SOLUCIÓN DE CASO BAJO EL USO DE LA TECNOLOGIA CISCO
EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JHOAN MANUEL LEON VILLAMIL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
BOGOTÁ, COLOMBIA
2020

SOLUCION DE CASO BAJO EL USO DE LA TECNOLOGIA CISCO EVALUACIÓN – PRUEBA DE HABILIDADES PRACTICAS CCNA

JHOAN MANUEL LEON VILLAMIL

INFORME PRUEBA DE HABILIDADES PRACTICAS CISCO CCNA PARA OPTAR AL TÍTULO EN INGENIERÍA DE SISTEMAS

JOSE IGNACIO CARDONA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
BOGOTÁ, COLOMBIA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 15 mayo 2020

CONTENIDO

LISTA DE ILUSTRACIONES

INTRODUCCIÓN

El presente trabajo contiene el desarrollo de las habilidades prácticas de Cisco y pretende evaluar los conocimientos adquiridos a lo largo del desarrollo del diplomado de Profundización Cisco y nos presenta dos escenarios donde será necesario implementar las configuraciones básicas de cada dispositivo, configuración la seguridad del switch, las VLAN y routing entre VLAN, implementación DHCP y NAT para IPv4 configuración NTP,PAT,DHCP y se realizan las respectivas verificaciones de conectividad y ejecución en cada caso, para estas pruebas se utiliza la herramienta de simulación Packet Tracer tal como se hizo a lo largo del desarrollo del diplomado, adicional a esto brinda un análisis posterior al desarrollo de cada punto con el fin de mostrar el conocimiento de los efectos y causas del uso de los diferentes comandos y protocolos.

En el primer escenario se configura una red pequeña a la que se asignan los protocolos solicitados, configura routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente y se brinda la seguridad requerida para que sea funcional y operativa.

El escenario 2 se desarrolla sobre dos redes ubicadas en diferentes ciudades que deberán comunicarse entre sí, plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación. Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

RESUMEN

Las telecomunicaciones y el uso de herramientas informáticas son de vital importancia en el desarrollo de cualquier actividad, actualmente lo son aún más teniendo en cuenta los nuevos retos que debe asumir la sociedad y el mundo, en este escenario las redes informáticas y la conectividad son claves en la comunicación del planeta, conocerlas entenderlas y apropiarnos de ellas son una obligación como estudiantes de ingeniería de sistemas. Este trabajo nos permite de mostrar el conocimiento adquirido en el desarrollo del diplomado y presentar un soporte de ese conocimiento. El desarrollo de las diferentes actividades a través de CISCO Networking Academy, han permitido entender y comprender el curso “CISCO diseño e implementación de redes LAN-WAN”, se desarrollaron dos cursos como plan de capacitación dentro del diplomado: el primero bajo el título de “Network Fundamentals”, orientando desde los conceptos más básicos del networking, hasta el diseño e implementación de subredes de menor a mayor complejidad, y el segundo ”Routing Protocols and Concepts”, orientado a la conceptualización, configuración y resolución de problemas de protocolos.

Escenario 1

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

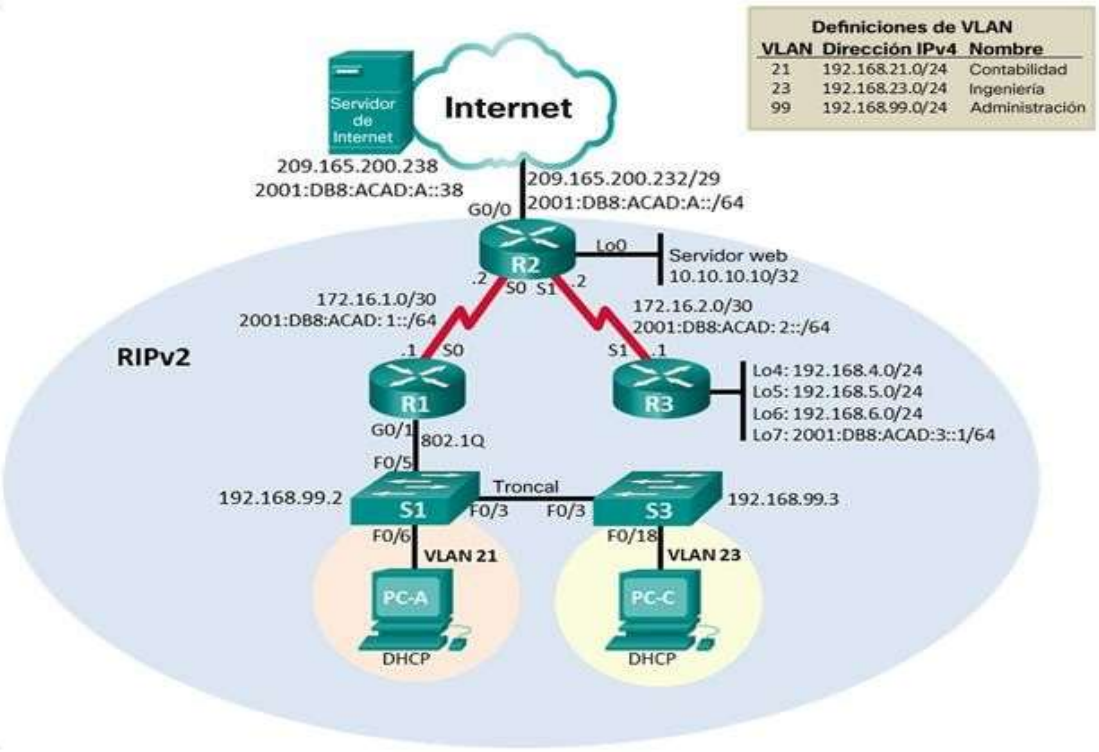


Ilustración 1. Topología, escenario 1

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Erase startup-config
Volver a cargar todos los routers	Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Write erase reload Dir flash: Delete flash:vlan.dat
Volver a cargar ambos switches	Reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show vlan Dir flash:

Análisis: Con estos comandos se evidencia la eliminación de todas las configuraciones anteriores y reinician los dispositivos con el fin de evitar afectación por antigua configuración en la nueva.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.240
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Análisis: En este paso se realiza la configuración de red para la computadora de internet, aquí se define la IPv 4, IPv6 y la puerta de enlace predeterminada.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	Service password-encription
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Description conexion a R2 Interface serial s0/0/0 Ip address 172.16.1.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:1::/64 Clock rate 128000 No shut
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 S0/0/0 Ipv6 route 2001:DB8:ACAD:1::/64 s0/0 Ipv6 route 2001:DB8:ACAD:2::/64 s0/0 Ipv6 route 2001:DB8:ACAD:3::/64 s0/0

Nota: Todavía no configure G0/1.

Análisis**:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de las mismas.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	Service password-encription
Habilitar el servidor HTTP	Ip http server Ip http secure-server Ip http authentication local
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Description conexion a R1 Ip address 172.16.1.2 255.255.255.252 Ipv6 address 2001:DB8:ACAD:1::/64 Clock rate 128000 No shut
Interfaz S0/0/1	Description conexion a R3 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::/64 Clock rate 128000 No shut
Interfaz G0/0 (simulación de Internet)	Description conexion a Internet. Ip address 209.165.200.233 255.255.255.248 Ipv6 address 2001:DB8:ACAD:A::/64 No shut
Interfaz loopback 0 (servidor web simulado)	Description servidor web. Ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Ip route 0.0.0.0 0.0.0.0 G0/0. Ipv6 route 2001:DB8:ACAD:1::/64 G0/0 Ipv6 route 2001:DB8:ACAD:2::/64 G0/0 Ipv6 route 2001:DB8:ACAD:3::/64 G0/0

Análisis**:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de las mismas.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	Service password-encription
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Description conexion a R2 Ip address 172.16.2.2 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::/64 Clock rate 128000 No shut
Interfaz loopback 4	Ip address 192.168.4.1 255.255.255.0 No shut
Interfaz loopback 5	Ip address 192.168.5.1 255.255.255.0 No shut
Interfaz loopback 6	Ip address 192.168.6.1 255.255.255.0 No shut
Interfaz loopback 7	Ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/1 Ipv6 route 2001:DB8:ACAD:3::/64 s/0/1

Análisis**:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de las mismas.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encription
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Análisis**:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de las mismas.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encription
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Análisis**:** Se da nombre a el dispositivo, contraseña de acceso a la consola y acceso privilegiado, se incluyó un mensaje de inicio para configurar los parámetros básicos de seguridad de acceso y se cifran las contraseñas con el fin de aumentar la seguridad de las mismas.

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.2	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.225	Exitoso

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Análisis**:** con la ejecución de estas pruebas se puede verificar que la configuración fue correcta y se tiene intercambio de paquetes entre los dispositivos.

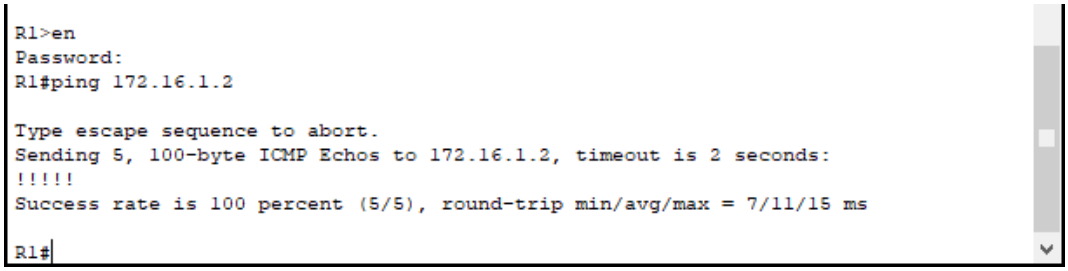


Ilustración 3. Paso 7, ping R1

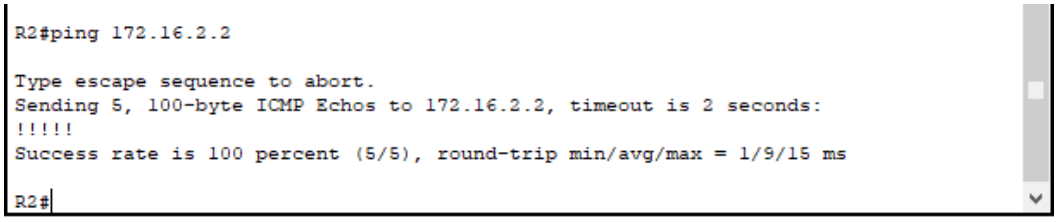


Ilustración 4. Paso 7 Ping R2

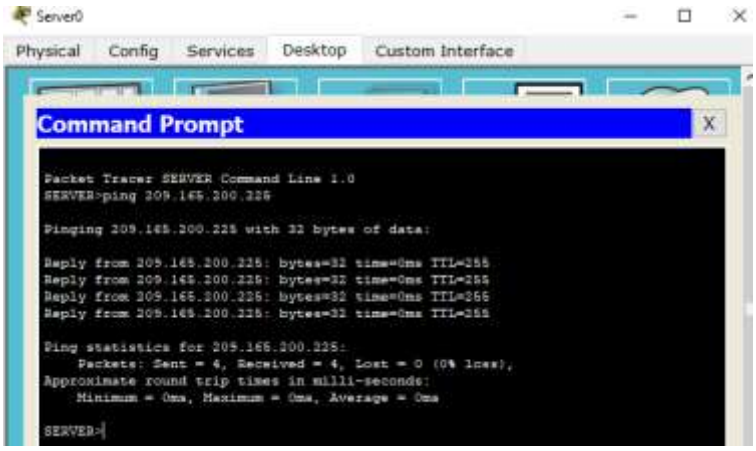


Ilustración 5. Paso 7 Ping PC internet

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Config term Vlan 21 Name contabilidad Vlan 23 Name ingenieria Vlan 99 Name administracion
Asignar la dirección IP de administración.	Interface vlan 99 Ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Interface f0/3 Switchport mode trunk Switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Interface f0/5 Switchport mode trunk Switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	interface range f0/1-2, f0/4, f0/7-24 switchport mode access
Asignar F0/6 a la VLAN 21	Interface f0/6 Switchport mode access Switchport access vlan 21
Apagar todos los puertos sin usar	interface range f0/1-2, f0/4, f0/7-24 shutdown

