

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

LEONARDO PAEZ NIEVES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
PROGRAMA DE INGENIERÍA ELÉCTRICA

YOPAL

2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

LEONARDO PAEZ NIEVES

Proyecto presentado como requisito parcial  
para aspirar al título de Ingeniero Electrónico

Director

Diego Edinson Ramírez Claros

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
PROGRAMA DE INGENIERÍA ELÉCTRICA

YOPAL

2020

Nota de Aceptación

---

---

---

---

---

Firma del Presidente del jurado

---

Firma del jurado 1 - Evaluador

---

Firma del jurado 2 - Evaluador

---

Firma del jurado 3 - Director

Yopal, 22 de Mayo de 2020

A mi Zamary mi compañera hasta el  
final, a mis padres, a mis hijos

## AGRADECIMIENTOS

A la Universidad Nacional Abierta y a Distancia UNAD, a la academia CISCO, a todas las personas involucradas en el desarrollo de este trabajo al director de curso, tutores y compañeros.

# CONTENIDO

	<b>pág.</b>
<b>1. GLOSARIO</b>	<b>12</b>
<b>2. RESUMEN</b>	<b>13</b>
<b>3. INTRODUCCIÓN</b>	<b>14</b>
<b>4. OBJETIVOS</b>	<b>15</b>
4.1. Objetivo General . . . . .	15
4.2. Objetivos Específicos . . . . .	15
<b>5. DESARROLLO DE LOS DOS ESCENARIOS</b>	<b>16</b>
5.1. Escenario 1 . . . . .	16
5.1.1. Parte 1: Inicializar dispositivos . . . . .	17
5.1.2. Parte 2: Configurar los parámetros básicos de los dispositivos . .	18
5.1.3. Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN . . . . .	29
5.1.4. Parte 4: Configurar el protocolo de routing dinámico RIPv2 . .	33
5.1.5. Parte 5: Implementar DHCP y NAT para IPv4 . . . . .	36
5.1.6. Parte 6: Configurar NTP . . . . .	39
5.1.7. Parte 7: Configurar y verificar las listas de control de acceso (ACL)	40
5.2. Escenario 2 . . . . .	42

5.2.1.	Parte 1: Configuración del enrutamiento. . . . .	52
5.2.2.	Parte 2: Tabla de Enrutamiento. . . . .	55
5.2.3.	Parte 3: Deshabilitar la propagación del protocolo OSPF. . . . .	58
5.2.4.	Parte 4: Verificación del protocolo OSPF. . . . .	58
5.2.5.	Configurar encapsulamiento y autenticación PPP. . . . .	61
5.2.6.	Parte 6: Configuración de NAT. . . . .	61
5.2.7.	Parte 7: Configuración del servicio DHCP. . . . .	63
<b>6.</b>	<b>Conclusiones</b>	<b>65</b>
<b>7.</b>	<b>Bibliografía</b>	<b>66</b>

## LISTA DE TABLAS

1.	Iniciar dispositivos . . . . .	17
2.	Configuración computadora de Internet . . . . .	18
3.	Configuración servidor web . . . . .	19
4.	Configuración R1 . . . . .	19
5.	Configuración R2 . . . . .	21
6.	Configuración R3 . . . . .	23
7.	Configuración S1 . . . . .	25
8.	Configuración S3 . . . . .	26
9.	Verificación conectividad escenario 1 . . . . .	27
10.	Configuración S1 routing Vlan . . . . .	29
11.	Configuración S3 routing Vlan . . . . .	30
12.	Configuración R1 routing Vlan . . . . .	31
13.	Verificación conectividad Switch a VLAN R1 . . . . .	32
14.	Configuración de RIPv2 en R1 . . . . .	33
15.	Configuración de RIPv2 en R2 . . . . .	34
16.	Configuración de RIPv2 en R3 . . . . .	34
17.	Verificar información RIPv2 . . . . .	35
18.	Router 1 servidor DHCP para van 21 y 23 . . . . .	36
19.	Router 2 NAT estática y dinámica . . . . .	37
20.	Verificación Protocolo DHCP y NAT . . . . .	38



21.	Configuración NTP . . . . .	39
22.	Configuración acceso a las líneas VTY en el R2 . . . . .	40
23.	Diferentes comandos CLI . . . . .	41
24.	Sumarización red Bogota . . . . .	54
25.	Sumarización red Medellin . . . . .	54

## LISTA DE FIGURAS

1.	Escenario 1 . . . . .	16
2.	Switch 1 no vlan dat . . . . .	17
3.	Switch 2 no vlan dat . . . . .	18
4.	Configuración R1 . . . . .	20
5.	Configuración R2 . . . . .	22
6.	Configuración R3 . . . . .	24
7.	Configuración S1 . . . . .	25
8.	Configuración S3 . . . . .	26
9.	Prueba de ping R1 a R2 . . . . .	27
10.	Prueba de ping R2 a R3 . . . . .	28
11.	Prueba de ping PC Internet a R2 . . . . .	28
12.	Visualización de las sub-interfaces R1 . . . . .	31
13.	Prueba ping conectividad S1 - R1 VLAN . . . . .	32
14.	Prueba ping conectividad S3 - R1 VLAN . . . . .	33
15.	Comando mostrar solo rutas RIP . . . . .	35
16.	Visualizar DHCP pool . . . . .	36
17.	Visualizar Configuración de NTP en R1 . . . . .	39
18.	Conexión telnet a R2 desde R1 . . . . .	40
19.	Escenario 2 . . . . .	42
20.	Tabla de enrutamiento B1 . . . . .	55

21.	Tabla de enrutamiento B2 . . . . .	55
22.	Tabla de enrutamiento M1 . . . . .	56
23.	Tabla de enrutamiento M2 . . . . .	56
24.	Tabla de enrutamiento M3 . . . . .	57
25.	Tabla de enrutamiento ISP . . . . .	58
26.	Comando sh ip protocols B1 . . . . .	59
27.	Comando sh ip route ospf B1 . . . . .	59
28.	Comando sh ip protocol M1 . . . . .	60
29.	Comando sh ip route ospf M1 . . . . .	60
30.	Ping entre redes LAN M2-M3 . . . . .	62
31.	Comando traceroute desde M2 hasta LAN B2 . . . . .	62

# 1. GLOSARIO

**CIFRADO:** Es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.

**DHCP:** El DHCP (Protocolo de configuración dinámica de host) es un protocolo de administración de red utilizado para asignar dinámicamente una dirección de Protocolo de Internet (IP) a cualquier dispositivo o nodo en una red para que puedan comunicarse mediante IP.

**DIRECCIÓN IP:** Dirección que se utiliza para identificar un equipo o dispositivo en una red.

**DIRECCIÓN IP DINÁMICA:** Dirección IP temporal que asigna un servidor DHCP.

**DIRECCIÓN IP ESTÁTICA:** Dirección fija asignada a un equipo o dispositivo conectado a una red.

**DNS:** (Servidor de nombres de dominio) la dirección IP de un servidor que traduce los nombres de los sitios Web a direcciones IP.

**ENRUTADOR:(ROUTER)** Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

**ENRUTAMIENTO ESTÁTICO:** Reenvío de datos de una red a través de una ruta fija.

**ENRUTAMIENTO DINÁMICO:** enrutamiento adaptativo, proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino específico.

**OSPF:** es un protocolo de red para encaminamiento jerárquico de pasarela interior que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

**RIP:** El Protocolo de Información de Encaminamiento, utilizado por los routers para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados.

## 2. RESUMEN

Las redes de comunicaciones son la interconexión de diferentes dispositivos se tienen niveles de extensión empezando por una red pequeña conocida como red de área local, una red de área metropolitana y red de área extensa entre otras. Las redes se deben configurar para su correcto funcionamiento, ayudados por protocolos como el protocolo RIP, el cual es un protocolo que trabaja con direccionamiento IP V4 y el protocolo OSPF el cual es dinámico teniendo una rápida adaptación a los cambios en la topología.

El objetivo de este trabajo es implementar en un escenario el protocolo RIP y en otro escenario el protocolo OSPF mediante la interfaz de línea de comando (CLI) en los equipos de la red de comunicaciones, no si haber realizado antes la configuración básica de los routers y switches en cuanto a seguridad y direccionamiento.

### 3. INTRODUCCIÓN

Cisco una empresa líder en el ambiente de redes de datos y TI, provee soluciones a través de componentes de red, como routers, firewalls de hardware, productos de telefonía IP, así mismo suministra programas educativos para la formación y certificación que dota de las habilidades prácticas necesarias para diagnosticar y solucionar problemas específicos de redes de comunicaciones.

El presente trabajo se realiza con el objetivo de evidenciar el resultado obtenido durante el desarrollo de los cursos Cisco CCNA1 y CCNA2, esta demostración se realizara a través del desarrollo de dos escenarios propuestos donde se aplicaran los conocimientos adquiridos en los temas como; 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.

## 4. OBJETIVOS

### 4.1. Objetivo General

Aplicar los conocimientos adquiridos durante el desarrollo del diplomado CISCO CCNA, a del desarrollo de dos escenarios practicos implementados en el software de simulación de redes Packet Tracer.

### 4.2. Objetivos Específicos

- Configurar de manera correcta dispositivos comunicación en redes como Switchs, Routers, Servidores.
- Aplicar niveles de seguridad básico en los dispositivos de red.
- Implementar los protocolos de enrutamiento dando respuesta a los requerimientos del problema.
- Implementar los protocolos de enrutamiento dando respuesta a los requerimientos del problema.
- Realizar los pasos necesarios para lograr la configuración correcta de los protocolos OSPF y RIP, así como operaciones de NAT y DHCP.
- Realizar y documentar pruebas que evidencien el correcto funcionamiento de los equipos y los protocolos implementados.

