DISEÑO DE IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

PRESENTADO POR:
NINFA PÉREZ PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
FLORENCIA, CAQUETÁ
MAYO 2020

DISEÑO DE IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

AUTOR

NINFA PÉREZ PARRA

DIPLOMADO DE PROFUNDIZACIÓN PARA OPTAR POR EL TÍTULO DE INGENIERA DE SISTEMAS

DIRECTOR DEL CURSO

ING. JUAN CARLOS VESGA FERREIRA

TUTOR

ING. HECTOR JULIAN PARRA MOGOLLÓN

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
FLORENCIA – CAQUETÁ
MAYO 2020

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

INGENIERIA DE SISTEMAS

FLORENCIA – CAQUETÁ

MAYO 2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Florencia, 22 de mayo (22, 05, 2020) (Mayo 22 de 2020)

DEDICATORIA Y AGRADECIMIENTOS

En este trabajo como debe ser todo en nuestro día a día, está dedicado primero a Dios, por permitirme un nuevo logro en mi vida, por ser tan maravilloso conmigo y darme salud y la oportunidad de ser una gran profesional, también a los estudiantes que apenas están inciando sus carreras para que no se desanimen, por el contrario, se esfuercen cada día a cumplir sus metas.

Agradezco a mi familia, en especial a mis hijos, por su apoyo incondicional, a todos los directivos y docentes de la universidad ya que cada uno fue parte fundamental en mi formación. A todos aquellos que me dieron una voz de aliento y también a los que no creyeron en mí porque todo eso me ayudó a no darme por vencida.

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

GLOSARIO

TOPOLOGÍA: es la rama de las matemáticas dedicada al estudio de aquellas propiedades de los cuerpos geométricos que permanecen inalteradas por transformaciones continuas, disciplina que estudia las propiedades de los espacios topológicos y las funciones continuas.

CISCO SYSTEMS: empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

NETWORKING: es una estrategia que consiste en ampliar nuestra red de contactos profesionales con el empleo de redes sociales de tipo profesional, haciendo que el Networking sea una estrategia muy usada por empresas, por ejemplo: en Linkedin las empresas buscan nuevas alianzas estratégicas o profesionales.

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

RESUMEN

En el desarrollo del presente trabajo, se ejecutará la evaluación final de habilidades prácticas del curso de profundización CISCO CCNA 2. En los que se desprende tender el cableado de red y verificar la configuración predeterminada del switch, configurar los parámetros básicos de los dispositivos de red, verificar y probar la conectividad de red y administrar la tabla de direcciones. Se armará una topología simple mediante cableado LAN Ethernet y accederá a un switch Cisco utilizando los métodos de acceso de consola y remoto; buscando identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

PALABRAS CLAVES: Redes, Telecomunicaciones, Packet Tracer, simulación, laboratorios.

1. INTRODUCCIÓN

Debido a la gran importancia de las redes de internet en el diario vivir de las personas, por eso, en el contenido de este trabajo se presenta a detalle el modo en que 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.

En este sentido, durante el desarrollo de los 2 escenarios, se plantea la problemática y se dan las herramientas necesarias para que se administre una red, es decir, se configurará cada uno de los dispositivos e interconectarán entre sí, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de una red.

1. OBJETIVOS

2.1 OBJETIVO GENERAL

Llevar a cabo el desarrollo de la prueba de habilidades práctica, como actividad final para el diplomado de grado CISCO CNNA2 para poner en práctica la temática llevada a cabo durante el transcurso del programa.

2.2 OBJETIVOS ESPECÍFICOS

- Desarrollar actividades de representación de red, que incluyen la exploración, conexión y configuración de dispositivos.
- Revisión de procesos de configuración de un sistema operativo de red e identificación de su funcionalidad y propósito.
- Identificación de los protocolos y comunicaciones de red.
- Exploración de las propiedades físicas y lógicas de los dispositivos de red.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Durante el desarrollo del presente trabajo, se articulan en su contenido diversas temáticas que permiten abordar el núcleo problémico: Gestión de Sistemas y Servicios de Telecomunicaciones en función del núcleo integrador del problema: Las telecomunicaciones como herramienta para la competitividad global con visión socio humanística, en donde hay un aprendizaje mediante la creación de una red empresarial eficaz y escalable; así como a través de instalar, configurar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de una red convergente.

3.2 JUSTIFICACIÓN

Con el desarrollo de esta prueba de habilidades, se puede decir que ya contamos con herramientas de gran experiencia efectiva como la configuración de sistemas operativos de red, protocolos de comunicación, mecanismos de acceso al medio y características de la capa de red la capa de transporte, asignación de direcciones IP, subnetting y capa de aplicación, también analizamos la forma adecuada de diseñar y configurar soluciones soportadas en el uso de dispositivos de conmutación acorde con las topologías de red requeridas bajo el uso de protocolos basados en STP y VLANs bajo una arquitectura jerárquica.

