PRUEBA DE HABILIDADES PRÁCTICAS CCNA – DIPLOMADO DE PROFUDIZACIÓN CISCO CCNA

AUTOR
HOOVER ARLEY SERNA VÉLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRONICA
MEDELLÍN
2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA – DIPLOMADO DE PROFUDIZACIÓN CISCO CCNA

AUTOR
HOOVER ARLEY SERNA VÉLEZ

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO ELECTRÓNICO.

ASESOR: INGENIERO NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
MEDELLÍN - ANTIOQUIA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Medellín y 20 de Julio 2020

Dedico este trabajo a mi madre, familiares y amigos quienes me apoyaron en conseguir el objetivo de ser profesional.

AGRADECIMIENTOS

Dedico este trabajo a mi madre Elena, a mis familiares y a mis amigos que me apoyaron en la consecución de este objetivo.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El presente trabajo muestra el desarrollo de dos escenarios de red que solucionan requerimientos de conectividad. El primer escenario comprende la configuración de una red pequeña que admite conectividad IPv4 e IPv6, seguridad en switches, enrutamiento InterVLAN y el protocolo de enrutamiento dinámico RIPv2, además de implementar NAT, ACL's y DHCP.

El segundo escenario comprende la implementación de una red multi-área en dos ciudades diferentes conectadas mediante un servicio de enlace dedicado provisto por un ISP, dicha red IPv4 e implementa el protocolo de Routing OSPFv2, así como NAT, interno y externo, servidor DHCP, listas de acceso entre otros.

ABSTRACT

This document covers the CCNA Practical skills test through the development of two scenarios of implementation of routing protocols, and network topologies. This include also the use of NAT, functionality on routers CISCO, DHCP services, access list and other topics.

Keywords.

RIPv2, Routing Protocols, Network configurations, IPv4, IPv6, Network topologies, NAT, OSPFv2, Access list implementations.

GLOSARIO

ACL: Lista que define el control de accesos a determinadas direcciones IP o redes permitiendo o denegando su acceso a ciertos hosts depende de cómo sea configurada.

DHCP: Protocolo de configuración dinámica de host. Permite asignar direcciones IP de forma dinámica a los diferentes Hosts.

DCHPv6: Protocolo DHCP para IPv6.

IPv4: Protocolo de internet versión 4.

IPv6: Protocolo de internet versión 6

NAT: Método de traducción de direcciones de red, por enmascaramiento de direcciones IP.

OSPFv2: Protocolo de enrutamiento dinámico tipo estado de enlace que permite mantener rutas.

RIPv2: Protocolo de enrutamiento tipo vector distancia usado para enrutar paquetes IPv4

INTRODUCCIÓN

El presente trabajo tiene como objetivo principal, demostrar las habilidades adquiridas en el diplomado de profundización CISCO CCNA. En este trabajo, se desarrollan dos escenarios propuestos para la implementación de una solución de red CISCO.

OBJETIVOS

OBJETIVO GENERAL

Demostrar las habilidades adquiridas a través del diplomado de profundización CISCO CCNA, por medio del desarrollo de una solución de red en dos escenarios diferentes propuestos.

OBJETIVOS ESPECÍFICOS

Implementar los escenarios de red asignados mediante los conocimientos adquiridos a lo largo del diplomado. Tales como protocolos de enrutamiento dinámico, direccionamiento IPv4 e IPv6, configuración de VLAN's, actividades de diagnóstico y solución de problemas de red entre otros.

Poner en práctica las habilidades adquiridas en la configuración de los distintos equipos que forman parte de cualquier infraestructura de red CISCO, en los escenarios a los cuales aplica para este trabajo.

