PRUEBA DE HABILIDADES PRACTICAS CCNA

EVALUACION

CAMILO ANDRES CERRO MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA INGENIERIA DE SISTEMAS

BOGOTA, 2019

TABLA DE CONTENIDO

1. Evaluación – Prueba de habilidades prácticas CCNA……...5

1.1 Descripción general de la prueba de habilidades……5

1.2 Lineamientos para la elaboración del Informe…….....5

1.3 Desarrollo de los dos escenarios……...5

2. Escenario 1

2.1 Topología de red…….7

2.2 Parte 1: Configuración del enrutamiento……....7

2.3 Parte 2: Tabla de Enrutamiento……..……8

2.4 Parte 3: Deshabilitar la propagación del protocolo RIP…….9

2.5 Parte 5: Configurar encapsulamiento y autenticación PPP……...10

2.6 Parte 6: Configuración de PAT…….11

2.7 Parte 7: Configuración del servicio DHCP……...……....11

3. Escenario 2……..13

3.1 Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario……...……..13

3.2 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios.

3.3 Verificar información de OSPF……15

3.4 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida……16

3.5 En el Switch 3 deshabilitar DNS lookup…….....16

3.6 Asignar direcciones IP a los Switches acorde a los lineamientos……16

3.7 Desactivar todas las interfaces que no sean utilizadas en el esquema de red……16

3.8 Implement DHCP and NAT for IPv4……...16

3.9 Configurar R1 como servidor DHCP para las VLANs 30 y 40...……16

3.10 Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas……16

3.11 Configurar NAT en R2 para permitir que los host puedan salir a internet……..... 17

3.12 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……17
3.13 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……17
3.14 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute……17

INTRODUCCIÓN

En el siguiente trabajo realizado se encuentra el desarrollo de cada una de las actividades propuesta para este módulo, el cual contienen los modelos OSI y el direccionamiento IP, escenarios de redes LAN/WAN, que se realizaron en diferentes topologías de red.

Analizando así el funcionamiento y comportamiento de diversas métricas de enrutamiento usando comandos de administración de redes.

La ayuda del software Cisco Packet Tracer como ayuda de la implementación de las redes, es fundamental para el desarrollo de cada una de las actividades ya que como grupo podemos revisar lo que los demás aportan al consolidado y el funcionamiento de cada una de las redes.

1. Evaluación – Prueba de habilidades prácticas CCNA

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.

1.2 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

1.3 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.

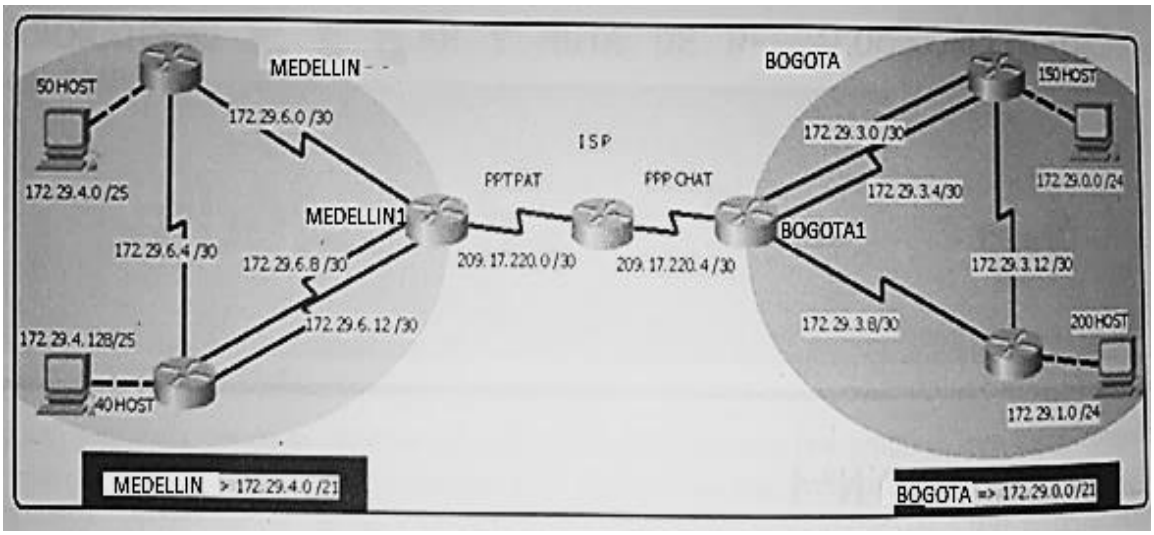
IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso.

2. Descripción de escenarios propuestos para la prueba de habilidades

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.

2.1 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.

2.2 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.

Medellin

```
router rip
 version 2
 network 172.29.0.0
 no auto-summary
!
router rip
 version 2
 network 172.29.0.0
 no auto-summary
!
```

Bogota

```
router rip
 version 2
 network 172.29.0.0
 no auto-summary
!
```

Ya que el enrutamiento rip funciona con la clase para esta caso la B, el rip se ve de la misma forma en las dos ciudades

Internet

```
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
!
```

2.3 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.

