**Laboratorio No. 7-parte1**

Capa de red y aplicación e Infraestructura.

Investigación y practica

**RECO**

Brayan Burgos, Daniel Vargas

Escuela Colombiana de Ingeniería Julio Garavito

brayan.burgos@mail.escuelaing.edu.co; [daniel.vargas-o@mail.escuelaing.edu.co](mailto:daniel.vargas-o@mail.escuelaing.edu.co)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_✦\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

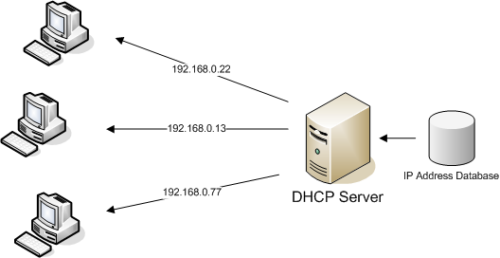
**Introducción.**

La configuración de protocolos de enrutamiento dinámico es la base de este laboratorio. Se observará como con protocolos con lo que se han tenido contacto, pero no mucho manejo, brindaran la posibilidad de cambiar casi que todos los aspectos que se han venido trabajando y observar como Packet Tracer sigue trayendo herramientas verdaderamente poderosas para poder ayudar a los usuarios a hacer sus montajes. Con ello los algoritmos de enrutamiento dinámico brindaran la posibilidad de mejorar el trabajo y las conexiones de cualquier tipo, con un poco menos de esfuerzo. También se observarán aspectos bastante interesantes en nuestras máquinas virtuales con los trócolos UDP y TCP.

**Marco teórico.**

**DHCP:** Protocolo de configuración dinámica de host.

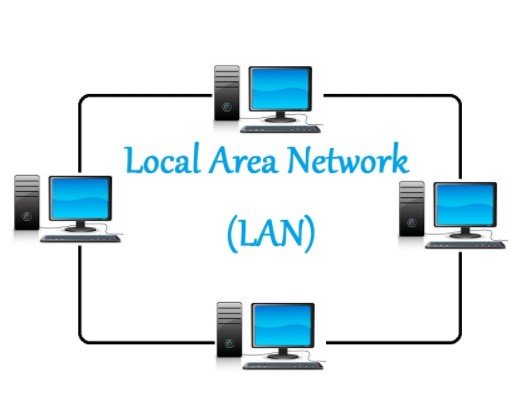
Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP. Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.[1]



**Figura 1.** Muestra de un montaje para mostrar la Arquitectura.

Para que tú puedas estar leyendo esto necesitas de una conexión Wi-Fi, pero esto implica que varios algoritmos se pongan a punto y funcionen conjuntamente. La dirección de protocolos y el servidor DNS son solo el principio, ya que también existen elementos como el servidor DHCP, que a continuación te mencionaré qué es.[2]

**LAN:**



**Figura 2.** Figura LAN

Es posible utilizar este tipo de red en múltiples instituciones para que se realicen sus tareas. Se comenzó introduciendo esta tecnología en redes militares, hasta llegar a escuelas y hospitales.

La red LAN (Local Area Network) es una red que conecta uno o más ordenadores dentro de un ámbito pequeño y limitado. Se puede encontrar a través de cable Ethernet, lo que significa que todos los dispositivos se interconectan mediante un router. Si se hace a través de ondas de radio hablamos de WLAN, lo que nos permite eliminar todo el problema de los cables.[3]

**TELNET:**

Telnet (Teletype Network1​) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Para usar telnet en Windows procedemos a usar este enlace:

