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

DARIN TORRES VELASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACION CISCO
IBAGUE
2020

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

DARIN TORRES VELASQUEZ

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE INGENIERO DE SISTEMAS

HECTOR JULIAN PARRA
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACION CISCO
IBAGUE
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ibagué, 17 de mayo 2020

Dedico este logro a Dios quien me dio fuerza espiritual para seguir con mis estudios. A mis padres y hermanos que me alentaron a no desfallecer, me educaron y apoyaron a seguir con constancia en el Diplomado en profundización de redes Cisco. A mis compañeros de estudio, a mis maestros y amigos, quienes sin su ayuda nunca hubiera podido hacer este Diplomado. A todos ellos se los agradezco desde el fondo de mi alma. Para todos ellos hago esta dedicatoria.

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

Mi profundo agradecimiento a todos los actores de la unidad educativa por confiar en mí, abrirme las puertas y permitirme realizar todo el proceso de aprendizaje dentro de su establecimiento educativo.

De igual manera mis agradecimientos a la Universidad Nacional Abierta y a Distancia, a mis profesores quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional.

Finalmente quiero expresar mi más grande y sincero agradecimiento al Ingeniero Hector Julian Parra, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza, colaboración me ha orientado y permitió el desarrollo de este trabajo.

RESUMEN

Este trabajo de grado es una prueba de habilidades para implementar la topología de red de dos escenarios.

El primer escenario se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

El segundo escenario es la simulación de la red de una empresa que posee sucursales distribuidas en las ciudades de Bogotá y Medellín, como estudiantes vamos asumir el rol de administrador de la red, se configura e interconecta 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.

Con el aplicativo de packet tracer se realiza la configuración de la topología de red, se identifican los host con direcciones ip, los router y switch se configuran con los parámetros básicos asignando nombres al router y switch, configurando la seguridad de estos equipos con contraseñas de acceso a usuarios y administradores con derechos privilegiados.

A través de comandos de consulta se visualiza la información de configuración de cada router y switch, tales como la conectividad entre host, la visualización de enrutamiento, las tablas de routing, los saltos de routing.

Al realizar todas estas configuraciones, estamos demostrando nuestras habilidades en la implementación y configuración de redes LAN y WAN.

PALABRAS CLAVE: Solución de dos estudios de caso bajo el uso de tecnología cisco, prueba de habilidades, trabajo de grado.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. INTRODUCCIÓN

El contenido de este trabajo brindara los conocimientos adquiridos en el Diplomado de Profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN) como opción de grado.

Se realizó una prueba de habilidades a través de dos escenarios, creando la topología de red, configuraciones básicas de router y switch, routing entre VLAN, protocolos de RIPV2 y OSPF, configuración de hosts dinámicos (DHCP), traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL), protocolo de tiempo de red (NTP) y configuración de PPP con enlaces a ISP.

Así mismo, este trabajo será una herramienta de guía para entender el funcionamiento de las redes en la vida real, siendo el simulador de packet tracer una herramienta muy poderosa que nos permitirá realizar y verificar las configuraciones del buen funcionamiento de una red.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Adquirir habilidades para implementar una red LAN y conocer los procesos de identificación / verificación de fallas en la conectividad de los dispositivos host.

2.2. OBJETIVOS ESPECÍFICOS

Implementar la topología de red con el software emulador Packet Tracer.

Configurar los dispositivos de red con los parámetros básicos de identificación y seguridad.

Conocer los procesos de enrutamiento con los protocolos RIPV2 y OSPF.

Verificar la conectividad y funcionamiento de la red.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. DEFINICIÓN DEL PROBLEMA

3.1.1. ESCENARIO 1

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

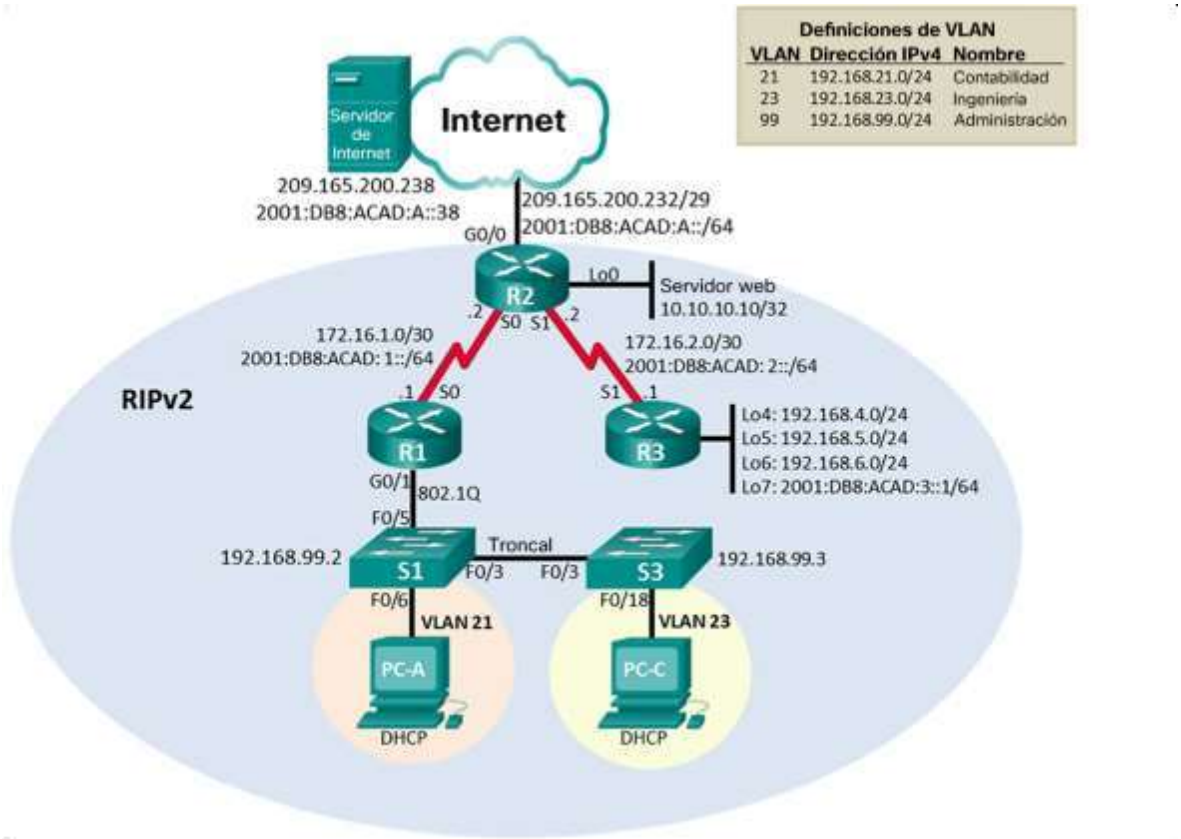


Figura 1 - Topología de Red propuesta del Escenario 1

3.1.2. 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.

