PRUEBA DE HABILIDADES PRACTICAS CCNA

Leonardo Prada Pérez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS
CEAD JOSE ACEVEDO Y GOMEZ
2019

SOLUCIÓN DE DOS ESTUDIOS DE CASO SOPORTADOS EN EL USO DE TECNOLOGÍA CISCO

LEONARDO PRADA

GRUPO: 203092_7

DIPLOMADO DE PROFUNDIZACIÓN CISCO
DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN / WLAN

ENTREGADO A:
IVAN GUSTAVO PENA

DIRECTOR
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
2019

Tabla de Contenidos

Tabla de Ilustraciones

1 INTRODUCCIÓN

El buen uso de redes en organizaciones es importante en la actualidad teniendo en cuenta que todos los procesos deben estar interconectados en la misma. La importancia de demostrar este conocimiento mediante la resolución de dos escenarios es lo que me lleva a exponer lo aprendido en esta etapa. Cada uno tiene retos y conocimientos diferentes, los cuales podrán ver a continuación que mucho que aprendí ha sido para mí muy importante darlo a conocer mediante este documento.

1.1 Descripción general de la prueba de habilidades

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.

- Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL y OBLIGATORIA.
- Toda evidencia de copy-paste o plagio (de la web o de otros informes) será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas ICONTEC 1486 para la presentación de trabajos escritos e incluir los siguientes elementos en su contenido:

- Portada
- Tabla de contenido
- Introducción
- Desarrollo de los dos escenarios

IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como ping, traceroute, show ip route, entre otros.

- Conclusiones
- Referencias Bibliográficas

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado. El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD.

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso.

2 ESCENARIO 1

2.1 Topología de red

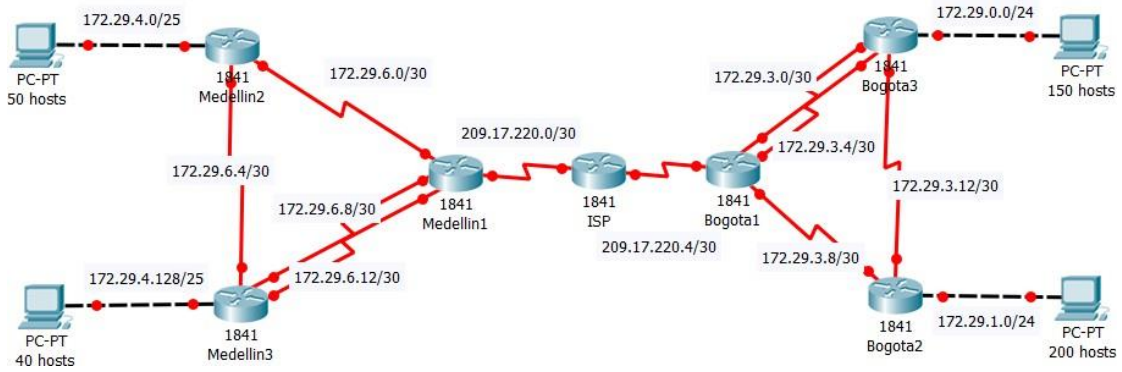


Ilustración 1 Topología de red

2.2 Denominación del router

Router (Config)#: Hostname (nombre del router) Para asignar nombre al router.

Router (Config)#: Hostname ISP

Router (Config)#: Hostname Bogota_1

Router (Config)#: Hostname Bogota_2

Router (Config)#: Hostname Bogota_3

Router (Config)#: Hostname Medellin_1

Router (Config)#: Hostname Medellin_2

Router (Config)#: Hostname Medellin_3

2.3 Configuración de contraseñas

Router(Config)#enable secret password:(En password, se coloca la clave)

Router(Config)#line console 0 (Para configurar el password de consola)

Router(Config-line)#password password(En password, se coloca la clave)

Router(Config-line)#login

Router(Config)#line vty 0 4 (password para la linea de terminal virtual)

Router(Config-line)#password password(En password, se coloca la clave)

Router(Config-line)#login

La siguiente configuración se hizo para todos los routers.

