DESARROLLO DE LA PRÁCTICA FINAL

ALVARO YESID LOPEZ CONTRERAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

DESARROLLO DE LA PRÁCTICA FINAL

ALVARO YESID LOPEZ CONTRERAS

PRUEBA DE HABILIDADES CCNA 2020

TUTOR
NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

Nota de Aceptación

_____

_____

_____

_____

Firma del Tutor

_____

Firma del Jurado

Valledupar, 19, Abril, 2020/ 20, Mayo 2020

Dedicatoria

Inicialmente a Dios, que es por quien nos movemos y existimos, porque he contado con su bendición y soporte siempre, un ejemplo de ello son mis padres quienes han estado conmigo persistentemente, apoyándome de forma incondicional ellos y mis hermanos son mi motor y fuerza. También agradezco a los tutores que acompañaron en este proceso de instrucción Haciéndolo una experiencia inolvidable.

AGRADECIMIENTOS

Primero que todo doy gracias a Dios por darme la fuerza, la capacidad, inteligencia y sabiduría necesaria para concluir con éxito mis estudios, a mis padres que siempre me apoyaron en este difícil camino, me brindaron su ayuda afectiva, económica, ética y moral ante las diferentes circunstancias que se presentaban. A mis hermanos quienes siempre estuvieron allí dándome una voz de aliento de motivación para seguir adelante y no desfallecer. A la Universidad Nacional Abierta y a Distancia (UNAD) a esta gran institución le agradezco por permitirme ser parte de ella, por compartir su conocimiento y metodología de aprendizaje; a los directores y tutores de curso que siempre estuvieron dispuestos a enseñarme y darme la formación profesional para mejorar en las diferentes áreas de conocimiento.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL: es una lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto.

CISCO PACKET TRACER: es un software propiedad de Cisco System, Inc.
Diseñado para la simulación de redes basadas en los equipos de la citada compañía.
Junto con los materiales didácticos diseñados con tal fin, es la principal herramienta de trabajo para pruebas y simulación de prácticas en los cursos de formación de Cisco System.

DHCP: es un protocolo de configuración dinámica del host, permite a un equipo unirse a una red basada en direcciones IP sin tener pre-configurado una dirección IP.

DIRECCIÓN IP: es un conjunto único de números que identifican a su equipo de forma que pueda enviar y recibir datos hacia y desde otros equipos, respectivamente.

DIRECCIONES IPV4: es la versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red. Es uno de los protocolos más importantes para el funcionamiento de internet y fue implementado en ARPANET en 1983.

DIRECCIONES IPV6: es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a internet.

LAN: son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada como (una habitación, un edificio, o un conjunto de edificios).
NIC: (Network Information Center) es la autoridad que delega los nombres de Dominio a quienes los solicitan. El NIC es quien se encarga de registrar los dominios de un país.

JUSTIFICACION

Las redes permanecen en el cotidiano vivir desde el más infortunado hasta el más próspero, este fenómeno no conoce clerecía, linaje, ni límites geográficos. Es por ello que las redes hoy día representan un progreso tecnológico especializado muy trascendental, hacen parte de nuestras vidas, procuramos que la mayoría de las tareas que realizamos estén en la red disponible para todo el que lo requiera, (moda, nutrición, salud, diversión, trabajo, enseñanza etc.…), por ejemplo, se puede distinguir que la escasez de tiempo, no es un pretexto para emprender un transcurso de estudio, actualmente existe una gran cifra de instituciones virtuales como la reconocida cisco networking que ofrece la tecnología de la información y la comunicación (Tic), para mejorar las competencias de carreras y las oportunidades económicas en todo el mundo, promueven la formación a distancia, facilitando que las personas obtengan sus títulos sin tener que salir de la casa y desde cualquier parte del mundo.

PALABRAS CLAVE: ACL, NTP, DHCP, CISCO, UNAD, RIPv2

INTRODUCCIÓN

La repercusión de la tecnología y los recursos de comunicación actualmente es cada vez mayor, razón por la cual diferentes estructuras e instituciones deben cada día originar uso de desiguales medios que le permitan estar intercomunicados de manera ágil, segura y eficaz. Las redes informáticas van creciendo cada día más, permitiendo la interconexión de diferentes dispositivos a escalón mundial, justo por el número de usuarios es que se debe implementar la seguridad de los datos.

Las redes como base importante de la información poseen entre su infraestructura, accesos que deben ser reducidos casi en su colectividad, así que, tener la red con la seguridad ya establecida ayuda al cuidado de la información y a la integralidad de la misma, manejando el tema de las identificaciones dentro de una organización; Es por esto, por lo que este diplomado fue una herramienta fundamental para aprender sobre la administración de la misma. La evaluación denominada “prueba de habilidades prácticas”, hace parte de las actividades del Diplomado de Profundización CCNA e indagación identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.

Lo vital es poner a prueba los niveles de comprensión y solución de conflictos relacionados con diversos aspectos de Networking. El desarrollo de esta actividad se basa en el diseño y la configuración de cada escenario propuesto a través de la herramienta Cisco Packet Tracer y GNS3, cumpliendo las sugerencias establecidas en cada una de las tareas. Que permite visualizar las conexiones físicas y ejecutar los comandos de manera simulada. Al final de este trabajo se realiza un diagnóstico para comprobar que cada uno de los puntos de la red se pueda ver y que tengan conectividad entre sí.

.

RESUMEN

El objetivo del trabajo es demostrar las habilidades prácticas adquiridas durante el diplomado de profundización CCNA, el primer escenario propuesto es una red donde se distribuye una serie de VLANS, se configurara el enrutamiento para permitirles la conexión con Internet, además se debe configurar e interconectar entre sí cada uno de los dispositivos de red.
Se llevó a cabo la configuración de protocolos de enrutamiento dinámico RIP V2 para interconectar los routers del escenario propuesto.

En el segundo escenario se crean dos sucursales BOGOTÁ y MEDELLÍN, las cuales se deben configurar variados aspectos para lograr una completa comunicación entre los dispositivos, entre las cuales tenemos:

- Aseguramiento de líneas de consola.
- Configuración de enrutamiento.
- Aseguramiento de líneas VTY, mediante el protocolo SSH y Telnet.
- Autenticación de enlaces entre routers.
- Cifrado de contraseñas en texto plano.
- Enrutamiento de VLANS.
- Creación de banners.
- Traducción de direcciones con NAT y PAT.
- Asignación de nombres descriptivos a los equipos.

ABSTRACT

The objective of the work is to demonstrate the practical skills acquired during the CCNA deepening diploma, the first scenario proposed is a network where a series of VLANS is distributed, routing will be configured to allow them to connect to the Internet, and each of the network devices must also be configured and interconnected.
Configuration of RIP V2 dynamic routing protocols was carried out
to interconnect the routers of the proposed scenario.

In the second scenario, two branches BOGOTÁ and MEDELLÍN are created, which must configure various aspects to achieve complete communication between the devices, among which we have:

- Securing of console lines.
- Routing configuration.
- VTY lines assurance, using the SSH and Telnet protocol.
- Authentication of links between routers.
- Encryption of passwords in plain text.
- VLANS routing.
- Creation of banners.
- Address translation with NAT and PAT.
- Assignment of descriptive names to the teams.

DESARROLLO DEL TRABAJO

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

1. ESCENARIO 1

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.

TOPOLOGIAS

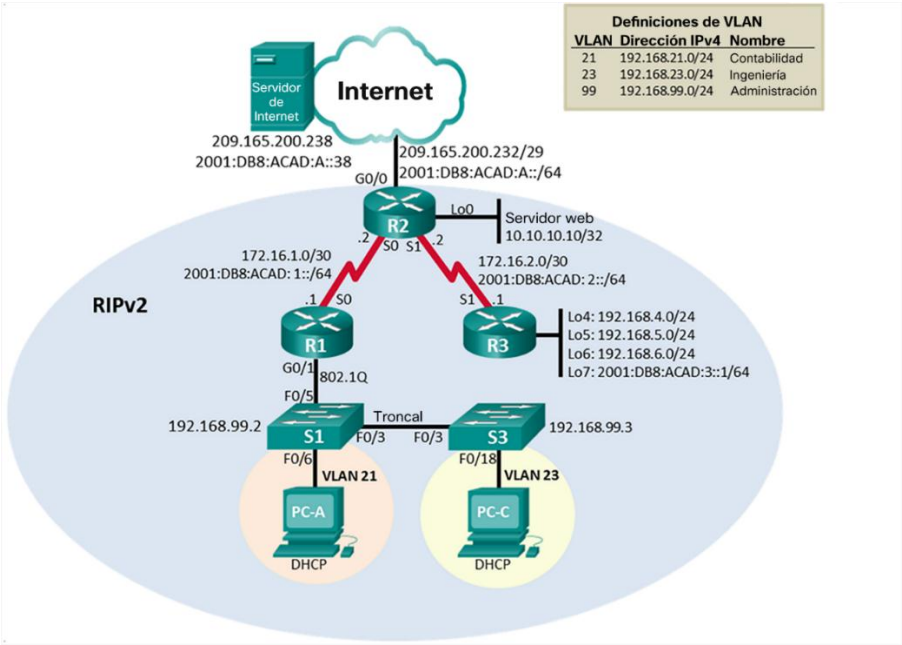


Figura 1. Topología escenario 1

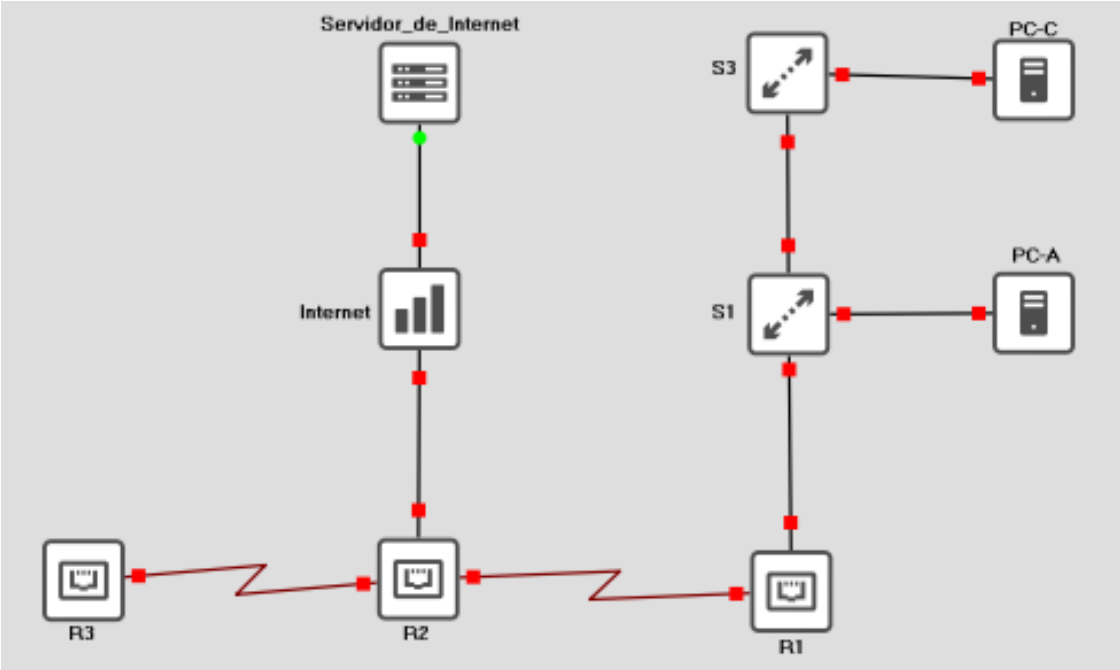


Figura 2. Topología 2 escenario 1

Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches.

