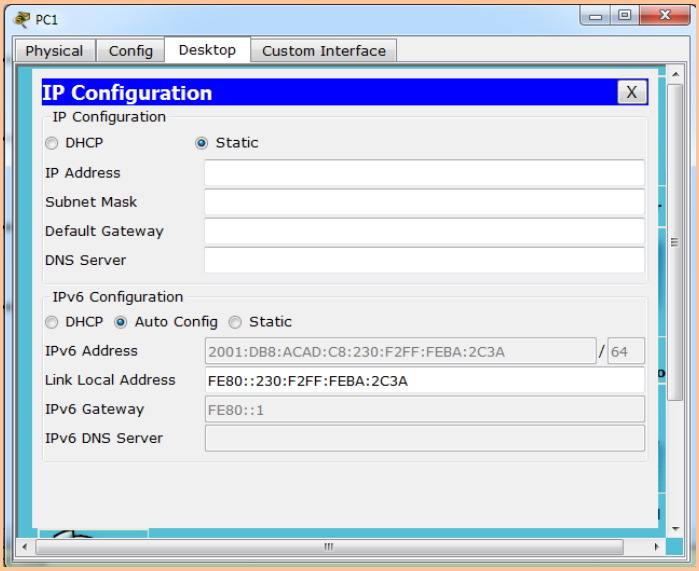
- **Configuración router 2.**

```
R2(config)#interface g0/0
R2(config-if)#ipv6 addres 2001:DB8:ACAD:00CA::1/64
R2(config-if)#ipv6 addres FE80::2 link-local
R2(config-if)#no shutdown

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

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

R2(config-if)#interface g0/1
R2(config-if)#ipv6 addres 2001:DB8:ACAD:00CB::1/64
R2(config-if)#ipv6 addres FE80::2 link-local
R2(config-if)#no shutdown

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

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

R2(config-if)#interface S0/0/0
R2(config-if)#ipv6 addres 2001:DB8:ACAD:00CC::2/64
R2(config-if)#ipv6 addres FE80::2 link-local
R2(config-if)#no shutdown

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

R2(config-if)#do wr
```

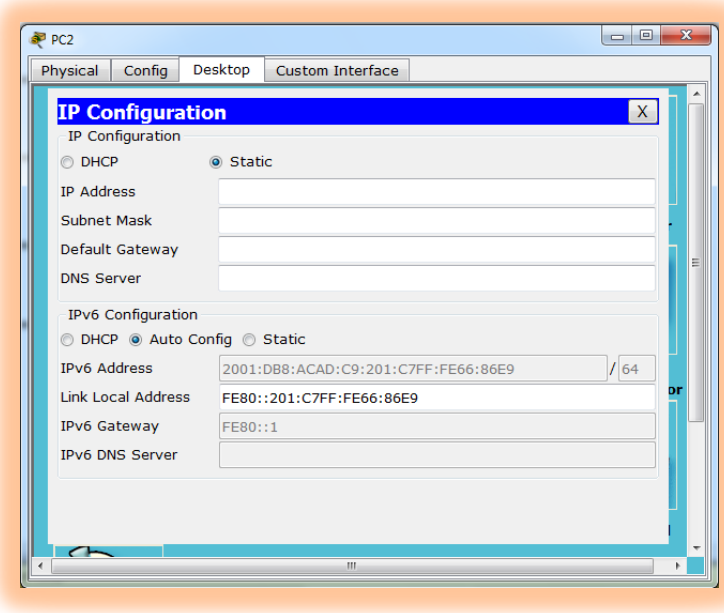
Paso 2: Configurar las PC para que reciban el direccionamiento IPv6 automáticamente

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

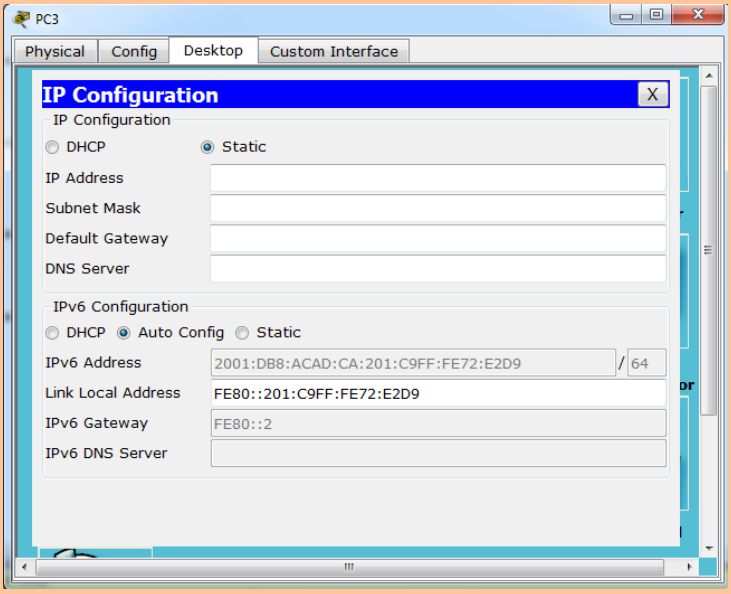
- PC1.


PC1
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:C8:230:F2FF:FEBA:2C3A
/ 64
Link Local Address
FE80::230:F2FF:FEBA:2C3A
IPv6 Gateway
FE80::1
IPv6 DNS Server

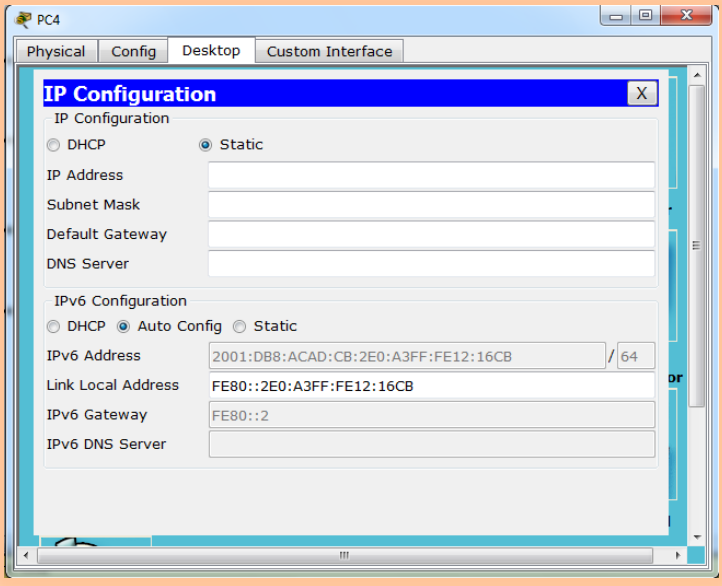
- PC2


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
FE80::1
IPv6 DNS Server

- PC3



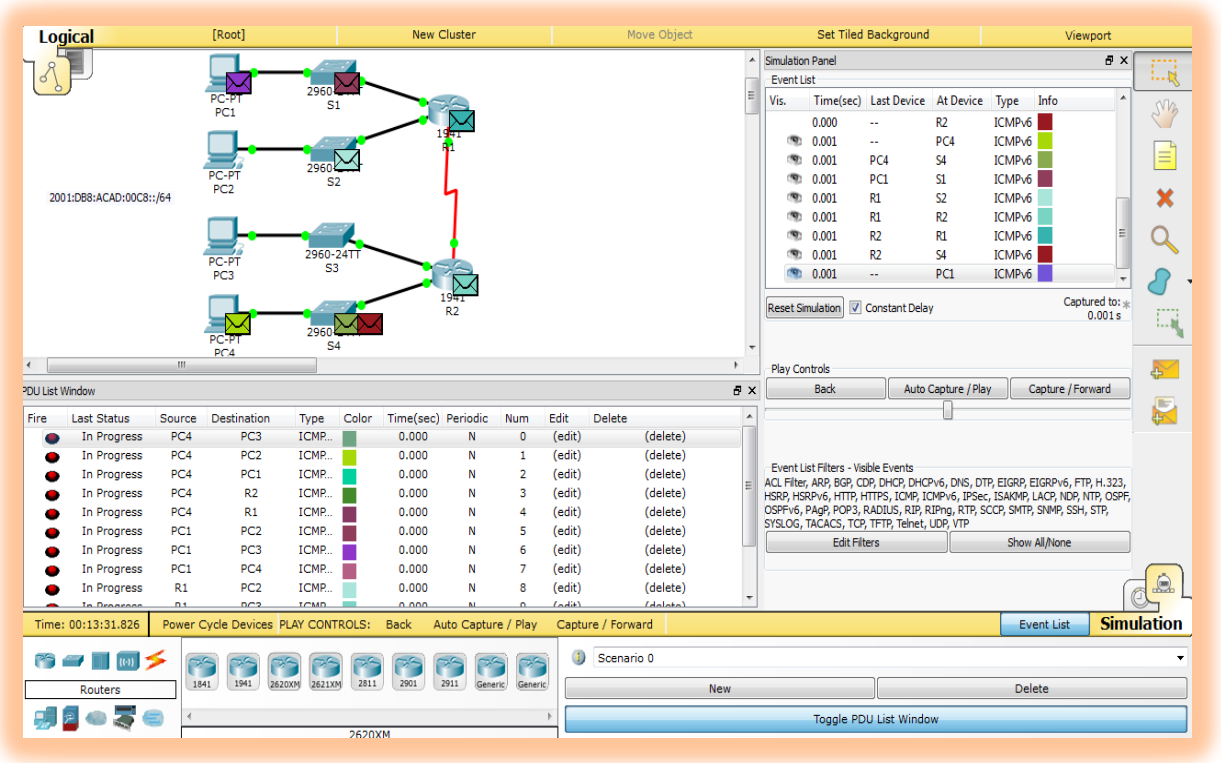
- PC4



Paso 3: Verificar la conectividad entre las PC

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

- Esta prueba la voy a realizar empleando el simulador con el fin de poder demostrar el estado de configuración tanto de lo Pc como de las interfaces de los routers..



	Successful	PC4	PC3	ICMP...		0.000	N	0	(edit)
	Successful	PC4	PC2	ICMP...		0.000	N	1	(edit)
	Successful	PC4	PC1	ICMP...		0.000	N	2	(edit)
	Successful	PC4	R2	ICMP...		0.000	N	3	(edit)
	Successful	PC4	R1	ICMP...		0.000	N	4	(edit)
	Successful	PC1	PC2	ICMP...		0.000	N	5	(edit)
	Successful	PC1	PC3	ICMP...		0.000	N	6	(edit)
	Successful	PC1	PC4	ICMP...		0.000	N	7	(edit)
	Successful	R1	PC2	ICMP...		0.000	N	8	(edit)
	Successful	R1	PC3	ICMP...		0.000	N	9	(edit)
	Successful	R2	PC1	ICMP...		0.000	N	10	(edit)
	Successful	R2	PC4	ICMP...		0.000	N	11	(edit)

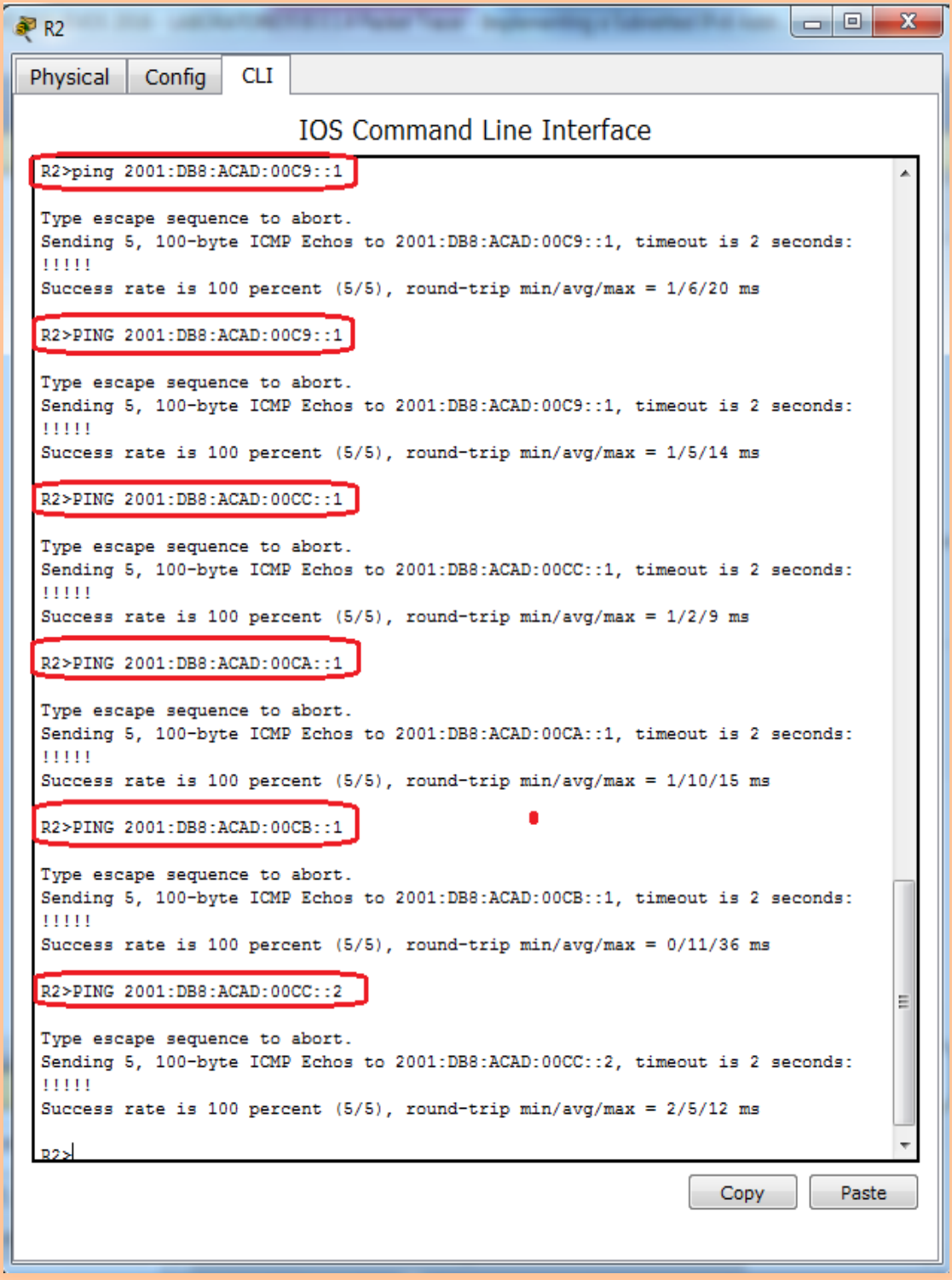
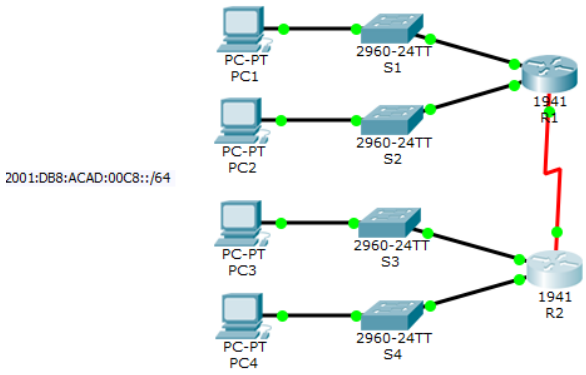
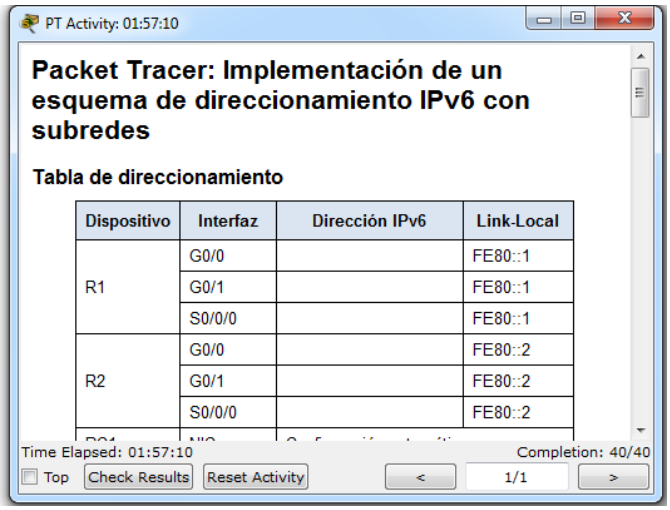

R2
Physical
Config
CLI
IOS Command Line Interface
R2>ping 2001:DB8:ACAD:00C9::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00C9::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
R2>PING 2001:DB8:ACAD:00C9::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00C9::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/14 ms
R2>PING 2001:DB8:ACAD:00CC::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00CC::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
R2>PING 2001:DB8:ACAD:00CA::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00CA::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/15 ms
R2>PING 2001:DB8:ACAD:00CB::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00CB::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/11/36 ms
R2>PING 2001:DB8:ACAD:00CC::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:00CC::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/12 ms
R2>
Copy
Paste

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Determinar las subredes y el esquema de direccionamiento IPv6	Tabla de subredes	30	
		30	
Total de la parte 1		**60**	
Puntuación de Packet Tracer		**40**	
Puntuación total		**100**	





Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Fee
GigabitEthernet0/1				
IPv6 Addresses				
2001:DB8:ACAD:...				
IP Address	Correct	3	IPv6 Host Add...	
Prefix Len...	Correct	1	IPv6 Host Add...	
Link Local	Correct	1	Ip	
Port Status	Correct	1	Device Interfa...	
Serial0/0/0				
IPv6 Addresses				
2001:DB8:ACAD:...				
IP Address	Correct	3	IPv6 Host Add...	
Prefix Len...	Correct	1	IPv6 Host Add...	
Link Local	Correct	1	Ip	
Port Status	Correct	1	Device Interfa...	
R2				
Ports				
GigabitEthernet0/0				
IPv6 Addresses				
2001:DB8:ACAD:...				
IP Address	Correct	3	IPv6 Host Add...	
Prefix Len...	Correct	1	IPv6 Host Add...	
Link Local	Correct	1	Ip	
Port Status	Correct	1	Device Interfa...	
GigabitEthernet0/1				
IPv6 Addresses				
2001:DB8:ACAD:...				
IP Address	Correct	3	IPv6 Host Add...	
Prefix Len...	Correct	1	IPv6 Host Add...	

Score : 40/40
Item Count : 28/28

Component	Items/Total	Score
Device Interface Configuration	6/6	6/6
IPv6 Address Configuration	4/4	4/4
IPv6 Host Address Calculation	12/12	24/24
Ip	6/6	6/6

Laboratorio 9.4.1.2

Packet Tracer: Reto de habilidades de integración (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

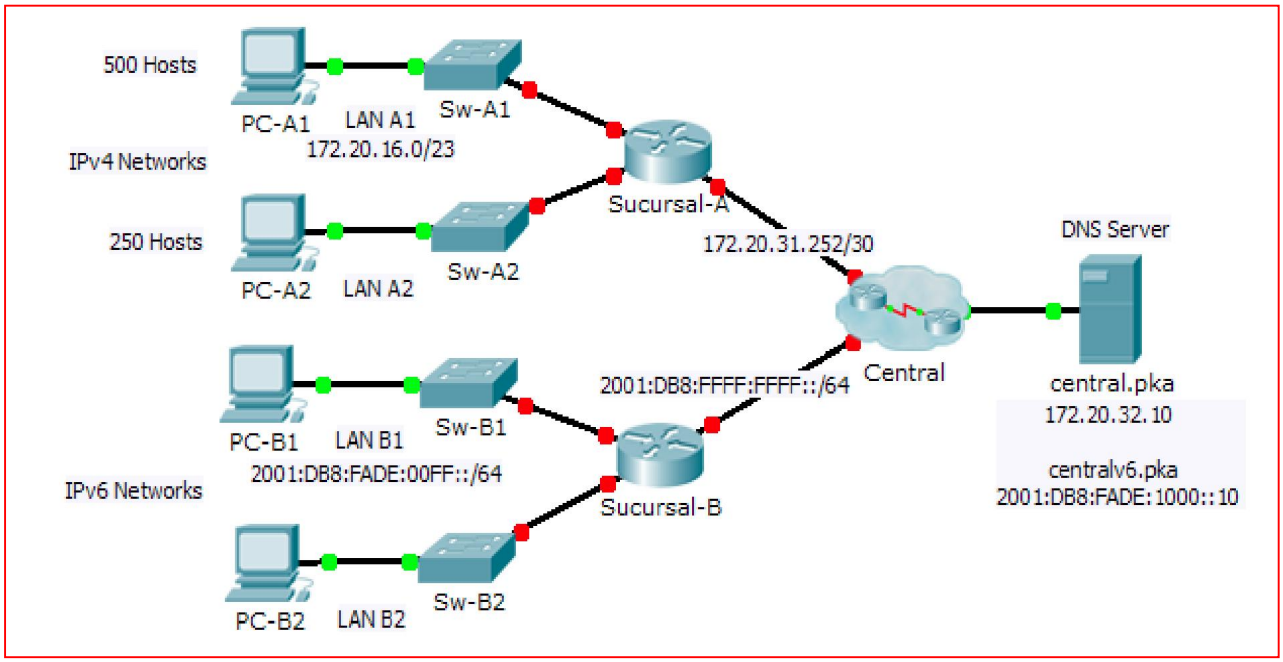


Tabla de direccionamiento

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.

```
Sucursal-A#config
Sucursal-A(config)#hostname Sucursal-A
Sucursal-A(config)#banner motd & WARNING &
Sucursal-A(config)#line console 0
Sucursal-A(config-line)#password cisco
Sucursal-A(config-line)#login
Sucursal-A(config-line)#exit
Sucursal-A(config)#enable secret class
Sucursal-A(config)#service password-encryption
Sucursal-A(config)#
```

```
Router(config)#hostname Sucursal-B
Sucursal-B(config)#banner motd &WARNING&
Sucursal-B(config)#line console 0
Sucursal-B(config-line)#password cisco
Sucursal-B(config-line)#login
Sucursal-B(config-line)#line vty 0 5
Sucursal-B(config-line)#password cisco
Sucursal-B(config-line)#login
Sucursal-B(config-line)#exit
Sucursal-B(config)#enable secret class
Sucursal-B(config)#service password-encryption
Sucursal-B(config)#
```

- 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.

	RED.	PRIMER IP	ULTIMA IP	BROADCAST
A1 500	172.20.16.0/23	172.20.16.1/23	172.20.17.254/23	172.20.17.255/23
A2 250	172.20.18.0/24	172.20.18.1/24	172.20.18.254/24	172.20.18.255/24

- LAN A2: 172.20.18.0/24 - 255.255.255.0

- LAN B1 utiliza la subred 2001:DB8:FADE:00FF::/64. Asigne la siguiente subred disponible a la B2 de LAN.

BI	2001:DB8:FADE:00FF::/64	2001	DB8	FADE	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
B2	2001:DB8:FADE:0100::/64	2001	DB8	FADE	0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

- LAN B2: 2001:DB8:FADE:0100::/64

- 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.

A1 500	G0/0	172.20.16.1	255.255.254.0
A2 250	G0/1	172.20.18.1	255.255.255.0

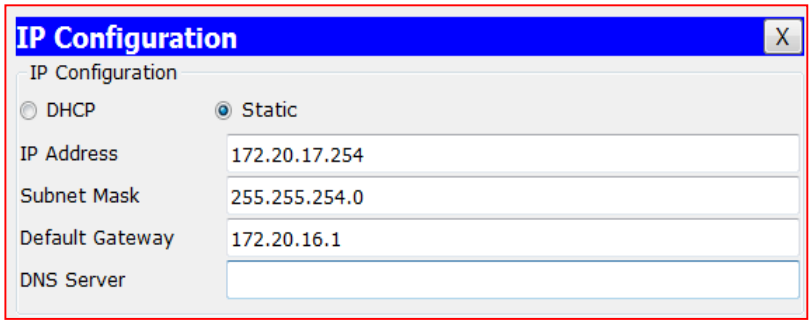
```
Sucursal-A#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Sucursal-A(config)#interface g0/0
Sucursal-A(config-if)#ip addres 172.20.16.1 255.255.254.0
Sucursal-A(config-if)#no shutdown
Sucursal-A(config-if)#interface g0/1
Sucursal-A(config-if)#ip addres 172.20.18.1 255.255.255.0
Sucursal-A(config-if)#no shutdown
Sucursal-A(config-if)#interface g0/2
Sucursal-A(config-if)#ip addres 172.20.31.254 255.255.255.252
Sucursal-A(config-if)#no shutdown
Sucursal-A(config-if)#
```

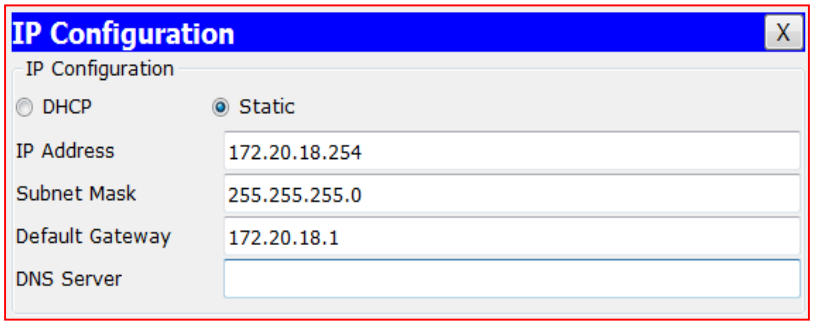
BI	G0/0	2001 :DB8:FADE:00FF::1/64
B2	G0/1	2001:DB8:FADE:0100::1/64

```
Sucursal-B#
Sucursal-B#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Sucursal-B(config)#interface g0/0
Sucursal-B(config-if)#ipv6 address 2001:DB8:FADE:00FF::1/64
Sucursal-B(config-if)#ipv6 address FE80::B link-local
Sucursal-B(config-if)#no shutdown
Sucursal-B(config-if)#interface g0/1
Sucursal-B(config-if)#ipv6 address 2001:DB8:FADE:0100::1/64
Sucursal-B(config-if)#ipv6 address FE80::B link-local
Sucursal-B(config-if)#no shutdown
Sucursal-B(config-if)#interface g0/2
Sucursal-B(config-if)#ipv6 address 2001:DB8:FFFF:FFFF::2/64
Sucursal-B(config-if)#ipv6 address FE80::B link-local
Sucursal-B(config-if)#no shutdown

Sucursal-B(config-if)#
```

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

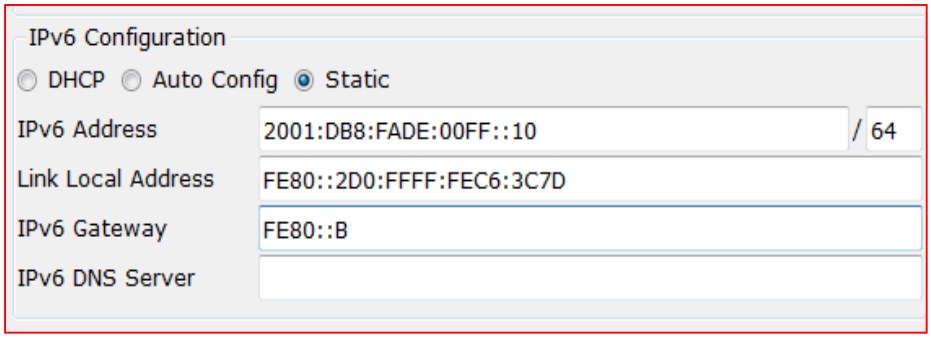
PC-A1	172.20.17.254	255.255.254.0	172.20.16.1
PC-A2	172.20.18.254	255.255.255.0	172.20.18.1

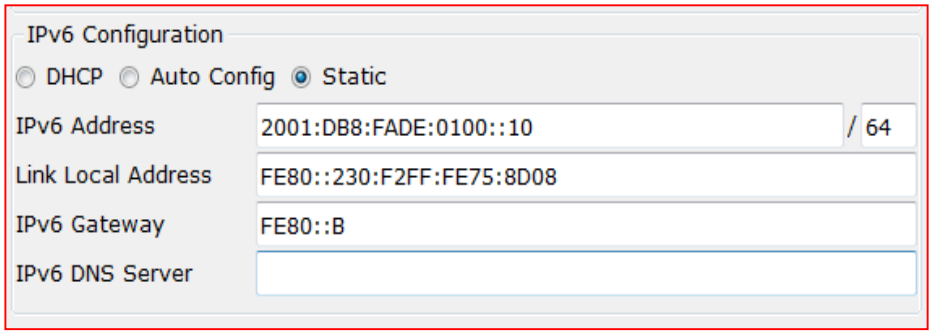




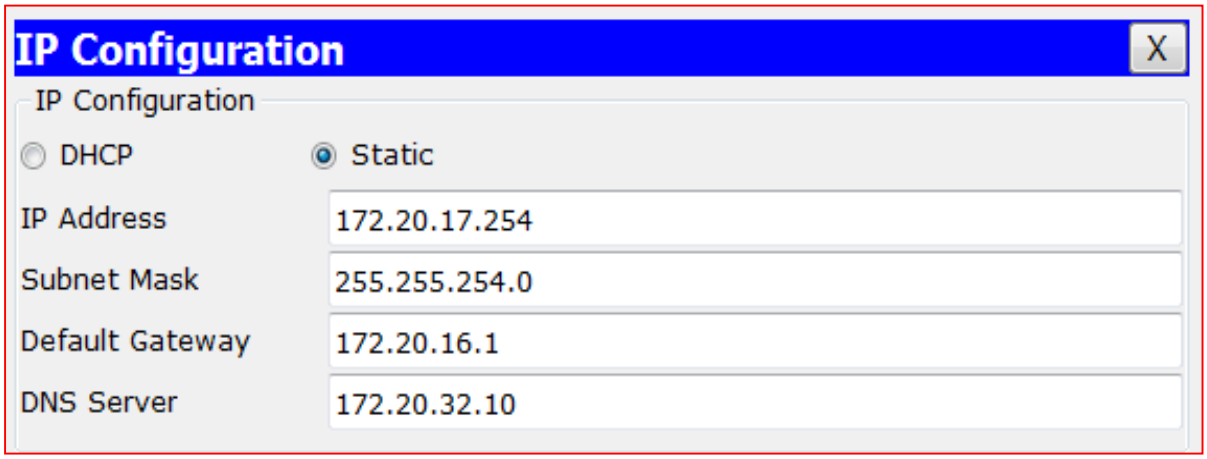
- Para las redes IPv6, asigne la 16.ª dirección IPv6 a las PC.

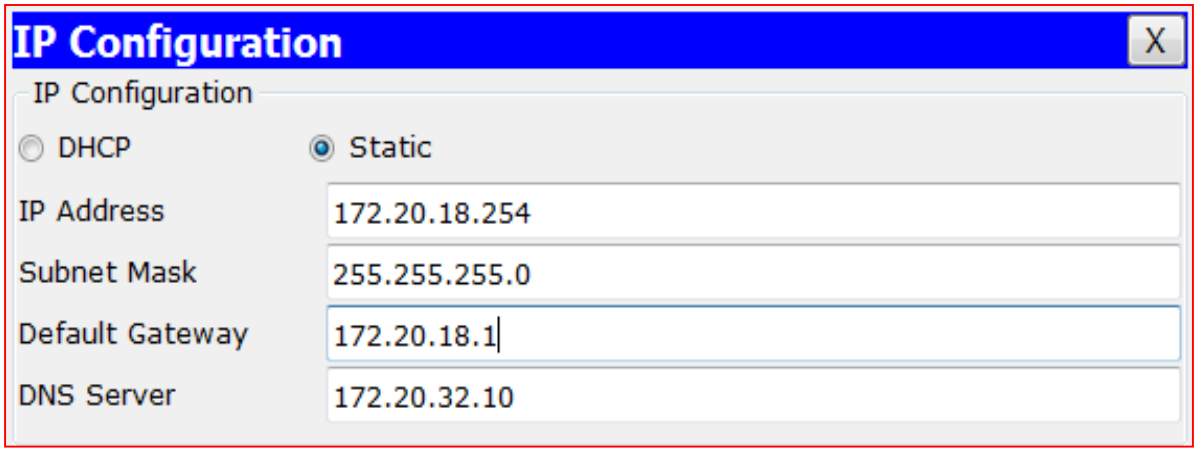
PC-B1	2001:DB8:FADE:00FF::10/64	FE80::B
PC-B2	2001:DB8:FADE:0100::10/64	FE80::B

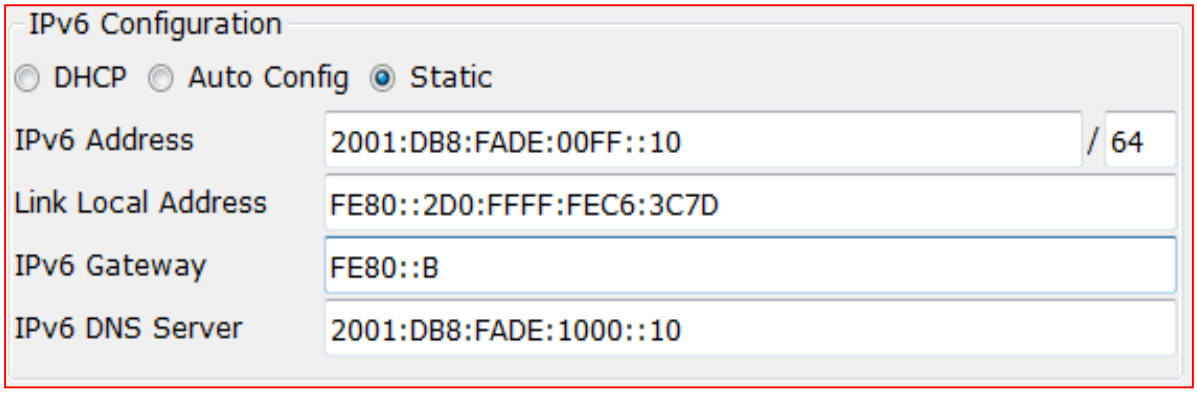


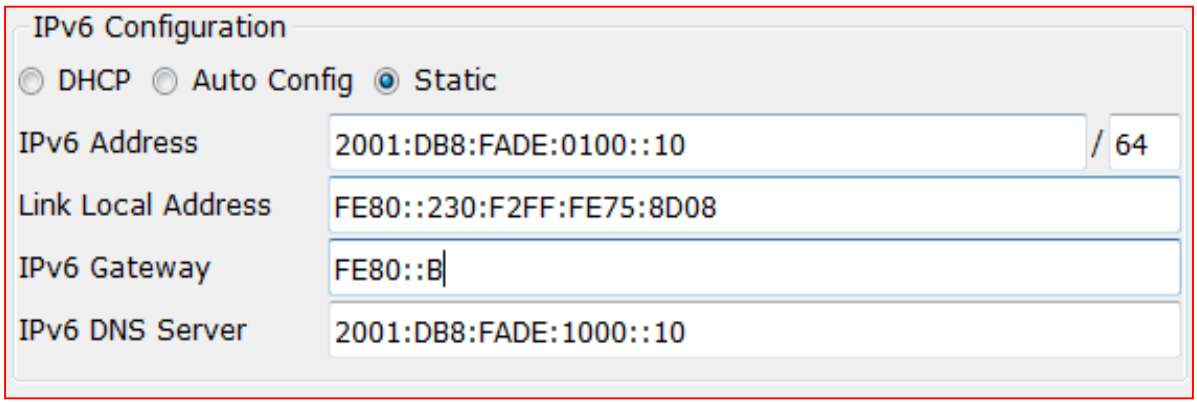


- Configure el direccionamiento de los routers según los registros. Incluya una descripción adecuada para cada interfaz del router. **Sucursal-B** utiliza FE80::B como dirección link-local.
- Configure el direccionamiento de las PC según los registros. Las direcciones del servidor DNS para IPv4 e IPv6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

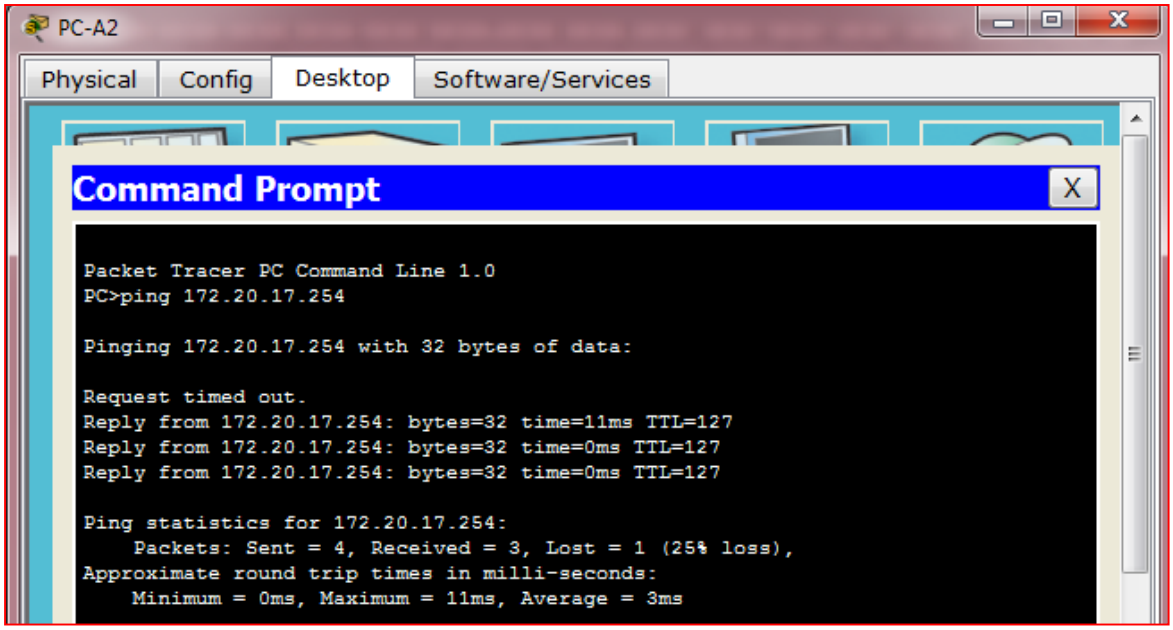


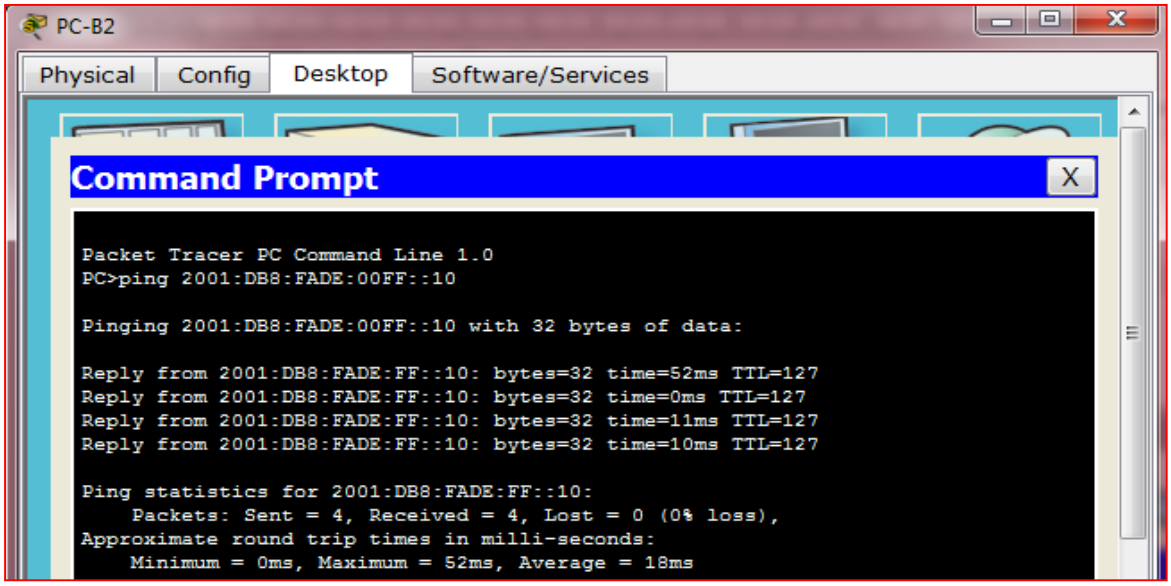




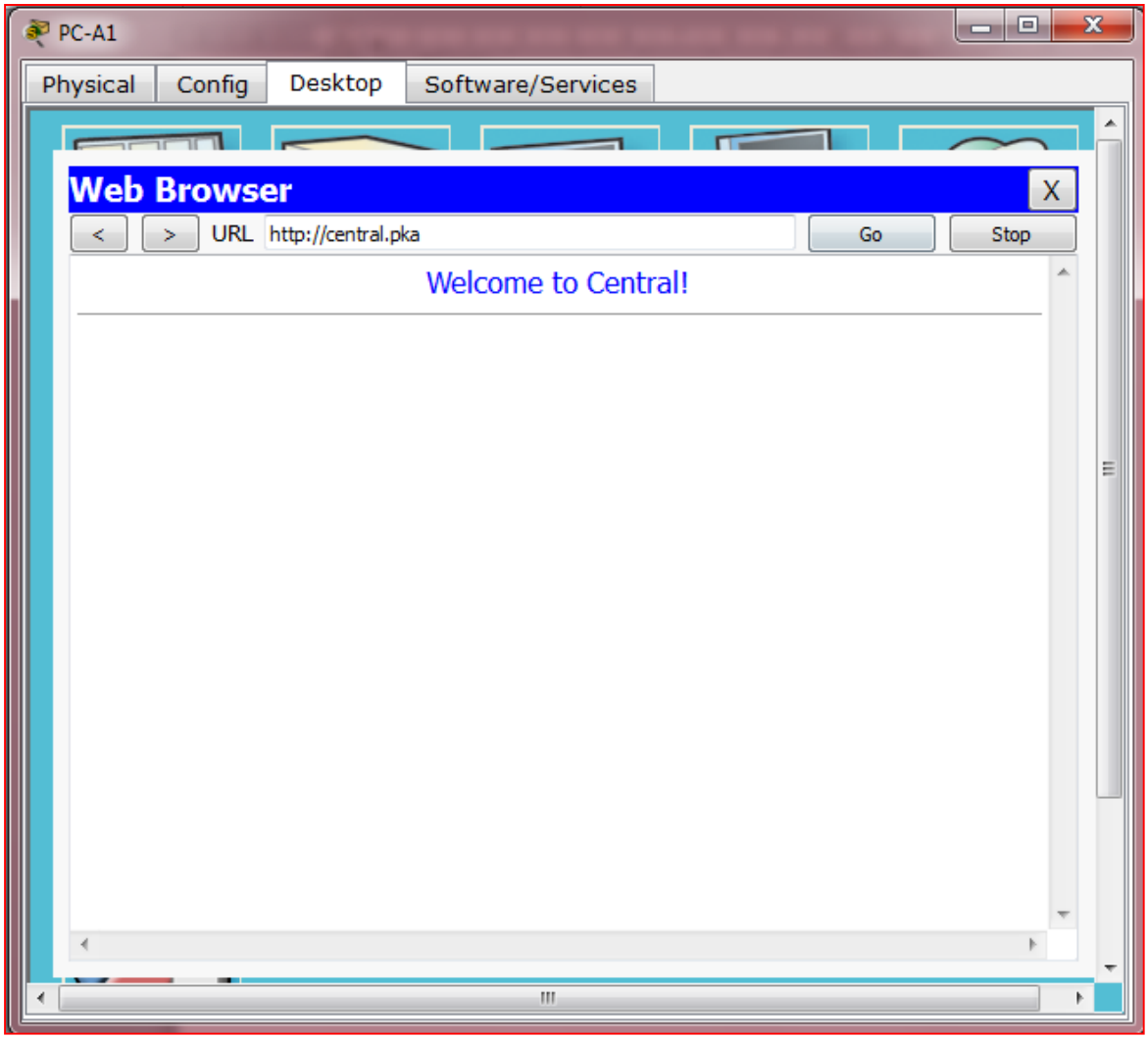


- Verifique la conectividad entre las PC IPv4 y entre las PC IPv6.