En el entorno en el cual los futuros ngenieros de la UNAD se van a desenvolver, es muy importante estar en la capacidad de solucionar problemas que responder a la demanda creciente de personal especializado en el área de las Tecnologías de la Información, acompañado de un alto componente práctico, mediante el uso de herramientas de simulación y laboratorios remotos.

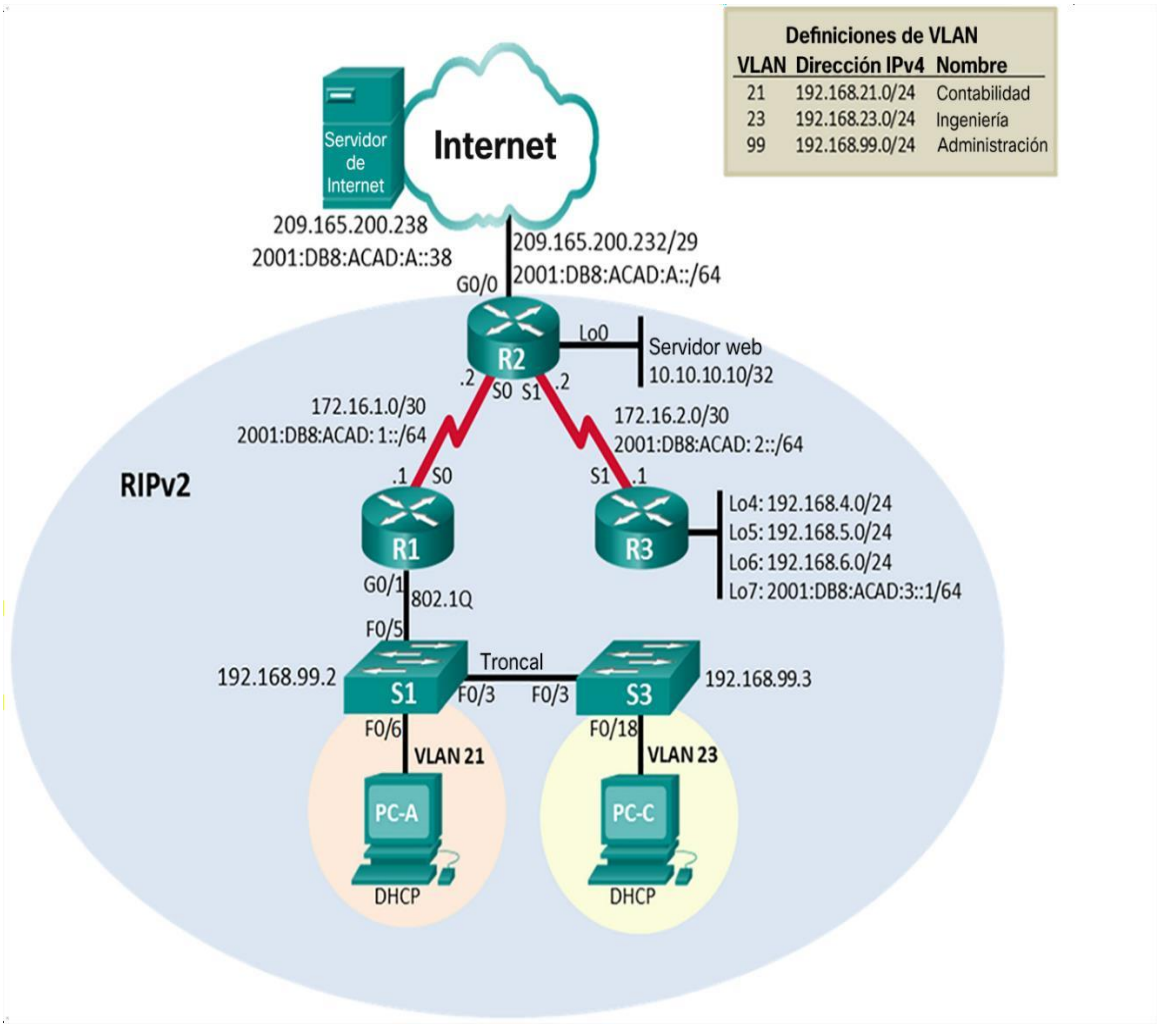
Así mismo, contamos con la orientación para utilizar el enrutamiento estático, enrutamiento dinámico, enrutamiento mediante protocolos de estado enlace, listas de acceso, asignación dinámica de direcciones IP y traducciones de direcciones IP mediante NAT.

