ANALISIS DE CASOS DE ESTUDIO MODULOS CCNA 1 Y 2

CINDY YULIANA SANCHEZ BERMUDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD

FACULTAD DE CIENCIAS BASICAS E INGENIERIA

INGENIERIA ELECTRONICA

ARMENIA

2018

ANALISIS DE CASOS DE ESTUDIO

CCNA MODULOS 1 Y 2

CINDY YULIANA SANCHEZ BERMUDEZ

Cod: 1061368474

Informe presentado como requisito para optar al título de Ingeniera electrónica

Asesor

Juan Carlos Vesga

Docente de la Facultad de Ingeniería

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD

FACULTAD DE CIENCIAS BASICAS E INGENIERIA

INGENIERIA ELECTRONICA

ARMENIA

2018

Nota de aceptación

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Armenia, 2018

DEDICATORIA

Dedico este trabajo a Dios por bendecirme y darme salud para poder culminar otro ciclo de mi vida como profesional.

Con todo mi amor a mi madre María, la cual es quien hace posible que pueda estudiar gracias al apoyo diario y al cuidado que brinda a mi hija, a mi hija Mariana quien con su nacimiento impulso en mí el deseo de continuar y buscar nuevas oportunidades laborales, a mis hermanos y tutores por animarme y guiarme en este proceso de educación y a mi novio Jhon Mario Gaviria por ser un nuevo apoyo en mi vida.

GRACIAS

CINDY YULIANA SANCHEZ

AGRADECIMIENTOS

Agradezco a Dios por permitirme estar finalizando este ciclo profesional, Agradezco a la Universidad Nacional Abierta y a Distancia – UNAD por permitir cambiar la educación tradicional y darme la oportunidad de adecuar mis horarios de estudio. Por último, doy las gracias a mis padres, familiares y amigos quienes son parte fundamental en la realización de este logro.

RESUMEN

La actividad realizada consiste en el análisis y solución de un caso de estudio en una empresa de Tecnología que posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde se tiene un administrador de la red. Se parte de la comprensión y análisis de la red para proceder con la configuración solicitada. Se muestra el marco teórico y el proceso que se sigue para la configuración de la red, exponiendo el proceso de direccionamiento IP, enrutamiento OSPF, la asignación de VLAN a las redes, la implementación de DHCP utilizando un Router, la configuración de NAT y el establecimiento de las listas de acceso.

Términos clave:

- Direccionamiento IP
- VLAN
- OSPF
- NAT
- Listas de acceso

INTRODUCCIÓN

Las redes surgieron de la necesidad de comunicación entre los seres humanos porque desde el inicio de los tiempos las necesidades de información fueron aumentando y por esto surgieron las redes para ajustarse a los requerimientos de diversos mercados. Las diferentes empresas se valen de las facilidades actuales de adquisición de los servicios de comunicación para lograr sus objetivos, proyectar sus metas y llegar a sus diferentes grupos de interés; porque cualquier tipo de empresa requiere de una red eficaz, fiable y con capacidad para permitir acceso a la información desde cualquier punto; siendo posible encontrar soluciones que se ajustan de acuerdo a las necesidades de múltiples sectores (Universidades, Aeropuertos, Administraciones, Banca e Industria entre otras).

La globalización de Internet fue muy rápida. El modo en que se producen las interacciones sociales, comerciales, políticas y personales cambia dia a dia con la evolución de internet. Todos los esfuerzos y soluciones que se diseñan tienen a internet como punto de partida, de manera que la capacidad de las redes juega un papel cada vez más importante en el éxito de los nuevos proyectos. Estamos conectados actualmente gracias a las redes, estas permiten comunicar de manera instantánea varias personas, hacer negocios, publicar ideas, noticias y descubrimientos y todo esto en unos pocos minutos. Las redes conectan a las personas y promueven la comunicación libre. Todos pueden conectarse, compartir y hacer una diferencia.

Las redes deben ser confiables por lo que se deben administrar teniendo claro los equipos que la conforman, los conceptos, procedimientos y protocolos que hacen que estas cumplan su función. No importando el tamaño de una red esta debe ser segura, la seguridad generalmente debe ser implementada en varias capas porque no existen soluciones únicas, por lo que cada infraestructura de red debe crecer y ajustarse a las necesidades de cada entorno, es en este punto donde la plataforma de routing y switching es la base de toda infraestructura de red. Los switch y los router son fundamentales porque permiten la comunicación con los demás dispositivos y con otras redes, por lo que es fundamental una administración eficaz de estos equipos dentro de cualquier red para proporcionan soluciones integrales de acuerdo a las necesidades.

Este trabajo forma parte del diplomado de profundización de Switching y Routing (CCNA Y CCNA 2) impartido por Cisco para la Universidad Nacional Abierta y a Distancia Unad, con su filosofía de trabajo enmarcada en el E-doing que aplica el principio de que se aprende mejor a través de la práctica. Se muestra la solución a un caso propuesto con el fin de administrar el Switching y routing aplicando los conocimientos adquiridos a lo largo del diplomado.

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

1. PROBLEMA

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Realizar la implementación de un caso de estudio en Packet Tracer, mostrando el proceso de configuración realizado a la red, con el fin de identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado CISCO como opción de grado.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar direccionamiento IP según la configuración entregada.
- Configurar el protocolo de enrutamiento OSPF.
- Configurar las VLAN (Administración, Mercadeo y Mantenimiento).
- Implementar DHCP and NAT for IPv4.
- Establecer Listas de control de acceso estándar y de tipo extendido.
- Realizar pruebas de conexión para cada una de las configuraciones realizadas.

3. MARCO TEÓRICO

- **PROTOCOLO DE ENRUTAMIENTO OSPF**

La versión actual de OSPF para IPv4 es OSPFv2, introducida en RFC 1247 y actualizada en RFC 2328 por John Moy. En 1999, OSPFv3 para IPv6 se publicó en RFC 2740.

OSPF es un protocolo de routing de estado de enlace sin clase con una distancia administrativa predeterminada de 110 y se indica en la tabla de routing con el código de origen de ruta O.

OSPF se habilita con el comando router ospf id-proceso del modo de configuración global. El valor id-proceso tiene importancia en el ámbito local, lo que significa que no necesita coincidir con otros routers OSPF para establecer adyacencias con esos vecinos.

El comando network utilizado con OSPF cumple la misma función que cuando se lo utiliza con otros protocolos de routing IGP, pero con una sintaxis ligeramente diferente. El valor máscara-wildcard es el valor inverso a la máscara de subred, y el valor id-área se debe establecer en 0.

De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos de accesos múltiples y punto a punto, y cada 30 segundos en los segmentos NBMA (Frame Relay, X.25, ATM), y OSPF los usa para establecer adyacencias de vecinos. De manera predeterminada, el intervalo muerto es equivalente a cuatro veces el valor del intervalo de saludo.

Para que los routers establezcan una adyacencia, sus intervalos de saludo, intervalos muertos, tipos de red y máscaras de subred deben coincidir. Use el comando show ip ospf neighbors para verificar las adyacencias OSPF.

En una red de accesos múltiples, OSPF elige un DR para que funcione como punto de recopilación y distribución de las LSA enviadas y recibidas. Un BDR se elige para cumplir la función del DR en caso de que este falle. Todos los demás routers se conocen como DROTHER. Todos los routers envían sus LSA al DR, que luego satura con la LSA todos los demás routers en la red de accesos múltiples.

El comando show ip protocols se utiliza para verificar la información importante de configuración OSPF, incluidas la ID del proceso OSPF, la ID del router y las redes que anuncia el router.[1]

[1] (CISCO, 2014)

OSPFv3 se habilita en una interfaz, no en el modo de configuración del router. OSPFv3 necesita que se configuren direcciones link-local. Se debe habilitar el routing de unidifusión IPv6 para OSPFv3. Para habilitar una interfaz para OSPFv3, antes se requiere una ID de router de 32 bits.

- **VLAN**

Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. Las VLAN son un mecanismo para permitir que los administradores de red creen dominios de difusión lógicos que puedan extenderse a través de un único switch o varios switches, independientemente de la cercanía física. Esta función es útil para reducir el tamaño de los dominios de difusión o para permitir la agrupación lógica de grupos o usuarios sin la necesidad de que estén ubicados físicamente en el mismo lugar.

Existen varios tipos de VLAN: VLAN predeterminada, VLAN de administración, VLAN nativa, VLAN de datos/de usuarios, VLAN de agujero negro y VLAN de voz

En los switches Cisco, la VLAN 1 es la VLAN Ethernet predeterminada, la VLAN nativa predeterminada y la VLAN de administración predeterminada. Las prácticas recomendadas sugieren que la VLAN nativa y la de administración se cambien a una VLAN distinta, y que los puertos de switch sin utilizar se trasladen a una VLAN de “agujero negro” para mayor seguridad.

El comando switchport access vlan se utiliza para crear una VLAN en un switch. Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. El comando show vlan brief muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. Cada VLAN debe corresponder a una subred IP única.

Se utiliza el comando show vlan para verificar si el puerto pertenece a la VLAN esperada. Si el puerto se asignó a una VLAN incorrecta, se utiliza el comando switchport access vlan para corregir la pertenencia de VLAN. Se utiliza el comando show mac address-table para revisar qué direcciones se obtuvieron en un puerto determinado del switch y a qué VLAN se asignó ese puerto.[2]

[2] (CISCO, 2014)

Un puerto de un switch es un puerto de acceso o un puerto de enlace troncal. Los puertos de acceso transportan el tráfico de una VLAN específica asignada al puerto.

Un puerto de enlace troncal pertenece a todas las VLAN de manera predeterminada; por lo tanto, transporta el tráfico para todas las VLAN.

Los enlaces troncales de VLAN facilitan la comunicación entre switches mediante el transporte de tráfico relacionado con varias VLAN. El etiquetado de tramas IEEE 802.1Q permite diferenciar tramas de Ethernet asociadas a distintas VLAN a medida que atraviesan enlaces troncales en común. Para habilitar los enlaces troncales, utilice el comando switchport mode trunk. Utilice el comando show interfaces trunk para verificar si se estableció un enlace troncal entre los switches.

La negociación de enlaces troncales entre dispositivos de red la maneja el protocolo de enlace troncal dinámico (DTP), que solo funciona de punto a punto. DTP es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560.

Para volver un switch a su condición predeterminada de fábrica con una VLAN predeterminada, use el comando delete flash:vlan.dat y erase startup-config.

- **DHCP**

Todos los nodos en una red requieren una dirección IP única que se comunique con otros dispositivos. La asignación estática de información de direccionamiento IP en una red grande produce una carga administrativa que puede eliminarse mediante el uso de DHCPv4 o DHCPv6 para asignar de forma dinámica información de direccionamiento IPv4 e IPv6, respectivamente.

DHCPv4 incluye tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones IP: Asignación manual: el administrador asigna una dirección IPv4 preasignada al cliente, y DHCPv4 comunica solo la dirección IPv4 al dispositivo, unad asignación automática cuando DHCPv4 asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. [3]

[3] (CISCO, 2014)

No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo y una asignación dinámica cuando DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado según lo configurado en el servidor o hasta que el cliente ya no necesite la dirección.

La asignación dinámica es el mecanismo DHCPv4 utilizado más comúnmente y comprende el intercambio de diversos paquetes entre el servidor de DHCPv4 y el cliente DHCPv4, lo que deriva en el arrendamiento de información de direccionamiento válida durante un período predefinido.

Los mensajes cuyo origen es el cliente (DHCPDISCOVER, DHCPREQUEST) son mensajes de difusión para permitir que todos los servidores de DHCPv4 en la red escuchen la solicitud de información de direccionamiento y la recepción de dicha información por parte del cliente. Los mensajes cuyo origen es el servidor de DHCPv4 (DHCPOFFER, DHCPACK) se envían como mensajes de unidifusión directamente al cliente que solicita la información.

Existen dos métodos disponibles para la configuración dinámica de las direcciones IPv6 de unidifusión global y son configuración automática de dirección sin estado (SLAAC) y Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Con la configuración automática sin estado, el cliente utiliza información proporcionada por el mensaje RA IPv6 para seleccionar y configurar automáticamente una dirección IPv6 única. La opción de DHCPv6 sin estado informa al cliente que utilice la información del mensaje RA para el direccionamiento, pero que hay más parámetros de configuración disponibles de un servidor de DHCPv6.

DHCPv6 con estado es similar a DHCPv4. En este caso, el mensaje RA le informa al cliente que no utilice la información contenida en el mensaje RA. Toda la información de direccionamiento y de configuración se obtiene de un servidor de DHCPv6 con estado. El servidor de DHCPv6 mantiene la información de estado IPv6 de manera similar a la que un servidor de DHCPv4 asigna direcciones para IPv4.[4]

[4] (CISCO, 2014)

Si el servidor de DHCP está ubicado en un segmento de red distinto del segmento del cliente DHCP, se debe configurar un agente de retransmisión. El agente de retransmisión reenvía mensajes de difusión específicos que se originan en un segmento LAN a un servidor especificado ubicado en un segmento LAN distinto (en este caso, un mensaje de difusión DHCP se reenviaría a un servidor de DHCP).

- **NAT.**

Se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4. La NAT para IPv4 permite que los administradores de red utilicen el espacio de direcciones privadas definido en RFC 1918, a la vez que proporciona conectividad a Internet, mediante una única dirección pública o una cantidad limitada de estas.

NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones. NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al ISP. Sin embargo, NAT presenta desventajas en términos de sus efectos negativos en el rendimiento de los dispositivos, la seguridad, la movilidad y la conectividad de extremo a extremo, y se debe considerar como una implementación a corto plazo para el agotamiento de direcciones, cuya solución a largo plazo es IPv6.

El primer paso para configurar una NAT dinámica es definir el conjunto de direcciones que se utilizará para la traducción con el comando ip nat pool. Por lo general, este conjunto es un grupo de direcciones públicas. Las direcciones se definen indicando la primera y la última dirección IP del conjunto. Las palabras clave netmask o prefix-length indican qué bits de la dirección pertenecen a la red y cuáles al host en el rango de direcciones.

Se configura una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles.

Para conectar la ACL al conjunto, se utiliza el comando ip nat inside source list número-lista-acceso number pool nombre-conjunto. El router utiliza esta configuración para determinar qué dirección (pool) recibe cada dispositivo (list).[5]

[5] (CISCO, 2014)

Por último se configura la interfaz interna con respecto a NAT es decir la interfaz que se conecta a la red interna y una interfaz externa con respecto a NAT es decir la interfaz que se conecta a la red externa

- **Listas de control de acceso (ACL).**

Los routers no filtran tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing.

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete. Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte.

Una ACL es una lista secuencial de instrucciones permit o deny. La última instrucción de una ACL siempre es una instrucción deny implícita que bloquea todo el tráfico. Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, es posible agregar la instrucción permit ip any any.

Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada entrada, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente.

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. La regla básica para la colocación de una ACL estándar es colocarla cerca del destino.

Las ACL extendidas filtran paquetes según varios atributos: el tipo de protocolo, la dirección IPv4 de origen o de destino y los puertos de origen o de destino. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen.
El comando de configuración global access-list define una ACL estándar con un número en el intervalo de 1 a 99 o una ACL extendida con un número en el intervalo de 100 a 199 y de 2000 a 2699. [6]

[6] (CISCO, 2014)

Tanto las ACL estándar como las extendidas pueden tener un nombre. El comando ip access-list standard nombre se utiliza para crear una ACL estándar con nombre, mientras que el comando ip access-list extended nombre se utiliza para una lista de acceso extendida. Las ACE de IPv4 incluyen el uso de máscaras wildcard.

Después de que se configura una ACL, se vincula a una interfaz mediante el comando ip access-group del modo de configuración de interfaz. Recuerde la regla de las tres P: una ACL por protocolo, por sentido y por interfaz.
Para eliminar una ACL de una interfaz, primero introduzca el comando no ip access-group en la interfaz y, a continuación, introduzca el comando global no access-list para eliminar la ACL completa.

Los comandos show running-config y show access-lists se utilizan para verificar la configuración de la ACL. El comando show ip interface se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.

El comando access-class configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada y las direcciones en una lista de acceso.
Al igual que las ACL de IPv4 con nombre, los nombres en IPv6 son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. A diferencia de IPv4, no hay necesidad de una opción estándar o extendida.

En el modo de configuración global, utilice el comando ipv6 access-list nombre para crear una ACL de IPv6. A diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir.

Después de que se configura una ACL de IPv6, se la vincula a una interfaz mediante el comando ipv6 traffic-filter.[7]

[7] (CISCO, 2014)

4. METODOLOGÍA

4.1 DESCRIPCIÓN DEL PROCESO

Este trabajo se basa en el caso de estudio propuesto como trabajo final para aplicar los conceptos de los módulos CCNA 1 y CCNA2 de CISCO. El caso propuesto trata de una serie de Router de una empresa que estan ubicados en distintas sucursales (ciudades).

Para dar esta solución nos indican las redes que se deben utilizar y se solicita la configuración de tres VLAN (30, 40 y 200) las cuales corresponden a Administración, Mercadeo y Mantenimiento; siendo necesario para establecimiento de adyacencia entre los router utilizar el protocolo de enrutamiento OSPF, uno de los Router debe ser configurado como servidor DHCP para los host de las VLAN configuradas 30 y 40; adicionalmente es necesario configurar NAT para permitir que los host salgan a internet y listas de acceso para restringir o permitir el tráfico en la red.

4.2 RESOLUCION CASO DE ESTUDIO

El planteamiento del problema es el siguiente:

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

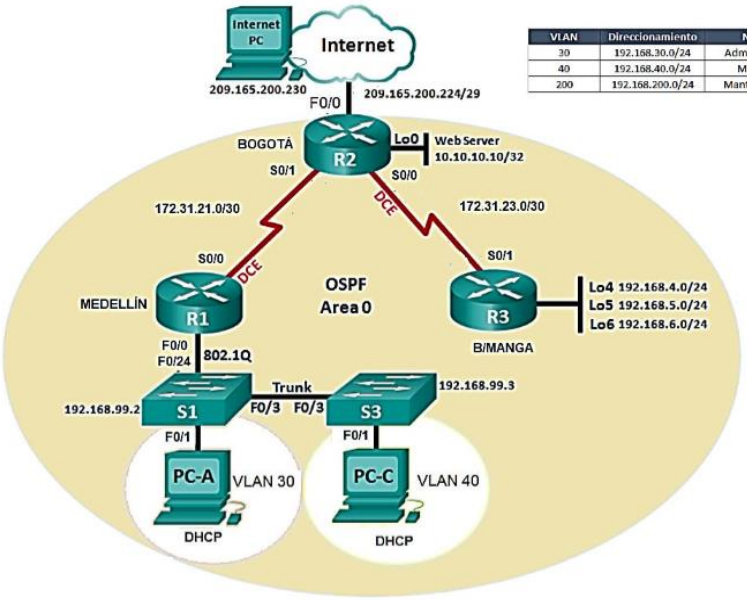

figura 1. Topología caso de estudio

Para esta topología se solicitó realizar la configuración de acuerdo a los siguientes criterios:

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.

2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

FIGURA 2. *CONFIGURACION PROPUESTA OSPFV2 AREA 0*

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switch acorde a la topología de red establecida.
4. En el Switch 3 deshabilitar DNS lookup
5. Asignar direcciones IP a los Switch acorde a los lineamientos.
6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.
10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet
11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Este caso se desarrolla para una empresa la cual necesita realizar sus actividades en un entorno de trabajo a distancia, como se observa, se manejan varias sedes, cada una de estas sedes está ubicada en una Ciudad distante, la conexión que se solicita requiere un protocolo de enrutamiento el cual hace que los Router puedan enviar paquetes, “la información” a las rutas de destino, siendo muy importante ya que sin esto no habría conexión coherente y no podrían enviarse la información de forma óptima.

5. 4.2.1. DIRECCIONAMIENTO IP.

El direccionamiento IP para esta topología fue establecido de acuerdo a las indicaciones entregadas en el caso de estudio, en donde se muestran las redes que pueden ser distribuidas de acuerdo a las necesidades de asignación.

Dirección de red	172.31.21.0/30	172.31.21.00000000
Primera Dirección de Host	172.31.21.1	172.31.21.00000001
Ultima Dirección de Host	172.31.21.2	172.31.21.00000010
Dirección de Broadcast	172.31.21.3	172.31.21.00000011
Cantidad de Hosts	2^2-2=2 hosts	

Tabla 1. Análisis direcciones IP red 172.31.21.0

Dirección de red	172.31.23.0/30	172.31.23.00000000
Primera Dirección de Host	172.31.23.1	172.31.23.00000001
Ultima Dirección de Host	172.31.23.2	172.31.23.00000010
Dirección de Broadcast	172.31.23.3	172.31.23.00000011
Cantidad de Hosts	2^2-2=2 hosts	

Tabla 2. Análisis direcciones IP red 172.31.23.0

Dirección de red	192.168.99.0/24	192.168.99.00000000
Primera Dirección de Host	192.168.99.1	192.168.99.00000001
Ultima Dirección de Host	192.168.99.254	192.168.99.11111110
Dirección de Broadcast	192.168.99.255	192.168.99.11111111
Cantidad de Hosts	2^8-2=254 hosts	

Tabla 3. Análisis direcciones IP red 192.168.99.0

Dirección de red	192.168.4.0/24	192.168.4.00000000
Primera Dirección de Host	192.168.4.1	192.168.4.00000001
Ultima Dirección de Host	192.168.4.254	192.168.4.11111110
Dirección de Broadcast	192.168.4.255	192.168.4.11111111
Cantidad de Hosts	2^8-2=254 hosts	

tabla 4. Análisis direcciones IP red 192.168.4.0

Dirección de red	192.168.5.0/24	192.168.5.00000000
Primera Dirección de Host	192.168.5.1	192.168.5.00000001
Ultima Dirección de Host	192.168.5.254	192.168.5.11111110
Dirección de Broadcast	192.168.5.255	192.168.5.11111111
Cantidad de Hosts	2^8-2=254 hosts	

tabla 5. Análisis direcciones IP red 192.168.5.0

Dirección de red	192.168.6.0/24	192.168.6.00000000
Primera Dirección de Host	192.168.6.1	192.168.6.00000001
Ultima Dirección de Host	192.168.6.254	192.168.6.11111110
Dirección de Broadcast	192.168.6.255	192.168.6.11111111
Cantidad de Hosts	2^8-2=254 hosts	

tabla 6. Análisis direcciones IP red 192.168.6.0

Dirección de red	209.165.200.224/29	209.165.200.11100000
Primera Dirección de Host	209.165.200.225	192.168.6. 11100001
Ultima Dirección de Host	209.165.200.230	192.168.6. 11100110
Dirección de Broadcast	209.165.200.231	192.168.6. 11100111
Cantidad de Hosts	2^3-2=6 hosts	

tabla 7. Análisis direcciones IP red 209.165.200.224

A continuación, se muestra el direccionamiento IP asignado a cada interfaz en el caso propuesto.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	F0/0.1	192.168.99.254	255.255.255.0	N/A
	F0/0.30	192.168.30.1	255.255.255.0	N/A
	F0/0.40	192.168.40.1	255.255.255.0	N/A
	S0/0/0 (DCE)	172.31.21.2	255.255.255.252	N/A
R2	Lo0	10.10.10.10	255.255.255.255	N/A
	S0/0/0 (DCE)	172.31.23.1	255.255.255.252	N/A
	S0/0/1	172.31.21.1	255.255.255.252	N/A
	F0/1.200	192.168.200.1	255.255.255.0	N/A
R3	Lo4	192.168.4.1	255.255.255.0	N/A
	Lo5	192.168.5.1	255.255.255.0	N/A
	Lo6	192.168.6.1	255.255.255.0	N/A
	S0/0/1	172.31.23.2	255.255.255.252	N/A
PC-A	NIC	DHCP	DHCP	DHCP
Internet –PC	NIC	192.168.200.2	255.255.255.0	192.168.200.1
PC-C	NIC	DHCP	DHCP	DHCP
S1	VLAN 1	192.168.99.2	255.255.255.0	192.168.99.254
S3	VLAN 1	192.168.99.3	255.255.255.0	192.168.99.254
S4	VLAN 1	_	_	192.198.200.1

Tabla 8. Asignación IP y Gateway determinado.

Puertos	Asignaciones	Red
S1 F0/3	Enlace Troncal	N/A
S3 F0/3	Enlace Troncal	N/A
S1 F0/24	Enlace troncal de 802.1Q	N/A
S4 F0/1	Enlace Troncal	N/A
S1 F0/1	VLAN 30: Administración	192.168.30.0/24
S3 F0/1	VLAN 40: Mercadeo	192.168.40.0/24
SZZS4 F0/2	VLAN 200: Mantenimiento	192.168.200.0/24

Tabla 9. Configuración puertos switches

6. 4.2.2. REINICIO DE EQUIPOS Y CONFIGURACIÓN INICIAL.

4.2.2.1 REINICIO DE EQUIPOS.

Los equipos a utilizar deben ser reiniciados con el fin de eliminar anteriores configuraciones que puedan afectar la nueva programación que será ingresada.

Los pasos para reiniciar un router son:

- Acceder al router mediante el puerto de consola y habilitar el modo EXEC privilegiado.
- Escribir el comando erase startup-config para eliminar el archivo de configuración de inicio de la NVRAM.
- Emitir el comando reload para eliminar una configuración antigua de la memoria. Cuando se recibe el mensaje Proceed with reload (Continuar con la recarga) se presiona Enter para confirmar.
- Una vez que se vuelve a cargar el router, se solicita introducir el diálogo de configuración inicial. Se escribe **no** y se presiona Enter.

Las contraseñas asignadas fueron elegidas de manera propia debido a que estos parámetros no fueron especificados de manera clara en el caso de estudio.

A continuación, se muestra el reinicio realizado para los Router 1, 2 y 3 del caso de estudio.

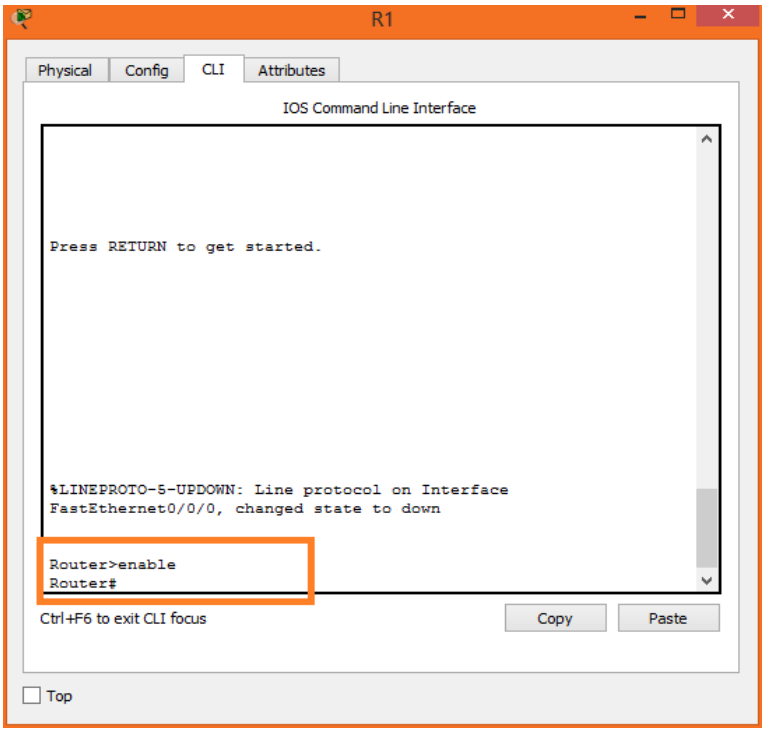

figura 3. Router 1 Acceso al mediante puerto de consola y habilitacion modo exec provilegiado

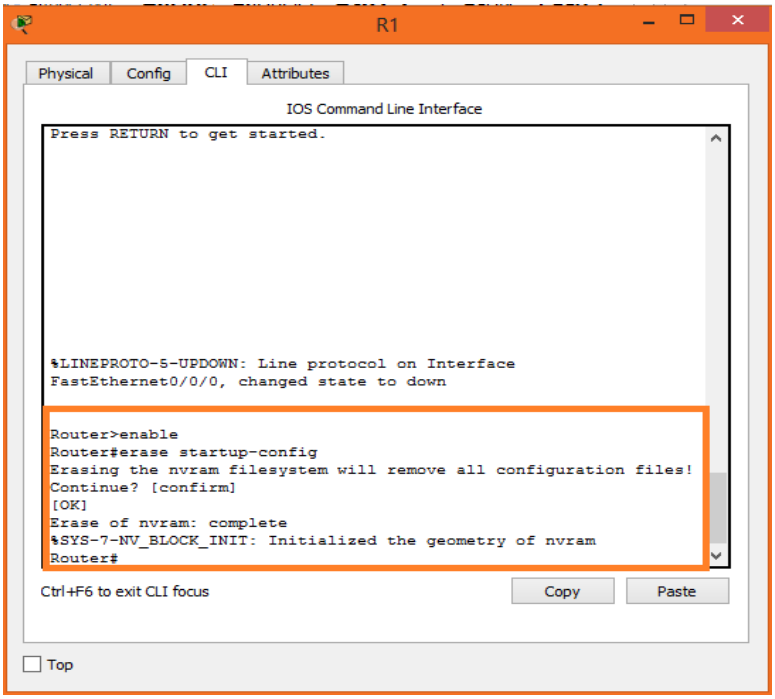

figura 4. Router 1 Ingreso comando erase startup-config para eliminar el archivo de configuración de inicio de la NVRAM.