Router(Config)#enable secret 1234

Router(Config)#line console 0

Router(Config-line)#password 1234

Router(Config-line)#login

Router(Config)#line vty 0 4

Router(Config-line)#password 1234

Router(Config-line)#login

2.4 Parte 1: configuración del enrutamiento

Medellin_1 (config)# router rip

Medellin_1 (config-router)# network 172.29.0.0

Medellin_1 (config-router)# version

Medellin_1 (config-router)# no auto-summary

Medellin_1 (config-router)# exit

Bogota_1 (config)# router rip

Bogota_1 (config-router)# network 172.29.0.0

Bogota_1 (config-router)# version

Bogota_1 (config-router)# no auto-summary

Bogota1 (config-router)# exit

Al implementar el protocolo RIP v2 para enrutamiento, simplifica bastante el proceso ya que al tener subredes que tienen en común los primeros 16 bits, se puede crear como una “super red” que haga la cobertura a todas las demás, esto sucede en ambos routers principales.

ISP

```
ip classless
ip route 209.17.220.4 255.255.255.252 209.17.220.6
ip route 172.29.0.0 255.255.255.0 209.17.220.6
ip route 172.29.1.0 255.255.255.0 209.17.220.6
ip route 172.29.4.128 255.255.255.128 209.17.220.1
ip route 172.29.4.0 255.255.255.128 209.17.220.1
!
```

Utilizando el comando anterior, determinamos a la tabla de enrutamiento, cuál es la mejor ruta para un paquete de destino.

Se crean las rutas estáticas para ambas subredes desde ISP.

ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.1

2.5 Parte 2: tabla de enrutamiento

```
MEDELLIN_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.1, 00:00:22, Serial0/1/1
R       172.29.4.128/25 [120/1] via 172.29.6.9, 00:00:01, Serial0/0/0
                        [120/1] via 172.29.6.13, 00:00:01, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/1/1
L       172.29.6.2/32 is directly connected, Serial0/1/1
R       172.29.6.4/30 [120/1] via 172.29.6.9, 00:00:01, Serial0/0/0
                      [120/1] via 172.29.6.13, 00:00:01, Serial0/0/1
                      [120/1] via 172.29.6.1, 00:00:22, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/0/1
L       172.29.6.14/32 is directly connected, Serial0/0/1
```

```
BOGOTA_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/2] via 172.29.3.9, 00:00:13, Serial0/1/1
R       172.29.1.0/24 [120/1] via 172.29.3.9, 00:00:13, Serial0/1/1
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.1/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/0/0
L       172.29.3.6/32 is directly connected, Serial0/0/0
C       172.29.3.8/30 is directly connected, Serial0/1/1
L       172.29.3.10/32 is directly connected, Serial0/1/1
R       172.29.3.12/30 [120/1] via 172.29.3.9, 00:00:13, Serial0/1/1


        172.29.0.0/16 is variably subnetted, 4 subnets, 2 masks
  S        172.29.0.0/24 [1/0] via 209.17.220.6
  S        172.29.1.0/24 [1/0] via 209.17.220.6
  S        172.29.4.0/25 [1/0] via 209.17.220.1
  S        172.29.4.128/25 [1/0] via 209.17.220.1
        209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
  C        209.17.220.0/30 is directly connected, Serial0/0/1
  L        209.17.220.2/32 is directly connected, Serial0/0/1
  C        209.17.220.4/30 is directly connected, Serial0/0/0
  L        209.17.220.5/32 is directly connected, Serial0/0/0

  Router#
```

En las tablas mostradas anteriormente se puede observar la conexión que hasta ahora se ha hecho en la red, cumpliendo a cabalidad con los pasos descritos hasta este punto.

