EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ÁNGEL DAVID BARCELÓ MORALES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
PROGRAMA DE INGENIERÍA DE SISTEMAS
BARRANQUILLA
2020

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ÁNGEL DAVID BARCELÓ MORALES

INFORME

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

TUTOR

HÉCTOR JULIÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

PROGRAMA DE INGENIERÍA DE SISTEMAS

BARRANQUILLA

2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Barranquilla mayo 23 del 2020

DEDICATORIA

Este trabajo final lo dedico primeramente a DIOS quien me dio la sabiduría, la salud y el entendimiento para desarrollar cada una de las actividades propuestas durante todo el curso, segundo a mi esposa e hijos que siempre estuvieron allí pendientes dándome fuerzas y ánimo para que no me rindiera aun en los momentos más difíciles, tercero a mis hermanos, y amigos quienes siempre con sus palabras me impulsaban a seguir adelante, gracias porque sin sus consejos no podría haberlo hecho solo. Dios los bendiga enormemente.

AGRADECIMIENTOS

Este trabajo es un esfuerzo en el cual tutores, compañeros y amigos participaron opinando, corrigiendo y brindando su apoyo de acuerdo a su experiencia y conocimiento, la cual fue de mucha ayuda para la presentación de este trabajo. Quiero agradecer de manera muy especial a mi tutor Héctor Julián Parra quien pacientemente y de forma diligente me brindó su apoyo y comprensión sobre todo en los momentos en los cuales pase por dificultades de salud, ya que supo entender dicha situación y siempre estuvo dispuesto a brindarme su ayuda y asesoría.

A mi compañero Jorge Dauss, quien trabaja conmigo en la misma empresa, su explicaciones y conocimientos sobre redes me ayudaron a entender y sacar adelante este curso infinitas gracias y que Dios los bendiga siempre para que sigan ayudando a otras personas.

CONTENIDO

1. INTRODUCCIÓN 11
2. OBJETIVOS 12
2.1. OBJETIVO GENERAL 12
2.2. OBJETIVOS ESPECÍFICOS 12
3. PLANTEAMIENTO DEL PROBLEMA 13
3.1. DEFINICIÓN DEL PROBLEMA 13
3.2. JUSTIFICACIÓN 13
4. MARCO TEÓRICO 14
5. MATERIALES Y METODOS 17
5.1. MATERIALES 17
5.2. METODOLOGÍA 17
6. DESARROLLO DEL PROYECTO 18
6.1. ANALISIS DEL DESARROLLO DEL PROYECTO 18
6.2. CRONOGRAMA 18
7. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES 19
7.1. ESCENARIO 1 19
Parte 1: Inicializar dispositivos 20
Parte 2: Configurar los parámetros básicos de los dispositivos 20
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 30
Parte 4: Configurar el protocolo de routing dinámico RIPv2 35
Parte 5: Implementar DHCP y NAT para IPv4 38
Parte 6: Configurar NTP 43
Parte 7: Configurar y verificar las listas de control de acceso (ACL) 44
7.2. ESCENARIO 2 47
Parte 1: Configuración del enrutamiento 51
Parte 2: Tabla de Enrutamiento 57
Parte 3: Deshabilitar la propagación del protocolo OSPF 61
Parte 4: Verificación del protocolo OSPF 62
Parte 5: Configurar encapsulamiento y autenticación PPP 67
Parte 6: Configuración de PAT 68
Parte 7: Configuración del servicio DHCP 70
CONCLUSIÓN 73
REFERENCIA BIBLIOGRÁFICA 74

LISTA DE FIGURAS

Pag.

Figura1. Topología de la Red. Fuente Propia 19

Figura 2. Topología de red. Fuente propia 47

Figura 3. Topología de la red en funcionamiento 51

Figura 4. Verificación de Enrutamiento Bogota1 57

Figura 5. Verificación de Enrutamiento medellin1 58

Figura 6. Verificar Balanceo de carga Bogota3 59

Figura 7. Verificar Balanceo de carga Medellin3 59

Figura 8. Demostración puntos C,D,E,F 60

Figura 9. Deshabilitar propagación del protocolo OSPF 62

Figura 10. Verificación del protocolo OSPF Medellin1 62

Figura 11. Verificación del protocolo OSPF Medellin2 63

Figura 12. Verificación del protocolo OSPF Medellin3 63

Figura 13. Verificación del protocolo OSPF Bogota1 64

Figura 14. Verificación del protocolo OSPF Bogota2 64

Figura 15. Verificación del protocolo OSPF Bogota3 65

Figura 16. Verificación base de datos OSPF Bogota1 66

Figura 17. Verificación base de datos OSPF Medellin1 67

Figura 18. Ping entre Medellin2 y Medellín 1 70

Figura 19. Configuración DHCP PC0 71

Figura 20. Configuración DHCP PC2 72

LISTA DE TABLAS

Pag.

Tabla 1. Tareas y Comandos de IOS 20
Tabla 2. Configuración Computadora de Internet. 20
Tabla 3. Configuración Router 1. 21
Tabla 4. Configuración Router 2. 23
Tabla 5. Configuración Router 3. 26
Tabla 6. Configuración Switch 1. 28
Tabla 7. Configuración Switch 3. 28
Tabla 8. Verificar conectividad de la red. 30
Tabla 9. Tareas del Switch 1. 31
Tabla 10. Tareas del Switch 3. 32
Tabla 11. Tareas del Router 1. 34
Tabla 12. Verificación de Conectividad. 35
Tabla 13. Configurar RIPV2 en el Router 1. 36
Tabla 14. Configurar RIPV2 en el Router 2. 36
Tabla 15. Configurar RIPV2 en el Router 3 37
Tabla 16. Verificar Información de RIP. 38
Tabla 17. R1 como servidor de DHCP para las VLAN 21 y 23. 38
Tabla 18. Configurar la NAT estática y dinámica en el R2. 40
Tabla 19. Verificar el protocolo DHCP y la NAT estática. 42
Tabla 20. Configuración de NTP 43
Tabla 21. Restringir el acceso a las líneas VTY en el R2. 44
Tabla 22. Comando CLI. 45
Tabla 23. Asignación de Direcciones IP. Fuente propia. 51
Tabla 24. Interfaces de Los routers. Fuente propia. 61

GLOSARIO

ACCESS POINT: Es un dispositivo que habilita la conexión inalámbrica. El módem que le ofrece su proveedor de Internet, es un Access Point.

DATA CENTER: Es el cerebro de la infraestructura tecnológica, agrupa todos los equipos y servidores esenciales para su buen funcionamiento

DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

FIREWALL: Es un dispositivo que le brinda seguridad a su red y protege a sus usuarios. Funciona como una aduana que revisa todo lo que entra y sale de su red

ROUTER: Los switches conectan los dispositivos en una red, y los routers conectan diferentes redes. Son dispositivos que crean los caminos para que viajen los datos y eligen las mejores rutas para que la información se transmita de forma rápida y segura.

SERVER Un servidor es una computadora con altos niveles de almacenamiento y procesamiento. En él, las organizaciones instalan y ejecutan sistemas y servicios como los de facturación, recursos humanos y aplicaciones de colaboración.

SNMP: el Protocolo simple de administración de redes (SNMP) es un estándar de red para almacenar y compartir información sobre dispositivos de red. SNMP facilita la gestión de la red, la resolución de problemas y el mantenimiento.

SWITCH: El switch es uno de los componentes fundamentales en el desarrollo de Internet. Funciona como lo hacían los conmutadores telefónicos: recibe paquetes de datos y los direcciona al destinatario correcto.

VLAN: una red de área local virtual (VLAN) es una red conmutada que está segmentada lógicamente por función, área o aplicación, independientemente de las ubicaciones físicas de los usuarios.

RESUMEN

En el presente trabajo se desarrollarán dos escenarios mediante el cual el estudiante a través del análisis y lo aprendido durante todo el curso aplicara las configuraciones correspondientes para el correcto funcionamiento de la red. En primera instancia realizará, la configuración de una red pequeña para que admita conectividad IPv4 e IPv6, en el segundo escenario aplicara el uso de OSPF como protocolo de enrutamiento, ambos escenerios permitiran al estudiante demostrar los conocimientos adquiridos durante el desarrollo del Diplomado de profundización CISCO.

PALABRAS CLAVE: Desactivar búsqueda DNS, Switch, Routers, Servidor HTTP, Networking, OSPF, RIP.

1. INTRODUCCIÓN

En el presente trabajo se realizarán las actividades concernientes a la prueba de habilidades practicas CCNA con el objetivo de identificar el grado de desarrollo de competencias y habilidades que el estudiante adquirió a lo largo del diplomado. Se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking. A continuación, se presentan dos escenarios en los cuales el estudiante realizara un informe documentando de forma detallada la solución correspondiente a cada etapa propuesta en los ejercicios.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Aplicar los conocimientos y habilidades adquiridas durante el desarrollo de las unidades del curso de CISCO por parte del estudiante con el fin de identificar y aplicar una solución práctica a los escenarios propuestos.

2.2. OBJETIVOS ESPECÍFICOS

- Identificar dispositivos para la construcción de la topología de red.
- Realizar configuración básica a dispositivos de comunicación. como Routers, Switch, Servidores. Etc.
- Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing. Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. DEFINICIÓN DEL PROBLEMA.

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.

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.

3.2. JUSTIFICACIÓN.

La dirección IP es el identificador perteneciente al protocolo IP (Internet Protocol), el cual es el sistema de direccionamiento IPv4 e IPv6 como versión más nueva y preparada para el futuro. Es un protocolo que opera en la capa de red y no orientado a la conexión, esto significa que la comunicación entre dos extremos de una red e intercambio de datos se puede hacer si un acuerdo previo. Es decir, el receptor transmite datos sin saber si el recetor está disponible, así que a este le llegaran cuando se encienda y esté conectado. Por otra parte, OSPF, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios.

Las herramientas que se brindan para la solución de problema son los routers, Switch, Servidores, redes, Pcs y el software para configuración de los dispositivos.

4. MARCO TEÓRICO

Para el mundo actual las redes de datos son de vital importancia para el desarrollo administrativo y tecnológico de cualquier sociedad o empresa, por tanto, el diseño e implementación de estas debe ser totalmente seguro, estable y eficiente.

