

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

HAROLD ANDRÉS GARRIDO GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS DE LA INFORMACIÓN
INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

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

HAROLD ANDRÉS GARRIDO GUZMÁN

Trabajo de Diplomado para optar por el título de Ingeniero de Sistemas

DIEGO EDINSON RAMÍREZ
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS DE LA INFORMACIÓN
INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Ibagué 1 de septiembre. de 2020

DEDICATORIA

Dedicado a mi madre cuyo ejemplo de amor, perseverancia y trabajo ha sido motor para superar cada uno de propósitos y metas trazadas, a mis hermanos cuyo apoyo emocional ha sido fundamental en este proceso educativo y a mis compañeros con quienes un día nos aventuramos a sacar adelante esta carrera.

AGRADECIMIENTOS

Agradecimientos muy especiales a todas las personas que de una u otra manera se han involucrado y me han apoyado en este proceso de aprendizaje, en especial a mi familia, por ellos que son mi razón de ser y mi motivación más grande.

También quisiera agradecer a algunos amigos, colegas y compañeros de estudio los cuales han aportado y compartido su conocimiento y buena voluntad cuando fue requerida, agradecimiento muy especial también a los tutores, directores y personal administrativo de la UNAD, los cuales siempre estuvieron dispuestos a colaborar con dedicación y profesionalismo.

CONTENIDO

	Pág.
1. INTRODUCCIÓN.....	15
2. OBJETIVOS	16
2.1 OBJETIVO GENERAL	16
2.2 OBJETIVOS ESPECÍFICOS	16
Descripción general de la prueba de habilidades.....	17
Escenario 1.....	17
Parte 1: Inicializar dispositivos.....	19
Paso 1: Inicializar y volver a cargar los routers y los switches.....	19
Parte 2: Configurar los parámetros básicos de los dispositivos	19
Paso 1: Configurar la computadora de Internet.....	19
Paso 2: Configurar R1.....	20
Paso 3: Configurar R2.....	21
Paso 4: Configurar R3.....	23
Paso 5: Configurar S1.....	24
Paso 6: Configurar el S3.....	24
Paso 7: Verificar la conectividad de la red.....	25
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	27
Paso 1: Configurar S1.....	27
Paso 2: Configurar el S3.....	31
Paso 3: Configurar R1.....	35
Paso 4: Verificar la conectividad de la red.....	36
Parte 4: Configurar el protocolo de routing dinámico RIPv2.....	37
Paso 1: Configurar RIPv2 en el R1	37
Paso 2: Configurar RIPv2 en el R2	37
Paso 3: Configurar RIPv3 en el R2	38
Paso 4: Verificar la información de RIP	38
Parte 5: Implementar DHCP y NAT para IPv4	40
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	40
Paso 2: Configurar la NAT estática y dinámica en el R2	41

Paso 3: Verificar el protocolo DHCP y la NAT estática.....	44
Parte 6: Configurar NTP	45
Parte 1: Configurar y verificar las listas de control de acceso (ACL).....	46
Paso 1: Restringir el acceso a las líneas VTY en el R2	46
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	47
Escenario 2.....	48
Topología de red.....	48
Parte 1: Configuración del enrutamiento.....	49
Paso 2: Configuración enrutamiento con protocolo OSPF	56
Paso 3: Configuración de rutas estáticas en Router ISP.....	58
Parte 2: Tabla de Enrutamiento.	59
Enrutamiento ISP.....	59
Enrutamiento Medellín1	60
Enrutamiento Medellín2.....	61
Enrutamiento Medellín3.....	62
Enrutamiento Bogota1	62
Enrutamiento Bogota2	64
Enrutamiento Bogota3	65
Parte 3: Deshabilitar la propagación del protocolo OSPF.	66
Parte 4: Verificación del protocolo OSPF.....	67
Enrutamiento Medellin1	68
Enrutamiento Medellin2	68
Enrutamiento Medellin3	69
Enrutamiento Bogota1	69
Enrutamiento Bogota2	70
Enrutamiento Bogota3	70
Enrutamiento ISP.....	71
Parte 5: Configurar encapsulamiento y autenticación PPP.	71
Habilitar autenticación PAP con el enlace MEDELLIN1.....	72
Habilitar autenticación CHAT de PPP entre BOGOTA1 y el ISP.....	72
Parte 6: Configuración de PAT.	73

Configurar NAT en MEDELLIN1	73
Configurar NAT en Bogota1	74
Verificar ping entre MEDELLIN1 y Medellin2	74
Parte 7: Configuración del servicio DHCP.....	75
Configurar DHCP en router Medellin2.....	75
Configurar DHCP en router Bogota2.....	75
Habilitar el paso de mensaje broadcast hacia la ip del router Bogota2	76
CONCLUSIONES	77
LINK SUSTENTACIÓN.....	77
BIBLIOGRAFÍA.....	78

LISTA DE TABLAS

Tabla 1 Inicializar dispositivos.....	19
Tabla 2 Parte 2: Configurar los parámetros básicos de los dispositivos	19
Tabla 3 Paso 2: Configurar R1	21
Tabla 4 Paso 3: Configurar R2.....	22
Tabla 5 Paso 4: Configurar R3.....	24
Tabla 6 Paso 5: Configurar S1	24
Tabla 7 Paso 6: Configurar el S3	25
Tabla 8 Paso 7: Verificar la conectividad de la red	26
Tabla 9 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	31
Tabla 10 Paso 2: Configurar el S3.....	34
Tabla 11 Paso 3: Configurar R1	35
Tabla 12 Paso 4: Verificar la conectividad de la red	36
Tabla 13 Parte 4: Configurar el protocolo de routing dinámico RIPv2.....	37
Tabla 14 Paso 2: Configurar RIPv2 en el R2.....	37
Tabla 15 Paso 3: Configurar RIPv3 en el R2.....	38
Tabla 16 Paso 4: Verificar la información de RIP	40
Tabla 17 Parte 5: Implementar DHCP y NAT para IPv4	41
Tabla 18 Paso 2: Configurar la NAT estática y dinámica en el R2.....	43
Tabla 19 Paso 3: Verificar el protocolo DHCP y la NAT estática	45
Tabla 20 Parte 6: Configurar NTP	46
Tabla 21 Parte 1: Configurar y verificar las listas de control de acceso (ACL).....	47
Tabla 22 Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	47
Tabla 23 Parte 3: Deshabilitar la propagación del protocolo OSPF.....	66

LISTA DE ILUSTRACIONES

	Pág
Ilustración 1 PRUEBA DE HABILIDADES CCNA 2020 Escenario 1	17
Ilustración 2 Topología Red Escenario 1	18
Ilustración 3 ping 172.16.1.2 desde R1	26
Ilustración 4 ping 209.165.200.233 desde servidor de internet	26
Ilustración 5 show ip protocols R1	39
Ilustración 6 debug ip rip R1	39
Ilustración 7 show ip route R1	40
Ilustración 8 show ip dhcp binding	44
Ilustración 9 dhcp PC-A	44
Ilustración 10 dhcp PC-B	45
Ilustración 11 ping 192.168.21.22 desde PC-A	45
Ilustración 12 show ntp associations R1	46
Ilustración 13 ping 192.168.21.1 desde S1	47
Ilustración 14 ping 192.168.21.1 desde R2	47
Ilustración 15 PRUEBA DE HABILIDADES CCNA 2020 Escenario 2	48
Ilustración 16 Topología de Red Escenario 2	48
Ilustración 17 show ip route ospf ISP	59
Ilustración 18 show ip protocols ISP	59
Ilustración 19 show ip route ospf MEDELLIN1	60
Ilustración 20 show ip protocols MEDELLIN1	60
Ilustración 21 show ip route ospf MEDELLIN2	61
Ilustración 22 show ip protocols MEDELLIN2	61
Ilustración 23 show ip route ospf MEDELLIN3	62
Ilustración 24 show ip protocols MEDELLIN3	62
Ilustración 25 show ip route ospf BOGOTA1	62
Ilustración 26 show ip protocols BOGOTA1	63
Ilustración 27 show ip route ospf BOGOTA2	64
Ilustración 28 show ip protocols BOGOTA2	64
Ilustración 29 show ip route ospf BOGOTA3	65
Ilustración 30 show ip protocols BOGOTA3	65
Ilustración 31 show ip protocols MEDELLIN1	68
Ilustración 32 show ip protocols MEDELLIN2	68
Ilustración 33 show ip protocols MEDELLIN3	69
Ilustración 34 show ip protocols BOGOTA1	69
Ilustración 35 show ip protocols BOGOTA2	70
Ilustración 36 show ip protocols BOGOTA3	70
Ilustración 37 show ip protocols ISP	71
Ilustración 38 ping 172.29.6.1 desde MEDELLIN2	74

GLOSARIO

ACL: Una lista de control de acceso, con respecto a un sistema de archivos de computadora, es una lista de permisos adjuntos a un objeto. Una ACL especifica qué usuarios o procesos del sistema tienen acceso a los objetos, así como qué operaciones están permitidas en determinados objetos.

BROADCAST: la difusión amplia, difusión ancha o broadcast, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CLI: La interfaz de línea de comandos o interfaz de línea de órdenes es un método que permite a los usuarios dar instrucciones a algún programa informático por medio de una línea de texto simple.

DHCP: El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

DNS: El sistema de nombres de dominio es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

FIREWALL: En informática, un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

GATEWAY: Puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

INTERFAZ: Una interfaz se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier

tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de información.

IPv4: Es el Protocolo de Internet versión 4, es la cuarta versión del Internet Protocol, un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET.

IPv6: Es un nuevo protocolo con el que se generan nuevos tipos de direcciones IP más largos y complejos. Estas direcciones son las matrículas que utilizan los dispositivos a la hora de conectarse a Internet.

ISP: El proveedor de servicios de Internet, es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como ADSL, cablemódem, GSM, dial-up, etc.

LAN: Red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

MÁSCARA DE SUBRED: La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

NAT: La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles

NTP: Network Time Protocol es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

OSPF: Open Shortest Path First, Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

PAP: Password Authentication Protocol o PAP es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet.

PAT: Port Address Translation (PAT) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet.

PPP: Protocolo punto a punto, es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

PUERTO: En informática, un puerto es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

ROUTER: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

ROUTING: El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN).

TELNET: Es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

VLAN: (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

Este trabajo es realizado en el desarrollo de la prueba de habilidades prácticas CCNA diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN), donde se pretende mediante dos escenarios realizar la configuración de redes LAN utilizando la herramienta Cisco Packet Tracer, con el objetivo de aplicar los conocimientos adquiridos a lo largo del diplomado, conocimientos que serán de gran importancia en el mundo laboral, teniendo en cuenta que las telecomunicaciones desempeñan un papel importante en la estructura de las empresas para el manejo de la información.

Esta actividad nos pone en el rol de un administrador de red en una empresa y nos enfrenta al desafío de diseñar, configurar y comprobar el buen funcionamiento de las redes informáticas, gracias a esto aplicamos muchos conceptos y conocimientos prácticos adquiridos a lo largo de este curso.

1. INTRODUCCIÓN

En la Prueba De Habilidades CCNA del Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN) ponemos en práctica las destrezas adquiridas a través del proceso de aprendizaje del curso, todo esto nos permite configurar una red de área local de forma simulada mediante la herramienta Cisco Packet Tracer, una red pequeña de equipos que permite conectividad 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. De igual manera el uso del OSPF como protocolo de enrutamiento entre dos routers que hacen parte redes ubicadas en dos ciudades diferentes.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Aplicar habilidades adquiridas en el manejo de herramientas para el diseño e implementación de soluciones integradas en una red LAN.

2.2 OBJETIVOS ESPECÍFICOS

Implementar la topología de red en un escenario de forma simulada con el Cisco Packet Tracer.

Configurar dispositivos en una red que permita conectividad entre sí.

Identificar procesos de enrutamiento y aplicación de debidos protocolos.

Validar conectividad y correcto funcionamiento de la red y sus dispositivos.

Descripción general de la prueba de habilidades
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

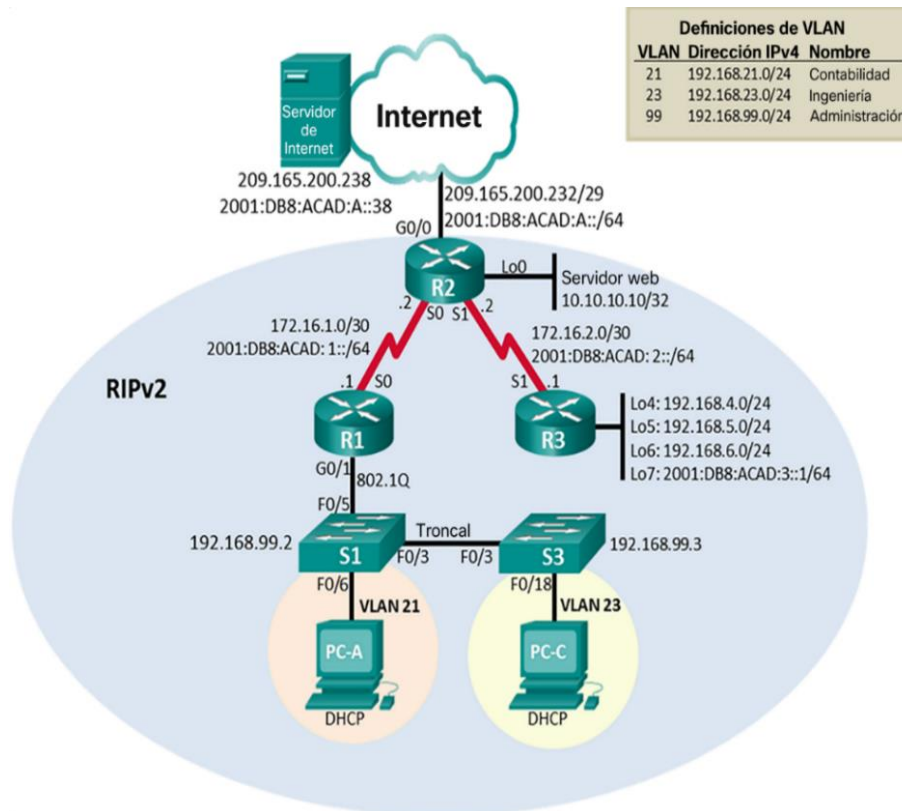


Ilustración 1 PRUEBA DE HABILIDADES CCNA 2020 Escenario 1

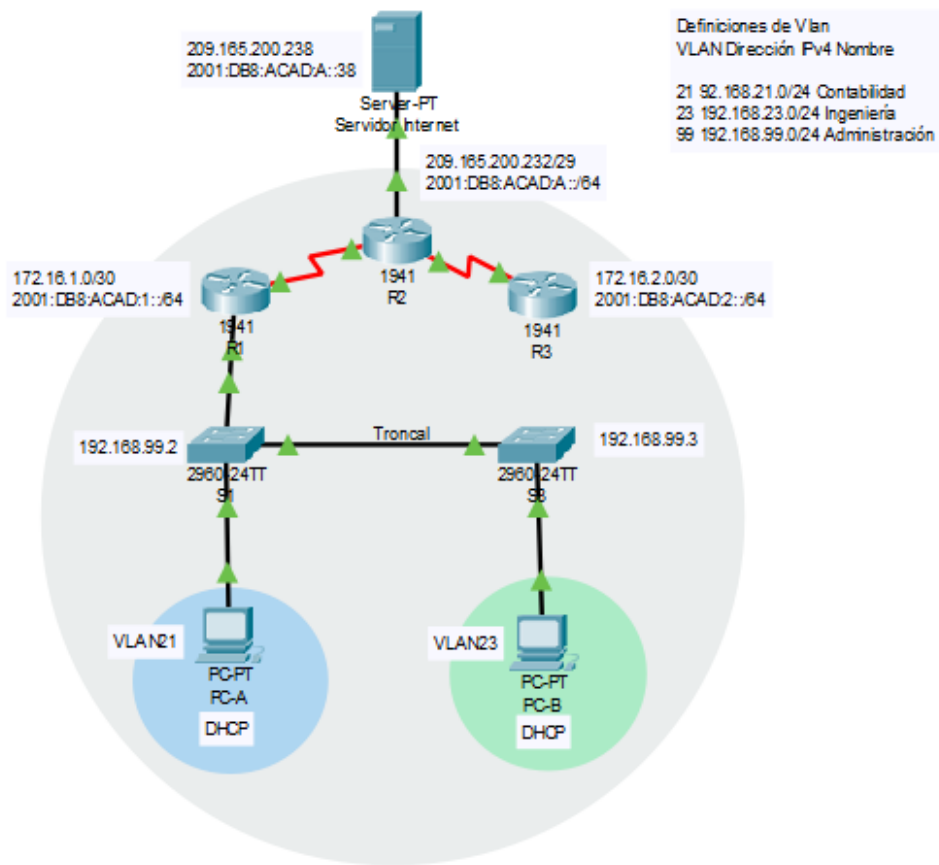


Ilustración 2 Topología Red Escenario 1

Descripción Topología Red Escenario 1

Para la realización de la red del escenario 1 seleccionamos cada uno de los dispositivos que forman parte de ella, servidor de red, routers, switches y PC's, realizamos las conexiones de acuerdo a las características de cada dispositivo dependiendo si es inalámbrico o alámbrico y se agregaron las direcciones IP de acuerdo a la topología, a cada dispositivo se le agregan contraseñas de seguridad sugeridas en la guía de actividades.

El router 1 que se conecta a dos switch los cuales están conectados mediante una troncal entre sí. este router también lo configuramos como servidor dhcp para que los PC's tomen el direccionamiento automáticamente según la VLAN a la que se conecten, en estos switches tenemos configurada la vlan21, la vlan23 y la vlan99.

El router 2 tiene configurado una loopback 0, también le configuramos las listas de acceso para permitir la v21 y v23 y otra para permitir acceso desde el router 1 al router 2 a través de telnet.

El router 3 tiene configurado las loopback 4, 5, 6 y 7.

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

Tabla 1 Inicializar dispositivos

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	209.165.200.232
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1/64

Tabla 2 Parte 2: Configurar los parámetros básicos de los dispositivos

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
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/1/0	Interface serial 0/1/0 Establezca la descripción description Enlace al R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Ipv6 address 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000 Clock rate 128000 Activar la interfaz No shutdown

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/1/0 Ip route 0.0.0.0 0.0.0.0 172.16.1.2 Configurar una ruta IPv6 predeterminada de S0/1/0 Ipv6 route 2001:DB8:ACAD:1::2
-----------------------	--

Tabla 3 Paso 2: Configurar R1

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
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	banner motd "Se prohíbe el acceso no autorizado."
Interfaz S0/1/0	Establezca la descripción Description Enlace al R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Ip address 172.16.1.2 255.255.255.252 No shutdown Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz No shutdown

<p>Interfaz S0/1/1</p>	<p>Establecer la descripción Description Enlace a R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. 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. Ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. Activar la interfaz No shutdown</p>
<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Establecer la descripción. Description Enlace a Servidor Internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Ip address 2001:DB8:ACAD:A::1/64 Activar la interfaz No shutdown</p>
<p>Interfaz loopback 0 (servidor web simulado)</p>	<p>Establecer la descripción. Description Enlace a servidor web simulado Establezca la dirección IPv4. Ip address 10.10.10.11 255.255.255.255</p>
<p>Ruta predeterminada</p>	<p>Configure una ruta IPv4 predeterminada de G0/0. Ip route 0.0.0.0 0.0.0.0 209.165.200.238 Configure una ruta IPv6 predeterminada de G0/0. Ipv6 route ::/0 2001:DB8:ACAD:A::38</p>

Tabla 4 Paso 3: Configurar R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/1/1	<p>Establecer la descripción Description Enlace a R2</p> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Ip address 172.16.2.1 255.255.255.252</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Ipv6 address 2001:DB8:ACAD:2::1/64</p> <p>Activar la interfaz No shutdown</p>
Interfaz loopback 4	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 4 Ip address 192.168.4.1 255.255.255.0</p>
Interfaz loopback 5	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 5 Ip address 192.168.5.1 255.255.255.0</p>

Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Interface loopback 7 Ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	

Tabla 5 Paso 4: Configurar R3

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
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 6 Paso 5: Configurar S1

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
Contraseña de exec privilegiado cifrada	class

Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 7 Paso 6: Configurar el S3

Paso 7: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	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 = 1/1/5 ms
R2	R3, S0/1/1	172.16.2.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms
PC de Internet	Gateway predeterminado	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

			<p>Reply from 209.165.200.233: bytes=32 time<1ms TTL=255</p> <p>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</p>
--	--	--	---

Tabla 8 Paso 7: Verificar la conectividad de la red

```

R1>enable
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

Ilustración 3 ping 172.16.1.2 desde R1

```

Packet Tracer SERVER Command Line 1.0
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=11ms 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 = 11ms, Average = 2ms

C:\>

```

Ilustración 4 ping 209.165.200.233 desde servidor de internet

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 23 S1(config-vlan)#name ingenieria S1(config)#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 native S1(config)#interface fastethernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk allowed vlan all

<p>Forzar el enlace troncal en la interfaz F0/5</p>	<p>Utilizar la red VLAN 1 como VLAN native S1(config)#interface fastethernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switch trunk allowed vlan all</p>
<p>Configurar el resto de los puertos como puertos de acceso</p>	<p>Utilizar el comando interface range S1(config-if-range)#interface range fastethernet 0/1-2, f0/4-5, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#</p>
<p>Asignar F0/6 a la VLAN 21</p>	<p>S1(config-if-range)#interface fastethernet 0/6 S1(config-if)#switchport access vlan 21</p>

<p>Apagar todos los puertos sin usar</p>	<pre> S1(config)#interface range fastethernet 0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down </pre>
--	--

	<p>%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down</p>
--	--

	<pre>%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down S1(config-if-range)#</pre>
--	---

Tabla 9 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

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	<p>Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.</p> <pre>S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#</pre>
Asignar la dirección IP de administración	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología</p> <pre>S3(config)#interface vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0</pre>
Asignar el gateway predeterminado.	<p>Asignar la primera dirección IP en la subred como gateway predeterminado.</p> <pre>S3(config)#ip default-gateway 192.168.99.1</pre>

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native S3(config)#interface f0/3 S3(config-if)#switch port mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#switchport trunk allowed vlan all
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switch port mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface f0/18 S3(config-if)#switchport access vlan 21

<p>Apagar todos los puertos sin usar</p>	<pre>S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down</pre>
--	---

	<p>%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down</p> <p>S3(config-if-range)#</p>
--	---

Tabla 10 Paso 2: Configurar el S3

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 R1(config-subif)#description LAN de contabilidad Asignar la VLAN 21 R1(config)#interface gigabitethernet 0/1.1 R1(config-subif)#encapsulation dot1q 21 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config-subif)#description LAN de Ingenieria Asignar la VLAN 23 R1(config-subif)#interface gigabitethernet 0/1.2 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.2, changed state to up R1(config-subif)#encapsulation dot1q 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config-subif)#description LAN de Administracion Asignar la VLAN 99 R1(config-if)#interface gigabitethernet 0/1.3 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.3, changed state to up R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Tabla 11 Paso 3: Configurar R1

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	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 = 0/3/6 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

Tabla 12 Paso 4: Verificar la conectividad de la red

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. R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface default
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13 Parte 4: Configurar el protocolo de routing dinámico RIPv2

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	Nota: Omitir la red G0/0. R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.10
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14 Paso 2: Configurar RIPv2 en el R2

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	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15 Paso 3: Configurar RIPv3 en el R2

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

```

R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 7 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
  GigabitEthernet0/1.99 2    2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.16.0.0
  192.168.99.0
Passive Interface(s):
  Vlan1
  GigabitEthernet0/0
  GigabitEthernet0/1
  Serial0/1/0
  Serial0/1/1
Routing Information Sources:
  Gateway         Distance      Last Update
  172.16.1.2      120           00:00:20
Distance: (default is 120)
R1#

```

Ilustración 5 show ip protocols R1

```

R1#debug ip rip
RIP protocol debugging is on
R1#RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/1.9
(192.168.99.1)
RIP: build update entries
  10.10.10.11/32 via 0.0.0.0, metric 2, tag 0
  172.16.1.0/30 via 0.0.0.0, metric 1, tag 0
  172.16.2.0/30 via 0.0.0.0, metric 2, tag 0
  192.168.4.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.5.0/24 via 0.0.0.0, metric 3, tag 0
  192.168.6.0/24 via 0.0.0.0, metric 3, tag 0
RIP: received v2 update from 172.16.1.2 on Serial0/1/0
  10.10.10.11/32 via 0.0.0.0 in 1 hops
  172.16.2.0/30 via 0.0.0.0 in 1 hops
  192.168.4.0/24 via 0.0.0.0 in 2 hops
  192.168.5.0/24 via 0.0.0.0 in 2 hops
  192.168.6.0/24 via 0.0.0.0 in 2 hops
RIP: received v2 update from 172.16.1.2 on Serial0/1/0
  10.10.10.11/32 via 0.0.0.0 in 1 hops
  172.16.2.0/30 via 0.0.0.0 in 1 hops
  192.168.4.0/24 via 0.0.0.0 in 2 hops
  192.168.5.0/24 via 0.0.0.0 in 2 hops
  192.168.6.0/24 via 0.0.0.0 in 2 hops

```

Ilustración 6 debug ip rip R1

<pre> R1#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 172.16.1.2 to network 0.0.0.0 10.0.0.0/32 is subnetted, 1 subnets R 10.10.10.11/32 [120/1] via 172.16.1.2, 00:00:13, Serial0/1/0 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks C 172.16.1.0/30 is directly connected, Serial0/1/0 L 172.16.1.1/32 is directly connected, Serial0/1/0 R 172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:13, Serial0/1/0 R 192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:13, Serial0/1/0 R 192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:13, Serial0/1/0 R 192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:13, Serial0/1/0 192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 L 192.168.21.1/32 is directly connected, GigabitEthernet0/1.21 192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 L 192.168.23.1/32 is directly connected, GigabitEthernet0/1.23 192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 L 192.168.99.1/32 is directly connected, GigabitEthernet0/1.99 S* 0.0.0.0/0 [1/0] via 172.16.1.2 </pre>	
<p><i>Ilustración 7 show ip route R1</i></p>	

Tabla 16 Paso 4: Verificar la información de RIP

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(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

<p>Crear un pool de DHCP para la VLAN 21.</p>	<pre> 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)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)# </pre>
<p>Crear un pool de DHCP para la VLAN 23</p>	<pre> Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)# </pre>

Tabla 17 Parte 5: Implementar DHCP y NAT para IPv4

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>	<pre> Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 password cisco12345 </pre>

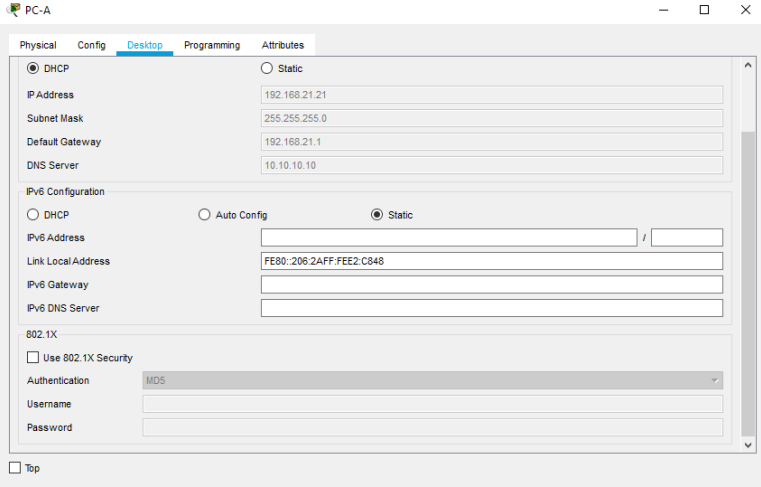
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Nota: Packet tracer no tiene habilitado este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local Nota: Packet tracer no tiene habilitado este comando
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 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 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255

<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</p> <pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</pre>
<p>Definir la traducción de NAT dinámica</p>	<pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>

Tabla 18 Paso 2: Configurar la NAT estática y dinámica en el R2

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>	<pre data-bbox="699 548 1437 724"> R1#show ip dhcp binding IP address Client-ID/ Hardware address 192.168.21.21 0006.2AE2.C848 -- Automatic 192.168.21.22 0001.6304.0B73 -- Automatic </pre> <p data-bbox="911 737 1242 764"><i>Ilustración 8 show ip dhcp binding</i></p>  <p data-bbox="963 1283 1190 1310"><i>Ilustración 9 dhcp PC-A</i></p>

<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p style="text-align: center;"><i>Ilustración 10 dhcp PC-B</i></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 style="text-align: center;"><i>Ilustración 11 ping 192.168.21.22 desde PC-A</i></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>	

Tabla 19 Paso 3: Verificar el protocolo DHCP y la NAT estática

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 mar 05 2016 R2#show clock 9:0:17.327 UTC Sat Mar 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	<pre>R1#show ntp associations address ref clock st when poll reach delay offset disp *-172.16.1.2 127.127.1.1 S 10 16 377 2.00 -1.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured</pre> <p><i>Ilustración 12 show ntp associations R1</i></p>

Tabla 20 Parte 6: Configurar NTP

Parte 1: 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	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	<pre>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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms Ilustración 13 ping 192.168.21.1 desde S1 R2#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 0 percent (0/5) Ilustración 14 ping 192.168.21.1 desde R2</pre>

Tabla 21 Parte 1: Configurar y verificar las listas de control de acceso (ACL)

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
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters [número de lista o nombre]
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show access-list
¿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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#show ip nat translations

Tabla 22 Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

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

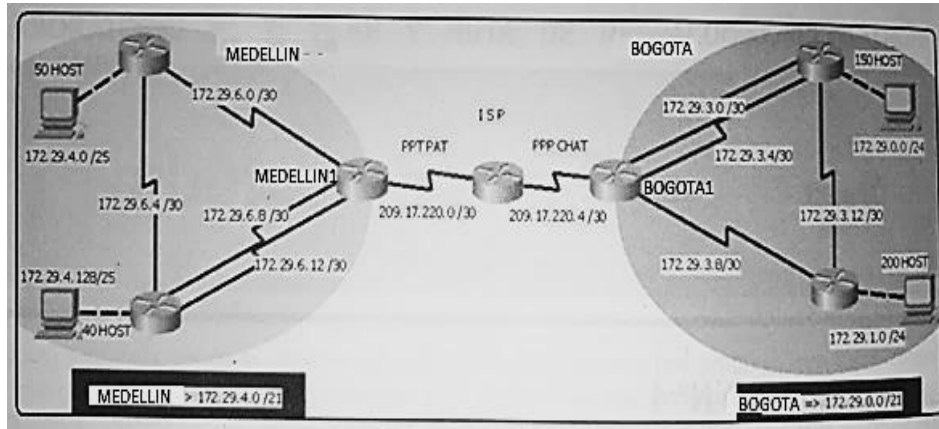


Ilustración 15 PRUEBA DE HABILIDADES CCNA 2020 Escenario 2

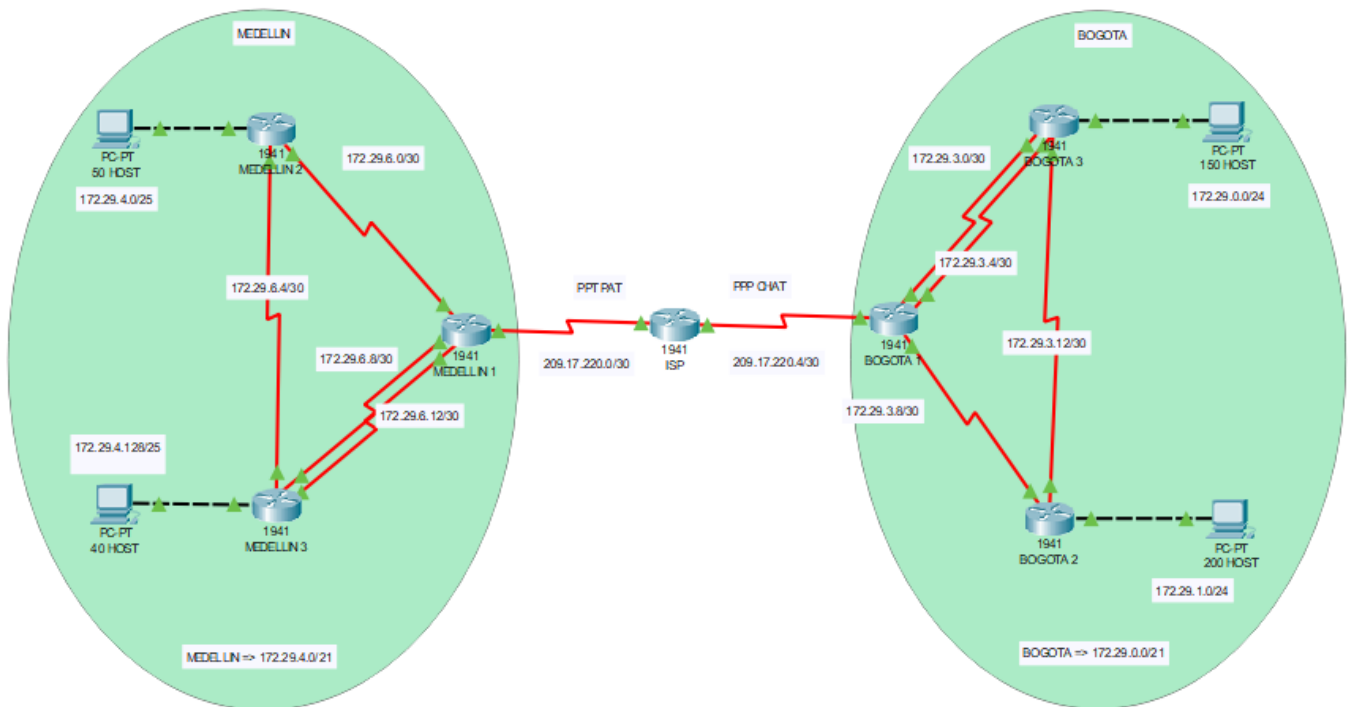


Ilustración 16 Topología de Red Escenario 2

Descripción Topología Red Escenario 2

De igual manera que en el escenario 1 se realizan las rutinas de diagnóstico y dejamos los equipos listos para su configuración: asignación de nombres de dispositivos, asignar claves de seguridad, etc También hacemos la conexión física de los equipos con base en la topología de red.

Tenemos dos redes ubicadas en dos ciudades diferentes, una en Bogotá y la otra en Medellín y un router de un proveedor de servicios de internet, configuramos DHCP, configuramos el encapsulamiento PPP y PAP para establecer una conexión directa entre dos nodos de una red.

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

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

Parte 1: Configuración del enrutamiento

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

Configuración básica

```
Router>enable
```

```
Router#config
```

```
Configuring from terminal, memory, or network [terminal]? t
```

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

```
Router(config)#hostname ISP
```

```
ISP(config)#enable secret cisco
```

```
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
```

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

```
ISP(config)#banner motd "Acceso no autorizado"
```

Direccionamiento ip interface s0/1/1

```
ISP(config)#interface s0/1/1
```

```
ISP(config-if)#description Enlace a MEDELLIN 1
```

```
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
```

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

```
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
```

Direccionamiento ip interface s0/1/0

```
ISP(config-if)#interface s0/1/0
```

```
ISP(config-if)#description Enlace a BOGOTA 1
```

```
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
```

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

Router MEDELLIN1

Configuración básica

```
Router>enable
```

```
Router#config
```

```
Configuring from terminal, memory, or network [terminal]? t
```

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

```
Router(config)#hostname MEDELLIN1
```

```
MEDELLIN1(config)#enable secret cisco
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
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#banner motd "Acceso no autorizado"
```

Configuración de ruta por defecto hacia ISP

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

Direccionamiento ip interface s0/0/0

```
MEDELLIN1(config)#interface s0/0/0
MEDELLIN1(config-if)#description Enlace a ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
```

Direccionamiento ip interface s0/0/1

```
MEDELLIN1(config-if)#interface s0/0/1
MEDELLIN1(config-if)#description Enlace a MEDELLIN 3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

Direccionamiento ip interface s0/1/1

```
MEDELLIN1(config-if)#interface s0/1/1
MEDELLIN1(config-if)#description Enlace MEDELLIN3_S011
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

Direccionamiento ip interface s0/1/0

```
MEDELLIN1(config-if)#interface s0/1/0
MEDELLIN1(config-if)#description Enlace a MEDELLIN2_S010
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

```
Router MEDELLIN2
Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#enable secret cisco
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
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#banner motd "Acceso no autorizado"
```

```
Direccionamiento ip interface s0/1/0
MEDELLIN2(config)#interface s0/1/0
MEDELLIN2(config-if)#description Enlace a MEDELLIN1_S010
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
```

```
Direccionamiento ip interface s0/1/1
MEDELLIN2(config-if)#interface s0/1/1
MEDELLIN2(config-if)#description Enlace MEDELLIN3_S011
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
```

```
Router MEDELLIN3
Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#enable secret cisco
```

```
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
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#banner motd "Acceso no autorizado"
```

```
Direccionamiento ip interface s0/0/0
MEDELLIN3(config)#interface s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
```

```
Direccionamiento ip interface s0/1/0
MEDELLIN3(config-if)#interface s0/1/0
MEDELLIN3(config-if)#description Enlace a MEDELLIN1_S010
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
```

```
Direccionamiento ip interface s0/1/1
MEDELLIN3(config-if)#interface s0/1/1
MEDELLIN3(config-if)#description Enlace a MEDELLIN2_S011
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
```

Router BOGOTA1

Configuración básica

```
Router>enable
```

```
Router#config
```

```
Configuring from terminal, memory, or network [terminal]? t
```

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

```
Router(config)#hostname BOGOTA1
```

```
BOGOTA1(config)#enable secret cisco
```

```
BOGOTA1(config)#line console 0
```

```
BOGOTA1(config-line)#password cisco
```

```
BOGOTA1(config-line)#login
```

```
BOGOTA1(config-line)#line vty 0 15
```

```
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#banner motd "Acceso no autorizado"
```

Configuración de ruta por defecto hacia ISP

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

Direccionamiento ip interface s0/0/0

```
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#description Enlace a ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
```

Direccionamiento ip interface s0/1/0

```
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#description Enlace a BOGOTA3_S010
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
```

Direccionamiento ip interface s0/0/1

```
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#description Enlace a BOGOTA3_S001
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
```

Direccionamiento ip interface s0/1/1

```
BOGOTA1(config-if)#interface s0/1/1
BOGOTA1(config-if)#description Enlace a BOGOTA2_S011
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
```

Router BOGOTA2

Configuración básica

```
Router>enable
```

```
Router#config
```

```
Configuring from terminal, memory, or network [terminal]? t
```

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

```
Router(config)#hostname BOGOTA2
BOGOTA2(config)#enable secret cisco
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
BOGOTA2(config-line)#exit
BOGOTA2(config)#banner motd "Acceso no autorizado"
```

Direccionamiento ip interface s0/1/1

```
BOGOTA2(config)#interface s0/1/1
BOGOTA2(config-if)#description Enlace a BOGOTA1_S011
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
```

Direccionamiento ip interface s0/1/0

```
BOGOTA2(config-if)#interface s0/1/0
BOGOTA2(config-if)#description BOGOTA3_S010
BOGOTA2(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
```

Router BOGOTA3

Configuración básica

```
Router>enable
```

```
Router#config
```

Configuring from terminal, memory, or network [terminal]? t

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

```
Router(config)#hostname BOGOTA3
BOGOTA3(config)#enable secret cisco
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
```

```
BOGOTA3(config-line)#exit
BOGOTA3(config)#banner motd "Acceso no autorizado"
```

```
Direccionamiento ip interface s0/1/0
BOGOTA3(config)#interface s0/1/0
BOGOTA3(config-if)#description Enlace BOGOTA1_S010
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
```

```
Direccionamiento ip interface s0/0/0
BOGOTA3(config-if)#interface s0/0/0
BOGOTA3(config-if)#description Enlace BOGOTA1_S000
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
```

```
Direccionamiento ip interface s0/1/1
BOGOTA3(config-if)#interface s0/1/1
BOGOTA3(config-if)#description Enlace a BOGOTA2_S011
BOGOTA3(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
```

Paso 2: Configuración enrutamiento con protocolo OSPF

```
Router ISP
ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 1
00:19:58: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/1/1 from
LOADING to FULL, Loading Done
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 1
```

```
Router MEDELLIN1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
00:16:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/1/0 from
LOADING to FULL, Loading Done
```


MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
00:16:53: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/1/1 from
LOADING to FULL, Loading Done

MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
00:17:26: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/0/1 from
LOADING to FULL, Loading Done

MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 1

Router MEDELLIN2

MEDELLIN2(config)#router ospf 1

MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1

MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1

MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 1

Router MEDELLIN3

MEDELLIN3(config)#router ospf 1

MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3

MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1

00:11:47: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/1/1 from
LOADING to FULL, Loading Done

MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1

MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1

MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 1

Router BOGOTA1

BOGOTA1(config)#router ospf 1

BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 1

00:22:56: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/0/0 from
LOADING to FULL, Loading Done

BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1

BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1

BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1

Router BOGOTA2

BOGOTA2(config)#router ospf 1

BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1

00:30:43: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.13 on Serial0/1/0 from
LOADING to FULL, Loading Done

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1

00:31:08: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/1 from
LOADING to FULL, Loading Done

BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 1

Router BOGOTA3

BOGOTA3(config)#router ospf 1

BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1

00:25:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from
LOADING to FULL, Loading Done

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1

00:26:21: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0 from
LOADING to FULL, Loading Done

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1

Paso 3: Configuración de rutas estáticas en Router ISP

Ruta estatica hacia la red de Medellín y sumarización a 22

ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/1/1

ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/1/1

Ruta estatica hacia la red de Bogotá y sumarización a 22

ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/1/0

ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/1/0

Parte 2: Tabla de Enrutamiento.

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

Enrutamiento ISP

```
ISP#show ip route ospf
      172.29.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.29.6.0 [110/128] via 209.17.220.2, 00:01:19, Serial0/1/1
O       172.29.6.8 [110/128] via 209.17.220.2, 00:01:19, Serial0/1/1
O       172.29.6.12 [110/128] via 209.17.220.2, 00:01:19, Serial0/1/1
```

Ilustración 17 show ip route ospf ISP

```
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 209.17.220.5
  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 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.17.220.2     110          00:04:34
    209.17.220.5     110          00:04:34
  Distance: (default is 110)
```

Ilustración 18 show ip protocols ISP

Enrutamiento Medellín1

```
MEDELLIN1>enable
MEDELLIN1#show ip route ospf
    172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O    172.29.3.0 [110/192] via 209.17.220.1, 00:50:35, Serial0/0/0
O    172.29.3.4 [110/192] via 209.17.220.1, 00:50:35, Serial0/0/0
O    172.29.3.8 [110/192] via 209.17.220.1, 00:50:35, Serial0/0/0
O    172.29.3.12 [110/256] via 209.17.220.1, 00:50:35, Serial0/0/0
O    172.29.6.4 [110/128] via 172.29.6.10, 00:50:35, Serial0/1/1
    [110/128] via 172.29.6.2, 00:50:35, Serial0/1/0
    209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O    209.17.220.4 [110/128] via 209.17.220.1, 00:50:35, Serial0/0/0
```

Ilustración 19 show ip route ospf MEDELLIN1

```
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 209.17.220.2
  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 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    209.17.220.0 0.0.0.3 area 1
  Routing Information Sources:
  Gateway         Distance      Last Update
  172.29.3.13     110          00:04:52
  172.29.3.14     110          00:04:50
  172.29.6.5      110          00:04:49
  172.29.6.14     110          00:04:50
  209.17.220.2    110          00:04:50
  209.17.220.5    110          00:04:50
  209.17.220.6    110          00:04:51
  Distance: (default is 110)
```

Ilustración 20 show ip protocols MEDELLIN1

Enrutamiento Medellín2

```
MEDELLIN2>ENABLE
MEDELLIN2#show ip route ospf
    172.29.0.0/16 is variably subnetted, 10 subnets, 2 masks
O       172.29.3.0 [110/256] via 172.29.6.1, 00:51:52, Serial0/1/0
O       172.29.3.4 [110/256] via 172.29.6.1, 00:51:52, Serial0/1/0
O       172.29.3.8 [110/256] via 172.29.6.1, 00:51:52, Serial0/1/0
O       172.29.3.12 [110/320] via 172.29.6.1, 00:51:52, Serial0/1/0
O       172.29.6.8 [110/128] via 172.29.6.6, 00:51:52, Serial0/1/1
        [110/128] via 172.29.6.1, 00:51:52, Serial0/1/0
O       172.29.6.12 [110/128] via 172.29.6.6, 00:51:52, Serial0/1/1
        [110/128] via 172.29.6.1, 00:51:52, Serial0/1/0
    209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.1, 00:51:52, Serial0/1/0
O       209.17.220.4 [110/192] via 172.29.6.1, 00:51:52, Serial0/1/0
```

Ilustración 21 show ip route ospf MEDELLIN2

```
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 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.0 0.0.0.3 area 1
    172.29.4.0 0.0.0.127 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:08:06
    172.29.3.14      110          00:08:04
    172.29.6.5       110          00:08:03
    172.29.6.14      110          00:08:04
    209.17.220.2     110          00:08:04
    209.17.220.5     110          00:08:04
    209.17.220.6     110          00:08:05
  Distance: (default is 110)
```