Análisis**:** se realiza la creación de las Vlan 21,23 y 99 y se establece la comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlan.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Config term Vlan 21 Name contabilidad Vlan 23 Name ingenieria Vlan 99 Name administracion
Asignar la dirección IP de administración	Interface vlan 99 Ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Interface f0/3 Switchport mode trunk Switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	interface range f0/1-2, f0/4-24 switchport mode access
Asignar F0/18 a la VLAN 23	Interface f0/18 Switchport mode access Switchport access vlan 23
Apagar todos los puertos sin usar	interface range f0/1-2, f0/4-17, f0/19-24 shutdown

Análisis**:** se realiza la creación de las Vlan 21,23 y 99 y se establece la comunicación entre los Switch de modo troncal con el de manejar el tráfico entre las Vlan.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Interface g0/1.21 Description LAN de Contabilidad Encapsulation dot1Q 21 Ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Interface g0/1.23 Descripción: LAN de Ingeniería Encapsulation dot1Q 23 Ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Interface g0/1.99 Descripción: LAN de Administración Encapsulation dot1Q 99 Ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	No shut

Análisis**:** se realiza la creación de las Vlan 21,23 y 99 y se establece la comunicación entre los Switch de modo troncal con el de manejar el tráfico entre las Vlan.

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Análisis**:** La ejecución de esta prueba permitió verificar la correcta configuración de tráfico entre las Vlan.

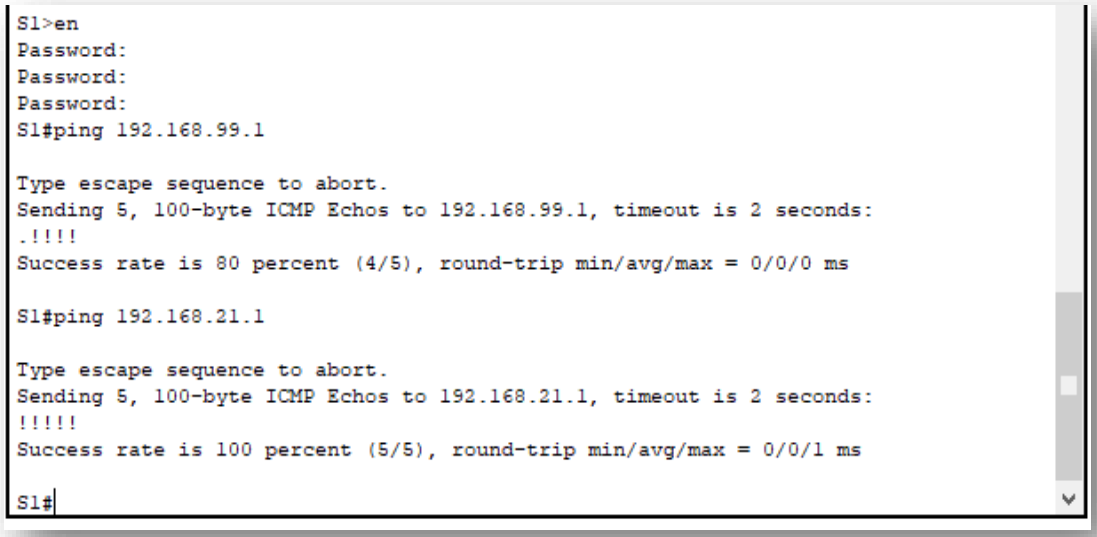


Ilustración 6. Paso 4, Prueba de conectividad S1

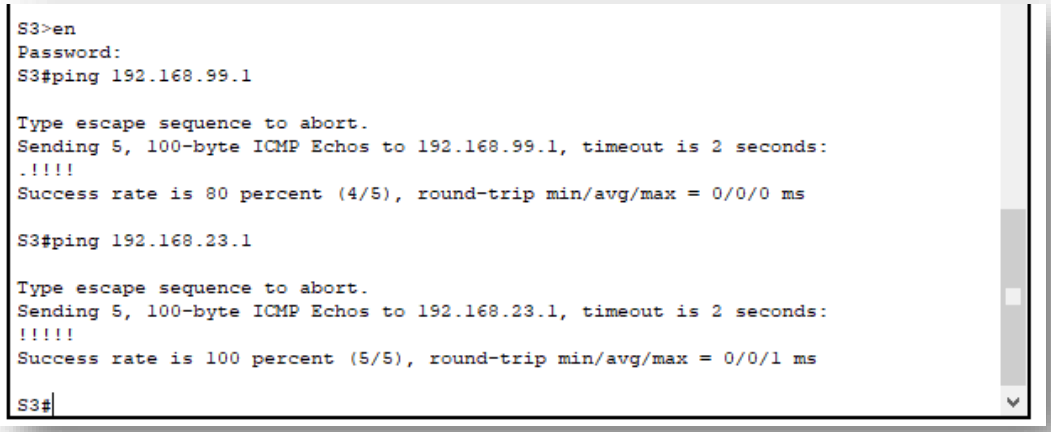


Ilustración 7. Paso 4, Prueba de conectividad S3

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config term Router rip Version 2
Anunciar las redes conectadas directamente	Network 172.16.1.0 Network 192.168.21.0 Network 192.168.23.0 Network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	Passive-interface g0/1.21 Passive-interface g0/1.23 Passive-interface g0/1.99
Desactive la sumarización automática	No auto-summary

Análisis**:** Se configura el protocolo RIPv2 con el fin de optimizar la comunicación entre routers, ya que este protocolo limita el máximo de saltos a 15 y desactivamos la sumarización ya que cuando se deshabilita la sumarización automática en RIP2 ya no resume las redes a su dirección con clase en routers fronterizos, sino que incluye todas las subredes y sus máscaras.

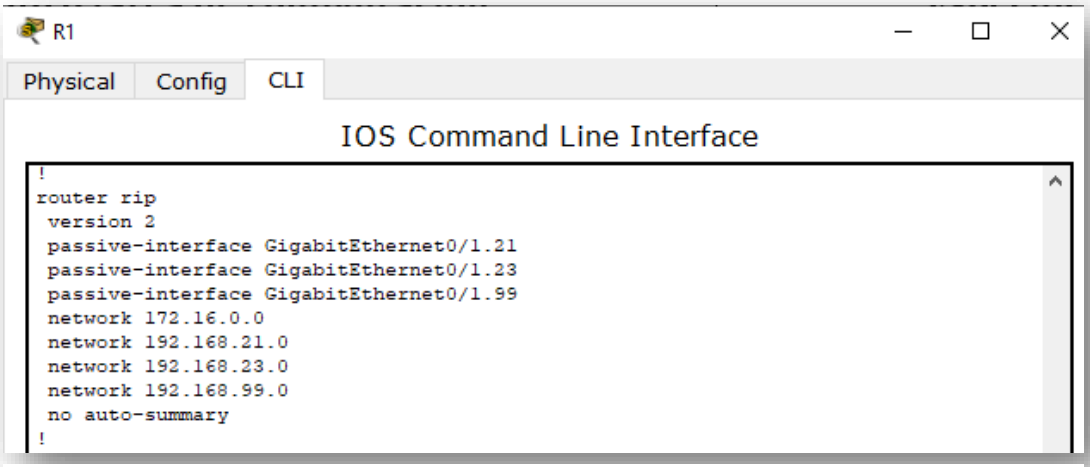


Ilustración 8 Paso 4 , Verificación de conectividad R1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config term Router rip Version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. Network 172.16.1.0 Network 172.16.2.0 Network 10.10.10.10
Establecer la interfaz LAN (loopback) como pasiva	Passive-interface loopback 0
Desactive la sumarización automática.	No auto-summary

Análisis**:** Se configura el protocolo RIPv2 con el fin de optimizar la comunicación entre routers, ya que este protocolo limita el máximo de saltos a 15 y desactivamos la sumarización ya que cuando se deshabilita la sumarización automática en RIP2 ya no resume las redes a su dirección con clase en routers fronterizos, sino que incluye todas las subredes y sus máscaras.

.

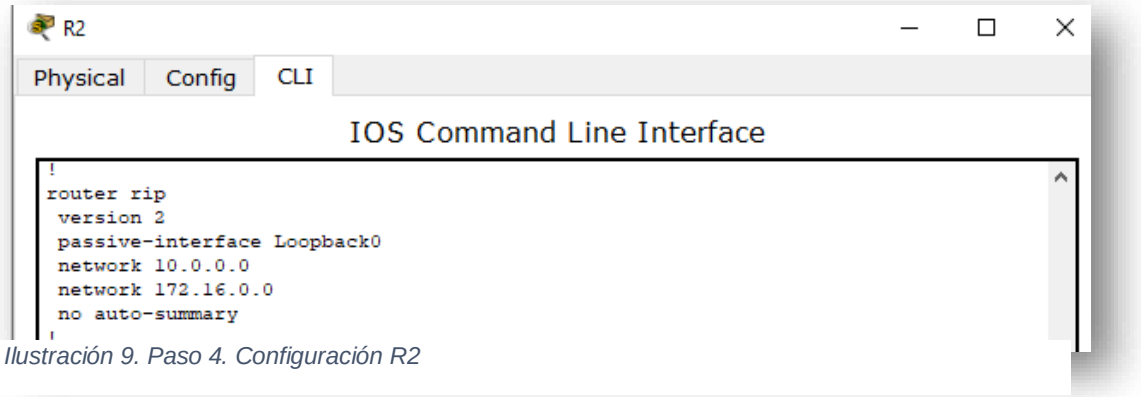


Ilustración 9. Paso 4. Configuración R2

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Config term Router rip Version 2
Anunciar redes IPv4 conectadas directamente	Network 172.16.2.0 Network 192.168.4.0 Network 192.168.5.0 Network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Passive-interface loopback 4 Passive-interface loopback 5 Passive-interface loopback 6
Desactive la sumarización automática.	No auto-summary

Análisis**:** Se configura el protocolo RIPv2 con el fin de optimizar la comunicación entre routers, ya que este protocolo limita el máximo de saltos a 15 y desactivamos la sumarización ya que cuando se deshabilita la sumarización automática en RIP2 ya no resume las redes a su dirección con clase en routers fronterizos, sino que incluye todas las subredes y sus máscaras.

.

