

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

CAMILO ANDRES AVILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTA, CUNDINAMARCA
2020

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

CAMILO ANDRES AVILA

INFORME DE PRÁCTICA DE PROFUNDIZACIÓN PARA OPTAR AL TÍTULO DE
INGENIERO DE SISTEMAS

PHD. JUAN CARLOS VESGA
DIRECTOR DE CURSO

MSC. JOSE IGNACIO CARDONA
DOCENTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTA, CUNDINAMARCA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá, Cundinamarca (08, 05, 2020)

Dedico este trabajo a mi familia que han sido el motor y la inspiración para sacar mi carrera adelante, con apoyo, comprensión y dedicación.

AGRADECIMIENTOS

En primera instancia agradezco a Dios por haberme brindado los medios para sacar este proyecto adelante, a mi familia por la comprensión y apoyo brindada, a los docentes y tutores de la UNAD por su acompañamiento durante este arduo proceso.

CONTENIDO

LISTA DE TABLAS	8
LISTA DE FIGURAS	9
GLOSARIO	10
RESUMEN	11
ABSTRACT	11
INTRODUCCIÓN	12
OBJETIVOS	13
General	13
Específicos	13
Escenario 1	14
Escenario	14
Topología	14
Parte 1: Inicializar dispositivos.....	15
Paso 1 Inicializar y volver a cargar los routers y los switches	15
Parte 2 Configurar los parámetros básicos de los dispositivos.....	16
Paso 1: Configurar la computadora de Internet.....	16
Paso 2: Configurar R1	17
Paso 3: Configurar R2	18
Paso 4: Configurar R3	21
Paso 5: Configurar S1.....	23
Paso 6: Configurar el S3.....	24
Paso 7: Verificar la conectividad de la red	24
Parte 3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN	26
Paso 1 Configurar S1	26
Paso 2 Configurar el S3	27
Paso 3 Configurar R1.....	27
Paso 4: Verificar la conectividad de la red	28
Parte 4 Configurar el protocolo de routing dinámico RIPv2.....	30
Paso 1 Configurar RIPv2 en el R1	30
Paso 2 Configurar RIPv2 en el R2.....	30
Paso 3 Configurar RIPv3 en el R2.....	31
Paso 4 Verificar la información de RIP.....	32
Parte 5 Implementar DHCP y NAT para IPv4	33
Paso 1 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	33

Paso 2 Configurar la NAT estática y dinámica en el R2	34
Paso 3 Verificar el protocolo DHCP y la NAT estática.....	35
Parte 6 Configurar NTP	36
Parte 7 Configurar y verificar las listas de control de acceso (ACL)	37
Paso 1 Restringir el acceso a las líneas VTY en el R2.....	37
Paso 2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	38
Escenario 2	41
Topología de red	41
Desarrollo.....	41
Parte 1: Configuración del enrutamiento	44
Parte 2: Tabla de Enrutamiento	53
Parte 3: Deshabilitar la propagación del protocolo OSPF	56
Parte 4: Verificación del protocolo OSPF	57
Parte 5: Configurar encapsulamiento y autenticación PPP	61
Parte 6: Configuración de PAT	64
Parte 7: Configuración del servicio DHCP	65
CONCLUSIONES	69
REFERENCIAS	70
ANEXOS	71

LISTA DE TABLAS

	Pág.
Table 1-Inicialización de dispositivos. Fuente El Autor	15
Table 2 - Configuración servidor - Fuente el Autor	16
Table 3 - Configuración R1 - Fuente El Autor.....	18
Table 4 Configuration R2 - Fuente El Autor	21
Table 5 Configuration R3 - Fuente El Autor	23
Table 6 Configuration S1 - Fuente El Autor.....	23
Table 7 Configuration S3 - Fuente El Autor.....	24
Table 8 - Verifcacion Conectividad con Ping Escenario 1 –Fuente el Autor	24
Table 9 Configuración S1 Fuente El Autor	27
Table 10 Configuración S3 Fuente El Autor	27
Table 11 Configuración VLAN en R1 Fuente El Autor	28
Table 12 Verificacion de conectividad de red Fuente El Autor	28
Table 13 Tabla 13 configuracion RIPv2 en R1 Fuente El Autor	30
Table 14 Configuracion RIPv2 EN R2 Fuente El Autor	31
Table 15 Configuracion RIPv2 en R3 Fuente El Autor.....	32
Table 16 verificación información RIP en R1, R2 y R3 Fuente El Autor	33
Table 17 Configuracion DHCP en R1 Fuente El Autor	34
Table 18 Configuración NAT en R2 Fuente El Autor	35
Table 19 Verificación de SErvicios Fuente El Autor.....	36
Table 20 Configuración NTP en R1 y R2 Fuente El Autor	36
Table 21 Configuración acceso VTY en R2 Fuente el Autor.....	37
Table 22 Comandos de verificación.....	39
Table 23 Propagación de Protocolo Fuente El Autor.....	57

LISTA DE FIGURAS

Pág

Figure 1 – Comando R3.....	16
Figure 2 Ping R1 con R2, S0/0/0 Fuente El autor.....	25
Figure 3 Ping R2 con R3, S0/0/1 Fuente El Autor.....	25
Figure 4 PC de internet con gateway predeterminado Fuente El Autor.....	25
Figure 5 Ping de S1 a R1 Fuente El Autor.....	29
Figure 6 Figura 6. Ping de S3 a R1 Fuente El Autor.....	29
Figure 7 Figura 6. Ping de S3 a R1, dirección VLAN 99 y R1, dirección VLAN 23 Fuente El Autor.....	29
Figure 8 Prueba de Telnet de R1 a R2 Fuente El Autor.....	38
Figure 9 Prueba de Telnet de R3 a R2 Fuente El Autor.....	38
Figure 10 Topología Escenario 1.....	40
Figure 11 Topología Escenario 2 -Fuente Unad.....	41
Figure 12 Conexión Equipos Topología Escenario 2.....	44
Figure 13 Enrutamiento Router Bogotá Fuente Autor.....	53
Figure 14 Enrutamiento Router Medellín1 Fuente Guía Autor.....	54
Figure 15 Balanceo de Carga Router 3 Fuente Autor.....	55
Figure 16 Punto c, d, e y f Fuente El Autor.....	56
Figure 17 Verificación OSPF Bogotá1 Fuente El Autor.....	57
Figure 18 Verificación OSPF Bogotá2 Fuente El Autor.....	58
Figure 19 Verificación OSPF Bogotá3 Fuente El Autor.....	58
Figure 20 Verificación OSPF Medellín1 Fuente El Autor.....	59
Figure 21 Verificación OSPF Medellín2 Fuente El Autor.....	59
Figure 22 Verificación OSPF Medellín2 Fuente El Autor.....	60
Figure 23 Verificación ISP Fuente El Autor.....	60
Figure 24 Ping de extremo a extremo – pc.....	68

GLOSARIO

DHCP: (Dynamic Host Configuration Protocol, protocolo de configuración de host dinámico), protocolo que permite a un dispositivo que navegue por internet poder obtener la configuración de red de forma automática y consecutiva.

DNS: Domain Name System (sistema de nombres de dominio), es el sistema que permite resolver nombres de una red, sin necesidad de conocer la IP.

GATEWAY: Es la puerta de enlace en una red, la cual permite la conexión a redes diferentes a la red interna del contexto.

