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

LINA MARIA CRUZ BARRAGÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI
INGENIERIA DE SISTEMAS
BOGOTÁ
2020

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

LINA MARIA CRUZ BARRAGÁN

PRUEBA DE HABILIDADES

JOSE IGNACIO CARDONA
TUTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI
INGENIERIA DE SISTEMAS
BOGOTÁ
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

BOGOTA (03/05/2020) (14/05/2020)

CONTENIDO

1. INTRODUCCIÓN 5

2. DECRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES 6

ESCENARIO 1 6

PARTE 1: INICIALIZAR DISPOSITIVOS 7

PARTE 2:CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS 8

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN 17

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2 21

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4 24

PARTE 6: CONFIGURAR NTP 27

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL) 28

ESCENARIO 2: 31

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO 33

PARTE 2: TABLA DE ENRUTAMIENTO 38

PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF 43

PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF 45

PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP 49

PARTE 6: CONFIGURACIÓN DE PAT 50

PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP 53

CONCLUSIONES 56

BIBLIOGRAFÍA 57

RESUMEN

La práctica desarrollada en dos escenarios, a través de la configuración de una red pequeña aborda las temáticas de conectividad aplicando los protocolos de: Seguridad de switches, routing entre VLAN, dinámico RIPv2. Adquiriendo conocimientos amplios y generando la práctica de enrutamiento en la topología de redes asignadas y la configuración necesaria para aplicar en nuestra carrera a lo largo de los casos que se nos presenten.

1. INTRODUCCIÓN

En el presente trabajo se solucionarán dos escenarios de CCNA, los cuales tienen como fin poner a prueba las habilidades y conocimientos adquiridos en el diplomado de profundización.

El primer escenario se basa en configurar una red pequeña para que admita conectividad IPv4 e IPv6 y seguridad de switches routing entre VLAN, También nos enseña a utilizar el protocolo de routing dinámico RIPv2.

En este escenario se ponen a prueba conocimientos de enrutamiento y configuración de redes. Además, se evidenciará como implementar el DHCP y NAT para IPV4 con el fin de utilizar el espacio de redes privadas.

El segundo escenario se basa en configurar e interconectar entre si los dispositivos siguiendo los lineamientos de direccionamiento, protocolos y enrutamiento para la topología de red que fue asignada, en él también se debe aplicar la configuración del DHCP para asignar direcciones de manera automática.

También veremos cómo se realiza la configuración de PPP, a nivel de la capa de enlace de los escenarios, TCP/IP entre los equipos que conforman la red de los escenarios.

El segundo escenario nos permitirá aprender a desactivar el enrutamiento dinámico de OSPF el cual se utilizará en la configuración de los routers que componen la topología y como hacer la configuración de PAT para definir una lista de acceso e identificar una interfaz si es interna o externa.

2. DECRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

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

Topología

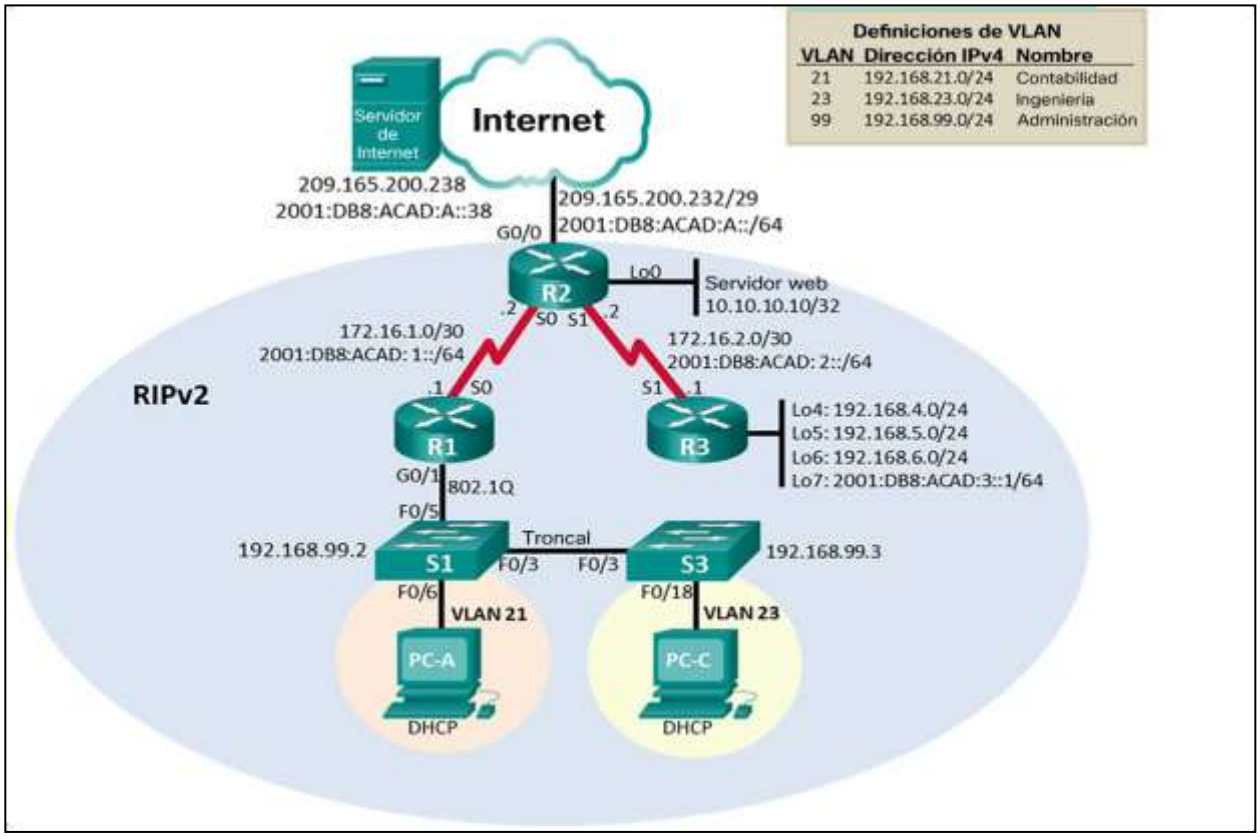


Fig. 1 Topología escenario 1 protocolo RIPv2

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.

Se da a conocer los comandos que se utilizan cuando es necesario cargar archivos de configuración sobre un router o switch ya sea por renovación tecnológica o falla del dispositivo, como eliminar configuraciones que se lleguen a corromper y se deban eliminar tanto en la configuración inicial como en la memoria flash y más que todo estos comandos son utilizados en procesos de cambio de tecnología y procesos de rollback.

Tarea	Comando de IOS

Eliminar el archivo startup-config de todos los routers	`Router#erase startup-config`
	`Erasing the nvram filesystem will remove all configuration files!`
	`Continue? [confirm]`
	`[OK]`
	`Erase of nvram: complete`

Volver a cargar todos los routers	`Router#reload`
	`Proceed with reload? [confirm]`
	`System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)`
	`Technical Support: http://www.cisco.com/techsupport`
	`Copyright (c) 2010 by cisco Systems, Inc.`
	`Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB`
	`CISCO1941/K9 platform with 524288 Kbytes of main memory`
	`Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled`

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	`Switch>en`
	`Switch# erase startup-config`
	`Erasing the nvram filesystem will remove all configuration files!`
	`Continue? [confirm]`
	`[OK]`
	`Erase of nvram: complete`

Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960-24TT starting... Base ethernet MAC Address: 0001.6491.B96E Xmodem file system is available. Initializing Flash... flashfs[0]: 1 files, 0 directories flashfs[0]: 0 orphaned files, 0 orphaned directories flashfs[0]: Total bytes: 64016384 flashfs[0]: Bytes used: 4414921 flashfs[0]: Bytes available: 59601463 flashfs[0]: flashfs fsck took 1 seconds. ...done Initializing Flash.
Verificar que Volver a cargar todos los routers la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]

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):

Se observa que las configuraciones básicas son necesarias para tener una mejor administración en los dispositivos de red (router o switch), donde se puede permitir y restringir el acceso, además se puede identificar que usuarios intentan acceder a los equipos y en los dispositivos finales como pc y servidores se configuran para que puedan ser parte de la red en general.