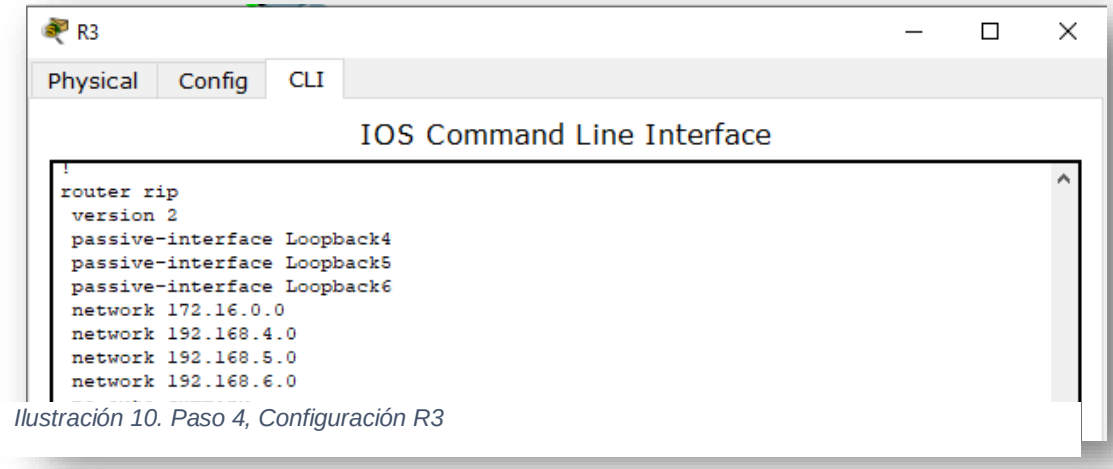


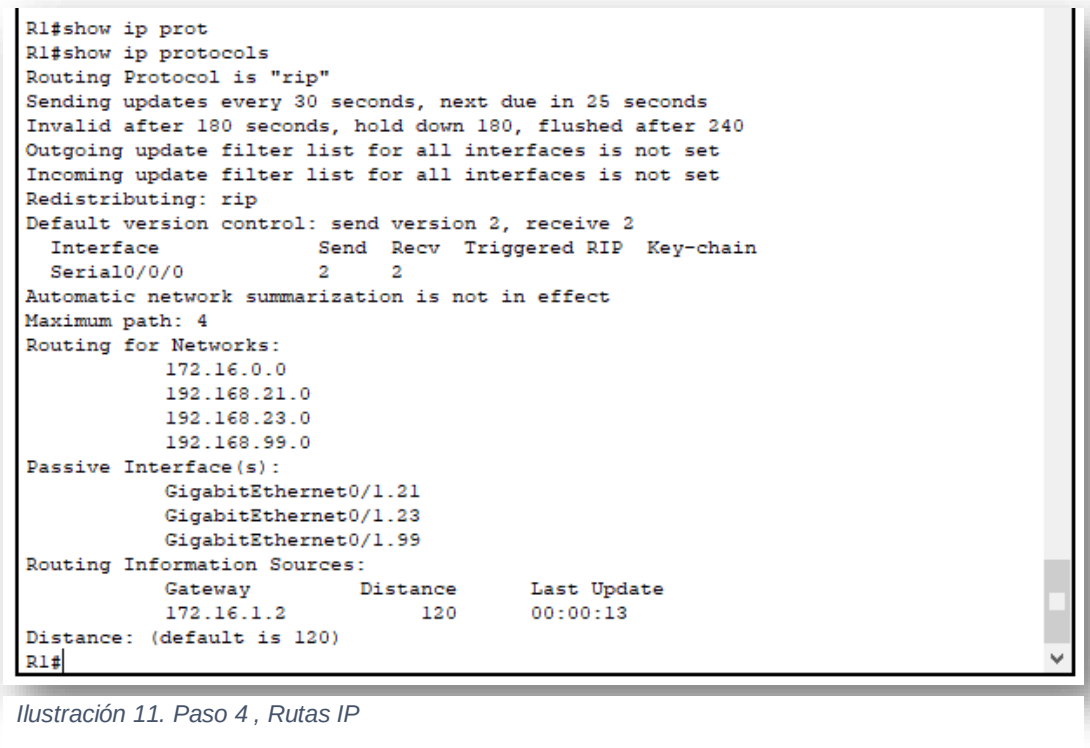
Ilustración 10. Paso 4, Configuración R3

Paso 4: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip rip database

Análisis: La ejecución de esta prueba permite verificar la información de las interfaces configuradas y la correcta ejecución de RIP.



```
R1#show ip prot
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 25 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
           172.16.0.0
           192.168.21.0
           192.168.23.0
           192.168.99.0
Passive Interface(s):
           GigabitEthernet0/1.21
           GigabitEthernet0/1.23
           GigabitEthernet0/1.99
Routing Information Sources:
           Gateway         Distance      Last Update
           172.16.1.2           120      00:00:13
Distance: (default is 120)
R1#
```

Ilustración 11. Paso 4 , Rutas IP

```
R1#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 0.0.0.0 to network 0.0.0.0

     10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10/32 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Serial0/0/0
L       172.16.1.1/32 is directly connected, Serial0/0/0
R       172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0
R    192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:04, Serial0/0/0
R    192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:04, Serial0/0/0
R    192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:04, Serial0/0/0
     192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
L       192.168.21.1/32 is directly connected, GigabitEthernet0/1.21
     192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
L       192.168.23.1/32 is directly connected, GigabitEthernet0/1.23
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
L       192.168.99.1/32 is directly connected, GigabitEthernet0/1.99
S*   0.0.0.0/0 is directly connected, Serial0/0/0
R1#
```

Ilustración 12. Paso 4 , Rutas IP

```
R1#show ip rip database
10.10.10.10/32    auto-summary
10.10.10.10/32
    [1] via 172.16.1.2, 00:00:10, Serial0/0/0
172.16.1.0/30    auto-summary
172.16.1.0/30    directly connected, Serial0/0/0
172.16.2.0/30    auto-summary
172.16.2.0/30
    [1] via 172.16.1.2, 00:00:10, Serial0/0/0
192.168.4.0/24    auto-summary
192.168.4.0/24
    [2] via 172.16.1.2, 00:00:10, Serial0/0/0
192.168.5.0/24    auto-summary
192.168.5.0/24
    [2] via 172.16.1.2, 00:00:10, Serial0/0/0
192.168.6.0/24    auto-summary
192.168.6.0/24
    [2] via 172.16.1.2, 00:00:10, Serial0/0/0
192.168.21.0/24    auto-summary
192.168.21.0/24    directly connected, GigabitEthernet0/1.21
192.168.23.0/24    auto-summary
192.168.23.0/24    directly connected, GigabitEthernet0/1.23
192.168.99.0/24    auto-summary
192.168.99.0/24    directly connected, GigabitEthernet0/1.99
R1#
```

Ilustración 13. Paso 4 , Data Base IP

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Ip dhcp pool ACCT Dns-server 10.10.10.10 Domain-name ccna-sa.com Default-router 192.168.21.1 Network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	Ip dhcp pool ENGNR Dns-server 10.10.10.10 Domain-name ccna-sa.com Default-router 192.168.23.1 Network 192.168.23.0 255.255.255.0

Análisis: Al configurar R1 como DHCP este equipo asignará las direcciones IP a los equipos en la red, de igual manera puede hacerlo con una o varias Vlan.

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	Ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Ip http authentication local

Crear una NAT estática al servidor web.	Ip nat inside source static 10.10.10.10 **209.165.200.238**
Asignar la interfaz interna y externa para la NAT estática	Int g0/0 Ip nat outside Int g0/1 Ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Access-list 1 permit 192.168.21.0 0.0.0.255 Access-list 1 permit 192.168.23.0 0.0.0.255 Access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye Ip nat pool INTERNET **209.165.200.225** – **209.165.200.238** netmask 255.255.255.240
Definir la traducción de NAT dinámica	Ip nat inside source list 1 pool INTERNET

Análisis: al configurar NAT estática en el R2 se asigna una IP fija externa que debe ser igual a la privada y se asigna una dinámica a la ACL privada. Esto sirve para que se lleve a cabo la traducción de IP entre las diferentes LAN (este protocolo se implementa pero no se ejecuta ya que todos los componentes están dentro de la misma red)

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Exitoso

Análisis: La ejecución de esta prueba se puede evidenciar el correcto funcionamiento del servidor DHCP ya que se valida la asignación de IP por parte del servidor.