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


PC-A1
Physical
Config
Desktop
Software/Services
Web Browser
X
URL
http://central.pka
Go
Stop
Welcome to Central!

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

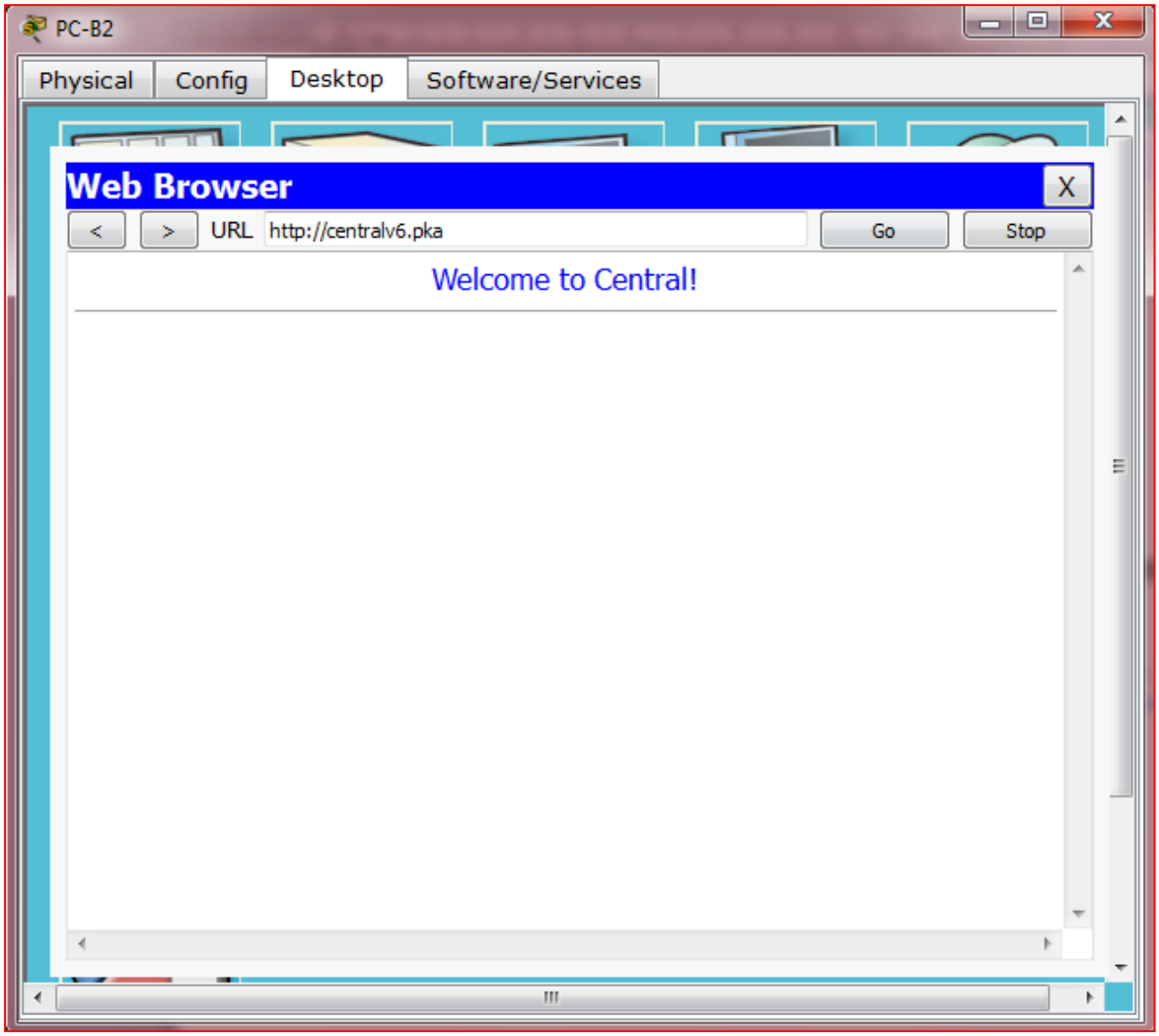
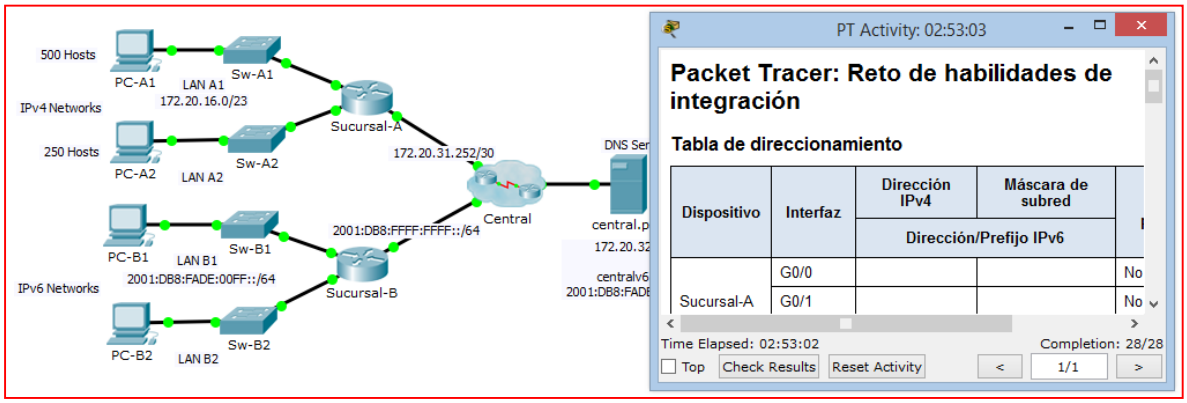
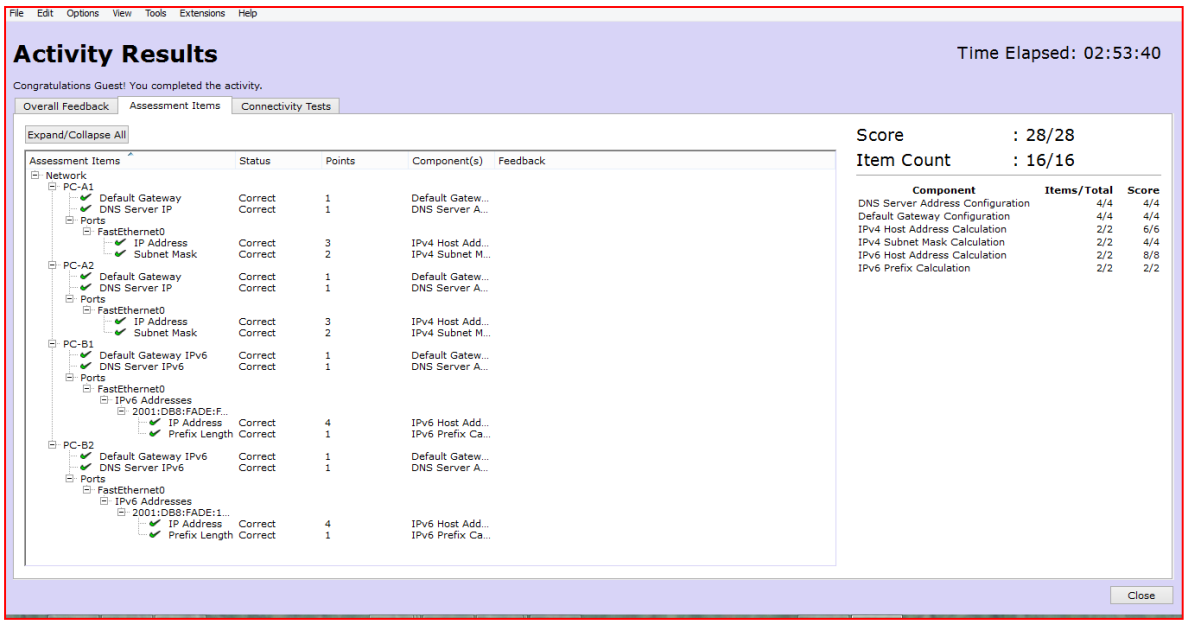


Tabla de calificación sugerida

Sección de la actividad	Posibles puntos	Puntos obtenidos
Registro de la tabla de direccionamiento	25	
Puntuación de Packet Tracer	75	
Puntuación total	100	



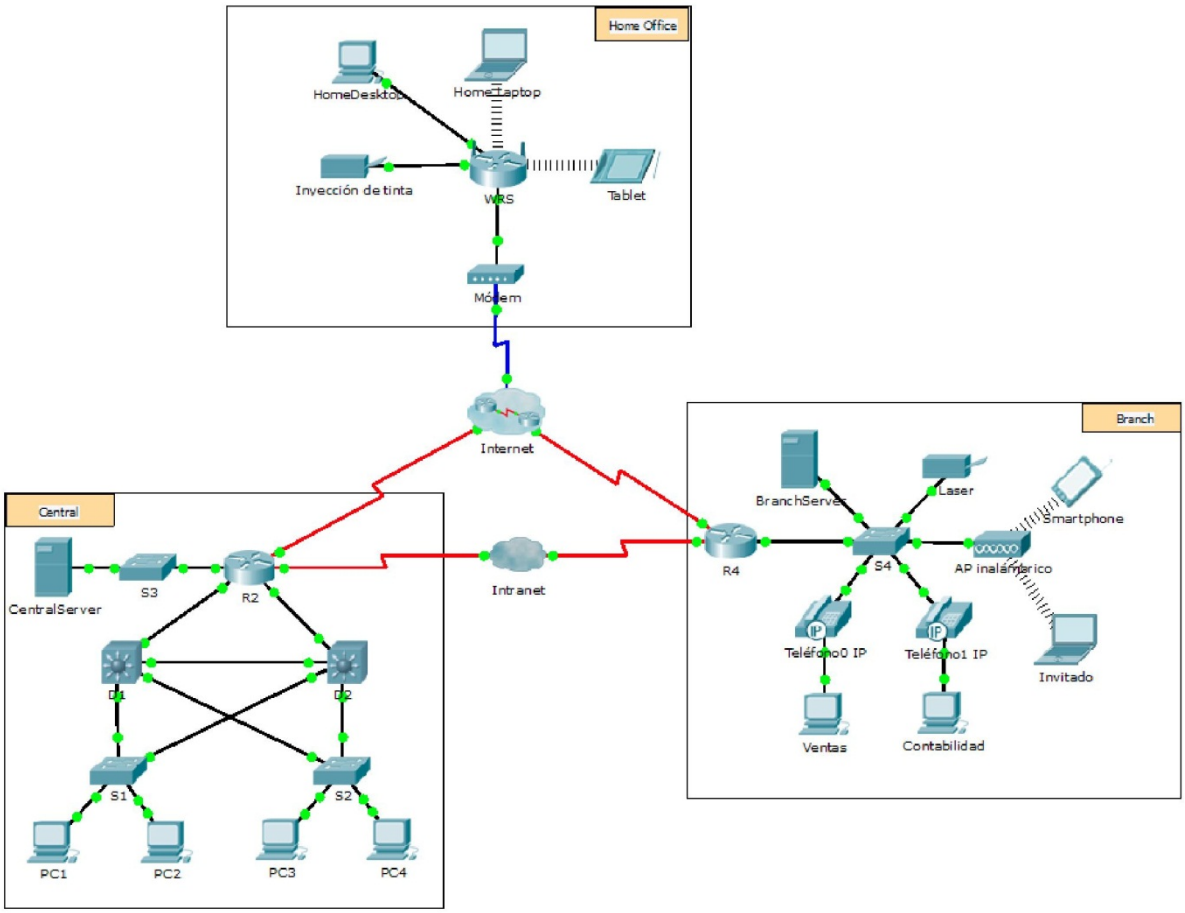


Laboratorio 10.2.1.8

Packet Tracer: Servidores Web y de correo electrónico (version para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

- Parte 1: Configurar y verificar los servicios Web
- Parte 2: Configurar y verificar los servicios de correo electrónico

Información básica

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

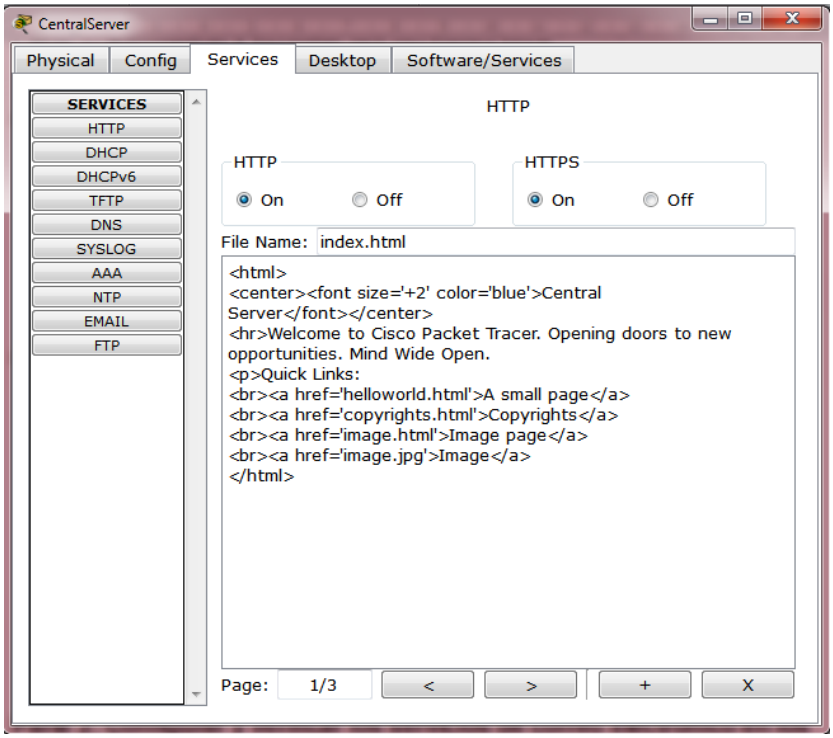
Nota: Packet Tracer simula solamente el proceso para configurar estos servicios. Cada paquete de software de HTTP y de correo electrónico tiene sus propias instrucciones exclusivas de configuración e instalación.

Parte 1: Configurar y verificar los servicios Web

Paso 1: Configurar servicios Web en CentralServer y BranchServer

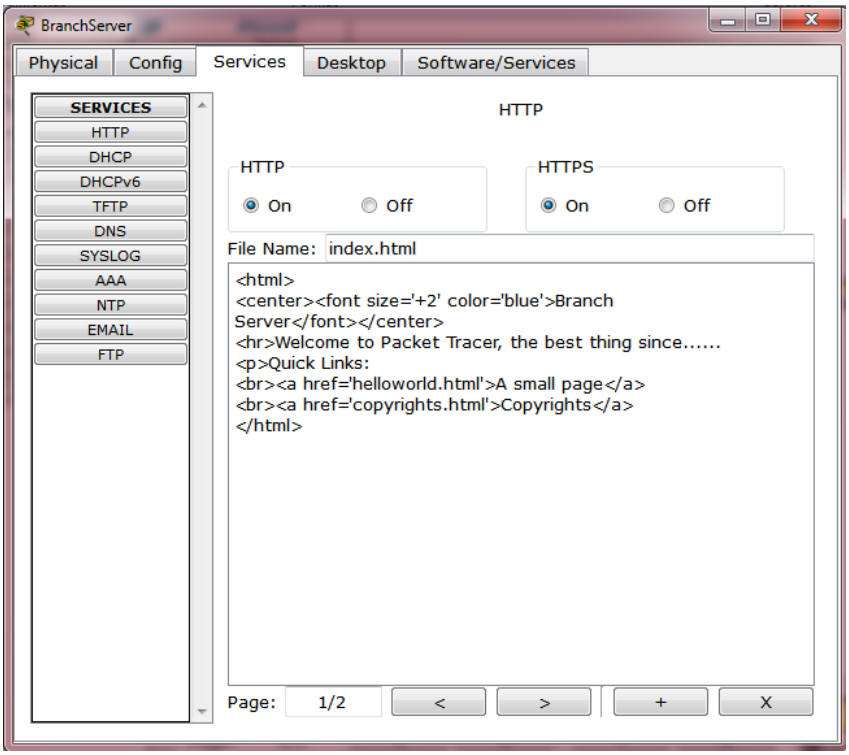
a. Haga clic en **CentralServer** y, a continuación, haga clic en la ficha **Config** > **HTTP**.

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



c. Optativo: personalice el código HTML.

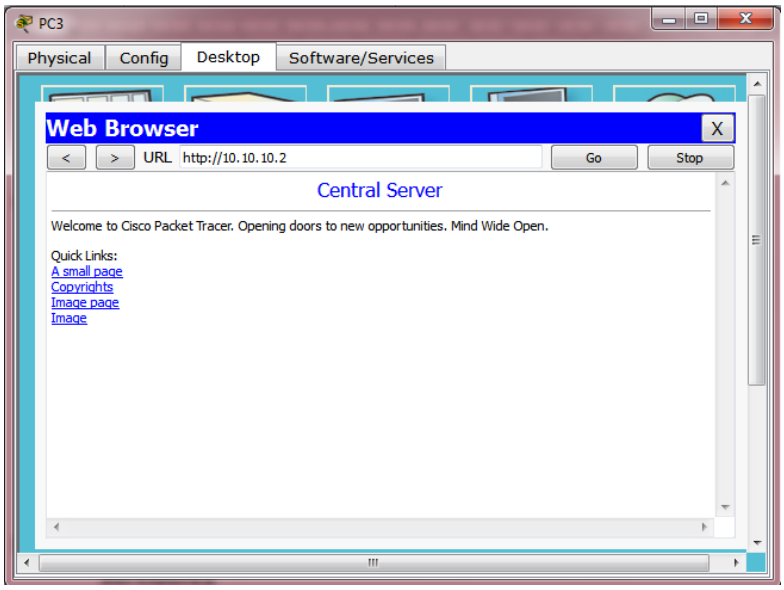
d. Repita desde el paso 1a hasta el paso 1c en **BranchServer**.



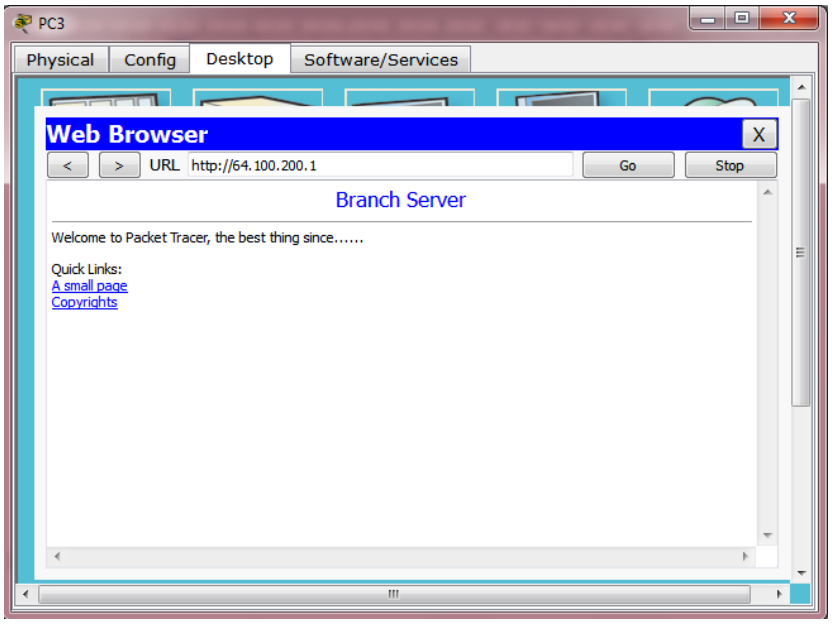
Paso 2: Verificar los servidores Web mediante el acceso a las páginas Web Existen muchos dispositivos terminales en esta red, pero para este paso, use **PC3**.

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

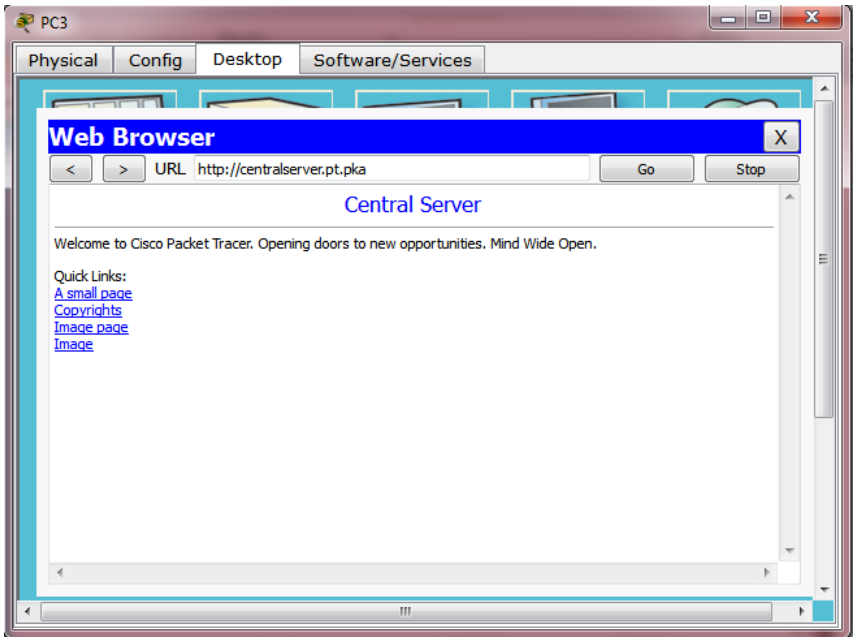
b. En el cuadro de dirección URL, introduzca **10.10.10.2** como dirección IP y haga clic en **Go** (Ir). Aparece el sitio Web de **CentralServer**.



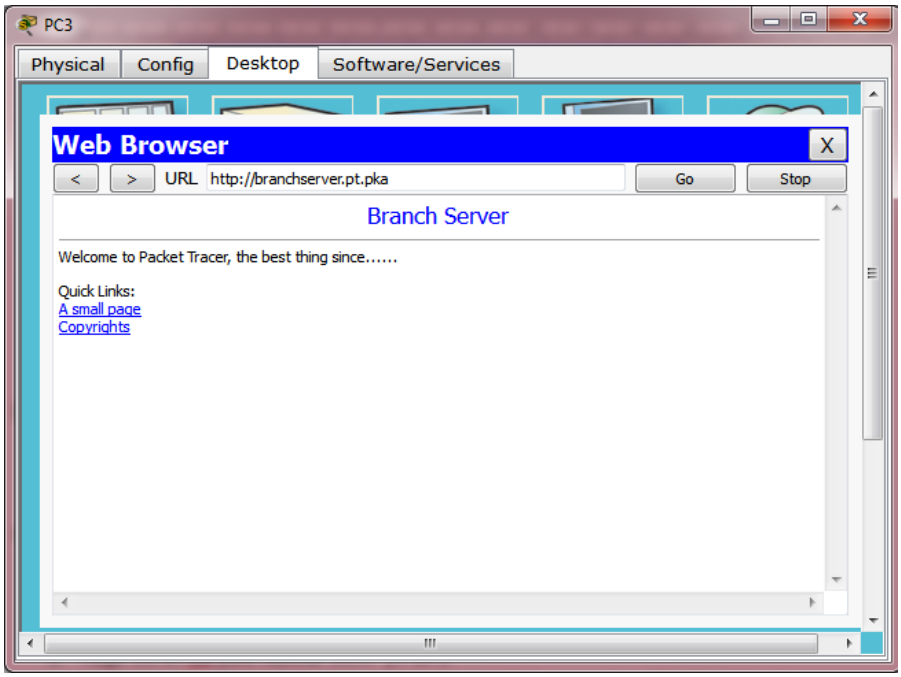
c. En el cuadro de dirección URL, introduzca **64.100.200.1** como dirección IP y haga clic en **Go**. Aparece el sitio Web de **BranchServer**.



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



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



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

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

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

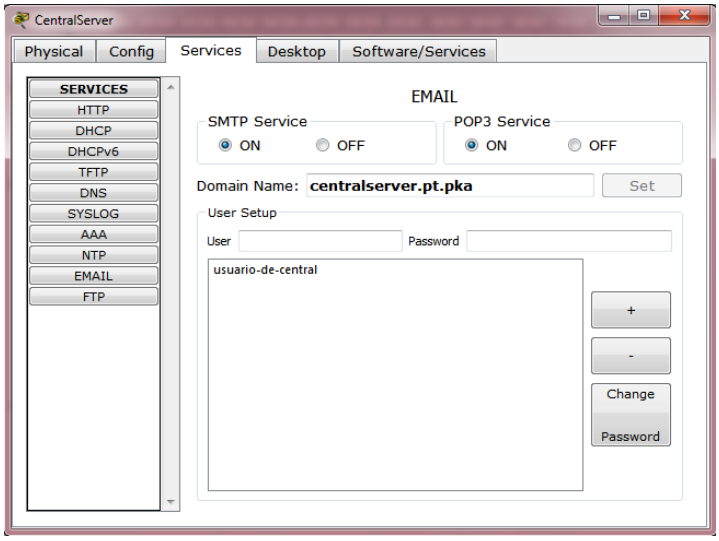
Paso 1: Configurar CentralServer para enviar (SMTP) y recibir (POP3) correo electrónico.

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

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

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

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



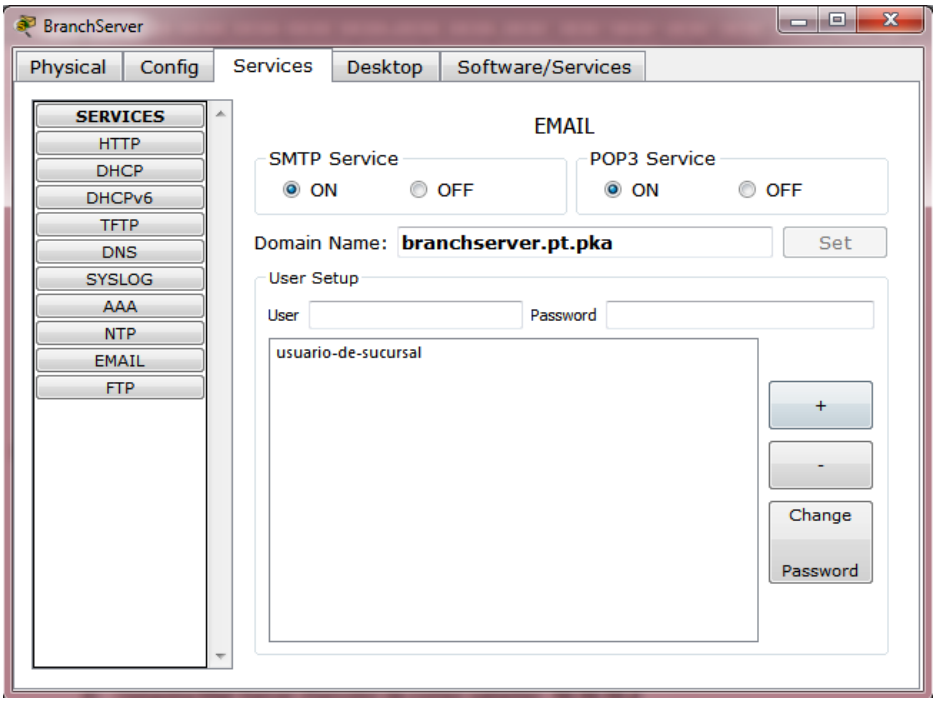
Paso 2: Configurar BranchServer para enviar (SMTP) y recibir (POP3) correo electrónico

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

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

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

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



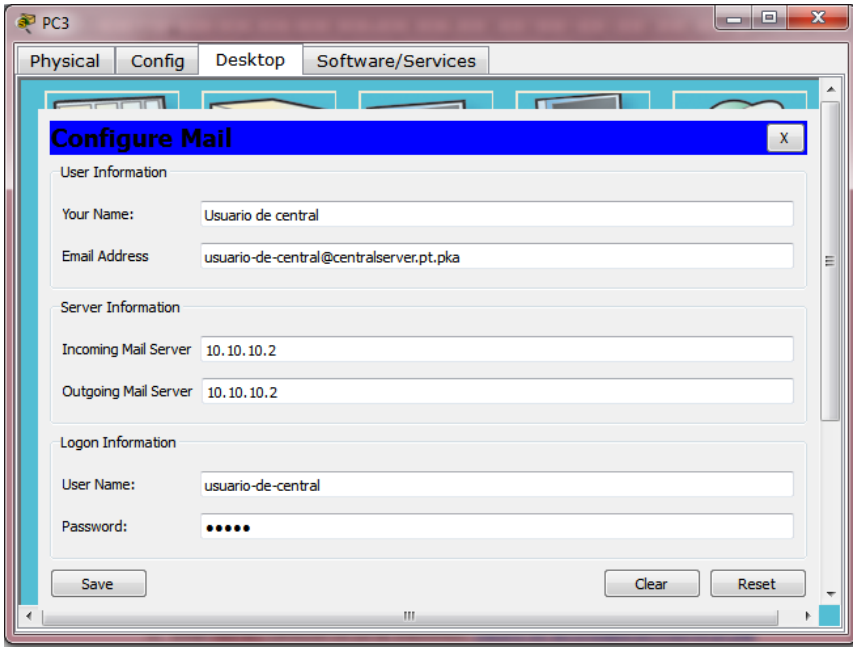
Paso 3: Configurar la PC3 para que use el servicio de correo electrónico de CentralServer

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

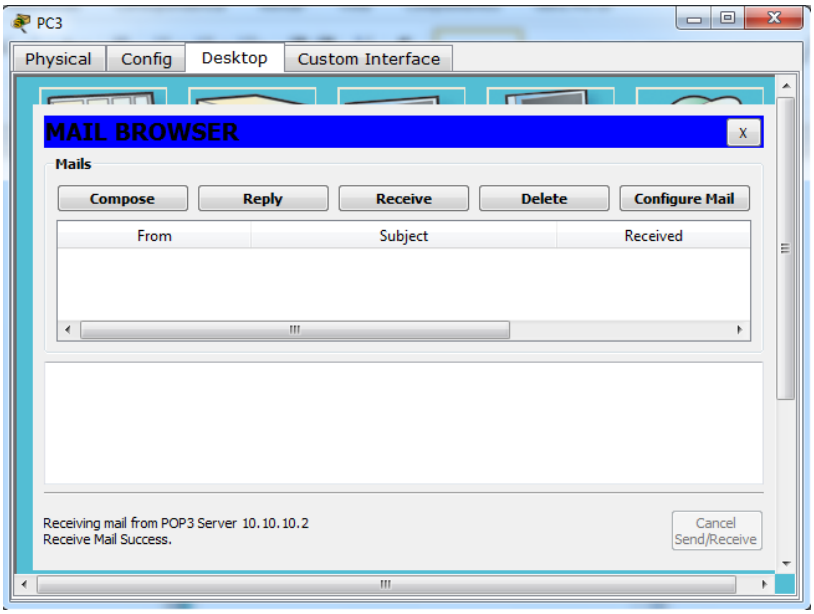
b. Introduzca los siguientes valores en los campos correspondientes:

1) Your Name (Su nombre): **Usuario de central**
2) Email Address (Dirección de correo electrónico): **usuario-de-central@centralserver.pt.pka**
3) Incoming Mail Server (Servidor de correo entrante): **10.10.10.2**
4) Outgoing Mail Server (Servidor de correo saliente): **10.10.10.2**
5) User Name (Nombre de usuario): **usuario-de-central**
6) Password (Contraseña): **cisco**

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



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



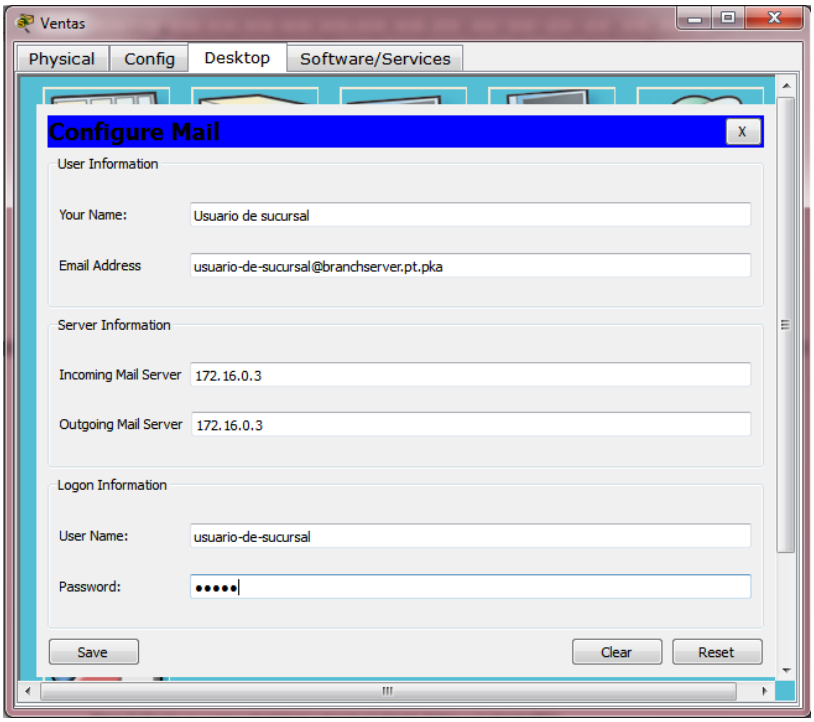
Paso 4: Configurar Sales para que use el servicio de correo electrónico de BranchServer

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

b. Introduzca los siguientes valores en los campos correspondientes:

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

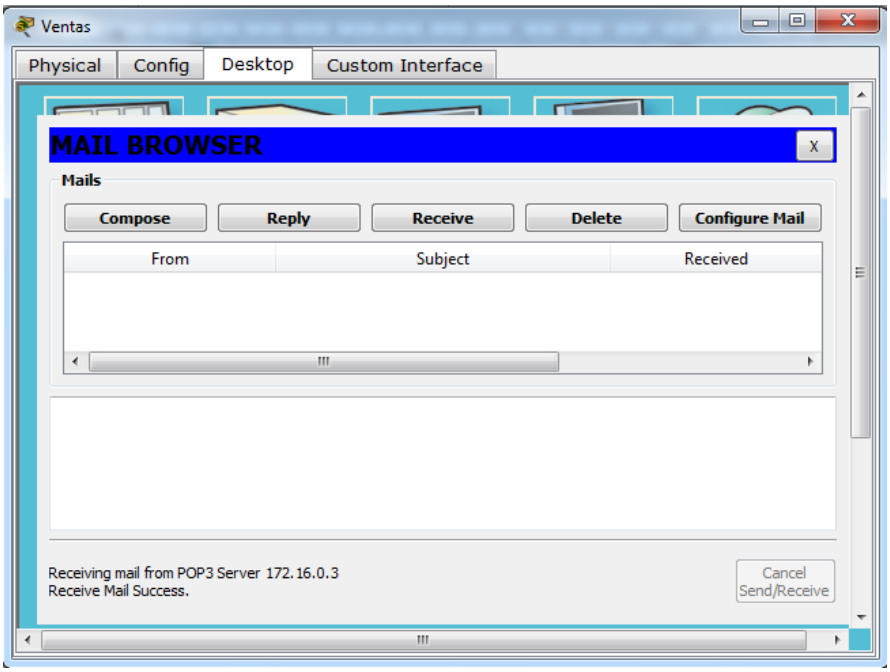
c. Haga clic en **Save** (Guardar). Aparece la ventana del explorador de correo.



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

Mail

`Success` (La función Recibir correo se realizó correctamente).



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

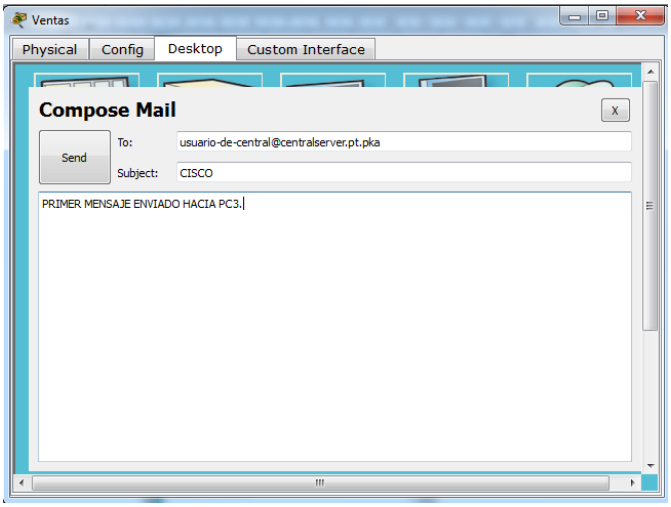
Paso 5: Envíe un correo electrónico desde el cliente Sales y el cliente PC3.

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

b. Introduzca los siguientes valores en los campos correspondientes:

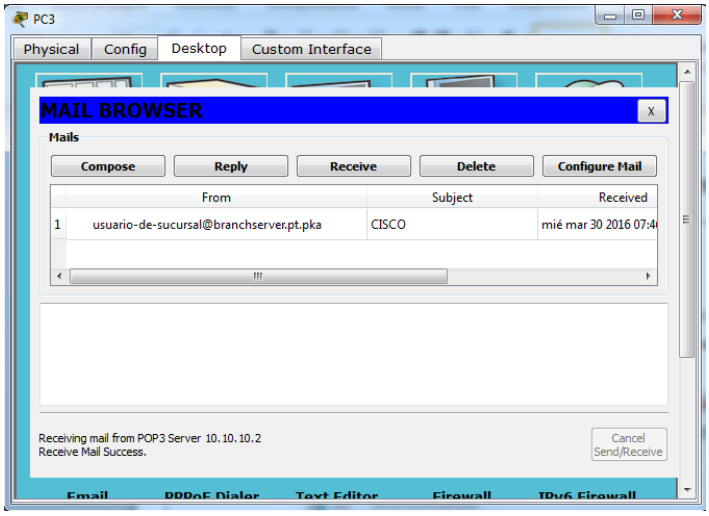
1) To (Para): **usuario-de-central@centralserver.pt.pka**
2) Subject (Asunto): *Personalice el asunto*.
3) **Email** body (Cuerpo del correo electrónico): *Personalice el correo electrónico*.

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

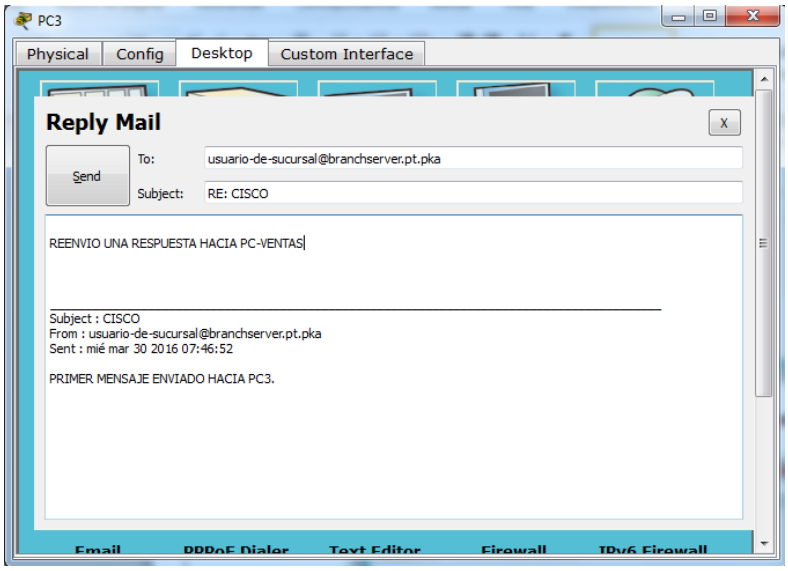


d. Verifique que la **PC3** haya recibido el correo electrónico. Haga clic en **PC3**. Si la ventana del explorador de correo está cerrada, haga clic en **E Mail**.

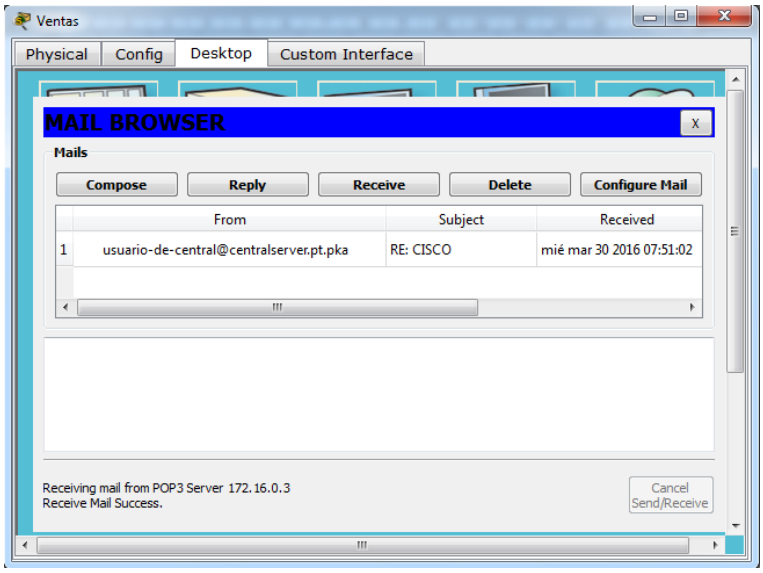
e. Haga clic en **Receive** (Recibir). Aparece un correo electrónico proveniente de Sales. Haga doble clic en el correo electrónico.



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



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



- Verificamos el estado de nuestro ejercicio.

Activity Results

Time Elapsed: 00:55:48

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points	Component(s)	Feedback
Network				
BranchServer				
Email Server				
Domain Name	Correct	4	PT Server Con...	
POP3 Service Enabled	Correct	4	PT Server Con...	
SMTP Service Enabled	Correct	4	PT Server Con...	
Users				
User branch-user				
User Name	Correct	4	PT Server Con...	
User Password	Correct	4	PT Server Con...	
HTTP Server		0	Ip	
HTTP Enable	Correct	3	PT Server Con...	
HTTPS Server		0	Ip	
HTTPS Enable	Correct	3	PT Server Con...	
CentralServer				
Email Server				
Domain Name	Correct	4	PT Server Con...	
POP3 Service Enabled	Correct	4	PT Server Con...	
SMTP Service Enabled	Correct	4	PT Server Con...	
Users				
User central-user				
User Name	Correct	4	PT Server Con...	
User Password	Correct	4	PT Server Con...	
HTTP Server		0	Ip	
HTTP Enable	Correct	3	PT Server Con...	
HTTPS Server		0	Ip	
HTTPS Enable	Correct	3	PT Server Con...	
PC3				
Email Client				
Email User				
Email	Correct	4	PT Client Conf...	
Incoming Mail Ser...	Correct	4	PT Client Conf...	
Name	Correct	4	PT Client Conf...	
Outgoing Mail Ser...	Correct	4	PT Client Conf...	
User Name	Correct	4	PT Client Conf...	
User Password	Correct	4	PT Client Conf...	

