DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP

Prueba de Habilidades Prácticas

Presentado por:

Ivan Castañeda Monsalve

Grupo:

203092_35

Tutor

Efraín Alejandro Pérez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

Junio

INDICE

INTRODUCCION

La evaluación denominada ñPrueba de habilidades prácticasò, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos escenarios, el estudiante deberá realizar el proceso de configuración de un escenario en el **Laboratorio SmartLab** y el otro mediante el uso de **herramientas de Simulación (Puede ser Packet Tracer o GNS3)**. El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario.

Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado al finalizar el curso.

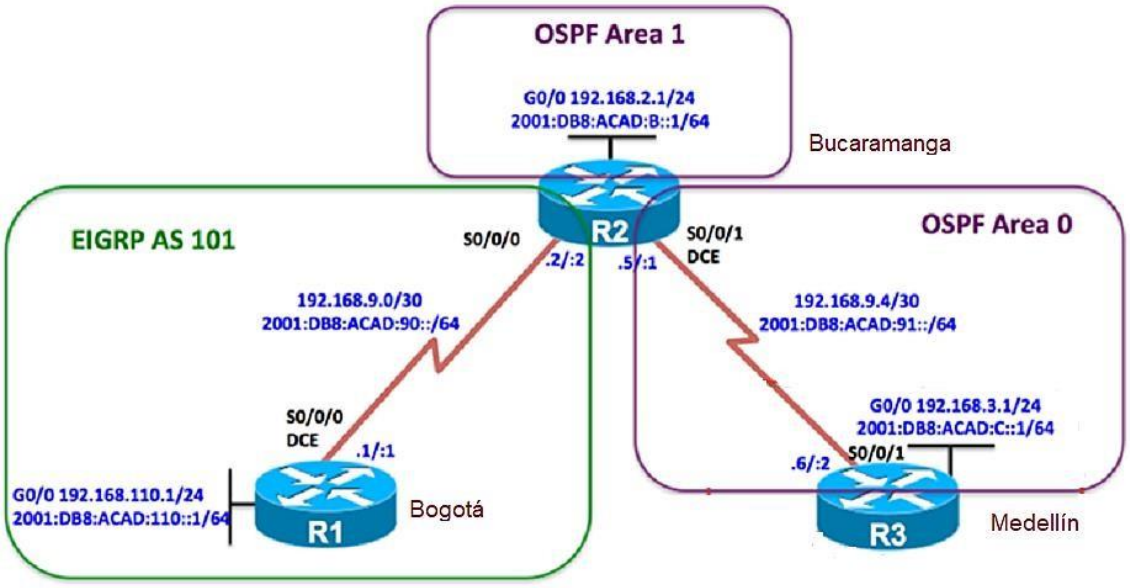
Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los

dispositivos, las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD**.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1: Una empresa de confecciones 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.

Topología de red



Configurar la topología de red, de acuerdo con las siguientes especificaciones.

OBJETIVOS

- Crear una red empresarial la cual tenga vlans con configuración estática.
- Aprender a utilizar e implementar las direcciones automáticas (DHCP) y NAT.
- Comprender el funcionamiento del trunking para la conexión entre vlans a través de los switches.
- Implementar y configurar enrutamiento OSPF para visualizar las listas de interfaces interconectadas

PALABRAS CLAVE

cisco, router, enrutamiento, interconexión, red, interfaz, lan, dirección, internet, configuración.

MARCO TEORICO.

EL SWITCH

Las redes Ethernet pueden mejorar su desempeño a partir de la conmutación de tramas. La conmutación permite segmentar una LAN creando dominios de colisión con anchos de banda exclusivos para cada segmento pudiendo transmitir y recibir al mismo tiempo sin el retardo que provocarían las colisiones. El ancho de banda dedicado por puerto es llamado microsegmentación. (Ariganello, 2009, p. 167)

Los puentes, switches y routers dividen las redes en segmentos. Los puentes trabajan a nivel de software generando alta latencia, los routers utilizan gran cantidad de recursos, mientras que los switches lo hacen a nivel de hardware siendo tan rápidos como el medio lo exija. (Ariganello, 2009, p. 167)

La conmutación permite:

- Comunicaciones dedicadas entre dispositivos. Los hosts poseen un dominio de colisión puro libre de colisiones, incrementando la rapidez de transmisión.
- Múltiples conexiones simultáneas. Los hosts pueden establecer conexiones simultáneas entre segmentos gracias a los circuitos virtuales proporcionados por los switch.
- Comunicaciones full-duplex. El ancho de banda dedicado por puerto permite transmitir y recibir a la vez, duplicando el ancho de banda teórico.
- Adaptación a la velocidad del medio. La conmutación creada por un switch funciona a nivel de hardware (ASIC: Circuito Integrado para Aplicación Específica), respondiendo tan rápidamente como el medio lo permita.
  (Ariganello, 2009, p. 168)

  Conmutación con switch

  Un switch segmenta una red en dominios de colisión, tantos como puertos activos posea. Aprender direcciones, reenviar, filtrar paquetes y evitar bucles también son funciones de un switch. (Ariganello, 2009, p. 168)

  El switch segmenta el tráfico de manera que los paquetes destinados a un dominio de colisión determinado no se propaguen a otro segmento, aprendiendo las direcciones MAC de los hosts. A diferencia de un hub, un switch no inunda todos los puertos con las tramas, por el contrario, el switch es selectivo con cada trama. (Ariganello, 2009, p. 168)

  Debido a que los switches controlan el tráfico para múltiples segmentos al mismo tiempo, han de implementar memoria búfer para que puedan recibir y transmitir tramas independientemente en cada puerto o segmento. (Ariganello, 2009, p. 168)

  Un switch nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como dirección de origen de la trama. Una trama de broadcast será transmitida a todos los puertos a la vez. (Ariganello, 2009, p. 168)

TECNOLOGÍAS DE CONMUTACIÓN

Atendiendo al método de direccionamiento de las tramas, los switches pueden clasificarse como:

De almacenamiento y envío (Store-and-Forward)

El switch debe recibir la trama completa antes de enviarla por el puerto de salida correspondiente. Lee la dirección MAC de destino, comprueba el CRC (verificación de redundancia cíclica, utilizado en las tramas para verificar errores de envío), aplica los filtrados correspondientes y retransmite. Si el CRC es incorrecto, se descarta la trama. El retraso de envío o latencia suele ser alto debido a que el switch debe almacenar la trama completa, verificarla y posteriormente enviarla al segmento correspondiente. (Ariganello, 2009, p. 169)