DESARROLLO DEL PROYECTO

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

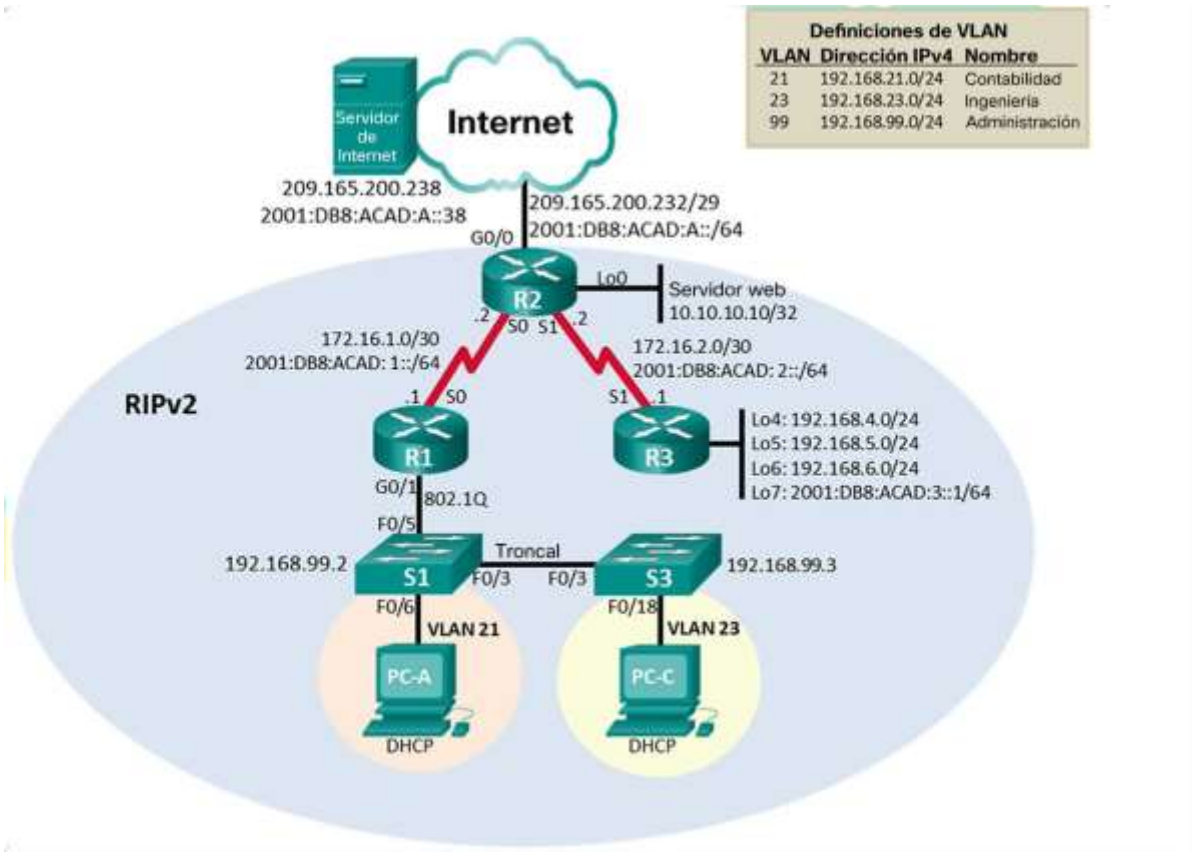


Figura 1

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	Enable Erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Enable Erase startup-config Delete vlan.dat
Volver a cargar ambos switches	Reload

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Enable
	Show flash
	`Switch#show flash`
	`Directory of flash:/`
	`1 -rw- 4414921 <no date> c2960-lanbase-mz.122-2`
	`64016384 bytes total (59601463 bytes free)`
	`Switch#`

Parte 2

Configurar los parámetros básicos de los dispositivos

Paso 2: 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	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Enable Configure terminal No ip domain-lookup
Nombre del router	hostname R1
Contraseña de exec privilegiado cifrada	Enable Configure terminal Enable secret class end
Contraseña de acceso a la consola	Configure terminal Line console 0 Password cisco Login end
Contraseña de acceso Telnet	Configure terminal Line vty 0 15 Password cisco login
Cifrar las contraseñas de texto no cifrado	Service password encryption
Mensaje MOTD	Configure terminal Banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/0	Configure terminal Interface serial 0/0/0 Description Conexion con R2 Ip address 172.16.1.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:A::38/64 Clock rate 128000 No shutdowndown Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 ip route 0.0.0.0 0.0.0.0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Configure terminal No ip domain-lookup
Nombre del router	Hostname R2
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password cisco Login Exit
Contraseña de acceso Telnet	Configure terminal Line vty 0 15 Password cisco login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Habilitar el servidor HTTP	Ip http server (NO disponible en Packet Tracert)
Mensaje MOTD	Banner motd % Se prohíbe el acceso no autorizado. %

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz Interface serial 0/0/0 Description conexion con R1 Ip address 172.16.1.2 255.255.255.252 Ipv6 address 2001:DB8:ACAD:1::2/64 No shutdowndown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz Interface serial 0/0/1 Description conexion con R3 Ip address 172.16.2.2 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::2/64 Clock rate 128000 No shutdowndown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz Interface g0/0 Description Conexion a internet ip address 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64 no shutdowndown

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. Interface loopback 0 Ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. ip route 0.0.0.0 0.0.0.0 g0/0 ipv6 route ::/0 g0/0

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Configure terminal No ip domain-lookup
Nombre del router	Configure terminal Hostname R3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Configure terminal Line console 0 Passwod cisco login
Contraseña de acceso Telnet	Configure terminal Line vty 0 15 Passwod cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz Interface serial 0/0/1 Description Conexion con R2 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::1/64
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 4 Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 5 Ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback 6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	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	ip route 0.0.0.0 0.0.0.0 serial 0/0/1 ipv6 route ::/0 serial 0/0/1

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Configure terminal No ip domain-lookup
Nombre del switch	hostname
Contraseña de exec privilegiado cifrada	Enable secret class

Contraseña de acceso a la consola	Configure terminal Line console 0 Password cisco Login exit
Contraseña de acceso Telnet	Configure terminal Line vty 0 15 Password cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Configure terminal No ip domain-lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Configure terminal Line console 0 Password cisco Login exit
Contraseña de acceso Telnet	Configure terminal Line vty 0 15 Password cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Paso 8: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeou !!!!! Success rate is 100 percent (5/5), round-trip min/av
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeou !!!!! Success rate is 100 percent (5/5), round-trip min/av
PC de Internet	Gateway predeter minado	209.165.200.233	C:\>ipconfig FastEthernet0 Connection:(default port) Link-local IPv6 Address.....: FE80::2D0:58FF:FED9:8EDD IP Address.....: 209.165.200.238 Subnet Mask.....: 255.255.255.240 Default Gateway.....: 209.165.200.233 C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

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

Parte 2: 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 Configure terminal Vlan 21 Name Accounting Vlan 23 Name Engineering Vlan 99 Name Management

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 Configure terminal Interface vlan 99 Ip addres 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ip default –gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Interface f0/3 Switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa Interface f0/5 Switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/1-2, f0/4, f0/6-24, g0/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	Interface f0/6 Switchport Access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4, f0/7-24, g0/1-2 shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. Configure terminal Vlan 21 Name Accounting Vlan 23 Name Engineering Vlan 99 Name Management
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología Interface vlan 99 ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. Ip default –gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Interface f0/3 Switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/1-2, f0/4-24, g0/1-2 switchport mode access
Asignar F0/18 a la VLAN 23	Interface f0/18 Switchport access vlan 23
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz Configure terminal Interface g0/1.21 Description VLAN 21 Encapsulation dot1q 21 ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz Configure terminal Interface g0/1.23 Description VLAN 23 Encapsulation dot1q 23 ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz Configure terminal Interface g0/1.99 Description VLAN 99 Encapsulation dot1q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	Configure terminal Interface g0/1 No shutdowndown

