EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JUAN MANUEL ORTIZ LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

BOGOTA D.C.

2018

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JUAN MANUEL ORTIZ LEON

Monografía para optar el título de ingeniero electrónico.

Tutor

Efrain Alejandro Perez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

BOGOTA D.C.

2018

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Bogotá D.C, 28 de mayo de 2018

DEDICATORIA

Gracias Dios por darme la posibilidad de revivir este sueño que pensé había muerto, a mi familia por su apoyo para poder llevar a buen término mi proceso de educación.

Dedico este trabajo con amor y cariño:
A mis padres CARMEN Y LUIS y mis hermanos que desde el inicio de mis estudios dieron todos sus esfuerzos morales, por su comprensión, entrega y animo en los momento más difíciles.

Los quiero demasiado a cada uno de ellos.

AGRADECIMIENTOS

Deseo expresar mi agradecimiento al director de este diplomado de profundización Ing. JUAN CARLOS VESGA por el acompañamiento que ha brindado en el transcurso del curso de profundización Cisco.

Gracias al tutor Ing. EFRAIN ALEJANDRO PEREZ que a lo largo de este curso me ayudo a progresar resolviendo dudas y enseñando todos sus conocimientos.

TABLA DE CONTENIDO

LISTAS DE TABLAS

LISTA DE FIGURAS

RESUMEN

Comprender el papel tan importante que desempeñan las telecomunicaciones en el desarrollo del mundo actual, es por esto que entender como es el funcionamiento a través de las redes de información es visto por la universidad nacional abierta y a distancia UNAD como base fundamental en desarrollo académico de los próximos ingenieros electrónicos, es por esto que en convenio con CISCO Networking Academy, han puesto a disposición el diplomado: “CISCO diseño e implementación de redes LAN-WAN”, donde el estudiante dispone de dos módulos, el primero bajo el título de CCNA1: Switching y routing: Introducción a redes, se enfoca en brindar la capacidad al estudiante de construir redes LAN simples, realizar configuraciones básicas para enrutadores e interruptores, e implementar esquemas de direccionamiento IP, el segundo CCNA2: Routing y switching: Principios básicos de routing y switching, ese encamina en presentar herramientas para configurar y solucionar problemas de enrutadores y cambia y resuelve problemas comunes con RIPv1, RIPv2, área única y área múltiple OSPF, LAN virtuales y enrutamiento entre VLAN en ambas redes IPv4 e IPv6, es por esto que como complemento y evaluación se dispone de la prueba de habilidades prácticas, la cual se desarrolla en este documento y que pretende demostrar al estudiante las habilidades desarrolladas.

JUSTIFICACIÓN

La Universidad Nacional Abierta y a Distancia UNAD, ofrece diferentes opciones de grado donde se encuentra la realización del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) que permite al estudiante la profundización especifica en el tema de redes de comunicaciones que no solamente es visto como uno de los requisitos para optar por el título profesional sino que además tiene un atractivo adicional como lo es estar a la vanguardia en el mundo de las telecomunicaciones, es por esto que este diplomado presenta la aplicabilidad y vigencia en el área de la electrónica y las telecomunicaciones que se necesita para enfrentar el campo laboral.

INTRODUCCIÓN

Sin lugar a duda la importancia de las telecomunicaciones en nuestro tiempo en donde vemos con gran interés y sombro la expansión que se está logrando en este ámbito, además de la mano a una empresa como Cisco Systems que es el líder mundial en redes para Internet, se ha permitido avanzar aún más en el área de las telecomunicaciones, es por esto que en asocio con la Universidad Nacional Abierta y a Distancia UNAD, se pretende dar una herramienta adicional en el ámbito profesional a los estudiantes que obtén por la realización del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, 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.

En este documento se desarrolla la solución un escenario propuesto, que condesa los conceptos teóricos y prácticos de los 2 módulos comprendidos en CCNA1 y CCNA2 los cuales comprenden Introducción a redes y Principios básicos de routing y switching, es indispensable el uso de la herramienta Cisco Packet Tracer Student para logra el desarrollo y comprensión del prueba.

OBJETIVOS

Objetivo General

Resolver la prueba de habilidades propuesta en el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), aplicando los conceptos básicos aprendidos en los módulos CCNA1 FUNDAMENTOS DE NETWORKING y CCNA2 PRINCIPIOS DE ENRUTAMIENTO ofrecidos por la Cisco Networking Academy.

Objetivos Específicos

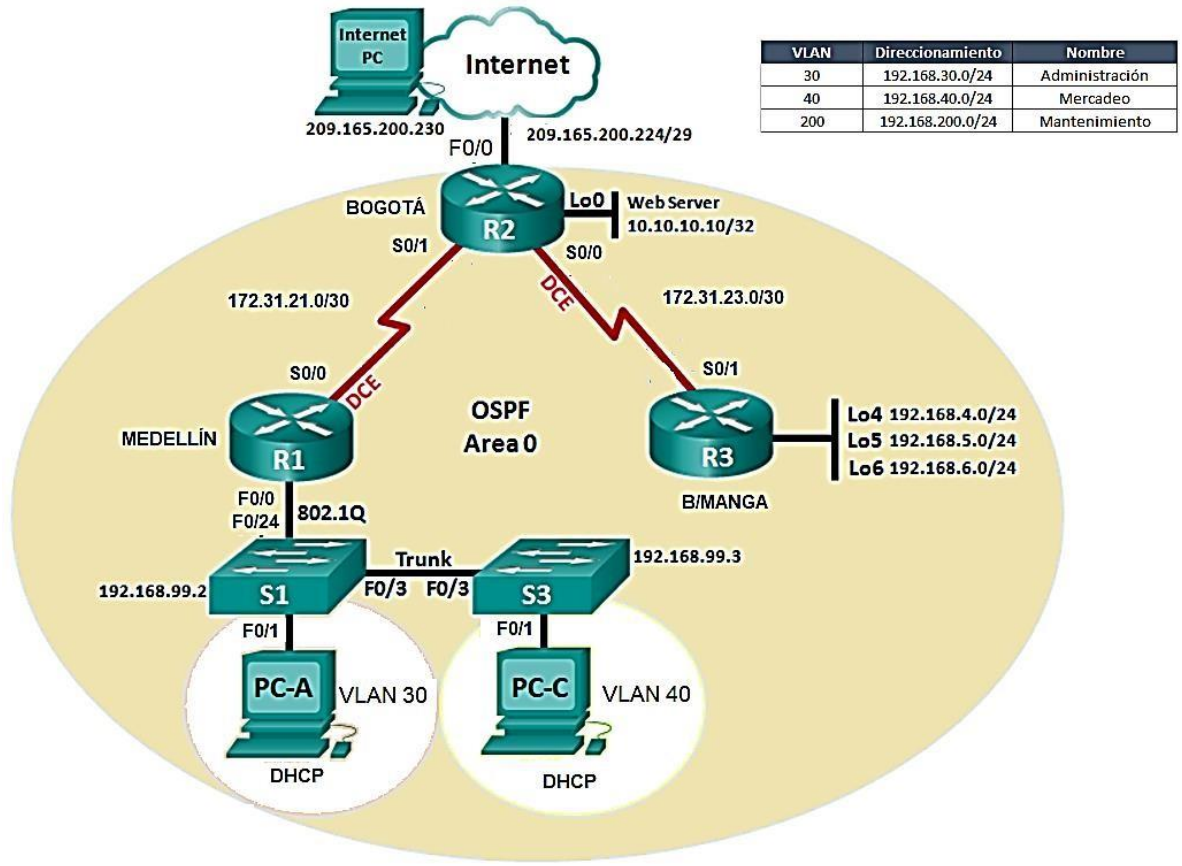
- Desarrollo de la actividad por medio del uso de la herramienta Cisco Packet Tracer.
- Elegir los dispositivos requeridos para la topología de la red.
- Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.
- Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida
- Configurar el protocolo de enrutamiento OSPFv2 bajo los criterios establecidos.
- Configurar cada dispositivo, según especificaciones exigidas.
- Comprobar la conectividad de los dispositivos de la red.

DESCRIPCIÓN DEL ESCENARIO PROPUESTO PARA LA PRUEBA DE HABILIDADES

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

Topología de red

Figura 1.Topología de red



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Fuente: Guía PRUEBA DE HABILIDADES CCNA. Recuperado de: https://1drv.ms/b/s!AmIJYei-NT1Inld9q3plaoaVvK5f

LINEAMIENTOS

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

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

OSPFv2 area 0

Tabla 1. Configuración OSPV area 0

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

Fuente: Guía PRUEBA DE HABILIDADES CCNA. Recuperado de: https://1drv.ms/b/s!AmIJYei-NT1Inld9q3plaoaVvK5f

Verificar información de OSPF

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

3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

4. En el Switch 3 deshabilitar DNS lookup

5. Asignar direcciones IP a los Switches acorde a los lineamientos.

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

7. Implementar DHCP y NAT para IPv4

8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Tabla 2. Configuración DHCP pool para VLAN 30 y 40

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Fuente: Guía PRUEBA DE HABILIDADES CCNA. Recuperado de: https://1drv.ms/b/s!AmIJYei-NT1Inld9q3plaoaVvK5f

10. Configurar NAT en R2 para permitir que los host puedan salir a internet

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

DESARROLLO

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

Recursos necesarios:

• Cisco Packet Tracer Student v6.1

• 3 Routers (Cisco 2621XM+Modulo interfaz WAN serial 2-Port (WIC-2T))

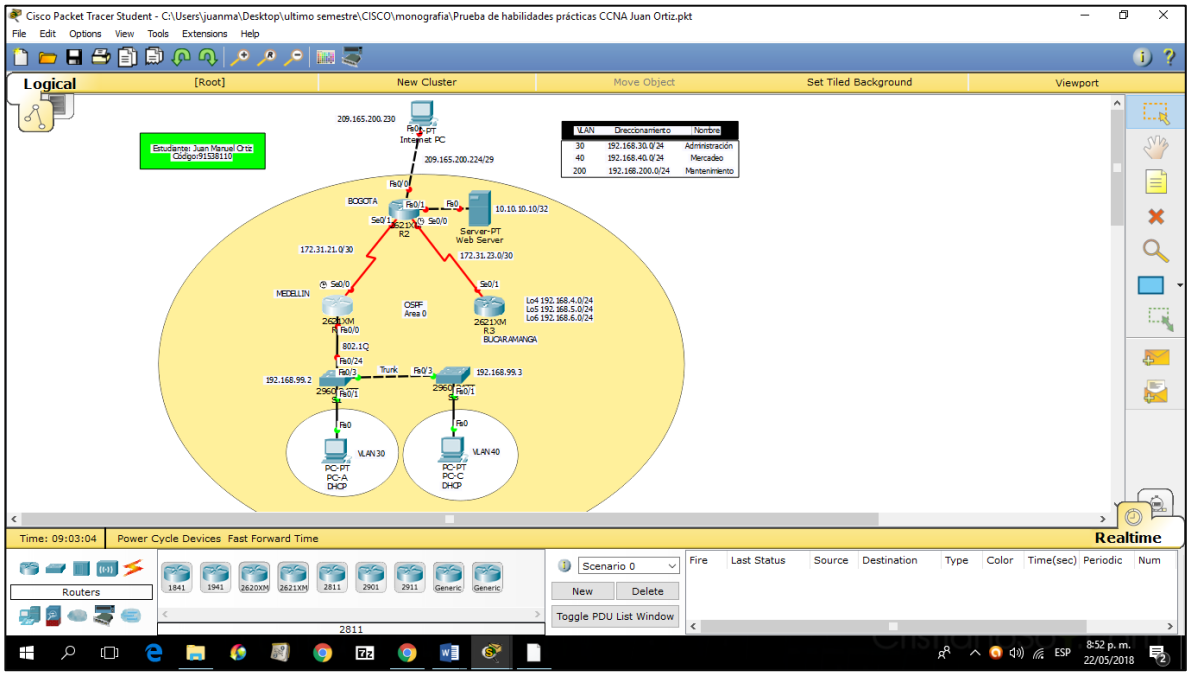
• 2 Switches (Cisco 2960 con Cisco IOS Release 15.0 (2) lanbasek9 image o similar)

• 3 PC (Windows 7, Vista o XP con programa de emulación de terminal, como Tera Term)

• Cable de consola para configurar los dispositivos Cisco IOS a través de los puertos de la consola

• Ethernet y cables serie como se muestra en la topología

Figura 2. Configuración del direccionamiento IP acorde con la topología de red.



Fuente. Elaboración propia.

Parte 1. Inicializar dispositivos

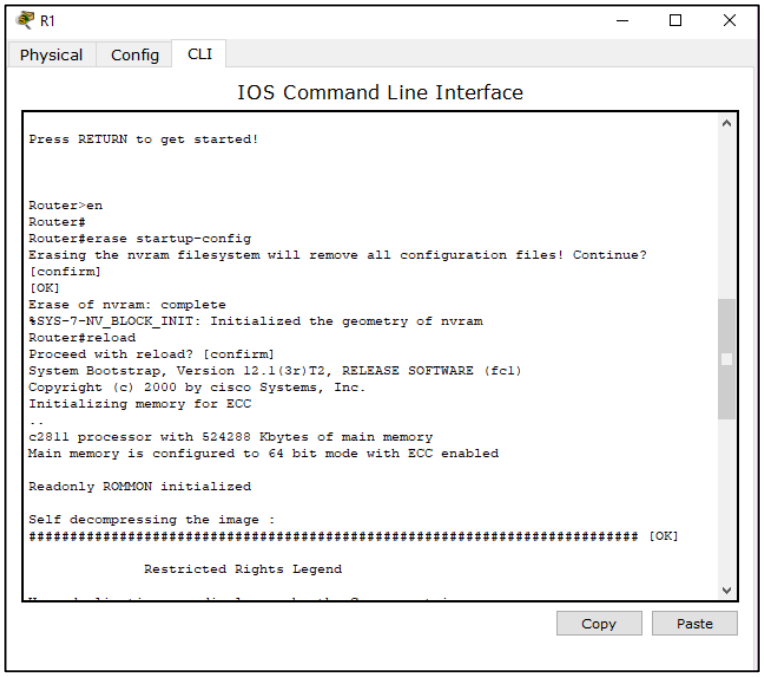
Lo primero que se debe realizar es el borrado de las configuraciones de inicio luego hay que reiniciar los dispositivos, así como borrar el startup-config en todos los Switches y borrar las bases de datos de las VLANS.

Paso 1. Borrar las configuraciones de inicio y reiniciar los routers y switches

Uso de comandos

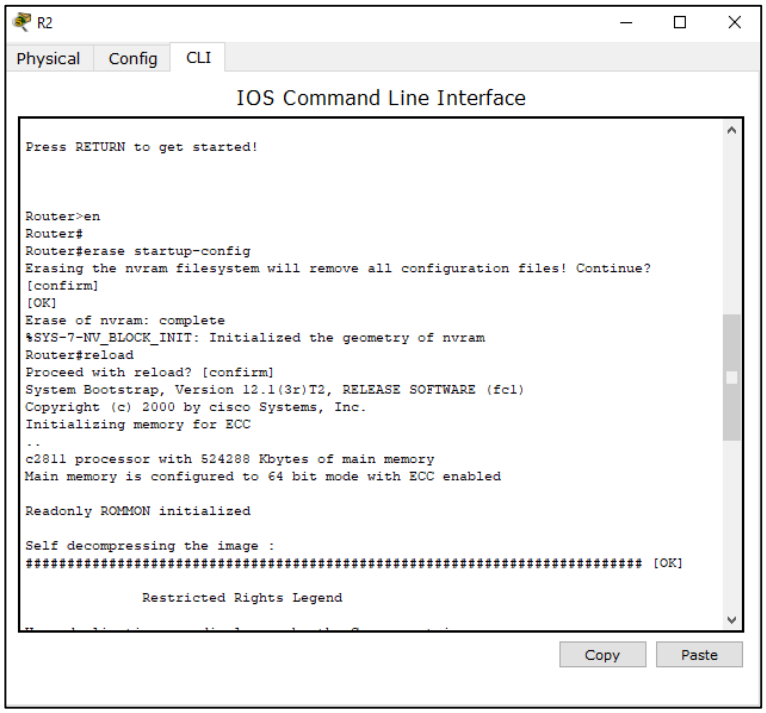
- ✓ `erase startup-config`
- ✓ `reload`

Figura 3. Borrado de configuraciones y reinicio de router R1.