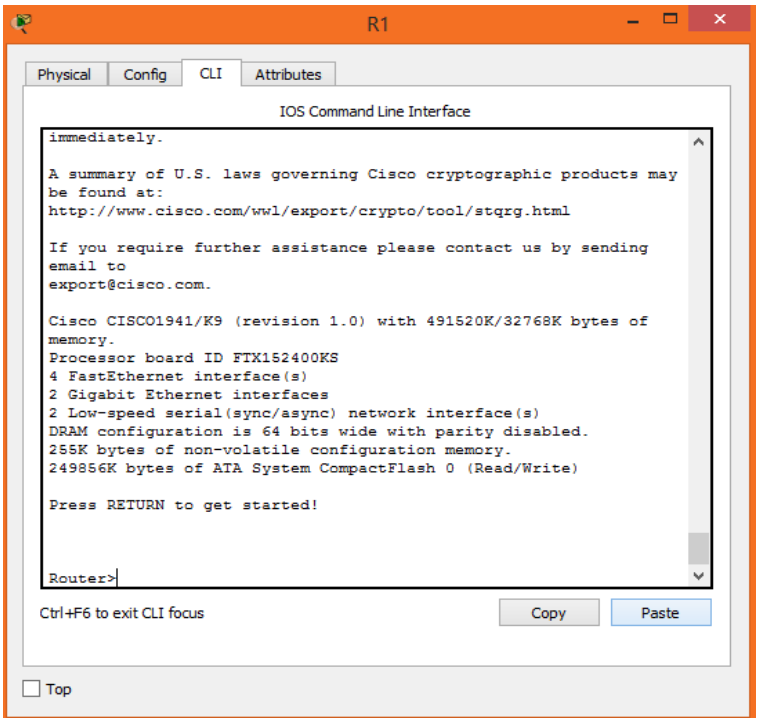

figura 5. Router 1 comando reload para eliminar una configuración antigua de la memoria.

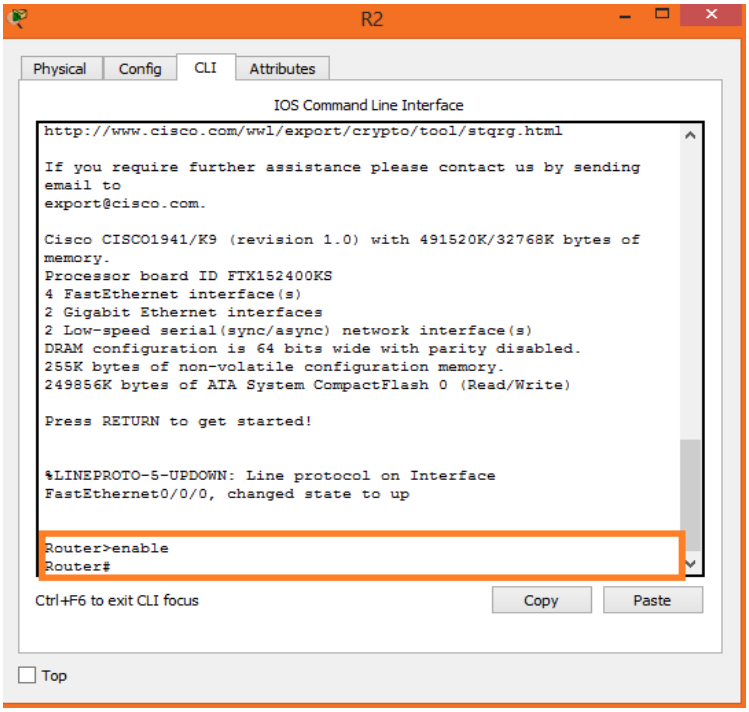

figura 6. Router 2 Acceso al mediante puerto de consola y habilitacion modo exec provilegiado

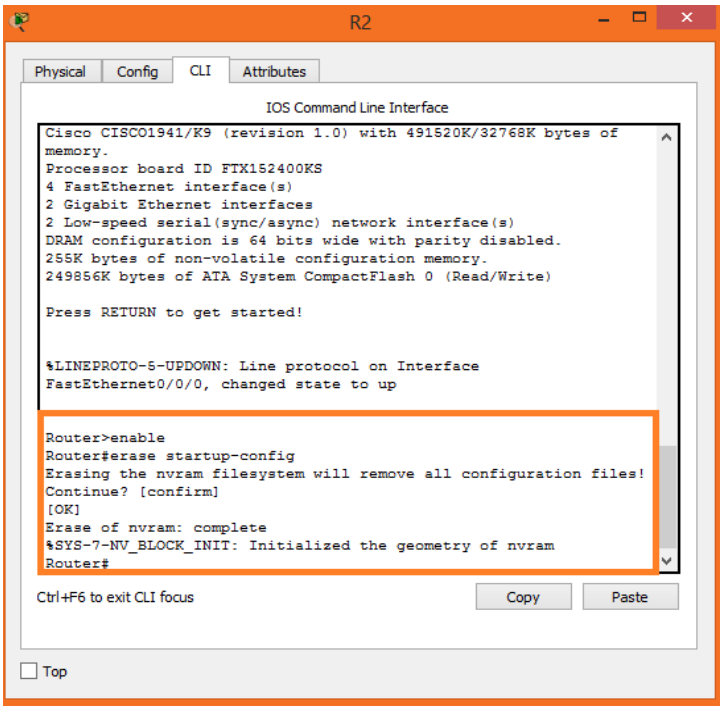

figura 7. Router 2 Ingreso comando startup-config para eliminar el archivo de configuración de inicio de la NVRAM.

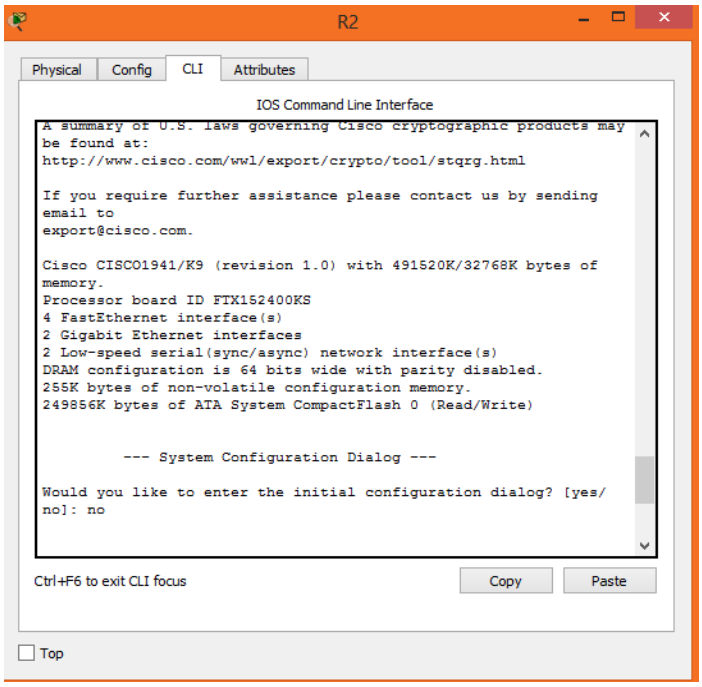

figura 8. Router 2 comando reload para eliminar una configuración antigua de la memoria.

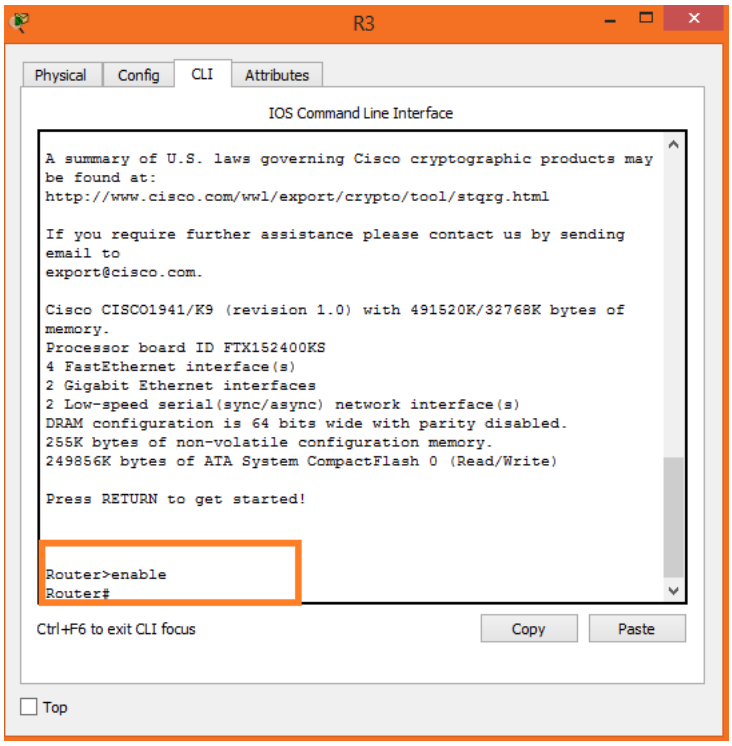

figura 9. Router 3 Acceso mediante puerto de consola y habilitacion modo exec provilegiado

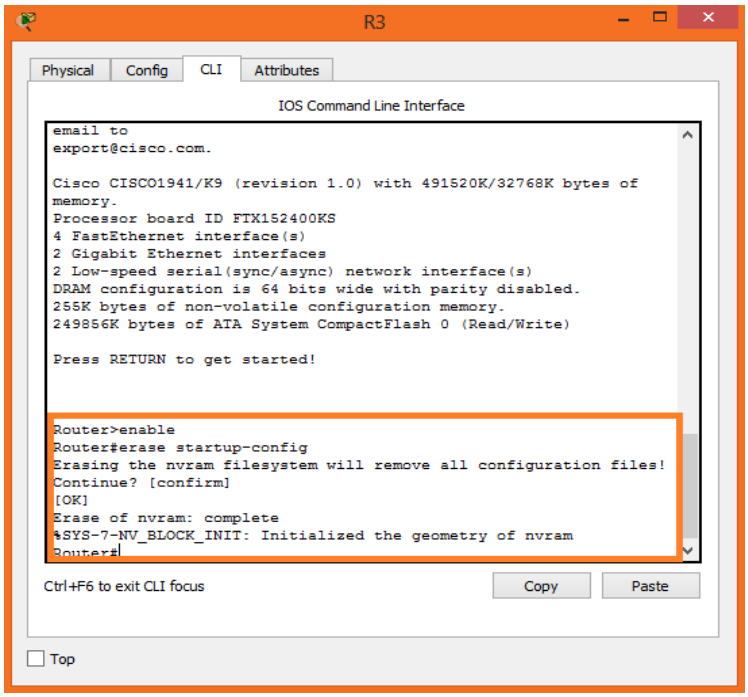

figura 10. Router 3 Ingreso comando startup-config para eliminar el archivo de configuración de inicio de la NVRAM.

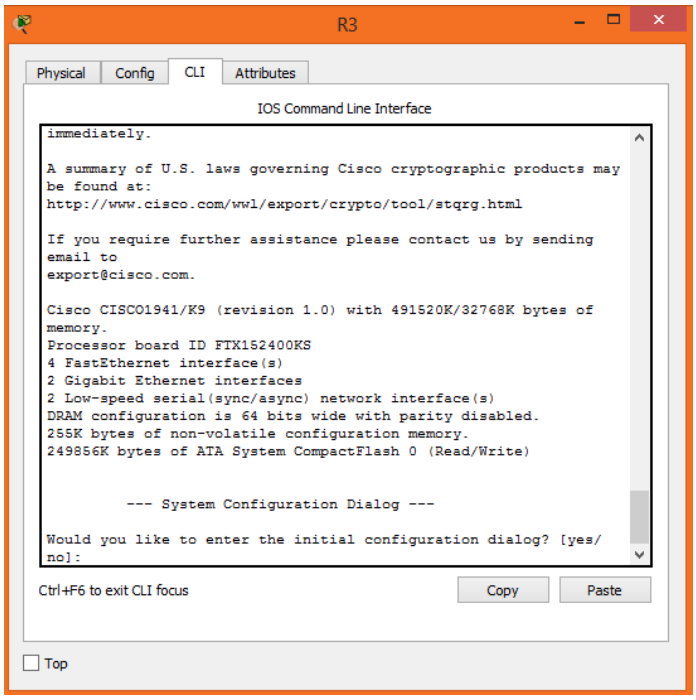

figura 11. Router 3 comando reload para eliminar una configuración antigua de la memoria

.

4.2.2.2 CONFIGURACION INICIAL:

Se programa para los Router 1, 2 y 3 la configuración inicial basada en los siguientes criterios:

- Nombre del dispositivo.
- Deshabilitar la búsqueda de DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Contraseña cifrada del modo EXEC privilegiado (cisco).
- Contraseña de consola (class), habilitando el inicio de sesión y agregando el comando logging synchronous. El comando logging synchronous sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.
- Contraseña de vty (class), habilitando el inicio de sesión y agregando el comando logging synchronous.
- Cifrado de contraseñas de texto no cifrado.

- Aviso de advierta a todo aquel que acceda al dispositivo, especificando que el acceso no autorizado está prohibido.
- Las contraseñas asignadas fueron elegidas según criterio propio.

A continuación, se muestra la configuración inicial para los Router 1, 2 y 3 del caso de estudio propuesto.

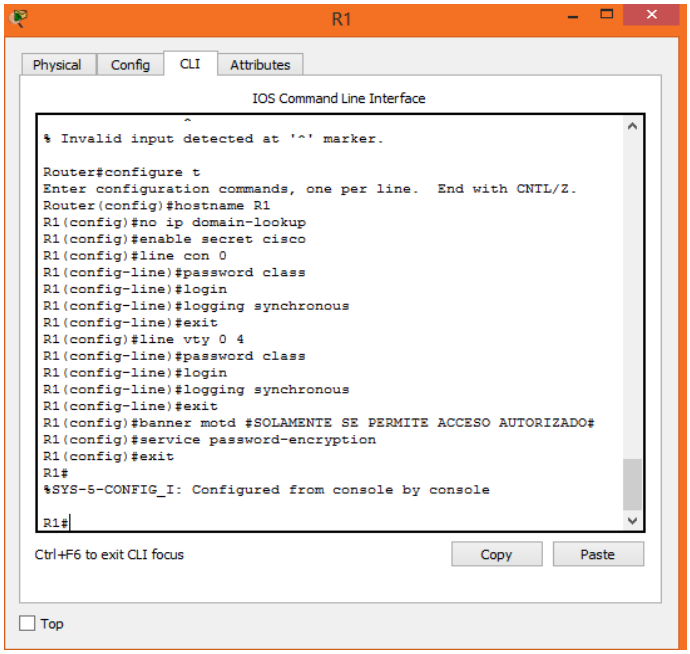

figura 12. Router 1 configuracion Inicial

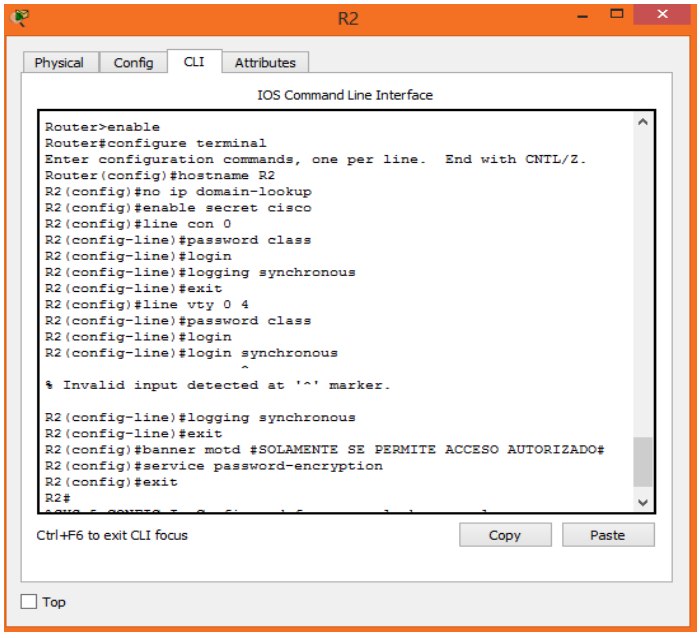

figura 13. Router 2 configuracion Inicial

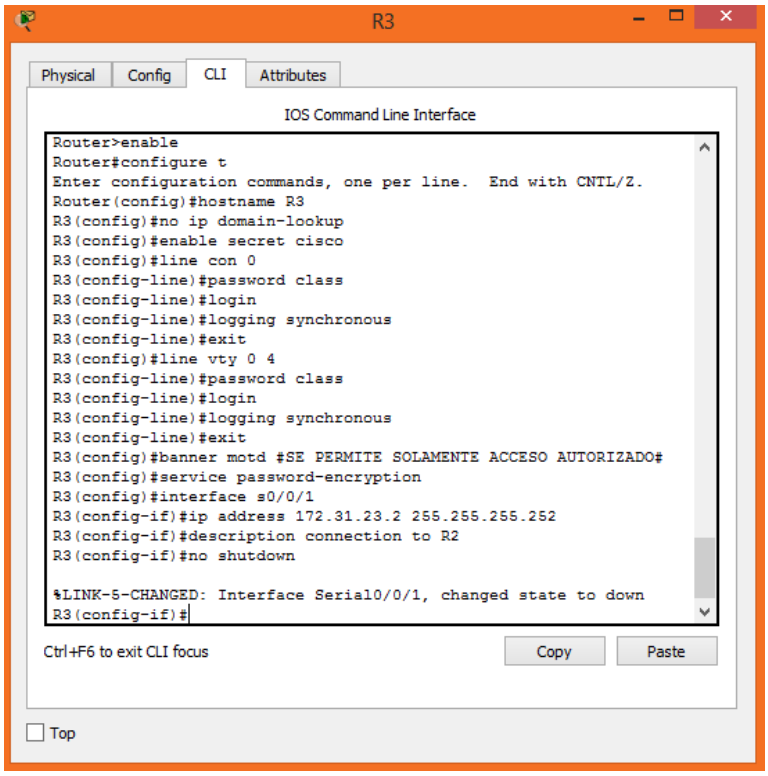

figura 14. Router 3 configuracion Inicial

4.2.2.3 ASIGNACIÓN DE DIRECCIONES IP A LAS INTERFACES.

Se asigna a cada interfaz de los Router 1,2 y 3 su dirección Ip, de acuerdo a las asignaciones establecidas en la tabla 1 Asignación IP y Gateway determinado.

A continuación, se muestra las asignaciones de direcciones IP para las interfaces de los Router 1,2 y 3.

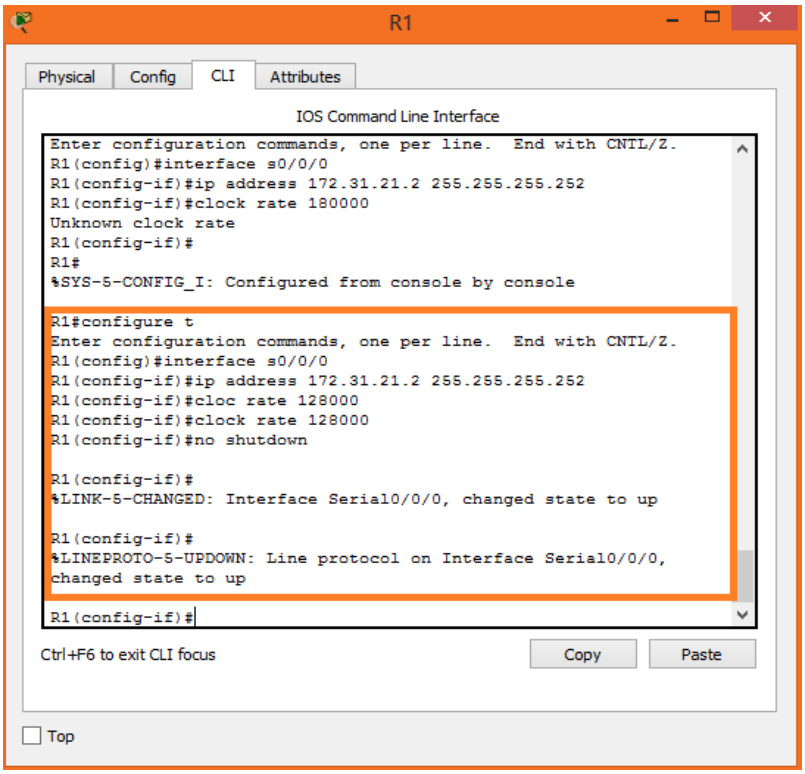

figura 15. Router 1 configuracion interfaz S0/0/0

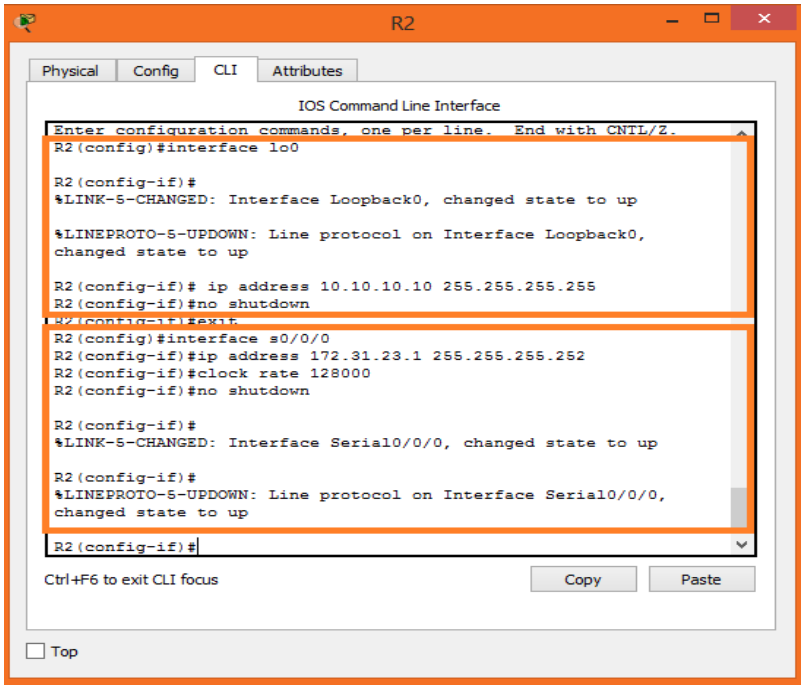

figura 16. Router 2. Configuracion interfaces Lo0 y S0/0/0

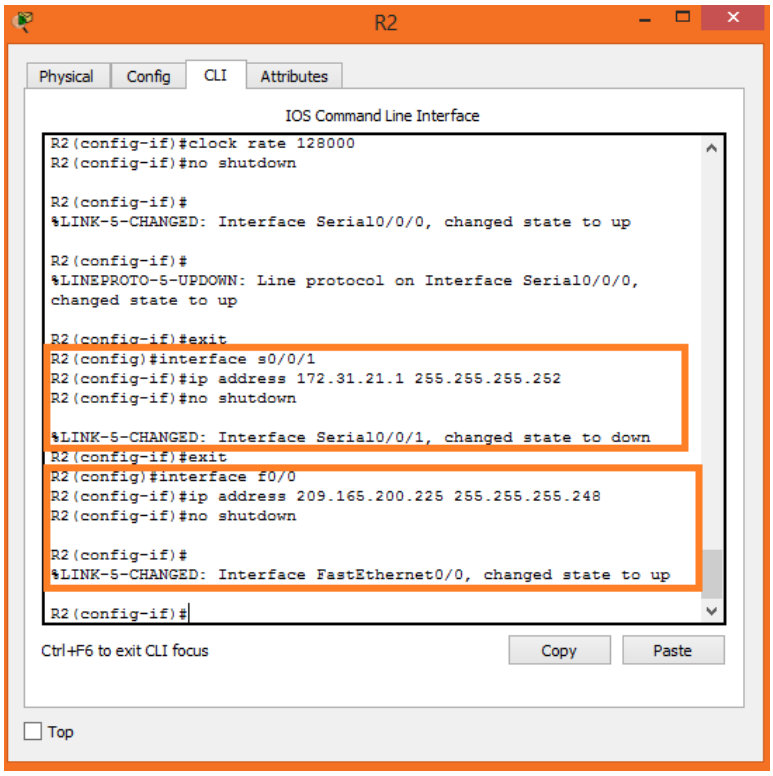

figura 17. Router 2. Configuracion interfaces s0/0/1 y F0/0

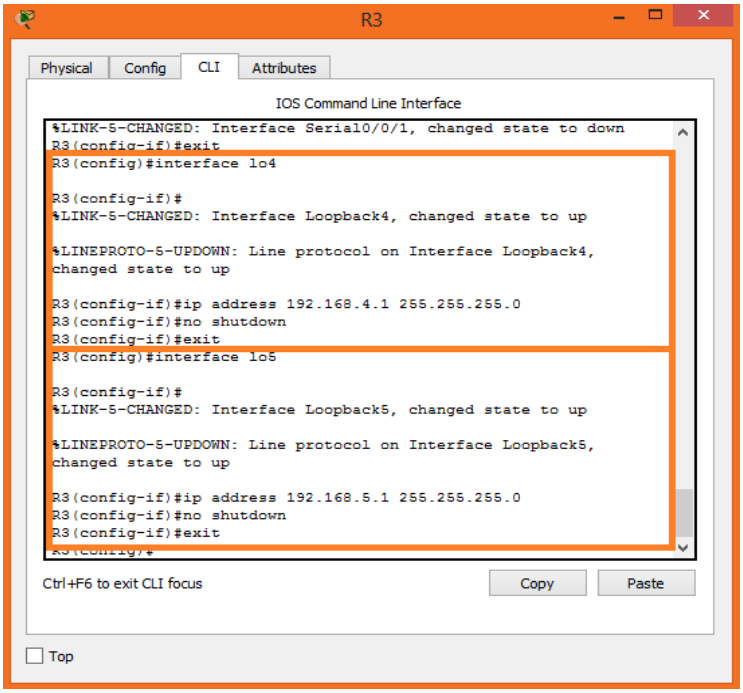

figura 18. Router 3. Configuracion interfaces lo4 y lo5

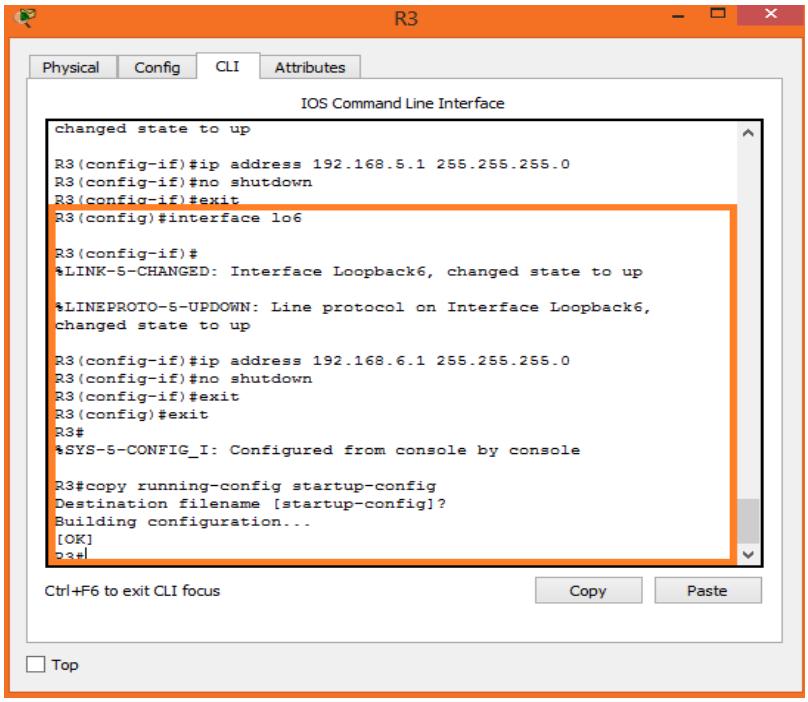

figura 19. Router 3. Configuracion interfaces lo6

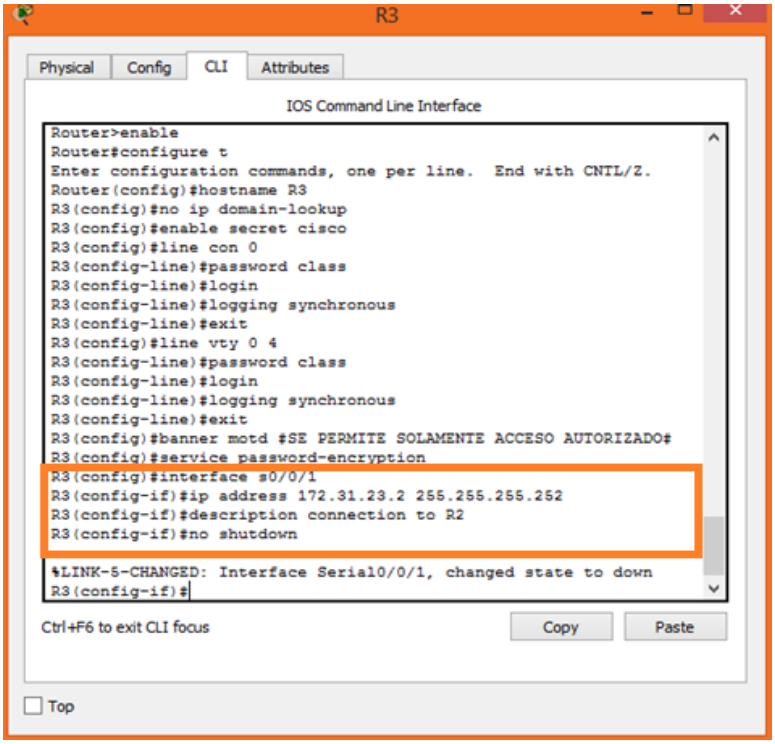

figura 20. Router 3. Configuracion interfaces S0/0/1

7. 4.2.3 OSPFV2 AREA 0.

OSPF es un protocolo estándar de enrutamiento que implementa el algoritmo de Dijkstra para calcular la ruta más corta a cada red de destino. Su métrica de enrutamiento es el costo de los enlaces, parámetro que se calcula en función del ancho de banda; por este motivo es de gran importancia la configuración del parámetro bandwidth en las interfaces que participan de este proceso de enrutamiento.
Este protocolo opera estableciendo relaciones de adyacencia con los dispositivos vecinos, a los que envía periódicamente paquetes hello. Adicionalmente, cada vez que un enlace cambia de estado inunda la red con la notificación de este cambio. Adicionalmente, cada 30 minutos envía a los dispositivos vecinos (o adyacentes) una actualización conteniendo todos los cambios de estado de enlaces de ese período.

4.2.3.1 CONFIGURACION DE LAS INTERFACES QUE PARTICIPAN EN EL PROCESO. COMANDO NETWORK.

Para configurar OSPF es necesario primero configurar las interfaces que participan en el proceso de Routing por lo que se utiliza el comando network, La sintaxis básica del comando es network dirección-red máscara-wildcard area id-área. Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección debe examinar para obtener una coincidencia.
A continuación, se muestra la configuración de OSPF para los router 1,2 y 3.