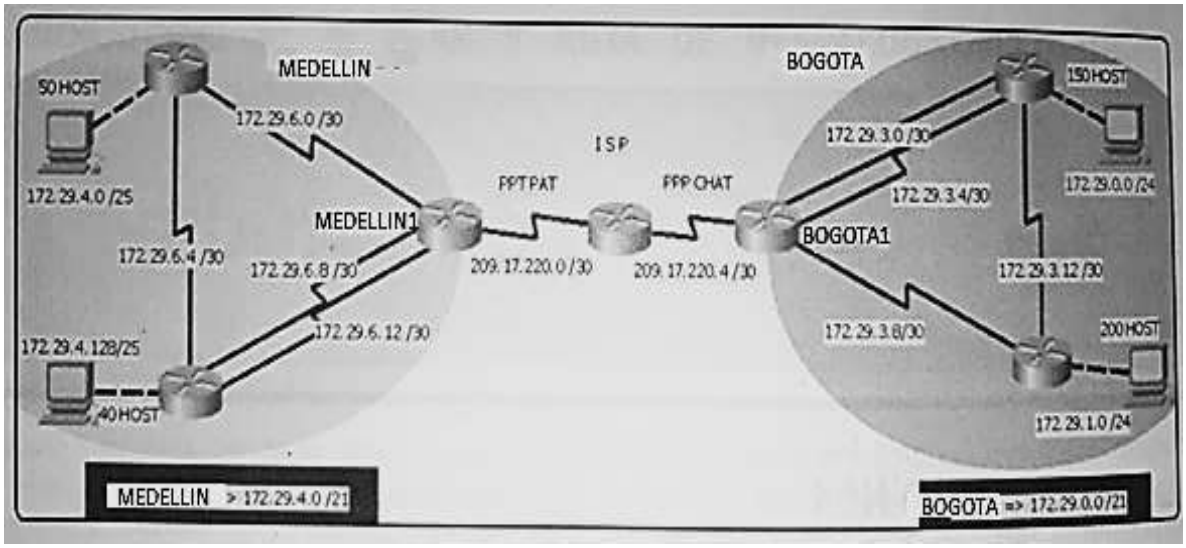


Figura 2 - Topología de Red propuesta para Escenario 2

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

Los routers 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.

3.2. JUSTIFICACIÓN

Estos son Escenarios de implementación de redes LAN que van a demostrar las competencias y habilidades practicas que he adquirido durante el proceso de formación, desde la creación de prototipos de redes LAN con la herramienta packet tracer, la configuración de los host hasta la identifiacion de fallas y visualización de conectividad y configuraciones realizadas.

4. DESARROLLO DE LOS DOS ESCENARIOS

4.1. ESCENARIO 1

Parte 1. Inicializar dispositivos

Se crea la topología en Packet Tracer utilizando dos pcs, dos switchs cisco 2960, tres router cisco 1941 y un servidor de internet. Eliminamos la configuración de inicio y la configuración de VLANS de los dispositivos y volvemos a recargar por defecto.

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.

Tabla 1 - Comandos para inicializar y volver a cargar los routers y los switches

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

Parte 2: Configurar los parámetros básicos de los dispositivos

La configuración básica es muy importante, aquí se se identifica estructura lógica de la red para cada uno de los host. Se nombra los dispositivos, se crean las contraseñas de acceso tanto para usuario como para administrador con privilegios y se crean las rutas predeterminadas.

Paso 1: Configurar la computadora de Internet

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

Tabla 2 - Comandos para configurar parámetros básicos de la computadora de Internet

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::1/64

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 - Comandos para configurar parámetros básicos del R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#Service password-encryption
Mensaje MOTD	R1(config)#banner motd “Se prohíbe el acceso no autorizado.”
Interfaz S0/1/0	Interface serial 0/1/0 Establezca la descripción R1(config)#interface s0/1/0 R1(config-if)#description Enlace al R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#Ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#Ipv6 address 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#Clock rate 128000 Activar la interfaz R1(config-if)#No shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/1/0 R1(config-if)#Ip route 0.0.0.0 0.0.0.0 172.16.1.2 Configurar una ruta IPv6 predeterminada de S0/1/0 R1(config-if)#Ipv6 route ::/0 2001:DB8:ACAD:1::2

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4 - Comandos para configurar parámetros básicos del R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#No ip domain-lookup

Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#Service password-encryption
Mensaje MOTD	R2(config)#banner motd “Se prohíbe el acceso no autorizado.”
Interfaz S0/1/0	Establezca la descripción R2(config)#interface s0/1/0 R2(config-if)#Description Enlace al R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config-if)#Ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)# Ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz R2(config-if)#No shutdown

Interfaz S0/1/1	Establecer la descripción R2(config)#interface s0/1/1 R2(config-if)#Description Enlace a R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#Ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#Ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config-if)#No shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config)#interface s0/1/1 R2(config-if)#Description Enlace a Servidor Internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. R2(config-if)#Ip address 2001:DB8:ACAD:A::1/64 Activar la interfaz R2(config-if)#No shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config)#interface loopback 0 R2(config-if)#Description Enlace a servidor web simulado Establezca la dirección IPv4. R2(config-if)#Ip address 10.10.10.11 255.255.255.255

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config-if)#Ip route 0.0.0.0 0.0.0.0 209.165.200.238 Configure una ruta IPv6 predeterminada de G0/0. R2(config-if)#Ipv6 route ::/0 2001:DB8:ACAD:A::38

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 - Comandos para configurar parámetros básicos del R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#No ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#Service password-encryption
Mensaje MOTD	R3(config)#banner motd “Se prohíbe el acceso no autorizado.”