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:A::1

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se procede a configurar los parámetros solicitados en la tabla donde indicara que clase de comandos utilice para llevar a cabo los pasos solicitados en el paso 2:

- ✓ Se des activa la búsqueda de DNS con el comando no ip domain-lookup:
- ✓ Nombre del swith utilizando el comando hostname R1
- ✓ Asignación de contraseña con el comando line console 0
- ✓ Contraseña de acceso Telnet con el comando line vty 0 15
- ✓ Asignación de contraseña Cifrada con el comando password encryption
- ✓ Se configura mensaje MOD con el comando banner motd “Acceso no autorizado”
- ✓ Se configura la interfaz S0/0/0
- ✓ Con ayuda del comando ip route se configuran las rutas predeterminadas

Cada configuración se ve reflejada con su respectivo comando e imagen a continuación:

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#no ip domain-lookup`

Nombre del router	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#hostname R1`
	`R1(config)#`

Contraseña de exec privilegiado cifrada	`R1#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#enable secret class`
	`R1(config)#exit`

Contraseña de acceso a la consola	`R1#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#line console 0`
	`R1(config-line)#password cisco`
	`R1(config-line)#login`

Contraseña de acceso Telnet	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#line vty 0 15`
	`R1(config-line)#password cisco`

Cifrar las contraseñas de texto no cifrado	`R1#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#service password-encryption`
	`R1(config)#exit`

Mensaje MOTD	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#banner motd 'Acceso no autorizado'`

Interfaz S0/0/0	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#int s0/0/0`
	`R1(config-if)#description Red 172.16.1.0/30`
	`R1(config-if)#ip address 172.16.1.1 255.255.255.252`
	`R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64`
	`R1(config-if)#clock rate 128000`
	`R1(config-if)#no shutdown`

Rutas predeterminadas	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0`
	`R1(config)#ipv6 route ::/0 s0/0/0`

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

- ✓ Se des activa la búsqueda de DNS con el comando no ip domain-lookup:
- ✓ Nombre del swith utilizando el comando hostname R2
- ✓ Asignación de contraseña con el comando line console 0

- ✓ Se configura la interfaz S0/0/0
- ✓ Se configura la interfaz G0/0
- ✓ Se configura la interfaz loopback con el comando Lo00
- ✓ Con ayuda del comando ip route se configuran las rutas predeterminadas
- ✓ Contraseña de acceso Telnet con el comando line vty 0 15
- ✓ Asignación de contraseña Cifrada con el comando password encryption
- ✓ Se habilita el servidor Habilitar el servidor HTTP
- ✓ Se configura mensaje MOD con el comando banner motd “Acceso no autorizado”

Cada configuración se ve reflejada con su respectivo comando e imagen a continuación:

Elemento o tarea de configuración	**Especificación**

Desactivar la búsqueda DNS	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#no ip domain-lookup`

Nombre del router	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#hostname R2`
	`R2(config)#`

Contraseña de exec privilegiado cifrada	`R2>en`
	`R2#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#enable secret class`
	`R2(config)#exit`

Contraseña de acceso a la consola	`R2#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#line console 0`
	`R2(config-line)#password cisco`
	`R2(config-line)#login`

Contraseña de acceso Telnet	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#line vty 0 15`
	`R2(config-line)#password cisco`

Cifrar las contraseñas de texto no cifrado	`R2#config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#service password-encryption`
	`R2(config)#exit`

Habilitar el servidor HTTP	`R2(config)#ip http server`
	`                ^`
	`% Invalid input detected at '^' marker.`
	Como se observa en la imagen este comando no es soportado por el simulador packet tracert.

Mensaje MOTD	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#banner motd 'Acceso no autorizado'`

Interfaz S0/0/0	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#int s0/0/0`
	`R2(config-if)#description Red 172.16.1.0/30`
	`R2(config-if)#ip address 172.16.1.2 255.255.255.252`
	`R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64`
	`R2(config-if)#no shutdown`

Interfaz S0/0/1	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#int s0/0/1`
	`R2(config-if)#description Red 172.16.2.0/30`
	`R2(config-if)#ip address 172.16.2.2 255.255.255.252`
	`R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64`
	`R2(config-if)#clock rate 128000`
	`R2(config-if)#no shutdown`

Interfaz G0/0 (simulación de Internet)	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#int g0/0`
	`R2(config-if)#description Simulacion de Internet`
	`R2(config-if)#ip address 209.165.200.233 255.255.255.248`
	`R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64`
	`R2(config-if)#no shutdown`

Interfaz loopback 0 (servidor web simulado)	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#int lo0`
	`R2(config-if)#description Servidor Web Simulado`
	`R2(config-if)#ip address 10.10.10.10 255.255.255.255`
	`R2(config-if)#no shutdown`

Ruta predeterminada	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0`
	`R2(config)#ipv6 route ::/0 g0/0`

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

- ✓ Se des activa la búsqueda de DNS con el comando no ip domain-lookup:
- ✓ Nombre del swith utilizando el comando hostname R3
- ✓ Asignación de contraseña con el comando line console 0
- ✓ Contraseña de acceso Telnet con el comando line vty 0 15
- ✓ Asignación de contraseña Cifrada con el comando password encryption
- ✓ Se habilita el servidor Habilitar el servidor HTTP
- ✓ Se configura mensaje MOD con el comando banner motd “Acceso no autorizado”
- ✓ Se configura la interfaz S0/0/1
- ✓ Se configura la interfaz Interfaz loopback 4
- ✓ Se configura la interfaz Interfaz loopback 5
- ✓ Se configura la interfaz Interfaz loopback 6
- ✓ Se configura la interfaz Interfaz loopback 7
- ✓ Se configura la interfaz G0/0
- ✓ Se configura la interfaz loopback con el comando Lo0
- ✓ Con ayuda del comando ip route se configuran las rutas predeterminadas

Cada configuración se ve reflejada con su respectivo comando e imagen a continuación:

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#no ip domain-lookup`

Nombre del router	`Router#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Router(config)#hostname R3`
	`R3(config)#`

Contraseña de exec privilegiado cifrada	`R3>en`
	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#enable secret class`
	`R3(config)#exit`

Contraseña de acceso a la consola	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#line console 0`
	`R3(config-line)#password cisco`
	`R3(config-line)#login`

Contraseña de acceso Telnet	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#line vty 0 15`
	`R3(config-line)#password cisco`

Cifrar las contraseñas de texto no cifrado	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#service password-encryption`
	`R3(config)#exit`

Mensaje MOTD	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#banner motd 'Acceso no autorizado'`

Interfaz S0/0/1	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#int s0/0/1`
	`R3(config-if)#description Red 172.16.2.0/30`
	`R3(config-if)#ip address 172.16.2.1 255.255.255.252`
	`R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64`
	`R3(config-if)#no shutdown`

Interfaz loopback 4	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#int lo4`
	`R3(config-if)#ip address 192.168.4.1 255.255.255.0`

Interfaz loopback 5	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#int lo5`
	`R3(config-if)#ip address 192.168.5.1 255.255.255.0`

Interfaz loopback 6	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#int lo6`
	`R3(config-if)#ip address 192.168.6.1 255.255.255.0`

Interfaz loopback 7	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#int lo7`
	`R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64`

Rutas predeterminadas	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1`
	`R3(config)#ipv6 route ::/0 s0/0/1`

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

- ✓ Se des activa la búsqueda de DNS con el comando no ip domain-lookup:
- ✓ Nombre del swith utilizando el comando hostname S1
- ✓ Asignación de contraseña con el comando line console 0
- ✓ Contraseña de acceso Telnet con el comando line vty 0 15
- ✓ Asignación de contraseña Cifrada con el comando password encryption
- ✓ Se configura mensaje MOD con el comando banner motd “Acceso no autorizado”

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	`Switch#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Switch(config)#no ip domain-lookup`

Nombre del switch	`Switch#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Switch(config)#hostname S1`
	`S1(config)#`

Contraseña de exec privilegiado cifrada	`S1>en`
	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#enable secret class`
	`S1(config)#exit`

Contraseña de acceso a la consola	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#line console 0`
	`S1(config-line)#password cisco`
	`S1(config-line)#login`

Contraseña de acceso Telnet	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#line vty 0 15`
	`S1(config-line)#password cisco`

Cifrar las contraseñas de texto no cifrado	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#service password-encryption`
	`S1(config)#exit`

Mensaje MOTD	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#banner motd 'Acceso no autorizado'`

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- ✓ Se des activa la búsqueda de DNS con el comando no ip domain-lookup:
- ✓ Nombre del swith utilizando el comando hostname S3
- ✓ Asignación de contraseña con el comando line console 0
- ✓ Contraseña de acceso Telnet con el comando line vty 0 15
- ✓ Asignación de contraseña Cifrada con el comando password encryption
- ✓ Se configura mensaje MOD con el comando banner motd “Acceso no autorizado”

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	`Switch#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Switch(config)#no ip domain-lookup`

Nombre del switch	`Switch#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Switch(config)#hostname S3`

Contraseña de exec privilegiado cifrada	`S3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S3(config)#enable secret class`
	`S3(config)#exit`

Contraseña de acceso a la consola	`S3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S3(config)#line console 0`
	`S3(config-line)#password cisco`
	`S3(config-line)#login`

Contraseña de acceso Telnet	`S3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S3(config)#line vty 0 15`
	`S3(config-line)#password cisco`

Cifrar las contraseñas de texto no cifrado	`S3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S3(config)#service password-encryption`
	`S3(config)#exit`

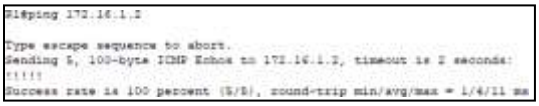
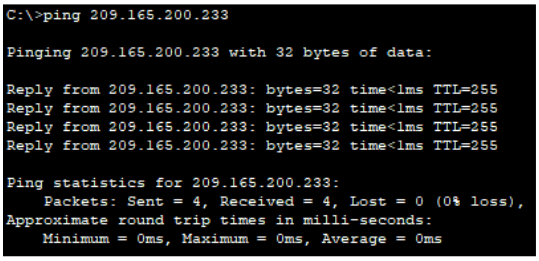
Mensaje MOTD	`S3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S3(config)#banner motd 'Acceso no autorizado'`

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:

Se realiza ping a las direcciones ip indicadas las cuales dan como resultado pruebas exitosas como se evidencia en las imágenes.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	
R2	R3, S0/0/1	172.16.2.1	
Servidor de Internet	Gateway predeterminado	209.165.200.233	

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

Se dan a conocer los parámetros que son necesarios configurar en un switch para tener un control en el acceso a los dispositivos, se realiza la configuración de las VLAN para hacer una segmentación en la red y poder identificar con mayor facilidad un problema, para que la administración sea más efectiva y se pueda controlar la comunicación entre una VLAN y otra.

