Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 3 - Comunicación entre dos redes LAN

Introducción a las redes de computadoras

Ingeniería en Desarrollo de Software

Tutor: Marco Alonso Rodríguez

Alumno: Fernando Pedraza Garate

Fecha: 04 de Septiembre del 2022

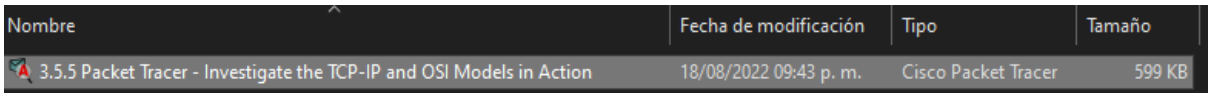
Índice

Introducción

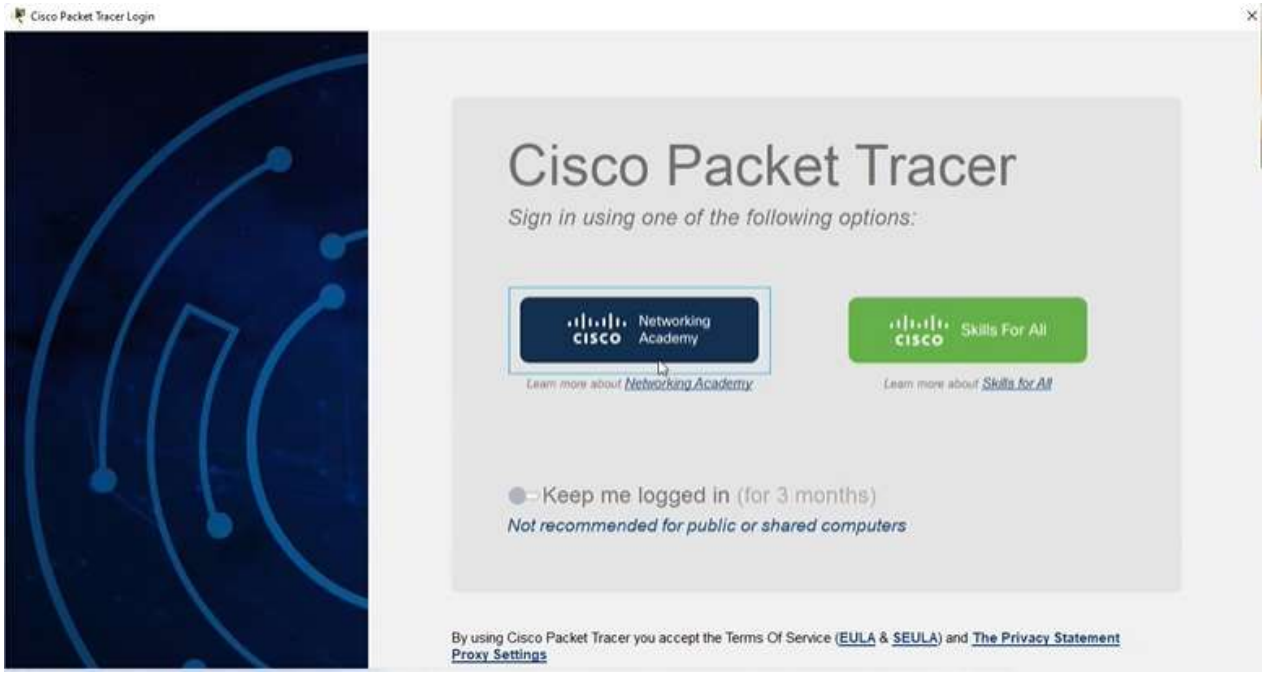
Esta actividad tiene como objetivo simular y comprender los protocolos TCP/IP y su relación con el modelo OSI, de tal modo que permita ver el contenido de los datos que se envían en la red a través de la capa.

Se deberá de realizar una simulación de un servidor web y un cliente web utilizando el modelo TCP/IP, donde se analizará el proceso de envío de información y comunicación entre el Servidor y la PC respondiendo algunas preguntas.

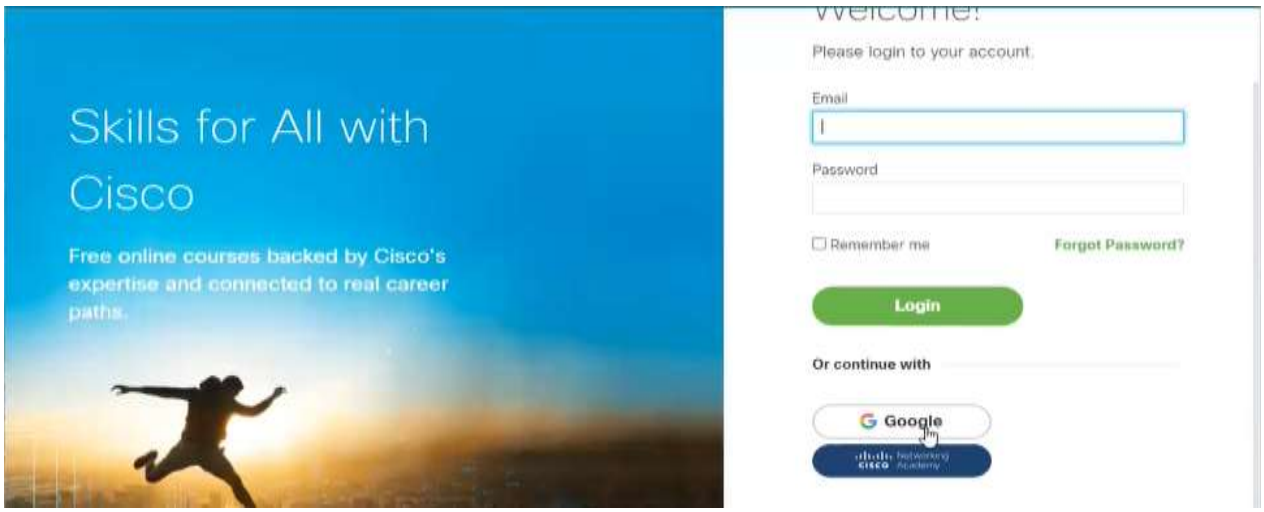
Capturas de pantalla



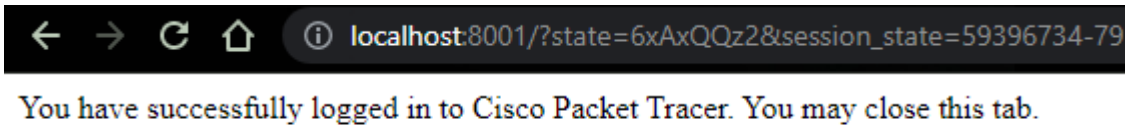
Programa descargado.



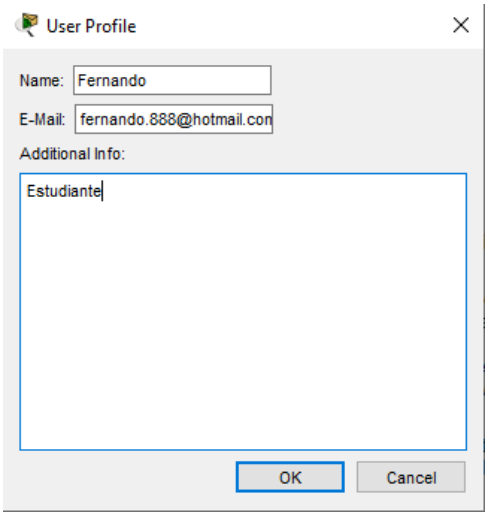
Al abrir nos solicita registrarnos en Cisco de alguna de sus dos alternativas.



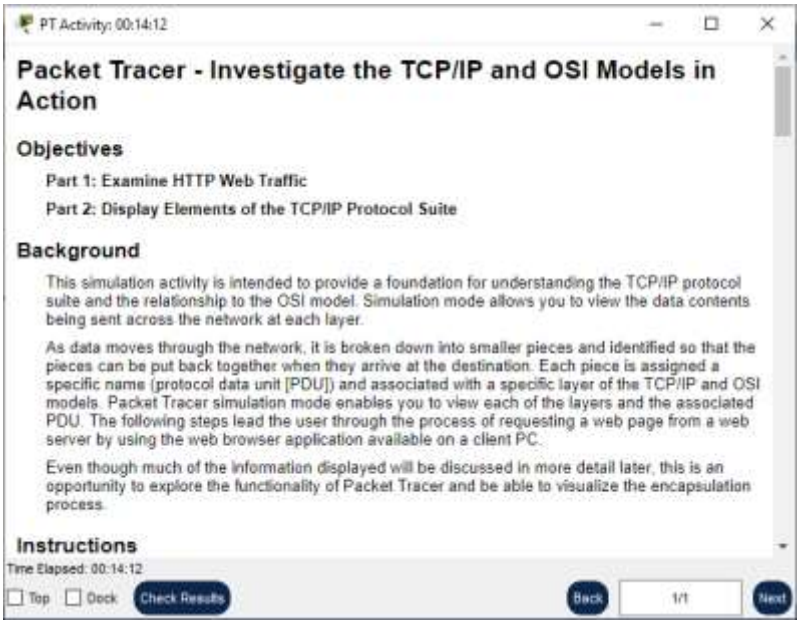
Nos registramos con cualquiera de las opciones presentadas.



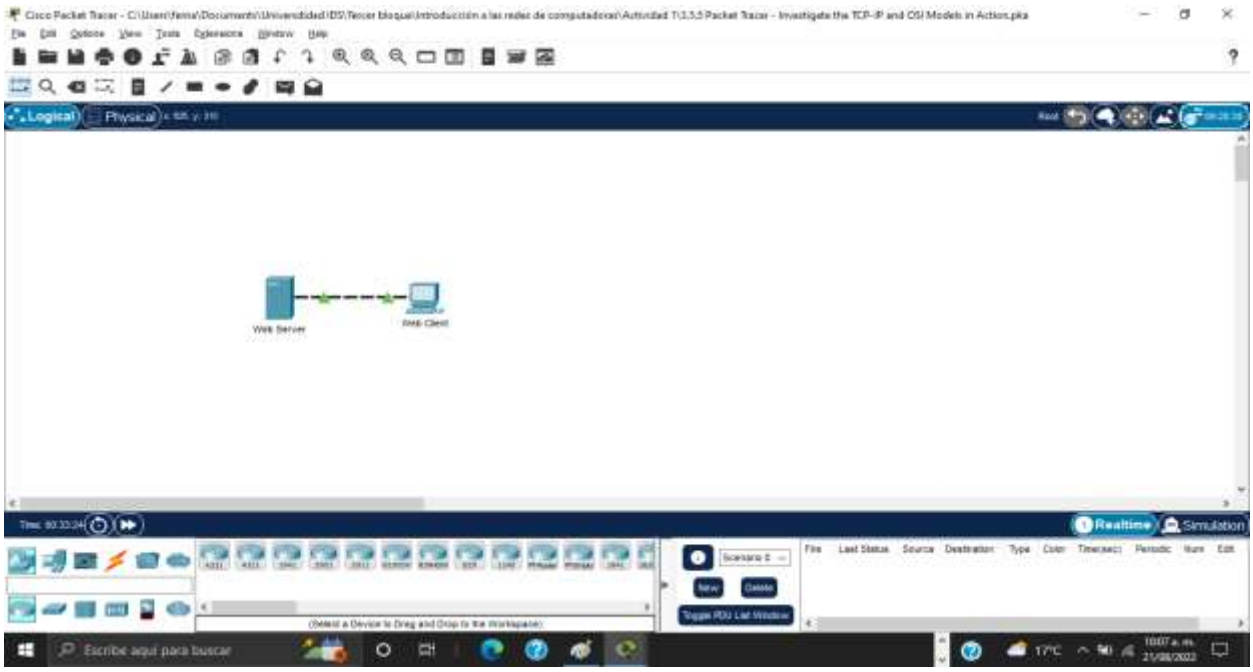
Después de registrarnos nos manda el siguiente mensaje en donde nos indica que hemos ingresado de forma exitosa.



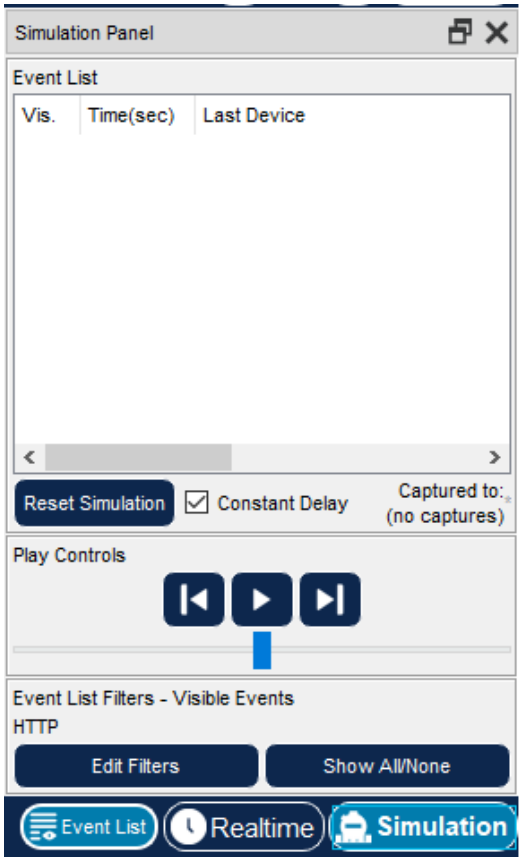
Nos aparece esta pantalla donde registramos nuestros datos para nuestra retroalimentación.



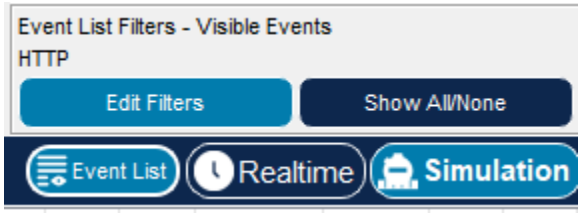
Nos muestra la pantalla de instrucciones relacionadas con la actividad.



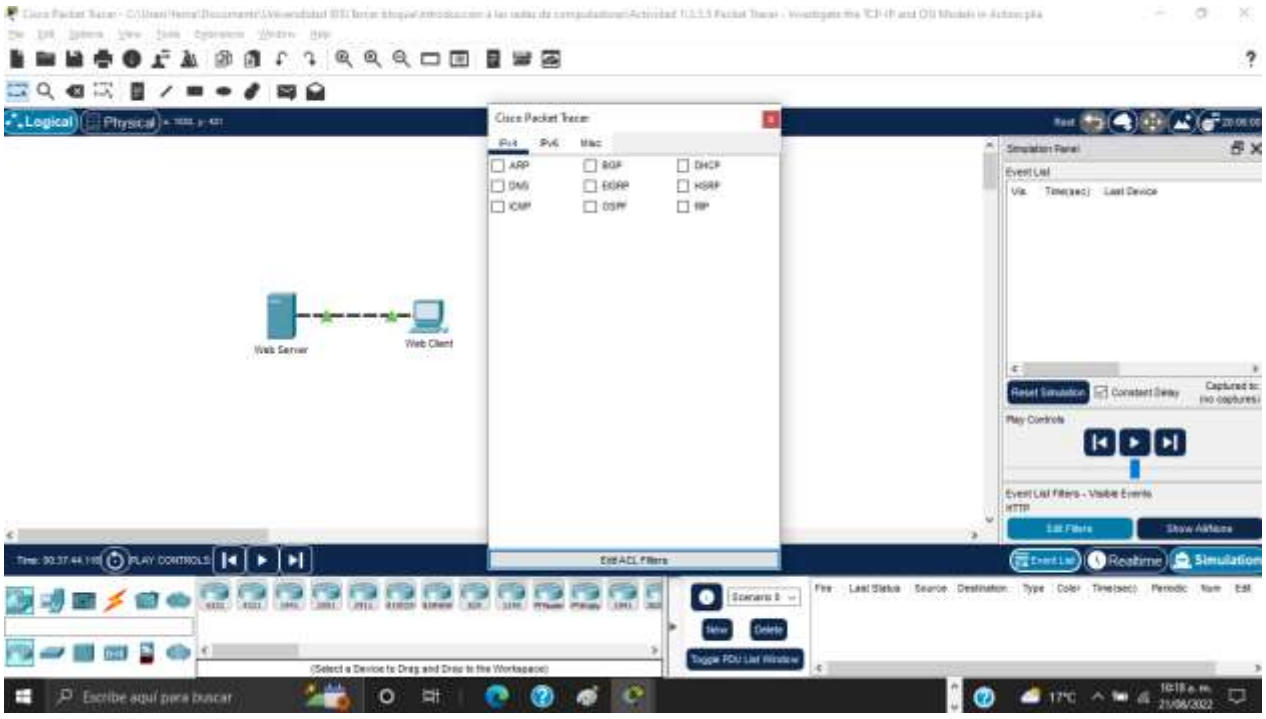
En esta pantalla de actividad cambiaremos a simulación en la parte inferior derecha.



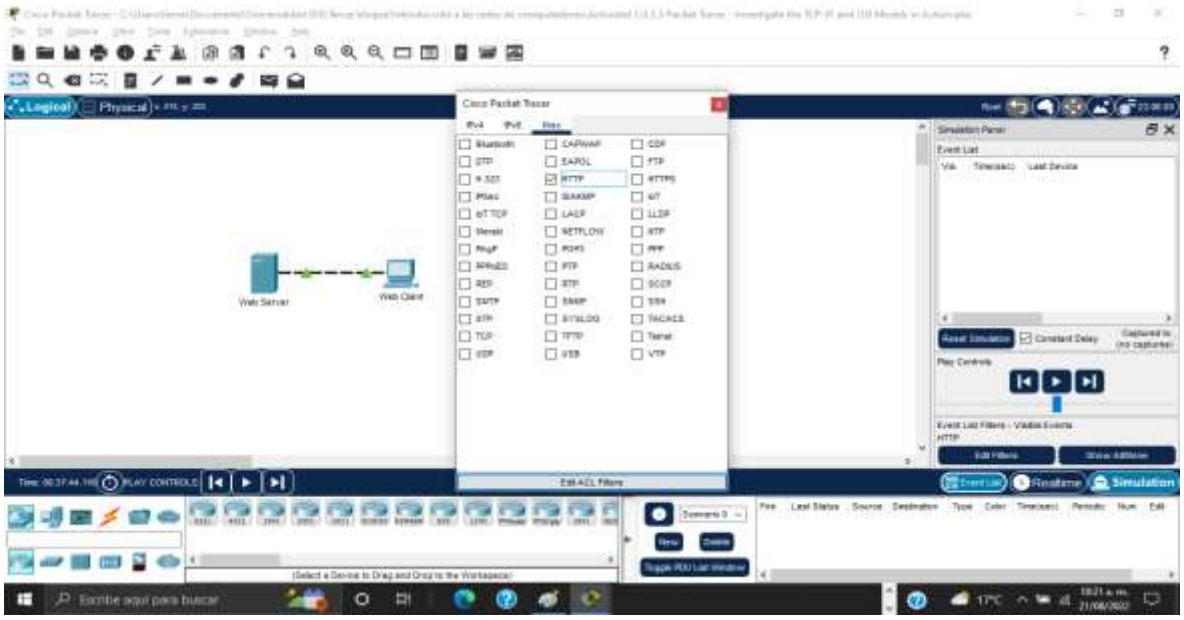
Nos muestra el panel de simulación.



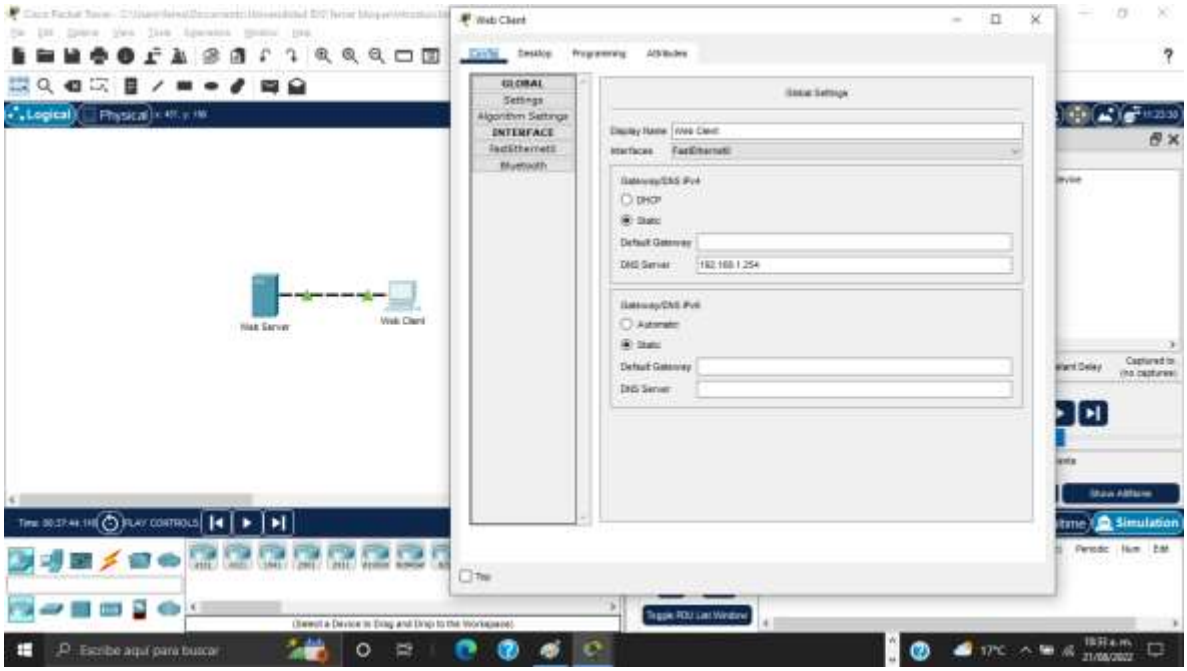
En base a la actividad nos solicita seleccionar HTTP en la lista de filtros la cual ya está predeterminada.



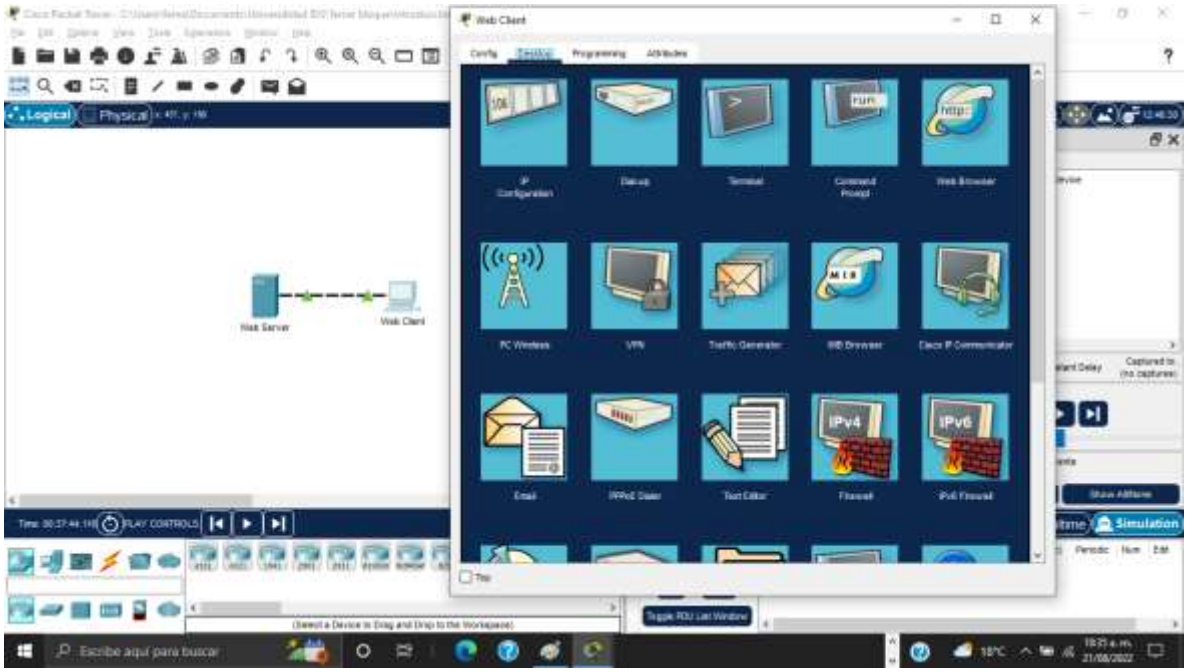
Seleccionamos edit filters y nos muestra esta pantalla, seleccionamos el apartado Misc para verificar que esta seleccionado HTTP.



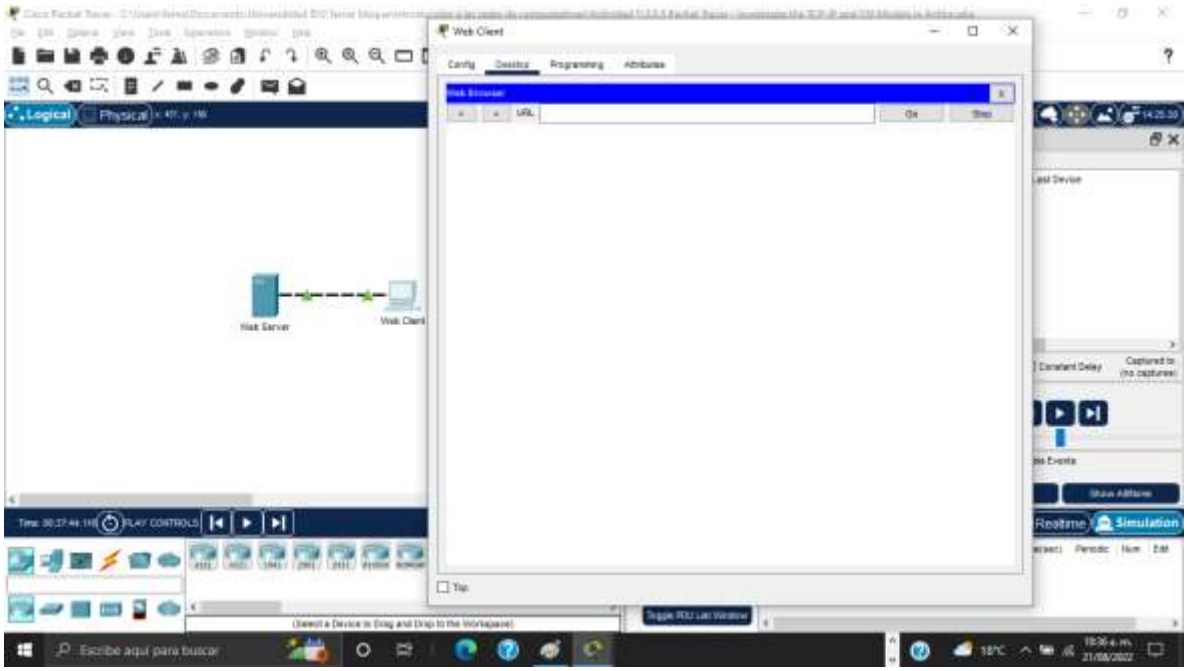
Salimos para continuar con la actividad.



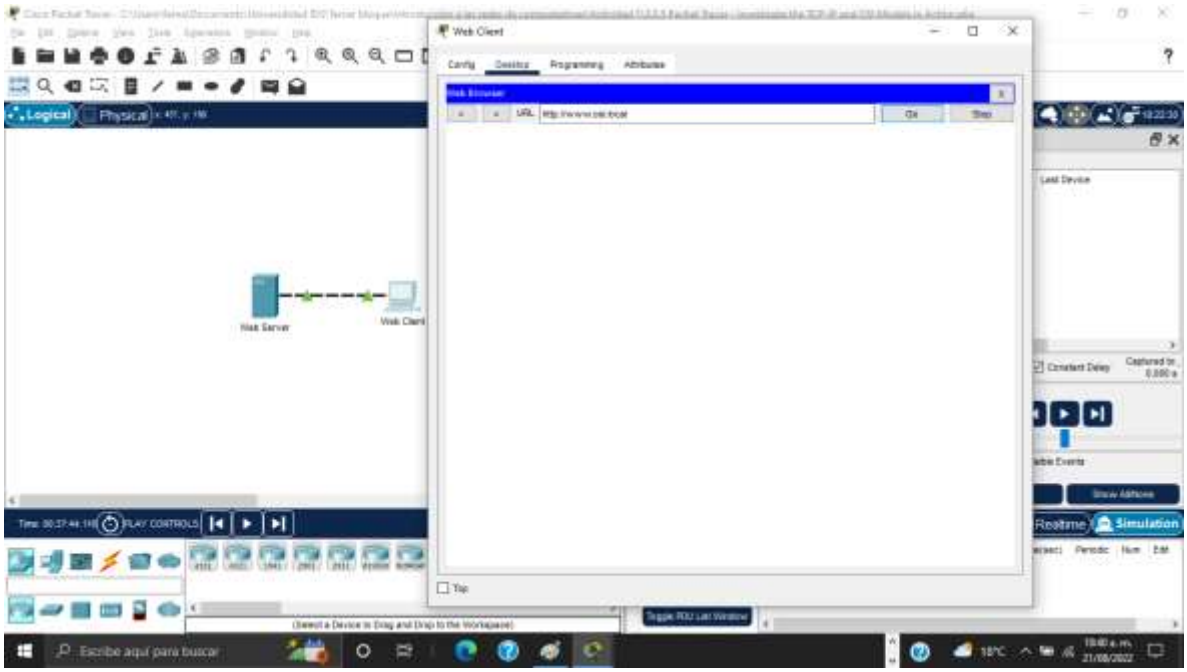
Hacemos clic en la PC de web client.



Seleccionamos Desktop y hacemos clic en el icono web browser.

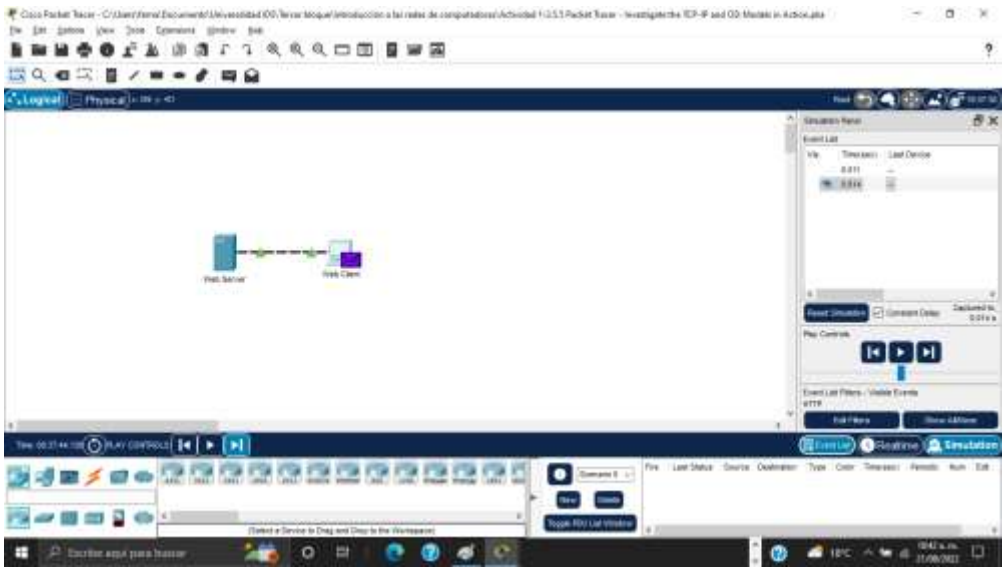


Nos muestra el navegador.