Medellin

```
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

```
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
```

Internet

```
     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#
```

2.4 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

```
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)#
```

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

2.5 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.

MEDELLIN

```
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
!
```

BOGOTA

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

INTERNET

```
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
```

2.6 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
```

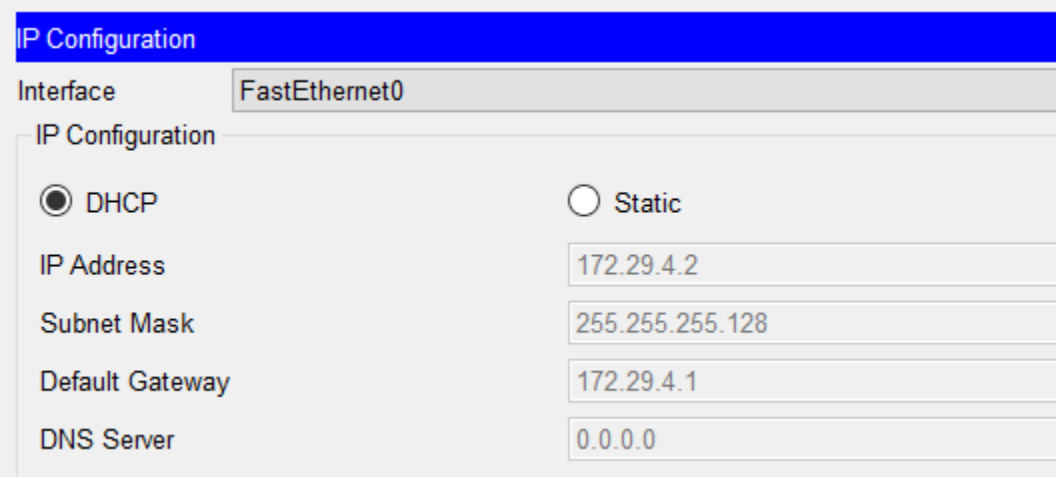
```
interface Serial0/1/0
 ip address 209.17.220.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ip nat outside
 clock rate 2000000
!
interface Serial0/1/1
 ip address 172.29.6.2 255.255.255.252
 ip nat inside
 clock rate 2000000
!
```

2,7 Parte 7: Configuración del servicio DHCP.

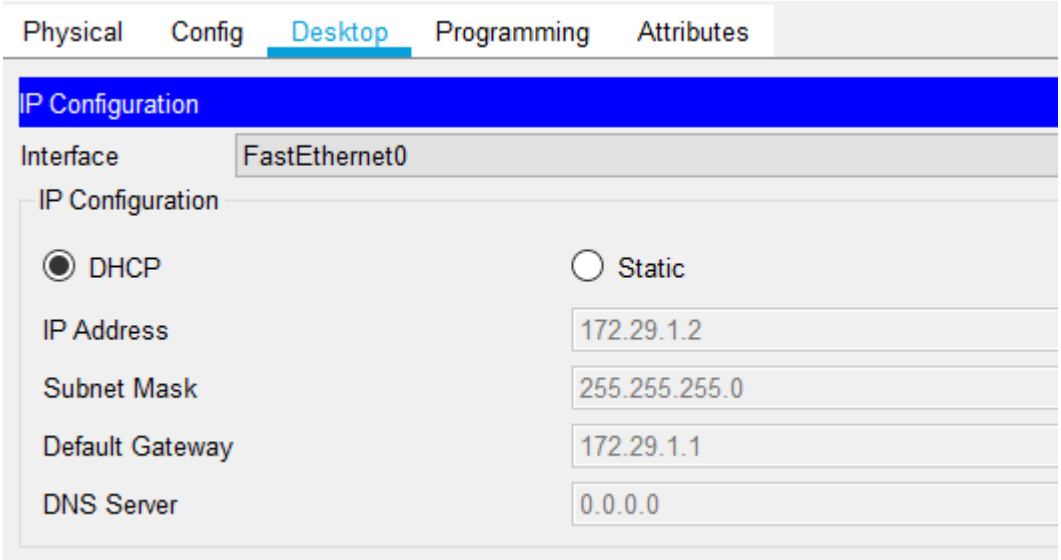
```
ip dhcp excluded-address 172.29.4.1
ip dhcp excluded-address 172.29.4.129
!
ip dhcp pool MEDELLIN
 network 172.29.4.0 255.255.255.128
 default-router 172.29.4.1
ip dhcp pool MEDELLIN_2
 network 172.29.4.128 255.255.255.128
 default-router 172.29.4.129
```

```
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
```