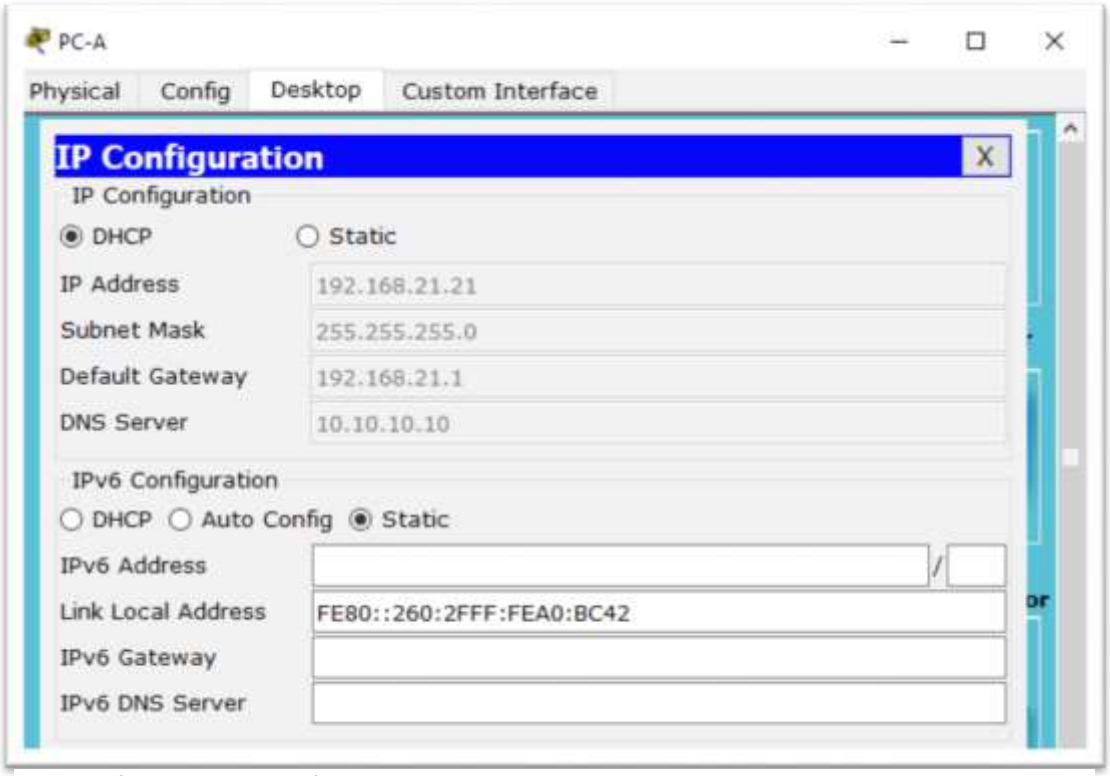


Ilustración 14, Configuración IP PC-A

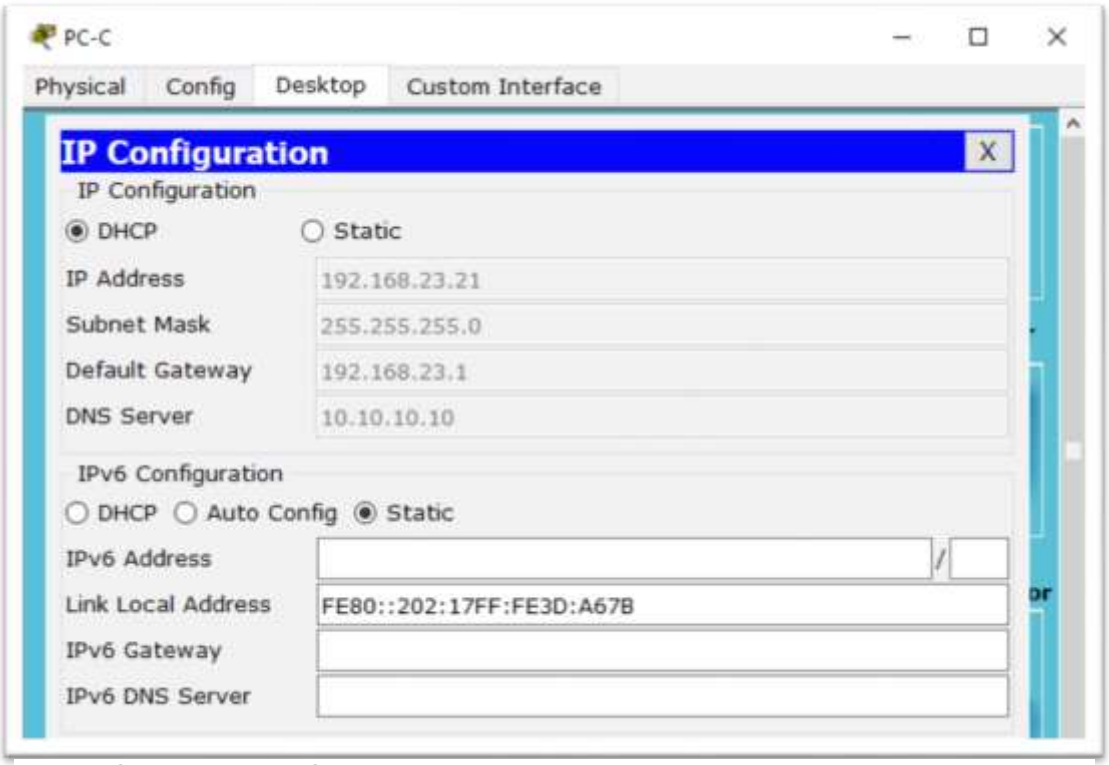


Ilustración 15. Configuración IP PC-C

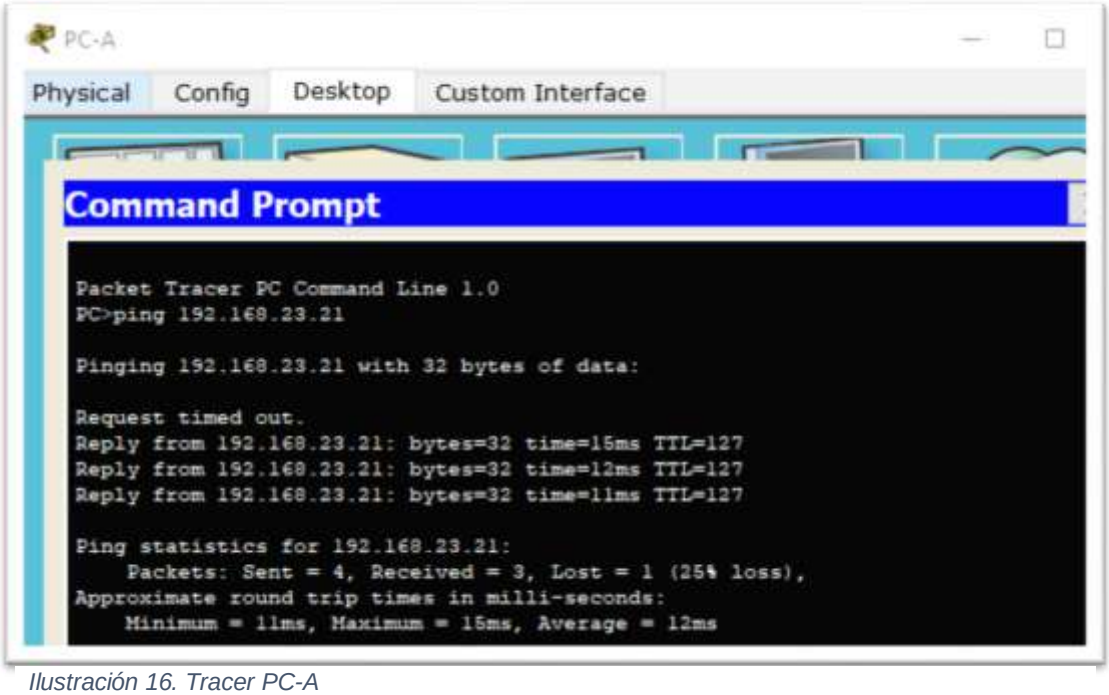


Ilustración 16. Tracer PC-A

Ilustración 17. Prueba de Navegación PC-A

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**clock set 09:00:00 05 MAR 2016**
Configure R2 como un maestro NTP.	Ntp server 172.16.1.2 level **5**
Configurar R1 como un cliente NTP.	Ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp status

Análisis: Se configura el protocolo NTP en R2 para configurar hora y fecha, queda R2 como maestro de modo que R1 tome esta información de él.

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	ip access-list standard **ADMIN-MGT** permit host 172.16.1.1

Aplicar la ACL con nombre a las líneas VTY	Line vty 0 4 Access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Line vty 0 4 Ip access-group 100 in Access-list 100 permit tcp any any eq 23
Verificar que la ACL funcione como se espera	telnet 172.16.1.2

Análisis: Al configurar las listas de acceso se delimita el acceso a R2 de manera que solo sea accesible a través de R1

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-list
Restablecer los contadores de una lista de acceso	Clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Config term Access-list ?
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. Show ip nat statics Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation

Escenario 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, 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.

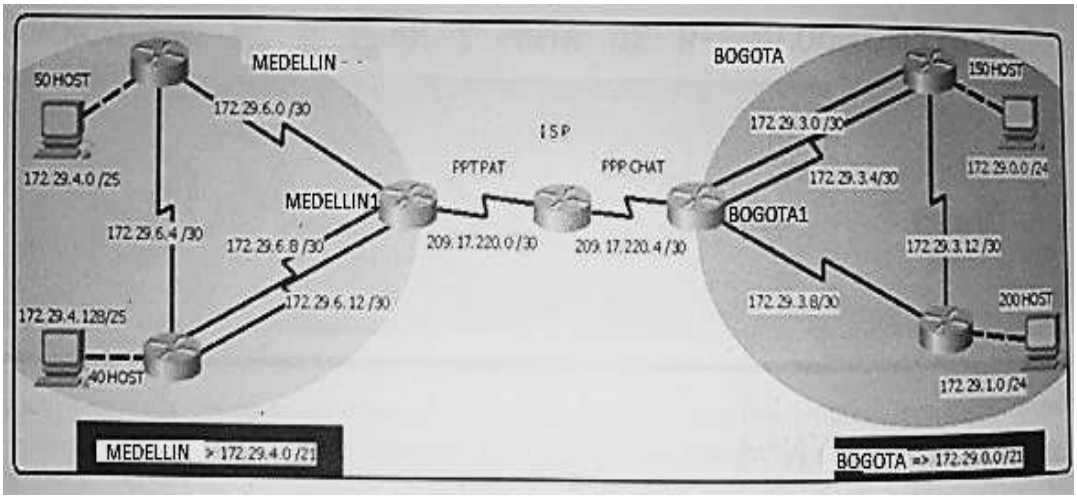


Ilustración 18. Topología escenario 2

Topología de red

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.
Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

Dentro de las rutinas normales de diagnóstico se realiza la configuración en cada uno de los routers con los siguientes parámetros, en los cuales lo único que se diferencia será las interfaces y las direcciones IP a asignar según la topología que se presenta.

ISP	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit ISP(config)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#exit ISP(config)#service password-encryption ISP(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Medellin 1	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Medellin1 Medellin1(config)#enable secret class Medellin1(config)#line console 0 Medellin1(config-line)#password cisco Medellin1(config-line)#login Medellin1(config-line)#exit Medellin1(config)#line vty 0 15 Medellin1(config-line)#password cisco Medellin1(config-line)#login Medellin1(config-line)#exit Medellin1(config)#service password-encryption Medellin1(config)#banner motd & enter text message. end with the character '&'. Se prohibe el acceso no autorizado &
Medellín 2	Router>enable Router#config t

	Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Medellin2 Medellin2(config)#enable secret class Medellin2(config)#line console 0 Medellin2(config-line)#password cisco Medellin2(config-line)#login Medellin2(config-line)#exit Medellin2(config)#line vty 0 15 Medellin2(config-line)#password cisco Medellin2(config-line)#login Medellin2(config-line)#exit Medellin2(config)#service password-encryption Medellin2(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Medellin 3	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Medellin3 Medellin3(config)#enable secret class Medellin3(config)#line console 0 Medellin3(config-line)#password cisco Medellin3(config-line)#login Medellin3config-line)#exit Medellin3(config)#line vty 0 15 Medellin3(config-line)#password cisco Medellin3(config-line)#login Medellin3(config-line)#exit Medellin3(config)#service password-encryption Medellin3(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Bogotá 1	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Bogota1 Bogota1(config)#enable secret class Bogota1(config)#line console 0

	Bogota1(config-line)#password cisco Bogota1(config-line)#login Bogota1(config-line)#exit Bogota1(config)#line vty 0 15 Bogota1(config-line)#password cisco Bogota1(config-line)#login Bogota1(config-line)#exit Bogota1(config)#service password-encryption Bogota1(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado &
Bogotá 2	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Bogota2 Bogota2(config)#enable secret class Bogota2(config)#line console 0 Bogota2(config-line)#password cisco Bogota2(config-line)#login Bogota2(config-line)#exit Bogota2(config)#line vty 0 15 Bogota2(config-line)#password cisco Bogota2(config-line)#login Bogota2(config-line)#exit Bogota2(config)#service password-encryption Bogota2(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado
Bogotá 3	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname Bogota3 Bogota3(config)#enable secret class Bogota3(config)#line console 0 Bogota3(config-line)#password cisco Bogota3(config-line)#login Bogota3(config-line)#exit Bogota3(config)#line vty 0 15 Bogota3(config-line)#password cisco Bogota3(config-line)#login

	Bogota3(config-line)#exit Bogota3(config)#service password-encryption Bogota3(config)#banner motd & Enter TEXT message. End with the character '&'. Se prohibe el acceso no autorizado

Esta configuración general se aplica a todos los routers que aparecen en la topología, las contraseñas y los accesos privilegiados se realizaron del mismo modo que se realizó en el escenario 1

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

Realizamos el calculo de las redes para identificar las IP utilizables para cada red

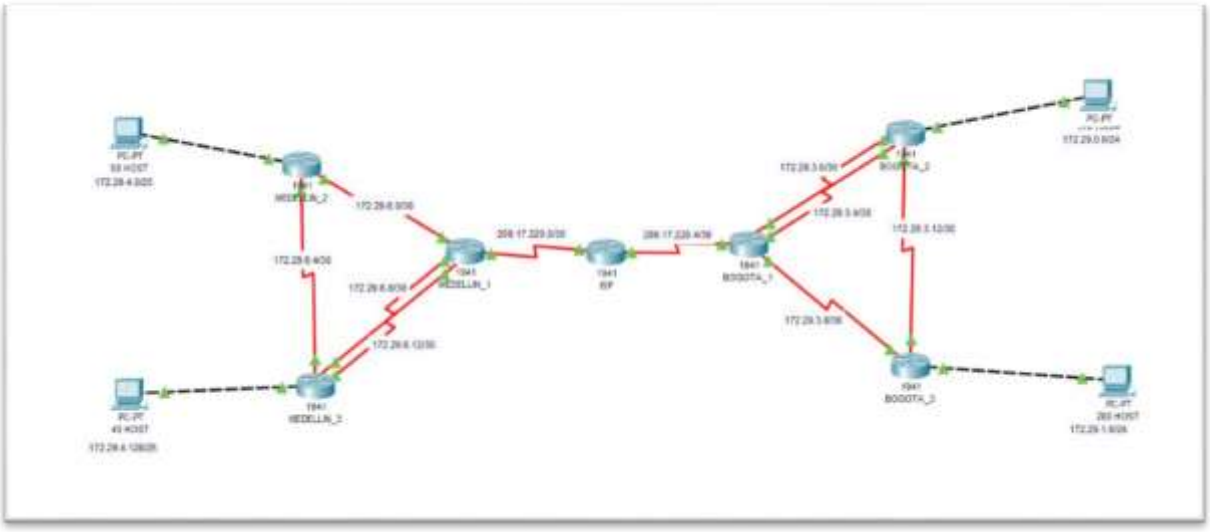


Ilustración 19 Topología de red Escenario 2

Parte 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.
b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

