

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

JAQUELINA ARDILA SEDANO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
MAYO DE 2020**

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

**PRESENTADO POR
JAQUELINA ARDILA SEDANO**

**PRUEBA DE HABILIDADES PRÁCTICAS CCNA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)**

**PRESENTADO A
TUTOR
JOSE IGNACIO CARDONA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
MAYO DE 2020**

TABLA DE CONTENIDO

INTRODUCCIÓN	3
DESARROLLO DE LOS DOS ESCENARIOS	4
ESCENARIO 1	4
Parte 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS	5
Parte 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN	17
Parte 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2	23
Parte 5: IMPLEMENTAR DHCP Y NAT PARA IPV4.....	27
Parte 6: CONFIGURAR NTP	33
Parte 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)	34
ESCENARIO 2	38
Parte 1: CONFIGURACIÓN DEL ENRUTAMIENTO.....	45
Parte 2: TABLA DE ENRUTAMIENTO.....	48
Parte 3: Deshabilitar la propagación del protocolo OSPF	55
Bogota1(config)#router ospf 1.....	56
Bogota1(config-router)#passive-interface serial 0/0/1	56
Bogota1(config-router)#passive-interface serial 0/1/1	56
Bogota1(config-router)#passive-interface serial 0/1/0.....	56
Parte 4: VERIFICACIÓN DEL PROTOCOLO OSPF.....	57
a. Se verifican y documentan 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.	57
Parte 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.	62
Parte 6: CONFIGURACIÓN DE PAT.	63
Parte 7: CONFIGURACIÓN DEL SERVICIO DHCP.	65
CONCLUSIONES	67
REFERENCIAS BIBLIOGRÁFICAS.....	68

LISTA DE FIGURAS

Ilustración 1. Topología Esc 1	4
Ilustración 2-Ping R1	15
Ilustración 3-Ping R2.....	16
Ilustración 4-Ping web server	16
Ilustración 5-Ping S1	22
Ilustración 6-Ping S3.....	22
Ilustración 7-Do show ip router connected R1.....	24
Ilustración 8-Configuración de RIP v2 en R2	24
Ilustración 9-Do show ip router connected R2.....	25
Ilustración 10-Show ip protocols	26
Ilustración 11-PC-A _DHCP	30
Ilustración 12-PC-C _DHCP.....	31
Ilustración 13-Ping PC-A a PC-C	31
Ilustración 14-Navegador web -servidor web	32
Ilustración 15-Ping de ip server.....	32
Ilustración 16-Lista de acceso CLI	35
Ilustración 17-Ping de PC-A 209.165.200.238	37
Ilustración 18-Ping PC-C 209.165.200.238	37
Ilustración 19-Navegador web.....	38
Ilustración 20-Topología de red.....	39
Ilustración 21-Conexión física de los equipos con base en la topología de red	40
Ilustración 22-Propagación del protocolo OSPF deshabilitado.....	57

LISTA DE TABLAS

Tabla 1- inicializar y cargar routers y switches.....	5
Tabla 2-Configuración de computadora de Internet.....	5
Tabla 3-configuración R1.....	6
Tabla 4-configuración R2.....	8
Tabla 5-configuración R3.....	11
Tabla 6-configuración S1.....	13
Tabla 7-configuración S3.....	14
Tabla 8-Verificar la conectividad de red.....	15
Tabla 9 -Configuración de seguridad de S1.....	17
Tabla 10-Configuración de seguridad de S3.....	19
Tabla 11-Configuración de seguridad de R1.....	20
Tabla 12-de verificación de conectividad de los dispositivos de red.....	21
Tabla 13-Configuración protocolo RIPV2 R1.....	23
Tabla 14-Elemento o tarea de configuración Especificación.....	25
Tabla 15-Comandos RIP.....	27
Tabla 16-Configuración DHCP Y NAT.....	27
Tabla 17-Configuración NAT estática y dinámica en el R2.....	28
Tabla 18-Ping verificación del protocolo DHCP y la NAT estática.....	30
Tabla 19-de configuración NTP.....	33
Tabla 20-Configuración y verificación ACL.....	34
Tabla 21-Comandos De CLI.....	35
Tabla 22-Interfaces de router que no necesitan desactivación. Protocolo OSPF	55

INTRODUCCIÓN

Con el desarrollo de la prueba de habilidades prácticas se espera identificar las habilidades y competencia de habilidades adquiridas por el estudiante a lo largo del diplomado poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para llevar a cabo esta prueba se trabajará en dos escenarios los cuales incluirán implementar configuración de Switches y Routers, enrutamiento entre Vlan, enrutamiento dinámico DHCP, NAT, Autenticación PAT, protocolo OSPF V2, para dar solución de problemas de conectividad y mejorar la seguridad de las redes, entre otras actividades que permitirán experimentar con la topología y analizar el comportamiento de las redes en los escenarios propuestos en la actividad.

DESARROLLO DE LOS DOS ESCENARIOS

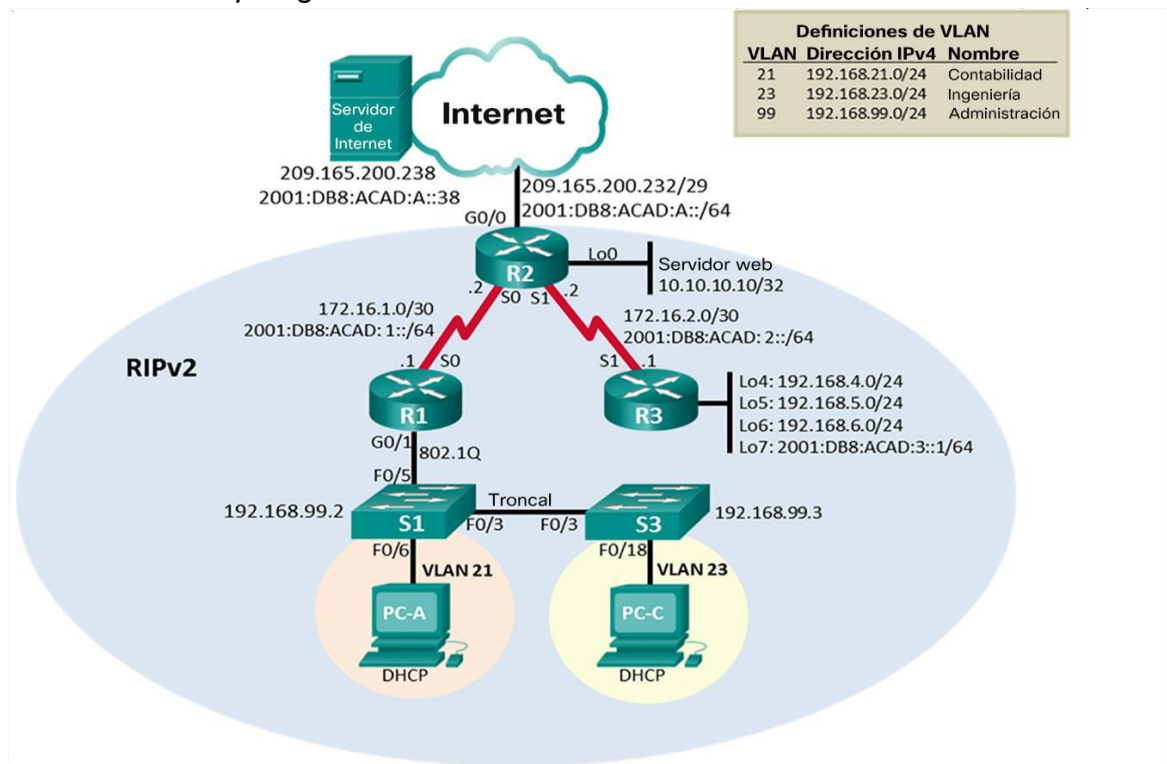
ESCENARIO 1

Descripción del escenario:

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.

Topología:

Ilustración 1. Topología Esc 1



Parte1: INICIALIZAR DISPOSITIVOS

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

Se eliminan las configuraciones de inicio y se vuelven a cargar los dispositivos.

Tabla 1- inicializar y cargar routers y switches

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

Parte 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 2: Configurar la computadora de Internet

Se realizan las tareas de configuración del servidor de Internet que incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 2-Configuración de computadora de Internet

Elemento o tarea de configuración	Especificación
<i>Dirección IPv4</i>	<i>209.165.200.238</i>
<i>Máscara de subred para IPv4</i>	<i>255.255.255.248</i>
<i>Gateway predeterminado</i>	<i>209.165.200.233</i>

<i>Dirección IPv6/subred</i>	<i>2001:DB8:ACAD:A::38/64</i>
<i>Gateway predeterminado IPv6</i>	<i>2001:DB8:ACAD:A::1 k</i>

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.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes tareas:

Tabla 3-configuración R1

Elemento o tarea de configuración	Especificación
<i>Desactivar la búsqueda DNS</i>	
<i>Nombre del router</i>	<i>R1</i>
<i>Contraseña de exec privilegiado cifrada</i>	<i>Class</i>
<i>Contraseña de acceso a la consola</i>	<i>Cisco</i>
<i>Contraseña de acceso Telnet</i>	<i>Cisco</i>
<i>Cifrar las contraseñas de texto no cifrado</i>	
<i>Mensaje MOTD</i>	<i>Se prohíbe el acceso no autorizado.</i>
<i>Interfaz S0/0/0</i>	<i>Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz</i>
<i>Rutas predeterminadas</i>	<i>Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0</i>

Nota: Todavía no configure G0/1.