Score : 76/76

Item Count : 20/20

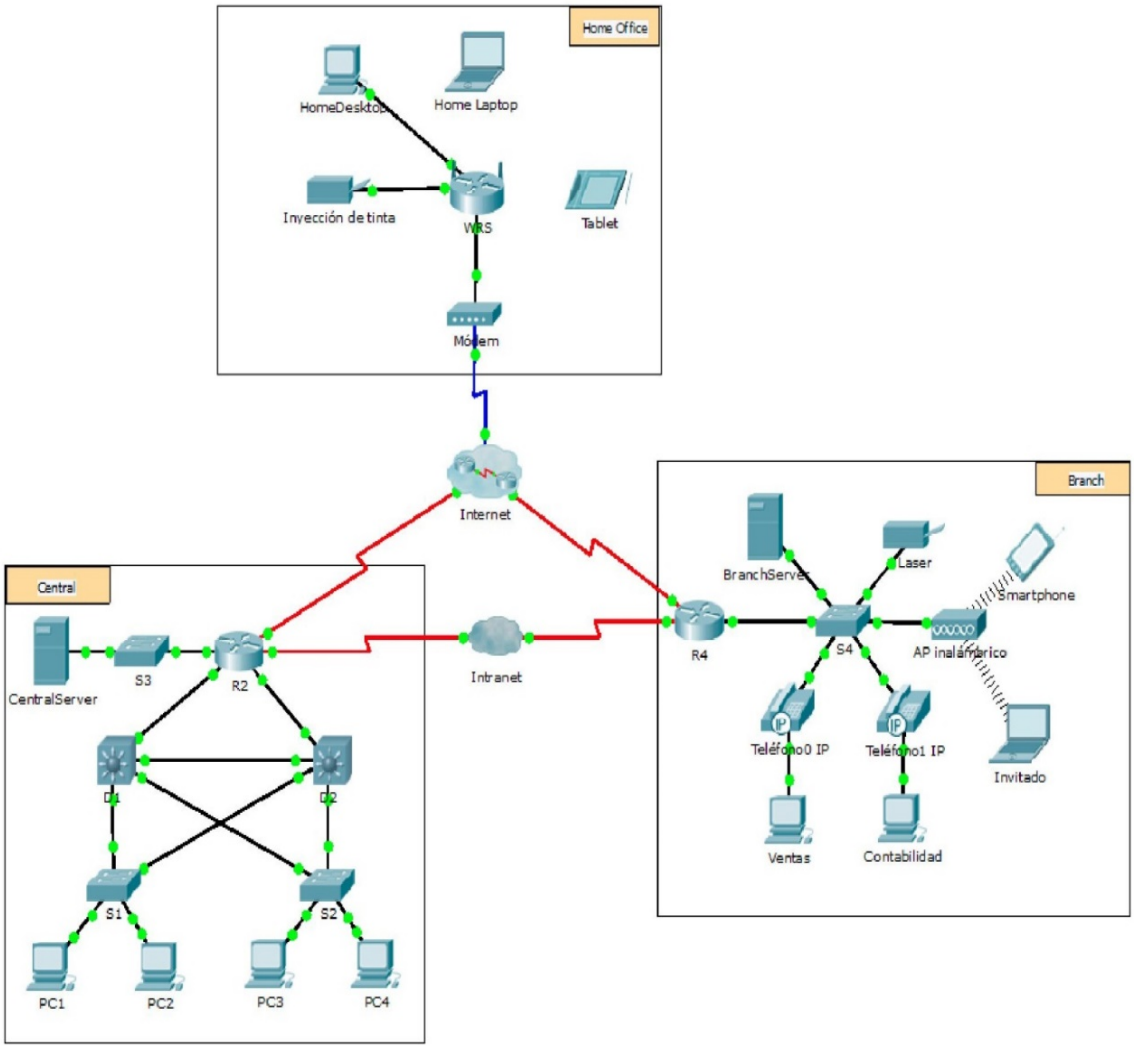
Component	Items/Total	Score
PT Client Configuration	6/6	24/24
PT Server Configuration	14/14	52/52

Laboratorio 10.2.2.8

Packet Tracer: Servidores de DHCP y servidores DNS (version para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología.



Objetivos

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

Información básica

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

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

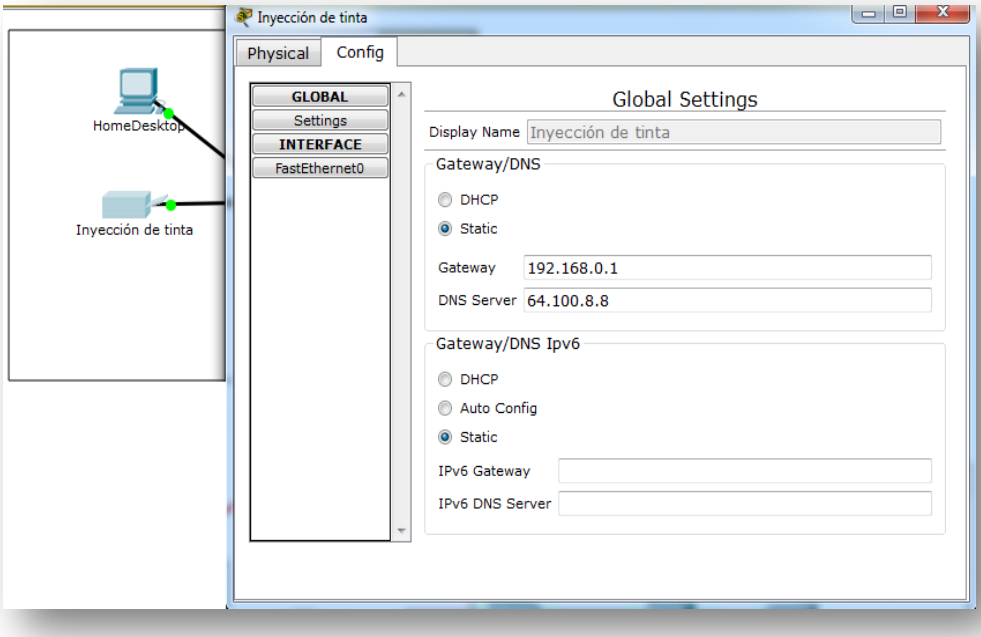
Parte 1: Configurar el direccionamiento IPv4 estático

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

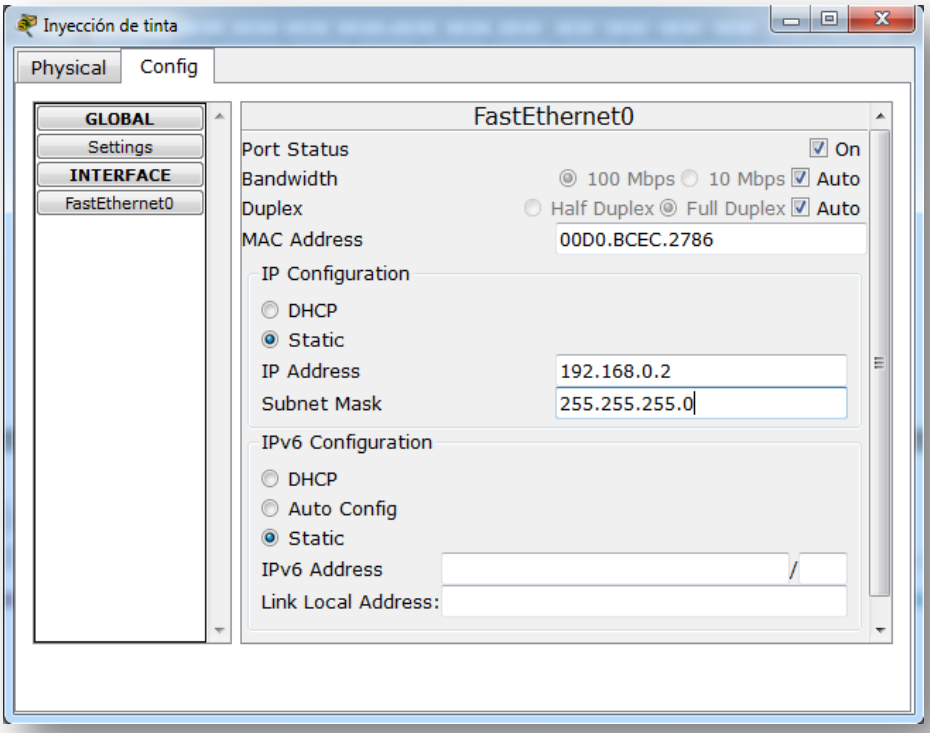
Las PC de oficinas domésticas necesitan conocer la dirección IPv4 de una impresora para enviarle información. Por lo tanto, la impresora debe utilizar una dirección IPv4 estática (invariable).

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**.



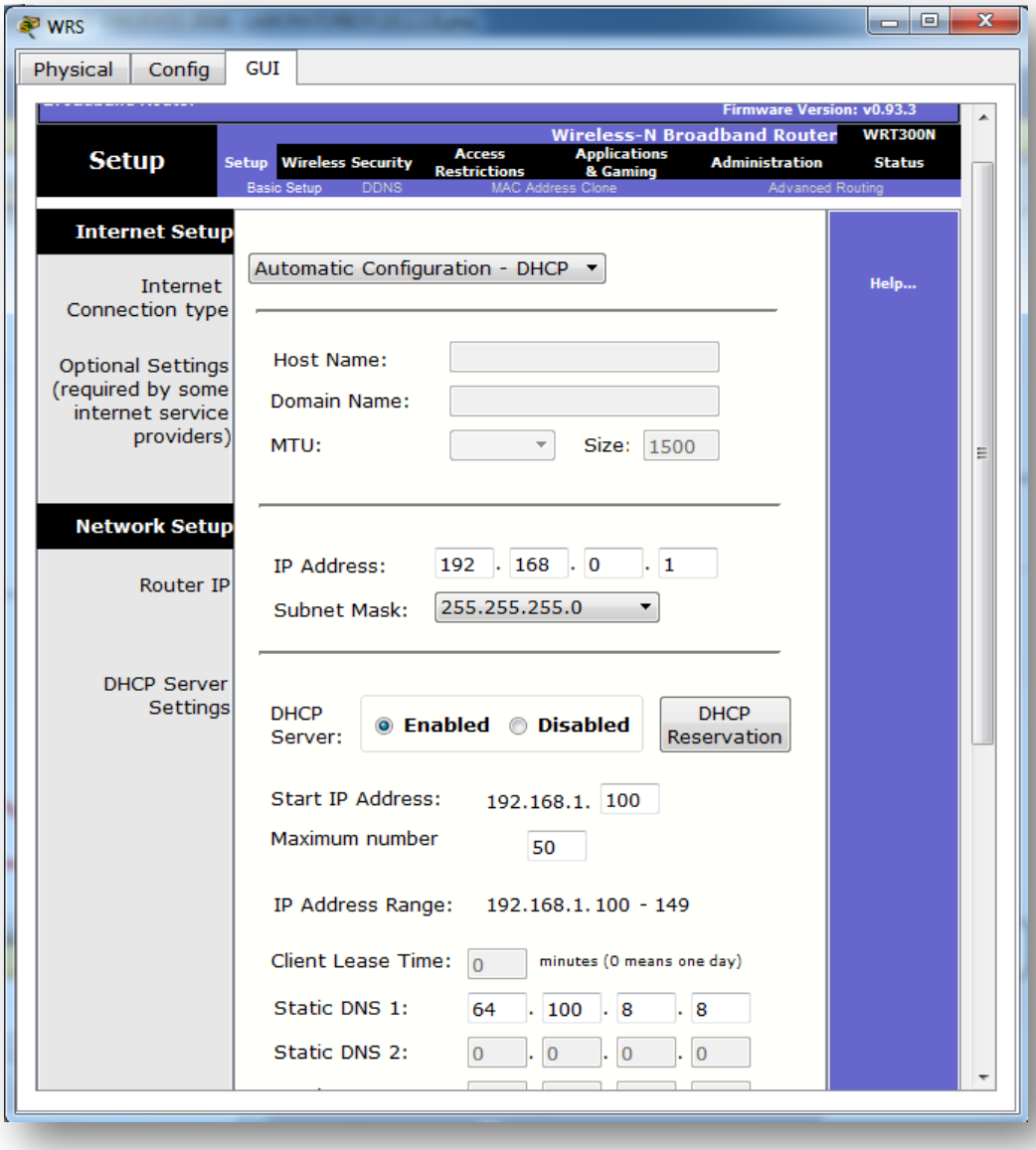
d. Cierre la ventana Inkjet.

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).

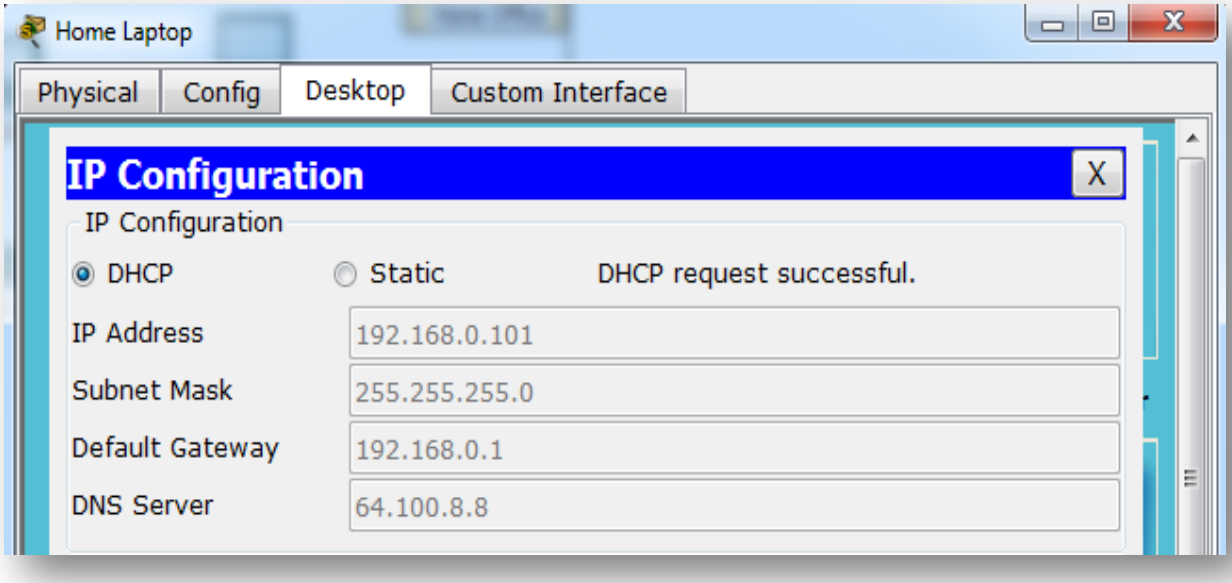


c. Cierre la ventana **WRS**.

Paso 3: Solicitar direccionamiento DHCP para la computadora portátil doméstica

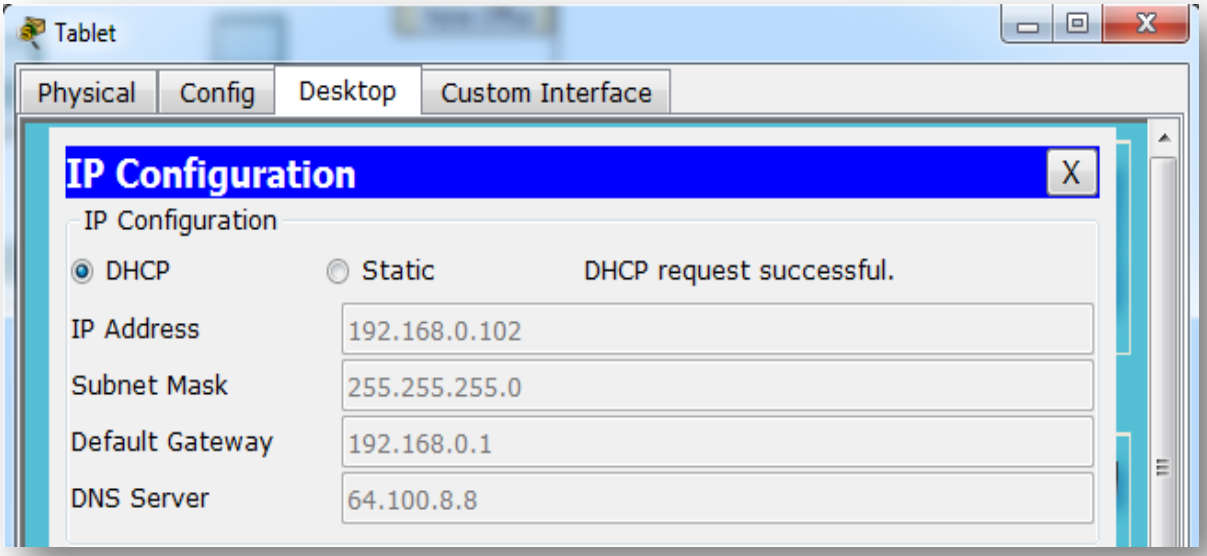
Esta actividad se centra en la oficina doméstica. Los clientes que configurará con DHCP son **Home Laptop** (Computadora portátil doméstica) y **Tablet PC**.

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**.



Paso 4: Solicitar direccionamiento DHCP para la tablet PC

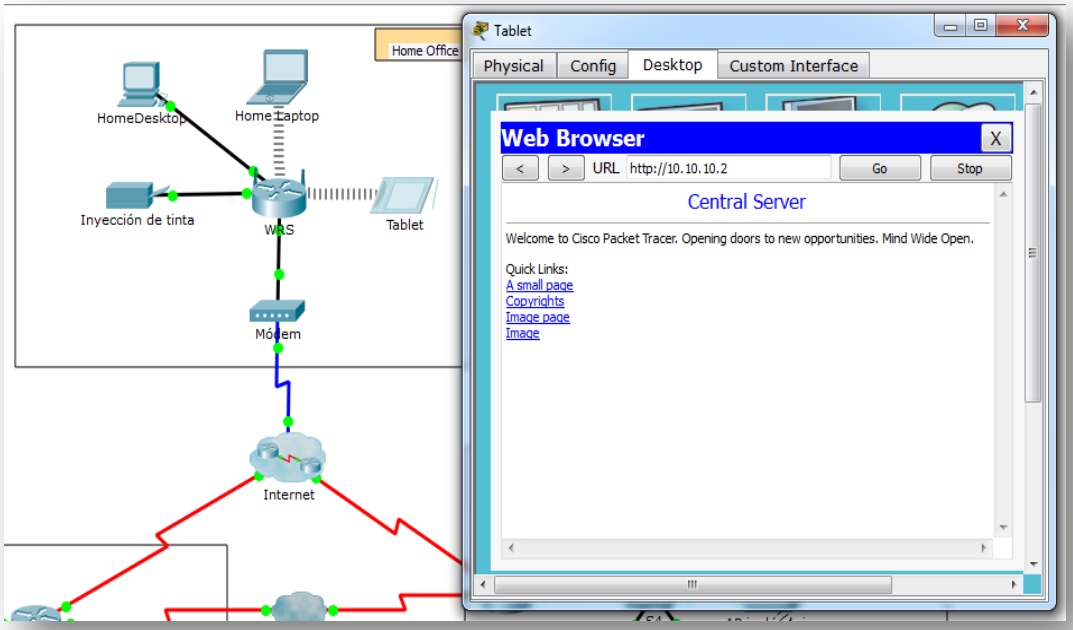
a. Haga clic en **Tablet** y, a continuación, haga clic en la ficha **Desktop** > **IP Configuration**.
b. Haga clic en **DHCP** y espere hasta que la solicitud de DHCP sea correcta.
c. Ahora, **Tablet** debe tener una configuración IP completa. De no ser así, vuelva al paso 2 y verifique las configuraciones en la **WRS**.



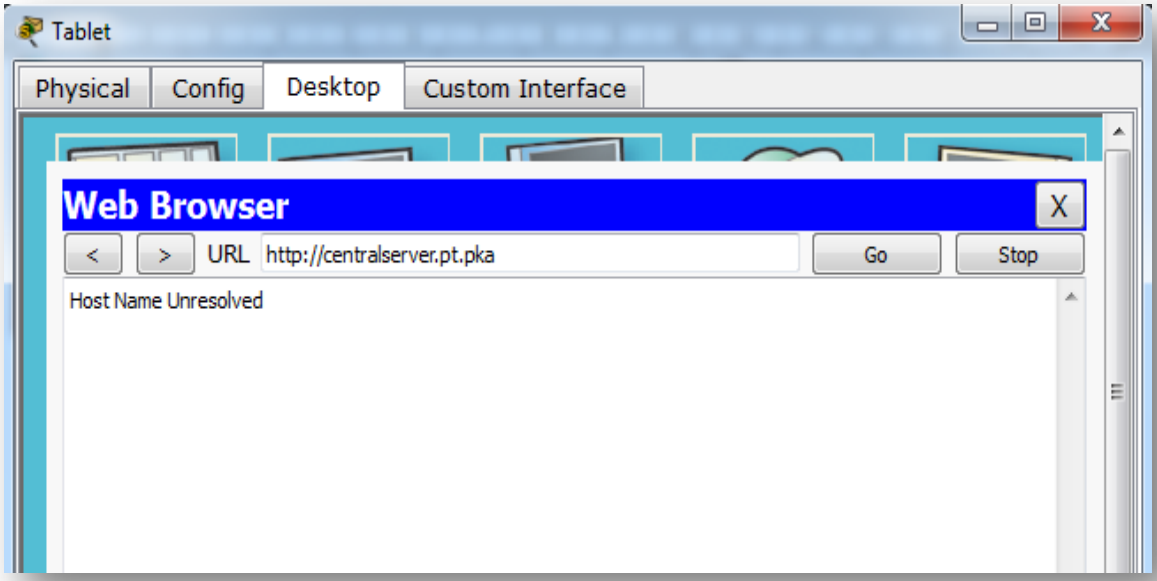
Paso 5: Probar el acceso a sitios Web

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.

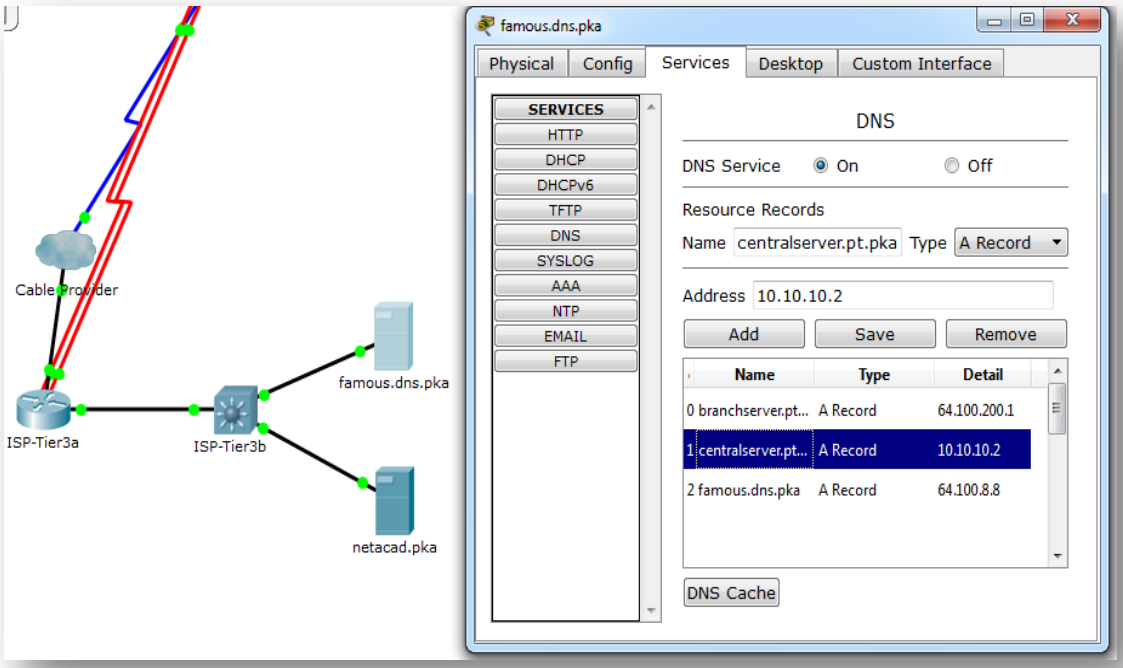
b. Haga clic en **famous.dns.pka** y, a continuación, haga clic en la ficha **Config** > **DNS**.

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.

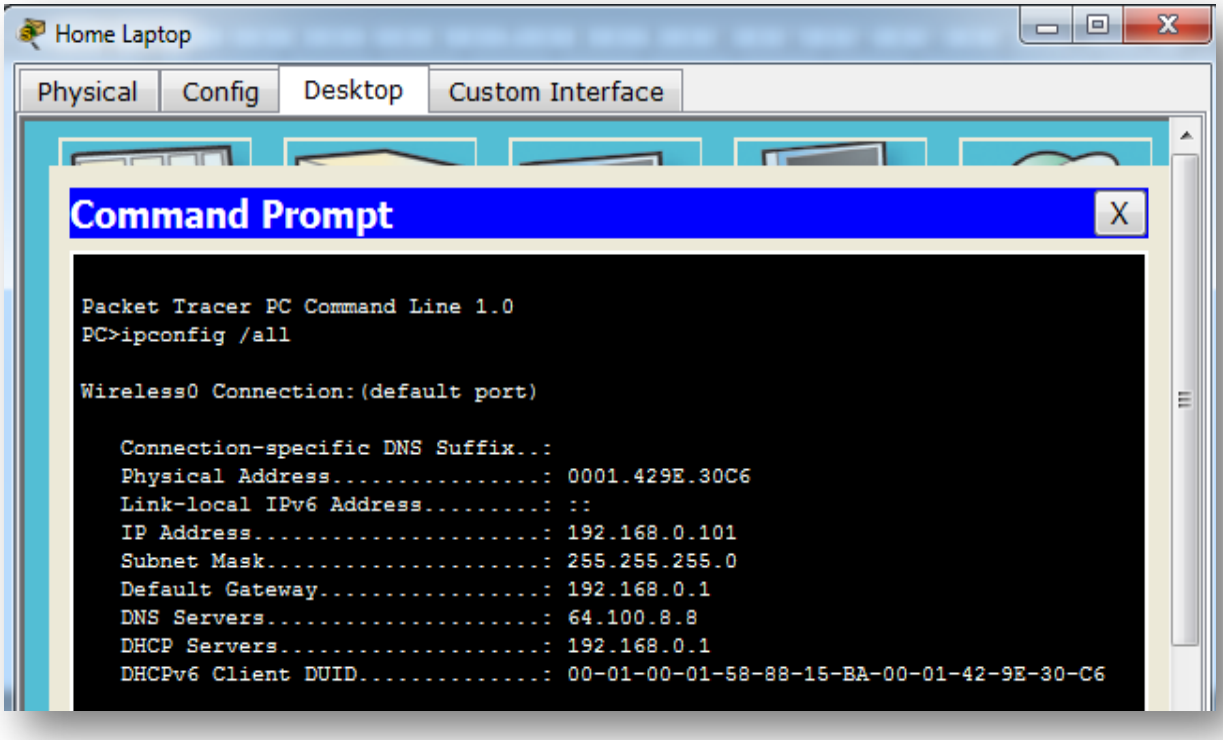
e. Haga clic en **Back** (Atrás) para salir de la nube de **Internet**.

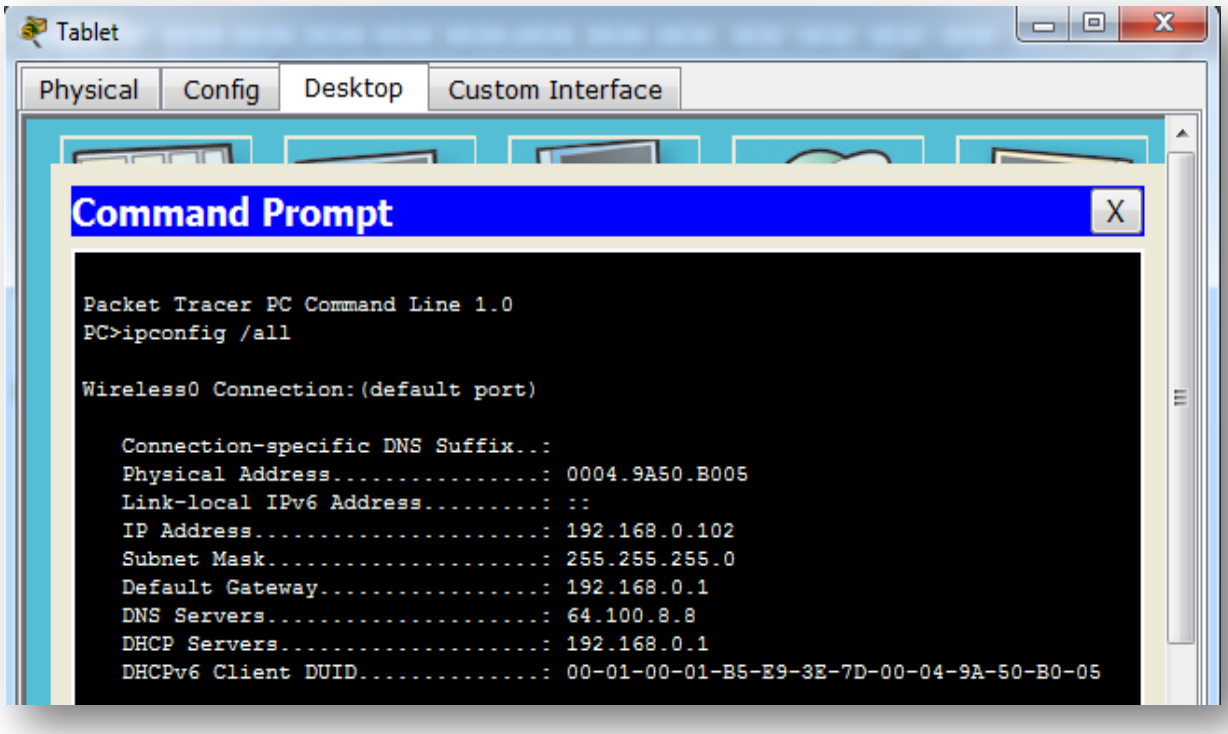


Paso 2: Verificar la capacidad de los equipos cliente para usar DNS

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.

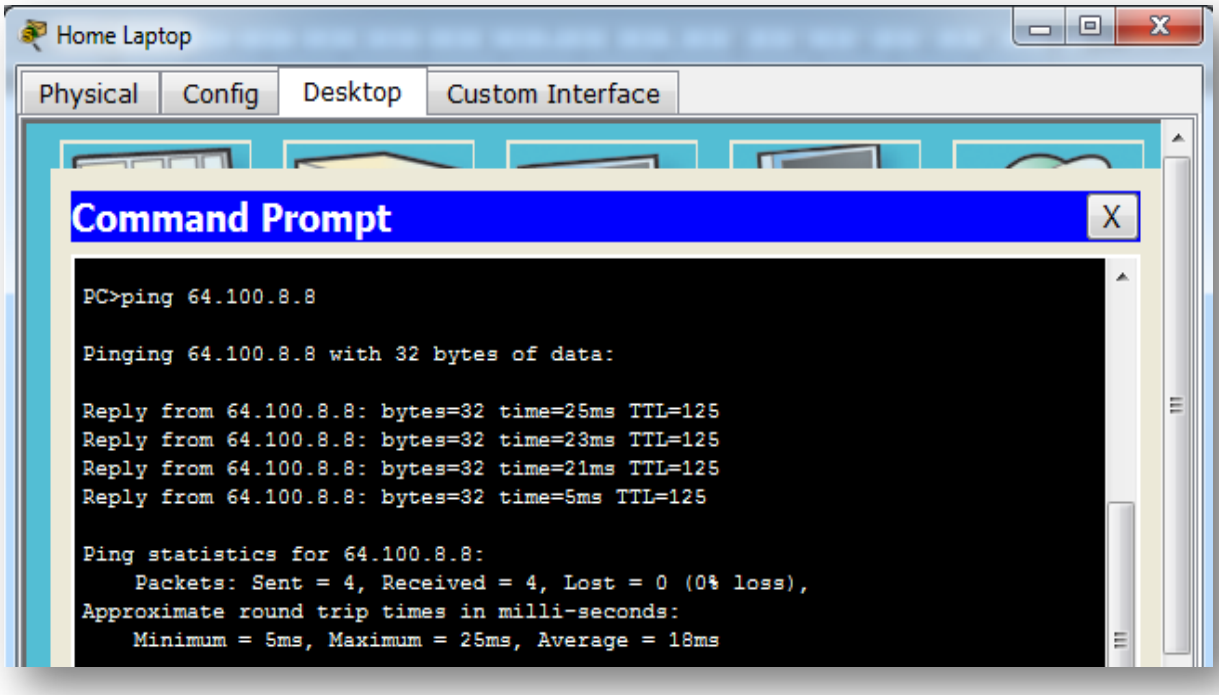
a. Haga clic en **Home Laptop** o **Tablet**.
b. Si el explorador Web está abierto, ciérrelo y seleccione **Command Prompt** (Símbolo del sistema).
c. Verifique el direccionamiento IPv4 mediante la introducción del comando ipconfig /all. Debe ver la dirección IP del servidor DNS.

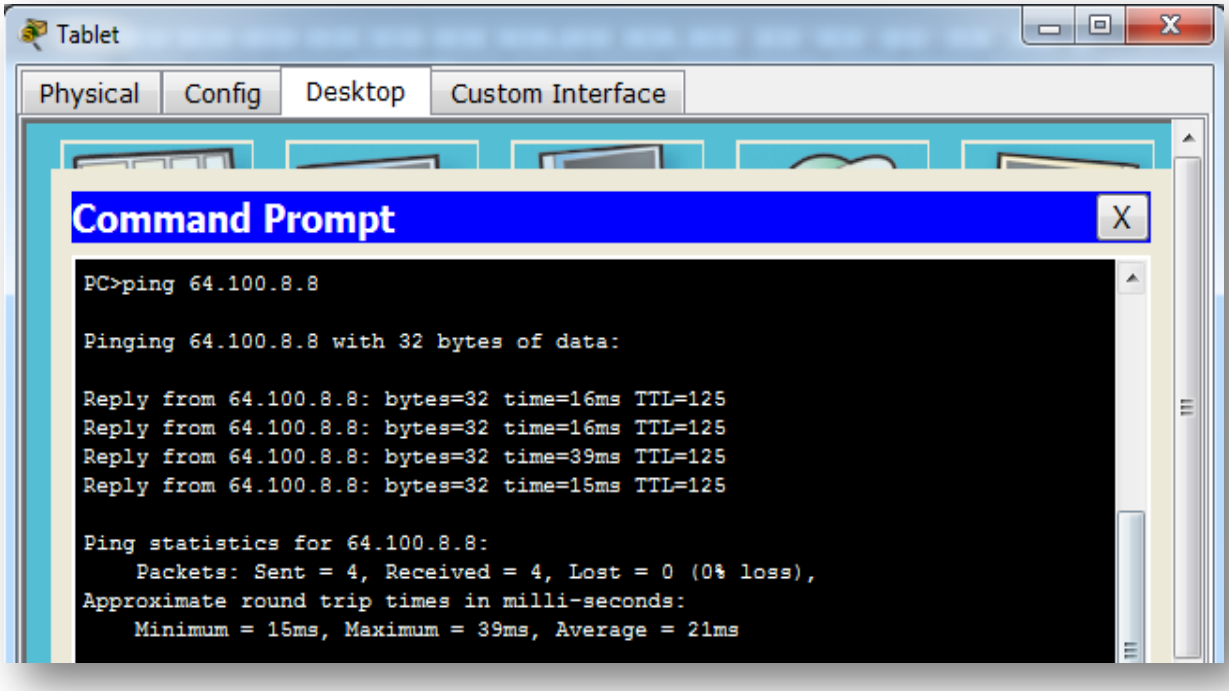

Home Laptop
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ipconfig /all
Wireless0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 0001.429E.30C6
Link-local IPv6 Address.....: ::
IP Address.....: 192.168.0.101
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 64.100.8.8
DHCP Servers.....: 192.168.0.1
DHCPv6 Client DUID.....: 00-01-00-01-58-88-15-BA-00-01-42-9E-30-C6


Tablet
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ipconfig /all
Wireless0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 0004.9A50.B005
Link-local IPv6 Address.....: ::
IP Address.....: 192.168.0.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.0.1
DNS Servers.....: 64.100.8.8
DHCP Servers.....: 192.168.0.1
DHCPv6 Client DUID.....: 00-01-00-01-B5-E9-3E-7D-00-04-9A-50-B0-05

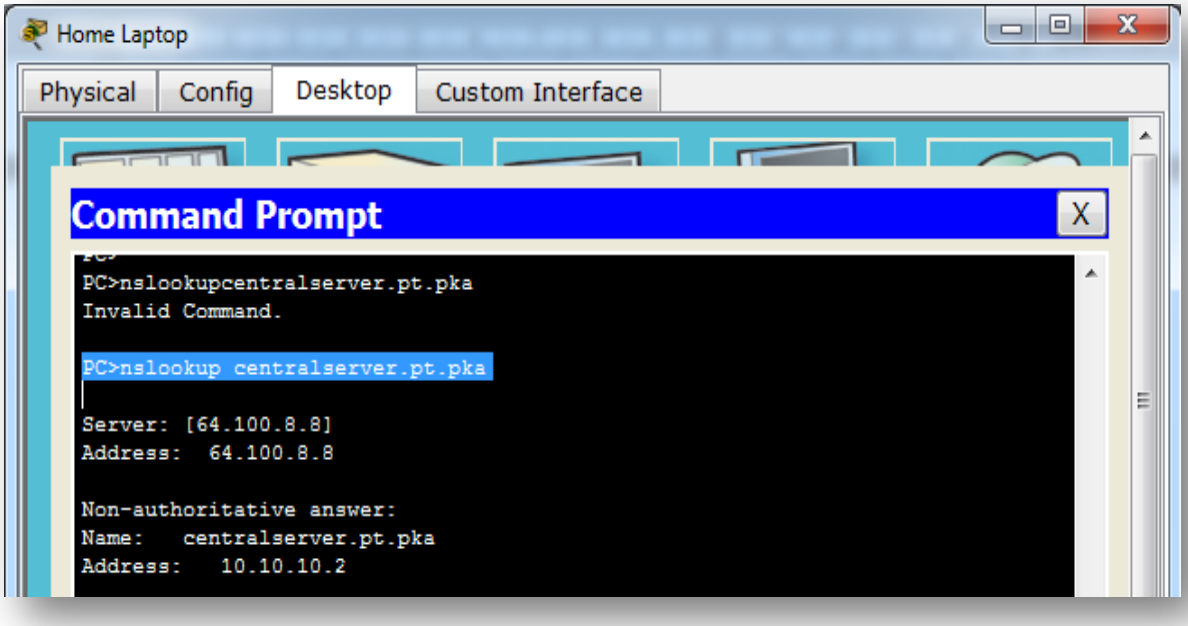
d. Haga ping al servidor DNS en **64.100.8.8** para verificar la conectividad.

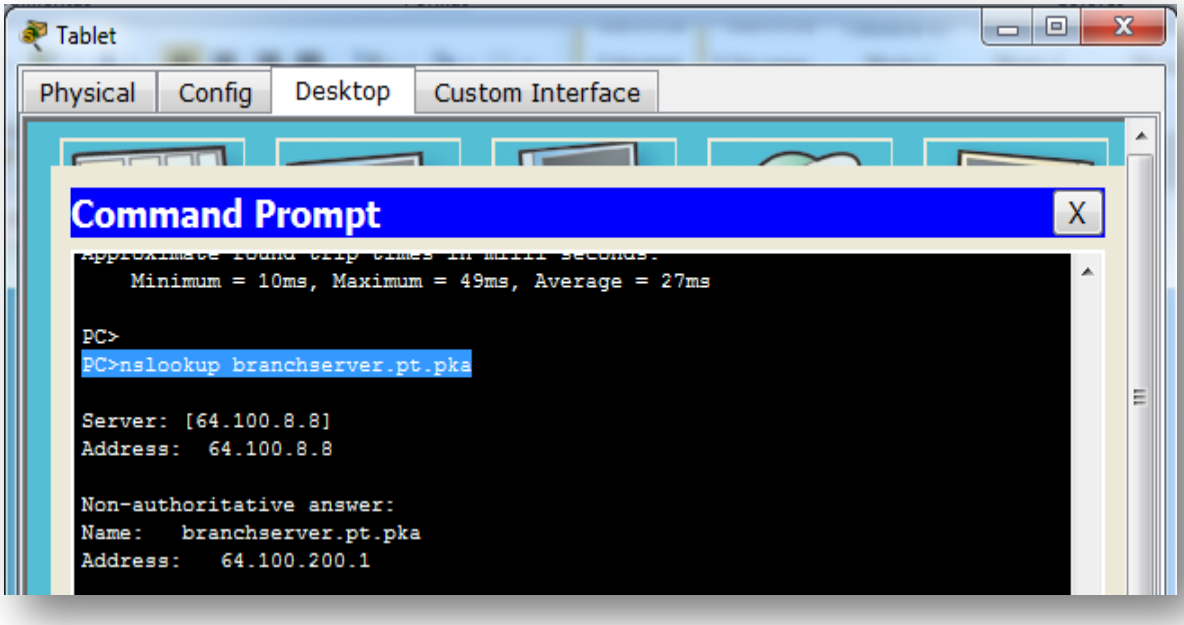
Nota: es posible que los primeros dos o tres pings fallen, ya que Packet Tracer simula los distintos procesos que deben ocurrir para que la conectividad a un recurso remoto sea correcta.



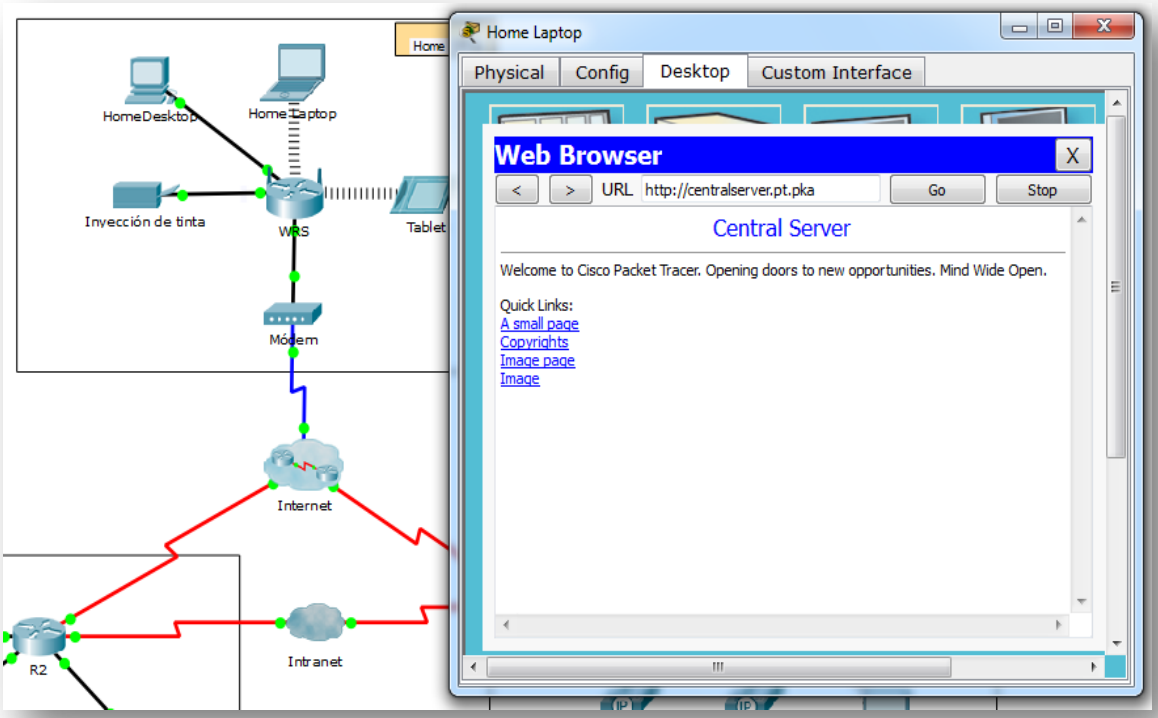


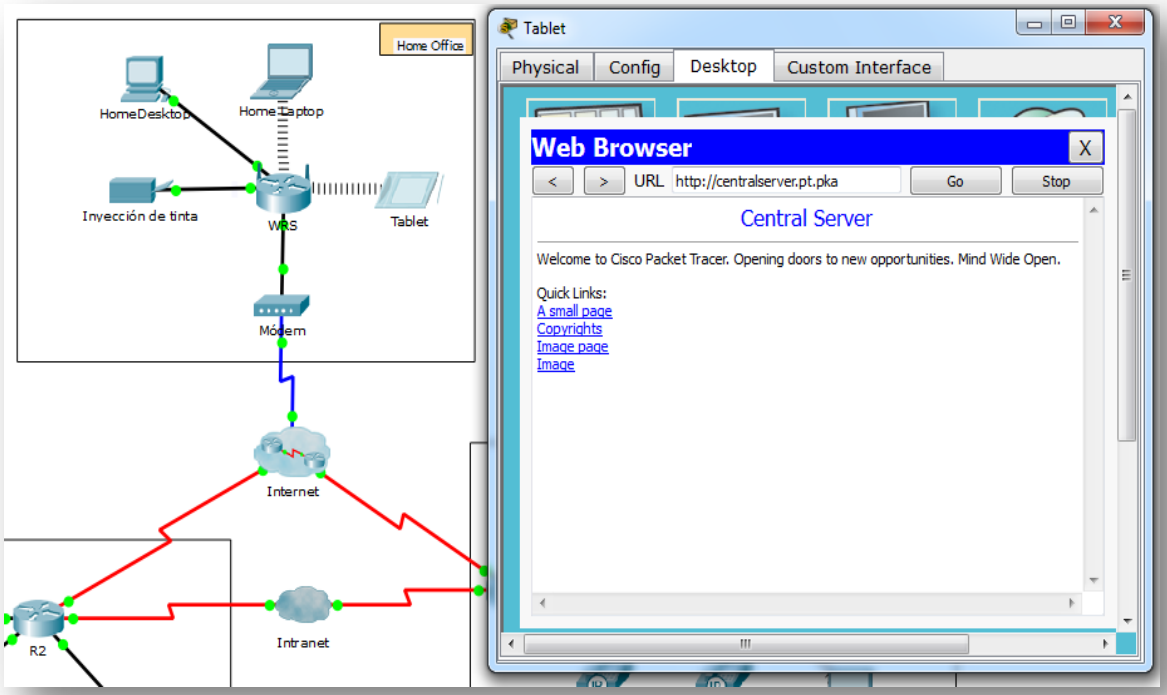
e. Pruebe la funcionalidad del servidor DNS mediante la introducción de los comandos **nslookup centralserver.pt.pka** y **nslookup branchserver.pt.pka**. Debe obtener una resolución de nombre que muestre la dirección IP de cada uno.