Interfaz S0/1/1	Establecer la descripción R3(config)#interface s0/1/1 R3(config-if)#Description Enlace a R2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config-if)#Ip addres 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#Ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz R3(config-if)#No shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#Interface loopback 4 R3(config-if)#Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#Interface loopback 5 R3(config-if)#Ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#Interface loopback 6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#Interface loopback 7 R3(config-if)#Ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6 - Comandos para configurar parámetros básicos del S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#No ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#Service password-encryption
Mensaje MOTD	S1(config)#banner motd “Se prohíbe el acceso no autorizado.”

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7 - Comandos para configurar parámetros básicos del S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#No ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login

Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#Service password-encryption
Mensaje MOTD	S3(config)#banner motd “Se prohíbe el acceso no autorizado.”

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8 - Comandos para verificar la conectividad entre Routers y del PC de Internet al Gareway predeterminado

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/5 ms
R2	R3, S0/1/1	172.16.2.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=1ms TTL=255

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

Para verificar la conectividad de los equipos utilizamos el comando ping especificando la dirección ip del host al cual queremos conocer si recibe los paquetes.

```
R1#ping 172.16.1.2

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

Figura 3 - Conectividad de R1 a R2 S0/1/0

```
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/5/13 ms
```

Figura 4 - Conectividad de R2 a R3 S0/1/1

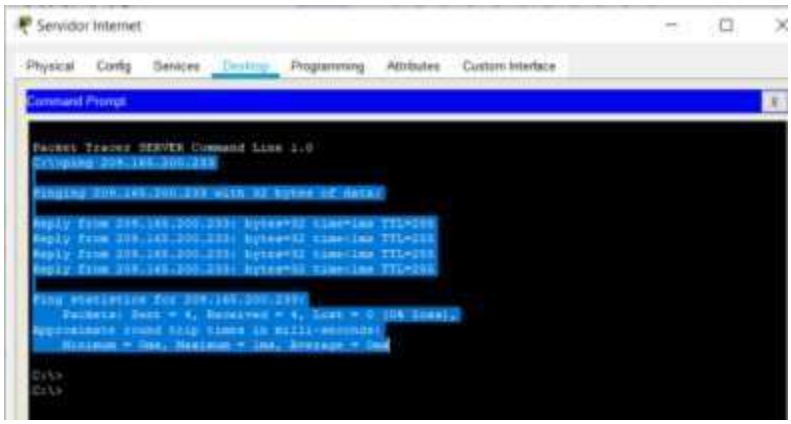


Figura 5 - Conectividad de PC internet a Gateway predeterminado

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 crean las VLAN en los S1 y S2, esto logra crear una estructura identificativa en la red para que un administrador de redes pueda organizar de una manera mas eficiente la red, se especifican los puertos de acceso y se fuerza el enlace troncal a puertos especificados.

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:
Tabla 9 - Configurar la seguridad del S1, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config)#vlan 23 S1(config-vlan)#name ingenieria S1(config)#vlan 99 S1(config-vlan)#name administracion

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native S1(config)#interface fastethernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk allowed vlan all
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native S1(config)#interface fastethernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switch trunk allowed vlan all
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config-if-range)#interface range fastethernet 0/1-2, f0/4-5, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface fastethernet 0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range fastethernet 0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10 - Configurar la seguridad del S3, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#interface vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native S3(config)#interface f0/3 S3(config-if)#switch port mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#switchport trunk allowed vlan all
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switch port mode access

Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface f0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 - Configurar el routing entre VLAN en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad R1(config-subif)#description LAN de contabilidad Asignar la VLAN 21 R1(config)#interface gigabitethernet 0/1.1 R1(config-subif)#encapsulation dot1q 21 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config-subif)#description LAN de Ingenieria Asignar la VLAN 23 R1(config-subif)#interface gigabitethernet 0/1.2 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/1.2, changed state to up R1(config-subif)#encapsulation dot1q 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0

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

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12 - Verificar la conectividad entre los switches y el R1

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

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

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Con el protocolo de routing dinamico creamos mas seguridad en la red y determinamos cuales son las rutas por las que pueden pasar los paquetes.

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 - Configurar el protocolo de routing dinámico RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.99.0

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

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 - Configurar el protocolo de routing dinámico RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.10