4. DESARROLLO DE LOS ESCENARIOS

4.1 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.

Gráfica 1. Topología – Escenario 1



4.1.1 Parte 1. Inicializar dispositivos

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

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

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

Tabla 1. Configuración básica del router y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Ejecutamos el siguiente código: Erase startup-config
Volver a cargar todos los routers	Introducimos el código: Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para borrar introducimos este código Delete vlan.dat
Volver a cargar ambos switches	Ejecutamos: no shutdown
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Utilizamos el siguiente código Show vlan brief

4.1.2 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):

Tabla 2. Configuración del servidor de Internet según topología

Elemento o tarea de configuración	Especificación
Dirección IPv4	Se ingresa al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla de IPV4 Introducimos la ruta 209.165.200.238

Máscara de subred para IPv4	Ingresamos al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla de subred Mask Introducimos la ruta: 255.255.255.248
Gateway predeterminado	Ingresamos al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla Default Gateway Introducimos la ruta: 209.165.200.225
Dirección IPv6/subred	Ingresamos al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla IPV6 Address Introducimos la ruta: 2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	Ingresamos al server en la pestaña desktop y ubicamos la ip configuración buscamos la pestaña o casilla Gateway de IPV6 Introducimos la ruta: 2001:DB8:ACAD:2::1

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

Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración del Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Router(config)#no ip domain-lookup
Nombre del router	Se ingresa el código: hostname R1
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco

Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption R1(config)#service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd Se prohíbe el acceso no autorizado. R1(config)#banner motd #se prohíbe el acceso no autorizado#
Interfaz S0/0/0	Establezca la descripción: se hace con este código: interface serial 0/0/0 description 1 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones es: 172.16.1.0/30 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones es: 2001:DB8:ACAD:1::/64 Establecer la frecuencia de reloj en 128000 Activar la interfaz Int s0/0/0 Clock rate 128000
Rutas predeterminadas	Configurar una ruta Ipv4 predeterminada de S0/0/0 El código es interface serial 0/0/0 ip address 172.16.1.2 255.255.255.0 Configurar una ruta Ipv6 predeterminada de S0/0/0 interface Serial0/0/0 ipv6 address 2001:DB8:ACAD:1::1/64

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configuración del Router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: no ip domain-lookup
Nombre del router	Se ingresa el código: hostname R2

Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Habilitar el servidor HTTP	Como no se pueden utilizar los comandos ip http server se emplea un servidor dentro de la topología ip nat inside source static 10.10.10.10 209.165.200.229 int f0/0 ip nat outside int f0/1 ip nat inside
Mensaje MOTD	Se ingresa el código: banner motd! ¡Se prohíbe el acceso no autorizado!
Interfaz S0/0/0	Establezca la descripción interface serial 0/0/0 description R2 a R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. ip address 172.16.1.2 255.255.255.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz int s0/0/0 ipv6 address 2001:DB8:ACAD:2::/64

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int s0/0/1 ip address 172.16.2.1 255.255.255.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. ipv6 address 2001:DB8:ACAD:3::/64 Establecer la frecuencia de reloj en 128000. clock rate 128000 Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ip address 209.165.200.236 255.255.255.250 Bad mask 0xFFFFFFFA for address 209.165.200.236 int g0/0 ip address 209.165.200.236 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. int G0/0 ipv6 address 2001:DB8:ACAD:A::/64 Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. Entramos al desktop y seleccionamos ip Configuración y escribimos en las casillas Ip address 10.10.10.10
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. ip address 172.16.1.3 255.255.255.0 Configure una ruta IPv6 predeterminada de G0/0. ipv6 address 2001:DB8:ACAD:A: :/64

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configuración del Router 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: no ip domain-look
Nombre del router	Se ingresa el código: hostname R3
Contraseña de exec privilegiado cifrada	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 password Cisco
Cifrar las contraseñas de texto no cifrado	Ingresamos el código: service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd !Se prohíbe el acceso no autorizado!
Interfaz S0/0/1	Establecer la descripción interface serial 0/0/0 description 1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred: 172.16.2.0/30 Se utiliza int s0/0/1 ip address 172.16.2.6 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. 2001:DB8:ACAD:2::/64 Se utiliza ipv6 address 2001:DB8:ACAD:2::/64 Activar la interfaz

Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int lo4 ip address 192.168.4.2 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int lo5 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. int lo6 ip address 192.168.6.2 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. int lo7 ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	lp route 0.0.0.0.0.0.0.0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración swith 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Ingresamos el Código: no ip domain-look up
Nombre del switch	Ingresamos el Código: hostname S1
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco

Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Mensaje MOTD	Se ingresa el código: banner motd #Se prohíbe el acceso no autorizado#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configuración swith 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el Código: no ip domain-lookup
Nombre del switch	Se ingresa el código: hostname S3
Contraseña de exec privilegiado cifrada	Se ingresa el código: enable secret Class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password Cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: service password-encryption
Mensaje MOTD	Se ingresa el código: 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.