Método de corte (Cut-Through)

Este switch verifica la dirección MAC de destino en cuanto recibe la cabecera de la trama, y comienza de inmediato a enviar la trama a través del puerto de salida. La desventaja de este modo es que el switch podría retransmitir una trama de colisión o una trama con un valor de CRC incorrecto, pero la latencia es muy baja. (Ariganello, 2009, p. 169)

Libre de fragmentos (fragment free)

Modo de corte modificado, el switch lee los primeros 64 bytes antes de retransmitir la trama. Normalmente las colisiones tienen lugar en los primeros 64 bytes de una trama. El switch sólo envía las tramas que están libres de colisiones. (Ariganello, 2009, p. 169)

APRENDIZAJE DE DIRECCIONES

Un switch crea circuitos virtuales entre segmentos; para ello debe identificar las direcciones MAC de destino, buscar en su tabla de direcciones MAC a qué puerto debe enviarla y ejecutar el envío. Cuando un switch se inicia no posee datos sobre los hosts conectados a sus puertos, por lo tanto, inunda todos los puertos esperando llegar a la MAC correspondiente. (Ariganello, 2009, p. 169)

A medida que el switch conmuta tramas provenientes de diferentes hosts, va registrando el segmento al cual pertenece cada host. De esta manera aprende que hosts pertenecen a cada segmento. (Ariganello, 2009, p. (Ariganello, 2009, p. 169)

LAN virtuales (VLAN)

Las VLAN proveen seguridad, segmentación, flexibilidad y permiten además agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común. (Ariganello, 2009, p. 181)

Utilizando la electrónica y los medios existentes es posible asociar usuarios lógicamente con total independencia de su ubicación física incluso a través de una WAN. Las VLAN pueden existir en un solo switch o bien abarcar varios de ellos. Las VLAN pueden extenderse a múltiples switches por medio de enlaces troncales que se encargan de transportar tráfico de múltiples VLANS. (Ariganello, 2009, p. 181)

El rendimiento de una red se ve ampliamente mejorado al no propagarse las difusiones de un segmento a otro, aumentando también los márgenes de seguridad. Para que las VLANS puedan comunicarse son necesarios los servicios de routers que pueden implementar el uso de listas de control de acceso (ACL) para mantener el margen de seguridad necesario. (Ariganello, 2009, p. 181)

TRUNKING

Muchas veces es necesario agrupar usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas. Para conseguir esta comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las VLANS que tienen configuradas a través de enlaces troncales es necesario que las tramas sean identificadas con el propósito de saber a qué VLAN pertenecen. (Ariganello, 2009, p. 182)

A medida que las tramas salen del switch son etiquetadas para indicar a que VLAN corresponden; esta etiqueta es retirada una vez que entra en el switch de destino para ser enviada al puerto de VLAN correspondiente. (Ariganello, 2009, p. 182)

Un puerto de switch que pertenece a una VLAN determinada es llamado puerto de acceso, mientras que un puerto que transmite información de varias VLANS a través de un enlace punto a punto es llamado puerto troncal. (Ariganello, 2009, p. 182)

La información de todas las VLANS creadas viajará por el enlace troce automáticamente,

la VLAN 1, que es la VLAN por defecto o nativa, lleva la información del estado de los puertos. También es la VLAN de gestión. (Ariganello, 2009, p. 182)

EL ROUTER

Es un tipo especial de computador que cuenta con los mismos componentes básicos que un PC estándar de escritorio, tales como:

- Unidad central de procesamiento (CPU)
- Memoria RAM y ROM.
- Bus del sistema
- Distintas interfaces de entrada y salida (I/O).

Los routers operan en la capa de red del modelo OSI y están diseñados para cumplir algunas funciones que los switches y bridges no pueden realizar porque estos operan en la capa de enlace de datos. Dos funciones adicionales que los routers pueden realizar incluyen la asignación de rutas dinámicas y la fragmentación. Los routers conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de ellas. Emplean sistemas operativos de internetworking (IOS) para ejecutar los archivos de configuración. (Cisco systems 1 y 2, 2004, p. 491)

Un archivo de configuración de un router contiene las instrucciones y los parámetros que permiten que el dispositivo realice el control del flujo del tráfico entrante y saliente. A través de los protocolos de enrutamiento, los routers deciden cuál es la mejor ruta para los paquetes a través de la red en un momento dado. (Cisco systems 1 y 2, 2004, p. 491)

Componentes del router.

Los principales componentes de que consta un router son:

- RAM: Se usa para almacenar la información de la tabla de enrutamiento, caché de conmutación rápida, configuración de funcionamiento y colas de paquetes.
- NVRAM: Se usa para almacenar un archivo de configuración respaldo/inicio
- MEMORIA FLASH: Se usa para almacenar imágenes completas del software IOS.
- ROM: Se usa para guardar de forma permanente el código de diagnóstico de inicio.

- INTERFAZ DE CONSOLA: Puerto que proporciona acceso físico al router para configurarlo.
- INTERFACES DE RED: Proporcionan conectividad a las LAN y WAN

(Cisco systems 1 y 2, 2004, p. 492)

INTERFACES

Las interfaces son los puertos a través de los cuales se interconecta el router con las redes LAN y WAN, es decir, conectan el router a la red para permitir que las tramas entren y salgan. Estas interfaces pueden estar en la mother-board o en un módulo separado.

El router se emplea fundamentalmente como dispositivo WAN; los routers se interconectan entre sí mediante conexiones WAN. Son la columna vertebral de las grandes redes internas y de Internet. Operan en la capa 3 del modelo OSI y toman decisiones con base en las direcciones de red. Puede decirse que sus principales funciones son: la selección de la mejor ruta y la conmutación de los paquetes hacia la interfaz correspondiente. Los routers logran esto por medio de la creación de tablas de enrutamiento y del intercambio de información sobre estado de los enlaces con otros routers. (Cisco systems 1 y 2, 2004, p. 492).

SERVIDORES DE RED

Un servidor de red es un sistema informático usado como repositorio central de datos y programas que son compartidos por los usuarios en una red. Un servidor es una computadora diseñada para procesar las solicitudes y entregar datos a otro equipo en internet o en una red local. (Cisco systems 3 y 4, 2004, p. 538)

Aunque cualquier equipo que ejecuta un software especial puede funcionar como un servidor, el uso más típico de la palabra hace referencia a máquinas muy grandes y de alta potencia que almacenan información y programas y que prestan servicios a los usuarios de una red como son: correo electrónico, almacenamiento de archivos, traducción de nombres de dominio, etc. (Cisco systems 3 y 4, 2004, p. 538)

La mayoría de las redes informáticas empresariales están soportadas por uno o más servidores que manejan tareas especializadas. Estrictamente hablando, el "servidor" es el software que controla una determinada tarea. Sin embargo, la máquina potente que soporta dicho software también generalmente es llamada ñservidorò (Cisco systems 3 y 4, 2004, p. 538)

Tipos comunes de servidores

Aunque algunos de estos servidores funcionan en forma dedicada, es decir, el dispositivo ejecuta solo una función específica, algunas implementaciones pueden utilizar un servidor para múltiples propósitos. Una red empresarial de tamaño mediano o grande regularmente está soportada por diferentes tipos de servidores. Algunos de los servidores más comúnmente utilizados son:

Servidores Web. Su función es mostrar páginas web y ejecutar aplicaciones a través de navegadores web.

Servidores de correo electrónico. Facilitan el envío y recepción de mensajes de correo electrónico.

Servidor FTP. Permiten el traslado de archivos a través de la red empleando herramientas como el File Transfer Protocol (FTP). Estos servidores son accesibles en forma remota a través de programas cliente FTP.

Servidor de identidad. Estos servidores controlan el acceso en forma segura a las redes privadas, permitiendo solo usuarios autorizados.

(Cisco systems 3 y 4, 2004, p. 540)

Parte 1: Configuración del escenario propuesto

1. Configurar las interfaces con las direcciones IPv4 que se muestran en la topología de red.

   Para el router 1 (Medellín) la configuración de direcciones IP es la siguiente, donde se muestra a continuación en la imagen.

```
Port                  Link   VLAN   IP Address          IPv6 Addres
GigabitEthernet0/0    Up     --     192.168.99.2/24     <not set>
GigabitEthernet0/1    Up     --     <not set>           <not set>
GigabitEthernet0/2    Down   --     <not set>           <not set>
Serial0/3/0           Up     --     172.31.21.1/30      <not set>
Serial0/3/1           Down   --     <not set>           <not set>
Vlan1                 Down   1      <not set>           <not set>
Hostname: MEDELLIN

Physical Location: Intercity, Home City, Corporate Office, Main
```

Para la configuración del router 2 (Bogotá) se determinan las direcciones IP que se van a usar para cada puerto, a continuación, en la siguiente imagen están establecidas.

```
Port                  Link   VLAN   IP Address
GigabitEthernet0/0    Up     --     209.165.200.225/29
GigabitEthernet0/1    Down   --     <not set>
GigabitEthernet0/2    Down   --     <not set>
FastEthernet0/2/0     Up     1      --
FastEthernet0/2/1     Up     1      --
FastEthernet0/2/2     Up     1      --
FastEthernet0/2/3     Up     1      --
Serial0/3/0           Up     --     172.31.21.2/30
Serial0/3/1           Up     --     172.31.23.1/30
Vlan1                 Down   1      <not set>
Hostname: Router

Physical Location: Intercity, Home City, Corporate Of
```

La configuración del router 3 consiste en la dirección IP a la que esta conectada con el otro router vecino y una serie de loopbacks, mostrado a continuación.

```
Port                  Link   VLAN   IP Address          IPv6 Address
GigabitEthernet0/0    Down   --     <not set>           <not set>
GigabitEthernet0/1    Down   --     <not set>           <not set>
GigabitEthernet0/2    Down   --     <not set>           <not set>
Serial0/3/0           Down   --     <not set>           <not set>
Serial0/3/1           Up     --     172.31.23.2/30      <not set>
Loopback4             Up     --     192.168.4.1/24      <not set>
Loopback5             Up     --     192.168.5.1/24      <not set>
Loopback6             Up     --     192.168.6.1/24      <not set>
Vlan1                 Down   1      <not set>           <not set>
Hostname: B/MANGA

Physical Location: Intercity, Home City, Corporate Office, Main Wi
```

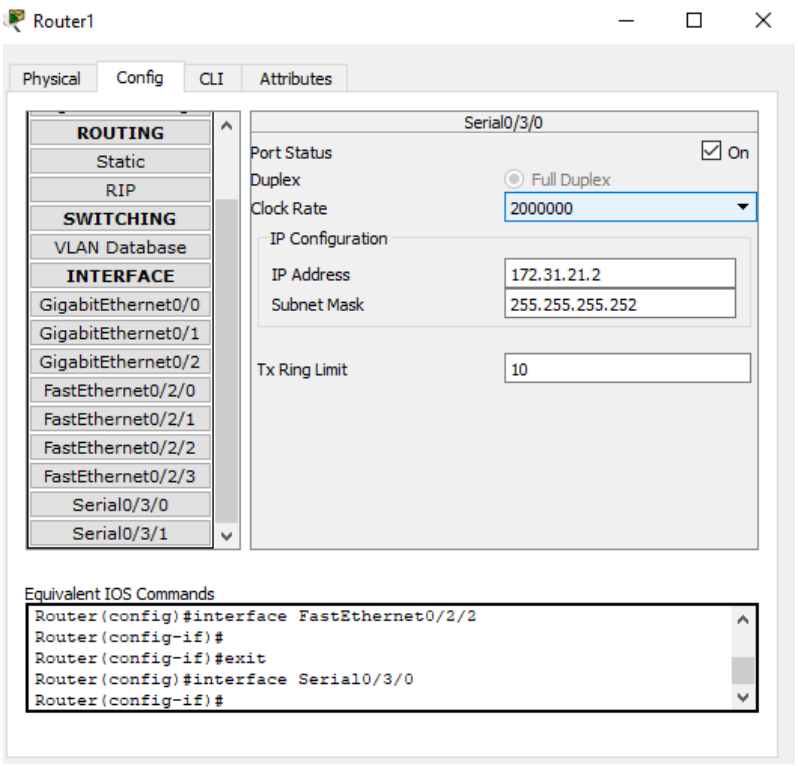
2. Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.

   Para el ajuste se configuran las interfaces que interconectan los routers, para esto se utiliza la siguiente instrucción como ejemplo.

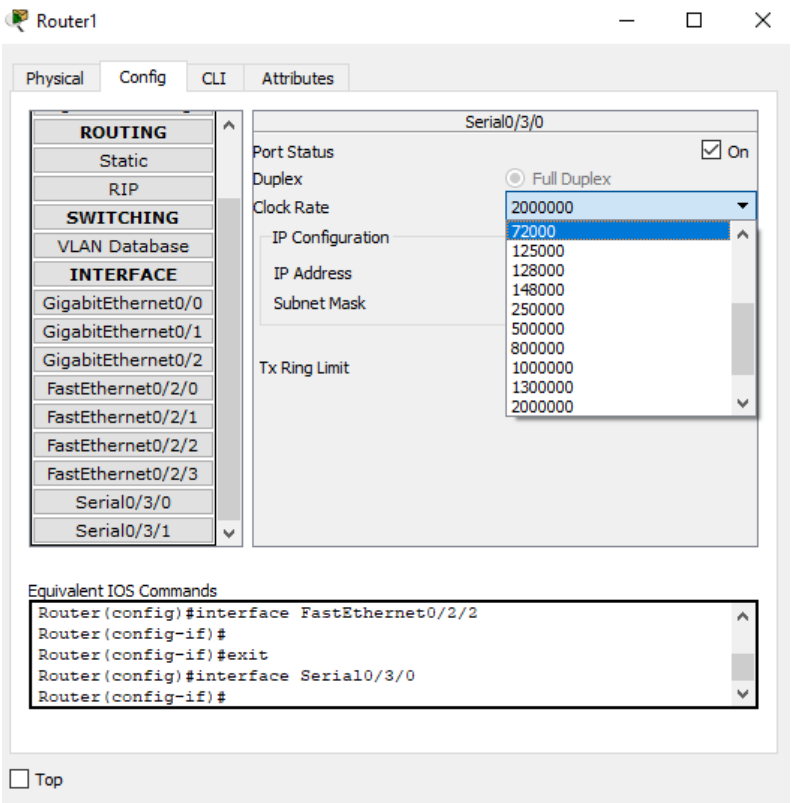
   ```
   Router(config)#interface s0/3/1
   Router(config-if)#bandwidth 128
   Router(config-if)#ip address 192.168.9.1 255.255.255.0
   Router(config)#exit
   ```

   Con la instrucción anterior se configuran todos los puertos en donde se requiere un ancho de banda de 128Kbps.

   Para la configuración del clock, tenemos que dar click en la config del router donde nos lleva a la siguiente ventana.



Después escogemos cuanto clock rate se necesita y lo escogemos.



OSPF.

Para la configuración del router se utiliza la siguiente instrucción, para OSPF.

OSPF-ADJCHG: Process 1, Nbr 192.18.15.1 on

Serial 2/0 from LOADING to FULL, Loading Done

Escriba el comando show ip ospf neighbor detail si desea más información acerca de la configuración del OSPF.

```
Brasilia#show ip ospf neighbor detail
 Neighbor 192.168.1.1, interface address 192.168.1.1
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 192.168.1.1 BDR is 192.168.1.2
    Options is 0x00
    Dead timer due in 00:00:39
    Neighbor is up for 00:22:01
    Index 1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 192.168.1.2, interface address 192.168.1.2
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 192.168.1.1 BDR is 192.168.1.2
    Options is 0x00
    Dead timer due in 00:00:31
    Neighbor is up for 00:21:59
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

NAT y DHCP.

Para la configuración de las direcciones con el protocolo DHCP se excluyen las direcciones reservadas para administradores o broadcast y a partir de ahí para los hosts de la red de la siguiente manera.

Router# ip dhcp pool redes

Router# network "*dirección de la red y su máscara"*

Router# default-router "*dirección del router"*

```
!
ip dhcp excluded-address 10.10.10.1 10.10.10.10
!
ip dhcp pool redes
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
!
```

El siguiente paso es configurar que direcciones IP quedan para la entrada y salida de NAT.

```
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 200.2.2.18 255.255.255.252
 ip nat outside
!
```

Y se asigna una red pública para la conversión hacia la internet.

```
!
ip nat pool public-access 199.99.9.32 199.99.9.35 netmask 255.255.255.252
ip nat inside source list 1 pool public-access overload
ip classless
ip route 0.0.0.0 0.0.0.0 200.2.2.17
!
ip flow-export version 9
!
!
access-list 1 permit 10.10.10.0 0.0.0.255
!
```

Ahora, para observar las conversiones que realiza NAT introduzca el comando debug ip nat en el modo EXEC privilegiado y ejecute varias veces el comando ping.

```
NAT#debug ip nat
IP NAT debugging is on
NAT#
NAT: s=10.10.10.13->199.99.9.33, d=200.200.50.2 [17]

NAT*: s=200.200.50.2, d=199.99.9.33->10.10.10.13 [4]

NAT: s=10.10.10.13->199.99.9.33, d=200.200.50.2 [18]

NAT*: s=200.200.50.2, d=199.99.9.33->10.10.10.13 [5]

NAT: s=10.10.10.13->199.99.9.33, d=200.200.50.2 [19]

NAT*: s=200.200.50.2, d=199.99.9.33->10.10.10.13 [6]

NAT: s=10.10.10.13->199.99.9.33, d=200.200.50.2 [20]

NAT*: s=200.200.50.2, d=199.99.9.33->10.10.10.13 [7]

NAT: s=10.10.10.13->199.99.9.33, d=172.16.1.1 [21]
```

VLANS

Para la reservación de direcciones en las vlans primero se definen las vlans en este caso 30 y 40, en donde se requieren 30 direcciones para cada una, entonces en el switch se configura cada puerto en donde se utilizarán estas direcciones de la siguiente manera.

```
Switch(config)#interface range fa0/1-31

Switch(config-if-range)#switchport access vlan 30

Switch(config-if-range)#exit
```

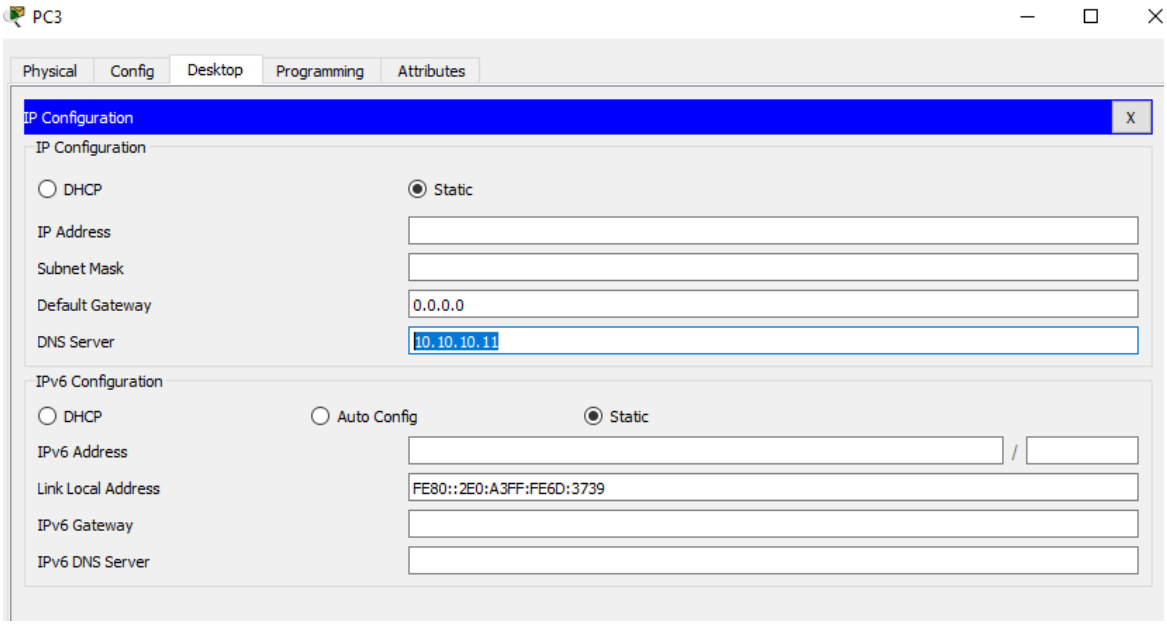
Con la instrucción anterior tenemos que en el rango de las interfaces de fastethernet de la 0/1 a la 0/31 (30 direcciones) serán de acceso para la vlan 30.

De igual manera se configura para la vlan 40.

DNS SERVER

La configuración del servidor DNS se configura desde los hosts que pertenecen a la red en este caso los hosts de la vlan 30 y vlan 40.

Se configura desde cada host de la red de la siguiente manera entrando a la configuración de la IP de cada host.



Se puede observar el DNS señalado en azul, se requiere un DNS server 10.10.10.11 como se muestra en la imagen.

ACL

Las listas de acceso nos permiten denegar o dejar acceder ciertas direcciones a una red o elemento de la red.

Para configurarlo se necesita el siguiente comando.

Access-list 1 deny “direccion IP con mascara invertida”

Access-list 1 permit “direccion IP con mascara invertida”

El caso que se requiere en este ejercicio es permitir o denegar trafico desde R1 o R3 hacia R2, entonces podemos denegar o permitir todo o algunas direcciones de R1 o R3.

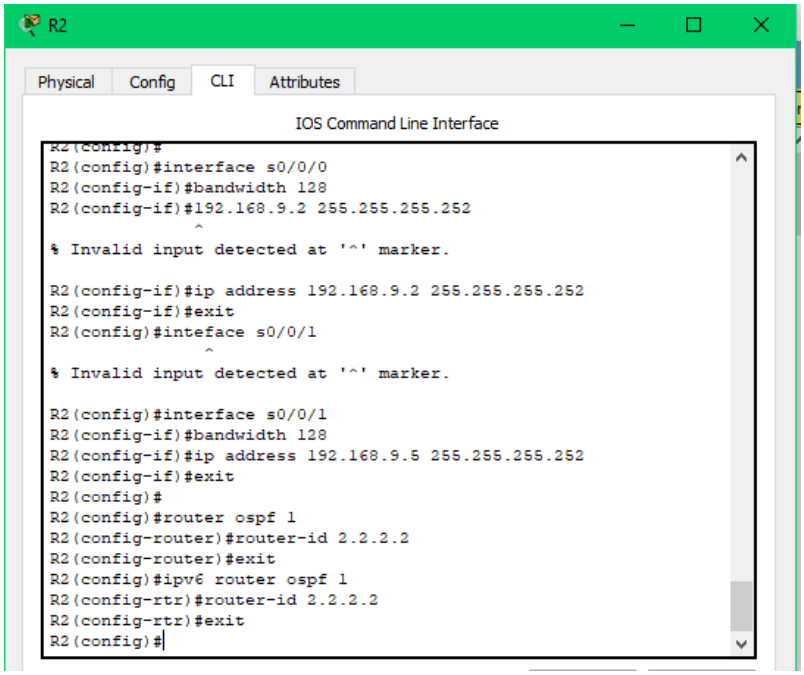
Para permitir o denegar todo seria de la siguiente manera. También teniendo en cuenta que se pueden crear mas de una lista de control de acceso.

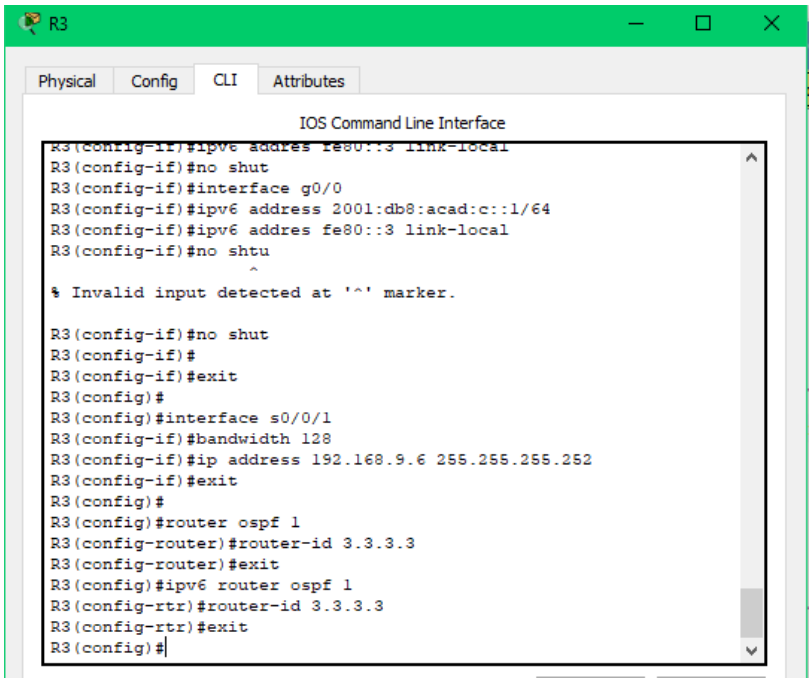
Access-list 1 permit any

Access-list 2 deny any

3. En R2 y R3 configurar las familias de direcciones OSPFv3 para IPv4 e IPv6. Utilice el

identificador de enrutamiento 2.2.2.2 en R2 y 3.3.3.3 en R3 para ambas familias de direcciones.





4. En R2, configurar la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3

en OSPF área 0.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.9.0 0.0.0.3 area 0
R2(config-router)#network 192.168.4.0 0.0.0.3 area 0
R2(config-router)#
```

Ctrl+F6 to exit CLI focus Copy

5. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0.

```
R3(config)#
R3(config)#router ospf 1
R3(config-router)#network 192.168.9.4 0.0.0.3 area 0
R3(config-router)#
```

Ctrl+F6 to exit CLI focus Copy

6. Configurar el área 1 como un área totalmente Stubby.

```
R2(config)#
R2(config)#
R2(config)#router ospf 1
R2(config-router)#area 1 nssa
R2(config-router)#
```

Ctrl+F6 to exit CLI focus

```
R3(config)#router ospf 1
R3(config-router)#area 1 nssa
R3(config-router)#exit
R3(config)#
```

Ctrl+F6 to exit CLI focus

7. Propagar rutas por defecto de IPv4 y IPv6 en R3 al interior del dominio OSPFv3. **Nota: Es importante tener en cuenta que una ruta por defecto es diferente a la definición de rutas estáticas.**

8. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Configurar la interfaz F0/0 de R1 y la conexión entre R1 y R2 para EIGRP con el sistema autónomo 101. Asegúrese de que el resumen automático está desactivado.

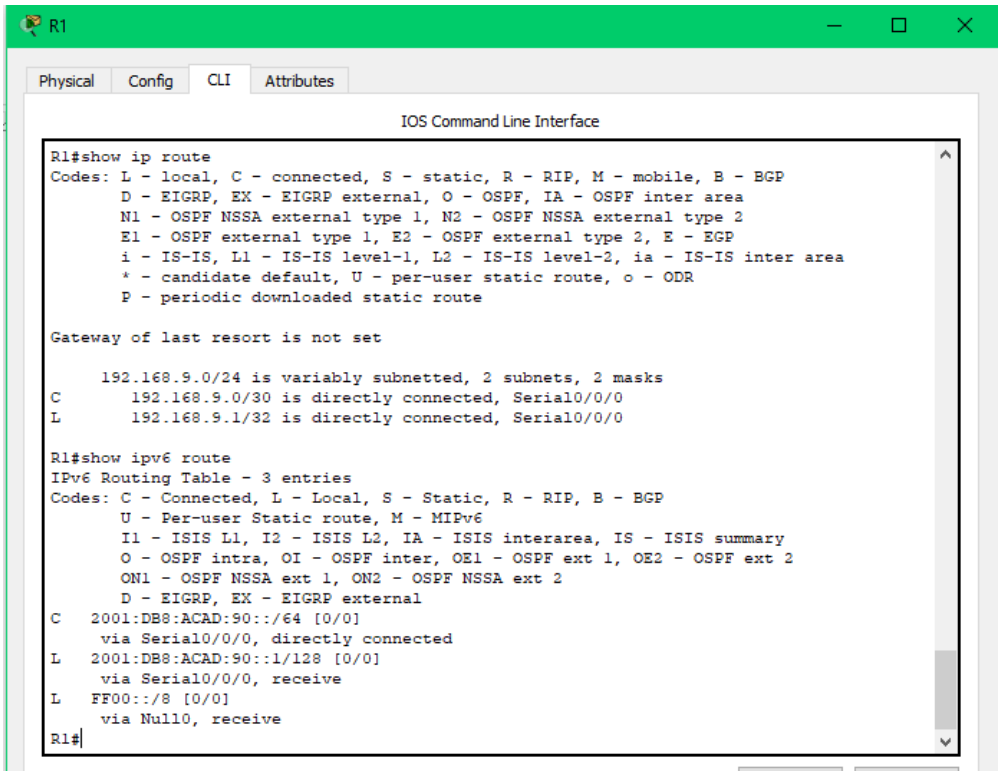
9. Configurar las interfaces pasivas para EIGRP según sea apropiado.

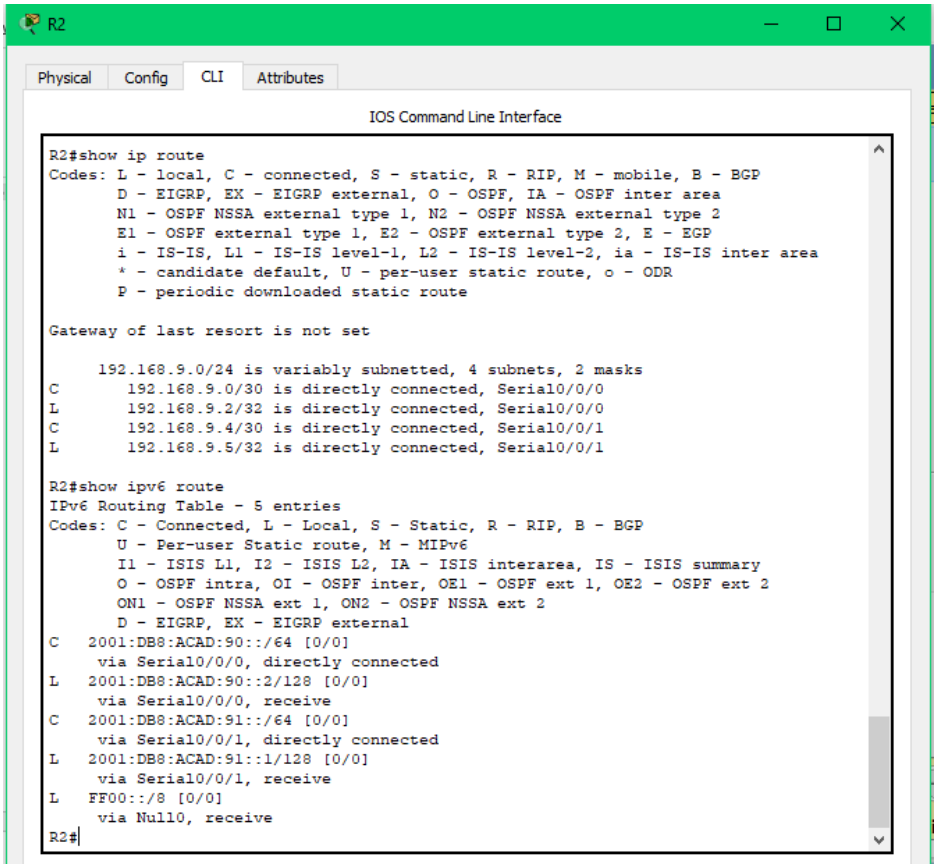
10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.

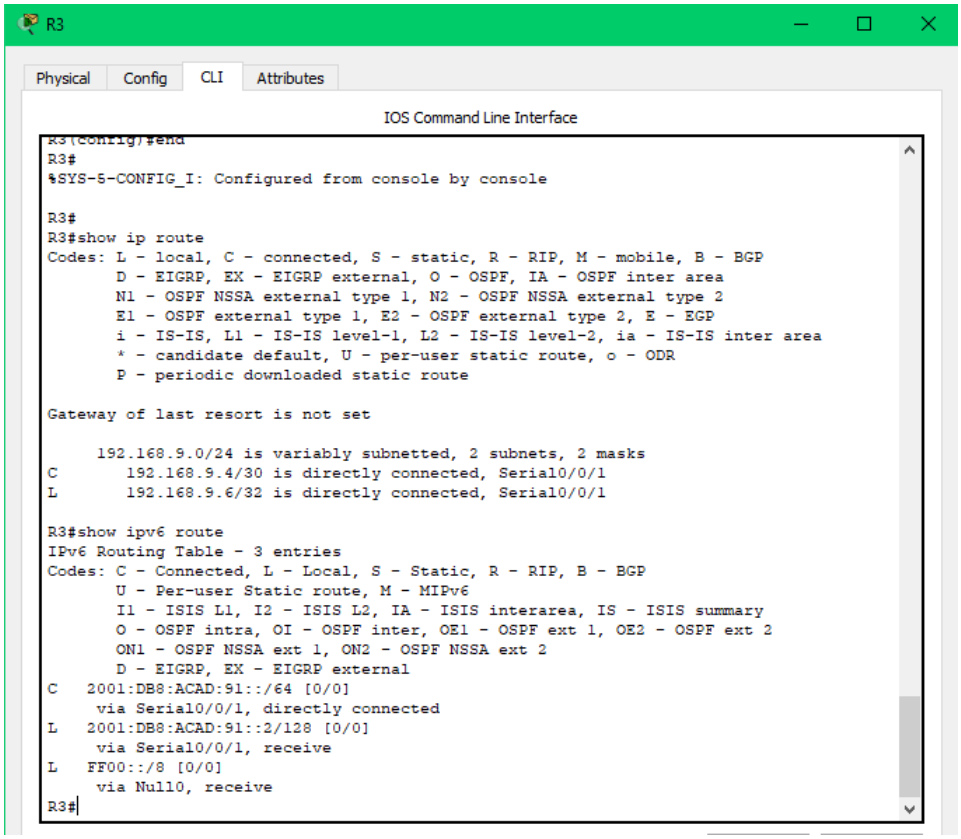
11. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL.

Parte 2: Verificar conectividad de red y control de la trayectoria.

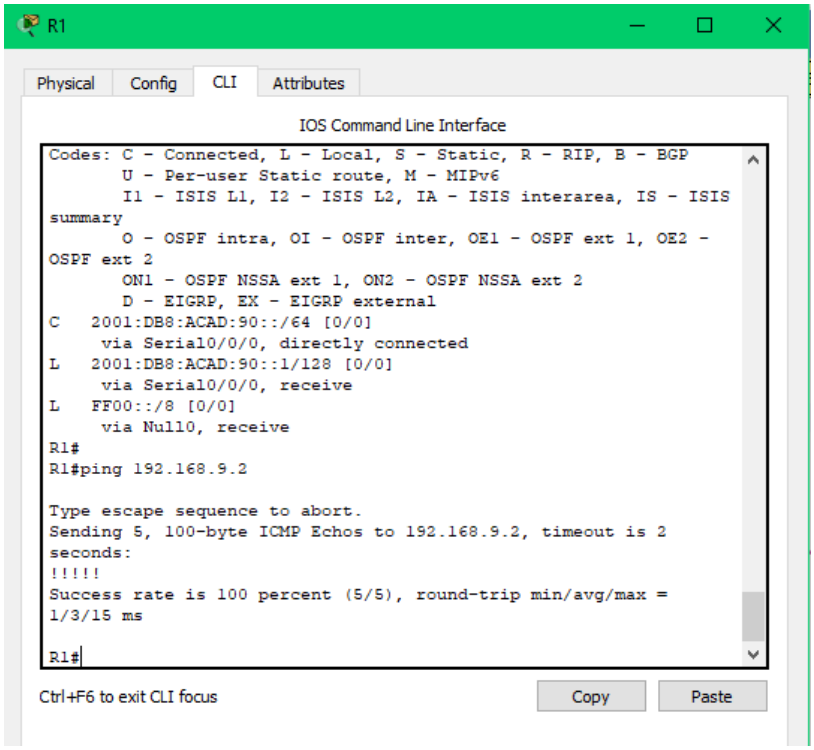
a. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.