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:
Tabla 15 - Configurar el protocolo de routing dinámico RIPv2 en R3

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

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

Paso 4: Verificar la información de RIP

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

Tabla 16 - Comandos para verificar la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Debug ip rip

Tabla 17 - Verificación visual de información RIP

Comandos para verificación de información de RIP – R1

Figura 6 - Verificación de RIP comando show ip protocols

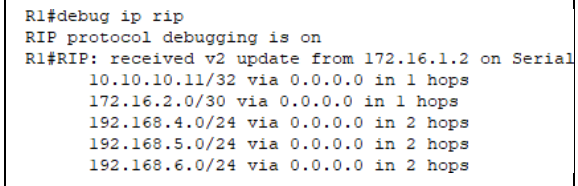


Figura 7 - Comando debug ip rip que muestra la configuración en ejecución

Figura 8 - Comando show ip route que muestra las rutas RIP

Parte 5: Implementar DHCP y NAT para IPv4

Se configura el conjunto de direcciones ip que vamos a excluir porque ya se tienen reservadas bien sea como puertas de enlace o asignadas a ciertos dispositivos de forma estatica, también se crea un conjunto de direcciones ip que los host configurados con DHCP pueden seleccionar automáticamente. Se crea la NAT para poder tener conectividad a través de un servidor virtual que se crea en el R1 a través de listas de control de acceso.

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 - Comandos para implementar el servidor DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.99.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.99.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#

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

La configuración del R2 incluye las siguientes tareas:

Tabla 19 - Comandos para configurar la NAT en el R2

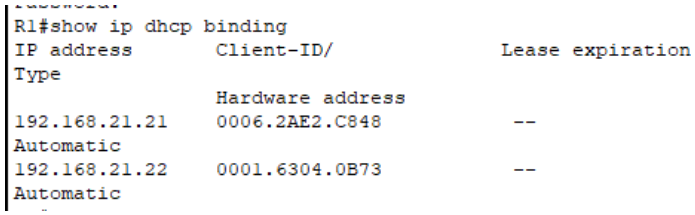
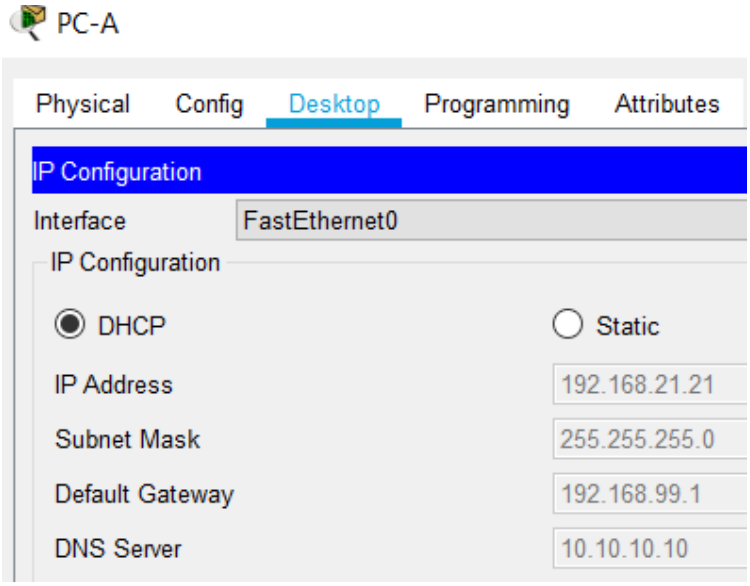
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Nota: Packet tracer no tiene habilitado este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local Nota: Packet tracer no tiene habilitado este comando
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#

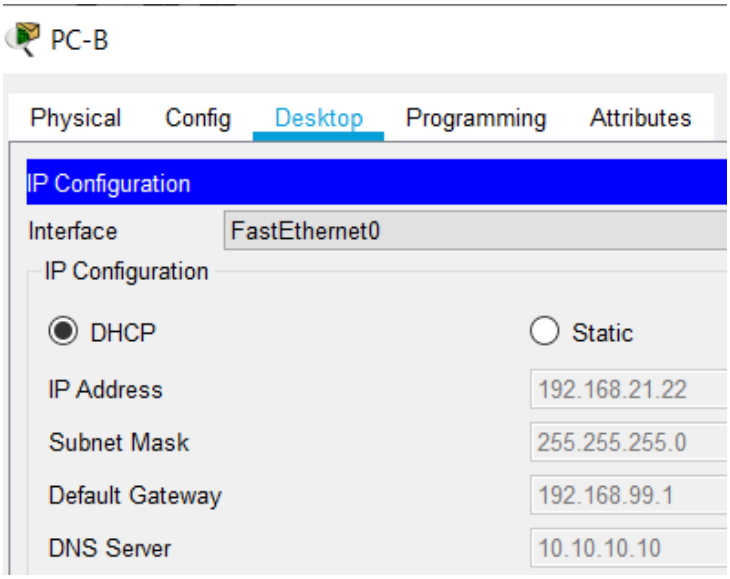
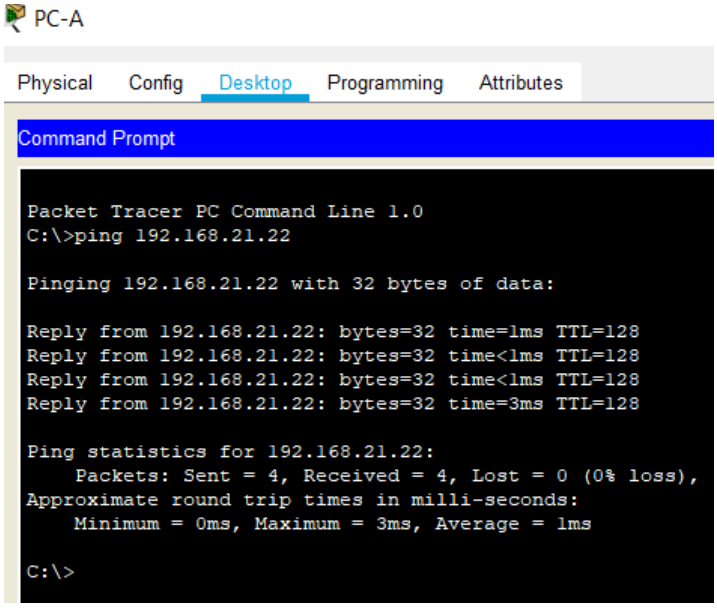
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 20 - Comandos para verificar la configuración DHCP y la NAT estatica

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 9 - Comando show ip dhcp binding que muestra la configuración DHCP*  *Figura 10 - Verificación DHCP en PC-A*

Verificar que la PC-B haya adquirido información de IP del servidor de DHCP	 *Figura 11 - Verificación DHCP en PC-B*
Verificar que la PC-A pueda hacer ping a la PC-B Nota: Quizá sea necesario deshabilitar el firewall de la PC.	 *Figura 12 - Ping de PC-A a PC-B*

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

Parte 6: Configurar NTP

Se configura el reloj en un dispositvo que va actuar como servidor y los demás equipos que actúan como clientes toman esta configuración para tener todos los equipos de la red sincronizados con el horario y fecha.

Tabla 21 - Comandos para configurar el NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 mar 05 2016 R2#show clock 9:0:17.327 UTC Sat Mar 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 1 16 1 2.00 0.00 0.00 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1# Figura 1 - Verificación configuración NTP

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

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

Se crean las listas de control de acceso, a través de estas podemos conectamos de forma remota utilizando telnet.

Tabla 22 - Comandos para restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms S1# Figura 2 - Verificiación conexión de S1 a 192.168.21.1 R2#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5) Figura 3 - Verificación de funcionamiento de la ACL de R2 a 192.168.21.1

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

Tabla 23 - Comandos para verificar la lista de control de acceso

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#Show access list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters [número de lista o nombre]
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show access-list
¿Con qué comando se muestran las traducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations *

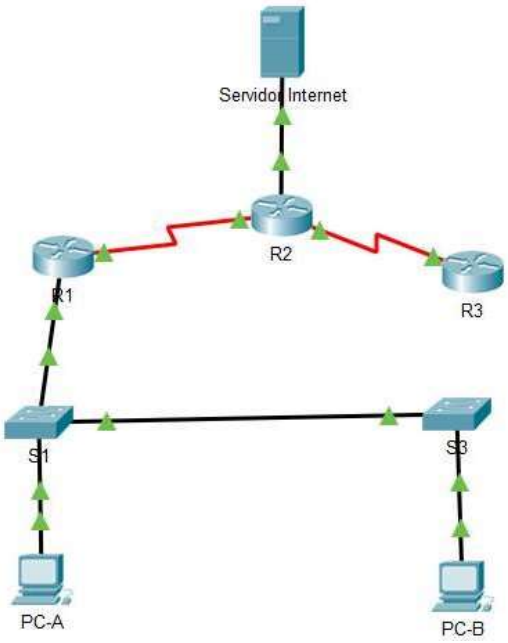


Figura 13 - Topología de red en funcionamiento de Escenario 1

4.2. ESCENARIO 2

Desarrollo
Como trabajo inicial se debe realizar lo siguiente.

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

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

Parte 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.
b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.
c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

Se realiza lo topología en packet tracer simulando la conexión entre dos ciudades Medellin y Bogota, conectadas a través de un ISP, se utiliza 6 PCs y siete Router Cisco 1941, se crean las configuraciones básicas de los dispositivos asignando nombre y configurando contraseñas de acceso a usuario y administrador con privilegios.

Paso 1. Se realiza la configuración básica de los dispositivos

Router ISP

Configuración básica

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#enable secret cisco
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
```

ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#banner motd "Acceso no autorizado"

Direccionamiento ip interface s0/1/1
ISP(config)#interface s0/1/1
ISP(config-if)#description Enlace a MEDELLIN 1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down

Direccionamiento ip interface s0/1/0
ISP(config-if)#interface s0/1/0
ISP(config-if)#description Enlace a BOGOTA 1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no shutdown

Router MEDELLIN1

Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#enable secret cisco
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#banner motd "Acceso no autorizado"

Configuración de ruta por defecto hacia ISP
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

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

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

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

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

Router MEDELLIN2

Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#enable secret cisco
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 15

MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#banner motd "Acceso no autorizado"

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

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

Router MEDELLIN3

Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#enable secret cisco
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#banner motd "Acceso no autorizado"

Direccionamiento ip interface s0/0/0
MEDELLIN3(config)#interface s0/0/0

MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown

Direccionamiento ip interface s0/1/0

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

Direccionamiento ip interface s0/1/1

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

Router BOGOTA1

Configuración básica

Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#enable secret cisco
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#banner motd "Acceso no autorizado"

Configuración de ruta por defecto hacia ISP

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

Direccionamiento ip interface s0/0/0

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

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

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

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

Router BOGOTA2

Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#enable secret cisco
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login

BOGOTA2(config-line)#exit
BOGOTA2(config)#banner motd "Acceso no autorizado"

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

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

Router BOGOTA3

Configuración básica
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#enable secret cisco
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#banner motd "Acceso no autorizado"

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

Direccionamiento ip interface s0/0/0

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

Direccionamiento ip interface s0/1/1

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

Paso 2: Configuración enrutamiento con protocolo OSPF y declaración de red principal

Router ISP

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

Router MEDELLIN1

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

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

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

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

Router MEDELLIN2
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 1

Router MEDELLIN3
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1
00:11:47: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/1/1 from LOADING to FULL, Loading Done

MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 1

Router BOGOTA1
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 1
00:22:56: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/0/0 from LOADING to FULL, Loading Done

BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1

Router BOGOTA2
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1
00:30:43: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.13 on Serial0/1/0 from LOADING to FULL, Loading Done

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1
00:31:08: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/1 from LOADING to FULL, Loading Done

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

Router BOGOTA3
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1
00:25:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from LOADING to FULL, Loading Done

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1
00:26:21: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0 from LOADING to FULL, Loading Done

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1

Paso 3: Configuración de rutas estáticas en Router ISP

Ruta estatica hacia la red de Medellín y sumarización a 22
ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/1/1
ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/1/1

Ruta estatica hacia la red de Bogotá y sumarización a 22
ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/1/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/1/0

Parte 2: Tabla de Enrutamiento.

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

Se utilizan comandos como show ip route ospf y show ip protocols para verificar las tablas de enrutamiento.

Paso 1: Se realiza verificación de rutas a través de comandos show ip route ospf y show ip protocols.

```
ISP#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/128] via 209.17.220.6, 00:46:52, Serial0/1/0
O       172.29.3.4 [110/128] via 209.17.220.6, 00:46:52, Serial0/1/0
O       172.29.3.8 [110/128] via 209.17.220.6, 00:46:52, Serial0/1/0
O       172.29.3.12 [110/192] via 209.17.220.6, 00:46:52, Serial0/1/0
O       172.29.6.0 [110/128] via 209.17.220.2, 00:46:52, Serial0/1/1
O       172.29.6.4 [110/192] via 209.17.220.2, 00:46:52, Serial0/1/1
O       172.29.6.8 [110/128] via 209.17.220.2, 00:46:52, Serial0/1/1
O       172.29.6.12 [110/128] via 209.17.220.2, 00:46:52, Serial0/1/1
```

Figura 14 - Tabla de enrutamiento ISP

```
ISP#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:06:46
    172.29.3.14          110      00:06:45
    172.29.6.5           110      00:06:44
    172.29.6.14          110      00:06:45
    209.17.220.2         110      00:06:45
    209.17.220.5         110      00:06:44
    209.17.220.6         110      00:06:45
  Distance: (default is 110)
```

Figura 15 - Tabla de enrutamiento ISP

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

Figura 16 - Tabla de enrutamiento MEDELLIN1

```
MEDELLIN1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    209.17.220.0 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:04:52
    172.29.3.14          110      00:04:50
    172.29.6.5           110      00:04:49
    172.29.6.14          110      00:04:50
    209.17.220.2         110      00:04:50
    209.17.220.5         110      00:04:50
    209.17.220.6         110      00:04:51
  Distance: (default is 110)
```

Figura 17 - Tabla de enrutamiento MEDELLIN1

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

Figura 18 - Tabla de enrutamiento MEDELLIN2

```
MEDELLIN2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.0 0.0.0.3 area 1
    172.29.4.0 0.0.0.127 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13           110      00:08:06
    172.29.3.14           110      00:08:04
    172.29.6.5            110      00:08:03
    172.29.6.14           110      00:08:04
    209.17.220.2          110      00:08:04
    209.17.220.5          110      00:08:04
    209.17.220.6          110      00:08:05
  Distance: (default is 110)
```

Figura 19 - Tabla de enrutamiento MEDELLIN2

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

Figura 20 - Tabla de enrutamiento MEDELLIN3

```
MEDELLIN3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    172.29.4.128 0.0.0.127 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:08:55
    172.29.3.14          110      00:08:53
    172.29.6.5           110      00:08:52
    172.29.6.14          110      00:08:53
    209.17.220.2         110      00:08:53
    209.17.220.5         110      00:08:53
    209.17.220.6         110      00:08:54
  Distance: (default is 110)
```