Home Laptop
Physical
Config
Desktop
Custom Interface
Command Prompt
PC>nslookupcentralserver.pt.pka
Invalid Command.
PC>nslookup centralserver.pt.pka
Server: [64.100.8.8]
Address: 64.100.8.8
Non-authoritative answer:
Name: centralserver.pt.pka
Address: 10.10.10.2

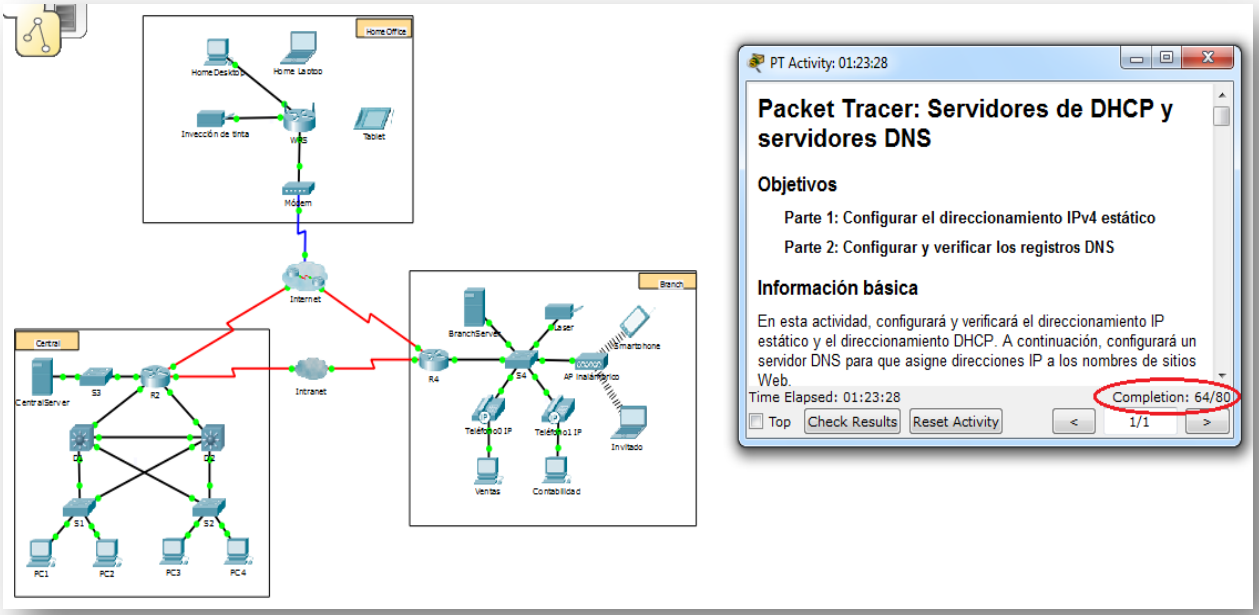

Tablet
Physical
Config
Desktop
Custom Interface
Command Prompt
Minimum = 10ms, Maximum = 49ms, Average = 27ms
PC>
PC>nslookup branchserver.pt.pka
Server: [64.100.8.8]
Address: 64.100.8.8
Non-authoritative answer:
Name: branchserver.pt.pka
Address: 64.100.200.1

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**.



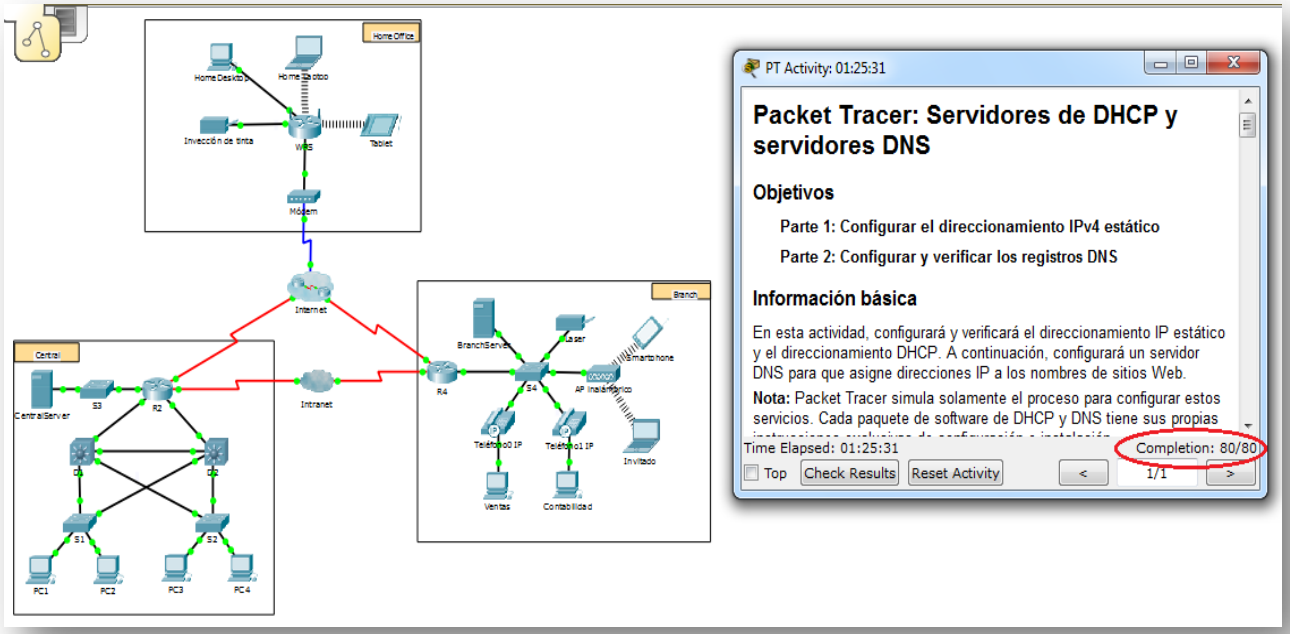


- Cuando iniciemos nuevamente el simulador el % del mismo baja, tal como lo indico a continuación.

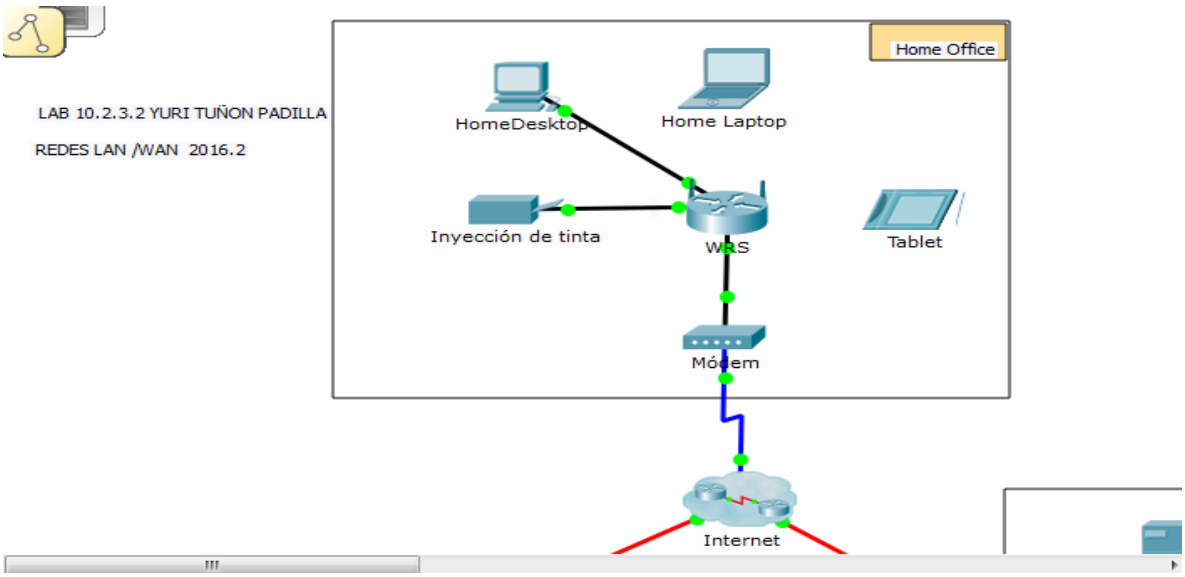


- Para regresar nuestra simulación al estado original debemos resetear el router WRS de la siguiente manera

- Volvemos a verificar el ejercicio y ya esta al 100%



Laboratorio 10.2.3.2



Packet Tracer: Servidores FTP

Objetivos

Parte 1: Configurar servicios FTP en los servidores

Parte 2: Subir un archivo al servidor FTP

Parte 3: Descargar un archivo del servidor FTP

Información básica

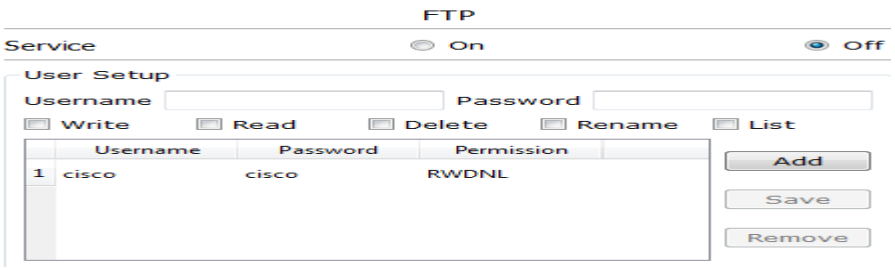
En esta actividad, configurará servicios FTP. Luego, utilizará los servicios FTP para transferir archivos entre los clientes y el servidor.

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

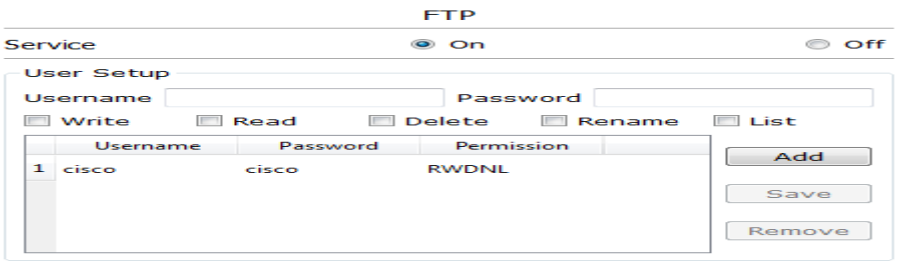
Parte 1: Configurar servicios FTP en los servidores

Paso 1: Configurar el servicio FTP en CentralServer.

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

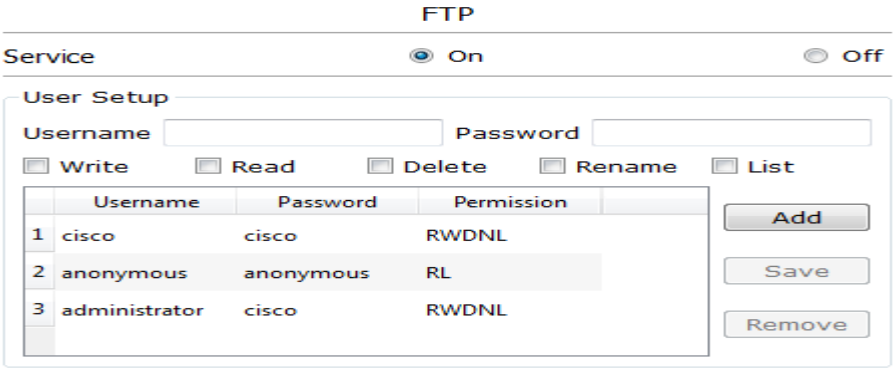


b. Haga clic en **On** (Activar) para habilitar el servicio FTP.

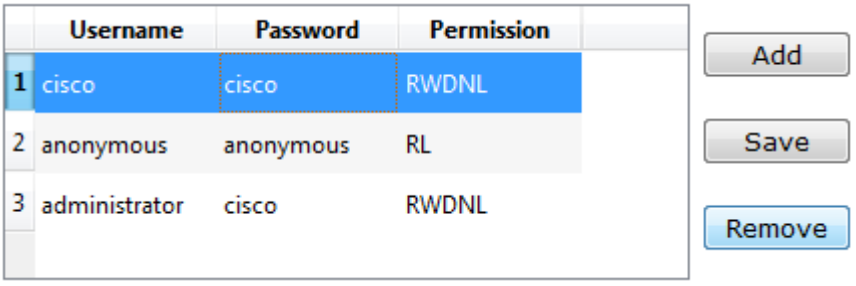


c. En **User Setup** (Configuración de usuario), cree las siguientes cuentas de usuario. Haga clic en el botón **+** para agregar la cuenta:

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



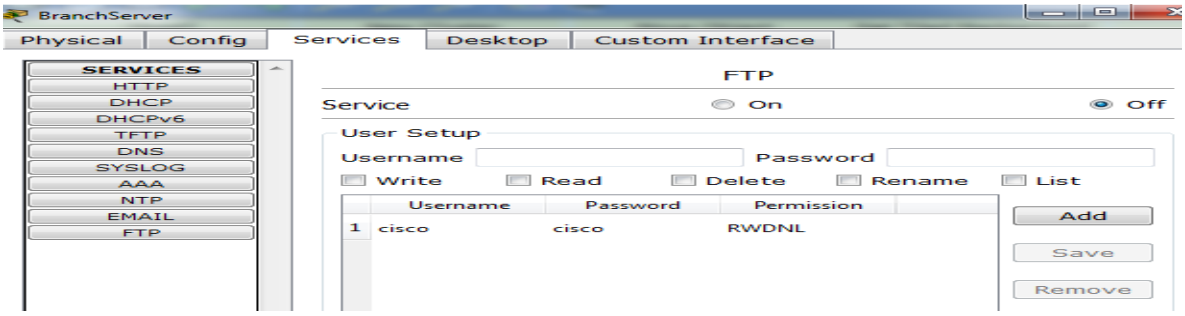
c. Haga clic en la cuenta de usuario **cisco** predeterminada y, a continuación, haga clic en el botón **-** para eliminarla. Cierre la ventana de configuración de la CentralServer.



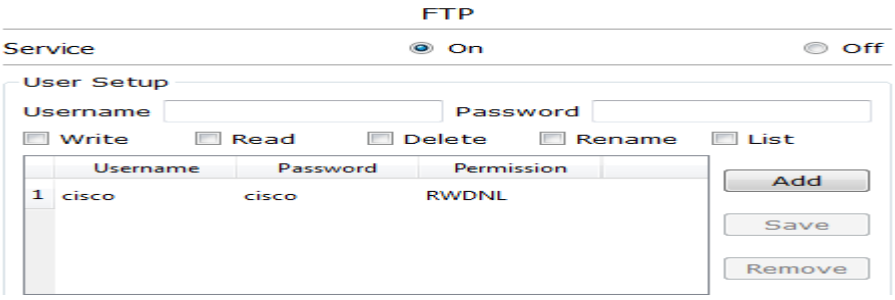
Paso 2: Configurar el servicio FTP en BranchServer.

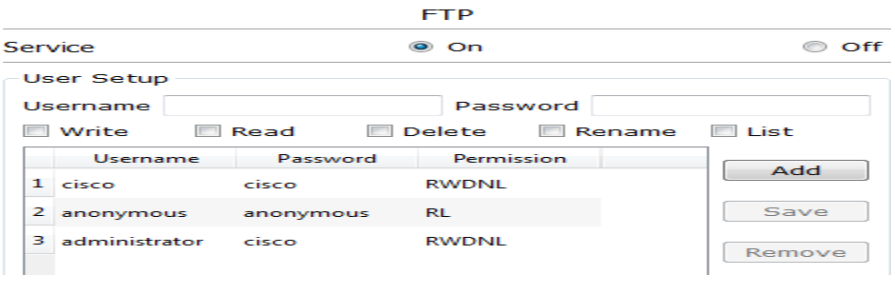
Repita el paso 1 en **BranchServer**.

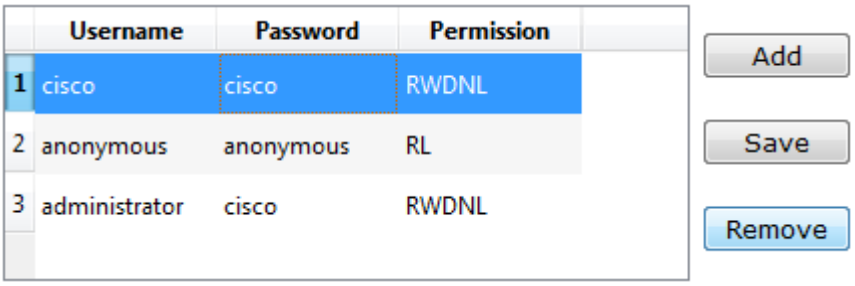
a)



b)





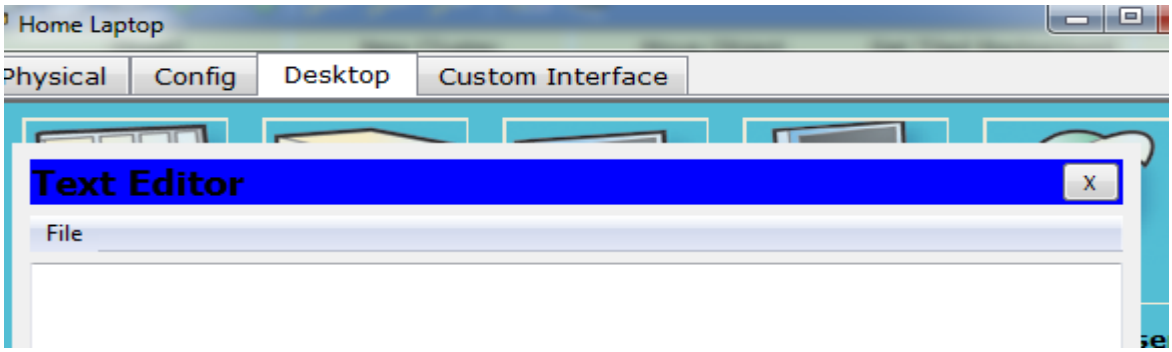


Parte 2: Subir un archivo al servidor FTP

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

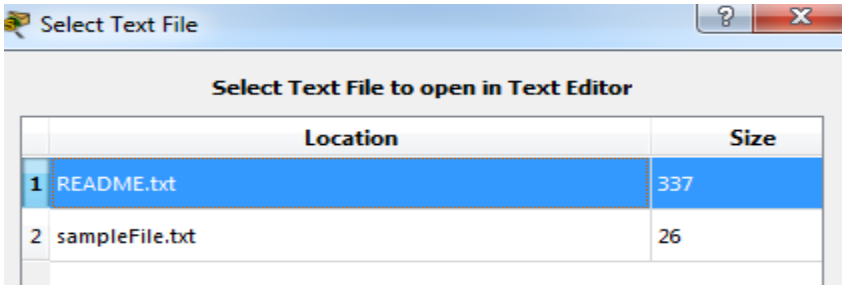
Como administrador de red, debe colocar un aviso en los servidores FTP. El documento se creó en la computadora portátil doméstica y se debe subir a los servidores FTP.

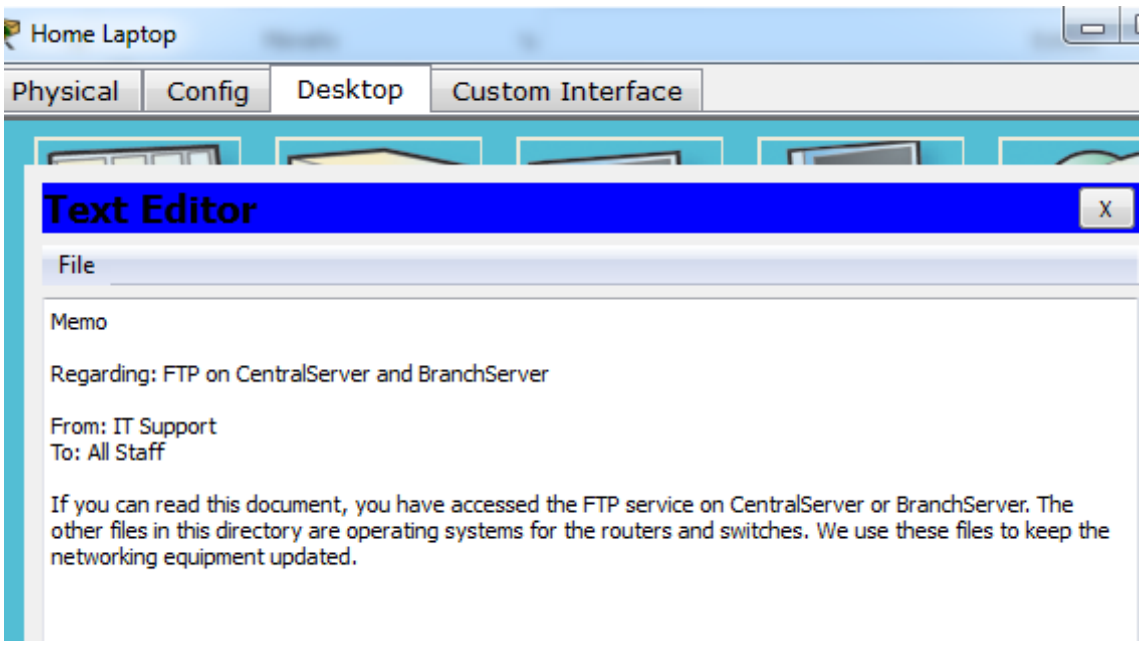
a. Haga clic en **Home Laptop** (Computadora portátil doméstica) y, a continuación, haga clic en la ficha **Desktop** > **Text Editor** (Escritorio > Editor de texto).



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

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

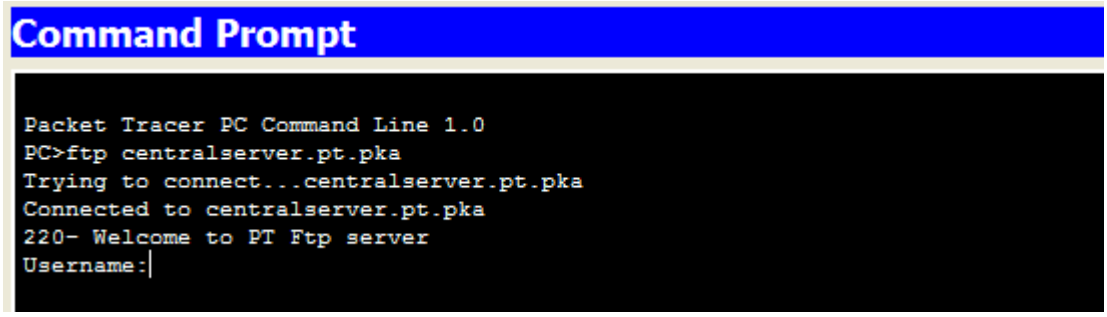




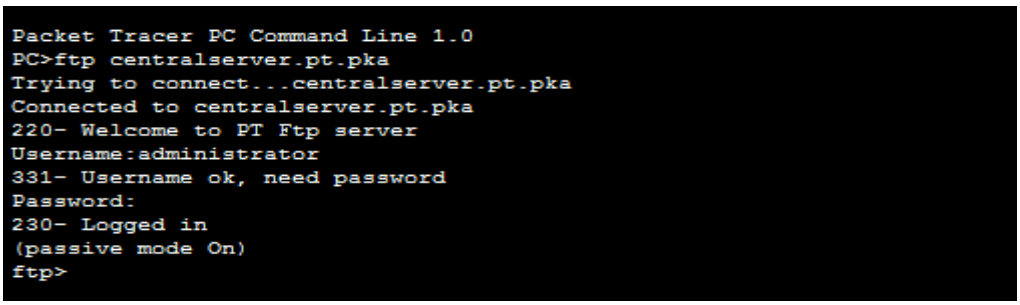
c. En la ficha **Desktop** , abra la ventana del símbolo del sistema y siga estos pasos:

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** .

```
ftp>dir

Listing /ftp directory from centralserver.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-i6q412-mz.121-22.EA4.bin               3058048
12   : c2950-i6q412-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-i6q412-mz.121-22.EA4.bin              3117390
ftp>
```

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**.

```
ftp>put README.txt

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

[Transfer complete - 337 bytes]

337 bytes copied in 0.057 secs (5912 bytes/sec)
ftp>
```

5) Para verificar la transferencia del archivo, escriba **dir**. El archivo README.txt ahora figura en el directorio de archivos.

```
ftp>dir

Listing /ftp directory from centralserver.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
```

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

```
ftp>quit

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

```
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
```

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

Parte 3: Descargar un archivo del servidor FTP

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

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

1) Escriba **ftp centralserver.pt.pka**.

```
Packet Tracer PC Command Line 1.0
PC>ftp centralserver.pt.pka
Trying to connect...centralserver.pt.pka
Connected to centralserver.pt.pka
220- Welcome to PT Ftp server
Username:
```

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

```
Packet Tracer PC Command Line 1.0
PC>ftp centralserver.pt.pka
Trying to connect...centralserver.pt.pka
Connected to centralserver.pt.pka
220- Welcome to PT Ftp server
Username:anonymous
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

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.

```
ftp>dir

Listing /ftp directory from centralserver.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
```

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**.

```
ftp>get README.txt

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

[Transfer complete - 337 bytes]

337 bytes copied in 0.024 secs (14041 bytes/sec)
ftp>
```

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).

```
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)
```

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

```
ftp>quit

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

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

```
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.

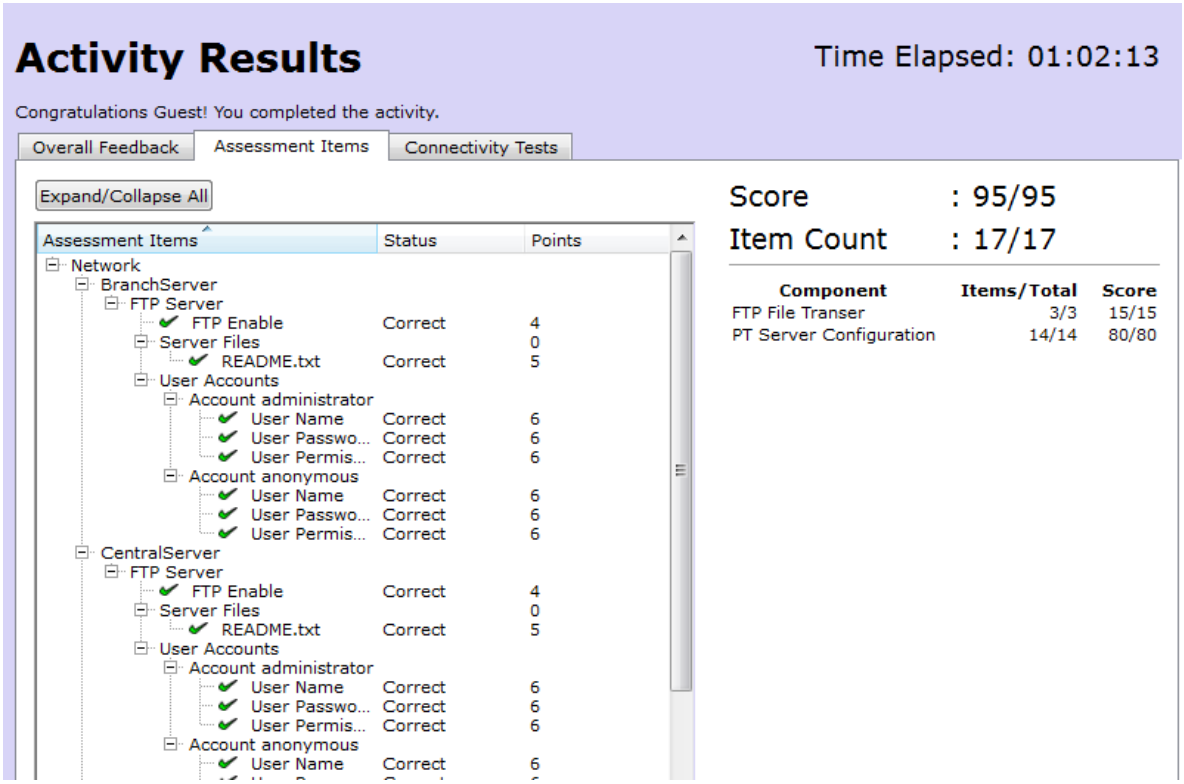
b. En la ficha **Desktop** , abra **Text Editor** y, a continuación, el archivo **README.txt** para verificar la integridad del archivo.

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**.

```
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>
```



Activity Results Time Elapsed: 01:02:13

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

Assessment Items	Status	Points
Network		
BranchServer		
FTP Server		
FTP Enable	Correct	4
Server Files		0
README.txt	Correct	5
User Accounts		
Account administrator		
User Name	Correct	6
User Passwo...	Correct	6
User Permis...	Correct	6
Account anonymous		
User Name	Correct	6
User Passwo...	Correct	6
User Permis...	Correct	6
CentralServer		
FTP Server		
FTP Enable	Correct	4
Server Files		0
README.txt	Correct	5
User Accounts		
Account administrator		
User Name	Correct	6
User Passwo...	Correct	6
User Permis...	Correct	6
Account anonymous		
User Name	Correct	6

Score : 95/95

Item Count : 17/17

Component	Items/Total	Score
FTP File Transer	3/3	15/15
PT Server Configuration	14/14	80/80

Laboratorio 10.4.1.2

Función Multiusuario de Packet Tracer: Tutorial (versión para el instructor)

Topología

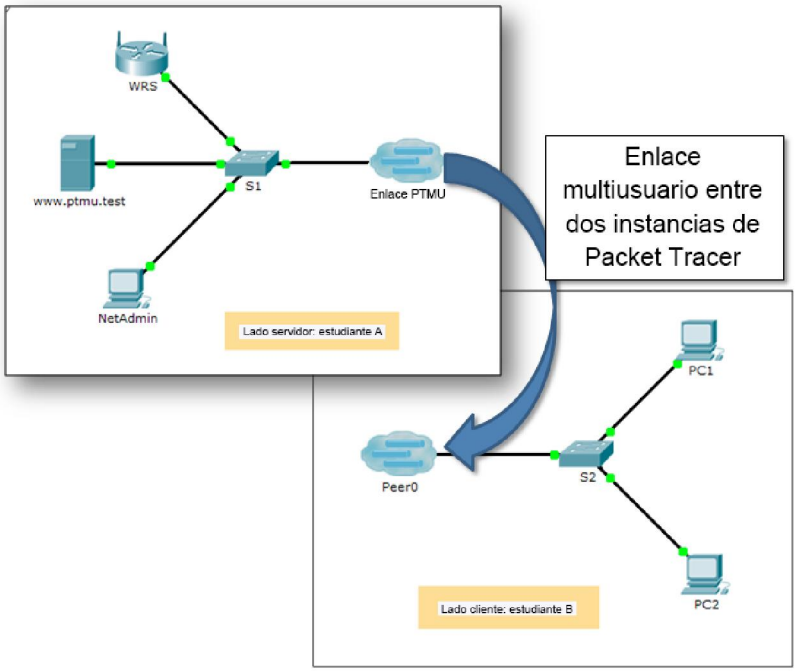


Tabla de direccionamiento

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

Objetivos

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

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

Información básica

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

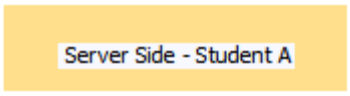
Parte 1: Establecer una conexión multiusuario local en otra instancia de Packet Tracer

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

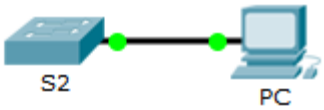
a. Busque un compañero de clase con el que cooperará para realizar esta actividad. Ambas PC deben estar conectadas a la misma LAN.

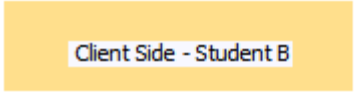
b. Determinen quién desempeñará la función del lado servidor y quién desempeñará la función del lado cliente en esta actividad.

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



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





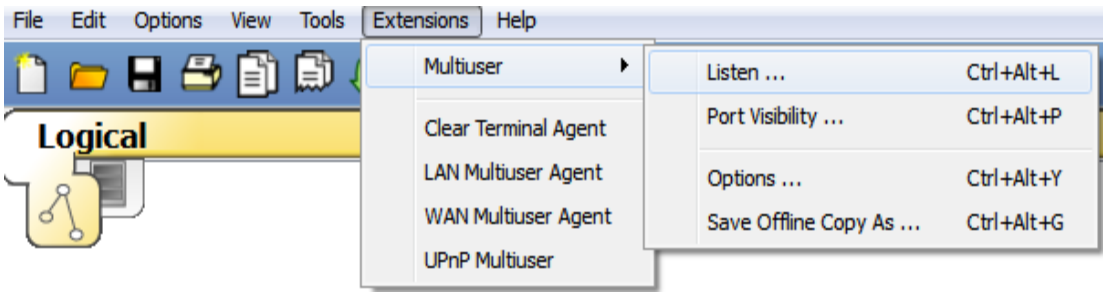
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

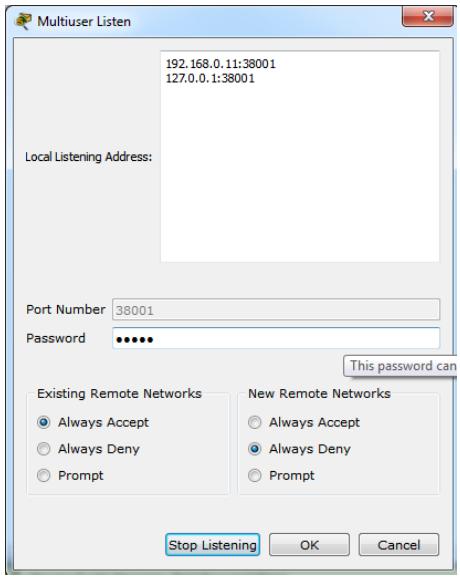
Paso 2: Jugador del lado servidor: configurar el lado servidor del enlace PTMU

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

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

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





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

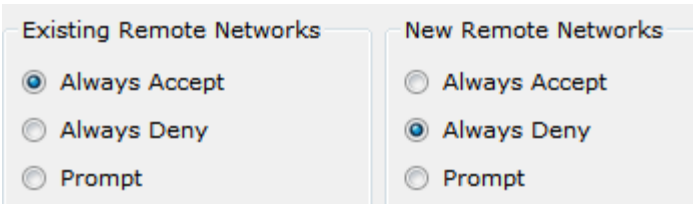
3) El número de puerto se indica junto a las direcciones IP y en el campo Port Number (Número de puerto). Si esta es la primera instancia de Packet Tracer que abrió en la PC, el número de

puerto será 38000. Sin embargo, si hay varias instancias abiertas, el número aumenta de a uno por cada instancia (38001, 38002, etcétera). El número de puerto es necesario para que el jugador del lado cliente configure la conexión multiusuario.

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

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

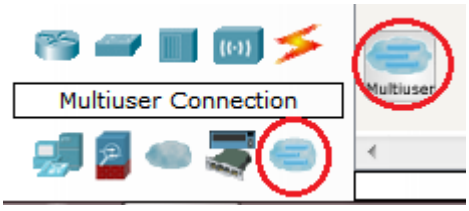
6) En la sección **Existing Remote Networks** (Redes remotas existentes), debe hacer clic en el botón de opción **Always Accept** (Aceptar siempre) o **Prompt** (Preguntar) para que el jugador del lado cliente se conecte de forma correcta.



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

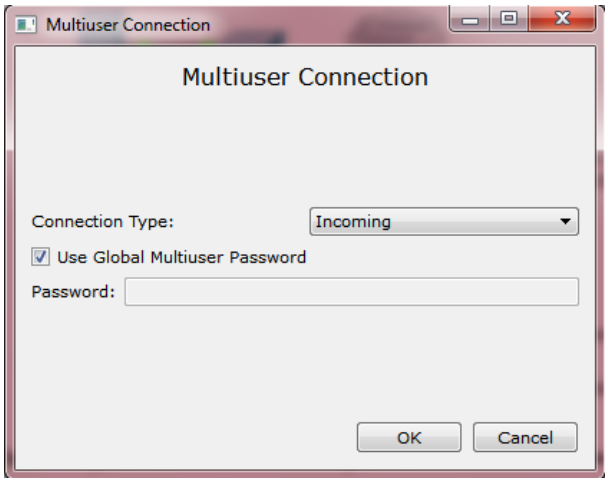
8) Haga clic en **OK** (Aceptar).

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



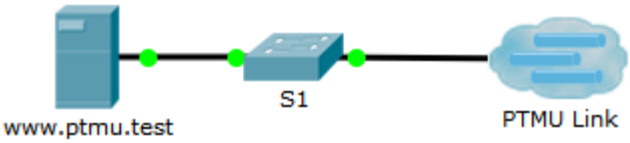
c. Haga clic en el nombre **Peer0** y cámbielo por **PTMU Link** (distingue mayúsculas de minúsculas).

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).



Server Side - Student A

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

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

Dirección IP: 192.168.0.11

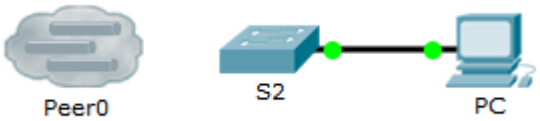
Número de puerto: 38001

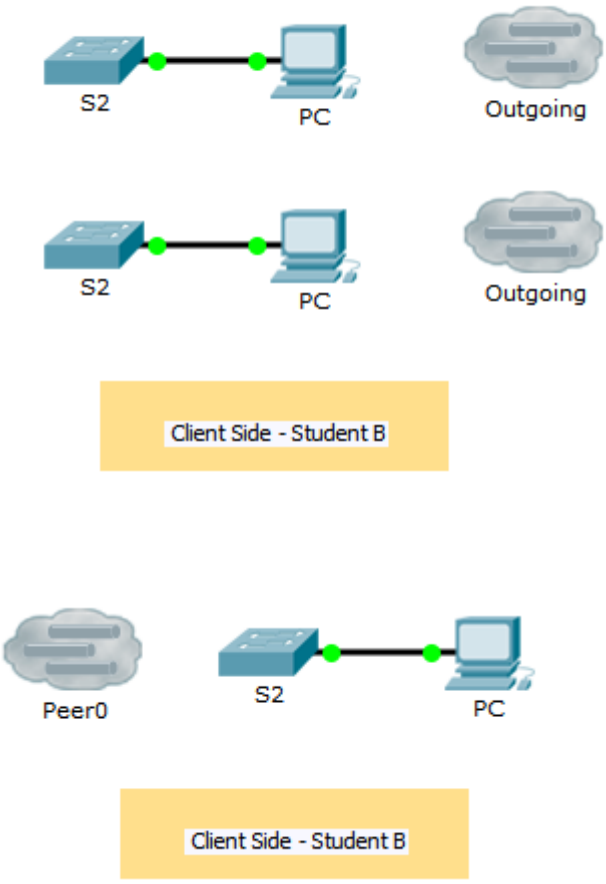
Contraseña (**cisco**, de manera predeterminada) cisco

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.

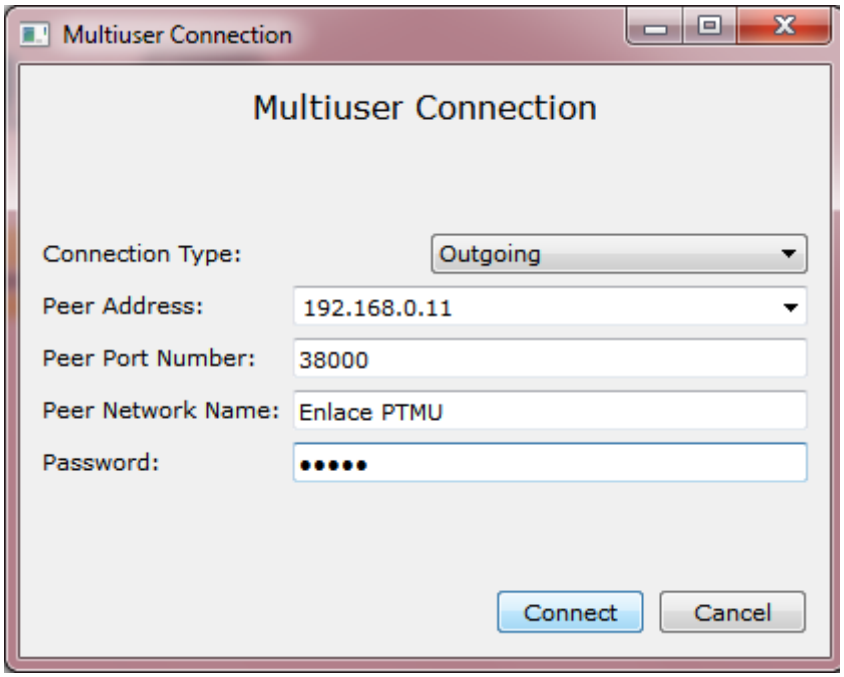
Client Side - Student B

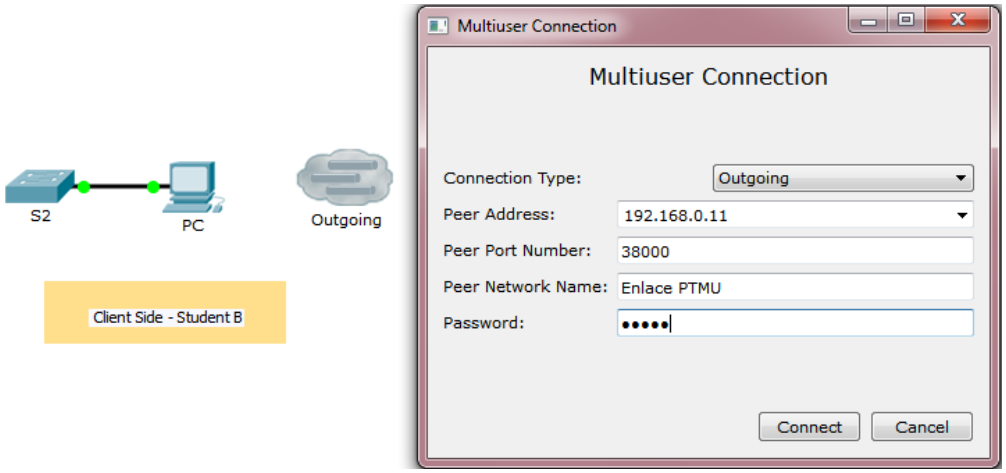
c. Haga clic en la nube de **Peer0** y cambie Connection Type por **Outgoing** (Saliente).