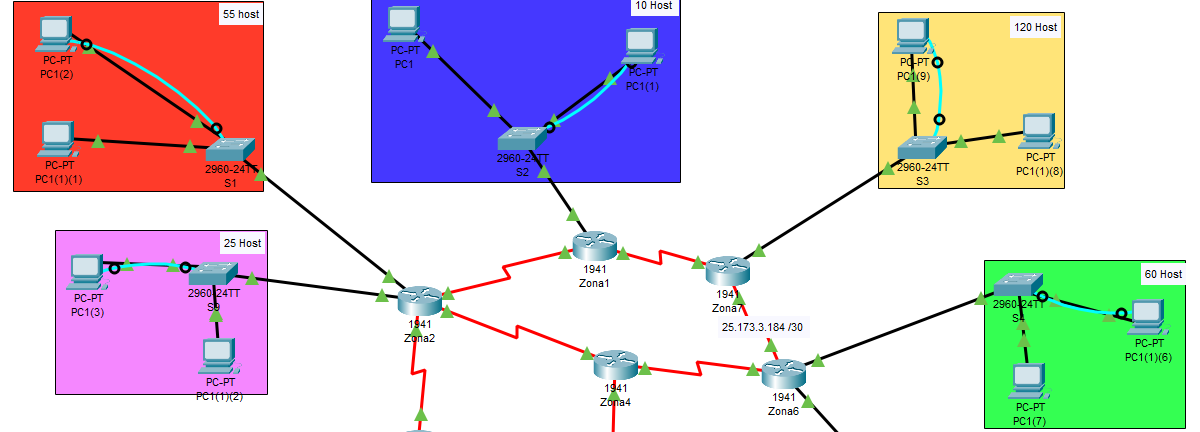
<https://www.acronis.com/es-es/articles/telnet/>

**DNS:** El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés)1​ es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

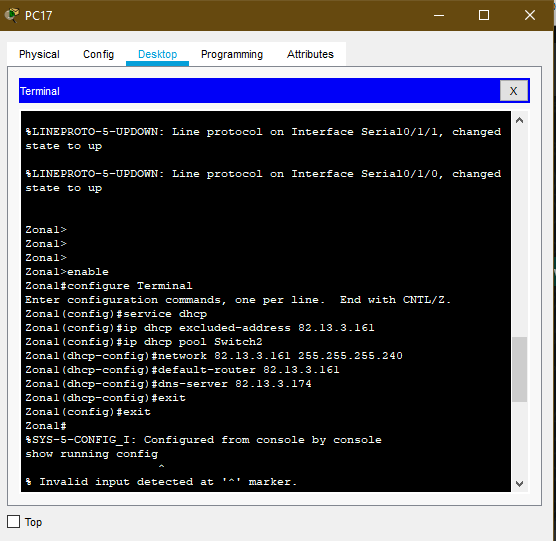
**GATEWAY:** puerta de enlace o pasarela, es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, acceder a otra red.