Base teórica del simulador Packet Tracer. Cisco Packet Tracer es un programa de simulación de red de gran alcance que permite a los estudiantes a experimentar con el comportamiento de la red

La versión actual soporta un conjunto de Protocolos de capa de aplicación simulados, al igual que enrutamiento básico con RIP, OSPF, y EIGRP.. Aunque Packet Tracer provee una simulación de redes funcionales, utiliza solo un pequeño número de características encontradas en el hardware real corriendo una versión actual del Cisco IOS. Packet Tracer no es adecuado para redes en producción.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego haciendo clic sobre ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IOS e incluso funciona el "tab completion". Una vez completada la configuración física y lógica de la red, también se pueden hacer simulaciones de conectividad (pings, traceroutes) todo ello desde las mismas consolas incluidas.

Una de las grandes ventajas de utilizar este programa es que permite "ver" (opción "Simulation") cómo deambulan los paquetes por los diferentes equipos (switchs, routers, PCs), además de poder analizar de forma rápida el contenido de cada uno de ellos en las diferentes "capas"y "datos".

Base teórica del Direccionamiento y Subnetting:

El subnetting es una colección de direcciones IP que permiten definir el número de redes y de host que se desean utilizar en una subred determinada; el VLSM es una técnica que permite dividir subredes en redes más pequeñas pero la regla que hay que tener en consideración siempre que se utilice VLSM es que solamente se puede aplicar esta técnica a las direcciones de redes/subredes que no están siendo utilizadas por ningún host, VLSM permite crear subredes más pequeñas que se ajusten a las necesidades reales de la red (los ROUTERS que utilizan protocolos de enrutamiento ‘sin clase’ como RIPv2, EIGRP y OSPF pueden trabajar con un esquema de direccionamiento IP que contenga diferentes tamaños de mascara, no así los protocolos de enrutamiento ‘con

clase' RIPv1 que solo pueden trabajar con un solo esquema de direcciones IP, es decir una misma mascara para todas las subredes dentro de la RED-LAN) y por ultimo tenemos el CIDR(Resumen de Rutas) que es la simplificación de varias direcciones de redes o subredes en una sola dirección IP Patrón que cubra todo ese esquema de direccionamiento IP. Existen dos tipos de subnetting: estático y de longitud variable. El de longitud variable es el más flexible de los dos. Qué tipo de subnetting está disponible depende del protocolo de enrutamiento que se está usando; el enrutamiento IP nativo soporta sólo subnetting estático, lo mismo que el protocolo RIP. Sin embargo, RIP versión 2 soporta subnetting de longitud variable. Ver protocolos de enrutamiento para más detalles.

Base teórica VLSM: A medida que las subredes IP han crecido, los administradores han buscado formas de utilizar su espacio de direccionamiento con más eficiencia. Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes con muchos hosts. Para poder implementar VLSM, un administrador de red debe usar un protocolo de enrutamiento que brinde soporte para él. Los ROUTERS Cisco admiten VLSM con los protocolos de enrutamiento OSPF, IS-IS, EIGRP, RIPv2 y enrutamiento estático. VLSM permite que una organización o empresa utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM maximiza la eficiencia del direccionamiento y con frecuencia se la conoce como división de subredes en subredes. Los protocolos de enrutamiento con clase necesitan que una sola red utilice la misma máscara de subred. Por ejemplo, una red con la dirección de 192.168.187.0 puede usar sólo una máscara de subred, por ejemplo 255.255.255.0. 10 Un protocolo de enrutamiento que admite VLSM le confiere al administrador de red la libertad para usar distintas máscaras de subred para redes que se encuentran dentro de un sistema autónomo. La Figura muestra un ejemplo de cómo un administrador de red puede usar una máscara de 30 bits para las conexiones de red, una máscara de 24 bits para las redes de usuario e incluso una máscara de 22 bits para las redes con hasta 1000 usuarios

Base teórica de los Protocolos de Enrutamiento. Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento. Un protocolo de enrutamiento es la aplicación de un algoritmo de enrutamiento en el software o hardware. Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de

los diferentes ROUTERS de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados

a. Enrutamiento Estático. El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los ROUTERS toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red.

b. Enrutamiento Predeterminado. Es una ruta estática que se refiere a una conexión de salida o Gateway de "último recurso". El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0.

c. Enrutamiento Dinámico. Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

El protocolo de enrutamiento RIPv2 es un primer protocolo de enrutamiento sin clase. Si bien RIPv2 es un protocolo de enrutamiento apropiado para algunos ambientes, pierde popularidad cuando se le compara con protocolos de enrutamiento tales como EIGRP, OSPF e IS-IS, que ofrecen más funciones y son más escalables. [3] 11 Aunque puede ser menos popular que otros protocolos de enrutamiento, las dos versiones de RIP siguen siendo apropiadas para algunas situaciones. Si bien RIP carece de las capacidades de muchos protocolos posteriores, su simplicidad y amplia utilización en varios sistemas operativos lo convierten en un candidato ideal para las redes homogéneas más pequeñas, donde es necesaria la compatibilidad con varios fabricantes, especialmente dentro de los ambientes UNIX. Como RIPv1, RIPv2 es un protocolo de enrutamiento vector distancia

5. MATERIALES Y METODOS

5.1. MATERIALES.

Software de simulación (Packet Tracer), Tutoriales y manuales de configuración de Dispositivos cisco (Routers, Swictch, pcs, Servidores e)

5.2. METODOLOGÍA.

Para el desarrollo de esta actividad previamente se debe hacer Revisión de fuentes bibliográficas que ayudaran con la solución de los dos escenarios, luego se procederá a construir la topología de red con los dispositivos solicitados, se realiza la conexión de red entre los dispositivos, una vez estén conectados se procede con la configuración y parametrización, por último, se realiza las pruebas para verificar que la red está totalmente en funcionamiento.

6. DESARROLLO DEL PROYECTO

6.1. ANALISIS DEL DESARROLLO DEL PROYECTO

Al momento de configurar una red es importante establecer cuál es el alcance que va tener, que medidas de seguridad se van a implementar para que esta no sea vulnerada, también debemos conocer qué tipo de configuración y conectividad va a tener y que dispositivos son los adecuados para su correcto funcionamiento. Una vez implementada nuestra red y su configuración se deben realizar las pruebas pertinentes que permitan evaluar el rendimiento, funcionamiento y seguridad de las misma.

6.2. CRONOGRAMA.

Cronograma de Actividades			
Nombre Actividad	**Duración DIAS**	**Fecha Inicial**	**Fecha Final**
Realizar Introducción	1	10/05/2020	10/05/2020
formulación de Objetivos	1	11/05/2020	11/05/2020
Planteamiento del Problema	1	12/05/2020	13/05/2020
Justificación del problema	1	13/05/2020	13/05/2020
Marco Teóricos	2	13/05/2020	14/05/2020
Metodología del trabajo	1	10/05/2020	10/05/2020
Desarrollo de los Escenarios	4	10/05/2020	14/05/2020
Conclusiones y Bibliología	1	14/05/2020	14/05/2020

7. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

7.1. 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.

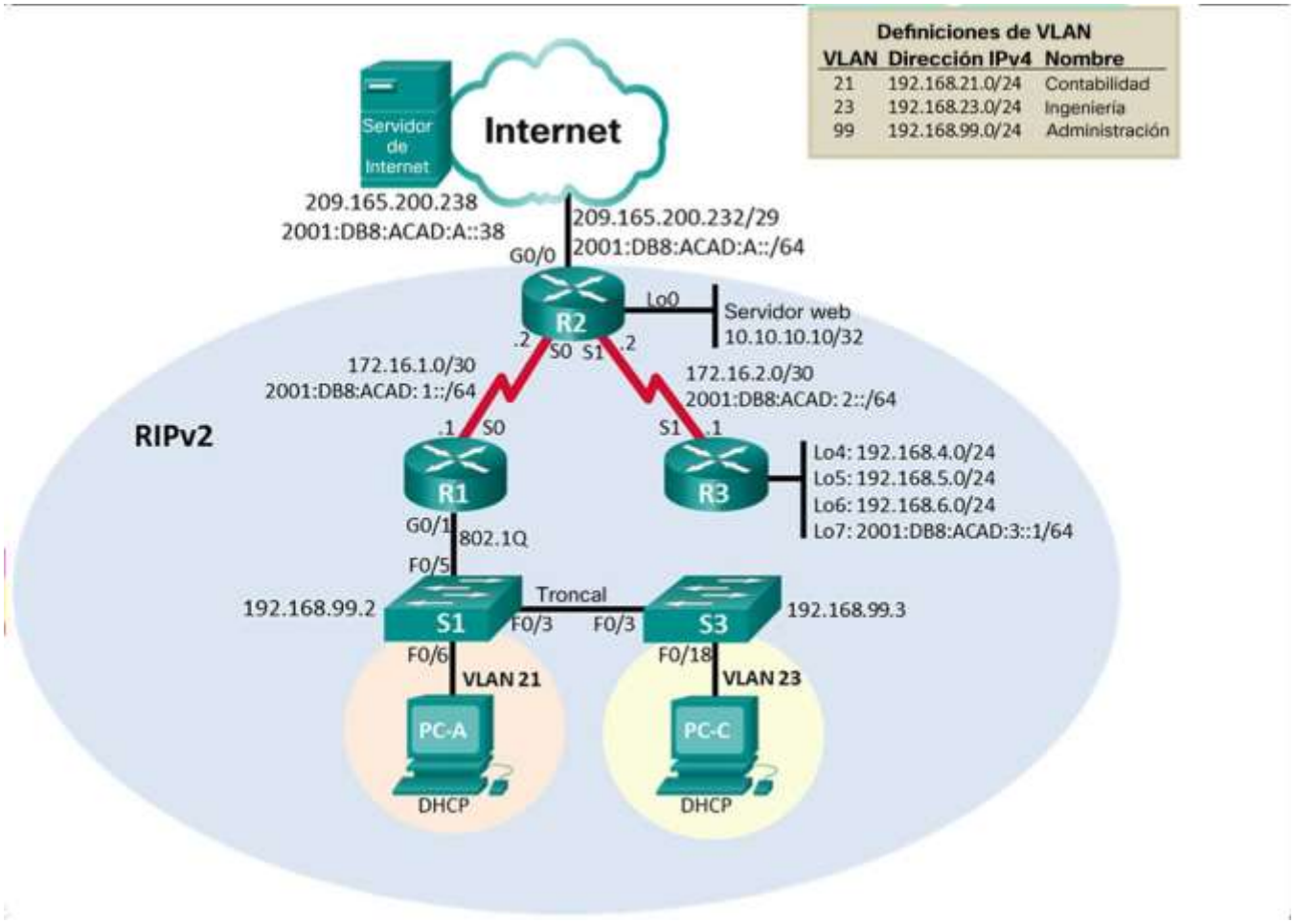


Figura1. Topología de la Red. Fuente Propia

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

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

Tabla 1. Tareas y Comandos de IOS

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

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

Tabla 2. Configuración Computadora de Internet

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Contraseña de acceso Telnet	Cisco R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd # Se prohibe el acceso no autorizado#

Interfaz S0/0/0	Establezca la descripción: R1(config-if)# description conectado 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::/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#clock rate 128000 Activar la interfaz: no shut down
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0: R/ Comando no soportado en mi versión de packet tracer. Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 unicast-routing R1(config)#ip route 0.0.0.0.0.0.0.0 s0/0/0

Tabla 3. Configuración Router 1.