INTERFAZ: En redes, el término se utiliza para mencionar cierto conector, que permite enviar y recibir paquetes. IP: Protocolo de internet, elemento lógico que permite enviar y recibir datos mediante una red.

LAN: (Local Area Network), Red de área local, la cual permite realizar conexión entre ordenadores y dispositivos en un contexto.

NAT: (Network Address Translation) Traducción de direcciones de red, permite una dirección IP privada traducir a una dirección IP pública, para evitar uso de más IP.

OSPF: (Open Shortest Path First), protocolo de direccionamiento el cual se basa en buscar la ruta más corta en una red.

SUMARIZACIÓN: Método para reducir número de entradas en tablas de ruteo.

WAN: (Wide Area Network), red de área amplia, red de conexión de ordenadores que puede dar comunicación a terminales hasta de una ciudad.

RESUMEN

En la siguiente actividad se documenta el desarrollo de una prueba de habilidades prácticas del diplomado de profundización en cisco con el cual demostramos los conocimientos adquiridos durante el desarrollo del curso, mostrando nuestras habilidades de manejo de packet tracer el cual es un software de mucha ayuda pues nos permite simular situaciones y entornos de red que nos permitirán saber cómo debemos hacer las configuraciones cuando nos encontremos en una situación real.

ABSTRACT

The following activity documents the development of a practical skills test of the in-depth diploma in cisco with which to demonstrate the knowledge acquired during the development of the course, showing our skills of handling the tracking package which is very helpful software since It allows us to simulate situations and network environments that allow us to know how we should do the settings when we are in a real situation.

INTRODUCCIÓN

En la siguiente actividad se documenta el desarrollo de una prueba de habilidades prácticas del diplomado de profundización en cisco con el cual demostramos los conocimientos adquiridos durante el desarrollo del curso, mostrando nuestras habilidades de manejo de packet tracer el cual es un software de mucha ayuda pues nos permite simular situaciones y entornos de red que nos permitirán saber cómo debemos hacer las configuraciones cuando nos encontremos en una situación real.

Mediante el estudio de este curso de CCNA1 y CCNA2 pretendemos conocer más a fondo los conceptos y tecnologías básicas que forman una red. Mediante el estudio buscamos desarrollar aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones.

Se realiza la prueba de habilidades prácticas para recordar los conocimientos adquiridos durante el curso

Actualmente, el diplomado es de gran importancia, ya que nos da un sentido analítico de las cosas y nos ayuda a mejorar en algunos otros cursos de nuestra carrera.

OBJETIVOS

General

- Realizar informe de la prueba de habilidades practicas del diplomado de cisco

Específicos.

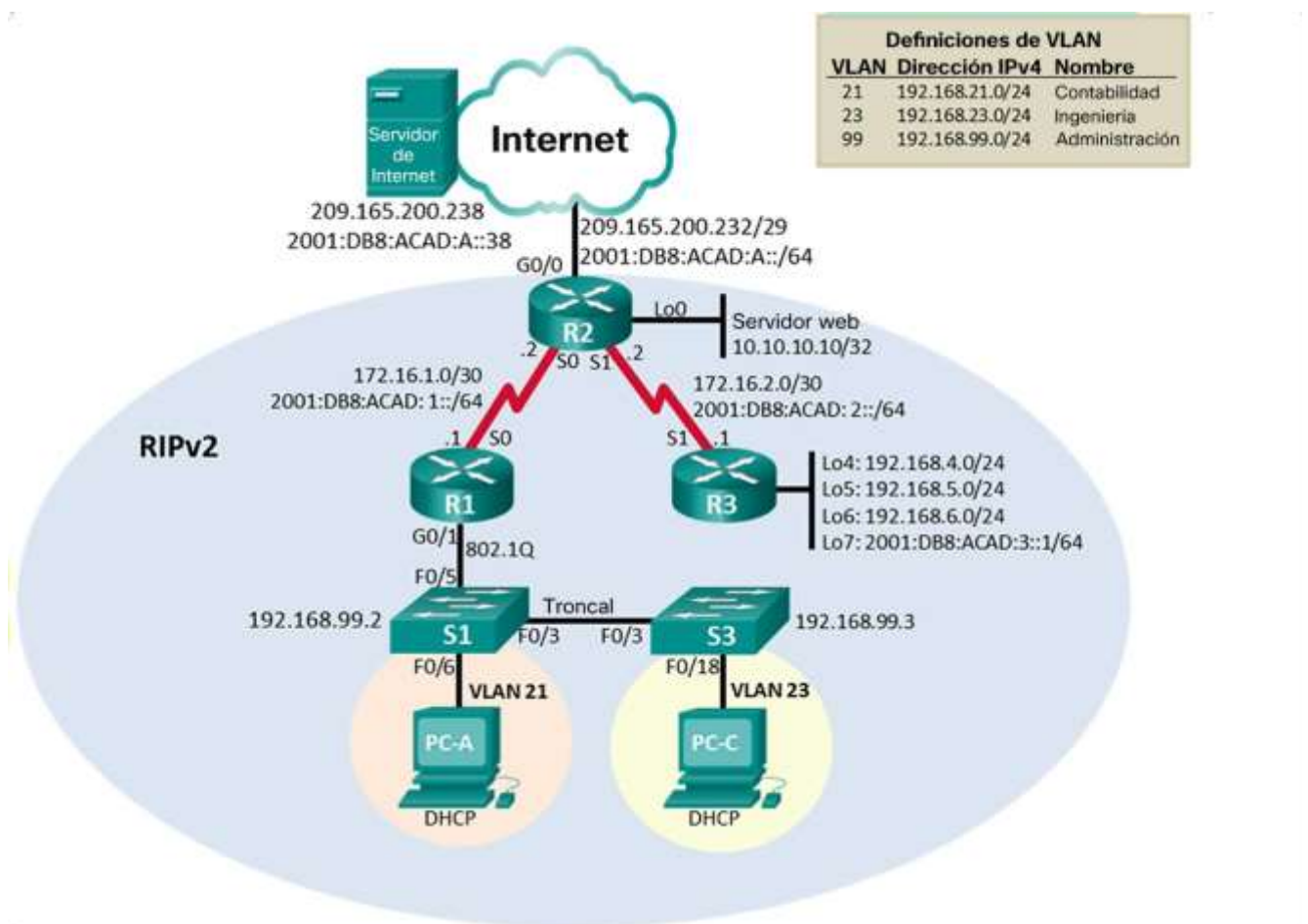
- Solucionar el ejercicio propuesto en la plataforma de cisco llamado prueba de habilidades practicas
- Demostrar los conocimiento adquiridos durante el desarrollo del diplomado de cisco
- Ejecutar conexiones básicas, acceso a la CLI y exploración de ayuda
- Realizar configuraciones en las interfaces de administración de los switches
- Establecer la configuración de los nombres de host y las direcciones IP los switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- Verificar la conectividad entre los dispositivos finales.
- Hacer recopilación de información de la PDU
- Examinar el proceso de ARP en comunicaciones remotas
- Identificar las características físicas de los dispositivos de internetworking
- Verificar la configuración predeterminada del router , configuración inicial y guardar archivos de ejecución

Escenario 1

Escenario:

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

Topología



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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Table 1-Inicialización de dispositivos. Fuente El Autor

Se realiza el reseteo de los 3 Router y también de los switch.