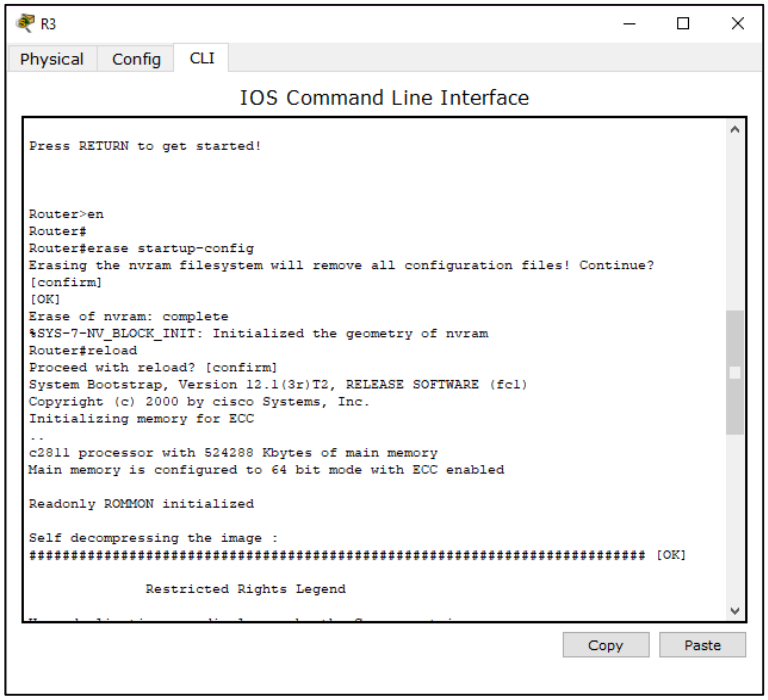
Fuente. Elaboración propia.

Figura 4. Borrado de configuraciones y reinicio de router R2.



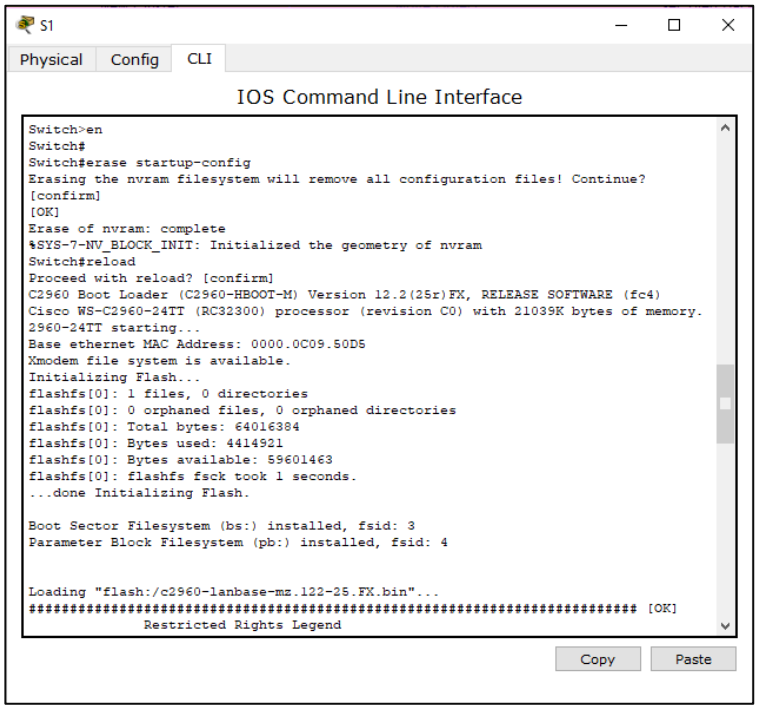
Fuente. Elaboración propia.

Figura 5. Borrado de configuraciones y reinicio de router R1.



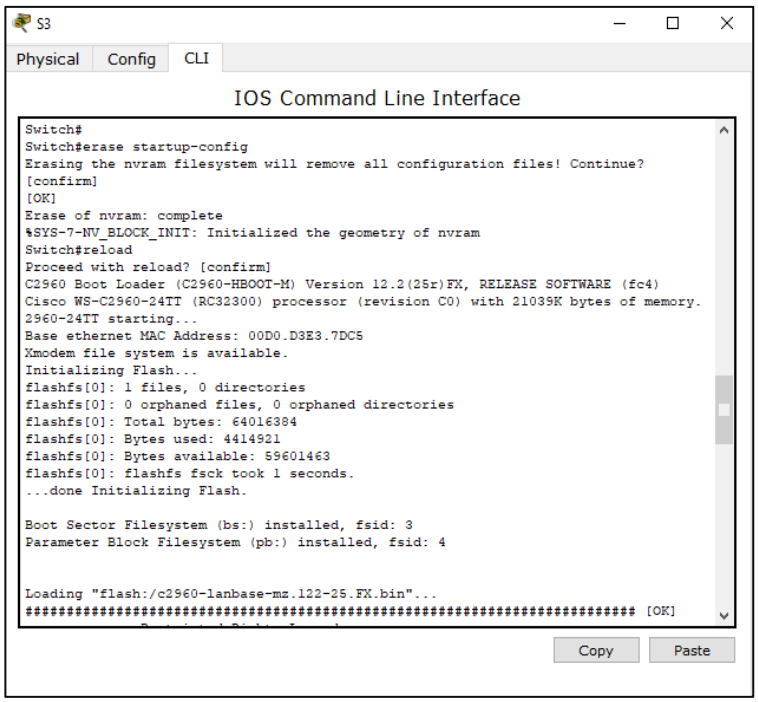
Fuente. Elaboración propia.

Figura 6. Borrado de configuraciones y reinicio de switch S1.



Fuente. Elaboración propia.

Figura 7. Borrado de configuraciones y reinicio de switch S3.



Fuente. Elaboración propia.

Parte 2. Establecer la configuración básica del dispositivo

Paso 1. Configurar la PC de Internet.

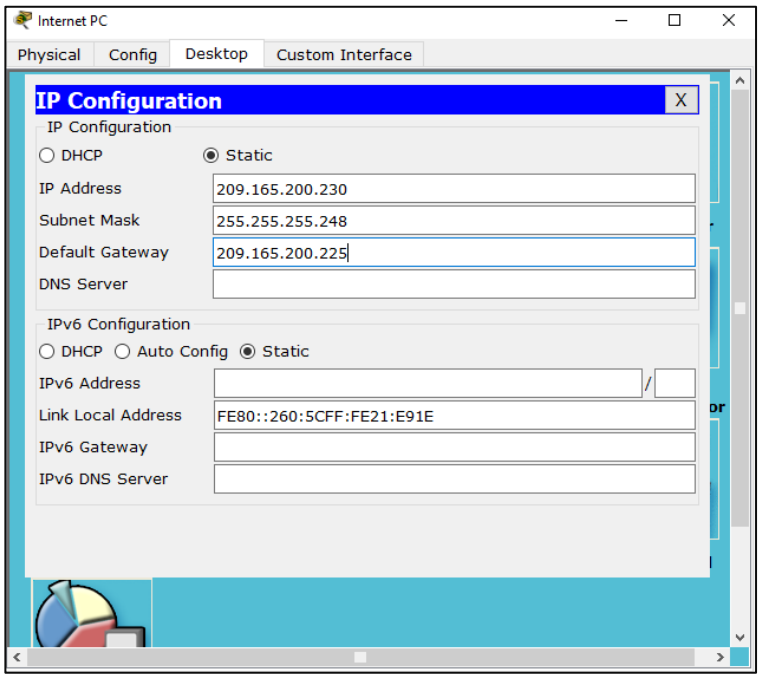
Las tareas de configuración para la PC con Internet incluyen lo siguiente (se consulta Topología para obtener información sobre la dirección IP):

Tabla 3. Configuración básica Internet PC.

Elemento de configuración	Especificación
IP Address	209.165.200.230
Subnet Mask	255.255.255.248
Default Gateway	209.165.200.225

Fuente. Elaboración propia.

Figura 8. Configuración básica Internet PC.



Fuente. Elaboración propia.

Paso 2. Configurar R1.

Las tareas de configuración para R1 incluyen lo siguiente:

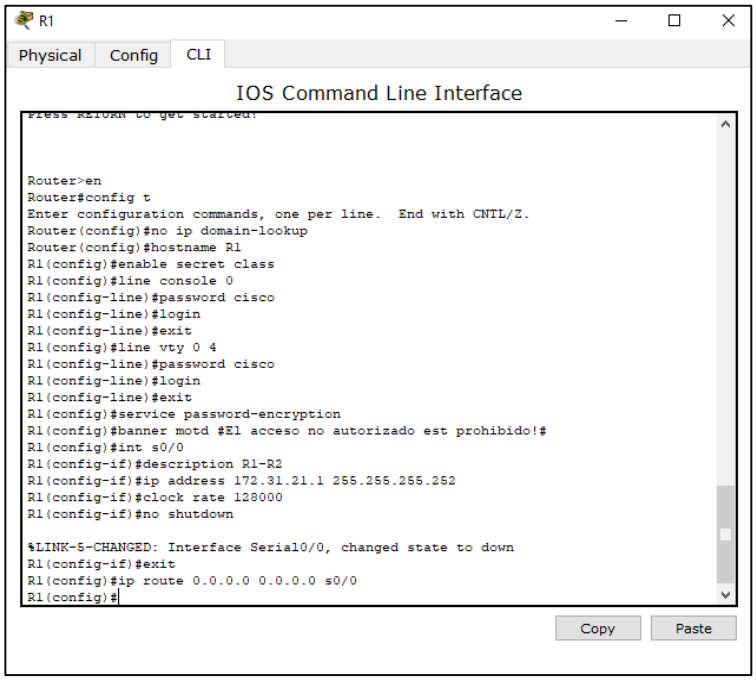
Tabla 4. Configuración básica para R1.

Elemento de configuración	Especificación
Desactivar la búsqueda de DNS	no ip domain-lookup
nombre del router	R1
Contraseña encriptada exec privilegiado	class
contraseña de acceso a la consola	cisco
contraseña de acceso telnet	cisco
Cifrar las contraseñas de texto	
banner MOTD	El acceso no autorizado está prohibido!
Interfaz S0/0	Establecer la descripción: description R1-R2 Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 172.31.21.1 255.255.255.252 Ajuste la velocidad del reloj de 128000 Interfaz Activar
Ruta por defecto	Configurar una ruta predeterminada de salida S0/0.

Fuente. Elaboración propia.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #El acceso no autorizado está prohibido!#
R1(config)#int s0/0
R1(config-if)#description R1-R2
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0
```

Figura 9. Configuración básica para R1.



Fuente. Elaboración propia.

Paso 3. Configurar R2.

Las tareas de configuración para R2 incluyen lo siguiente:

Tabla 5. Configuración básica para R2.

Elemento de configuración	Especificación
Desactivar la búsqueda de DNS	no ip domain-lookup
nombre del router	R2
Contraseña encriptada exec privilegiado	class
contraseña de acceso a la consola	cisco
contraseña de acceso telnet	cisco
Cifrar las contraseñas de texto	
Habilitar servidor HTTP	
banner MOTD	El acceso no autorizado está prohibido!
Interfaz S0/1	Establecer la descripción description R2-R1 Ajustar la dirección IPv4 de Capa 3. Usar la siguiente dirección disponible en la subred. 172.31.21.2 255.255.255.252 Interfaz Activar
Interfaz S0/0	Establecer la descripción description R2-R3 Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 172.31.23.1 255.255.255.252 Ajuste la velocidad del reloj de 128000 Interfaz Activar
Interfaz F0/0 (Internet simulado)	Establecer la descripción description R2-Internet Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 209.165.200.225 255.255.255.248 Interfaz Activar
Interfaz loopback F0/1 (simulado servidor Web)	Establecer la descripción. description R2-Web Server Ajustar la dirección IPv4 de Capa 3. 10.10.10.1 255.255.255.0
Ruta por defecto	Configurar una ruta predeterminada F0/0.

Fuente. Elaboración propia.

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
```

```
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #El acceso no autorizado está prohibido!#
R2(config)#ip http sever
R2(config)#int s0/1
R2(config-if)#description R2-R1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown

R2(config)#int s0/0
R2(config-if)#description R2-R3
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

R2(config)#int f0/0
R2(config-if)#description R2-Internet
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown

R2(config)#int f0/1
R2(config-if)#description R2-Web Server
R2(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 f0/0
R2(config)#
```

Figura 10. Configuración básica para R2.

Fuente. Elaboración propia.

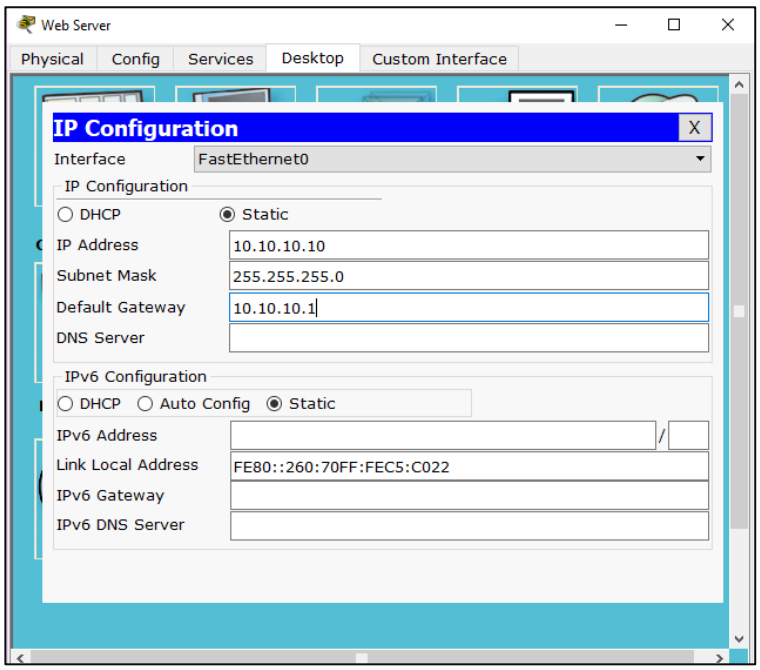
Paso 4. Configurar Web Server.

Tabla 6. Configuración básica Web Server.

Elemento de configuración	Especificación
IP Address	10.10.10.10
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1

Fuente. Elaboración propia.

Figura 11. Configuración básica Web Server.



Fuente. Elaboración propia.

Paso 5. Configurar R3.

Las tareas de configuración para R3 incluyen lo siguiente:

Tabla 7. Configuración básica R3.

Elemento de configuración	Especificación
Desactivar la búsqueda de DNS	no ip domain-lookup
nombre del router	R3
Contraseña encriptada exec privilegiado	class
contraseña de acceso a la consola	cisco
contraseña de acceso telnet	cisco
Cifrar las contraseñas de texto	
banner MOTD	El acceso no autorizado está prohibido!
Interfaz S0/1	Establecer la descripción description R3-R2 Ajustar la dirección IPv4 de Capa 3. Usar la siguiente dirección disponible en la subred. 172.31.23.2 255.255.255.252 Interfaz Activar
Loopback Interface 4	Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 192.168.4.1 255.255.255.0
Loopback Interface 5	Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 192.168.5.1 255.255.255.0
Loopback Interface 6	Ajustar la dirección IPv4 de Capa 3. Utilizar la primera dirección disponible en la subred. 192.168.6.1 255.255.255.0
Ruta por defecto	Configurar una ruta predeterminada S0/1. 0.0.0.0 0.0.0.0 s0/1

Fuente. Elaboración propia.