2.6 Parte 3. Deshabilitar la propagación del protocolo RIP

En las siguientes imágenes tomadas de cada router, se podrá observar la configuración implementada de acuerdo con este paso.

```
MEDELLIN_1(config-router)#passive-interface se 0/1/1
MEDELLIN_1(config-router)#passive-interface se 0/1/0
MEDELLIN_1(config-router)#passive-interface se 0/1/0
```

```
router rip
 version 2
 passive-interface Serial0/1/0
 passive-interface Serial0/1/1
 network 172.29.0.0
```

```
BOGOTA_1(config-router)#passive-interface se 0/0/1
BOGOTA_1(config-router)#passive-interface se 0/1/1
BOGOTA_1(config-router)#passive-interface se 0/1/0
BOGOTA_1(config-router)#
```

2.7 Parte 4: verificación del protocolo RIP

```
MEDELLIN_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.1, 00:00:22, Serial0/1/1
R       172.29.4.128/25 [120/1] via 172.29.6.9, 00:00:01, Serial0/0/0
                        [120/1] via 172.29.6.13, 00:00:01, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/1/1
L       172.29.6.2/32 is directly connected, Serial0/1/1
R       172.29.6.4/30 [120/1] via 172.29.6.9, 00:00:01, Serial0/0/0
                      [120/1] via 172.29.6.13, 00:00:01, Serial0/0/1
                      [120/1] via 172.29.6.1, 00:00:22, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/0/1
L       172.29.6.14/32 is directly connected, Serial0/0/1
```

Se puede observar que el protocolo RIP está activado y directamente establecido en las interfaces propuestas.

2.8 Parte 5: configurar encapsulamiento y autenticación PPP

- Medellín

```
interface Serial0/1/0
 ip address 209.17.220.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ip nat outside
 clock rate 2000000
!
```

- Bogotá

```
interface Serial0/1/0
 ip address 209.17.220.6 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 no keepalive
 clock rate 2000000
```

ISP

```
interface Serial0/0/0
 ip address 209.17.220.5 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 clock rate 2000000
!
interface Serial0/0/1
 ip address 209.17.220.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 2000000
```

Para realizar la configuración de encapsulamiento y autenticación PPP se establecen los parámetros anteriormente descritos en cada uno de los routers.

2.9 Parte 6: Configuración de PAT

```
ip nat inside source list 1 interface Serial0/1/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.2
!
ip flow-export version 9
!
!
access-list 1 permit 172.29.6.0 0.0.0.3


interface Serial0/1/0
 ip address 209.17.220.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ip nat outside
 clock rate 2000000
!
interface Serial0/1/1
 ip address 172.29.6.2 255.255.255.252
 ip nat inside
 clock rate 2000000
```

Para garantizar que los Routers tengan acceso o alcance hasta los Routers de los extremos se realizó la configuración descrita en la imagen anterior. En las interfaces acordadas se hizo la configuración ppp y chap garantizando la comunicación en la red.

2.10 Parte 7: Configuración del servicio DHCP

```
ip dhcp excluded-address 172.29.4.1
ip dhcp excluded-address 172.29.4.129
!
ip dhcp pool MEDELLIN
 network 172.29.4.0 255.255.255.128
 default-router 172.29.4.1
ip dhcp pool MEDELLIN_2
 network 172.29.4.128 255.255.255.128
 default-router 172.29.4.129
```

```
ip dhcp excluded-address 172.29.0.1
ip dhcp excluded-address 172.29.1.1
!
ip dhcp pool BOGOTA
 network 172.29.0.0 255.255.255.0
 default-router 172.29.0.1
ip dhcp pool BOGOTA_2
 network 172.29.1.0 255.255.255.0
 default-router 172.29.1.1
```

En la configuración del protocolo DHCP, se puso en práctica lo estipulado en el escenario, mostrando en la imagen anterior esta configuración. Fue necesario crear un pool de direcciones para cada subred para así garantizar que se propaguen las direcciones de manera correcta por la red.