Computador de Medellín tomando DHCP



Computador de Bogotá tomando DHCP

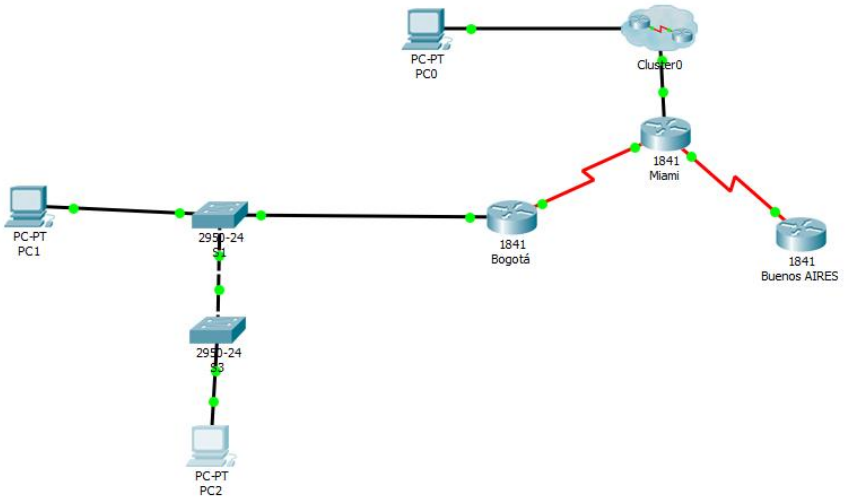


DHCP relay

```
interface GigabitEthernet0/0
 ip address 172.29.4.129 255.255.255.128
 ip helper-address 172.29.6.5
 duplex auto
 speed auto
```

3. Escenario 2

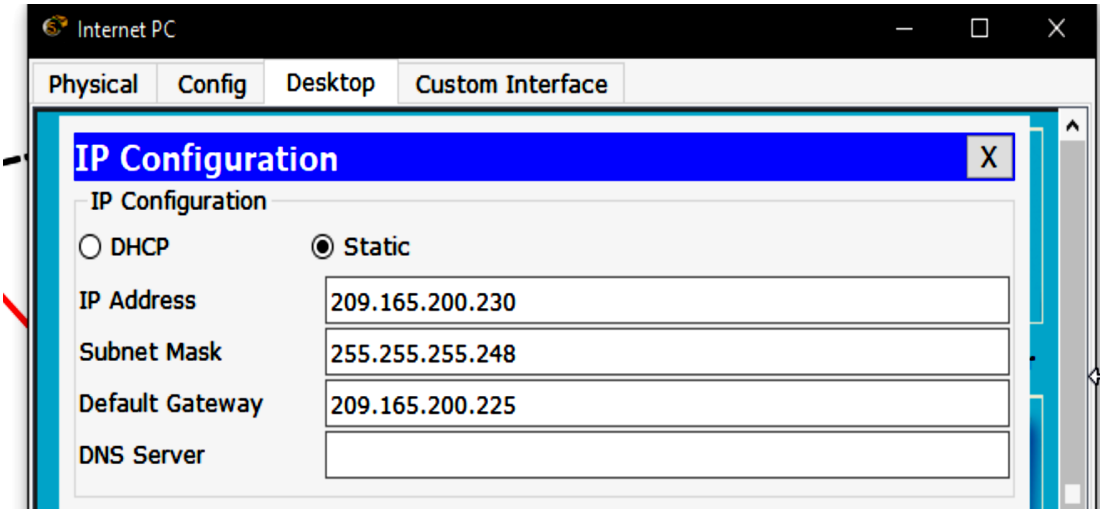
Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos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



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

Se configura la ip del PC internet con Ip address 209.165.200.230, Subnet Mask 255.255.255.248, Default Gateway 209.165.200.225

Se anexa evidencia del cambio por una ip estática:



Se configura el Router 1 o R1:

Se relacionan los comandos a ejecutar que servirán para crear políticas de acceso, direccionamientos, políticas de seguridad:

Configuración Router R1:

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Prohibido el acceso no autorizado#
R1(config)#int s0/0
```

Configuracion de los puertos seriales entre R1 y R2

```
R1(config-if)#description R1-R2
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#no shutdown
R1(config-if)#exit
```

Se crea una ruta estatica por defecto que direccione el tráfico que no está explícitamente defino

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0
R1(config)#exit
```

Se configura el Router 2 o R2:

R/ Se relacionan los comandos a ejecutar que servirán para crear políticas de acceso, direccionamientos entre los diferentes dispositivos como R1, R3, Pc Internet y Web Server, Además de las políticas de seguridad y mensajes:

Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#enable
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner
R2(config)#banner motd #Prohibido el acceso no autorizado!#

Configuracion de los puertos seriales entre R2 y R3 R2(config)#int s0/1
R2(config-if)#description R2-R1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown

Configuracion de los puertos seriales entre R2 y R3
R2(config-if)#int s0/0
R2(config-if)#description R2-R3
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut

Configuracion de los puertos entre R2 y pc Internet
R2(config-if)#int f0/0
R2(config-if)#description R2-Intertet
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown

Configuracion de los puertos entre R2 y WebServer

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

Se crea una ruta estatica por defecto que direccione el tráfico que no está explícitamente defino

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

Se configuran los siguientes dispositivos en este caso el Router 3 o R3:

Se relacionan los comandos a ejecutar que servirán para crear políticas de acceso, direccionamientos entre los diferentes dispositivos como R1, R3, Pc Internet y Web Server, Además de las políticas de seguridad y mensajes, también los loopback 4,5,6 de Web server:

Router>en Router#conf t
R3(config)#hostname R3
R3(config)#no ip domain-lookup (más adelante se pedirá, se configure de una vez)
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #Prohibido el acceso no autorizado!#
R3(config)#int s0/1
R3(config-if)#Description R3-R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shut

Configuracion ip del loopback 4 de WebServer

R3(config-if)#int lo4
R3(config-if)#ip add 192.168.4.1 255.255.255.0

Configuracion ip del loopback 5 de WebServer

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

Configuracion ip del loopback 6 de WebServer

R3(config-if)#int lo6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit

Se crea una ruta estatica por defecto que direccione el tráfico que no está explícitamente defino

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1
R3(config)#exit
R3#

Se configuran los siguientes dispositivos en este caso el Web Server:

Se realiza la configuración directamente en el modo ambientación del packet tracer del web server con la ip estática correcta, en este caso: Ip address 10.10.10.10., Subnet Mask 255.255.255.0, Default Gateway 10.10.10.1

Se configuran los siguientes dispositivos en este caso el Switch 1 o S1:

Se relacionan los comandos a ejecutar que servirán para crear políticas de acceso, además de las políticas de seguridad y mensajes:

Switch>en
Switch#conf t
Switch(config)#hostname s1
s1(config)#enable secret class
s1(config)#line console 0

```
s1(config-line)#password cisco
s1(config-line)#login
s1(config-line)#line vty 0 4
s1(config-line)#password cisco
s1(config-line)#login
s1(config-line)#service password-encryption
s1(config)#banner
s1(config)#banner motd #Prohibido el acceso no autorizado!#
s1(config)#exit
```

Se configuran los siguientes dispositivos en este caso el Switch 3 o S3:

Se relacionan los comandos a ejecutar que servirán para crear políticas de acceso, además de las políticas de seguridad y mensajes:

```
Switch>en
Switch#conf t
Switch(config)#hostname s3
s3(config)#enable secret class
s3(config)#line console 0
s3(config-line)#password cisco
s3(config-line)#login
s3(config-line)#line vty 0 4
s3(config-line)#password cisco
s3(config-line)#login
s3(config-line)#service pass
s3(config-line)#service password-encryption
s3(config)#banner motd #Prohibido el acceso no autorizado!#
s3(config)#exit
```

Verificar que los equipos tengan conectividad usando el comando ping.

Conexión entre R1 y R2:

```
R1>en
Password:
R1#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/25 ms

R1#
```

Copy

Conexión entre R2 y R3:

```
R2>en
Password:
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/20 ms

R2#
```

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

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

• Paso 1: Configuramos OSPFv2 para el Router R1 según especificación de la tabla:

R1(config)#router ospf 1
Especificacamos al router:
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0

Configuramos para calcular dinámicamente el costo de la interfaz OSPF:

R1(config-router)#auto-cost reference-bandwidth 1000
R1(config-router)#exit

Indicamos la velocidad de la interfaz:

R1(config)#int s0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#exit

• Paso 2: Configuramos OSPFv2 para el Router R2 según especificación de la tabla:

R2>en R2#conf t
R2(config)#router ospf 1

Especificamos al router:

R2(config-router)#router-id 5.5.5.5
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/1

Configuramos para calcular dinámicamente el costo de la interfaz OSPF:

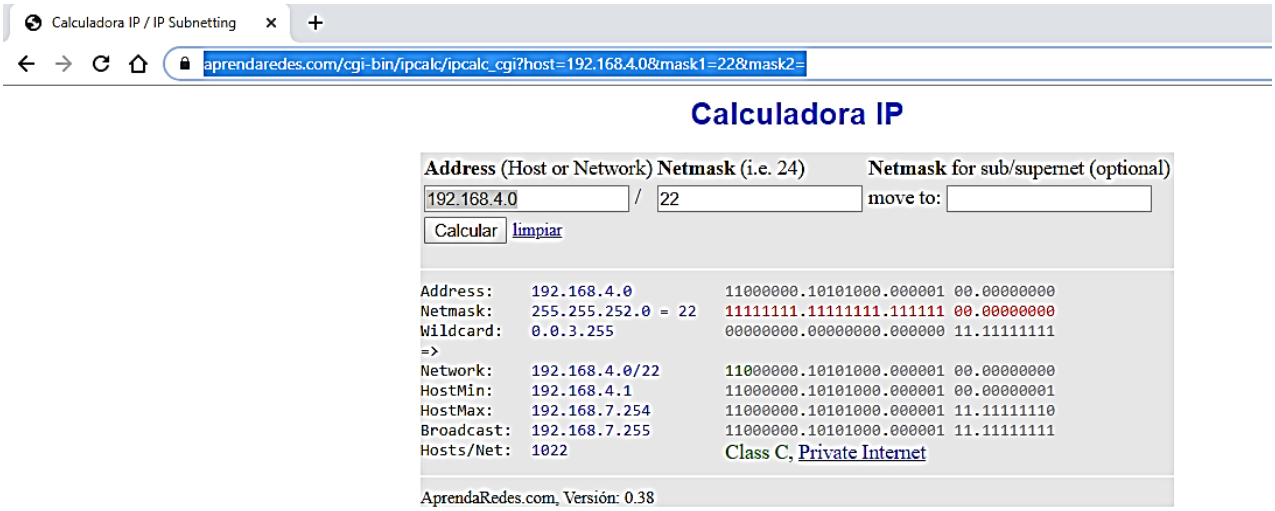
R2(config-router)#auto-cost reference-bandwidth 1000
R2(config-router)#exit