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
```

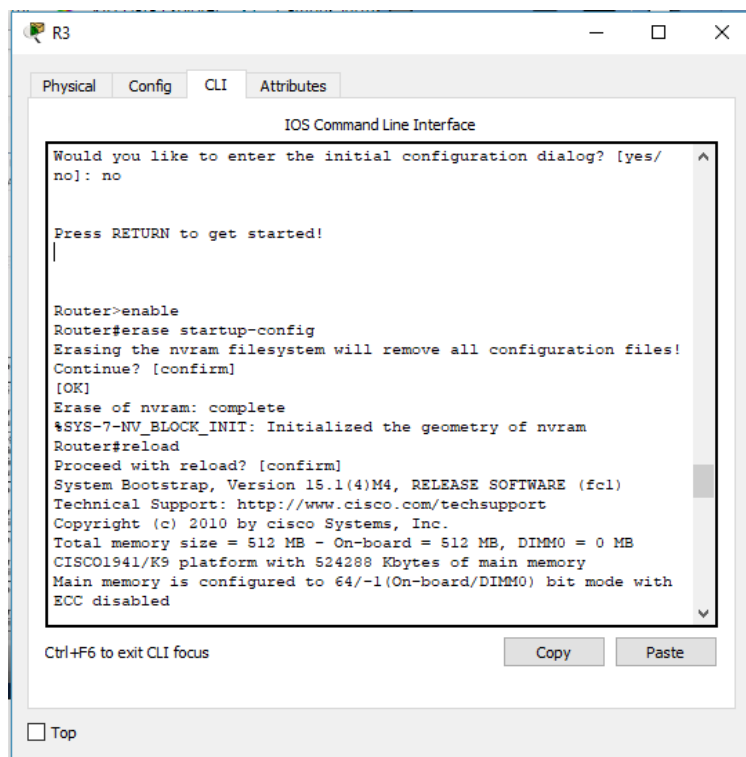


Figure 1 – Comando R3

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):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Table 2 - Configuración servidor - Fuente el Autor

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	Cisco R1(config)#line vty 0 4 R1(config-line)#password Telnet R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd #Se prohíbe el acceso no autorizado#

Interfaz S0/0/0	<p>Establezca la descripción</p> <p>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones 172.16.1.1/30 255.255.255.252</p> <pre>R1(config)#interface serial 0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252</pre> <p>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones 2001:DB8:ACAD:1::1/64</p> <pre>R1(config)#ipv6 unicast-routing R1(config)#interface serial 0/0/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64</pre> <p>Establecer la frecuencia de reloj en 128000</p> <pre>R1(config-if)#clock rate 128000</pre> <p>Activar la interfaz</p> <pre>R1(config-if)#no shutdown</pre>
Rutas predeterminadas	<p>Configurar una ruta IPv4 predeterminada de S0/0/0</p> <pre>R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2</pre> <p>Configurar una ruta IPv6 predeterminada de S0/0/0</p> <pre>R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2</pre>

Table 3 - Configuración R1 - Fuente El Autor

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class

Contraseña de acceso a la consola	<pre> Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login </pre>
Contraseña de acceso Telnet	<pre> Cisco R2(config)#line vty 0 4 R2(config-line)#password Telnet R2(config-line)#login </pre>
Cifrar las contraseñas de texto no cifrado	<pre> R2(config)#service password-encryption </pre>
Habilitar el servidor HTTP	<pre> R2(config)#ip http server Router(config)# ip http secure-server Router(config)# ip http authentication local </pre> <p>Packet tracer no reconoce estos comandos</p>
Mensaje MOTD	<pre> Se prohíbe el acceso no autorizado. R2(config)#banner motd #Se prohíbe el acceso no autorizado# </pre>
Interfaz S0/0/0	<p>Establezca la descripción</p> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <pre> 172.16.1.2/30 255.255.255.252 R2(config)#interface serial 0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 </pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre> 2001:DB8:ACAD:1::2/64 R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 </pre> <p>Activar la interfaz</p> <pre> R2(config-if)#no shutdown </pre>

<p>Interfaz S0/0/1</p>	<p>Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. información de direcciones 172.16.2.2/30 255.255.255.252 R2(config)#interface serial 0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. 2001:DB8:ACAD:2::2/64 R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown</p>
<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz</p> <p>R2(config)#interface s0/0/1 R2(config-if)#description R2-R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown</p>

Interfaz loopback 0 (servidor web simulado)	<p>Establecer la descripción. Establezca la dirección IPv4. R2(config)#interface loopback 0 R2(config-if)#description servidor web simulado</p> <p>R2(config-if)#ip address 10.10.10.10 255.255.255.255</p>
Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0</p>

Table 4 Configuration R2 - Fuente El Autor

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	commando no ip domain-lookup
Nombre del router	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	Cisco R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Cisco R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config)#int s0/0/1 R3(config-if)#description R3-R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 4 R3(config-if)#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. R3(config)#interface loopback 5 R3(config-if)#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. R3(config)#interface loopback 6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface loopback 7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Rutas predeterminadas	<pre>R3(config)#interface s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#interface s0/0/1 R3(config-if)#ipv6 route ::/0 s0/0/1</pre>
-----------------------	---

Table 5 Configuration R3 - Fuente El Autor

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Table 6 Configuration S1 - Fuente El Autor

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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

Table 7 Configuration S3 - Fuente El Autor

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:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Correcto
R2	R3, S0/0/1	172.16.2.2	Correcto
PC de Internet	Gateway predeterminado	10.10.10.10	Correcto

Table 8 - Verificación Conectividad con Ping Escenario 1 –Fuente el Autor


```

R1>en
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 = 1/1/4 ms

R1#

```

Figure 2 Ping R1 con R2, S0/0/0 Fuente El autor

Fuente autor

```

R2>en
Password:
R2#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 = 1/2/9 ms

