

## **EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA**

**ANDERSON JAVIER QUINTERO ARGOTY**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS**

**INGENIERÍA DE SISTEMAS**

**SAJ JUAN DE PASTO**

**2020**

# **EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA**

**ANDERSON JAVIER QUINTERO ARGOTY**

**Diplomado de profundización cisco**

**Diseño e implementación de soluciones integradas LAN / WLAN**

**Tutor**

**Gustavo Adolfo Rodríguez**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**

**ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS**

**INGENIERÍA DE SISTEMAS**

**SAN JUAN DE PASTO**

**2020**

**Nota de aceptación**

---

---

---

---

---

**Firma del presidente del jurado**

---

**Firma del jurado**

---

**Firma del jurado**

**San Juan de Pasto, 07 de julio del 2020**

## CONTENIDO

INTRODUCCIÓN .....	11
OBJETIVOS .....	12
GENERAL .....	12
ESPECIFICOS .....	12
ESCENARIO UNO .....	13
PARTE 1: INICIALIZAR DISPOSITIVOS .....	13
Paso 1: Inicializar y volver a cargar los routers y los switches .....	13
PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS .....	14
Paso 1: Configurar la computadora de Internet.....	14
Paso 2: Configurar R1 .....	15
Paso 3: Configurar R2 .....	16
Paso 4: Configurar R3 .....	17
Paso 5: Configurar S1 .....	18
Paso 6: Configurar el S3 .....	19
Paso 7: Verificar la conectividad de la red.....	19
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN ..	21
Paso 1: Configurar S1 .....	21
Paso 2: Configurar el S3 .....	22
Paso 3: Configurar R1 .....	23
Paso 4: Verificar la conectividad de la red.....	24
Parte 4: Configurar el protocolo de routing dinámico RIPv2 .....	25
Paso 1: Configurar RIPv2 en el R1 .....	25
Paso 2: Configurar RIPv2 en el R2 .....	26
Paso 3: Configurar RIPv2 en el R3 .....	27
Paso 4: Verificar la información de RIP .....	27
Parte 5: Implementar DHCP y NAT para IPv4 .....	30
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 .....	30
Paso 2: Configurar la NAT estática y dinámica en el R2 .....	30

Paso 3: Verificar el protocolo DHCP y la NAT estática .....	31
Parte 6: Configurar NTP .....	33
Parte 7: Configurar y verificar las listas de control de acceso (ACL) .....	34
Paso 1: Restringir el acceso a las líneas VTY en el R2 .....	34
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente .....	34
ECENARIO 2 .....	37
Parte 1: Configuración básica de los equipos.....	37
Paso 1: Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).	
.....	37
Parte 2: Configuración del enrutamiento .....	42
Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática .....	42
Paso 2: 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 .....	42
Paso 3: 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. ....	43
Parte 4: Tabla de Enrutamiento.....	43
Paso 2: Verificar el balanceo de carga que presentan los routers. ....	44
Parte 5: Deshabilitar la propagación del protocolo OSPF.....	46
Parte 6: Verificación del protocolo OSPF. ....	47
Paso 1: 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..	47
Paso 2: 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. ....	48
Parte 7: Configurar encapsulamiento y autenticación PPP .....	50
Paso 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.....	50
Parte 8 configuración de PAT .....	51

Paso 1: 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, como diferente puerto. ....	51
Parte 9: Configuración del servicio DHCP .....	52
Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN. ....	52
Paso 2: Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan. ....	52
.....	53
CONCLUSIONES .....	56
BIBLIOGRAFIA .....	57
ANEXOS.....	58
LINK DE ACCESO ESCENARIOS PACKET TRACER .....	58

## LISTA DE TABLAS

Tabla 1. Eliminar Configuración Inicial.....	14
Tabla 2. Direccionamiento IP Servidor .....	14
Tabla 3. Configuración en Router 1 .....	15
Tabla 4. Configuración en Router 2 .....	16
Tabla 5. Configuración en Router 3 .....	17
Tabla 6. Configuración en Switch 1 .....	18
Tabla 7. Configuración en Switch 3.....	19
Tabla 8. Verificar Conectividad .....	20
Tabla 9. Configuración de VLAN en Switch 1.....	22
Tabla 10. Configuración de Vlan en Switch 3.....	22
Tabla 11. Configuración de subinterfaces en Router 1 .....	23
Tabla 12. Verificar Segunda Conectividad.....	24
Tabla 13. Configuración Protocolo RIP en Router 1 .....	26
Tabla 14. Configuración Protocolo RIP en Router 2 .....	26
Tabla 15. Configuración protocolo RIP en Router 3 .....	27
Tabla 16. Verificación Protocolo RIP .....	27
Tabla 17. Creación Pool DHCP en Router 1 .....	30
Tabla 18. Configuración NAT en Router 2 .....	31
Tabla 19. Verificación protocolo DHCP y NAT .....	31
Tabla 20. Verificar NAT.....	34
Tabla 21. Configuración Básica Router Escenario 2.....	38
Tabla 22. Configuración Protocolo OSPF .....	42
Tabla 23. Configuración rutas estáticas .....	43
Tabla 24. Deshabilitar propagación protocolo OSPF .....	46
Tabla 25. Configurar autenticación PAP .....	50
Tabla 26. Configurar autenticación CHAP .....	50
Tabla 27. Configuración de PAT.....	51
Tabla 28. Configuración router Medellin2 como DHCP .....	52
Tabla 29. Configuración router Bogota2 como DCHP .....	53

## **LISTA DE ILUSTRACIONES**

Ilustración 1. Topología Escenario Uno .....	13
Ilustración 2. Verificar conectividad1.....	20
Ilustración 3. Verificar conectividad2.....	21
Ilustración 4. Verificar conectividad3.....	25
Ilustración 5. Verificación Protocolo RIP .....	28
Ilustración 6. Verificación Protocolo RIP_2 .....	29
Ilustración 7. Verificación Protocolo RIP_3 .....	29
Ilustración 8. Verificación Protocolo DHCP .....	32
Ilustración 9. Verificar configuración NTP .....	33
Ilustración 10. Verificar ACL .....	35
Ilustración 11. Verificar Interfaz.....	36
Ilustración 12. Topología escenario dos.....	37
Ilustración 13. Verificar enrutamiento Router medellin1 .....	44
Ilustración 14. Verificar enrutamiento router Bogota1 .....	45
Ilustración 15. Verificar enrutamiento router Medellin2.....	46
Ilustración 16. Verificar Protocolo OSPF router Medellin1 .....	47
Ilustración 17. Verificar protocolo OSPF en router Bogota1 .....	48
Ilustración 18. Verificar protocolo OSPF en router Medellin1 .....	49
Ilustración 19. Verificar protocolo OSPF en router Bogota3 .....	49
Ilustración 20. DCHP LAN1 Medellín .....	53
Ilustración 21. DHCP LAN2 Medellín .....	54
Ilustración 22. DHCP LAN1 Bogotá .....	54
Ilustración 23. DHCP LAN2 Bogotá .....	55

## GLOSARIO

**NETWORKING:** El networking es una práctica común en el mundo empresarial y emprendedor. Es una palabra que ya se utiliza de forma cotidiana en el ámbito profesional y que hace referencia a eventos, tanto de tipo formal como informal, en los que puedes construir una red de contactos que te ayuden a generar oportunidades tanto de negocio como laborales.

**ENRUTAMIENTO:** es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda.

**TOPOLOGÍA DE RED:** se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

**PACKET TRACER:** de Cisco es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver preguntas del tipo «¿qué pasaría si...?».

## **RESUMEN**

El presente trabajo se realiza en atención a los parámetros establecidos por la Universidad Nacional Abierta y a Distancia, en colaboración de la plataforma NETCAD de CISCO, en el desarrollo de los cursos CCNA1 y CCNA2, la aplicación de los conceptos adquiridos a lo largo del curso, son aplicados de manera progresiva en la construcción del trabajo final.

El presente trabajo se distribuye en el desarrollo de ejercicios prácticos, desarrollado en el simulador Packet tracer de CISCO, el escenario uno plantea el ejercicio de enrutamiento a través de la implementación del protocolo RIP versión 2, de igual manera la aplicación de conceptos para creación de un servidor web y la aplicación de conceptos para dirección ip dinámico, por intermedio de un router empleado como servidor DHCP, de igual manera la distribución de la redes por intermedio de VLAN debida administradas.

El segundo escenario plantea un problema para la interconexión de sedes ubicadas en diferentes ciudades, se utiliza el protocolo OSPF de manera interna para la propagación de la conectividad, de igual manera se emplean rutas estáticas en los router de borde para su salida a la red WAN, así mismo se emplean conceptos tales como uso de un router como servidor DCHP, protocolo de seguridad para las redes WAN por medio del encapsulamiento PPP bien sea CHAP o PAP.

## **INTRODUCCIÓN**

La presente actividad está enfocada a la verificación de los conceptos aprendidos a lo largo del presente diplomado, por intermedio del presente documento se puede identificar la apropiación de conceptos y la habilidad a la hora de configurar los diferentes elementos que componen una red, identificando todas las capas del modelo OSI, y la aplicación de cada una de estas.

Con la presente actividad se busca identificar la comprensión y habilidades para la solución de problemas relacionados con los diversos aspectos de Networking, con base en lo anterior se plantea el desarrollo de dos (02) escenarios con la debida documentación y evidencias que permitan observar el desarrollo de cada uno de estos.

Para el primer escenario se trabajará en una red pequeña, donde se admitirá conectividad IPV4 e IPV6, aplicando el protocolo de routing dinámico RIPV2, protocolo de configuración de host dinámicos DHCP, traducción de direcciones de red dinámicas y estáticas NAT, lista de control de acceso ACL y protocolo de red NTP, servidor/cliente.

Para el segundo escenario se trabajará el uso del protocolo OSPF, considerando rutas por defecto redistribuidas, se habilitará el encapsulamiento PPP y su autenticación, proporción de servicio DHCP por parte de los router a la red LAN.

Al realizar las prácticas se concluye con la actividad de verificación y conectividad plena de los dos escenarios planteados, demostrando así la capacidad para el desarrollo de este tipo de actividades.

## **OBJETIVOS**

### **GENERAL**

Implementar las habilidades y conocimientos adquiridos, mediante la aplicación de los diferentes conceptos prácticos en el desarrollo de los escenarios propuestos, con el fin de presentar las competencias adquiridas en el desarrollo del presente diplomado.