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

R1, R2, R3

Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]

S1,S3

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Configurar los parámetros básicos de los dispositivos

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):

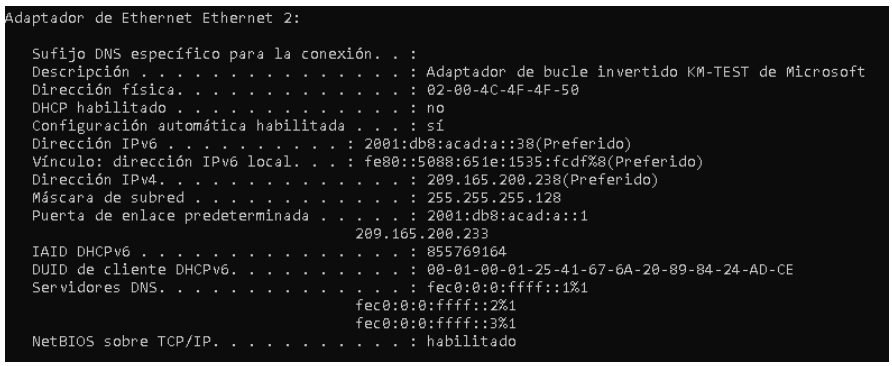


Figura 3. Configuración de computadora Internet

Configurar R1

R1(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 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 @ Se prohibe el acceso no autorizado @
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.12.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#clock rate 128000
R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#
```

Configurar R2

```
R2(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line con 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)#ip http server
R2(config)#ip http secure-server
R2(config)#banner motd @ Se prohibe el acceso no autorizado @
R2(config)#int s0/0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#clock rate 128000
R2(config-if)# no shutdown
R2(config-if)#exit
R2(config)#int g0/0
R2(config-if)#description Connection to ISP
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R2(config-if)# no shutdown
R2(config-if)#exit
```

Configurar R3

```
R3(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line con 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 @ Se prohibe el acceso no autorizado @
R3(config)#int s0/0/1
R3(config-if)#description Connection to R2
R3(config-if)#ip address 172.16.23.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:23::1/64
R3(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R3(config-if)#exit
R3(config)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)# no shutdown
R3(config)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)# no shutdown
R3(config)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)# no shutdown
R3(config)#int loopback 7
R3(config-if)#ip address 192.168.7.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
```

Configurar S1

```
Switch(config)#hostname S1
S1(config)#no ip domain lookup
```

```
S1(config)#enable secret class
S1(config)#line con 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 @ Se prohbe el acceso no autorizado @
S1(config)#
```

Configurar S3

```
Switch(config)#hostname S3
S3(config)#no ip domain lookup
S3(config)#enable secret class
S3(config)#line con 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 @ Se prohibe el acceso no autorizado @
```

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:

Tabla 1: Conectividad Routers y PC Internet

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

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

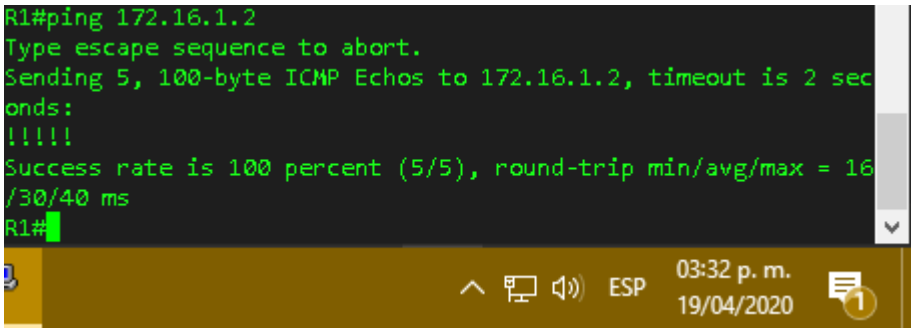


Figura 4. Ping de R1 a R2

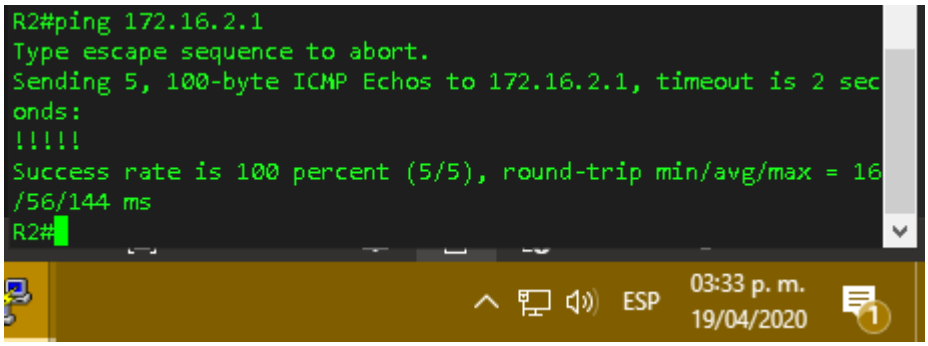


Figura 5. Ping de R2 a R3

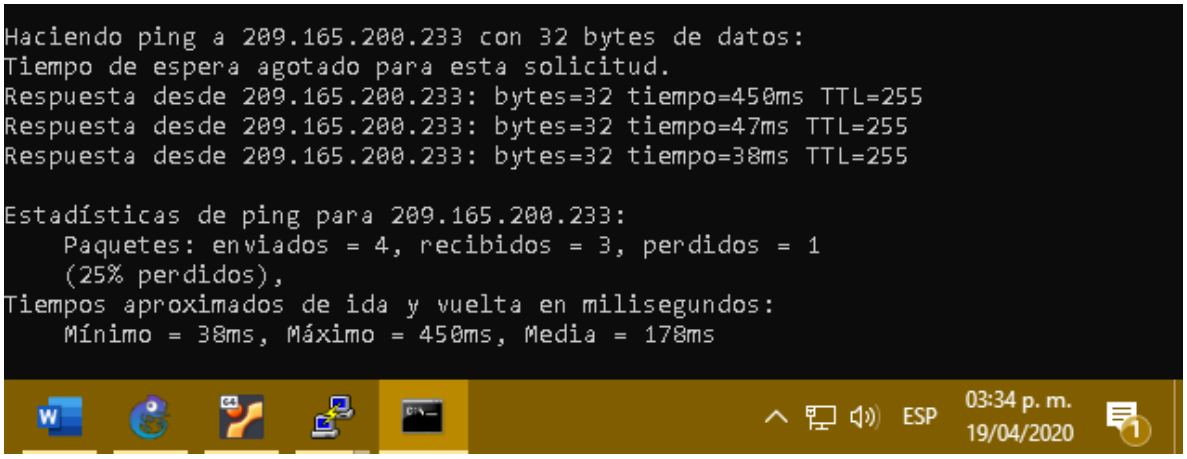


Figura 6. Ping de PC de Internet a Gateway Predeterminado

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

Configurar S1

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#
S1(config-vlan)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#interface F0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface F0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface range F0/1-2, F0/4, F0/6-24, G0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#
S1(config-if-range)#interface F0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#interface range F0/1-2, F0/4, F0/7-24, G0/1-2
S1(config-if-range)#shutdown
```

Configurar S3

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#
S1(config-vlan)#interface vlan 99
S1(config-if)#ip address 192.168.99.3 255.255.255.0
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#interface F0/3
S1(config-if)#switchport mode trunk
```

```
S1(config-if)#switchport trunk native vlan 1
S1(config-if)# interface range F0/1-2, F0/4, F0/6-24,G0/1-2
S1(config-if)#switchport mode access
S1(config-if-range)#interface F0/18
S1(config-if)#switchport access vlan 23
S1(config-if)#interface range F0/1-2, F0/4, F0/6-17,
F0/19-24, G0/1-2
S1(config-if-range)#shutdown
```

Configurar R1

