

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

HECTOR ANDRES CORREA ACOSTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE SISTEMAS  
DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PEREIRA - RISARALDA  
2020

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

HECTOR ANDRES CORREA ACOSTA

Proyecto de grado. presentado para obtener el título de  
INGENIERO DE SISTEMAS

Docente  
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE SISTEMAS  
DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PEREIRA – RISARALDA

2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente de Jurado

---

Firma del Jurado

---

Firma del Jurado

Pereira, 15 de mayo de 2020

## TABLA DE CONTENIDO

	Pág.
TABLA DE CONTENIDO .....	4
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
LISTA DE ANEXOS .....	8
INTRODUCCIÓN .....	9
OBJETIVOS.....	10
OBJETIVO GENERAL .....	10
OBJETIVOS ESPECIFICOS .....	10
1 ESCENARIO 1 .....	11
1.1 TOPOLOGÍA.....	11
1.2 INICIALIZAR DISPOSITIVOS .....	11
1.2.1 INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES .....	11
1.3 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS.....	12
1.3.1 CONFIGURAR LA COMPUTADORA DE INTERNET .....	12
1.3.2 CONFIGURAR R1 .....	13
1.3.3 CONFIGURAR R2 .....	14
1.3.4 CONFIGURAR R3 .....	16
1.3.5 CONFIGURAR S1 .....	18
1.3.6 CONFIGURAR EL S3.....	19
1.3.7 VERIFICAR LA CONECTIVIDAD DE LA RED.....	19
1.4 CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN.....	20
1.4.1 CONFIGURAR S1 .....	20
1.4.2 CONFIGURAR EL S3.....	21
1.4.3 CONFIGURAR R1 .....	23
1.4.4 VERIFICAR LA CONECTIVIDAD DE LA RED.....	24
1.5 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2 24	24
1.5.1 CONFIGURAR RIPV2 EN EL R1.....	24
1.5.2 CONFIGURAR RIPV2 EN EL R2.....	25
1.5.3 CONFIGURAR RIPV3 EN EL R2.....	25
1.5.4 VERIFICAR LA INFORMACIÓN DE RIP .....	26
1.6 IMPLEMENTAR DHCP Y NAT PARA IPV4 .....	27
1.6.1 CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23.....	27
1.6.2 CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2 28	28
1.6.3 VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA 29	29
1.7 CONFIGURAR NTP .....	30

1.8	CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL) .....	31
1.8.1	RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2	31
1.8.2	INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE .....	31
2	ESCENARIO 2 .....	33
2.1	TOPOLOGÍA DE RED.....	33
2.1.1	CONFIGURACIÓN BÁSICA DE ROUTER .....	33
2.1.2	DIRECCIONAMIENTO.....	34
2.2	CONFIGURACIÓN DEL ENRUTAMIENTO .....	36
2.3	TABLA DE ENRUTAMIENTO. ....	38
2.4	DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF. ....	39
2.5	VERIFICACIÓN DEL PROTOCOLO OSPF. ....	40
2.6	CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP ...	40
	❖ MEDELLIN1(CONFIG)#USERNAME ISP PASSWORD CISCO	41
	❖ MEDELLIN1(CONFIG)#INT S0/0/0 .....	41
	❖ MEDELLIN1(CONFIG-IF)#ENCAPSULATION PPP.....	41
	❖ MEDELLIN1(CONFIG-IF)#PPP AUTHENTICATION PAP .....	41
	❖ MEDELLIN1(CONFIG-IF)#PPP PAP SENT-USERNAME	
	MEDELLIN1 PASSWORD CISCO .....	41
2.7	CONFIGURACIÓN DE PAT.....	41
2.8	PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.....	42
	CONCLUSIONES .....	44
	BIBLIOGRAFÍA.....	45
	ANEXOS .....	46

## LISTA DE TABLAS

	Pág.
Tabla 1. Inicializar y volver a cargar los R y S.....	12
Tabla 2. Configurar la computadora de Internet.....	12
Tabla 3. Configurar R1.....	13
Tabla 4. Configurar R2.....	14
Tabla 5. Configurar R3.....	16
Tabla 6. Configurar S1.....	18
Tabla 7. Configurar S3.....	19
Tabla 8. Verificar la Conectividad de la Red .....	20
Tabla 9. Configurar la Seguridad. Configurar S1 .....	20
Tabla 10. Configurar la Seguridad. Configurar S3 .....	22
Tabla 11. Configurar la Seguridad. Configurar R1 .....	23
Tabla 12. Configurar la Seguridad. Verificar la Conectividad de la Red.....	24
Tabla 13. Configurar RIPV2 en el R1 .....	24
Tabla 14. Configurar RIPV2 en el R2.....	25
Tabla 15. Configurar RIPV3 en el R2.....	26
Tabla 16. Verificar la información de RIP .....	26
Tabla 17. Configurar el R1 como servidor de DHCP.....	27
Tabla 18. Configurar la NAT estática y dinámica en el R2.....	28
Tabla 19. Verificar el Protocolo DHCP y la NAT Estática.....	29
Tabla 20. Configurar NTP .....	30
Tabla 21. Restringir el acceso a las líneas líneas VTY en el R2 .....	31
Tabla 22. Introducir el comando de CLI .....	32
Tabla 23. Red Sumarizada. Medellín .....	38
Tabla 24. Red sumarizada. Bogotá.....	38
Tabla 25. Deshabilitar la Propagación del Protocolo OSPF .....	39

## LISTA DE FIGURAS

	Pág.
Figura 1. Topología de Red. Escenario 1.....	11
Figura 2. Topología de Red. Escenario 2.....	33

## LISTA DE ANEXOS

	Pág.
Anexo 1. Registro Fotográfico. Ping R1 a R2.....	46
Anexo 2. Registro Fotográfico. Ping R2 a R3.....	46
Anexo 3. Registro Fotográfico. Ping PC de Internet a Gateway Predeterminado .....	46
Anexo 4. Registro Fotográfico. Ping S1 a R1 Dirección VLAN 99 - 21 .....	47
Anexo 5. Registro Fotográfico. Ping S3 a R1 Dirección VLAN 99 - 23 .....	47
Anexo 6. Registro Fotográfico. Verificar la Información de RIP .....	48
Anexo 7. Registro Fotográfico. Verificar la Información de RIP .....	48
Anexo 8. Registro Fotográfico. Verificar IP en PC-A y PC-C del Servidor de DHCP.....	49
Anexo 9. Registro Fotográfico. Ping PC-A a PC-C .....	49
Anexo 10. Registro Fotográfico. Acceder al servidor web (209.165.200.237) .....	50
Anexo 11. Registro Fotográfico. Configuración NTP en R1 .....	50
Anexo 12. Registro Fotográfico. Verificar el Acceso a las Líneas Vty En El R2 .....	51
Anexo 13. Registro Fotográfico. Comandos (show ip access-list) y (show ip interface).....	51
Anexo 14. Registro Fotográfico. Comandos (show ip nat translations) y (clear ip nat translations).....	52
Anexo 15. Registro Fotográfico. Comprobar conexión con ISP .....	52
Anexo 16. Registro Fotográfico. Conectividad entre Medellín y Bogotá.....	53
Anexo 17. Registro Fotográfico. Tabla de Enrutamiento Medellín3 .....	53
Anexo 18. Registro Fotográfico. Balanceo de carga .....	54
Anexo 19. Registro Fotográfico. Rutas Estáticas ISP .....	54
Anexo 20. Registro Fotográfico. Verificación Protocolo OSPF.....	55
Anexo 21. Registro Fotográfico. Lista de Interfaces.....	55
Anexo 22. Registro Fotográfico. Comando show ip nat translations .....	56
Anexo 23. Registro Fotográfico. Configuración IP DHCP PC0 – PC1 .....	56
Anexo 24. Registro Fotográfico. Configuración IP DHCP PC2 – PC3 .....	57



## INTRODUCCIÓN

El presente trabajo forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, se presentan problemas relacionados con diversos aspectos de Networking que fueron vistos durante el desarrollo del diplomado. se desarrollan (2) escenarios en los cuales se documenta la solución de cada uno y se deja la evidencia de las configuraciones de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas y el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

El proceso es realizado en Packet Tracer y entre las configuraciones realizadas para el escenario (1) se encuentra: configuración básica del router, configuración de seguridad, configuración de RIPv2, implementación DHCP y NAT, configuración NTP, etc.

Entre las configuraciones del escenario (2) se encuentran: configuración básica del router, enrutamiento, configuración de PAT, configuración DHCP, etc

## OBJETIVOS

### OBJETIVO GENERAL

Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking

### OBJETIVOS ESPECIFICOS

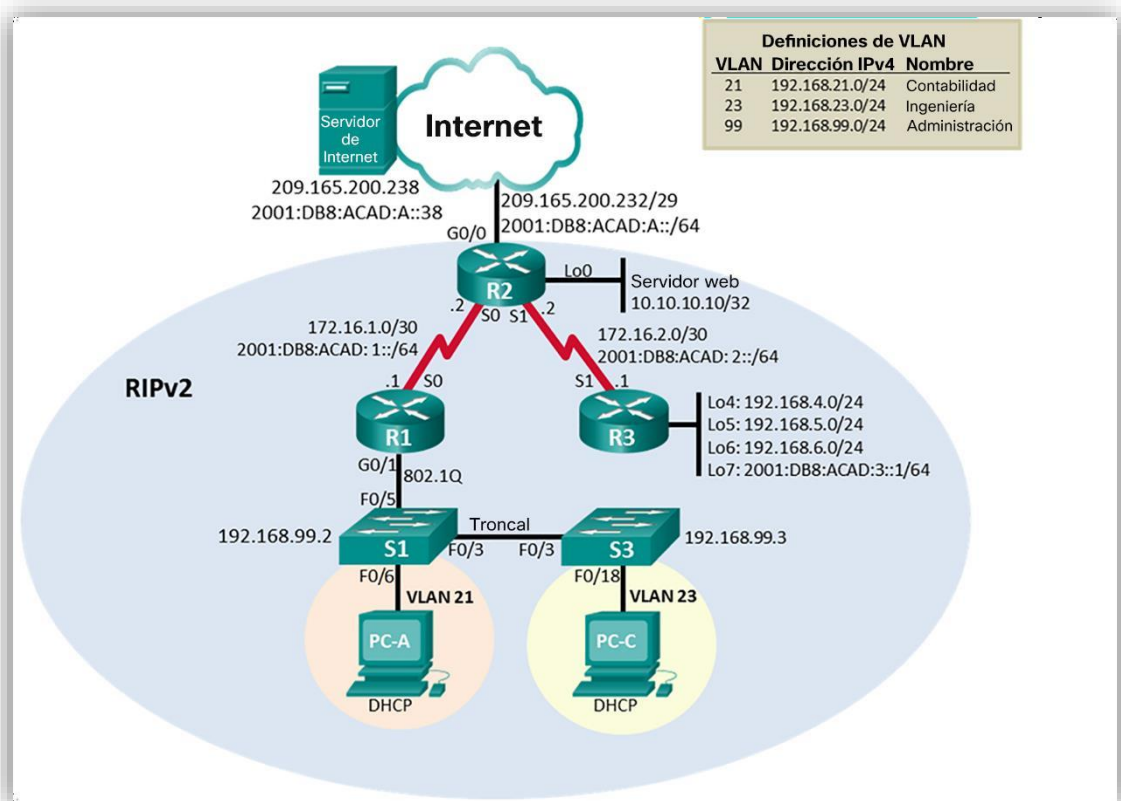
- ❖ Mediante Packet Tracer configurar una red pequeña para que admita conectividad IPV4 e IPV6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente
- ❖ Configurar e interconectar los dispositivos que se encuentran en dos ciudades utilizando el protocolo OSPF habilitar encapsulamiento PPP y su autenticación, proporcionar servicio DHCP en las LAN y habilitar NAT de sobrecarga

## 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

### 1.1 TOPOLOGÍA

Figura 1. Topología de Red. Escenario 1



### 1.2 INICIALIZAR DISPOSITIVOS

#### 1.2.1 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. Inicializar y volver a cargar los R y S

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

### 1.3 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

#### 1.3.1 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. Configurar la computadora de Internet

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
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:A::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.