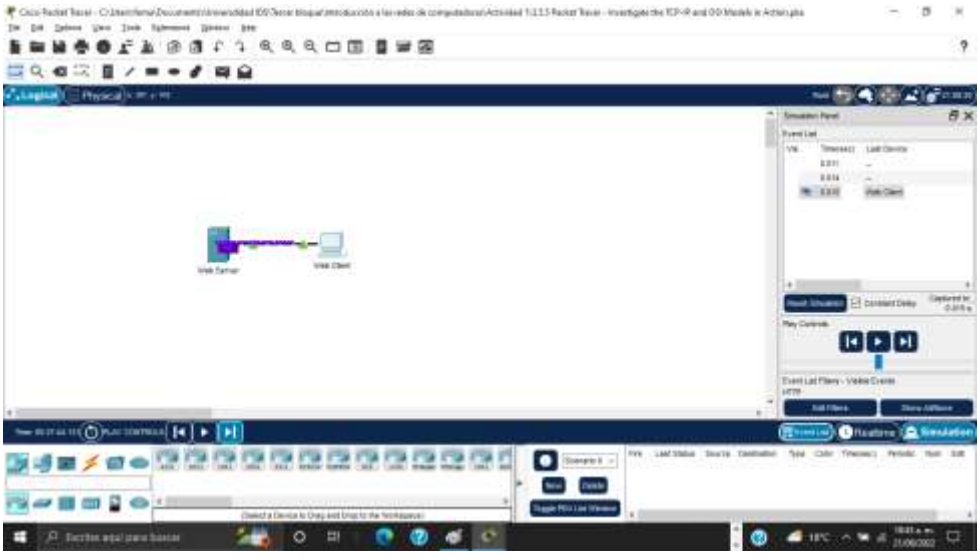


Ingresamos la dirección www.osi.local y damos clic en GO.

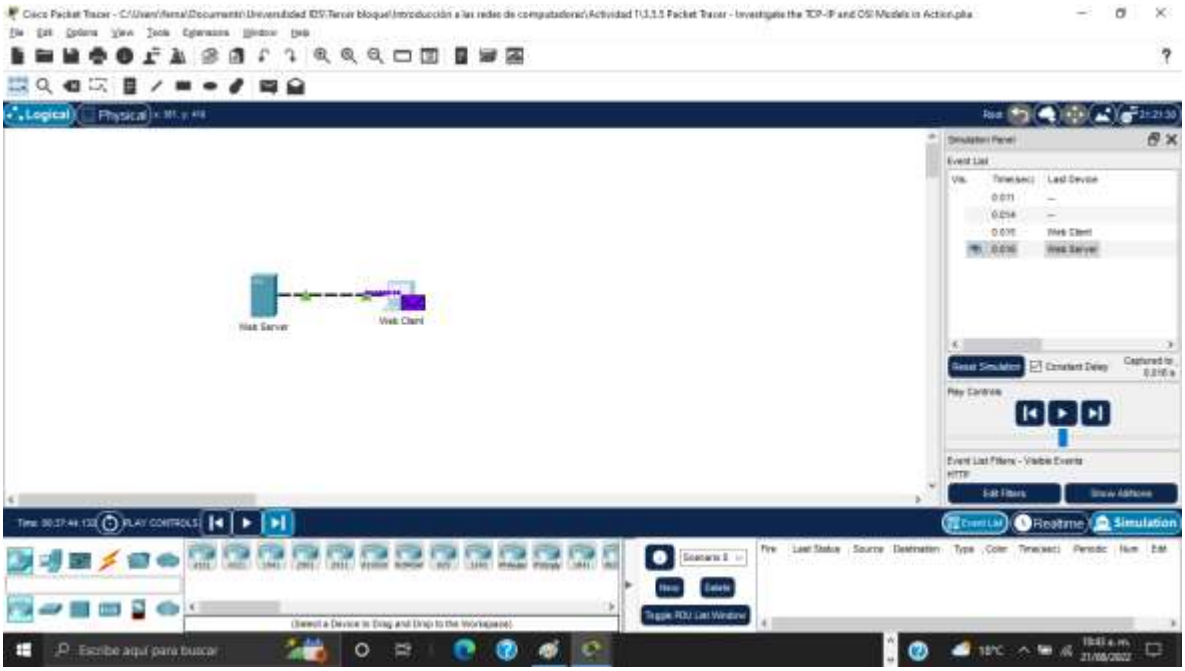
Damos clic en el botón capture then forward 4 veces.



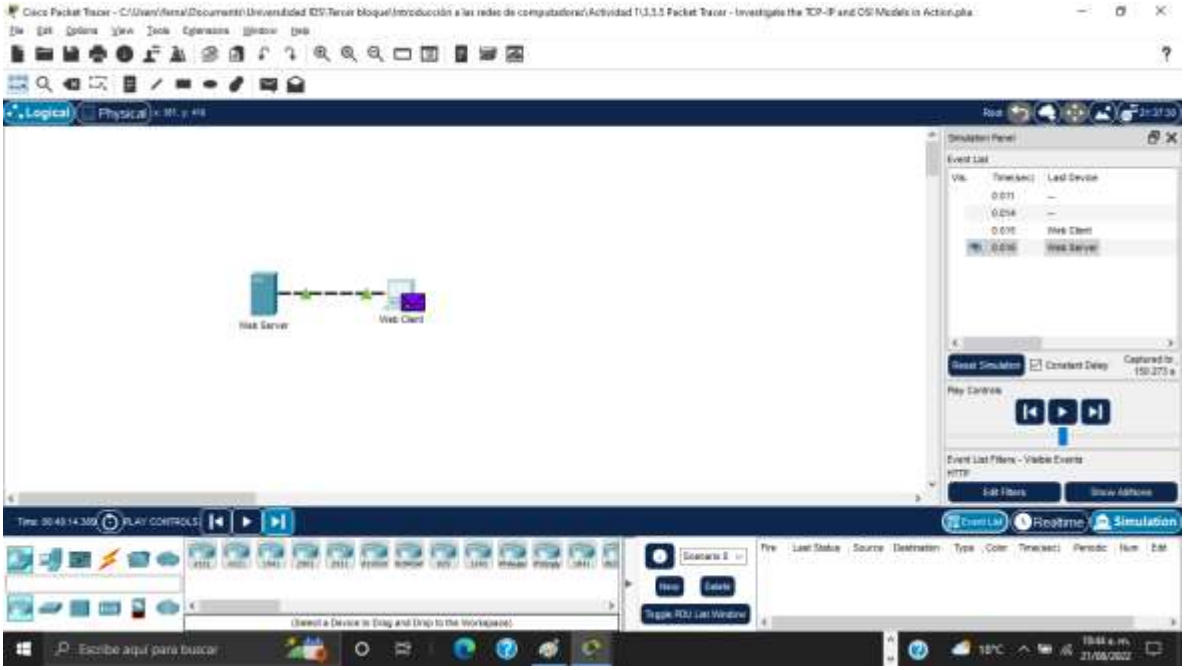
Nos muestra el recorrido de nuestra solicitud de la pc…



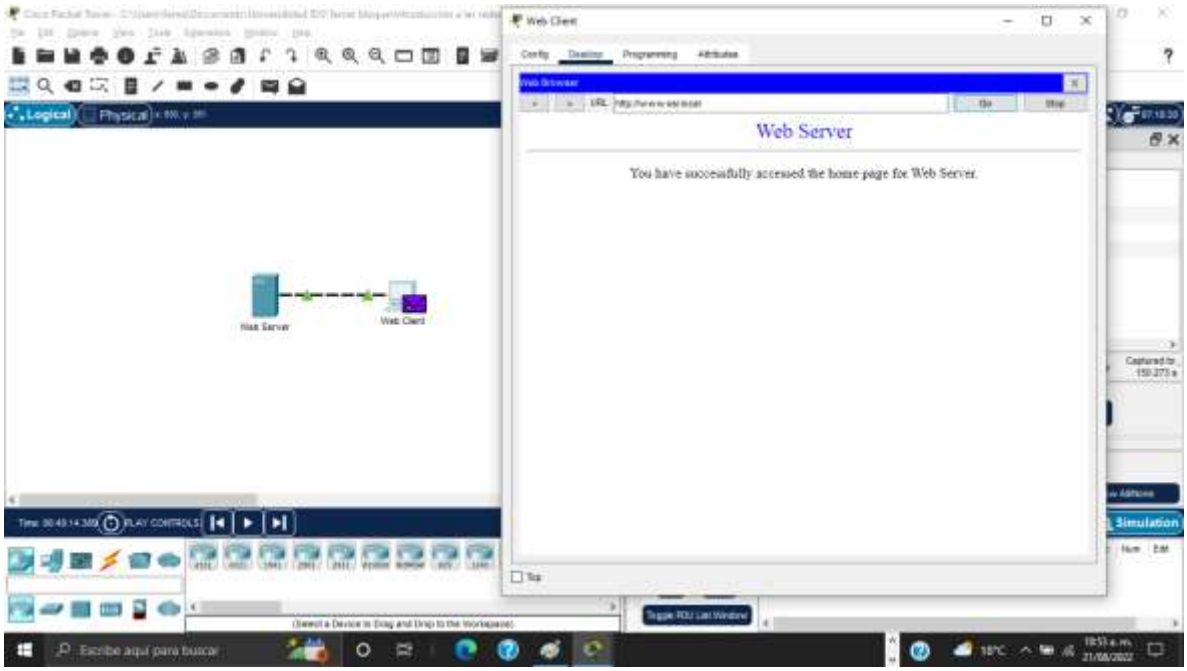
…hacia el servidor…



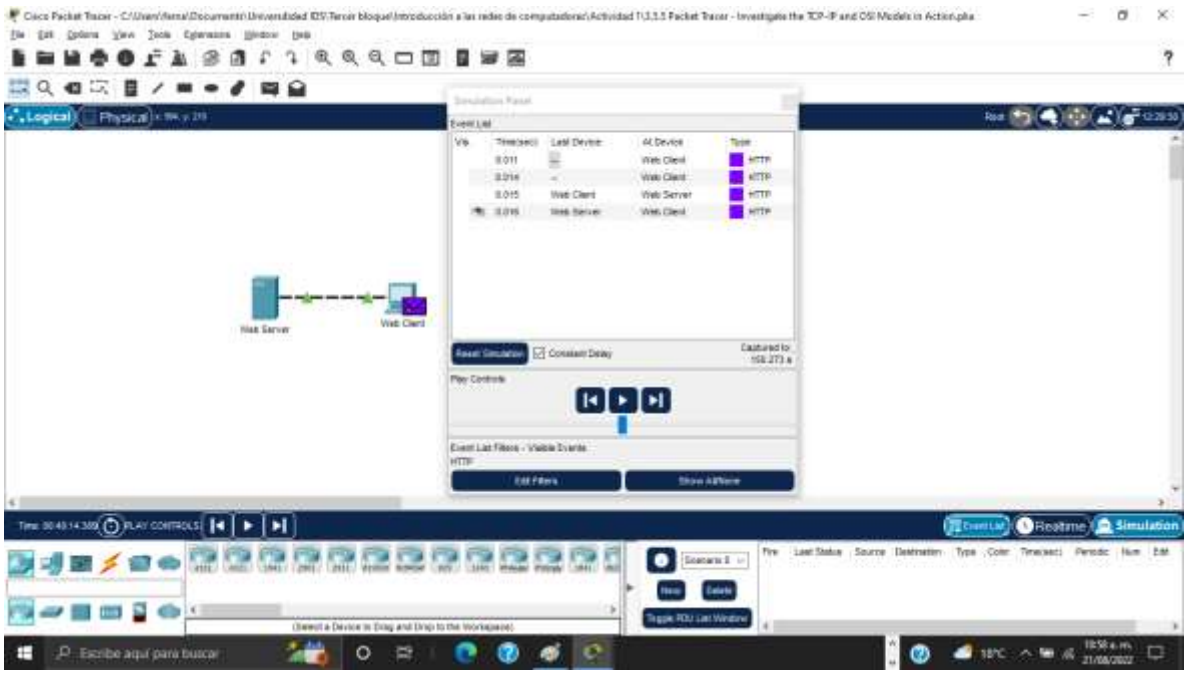
…y de regreso…



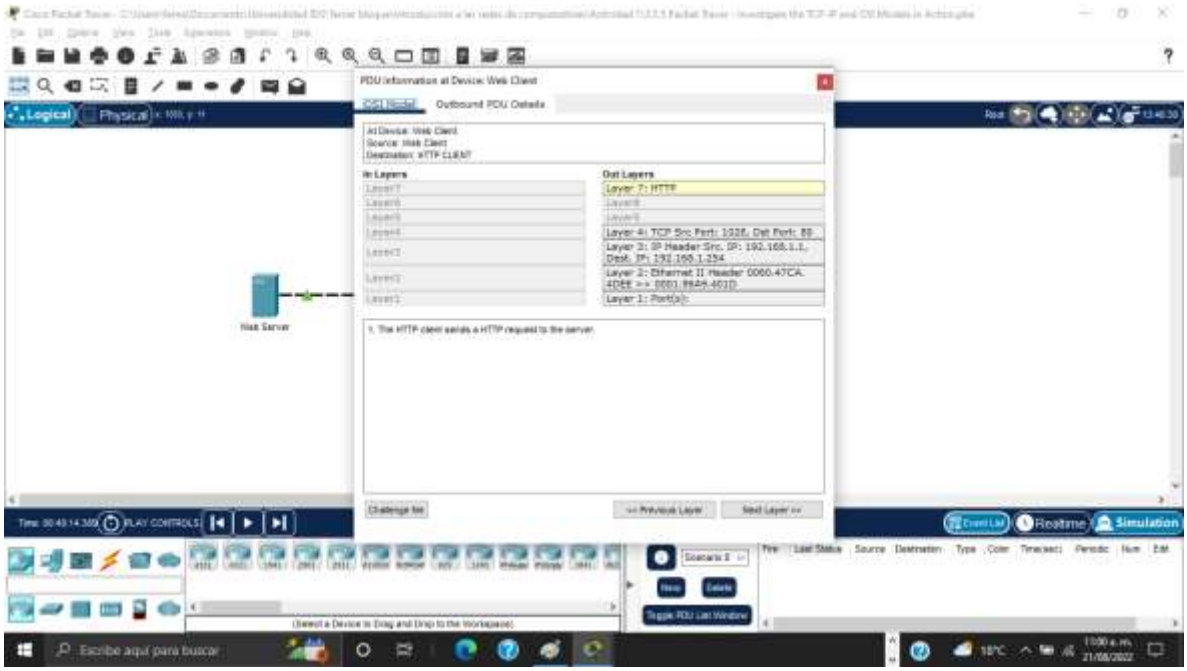
…donde al finalizar pondrá una paloma indicando que todo estuvo correcto.



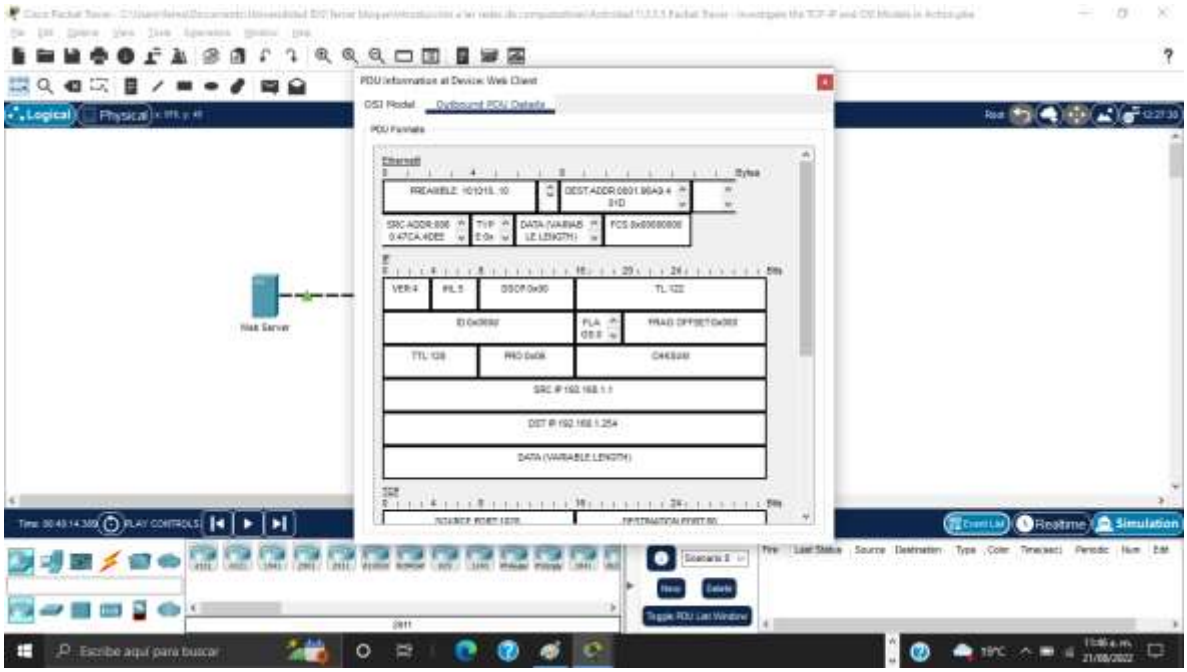
Nos muestra la siguiente leyenda en pantalla después de hecha nuestra solicitud.

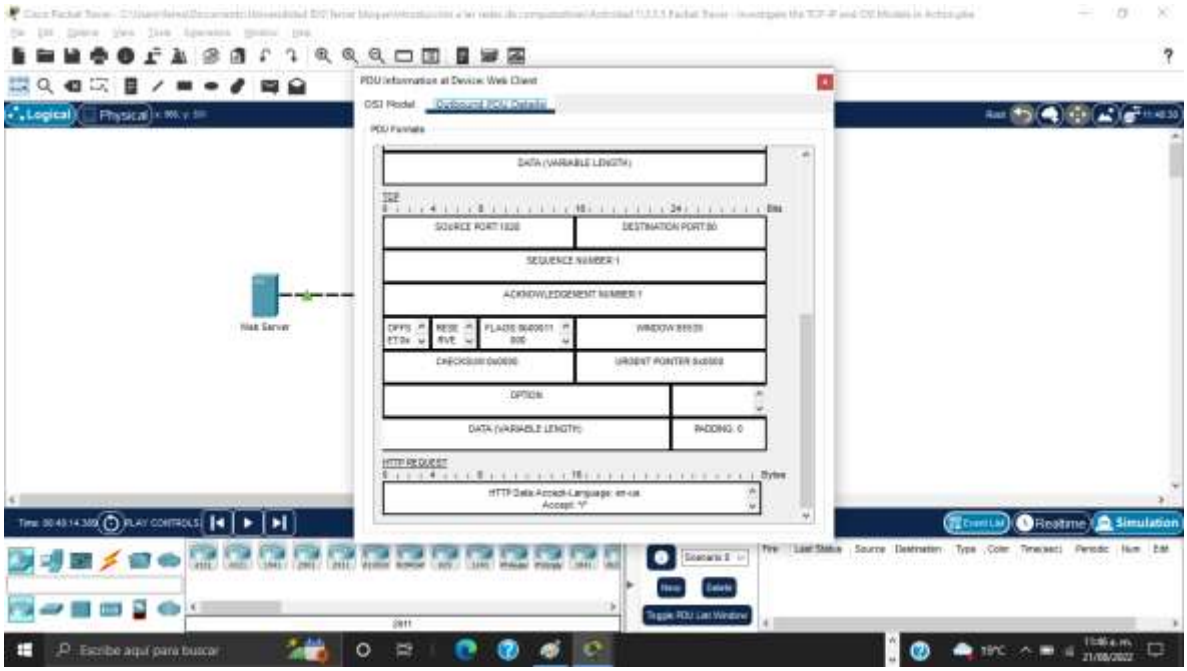


En la lista de eventos seleccionamos el primer cuadro morado de la columna type.



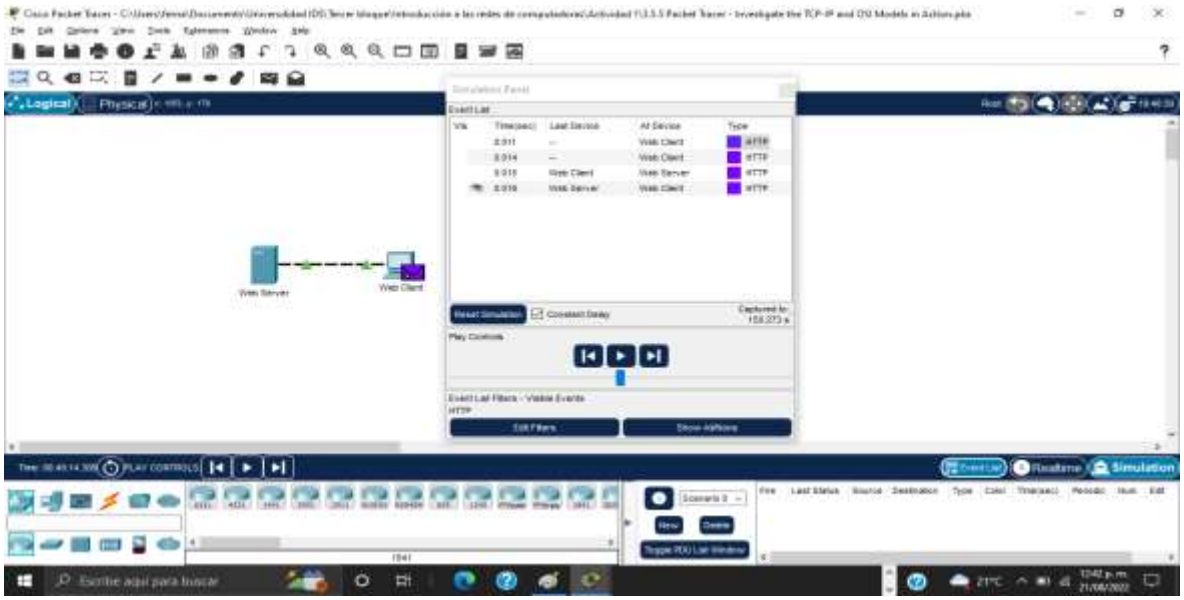
En el apartado OSI Model nos muestra los layers.





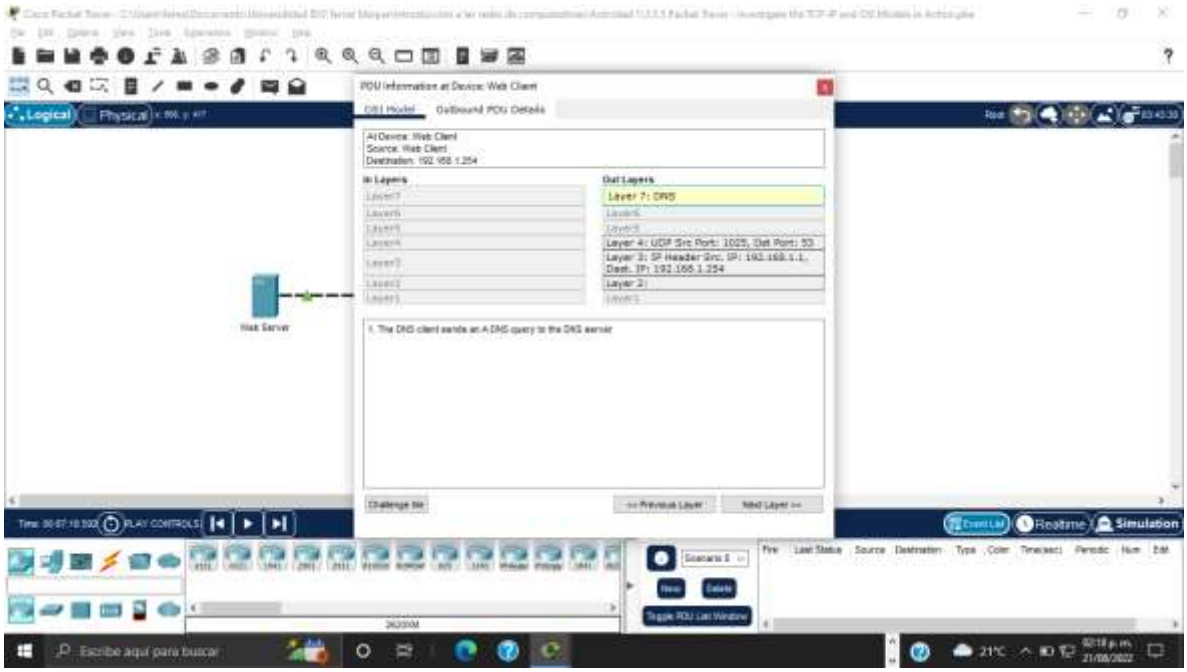
En el apartado Outbound PDU details nos muestra información que se responderá en la sección de preguntas.

Cerramos ventana.

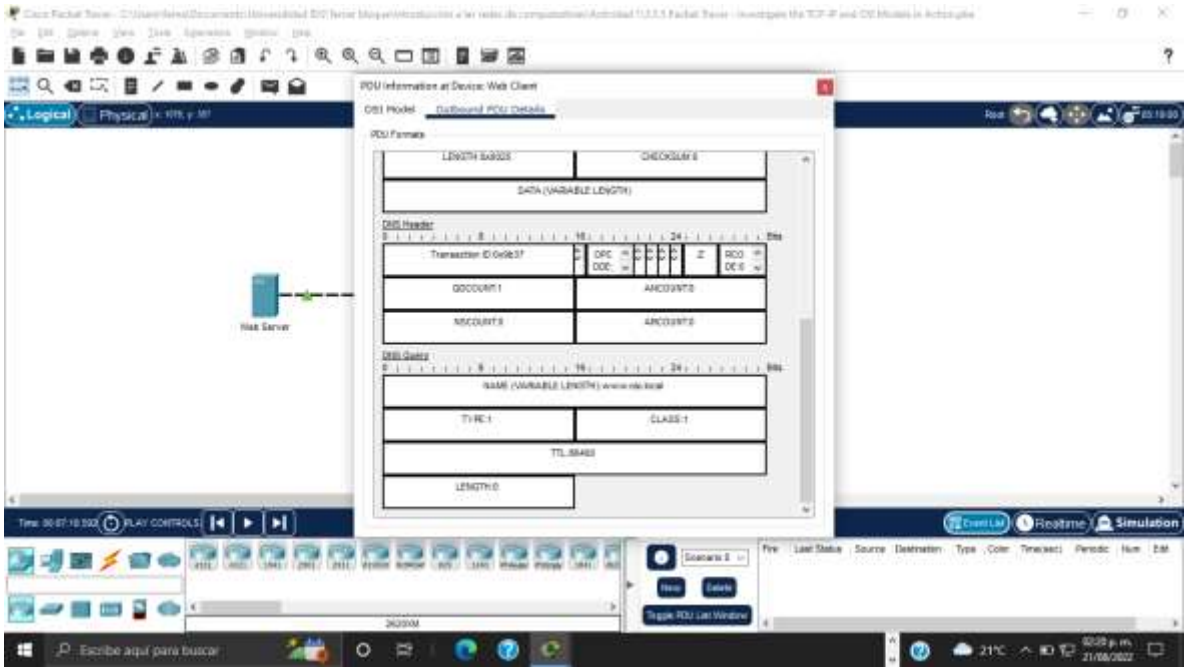


Nuevamente en la lista de eventos seleccionamos Show all/None dos veces.

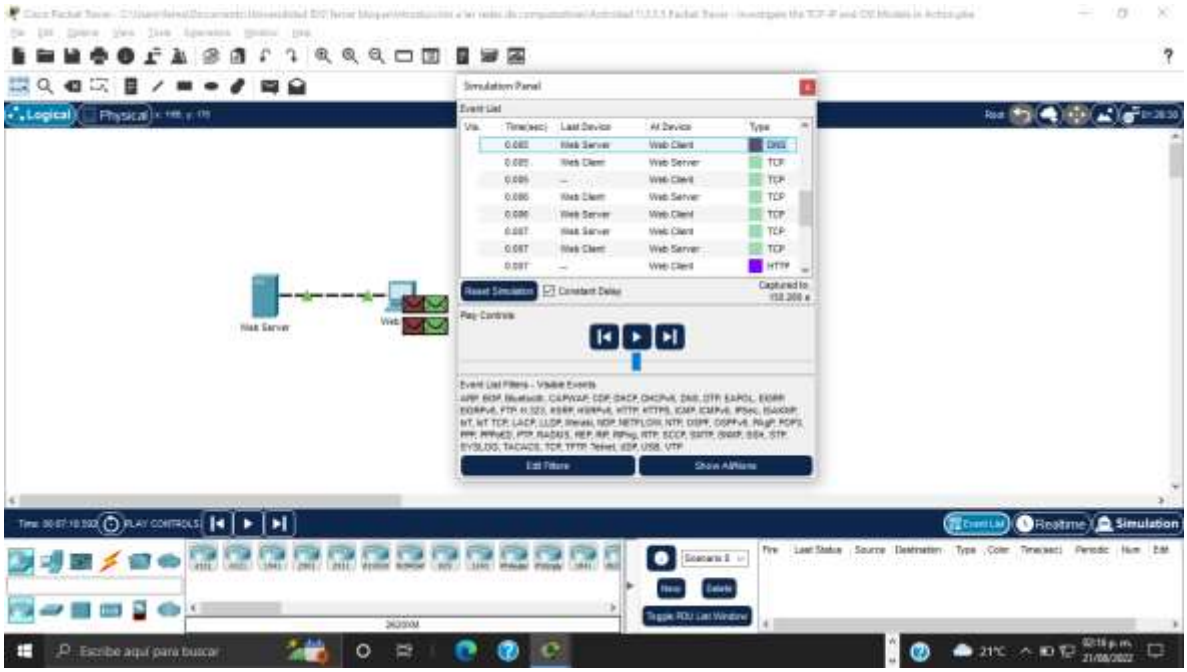
Nos muestra la siguiente ventana y damos doble clic en el primer evento DNS.



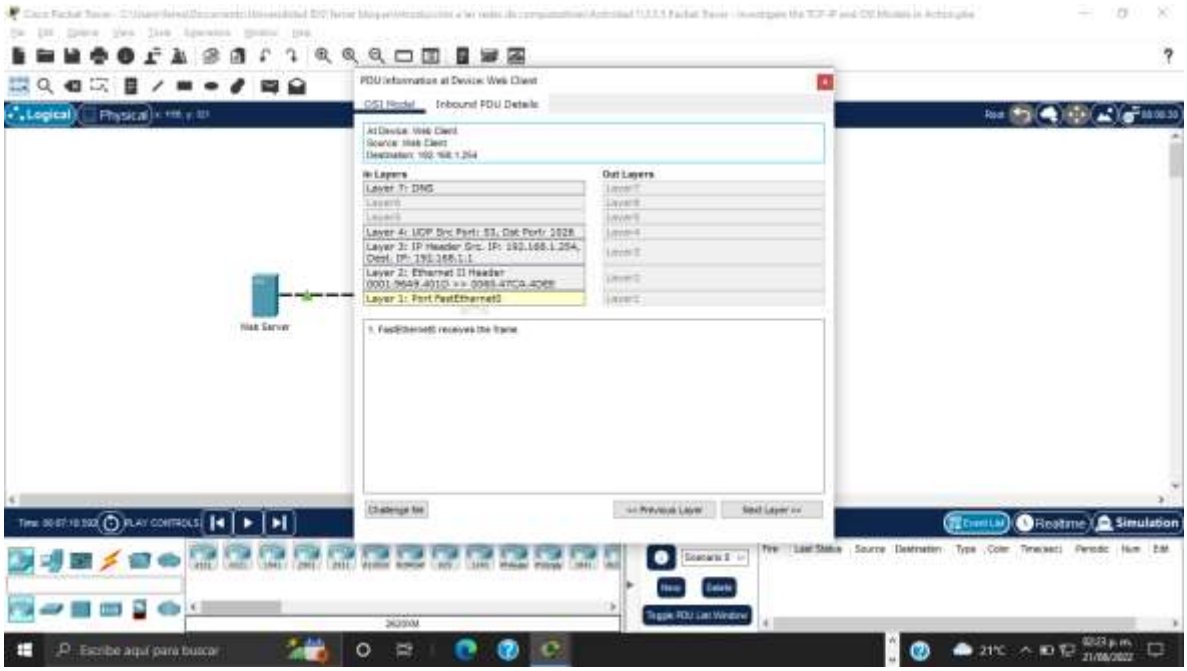
En la capa 7 nos indica que el cliente DNS envía una consulta DNS al servidor DNS.



