PRUEBA DE HABILIDADES CCNA 2019

KATHERIN JULIET SANDOVAL GARZON

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD

INGENERIA DE SISTEMAS

CEAD BARRANQUILLA

BARRANQUILLA

2019

PRUEBA DE HABILIDADES CCNA 2019

KATHERIN JULIET SANDOVAL GARZON

Prueba de Habilidades Cisco

Jose Ignacio Cardona

UNIVERSIDAD NACIONAL Y A DISTANCIA UNAD

INGENERIA DE SISTEMAS

CEAD BARRANQUILLA

BARRANQUILLA

2019

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Barranquilla, 19 de Julio del 2019

Resumen

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.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

Tabla de contenido

Introducción

La certificación CCNA es un referente desde hace muchos años utilizado en el aprendizaje de las redes, no solo es utilizado por profesionales, sino también por institutos, universidades, y centros educativos de referencia para iniciar a las personas en el ámbito de las comunicaciones.

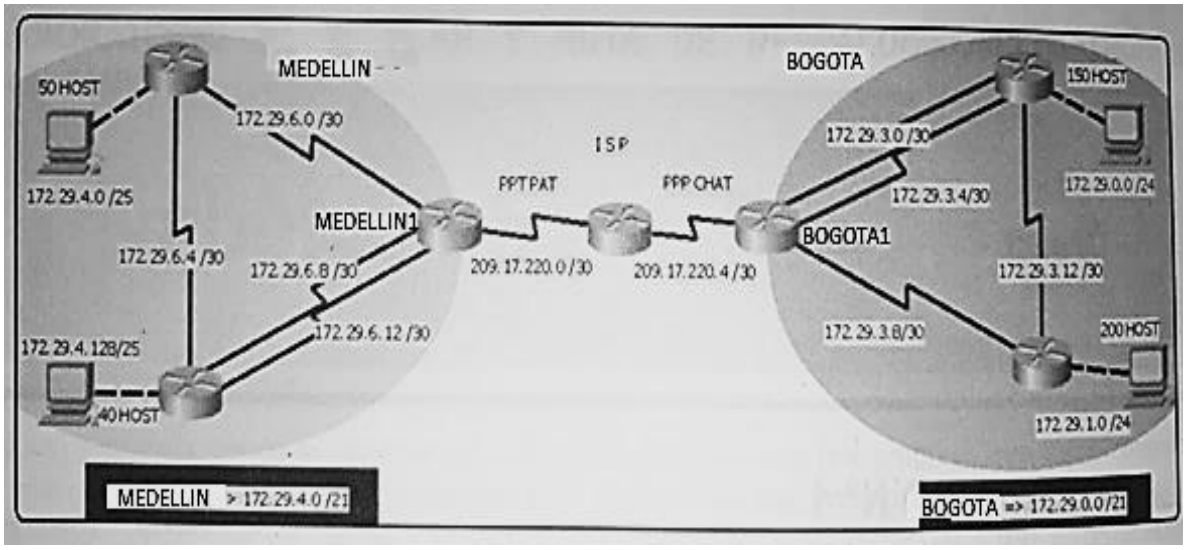
En este primer curso os presentamos un temario desarrollado a partir de los contenidos necesarios para superar la certificación CCNA 200-125 de Cisco (última actualización 2016) realizando un enfoque de aprendizaje y metodología totalmente diferente. Podréis entender de una manera entretenida y en poco tiempo todos los entresijos necesarios para realizar la certificación a través de contenido audiovisual. El objetivo principal es entender las redes desde un punto de vista real y práctico, trabajando de una manera lo más cercana posible a situaciones cotidianas de la profesión del ingeniero o técnico de redes.

Problema

Escenario 1

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 1 Topología de red



Este escenario plantea el uso de RIP 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.

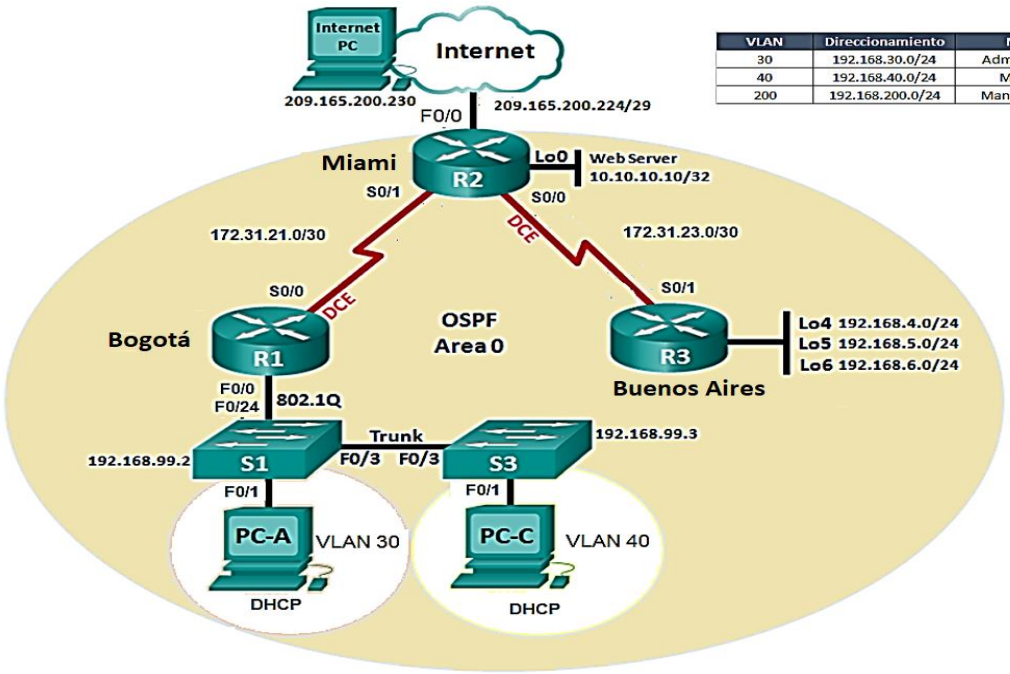
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Escenario 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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 2. Escenario 2



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

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

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios.

Justificación

La presente prueba de habilidades, se enfocará en dar solución a los escenarios propuestos y en los cuales estableceremos el direccionamiento IP, protocolos de enrutamiento y demás aspectos; Cada dispositivo es muy diferente en lo que respecta al hardware, el uso y la capacidad. Sin embargo, en todos los casos, el sistema operativo es lo que permite que el hardware funcione de manera correcta en cada parte de la topología de red.

Adicionalmente con esta prueba lograremos culminar nuestras carreras profesionales y así crecer personalmente y profesionalmente.

Objetivos

- El objetivo principal es entender las redes desde un punto de vista real y práctico, trabajando de una manera lo más cercana posible a situaciones cotidianas de la profesión del ingeniero o técnico de redes.

- Identificaremos el funcionamiento de los protocolos, elementos de una red y demás elementos que la componen.

Metodología

- ✓ La investigación explicativa se orienta a establecer las causas que originan un fenómeno determinado. Se trata de un tipo de investigación cuantitativa que descubre el por qué y el para qué de un fenómeno.

- ✓ Tipos de datos arrogados por la red propuesta

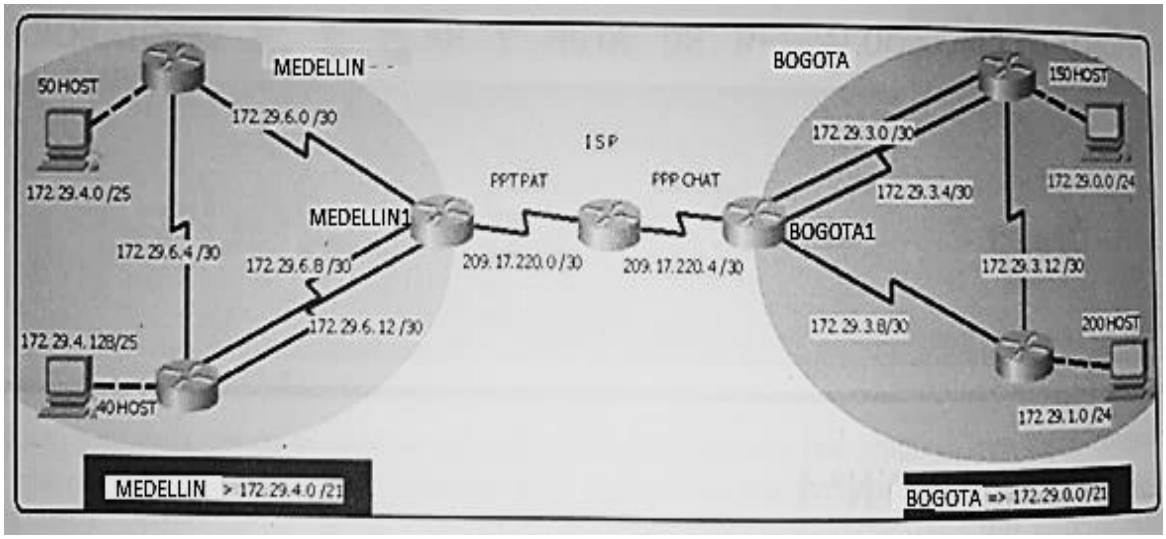
- ✓ Esta prueba de habilidades, se elaborará de forma coherente al desarrollo y pruebas que arroje los pings realizados.

Resultado y discusión

Escenario 1

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 1 Topología de red



Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.
- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

RESPUESTA: Password: cisco – Nombre dispositivo MEDELLIN1

- Realizar la conexión fisica de los equipos con base en la topología de red

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

Parte 1: Configuración del enrutamiento

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

RESPUESTA:

Configuracion de rutas estaticas en isp :

```
ISP>en
ISP#conf t
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.5.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#ip route 172.29.4.128 255.255.255.128 209.17.220.2
ISP(config)#ip route 172.29.1.0 255.255.255.0 209.17.220.6
ISP(config)#exit
```

Parte 2: Tabla de Enrutamiento.