R2#

```

Figure 3 Ping R2 con R3, S0/0/1 Fuente El Autor

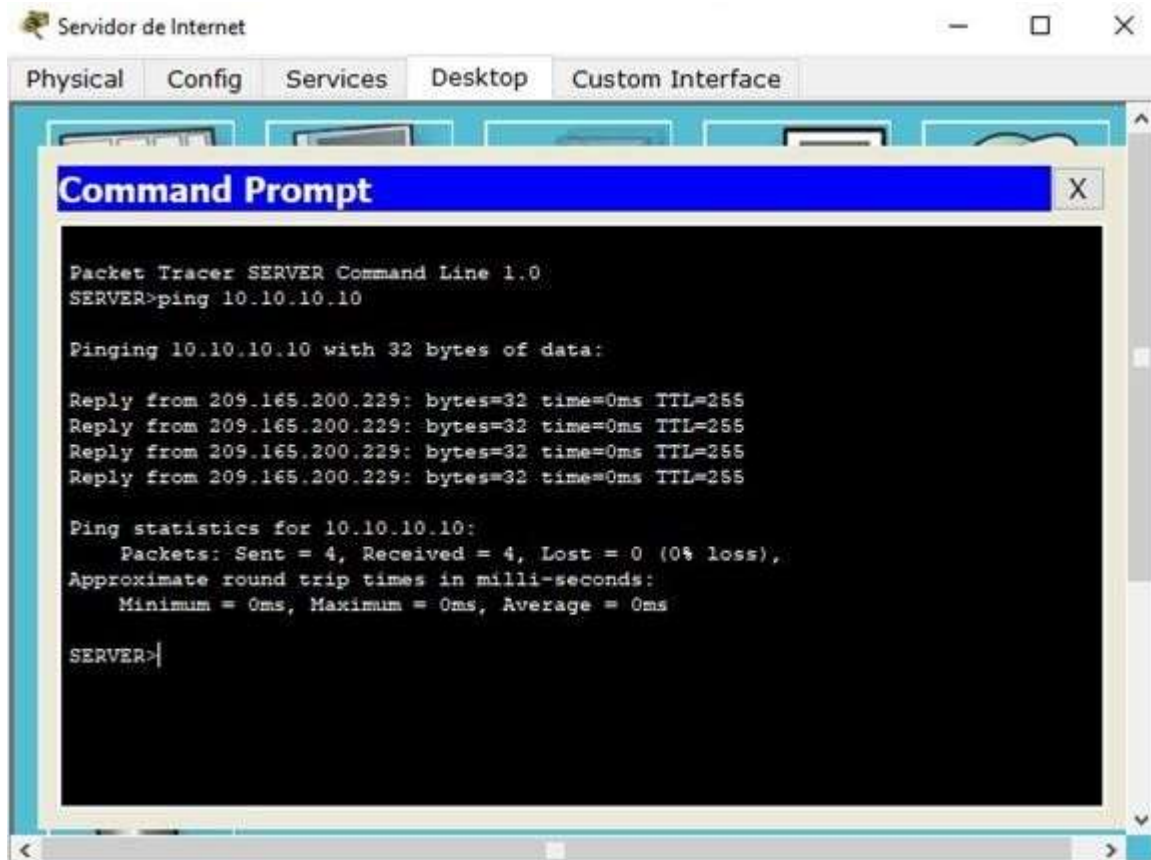


Figure 4 PC de internet con gateway predeterminado Fuente El Autor

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

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

Paso 1 Configurar S1

La configuración del S1 incluye las siguientes tareas:

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 S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface F0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface F0/5 S1(config-if)#switch mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range

Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Table 9 Configuración S1 Fuente El Autor

Paso 2 Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	S3(config)#int f0/8 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Table 10 Configuración S3 Fuente El Autor

Paso 3 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown

Table 11 Configuración VLAN en R1 Fuente El Autor

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:

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

Table 12 Verificación de conectividad de red Fuente El Autor

```

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 = 0/0/0 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#

```

Figure 5 Ping de S1 a R1 Fuente El Autor

```

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#

```

Figure 6 Figura 6. Ping de S3 a R1 Fuente El Autor

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#

```

Figure 7 Figura 6. Ping de S3 a R1, dirección VLAN 99 y R1, dirección VLAN 23 Fuente El Autor

Parte 4 Configurar el protocolo de routing dinámico RIPv2

Paso 1 Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config-router)#no auto-summary

Table 13 Tabla 13 configuracion RIPv2 en R1 Fuente El Autor

Paso 2 Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2

Anunciar las redes conectadas directamente	<p>Nota: Omitir la red G0/0. Revisamos que redes están conectadas R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0</p>
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Table 14 Configuración RIPV2 EN R2 Fuente El Autor

Paso 3 Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2

Anunciar redes IPv4 conectadas directamente	<p>Revisamos que redes están conectadas</p> <pre>R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6</pre> <pre>R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0</pre>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<pre>R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6</pre>
Desactive la sumarización automática.	<pre>R3(config-router)#no auto-summary</pre>

Table 15 Configuración RIPv2 en R3 Fuente El Autor

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:

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?	R1#Show ip protocols
¿Qué comando muestra solo las rutas RIP?	R1# Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1# Show run

Table 16 verificación información RIP en R1, R2 y R3 Fuente El Autor

Parte 5 Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)# R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccnasa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1

<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 R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccnasa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp- config)#default-router 192.168.23.1</p>
--	--

Table 17 Configuración DHCP en R1 Fuente El Autor

Paso 2 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

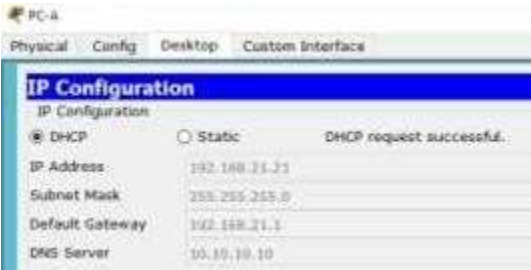

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 secret cisco12345</p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>R2(config)#ip http server</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>R2(config)# R2(config)#ip http authentication local</p>
<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: 209.165.200.229</p>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<p>R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config- if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit</p>

<p>Configurar la NAT dinámica dentro de una ACL privada</p>	<p>Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255</p>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</p>
<p>Definir la traducción de NAT dinámica</p>	<p>R2(config)#ip nat inside source list 1 pool INTERNET</p>

Table 18 Configuración NAT en R2 Fuente El Autor

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.

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	 <p>The screenshot shows the IP Configuration window for PC-A. The DHCP radio button is selected, and the status indicates 'DHCP request successful'. The assigned IP address is 192.168.21.21, with a subnet mask of 255.255.255.0, a default gateway of 192.168.21.1, and a DNS server of 10.10.10.10.</p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p>The screenshot shows the IP Configuration window for PC-C. The DHCP radio button is selected, and the status indicates 'DHCP request successful'. The assigned IP address is 192.168.21.21, with a subnet mask of 255.255.255.0, a default gateway of 192.168.21.1, and a DNS server of 10.10.10.10.</p>

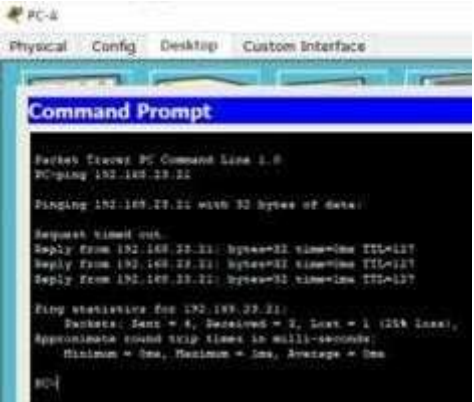
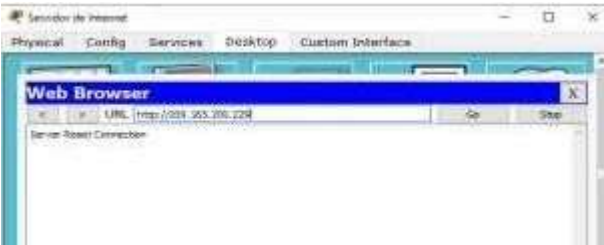
<p>Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	

Table 19 Verificación de SERvicios Fuente El Autor

Parte 6 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configure R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Table 20 Configuración NTP en R1 y R2 Fuente El Autor

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	<p>Nombre de la ACL: ADMIN-MGT</p> <p>R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip access-list standard ADMINMGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit</p>
Aplicar la ACL con nombre a las líneas VTY	<p>R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in</p>
Permitir acceso por Telnet a las líneas de VTY	<p>R2(config-line)#transport input telnet</p>
Verificar que la ACL funcione como se espera	<p>R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado! User Access Verification Password:</p> <p>R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host</p>

Table 21 Configuración acceso VTY en R2 Fuente el Autor

```

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado!

User Access Verification

Password:
% Password: timeout expired!

[Connection to 172.16.1.2 closed by foreign host]
R1#

```

Figure 8 Prueba de Telnet de R1 a R2 Fuente El Autor

```

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