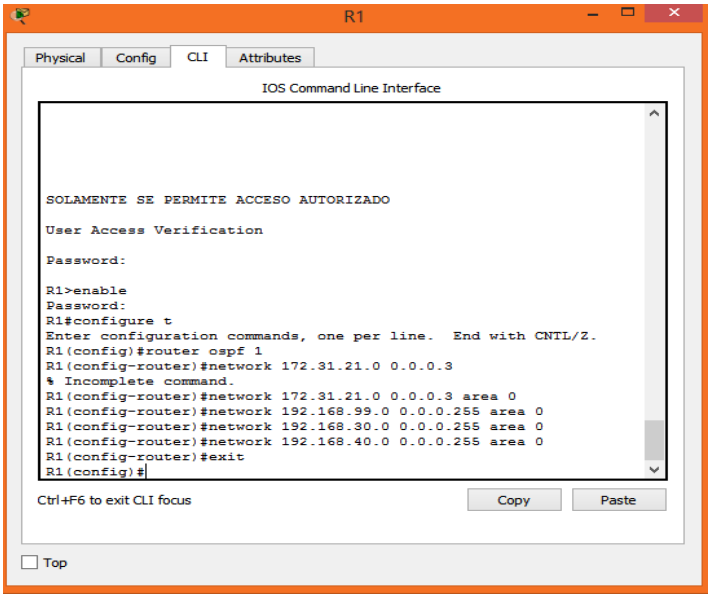

figura 21. Router 1 comando network

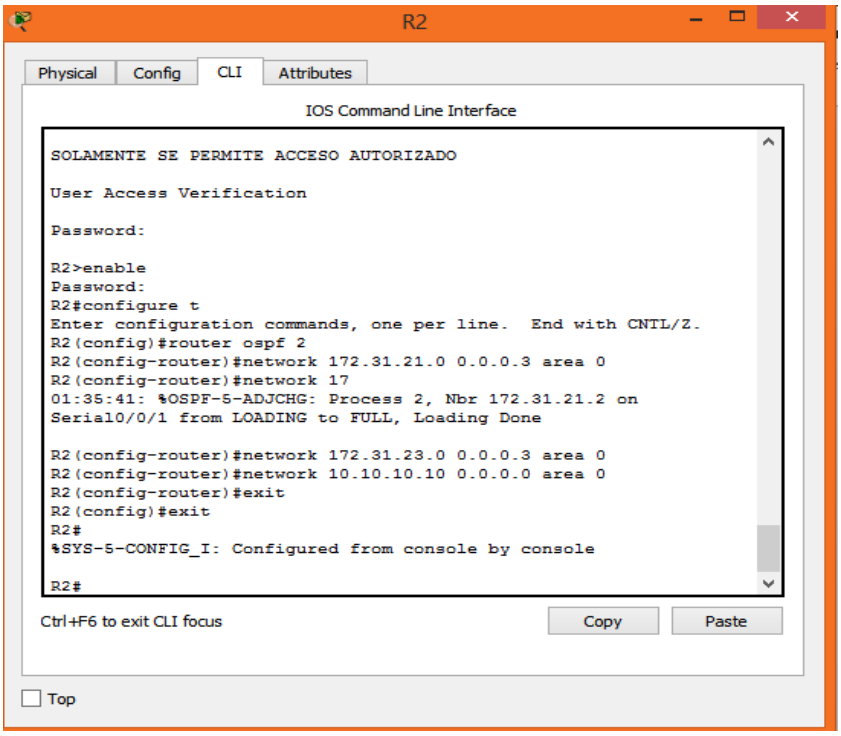

figura 22. Router 2 comando network

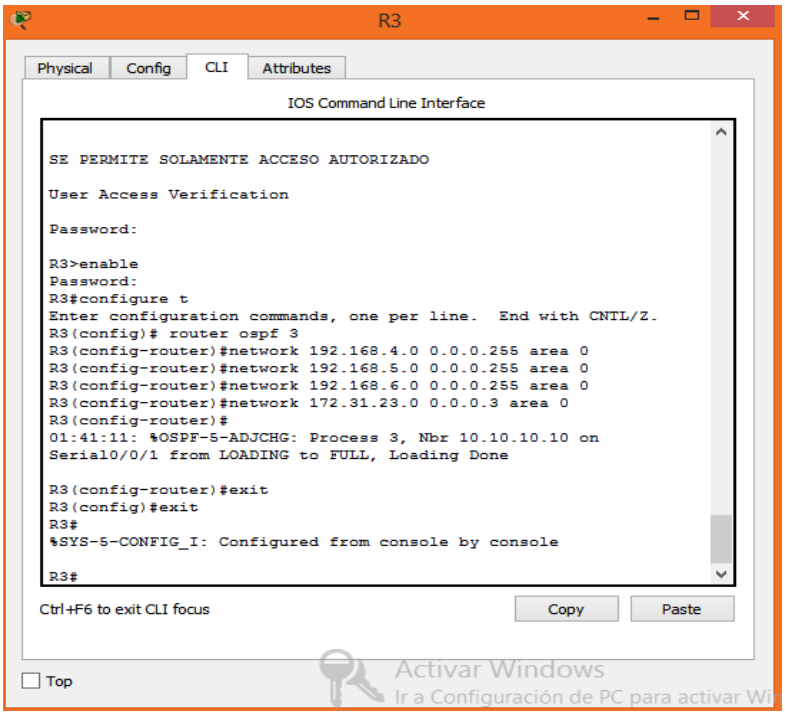

figura 23. Router 3 comando network

4.3.2.2 CONFIGURACION DE ID DE ROUTER OSPF.

Se utiliza el comando router-id id-router del modo de configuración del router para asignar manualmente un valor de 32 bits expresado como dirección IPv4 a un router. Un router OSPF se identifica ante otros routers mediante esta ID del router.

A continuación, se muestra la configuración de ID para los router 1,2 y 3 de acuerdo a los valores entregados en el caso de estudio.

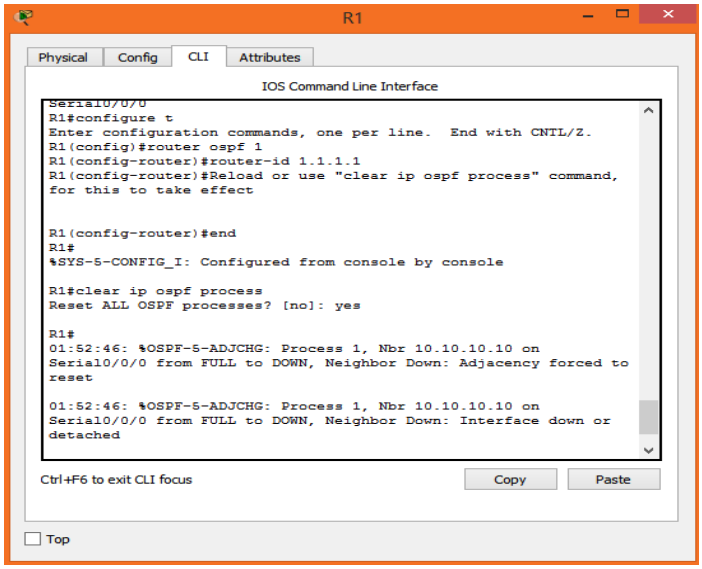

figura 24. Router 1 asignacion de ID OSPF

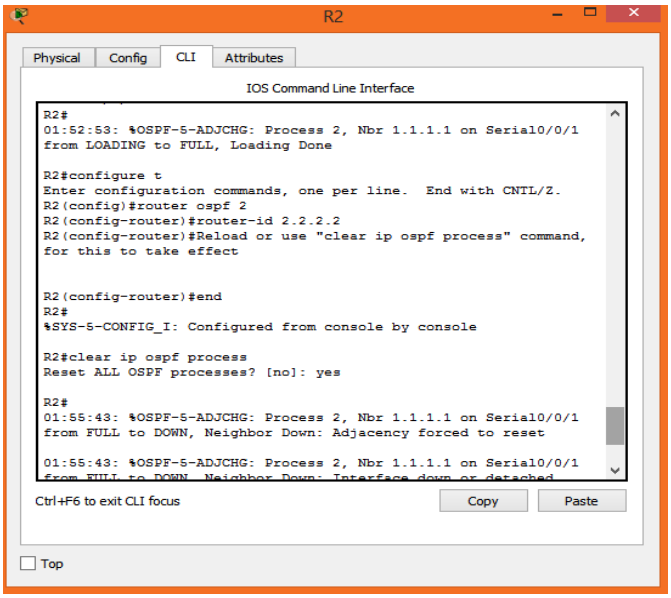

figura 25. Router 2 asignacion de ID OSPF

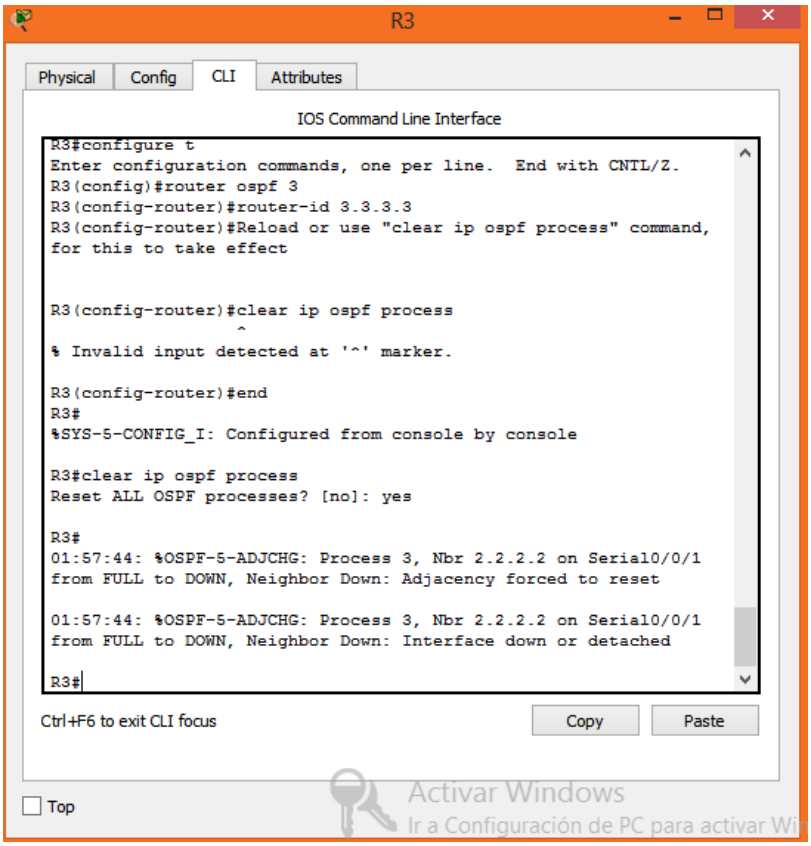

figura 26. Router 3 asignacion de ID OSPF

4.3.2.3 CONFIGURACION DE LAS INTERFACES PASIVAS.

Una vez se han configurado las interfaces participantes con el comando network se deben configurar las interfaces pasivas, a las que no llegaran los mensajes OSPF, debido a que estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado.

Para nuestro caso de estudio se configura la interfaz FastEthernet 0/0 del router 1 como pasiva. Porque esta interfaz no se conecta a otros router y no es necesario el envío de este tipo de mensajes.

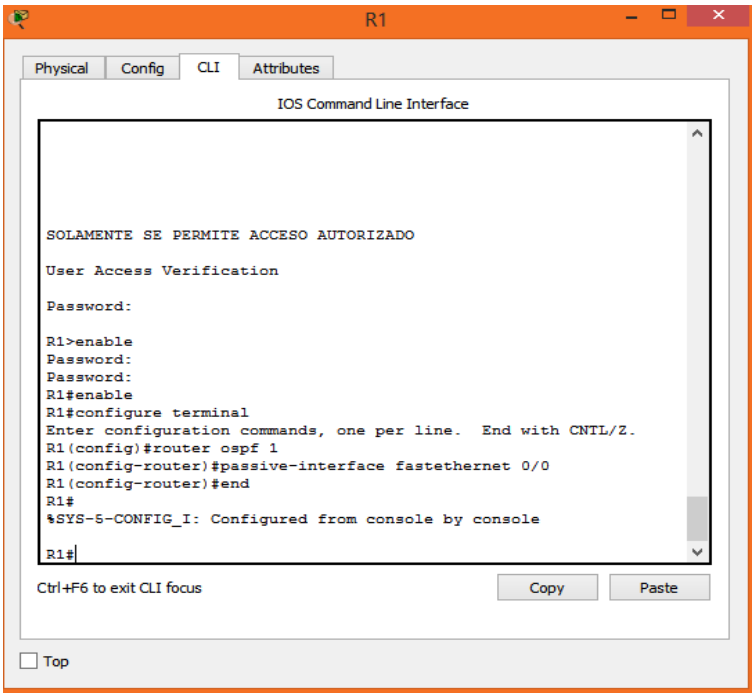

figura 27. Router 1 configuracion interfaz f0/0 como pasiva

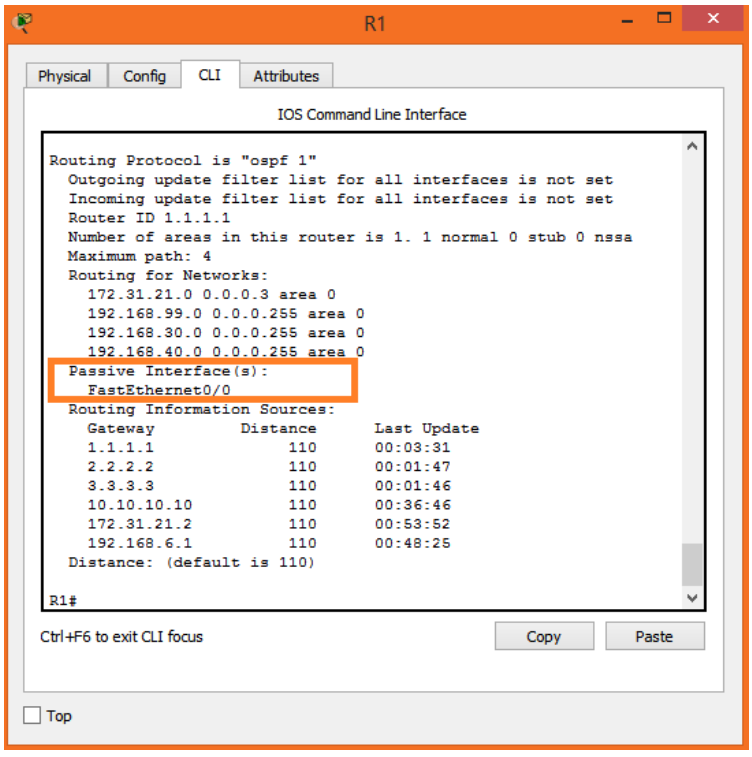

figura 28. Router 1 Verificacion configuracion interfaz pasiva F0/0

4.3.2.4 CONFIGURACION ANCHO DE BANDA INTERFACES SERIALES.

Para ajustar el ancho de banda de una interfaz se utiliza el comando de configuración de interfaz bandwidth kilobits. Se utiliza el comando no bandwidth para restaurar el valor predeterminado. Teniendo presente que se debe ajustar el ancho de banda en cada extremo de los enlaces seriales.

A continuación, se muestra la configuración de ancho de banda de las interfaces seriales según lo solicitado en 128kb/s.

- Configuración Router 1.

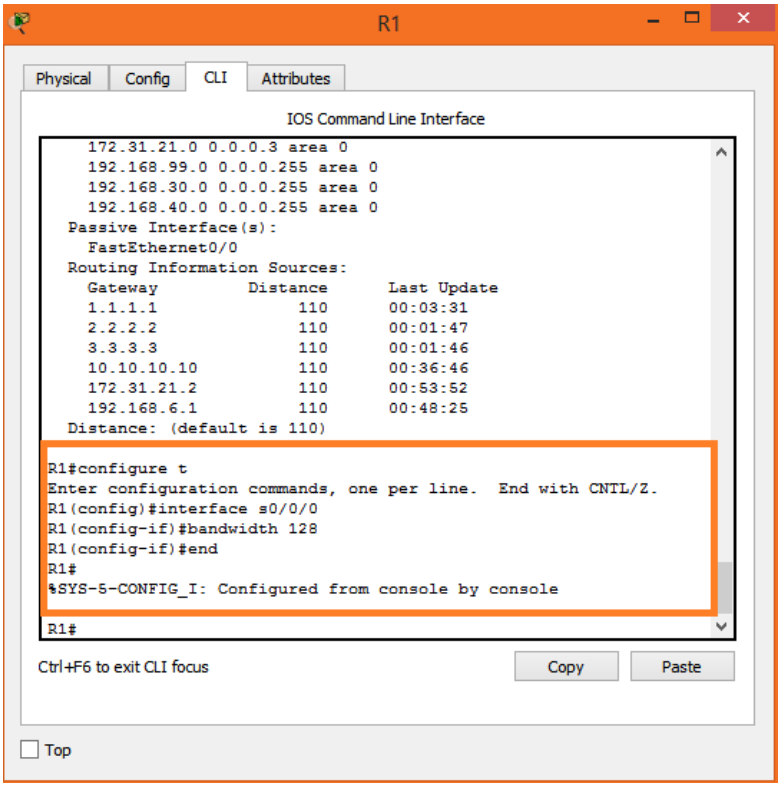

figura 29. Router 1 configuracion ancho de banda interfaz S0/0/0

Utilizando el comando Show interface Serial 0/0/0 de puede comprobar que la interfaz haya cambiado su configuracion según lo programado, para nuestro caso 128.

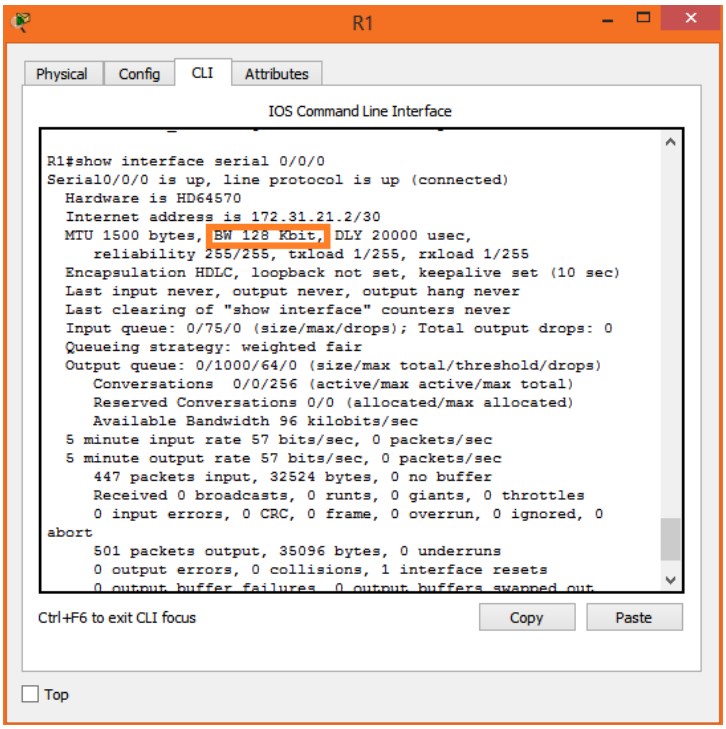

figura 30. Router 1 Verificacion configuracion ancho de banda interfaz S0/0/0

- Configuración Router 2.

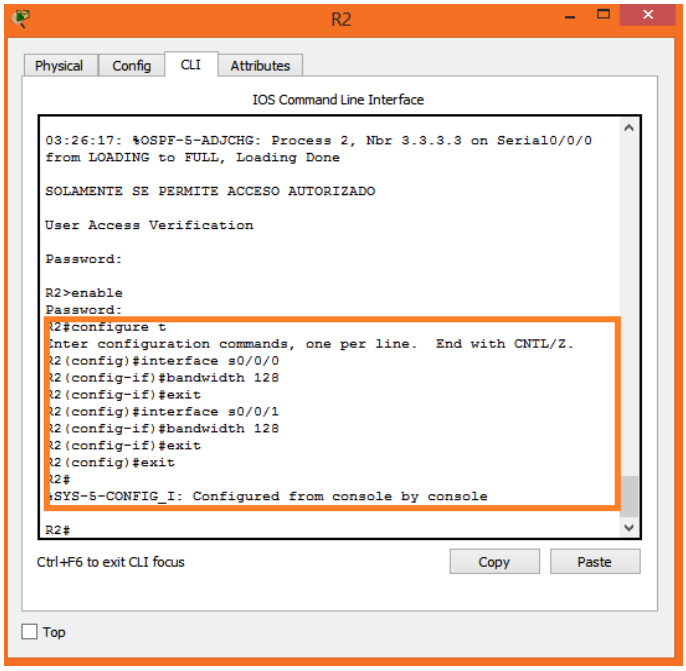

figura 31. Router 2 configuracion ancho de banda interfaz S0/0/0 y S0/0/1

Utilizando el comando Show interfaz Serial 0/0/0 y Show interfaz Serial 0/0/01 se puede comprobar que las interfaces hayan cambiado su configuracion según lo programado, para nuestro caso 128.

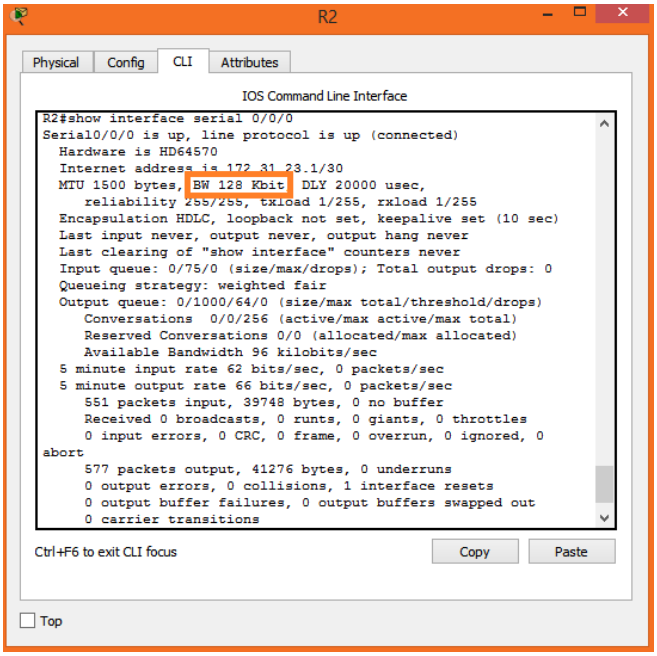

figura 32. Router 2 Verificacion configuracion ancho de banda interfaz S0/0/0

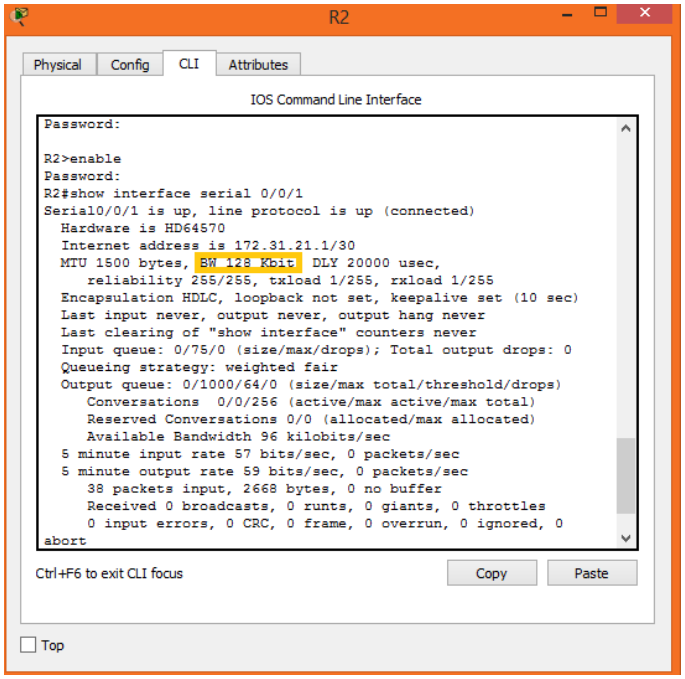

figura 33. Router 2 Verificacion configuracion ancho de banda interfaz S0/0/1

- Configuración Router 3.

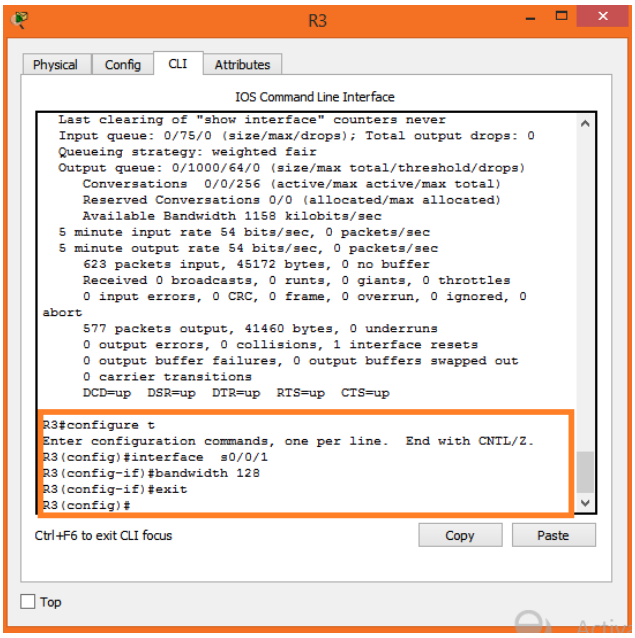

figura 34. Router 3 configuracion ancho de banda interfaz S0/0/1

Utilizando el comando Show interfaz Serial 0/0/1 se puede comprobar que la interfaz haya cambiado su configuracion según lo programado, para nuestro caso 128.

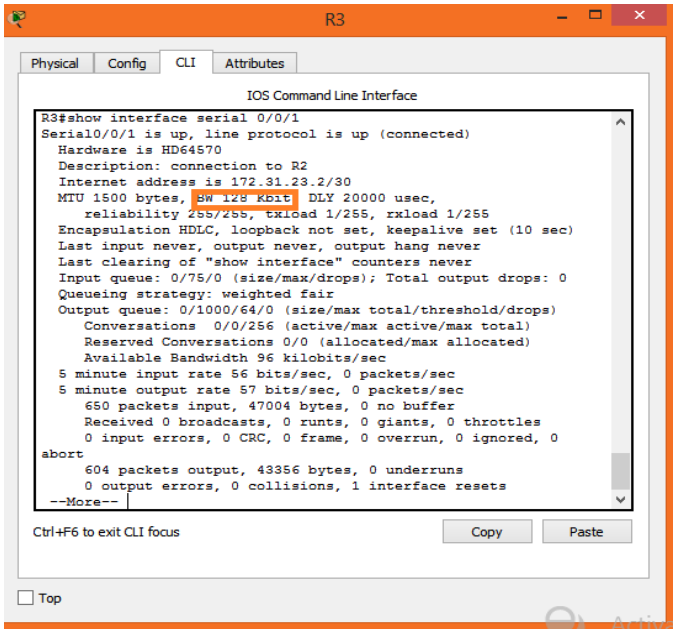

figura 35. Router 3 Verificacion configuracion ancho de banda interfaz S0/0/1

4.3.2.5 AJUSTE DEL COSTO DE LA MÉTRICA.

Se configura el costo de forma manual en una interfaz con el comando de configuración de interfaz ip ospf costo valor**.**

Una ventaja de configurar un costo en lugar del ancho de banda de la interfaz es que cuando se configura el costo manualmente, el router no necesita calcular la métrica. En cambio, cuando se configura el ancho de banda de la interfaz, el router debe calcular el costo de OSPF sobre la base del ancho de banda.

A continuación, se muestra la configuración del costo de la métrica para las interfaces S0/0/0 en 7500, esta métrica se cambió para los Router 1 y 2 los cuales son los equipos que cuentan con una interfaz S0/0/0.

- Configuración Router 1.

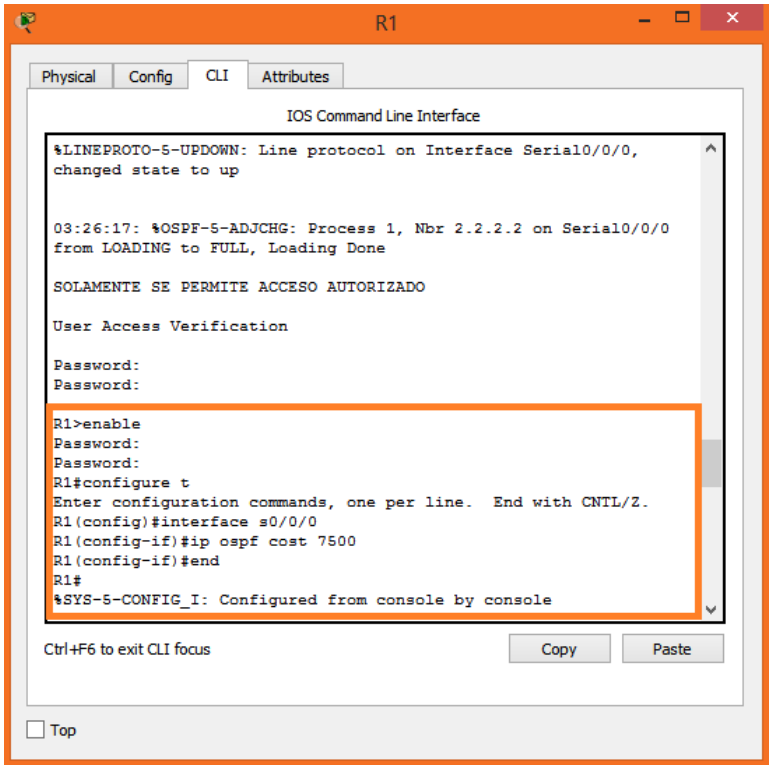

figura 36. Router 1 configuracion costo de la metrica interfaz S0/0/0

Con el comando show ip ospf interface serial 0/0/0 se puede verificar el cambio de métrica realizado.