Desarrollo

Se inicia configurando el enrutamiento OSPF en el router ISP el cual se describe como el enrutador que permite establecer el enlace entre los routers de BOGOTA_1 y MEDELLIN_1	ISP#config term Aplicamos el protocolo de enrutamiento que vamos a utilizar ISP(config)#router ospf 10 Identificadas las interfaces que estan interactuando en el enrutamiento, se procede a asiganarlas a traves de la direccion de red y la mascara wild card, asignando a todas las redes que se configuren la area 0 ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0 ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0 Una vez terminamos de asignar las interfaces, se procede a salir. ISP(config-router)#exit Ahora asignamos las rutas estaticas solicitadas. ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2 ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.4 ISP(config)#
Se analiza la topologia y se configura el OSPF en los routers de MEDELLIN teniendo en cuenta el direccionamiento descrito en la topologia, asi como tambien el analisis realizado con el show ip route una vez se asignaron a todas las interfaces el direccionamiento IP.	MEDELLIN_1(config)#router ospf 10 MEDELLIN_1(config-router)#network 209.17.220.0 0.0.0.3 area 0 MEDELLIN_1(config-router)#network 172.16.6.12 0.0.0.3 area 0

	MEDELLIN_1(config-router)#network 172.16.6.8 0.0.0.3 area 0 MEDELLIN_1(config-router)#network 172.16.6.0 0.0.0.3 area 0 MEDELLIN_1(config-router)#exit MEDELLIN_1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN_1(config)# MEDELLIN_2(config)#router ospf 10 MEDELLIN_2(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN_2(config-router)#network 172.29.4.0 0.0.0.127 area 0 MEDELLIN_2(config-router)# MEDELLIN_3(config)#router ospf 10 MEDELLIN_3(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN_3(config-router)#network 172.29.6.8 0.0.0.3 area 0 MEDELLIN_3(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN_3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Se analiza la topologia y se configura el OSPF en los routers de BOGOTA teniendo en cuenta el direccionamiento descrito en la topologia, asi como tambien el analisis realizado con el show ip route una vez se asignaron a todas las interfaces el direccionamiento IP.	BOGOTA_1(config)#router ospf 10 BOGOTA_1(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA_1(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA_1(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA_1(config-router)#network 209.17.220.4 0.0.0.3 area 0 BOGOTA_1(config-router)#exit BOGOTA_1(config)#

	BOGOTA_2#config term BOGOTA_2(config)#router ospf 10 BOGOTA_2(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA_2(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA_2(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA_2(config-router)#network 172.29.0.0 0.0.0.255 area 0 BOGOTA_2(config-router)#exit BOGOTA_2(config)# BOGOTA_3(config)#router ospf 10 BOGOTA_3(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA_3(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA_3(config-router)#network 172.29.1.0 0.0.0.255 area 0 BOGOTA_3(config-router)#exit BOGOTA_3(config)# BOGOTA_3#

Análisis: De esta manera se configura el direccionamiento de cada uno de los equipos y se establece la configuración routers del protocolo OSPF para jerarquizar la pasarela interior, es decir calcular la ruta más corta entre los nodos.

Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
b. Verificar el balanceo de carga que presentan los routers.
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