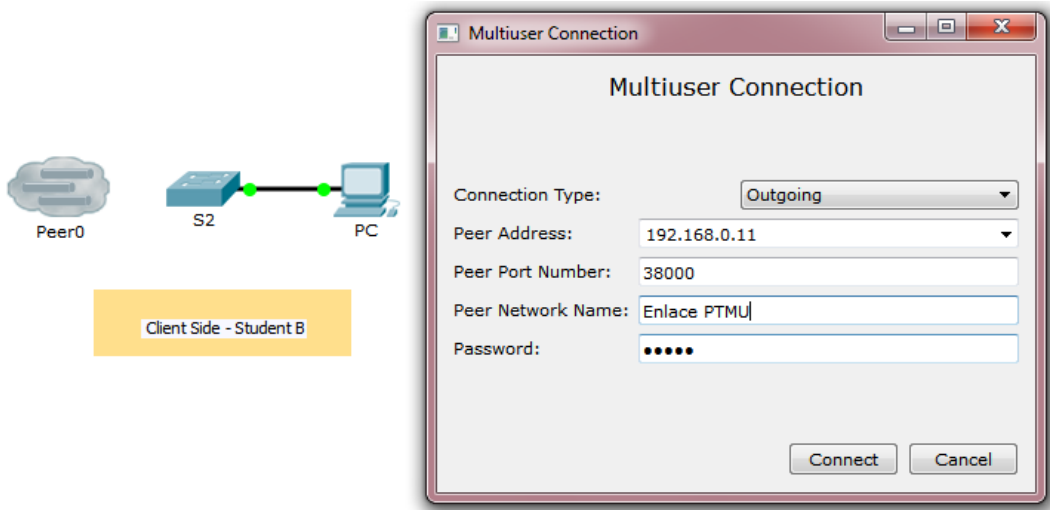




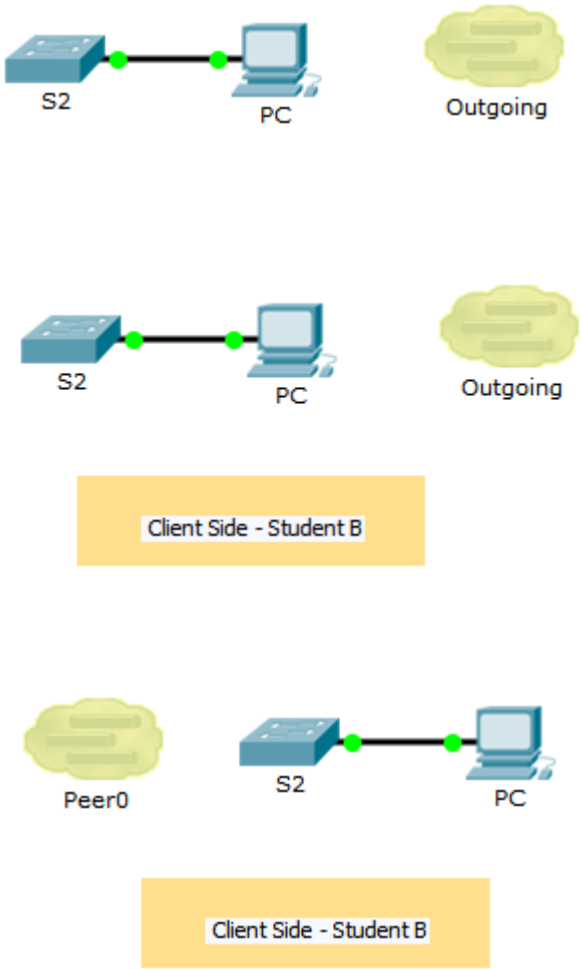
1) En el campo Peer Address (Dirección del punto), introduzca la dirección IP del lado servidor que registró en el paso 3a.
2) En el campo Peer Port Number (Número de puerto del punto), introduzca el número de puerto del lado servidor que registró en el paso 3a.
3) En el campo Peer Network Name (Nombre 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).


Multiuser Connection
Multiuser Connection
Connection Type:
Outgoing
Peer Address:
192.168.0.11
Peer Port Number:
38000
Peer Network Name:
Enlace PTMU
Password:
Connect
Cancel


S2
PC
Outgoing
Client Side - Student B
Multiuser Connection
Multiuser Connection
Connection Type:
Outgoing
Peer Address:
192.168.0.11
Peer Port Number:
38000
Peer Network Name:
Enlace PTMU
Password:
Connect
Cancel

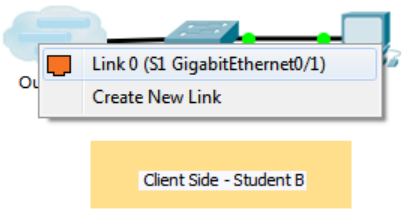


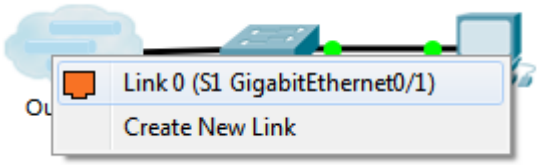
d. La nube de **Peer0** ahora debería ser amarilla, lo que indica que las dos instancias de Packet Tracer están conectadas.

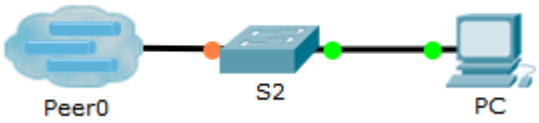


e. Haga clic en el ícono **Connections** (Conexiones) y elija la conexión negro sólido **Copper Straight-Through** (cable de cobre de conexión directa).

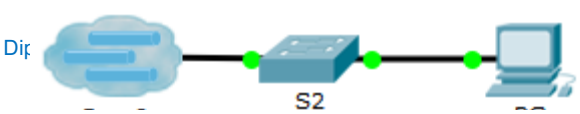
f. Haga clic en el **S2** y elija la conexión **GigabitEthernet0/1**. A continuación, haga clic en **Peer0** > **Link 0 (S1 GigabitEthernet 0/1)**.

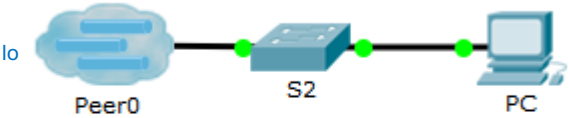






Tanto la nube de **Peer0** del jugador del lado cliente como la nube de **Enlace PTMU** del jugador del lado servidor ahora deben ser azules. Después de un período breve, la luz de enlace entre el switch y la nube pasa de color ámbar a verde.



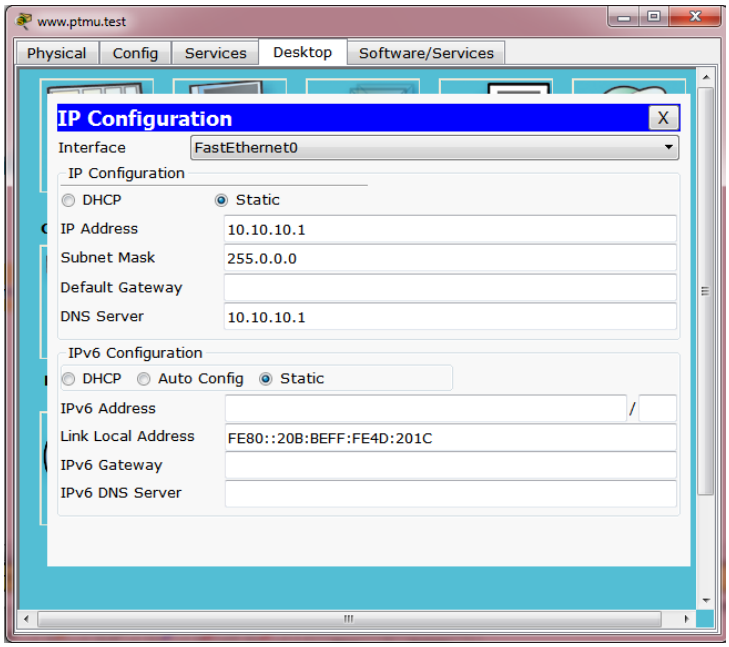


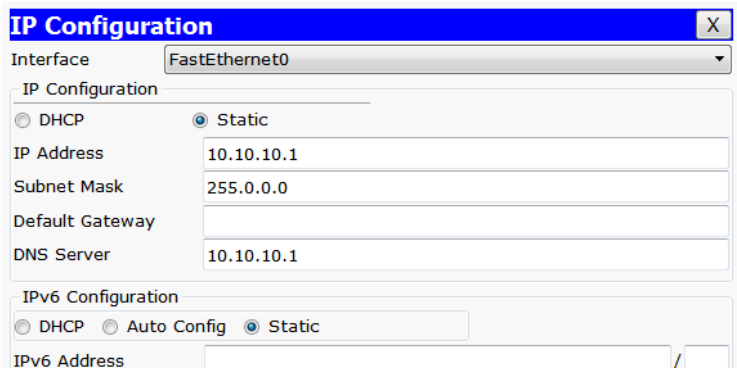
El enlace de multiusuario está establecido y listo para probar.

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

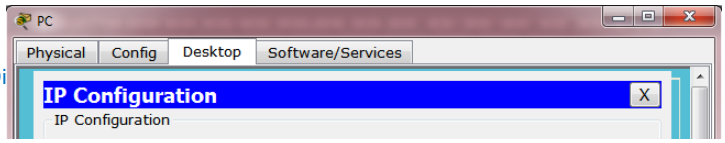
Paso 1: Configurar el direccionamiento IP

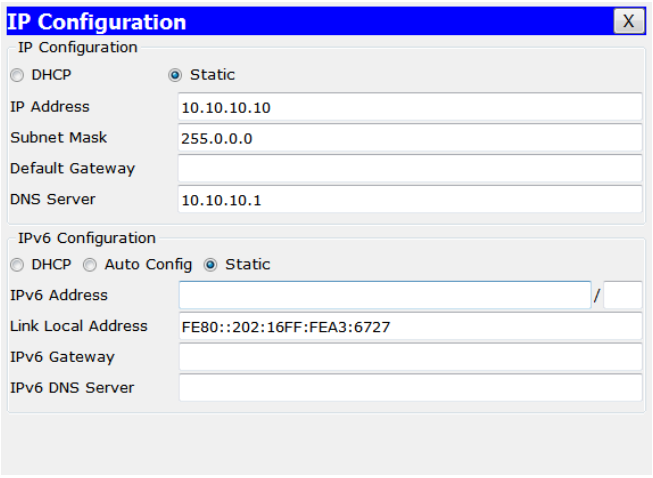
a. El jugador del lado servidor configura el servidor de **www.ptmu.test** con la dirección IP **10.10.10.1**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.





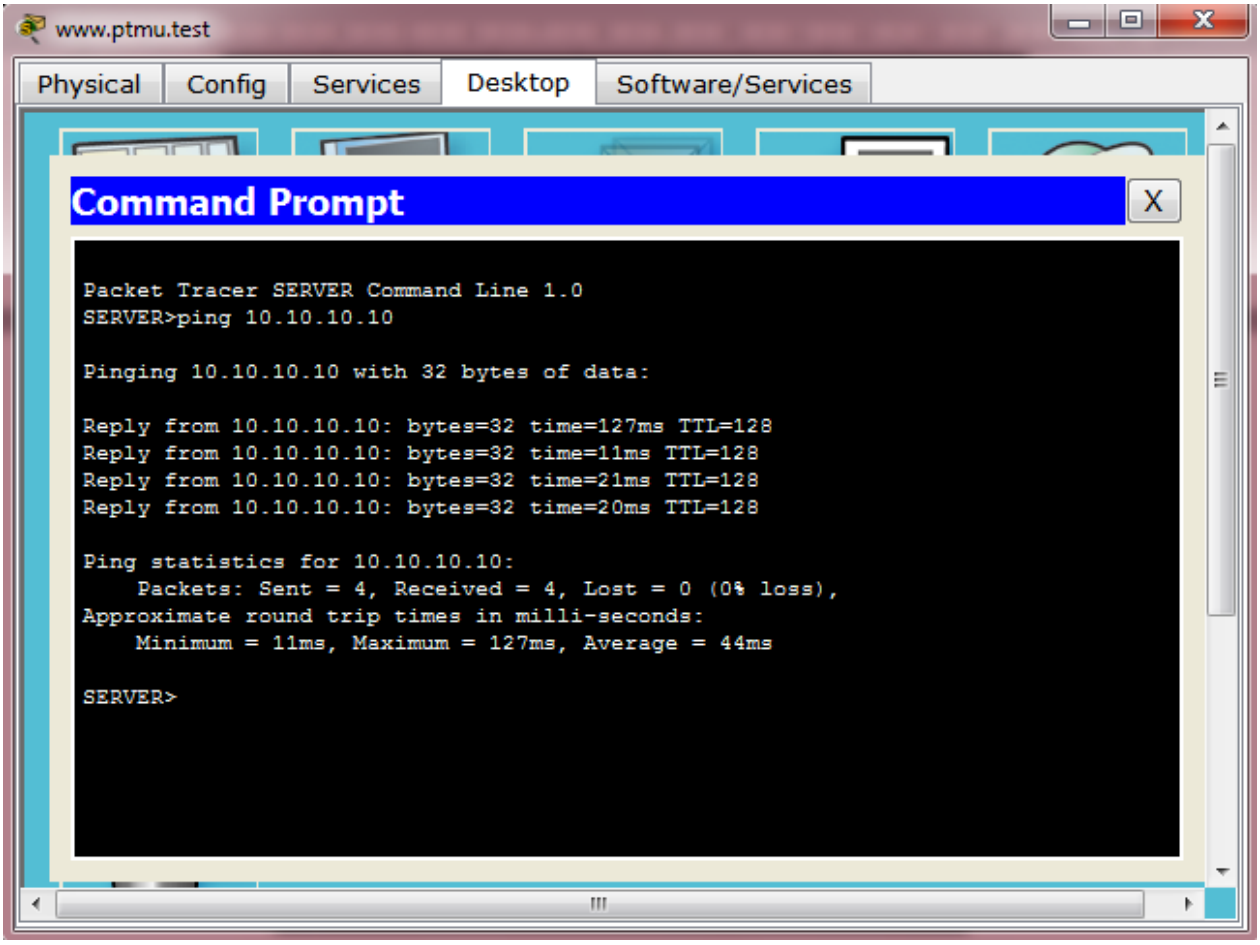
b. El jugador del lado cliente configura la PC con la dirección IP **10.10.10.10**, la máscara de subred **255.0.0.0** y la dirección de servidor DNS **10.10.10.1**.

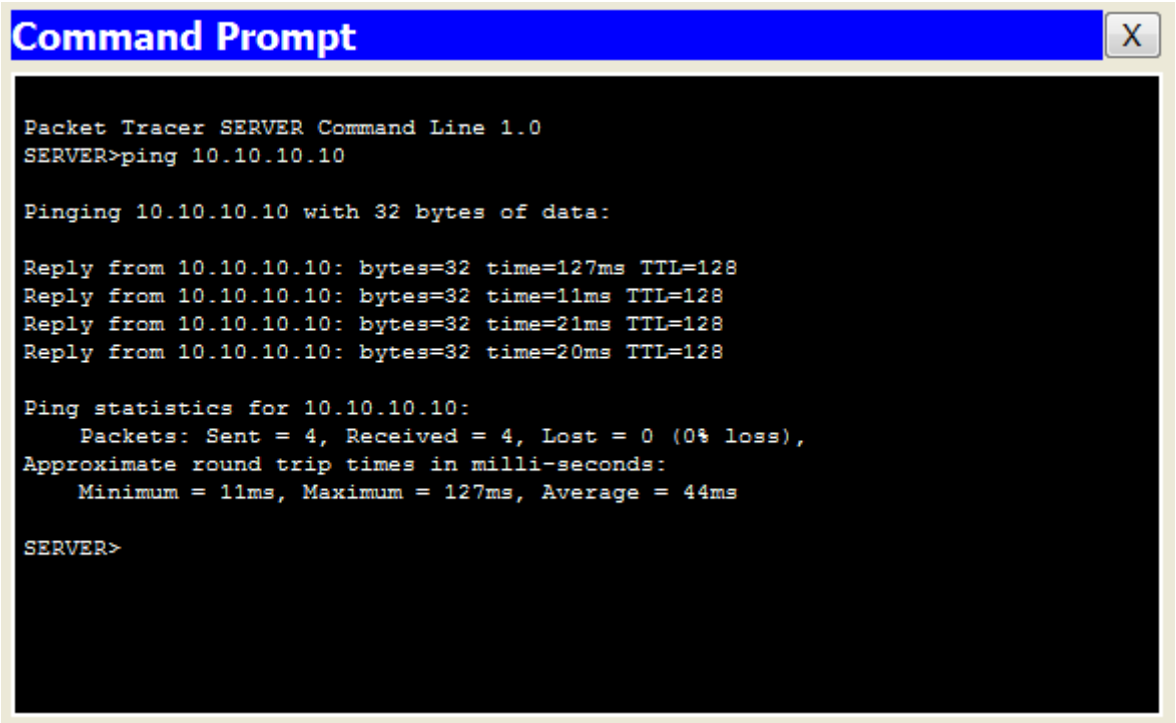




Paso 2: Verificar la conectividad y acceder a una página Web desde el lado servidor

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.





Packet Tracer SERVER Command Line 1.0
SERVER>ping 10.10.10.10

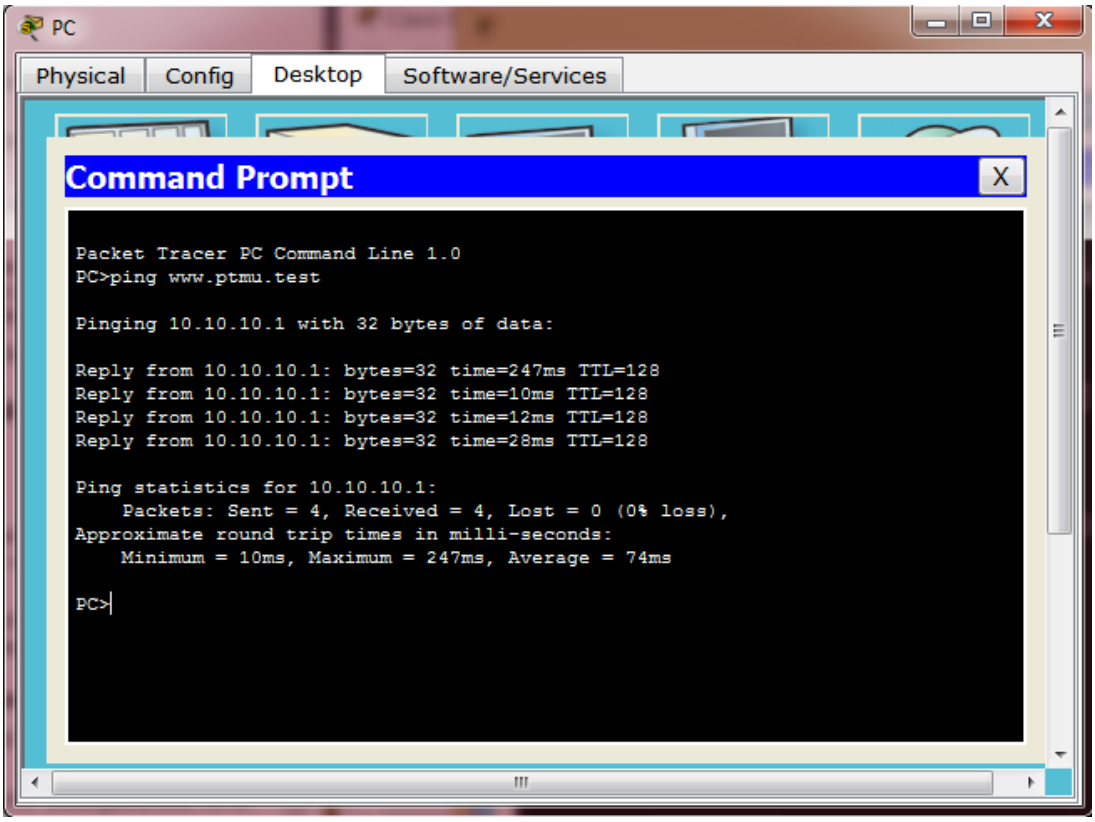
Pinging 10.10.10.10 with 32 bytes of data:

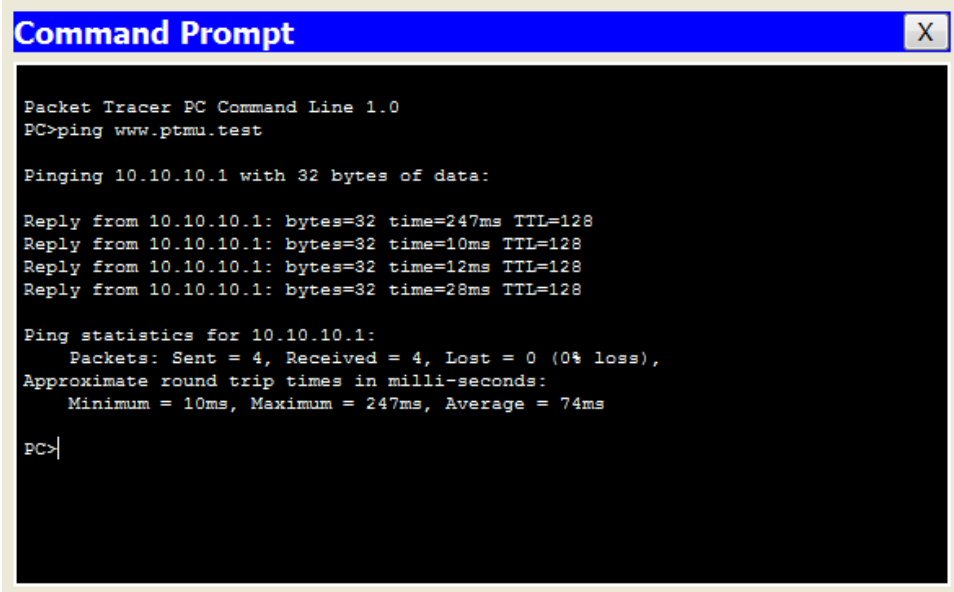
Reply from 10.10.10.10: bytes=32 time=127ms TTL=128
Reply from 10.10.10.10: bytes=32 time=11ms TTL=128
Reply from 10.10.10.10: bytes=32 time=21ms TTL=128
Reply from 10.10.10.10: bytes=32 time=20ms TTL=128

Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 127ms, Average = 44ms

SERVER>

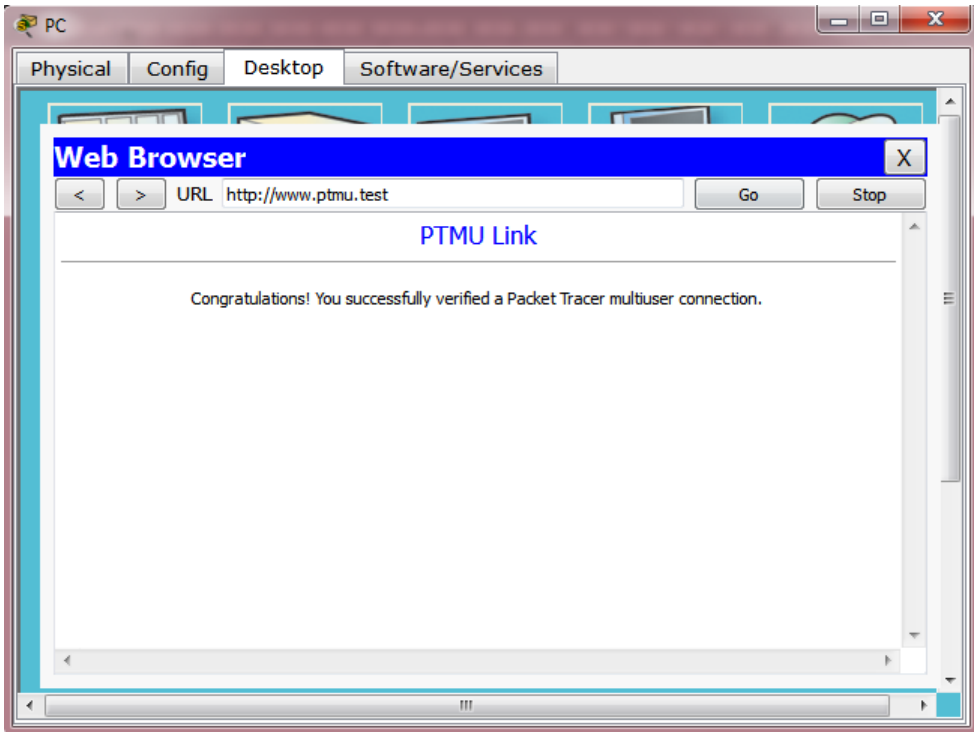
b. El jugador del lado cliente ahora debe poder hacer ping al servidor de **www.ptmu.test**.

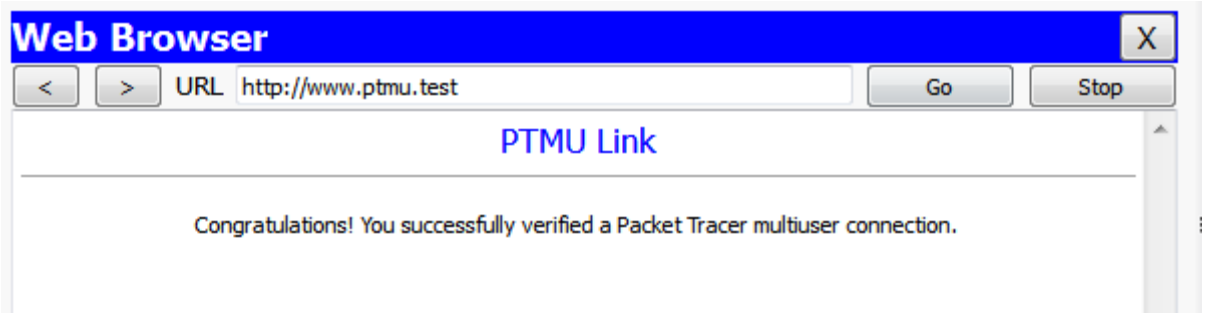

PC
Physical
Config
Desktop
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping www.ptmu.test
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=247ms TTL=128
Reply from 10.10.10.1: bytes=32 time=10ms TTL=128
Reply from 10.10.10.1: bytes=32 time=12ms TTL=128
Reply from 10.10.10.1: bytes=32 time=28ms TTL=128
Ping statistics for 10.10.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 247ms, Average = 74ms
PC>


Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping www.ptmu.test
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=247ms TTL=128
Reply from 10.10.10.1: bytes=32 time=10ms TTL=128
Reply from 10.10.10.1: bytes=32 time=12ms TTL=128
Reply from 10.10.10.1: bytes=32 time=28ms TTL=128
Ping statistics for 10.10.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 247ms, Average = 74ms
PC>

```
Packet Tracer PC Command Line 1.0
PC>ping www.ptmu.test

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=247ms TTL=128
Reply from 10.10.10.1: bytes=32 time=10ms TTL=128
Reply from 10.10.10.1: bytes=32 time=12ms TTL=128
Reply from 10.10.10.1: bytes=32 time=28ms TTL=128

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 247ms, Average = 74ms

PC>
```

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




Web Browser
X
<
>
URL
http://www.ptmu.test
Go
Stop
PTMU Link
Congratulations! You successfully verified a Packet Tracer multiuser connection.

Laboratorio 10.4.1.3

Función Multiusuario de Packet Tracer: Implementación de servicios

(versión para el instructor)..

Topología

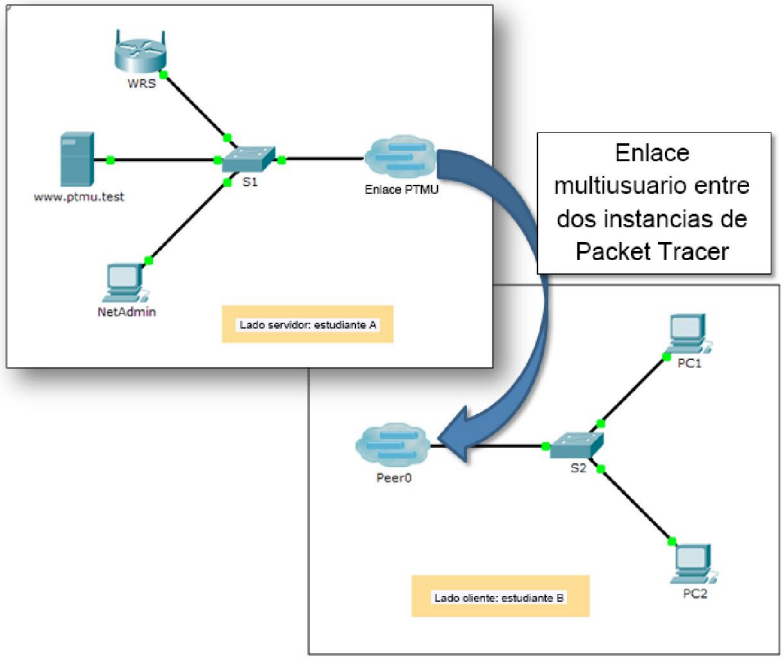


Tabla de direccionamiento

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

Información básica

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

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

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

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

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

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

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

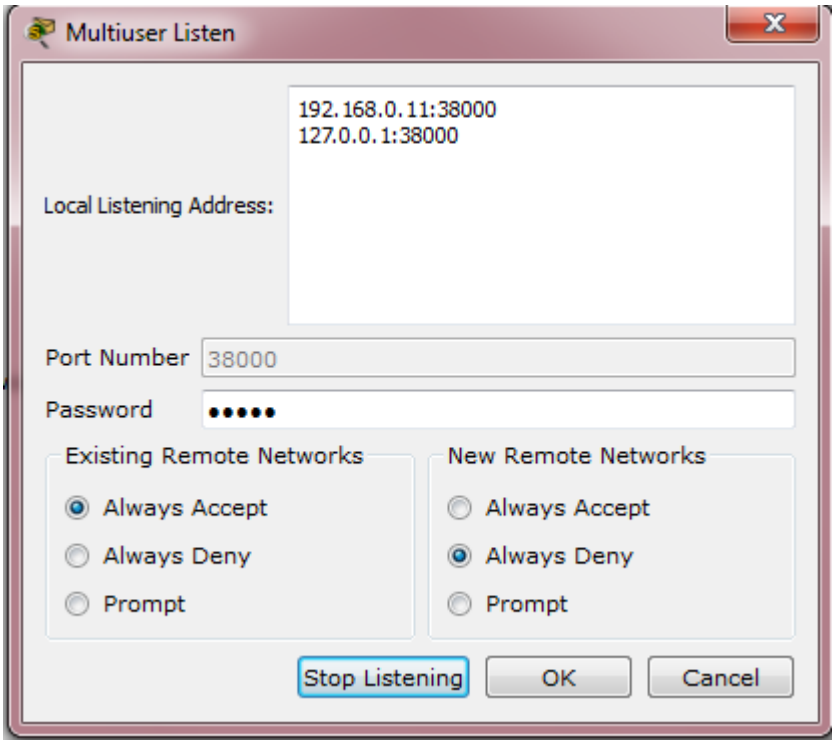
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los switches

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

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

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



a. Complete los pasos necesarios para verificar que el **enlace PTMU** esté listo para recibir una conexión entrante.

b. Comunique la información de configuración necesaria al jugador del lado cliente.

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

a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor:

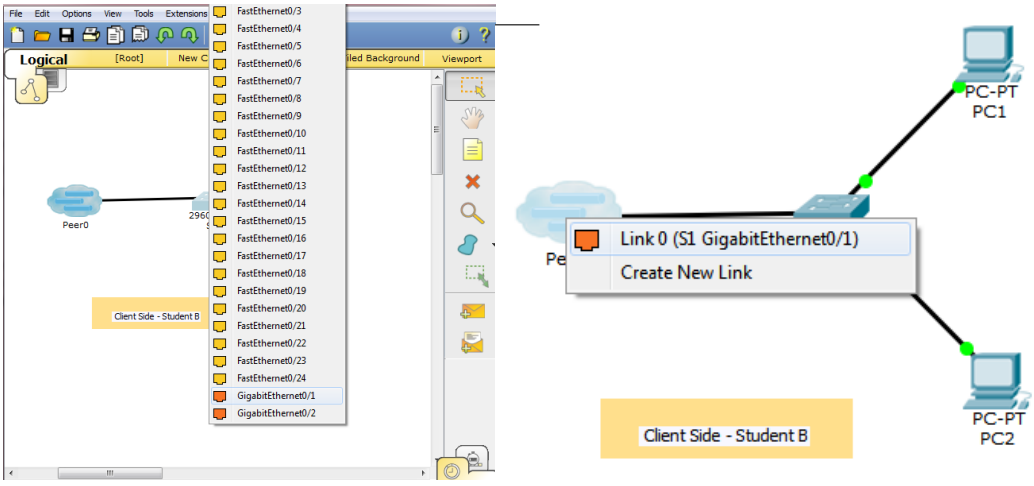
Dirección IP: 192.168.0.11

Número de puerto: 38000

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

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

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



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

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

```
S1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/23/34 ms

S1#
```

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

```
S2#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/27 ms

S2#
```

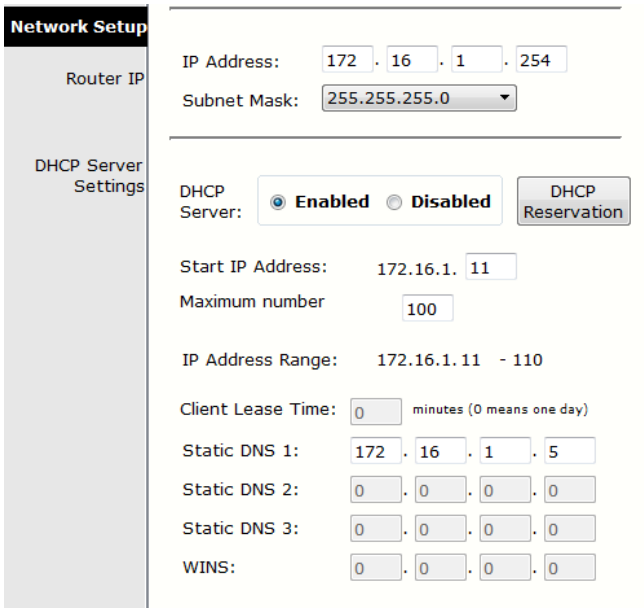
S2#ping 172.16.1.1

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

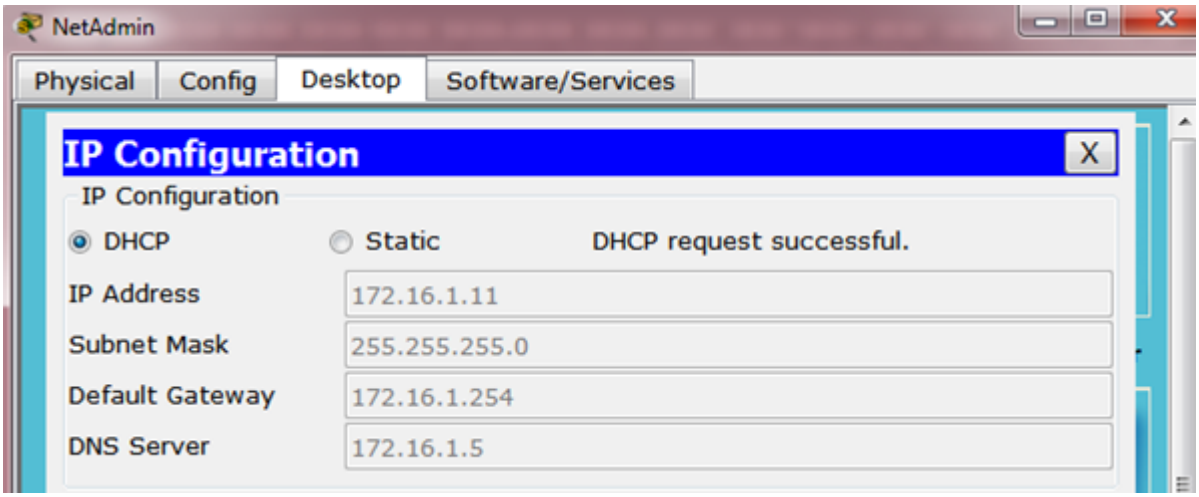
Paso 1: Configurar WRS como servidor de DHCP

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

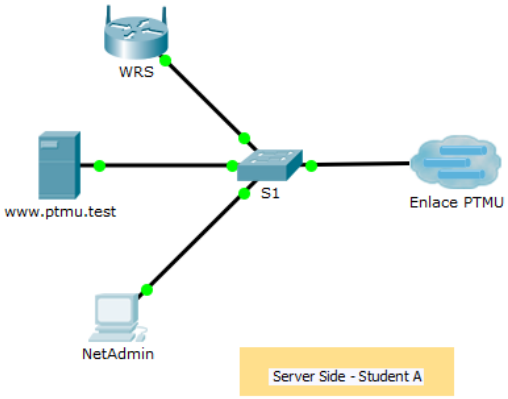
- La dirección IP de inicio es 172.16.1.11.
- La cantidad máxima de usuarios es 100.
- El DNS 1 estático es 172.16.1.5.

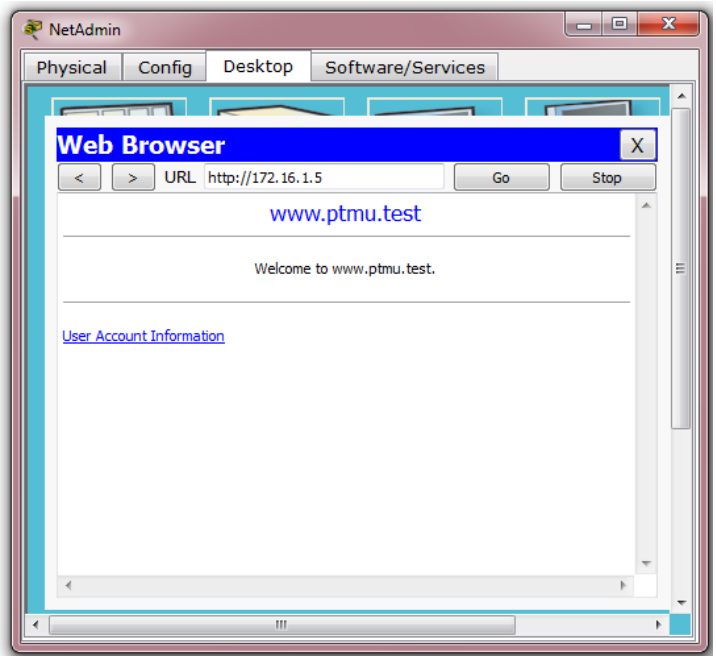


- Verifique si **NetAdmin** recibió el direccionamiento IP mediante DHCP.



- En **NetAdmin**, acceda a la página Web User Account Information (Información de cuenta de usuario) en **172.16.1.5**. Utilizará esta información para configurar las cuentas de usuario en el paso 2.

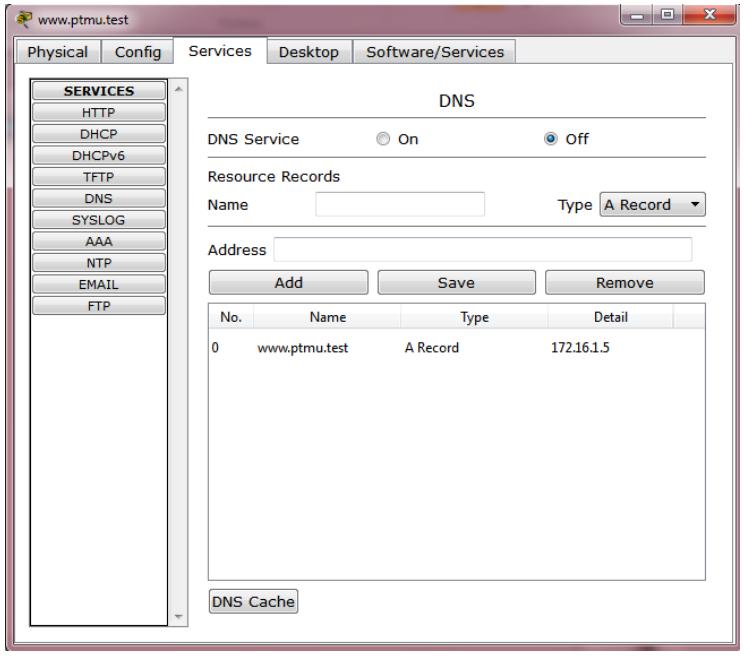




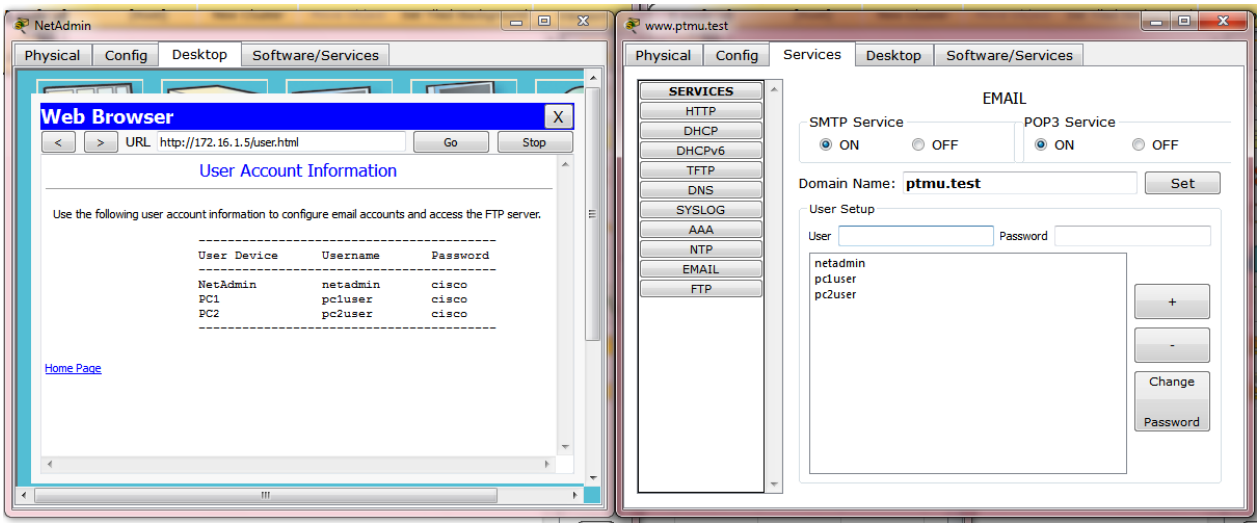
Paso 2: Configurar servicios en www.ptmu.test

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

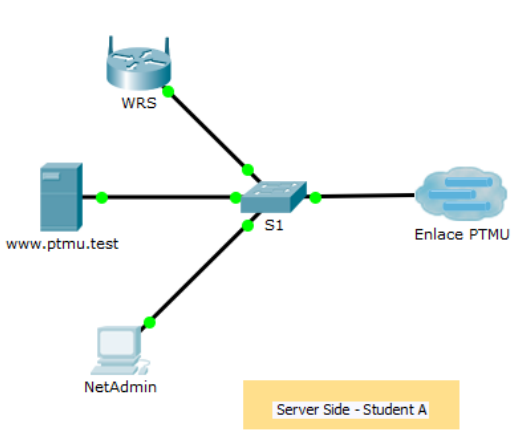
- Un registro DNS que asocie la dirección IP del servidor **www.ptmu.test** al nombre www.ptmu.test.