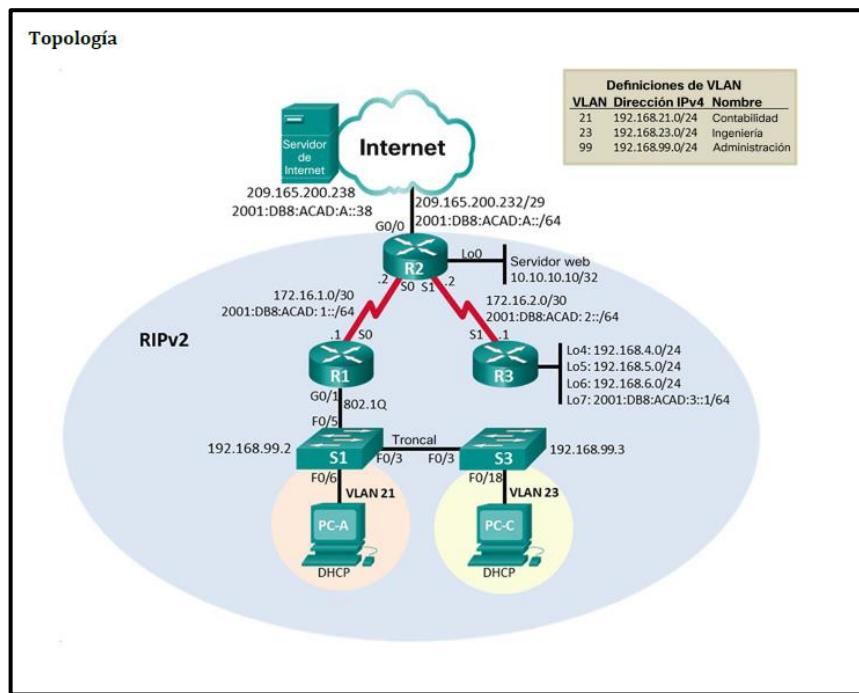
### **ESPECIFICOS**

- ✓ Verificar los requisitos planteados en la guía de aprendizaje, con el fin de plantear las soluciones a las temáticas planteadas.
- ✓ Buscar la asesoría del caso, mediante charlas síncronas con los educadores del presente diplomado, con el fin de validar la presentación del documento final.
- ✓ Identificar los diferentes elementos que sean necesarios para la construcción de las topologías de red planteadas en la presente actividad.
- ✓ Aplicar las diferentes configuraciones, de acuerdo con los protocolos señalados en cada caso, permitiendo la conectividad de los elementos empleados en cada topología.
- ✓ Validar la conectividad en cada uno de los escenarios, con el fin de validar la pertinencia de cada configuración, con el fin de realizar la entrega de un producto funcional.

## ESCENARIO UNO

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.

*Ilustración 1. Topología Escenario Uno*



*Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero*

## PARTE 1: INICIALIZAR DISPOSITIVOS

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

El objetivo de la presente parte es el de eliminar el registro de configuración inicial de todos los dispositivos a utilizar en el desarrollo de la presente práctica.

## Configuración realizada

Tabla 1. Eliminar Configuración Inicial

Dispositivo	Comandos Utilizados
Router 1	<b>R1&gt;Enable</b> <b>R1#erase startup-config</b> <b>R1# reload</b>
Router 2	<b>R2&gt;Enable</b> <b>R2#erase startup-config</b> <b>R2# reload</b>
Router 3	<b>R3&gt;Enable</b> <b>R3#erase startup-config</b> <b>R3# Reload</b>
Switch 1	<b>S1&gt;Enable</b> <b>S1#erase startup-config</b> <b>S1#delete Vlan.dat</b> <b>S1# reload</b> <b>S1# show flash</b>
Switch 3	<b>S3&gt;Enable</b> <b>S3#erase startup-config</b> <b>S3#delete Vlan.dat</b> <b>S3#reload</b> <b>S3#show flash</b>

## PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

### Paso 1: Configurar la computadora de Internet

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

Tabla 2. Direccionamiento IP Servidor

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

En el presente paso se realiza la configuración del servidor WEB, se asigna el direccionamiento IPV4 e IPV6 que tendrá en la presente actividad.

## Paso 2: Configurar R1

En el presente paso se realiza la configuración básica del Router 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, esta configuración inicial permite ajustar de una manera práctica y segura los diferentes elementos que se utilizan en la topología.

Se realiza la descripción de la interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6, se habilita la interfaz como DCE y se habilita el puerto utilizado por la interfaz, configuración realizada con el fin de garantizar la conectividad de la red.

### Configuración realizada

Tabla 3. Configuración en Router 1

Dispositivo	Comandos Utilizados
Router 1	<pre>R1&gt;Enable R1#configure terminal 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 4 R1(config-line)#Password cisco R1(config-line)#Exit R1(config)#Service password-encryption R1(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R1(config)#Interface serial S0/0/0 R1(config-if)#Description CONECTADO A 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-if)#No shutdown R1(config-if)#exit R1(config)#ipv6 unicast-routing R1(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0 R1(config)#ipv6 route ::/0 S0/0/0</pre>

### Paso 3: Configurar R2

En el presente paso se realiza la configuración básica del Router 2, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de las interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, descripción interfaz serial 0/0/1, asignación dirección IPV4 e IPV6, se habilita la interfaz como DCE, se habilita el puerto utilizado por la interfaz, para finalizar se habilita el router como servidor HTTP, se habilita interfaz gigabit ethernet como simulador de internet, se establece dirección IPV4 a dirección loopback 0 como servidor web simulado y se establecen rutas predeterminadas IPV4 e IPV6.

### Configuración realizada

Tabla 4. Configuración en Router 2

Dispositivo	Comandos Utilizados
Router 2	<pre>R2&gt;Enable R2#configure terminal R2(config)#No ip domain-lookup R2(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 4 R2(config-line)#Password cisco R2(config-line)#Exit R2(config)#Service password-encryption R2(config)#Ip http server R2(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R2(config)#Interface serial S0/0/0 R2(config-if)#Description CONECTADO A 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)#exit R2(config)#Ipv6 unicast-routing R2(config)#Interface serial S0/0/1 R2(config-if)#Description CONECTADO A R3</pre>

	<pre>R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:ACAD:2::2/64 R2(config-if)#Clock rate 128000 R2(config-if)#No shutdown R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0 R2(config)#ipv6 route ::0/0 S0/0/0 R2(config)#Interface g0/0 R2(config-if)#Description Simulador de internet R2(config-if)#ip address 209.165.200.232 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#No shutdown R2(config-if)#exit R2(config)#Interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#Description Simulación servidor web R2(config-if)#exit R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)#ipv6 route ::0/0 G0/0</pre>
--	---

#### Paso 4: Configurar R3

En el presente paso se realiza la configuración básica del Router 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de la interfaz serial 0/0/1, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, se habilitan interfaces loopback de la 4 a la 7, se establecen las descripciones y direcciones IPV4, utilizadas como servidores web simulados, para finalizar se asigna una ruta IPV4 e IPV6 predeterminada para la interfaz gigabit ethernet.

#### Configuración realizada

Tabla 5. Configuración en Router 3

Dispositivo	Comandos Utilizados
Router 3	<pre>R3&gt;enable R3#configure terminal R3(config)#No ip domain-lookup R3(config)#Hostname R3</pre>

	<pre> 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 4 R3(config-line)#Password cisco R3(config-line)#Exit R3(config)#Service password-encryption R3(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R3(config)#Interface serial S0/0/1 R3(config-if)#Description CONECTADO A 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)#Interface loopback 4 R3(config-if)#Ip address 192.168.4.1 255.255.255.0 R3(config-if)#Interface loopback 5 R3(config-if)#Ip address 192.168.5.1 255.255.255.0 R3(config-if)#Interface loopback 6 R3(config-if)#Ip address 192.168.6.1 255.255.255.0 R3(config-if)#Interface loopback 7 R3(config-if)#Ip address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#Ipv6 unicast-routing R3(config)#Ip route 0.0.0.0 0.0.0.0 S0/0/1 R3(config)#Ipv6 route ::/0 S0/0/1 </pre>
--	---

## Paso 5: Configurar S1

En el presente paso se realiza la configuración básica del Switch 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

### Configuración realizada

Tabla 6. Configuración en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	<pre> S1&gt;enable S1#configure terminal S1(Config)#No ip domain-lookup S1(Config)#Hostname S# S1(Config)#Enable secret class S1(Config)#Line console 0 S1(Config-line)#Password cisco </pre>

	<b>S1(Config-line)#Login</b> <b>S1(Config-line)#Line vty 0 4</b> <b>S1(Config-line)#Password cisco</b> <b>S1(Config-line)#Exit</b> <b>S1(Config)#Service password-encryption</b> <b>S1(Config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#</b>
--	--

### Paso 6: Configurar el S3

En el presente paso se realiza la configuración básica del Switch 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

#### Configuración Realizada

*Tabla 7. Configuración en Switch 3*

Dispositivo	Comandos Utilizados
Switch 3	<b>S3&gt;enable</b> <b>S3#configure terminal</b> <b>S3(Config)#No ip domain-lookup</b> <b>S3(Config)#Hostname S#</b> <b>S3(Config)#Enable secret class</b> <b>S3(Config)#Line console 0</b> <b>S3(Config-line)#Password cisco</b> <b>S3(Config-line)#Login</b> <b>S3(Config-line)#Line vty 0 4</b> <b>S3(Config-line)#Password cisco</b> <b>S3(Config-line)#Exit</b> <b>S3(Config)#Service password-encryption</b> <b>S3(Config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#</b>

### Paso 7: Verificar la conectividad de la red

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Verificar Conectividad

Desde	A	Dirección IP	Resultado de Ping
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.225 2001:DB8:ACAD:A::1	Satisfactorio

En el presente paso se verifica la conectividad que debe existir entre R1 y R2, de igual manera del PC de internet al Gateway predeterminado.

Ilustración 2. Verificar conectividad1.