## 5. DESARROLLO DE LOS DOS ESCENARIOS

### 5.1. Escenario 1

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

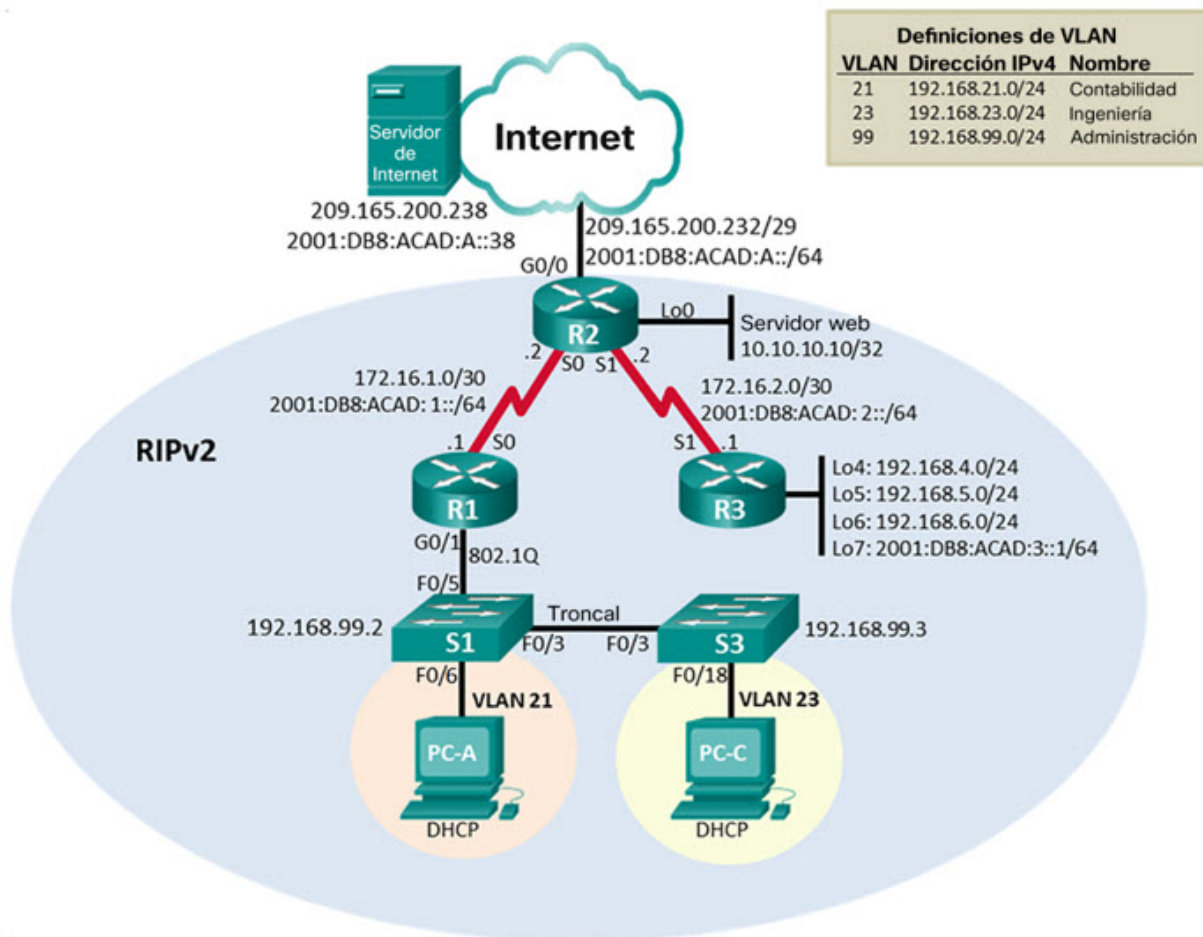


Figura 1: Escenario 1



### 5.1.1. Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches.

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

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1: Iniciar dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

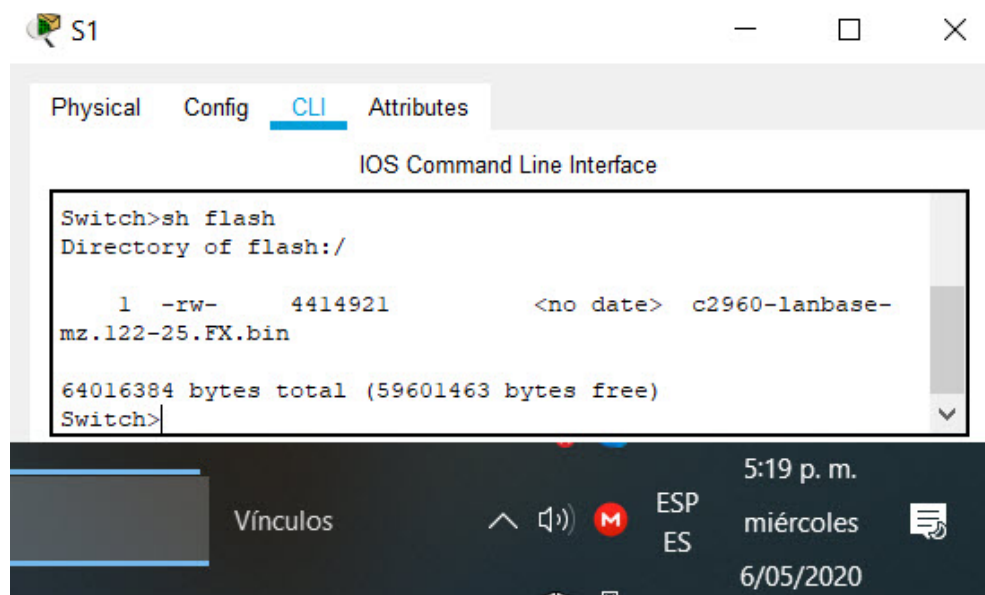


Figura 2: Switch 1 no vlan dat

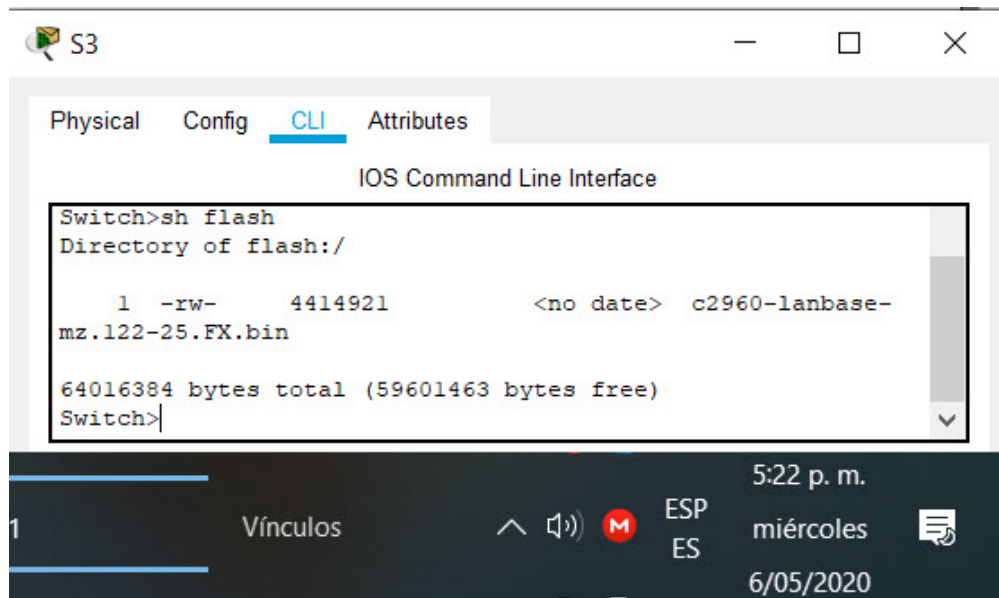


Figura 3: Switch 2 no vlan dat

### 5.1.2. Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet. Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 2: Configuración computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Tabla 3: Configuración servidor web

Elemento o tarea de configuración	Especificación
Dirección IPv4	10.10.10.10
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	10.10.10.1

Paso 2: Configurar R1. Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4: Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # mensaje #
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 enable R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)# ipv6 route ::/0 s0/0/0

```
R1#sh run
Building configuration...

Current configuration : 1074 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX1524B5CC-
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
description Conexión a R2
ip address 172.16.1.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:1::1/64
ipv6 enable
clock rate 128000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
ipv6 route ::/0 Serial0/0/0
!
banner motd ^CSe prohbe el acceso no autorizado.^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
!
end
R1#
```

Figura 4: Configuración R1

Paso 3: Configurar R2. La configuración del R2 incluye las siguientes tareas:

Tabla 5: Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado	R2(config)#enable secret class
Contraseña de acceso a consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config-line)#ip http server R2(config-line)#ip http secure-server R2(config-line)#ip http autenticación local
Mensaje MOTD	R2(config)#banner motd # mensaje #
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 enable R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0	R2(config-if)#interface G0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#description Conexion PC Internet R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz G0/1(servidor web simulado)	R2(config)#interface G0/1 R2(config-if)#description Conexion Servidor Web R2(config-if)#ip address 10.1.10.1 255.255.255.0 R2(config-if)#description Conexion Servidor Web R2(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)# ipv6 route ::/0 s0/0/0

```
R2#sh run
Building configuration...

Current configuration : 1781 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCii
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX1524B972-
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description Conexion PC Internet
ip address 209.165.200.233 255.255.255.248
ip nat outside
duplex auto
speed auto
ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
description Conexion Servidor web
ip address 10.10.10.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
description Conexion a R1
ip address 172.16.1.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Serial0/0/1
description Conexion a R3
ip address 172.16.2.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::2/64
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
ipv6 route ::/0 Serial0/0/0
!
banner motd ^CSe prohíbe el acceso no autorizado^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
!
end
R2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Cisco P... Vínculos 12:00 a. m. jueves 7/05/2020

Figura 5: Configuración R2

Paso 4: Configurar R3. La configuración del R3 incluye las siguientes tareas:

Tabla 6: Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd # mensaje #
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description Conexión a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 enable R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
interfaz loopback 5	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
interfaz loopback 6	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)# ipv6 route ::/0 s0/0/1

```
R3#sh run
Building configuration...

Current configuration : 1308 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQ1FU.ZeC1l
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX15241T6I-
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Loopback4
ip address 192.168.4.1 255.255.255.0
!
interface Loopback5
ip address 192.168.5.1 255.255.255.0
!
interface Loopback6
ip address 192.168.6.1 255.255.255.0
!
interface Loopback7
no ip address
ipv6 address 2001:DB8:ACAD:3::1/64
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
description Conexion a R2
ip address 172.16.2.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::1/64
ipv6 enable
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip flow-export version 9
!
ipv6 route ::0 Serial0/0/0
!
banner motd ^CSe prohíbe el acceso no autorizado^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
!
end
R3#
```

Figura 6: Configuración R3



Paso 5: Configurar S1. La configuración del S1 incluye las siguientes tareas:

Tabla 7: Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd # mensaje #

```

Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#no ip domain-lookup
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)#
S1(config-line)#service password-encryption
S1(config)#service password-encryption
S1(config)#banner motd # Se prohíbe el acceso no autorizado
#
S1(config)#exit
S1#reload
System configuration has been modified. Save? [yes/no]:y
Building configuration...
[OK]
Proceed with reload? [confirm]
  
```

Figura 7: Configuración S1

Paso 6: Configurar el S3. La configuración del S3 incluye las siguientes tareas:

Tabla 8: Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd # mensaje #

```

Switch>
Switch#enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup
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 password-e
S3(config-line)#exit
S3(config)#ser
S3(config)#service p
S3(config)#service password-encryption
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#
  
```

Figura 8: Configuración S3

Paso 7: Verificar la conectividad de la red Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 9: Verificación conectividad escenario 1

Desde	A	Dirección IP	Resultados ping
R1	R2, S0/0/0	2001:DB8:ACAD:1::2	R1#ping ipv6 2001:DB8:ACAD:1::2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/25 ms
R2	R3, S0/0/1	2001:DB8:ACAD:2::1	R2#ping ipv6 2001:DB8:ACAD:2::1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
PC de internet	Gateway predeterminado	209.165.200.233	C:\>ping 2001:DB8:ACAD:A::1 Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time=50ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 50ms, Average = 12ms

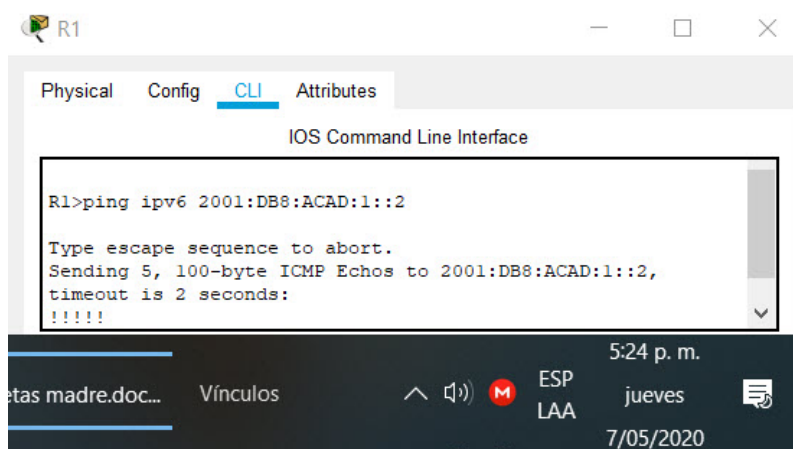


Figura 9: Prueba de ping R1 a R2

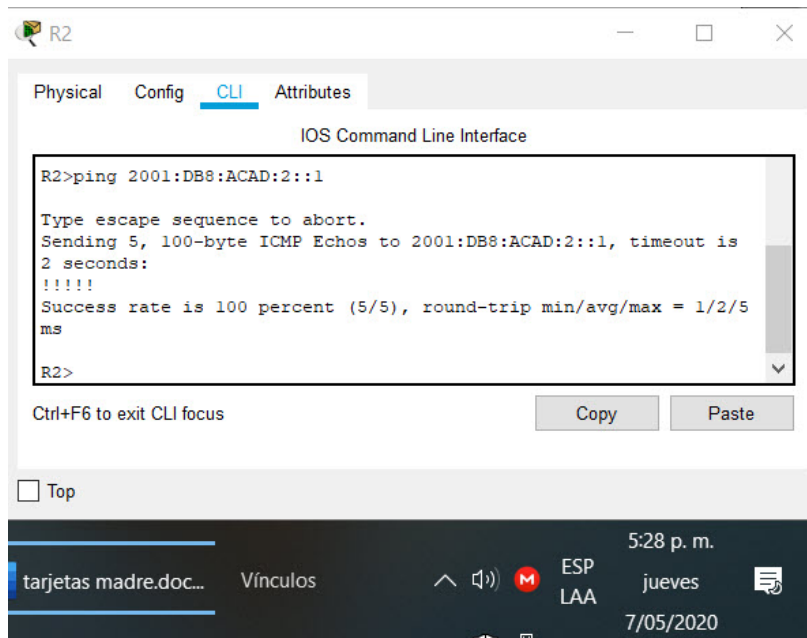


Figura 10: Prueba de ping R2 a R3

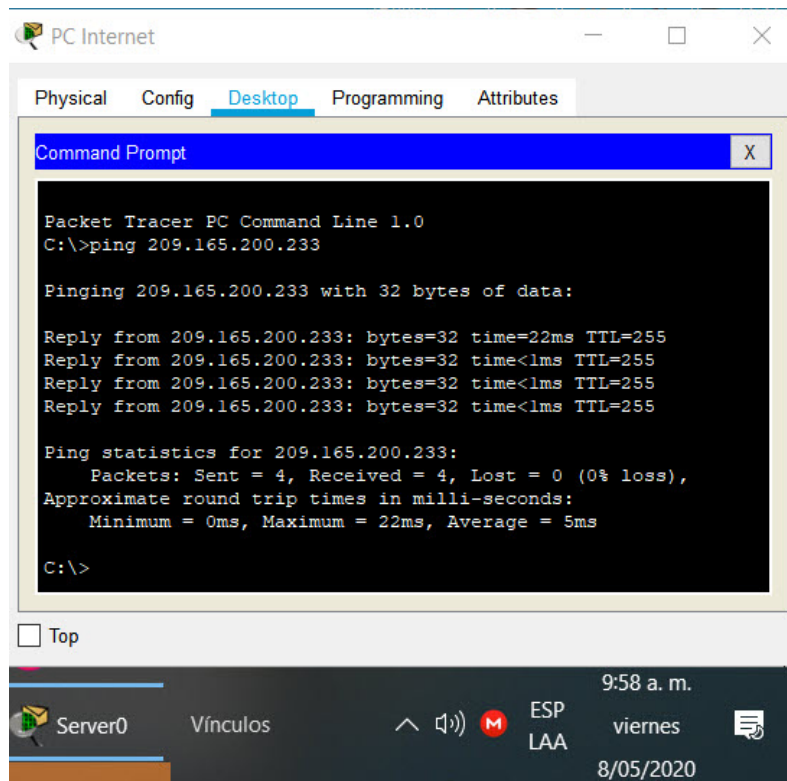


Figura 11: Prueba de ping PC Internet a R2

### 5.1.3. Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1. La configuración del S1 incluye las siguientes tareas:

Tabla 10: Configuración S1 routing Vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>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</pre>
Asignar la dirección IP de administración.	<pre>S1#config terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up  S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S1(config)#int fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Forzar el enlace troncal en la interfaz F0/5	<pre>S1(config)#int fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config)#int fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21</pre>
Apagar todos los puertos sin usar	<pre>S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown</pre>

Paso 2: Configurar el S3.La configuración del S3 incluye las siguientes tareas:

Tabla 11: Configuración S3 routing Vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>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</pre>
Asignar la dirección IP de administración.	<pre>S3(config)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up  S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown</pre>
Asignar el gateway predeterminado	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access</pre>
Asignar F0/18 a la VLAN 23	<pre>S3(config)#int fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23</pre>
Apagar todos los puertos sin usar	<pre>S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access</pre>

Paso 3: Configurar R1. Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12: Configuración R1 routing Vlan

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<pre>R1(config)#int g0/1.21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#description Lan Contabilidad R1(config-subif)#exit</pre>
Configurar la subinterfaz 802.1Q .23 en G0/1	<pre>R1(config)#int g0/1.23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#description Lan Ingenieria R1(config-subif)#exit</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>R1(config)#int g0/1.99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#description Lan Administracion R1(config-subif)#exit</pre>
Activar la interfaz G0/1	<pre>R1(config)#interface g0/1 R1(config-if)#no shutdown</pre>

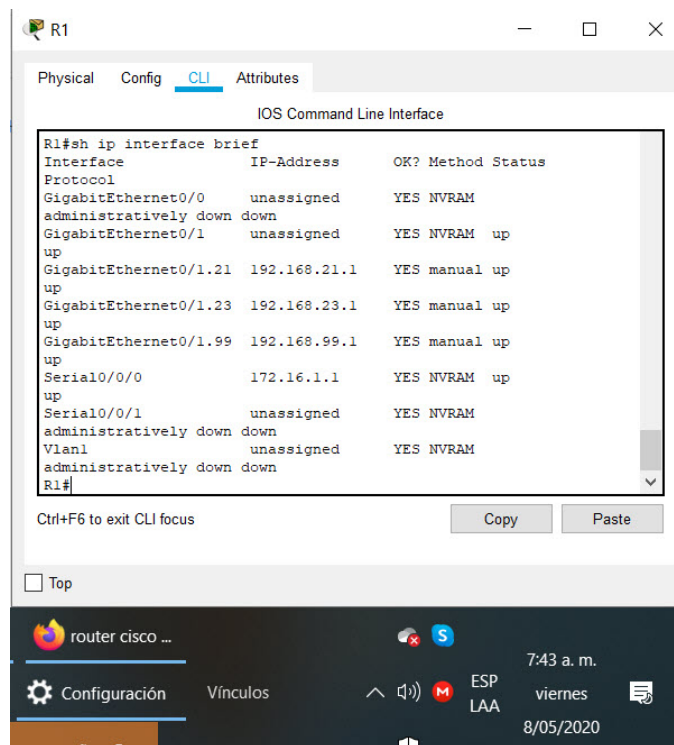


Figura 12: Visualización de las sub-interfaces R1

Tabla 13: Verificación conectividad Switch a VLAN R1

Desde	A	Dirección IP	Resultados ping
S1	R1, VLAN 99	192.168.99.1	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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, VLAN 99	192.168.99.1	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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, VLAN 21	192.168.21.1	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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, VLAN 23	192.168.23.1	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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

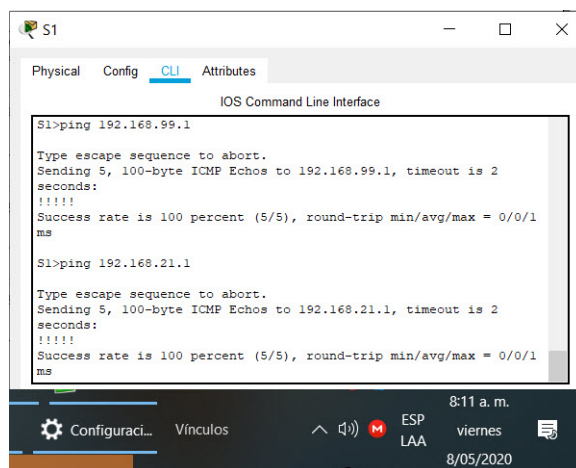


Figura 13: Prueba ping conectividad S1 - R1 VLAN



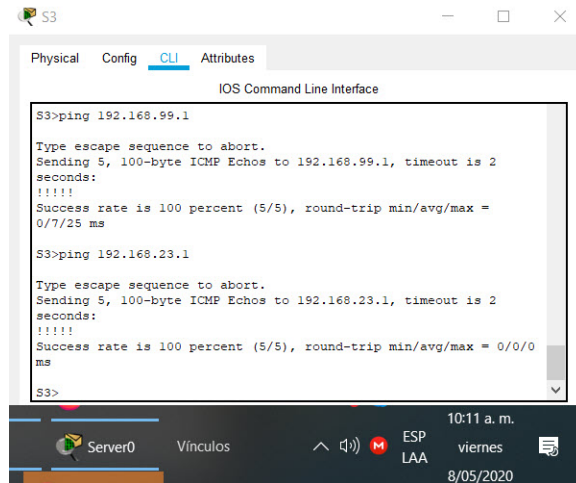


Figura 14: Prueba ping conectividad S3 - R1 VLAN

#### 5.1.4. Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1. Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14: Configuración de RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIPv2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	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
Establecer las interfaces LAN como pasivas	R1(config-router)#passive-interface G0/1
Desactive la sumarización automática.	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2. La configuración del R2 incluye las siguientes tareas:

Tabla 15: Configuración de RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.0
Establecer las interfaces LAN como pasivas	R2(config-router)#passive-interface G0/0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R3. La configuración del R3 incluye las siguientes tareas:

Tabla 16: Configuración de RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar las redes conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer las interfaces LAN como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo4
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: 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 17: Verificar información RIPv2

Elemento o tarea de configuración	Especificación
¿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?	R2#sh ip protocols
¿Qué comando muestra solo las rutas RIP?	R2#sh ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R2#sh ip route rip

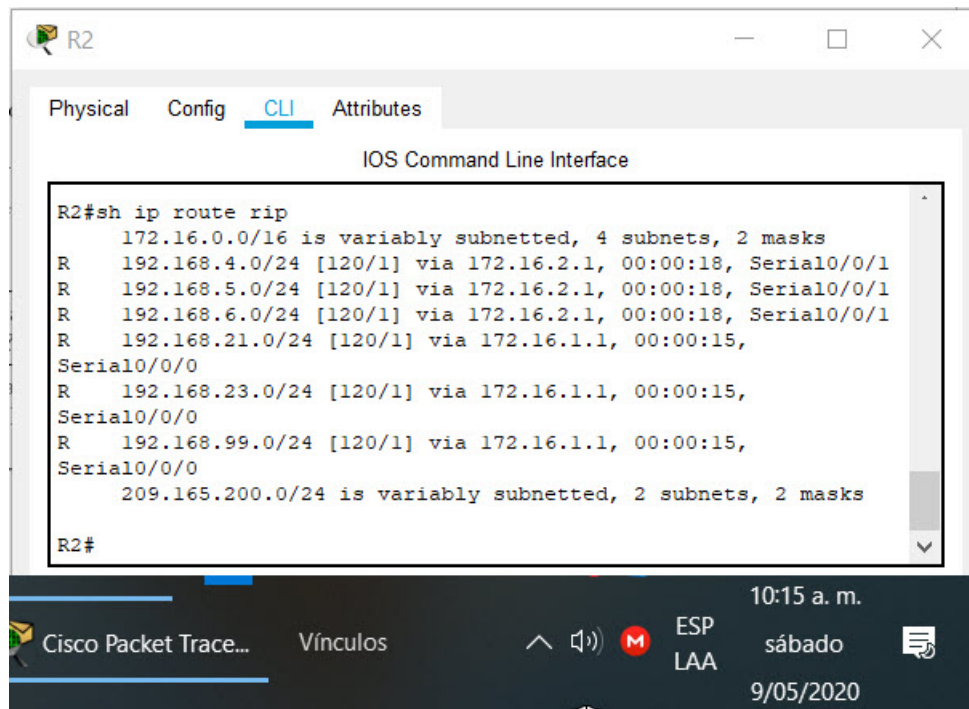


Figura 15: Comando mostrar solo rutas RIP

### 5.1.5. Parte 5: Implementar DHCP y NAT para IPv4

Tabla 18: Router 1 servidor DHCP para van 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 - VLAN 23 para configuraciones estáticas	<pre>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</pre>
Crear un pool de DHCP para la VLAN 21.	<pre>R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0</pre>
Crear un pool de DHCP para la VLAN 23.	<pre>R1(config)#ip dhcp pool ENGR 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 R1(dhcp-config)#network 192.168.23.0 255.255.255.0</pre>



Figura 16: Visualizar DHCP pool

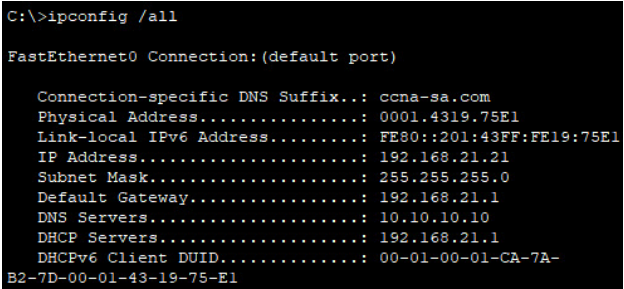
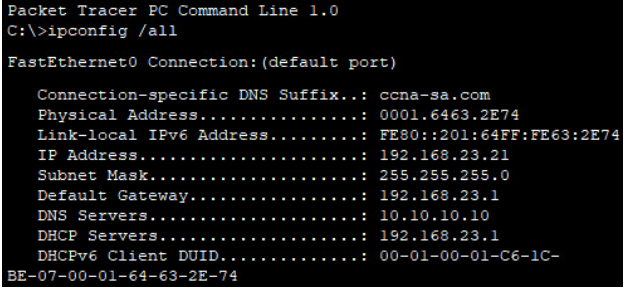
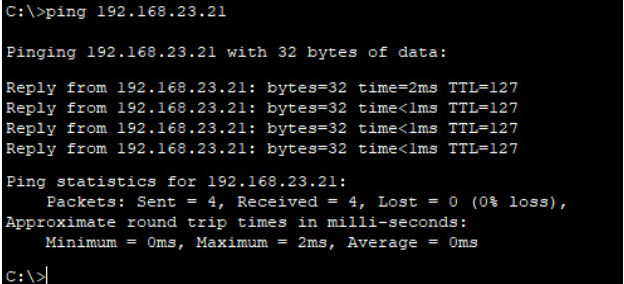
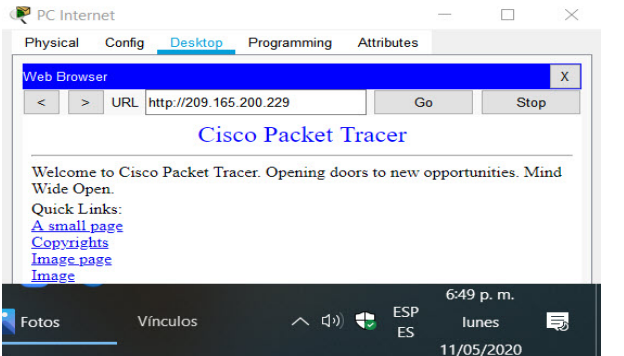
Paso 2: Configurar la NAT estática y dinámica en el R2. La configuración del R2 incluye las siguientes tareas:

Tabla 19: Router 2 NAT estática y dinámica

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	<pre>R2#config terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#username webuser privilege 15 secret cisco 12345</pre>
Habilitar el servicio del servidor HTTP	<pre>R2(config)#ip http server</pre>
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	<pre>R2(config)#ip http authentication local</pre>
Crear una NAT estática al servidor web.	<pre>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229</pre>
Asignar la interfaz interna y externa para la NAT estática	<pre>R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface g0/1 R2(config-if)#ip nat inside</pre>
Configurar la NAT dinámica dentro de una ACL privada	<pre>R2(config)#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</pre>
Defina el pool de direcciones IP públicas utilizables.	<pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</pre>
Definir la traducción de NAT dinámica	<pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>

Paso 3: Verificar el protocolo DHCP y la NAT estática Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta.

Tabla 20: Verificación Protocolo DHCP y NAT

Prueba IP	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	 <pre> C:\&gt;ipconfig /all  FastEthernet0 Connection: (default port)      Connection-specific DNS Suffix...: ccna-sa.com     Physical Address...: 0001.4319.75E1     Link-local IPv6 Address...: FE80::201:43FF:FE19:75E1     IP Address...: 192.168.23.21     Subnet Mask...: 255.255.255.0     Default Gateway...: 192.168.23.1     DNS Servers...: 10.10.10.10     DHCP Servers...: 192.168.23.1     DHCPv6 Client DUID...: 00-01-00-01-CA-7A-B2-7D-00-01-43-19-75-E1         </pre>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <pre> Packet Tracer PC Command Line 1.0 C:\&gt;ipconfig /all  FastEthernet0 Connection: (default port)      Connection-specific DNS Suffix...: ccna-sa.com     Physical Address...: 0001.6463.2E74     Link-local IPv6 Address...: FE80::201:64FF:FE63:2E74     IP Address...: 192.168.23.21     Subnet Mask...: 255.255.255.0     Default Gateway...: 192.168.23.1     DNS Servers...: 10.10.10.10     DHCP Servers...: 192.168.23.1     DHCPv6 Client DUID...: 00-01-00-01-C6-1C-BE-07-00-01-64-63-2E-74         </pre>
<p>Verificar que la PC-A pueda hacer ping a la PC-C</p>	 <pre> C:\&gt;ping 192.168.23.21  Pinging 192.168.23.21 with 32 bytes of data:  Reply from 192.168.23.21: bytes=32 time=2ms TTL=127 Reply from 192.168.23.21: bytes=32 time&lt;1ms TTL=127 Reply from 192.168.23.21: bytes=32 time&lt;1ms TTL=127 Reply from 192.168.23.21: bytes=32 time&lt;1ms TTL=127  Ping statistics for 192.168.23.21:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 2ms, Average = 0ms  C:\&gt;         </pre>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	

### 5.1.6. Parte 6: Configurar NTP

Tabla 21: Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 9:00:00 March 5 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#ntp up

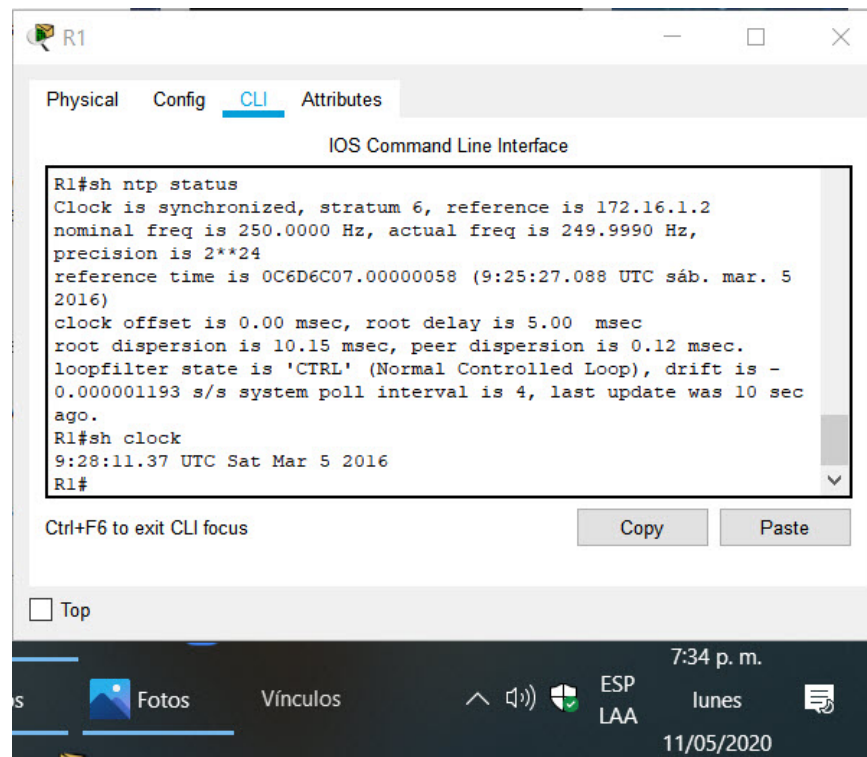


Figura 17: Visualizar Configuración de NTP en R1

### 5.1.7. Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 22: Configuración acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	<pre>R2(config)#ip access-list standar ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1</pre>
Aplicar la ACL con nombre a las líneas VTY	<pre>R2(config-std-nacl)#line vty 0 4</pre>
Permitir acceso por Telnet a las líneas de VTY	<pre>R2(config-line)#transport input telnet R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit</pre>
Verificar que la ACL funcione como se espera	<pre>R1#line telnet 172.16.1.2 password R2&gt;</pre>

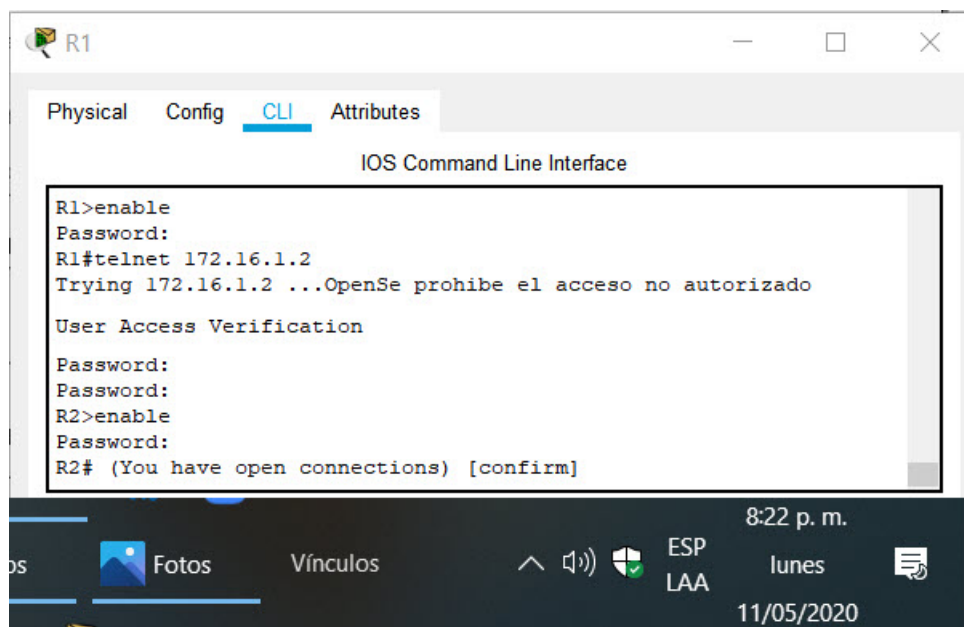


Figura 18: Conexión telnet a R2 desde R1



Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 23: Diferentes comandos CLI

Descripción del comando	Comando
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	<pre>R2#sh access-list Standard IP access list 1  10 permit 192.168.21.0 0.0.0.255  20 permit 192.168.23.0 0.0.0.255  30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT  10 permit host 172.16.1.1</pre>
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
Con qué comando se muestran las traducciones NAT?	<pre>R2#sh ip nat translations Pro Inside global   Inside local   Outside local Outside global --- 209.165.200.229 10.10.10.10   ---  R2#</pre>
Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

## 5.2. Escenario 2

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

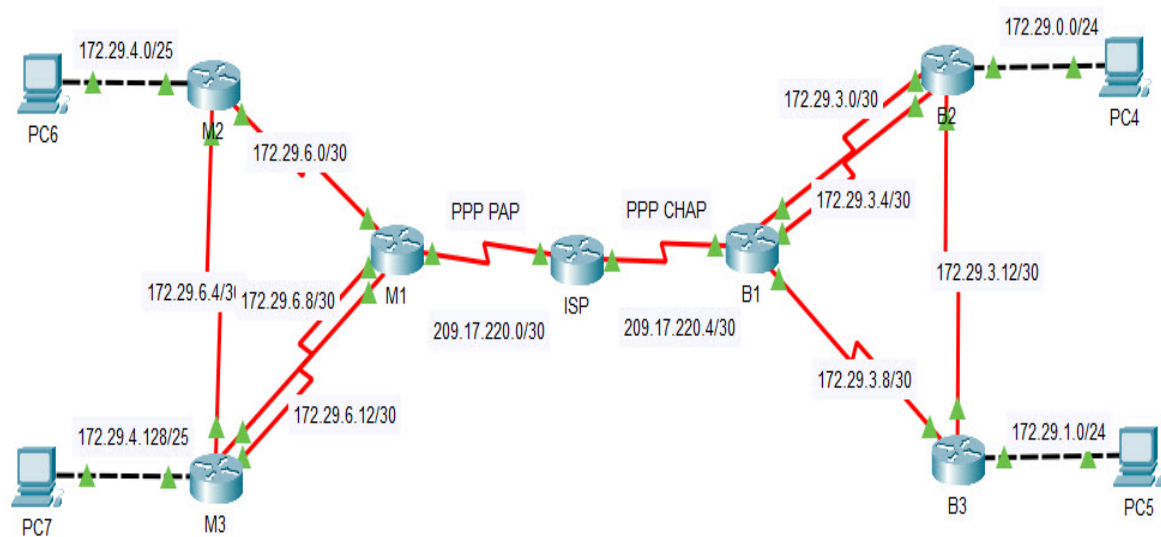


Figura 19: Escenario 2

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

Los routers Bogotá2 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 Bogotá1 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).

Configuración Router Bogota 1

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

```
Router(config)#hostname B1
```

```
B1(config)#enable secret class
```

```
B1(config)#line console 0
```

```
B1(config-line)#password cisco
```

```
B1(config-line)#login
```

```
B1(config-line)#line vty 0 4
```

```
B1(config-line)#password cisco
```

```
B1(config-line)#login
```

```
B1(config)#service password-encryption
```

```
B1(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO#
```

Configuración Router Bogota 2

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

```
Router(config)#hostname B2
```

```
B2(config)#enable secret class
```

```
B2(config)#line console 0
```

```
B2(config-line)#password cisco
```

```
B2(config-line)#login
```

```
B2(config-line)#line vty 0 4
```

```
B2(config-line)#password cisco
B2(config-line)#login
B2(config)#service password-encryption
B2(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO #
```

### Configuración Router Bogota 3

```
Router(config)#no ip domain-lookup
Router(config)#hostname B3
B3(config)#enable secret class
B3(config)#line console 0
B3(config-line)#password cisco
B3(config-line)#login
B3(config-line)#line vty 0 4
B3(config-line)#password cisco
B3(config-line)#login
B3(config)#service password-encryption
B3(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO #
```

### Configuración Router Medellin 1

```
Router(config)#no ip domain-lookup
Router(config)#hostname M1
M1(config)#enable secret class
M1(config)#line console 0
M1(config-line)#password cisco
M1(config-line)#login
M1(config-line)#line vty 0 4
M1(config-line)#password cisco
M1(config-line)#login
```

```
M1(config)#service password-encryption
M1(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO#

Configuración Router Medellin 2
Router(config)#no ip domain-lookup
Router(config)#hostname M2
M2(config)#enable secret class
M2(config)#line console 0
M2(config-line)#password cisco
M2(config-line)#login
M2(config-line)#line vty 0 4
M2(config-line)#password cisco
M2(config-line)#login
M2(config)#service password-encryption
M2(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO#

Configuración Router Medellin 3
Router(config)#no ip domain-lookup
Router(config)#hostname M3
M3(config)#enable secret class
M3(config)#line console 0
M3(config-line)#password cisco
M3(config-line)#login
M3(config-line)#line vty 0 4
M3(config-line)#password cisco
M3(config-line)#login
M3(config)#service password-encryption
M3(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO #
```

## Configuración Router ISP

```
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config)#service password-encryption
ISP(config)#banner motd #SE PROHIBE EL INGRESO NO AUTORIZADO #
```

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

## Configuración de direcciones IP.

### Router B1.

#### Conexión con Router B2 Uno

```
B1(config)#interface serial 0/0/1
B1(config-if)#description Conexion B1-B2 Uno
B1(config-if)#ip address 172.29.3.1 255.255.255.252
B1(config-if)#no shutdown
```

#### Conexión con Router B2 Dos

```
B1(config)#interface serial 0/1/0
B1(config-if)#description Conexion B1-B2 Dos
B1(config-if)#ip address 172.29.3.5 255.255.255.252
B1(config-if)#no shutdown
```

Conexión con Router B3

```
B1(config)#interface serial 0/1/1
```

```
B1(config-if)#description Conexion B1-B3
```

```
B1(config-if)#ip address 172.29.3.9 255.255.255.252
```

```
B1(config-if)#no shutdown
```

Conexión con Router ISP

```
B1(config)#interface serial 0/0/0
```

```
B1(config-if)#description Conexion B1-ISP
```

```
B1(config-if)#ip address 209.17.220.6 255.255.255.252
```

```
B1(config-if)#no shutdown
```

Router B2.

Conexión con Router B1 Uno

```
B2(config)#interface serial 0/0/0
```

```
B2(config-if)#description Conexion B2-B1 Uno
```

```
B2(config-if)#ip address 172.29.3.2 255.255.255.252
```

```
B2(config-if)#no shutdown
```

Conexión con Router B1 Dos

```
B2(config)#interface serial 0/0/1
```

```
B2(config-if)#description Conexion B2-B1 Dos
```

```
B2(config-if)#ip address 172.29.3.6 255.255.255.252
```

```
B2(config-if)#no shutdown
```

Conexión con Router B3

```
B2(config)#interface serial 0/1/0
```

```
B2(config-if)#description Conexion B2-B3
```

```
B2(config-if)#ip address 172.29.3.13 255.255.255.252
```

B2(config-if)#no shutdown

Router B3.

Conexión con Router B2

B3(config)#interface serial 0/0/1

B3(config-if)#description Conexion B3-B2

B3(config-if)#ip address 172.29.3.14 255.255.255.252

B3(config-if)#no shutdown

Conexion con Router B1

B3(config)#interface serial 0/0/0

B3(config-if)#description Conexion B3-B1

B3(config-if)#ip address 172.29.3.10 255.255.255.252

B3(config-if)#no shutdown

Router ISP.

Conexión con Router B1

ISP(config)#interface serial 0/0/1

ISP(config-if)#description Conexion ISP-B1

ISP(config-if)#ip address 209.17.220.5 255.255.255.252

ISP(config-if)#no shutdown

Conexion con Router M1

ISP(config)#interface serial 0/0/0

ISP(config-if)#description Conexion ISP-M1

ISP(config-if)#ip address 209.17.220.1 255.255.255.252

ISP(config-if)#no shutdown



Router M1.

Conexion con Router ISP

```
M1(config)#interface serial 0/0/0
```

```
M1(config-if)#description Conexion M1-ISP
```

```
M1(config-if)#ip address 209.17.220.2 255.255.255.252
```

```
M1(config-if)#no shutdown
```

Conexion con Router M2

```
M1(config)#interface serial 0/1/1
```

```
M1(config-if)#description Conexion M1-M2
```

```
M1(config-if)#ip address 172.29.6.1 255.255.255.252
```

```
M1(config-if)#no shutdown
```

Conexion con Router M3 Uno

```
M1(config)#interface serial 0/0/1
```

```
M1(config-if)#description Conexion M1-M3 Uno
```

```
M1(config-if)#ip address 172.29.6.9 255.255.255.252
```

```
M1(config-if)#no shutdown
```

Conexion con Router M3 Dos

```
M1(config)#interface serial 0/1/0
```

```
M1(config-if)#description Conexion M1-M3 Dos
```

```
M1(config-if)#ip address 172.29.6.13 255.255.255.252
```

```
M1(config-if)#no shutdown
```

Router M2.

Conexion con Router M1

```
M2(config)#interface serial 0/0/0
```

```
M2(config-if)#description Conexion M2-M1
```

```
M2(config-if)#ip address 172.29.6.2 255.255.255.252
```

```
M2(config-if)#no shutdown
```

Conexion con Router M3

```
M2(config)#interface serial 0/0/1
```

```
M2(config-if)#description Conexion M2-M3
```

```
M2(config-if)#ip address 172.29.6.5 255.255.255.252
```

```
M2(config-if)#no shutdown
```

Router M3.

Conexion con Router M1 Uno

```
M3(config)#interface serial 0/0/0
```

```
M3(config-if)#description Conexion M3-M1 Uno
```

```
M3(config-if)#ip address 172.29.6.10 255.255.255.252
```

```
M3(config-if)#no shutdown
```

Conexion con Router M1 Dos

```
M3(config)#interface serial 0/0/1
```

```
M3(config-if)#description Conexion M3-M1 Dos
```

```
M3(config-if)#ip address 172.29.6.14 255.255.255.252
```

```
M3(config-if)#no shutdown
```

Conexion con Router M2

```
M3(config)#interface serial 0/1/0
```

```
M3(config-if)#description Conexion M3-M2
```

```
M3(config-if)#ip address 172.29.6.6 255.255.255.252
```

```
M3(config-if)#no shutdown
```

Redes LAN.

Conexion con LAN B2

```
B2(config)#interface FastEthernet0/0
```

```
B2(config-if)#description Conexion LAN B2
```

```
B2(config-if)#ip address 172.29.0.1 255.255.255.0
```

```
B2(config-if)#no shutdown
```

Conexion con LAN B3

```
B3(config)#interface FastEthernet0/0
```

```
B3(config-if)#description Conexion LAN B3
```

```
B3(config-if)#ip address 172.29.1.1 255.255.255.0
```

```
B3(config-if)#no shutdown
```

Conexion con LAN M2

```
M2(config)#interface FastEthernet0/0
```

```
M2(config-if)#description Conexion LAN M2
```

```
M2(config-if)#ip address 172.29.4.1 255.255.255.128
```

```
M2(config-if)#no shutdown
```

Conexion con LAN M3

```
M3(config)#interface FastEthernet0/0
```

```
M3(config-if)#description Conexion LAN M3
```

```
M3(config-if)#ip address 172.29.4.129 255.255.255.128
```

```
M3(config-if)#no shutdown
```

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

### 5.2.1. Parte 1: Configuración del enrutamiento.

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

Router B1.

```
B1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

```
B1(config)#router ospf 10
```

```
B1(config-router)#network 209.17.220.4 0.0.0.3 area 1
```

```
B1(config-router)#network 172.29.3.8 0.0.0.3 area 1
```

```
B1(config-router)#network 172.29.3.4 0.0.0.3 area 1
```

```
B1(config-router)#network 172.29.3.0 0.0.0.3 area 1
```

```
B1(config-router)#default-information originate
```

Router B2

```
B2(config)#router ospf 10
```

```
B2(config-router)#network 172.29.0.0 0.0.0.255 area 1
```

```
B2(config-router)#network 172.29.3.0 0.0.0.3 area 1
```

```
B2(config-router)#network 172.29.3.4 0.0.0.3 area 1
```

```
B2(config-router)#network 172.29.3.12 0.0.0.3 area 1
```

```
B2(config-router)#passive-interface fastEthernet 0/0
```

Router B3

```
B3(config)#router ospf 10
```

```
B3(config-router)#network 172.29.1.0 0.0.0.255 area 1
```

```
B3(config-router)#network 172.29.3.8 0.0.0.3 area 1
```

```
B3(config-router)#network 172.29.3.12 0.0.0.3 area 1
```

```
B3(config-router)#passive-interface fastEthernet 0/0
```

Router M1.

```
M1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

```
M1(config)#router ospf 20
M1(config-router)#network 209.17.220.0 0.0.0.3 area 0
M1(config-router)#network 172.29.6.0 0.0.0.3 area 0
M1(config-router)#network 172.29.6.8 0.0.0.3 area 0
M1(config-router)#network 172.29.6.12 0.0.0.3 area 0
M1(config-router)#default-information originate
```

Router M2.

```
M2(config)#router ospf 20
M2(config-router)#network 172.29.6.0 0.0.0.3 area 0
M2(config-router)#network 172.29.6.4 0.0.0.3 area 0
M2(config-router)#network 172.29.4.0 0.0.0.127 area 0
M2(config-router)#passive-interface fastEthernet 0/0
```

Router M3.

```
M3(config)#router ospf 20
M3(config-router)#network 172.29.6.4 0.0.0.3 area 0
M3(config-router)#network 172.29.6.9 0.0.0.3 area 0
M3(config-router)#network 172.29.6.12 0.0.0.3 area 0
M3(config-router)#network 172.29.4.128 0.0.0.127 area 0
M3(config-router)#passive-interface fastEthernet 0/0
```

- 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 OSPF.

```
B1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

```
M1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

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

Sumarización de redes:

Tabla 24: Sumarización red Bogota

Decimal	Binario
172.29.0.0	<b>10101100 00011101 00000000 00000000</b>
172.29.1.0	<b>10101100 00011101 00000001 00000000</b>
172.29.3.0	<b>10101100 00011101 00000011 00000000</b>
172.29.3.4	<b>10101100 00011101 00000011 00000100</b>
172.29.3.8	<b>10101100 00011101 00000011 00001000</b>
172.29.3.12	<b>10101100 00011101 00000000 00001100</b>

Nueva red 172.29.0.0 255.255.252.0

ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

Tabla 25: Sumarización red Medellin

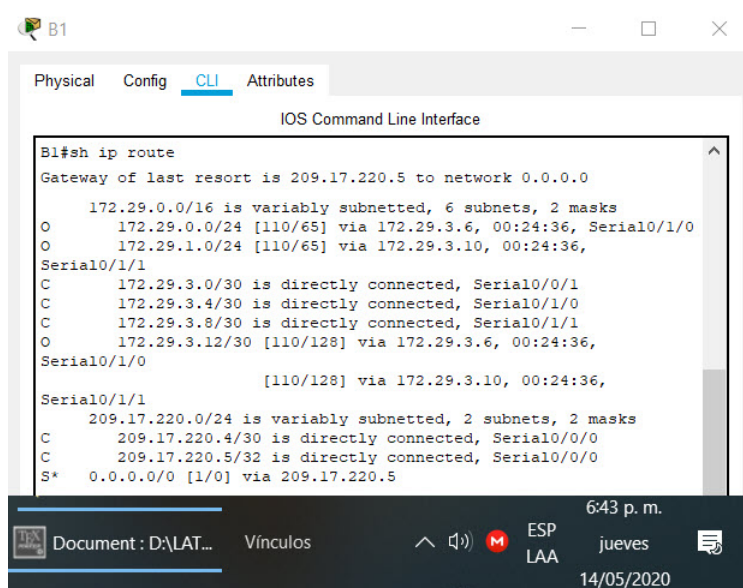
Decimal	Binario
172.29.4.0	<b>10101100 00011101 00000100 00000000</b>
172.29.4.128	<b>10101100 00011101 00000100 10000000</b>
172.29.6.0	<b>10101100 00011101 00000110 00000000</b>
172.29.6.4	<b>10101100 00011101 00000110 00000100</b>
172.29.6.8	<b>10101100 00011101 00000110 00001000</b>
172.29.6.12	<b>10101100 00011101 00000110 00001100</b>

Nueva red 172.29.4.0 255.255.252.0

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2

## 5.2.2. Parte 2: Tabla de Enrutamiento.

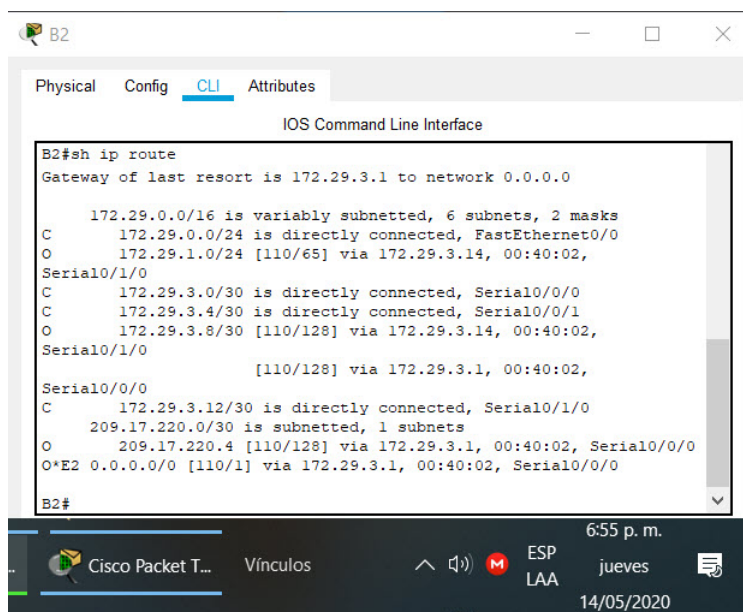
- a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.



```
B1#sh ip route
Gateway of last resort is 209.17.220.5 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.29.0.0/24 [110/65] via 172.29.3.6, 00:24:36, Serial0/1/0
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:24:36,
Serial0/1/1
C       172.29.3.0/30 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/0
C       172.29.3.8/30 is directly connected, Serial0/1/1
O       172.29.3.12/30 [110/128] via 172.29.3.6, 00:24:36,
Serial0/1/0
                                                [110/128] via 172.29.3.10, 00:24:36,
Serial0/1/1
C       209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
C       209.17.220.5/32 is directly connected, Serial0/0/0
S*    0.0.0.0/0 [1/0] via 209.17.220.5
```

Figura 20: Tabla de enrutamiento B1



```
B2#sh ip route
Gateway of last resort is 172.29.3.1 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.29.0.0/24 is directly connected, FastEthernet0/0
O       172.29.1.0/24 [110/65] via 172.29.3.14, 00:40:02,
Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/0/1
O       172.29.3.8/30 [110/128] via 172.29.3.14, 00:40:02,
Serial0/1/0
                                                [110/128] via 172.29.3.1, 00:40:02,
Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/1/0
C       209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.4 [110/128] via 172.29.3.1, 00:40:02, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:40:02, Serial0/0/0
B2#
```

Figura 21: Tabla de enrutamiento B2

```

M1#sh ip route
Gateway of last resort is 209.17.220.1 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 00:45:53, Serial0/1/1
O       172.29.4.128/25 [110/65] via 172.29.6.14, 00:45:53,
Serial0/1/0
C       172.29.6.0/30 is directly connected, Serial0/1/1
O       172.29.6.4/30 [110/128] via 172.29.6.14, 00:45:53,
Serial0/1/0
                [110/128] via 172.29.6.2, 00:45:53,
Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/0/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
O       209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
C       209.17.220.1/32 is directly connected, Serial0/0/0
S*    0.0.0.0/0 [1/0] via 209.17.220.1
--More--

```

Figura 22: Tabla de enrutamiento M1

```

M2#sh ip route
    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.29.4.0/25 is directly connected, FastEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 00:00:32,
Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
O       172.29.6.8/30 [110/128] via 172.29.6.6, 00:00:22, Serial0/0/1
                [110/128] via 172.29.6.1, 00:00:22, Serial0/0/0
O       172.29.6.12/30 [110/128] via 172.29.6.6, 00:00:22,
Serial0/0/1
                [110/128] via 172.29.6.1, 00:00:22,
Serial0/0/1
O       209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.0 [110/128] via 172.29.6.1, 00:00:22, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:00:22, Serial0/0/0
M2#

```

Figura 23: Tabla de enrutamiento M2



```

M3#sh ip route
Gateway of last resort is 172.29.6.13 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.29.4.0/25 [110/65] via 172.29.6.5, 00:50:59, Serial0/1/0
C       172.29.4.128/25 is directly connected, FastEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.5, 00:50:49,
Serial0/1/0
                [110/128] via 172.29.6.13, 00:50:49,
Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/1/0
C       172.29.6.8/30 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/0/1
O       209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.0 [110/128] via 172.29.6.13, 00:50:49,
Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:50:49, Serial0/0/1
M3#

```

Figura 24: Tabla de enrutamiento M3

- 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 OSPF.
- 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.

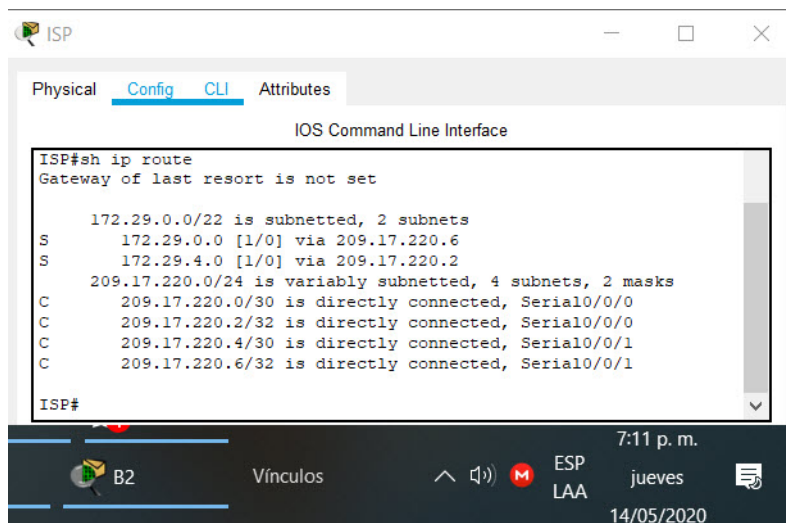


Figura 25: Tabla de enrutamiento ISP

### 5.2.3. Parte 3: Deshabilitar la propagación del protocolo OSPF.

- a. 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.

B2(config-router)#passive-interface fastEthernet 0/0

B3(config-router)#passive-interface fastEthernet 0/0

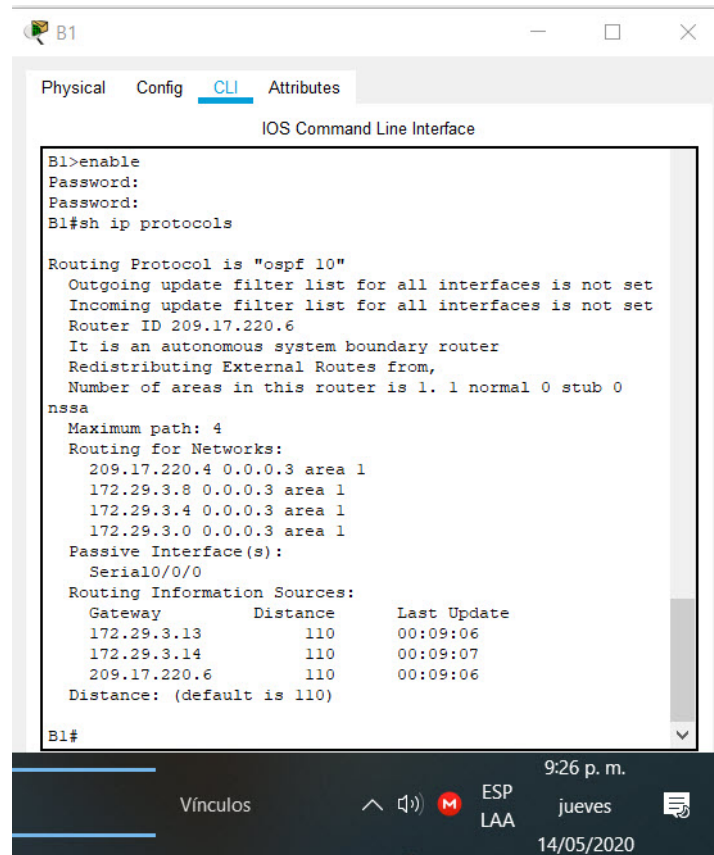
M2(config-router)#passive-interface fastEthernet 0/0

M3(config-router)#passive-interface fastEthernet 0/0

### 5.2.4. Parte 4: Verificación del protocolo OSPF.

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

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

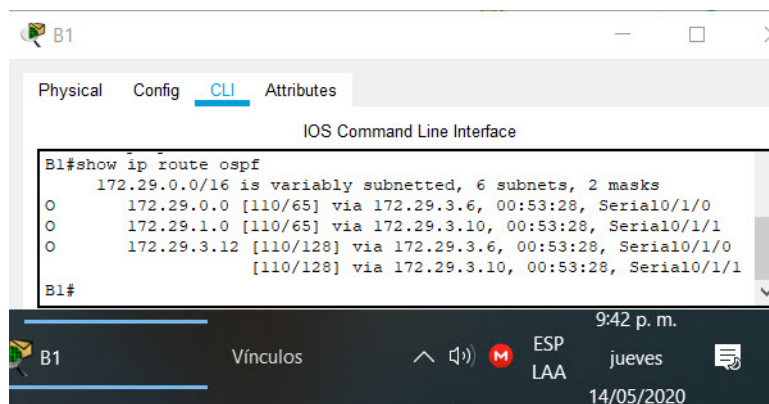


```
B1>enable
Password:
Password:
B1#sh ip protocols

Routing Protocol is "ospf 10"
  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,
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.0 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:09:06
    172.29.3.14      110          00:09:07
    209.17.220.6     110          00:09:06
  Distance: (default is 110)

B1#
```

Figura 26: Comando sh ip protocols B1



```
B1#show ip route ospf
 172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       172.29.0.0 [110/65] via 172.29.3.6, 00:53:28, Serial0/1/0
O       172.29.1.0 [110/65] via 172.29.3.10, 00:53:28, Serial0/1/1
O       172.29.3.12 [110/128] via 172.29.3.6, 00:53:28, Serial0/1/0
        [110/128] via 172.29.3.10, 00:53:28, Serial0/1/1

B1#
```

Figura 27: Comando sh ip route ospf B1

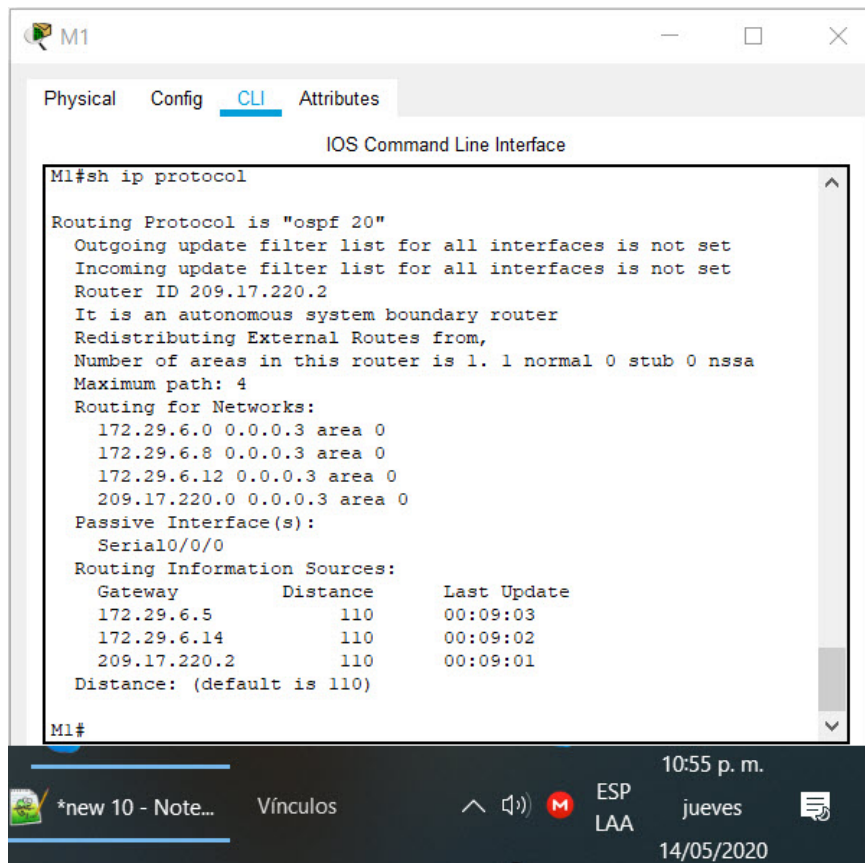


Figura 28: Comando sh ip protocol M1

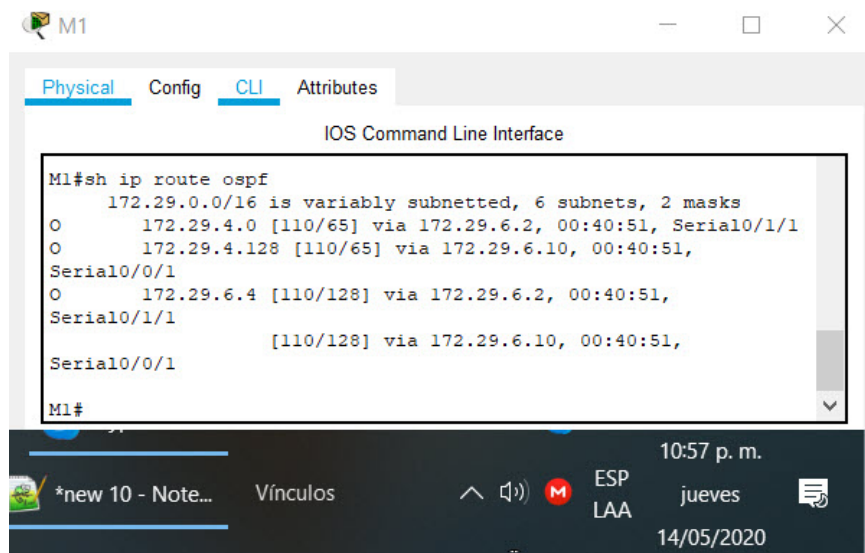


Figura 29: Comando sh ip route ospf M1

### 5.2.5. Configurar encapsulamiento y autenticación PPP.

- a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

```
ISP(config)#int s0/0/0
```

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

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

```
ISP(config-if)#ppp pap sent-username M1 password cisco
```

- b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

```
ISP(config)#int s0/0/1
```

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

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

```
ISP(config-if)#ppp pap sent-username M1 password cisco
```

### 5.2.6. Parte 6: Configuración de NAT.

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

- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

```
M1(config)#access-list 20 permit 172.29.4.0 0.0.3.255
```

```
M1(config)#ip nat inside source list 20 interface serial 0/0/0 overload
```

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

```
B1(config)#access-list 20 permit 172.29.0.0 0.0.3.255
```

```
B1(config)#ip nat inside source list 20 interface serial 0/0/0 overload
```

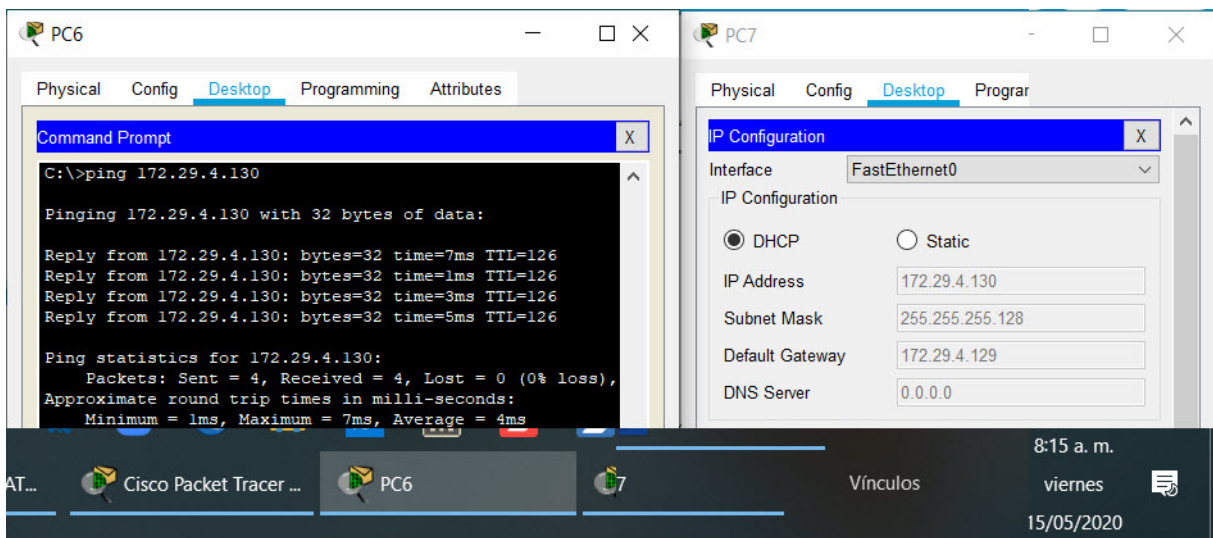


Figura 30: Ping entre redes LAN M2-M3

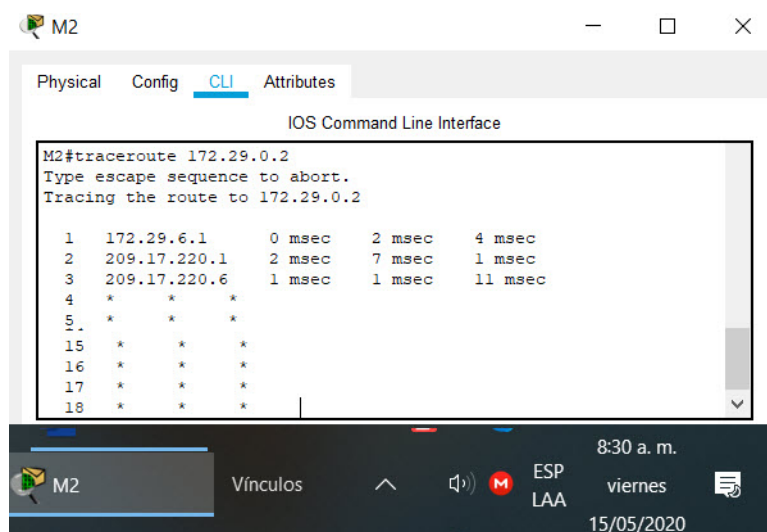


Figura 31: Comando traceroute desde M2 hasta LAN B2

### 5.2.7. Parte 7: Configuración del servicio DHCP.

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

```
M2(config)#ip dhcp excluded-address 172.29.4.1
M2(config)#ip dhcp excluded-address 172.29.4.129
M2(config)#ip dhcp pool M2
M2(dhcp-config)#network 172.29.4.0 255.255.255.128
M2(dhcp-config)#default-router 172.29.4.1
M2(config)#ip dhcp pool M3
M2(dhcp-config)#network 172.29.4.128 255.255.255.128
M2(dhcp-config)#default-router 172.29.4.129
```

- b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2. M3(config)#interface fa0/0

```
M3(config-if)#ip ip helper-address 172.29.6.5
```

- c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota 2 debe ser el servidor DHCP para ambas redes Lan.

```
B2(config)#ip dhcp excluded-address 172.29.0.1
B2(config)#ip dhcp excluded-address 172.29.1.1
B2(config)#ip dhcp pool B2
B2(dhcp-config)#network 172.29.0.0 255.255.255.0
B2(dhcp-config)#default-router 172.29.0.1
B2(config)#ip dhcp pool B3
B2(dhcp-config)#network 172.29.1.0 255.255.255.0
B2(dhcp-config)#default-router 172.29.1.1
```

- d. Configure el router Bogotá 3 para que habilite el paso de los mensajes Broadcast

hacia la IP del router Bogotá 2.

```
B3(config)#interface fa0/0
```

```
B3(config-if)#ip ip helper-address 172.29.3.13
```



## 6. Conclusiones

En la practica el software packet tracert no soporta todos los comando que pueden soportar los equipos de la linea CISCO en un laboratorio fisico, caso puntual los comandos de configuración de http.

En RIPv2 se puede aplicar la desactivación de la sumarización automática, en OSPF no es posible.

RIPv2 solo se puede trabajar con direcciones IP versión 4, para trabajar con direcciones IP versión 6 se puede hacer uso de RIP de última generación (RIPng).

Las interfaces loopback no están relacionadas con una interfaz física de un router, nunca se pueden conectar a un dispositivo, es una interfaz interna logica interna que dada su disponibilidad se utiliza para pruebas y administración.

La sumarización permite abreviar diversas direcciones IP adyacentes en una sola ruta, generando entre otros beneficios la disminución de la complejidad de las tablas de enrutamiento y de los requerimientos de la memoria RAM y de procesamiento.

El protocolo RIP tiene limitación en el control de redes grandes, pero a su favor tiene la facilidad y sencillez en su configuración.

El protocolo OSPF puede manejar grandes redes hallando la mejor ruta o el camino más corto.

## 7. Bibliografía

CISCO. Configuración de ejemplo para la autenticación en RIPv2. (2020, Enero 17). [Consultado: 02 de mayo de 2020]. Disponible en [https://www.cisco.com/c/es\\_mx/support/docs/ip/routing-information-protocol-rip/13719-50.html](https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13719-50.html)

CISCO. Configuración de ejemplo para la autenticación en OSPF. (2019, Junio 5). [Consultado: 06 de mayo de 2020]. Disponible en [https://www.cisco.com/c/es\\_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html](https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html)

CISCO. Ejemplo de configuración usando el comando ip nat outside source static. (2020, Enero 9). [Consultado: 06 de mayo de 2020]. Disponible en [https://www.cisco.com/c/es\\_mx/support/docs/ip/network-address-translation-nat/13773-2.html](https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/13773-2.html)

Implementaciones de VLAN. (s.f.). [Consultado: 05 de mayo de 2020]. Disponible en <https://www.itesa.edu.mx/netacad/switching/course/module3/3.2.2.1/3.2.2.1.html>

Ariganello, E., & Sevilla, E. B. (2015). Redes Cisco: guía de estudio para la certificación Ccnp. Paracuellos de Jarama (Madrid): Ra-Ma. ISBN: 9788499644462.