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

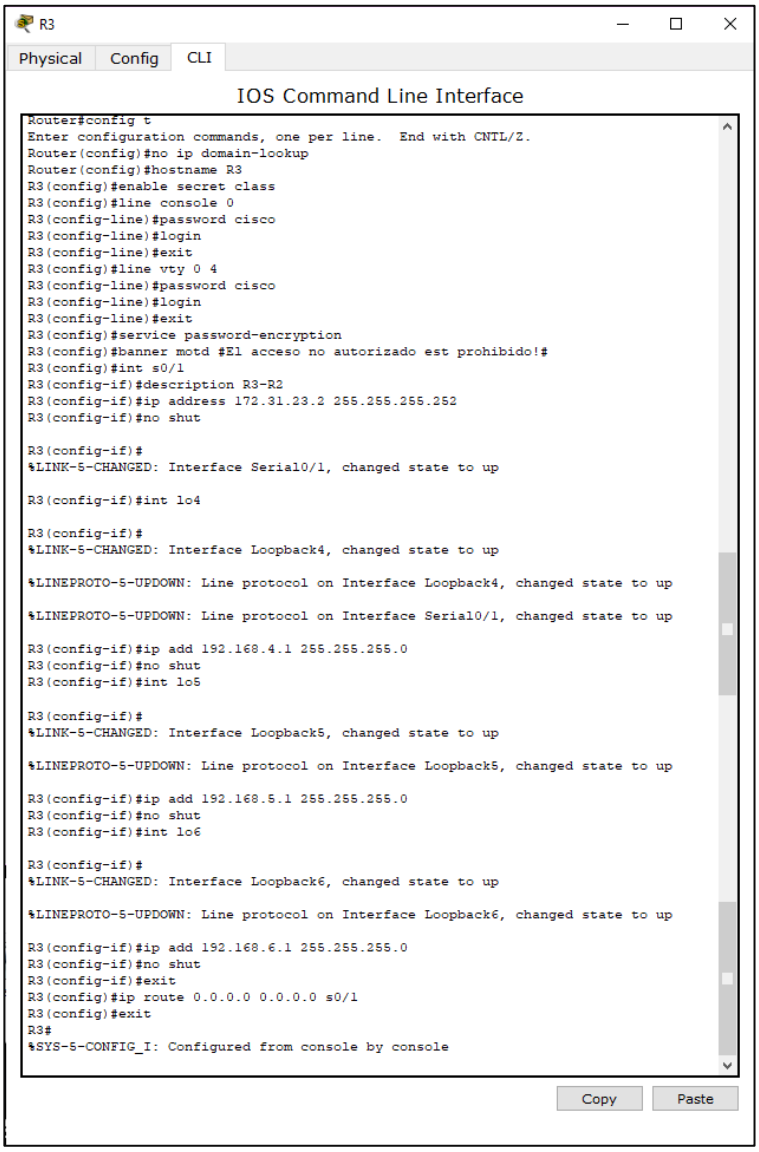
```
R3(config)#service password-encryption
R3(config)#banner motd #El acceso no autorizado está prohibido!#
R3(config)#int s0/1
R3(config-if)#description R3-R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shut

R3(config-if)#int lo4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#int lo5
R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#int lo6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1
R3(config)#exit
```

Figura 12. Configuración básica R3.



Fuente. Elaboración propia.

Paso 6. Configurar S1.

Las tareas de configuración para S1 incluyen lo siguiente:

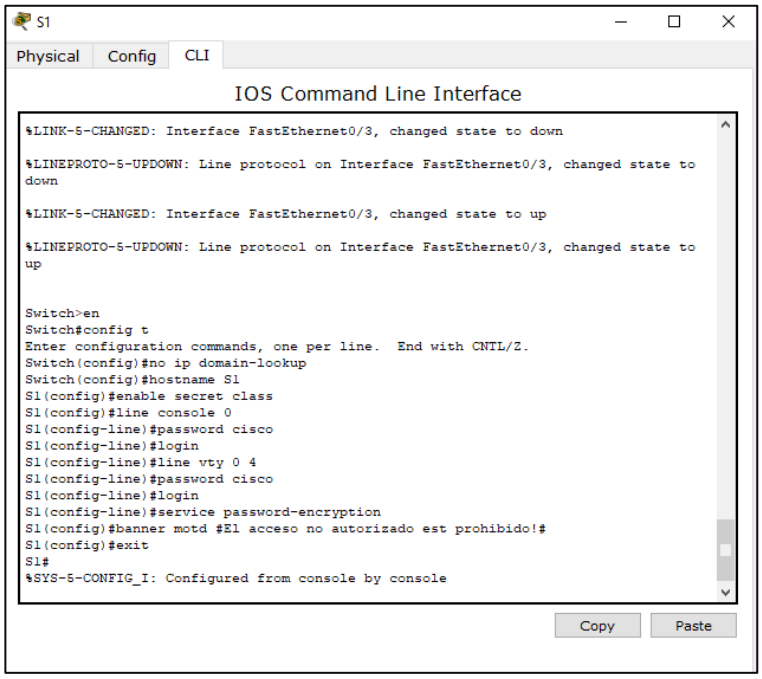
Tabla 8. Configuración básica S1.

Elemento de configuración	Especificación
Desactivar la búsqueda de DNS	no ip domain-lookup
nombre de conmutador	S1
Contraseña encriptada exec privilegiado	class
contraseña de acceso a la consola	cisco
contraseña de acceso telnet	cisco
Cifrar las contraseñas de texto	
banner MOTD	El acceso no autorizado está prohibido!

Fuente. Elaboración propia.

```
Switch>en
Switch#config t
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #El acceso no autorizado está prohibido!#
S1(config)#exit
```

Figura 13. Configuración básica S1.



Fuente. Elaboración propia.

Paso 7. Configurar S3.

Las tareas de configuración para S3 incluyen lo siguiente:

Tabla 9. Configuración básica S3.

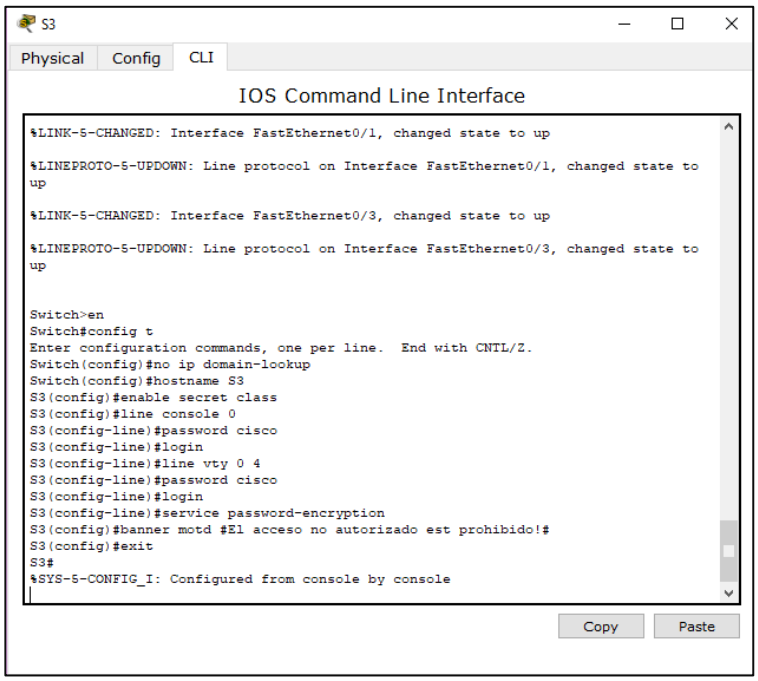
Elemento de configuración	Especificación
Desactivar la búsqueda de DNS	no ip domain-lookup
nombre de conmutador	S3
Contraseña encriptada exec privilegiado	class
contraseña de acceso a la consola	cisco
contraseña de acceso telnet	cisco
Cifrar las contraseñas de texto	
banner MOTD	El acceso no autorizado está prohibido!

Fuente. Elaboración propia.

```
Switch>en
Switch#config t
Switch(config)#no ip domain-lookup
```

```
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #El acceso no autorizado está prohibido!#
S3(config)#exit
```

Figura 14. Configuración básica S3.

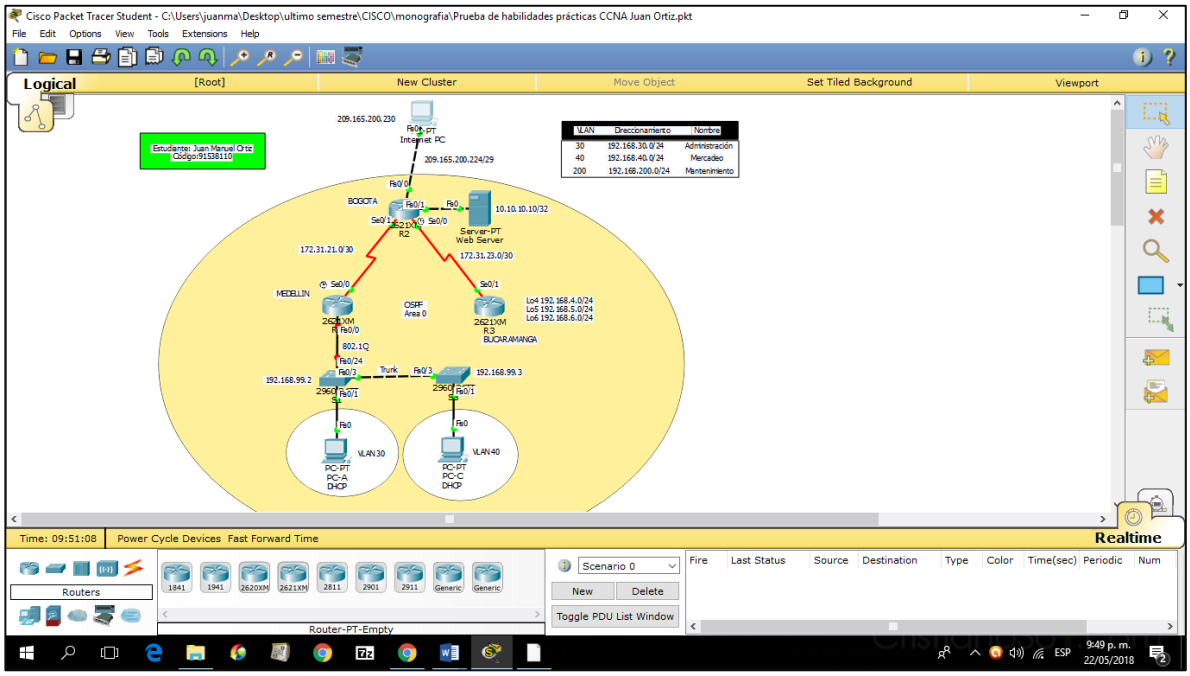


Fuente. Elaboración propia.

Paso 8. Verificar la conectividad de la red.

Después de la configuración de los dispositivos se observa en la simulación que todos los puntos de conexión se encuentran en color verde lo que indica su correcta comunicación pero se debe comprobar usando el comando ping.

Figura 15. Conectividad básica de la red.



Fuente. Elaboración propia.

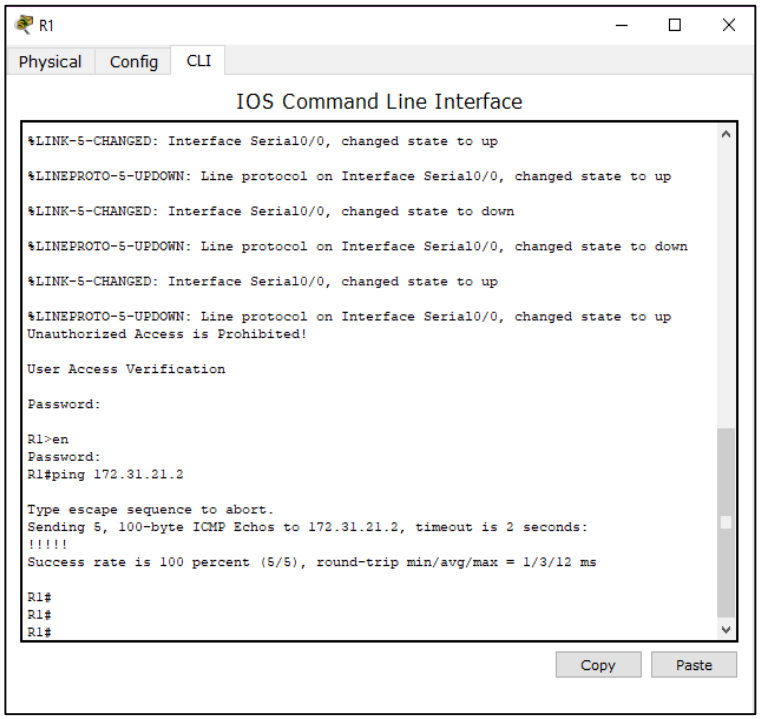
Se usa el comando ping para probar la conectividad entre dispositivos de red.

Tabla 10. Probación de la conectividad entre dispositivos de red.

De	A	Dirección IP	resultados de ping
R1	R2, S0/1	172.31.21.2	Successful (exitoso)
R2	R3, S0/1	172.31.23.2	Successful (exitoso)
Internet PC	Default Gateway	209.165.200.225	Successful (exitoso)

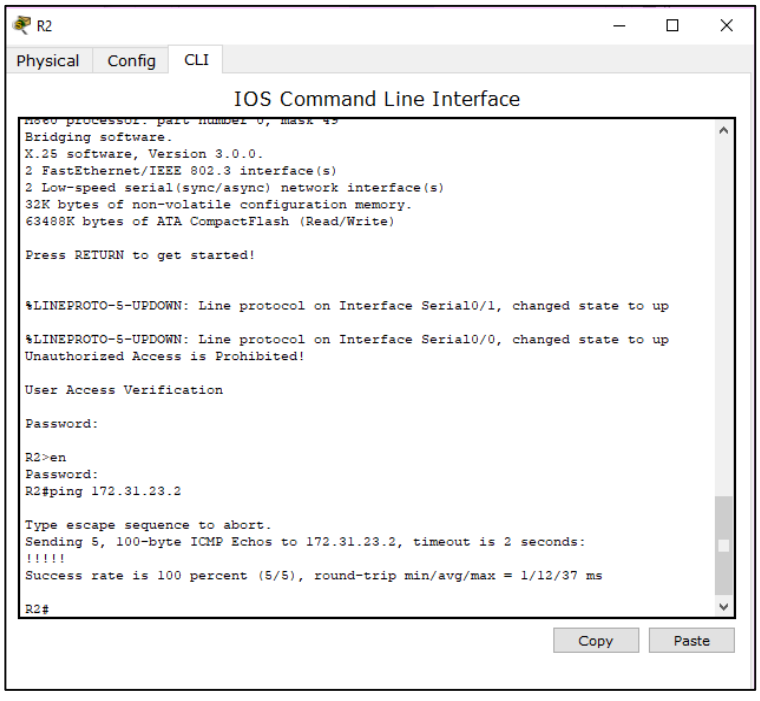
Fuente. Elaboración propia.

Figura 16. Ping R1-R2



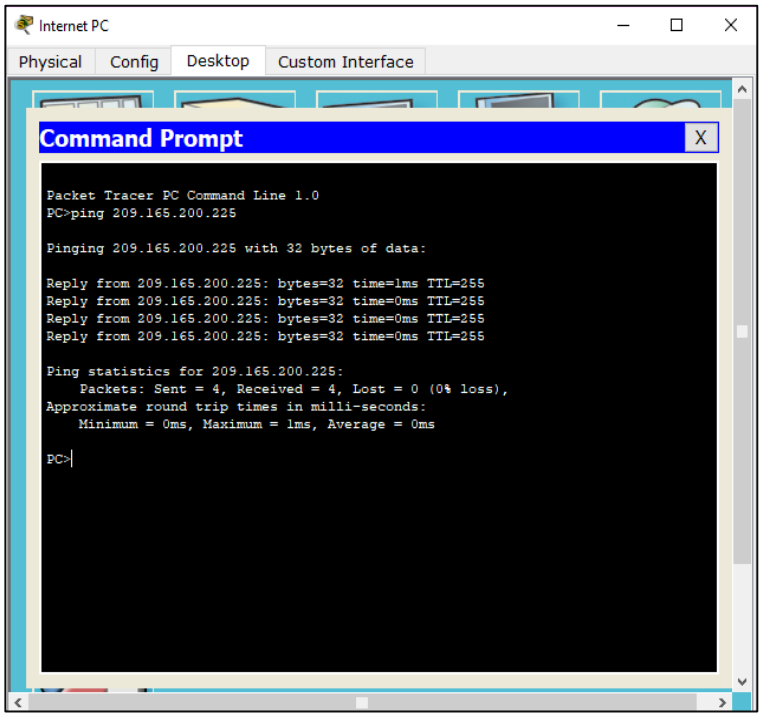
Fuente. Elaboración propia.

Figura 17. Ping R2-R3.



Fuente. Elaboración propia.

Figura 18. Ping Internet PC-Default Gateway



Fuente. Elaboración propia.