```
R1(config)#interface g0/1.21
R1(config-subif)#description LAN de contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#interface g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#interface g0/1.99
R1(config-subif)#description Lan de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#interface g0/1
R1(config-if)#no shutdown
```

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:

Tabla 2: Verificación de la conectividad de la red

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

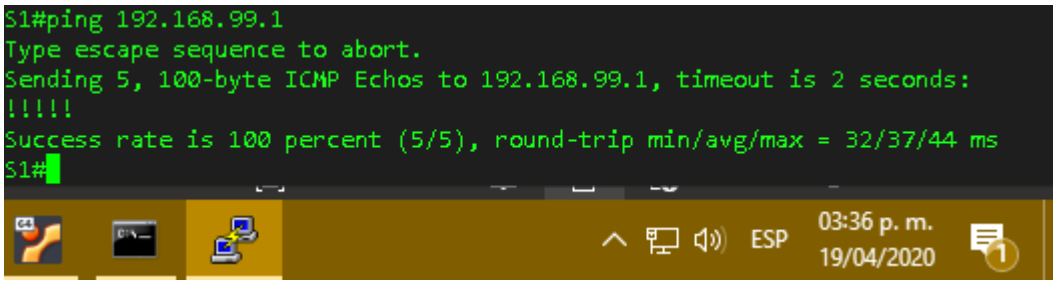


Figura 7 Ping de S1 a Gateway VLAN 99

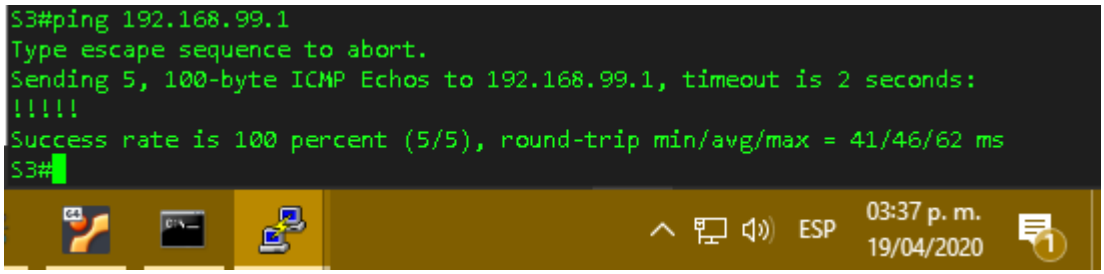


Figura 8. Ping de S3 a Gateway VLAN 99

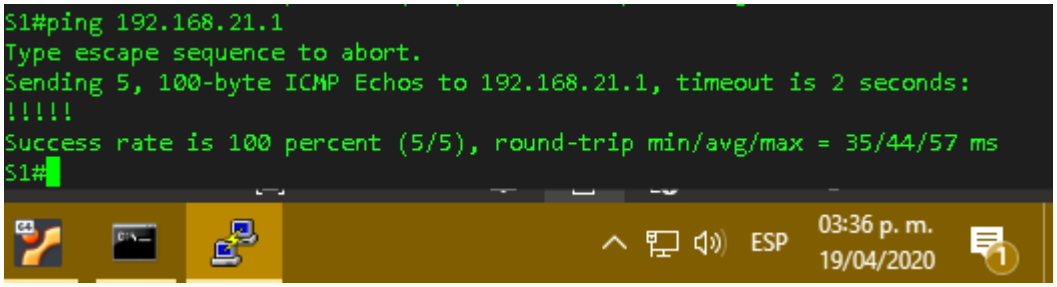


Figura 9. Ping de S1 a Gateway VLAN 21

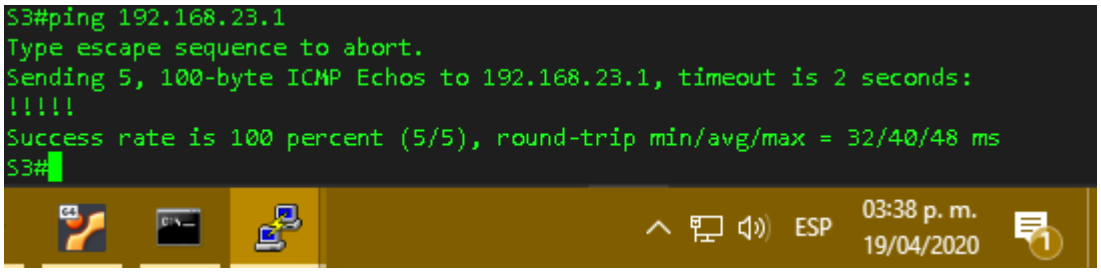


Figura 10. Ping de S3 a Gateway VLAN 23

Configurar el protocolo de routing dinámico RIPv2

Configurar RIPv2 en el R1

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary

Configurar RIPv2 en el R2

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 172.16.0.0
R2(config-router)#network 10.10.10.10
R2(config-router)#passive-interface lo0
R2(config-router)#no auto-summary

Configurar RIPv2 en el R3

R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 172.16.0.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6

