DIPLOMADO DE PROFUNDIZACIÓN CISCO

LUIS ÁNGEL SALCEDO SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

INGENIERÍA DE SISTEMAS

BOGOTA D.C.

ABRIL DE 2018

DIPLOMADO DE PROFUNDIZACIÓN CISCO

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

TUTOR:

JUAN CARLOS VEGA FERREIRO

ESTUDIANTE:

LUIS ÁNGEL SALCEDO SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

INGENIERÍA DE SISTEMAS

BOGOTA D.C.

ABRIL DE 2018

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BROADCAST: difusión masiva de información o paquetes de datos a través de redes informáticas.

IPv4: cuarta versión del protocolo de internet que fue adaptado y ahora se utiliza ampliamente en la comunicación de datos a través de diferentes tipos de redes.

IPv6: sexta versión del protocolo de internet que hace posible conectar dispositivos en Internet, identificándolos con una dirección unívoca.

MULTICAST: difusión múltiple, tipo de transmisión en la que se emiten el envío de datos desde un emisor a muchos receptores, o desde muchos emisores a muchos receptores.

ROUTER: dispositivo que conecta diferentes computadoras de una misma red de área local, permitiendo el intercambio de paquetes de datos entre los ordenadores que se encuentran en esa red.

SWITCH: dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un PC, una impresora, una televisión, una consola o cualquier aparato que posea una tarjeta Ethernet o Wifi.

UNICAST: difusión única, es un tipo de transmisión en la que el envío se produce desde un único emisor a un único receptor, sin importar si tiene lugar en ambas direcciones.

INTRODUCCIÓN

El presente documento escrito corresponde al desarrollo de las actividades necesarias para obtener certificación el curso Cisco CCNA, módulo “Routing & Switching: Principios básicos de routing y switching”. trabajos enfocados al desarrollo de laboratorios prácticos y teóricos sobre uso de protocolos de enrutamiento avanzados.

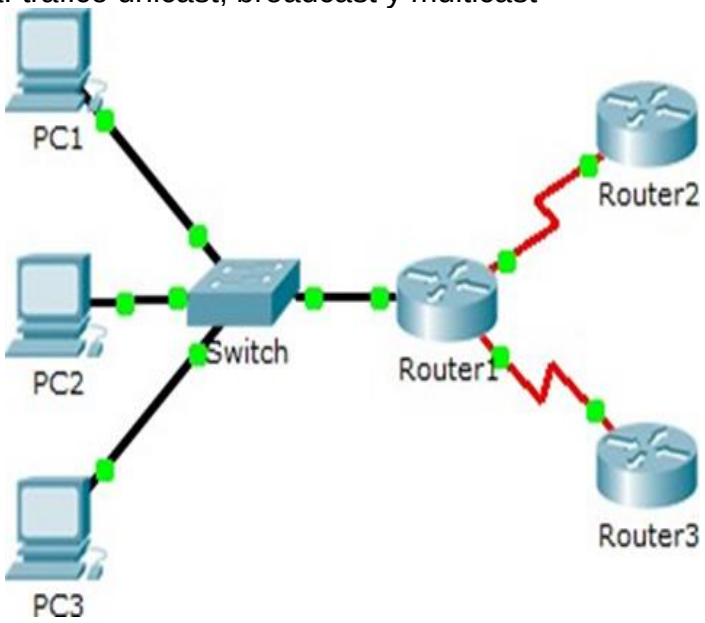
Las diferentes actividades fueron realizadas según instrucciones del tutor encargado para el año 2018, del diplomado de profundización CISCO y exponen, paso a paso de manera estructurada e ilustrada, los comandos de configuración trabajados y los diferentes resultados obtenidos.

Con el desarrollo de las actividades del módulo CCNA Routing & Switching: Principios básicos de routing y switching, se busca afianzar conceptos y procedimientos de configuración necesarios en las tecnologías switching y routing mejoradas, al igual que identificar los beneficios de los protocolos de dinámicos de host como (DHCP) y protocolos de dominio (DNS) para los protocolos de internet IPV4 e IPV6.

1. DESARROLLO DE LAS ACTIVIDADES PROPUESTAS

1.1. PACKET TRACER: INVESTIGACIÓN DEL TRÁFICO UNICAST, BROADCAST Y MULTICAST

Figura 1. Topología: tráfico unicast, broadcast y multicast



Fuente: elaboración Propia

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.

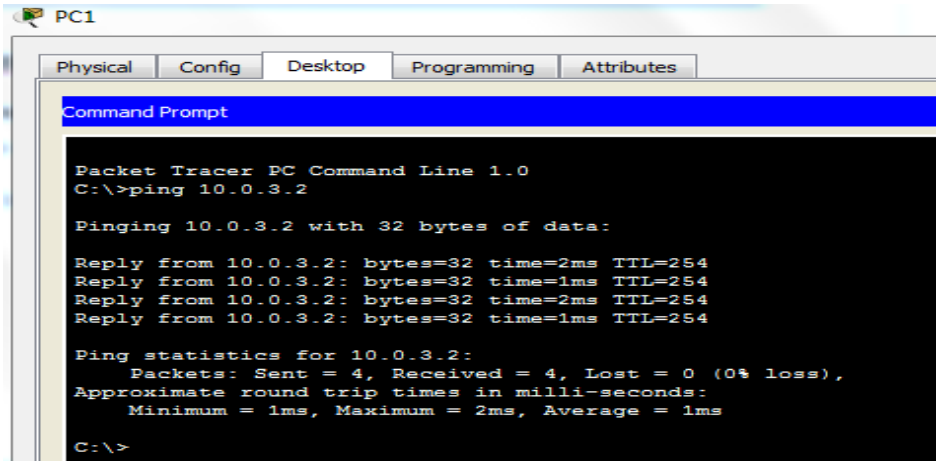
1.1.1. Desarrollo Parte 1: Generar tráfico de unicast.

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.

Figura 2. Ping éxito a la ip 10.0.3.2.

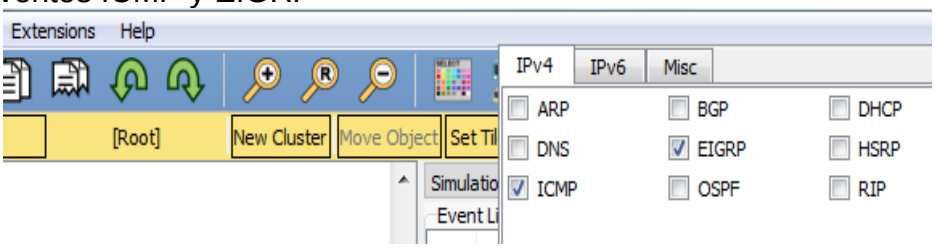


Fuente: elaboración Propia

Paso 2: Ingrese al modo de simulación.

a. Haga clic en la ficha **Simulation** (Simulación) para ingresar al modo de simulación.
b. clic en **Edit Filters** (Editar filtros) y verifique que solo los eventos ICMP y EIGRP estén seleccionados.

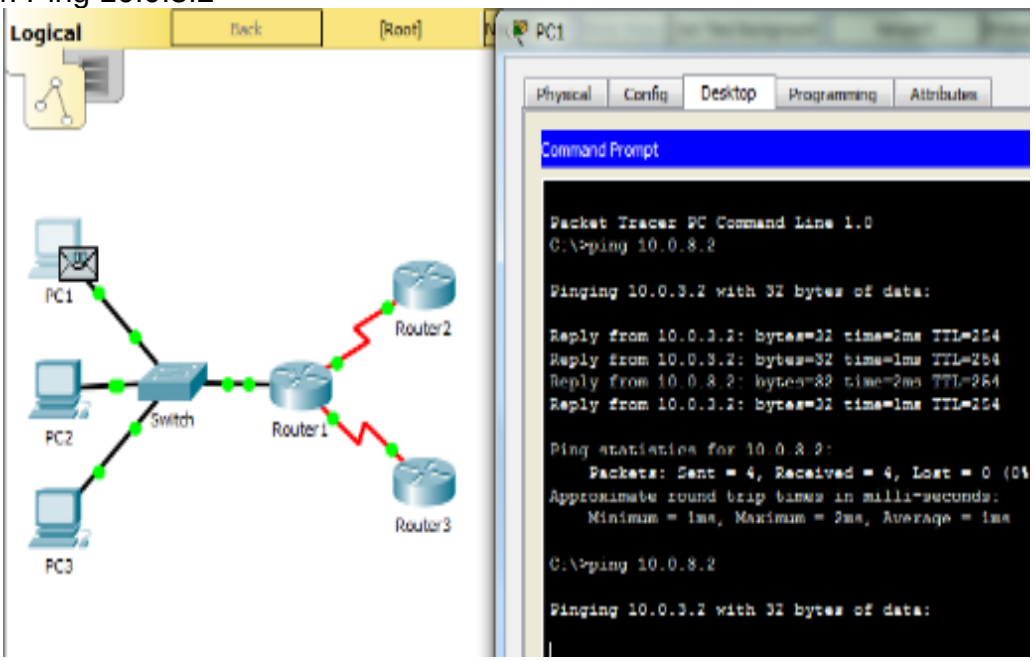
Figura 3. Eventos ICMP y EIGRP



Fuente: elaboración Propia

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

Figura 4. Ping 10.0.3.2



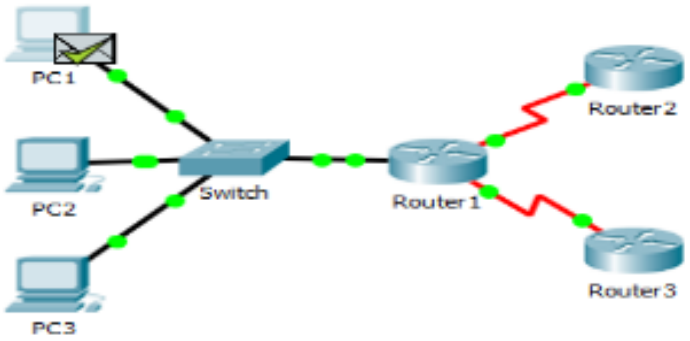
Fuente: elaboración Propia

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.

Figura 5. Topología: tráfico unicast, broadcast y multicast



Fuente: elaboración Propia

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

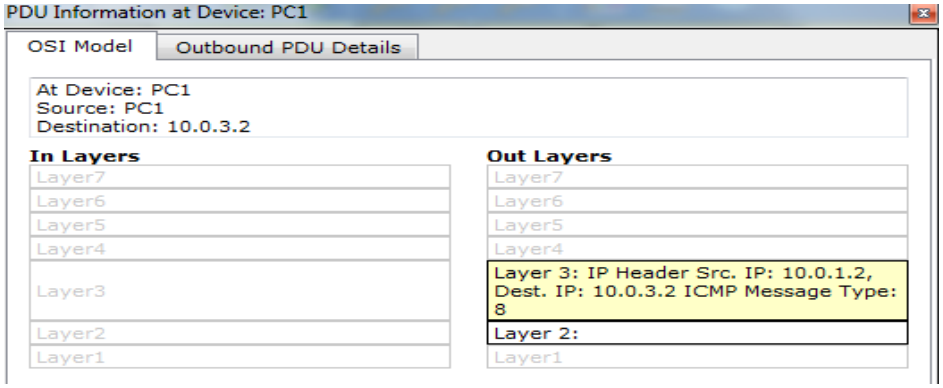
De la PC1 al Switch1, después al Router1 y, finalmente, al Router3, y viceversa.

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 abre la ventana PDU Information (Información de PDU).

¿En qué capa comienza esta transmisión y por qué?

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

Figura 6. Transmisión IP e ICMP.



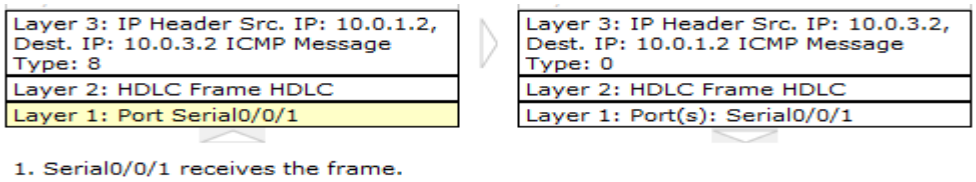
Fuente: elaboración Propia

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?

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

Figura 7. Transmisión ICMP



Fuente: elaboración Propia

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

1.1.2. 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 (+).

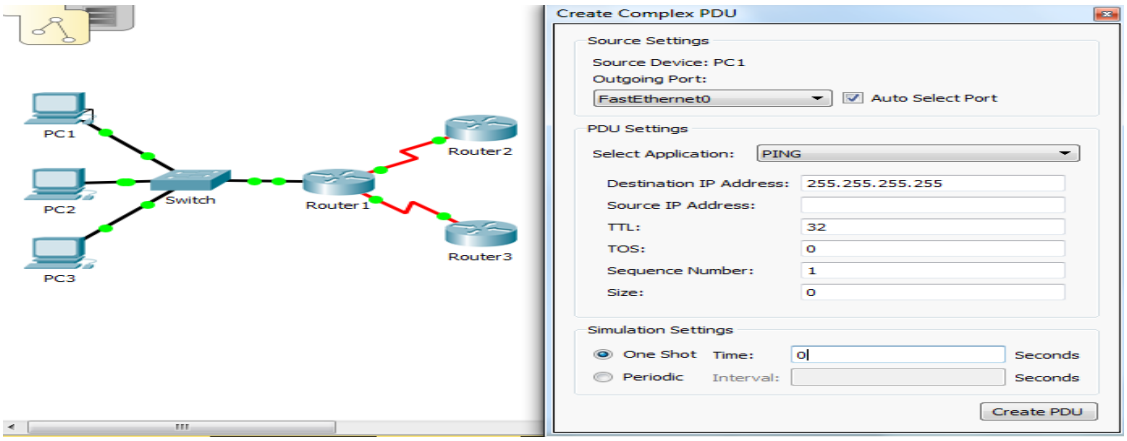
c. Haga clic en **PC1** para que funcione como origen de este mensaje de prueba, y se abrirá la ventana de diálogo **Create Complex PDU** (Crear una PDU compleja). Introduzca los siguientes valores:

- 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?

Respuesta: DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP y OTHER.

Figura 8. PDU

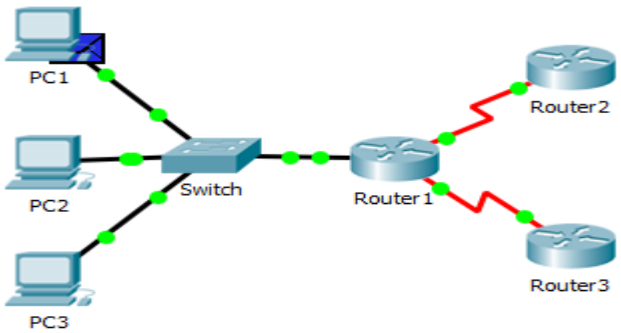


Fuente: elaboración Propia

d. Haga clic en **Create PDU** (Crear PDU). Este paquete de broadcast de prueba ahora aparece

en **Simulation Panel Event List.** También aparece en la ventana PDU List (Lista de PDU). Es la primera PDU para la Situación 0.

Figura 9. Simulación PDU Lista.



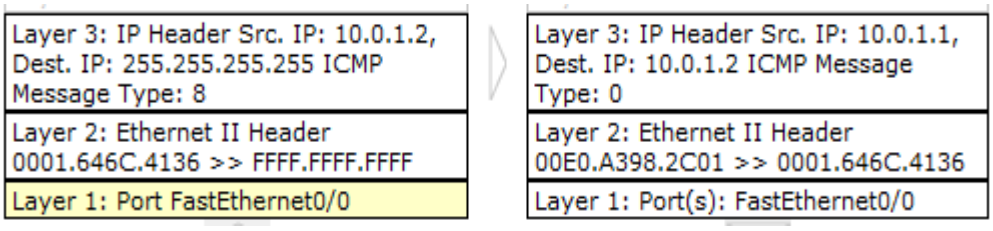
Fuente: elaboración Propia

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.