R1:

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

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

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

```
R1(config)#line console 0
```

```
R1(config-line)#password cisco
```

```
R1(config-line)#login
```

```
R1(config-line)#line vty 0 15
```

```
R1(config-line)#password cisco
```

```
R1(config-line)#login
```

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

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

```
R1(config)#banner motd $Unauthorized Access is Prohibited!$
```

```
R1(config)#int s0/0/0
```

```
R1(config-if)#description connection R2
```

```
R1(config-if)#ip address 172.16.1.1 255.255.255.252
```

```
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
```

```
R1(config-if)#clock rate 128000
```

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

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

Paso 4: CONFIGURAR R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4-configuración R2

Elemento o tarea de configuración	Especificación
<i>Desactivar la búsqueda DNS</i>	
<i>Nombre del router</i>	<i>R2</i>
<i>Contraseña de exec privilegiado cifrada</i>	<i>class</i>
<i>Contraseña de acceso a la consola</i>	<i>cisco</i>
<i>Contraseña de acceso Telnet</i>	<i>cisco</i>
<i>Cifrar las contraseñas de texto no cifrado</i>	
<i>Habilitar el servidor HTTP</i>	
<i>Mensaje MOTD</i>	<i>Se prohíbe el acceso no autorizado.</i>
<i>Interfaz S0/0/0</i>	<i>Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</i>
<i>Interfaz S0/0/1</i>	<i>Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz</i>

<i>Interfaz G0/0 (simulación de Internet)</i>	<i>Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz</i>
<i>Interfaz loopback 0 (servidor web simulado)</i>	<i>Establecer la descripción. Establezca la dirección IPv4.</i>
<i>Ruta predeterminada</i>	<i>Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.</i>

R2:

```

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#ip http server

```

^

% Invalid input detected at '^' marker.

```

R2(config)#banner motd $Unauthorized Access is Prohibited!$
R2(config)#int s0/0/0
R2(config-if)#description connection R1

```

```
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#int s0/0/1
R2(config-if)#description connection 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 shut
R2(config-if)#no shutdown
R2(config-if)#int g0/0
R2(config-if)#description connection to internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdow
R2(config-if)#int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description connection to simulated web server
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 g0/0
```

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5-configuración R3

Elemento o tarea de configuración	Especificación
<i>Desactivar la búsqueda DNS</i>	
<i>Nombre del router</i>	<i>R3</i>
<i>Contraseña de exec privilegiado cifrada</i>	<i>class</i>
<i>Contraseña de acceso a la consola</i>	<i>cisco</i>
<i>Contraseña de acceso Telnet</i>	<i>cisco</i>
<i>Cifrar las contraseñas de texto no cifrado</i>	
<i>Mensaje MOTD</i>	<i>Se prohíbe el acceso no autorizado.</i>
<i>Interfaz S0/0/1</i>	<i>Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</i>
<i>Interfaz loopback 4</i>	<i>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</i>
<i>Interfaz loopback 5</i>	<i>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</i>
<i>Interfaz loopback 6</i>	<i>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</i>
<i>Interfaz loopback 7</i>	<i>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</i>
<i>Rutas predeterminadas</i>	

R3:

```
Router>enable
Router#conf
Router#configure t
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized Access is Prohibited!$
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown
R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#ip address 2001:DB8:ACAD:3::1/64
```

```

R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#exit

```

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6-configuración S1

Elemento o tarea de configuración	Especificación
<i>Desactivar la búsqueda DNS</i>	
<i>Nombre del switch</i>	<i>S1</i>
<i>Contraseña de exec privilegiado cifrada</i>	<i>class</i>
<i>Contraseña de acceso a la consola</i>	<i>cisco</i>
<i>Contraseña de acceso Telnet</i>	<i>cisco</i>
<i>Cifrar las contraseñas de texto no cifrado</i>	
<i>Mensaje MOTD</i>	<i>Se prohíbe el acceso no autorizado.</i>

S1:

```

S1(config)#
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15

```

S1(config-line)#password cisco
 S1(config-line)#login
 S1(config-line)#exit
 S1(config)#service password-encryption
 S1(config)#banner motd \$Unauthorized Access is Prohibited!\$

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7-configuración S3

Elemento o tarea de configuración	Especificación
<i>Desactivar la búsqueda DNS</i>	
<i>Nombre del switch</i>	S3
<i>Contraseña de exec privilegiado cifrada</i>	class
<i>Contraseña de acceso a la consola</i>	cisco
<i>Contraseña de acceso Telnet</i>	cisco
<i>Cifrar las contraseñas de texto no cifrado</i>	
<i>Mensaje MOTD</i>	<i>Se prohíbe el acceso no autorizado.</i>

S3:

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 15
 S3(config-line)#password cisco
 S3(config-line)#login
 S3(config-line)#exit

S3(config)#service password-encryption

S3(config)#banner motd \$Unauthorized Access is Prohibited!\$

Paso 8: Verificar la conectividad de la red

Se utiliza el comando **ping** para probar la conectividad entre los dispositivos de red.

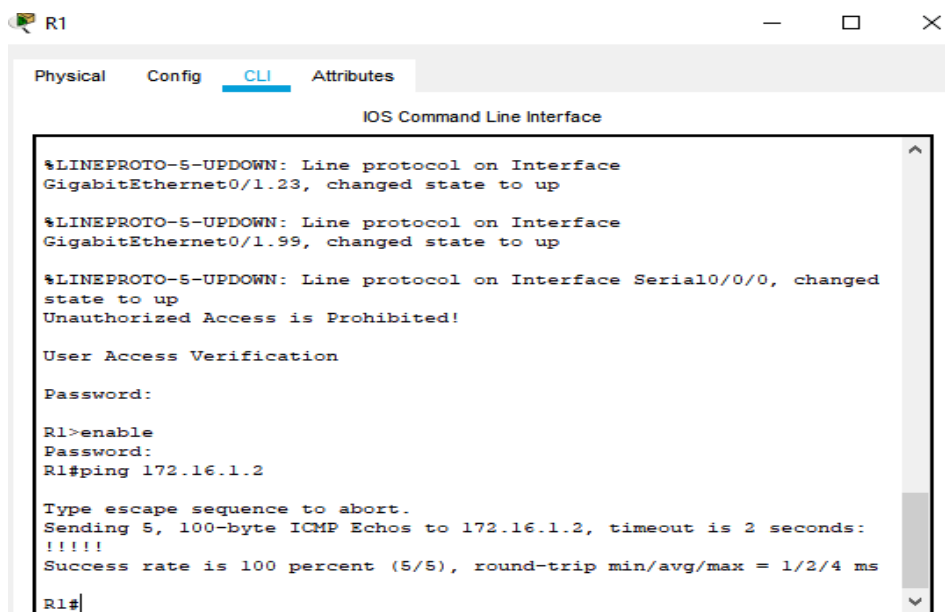
La siguiente tabla se usa para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 8-Verificar la conectividad de red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5)
R2	R3, S0/0/1	172.16.2.1	Success rate is 100 percent (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233	Ping statistics for 209.165.200.233

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Ilustración 2-Ping R1



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
Unauthorized Access is Prohibited!

User Access Verification

Password:

R1>enable
Password:
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 = 1/2/4 ms

R1#
```

Ilustración 3-Ping R2

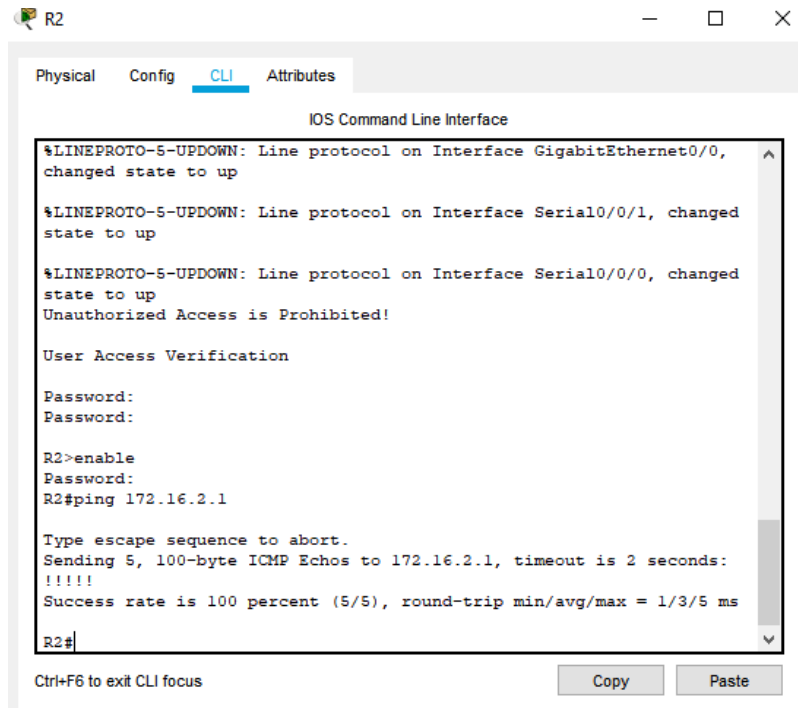
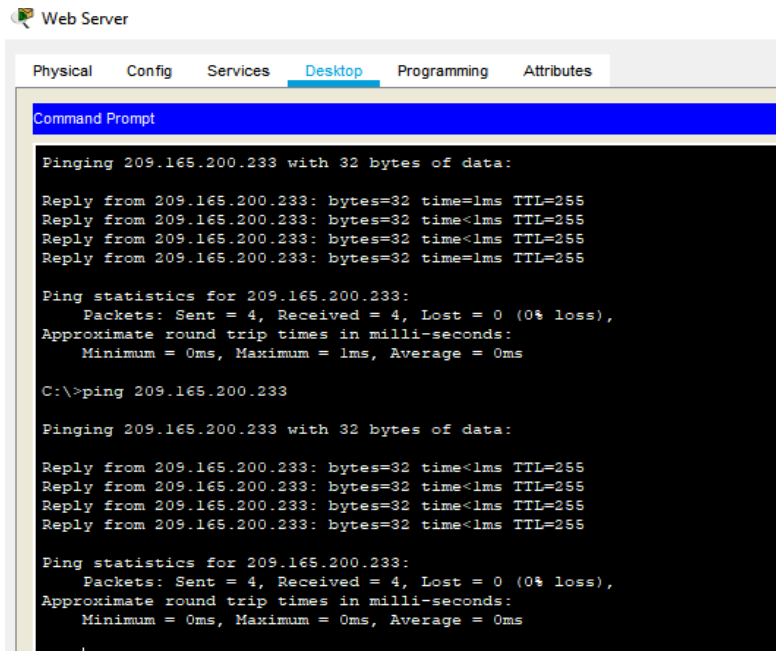


Ilustración 4-Ping web server



Parte 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 -Configuración de seguridad de S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

S1:

```
S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#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
S1(config-if)#exit
S1(config-if)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

Paso 10: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10-Configuración de seguridad de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

S3:

```
S3(config)#vlan 21
```

```
S3(config-vlan)#name contabilidad
```

```
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
```

```
S3(config-vlan)#exit
```

```
S3(config)#int vlan 99
```

```
S3(config-if)#
```

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

```

S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

```

Paso 11: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11-Configuración de seguridad de R1

Elemento o tarea de configuración	Especificación
<i>Configurar la subinterfaz 802.1Q .21 en G0/1</i>	<i>Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz</i>
<i>Configurar la subinterfaz 802.1Q .23 en G0/1</i>	<i>Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz</i>
<i>Configurar la subinterfaz 802.1Q .99 en G0/1</i>	<i>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</i>
<i>Activar la interfaz G0/1</i>	

```

R1(config)#int g0/1.21
R1(config-subif)#description vlan 21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description vlan 23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description vlan 99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-subif)#no shutdown

```

Paso 12: Verificar la conectividad de la red

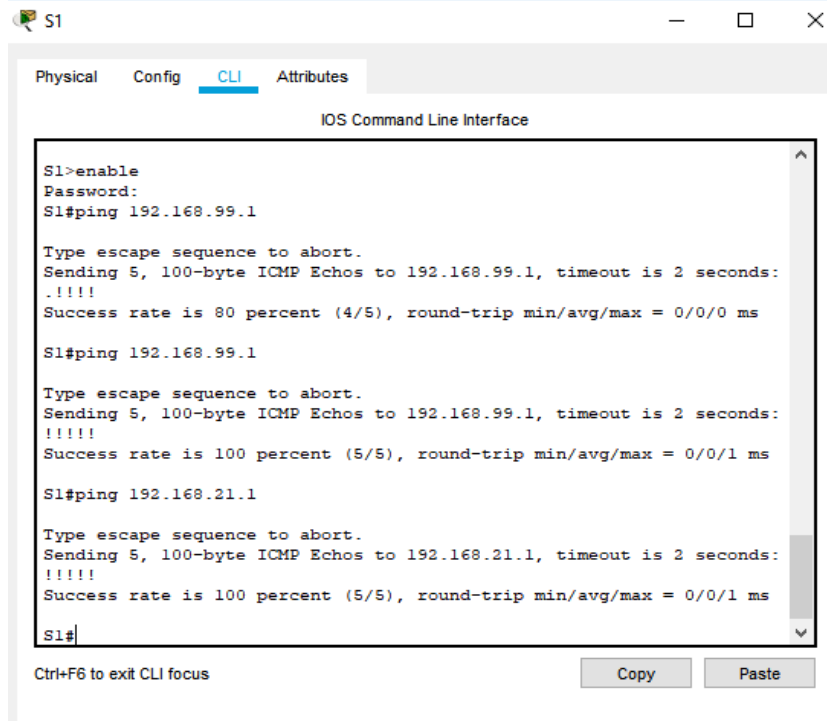
Se utiliza el comando **ping** para probar la conectividad entre los switches y el R1.

La siguiente tabla sirve para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 12-de verificación de conectividad de los dispositivos de red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5)
S3	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5)
S1	R1, dirección VLAN 21	192.168.21.1	Success rate is 100 percent (5/5)
S3	R1, dirección VLAN 23	192.168.23.1	Success rate is 100 percent (5/5)

Ilustración 5-Ping S1



The screenshot shows the CLI interface of a device named S1. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the following text:

```
S1>enable
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 = 0/0/0 ms

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

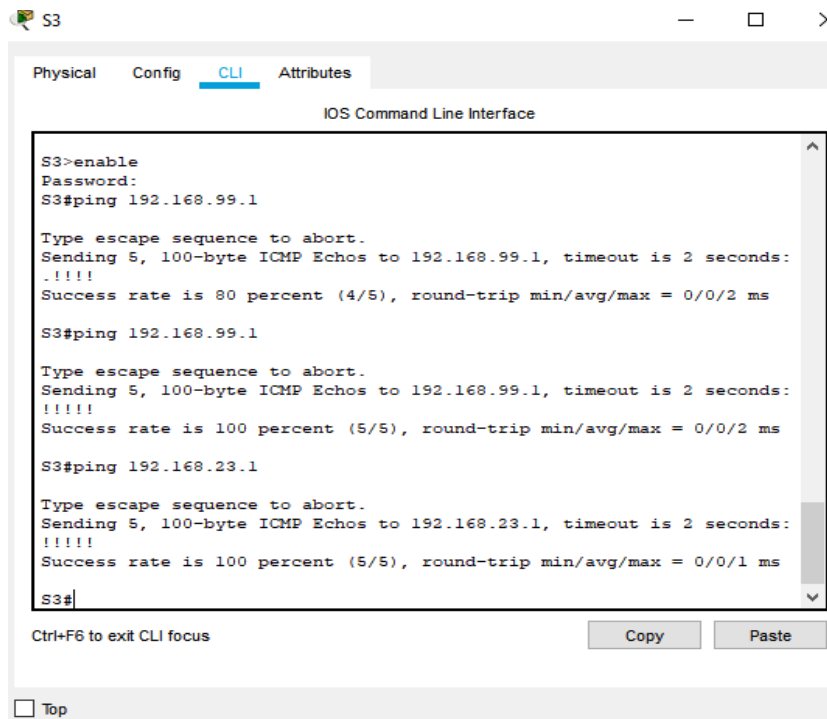
S1#ping 192.168.21.1

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

S1#
```

Below the terminal window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Ilustración 6-Ping S3



The screenshot shows the CLI interface of a device named S3. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the following text:

```
S3>enable
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 = 0/0/2 ms

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 = 0/0/2 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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#
```

Below the terminal window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

At the bottom left of the window, there is a checkbox labeled "Top".

Parte 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

Paso 13: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13-Configuración protocolo RIPv2 R1

Elemento o tarea de configuración	Especificación
<i>Configurar RIPv2 versión 2</i>	
<i>Anunciar las redes conectadas directamente</i>	<i>Asigne todas las redes conectadas directamente.</i>
<i>Establecer todas las interfaces LAN como pasivas</i>	
<i>Desactive la sumarización automática</i>	

R1:

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

```
R1(config)#router rip
```

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

```
R1(config-router)#do show ip route connected
```

```
C 172.16.1.0/30 is directly connected, Serial0/0/0
```

```
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
```

```
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
```

```
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
```

```
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
```

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

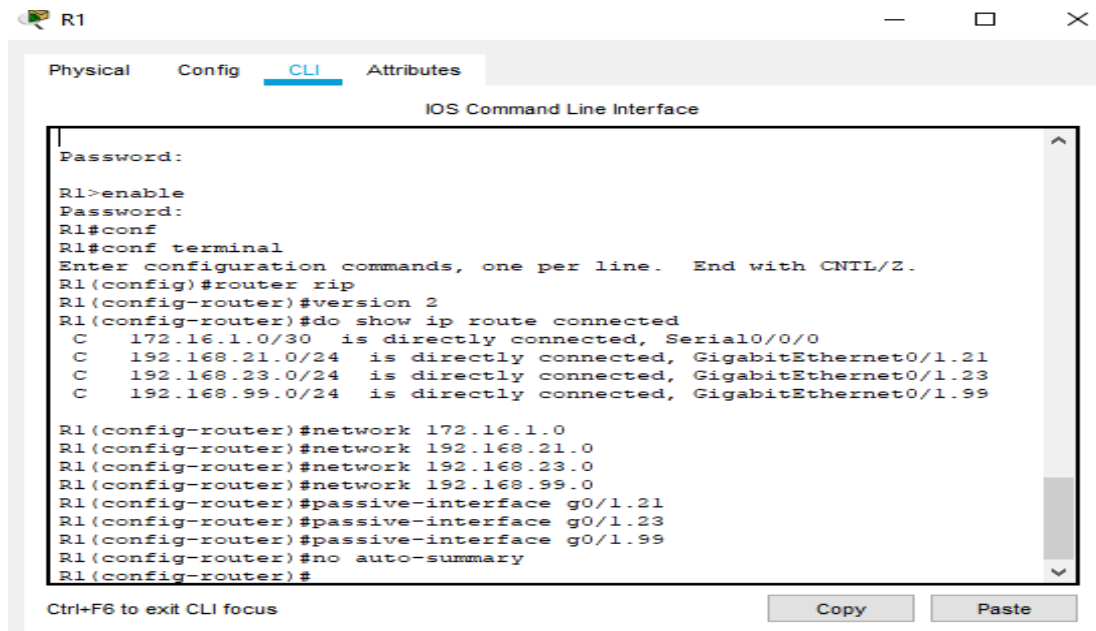
```
R1(config-router)#passive-interface g0/1.23
```

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

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

Con este comando podemos ver todas las redes conectadas directamente

Ilustración 7-Do show ip route connected R1



Paso 14: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Ilustración 8-Configuración de RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIPv2 versión 2	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