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación

Crear la base de datos de VLAN	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#vlan 21`
	`S1(config-vlan)#Name Contabilidad`
	`S1(config-vlan)#exit`
	`S1(config)#vlan 23`
	`S1(config-vlan)#Name Ingenieria`
	`S1(config-vlan)#exit`
	`S1(config)#vlan 99`
	`S1(config-vlan)#Name Admin`
	`S1(config-vlan)#exit`

Asignar la dirección IP de administración.	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int vlan 99`
	`S1(config-if)#ip address 192.168.99.2 255.255.255.0`
	`S1(config-if)#no shutdown`

Asignar el Gateway predeterminado	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#ip default-gateway 192.168.99.1`

Forzar el enlace troncal en la interfaz F0/3	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int fa0/3`
	`S1(config-if)#switchport mode trunk`
	`S1(config-if)#switchport trunk native vlan 1`

Forzar el enlace troncal en la interfaz F0/5	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int fa0/5`
	`S1(config-if)#switchport mode trunk`
	`S1(config-if)#switchport trunk native vlan 1`

Configurar el resto de los puertos como puertos de acceso	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int range f0/1-2`
	`S1(config-if-range)#switchport mode access`
	
	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int range f0/6-24`
	`S1(config-if-range)#switchport mode access`

Asignar F0/6 a la VLAN 21	`S1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`S1(config)#int f0/6`
	`S1(config-if)#switchport access vlan 21`

Apagar todos los puertos sin usar	S1#conf t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int range f0/1-2 S1(config-if-range)#shutdown S1#conf t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int range f0/7-24 S1(config-if-range)#shutdown

Paso 10: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#vlan 21 S3(config-vlan)#Name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#Name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#Name Admin S3(config-vlan)#exit
Asignar la dirección IP de administración	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el Gateway predeterminado.	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int range fa0/1-2 S3(config-if-range)#switchport mode access S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int range fa0/4-24 S3(config-if-range)#switchport mode access

Asignar F0/18 a la VLAN 21	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int f0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int range fa0/1-2 S3(config-if-range)#shutdown S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int range fa0/4-17 S3(config-if-range)#shutdown S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#int range fa0/19-24 S3(config-if-range)#shutdown

Paso 11: 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	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1 R1(config-if)#no shutdown

Paso 12: 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 = 0/0/1 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 = 0/0/3 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 = 0/2/7 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 = 0/0/0 ms

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

Se realiza la configuración de un enrutamiento dinámico que para este escenario es el protocolo RIPv2, donde se configuran las redes que están directamente conectadas a cada uno de los router y así intercambiar información de enrutamiento con las otras redes que integran el escenario.

Paso 13: 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#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#route rip`
	`R1(config-router)#version 2`

Anunciar las redes conectadas directamente	`R1(config-router)#network 172.16.1.0`
	`R1(config-router)#network 192.168.21.0`
	`R1(config-router)#network 192.168.23.0`
	`R1(config-router)#network 192.168.99.0`

Establecer todas las interfaces LAN como pasivas	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#route rip`
	`R1(config-router)#version 2`
	`R1(config-router)#passive-interface g0/1`

Desactive la sumarización automática	`R1(config)#route rip`
	`R1(config-router)#version 2`
	`R1(config-router)#no auto-summary`

Paso 14: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación

Configurar RIP versión 2	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#route rip`
	`R2(config-router)#version 2`

Anunciar las redes conectadas directamente	`R2(config-router)#network 10.10.10.10`
	`R2(config-router)#network 172.16.1.0`
	`R2(config-router)#network 172.16.2.0`

Establecer la interfaz LAN (loopback) como pasiva	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#route rip`
	`R2(config-router)#version 2`
	`R2(config-router)#passive-interface g0/0`
	`R2(config-router)#passive-interface lo0`

Desactive la sumarización automática.	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#route rip`
	`R2(config-router)#version 2`
	`R2(config-router)#no auto-summary`

Paso 15: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación

Configurar RIP versión 2	`R3#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#route 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#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R3(config)#route rip`
	`R3(config-router)#version 2`
	`R3(config-router)#passive-interface lo4`
	`R3(config-router)#passive-interface lo5`
	`R3(config-router)#passive-interface lo6`

Desactive la sumarización automática.	`R3(config)#route rip`
	`R3(config-router)#version 2`
	`R3(config-router)#no auto-summary`

Paso 16: Verificar la información de RIP

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

Con el uso del comando show ip protocols obtengo la información de las redes de routing y las interfaces pasivas configuradas en el router.

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?	R3#sh ip protocols Routing Protocol is "rip" Sending updates every 30 seconds, next due in 27 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 Serial0/0/1 2 2 Automatic network summarization is not in effect Maximum path: 4 Routing for Networks: 172.16.0.0 192.168.4.0 192.168.5.0 192.168.6.0 Passive Interface(s): Loopback4 Loopback5 Loopback6 Routing Information Sources: Gateway Distance Last Update 172.16.2.2 120 00:00:02 Distance: (default is 120)
¿Qué comando muestra solo las rutas RIP?	R2#sh ip route rip 172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks R 192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:13, Serial0/0/1 R 192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:13, Serial0/0/1 R 192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:13, Serial0/0/1 R 192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:02, Serial0/0/0 R 192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:02, Serial0/0/0 R 192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:02, Serial0/0/0
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#debug ip rip RIP protocol debugging is on R1#RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/1.21 (192.168.21.1) RIP: build update entries 10.10.10.10/32 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 0 192.168.23.0/24 via 0.0.0.0, metric 1, tag 0 192.168.99.0/24 via 0.0.0.0, metric 1, tag 0

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

Se implementa la configuración de un servicio DHCP para que asigne de manera dinámica direcciones IP, mascara de red, puerta de enlace y servidores DNS a dispositivos finales. La configuración de NAT se realiza para poder navegar desde redes privadas a internet a través de una dirección pública o un pool de direcciones públicas, se puede configurar de manera estática o dinámica según la necesidad y para el escenario se configuro de las 2 maneras.

Paso 17: 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#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`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#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20`

Crear un pool de DHCP para la VLAN 21.	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ip dhcp pool ACCT`
	`R1(dhcp-config)#network 192.168.21.0 255.255.255.0`
	`R1(dhcp-config)#dns-server 10.10.10.10`
	`R1(dhcp-config)#domain-name ccna-sa.com`
	`R1(dhcp-config)#default-router 192.168.21.1`

Crear un pool de DHCP para la VLAN 23	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ip dhcp pool ENGNR`
	`R1(dhcp-config)#network 192.168.23.0 255.255.255.0`
	`R1(dhcp-config)#dns-server 10.10.10.10`
	`R1(dhcp-config)#domain-name ccna-sa.com`
	`R1(dhcp-config)#default-router 192.168.23.1`

Paso 18: 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	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#username webuser privilege 15 password ciscol2345`

Habilitar el servicio del servidor HTTP	`R2(config)#ip http server`
	`                ^`
	`% Invalid input detected at '^' marker.`
	Como se observa en la imagen este comando no es soportado por el simulador packet tracert.

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	`R2(config)#ip http secure-server`
	`                ^`
	`% Invalid input detected at '^' marker.`
	
	`R2(config)#ip http authentication local`
	`                ^`
	`% Invalid input detected at '^' marker.`
	Como se observa en la imagen este comando no es soportado por el simulador packet tracert.

Crear una NAT estática al servidor web.	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237`

Asignar la interfaz interna y externa para la NAT estática	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#int lo0`
	`R2(config-if)#ip nat inside`
	`R2(config-if)#int g0/0`
	`R2(config-if)#ip nat outside`

Configurar la NAT dinámica dentro de una ACL privada	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#access-list 1 permit 192.168.21.0`
	`R2(config)#access-list 1 permit 192.168.23.0`
	`R2(config)#access-list 1 permit 192.168.4.0`
	`R2(config)#access-list 1 permit 192.168.5.0`
	`R2(config)#access-list 1 permit 192.168.6.0`

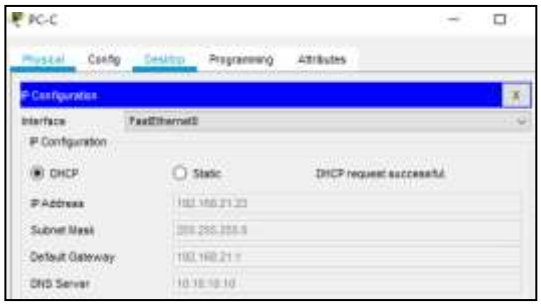
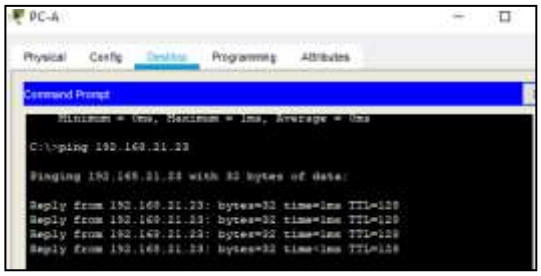
Defina el pool de direcciones IP públicas utilizables.	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236`
	`netmask 255.255.255.248`

Definir la traducción de NAT dinámica	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip nat inside source list 1 pool INTERNET`

Paso 19: 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.