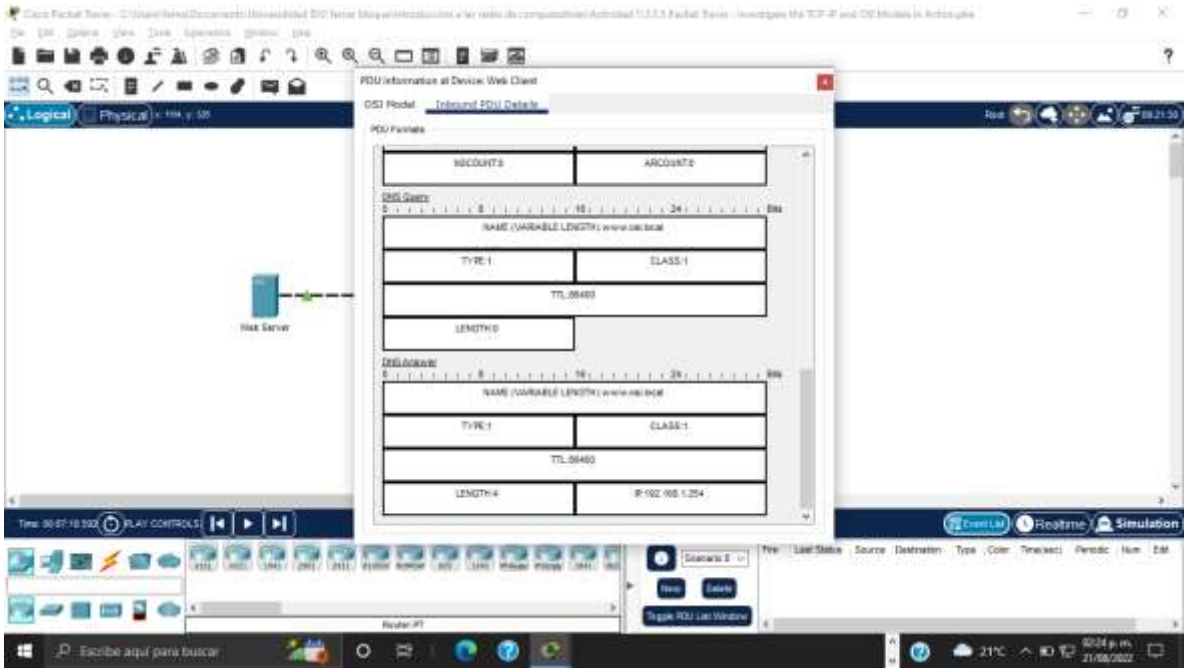
En DNS query tiene el nombre www.osi.local



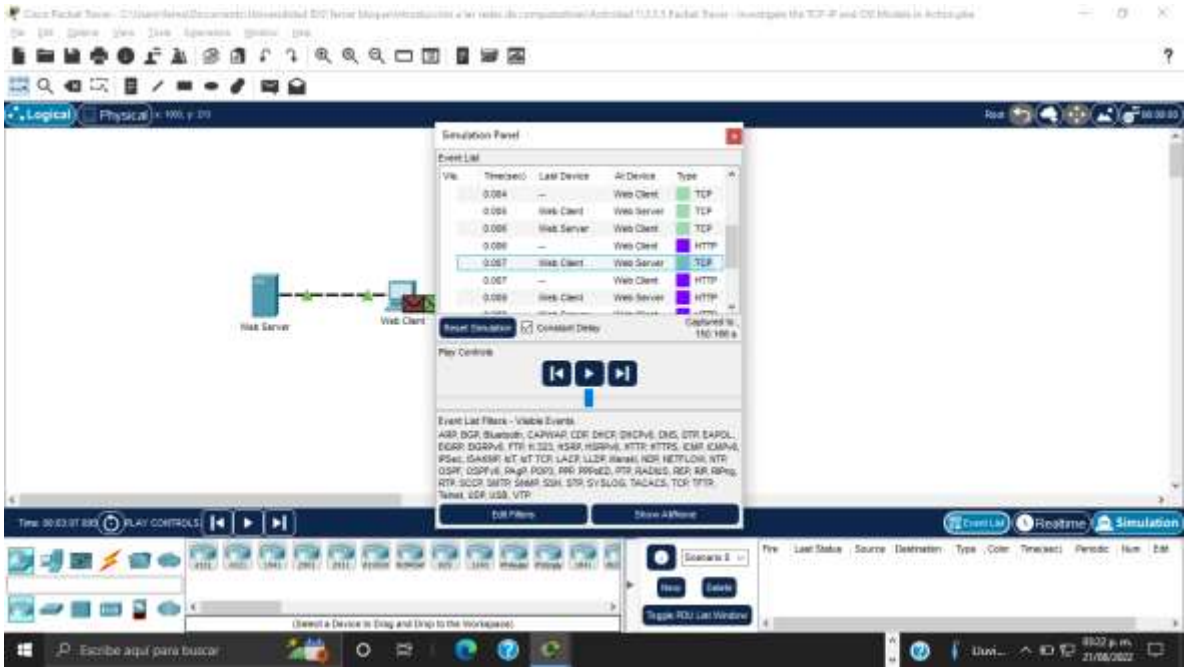
Vamos al último cuadro DNS de la lista y damos doble clic.



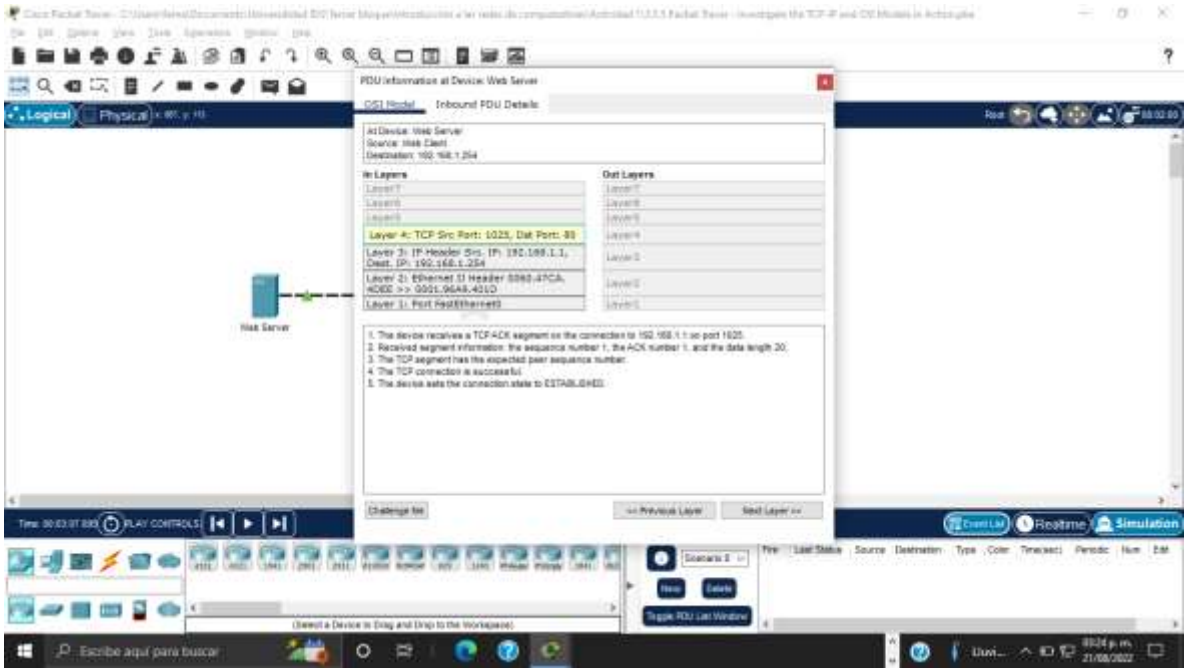
Nos muestra que se capturo en el dispositivo web client.



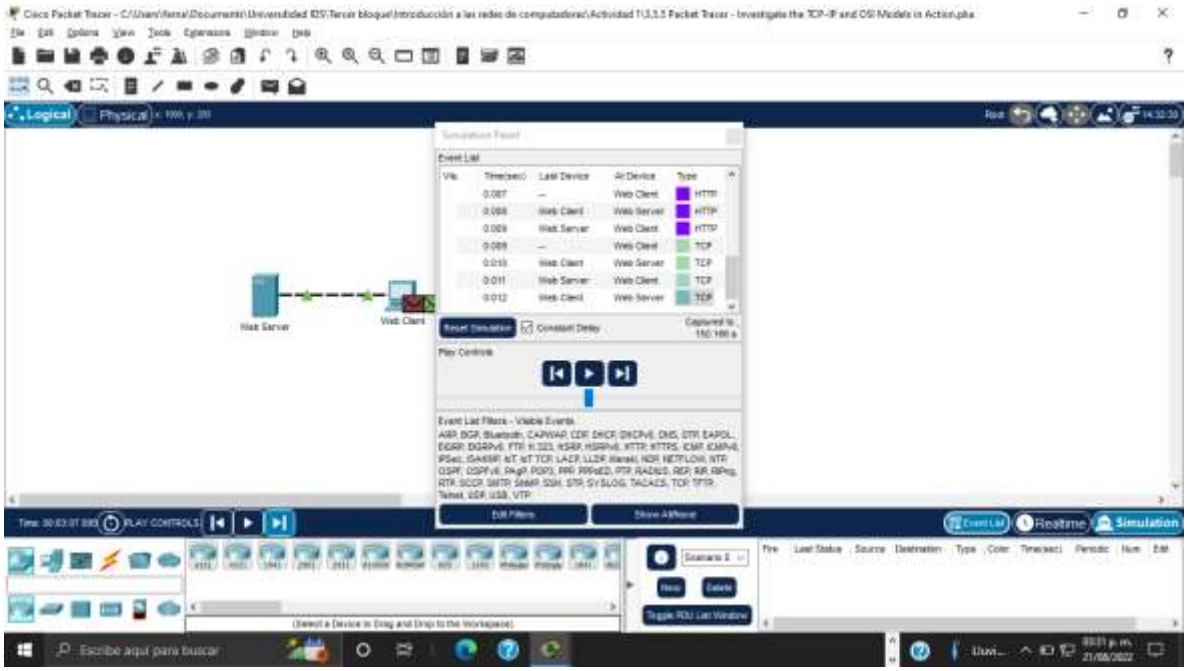
El valor junto a adress de DNS answer es 4.



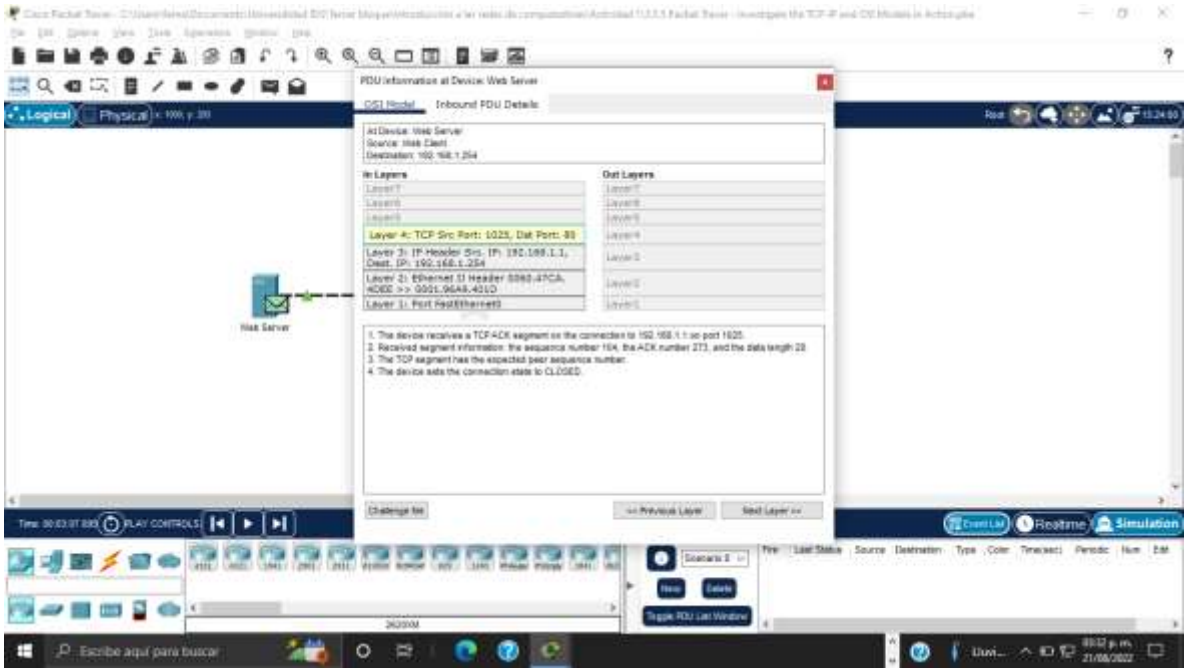
Buscamos el primer evento HTTP y seleccionamos el evento TCP siguiente y damos doble clic.



Seleccionamos layer 4 y la información que muestra en el punto 4 es que la conexión fue exitosa y en el punto 5 indica que el dispositivo establece el estado de conexión en establecido.



Seleccionamos el último evento TCP y damos doble clic.



Seleccionamos layer 4 y nos indica que por parte del dispositivo establece el estado de conexión como cerrado.

Preguntas

- ¿Cambio algo?

  Si, nos muestra la leyenda en pantalla: “has accesado satisfactoriamente a la página principal del servidor web”.

- ¿Qué información se enumera en los pasos numerados directamente debajo de los cuadros In Layers y Out Layers para Layer 7?

  Para In Layers enlista las 7 capas del modelo OSI, donde en Out Layers para Layer 7 nos indica que el cliente http envía una solicitud http al servidor.

- ¿Cuál es el valor del Dst Port para Layer 4 en la columna Out Layers?

  El valor para Dst Port es 80.

- ¿Cuál es el Dest?

  El Dest es: IP 192.168.1.254

- ¿IP para Layer 3 en la columna Out Layers?

  La IP es: 192.168.1.1

- ¿Qué información se muestra en Layer 2 en la columna Out Layers?

  Nos muestra las direcciones MAC de cada dispositivo.

- ¿Cuál es la información común que figura en la sección IP de los PDU Details en comparación con la información que figura en la pestaña del OSI Model?

  Las direcciones IP.

- ¿Con qué capa está asociado?

  Con la capa 3.

- ¿Cuál es la información común que aparece en la sección TCP de PDU Details, en comparación con la información que aparece en la pestaña del OSI Model, y con qué capa está asociada?

  Muestra la información de los puertos y está asociada con la capa 4.

- ¿Cuál es el host que aparece en la sección HTTP de los PDU Details?

  www.osi.local

- ¿Con qué capa se asociaría esta información en la pestaña del Modelo OSI?

  Con la capa 7.

Segunda parte

- ¿Qué información se indica en el campo NAME: en la sección de DNS QUERY?

  Se muestra el host www.osi.local

- ¿En qué dispositivo se capturó la PDU?

  En el dispositivo web client.

- ¿Cuál es el valor que aparece junto a ADDRESS: en la sección DNS ANSWER de Inbound PDU Details?

  4.

- En la lista numerada directamente debajo de In Layers y Out Layers, ¿cuál es la información que se muestra en los elementos 4 y 5?

- ¿Cuál es el propósito de este evento, basado en la información proporcionada en el último elemento de la lista (debe ser el elemento 4)?

  El propósito de este evento es concretar el proceso de solicitud por parte del dispositivo y lo establece como cerrado.

Conclusión

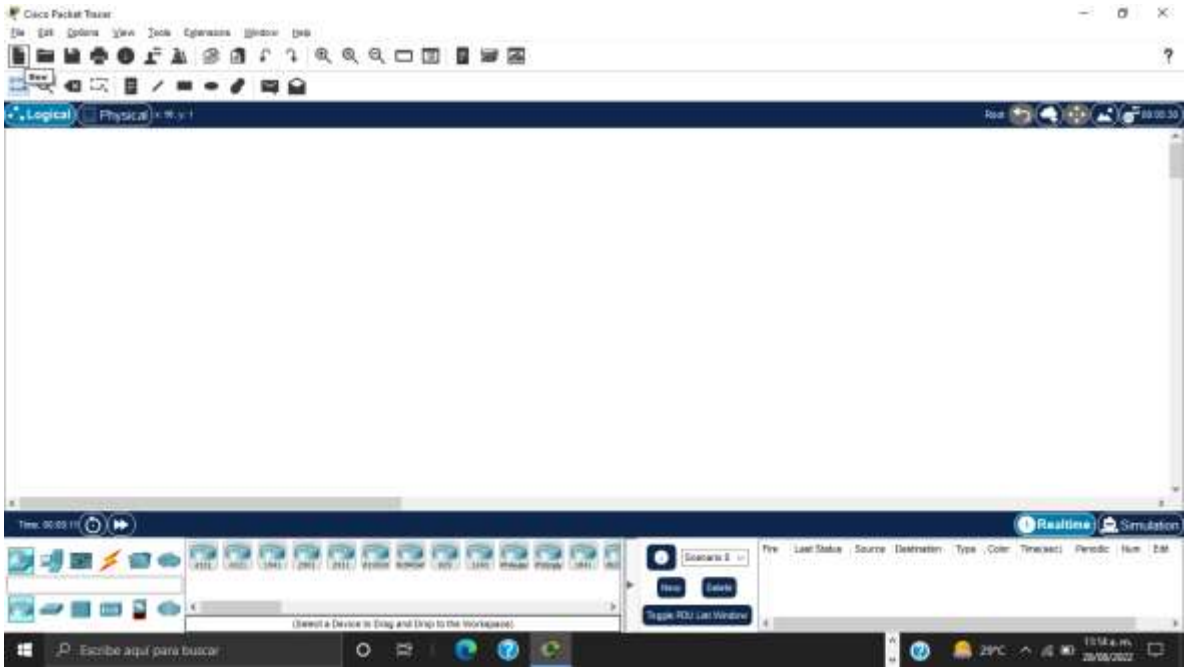
En base a esta actividad se puede apreciar el camino que recorre una solicitud entre dos clientes en cada capa del proceso, como se relacionan entre si y cuál es la finalidad de cada una de estas, permitiendo así, que la información que se transmite sea de forma íntegra, garantizando esta misma entre cada uno de los puntos.

Introducción

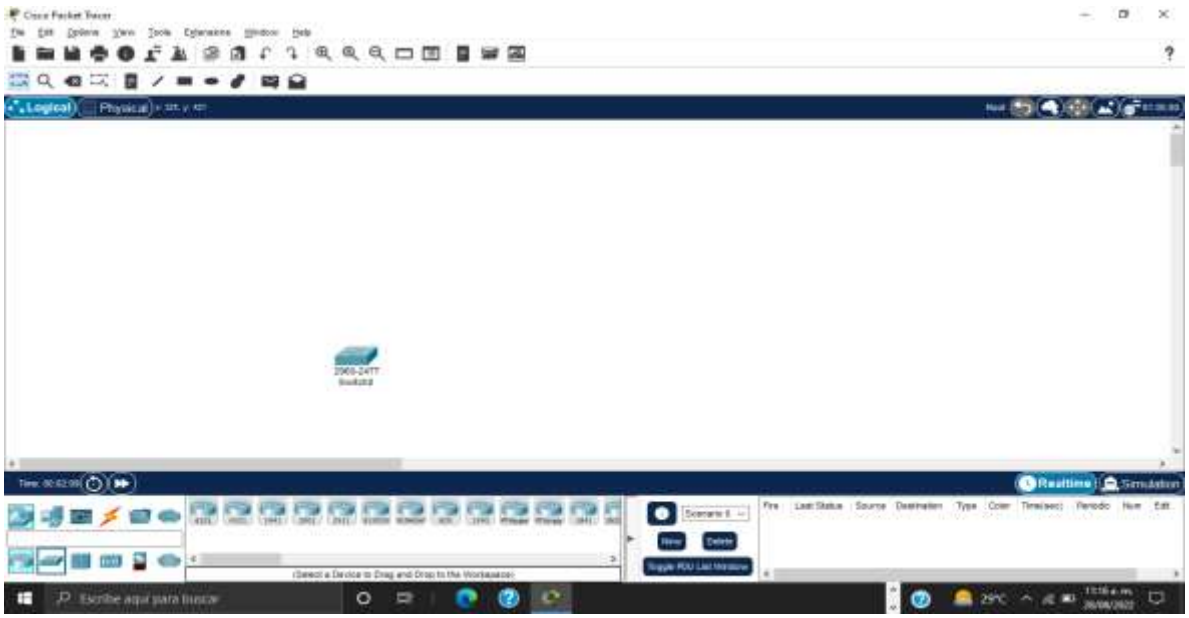
En base a la actividad anterior, crearás un entorno de una red local donde exista la comunicación entre un servidor web y su cliente.

Se creara una conexión de red local agregando un switch que se conectará con todos los equipos, un nuevo servidor que hará la función de DNS y 3 nuevas PC que serán también Clientes Web, deberás de asignarles las direcciones que se indican en la tabla de direccionamiento.

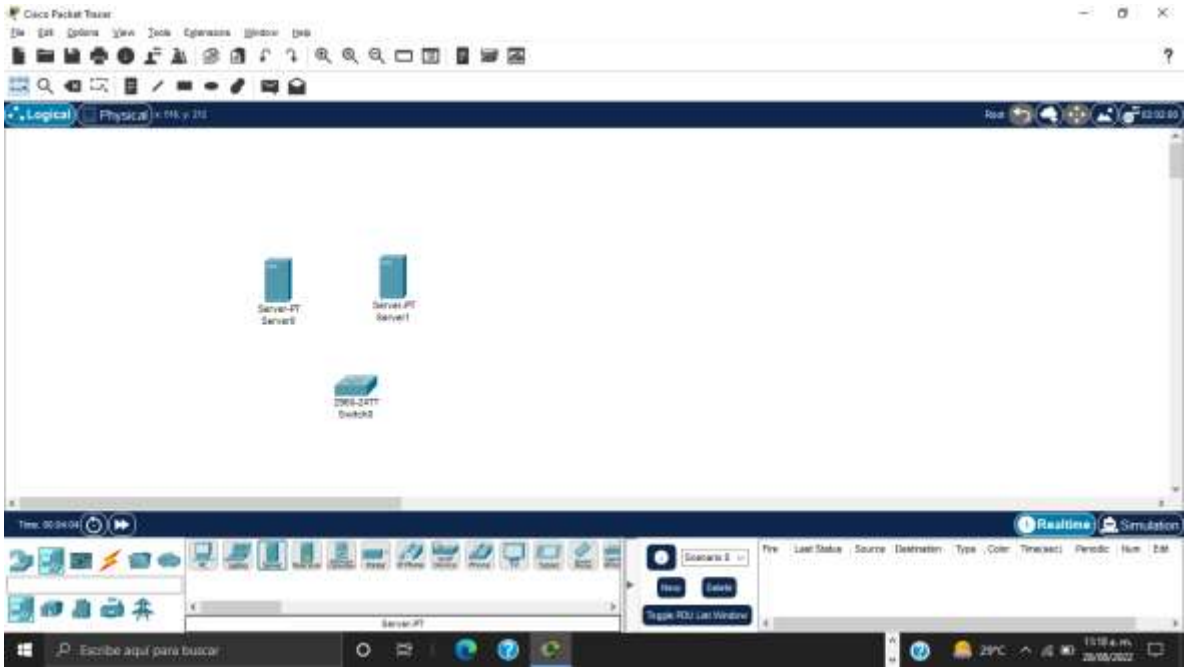
Capturas de pantalla



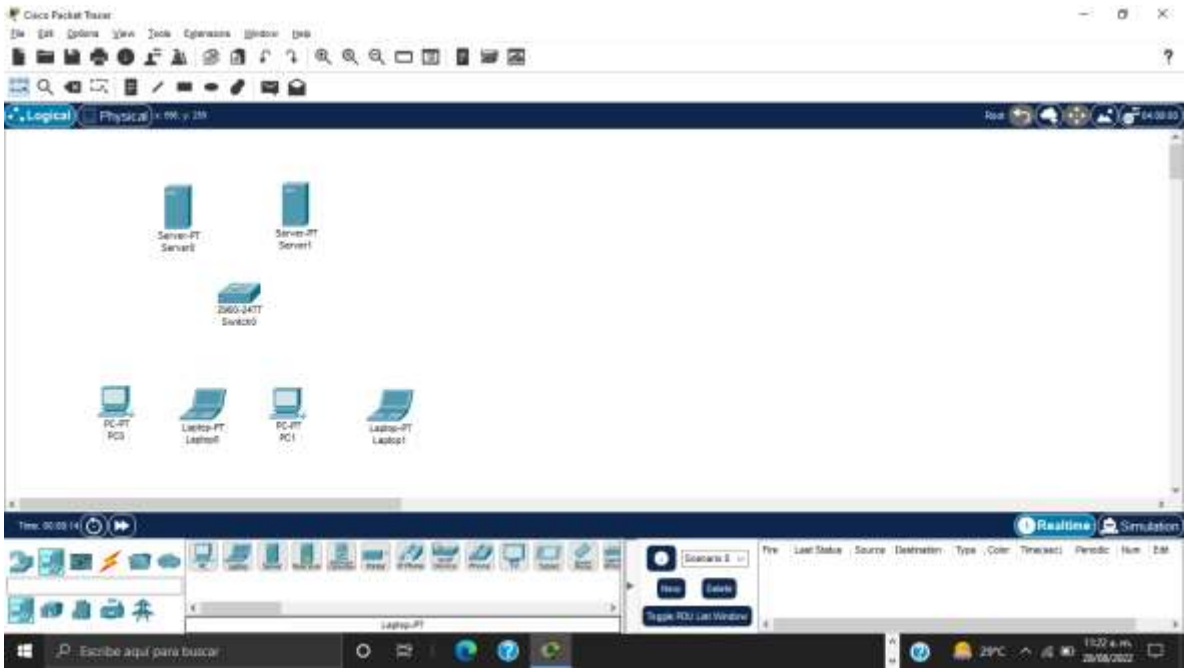
Para le segunda actividad crearemos un nuevo archivo.



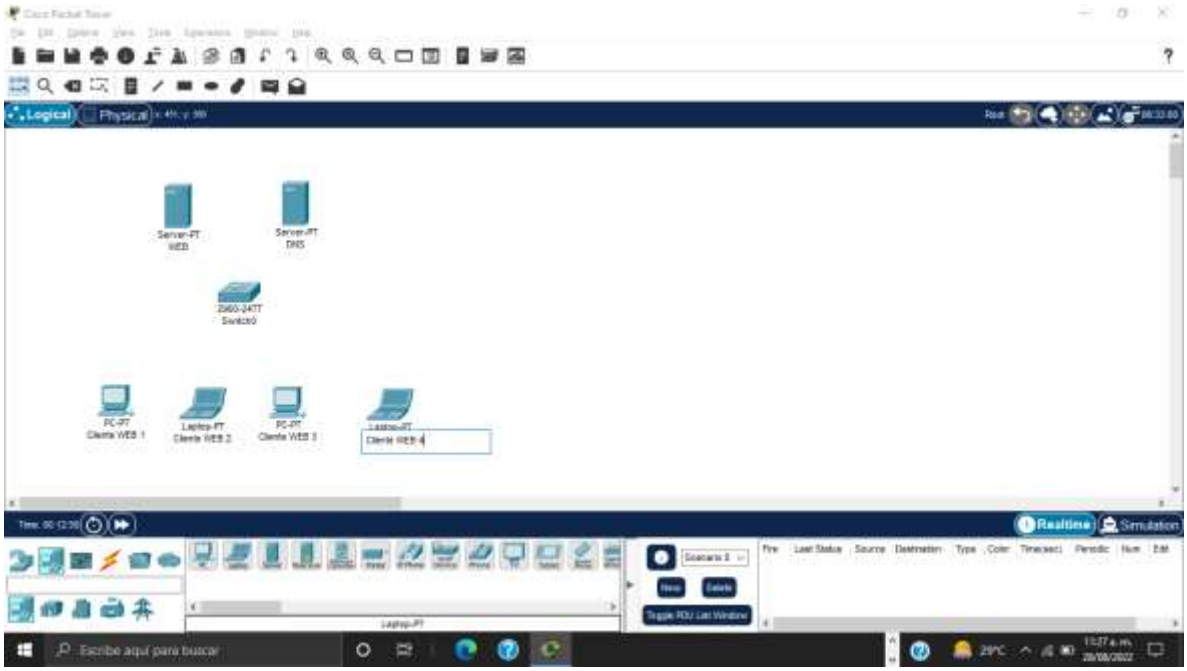
Utilizaremos un Switch.



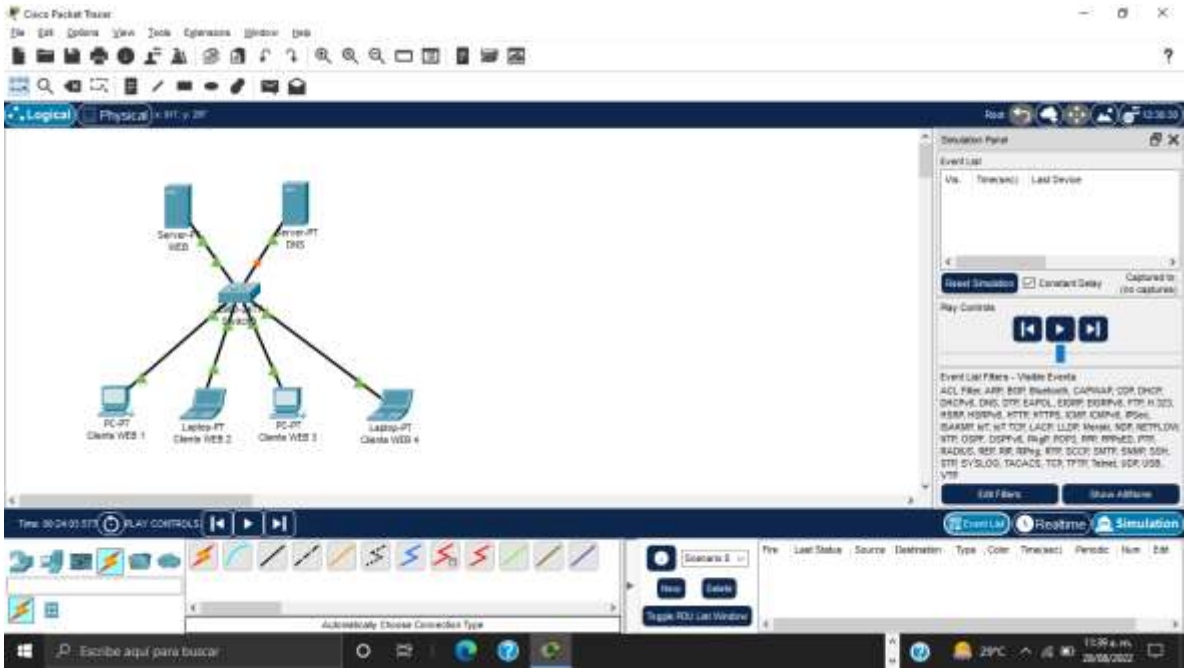
Utilizaremos dos servidores.



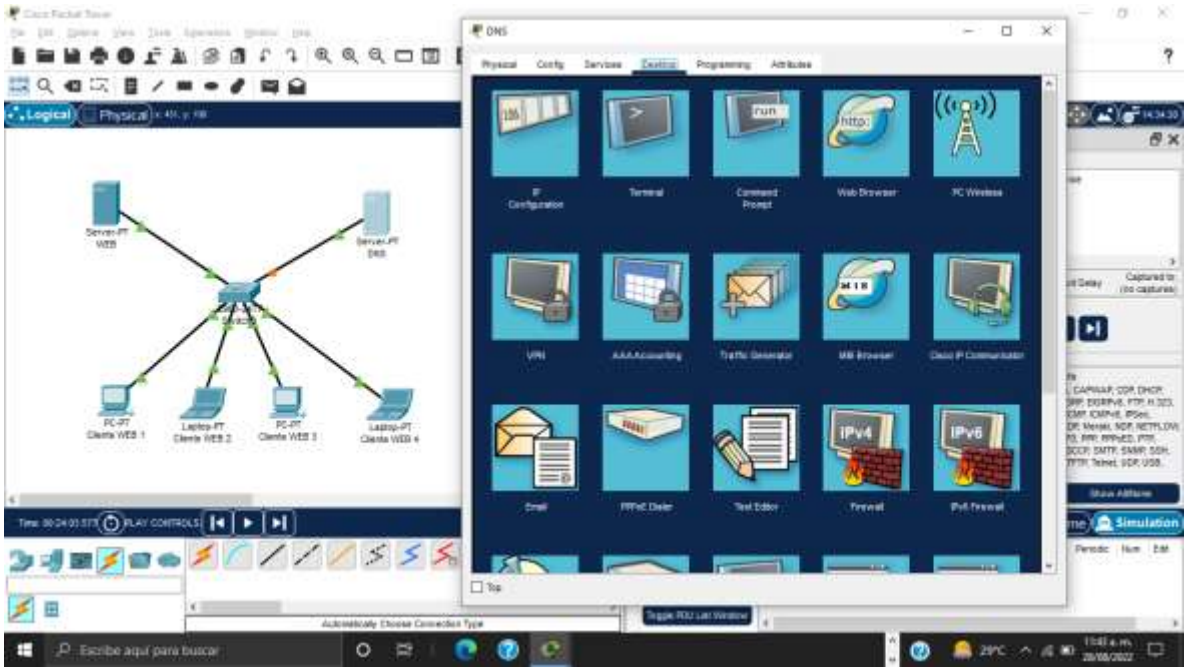
Utilizaremos 4 clientes web.