**SNMP**: El Protocolo simple de administración de red o **SNMP** (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

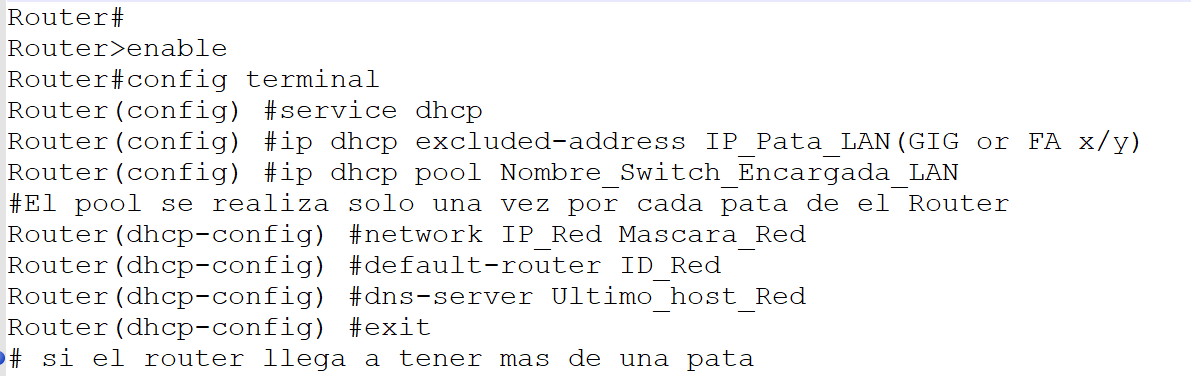
**Pt.**



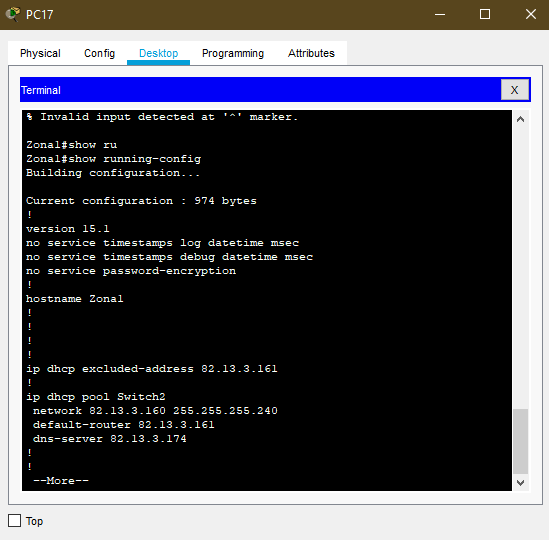