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class
Contraseña de acceso a la consola	Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service passeord-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#banner motd #Se prohbe el acceso no autorizado.#

Interfaz S0/0/0	Establezca la descripción: R2(config-if)# int s0/0/0 R2(config-if)# description conectado al R1 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones: R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones: R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Establecer la frecuencia de reloj en 128000: R/: La frecuencia fue establecida en El R1 Activar la interfaz: R2(config-if)# no Shut down
Interfaz S0/0/1	Establecer la descripción: R2(config-if)# int s0/0/1 R2(config-if)# description conectado al 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. R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz: R2(config-if)# no Shut down

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config-if)# int g0/0 R2(config-if)# description conectado a 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)# ipv6 address 2001:DB8:ACAD:A:.1/64 Activar la interfaz: R2(config-if)# no shut down
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción: R2(config-if)# int loopback0 R2(config-if)# description Servidor Web Establezca la dirección IPv4. R2(config-if)# ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R/ Comando no soportado en mi versión de packet trace Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ipv6 unicast-routing R2(config)#ipv6 route ::/0 g0/0

Tabla 4. Configuración Router 2.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

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

Interfaz S0/0/1	Establecer la descripción: R3(config)# int s0/0/1 R3(config)#description conectado al R2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred: R3(config)#ip address 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)#ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz: R3(config)# no Shut down
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#int loopback4 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)#int loopback5 R3(config-if)#ip address 192.168.5.2 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#ip address 192.168.6.3 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ipv6 unicast-routing R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Configuración Router 3.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Tabla 6. Configuración Switch 1.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S3 Switch(config)#hostname S3

Contraseña de exec privilegiado cifrada	Class S3(config)#enable secret class
Contraseña de acceso a la consola	Cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	Cisco S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)#banner motd #Se prohbe el acceso no autorizado.#

Tabla 7. Configuración Switch 3.

Paso 7: Verificar la conectividad de la red

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

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

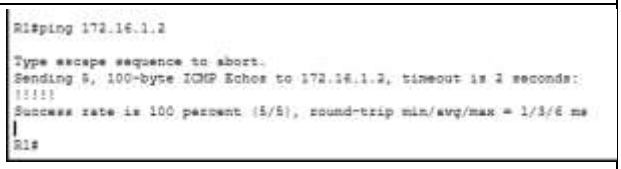
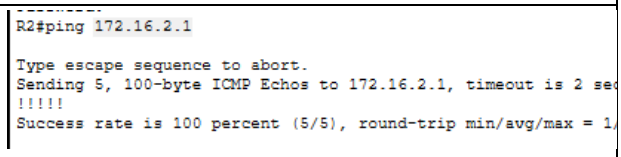
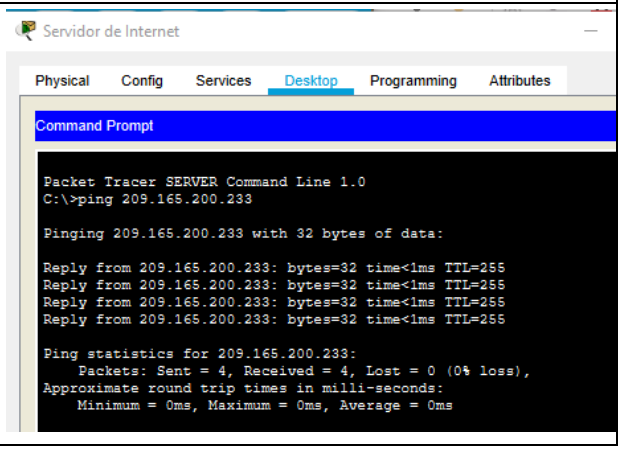
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	
R2	R3, S0/0/1	172.16.2.1	
PC de Internet	Gateway predeterminado	209.165.200.233	

Tabla 8. Verificar conectividad de la red.

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name Accounting S1(config-vlan)#vlan 23 S1(config-vlan)#name Engineering S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración
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)#int vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 9. Tareas del Switch 1.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config-vlan)#name Accouting S3(config-vlan)#vlan 23 S3(config-vlan)#name Engineering 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)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
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 nativa S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if-range)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 10. Tareas del Switch 3.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 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	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 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	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 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(config-subif)#int g0/1 R1(config-if)#no shut down

Tabla 11. Tareas del Router 1.

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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

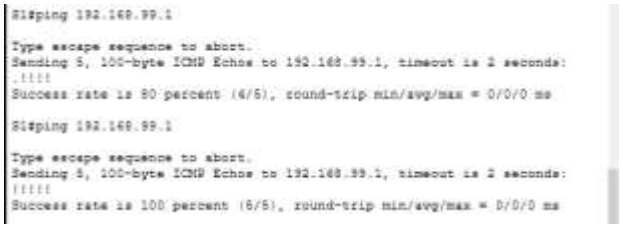
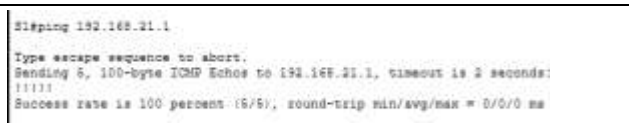
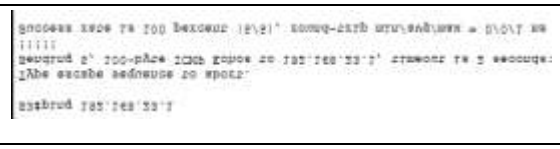
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	
S3	R1, dirección VLAN 99	192.168.99.1	
S1	R1, dirección VLAN 21	192.168.21.1	
S3	R1, dirección VLAN 23	192.168.23.1	

Tabla 12. Verificación de Conectividad.

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)# version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13. Configurar RIPV2 en el Router 1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 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(config-router)#passive-interface loopback 0

Desactive la sumarización automática.	R2(config-router)# no auto-summary

Tabla 14. Configurar RIPV2 en el Router 2

Paso 3: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15. Configurar RIPV2 en el Router 3

Paso 4: Verificar la información de RIP

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

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

Tabla 16. Verificar Información de RIP

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

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

Tabla 17. R1 como servidor de DHCP para las VLAN 21 y 23

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

La configuración del R2 incluye las siguientes tareas:

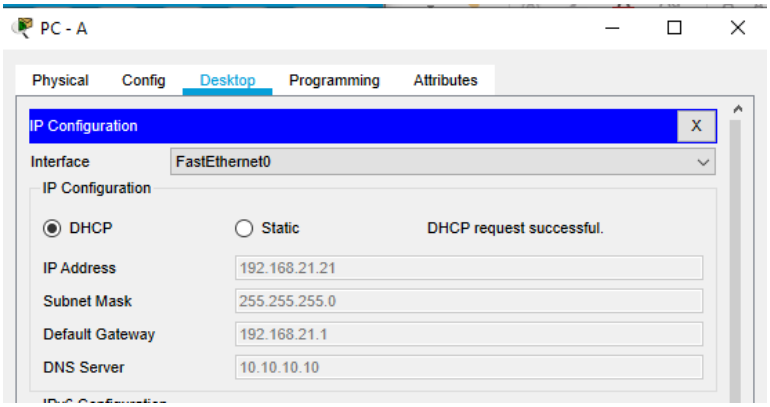
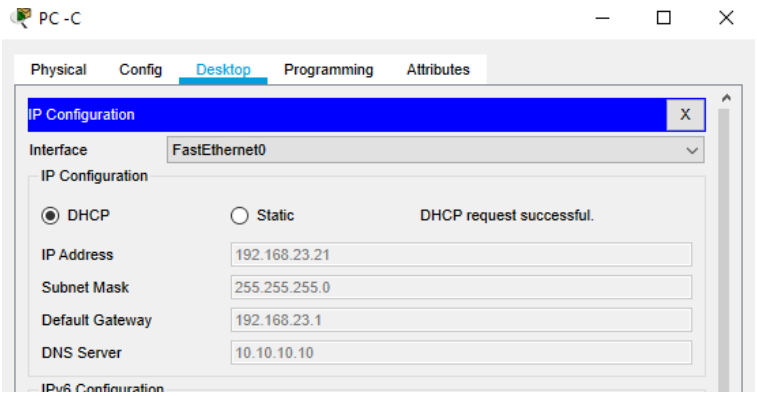
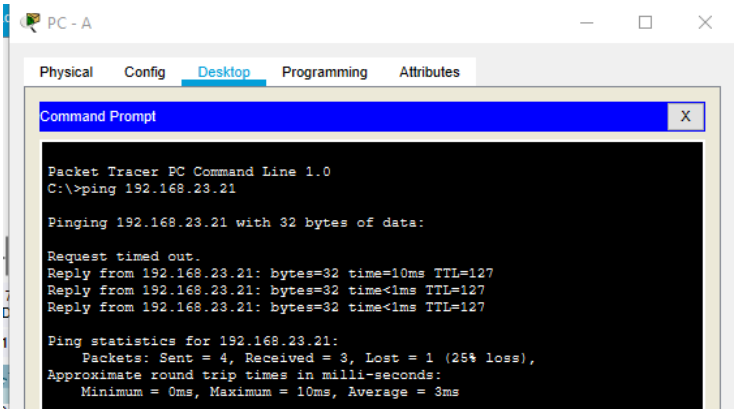
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237** 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(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside

Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 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 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233** – **209.165.200.236** 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(config)#ip nat inside source list 1 pool INTERNET

Tabla 18. Configurar la NAT estática y dinámica en el R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
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.	