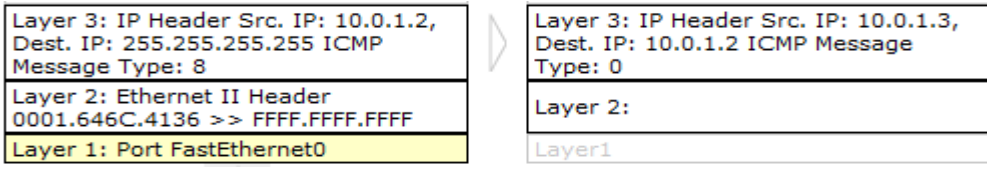
Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

Figura 10. Capture/Forward.

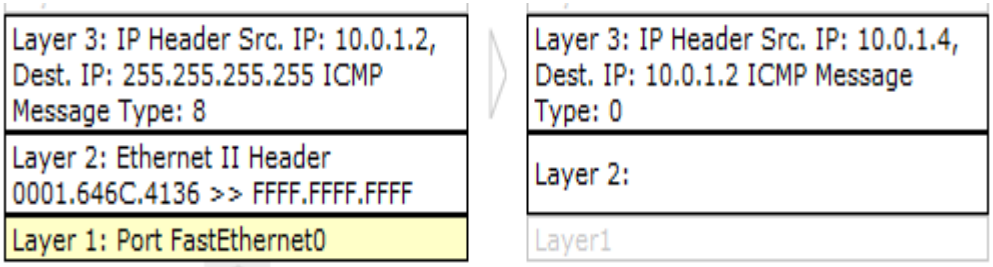
Router1



PC2



PC1



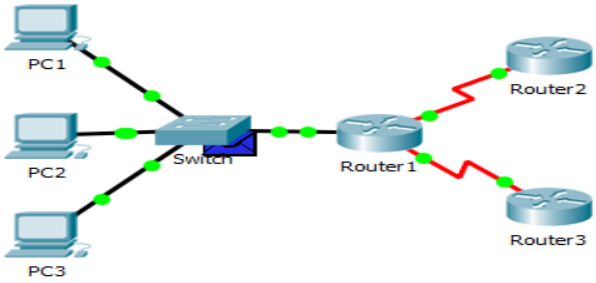
Fuente: elaboración Propia

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?

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

Figura 11. PDU se convierte en un unicast que contesta a la PC1.



Fuente: elaboración Propia

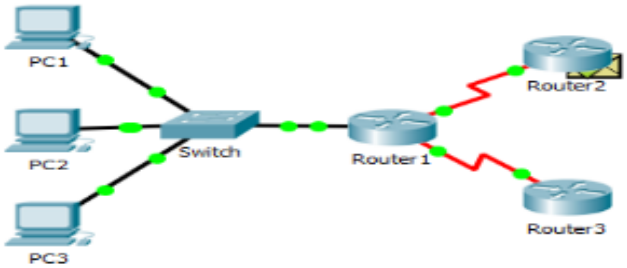
g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en **Delete** (Eliminar) debajo de **Scenario 0** (Situación 0).

1.1.3. 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.

Figura 12. Tráfico de multicast

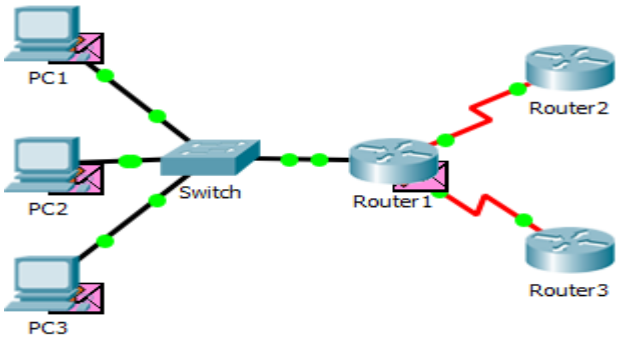


Fuente: elaboración Propia

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.

Figura 13. Paquete EIGRP



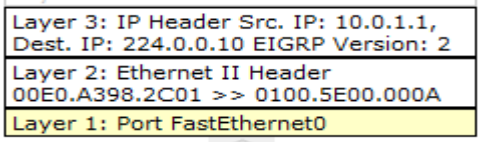
Fuente: elaboración Propia

¿Qué hacen los hosts con los paquetes?

Los hosts rechazan y descartan los paquetes.

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

Figura 14. Eventos EIGRP



Fuente: elaboración Propia

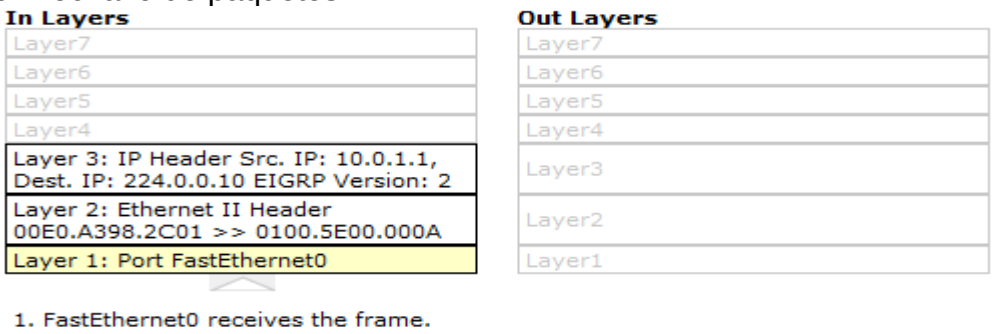
¿Cuál es la dirección de destino de cada uno de los paquetes?

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?**

Los paquetes se descartan y no se realiza ningún procesamiento adicional.

Figura 15. Rechazo de paquetes



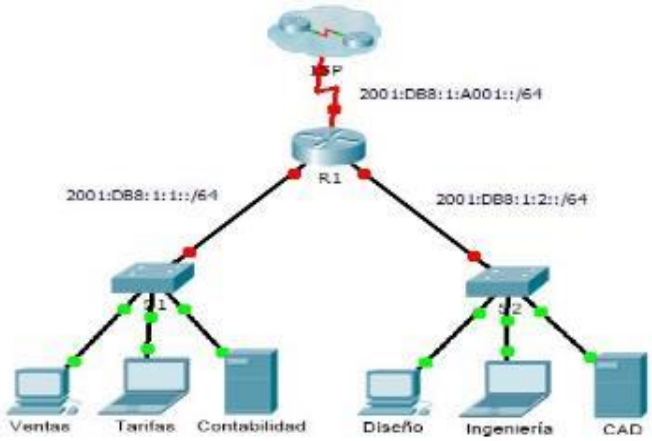
Fuente: elaboración Propia

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

Respuesta: 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.

1.2. PACKET TRACER: CONFIGURACIÓN DE DIRECCIONAMIENTO IPV6

Figura 16. Direccionamiento IPV6



Fuente: elaboración Propia

Tabla 1: Direccionamiento IPV6

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

Fuente: elaboración Propia

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.

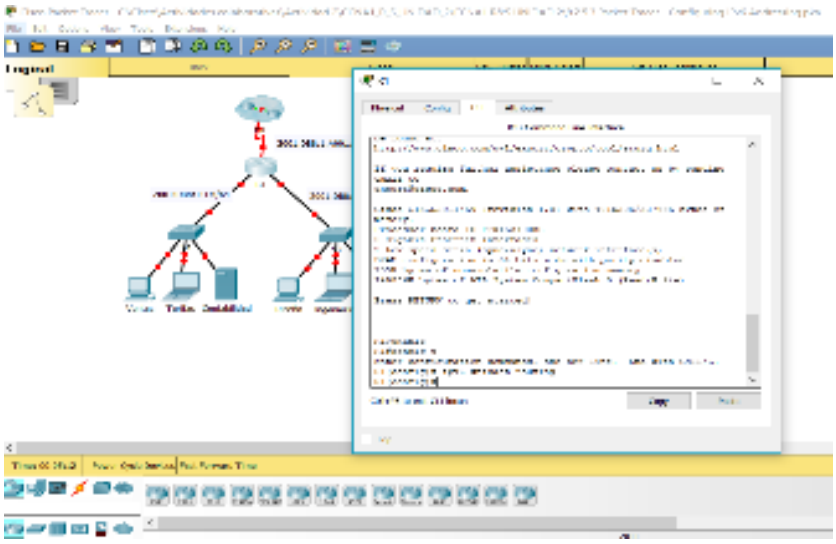
1.2.1. Parte 1: Configurar el direccionamiento IPv6 en el router

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

Figura 17. Direccionamiento IPV6 en router



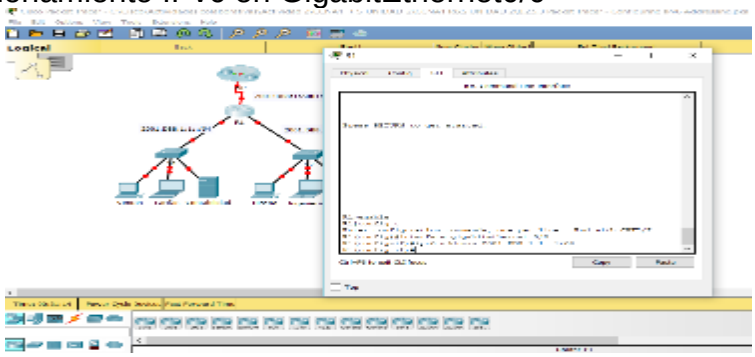
Fuente: elaboración Propia

Paso 2: Configurar el direccionamiento IPv6 en *GigabitEthernet0/0*

a. Haga clic en *R1* y, a continuación, haga clic en la ficha *CLI*. Presione **Entrar**.
b. Ingrese al modo EXEC privilegiado.
c. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/0.
d. Configure la dirección IPv6 con el siguiente comando:

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

Figura 18. Direccionamiento IPv6 en GigabitEthernet0/0

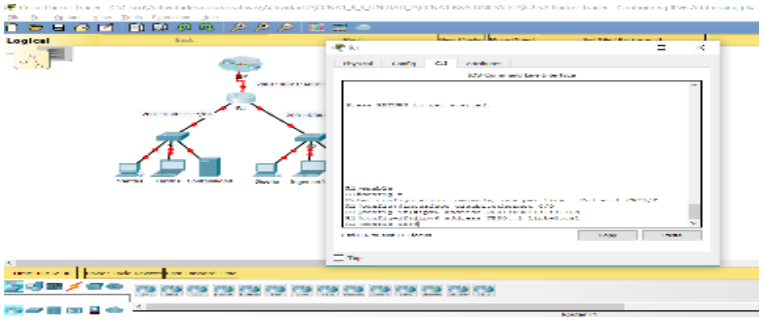


Fuente: elaboración Propia

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

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

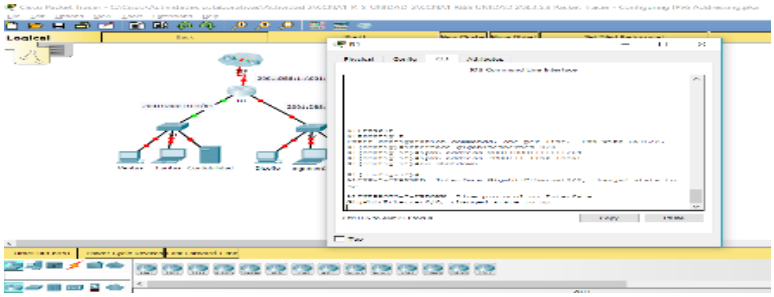
Figura 19. Dirección IPv6 link-local



Fuente: elaboración Propia

f. Active la interfaz.

Figura 20. Dirección IPv6 active la interfaz

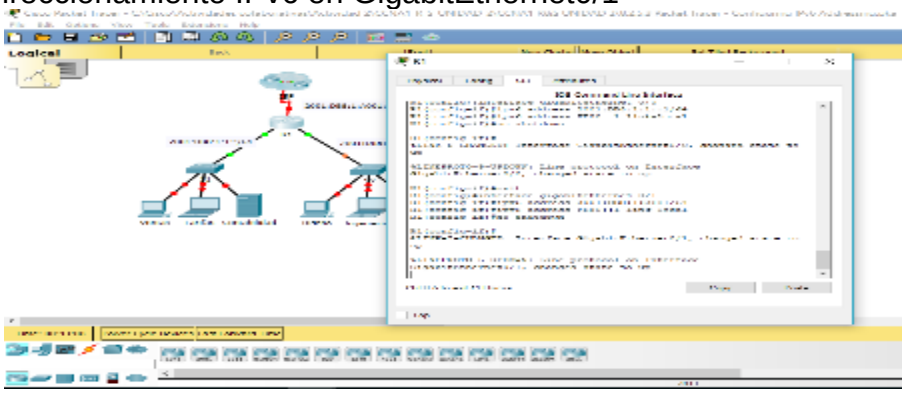


Fuente: elaboración Propia

Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para GigabitEthernet0/1.
b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.
c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Figura 21. Direccionamiento IPv6 en GigabitEthernet0/1

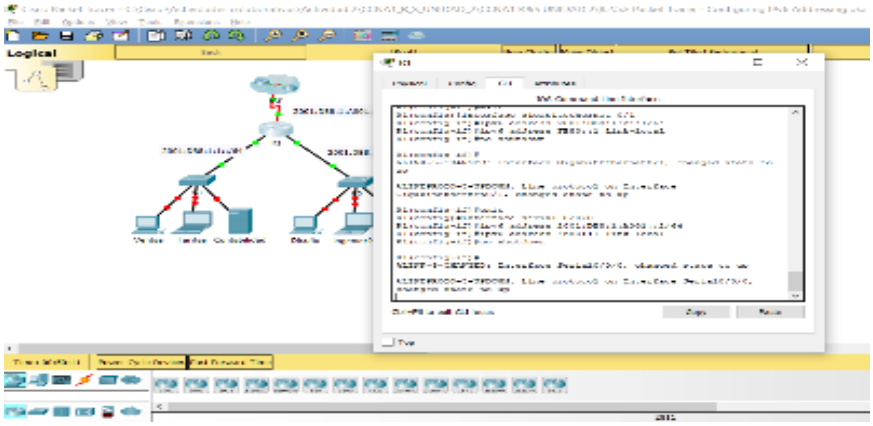


Fuente: elaboración Propia

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

a. Introduzca los comandos necesarios para la transición al modo de configuración de interfaz para Serial0/0/0.
b. Consulte la **tabla de direccionamiento** para obtener la dirección IPv6 correcta.
c. Configure la dirección IPv6, la dirección link-local y active la interfaz.

Figura 22. Direccionamiento IPv6 en Serial0/0/0



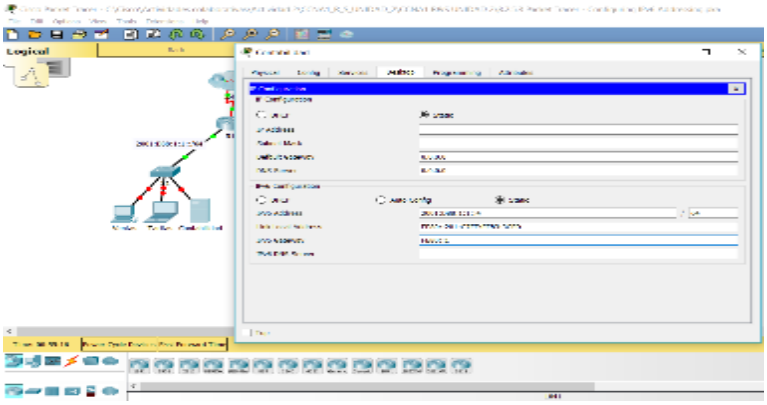
Fuente: elaboración Propia

1.2.2. 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**.