Se realizan las verificaciones correspondientes de cada ítem y mediante las imágenes se verá evidenciado el proceso que he realizado:

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 (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No se puede hacer la prueba porque el simulador packet tracert no soporta la configuracion HTTP sobre el router R2, por este motivo muestra ese reset en la conexion. 

PARTE 6: CONFIGURAR NTP

Se configura un servidor NTP para que los equipos de red sincronicen la misma fecha y hora desde un punto central.

Elemento o tarea de configuración	Especificación

Ajuste la fecha y hora en R2.	`R2>en`
	`Password:`
	`R2#clock set 9:00:00 march 5 2016`

Configure R2 como un maestro NTP.	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ntp master 5`

Configurar R1 como un cliente NTP.	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ntp server 172.16.1.2`

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	`R1#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R1(config)#ntp update-calendar`

Verifique la configuración de NTP en R1.	`R1#sh ntp status`
	`Clock is synchronized, stratum 6, reference is 172.16.1.2`
	`nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24`
	`reference time is 0C6D67EB.00000042 (9:7:55.066 UTC sáb. mar. 5 2016)`
	`clock offset is 2.00 msec, root delay is 8.00  msec`
	`root dispersion is 10.02 msec, peer dispersion is 0.12 msec.`
	`loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000001193 s/s system poll interval is 4, last update was 13 sec ago.`

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Las listas de acceso se utilizan para permitir o denegar la conexión desde una red, un protocolo, un puerto y un host.

Paso 20: 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	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip access-list standard ADMIN-MGT`
	`R2(config-std-nacl)#`

Aplicar la ACL con nombre a las líneas VTY	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#line vty 0 15`
	`R2(config-line)#access-class ADMIN-MGT in`
	`R2(config-line)#login local`

Permitir acceso por Telnet a las líneas de VTY	`R2#conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#ip access-list standard ADMIN-MGT`
	`R2(config-std-nacl)#permit host 172.16.1.1`

Verificar que la ACL funcione como se espera	`R1#telnet 172.16.1.2`
	`Trying 172.16.1.2 ...OpenAcceso no autorizado`
	
	`User Access Verification`
	
	`Username: webuser`
	`Password:`
	`R2#`
	
	`R3#telnet 172.16.2.2`
	`Trying 172.16.2.2 ...`
	`% Connection refused by remote host`
	`R3#telnet 172.16.1.2`
	`Trying 172.16.1.2 ...`
	`% Connection refused by remote host`

Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Se procede a ingresar en el comando de CLI según la descripción de cada ítem como se muestra en la imagen relacionada en cada espacio de la tabla:

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	`R2#show access-list`
	`Standard IP access list ADMIN-MGT`
	`    10 permit host 172.16.1.1 (4 match(es))`
	`Standard IP access list 1`
	`    10 permit host 192.168.21.0`
	`    20 permit host 192.168.23.0`
	`    30 permit host 192.168.4.0`
	`    40 permit host 192.168.5.0`
	`    50 permit host 192.168.6.0`

Restablecer los contadores de una lista de acceso	`R2#clear access-list counter`

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	`R2#show ip interface`
	`GigabitEthernet0/0 is up, line protocol is up (connected)`
	`  Internet address is 209.165.200.233/29`
	`  Broadcast address is 255.255.255.255`
	`  Address determined by setup command`
	`  MTU is 1500 bytes`
	`  Helper address is not set`
	`  Directed broadcast forwarding is disabled`
	`  Outgoing access list is not set`
	`  Inbound  access list is not set`

¿Con qué comando se muestran las traducciones NAT?	`R2#sh 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 10.10.10.10:80 209.165.200.238:1027209.165.200.238:1027`
	`tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1028209.165.200.238:1028`
	`tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1029209.165.200.238:1029`
	`tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1030209.165.200.238:1030`
	`tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1031209.165.200.238:1031`
	`tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1032209.165.200.238:1032`

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	`R2#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:

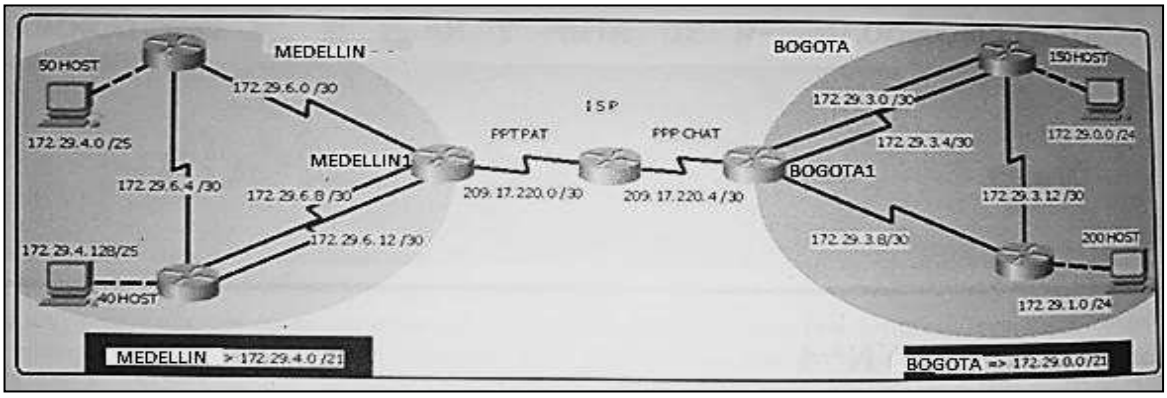


Fig. 2 Topología escenario 2 Protocolo OSPF

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).

Solución:

•Se procede con la agrupación de los puertos seriales de la siguiente manera para cada uno de los routers:

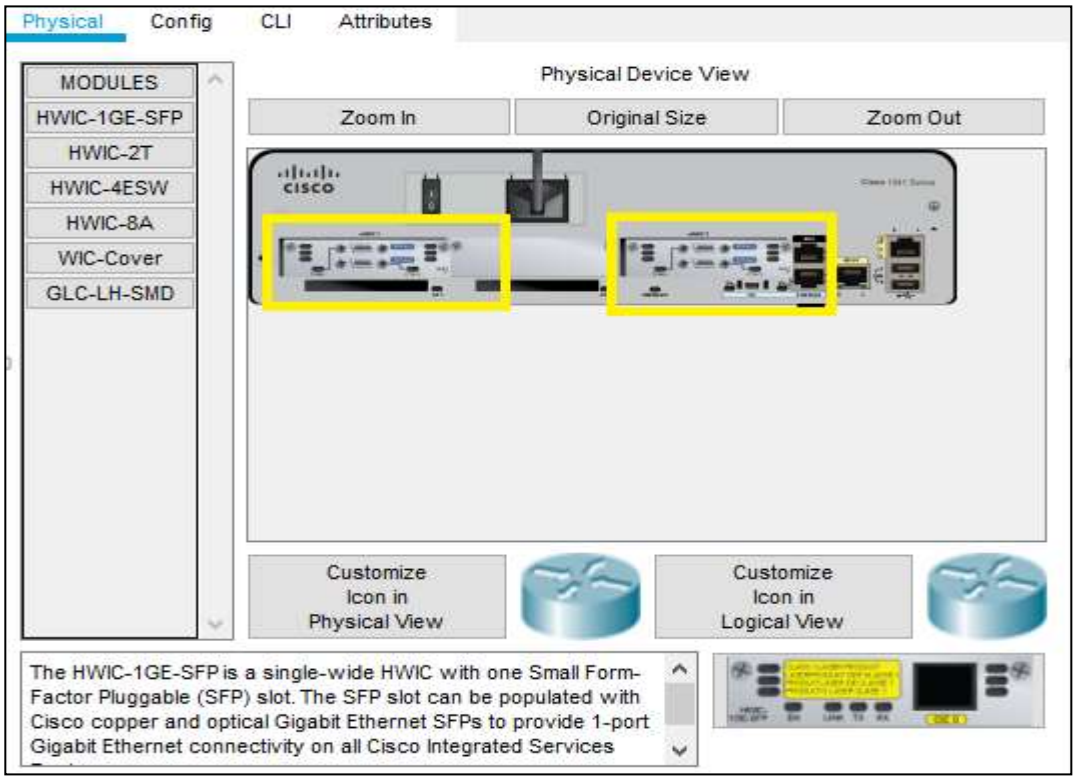


Fig. 3 Adición Tarjetas Serial Router

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

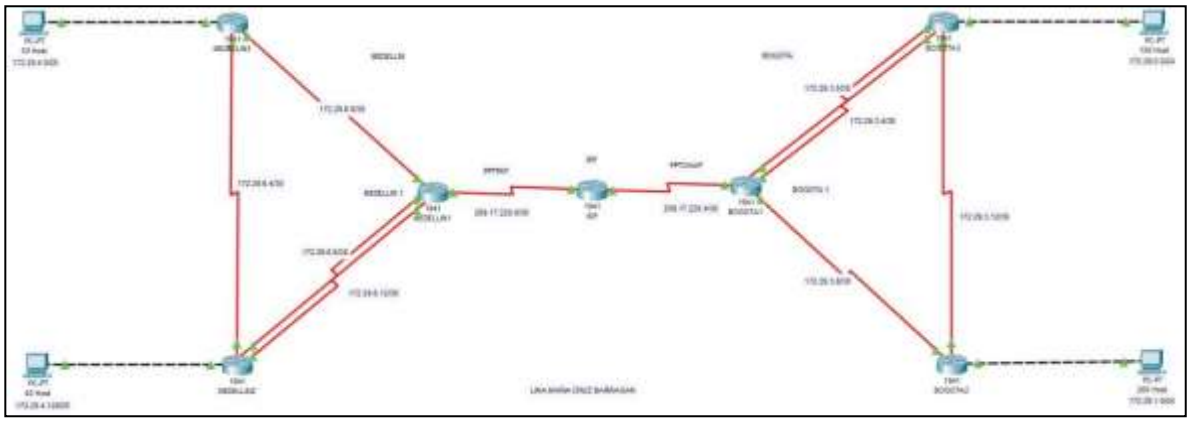


Fig. 4 Topología escenario2 packet tracert

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

Se realiza la configuración de un enrutamiento dinámico que para este escenario es el protocolo OSPF, donde se configuran las redes que están directamente conectadas a cada uno de los router y se diferencia del protocolo RIPv2 porque este utiliza áreas para realizar el intercambio de información de enrutamiento con otras redes.