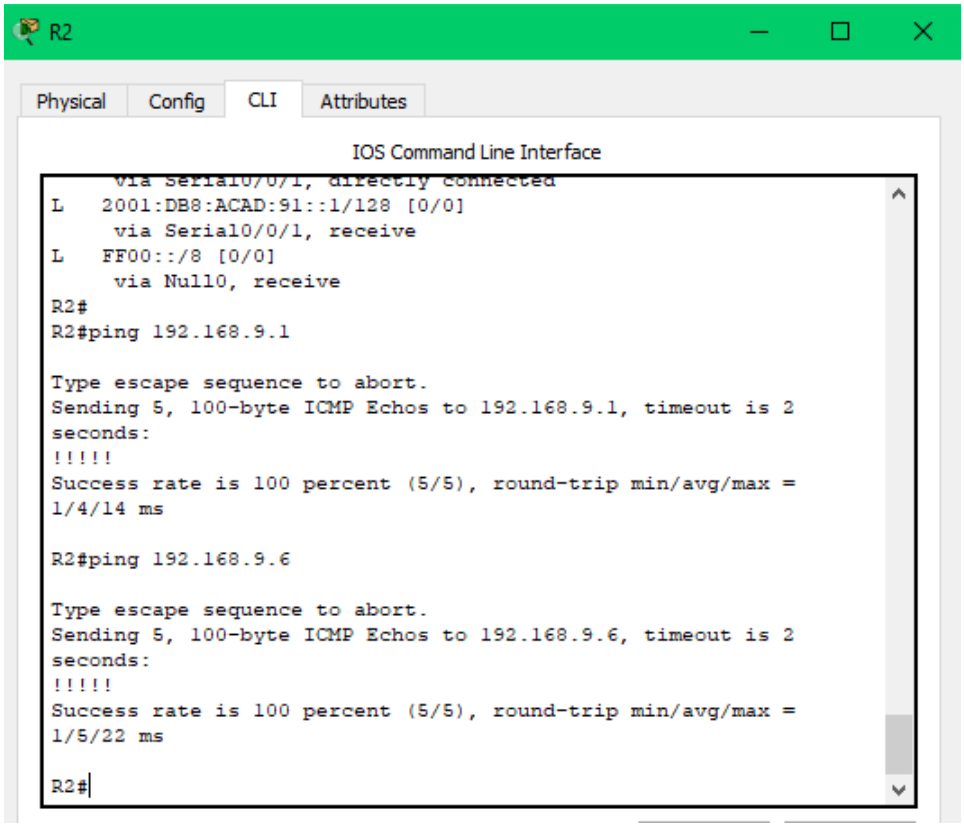


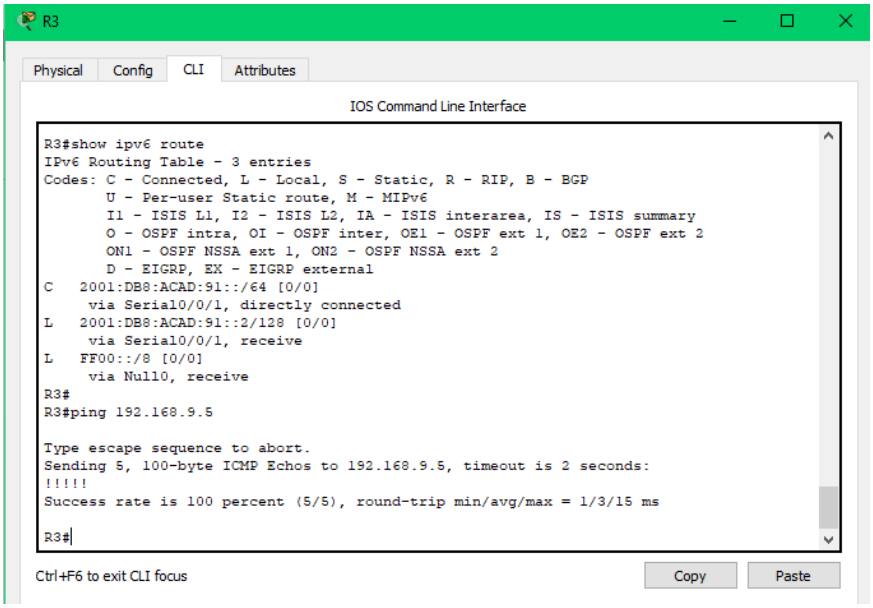

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.9.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.9.0/30 is directly connected, Serial0/0/0
L 192.168.9.2/32 is directly connected, Serial0/0/0
C 192.168.9.4/30 is directly connected, Serial0/0/1
L 192.168.9.5/32 is directly connected, Serial0/0/1
R2#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:90::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:90::2/128 [0/0]
via Serial0/0/0, receive
C 2001:DB8:ACAD:91::/64 [0/0]
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:91::1/128 [0/0]
via Serial0/0/1, receive
L FF00::/8 [0/0]
via Null0, receive
R2#



b. Verificar comunicación entre routers mediante el comando ping y traceroute


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:DB8:ACAD:90::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:ACAD:90::1/128 [0/0]
via Serial0/0/0, receive
L FF00::/8 [0/0]
via Null0, receive
R1#
R1#ping 192.168.9.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/15 ms
R1#
Ctrl+F6 to exit CLI focus
Copy
Paste


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
via Serial0/0/1, directly connected
L 2001:DB8:ACAD:91::1/128 [0/0]
via Serial0/0/1, receive
L FF00::/8 [0/0]
via Null0, receive
R2#
R2#ping 192.168.9.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms
R2#ping 192.168.9.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms
R2#



c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Nota: Puede ser que Una o más direcciones no serán accesibles desde todos los routers después de la configuración final debido a la utilización de listas de distribución para filtrar rutas y el uso de IPv4 e IPv6 en la misma red.

CONCLUSIONES

- Se debe definir una ACL para cada protocolo enrutado habilitado en la interfaz. Además, se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente.
- Las NAT son el único mecanismo utilizado para intercomunicar redes con distintos tipos de clases. Este mecanismo consiste en transportar la información mediante paquetes a través del router sin importar la clase de esta. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino. Esta combinación de números define una única conexión.
- DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de las direcciones IP de la red.

BIBLIOGRAFÍA

Ariganello E. (2009). Redes Cisco. Guía de estudio para la certificación CCNA 640-802. México: Alfaomega grupo editor.

Academia de networking de Cisco systems. (2004). Guía del primer año CCNA 1 y 2. Madrid: Pearson education S.A

Academia de networking de Cisco systems. (2004). Guía del primer año CCNA 3 y 4. Madrid: Pearson education S.A

Todd Lammle, ñCCNA: Cisco Certified Network Associate. Study Guideò 4ª Edición. Sybex Inc. 2004.

Cano, M. A. & López N. (2017). Práctica: Listas de control de acceso. Recuperado de://ocw.bib.upct.es/pluginfile.php/6732/mod_resource/content/1/PracticaCortafuegos.pdf.

Cisco. (2007, 27 de diciembre). Configuración de Listas de Acceso IP. Recuperado el 16 mayo de 2018 de https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html.