R2(config)#router rip

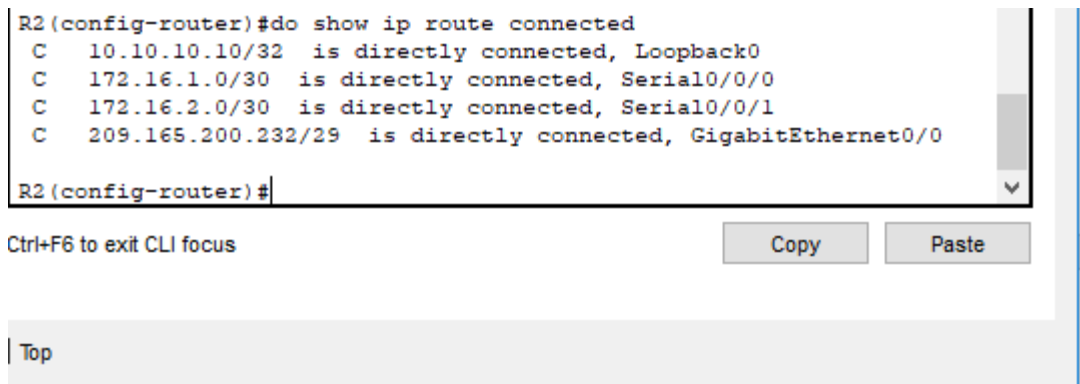
R2(config-router)#version 2

R2(config-router)#do show ip route connected

- C 10.10.10.10/32 is directly connected, Loopback0
- C 172.16.1.0/30 is directly connected, Serial0/0/0
- C 172.16.2.0/30 is directly connected, Serial0/0/1
- C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

```
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
```

Ilustración 9-Do show ip route connected R2



Paso 15: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 14-Elemento o tarea de configuración Especificación

Elemento o tarea de configuración	Especificación
<i>Configurar RIPv3 versión 2</i>	
<i>Anunciar redes IPv4 conectadas directamente</i>	
<i>Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas</i>	
<i>Desactive la sumarización automática.</i>	

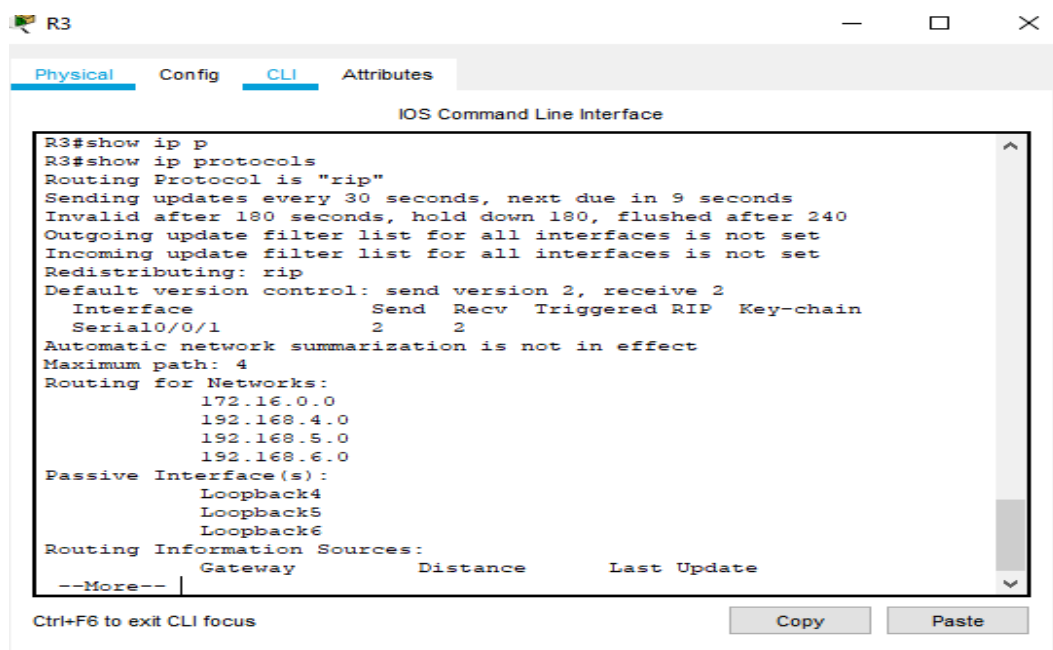
```
R3(config)#router rip
```

```
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
```

```
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
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
```

Muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router

Ilustración 10-Show ip protocols



```
R3#show ip p
R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 9 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/1        2      2
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
Routing Information Sources:
  Gateway            Distance      Last Update
--More--
```

Paso 16: Verificar la información de RIP

En el siguiente paso se Verifica que RIP esté funcionando como se espera. Se introduce el comando de CLI adecuado para obtener la siguiente información:

Tabla 15-Comandos RIP

Pregunta	Respuesta
<i>¿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?</i>	<i>show ip protocols</i>
<i>¿Qué comando muestra solo las rutas RIP?</i>	<i>show ip route rip</i>
<i>¿Qué comando muestra la sección de RIP de la configuración en ejecución?</i>	<i>show run section router rip</i>

Parte 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

Paso 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16-Configuración DHCP Y NAT

Elemento o tarea de configuración	Especificación
<i>Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas</i>	
<i>Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas</i>	
<i>Crear un pool de DHCP para la VLAN 21.</i>	<i>Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</i>
<i>Crear un pool de DHCP para la VLAN 23</i>	<i>Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</i>

R1:

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

R1(config)#ip dhcp pool ACCT

R1(dhcp-config)#network 192.168.21.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.21.1

R1(dhcp-config)#dns-server 10.10.10.10

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

R1(dhcp-config)#ip dhcp pool ENGR

R1(dhcp-config)#network 192.168.23.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.23.1

R1(dhcp-config)#dns-server 10.10.10.10

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

Paso 18: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17-Configuración NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
<i>Crear una base de datos local con una cuenta de usuario</i>	<i>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15</i>
<i>Habilitar el servicio del servidor HTTP</i>	
<i>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</i>	
<i>Crear una NAT estática al servidor web.</i>	<i>Dirección global interna: 209.165.200.237</i>
<i>Asignar la interfaz interna y externa para la NAT estática</i>	

<p><i>Configurar la NAT dinámica dentro de una ACL privada</i></p>	<p><i>Lista de acceso: 1</i> <i>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1</i> <i>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3</i></p>
<p><i>Defina el pool de direcciones IP públicas utilizables.</i></p>	<p><i>Nombre del conjunto: INTERNET</i> <i>El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236</i></p>
<p><i>Definir la traducción de NAT dinámica</i></p>	

R2:

```

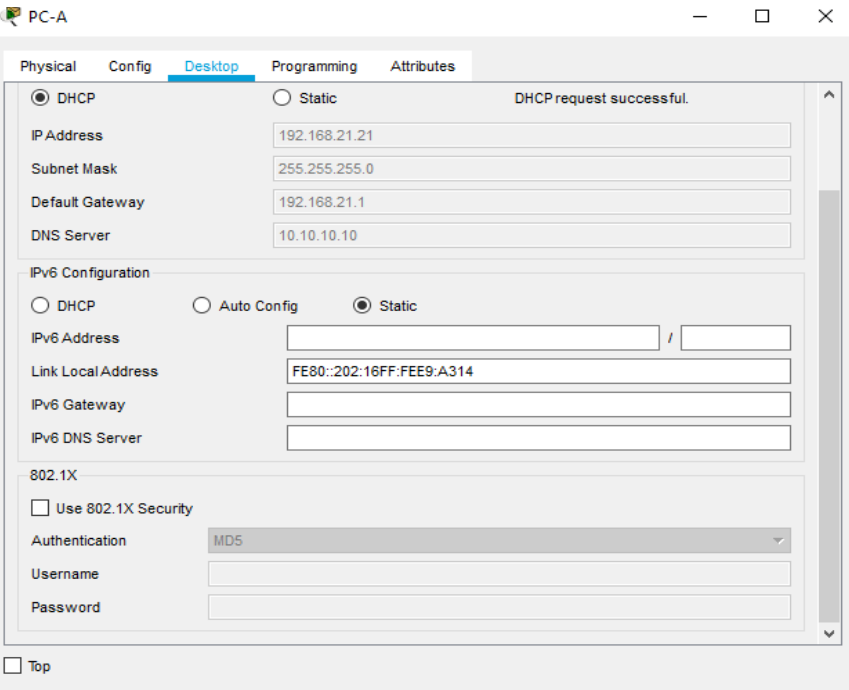
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0.0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0.0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
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

```

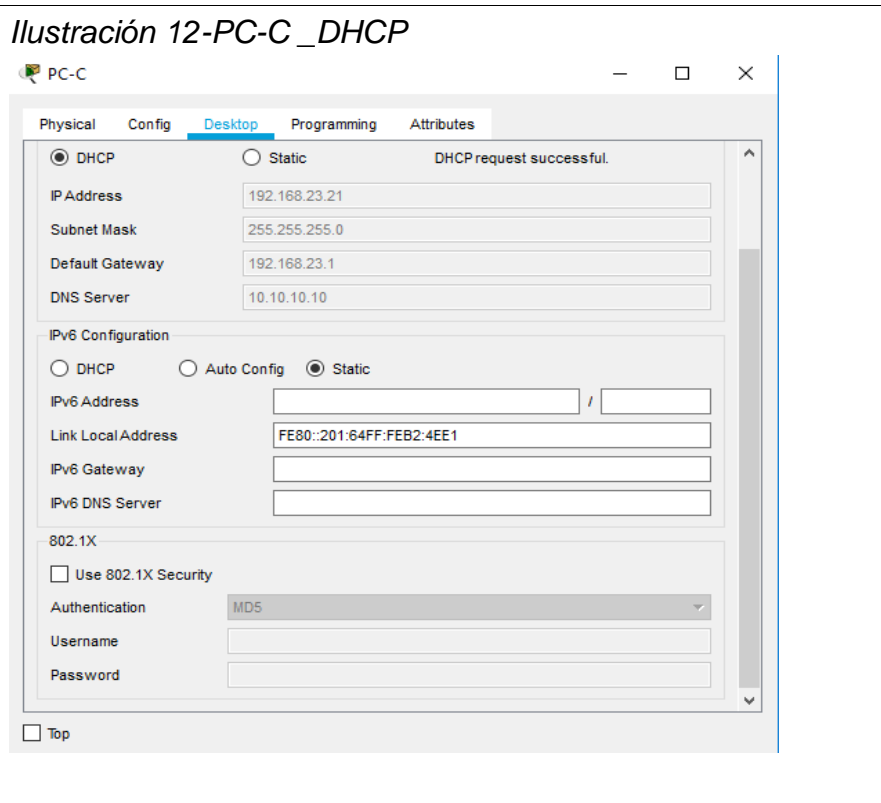
Paso 19: Verificar el protocolo DHCP y la NAT estática

Se utilizan las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 18-Ping verificación del protocolo DHCP y la NAT estática.