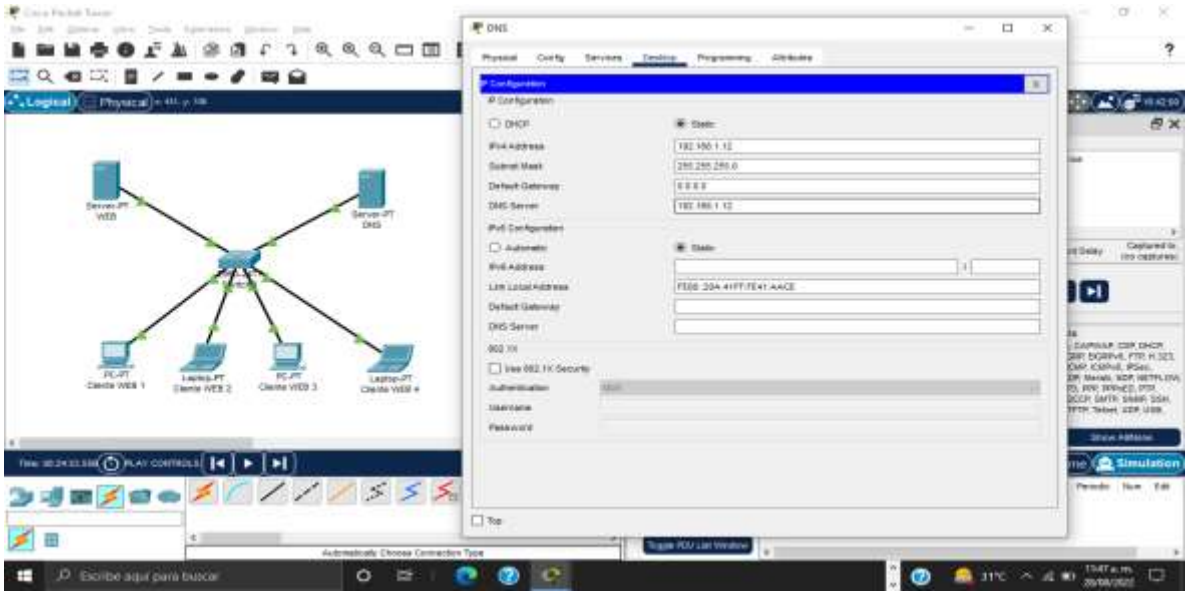
Cambiamos los nombres a nuestros servidores y clientes para identificarlos.



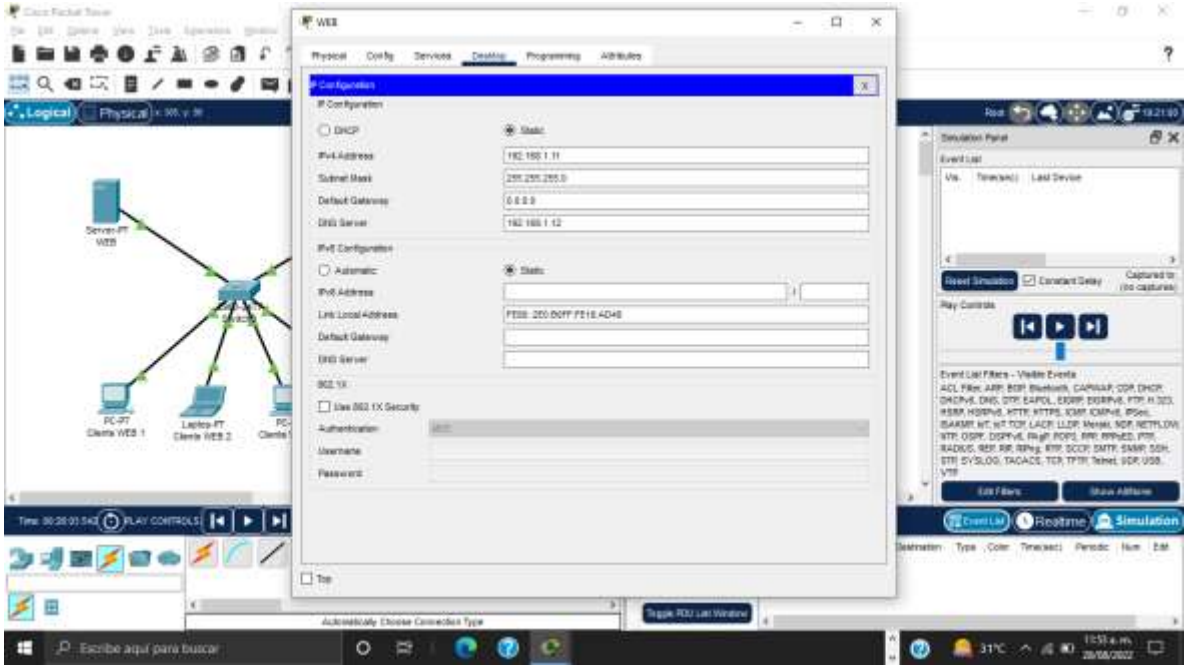
Interconectamos todos los equipos y ponemos en modo simulation nuestro panel.



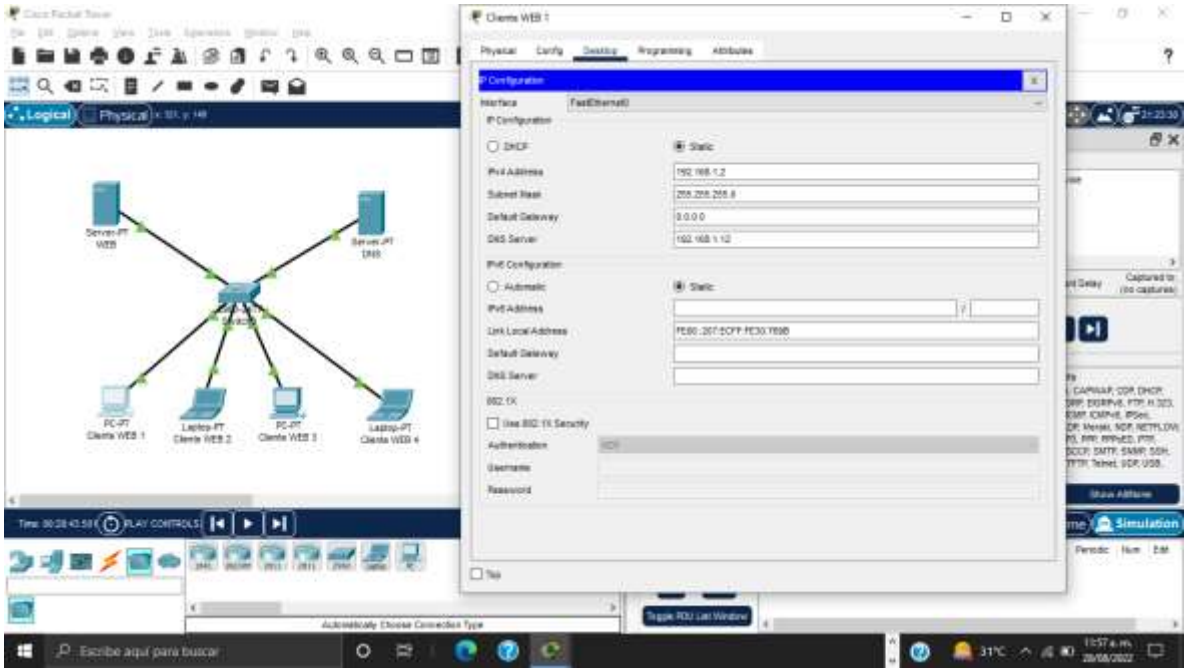
Asignaremos la dirección IP del servidor DNS, dando un click sobre él y seleccionamos el apartado Desktop.



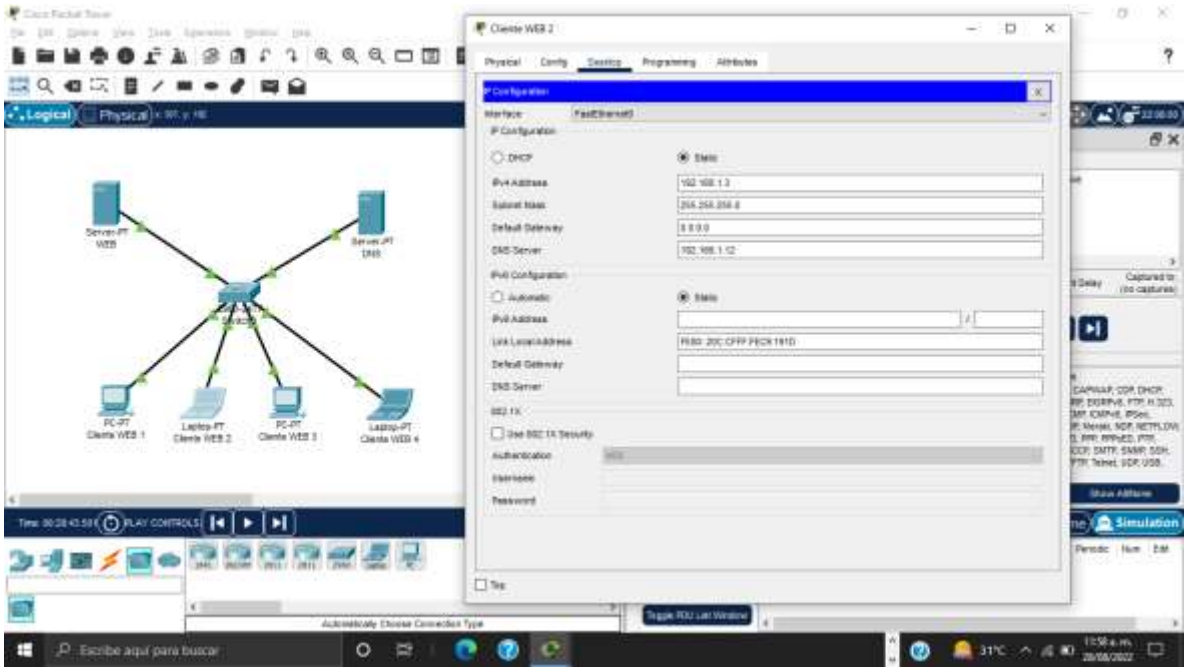
Las direcciónes IP que les corresponde van a ser estáticas y en el servidor DNS es 192.168.1.12, tanto en la IPv4 como en la del servidor.



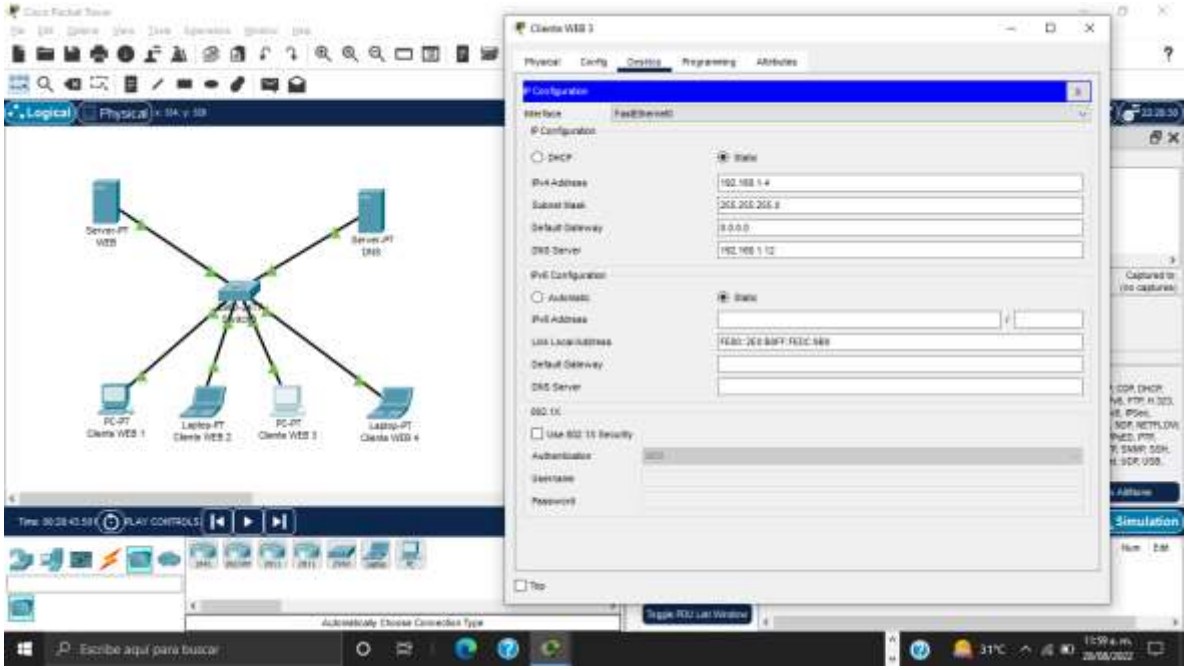
La dirección del servidor web es 192.168.1.11 en IPv4 y la del servidor DNS es 192.168.1.12



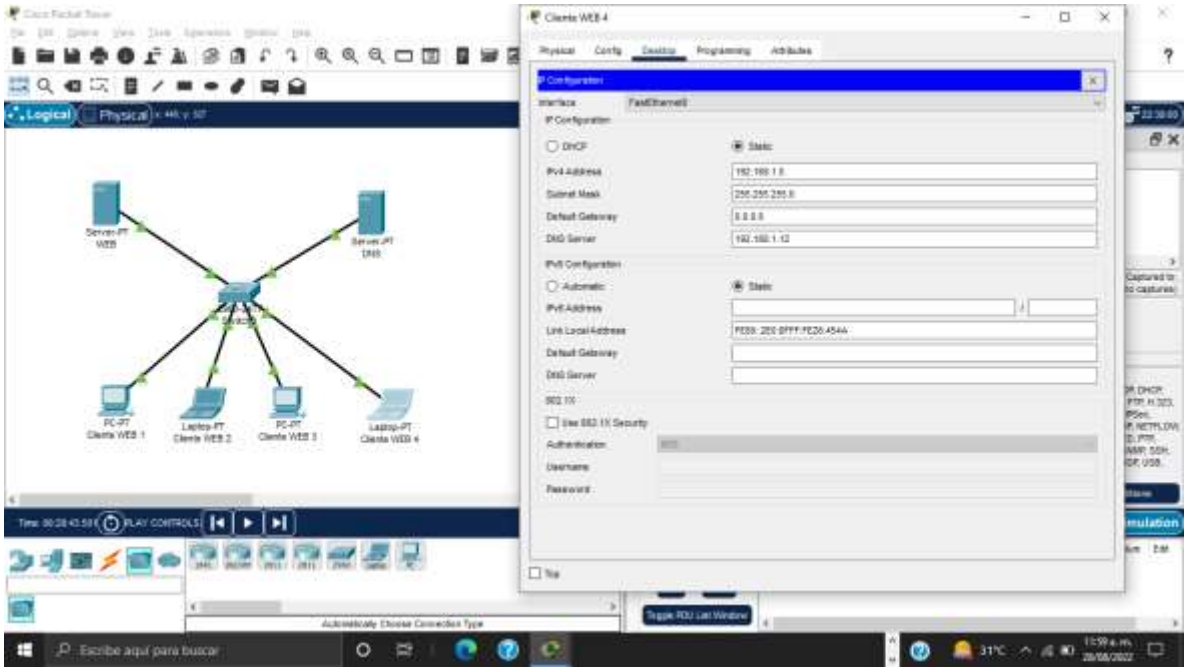
Para el cliente WEB 1 la dirección es 192.168.1.2 en IPv4 y la del servidor DNS es 192.168.1.12



Para el cliente WEB 2 la dirección es 192.168.1.3 en IPv4 y la del servidor DNS es 192.168.1.12

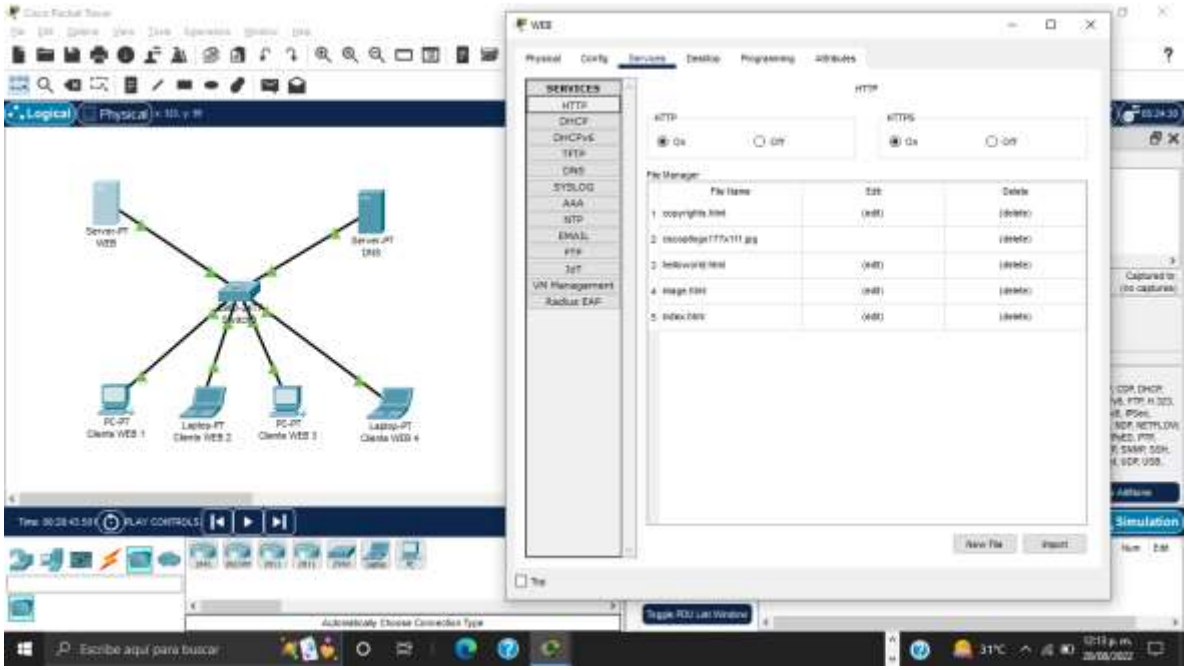


Para el cliente WEB 3 la dirección es 192.168.1.4 en IPv4 y la del servidor DNS es 192.168.1.12



Para el cliente WEB 4 la dirección es 192.168.1.5 en IPv4 y la del servidor DNS es 192.168.1.12.

A continuación activaremos el servicio HTTP en el servidor WEB y apagaremos los demás servicios.




Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCP
Interface
FastEthernet0
Service
On
Off


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
DHCPv6
Interface
FastEthernet0
DHCPv6 Pool
Service
On
Off


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
TFTP
Service
On
Off
File


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
Syslog
Service
On
Off
Time
Hostname
Message


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
NTP
Service
On
Off
Authentication
Key
Password
agosto_2022

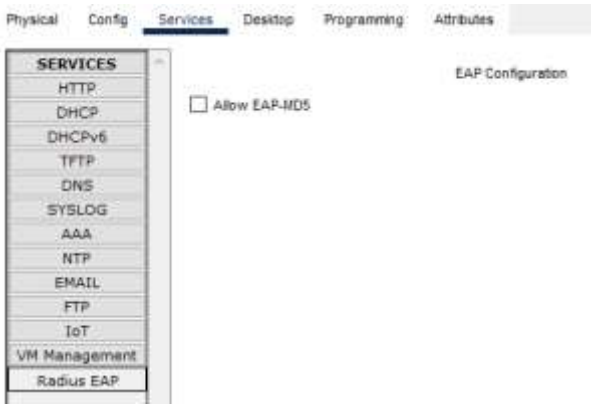

Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius

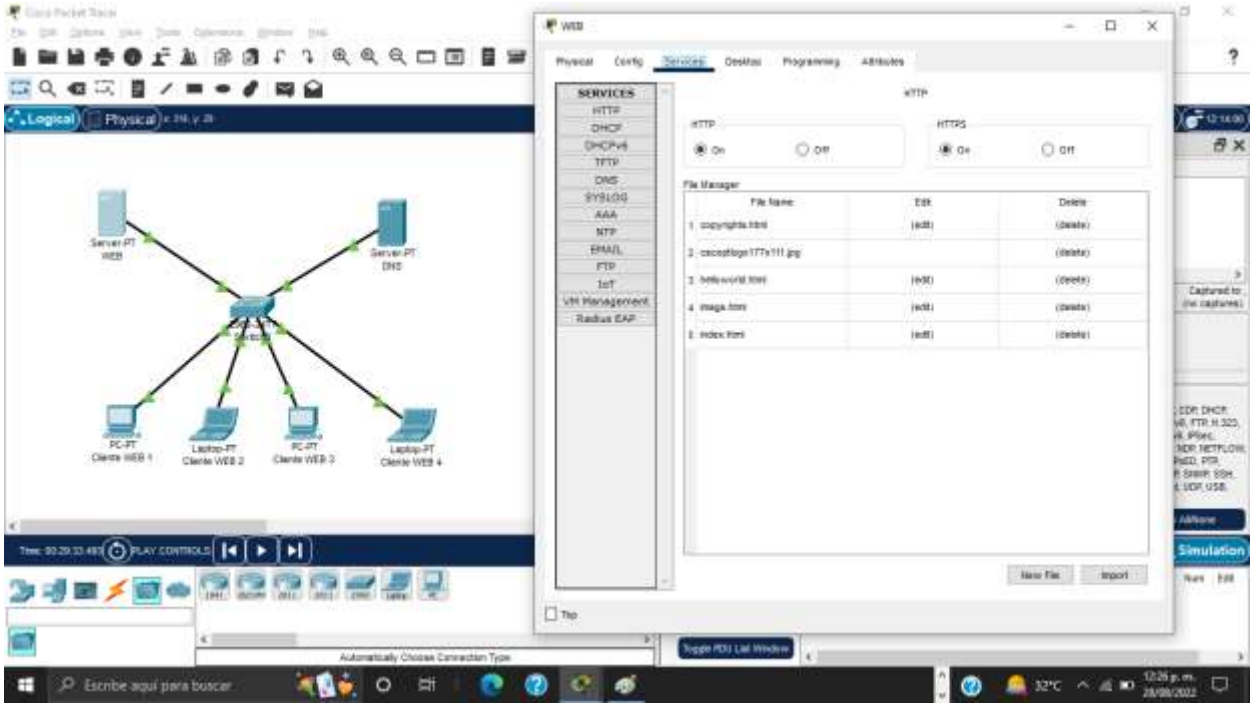

Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
EMAIL
SMTP Service
On
Off
POP3 Service
On
Off
Domain Name
Set
User Setup
User
Password


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1
cisco
cisco
RWDNL
Add

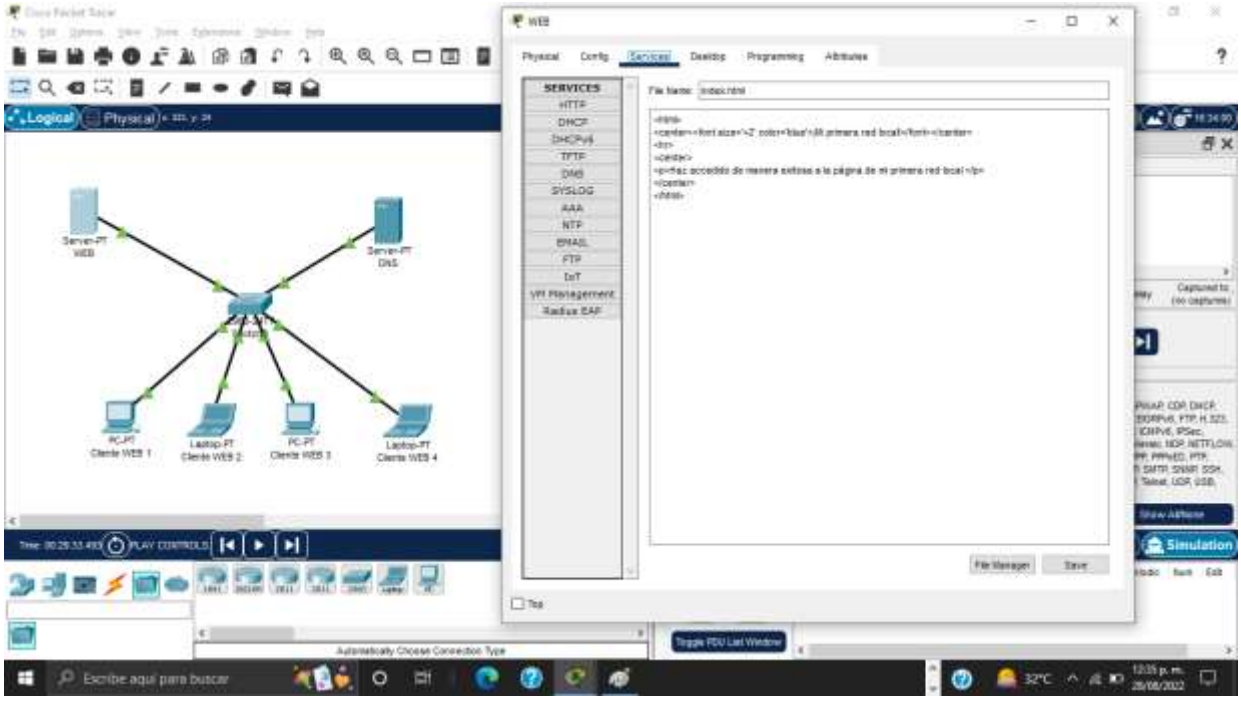

Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
Registration Server
This service runs on top of the HTTP or HTTPS service.
Service
On
Off


Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
VM Management
Service
On
Off
VM
Status

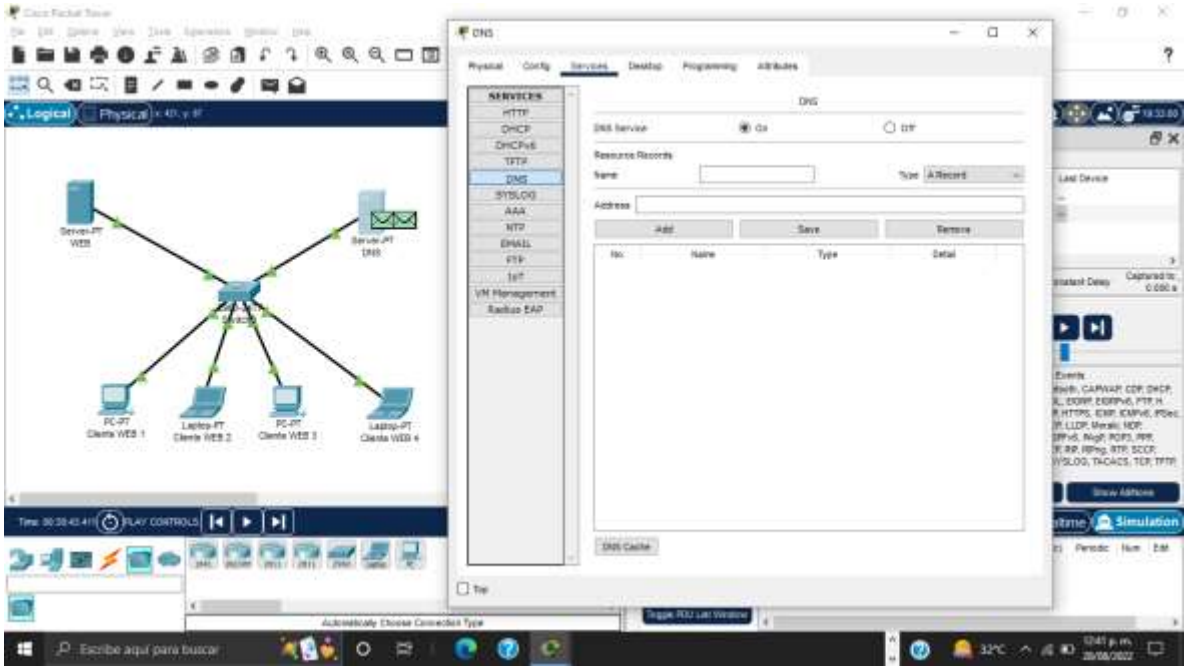

Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
EAP Configuration
Allow EAP-MD5

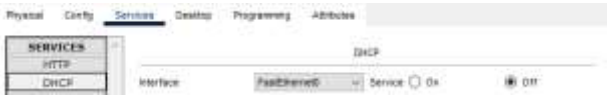


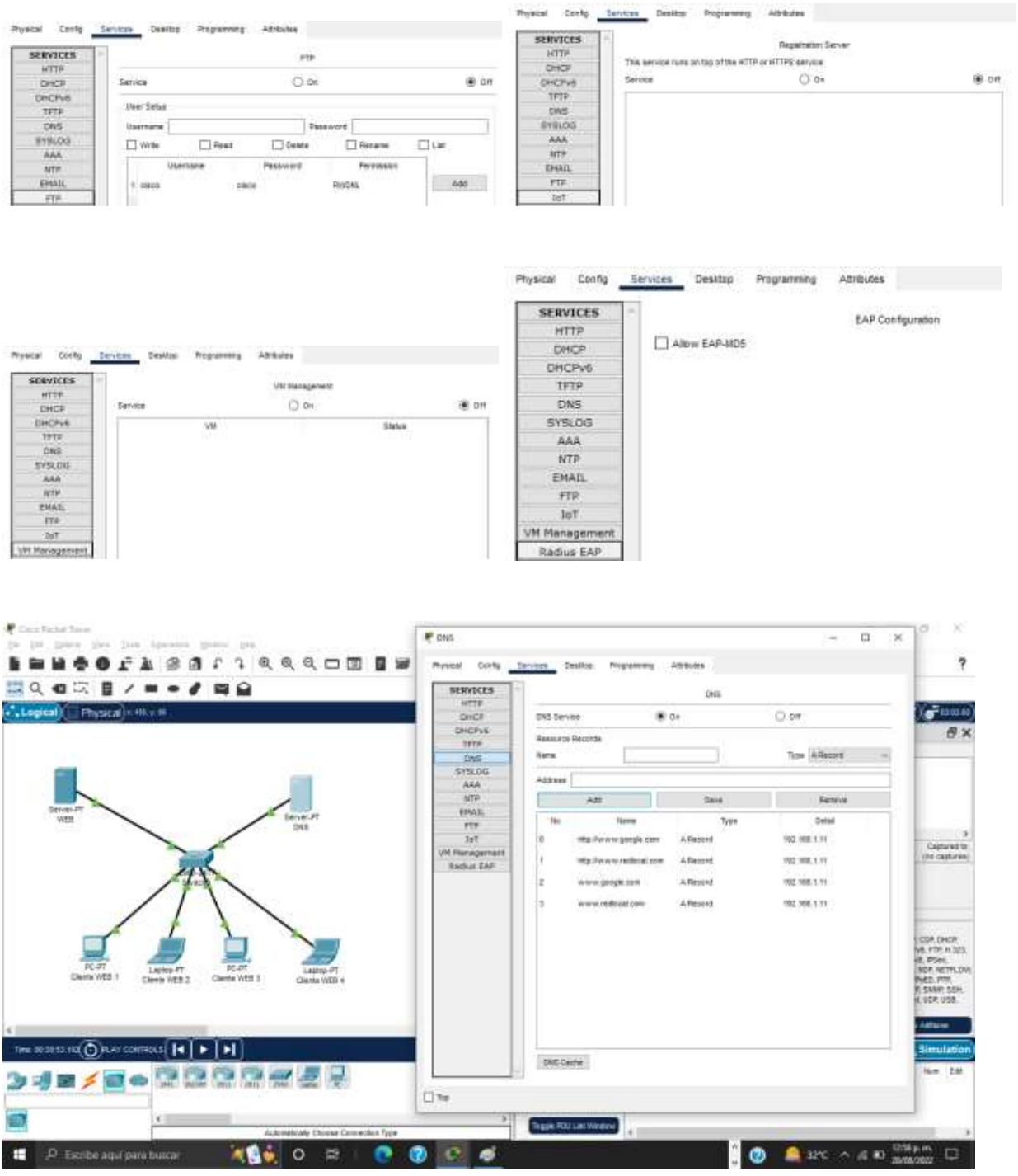
Regresamos al servicio HTTP y editamos el index de la fila 5 como lo pide la actividad.