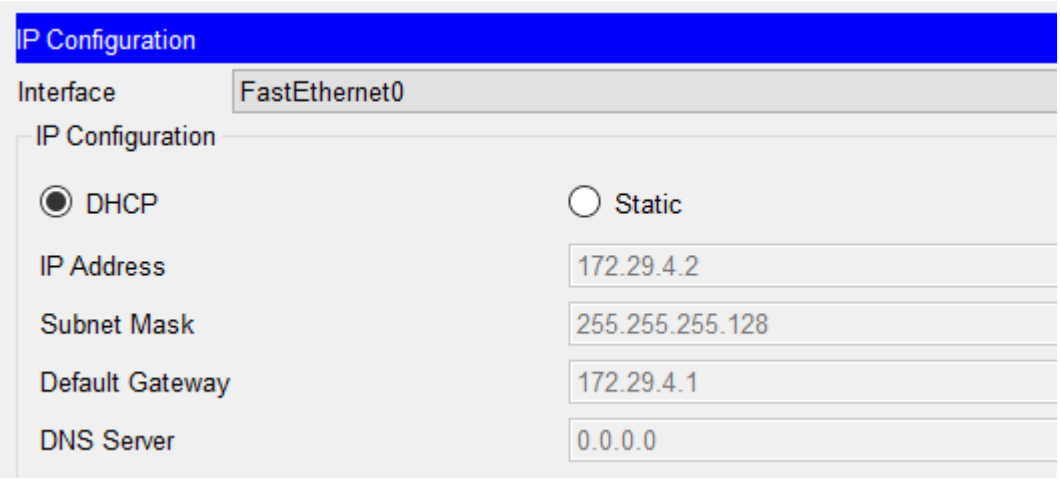


Ilustración 2 Computador de Medellín tomando DHCP

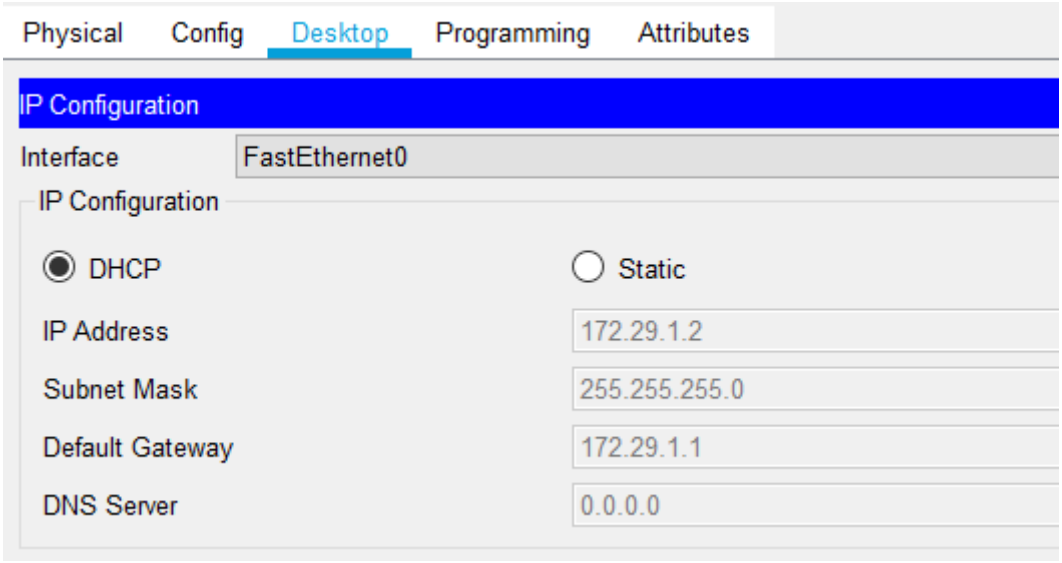


Ilustración 3 Ilustración 3 Computador de Bogotá tomando DHCP

3 ESCENARIO 2

3.1 Topología de red

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.