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

OSPFv2 area 0

Tabla 1. Configuración OSPV area 0

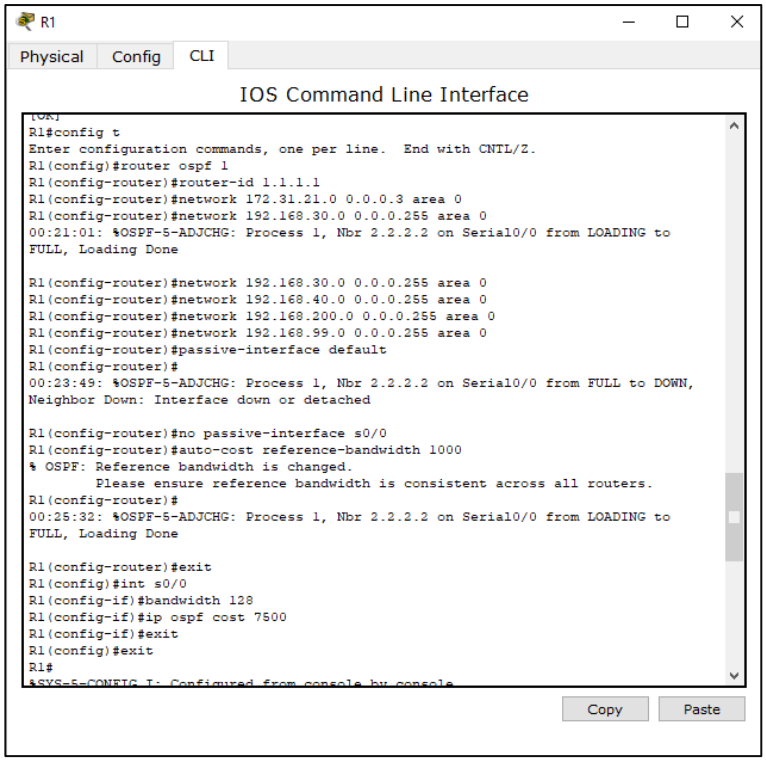
Elemento de configuración	Especificación
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Fuente: Guía PRUEBA DE HABILIDADES CCNA. Recuperado de: https://1drv.ms/b/s!AmIJYei-NT1Inld9q3plaoaVvK5f

Paso 1: Configurar OSPFv2 en R1.

```
R1#config t
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0
R1(config-router)#auto-cost reference-bandwidth 1000
R1(config-router)#exit
R1(config)#int s0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#exit
```

Figura 19. Configurar OSPFv2 en R1.

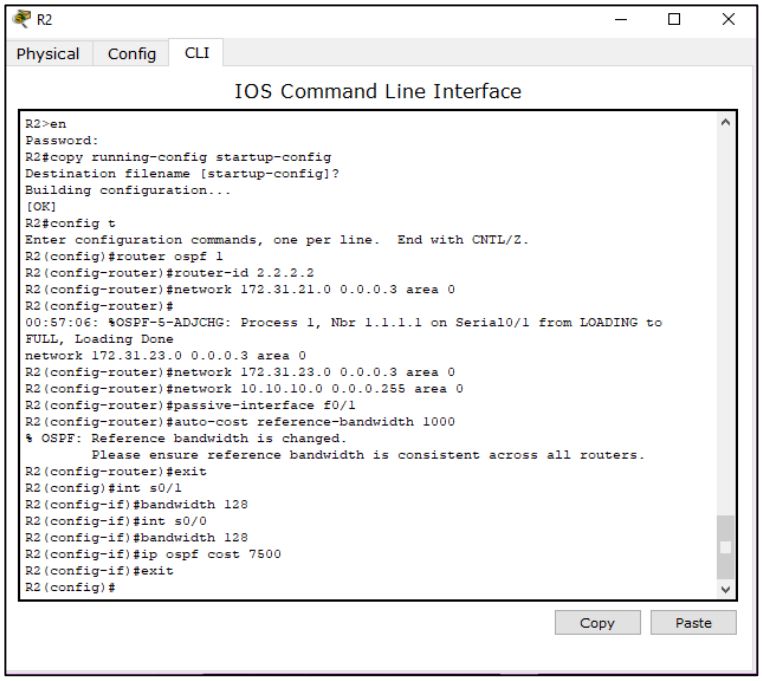


Fuente. Elaboración propia.

Paso 2: configurar OSPFv2 en R2.

```
R2#config t
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/1
R2(config-router)#auto-cost reference-bandwidth 1000
R2(config-router)#exit
R2(config)#int s0/1
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#exit
```

Figura 20. Configurar OSPFv2 en R2.



Fuente. Elaboración propia.

Paso 3. Configurar OSPFv2 en R3.

Se usa una sola dirección de sumatoria (summary) para las interfaces LAN (loopback).en el siguiente cuadro se visualiza la operación:

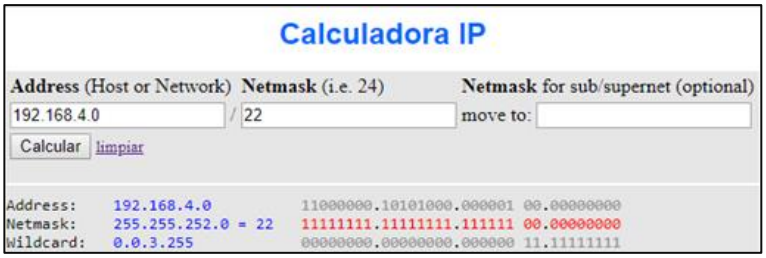
Tabla 11. Sumatoria (summary) para las interfaces LAN (loopback).

192	168	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0		192.168.4.0
192	168	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0		192.168.5.0
192	168	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0		192.168.6.0
192	168	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0		192.168.4.0/22

Fuente. Elaboración propia.

Se usa una calculadora IP online para encontrar la Wildcard

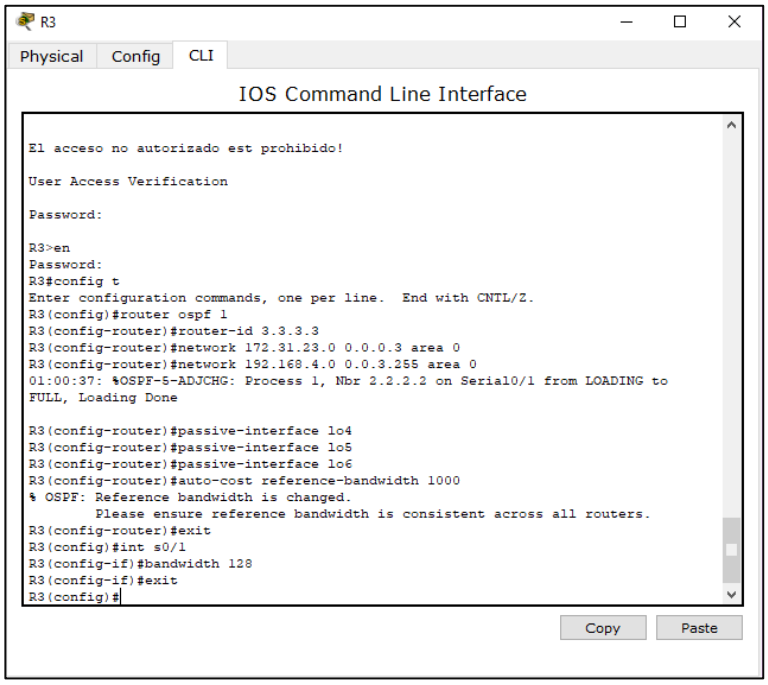
Figura 21. Wildcard Summary.



Fuente. Elaboración propia.

```
R3#config t
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#auto-cost reference-bandwidth 1000
R3(config-router)#exit
R3(config)#int s0/1
R3(config-if)#bandwidth 128
R3(config-if)#exit
```

Figura 22. Configurar OSPFv2 en R3.



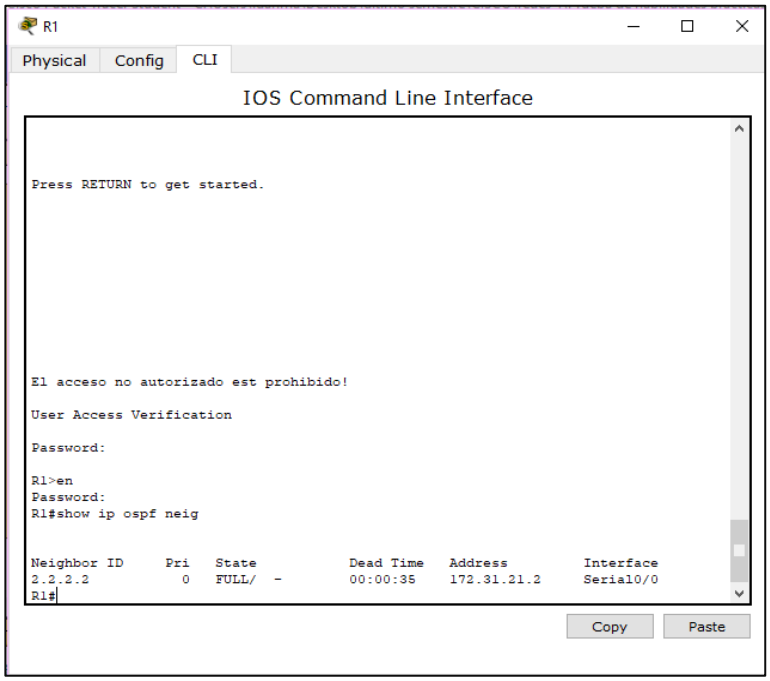
Fuente. Elaboración propia.

Verificar información de OSPF

Paso1. Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Para R1 usando el comando `R1#show ip ospf neig`

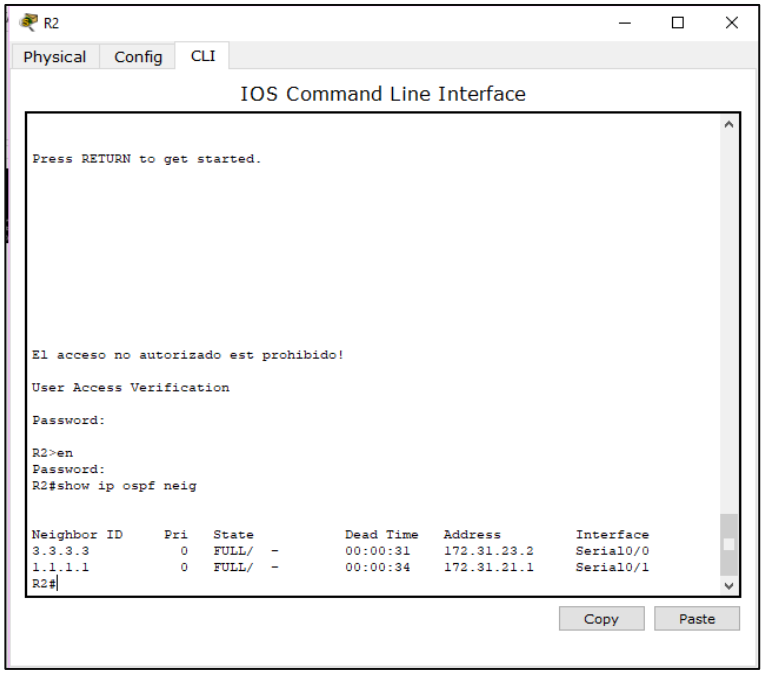
Figura 23. Visualización tablas de enrutamiento R1 conectado por OSPFv2.



Fuente. Elaboración propia.

Para R2 usando el comando `R2#show ip ospf neig`

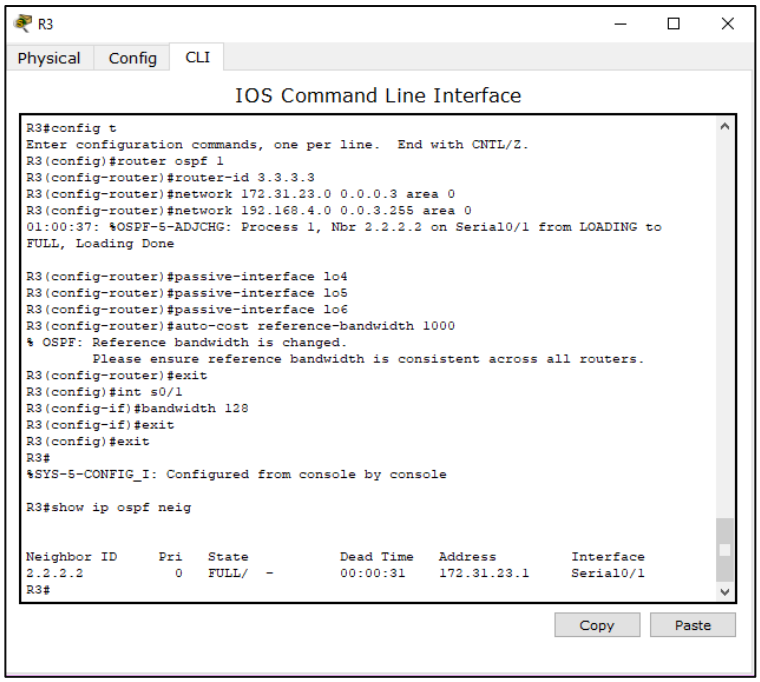
Figura 24. Visualización tablas de enrutamiento R2 conectado por OSPFv2.



Fuente. Elaboración propia.

Para R3 usando el comando `R3#show ip ospf neig`

Figura 25. Visualización tablas de enrutamiento R3 conectado por OSPFv2.

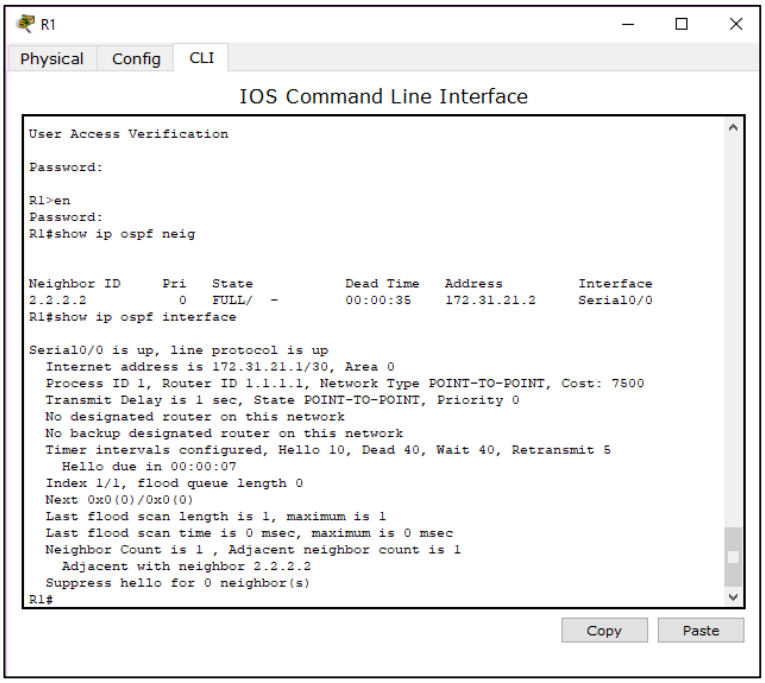


Fuente. Elaboración propia.

Paso 2. Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

Para R1 usando el comando `R1#show ip ospf interface`

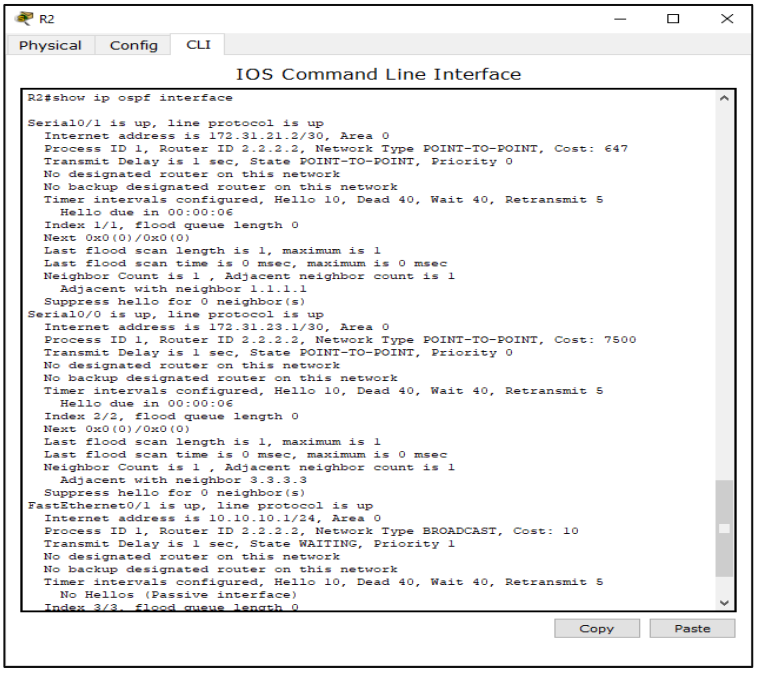
Figura 26. Visualización lista resumida de interfaces por OSPF R1.



Fuente. Elaboración propia.