**Figura 1.**  Montaje clase anterior



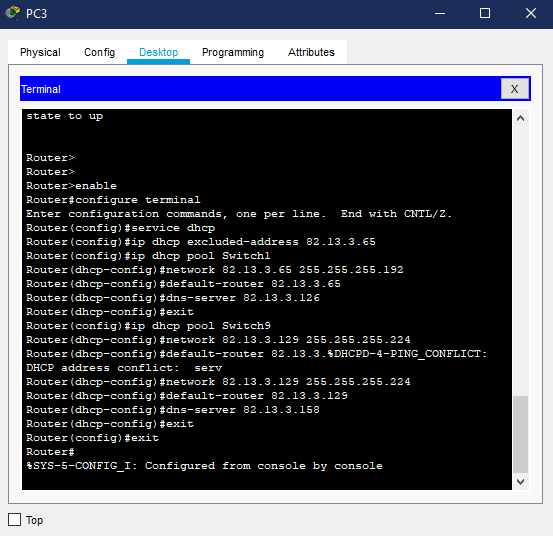
**Figura 2.**  Configuración DHCP



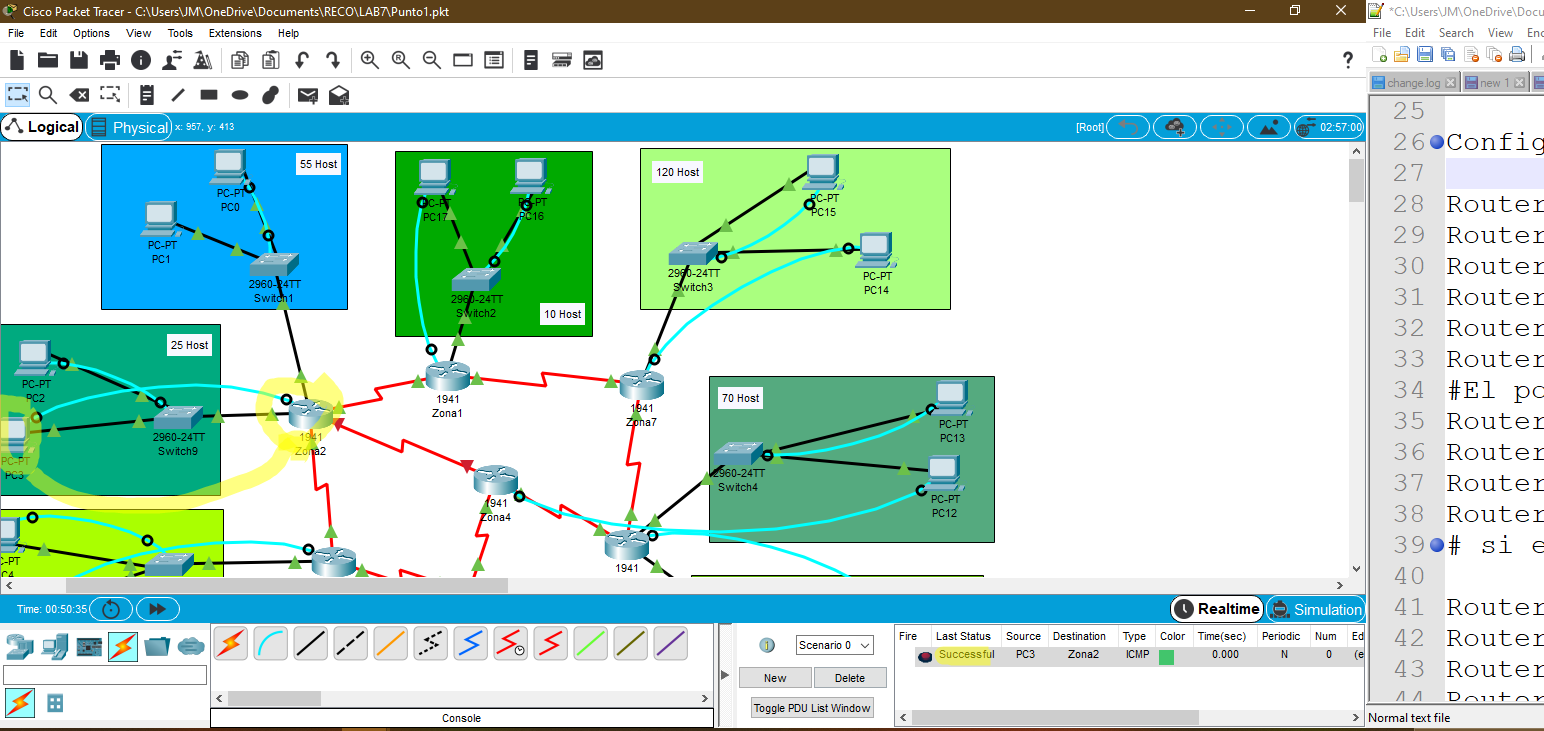
**Figura 3.**  Sintaxis para la configuración