R3(config-router)#no auto-summary

Verificar la información de RIP

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

Tabla 3: Verificar la información de RIP

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 rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run | section router RIP

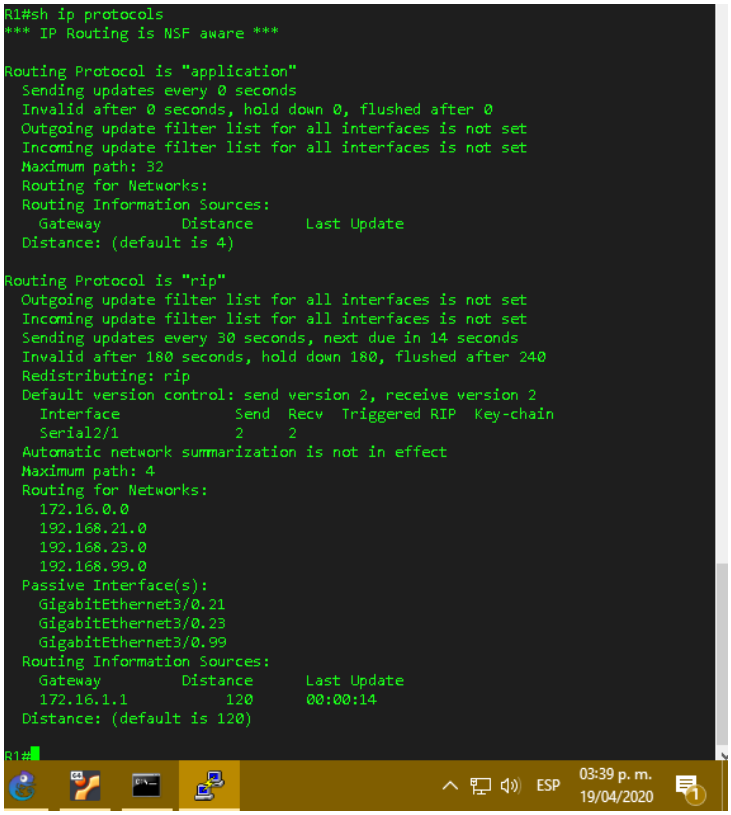


Figura 11. Protocolos de Enrutamiento R1

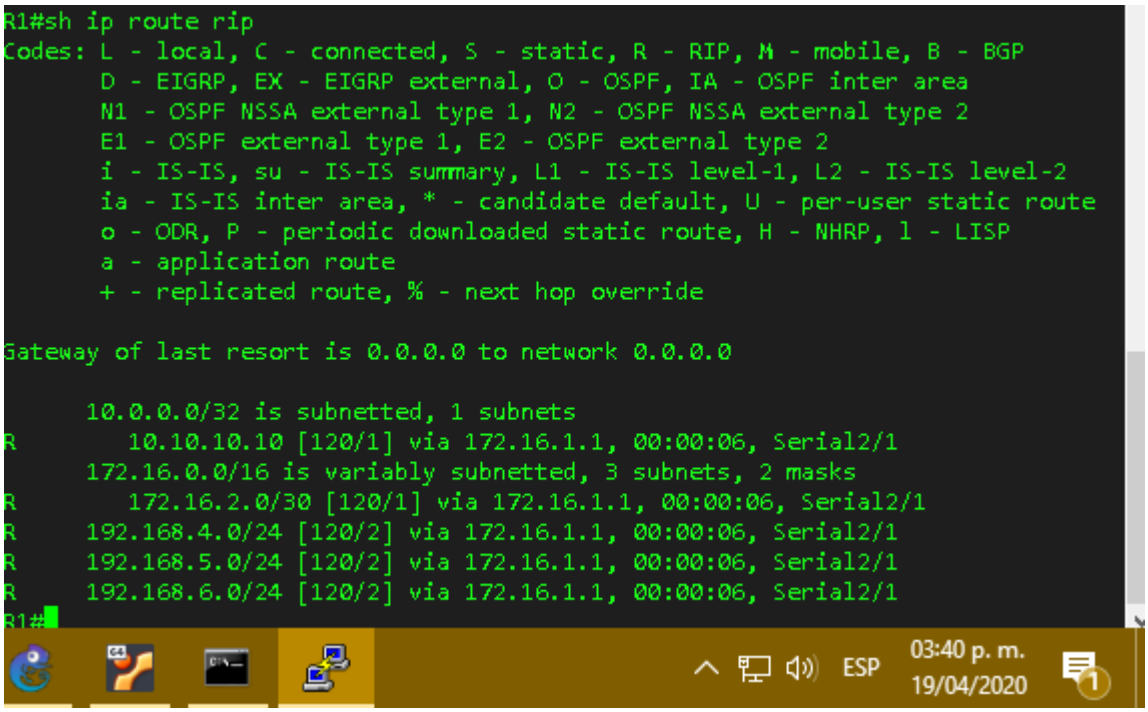


Figura 12. Tabla de enrutamiento RIP en R1

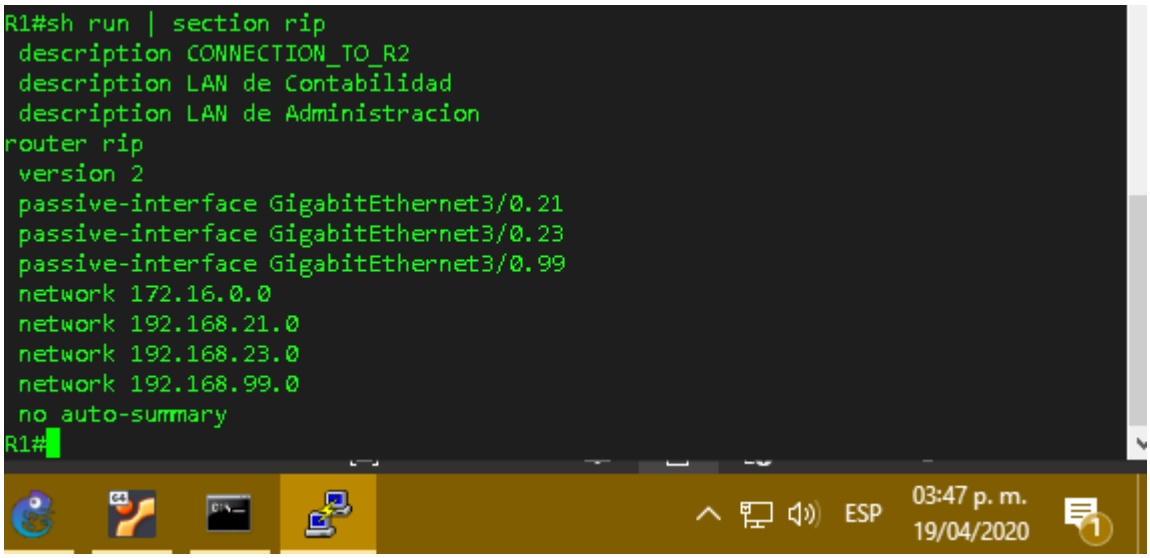


Figura 13. Sección RIP en R1

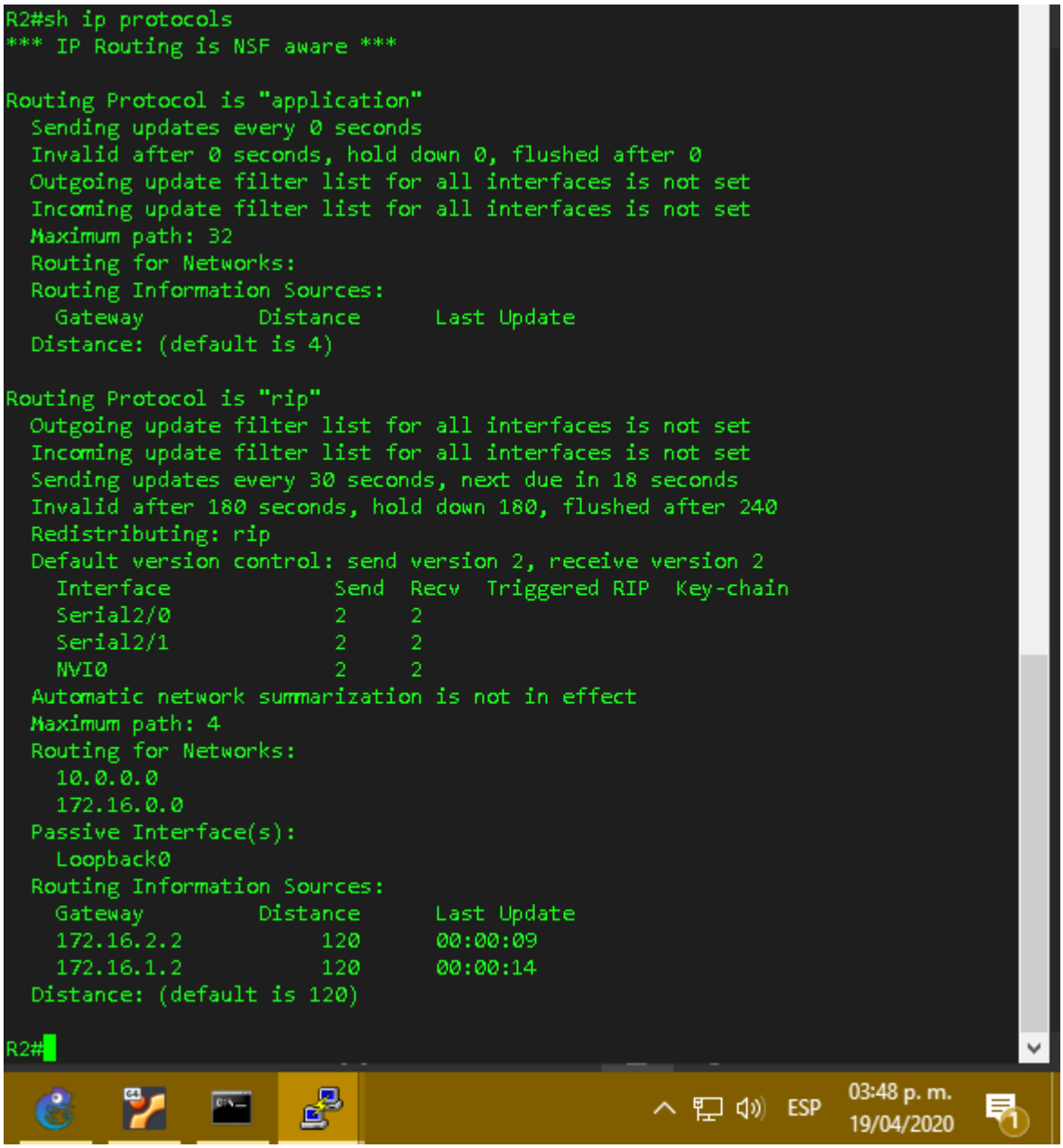


Figura 14. Protocolos de Enrutamiento R2

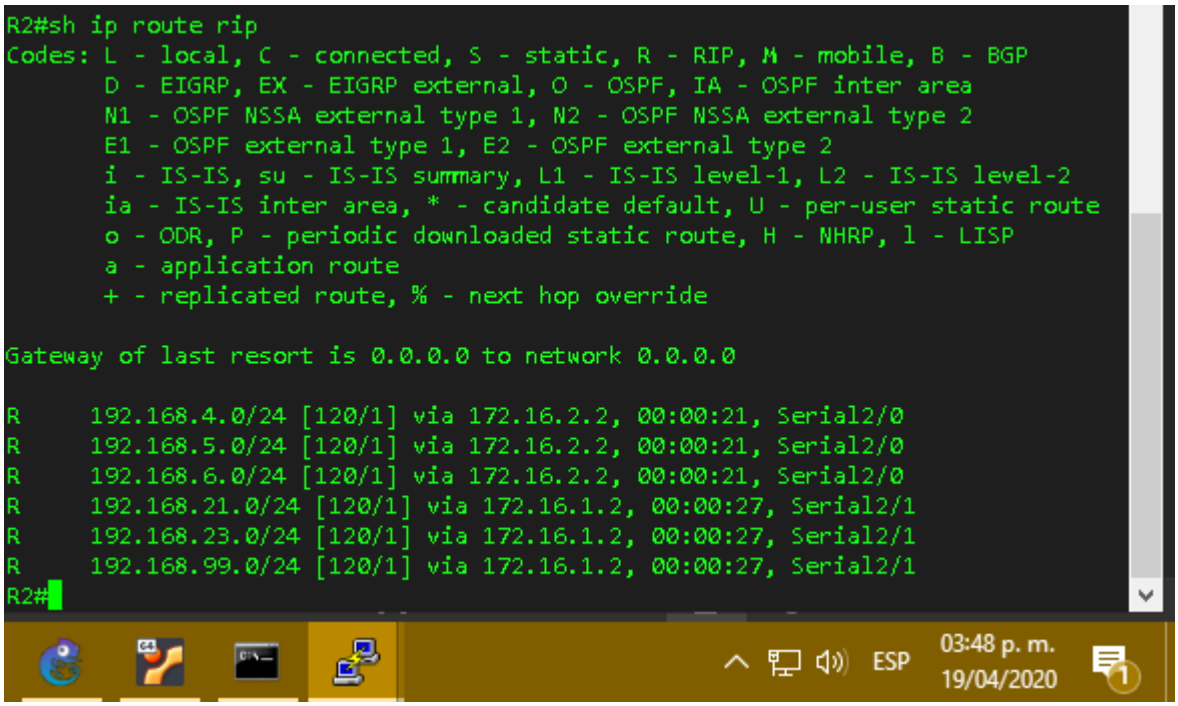


Figura 15. Tabla de enrutamiento RIP en R2

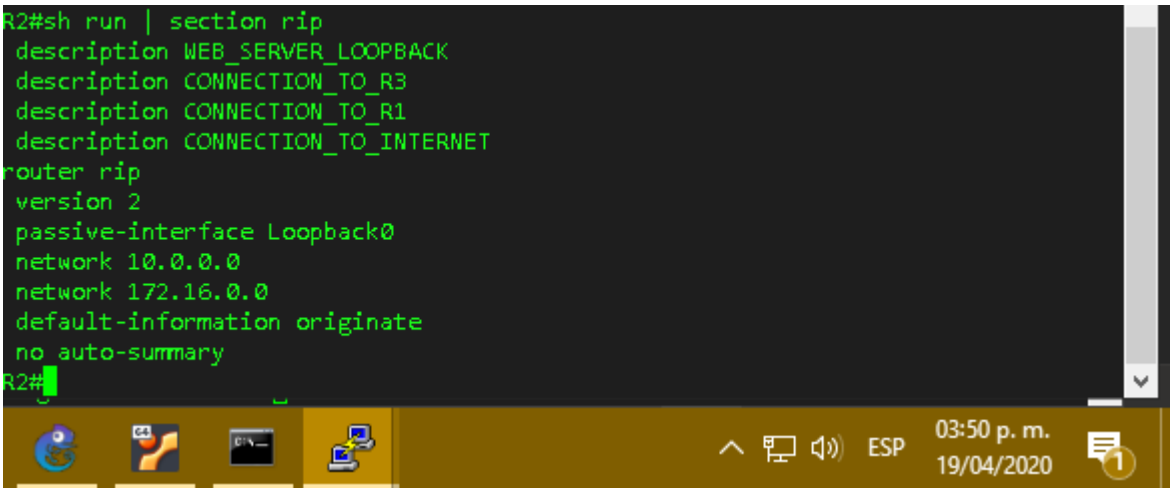


Figura 16. Sección de RIP en R2

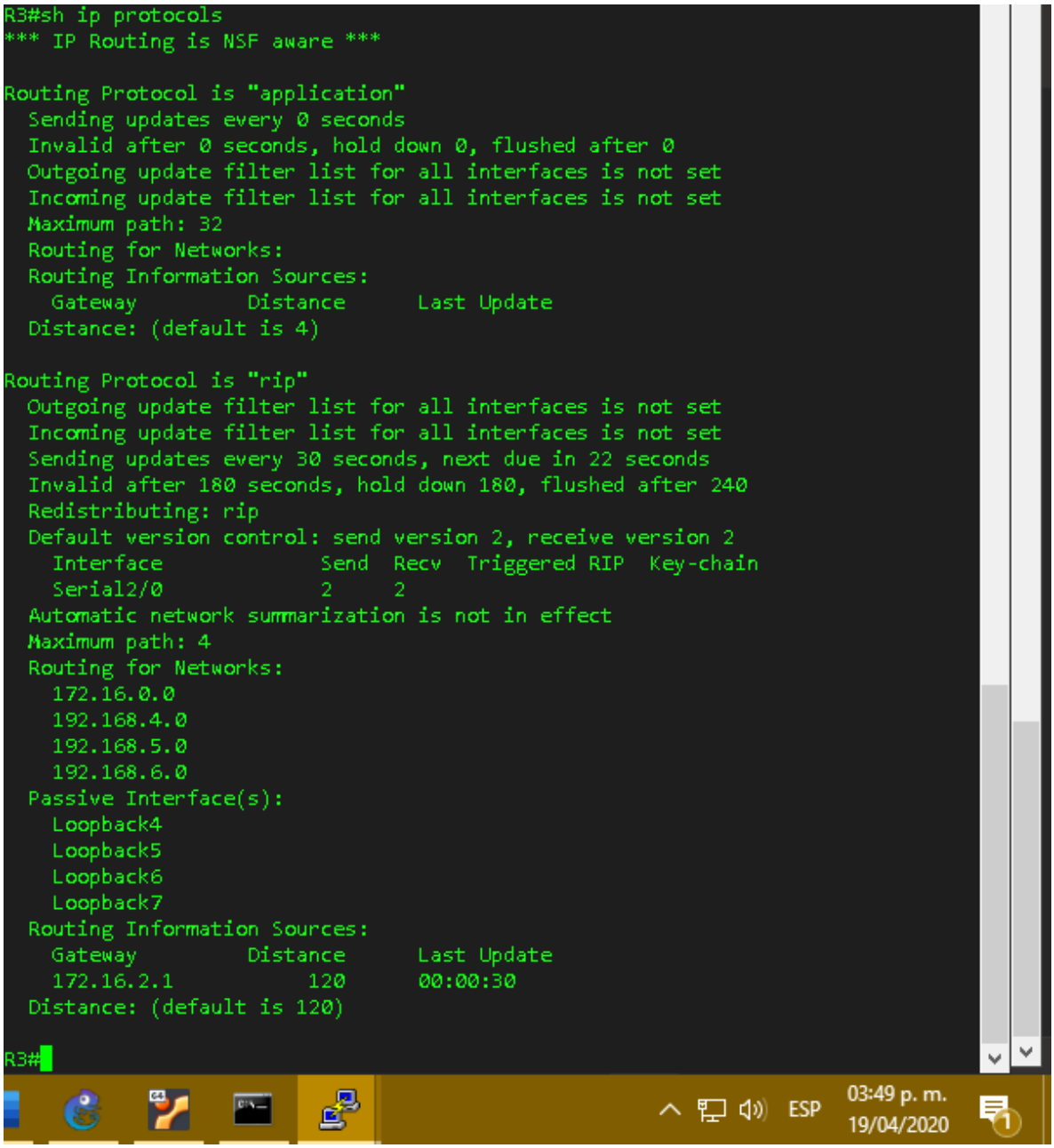


Figura 17. Protocolos de Enrutamiento R3

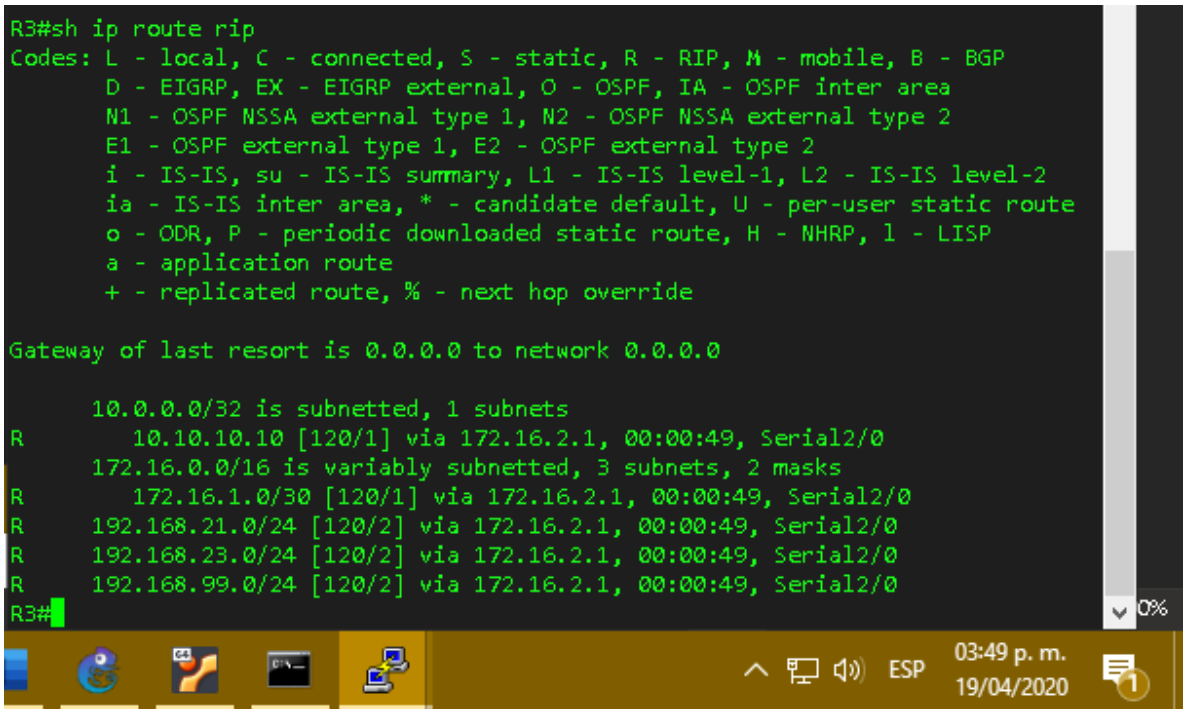


Figura 18. Tabla de enrutamiento RIP en R3

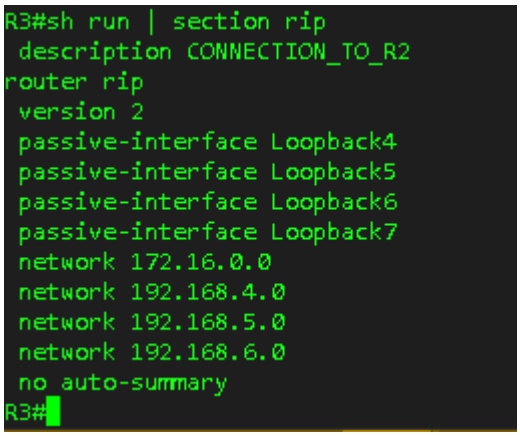


Figura 19. Sección RIP en R3

Implementar DHCP y NAT para IPv4

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

Configurar R1

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.31.0 255.255.255.0