Para R2 usando el comando `R2#show ip ospf interface`

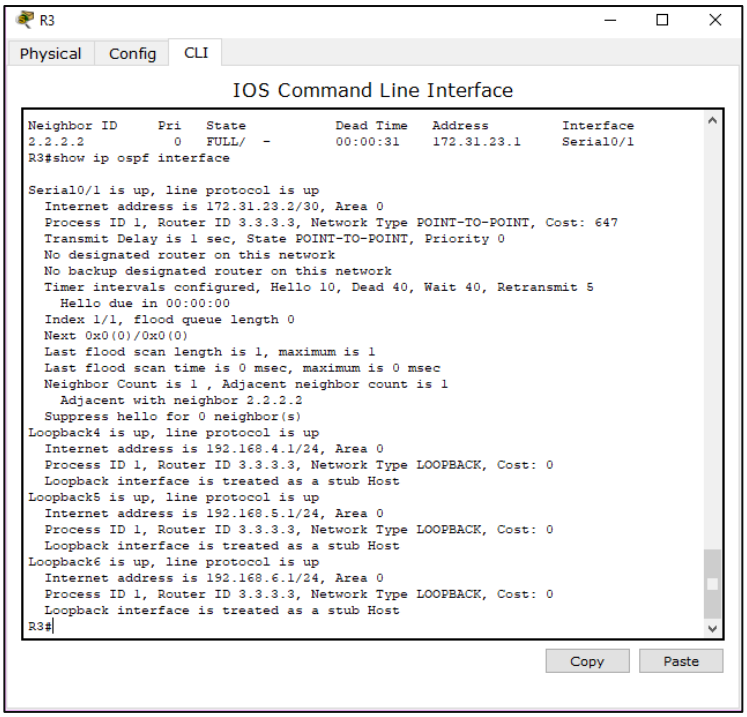
Figura 27. Visualización lista resumida de interfaces por OSPF R2.



Fuente. Elaboración propia.

Para R3 usando el comando `R3#show ip ospf interface`

Figura 28. Visualización lista resumida de interfaces por OSPF R3.

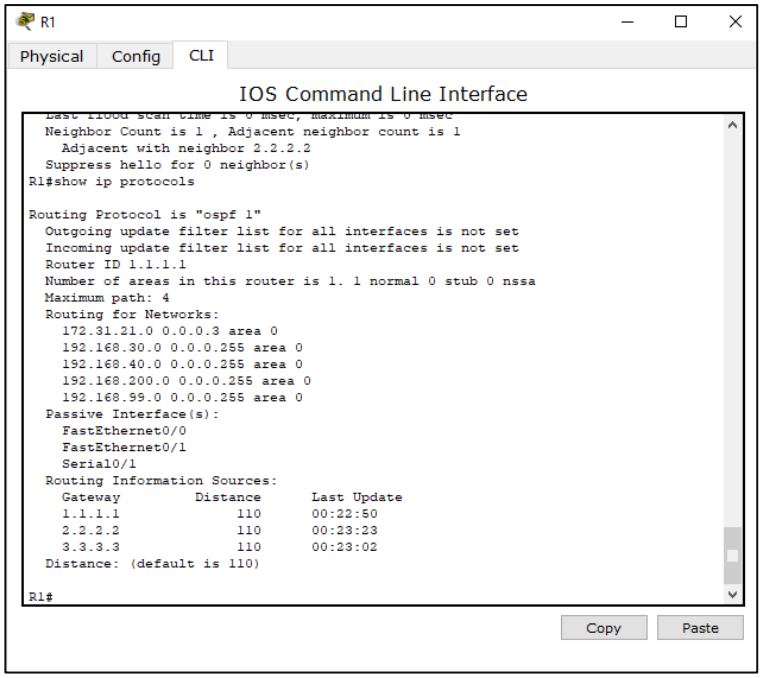


Fuente. Elaboración propia.

Paso 3. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en cada router.

Para R1 usando el comando `R1#show ip protocols`

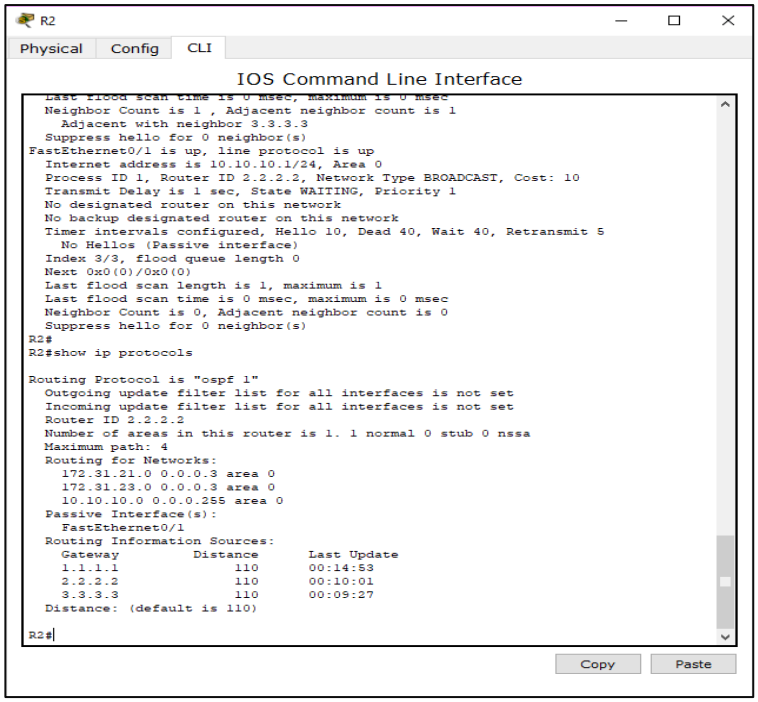
Figura 29. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en R1.



Fuente. Elaboración propia.

Para R2 usando el comando `R2#show ip protocols`

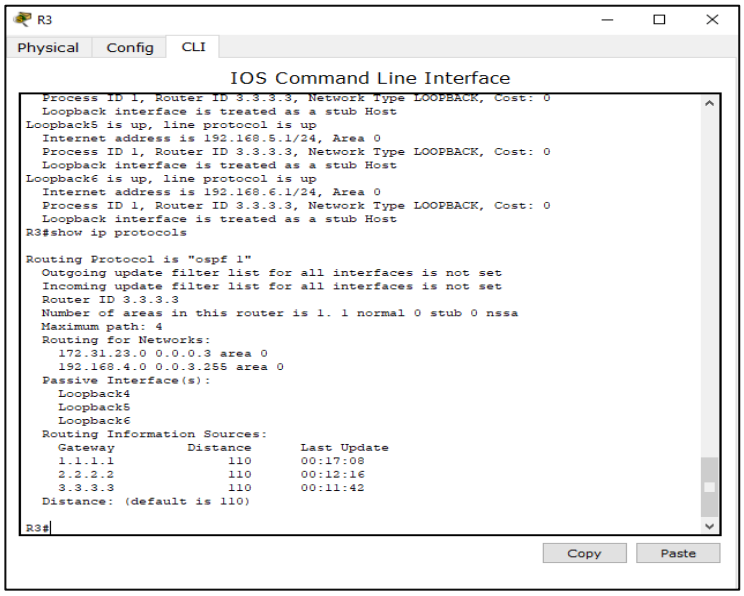
Figura 30. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en R2.



Fuente. Elaboración propia.

Para R3 usando el comando `R3#show ip protocols`

Figura 31. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en R3.



Fuente. Elaboración propia.

3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

4. En el Switch 3 deshabilitar DNS lookup

5. Asignar direcciones IP a los Switches acorde a los lineamientos.

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Paso 1. Configurar S1.
Las tareas de configuración para S1 incluyen lo siguiente:

Tabla 12. Configuración VLANs S1.

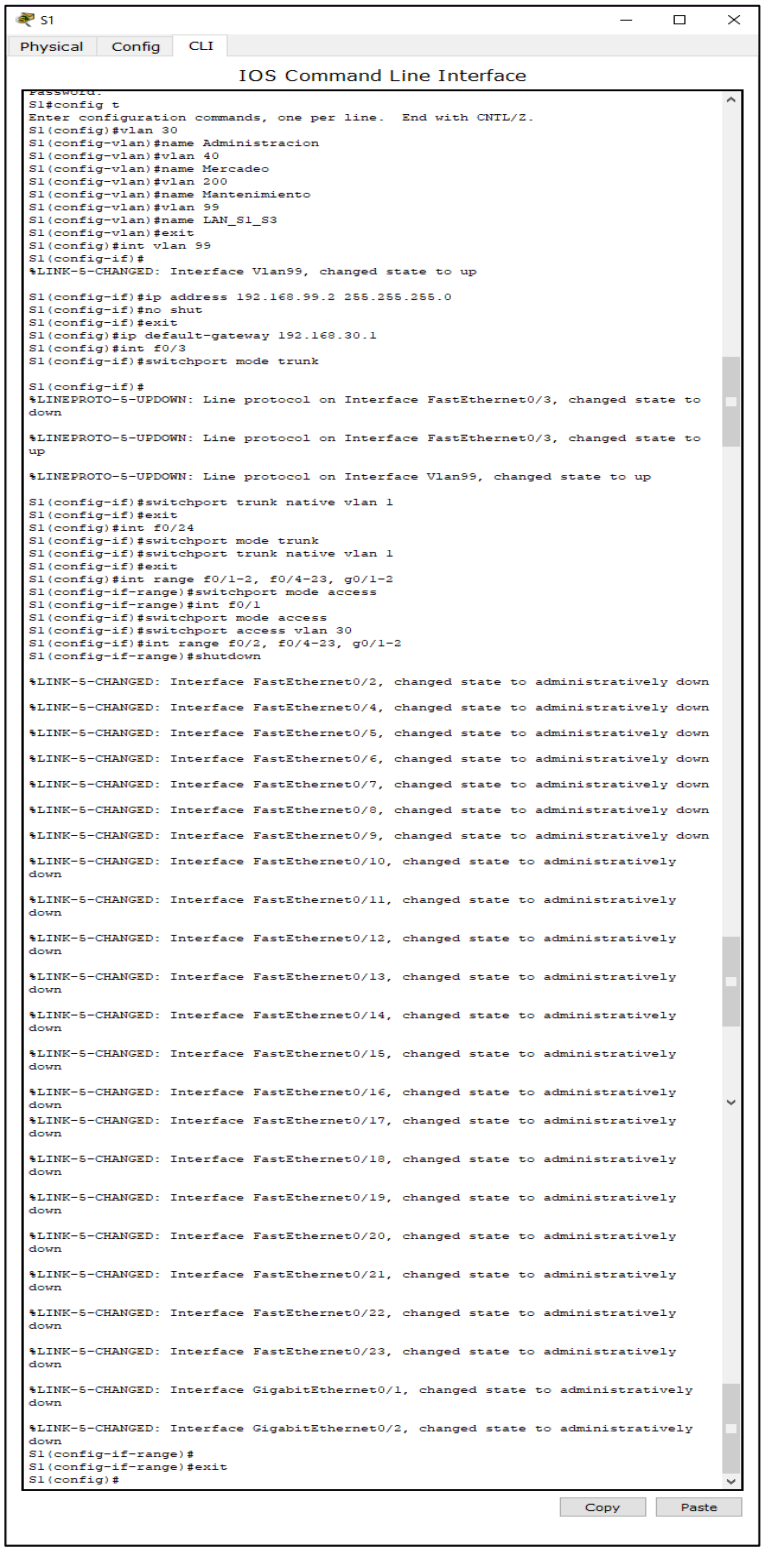
Elemento de configuración	Especificación
Crear la base de datos de VLAN	El uso de topologías de VLAN tabla de claves para crear y nombrar cada una de las VLAN en la lista.
Asignar la dirección IP de administración.	Asignar la dirección IPv4 de Capa 3 a la VLAN de Administración. Utilice la dirección IP asignada a S1 en el diagrama de topología.
Asignar el default-gateway	Asigne la primera dirección IP en la subred que el default-gateway. 192.168.30.1
Forzar trunking el interfaz F0/3	Utilizar VLAN 1 como la VLAN nativa.
Forzar trunking el interfaz F0/24	Utilizar VLAN 1 como la VLAN nativa.
Configurar todos los otros puertos como puertos de acceso	Utilizar el comando interface range.
Asignar F0/1 a la VLAN 30	
Apagado de todos los puertos no utilizados.	

Fuente. Elaboración propia.

```
S1#config t
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#vlan 99
S1(config-vlan)#name LAN_S1_S3
S1(config-vlan)#exit
S1(config)#int vlan 99
```

```
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.30.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int range f0/1-2, f0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int range f0/2, f0/4-23, g0/1-2
S1(config-if)#shutdown
S1(config-if)#exit
```

Figura 32. Configuración VLANs S1.



Fuente. Elaboración propia.

Paso 2: Configura S3.

Las tareas de configuración para S3 incluyen lo siguiente:

Tabla 13. Configuración VLANs S3.

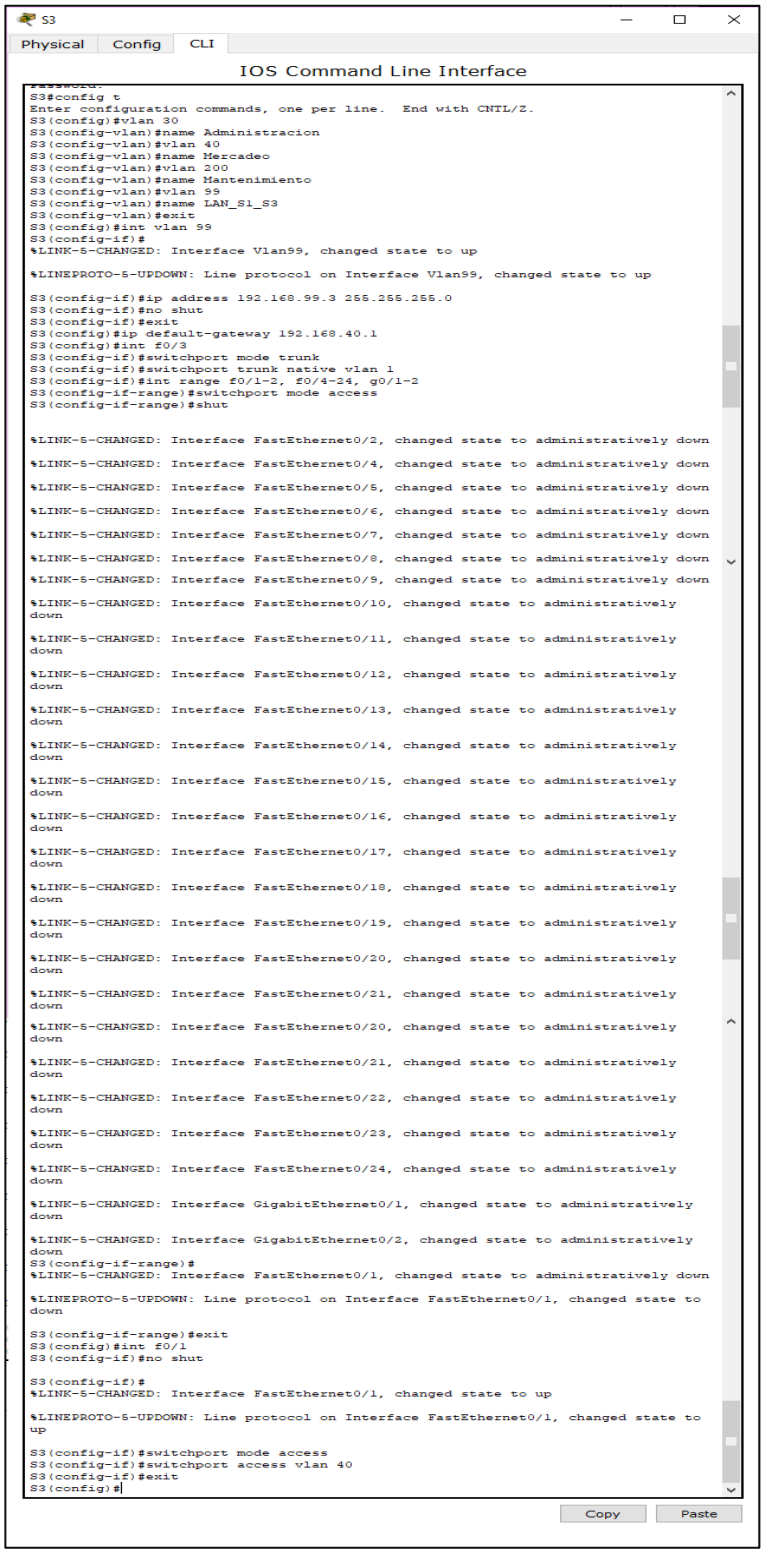
Elemento de configuración	Especificación
Disable DNS lookup	no ip domain-lookup
Crear la base de datos de VLAN	Utilizar VLAN topología Tabla de claves para crear cada una de las VLAN en la lista. Nombre cada VLAN.
Asignar la dirección IP de administración.	Asignar la dirección IPv4 de Capa 3 a la VLAN de administración. Utilice la dirección IP asignada a S3 en el diagrama de topología.
Asignar el default-gateway	Asigne la primera dirección IP en la subred que la puerta de entrada por defecto,
Forzar trunking el interfaz F0 / 3	Utilizar VLAN 1 como la VLAN nativa.
Configurar todos los otros puertos como puertos de acceso	Utilice el comando interface range.
Asignar F0/1 a la VLAN 40	
Apagado de todos los puertos no utilizados.	