Posteriormente en el servidor DNS activamos solo el servicio DNS y los demás los apagaremos.

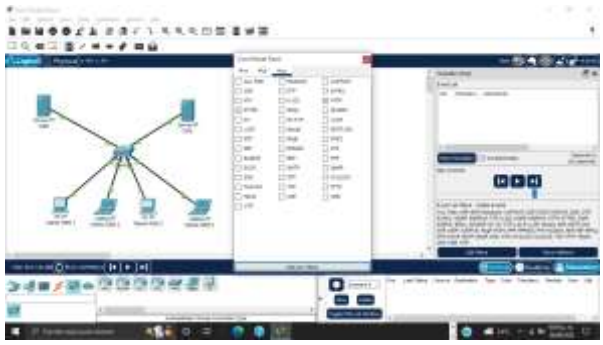




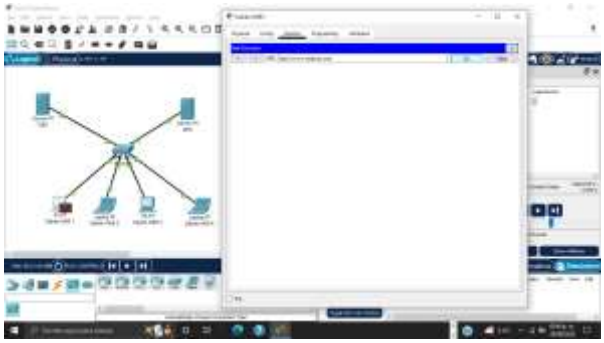


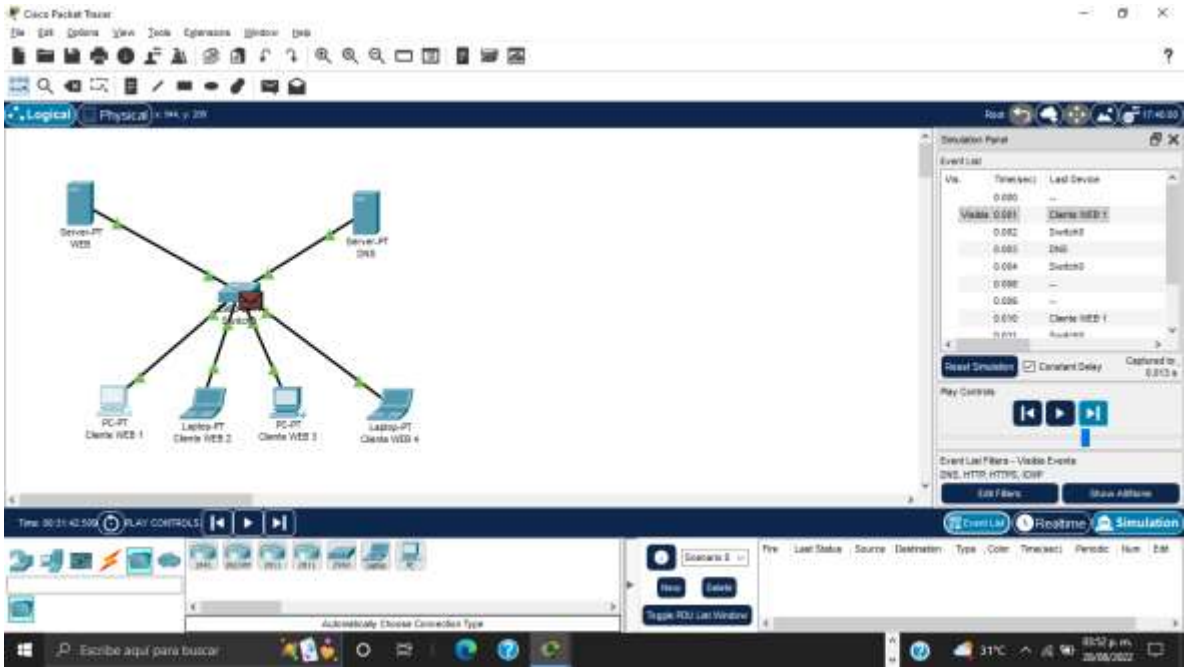
En el apartado de DNS editamos el nombre o los nombres y la dirección IP, que va a ser la del servidor web.

Editamos los filtros seleccionando en IPv4 solo las casillas DNS e ICMP, en IPv6 desactivamos todas y en Misc dejamos solo activas las casillas HTTP y HTTPS.

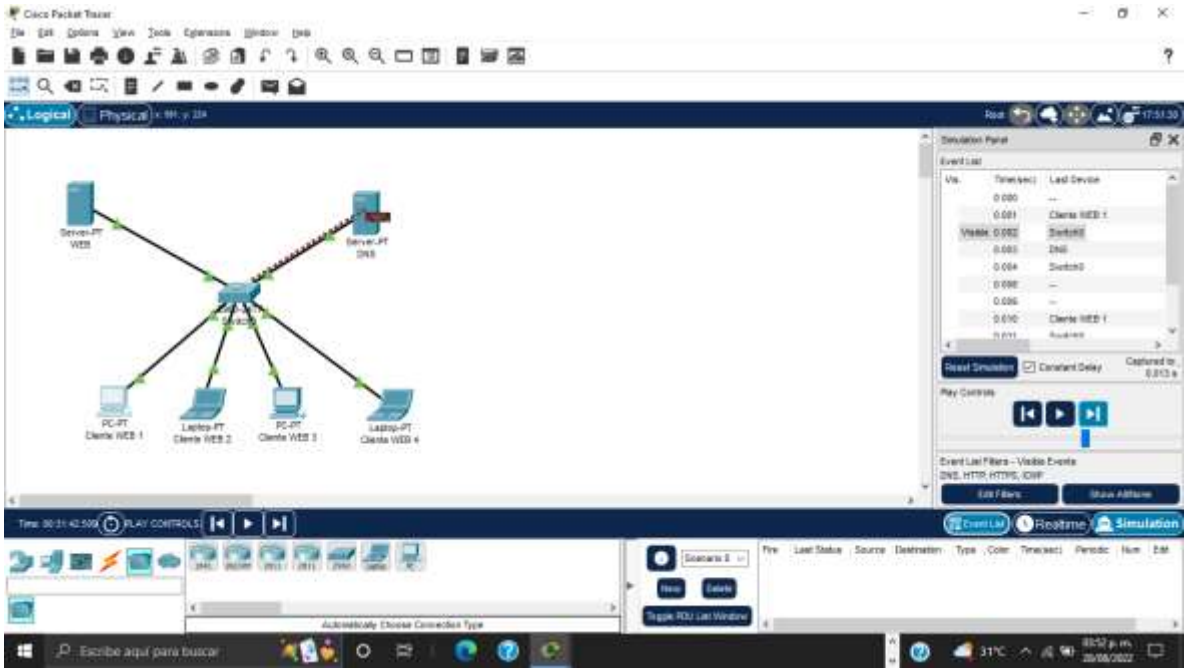


Posteriormente ingresamos a la primera PC para ingresar al navegador e ingresar la dirección de la red local creada www.redlocal.com

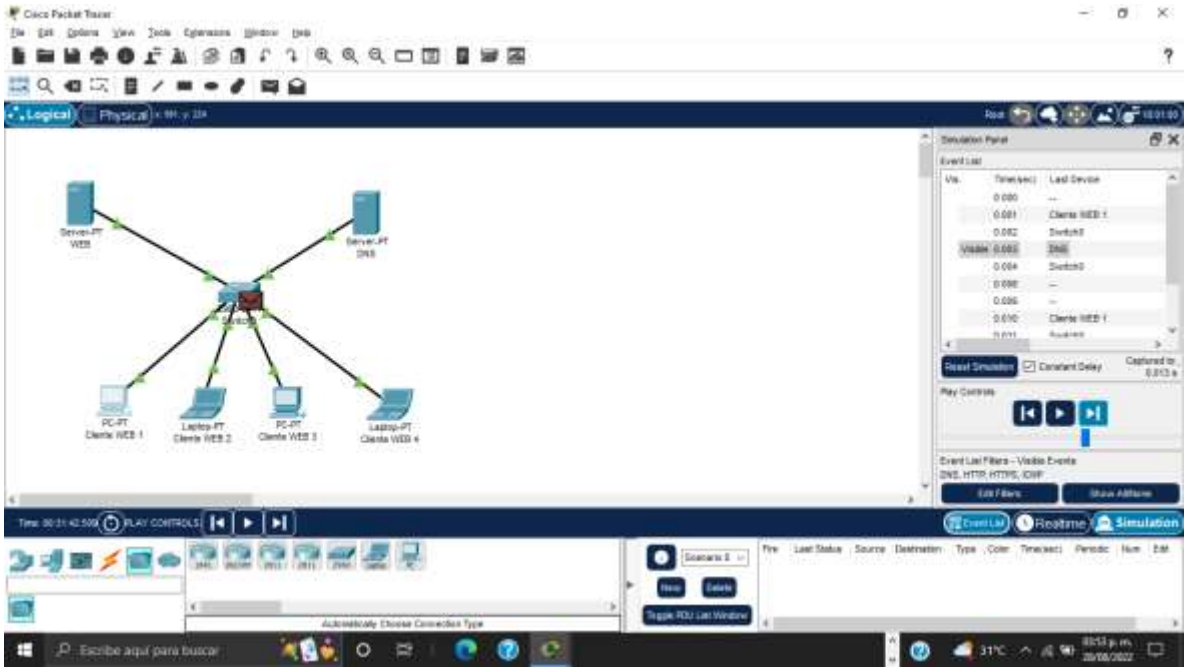




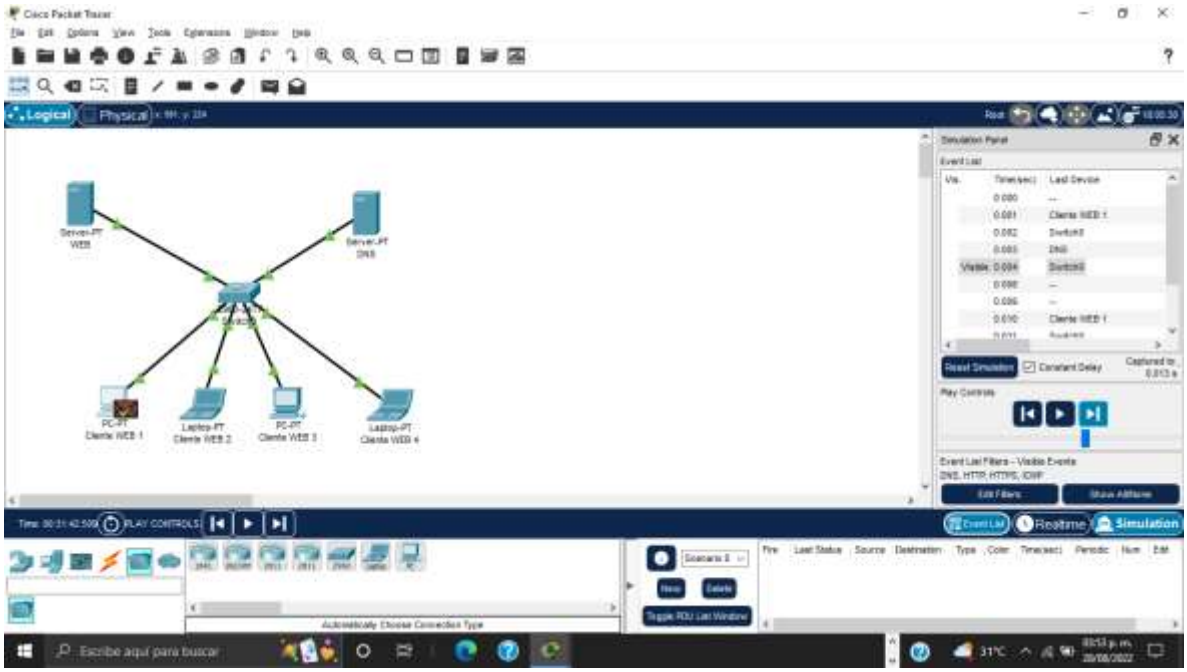
Se envía la solicitud al switch



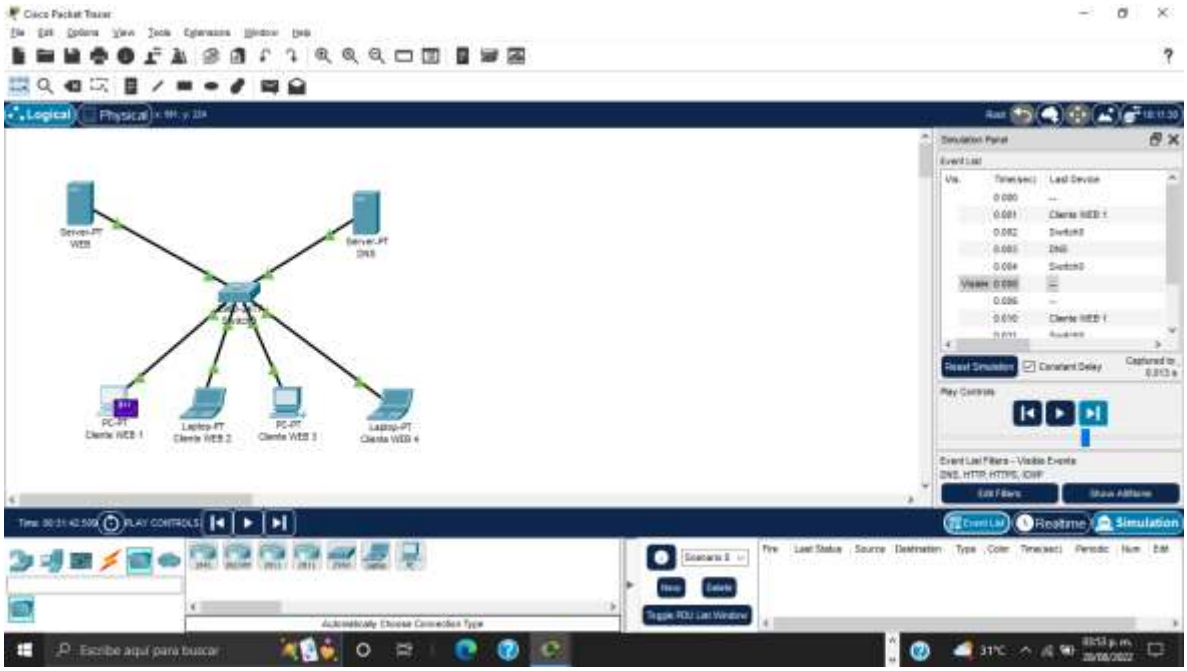
Este la envía al servidor DNS para validar que sea de la misma red

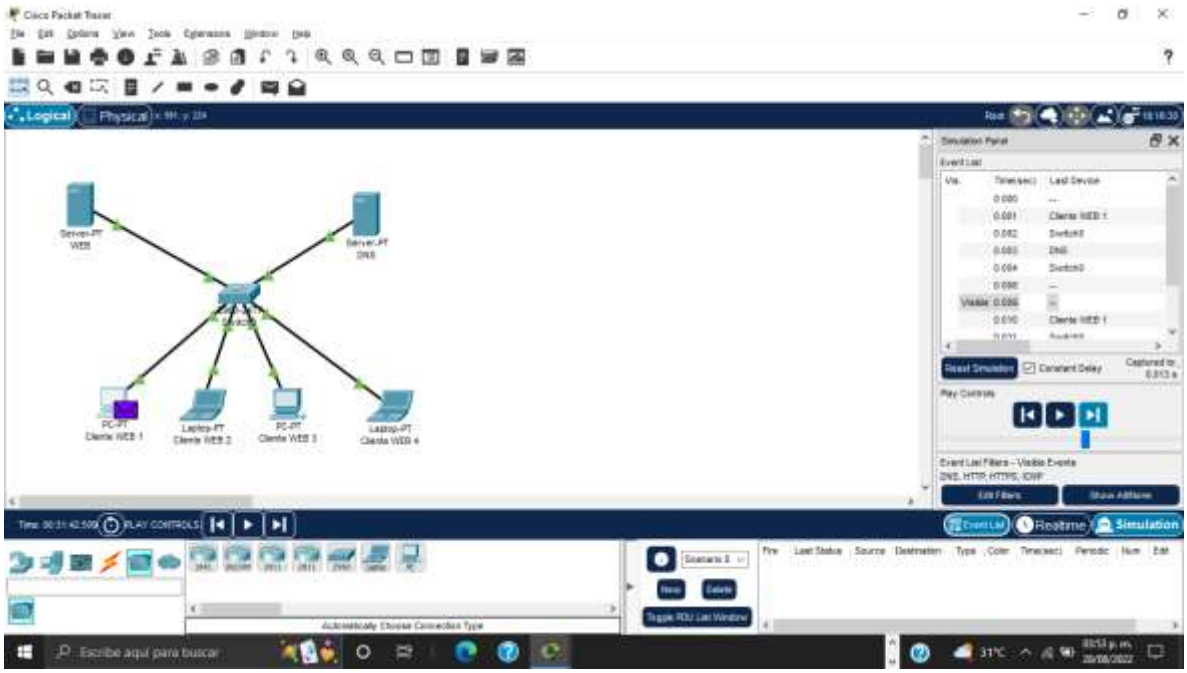


El switch recibe la confirmación por parte del servidor DNS

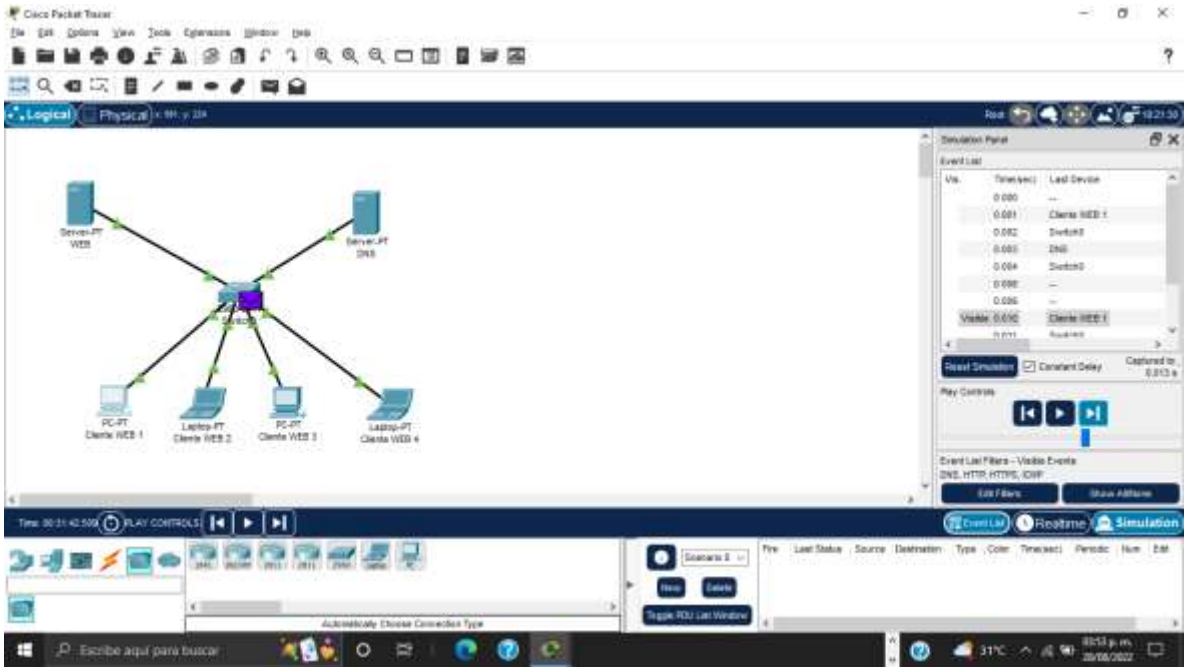


Recibe la confirmación por parte del switch

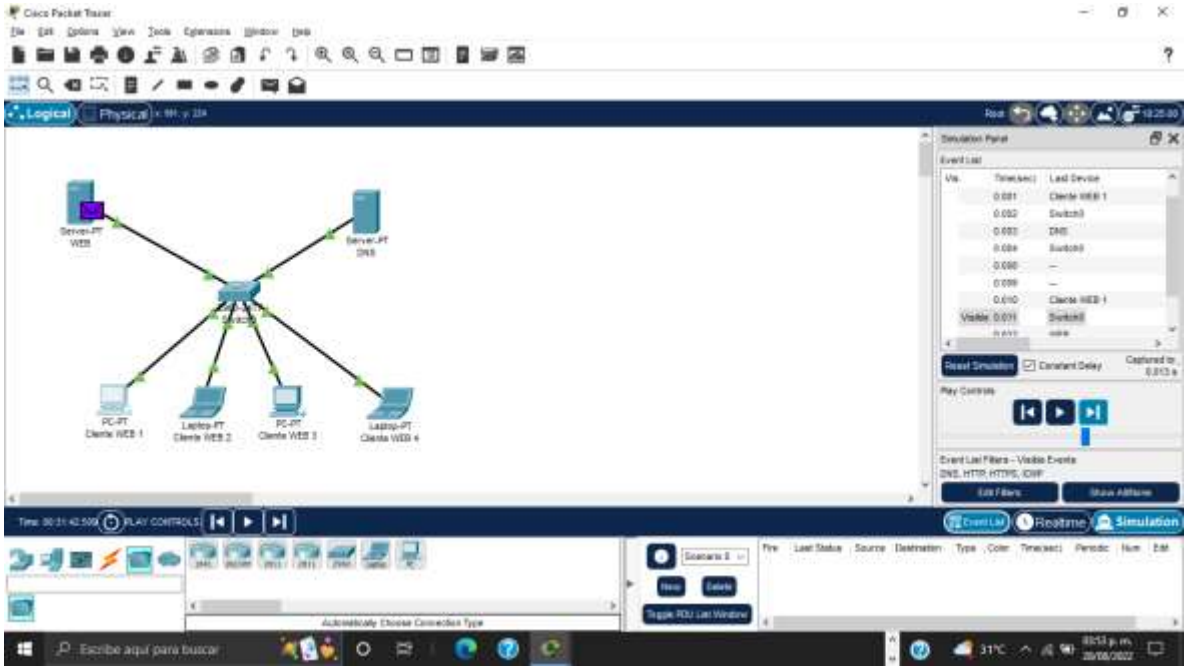




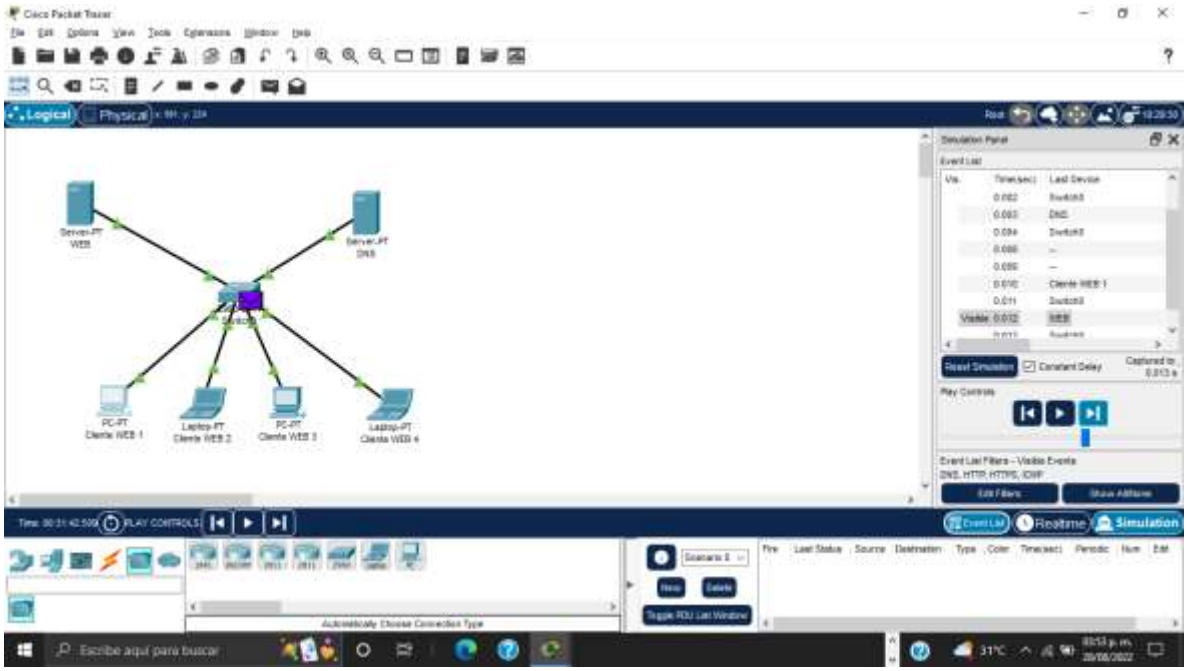
Una vez validado se envia el mensaje al switch



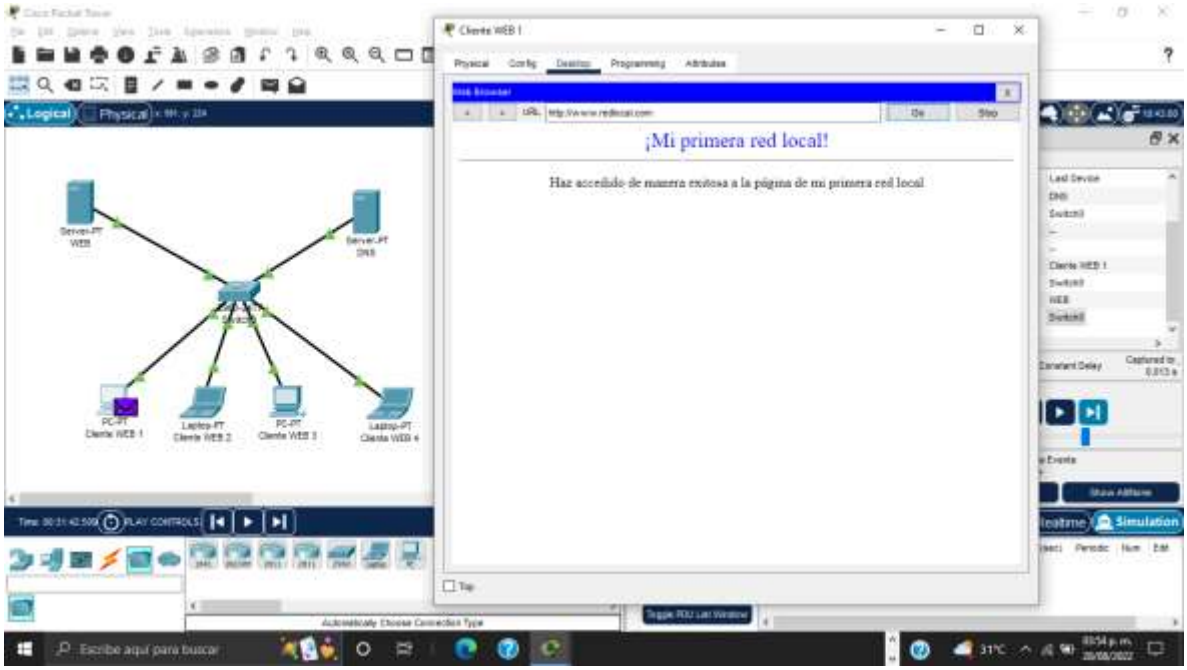
Y este lo envia al servidor web



Este lo envia nuevamente al switch

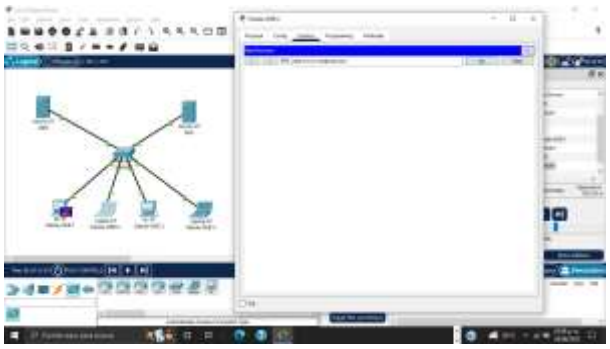


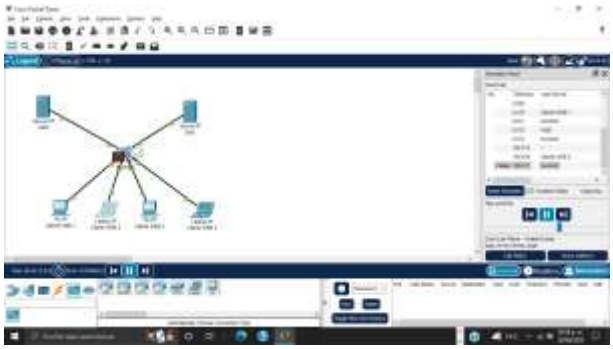
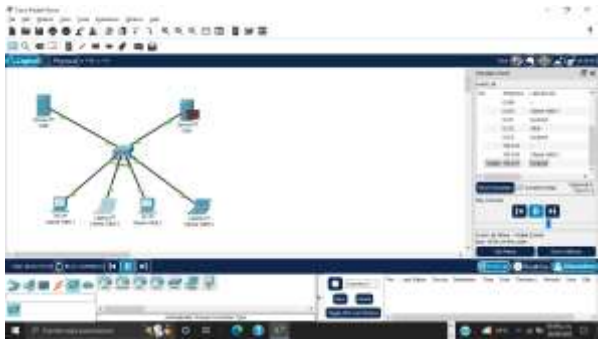
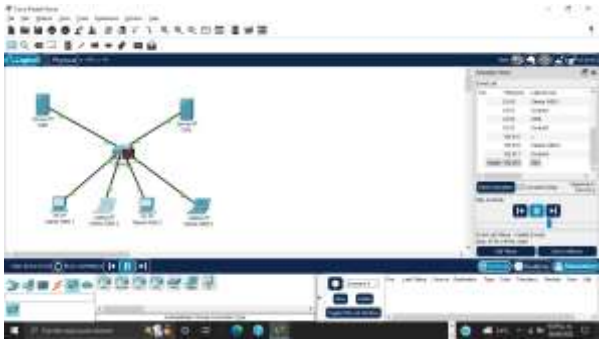
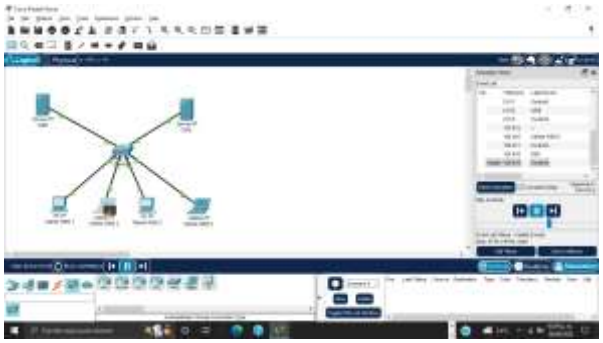
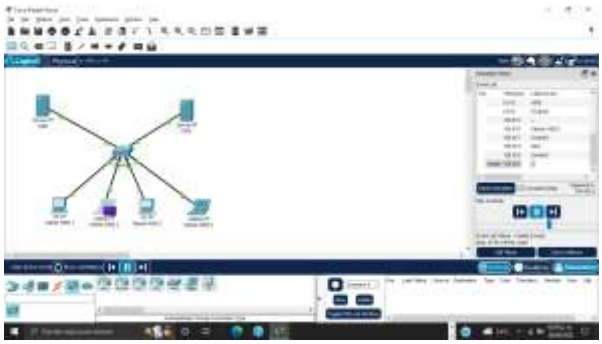
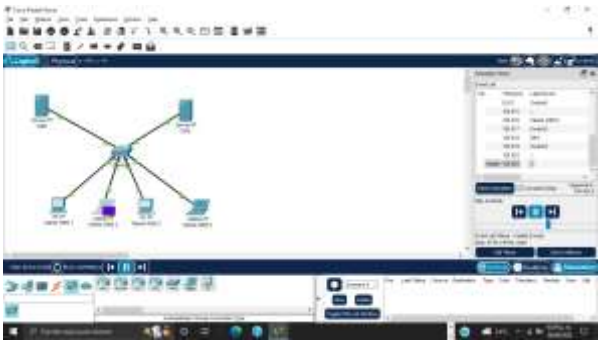
Recibe la respuesta y la envia al cliente

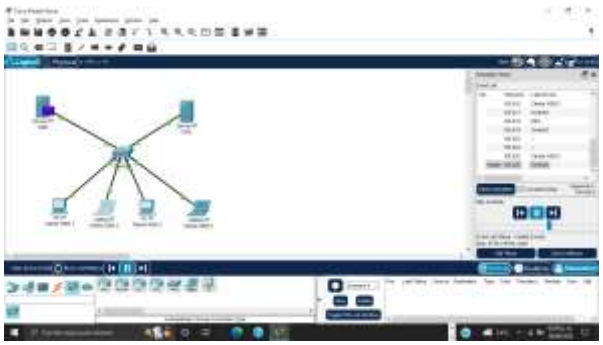


El cliente visualiza la información solicitada en su navegador.