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

RESPUESTA:

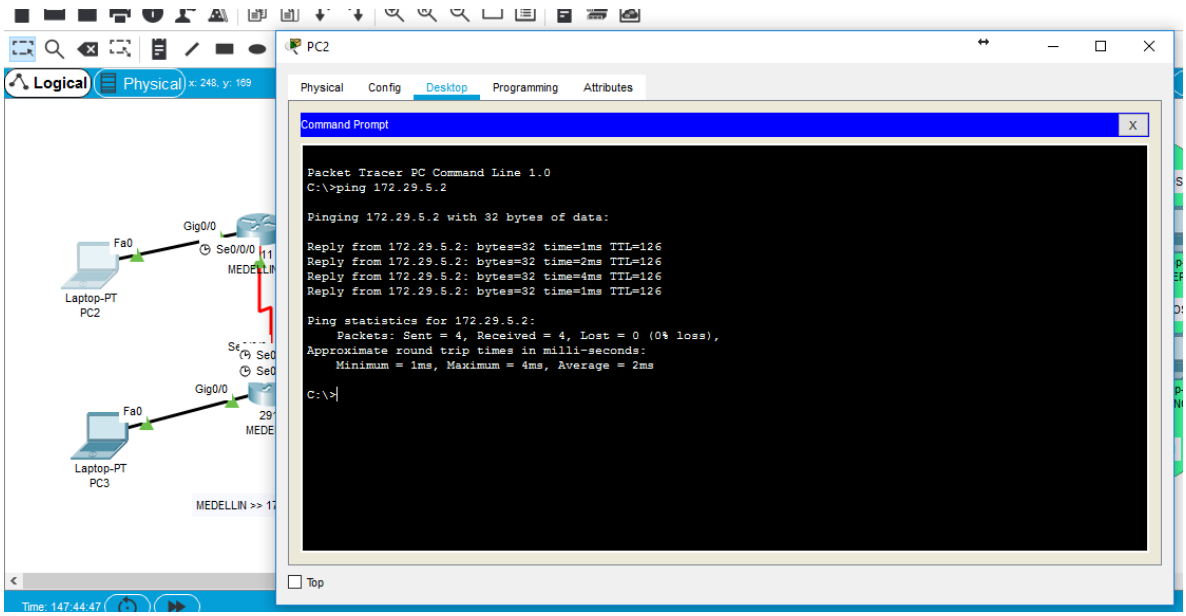
Comandos usados para la propagación de la ruta statica predeterminada en medellin

MEDELLIN1>en MEDELLIN1#conf t

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#exit

Pruebas ping de pc2 a pc3



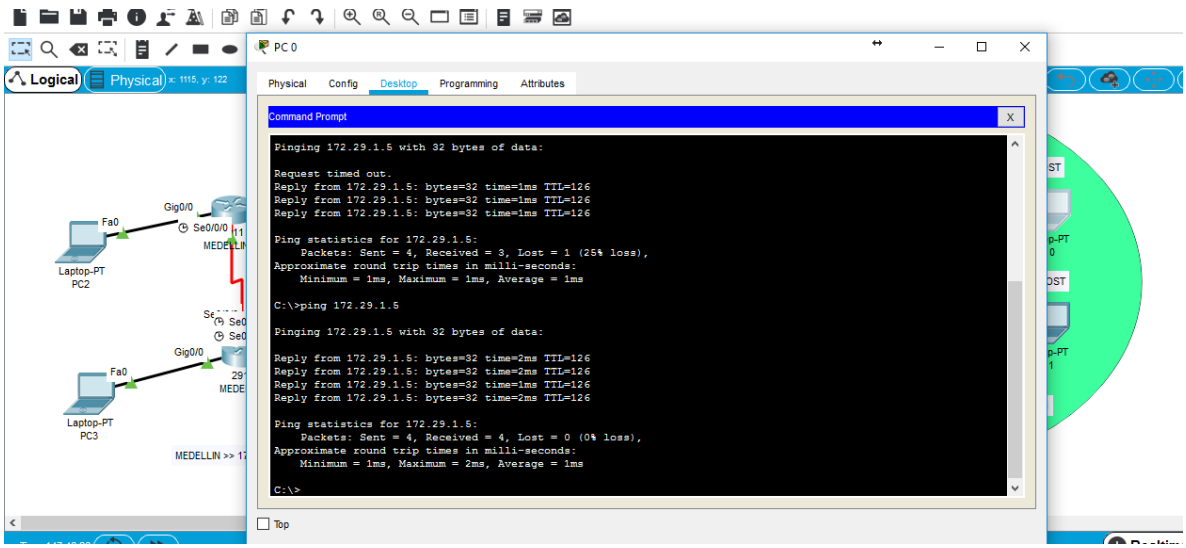
Comandos usados para la propagación de la ruta statica predeterminada en bogotá

BOGOTA1>en BOGOTA1#conf t

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#exit

Pruebas realizadas en la red bogota desde pc 0 a pc 1



Parte 3: Deshabilitar la propagación del protocolo RIP.

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

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

RESPUESTA:

Configuración de interfaces pasivas

- En router MEDELLIN1:

MEDELLIN1>en

MEDELLIN1#conf t

MEDELLIN1(config)#router rip

MEDELLIN1(config)#versión 2

MEDELLIN1(config-router)#Passive-interface s0/0/1

- En router MEDELLIN2:

MEDELLIN2>en

MEDELLIN2#conf t

MEDELLIN2(config)#router rip

MEDELLIN2(config)#versión 2

MEDELLIN2(config-router)#Passive-interface g0/0

- En router MEDELLIN:

MEDELLIN>en

MEDELLIN#conf t

MEDELLIN(config)#router rip

MEDELLIN(config)#versión 2

MEDELLIN(config-router)#Passive-interface g0/0

MEDELLIN(config-router)#Passive-interface s0/0/0

- En router BOGOTA1:

BOGOTA1>en

BOGOTA1#conf t

BOGOTA1(config)#router rip

BOGOTA1(config)#versión 2

BOGOTA1(config-router)#Passive-interface s0/0/1

- En router BOGOTA2:

BOGOTA2>en

BOGOTA2#conf t

BOGOTA2(config)#router rip

BOGOTA2(config)#versión 2

BOGOTA2(config-router)#Passive-interface g0/0

BOGOTA2(config-router)#Passive-interface s0/0/1

- En router BOGOTA:

BOGOTA>en

BOGOTA#conf t

BOGOTA(config)# router rip

BOGOTA(config)# version 2

BOGOTA(config-router)#Passive-interface g0/0

Parte 4: Verificación del protocolo RIP.

1. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos.

Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

RESPUESTA:

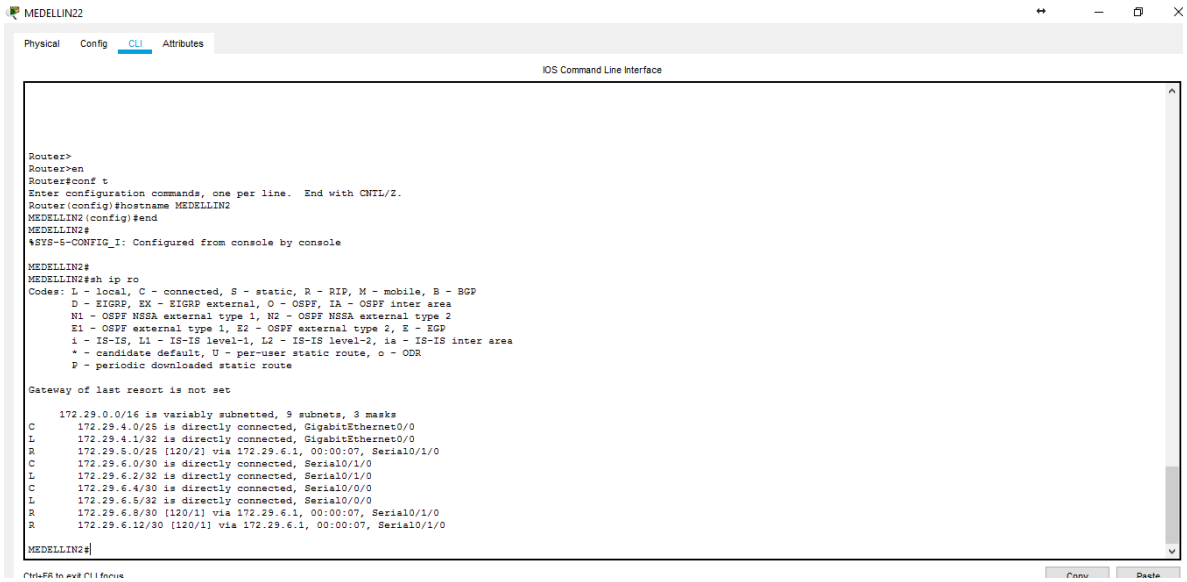
Verificación del protocolo RIP. a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos. b. Verificar y documentar la base de datos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

Sh ip route en medellin1

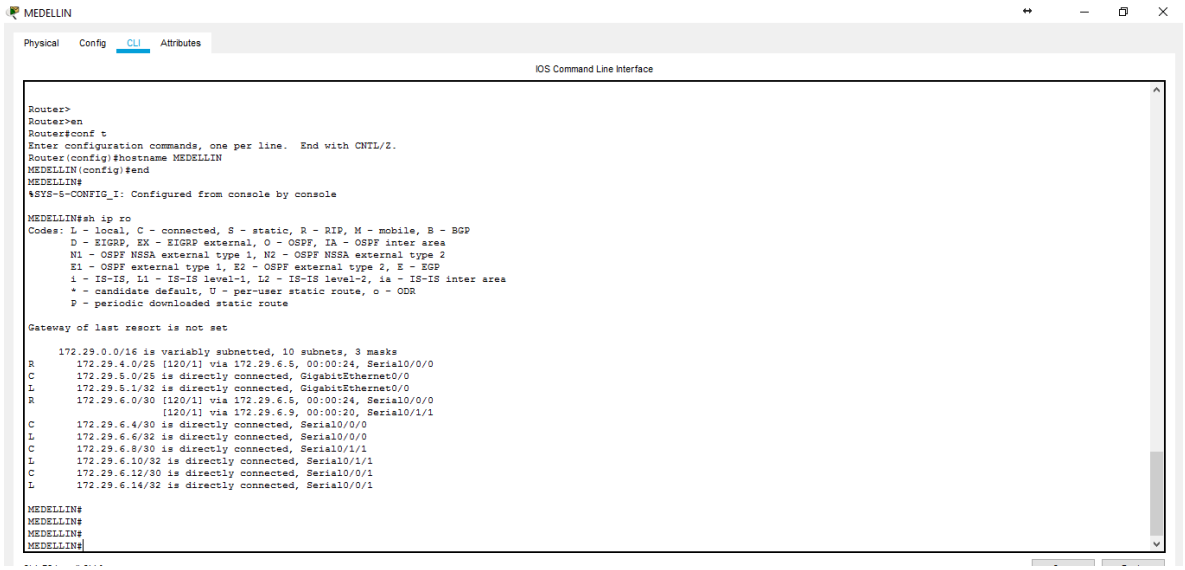
IOS Command Line Interface

```
Router>
Router>en
Router#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:02, Serial0/1/0
R       172.29.5.0/25 [120/1] via 172.29.6.10, 00:00:16, Serial0/1/1
                      [120/1] via 172.29.6.14, 00:00:16, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/1/0
L       172.29.6.1/32 is directly connected, Serial0/1/0
R       172.29.6.4/30 [120/1] via 172.29.6.10, 00:00:16, Serial0/1/1
                      [120/1] via 172.29.6.14, 00:00:16, Serial0/0/1
                      [120/1] via 172.29.6.2, 00:00:02, Serial0/1/0
C       172.29.6.8/30 is directly connected, Serial0/1/1
L       172.29.6.9/32 is directly connected, Serial0/1/1
C       172.29.6.12/30 is directly connected, Serial0/0/1
L       172.29.6.13/32 is directly connected, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.1

Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname MEDELLIN1
```