### 1.3.2 CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ no ip domain-lookup</li> </ul>
Nombre del router	<ul style="list-style-type: none"> <li>❖ hostname r1</li> </ul>
Contraseña de exec privilegiado cifrada	<ul style="list-style-type: none"> <li>❖ enable secret class</li> </ul>
Contraseña de acceso a la consola	<ul style="list-style-type: none"> <li>❖ line console 0</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>
Contraseña de acceso Telnet	<ul style="list-style-type: none"> <li>❖ line vty 0 15</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>
Cifrar las contraseñas de texto no cifrado	<ul style="list-style-type: none"> <li>❖ service password-encryption</li> </ul>
Mensaje MOTD	<ul style="list-style-type: none"> <li>❖ banner motd %se prohíbe el acceso no autorizado%</li> </ul>
Interfaz S0/0/0	Establezca la descripción <ul style="list-style-type: none"> <li>❖ interface s0/0/0</li> <li>❖ description conexión a r2</li> </ul> Establecer la dirección ipv4 consultar el diagrama de topología para conocer la información de direcciones <ul style="list-style-type: none"> <li>❖ ip address 172.16.1.1 255.255.255.252</li> <li>❖ no shutdown</li> </ul>

	<p>Establecer la dirección ipv6 consultar el diagrama de topología para conocer la información de direcciones</p> <ul style="list-style-type: none"> <li>❖ ipv6 address 2001:db8:acad:1::1/64</li> <li>establecer la frecuencia de reloj en 128000</li> <li>❖ clock rate 128000</li> <li>activar la interfaz</li> <li>❖ no shutdown</li> <li>❖ exit</li> </ul>
Rutas predeterminadas	<p>Configurar una ruta IPv4 predeterminada de S0/0/0</p> <ul style="list-style-type: none"> <li>❖ ip route 0.0.0.0 0.0.0.0 s0/0/0</li> </ul> <p>configurar una ruta ipv6 predeterminada de s0/0/0</p> <ul style="list-style-type: none"> <li>❖ ipv6 route ::/0 s0/0/0</li> </ul>

**Nota:** Todavía no configure G0/1.

### 1.3.3 CONFIGURAR R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ no ip domain-lookup</li> </ul>
Nombre del router	<ul style="list-style-type: none"> <li>❖ hostname r2</li> </ul>
Contraseña de exec privilegiado cifrada	<ul style="list-style-type: none"> <li>❖ enable secret class</li> </ul>
Contraseña de acceso a la consola	<ul style="list-style-type: none"> <li>❖ line console 0</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>
Contraseña de acceso Telnet	<ul style="list-style-type: none"> <li>❖ line vty 0 15</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>

Cifrar las contraseñas de texto no cifrado	❖ service password-encryption
Habilitar el servidor HTTP	❖ ip http server
Mensaje MOTD	❖ banner motd %se prohíbe el acceso no autorizado%
Interfaz S0/0/0	<p>Establezca la descripción</p> <ul style="list-style-type: none"> <li>❖ interface s0/0/0</li> <li>❖ description conexión a R1</li> </ul> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <ul style="list-style-type: none"> <li>❖ ip address 172.16.1.2 255.255.255.252</li> </ul> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <ul style="list-style-type: none"> <li>❖ ipv6 address 2001:db8:acad:1::2/64</li> </ul> <p>Activar la interfaz</p> <ul style="list-style-type: none"> <li>❖ no shutdown</li> </ul>
Interfaz S0/0/1	<p>Establecer la descripción</p> <ul style="list-style-type: none"> <li>❖ interface s0/0/1</li> <li>❖ description Conexión a R3</li> </ul> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <ul style="list-style-type: none"> <li>❖ ip address 172.16.2.2 255.255.255.252</li> </ul> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <ul style="list-style-type: none"> <li>❖ ipv6 address 2001:db8:acad:2::2/64</li> </ul> <p>Establecer la frecuencia de reloj en 128000.</p> <ul style="list-style-type: none"> <li>❖ clock rate 128000</li> </ul> <p>Activar la interfaz</p> <ul style="list-style-type: none"> <li>❖ no shutdown</li> </ul>

Interfaz G0/0 (simulación de Internet)	<p>Establecer la descripción.</p> <ul style="list-style-type: none"> <li>❖ interface g0/0</li> <li>❖ description conexión a internet</li> </ul> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <ul style="list-style-type: none"> <li>❖ ip address 209.165.200.233 255.255.255.248</li> </ul> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <ul style="list-style-type: none"> <li>❖ ipv6 address 2001:db8:acad:a::1/64</li> </ul> <p>Activar la interfaz</p> <ul style="list-style-type: none"> <li>❖ no shutdown</li> </ul>
Interfaz loopback 0 (servidor web simulado)	<p>Establecer la descripción.</p> <ul style="list-style-type: none"> <li>❖ interface loopback 0</li> <li>❖ description servidor web simulado</li> </ul> <p>Establezca la dirección IPv4.</p> <ul style="list-style-type: none"> <li>❖ ip address 10.10.10.10 255.255.255.255</li> <li>❖ exit</li> </ul>
Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <ul style="list-style-type: none"> <li>❖ ip route 0.0.0.0 0.0.0.0 g0/0</li> </ul> <p>Configure una ruta IPv6 predeterminada de G0/0.</p> <ul style="list-style-type: none"> <li>❖ ipv6 route ::/0 g0/0</li> </ul>

### 1.3.4 CONFIGURAR R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configurar R3

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ no ip domain-lookup</li> </ul>



Nombre del router	❖ hostname r3
Contraseña de exec privilegiado cifrada	❖ enable secret class
Contraseña de acceso a la consola	❖ line console 0 ❖ password cisco ❖ login
Contraseña de acceso Telnet	❖ line vty 0 15 ❖ password cisco ❖ login
Cifrar las contraseñas de texto no cifrado	❖ service password-encryption
Mensaje MOTD	❖ banner motd %se prohíbe el acceso no autorizado.%
Interfaz S0/0/1	Establecer la descripción ❖ interface s0/0/1 ❖ description conexión r2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. ❖ ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz ❖ no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ❖ interface loopback 4 ❖ ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ❖ interface loopback 5 ❖ ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ❖ interface loopback 6 ❖ ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7	<p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <ul style="list-style-type: none"> <li>❖ interface loopback 7</li> <li>ipv6 address 2001:db8:acad:3::1/64</li> </ul>
Rutas predeterminadas	<p>Configure una ruta IPv4 predeterminada de s0/0/1</p> <ul style="list-style-type: none"> <li>❖ ip route 0.0.0.0 0.0.0.0 s0/0/1</li> </ul> <p>Configure una ruta IPv6 predeterminada de s0/0/1</p> <ul style="list-style-type: none"> <li>❖ ipv6 route ::/0 s0/0/1</li> </ul>

### 1.3.5 CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ no ip domain-lookup</li> </ul>
Nombre del switch	<ul style="list-style-type: none"> <li>❖ hostname s1</li> </ul>
Contraseña de exec privilegiado cifrada	<ul style="list-style-type: none"> <li>❖ enable secret class</li> </ul>
Contraseña de acceso a la consola	<ul style="list-style-type: none"> <li>❖ line console 0</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>
Contraseña de acceso Telnet	<ul style="list-style-type: none"> <li>❖ line vty 0 15</li> <li>❖ password cisco</li> <li>❖ login</li> </ul>
Cifrar las contraseñas de texto no cifrado	<ul style="list-style-type: none"> <li>❖ service password-encryption</li> </ul>
Mensaje MOTD	<ul style="list-style-type: none"> <li>❖ banner motd %se prohíbe el acceso no autorizado%</li> </ul>

### 1.3.6 CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<ul style="list-style-type: none"><li>❖ enable</li><li>❖ configure terminal</li><li>❖ no ip domain-lookup</li></ul>
Nombre del switch	<ul style="list-style-type: none"><li>❖ hostname s3</li></ul>
Contraseña de exec privilegiado cifrada	<ul style="list-style-type: none"><li>❖ enable secret class</li></ul>
Contraseña de acceso a la consola	<ul style="list-style-type: none"><li>❖ line console 0</li><li>❖ password cisco</li><li>❖ login</li></ul>
Contraseña de acceso Telnet	<ul style="list-style-type: none"><li>❖ line vty 0 15</li><li>❖ password cisco</li><li>❖ login</li></ul>
Cifrar las contraseñas de texto no cifrado	<ul style="list-style-type: none"><li>❖ service password-encryption</li></ul>
Mensaje MOTD	<ul style="list-style-type: none"><li>❖ banner motd %se prohíbe el acceso no autorizado%</li></ul>

### 1.3.7 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 8. Verificar la Conectividad de la Red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio (véase anexo 1)
R2	R3, S0/0/1	172.16.2.1	Satisfactorio (véase anexo 2)
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio (véase anexo 3)

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

#### 1.4 CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

##### 1.4.1 CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configurar la Seguridad. Configurar 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 <ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ vlan 21</li> <li>❖ name contabilidad</li> <li>❖ vlan 23</li> <li>❖ name ingenieria</li> <li>❖ vlan 99</li> <li>❖ name administracion</li> <li>❖ exit</li> </ul>

Asignar la dirección IP de administración.	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología</p> <ul style="list-style-type: none"> <li>❖ interface vlan 99</li> <li>❖ ip address 192.168.99.2 255.255.255.0</li> <li>❖ no shutdown</li> <li>❖ exit</li> </ul>
Asignar el gateway predeterminado	<p>Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.</p> <ul style="list-style-type: none"> <li>❖ Ip default-gateway 192.168.99.1</li> </ul>
Forzar el enlace troncal en la interfaz F0/3	<p>Utilizar la red VLAN 1 como VLAN nativa</p> <ul style="list-style-type: none"> <li>❖ interface f0/3</li> <li>❖ switchport mode trunk</li> <li>❖ switchport trunk native vlan 1</li> </ul>
Forzar el enlace troncal en la interfaz F0/5	<p>Utilizar la red VLAN 1 como VLAN nativa</p> <ul style="list-style-type: none"> <li>❖ interface f0/5</li> <li>❖ switchport mode trunk</li> <li>❖ switchport trunk native vlan 1</li> </ul>
Configurar el resto de los puertos como puertos de acceso	<p>Utilizar el comando interface range</p> <ul style="list-style-type: none"> <li>❖ interface range f0/1-2, f0/4, f0/6-24, g0/1-2</li> <li>❖ switchport mode access</li> </ul>
Asignar F0/6 a la VLAN 21	<ul style="list-style-type: none"> <li>❖ interface f0/6</li> <li>❖ switchport access vlan 21</li> </ul>
Apagar todos los puertos sin usar	<ul style="list-style-type: none"> <li>❖ interface range f0/1-2, f0/4, f0/7-24, g0/1-2</li> <li>❖ shutdown</li> </ul>

#### 1.4.2 CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configurar la Seguridad. Configurar 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. ❖ enable ❖ configure terminal ❖ vlan 21 ❖ name accounting ❖ vlan 23 ❖ name engineering ❖ vlan 99 ❖ name management ❖ exit
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 ❖ interface vlan 99 ❖ ip address 192.168.99.3 255.255.255.0 ❖ no shutdown ❖ exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. ❖ Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa ❖ interface f0/3 ❖ switchport mode trunk ❖ switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range ❖ interface range f0/1-2, f0/4-24, g0/1-2 ❖ switchport mode access
Asignar F0/18 a la VLAN 23	❖ interface f0/18 ❖ switchport access vlan 23

Apagar todos los puertos sin usar	<ul style="list-style-type: none"> <li>❖ interface-range f0/1-2, f0/4-17, f0/19-24, g0/1-2</li> <li>❖ shutdown</li> </ul>
-----------------------------------	---

### 1.4.3 CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar la Seguridad. Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz</p> <ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ interface g0/1.21</li> <li>❖ description lan de contabilidad</li> <li>❖ encapsulation dot1q 21</li> <li>❖ ip address 192.168.21.1 255.255.255.0</li> </ul>
Configurar la subinterfaz 802.1Q .23 en G0/1	<p>Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz</p> <ul style="list-style-type: none"> <li>❖ interface g0/1.23</li> <li>❖ description lan de ingenieria</li> <li>❖ encapsulation dot1q 23</li> <li>❖ ip address 192.168.23.1 255.255.255.0</li> </ul>
Configurar la subinterfaz 802.1Q .99 en G0/1	<p>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</p> <ul style="list-style-type: none"> <li>❖ interface g0/1.99</li> <li>❖ description lan de administracion</li> <li>❖ encapsulation dot1q 99</li> <li>❖ ip address 192.168.99.1 255.255.255.0</li> </ul>

Activar la interfaz G0/1	❖ int g0/1 ❖ no shutdown
--------------------------	-----------------------------

#### 1.4.4 VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. 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 12. Configurar la Seguridad. Verificar la Conectividad de la Red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio (véase anexo 4)
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio (véase anexo 5)
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio (véase anexo 4)
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio (véase anexo 5)

### 1.5 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

#### 1.5.1 CONFIGURAR RIPV2 EN EL R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configurar RIPV2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	❖ enable ❖ configure terminal ❖ router rip ❖ versión 2 ❖ do show ip route connected



Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. ❖ network 172.16.1.0 ❖ network 192.168.21.0 ❖ network 192.168.23.0 ❖ network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	❖ passive-interface g0/1.21 ❖ passive-interface g0/1.23 ❖ passive-interface g0/1.99
Desactive la sumarización automática	❖ no auto-summary

### 1.5.2 CONFIGURAR RIPV2 EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configurar RIPV2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	❖ enable ❖ configure terminal ❖ router rip ❖ versión 2 ❖ do show ip route connected
Anunciar las redes conectadas directamente	<b>Nota:</b> Omitir la red G0/0. ❖ network 10.10.10.10 ❖ network 172.16.1.0 ❖ network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	❖ passive-interface loopback 0
Desactive la sumarización automática.	❖ no auto-summary