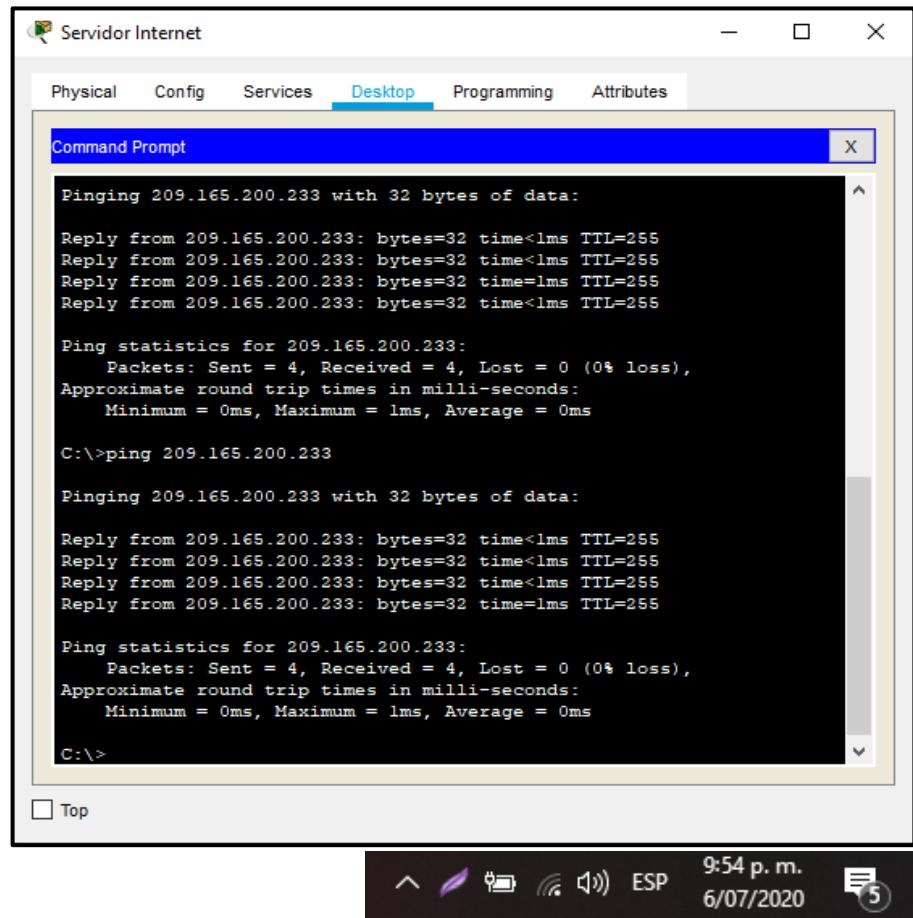
```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Se prohíbe el ingreso a personal no autorizado
User Access Verification
Password:
R1>en
R1>enable
Password:
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 = 1/3/6 ms
R1#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms
R1#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
9:49 p.m.
6/07/2020

```

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 3. Verificar conectividad2



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window is part of a larger interface titled "Servidor Internet" with tabs for Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. The Command Prompt window displays the following output:

```
Pinging 209.165.200.233 with 32 bytes of data:  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time=1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
  
Ping statistics for 209.165.200.233:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>ping 209.165.200.233  
  
Pinging 209.165.200.233 with 32 bytes of data:  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  
Reply from 209.165.200.233: bytes=32 time=1ms TTL=255  
  
Ping statistics for 209.165.200.233:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>
```

The taskbar at the bottom shows icons for file, edit, and search, along with system status (9:54 p.m., 6/07/2020, battery level).

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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

#### Paso 1: Configurar S1

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 21 contabilidad, VLAN 23 ingeniería, VLAN 99 administración, se realiza la asignación de las direcciones IP según la topología, se habilita como enlace troncal las interfaces F0/3 y F0/5 como VLAN nativas, se configuran los demás puertos como acceso, se asigna la interfaz F0/6 como puerto de acceso de la VLAN 21 y se apagan los puertos que no se utilizaran en el Switch.

## Configuración Realizada

Tabla 9. Configuración de VLAN en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	<pre>S1(config)#Vlan 21 S1(config-vlan)#Name CONTABILIDAD S1(config-vlan)#Vlan 23 S1(config-vlan)#Name INGENIERIA S1(config-vlan)#Vlan 99 S1(config-vlan)#Name ADMINISTRATIVA S1(config-vlan)#Exit S1(config)#interface vlan99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#ip default-gateway 192.168.99.1 S1(config-if)#Interface f0/3 S1(config-if)#Switchport mode trunk S1(config-if)#Switchport native vlan1 S1(config-if)#Interface f0/5 S1(config-if)#Switchport mode trunk S1(config-if)#Switchport native vlan1 S1(config-if)#Exit S1(config)#Interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#Switchport mode Access S1(config-if-range)#Exit S1(config)#Interface fa0/6 S1(config-if)#Switchport mode Access vlan21 S1(config-if)#Interface range fa0/1-2, fa0/4, fa0/7-24 S1(config-if-range)#Shutdown</pre>

## Paso 2: Configurar el S3

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 21 contabilidad, VLAN 23 ingeniería, VLAN 99 administración, se realiza la asignación de las direcciones IP según la topología, se asigna como enlace troncal el puerto F0/3 para la VLAN 1 Nativa, se configuran los puertos restantes como acceso, se asigna el puerto F0/18 a la VLAN 21, por último se apagan los puertos sin utilizar.

## Comandos Utilizados

Tabla 10. Configuración de Vlan en Switch 3

Dispositivo	Comandos Utilizados
Switch 3	<pre>S3&gt;Enable</pre>

	<pre> S3#Configure terminal S3(config)#Vlan 21 <b>S3(config-vlan)#Name CONTABILIDAD</b> S3(config-vlan)#Vlan 23 <b>S3(config-vlan)#Name INGENIERIA</b> S3(config-vlan)#Vlan 99 <b>S3(config-vlan)#Name ADMINISTRATIVA</b> S3(config-vlan)#Exit S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#ip default-gateway 192.168.99.1 <b>S3(config-if)#Interface f0/3</b> S3(config-if)#Switchport mode trunk <b>S3(config-if)#Switchport native vlan1</b> <b>S3(config-if)#Interface f0/5</b> S3(config-if)#Switchport mode trunk S3(config-if)#Switchport native vlan1 <b>S3(config-if)#Exit</b> <b>S3(config)#Interface range fa0/1-2, fa0/4-24</b> <b>S3(config-if-range)#Switchport mode Access</b> <b>S3(config-if-range)#Exit</b> <b>S3(config)#Interface fa0/18</b> <b>S3(config-if)#Switchport mode Access vlan 23</b> <b>S3(config-if)#Interface range fa0/1-2, fa0/4-17, fa0/19-24</b> <b>S3(config-if-range)#Shutdown</b> </pre>
--	--

### Paso 3: Configurar R1

En el presente paso se realiza la configuración de las subinterfaces del puerto gigabit ethernet 0/1, se asignan las vlan a las diferentes subinterfaces creadas con el número de VLAN correspondiente Subinterfaz 802.1Q.21 Vlan de contabilidad se le asigna la dirección IP disponible, Subinterfaz 802.1Q.23 Vlan de ingeniería se le asigna la dirección IP disponible, Subinterfaz 802.1Q.99 Vlan de administración se le asigna la dirección IP disponible, se activa la interfaz Gigabit ethernet 0/1.

### Configuración realizada

Tabla 11. Configuración de subinterfaces en Router 1

Dispositivo	Comandos Utilizados
Router 1	<pre> R1&gt;Enable R1#Configure terminal <b>R1(config)#Interface fa0/0.21</b> <b>R1(config-subif)#Description LAN DE CONTABILIDAD</b> <b>R1(config-subif)#Encapsulation dot1Q 21</b> <b>R1(config-subif)#Ip address 192.168.21.1 255.255.255.0</b> </pre>

	<pre>R1(config-subif)#Interface fa0/0.23 R1(config-subif)#Description LAN DE INGENIERIA R1(config-subif)#Encapsulation dot1Q 23 R1(config-subif)#Ip address 192.168.23.1 255.255.255.0 R1(config-subif)#Interface fa0/0.99 R1(config-subif)#Description LAN DE ADMINISTRACIÓN R1(config-subif)#Encapsulation dot1Q 99 R1(config-subif)#Ip address 192.168.99.1 255.255.25 R1(config-subif)#Exit R1(config)#Interface g0/0 R1(config-if)#No shutdown</pre>
--	---

#### Paso 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. Verificar Segunda Conectividad*

Desde	A	Dirección IP	Resultado de Ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

En el presente paso se verifica la conectividad desde los Switch 1 y 3 a las direcciones ip de las subinterfaces del Router 1, se puede observar que existe conectividad en todas las subinterfaces, donde se evidencia la creación adecuada de las VLAN utilizadas en el desarrollo del presente ejercicio.

Ilustración 4. Verificar conectividad3

```
S1>en
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#
```

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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

##### Paso 1: Configurar RIPv2 en el R1

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfaces como pasivas, se desactiva la summarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio, se realiza la aplicación del protocolo dinámico RIPv2, se configura en cada uno de los router a vincular.

## Configuración realizada

Tabla 13. Configuración Protocolo RIP en Router 1

Dispositivo	Comandos Utilizados
Router 1	<b>R1&gt;enable</b> <b>R1#Configure terminal</b> <b>R1(config)#Router rip</b> <b>R1(config-router)#Versión 2</b> <b>R1(config-router)#do show ip route connected</b> <b>R1(config-router)#network 172.16.1.0</b> <b>R1(config-router)#network 192.168.21.0</b> <b>R1(config-router)#network 192.168.23.0</b> <b>R1(config-router)#network 192.168.99.0</b> <b>R1(config-router)#passive-interface g0/0.21</b> <b>R1(config-router)#passive-interface g0/0.23</b> <b>R1(config-router)#passive-interface g0/0.99</b> <b>R1(config-router)#no auto-summary</b>

## Paso 2: Configurar RIPv2 en el R2

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la rede Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfaces como pasivas, se desactiva la summarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

## Configuración realizada

Tabla 14. Configuración Protocolo RIP en Router 2

Dispositivo	Comandos Utilizados
Router 2	<b>R2&gt;enable</b> <b>R2#Configure terminal</b> <b>R2(config)#Router rip</b> <b>R2(config-router)#Versión 2</b> <b>R2(config-router)#do show ip route connected</b> <b>R2(config-router)#network 10.10.10.10</b> <b>R2(config-router)#network 172.16.1.0</b> <b>R2(config-router)#network 172.16.23.0</b> <b>R2(config-router)#passive-interface loopback 0</b> <b>R2(config-router)#no auto-summary</b>

### Paso 3: Configurar RIPv2 en el R3

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la rede Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfaces como pasivas, se desactiva la summarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

#### Configuración realizada

Tabla 15. Configuración protocolo RIP en Router 3

Dispositivo	Comandos Utilizados
Router 3	<pre>R3&gt;enable R3#Configure terminal R3(config)#Router rip R3(config-router)#Versión 2 R3(config-router)#do show ip route connected R3(config-router)#network 172.16.23.0 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 R3(config-router)#end R3#show ip protocols R3#show ip route R3#show run   section rip</pre>

### Paso 4: Verificar la información de RIP

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

Tabla 16. Verificación Protocolo RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols

¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run   section rip – no funciona en packe tracer

En este paso se verifica la implementación del protocolo RIP, se observan las ID de los router, las redes e interfaces pasivas configuradas en el dispositivo, se observan las rutas RIP y la configuración de ejecución, en el presente paso se observa la correcta implementación del protocolo.

*Ilustración 5. Verificación Protocolo RIP*

```
R2#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
    GigabitEthernet0/0  2       2
    Serial0/0/1      2       2
    Serial0/0/0      2       2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    172.16.0.0
    209.165.200.0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.16.2.1        120          00:00:10
    172.16.1.1        120          00:00:11
  Distance: (default is 120)
R2#
R2#
R2#
Ctrl+F6 to exit CLI focus
```

*Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero*

Ilustración 6. Verificación Protocolo RIP\_2

```
Routing for Networks:
  10.0.0.0
  172.16.0.0
  209.165.200.0
Passive Interface(s):
  Loopback0
Routing Information Sources:
  Gateway          Distance      Last Update
  172.16.2.1        120          00:00:10
  172.16.1.1        120          00:00:11
Distance: (default is 120)
R2#
R2#
R2#
R2#sho
R2#show ip ro
R2#show ip route rip
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R  192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:15, Serial0/0/1
R  192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:15, Serial0/0/1
R  192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:15, Serial0/0/1
R  192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
R  192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
R  192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
R2#
```

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 7. Verificación Protocolo RIP\_3

```
Physical Config CLI Attributes
IOS Command Line Interface
!
interface Serial0/0/1
  description SERIAL 0/0/1 CONECTA A R3
  ip address 172.16.2.2 255.255.255.252
  ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Vlan1
  no ip address
  shutdown
!
router rip
  version 2
  passive-interface Loopback0
  network 10.0.0.0
  network 172.16.0.0
  network 209.165.200.0
  no auto-summary
!
ip nat pool INTERNET 209.165.200.235 209.165.200.237 netmask
  255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.234
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
ip route 0.0.0.0 0.0.0.0 209.165.200.238
Ctrl+F6 to exit CLI focus
Copy Paste
Top
5:34 p.m.
7/07/2020
```

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

## Parte 5: Implementar DHCP y NAT para IPv4

### Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

En el presente paso se reservan las 20 primeras direcciones IP del segmento de direcciones asignadas para las VLAN 21 y 23, posteriormente en cada una de estas se realiza la creación del pool de DHCP para cada una de las VLAN.

#### Configuración realizada

Tabla 17. Creación Pool DHCP en Router 1

Dispositivo	Comandos Utilizados
Router 1	<pre>R1&gt;enable R1#Configure terminal R1(config)#ip dhcp exclude-address 192.168.21.1 192.168.21.20 R1(config)#ip dhcp exclude-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)#Dns-server 10.10.10.10 R1(dhcp-config)#Domain-name ccna-aa.com R1(dhcp-config)#Defalut router 1192.168.21.1 R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#Network 192.168.23.0 255.255.255.0 R1(dhcp-config)#Dns-server 10.10.10.10 R1(dhcp-config)#Domain-name ccna-aa.com R1(dhcp-config)#Defalut router 1192.168.23.1</pre>

### Paso 2: Configurar la NAT estática y dinámica en el R2

En el presente paso se realiza la configuración de NAT estática y dinámica en el router 2, en primera instancia se realiza la creación de una base de datos local, se procede habilitar el servicio del servidor HTTP, se configura el servidor de tal manera que pueda utilizar los datos locales para su autenticación, posteriormente se crea la NAT estática en el servidor web, se asignan las interfaces interna y externa a la NAT, se realiza la configuración de NAT dinámica en un ACL privada, se define el pool de direcciones IP utilizables y para finalizar se define la traducción de NATA dinámica.

## Configuración realizada

Tabla 18. Configuración NAT en Router 2

Dispositivo	Comandos Utilizados
Router 2	<pre>R2&gt;enable R2#Configure terminal R2(config)#Username Webuser privilege 15 secret cisco12345 R2(config)#Ip http server R2(config)#Ip http autententication local R2(config)#ip nat inside source static 10.10.10.10 209.165.200.234 R2(config)#Interface loopback 0 R2(config-if)#Ip nat inside R2(config-if)#Interface g0/0 R2(config-if)#Ip nat outside 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)#Ip nat pool INTERNET 209.165.200.235 209.165.200.237 R2(config)#Netmask 255.255.255.248 R2(config)#Ip nat inside source list 1 pool INTERNET</pre>

## Paso 3: Verificar el protocolo DHCP y la NAT estática

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

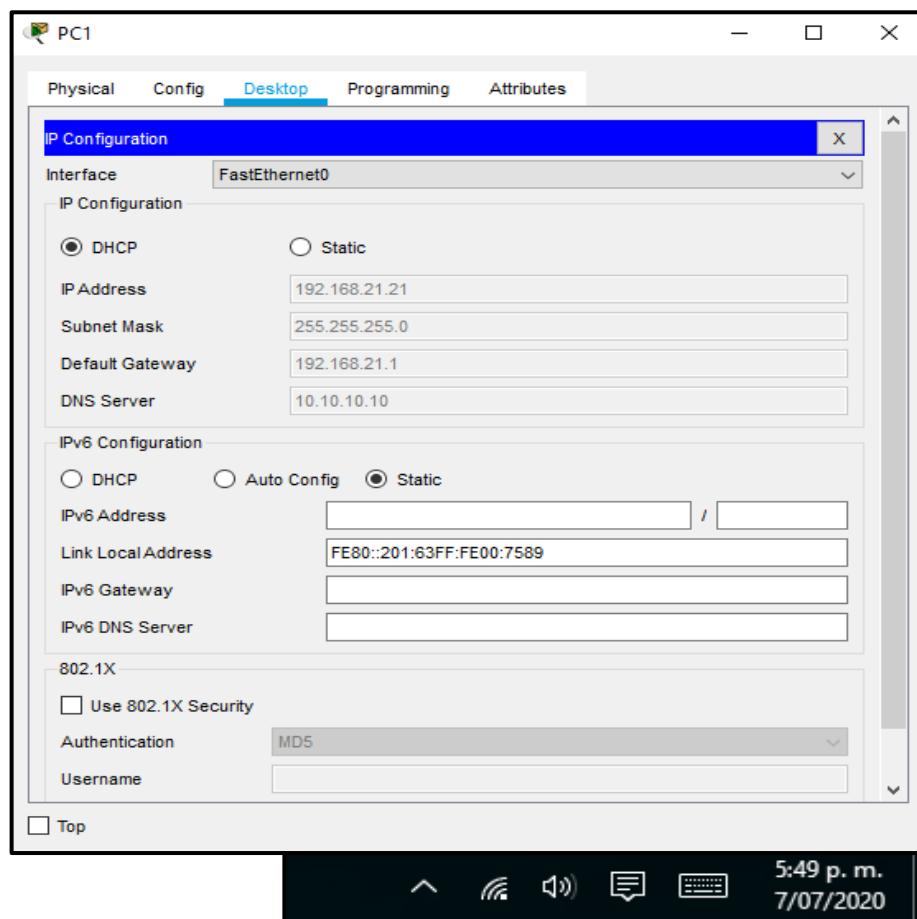
Tabla 19. Verificación protocolo DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Respuesta satisfactoria
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.234) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	No soportado por packet tracer

Se verifica la información IP del servidor DHCP en cada uno de los hosts, se verifica la respuesta de cada uno de estos, se verifica el servicio WEB ingresando a la dirección global del servidor WEB.

En el presente paso se puede observar como el router inicia su función como servidor DHCP, se puede comprobar en los equipos de cómputo, teniendo en cuenta que cada uno de estos obtiene su dirección IP de manera automática, como se puede evidenciar en la siguiente ilustración.

*Ilustración 8. Verificación Protocolo DHCP*



*Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero*

## Parte 6: Configurar NTP

En el presente paso se ajusta la fecha y hora en el router 2, se procede a establecer a este como router maestro NTP, se configura al router 1 como cliente NTP, se configuran las actualizaciones de calendarios periódicos con hora NTP en router 1, por último, se verifica la configuración NTP en R1.

### Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	R2(config)#Clock set 9:00:00 march 5 2016 R2(config)#Ntp master 5
Router 2	R1(config)#Ntp server 172.16.1.2 ntp update-calendar R1(config)#Exit R1#Show ntp assosiations

Ilustración 9. Verificar configuración NTP

The screenshot shows a Windows application window titled "R1". Inside, there's a tab bar with "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is a title bar "IOS Command Line Interface". The main area contains the following command history:

```
Password:  
Password:  
R1#con  
R1#conf  
R1#configure te  
R1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ntp ser  
R1(config)#ntp server 172.16.12.2  
R1(config)#nt  
R1(config)#ntp up  
R1(config)#ntp update-calendar  
R1(config)#exit  
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
R1#sho  
R1#show n  
R1#show ntp a  
R1#show ntp associations  
  
address      ref clock      st  when      poll      reach    delay  
offset          disp          -      -        64       0       0.00  
~172.16.12.2  .INIT.        16      -        64       0       0.00  
0.00           0.12  
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~  
configured  
R1#
```

At the bottom of the window, there are "Copy" and "Paste" buttons. The taskbar at the bottom of the screen shows the date and time as "6:02 p. m. 7/07/2020".

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

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

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

En el presente paso, se realiza la configuración de las listas de control de acceso, se nombra una ACL que solo establezca una conexión telnet entre R1 y R2, se aplica la ACL con nombre para las líneas VTY, por último, se verifica su funcionamiento.

#### Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	R1(config)#Telenet 172.16.1.2
Router 2	R2(config)#Ip Access-list standard ADMIN-MGT R2(config-std-nacl)#Permit host 172.16.1.1 R2(config-std-nacl)#Line vty 0 15 R2(config-line)#Access-list ADMIN-MGT in R2(config-line)#Transport input telnet

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

Tabla 20. Verificar NAT.

Descripción del Comando	Entrada del Estudiante
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-lists
Restablecer los contadores de una lista de acceso	Clear Access-list
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface #Nombre interfaz#
¿Con qué comando se muestran las traducciones NAT?	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. Show ip nat trans

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	No ip nat inside source list #Nombre lista#
--	---

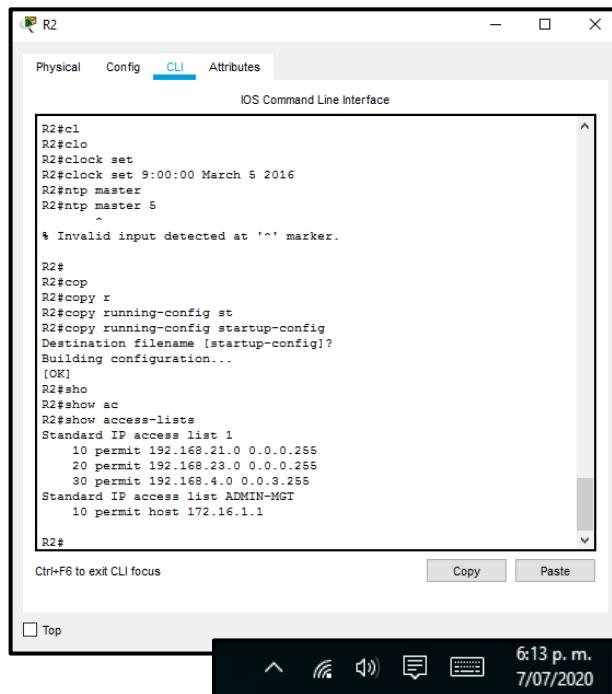
Fuente: Prueba de habilidades prácticas CCNA – UNAD

En el presente paso, se verifican las coincidencias recibidas por la ACL desde la última vez que se restableció, se realiza el restablecimiento de la ACL, en seguida se verifica la ACL aplicada a una interfaz junto a su dirección IP, de igual manera se verifican las traducciones NAT y para finalizar se procede a practicar el cómo se eliminan las direcciones NAT dinámicas.

### Configuración realizada

Dispositivo	Comandos Utilizados
Router 2	<b>R2#Show Access-list</b> <b>R2(config)#Clear Access-list</b> <b>R2(config)#exit</b> <b>R2#Show ip interface S0/0/0</b> <b>R2#Show ip nat trans</b> <b>R2#Configure terminal</b> <b>R2(config)#No ip nat inside source list #</b>

Ilustración 10. Verificar ACL



```

R2
Physical Config CLI Attributes
IOS Command Line Interface
R2#cl
R2#clo
R2#clock set
R2#clock set 9:00:00 March 5 2016
R2#ntp master
R2#ntp master 5
^
% Invalid input detected at '^' marker.

R2#
R2#cop
R2#copy r
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#sho
R2#show ac
R2#show access-lists
Standard IP access list 1
  10 permit 192.168.21.0 0.0.0.255
  20 permit 192.168.23.0 0.0.0.255
  30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
  10 permit host 172.16.1.1
R2#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
6:13 p.m.
7/07/2020

```

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

Ilustración 11. Verificar Interfaz

R2#SH  
R2#SHow IP  
R2#SHow IP IN  
R2#SHow IP INterface S0/0/0  
Serial0/0/0 is up, line protocol is up (connected)  
Internet address is 172.16.1.2/30  
Broadcast address is 255.255.255.255  
Address determined by setup command  
MTU is 1500  
Helper address is not set  
Directed broadcast forwarding is disabled  
Outgoing access list is not set  
Inbound access list is not set  
Proxy ARP is enabled  
Security level is default  
Split horizon is enabled  
ICMP redirects are always sent  
ICMP unreachables are always sent  
ICMP mask replies are never sent  
IP fast switching is disabled  
IP fast switching on the same interface is disabled  
IP Flow switching is disabled  
IP Fast switching turbo vector  
IP multicast fast switching is disabled  
IP multicast distributed fast switching is disabled  
Router Discovery is disabled  
--More--

Ctrl+F6 to exit CLI focus      Copy      Paste

Top

6:15 p. m.  
7/07/2020

Nota: recuperado de packet tracer Escenario 1. Autor Anderson Quintero

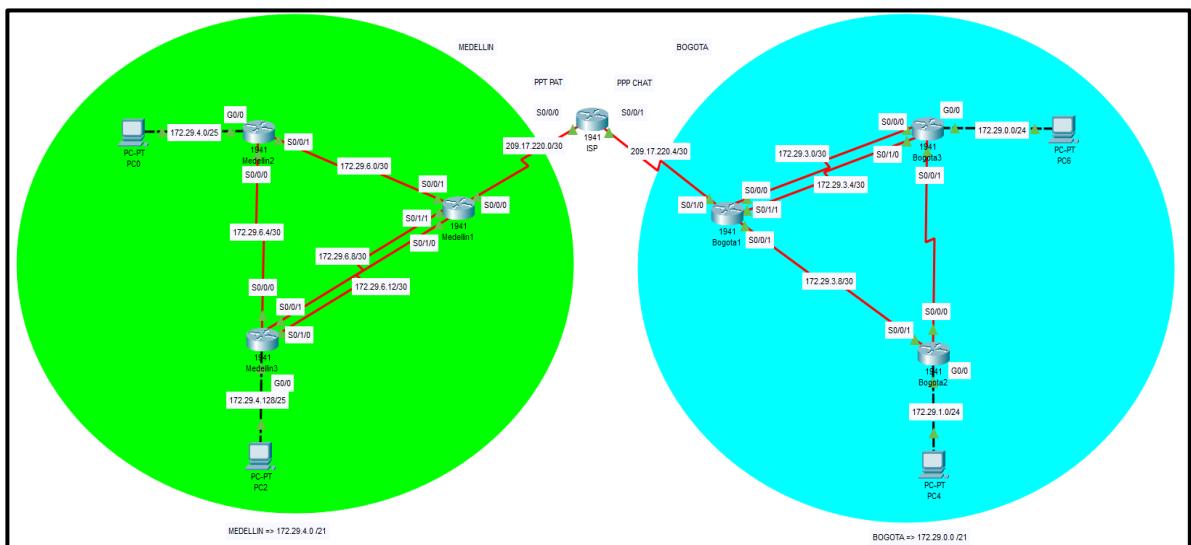
## ECENARIO 2

### Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- ✓ Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).
- ✓ Realizar la conexión física de los equipos con base en la topología de red

*Ilustración 12. Topología escenario dos*



*Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero*

### Parte 1: Configuración básica de los equipos

**Paso 1: Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).**

En el presente paso se realiza la conexión de los diferentes elementos, se realiza la configuración básica de todos los elementos utilizados en el presente escenario, se establece nombre de host, seguridad de telnet y líneas vty, mensaje de restricción, encriptación de claves de seguridad y configuración del direccionamiento IPV4 de cada una de las interfaces, de igual manera se habilitan los puertos a utilizar en cada una de las redes y se verifica conectividad en la red.

## Configuración realizada

Tabla 21. Configuración Básica Router Escenario 2

Dispositivo	Comandos Utilizados
Router ISP	<pre> <b>Router&gt;enable</b> <b>Router#configure terminal</b> <b>Router(config)#hostname ISP</b> <b>ISP(config)#enable secret class</b> <b>ISP(config)#line console 0</b> <b>ISP(config-line)#password cisco</b> <b>ISP(config-line)#login</b> <b>ISP(config-line)#line vty 0 4</b> <b>ISP(config-line)#password cisco</b> <b>ISP(config-line)#login</b> <b>ISP(config-line)#exit</b> <b>ISP(config)#banner motd #se prohíbe el acceso no autorizado#</b> <b>ISP(config)#service password-encryption</b> <b>ISP(config)#interface serial 0/0/0</b> <b>ISP(config-if)#ip address 209.17.220.1 255.255.255.252</b> <b>ISP(config-if)#description conecta a medellin1</b> <b>ISP(config-if)#clock rate 128000</b> <b>ISP(config-if)#no shutdown</b> <b>ISP(config-if)#interface serial 0/0/1</b> <b>ISP(config-if)#ip address 209.17.220.5 255.255.255.252</b> <b>ISP(config-if)#description conecta a Bogota1</b> <b>ISP(config-if)#clock rate 128000</b> <b>ISP(config-if)#no shutdown</b> </pre>
Router Medellín 1	<pre> <b>Router&gt;enable</b> <b>Router#configure terminal</b> <b>Router(config)#hostname medellin1</b> <b>medellin1(config)#enable secret class</b> <b>medellin1(config)#line console 0</b> <b>medellin1(config-line)#password cisco</b> <b>medellin1(config-line)#login</b> <b>medellin1(config-line)#line vty 0 4</b> <b>medellin1(config-line)#password cisco</b> <b>medellin1(config-line)#login</b> <b>medellin1(config-line)#exit</b> <b>medellin1(config)#banner motd #se prohíbe el acceso no autorizado#</b> <b>medellin1(config)#service password-encryption</b> <b>medellin1(config)#interface serial 0/0/0</b> <b>medellin1(config-if)#ip address 209.17.220.2 255.255.255.252</b> <b>medellin1(config-if)#description conecta a ISP</b> <b>medellin1(config-if)#no shutdown</b> <b>medellin1(config-if)#interface serial 0/0/1</b> <b>medellin1(config-if)#ip address 172.29.6.1 255.255.255.252</b> <b>medellin1(config-if)#description conecta a medellin2</b> </pre>

	<pre> medellin1(config-if)#clock rate 128000 medellin1(config-if)#no shutdown medellin1(config-if)#interface serial 0/1/1 medellin1(config-if)#ip address 172.29.6.10 255.255.255.252 medellin1(config-if)#description conecta a medellin3 medellin1(config-if)#clock rate 128000 medellin1(config-if)#no shutdown medellin1(config-if)#interface serial 0/1/0 medellin1(config-if)#ip address 172.29.6.14 255.255.255.252 medellin1(config-if)#description conecta a medellin3 medellin1(config-if)#no shutdown </pre>
Router Medellín 2	<pre> Router&gt;enable Router#configure terminal Router(config)#hostname medellin2 medellin2(config)#enable secret class medellin2(config)#line console 0 medellin2(config-line)#password cisco medellin2(config-line)#login medellin2(config-line)#line vty 0 4 medellin2(config-line)#password cisco medellin2(config-line)#login medellin2(config-line)#exit medellin2(config)#banner motd #se prohíbe el acceso no autorizado# medellin2(config)#service password-encryption medellin2(config-if)#interface serial 0/0/1 medellin2(config-if)#ip address 172.29.6.2 255.255.255.252 medellin2(config-if)#description conecta a medellin1 medellin2(config-if)#no shutdown medellin2(config-if)#interface serial 0/0/0 medellin2(config-if)#ip address 172.29.6.5 255.255.255.252 medellin2(config-if)#description conecta a medellin3 medellin2(config-if)#no shutdown medellin2(config-if)#interface g0/0 medellin2(config-if)#ip address 172.29.4.1 255.255.255.128 medellin2(config-if)#description conecta a red LAN medellin2(config-if)#no shutdown </pre>
Router Medellín 3	<pre> Router&gt;enable Router#configure terminal Router(config)#hostname medellin3 medellin3(config)#enable secret class medellin3(config)#line console 0 medellin3(config-line)#password cisco medellin3(config-line)#login medellin3(config-line)#line vty 0 4 medellin3(config-line)#password cisco medellin3(config-line)#login medellin3(config-line)#exit medellin3(config)#banner motd #se prohíbe el acceso no autorizado# medellin3(config)#service password-encryption </pre>

	<pre> <b>medellin3(config-if)#interface serial 0/0/0</b> <b>medellin3(config-if)#ip address 172.29.6.6 255.255.255.252</b> <b>medellin3(config-if)#description conecta a medellin2</b> <b>medellin3(config-if)#no shutdown</b> <b>medellin3(config-if)#interface serial 0/0/1</b> <b>medellin3(config-if)#ip address 172.29.6.9 255.255.255.252</b> <b>medellin3(config-if)#description conecta a medellin1</b> <b>medellin3(config-if)#no shutdown</b> <b>medellin3(config-if)#interface serial 0/1/0</b> <b>medellin3(config-if)#ip address 172.29.6.13 255.255.255.252</b> <b>medellin3(config-if)#description conecta a medellin1</b> <b>medellin3(config-if)#no shutdown</b> <b>medellin3(config-if)#interface g0/0</b> <b>medellin3(config-if)#ip address 172.29.4.128 255.255.255.128</b> <b>medellin3(config-if)#description conecta a red LAN</b> <b>medellin3(config-if)#no shutdown</b> </pre>
Router Bogotá 1	<pre> <b>Router&gt;enable</b> <b>Router#configure terminal</b> <b>Router(config)#hostname bogota1</b> <b>bogota1(config)#enable secret class</b> <b>bogota1(config)#line console 0</b> <b>bogota1(config-line)#password cisco</b> <b>bogota1(config-line)#login</b> <b>bogota1(config-line)#line vty 0 4</b> <b>bogota1(config-line)#password cisco</b> <b>bogota1(config-line)#login</b> <b>bogota1(config-line)#exit</b> <b>bogota1(config)#banner motd #se prohíbe el acceso no autorizado#</b> <b>bogota1(config)#service password-encryption</b> <b>bogota1(config)#interface serial 0/1/0</b> <b>bogota1(config-if)#ip address 209.17.220.6 255.255.255.252</b> <b>bogota1(config-if)#description conecta a ISP</b> <b>bogota1(config-if)#no shutdown</b> <b>bogota1(config-if)#interface serial 0/0/0</b> <b>bogota1(config-if)#ip address 172.29.3.1 255.255.255.252</b> <b>bogota1(config-if)#description conecta a bogota3</b> <b>bogota1(config-if)#clock rate 128000</b> <b>bogota1(config-if)#no shutdown</b> <b>bogota1(config-if)#interface serial 0/1/1</b> <b>bogota1(config-if)#ip address 172.29.3.5 255.255.255.252</b> <b>bogota1(config-if)#description conecta a bogota3</b> <b>bogota1(config-if)#no shutdown</b> <b>bogota1(config-if)#interface serial 0/0/1</b> <b>bogota1(config-if)#ip address 172.29.3.10 255.255.255.252</b> <b>bogota1(config-if)#description conecta a bogota2</b> <b>bogota1(config-if)#no shutdown</b> </pre>
Router Bogotá 2	<pre> <b>Router&gt;enable</b> <b>Router#configure terminal</b> <b>Router(config)#hostname bogota2</b> </pre>

	<pre> <b>bogota2(config)#enable secret class</b> <b>bogota2(config)#line console 0</b> <b>bogota2(config-line)#password cisco</b> <b>bogota2(config-line)#login</b> <b>bogota2(config-line)#line vty 0 4</b> <b>bogota2(config-line)#password cisco</b> <b>bogota2(config-line)#login</b> <b>bogota2(config-line)#exit</b> <b>bogota2(config)#banner motd #se prohíbe el acceso no autorizado#</b> <b>bogota2(config)#service password-encryption</b> <b>bogota2(config-if)#interface serial 0/0/1</b> <b>bogota2(config-if)#ip address 172.29.3.9 255.255.255.252</b> <b>bogota2(config-if)#description conecta a bogota1</b> <b>bogota2(config-if)#no shutdown</b> <b>bogota2(config-if)#interface serial 0/0/0</b> <b>bogota2(config-if)#ip address 172.29.3.13 255.255.255.252</b> <b>bogota2(config-if)#description conecta a bogota3</b> <b>bogota2(config-if)#no shutdown</b> <b>bogota2(config-if)#interface g0/0</b> <b>bogota2(config-if)#ip address 172.29.1.1 255.255.255.0</b> <b>bogota2(config-if)#description conecta a red LAN</b> <b>bogota2(config-if)#no shutdown</b> </pre>
Router Bogotá 3	<pre> <b>Router&gt;enable</b> <b>Router#configure terminal</b> <b>Router(config)#hostname bogota3</b> <b>bogota3(config)#enable secret class</b> <b>bogota3(config)#line console 0</b> <b>bogota3(config-line)#password cisco</b> <b>bogota3(config-line)#login</b> <b>bogota3(config-line)#line vty 0 4</b> <b>bogota3(config-line)#password cisco</b> <b>bogota3(config-line)#login</b> <b>bogota3(config-line)#exit</b> <b>bogota3(config)#banner motd #se prohíbe el acceso no autorizado#</b> <b>bogota3(config)#service password-encryption</b> <b>bogota3(config-if)#interface serial 0/0/0</b> <b>bogota3(config-if)#ip address 172.29.3.2 255.255.255.252</b> <b>bogota3(config-if)#description conecta a bogota1</b> <b>bogota3(config-if)#no shutdown</b> <b>bogota3(config-if)#interface serial 0/1/0</b> <b>bogota3(config-if)#ip address 172.29.3.6 255.255.255.252</b> <b>bogota3(config-if)#description conecta a bogota1</b> <b>bogota3(config-if)#no shutdown</b> <b>bogota3(config-if)#interface serial 0/0/1</b> <b>bogota3(config-if)#ip address 172.29.3.14 255.255.255.252</b> <b>bogota3(config-if)#description conecta a bogota2</b> <b>bogota3(config-if)#no shutdown</b> <b>bogota3(config-if)#interface g0/0</b> <b>bogota3(config-if)#ip address 172.29.0.1 255.255.255.0</b> </pre>

	<b>bogota3(config-if)#description conecta a red LAN</b> <b>bogota3(config-if)#no shutdown</b>
--	--

## Parte 2: Configuración del enrutamiento

**Paso 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la summarización automática.**

**Paso 2: 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**

En el presente paso se habilita el protocolo ospf versión 2, se declara la red principal y el área con el que se trabajara que por defecto es la cero.

### Configuración realizada

*Tabla 22. Configuración Protocolo OSPF*

Dispositivo	Comandos Utilizados
Router Medellín 1	<b>medellin1(config)#router ospf 1</b> <b>medellin1(config)#router id 1.1.1.1</b> <b>medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0</b> <b>medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0</b> <b>medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0</b> <b>medellin1(config-router)#defalut-information originate</b>
Router Medellín 2	<b>medellin2(config)#router ospf 1</b> <b>medellin2(config)# router id 2.2.2.2</b> <b>medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0</b> <b>medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0</b> <b>medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0</b> <b>medellin1(config-router)#defalut-information originate</b>
Router Medellín 3	<b>medellin3(config)#router ospf 1</b> <b>medellin3(config)# router id 3.3.3.3</b> <b>medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0</b> <b>medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0</b> <b>medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0</b> <b>medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0</b> <b>medellin3(config-router)#defalut-information originate</b>
Router Bogotá 1	<b>bogota1(config)#router ospf 1</b> <b>bogota1(config)# router id 4.4.4.4</b> <b>bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0</b> <b>bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0</b> <b>bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0</b> <b>bogota1(config-router)#defalut-information originate</b>

Router Bogotá 2	<b>bogota2(config)#router ospf 1</b> <b>bogota2(config)#router id 5.5.5.5</b> <b>bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0</b> <b>bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0</b> <b>bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 0</b> <b>bogota2(config-router)#defalut-information originate</b>
Router Bogotá 3	<b>bogota3(config)#router ospf 1</b> <b>bogota3(config)# router id 6.6.6.6</b> <b>bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0</b> <b>bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0</b> <b>bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0</b> <b>bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0</b> <b>bogota3(config-router)#defalut-information originate</b>

**Paso 3: 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.**

En el presente paso se realiza la Sumarización de las redes internas de Bogotá y Medellín, en este caso las redes son 172.29.0.0 /24, 172.29.1.0/24, 172.29.4.0 /25 y 172.29.4.128 /25, para el presente caso según lo señalado en la guía se realizará con máscara /22, se realiza la configuración de las rutas estáticas para el vínculo del router ISP a la conectividad de la RED.

### Configuración realizada

*Tabla 23. Configuración rutas estáticas*

Dispositivo	Comandos Utilizados
Router ISP	<b>ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2</b> <b>ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6</b>
Router Medellín 1	<b>medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1</b>
Router Bogotá 1	<b>bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5</b>

### Parte 4: Tabla de Enrutamiento.

**Paso 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas**

Se procede a utilizar el comando show ip route, con el fin de verificar la tabla de enrutamiento de la red, para el presente ejemplo tomamos la imagen aplicada sobre

el router Medellin1, se puede observar el enrutamiento, donde se conocen las redes directamente conectadas y propagadas por el protocolo OSPF.

Ilustración 13. Verificar enrutamiento Router medellin1

The screenshot shows the Cisco IOS CLI interface for router Medellin1. The window title is "Medellin1". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main pane displays the output of the "show ip route" command:

```
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 209.17.220.2 to network 0.0.0.0

      172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
O       172.29.0.0/24 [110/193] via 209.17.220.2, 00:02:17,
Serial0/0/0
O       172.29.1.0/24 [110/193] via 209.17.220.2, 00:02:17,
Serial0/0/0
O       172.29.3.0/30 [110/192] via 209.17.220.2, 00:02:17,
Serial0/0/0
O       172.29.3.4/30 [110/192] via 209.17.220.2, 00:02:17,
Serial0/0/0
O       172.29.3.8/30 [110/192] via 209.17.220.2, 00:02:17,
Serial0/0/0
O       172.29.3.12/30 [110/256] via 209.17.220.2  00:02:17
```

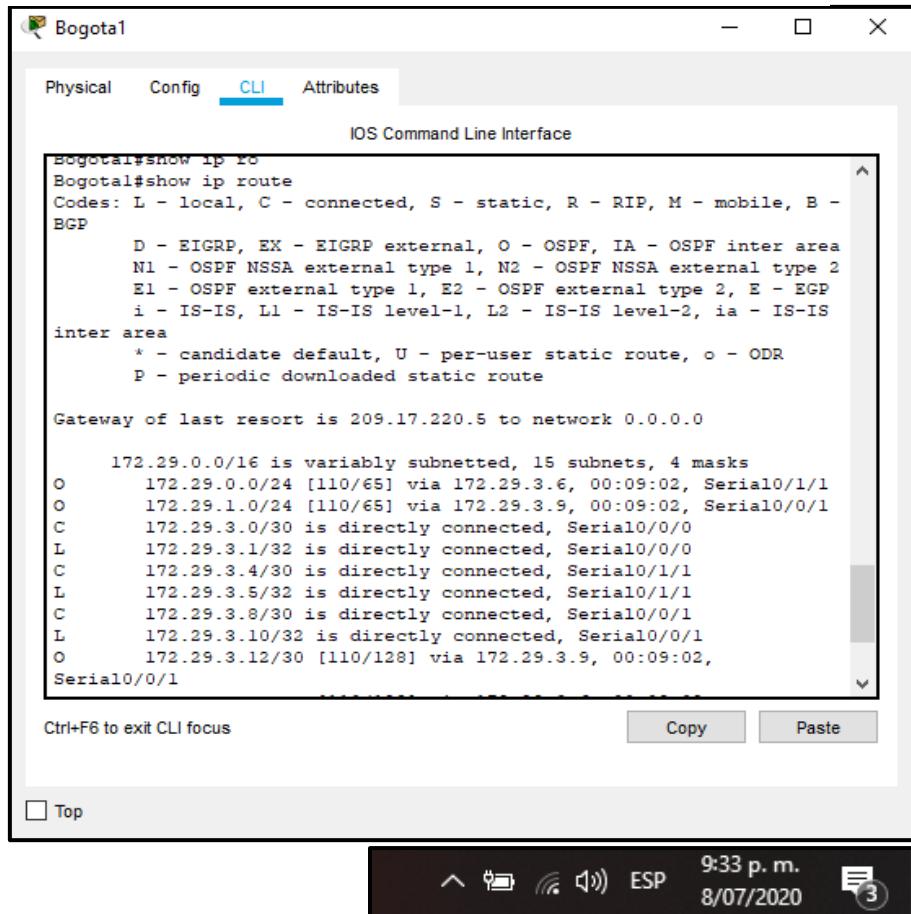
Below the output, there are "Copy" and "Paste" buttons. At the bottom left is a "Top" button. The bottom right corner shows the system status: battery icon, signal strength, volume, "ESP", "9:27 p. m.", "8/07/2020", and a notification icon with the number "3".

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

## Paso 2: Verificar el balanceo de carga que presentan los routers.

Se verifica la tabla de enrutamiento en los router principales de las ciudades, en este bogota1, con el fin de verificar la aplicación del protocolo OSPF y la distribución de las cargas, una vez se realice la configuración señalada en la guía de la actividad.

Ilustración 14. Verificar enrutamiento router Bogota1



```
Bogota1#show ip route
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 209.17.220.5 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 15 subnets, 4 masks
o      172.29.0.0/24 [110/65] via 172.29.3.6, 00:09:02, Serial0/1/1
o      172.29.1.0/24 [110/65] via 172.29.3.9, 00:09:02, Serial0/0/1
C      172.29.3.0/30 is directly connected, Serial0/0/0
L      172.29.3.1/32 is directly connected, Serial0/0/0
C      172.29.3.4/30 is directly connected, Serial0/1/1
L      172.29.3.5/32 is directly connected, Serial0/1/1
C      172.29.3.8/30 is directly connected, Serial0/0/1
L      172.29.3.10/32 is directly connected, Serial0/0/1
o      172.29.3.12/30 [110/128] via 172.29.3.9, 00:09:02,
Serial0/0/1
```

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

### Notas adicionales de la guía

- ✓ 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.
- ✓ Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- ✓ El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Ilustración 15. Verificar enrutamiento router 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, 15 subnets, 4 masks
O   172.29.0.0/24 [110/257] via 172.29.6.1, 00:13:00, Serial0/0/1
O   172.29.1.0/24 [110/257] via 172.29.6.1, 00:13:00, Serial0/0/1
O   172.29.3.0/30 [110/256] via 172.29.6.1, 00:13:00, Serial0/0/1
O   172.29.3.4/30 [110/256] via 172.29.6.1, 00:13:00, Serial0/0/1
O   172.29.3.8/30 [110/256] via 172.29.6.1, 00:13:00, Serial0/0/1
O   172.29.3.12/30 [110/320] via 172.29.6.1, 00:13:00,
Serial0/0/1
C   172.29.4.0/25 is directly connected, GigabitEthernet0/0
L   172.29.4.1/32 is directly connected, GigabitEthernet0/0
O   172.29.4.128/25 [110/65] via 172.29.6.6, 00:13:00,
Serial0/0/0

```

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

## Parte 5: Deshabilitar la propagación del protocolo OSPF

En el presente paso se desactivan las interfaces que no requieren la propagación del protocolo, en este caso se refiere a las redes las de cada uno de las ciudades, se aplica a las interfaces gigabit ethernet de los router medellin2, medellin3, bogota2 y bogota3.

### Configuración realizada

Tabla 24. Deshabilitar propagación protocolo OSPF

Dispositivo	Comandos Utilizados
Router Medellín 2	<b>medellin1(config-router)#passive-interface g0/0</b>
Router Medellín 3	<b>medellin3(config-router)#passive-interface g0/0</b>

Router Bogotá 2	bogota2(config-router)#passive-interface g0/0
Router Bogotá 3	bogota3(config-router)#passive-interface g0/0

## Parte 6: Verificación del protocolo OSPF.

**Paso 1: 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.**

En el presente paso se verifica e los router principales de las ciudades el protocolo de enrutamiento utilizado, para el presente caso el protocolo OSPF.

*Ilustración 16. Verificar Protocolo OSPF router Medellin1*

```

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 209.17.220.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.3 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
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:15:54
    172.29.3.14      110          00:15:54
    172.29.6.5       110          00:15:54
    172.29.6.13      110          00:15:54
    209.17.220.1     110          00:00:07
    209.17.220.2     110          00:15:54
    209.17.220.6     110          00:15:54
  Distance: (default is 110)

Medellin1#

```

Ctrl+F6 to exit CLI focus     

Top

9:33 a. m.  
9/07/2020

*Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero*

Ilustración 17. Verificar protocolo OSPF en router Bogota1

The screenshot shows the Cisco IOS CLI interface for router 'Bogota1'. The window title is 'Bogota1'. The tabs at the top are 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The main area displays the output of the 'show ip protocols' command:

```
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 209.17.220.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.3 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
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:11:54
    172.29.3.14      110          00:11:54
    172.29.6.5       110          00:11:54
    172.29.6.13      110          00:11:54
    209.17.220.1     110          00:11:49
    209.17.220.2     110          00:11:49
    209.17.220.6     110          00:00:11
  Distance: (default is 110)

Bogota1#
```

Below the command output, there are 'Copy' and 'Paste' buttons. At the bottom left is a 'Top' button. The bottom right corner shows the system status: 9:29 a.m., 9/07/2020, and a notification icon with the number 2.

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

**Paso 2: 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.**

En el presente paso se continua la verificación del protocolo OSPF, en este caso se verificarán para complementar las rutas directamente conectadas, en el paso anterior se verificó el enrutamiento del protocolo, la presente sería una imagen complementaria de la conectividad de la tipología de red.

Ilustración 18. Verificar protocolo OSPF en router Medellin1

```
209.17.220.1      110      00:00:07
209.17.220.2      110      00:15:54
209.17.220.6      110      00:15:54
Distance: (default is 110)

Medellin1#do show ip ro
Medellin1#do show ip route connected
^
* Invalid input detected at '^' marker.

Medellin1#conf
Medellin1#configure te
Medellin1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#do sh
Medellin1(config)#do sho
Medellin1(config)#do show ip route connected
Medellin1(config)#do show ip route connected
Medellin1(config)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.0/30 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
C 209.17.220.0/30 is directly connected, Serial0/0/0

Medellin1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
9:46 a.m. 9/07/2020
```

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 19. Verificar protocolo OSPF en router Bogota3

```
Bogota2#show ip pro
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 172.29.3.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.255 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:12:24
    172.29.3.14      110          00:12:22
    172.29.6.5       110          00:42:23
    172.29.6.13      110          00:42:23
    209.17.220.1     110          00:42:18
    209.17.220.2     110          00:42:18
    209.17.220.6     110          00:00:40
  Distance: (default is 110)
--More--
```

Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

## Parte 7: Configurar encapsulamiento y autenticación PPP

**Paso 1: Segundo la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.**

En el presente paso se realiza la configuración del encapsulamiento y autenticación PPP, para el caso de ISP con enlace a Medellin1 se utilizará la autenticación PAP, que básicamente son medidas de seguridad para proteger la conexión WAN.

*Tabla 25. Configurar autenticación PAP*

Dispositivo	Comandos Utilizados
Router ISP	<b>ISP(config-if)#int s0/0/0</b> <b>ISP(config-if)# encapsulation ppp</b> <b>ISP(config-if)# ppp authentication pap</b> <b>ISP(config-if)# ppp pap sent-username ISP password cisco</b>
Router Medellín1	<b>Medellin1(config-if)#int s0/0/0</b> <b>Medellin1 (config-if)# encapsulation ppp</b> <b>Medellin1 (config-if)# ppp authentication pap</b> <b>Medellin1 (config-if)# ppp pap sent-username Medellin1 password cisco</b>

**Paso 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.**

En el presente paso se realiza la configuración del encapsulamiento y autenticación PPP, para el caso de ISP con enlace a Medellin1 se utilizará la autenticación CHAP, que básicamente son medidas de seguridad para proteger la conexión WAN.

*Tabla 26. Configurar autenticación CHAP*

Dispositivo	Comandos Utilizados
Router ISP	<b>ISP(config)#username Bogota1 password cisco</b> <b>ISP(config-if)#int s0/0/1</b> <b>ISP(config-if)# encapsulation ppp</b> <b>ISP(config-if)# ppp authentication chap</b>
Router Bogota1	<b>Bogota1(config)# username ISP password cisco</b> <b>Bogota1(config-if)#int s0/1/0</b> <b>Bogota1(config-if)# encapsulation ppp</b> <b>Bogota1(config-if)# ppp authentication chap</b>

## Parte 8 configuración de PAT

### Notas de la guía

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.

**Paso 1: 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.**

Tabla 27. Configuración de PAT

Dispositivo	Comandos Utilizados
Router Medellin1	<pre>Medellin1(config)#ip access-list standard LAN-MEDELLIN Medellin1(config-std-nacl)#permit 172.29.0.0 0.0.255.255 Medellin1(config-std-nacl)#exit Medellin1(config)#ip nat inside source list LAN-MEDELLIN interface s0/1/0 overload Medellin1(config)#interface s0/1/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit Medellin1(config)#interface s0/0/1 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit Medellin1(config)#interface s0/0/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit Medellin1(config)#interface s0/1/1 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit</pre>
Router Bogota1	<pre>Bogota1(config)#ip access-list standard LAN-BOGOTA Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.255.255 Bogota1(config-std-nacl)#exit Medellin1(config)#ip nat inside source list LAN-BOGOTA interface s0/1/0 overload Bogota1(config)#interface s0/0/0 Bogota1(config-if)#ip nat outside Bogota1(config-if)#exit Bogota1(config)#interface s0/0/1 Bogota1(config-if)#ip nat outside Bogota1(config-if)#exit Bogota1(config)#interface s0/1/0</pre>

	<b>Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit Medellin1(config)#interface s0/1/1 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit</b>
--	---

## Parte 9: Configuración del servicio DHCP

**Paso 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.**

En el presente paso se realizará la configuración al router Medellin2 como DHCP de las redes LAN de esta ciudad.

*Tabla 28. Configuración router Medellin2 como DHCP*

<b>Dispositivo</b>	<b>Comandos Utilizados</b>
Router Medellin2	<b>Medellin2(config)#ip dhcp excluded-address 172.29.4.0 172.29.4.9 Medellin2(config)#ip dhcp pool MEDELLIN-LAN1 Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.1 Medellin2(dhcp-config)#domain-name LAN1-MEDELLIN.COM Medellin2(dhcp-config)#exit Medellin2(config)#ip dhcp excluded-address 172.29.4.128 172.29.4.139 Medellin2(config)#ip dhcp pool MEDELLIN-LAN2 Medellin2(dhcp-config)#NETwork 172.29.4.128 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.129 Medellin2(dhcp-config)#domain-name LAN2-MEDELLIN.COM Medellin2(dhcp-config)#end</b>
Router Medellin3	<b>Medellin3(config)#interface g0/0 Medellin3(config-if)#ip helper-address 172.29.6.5</b>

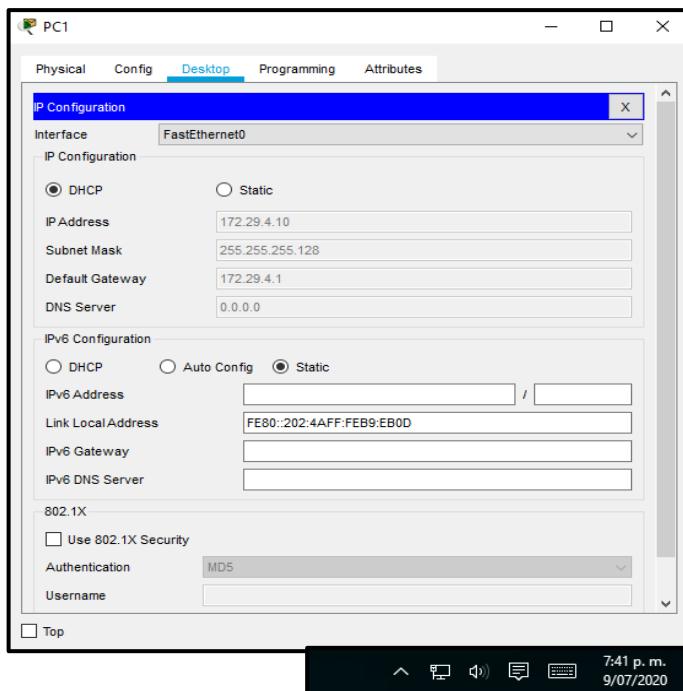
**Paso 2: Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan.**

En el presente paso se realizará la configuración al router Medellin2 como DHCP de las redes LAN de esta ciudad.

Tabla 29. Configuración router Bogota2 como DHCP

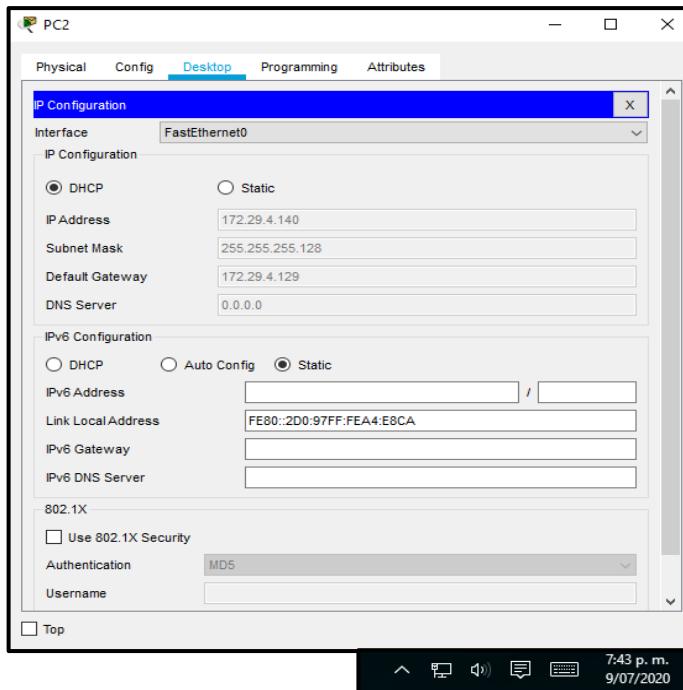
Dispositivo	Comandos Utilizados
Router Bogota2	<pre>Bogota2(config)#ip dhcp excluded-address 172.29.0.0 172.29.0.9 Bogota2 (config)#ip dhcp pool BOGOTA-LAN1 Bogota2 (dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2 (dhcp-config)#default-router 172.29.0.1 Bogota2 (dhcp-config)#domain-name LAN1-BOGOTA.COM Bogota2 (dhcp-config)#exit Bogota2 (config)#ip dhcp excluded-address 172.29.1.0 172.29.1.9 Bogota2 (config)#ip dhcp pool BOGOTA-LAN2 Bogota2 (dhcp-config)#NETwork 172.29.1.0 255.255.255.0 Bogota2 (dhcp-config)#default-router 172.29.1.1 Bogota2 (dhcp-config)#domain-name LAN2-BOGOTA.COM Bogota2 (dhcp-config)#end</pre>
Router Bogota3	<pre>Bogota3(config)#interface g0/0 Bogota3(config-if)#ip helper-address 172.29.3.13</pre>

Ilustración 20. DHCP LAN1 Medellín



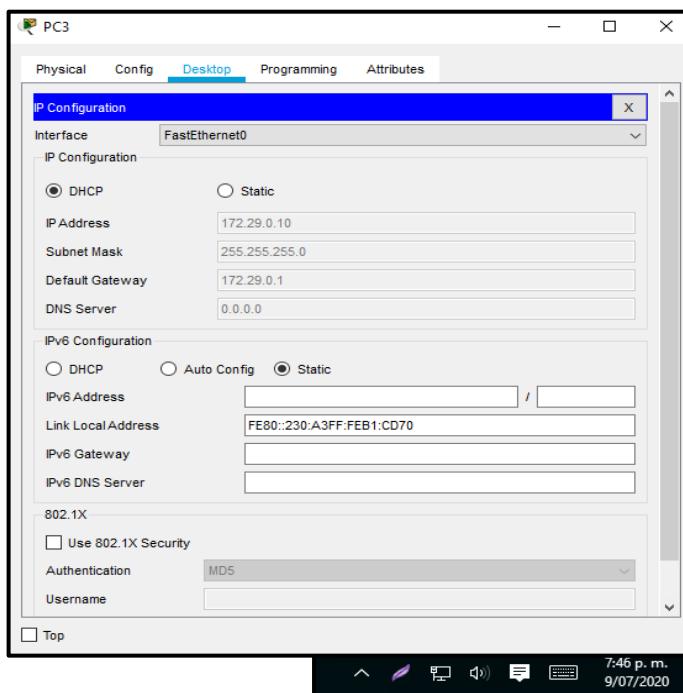
Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 21. DHCP LAN2 Medellín



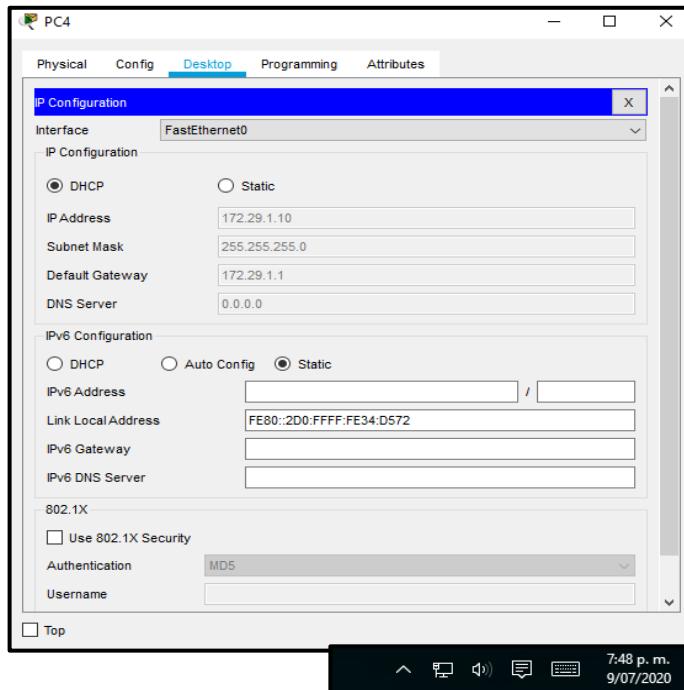
Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 22. DHCP LAN1 Bogotá



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

Ilustración 23. DHCP LAN2 Bogotá



Nota: recuperado de packet tracer Escenario 2. Autor Anderson Quintero

## CONCLUSIONES

- ✓ El presente trabajo permitió plantear las diferentes habilidades obtenidas a lo largo del desarrollo del curso, aplicación de competencias prácticas en la resolución de problemas de configuración real en una red empresarial, siempre aplicada al mejoramiento de la comunicación empresarial.
- ✓ La configuración básica aplicada a cada uno de los elementos, permite un campo práctico de experiencia, teniendo en cuenta que es la configuración mínima aplicar en la construcción de una nueva red de comunicaciones.
- ✓ Los diferentes tipos de configuraciones realizadas en los diferentes elementos, se ajustan a las necesidades identificadas, se aplican los protocolos y se crean las diferentes redes que permiten la comunicación por diferentes medios, permitiendo así una red completa y ajustada detalladamente.
- ✓ Se realizan las configuraciones acordes al desarrollo de la guía, se realiza la configuración básica de cada elemento, se crean vlan y se configuran en las subinterfaces de los router, se simula un servidor web y http, se configura el direccionamiento dhcp en un rango asignado de direcciones ip, se aplica el protocolo rip versión 2, se configura NAT estática y dinámica dependiendo de las observaciones del documento, se estructura una red ajustada a las necesidades empresariales. Con base en lo anterior se culmina a satisfacción la prueba práctica de conocimientos.
- ✓ Se aplica la configuración del protocolo OSPF versión como protocolo de enrutamiento dinámico, se observa su método de propagación e interconexión para dar a conocer las redes que no están directamente conectadas, el uso del protocolo se recomienda para redes de gran tamaño.

## BIBLIOGRAFIA

- CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>
- Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de [https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl\\_pLtPD9](https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl_pLtPD9)
- CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>
- CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>
- CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>
- CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>
- CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>
- CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>
- CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>
- CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>
- CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11>
- CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Comutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>
- CISCO. (2019). Routing Estático. Principios de Enrutamiento y Comutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2>

## **ANEXOS**

### **LINK DE ACCESO ESCENARIOS PACKET TRACER**

<https://drive.google.com/drive/folders/1ekxvd96LScvTiDMnhk5IfHymcc0MW5CE?usp=sharing>