Fuente. Elaboración propia.

```
S3#config t
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#vlan 99
S3(config-vlan)#name LAN_S1_S3
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.40.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#shut
S3(config-if-range)#exit
S3(config)#int f0/1
S3(config-if)#no shut
```

```
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#exit
```

Figura 33. Configuración VLANs S3.



Fuente. Elaboración propia.

Paso 3. Configura R1.

Las tareas de configuración para R1 incluyen lo siguiente:

Tabla 14. Configuración 802.1Q en R1.

Elemento de configuración	Especificación
Configurar 802.1Q subinterface .30 en F0/0	Descripción Administracion_LAN Asignar VLAN 30. Asigne la primera dirección disponible para esta interfaz.
Configurar 802.1Q subinterface .40 en F0/0	Descripción Mercadeo_LAN Asignar VLAN 40. Asigne la primera dirección disponible para esta interfaz.
Configurar 802.1Q subinterface .200 en F0/0	Descripción Mantenimiento_LAN Asignar VLAN 200. Asigne la primera dirección disponible para esta interfaz.
Configurar 802.1Q subinterface .99 en F0/0	Descripción S1_S3_LAN Asignar VLAN 99. Asigne la primera dirección disponible para esta interfaz.
Activar Interface F0/0	

Fuente. Elaboración propia.

```
R1#config t
R1(config)#int f0/0.30
R1(config-subif)#description Administracion_LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.40
R1(config-subif)#description Mercadeo_LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.200
R1(config-subif)#description Mantenimiento_LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.99
R1(config-subif)#description S1_S3_LAN
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0
```

```
R1(config-if)#no shut
R1(config-subif)#exit
```

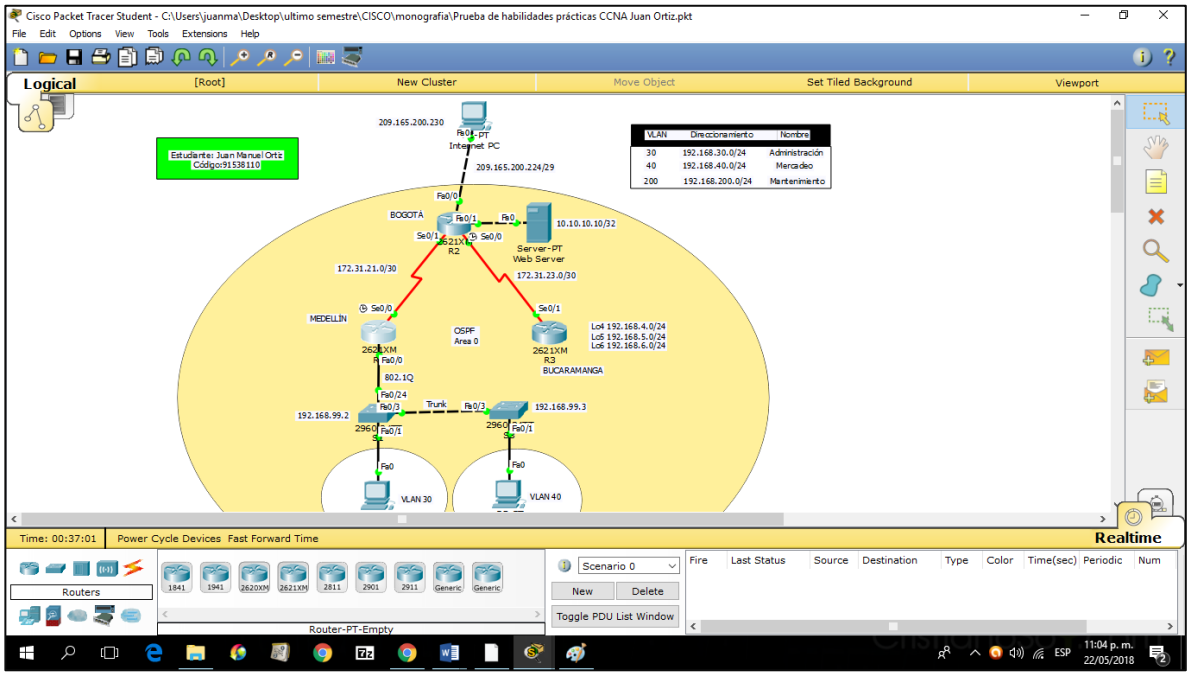
Figura 34. Configuración 802.1Q en R1.

Fuente. Elaboración propia.

Paso 4. Verificar la conectividad de la red.

Después de la configuración de los dispositivos S1, S2 y R1 se observa en la simulación que todos los puntos de conexión se encuentran en color verde lo que indica su correcta comunicación pero se debe comprobar usando el comando ping.

Figura 35. Verificación de la conectividad de la red.



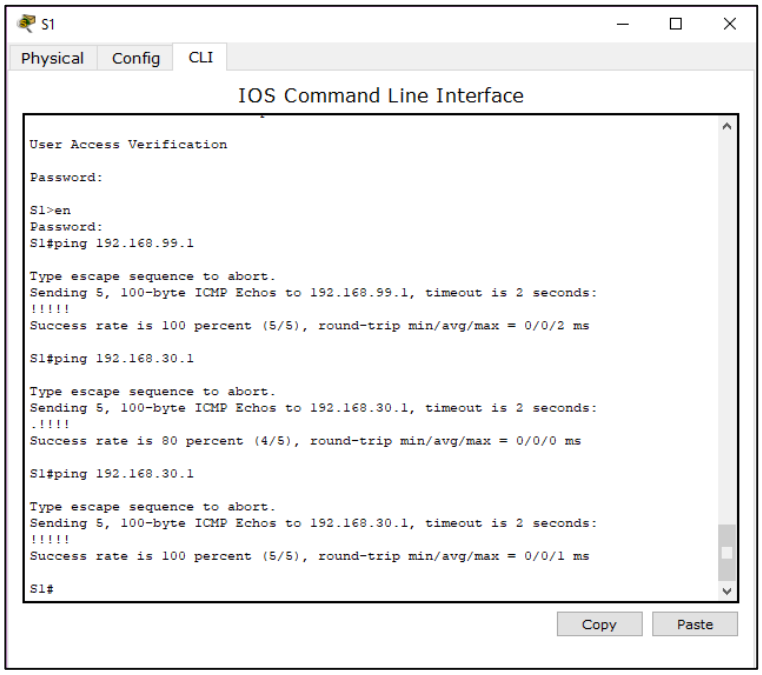
Fuente. Elaboración propia.

Tabla 15. Verificación de la conectividad de la red.

De	A	Dirección IP	resultados de ping
S1	R1, VLAN 99 address	192.168.99.1	Successful (exitoso)
S3	R1, VLAN 99 address	192.168.99.1	Successful (exitoso)
S1	R1, VLAN 30 address	192.168.30.1	Successful (exitoso)
S3	R1, VLAN 40 address	192.168.40.1	Successful (exitoso)

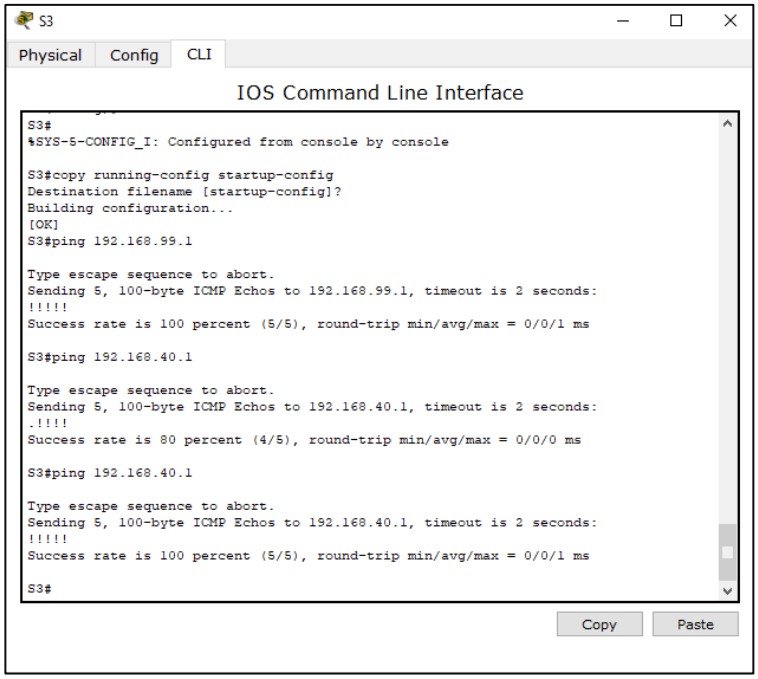
Fuente. Elaboración propia.

Figura 36. Ping S1 con R1 VLAN 99 y R1 VLAN 30.



Fuente. Elaboración propia.

Figura 37. Ping S3 con R1 VLAN 99 y R1 VLAN 40.



Fuente. Elaboración propia.

7. Implementar DHCP y NAT para IPv4

8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Las tareas de configuración para R1 incluyen lo siguiente:

Tabla 16. Configuración DHCP en R1.

Elemento de configuración	Especificación
Reservar las primeras 30 direcciones IP en la VLAN 30 para configuraciones estáticas	192.168.30.1 192.168.30.30
Reservar las primeras 30 direcciones IP en la VLAN 40 para configuraciones estáticas	192.168.40.1 192.168.40.30
Crear un conjunto DHCP para la VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer la puerta de enlace predeterminada.
Crear un conjunto DHCP para la VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer la puerta de enlace predeterminada.

Fuente. Elaboración propia.

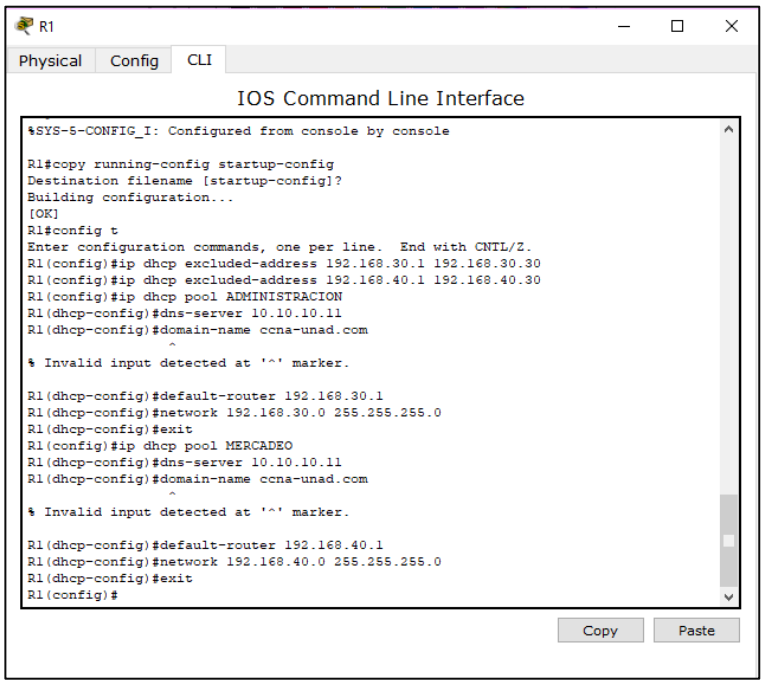
```
R1#config t
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#exit

R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
```

```
R1(dhcp-config)#exit
```

Figura 38. Configuración DHCP en R1.



Fuente. Elaboración propia.

10. Configurar NAT en R2 para permitir que los host puedan salir a internet

Paso 1. Configurar NAT estática y dinámica en R2.

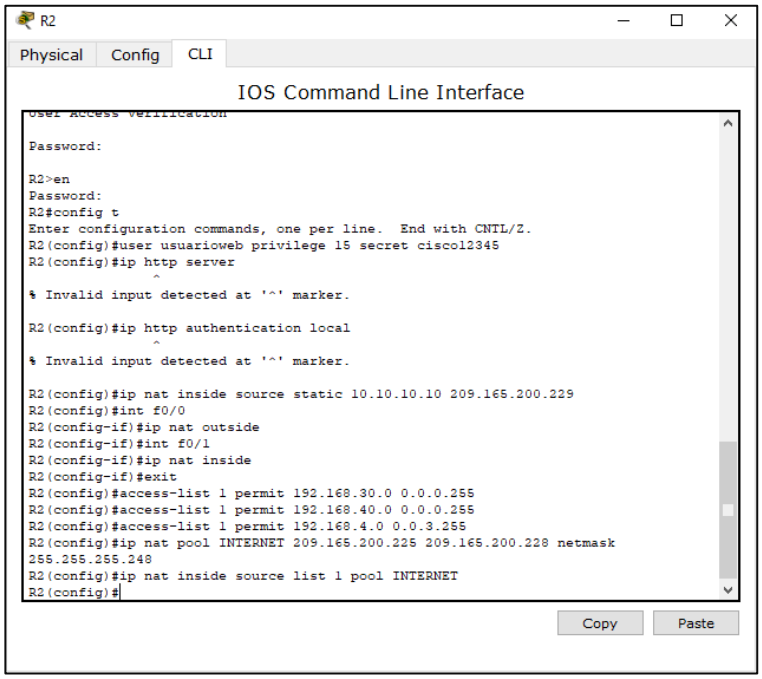
Tabla 17. Configuración NAT estática y dinámica en R2

Elemento de configuración	Especificación
Crear una base de datos local con la cuenta de usuario 1	Nombre de usuario: **usuarioweb** Contraseña: **cisco12345** nivel de privilegios: **15**
Habilitar el servicio de servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear un NAT estático para el servidor Web	Dentro de direcciones global: **209.165.200.229**
Asignar la interfaz dentro y fuera de la NAT estática	
Configurar la NAT dinámica dentro del ACL privada	Lista de acceso: 1 Permitir a las redes de Administracion y Mercadeo en R1 a ser traducidos.
Definir el pool de direcciones IP públicas utilizables	Pool Name: **INTERNET** Pool de direcciones: **209.165.200.225 – 209.165.200.228**
Definir la traducción NAT dinámico	

Fuente. Elaboración propia.

```
R2#config t
R2(config)#user usuarioweb privilege 15 secret cisco12345
R2(config)#ip http server
R2(config)#ip http authentication local
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
```

Figura 39. Configuración NAT estática y dinámica en R2



Fuente. Elaboración propia.

Paso 2. Verificar DHCP y NAT estática.

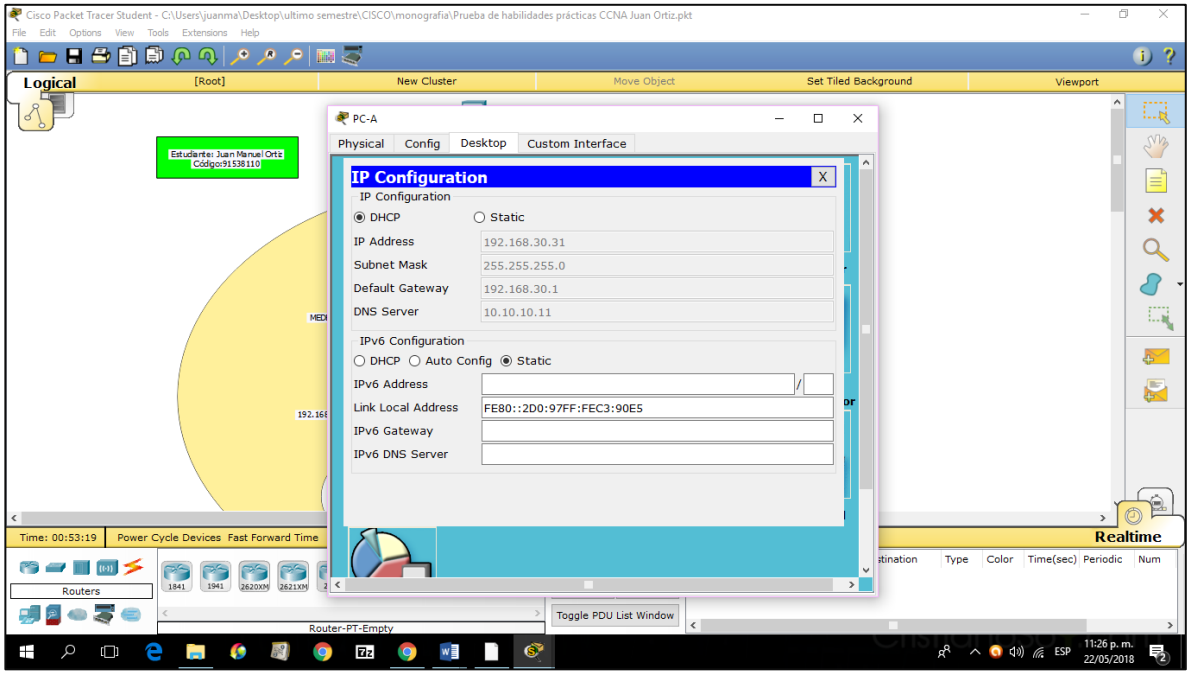
Tabla 18. Verificación DHCP y NAT estática.