Empezemos la solicitud del cliente 2.

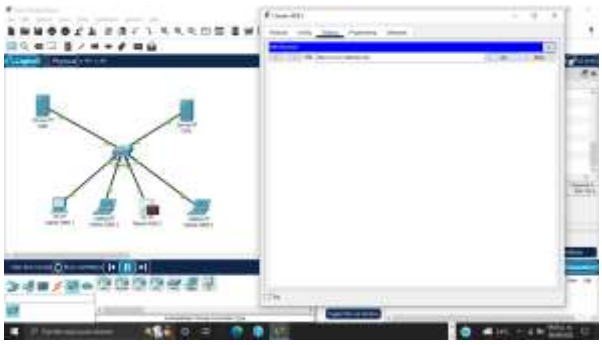


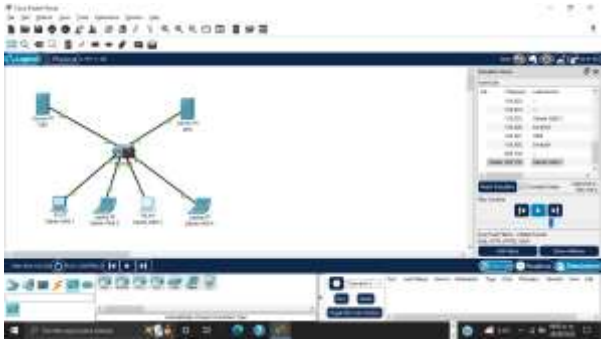







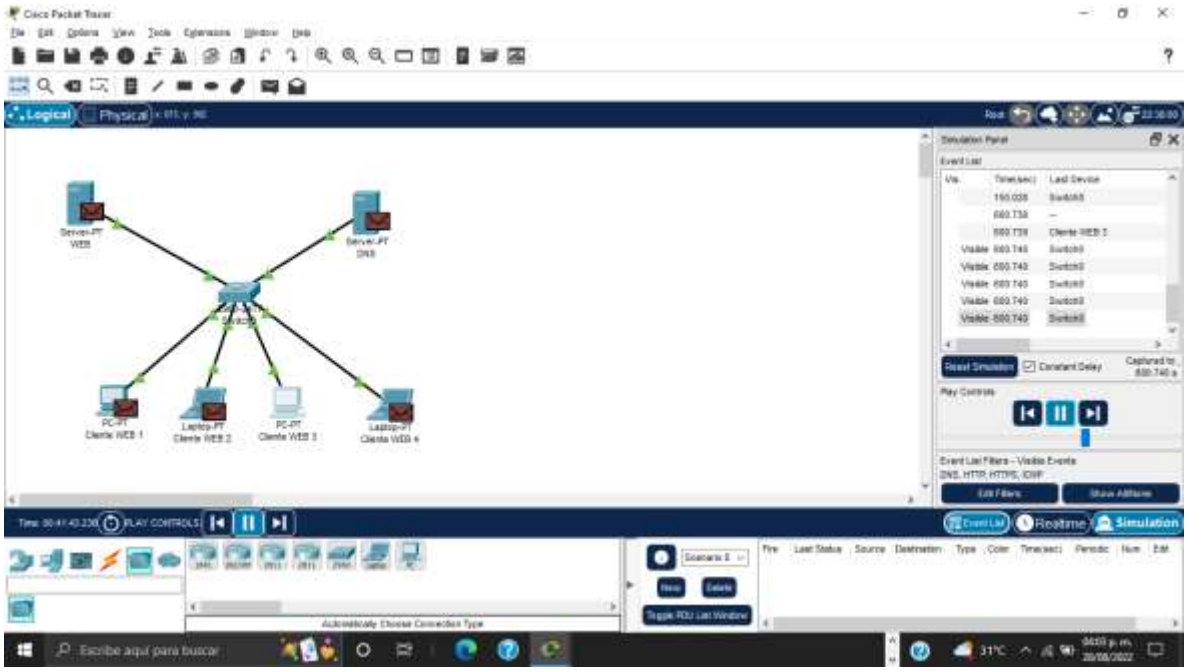


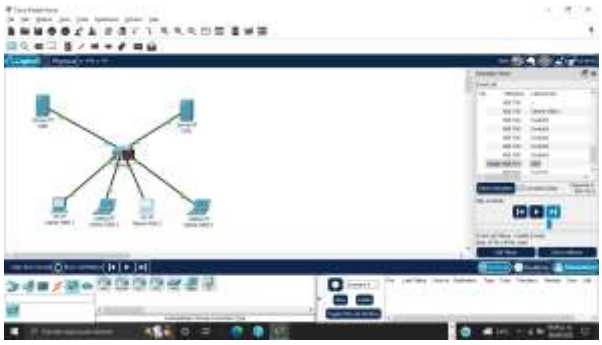
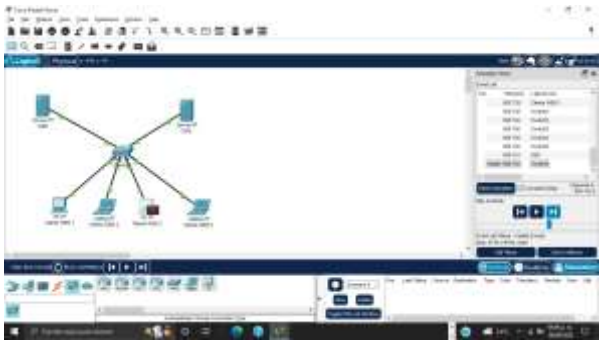
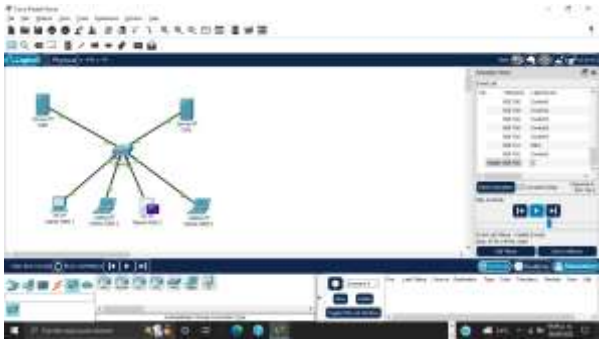
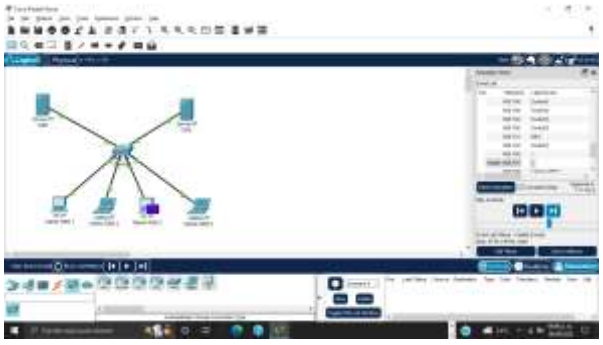
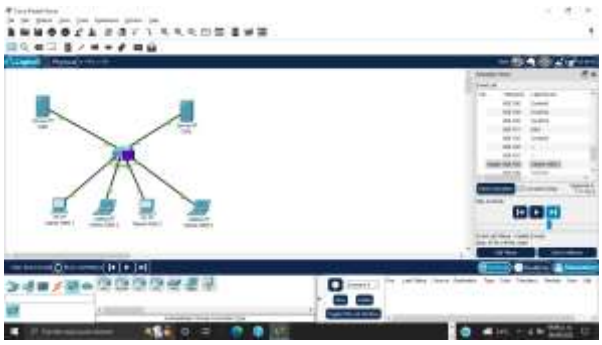
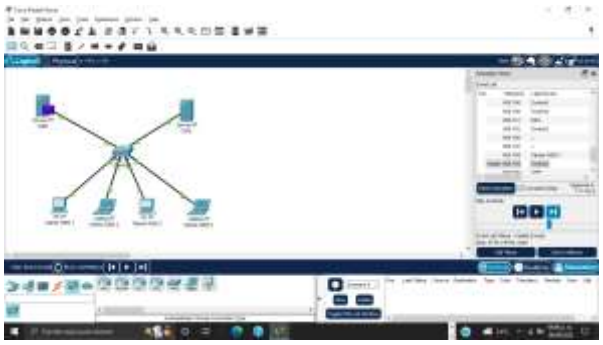
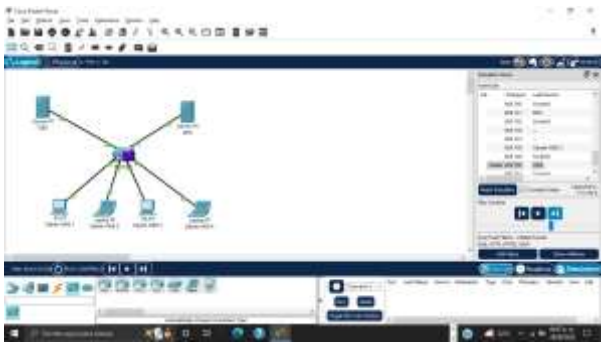

¡Mi primera red local!

Empezemos la solicitud del cliente 3.



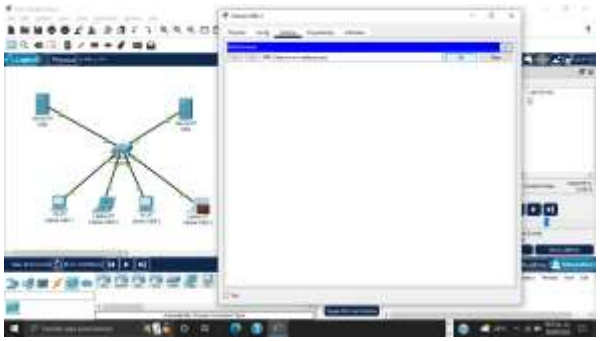
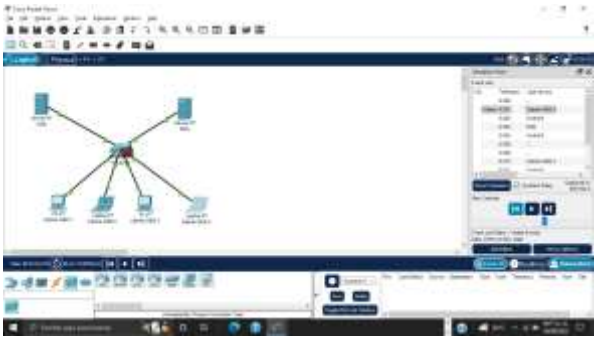
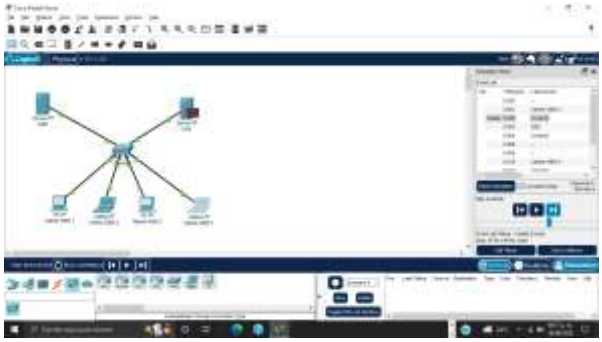
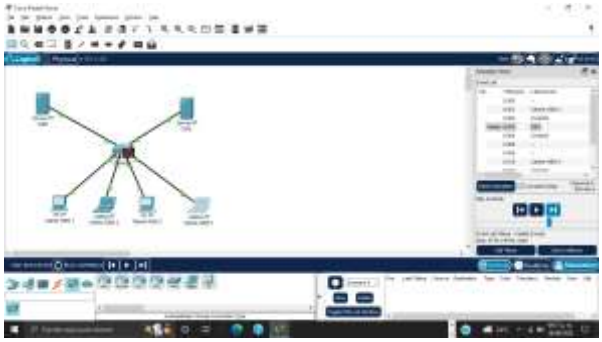
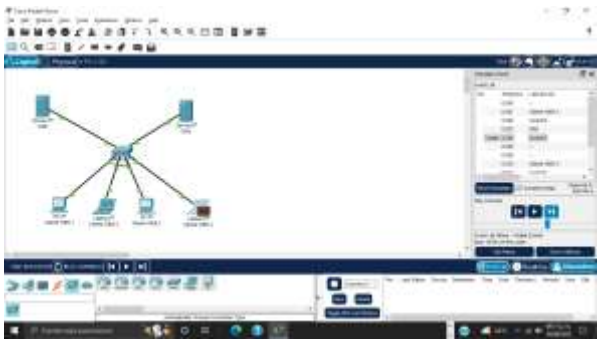
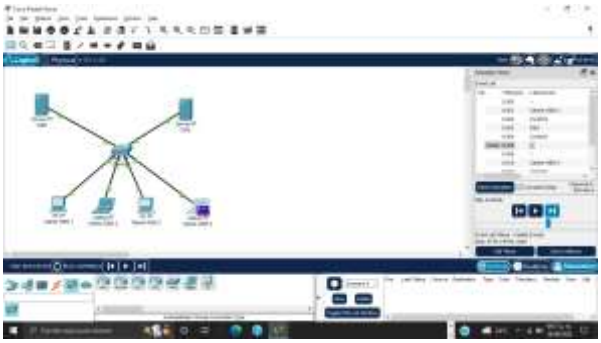
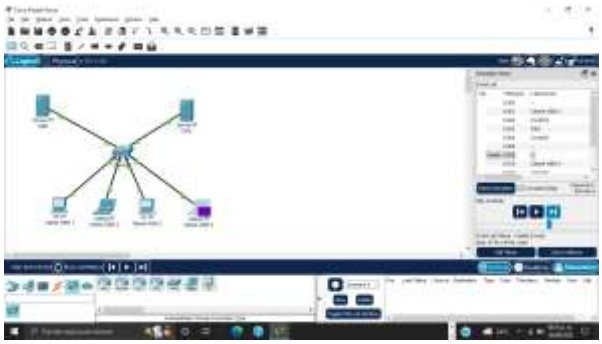
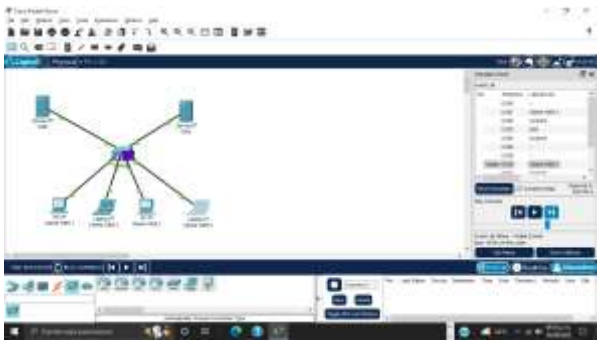


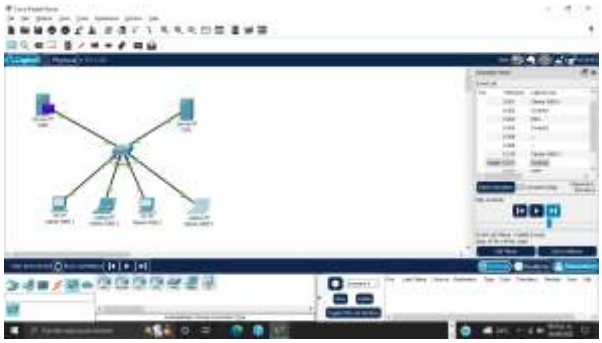


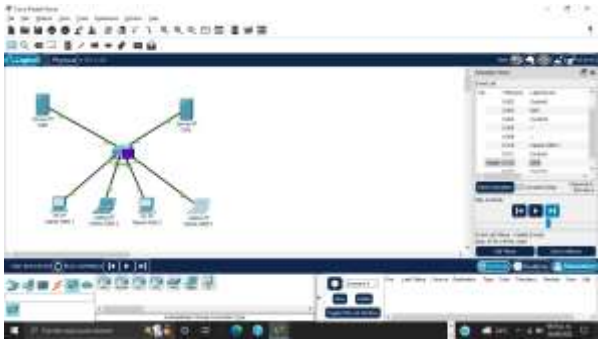








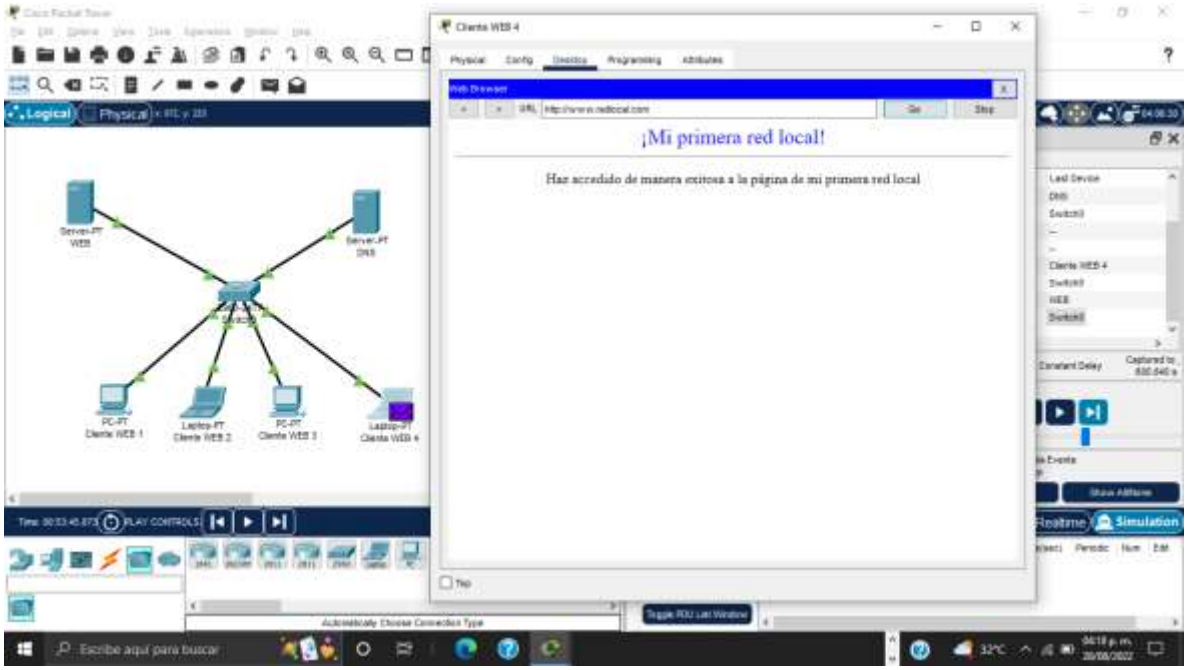
¡Mi primera web local!

Empezemos la solicitud del cliente 4.






Cliente WEB 4
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
Go
Stop
¡Mi primera red local!
Haz accedido de manera exitosa a la página de mi primera red local
Logical
Physical
Server-PT
WEB
Server-PT
DNS
PC-PT
Cliente WEB 1
Laptop-PT
Cliente WEB 2
PC-PT
Cliente WEB 3
Laptop-PT
Cliente WEB 4
Realtime
Simulation
Escribe aquí para buscar

Preguntas

¿Entró al sitio web del servidor?

Si

¿Qué viste en la página de los Clientes Web?

La leyenda que se editó “Has accedido de manera exitosa a la página de mi primera red local”

¿Cómo funciona el envío de datos en DNS y HTTP?

Por medio de la validación de las IP, ya que al iniciar empieza por identificar que pertenezca a la misma red para así asegurar que el cliente pertenece a esta misma, una vez validada la información, envía la confirmación de regreso al switch para que el cliente pueda solicitarla al servidor web por medio del switch y el servidor envíe los datos solicitados por el cliente nuevamente por medio del switch para así poder visualizar el texto, imágenes o video solicitado por medio de la dirección web.

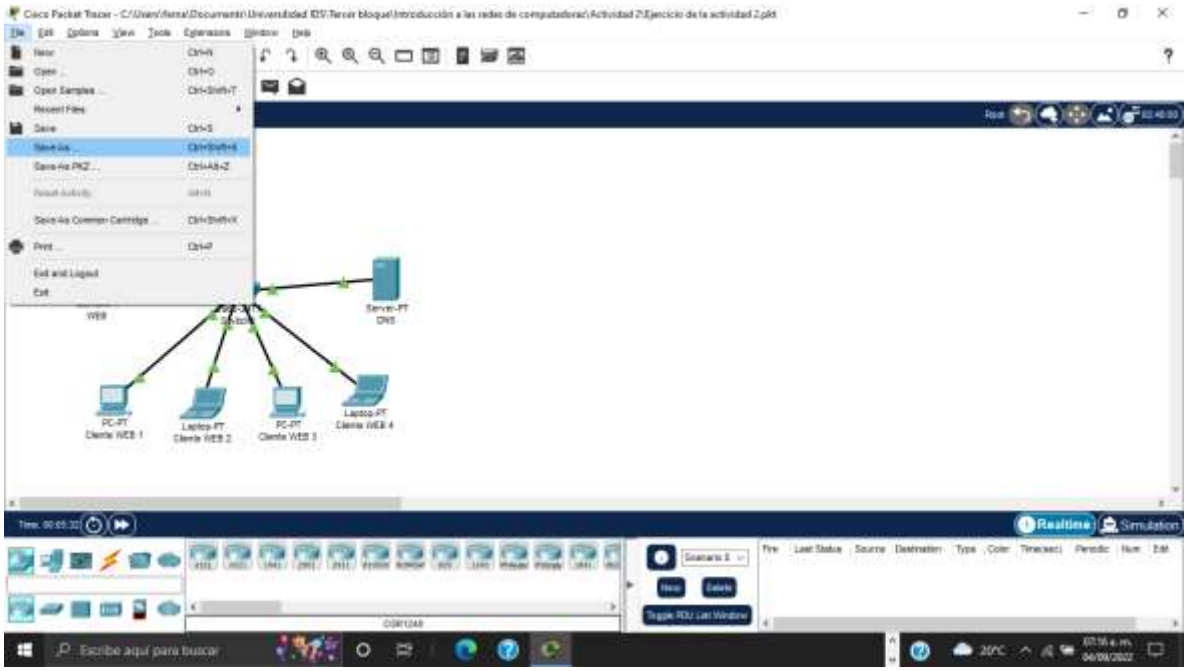
Conclusión

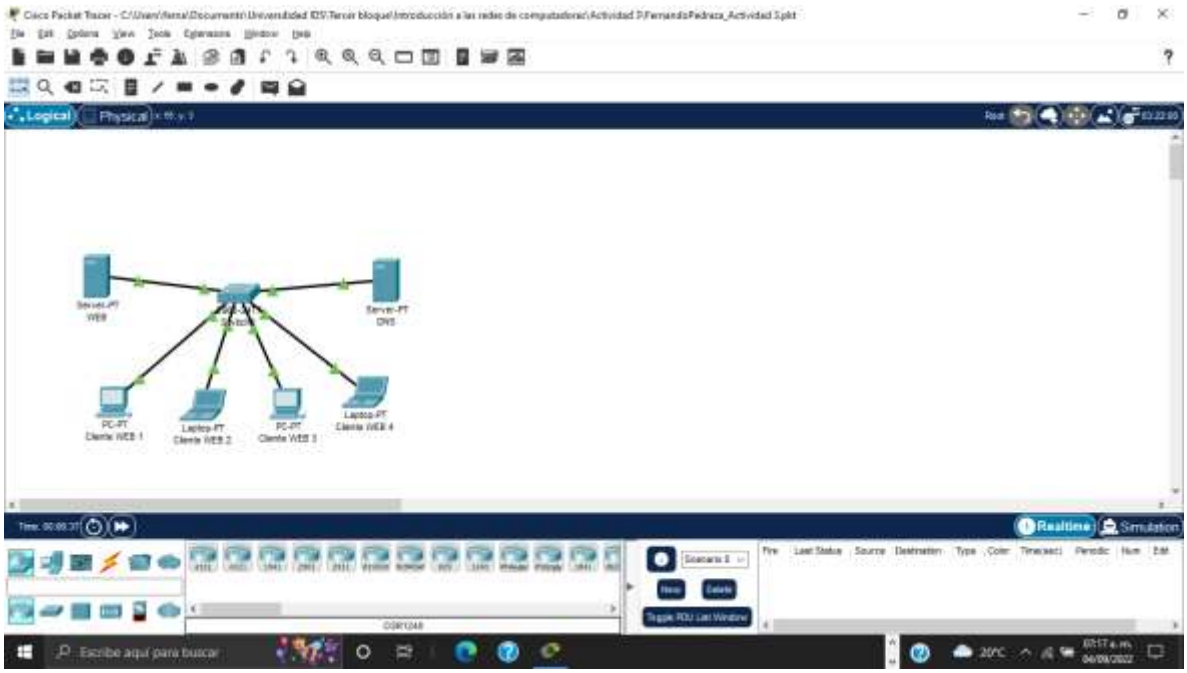
En esta actividad se pudo apreciar el camino que recorre una solicitud de una página web, desde el momento en que hacemos la solicitud de búsqueda desde el navegador hasta los servidores por medio del switch que funciona como intermediario entre los equipos. Así como la configuración de los servidores para que puedan validar de forma segura la transferencia de datos por medio de la configuración y asignación de las direcciones IP.

Introducción

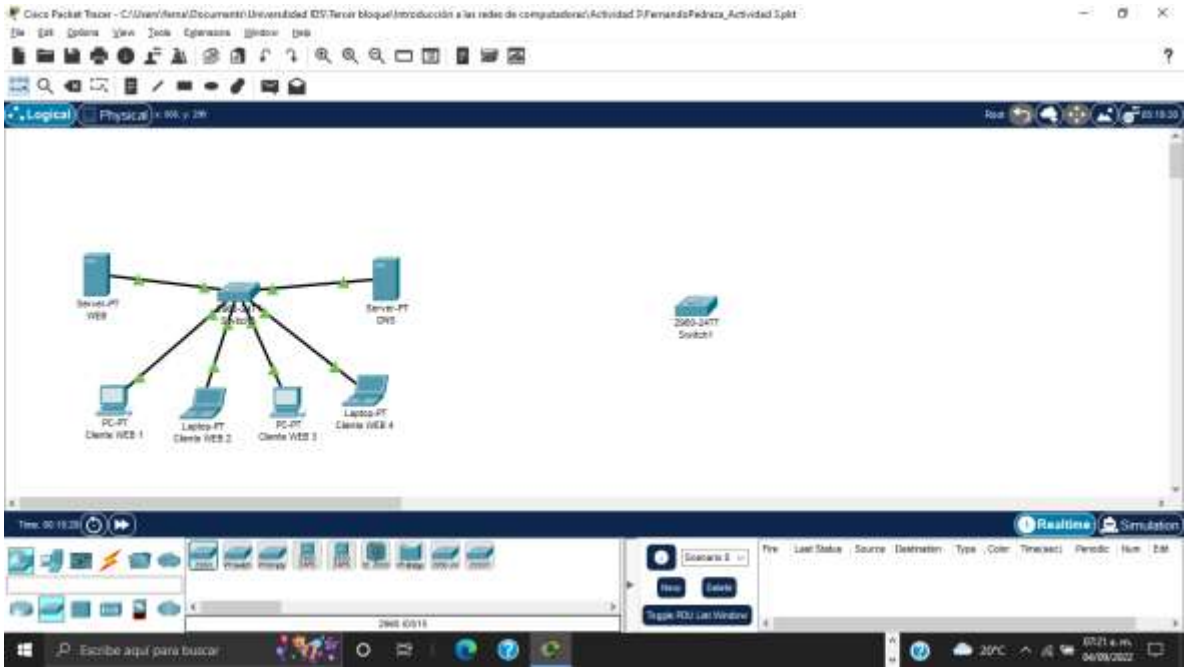
Continuando con las actividades, y en base a la actividad 2, ahora crearemos una nueva red LAN la cual deberá de comunicarse con la primera red LAN creada mediante un router.

Se creara una nueva Red LAN que se llamará zona verde, y la que ya estaba creada ahora será la zona rosa, estas dos redes deberán de tener comunicación y esto deberá lograrse mediante un router que se conectará a cada switch de cada zona. Se deberán configurar los equipos de la zona verde como indica la tabla de direccionamiento y también se configurará el router de tal manera que se pueda crear un Gateway o una Puerta de Enlace para lograr la comunicación entre ambas zonas.