Figura 23. Direccionamiento IPv6 en los servidores

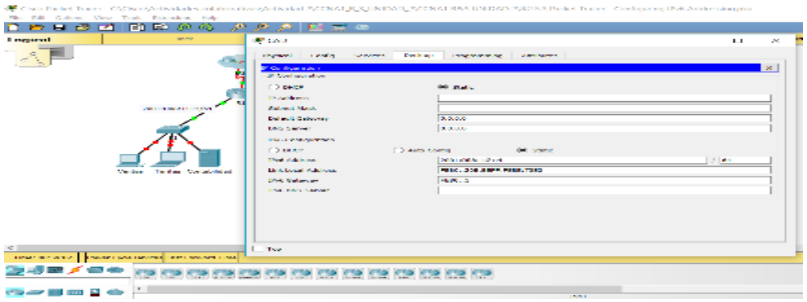


Fuente: elaboración Propia

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.

Figura 24. Direccionamiento IPv6 en el servidor CAD



Fuente: elaboración Propia

1.2.3. Parte 3: Configurar el direccionamiento IPv6 en los clientes.

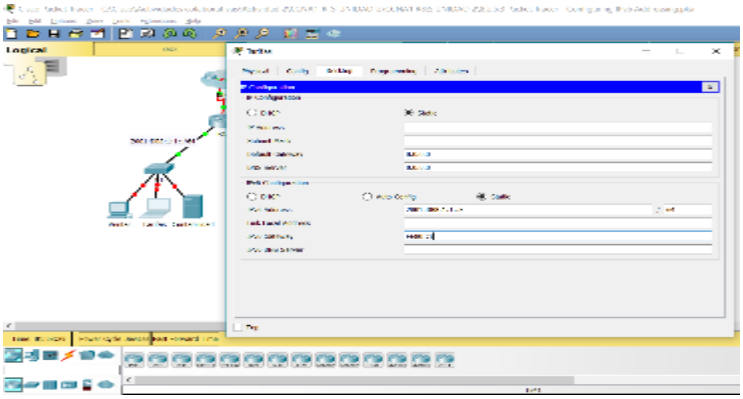
Paso 1: Configurar el direccionamiento IPv6 en los clientes de ventas y facturación

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.

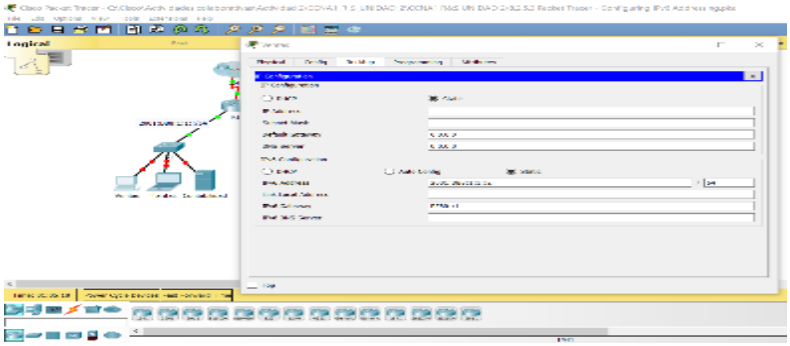
Figura 25. Direccionamiento IPv6 en los clientes



Fuente: elaboración Propia

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

Figura 26. Direccionamiento IPv6 en cliente ventas

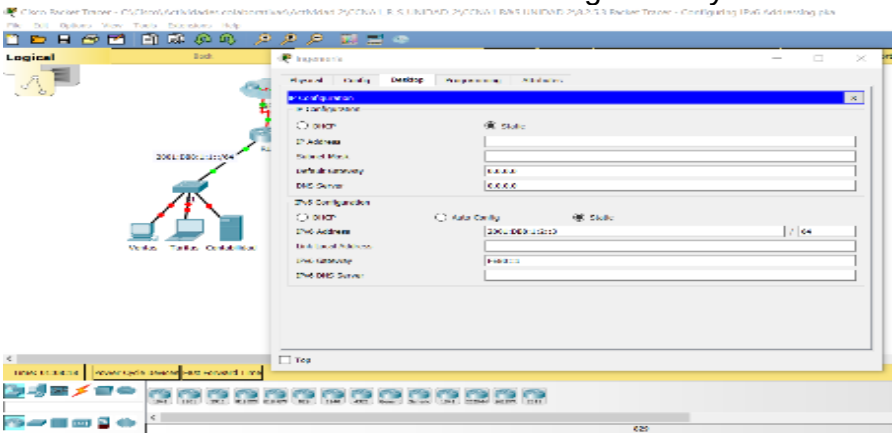


Fuente: elaboración Propia

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**.

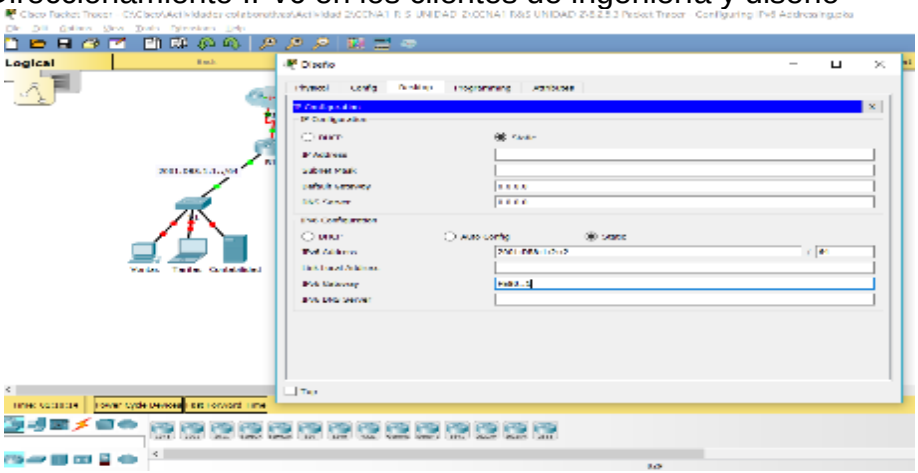
Figura 27. Direccionamiento IPv6 en los clientes de ingeniería y diseño



Fuente: elaboración Propia

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

Figura 28. Direccionamiento IPv6 en los clientes de ingeniería y diseño



Fuente: elaboración Propia

1.2.4. Parte 4: Probar y verificar la conectividad de la red

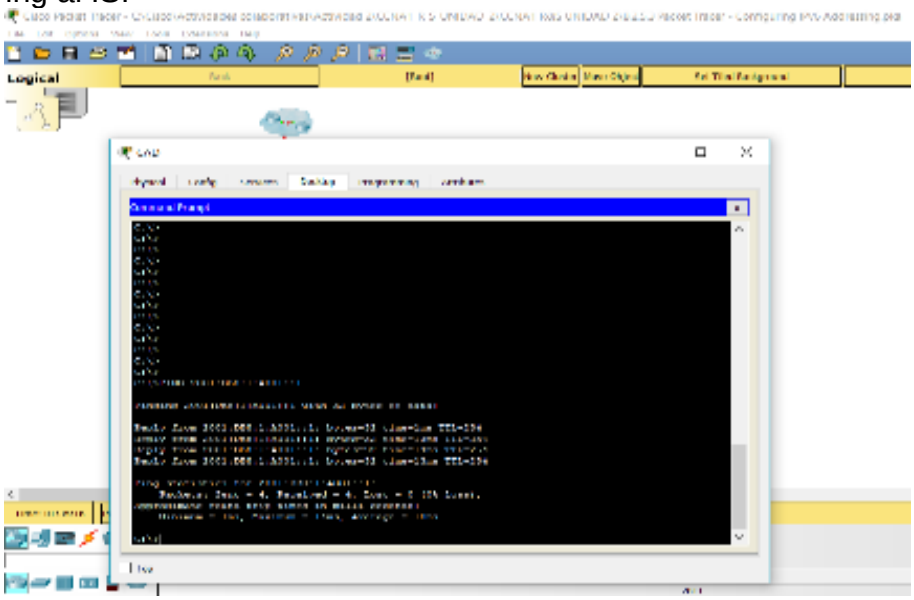
Paso 1: Abrir las páginas Web del servidor de los clientes

a. Haga clic en **Sales** y, a continuación, en la ficha **Desktop**. Si es necesario, cierre la ventana **IP Configuration**.
b. Haga clic en **Web Browser** (Explorador Web). Introduzca **2001:DB8:1:1::4** en el cuadro de dirección URL y haga clic en **Go** (Ir). Debería aparecer el sitio Web de **Accounting**.
c. Introduzca **2001:DB8:1:2::4** en el cuadro de dirección URL y haga clic en **Go**. Debería aparecer el sitio Web de **CAD**.
d. Repita los pasos 1a a 1d para el resto de los clientes.

Paso 2: Hacer ping al ISP

a. Abra una ventana de configuración de cualquier equipo cliente haciendo clic en el ícono.
b. Haga clic en la ficha Desktop > Command Prompt (Símbolo del sistema).
c. Pruebe la conectividad al ISP con el siguiente comando:
PC> ping 2001:DB8:1:A001::1
d. Repita el comando ping con otros clientes hasta que se haya verificado la conectividad completa.

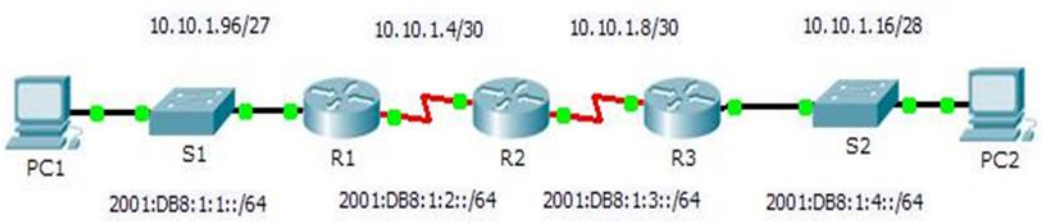
Figura 29. Ping al ISP



Fuente: elaboración Propia

1.3. PACKET TRACER: VERIFICACIÓN DIRECCIONAMIENTO IPV4 E IPV6

Figura 30. Topología verificación del direccionamiento IPV4 e IPV6



Fuente: elaboración Propia

Packet Tracer: Verificación del direccionamiento IPv4 e IPv6

Tabla 2. Direccionamiento ipv4 e ipv6

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	10.10.1.20	255.255.255.240	10.10.1.17
		2001:DB8:1:1::A/64		FE80::1
PC2	NIC	10.10.1.100	255.255.255.2240	10.10.1.97
		2001:DB8:1:4::A/64		FE80::3

Fuente: elaboración Propia

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.

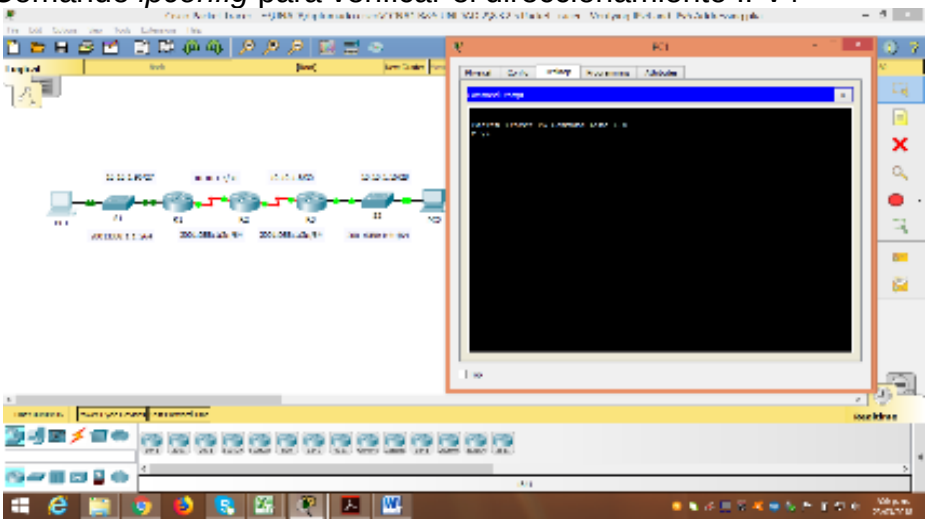
Packet Tracer: Verificación del direccionamiento IPv4 e IPv6

1.3.1. Parte 1: Completar la documentación 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).

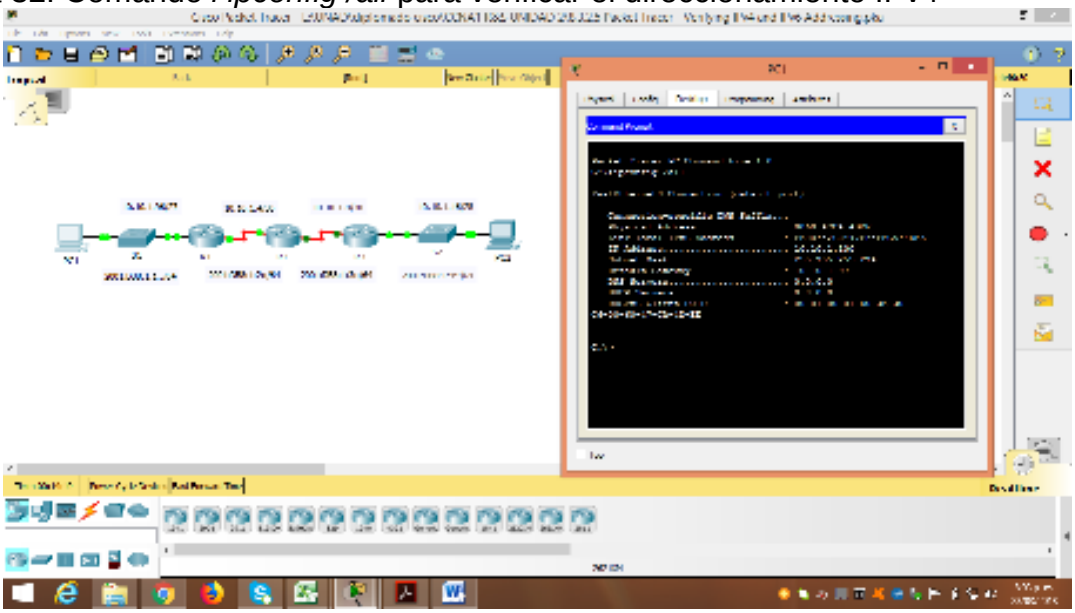
Figura 31. Comando *ipconfig* para verificar el direccionamiento IPv4



Fuente: elaboración Propia

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.

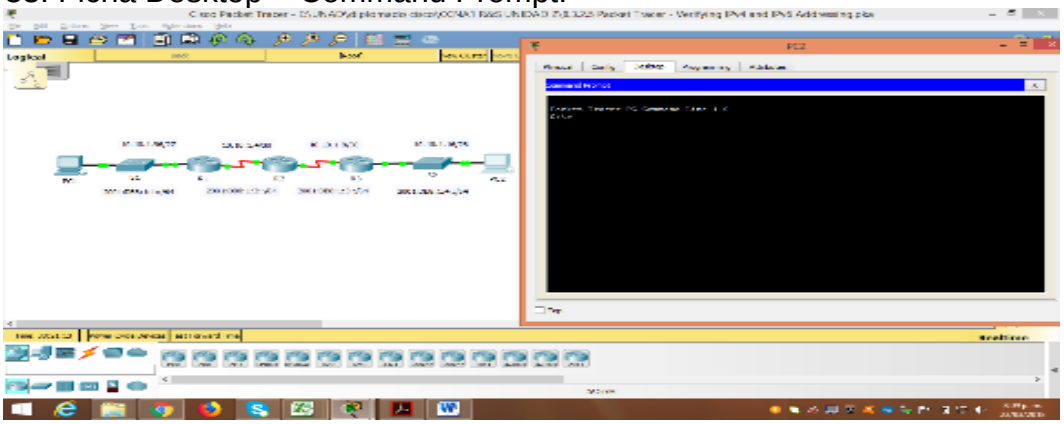
Figura 32. Comando *i ipconfig /all* para verificar el direccionamiento IPv4



Fuente: elaboración Propia

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

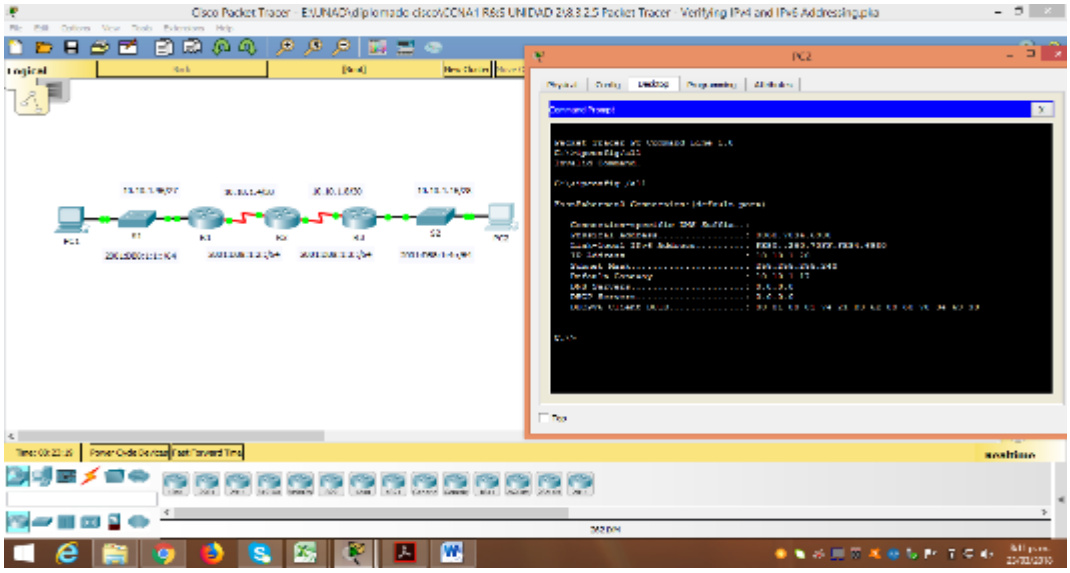
Figura 33. Ficha Desktop > Command Prompt.