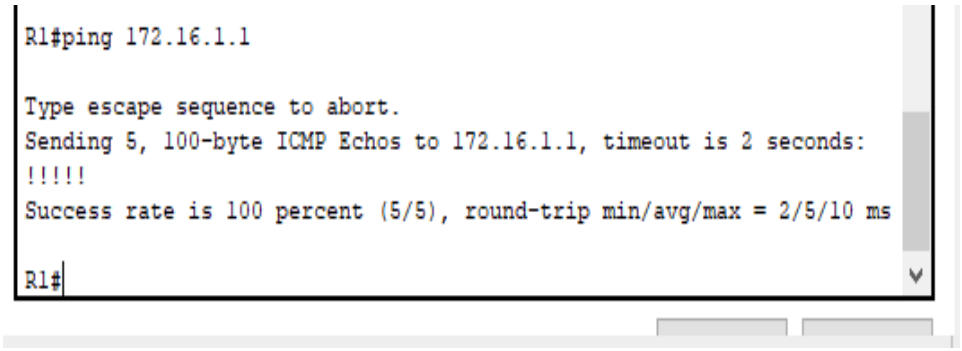
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Verificación de la red

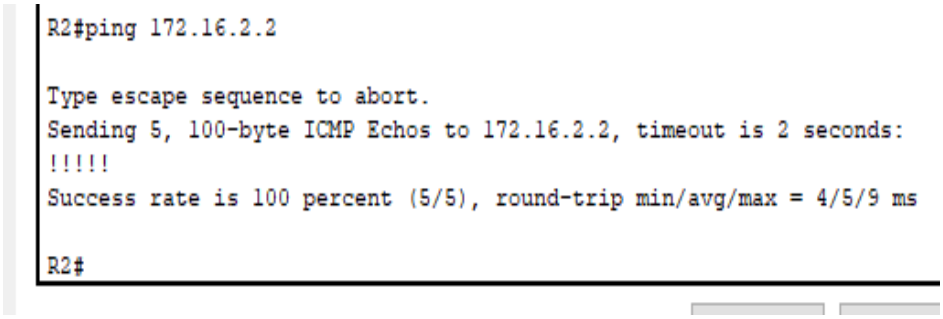
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	Efectivo
R2	R3, S0/0/1	172.16.2.2	Efectivo
PC de Internet	Gateway predeterminado	209.165.200.229	Efectivo

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

Gráfica 2. Verificación Ping de R1 a R2



Gráfica 3. Verificación Ping de R2 a R3



4.1.3 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:

Tabla 9. Seguridad del switches 1 de 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 indicant vlan 21 name Contabilidad vlan 23 name Ingeniería vlan 99 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 Ingresamos el siguiente código int vlan 99 ip address 192.168.99.1 255.255.255.0 int vlan 21 ip address 192.168.21.1 255.255.255.0 int vlan 23 ip address 192.168.23.1 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Escribimos el siguiente código: ip default-Gateway 192.168.199.3
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native Utlizamos el siguiente código: int f0/3 switchport mode trunk switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native utilizamos el siguiente código: int f0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/2, f0/4, f0/6-23 switch mode access int f0/1
Asignar F0/6 a la VLAN 21	Utilizamos los siguientes códigos interface f0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	Ingresamos el siguiente código: interface range f0/1-24

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Seguridad del switches 3 de 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. vlan 21 name Contabilidad vlan 23 name Ingeniería vlan 99 name Administracion

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 int vlan 99 ip address 192.168.99.2 255.255.255.0 int vlan 21 ip address 192.168.21.2 255.255.255.0 int vlan 23 ip address 192.168.23.2 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. ip default-gateway 192.168.199.2
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native int f0/3 switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range fa0/1-2, fa0/4-24 switchport mode access
Asignar F0/18 a la VLAN 21	Ingresamos el siguiente código: int f0/18 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	Ingresamos el siguiente código: int range f0/1-2, f0/4-17, f0/19-24

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuración del Router de la subinterfaz

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Ingresamos el siguiente código: int g0/1.1 description LAN de Contabilidad encapsulation dot1Q 21 Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 21 ip address 192.168.21.4 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Introducimos el siguiente código int g0/1.2 Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 23 ip address 192.168.23.4 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 int g0/1.3 description LAN de Administracion encapsulation dot1Q 99 Asignar la primera dirección disponible a esta interfaz ip address 192.168.99.4 255.255.255.0
Activar la interfaz G0/1	No shutdown

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.

