CURSO DE PROFUNDIZACION CISCO

Actividad Colaborativa

MOMENTO 3

Presentación:

Francisco Antonio Prado

Jorge Orejuela

Sigfredo Monsalve

Jefferson Pasto

Efrén Ricardo Paz Jiménez

Grupo: 203092A_24

TUTOR

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

INGENIERIA EN ELECTRONICA

CEAD PALMIRA

OCTUBRE 2015

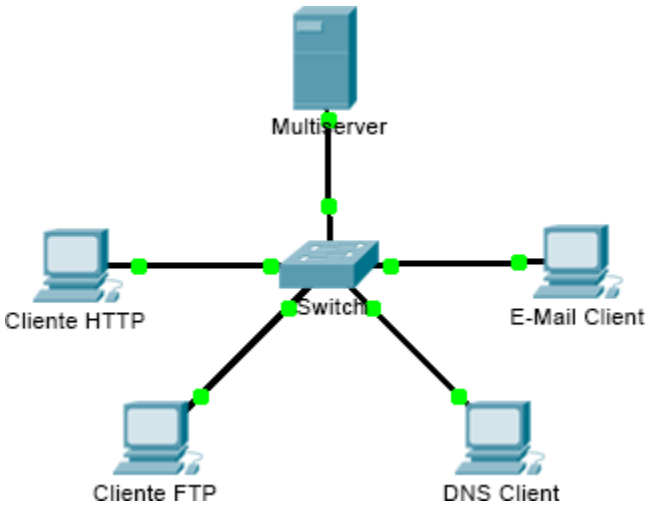
INTRODUCCIÓN

Como futuros ingenieros en los diferentes campos de la ingeniería (electrónica, telecomunicación, sistemas. etc.), y con la realización de los laboratorios propuestos en el curso diplomado de profundización Cisco CCNA1 R&S UNIDAD 2, se busca ampliar los conocimientos y afianzar los conceptos impartidos desde el estudio del Modelo OSI Direccionamiento IP que esta orientado al uso de protocolos de enrutamiento avanzado utilizando el programa de simulación Packt Tracer. Veremos el funcionamiento del Protocolo de Internet IP, mostrando como opera este dentro del Modelo OSI, los tipos de IP versión 4, Igualmente los tipos de IP versión 6, En este sentido esta actividad permitirá entender como se hizo posible la comunicación entre equipos.

El modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios. Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes

7.3.1.2 Simulación de Packet Tracer: Comunicaciones TCP y UDP

Topología



Objetivos

Parte 1: Generar tráfico de red en modo de simulación

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

Información básica

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

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

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

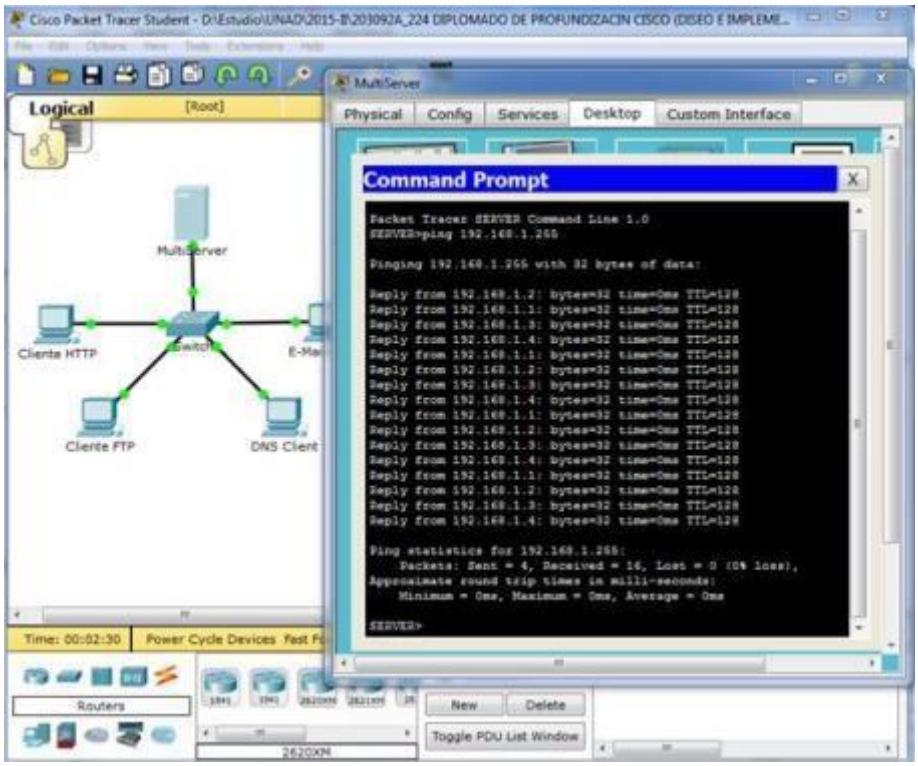
Parte 1: Generar tráfico de red en modo de simulación

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

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

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

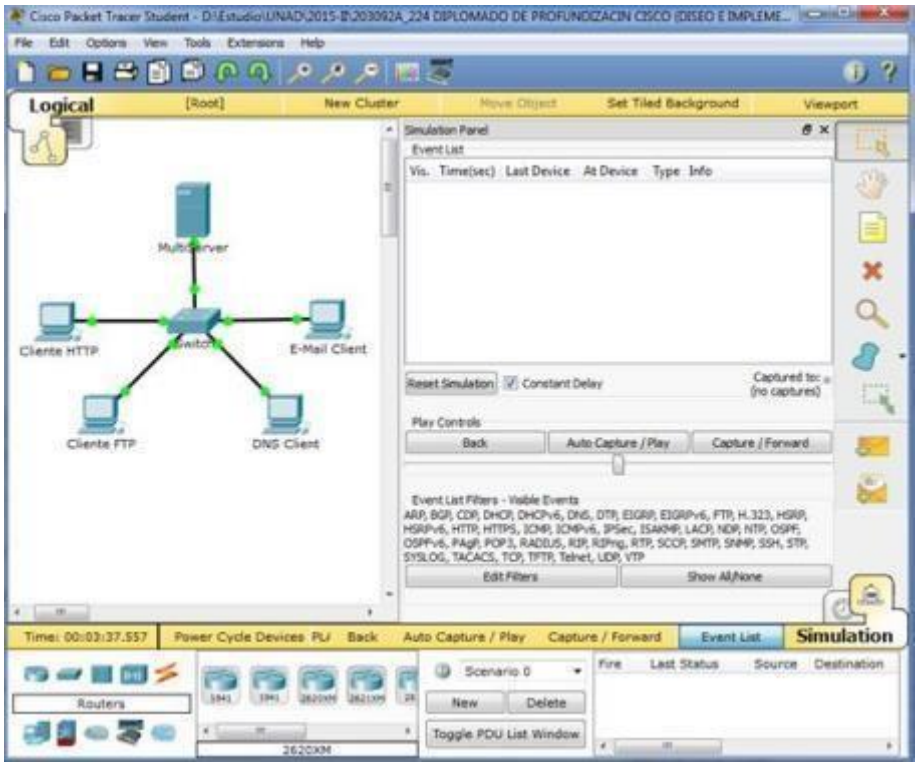
b. Introduzca el comando ping 192.168.1.255. Esto toma unos segundos, ya que todos los dispositivos en la red responden a MultiServer.



c. Cierre la ventana de MultiServer.

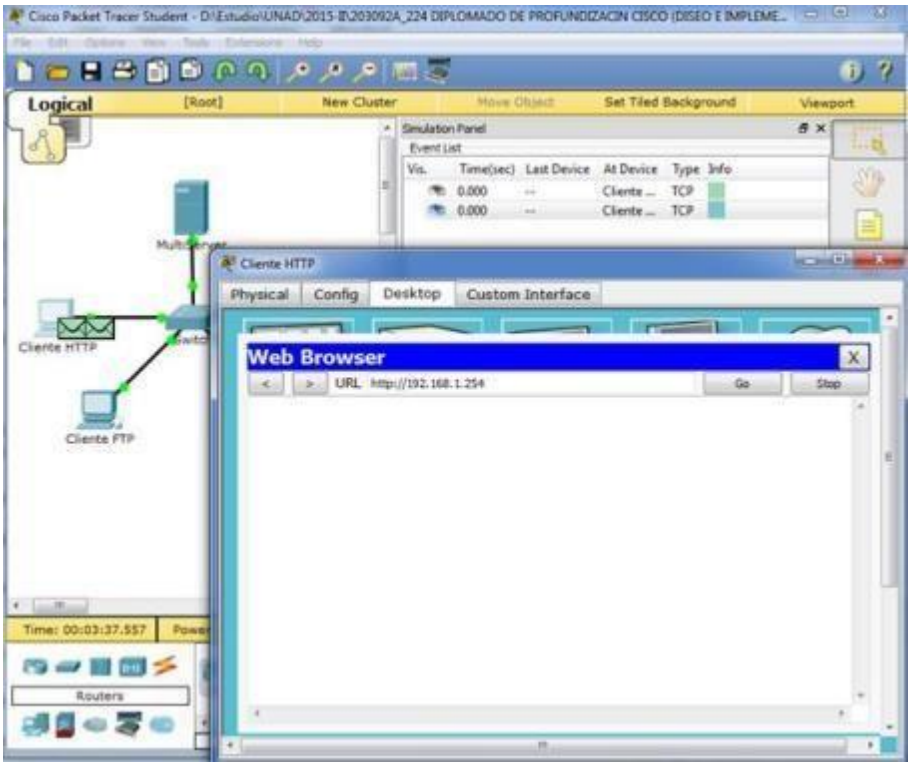
Paso 2: Genere tráfico web (HTTP).

a. Cambie a modo de simulación.



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

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

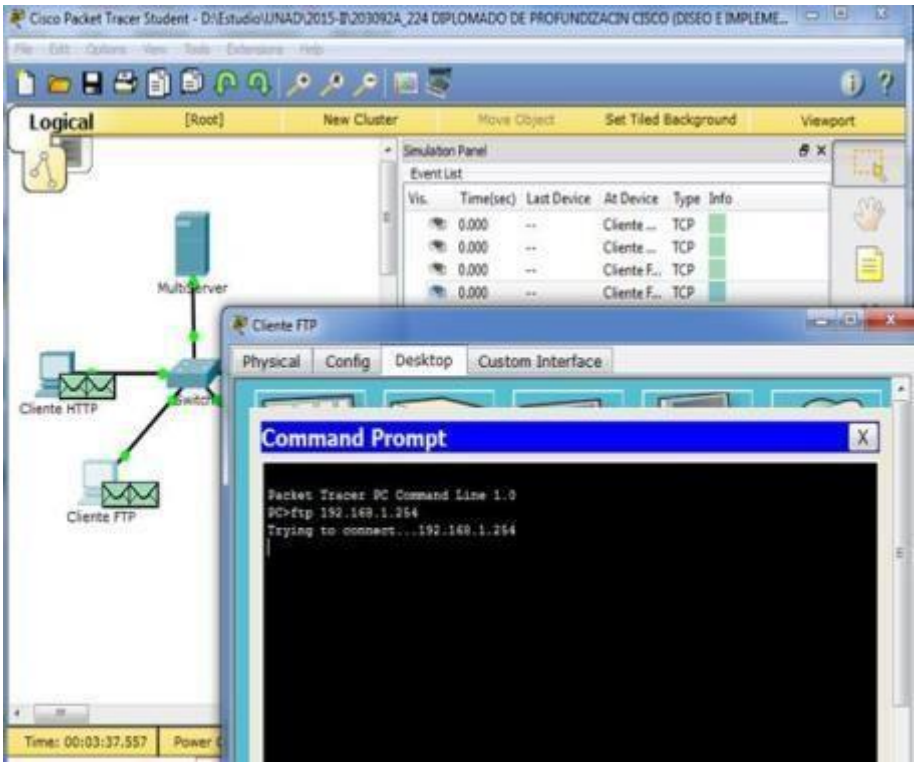


d. Minimice (pero no cierre) la ventana de configuración de HTTP Client.

Paso 3: Generar tráfico FTP.

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

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

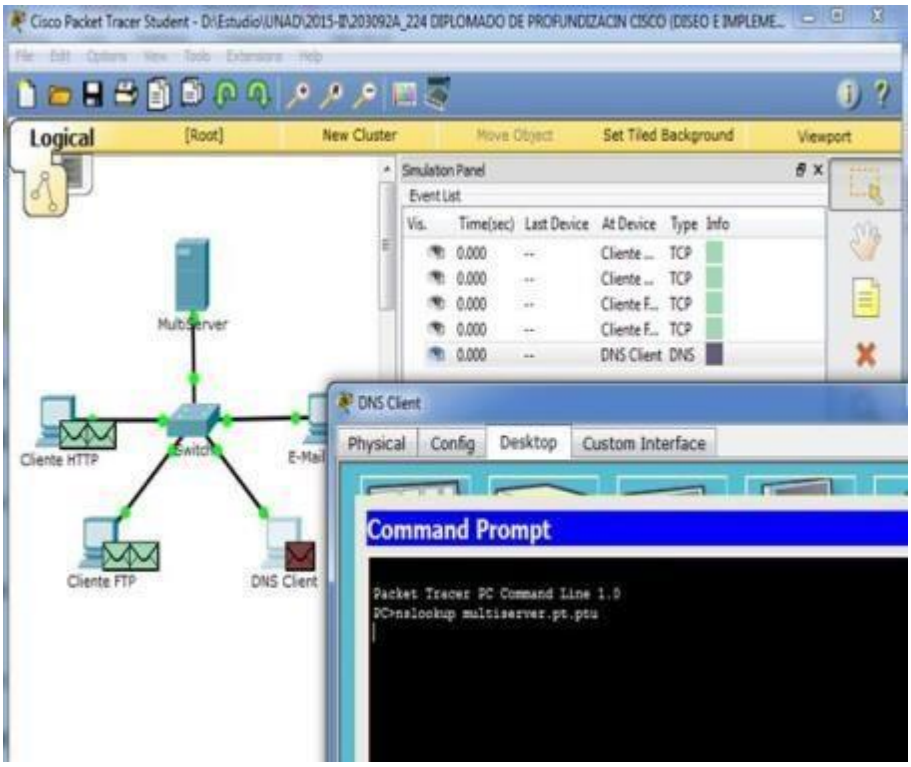


c. Minimice (pero no cierre) la ventana de configuración de FTP Client.

Paso 4: Generar tráfico DNS.

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

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



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

Paso 5: Generar tráfico de correo electrónico.

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

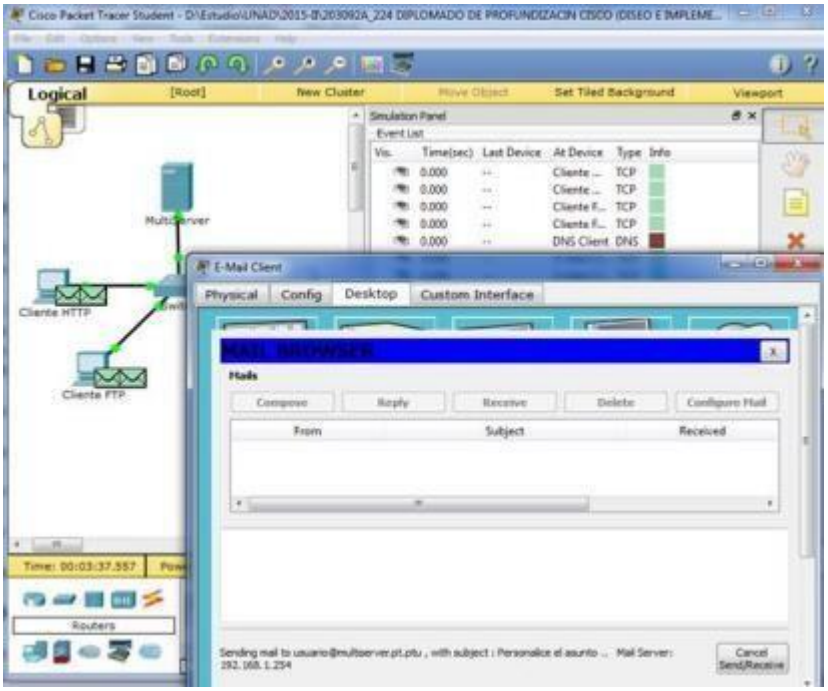
b. Haga clic en Compose (Redactar) e introduzca la siguiente información:

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

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

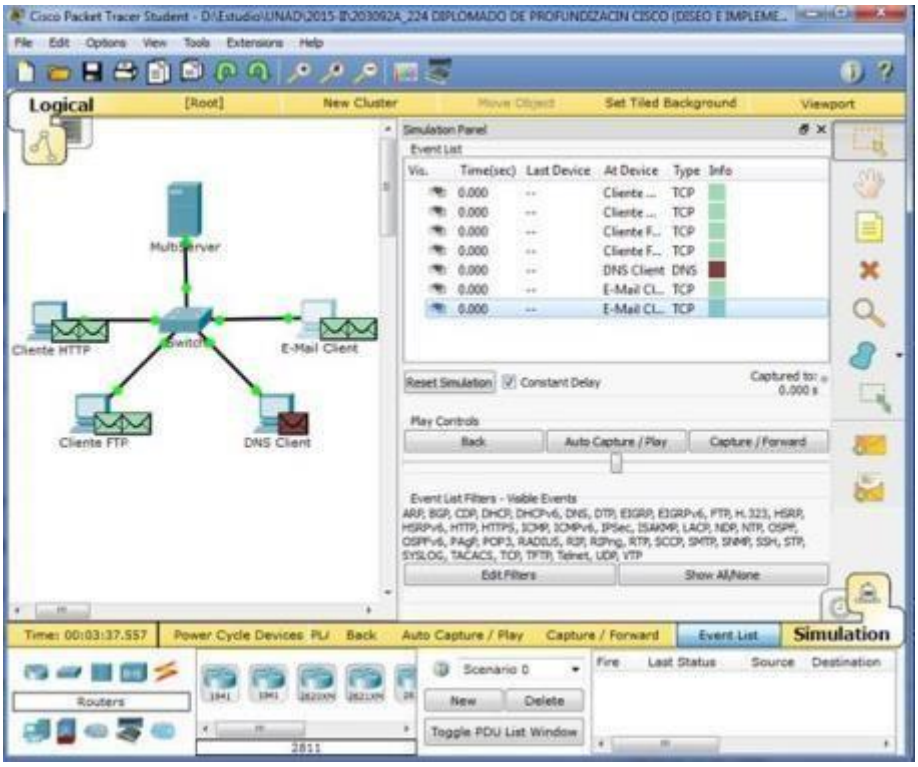
3) E-Mail Body: (Cuerpo del correo electrónico:) personalice el correo electrónico.

c. Haga clic en Send (Enviar).



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

Paso 6: Verifique que se haya generado tráfico y que esté preparado para la simulación.
Cada equipo cliente debe tener PDU enumeradas en el panel de simulación.

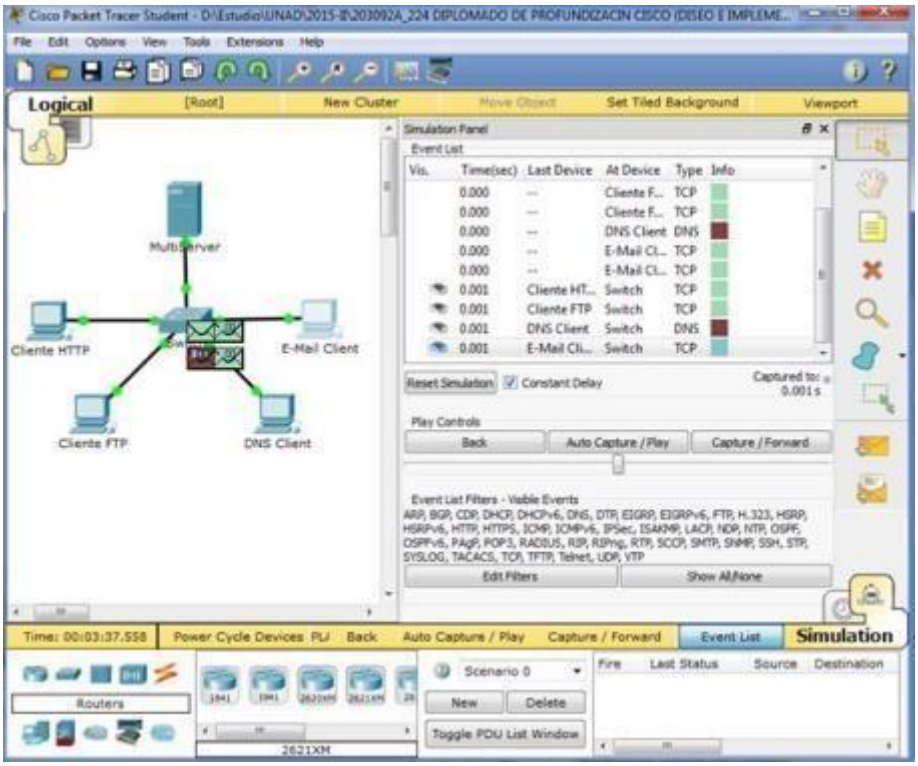


Parte 2: Examinar la funcionalidad de los protocolos TCP y UDP

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

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

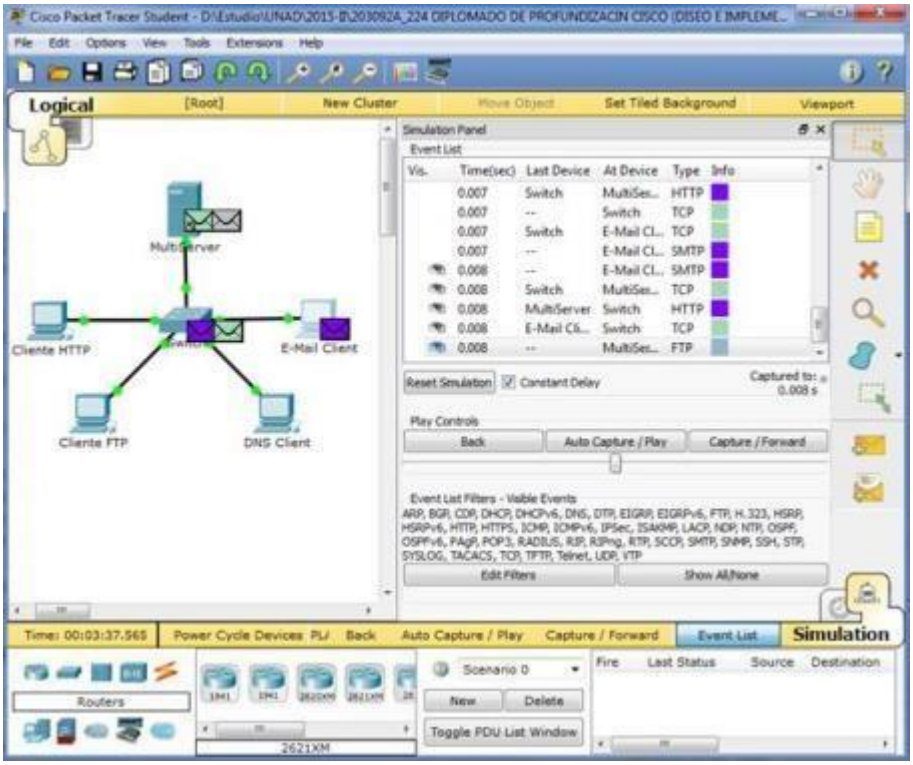
a. Haga clic en Capture/Forward (Capturar/avanzar) una vez. Todas las PDU se transfieren al switch.



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

c. Haga clic en Capture/Forward seis veces. Todos los clientes deberían haber recibido una respuesta.

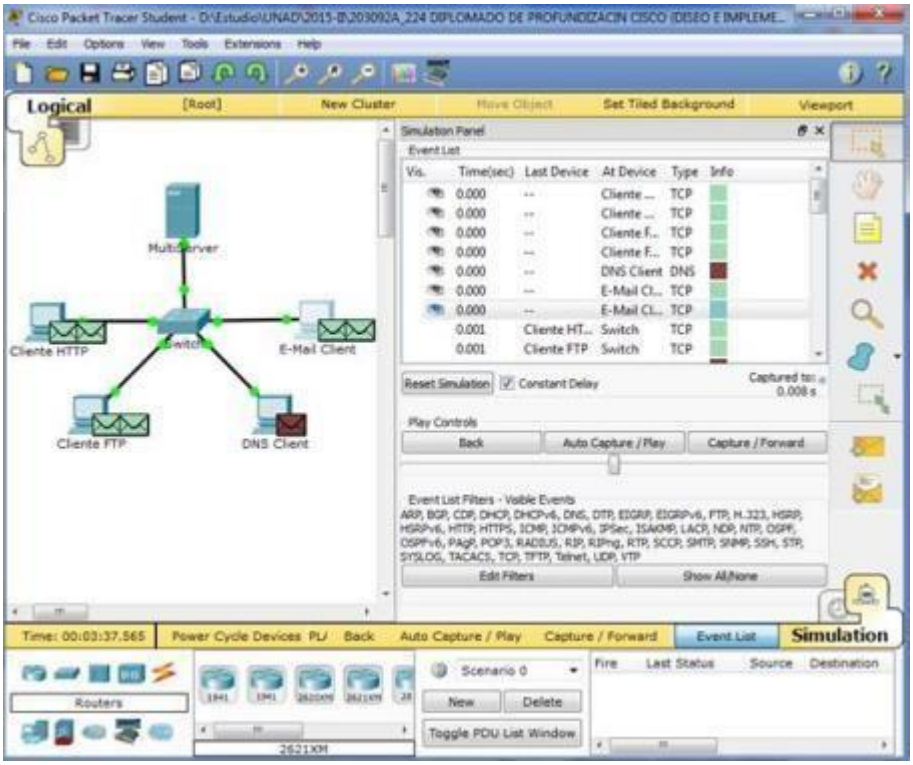
Observe que solo una PDU puede cruzar un cable en cada dirección en cualquier momento dado.



¿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**.

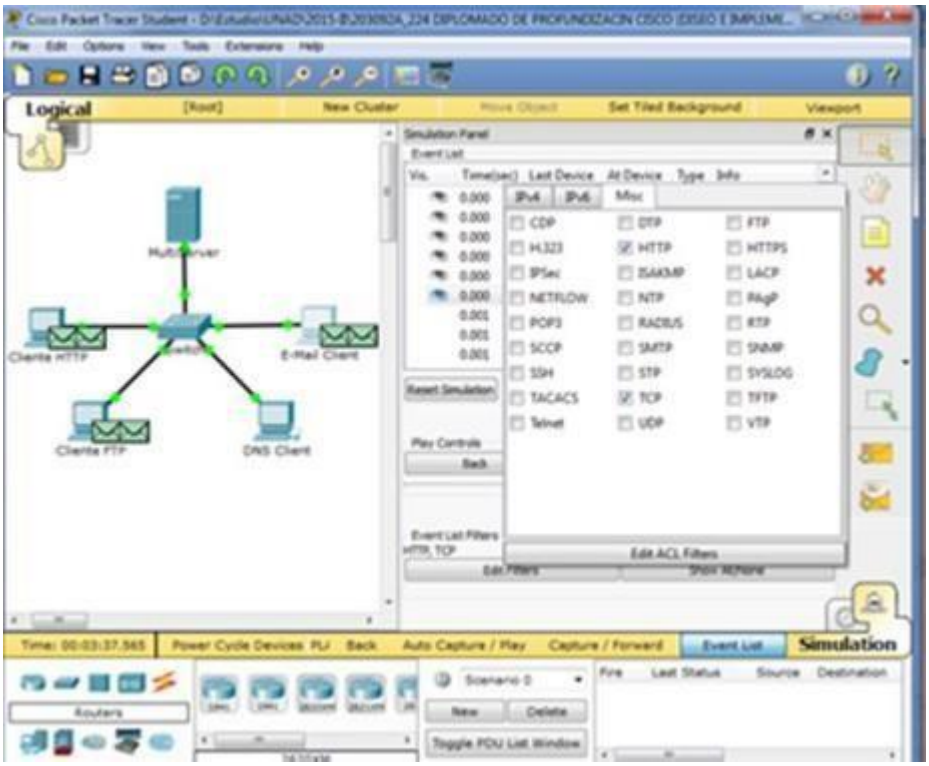
e. Haga clic en Back ocho veces. Esto restablecerá la simulación.