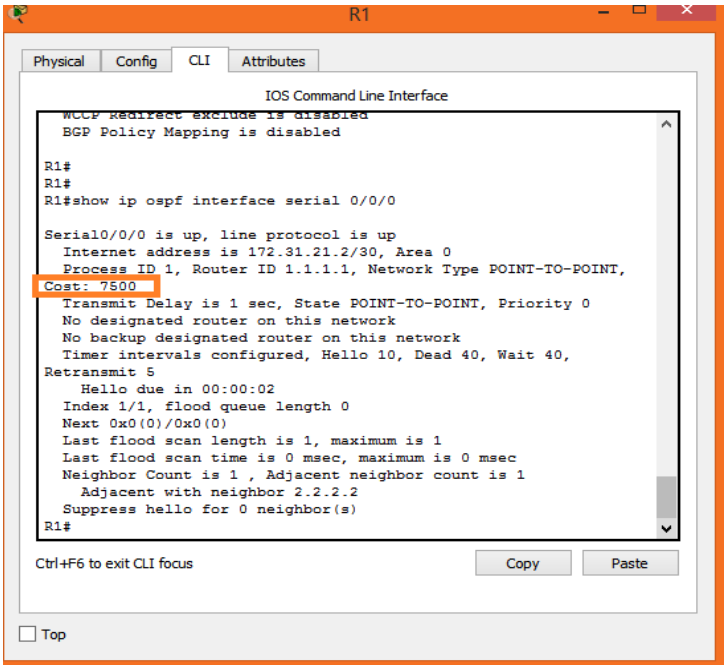

figura 37. Router 1 verificacion configuracion costo de la metrica interfaz S0/0/0

- Configuración Router 2.

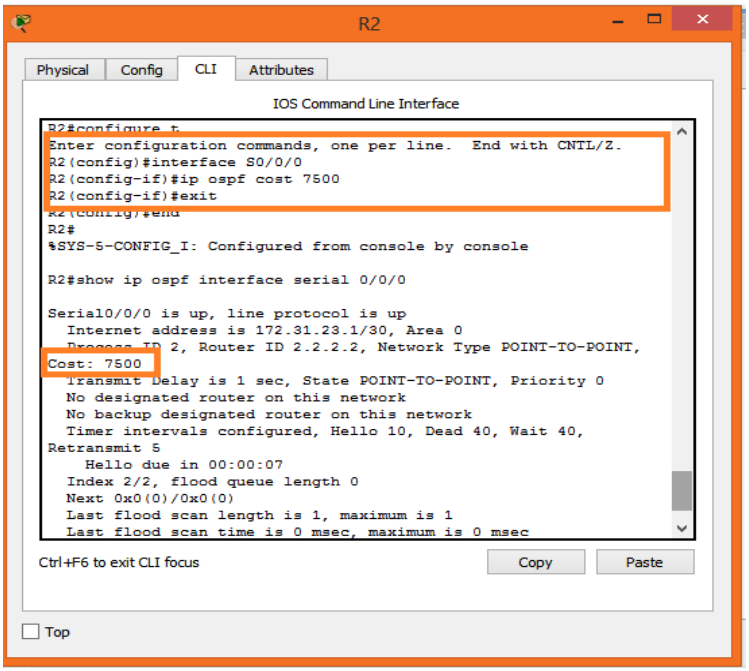

figura 38. Router 2 cambio y verificacion configuracion costo de la metrica interfaz S0/0/0

4.3.2.6 VERIFICAR INFORMACIÓN DE OSPF.

Comando show ip route: Se utiliza el comando show ip route para visualizar el contenido de la tabla de enrutamiento de cada router.

A continuación, se muestra la tabla de enrutamiento para los router 1,2 y 3

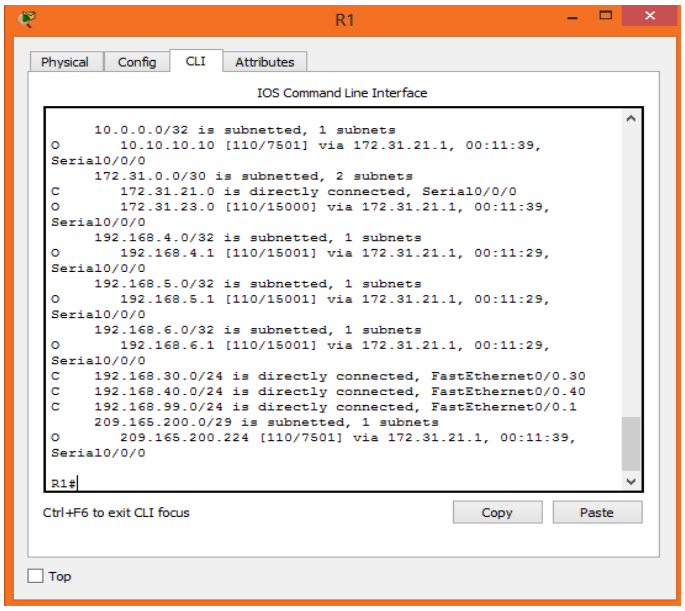

figura 39. Router 1 tabla de enrutamiento comando show ip route

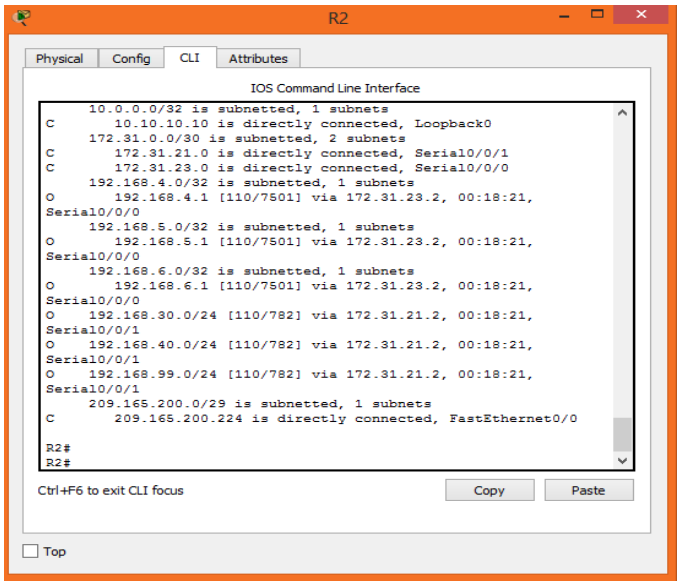

figura 40. Router 2 tabla de enrutamiento comando show ip route

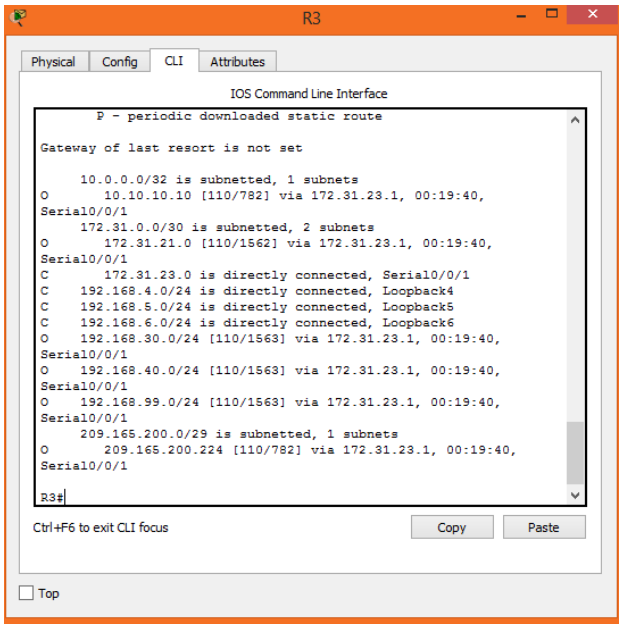

figura 41. Router 3 tabla de enrutamiento comando show ip route

Comando show ip ospf neighbor: Se utiliza el comando show ip ospf neighbor para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

A continuación, se muestra la adyacencia para los router 1, 2 y 3.

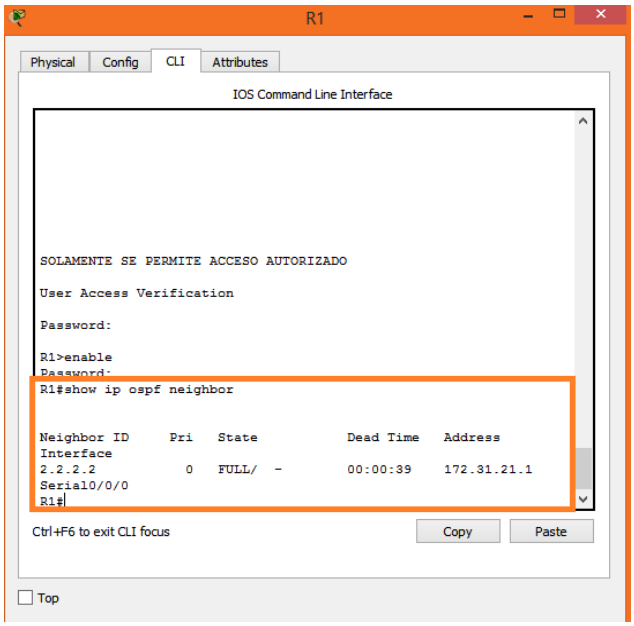

figura 42. Router 1 Verificacion adyacencia con los router vecinos

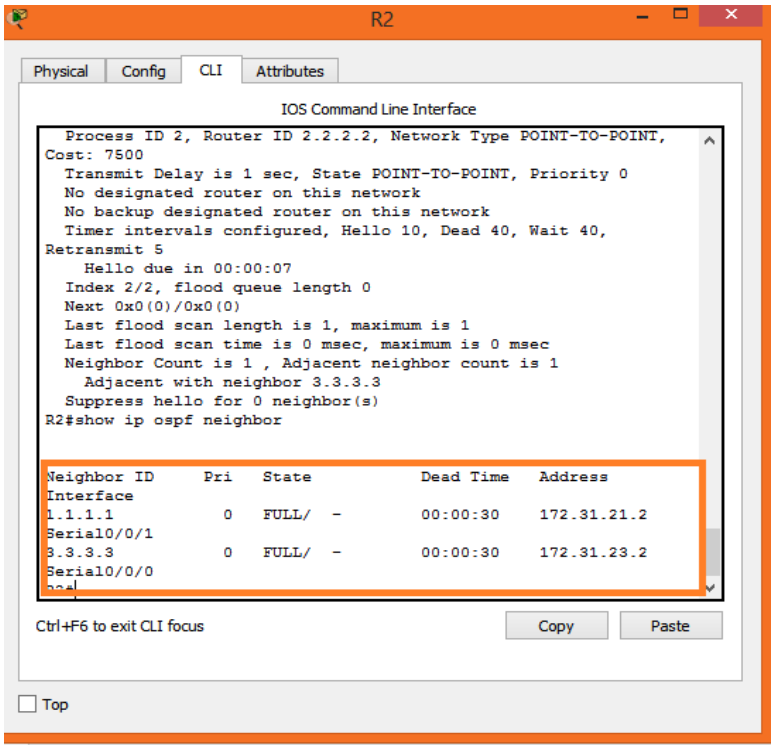

figura 43. Router 2 Verificacion adyacencia con los router vecinos

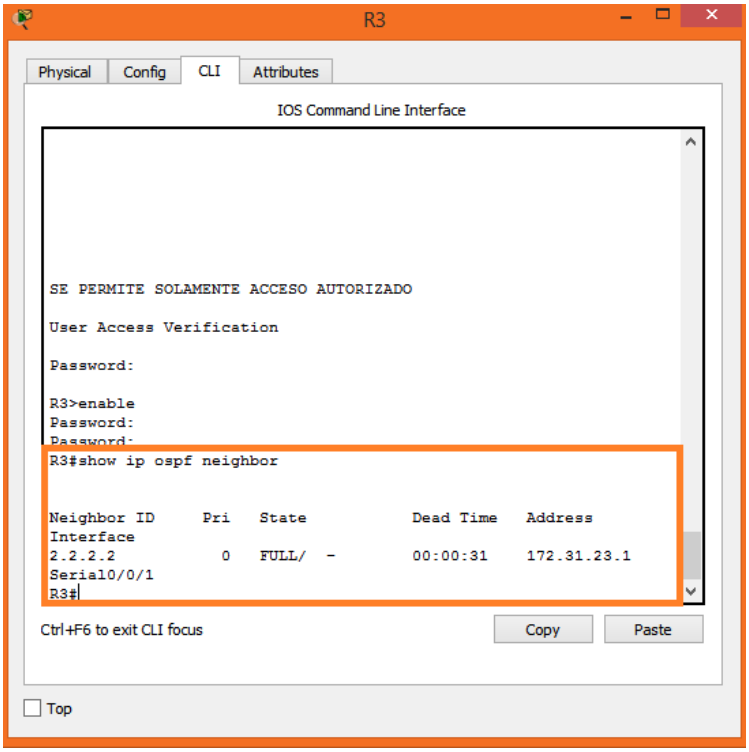

figura 44. Router 3 Verificacion adyacencia con los router vecinos

Comado Show ip route ospf: Se utiliza el comando show ip route ospf para mostrar solo las rutas OSPF descubiertas en la tabla de routing.

A continuacion, se muestra solo las rutas OSPF para los router 1,2 y 3 aplicando el comando show ip route ospf.

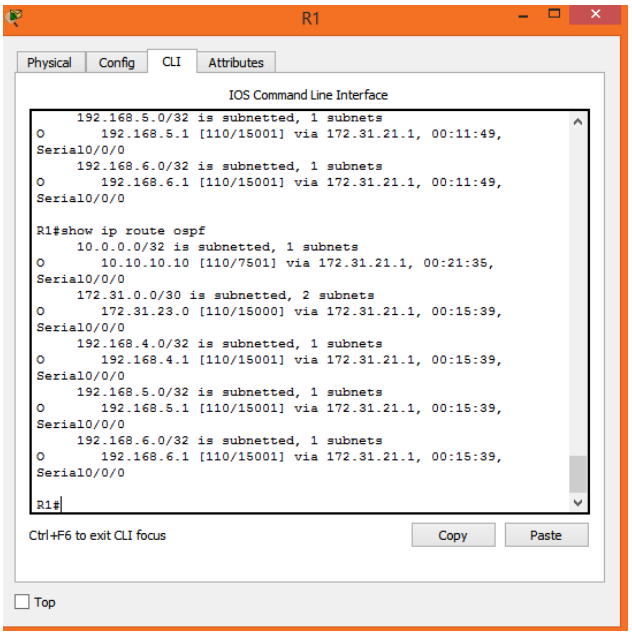

figura 45. Router 1 solo rutas OSPF comando show ip route ospf

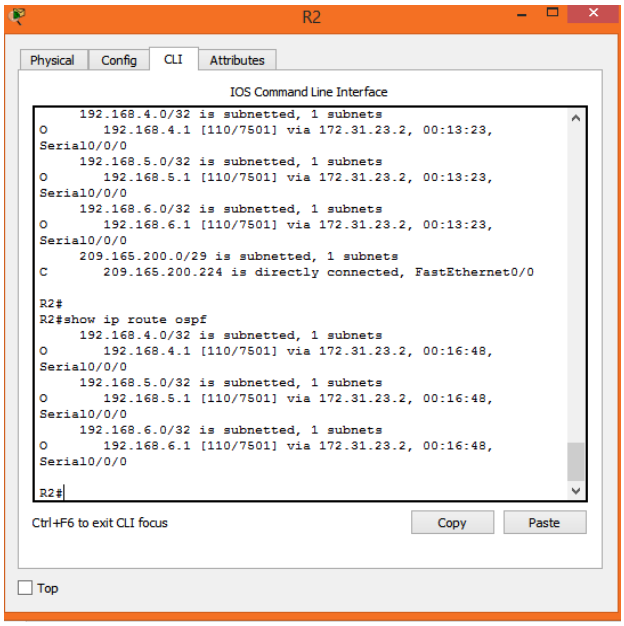

figura 46. Router 2 solo rutas OSPF comando show ip route ospf

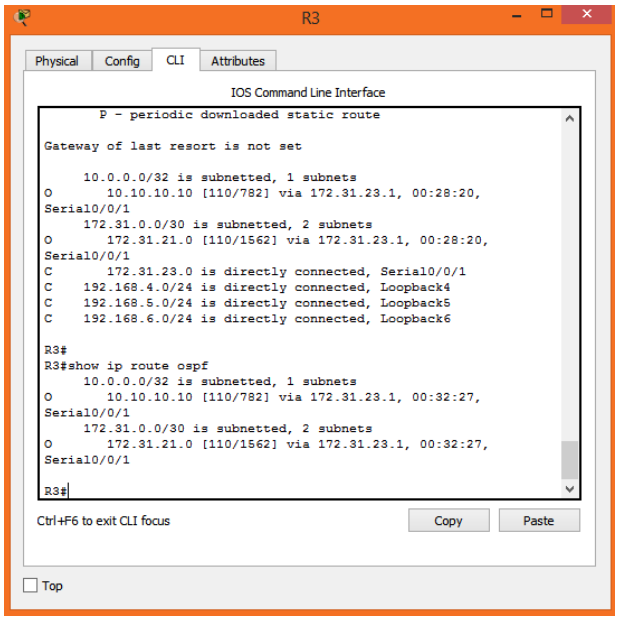

figura 47. Router 3 solo rutas OSPF comando show ip route ospf

Comando show ip protocols: El comando show ip protocols es una manera rápida de verificar información fundamental de configuración de OSPF. Esta información incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

A continuacion, se visualiza la informacion fundamental de la configuracion OSPF para los router 1, 2, 3 aplicando el comando show ip protocols.

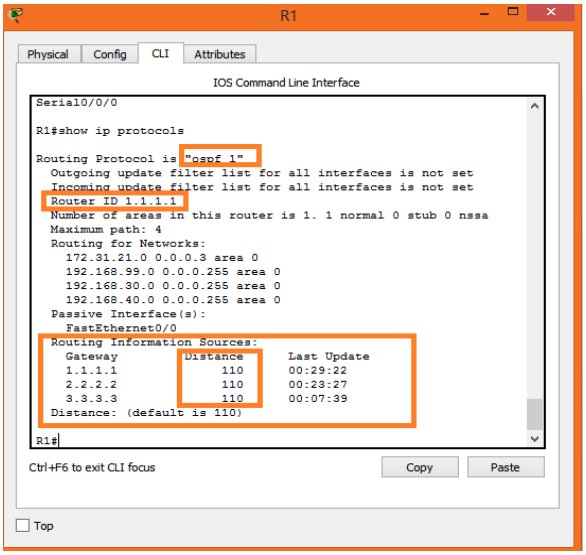

figura 48. Router 1 comando show ip protocols

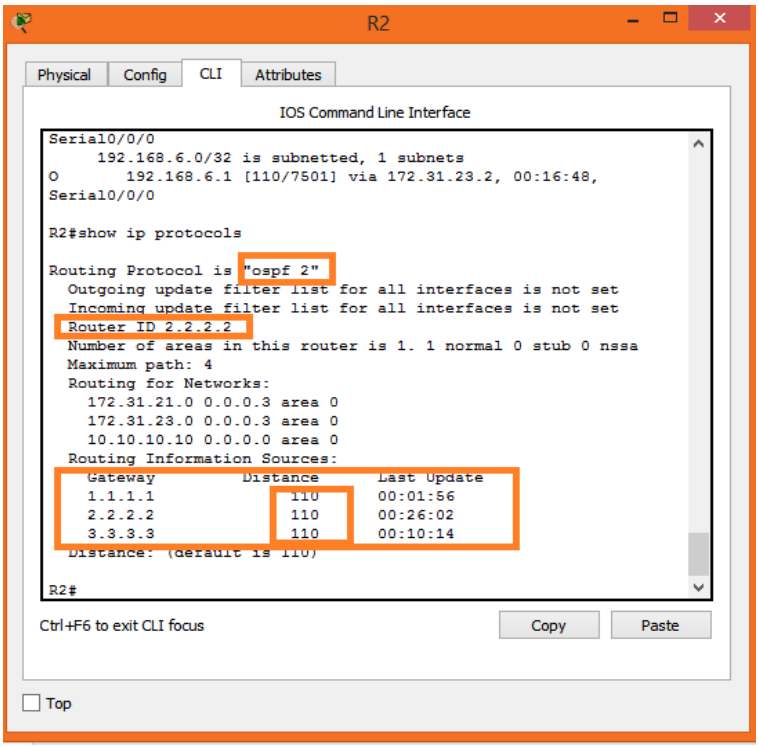

figura 49. Router 2 comando show ip protocols

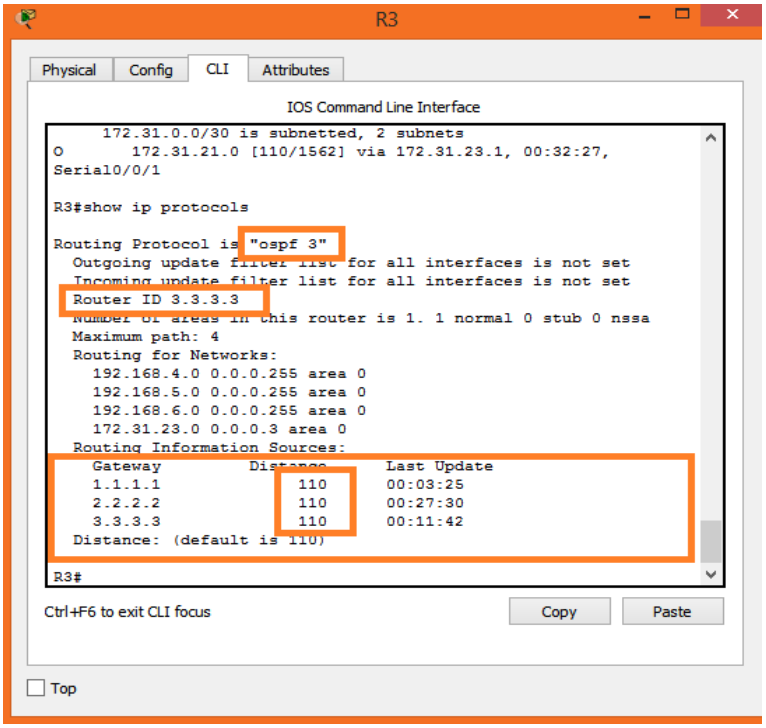

figura 50. Router 3 comando show ip protocols

Comando show ip ospf : El comando show ip ospf se utiliza para examinar la ID del proceso OSPF y la ID del router. Este comando muestra información del área OSPF y la última vez que se calculó el algoritmo SPF.

A continuacion, se muestra la ID del proceso OSPF y la ID del router para los Router 1,2 y 3 aplicando el comando show ip ospf .

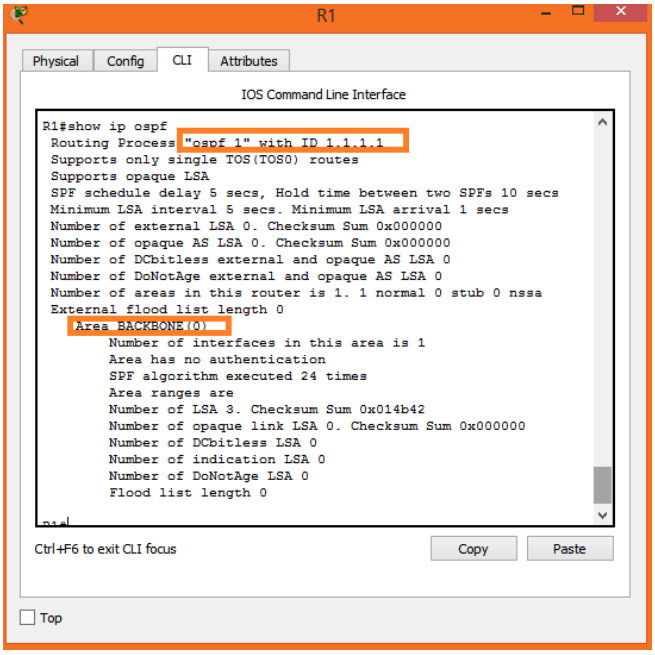

figura 51. Router 1 comando show ip ospf

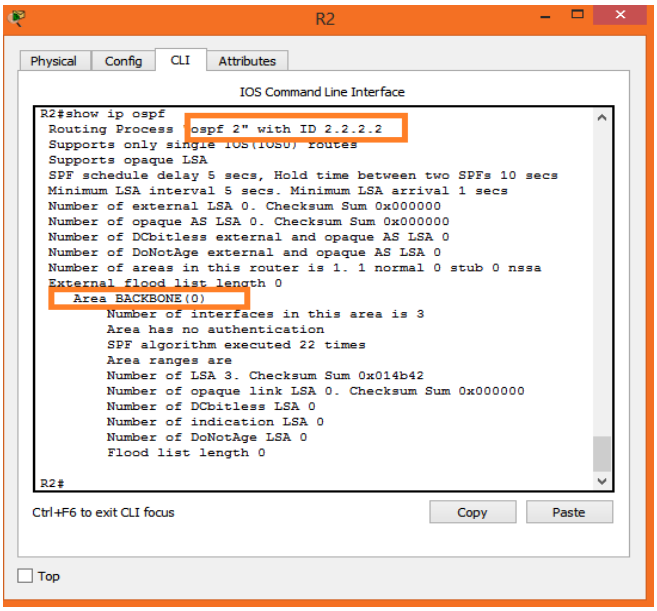

figura 52. Router 2 comando show ip ospf

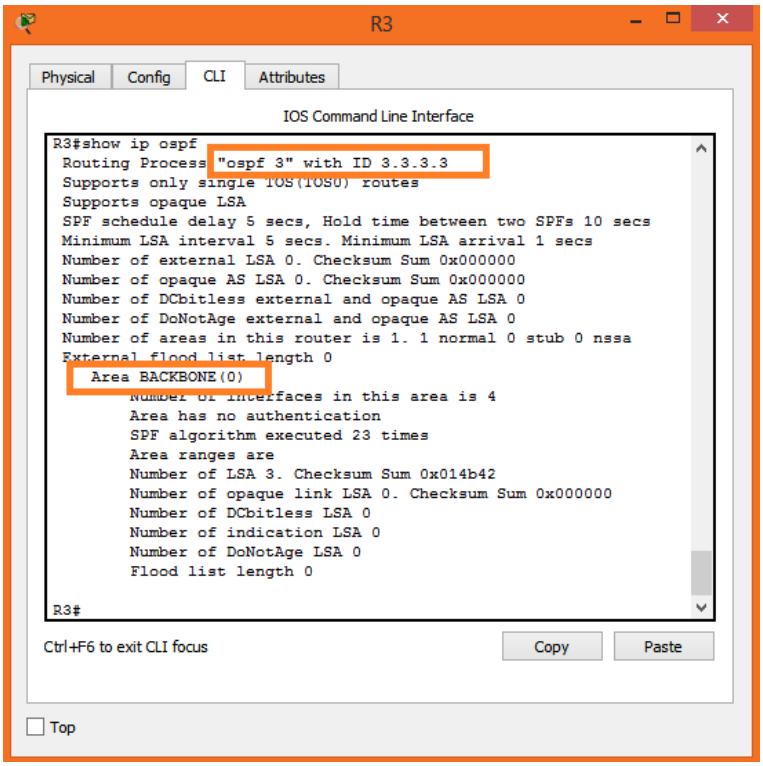

figura 53. Router 3 comando show ip ospf

8. 4.2.4. CONFIGURACION VLANS.

Las VLAN se utilizan para segmentar redes conmutadas. Una VLAN es un dominio de difusión, por lo que las computadoras en VLAN separadas no pueden comunicarse sin la intervención de un dispositivo de routing.

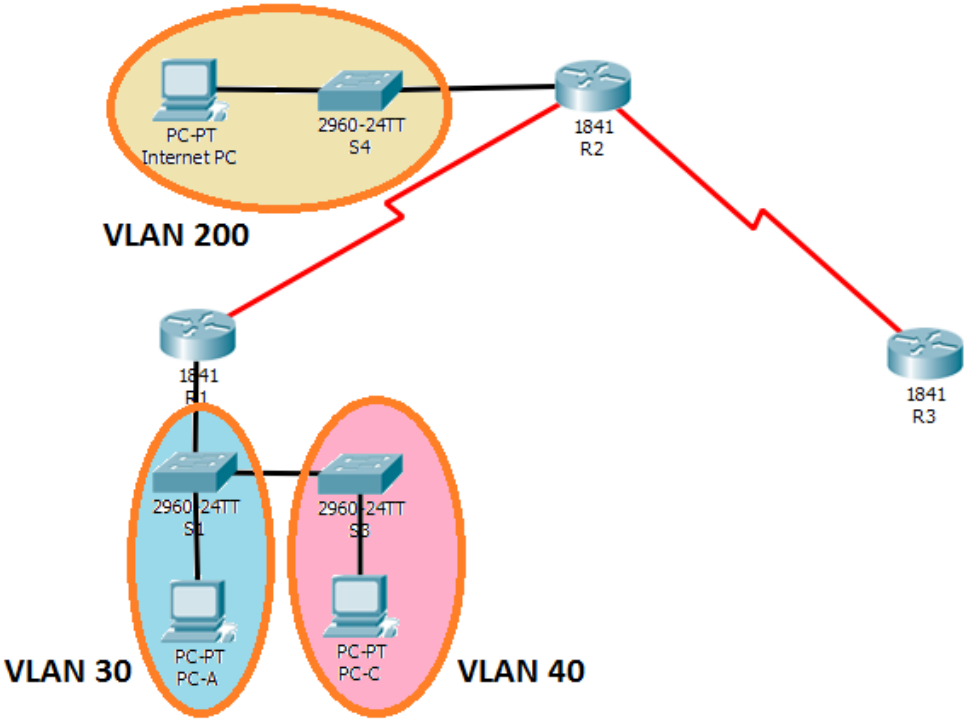

figura 54. Esquema VLAN configuradas. Fuente Propia

4.2.4.1 CREACION DE VLAN.

Para configurar las VLAN el primer paso es realizar la creacion de las VLAN en el switch, entrando al modo de configuracion global, emitiendo el comando VLAN y especificando el identificador id-vlan, luego con el comando name se agrega el nombre de la VLAN creada y se regresa al modo EXEC privilegiado.

La configuracion entregada para el caso de estudio fue modificada debido a que era necesario para la configuracion de la VLAN 200, agregar un switch en este caso nombrado como S4.

A continuacion, se muestra la configuracion de las VLAN 30, 40 y 200 solicitadas para el caso de estudio.

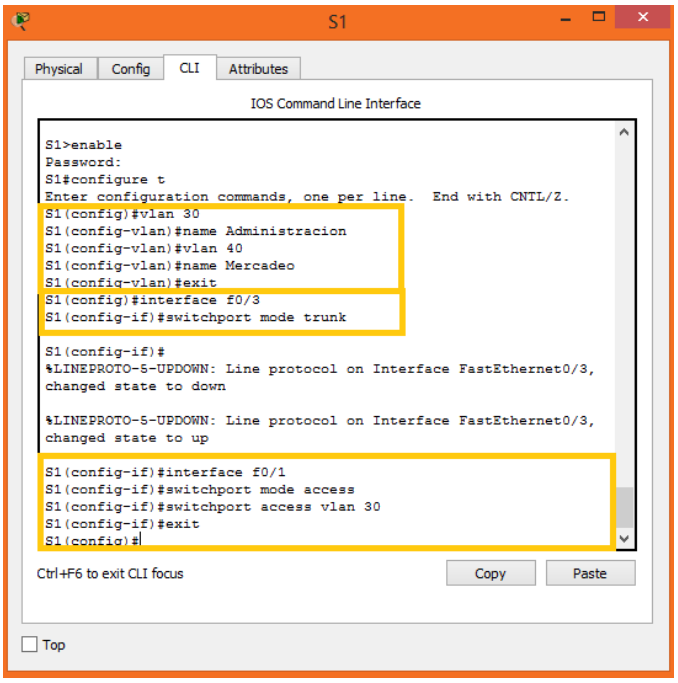

figura 55. S1 Creacion VLAN 30 y VLAN 40

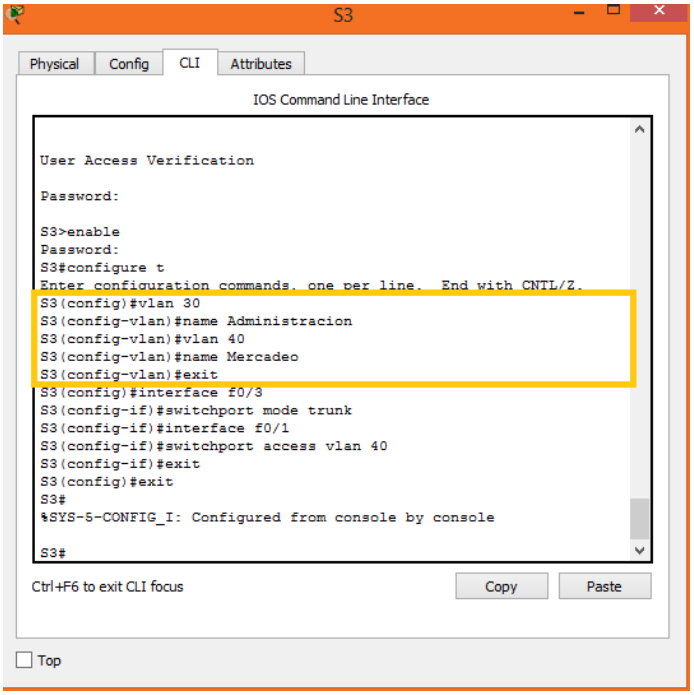

figura 56. S3 Creacion VLAN 30 y VLAN 40

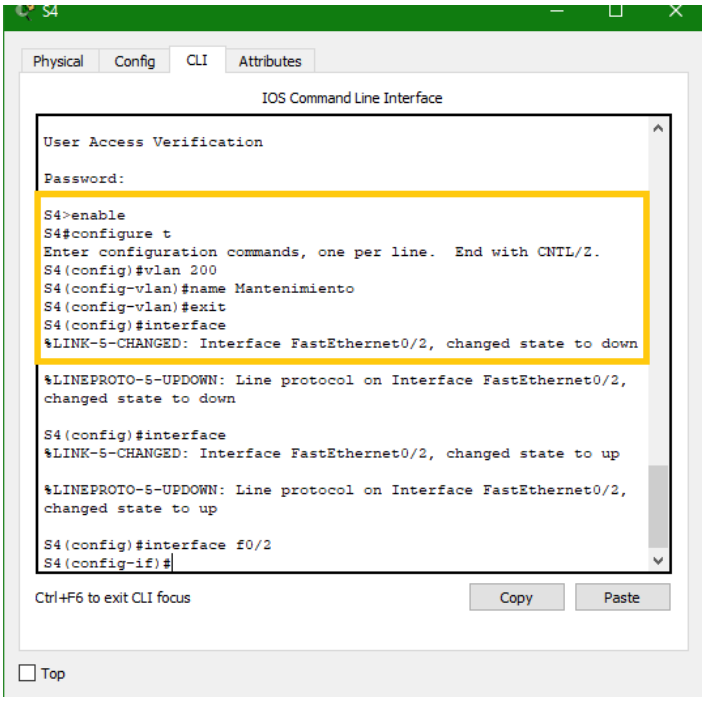

Figura 57. S4 Creacion VLAN 200

Aplicando el comando show vlan brief a continuacion se puede visualizar la VLAN Configuradas.

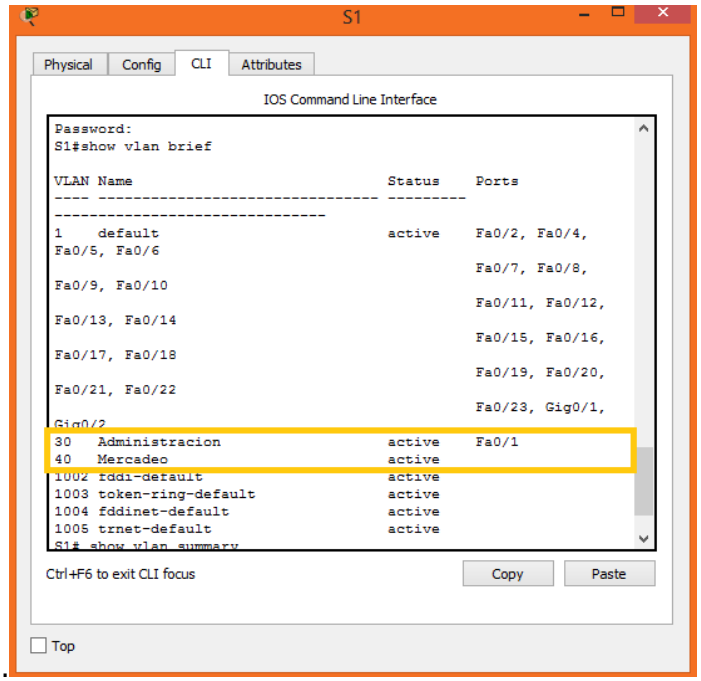

Figura 58. S1 Verificacion Creacion VLAN 30 y VLAN 40 utilizando comando show vlan brief.

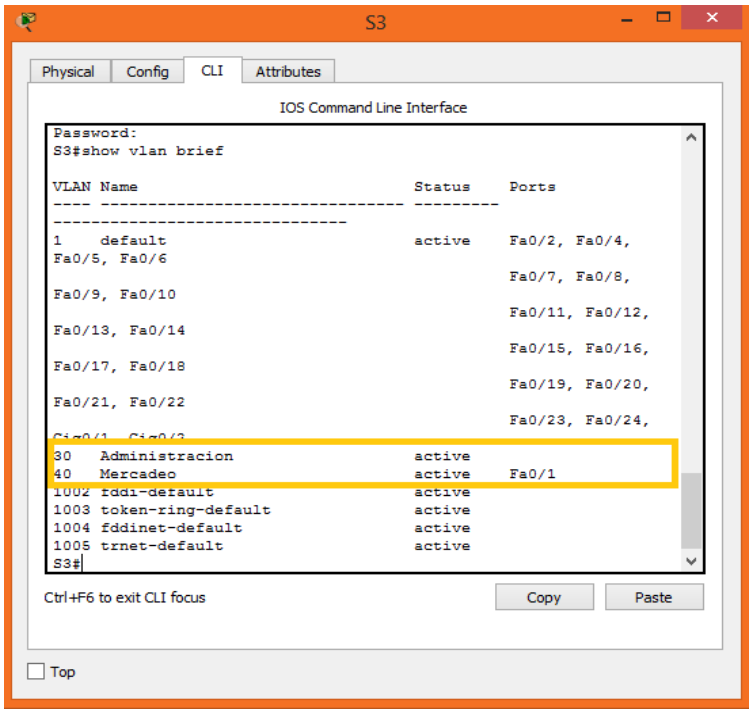

Figura 59. S2 Verificacion Creacion VLAN 30 y VLAN 40 utilizando comando show vlan brief.

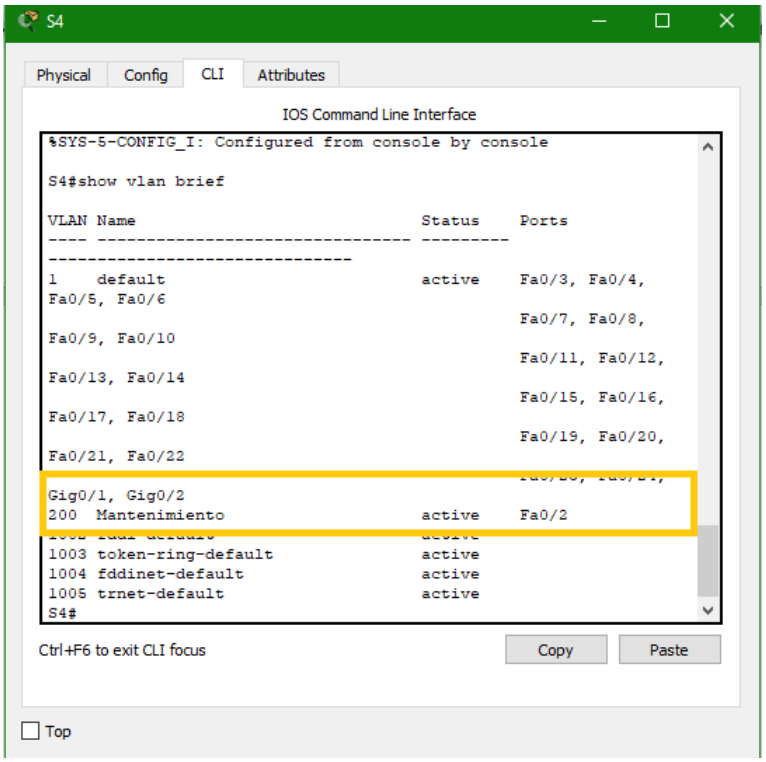

Figura 60. Verificación S4 Creacion VLAN 200 utilizando comando show vlan brief.

4.2.4.2 PUERTOS DE ACCESO.

Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.

Para asignar un puerto a una Vlan se debe ingresar al modo de configiracion global del switch, se ingresa al modo de configuracion de interfaz para la SVI, se establece el puerto en modo de acceso, se asigna el puerto a una VLAN y se regresa al modo EXEC privilegiado. Para ambos swtches (S1 y S3) el puerto de acceso es la interfaz F0/1, configuracion que se muestra a continuacion.

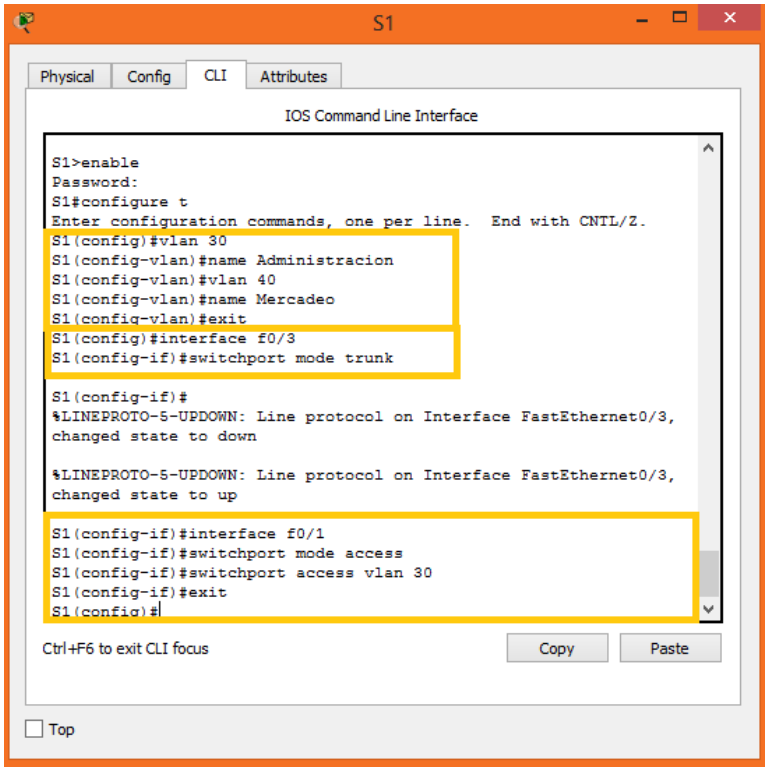

Figura 61. S1 Configuracion F0/1 como puerto de acceso VLAN 30

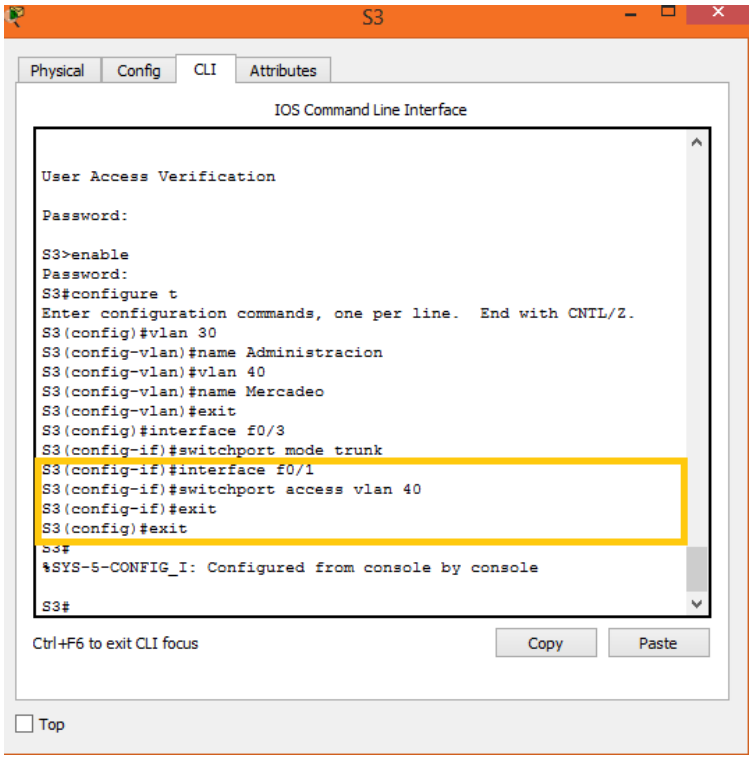

Figura 62. S3 Configuracion F0/1 como puerto de acceso VLAN 40

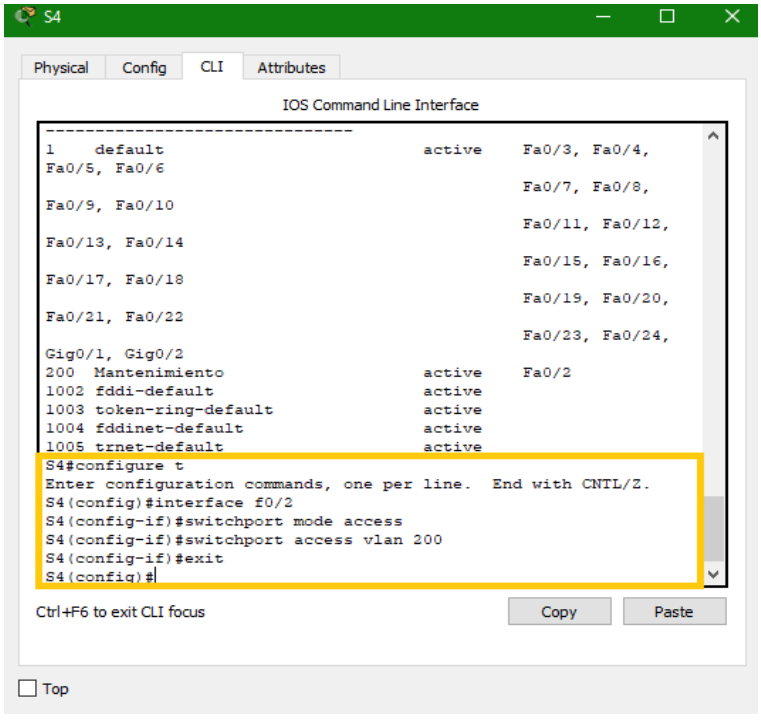

Figura 63. S4 Configuracion F0/2 como puerto de acceso VLAN 200

4.2.4.3 PUERTOS TRONCALES.

Un enlace troncal de VLAN es un enlace de capa 2 del modelo OSI entre dos switches que transporta el tráfico para todas las VLAN (a menos que se restrinja la lista de VLAN permitidas de manera manual o dinámica). Para habilitar los enlaces troncales se debe configurar los puertos en cualquier extremo del enlace físico con conjuntos de comandos paralelos.

Para configurar un puerto de switch en un extremo de un enlace troncal, se utiliza el comando switchport mode trunk. Con este comando, la interfaz cambia al modo de enlace troncal permanente. El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio.

A continuacion, se muestra la configuracion del enlace troncal para la interfaz F0/3 y F0/24 del switch S1 y F0/3 para el swtch S3.

La VLAN nativa para estos enlaces troncales es la VLAN 1.

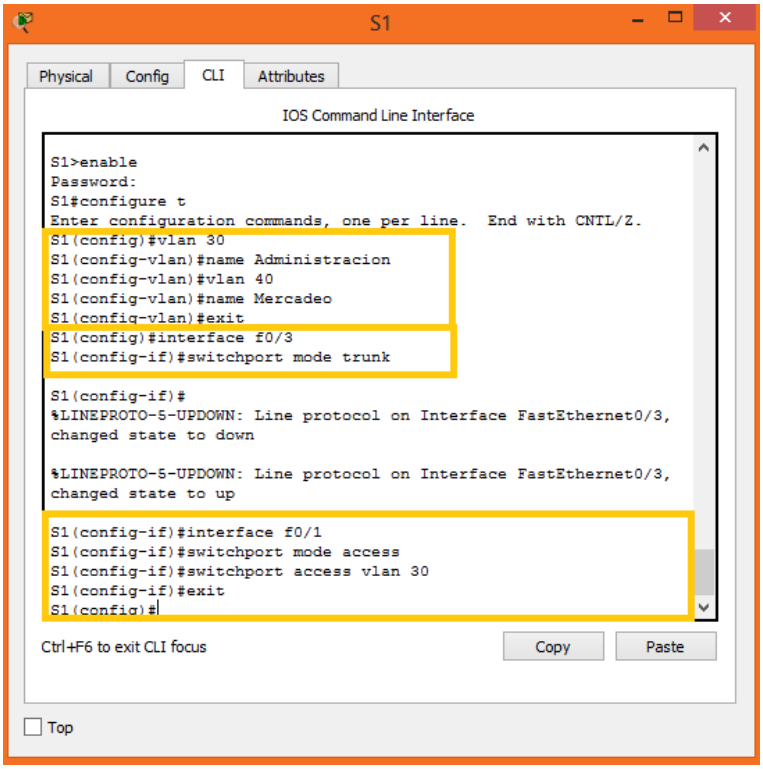

Figura 64. S1 Configuracion F0/3 trunk

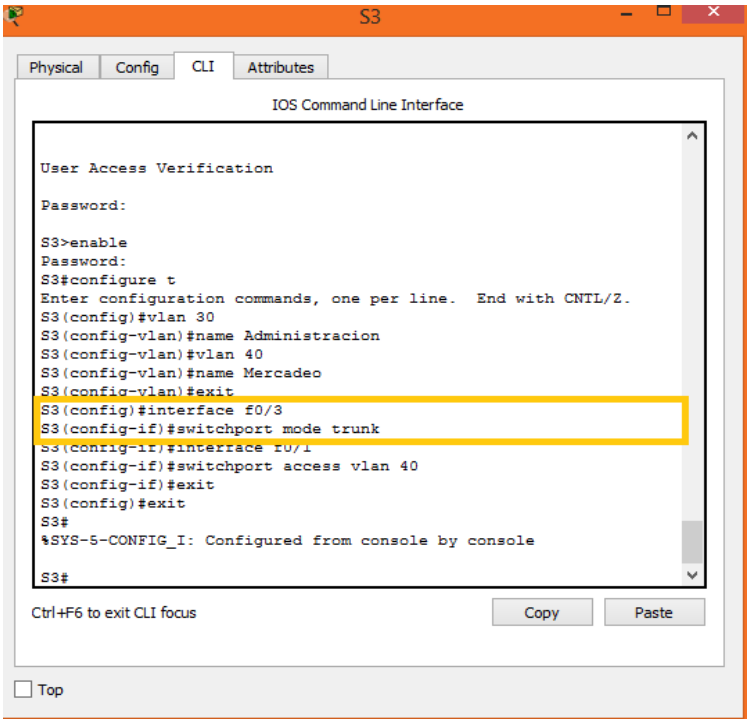

Figura 65. S3 Configuracion F0/3 trunk

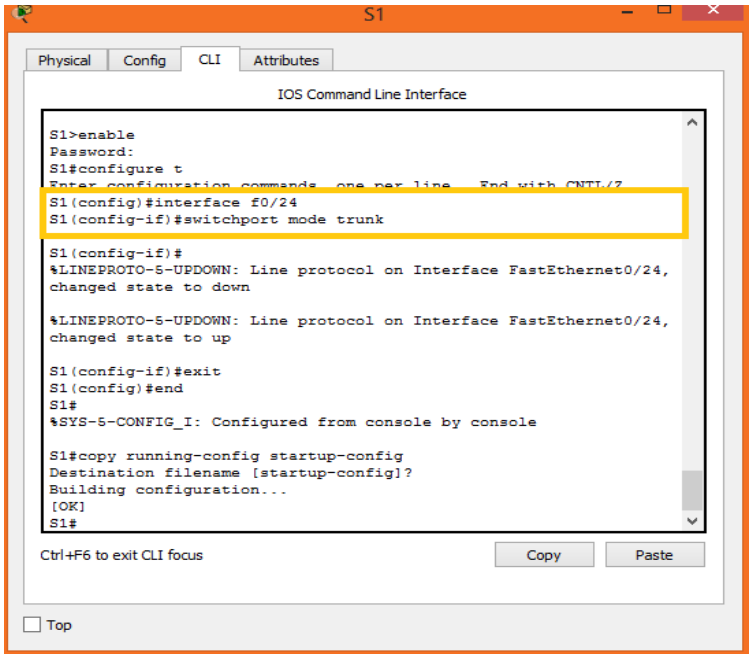

Figura 66. S1 Configuracion F0/24 trunk

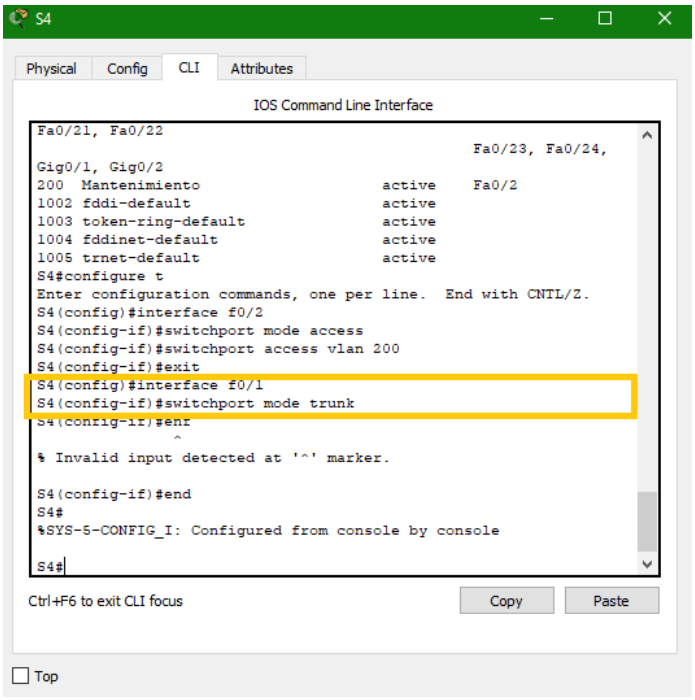

Figura 67. S4 Configuracion F0/1 trunk

Para verificar la configuracion de los puertos troncales se utiliza el comando show interfaces ID-interfaz switchport. A continuación, se puede visuallizar la aplicación del comando show interfaces ID-interfaz switchport a las interfaces configuradas como enlaces troncales.

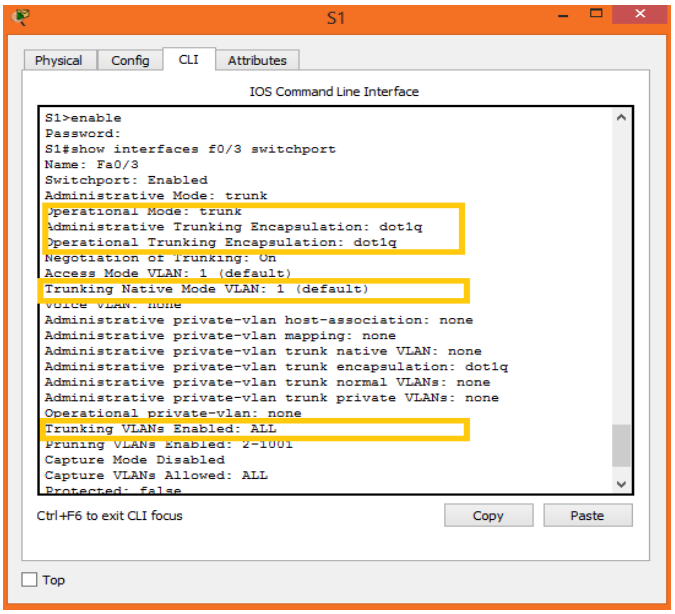

Figura 68. S1 Verificacion configuracion F0/3 trunk utilizando comando show interfaces ID-interfaz switchport

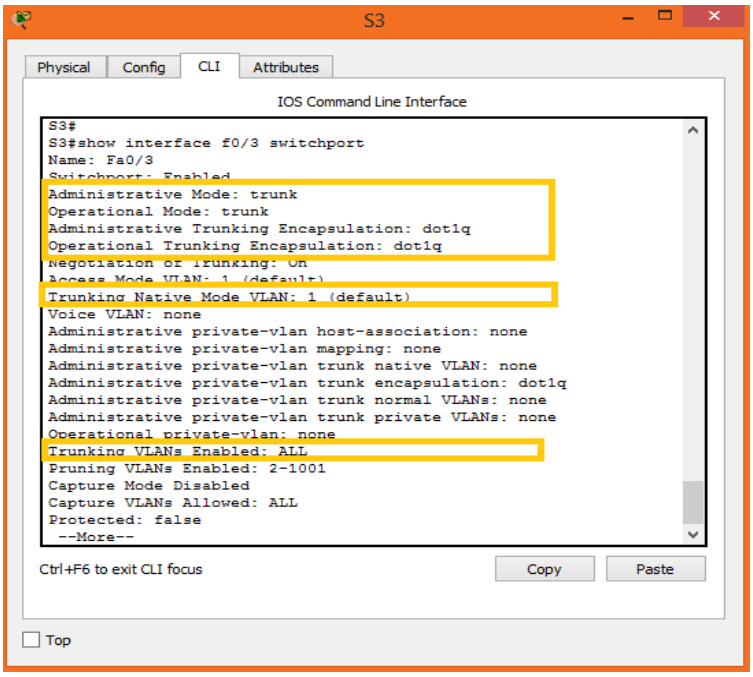

Figura 69. S3 Verificacion configuracion F0/3 trunk utilizando comando show interfaces ID-interfaz switchport

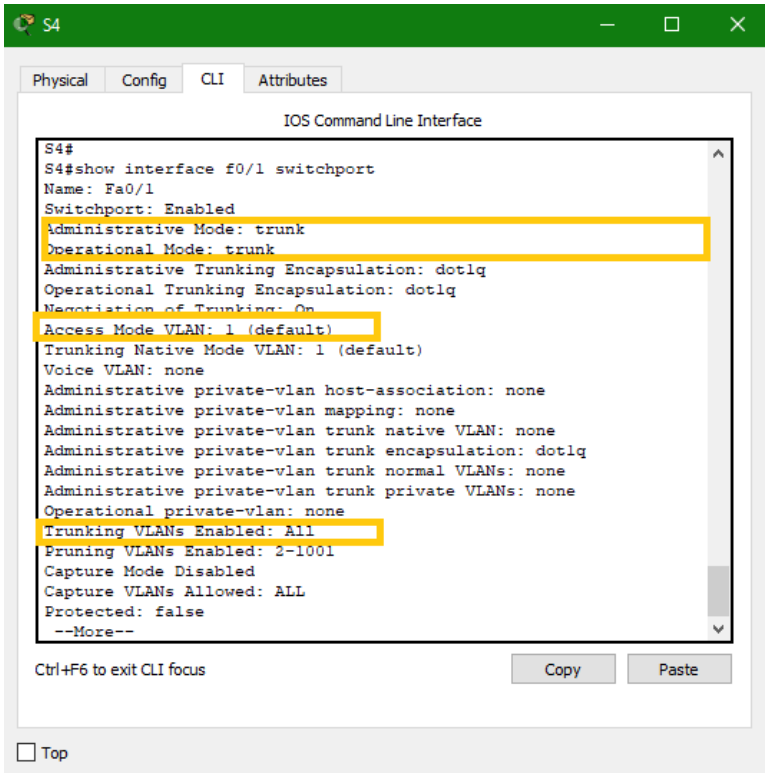

Figura 70. S4 Verificacion configuracion F0/1 trunk utilizando comando show interfaces ID-interfaz switchport

Como se estan usando switches Cisco Catalyst 2960 se utiliza de manera automática la encapsulación 802.1Q en los enlaces troncales. para otros switches generalmente se requiere la configuración manual de la encapsulación.

4.2.4.4 ENRUTAMIENTO EN LAS VLAN.

Un método para proporcionar routing y conectividad a varias VLAN es mediante el uso de un enlace troncal 802.1Q entre uno o más switches y una única interfaz del router. Este método también se conoce como “routing entre VLAN con router-on-a-stick”. En este método, se divide la interfaz física del router en varias subinterfaces que proporcionan rutas lógicas a todas las VLAN conectadas.

Las subinterfaces son interfaces virtuales basadas en software, asociadas con una única interfaz física. Las subinterfaces se configuran en software en un router, y cada subinterfaz se configura de manera independiente con una dirección IP y una asignación de VLAN. Las subinterfaces se configuran para subredes diferentes que corresponden a su asignación de VLAN para facilitar el routing lógico.

Para habilitar el routing entre VLAN utilizando el método router-on-a stick se debe habilitar el enlace troncal en el puerto del switch que está conectado al router. actividad que se realizó en el punto 4.2.4.3 Puertos troncales soporte Figura.
A continuacion, se muestra la configuracion de las subinterfaces para la VLAN 30 y VLAN 40 Router 1 sobre la interfaz fisica F0/0.

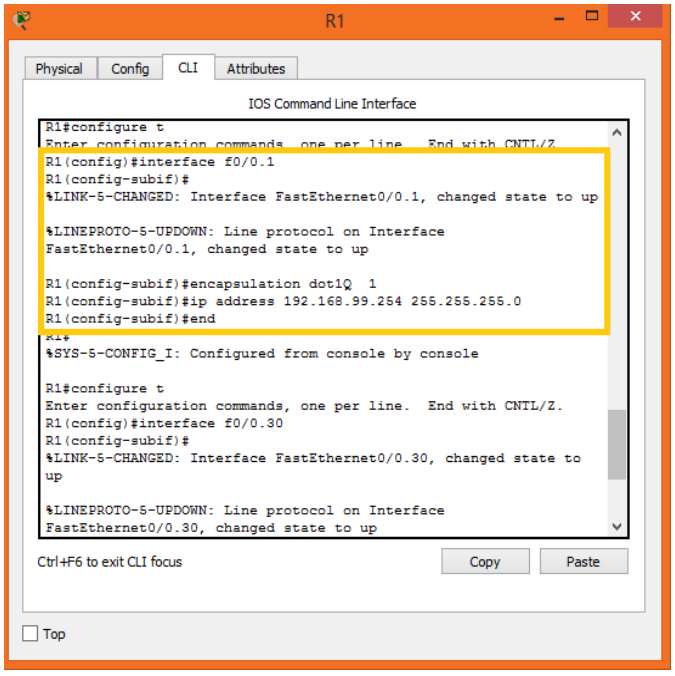

Figura 71. R1 Configuracion subinterfaz F0/0.1

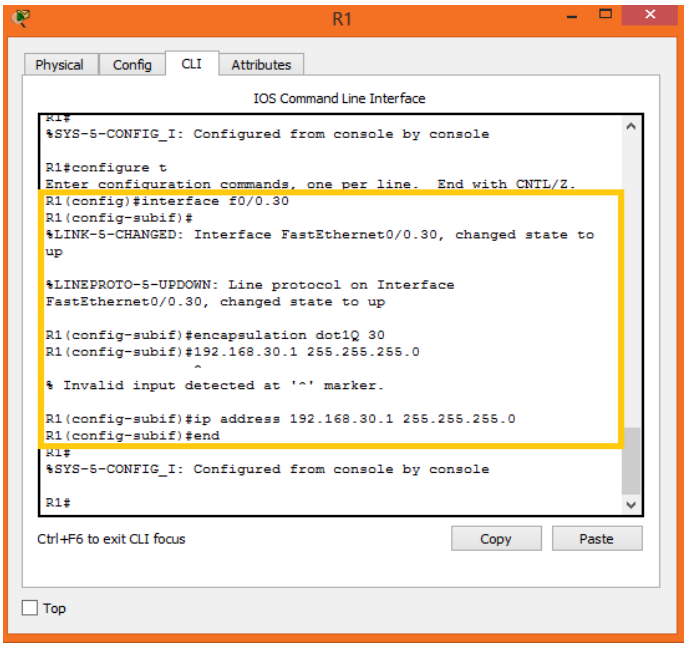

Figura 72. R1 Configuracion subinterfaz F0/0.30

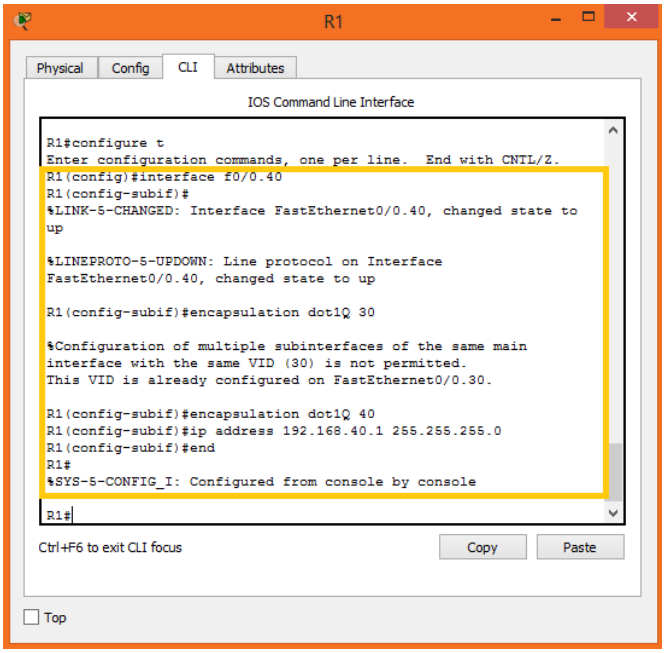

Figura 73. R1 Configuracion subinterfaz F0/0.40

Una vez configuradas estas subinterfaces se debe habilitar la interfaz física F0/0 con el comando no shutdown. Al consultar las rutas definidas en la tabla de routing mediante el comando show ip route se evidencia que están asociadas a subinterfaces específicas, en lugar de interfaces físicas separadas.

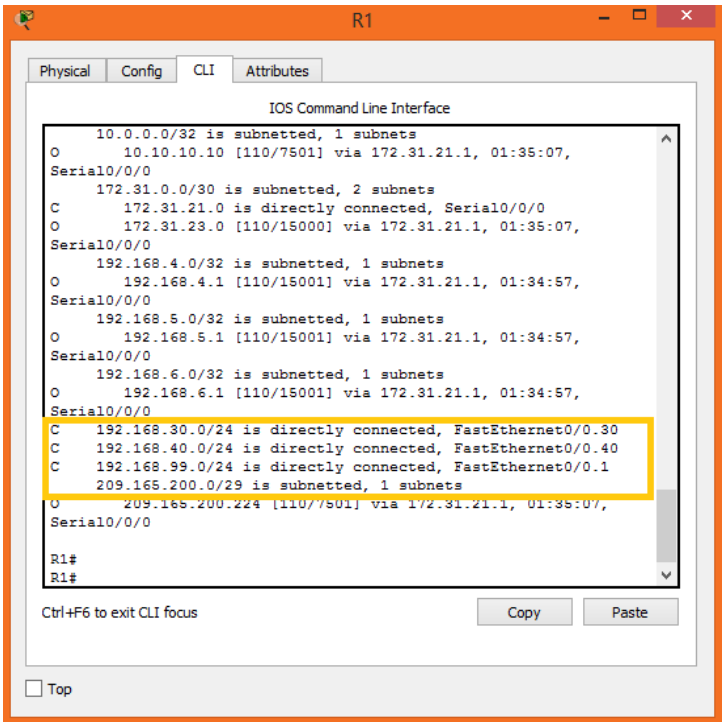

Figura 74. R1 verificacion subinterfaces configuradas en la tabla de routing comando show ip route

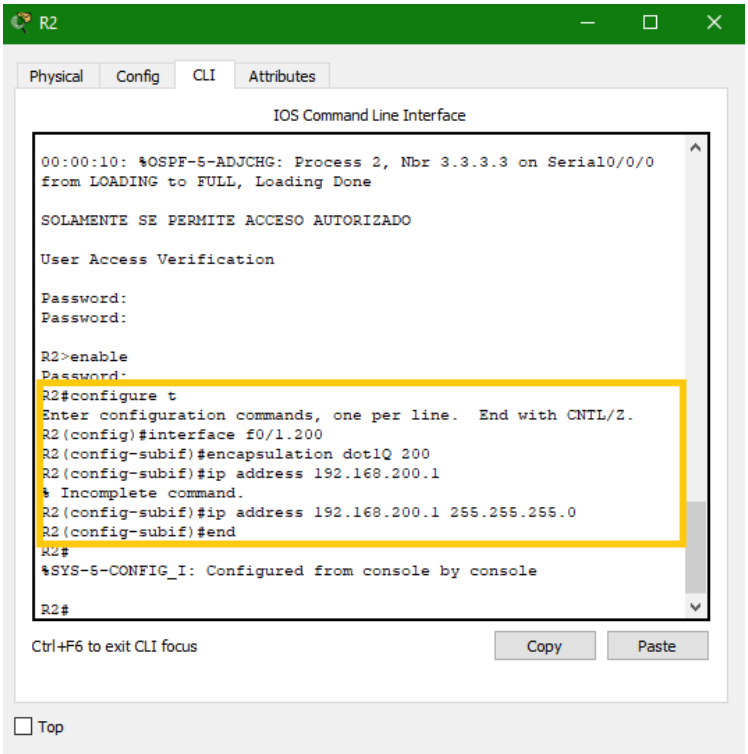

Figura 75. R2 Configuracion subinterfaz F0/1.200

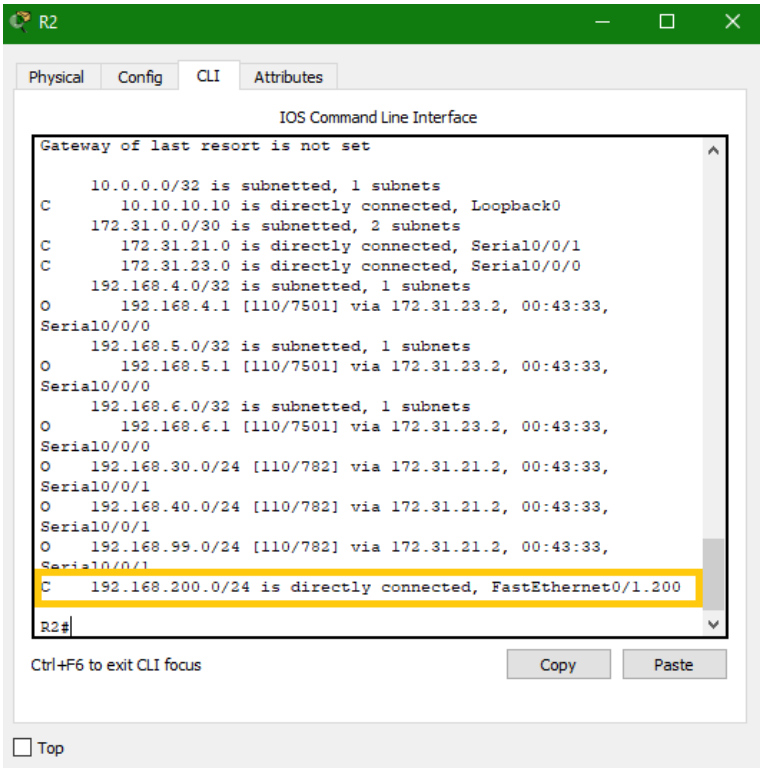

Figura 76. R2 verificacion subinterfaces configuradas en la tabla de routing comando show ip route

4.2.5. DNS LOOKUP.

Generalmente cuando se utiliza un switch o un router y se esta programando se cometen errores en la digitacion de los comandos lo que autimaticamente nos lleva a Translating “conft” … domain server (255.255.255.255), el cual obliga a esperar un tiempo por el momento en que dura dicho proceso. Para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host se utiliza el comando no ip domain-lookup.

A continuacion, se muestra la deshabilitacion de DNS lookup para el S3 utilizando el comando no ip domain-lookup.

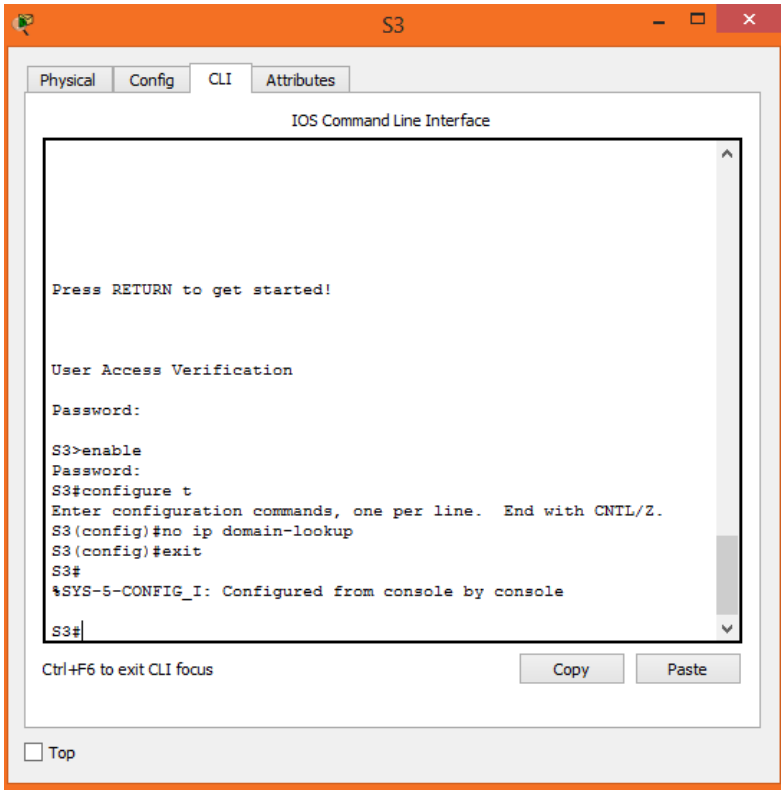

Figura 77. S3 Deshabilitar DNS lookup comando no ip domain-lookup

4.2.6 CONFIGURACION DE LOS SWITCHES.

Se programa para los switches 1 y 3 la configuración inicial basada en los siguientes criterios:

- Nombre del dispositivo.
- Deshabilitar la búsqueda de DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- Contraseña cifrada del modo EXEC privilegiado.
- Contraseña de consola, habilitando el inicio de sesión y agregando el comando logging synchronous. El comando logging synchronous sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.
- Contraseña de vty, habilitando el inicio de sesión y agregando el comando logging synchronous.
- Cifrado de contraseñas de texto no cifrado.
- Aviso de advierta a todo aquel que acceda al dispositivo, especificando que el acceso no autorizado está prohibido.
- Configuración de la dirección IP.
- Configuración del gateway predeterminado.
- Copiar la configuración en ejecución en la configuración de inicio

Las contraseñas asignadas fueron elegidas según criterio propio.

A continuación, se muestra la configuración inicial para los switches 1 y 3 del caso de estudio.

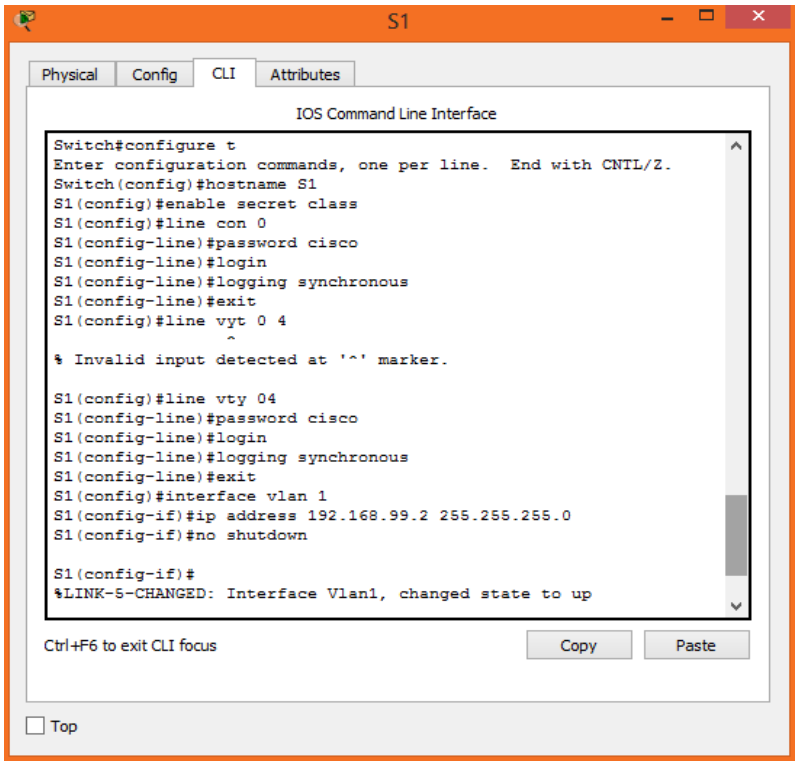

Figura 78. S1 configuracion inicial

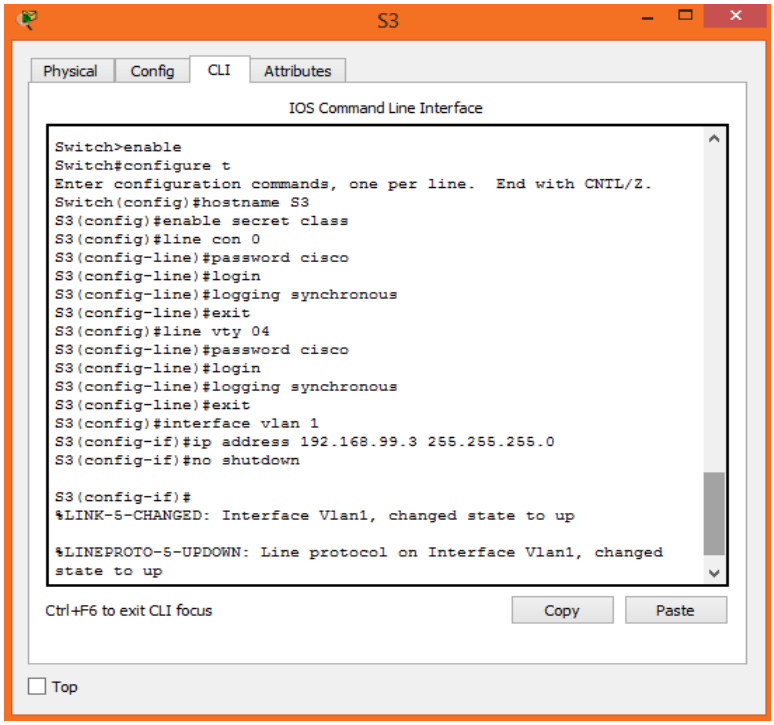

Figura 79. S3 configuracion inicial

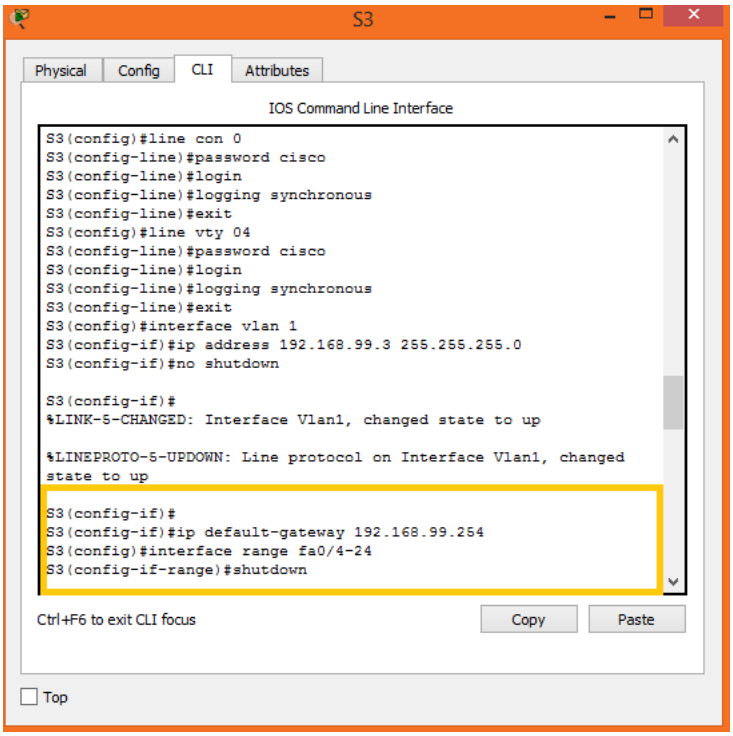

Figura 80. S3 configuracion inicial asignación Gateway

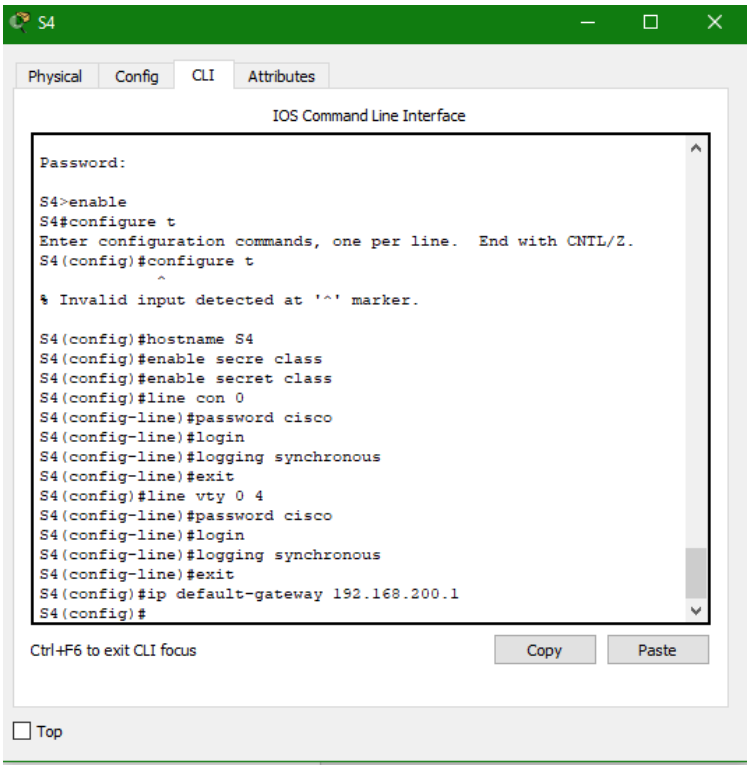

Figura 81. S4 configuracion inicial con configuracion gateway

4.2.7 DESHABILITACION DE PUERTOS.

Se deben deshabilitar administrativamente los puertos de los switches que no van a ser urilizados.

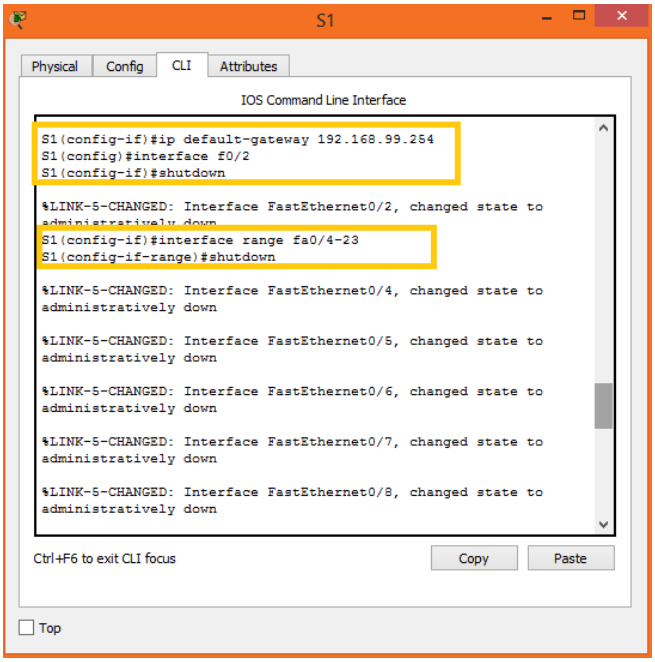

Figura 82. S1 deshabilitacion puertos no utilizados fastethernet

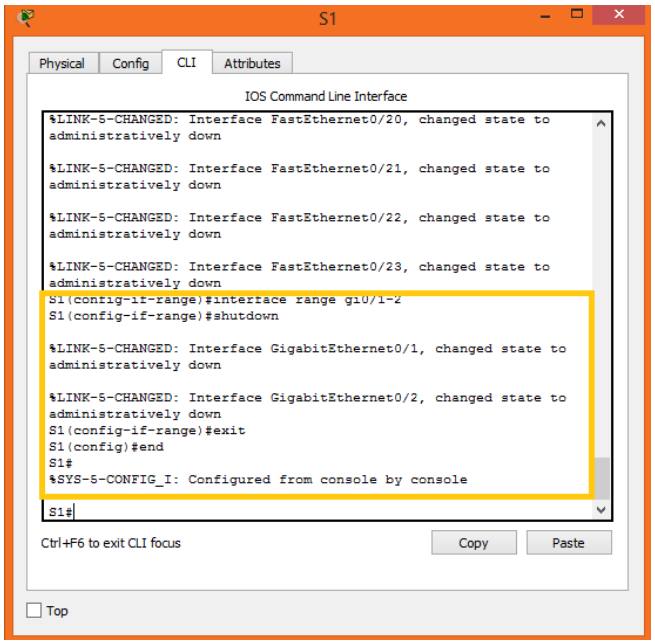

Figura 83. S1 deshabilitacion puertos no utilizados Gigabit ethernet

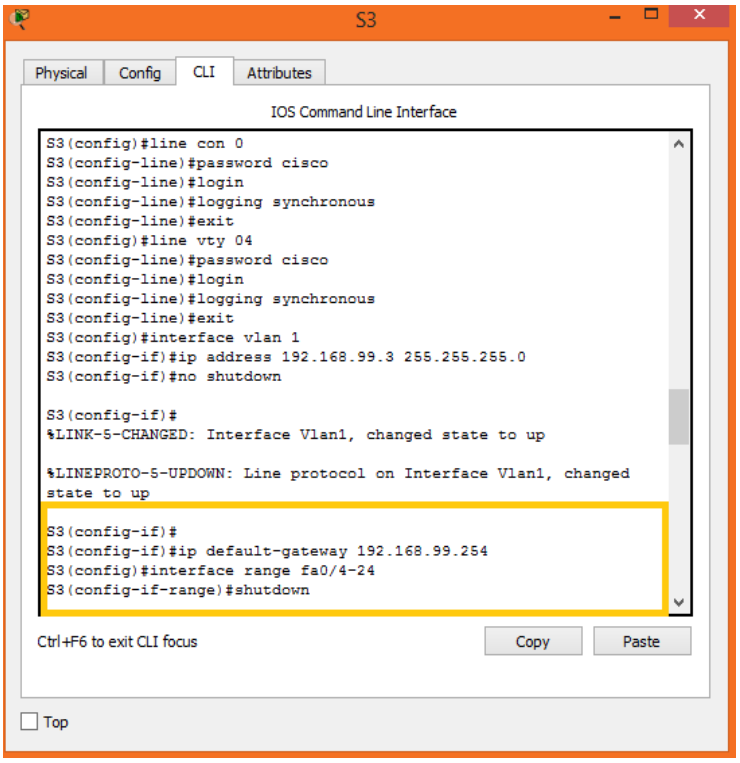

Figura 84. S3 deshabilitacion puertos no utilizados fastethernet

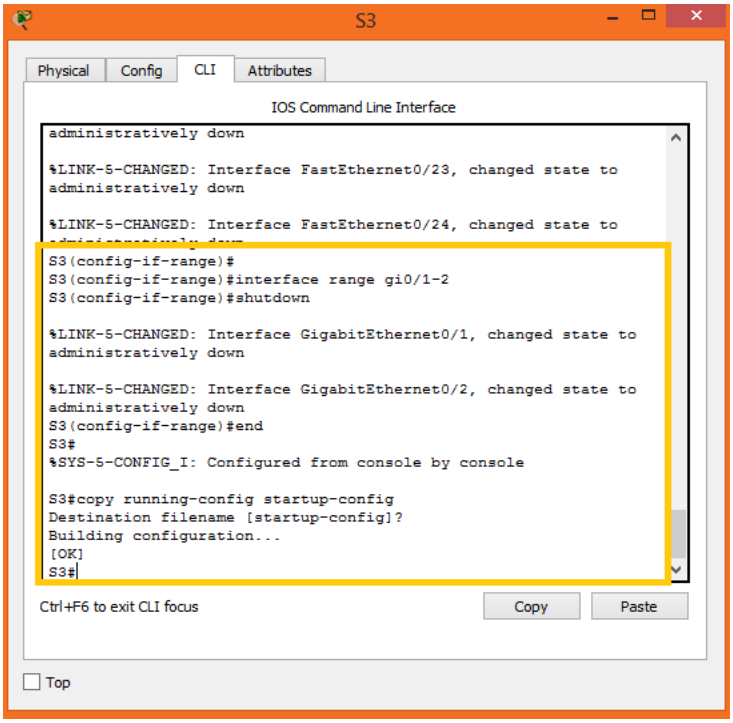

Figura 85. S3 deshabilitacion puertos no utilizados Gigabit ethernet

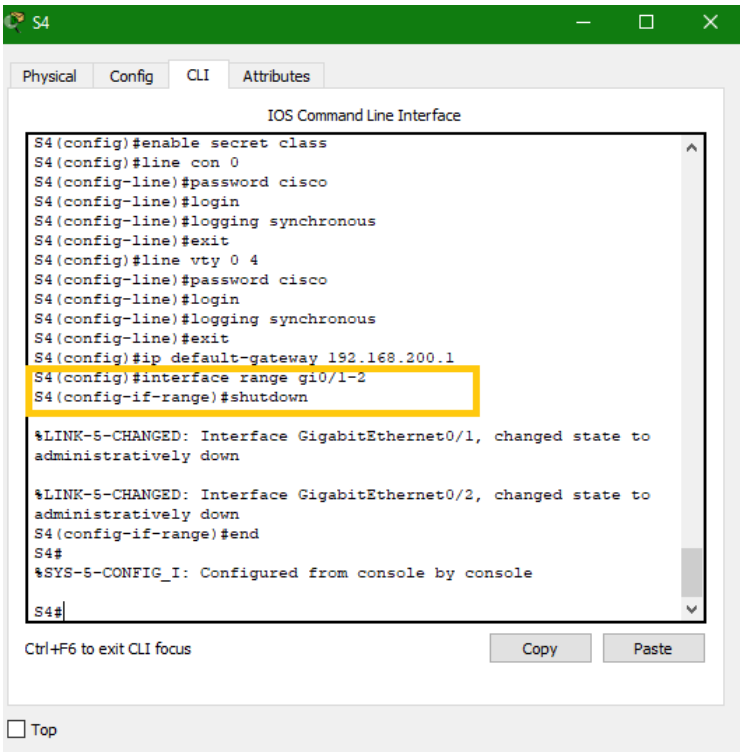

Figura 86. S4 deshabilitacion puertos no utilizados Gigabit ethernet

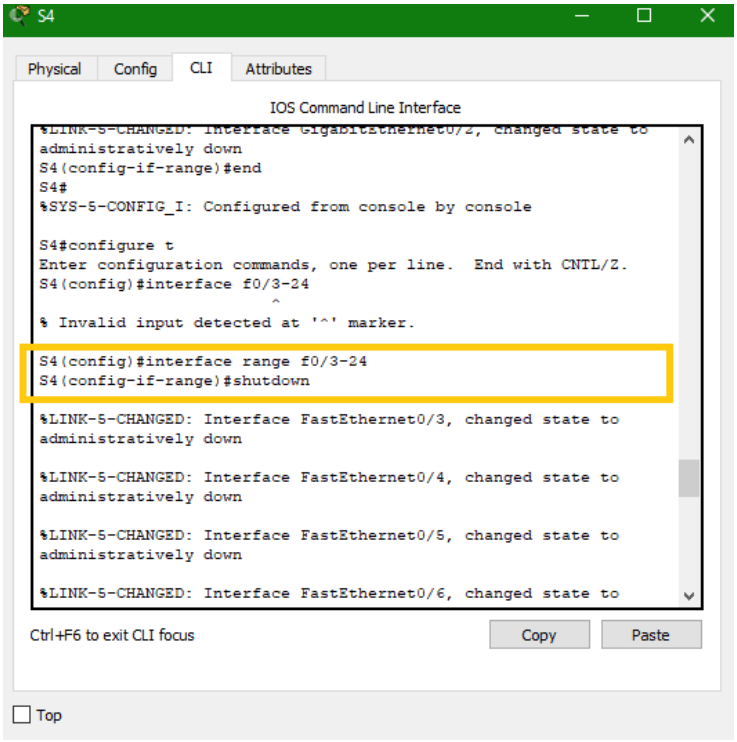

Figura 87. S4 deshabilitacion puertos no utilizados fastethernet

4.2.8 IMPLEMENTACION DHCP.

DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica.