**Figura 4.** Configuración de muestra

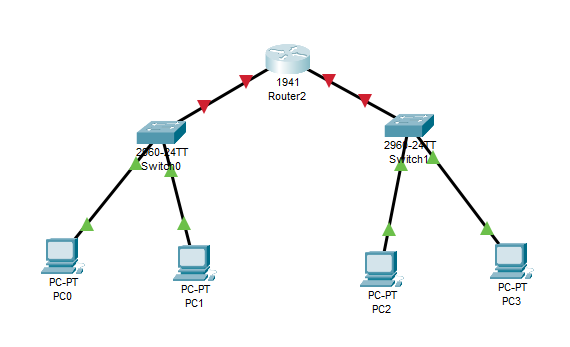


**Figura 5.** Terminación en terminal

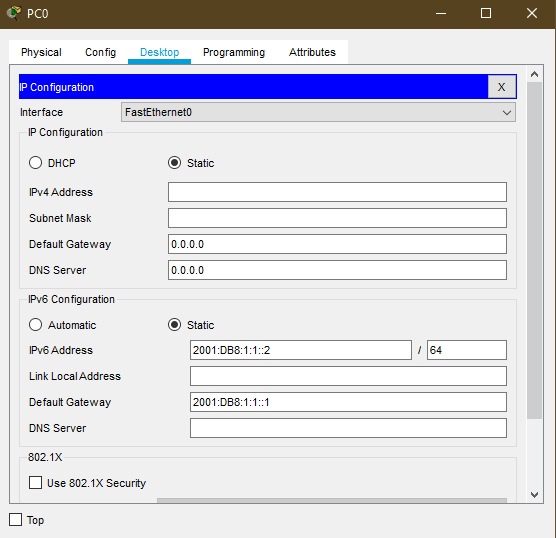


**Figura 6.**  Finalización en montaje

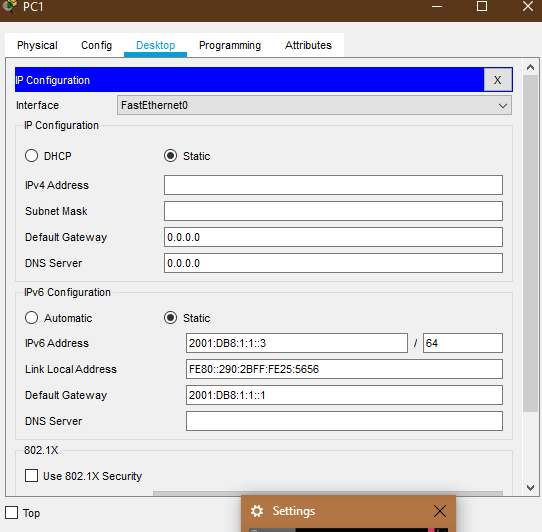
IPV6



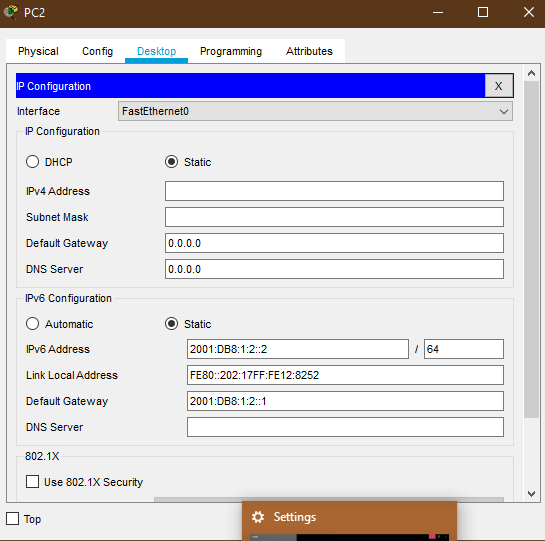
**Figura 1.**  Montaje inicial



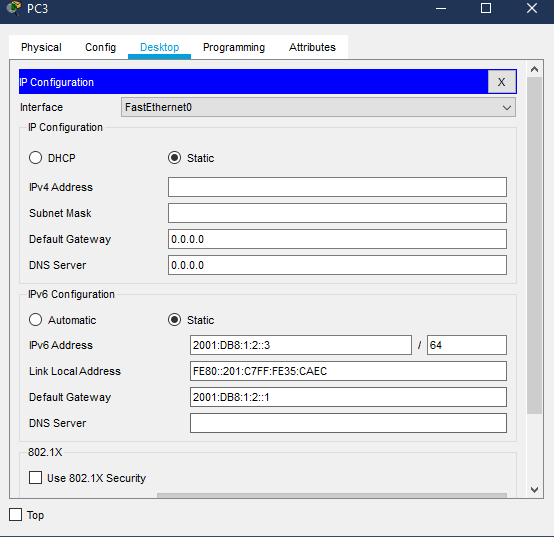
**Figura 2.**  Configuración de equipos



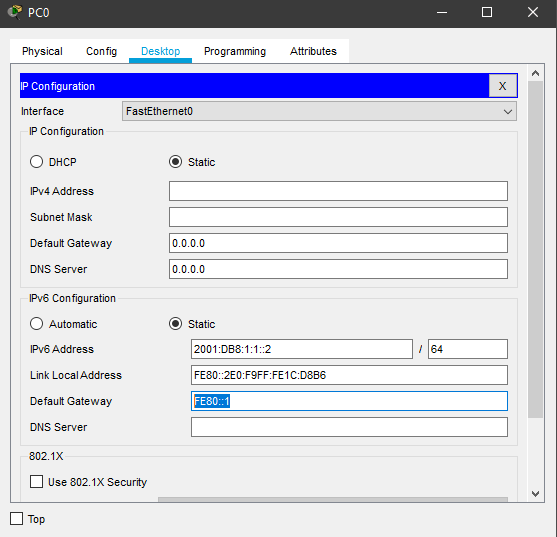
**Figura 4.**  Configuraciones IPV6 pc1



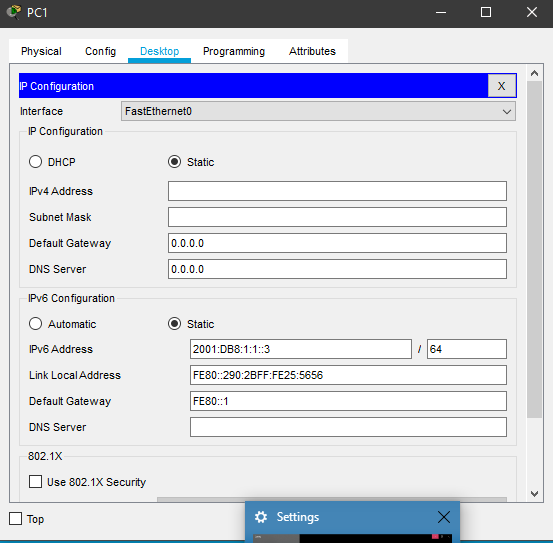
**Figura 5.**  Configuraciones IPV6 pc2



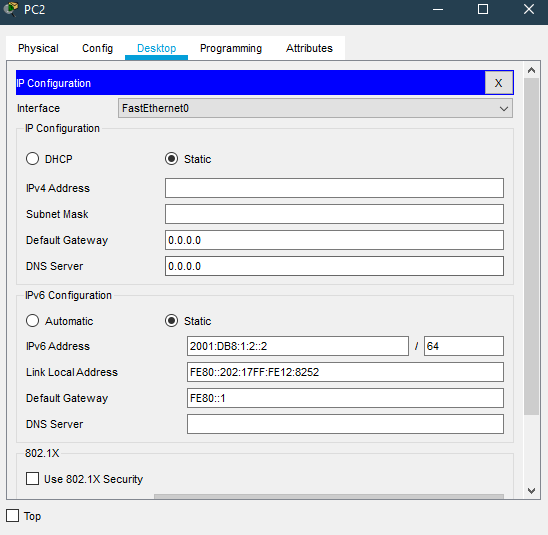
**Figura 6.**  Configuraciones IPV6 pc3



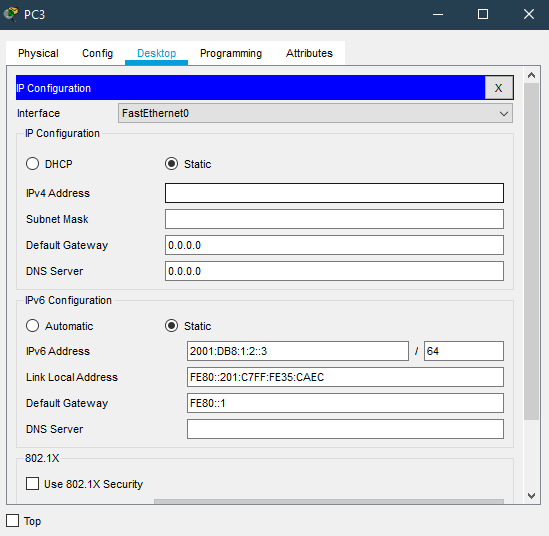