Ilustración 22 show ip protocols MEDELLIN2

Enrutamiento Medellín3

```
MEDELLIN3>enable
MEDELLIN3#show ip route ospf
      172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O       172.29.3.0 [110/256] via 172.29.6.9, 00:53:06, Serial0/1/0
O       172.29.3.4 [110/256] via 172.29.6.9, 00:53:06, Serial0/1/0
O       172.29.3.8 [110/256] via 172.29.6.9, 00:53:06, Serial0/1/0
O       172.29.3.12 [110/320] via 172.29.6.9, 00:53:06, Serial0/1/0
O       172.29.6.0 [110/128] via 172.29.6.5, 00:53:06, Serial0/1/1
        [110/128] via 172.29.6.9, 00:53:06, Serial0/1/0
      209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.9, 00:53:06, Serial0/1/0
O       209.17.220.4 [110/192] via 172.29.6.9, 00:53:06, Serial0/1/0
```

Ilustración 23 show ip route ospf MEDELLIN3

```
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 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    172.29.4.128 0.0.0.127 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:08:55
    172.29.3.14      110          00:08:53
    172.29.6.5       110          00:08:52
    172.29.6.14      110          00:08:53
    209.17.220.2     110          00:08:53
    209.17.220.5     110          00:08:53
    209.17.220.6     110          00:08:54
  Distance: (default is 110)
```

Ilustración 24 show ip protocols MEDELLIN3

Enrutamiento Bogota1

```
BOGOTA1>ENABLE
BOGOTA1#show ip route ospf
      172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O       172.29.3.12 [110/128] via 172.29.3.6, 00:54:32, Serial0/0/1
        [110/128] via 172.29.3.10, 00:54:32, Serial0/1/1
O       172.29.6.0 [110/192] via 209.17.220.5, 00:54:22, Serial0/0/0
O       172.29.6.4 [110/256] via 209.17.220.5, 00:54:22, Serial0/0/0
O       172.29.6.8 [110/192] via 209.17.220.5, 00:54:22, Serial0/0/0
O       172.29.6.12 [110/192] via 209.17.220.5, 00:54:22, Serial0/0/0
      209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
O       209.17.220.0 [110/128] via 209.17.220.5, 00:54:32, Serial0/0/0
```

Ilustración 25 show ip route ospf BOGOTA1

```

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:
    209.17.220.4 0.0.0.3 area 1
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:10:01
    172.29.3.14      110          00:09:59
    172.29.6.5       110          00:09:58
    172.29.6.14      110          00:09:59
    209.17.220.2     110          00:09:59
    209.17.220.5     110          00:09:59
    209.17.220.6     110          00:09:59
  Distance: (default is 110)

```

Ilustración 26 show ip protocols BOGOTA1

Enrutamiento Bogota2

```
BOGOTA2#show ip route ospf
 172.29.0.0/16 is variably subnetted, 10 subnets, 2 masks
O   172.29.3.0 [110/128] via 172.29.3.13, 01:13:17, Serial0/1/0
   [110/128] via 172.29.3.9, 01:13:17, Serial0/1/1
O   172.29.3.4 [110/128] via 172.29.3.13, 01:13:17, Serial0/1/0
   [110/128] via 172.29.3.9, 01:13:17, Serial0/1/1
O   172.29.6.0 [110/256] via 172.29.3.9, 01:13:07, Serial0/1/1
O   172.29.6.4 [110/320] via 172.29.3.9, 01:13:07, Serial0/1/1
O   172.29.6.8 [110/256] via 172.29.3.9, 01:13:07, Serial0/1/1
O   172.29.6.12 [110/256] via 172.29.3.9, 01:13:07, Serial0/1/1
209.17.220.0/30 is subnetted, 2 subnets
O   209.17.220.0 [110/192] via 172.29.3.9, 01:13:07, Serial0/1/1
O   209.17.220.4 [110/128] via 172.29.3.9, 01:13:17, Serial0/1/1
```

Ilustración 27 show ip route ospf BOGOTA2

```
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:
    172.29.3.12 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    172.29.1.0 0.0.0.255 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13     110          00:12:16
    172.29.3.14     110          00:12:14
    172.29.6.5      110          00:12:14
    172.29.6.14     110          00:12:15
    209.17.220.2    110          00:12:15
    209.17.220.5    110          00:12:14
    209.17.220.6    110          00:12:15
  Distance: (default is 110)
```

Ilustración 28 show ip protocols BOGOTA2

Enrutamiento Bogota3

```
BOGOTA3>enable
BOGOTA3#show ip route ospf
    172.29.0.0/16 is variably subnetted, 11 subnets, 2 masks
O       172.29.3.8 [110/128] via 172.29.3.14, 00:56:45, Serial0/1/1
        [110/128] via 172.29.3.5, 00:56:45, Serial0/0/0
O       172.29.6.0 [110/256] via 172.29.3.5, 00:56:45, Serial0/0/0
O       172.29.6.4 [110/320] via 172.29.3.5, 00:56:45, Serial0/0/0
O       172.29.6.8 [110/256] via 172.29.3.5, 00:56:45, Serial0/0/0
O       172.29.6.12 [110/256] via 172.29.3.5, 00:56:45, Serial0/0/0
    209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/192] via 172.29.3.5, 00:56:45, Serial0/0/0
O       209.17.220.4 [110/128] via 172.29.3.5, 00:56:45, Serial0/0/0
```

Ilustración 29 show ip route ospf BOGOTA3

```
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 209.17.220.5
  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 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110          00:14:07
    172.29.3.14      110          00:14:07
    172.29.6.5       110          00:14:06
    172.29.6.14      110          00:14:06
    209.17.220.2     110          00:14:06
    209.17.220.5     110          00:14:06
    209.17.220.6     110          00:14:06
  Distance: (default is 110)
```

Ilustración 30 show ip protocols BOGOTA3

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

Tabla 23 Parte 3: Deshabilitar la propagación del protocolo OSPF.

Router BOGOTA1

```
BOGOTA1(config-router)#passive-interface s0/1/1
BOGOTA1(config-router)#passive-interface s0/0/1
BOGOTA1(config-router)#passive-interface s0/1/0
```

Router BOGOTA2

```
BOGOTA2(config-router)#passive-interface s0/1/0
BOGOTA2(config-router)#passive-interface s0/1/1
07:21:21: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

Router BOGOTA3

```
BOGOTA3(config-router)#passive-interface s0/0/0
07:16:44: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

```
BOGOTA3(config-router)#passive-interface s0/1/0
```

```
07:17:26: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

```
BOGOTA3(config-router)#passive-interface s0/1/1
07:18:03: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.14 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

Router MEDELLIN1

```
MEDELLIN1(config-router)#passive-interface s0/0/1
07:25:35: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
MEDELLIN1(config-router)#passive-interface s0/1/0
07:26:44: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/1/0 from FULL
to DOWN, Neighbor Down: Interface down or detached
```

```
MEDELLIN1(config-router)#passive-interface s0/1/1
07:27:01: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

Router MEDELLIN2

```
MEDELLIN2(config-router)#passive-interface s0/1/0
MEDELLIN2(config-router)#passive-interface s0/1/1
07:29:00: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.14 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

Router MEDELLIN3

```
MEDELLIN3(config-router)#passive-interface s0/0/0
MEDELLIN3(config-router)#passive-interface s0/1/0
MEDELLIN3(config-router)#passive-interface s0/1/1
```

Parte 4: Verificación del protocolo OSPF.

- a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.
- b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Verificación de rutas a través de comandos show ip route ospf y show ip protocols.

Enrutamiento 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 209.17.220.2
  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 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    209.17.220.0 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/1
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.17.220.2    110          00:04:21
    209.17.220.5    110          00:04:21
  Distance: (default is 110)
```

Ilustración 31 show ip protocols MEDELLIN1

Enrutamiento Medellin2

```
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 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.0 0.0.0.3 area 1
    172.29.4.0 0.0.0.127 area 1
    172.29.4.128 0.0.0.127 area 1
  Passive Interface(s):
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5      110          00:06:50
  Distance: (default is 110)
```

Ilustración 32 show ip protocols MEDELLIN2

Enrutamiento Medellin3

```
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 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    172.29.4.128 0.0.0.127 area 1
  Passive Interface(s):
    Serial0/0/0
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.14     110          00:10:00
  Distance: (default is 110)
```

Ilustración 33 show ip protocols MEDELLIN3

Enrutamiento Bogota1

```
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:
    209.17.220.4 0.0.0.3 area 1
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/1
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.17.220.6    110          00:00:14
  Distance: (default is 110)
```

Ilustración 34 show ip protocols BOGOTA1

Enrutamiento Bogota2

```
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:
    172.29.3.12 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    172.29.1.0 0.0.0.255 area 1
  Passive Interface(s):
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.14     110          00:02:00
  Distance: (default is 110)
```

Ilustración 35 show ip protocols BOGOTA2

Enrutamiento Bogota3

```
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 172.29.3.13
  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 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.12 0.0.0.3 area 1
    172.29.0.0 0.0.0.255 area 1
  Passive Interface(s):
    Serial0/0/0
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13     110          00:05:08
  Distance: (default is 110)
```

Ilustración 36 show ip protocols BOGOTA3

Enrutamiento ISP

```
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 209.17.220.5
  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 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.17.220.2           110          00:00:31
    209.17.220.5           110          00:00:31
  Distance: (default is 110)
```

Ilustración 37 show ip protocols ISP

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.

Encapsulamiento en MEDELLIN1

```
MEDELLIN1(config)#interface s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#no shutdown
```

Encapsulamiento en BOGOTA1

```
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#no shutdown
```

Encapsulamiento en ISP s0/1/1

```
ISP(config)#interface s0/1/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#interface
```

```
Encapsulamiento en ISP s0/1/0
ISP(config-if)#interface s0/1/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
```

Habitar autenticación PAP con el enlace MEDELLIN1

Configuración PAP en ISP con enlace MEDELLIN1

```
ISP(config)#username medellin1 secret medellin1
ISP(config)#interface s0/1/1
ISP(config-if)#ppp authentication pap
09:18:23: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/1/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
ISP(config-if)#ppp pap sent-username isp password isp
```

Habilitar autenticación CHAT de PPP entre BOGOTA1 y el ISP

Configuración CHAP de PPP en ISP con BOGOTA1

```
ISP(config)#username bogota1 secret bogota1
ISP(config)#interface s0/1/0
ISP(config-if)#ppp authentication chap
```

```
09:27:58: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

Configuración CHAP de PPP en BOGOTA1 con ISP

```
BOGOTA1(config)#username isp secret isp
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#end
```


Configuración PAP en MEDELLIN1 con enlace ISP

```
MEDELLIN1(config)#username isp secret isp
```

```
MEDELLIN1(config)#interface s0/0/0
```

```
MEDELLIN1(config-if)#ppp authentication pap
```

```
MEDELLIN1(config-if)#ppp pap sent-username medellin1 password medellin1
```

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.

Configurar NAT en MEDELLIN1

```
MEDELLIN1(config)#ip access-list standard HOST
```

```
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
```

```
MEDELLIN1(config-std-nacl)#exit
```

```
MEDELLIN1(config)#ip nat inside source list HOST interface s0/1/0 overload
```

```
MEDELLIN1(config)#interface s0/1/0
```

```
MEDELLIN1(config-if)#ip nat inside
```

```
MEDELLIN1(config-if)#interface s0/0/0
```

```
MEDELLIN1(config-if)#ip nat outside
```

```
MEDELLIN1(config-if)#interface s0/0/1
```

```
MEDELLIN1(config-if)#ip nat inside
```

```
MEDELLIN1(config-if)#interface s0/1/1
```

```
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#end
```

Configurar NAT en Bogota1

```
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/1/1 overload
BOGOTA1(config)#interface s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#end
```

Verificar ping entre MEDELLIN1 y Medellin2

```
MEDELLIN2#ping 172.29.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/70
ms
```

Ilustración 38 ping 172.29.6.1 desde MEDELLIN2

Parte 7: Configuración del servicio DHCP.

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

Configurar DHCP en router Medellin2

```
MEDELLIN2(config)#ip dhcp excluden-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN2(dhcp-config)#exit
```

Habilitar el paso de mensaje broadcast hacia la ip del router MEDELLIN2

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

Configurar DHCP en router Bogota2

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
```

```
BOGOTA2(config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
```

Habilitar el paso de mensaje broadcast hacia la ip del router Bogota2

```
BOGOTA3(config)#interface g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.14
```

CONCLUSIONES

En el primer escenario se logra la optimización y configuración de esta red es necesario aplicar algunos protocolos que permitan la conectividad de los equipos, entre ellos se destacan protocolos de red IPv4 e IPv6, protocolo de routing dinámico RIPv2, protocolo de configuración de hosts dinámicos (DHCP), mediante la Interfaz de línea de comandos CLI.

A través de las VLAN podemos crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch.

Mientras que en el segundo escenario nos enfrentamos al rol de administrador de red de una empresa la cual requiere una interconexión entre dos sucursales en dos ciudades diferentes, en este caso el uso de OSPF como protocolo de enrutamiento para distribuir la información de ruteo.

Podemos afirmar que la configuración OSPF contribuye a mejorar el balanceo de carga, además permite que se definan las redes lógicamente en donde los routers se pueden diferentes áreas.

LINK SUSTENTACIÓN

Prueba de Habilidades Prácticas CCNA Diplomado de Profundización CISCO
(diseño e implementación de soluciones integradas LAN / WAN)

Harold Andrés Garrido Guzmán

<<https://youtu.be/ek72jBFAuRE>>

BIBLIOGRAFÍA

CISCO NETWORKING ACADEMY. “Exploración de la red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>).

CISCO NETWORKING ACADEMY. “Configuración de un sistema operativo de red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>).

CISCO NETWORKING ACADEMY. “Protocolos y comunicaciones de red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>).

CISCO NETWORKING ACADEMY. “Acceso a la red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>).

CISCO NETWORKING ACADEMY. “Ethernet. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>).

CISCO NETWORKING ACADEMY. “Capa de red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>).

CISCO NETWORKING ACADEMY. “Capa de red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>).

CISCO NETWORKING ACADEMY. “Asignación de direcciones IP. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>).

CISCO NETWORKING ACADEMY. “SubNetting. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>).

CISCO NETWORKING ACADEMY. “Capa de Aplicación. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>).

CISCO NETWORKING ACADEMY. “Soluciones de Red. Fundamentos de Networking”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>).

CISCO NETWORKING ACADEMY. “Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>).

CISCO NETWORKING ACADEMY. “Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>).

CISCO NETWORKING ACADEMY. VLANs. “Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>).

CISCO NETWORKING ACADEMY. “Conceptos de Routing. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>).

CISCO NETWORKING ACADEMY. “Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>).

CISCO NETWORKING ACADEMY. “Enrutamiento Estático. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>).

CISCO NETWORKING ACADEMY. “Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>).

CISCO NETWORKING ACADEMY. “OSPF de una sola área. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>).

CISCO NETWORKING ACADEMY. “Listas de control de acceso. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>).

CISCO NETWORKING ACADEMY. “DHCP. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>).

CISCO NETWORKING ACADEMY. “Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación”. {En línea}. {Consultado junio 2020} disponible en: (<https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>).

VESGA, Juan. “OVI: Introducción al laboratorio remoto SmartLab”. {En línea}. {Consultado junio 2020} disponible en: (<http://hdl.handle.net/10596/24167>).