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

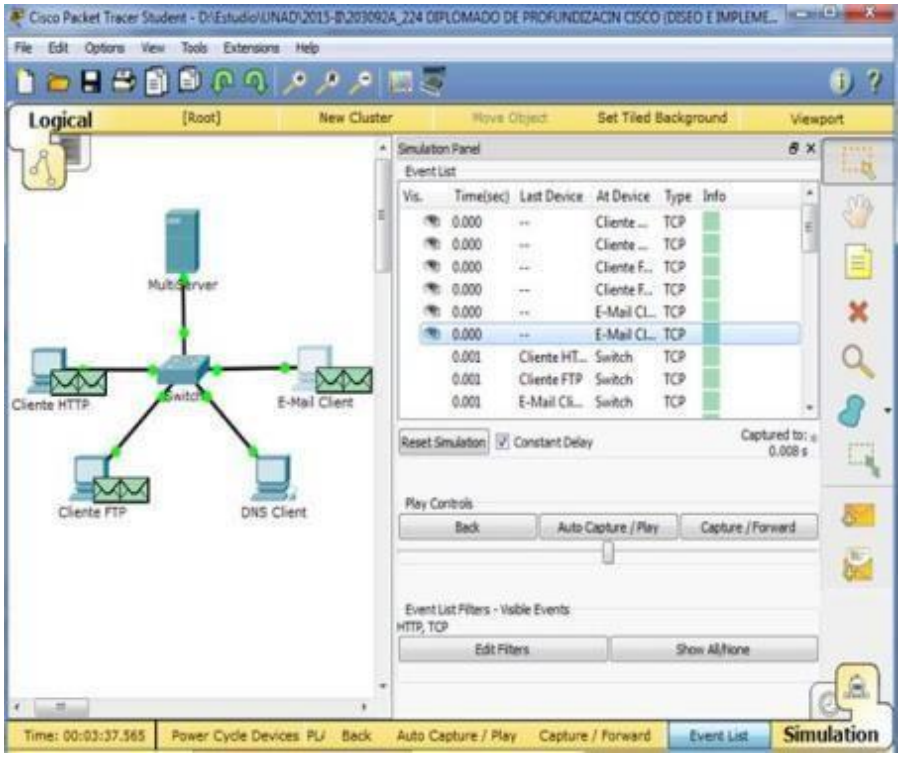
Paso 2: Examinar el tráfico HTTP cuando los clientes se comunican con el servidor.

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

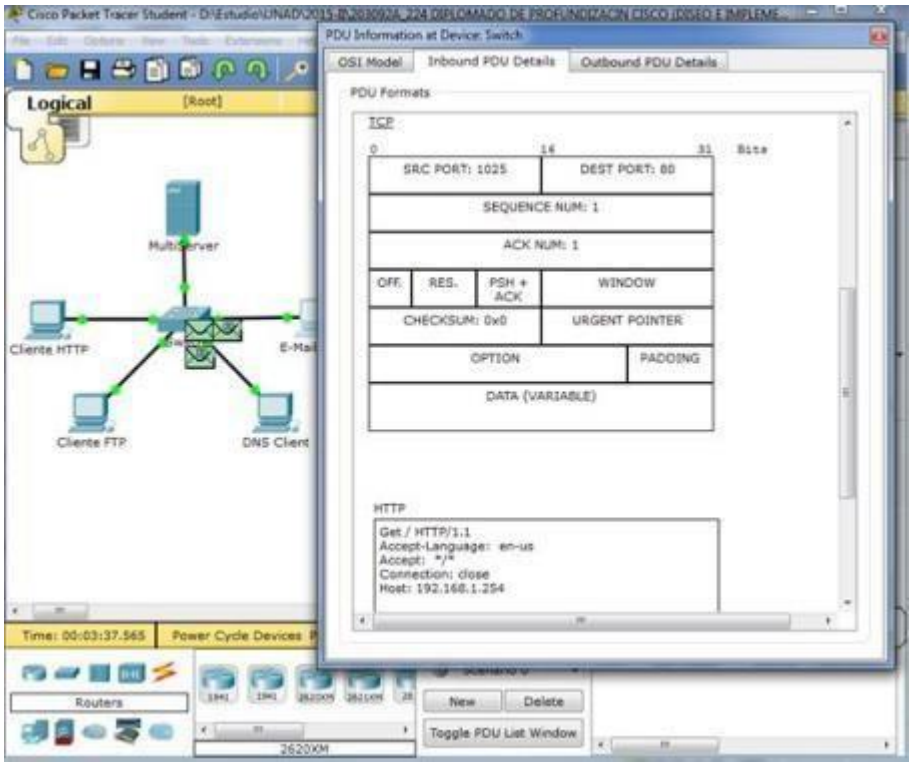


1) Haga clic en Edit Filters (Editar filtros) y cambie el estado de la casilla de verificación Show All/None (Mostrar todos/ninguno).

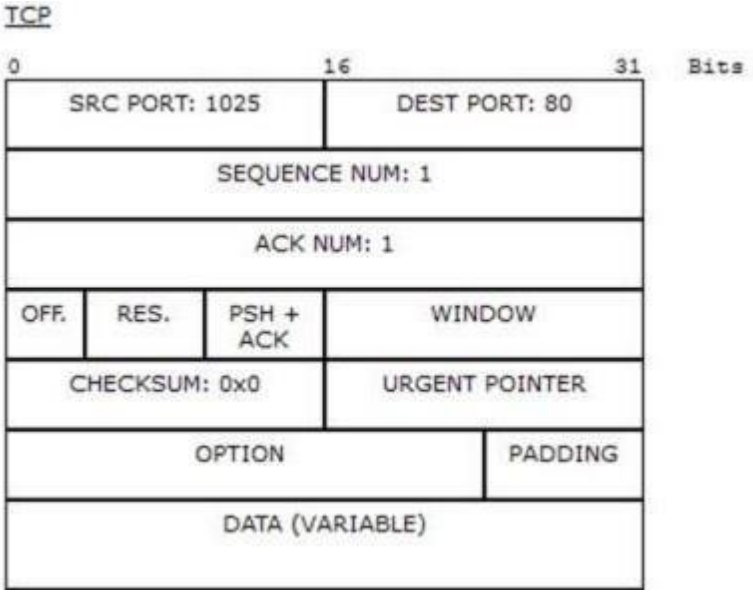
2) Seleccione HTTP y TCP. Haga clic en cualquier lugar fuera del cuadro Edit Filters (Editar filtros) para ocultarlo. En Visible Events (Eventos visibles), ahora solo se deberían mostrar las PDU de HTTP y TCP.



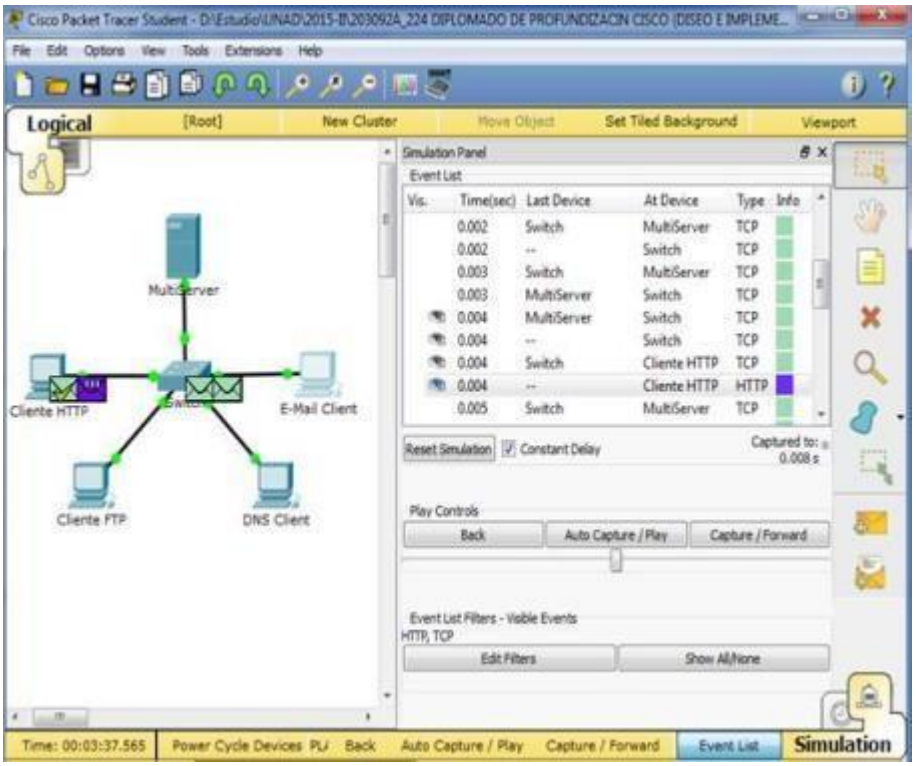
b. Haga clic en Capture/Forward (Capturar/avanzar). Pase el mouse sobre cada PDU hasta que encuentre una que se origine en HTTP Client. Haga clic en el sobre de PDU para abrirlo.
c. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante) y desplácese hasta la última sección.
¿Cómo se rotula 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 (puede ser diferente), 80, 0, 0 SYN

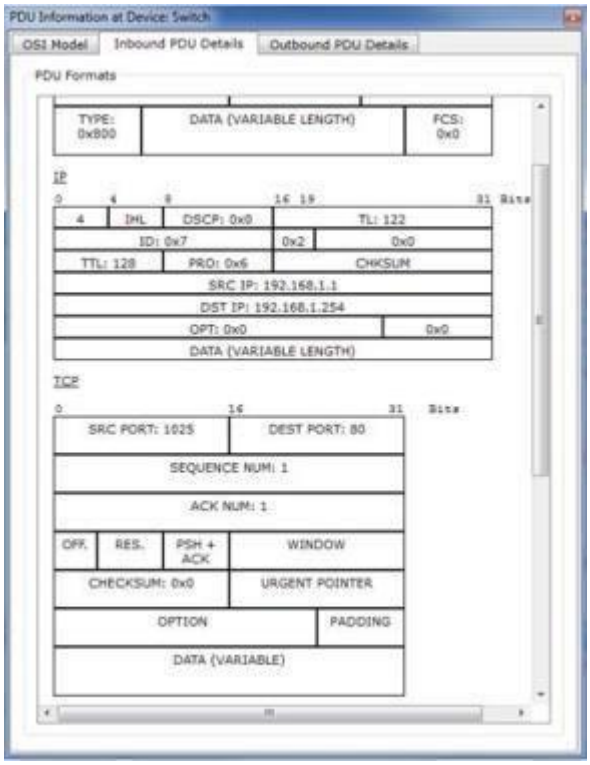


e. Cierre la PDU y haga clic en Capture/Forward hasta que una PDU vuelva a HTTP Client con una marca de verificación.

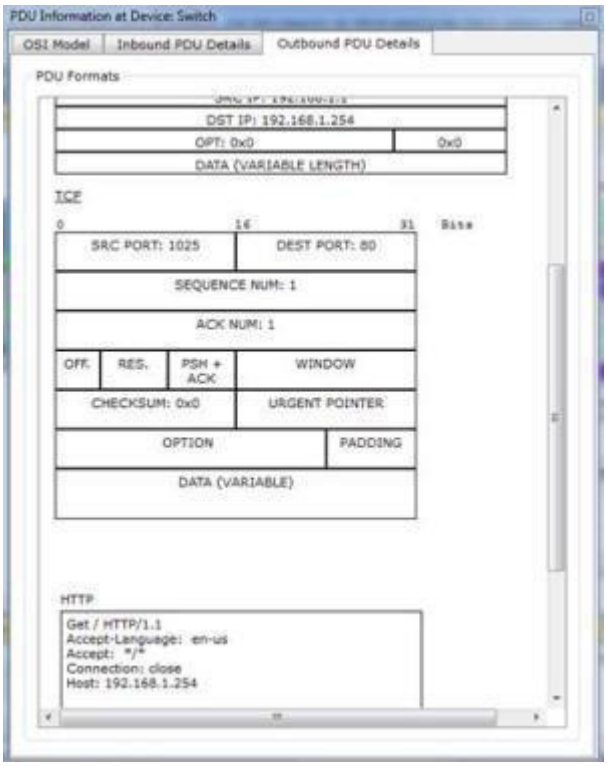


f. Haga clic en el sobre de PDU y seleccione Inbound PDU Details. ¿En qué cambiaron los números de puerto y de secuencia?

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



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



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

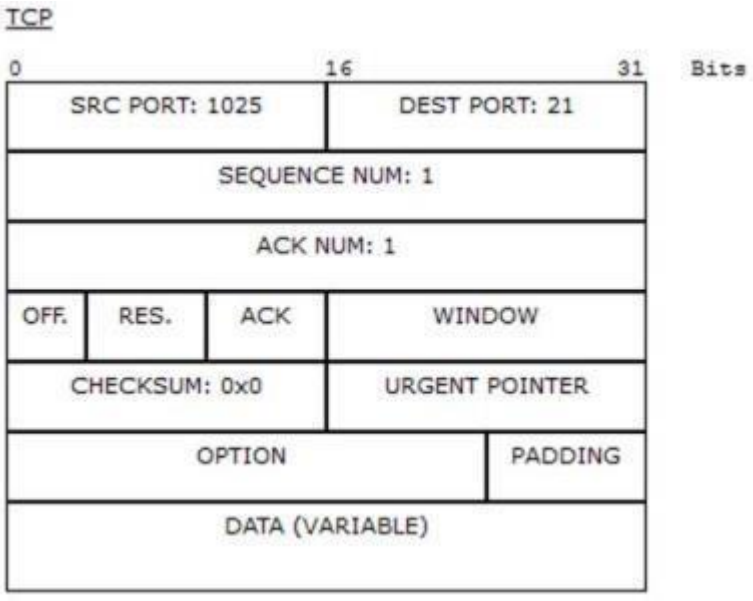
1025, 80, 1, 1. PSH+ACK: los puertos de origen y destino están invertidos, y tanto el número de secuencia como el de acuse de recibo son 1.

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

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

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

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



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

¿Cómo se rotula la sección? **TCP**

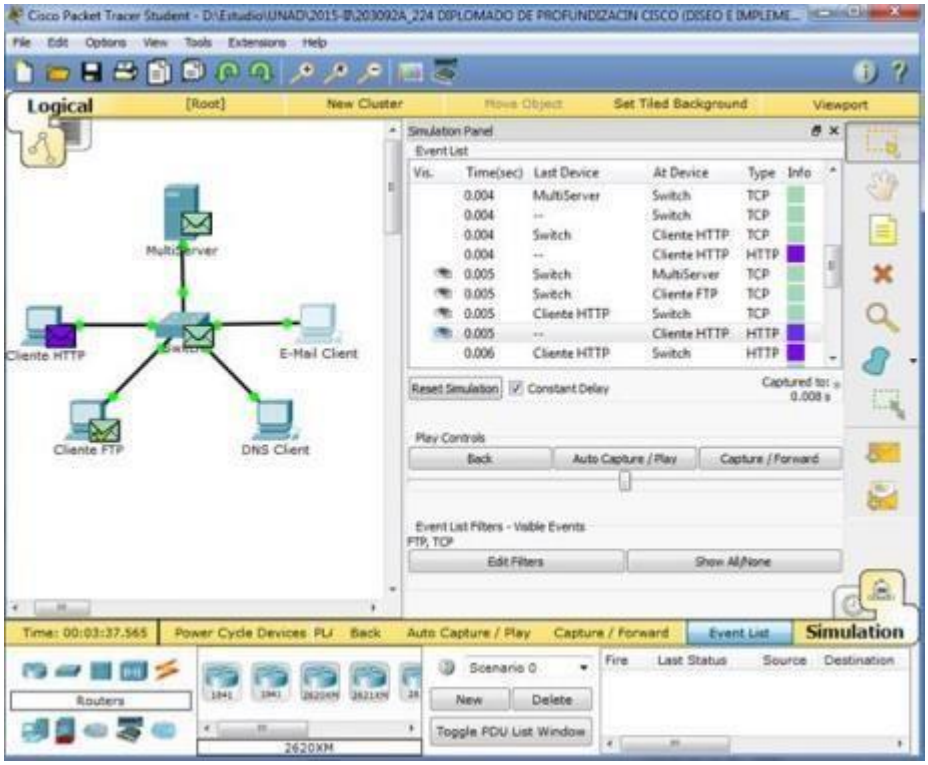
¿Estas comunicaciones se consideran confiables? **Sí**.

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

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

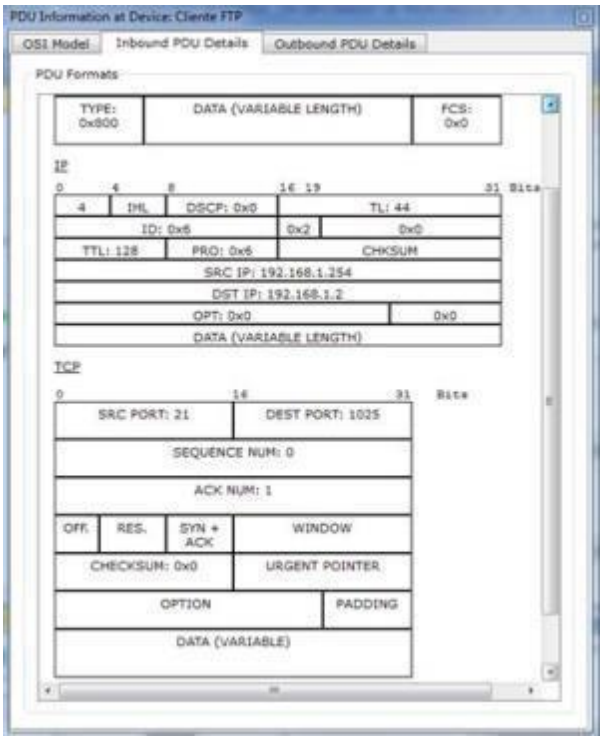
1025, 21, 0, 0. SYN

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

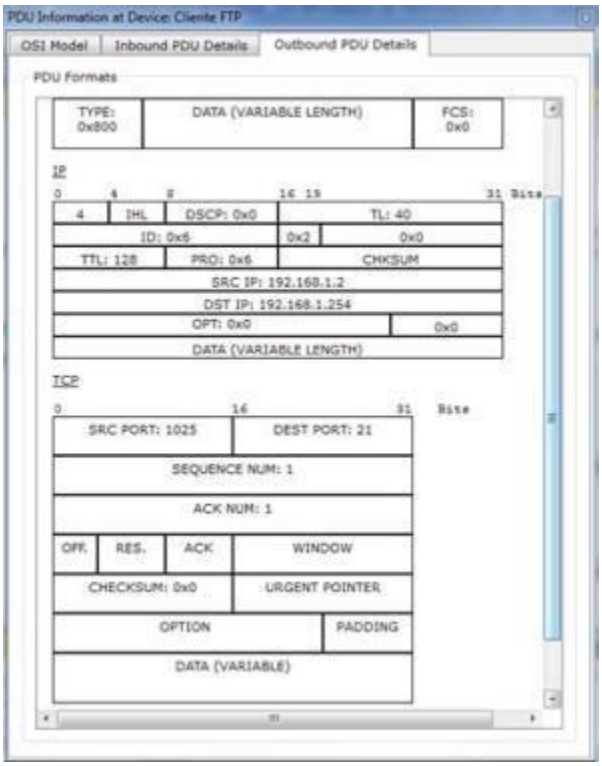


f. Haga clic en el sobre de PDU y seleccione Inbound PDU Details. ¿En qué cambiaron los números de puerto y de secuencia?

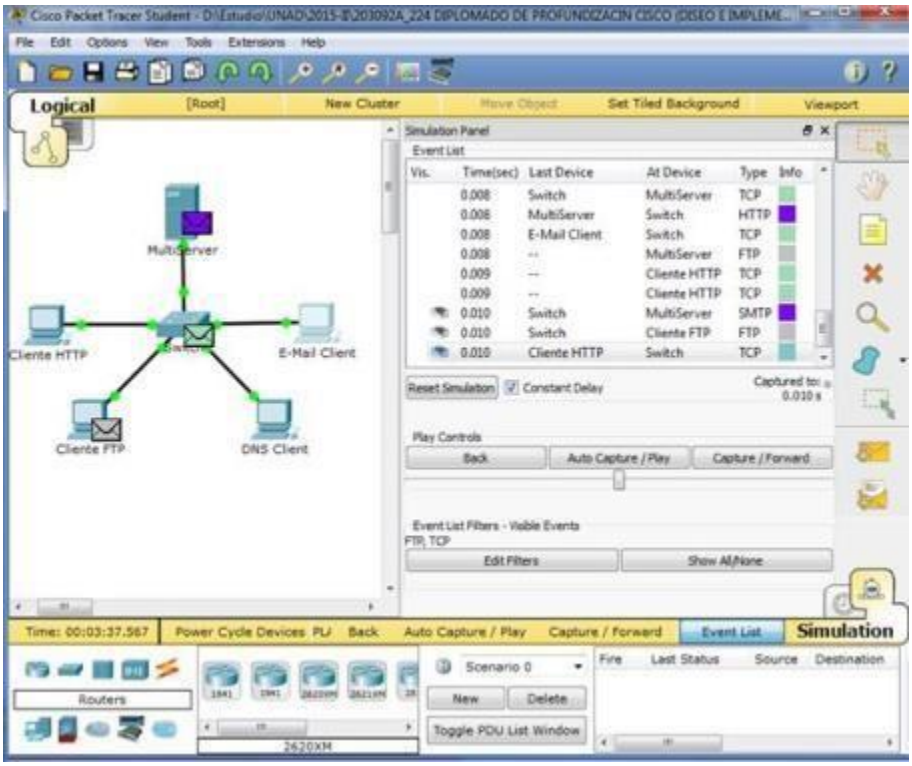
21, 1025, 0, 1. SYN+ACK. Se invierten los puertos de origen y de destino, y el número de acuse de recibo es 1.



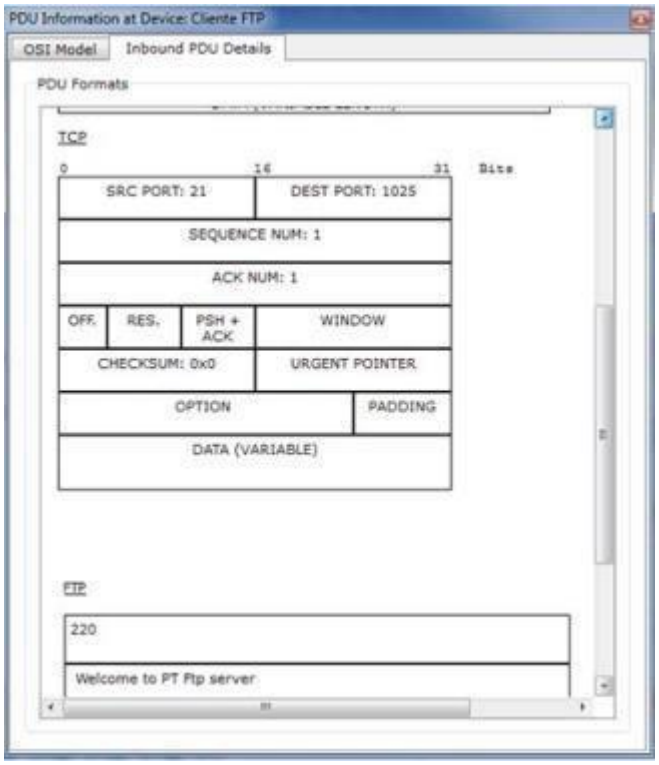
g. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?
1025, 21, 1, 1. ACK. Se invierten los puertos de origen y de destino, y los números de secuencia y de acuse de recibo son 1.



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



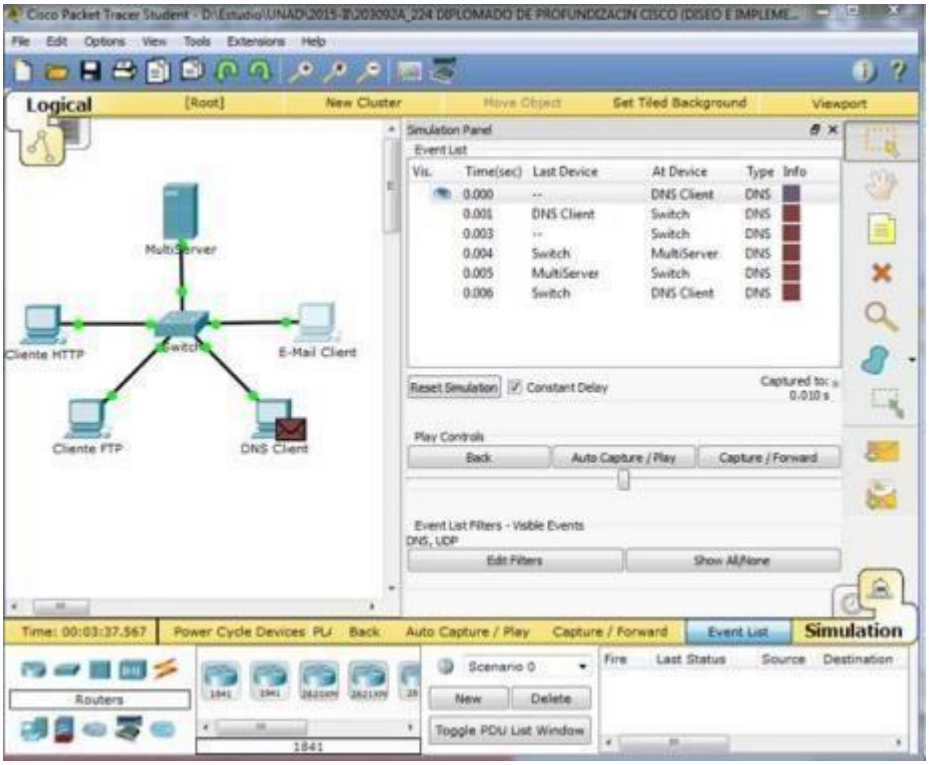
i. Abra la PDU y seleccione Inbound PDU Details. Desplácese hasta después de la sección TCP. ¿Cuál es el mensaje del servidor?
Puede decir “Username ok, need password” (Nombre de usuario correcto, se necesita contraseña) o “Welcome to PT Ftp server” (Bienvenido al servidor FTP de PT).



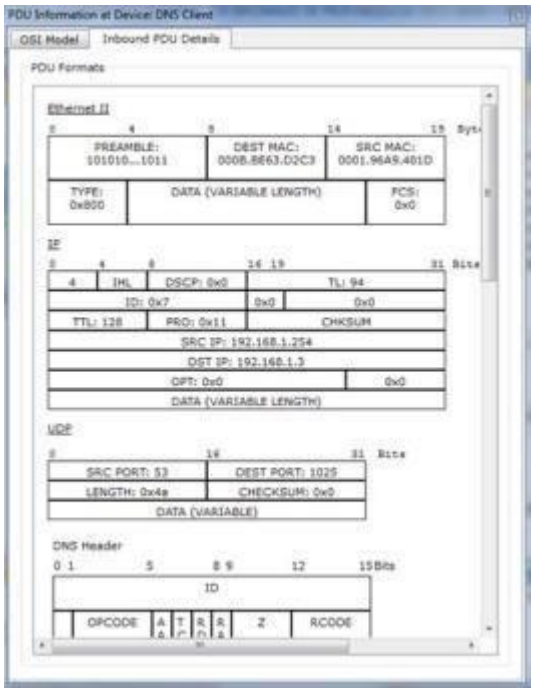
j. Haga clic en Back hasta que se restablezca la simulación.

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

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



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



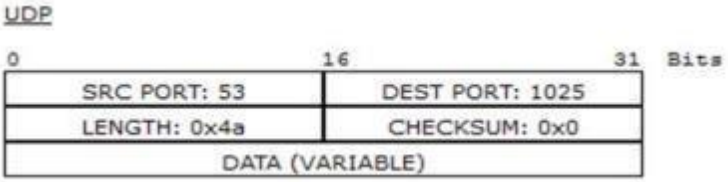
c. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante) y desplácese hasta la última sección.