```
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.31.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
```

Configurar la NAT estática y dinámica en el R2

```
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
R2(config)#ip http secure-server
R2(config)#ip http authentication local
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#interface lo0
R2(config-if)#ip nat inside
R2(config-if)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

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.

Tabla 4: Verificar DHCP y NAT estática

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 (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Exitoso

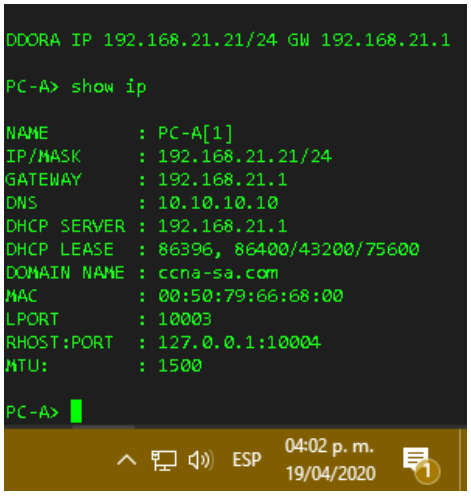


Figura 20. PC_A

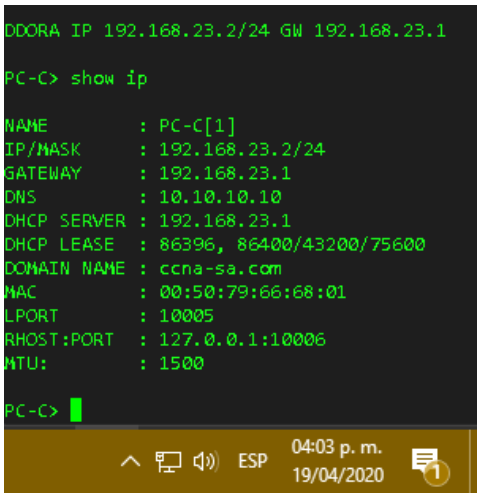


Figura 21. PC_C

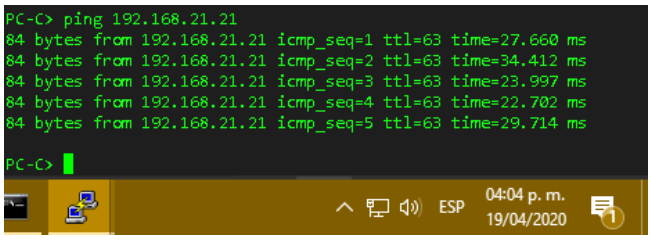


Figura 22. Ping de PC-A a PC-C

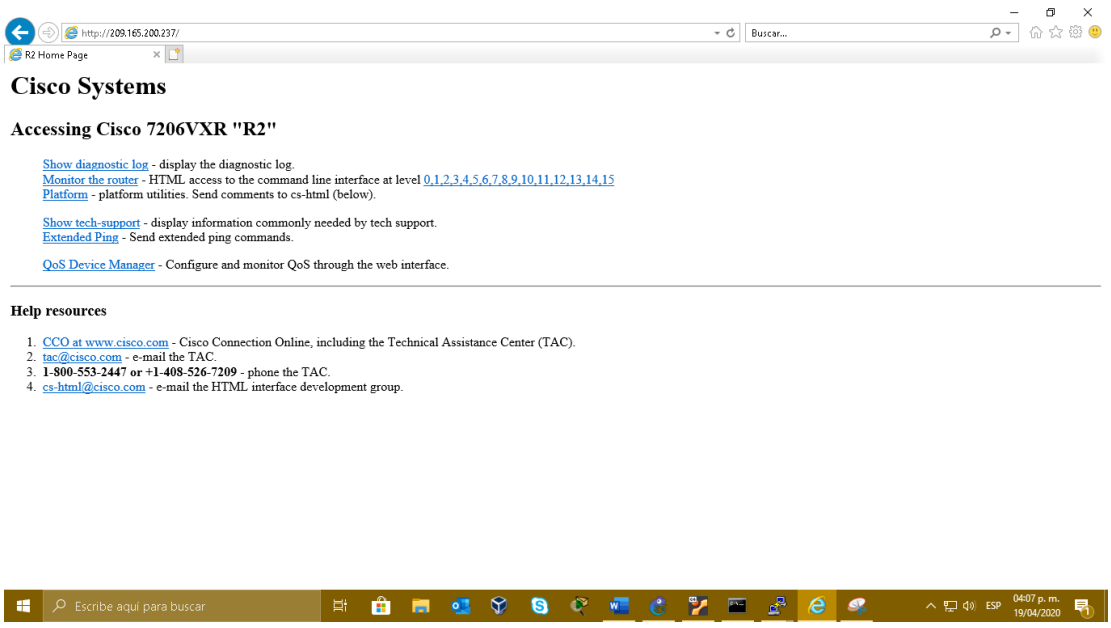


Figura 23. Navegador Web

Configurar NTP

Configurar R2

R2# clock set 9:00:00 5 march 2016

R2(config)# ntp master 5

Configurar R1

R1(config)# ntp server 172.16.1.2

R1 (config)# ntp update-calendar

R1# show ntp associations

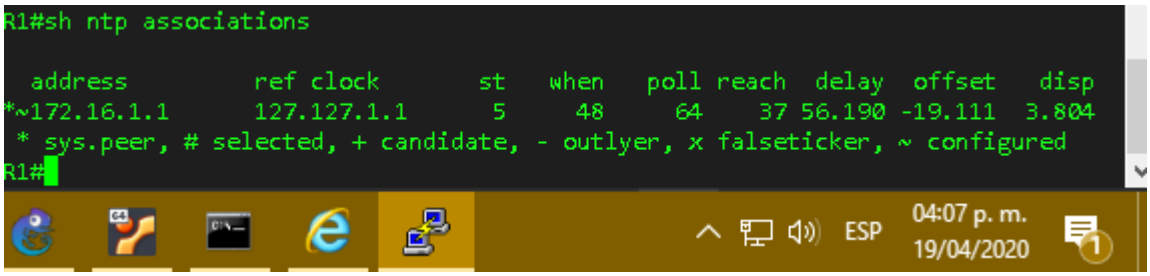


Figura 24. Asociaciones NTP en R1

Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

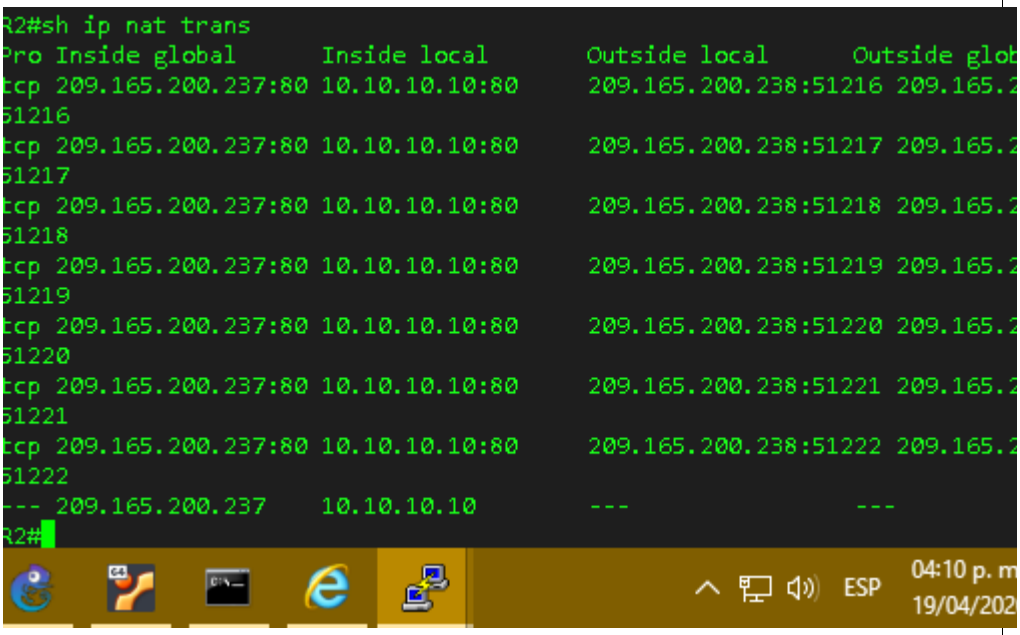
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet

Figura 25. Telnet a R2

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

Tabla 5: Detalles de Comandos

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  Figura 26. Listas de acceso en R2
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface

¿Con qué comando se muestran las traducciones NAT?	show ip nat translations  Figura 27. Traducciones en R2 **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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translation *

2. 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.

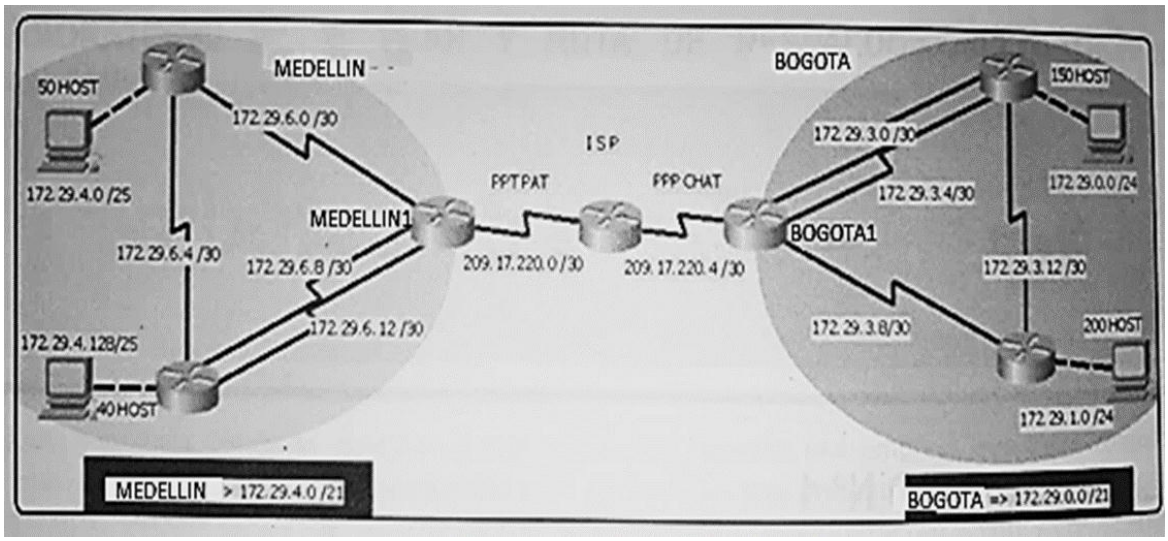


Figura 28. Topología 1 Escenario 2

Este escenario 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.
- 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).

MEDELLIN1

Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#enable secret class
MEDELLIN1 (config)#line con 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 : Se prohíbe el acceso no autorizado :

MEDELLIN2

Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#enable secret class
MEDELLIN2 (config)#line con 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 : Se prohíbe el acceso no autorizado :

MEDELLIN3

Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#enable secret class
MEDELLIN3 (config)#line con 0
MEDELLIN3 (config-line)#password cisco
MEDELLIN3 (config-line)#login
MEDELLIN3 (config-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 : Se prohíbe el acceso no autorizado :

ISP

Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP (config)#enable secret class
ISP (config)#line con 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 : Se prohíbe el acceso no autorizado :

BOGOTA1

Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA1
BOGOTA1 (config)#enable secret class
BOGOTA1 (config)#line con 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 : Se prohíbe el acceso no autorizado :

BOGOTA2

Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA2
BOGOTA2 (config)#enable secret class
BOGOTA2 (config)#line con 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 : Se prohíbe el acceso no autorizado :

BOGOTA3

Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA3
BOGOTA3 (config)#enable secret class
BOGOTA3 (config)#line con 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 : Se prohíbe el acceso no autorizado :

CONFIGURACIÓN DEL ENRUTAMIENTO

Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarizacion automática.

MEDELLIN1

MEDELLIN1 (config)#router ospf 1
MEDELLIN1 (router-config)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1 (router-config)#network 172.29.6.8 0.0.0.3 area 0

MEDELLIN1 (router-config)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1 (router-config)#network 209.17.220.0 0.0.0.3 area 0

MEDELLIN2

MEDELLIN2 (config)#router ospf 1
MEDELLIN2 (router-config)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN2 (router-config)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2 (router-config)#network 172.29.6.4 0.0.0.3 area 0

MEDELLIN3

MEDELLIN3(config)#router ospf 1
MEDELLIN3(router-config)#network 172.29.4.128 0.0.0.127 area 0
MEDELLIN3(router-config)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(router-config)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN3(router-config)#network 172.29.6.12 0.0.0.3 area 0

ISP

ISP(router)#router ospf 1
ISP(router-config)#network 209.17.220.0 0.0.0.3 area 0
ISP(router-config)#network 209.17.220.4 0.0.0.3 area 0

BOGOTA1

BOGOTA1(router)#router ospf 1
BOGOTA1(router-config)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(router-config)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(router-config)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(router-config)#network 209.17.220.4 0.0.0.3 area 0

BOGOTA2

BOGOTA2(router)#router ospf 1
BOGOTA2(router-config)#network 172.29.1.0 0.0.0.255 area 0
BOGOTA2(router-config)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA2(router-config)#network 172.29.3.12 0.0.0.3 area 0

BOGOTA3

BOGOTA3(router)#router ospf 1
BOGOTA3(router-config)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA3(router-config)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA3(router-config)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA3(router-config)#network 172.29.3.12 0.0.0.3 area 0

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.

BOGOTA1
BOGOTA1(router)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
BOGOTA1(router)#router ospf 1
BOGOTA1(router-config)#redistribute static subnets

MEDELLIN1
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
MEDELLIN1(config)#router ospf 1
MEDELLIN1(router-config)#redistribute static subnets

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.

ISP
ISP(config)#ip route 172.29.4.0 255.255.252.0 Serial0/3/0
ISP(config)#ip route 172.29.4.128 255.255.255.128 Serial0/3/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 Serial0/3/1
ISP(config)#ip route 172.29.0.0 255.255.252.0 Serial0/3/1

Tabla de Enrutamiento.

Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

ISP

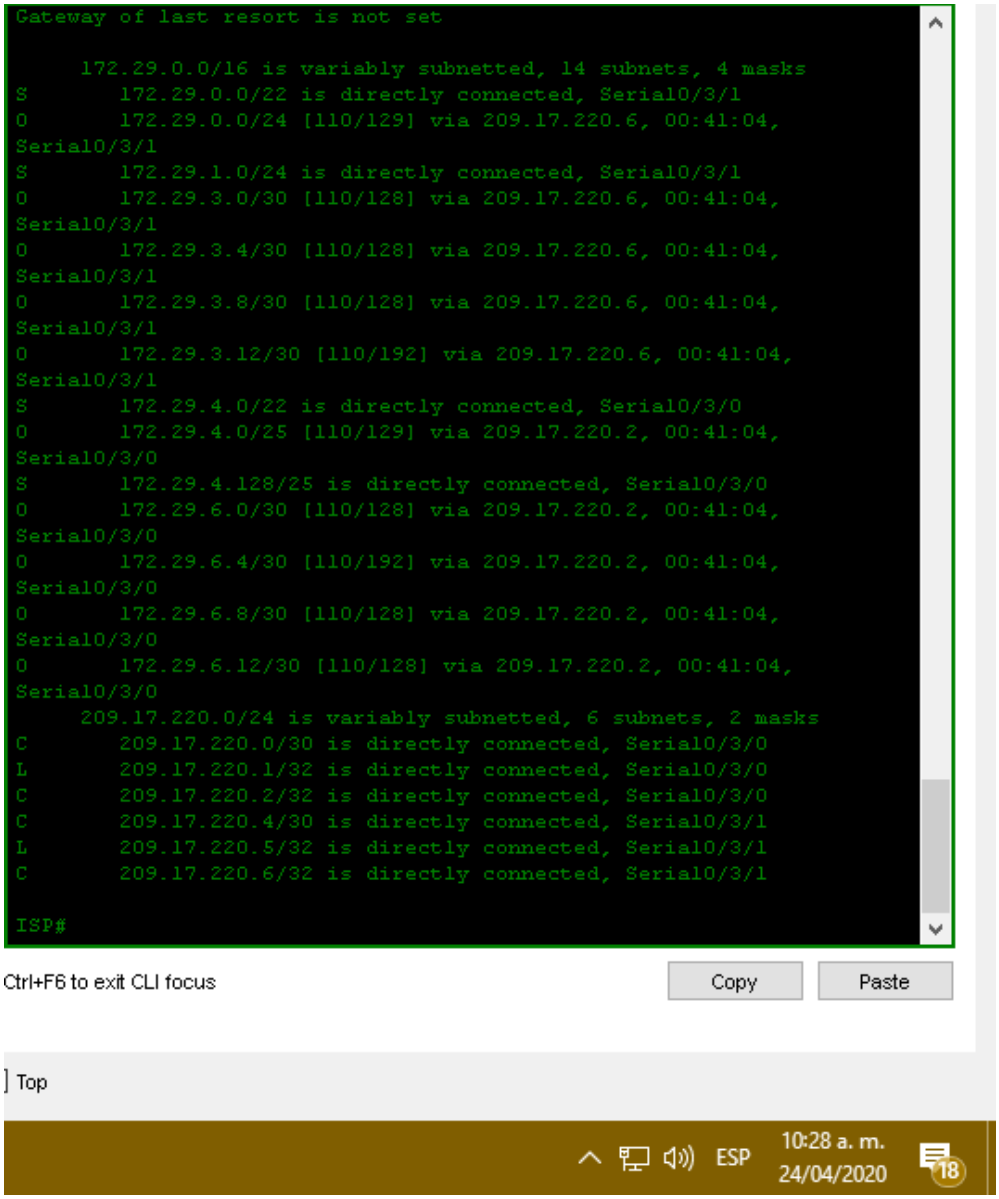


Figura 29. Tabla de enrutamiento ISP

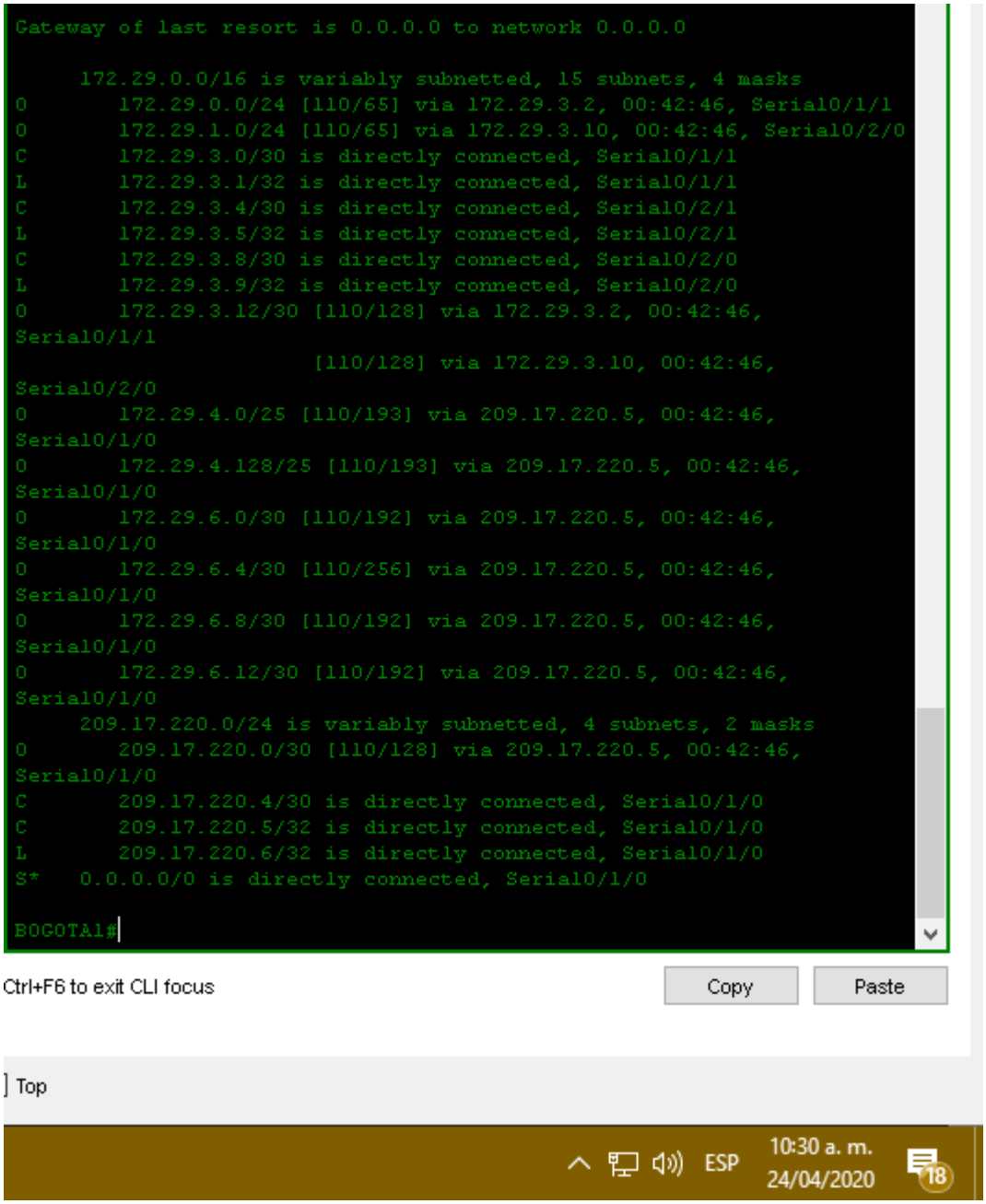


Figura 30. Tabla de enrutamiento BOGOTA1

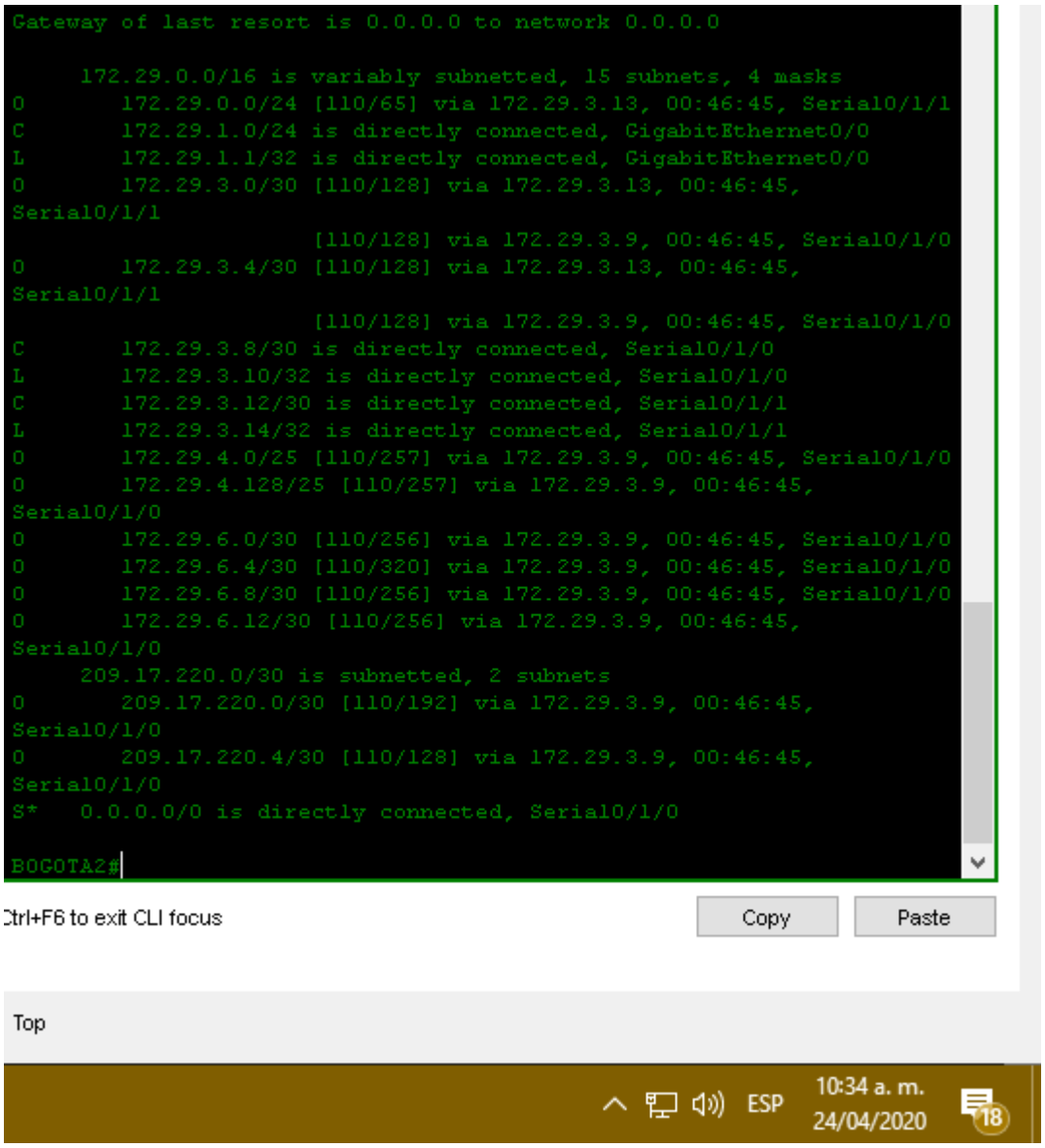


Figura 31. Tabla de enrutamiento BOGOTA2

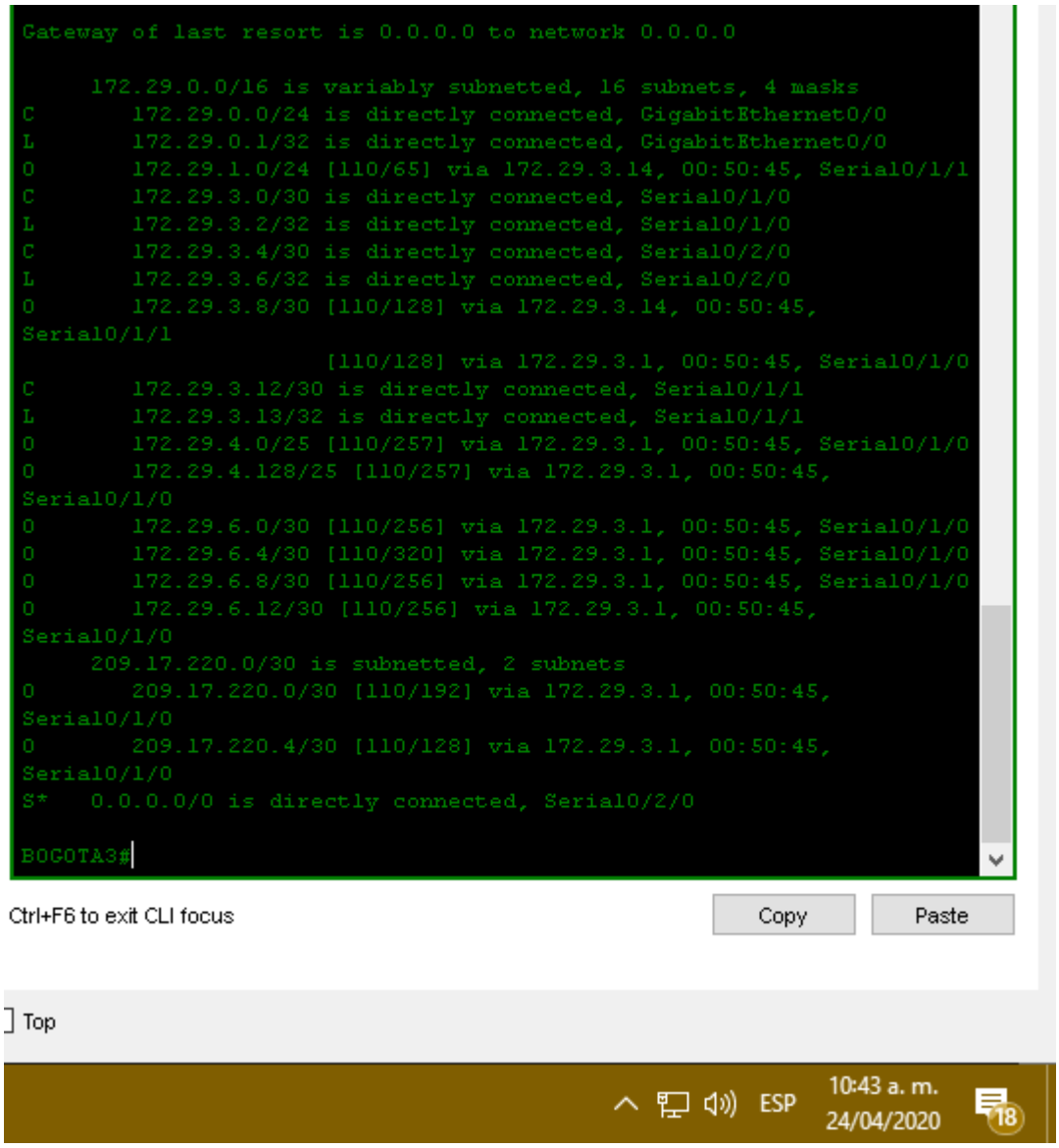


Figura 32. Tabla de enrutamiento BOGOTA3

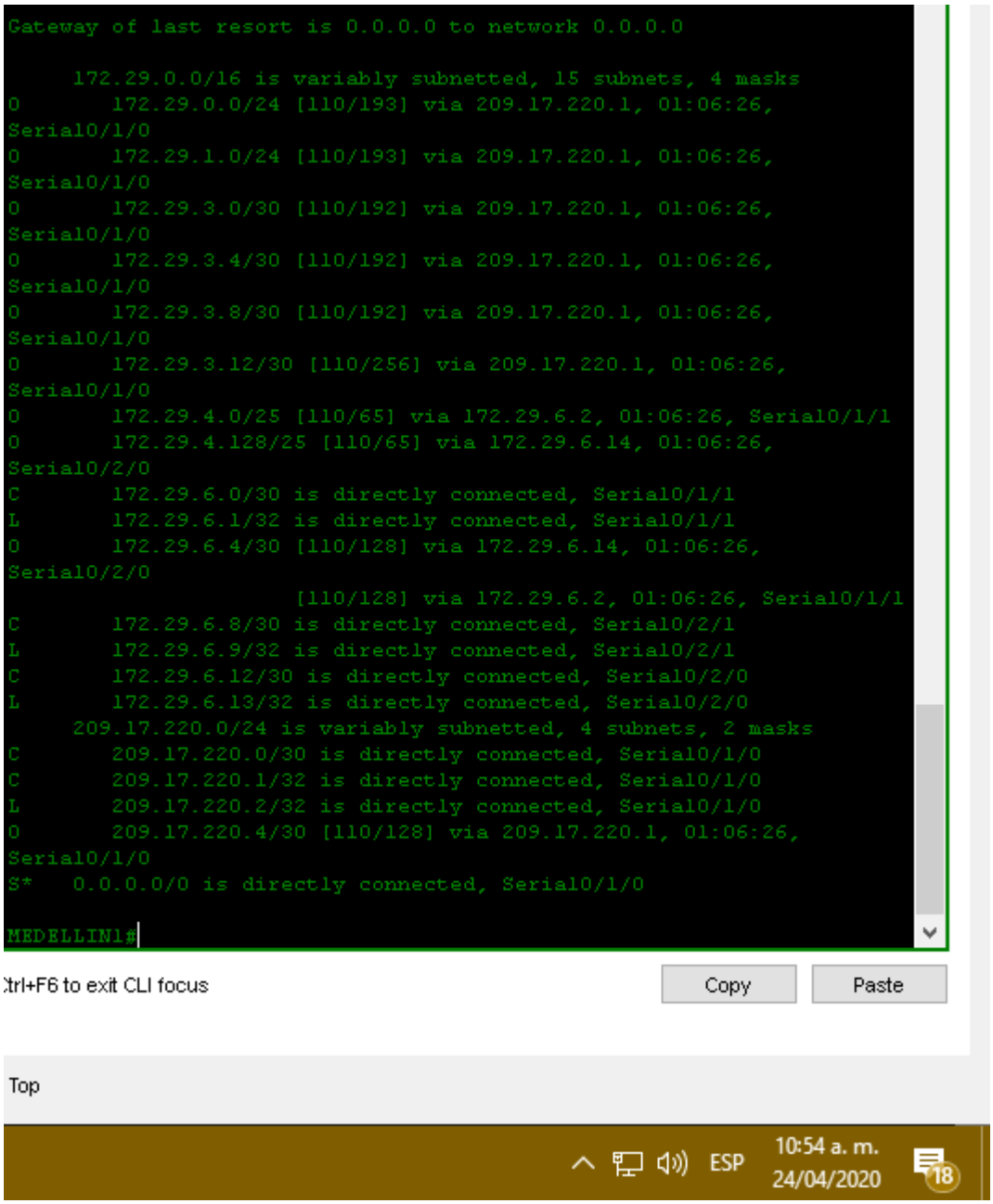


Figura 33. Tabla de enrutamiento MEDELLIN1

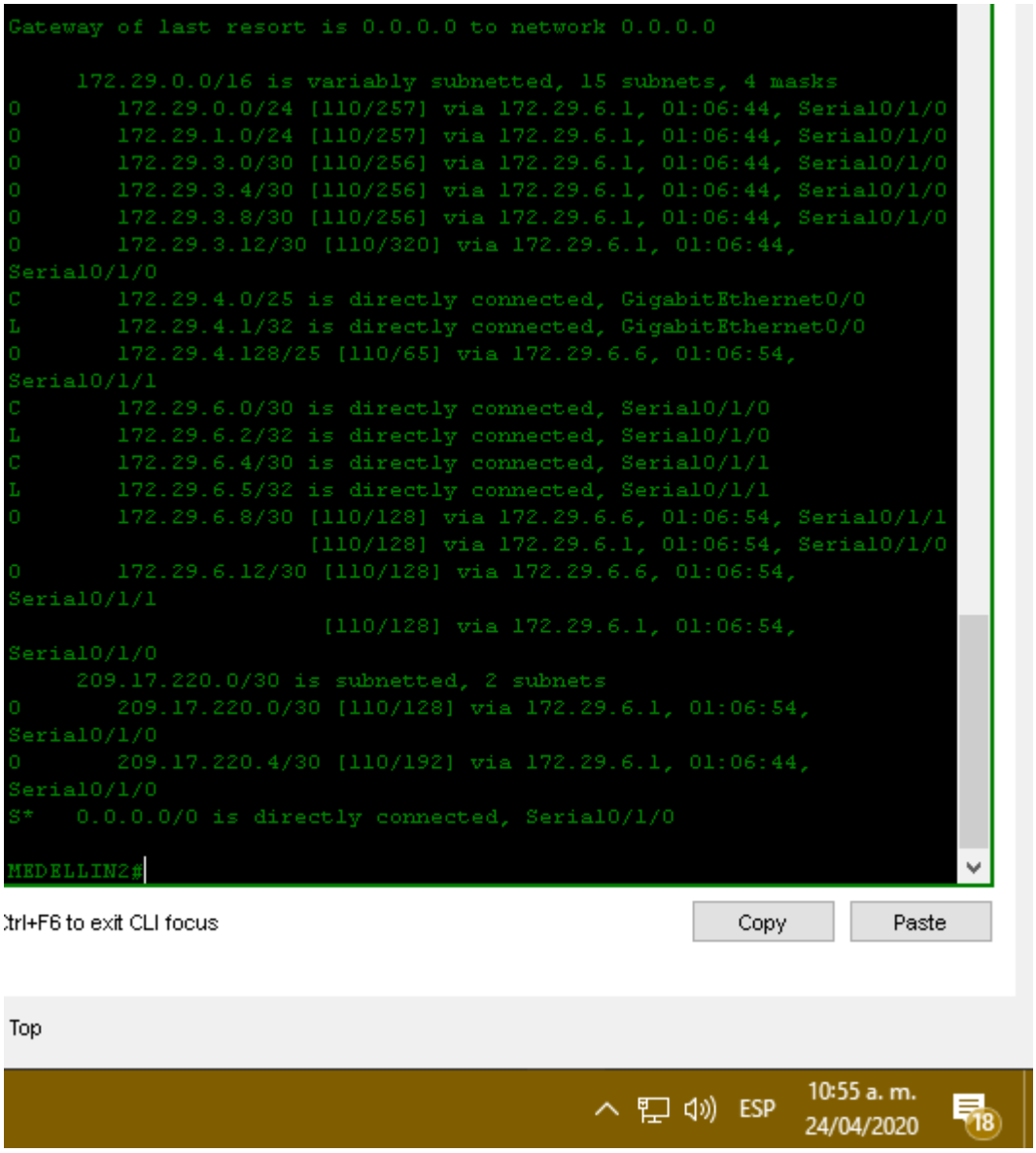


Figura 34. Tabla de enrutamiento MEDELLIN2

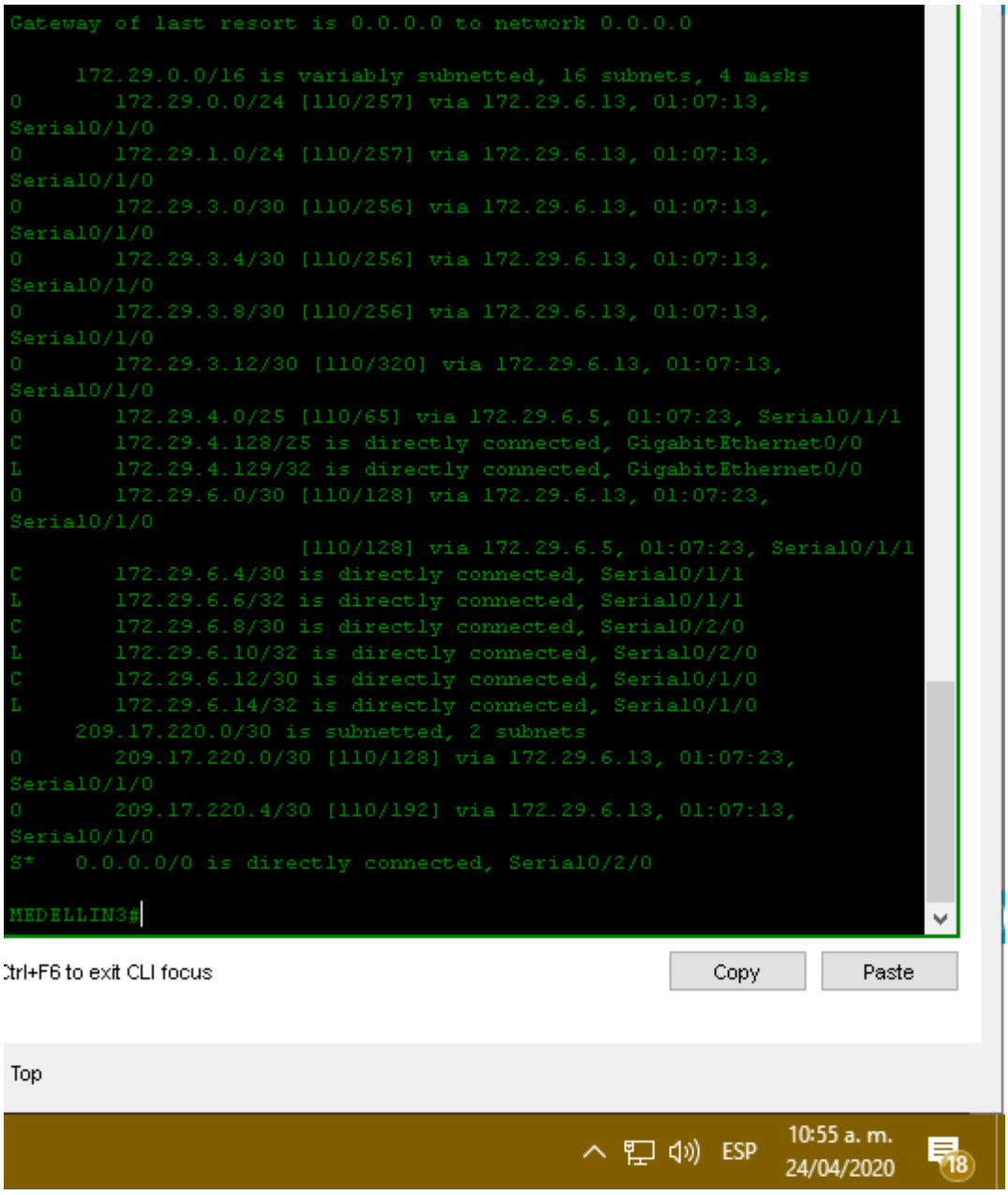


Figura 35. Tabla de enrutamiento MEDELLIN3

Deshabilitar la propagación del protocolo OSPF.

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.

BOGOTA1

BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface s0/2/1

BOGOTA2

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface ss0/2/1

MEDELLIN2

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0

MEDELLIN3

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0

Verificación del protocolo OSPF.

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.

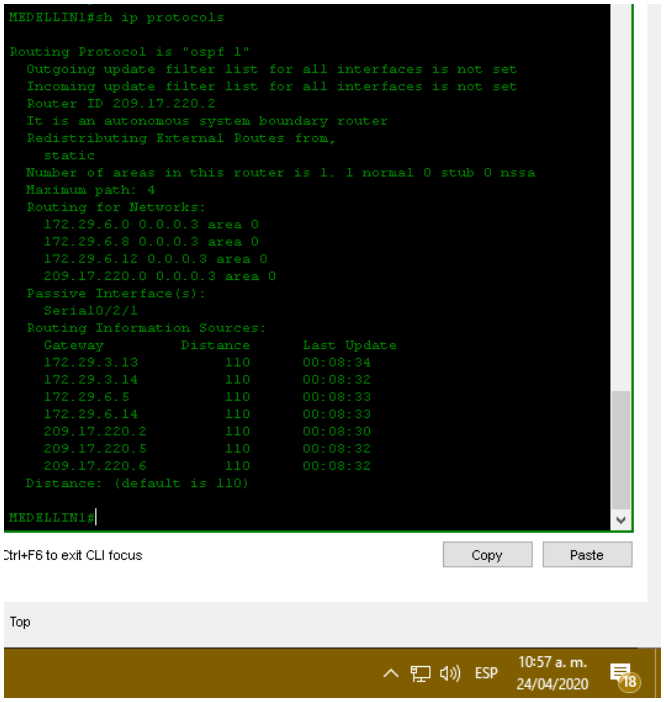