DHCPv4 funciona en un modo cliente/servidor. Cuando un cliente se comunica con un servidor de DHCPv4, el servidor asigna o arrienda una dirección IPv4 a ese cliente.

Los router pueden ser configurados como servidor para que asigne y administre direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4.

4.2.8.1 EXCLUIR DIRECCIONES IPV4

Algunas direcciones IPv4 deben ser excluidas de asignación debido a que hay dispositivos de red que requieren asignación de direcciones estáticas.

Para excluir direcciones específicas, utilice el comando ip dhcp excluded-address.

Para nuestro caso de estudio se deben reservas las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas, utilizando el router 1 como servidor DHCP.
A continuación, se muestra esta configuración.

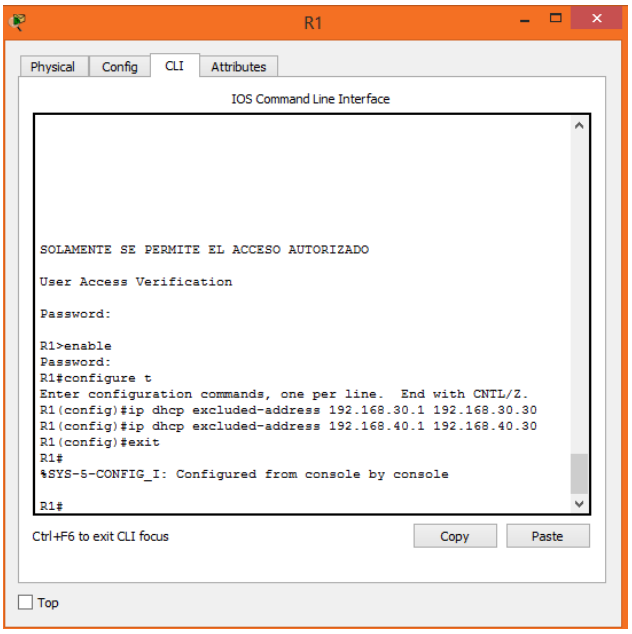

Figura 88. R1 Reserva de direcciones IP comando ip dhcp excluded-address

4.2.8.2 CONFIGURACION POOL DE DHCPV4.

La configuración de un servidor de DHCPv4 implica definir un conjunto de direcciones que se deben asignar. El comando ip dhcp pool nombre-pool se utiliza para crea un pool con el nombre especificado.

Se Utiliza la instrucción network para definir el rango de direcciones disponibles, el comando default-router para definir el router de gateway predeterminado. Normalmente, el gateway es la interfaz LAN del router más cercano a los dispositivos clientes. Se requiere un gateway, pero se pueden indicar hasta ocho direcciones si hay varios gateways. Para nuestro caso se utiliza la siguiente información:

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Figura 89. Configuración solicitad DHCP pool para VLAN 30

Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Figura 90. Configuración solicitad DHCP pool para VLAN 40

A continuación, se muestra la configuración del pool para la VLAN 30 y VLAN 40.

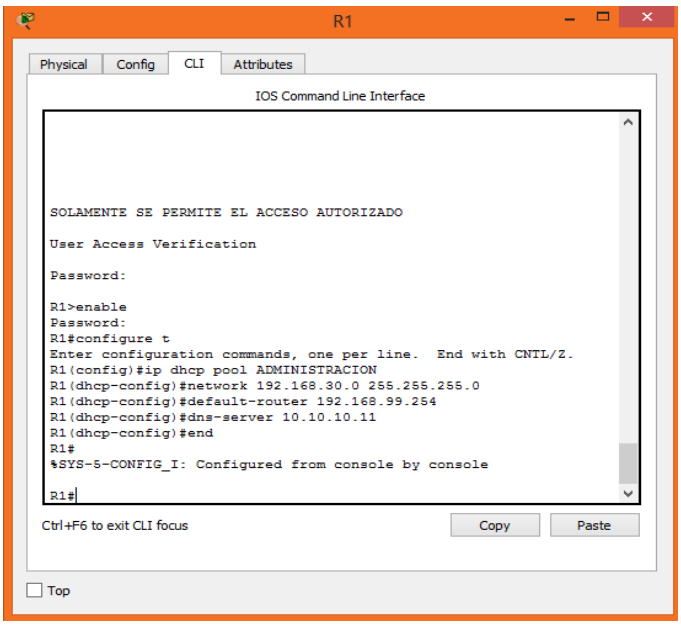

Figura 91. R1 Configuración pool VLAN 30

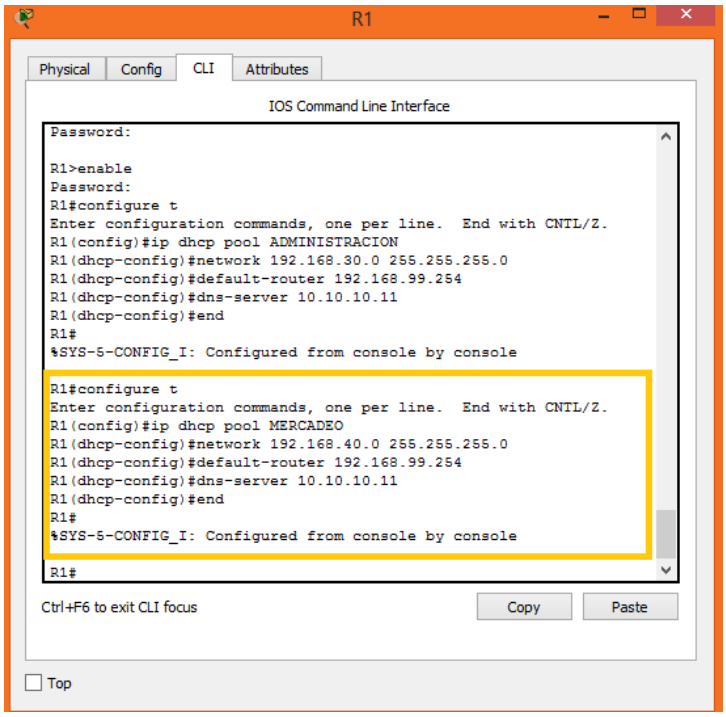

figura 92. R1 Configuración Pool VLAN 40

Para este caso no se configuro el nombre de dominio con el comando domain-name ni la duración del arrendamiento mediante el comando léase, debido a que estos comandos no son soportados por Packet Tracer. En este caso el valor de arrendamiento predeterminado para la dirección IP asignada es un día.

En cuanto a la configuración de un agente de retransmisión esta no es necesaria para el caso de estudio, debido a que el servidor está ubicado en la misma LAN del cliente.

4.2.8.3 VERIFICACIÓN DHCPV4 CONFIGURADO.

Se puede verificar el funcionamiento de DHCPv4 mediante el comando show ip dhcp binding, este nos permite ver los arrendamientos de direcciones DHCP.

A continuación, se muestra la verificación del DHCP configurado para la VLAN 30 y 40.

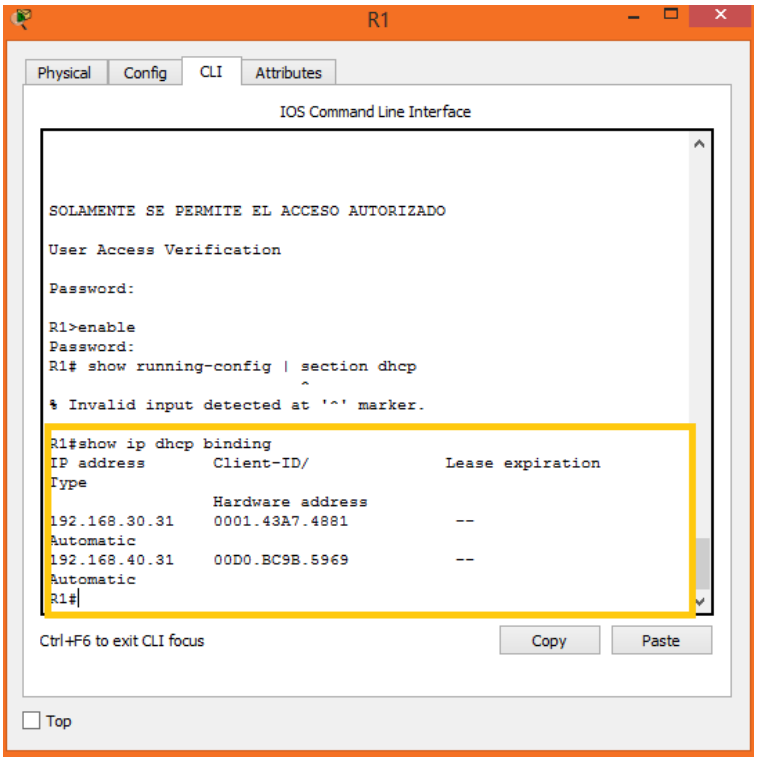

figura 93. R1 Verificación arrendamiento VLAN 30 y 40 comando show ip dhcp binding

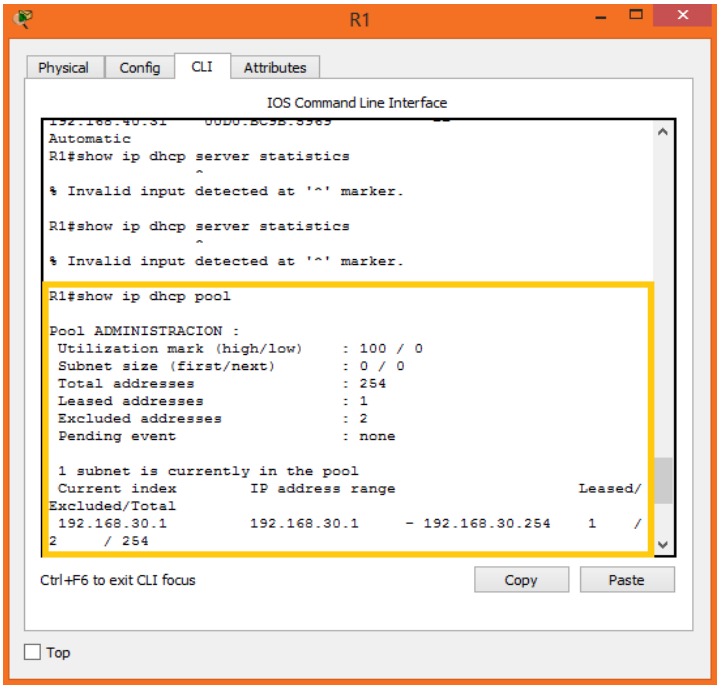

figura 94. R1 verificación configuración del Pool de DHCP ADMINISTRACION comando show ip dhcp pool

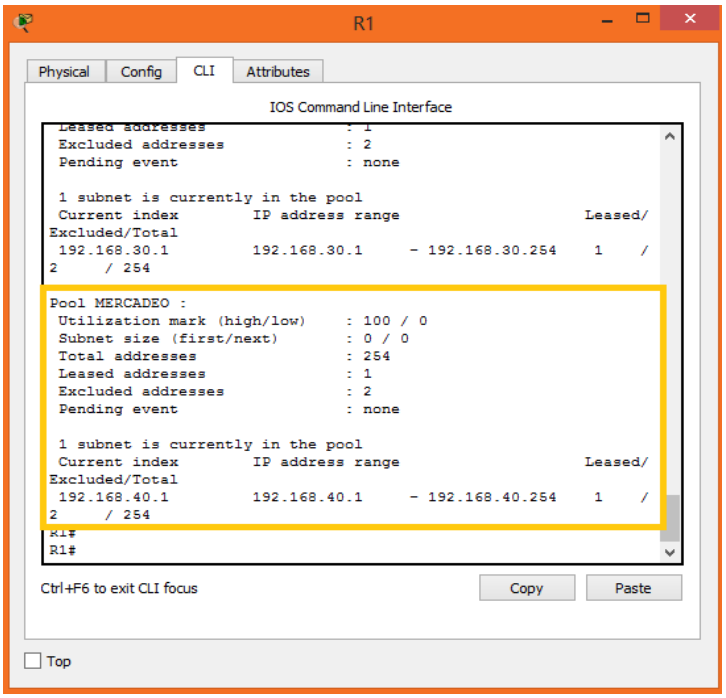

figura 95. R1 Verificación configuración del Pool de DHCP MERCADEO comando show ip dhcp pool

4.2.8.3 ASIGNACIÓN DIRECCIONAMIENTO IP PC-A Y PC-C.

Para los PC-A y PC-C se habilita la opción para que puedan recibir el direccionamiento IP desde el servidor DHCP (R1).

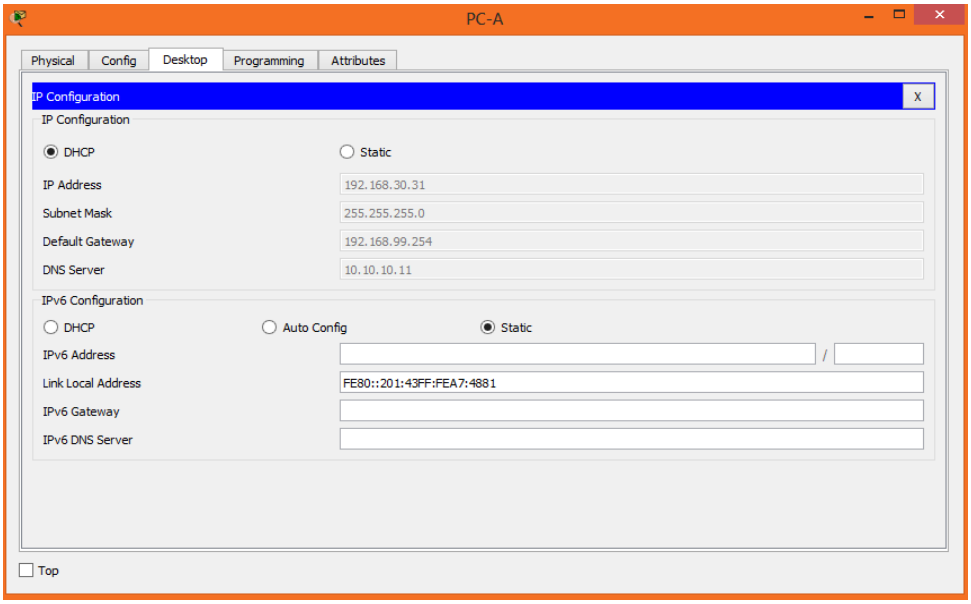

figura 96. PC-A Habilitación opción DHCP y visualización IP asignada

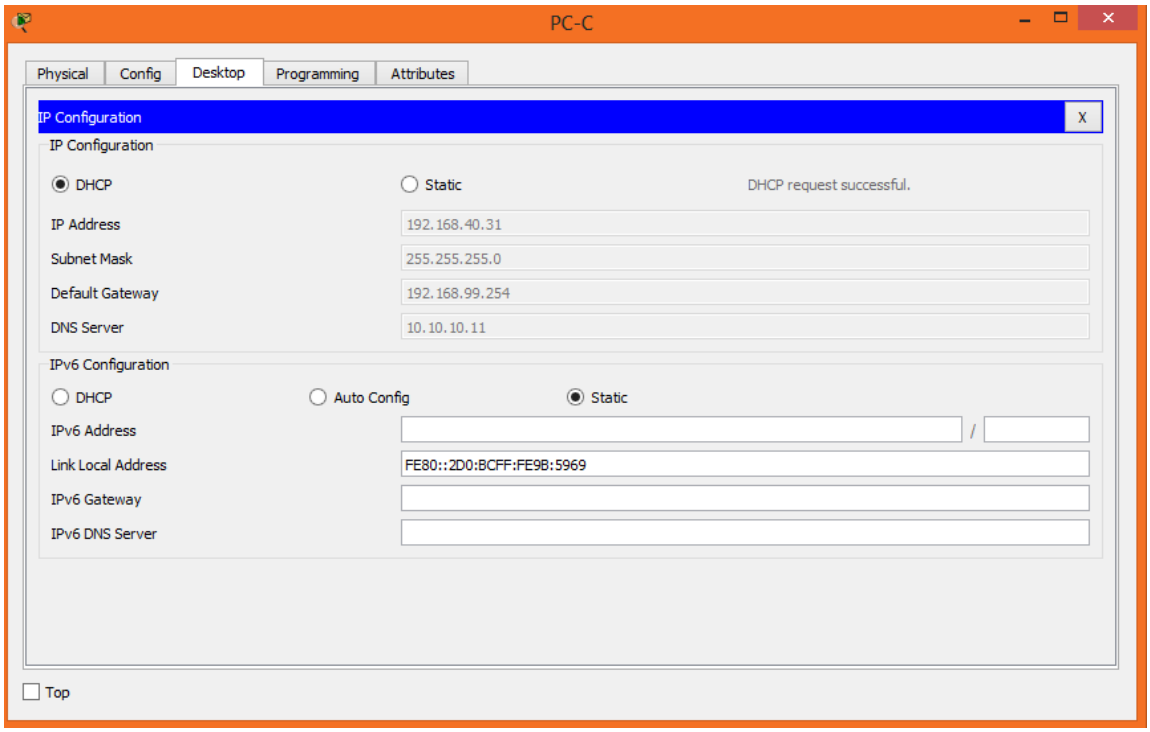

figura 97. PC-C Habilitación opción DHCP y visualización IP asignada.

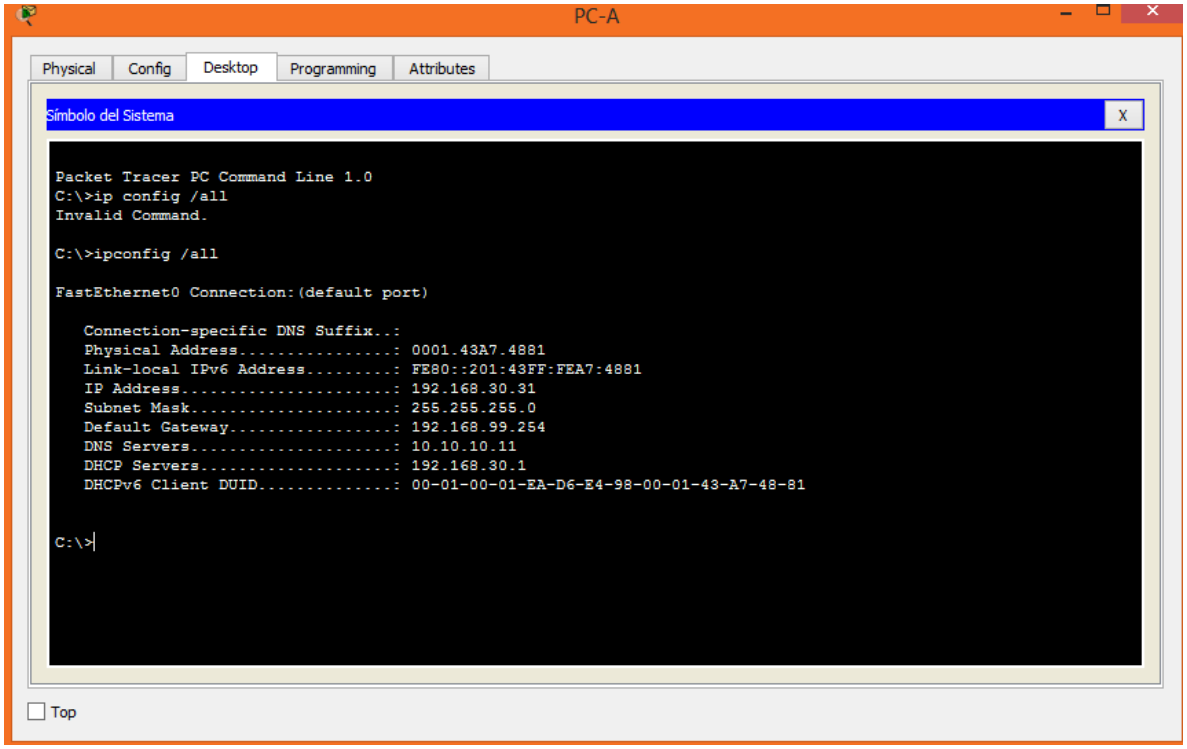

figura 98. PC-A Verificación asignación Direccionamiento IP comando ipconfig /all

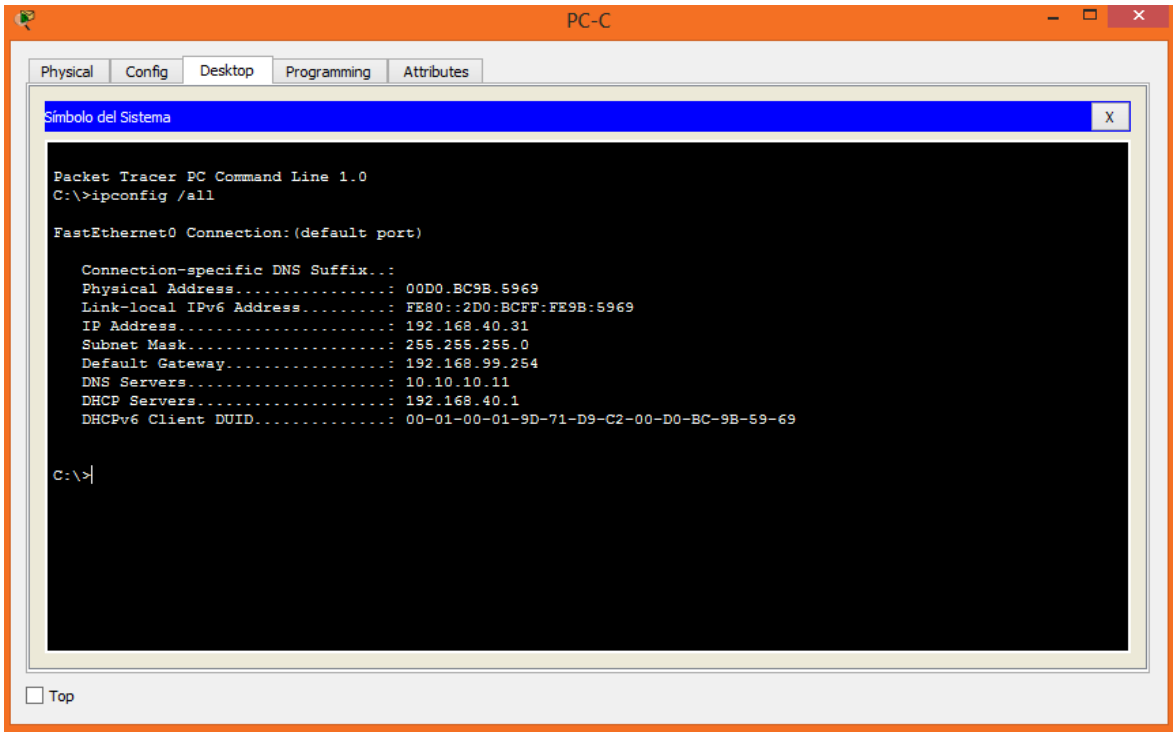

figura 99. PC-C Verificación asignación Direccionamiento IP comando ipconfig /all

Para el Internet-PC se asignó una dirección estática según lo establecido en el caso de estudio.

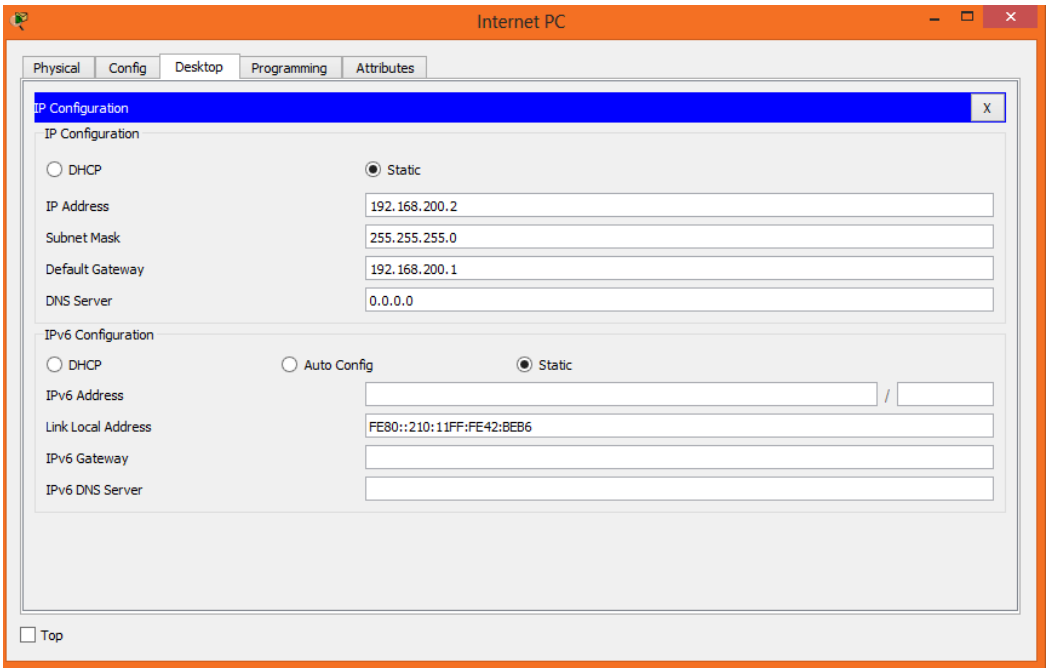

figura 100. Internet-PC asignación Direccionamiento IP manera estática

4.2.9 CONFIGURAR NAT.

La NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. La NAT dinámica utiliza un grupo o un conjunto de direcciones IPv4 públicas para la traducción. Para nuestro caso de estudio se realiza la configuración de NAT dinámica.

4.2.9.1 CONJUNTO DE DIRECCIONES NAT.

El primer paso para configurar una NAT dinámica es definir el conjunto de direcciones que se utilizará para la traducción con el comando ip nat pool. Por lo general, este conjunto es un grupo de direcciones públicas. Las direcciones se definen indicando la primera y la última dirección IP del conjunto. Las palabras clave netmask o prefix-length indican qué bits de la dirección pertenecen a la red y cuáles al host en el rango de direcciones.

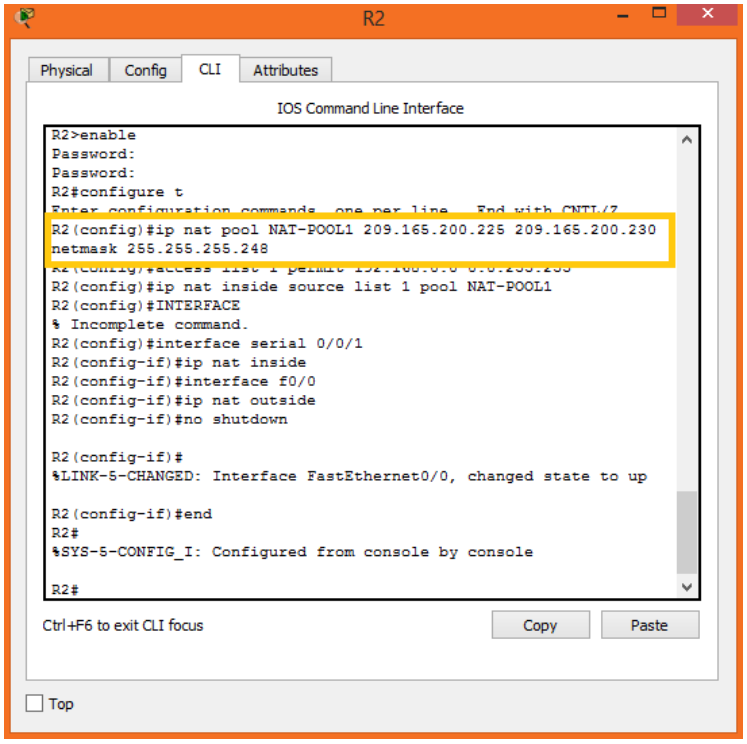

figura 101. R2 Conjunto de direcciones NAT

4.2.9.2 CONFIGURACION ACL ESTANDAR NAT.

Se configura una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles.