Fuente: elaboración Propia

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.

Figura 34. Tabla de direccionamiento con la dirección IPv4

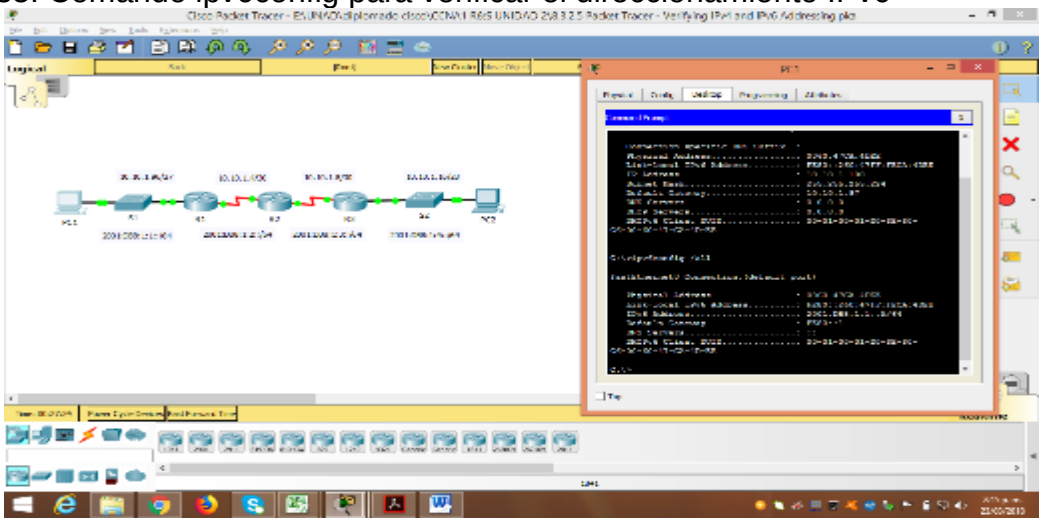


Fuente: elaboración Propia

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.

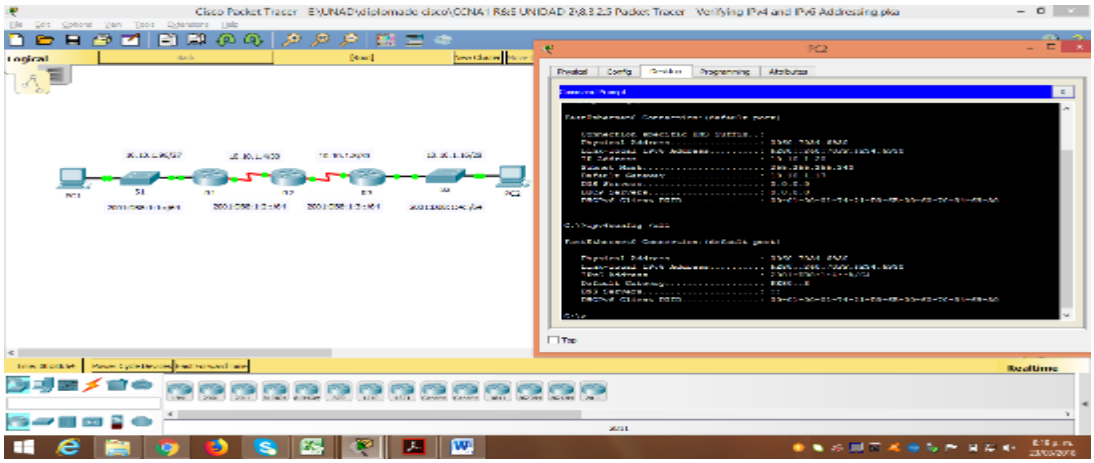
Figura 35. Comando ipv6config para verificar el direccionamiento IPv6



Fuente: elaboración Propia

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.

Figura 36. Tabla de direccionamiento con la dirección IPv6



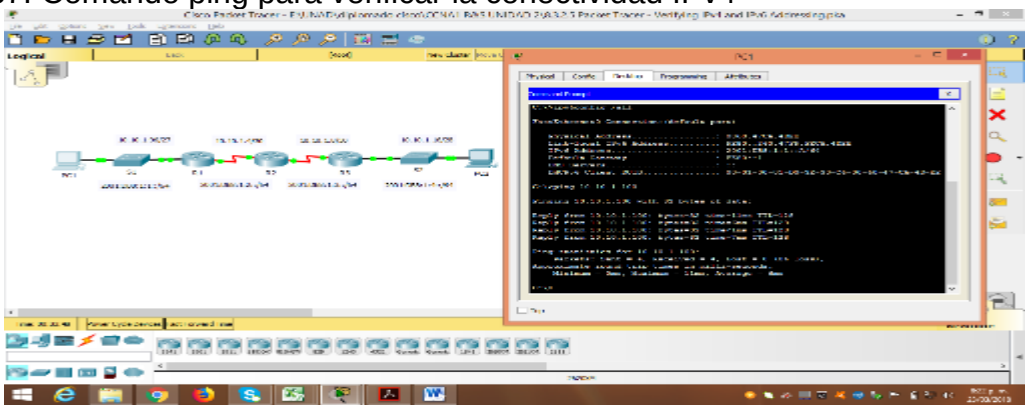
Fuente: elaboración Propia

1.3.2. 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? Sí, con un tiempo de respuesta promedio de 6ms y máximo de 11ms.

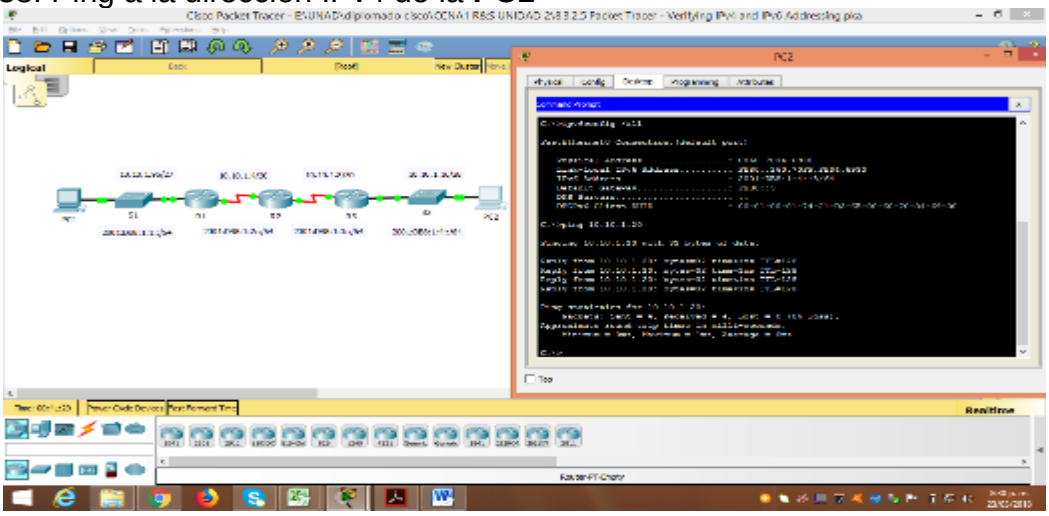
Figura 37. Comando ping para verificar la conectividad IPv4



Fuente: elaboración Propia

b. Desde la **PC2**, haga ping a la dirección IPv4 de la **PC1**. ¿El resultado fue satisfactorio? Sí, con un tiempo de respuesta promedio de 0ms y máximo de 1ms.

Figura 38. Ping a la dirección IPv4 de la **PC1**

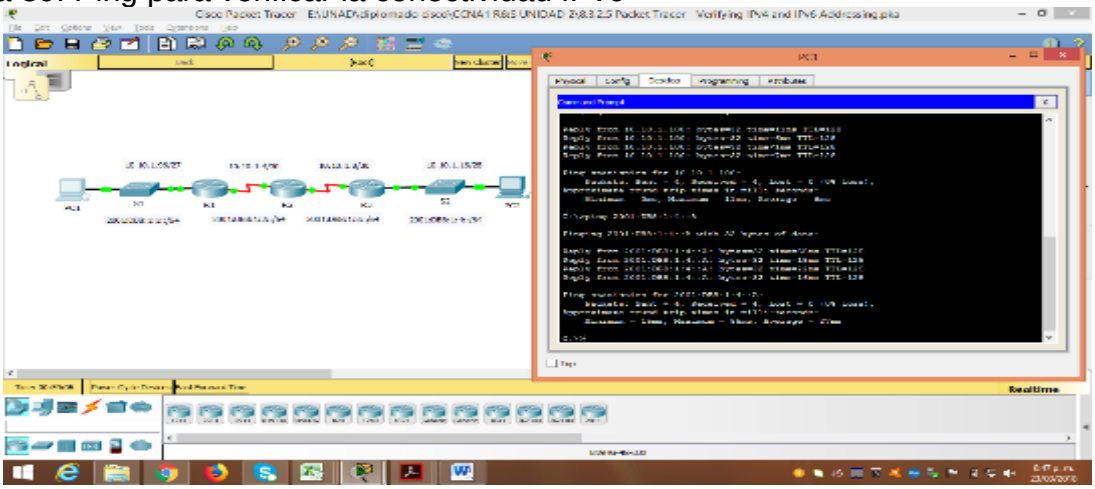


Fuente: elaboración Propia

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? Sí, con un tiempo de respuesta promedio de 27ms y máximo de 55ms.

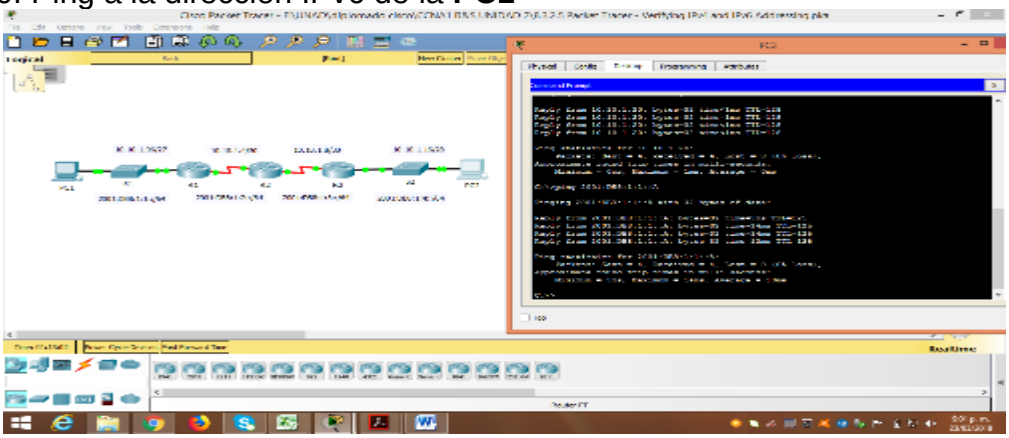
Figura 39. Ping para verificar la conectividad IPv6



Fuente: elaboración Propia

b. Desde la **PC2**, haga ping a la dirección IPv6 de la **PC1**. ¿El resultado fue satisfactorio? Sí, con un tiempo de respuesta promedio de 10ms y máximo de 14ms.

Figura 40. Ping a la dirección IPv6 de la **PC1**



Fuente: elaboración Propia

1.3.3. 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**

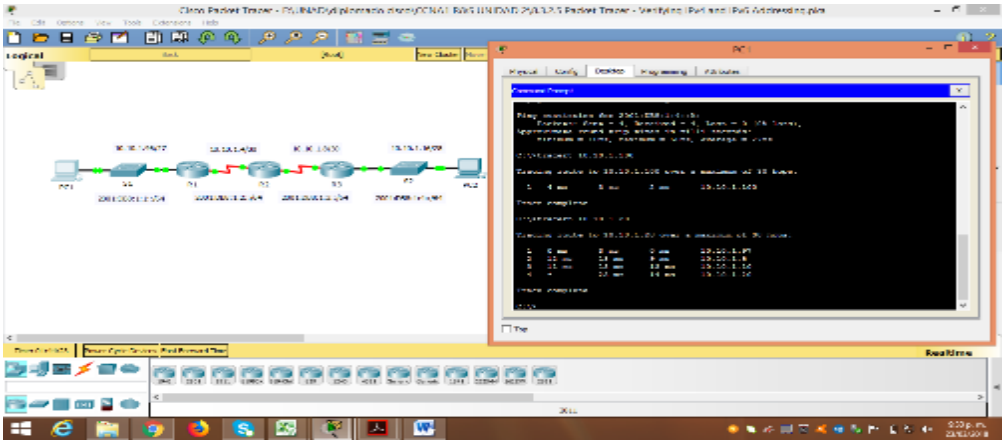
¿Qué direcciones se encontraron a lo largo de la ruta? Las direcciones encontradas son:

- 10.10.1.97
- 10.10.1.5
- 10.10.1.10
- 10.10.1.20

¿Con qué interfaces se asocian las cuatro direcciones? Las interfaces asociadas son:

- G0/0 del R1
- S0/0/0 en el R2
- S0/0/01 en el R3
- NIC de la PC2.