Prueba	resultados
Verificar que el PC-A información de IP adquirida desde el servidor DHCP	
Compruebe que la PC-C adquirió información de IP desde el servidor DHCP	
Compruebe que PC-A puede hacer ping PC-C. **Nota**: Puede que sea necesario desactivar el firewall de PC	ping 192.168.40.31
Utilizar un navegador web en el PC de Internet para acceder al servidor Web (209.165.200.229). Ingresar con nombre de usuario: webuser, Contraseña: cisco12345	

Fuente. Elaboración propia.

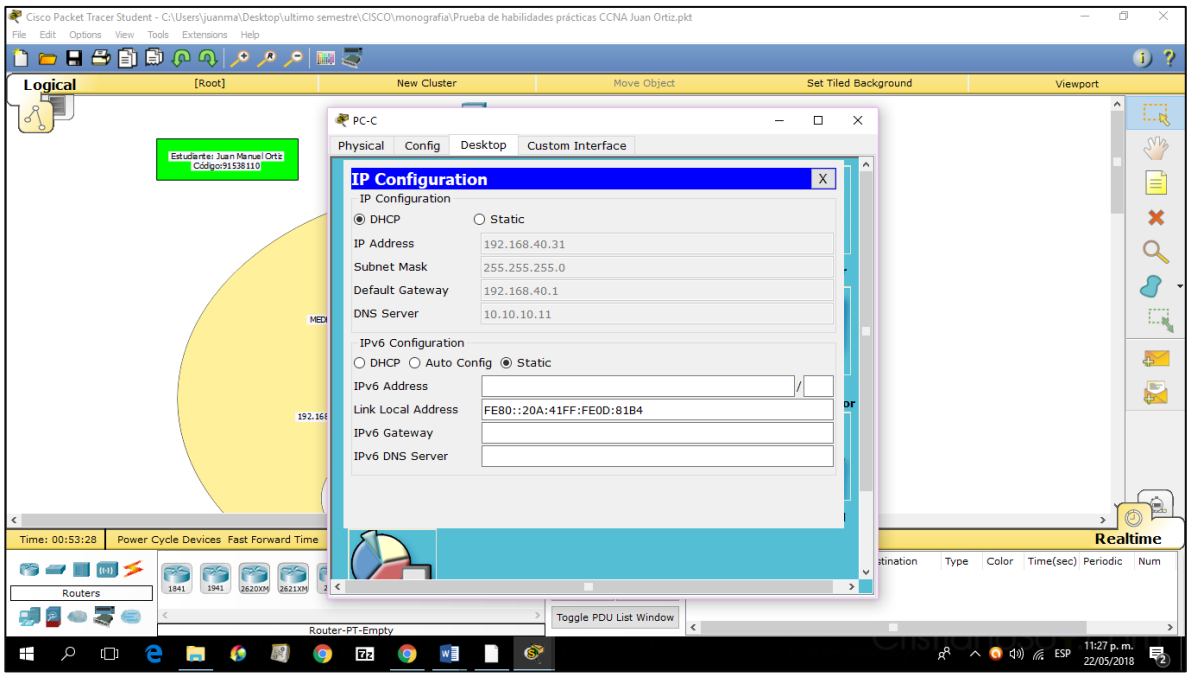
Para esto pasamos las computadoras PC-A y PC-C a modo DHCP

Figura 40. Computadoras PC-A modo DHCP.



Fuente. Elaboración propia.

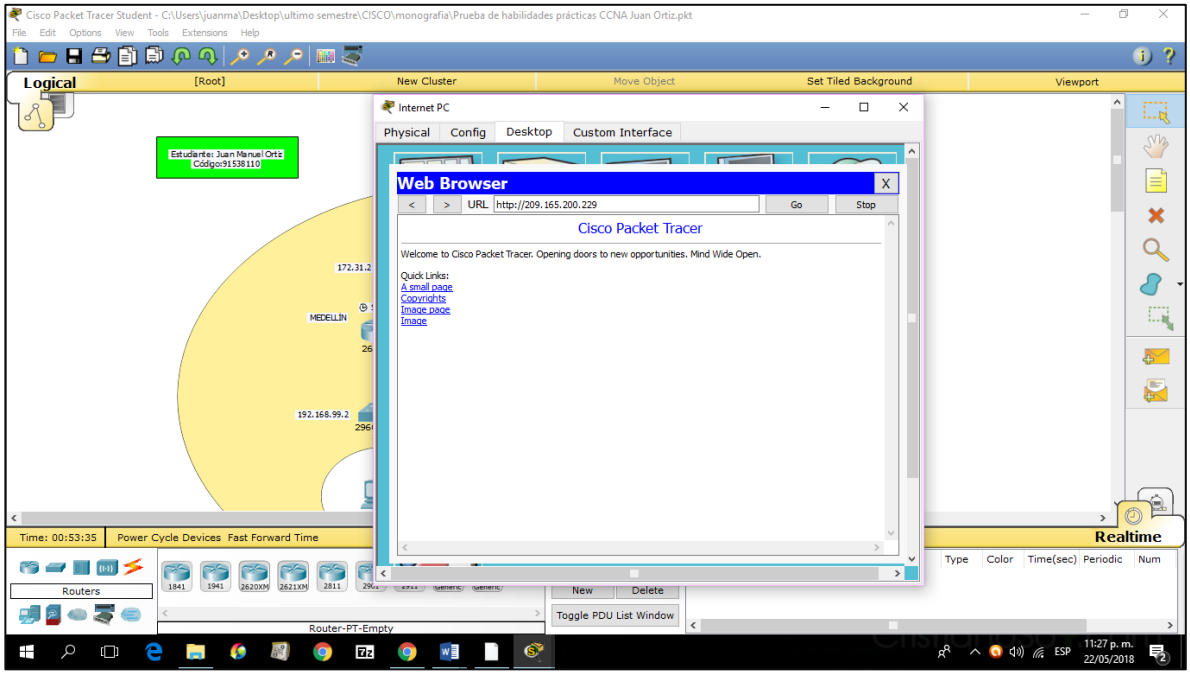
Figura 41. Computadoras PC-C a modo DHCP.



Fuente. Elaboración propia.

Se accede al sitio web 209.165.200.229 desde la PC de Internet.

Figura 42. Acceso al sitio web 209.165.200.229 desde la PC de Internet.



Fuente. Elaboración propia.

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

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

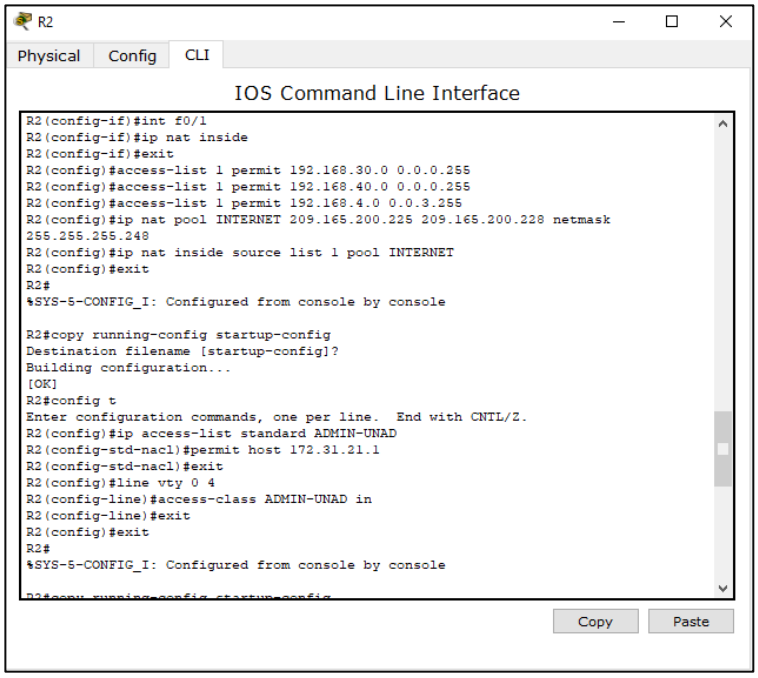
Tabla 19. Configuración de acceso a las líneas VTY en R2.

Elemento de Configuración	Especificación
Configurar una lista de acceso llamado sólo para permitir R1 hacer telnet a R2.	Nombre de ACL: ADMIN-UNAD
Aplicar la ACL nombrada a las líneas vty	
Verificar que la ACL está funcionando como se esperaba,	

Fuente. Elaboración propia.

```
R2#config t
R2(config)#ip access-list standard ADMIN-UNAD
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-UNAD in
R2(config-line)#exit
```

Figura 43. Configuración de acceso a las líneas VTY en R2.



Fuente. Elaboración propia.

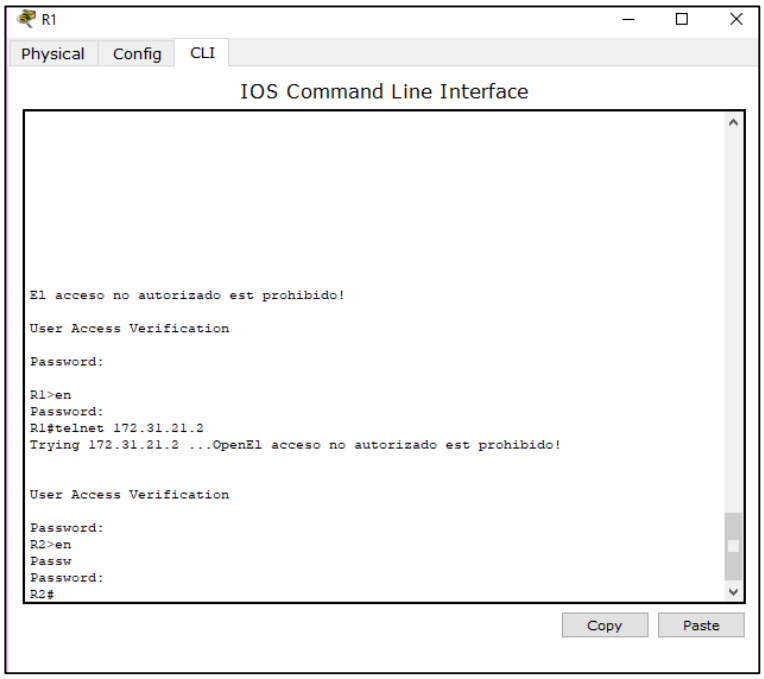
Comprobación desde R1

```
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenEl acceso no autorizado est prohibido!
```

```
User Access Verification

Password:
R2>en
Passw
Password:
R2#
```

Figura 44. R1 telnet a R2.

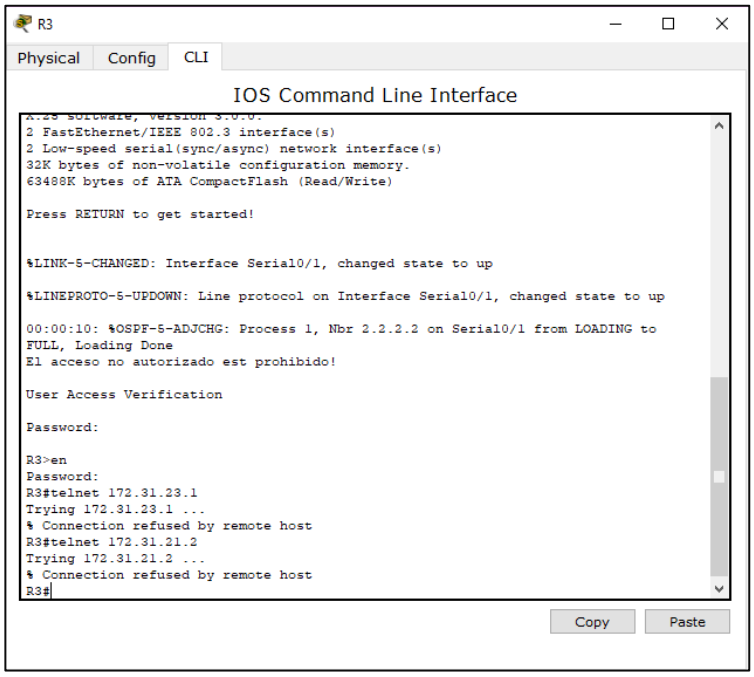


Fuente. Elaboración propia.

Comprobación desde R3

```
R3#telnet 172.31.23.1
Trying 172.31.23.1 ...
% Connection refused by remote host
R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
```

Figura 45. R3 telnet a R2.



Fuente. Elaboración propia.

Nota: Se verifica que la ACL está funcionando correctamente, solo permite hacer telnet con R1, con R3 Conexión rechazada.

Paso 2: proteger la red del tráfico de Internet.

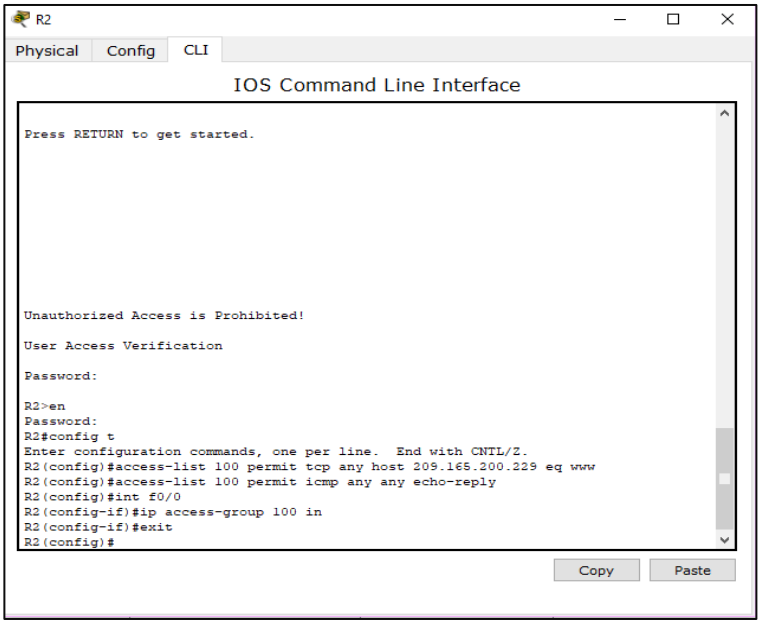
Tabla 20. Configuración ACL extendida en R2.

Elemento de configuración	Especificación
Configurar una ACL extendida a: • Permitir el acceso de los servidores de Internet WWW al servidor web simulada en R2 accediendo a la dirección de NAT estática (209.165.200.229). • Evitar que el tráfico de Internet de ping redes internas, sin dejar de permitir que las interfaces LAN para hacer ping a la PC a Internet.	ACL No: 100
Aplicar ACL a la interfaz apropiada (s)	
Verificar ACL está funcionando como se esperaba	Desde el PC de Internet a cualquier dispositivo los pings deben ser inalcanzables. Desde cualquier dispositivo al PC de Internet los pings deben tener éxito.

Fuente. Elaboración propia.

```
R2#config t
R2(config)#access-list 100 permit tcp any host 209.165.200.229 eq www
R2(config)#access-list 100 permit icmp any any echo-reply
R2(config)#int f0/0
R2(config-if)#ip access-group 100 in
R2(config-if)#exit
```

Figura 46. Configuración ACL extendida en R2.

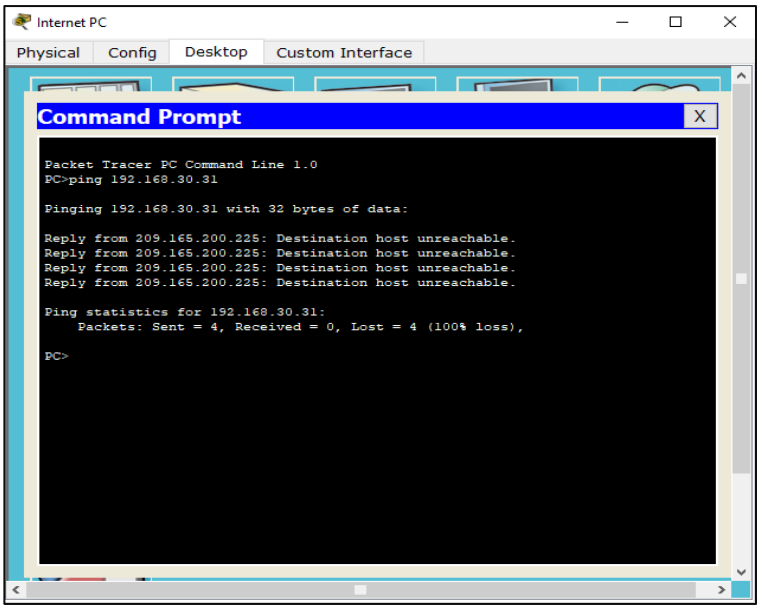


Fuente. Elaboración propia.