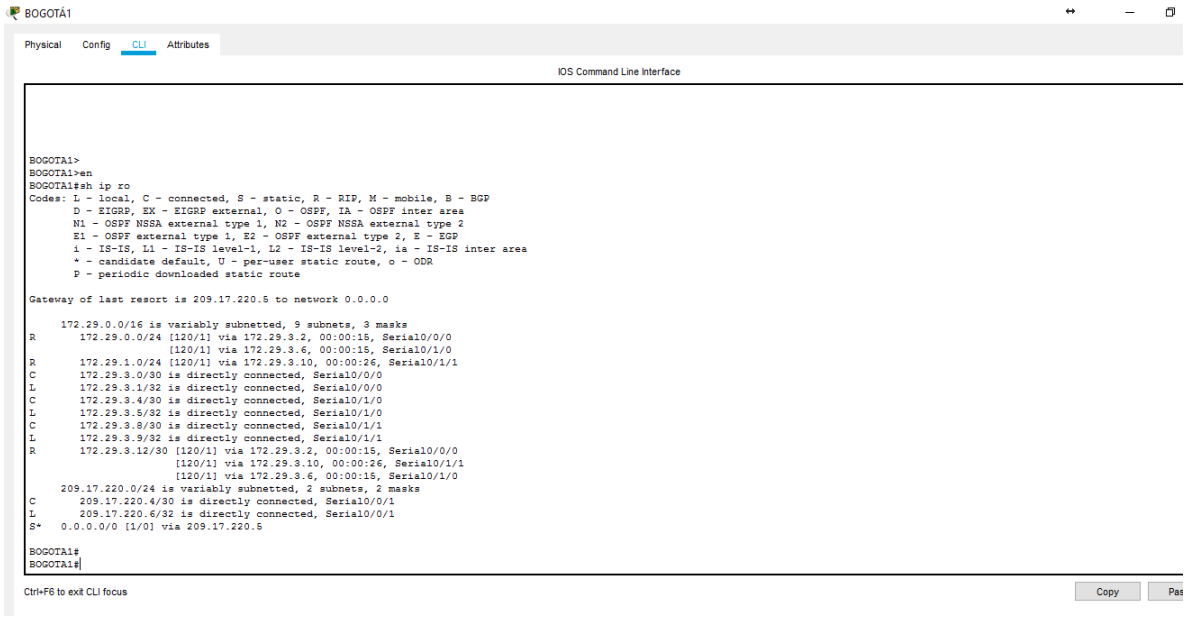
Sh ip route en medellin2



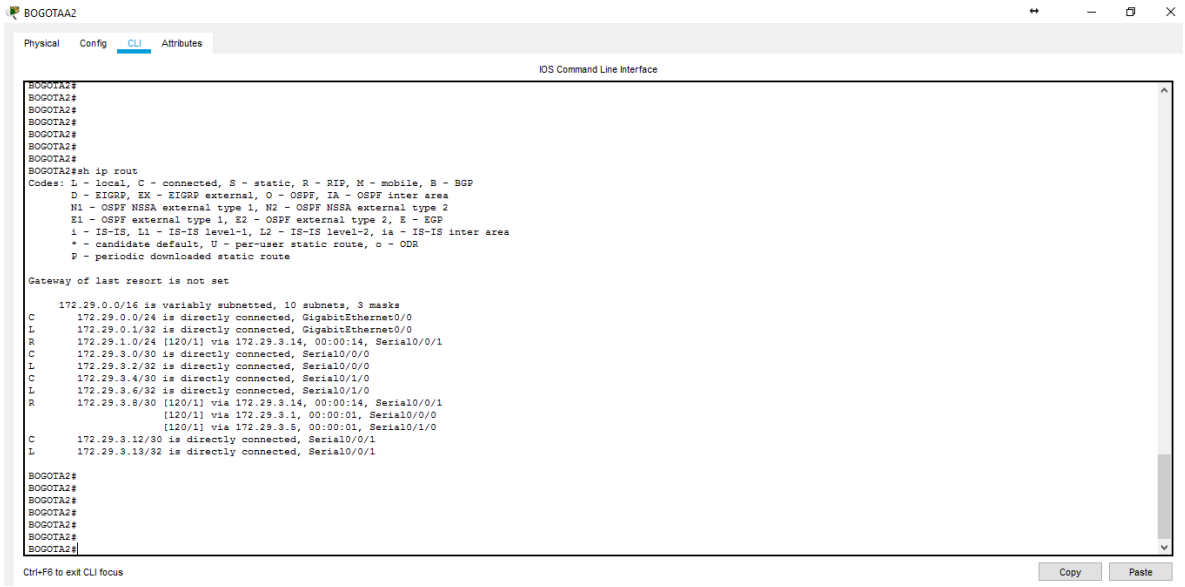
Sh ip route en medellin



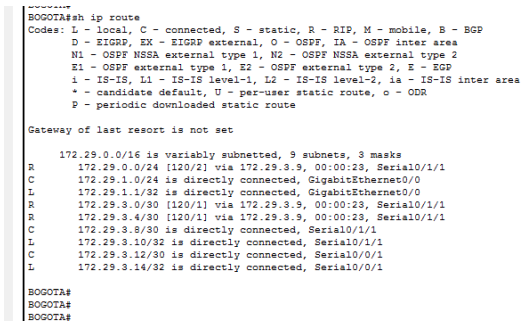
Sh ip route en bogota1



Sh ip route en bogota2



Sh ip route en bogota



Parte 5: Configurar encapsulamiento y autenticación PPP.

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

RESPUESTA:

MEDELLIN1>en

MEDELLIN1#conf t

MEDELLIN1(config)#int s0/0/0

MEDELLIN1(config-if)#encapsulation PPP

MEDELLIN1(config-if)#no shu

MEDELLIN1(config-if)#exit

Para bogota :

BOGOTA1>en

BOGOTA1#conf t

BOGOTA1(config)#int s0/0/1

BOGOTA1(config-if)#encapsulation PPP

BOGOTA1(config-if)#no shu

BOGOTA1(config-if)#exit

En isp :

ISP>en

ISP#conf t

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation PPP

ISP(config-if)#no shu

ISP(config-if)#exit

HABILITAR AUTENTICACION DE PAP Y DE PPP MEDELLIN>>IPS

ISP>en

ISP#conf t

ISP(config)#username MEDELLIN1 secret MEDELLIN

ISP(config)#int se0/0/0

ISP(config-if)#PPP authentication PAP

ISP(config-if)#PPP PAP sent-username ISP password ISP

ISP(config-if)#exit

Configuración PAP DE PPP en ISP en MEDELLIN1:

ISP>en

ISP#conf t

ISP(config)#username MEDELLIN1 secret MEDELLIN

ISP(config)#int se0/0/0

ISP(config-if)#PPP authentication PAP

ISP(config-if)#PPP PAP sent-username ISP password ISP

ISP(config-if)#exit

Configuración PAP de PPP en MEDELLIN1 CON ISP:

MEDELLIN1>en

MEDELLIN1#conf t

MEDELLIN1(config)#username ISP secret ISP

MEDELLIN1(config)#int se0/0/0

MEDELLIN1(config-if)#PPP authentication PAP

MEDELLIN1(config-if)#PPP PAP sent-username MEDELLIN1 password MEDELLIN

MEDELLIN1(config-if)#exit

autenticación CHAP DE PPP entre BOGOTA1 Y EL ISP:

- Configuración CHAP DE PPP en ISP CON BOGOTA1:

ISP>en

ISP#conf t

ISP(config)#username BOGOTA1 secret BOGOTA1

ISP(config)#int se0/0/1

ISP(config-if)#encasulaption ppp

ISP(config-if)#PPP authentication CHAP

ISP(config-if)#exit

Configuración CHAP de PPP en BOGOTA1 CON ISP:

BOGOTA1>en

BOGOTA1#conf t

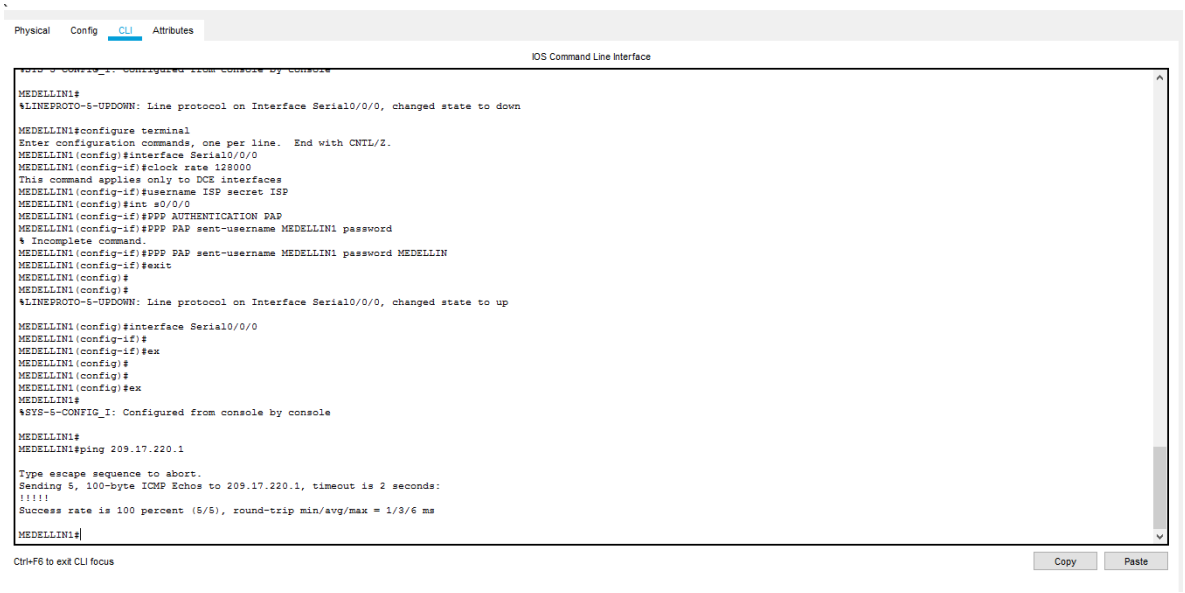
BOGOTA1(config)#username ISP secret BOGOTA1