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

Configuración Router ISP

Lo primero que realizo en la configuración del router ISP configurando las interfaces como se evidencia en las imágenes:

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int s0/1/1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#no shutdown
```

```
ISP(config-if)#int s0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no shutdown
```

Posteriormente realizo la configuración de las demás interfaces para cada uno de los routers:

Configuración Router MEDELLIN1

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

```
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#no shut
```

```
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#no shut
```

```
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#no shut
```

Configuración Router MEDELLIN2

```
MEDELLIN2(config-if)#int s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN2(config-if)#no shutdown
```

```
MEDELLIN2(config)#int s0/1/1
MEDELLIN2(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN2(config-if)#no shutdown
```

```
MEDELLIN2(config-if)#int g0/1
MEDELLIN2(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN2(config-if)#no shutdown
```

```
MEDELLIN2(config-if)#int s0/1/0
MEDELLIN2(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN2(config-if)#no shutdown
```

Configuración Router MEDELLIN3

```
MEDELLIN3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN3(config-if)#no shutdown
```

```
MEDELLIN3(config)#int s0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN3(config-if)#no shutdown
```

```
MEDELLIN3(config-if)#int g0/0
MEDELLIN3(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN3(config-if)#no shutdown
```

Configuración Router BOGOTA1

```
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

Configuración Router BOGOTA2

```
BOGOTA2(config-if)#int s0/1/1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
```

```
BOGOTA2(config-if)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA2(config-if)#no shutdown
```

```
BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown
```

Configuración Router BOGOTA3

```
BOGOTA3(config-if)#int s0/1/1
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config-if)#int s0/0/1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config-if)#int s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config-if)#int g0/1
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
```

Procedo a realizar la configuración de enrutamiento del Ospf v2 y configurándolo para la ip y mascara de cada uno de los routers como se muestra en las imágenes de cada uno de los routers:

Configuración Router MEDELLIN1

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#route ospf 1
MEDELLIN1(config-router)#router-id 1.1.1.1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
```

Configuración Router MEDELLIN2

```
MEDELLIN2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN2(config)#route ospf 1
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#network 172.29.4.128 0.0.0.127 area 1
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.3 area 1
```

Configuración Router MEDELLIN3

```
MEDELLIN3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN3(config)#route ospf 1
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.127 area 1
MEDELLIN3(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1
```

Configuración Router BOGOTA1

```
BOGOTA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA1(config)#route ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 2
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 2
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 2
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
```

Configuración Router BOGOTA2

```
BOGOTA2(config-router)#route ospf 1
BOGOTA2(config-router)#router-id 2.2.2.2
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 2
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 2
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 2
```

Configuración Router BOGOTA3

```
BOGOTA3(config-router)#route ospf 1
BOGOTA3(config-router)#router-id 3.3.3.3
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 2
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 2
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 2
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 2
```

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.

Se procede a realizar la configuración de enrutamiento para los dos routers y a su ves se realiza la redistribución de la misma como se puede evidenciar en las imágenes:

Configuración Router MEDELLIN1

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#route ospf 1
MEDELLIN1(config-router)#default-information originate
```

Configuración Router BOGOTA1

```
BOGOTA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

```
BOGOTA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA1(config)#route ospf 1
BOGOTA1(config-router)#default-information originate
```

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.

Configuración Router ISP

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
```

PARTE 2: TABLA DE ENRUTAMIENTO

Las tablas de enrutamiento nos permiten identificar que redes están conectadas y cuales fueron aprendidas de acuerdo al enrutamiento utilizado, nos ayuda a identificar el camino que puede tomar el tráfico para llegar a una red.

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

Se procede a realizar la verificación de la tabla de enrutamiento utilizando el comando show ip route para cada uno de los routers:

Tabla de enrutamiento MEDELLIN1

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 02:21:24, Serial0/1/1
O       172.29.4.128/25 [110/65] via 172.29.6.14, 02:21:24,
Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/1/1
L       172.29.6.1/32 is directly connected, Serial0/1/1
O       172.29.6.4/30 [110/128] via 172.29.6.14, 02:21:24,
Serial0/0/1
                      [110/128] via 172.29.6.2, 02:21:24, 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, Serial0/0/1
L       172.29.6.13/32 is directly connected, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
                [1/0] via 209.17.220.1
                is directly connected, Serial0/1/1
```

Tabla de enrutamiento MEDELLIN2

```
Gateway of last resort is 172.29.6.9 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, 02:23:09, Serial0/1/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/1
L       172.29.4.129/32 is directly connected, GigabitEthernet0/1
O       172.29.6.0/30 [110/128] via 172.29.6.5, 02:23:09, Serial0/1/0
                      [110/128] via 172.29.6.9, 02:23:09, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/1/0
L       172.29.6.6/32 is directly connected, Serial0/1/0
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
     209.17.220.0/30 is subnetted, 1 subnets
O IA    209.17.220.0/30 [110/128] via 172.29.6.9, 02:23:09,
Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.9, 02:23:09, Serial0/0/0
```

Tabla de enrutamiento MEDELLIN3

```
Gateway of last resort is 172.29.6.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 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, 02:24:56,
Serial0/1/0
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.2/32 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/1/0
L       172.29.6.5/32 is directly connected, Serial0/1/0
O       172.29.6.8/30 [110/128] via 172.29.6.6, 02:24:46, Serial0/1/0
                      [110/128] via 172.29.6.1, 02:24:46, Serial0/0/0
O       172.29.6.12/30 [110/128] via 172.29.6.6, 02:24:46,
Serial0/1/0
                       [110/128] via 172.29.6.1, 02:24:46,
Serial0/0/0
     209.17.220.0/30 is subnetted, 1 subnets
O IA    209.17.220.0/30 [110/128] via 172.29.6.1, 02:24:46,
Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 02:24:46, Serial0/0/0
```

Tabla de enrutamiento BOGOTA1

```
Gateway of last resort is 0.0.0.0 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, 00:36:23, Serial0/1/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:36:23, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/1/1
L       172.29.3.1/32 is directly connected, Serial0/1/1
C       172.29.3.4/30 is directly connected, Serial0/0/0
L       172.29.3.5/32 is directly connected, Serial0/0/0
C       172.29.3.8/30 is directly connected, Serial0/1/0
L       172.29.3.9/32 is directly connected, Serial0/1/0
O       172.29.3.12/30 [110/128] via 172.29.3.10, 00:36:23,
Serial0/1/0
                       [110/128] via 172.29.3.2, 00:36:23,
Serial0/1/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/1
C       209.17.220.5/32 is directly connected, Serial0/0/1
L       209.17.220.6/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.17.220.5
                is directly connected, Serial0/0/1
                is directly connected, Serial0/1/0
```

Tabla de enrutamiento BOGOTA2

```
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, 00:48:15, 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 172.29.3.13, 00:19:12,
Serial0/0/1
                      [110/128] via 172.29.3.9, 00:19:12, Serial0/1/1
O       172.29.3.4/30 [110/128] via 172.29.3.13, 00:19:12,
Serial0/0/1
                      [110/128] via 172.29.3.9, 00:19:12, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/1/1
L       172.29.3.10/32 is directly connected, Serial0/1/1
C       172.29.3.12/30 is directly connected, Serial0/0/1
L       172.29.3.14/32 is directly connected, Serial0/0/1
     209.17.220.0/30 is subnetted, 1 subnets
O IA    209.17.220.4/30 [110/128] via 172.29.3.9, 00:19:12,
Serial0/1/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:19:12, Serial0/1/1
```

Tabla de enrutamiento BOGOTA3

```
Gateway of last resort is 172.29.3.1 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, GigabitEthernet0/1
L       172.29.0.1/32 is directly connected, GigabitEthernet0/1
O       172.29.1.0/24 [110/65] via 172.29.3.14, 01:24:57, Serial0/0/0
C       172.29.3.0/30 is directly connected, Serial0/1/1
L       172.29.3.2/32 is directly connected, Serial0/1/1
C       172.29.3.4/30 is directly connected, Serial0/0/1
L       172.29.3.6/32 is directly connected, Serial0/0/1
O       172.29.3.8/30 [110/128] via 172.29.3.14, 00:20:43,
Serial0/0/0
                      [110/128] via 172.29.3.1, 00:20:43, Serial0/1/1
C       172.29.3.12/30 is directly connected, Serial0/0/0
L       172.29.3.13/32 is directly connected, Serial0/0/0
     209.17.220.0/30 is subnetted, 1 subnets
O IA    209.17.220.4/30 [110/128] via 172.29.3.1, 00:20:43,
Serial0/1/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:20:43, Serial0/1/1
```

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

Router MEDELLIN1