Figura 41. Interfaces asociadas



Fuente: elaboración Propia

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

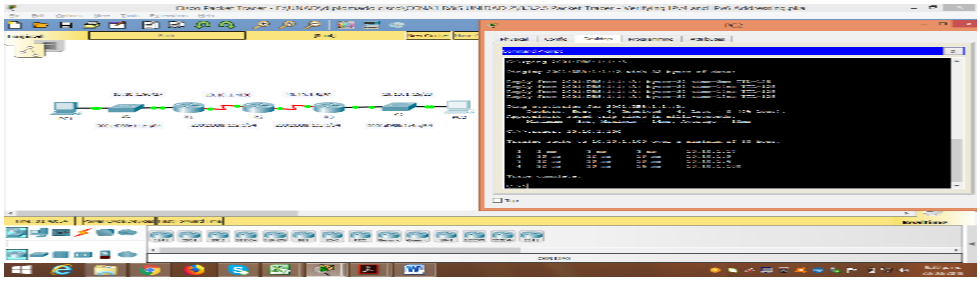
¿Qué direcciones se encontraron a lo largo de la ruta? Las direcciones encontradas son:

- 10.10.1.17
- 10.10.1.9
- 10.10.1.6
- 10.10.1.100

¿Con qué interfaces se asocian las cuatro direcciones? Las interfaces asociadas son:

- G0/0 del R3
- S0/0/1 del R2
- S0/0/1 del R1
- NIC de la PC1

Figura 42. Interfaces asociadas dos



Fuente: elaboración Propia

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**

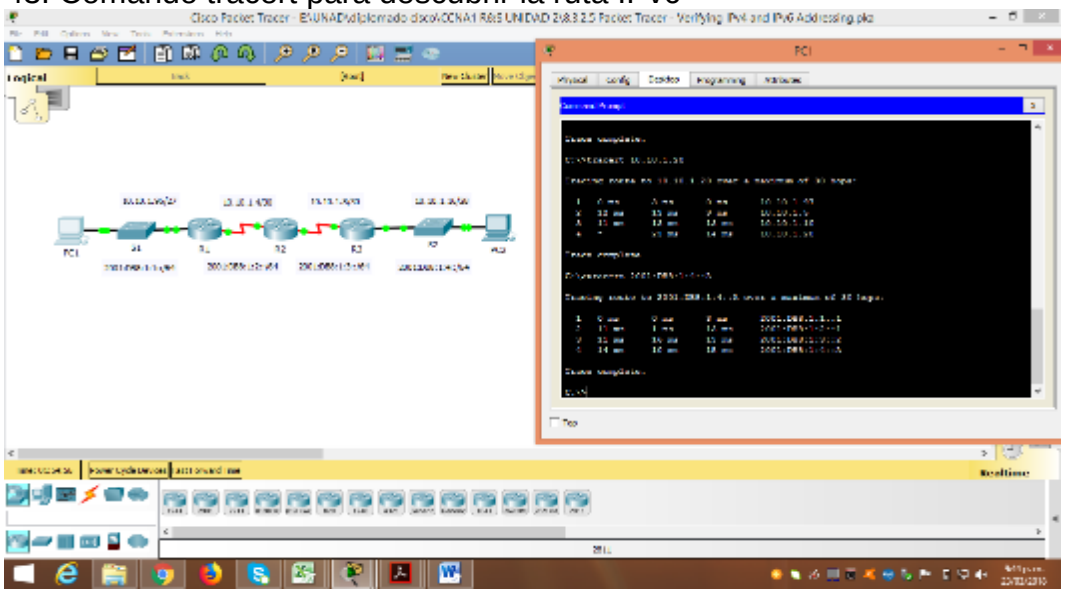
¿Qué direcciones se encontraron a lo largo de la ruta? Las direcciones encontradas son:

- 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? Las interfaces asociadas son:

- G0/0 del R1
- S0/0/0 del R2
- S0/0/1 del R3
- NIC de la PC2.

Figura 43. Comando tracert para descubrir la ruta IPv6



Fuente: elaboración Propia

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

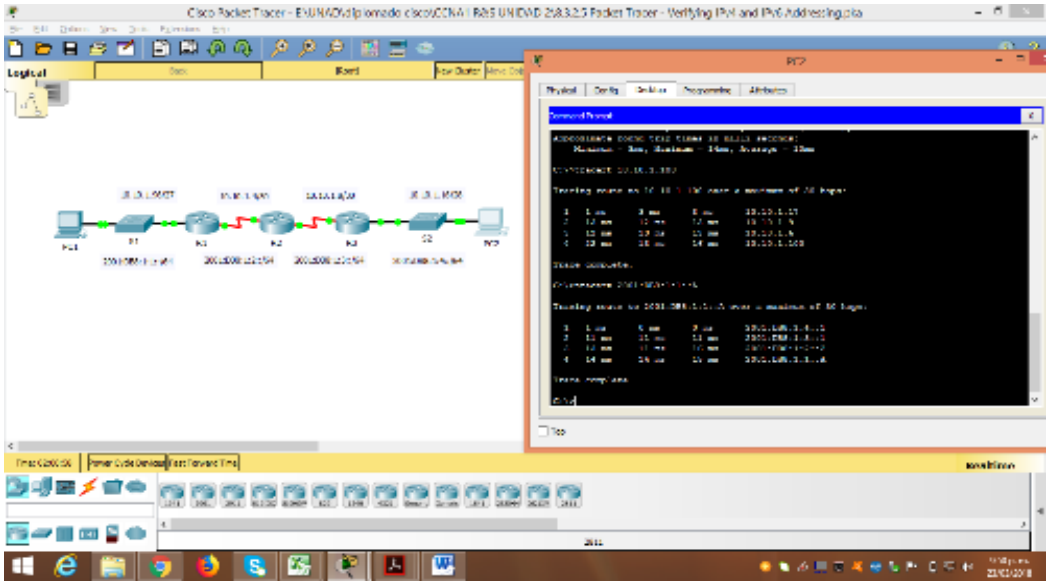
¿Qué direcciones se encontraron a lo largo de la ruta? Las direcciones encontradas son:

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? Las interfaces asociadas son:

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

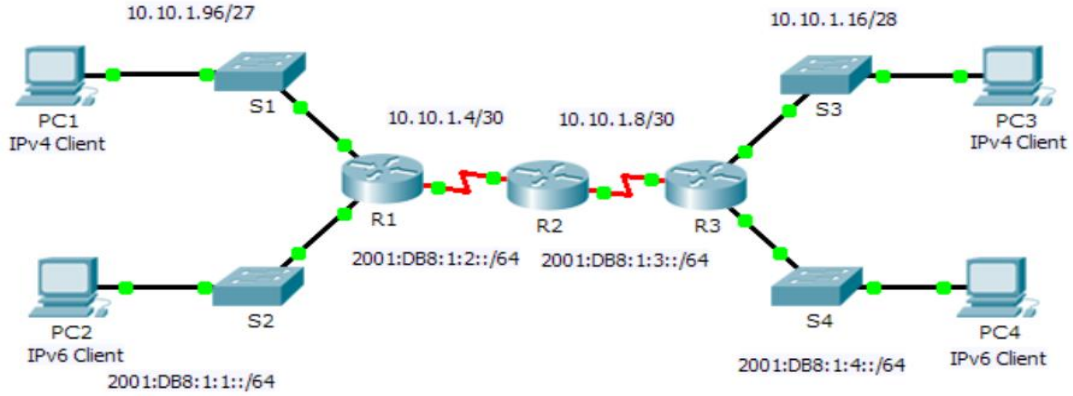
Figura 44. Interfaces asociadas la ruta IPv6



Fuente: elaboración Propia

1.4. PACKET TRACER: PINGING AND TRACING TO TEST THE PATH

Figura 45. Topología pinging and tracing to test the path



Fuente: elaboración Propia

Tabla 3. Ping y rastreo para probar la ruta

Dispositivo	**Interfaz**	**Dirección IPv4**	**Mascara de subred**	**Gateway predeterminado**
		Dirección / prefijo IPv6		
R1	G0/0	2001:db8:1:1::1/64		No aplicable
	G0/1	10.10.1.97	255.255.255.224	No aplicable
	S0/0/1	10.10.1.6	255.255.255.252	No aplicable
		2001:db8:1:2::2/64		No aplicable
	Link-local	Fe80::1		No aplicable
R2	S0/0/0	10.10.1.5	255.255.255.252	No aplicable
		2001:db8:1:2::1/64		No aplicable
	S0/0/1	10.10.1.9	255.255.255.252	No aplicable
		2001:db8:1:3::1/64		No aplicable
	Link-local	Fe80::2		No aplicable
R3	G0/0	2001:db8:1:4::1/64		No aplicable
	G0/1	10.10.1.17	255.255.255.240	No aplicable
	S0/0/1	10.10.1.10	255.255.255.252	No aplicable
		2001:db8:1:3::2/64		No aplicable
	Link-local	Fe80::3		No aplicable
PC1	NIC	10.10.1.98	255.255.255.224	10.10.1.97
PC2	NIC	2001:db8:1:1::2/64		Fe80::1
PC3	NIC	10.10.1.18	255.255.255.240	10.10.1.17
PC4	NIC	2001:db8:1:4::2/64		Fe80::2

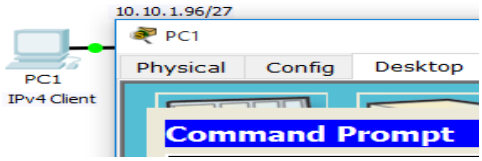
Fuente: elaboración Propia

1.4.1. 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).

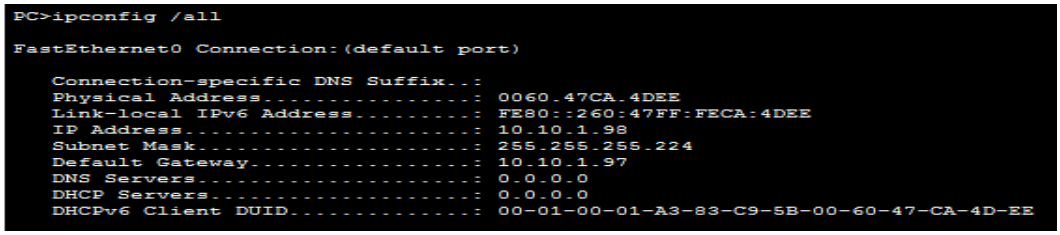
Figura 46. Comandos *ipconfig* y ping para verificar la conectividad



Fuente: elaboración Propia

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.

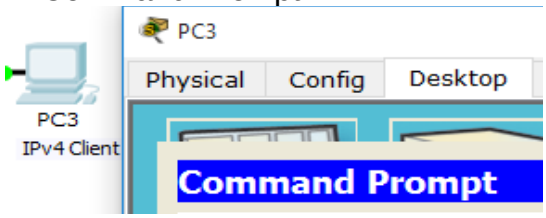
Figura 47. Direccionamiento IPV4



Fuente: elaboración Propia

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

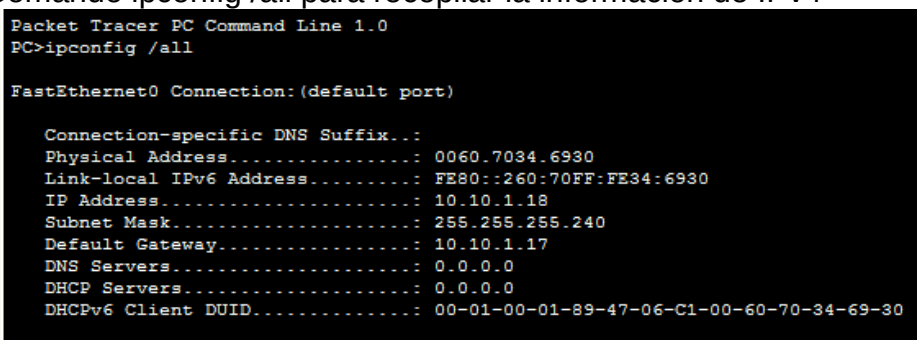
Figura 48. Ficha Desktop > Command Prompt



Fuente: elaboración Propia

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.

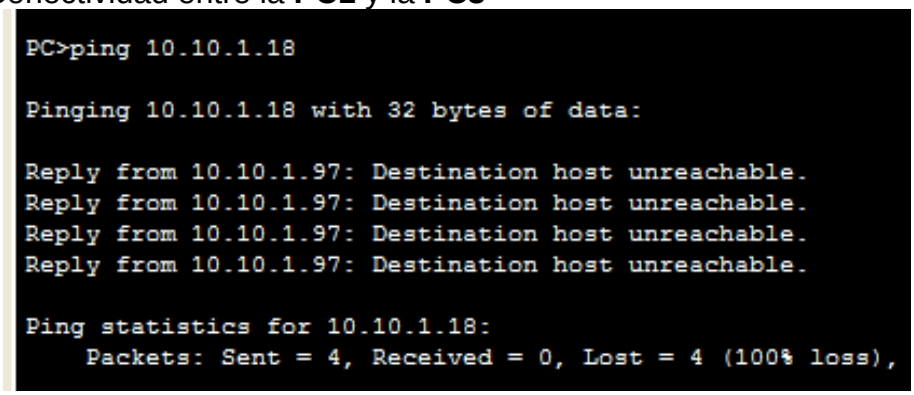
Figura 49. Comando ipconfig /all para recopilar la información de IPv4



Fuente: elaboración Propia

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

Figura 50. Conectividad entre la **PC1** y la **PC3**



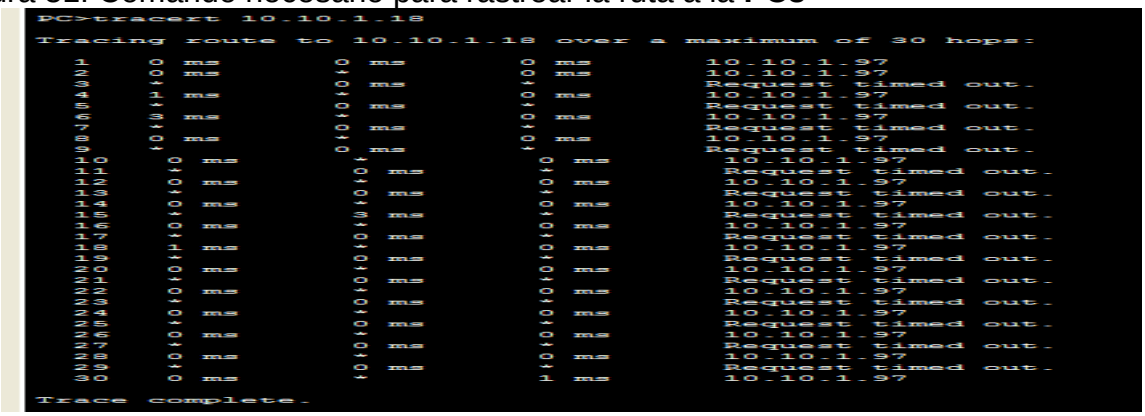
Fuente: elaboración Propia

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**. TRACERT

¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.97

Figura 51. Comando necesario para rastrear la ruta a la **PC3**

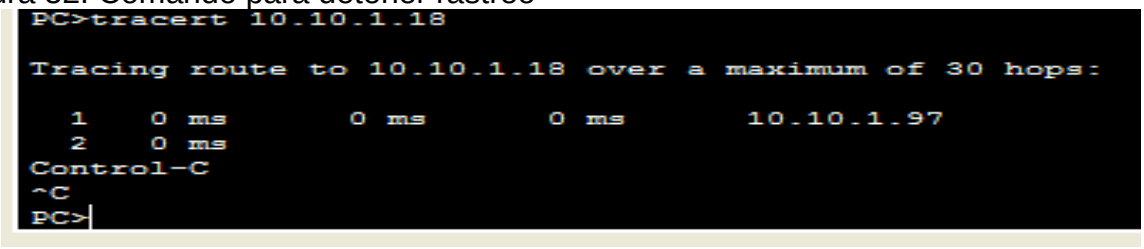


Fuente: elaboración Propia

b. El rastreo finalmente terminará después de 30 intentos.

Introduzca **Ctrl**+**C** para detener el rastreo antes de los 30 intentos.

Figura 52. Comando para detener rastreo



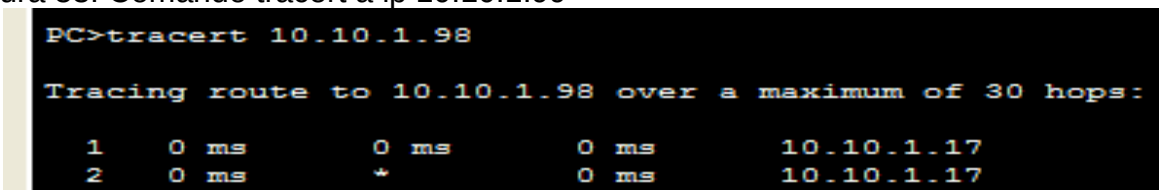
Fuente: elaboración Propia

c. Desde la **PC3**, introduzca el comando necesario para rastrear la ruta a la **PC1**. TRACERT

d.