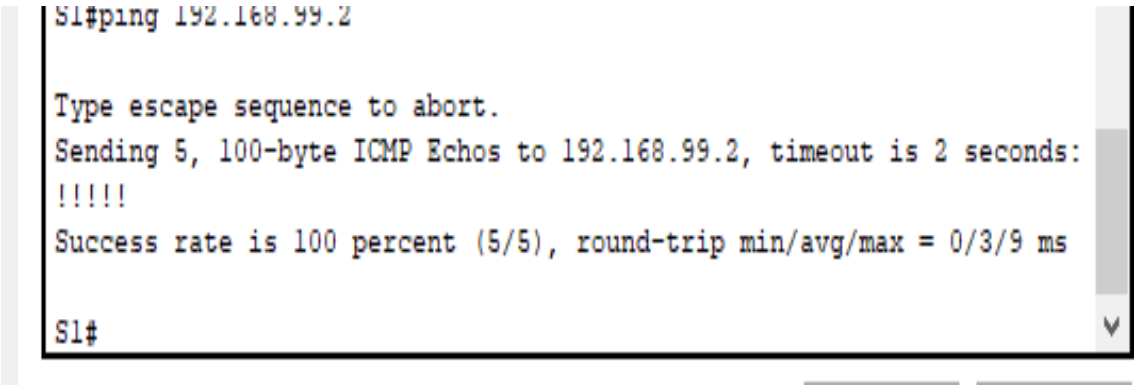
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	efectivo
S3	R1, dirección VLAN 99	192.168.99.2	efectivo
S1	R1, dirección VLAN 21	192.168.21.1	efectivo
S3	R1, dirección VLAN 23	192.168.23.2	efectivo

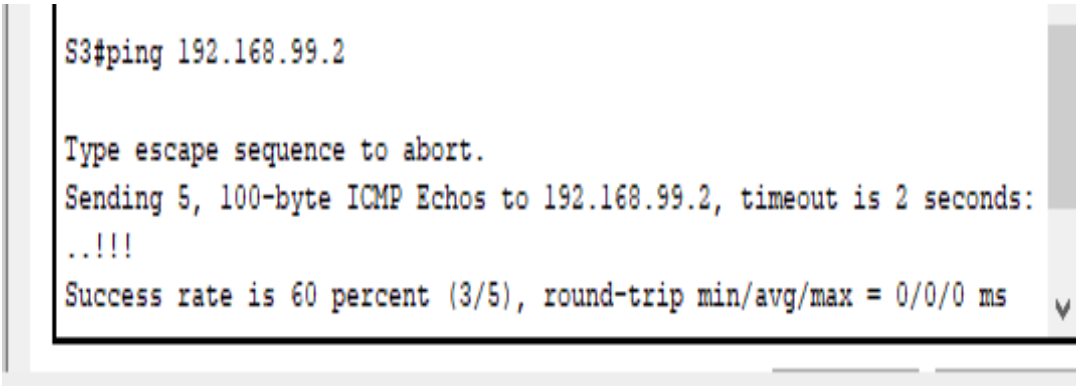
Gráfica 4. Verificación de conectividad en S1 al R1

Ping de S1 al R1



Gráfica 5. Verificación de conectividad en S3 al R1

Ping de S3 al R1



4.1.4 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:

Tabla 13. Configuración el protocolo de routing 1, dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Ejecutamos el siguiente código: router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. router-id 2.2.2.2 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	Utilizamos el código: passive-interface g0/1.1 passive-interface g0/1
Desactive la sumarización automática	Utilizamos el código: router rip no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuración del protocolo de routing 2, dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router ospf 1
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	router ospf 2 router-id 2.2.2.2 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0 network 10.10.10.10 0.0.0.255 area 0 passive-in passive-interface g0/1
Desactive la sumarización automática.	no auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuración del protocolo de routing 2, dinámico RIPv3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router ospf 1
Anunciar redes IPv4 conectadas directamente	network 172.16.3.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Network 192.168.4.0 0.0.3.255 area 0 passive-interface lo4 passive-interface lo5 passive-interface lo6 passive-interface lo7
Desactive la sumarización automática.	no auto-summary

Paso 4: Verificar la información de RIP

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

Tabla 16. 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 ospf neig
¿Qué comando muestra solo las rutas RIP?	show ip ospf interface
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip protocols

4.1.5 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:

Tabla 17. Implementación DHCP y NAT para IPv4 en el router 1

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

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

Paso 2 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración de la NAT estática y dinámica en el R2