Indicamos la velocidad de la interfaz:

R2(config)#int s0/1
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#exit

• Paso 3: Se usa una sola dirección por sumatoria, la cual es 192.168.4.0/22 para las interfaces LAN (loopback), después busco la wildcar en una calculadora en línea:

https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi?host=192.168.4.0&mask1=22&mask2=



• Paso 4: Configuramos OSPFv2 para el Router R3 según especificación de la tabla:

R3>en R3#conf t
R3(config)#router ospf 1
R3(config-router)#router-id 8.8.8.8
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0

Se suman las direcciones y la Wildcar hallada en el paso anterior:

R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6

Configuramos para calcular dinámicamente el costo de la interfaz OSPF:
R3(config-router)#auto-cost reference-bandwidth 1000
R3(config-router)#exit

Indicamos la velocidad de la interfaz:
R3(config)#int s0/1
R3(config-if)#bandwidth 128
R3(config-if)#exit

• Paso 5: Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Primero visualizamos tablas de enrutamiento y routers conectados por OSPFv2

Visualizamos en R1 usando “show ip ospf neig” Evidencia en packet tracer:

```
R1>en
Password:
Password:
R1#show ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:39    172.31.21.2     Serial0/0
R1#
```

Visualizamos en R2 usando “show ip ospf neig” Evidencia en packet tracer:

```
Password:
R2#show ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:31    172.31.21.1     Serial0/1
8.8.8.8           0   FULL/  -        00:00:35    172.31.23.2     Serial0/0
R2#
```

Visualizamos en R3 usando “show ip ospf neig” Evidencia en packet tracer:

```
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip ospf neig


Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:32    172.31.23.1     Serial0/1
R3#
```

- Visualizamos un resumen de las interfaces por OSPF:

En R1:

R1# show ip ospf interface

```
R1#show ip ospf interface

Serial0/0 is up, line protocol is up
  Internet address is 172.31.21.1/30, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
R1#
```

En R2:

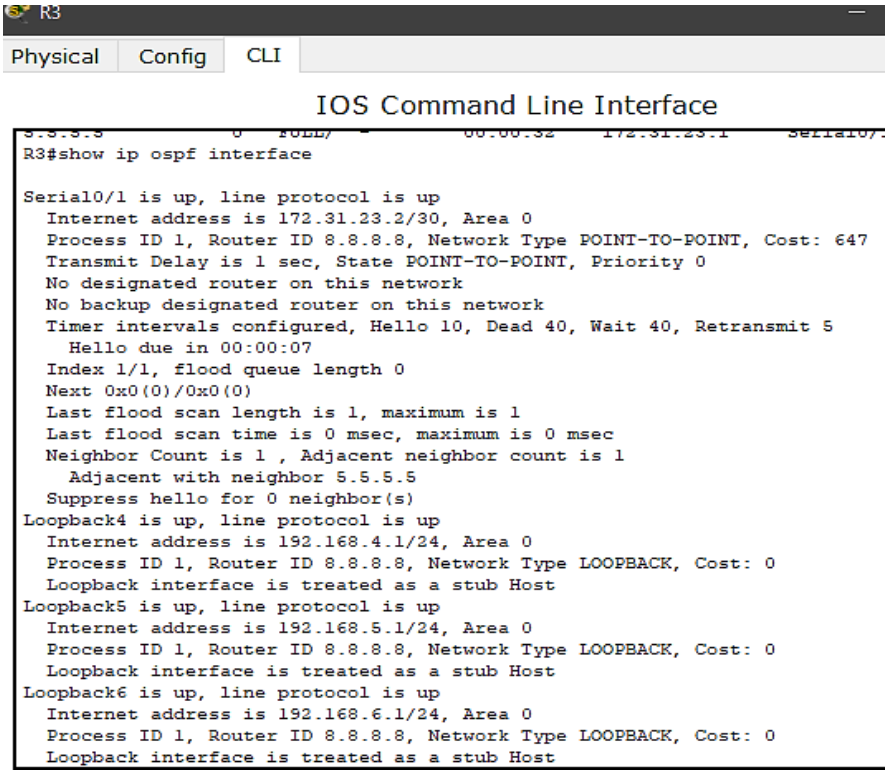
R2# show ip ospf interface

```
R2#
R2#show ip ospf interface

Serial0/1 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 647
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 750
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
 --More--
```

En R3:

R3# show ip ospf interface



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

En R1: Con el comando: Show ip protocols:

```
R1#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/1
    Serial0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:08:44
    5.5.5.5              110      00:20:02
    8.8.8.8              110      00:17:45
  Distance: (default is 110)
```

En R2: Con el comando: Show ip protocols:

```
R2#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:09:50
    5.5.5.5              110      00:21:06
    8.8.8.8              110      00:18:49
  Distance: (default is 110)
```

En R3, con el comando: Show ip protocols:

```
R3#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 8.8.8.8
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:11:32
    5.5.5.5              110      00:22:49
    8.8.8.8              110      00:20:32
  Distance: (default is 110)

R3#
```

• Paso 6: Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, InterVLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Configuramos en S1 con los siguientes comandos:

s1>en
s1#conf t

Configuramos las Vlan con su respectivo nombre:

s1(config)#vlan 30
s1(config-vlan)#name Administración
s1(config-vlan)#vlan 40
s1(config-vlan)#name Mercadeo
s1(config-vlan)#Vlan 200
s1(config-vlan)#name Mantenimiento
s1(config-vlan)#vlan 99
s1(config-vlan)#name LAN_S1_S3
s1(config-vlan)#exit
s1(config)#int vlan 99
s1(config-if)#ip address 192.168.99.2 255.255.255.0
s1(config-if)#no shut
s1(config-if)#exit
s1(config)#ip default-gateway 192.168.30.1

Configuramos los puertos troncales:

s1(config)#int f0/3
s1(config-if)#switchport mode trunk
s1(config-if)#switchport trunk native vlan 1
s1(config-if)#exit
s1(config)#int f0/24
s1(config-if)#switchport mode trunk
s1(config-if)#switchport trunk native vlan 1
s1(config-if)#exit

Configuramos los puertos de acceso y seguridad:

s1(config)#int range f0/1-2, f0/4-23, g0/1-2
s1(config-if-range)#switchport mode access
s1(config-if-range)#int f0/1
s1(config-if)#switchport mode access
s1(config-if)#switchport access vlan 30
s1(config-if)#int range f0/2, f0/4-23, g0/1-2
s1(config-if-range)#shutdown
s1(config-if-range)#exit

Configuramos en S3 con los siguientes comandos:

s3>en
s3#conf t

Configuramos las Vlan con su respectivo nombre:

s3(config)#vlan 30
s3(config-vlan)#name Administracion
s3(config-vlan)#vlan 40
s3(config-vlan)#name Mercadeo
s3(config-vlan)#vlan 200
s3(config-vlan)#name Mantenimiento
s3(config-vlan)#vlan 99
s3(config-vlan)#Name LAN_S1_S3
s3(config-vlan)#exit
s3(config)#int vlan 99
s3(config-if)#ip address 192.168.99.3 255.255.255.0
s3(config-if)#no shut
s3(config-if)#exit
s3(config)#ip default-gateway 192.168.40.1

Configuramos los puertos troncales:

s3(config)#int f0/3
s3(config-if)#switchport mode trunk
s3(config-if)#switchport trunk native vlan 1

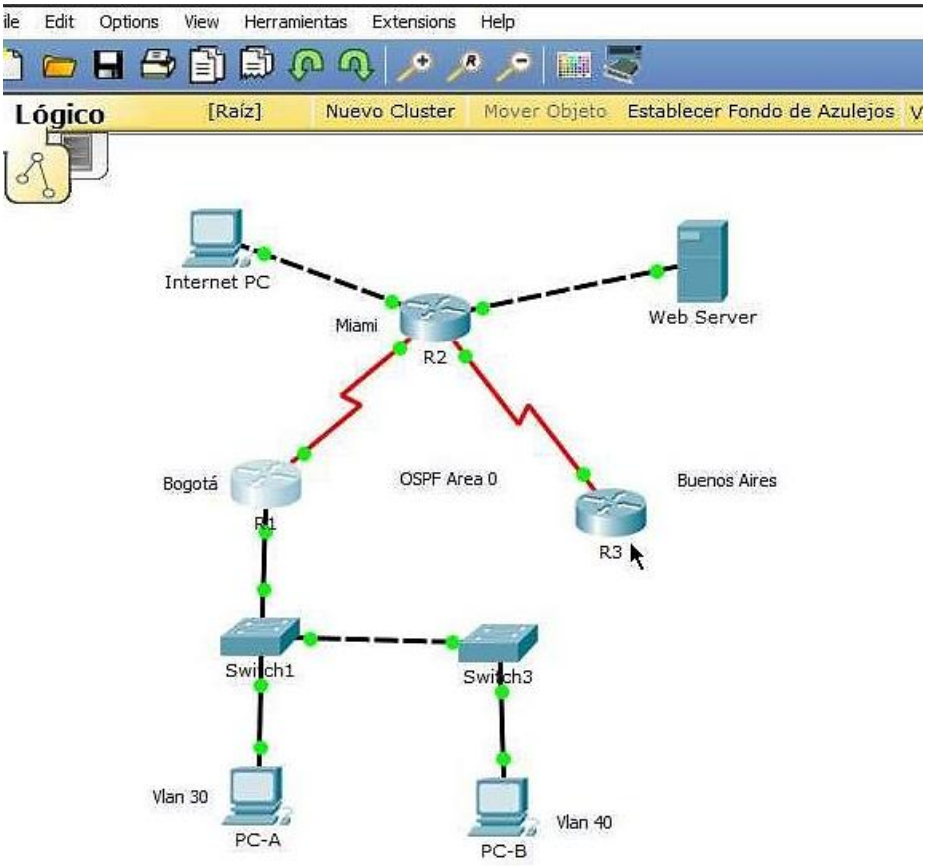
Configuramos los puertos de acceso y seguridad:

s3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
s3(config-if-range)#switchport mode access
s3(config-if-range)#shut
s3(config-if-range)#exit
s3(config)#int f0/1
s3(config-if)#no shut
s3(config-if)#switchport mode access
s3(config-if)#switchport access vlan 40
s3(config-if)#exit
s3(config)#

Configuramos 802.1Q en R1 con los siguientes comandos:

```
R1>en R1#conf t
R1(config)#int f0/0.30
R1(config-subif)#description Administracion_LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.40
R1(config-subif)#description Mercadeo_LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.200
R1(config-subif)#description Mantenimiento_RED
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.99
R1(config-subif)#description s1_s3_red
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0
R1(config-if)#no shut
R1(config-if)#exit
```

Evidencia la correcta conectividad de los dispositivos en la red.



Basados en la gráfica anterior se analiza que todos los puntos interconectan de manera correcta porque los puntos en las conexiones son de color verde, además de unas pruebas de ping que fueron satisfactorias.

- En el Switch 3 deshabilitar DNS lookup.

R3>en
R3#conf t
R3 (config)# no ip domain-lookup
R3 (config)#exit

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

En pasos anteriores las configuraciones ip se realizaron de manera correcta de los switch.

• Paso 7: Implement DHCP and NAT for IPv4, Configurar R1 como servidor DHCP para las VLANs 30 y 40, Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

A continuación, se realizará la configuración correcta para que R1 sirva de DHCP para las Vlan antes mencionadas con su respectivo rango:

```
R1>en
R1#conf t
```

Configuramos el DHCP excluyendo las primeras 30 ip de las Vlan 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
```

Configurar R1 como servidor DHCP:

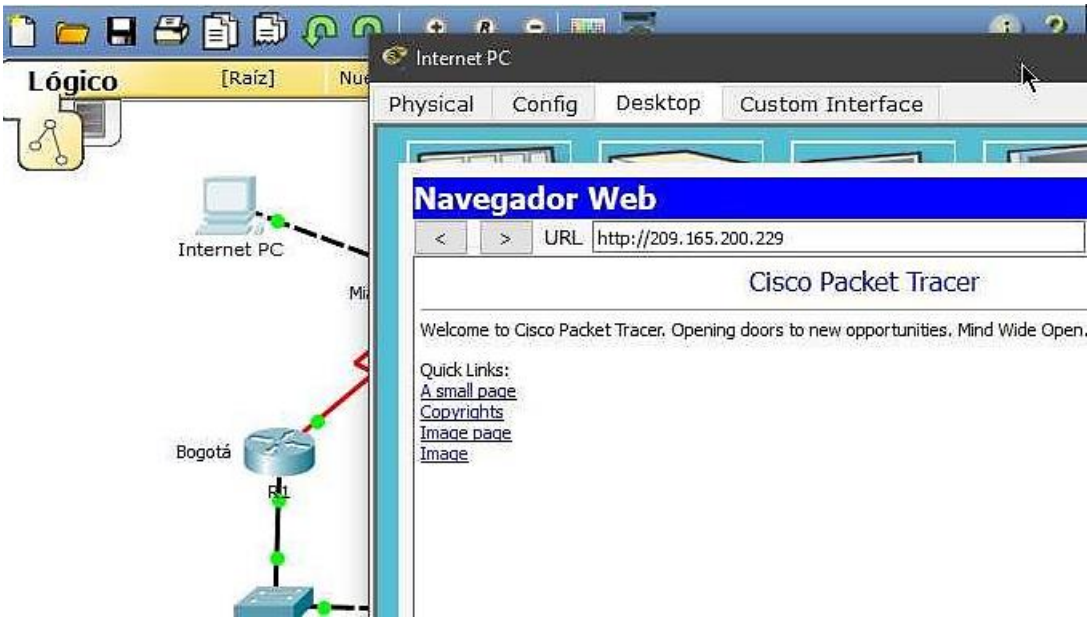
```
R1(config)#ip dhcp pool Administracion
R1(dhcp-config)#dns-server 10.10.10.11
R1(config)#ip dhcp pool Administracion
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool Mercadeo
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#ip domain-name ccna.com
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#exit
```

A continuación, se realizará la configuración del NAT estática y dinámica correcta para R2.

```
R2>en
R2#conf t
R2(config)#user usuarioweb privilege 15 secret cisco
R2(config)#ip http server
R2(config)#ip http secure-server
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

```
R2(config)#ip nat pool Internet 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool Internet
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#exit
```

• Para verificar el DHCP y NAT accediendo al sitio web 209.165.200.229 desde la PC de Internet, demostrando que los hosts pueden salir a internet:



Paso 8:

• 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.

• 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.

Se realizará la restricción de acceso a las líneas VTY en el Router R2

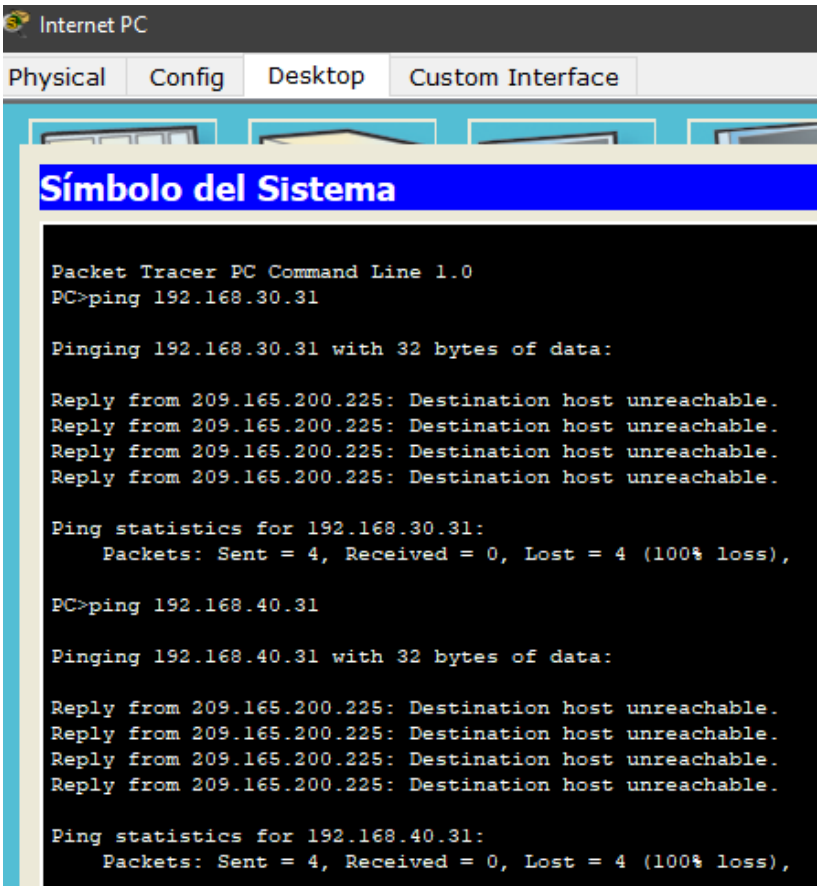
```
R2>en
R2#conf t
R2(config)#ip access-list standard Admin
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class Admin in
R2(config-line)#exit
```

Se realizará unos pasos de ACL extendida en R2 para proteger la red del tráfico que genera el acceso a internet.

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

• Paso 9: Verificamos los procesos de comunicación y redireccionamiento de tráfico en la red:

Ping de Internet PC a PC-A y PC-C:



```
R1>en
Password:
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/10 ms

R1#traceroute 192.168.30.31
Type escape sequence to abort.
Tracing the route to 192.168.30.31
```

CONCLUSIONES

En el presente trabajo se logró realizar el desarrollo de cada una de las actividades propuesta para este módulo, en el cual se realizaron actividades relacionada con los modelos OSI y el direccionamiento IP, escenarios de redes LAN/WAN, que se realizaron en diferentes topologías de red.

Se logró analizar el funcionamiento y comportamiento de diversas métricas de enrutamiento usando comandos de administración de redes. Estos ejercicios se realizaron mediante el software Cisco Paquet Traicer para la implementación de las redes.

Referencias Bibliográficas

CISCO. 2018. Configurar ACL de IP de uso general. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/28447- ACLsamples.html

Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://staticcourse- assets.s4.amazonaws.com/RSE50ES/module3/index.html#3.2.1.3

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course- assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route- router-cisco/

Eugenio Duarte, E. D. (2016, 12 abril). Cisco CCNA – Cómo Configurar NAT Overload En Cisco Router. Recuperado 5 junio, 2019, de http://blog.capacityacademy.com/2014/06/18/cisco-ccna-como-configurar- nat-overload-en-cisco-router/

Ángel Calvo, A. C. (2015, 11 mayo). RIP Cisco, aprende a configurar este protocolo facilmente.. Recuperado 5 junio, 2019, de https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-y- sencilla/