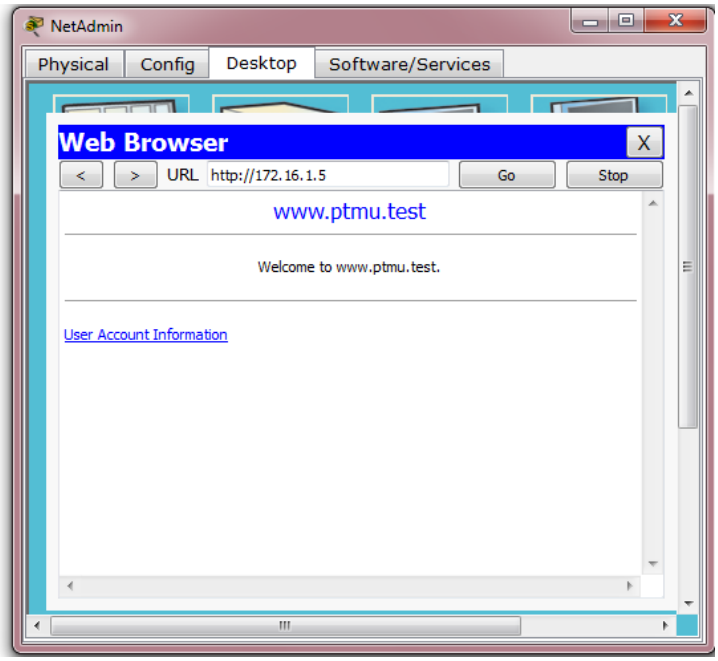


- Cuentas de usuario y servicios de correo electrónico según la lista de usuarios. El nombre de dominio es **ptmu.test.**



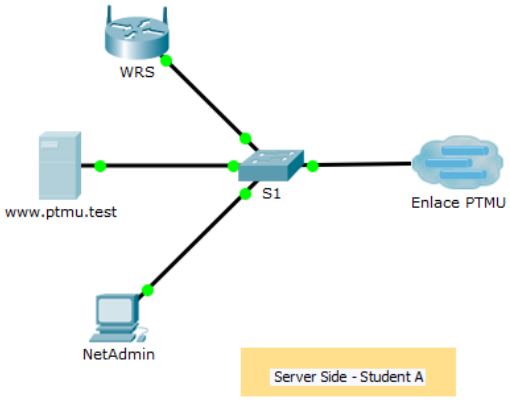
- Cuentas de usuario y servicios FTP según la lista de usuarios. Otorgue permiso a cada usuario para escribir, leer y enumerar.

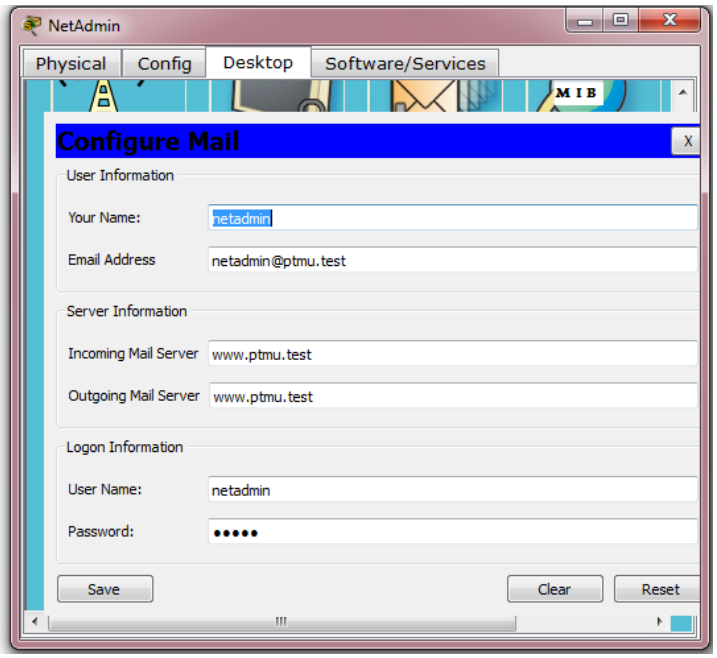




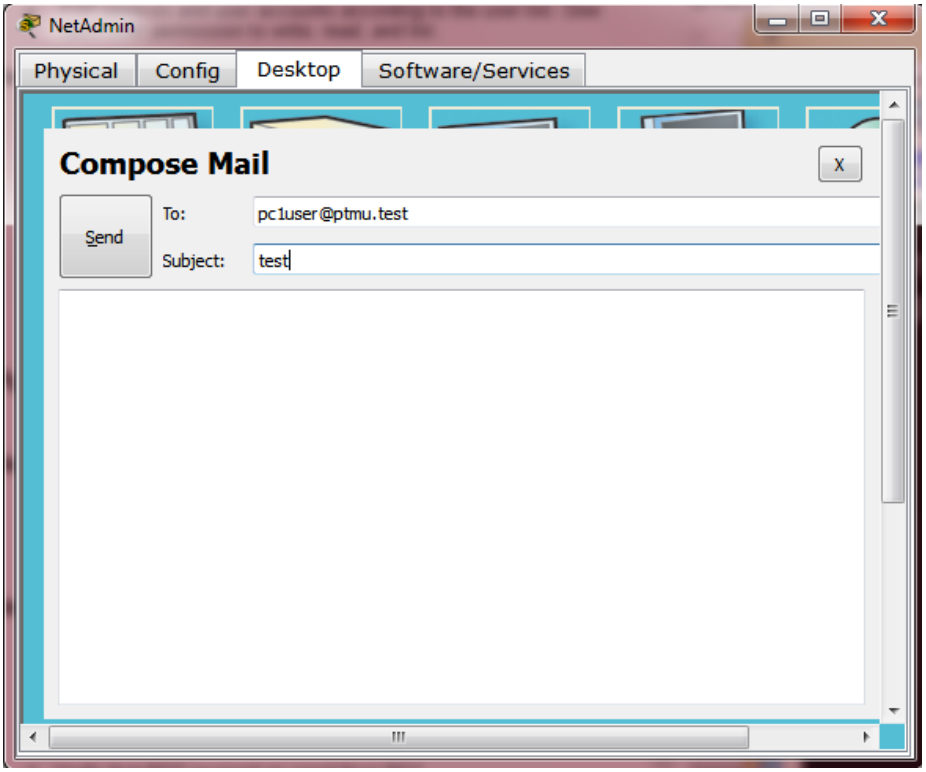
Paso 3: Verificar que todos los servicios estén implementados de acuerdo con los requisitos En **NetAdmin**, realice lo siguiente:

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

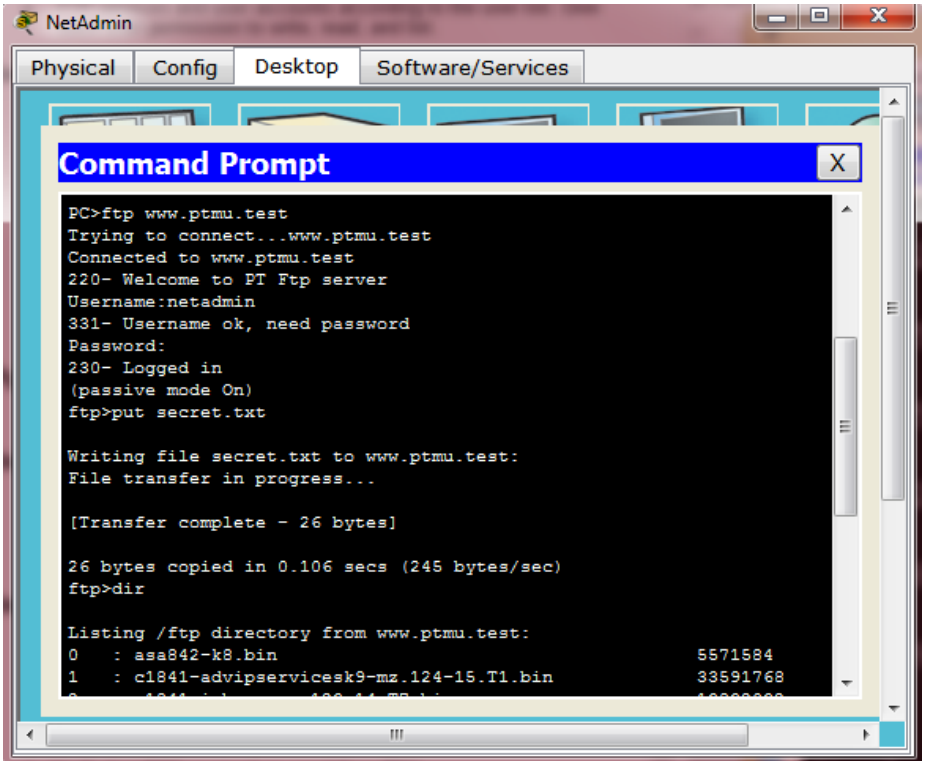




- Envíe un correo electrónico al usuario de la **PC1**.



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

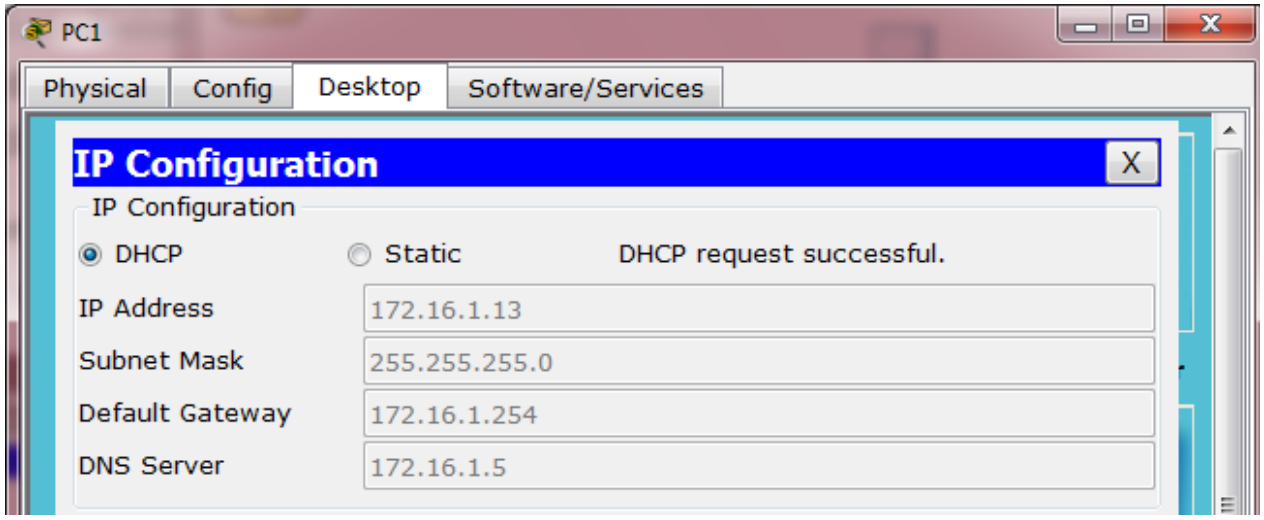


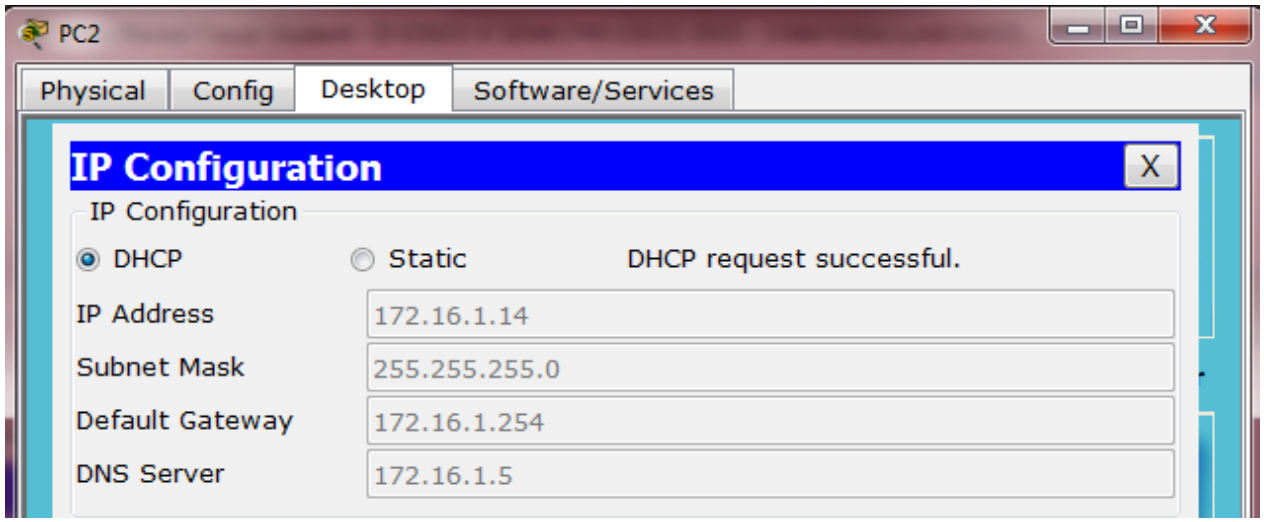
Nota: la puntuación para el jugador del lado servidor será de **43/44** hasta que el jugador del lado cliente descargue correctamente el archivo **secret.txt**, lo modifique y lo suba al servidor FTP **www.ptmu.test**.

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

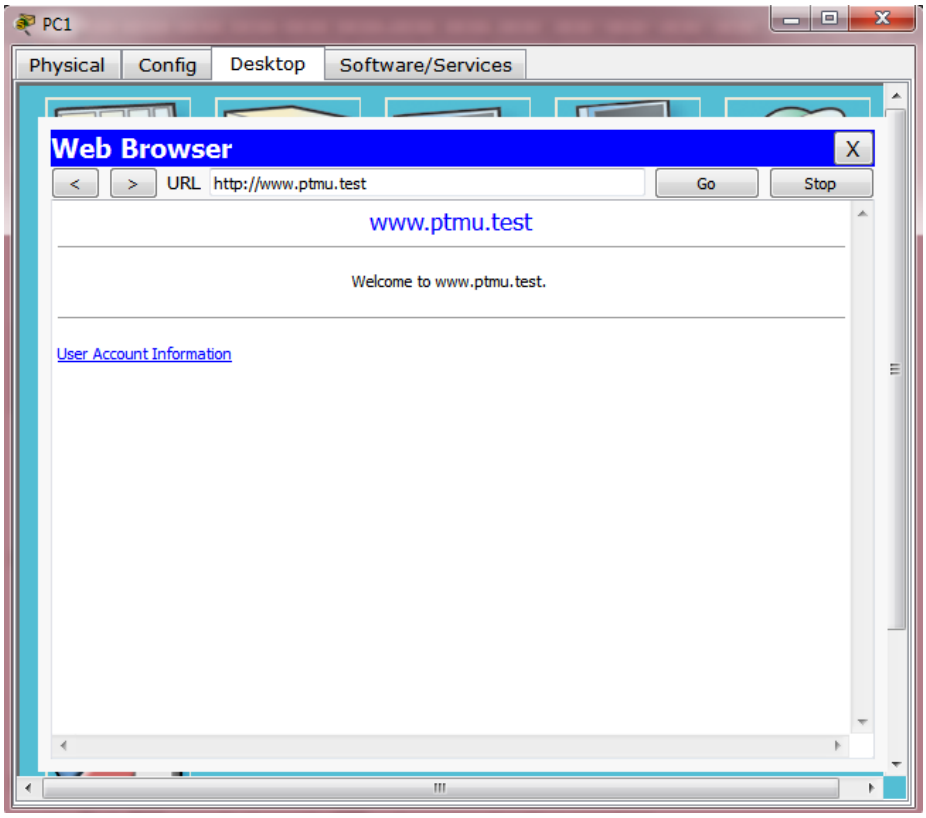
Paso 1: Configurar y verificar el direccionamiento de las PC

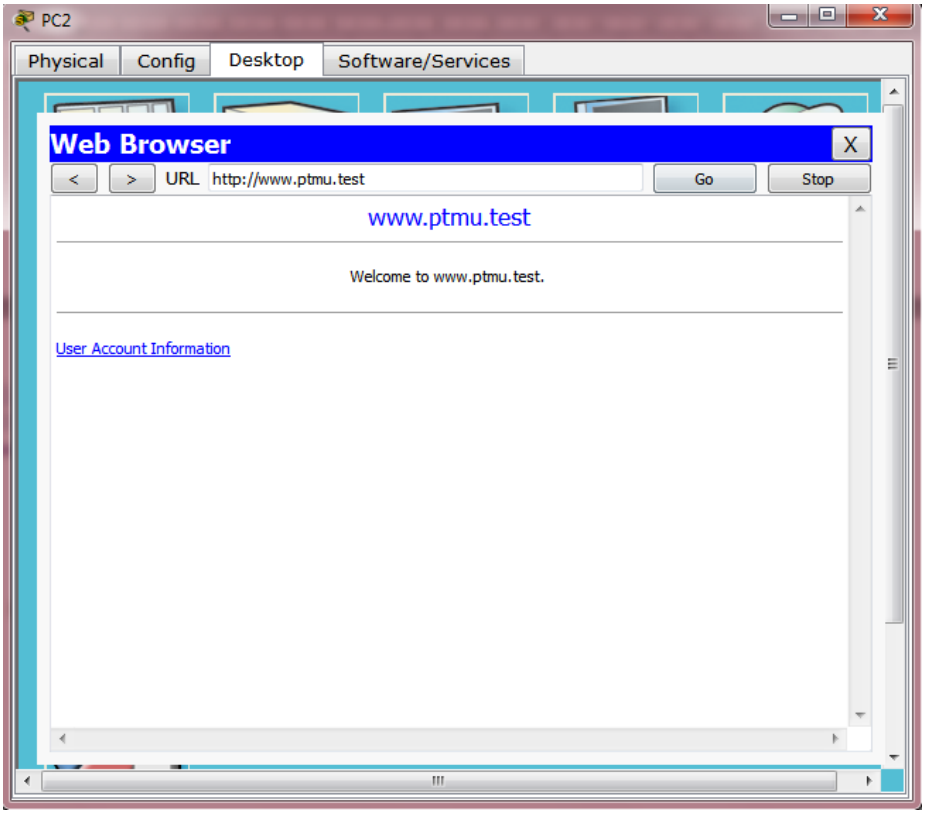
a. Configure la **PC1** y **la PC2** para obtener el direccionamiento automáticamente.

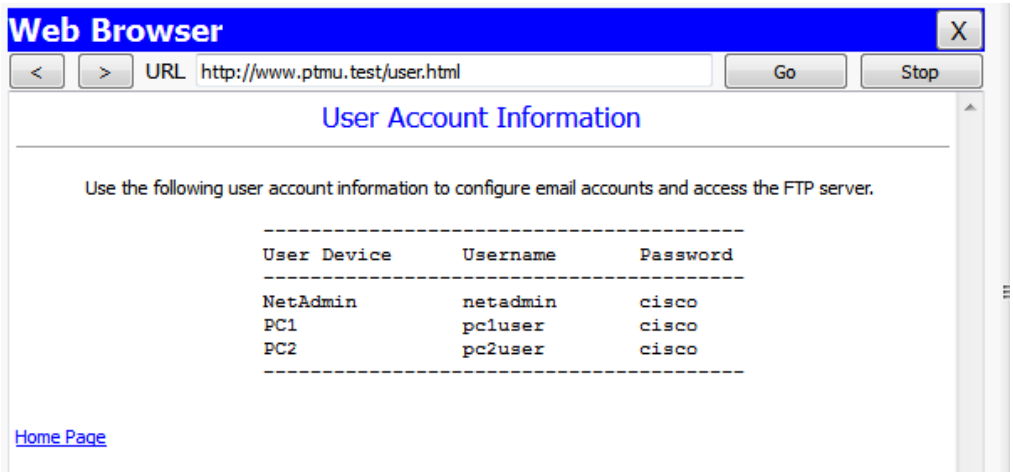




b. Las PC1 y PC2 deben poder acceder a la página Web **http://www.ptmu.test**.

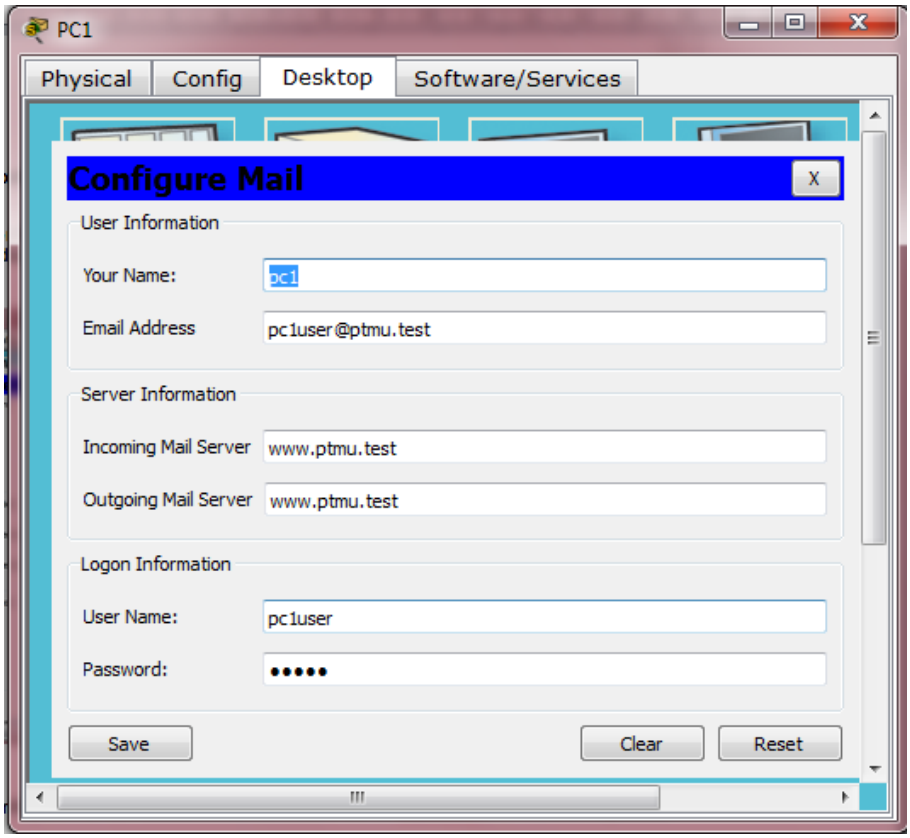

PC1
Physical
Config
Desktop
Software/Services
Web Browser
X
URL
http://www.ptmu.test
Go
Stop
www.ptmu.test
Welcome to www.ptmu.test.
User Account Information


PC2
Physical
Config
Desktop
Software/Services
Web Browser
X
URL
http://www.ptmu.test
Go
Stop
www.ptmu.test
Welcome to www.ptmu.test.
User Account Information

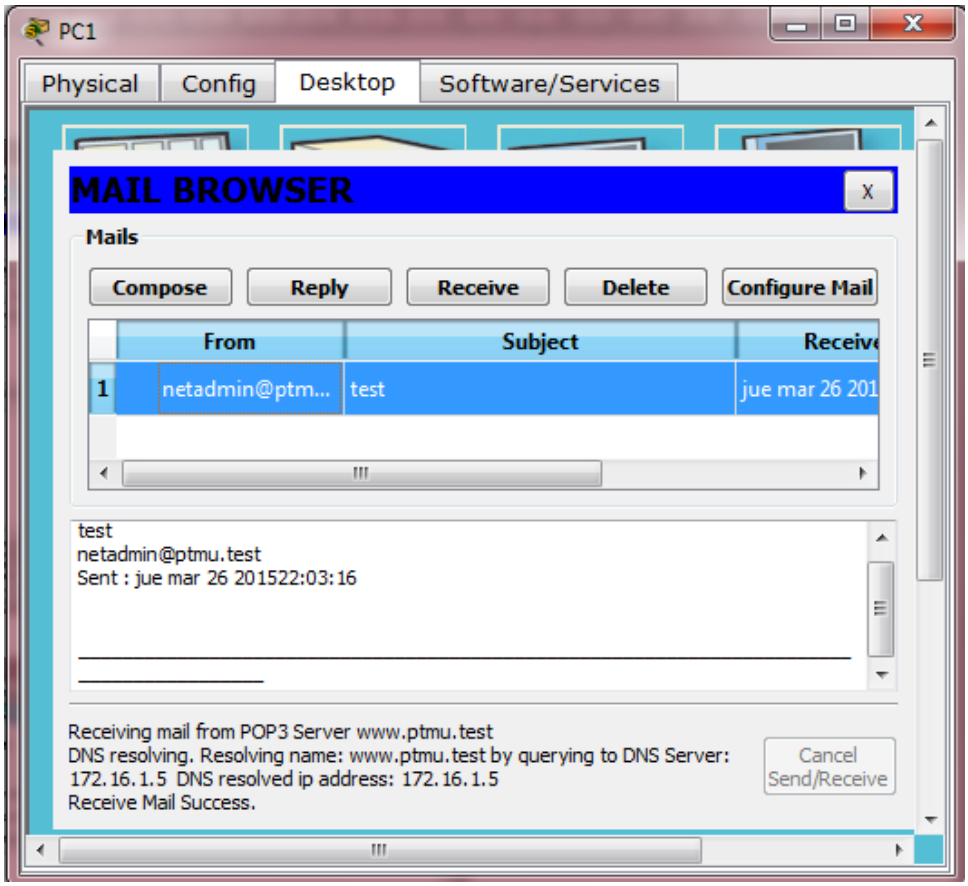


Paso 2: Configurar y verificar las cuentas de correo electrónico de las PC

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

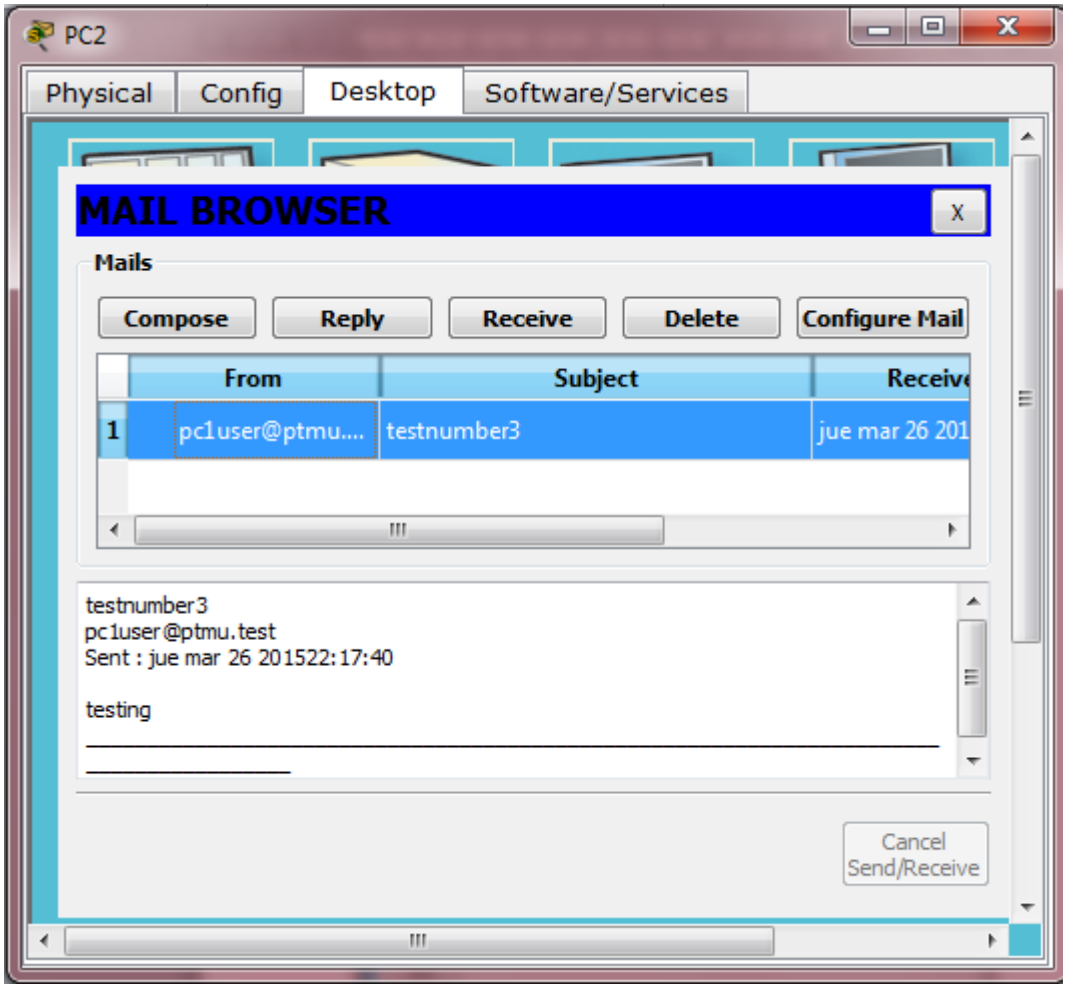


b. Verifique si la PC1 recibió un correo electrónico de NetAdmin y envíe una respuesta.



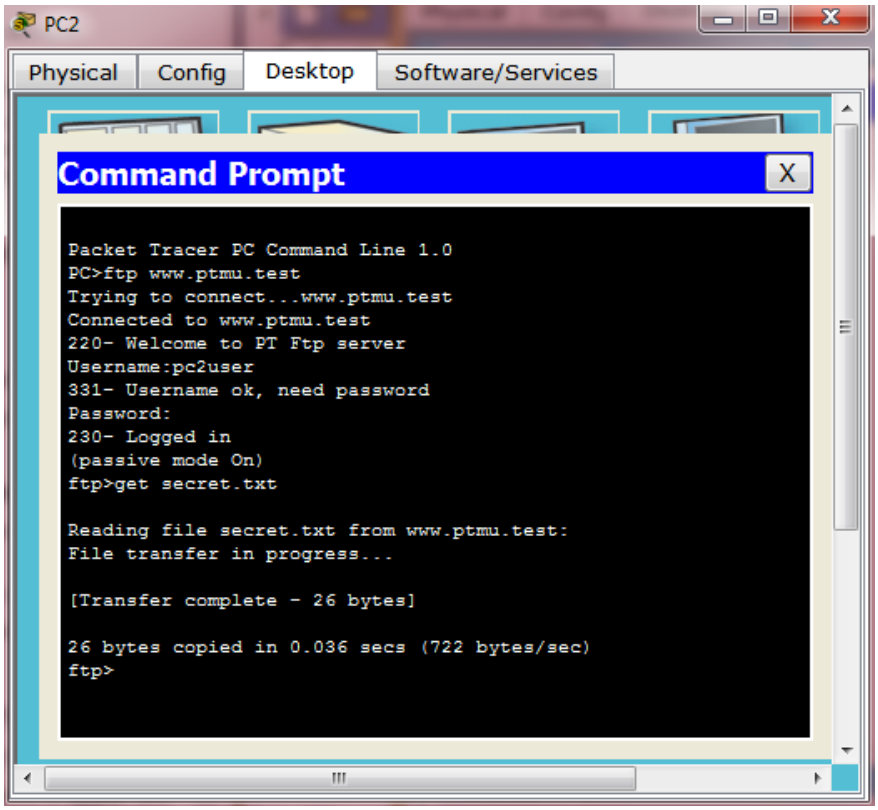
c. Envíe un correo electrónico de la PC1 a la PC2. **Nota:** la puntuación no cambiará.

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

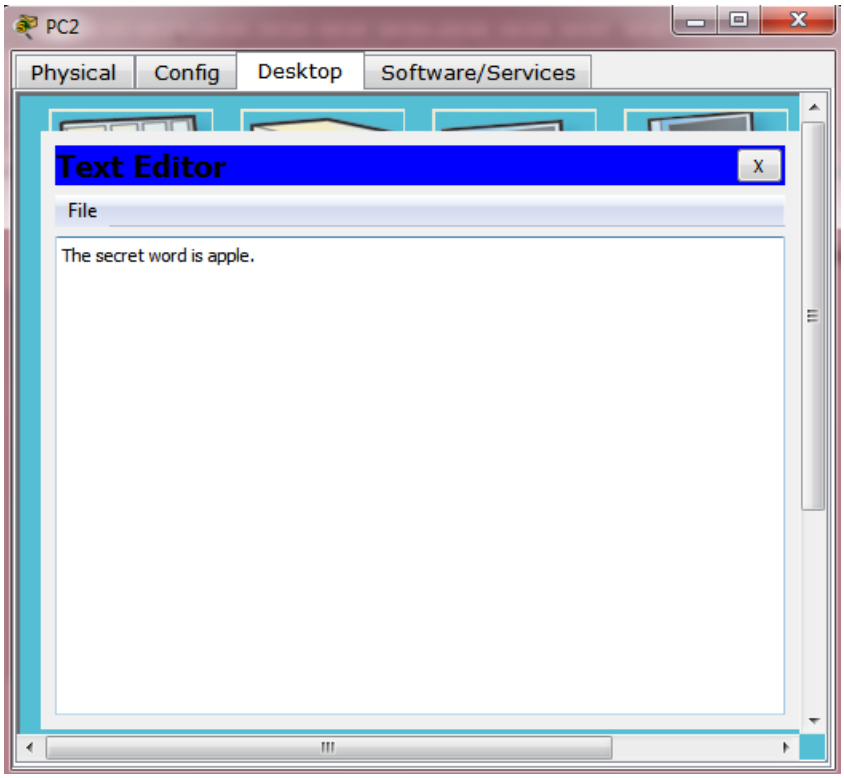


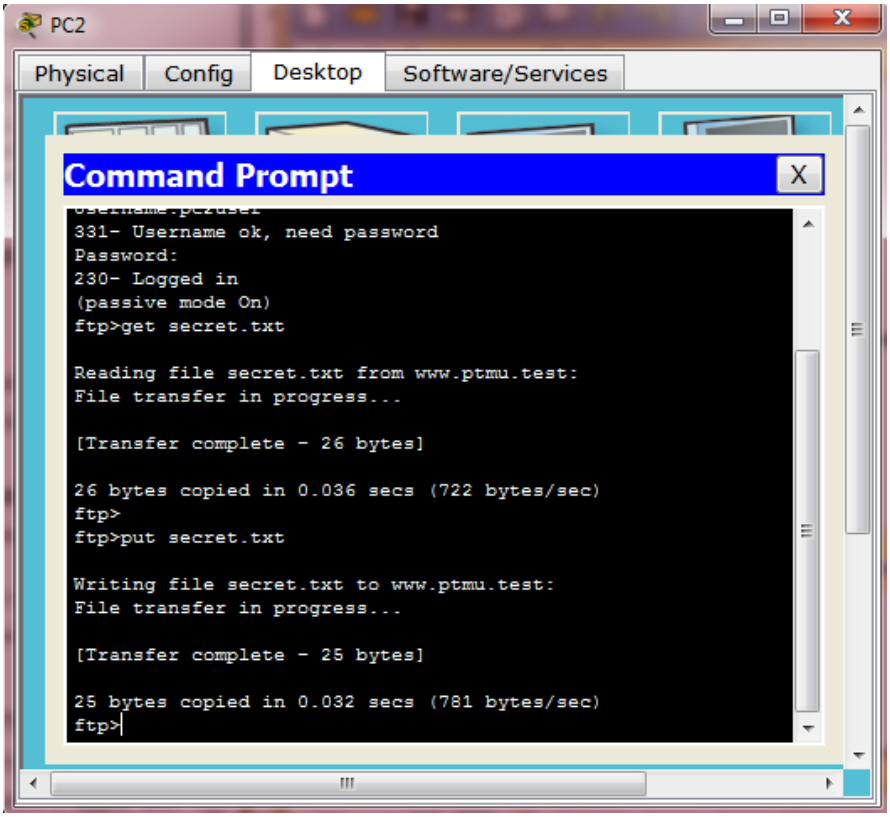
Paso 3: Subir un archivo al servidor FTP y descargarlo de dicho servidor

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

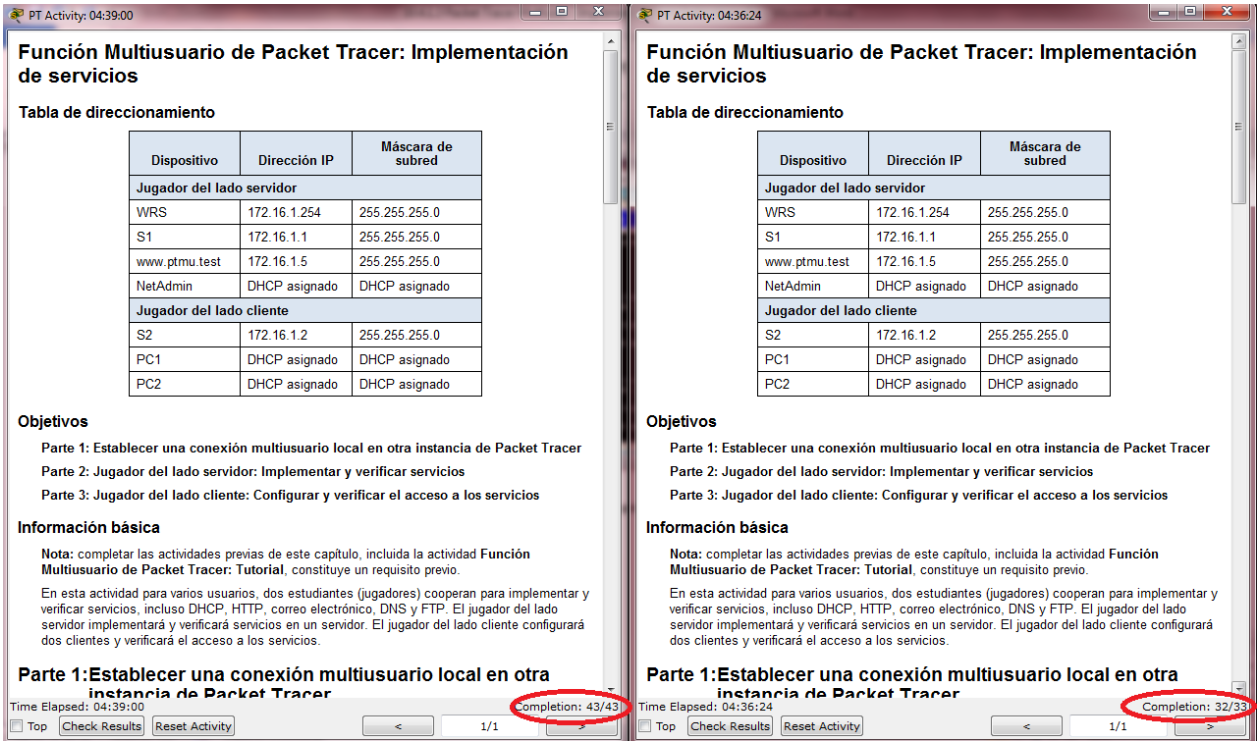


b. Abra el archivo **secret.txt**, solo cambie la palabra secreta por **apple** y suba el archivo.


PC2
Physical
Config
Desktop
Software/Services
Text Editor
X
File
The secret word is apple.


PC2
Physical
Config
Desktop
Software/Services
Command Prompt
X
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get secret.txt
Reading file secret.txt from www.ptmu.test:
File transfer in progress...
[Transfer complete - 26 bytes]
26 bytes copied in 0.036 secs (722 bytes/sec)
ftp>
ftp>put secret.txt
Writing file secret.txt to www.ptmu.test:
File transfer in progress...
[Transfer complete - 25 bytes]
25 bytes copied in 0.032 secs (781 bytes/sec)
ftp>

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



PT Activity: 04:39:00

Función Multiusuario de Packet Tracer: Implementación de servicios

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

Información básica

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

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

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

Time Elapsed: 04:39:00 Completion: 43/43

Top Check Results Reset Activity < 1/1 >

PT Activity: 04:36:24

Función Multiusuario de Packet Tracer: Implementación de servicios

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

Información básica

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

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

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

Time Elapsed: 04:36:24 Completion: 32/33

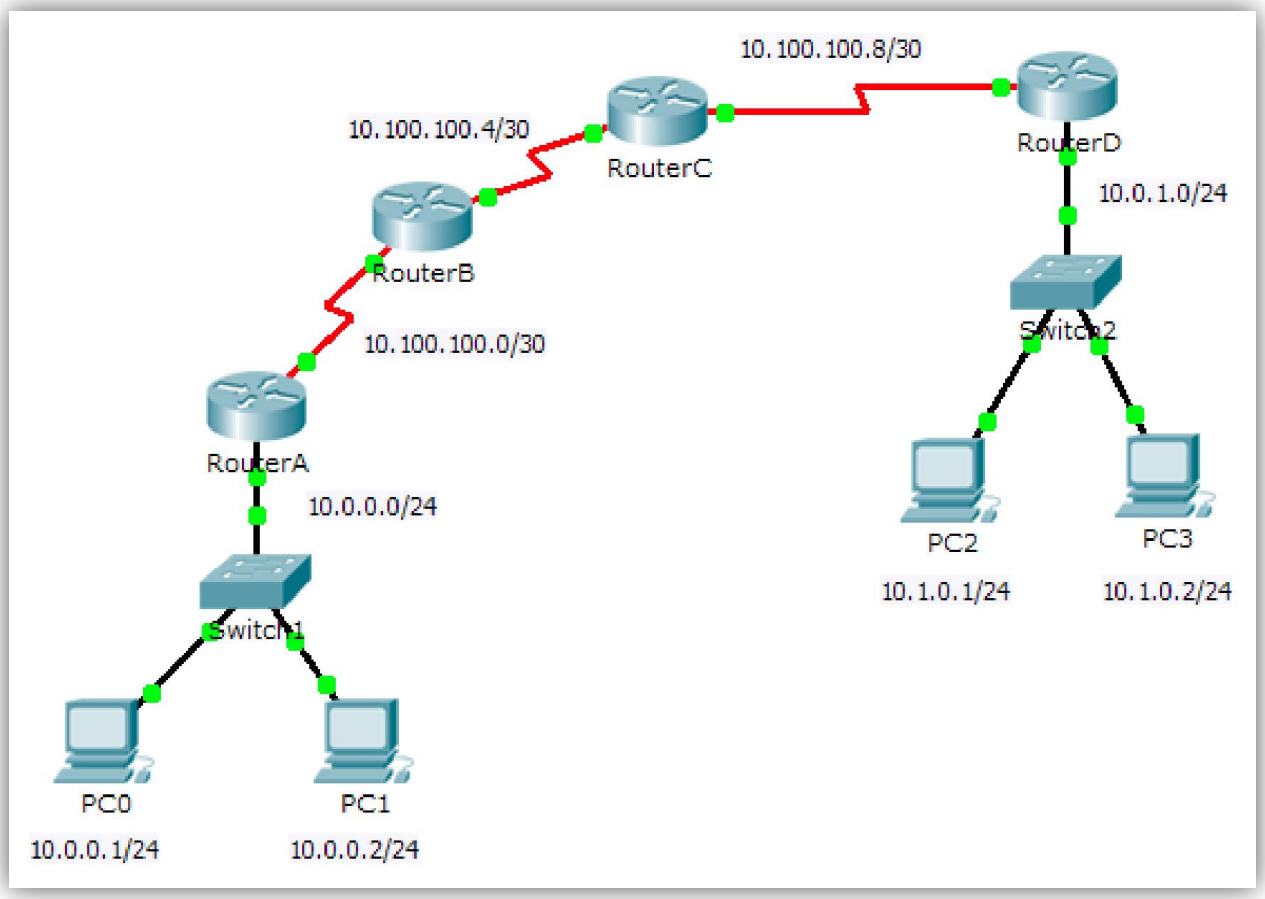
Top Check Results Reset Activity < 1/1 >

Laboratorio 11.3.2.2

Packet Tracer: Prueba de la conectividad con traceroute (versión para el instructor).