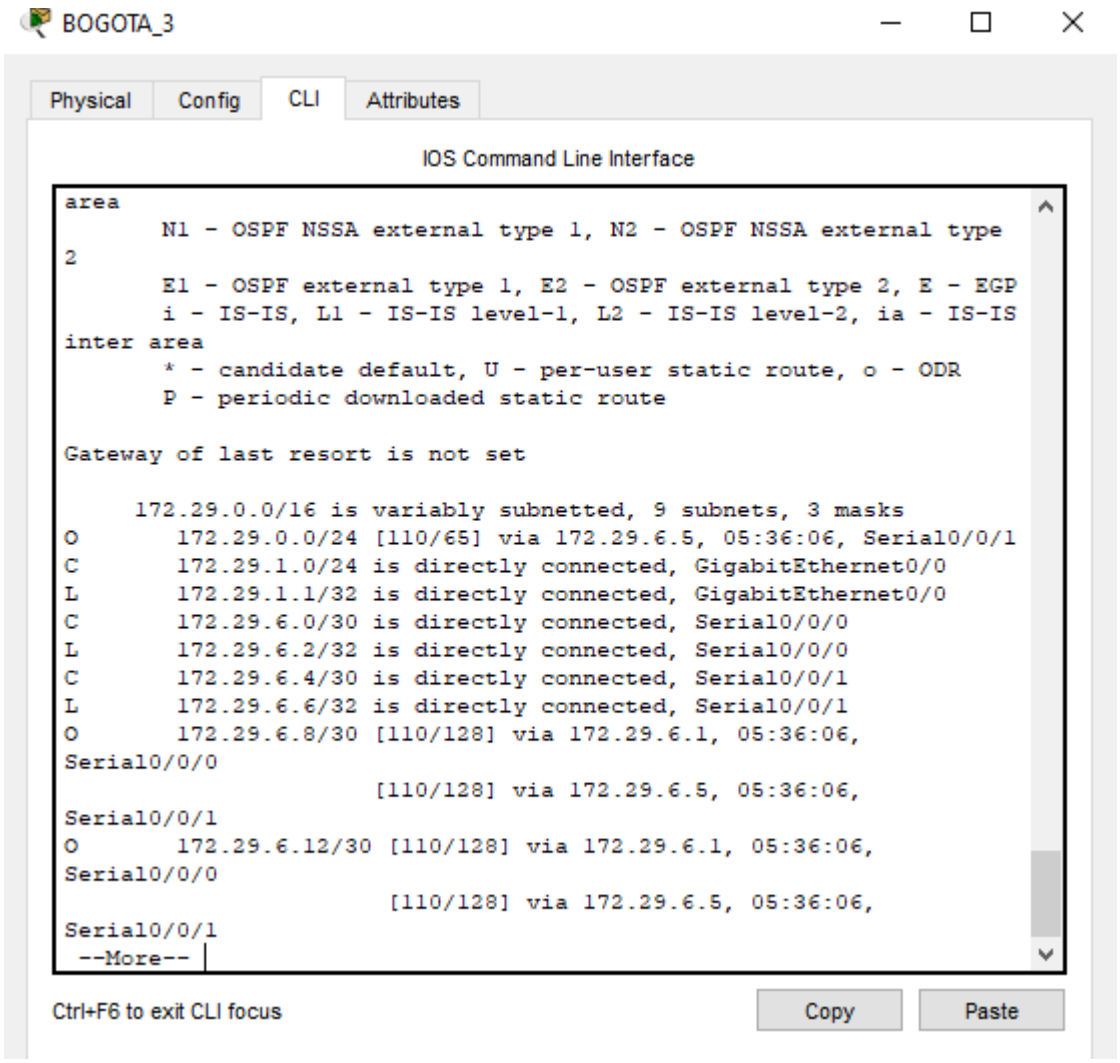


Ilustración 20. Rutas IP, Bogotá_3

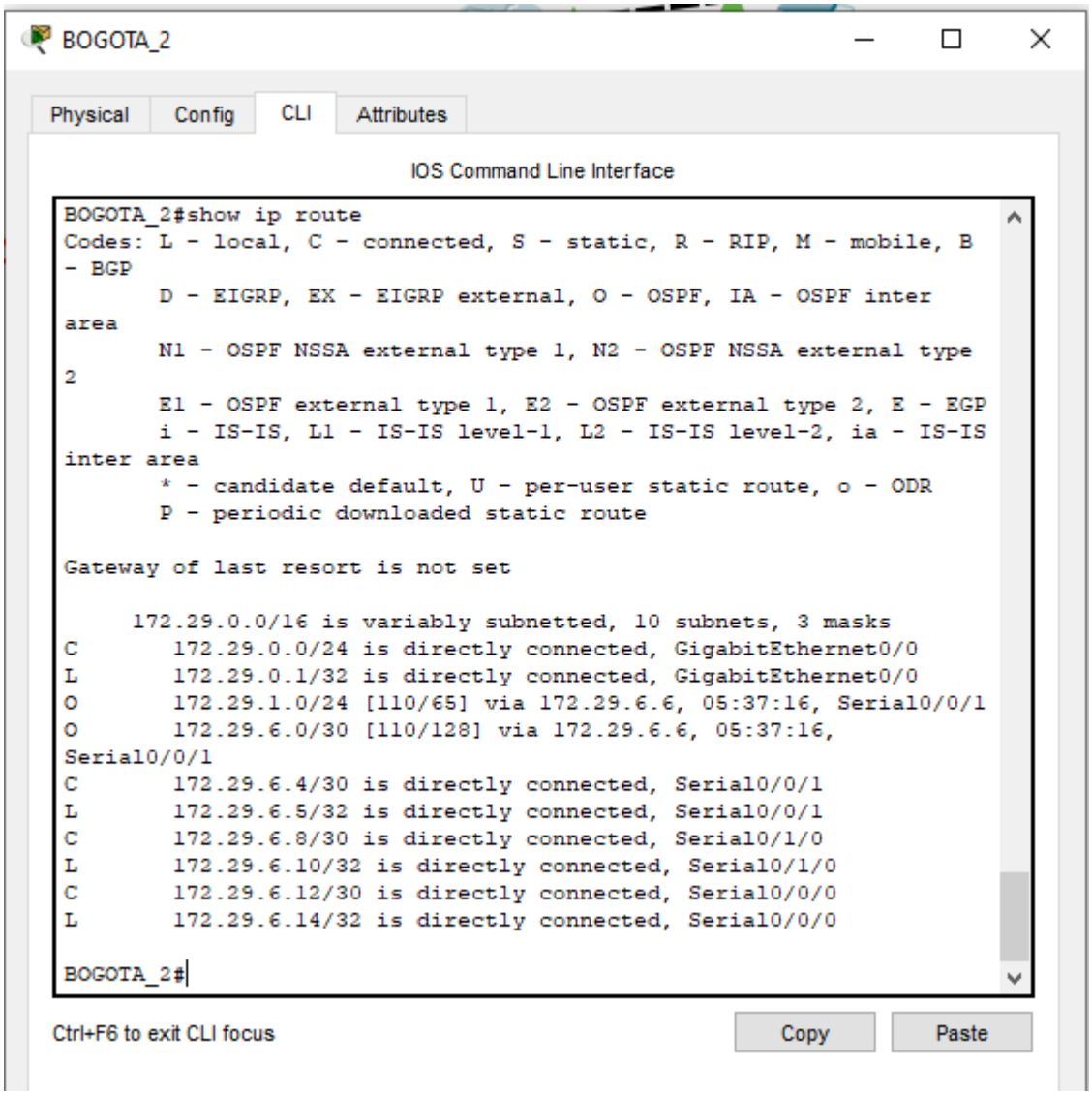


Ilustración 21. Rutas IP, Bogotá_2

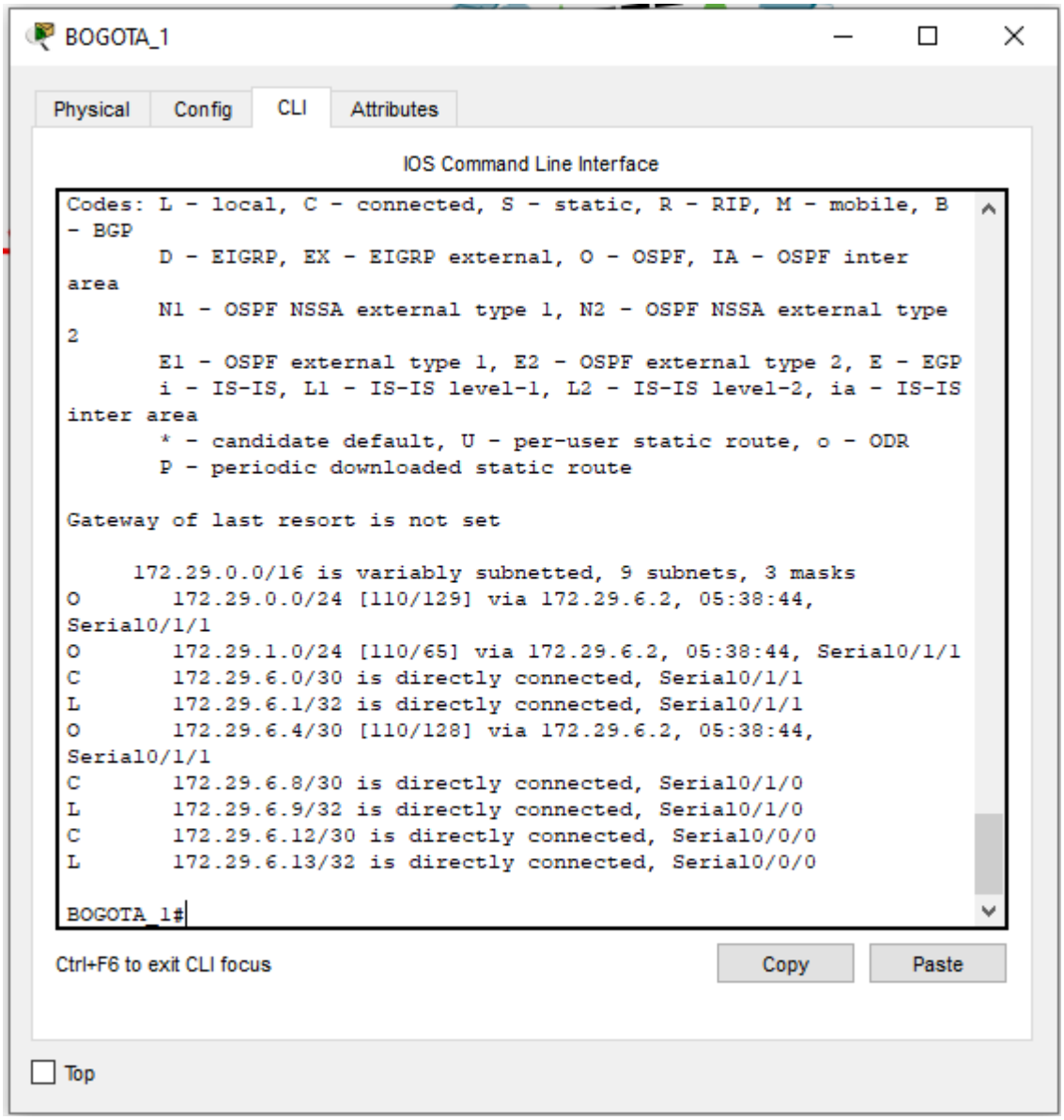


Ilustración 22. Rutas IP, Bogotá_5

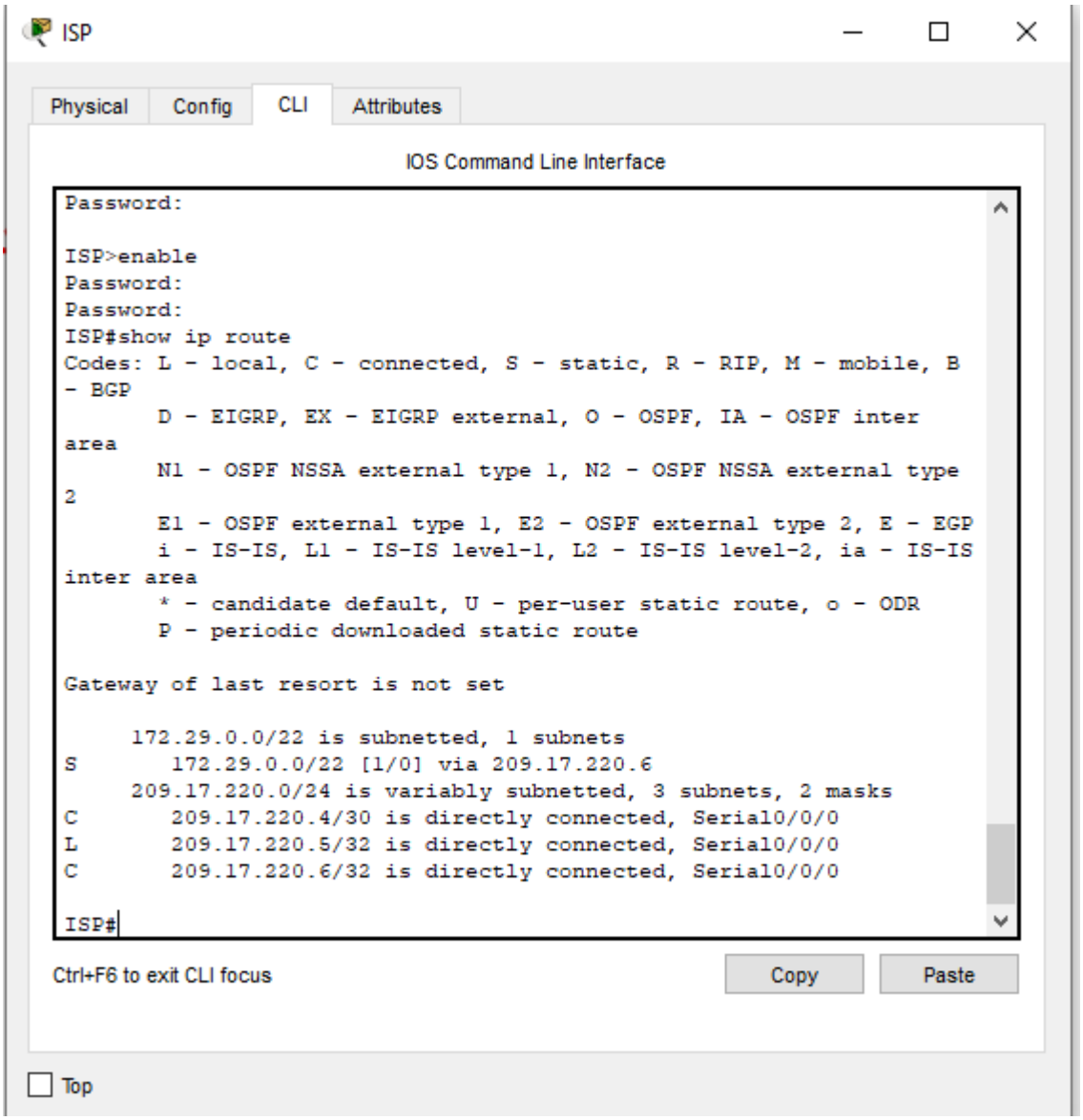


Ilustración 23. Rutas ISP

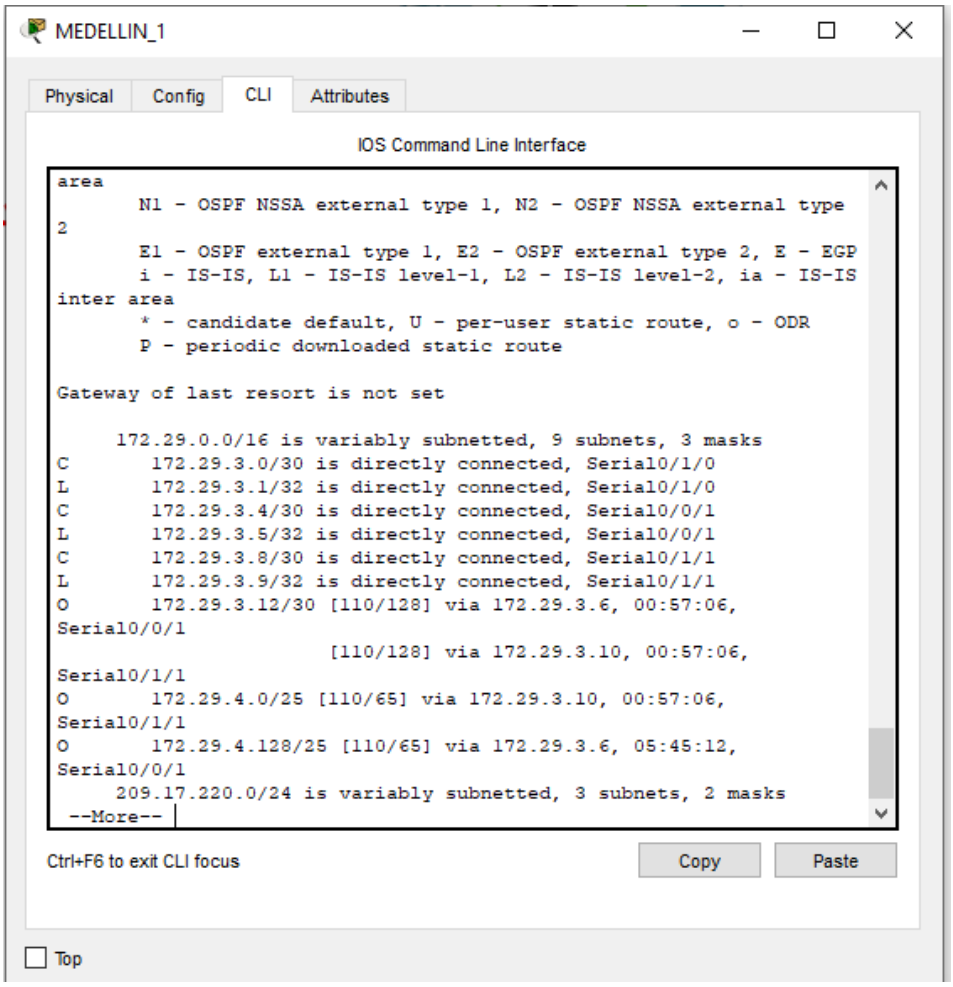


Ilustración 24. Rutas IP, Medellin_1

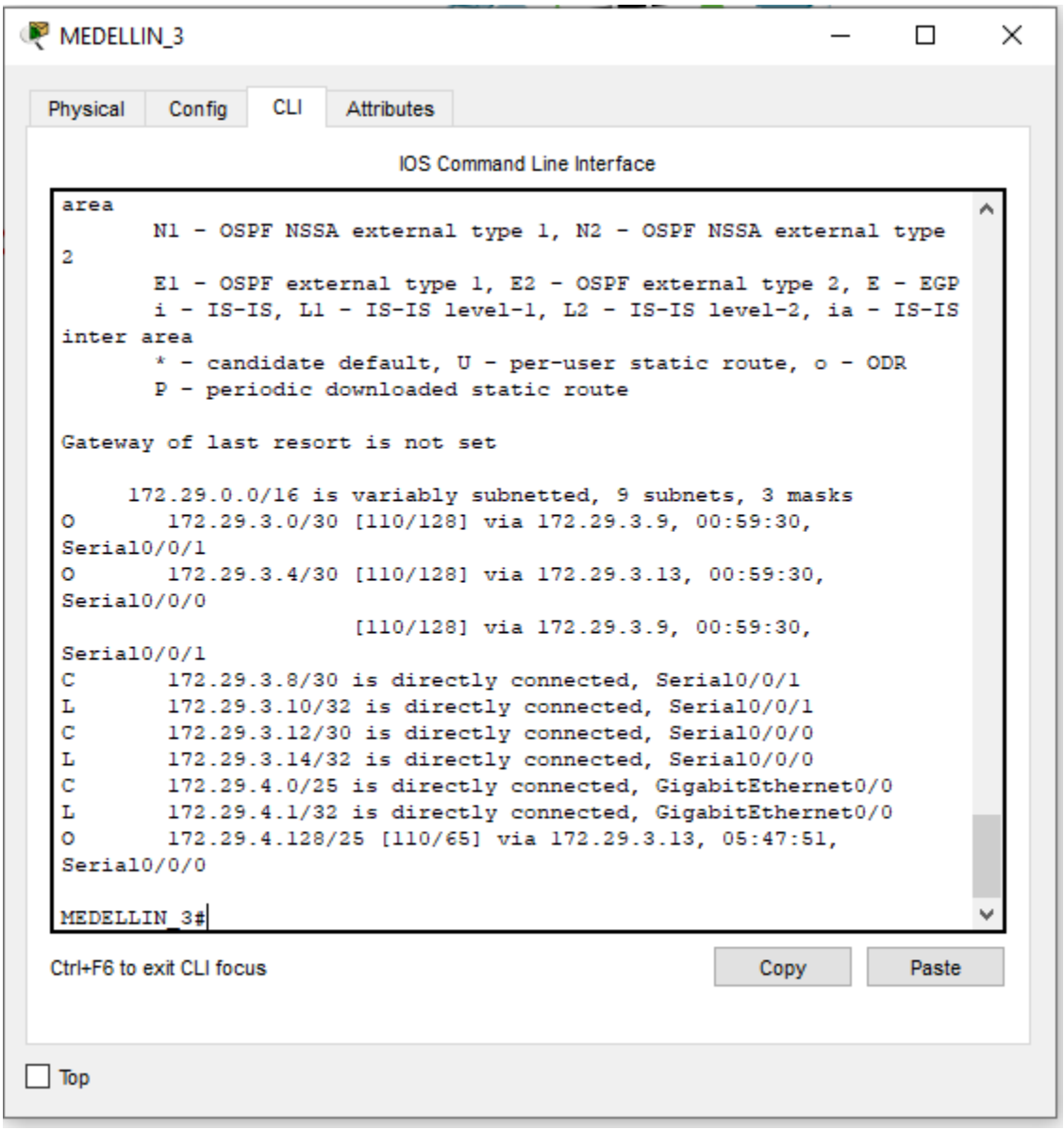


Ilustración 266. Rutas IP, Medellin_3

Como se puede observar en las graficas anteriores como evidencia, se aprecian las rutas aplicadas con OSPF en las cuales dentro de la tabla de enrutamiento se ven con la sigla de (O).

Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

ROUTER	**INTERFAZ**
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

En este protocolo de enrutamiento a diferencia del protocolo de enrutamiento RIP versión 2, no se deshabilita la propagación del protocolo como se aplica en el rip como el comando no auto-summary.

Parte 4: Verificación del protocolo OSPF.

a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.
b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Las conexiones que se configuran con el passive-interface son las interfaces que conectan los diferentes equipos sobre una LAN, en este caso con las interfaces g0/0 que están en los routers BOGOTA_2 y 3 y MEDELLIN_2 y 3, las cuales más adelante permiten generar un DHCP que permite a los equipos o host que se encuentren sobre esa red recibir una dirección ip conforme a la cuidad donde están configurados con su respectiva mascara de subred.

En este caso para los router se hace lo siguiente

- Config term
- Router OSPF 10
- Passive-interface g/0/0
- Exit

De esta manera se configura, se aclara que en cada uno de los routers que propagan o tienen conectadas redes LAN, se utilizó la interfaz g/0/0.

Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Iniciamos configurando en el ROUTER intermediario el encapsulamiento sobre los routers que se encuentran en cada uno de sus extremos y los cuales se comunican a través de sus interfaces seriales.

PAP	ISP#config ter ISP(config)#username MEDELLIN1 password system ISP(config)#interface serial 0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password system ISP(config-if)#exit
CHAP	ISP(config-if)#exit ISP(config)#username BOGOTA1 password system

	ISP(config)#interface serial 0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap ISP(config-if)#exit ISP(config)#
Ahora se procede a configurar el encapsulamiento PAP en el router MEDELLIN_1	MEDELLIN_1#config term MEDELLIN_1(config)#interface serial 0/1/1 MEDELLIN_1(config-if)#encapsulation ppp MEDELLIN_1(config-if)#ppp authentication pap MEDELLIN_1(config-if)#ppp pap sent-username MEDELLIN1 password system MEDELLIN_1(config-if)#
Ahora se procede a configurar el encapsulamiento CHAP en el router MEDELLIN_1	BOGOTA_1#config term BOGOTA_1(config)#username ISP password system BOGOTA_1(config)#interface serial 0/0/1 BOGOTA_1(config-if)#encapsulation ppp BOGOTA_1(config-if)#ppp authentication chap BOGOTA_1(config-if)#

Parte 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

Los NAT se aplican a los enrutadores que están a los extremos del ISP, en este caso MEDELLIN_1 y BOGOTA_1, de esta manera se programan las interfaces para la traducción de direcciones a nivel de	MEDELLIN_1#config t MEDELLIN_1(config)#ip nat inside source list 1 interface s0/1/1 overload MEDELLIN_1(config)#access-list 1 permit 172.29.4.0 0.0.3.255 MEDELLIN_1(config)#int s0/1/1

entrada o salida (NAT inside, NAT outside).	MEDELLIN_1(config-if)#ip nat outside MEDELLIN_1(config-if)#int s0/0/0 MEDELLIN_1(config-if)#ip nat inside MEDELLIN_1(config-if)#int s0/1/0 MEDELLIN_1(config-if)#ip nat inside MEDELLIN_1(config-if)#int s0/0/1 MEDELLIN_1(config-if)#ip nat inside MEDELLIN_1(config-if)#exit MEDELLIN_1(config)#