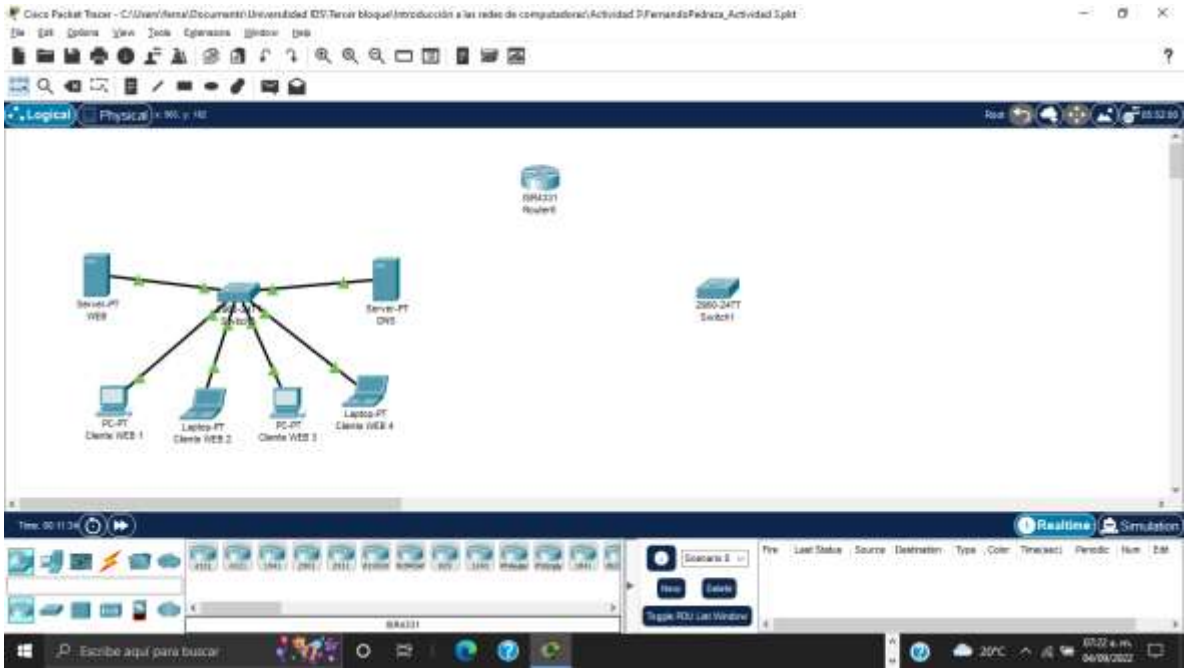




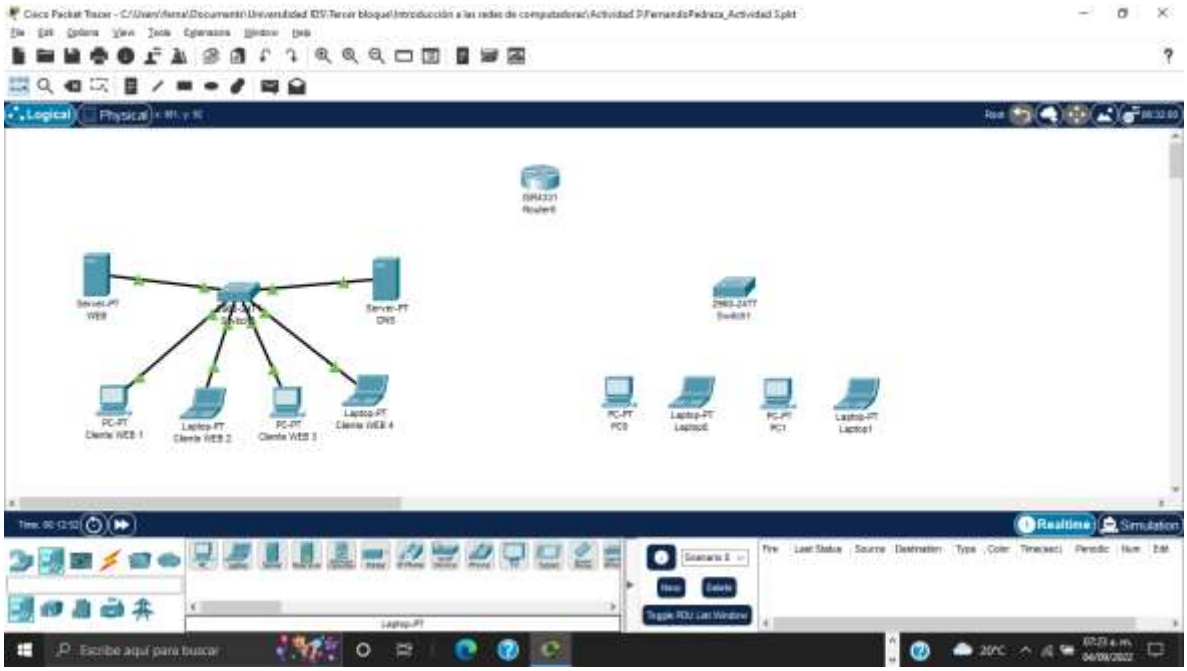
Partimos de la actividad 2 y guardamos nuestra actividad como NombreApellido_Actividad3.pkt



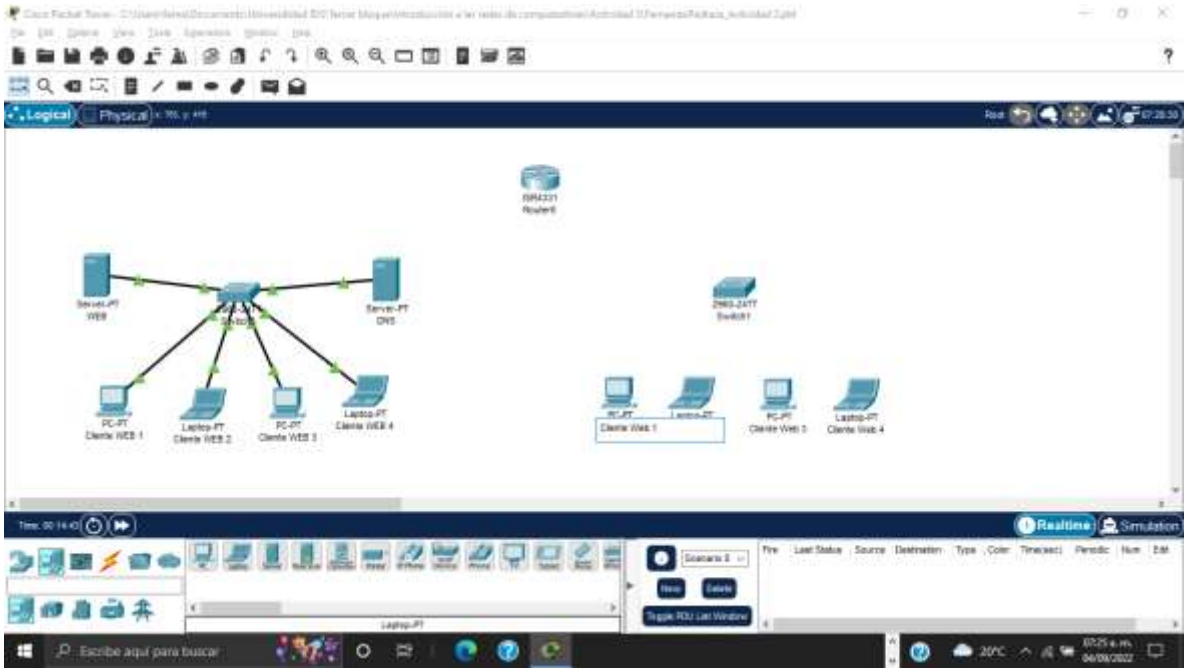
Empezamos por agregar un switch.



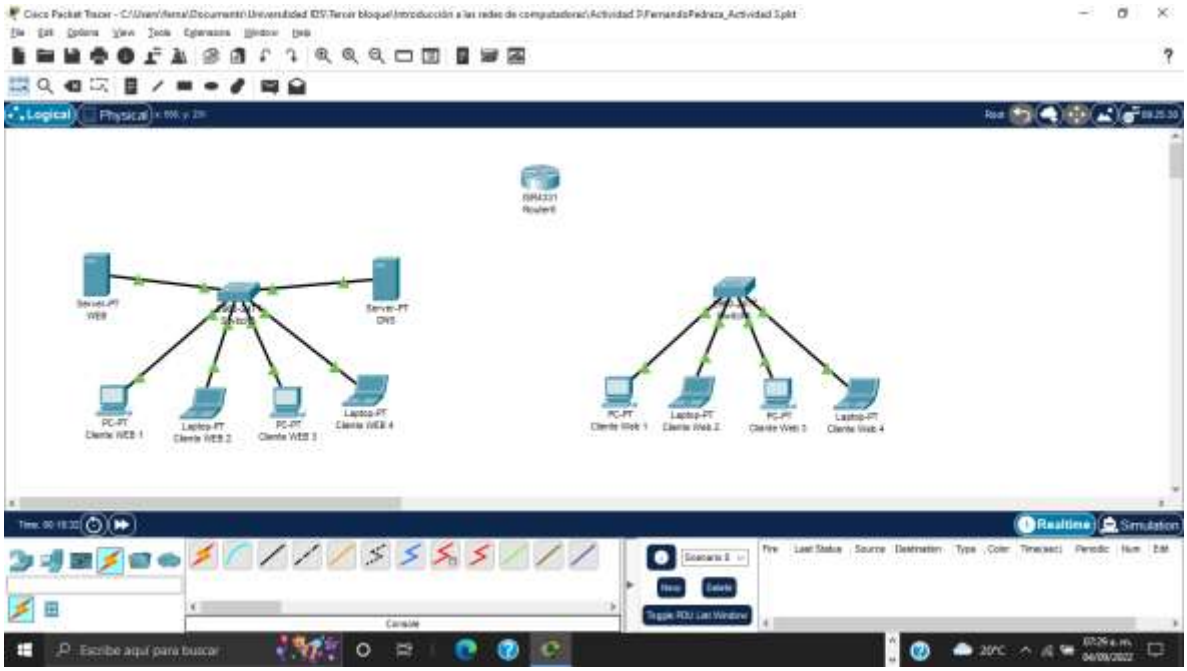
Seleccionamos el router a utilizar.



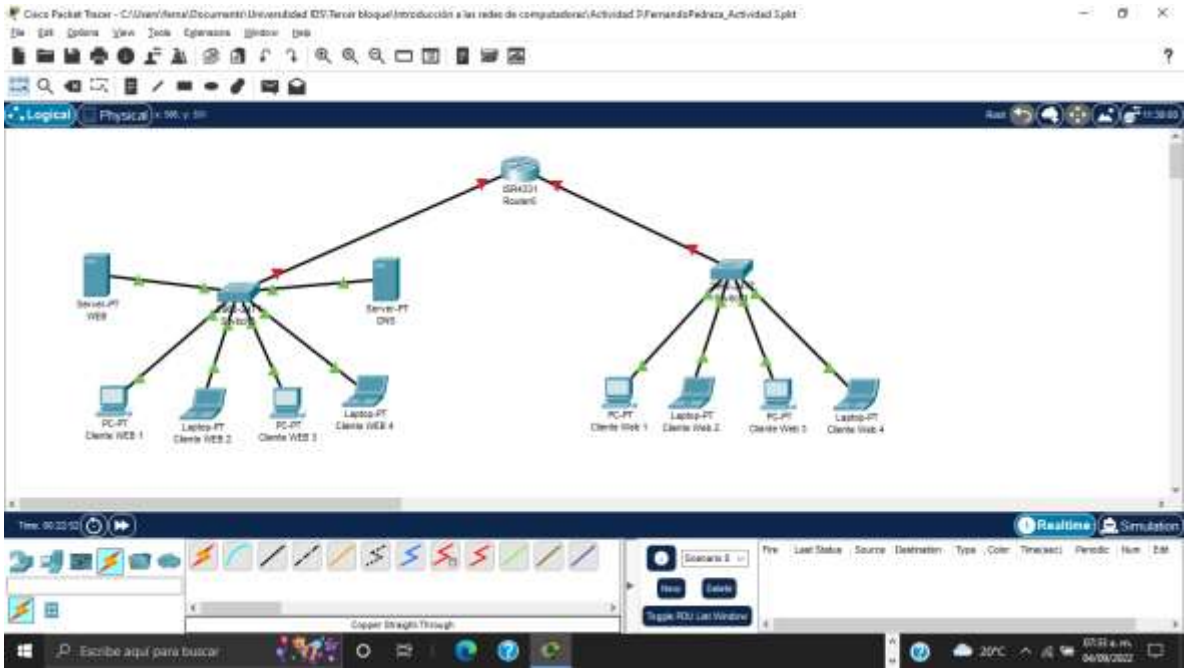
Agregamos nuestros dispositivos a conectar a la red.



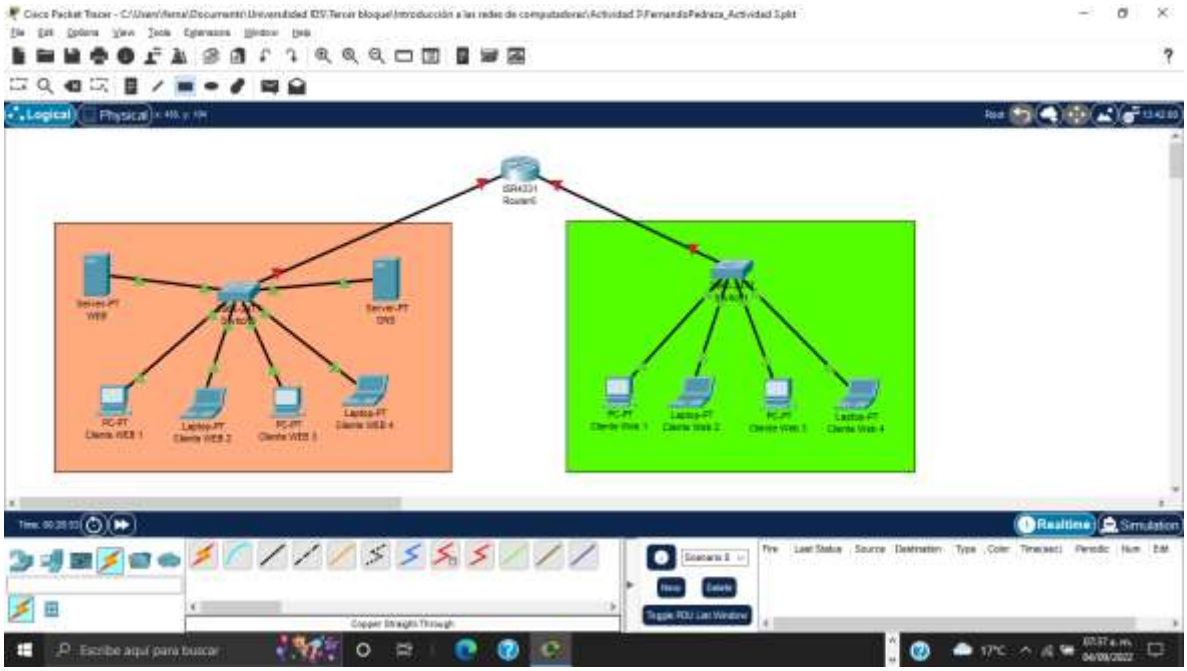
Renombramos nuestros equipos para poder identificarlos.



Conectamos nuestros equipos al switch.

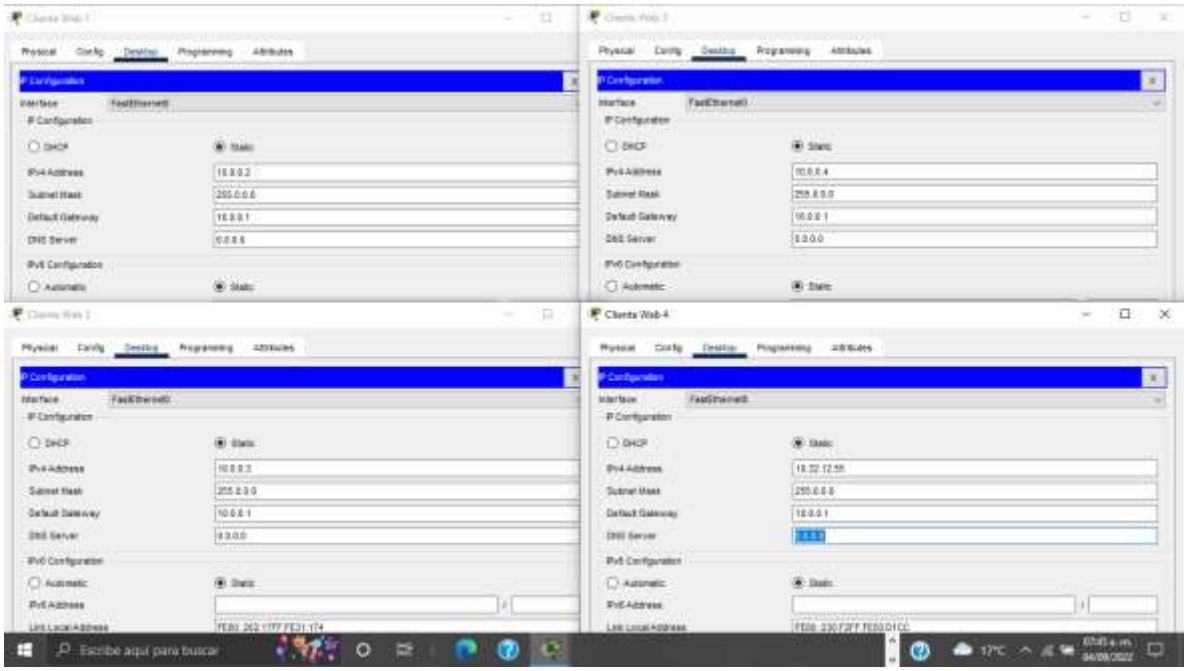


Conectamos nuestras redes al router por medio de las conexiones GigabitEthernet.

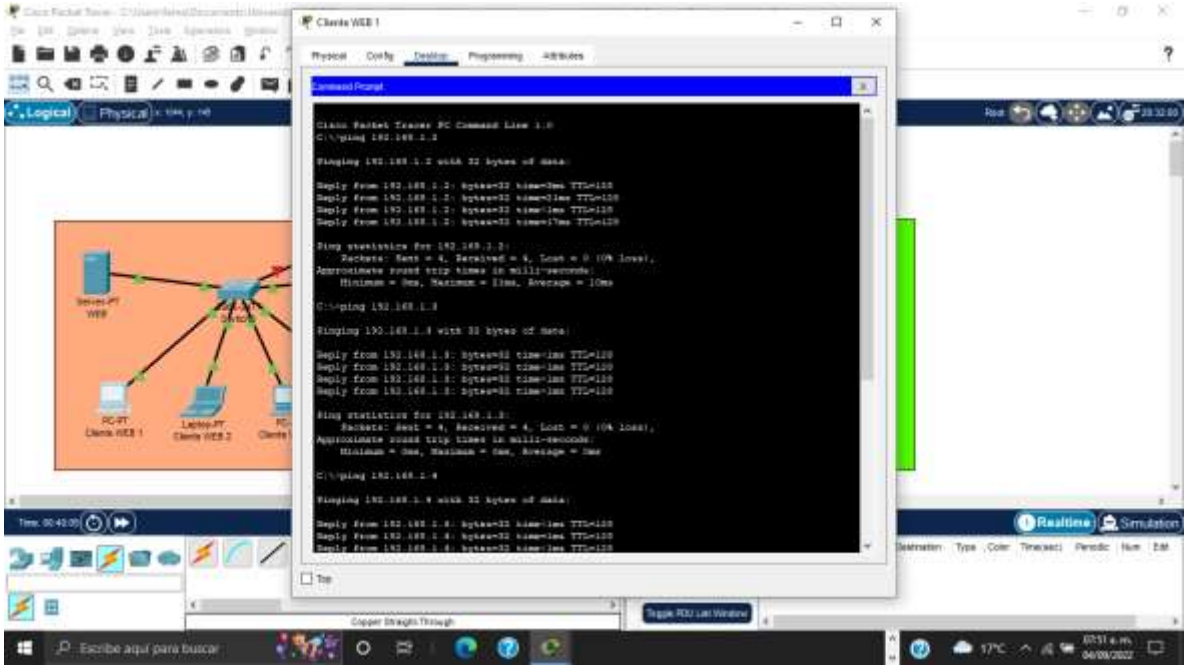


Identificamos nuestras redes.

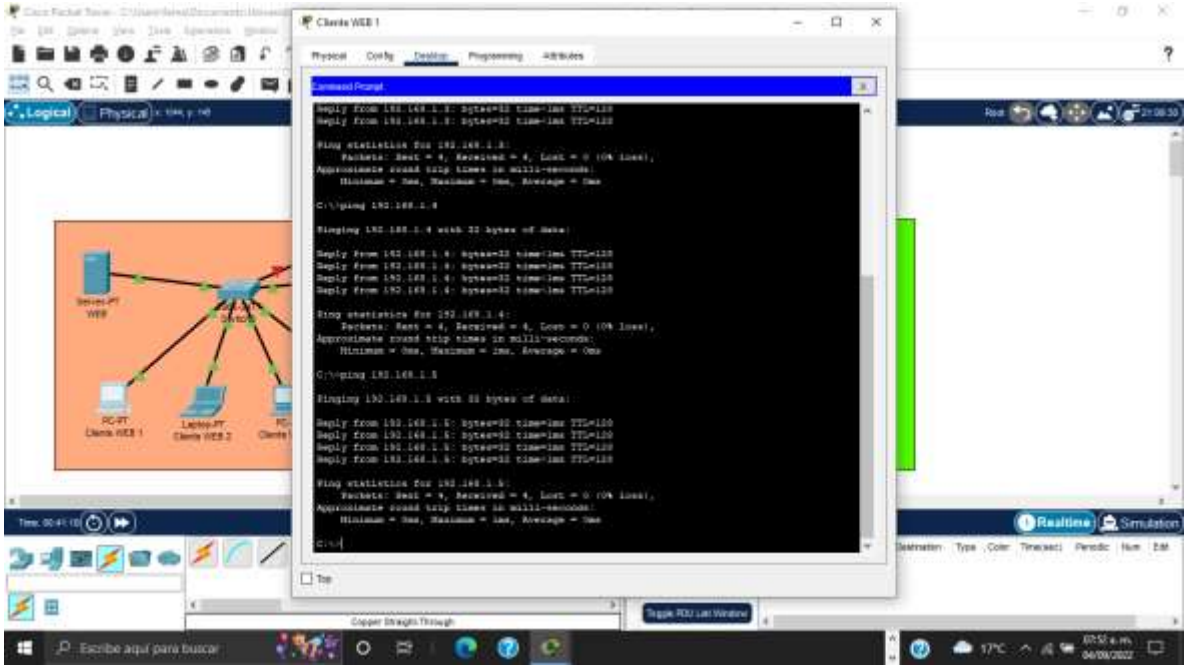
Continuamos con la configuración de direcciones IP de nuestros equipos para que tengan comunicación.

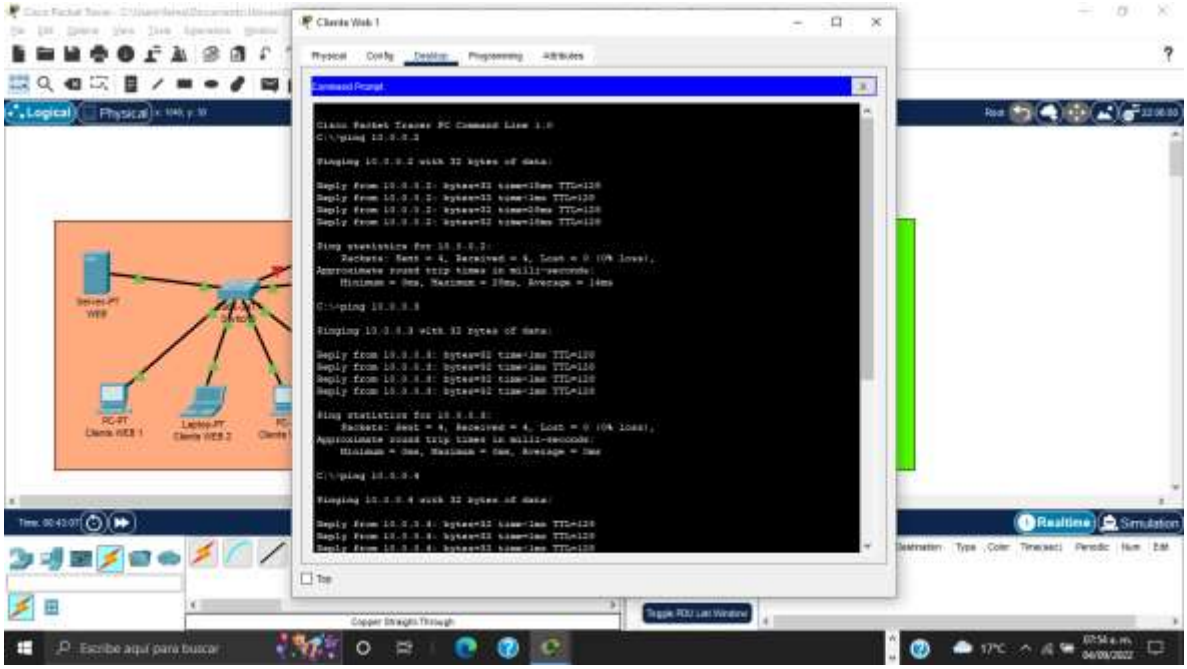


Asignamos las IP en base al requerimiento de la actividad.

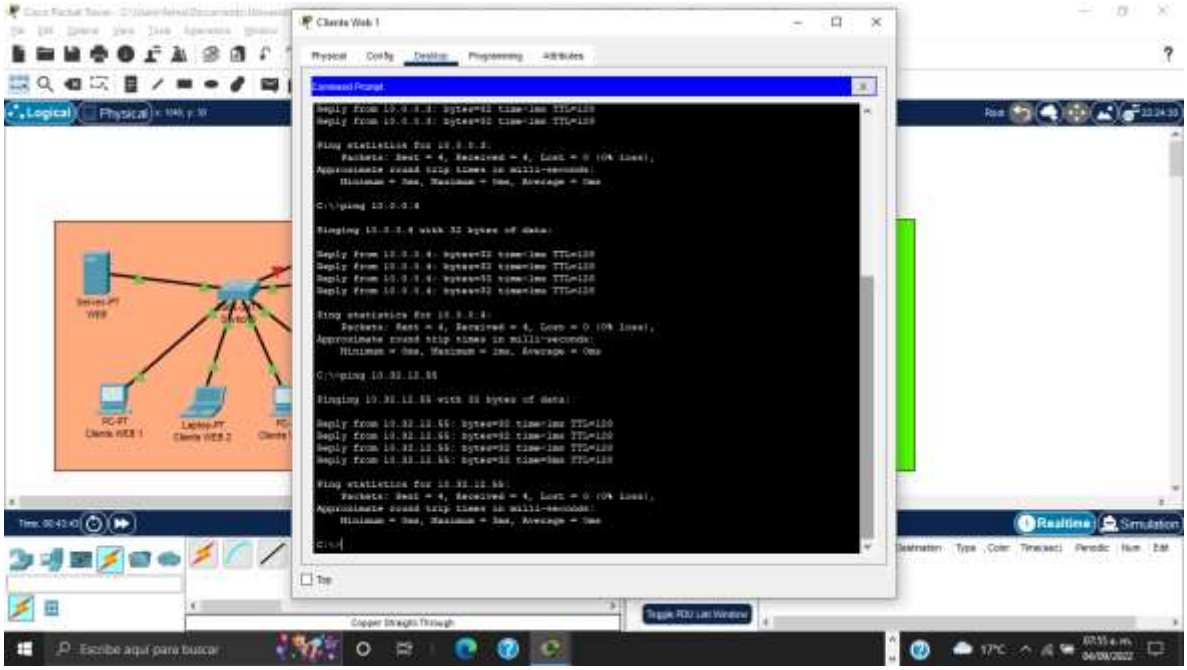


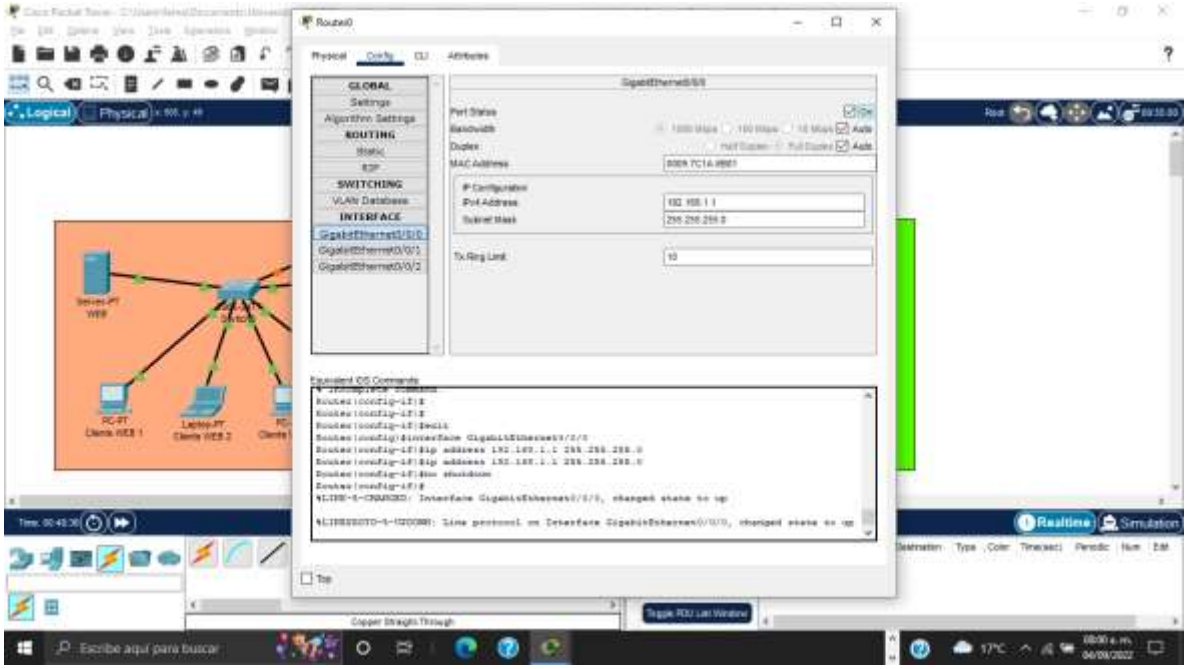
Hacemos ping a cada uno de los equipos de la red marcada en rosa para ver que tengan comunicación entre ellos.



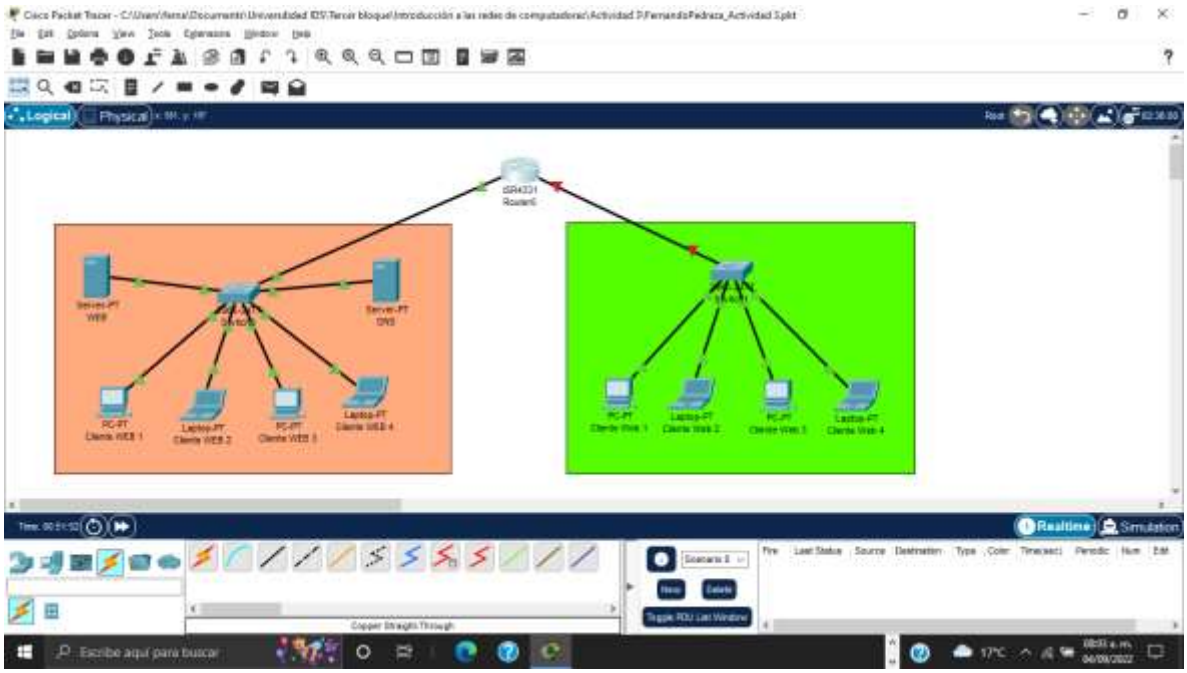


Hacemos lo mismo pero ahora con la red marcada en verde.