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

- Parte 1: Probar la conectividad de extremo a extremo con el comando tracert
- Parte 2: Comparar con el comando traceroute en un router

Información básica

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

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

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

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

PC>ping 10.1.0.2

Pinging 10.1.0.2 with 32 bytes of data:

Reply from 10.100.100.6: Destination host unreachable.

Reply from 10.100.100.6: Destination host unreachable.

Reply from 10.100.100.6: Destination host unreachable.

Reply from 10.100.100.6: Destination host unreachable.

Ping statistics for 10.1.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

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**.

PC>tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 10.0.0.254

2 0 ms 0 ms 0 ms 10.100.100.2

3 1 ms 0 ms 0 ms 10.100.100.6

4 11 ms * 11 ms 10.100.100.6

5 * 0 ms * Request timed out.

6 0 ms * 10 ms 10.100.100.6

7

Control-C

^C

PC>

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**?

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**?

10.100.100.6

Paso 3: Corregir el problema de red

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

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

c. ¿Cuál es el estado de las interfaces?

Parecen estar activas.

RouterC>enable

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

Vlan1 unassigned YES unset administratively down down

RouterC#

d. Compare las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo común?

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

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

Cambiar la dirección IP de la S0/0/0 a 10.100.100.9/30.

RouterC#config

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

RouterC(config)#interface s0/0/0

RouterC(config-if)#ip addres 10.100.100.9 255.255.255.252

RouterC(config-if)#no shutdown

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**.

PC>tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 10.0.0.254

2 1 ms 1 ms 0 ms 10.100.100.2

3 1 ms 0 ms 4 ms 10.100.100.6

4 2 ms 12 ms 2 ms 10.100.100.10

5 * 2 ms 2 ms 10.1.0.2

Trace complete.

PC>

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

Parte 2: Comparar con el comando traceroute en un router

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

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

RouterA>

RouterA>traceroute 10.1.0.2

Type escape sequence to abort.

Tracing the route to 10.1.0.2

1 10.100.100.2 32 msec 4 msec 9 msec

2 10.100.100.6 0 msec 5 msec 1 msec

3 10.100.100.10 1 msec 14 msec 1 msec

4 10.1.0.2 14 msec 3 msec 2 msec

RouterA>

b. Compare el resultado del comando **traceroute** del router con el del comando **tracert** de la PC. ¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió?
El router tiene una dirección IP menos, porque el próximo dispositivo que utilizará en la ruta será el RouterB.

```
PC>tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops:

  1    1 ms       0 ms       0 ms       10.0.0.254
  2    1 ms       1 ms       0 ms       10.100.100.2
  3    1 ms       0 ms       4 ms       10.100.100.6
  4    2 ms       12 ms      2 ms       10.100.100.10
  5    *          2 ms       2 ms       10.1.0.2

Trace complete.

PC>
```

```
RouterA>
RouterA>traceroute 10.1.0.2
Type escape sequence to abort.
Tracing the route to 10.1.0.2

  1    10.100.100.2     32 msec    4 msec     9 msec
  2    10.100.100.6     0 msec     5 msec     1 msec
  3    10.100.100.10    1 msec     14 msec    1 msec
  4    10.1.0.2         14 msec    3 msec     2 msec
RouterA>
```

Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 1: Probar la conectividad de extremo a extremo con el comando **tracert**	Paso 1	10	
	Paso 2b	10	
	Paso 2c	10	
	Paso 3a	10	
	Paso 3c	10	
	Paso 3d	10	
	Paso 3e	10	
	Paso 4b	10	
Total de la parte 1		**80**	
Parte 2: Comparar con el comando **traceroute** en un router	a	10	
	b	10	
Total de la parte 2		**20**	
Puntuación total		**100**	

Laboratorio 11.3.3.4

Packet Tracer: Uso de los comandos show (versión para el instructor)..

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Objetivos

- Parte 1: Analizar el resultado del comando show
- Parte 2: Preguntas de reflexión

Información básica

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

Parte 1: Analizar el resultado del comando show

Paso 1: Conectarse a ISPRouter

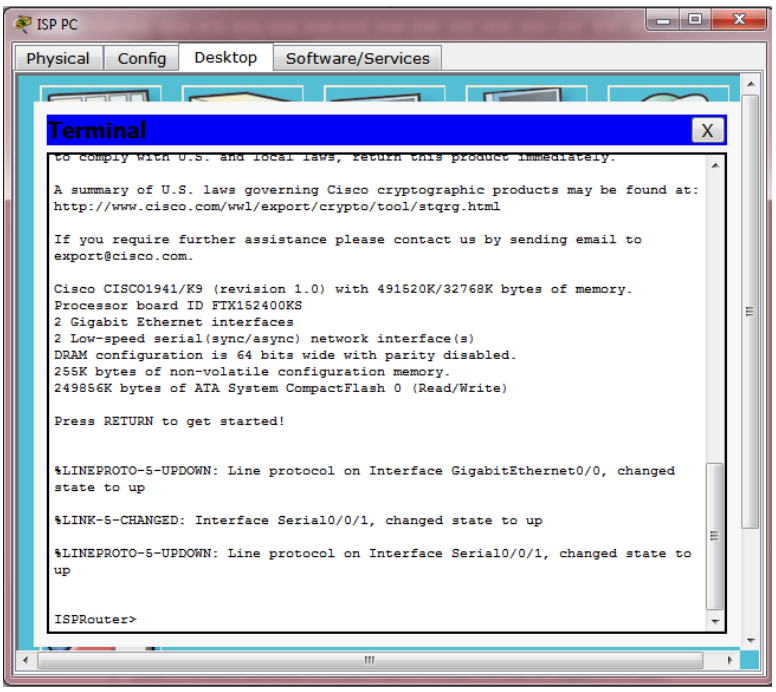
a. Haga clic en **PC ISP** y, a continuación, en la ficha **Desktop** (Escritorio), seguida de **Terminal**.

b. Ingrese al modo EXEC privilegiado.

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

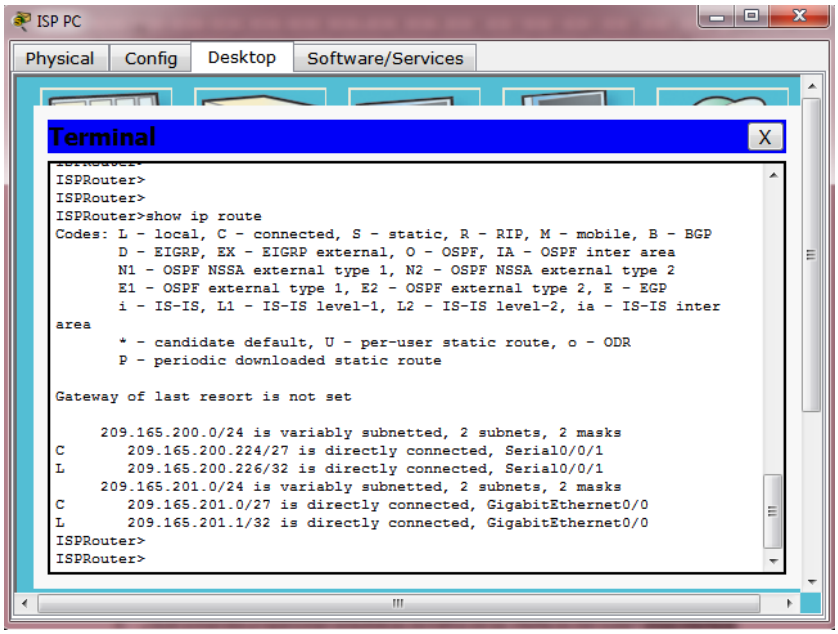
- `show arp`

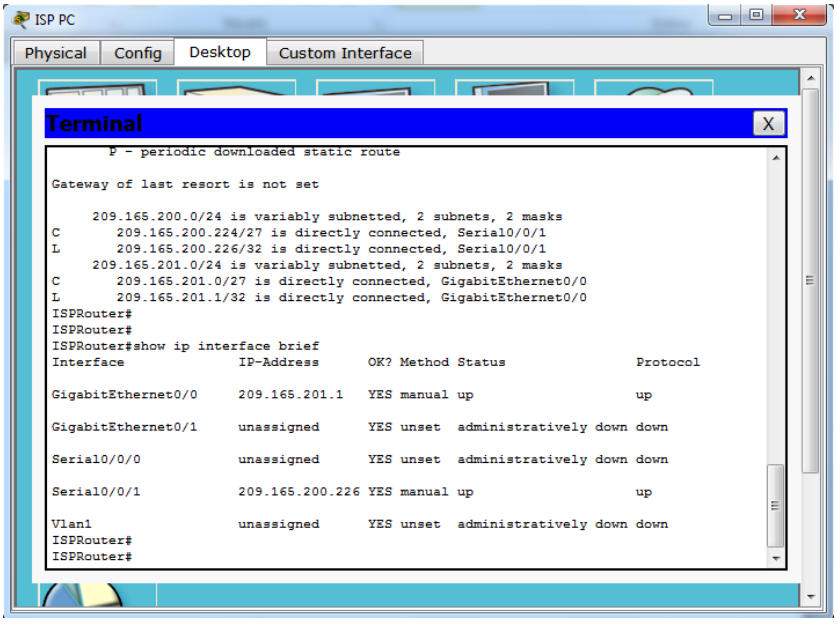
- `show flash:`
- `show ip route`
- `show interfaces`
- `show ip interface brief`
- `show protocols`
- `show users`
- `show version`

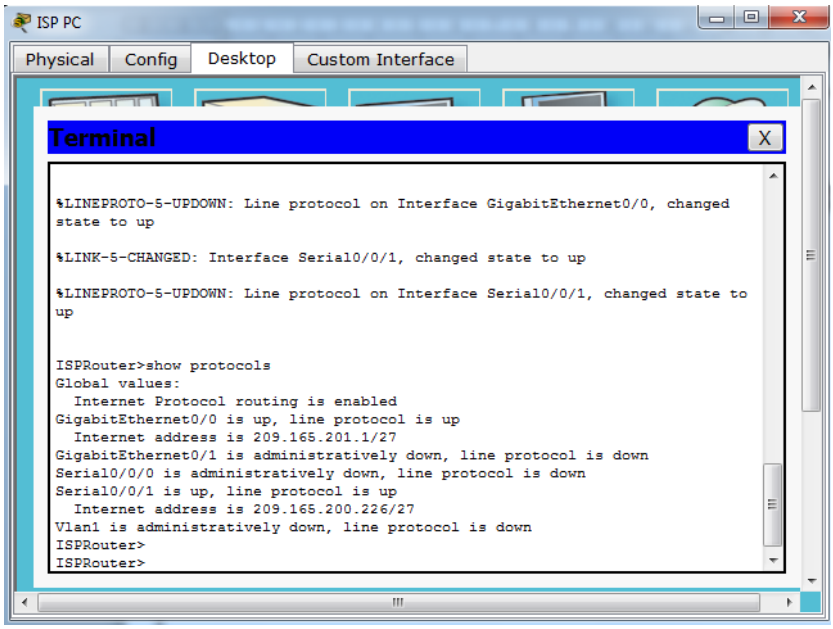


Parte 2: Preguntas de reflexión

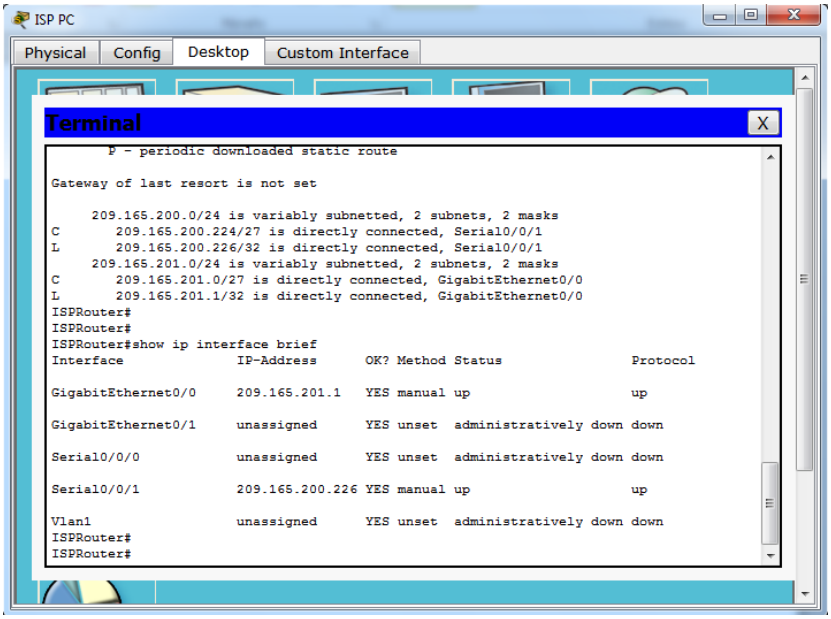
1. ¿Qué comandos proporcionarían la dirección IP, el prefijo de red y la interfaz?
   - show ip route, show interfaces, show protocols (antes de IOS 15, el comando show ip route no mostraba la dirección IP de las interfaces).


ISP PC
Physical
Config
Desktop
Software/Services
Terminal
X
ISPRouter>
ISPRouter>
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>
ISPRouter>


ISP PC
Physical
Config
Desktop
Custom Interface
Terminal
X
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#
ISPRouter#
ISPRouter#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 209.165.201.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 unassigned YES unset administratively down down
Serial0/0/1 209.165.200.226 YES manual up up
Vlan1 unassigned YES unset administratively down down
ISPRouter#
ISPRouter#

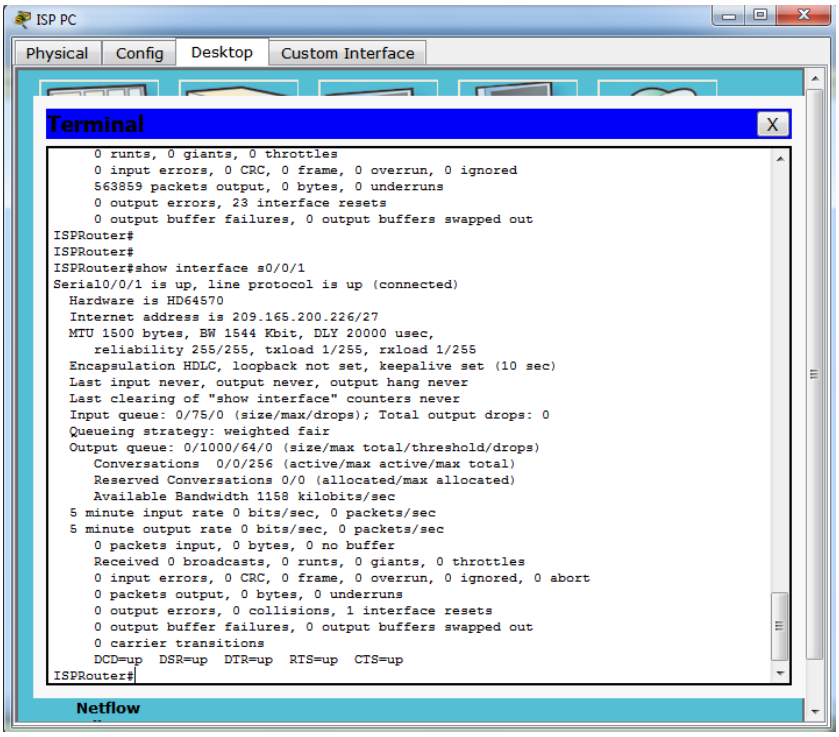


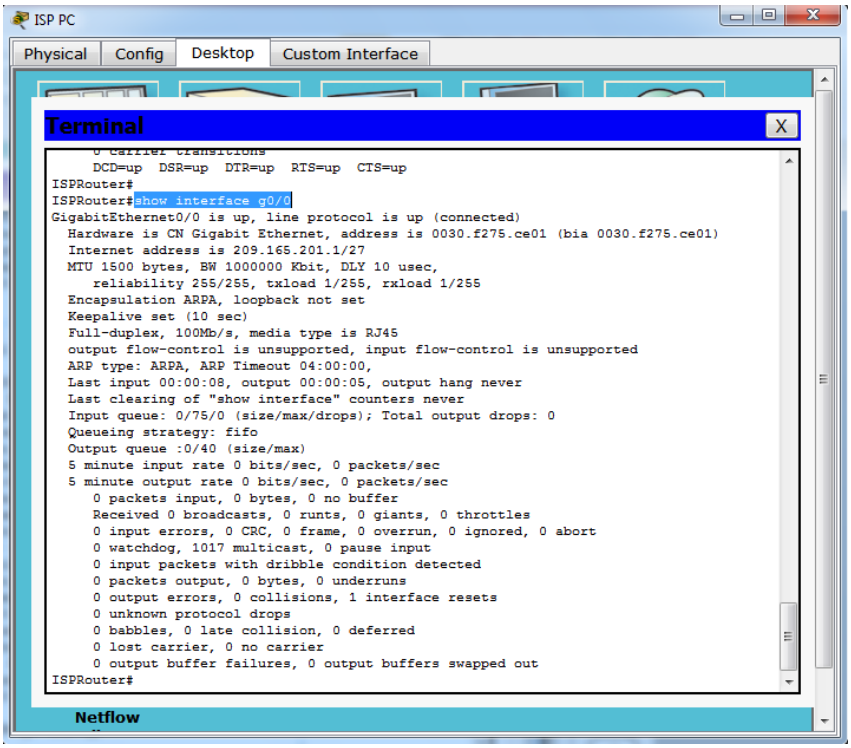
2. ¿Qué comandos proporcionan la dirección IP y la asignación de interfaces, pero no el prefijo de red? show ip interface brief



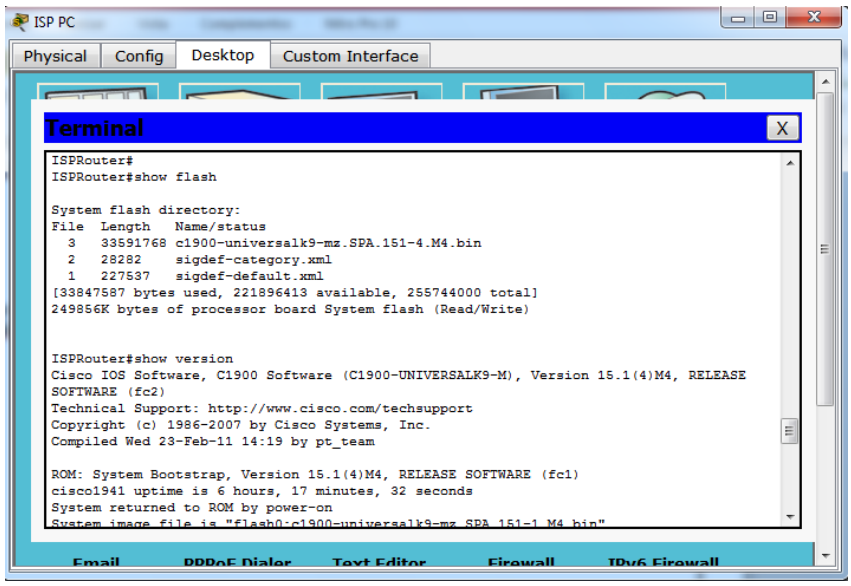
3. ¿Qué comandos proporcionan el estado de las interfaces? show interfaces, show ip interface

brief.

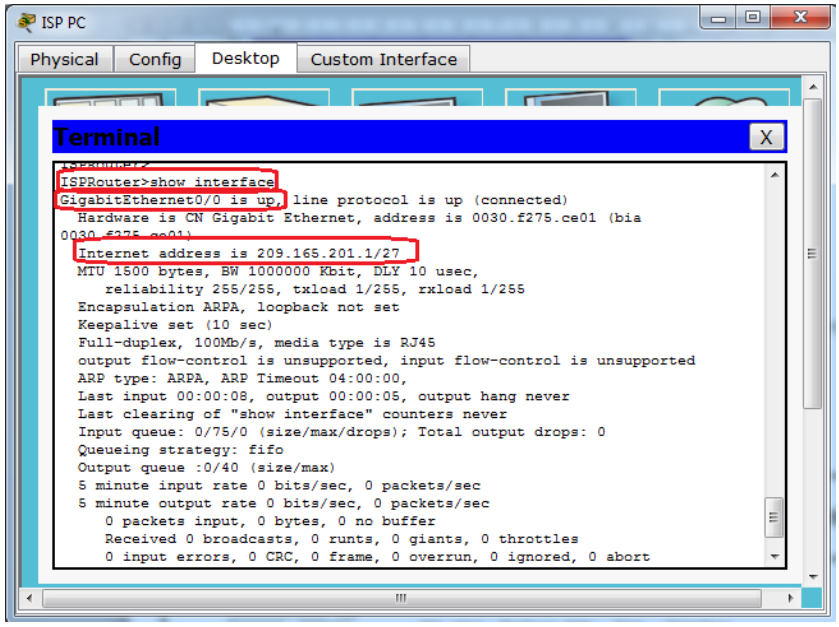

ISP PC
Physical
Config
Desktop
Custom Interface
Terminal
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
ISPRouter#
ISPRouter#
ISPRouter#show interface s0/0/1
Serial0/0/1 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 209.165.200.226/27
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
ISPRouter#
Netflow


ISP PC
Physical
Config
Desktop
Custom Interface
Terminal
DCD=up DSR=up DTR=up RTS=up CTS=up
ISPRouter#
ISPRouter#show interface g0/0
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
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
ISPRouter#
Netflow

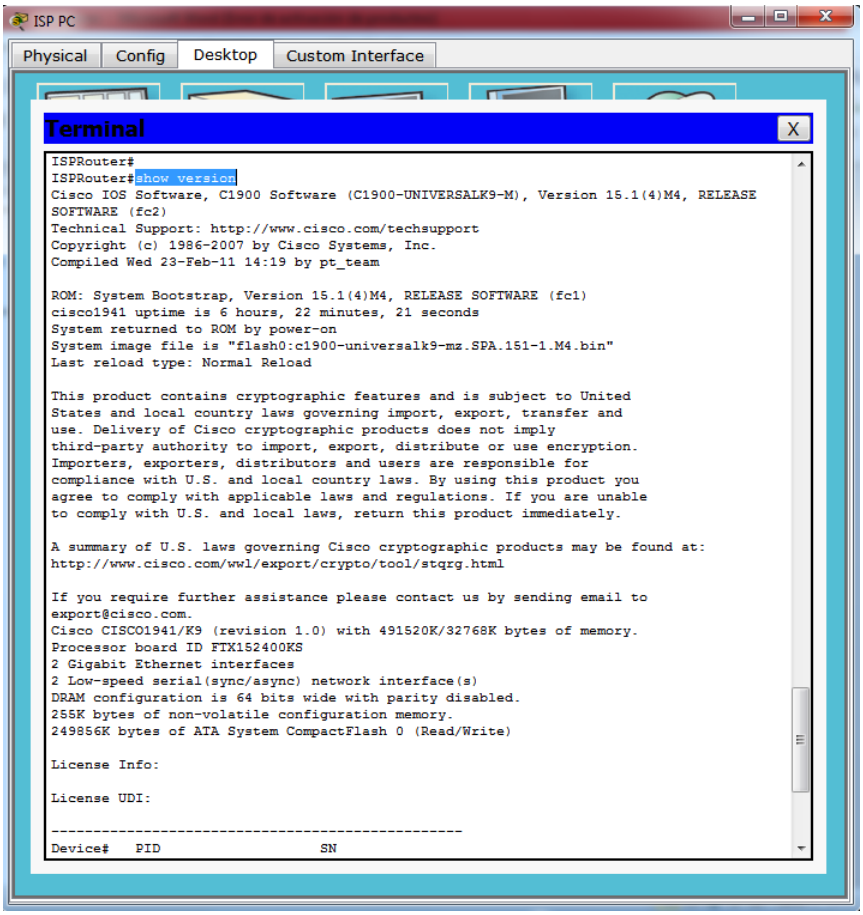
4. ¿Qué comandos proporcionan información sobre el IOS que se encuentra cargado en el router? show flash, show version.



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



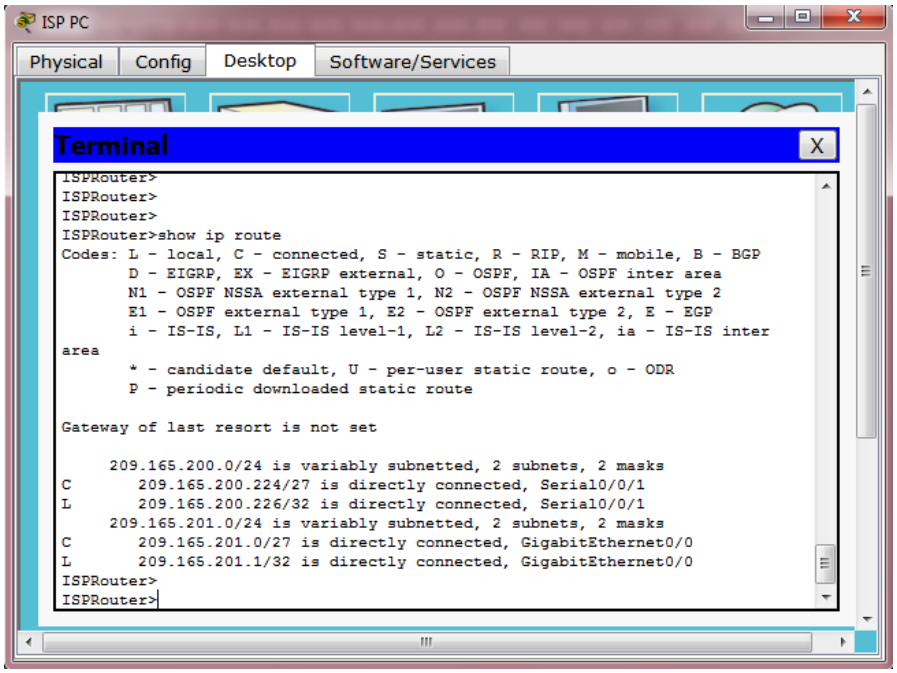
6. ¿Qué comandos proporcionan información sobre la cantidad de memoria flash disponible? show versión



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

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

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



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

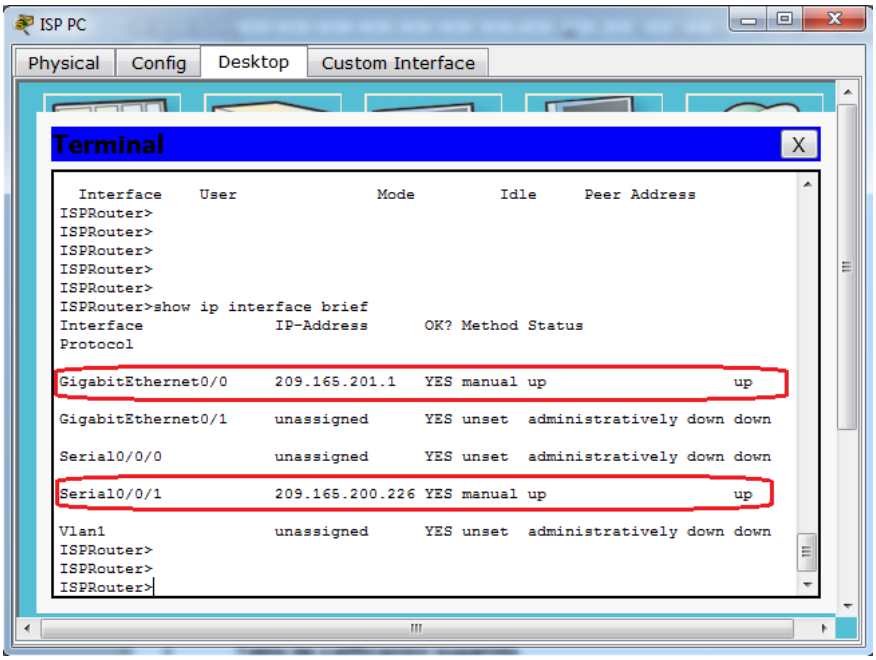
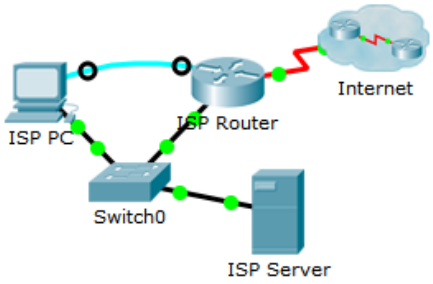


Tabla de calificación sugerida

Cada pregunta vale 10 puntos, para obtener una puntuación total de 100.

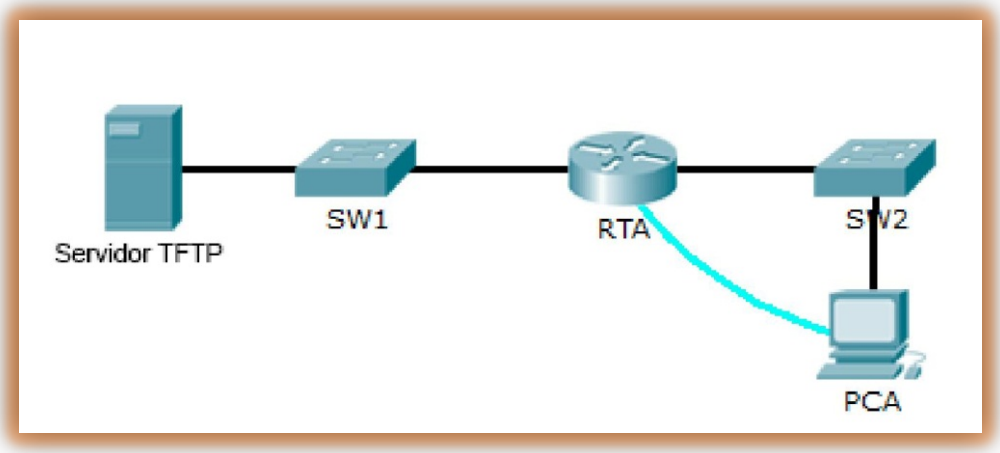


Laboratorio 11.4.2.5

Packet Tracer: Realización de copias de seguridad de archivos de configuración (versión para el instructor)..

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

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

Información básica/Situación

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

Parte 1: Establecer la conectividad al servidor TFTP

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

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

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

```
Router(config)#interface g0/0
Router(config-if)#ip addres 172.16.1.1 255.255.255.0
Router(config-if)#no shutdown

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

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

Router(config-if)#do wr
Building configuration...
[OK]
Router(config-if)#
```

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

```
Router#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

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#
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#
```

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

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

```
RTA#show ip interface 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#
```

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

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

b. Guarde la configuración en la NVRAM.

```
RTA(config)#hostname RTA-1
RTA-1(config)#exit
RTA-1#
%SYS-5-CONFIG_I: Configured from console by console

RTA-1#copy runni?
running-config
RTA-1#copy runni
RTA-1#copy running-config star?
startup-config
RTA-1#copy running-config star
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 - 845 bytes]

845 bytes copied in 0.029 secs (29137 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:

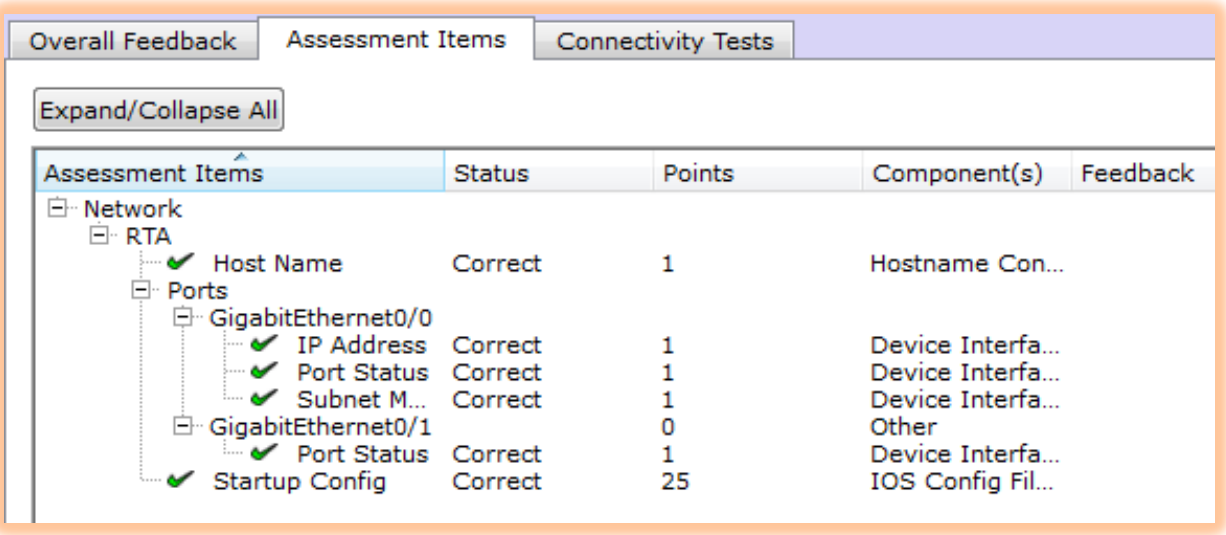
RTA-1# **copy flash tftp:**

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>