Verificar procesos de comunicación y redireccionamiento de tráfico.

Ping de Internet PC a PC-A. `PC>ping 192.168.30.31`

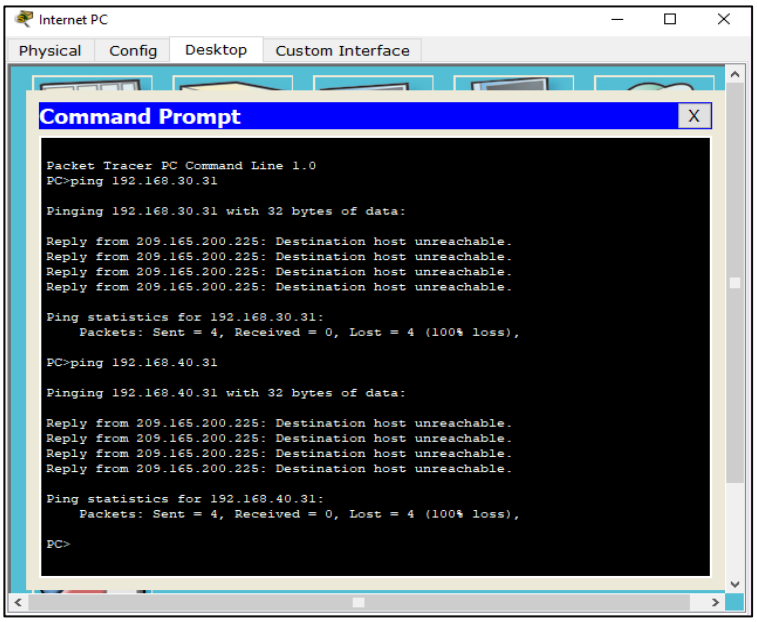
Figura 47. Ping de Internet PC a PC-A.



Fuente. Elaboración propia.

Ping de Internet PC a PC-C. `PC>ping 192.168.40.31`

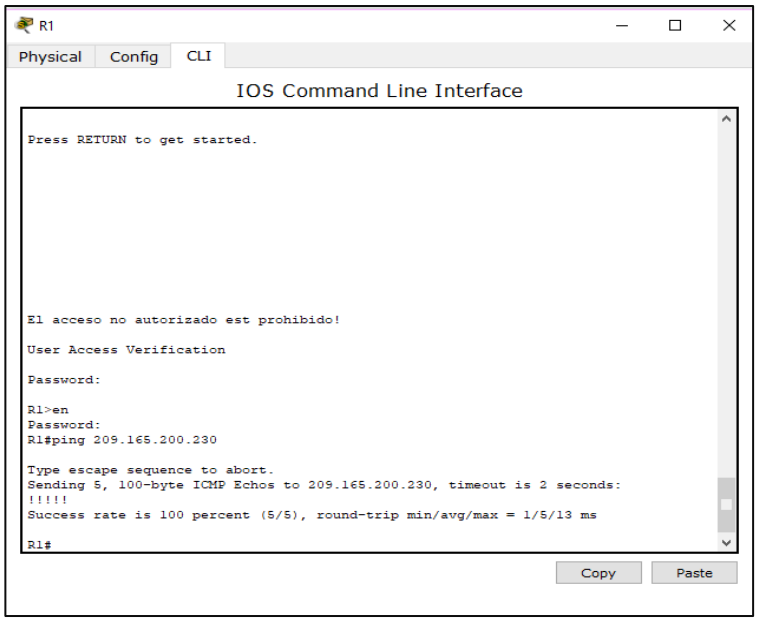
Figura 48. Ping de Internet PC a PC-C.



Fuente. Elaboración propia.

Ping de R1 a Internet PC. `R1#ping 209.165.200.230`

Figura 49. Ping de R1 a Internet PC.

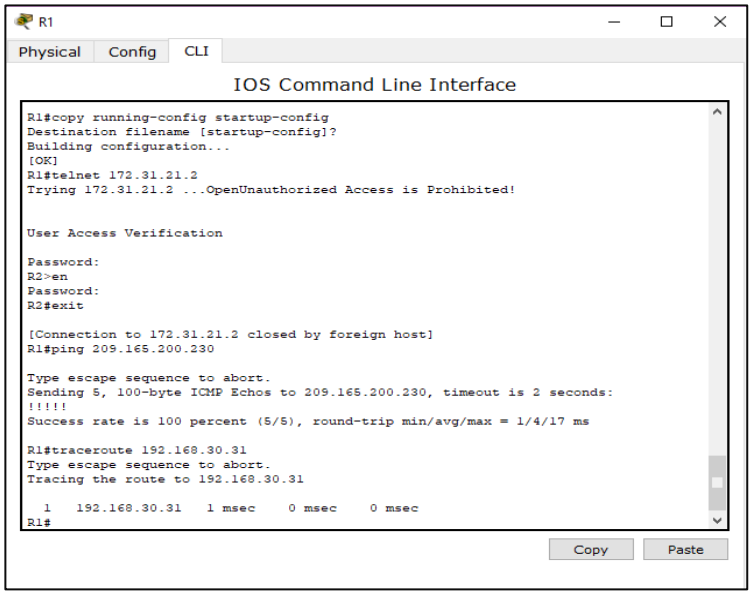


Fuente. Elaboración propia.

Se verifica que ACL está funcionando correctamente, ping exitoso.

Traceroute entre R1 y PC-A. `R1#traceroute 192.168.30.31`

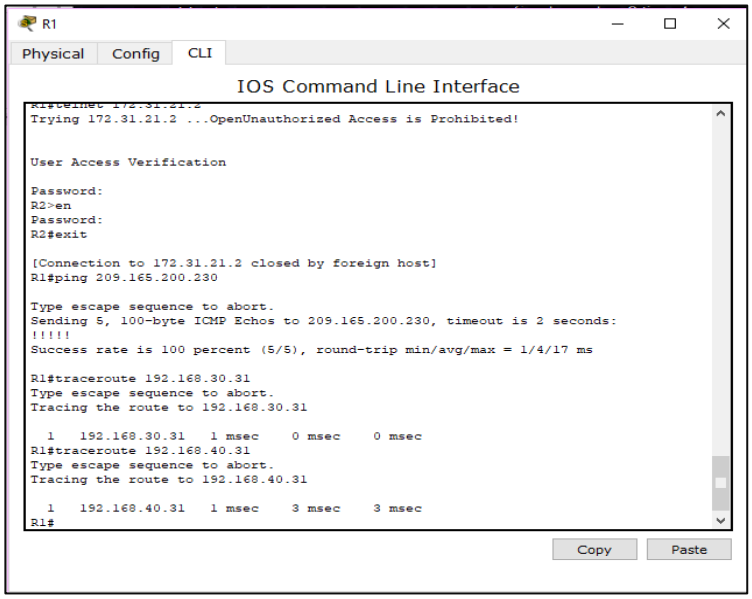
Figura 50. Traceroute entre R1 y PC-A.



Fuente. Elaboración propia.

Traceroute entre R1 y PC-C. `R1#traceroute 192.168.40.31`

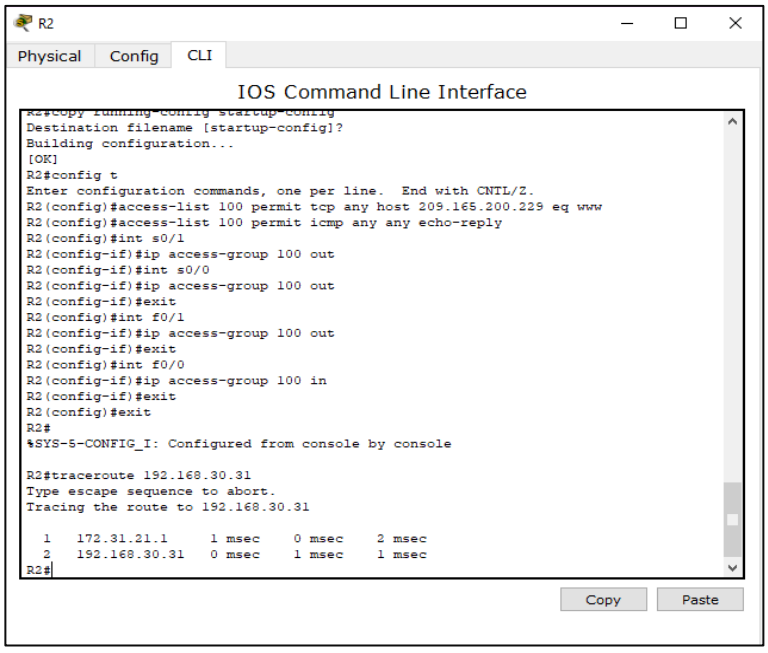
Figura 51. Traceroute entre R1 y PC-C.



Fuente. Elaboración propia.

Traceroute entre R2 y PC-A. `R2#traceroute 192.168.30.31`

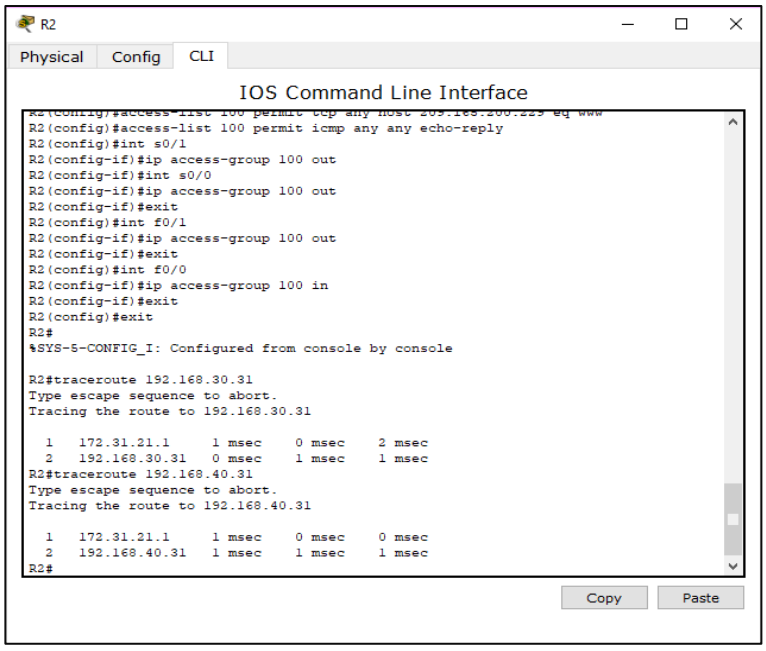
Figura 52. Traceroute entre R2 y PC-A.



Fuente. Elaboración propia.

Traceroute entre R2 y PC-C. `R2#traceroute 192.168.40.31`

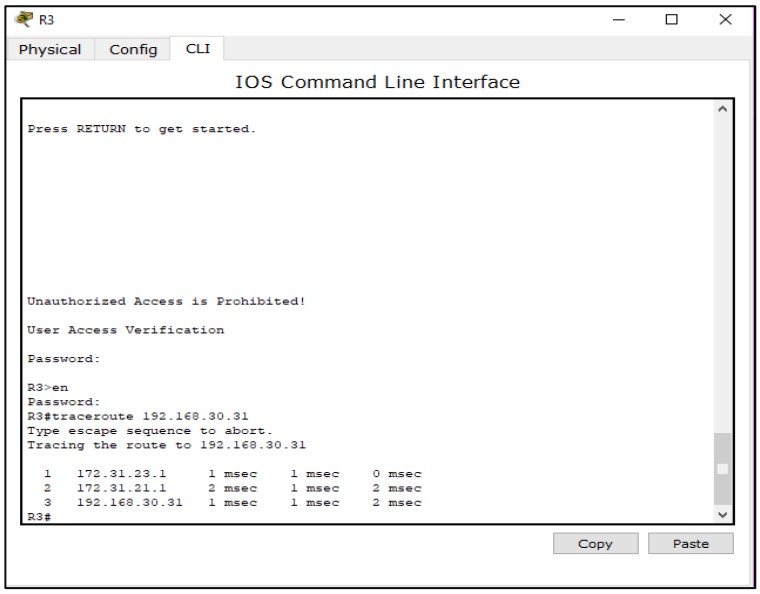
Figura 53. Traceroute entre R2 y PC-C.



Fuente. Elaboración propia.

Traceroute entre R3 y PC-A. `R3#traceroute 192.168.30.31`

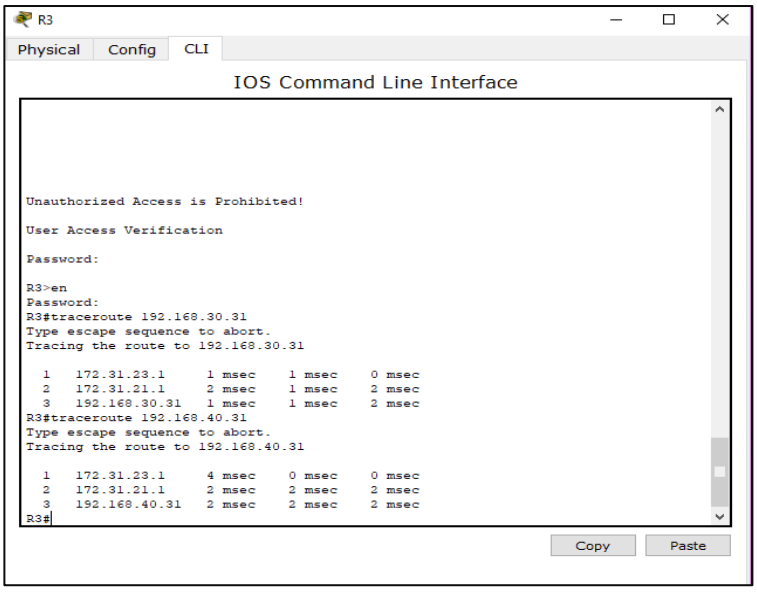
Figura 54. Traceroute entre R3 y PC-A.



Fuente. Elaboración propia.

Traceroute entre R3 y PC-C. `R3#traceroute 192.168.40.31`

Figura 55. Traceroute entre R3 y PC-C.



Fuente. Elaboración propia.

Se verificar procesos de comunicación y redireccionamiento de tráfico por medio del comando Tracert se muestran los host por los que pasan los datos y el tiempo que se toma en cada salto hasta llegar al destino.

CONCLUSIONES

En la configuración del direccionamiento IP acorde con la topología de red para del escenario dado, se debió tener presentes los elementos idóneos para la representación de la misma así como el especial cuidado en las asignaciones de las IP´s puesto que de allí deriva el éxito o el error al momento de realizar las respectivas pruebas.

Para la configuración del protocolo de enrutamiento del OSPFv2 se debe crear el proceso de OSPF desde la configuración global con el comando “router ospf”, después se deben configurar los rangos de red mediante “network área”, todas las interfaces que se incluyan mediante ese comando estarán participando en esa área de OSPF.

Cuando se implementa un servidor para la asignación de la direcciones de red es muy eficaz y práctica la asignación de direcciones de red, por esto un servidor DHCP es determinante a la hora de asignar direcciones de red a una gran cantidad de ordenadores obviando asignarlas una por una.

Las NAT son el único mecanismo utilizado para intercomunicar redes de distintas clases, consiste en transportar la información mediante paquetes a través del router sin importar la clase de la misma.

El comando ping es una opción muy frecuente para verificar conexión entre dispositivos para luego resolver problemas con la accesibilidad de dispositivos, además en conjunto con comando traceroute que se usa para realizar el seguimiento que los paquetes toman realmente al desplazarse hacia su destino, se constituyeron en herramientas fundamentales para determinar el éxito de las configuraciones realizadas en la tipología dada.

BIBLIOGRAFIA

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Módulo del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013. 426 páginas.

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Guías de prácticas del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013.

Cisco Networking Academy, MODULO DE ESTUDIO CCNA1 EXPLORATION (Network Fundamentals). Disponible en: http://www.mediafire.com/?9cq9h4jo23c1359

Cisco Networking Academy, MODULO DE ESTUDIO CCNA2 EXPLORATION (Routing Protocols and Concepts). Disponible en: http://www.mediafire.com/?5y052miul2vezhj

Mario A. Reyes Reynaud, 2011. Calculo de Subredes de Mexico. [Video] Disponible en: http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTBK7P&index=5