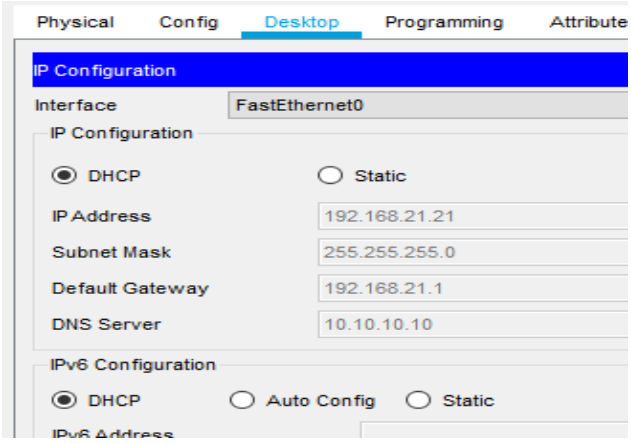
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** user webuser privilege 15 secret Cisco
Habilitar el servicio del servidor HTTP	No soporta el código HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	ip nat inside source static 10.10.10.10 209.165.200.229
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

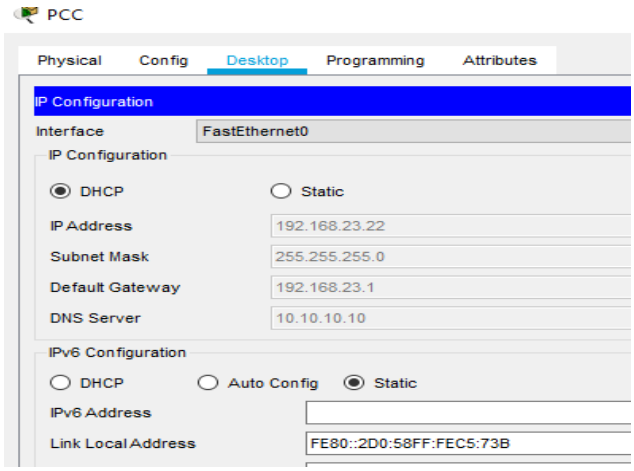
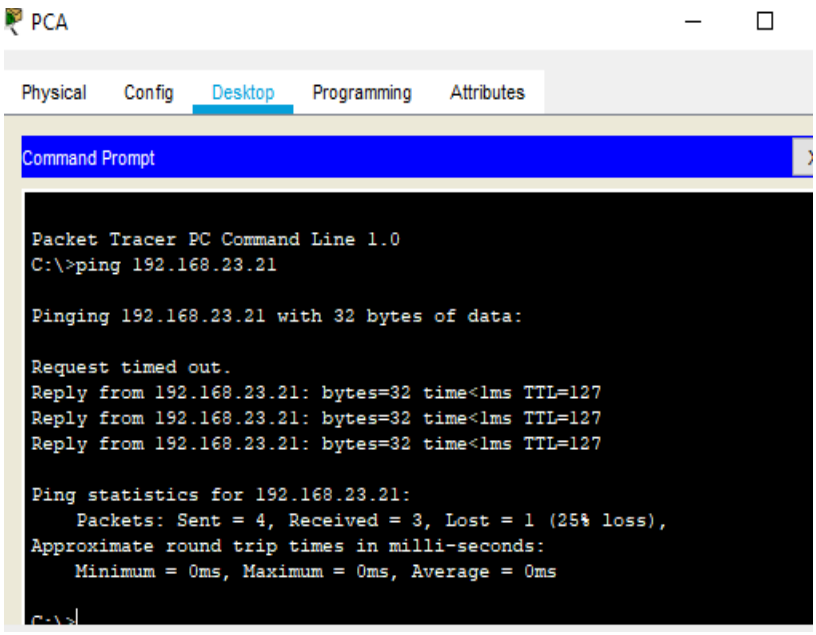
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	ip nat pool Internet 209.165.200.229 209.165.200.228 netmask 255.255.255.248

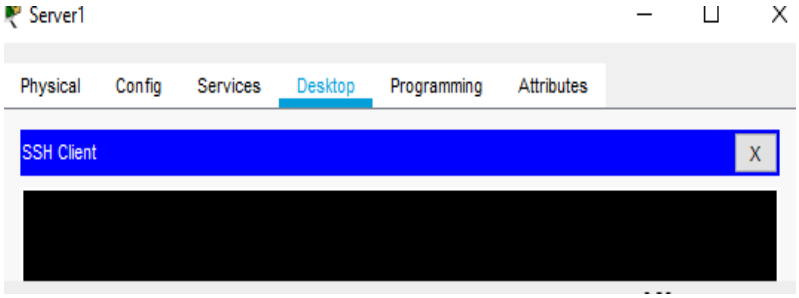
Paso 3: Verificar el protocolo DHCP y la NAT estática

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 19. Verificación el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Gráfica 6. Verificación de la PC-A Información de IP del servidor DHCP 

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Gráfica 7. Verificación de la PC-C Información IP del servidor DHCP 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Gráfica 8. Verificación de la PC-A al PC-C 

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**	Gráfica 9. Iniciamos sesion desde el servidor web 

4.1.6 Parte 6: Configurar NTP

Tabla 20. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	clock set 09:00:00 mar 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
configure R1 para actualizaciones de calendario dicas con hora NTP.	ntp server 209.165.200.229
Verifique la configuración de NTP en R1.	show ntp associations

Gráfica 10. Verifique la configuración de NTP en R1.