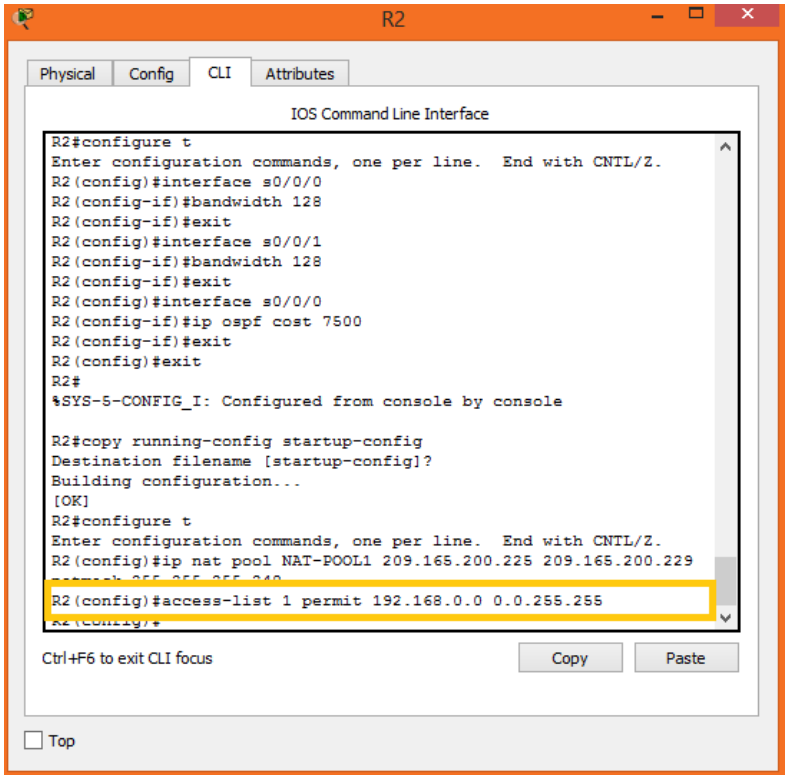

figura 102. R2 Configuración ACL estándar

4.2.9.3 CONFIGURACIÓN ACL AL CONJUNTO DIRECCIONES NAT.

Para conectar la ACL al conjunto, se utiliza el comando ip nat inside source list número-lista-acceso number pool nombre-conjunto. El router utiliza esta configuración para determinar qué dirección (pool) recibe cada dispositivo (list).

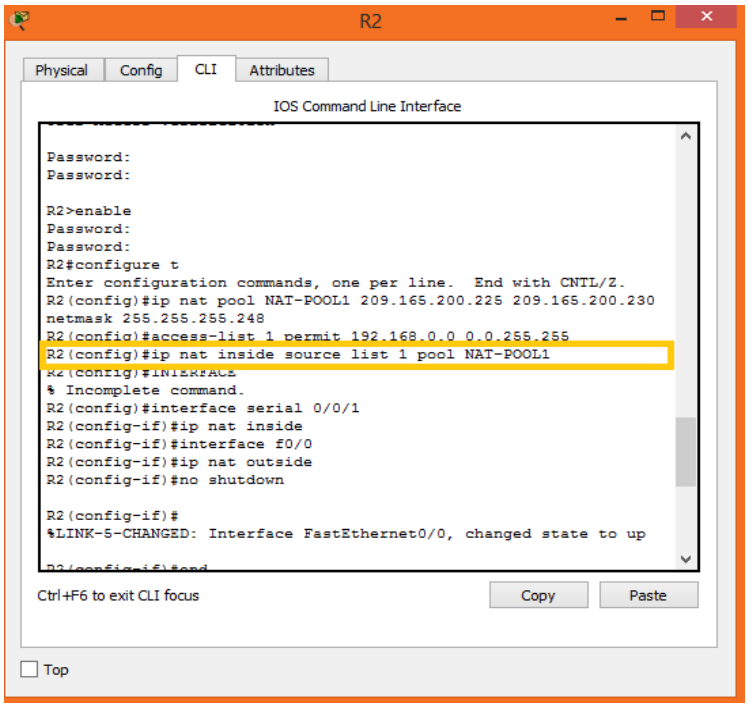

figura 103. R2 Configuración ACL al conjunto direcciones NAT

4.2.9.4 INTERFAZ INTERNA Y EXTERNA RESPECTO A NAT.

Se configura la interfaz interna con respecto a NAT es decir la interfaz que se conecta a la red interna.

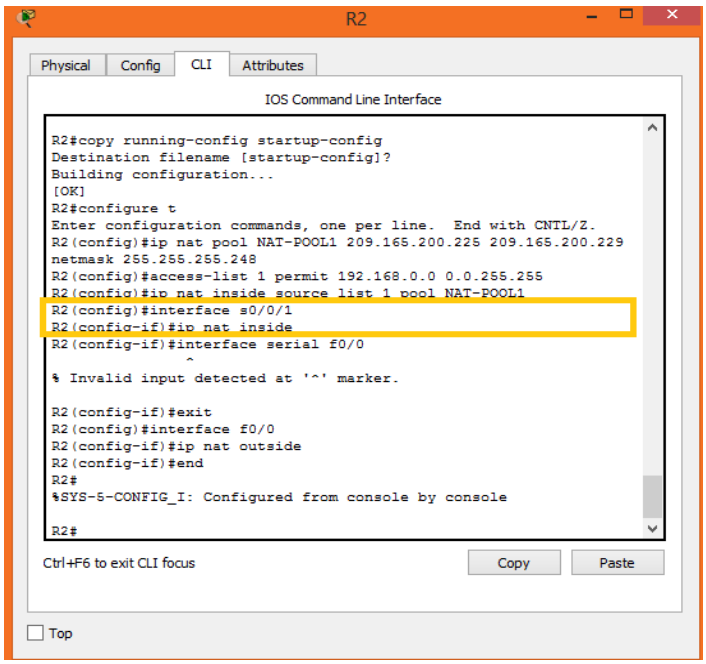

figura 104. R2 configuración Interfaz interna NAT

Se configura la interfaz externa con respecto a NAT es decir la interfaz que se conecta a la red externa.

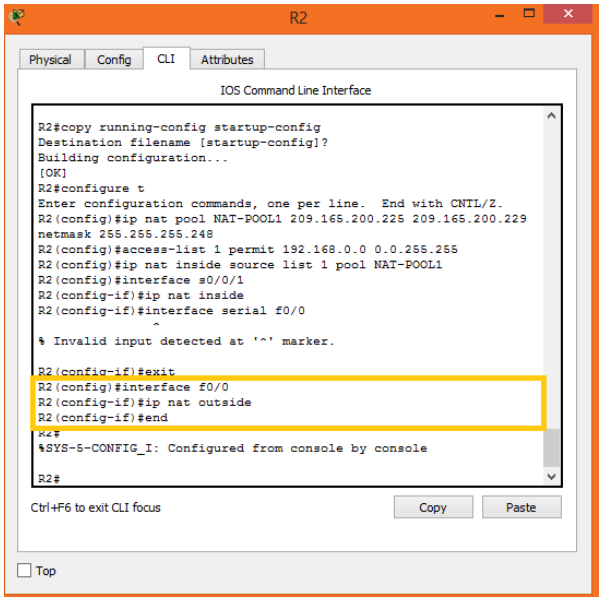

figura 105. R2 configuración Interfaz externa NAT

4.2.9.4 VERIFICACIÓN CONFIGURACIÓN NAT.

Para verificar la configuración establecida se puede usar el comando show ip nat statistics para mostrar la información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

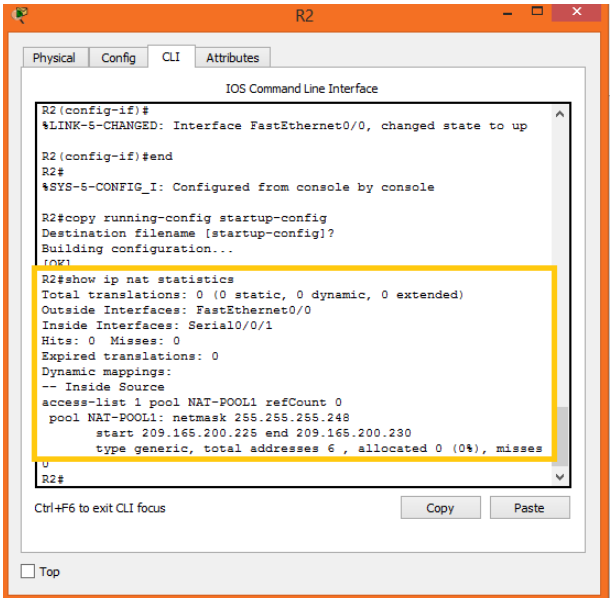

figura 106. R2 verificación configuración establecida NAT comando show ip nat statistics

4.2.10 LISTAS DE ACCESO ACL.

Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

Las ACL pueden ser estándar o extendidas. Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan; mientras que en la ACL extendidas filtran paquetes IPv4 según varios atributos como son: tipo de protocolo, dirección IPv4 de origen, dirección IPv4 de destino, puertos TCP o UDP de origen, puertos TCP o UDP de destino e Información optativa de tipo de protocolo para un control más preciso.

Se debe tener muy presente que la ubicación de las ACL estándar es lo más cerca posible del destino y la ubicación de las ACL extendidas es lo más cerca posible del origen.

4.2.10.1 CONFIGURACIÓN LISTAS DE ACCESO DE TIPO ESTANDAR.

Para crear una ACL estándar se debe utilizar el comando de configuración global Access-list, luego se utiliza el comando de configuración interface para seleccionar la interfaz a la cual se le aplicara la ACL y por último se utiliza el comando de configuración de interfaz ip Access-group para activar la ACL en la interfaz elegida.

A continuación, se muestra la configuración de al menos dos listas de acceso de tipo estándar a criterio propio para restringir o permitir tráfico desde R1 o R3 hacia R2.

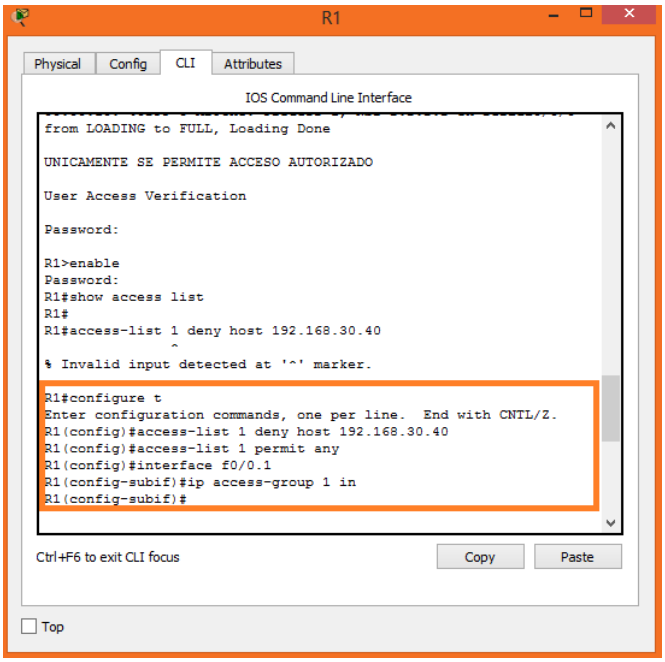

figura 107. R1 Configuración ACL estándar

Esta ACL deniega un host específico. Se bloquea el tráfico del PC con dirección 192.168.30.40, pero se permite el resto del tráfico.

El comando show ip interface se utiliza para verificar la ACL en la interfaz El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL.

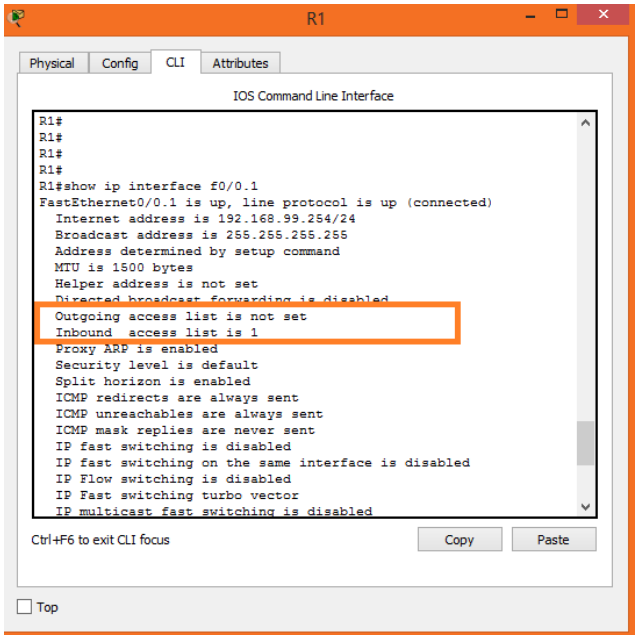

figura 108. R1 verificación ACL estándar comando show ip interface f0/0.1

Se utiliza el comando show access-lists seguido del número o el nombre de la lista de acceso permite ver una lista de acceso individual, de igual manera el comando show access-lists sin indicar el nombre de la lista muestra todas las lista configuradas.

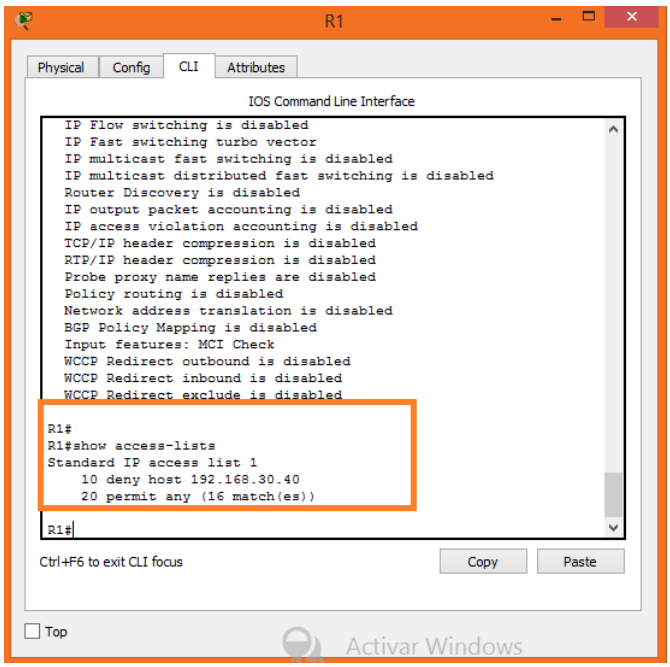

figura 109. R1 verificación ACL estándar comando show access-lists

4.2.10.2 CONFIGURACION LISTAS DE ACCESO DE TIPO EXTENDIDAS CON NOMBRE.

Para crear una ACL extendida nombradas ACL extendidas con nombre se debe ingresar al modo de configuración global y utilizar el comando ip access-list exntended nombre para definir un nombre para la ACL extendida, en el modo de configuración de ACL con nombre se especifican las condiciones para permit o deny, se regresa al modo exec privilegiado y se verifica la ACL con el comando show access-lists nombre y finalmente se guarda la configuración mediante el comando copy running-config startup-config.

A continuación, se muestra la configuración de al menos dos listas de acceso de tipo extendido nombradas a criterio propio para restringir o permitir tráfico desde R1 o R3 hacia R2.

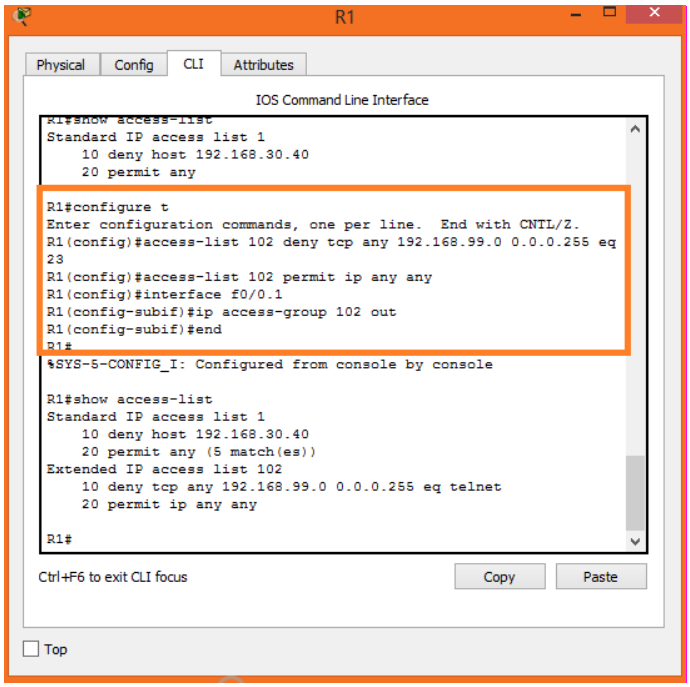

figura 110. R1 Configuración ACL extendida sin nombre

La ACL extendida configurada deniega el tráfico de Telnet de cualquier origen a la LAN 192.168.99.0/24, pero se permite el resto del tráfico IP Debido a que el tráfico destinado a la LAN 192.168.99.0/24 sale de la interfaz f0/0.1, la ACL se aplica a f0/0.1 con la palabra clave out.

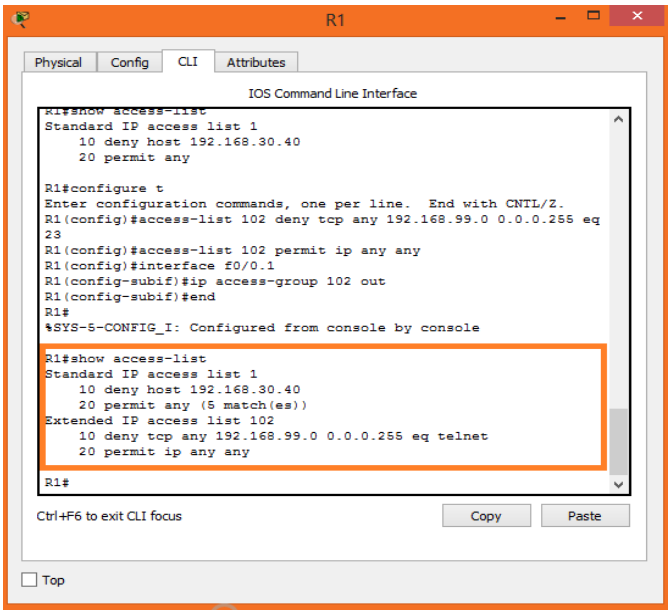

figura 111. R1 Verificación Configuración ACL extendida comando show acces-lists

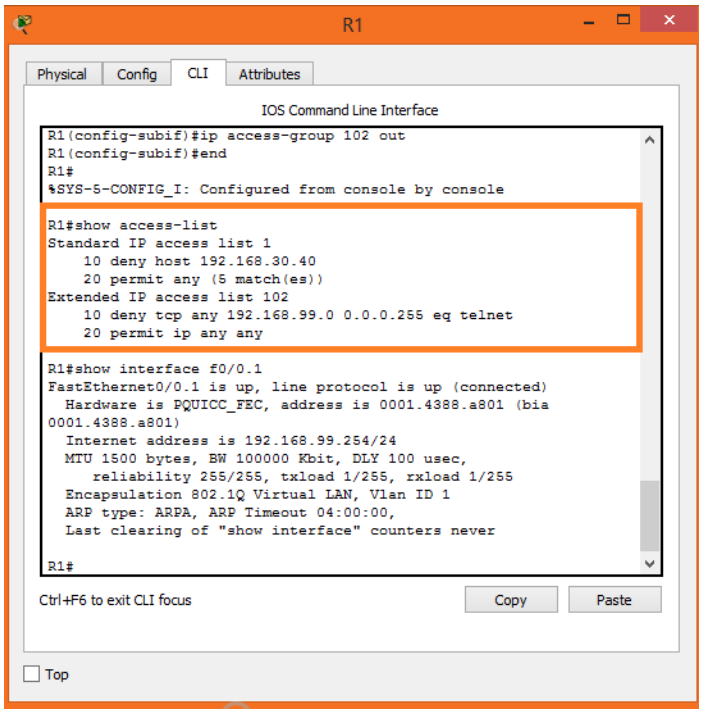

figura 112. R1 Verificación Configuración ACL extendida comando show interface f0/0.1

4.2.11 VERIFICACIÓN PROCESO COMUNICACIÓN Y REDIRECCIONAMIENTO DE TRÁFICO.

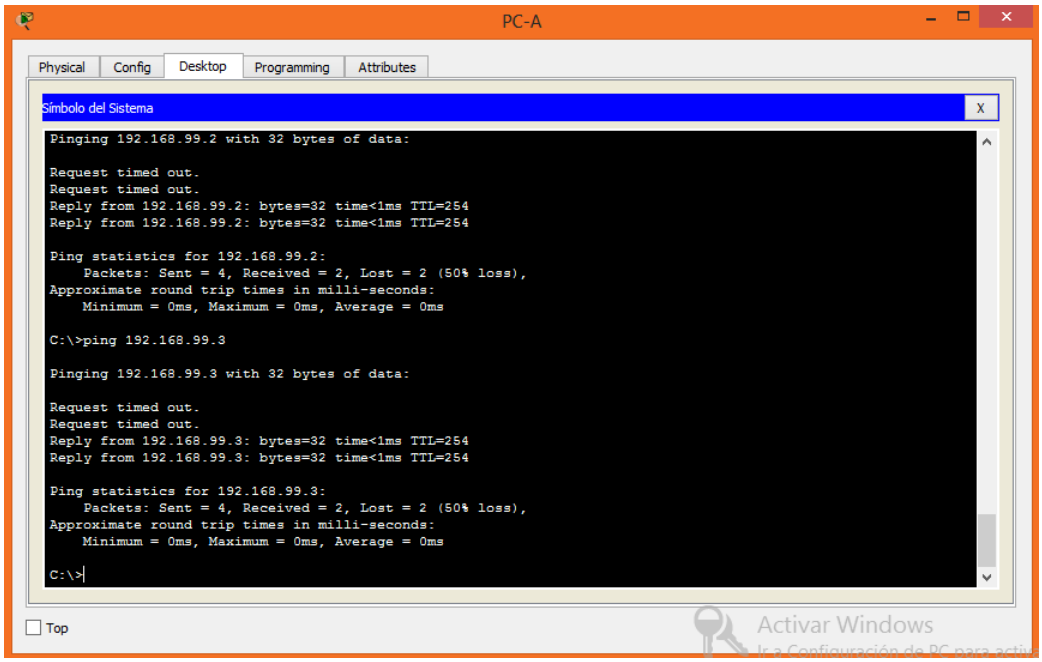

figura 113. Verificación conectividad de PC-A con toda la red

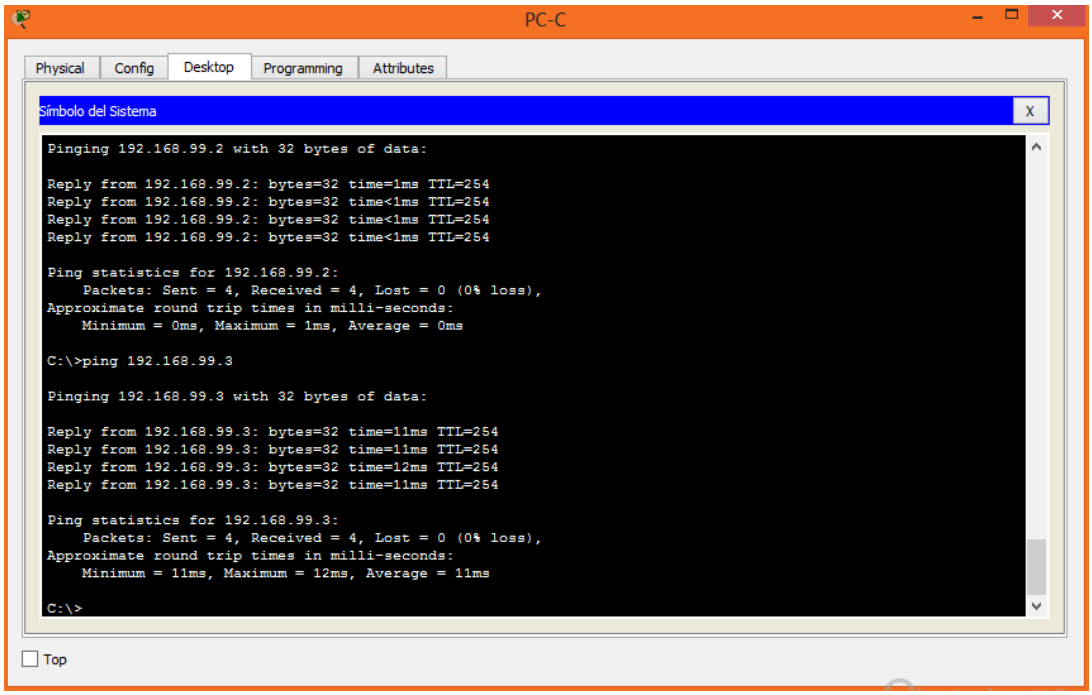

figura 114. Verificación conectividad de PC-C con toda la red

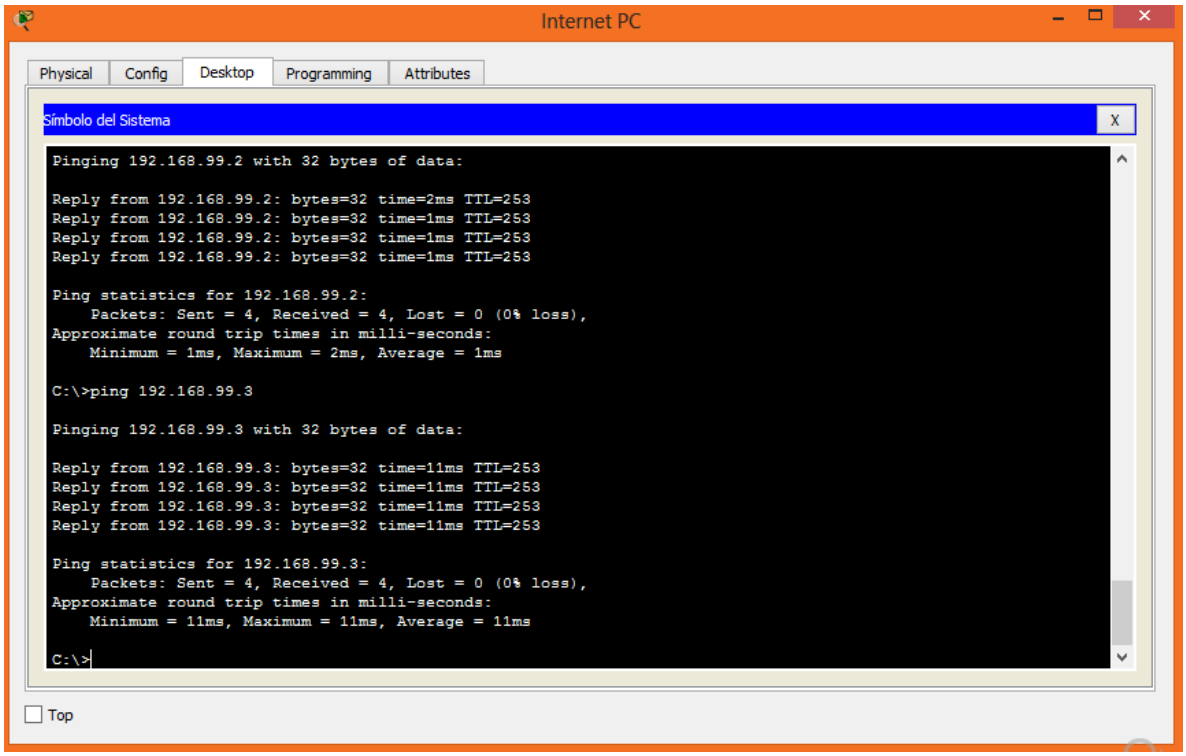

figura 115. Verificación conectividad de Internet-PC con toda la red

A continuación, se puede observar el archivo de Packet Tracer trabajado sobre el cual se basa la solución documentada.

FINALok.pkt

CONCLUSIONES

- AL realizar este trabajo fue posible poner en práctica y entender como el protocolo OSPF es un protocolo de enrutamiento muy útil para redes porque maneja las bases de datos de adyacencias, las bases de datos de estado de enlace y las bases de datos de reenvio, con el fin de mantener actualizada la información de routing; teniendo claro que para redes pequeñas con pocos router es recomendable utilizar OSPF de area única y para grandes redes el OSPF multiarea, lográndose visualizar como al configurar un router con OSPF lo primera tarea que intenta realizar es crear adyacencias con sus vecinos, Intercambiar información de routing, calcular las mejores rutas y lograr la convergencia.

- Fue posible implementar el concepto de VLAN al proporcionar segmentación para mercadeo, administración y mantenimiento, siendo necesario tener claro que un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable; por lo que en este ejercicio se dividió la red en segmentos según factores como la función, el equipo del proyecto o la aplicación y como cada VLAN se considera una red lógica independiente, fue necesario reenviar los paquetes a través de un dispositivo de routing.

- Se pudo implementar la configuración de un router como DHCP y evidenciar la importancia de este al permitir dar soluciones efectivas al momento de realizar la asignación de direcciones IP a los hosts, evidenciándose como no siempre debe tenerse un servidor para esta tarea ya que puede ser posible configurar el router de acuerdo a un pool de direcciones IP establecidas por el administrador de la red.

- Se utilizó NAT para permitir que los hosts puedan salir a internet realizando NAT la traducción de las direcciones privadas en intranet a direcciones públicas extranet, todo esto con el fin de hacer la red más segura debido a que las redes privadas no deben anuncian sus direcciones ni su topología interna, por lo que se utiliza NAT para obtener acceso externo controlado.

- La importancia de las listas de control de acceso radica en que pueden volver más segura la red, es una herramienta fundamental para los administradores que a través de condiciones programadas controlan diferentes tipos de tráfico haciendo menos vulnerable una red.

BIBLIOGRAFIA

- **Temática: OSPF de una sola área**
  CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

- **Temática: Listas de control de acceso**
  CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

- **Temática: DHCP**
  CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

- **Temática: Traducción de direcciones IP para IPv4**
  CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

- **Temática: VLANs**
  CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

- **Temática: Enrutamiento entre VLANs**
  CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1