```
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 1.744 secs (2022360 bytes/sec)
RTA-1#
```

- LISTO, con esto termina el desarrollo del laboratorio, procedemos a verificar la configuración del mismo con las ayudas que el simulador no sumunistra.



Laboratorio 11.5.2.4

Packet Tracer: Configuración de un router Linksys (versión para el instructor)..

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Objetivos

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

Información básica

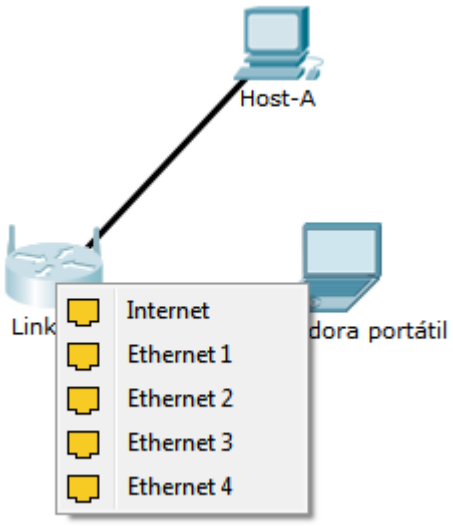
En esta actividad, configurará un router inalámbrico Linksys, lo que permite el acceso remoto a los clientes inalámbricos así como conectividad con seguridad WPA.

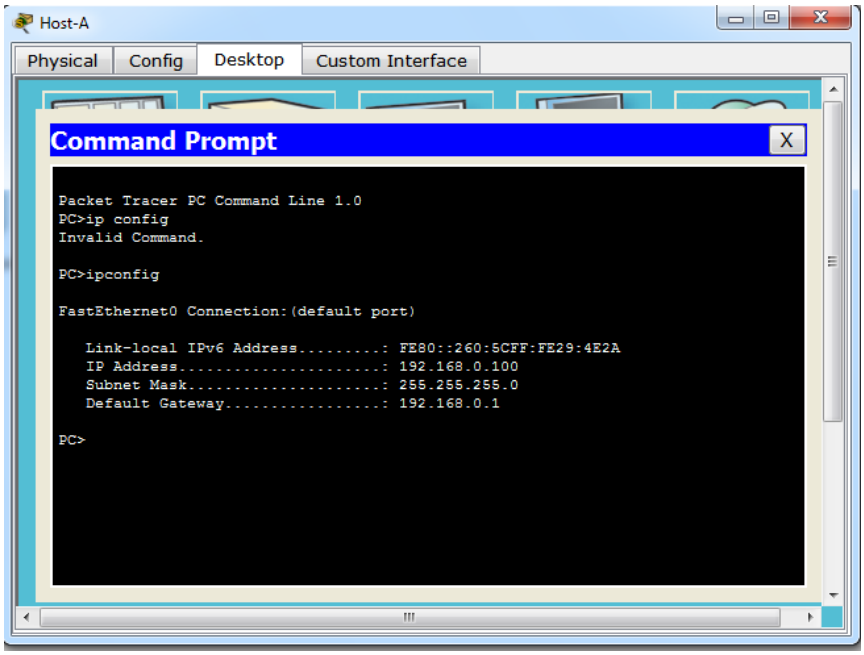
Parte 1: Conectar al router Linksys

Paso 1: Establecer y verificar la conectividad al router Linksys

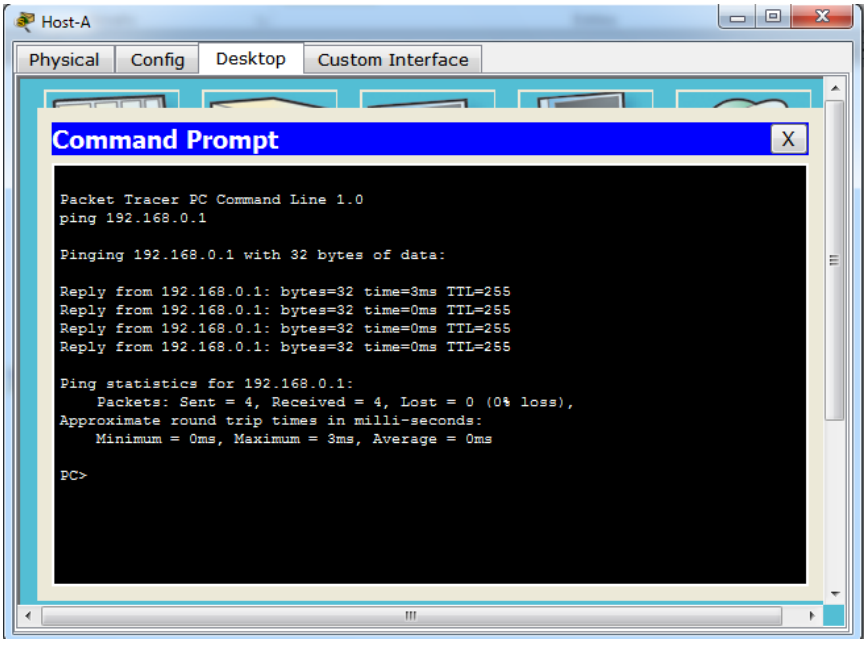
a. Conecte el cable adecuado del **Host-A** al puerto Ethernet 1 en **Linksys**.

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**.



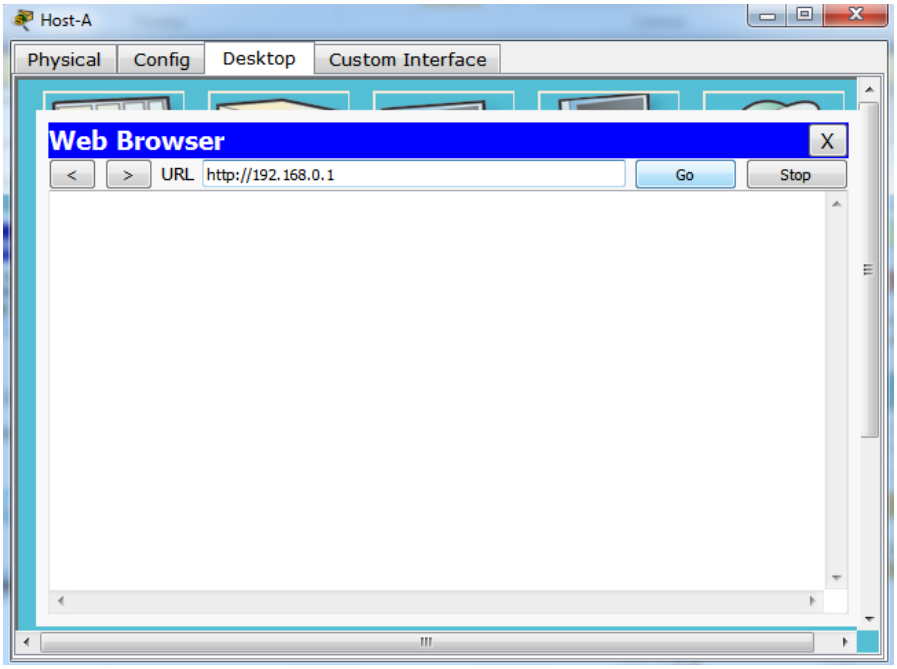


c. Introduzca el comando **ping 192.168.0.1** para verificar que el **Host-A** pueda acceder al gateway predeterminado.

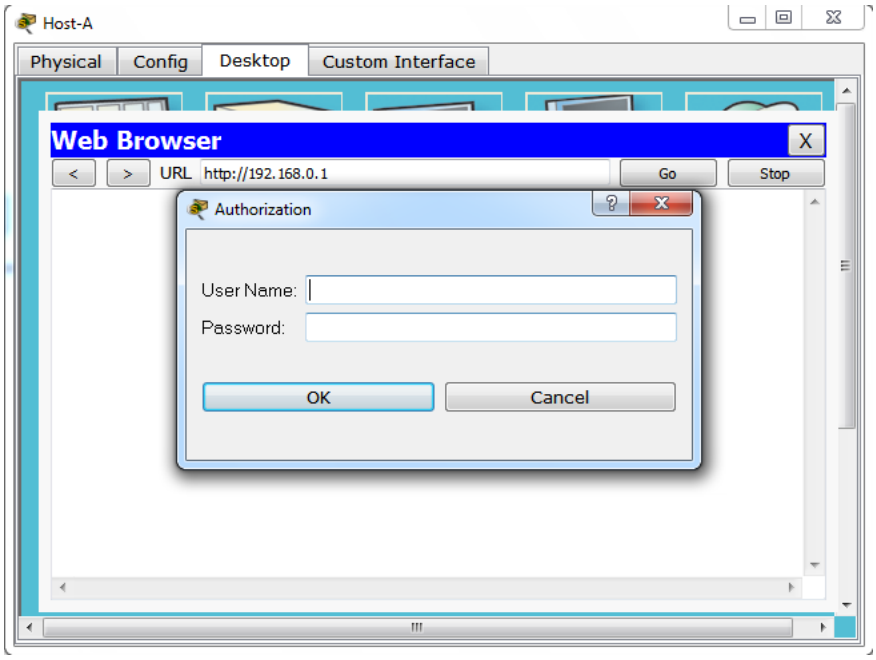


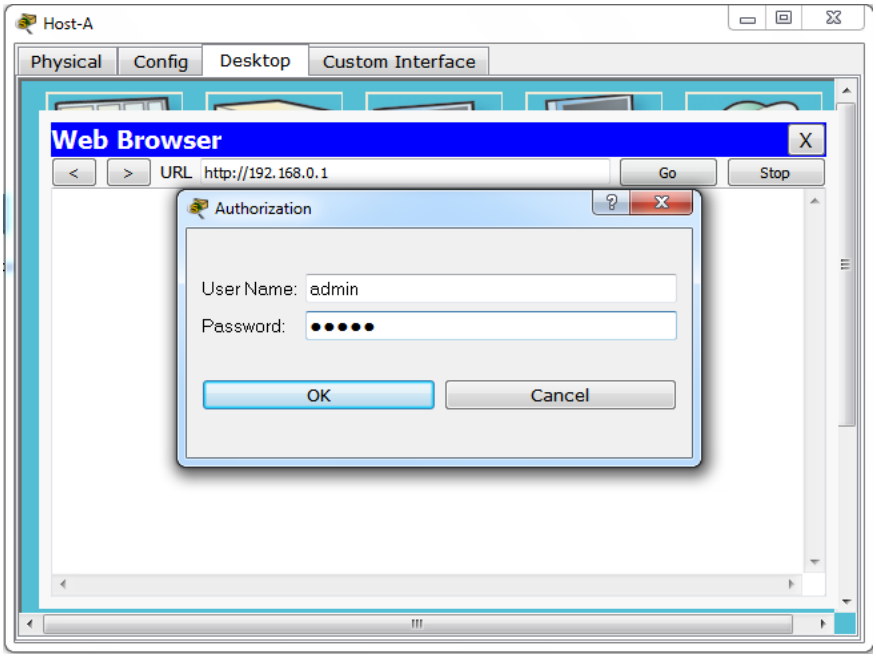
Paso 2: Acceda a la interfaz gráfica de usuario (GUI) de Linksys mediante un explorador Web.

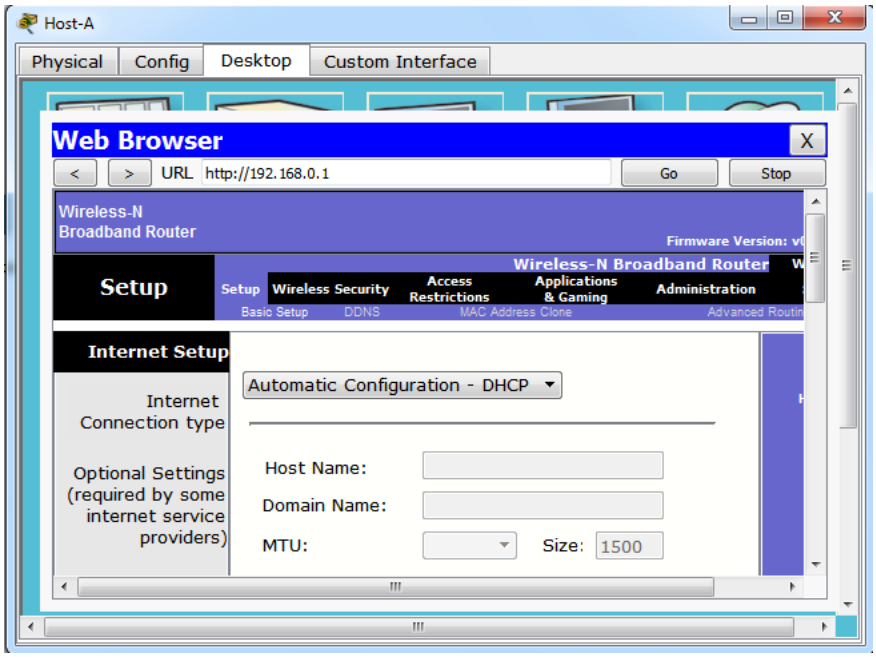
a. Para configurar el router **Linksys** con la GUI, debe acceder a este mediante el explorador Web del **Host-A**. Abra el explorador Web y escriba la dirección de gateway predeterminado en el campo de dirección URL para acceder a **Linksys**.



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


Host-A
Physical
Config
Desktop
Custom Interface
Web Browser
X
URL
http://192.168.0.1
Go
Stop
Authorization
User Name:
Password:
OK
Cancel


Host-A
Physical
Config
Desktop
Custom Interface
Web Browser
X
URL
http://192.168.0.1
Go
Stop
Authorization
User Name:
admin
Password:
OK
Cancel



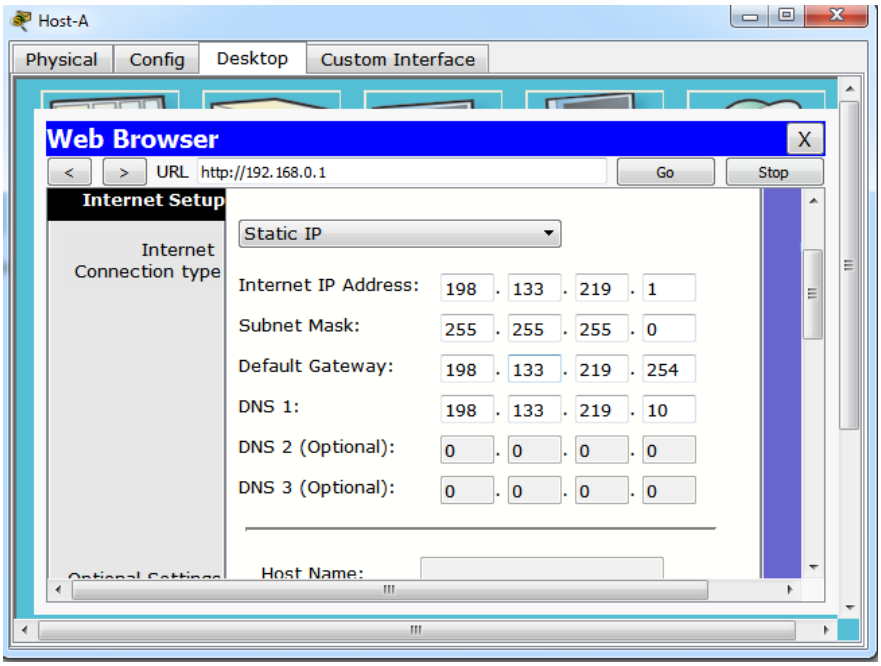
Nota: no podrá ver el cambio en la puntuación al configurar el router **Linksys** hasta que haya hecho clic en **Save Settings** (Guardar configuración).

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**

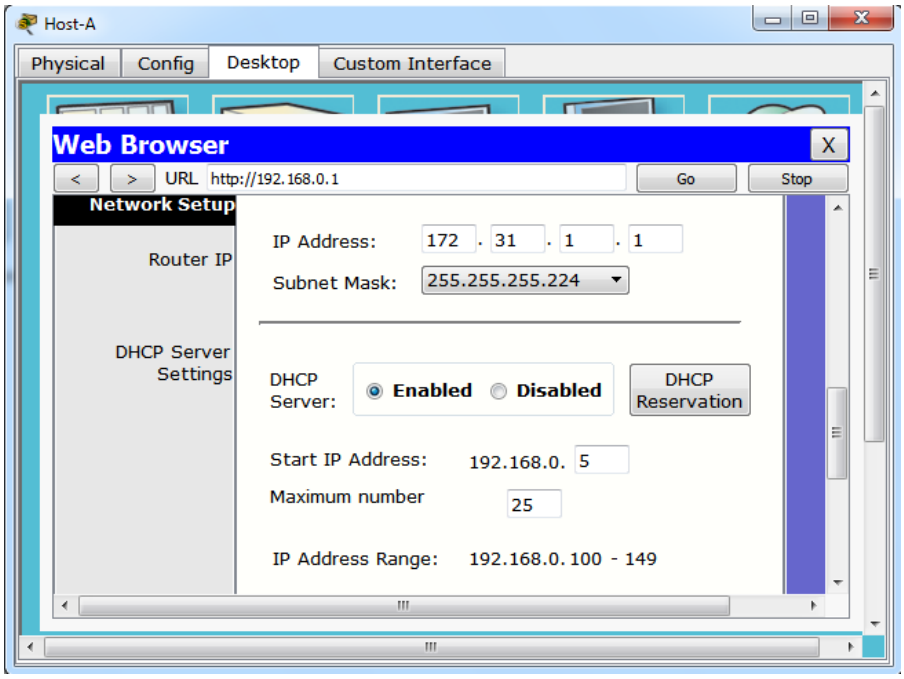


Paso 2: Configure los parámetros de red internos.

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**.

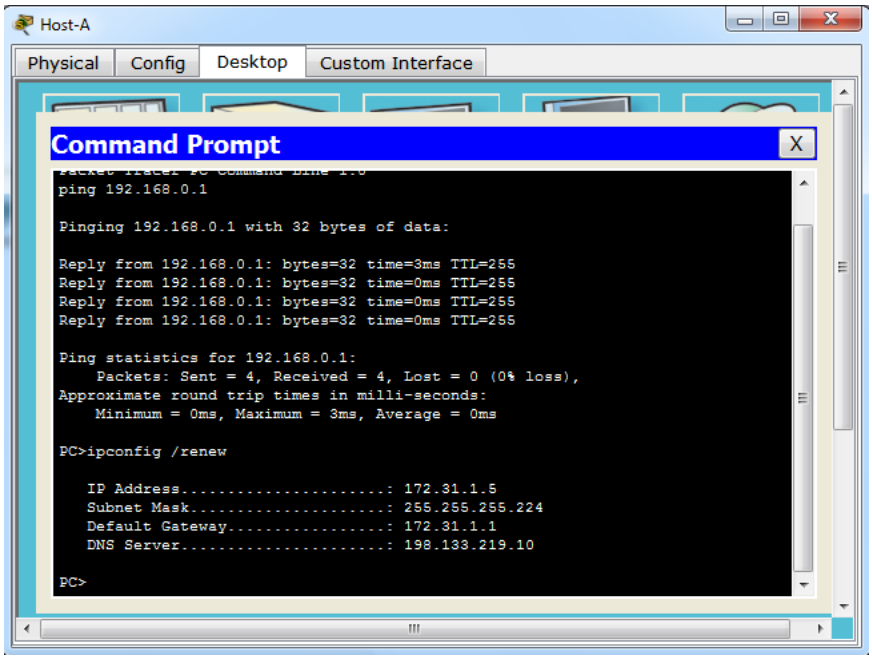


Paso 3: Guardar la configuración y volver a conectarse al router Linksys

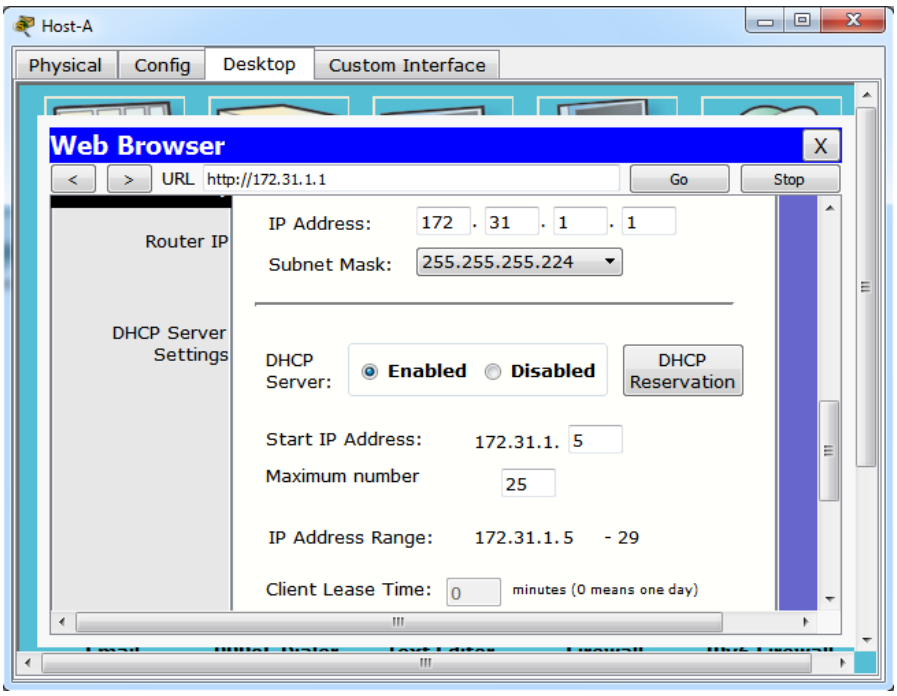
a. Desplácese hasta la parte inferior de la página y haga clic en **Save Settings**. Si pasa de una ficha a otra sin guardar la configuración, esta se perderá.

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.

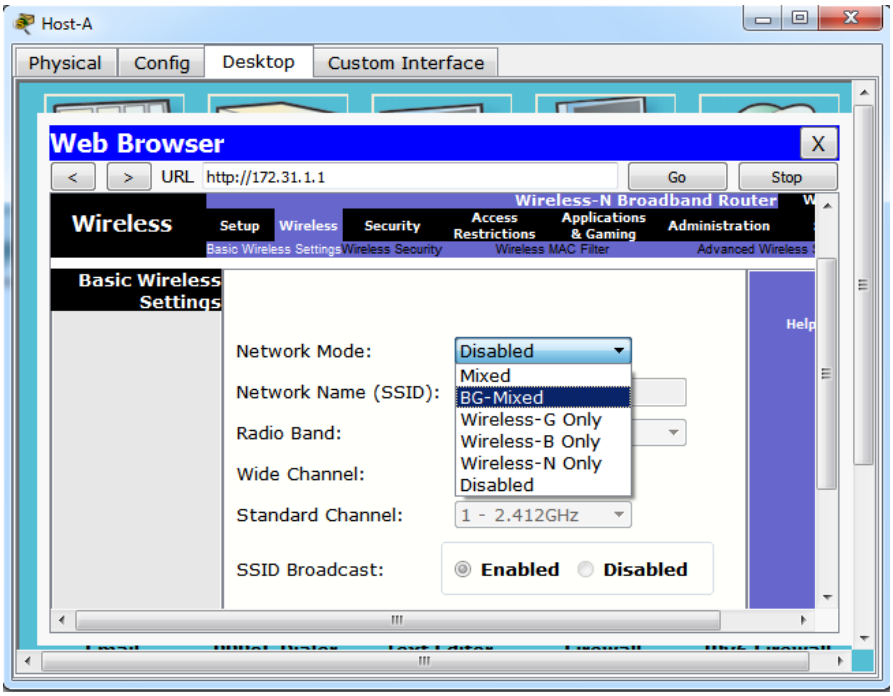


d. Utilice el explorador Web del **Host-A** para volver a conectarse al router **Linksys**. Deberá utilizar la nueva dirección de gateway predeterminado. Verifique la configuración de **Internet Connection** (Conexión a Internet) en la ficha **Status** (Estado). La configuración debe coincidir con los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

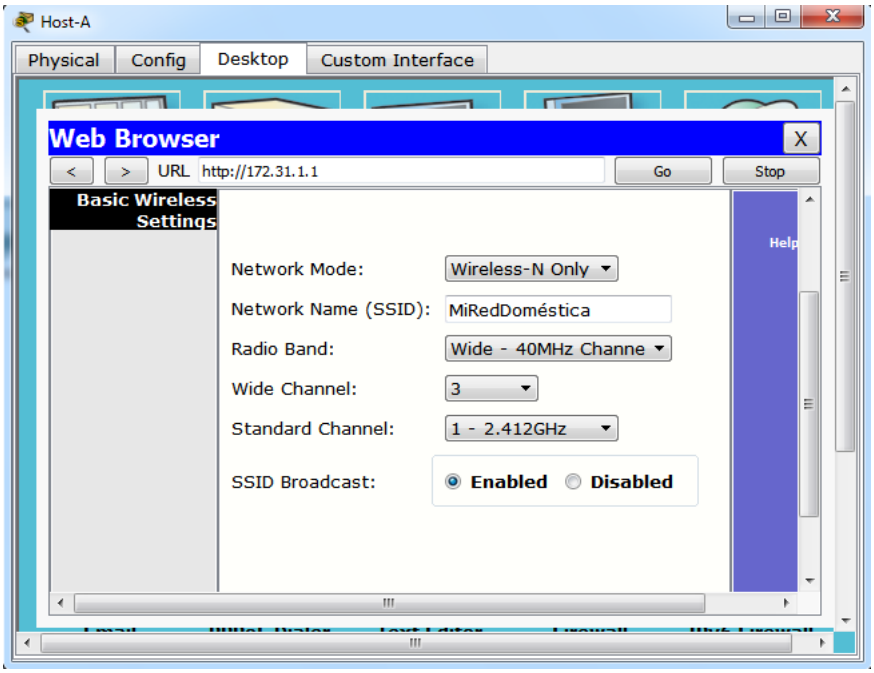
¿Cuáles son dos características de un SSID?

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

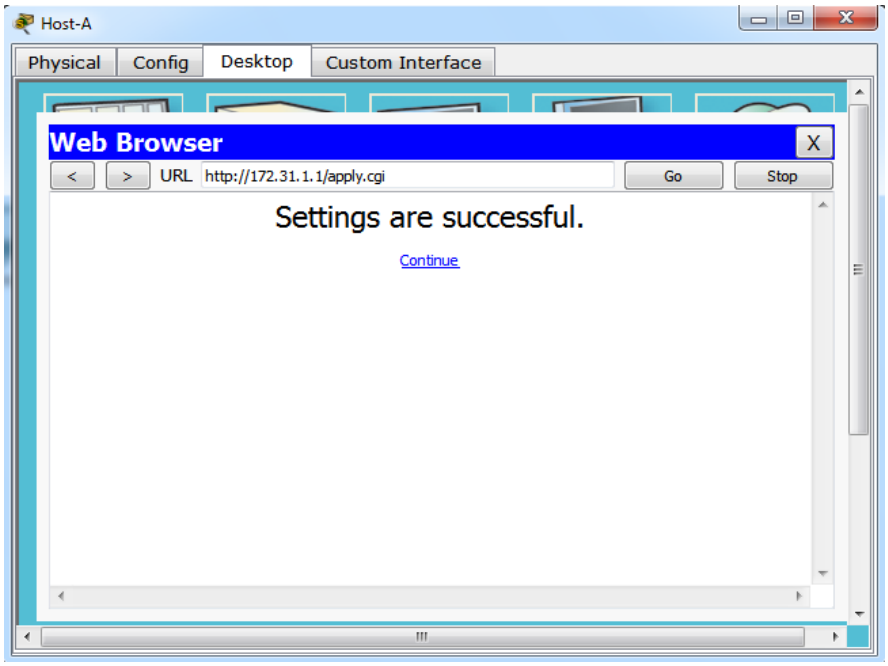
d. Cuando un cliente inalámbrico busca redes inalámbricas en el área, este detecta cualquier transmisión del SSID. Las transmisiones del SSID están habilitadas de manera predeterminada.

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.

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).

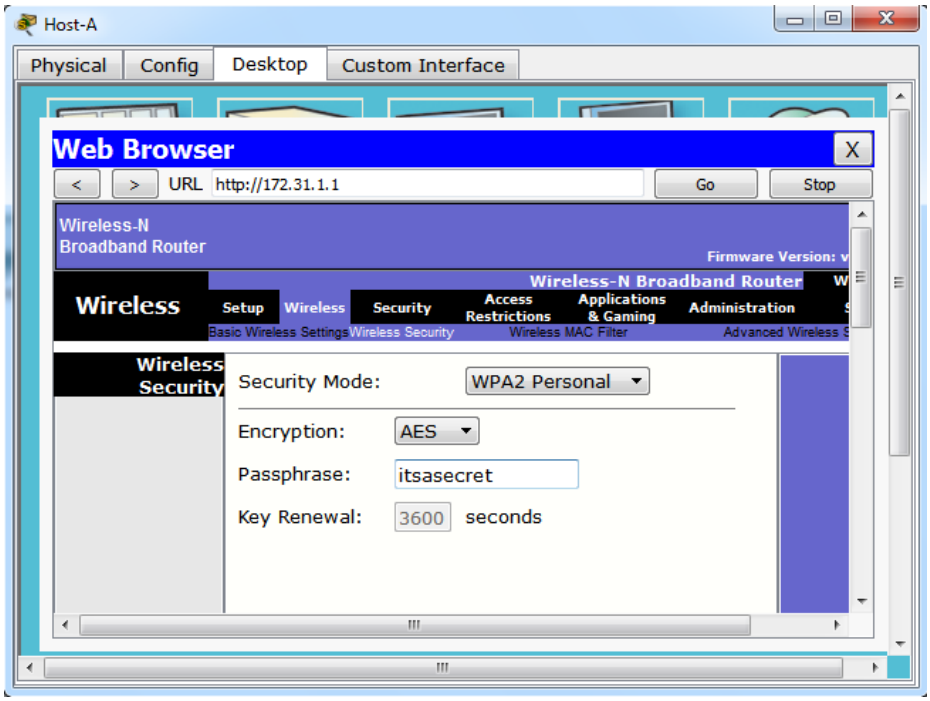


Paso 5: Configure la seguridad inalámbrica de modo que los clientes deban autenticarse para poder conectarse a la red inalámbrica.

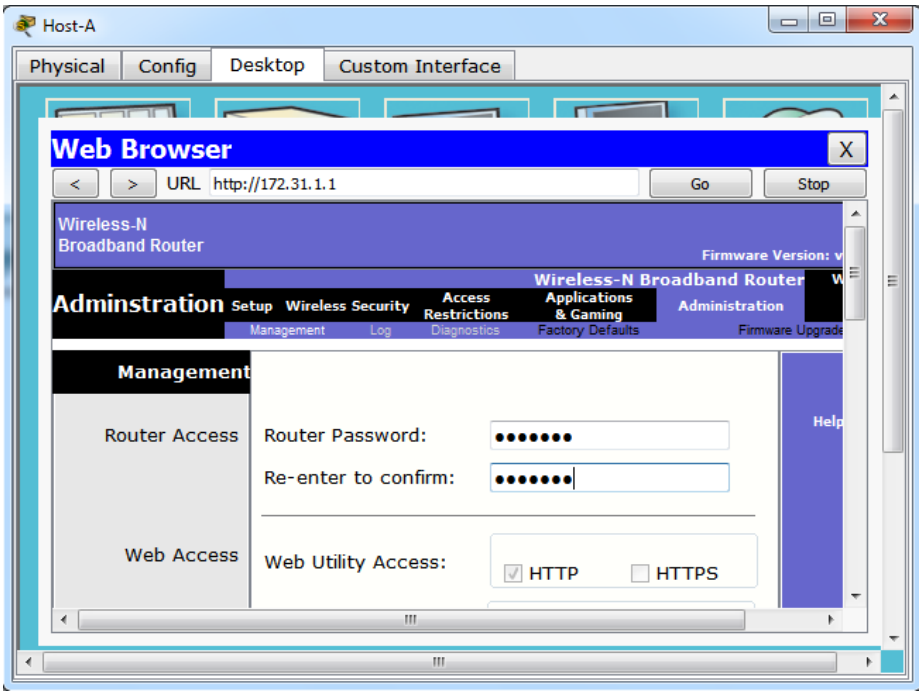
a. Haga clic en la opción **Wireless Security** (Seguridad inalámbrica) en la ficha **Wireless**.

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

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



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

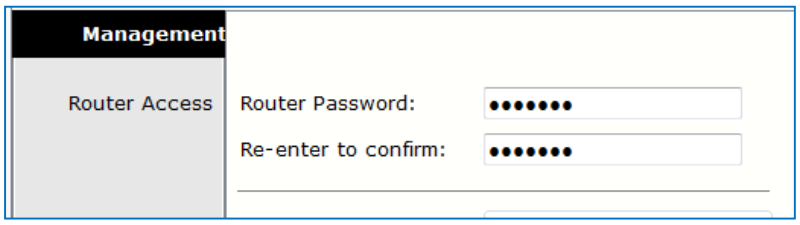


c. Haga clic en **Save settings** (Guardar configuración) y, a continuación, haga clic en **Continue**

(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**.



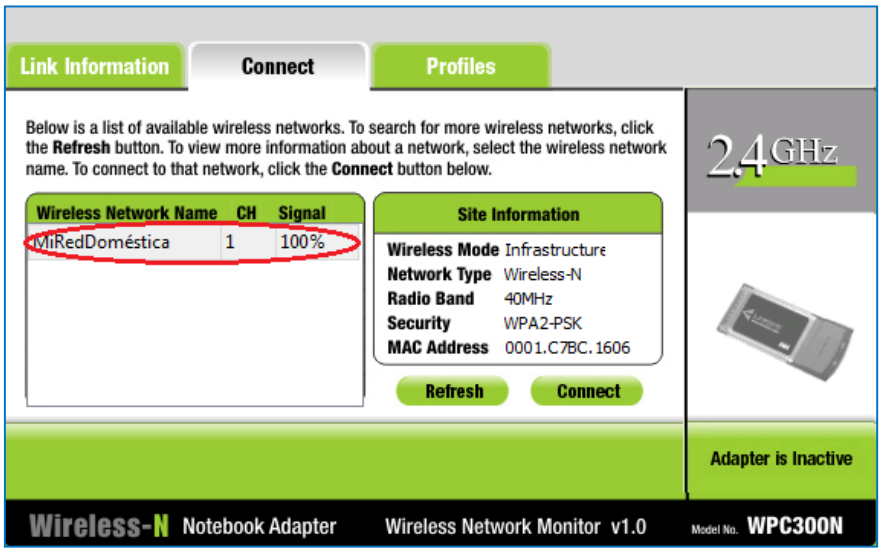
b. Haga clic en **Save Settings**. Introduzca el nombre de usuario **admin** y la nueva contraseña.

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.

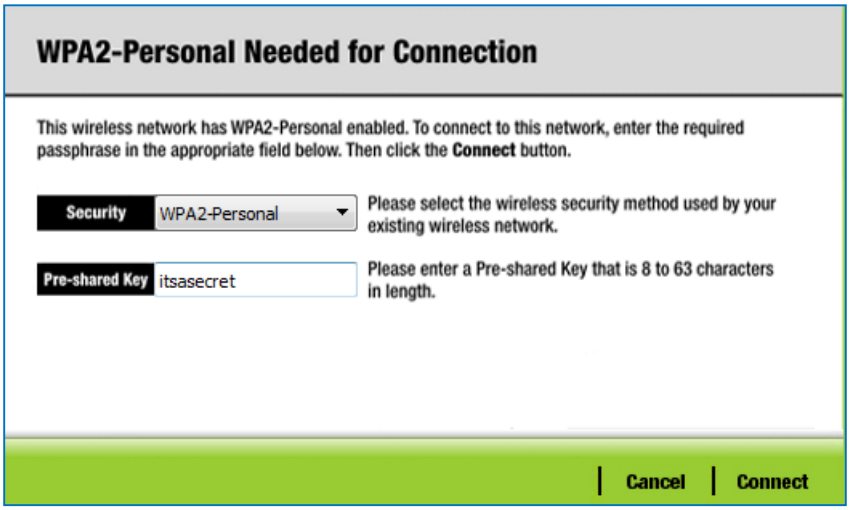
b. Haga clic en la ficha **Connect** (Conectar) y después en **Refresh** (Actualizar), si es necesario. Debería ver la red **MiRedDoméstica** indicada en Wireless Network Name (Nombre de red inalámbrica).

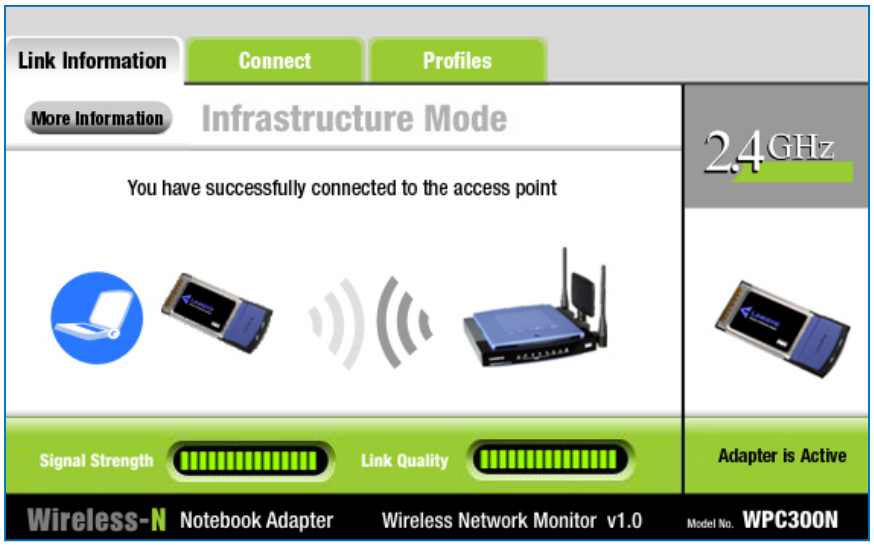


c. Haga clic en **MiRedDoméstica** y después en **Connect**.

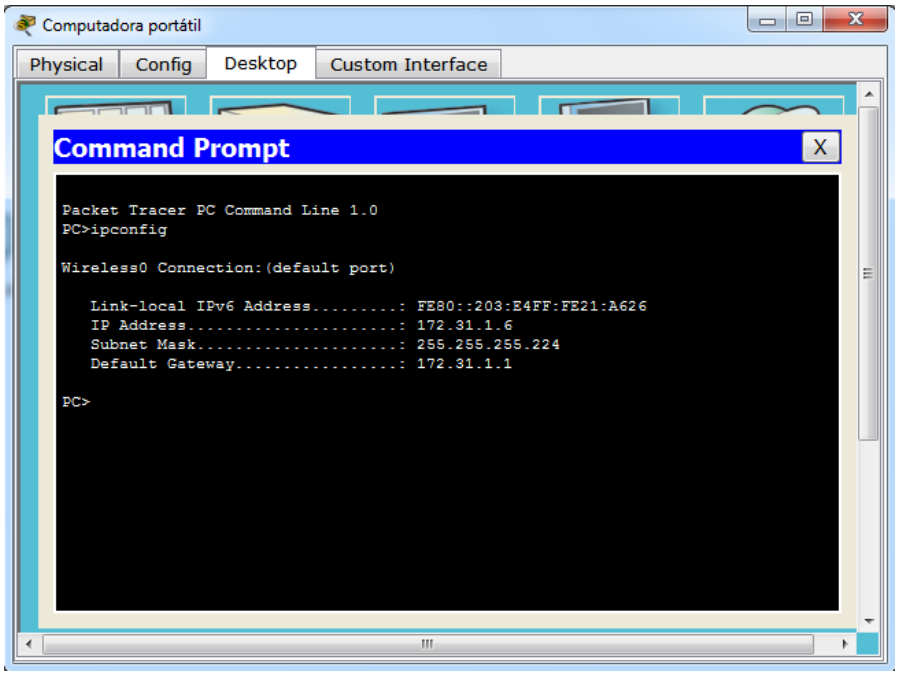
d. Ahora debería ver la red **MiRedDoméstica**. Haga clic en esta y después en **Connect**.

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**.



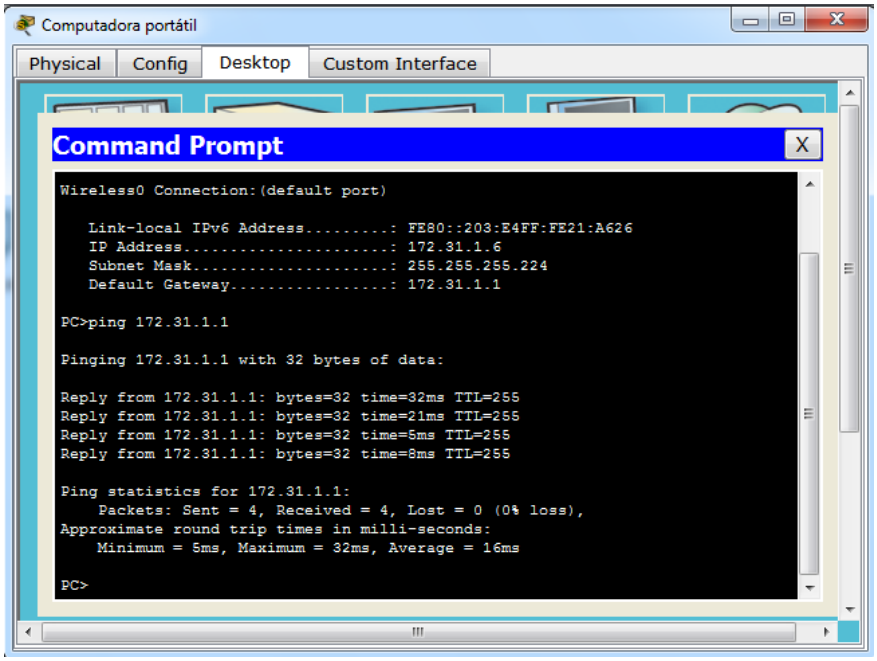


f. Cierre la GUI de Linksys y haga clic en **Command Prompt** (Símbolo del sistema). Introduzca el comando **ipconfig** para verificar si **Laptop** recibió el direccionamiento IP.



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.**

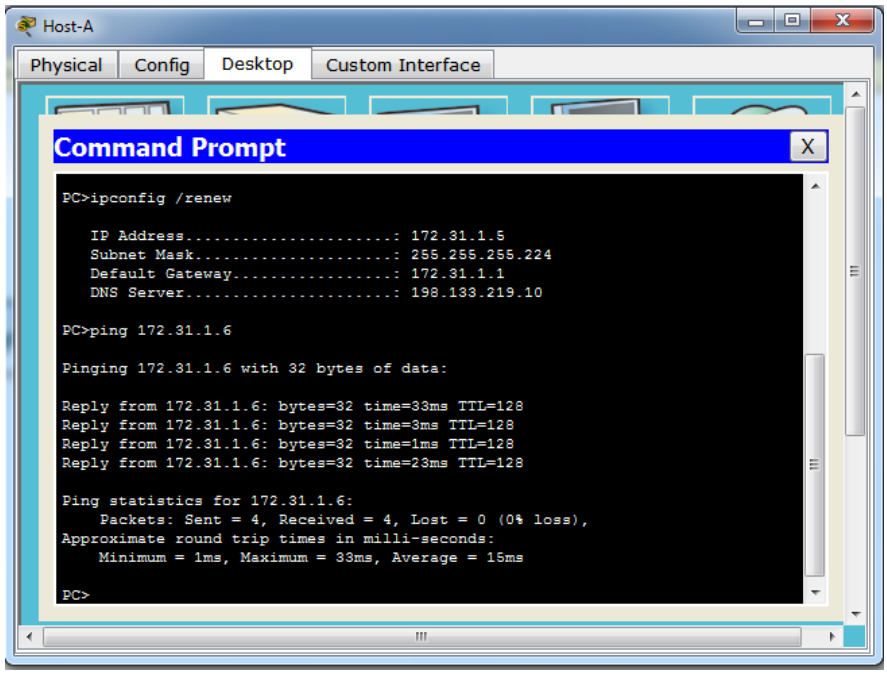
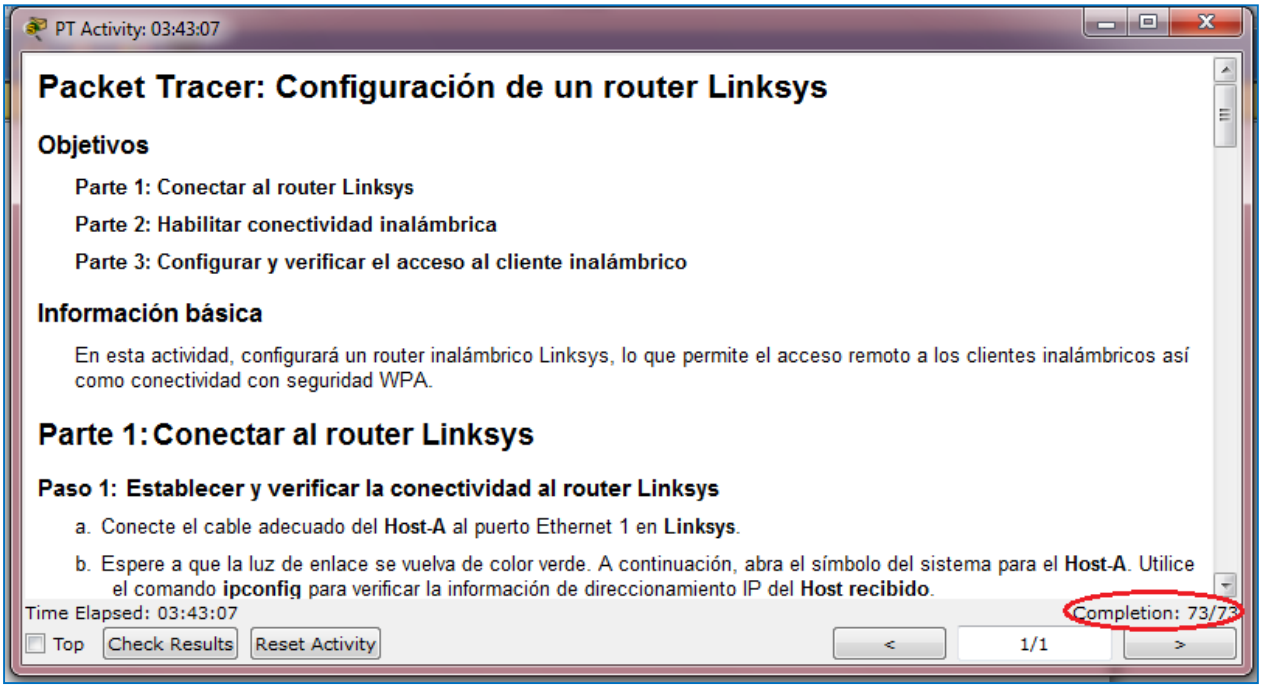


Tabla de calificación sugerida

Sección de la actividad	Ubicación de la consulta	Posibles puntos	Puntos obtenidos
Parte 2: Habilitar conectividad inalámbrica	Paso 4	4	
		1	
Total de la parte 2		**5**	
Puntuación de Packet Tracer		**95**	
Puntuación total		**100**	


PT Activity: 03:43:07
Packet Tracer: Configuración de un router Linksys
Objetivos
Parte 1: Conectar al router Linksys
Parte 2: Habilitar conectividad inalámbrica
Parte 3: Configurar y verificar el acceso al cliente inalámbrico
Información básica
En esta actividad, configurará un router inalámbrico Linksys, lo que permite el acceso remoto a los clientes inalámbricos así como conectividad con seguridad WPA.
Parte 1: Conectar al router Linksys
Paso 1: Establecer y verificar la conectividad al router Linksys
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.
Time Elapsed: 03:43:07
Completion: 73/73
Top
Check Results
Reset Activity
<
1/1
>

Laboratorio 11.6.1.2

Packet Tracer: Reto de habilidades de integración (versión para el instructor)..

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

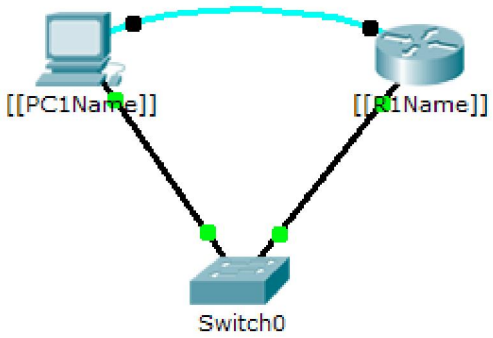


Tabla de direccionamiento

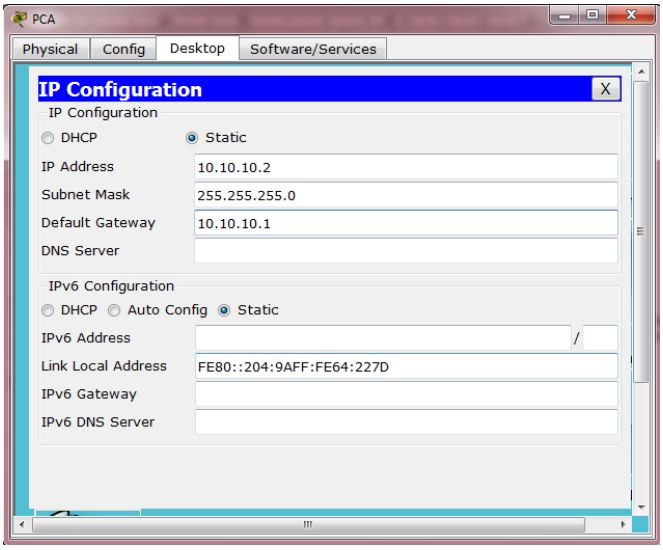
Dispositivo	Interfaz	Dirección IP	Máscara de subred
RTA	G0/0	10.10.10.1	255.255.255.0
PCA	NIC	10.10.10.2	255.255.255.0

Situación

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

Requisitos

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




```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#ip addres 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown

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

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

Router(config-if)#
```

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

```
Router(config)#
Router(config)#hostname RTA
RTA(config)#
```

```
RTA(config)#service pass?
password-encryption
RTA(config)#service pass
RTA(config)#service password-encryption
RTA(config)#
```

- Establezca la contraseña secreta segura que desee.

```
RTA(config)#
RTA(config)#enable secret cisco
RTA(config)#
```

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

  RTA(config)# **ip domain-name RTA**

```
RTA(config)#ip domain-name RTA
RTA(config)#
```

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

  RTA(config)# **user *any_user* password *any_password***

```
RTA(config)#
RTA(config)#username cisco password class
RTA(config)#
```

- Genere claves RSA de 1024 bits.

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

  RTA(config)# **crypto key generate rsa**

  The name for the keys will be: RTA.RTA

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
RTA(config)#crypto key generate RSA
The name for the keys will be: RTA.RTA
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

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

  RTA(config)# **login block-for 180 attempts 4 within 120**

```
RTA(config)#
RTA(config)#login block-for  180 attempts 4 within 120
RTA(config)#
```

- Configure las líneas vty para el acceso por SSH y solicite los perfiles de usuarios locales. RTA(config-line)# **transport input ssh**
  RTA(config-line)# **login local**

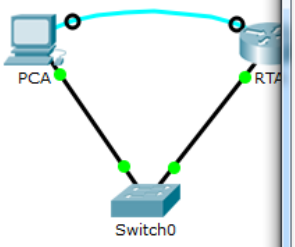
```
RTA(config)#line vty 0 4
RTA(config-line)#login local
RTA(config-line)#transport input ssh
RTA(config-line)#exit
RTA(config)#
```

- Guardar la configuración en la NVRAM.

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

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

  ID: 10



PT Activity: 01:18:22

Packet Tracer: Reto de habilidades de integración

Tabla de direccionamiento

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

Situación

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

Time Elapsed: 01:18:22 Completion: 100%

Top | Check Results | Reset Activity | < | 1/1 | >

CONCLUSIONES

- En esta práctica de laboratorio realizamos la configuración de los servicios de red HTTP y de CORREO ELECTRÓNICO dentro del simulador de PACKET TRACER, el cual nos ha permitido observar el funcionamiento del proceso realizado. Se crearon una cuentas con el fin de tener acceso a los correos electrónicos en el cual se enviaron y recibieron mensajes con lo cual constatamos el funcionamiento general.

- Tratamos toda la temática relacionada con DHCP el cual es el proceso de configuración automática de las direcciones IP, proceso que sin duda ahorra mucho tiempo para el administrador de la red. Realizamos también la configuración de un servidor DNS el cual nos permite realzar la traducción de un nombre de dominio a una IP, con lo cual la búsqueda para las personas es mucho más eficiente.

- Observamos el funcionamiento del servicio FTP el cual sirve para realizar la transferencia de archivos, se configuraron una serie de cuentas las cuales permitían el acceso y los permisos para cada uno de estas cuentas. Se realizaron las pruebas del proceso realizado y todo funciona bien.

- Se creó el presente laboratorio empleando varias instancias del simulador, 2 archivos independientes que podían comunicarse entre sí, se realizaron las pruebas pertinentes de funcionamiento. Se configuraron además los servicios DNS con lo cual los PC del lado SERVIDOR como del lado CLIENTE tienes acceso al mismo.

- En esta práctica realizamos la configuración de una sesión multiusuarios en Packet Tracer pero esta vez realizando también la configuración de unos servicios adicionales tales como DHCP, DNS, FTP. Realizamos la configuración de un cliente de correo electrónico y además creamos una serie de cuenta en la cual verificamos el envío y recibo de mensajes.

- Con la realización de esta práctica evidenciamos que la computadora portátil después de que se cumple la totalidad del procedimiento de verificar la conectividad entre la computadora portátil, el Host-A y cerramos el simulador esta conectividad inalámbrica se pierde y la calificación total pasa de 73 a 66, para completar nuevamente la calificación máxima hay que realizar nuevamente la conexión inalámbrica de la computadora portátil la cual es sencilla de realizar y de esta manera los parámetros son asignados nuevamente y el ejercicio llega al 100%.

BIBLIOGRAFIA

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado dehttps://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

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