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay
offset            disp
 ~209.165.200.229.INIT.          16   -        64      0      0.00
0.00              0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

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

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

Tabla 21. Configuración y verificación las listas de control de acceso (ACL)

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**
Aplicar la ACL con nombre a las líneas VTY	permit host 172.16.1.1
Permitir acceso por Telnet a las líneas de VTY	access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	show access-lists

Gráfica 11. Verificar que la ACL funcione como se espera

```
R2#
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.99.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
Extended IP access list 100
    10 permit tcp any host 209.165.200.229 eq www
    20 permit icmp any any echo-reply

R2#
```

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

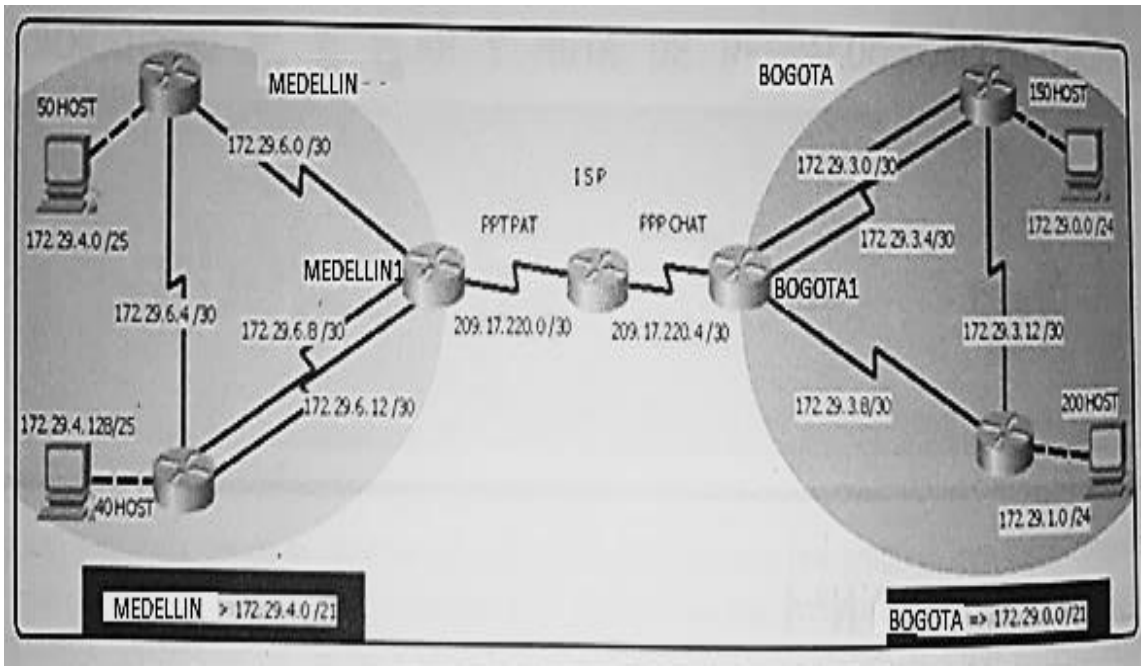
Tabla 22. Comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	ip access-list standard 2 18 permit 172.22.1.1
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

4.2 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.

Gráfica 12. Topología de red



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.

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.

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.

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

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.

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.

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.

Parte 7: Configuración del servicio DHCP.

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

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

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

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

Comenzamos con el desarrollo del escenario 2 de acuerdo a la problemática planteada.

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.

4.2.1 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.