BOGOTA1(config)#int S0/0/1

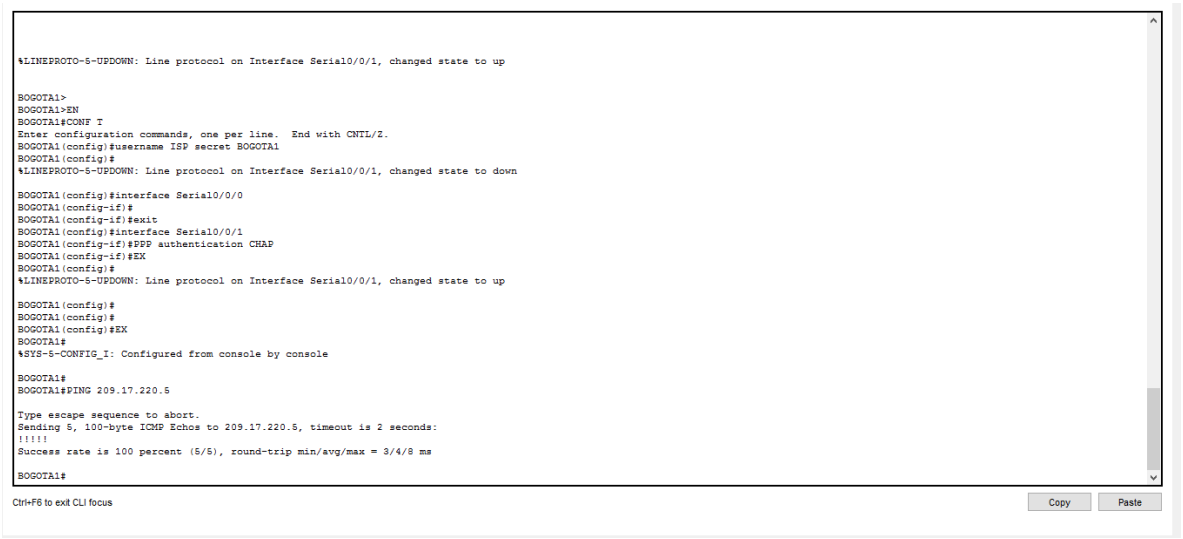
BOGOTA1(config-if)#PPP authentication CHAP

BOGOTA1(config-if)#exit

Prueba de conectividad por pap en Medellín usando ping hacia ISP



PRUEBA DE (CHAP)PING BOGOTA1 HASTA ISP



Parte 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.
c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

RESPUESTA:

MEDELLIN1>en

MEDELLIN1#conf t

Definimos la acl para poner el pat

MEDELLIN1(config)#ip access-list standard HOST

MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255

MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#Ip nat inside source list HOST interface s0/0 overload

MEDELLIN1(config)#int s0/0/0

MEDELLIN1(config-if)#ip nat outside

MEDELLIN1(config-if)#exit

MEDELLIN1(config)#int s0/0/1

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#exit

MEDELLIN1(config)#int s0/1/1

MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#exit

MEDELLIN1(config)#int s0/1/0

Iniciamos con la configuración NAT en BOGOTA1:

BOGOTA1>en

BOGOTA1#conf t

"definimos la acl para configurar el pat"

BOGOTA1(config)#ip access-list standard HOST

BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255

BOGOTA1(config-std-nacl)#exit

"Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP"

BOGOTA1(config)#Ip nat inside source list HOST interface s0/0/1 overload

BOGOTA1(config)#int s0/0/1

BOGOTA1(config-if)#ip nat outside

BOGOTA1(config-if)#exit

BOGOTA1|(config)#int s0/0/0

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#exit

BOGOTA1(config)#int s0/1/0

BOGOTA1(config-if)#ip nat inside

BOGOTA1(config-if)#exit

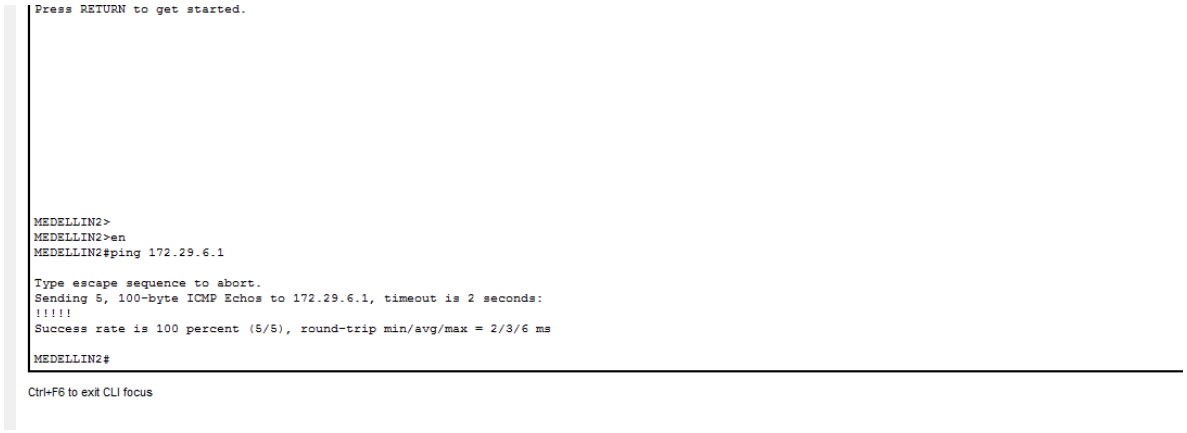
BOGOTA1(config)#int s0/1/1

BOGOTA1(config-if)#ip nat inside

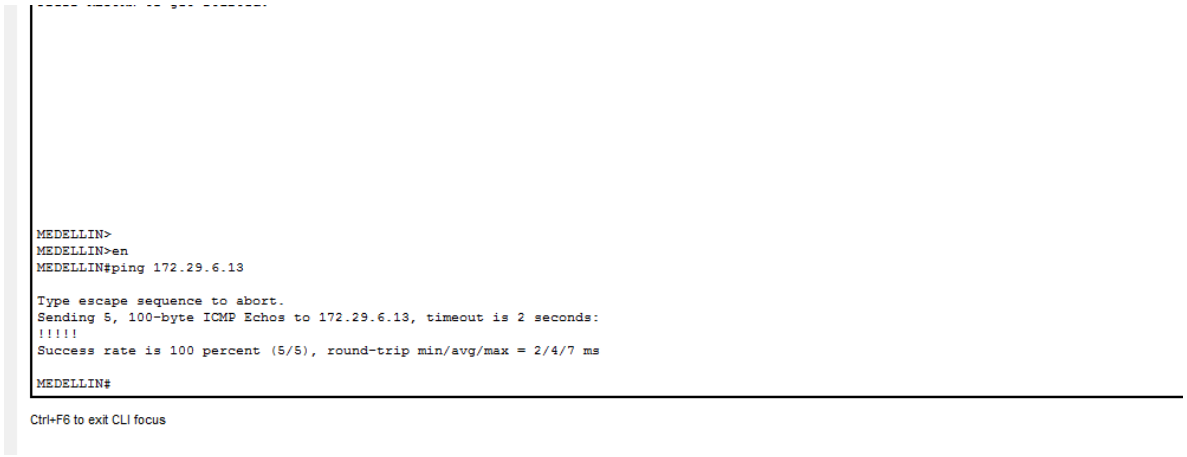
BOGOTA1(config-if)#exit

BOGOTA1(config)#exit

Verificamos con un ping desde medellin2 a medellin1



Verificamos con un ping desde medellin a medellin 1



Parte 7: Configuración del servicio DHCP.

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

RESPUESTA:

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3

MEDELLIN2(config)#ip dhcp excluded-address 172.29.5.1 172.29.5.2

MEDELLIN2(dhcp-config)#ip dhcp pool MEDELLIN2

MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128

MEDELLIN2(dhcp-config)#default-router 172.29.4.1

MEDELLIN2(dhcp-config)#dns-server 8.8.4.4

MEDELLIN2(dhcp-config)#exit

MEDELLIN2(config)#ip dhcp pool MEDELLIN

MEDELLIN2(dhcp-config)#network 172.29.5.6 255.255.255.128

-Definimos la dirección del Gateway para los Host.

MEDELLIN2(dhcp-config)#default-router 172.29.5.1

MEDELLIN2(dhcp-config)#dns-server 8.8.4.4

MEDELLIN2(dhcp-config)#exit

CONFIGURACION DHCP EN EL CLIENTE :

Con éste comando especificamos de que se haga la peticion dhcp al servidor anteriormente configurado MEDELLIN2

MEDELLIN>en

MEDELLIN#conf t

MEDELLIN(config)#Int fa0/0

MEDELLIN(config-if)#ip helper-addres 172.29.6.5

MEDELLIN(config-if)#exit

Configuración de server dhcp en BOGOTA2:

BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.6

BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.6

BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA2

BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0

BOGOTA2(dhcp-config)#default-router 172.29.1.1

BOGOTA2(dhcp-config)#dns-server 8.8.4.4

BOGOTA2(dhcp-config)#exit

BOGOTA2(config)#ip dhcp pool BOGOTA

-Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.

BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0

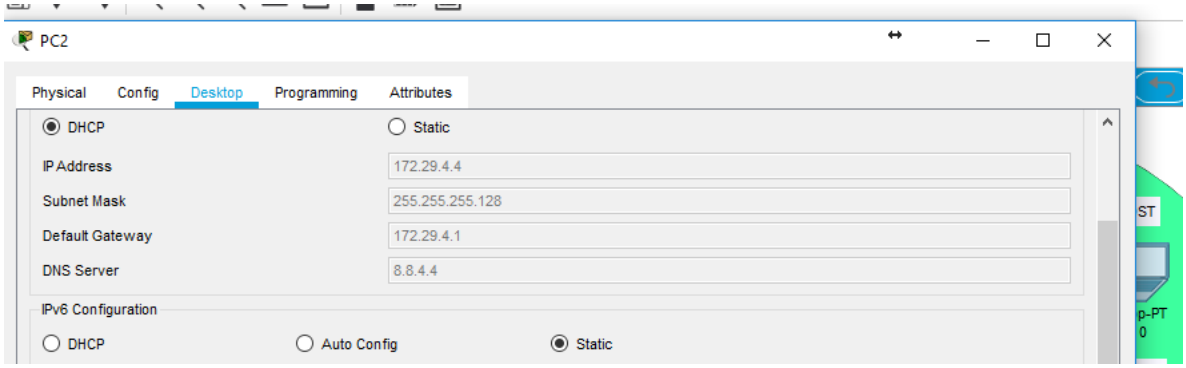
-Definimos la dirección del Gateway para los Host.

BOGOTA2(dhcp-config)#default-router 172.29.0.1

BOGOTA2(dhcp-config)#dns-server 8.8.4.4

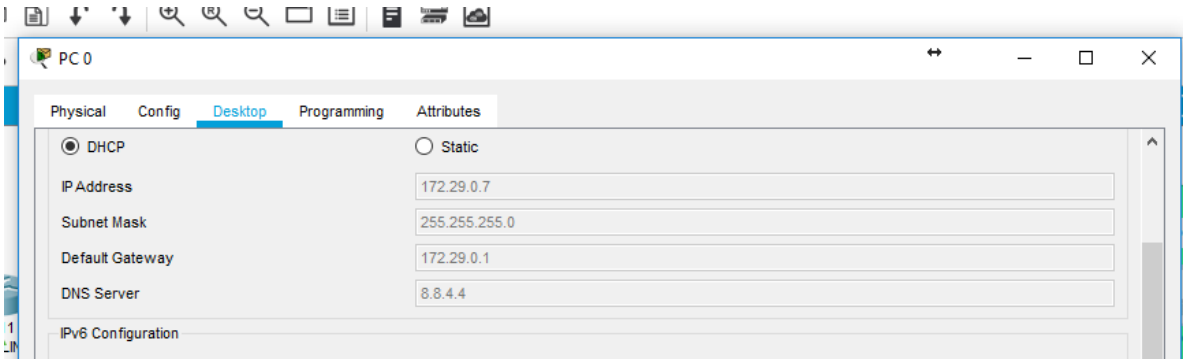
BOGOTA2(dhcp-config)#exit

Prueba de dhcp para el pc2 de medellin

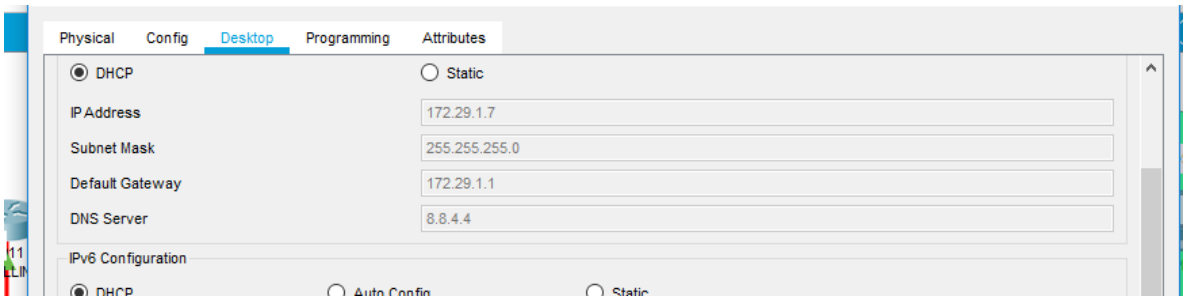


Prueba para el pc3 de medellin

Prueba dhcp para pc0 en bogota



Prueba dhcp para pc1 en Bogotá



CONFIGURACION BASICA DE SEGURIDAD EN TODOS LOS ROUTERS :

ISP>en

ISP#conf t

ISP(config)#enable secret ISP

ISP(config)#line console 0

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#exit

ISP(config)#line vty 0 4

ISP(config-line)#password cisco

ISP(config-line)#login

ISP(config-line)#exit

ISP(config)#service password-encryption

ISP(config)#banner motd #Prohibido el acceso no autorizado!#

ISP(config)#exit

Configuracipon en Router MEDELLIN1:

MEDELLIN1>en

MEDELLIN1#consf t

MEDELLIN1(config)#enable secret MEDELLIN1

MEDELLIN1(config)#line console 0

MEDELLIN1(config-line)#password cisco

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#exit

MEDELLIN1(config)#line vty 0 4

MEDELLIN1(config-line)#password cisco

MEDELLIN1(config-line)#login

MEDELLIN1(config-line)#exit

MEDELLIN1(config)#service password-encryption

MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado!#

MEDELLIN1(config)#exit

Configuracipon en Router MEDELLIN2:

MEDELLIN2>en

MEDELLIN2#conf t

MEDELLIN2(config)#enable secret MEDELLIN2

37

MEDELLIN2(config)#line console 0

MEDELLIN2(config-line)#password cisco

MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#exit

MEDELLIN2(config)#line vty 0 4

MEDELLIN2(config-line)#password cisco

MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#exit

MEDELLIN2(config)#service password-encryption

MEDELLIN2(config)#banner motd #Prohibido el acceso no autorizado!#

MEDELLIN2(config)#exit

Configuracipon en Router MEDELLIN:

MEDELLIN>en

MEDELLIN#conf t

MEDELLIN(config)#enable secret MEDELLIN

MEDELLIN(config)#line console 0

MEDELLIN(config-line)#password cisco

MEDELLIN(config-line)#login

MEDELLIN(config-line)#exit

MEDELLIN(config)#line vty 0 4

MEDELLIN(config-line)#password cisco

MEDELLIN(config-line)#login

MEDELLIN(config-line)#exit

MEDELLIN(config)#service password-encryption

MEDELLIN(config)#banner motd #Prohibido el acceso no autorizado!#

MEDELLIN(config)#exit

Configuracipon en Router BOGOTA1:

BOGOTA1>en

BOGOTA1#conf t

BOGOTA1(config)#enable secret BOGOTA1

BOGOTA1(config)#line console 0

BOGOTA1(config-line)#password cisco

BOGOTA1(config-line)#login

BOGOTA1(config-line)#exit

BOGOTA1(config)#line vty 0 4

BOGOTA1(config-line)#password cisco

BOGOTA1(config-line)#login

BOGOTA1(config-line)#exit

BOGOTA1(config)#service password-encryption

BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado!#

BOGOTA1(config)#exit

38

Configuracipon en Router BOGOTA2:

BOGOTA2>en

BOGOTA2#conf t

BOGOTA2(config)#enable secret BOGOTA2

BOGOTA2(config)#line console 0

BOGOTA2(config-line)#password cisco

BOGOTA2(config-line)#login

BOGOTA2(config-line)#exit

BOGOTA2(config)#line vty 0 4

BOGOTA2(config-line)#password cisco

BOGOTA2(config-line)#login

BOGOTA2(config-line)#exit

BOGOTA2(config)#service password-encryption

BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado!#

BOGOTA2(config)#exit

Configuracipon en Router BOGOTA:

BOGOTA>en

BOGOTA#conf t

BOGOTA(config)#enable secret BOGOTA

BOGOTA(config)#line console 0

BOGOTA(config-line)#password cisco

BOGOTA(config-line)#login

BOGOTA(config-line)#exit

BOGOTA(config)#line vty 0 4

BOGOTA(config-line)#password cisco

BOGOTA(config-line)#login

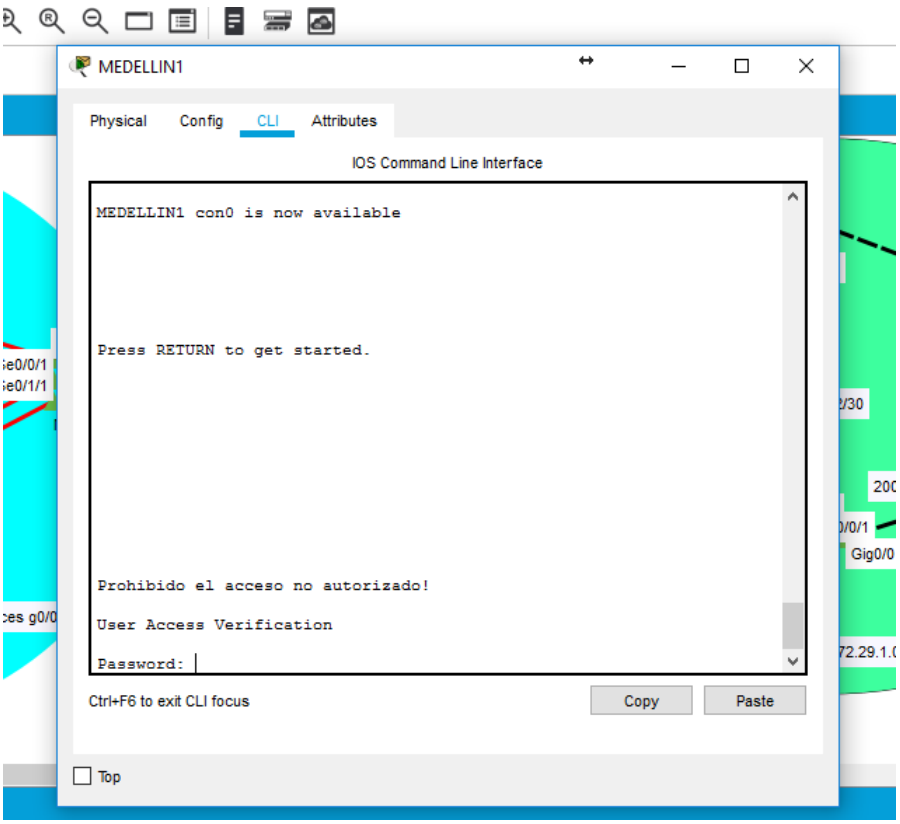
BOGOTA(config-line)#exit

BOGOTA(config)#service password-encryption

BOGOTA(config)#banner motd #Prohibido el acceso no autorizado!#

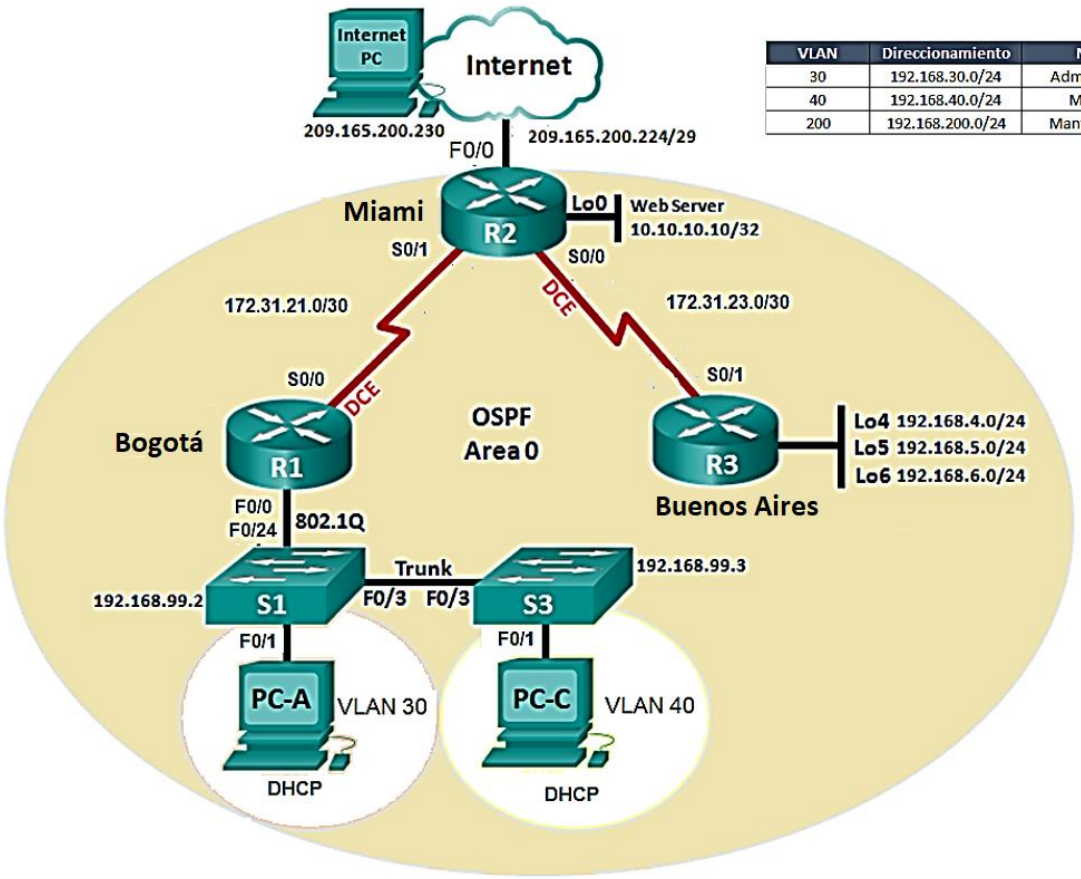
BOGOTA(config)#exit

Ejemplo de la seguridad :


MEDELLIN1
Physical
Config
CLI
Attributes
IOS Command Line Interface
MEDELLIN1 con0 is now available
Press RETURN to get started.
Prohibido el acceso no autorizado!
User Access Verification
Password:
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

Escenario 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.



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

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

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

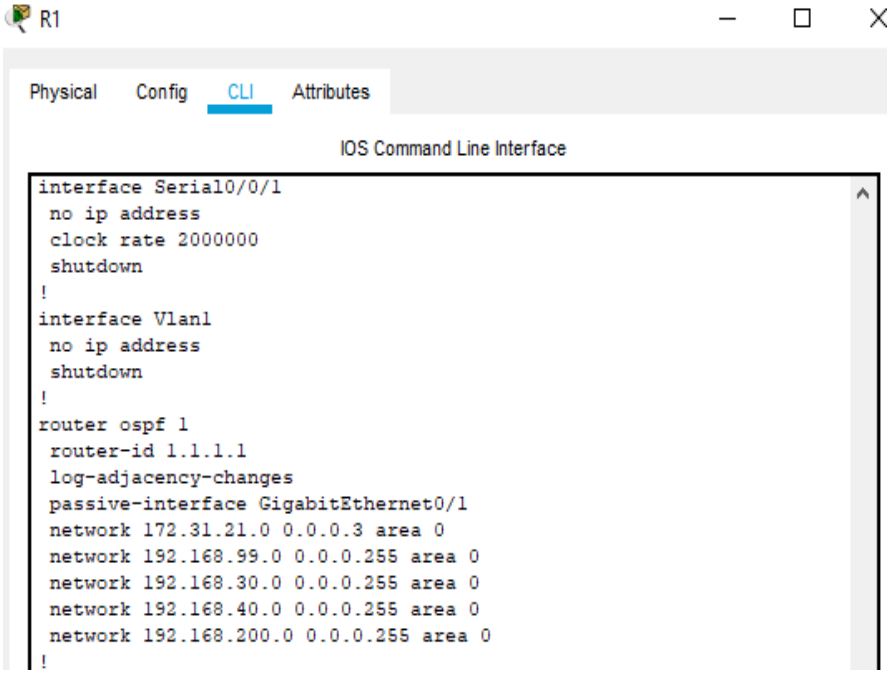
OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Verificar información de OSPF

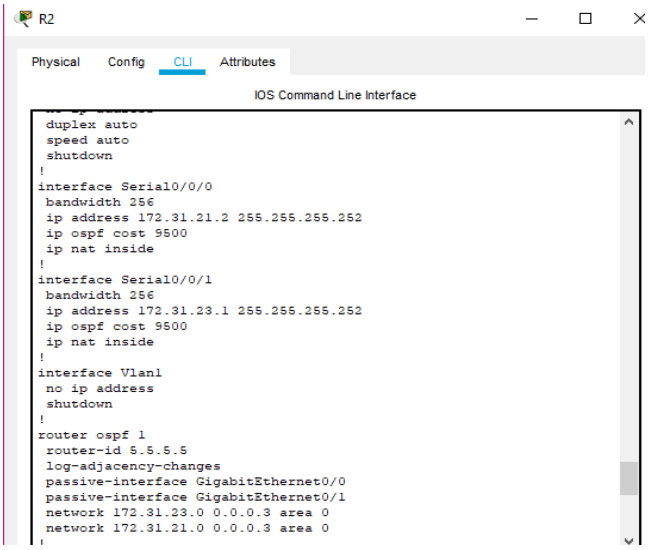
- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

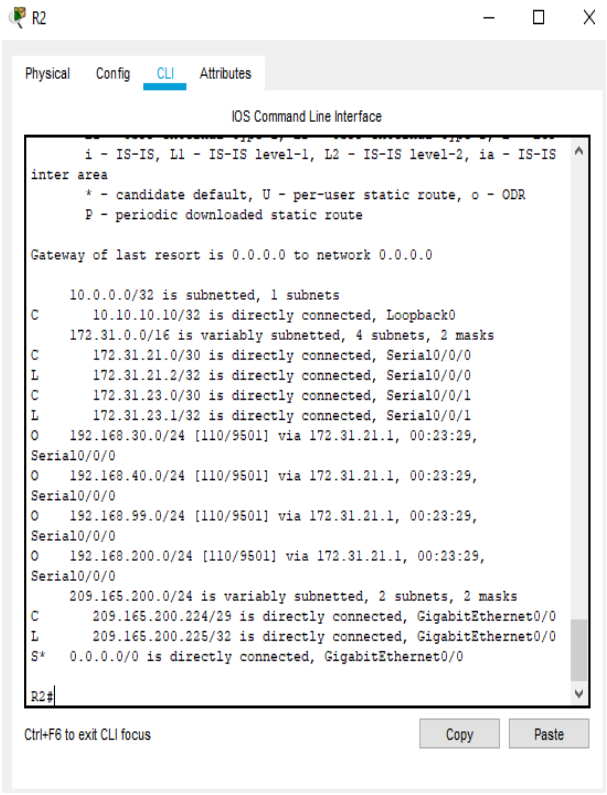
  RESPUESTA:



- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

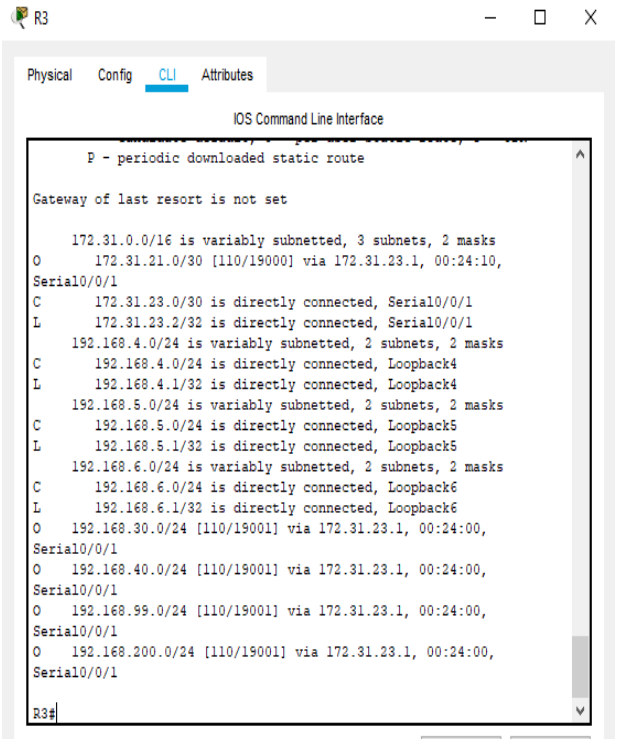
RESPUESTA:





- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router

RESPUESTA



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

Seguridad en los Switches acorde a la topología de red establecida.

```
S1#sh int gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,30,40,99,200
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

```
S1#sh int fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,30,40,99,200
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

```
S1#sh port
S1#sh port-security int fa0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
S1#sh int tr
S1#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1,30,40,99,200
Gig0/1      1,30,40,99,200

Port        Vlans allowed and active in management domain
Fa0/1       1,30,40,99,200
Gig0/1      1,30,40,99,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,30,40,99,200
Gig0/1      1,30,40,99,200
```

```
S3#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1,30,40,99,200

Port        Vlans allowed and active in management domain
Fa0/1       1,30,40,99,200

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,30,40,99,200
```