	BOGOTA_1#config term BOGOTA_1(config)#ip nat inside source list 1 interface s0/0/1 overload BOGOTA_1(config)#access-list 1 permit 172.29.0.0 0.0.3.255 BOGOTA_1(config)#interface s0/0/1 BOGOTA_1(config-if)#ip nat outside BOGOTA_1(config-if)#interface s0/1/0 BOGOTA_1(config-if)#ip nat inside BOGOTA_1(config-if)#interface s0/0/0 BOGOTA_1(config-if)#ip nat inside BOGOTA_1(config-if)#interface s0/1/1 BOGOTA_1(config-if)#ip nat inside BOGOTA_1(config-if)#exit BOGOTA_1(config)#

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

```
MEDELLIN_1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.1:6    172.29.4.6:6       209.17.220.2:6     209.17.220.2:6
icmp 209.17.220.1:7    172.29.4.6:7       209.17.220.2:7     209.17.220.2:7
icmp 209.17.220.1:8    172.29.4.6:8       209.17.220.2:8     209.17.220.2:8
icmp 209.17.220.1:9    172.29.4.6:9       209.17.220.2:9     209.17.220.2:9
```

Ilustración 27. NAT en el router Medellín1

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

```
BOGOTA_1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.1:6    172.29.4.6:6       209.17.220.2:6     209.17.220.2:6
icmp 209.17.220.1:7    172.29.4.6:7       209.17.220.2:7     209.17.220.2:7
icmp 209.17.220.1:8    172.29.4.6:8       209.17.220.2:8     209.17.220.2:8
icmp 209.17.220.1:9    172.29.4.6:9       209.17.220.2:9     209.17.220.2:9
```

Ilustración 28. NAT en el router Bogotá 1

Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Se define en la topología de los routers del área de MEDELLIN que el enrutador MEDELLIN_2 se comportara como el servidor DHCP para las redes propias en su conexión, como también para el enrutador de MEDELLIN_3.	Procedemos a configurar el router. MEDELLIN_2#config term Reservaremos direccionamiento IP para que no sea asignado automaticamente a los equipos que se conecten a la red. MEDELLIN_2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 MEDELLIN_2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
Ahora se configurará el Pool de Direcciones en la cual por la red que se nombre y la máscara de subred que se asigne, el DHCP cuantas direcciones tiene capacidad de asignar.	MEDELLIN_2(config)#ip dhcp pool MEDELLIN_2 MEDELLIN_2(dhcp-config)#network 172.29.4.0 255.255.255.128 Ahora asignamos como puerta de enlace la direccion de la interfaz g0/0

	MEDELLIN_2(dhcp-config)#default-router 172.29.4.1 Se asigna los servidores DNS que se aplicaran a los equipos que se conecten a la red. MEDELLIN_2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN_2(dhcp-config)#exit
	Este mismo proceso se repite ahora para la LAN que esta sobre los equipos del router MEDELLIN_3, pero que se configuran en el router MEDELLIN_2 el cual sera quien asigne y controle el DHCP. MEDELLIN_2(config)#ip dhcp pool MEDELLIN_3 MEDELLIN_2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN_2(dhcp-config)#default-router 172.29.4.129 MEDELLIN_2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN_2(dhcp-config)#exit
Ahora sobre el router de MEDELLIN_3 se configurara como un equipo de peticiones DHCP, a traves de la interfaz g0/0 la cual sera la salida y entrada de conexiones LAN.	MEDELLIN_3(config)#int g0/0 MEDELLIN_3(config-if)#ip helper-address 172.29.6.5 MEDELLIN_3(config-if)#exit
La configuración anteriormente aplicada en los routers de MEDELLIN, será aplicado a los routers de BOGOTA de la misma manera, identificando que el router que funcionara como servidor DHCP, el esclavo y la interfaz de petición de direcciones IP.	BOGOTA_2#config term BOGOTA_2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5 BOGOTA_2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 BOGOTA_2(config)#ip dhcp pool BOGOTA_2 BOGOTA_2(dhcp-config)#network 172.29.0.0 255.255.255.0 BOGOTA_2(dhcp-config)#default-router 172.29.0.1 BOGOTA_2(dhcp-config)#dns-server 8.8.8.8 BOGOTA_2(dhcp-config)#exit

	BOGOTA_2(config)#ip dhcp pool BOGOTA_3 BOGOTA_2(dhcp-config)#network 172.29.1.0 255.255.255.0 BOGOTA_2(dhcp-config)#default-router 172.29.1.1 BOGOTA_2(dhcp-config)#dns-server 8.8.8.8 BOGOTA_2(dhcp-config)#exit BOGOTA_3(config)#int g0/0 BOGOTA_3(config-if)#ip helper-address 172.29.3.13 BOGOTA_3(config-if)#