¿Cuál es la última dirección IPv4 correcta que alcanzó? 10.10.1.17

Figura 53. Comando tracert a ip 10.10.1.99



Fuente: elaboración Propia

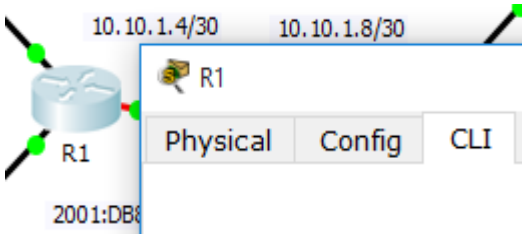
e. Introduzca Ctrl+C para detener el rastreo.

Figura 54. Comando Ctrl+C para detener el rastreo

Fuente: elaboración Propia

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

Figura 55. Inicio de sesión en el router



Fuente: elaboración Propia

g. Introduzca el comando **show ip interface brief** para obtener una lista de las interfaces y su estado.

Figura 56. Comando *show ip interface*

```
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>
```

Fuente: elaboración Propia

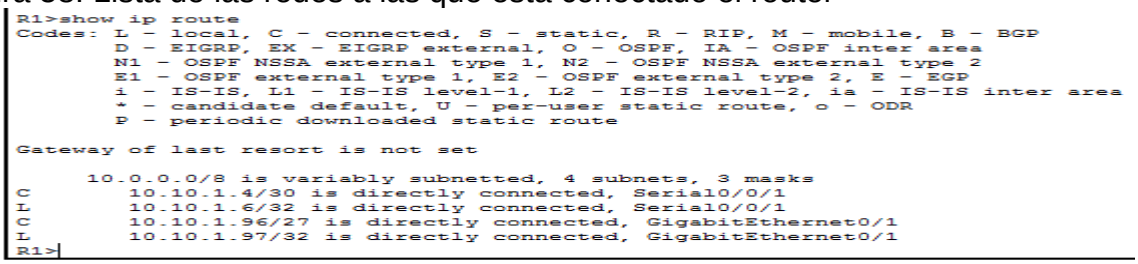
Hay dos direcciones IPv4 en el router. Una se debió haber registrado en el paso 2a. ¿Cuál es la otra? 10.10.1.6

Figura 57. Serial 10/0/1 e IP 10.10.1.6

Fuente: elaboración Propia

h. Introduzca el comando show ip route para obtener una lista de las redes a las que está conectado el router.

Figura 58. Lista de las redes a las que está conectado el router

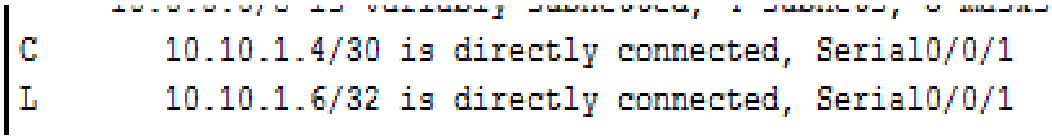


Fuente: elaboración Propia

Observe que hay dos redes conectadas a la interfaz **Serial0/0/1**.

¿Cuáles son? 10.10.1.6/32, 10.10.1.4/30

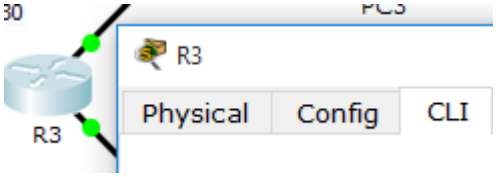
Figura 59. Redes conectadas a la interfaz **Serial0/0/1**



Fuente: elaboración Propia

i. 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

Figura 60. Configuración router tres



Fuente: elaboración Propia

Figura 61. Ip interface brief

```
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>
```

Fuente: elaboración Propia

Figura. Ip route

```
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>
```

Fuente: elaboración Propia

Observe cómo cambia la interfaz serial para el R3.

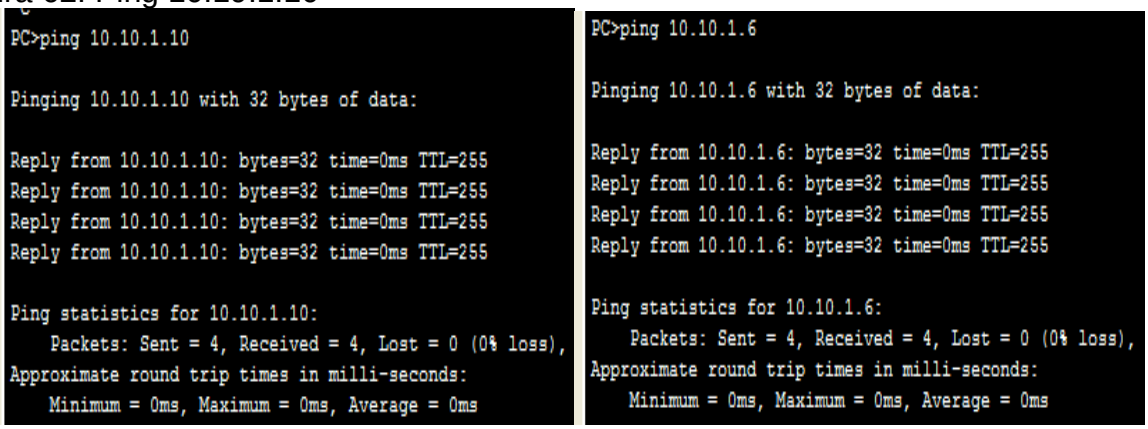
j. Ejecute más pruebas si eso permite visualizar el problema. El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red.

Desde el PC1 a R1 hay respuesta, desde el PC3 a R3 hay respuesta.

Figura 62. Ping 10.19.1.10

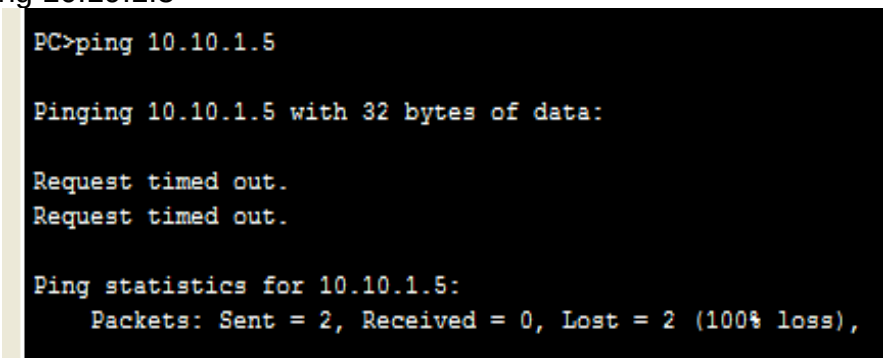


Fuente: elaboración Propia

¿Cuál es el error?

La interfaz Serial 0/0/0 del R2 está configurada con una dirección IP incorrecta.

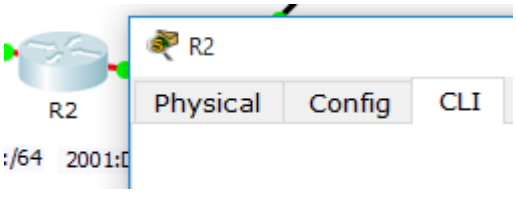
Figura 63. Ping 10.19.1.5



Fuente: elaboración Propia

b. ¿Qué solución propondría para corregir el problema?

Figura 64. Configuración router dos



Fuente: elaboración Propia

Escribimos show ip interface brief

Figura 65. Comando show ip interface brief

```
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>
```

Fuente: elaboración Propia

Insertamos en y luego *show run*

Figura 66. Comando *show run*

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

Fuente: elaboración Propia

Buscamos la interfaz *serial 0/0/0*

Figura 67. Configuración de interface Serial 10/0/0

```
!
interface Serial0/0/0
 ip address 10.10.1.2 255.255.255.252
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:1:2::1/64
 ipv6 eigrp 1
 clock rate 2000000
!
```

Fuente: elaboración Propia

Podemos observar que en la tabla la dirección es 10.10.1.5 mientras que en R2 es 10.10.1.2 Insertamos *show ip route*

Figura 68. Comando *show ip route* en router dos

```
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, 01:22:14, Serial0/0/1
R2#
```

Fuente: elaboración Propia

Figura 69. Comando *conf t* en router dos

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
```

Fuente: elaboración Propia

Figura 70. Comando int 0/0/0

```
R2(config)#int s0/0/0
R2(config-if)#
```

Fuente: elaboración Propia

Figura 71. Comando *no ip address*

```
R2(config-if)#no ip address
R2(config-if)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Serial0/0/0            unassigned      YES manual up                    up

Serial0/0/1            10.10.1.9       YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
R2(config-if)#
```

Fuente: elaboración Propia

Se Observa observar que se quitó la dirección de la interfaz *serial 0/0/0*

Configurar la dirección IP correcta en la interfaz Serial 0/0/0 del R2 (10.10.1.5).

Figura 72. Configuración de ip en router dos

```
R2(config-if)#
R2(config-if)#ip address 10.10.1.5 255.255.255.252
R2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.1.6 (Serial0/0/0) is up: new
adjacency
```

Fuente: elaboración Propia

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**.

   Hacemos *tracert* desde el PC1 al PC3

Figura 73. Comando *tracert* para 10.10.1.18

```
PC>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      1 ms      10.10.1.5
  3    10 ms     3 ms      1 ms      10.10.1.10
  4    12 ms     2 ms      12 ms     10.10.1.18

Trace complete.
```

Fuente: elaboración Propia

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

Hacemos tracert desde el PC3 al PC1.

Figura 74. Comando *tracert* desde el PC3 al PC1

```
PC>tracert 10.10.1.98

Tracing route to 10.10.1.98 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.10.1.17
  2    0 ms      1 ms      1 ms      10.10.1.9
  3    11 ms     10 ms     1 ms      10.10.1.6
  4    13 ms     11 ms     1 ms      10.10.1.98

Trace complete.
```

Fuente: elaboración Propia

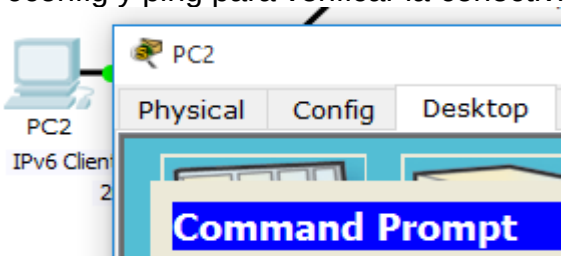
¿Se resolvió el problema? Sí

1.4.2. 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**.

Figura 75. Comandos ipv6config y ping para verificar la conectividad



Fuente: elaboración Propia

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.

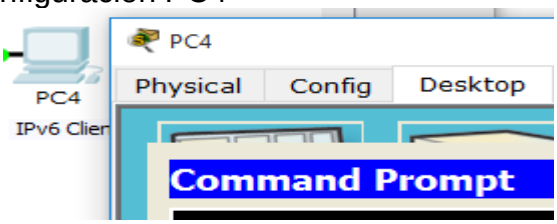
Figura 76. Comando ipv6config /all para recopilar la información de IPv6

```
Packet Tracer PC Command Line 1.0
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.....................: 00-01-00-01-3E-6D-BD-B0-00-E0-B0-35-82-B8
```

Fuente: elaboración Propia

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

Figura 77. Interfaz de configuración PC4



Fuente: elaboración Propia

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.

Figura 78. Comando ipv6config /all para recopilar la información de IPv6

```
Packet Tracer PC Command Line 1.0
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.....................: 00-01-00-01-83-CC-E0-C8-00-06-2A-BC-7C-D4
```

Fuente: elaboración Propia

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

Figura 79. Conectividad entre la **PC2** y la **PC4**

```
PC>ping 2001:bd8:1:4::2

Pinging 2001:bd8:1:4::2 with 32 bytes of data:

Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.

Ping statistics for 2001:BD8:1:4::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

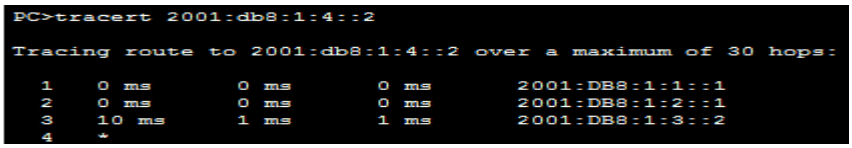
Fuente: elaboración Propia

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**. TRACERT

¿Cuál es la última dirección IPv6 correcta que se alcanzó? 2001:DB8:1:3::2.

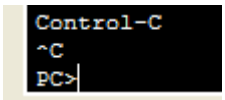
Figura 80. Comando tracert



Fuente: elaboración Propia

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

Figura 81. Comando Ctrl+C para detener el rastreo antes de los 30 intentos

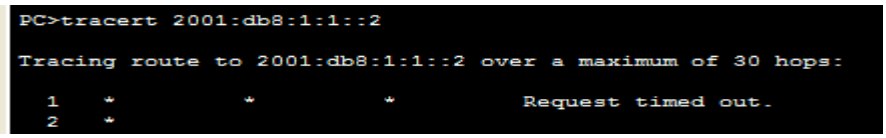


Fuente: elaboración Propia

c. Desde la PC4, introduzca el comando necesario para rastrear la ruta a la PC2. TRACERT

¿Cuál es la última dirección IPv6 correcta que se alcanzó?

Figura 82. Comando tracert sin alcanzar dirección IPv6



Fuente: elaboración Propia

No se alcanzó ninguna dirección IPv6.

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

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

Figura 83. Configuración router R3

Fuente: elaboración Propia

f. Introduzca el comando ***show ipv6*** **interface brief** para obtener una lista de las interfaces y su estado

. Figura 84. Lista de las interfaces

```
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>
```

Fuente: elaboración Propia

Hay dos direcciones IPv6 en el router.

Figura 85. Lista de direcciones IPv6

```
    2001:DB8:1:4::1
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
    FE80::3
    2001:DB8:1:3::2
```

Fuente: elaboración Propia

Una debe coincidir con la dirección de gateway registrada en el paso 1d.

Figura 86. Dirección IPv6

Fuente: elaboración Propia

¿Hay alguna discrepancia? Sí

g. Ejecute más pruebas si eso permite visualizar el problema.

El modo de simulación está disponible.

Paso 3: Proponga una solución para resolver el problema.

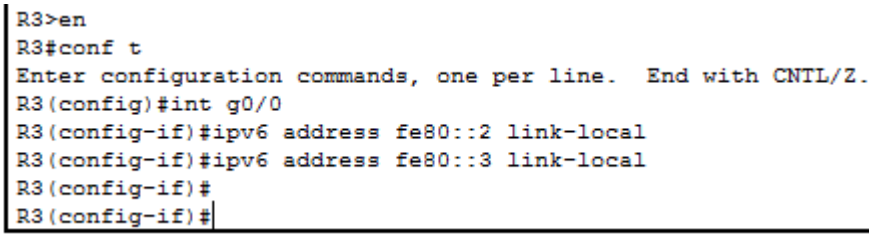
a. Compare sus respuestas del paso 2 con la documentación que tiene disponible para la red.

¿Cuál es el error?

La PC4 utiliza una configuración de gateway predeterminado incorrecta.

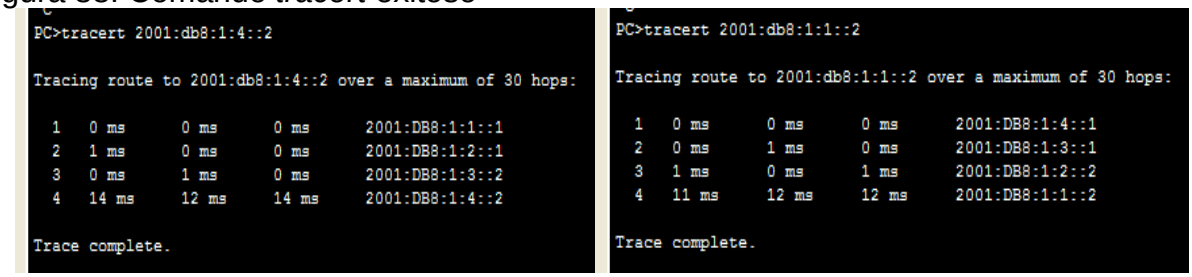
b. ¿Qué solución propondría para corregir el problema? Configurar la PC4 con la dirección de gateway predeterminado correcta: FE80::3.