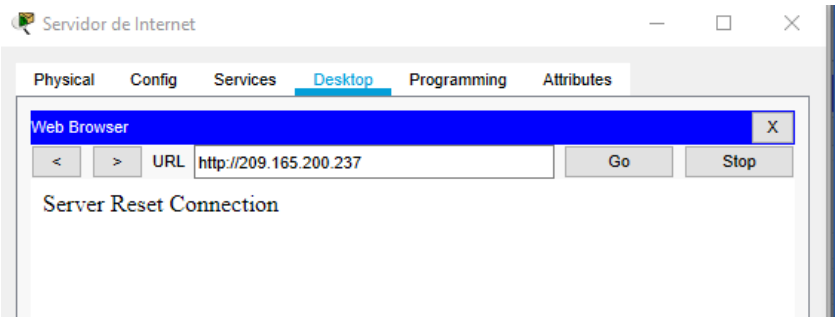
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet no soporto el comando **ip http serve**r para activar el servidor web por eso no responde al ip **209.165.200.237** 

Tabla 19. Verificar el protocolo DHCP y la NAT estática

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**15 de mayo de 2020, 19:44:00** R2#clock set 19:44:00 15 may 2020**.**
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 R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 10 16 37 4.00 858601895170.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#

Tabla 20. Configuración de 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

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 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado. User Access Verification Password: R2>exit

Tabla 21. Restringir el acceso a las líneas VTY en el R2

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

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
	`R2#show access-list`
	`Standard IP access list 1`
	`    10 permit 192.168.21.0 0.0.0.255`
	`    20 permit 192.168.23.0 0.0.0.255`
	`    30 permit 192.168.4.0 0.0.3.255`
	`Standard IP access list ADMIN-MGT`
	`    10 permit host 172.16.1.1 (2 match(es))`
	
	R2#show ip access-list
	`R2#show ip access-list`
	`Standard IP access list 1`
	`    10 permit 192.168.21.0 0.0.0.255`
	`    20 permit 192.168.23.0 0.0.0.255`
	`    30 permit 192.168.4.0 0.0.3.255`
	`Standard IP access list ADMIN-MGT`
	`    10 permit host 172.16.1.1 (2 match(es))`

Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

¿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 R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1026209.165.200.238:1026 tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1037209.165.200.238:1037
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 22. Comando CLI

7.2. 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.

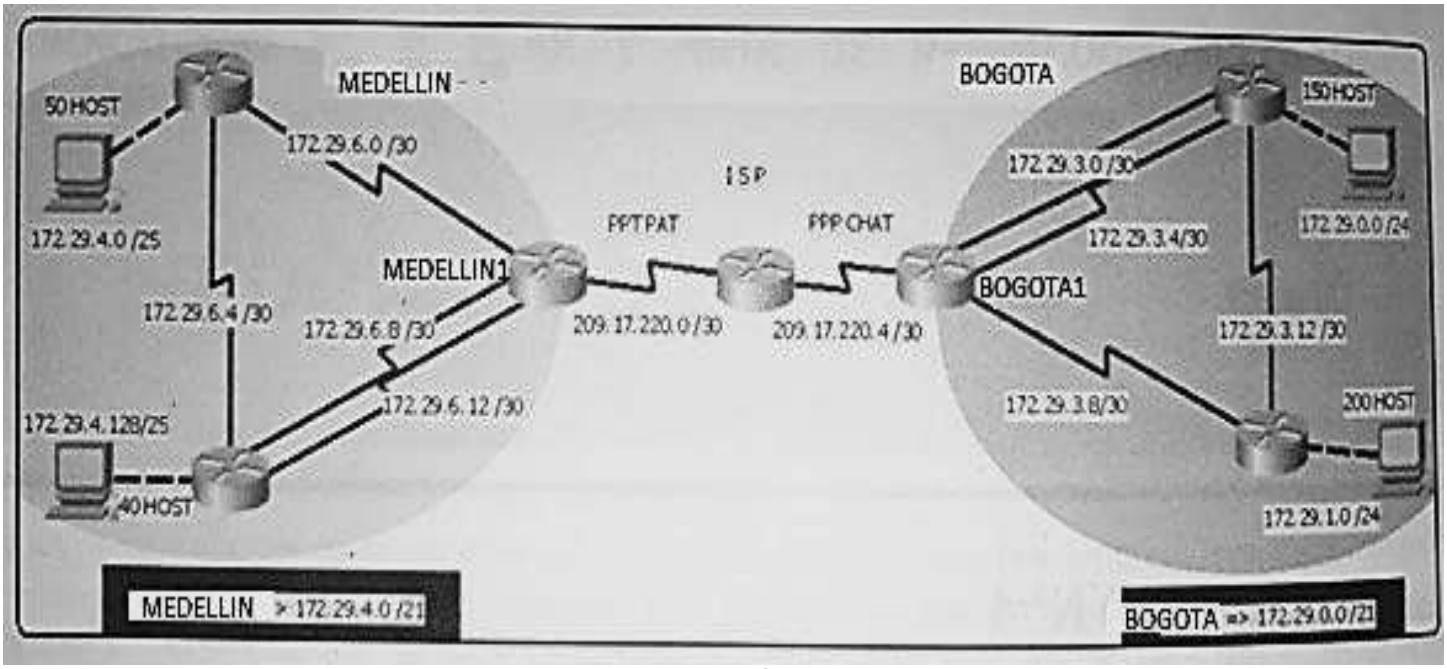


Figura 2. Topología de red. Fuente propia.

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.

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).

- Asignamos nombres a los Routers con el comando “hostaname”
- Desactivamos la Búsqueda DNS usando el comando “no ip domain-lookup”
- Ciframos la contraseña de texto no cifrado usando el comando “service password-encription”
- Contraseña de exec privilegiado cifrada asignamos “class”, con el comando “enable secret”.
- se usa el comando “line console 0” para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.
- Contraseña de acceso a la Consola asignamos “cisco” con el comando “password”
- Contraseña de Acceso Telnet: Las líneas VTY son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes

Aplicamos esta configuracion a los Routers MEDELLIN 1, 2 Y 3, BOGOTA 1,2 Y 3 e ISP asi:

MEDELLIN 1:

Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login

MEDELLIN 2:
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit

MEDELLIN 3:

Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit

ISP:

Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit

BOGOTA 1:

Router(config)#hostname BOGOTA1
BOGOTA1(config)#ip domain-lookup
BOGOTA1(config)# service password-encryption
BOGOTA1(config)#enable secret class
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

BOGOTA 2:
Router(config)#hostname BOGOTA2
BOGOTA2(config)# service password-encryption
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login

BOGOTA 3:
Router(config)#hostname BOGOTA3
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login

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

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

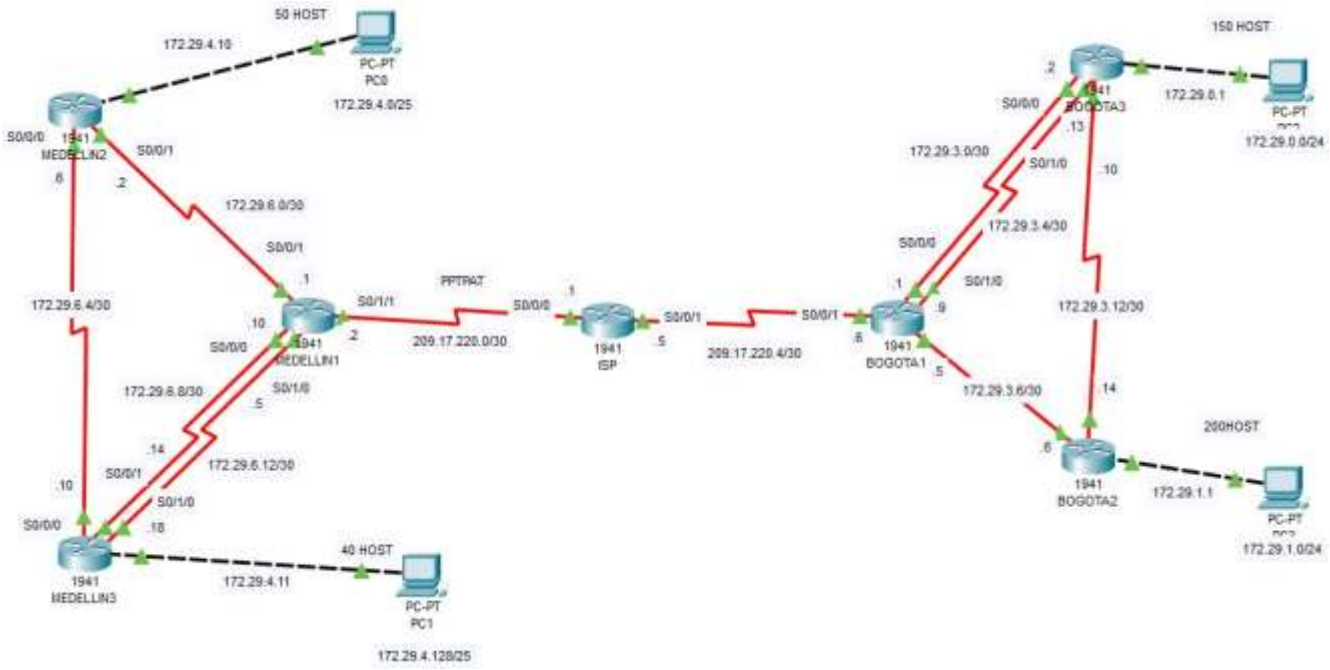


Figura 3. *Topologia de la red en funcionamiento*. Fuente propia.

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.