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 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
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 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
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 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
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 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =

Parte 3: 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	Configure terminal Router rip Version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. Network 172.16.1.0 Network 192.168.21.0 Network 192.168.23.0 Network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	passive-interface gigabitEthernet 0/1.21 passive-interface gigabitEthernet 0/1.23 passive-interface gigabitEthernet 0/1.99
Desactive la sumarización automática	No auto-summary

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	Configure terminal Router rip Version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. network 10.10.10.10 network 172.16.1.0 network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	No auto-summary

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Configure terminal Router rip Version 2
Anunciar redes IPv4 conectadas directamente	Network 172.16.2.0 Network 192.168.4.0 Network 192.168.5.0 Network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6
Desactive la sumarización automática.	No auto-summary

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 rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show run | section router rip

Parte 4: 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	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	ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10 domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 domain-name ccna-sa.com

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

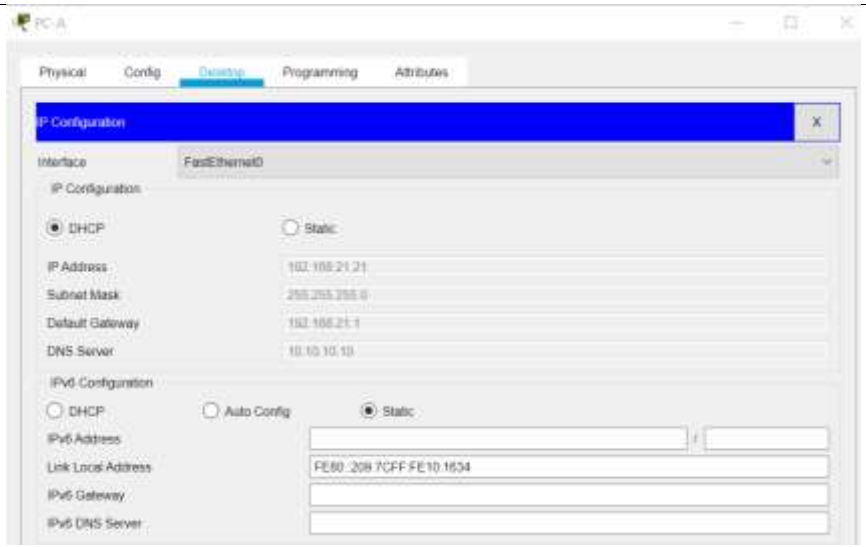
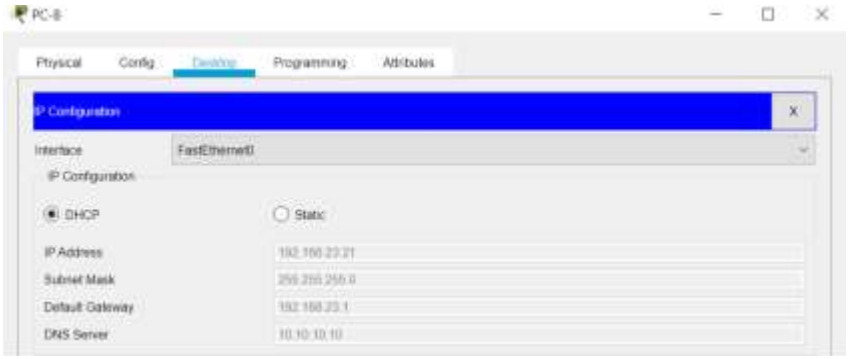
La configuración del R2 incluye las siguientes tareas:

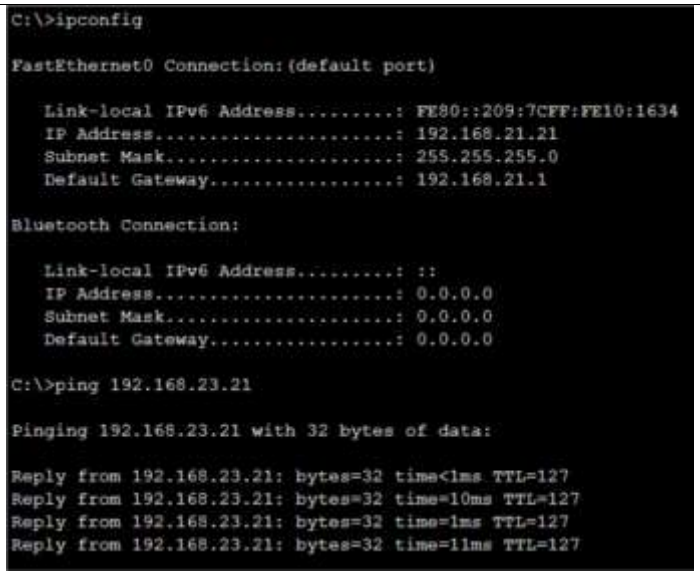
Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** **Configure terminal** username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** Configure terminal ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	Interface g0/0 Ip nat outside Interface serial0/0/0 Ip nat inside Interface serial0/0/1 Ip nat inside
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 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

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

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

Parte 5: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** clock set 18:15:00 15 may 2020
Configure R2 como un maestro NTP.	Nivel de estrato: **5** Configigure terminal Ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** Configure terminal Ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Ntp update calendar
Verifique la configuración de NTP en R1.	Show NTP associations

Parte 5: 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** **Configure terminal** Ip access-list standard ADMIN-MGT Permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	Configure terminal Line vty 0 15 Access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Transport input telnet

Verificar que la ACL funcione como se espera	telnet 172.16.1.2
	`R1#telnet 172.16.1.2`
	`Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado`
	
	`User Access Verification`
	
	`Password:`
	`R2>enable`

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	Show Access-list R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) Show ip Access-list R2#show ip access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es))
Restablecer los contadores de una lista de acceso	Clear ip Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface g0/0

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. Show ip nat translations R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1027209.165.200.2 tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1028209.165.200.2
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation *

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

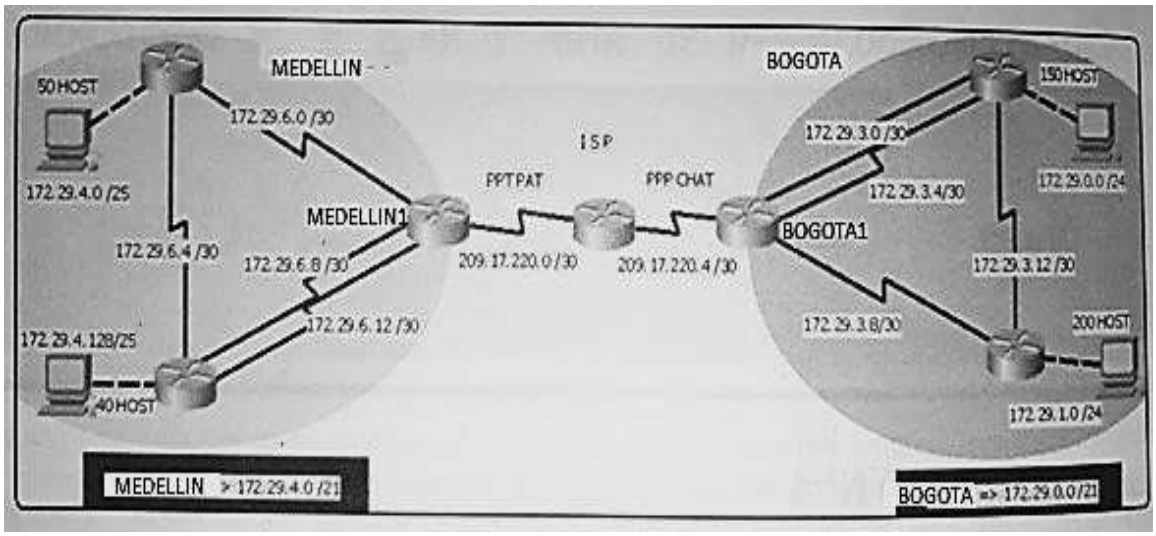


Figura 2

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

Los routers R6 y R3 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).

Configuraciones generales

ISP

```
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#LINE VTY 0 15 10
ISP(config-line)#password cisco
ISP(config-line)#login
```

MED1

```
Router>enable
Router#Configure terminal
Router(config)#hostname MED1
MED1(config)#no ip domain-lookup
MED1(config)#service password-encryption
MED1(config)#enable secret class
MED1(config)#line console 0
MED1(config-line)#password cisco
MED1(config-line)#login
MED1(config-line)#LINE VTY 0 15
MED1(config-line)#password cisco
```

BOG

```
Router>enable
Router#configure terminal
Router(config)#hostname BOG
BOG(config)#no ip domain-lookup
BOG(config)#service password-encryption
```

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

R3

Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#service password-encryption
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#LINE VTY 0 15
R3(config-line)#password cisco
R3(config-line)#login

R4

Router(config)#hostname R4
R4(config)#no ip domain-lookup R4(config)#service password-encryption
R4(config)#enable secret class
R4(config)#line console 0
R4(config-line)#password cisco
R4(config-line)#login
R4(config-line)#LINE VTY 0 15
R4(config-line)#password cisco
R4(config-line)#login

R6

Router>enable
Router#configure terminal
Router(config)#hostname R6
R6(config)#no ip domain-lookup
R6(config)#service password-encryption
R6(config)#enable secret class
R6(config)#line console 0
R6(config-line)#password cisco 11

R6(config-line)#login
R6(config-line)#LINE VTY 0 15
R6(config-line)#password cisco
R6(config-line)#login

R5

Router>enable
Router#configure terminal
Router(config)#hostname R5
R5(config)#no ip domain-lookup
R5(config)#service password-encryption
R5(config)#enable secret class
R5(config)#line console 0
R5(config-line)#password cisco
R5(config-line)#login
R5(config-line)#LINE VTY 0 15
R5(config-line)#password cisco
R5(config-line)#login

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

  Topología de la red.

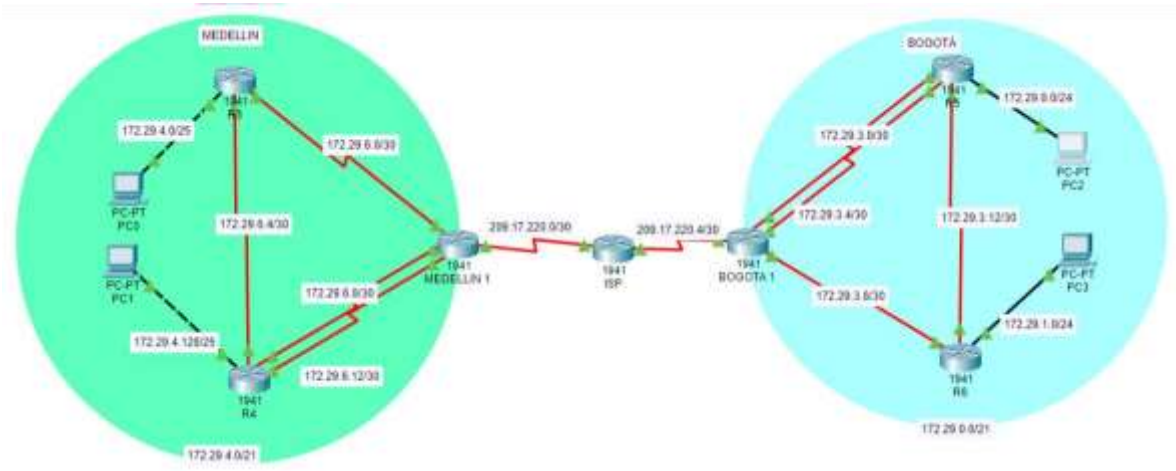


Figura 3

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

Tabla de Direccionamiento:

ISP			MED			R3			R4		
Se0/0/0	Subnet	209.17.220.0/30	**Se0/0/0**	Subnet	209.17.220.0/30	**S0/0/0**	Subnet	172.29.6.0/30	**Se0/0/0**	Subnet	172.29.6.8/30
	IP	209.17.220.1		IP	209.17.220.2		IP	172.17.6.2		IP	172.29.6.10
	WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	0.0.0.3
Se0/0/1	Subnet	209.17.220.4/30	**Se0/0/1**	Subnet	172.29.6.0/30	**Se0/0/1**	Subnet	172.29.6.4/30	**Se0/0/1**	Subnet	172.29.6.4/30
	IP	209.17.220.5		IP	172.29.6.1		IP	172.29.6.5		IP	172.29.6.6
	WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	0.0.0.3
			Se0/1/0	Subnet	172.29.6.8/30	**NA**	Subnet			Subnet	
				IP	172.29.6.9		IP			IP	
				WildCard	0.0.0.3		WildCard			WildCard	
			Se0/1/1	Subnet	172.29.6.12/30		Subnet		**Se0/1/1**	Subnet	172.29.6.12/30
				IP	172.29.6.13		IP			IP	172.29.6.14
				WildCard	0.0.0.3		WildCard			WildCard	0.0.0.3
			BOG			**R5**			**R6**		
			Se0/0/0	Subnet	209.17.220.4/30	**Se0/0/0**	Subnet	172.29.3.0/30	**Se0/0/0**	Subnet	172.29.3.8/30
				IP	209.17.220.6		IP	172.29.3.2		IP	172.29.3.10
				WildCard	0.0.03		WildCard	0.0.0.3		WildCard	0.0.0.3
			Se0/0/1	Subnet	172.29.3.0/30	**Se0/0/1**	Subnet	172.29.3.12/30	**Se0/0/1**	Subnet	172.29.3.12/30
				IP	172.29.3.1		IP	172.29.3.13		IP	172.29.3.14
				WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	0.0.0.3
			Se0/1/0	Subnet	172.29.3.4/30	**Se0/1/0**	Subnet	172.29.3.4/30		Subnet	
				IP	172.29.3.5		IP	172.29.3.6		IP	
				WildCard	0.0.0.3		WildCard	0.0.0.3		WildCard	
			Se0/1/1	Subnet	172.29.3.8/30		Subnet			Subnet	
				IP	172.29.3.9		IP			IP	
				WildCard	0.0.0.3		WildCard			WildCard	

Tabla 1

Nota: para este escenario los Routers R3 y R4 están localizados en Medellín, y R5 y R6 en Bogotá como se muestra en la topología

Configuración de las interfaces:

Router ISP

```
ISP>enable
ISP#configure terminal
ISP(config)#interface serial0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#interface serial0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
```

Router Medellín 1

```
MED1>ENABLE
MED1#Configure terminal
MED1(config-if)#ip address 209.17.220.2 255.255.255.252
MED1(config-if)#no shutdown
MED1(config-if)#interface serial0/0/1
MED1(config-if)#ip address 172.29.6.1 255.255.255.252
MED1(config-if)#clock rate 128000
MED1(config-if)#no shutdown
MED1(config-if)#interface serial0/1/0
MED1(config-if)#ip address 172.29.6.9 255.255.255.252
MED1(config-if)#clock rate 128000
MED1(config-if)#no shutdown
MED1(config-if)#interface serial0/1/1
MED1(config-if)#ip address 172.29.6.13 255.255.255.252
MED1(config-if)#clock rate 128000
MED1(config-if)#no shutdown
```

Router R3 / Medellín

```
R3>enable
R3#configure terminal
R3(config)#interface serial0/0/0
R3(config-if)#ip address 172.29.6.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#interface serial0/0/1
R3(config-if)#ip address 172.29.6.5 255.255.255.252
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
R3(config-if)#int g0/0
R3(config-if)#ip address 172.29.4.1 255.255.255.128
R3(config-if)#no shutdown
```

Router R4 / Medellín

```
R4>enable
R4#configure terminal
R4(config)#interface serial0/0/0
R4(config-if)#ip address 172.29.6.10 255.255.255.252
R4(config-if)#no shutdown
```

```
R4(config-if)#interface serial0/0/1
R4(config-if)#interface serial0/0/1
R4(config-if)#ip address 172.29.6.14 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#interface serial0/1/0
R4(config-if)#ip address 172.29.6.6 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#int g0/0
R4(config-if)#ip address 172.29.4.129 255.255.255.128
R4(config-if)#no shutdown 15
```

Router Bogotá

```
BOG>enable
BOG#configure terminal
BOG(config)#interface serial0/0/0
BOG(config-if)#ip address 209.17.220.6 255.255.255.252
BOG(config-if)#no shutdown
BOG(config-if)#interface serial0/0/1
BOG(config-if)#ip address 172.29.3.9 255.255.255.252
BOG(config-if)#clock rate 128000
BOG(config-if)#no shutdown
BOG(config-if)#interface serial0/1/0
BOG(config-if)#ip address 172.29.3.1 255.255.255.252
BOG(config-if)#clock rate 128000
BOG(config-if)#no shutdown
BOG(config-if)#interface serial0/1/1
BOG(config-if)#ip address 172.29.3.5 255.255.255.252
BOG(config-if)#clock rate 128000
BOG(config-if)#no shutdown
```

Router R6 / Bogotá

```
R6(config-if)#int g0/0
R6(config-if)#ip address 172.29.1.1 255.255.255.0
R6(config-if)#no shutdown
R6(config-if)#interface serial0/0/0
R6(config-if)#ip address 172.29.3.10 255.255.255.252
R6(config-if)#no shutdown
R6(config-if)#interface serial0/0/1
R6(config-if)#ip address 172.29.3.13 255.255.255.252
R6(config-if)#clock rate 128000
```

R6(config-if)#no shutdown

Router R5 / Bogotá

R5>enable
R5#configure terminal
R5(config)#interface serial0/0/0
R5(config-if)#ip address 172.29.3.2 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#interface serial0/0/1
R5(config-if)#ip address 172.29.3.6 255.255.255.252 R5(config-if)#no shutdown
R5(config-if)#int g0/0
R5(config-if)#ip address 172.29.3.6 255.255.255.252
R5(config-if)#int g0/0
R5(config-if)#ip address 172.29.0.1 255.255.255.0
R5(config-if)#no shutdown

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.

MED1(config)#router ospf 1
MED1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MED1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MED1(config-router)#network 172.29.6.12 0.0.0.3 area 0

R3(config)#router ospf 1
R3(config-router)#network 172.29.6.0 0.0.0.3 area 0
R3(config-router)#network 172.29.6.4 0.0.0.3 area 0
R3(config-router)#network 172.29.4.0 0.0.0.127 area 0

R4(config)#router ospf 1
R4(config-router)#network 172.29.6.8 0.0.0.3 area 0
R4(config-router)#network 172.29.6.4 0.0.0.3 area 0
R4(config-router)#network 172.29.6.12 0.0.0.3 area 0
R4(config-router)#network 172.29.4.128 0.0.0.127 area 0

BOG(config)#router ospf 1
BOG(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOG(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOG(config-router)#network 172.29.3.8 0.0.0.3 area 0

```
R5(config)#router ospf 1
R5(config-router)#network 172.29.3.0 0.0.0.3 area 0
R5(config-router)#network 172.29.3.12 0.0.0.3 area 0
R5(config-router)#network 172.29.3.4 0.0.0.3 area 0
R5(config-router)#network 172.29.0.0 0.0.0.255 area 0
```

```
R6(config)#router ospf 1
R6(config-router)#network 172.29.3.8 0.0.0.3 area 0
R6(config-router)#network 172.29.3.12 0.0.0.3 area 0
R6(config-router)#network 172.29.1.0 0.0.0.255 area 0
```

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

Router MED1

```
Router>enable
Router#configure terminal
MED1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MED1(config)#router ospf 1
MED1(config-router)#default-information originate
MED1(config-router)#
```

Router BOG

```
Router>enable
Router#configure terminal
BOG(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOG(config)#route ospf 1
BOG(config-router)#default-information originate
BOG(config-router)#
```

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

```
ISP>enable
ISP#configure terminal
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#
```

Parte 2: Tabla de Enrutamiento.

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

Comprobación tablas de enrutamiento

MED1

IOS Command Line Interface

```
MED1>
MED1>
MED1>show ip rou
MED1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/129] via 172.29.6.14, 01:10:37, Serial0/1/1
O       172.29.4.128/25 [110/65] via 172.29.6.14, 01:10:37, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/0/1
L       172.29.6.1/32 is directly connected, Serial0/0/1
O       172.29.6.4/30 [110/128] via 172.29.6.14, 01:10:37, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/1/0
L       172.29.6.9/32 is directly connected, Serial0/1/0
C       172.29.6.12/30 is directly connected, Serial0/1/1
L       172.29.6.13/32 is directly connected, Serial0/1/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
C       209.17.220.1/32 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.1

MED1>
```

R4

IOS Command Line Interface

```
R4>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 172.29.6.13 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.5, 01:12:05, Serial0/0/1
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.13, 01:12:05, Serial0/1/1
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.6/32 is directly connected, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/1/1
L       172.29.6.14/32 is directly connected, Serial0/1/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 01:12:05, Serial0/1/1

R4>
R4>
R4>
R4>
```

R3

IOS Command Line Interface

```
R3>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 172.29.6.6 to network 0.0.0.0

     172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.17.6.0/30 is directly connected, Serial0/0/0
L       172.17.6.2/32 is directly connected, Serial0/0/0
     172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 01:12:33, Serial0/0/1
O       172.29.6.0/30 [110/192] via 172.29.6.6, 01:12:33, Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.5/32 is directly connected, Serial0/0/1
O       172.29.6.8/30 [110/128] via 172.29.6.6, 01:12:33, Serial0/0/1
O       172.29.6.12/30 [110/128] via 172.29.6.6, 01:12:33, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.6, 01:12:33, Serial0/0/1
```

ISP

IOS Command Line Interface

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

Gateway of last resort is not set

     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
     209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.1/32 is directly connected, Serial0/0/0
C       209.17.220.2/32 is directly connected, Serial0/0/0
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
C       209.17.220.6/32 is directly connected, Serial0/0/1
```

BOG

IOS Command Line Interface

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

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.2, 01:13:49, Serial0/0/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 01:13:49, Serial0/1/1
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.1/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.5/32 is directly connected, Serial0/1/0
C       172.29.3.8/30 is directly connected, Serial0/1/1
L       172.29.3.9/32 is directly connected, Serial0/1/1
O       172.29.3.12/30 [110/128] via 172.29.3.10, 01:13:49, Serial0/1/1
                       [110/128] via 172.29.3.2, 01:13:49, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
 --More-- |
```

R5

IOS Command Line Interface

```
R5>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 172.29.3.5 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
O       172.29.1.0/24 [110/65] via 172.29.3.14, 01:14:30, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.2/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.6/32 is directly connected, Serial0/1/0
O       172.29.3.8/30 [110/128] via 172.29.3.5, 01:14:30, Serial0/1/0
                      [110/128] via 172.29.3.14, 01:14:30, Serial0/0/1
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.5, 01:14:30, Serial0/1/0
```

R6

IOS Command Line Interface

```
R6>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 172.29.3.9 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.13, 01:15:08, Serial0/0/1
C       172.29.1.0/24 is directly connected, GigabitEthernet0/0
L       172.29.1.1/32 is directly connected, GigabitEthernet0/0
O       172.29.3.0/30 [110/128] via 172.29.3.9, 01:15:08, Serial0/0/0
                      [110/128] via 172.29.3.13, 01:15:08, Serial0/0/1
O       172.29.3.4/30 [110/128] via 172.29.3.9, 01:15:08, Serial0/0/0
                      [110/128] via 172.29.3.13, 01:15:08, Serial0/0/1
C       172.29.3.8/30 is directly connected, Serial0/0/0
L       172.29.3.10/32 is directly connected, Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.14/32 is directly connected, Serial0/0/1
```

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
R6	SERIAL0/0/0; SERIAL0/0/1
R5	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 2

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.

Para deshabilitar la propagación de paquetes Hello o tráfico ospf en las interfaces que no lo necesitan se debe ejecutar el siguiente comando en cada una de las interfaces:

Router#Configure terminal
Router(config)router ospf 1
Router(config-router)#passive-interface g0/0

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.

Resultado mostrado en la parte 2, apartado “Comprobación de tablas de enrutamiento”

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

ISP Router>enable
ISP#configure terminal

```
ISP(config)#username MED1 password cisco
ISP(config)#interface serial0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username BOG password cisco
ISP(config)#interface serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap cisco

MED1#configure terminal
MED1(config)#username ISP password cisco
MED1(config)#interface serial0/0/0
MED1(config-if)#encapsulation ppp
MED1(config-if)#ppp authentication pap
MED1(config-if)#ppp pap sent-username MED1 password cisco

BOG>enable
BOG#Configure terminal
BOG (config)#username ISP password cisco
BOG(config)#int serial0/0/0
BOG(config-if)#encapsulation ppp
BOG(config-if)#ppp authentication chap
```

Parte 6: Configuración de PAT.

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

MED1

```
MED1>enable
MED1#configure terminal
MED1(config)#ip nat inside source list 1 interface s0/0/0 overload
MED1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MED1(config)#interface serial0/0/0
MED1(config-if)#ip nat outside
MED1(config-if)#ip nat inside
MED1(config-if)# Interface serial0/0/1
MED1(config-if)#ip nat intside
MED1(config-if)#ip nat inside
MED1(config-if)# interface serial0/1/1
MED1(config-if)#ip nat inside
MED1(config-if)#interface serial0/1/0
MED1(config-if)#ip nat inside
MED1(config-if)#
```

BOG

```
BOG>ENABLE
BOG#configure terminal
BOG(config)#ip nat inside source list 1 interface s0/0/0 overload
BOG(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOG(config)#interface serial0/0/0
BOG(config-if)#ip nat outside
BOG(config-if)#ip nat inside
BOG(config-if)#interface serial0/1/0
BOG(config-if)#ip nat inside
BOG(config-if)#interface serial0/1/1
BOG(config-if)#ip nat inside
BOG(config-if)#
```

Parte 7: Configuración del servicio DHCP.

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

Configuración DHCP

Configuramos R3 para que sea el DHCP para las LAN de Medellín

```
R3
R3>enable
R3#configure terminal
R3(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
R3(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
R3(config)#ip dhcp pool MEDELLIN2
R3(dhcp-config)#network 172.29.4.0 255.255.255.128
R3(dhcp-config)#default-router 172.29.4.1
R3(dhcp-config)#dns-server 8.8.8.8
R3(dhcp-config)#exit
R3(config)#ip dhcp pool MEDELLIN3
R3(dhcp-config)#network 172.29.4.128 255.255.255.128
R3(dhcp-config)#default-router 172.29.4.129
R3(dhcp-config)#dns-server 8.8.8.8
R3(dhcp-config)#exit
```

Configuración en R4 como bypass para DHCP de R3 [Permite el tráfico broadcast hacia R3]

```
Router>enable
Router#configure terminal
R3(config)#int g0/0
R3(config-if)#ip helper-address 172.29.6.5
```

Configuramos R6 para que sea el DHCP para las LAN de Bogotá

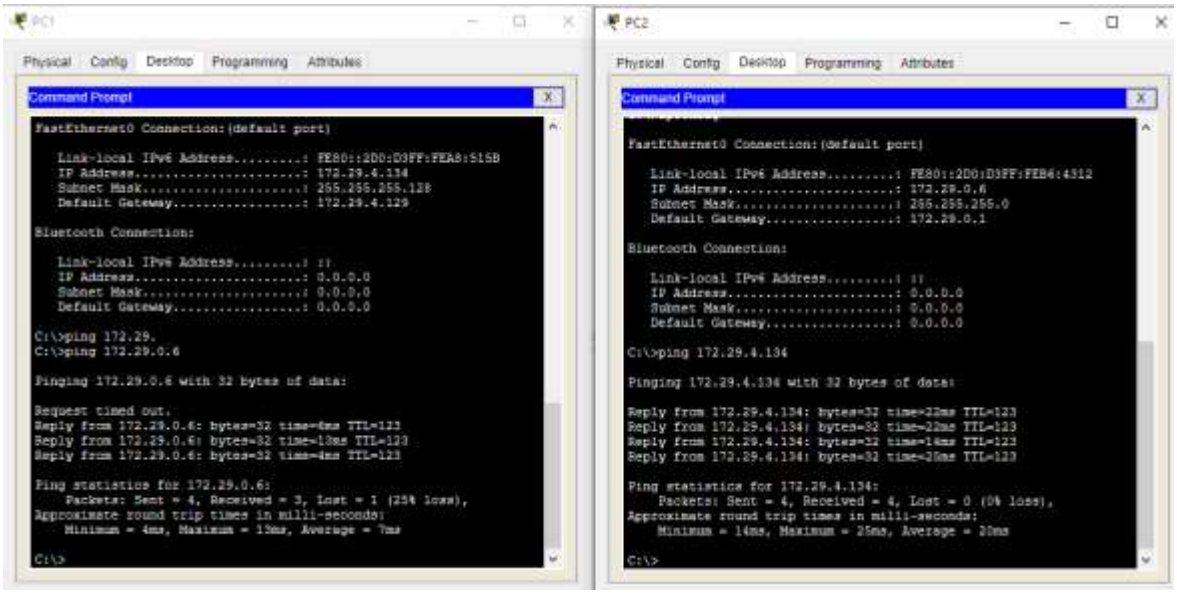
```
R6>enable
R6#configure terminal
R6(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
R6(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
R6(config)#ip dhcp pool BOGOTA2
```

R6(dhcp-config)#network 172.29.1.0 255.255.255.0
R6(dhcp-config)#default-router 172.29.1.1
R6(dhcp-config)# default-router 172.29.1.1
R6(dhcp-config)#dns-server 8.8.8.8
R6(dhcp-config)#ip dhcp pool BOGOTA3
R6(dhcp-config)#network 172.29.0.0 255.255.255.0
R6(dhcp-config)# default-router 172.29.0.1
R6(dhcp-config)#dns-server 8.8.8.8

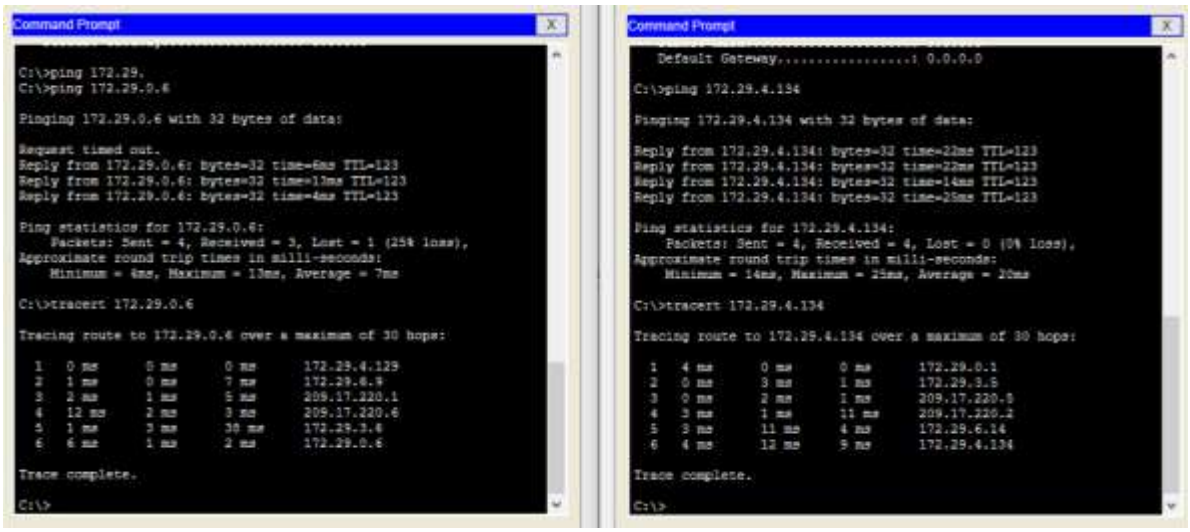
Configuración en R5 como bypass para DHCP de R3 [Permite el tráfico broadcast hacia R6]

R5>ENABLE
R5#configure terminal
R5(config)#int g0/0
R5(config-if)#ip helper-address 172.29.3.13

Resultados y pruebas de conectividad entre una PC de Medellín y una de Bogotá mediante ping.



Ping de PC1 en Medellín a PC2 en Bogotá y vice versa



Tracert entre los computadores anteriores.

En el ejercicio anterior, se pueden ver los routers por los que pasan los paquetes para llegar a cada uno de los destinos.

CONCLUSIONES

El desarrollo de los escenarios anteriores permitió poner en práctica los contenidos aprendidos durante el curso, con especial énfasis en los protocolos de enrutamiento dinámico, particularmente OSPFv2. También aplicar los conceptos aprendidos de las diferentes capas del modelo OSI como encapsulamiento en capada 2 entre otros.

Los escenarios planteados permitieron el fortalecimiento de habilidades al trabajar con los dos tipos de direccionamiento existente hoy en día IPv6 y IPv4.

Cisco al igual que otros fabricantes permiten diseñar e implementar soluciones de conectividad en la WAN para conectar sucursales y proveer servicios a través de estas. Es importante tener todas las consideraciones de seguridad correspondientes, así como los objetivos, para implementar una arquitectura de red adecuada.

BIBLIOGRAFÍA

Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. Recuperado 5 junio, 2019, de https://byspel.com/configurar-servidor-dhcpen-cisco-packet-tracer

DHCP CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Enrutamiento Dinámico CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado 5 junio, 2019, de http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurardhcp-en-cisco-router/

OSPF de una sola área: CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Rosbarbosa, R. B. (2017, 25 septiembre). IP Helper y Relay Agent – Manteniendo un servidor DHCP en otra red. Recuperado 5 junio, 2019, de https://www.seaccna.com/ip-helper-relay-agent/

Traducción de direcciones IP para IPv4 CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1