```
O       172.29.6.4/30 [110/128] via 172.29.6.14, 02:21:24,
Serial0/0/1
                      [110/128] via 172.29.6.2, 02:21:24, Serial0/1/1
```

Router MEDELLIN2

```
O       172.29.6.0/30 [110/128] via 172.29.6.5, 02:23:09, Serial0/1/0
                      [110/128] via 172.29.6.9, 02:23:09, Serial0/0/0
```

Router MEDELLIN3

```
O       172.29.6.8/30 [110/128] via 172.29.6.6, 02:24:46, Serial0/1/0
                      [110/128] via 172.29.6.1, 02:24:46, Serial0/0/0
O       172.29.6.12/30 [110/128] via 172.29.6.6, 02:24:46,
Serial0/1/0
                       [110/128] via 172.29.6.1, 02:24:46,
Serial0/0/0
```

Router BOGOTA1

```
O       172.29.3.12/30 [110/128] via 172.29.3.10, 00:10:03, Serial0/1/0
                       [110/128] via 172.29.3.2, 00:10:03, Serial0/1/1
```

Router BOGOTA2

```
O       172.29.3.0/30 [110/128] via 172.29.3.13, 00:12:34, Serial0/0/1
                      [110/128] via 172.29.3.9, 00:12:34, Serial0/1/1
O       172.29.3.4/30 [110/128] via 172.29.3.13, 00:12:34, Serial0/0/1
                      [110/128] via 172.29.3.9, 00:12:34, Serial0/1/1
```

Router BOGOTA3

```
O       172.29.3.8/30 [110/128] via 172.29.3.5, 00:13:07, Serial0/0/1
                      [110/128] via 172.29.3.14, 00:13:07, Serial0/0/0
```

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.

Router MEDELLIN1

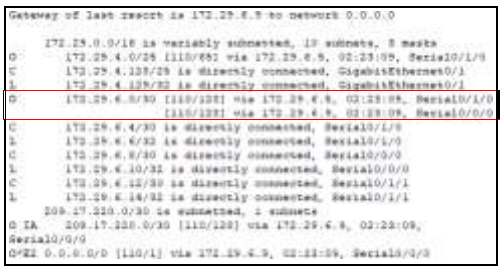
```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 02:21:24, Serial0/1/1
O       172.29.4.128/25 [110/65] via 172.29.6.14, 02:21:24,
Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/1/1
L       172.29.6.1/32 is directly connected, Serial0/1/1
O       172.29.6.4/30 [110/128] via 172.29.6.14, 02:21:24,
Serial0/0/1
                      [110/128] via 172.29.6.2, 02:21:24, 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, Serial0/0/1
L       172.29.6.13/32 is directly connected, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/0
L       209.17.220.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
                [1/0] via 209.17.220.1
                is directly connected, Serial0/1/1
```

Router BOGOTA1

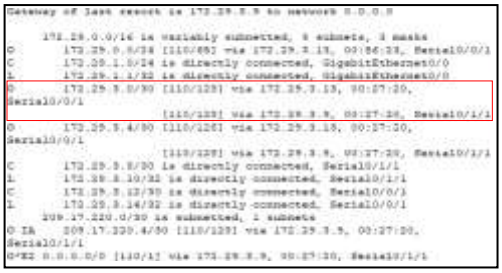
```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     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, 00:36:23, Serial0/1/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:36:23, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/1/1
L       172.29.3.1/32 is directly connected, Serial0/1/1
C       172.29.3.4/30 is directly connected, Serial0/0/0
L       172.29.3.5/32 is directly connected, Serial0/0/0
C       172.29.3.8/30 is directly connected, Serial0/1/0
L       172.29.3.9/32 is directly connected, Serial0/1/0
O       172.29.3.12/30 [110/128] via 172.29.3.10, 00:36:23,
Serial0/1/0
                       [110/128] via 172.29.3.2, 00:36:23,
Serial0/1/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/1
C       209.17.220.5/32 is directly connected, Serial0/0/1
L       209.17.220.6/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.17.220.5
                is directly connected, Serial0/0/1
                is directly connected, Serial0/1/0
```

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

Router MEDELLIN2

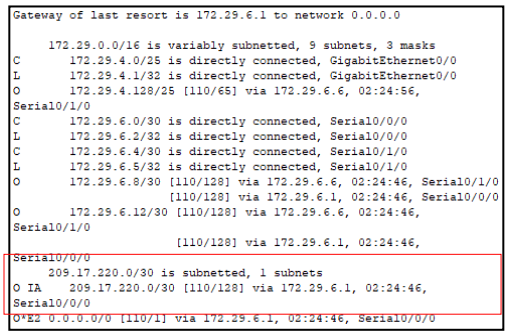


Router BOGOTA2

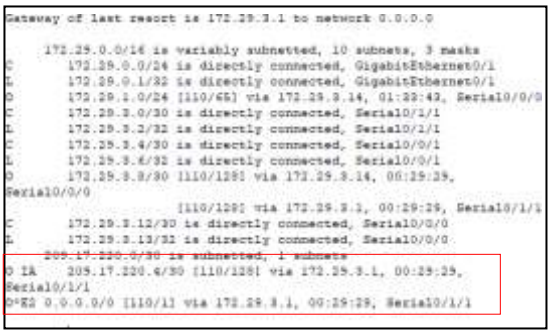


e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Router Medellin3



Router Bogota3



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

Se procede a realizar la tabla de enrutamiento para el router ISP como se muestra a continuación:

Tabla de Enrutamiento Router ISP

```
ISP#sh 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, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/1
L       209.17.220.1/32 is directly connected, Serial0/1/1
C       209.17.220.4/30 is directly connected, Serial0/0/1
L       209.17.220.5/32 is directly connected, Serial0/0/1
```

PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF

Se realiza la des habilitación del protocolo OSPF en interfaces que no intervienen en el intercambio de información de enrutamiento, lo que optimiza el intercambio de la información al momento de la propagación del protocolo en la red.

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.

   Procedo a deshabilitar la propagación del protocolo OSPF, con el passive interface de los routers indicados en la tabla:

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

Passive Interface Router MEDELLIN1

```
MEDELLIN1(config-router)#route ospf 1
MEDELLIN1(config-router)#passive-interface g0/0
MEDELLIN1(config-router)#passive-interface g0/1
MEDELLIN1(config-router)#passive-interface s0/0/0
```

Passive Interface Router MEDELLIN2

```
MEDELLIN2(config)#route ospf 1
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#passive-interface s0/0/1
```

Passive Interface Router MEDELLIN3

```
MEDELLIN3(config)#route ospf 1
MEDELLIN3(config-router)#passive-interface g0/1
MEDELLIN3(config-router)#passive-interface s0/0/1
MEDELLIN3(config-router)#passive-interface s0/1/1
```

Passive Interface Router BOGOTA1

```
BOGOTA1(config-router)#route ospf 1
BOGOTA1(config-router)#passive-interface s0/0/1
BOGOTA1(config-router)#passive-interface g0/0
BOGOTA1(config-router)#passive-interface g0/1
```

Passive Interface Router BOGOTA2

```
BOGOTA2(config)#route ospf 1
BOGOTA2(config-router)#passive-interface g0/1
BOGOTA2(config-router)#passive-interface s0/0/0
BOGOTA2(config-router)#passive-interface s0/1/0
BOGOTA2(config-router)#passive-interface s0/1/0
```

Passive Interface Router BOGOTA3

```
BOGOTA3(config-router)#route ospf 1
BOGOTA3(config-router)#passive-interface s0/1/0
BOGOTA3(config-router)#passive-interface g0/0
```

PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

Es necesario verificar la configuración del protocolo OSPF, para poder garantizar un correcto funcionamiento de conexión en la red, poder ver la configuración de los neighbors y la base de datos en cada uno de los router que intervienen en la red.

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.

Se procede con la verificación del passive interface de cada uno de los routers

Router MEDELLIN1 protocolo OSPF

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 passive-interface Serial0/0/0
 network 209.17.220.0 0.0.0.3 area 0
 network 172.29.6.0 0.0.0.3 area 1
 network 172.29.6.8 0.0.0.3 area 1
 network 172.29.6.12 0.0.0.3 area 1
 default-information originate
```

Router MEDELLIN2 protocolo OSPF

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface Serial0/0/1
 network 172.29.4.128 0.0.0.127 area 1
 network 172.29.6.4 0.0.0.3 area 1
 network 172.29.6.8 0.0.0.3 area 1
 network 172.29.6.12 0.0.0.3 area 1
```

Router MEDELLIN3 protocolo OSPF

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 passive-interface Serial0/0/1
 passive-interface Serial0/1/1
 network 172.29.4.0 0.0.0.127 area 1
 network 172.29.6.0 0.0.0.3 area 1
 network 172.29.6.4 0.0.0.3 area 1
```

Router BOGOTA1 protocolo OSPF

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 passive-interface Serial0/0/1
 network 209.17.220.4 0.0.0.3 area 0
 network 172.29.3.0 0.0.0.3 area 2
 network 172.29.3.4 0.0.0.3 area 2
 network 172.29.3.8 0.0.0.3 area 2
 default-information originate
```

Router BOGOTA2 protocolo OSPF

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 passive-interface Serial0/0/0
 passive-interface Serial0/1/0
 network 172.29.1.0 0.0.0.255 area 2
 network 172.29.3.8 0.0.0.3 area 2
 network 172.29.3.12 0.0.0.3 area 2
```