Figura 21 - Tabla de enrutamiento MEDELLIN3

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

Figura 22 - Tabla de enrutamiento BOGOTA1

```
BOGOTA1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.4 0.0.0.3 area 1
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:10:01
    172.29.3.14          110      00:09:59
    172.29.6.5           110      00:09:58
    172.29.6.14          110      00:09:59
    209.17.220.2         110      00:09:59
    209.17.220.5         110      00:09:59
    209.17.220.6         110      00:09:59
  Distance: (default is 110)
```

Figura 23 - Tabla de enrutamiento BOGOTA1

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

Figura 24 - Tabla de enrutamiento BOGOTA2

```
BOGOTA2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.12 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    172.29.1.0 0.0.0.255 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13           110      00:12:16
    172.29.3.14           110      00:12:14
    172.29.6.5            110      00:12:14
    172.29.6.14           110      00:12:15
    209.17.220.2          110      00:12:15
    209.17.220.5          110      00:12:14
    209.17.220.6          110      00:12:15
  Distance: (default is 110)
```

Figura 25 - Tabla de enrutamiento BOGOTA2

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

BOGOTA3#
```

Figura 26 - Tabla de enrutamiento BOGOTA3

```
ISP#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13           110      00:14:07
    172.29.3.14           110      00:14:07
    172.29.6.5            110      00:14:06
    172.29.6.14           110      00:14:06
    209.17.220.2          110      00:14:06
    209.17.220.5          110      00:14:06
    209.17.220.6          110      00:14:06
  Distance: (default is 110)
```

Figura 27 - Tabla de enrutamiento BOGOTA3

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Tabla 24 - Interfaces a deshabilitar la propagación del protocolo OSPF

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

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

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

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

BOGOTA3(config-router)#passive-interface s0/1/0
07:17:26: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

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

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

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

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