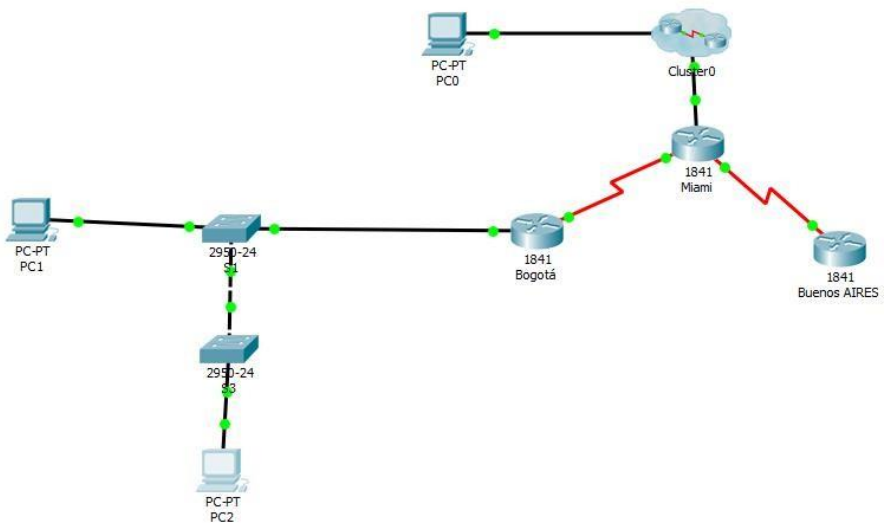
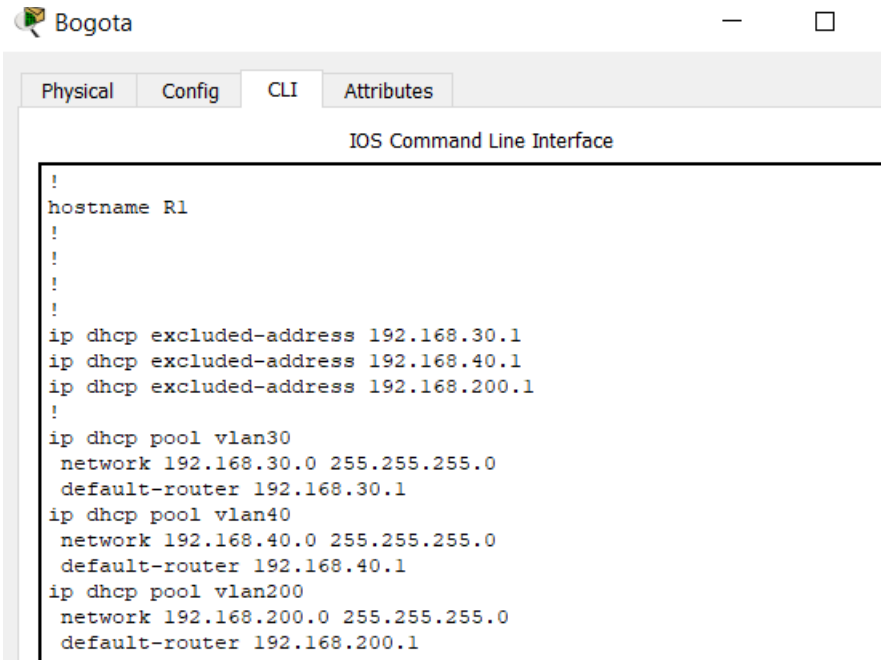


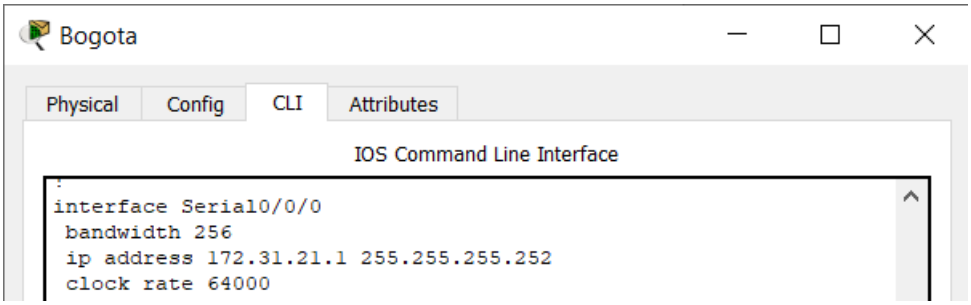
Ilustración 4 Topología de red Escenario 2