```

Figure 9 Prueba de Telnet de R3 a R2 Fuente El Autor

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

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 access-list Standard IP access list 1 10 permit 192.168.4.0 0.0.0.255 20 permit 192.168.5.0 0.0.0.255 30 permit 192.168.6.0 0.0.0.255 40 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) R2#
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <pre>R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- R2#</pre>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<pre>R2(config)#clear ip nat translation *</pre>

Table 22 Comandos de verificación

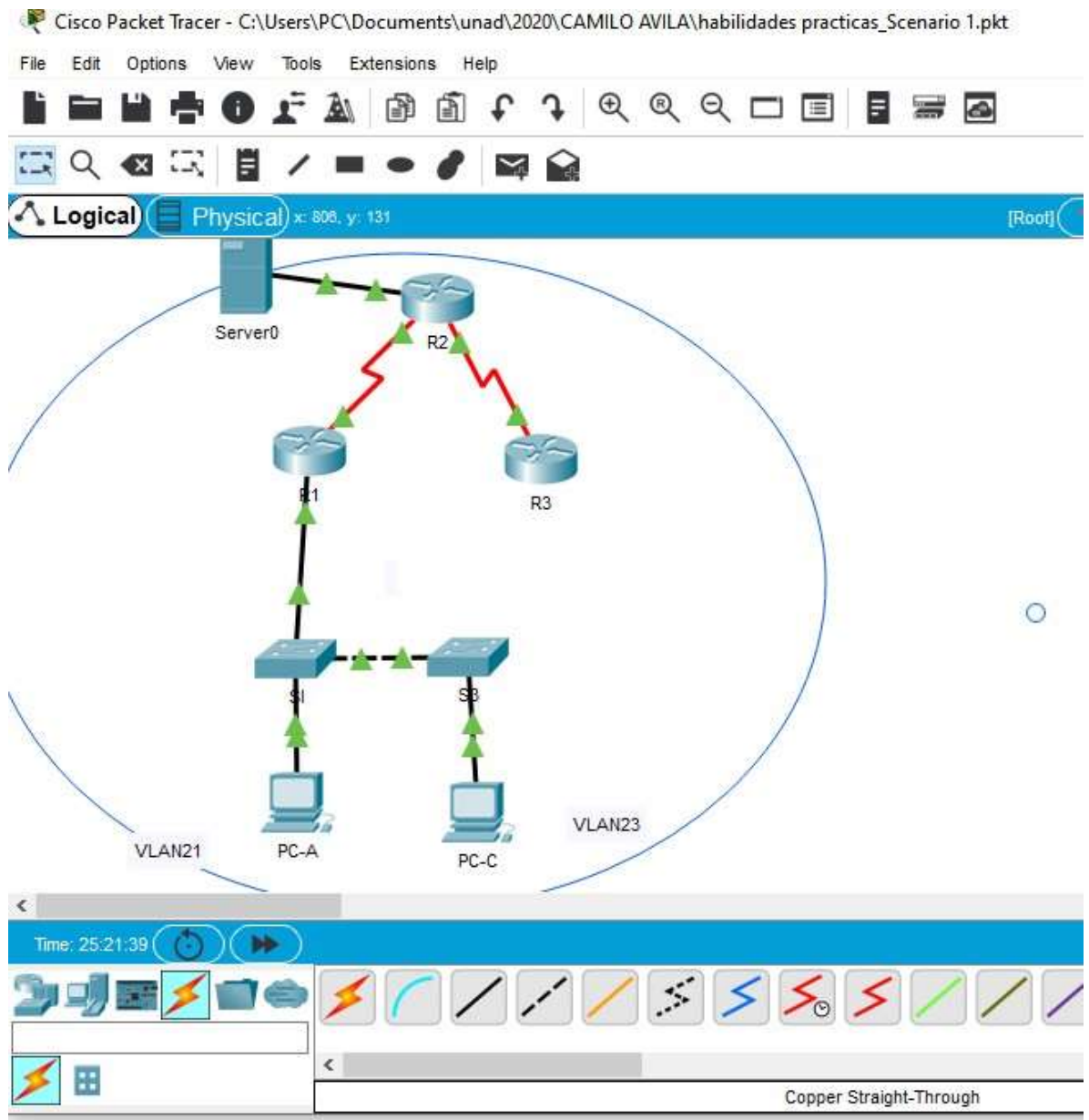


Figure 10 Topologia Escenario 1

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.

Topología de red

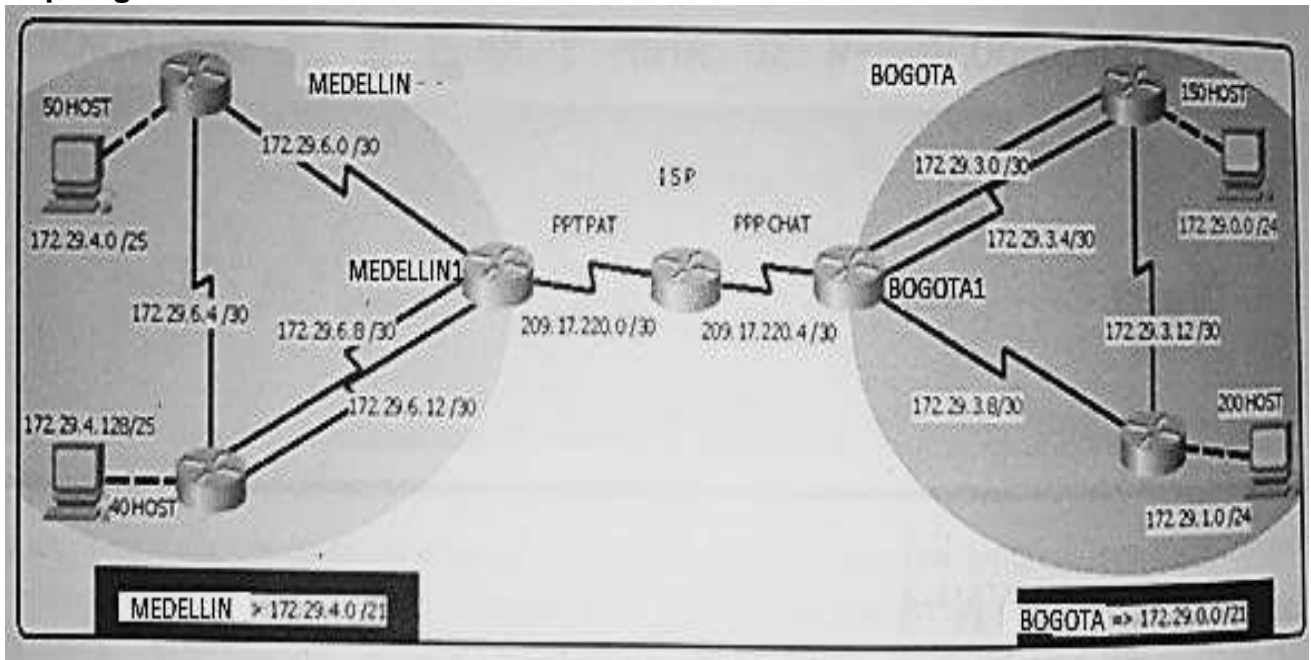


Figure 11 Topología Escenario 2 -Fuente Unad

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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

```
MEDELLIN2(config)#hostname MEDELLIN2
```

```
MEDELLIN2(config)#no ip domain-lookup
```

```
MEDELLIN2(config)#service password-encryption
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 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
```

```
MEDELLIN3(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
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 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
```

```
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#LINE VTY 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
```

```
MEDELLIN>ENABLE
MEDELLIN#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#hostname MEDELLIN1
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
```

```
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#LINE VTY 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
```

```
BOGOTA>ENABLE
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#service password-encryption
BOGOTA(config)#enable secret class
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#LINE VTY 0 15
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#LINE VTY 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
```

```

BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#LINE VTY 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login

```

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

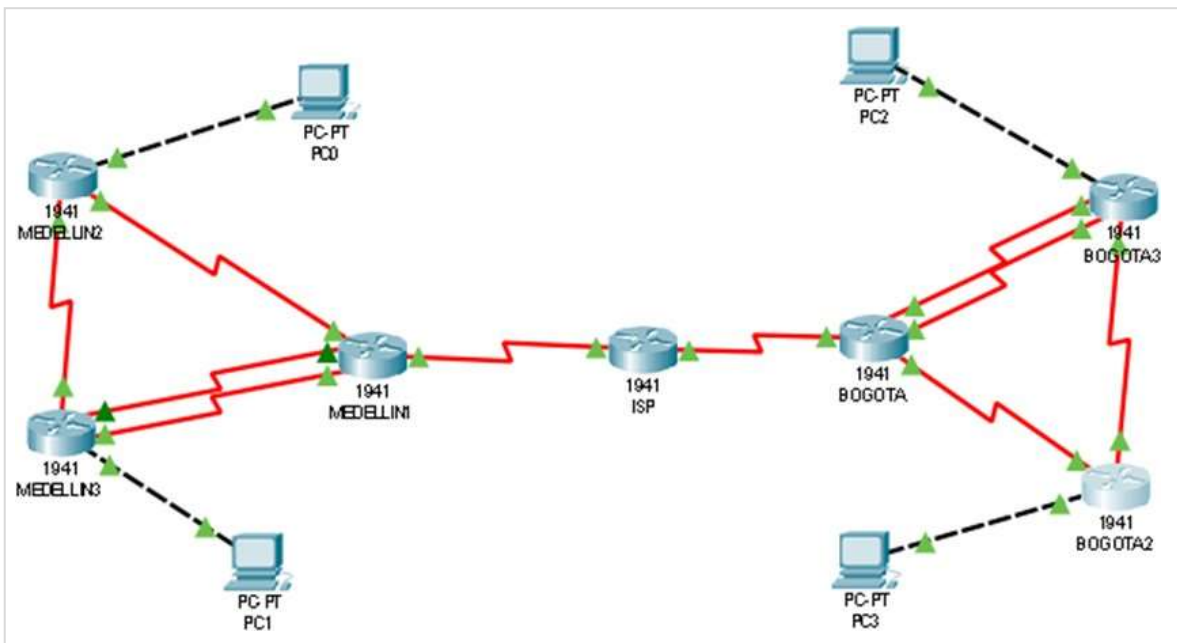


Figure 12 Conexión Equipos Topología Escenario 2

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

Parte 1: Configuración del enrutamiento

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

Router

```
Router>ENABLE
```

```
Router#conf t
```

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

```
Router(config)#int s0/0/0
Router(config-if)#ip address 209.17.220.1 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#int s0/0/1
Router(config-if)#ip address 209.17.220.5 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
```

ROUTER_MEDELLIN1

```
Router>ENABLE
Router#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 209.17.220.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.6.1 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#int s0/1/0
Router(config-if)#ip address 172.29.6.9 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#int s0/1/1
Router(config-if)#ip address 172.29.6.13 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Router(config-if)#
```

ROUTER_MEDELLIN2

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 172.29.6.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.6.5 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#int g0/0
Router(config-if)#ip address 172.29.4.1 255.255.255.128
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

ROUTER_MEDELLIN3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#int s0/0/0
Router(config-if)#ip address 172.29.6.10 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed st
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.6.14 255.255.255.252
```

```
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
Router(config-if)#int s0/1/0
Router(config-if)#ip address 172.29.6.6 255.255.255.252
Router(config-if)#no shut
```

```
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to up
Router(config-if)#int g0/0
Router(config-if)#ip address 172.29.4.129 255.255.255.128
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#
```

BOGOTA1

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 209.17.220.6 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.3.9 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
```

```
Router(config-if)#int s0/1/0
Router(config-if)#ip address 172.29.3.1 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#int s0/1/1
Router(config-if)#ip address 172.29.3.5 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Router(config-if)#
```

BOGOTA2

```
Router(config-if)#int g0/0
Router(config-if)#ip address 172.29.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#int s0/0/0
Router(config-if)#ip address 172.29.3.10 255.255.255.252
Router(config-if)#no shut
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.3.13 255.255.255.252
Router(config-if)#clock rate 4000000
Router(config-if)#no shut
Router(config-if)#
```

BOGOTA3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 172.29.3.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#int
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Router(config-if)#int s0/0/1
Router(config-if)#ip address 172.29.3.6 255.255.255.252
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Router(config-if)#int g0/0
Router(config-if)#ip address 172.29.3.6 255.255.255.252
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
% 172.29.3.4 overlaps with Serial0/0/1
Router(config-if)#int g0/0
Router(config-if)#ip address 172.29.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#
```

MEDELLIN1

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
Router(config-router)#network 172.29.6.0
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#passive-interface s0/0/0
Router(config-router)#
```

MEDELLIN2

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
Router(config-router)#network 172.29.4.0
Router(config-router)#network 172.29.6.0
Router(config-router)#network 172.29.6.4
Router(config-router)#passive-interface g0/0
Router(config-router)#
```

MEDELLIN3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1
Router(config-router)#network 172.29.4.128
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#passive-interface g0/0
Router(config-router)#
```

BOGOTA1

```
Router>
```

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
Router(config-router)#network 172.29.3.0
Router(config-router)#network 172.29.3.4
Router(config-router)#network 172.29.3.8
Router(config-router)#passive-interface s0/0/0
Router(config-router)#
```

BOGOTA2

```
Router(config-router)#
Router(config-router)#
Router(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
Router(config-router)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
Router(config-router)#network 172.29.1.0
Router(config-router)#network 172.29.3.8
Router(config-router)#network 172.29.3.12
Router(config-router)#passive-interface g0/0
Router(config-router)#
```

BOGOTA3

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
Router(config-router)#network 172.29.0.0
Router(config-router)#network 172.29.3.0
Router(config-router)#network 172.29.3.4
Router(config-router)#passive-interface g0/0
Router(config-router)#

```

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

ROUTER MEDELLIN1

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Router(config)#router rip
Router(config-router)#default-information originate
Router(config-router)#

```

ROUTER BOGOTA1

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Router(config)#route rip
Router(config-router)#default-information origina

```

Router(config-router)#

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

Router>enable

Router#conf t

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

Router(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2

Router(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

Router(config)#

Parte 2: Tabla de Enrutamiento.

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

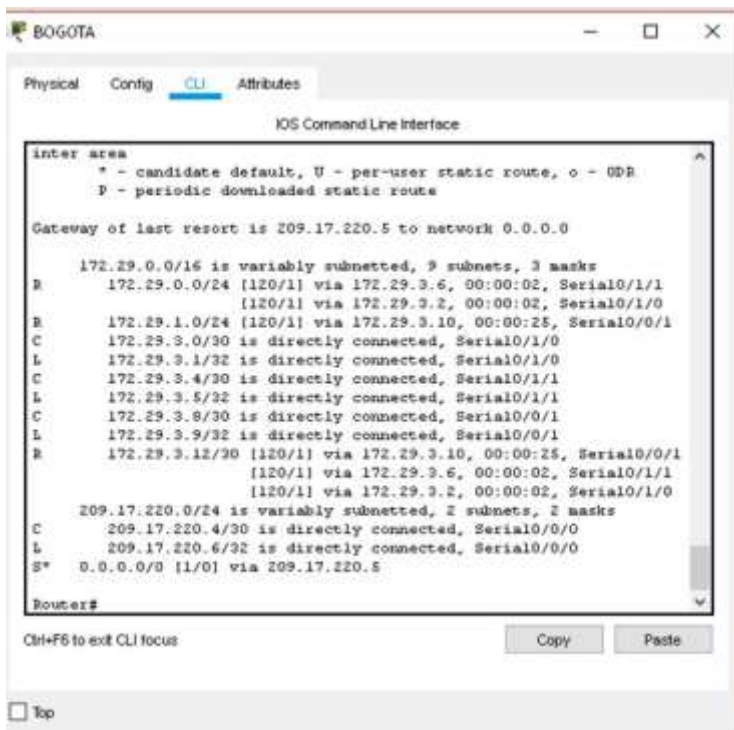


Figure 13 Enrutamiento Router Bogotá Fuente Autor



Figure 14 Enrutamiento Router Medellin1 Fuente Guía Autor

b. Verificar el balanceo de carga que presentan los routers.

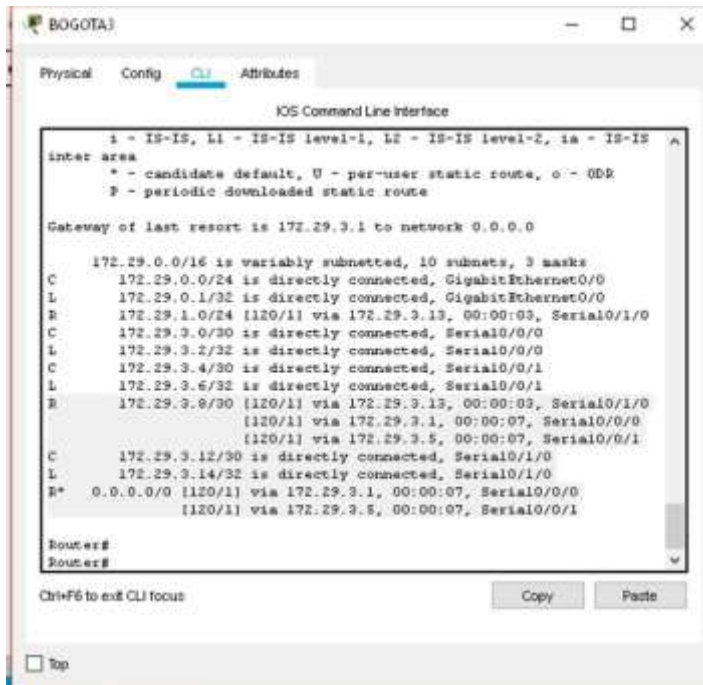


Figure 15 Balanceo de Carga Router 3 Fuente Autor

- c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
- d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
- e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

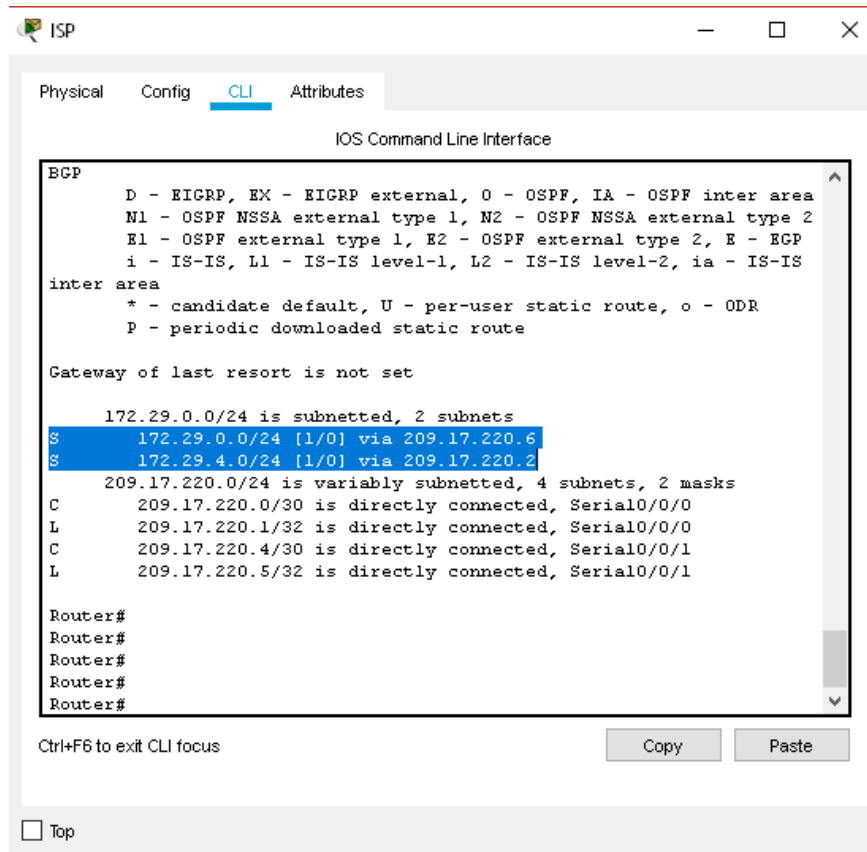


Figure 16 Punto c, d, e y f Fuente El Autor

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1

Medellín3	SERIAL0/0/0; SERIAL0/1/0	SERIAL0/0/1;
ISP	No lo requiere	

Table 23 Propagación de Protocolo Fuente El Autor

Parte 4: Verificación del protocolo OSPF.

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

```

Bogotal#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:12:02
    2.2.2.2          110          00:22:37
    3.3.3.3          110          00:11:24
    4.4.4.4          110          00:07:17
    5.5.5.5          110          00:06:39
    6.6.6.6          110          00:14:48
    7.7.7.7          110          00:11:41
  Distance: (default is 110)

Bogotal#

```

Figure 17 Verificación OSPF Bogotá1 Fuente El Autor

```
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 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.255 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:14:08
    2.2.2.2          110          00:24:44
    3.3.3.3          110          00:13:30
    4.4.4.4          110          00:09:23
    5.5.5.5          110          00:08:45
    6.6.6.6          110          00:16:53
    7.7.7.7          110          00:13:47
  Distance: (default is 110)

Bogota2#
```

Figure 18 Verificación OSPF Bogotá2 Fuente El Autor

```
Bogota3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 6.6.6.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:14:54
    2.2.2.2          110          00:25:29
    3.3.3.3          110          00:14:17
    4.4.4.4          110          00:10:10
    5.5.5.5          110          00:09:31
    6.6.6.6          110          00:17:39
    7.7.7.7          110          00:14:33
  Distance: (default is 110)

Bogota3#
```