Figura 87. Posible solución



Fuente: elaboración Propia

Figura 88. Comando *tracert* exitoso

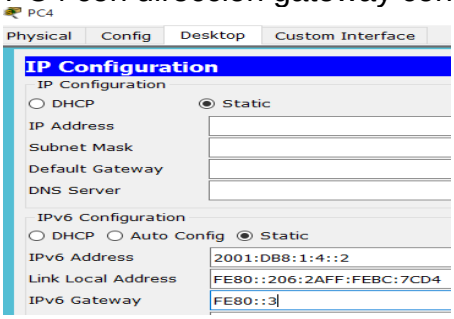


Fuente: elaboración Propia

Paso 4: Implemente el plan.

Implemente la solución que propuso en el paso 3b.

Figura 89. Configuración de PC4 con dirección gateway correcta

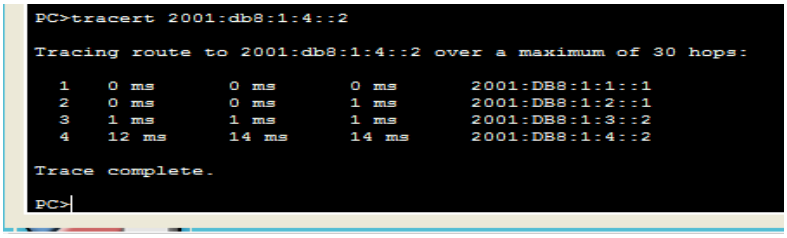


Fuente: elaboración Propia

Paso 5: Verifique que la conectividad esté restaurada.

Desde la PC2, pruebe la conectividad a la PC4.

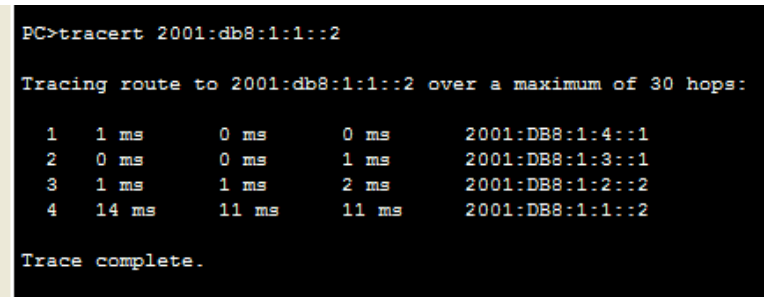
Figura 90. Conectividad a la PC4



Fuente: elaboración Propia

Desde la PC4, pruebe la conectividad a la PC2.

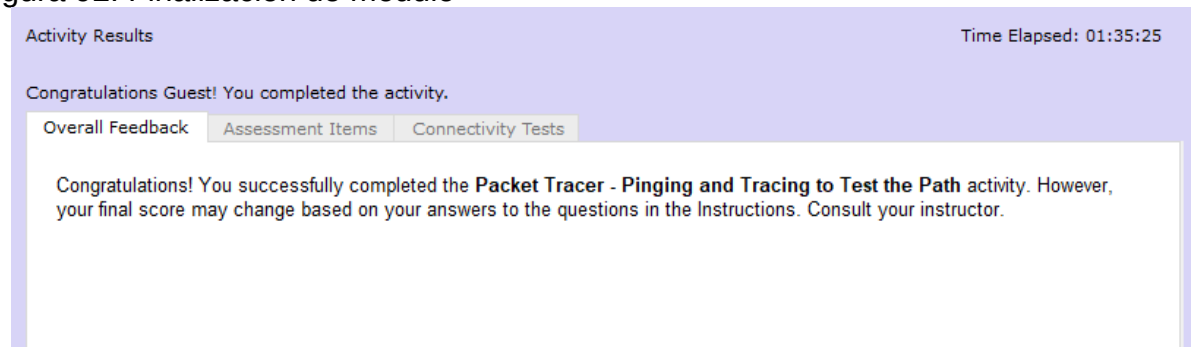
Figura 91. Conectividad a la PC2



Fuente: elaboración Propia

¿Se resolvió el problema? Sí

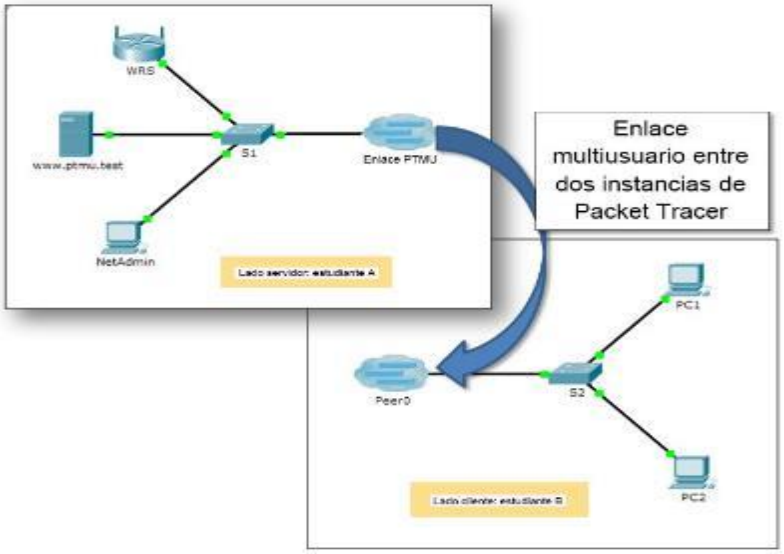
Figura 92. Finalización de modulo



Fuente: elaboración Propia

1.5. PACKET TRACER: IMPLEMENT SERVICES INSTRUCTIONS

Figura 93. Topología implement services instructions



Fuente: elaboración Propia

Tabla 4. Instrucciones de implementar servicios

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

Fuente: elaboración Propia

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.

1.5.1. 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.
c. El jugador del lado servidor abre el archivo *Packet Tracer Multiuser - Implement Services - Server Side.pka.*
d. El jugador del lado cliente abre el archivo *Packet Tracer Multiuser - Implement Services - Client Side.pka.*

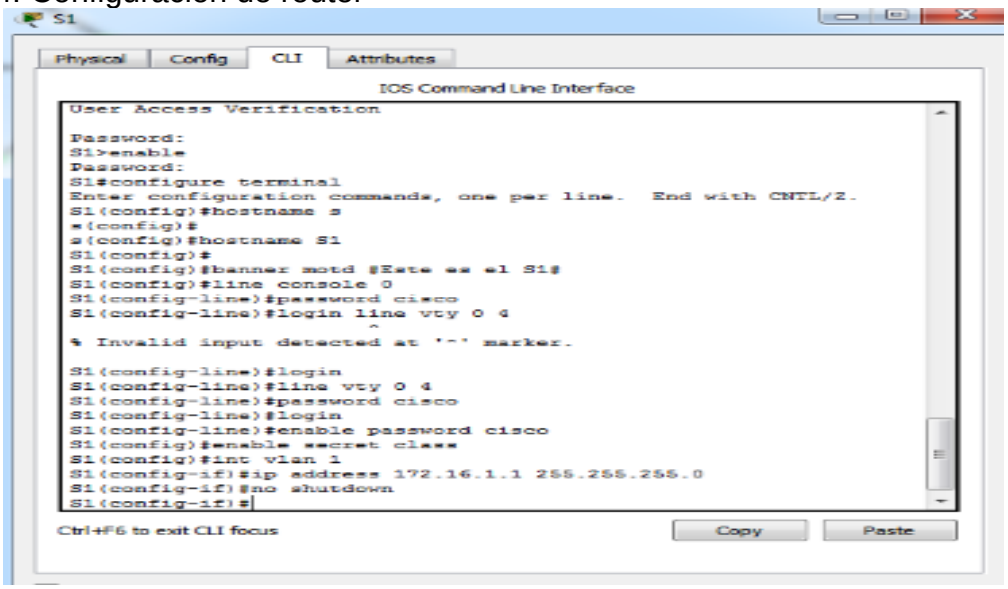
Nota: los estudiantes que realicen la actividad de forma individual pueden abrir los dos archivos y completar los pasos para los dos lados.

Paso 2: Configurar los parámetros iniciales de los *switches.*

Cada jugador: configure su respectiv*o switch* con los siguientes parámetros:

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

Figura 94. Configuración de router

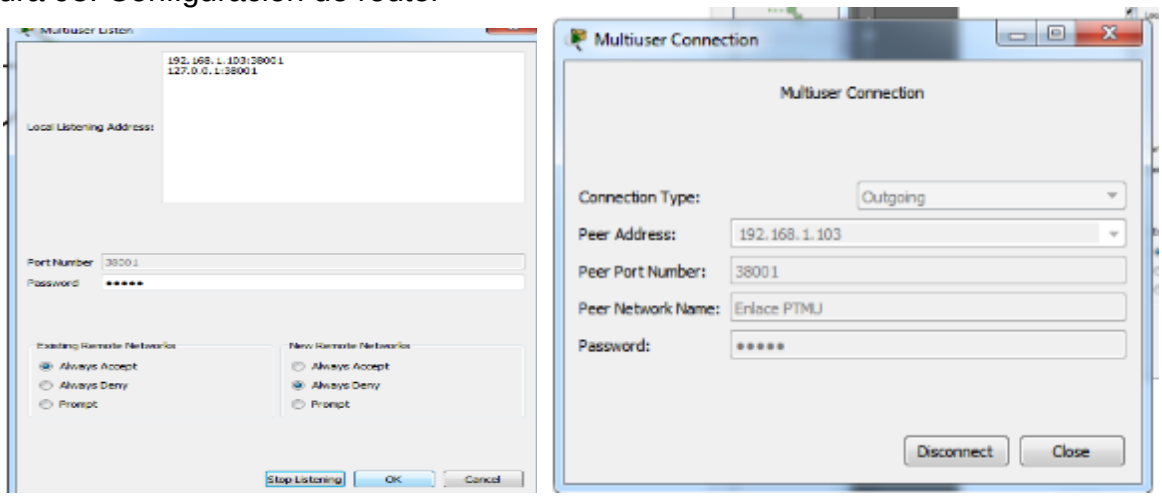


Fuente: elaboración Propia

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.

Figura 95. Configuración de router



Fuente: elaboración Propia

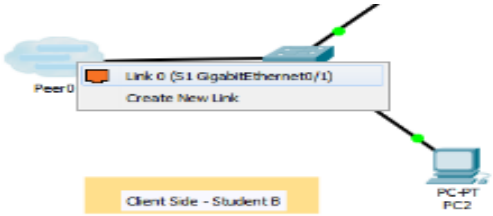
Paso 4: Jugador del lado cliente: Configurar la conexión multiusuario saliente

a. Jugador del lado cliente: registre la siguiente información que le proporcionó el jugador del lado servidor: Dirección IP: 192.168.1.103, número de puerto: 38001.

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

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

Figura 96. Configuración de la conexión multiusuario saliente

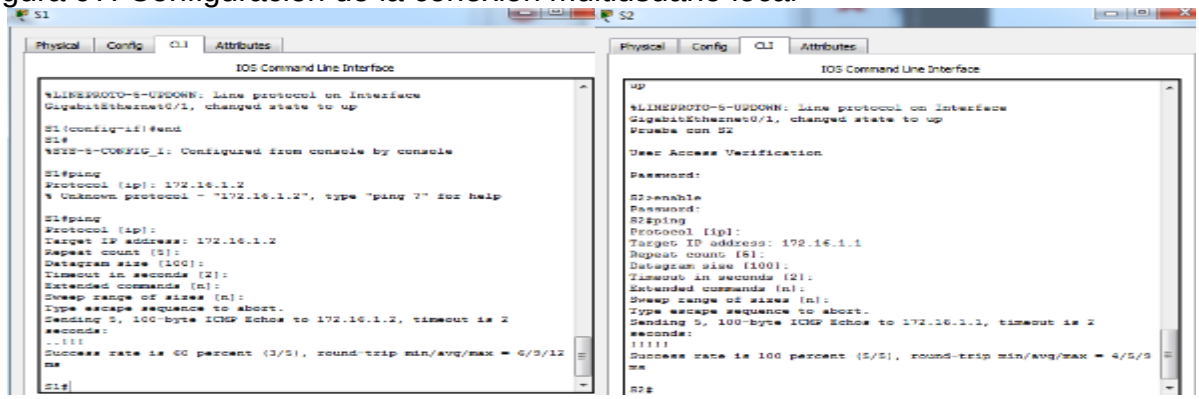


Fuente: elaboración Propia

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

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

Figura 97. Configuración de la conexión multiusuario local



Fuente: elaboración Propia

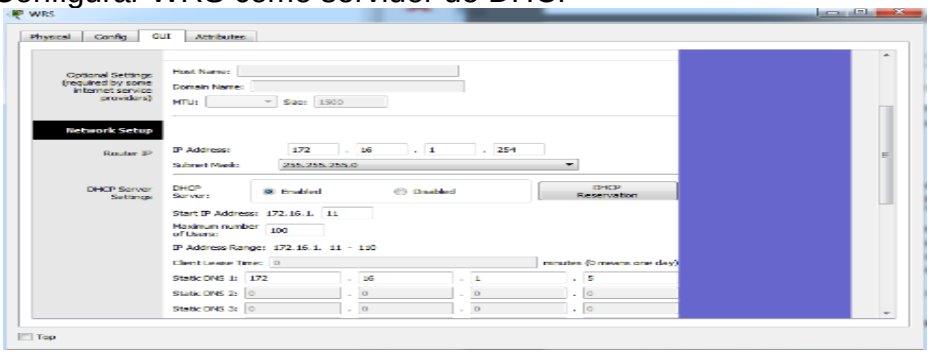
1.5.2. Parte 2: Jugador del lado servidor. Implementar y verificar todos los servicios.

Paso 1: Configurar WRS como servidor de DHCP

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

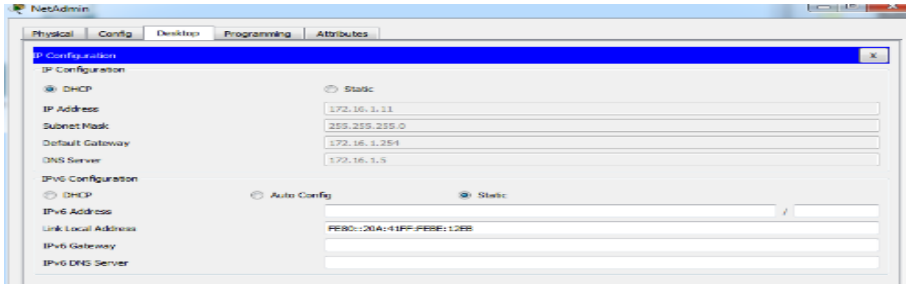
- La dirección IP de inicio es **172.16.1.11**.
- La cantidad máxima de usuarios es **100**.
- El **DNS 1 estático** es **172.16.1.5**.
- Verifique si **NetAdmin** recibió el direccionamiento IP mediante DHCP.
- En **NetAdmin**, acceda a la página Web User Account Information (Información de cuenta de usuario) en **172.16.1.5**. Utilizará esta información para configurar las cuentas de usuario en el paso 2.

Figura 98. Configurar WRS como servidor de DHCP



Fuente: elaboración Propia

Figura 99. Direccionamiento IP del servidor.



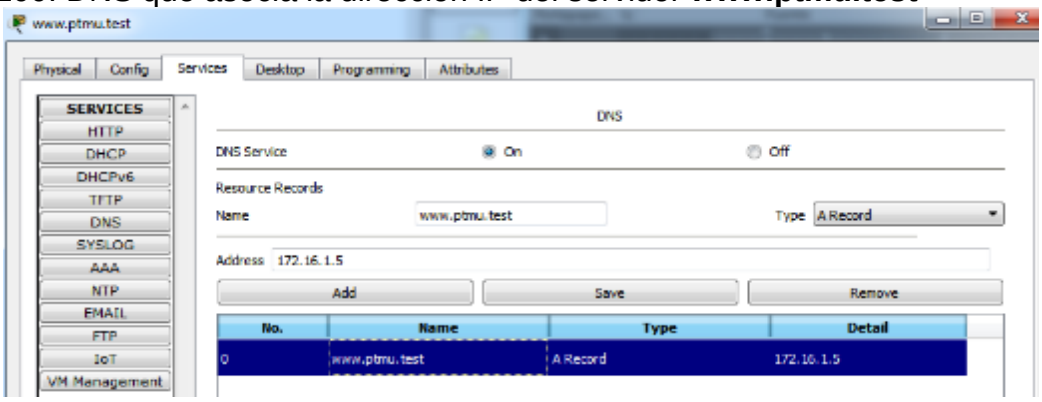
Fuente: elaboración Propia

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.