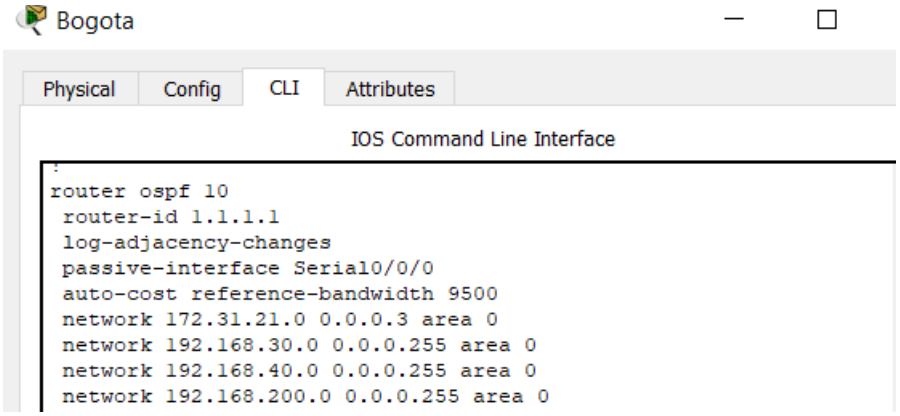
1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

Tabla 1. Parámetros configuración 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	







En las imágenes anteriores se observa la configuración del router R1 (Bogotá), cumpliendo con los parámetros establecidos para este punto. La misma configuración se realizó para los routers R2 y R3.

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

Para la configuración de este punto se ejecutaron los siguientes pasos y comandos:

3.2 Creacion de VLAN

Switch#vlan database

Switch(vlan)#vlan [número de vlan] name [nombre de vlan]

Switch(vlan)#exit

3.3 Asignamos una Vlan a un Puerto (Modo access)

Switch(config)#interface [Interfaz]

Switch(config-if)#switchport access vlan [número de vlan]

3.4 Asignamos el modo trunk a un puerto

Switch(config)#interface [Interfaz]

Switch(config-if)#switchport mode trunk

Switch (config-if)#switchport trunk native vlan [NUMERO DE VLAN]

3.5 Asignar una IP a una Vlan

Switch (config)#interface vlan [NUMERO DE VLAN]

Switch (config-if)#ip address [IP] [MASCARA DE RED]

3.6 Configuracion del Router para Vlan

Router>en

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#no shut

Router(config-if)#interface fastEthernet 0/0.x

Router(config-subif)#encapsulation dot1Q [Número de la VLAN]

Router(config-subif)#ip address [IP] [Mascara]

3.7 Configurar interfaz para Vlan Nativa

Router(config-subif)#interface [INTERFAZ.UnNumero]

Router(config-subif)#encapsulation dot1Q [NUMERO DE VLAN] native

Router(config-subif)#ip address [IP] [MASCARA DE RED]

Con estos comandos se realizó la configuración para todo lo pedido en este paso.

4. En el Switch 3 deshabilitar DNS lookup.

   S3(config)# no ip domain-lookup

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

```
S1(config-if)#int vlan 99
S1(config-if)# ip address 192.168.99.2 255.255.255.

S3(config-if)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
```

Es necesario asignar directamente a las vlan's creadas una dirección ip, primero para cumplir con los requerimientos de la topología y segundo para garantizar la propagación por la red.

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

   S1(config) #int fa 0/2

   S1(config-if) # sh

   S1(config-if) # int ra fa 0/4-23

   S1(config-if) # sh

   S3(config) #int fa 0/2

   S3(config-if) # sh

   S3(config-if) # int ra fa 0/4-23

   S3(config-if) # sh

7. Implementar DHCP y NAT para IPv4

   Implementando NAT estamos garantizando que nuestros dispositivos tengan conexión hacia internet, con esta configuración se está garantizando que al momento de hacer una petición desde/hacia una dirección ip pública desde una privada, nuestro router la convierte garantizando que los paquetes lleguen a la dirección destino y la respuesta sea recibida.