**Figura 7.**  Configuraciones IPV6 pc4



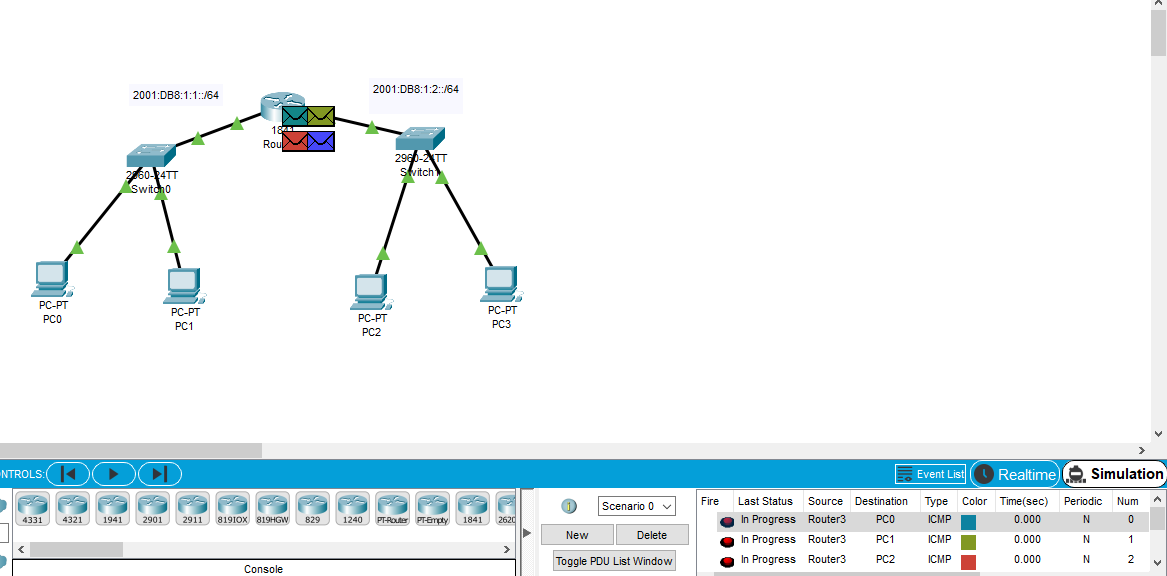
**Figura 8.**  Configuraciones IPV6 pc1, con todos los campos



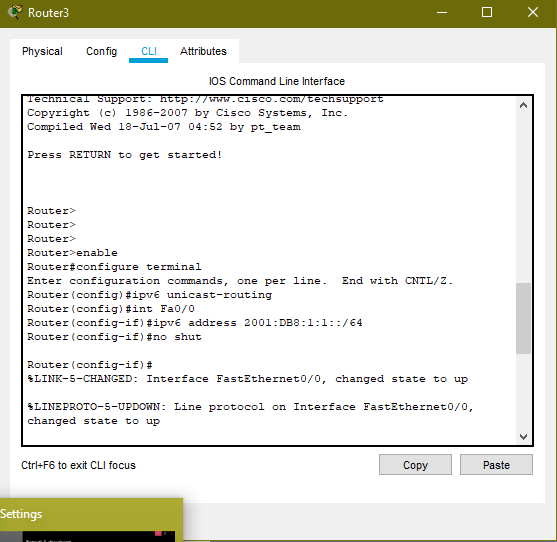
**Figura 8.**  Configuraciones IPV6 pc2, con todos los campos



**Figura 9.**  Configuraciones IPV6 pc3, con todos los campos.



**Figura 10.**  Envió de mensajes



**Conclusiones.**

En este laboratorio podemos observar las grandes ganancias con los protocolos nuevos como DHCP y con direccionamientos diferentes como lo es IPV6. La optimización de tiempo y lo fácil que se vuelve para la red asignar IPS, sobre todo cuando en una LAN se pueden observar que pueden ser sumamente difíciles de manejar y sortear el direccionamiento.

También aprendimos con IP6 que el cambio es difícil, pero es lo mejor para tener mas capacidad en nuestras LAN disponibles y que packet Tracer en definitiva es un arma de diseño que nos permite realizar todos estos cambios

**Bibliografía.**

[1] <https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host>

[2] <https://sistemas.tecnoderecho.com/que-es-el-servidor-dhcp/>

[3] <https://netcloudengineering.com/funcionamiento-redes-lan/>

[4] <https://es.wikipedia.org/wiki/Telnet>

[5] <https://help.wnpower.com/hc/es/articles/360036342231-C%C3%B3mo-abrir-y-cerrar-puertos-en-el-firewall-ufw-en-Ubuntu>

[6] <https://xpertix.com/cambiar-el-puerto-ssh-en-linux/>

[7]