Figura 36. Protocolo OSPF en MEDELLIN1

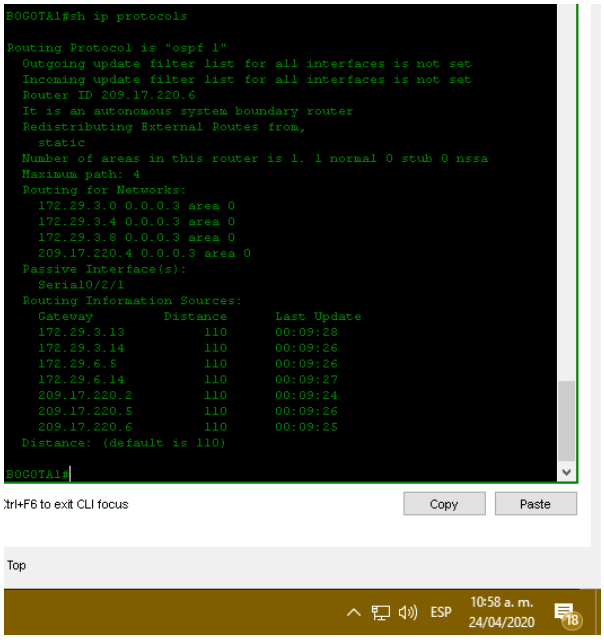


Figura 37. Protocolo OSPF en BOGOTA1

Configurar encapsulamiento y autenticación PPP.
a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

MEDELLIN 1

```
MEDELLIN1(config)#username ISP secret ISP
MEDELLIN1(config)#interface Serial0/1/0
MEDELLIN1(config)#encapsulation ppp
MEDELLIN1(config)#ppp authentication pap
MEDELLIN1(config)#ppp pap sent-username MEDELLIN1 password MEDELLIN
```

ISP

```
ISP(config)#username BOGOTA1 secret BOGOTA1
ISP(config)#username MEDELLIN1 secret MEDELLIN1
ISP(config)#interface Serial0/3/0
ISP(config)#encapsulation ppp
ISP(config)#ppp authentication pap
ISP(config)#ppp pap sent-username ISP password ISP
ISP(config)#no keepalive
ISP(config)#interface Serial0/3/1
ISP(config)#encapsulation ppp
ISP(config)#ppp authentication chap
ISP(config)#no keepalive
```

BOGOTA1

```
BOGOTA1(config)#username ISP secret ISP
BOGOTA1(config)#interface Serial0/1/0
BOGOTA1(config)#encapsulation ppp
BOGOTA1(config)#ppp authentication chap
```

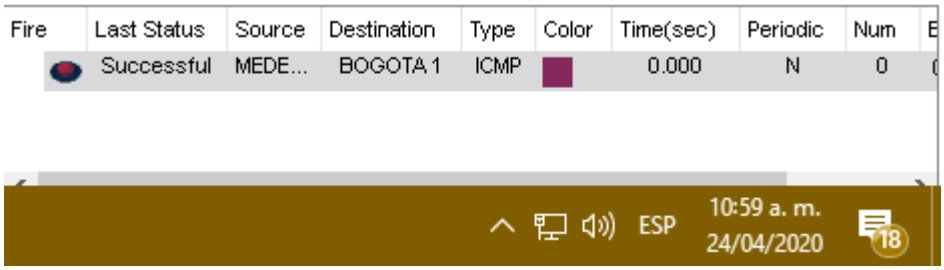


Figura 38. Ping de MEDELLIN1 a BOGOTA1

Configuración de PAT.