Nombre	Interfaz	Direccion IP	Subdireccion	Gateway
Medellin 1	S0/0/0	172.29.6.10	255.255.255.252	
	S0/0/1	172.29.6.1	255.255.255.252	
	S0/1/0	172.29.6.5	255.255.255.252	
	S0/1/1	209.17.220.2	255.255.255.252	
Medellin 2	S0/0/0	172.29.6.6	255.255.255.252	
	S0/0/1	172.29.6.2	255.255.255.252	
	G0/0	172.29.4.1	252.255.255.128	
Medellin 3	S0/0/0	172.29.6.10	255.255.255.252	
	S0/0/1	172.29.6.14	255.255.255.252	
	S0/1/0	172.29.6.18	255.255.255.252	
	G0/0	172.29.4.11	255.255.255.128	
ISP	S0/0/0	209.17.220.1	255.255.255.252	
	S0/0/1	209.17.220.5	255.255.255.252	

Bgota 1	S0/0/1	209.17.220.6	255.255.255.252	
	S0/0/0	172.29.3.1	255.255.255.252	
	S0/1/0	172.29.3.9	255.255.255.252	
	S0/1/1	172.29.3.5	255.255.255.252	
Bogota 2	S0/0/0	172.29.3.6	255.255.255.252	
	S0/0/1	172.29.3.14	255.255.255.252	
	G0/0	172.29.1.1	255.255.255.0	
Bogota 3	S0/0/0	172.29.3.2	255.255.255.252	
	S0/1/0	172.29.3.13	255.255.255.252	
	S0/1/1	172.29.3.10	255.255.255.252	
	G0/0	172.29.0.1	255.255.255.0	

Tabla 23. Asignacion de Direcciones IP. Fuente propia.

- Para que los routers sean accesibles, se deben configurar sus interfaces asignando las direcciones IP usando el comando **"ip address"** y activando la interfaz con el comando **"no shutdown".**
- Utilizamos **"clock rate"**, para poner el reloj en el router (DCE) clock rate se usa para el sincronismo de la conexión en serie. Sin el clockrate, la conexión no funciona porque no hay ningún conocimiento de la velocidad de los datos enviados entre los dos extremos de la conexión. Utilizaremos una velocidad de datos de 128000 bits por segundo.
- El protocolo de routing de estado de enlace **OSPF** utiliza el concepto de áreas, que son subdominios dentro del dominio OSPF. Un router dentro de un área mantiene la información completa de la topología del área.
- el comando **"passive-interface"** detiene las actualizaciones de ruteo de salida y de entrada, ya que el efecto del comando hace que el router deje de enviar y recibir paquetes de saludo sobre una interfaz.
- El comando **"no auto-summary"** evita que RIP haga un resumen automático de la red, si no lo hacemos así, los routers no van a ser capaces de conocer las subredes de esa red principal

Aplicamos lo anterior a los routers ISP, MEDELLIN 1,2,3 Y BOGOTA 1,2,3:

ROUTER ISP:

ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#no shutdown

```
ISP(config)#int s0/0/1
ISP(config-if)#ip addres 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config)#router ospf 3
ISP(config-router)#network 209.17.0.0 0.0.0.255 area 1
```

ROUTER MEDELLIN1:

```
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN1(config-if)#no shut down
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shut down

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 0
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.255 area 0
MEDELLIN1(config-router)#passive-interface s0/0/0

MEDELLIN1(config-router)#no auto-summary
```

ROUTER MEDELLIN2

```
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#int s0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shut down
```

MEDELLIN2(config-if)#int g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shut down

MEDELLIN2(config)#router ospf 2
MEDELLIN2(config-router)#network 172.29.0.0 0.0.0.255 area 0
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#exit

MEDELLIN2(config-router)#no auto-summary

ROUTER MEDELLIN3

MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shut down
MEDELLIN3(config-if)#int s0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#no shut down
MEDELLIN3(config-if)#int s0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.18 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#int g0/0
MEDELLIN3(config-if)#ip address 172.29.4.11 255.255.255.128
MEDELLIN3(config-if)#no shut down

MEDELLIN3(config)#router ospf 3
MEDELLIN3(config-router)#network 172.29.0.0 0.0.0.255 area 0
MEDELLIN3(config-router)#passive-interface g0/0

MEDELLIN3(config-router)#exit
MEDELLIN3(config)#

MEDELLIN3(config-router)#no auto-summary

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 shut down
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#no shut down
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shut down
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#no shut down

BOGOTA1(config)#router ospf 4
BOGOTA1(config-router)#network 172.29.0.0 0.0.0.255 area 2
BOGOTA1(config-router)#network 209.17.0.0 0.0.0.255 area 2
BOGOTA1((config-router)#passive-interface s0/0/0
BOGOTA1(config-router)#no auto-summary

ROUTER BOGOTA2:
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#no shut down
BOGOTA2(config)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA2(config-if)#no shut down
BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#no shut down

BOGOTA2(config)#router ospf 5
BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 2
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#router rip
BOGOTA2(config-router)#no auto-summary

ROUTER BOGOTA3

BOGOTA3(config)#int s0/0/0

```
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#int s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA3(config-if)#no shut down
BOGOTA3(config-if)#int s0/1/1
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shut down
BOGOTA3(config-if)#int g0/0
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shut down

BOGOTA3(config)#router ospf 6
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 2
BOGOTA3(config-router)#passive-interface g0/0

BOGOTA3(config-router)#router rip
BOGOTA3(config-router)#no auto-summary
```

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

ROUTER MEDELLIN 1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#do wr
```

ROUTER BOGOTA 1

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config-router)#router ospf 4
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#do wr
```

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

ROUTER ISP

ISP(config)#ip route 172.29.4.0 255.255.255.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#do wr

Parte 2: Tabla de Enrutamiento.

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

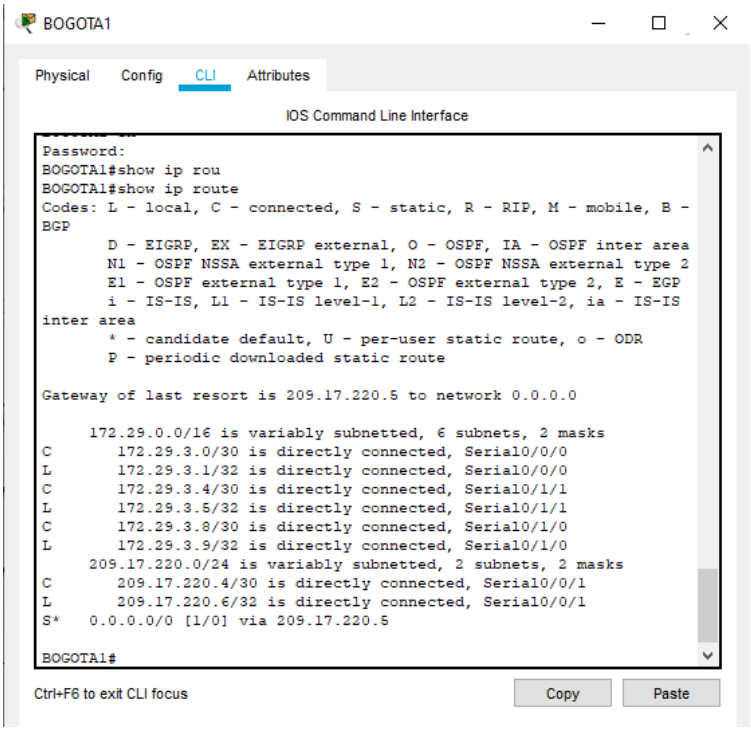


Figura 4. Verificacion de Enrutamiento Bogota1. Fuente propia

Figura 5. Verificacion de Enrutamiento medellin1. Fuente propia

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

El balanceo de cargas se nota en las conexiones dobles donde se balancea el envio de informacion y lo podemos ver en las rutas delos router con mas de una conexión. Tomamos como ejemplo Bogota3 y Medellin 3 . **(Ver Figura 6 y 7)**

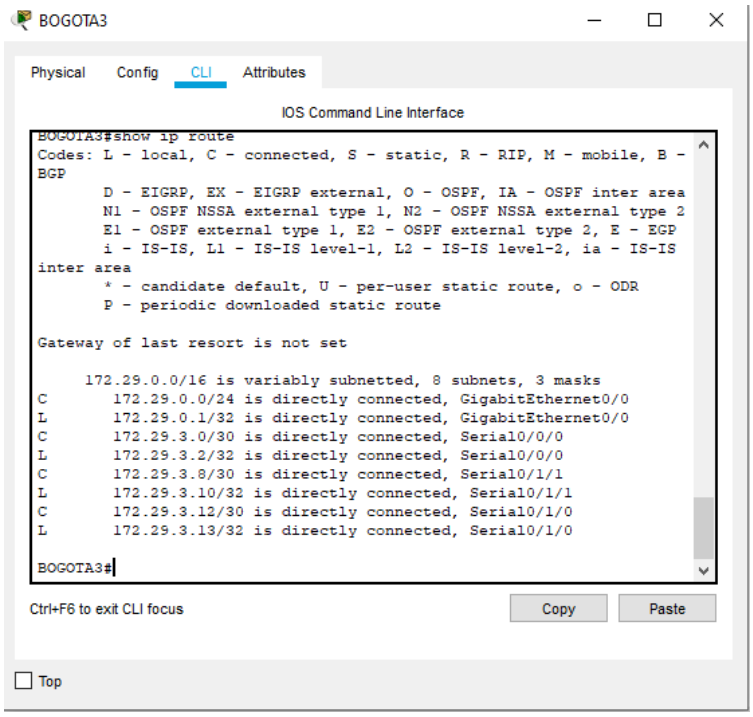


Figura 6. Verificar Balanceo de carga Bogota3. Fuente propia

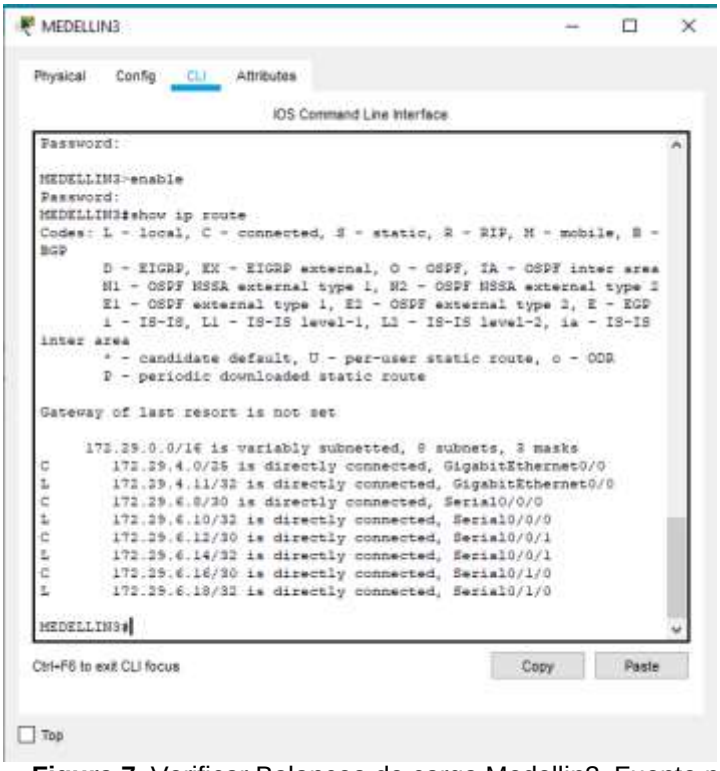


Figura 7. Verificar Balanceo de carga Medellin3. Fuente propia

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.