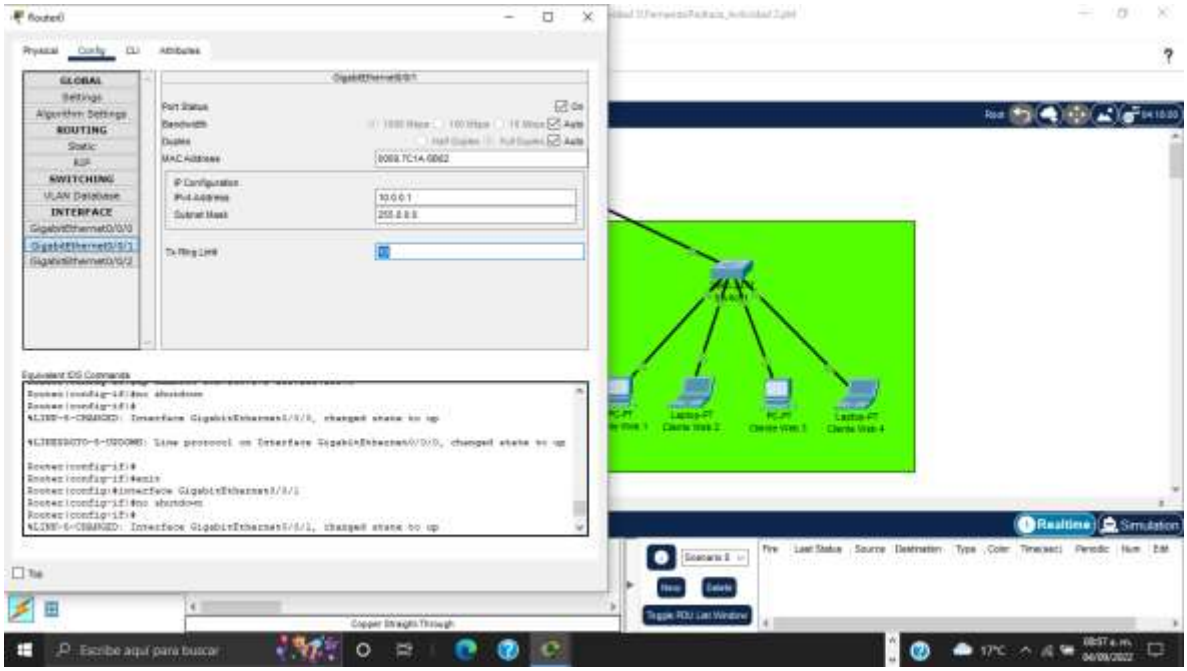




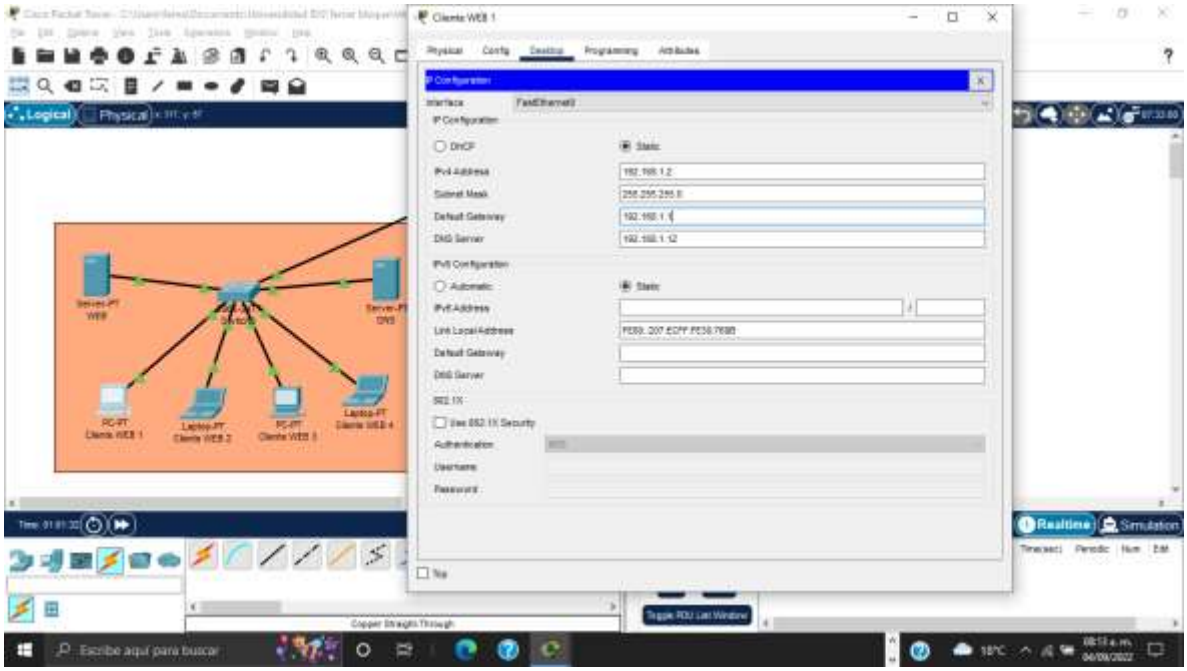
Asignamos la dirección IP 192.168.1.1 con la máscara de subred 255.255.255.0 que tendrá nuestro router para con la red marcada en rosa en la conexión GigabitEthernet 0/0/0 y lo activamos con On para que funcione.



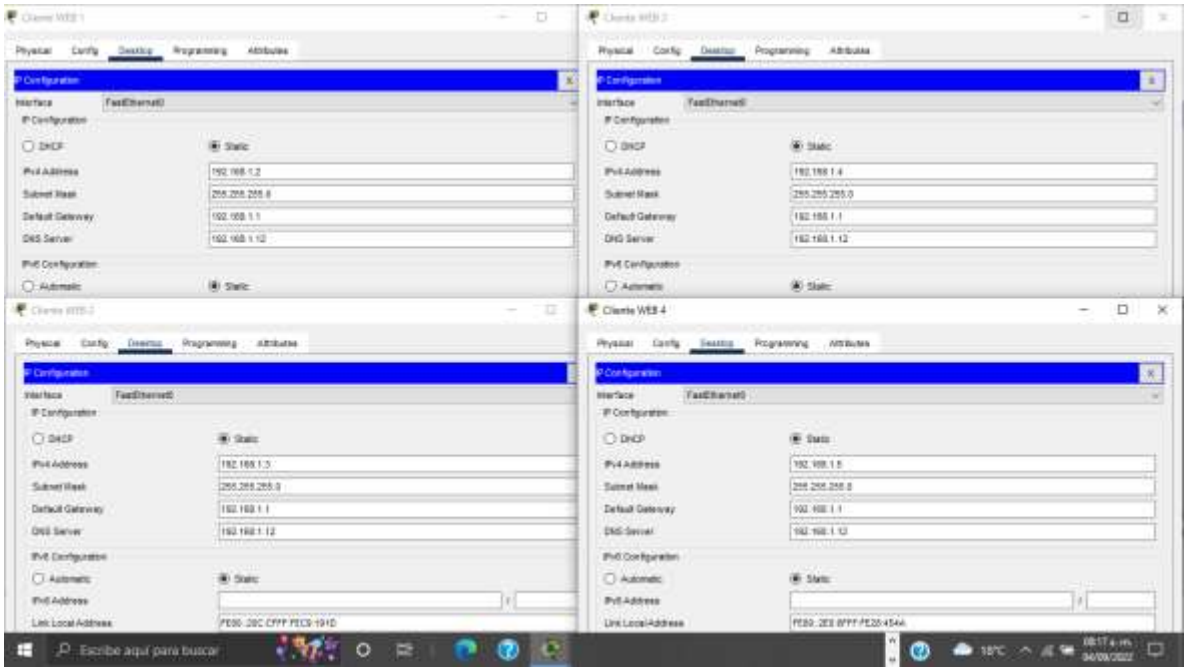
Nuestra línea ya tendrá comunicación al cambiar de color rojo a verde.

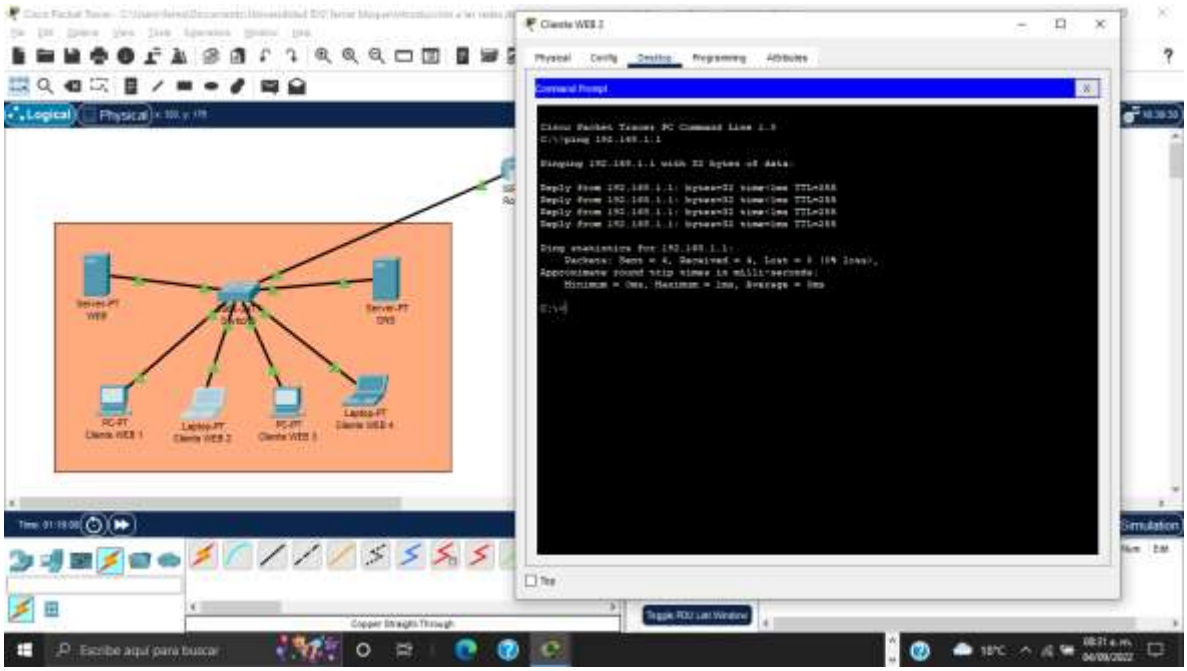


Hacemos lo mismo pero ahora con la red marcada en verde asignando la IP 10.0.0.1 con mascara de subred 255.0.0.0 en la conexión GigabitEthernet 0/0/1 y lo activamos con On para que funcione.

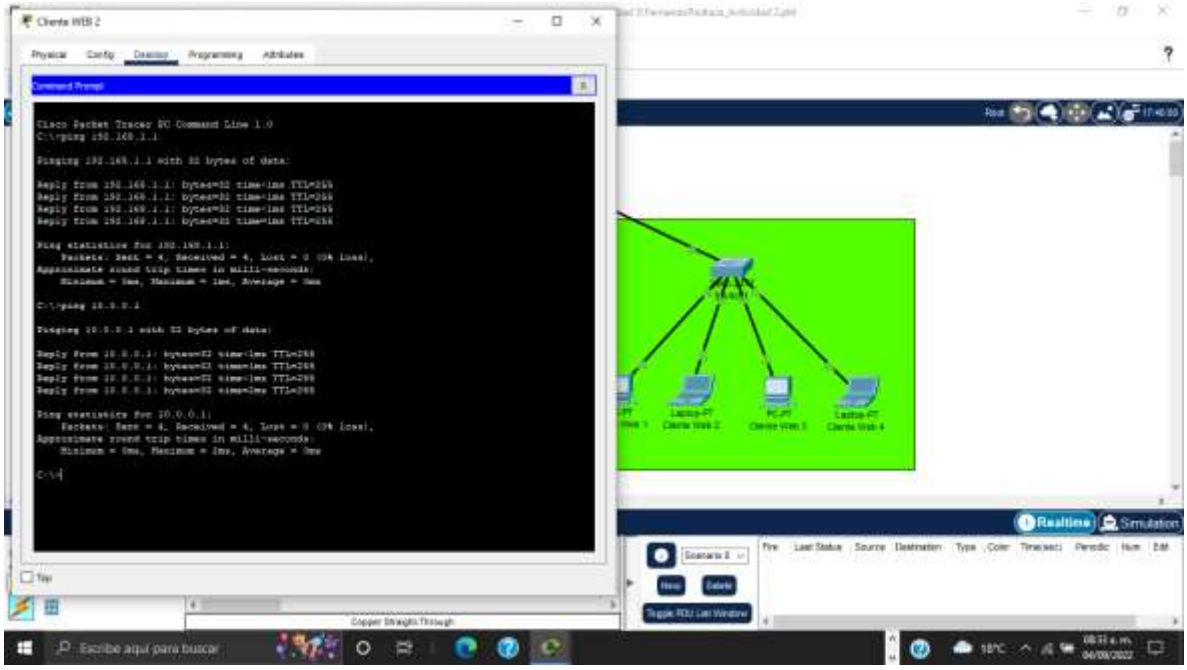


Posteriormente asignaremos la dirección IP 192.168.1.1 de nuestro portal a todos los equipos de la red marcada en rosa.

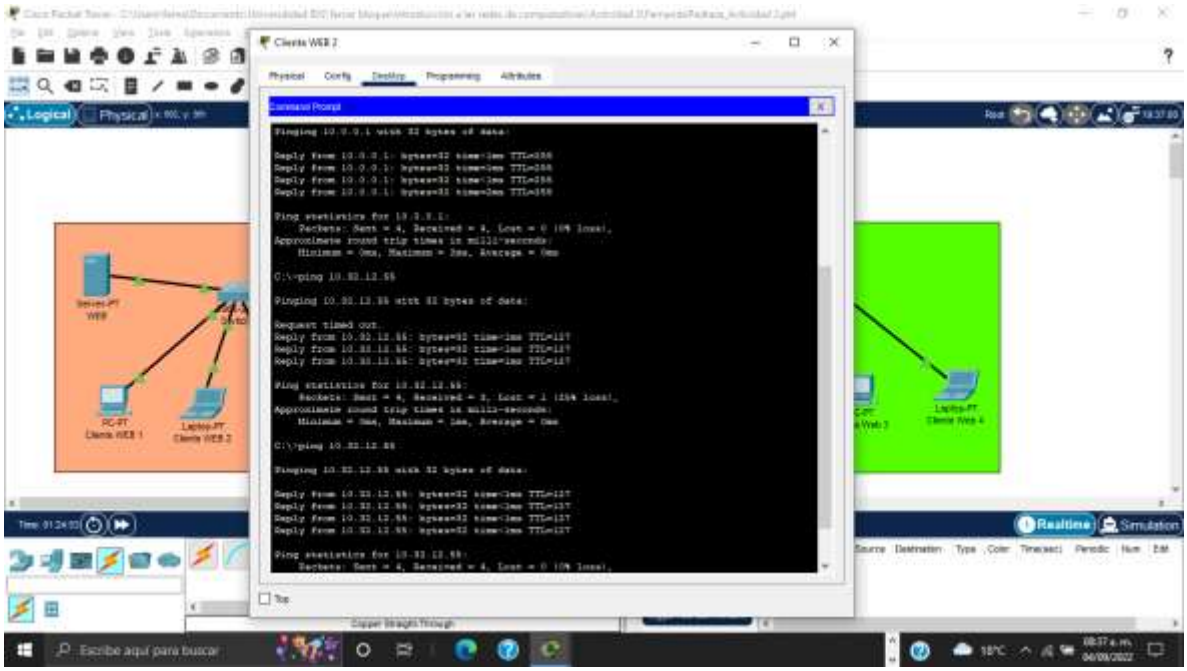




A continuación daremos ping desde cualquier equipo de la red marcada en rosa para ver si hay comunicación al router con la dirección IP 192.168.1.1

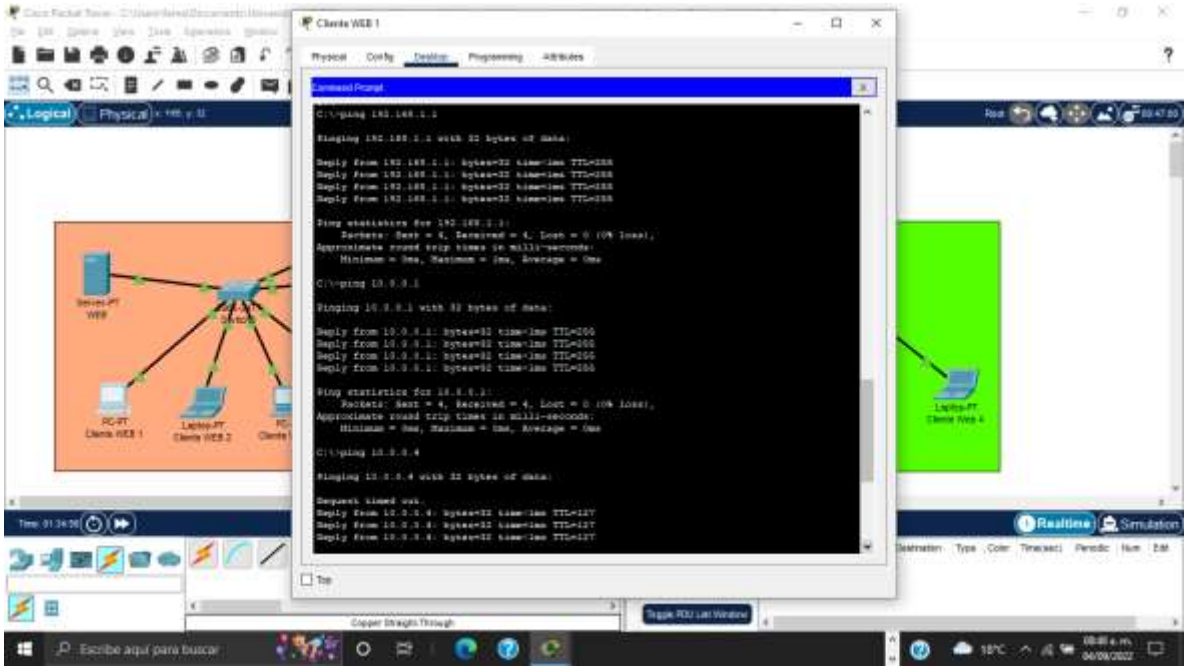


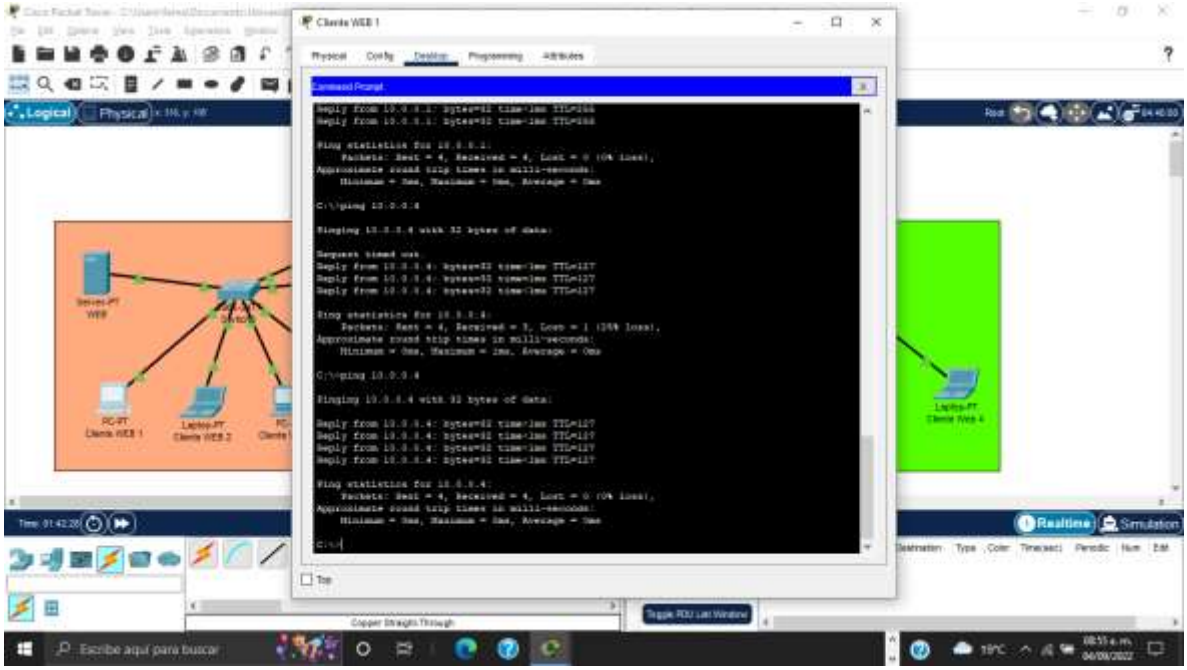
Ahora haremos lo mismo pero con la dirección IP 10.0.0.1

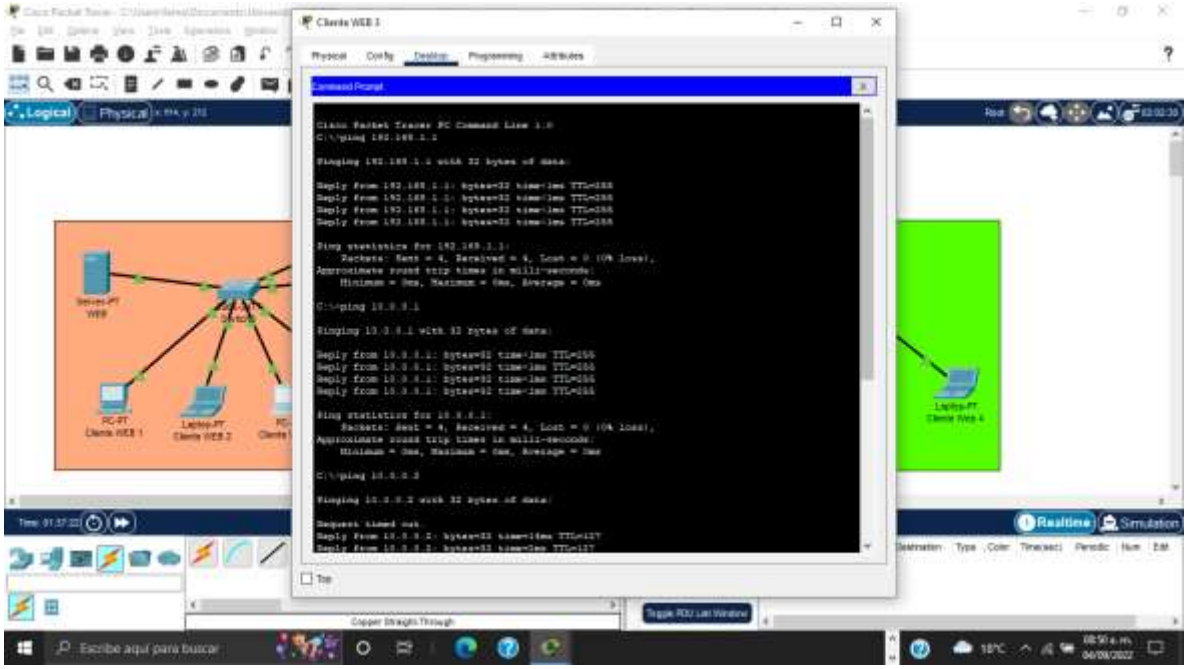


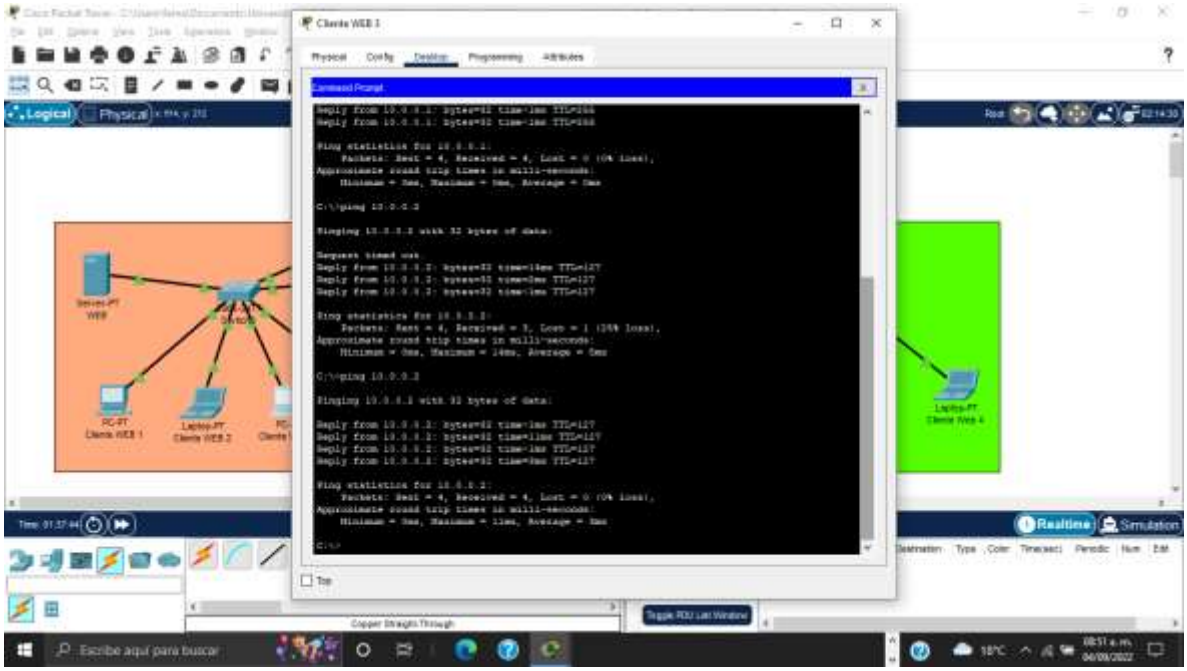
Y ahora lo haremos con cualquier equipo de la red marcada en verde.

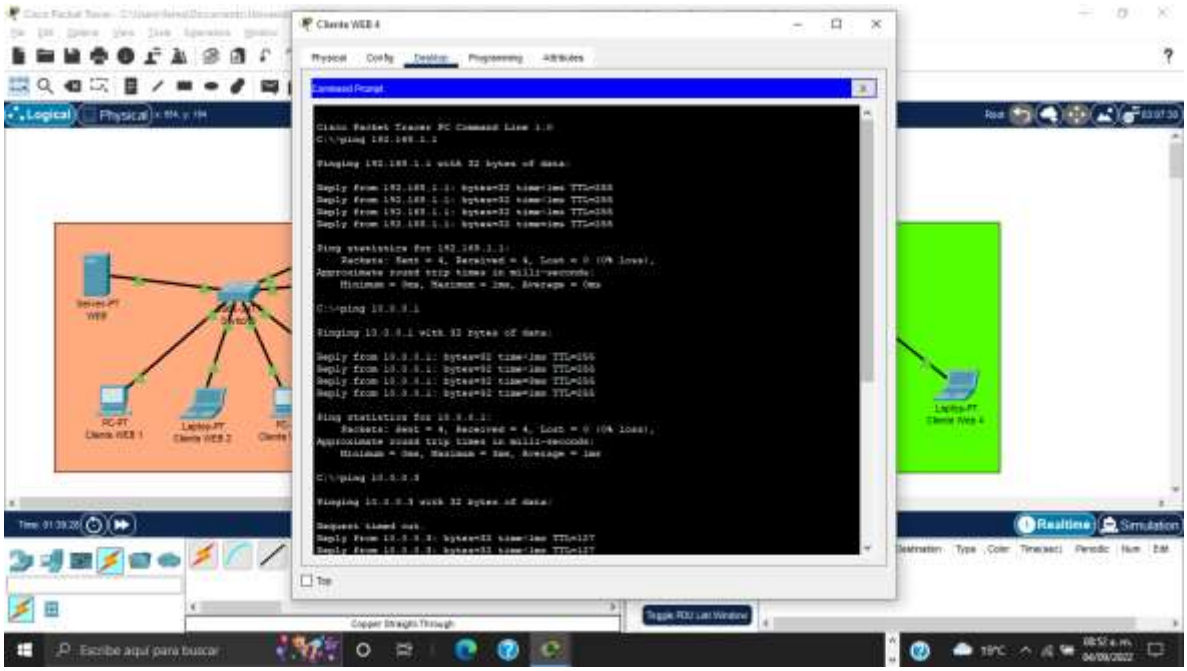
Hacemos lo mismo con el resto de clientes.

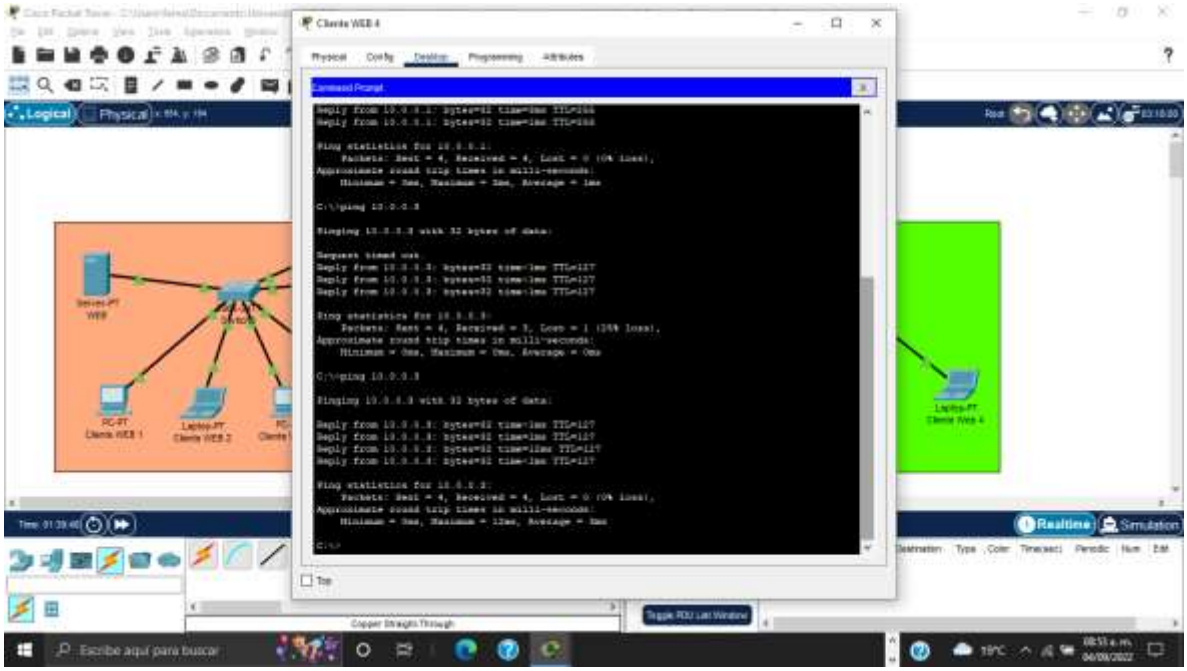





Cliente WEB 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Top
Realtime
Simulation


Cliente WEB 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Top
Realtime
Simulation





Como se puede apreciar en el primer intento al hacer ping desde los clientes de la red marcada en rosa a los clientes de la red verde se tuvo una pérdida de paquete, pero al segundo intento de ping la comunicación fue continua y ya no hubo perdida de paquetes.

Preguntas

¿Qué diferencia hay entre las direcciones IP de la Zona Rosa a la de la Zona Verde?

La diferencia es que la numeración es diferente, al ser de diferentes clases, las direcciones que empiezan con 10 corresponden a la clase A y las que empiezan con 198 corresponden a la clase C. de las cuales la clase A se utiliza por grandes redes privadas como multinacionales y las de clase C son adecuadas para redes con pocos host como las del hogar.

¿La red LAN de 10.0.0.0 de cuántos octetos es?

Es de 4, el primer octeto denota la dirección de red y los últimos 3 octetos son la parte del host.

¿La red LAN de 192.168.0.0 de cuántos octetos es?

Es de 4 también en donde los 3 primeros denotan la dirección de red y el último es la parte del host.

¿La red LAN de la zona verde cuántos equipos como máximo puede identificar?

Puede identificar 16,387,064 computadoras o servidores.

¿La red LAN de la zona rosa cuántos equipos como máximo puede identificar?

Puede identificar 254 computadoras o equipos.

Con tus propias palabras y en base a la experiencia adquirida en la práctica, explica para qué sirve el Gateway o la Puerta de Enlace:

Como su nombre lo indica es un portal o una puerta de enlace que sirve para permitir o controlar el acceso a ciertos equipos de diferentes redes para poder tener comunicación entre ellos o denegarla.

Conclusión

En conclusión en esta parte vimos cómo están compuestas las distintas redes, sus clases, cantidad de equipos que se pueden conectar u hospedar así como su correcta configuración para que tengan comunicación entre ellos y que el envío de información sea integro entre los equipos de las distintas redes.

Referencias

Decodificando Conocimientos (2020),

3.5.5 Packet Tracer - Investigue Los Modelos TCP-IP y OSI En Acción,

21 de Agosto 2022, de Youtube, sitio web:

https://www.youtube.com/watch?v=EKuzT0h58Bo

Introducción a las redes de computadoras (2022),

21 de Agosto 2022, de tutoría 1, sitio web:

https://us06web.zoom.us/rec/play/w_UB9K9dYYs2hgGZumcB-NEsMwyqXX1xO6IMZw6tblQITAoGm1I-eQXDI08WaNLdEVDJZcGDjhCFCds8.YlxyJZDd_AO9-N0Q?continueMode=true&_x_zm_rtaid=H3KtTrbqT0upaNOaqfCF7w.1661108288420.1f642e3b61879271fcab555ad405d354&_x_zm_rhtaid=313

Las direcciones IP (2009),

04 de septiembre del 2022, de INFO@CITEL, sitio web:

https://www.oas.org/en/citel/infocitel/2009/junio/protocolo2_e.asp