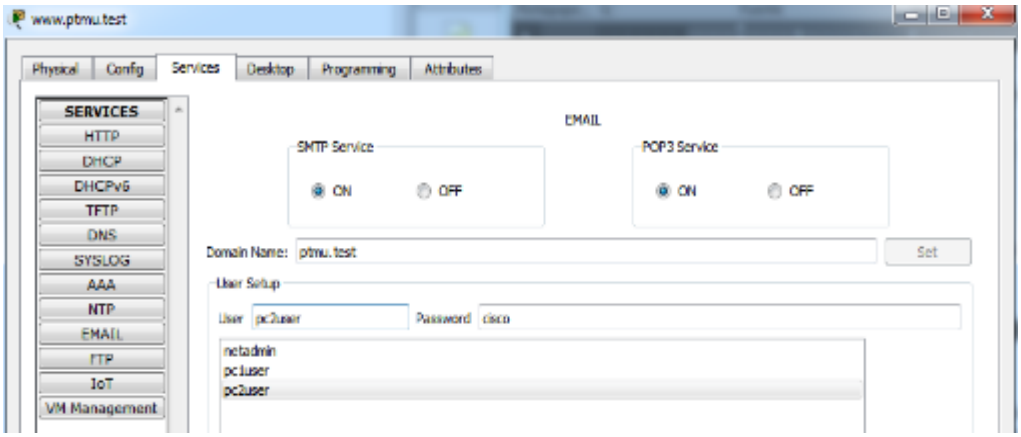
Figura 100. DNS que asocia la dirección IP del servidor **www.ptmu.test**



Fuente: elaboración Propia

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

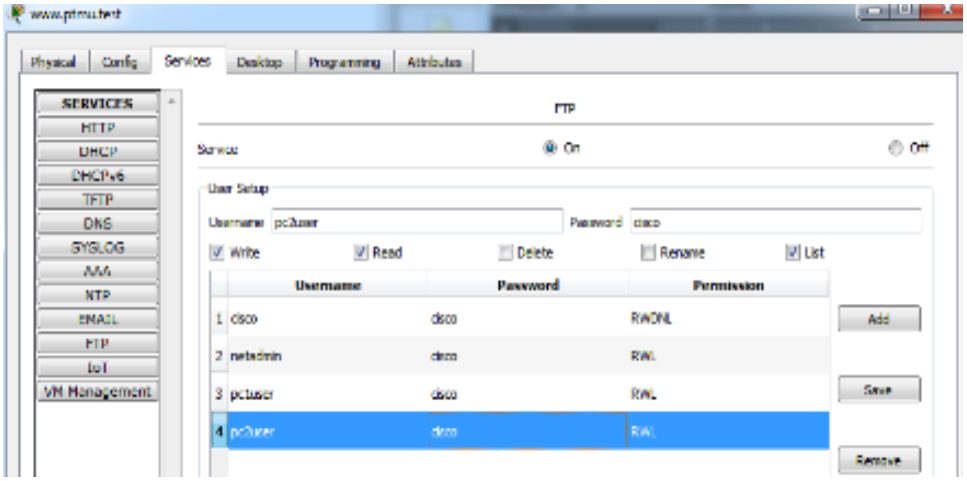
Figura 101. Configurar nombre de dominio con ptmu.test



Fuente: elaboración Propia

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

Figura 102. Permisos de lectura, escritura y enumeración.



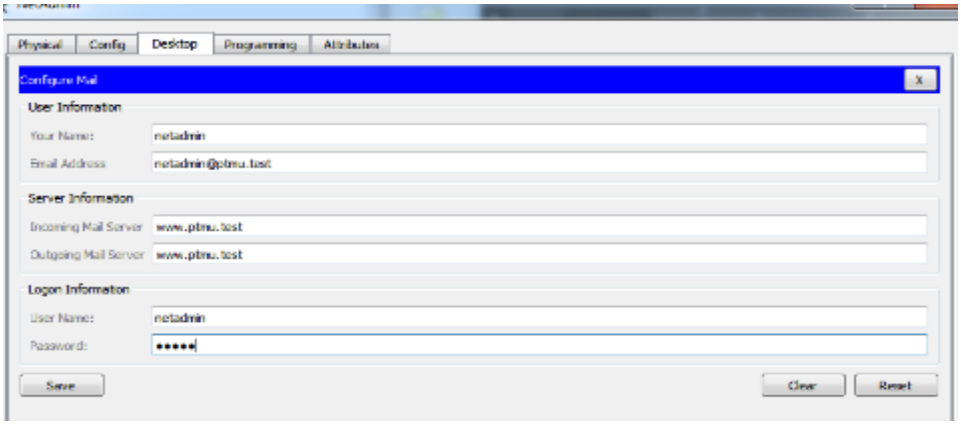
Fuente: elaboración Propia

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.

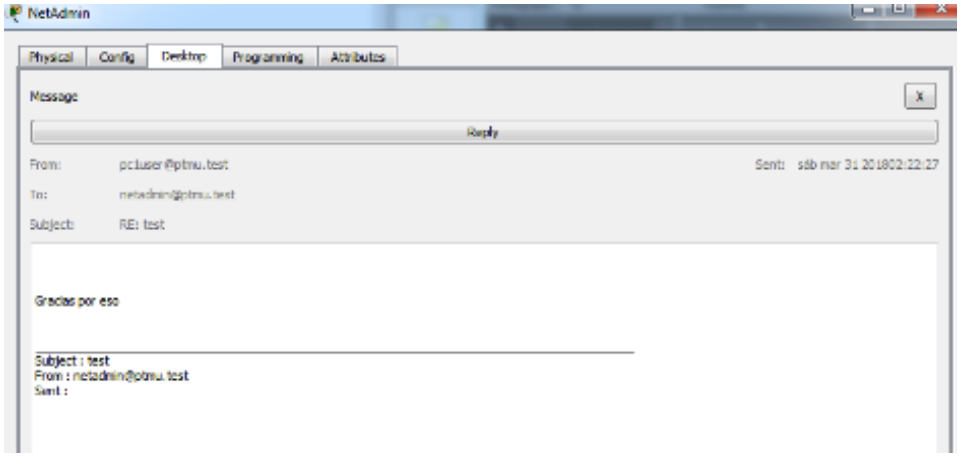
Figura 103. Cliente de correo electrónico en cuenta de usuario de NetAdmin.



Fuente: elaboración Propia

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

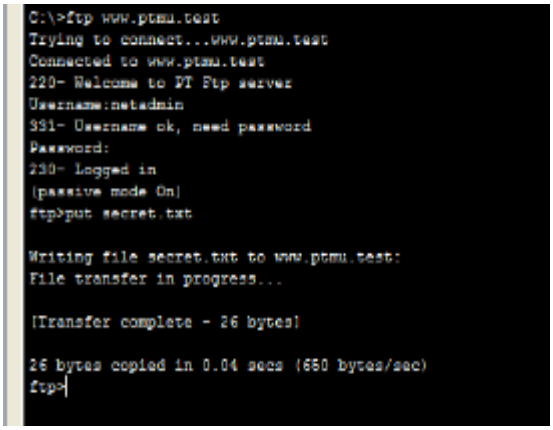
Figura 104. Correo electrónico al usuario de la **PC1**



Fuente: elaboración Propia

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

Figura 105. Archivo secret.txt al servidor FTP



Fuente: elaboración Propia

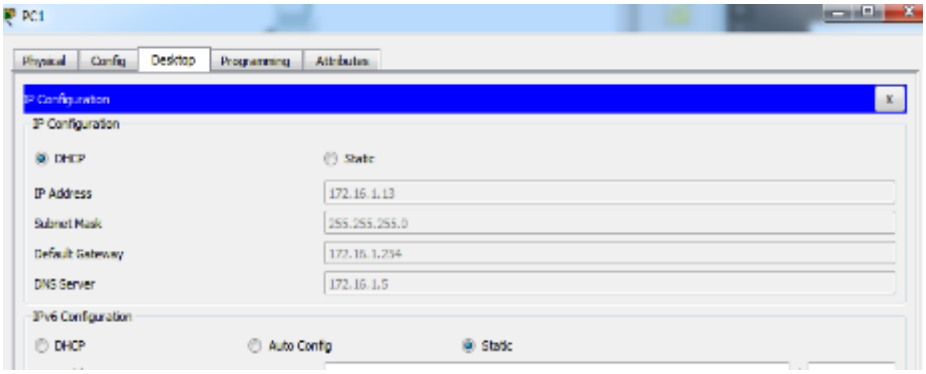
Nota: la puntuación para el jugador del lado servidor será de 43/44 hasta que el jugador del lado cliente descargue correctamente el archivo secret.txt, lo modifique y lo suba al servidor FTP www.ptmu.test.

1.5.3. 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.

Figura 106. Direccionamiento de la PC1



Fuente: elaboración Propia

Mismo procedimiento en PC2

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

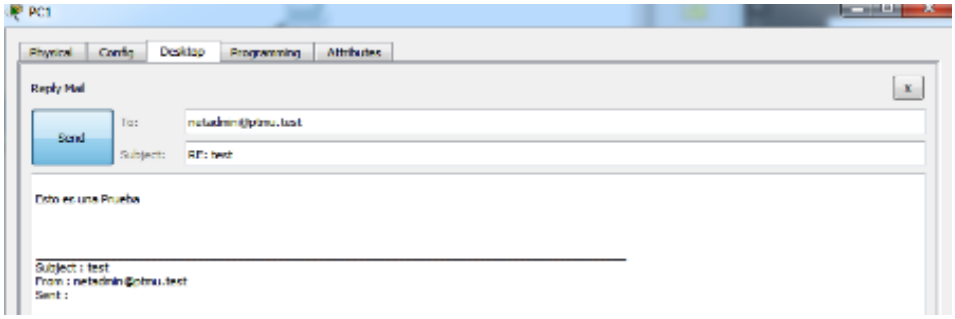
Figura 107. Página Web http://www.ptmu.test

Fuente: elaboración Propia

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.

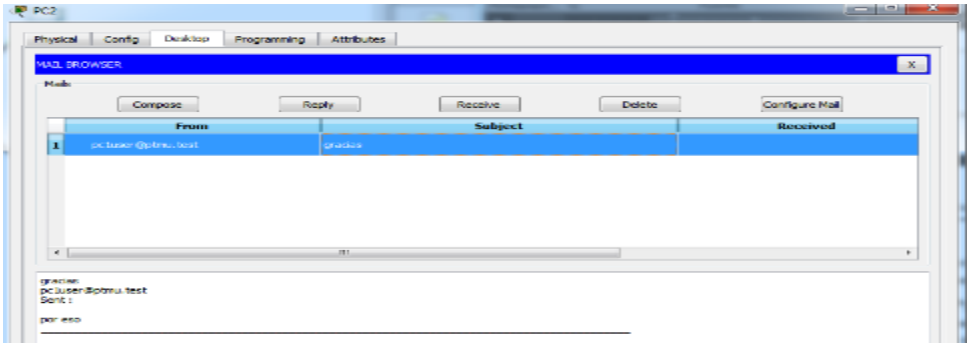
Figura 108. Verificacion de recepción de correo desde PC1.



Fuente: elaboración Propia

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.

Figura 109. Verificacion de envio de correo desde PC1 a PC2

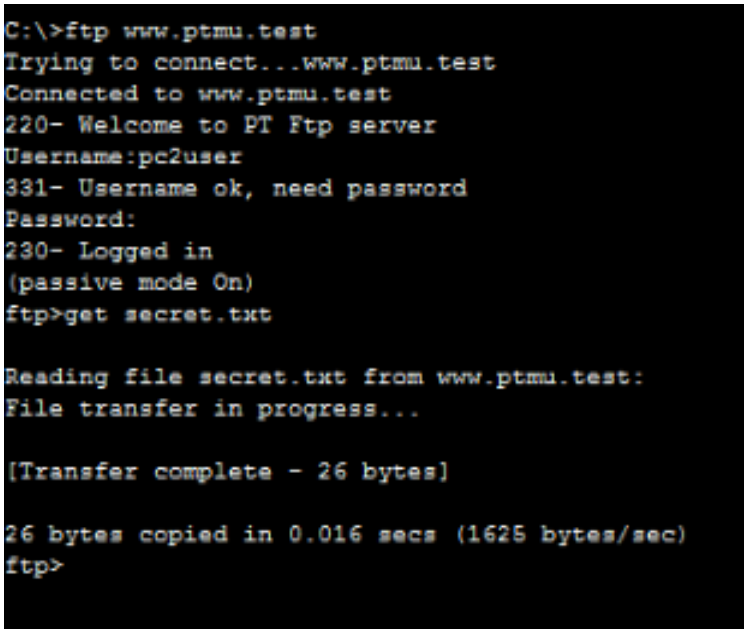


Fuente: elaboración Propia

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**.

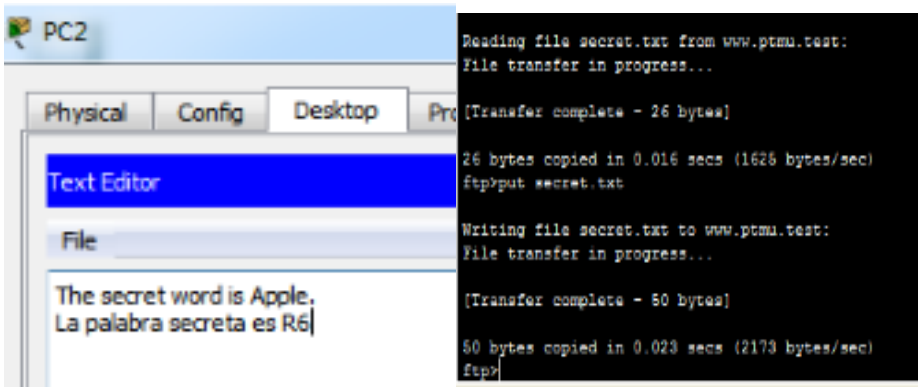
Figura 110. Acceso al servidor FTP desde PC2



Fuente: elaboración Propia

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

Figura 111. Cambio de palabra secreta



Fuente: elaboración Propia

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

CONCLUSIONES

Al desarrollar las actividades del módulo CCNA Routing & Switching: Principios básicos de routing y switching, se comprende y se describen conceptos básicos de switching y del funcionamiento de los switches de Cisco.

Al desarrollar las actividades del módulo CCNA Routing & Switching: Principios básicos de routing y switching, se comprende y se describen protocolos de routing dinámico, los protocolos de routing de vector de distancia y los protocolos de routing de estado de enlace.

Cursar el diplomado de profundización cisco permitió comprender y practicar las tecnologías de switching mejoradas, al igual que las operaciones y beneficios del protocolo dinámico de host (DHCP) y del sistema de nombres de dominio (DNS) para IPV4 e IPV6.

Todo lo aprendido en el diplomado de profundización cisco servirá en los diferentes cargos relacionados con la ingeniería de sistemas, para reconocer y corregir fallas y problemas de enrutamiento comunes. Las actividades del Packet Tracer refuerzan nuevos conceptos y permiten a los ingenieros modelar y analizar procesos de enrutamiento que puedan ser difíciles de visualizar o entender.

Con la realización de este trabajo se logró conocer y comprender como se debe de hacer la configuración básica entre redes LAN y WAN, usando la herramienta Packet Tracer con la que es posible diseñar redes y realizar simulaciones sobre su uso.

BIBLIOGRAFIA

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

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-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.comITN50ES/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

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1