Router BOGOTA3 protocolo OSPF

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface Serial0/1/0
 network 172.29.0.0 0.0.0.255 area 2
 network 172.29.3.0 0.0.0.3 area 2
 network 172.29.3.4 0.0.0.3 area 2
 network 172.29.3.12 0.0.0.3 area 2
```

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

Procedemos a obtener los datos de verificación utilizando el comando show ip ospf database:

Base Datos Router MEDELLIN1

```
MEDELLIN1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
1.1.1.1         1.1.1.1         1045        0x80000007 0x00fc4a 1

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.29.6.8      1.1.1.1         1025        0x8000001f 0x00ea3d
172.29.6.12     1.1.1.1         1025        0x80000020 0x00c062
172.29.6.0      1.1.1.1         1025        0x80000021 0x0037f6
172.29.4.128    1.1.1.1         1025        0x80000022 0x0065c4
172.29.6.4      1.1.1.1         1025        0x80000023 0x008d5a
172.29.4.0      1.1.1.1         1025        0x80000024 0x006642

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
1.1.1.1         1.1.1.1         1036        0x8000000e 0x002034 6
3.3.3.3         3.3.3.3         1036        0x8000000b 0x00d97c 5
2.2.2.2         2.2.2.2         1034        0x8000000d 0x00ff6d 7

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.0    1.1.1.1         1042        0x80000006 0x00df79

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         1045        0x80000006 0x00f4d4 1
```

Base Datos Router MEDELLIN2

```
MEDELLIN2#show ip ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
2.2.2.2         2.2.2.2         1556        0x80000011 0x00f771 7
1.1.1.1         1.1.1.1         1560        0x80000012 0x001838 6
3.3.3.3         3.3.3.3         1558        0x8000000f 0x00d180 5

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.0    1.1.1.1         1566        0x8000000a 0x00d77d

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         1569        0x8000000a 0x00ecd8 1
```

Base Datos Router MEDELLIN3

```
MEDELLIN3#show ip ospf database
            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
3.3.3.3         3.3.3.3         1650        0x8000000f 0x00d180 5
1.1.1.1         1.1.1.1         1652        0x80000012 0x001838 6
2.2.2.2         2.2.2.2         1649        0x80000011 0x00f771 7

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.0    1.1.1.1         1658        0x8000000a 0x00d77d

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         1662        0x8000000a 0x00ecd8 1
```

Base Datos Router BOGOTA1

```
BOGOTA1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
1.1.1.1         1.1.1.1         1018        0x80000003 0x002dla 1

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.29.3.0      1.1.1.1         1004        0x80000007 0x008cbe
172.29.3.4      1.1.1.1         1004        0x80000008 0x0062e3
172.29.3.8      1.1.1.1         1004        0x80000009 0x003809
172.29.3.12     1.1.1.1         1004        0x8000000a 0x00916a
172.29.0.0      1.1.1.1         1004        0x8000000b 0x00c184
172.29.1.0      1.1.1.1         1004        0x8000000c 0x00b48f

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
1.1.1.1         1.1.1.1         1076        0x8000000a 0x006511 6
3.3.3.3         3.3.3.3         1010        0x80000011 0x00632a 7
2.2.2.2         2.2.2.2         1009        0x8000000b 0x00c701 5

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.4    1.1.1.1         176         0x80000003 0x00bd9a

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         1018        0x80000002 0x00fcd0 1
```

Base Datos Router BOGOTA2

```
BOGOTA2#show ip ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
2.2.2.2         2.2.2.2         1073        0x8000000b 0x00c701 5
1.1.1.1         1.1.1.1         1141        0x8000000a 0x006511 6
3.3.3.3         3.3.3.3         1074        0x80000011 0x00632a 7

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.4    1.1.1.1         240         0x80000003 0x00bd9a

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         2941        0x80000003 0x00fad1 1
```

Base Datos Router BOGOTA3

```
BOGOTA3>en
BOGOTA3#show ip ospf database
            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
3.3.3.3         3.3.3.3         1141        0x80000011 0x00632a 7
1.1.1.1         1.1.1.1         1208        0x8000000a 0x006511 6
2.2.2.2         2.2.2.2         1141        0x8000000b 0x00c701 5

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
209.17.220.4    1.1.1.1         307         0x80000003 0x00bd9a

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         3008        0x80000003 0x00fad1 1
```

PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

Configuración Router ISP

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#username MEDELLIN1 password Clsc0
ISP(config)#interface Serial0/1/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password Clsc0
```

Configuración Router MEDELLIN1

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#username ISP password Clsc0
MEDELLIN1(config)#interface Serial0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password Clsc0
```

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Configuración Router ISP

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#username BOGOTA1 password Clsc0
ISP(config)#interface Serial0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

Configuración Router BOGOTA1

```
BOGOTA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA1(config)#username ISP password Clsc0
BOGOTA1(config)#interface Serial0/0/1
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
```

PARTE 6: CONFIGURACIÓN DE PAT

Se realiza la configuración de PAT para que una sola dirección IP sea la salida hacia internet de varias máquinas en una red privada y el único cambio que se observa es en el puerto de salida global.

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.

A continuación, se procede a configurar las listas de acceso para la configuración de los routers:

Configuración Router MEDELLIN1

```
MEDELLIN1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN1(config)#ip nat inside source list 1 interface Serial0/0/0
overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#interface Serial0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#interface Serial0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface Serial0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface Serial0/1/1
MEDELLIN1(config-if)#ip nat inside
```

Configuración Router BOGOTA1

```
BOGOTA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA1(config)#ip nat inside source list 1 interface Serial0/0/1
overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#interface Serial0/0/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface Serial0/0/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface Serial0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface Serial0/1/1
BOGOTA1(config-if)#ip nat inside
```

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.

Se procede a configurar la NAT en el router Medellín y para verificar dicha configuración hago uso del comando show ip nat translations:

Configuración Router MEDELLIN1

```
MEDELLIN1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.2:25   172.29.4.2:25      209.17.220.1:25    209.17.220.1:25
icmp 209.17.220.2:26   172.29.4.2:26      209.17.220.1:26    209.17.220.1:26
icmp 209.17.220.2:27   172.29.4.2:27      209.17.220.1:27    209.17.220.1:27
icmp 209.17.220.2:28   172.29.4.2:28      209.17.220.1:28    209.17.220.1:28
```

```
C:\>ping 209.17.220.1

Pinging 209.17.220.1 with 32 bytes of data:

Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=16ms TTL=253

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 16ms, Average = 5ms
```

Fig. 5 Prueba de conectividad ping router ISP

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

Procedo a realizar el mismo proceso del punto anterior haciendo uso del comando show ip nat translation para el router Bogota1:

Configuración Router BOGOTA1

```
BOGOTA1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.17.220.6:29   172.29.1.2:29      209.17.220.5:29    209.17.220.5:29
icmp 209.17.220.6:30   172.29.1.2:30      209.17.220.5:30    209.17.220.5:30
icmp 209.17.220.6:31   172.29.1.2:31      209.17.220.5:31    209.17.220.5:31
icmp 209.17.220.6:32   172.29.1.2:32      209.17.220.5:32    209.17.220.5:32
icmp 209.17.220.6:54   172.29.0.2:54      209.17.220.5:54    209.17.220.5:54
icmp 209.17.220.6:55   172.29.0.2:55      209.17.220.5:55    209.17.220.5:55
icmp 209.17.220.6:56   172.29.0.2:56      209.17.220.5:56    209.17.220.5:56
icmp 209.17.220.6:57   172.29.0.2:57      209.17.220.5:57    209.17.220.5:57
```

```
C:\>ping 209.17.220.5

Pinging 209.17.220.5 with 32 bytes of data:

Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253

Ping statistics for 209.17.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Fig. 6 Prueba de conectividad ping router ISP

PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

Se implementa la configuración de un servicio DHCP para que asigne de manera dinámica direcciones IP, mascara de red y puerta de enlace a dispositivos finales, se debe tener en cuenta realizar exclusiones de direcciones ip para no crear conflictos en la configuración realizada en la red.