R/ BOGOTA 1 Y MEDELLIN1 son redes similares, en numero de conexiones, se conectan a igual numero de routers y se conectan con ISP

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.

R/ El balanceo de cargas tambien se representa con los conexiones redundantes, esto lo podemos observar en MEDELLIN 3 Y BOGOTA 3, por medio del codigo show ip route.

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

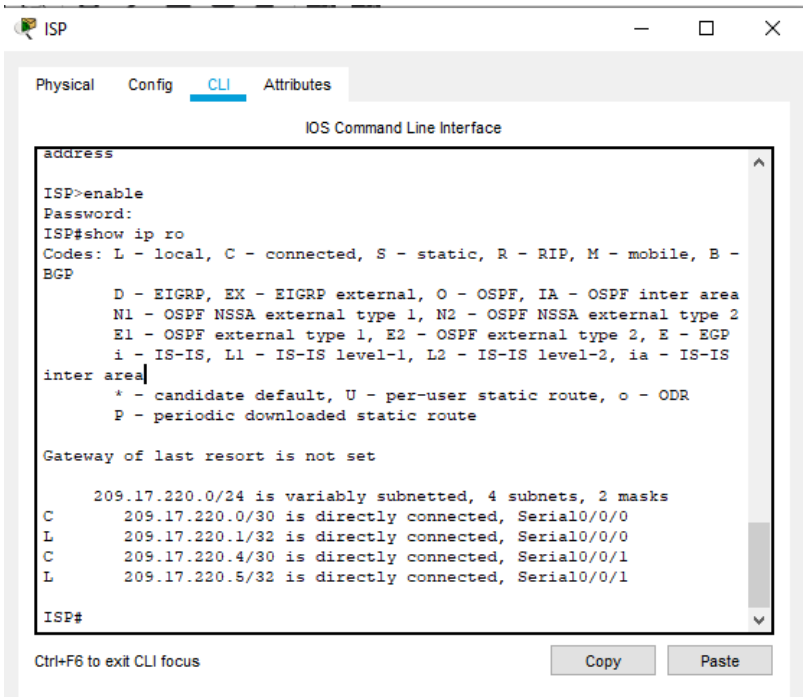


Figura 8. Demostracion puntos C,D,E,F. Fuente propia

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

ROUTER	**INTERFAZ**
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Tabla 24. Interfaces de Los routers. Fuente propia.

Se aplico cuando se configuró OSPF. todo lo demás se deshabilito porque no era necesario.

EJEMPLO:

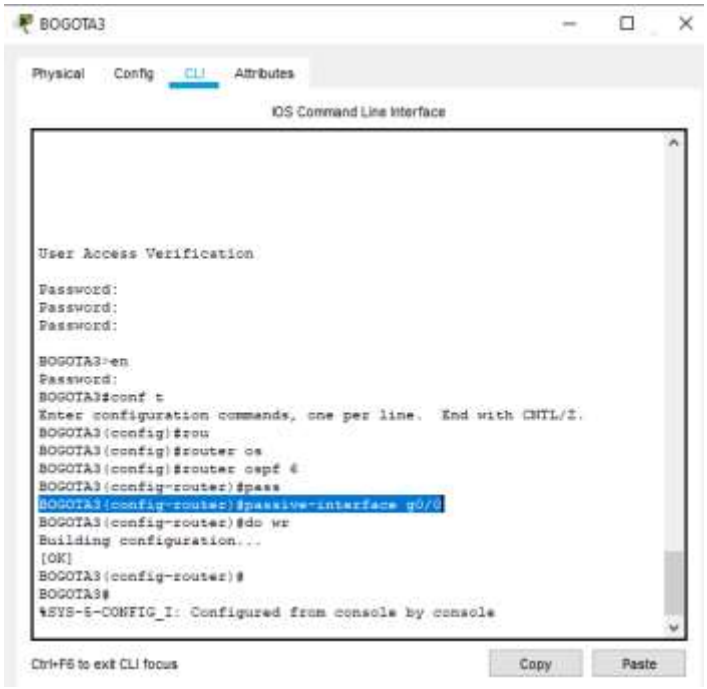


Figura 9. Deshabilitar propagaciond del protocolo OSPF. Fuente propia

Parte 4: Verificación del protocolo OSPF.

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.