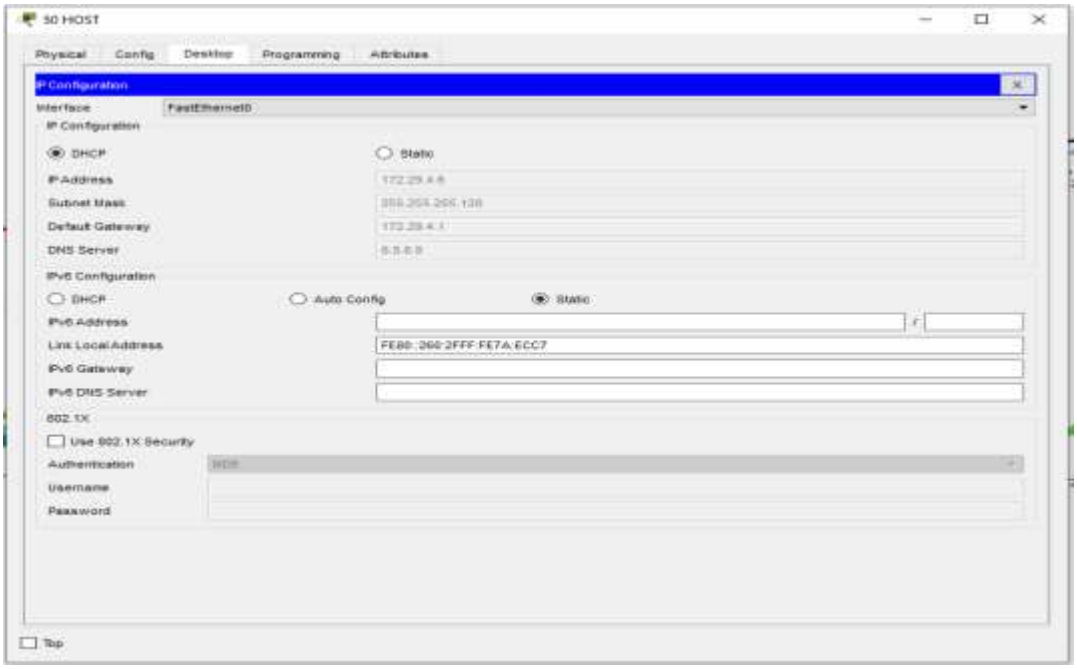


Ilustración 29. DHCP_IP50 Host

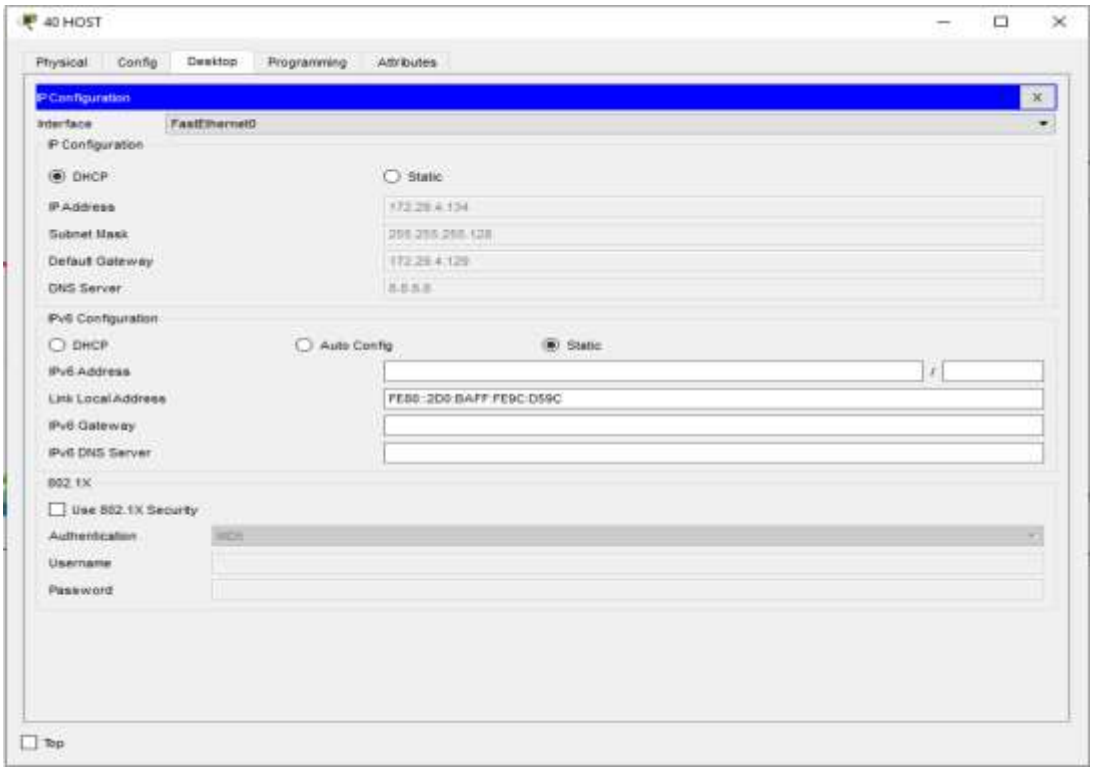


Ilustración 30. DHCP_IP40 Host

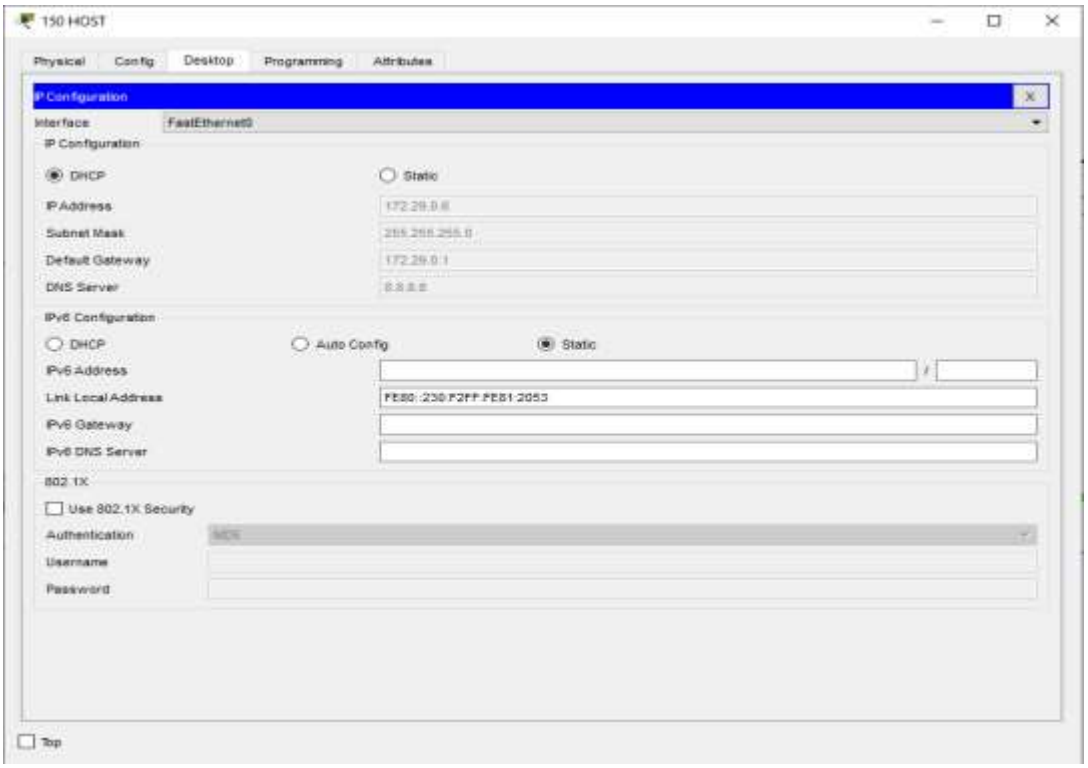


Ilustración 31. DHCP_IP 150 Host

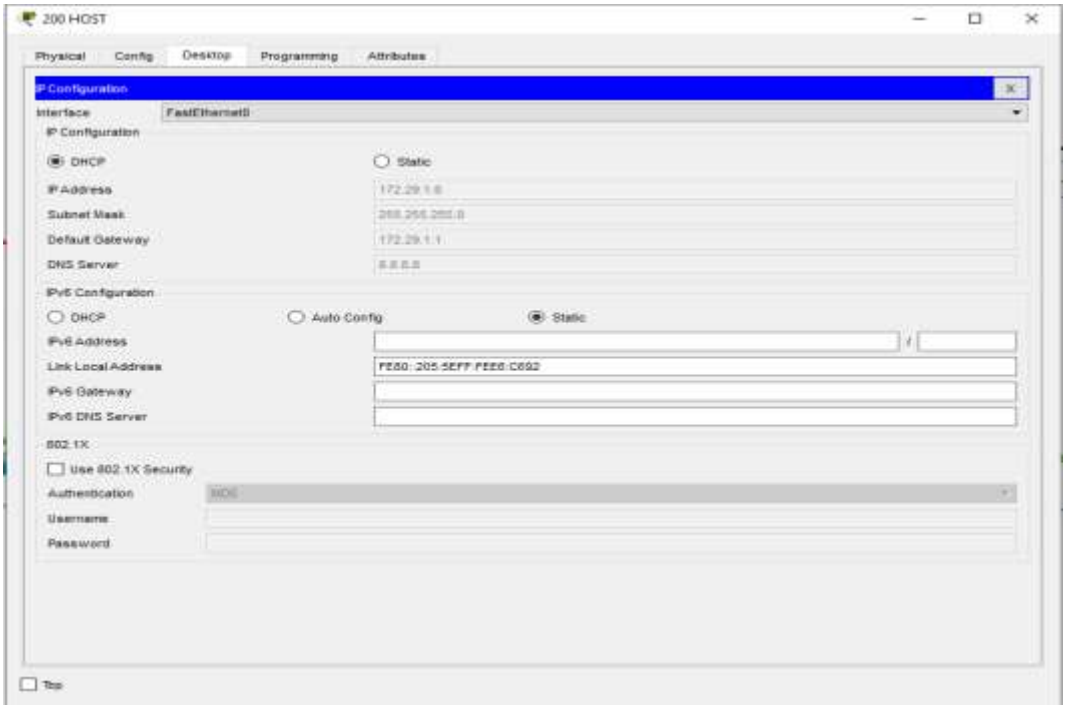


Ilustración 32. DHCP_IP200 Host

CONCLUSIONES

El desarrollo de este trabajo permite poner a prueba los conocimientos adquiridos enfrentando a dos escenarios diferentes donde se puede configurar y modificar las configuraciones entre dispositivos, se realiza encapsulamiento y proporciona seguridad con el objetivo de mitigar los ataques de forma remota.

Al realizar la configuración de NAT se verifica la conectividad de cada uno de los puertos asignados y las estaciones de trabajo brindando así la seguridad de haber cumplido con los requerimientos de cada uno de los problemas planteados.

Sobre el escenario 1 podemos concluir que el uso y la implementación de los comandos fue el adecuado y que como resultado de esto las pruebas fueron efectivas, se evidencia comunicación entre todos los dispositivos y con la implementación de NAT observamos que no es posible validar la traducción por parte del protocolo ya que todos los equipos esta conectados a una misma LAN.

En el escenario 2 se establecieron de igual manera los protocolos pero se presentaron problemas de comunicación entre las ciudades con la aplicación de NAT, por lo que fue necesario realizar verificación de los protocolos y las configuración en más de una ocasión para poder confirmar la correcta configuración de los protocolos y tener la correcta conectividad, también se utilizó el protocolo de enrutamiento OSPF el cual mejora algunas limitaciones de RIP ofrece escalabilidad en redes mayores y converge más rápido.

BIBLIOGRAFÍA

CICO NETWORKING ACADEMY – CCNA 1
https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#10.1.1

CICO NETWORKING ACADEMY – CCNA 2
https://1314297.netacad.com/courses/1003497/pages/iniciar-el-capitulo-9?module_item_id=66668563

Cisco CCNA – configuración DHCP
https://1314297.netacad.com/courses/1003497/pages/practica-de-terminos-y-conceptos-del-capitulo-8

Como configurar switch
https://1314297.netacad.com/courses/1003497/pages/iniciar-el-capitulo-5?module_item_id=66668546

Vlan
https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6.0.1.1