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.

MEDELLIN1

```
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config)#ip nat inside source list HOST interface Serial0/1/0 overload
MEDELLIN1(config)#interface Serial0/1/0
MEDELLIN1(config)#ip nat outside
MEDELLIN1(config)#interface Serial0/1/1
MEDELLIN1(config)#ip nat inside
MEDELLIN1(config)#interface Serial0/2/0
MEDELLIN1(config)#ip nat inside
MEDELLIN1(config)#interface Serial0/2/1
MEDELLIN1(config)#ip nat inside
```

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.

BOGOTA1

```
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config)#ip nat inside source list HOST interface Serial0/1/0 overload
BOGOTA1(config)#interface Serial0/1/0
BOGOTA1(config)#ip nat outside
BOGOTA1(config)#interface Serial0/1/1
BOGOTA1(config)#ip nat inside
BOGOTA1(config)#interface Serial0/2/0
BOGOTA1(config)#ip nat inside
BOGOTA1(config)#interface Serial0/2/1
BOGOTA1(config)#ip nat inside
```

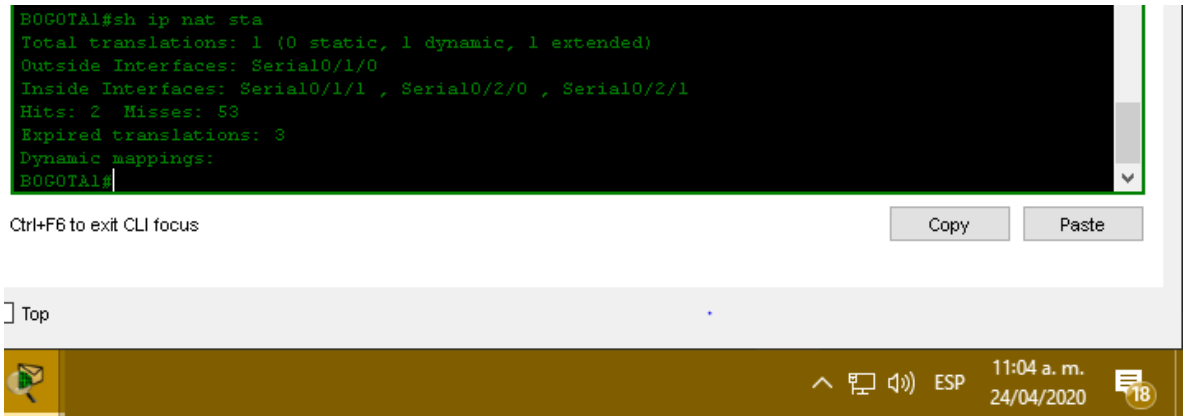


Figura 39. Traducciones en BOGOTA1

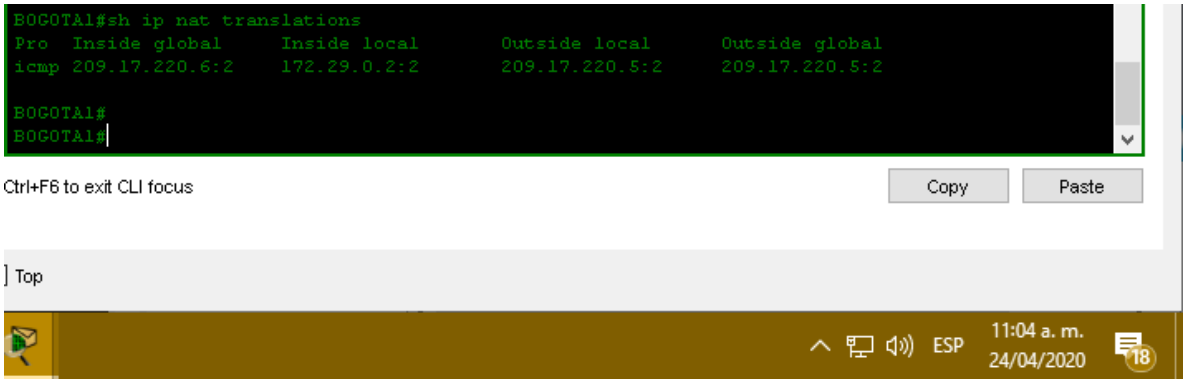


Figura 40. Traducciones_2 en BOGOTA1

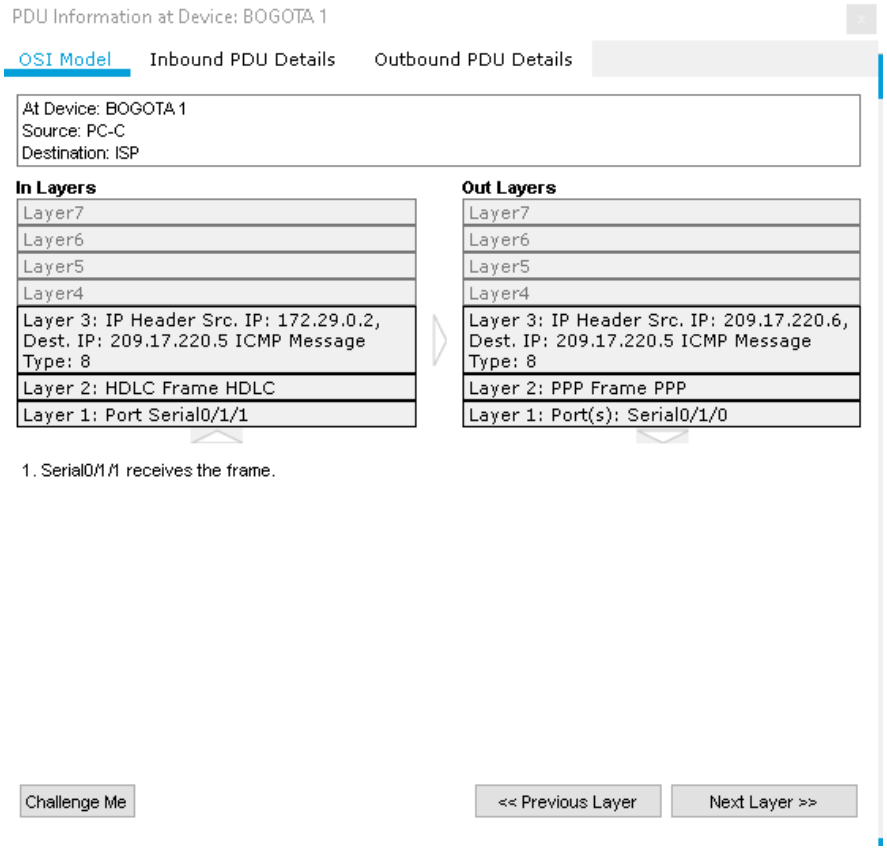


Figura 41. Traducciones_3 en BOGOTA1

Configuración del servicio DHCP.

Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

MEDELLIN2

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(config)#default-router 172.29.4.1
MEDELLIN2(config)#dns-server 8.8.4.4
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(config)#default-router 172.29.4.129
MEDELLIN2(config)#dns-server 8.8.4.4
MEDELLIN2(config)#ip dhcp pool BOGOTA2

MEDELLIN2(config)#network 172.29.0.0 255.255.255.0
MEDELLIN2(config)#default-router 172.29.0.1
MEDELLIN2(config)#dns-server 8.8.8.8
MEDELLIN2(config)#ip dhcp pool BOGOTA3
MEDELLIN2(config)#network 172.29.1.0 255.255.255.0
MEDELLIN2(config)#default-router 172.29.1.1
MEDELLIN2(config)#dns-server 8.8.8.8

El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

MEDELLIN3
MEDELLIN3(config)#interface GigabitEthernet0/0
MEDELLIN3(config)#ip helper-address 172.29.6.5

Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

BOGOTA2
interface GigabitEthernet0/0
ip helper-address 172.29.6.2

BOGOTA3
interface GigabitEthernet0/0
ip helper-address 172.29.6.2

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Medellin2.

BOGOTA1
Interface s0/2/0
ip helper-address 172.29.6.2

Interface s0/1/1
ip helper-address 172.29.6.2

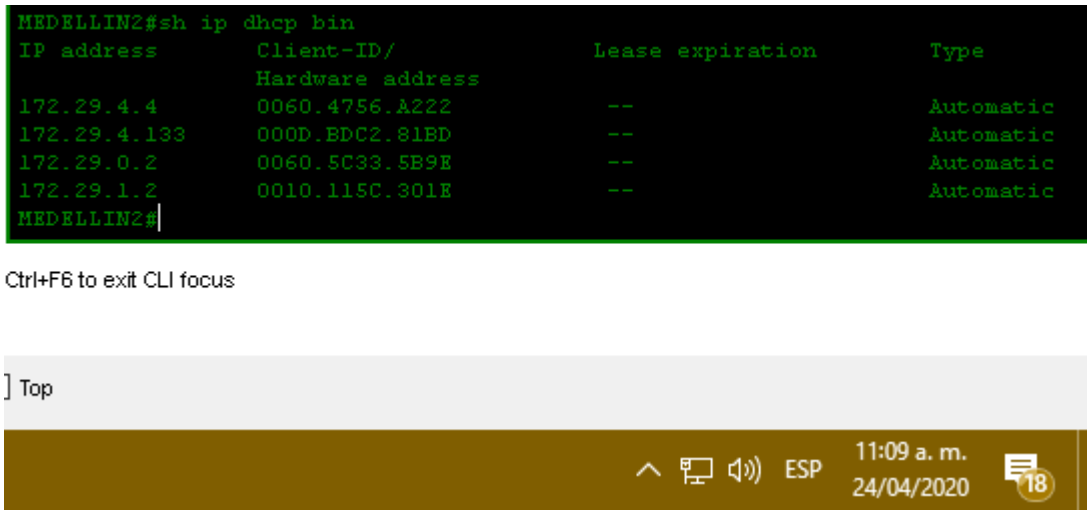


Figura 42. Asociaciones DHCP en MEDELLIN2

CONCLUSIONES

Este documento proporciona la realización de la actividad “prueba de habilidades práctica final”, acorde a las indicaciones establecidas y conocimiento adquirido mediante el material otorgado por la compañía CISCO, mediante sus ambientes virtuales. En el caso de estudio se ha logrado con éxito la configuración y conexión de los equipos, como Routers y Switches.

Cuando desarrollamos el ensayo de habilidades, definimos que hay varios tipos de protocolos que nos ayudan a programar las diferentes direcciones IP, interfaces y dispositivos que pueden constituir una red. Actualmente el diseño de una red es meticulosamente revisado. Existen varios factores que influyen para conseguir un buen esquema, entre ellos: la flexibilidad con respecto a los servicios soportados, la vida útil requerida, el tamaño del sitio y la cantidad de usuarios que estarán interconectados y los costos, entre otros.

En la actividad se efectuó de buena manera los protocolos de OSPF por lo cual se hizo un seguimiento estable de las conexiones; se observó también el servicio DHCP que asigna dinámicamente una dirección IP.

BIBLIOGRAFÍA

ALVAREZ, Alex. “Obtenido de Entre redes y servidores”. {En línea}. {5 mayo de 2020} disponible en: (https://alexalvarez0310.wordpress.com/category/listas-de-control-de-acceso-en-router-cisco/)

BEACKER SALAZAR, Steven y HERNANDEZ, Jhon Jader. “Sumarizacion de Rutas”. {En línea}. {5 mayo de 2020} disponible en: https://networksysolutionspkt.blogspot.com/p/sumarizacion-de-ruta.html

CALVO, Ángel. “aprende cómo configurar el protocolo (Parte 1)”. {En línea}. {7 mayo de 2020} disponible en: https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-y-sencilla/

CISCO. “Configuring IP Access Lists”. {En línea}. {7 mayo de 2020} disponible en: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html