Figura 10. Verificacion del protocolo OSPF Medellin1. Fuente propia

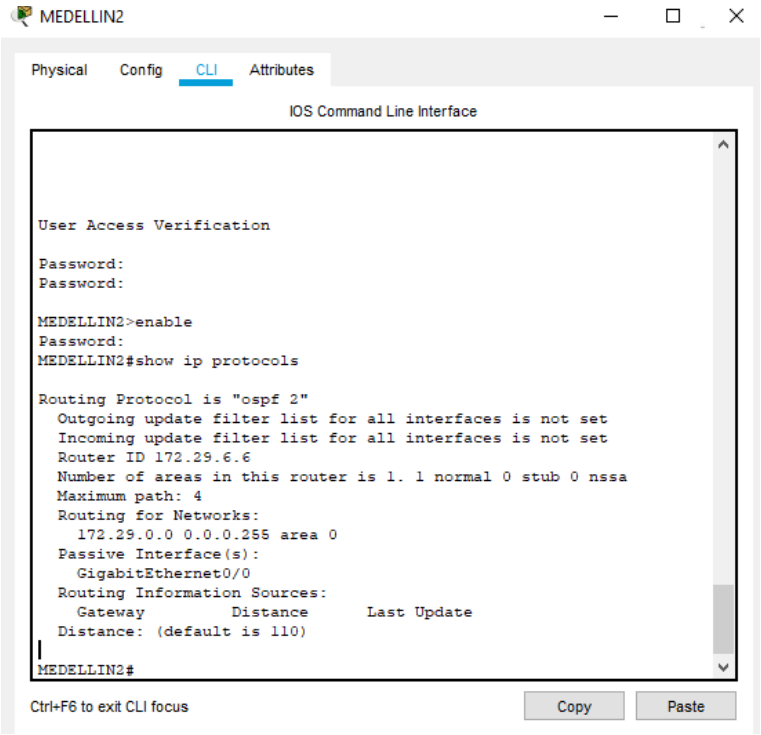


Figura 11. Verificacion del protocolo OSPF Medellin2. Fuente propia

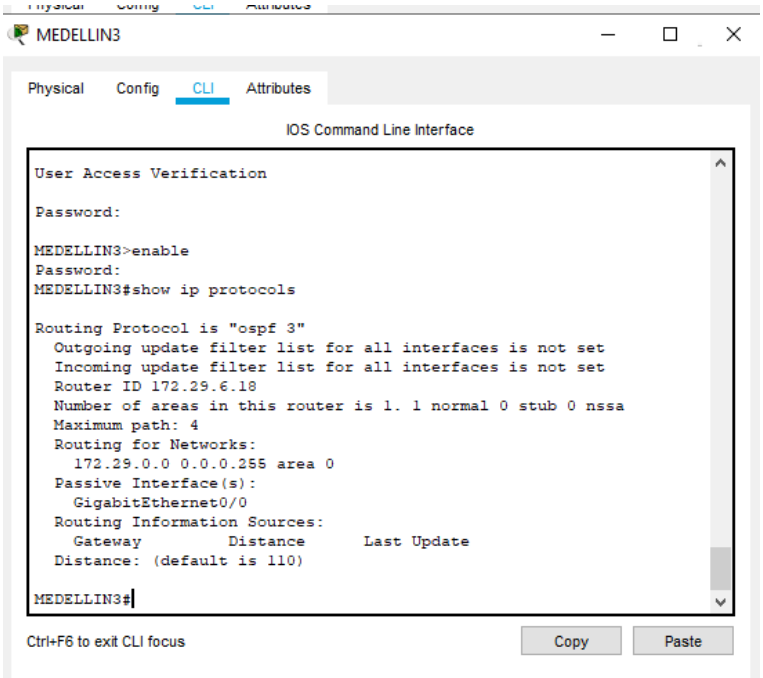


Figura 12. Verificacion del protocolo OSPF Medellin3. Fuente propia

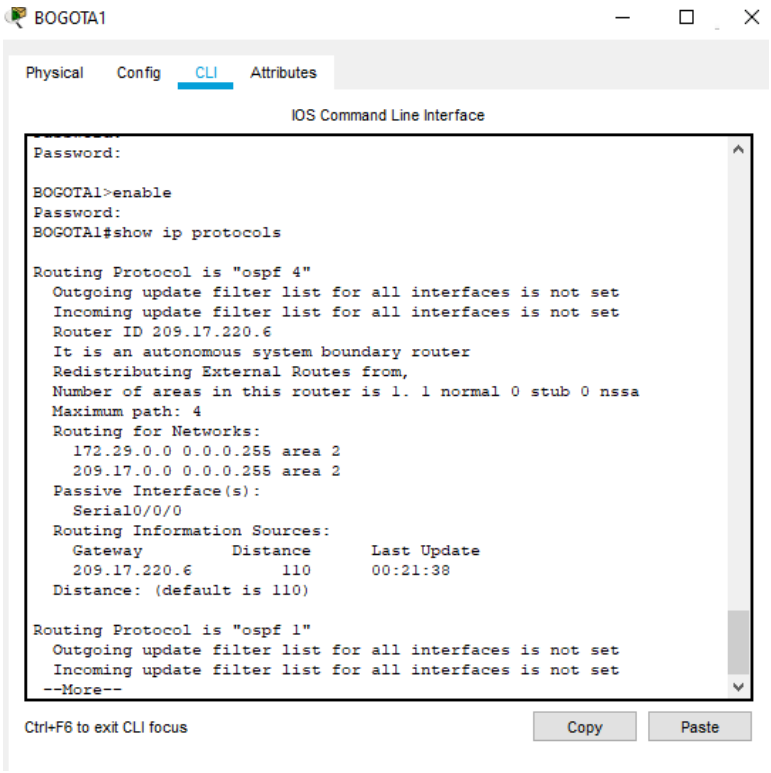


Figura 13. Verificacion del protocolo OSPF Bogota1. Fuente propia

Figura 14. Verificacion del protocolo OSPF Bogota2. Fuente propia

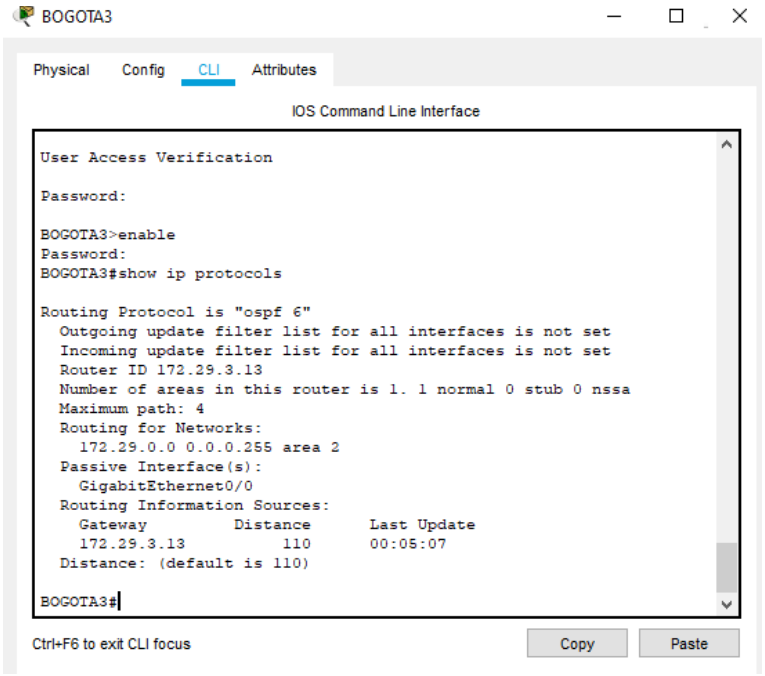


Figura 15. Verificacion del protocolo OSPF Bogota3. Fuente propia

passive interface: interface pasiva, que no envía ningún tipo de paquete, ni hellos ni cualquier otro tipo de paquetes. Es decir que por esa interfaces no podremos tener neighbors o vecinos, pero si anunciara las redes de dichas interfaces.

OSPF usa la multidifusión IP para enviar actualizaciones de estado de enlace. Esto garantiza menos procesamiento en los enrutadores que no escuchan los paquetes OSPF. Además, las actualizaciones solo se envían en caso de que se produzcan cambios de enrutamiento en lugar de periódicamente. Esto asegura un mejor uso del ancho de banda.

OSPF tiene una mejor convergencia que RIP. Esto se debe a que los cambios de enrutamiento se propagan instantáneamente y no periódicamente.

OSPF permite un mejor equilibrio de carga.

OSPF permite una definición lógica de redes donde los enrutadores se pueden dividir en áreas. Esto limita la explosión de actualizaciones de estado de enlace en toda la red. Esto también proporciona un mecanismo para agregar rutas y reducir la propagación innecesaria de información de subred.

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

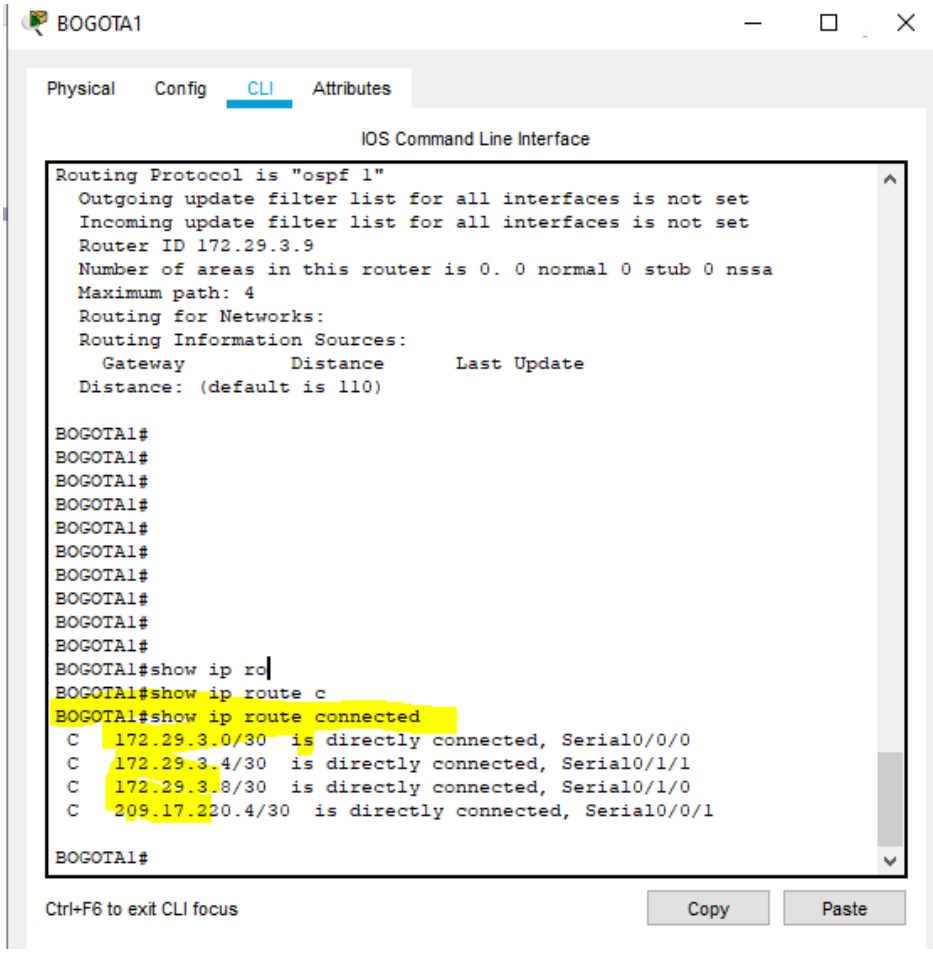


Figura 16. Verificacion base de datos OSPF Bogota1. Fuente propia

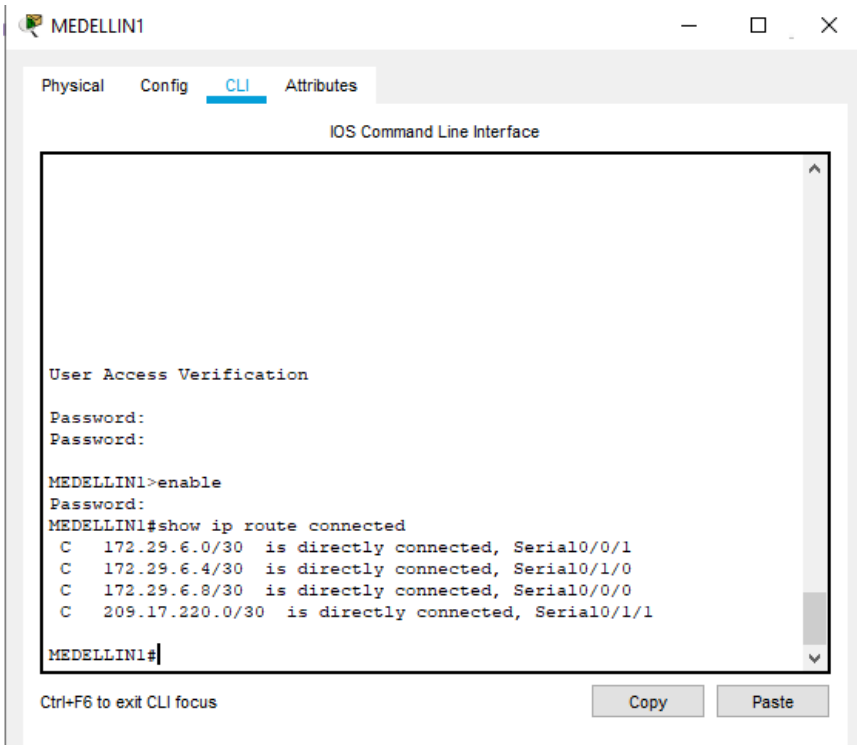


Figura 17. Verificacion base de datos OSPF Medellin1. Fuente propia

En las figuras podemos apreciar las rutas que están conectadas con su dirección ip y el puerto de conexión.

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.

ROUTER ISP

ISP(config)#username MEDELLIN password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#ping 209.17.220.1

ISP(config)#username BOGOTA password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp auth
ISP(config-if)#ppp authentication chap

ROUTER MEDELLIN1

MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN password cisco
MEDELLIN1(config-if)#do wr

ROUTER BOGOTA 1

BOGOTA1(config)# username ISP password cisco
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#

Parte 6: Configuración de PAT.

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

MEDELLIN1

MEDELLIN1(config)#ip nat inside source list 1 interface s0/1/1 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside

BOGOTA 1

BOGOTA1(config)#ip nat inside source list 1 interface s0/0/1 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#

Comprobamos por medio de ping desde la computadora PC0 a ISP cuya dirección IP por esa red es: 209.17.220.1

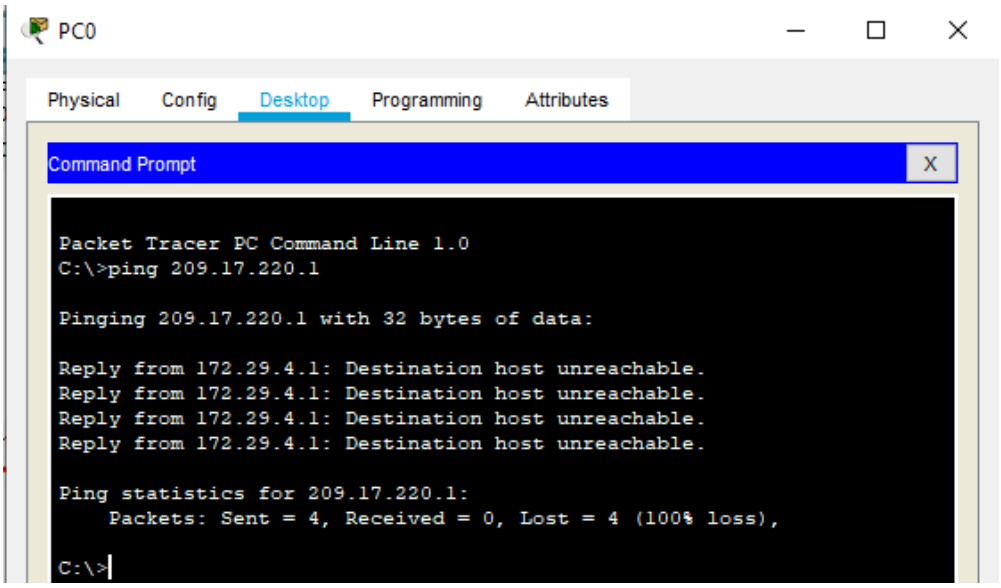


Figura 18. Ping entre PC0 e ISP. Fuente propia

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.

```
MEDELLIN2#conf t
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.5
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 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
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 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#end
```

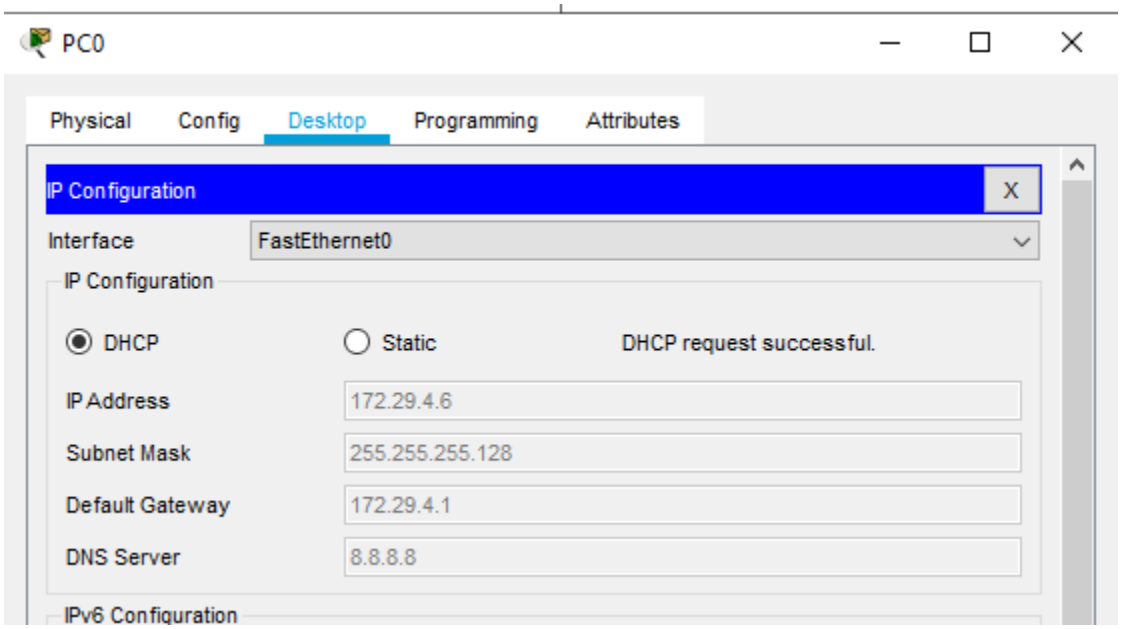


Figura 19. Configuracion DHCP PC0. Fuente propia

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

Habilitamos MEDELLIN3 como paso de mensajes broadcast

MEDELLIN 3

MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.10
MEDELLIN3(config-if)#do wr

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

BOGOTA 3

BOGOTA3#config t
BOGOTA3(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA3(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5

BOGOTA3(config)#ip dhcp pool BOGOTA2
BOGOTA3(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA3(dhcp-config)#default-router 172.29.1.1
BOGOTA3(dhcp-config)#dns-server 8.8.8.8
BOGOTA3(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA3(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA3(dhcp-config)#default-router 172.29.0.1
BOGOTA3(dhcp-config)#dns-server 8.8.8.8

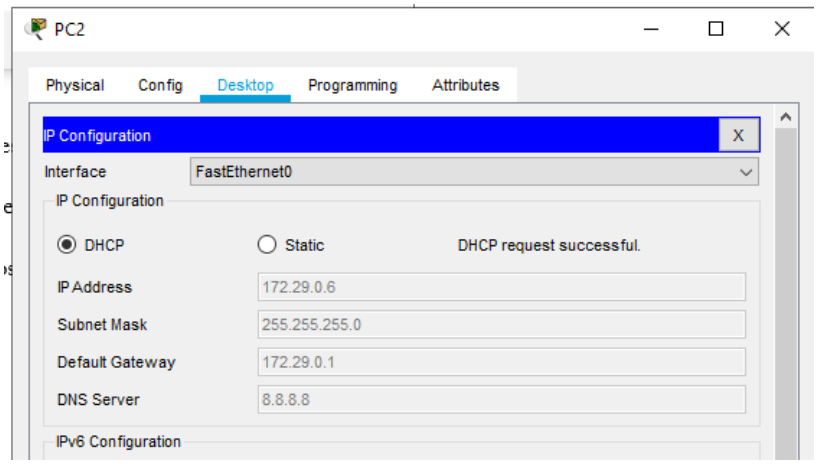


Figura 20. Configuracion DHCP PC2. Fuente propia

Habilitamos BOGOTA 3 como paso de mensajes broadcast

BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.10
BOGOTA3(config-if)#exit

BOGOTA3(config)#

CONCLUSIÓN

Este Informe ha sido de suma importancia para reforzar lo aprendido a lo largo de este curso de redes CISCO. Cada uno de los escenarios propuestos brindo al estudiante la oportunidad de afianzar y llevar a la práctica los conocimientos adquiridos en cada unidad el uso de herramientas tecnológicas y software dio un valor agregado al aprendizaje, ya que a través de estas nos pudimos acercar a lo que es en realidad el día a día.

Como estudiantes tuvimos la oportunidad de profundizar en cada uno de los temas tratados y aplicar lo aprendido en los diferentes laboratorios. El primer escenario propuesto por este laboratorio permite al estudiante realizar configuraciones de redes pequeña para que admita conectividad IPv4 e IPv6, aplicar seguridad de switches, routing entre otros. En el escenario se planteó el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

REFERENCIA BIBLIOGRÁFICA

APSER IT. (2017). REDES COMPUTACIONALES. Obtenido de https://blog.apser.es/2015/07/27/la-gran-red-de-computadoras-como-funcionainternet

APSER IT. (2017). REDES COMPUTACIONALES. Obtenido de https://blog.apser.es/2015/07/27/la-gran-red-de-computadoras-como-funcionainternet

CCNA 2. Conceptos y protocolos de enrutamiento, Material de apoyo en formato PDF(2012). Recuperado el 3 de Septiembre de 2012, de http://66.165.175.206/campus14/mod/resource/view.php?id=10805

Cisco Network. (s.f.). Ospfv. Obtenido de http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospfen-cisco-router/

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

CISCO Packet Tracer (2012). Recuperado el 10 de diciembre de 2012, de http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

Comandos Cisco IOS - Comandos para Configuración de Router. Recuperado el 12 de Octubre de 2012, de **http://www.garciagaston.com.ar/verpost.php?id_noticia=101**

¿Cómo funciona el protocolo OSPF? Recuperado el 15de Diciembre de 2012, de http://www.ordenadores-y-portatiles.com/protocolo-ospf.html

Configurar el enrutamiento EIGRP. Recuperado el 15de Diciembre de 2012, de http://rodri.wordpress.com/2007/01/19/configurar-enrutamiento-eigrp/

DIRECCIONAMIENTO IP. Recuperado el 9 de Octubre de 2012, de http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/redes/Archivos/CreacSubr

DIVISIÓN BÁSICA EN SUBREDES. SUBNETTING. Recuperado el 9 de Octubre de 2012,

De http://redesdecomputadores.umh.es/red/ip/Divisi%C3%B3n%20en%20subredes%20ok%20I**I.htm**

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

Estudio de Subnetting, VLSM, CIDR y Comandos de Administración y Configuración de Routers (2010). Recuperado el 10 de diciembre de 2012, de http://www.plusformacion.com/Recursos/r/Estudio-Subnetting-Vlsm-CIDR-ComandosAdministracion-Configuracion-Routers

EL SUBNETEO Recuperado el 3 de Septiembre de 2012, de http://www.ie.itcr.ac.cr/egarcia/Presentaciones/Modulo1/Subneteo.pdf

Gonzales J. (2013). Switch. Obtenido de http://redestelematicas.com/el-switch-comofunciona-y-sus-principales-caracteristicas/

Introducción a IP versión 4. Recuperado el 3 de Septiembre de 2012, de http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4

Kurose, J. R. (2008). Computer networking. Pearson. Obtenido de ISBN 987-0-321- 51325-0.: https://es.wikipedia.org/wiki/Router

Masadelante.com. (s.f.). LAN. Obtenido de www.masadelante.com/faqs/lan Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#11.0

PRINCIPIOS BÁSICOS DEL RIP V2. Recuperado el 10 de Septiembre de 2012, de http://librosnetworking.blogspot.com/2006/07/principios-bsicos-de-ripv2.html

Segui, F. B. (2015). Configuración DHCP en routers CISCO. Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software

INTRODUCCIÓN AL ENRUTAMIENTO SIN CLASE. Recuperado el 9 de Octubre de 2012, de http://www.elmundodelastics.net/2008/09/introduccin-al-enrutamiento-sin-clase.html