### 1.5.3 CONFIGURAR RIPV3 EN EL R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configurar RIPV3 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ router rip</li> <li>❖ versión 2</li> <li>❖ do show ip route connected</li> </ul>
Anunciar redes IPv4 conectadas directamente	<ul style="list-style-type: none"> <li>❖ network 172.16.2.0</li> <li>❖ network 192.168.4.0</li> <li>❖ network 192.168.5.0</li> <li>❖ network 192.168.6.0</li> </ul>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<ul style="list-style-type: none"> <li>❖ passive-interface loopback 4</li> <li>❖ passive-interface loopback 5</li> <li>❖ passive-interface loopback 6</li> </ul>
Desactive la sumarización automática.	<ul style="list-style-type: none"> <li>❖ no auto-summary</li> </ul>

#### 1.5.4 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 16. Verificar la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ show ip protocols</li> <li>❖ para los resultados (véase anexo 6)</li> </ul>
¿Qué comando muestra solo las rutas RIP?	<ul style="list-style-type: none"> <li>❖ show ip route rip</li> <li>❖ para los resultados (véase anexo 6)</li> </ul>

¿Qué comando muestra la sección de RIP de la configuración en ejecución?	<ul style="list-style-type: none"> <li>❖ show run   section router rip</li> <li>❖ para los resultados (véase anexo 7)</li> </ul>
--	--

## 1.6 IMPLEMENTAR DHCP Y NAT PARA IPV4

### 1.6.1 CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configurar el R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	<ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ ip dhcp excluded-address 192.168.21.1 192.168.21.20</li> </ul>
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	<ul style="list-style-type: none"> <li>❖ ip dhcp excluded-address 192.168.23.1 192.168.23.20</li> </ul>
Crear un pool de DHCP para la VLAN 21.	<p>Nombre: ACCT  Servidor DNS: 10.10.10.10  Nombre de dominio: ccna-sa.com  Establecer el gateway predeterminado</p> <ul style="list-style-type: none"> <li>❖ ip dhcp pool acct</li> <li>❖ network 192.168.21.0 255.255.255.0</li> <li>❖ default-router 192.168.21.1</li> <li>❖ dns-server 10.10.10.10</li> <li>❖ domain-name ccna-sa.com</li> </ul>

<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Nombre: ENGNR          Servidor DNS: 10.10.10.10          Nombre de dominio: ccna-sa.com          Establecer el gateway predeterminado</p> <ul style="list-style-type: none"> <li>❖ ip dhcp pool engnr</li> <li>❖ network 192.168.23.0 255.255.255.0</li> <li>❖ default-router 192.168.23.1</li> <li>❖ dns-server 10.10.10.10</li> <li>❖ domain-name ccna-sa.com</li> </ul>
--	--

### 1.6.2 CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configurar la NAT estática y dinámica en el R2

<p><b>Elemento o tarea de configuración</b></p>	<p><b>Especificación</b></p>
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: <b>webuser</b>            Contraseña: <b>cisco12345</b>            Nivel de privilegio: <b>15</b></p> <ul style="list-style-type: none"> <li>❖ enable</li> <li>❖ configure terminal</li> <li>❖ username webuser privilege 15 secret cisco12345</li> </ul>
<p>Habilitar el servicio del servidor HTTP</p>	<ul style="list-style-type: none"> <li>❖ ip http server</li> </ul>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<ul style="list-style-type: none"> <li>❖ ip http authentication local</li> </ul>
<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: <b>209.165.200.237</b></p> <ul style="list-style-type: none"> <li>❖ ip nat inside source static 10.10.10.10 209.165.200.237</li> </ul>

Asignar la interfaz interna y externa para la NAT estática	<ul style="list-style-type: none"> <li>❖ interface g0/0</li> <li>❖ ip nat outside</li> <li>❖ interface s0/0/0</li> <li>❖ ip nat inside</li> <li>❖ interface s0/0/1</li> <li>❖ ip nat inside</li> <li>❖ exit</li> </ul>
Configurar la NAT dinámica dentro de una ACL privada	<p>Lista de acceso: 1</p> <p>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1</p> <p>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3</p> <ul style="list-style-type: none"> <li>❖ access-list 1 permit 192.168.21.0 0.0.0.255</li> <li>❖ access-list 1 permit 192.168.23.0 0.0.0.255</li> <li>❖ access-list 1 permit 192.168.4.0 0.0.3.255</li> </ul>
Defina el pool de direcciones IP públicas utilizables.	<p>Nombre del conjunto: <b>INTERNET</b></p> <p>El conjunto de direcciones incluye:</p> <p><b>209.165.200.233 – 209.165.200.236</b></p> <ul style="list-style-type: none"> <li>❖ ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248</li> </ul>
Definir la traducción de NAT dinámica	<ul style="list-style-type: none"> <li>❖ ip nat inside source list 1 pool INTERNET</li> </ul>

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

Tabla 19. Verificar el Protocolo DHCP y la NAT Estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio. (Véase anexo 8)

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	❖ Satisfactorio. (Véase anexo 8)
Verificar que la PC-A pueda hacer ping a la PC-C <b>Nota:</b> Quizá sea necesario deshabilitar el firewall de la PC.	❖ Satisfactorio. (Véase anexo 9)
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 <b>webuser</b> y la contraseña <b>cisco12345</b>	❖ Satisfactorio. (Véase anexo 10)

## 1.7 CONFIGURAR NTP

Tabla 20. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	<b>5 de marzo de 2016, 9 a. m.</b> ❖ enable ❖ clock set 09:00:00 05 mar 2016
Configure R2 como un maestro NTP.	Nivel de estrato: <b>5</b> ❖ configure terminal ❖ ntp master 5
Configurar R1 como un cliente NTP.	Servidor: <b>R2</b> ❖ enable ❖ configure terminal ❖ ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	❖ ntp update-calendar ❖ end

Verifique la configuración de NTP en R1.	❖ show ntp associations (Véase anexo 11)
--	---

## 1.8 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

### 1.8.1 RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Tabla 21. Restringir el acceso a las líneas 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	Nombre de la ACL: <b>ADMIN-MGT</b> ❖ enable ❖ configure terminal ❖ ip access-list standard ADMIN-MGT ❖ permit host 172.16.1.1 ❖ exit
Aplicar la ACL con nombre a las líneas VTY	❖ line vty 0 15 ❖ access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	❖ transport input telnet
Verificar que la ACL funcione como se espera	❖ R1#telnet 172.16.1.2 (Véase anexo 12) ❖ R3#telnet 172.16.1.2 (Véase anexo 12)

### 1.8.2 INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

Tabla 22. Introducir el comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	❖ R2#show ip access-list (Véase anexo 13)
Restablecer los contadores de una lista de acceso	❖ R2#clear ip access-list (PT no soporta este comando)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	❖ R2#show ip interface (Véase anexo 13)
¿Con qué comando se muestran las traducciones NAT?	<p><b>Nota:</b> 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>❖ R2#Show ip nat translations (Véase anexo 14)</p>
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	❖ R2#clear ip nat translation * (Véase anexo 14)

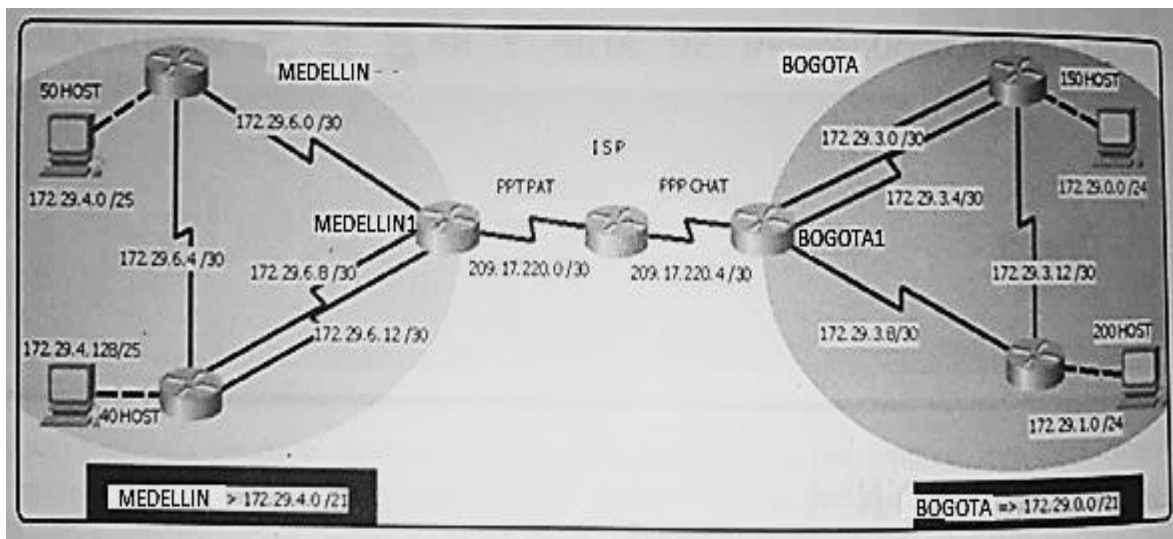


## 2 ESCENARIO 2

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.

### 2.1 TOPOLOGÍA DE RED

Figura 2. Topología de Red. 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 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.

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).

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

#### 2.1.1 CONFIGURACIÓN BÁSICA DE ROUTER

- ❖ enable
- ❖ configure terminal
- ❖ no ip domain-lookup
- ❖ hostname ISP
- ❖ enable secret class
- ❖ line console 0
- ❖ password cisco
- ❖ login
- ❖ line vty 0 15
- ❖ password cisco
- ❖ login
- ❖ service password-encryption
- ❖ banner motd %prohibido el acceso no autorizado%
- ❖ copy running-config startup-config

### 2.1.2 DIRECCIONAMIENTO

- ❖ ISP(config)#int s0/0/0
- ❖ ISP(config-if)#ip address 209.17.220.1 255.255.255.252
- ❖ ISP(config-if)#clock rate 128000
- ❖ ISP(config-if)#no shut
  
- ❖ ISP(config-if)#int s0/0/1
- ❖ ISP(config-if)#ip address 209.17.220.5 255.255.255.252
- ❖ ISP(config-if)#clock rate 128000
- ❖ ISP(config-if)#no shut
  
- ❖ MEDELLIN1(config)#int s0/0/0
- ❖ MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
- ❖ MEDELLIN1(config-if)#no shut
  
- ❖ MEDELLIN1(config-if)#int s0/0/1
- ❖ MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
- ❖ MEDELLIN1(config-if)#clock rate 128000
- ❖ MEDELLIN1(config-if)#no shut
  
- ❖ MEDELLIN1(config-if)#int s0/1/0
- ❖ MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
- ❖ MEDELLIN1(config-if)#clock rate 128000
- ❖ MEDELLIN1(config-if)#no shut
  
- ❖ MEDELLIN1(config-if)#int s0/1/1
- ❖ MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
- ❖ MEDELLIN1(config-if)#clock rate 128000
- ❖ MEDELLIN1(config-if)#no shut

- ❖ MEDELLIN2(config)#int s0/0/0
- ❖ MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
- ❖ MEDELLIN2(config-if)#no shut
  
- ❖ MEDELLIN2(config-if)#int s0/0/1
- ❖ MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
- ❖ MEDELLIN2(config-if)#clock rate 128000
- ❖ MEDELLIN2(config-if)#no shut
  
- ❖ MEDELLIN2(config-if)#int g0/0
- ❖ MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
- ❖ MEDELLIN2(config-if)#no shut
  
- ❖ MEDELLIN3(config)#int s0/0/0
- ❖ MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
- ❖ MEDELLIN3(config-if)#no shut
  
- ❖ MEDELLIN3(config-if)#int s0/0/1
- ❖ MEDELLIN3(config-if)#ip address 172.29.2.14 255.255.255.252
- ❖ MEDELLIN3(config-if)#no shut
  
- ❖ MEDELLIN3(config-if)#int s0/1/0
- ❖ MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
- ❖ MEDELLIN3(config-if)#no shut
  
- ❖ MEDELLIN3(config-if)#int g0/0
- ❖ MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
- ❖ MEDELLIN3(config-if)#no shut
  
- ❖ BOGOTA1(config)#int s0/0/0
- ❖ BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
- ❖ BOGOTA1(config-if)#no shut
  
- ❖ BOGOTA1(config-if)#int s0/0/1
- ❖ BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
- ❖ BOGOTA1(config-if)#clock rate 128000
- ❖ BOGOTA1(config-if)#no shut
  
- ❖ BOGOTA1(config-if)#int s0/1/0
- ❖ BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
- ❖ BOGOTA1(config-if)#clock rate 128000
- ❖ BOGOTA1(config-if)#no shut
  
- ❖ BOGOTA1(config-if)#int s0/1/1

- ❖ BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
- ❖ BOGOTA1(config-if)#clock rate 128000
- ❖ BOGOTA1(config-if)#no shut
  
- ❖ BOGOTA2(config)#int s0/0/0
- ❖ BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
- ❖ BOGOTA2(config-if)#no shut
  
- ❖ BOGOTA2(config-if)#int s0/0/1
- ❖ BOGOTA2(config-if)#ip address 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 address 172.29.1.1 255.255.255.0
- ❖ BOGOTA2(config-if)#no shut
  
- ❖ BOGOTA3(config)#int s0/0/0
- ❖ BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
- ❖ BOGOTA3(config-if)#no shut
  
- ❖ BOGOTA3(config-if)#int s0/0/1
- ❖ BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
- ❖ BOGOTA3(config-if)#no shut
  
- ❖ BOGOTA3(config-if)#int s0/1/0
- ❖ BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
- ❖ BOGOTA3(config-if)#no shut
  
- ❖ BOGOTA3(config-if)#int g0/0
- ❖ BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
- ❖ BOGOTA3(config-if)#no shut

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

## 2.2 CONFIGURACIÓN DEL ENRUTAMIENTO

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

- ❖ MEDELLIN1(config)#router ospf 1
- ❖ MEDELLIN1(config-router)#net 172.29.6.0 0.0.0.3 area 0
- ❖ MEDELLIN1(config-router)#net 172.29.6.8 0.0.0.3 area 0
- ❖ MEDELLIN1(config-router)#net 172.29.6.12 0.0.0.3 area 0

- ❖ MEDELLIN2(config)#router ospf 1
- ❖ MEDELLIN2(config-router)#net 172.29.4.0 0.0.0.255 area 0
- ❖ MEDELLIN2(config-router)#net 172.29.6.0 0.0.0.3 area 0
- ❖ MEDELLIN2(config-router)#net 172.29.6.4 0.0.0.3 area 0
  
- ❖ MEDELLIN3(config)#router ospf 1
- ❖ MEDELLIN3(config-router)#net 172.29.4.128 0.0.0.255 area 0
- ❖ MEDELLIN3(config-router)#net 172.29.6.4 0.0.0.3 area 0
- ❖ MEDELLIN3(config-router)#net 172.29.6.8 0.0.0.3 area 0
- ❖ MEDELLIN3(config-router)#net 172.29.6.12 0.0.0.3 area 0
  
- ❖ BOGOTA1(config)#router ospf 1
- ❖ BOGOTA1(config-router)#net 172.29.3.0 0.0.0.3 area 1
- ❖ BOGOTA1(config-router)#net 172.29.3.4 0.0.0.3 area 1
- ❖ BOGOTA1(config-router)#net 172.29.3.8 0.0.0.3 area 1
  
- ❖ BOGOTA2(config)#router ospf 1
- ❖ BOGOTA2(config-router)#net 172.29.1.0 0.0.0.255 area 1
- ❖ BOGOTA2(config-router)#net 172.29.3.8 0.0.0.3 area 1
- ❖ BOGOTA2(config-router)#net 172.29.3.12 0.0.0.3 area 1
  
- ❖ BOGOTA3(config)#router ospf 1
- ❖ BOGOTA3(config-router)#net 172.29.0.0 0.0.0.255 area 1
- ❖ BOGOTA3(config-router)#net 172.29.3.0 0.0.0.3 area 1
- ❖ BOGOTA3(config-router)#net 172.29.3.4 0.0.0.3 area 1
- ❖ BOGOTA3(config-router)#net 172.29.3.12 0.0.0.3 area 1

Los routers Bogota1 y Medellín1 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
- ❖ MEDELLIN1(config)#router ospf 1
- ❖ MEDELLIN1(config-router)#default-information originate
- ❖ MEDELLIN1(config-router)#exit
  
- ❖ BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
- ❖ BOGOTA1(config)#router ospf 1
- ❖ BOGOTA1(config-router)#default-information originate
- ❖ BOGOTA1(config-router)#exit

Con el comando show ip route se puede comprobar los caminos para conectarse con ISP (véase anexo 15)

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

Tabla 23. Red Sumarizada. Medellín

10101100	00011101	00000100	00000000	172.29.4.0/25
10101100	00011101	00000100	10000000	172.29.4.128/25
10101100	00011101	00000110	00000100	172.29.6.4/30
10101100	00011101	00000110	00001000	172.29.6.8/30
10101100	00011101	00000110	00001100	172.29.6.12/30
10101100	00011101	00000110	00000000	172.29.6.0/30
<b>10101100</b>	<b>00011101</b>	<b>00000100</b>	<b>00000000</b>	<b>172.29.4.0/22</b>

Tabla 24. Red sumarizada. Bogotá

10101100	00011101	00000000	00000000	172.29.0.0/24
10101100	00011101	00000001	00000000	172.29.1.0/24
10101100	00011101	00000011	00001100	172.29.3.12/30
10101100	00011101	00000011	00001000	172.29.3.8/30
10101100	00011101	00000011	00000000	172.29.3.0/30
10101100	00011101	00000011	00000100	172.29.3.4/30
<b>10101100</b>	<b>00011101</b>	<b>00000000</b>	<b>00000000</b>	<b>172.29.0.0/22</b>

- ❖ ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
- ❖ ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

Con el comando ping, se comprueba conectividad entre Medellín y Bogotá (véase anexo 16)

### 2.3 TABLA DE ENRUTAMIENTO.

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

- ❖ Show ip route (véase anexo 17)

Verificar el balanceo de carga que presentan los routers.

- ❖ Show ip route

Se comprueba que para un destino tiene dos interfaces (véase anexo 18)

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.

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

- ❖ Show ip route (véase anexo 17-18)

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

- ❖ El balanceo de carga hace referencia a rutas redundantes. (véase anexo 18)

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

- ❖ ISP#Show ip route (véase anexo 19)

## 2.4 DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

Tabla 25. Deshabilitar la Propagación del Protocolo OSPF

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

- ❖ BOGOTA1(config)#router ospf 1
- ❖ BOGOTA1(config-router)#passive-interface s0/0/0
  
- ❖ BOGOTA2(config)#router ospf 1

- ❖ BOGOTA2(config-router)#passive-interface g0/0
- ❖ BOGOTA3(config)#router ospf 1
- ❖ BOGOTA3(config-router)#passive-interface g0/0
- ❖ MEDELLIN1(config)#router ospf 1
- ❖ MEDELLIN1(config-router)#passive-interface s0/0/0
- ❖ MEDELLIN2(config)#router ospf 1
- ❖ MEDELLIN2(config-router)#passive-interface g0/0
- ❖ MEDELLIN3(config)#router ospf 1
- ❖ MEDELLIN3(config-router)#passive-interface g0/0

## 2.5 VERIFICACIÓN DEL PROTOCOLO OSPF.

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

Para verificar el protocolo OSPF se utiliza el comando show ip protocols, el cual nos permite ver ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

- ❖ MEDELLIN1#show ip protocols (véase anexo 20)
- ❖ BOGOTA1#show ip protocols (véase anexo 20)

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.

A través del comando show ip ospf interface se puede obtener una lista detallada de todas las interfaces.

- ❖ BOGOTA3#show ip ospf interface (véase anexo 21)

## 2.6 CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

Según la topología se requiere que el enlace medellín1 con ISP sea configurado con autenticación PAP

- ❖ ISP(config)#username MEDELLIN1 password cisco
- ❖ ISP(config)#int s0/0/0
- ❖ ISP(config-if)#encapsulation ppp
- ❖ ISP(config-if)#



- ❖ ISP(config-if)#ppp authentication pap
- ❖ ISP(config-if)#ppp pap sent-username ISP password cisco
  
- ❖ MEDELLIN1(config)#username ISP password cisco
- ❖ MEDELLIN1(config)#int s0/0/0
- ❖ MEDELLIN1(config-if)#encapsulation ppp
- ❖ MEDELLIN1(config-if)#ppp authentication pap
- ❖ MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco

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

- ❖ ISP(config)#username BOGOTA1 password cisco
- ❖ ISP(config)#int s0/0/1
- ❖ ISP(config-if)#encapsulation ppp
- ❖ ISP(config-if)#ppp authentication chap
  
- ❖ BOGOTA1(config)#username ISP password cisco
- ❖ BOGOTA1(config)#int s0/0/0
- ❖ BOGOTA1(config-if)#encapsulation ppp
- ❖ BOGOTA1(config-if)#ppp authentication chap

## 2.7 CONFIGURACIÓN DE PAT.

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

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.

- ❖ MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
- ❖ MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
- ❖ MEDELLIN1(config)#int s0/0/0
- ❖ MEDELLIN1(config-if)#ip nat outside
- ❖ 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
- ❖ MEDELLIN1(config-if)#int s0/1/1
- ❖ MEDELLIN1(config-if)#ip nat inside

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

- ❖ BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
- ❖ 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

Se realiza prueba de ping y con el comando show ip nat translations se visualiza la traducción de la dirección automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1. (véase anexo 22)

## 2.8 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

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

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

- ❖ MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
- ❖ MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
- ❖ MEDELLIN2(config)#ip dhcp pool MEDELLIN2
- ❖ MEDELLIN2(dhcp-config)#net 172.29.4.0 255.255.255.128
- ❖ MEDELLIN2(dhcp-config)#default-router 172.29.4.1
- ❖ MEDELLIN2(dhcp-config)#dns-server 0.0.0.0
- ❖ MEDELLIN2(dhcp-config)#ex
- ❖
- ❖ MEDELLIN2(config)#ip dhcp pool MEDELLIN3
- ❖ MEDELLIN2(dhcp-config)#net 172.29.4.128 255.255.255.128
- ❖ MEDELLIN2(dhcp-config)#default-router 172.29.4.129
- ❖ MEDELLIN2(dhcp-config)#dens-server 0.0.0.0
- ❖ MEDELLIN2(dhcp-config)#dns-server 0.0.0.0

Acceso de PC1 a DHCP

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

Configuración IP DHCP en PC0 y PC1 véase anexo 23

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

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
❖ BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
❖ BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
❖ BOGOTA2(config)#ip dhcp pool BOGOTA2
❖ BOGOTA2(dhcp-config)#net 172.29.1.0 255.255.255.0
❖ BOGOTA2(dhcp-config)#default-router 172.29.1.1
❖ BOGOTA2(dhcp-config)#dns-server 0.0.0.0
❖ BOGOTA2(dhcp-config)#ex
❖
❖ BOGOTA2(config)#ip dhcp pool BOGOTA3
❖ BOGOTA2(dhcp-config)#net 172.29.0.0 255.255.255.0
❖ BOGOTA2(dhcp-config)#default-router 172.29.0.1
❖ BOGOTA2(dhcp-config)#dns-server 0.0.0.0
```

Acceso de PC2 a DHCP

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```

Configuración IP DHCP en PC2 y PC3 (véase anexo 24)

## CONCLUSIONES

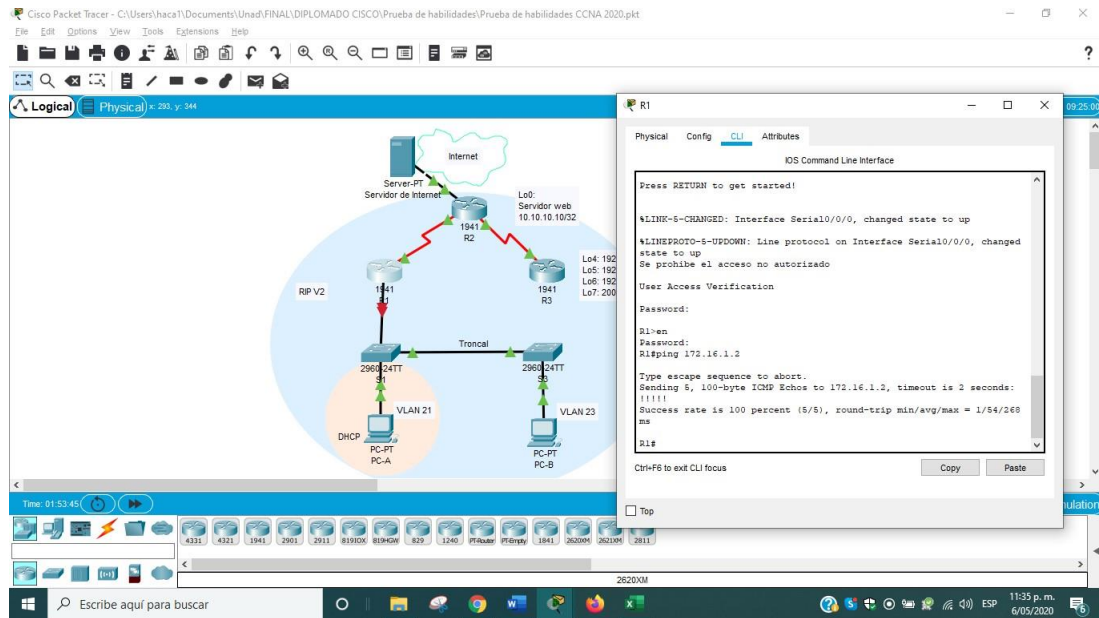
- ❖ Con el desarrollo del escenario (1) se logra configurar una red pequeña en donde acepta conectividad IPV4 e IPV6.
- ❖ Se configura la seguridad del switch, las VLAN y routing entre VLAN; además se logra utilizar el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (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
- ❖ Se obtiene el resultado esperado al configurar e interconectar los dispositivos que se encuentran en dos ciudades utilizando el protocolo OSPF y habilitando el encapsulamiento PPP y su autenticación, finalmente se proporciona el servicio DHCP en las LAN y se habilita NAT de sobrecarga en los router.

## BIBLIOGRAFÍA

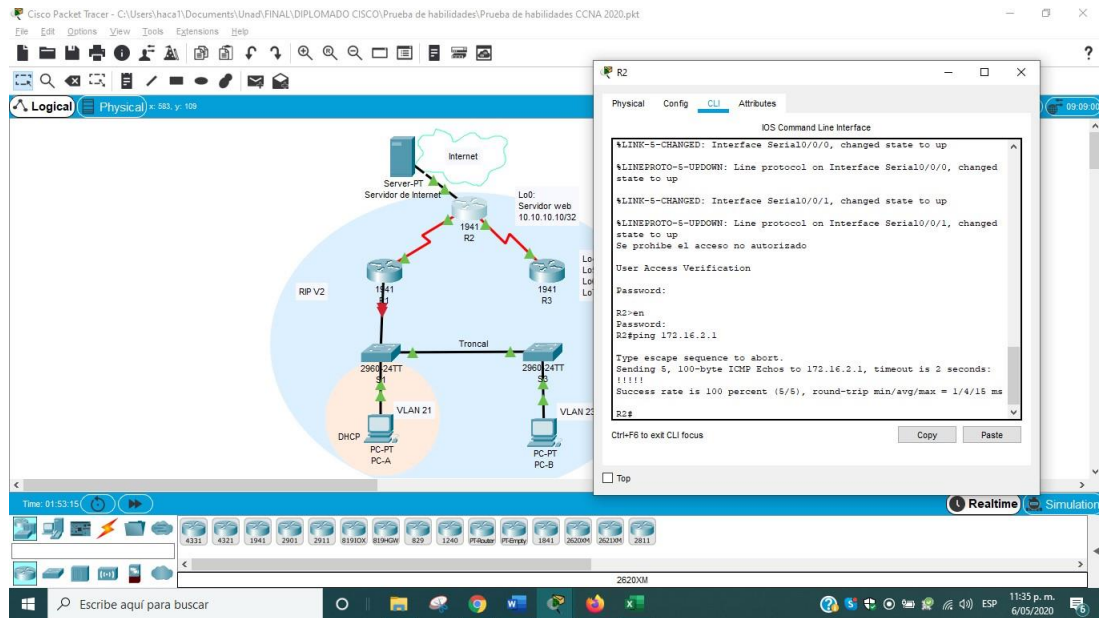
- ❖ Academy, Cisco Networking. (2020). *Servidores de DHCP y servidores DNS*. Obtenido de <https://www.netacad.com/es>
- ❖ Cisco Networking Academy. (2020). *Configuring Basic Single-Area OSPFv2*. Obtenido de <https://www.netacad.com/es>
- ❖ Di Tommaso, L. (28 de Febrero de 2010). *Mikro Ways*. Obtenido de Configuración de PPP y PAP en Cisco: <https://www.mikroways.net/2010/02/28/configuracion-de-ppp-y-pap-en-cisco/>
- ❖ Veato, v. (Mayo de 2015). *Redes locales y globales*. Obtenido de 6. Configuración del protocolo OSPF: <https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/6-configuracion-del-encaminamiento/2-encaminamiento-dinamico/6-protocolo-ospf/6-configuracion-del-protocolo-ospf>

# ANEXOS

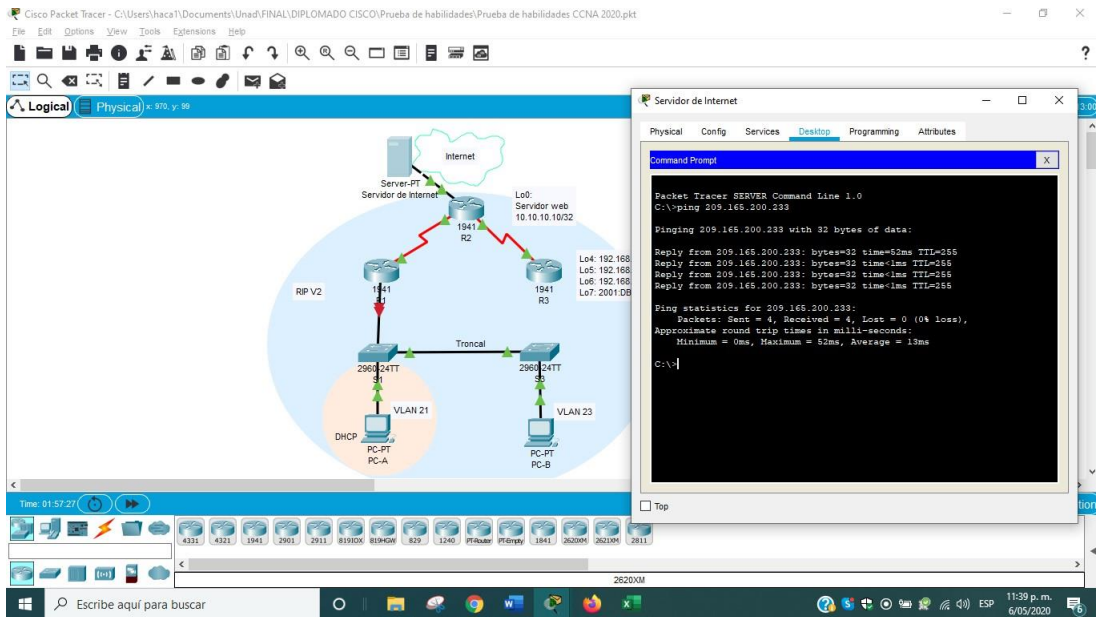
## Anexo 1. Registro Fotográfico. Ping R1 a R2



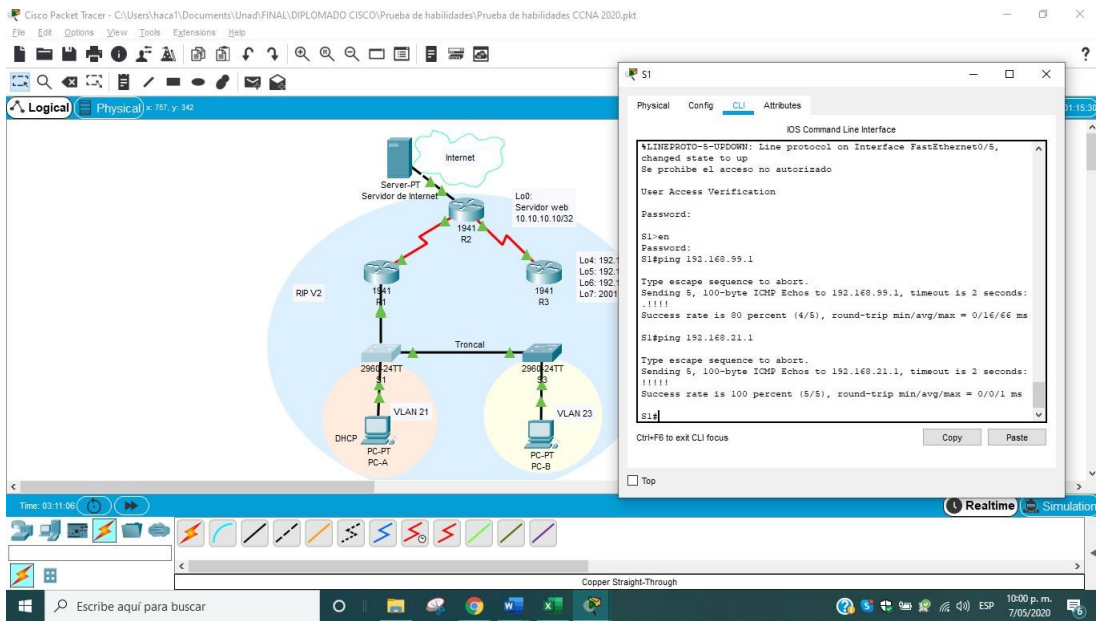
## Anexo 2. Registro Fotográfico. Ping R2 a R3



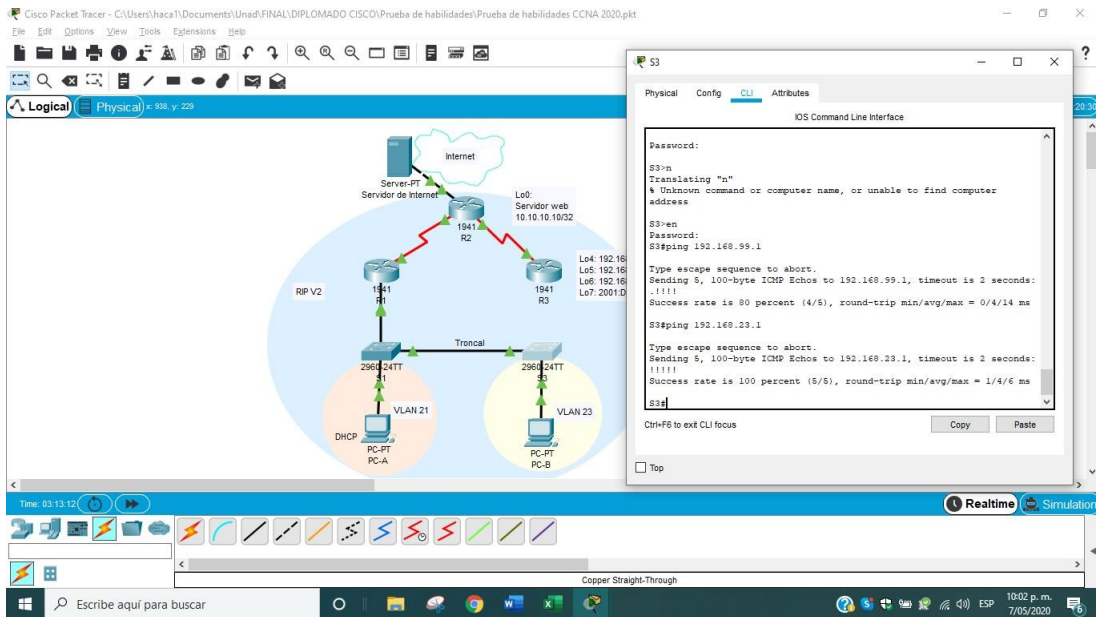
## Anexo 3. Registro Fotográfico. Ping PC de Internet a Gateway Predeterminado



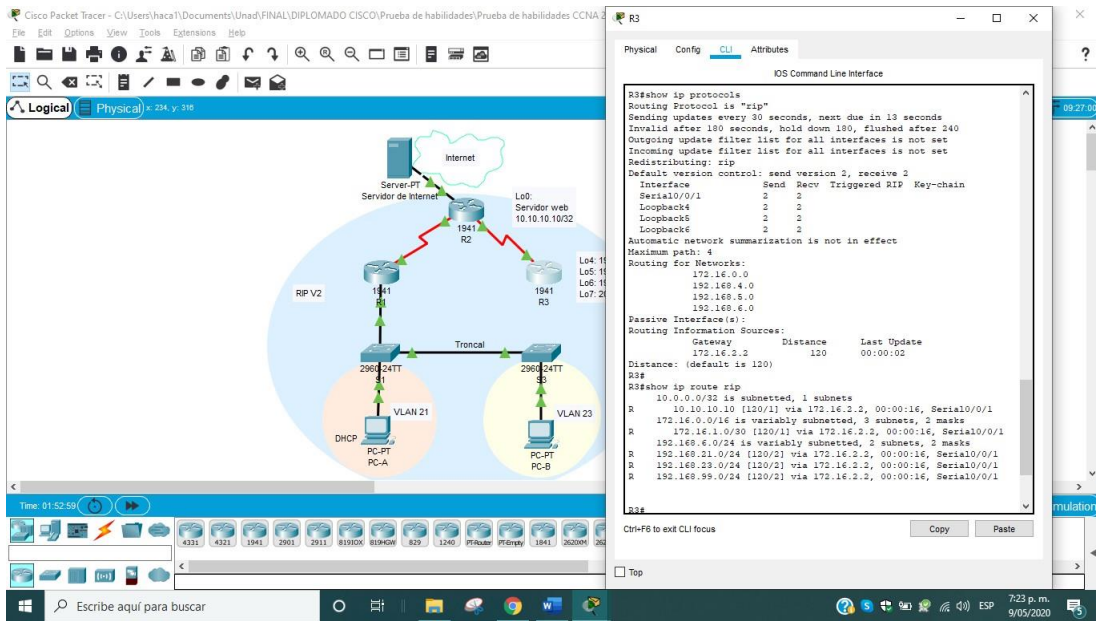
#### Anexo 4. Registro Fotográfico. Ping S1 a R1 Dirección VLAN 99 - 21



#### Anexo 5. Registro Fotográfico. Ping S3 a R1 Dirección VLAN 99 - 23

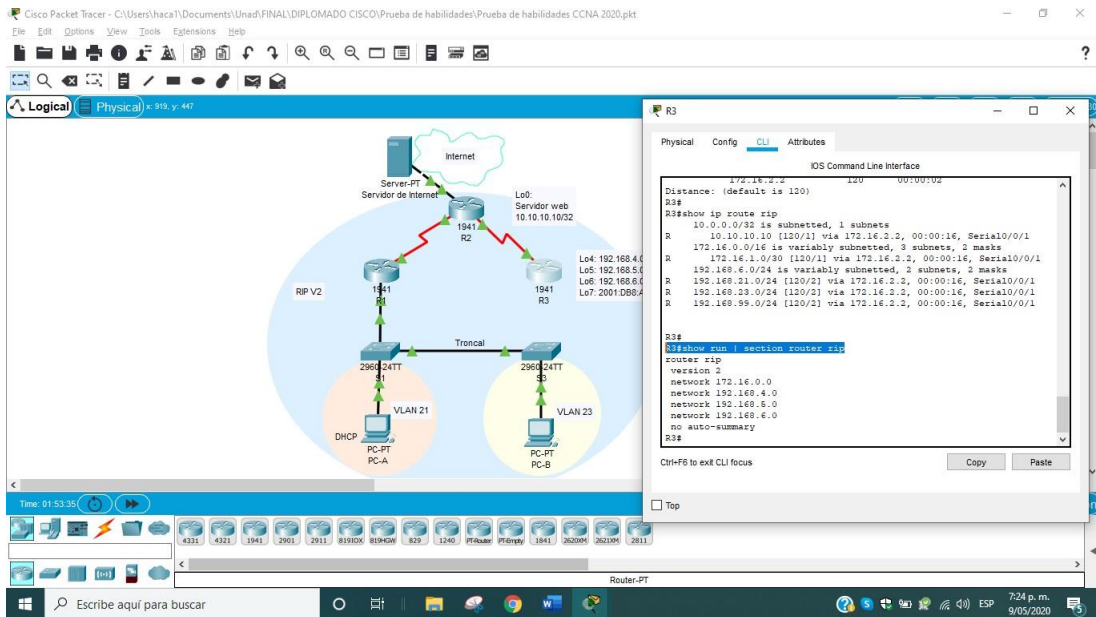


## Anexo 6. Registro Fotográfico. Verificar la Información de RIP

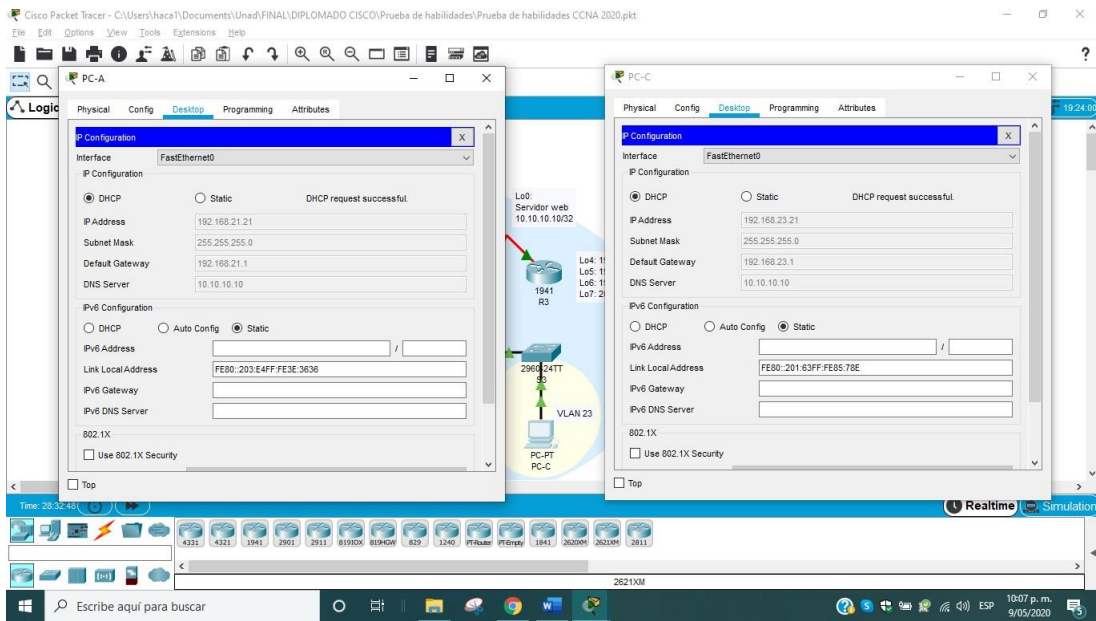


## Anexo 7. Registro Fotográfico. Verificar la Información de RIP

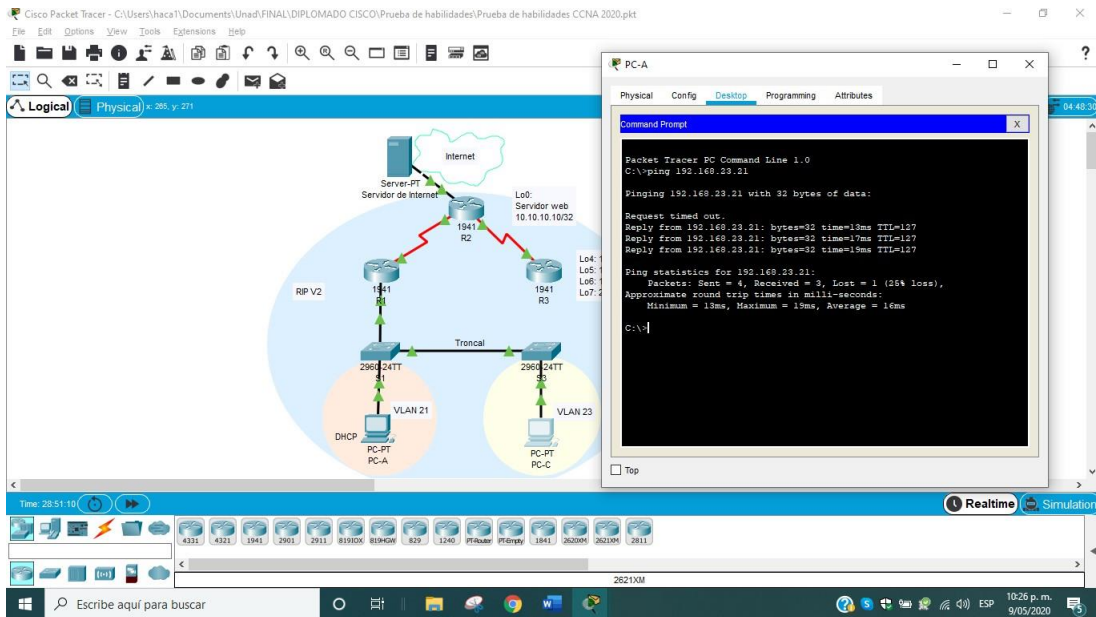




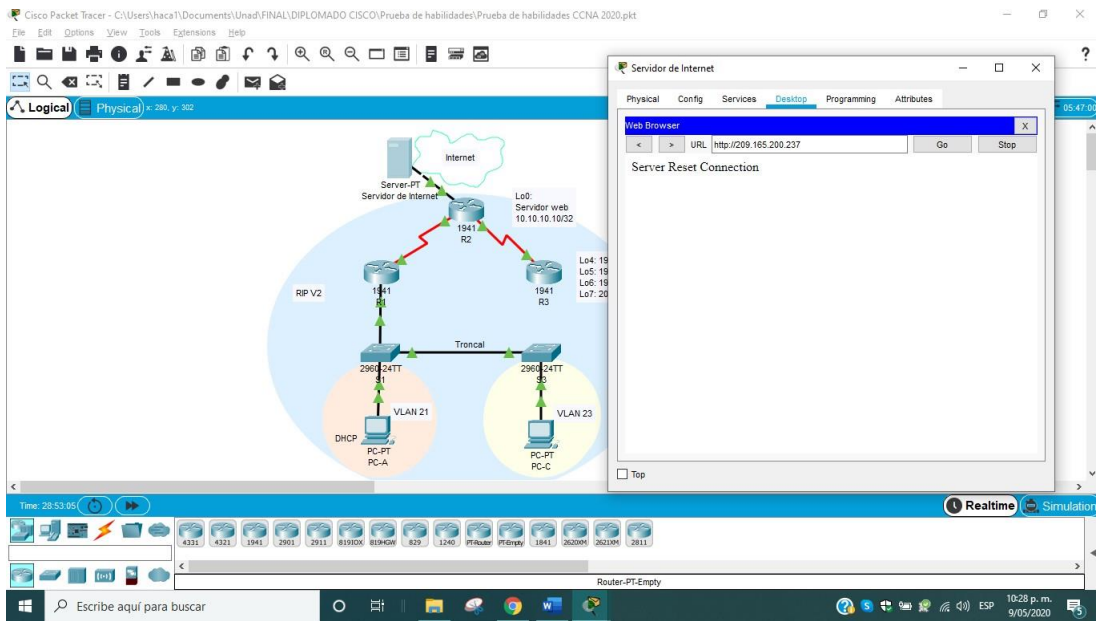
### Anexo 8. Registro Fotográfico. Verificar IP en PC-A y PC-C del Servidor de DHCP



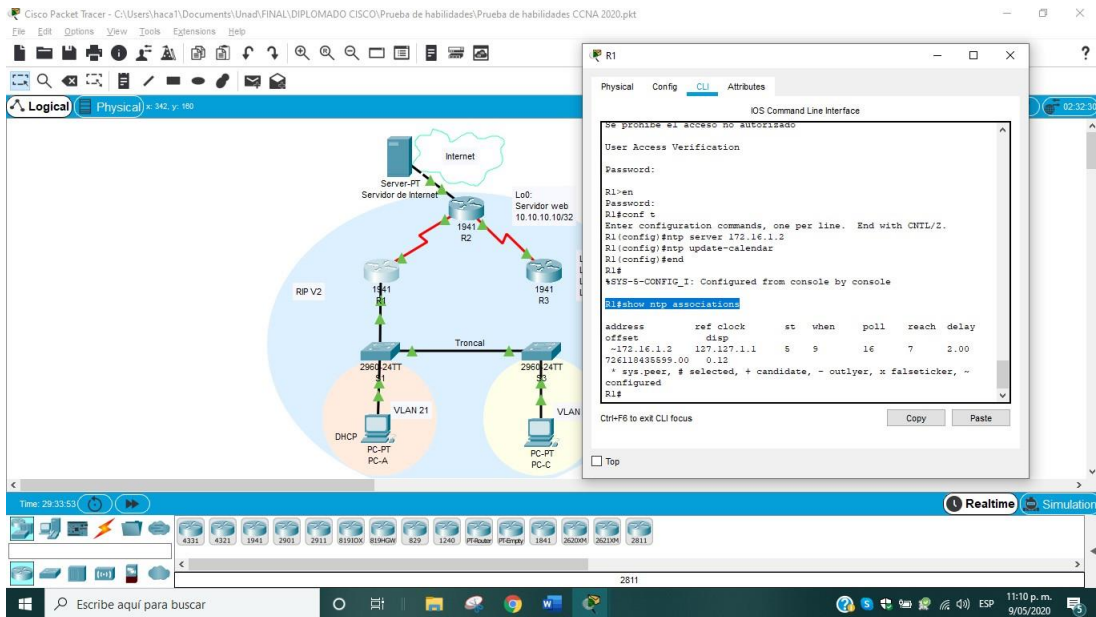
### Anexo 9. Registro Fotográfico. Ping PC-A a PC-C



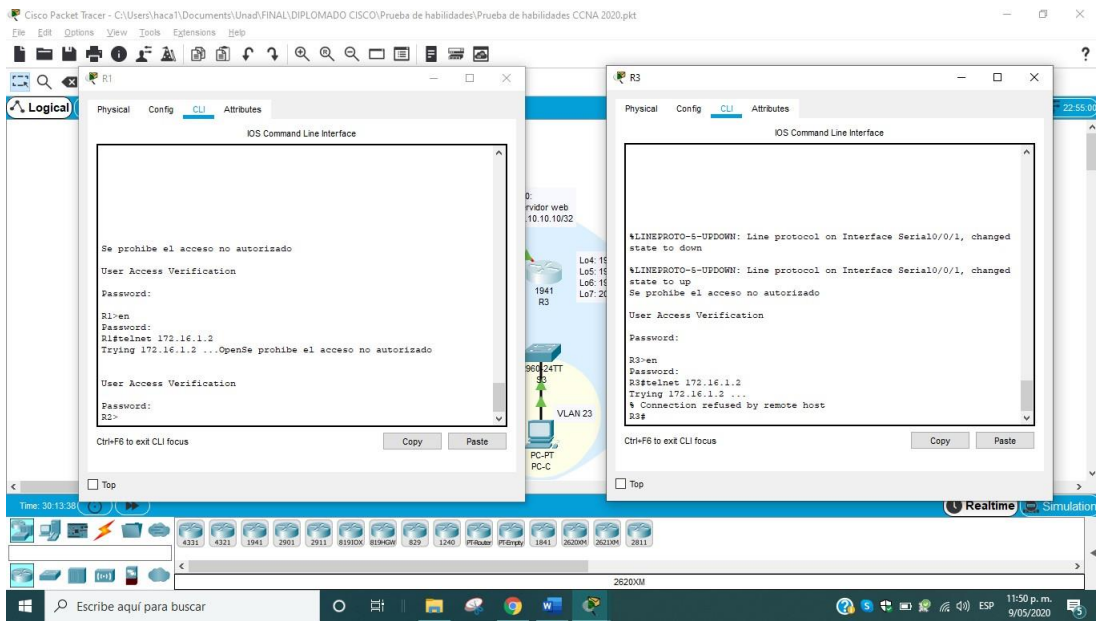
Anexo 10. Registro Fotográfico. Acceder al servidor web (209.165.200.237)



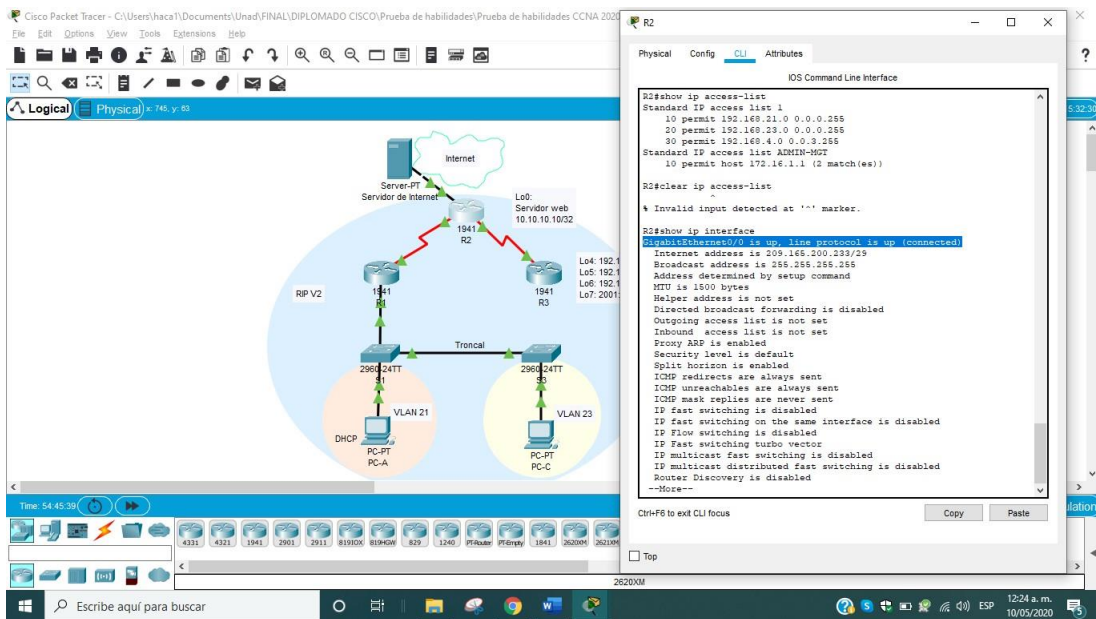
Anexo 11. Registro Fotográfico. Configuración NTP en R1



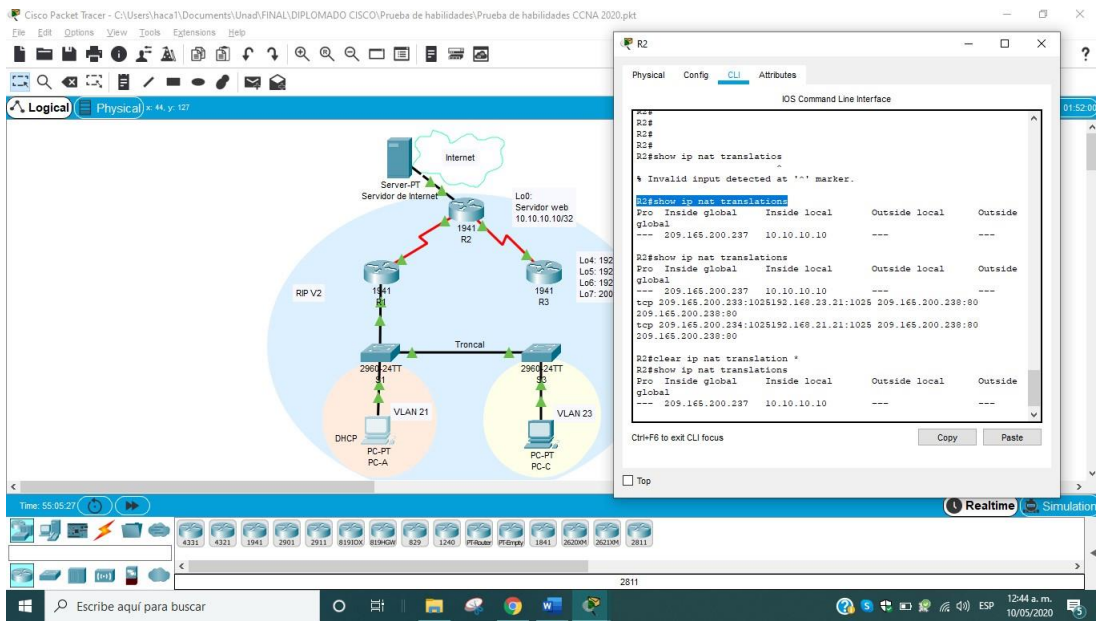
## Anexo 12. Registro Fotográfico. Verificar el Acceso a las Líneas Vty En El R2



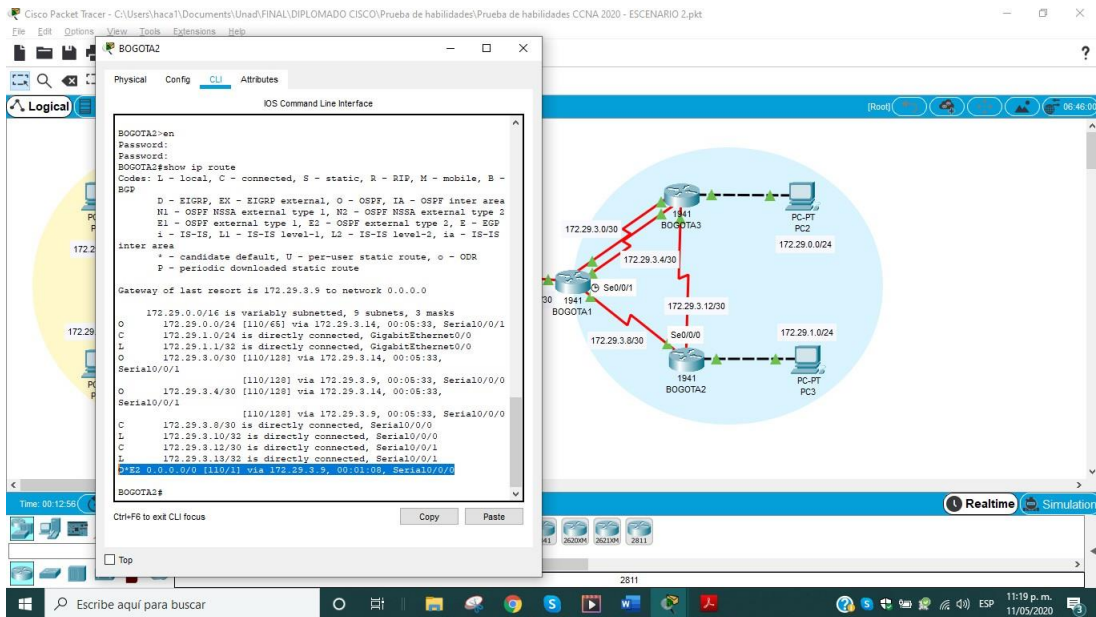
## Anexo 13. Registro Fotográfico. Comandos (show ip access-list) y (show ip interface)



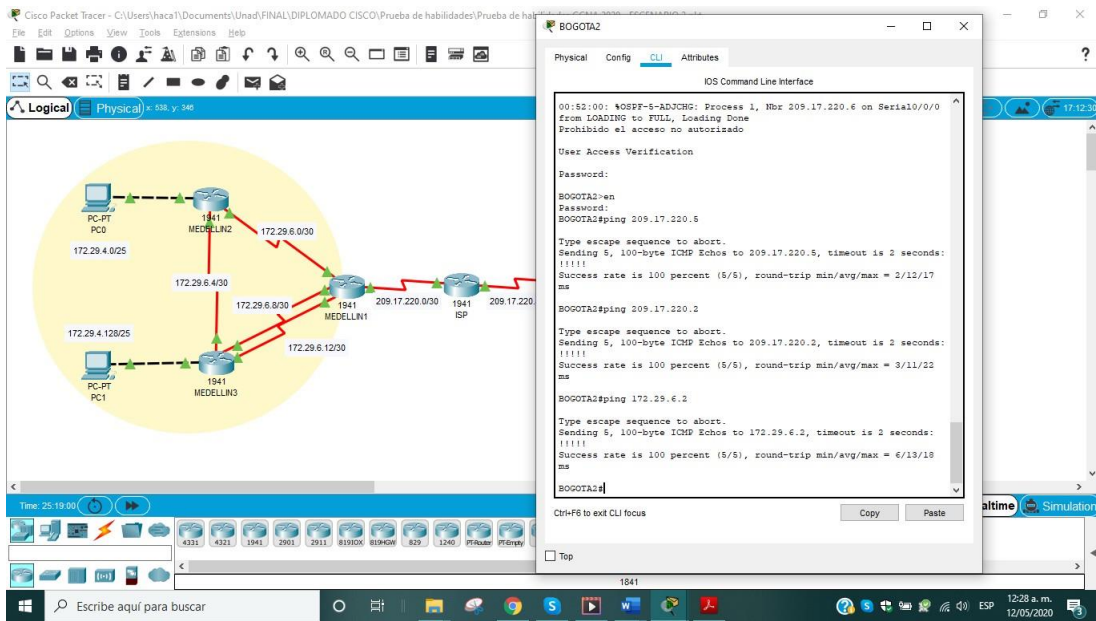
#### Anexo 14. Registro Fotográfico. Comandos (show ip nat translations) y (clear ip nat translations)



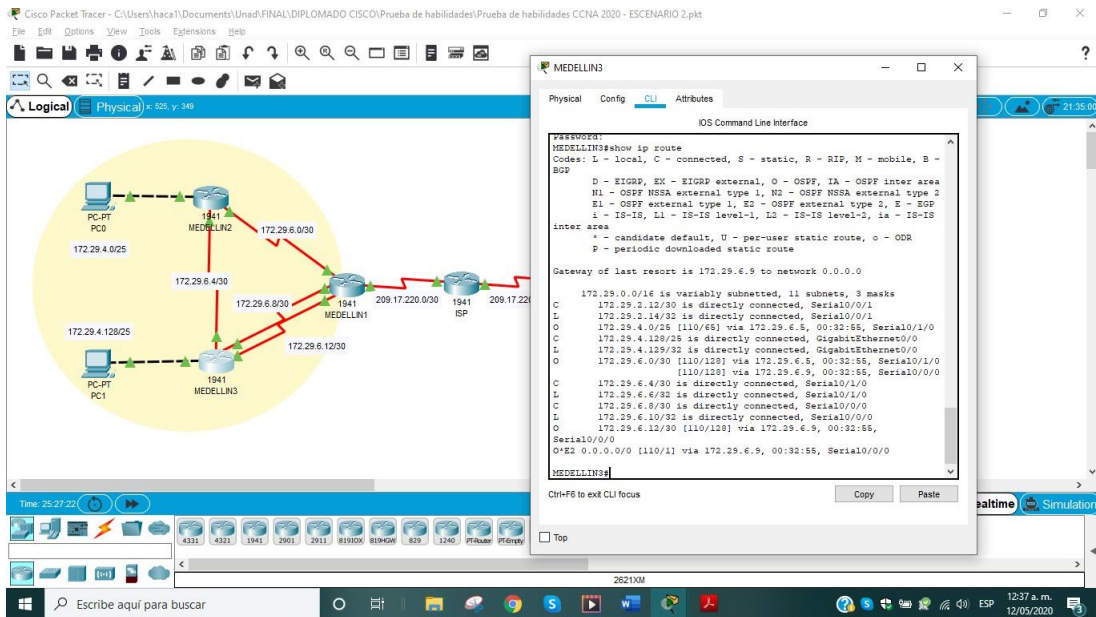
#### Anexo 15. Registro Fotográfico. Comprobar conexión con ISP



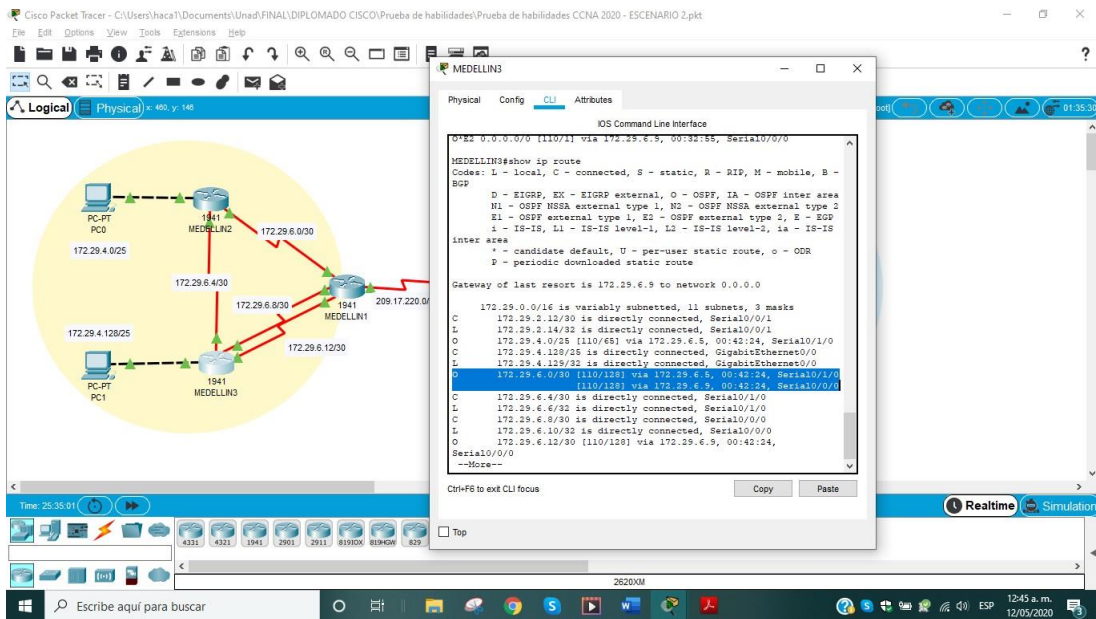
## Anexo 16. Registro Fotográfico. Conectividad entre Medellín y Bogotá



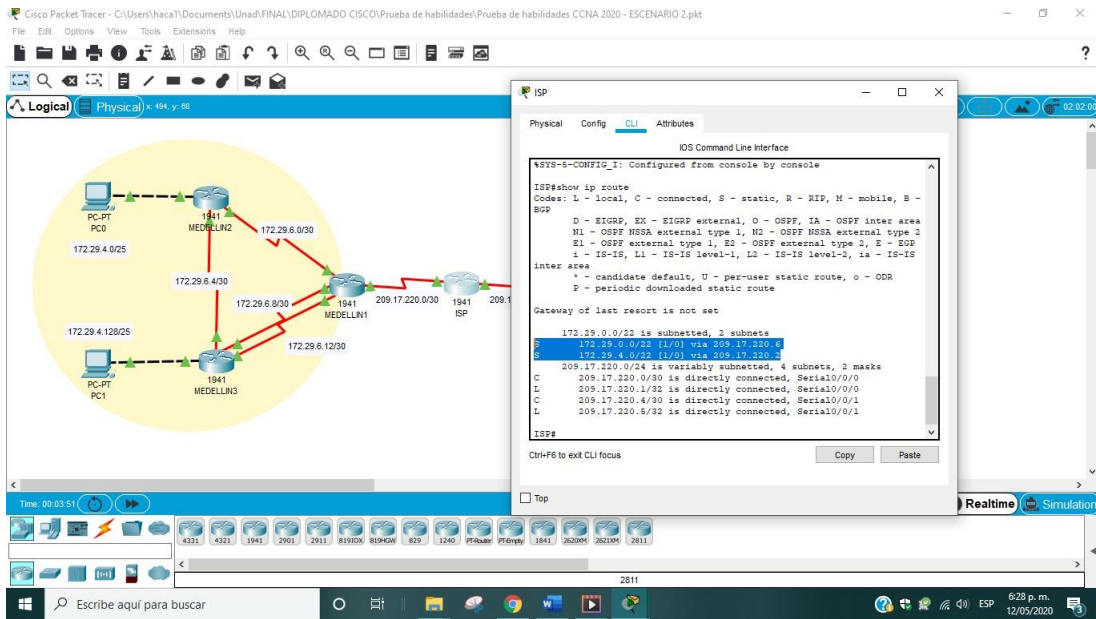
## Anexo 17. Registro Fotográfico. Tabla de Enrutamiento Medellín3



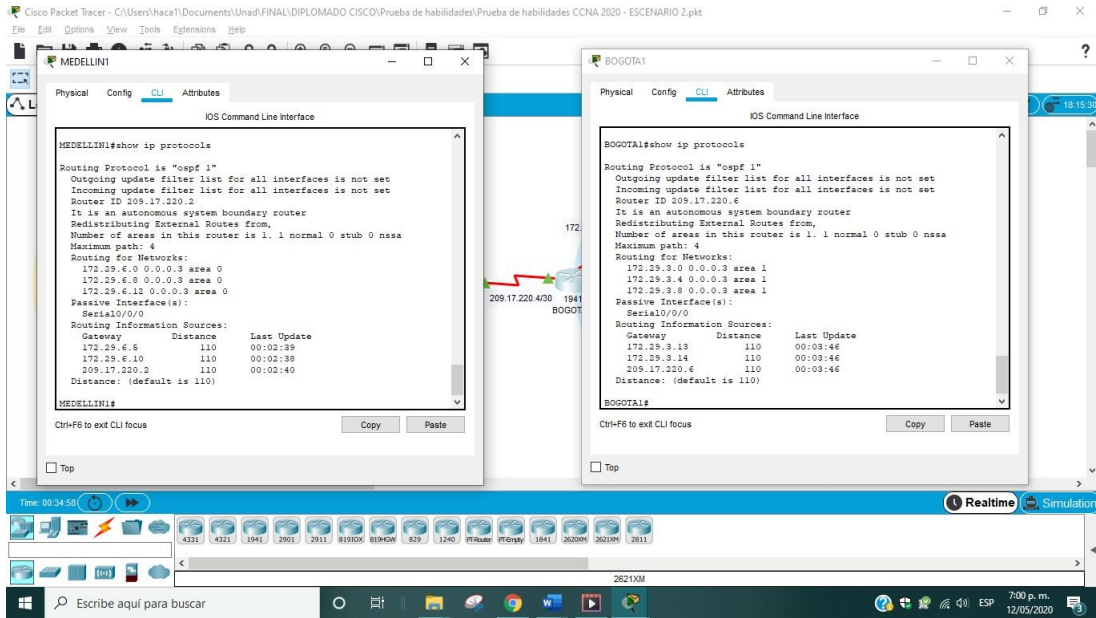
### Anexo 18. Registro Fotográfico. Balanceo de carga



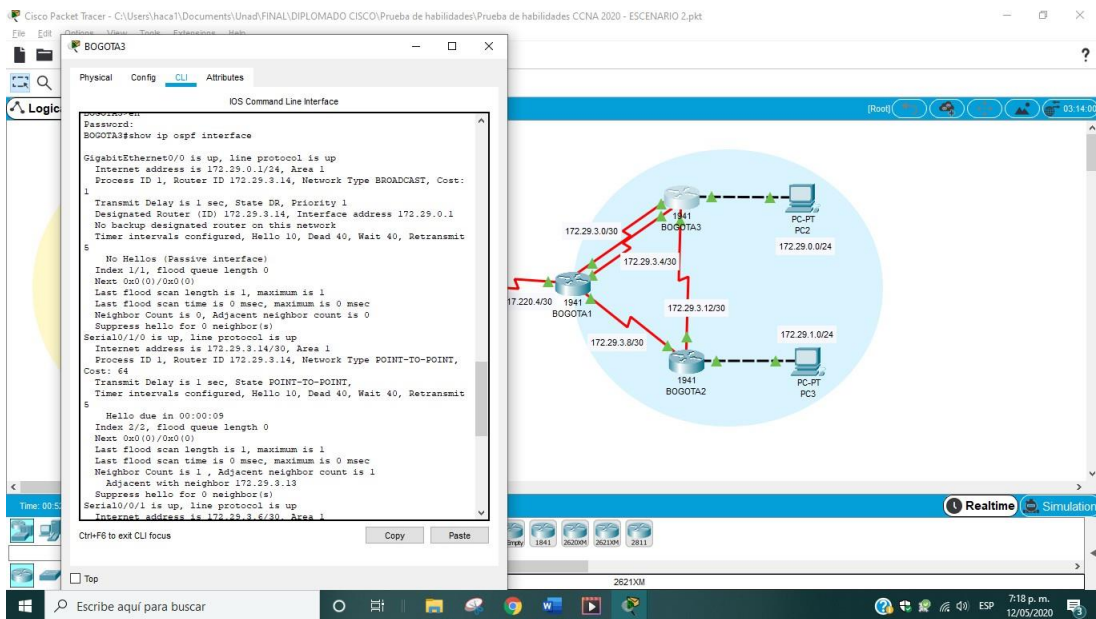
### Anexo 19. Registro Fotográfico. Rutas Estáticas ISP



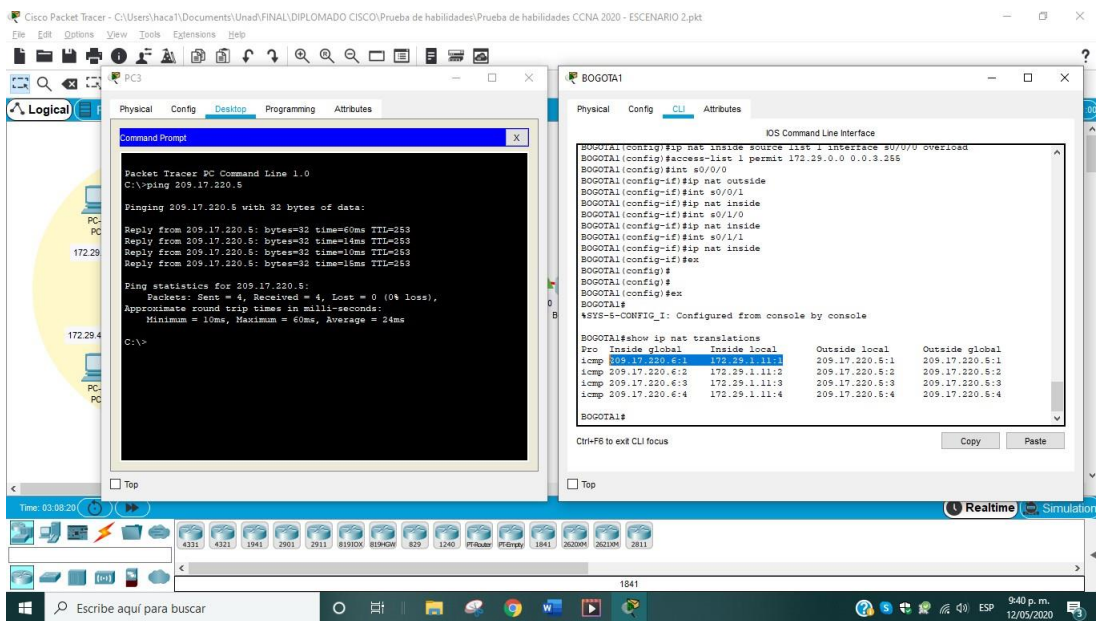
## Anexo 20. Registro Fotográfico. Verificación Protocolo OSPF



## Anexo 21. Registro Fotográfico. Lista de Interfaces

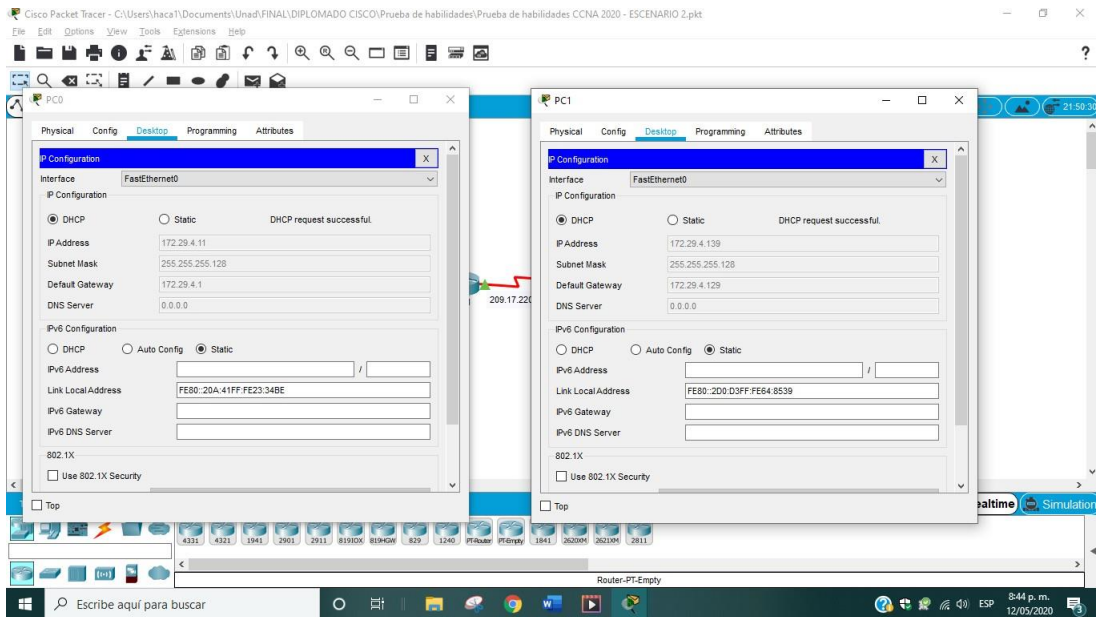


## Anexo 22. Registro Fotográfico. Comando show ip nat translations



## Anexo 23. Registro Fotográfico. Configuración IP DHCP PC0 – PC1





#### Anexo 24. Registro Fotográfico. Configuración IP DHCP PC2 – PC3