4. En el Switch 3 deshabilitar DNS lookup

RESPUESTA:

```
S3(config)#no ip domain
S3(config)#no ip domain-lo
S3(config)#no ip domain-lookup
S3(config)#
```

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

RESPUESTA:

```
down
Vlan1                  unassigned      YES manual administratively
down down
Vlan99                 192.168.99.3    YES manual up
up
S3#
```

```
S1#sh ip int br | ex una
Interface              IP-Address      OK? Method Status
Protocol
Vlan99                 192.168.99.2    YES manual up
up
```

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

RESPUESTA:

```
S1(config)#int ra
S1(config)#int range fa0/3-23
S1(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down
```

```
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#int ra
S3(config)#int range fa0/3-23
S3(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
```

7. Implement DHCP and NAT for IPv4

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

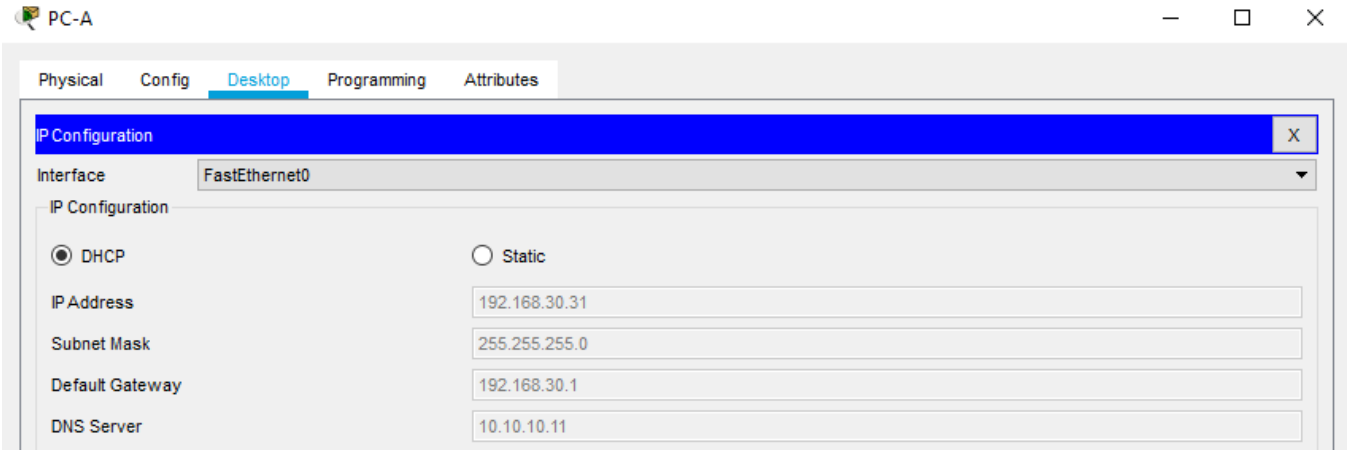
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

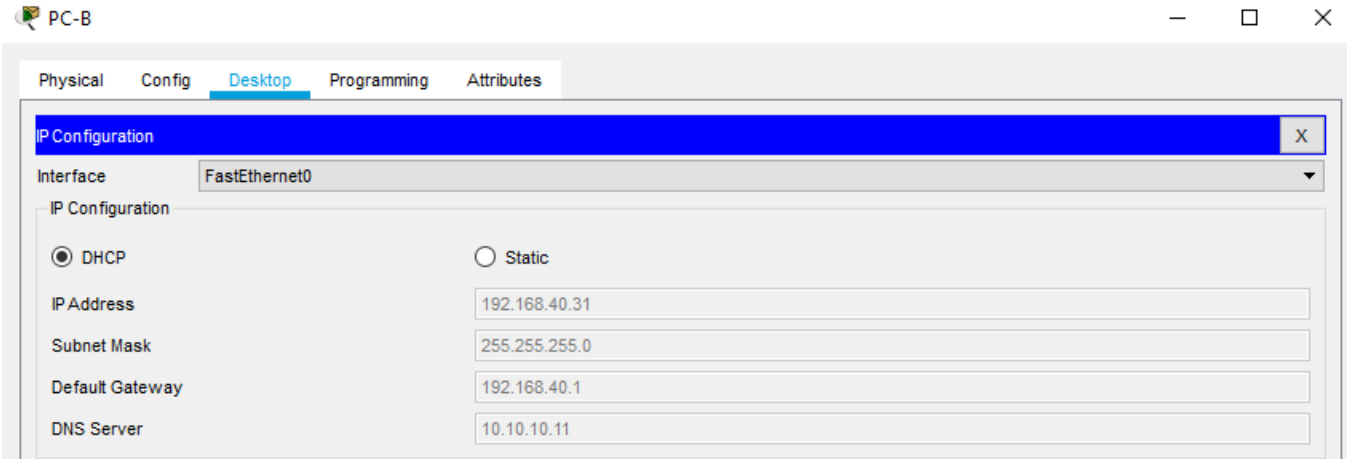
Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

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

RESPUESTA 7 – 8 Y 9:

```
hostname R1
!
!
!
!
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.40.254
!
ip dhcp pool Administracion
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.10.10.11
 domain-name ccna-unad.com
ip dhcp pool Mercadeo
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 10.10.10.11
 domain-name ccna-unad.com
!
```





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

RESPUESTA 10:

```
R2(config)#int serial 0/0/0
R2(config-if)#ip nat
R2(config-if)#ip nat  ins
R2(config-if)#ip nat  inside
R2(config-if)#
R2(config-if)#int gi0/0
R2(config-if)#ip nat
R2(config-if)#ip nat  out
R2(config-if)#ip nat  outside
R2(config-if)#
R2(config-if)#
R2(config-if)#
R2(config-if)#ip nat
R2(config-if)#ip nat  ins
R2(config-if)#ip nat  inside sout
R2(config-if)#ip nat  inside sour
R2(config-if)#ip nat  inside source
R2(config-if)#exit
R2(config)#
R2(config)#ip nat ins
R2(config)#ip nat inside sour
R2(config)#ip nat inside source lis
R2(config)#ip nat inside source list 1 pool Internet
R2(config)#
R2(config)#ip nat
R2(config)#ip nat poo
R2(config)#ip nat pool Internet 209.200
R2(config)#ip nat pool Internet 209.165.200.226 209.165.200.229 net
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access
R1(config)#ip access-list sta
R1(config)#ip access-list standard 10
R1(config-std-nacl)#per
R1(config-std-nacl)#de
R1(config-std-nacl)#deny
R1(config-std-nacl)#deny host
R1(config-std-nacl)#deny host 192.168.30.31
R1(config-std-nacl)#permit ip any any
                           ^
```

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.

RESPUESTA:

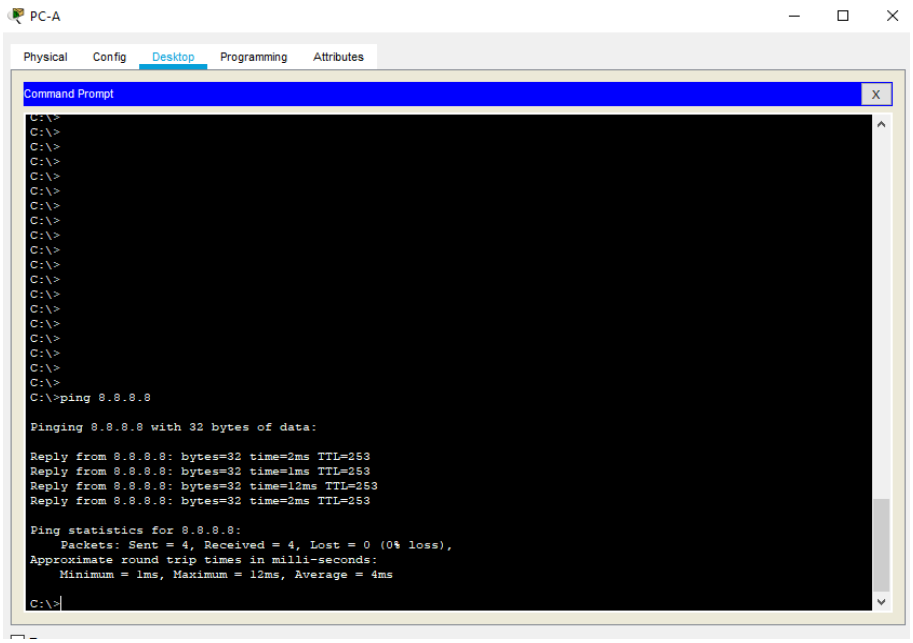
```
C:\>ping 172.31.21.2

Pinging 172.31.21.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 172.31.21.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
R1(config-subif)#ip access
R1(config-subif)#exit
R1(config)#ip access
R1(config)#ip access-list sta
R1(config)#ip access-list standard 1
R1(config-std-nacl)#per
R1(config-std-nacl)#permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gi0/0.40
R1(config-subif)#ip acccess
R1(config-subif)#ip access
R1(config-subif)#ip access-group 1
% Incomplete command.
R1(config-subif)#ip access-group 1 in
R1(config-subif)#
R1(config-subif)#end
```

```
C:\>
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

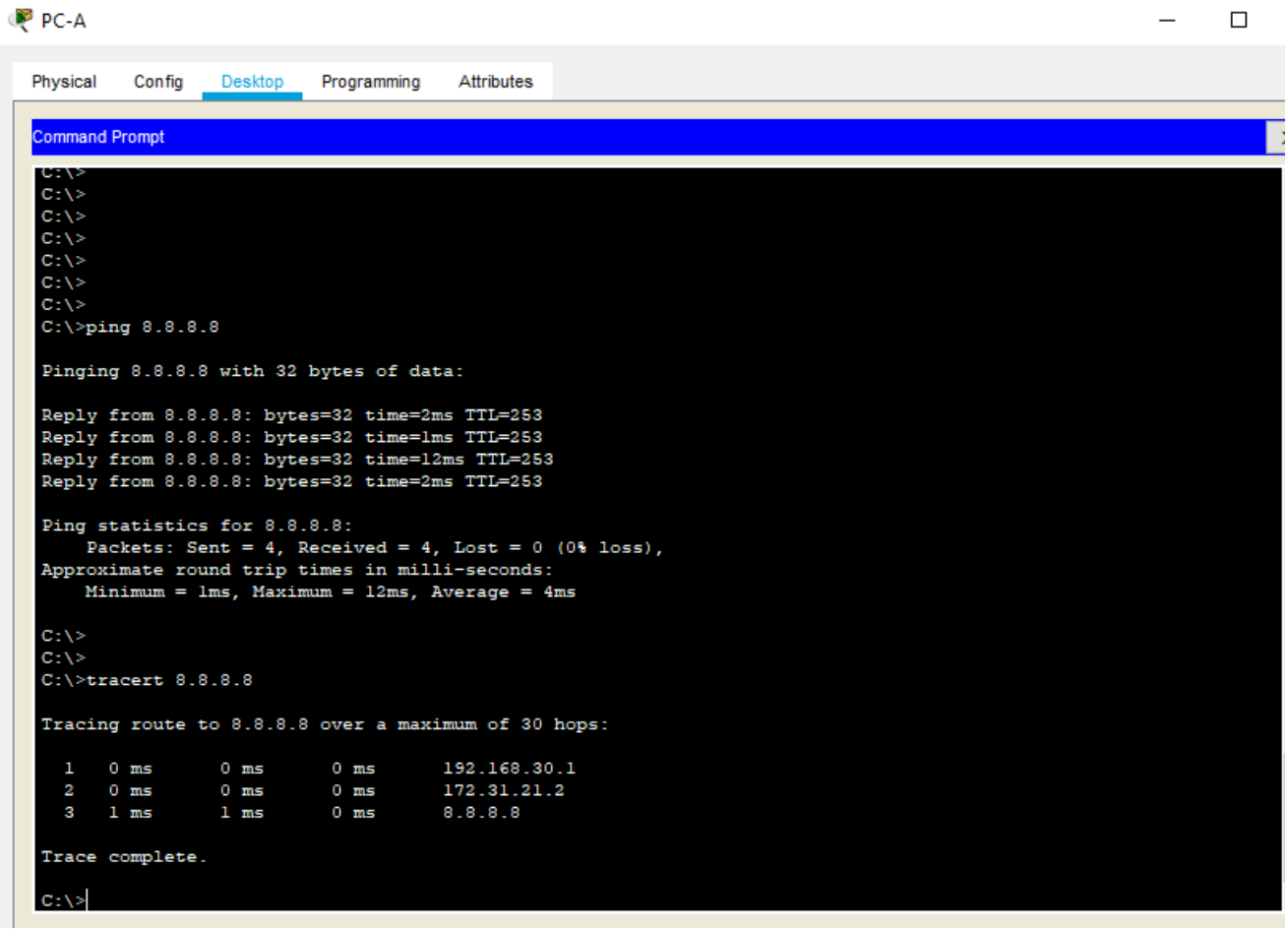
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

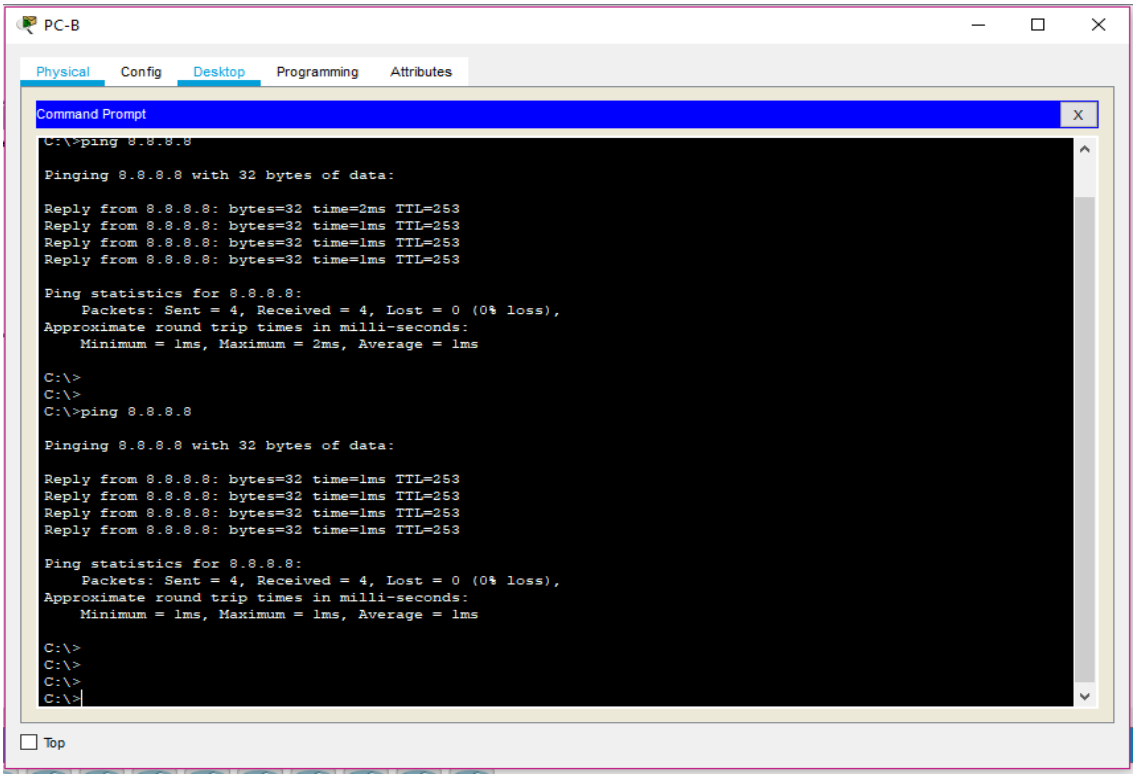
RESPUESTA:

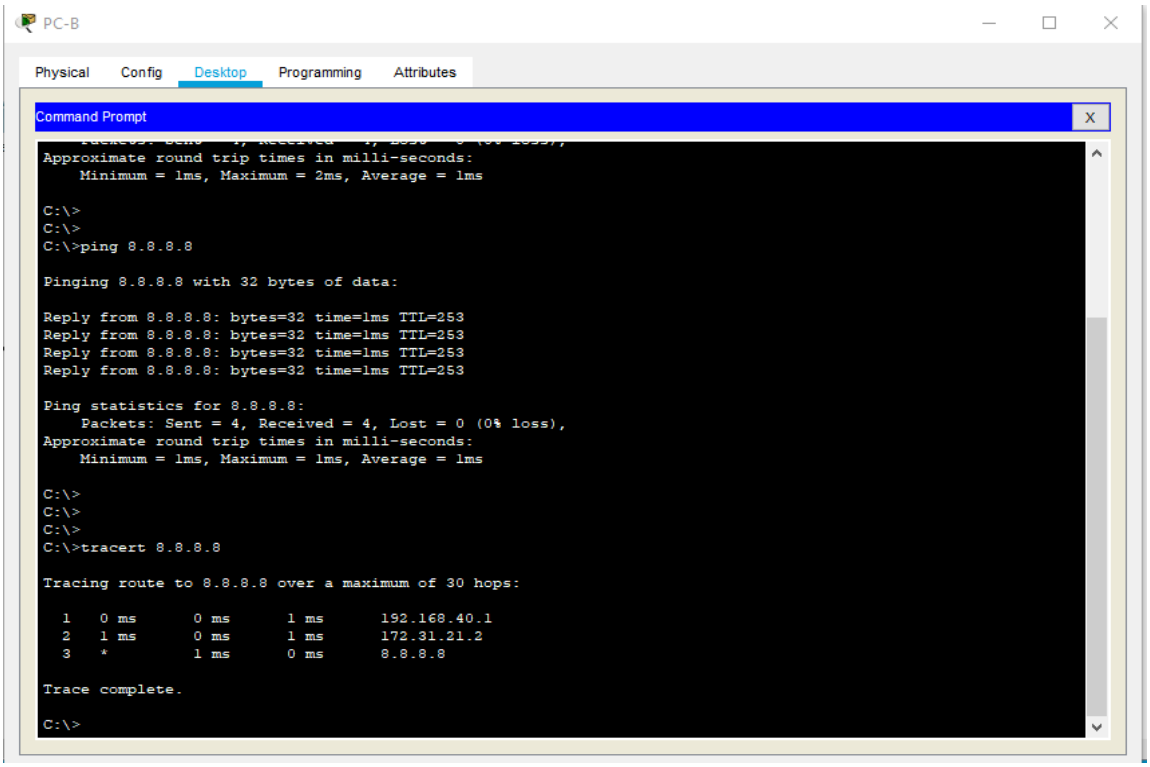


13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

RESPUESTA:




PC-B
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=2ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
C:\>
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>
C:\>
C:\>
C:\>
Top


PC-B
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
C:\>
C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Reply from 8.8.8.8: bytes=32 time=1ms TTL=253
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>
C:\>
C:\>
C:\>tracert 8.8.8.8
Tracing route to 8.8.8.8 over a maximum of 30 hops:
1 0 ms 0 ms 1 ms 192.168.40.1
2 1 ms 0 ms 1 ms 172.31.21.2
3 * 1 ms 0 ms 8.8.8.8
Trace complete.
C:\>

Conclusiones

Al desarrollar esta prueba de habilidades, puedo concluir que hay varios tipos de protocolos que nos ayudan a programar las diferentes direcciones IP, interfaces y dispositivos que conforman una red.

El esquema de una red en la actualidad, debe ser rigurosamente analizado. Entre los factores que influyen para lograr un buen esquema se deben tener en cuenta: la flexibilidad con respecto a los servicios soportados, la vida útil requerida, el tamaño del sitio y la cantidad de usuarios que estarán conectados y los costos, entre otros. Teniendo en cuenta estos factores no se debe dudar en utilizar el mecanismo que provea las facilidades de estandarización, orden, rendimiento, durabilidad, integridad y facilidad de expansión.

Bibliografía

YANEZ, Deisy. Investigación Explicativa: Características, Técnicas, Ejemplos. Edicion 1. Editorial Iidefer.com. 2015. Comunicador social, especialista en Comunicación Organizacional con interés y experiencia en temas de Marketing Digital y Responsabilidad Social.

ICONTEC. Diseño y Desarrollo por Jeduca S.A.S. 2016. Actualización de Referencias Internacionales (SARI).

Anexos

Se adjunta archivos. pkt para cada escenario, desarrollados en **Packet Tracer**