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

   Se procede con la configuración del servidor DHCP para las redes con el comando ip dhcp pool 50host como lo muestran las imágenes:

   Configuración Router MEDELLIN2

```
MEDELLIN2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN2(config)#ip dhcp pool 50host
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#ip dhcp pool 40host
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
```

   Se realiza la exclusión de las direcciones DHCP:

   Exclusión Direcciones DHCP

```
ip dhcp excluded-address 172.29.4.129
ip dhcp excluded-address 172.29.4.1
```

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

   Procedo a habilitar el paso de los mensajes del broadcast con el comando ip helper-address y la ip 172.29.6.6

   Configuración Router MEDELLIN3

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.6
```

c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Procedo a realizar la configuración haciendo uso del comando ip dhcp pool para configurar la red de los 150host y 200host después adiciono las networks 172.29.0.0 y 172.29.1.0 máscara 255.255.255.0 para el router de bogota2

Configuración Router BOGOTA2

```
BOGOTA2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOGOTA2(config)#ip dhcp pool 150Host
BOGOTA2(dhcp-config)# network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#ip dhcp pool 200Host
BOGOTA2(dhcp-config)# network 172.29.1.0 255.255.255.0
```

Exclusión Direcciones DHCP

```
ip dhcp excluded-address 172.29.1.1
ip dhcp excluded-address 172.29.0.1
```

d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

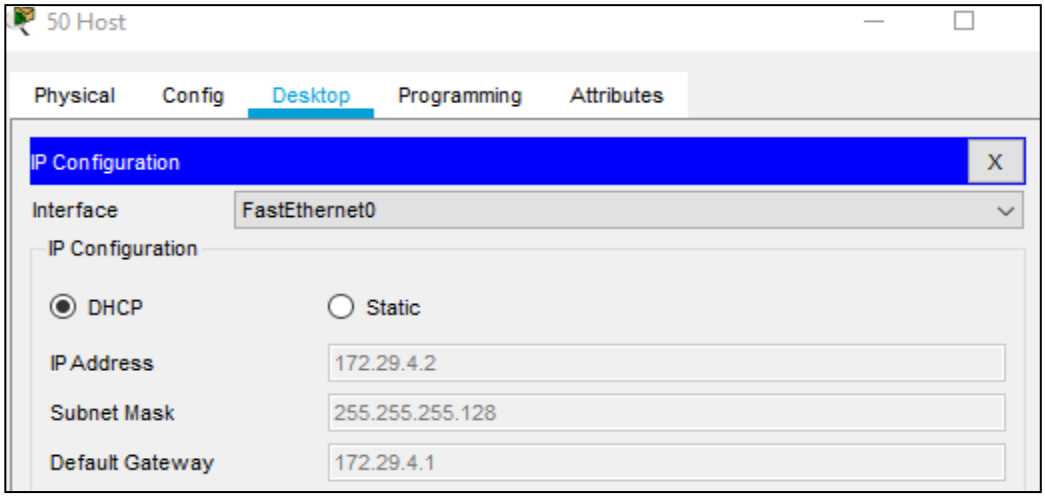
Procedo a realizar la habilitación del paso de los mensajes utilizando el comando ip helper-address 172.29.3.14

Configuración Router BOGOTA3

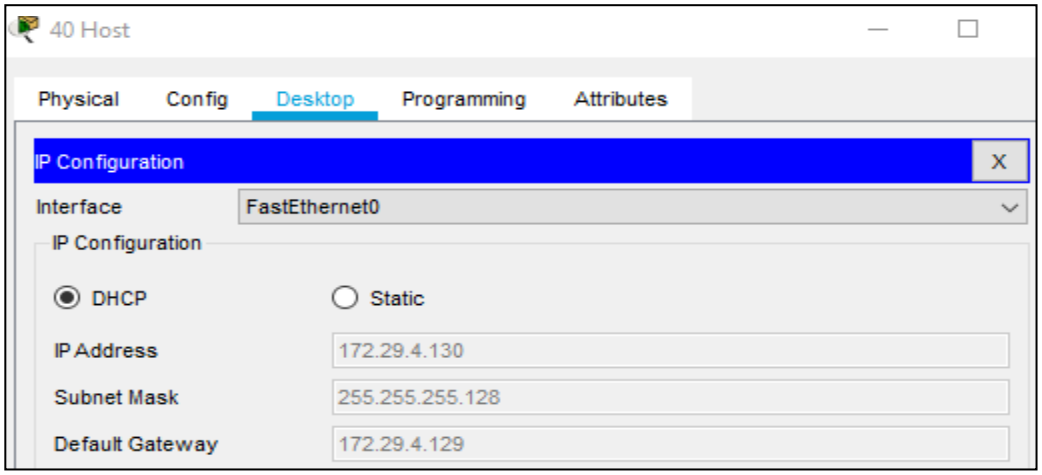
```
BOGOTA3(config)#int g0/1
BOGOTA3(config-if)#ip helper-address 172.29.3.14
```

Se realizan las verificaciones correspondientes adjunto evidencias

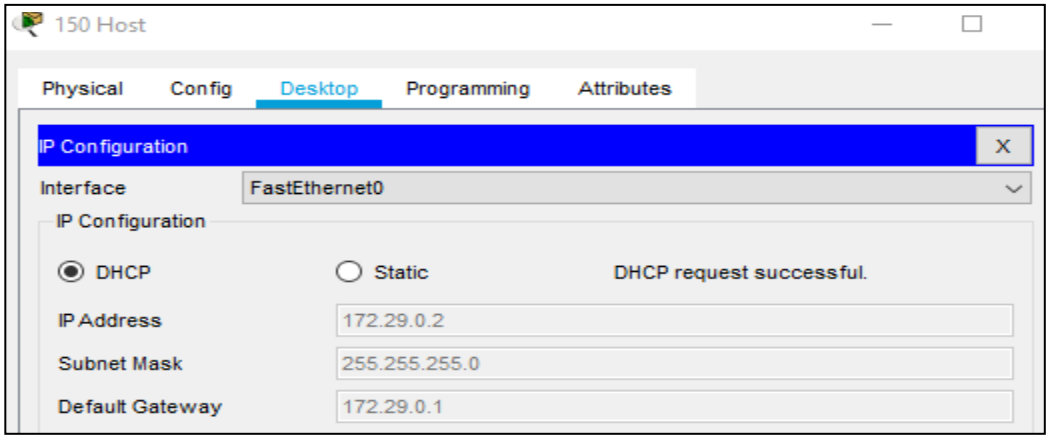
PC RED LAN 172.29.4.0/25



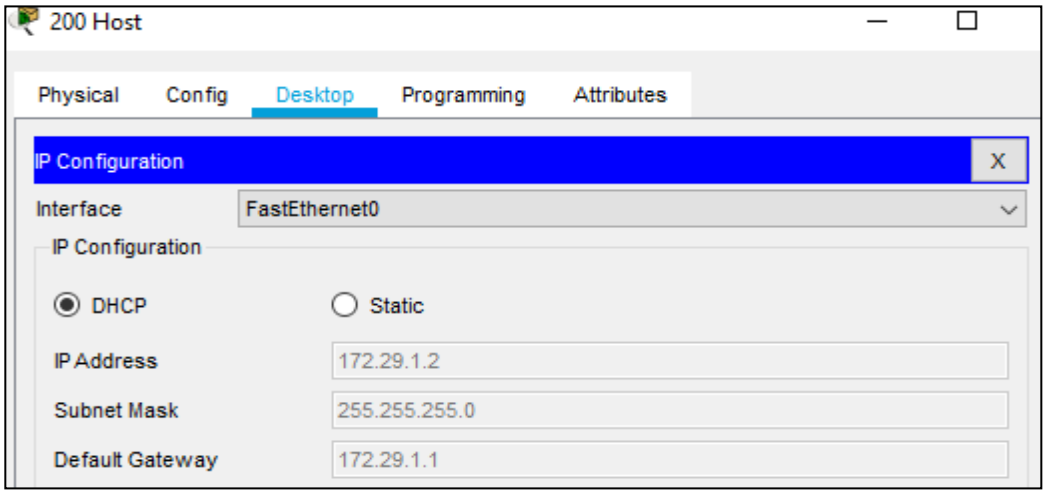
PC RED LAN 172.29.4.128/25



PC RED LAN 172.29.0.0/24



PC RED LAN 172.29.1.0/24



CONCLUSIONES

El simulador de redes packet Tracert permite identificar diferentes formas de configuración de los diferentes dispositivos de red como los routers, switches, servidores etc en escenarios prácticos.

El protocolo OSPF es el más importante del estado de enlace, ya que se basa en normas de código abierto permitiendo que sea utilizado por cualquier empresa lo cual lo convierte en un protocolo de enrutamiento sólido.

La configuración de Port Address Traslation (PAT) permite que una sola dirección ip sea utilizada por varios dispositivos a través de internet lo cual sirve para conservar el direccionamiento IP público.

Con las actividades realizadas en cada uno de los escenarios demuestro lo aprendido en el diplomado, ya que reúne métodos de configuración básica en los dispositivos de red, protocolos de enrutamiento, configuración de NAT y PAT para la salida hacia internet, segmentación de red e implementación de un DHCP.

BIBLIOGRAFÍA

(s.f.). Capiulo 1 Marco Teorico . Obtenido dehttp://catarina.udlap.mx/u_dl_a/tales/documentos/lis/aldrette_m_a/capitulo1.pdf

CISCO. (s.f.). Transformación digial para la PYME. Obtenido de https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf

IP, C. e. (s.f.). Obtenido de https://www.cual-es-mi-ip.net/

Oscar, G. (Julio de 2006). Mis Libros de Networking. Obtenido de 1: http://librosnetworking.blogspot.com/2006/07/principios-bsicos-de-ripv2.html

Prat, D. d. (2011). Comandos para Routers Cisco. Obtenido de https://eltallerdelbit.com/comandos-routers-cisco/

Wikipedia. (27 de Agosto de 2019). Lista de control de acceso. Obtenido de https://es.wikipedia.org/wiki/Lista_de_control_de_acceso

Wikipedia. (25 de Marzo de 2020). Máscara de red. Obtenido de Máscara de red: https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

Wikipedia. (20 de Febrero de 2020). Network Time Protocol. Obtenido de Network Time Protocol: https://es.wikipedia.org/wiki/Network_Time_Protocol

Wikipedia. (11 de Mayo de 2020). Protocolo de configuración dinámica de host. Obtenido de Protocolo de configuración dinámica de host: https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

Wikipedia. (26 de abril de 2020). Sistema de nombres de dominio. Obtenido de Sistema de nombres de dominio: https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio