

PRUEBA DE HABILIDADES Y PRACTICAS CCNA

CECILIA CAMAÑO NIETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIAS
PROGRAMA INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

PRUEBA DE HABILIDADES Y PRACTICAS CCNA

CECILIA CAMAÑO NIETO

TRABAJO PARA OBTENER EL TITULO DE INGENIERIA DE SISTEMAS

ASESOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA
PROGRAMA INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

CONTENIDO

	Pág.
1. INTRODUCCIÓN	4
2. OBJETIVOS.....	5
2.1 OBJETIVO GENERAL.....	5
2.2 OBJETIVOS ESPECÍFICOS.....	5
5. ESCENARIO 1	6
5.1 TOPOLOGIA DESARROLLADA EN EL LABORATORIO.....	7
5.2 Inicializar dispositivos	8
5.3 Configurar los parámetros básicos de los dispositivos	9
5.5 Configurar la seguridad del switch, las VLAN y el routing entre VLAN	18
5.6 Configurar el protocolo de routing dinámico RIPv2.....	23
5.7 Implementar DHCP y NAT para IPv4.....	30
5.8 Configurar NTP.....	34
6. ESCENARIO 2	37
Router 6.1 CONFIGURACIÓN DEL ENRUTAMIENTO	44
6.2 Tabla de Enrutamiento.....	48
6.2 Deshabilitar la propagación del protocolo OSPF	55
6.3 Verificación del protocolo OSPF	56
Configurar encapsulamiento y autenticación PPP	67
CONCLUSIONES	70
BIBLIOGRAFÍA.....	71

LISTAS DE TABLAS

Tabla 1 Verificar la conectividad de la red.....	17
Tabla 2 Verificar la conectividad de la red	21
Tabla 3 Verificar informacion de RIP.....	24
Tabla 4 Verificar el protocolo DHCP Y LA NAT.....	31
Tabla 5 Verificacion con comandos	35
Tabla 6 tabla enrutamiento	48

TABLA DE FIGURAS

FIGURA 1 Escenario 1 Topologia.....	6
FIGURA 2 Topologia de Laboratorio.....	7
FIGURA 3 Configurar la computadora de Internet.....	10
FIGURA 4 Configurar IPv6 en la computadora de Internet.....	11
FIGURA 5 Ping de R1 a R2.....	17
FIGURA 6 Ping de R2 a R3.....	18
FIGURA 7 Ping de pc de internet a gateway predeterminado.....	18
FIGURA 8 Ping de S1 a gateway vlan 99.....	22
FIGURA 9 Ping de S3 a gateway vlan 99.....	22
FIGURA 10 Ping de S1 a gateway vlan 21.....	22
FIGURA 11 Ping de S3 a gateway vlan 23.....	22
FIGURA 12 Enrutamiento en R1.....	25
FIGURA 13 Tabla de rutas en R1.....	26
FIGURA 14 Seccion RIP en R1.....	26
FIGURA 15 Enrutamiento en R2.....	26
FIGURA 16 Tabla de rutas en R2.....	27
FIGURA 17 Seccion de RIP en R2.....	28
FIGURA 18 Enrutamiento en R3.....	28
FIGURA 19 Tabla de rutas RIP en R3.....	29
FIGURA 20 Seccion de RIP en R3.....	29
FIGURA 21 PC-A.....	32
FIGURA 22 PC_C.....	32
FIGURA 23 Ping pc-c a pc-a.....	32
FIGURA 24 Navegador web.....	33
FIGURA 25 Asociaciones ntp en r1.....	34
FIGURA 26 Telnet a R2.....	35
FIGURA 27 Topologias Escenario 2.....	37
FIGURA 28 Tabla de enrutamiento MEDELLIN2.....	48
FIGURA 29 Tabla de enrutamiento MEDELLIN3.....	49
FIGURA 30 Tabla de enrutamiento MEDELLIN1.....	50
FIGURA 32 Tabla de enrutamiento BOGOTA1.....	52
FIGURA 33 Tabla de enrutamiento BOGOTA3.....	53
FIGURA 34 Tabla de enrutamiento BOGOTA2.....	54
FIGURA 35 Protocolo ospf en MEDELLIN2.....	56
FIGURA 36 Protocolo ospf en MEDELLIN3.....	57
FIGURA 37 Protocolo ospf en MEDELLIN1.....	58
FIGURA 38 Protocolo ospf en BOGOTA1.....	59

FIGURA 39 Protocolo ospf en BOGOTA3	60
FIGURA 40 Protocolo ospf en BOGOTA2	61
FIGURA 41 Verificacion protocolo ppp	63
FIGURA 42 Traducción de direcciones en MEDELLIN1	65
FIGURA 43 Traducciones en BOGOTA1	66
FIGURA 44 Prueba DHCP PC1	69
FIGURA 45 Prueba DHCP PC	69
FIGURA 1 Arrendamiento de direcciones en MEDELLIN2	69

RESUMEN

El propósito de este trabajo es desarrollar la evaluación denominada “Prueba de habilidades prácticas”, la cual es parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias, habilidades y conocimiento que fueron adquiridas a lo largo del diplomado creado por la Universidad Nacional Abierta y a Distancia.

Lo fundamental es comprobar recursivamente los niveles de comprensión y solución de problemas referentes a diversos aspectos de Networking. Para esta actividad, se realizaron los ejercicios asignados en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación y muestras de evidencia 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.

Tomando en cuenta que la evaluación de habilidades está conformada por dos escenarios, el paso a paso de configuración para este trabajo fue desarrollado con la herramienta Packet Tracer y GNS3.

ABSTRACT

The purpose of this work is to develop the evaluation called "Practical Skills Test", which is part of the evaluation activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of competencies, skills and knowledge that were acquired throughout of the diploma created by the National Open and Distance University.

The fundamental thing is to recursively check the levels of understanding and problem solving regarding various aspects of Networking. For this activity, the exercises assigned in each of the two (2) proposed scenarios were performed, accompanied by the respective documentation processes and evidence samples of the solution, corresponding to the registration of the configuration of each of the devices, the detailed description of the step-by-step of each of the stages carried out during its development, the registration of the connectivity verification processes through the use of ping, traceroute, show ip route commands, among others.

Taking into account that the skills assessment is made up of two scenarios, the stepby-step configuration for this work was developed with the Packet Tracer tool and GNS3

GLOSARIO

Conectividad: es la capacidad de un dispositivo de conectarse con otro Dispositivo de una forma autónoma.

Ping: comando utilizado para realizar un diagnóstico de estado de comunicación Entre dos o más equipos en el cual se puede determinar la velocidad, calidad y Estado de red.

Dirección IP: es un direccionamiento utilizado para identificar un dispositivo en la Red.

Protocolos de enrutamiento: conjunto de reglas que permiten determinar la mejor Ruta para enviar paquetes de datos entre routers.

Puertos troncales: enlace punto a punto para enviar y recibir el tráfico entre routers o switches

DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar Información de dominio y la dirección IP de cada uno de los dispositivos que Conforman o acceden a una red.

DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en El que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna A los clientes en el momento en el que se encuentran disponibles.

Encapsulamiento: es el proceso en el que los datos que se encuentran Dispuestos para ser enviados a través de una red se ubican en paquetes con la Capacidad de ser administrados y rastreados por el administrador de la red NAT. Protocolo con el cual se intercambian o transportan paquetes entre dos redes Normalmente incompatibles.

OSPF: protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-Estado.

Topología física: disposición de cada uno de los dispositivos o hardware dentro De una red.

Topología lógica: es la forma que utilizan los hosts para comunicarse a través de Una red

1. INTRODUCCIÓN

El actual documento, hace parte del proceso de la prueba de habilidades prácticas, la cual hace parte de las actividades evaluativas de Diplomado de profundización CCNA, la cual busca comprobar el nivel de desarrollo de competencias y habilidades que se adquirieron en el transcurso del diplomado y a través de la cual se pondrá a prueba los grados de conocimiento y solución de problemas relacionados con diversos aspectos de Networking.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar todas las habilidades prácticas, teóricas y experiencia como futura ingeniera de la Universidad Nacional Abierta y a Distancia, para identificar y aplicar una solución a un caso o situación estudio de problema de Networking.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar que dispositivos utilizar para la construcción de una topología de Red. Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar VLANs en switches, configuración de NTP e inter Vlan Routing.
- Determinar la configuración necesaria para la implementación de RIPv2, Protocolo dinámico de Routing.
- Implementación de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.

ESCENARIO 1

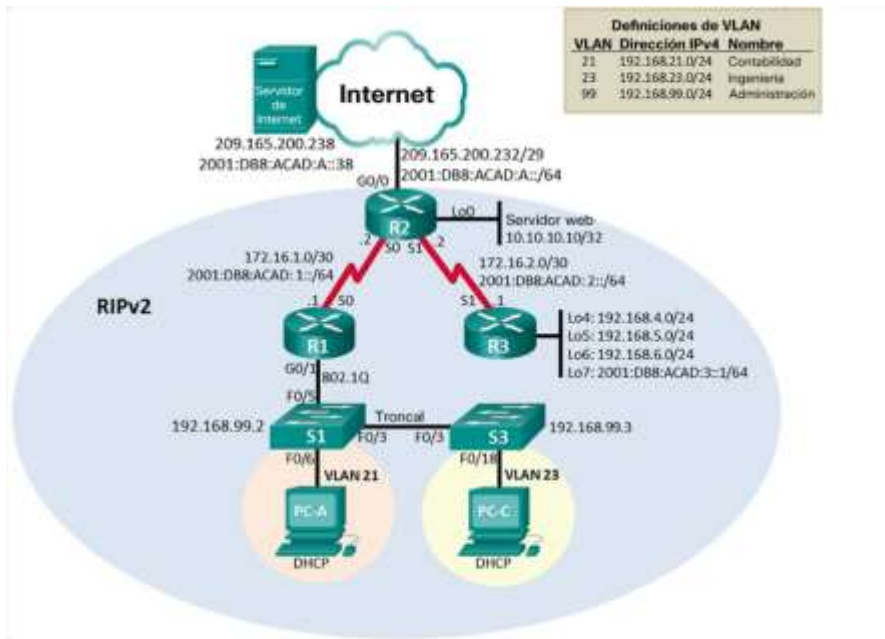


FIGURA 2 Escenario 1 Topología

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

TOPOLOGIA DESARROLLADA EN EL LABORATORIO

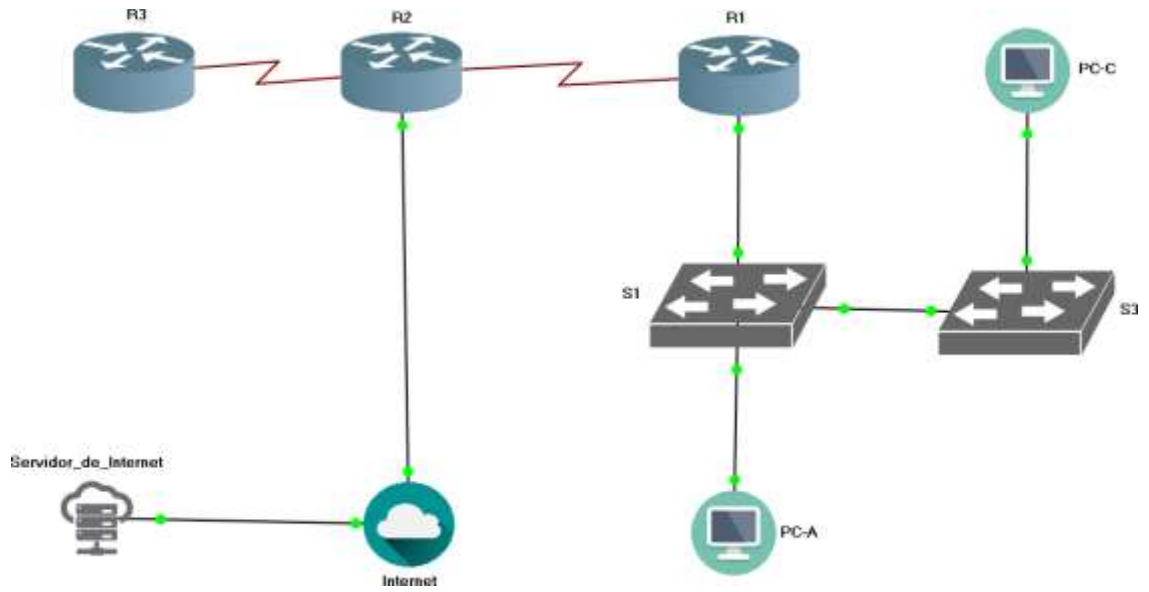


FIGURA 3 Topología de Laboratorio

Inicializar dispositivos

En la inicialización de los dispositivos se eliminan los startup-config de los routers y Switches y se eliminan los datos de la VLAN anterior a su vez se cargan nuevamente los dispositivos mediante los siguientes comandos

R1

```
#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
Presionamos enter*  
Router#reload  
Proceed with reload? [confirm]  
Presionamos enter
```

R2

```
Router#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
Presionamos enter  
Router#reload  
Proceed with reload? [confirm]  
Presionamos enter
```

R3

```
Router#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
Presionamos enter  
Router#reload  
Proceed with reload? [confirm]  
Presionamos enter
```

S1

```
Switch#erase startup-config  
Switch#reload  
Proceed with reload? [confirm]
```

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

Presionamos enter

S3

Switch#erase startup-config

Switch#reload

Proceed with reload? [confirm]

Presionamos enter

Switch#delete flash: vlan.dat

Delete flash:/vlan.dat? [confirm]

5.3 Configurar los parámetros básicos de los dispositivos

Los parámetros básicos se configuran por medio de la dirección ip predeterminadas

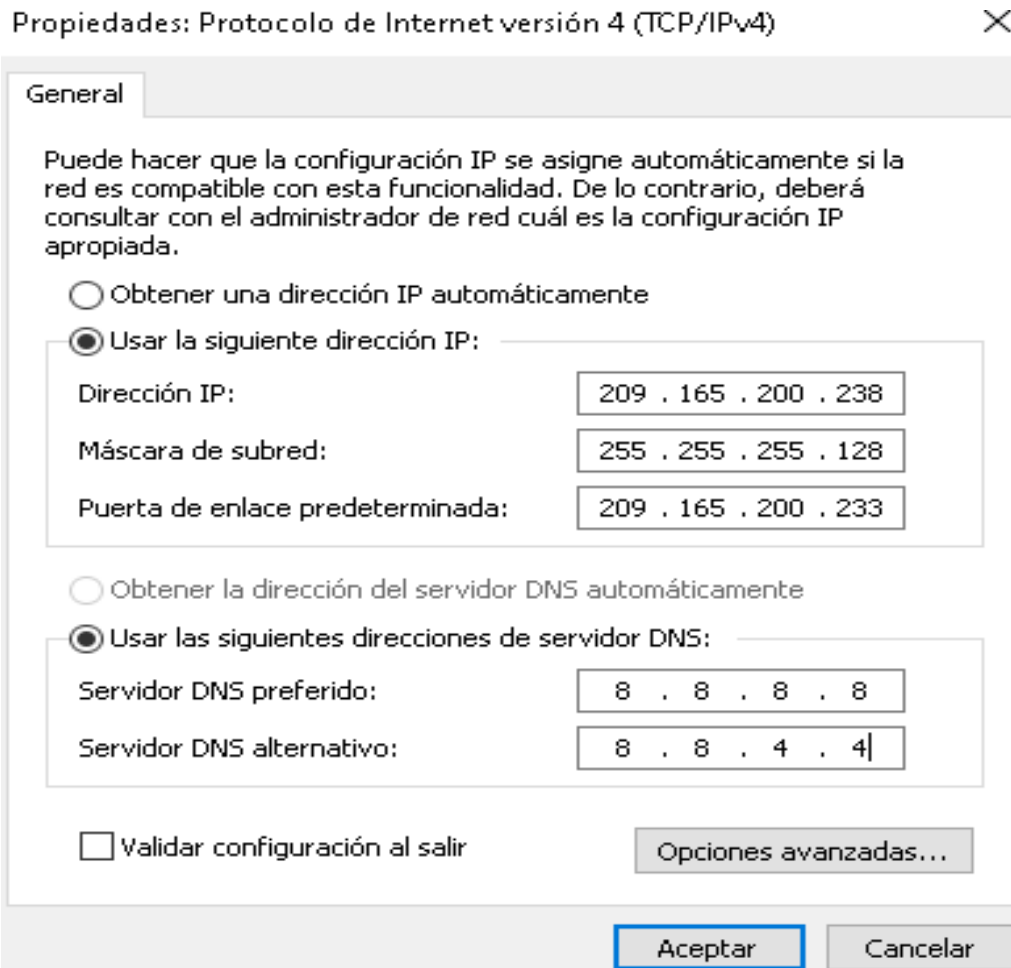


FIGURA 4 Configurar la computadora de Internet

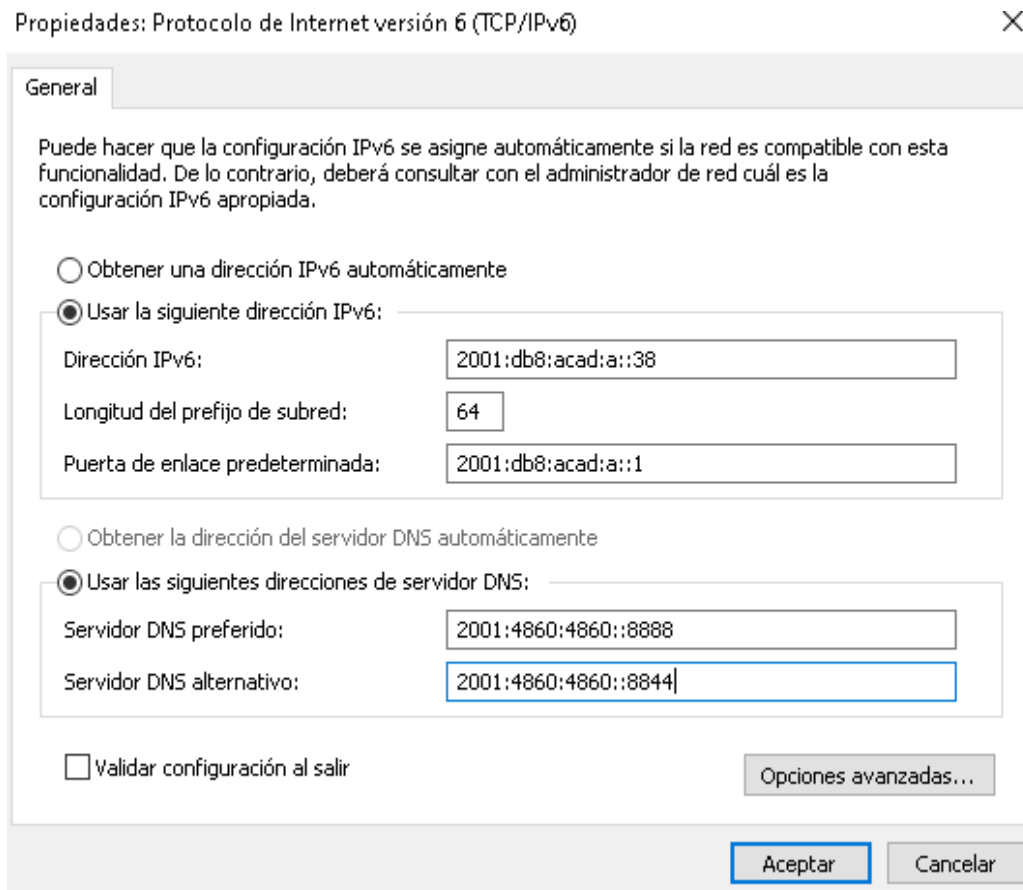


FIGURA 5 Configurar IPv6 en la computadora de Internet

Configuración de R1

Se le asignan los nombres, contraseñas al router de la siguiente manera

Asignamos un nombre al dispositivo

```
R1(config)#hostname R1
```

Desactivamos la búsqueda de nombres por DNS

```
R1(config)#no ip domain-lookup
```

Configuramos una contraseña de modo privilegiado

```
R1(config)#enable secret class
```

Configuramos la contraseña de consola

```
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

*Configuramos una contraseña en las líneas vty**

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Encriptamos todas las contraseñas en texto plano

```
R1(config)#service password-encryption
```

Asignamos un banner al dispositivo

```
R1(config)#banner motd & Se prohíbe el acceso no autorizado &
Configuramos el serial 0.0.0*
```

```
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#exit
```

Asignamos rutas IPV4 e IPV6 por defecto

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::0 s0/0/0
R1(config)#
```

Configuración de R2

Se le asignan los nombres, contraseñas al router de la siguiente manera

Asignamos un nombre al dispositivo

```
R2(config)#hostname R2
```

Desactivamos la búsqueda de nombres por DNS

```
R2(config)#no ip domain-lookup
```

Configuramos una contraseña de modo privilegiado

```
R2(config)#enable secret class
Configuramos la contraseña de consola*
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

Configuramos una contraseña en las líneas vty

```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

Encriptamos todas las contraseñas en texto plano

```
R2(config)#service password-encryption
```

Habilitamos el servicio http

```
R2(config)#ip http server
R2(config)#ip http secure-server
```

Asignamos un banner al dispositivo

```
R2(config)#banner motd & Se prohíbe el acceso no autorizado &
*Configuramos el serial 0.0.0*
R2(config)#int s0/0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)# no shutdown
R2(config-if)#exit
```

Configuramos el serial 0.0.1

```
R2(config)#int s0/0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#clock rate 128000
R2(config-if)# no shutdown
R2(config-if)#exit
```

Configuramos la interfaz g0.0

```
R2(config)#int g0/0
R2(config-if)#description Connection to ISP
R2(config-if)#ip address 209.165.200.225 255.255.255.248
```

```
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R2(config-if)# no shutdown
R2(config-if)#exit
```

Configuración de R3

Se le asignan los nombres, contraseñas al router de la siguiente manera

Asignamos un nombre al dispositivo

```
R3(config)#hostname R3
```

Desactivamos la búsqueda de nombres por DNS

```
R3(config)#no ip domain-lookup
```

Configuramos una contraseña de modo privilegiado

```
R3(config)#enable secret class
```

Configuramos la contraseña de consola

```
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Configuramos la contraseña de las líneas vty

```
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Encriptamos todas las contraseñas en texto plano

```
R3(config)#service password-encryption
```

Asignamos un banner al dispositivo

```
R3(config)#banner motd & Se prohíbe el acceso no autorizado &
```

Configuramos el serial 0.0.1

```
R3(config)#int s0/0/1
R3(config-if)#description Connection to R2
R3(config-if)#ip address 172.16.23.1 255.255.255.252
```

```
R3(config-if)#ipv6 address 2001:db8:acad:23::1/64
R3(config-if)# no shutdown
R3(config-if)#exit
```

Configuramos el loopback 4

```
R3(config)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)# no shutdown
```

Configuramos el loopback 5

```
R3(config)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)# no shutdown
```

Configuramos el loopback 6

```
R3(config)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)# no shutdown
```

Configuramos el loopback 7

```
R3(config)#int loopback 7
R3(config-if)#ip address 192.168.7.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#exit
```

Asignamos rutas IPV4 e IPV6 por defecto

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
```

Configuración de S1

Se le asignan los nombres, contraseñas al router de la siguiente manera

Asignamos un nombre al dispositivo

```
Switch(config)#hostname S1
```

Desactivamos la búsqueda de nombres por DNS

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

Configuramos una contraseña de modo privilegiado

```
S1(config)#enable secret class
```

Configuramos la contraseña de consola

```
S1(config)#line con 0
```

```
S1(config-line)#password cisco
S1(config-line)#login
```

Configuramos la contraseña de las líneas vty

```
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
```

Encriptamos todas las contraseñas en texto plano

```
S1(config-line)#service password-encryption
*Asignamos un banner al dispositivo*
S1(config)#banner motd & Se prohíbe el acceso no autorizado &
```

Configuración de S3

Se le asignan los nombres, contraseñas al router de la siguiente manera

Asignamos un nombre al dispositivo

```
Switch(config)#hostname S3
```

Desactivamos la búsqueda de nombres por DNS

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

Configuramos una contraseña de modo privilegiado

```
S3(config)#enable secret class
*Configuramos la contraseña de consola*
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
```

Configuramos la contraseña de las líneas vty

```
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
```

Encriptamos todas las contraseñas en texto plano

```
S3(config-lin
```

Asignamos un banner al dispositivo

```
e)#service password-encryption
S3(config)#banner motd @ Se prohíbe el acceso no autorizado @
```

Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Tabla 1 Verificar la conectividad de la red

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

```
R1#  
R1#ping 172.16.1.2  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/52 ms  
R1#
```

FIGURA 6 Ping de R1a R2

```
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/56 ms
R2#
```

^ [] [] [] ESP 04:23 p.m. []

FIGURA 7 Ping de R2 a R3

```
Microsoft Windows [Versión 10.0.18362.720]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\diego>ping 209.165.200.237

Haciendo ping a 209.165.200.237 con 32 bytes de datos:
Respuesta desde 209.165.200.237: bytes=32 tiempo=423ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=526ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=34ms TTL=255
Respuesta desde 209.165.200.237: bytes=32 tiempo=46ms TTL=255

Estadísticas de ping para 209.165.200.237:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 34ms, Máximo = 526ms, Media = 257ms

C:\Users\diego>
```

FIGURA 8 Ping de pc de internet a Gateway predeterminado

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

Configurar S1 se incluyen las siguientes tareas

Creamos las vlans y asignamos su nombre correspondiente

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
```

Asignamos las direcciones ip correspondientes a las vlans

```
S1(config-vlan)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)# no shutdown
```

Configuramos la puerta de salida del switch

```
S1(config-if)#ip default-gateway 192.168.99.1
```

Configuramos y forzamos el enlace troncal en las interfaces necesarias

```
S1(config)#interface F0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface F0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

Configuramos el resto de puertos como modo de acceso

```
S1(config-if)#interface range F0/1-2, F0/4, F0/6-24, G0/1-2
S1(config-if-range)#switchport mode access
```

Asignamos la interfaz f0.6 a la VLAN 2

```
S1(config-if-range)#interface F0/6
S1(config-if)#switchport access vlan 21
```

Apagamos los puertos sin usar

```
S1(config-if)#interface range F0/1-2, F0/4, F0/7-24, G0/1-2
S1(config-if-range)#shutdown
```

Configurar S3 se incluyen las siguientes tareas

Creamos las vlans y asignamos su nombre correspondiente

```
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
```

Asignamos las direcciones ip correspondientes a las vlans

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

Configuramos la puerta de salida del switch

```
S3(config-if)#ip default-gateway 192.168.99.1
```

Configuramos y forzamos el enlace troncal en las interfaces necesarias

```
S3(config)#interface F0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
```

Configuramos el resto de puertos como modo de acceso

```
S3(config-if)# interface range F0/1-2, F0/4, F0/6-24,G0/1-2
S3(config-if)#switchport mode Access
```

*Asingamos la interfaz f0.18 a la VLAN 23**

```
S3(config-if-range)#interface F0/18
S3(config-if)#switchport access vlan 23
```

Apagamos los puertos sin usar

```
S3(config-if)#interface range F0/1-2, F0/4, F0/6-17,
F0/19-24, G0/1-2
S3(config-if-range)#shutdown
```

Configurar R1 se incluyen las siguientes tareas

Configuramos las subinterfaces y asignamos su dirección IP y su descripción

```
R1(config)#interface g0/1.21
R1(config-subif)#description LAN de contabilidad
R1(config-subif)#encapsulation dot1q 21
```

```

R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#interface g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#interface g0/1.99
R1(config-subif)#description Lan de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0

```

Encendemos la interfaz principal

```

R1(config-subif)#interface g0/1
R1(config-if)#no shutdown

```

Tabla 2 Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

User Access Verification

```
Password:  
S1#ping 192.168.99.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 31/79/172 ms  
S1#
```

ESP 04:26 p. m.

FIGURA 9 Ping de s1 a Gateway vlan 99

```
Password:  
S3#ping 192.168.99.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 31/45/67 ms  
S3#
```

ESP 04:27 p. m.

FIGURA 10 Ping de s3 a gateway vlan 99

```
S1#ping 192.168.21.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 51/59/75 ms  
S1#
```

ESP 04:28 p. m.

FIGURA 11 Ping de s1 a gateway vlan 21

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 31/45/67 ms  
S3#ping 192.168.23.1  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 41/51/66 ms  
S3#
```

ESP 04:27 p. m.

FIGURA 12 Ping de s3 a gateway vlan 23

5.6 Configurar el protocolo de routing dinámico RIPv2

Configurar RIPv2 en el R1

Configuramos RIP versión

```
R1(config)#router rip
R1(config-router)#version 2
```

Añadimos las redes directamente conectadas

```
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
```

Habilitamos las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
```

Desactivamos la sumarización automática

```
R1(config-router)#no auto-summary
```

Configurar RIPv2 en el R2 se incluyen las siguientes tareas

Configuramos RIP versión

```
R2(config)#router rip
R2(config-router)#version 2
```

Añadimos las redes directamente conectadas

```
R2(config-router)#network 172.16.0.0
R2(config-router)#network 10.10.10.10
```

Habilitamos las interfaces LAN como pasivas

```
R2(config-router)#passive-interface lo0
```

Desactivamos la sumarización automática

```
R2(config-router)#no auto-summary
```

Configurar RIPv2 en el R3 se incluyen las siguientes tareas

Configuramos RIP versión

```
R3(config)#router rip
```

```
R3(config-router)#version 2
```

Añadimos las redes directamente conectadas

```
R3(config-router)#network 172.16.0.0
```

```
R3(config-router)#network 192.168.4.0
```

```
R3(config-router)#network 192.168.5.0
```

```
R3(config-router)#network 192.168.6.0
```

Habilitamos las interfaces LAN como pasivas

```
R3(config-router)#passive-interface lo4
```

```
R3(config-router)#passive-interface lo5
```

```
R3(config-router)#passive-interface lo6
```

*Desactivamos la sumarización automática**

```
R3(config-router)#no auto-summary
```

Verificar la información de RIP

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

Tabla 3 Verificar información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas RIP?	show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run section router RIP

```
Redistributing: rip
Default version control: send version 2, receive version 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial2/1          2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.16.0.0
  192.168.21.0
  192.168.23.0
  192.168.99.0
Passive Interface(s):
  GigabitEthernet3/0.21
  GigabitEthernet3/0.23
  GigabitEthernet3/0.99
Routing Information Sources:
  Gateway          Distance    Last Update
  172.16.1.1       120        00:00:12
Distance: (default is 120)

R1#
```

FIGURA 13 Enrutamiento en R1

```
R1#sh ip route rip
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10 [120/1] via 172.16.1.1, 00:00:16, Serial2/1
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.2.0/30 [120/1] via 172.16.1.1, 00:00:16, Serial2/1
R       192.168.4.0/24 [120/2] via 172.16.1.1, 00:00:16, Serial2/1
R       192.168.5.0/24 [120/2] via 172.16.1.1, 00:00:16, Serial2/1
R       192.168.6.0/24 [120/2] via 172.16.1.1, 00:00:16, Serial2/1
R1#
```

FIGURA 14 Tabla de rutas en R1

```
R1# sh run | section rip
description CONNECTION_TO_R2
description LAN de Contabilidad
description LAN de Administracion
router rip
version 2
passive-interface GigabitEthernet3/0.21
passive-interface GigabitEthernet3/0.23
passive-interface GigabitEthernet3/0.99
network 172.16.0.0
network 192.168.21.0
network 192.168.23.0
network 192.168.99.0
no auto-summary
R1#
Apr 20 21:21:17.956: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1,
changed state to down
R1#
```

FIGURA 15 Seccion RIP en R1

```

R2#sh ip rip
Redistributing: rip
Default version control: send version 2, receive version 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial2/0          2    2
  Serial2/1          2    2
  NVI0               2    2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.16.0.0
Passive Interface(s):
  Loopback0
Routing Information Sources:
  Gateway            Distance    Last Update
  172.16.2.2         120        00:00:03
  172.16.1.2         120        00:00:28
Distance: (default is 120)
R2#

```

FIGURA 16 Enrutamiento en R2

```

R2#sh ip route rip
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R    192.168.4.0/24 [120/1] via 172.16.2.2, 00:00:09, Serial2/0
R    192.168.5.0/24 [120/1] via 172.16.2.2, 00:00:09, Serial2/0
R    192.168.6.0/24 [120/1] via 172.16.2.2, 00:00:09, Serial2/0
R    192.168.21.0/24 [120/1] via 172.16.1.2, 00:00:51, Serial2/1
R    192.168.23.0/24 [120/1] via 172.16.1.2, 00:00:51, Serial2/1
R    192.168.99.0/24 [120/1] via 172.16.1.2, 00:00:51, Serial2/1
R2#

```

FIGURA 17 Tabla de rutas en R2

```

R2# sh run | sec rip

Apr 20 21:21:26.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1,
changed state to up description WEB_SERVER_LOOPBACK
  description CONNECTION_TO_R3
  description CONNECTION_TO_R1
  description CONNECTION_TO_INTERNET
router rip
version 2
passive-interface Loopback0
network 10.0.0.0
network 172.16.0.0
default-information originate
no auto-summary
R2#

```

FIGURA 18 Seccion de RIP en R2

```

Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.16.0.0
 192.168.4.0
 192.168.5.0
 192.168.6.0
Passive Interface(s):
 Loopback4
 Loopback5
 Loopback6
 Loopback7
Routing Information Sources:
 Gateway      Distance    Last Update
 172.16.2.1    120        00:00:26
Distance: (default is 120)
R3#

```

FIGURA 19 Enrutamiento en R3

```
R3#sh ip route rip
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10 [120/1] via 172.16.2.1, 00:00:53, Serial2/0
R3#
```

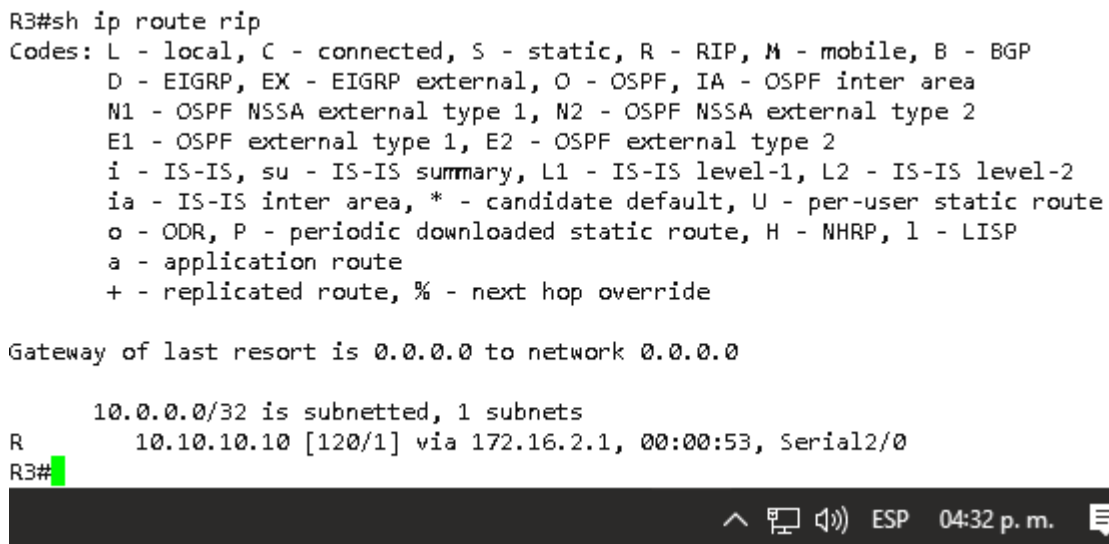


FIGURA 20 Tabla de rutas RIP en R3

```
R3#sh run | sec rip
description CONNECTION_TO_R2
router rip
version 2
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
passive-interface Loopback7
network 172.16.0.0
network 192.168.4.0
network 192.168.5.0
network 192.168.6.0
no auto-summary
R3#
```

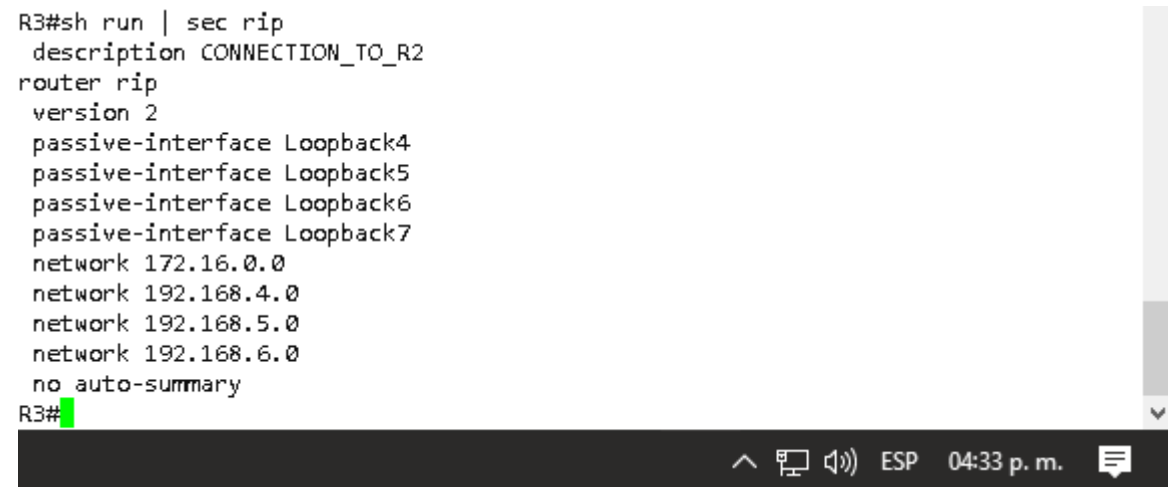


FIGURA 21 Seccion de RIP en R FIGURA 22 Seccion de RIP en R

5.7 Implementar DHCP y NAT para IPv4

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

Configurar R1

excluimos el rango de direcciones indicadas

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
```

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

Creamos el primer pool DHCP

```
R1(config)#ip dhcp pool ACCT
```

```
R1(dhcp-config)#network 192.168.31.0 255.255.255.0
```

```
R1(dhcp-config)#dns-server 10.10.10.10
```

```
R1(dhcp-config)#domain-name ccna-sa.com
```

```
R1(dhcp-config)#default-router 192.168.31.1
```

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

Creamos el pool de ingeniería

```
R1(config)#ip dhcp pool ENGR
```

```
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
```

```
R1(dhcp-config)#dns-server 10.10.10.10
```

```
R1(dhcp-config)#domain-name ccna-sa.com
```

```
R1(dhcp-config)#default-router 192.168.23.1
```

Configurar la NAT estática y dinámica en el R2

creamos un usuario con contraseña en el dispositivo

```
R2(config)#username webuser privilege 15 secret cisco12345
```

habilitamos el servicio http en el router

```
R2(config)#ip http server
```

```
R2(config)#ip http secure-server
```

le indicamos al servicio http que use la base de datos de usuarios local

```
R2(config)#ip http authentication local
```

configuramos una nat estática para el servidor en el loopback

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

asignamos interfaces externas e internas para el nat

```
R2(config)#interface lo0
```

```
R2(config-if)#ip nat inside
```

```
R2(config-if)#interface g0/0
R2(config-if)#ip nat outside
```

creamos una lista de acceso para que las LAN de R1 puedan verse incluidas

```
R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

configuramos el pool de direcciones en el nat

```
R2 (config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

Tabla 4 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Exitoso

```
PC-A> show ip

NAME       : PC-A[1]
IP/MASK    : 192.168.21.21/24
GATEWAY    : 192.168.21.1
DNS        : 10.10.10.10
DHCP SERVER : 192.168.21.1
DHCP LEASE : 86398, 86400/43200/75600
DOMAIN NAME : ccna-sa.com
MAC       : 00:50:79:66:68:00
LPORT    : 10005
RHOST:PORT : 127.0.0.1:10006
MTU      : 1500

PC-A> █
```

FIGURA 21 PC-A

```
PC-C> show ip

NAME       : PC-C[1]
IP/MASK    : 192.168.23.2/24
GATEWAY    : 192.168.23.1
DNS        : 10.10.10.10
DHCP SERVER : 192.168.23.1
DHCP LEASE : 86184, 86400/43200/75600
DOMAIN NAME : ccna-sa.com
MAC       : 00:50:79:66:68:01
LPORT    : 10003
RHOST:PORT : 127.0.0.1:10004
MTU      : 1500
```

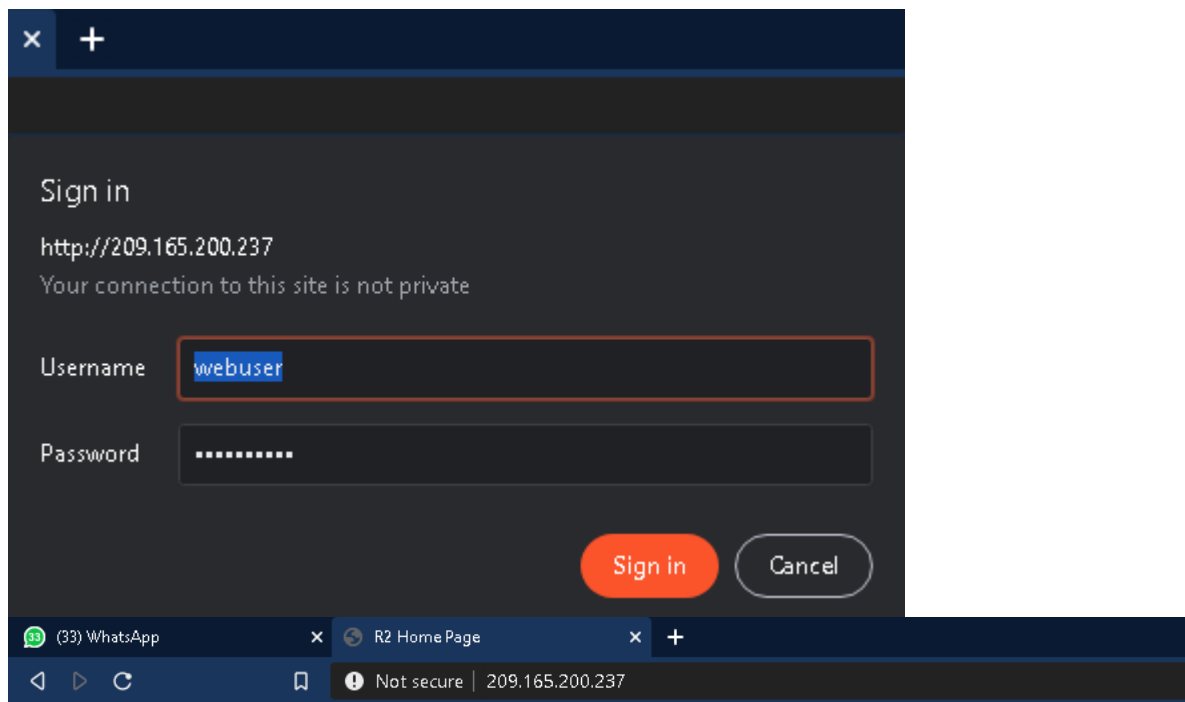
FIGURA 22 PC_C

```
PC-C> ping 192.168.21.21
192.168.21.21 icmp_seq=1 timeout
192.168.21.21 icmp_seq=2 timeout
84 bytes from 192.168.21.21 icmp_seq=3 ttl=63 time=35.331 ms
84 bytes from 192.168.21.21 icmp_seq=4 ttl=63 time=30.649 ms
84 bytes from 192.168.21.21 icmp_seq=5 ttl=63 time=29.375 ms

PC-C> █
```



FIGURA 23 PING PC-A PC-A



Cisco Systems

Accessing Cisco 7206VXR "R2"

[Show diagnostic log](#) - display the diagnostic log.

[Monitor the router](#) - HTML access to the command line interface at level [0](#), [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#), [13](#), [14](#), [15](#)

[Platform](#) - platform utilities. Send comments to cs-html (below).

[Show tech-support](#) - display information commonly needed by tech support.

[Extended Ping](#) - Send extended ping commands.

[QoS Device Manager](#) - Configure and monitor QoS through the web interface.

Help resources

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

FIGURA 23 Navegador web

5.8 Configurar NTP

Configurar R2

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

```
R2(config)# ntp master 5
```

Configurar R1

```
R1(config)# ntp server 172.16.1.2
```

```
R1 (config)# ntp update-calendar
```

```
R1# show ntp associations
```

```
R1#show ntp assoc
R1#show ntp associations

  address          ref clock      st  when  poll reach  delay  offset  disp
*~172.16.1.1      127.127.1.1    5   17    64    1 56.134 -48.163 939.82
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

FIGURA 24 Asociaciones ntp en r1

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

Restringir el acceso a las líneas VTY en el R2

```
R2(config)#ip access-list standard ADMIN-MGT
```

```
R2(config-std-nacl)#permit host 172.16.1.1
```

```
R2(config-std-nacl)#line vty 0 4
```

```
R2(config-line)#access-class ADMIN-MGT in
```

```
R2(config-line)#transport input telnet
```

```

R1#telnet 172.16.1.1
Trying 172.16.1.1 ... Open
Se prohíbe el acceso no autorizado

User Access Verification

Password:
R2>

```

FIGURA 25 Telnet a R2

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

Tabla 5 Verificación con comandos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	<p><i>Tabla 4 ACLs en R2</i></p> <pre> R2#show acces R2#show access-1 R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0, wildcard bits 0.0.0.255 20 permit 192.168.23.0, wildcard bits 0.0.0.255 30 permit 192.168.4.0, wildcard bits 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit 172.16.1.2 (2 matches) R2# </pre>
Restablecer los contadores de una lista de acceso	<pre> clear ip access-list counters </pre>

<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<p>Show ip interface</p>
<p>¿Con qué comando se muestran las traducciones NAT?</p>	<pre>R2#show ip nat trans Pro Inside global Inside local Outside local Outside global icmp 209.165.200.237:11288 10.10.10.10:11288 192.168.21.21:11288 192.168.21.21:11288 icmp 209.165.200.237:11800 10.10.10.10:11800 192.168.21.21:11800 192.168.21.21:11800 --- 209.165.200.237 10.10.10.10 --- --- R2#</pre> <p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>#clear ip nat translation *</p>

6. ESCENARIO 2

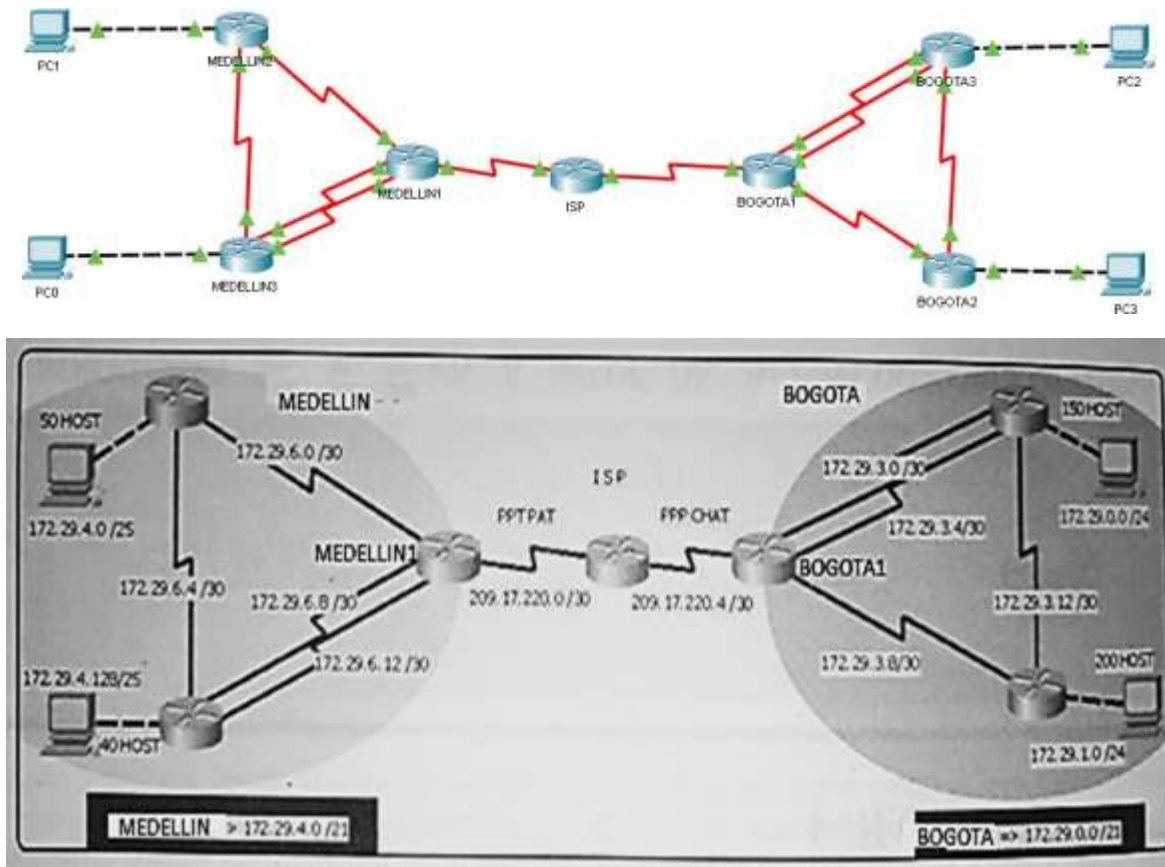


FIGURA 26 Topologías Escenario 2

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

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

- Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
- Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
- Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

MEDELLIN1

Desactivamos la búsqueda de nombres dns

Router(config)#no ip domain-lookup

Configuramos un nombre al dispositivo

Router(config)#hostname MEDELLIN1

Asignamos class como contraseña de privilegiado

MEDELLIN1(config)#enable secret class

Asignamos una contraseña a la consola

MEDELLIN1 (config)#line con 0

MEDELLIN1 (config-line)#password cisco

MEDELLIN1 (config-line)#login

MEDELLIN1 (config-line)#exit

Asignamos una contraseña a las líneas vty

MEDELLIN1 (config)#line vty 0 15

MEDELLIN1 (config-line)#password cisco

MEDELLIN1 (config-line)#login

MEDELLIN1 (config-line)#exit

Encriptamos las contraseñas de texto plano

MEDELLIN1(config)#service password-encryption

configuramos un banner de acceso

MEDELLIN1 (config)#banner motd : Se prohíbe el acceso no autorizado :

MEDELLIN2

Desactivamos la búsqueda de nombres dns

Router(config)#no ip domain-lookup

Configuramos un nombre al dispositivo

Router(config)#hostname MEDELLIN2

Asignamos class como contraseña de privilegiado

MEDELLIN2(config)#enable secret class

Asignamos una contraseña a la consola

MEDELLIN2 (config)#line con 0

MEDELLIN2 (config-line)#password cisco

MEDELLIN2 (config-line)#login

MEDELLIN2 (config-line)#exit

Asignamos una contraseña a las líneas vty

MEDELLIN2 (config)#line vty 0 15

MEDELLIN2 (config-line)#password cisco

MEDELLIN2 (config-line)#login

MEDELLIN2 (config-line)#exit

Encriptamos las contraseñas de texto plano

MEDELLIN2(config)#service password-encryption

configuramos un banner de acceso

MEDELLIN2 (config)#banner motd : Se prohíbe el acceso no autorizado :

MEDELLIN3

Desactivamos la búsqueda de nombres dns

Router(config)#no ip domain-lookup

Configuramos un nombre al dispositivo

```
Router(config)#hostname MEDELLIN3
```

Asignamos class como contraseña de privilegiado

```
MEDELLIN3(config)#enable secret class
```

Asignamos una contraseña a la consola

```
MEDELLIN3 (config)#line con 0
```

```
MEDELLIN3 (config-line)#password cisco
```

```
MEDELLIN3 (config-line)#login
```

```
MEDELLIN3 (config-line)#exit
```

Asignamos una contraseña a las líneas vty

```
MEDELLIN3 (config)#line vty 0 15
```

```
MEDELLIN3 (config-line)#password cisco
```

```
MEDELLIN3 (config-line)#login
```

```
MEDELLIN3 (config-line)#exit
```

Encriptamos las contraseñas de texto plano

```
MEDELLIN3 (config)#service password-encryption
```

configuramos un banner de acceso

```
MEDELLIN3 (config)#banner motd : Se prohíbe el acceso no autorizado :
```

ISP

Desactivamos la búsqueda de nombres dns

```
Router(config)#no ip domain-lookup
```

Configuramos un nombre al dispositivo

```
Router(config)#hostname ISP
```

Asignamos class como contraseña de privilegiado

```
ISP (config)#enable secret class
```

Asignamos una contraseña a la consola

```
ISP (config)#line con 0
```

```
ISP (config-line)#password cisco
```

```
ISP (config-line)#login
```

```
ISP (config-line)#exit
```

Asignamos una contraseña a las líneas vty

```
ISP (config)#line vty 0 15
```

```
ISP (config-line)#password cisco
```

```
ISP (config-line)#login
```

```
ISP (config-line)#exit
```

Encriptamos las contraseñas de texto plano

```
ISP (config)#service password-encryption
```

configuramos un banner de acceso

```
ISP (config)#banner motd : Se prohíbe el acceso no autorizado :
```

BOGOTA1

Desactivamos la búsqueda de nombres dns

```
Router(config)#no ip domain-lookup
```

Configuramos un nombre al dispositivo

```
Router(config)#hostname BOGOTA1
```

Asignamos class como contraseña de privilegiado

```
BOGOTA1 (config)#enable secret class
```

Asignamos una contraseña a la consola

```
BOGOTA1 (config)#line con 0
BOGOTA1 (config-line)#password cisco
BOGOTA1 (config-line)#login
BOGOTA1 (config-line)#exit
```

Asignamos una contraseña a las líneas vty

```
BOGOTA1 (config)#line vty 0 15
BOGOTA1 (config-line)#password cisco
BOGOTA1 (config-line)#login
BOGOTA1 (config-line)#exit
```

Encriptamos las contraseñas de texto plano

```
BOGOTA1 (config)#service password-encryption
```

configuramos un banner de acceso

```
BOGOTA1 (config)#banner motd : Se prohíbe el acceso no autorizado :
```

BOGOTA2

Desactivamos la búsqueda de nombres dns

```
Router(config)#no ip domain-lookup
```

Configuramos un nombre al dispositivo

```
Router(config)#hostname BOGOTA2
```

Asignamos class como contraseña de privilegiado

```
BOGOTA2 (config)#enable secret class
```

Asignamos una contraseña a la consola

```
BOGOTA2 (config)#line con 0
BOGOTA2 (config-line)#password cisco
```

BOGOTA2 (config-line)#login

BOGOTA2 (config-line)#exit

Asignamos una contraseña a las líneas vty

BOGOTA2 (config)#line vty 0 15

BOGOTA2 (config-line)#password cisco

BOGOTA2 (config-line)#login

BOGOTA2 (config-line)#exit

Encriptamos las contraseñas de texto plano

BOGOTA2 (config)#service password-encryption

configuramos un banner de acceso

BOGOTA2 (config)#banner motd : Se prohíbe el acceso no autorizado :

BOGOTA3

Desactivamos la búsqueda de nombres dns

Router(config)#no ip domain-lookup

Configuramos un nombre al dispositivo

Router(config)#hostname BOGOTA3

Asignamos class como contraseña de privilegiado

BOGOTA3 (config)#enable secret class

Asignamos una contraseña a la consola

BOGOTA3 (config)#line con 0

BOGOTA3 (config-line)#password cisco

BOGOTA3 (config-line)#login

BOGOTA3 (config-line)#exit

Asignamos una contraseña a las líneas vty

```
BOGOTA3 (config)#line vty 0 15
BOGOTA3 (config-line)#password cisco
BOGOTA3 (config-line)#login
BOGOTA3 (config-line)#exit
```

Encriptamos las contraseñas de texto plano

```
BOGOTA3 (config)#service password-encryption
```

configuramos un banner de acceso

```
BOGOTA3 (config)#banner motd : Se prohíbe el acceso no autorizado :
```

ROUTER 6.1 CONFIGURACIÓN DEL ENRUTAMIENTO

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

En este paso se realizó el enrutamiento entre las diferentes redes de la topología; para ello se ingresó al apartado CLI, donde se ingresaron los siguientes comandos:

enable: para acceder al modo privilegiado del router.

configure terminal: para ingresar al modo de configuración global.

router ospf 1: para activar el protocolo de información de enrutamiento.

network: para agregar la red, con la que se desea enrutar.

Cabe resaltar que OSPF no sumariza redes.

MEDELLIN1

```
MEDELLIN1 (config)#router ospf 1
MEDELLIN1 (router-config)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1 (router-config)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1 (router-config)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN1 (router-config)#network 209.17.220.0 0.0.0.3 area 0
```

MEDELLIN2

MEDELLIN2 (config)#router ospf 1

MEDELLIN2 (router-config)#network 172.29.4.0 0.0.0.127 area 0

MEDELLIN2 (router-config)#network 172.29.6.0 0.0.0.3 area 0

MEDELLIN2 (router-config)#network 172.29.6.4 0.0.0.3 area 0

MEDELLIN3

MEDELLIN3(config)#router ospf 1

MEDELLIN3(router-config)#network 172.29.4.128 0.0.0.127 area 0

MEDELLIN3(router-config)#network 172.29.6.4 0.0.0.3 area 0

MEDELLIN3(router-config)#network 172.29.6.8 0.0.0.3 area 0

MEDELLIN3(router-config)#network 172.29.6.12 0.0.0.3 area 0

ISP

ISP(router)#router ospf 1

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

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

BOGOTA1

BOGOTA1(router)#router ospf 1

BOGOTA1(router-config)#network 172.29.3.0 0.0.0.3 area 0

BOGOTA1(router-config)#network 172.29.3.4 0.0.0.3 area 0

BOGOTA1(router-config)#network 172.29.3.8 0.0.0.3 area 0

BOGOTA1(router-config)#network 209.17.220.4 0.0.0.3 area 0

BOGOTA2

BOGOTA2(router)#router ospf 1

BOGOTA2(router-config)#network 172.29.1.0 0.0.0.255 area 0

BOGOTA2(router-config)#network 172.29.3.8 0.0.0.3 area 0

BOGOTA2(router-config)#network 172.29.3.12 0.0.0.3 area 0

BOGOTA3

BOGOTA3(router)#router ospf 1

BOGOTA3(router-config)#network 172.29.0.0 0.0.0.255 area 0

BOGOTA3(router-config)#network 172.29.3.0 0.0.0.3 area 0

BOGOTA3(router-config)#network 172.29.3.4 0.0.0.3 area 0

BOGOTA3(router-config)#network 172.29.3.12 0.0.0.3 area 0

Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

El primer grupo de ceros hace referencia a la dirección de red a la que se desea conectar, el segundo grupo de ceros, a la máscara de red, y el serial es la interfaz por donde se va a comunicar hacia esa ruta «esta última puede variar dependiendo de la interfaz»

BOGOTA1

Asignamos una ruta de ultimo recurso a BOGOTA1

```
BOGOTA1(router)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

redistribuimos la ruta por el protocolo de enrutamiento

```
BOGOTA1(router)#router ospf 1
```

```
BOGOTA1(router-config)#redistribute static subnets
```

MEDELLIN1

Asignamos una ruta de ultimo recurso a BOGOTA1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
```

redistribuimos la ruta por el protocolo de enrutamiento

```
MEDELLIN1(config)#router ospf 1
```

```
MEDELLIN1(router-config)#redistribute static subnets
```

El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

ISP

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 Serial0/3/0
```

```
ISP(config)#ip route 172.29.4.128 255.255.255.128 Serial0/3/0
```

```
ISP(config)#ip route 172.29.1.0 255.255.255.0 Serial0/3/1
```

```
ISP(config)#ip route 172.29.0.0 255.255.252.0 Serial0/3/1
```

6.2 Tabla de Enrutamiento

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

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

  172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O   172.29.0.0/24 [110/257] via 172.29.6.1, 01:40:34, Serial0/1/0
O   172.29.1.0/24 [110/257] via 172.29.6.1, 01:40:34, Serial0/1/0
O   172.29.3.0/30 [110/256] via 172.29.6.1, 01:40:34, Serial0/1/0
O   172.29.3.4/30 [110/256] via 172.29.6.1, 01:40:34, Serial0/1/0
O   172.29.3.8/30 [110/256] via 172.29.6.1, 01:40:34, Serial0/1/0
O   172.29.3.12/30 [110/320] via 172.29.6.1, 01:40:34,
Serial0/1/0
C   172.29.4.0/25 is directly connected, GigabitEthernet0/0
L   172.29.4.1/32 is directly connected, GigabitEthernet0/0
O   172.29.4.128/25 [110/65] via 172.29.6.6, 01:41:59,
Serial0/1/1
C   172.29.6.0/30 is directly connected, Serial0/1/0
L   172.29.6.2/32 is directly connected, Serial0/1/0
C   172.29.6.4/30 is directly connected, Serial0/1/1
L   172.29.6.5/32 is directly connected, Serial0/1/1
O   172.29.6.8/30 [110/128] via 172.29.6.6, 01:41:59, Serial0/1/1
    [110/128] via 172.29.6.1, 01:41:59, Serial0/1/0
O   172.29.6.12/30 [110/128] via 172.29.6.6, 01:41:59,
Serial0/1/1
    [110/128] via 172.29.6.1, 01:41:59,
Serial0/1/0
O   209.17.220.0/30 is subnetted, 2 subnets
O   209.17.220.0/30 [110/128] via 172.29.6.1, 01:41:59,
Serial0/1/0
O   209.17.220.4/30 [110/192] via 172.29.6.1, 01:40:48,
Serial0/1/0
S*  0.0.0.0/0 is directly connected, Serial0/1/0

MEDELLIN2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

03:15 p. m. 24/04/2020

FIGURA 27 Tabla de enrutamiento MEDELLIN2

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 16 subnets, 4 masks
O    172.29.0.0/24 [110/257] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.1.0/24 [110/257] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.3.0/30 [110/256] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.3.4/30 [110/256] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.3.8/30 [110/256] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.3.12/30 [110/320] via 172.29.6.13, 01:51:23,
Serial0/1/0
O    172.29.4.0/25 [110/65] via 172.29.6.5, 01:52:43, Serial0/1/1
C    172.29.4.128/25 is directly connected, GigabitEthernet0/0
L    172.29.4.129/32 is directly connected, GigabitEthernet0/0
O    172.29.6.0/30 [110/128] via 172.29.6.5, 01:52:43, Serial0/1/1
    [110/128] via 172.29.6.13, 01:52:43,
Serial0/1/0
C    172.29.6.4/30 is directly connected, Serial0/1/1
L    172.29.6.6/32 is directly connected, Serial0/1/1
C    172.29.6.8/30 is directly connected, Serial0/2/0
L    172.29.6.10/32 is directly connected, Serial0/2/0
C    172.29.6.12/30 is directly connected, Serial0/1/0
L    172.29.6.14/32 is directly connected, Serial0/1/0
    209.17.220.0/30 is subnetted, 2 subnets
O    209.17.220.0/30 [110/128] via 172.29.6.13, 01:52:43,
Serial0/1/0
O    209.17.220.4/30 [110/192] via 172.29.6.13, 01:51:37,
Serial0/1/0
S*  0.0.0.0/0 is directly connected, Serial0/2/0

MEDELLIN3#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

] Top

System tray area containing icons for network, volume, and language (ESP), along with the time 03:23 p.m. and date 24/04/2020.

FIGURA 28 Tabla de enrutamiento MEDELLIN3

```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O    172.29.0.0/24 [110/193] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.1.0/24 [110/193] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.3.0/30 [110/192] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.3.4/30 [110/192] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.3.8/30 [110/192] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.3.12/30 [110/256] via 209.17.220.1, 01:51:51,
Serial0/1/0
O    172.29.4.0/25 [110/65] via 172.29.6.2, 01:53:11, Serial0/1/1
O    172.29.4.128/25 [110/65] via 172.29.6.14, 01:53:11,
Serial0/2/0
C    172.29.6.0/30 is directly connected, Serial0/1/1
L    172.29.6.1/32 is directly connected, Serial0/1/1
O    172.29.6.4/30 [110/128] via 172.29.6.14, 01:53:11,
Serial0/2/0
                                     [110/128] via 172.29.6.2, 01:53:11, Serial0/1/1
C    172.29.6.8/30 is directly connected, Serial0/2/1
L    172.29.6.9/32 is directly connected, Serial0/2/1
C    172.29.6.12/30 is directly connected, Serial0/2/0
L    172.29.6.13/32 is directly connected, Serial0/2/0
    209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C    209.17.220.0/30 is directly connected, Serial0/1/0
C    209.17.220.1/32 is directly connected, Serial0/1/0
L    209.17.220.2/32 is directly connected, Serial0/1/0
O    209.17.220.4/30 [110/128] via 209.17.220.1, 01:52:05,
Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0

MEDELLIN1#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

System tray area containing icons for network, volume, and power, along with the text "ESP 03:23 p. m. 24/04/2020" and a notification icon.

FIGURA 29 Tabla de enrutamiento MEDELLIN1

```
Gateway of last resort is not set

    172.29.0.0/16 is variably subnetted, 14 subnets, 4 masks
S    172.29.0.0/22 is directly connected, Serial0/3/1
O    172.29.0.0/24 [110/129] via 209.17.220.6, 01:52:23,
Serial0/3/1
S    172.29.1.0/24 is directly connected, Serial0/3/1
O    172.29.3.0/30 [110/128] via 209.17.220.6, 01:52:23,
Serial0/3/1
O    172.29.3.4/30 [110/128] via 209.17.220.6, 01:52:23,
Serial0/3/1
O    172.29.3.8/30 [110/128] via 209.17.220.6, 01:52:23,
Serial0/3/1
O    172.29.3.12/30 [110/192] via 209.17.220.6, 01:52:23,
Serial0/3/1
S    172.29.4.0/22 is directly connected, Serial0/3/0
O    172.29.4.0/25 [110/129] via 209.17.220.2, 01:53:39,
Serial0/3/0
S    172.29.4.128/25 is directly connected, Serial0/3/0
O    172.29.6.0/30 [110/128] via 209.17.220.2, 01:53:39,
Serial0/3/0
O    172.29.6.4/30 [110/192] via 209.17.220.2, 01:53:39,
Serial0/3/0
O    172.29.6.8/30 [110/128] via 209.17.220.2, 01:53:39,
Serial0/3/0
O    172.29.6.12/30 [110/128] via 209.17.220.2, 01:53:39,
Serial0/3/0
    209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C    209.17.220.0/30 is directly connected, Serial0/3/0
L    209.17.220.1/32 is directly connected, Serial0/3/0
C    209.17.220.2/32 is directly connected, Serial0/3/0
C    209.17.220.4/30 is directly connected, Serial0/3/1
L    209.17.220.5/32 is directly connected, Serial0/3/1
C    209.17.220.6/32 is directly connected, Serial0/3/1

ISP#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

] Top

System tray area containing icons for network, volume, and power, along with the text 'ESP 03:24 p. m. 24/04/2020' and a notification icon.

FIGURA 31 Tabla de enrutamiento ISP

```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O    172.29.0.0/24 [110/65] via 172.29.3.2, 01:54:02, Serial0/1/1
O    172.29.1.0/24 [110/65] via 172.29.3.10, 01:54:02, Serial0/2/0
C    172.29.3.0/30 is directly connected, Serial0/1/1
L    172.29.3.1/32 is directly connected, Serial0/1/1
C    172.29.3.4/30 is directly connected, Serial0/2/1
L    172.29.3.5/32 is directly connected, Serial0/2/1
C    172.29.3.8/30 is directly connected, Serial0/2/0
L    172.29.3.9/32 is directly connected, Serial0/2/0
O    172.29.3.12/30 [110/128] via 172.29.3.2, 01:54:02,
Serial0/1/1
                                     [110/128] via 172.29.3.10, 01:54:02,
Serial0/2/0
O    172.29.4.0/25 [110/193] via 209.17.220.5, 01:52:42,
Serial0/1/0
O    172.29.4.128/25 [110/193] via 209.17.220.5, 01:52:42,
Serial0/1/0
O    172.29.6.0/30 [110/192] via 209.17.220.5, 01:52:42,
Serial0/1/0
O    172.29.6.4/30 [110/256] via 209.17.220.5, 01:52:42,
Serial0/1/0
O    172.29.6.8/30 [110/192] via 209.17.220.5, 01:52:42,
Serial0/1/0
O    172.29.6.12/30 [110/192] via 209.17.220.5, 01:52:42,
Serial0/1/0
    209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
O    209.17.220.0/30 [110/128] via 209.17.220.5, 01:52:42,
Serial0/1/0
C    209.17.220.4/30 is directly connected, Serial0/1/0
C    209.17.220.5/32 is directly connected, Serial0/1/0
L    209.17.220.6/32 is directly connected, Serial0/1/0
S*  0.0.0.0/0 is directly connected, Serial0/1/0

BOGOTA1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

03:24 p. m. 24/04/2020

FIGURA 302 Tabla de enrutamiento BOGOTA1

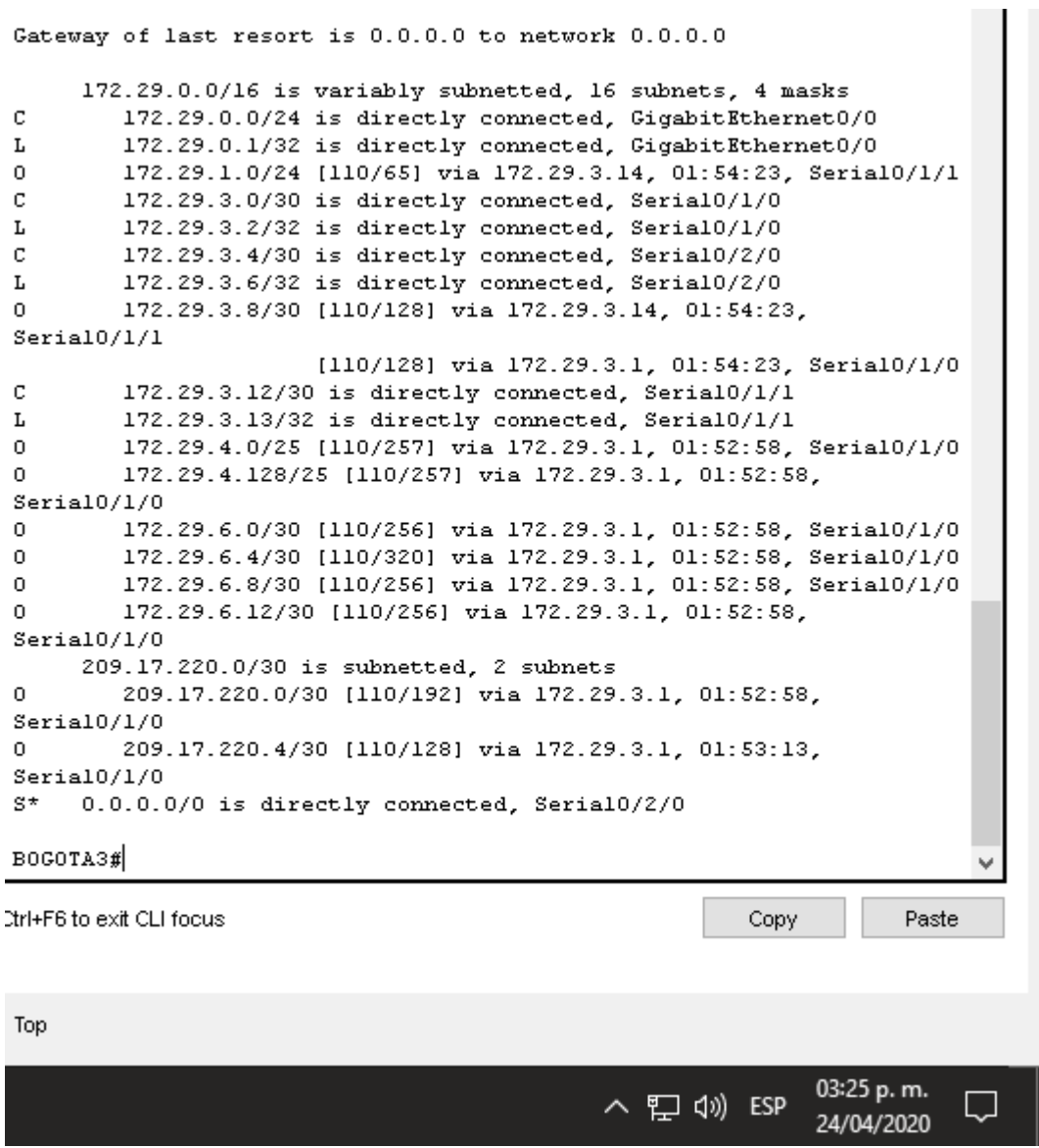


FIGURA 33 Tabla de enrutamiento BOGOTA3

```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O   172.29.0.0/24 [110/65] via 172.29.3.13, 01:54:26, Serial0/1/1
C   172.29.1.0/24 is directly connected, GigabitEthernet0/0
L   172.29.1.1/32 is directly connected, GigabitEthernet0/0
O   172.29.3.0/30 [110/128] via 172.29.3.13, 01:54:26,
Serial0/1/1
                                     [110/128] via 172.29.3.9, 01:54:26, Serial0/1/0
O   172.29.3.4/30 [110/128] via 172.29.3.13, 01:54:26,
Serial0/1/1
                                     [110/128] via 172.29.3.9, 01:54:26, Serial0/1/0
C   172.29.3.8/30 is directly connected, Serial0/1/0
L   172.29.3.10/32 is directly connected, Serial0/1/0
C   172.29.3.12/30 is directly connected, Serial0/1/1
L   172.29.3.14/32 is directly connected, Serial0/1/1
O   172.29.4.0/25 [110/257] via 172.29.3.9, 01:53:16, Serial0/1/0
O   172.29.4.128/25 [110/257] via 172.29.3.9, 01:53:16,
Serial0/1/0
O   172.29.6.0/30 [110/256] via 172.29.3.9, 01:53:16, Serial0/1/0
O   172.29.6.4/30 [110/320] via 172.29.3.9, 01:53:16, Serial0/1/0
O   172.29.6.8/30 [110/256] via 172.29.3.9, 01:53:16, Serial0/1/0
O   172.29.6.12/30 [110/256] via 172.29.3.9, 01:53:16,
Serial0/1/0
    209.17.220.0/30 is subnetted, 2 subnets
O   209.17.220.0/30 [110/192] via 172.29.3.9, 01:53:16,
Serial0/1/0
O   209.17.220.4/30 [110/128] via 172.29.3.9, 01:53:31,
Serial0/1/0
S*  0.0.0.0/0 is directly connected, Serial0/1/0

BOGOTA2#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

03:25 p. m.
24/04/2020

FIGURA 31 Tabla de enrutamiento BOGOTA2

6.3 Deshabilitar la propagación del protocolo OSPF.

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

En este paso se cambiaron las interfaces que no se usan, a modo pasivo, con el fin de disminuir el ancho de banda que consumen al momento de la propagación, para ello se utilizó el comando «passive-interface» seguido del tipo de interfaz y su slot.

BOGOTA1

```
BOGOTA1(config)#router ospf 1
```

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

BOGOTA2

```
BOGOTA2(config)#router ospf 1
```

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

BOGOTA3

```
BOGOTA3(config)#router ospf 1
```

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

MEDELLIN1

```
MEDELLIN1(config)#router ospf 1
```

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

MEDELLIN2

```
MEDELLIN2(config)#router ospf 1
```

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

MEDELLIN3

```
MEDELLIN3(config)#router ospf 1
```

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

6.4 Verificación del protocolo OSPF.

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

Para verificar el protocolo OSPF y la versión del mismo en un router, solo es Necesario ingresar al modo privilegiado e ingresar el comando «show ip protocols»;

```
MEDELLIN2#sh ip proto

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 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:12:48
    172.29.3.14      110          00:12:49
    172.29.6.5       110          00:12:49
    172.29.6.14      110          00:12:47
    209.17.220.2     110          00:12:47
    209.17.220.5     110          00:11:29
    209.17.220.6     110          00:11:27
  Distance: (default is 110)

MEDELLIN2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

04:47 p. m.
24/04/2020

FIGURA 32 Protocolo ospf en MEDELLIN2

```
MEDELLIN3#sh 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 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.128 0.0.0.127 area 0
    172.29.6.4 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  172.29.3.13       110          00:13:10
  172.29.3.14       110          00:13:11
  172.29.6.5        110          00:13:12
  172.29.6.14       110          00:13:09
  209.17.220.2      110          00:13:09
  209.17.220.5      110          00:11:51
  209.17.220.6      110          00:11:49
  Distance: (default is 110)

MEDELLIN3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

^ [] [] ESP 04:47 p. m. 24/04/2020 [] 2

FIGURA 33 Protocolo ospf en MEDELLIN3

```

MEDELLIN1#sh ip protoc

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 209.17.220.2
  It is an autonomous system boundary router
  Redistributing External Routes from,
    static
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
    209.17.220.0 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/2/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:13:32
    172.29.3.14      110          00:13:33
    172.29.6.5       110          00:13:33
    172.29.6.14      110          00:13:31
    209.17.220.2     110          00:13:30
    209.17.220.5     110          00:12:13
    209.17.220.6     110          00:12:11
  Distance: (default is 110)

MEDELLIN1#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

^ [] [] ESP

04:48 p. m.
24/04/2020

2

FIGURA 34 Protocolo ospf en MEDELLIN1

```
BOGOTA1#sh 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 209.17.220.6
  It is an autonomous system boundary router
  Redistributing External Routes from,
    static
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/2/1
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13       110          00:13:52
    172.29.3.14       110          00:13:53
    172.29.6.5        110          00:13:53
    172.29.6.14       110          00:13:51
    209.17.220.2      110          00:13:50
    209.17.220.5      110          00:12:33
    209.17.220.6      110          00:12:30
  Distance: (default is 110)

BOGOTA1#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

System tray area containing icons for network, volume, and power, along with the text "ESP 04:48 p. m. 24/04/2020" and a notification icon with the number "2".

FIGURA 35 Protocolo ospf en BOGOTA1

```
BOGOTA3#sh 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 172.29.3.13
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.255 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:14:15
    172.29.3.14      110          00:14:16
    172.29.6.5       110          00:14:16
    172.29.6.14      110          00:14:15
    209.17.220.2     110          00:14:14
    209.17.220.5     110          00:12:56
    209.17.220.6     110          00:12:54
  Distance: (default is 110)

BOGOTA3#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

^ [] [] ESP 04:49 p. m. 24/04/2020 [] 2

FIGURA 36 Protocolo ospf en BOGOTA3

```
BOGOTA2#sh 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 172.29.3.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13       110          00:14:37
    172.29.3.14       110          00:14:37
    172.29.6.5        110          00:14:38
    172.29.6.14       110          00:14:36
    209.17.220.2       110          00:14:35
    209.17.220.5       110          00:13:18
    209.17.220.6       110          00:13:15
  Distance: (default is 110)

BOGOTA2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

^ [ESP] 04:49 p. m. 24/04/2020 [2]

FIGURA 40 Protocolo OSPF en BOGOTA2

6.5 Configurar encapsulamiento y autenticación PPP.

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

MEDELLIN 1

Necesitaremos tener un usuario con su contraseña desde ISP

```
MEDELLIN1(config)#username ISP secret ISP
```

Configuramos la interfaz con encapsulamiento ppp con nuestro usuario local

```
MEDELLIN1(config)#interface Serial0/1/0
```

```
MEDELLIN1(config)#encapsulation ppp
```

```
MEDELLIN1(config)#ppp authentication pap
```

```
MEDELLIN1(config)#ppp pap sent-username MEDELLIN1 password MEDELLIN
```

ISP

para Bogotá crearemos un usuario local

```
ISP(config)#username BOGOTA1 secret BOGOTA1
```

lo mismo haremos con Medellín

```
ISP(config)#username MEDELLIN1 secret MEDELLIN1
```

configuraremos la interfaz con ppp y autenticación pap

```
ISP(config)#interface Serial0/3/0
```

```
ISP(config)#encapsulation ppp
```

```
ISP(config)#ppp authentication pap
```

```
ISP(config)#ppp pap sent-username ISP password ISP
```

```
ISP(config)#no keepalive
```

Lo mismo haremos con para la interfaz que lleva hacia bogota

```
ISP(config)#interface Serial0/3/1
```

```
ISP(config)#encapsulation ppp
```

```
ISP(config)#ppp authentication chap
```

```
ISP(config)#no keepalive
```

BOGOTA1

para bogota crearemos un usuario local





```
BOGOTA1(config)#username ISP secret ISP
```

configuraremos la interfaz con ppp y autenticación chap

BOGOTA1(config)#interface Serial0/1/0

BOGOTA1(config)#encapsulation ppp

BOGOTA1(config)#ppp authentication chap

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ec
	Successful	MEDE...	BOGOTA1	ICMP		0.000	N	0	(e
	Successful	BOG...	MEDELLIN1	ICMP		0.000	N	1	(e

Taskbar: ^ [ESP] 05:09 p. m. 24/04/2020 [2]

FIGURA 37 Verificacion protocolo ppp

6.6 Configuración de NAT Sobrecargado(PAT).

En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

MEDELLIN1

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

Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, como diferente puerto.

BOGOTA1

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

At Device: MEDELLIN1
 Source: PC1
 Destination: ISP

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 172.29.4.4, Dest. IP: 209.17.220.1 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC
Layer 1: Port Serial0/1/1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 209.17.220.2, Dest. IP: 209.17.220.1 ICMP Message Type: 8
Layer 2: PPP Frame PPP
Layer 1: Port(s): Serial0/1/0

1. Serial0/1/1 receives the frame.

Challenge Me

<< Previous Layer

Next Layer >>



FIGURA 38 Traducción de direcciones en MEDELLIN1

```
BOGOTA1#sh ip nat trans
Pro Inside global    Inside local    Outside local    Outside global
icmp 209.17.220.6:1  172.29.0.2:1   209.17.220.5:1  209.17.220.5:1
BOGOTA1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

04:07 p. m.
25/04/2020

FIGURA 39 Traducciones en BOGOTA1

“Al momento de la configuración del PAT logramos evidenciar que las interfaces internas en el documento no se encontraban configuradas, logrando así dar una solución al problema”

6.7 Configuración del servicio DHCP.

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

MEDELLIN2

Necesitamos excluir las direcciones que nos indican

```
MEDELLIN2 (config)#ip DHCP excluded-address 172.29.4.1 172.29.4.3
```

```
MEDELLIN2 (config)#ip DHCP excluded-address 172.29.4.129 172.29.4.132
```

creamos el primer pool de direcciones para medellin2

```
MEDELLIN2 (config)#ip DHCP pool MEDELLIN2
```

```
MEDELLIN2 (config)#network 172.29.4.0 255.255.255.128
```

```
MEDELLIN2 (config)#default-router 172.29.4.1
```

```
MEDELLIN2(config)#dns-server 8.8.4.4
```

creamos el tercer pool de direcciones para medellin3

```
MEDELLIN2(config)#ip DHCP pool MEDELLIN3
```

```
MEDELLIN2(config)#network 172.29.4.128 255.255.255.128
```

```
MEDELLIN2(config)#default-router 172.29.4.129
```

```
MEDELLIN2(config)#dns-server 8.8.4.4
```

creamos el pool de direcciones para bogota2

```
MEDELLIN2(config)#ip DHCP pool BOGOTA2
```

```
MEDELLIN2(config)#network 172.29.0.0 255.255.255.0
```

```
MEDELLIN2(config)#default-router 172.29.0.1
```

```
MEDELLIN2(config)#dns-server 8.8.8.8
```

creamos el pool de direcciones para bogota3

```
MEDELLIN2(config)#ip DHCP pool BOGOTA3
```

```
MEDELLIN2(config)#network 172.29.1.0 255.255.255.0
```

```
MEDELLIN2(config)#default-router 172.29.1.1
```

```
MEDELLIN2(config)#dns-server 8.8.8.8
```

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

MEDELLIN3

Para que medellin3 pueda recibir direcciones debemos permitir el paso de broadcast

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

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

Para que bogota2 y bogota3 puedan recibir direcciones debemos permitir el paso de broadcast

BOGOTA2

```
interface GigabitEthernet0/0  
ip helper-address 172.29.6.2
```

BOGOTA3

```
interface GigabitEthernet0/0  
ip helper-address 172.29.6.2
```

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Medellín2.

Para que bogota1 pueda permitir direcciones debemos permitir el paso de broadcast

BOGOTA1

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

Interface s0/1/1

```
ip helper-address 172.29.6.2
```

DHCP Static DHCP request successful.

IP Address: 172.29.0.2
 Subnet Mask: 255.255.255.0
 Default Gateway: 172.29.0.1
 DNS Server: 8.8.8.8

IPv6 Configuration

FIGURA 40 Prueba DHCP PC1

IP Configuration

DHCP Static DHCP request successful.

IP Address: 172.29.4.133
 Subnet Mask: 255.255.255.128
 Default Gateway: 172.29.4.129
 DNS Server: 8.8.4.4

FIGURA 41 Prueba DHCP PC

```

MEDELLIN2#sh ip dhcp bin
IP address      Client-ID/      Lease expiration  Type
                Hardware address
172.29.4.4      0060.4756.A222  --                Automatic
172.29.4.133   000D.BDC2.81BD  --                Automatic
172.29.0.2     0060.5C33.5B9E  --                Automatic
172.29.1.2     0010.115C.301E  --                Automatic
MEDELLIN2#
  
```

FIGURA 42 Arrendamiento de direcciones en MEDELLIN2

CONCLUSIONES

Exitosamente se obtuvo una satisfactoria conexión, configuración y simulación de los dispositivos de la red en el proporcionado caso de estudio.

Por medio del diplomado de profundización de Cisco, se logró que todos los estudiantes a través del trabajo componente práctico, verifiquen las fortalezas y debilidades frente al tema Configuramos las operaciones básicas de una red conmutada pequeña y resolvimos problemas relacionados.

Gracias al acompañamiento y asesoramiento de los tutores, se logró aclarar dudas en inquietudes frente al tema.

Configuramos y controlamos ACL para IPv4, y resolvimos problemas relacionados. Por medio del desarrollo de cada una de las actividades, se ha adquirido grandes competencias basadas en la toma de decisiones y solución a diversas problemáticas por medio del componente práctico.

Con el diplomado de Cisco, se realizó enrutamiento en soluciones de red, lo que nos permite adquirir bases necesarias para el progreso laboral, profesional y personal.

La universidad nacional abierta y a Distancia UNAD nos da la oportunidad gracias al diplomado de Cisco en tener la capacidad de ejecutar diferentes procesos de configuración en los dispositivos, trabajando cada aspecto en sistemas que promueven soluciones de red.

BIBLIOGRAFÍA

Lammle, T. "CISCO Press (Ed). Cisco Certified Network Associate Study Guide". {En línea} {2010} Disponible en: (<http://gonda.nic.in/swangonda/pdf/ccna1.pdf>)

Lucas, M. "Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: NoStarchPress". {En línea} {2009} Disponible en: (<http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live>)

Macfarlane, J. "Network Routing Basics: Understanding IP Routing in Cisco Systems". {En línea} {2014} Disponible en: (<http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>)

Odom, W. "CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide". {En línea} {2013} Disponible en: (<http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>)

Odom, W. "CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide" {En línea} {2013} Disponible en: (<http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/CiscoICND2.pdf>)