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

Parte 4: Verificación del protocolo OSPF.

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

Paso 1: Se realiza verificación de rutas a través de comandos show ip route ospf y show ip protocols.

Figura 28 - Verificación de rutas OSPF en MEDELLIN1

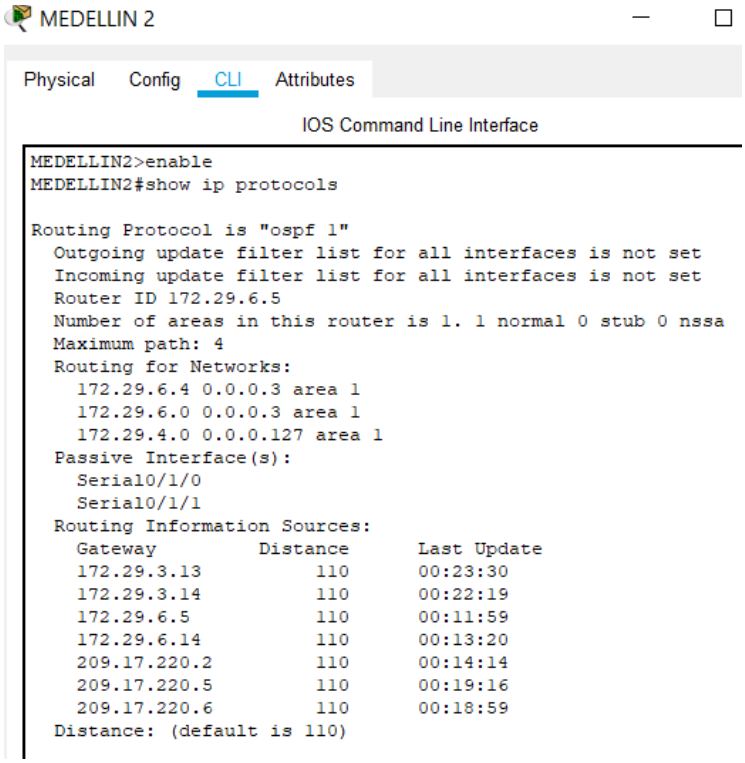


Figura 29 - Verifiación de rutas OSPF en MEDELLIN2

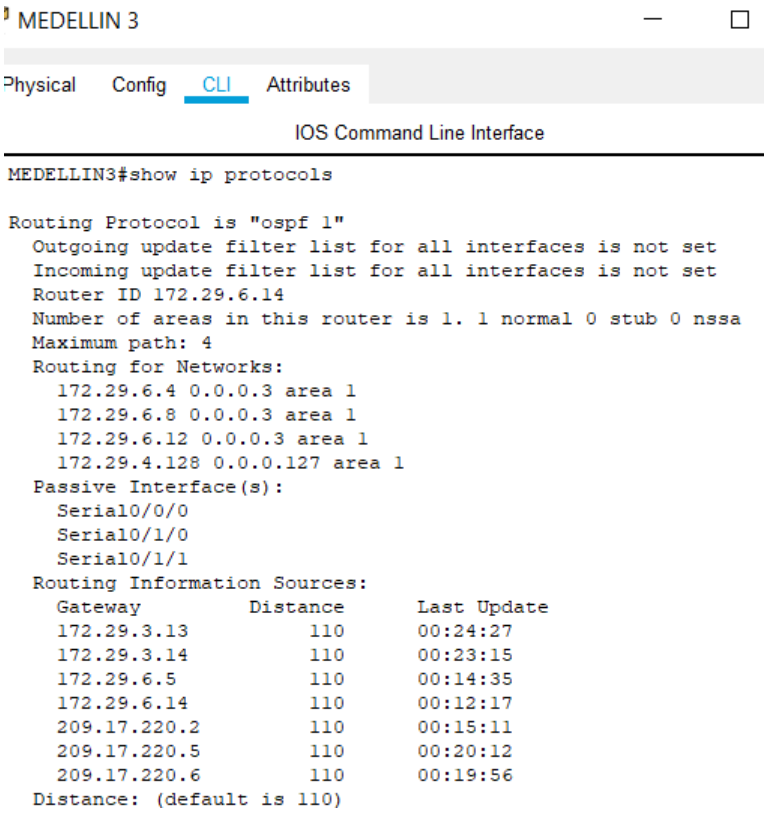


Figura 30 - Verifiación de rutas OSPF en MEDELLIN3

Figura 31 - Verifiación de rutas OSPF en BOGOTA1

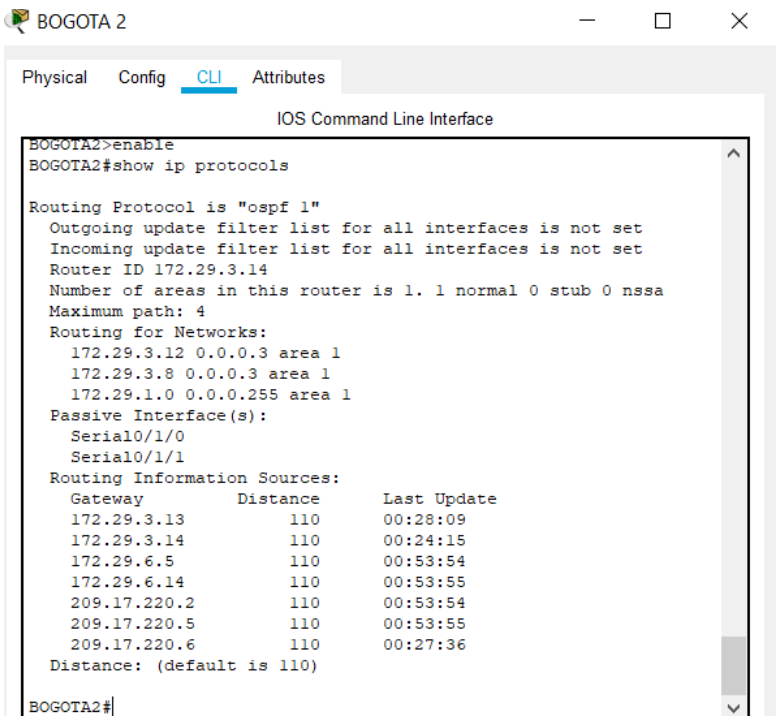


Figura 32 - Verifiación de rutas OSPF en BOGOTA2

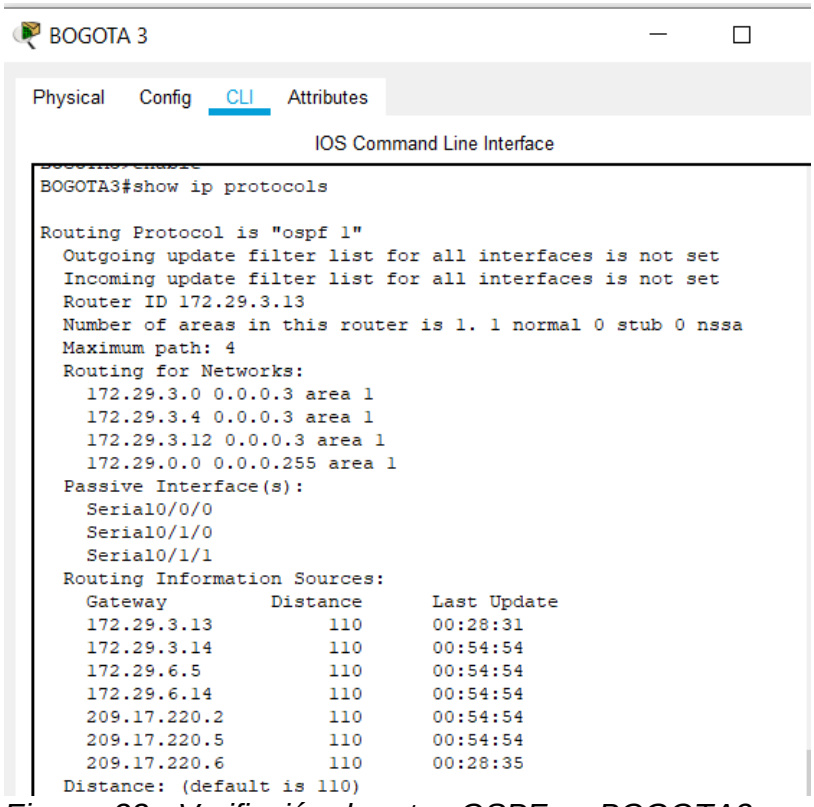


Figura 33 - Verifiación de rutas OSPF en BOGOTA3

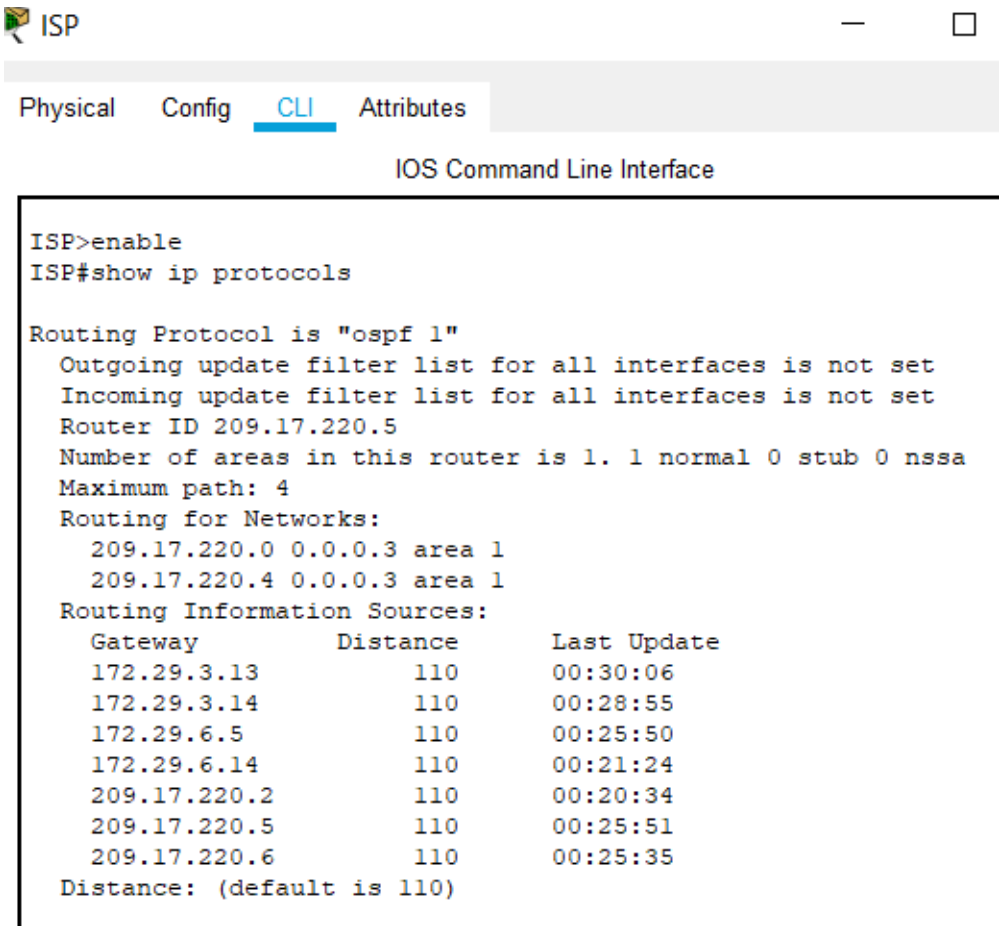


Figura 34 - Verifiación de rutas OSPF en ISP

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Paso 1. Se habilita el método de encapsulamiento PPP

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

Encapsulamiento en BOGOTA1
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#encapsulation ppp

BOGOTA1(config-if)#no shutdown

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

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

Paso 2. Habilitación autenticación PAP con el enlace MEDELLIN1

Configuración PAP en ISP con enlace MEDELLIN1
ISP(config)#username medellin1 secret medellin1
ISP(config)#interface s0/1/1
ISP(config-if)#ppp authentication pap
09:18:23: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached
ISP(config-if)#ppp pap sent-username isp password isp

Configuración PAP en MEDELLIN1 con enlace ISP
MEDELLIN1(config)#username isp secret isp
MEDELLIN1(config)#interface s0/0/0
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username medellin1 password medellin1

Paso 3. Habilitación autenticación CHAT de PPP entre BOGOTA1 y el ISP

Configuración CHAP de PPP en ISP con BOGOTA1
ISP(config)#username bogota1 secret bogota1
ISP(config)#interface s0/1/0
ISP(config-if)#ppp authentication chap

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

Configuración CHAP de PPP en BOGOTA1 con ISP
BOGOTA1(config)#username isp secret isp
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#end

Parte 6: Configuración de PAT.

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

Paso 1. Configuración NAT en MEDELLIN1
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside source list HOST interface s0/1/0 overload