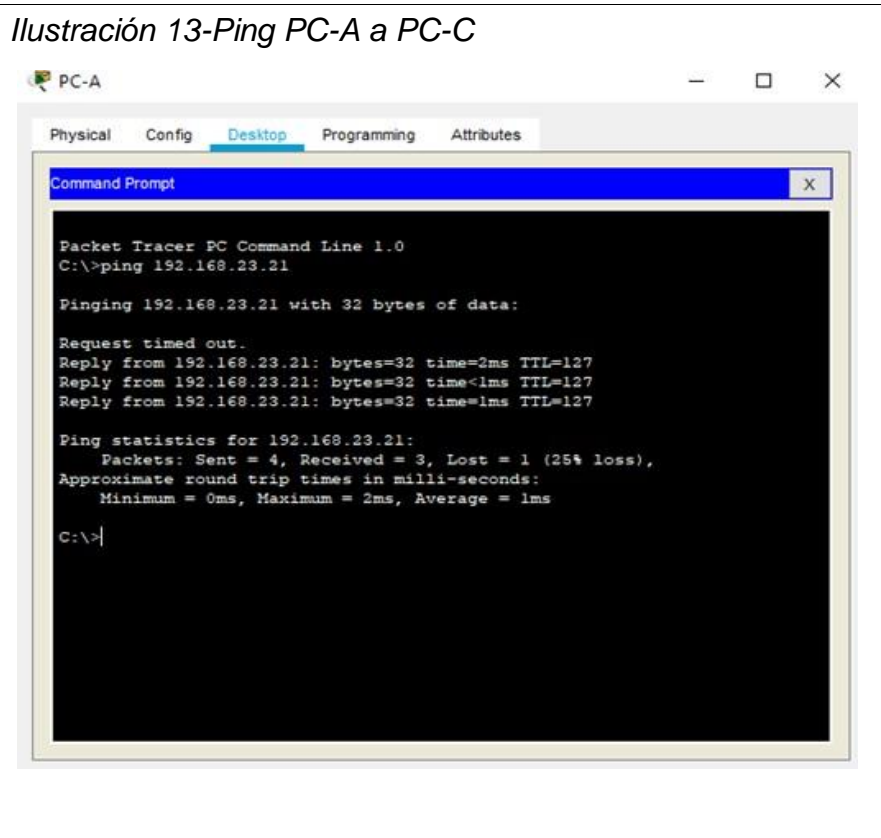
Prueba	Resultados
<p><i>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</i></p>	<p><i>Ilustración 11-PC-A _DHCP</i></p>  <p>The screenshot shows the network configuration interface for PC-A. The 'Desktop' tab is active, and the 'DHCP' radio button is selected. The configuration fields are filled with the following values: IP Address (192.168.21.21), Subnet Mask (255.255.255.0), Default Gateway (192.168.21.1), and DNS Server (10.10.10.10). A status message 'DHCP request successful.' is displayed in the top right corner. Below the DHCP section, the 'IPv6 Configuration' section is visible, with 'Static' selected. The '802.1X' section is also present, with 'Use 802.1X Security' unchecked and 'Authentication' set to 'MD5'. A 'Top' button is located at the bottom left of the configuration window.</p>

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Verificar que la PC-A pueda hacer ping a la PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.



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**

PKT no soporta esta operación.

Ilustración 14-Navegador web -servidor web

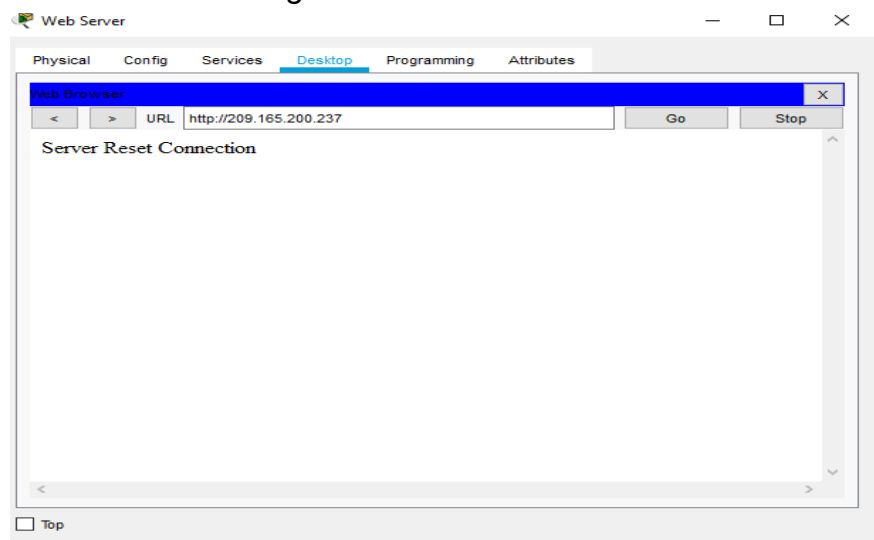
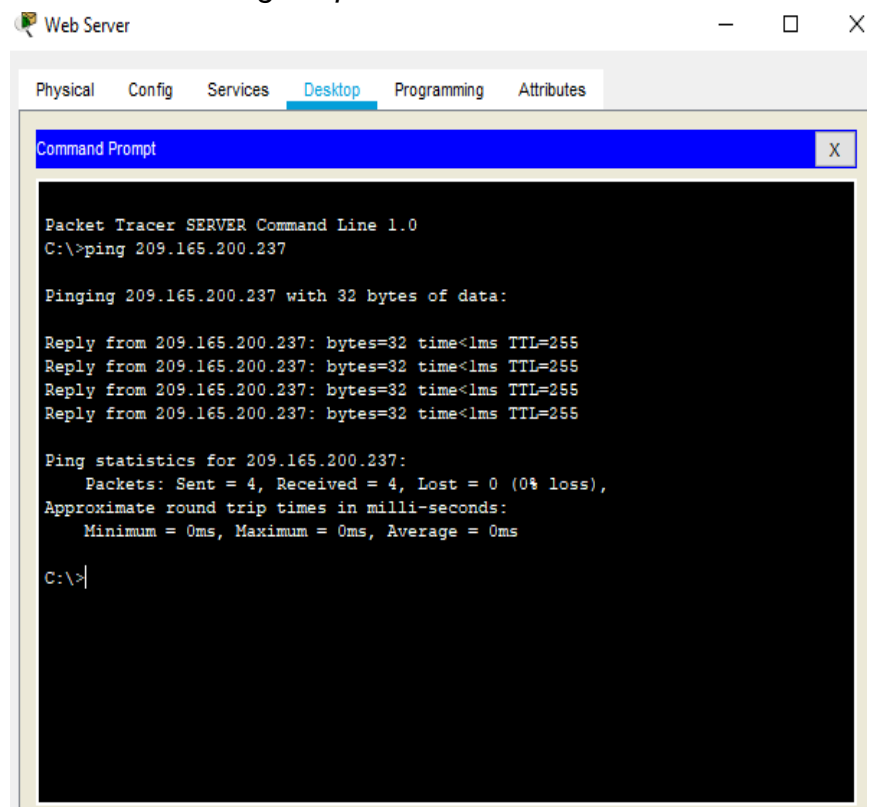


Ilustración 15-Ping de ip server



Pero si se puede hacer ping a esta Ip

Parte 6: CONFIGURAR NTP

Se utilizan las siguientes tareas para verificar que las configuraciones NTP en R2.

Tabla 19-de configuración NTP

Elemento o tarea de configuración	Especificación
<i>Ajuste la fecha y hora en R2.</i>	5 de marzo de 2016, 9 a. m.
<i>Configure R2 como un maestro NTP.</i>	Nivel de estrato: 5
<i>Configurar R1 como un cliente NTP.</i>	Servidor: R2
<i>Configure R1 para actualizaciones de calendario periódicas con hora NTP.</i>	
<i>Verifique la configuración de NTP en R1.</i>	

R2:

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

```
R2#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

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

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

```
R1(config)#end
```

```
R1#
```

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

```
R1#show ntp associations
```

```
address      ref clock    st when  poll reach delay      offset  
disp
```

```
~172.16.1.2  127.127.1.1  5  1    16   17   6.00  
726184533724.00  0.12
```

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Parte 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Paso 20: Restringir el acceso a las líneas VTY en el R2

Tabla 20-Configuración y verificación ACL

Elemento o tarea de configuración	Especificación
<i>Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2</i>	<i>Nombre de la ACL: ADMIN-MGT</i>
<i>Aplicar la ACL con nombre a las líneas VTY</i>	
<i>Permitir acceso por Telnet a las líneas de VTY</i>	
<i>Verificar que la ACL funcione como se espera</i>	

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
```

```
R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!
User Access Verification
Password:
R2>exit
```

```
[Connection to 172.16.1.2 closed by foreign host]
R1#
R3>enable
```

Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#

Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

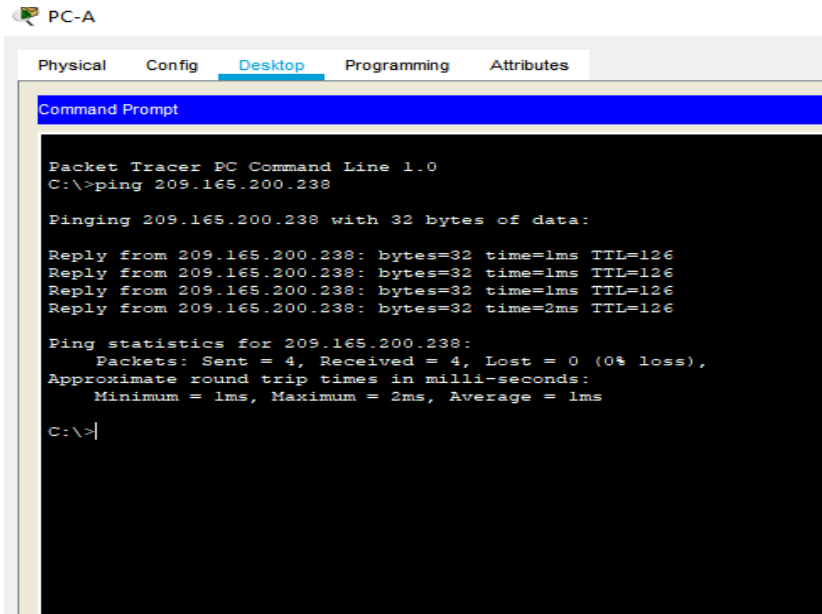
Tabla 21-Comandos De CLI

Descripción del comando	Entrada del estudiante (comando)
<i>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</i>	<i>show access-lists o Tambien show ip access-lists</i> <i>Ilustración 16-Lista de acceso CLI</i>

<i>Restablecer los contadores de una lista de acceso</i>	<i>clear ip access-list counters</i>
<i>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</i>	<i>show ip interface</i>

show ip nat translations

Ilustración 17-Ping de PC-A 209.165.200.238



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

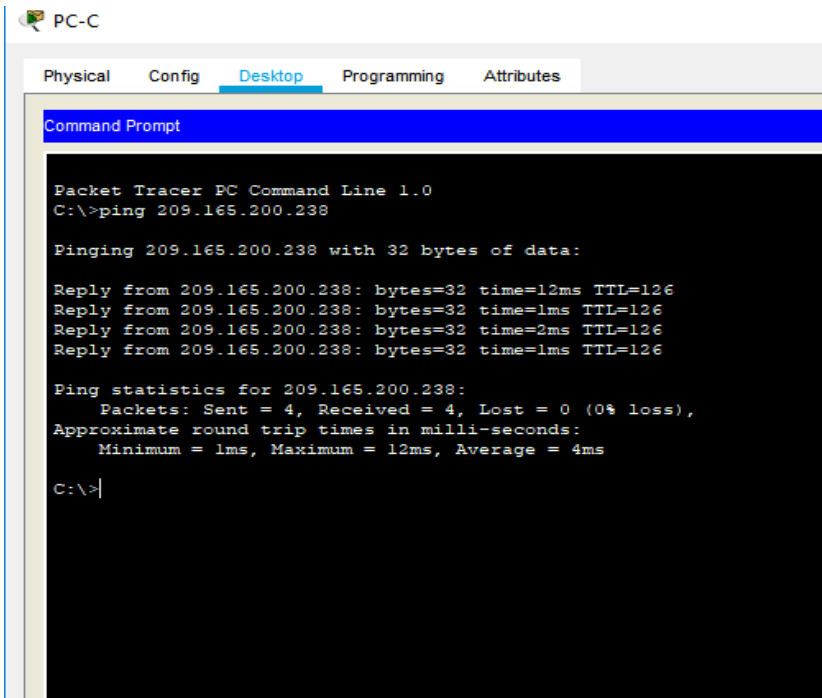
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>|
```

¿Con qué comando se muestran las traducciones NAT?

Ilustración 18-Ping PC-C 209.165.200.238



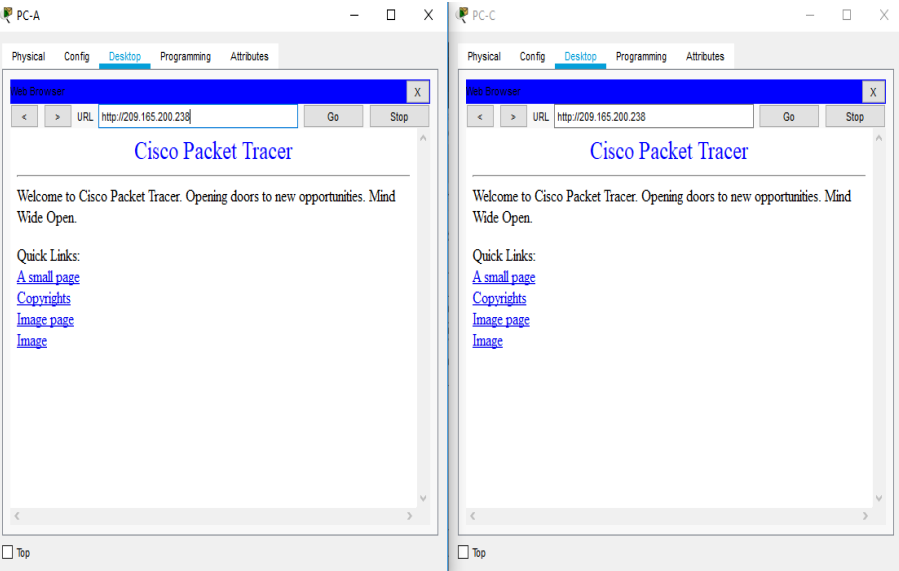
```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>|
```

<p><i>Ilustración 19-Navegador web</i></p>	
	 <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><i>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</i></p>	<pre>Clear ip nat translation show ip nat translations</pre>

ESCENARIO 2

Descripción del escenario:

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 tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

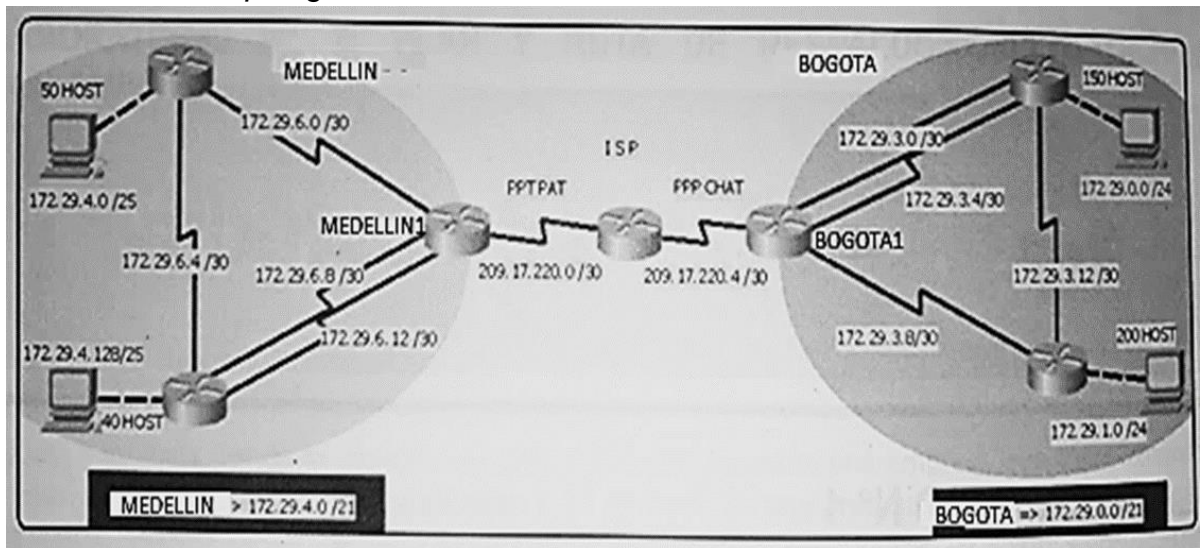
Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

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

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

Topología de red:

Ilustración 20-Topología de red

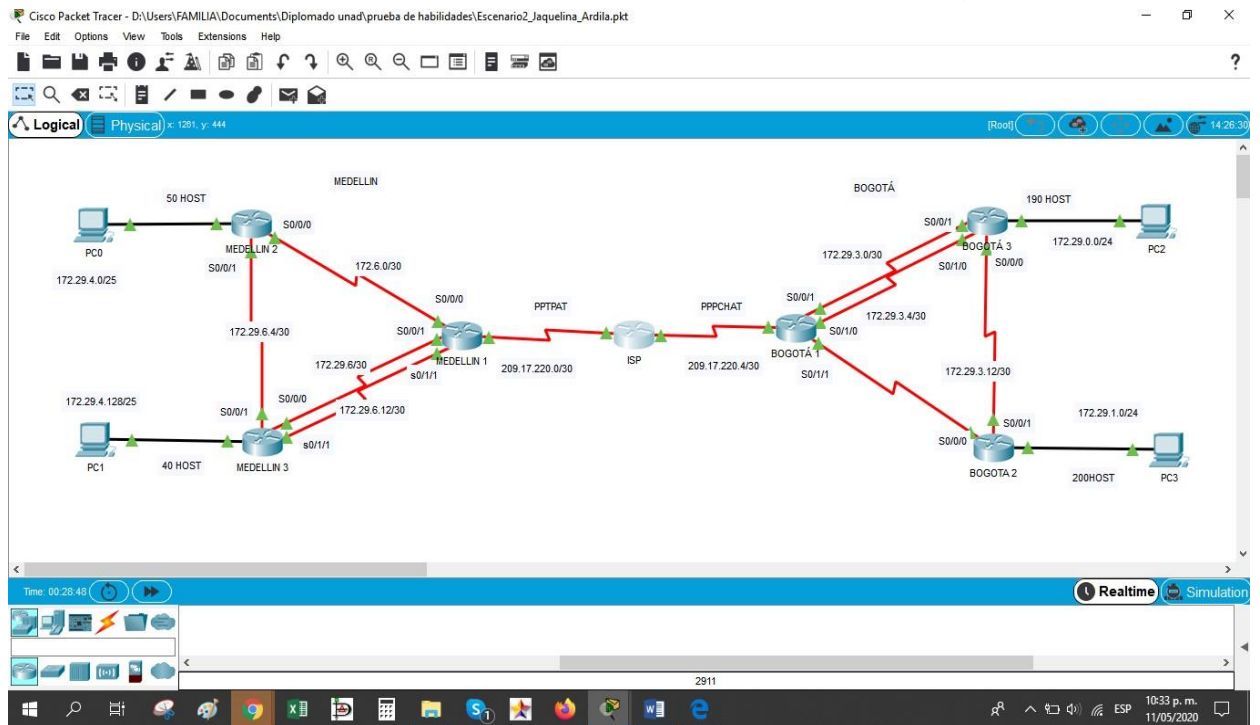


DESARROLLO

Parte 1: Configuración del enrutamiento

- Se realizan las rutinas de diagnóstico y se dejan los equipos listos para su configuración se asignan los nombres de equipos, claves de seguridad, etc.
- Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Ilustración 21-Conexión física de los equipos con base en la topología de red



Configurar los parámetros básicos para todos los Router

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#hostname Bogota1
```

```
Bogota1(config)#line console 0
```

```
Bogota1(config-line)#password cisco
```

```
Bogota1(config-line)#login
```

```
Bogota1(config-line)#exit
```

```
Bogota1(config)#line vty 0 15
```

```
Bogota1(config-line)#password cisco
```

```
Bogota1(config-line)#login
```

```
Bogota1(config-line)#exit
```

```
Bogota1(config)#baner motd & warning &
```

```
Bogota1(config)#enable secret class
Bogota1(config)#service password-encryption
Bogota1(config)#exit
Bogota1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota1#
```

CONECTAR PUERTOS

ISP

```
ISP(config)#int s0/0/0
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#int s0/0/1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#no shut
```

Bogota 1:

```
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip add 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shut
Bogota1(config-if)#s0/1/0
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#ip add 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shut
```

```
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#ip add 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shut
Bogota1(config-if)#int s0/0/0
Bogota1(config-if)#ip add 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 2000000
Bogota1(config-if)#no shut
```

Bogota 2:

```
Bogota2(config)#int s0/0/0
Bogota2(config-if)#ip add 172.29.3.10 255.255.255.252
Bogota2(config-if)#no shut
Bogota2(config-if)#int s0/0/1
Bogota2(config-if)#ip add 172.29.3.13 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shut
Bogota2(config-if)#int g0/0
Bogota2(config-if)#ip add 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shut
```

Bogota 3:

```
Bogota3(config)#int s0/0/0
Bogota3(config-if)#ip add 172.29.3.14 255.255.255.252
Bogota3(config-if)#Router(config-if)#no shut
Bogota3(config-if)#ip add 172.29.3.14 255.255.255.252
Bogota3(config-if)#int s0/0/0
Bogota3(config-if)#ip add 172.29.3.14 255.255.255.252
Bogota3(config-if)#no shut
```

```
Bogota3(config-if)#int s0/1/0
Bogota3(config-if)#ip add 172.29.3.6 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shut
Bogota3(config-if)#int s0/0/1
Bogota3(config-if)#ip add 172.29.3.2 255.255.255.252
Bogota3(config-if)#no shut
```

```
Bogota3(config-if)#int g0/0
Bogota3(config-if)#ip add 172.29.0.1 255.255.255.0
Bogota3(config-if)#no shut
```

Medellin 1:

```
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ip add 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shut
Medellin1(config-if)#int s0/1/1
Medellin1(config-if)#ip add 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shut
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#ip add 209.17.220.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shut
Medellin1(config)#int s0/0/1
Medellin1(config-if)#ip add 172.29.6.3 255.255.255.252
```

Bad mask /30 for address 172.29.6.3
Medellin1(config-if)#clock rate 128000

Medellin 2:

Medellin2(config)#int s0/0/0
Medellin2(config-if)# ip add 172.29.6.2 255.255.255.252
Medellin2(config-if)#no shut
Medellin2(config-if)#int s0/0/1
Medellin2(config-if)# ip add 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config)#int g0/0
Medellin2(config-if)#ip add 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shut

Medellin 3:

Medellin3(config)#int s0/0/0
Medellin3(config-if)#ip add 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shut
Medellin3(config-if)#int s0/1/1
Medellin3(config-if)#ip add 172.29.6.9 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shut
Medellin3(config-if)#int s0/0/1
Medellin3(config-if)#ip add 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shut
Medellin3(config)#int g0/0
Medellin3(config-if)#ip add 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shut

Parte 1: CONFIGURACIÓN DEL ENRUTAMIENTO

a. Se configura el enrutamiento en la red usando el protocolo OSPF versión 2, declarando la red principal, desactivando la sumarización automática en cada router.

Bogota1

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#router-id 1.1.1.1
Bogota1(config-router)#no auto-summary
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#passive-interface gigabitEthernet 0/0
```

Bogota2

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 2.2.2.2
Bogota2(config-router)#no auto-summary
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#passive-interface gigabitEthernet 0/0
```

Bogota3

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 3.3.3.3
Bogota3(config-router)#no auto-summary
```

```
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota3(config-router)#passive-interface gigabitEthernet 0/0
Bogota3(config-router)#
```

Medellin1

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 4.4.4.4
Medellin1(config-router)#no auto-summary
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#passive-interface gigabitEthernet 0/0
```

Medellin 2

```
Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 5.5.5.5
Medellin2(config-router)#no auto-summary
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#passive-interface gigabitEthernet 0/0
```

Medellin3

```
Medellin3(config)#router ospf 1
Medellin3(config-router)#router-id 6.6.6.6
Medellin3(config-router)#no auto-summary
```

```
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#passive-interface gigabitEthernet 0/0
```

ISP

```
ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.1 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.5 0.0.0.3 area 0
ISP(config-router)#no auto-summary
```

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.

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

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

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.6
```

Parte 2: TABLA DE ENRUTAMIENTO.

a. Se verifican las tablas de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Bogota1

Bogota1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks

C 172.29.3.0/30 is directly connected, Serial0/0/1

L 172.29.3.1/32 is directly connected, Serial0/0/1

C 172.29.3.4/30 is directly connected, Serial0/1/0

L 172.29.3.5/32 is directly connected, Serial0/1/0

C 172.29.3.8/30 is directly connected, Serial0/1/1

L 172.29.3.9/32 is directly connected, Serial0/1/1

Bogota2

Bogota2#show ip route

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 6 subnets, 3 masks

C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
L 172.29.1.1/32 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
L 172.29.3.10/32 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
L 172.29.3.13/32 is directly connected, Serial0/0/1

Bogota3

Bogota3#show ip route

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks

```
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/1
L 172.29.3.2/32 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
L 172.29.3.6/32 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/0/0
L 172.29.3.14/32 is directly connected, Serial0/0/0
```

Medellin1

Medellin1>enable

Password:

Medellin1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 4 subnets, 2 masks

```
C 172.29.6.0/30 is directly connected, Serial0/0/0
```

```
L    172.29.6.1/32 is directly connected, Serial0/0/0
C    172.29.6.12/30 is directly connected, Serial0/1/1
L    172.29.6.13/32 is directly connected, Serial0/1/1
```

Medellin2

```
Medellin2#show ip route
```

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

```
Gateway of last resort is not set
```

```
172.29.0.0/16 is variably subnetted, 6 subnets, 3 masks
C    172.29.4.0/25 is directly connected, GigabitEthernet0/0
L    172.29.4.1/32 is directly connected, GigabitEthernet0/0
C    172.29.6.0/30 is directly connected, Serial0/0/0
L    172.29.6.2/32 is directly connected, Serial0/0/0
C    172.29.6.4/30 is directly connected, Serial0/0/1
L    172.29.6.5/32 is directly connected, Serial0/0/1
```

Medellin3

Medellin3#show ip route

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks

C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
L 172.29.4.129/32 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.6/32 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/1
L 172.29.6.9/32 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/0/0
L 172.29.6.14/32 is directly connected, Serial0/0/0

ISP

ISP#enable

ISP#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

b. Se verifica el balanceo de carga que presentan los routers.

Medellin 1

- O 172.29.6.4/30 [110/128] via 172.29.6.14, 03:42:47, Serial0/1/1
[110/128] via 172.29.6.2, 03:42:47, Serial0/0/0
- O 172.29.6.8/30 [110/128] via 172.29.6.14, 03:42:47, Serial0/1/1

Medellin 2

- O 172.29.6.8/30 [110/128] via 172.29.6.6, 03:42:31, Serial0/0/1
- O 172.29.6.12/30 [110/128] via 172.29.6.1, 03:42:31, Serial0/0/0
[110/128] via 172.29.6.6, 03:42:31, Serial0/0/1

Medellin 3

- O 172.29.6.0/30 [110/128] via 172.29.6.5, 03:42:37, Serial0/0/1
[110/128] via 172.29.6.13, 03:42:37,

Bogota 1

- O 172.29.3.12/30 [110/128] via 172.29.3.10, 03:42:44, Serial0/1/1
[110/128] via 172.29.3.2, 03:42:44, Serial0/0/1

Bogota 2

O 172.29.3.0/30 [110/128] via 172.29.3.9, 03:42:39, Serial0/0/0
[110/128] via 172.29.3.14, 03:42:39, Serial0/0/1

O 172.29.3.4/30 [110/128] via 172.29.3.9, 03:42:39, Serial0/0/0
[110/128] via 172.29.3.14, 03:42:39, Serial0/0/1

Bogota 3

O 172.29.3.8/30 [110/128] via 172.29.3.1, 03:42:39, Serial0/0/1
[110/128] via 172.29.3.13, 03:42:39, Serial0/0/0

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.

Bogota1

172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks

O 172.29.3.12 [110/128] via 172.29.3.10, 03:42:44, Serial0/1/1
[110/128] via 172.29.3.2, 03:42:44, Serial0/0/1

Medellin1

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks

O 172.29.6.4 [110/128] via 172.29.6.14, 03:42:47, Serial0/1/1
[110/128] via 172.29.6.2, 03:42:47, Serial0/0/0

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

c. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

e. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Medellin2

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks

O 172.29.6.8 [110/128] via 172.29.6.6, 03:42:42, Serial0/0/1

O 172.29.6.12 [110/128] via 172.29.6.1, 03:42:42, Serial0/0/0

[110/128] via 172.29.6.6, 03:42:42, Serial0/0/1

Bogota2

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks

- O 172.29.3.0 [110/128] via 172.29.3.9, 03:42:39, Serial0/0/0
[110/128] via 172.29.3.14, 03:42:39, Serial0/0/1
- O 172.29.3.4 [110/128] via 172.29.3.9, 03:42:39, Serial0/0/0
[110/128] via 172.29.3.14, 03:42:39, Serial0/0/1

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.

Tabla 22-Interfaces de router que no necesitan desactivación. Protocolo OSPF

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

Bogota1

```
Bogota1(config)#router ospf 1  
Bogota1(config-router)#passive-interface serial 0/0/1  
Bogota1(config-router)#passive-interface serial 0/1/1  
Bogota1(config-router)#passive-interface serial 0/1/0
```

Bogota2

```
Bogota2(config)#router ospf 1  
Bogota2(config-router)#passive-interface serial 0/0/1  
Bogota2(config-router)#passive-interface serial 0/0/0
```

Bogota3

```
Bogota3(config)#router ospf 1  
Bogota3(config-router)#passive-interface serial 0/0/0  
Bogota3(config-router)#passive-interface serial 0/1/0  
Bogota3(config-router)#passive-interface serial 0/0/0
```

Medellin1

```
Medellin1(config)#router ospf 1  
Medellin1(config-router)#passive-interface serial 0/0/0  
Medellin1(config-router)#passive-interface serial 0/0/1  
Medellin1(config-router)#passive-interface serial 0/1/1
```

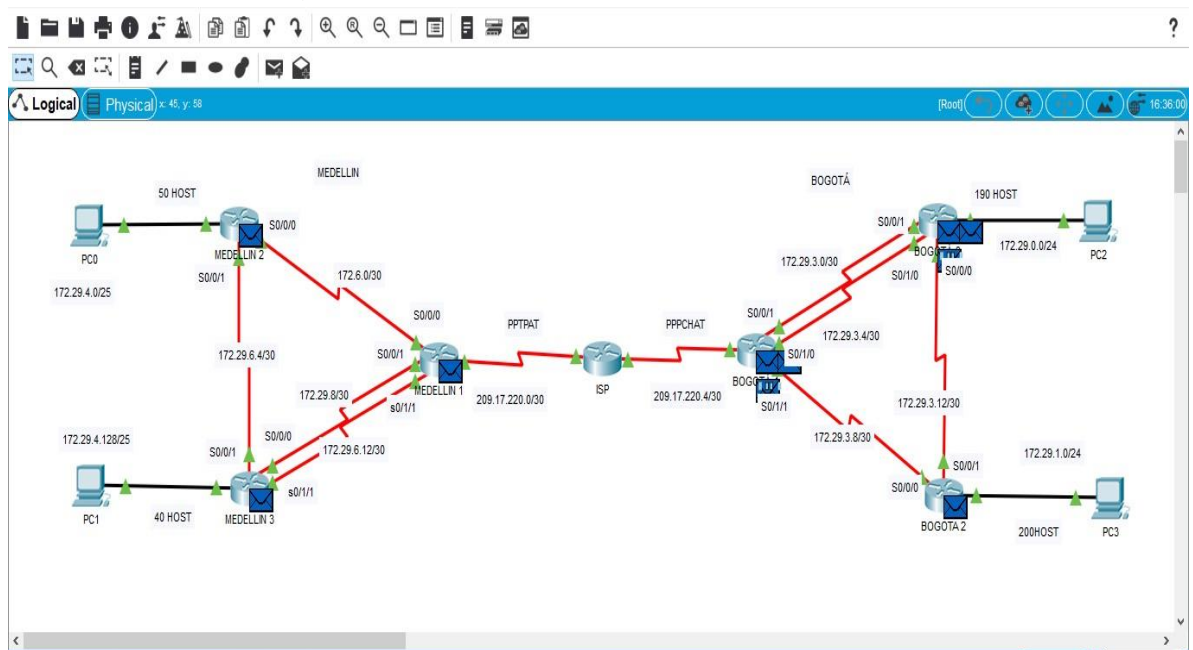
Medellin2

```
Medellin2(config)#router ospf 1  
Medellin2(config-router)#passive-interface serial 0/0/0  
Medellin2(config-router)#passive-interface serial 0/0/1
```

Medellin3

```
Medellin3(config)#router ospf 1  
Medellin3(config-router)#passive-interface serial 0/0/0  
Medellin3(config-router)#passive-interface serial 0/0/1  
Medellin3(config-router)#passive-interface serial 0/1/0
```

Ilustración 22-Propagación del protocolo OSPF deshabilitado.



Parte 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

- Se verifican y documentan 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.

RPTA: **show ip protocols**

- 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.

Medellin1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 4.4.4.4

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

209.17.220.0 0.0.0.3 area 0

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

Passive Interface(s):

Serial0/0/0

Serial0/0/1

Serial0/1/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

4.4.4.4	110	00:00:15
---------	-----	----------

Distance: (default is 110)

Medellin2#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 5.5.5.5

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.6.0 0.0.0.3 area 0

172.29.6.4 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Serial0/0/0

Serial0/0/1

Routing Information Sources:

Gateway	Distance	Last Update
5.5.5.5	110	00:02:17

Distance: (default is 110)

Medellin3#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 6.6.6.6

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

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

Serial0/0/0

Serial0/0/1

Serial0/1/0

Routing Information Sources:

Gateway	Distance	Last Update
6.6.6.6	110	00:03:15

Distance: (default is 110)

Bogota1#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

20.17.220.0 0.0.0.3 area 0

172.29.3.0 0.0.0.3 area 0

172.29.3.4 0.0.0.3 area 0

172.29.3.8 0.0.0.3 area 0

20.17.220.4 0.0.0.3 area 0

209.17.220.0 0.0.0.3 area 0

172.19.3.0 0.0.0.3 area 0

209.17.220.4 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

1.1.1.1	110	00:04:05
---------	-----	----------

Distance: (default is 110)

Bogota2#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 2.2.2.2

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

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

Serial0/0/1

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

2.2.2.2	110	00:05:31
---------	-----	----------

Distance: (default is 110)

Bogota3#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 3.3.3.3

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.3.12 0.0.0.3 area 0

172.29.3.0 0.0.0.3 area 0

172.29.3.4 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Serial0/0/0

Serial0/0/1

Serial0/1/0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

3.3.3.3	110	00:06:41
---------	-----	----------

Distance: (default is 110)

Parte 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

Configuración ISP

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

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

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

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
```

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

```
ISP(config-if)#ppp pap sent-username ISP password 12345
```

Configuración medellin1

```
Medellin1(config)#int s0/1/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username MED1 password 12345
Medellin1(config-if)#end
```

Configuración ISP

```
ISP(config)#username BOG1 password 12345
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

Configuración Bogota1

```
Bogota1(config-if)#int s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
```

Parte 6: CONFIGURACIÓN DE PAT.

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

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

Configuración NAT en el router Medellín1

Medellin1

```
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)# ip nat outside
Medellin1(config-if)#int s0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/1/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#ip nat inside
```

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.

Bogota 1

```
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#
```

Parte 7: CONFIGURACIÓN DEL SERVICIO DHCP.

- a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
- b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Configuración medellin2

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.6
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.134
Medellin2(config)#ip dhcp pool Medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 10.10.10.10
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool Medellin3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 10.10.10.10
Medellin2(dhcp-config)#exit
```

Configuración Medellin 3

```
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
```

- c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
- d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Bogota2

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.6
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.6
```

```
Bogota2(config)#ip dhcp pool Bogota2
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#dns-server 10.10.10.10
Bogota2(dhcp-config)#ip dhcp pool Bogota3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns-server 10.10.10.10
Bogota2(dhcp-config)#exit
```

Configuración Bogota3

```
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config-if)#exit
```

CONCLUSIONES

- Los conocimientos adquiridos con diversos aspectos de Networking permiten hacer una correcta instalación de cualquier red.
- Cisco es una herramienta que ofrece gran variedad de dispositivos que permiten al estudiante familiarizarse con el ambiente de trabajo en redes permitiendo solucionar cualquier inconveniente en un ambiente virtual pero perfectamente adecuado para el aprendizaje.
- El protocolo RIP V2 puede incluir más información de paquetes y permite un mecanismo de autenticación simple.
- OSPF V2 ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.
- Por medio del uso de la plataforma y del desarrollo de los escenarios se logra implementar y comprender las configuraciones de red, permitiendo solucionar los distintos problemas encontrados en las actividades propuestas, ampliando el conocimiento del estudiante, lo cual tiene como resultado que el estudiante pueda conectar cada uno de los dispositivos, realizar y aplicar la configuración y protocolos para el diseño de una topología de red.

REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC>

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>