   R2(config)#ip nat inside source static 209.165.200.224 10.10.10.10

   R2(config)#interface fa0/0

R2(config-if)#ip nat outside

R2(config-if)#ip nat inside

R2(config-if)#int s0/0/1

R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

R2(config)#interface fa0/0

R2(config-if)#ip nat outside

R2(config-if)#ip nat inside

R2(config-if)#int s0/0/0

R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

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

```
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#ip domain-name ccna-unad.com
```

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

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

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

```
R2(config)#interface FastEthernet0/0
R2(config-if)# ip nat outside
R2(config-if)#interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)#interface Serial0/0/1
R2(config-if)# ip nat inside
R2(config-if)#ip access-list extended NAT
R2(config-ext-nacl)# permit ip host 0.0.0.0 any
R2(config-ext-nacl)#ip nat inside source list NAT interface
FastEthernet0/0 overload
```

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

```
R3(config)#access-list 100 permit icmp 192.168.4.0 0.0.0.255 209.165.200.224 0.0.0.7
R3(config)#access-list 100 deny icmp 192.168.5.0 0.0.0.255 host 209.165.200.230
```

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

```
R2(config)#access-list 1 deny 192.168.6.0 0.0.0.255
R2(config)#access-list 1 permit host 192.168.40.2
```

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

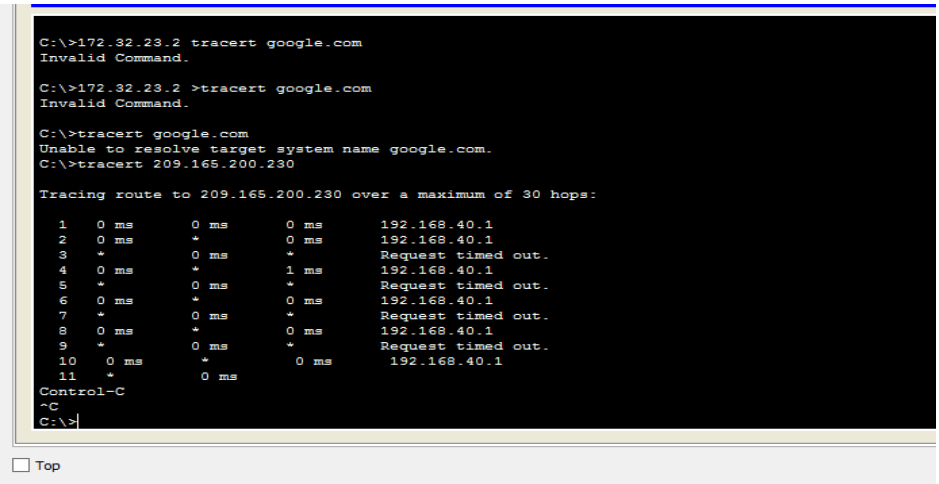


Ilustración 5 Verificación Tracert

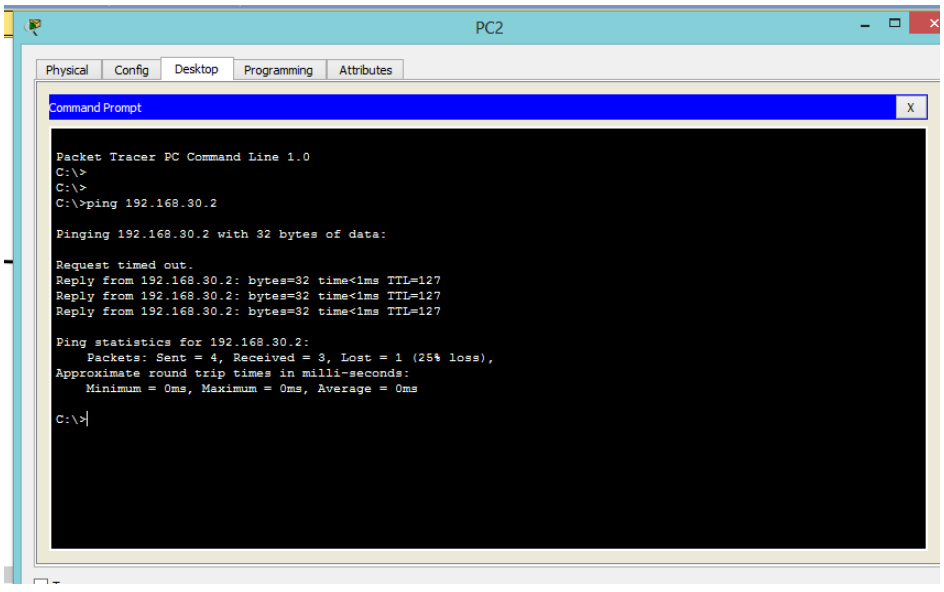


Ilustración 6 Verificación Ping

4 CONCLUSIONES

El presente trabajo implicó poner en práctica e interrelacionar los conceptos aprendidos a lo largo del desarrollo del Curso.

Se reforzó y entreno para conocer y configurar equipos activos de red como son Switch y Routers.

Se logro identificar y desarrollar habilidades para resolver problemas típicos como son validaciones de conexión, utilizando y entendiendo convenientemente el comando PING configuración según topologías.

Se identificó y entendió que clase de protocolos dinámicos de enrutamiento son más convenientemente de usar.

Se demostró lo útil y real que puede ser el software PACKET TRACER como herramienta de diseño y desarrollo, el cual nos puede ofrecer un panorama virtual de un proyecto y nos servirá como maqueta constructiva.

Todo este desarrollo va encaminado a asegurar una red ante posibles ataques y mal utilización de los recursos.

Con el desarrollo de esta actividad, pude aclarar conceptos teóricos los cuales no tenía tan claros. Cada una de las actividades tenía su propio reto y progreso, el cual sino se llevaba en debido orden podía entorpecer o retrasar de forma relativa el adelanto de esta. Tema como la implementación de VLANs se encuentra bastante en las organizaciones y, es una buena manera de empezar a otorgar seguridad en una topología de red.

Un tema el cual me ha llamado la atención y logré establecer como conocimiento fue el configurar el router como servidor DHCP, es práctico y pude quitarme ese mal hábito de pensar que era complicado. El establecer enrutamiento dinámico es la mejor alternativa, desde luego cabe aclarar que se debe tener en claro el direccionamiento estático para temas muy puntuales, teniendo en cuenta que hay dispositivos o servicios los cuales debemos tener fijos, el leer, comprender y aprender RIPv2 y OSPFv2 es una ganancia para mí.

Por último, como administrador de red, el tema más prescindible o que debemos garantizar a nuestro cliente, es el tema de seguridad, algo tan sencillo y simple como

poner o configurar una contraseña para el acceso al router, son cosas que se deben tener en cuenta, porque he tenido la oportunidad de conocer administradores que no tienen esta práctica y, también he conocido las consecuencias de no hacerlo. Sin más, agradecer por todo lo aprendido con este trabajo final.

5 LISTA DE REFERENCIAS

- DevTics, D. (18 de abril del 2017). Configuración Encapsulamiento PPP. []. Recuperado de http://devtics.blogspot.com.

- Del Barrio, David. (7 de enero 2012). Configurar un servidor de DHCP del IOS de Cisco | Packet Tracer. Taller del Bit Recuperado de https://eltallerdelbit.com/servidor-dhcp-packet-tracer/

- Gordon, A [Andrew Gordon]. (2012 febrero 19). Setting up a Loopback Address. [Video]. Recuperado de https://www.youtube.com/watch?v=z9tMTc1_qYg

- Romero Goyzueta, C. A. [Christian Augusto Romero Goyzueta]. (2016 junio 30). How to Create a Cluster on Packet Tracer - Cómo Crear un Cluster en Packet Tracer. [Video]. Recuperado de https://www.youtube.com/watch?v=14pVM2QgeDA.

- Perez, D. (29 de septiembre del 2018). Configuración de VLANs. []. Recuperado de https://todopacketracer.com

- Perez, D. (03 de marzo del 2012). Enrutamiento entre VLANs. []. Recuperado de https://todopacketracer.com.

- Walton, A. (). Implementación Básica de OSPFv2 y OSPFv3. []. Recuperado de https://ccnadesdecero.es