MEDELLIN1(config)#interface s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#interface s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#end

Paso 2. Configuración NAT en BOGOTA1

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

Paso 3. Verificación ping entre MEDELLIN 2 Y MEDELLIN 1

Figura 35 - Verifiación conectividad entre MEDELLIN2 y MEDELLIN1

Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes Lan.
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Paso 1. Configuracion DHCP en router MEDELLIN2

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

Habilitar el paso de mensaje broadcast hacia la ip del router MEDELLIN2
MEDELLIN3(config)#interface g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5

Paso 2. Configuracion DHCP en Router BOGOTA2

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

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

Habilitar el paso de mensaje broadcast hacia la ip del router BOGOTA2
BOGOTA3(config)#interface g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.14

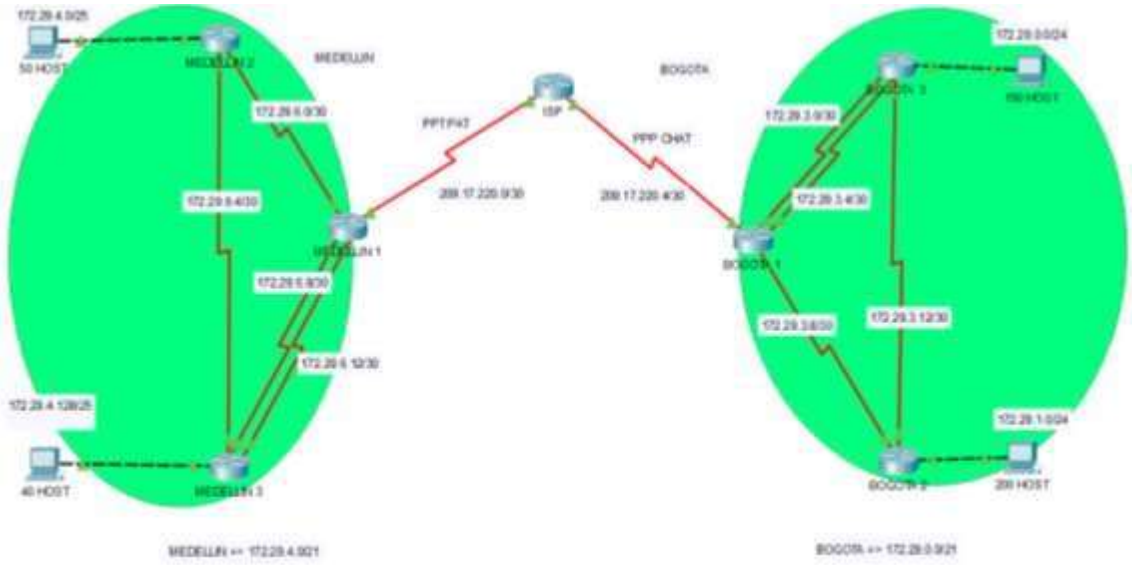


Figura 36 - Topología de red creada Escenario 2

5. CONCLUSIONES

Con los conocimientos adquiridos en los dos modulos del curso de profundización Cisco y con las actividades practicas realizadas en packet tracer se logro implementar la topología de red de los dos escenarios propuestos. Se utilizaron los comandos de verificación de conectividad y verificación de la configuración de cada uno de los parámetros implementados en los dispositivos de routing.

Con los escenarios desarollados en packet tracer se demuestra las habilidades adquiridas y desarrollas en cada una de las etapas del conocimiento de redes, se enfatiza el papel que debe realizar un administrador de red para lograr diseñar, implementar y verificar el funcionamiento de una red LAN y WAN.

Las competencias laborales que el desarrollo de este diplomado de profundización de Cisco puede lograr es asombroso, ya que abre una visión como Ingeniero de Sistemas no solo a la administración de una red LAN sino también a llevar mas alla de lo esperado, me he proyectado con la visión no solo de administrar una red sino también el desarrollar aplicaciones de gestión de información a través de los insumos que puede ofrecer la red.

6. BIBLIOGRAFÍA

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1lhgCT9VCtl_pLtPD9

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgOyjWeh6timi_Tm

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3