Figure 19 Verificación OSPF Bogotá3 Fuente El Autor

```
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 1.1.1.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
    209.17.220.0 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:15:43
    2.2.2.2          110          00:26:18
    3.3.3.3          110          00:15:06
    4.4.4.4          110          00:10:58
    5.5.5.5          110          00:10:20
    6.6.6.6          110          00:18:28
    7.7.7.7          110          00:15:22
  Distance: (default is 110)

Medellin1#
```

Figure 20 Verificación OSPF Medellín1 Fuente El Autor

```
Medellin2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.0 0.0.0.127 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:16:47
    2.2.2.2          110          00:27:21
    3.3.3.3          110          00:16:10
    4.4.4.4          110          00:12:03
    5.5.5.5          110          00:11:24
    6.6.6.6          110          00:19:32
    7.7.7.7          110          00:16:26
  Distance: (default is 110)

Medellin2#
```

Figure 21 Verificación OSPF Medellín2 Fuente El Autor

```
Medellin3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.4.128 0.0.0.127 area 0
    172.29.6.4 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:17:33
    2.2.2.2          110          00:29:08
    3.3.3.3          110          00:16:55
    4.4.4.4          110          00:12:49
    5.5.5.5          110          00:12:10
    6.6.6.6          110          00:20:18
    7.7.7.7          110          00:17:12
  Distance: (default is 110)

Medellin3#
```

Figure 22 Verificación OSPF Medellín2 Fuente El Autor

```
ISP#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 7.7.7.7
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 0
    209.17.220.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:18:54
    2.2.2.2          110          00:29:29
    3.3.3.3          110          00:18:17
    4.4.4.4          110          00:14:10
    5.5.5.5          110          00:13:31
    6.6.6.6          110          00:21:40
    7.7.7.7          110          00:18:33
  Distance: (default is 110)

ISP#
```

Figure 23 Verificación ISP Fuente El Autor

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

MEDELLIN1

```
Router(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
```

BOGOTA1

```
Router(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

ISP

Router>ENABLE

Router#conf t

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

Router(config)#hostname ISP

ISP(config)#username MEDELLIN password cisco

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#

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

ISP(config-if)#ppp authentication pap

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

ISP(config-if)#

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

MEDELLIN1

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#hostname MEDELLIN
MEDELLIN(config)#username ISP password cisco
MEDELLIN(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#encapsulation ppp
MEDELLIN(config-if)#ppp authentication pap
MEDELLIN(config-if)#ppp pap sent-username MEDELLIN password cisco
MEDELLIN(config-if)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#ping 209.17.220.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
-----
Success rate is 0 percent (0/5)

MEDELLIN#ping 209.17.220.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/9 ms
```

BOGOTA

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#username ISP password cisco
BOGOTA(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down

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

```

Parte 6: Configuración de PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.
- c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

MEDELLIN 1

```

MEDELLIN>enable
MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN(config)#

```



```
MEDELLIN(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN(config)#
MEDELLIN(config)# INT S0/0/0
MEDELLIN(config-if)#ip nat outside
MEDELLIN(config-if)# INT S0/0/1
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)# INT S0/1/1
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#INT S0/1/0
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#
```

BOGOTA1

```
BOGOTA>ENABLE
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#ip nat outside
BOGOTA(config-if)#int s0/1/0
BOGOTA(config-if)#ip nat inside
BOGOTA(config-if)#int s0/1/1
BOGOTA(config-if)#ip nat inside
BOGOTA(config-if)#
```

Parte 7: Configuración del servicio DHCP.

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

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
Router(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
Router(config)#ip dhcp pool MEDELLIN2
Router(dhcp-config)#network 172.29.4.0 255.255.255.128
Router(dhcp-config)#default-router 172.29.4.1
```

```
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool MEDELLIN3
Router(dhcp-config)#network 172.29.4.128 255.255.255.128
Router(dhcp-config)#default-router 172.29.4.129
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
```

MEDELLIN3

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip helper-address 172.29.6.5
Router(config-if)#
```

- b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
- c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
- d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

BOGOTA3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
Router(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
Router(config)#ip dhcp pool BOGOTA2
Router(dhcp-config)#NETWORK 172.29.1.0 255.255.255.0
Router(dhcp-config)#DEFAULT-ROUTER 172.29.1.1
Router(dhcp-config)#DEFAULT-ROUTER 172.29.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool BOGOTA3
Router(dhcp-config)#NETWORK 172.29.0.0 255.255.255.0
Router(dhcp-config)#DEFAULT-ROUTER 172.29.0.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#
```

BOGOTA3

```
Router>ENABLE
```

```
Router#conf t
```

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

```
Router(config)#int g0/0
```

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

```
Router(config-if)#
```

```
PC2
Physical  Config  Desktop  Programming  Attributes
Símbolo del Sistema
Pinging 172.29.1.6 with 32 bytes of data:
Reply from 172.29.1.6: bytes=32 time=4ms TTL=126
Reply from 172.29.1.6: bytes=32 time=2ms TTL=126
Reply from 172.29.1.6: bytes=32 time=1ms TTL=126
Reply from 172.29.1.6: bytes=32 time=2ms TTL=126

Ping statistics for 172.29.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>ping 172.29.4.6

Pinging 172.29.4.6 with 32 bytes of data:
Reply from 172.29.4.6: bytes=32 time=0ms TTL=123
Reply from 172.29.4.6: bytes=32 time=4ms TTL=123
Reply from 172.29.4.6: bytes=32 time=5ms TTL=123
Reply from 172.29.4.6: bytes=32 time=4ms TTL=123

Ping statistics for 172.29.4.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 7ms, Average = 5ms

C:\>ping 172.29.4.134

Pinging 172.29.4.134 with 32 bytes of data:
Request timed out.
Reply from 172.29.4.134: bytes=32 time=4ms TTL=123
Reply from 172.29.4.134: bytes=32 time=4ms TTL=123
Reply from 172.29.4.134: bytes=32 time=4ms TTL=123

Ping statistics for 172.29.4.134:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\>
```

Figure 24 Ping de extremo a extremo – pc

CONCLUSIONES

- Se pudo lograr la comprobación de la conectividad de los equipos y encontrar los datos faltantes. También se logró la implementación de las claves de seguridad y la encriptación de las mismas.
- Pudimos identificar el entorno de línea de comando (CLI), incluyendo el ingreso por el modo EXEC de uno de los switch, el cual nos permitió conocer comandos para el ingreso a los modos de configuración tanto global como privilegiado, así mismo la configuración de comandos como lo es Clock (hora)
- Pudimos conocer como el tráfico de un paquete es transmitido de un servidor web a un cliente, así mismo como este paquete se transporta por cada una de las capas de modelo osi, donde se puede verificar los puertos utilizados, direcciones IP, mac de cada uno y los diferentes acciones que estos realizan.
- Pudimos identificar mediante la ejecución url en un web browser como se realiza el proceso de envío y solicitud de paquetes ARP, DNS, HTTP y TCP los cuales viajan a través de los diferentes equipos activos que se encuentran en la red para así desplegarlos en la ventana de un explorador la información solicitada.

REFERENCIAS

Temática: Acceso a la red

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>

Temática: Configuración de un sistema operativo de red

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>

Temática: Ethernet

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

Temática: Exploración de la red

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

Temática: Protocolos y comunicaciones de red

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

ANEXOS

Link con escenarios en PKT

<https://drive.google.com/drive/u/1/folders/1MfDLsQL5ZvZ0k4Gb5gkz8nPVFCTVBPbQ>