¿Cómo se rotula la sección? **UDP**

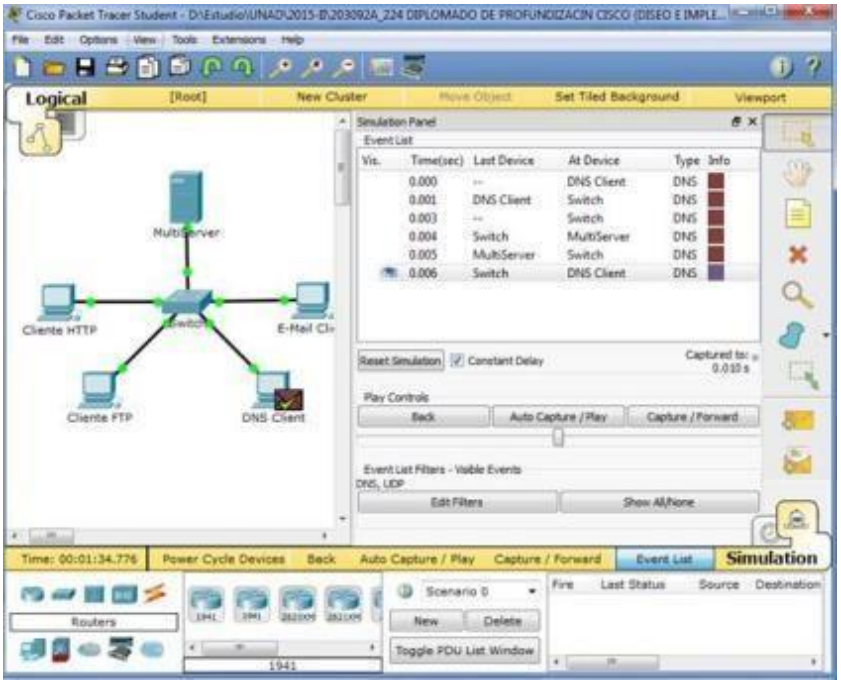
¿Estas comunicaciones se consideran confiables? **No**

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

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

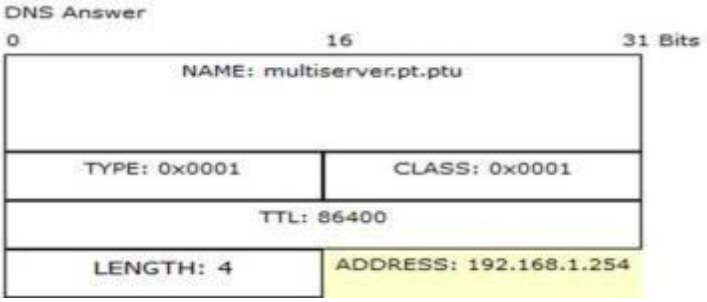


e. Cierre la PDU y haga clic en Capture/Forward hasta que una PDU vuelva al cliente DNS con una marca de verificación.



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

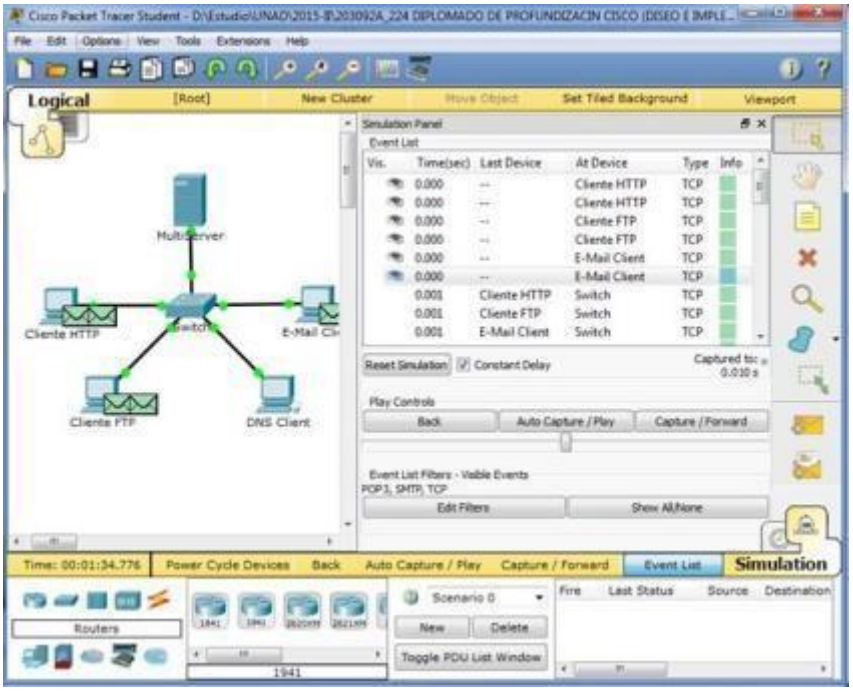
g. ¿Cómo se llama la última sección de la PDU? **DNS ANSWER (Respuesta DNS)**



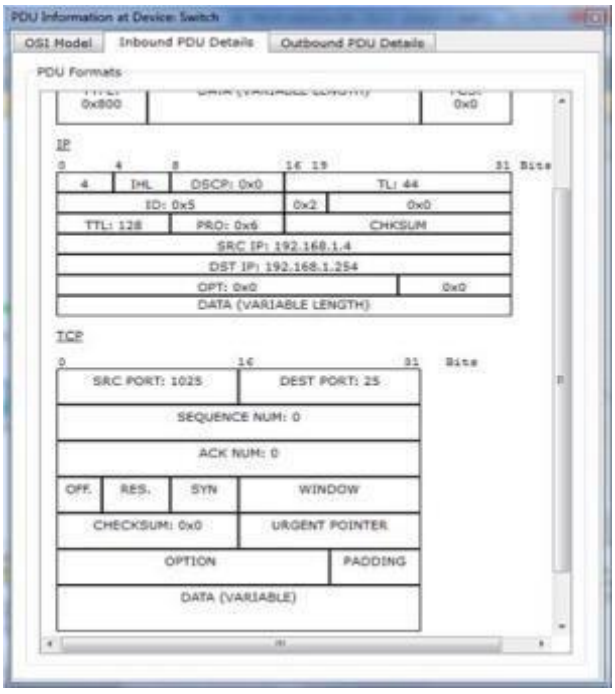
h. Haga clic en Back hasta que se restablezca la simulación.

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.

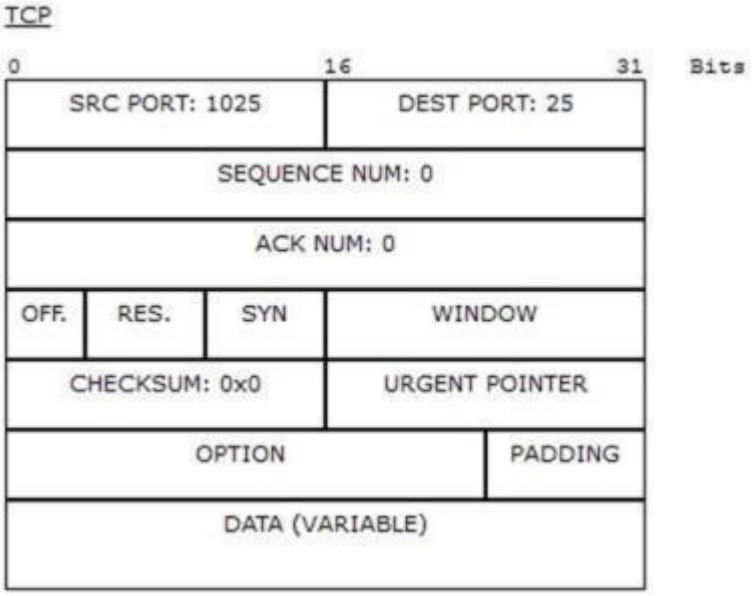


c. Haga clic en la ficha Inbound PDU Details (Detalles de PDU entrante) y desplácese hasta la última sección. ¿Qué protocolo de la capa de transporte utiliza el tráfico de correo electrónico? **TCP**

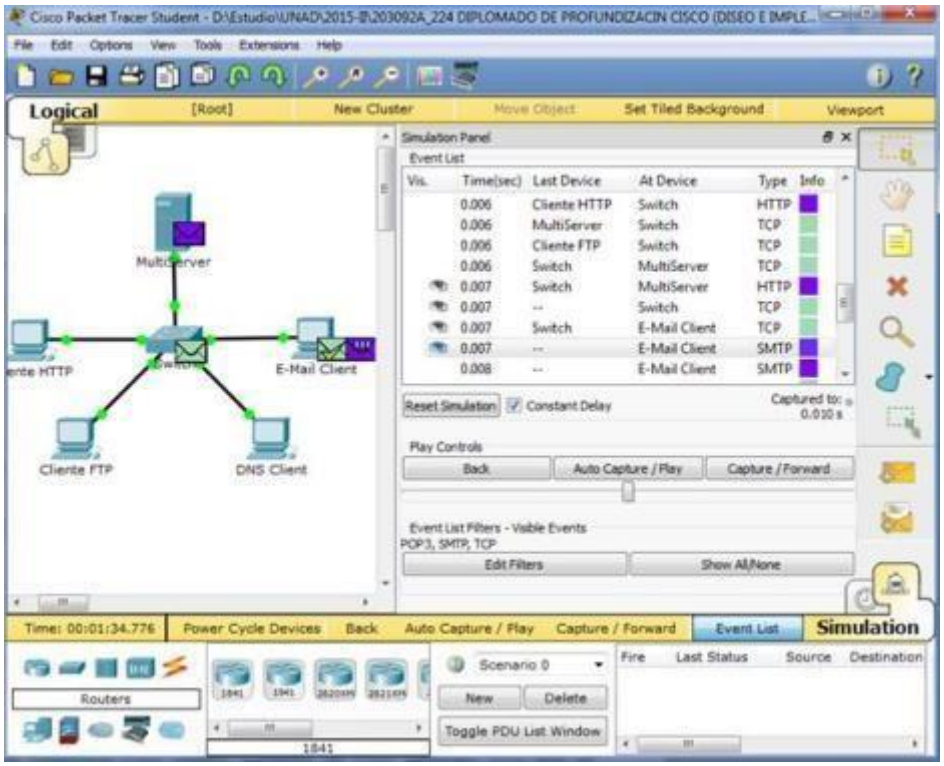
¿Estas comunicaciones se consideran confiables? **Sí**.

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**

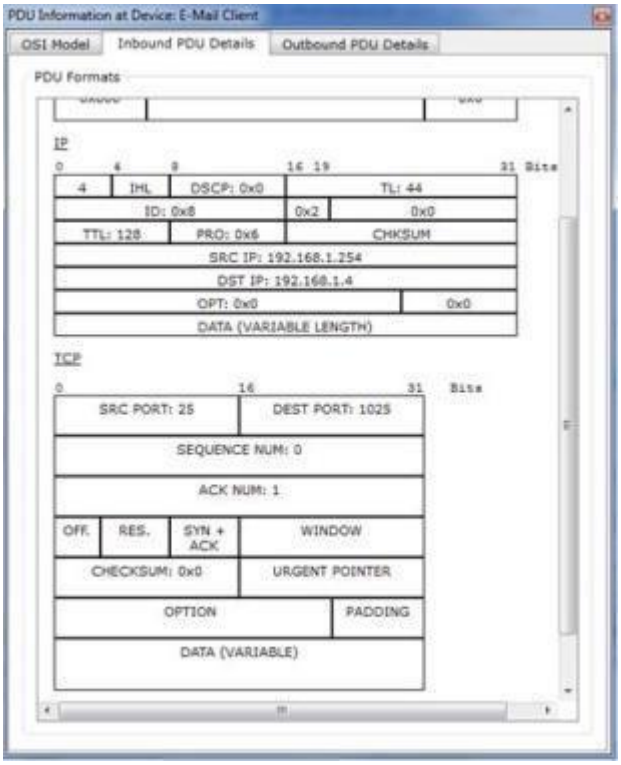


e. Cierre la PDU y haga clic en Capture/Forward hasta que una PDU vuelva a E-Mail Client con una marca de verificación.



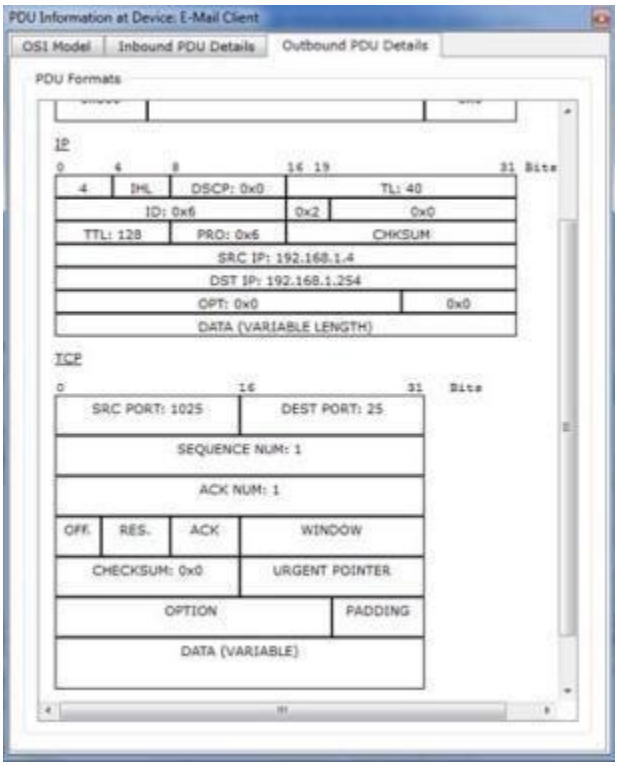
f. Haga clic en el sobre de PDU y seleccione Inbound PDU Details. ¿En qué cambiaron los números de puerto y de secuencia?

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

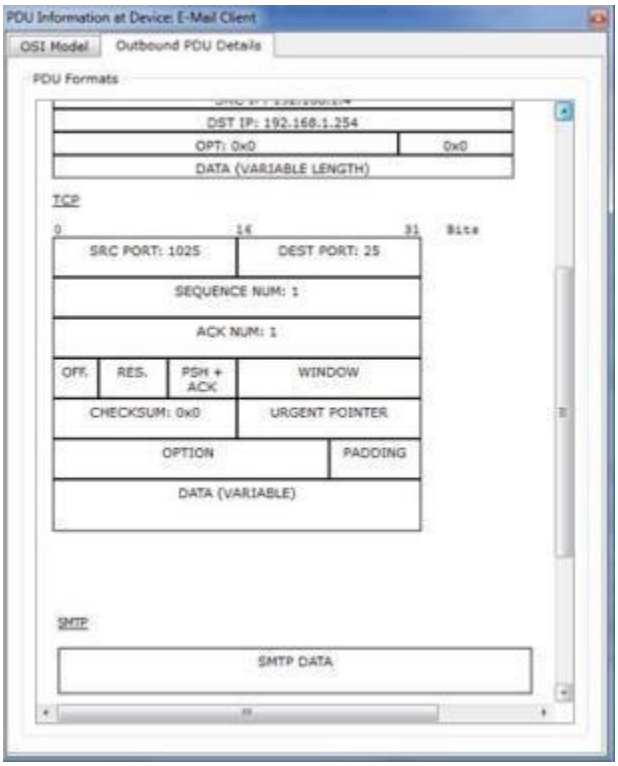


g. Haga clic en la ficha Outbound PDU Details (Detalles de PDU saliente). ¿En qué se diferencian los números de puerto y de secuencia respecto de los dos resultados anteriores?

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

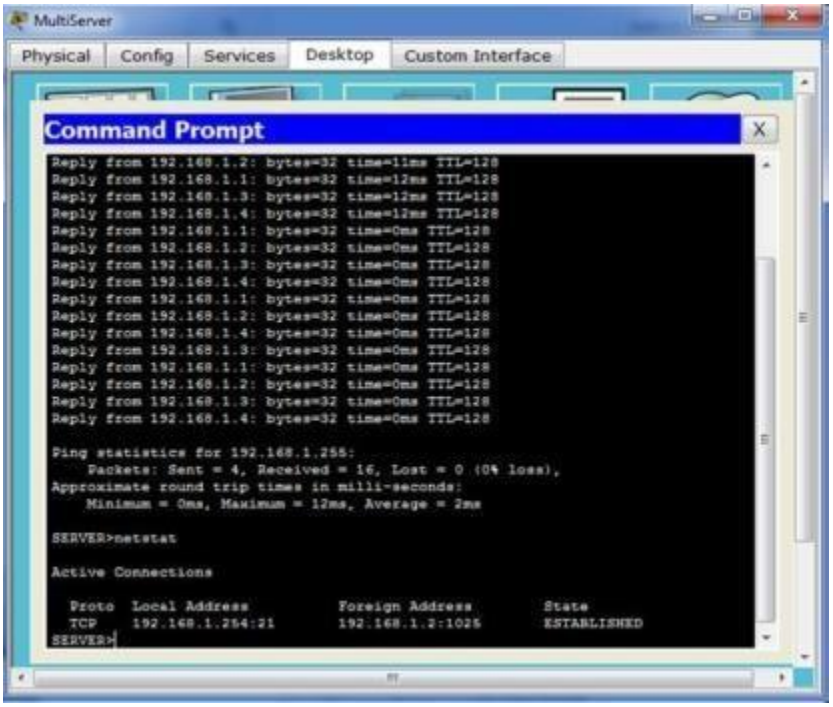
Paso 6: Examinar el uso de números de puerto del servidor.

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

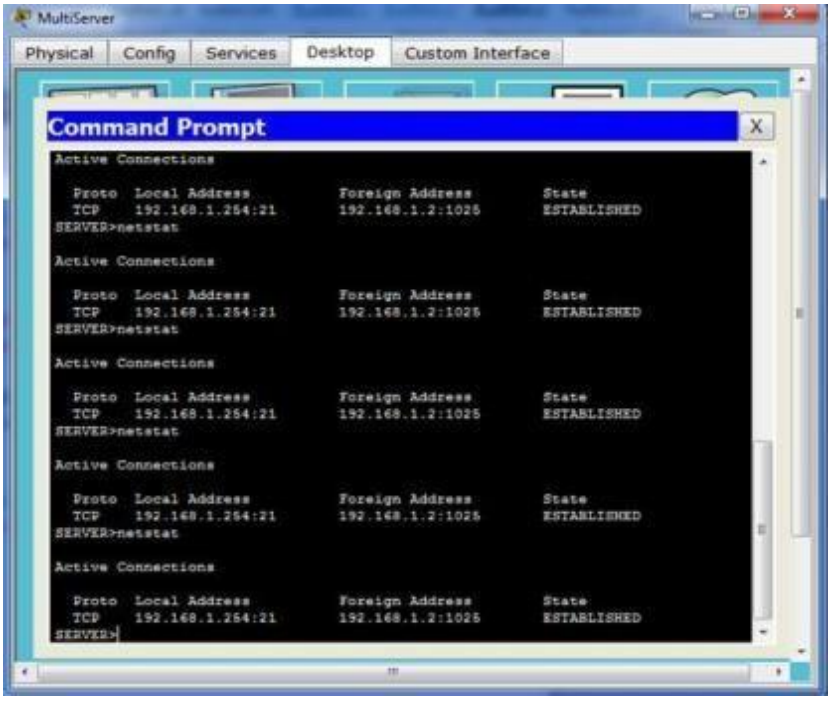


¿Qué números de puerto utiliza el servidor? **Las respuestas varían, pero los estudiantes pueden ver los tres: 21, 25 y 80. Definitivamente deben ver el puerto 21**.

c. ¿En qué estados están las sesiones?

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

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

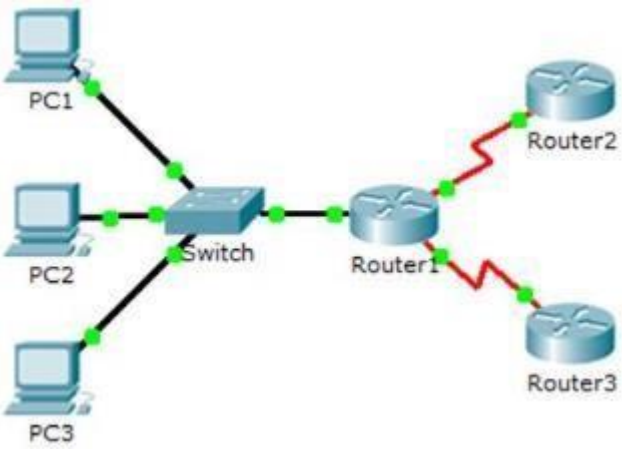


¿Por qué esta sesión no se cierra como las otras tres? (Sugerencia: revise los clientes minimizados) **El servidor está esperando una contraseña del cliente**.

Tabla de la actividad:

8.1.3.8 Investigación del tráfico unicast, broadcast y multicast

Topología



Objetivos

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

Información básica/situación

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

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

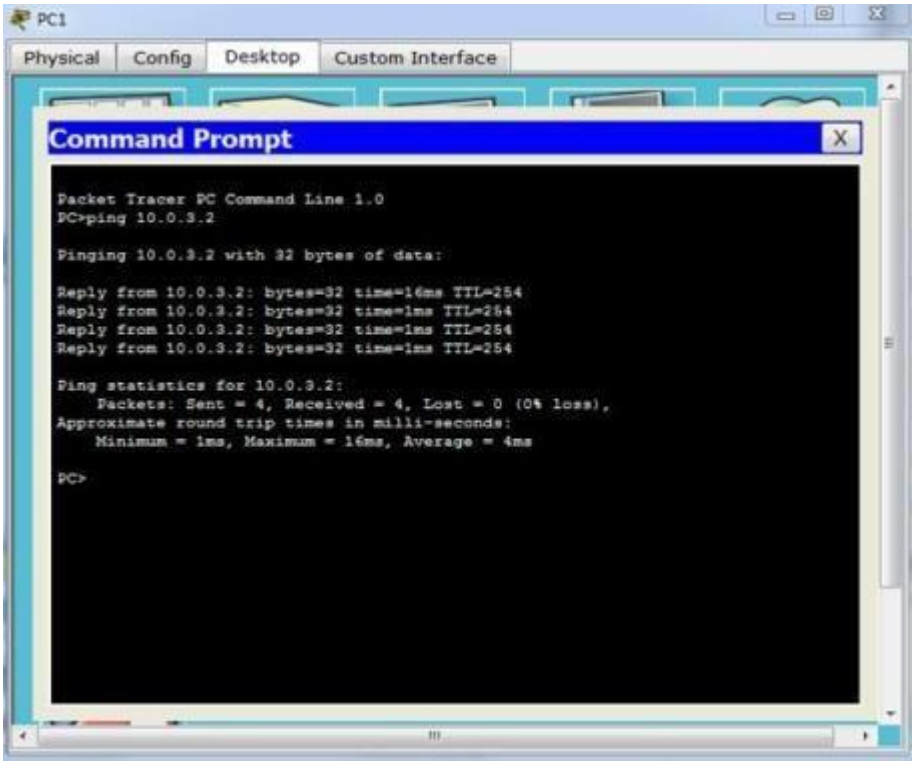
Para el tráfico de multicast, consultará el tráfico de EIGRP. Los routers Cisco utilizan EIGRP para intercambiar información de enrutamiento entre routers. Los routers que utilizan EIGRP envían paquetes a la dirección multicast 224.0.0.10, que representa el grupo de routers EIGRP. Si bien estos paquetes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

Parte 1: Generar tráfico de unicast

Paso 1: Utilizar el comando ping para generar tráfico

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

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

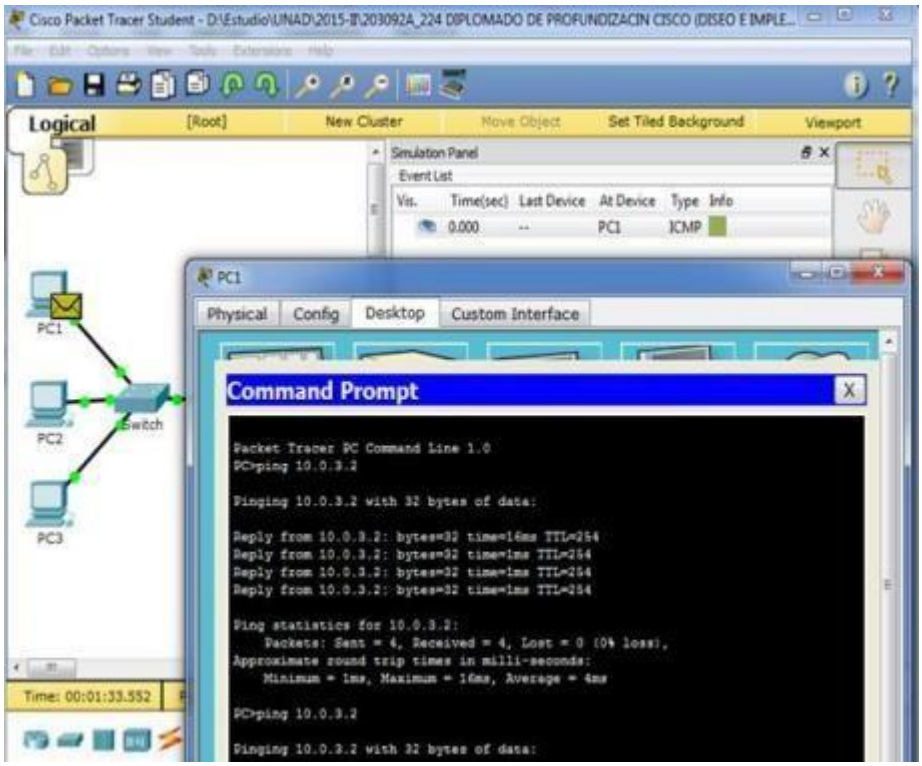


Paso 2: Ingrese al modo de simulación.

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

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

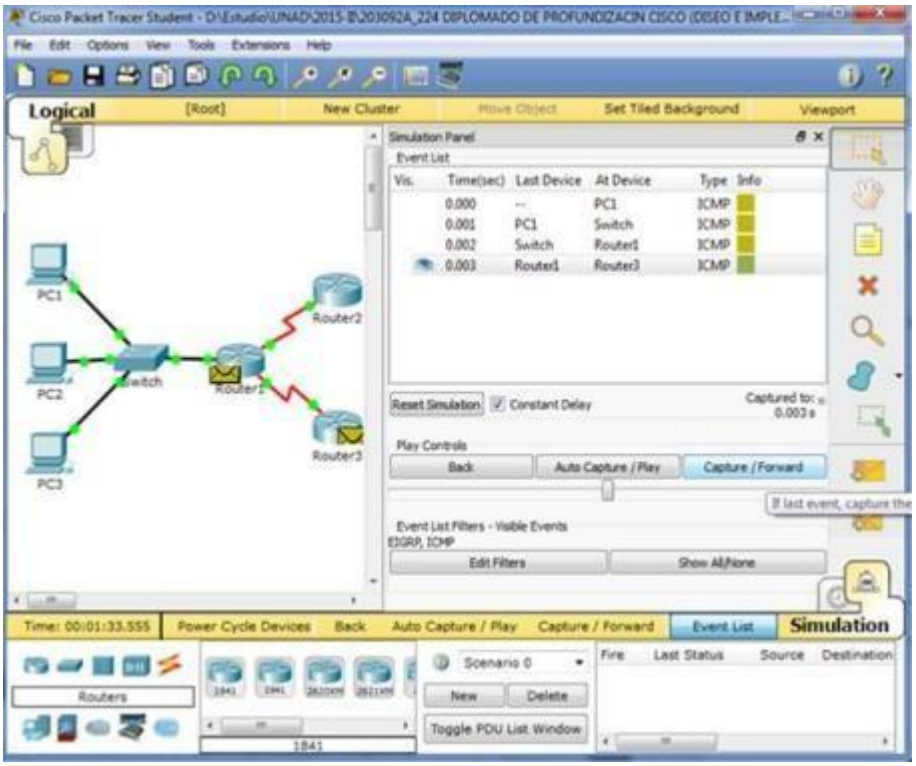
c. Haga clic en PC1 e introduzca el comando ping 10.0.3.2.



Paso 3: Examinar el tráfico de unicast

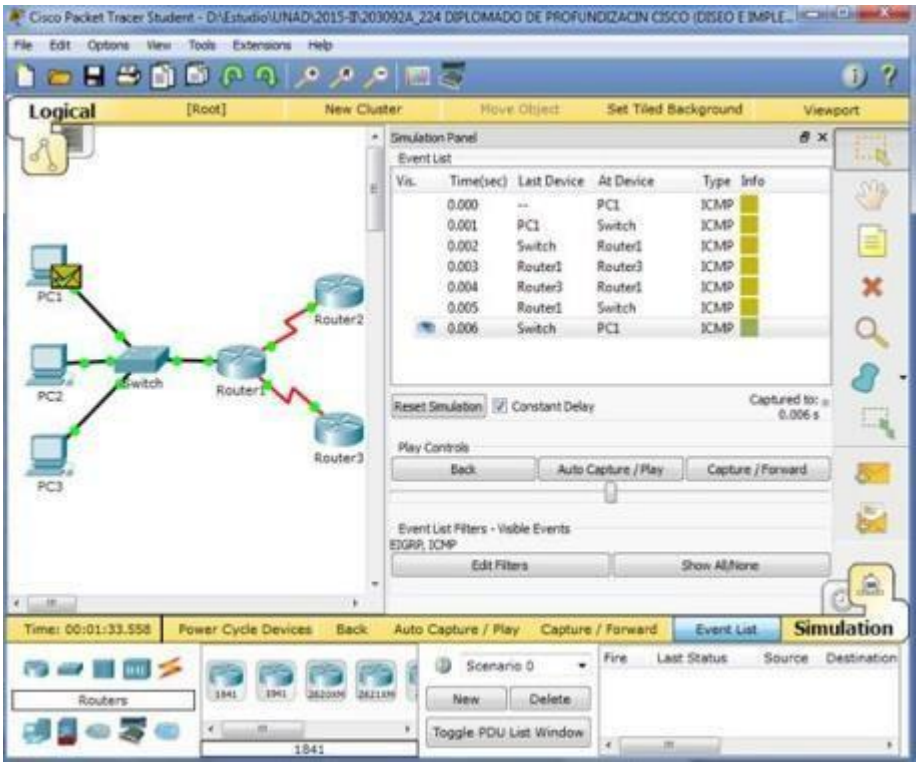
La PDU en la PC1 es una solicitud de eco de ICMP dirigida a la interfaz serial en el Router3.

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



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

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

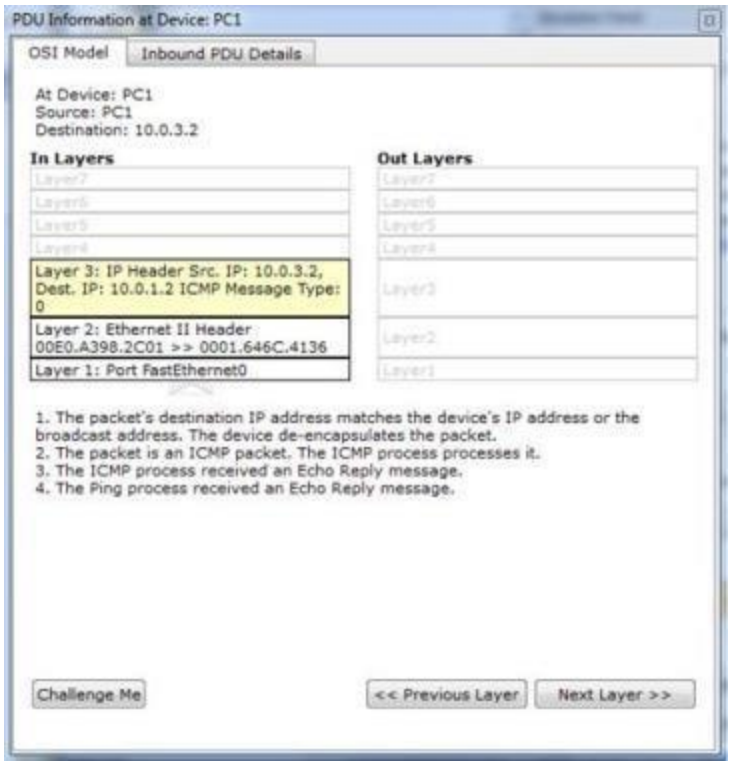


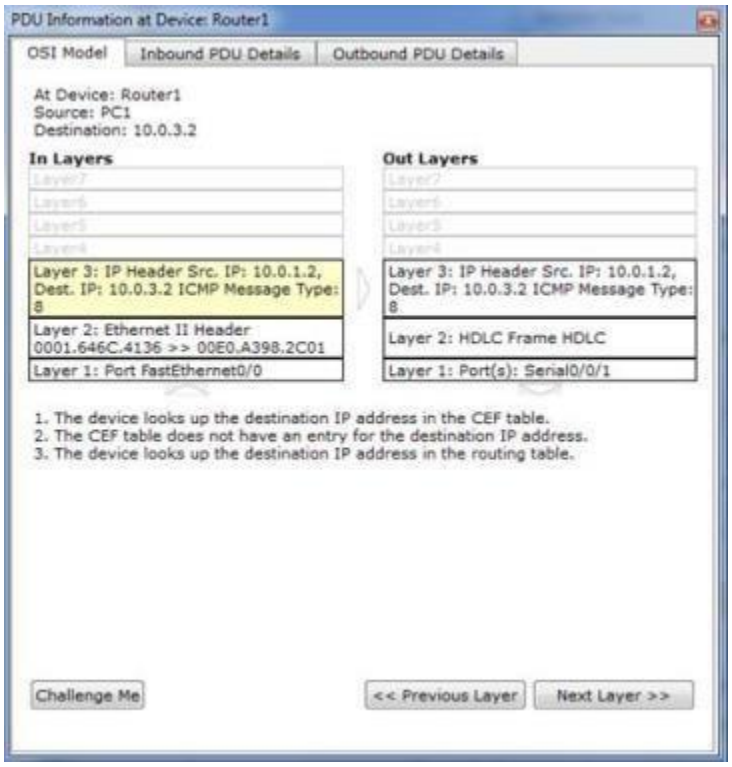
b. En la sección Simulation Panel Event List (Lista de eventos del panel de simulación), la última columna incluye un cuadro de color que proporciona acceso a información detallada sobre un evento. Haga clic en el cuadro de color de la última columna para obtener el primer evento. Se abre la ventana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

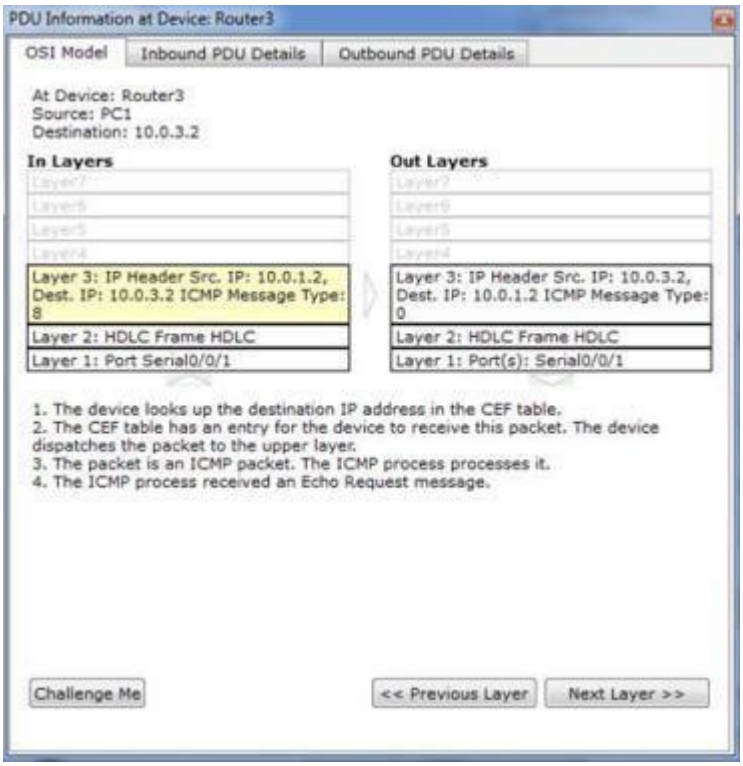
¿En qué capa comienza esta transmisión y por qué?

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

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.

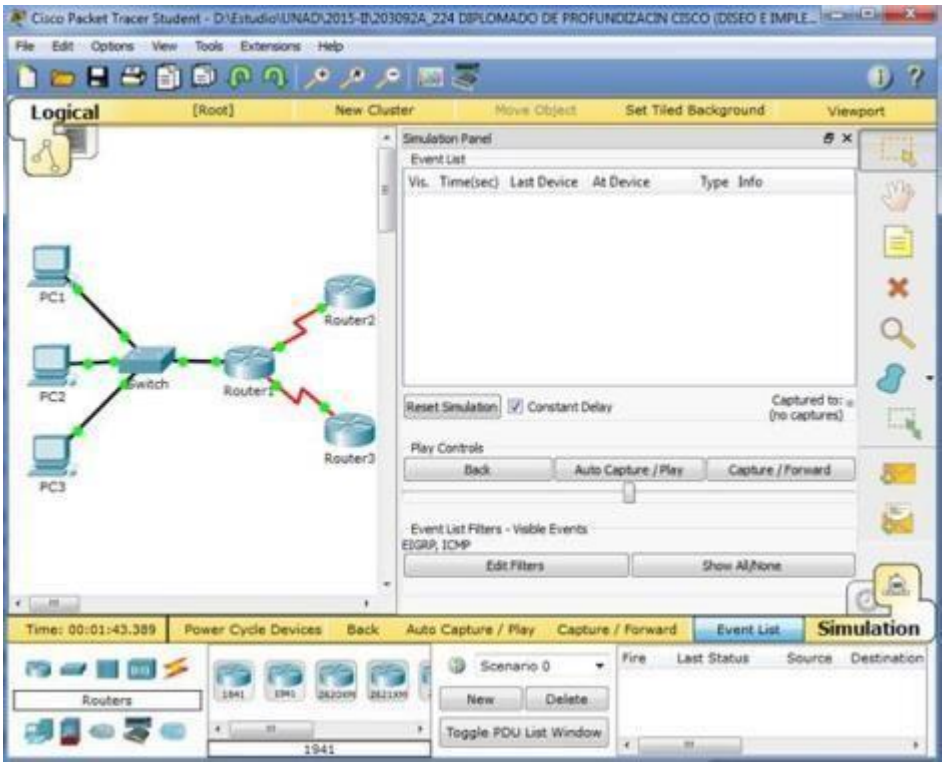

PDU Information at Device: PC1
OSI Model
Inbound PDU Details
At Device: PC1
Source: PC1
Destination: 10.0.3.2
In Layers
Out Layers
Layer 3: IP Header Src. IP: 10.0.3.2, Dest. IP: 10.0.1.2 ICMP Message Type: 0
Layer 2: Ethernet II Header 00E0.A398.2C01 >> 0001.646C.4136
Layer 1: Port FastEthernet0
1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
2. The packet is an ICMP packet. The ICMP process processes it.
3. The ICMP process received an Echo Reply message.
4. The Ping process received an Echo Reply message.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: Router1
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router1
Source: PC1
Destination: 10.0.3.2
In Layers
Out Layers
Layer 3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.646C.4136 >> 00E0.A398.2C01
Layer 1: Port FastEthernet0/0
Layer 3: IP Header Src. IP: 10.0.1.2, Dest. IP: 10.0.3.2 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC
Layer 1: Port(s): Serial0/0/1
1. The device looks up the destination IP address in the CEF table.
2. The CEF table does not have an entry for the destination IP address.
3. The device looks up the destination IP address in the routing table.
Challenge Me
<< Previous Layer
Next Layer >>



¿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**.

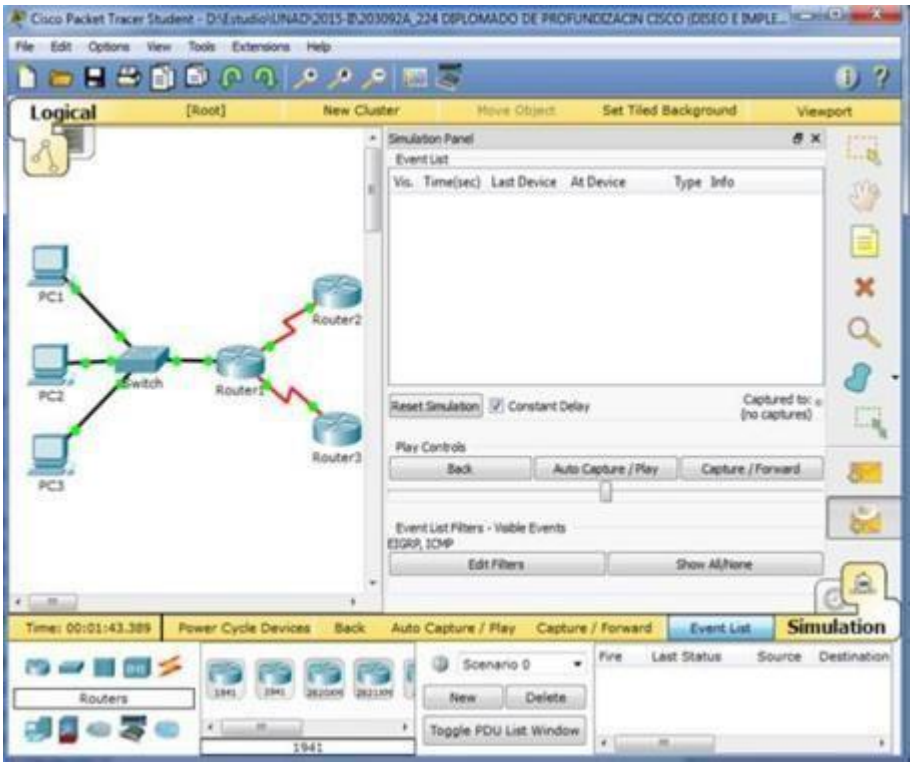
d. Haga clic en Reset Simulation (Restablecer simulación).



Parte 2: Generar tráfico de broadcast

Paso 1: Agregar una PDU compleja

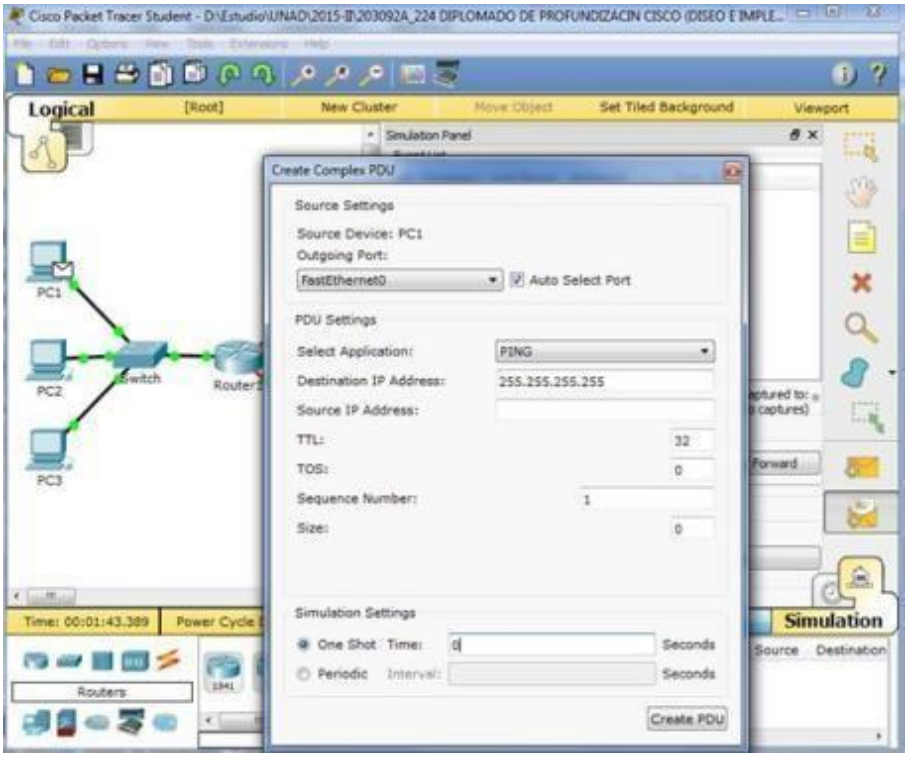
a. Haga clic en Add Complex PDU (Agregar una PDU compleja). Este ícono se ubica en la barra de herramientas de la derecha y muestra un sobre abierto.



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

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

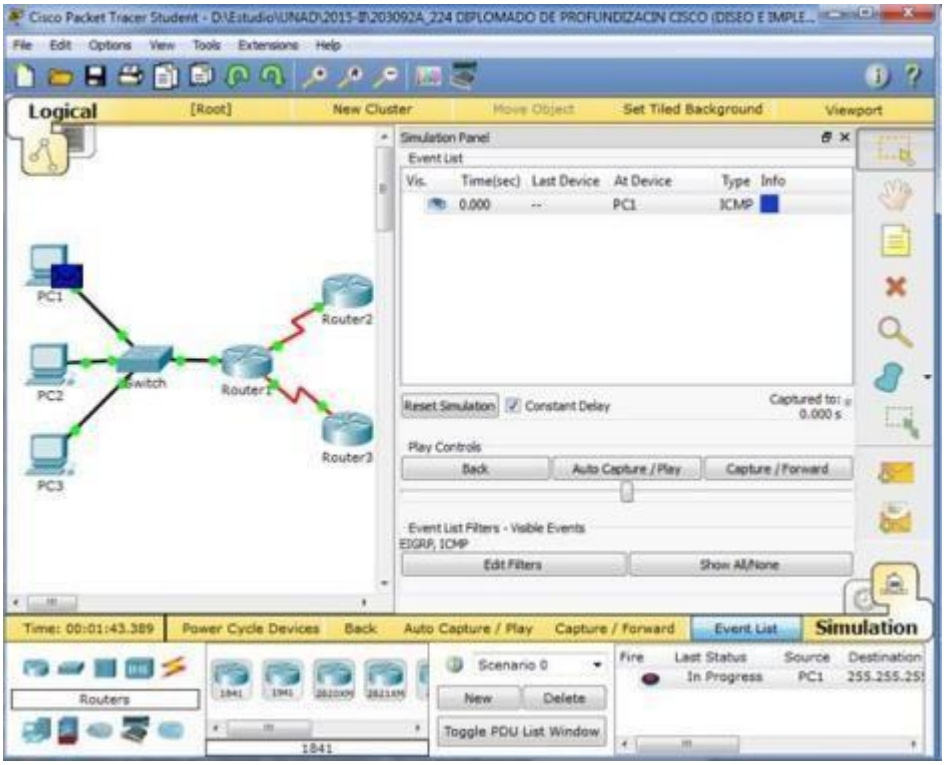
- Dirección IP de destino: 255.255.255.255 (dirección de broadcast)
- Número de secuencia: 1
- Tiempo de intento único: 0



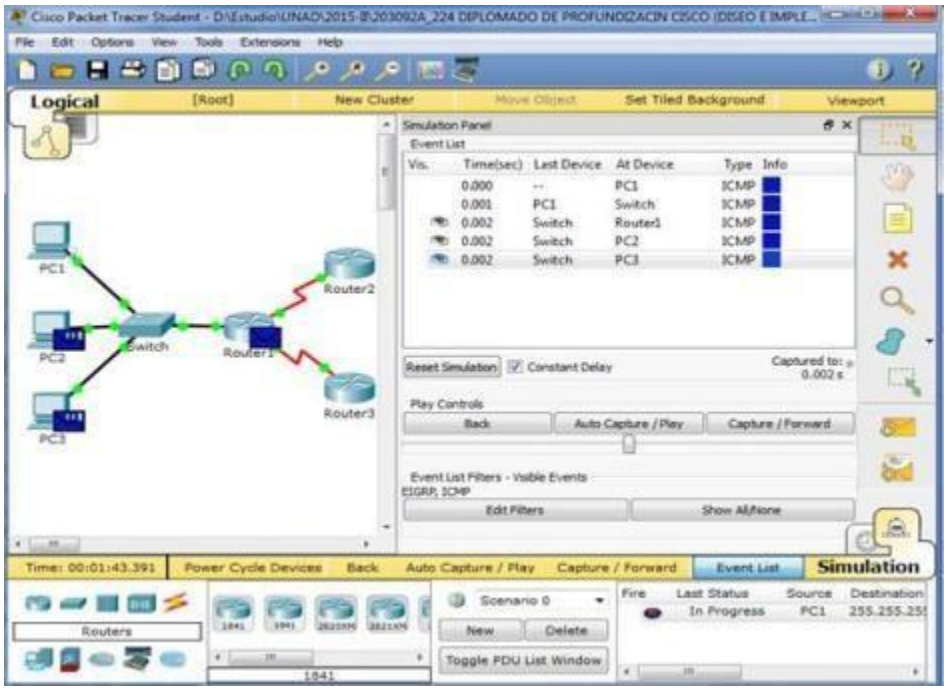
Dentro de la configuración de la PDU, el valor predeterminado para Select Application (Seleccionar aplicación) es PING. ¿Qué otras tres aplicaciones, como mínimo, están disponibles para utilizar?

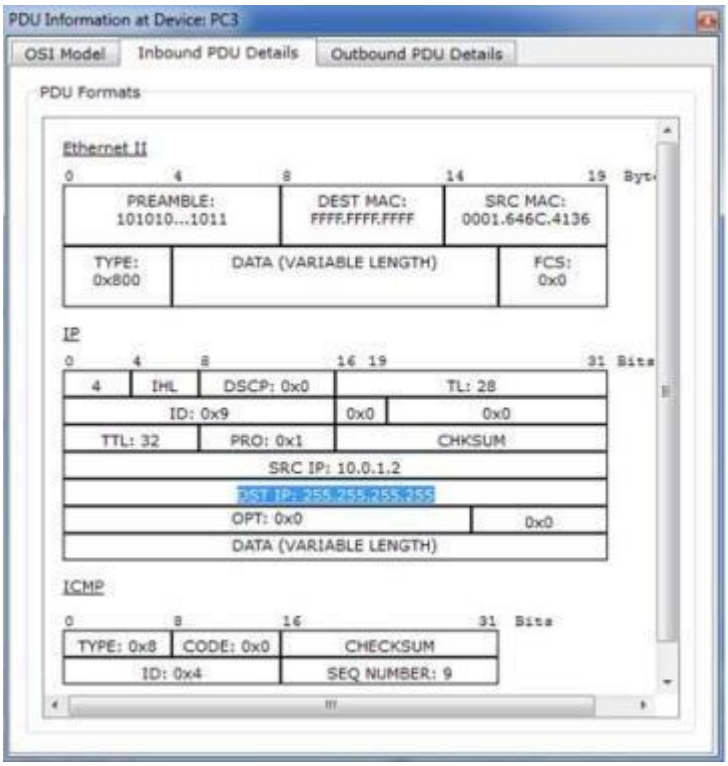
DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP y OTHER.

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



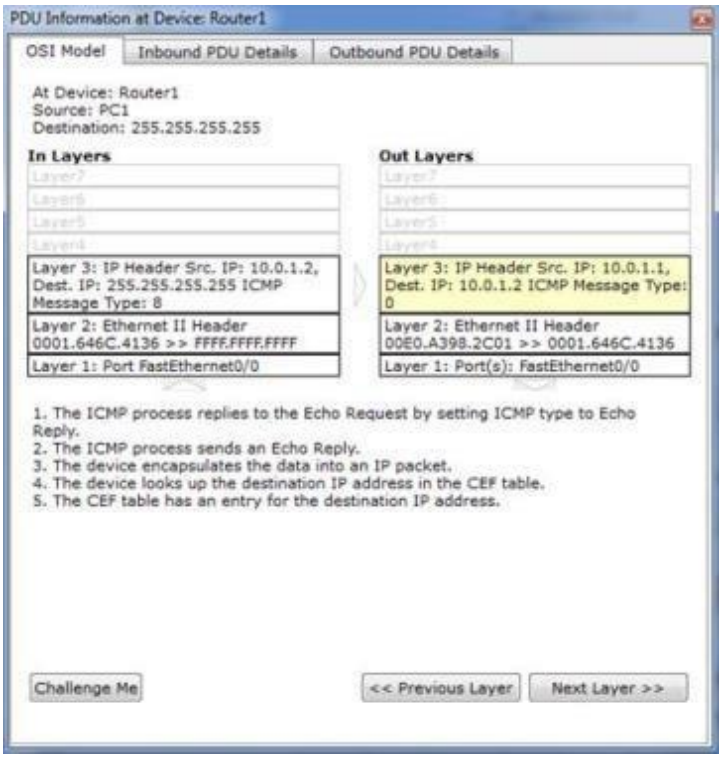
e. Haga clic en Capture/Forward dos veces. Este paquete se envía al switch y después se transmite por broadcast a la PC2, la PC3, y el Router1. Examine la información de la Capa 3 para todos los eventos. Observe que la dirección IP de destino es 255.255.255.255, que es la dirección IP de broadcast que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

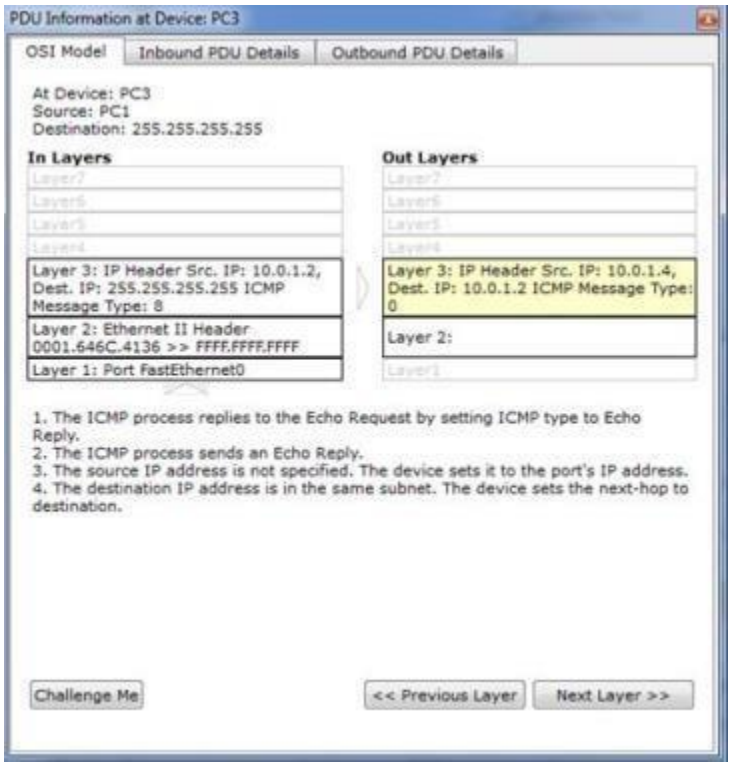




Si analiza la información del modelo OSI, ¿qué cambios se produjeron en la información de la capa 3 en la columna Out Layers (Capas de salida) en el Router1, la PC2 y la PC3?

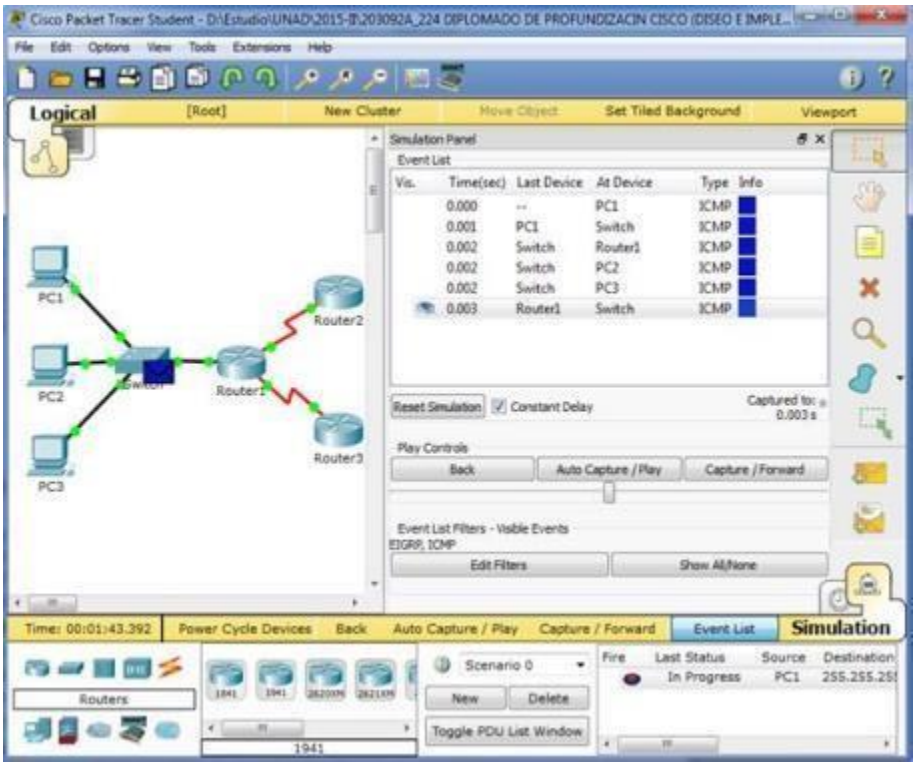
La PDU se convierte en un unicast que contesta a la PC1.



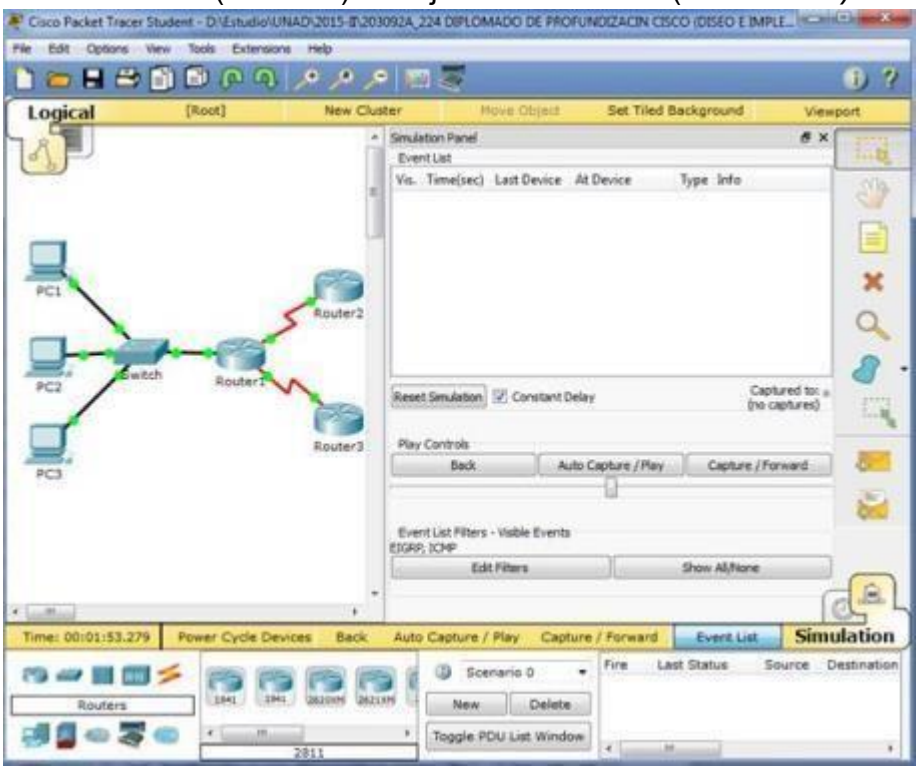


f. Haga clic en Capture/Forward nuevamente. ¿La PDU de broadcast se reenvía en algún momento al Router2 o al Router3? ¿Por qué?

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



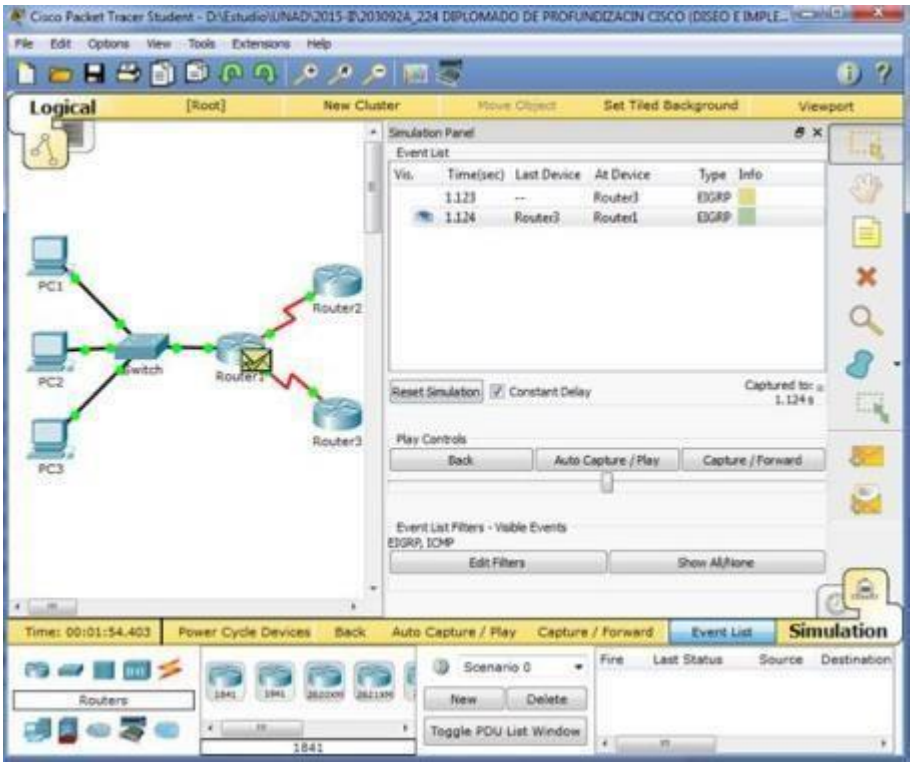
g. Después de que termine de examinar el comportamiento de broadcast, elimine el paquete de prueba haciendo clic en Delete (Eliminar) debajo de Scenario 0 (Situación 0).



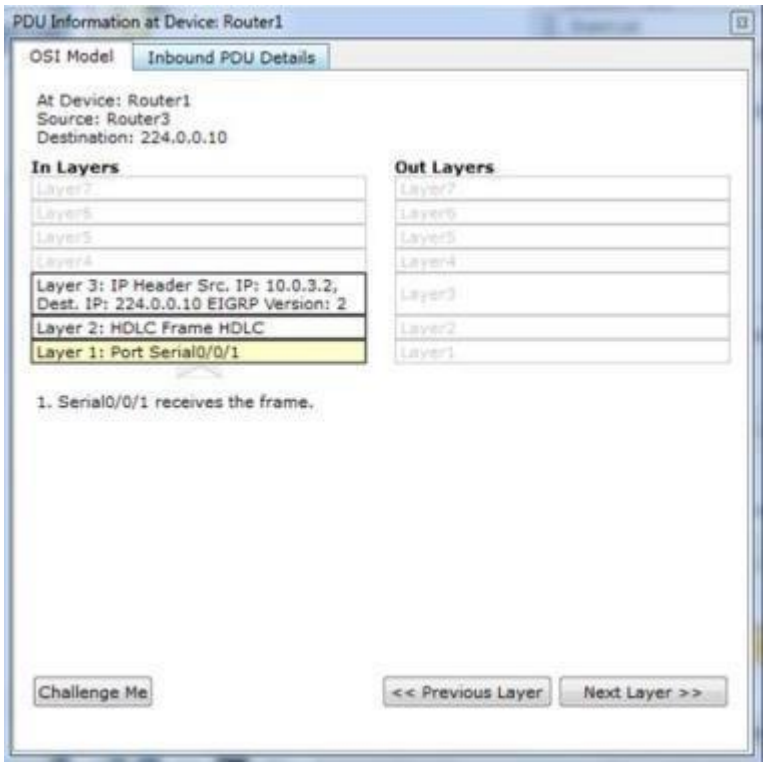
Parte 3: Investigar el tráfico de multicast

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.

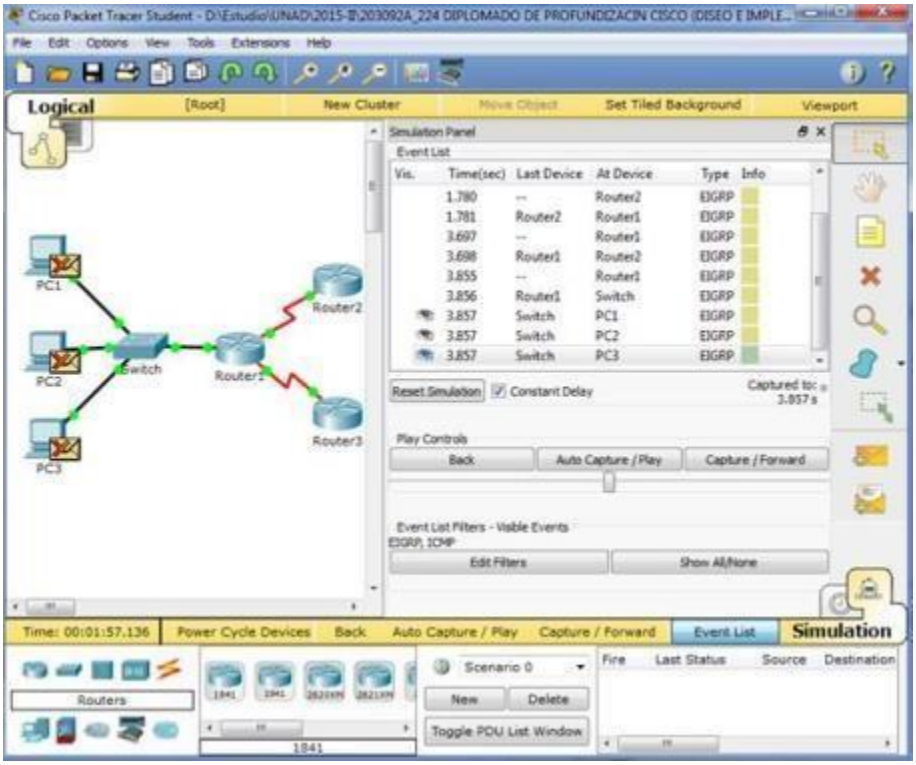


b. Examine el contenido de estos paquetes abriendo la ventana de información de PDU y vuelva a hacer clic en Capture/Forward. Los paquetes se envían a los otros dos routers y al switch. Los routers aceptan y procesan los paquetes porque son parte del grupo multicast. El switch reenviará los paquetes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



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

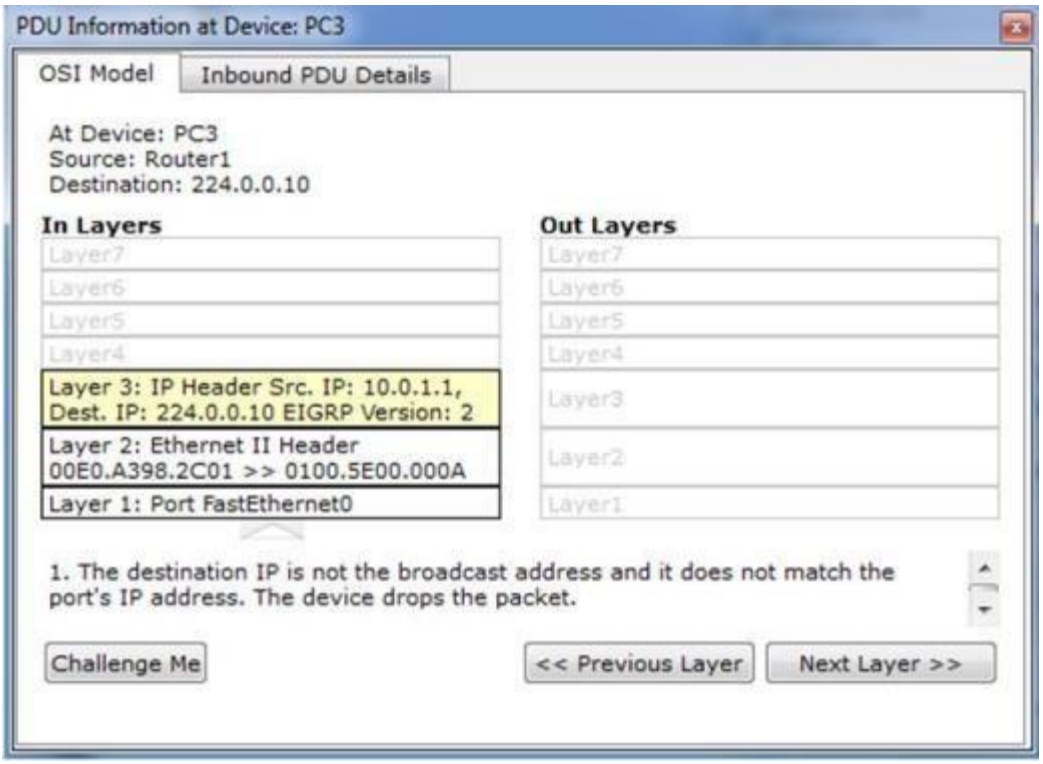
¿Qué hacen los hosts con los paquetes? **Los hosts rechazan y descartan los paquetes**.

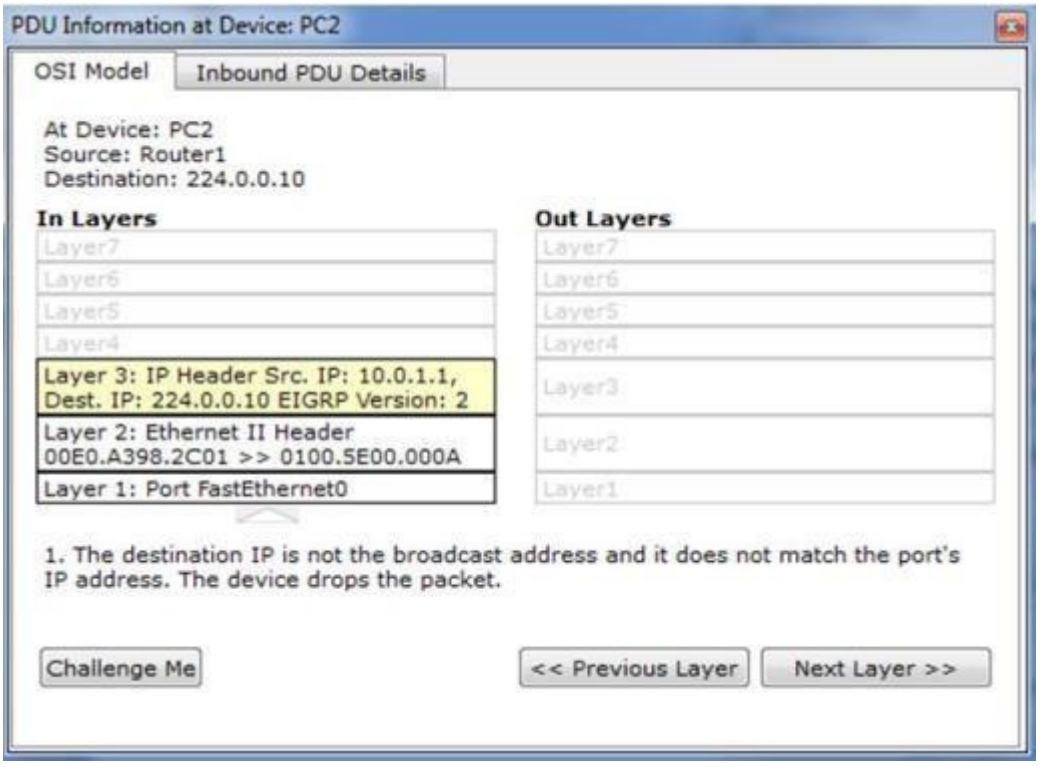


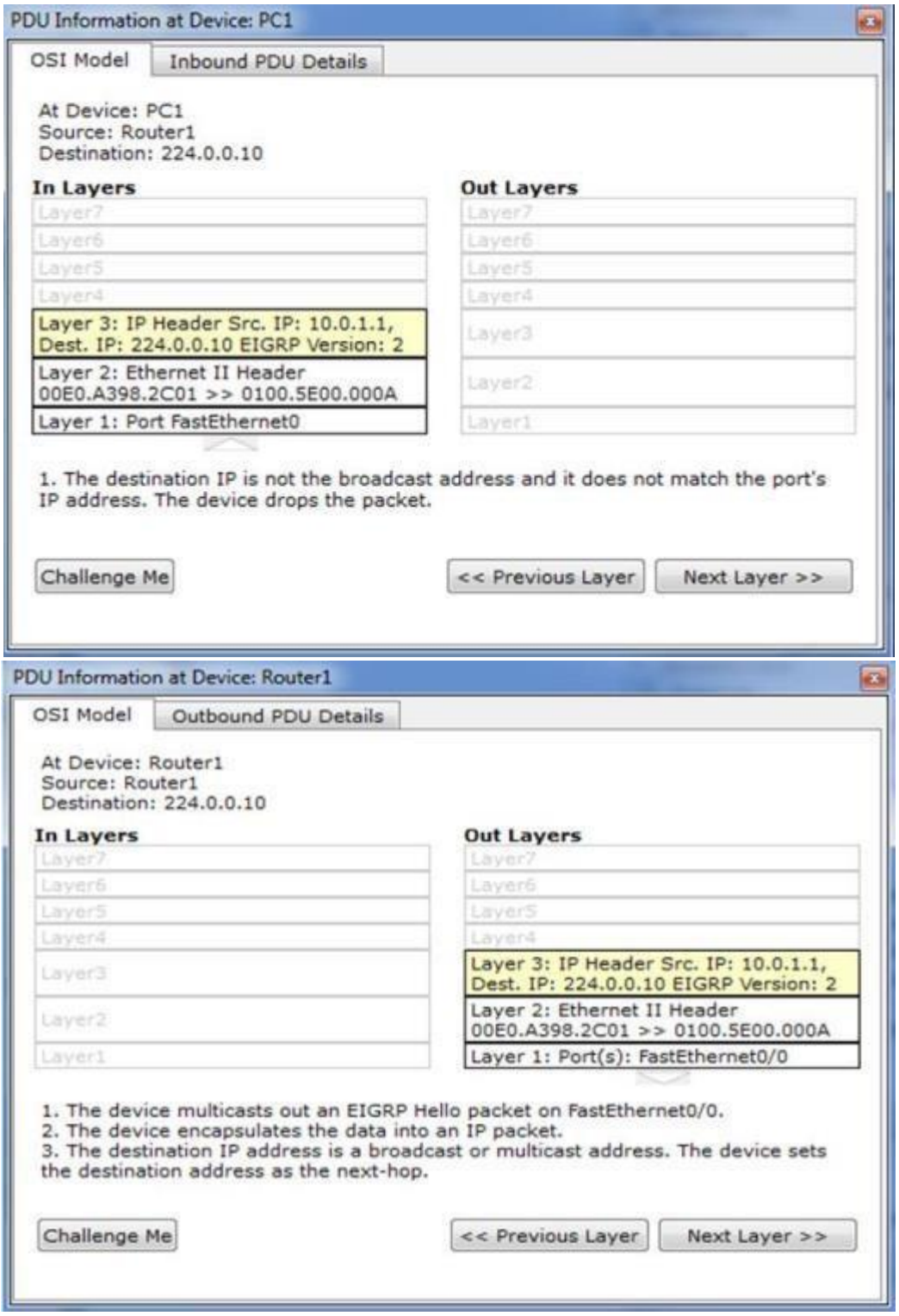
Examine la información de las capas 3 y 4 para todos los eventos EIGRP.

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

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


PDU Information at Device: PC3
OSI Model
Inbound PDU Details
At Device: PC3
Source: Router1
Destination: 224.0.0.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 10.0.1.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
Layer3
Layer 2: Ethernet II Header 00E0.A398.2C01 >> 0100.5E00.000A
Layer2
Layer 1: Port FastEthernet0
Layer1
1. The destination IP is not the broadcast address and it does not match the port's IP address. The device drops the packet.
Challenge Me
<< Previous Layer
Next Layer >>

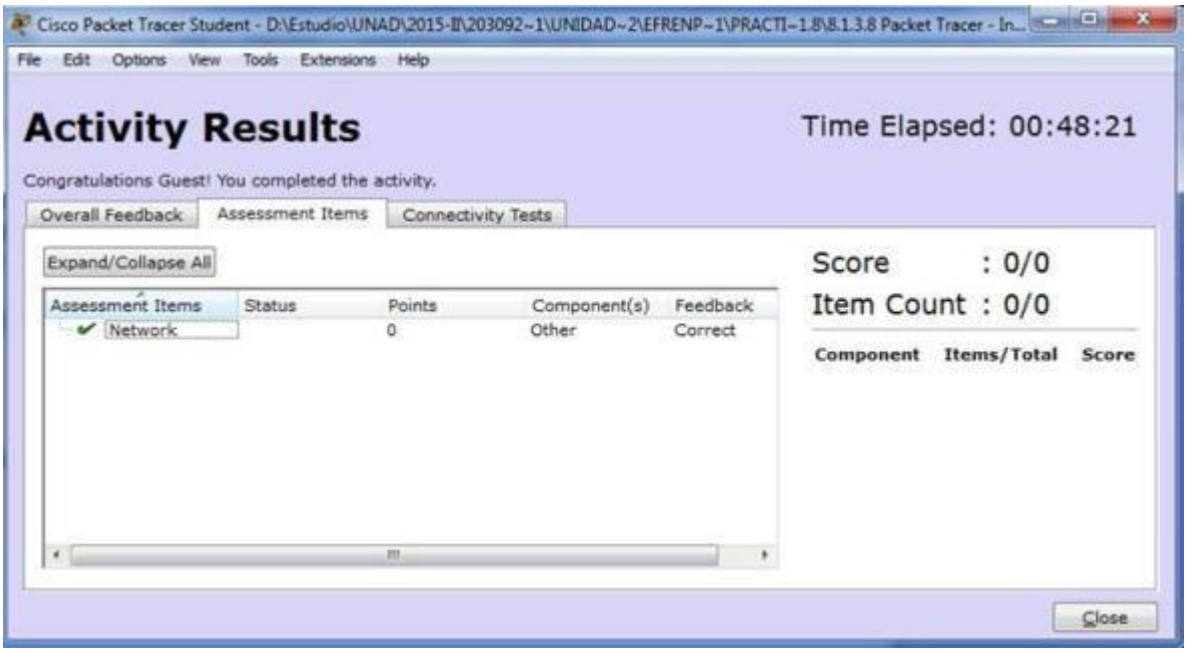

PDU Information at Device: PC2
OSI Model
Inbound PDU Details
At Device: PC2
Source: Router1
Destination: 224.0.0.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 10.0.1.1, Dest. IP: 224.0.0.10 EIGRP Version: 2
Layer3
Layer 2: Ethernet II Header 00E0.A398.2C01 >> 0100.5E00.000A
Layer2
Layer 1: Port FastEthernet0
Layer1
1. The destination IP is not the broadcast address and it does not match the port's IP address. The device drops the packet.
Challenge Me
<< Previous Layer
Next Layer >>



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

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

Tabla de la actividad:



8.2.5.3 Configuración de direccionamiento IPv6

Topología

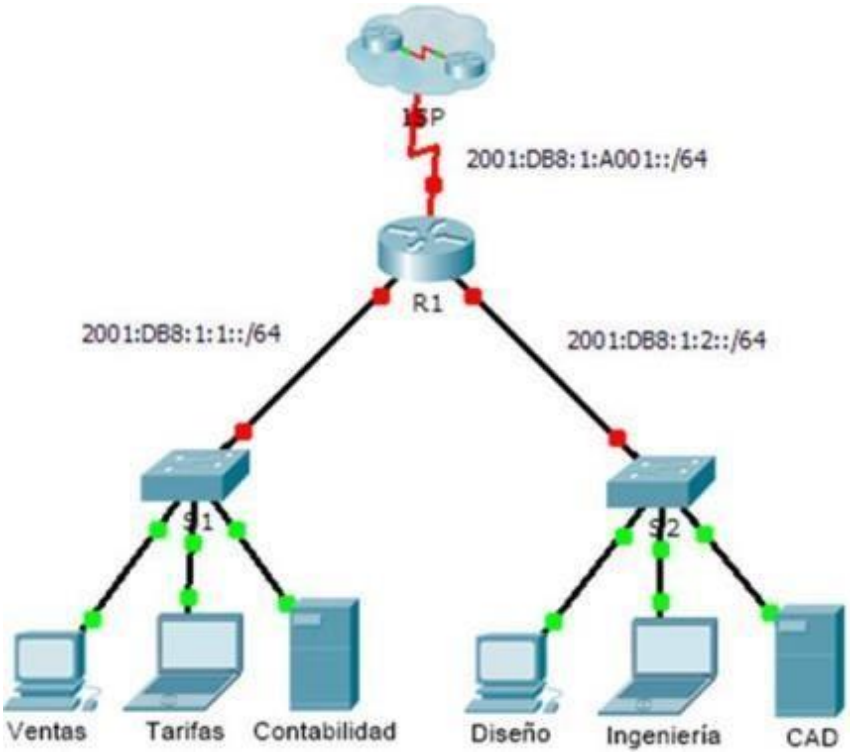


Tabla de direccionamiento

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

Objetivos

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

Información básica

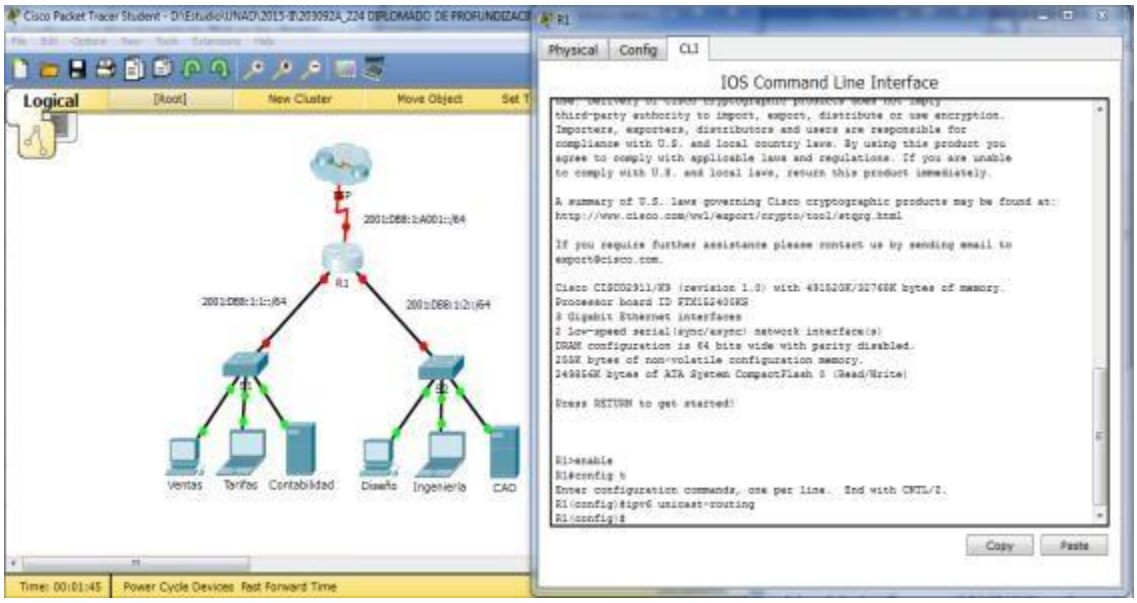
En esta actividad, practicará la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificará la implementación de las direcciones IPv6.

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Habilitar el router para reenviar paquetes IPv6

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

R1(config)# ipv6 unicast-routing



Paso 2: Configurar el direccionamiento IPv6 en GigabitEthernet0/0

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

b. Ingrese al modo EXEC privilegiado.

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

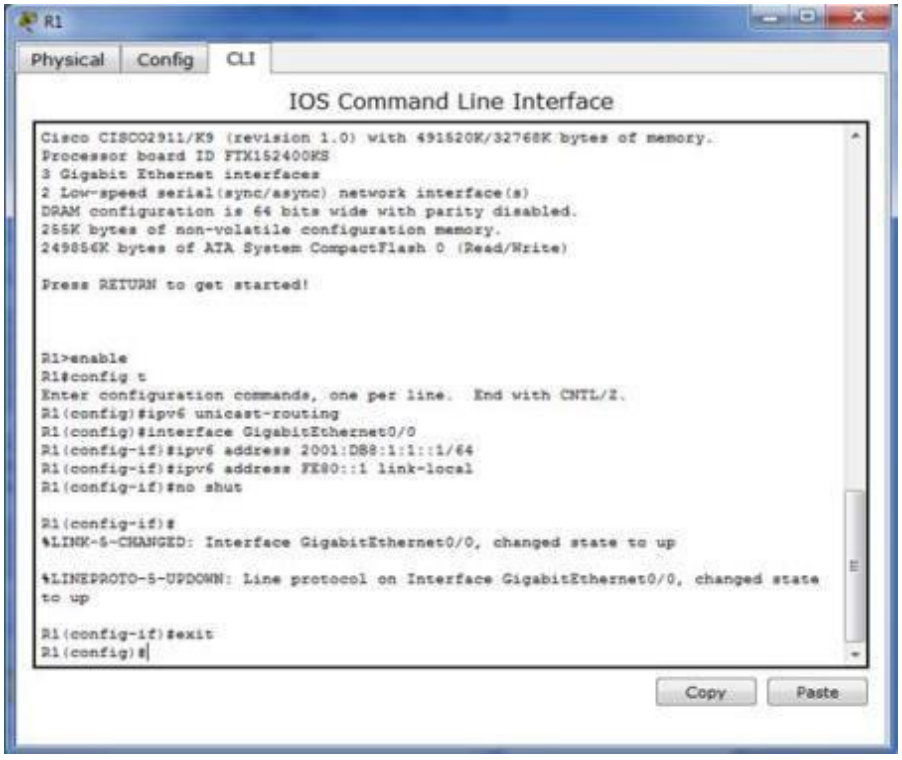
d. Configure la dirección IPv6 con el siguiente comando:

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

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

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

f. Active la interfaz.

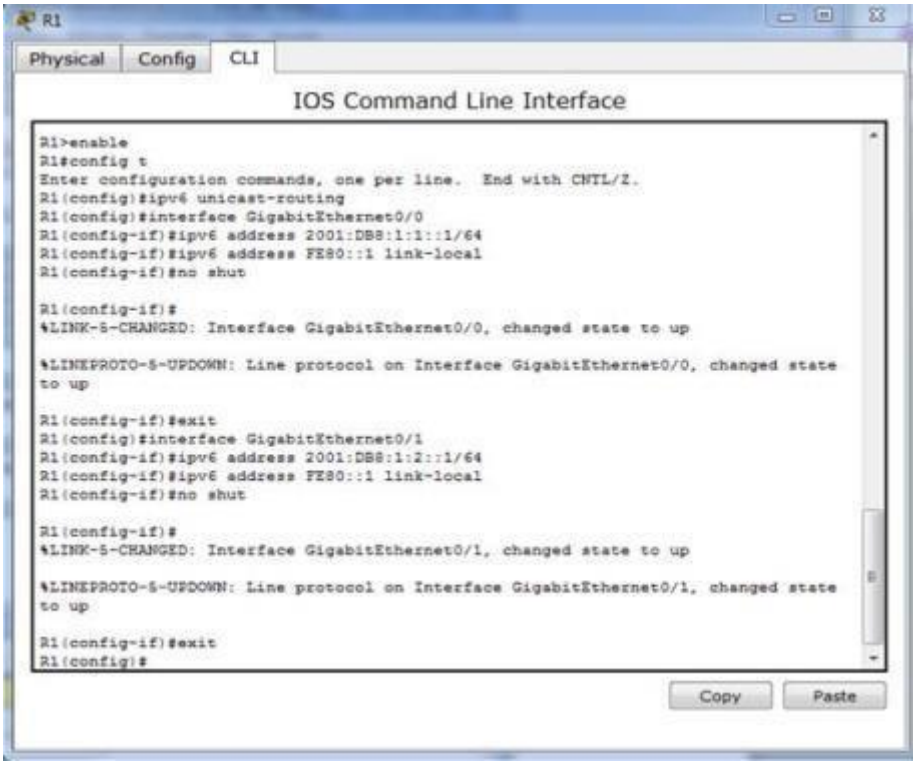


Paso 3: Configurar el direccionamiento IPv6 en GigabitEthernet0/1

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.

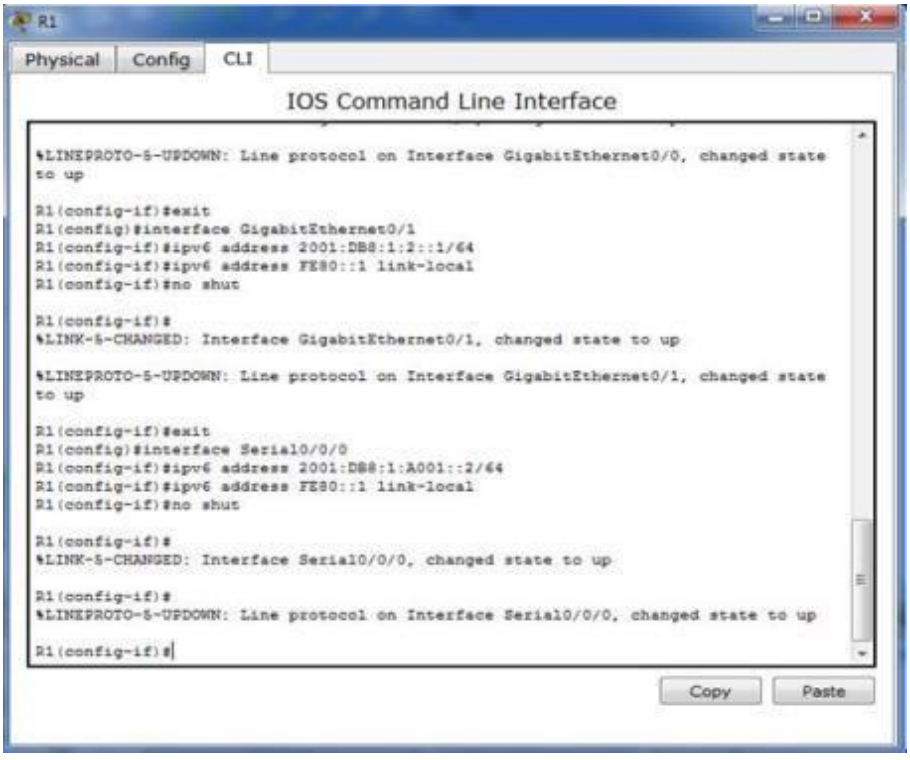


Paso 4: Configurar el direccionamiento IPv6 en Serial0/0/0

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.



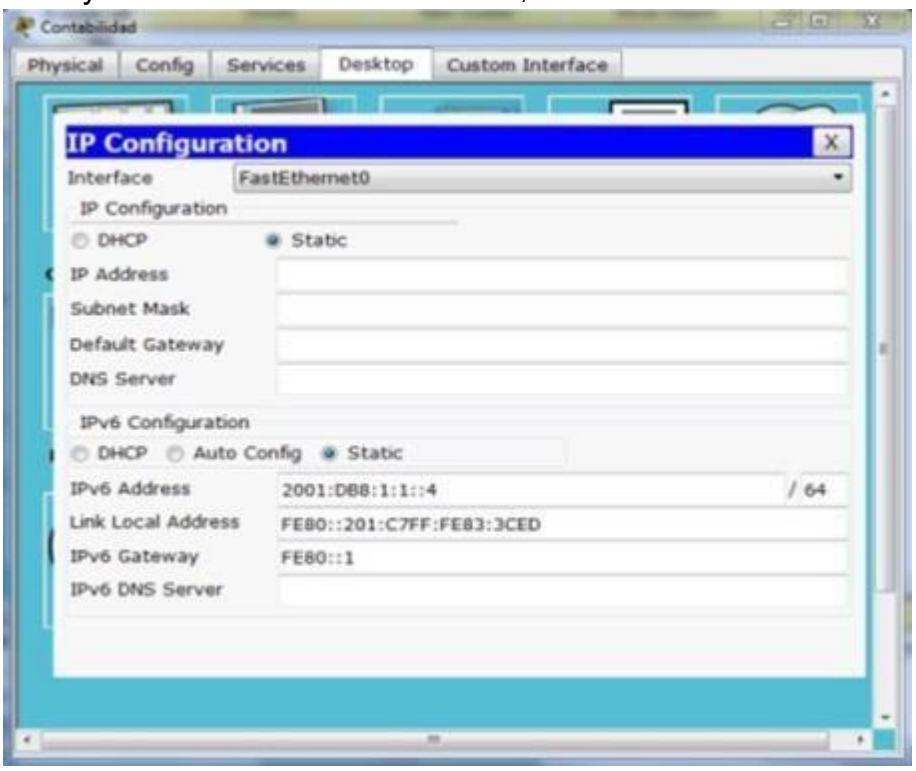
Parte 2: Configurar el direccionamiento IPv6 en los servidores

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).

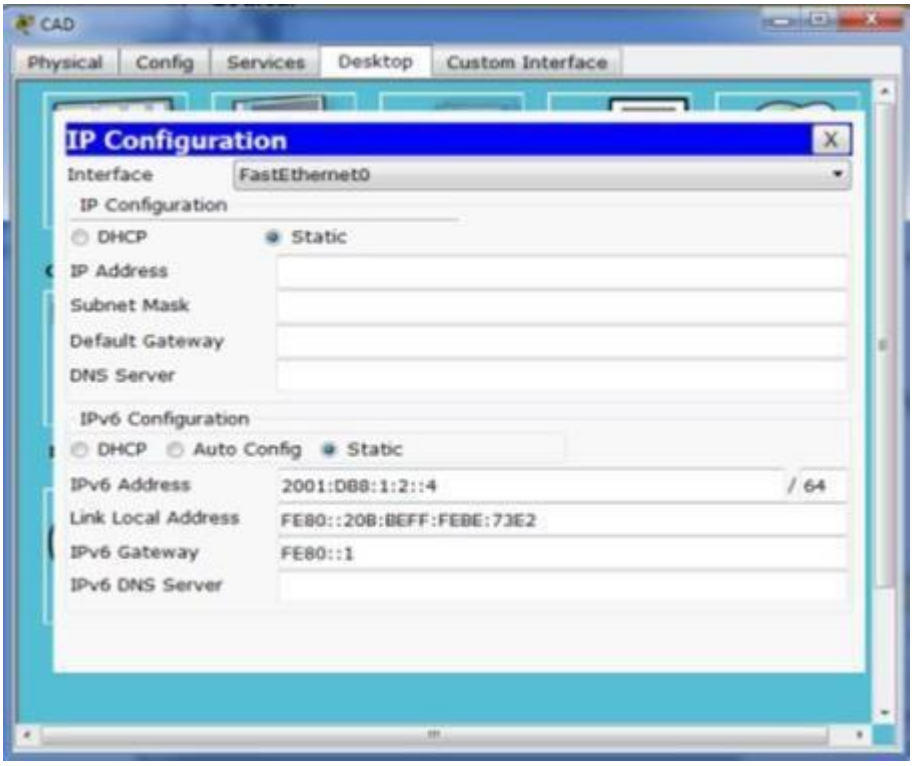
b. Establezca la dirección IPv6 2001:DB8:1:1::4 con el prefijo /64.

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.



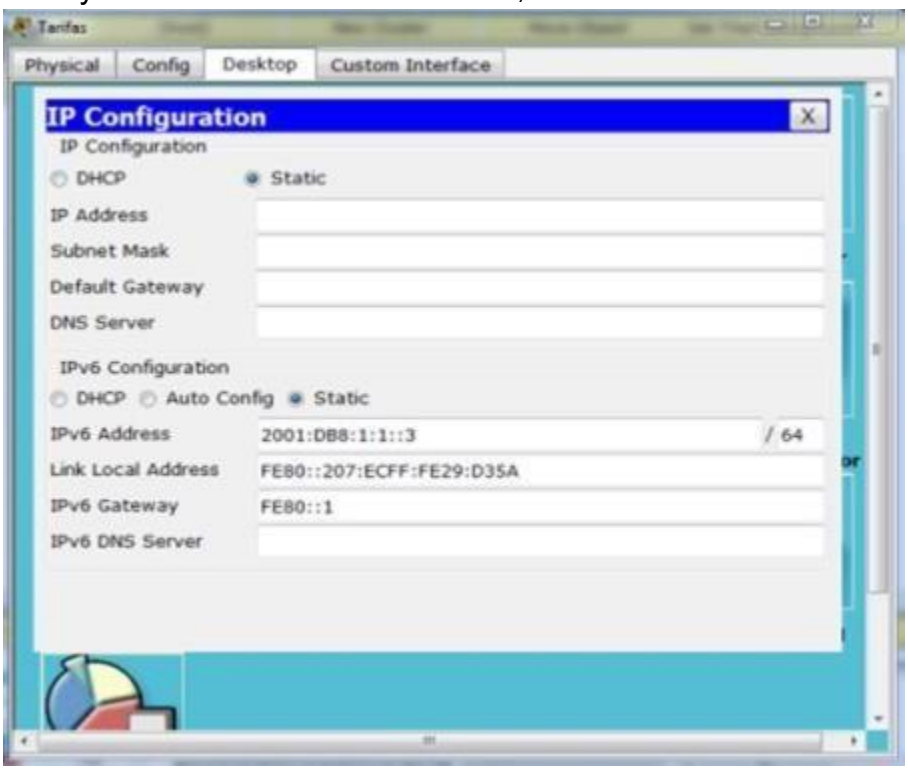
Parte 3: Configurar el direccionamiento IPv6 en los clientes

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

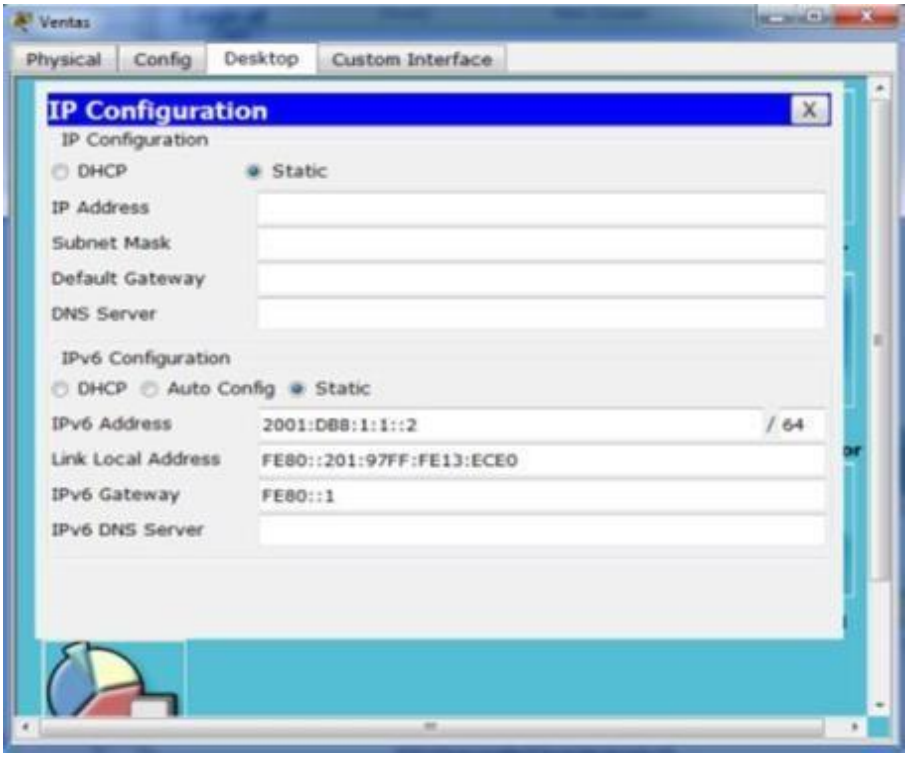
a. Haga clic en Billing (Facturación) y, a continuación, seleccione la ficha Desktop seguida de IP Configuration.

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.

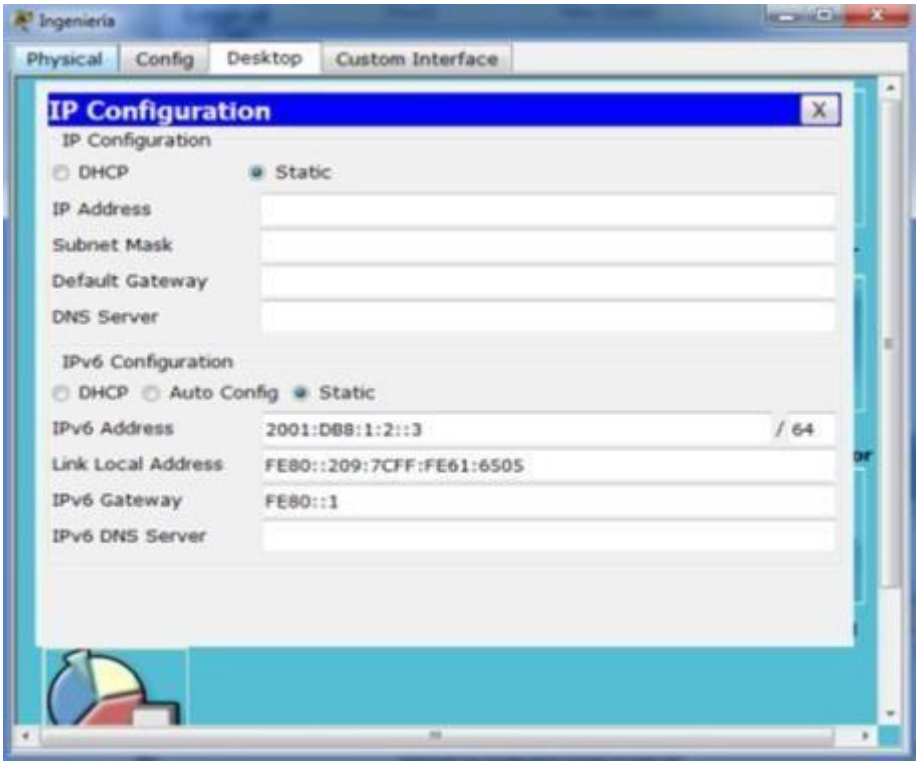


Paso 2: Configurar el direccionamiento IPv6 en los clientes de ingeniería y diseño

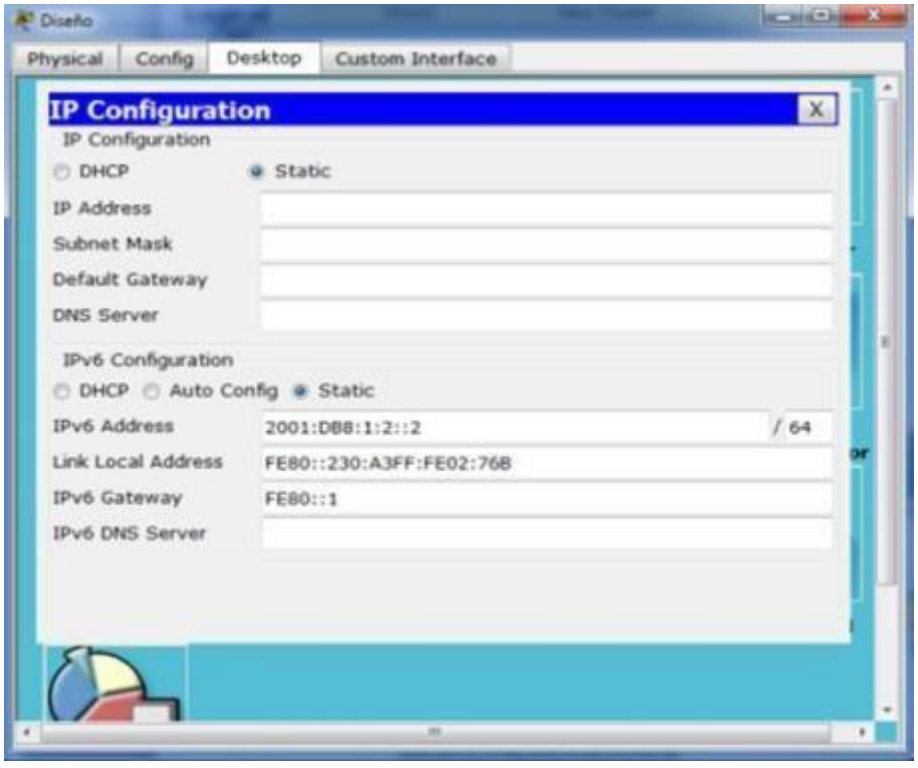
a. Haga clic en Engineering (Ingeniería) y, a continuación, seleccione la ficha Desktop seguida de IP Configuration.

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.

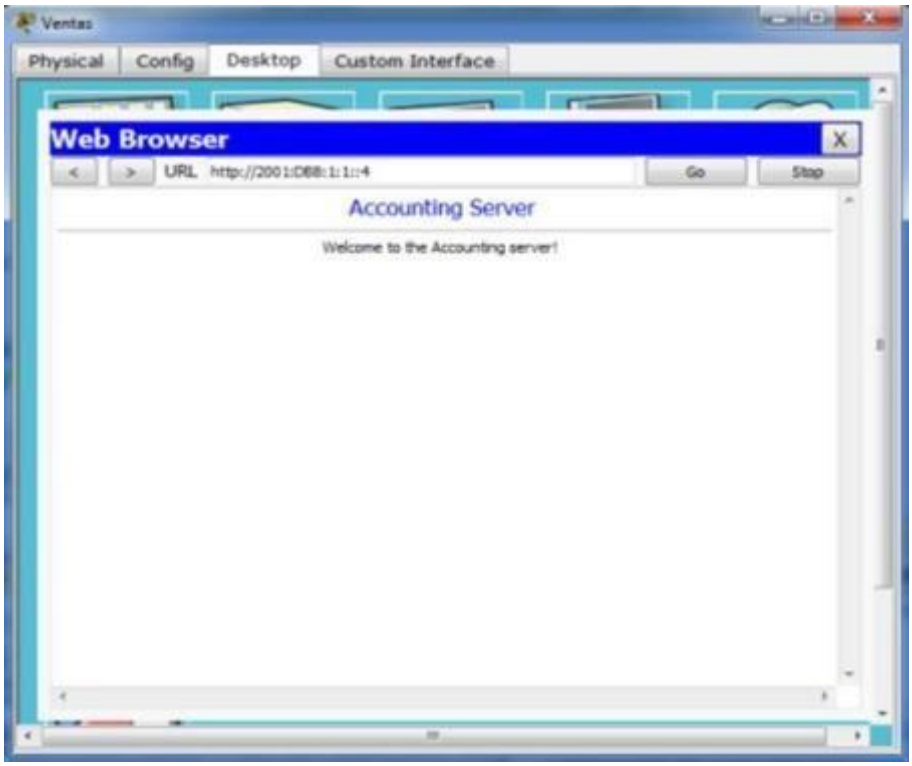


Parte 4: Probar y verificar la conectividad de la red

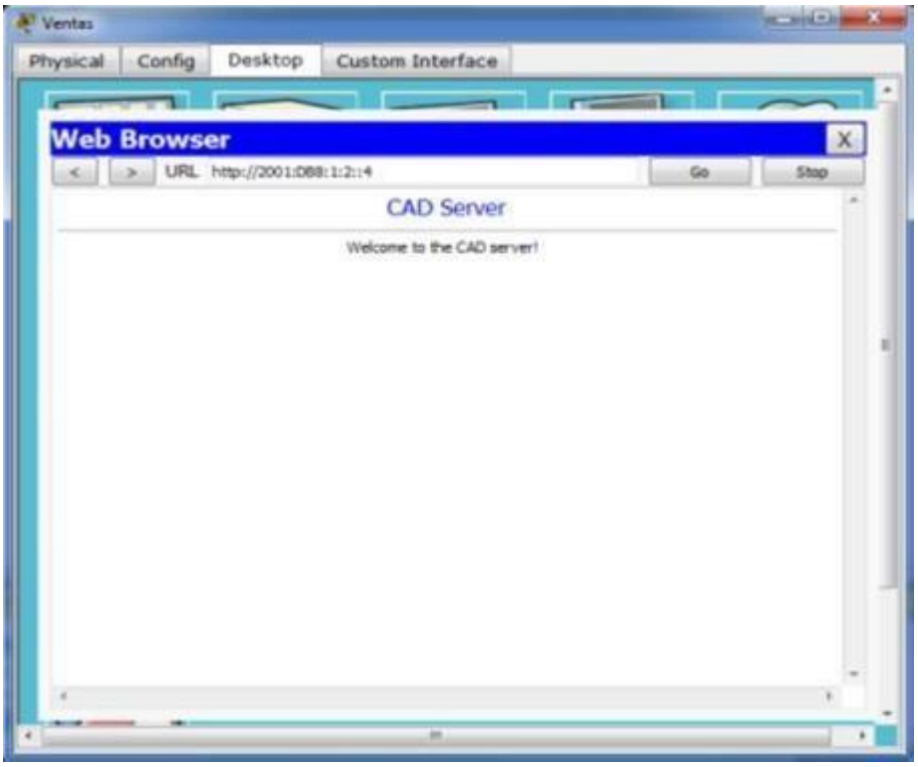
Paso 1: Abrir las páginas Web del servidor de los clientes

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.

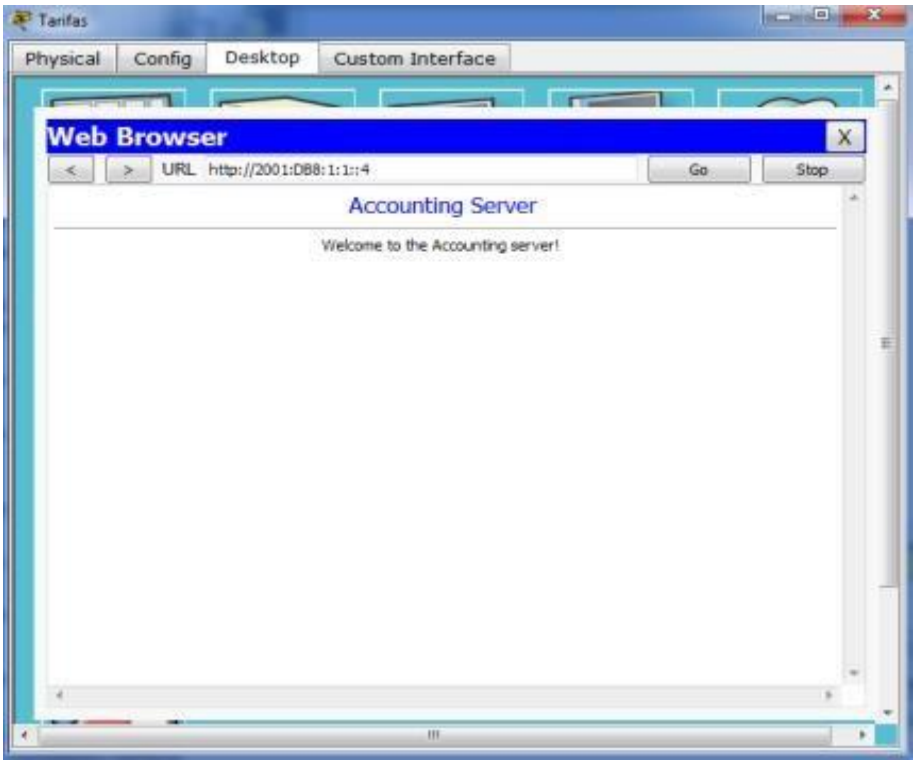


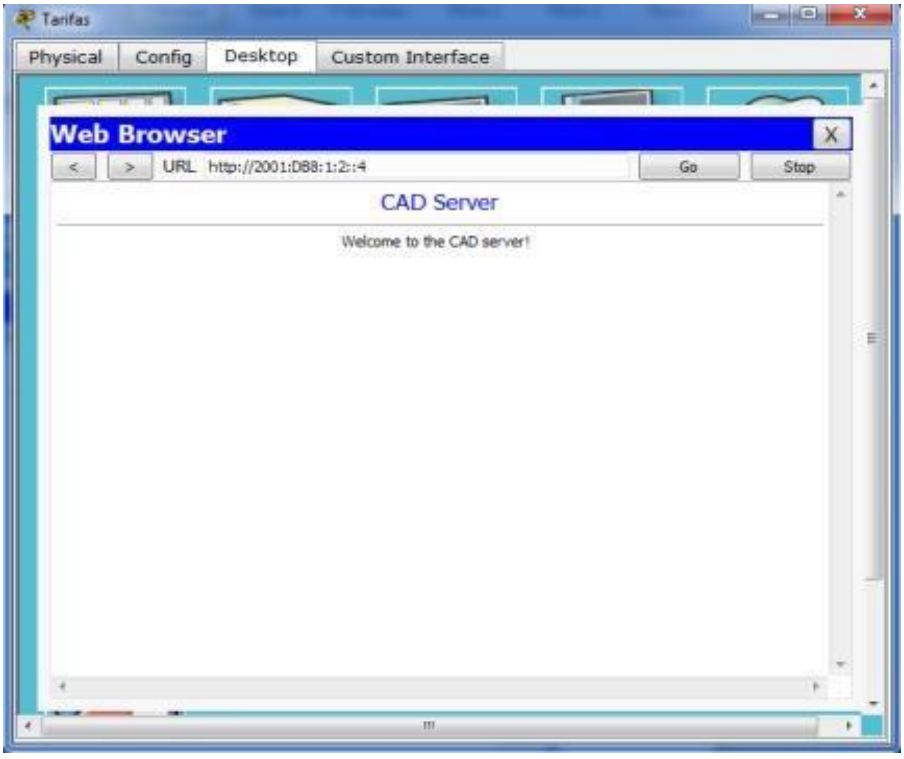
c. Introduzca 2001:DB8:1:2::4 en el cuadro de dirección URL y haga clic en Go. Debería aparecer el sitio Web de CAD.



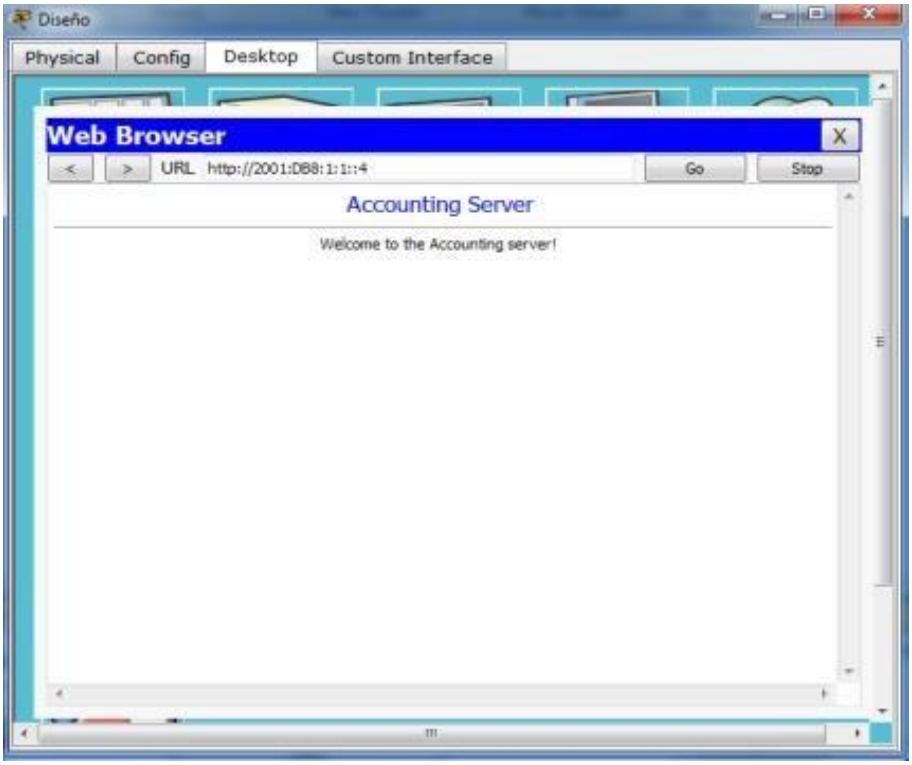
d. Repita los pasos 1a a 1d para el resto de los clientes.

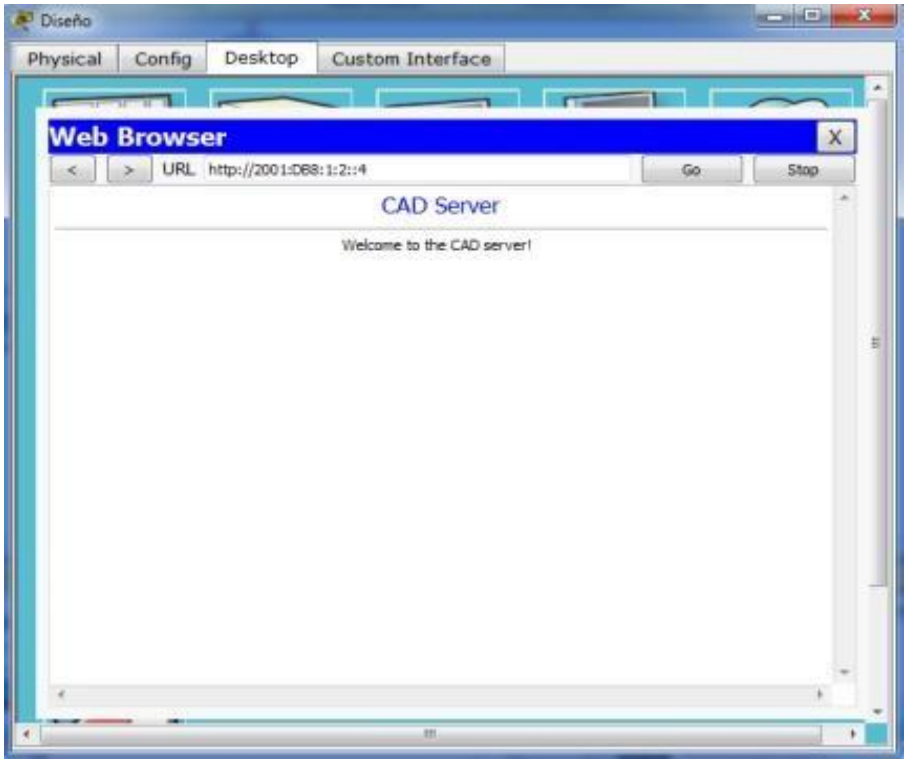
Tarifas



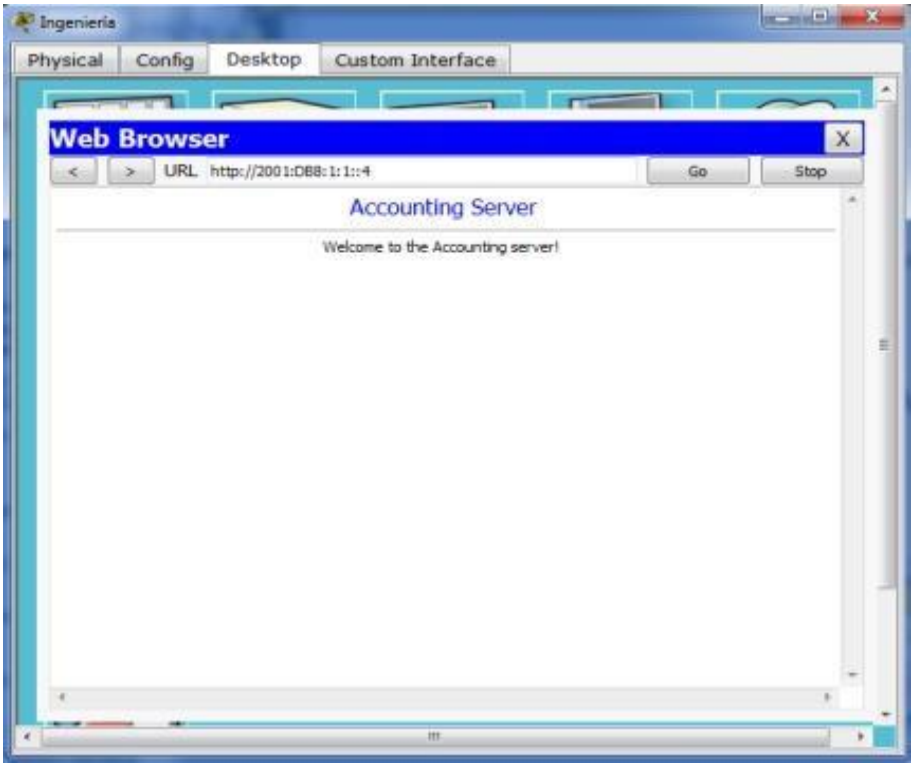


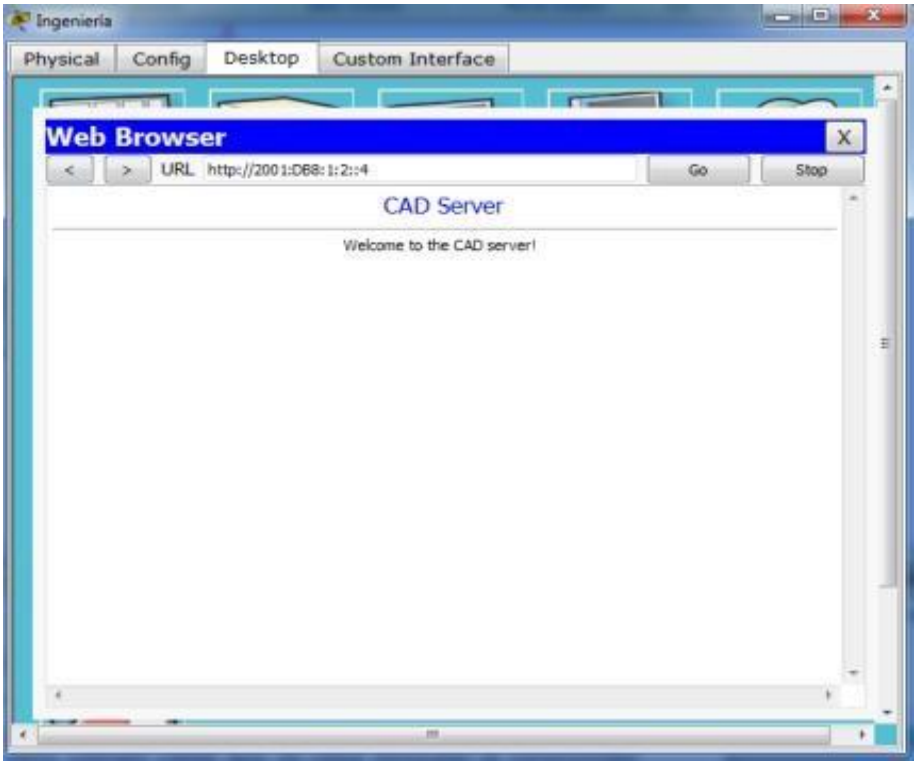
Diseño


Diseño
Physical
Config
Desktop
Custom Interface
Web Browser
X
URL http://2001:DB8:1:1::4
Go
Stop
Accounting Server
Welcome to the Accounting server!


Diseño
Physical
Config
Desktop
Custom Interface
Web Browser
X
URL http://2001:DB8:1:2::4
Go
Stop
CAD Server
Welcome to the CAD server!

Ingeniería





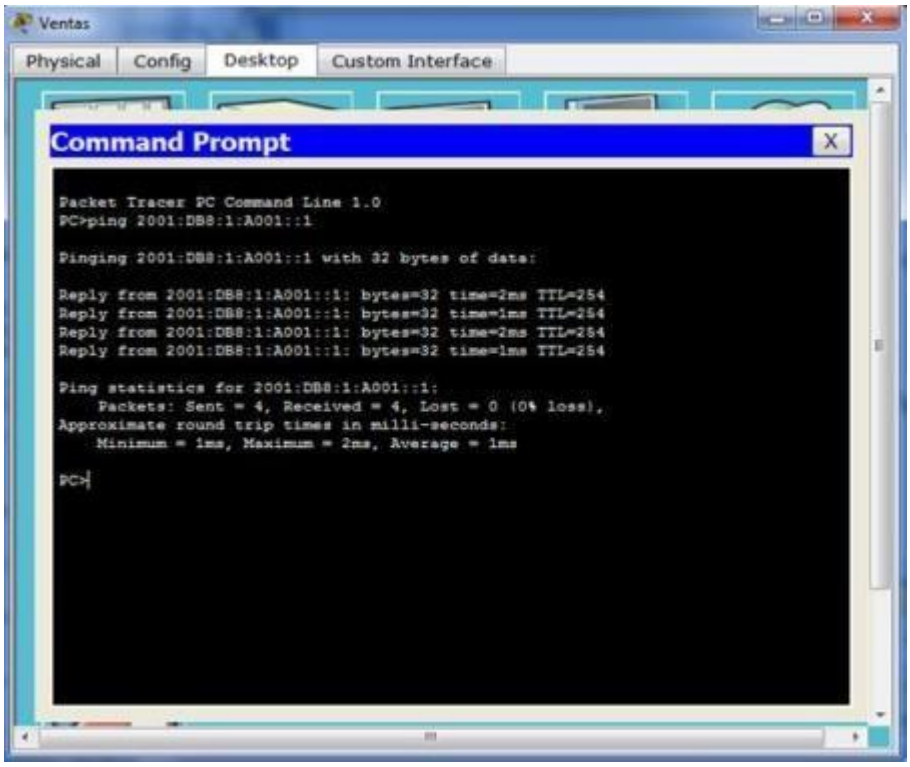
Paso 2: Hacer ping al ISP

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).

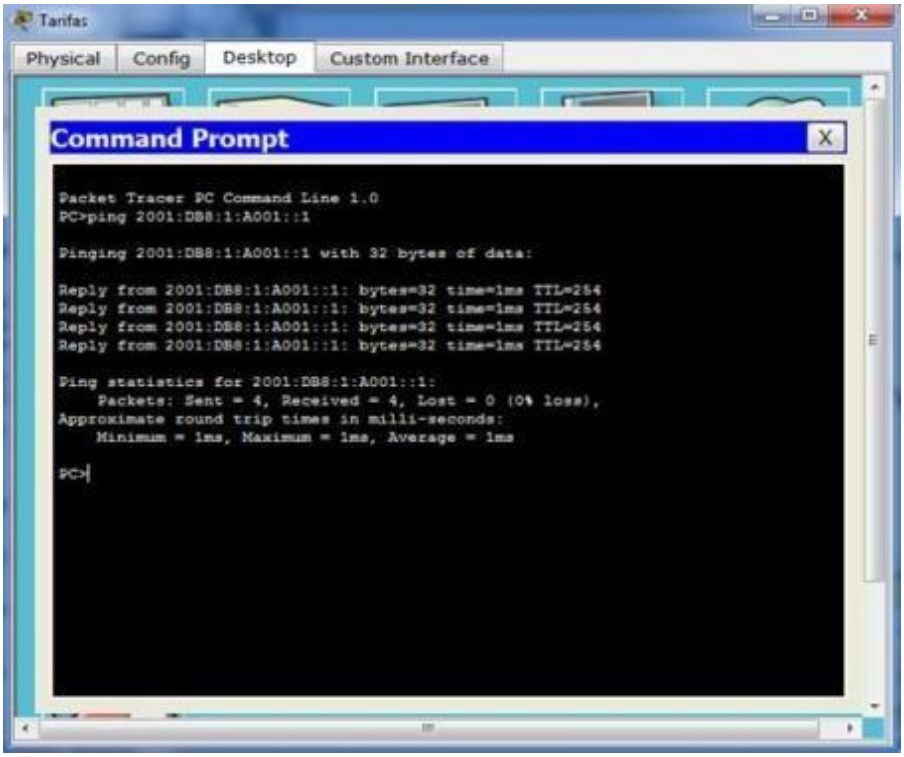
c. Pruebe la conectividad al ISP con el siguiente comando:

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

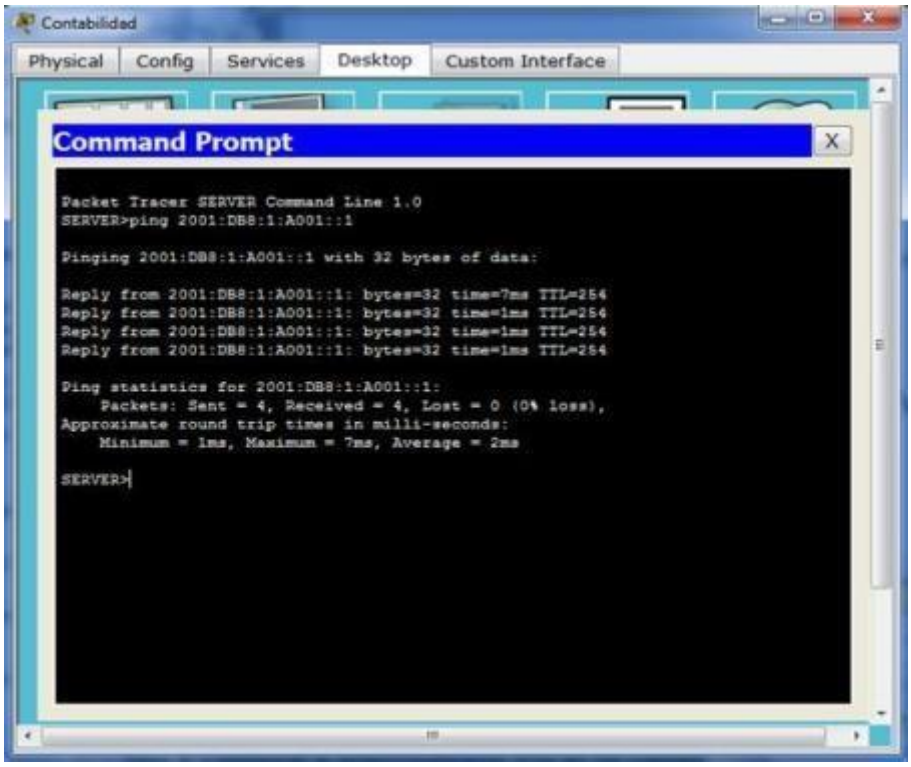


d. Repita el comando ping con otros clientes hasta que se haya verificado la conectividad completa.

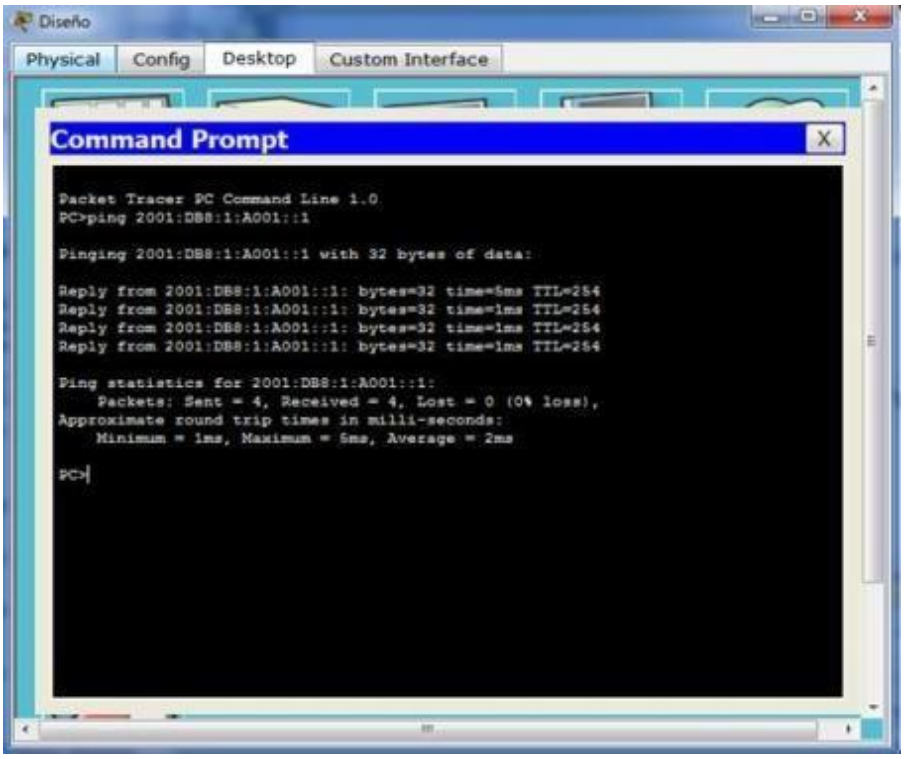
Tarifas



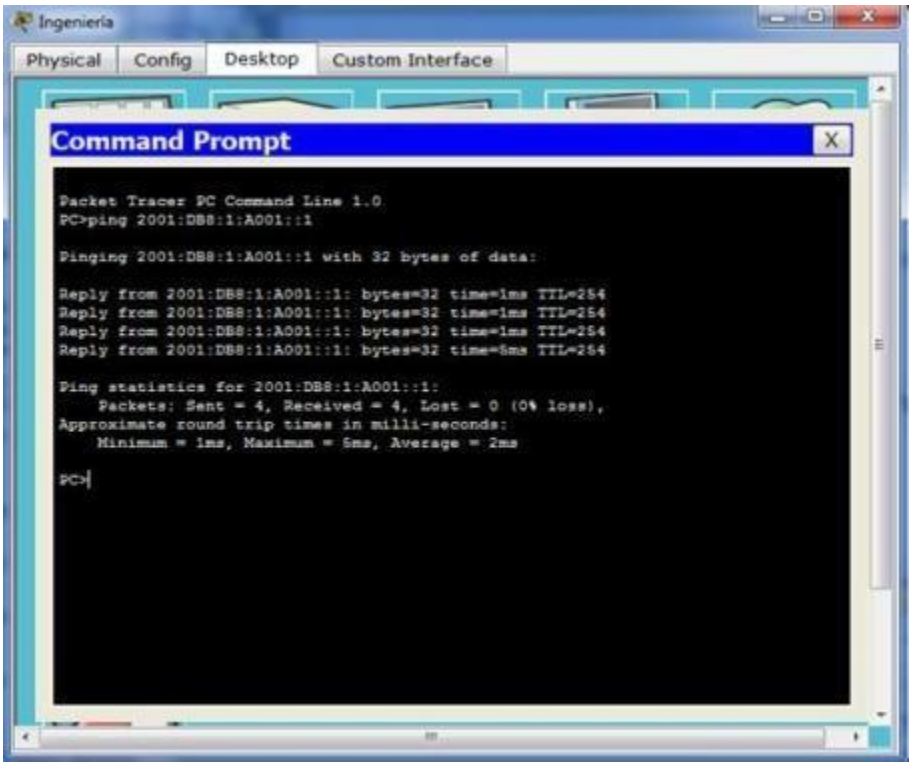
Contabilidad



Diseño



Ingeniería



CAD

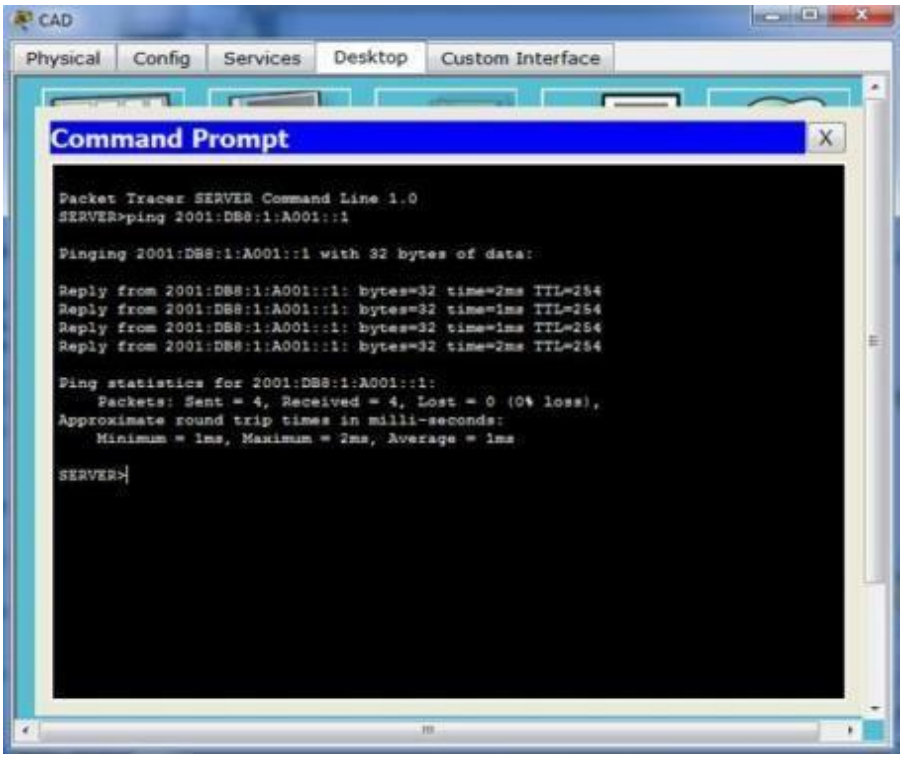
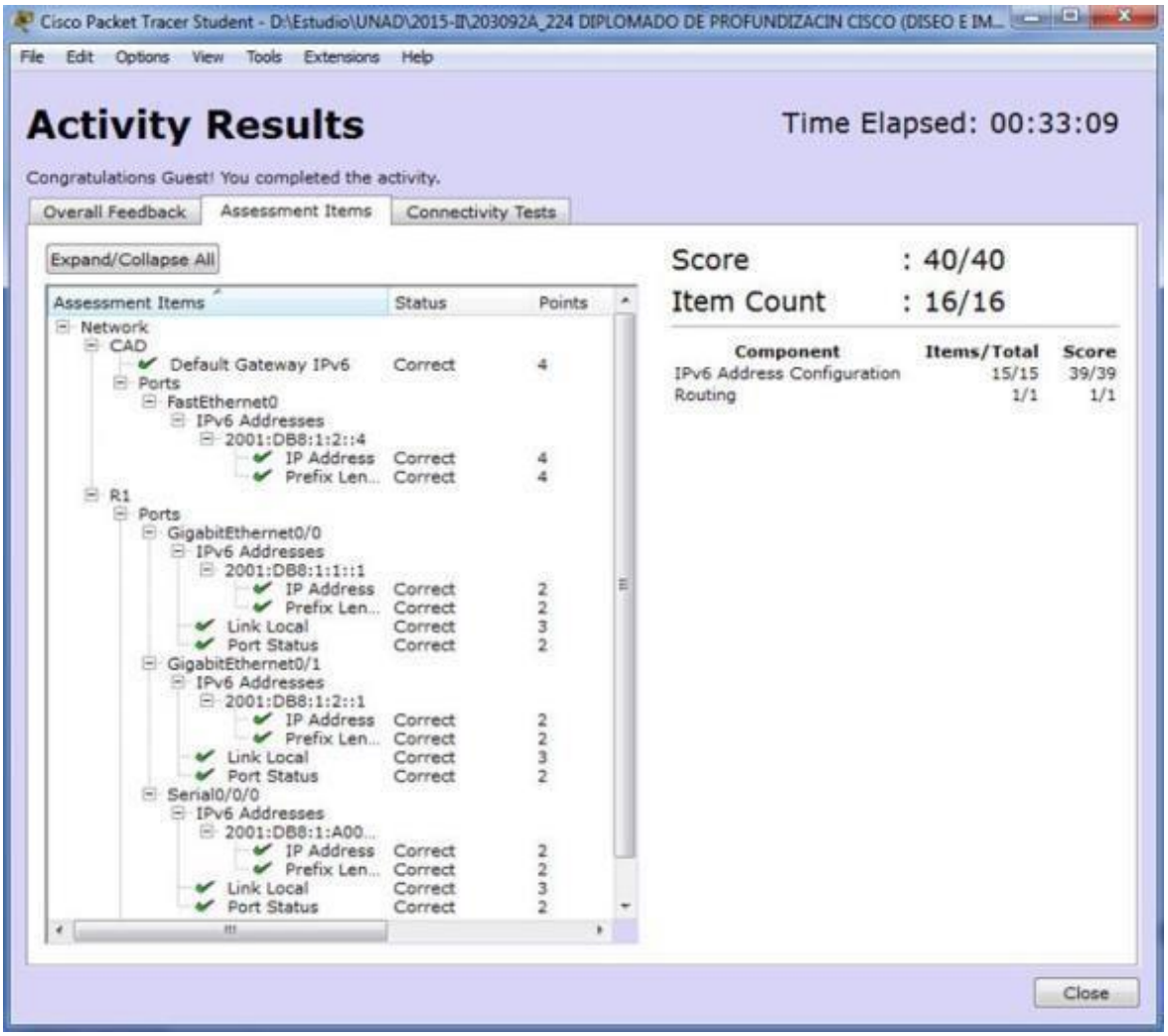


Tabla de la actividad:



8.3.2.5 Verificación del direccionamiento IPv4 e IPv6

Topología

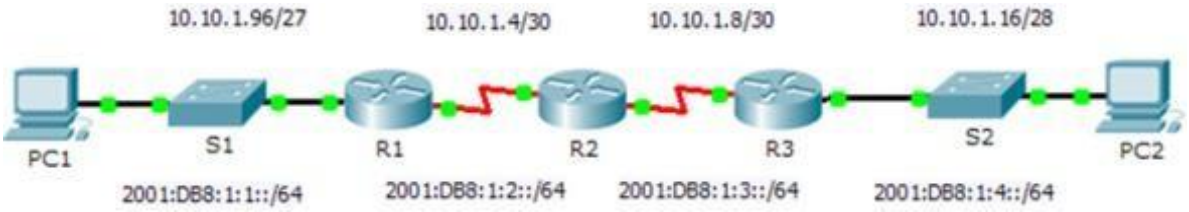


Tabla de direccionamiento

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

Objetivos

Parte 1: Completar la documentación de la tabla de direccionamiento
Parte 2: Probar la conectividad mediante el comando ping
Parte 3: Descubrir la ruta mediante su rastreo

Información básica

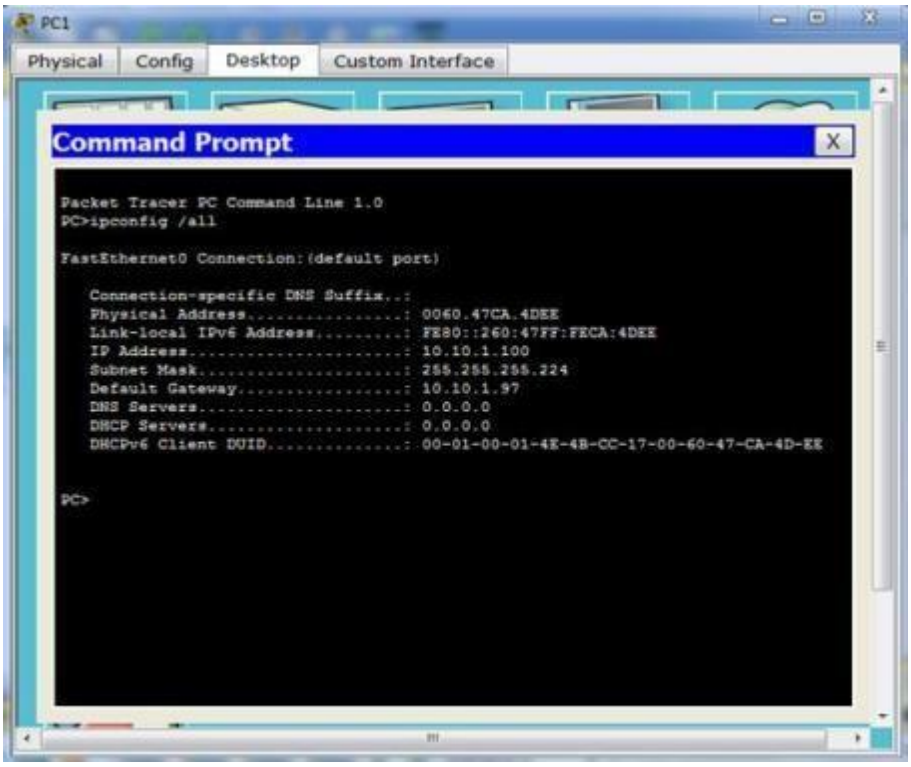
La técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. En esta actividad, investigará la implementación de una técnica dual-stack incluidos la documentación de la configuración de IPv4 e IPv6 para dispositivos finales, la prueba de conectividad para IPv4 e IPv6 mediante el comando ping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

Parte 1: Completar la documentación de la tabla de direccionamiento

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

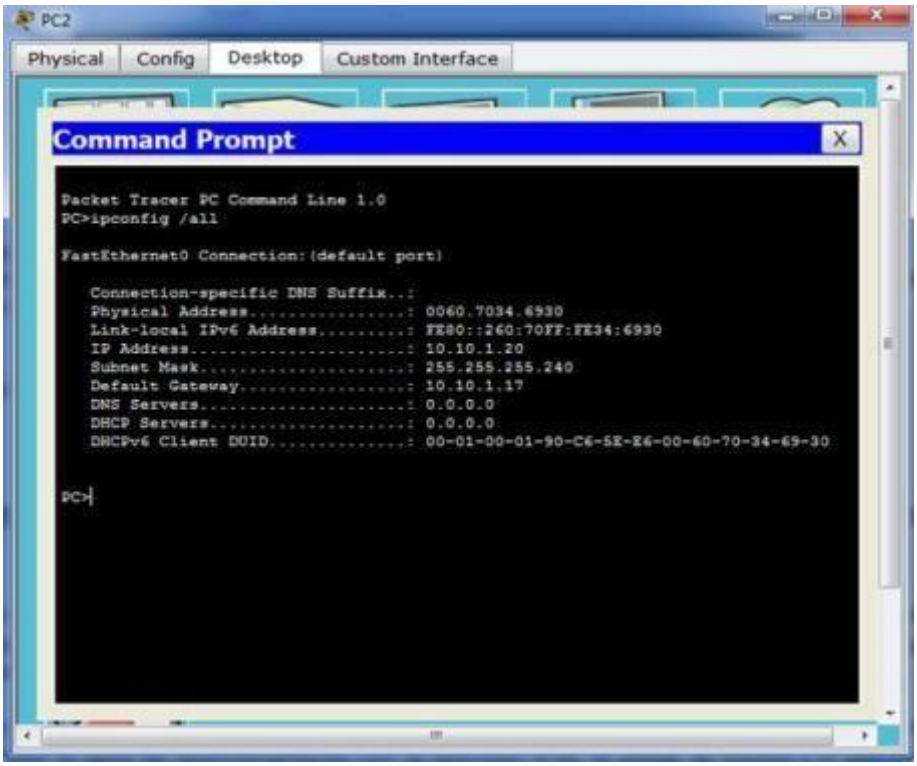
a. Haga clic en PC1 y, a continuación, haga clic en la ficha Desktop > Command Prompt (Escritorio > Símbolo del sistema).

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



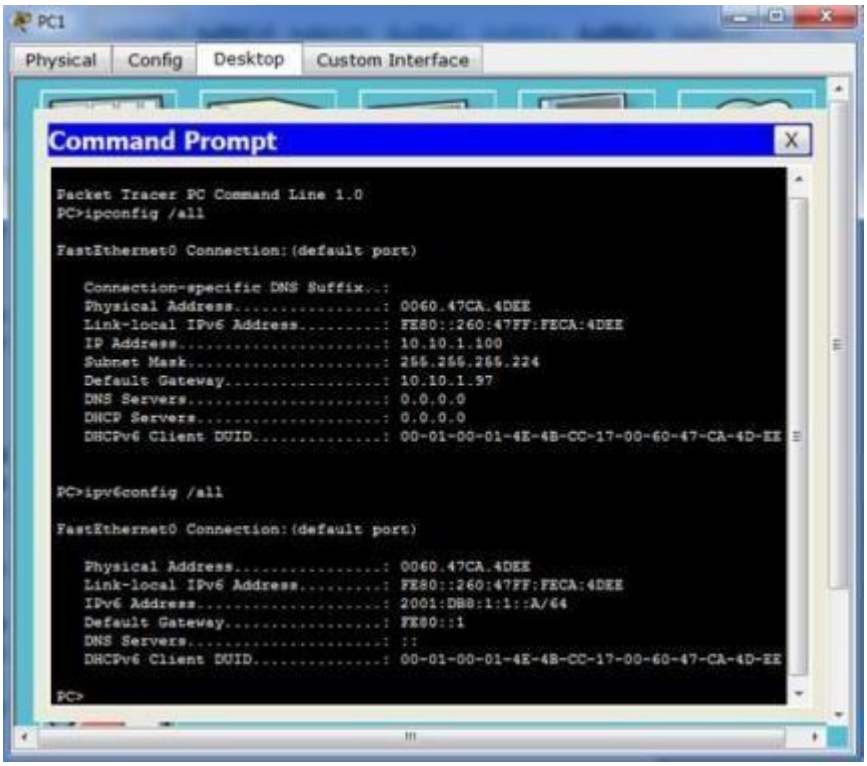
c. Haga clic en PC2 y, a continuación, haga clic en la ficha Desktop > Command Prompt.

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.

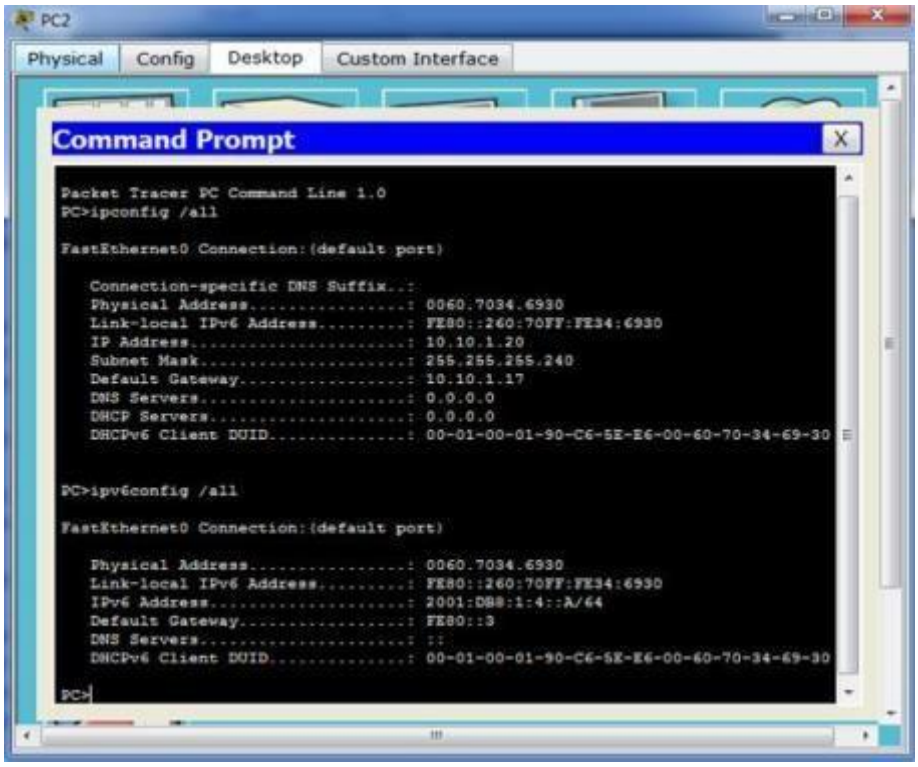


Paso 2: Usar el comando ipv6config para verificar el direccionamiento IPv6

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



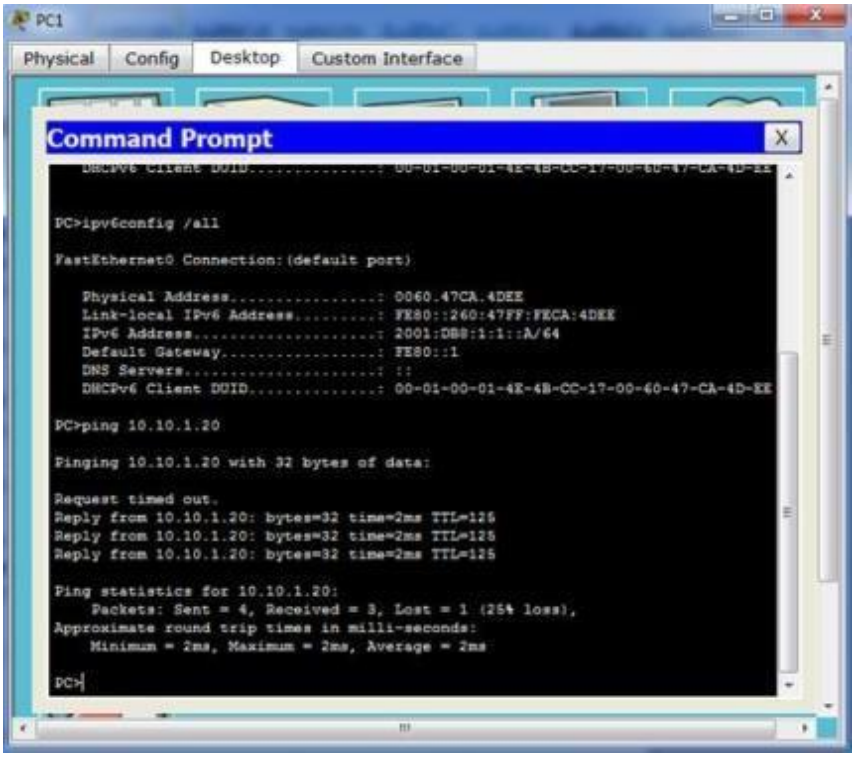
b. En la PC2, introduzca el comando ipv6config /all para recopilar la información de IPv6. Complete la tabla de direccionamiento con la dirección IPv6, el prefijo de subred y el gateway predeterminado.



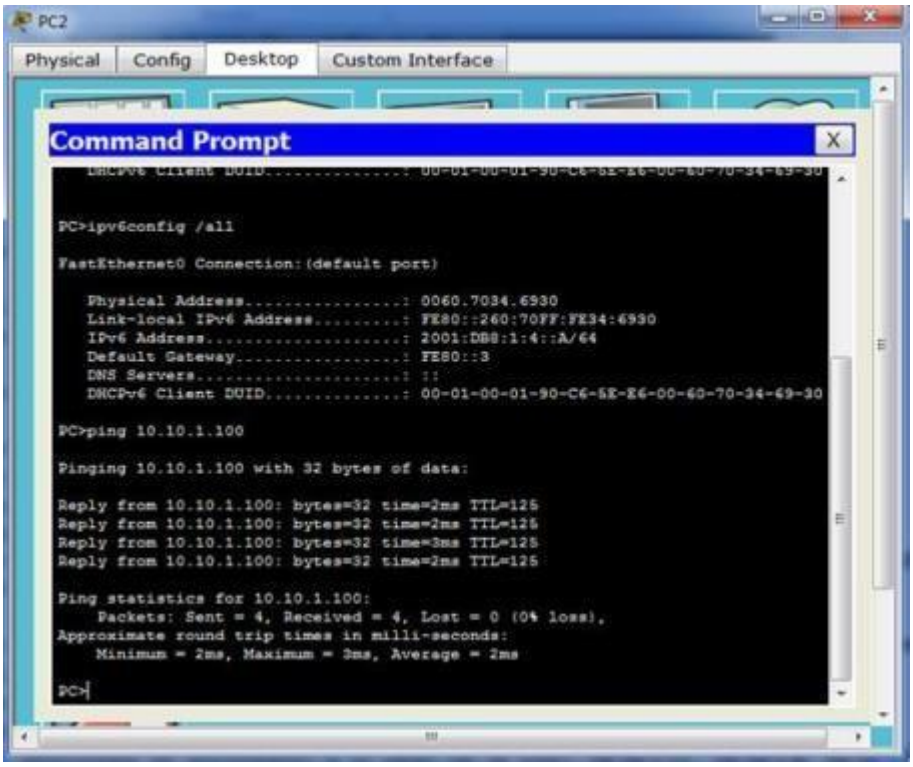
Parte 2: Probar la conectividad mediante el comando ping

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

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

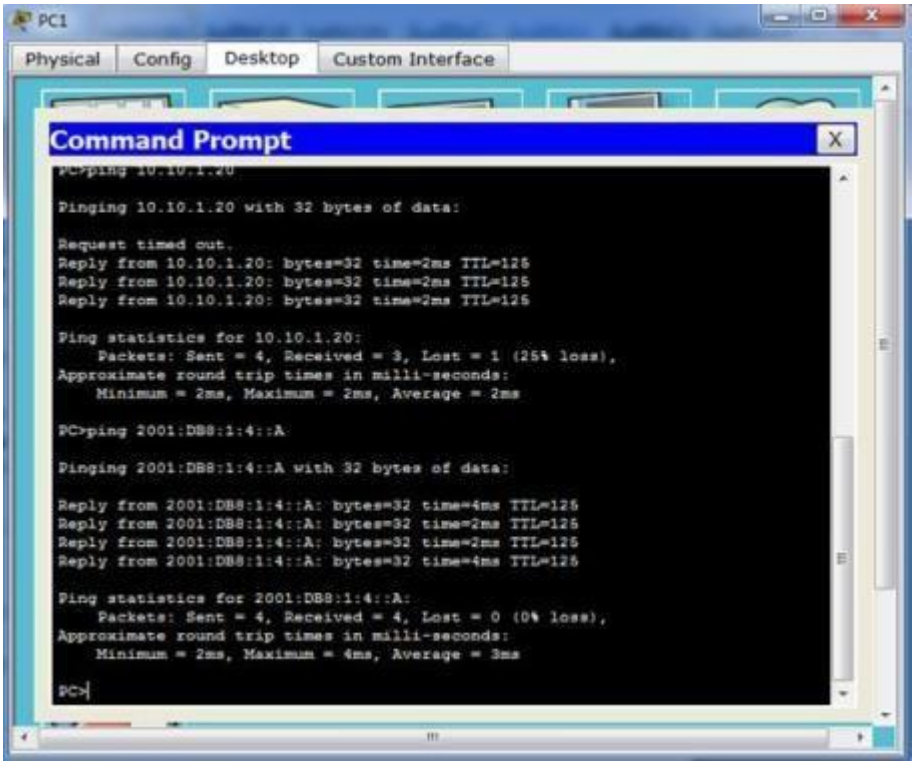


b. Desde la PC2, haga ping a la dirección IPv4 de la PC1. ¿El resultado fue satisfactorio? **Sí**

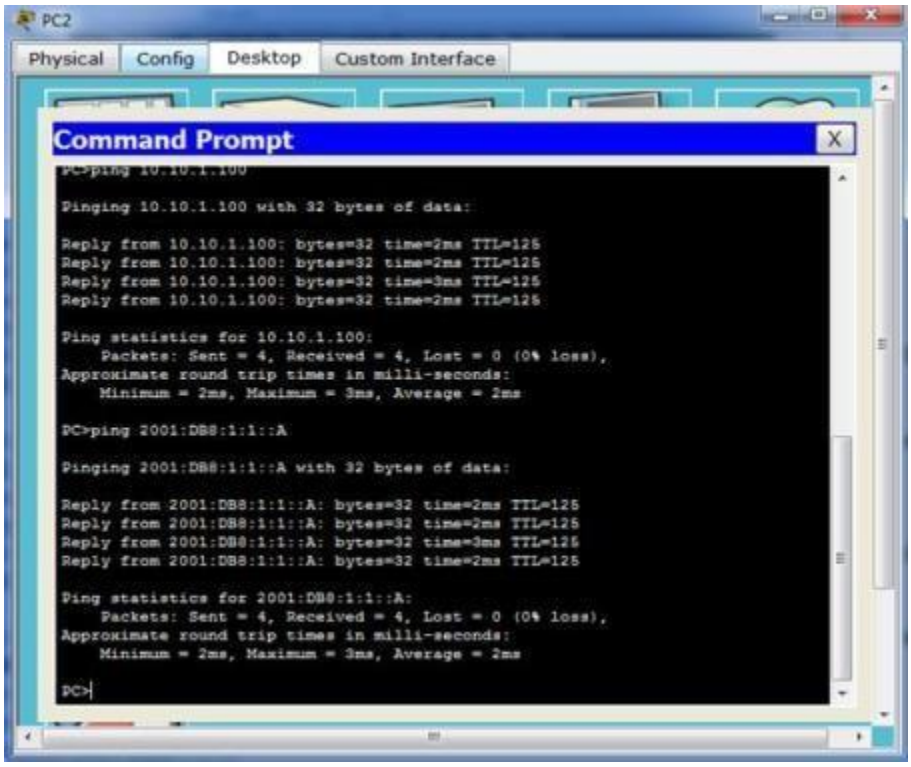


Paso 2: Usar el comando ping para verificar la conectividad IPv6

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



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



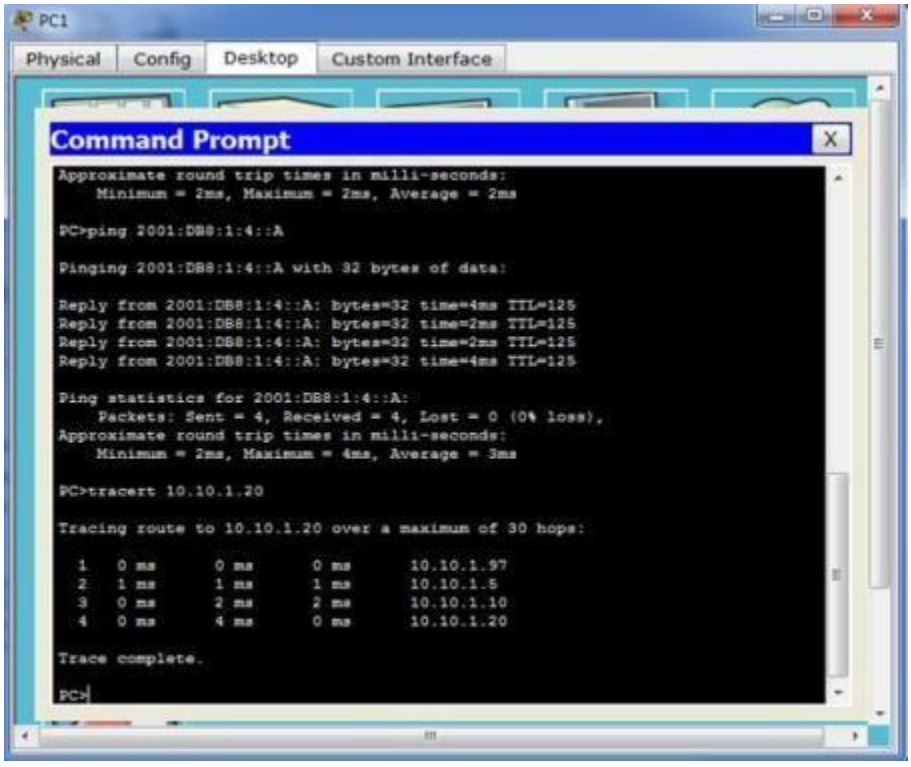
Parte 3: Descubrir la ruta mediante su rastreo

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

¿Qué direcciones se encontraron a lo largo de la ruta? **10.10.1.97, 10.10.1.5, 10.10.1.10, 10.10.1.20**

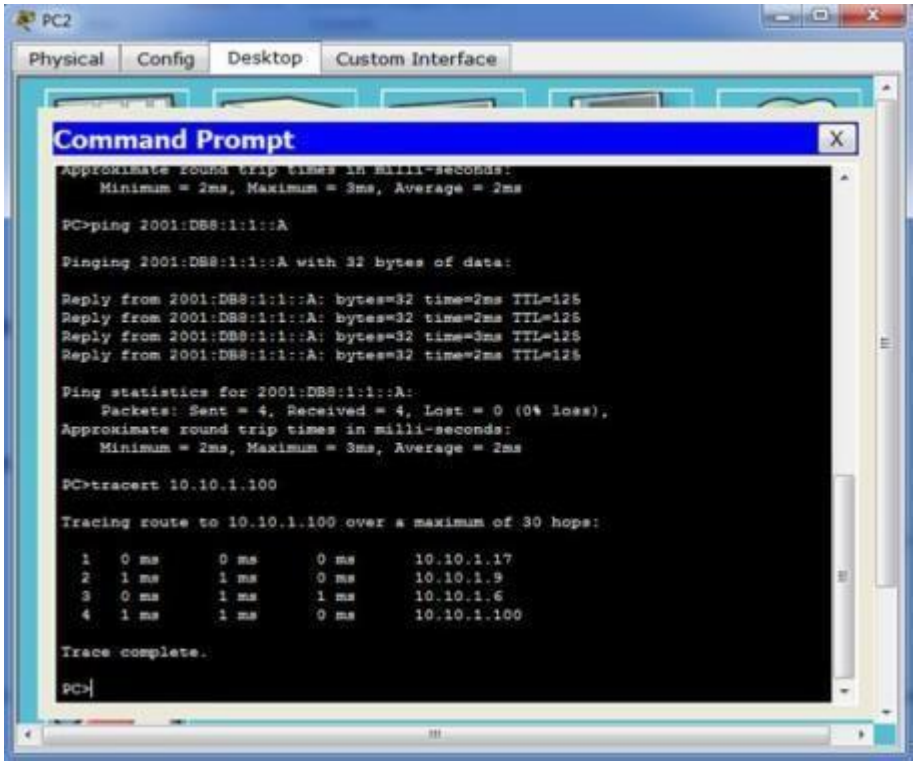


¿Con qué interfaces se asocian las cuatro direcciones? **G0/0 del R1, S0/0/0 en el R2, S0/0/01 en el R3, NIC de la PC2**

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

PC> tracert 10.10.1.100

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



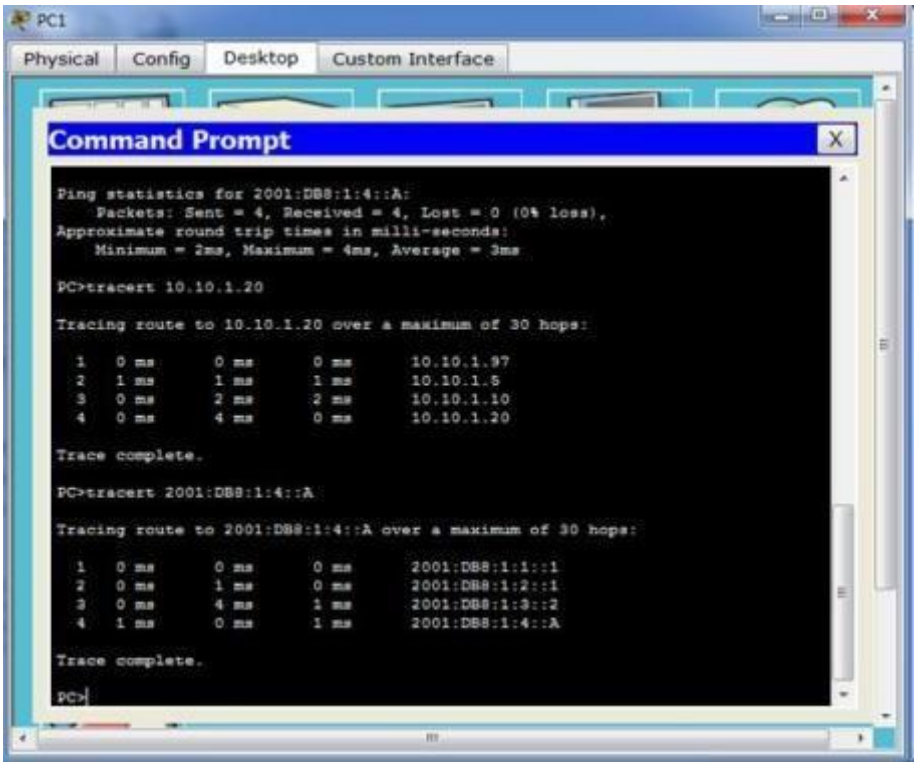
¿Con qué interfaces se asocian las cuatro direcciones? **G0/0 del R3, S0/0/1 del R2, S0/0/1 del R1, NIC de la PC1**

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

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

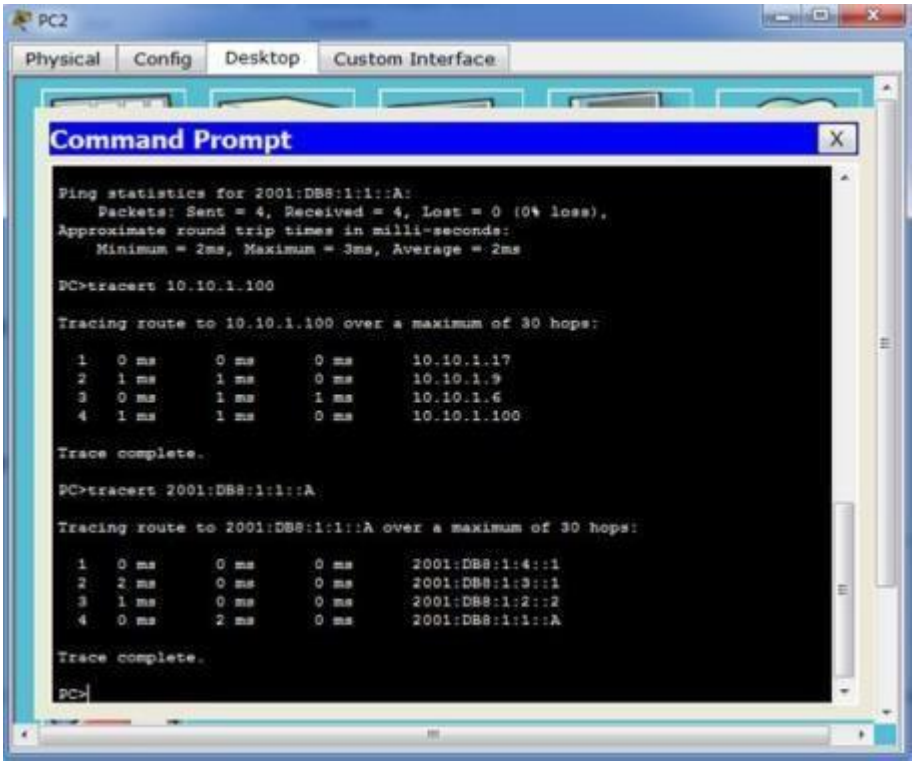


¿Con qué interfaces se asocian las cuatro direcciones? **G0/0 del R1, S0/0/0 del R2, S0/0/1 del R3, NIC de la PC2**

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

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

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



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

Tabla de la actividad:

COMCLUSION

- Con la realización de los laboratorios se afianzo el conocimiento en cuanto a configuración de claves de usuario básico y privilegiado para la configuración de dispositivos.

- Se logra realizar la configuración básica de un Router y un Switch.

- Se logra generar tráfico de red en modo de simulación y examinar la funcionalidad de los protocolos TCP y UDP.

- Se logra examinar el comportamiento de unicast, broadcast y multicast.

- 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.

- Se aprende a configurar el direccionamiento IPv6 en el router, en los servidores, en los clientes para así probar y verificar la conectividad de la red.

- Se prueba el direccionamiento IPv4 e IPv6 mediante el comando ping.

- Se logra conocer la ruta mediante su rastreo a través del comando tracert.

Bibliografía

Academy, C. N. (s.f.). *Cisco Packt Tracer student*. Recuperado el 26 de Septiemvre de 2015, de https://www.netacad.com

campus-UNAD. (2015). Recuperado el 28 de Septiembre de 2015, de http://66.165.175.209/campus17_20152/course/view.php?id=19

campus-UNAD Guía Integrada de Actividades. (s.f.). Recuperado el 25 de Septiembre de 2015, de http://66.165.175.209/campus17_20152/course/view.php?id=19#

Cisco Networking Academy. (s.f.). Recuperado el 15 de Septiembre de 2015, de https:ww.netacad.com