Comandos ejecutados en el Router ISP:

```
Router>en
Router#conf t
Router(config)#hostname ISP
```

Configuramos interfaz

s0/0

```
ISP(config)#int s0/0
ISP(config-if)#description ISP-MEDELLIN1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu
ISP(config-if)#exit
```

Configuramos la otra interfaz

s0/1

```
ISP(config)#int s0/1
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
```

ISP(config-if)#clock rate 128000
ISP(config-if)#no shu
ISP(config-if)#exit

Configuramos el Protocolo OSPF V2
ISP(config-router)#router ospf
ISP(config-router)#version 2
ISP(config-router)#network 209.17.220.0

Desactivamos la Sumarización automática
ISP(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN1:

Router>en
Router#conf t
Router(config)#hostname MEDELLIN1

Configuramos interfaz s0/0 (Ruta por defecto al ISP)
MEDELLIN1(config)#interface Serial0/0
MEDELLIN1(config-if)#description MEDELLIN1-ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit

Configuramos interfaz s0/1
MEDELLIN1(config)#interface Serial0/1
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos interfaz s0/2
MEDELLIN1(config)#interface Serial0/2
MEDELLIN1(config-if)# description MEDELLIN-MEDELLIN1
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu

MEDELLIN1(config-if)#exit

Configuramos interfaz s0/3
MEDELLIN1(config)#interface Serial0/3
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos el Protocolo OSPF V2
MEDELLIN1(config-router)#router ospf
MEDELLIN1(config-router)#version 2
MEDELLIN1(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
MEDELLIN1(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN2:

Router>en
Router#conf t
Router(config)#hostname MEDELLIN2

Configuramos interfaz s0/0
MEDELLIN2(config)#interface Serial0/0
MEDELLIN2(config-if)#description MEDELLIN2-MEDELLIN1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#shutdown
MEDELLIN2(config-if)#exit

Configuramos interfaz s0/1
MEDELLIN2(config)#interface Serial0/1
MEDELLIN2(config-if)# description MEDELLIN2-MEDELLIN
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shu
MEDELLIN2(config-if)#exit

Configuramos interfaz fa0/0
MEDELLIN2(config)#interface fa0/0

MEDELLIN2(config-if)# description MEDELLIN2-PC2
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shu
MEDELLIN2(config-if)#exit

Configuramos el Protocolo RIP V2
MEDELLIN2(config-router)#router rip
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
MEDELLIN2(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN:

Router>en
Router#conf t
Router(config)#hostname MEDELLIN

Configuramos interfaz s0/0
MEDELLIN(config)#interface Serial0/0
MEDELLIN(config-if)#description MEDELLIN-MEDELLIN1
MEDELLIN(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#shutdown
MEDELLIN(config-if)#exit

Configuramos interfaz s0/1
MEDELLIN(config)#interface Serial0/1
MEDELLIN(config-if)#description MEDELLIN1-MEDELLIN
MEDELLIN(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#exit

Configuramos interfaz s0/2
MEDELLIN(config)#interface Serial0/2
MEDELLIN(config-if)#description MEDELLIN-MEDELLIN2
MEDELLIN(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN(config-if)#clock rate 128000

MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#exit
Configuramos interfaz fa0/0
MEDELLIN(config)#interface fa0/0
MEDELLIN(config-if)#description MEDELLIN-PC3
MEDELLIN(config-if)#ip address 172.29.4.2 255.255.255.128
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#exit

Configuramos el Protocolo OSPF V2
MEDELLIN(config-router)#router ospf
MEDELLIN(config-router)#version 2
MEDELLIN(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
MEDELLIN(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA1:

Router>en Router#conf t
Router(config)#hostname BOGOTA1

Configuramos interfaz s0/0 (Ruta por defecto al ISP)
BOGOTA1(config)#interface Serial0/0
BOGOTA1(config-if)#description
BOGOTA1-ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#shutdown
BOGOTA1(config-if)#exit

Configuramos interfaz s0/1
BOGOTA1(config)#interface Serial0/1
BOGOTA1(config-if)#description BOGOTA1-BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos interfaz s0/2
BOGOTA1(config)#interface Serial0/2
BOGOTA1(config-if)#description BOGOTA2-BOGOTA1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos interfaz s0/3
BOGOTA1(config)#interface Serial0/3
BOGOTA1(config-if)#description BOGOTA1-BOGOTA
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos el Protocolo RIP V2
BOGOTA1(config-router)#router rip
BOGOTA1(config-router)#version 2
BOGOTA1(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA1(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA2:
Router>en
Router#conf t
Router(config)#hostname BOGOTA2

Configuramos interfaz s0/0
BOGOTA2(config)#interface Serial0/0
BOGOTA2(config-if)#description BOGOTA2-BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#shutdown
BOGOTA2(config-if)#exit

Configuramos interfaz s0/1
BOGOTA2(config)#interface Serial0/1

BOGOTA2(config-if)#description BOGOTA1-BOGOTA2
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos interfaz s0/2
BOGOTA2(config)#interface Serial0/2
BOGOTA2(config-if)#description BOGOTA2-BOGOTA
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos interfaz fa0/0
BOGOTA2(config)#interface fa0/0
BOGOTA2(config-if)#description BOGOTA2-PC0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos el Protocolo RIP V2
BOGOTA2(config-router)#router rip
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA2(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA:
Router>en
Router#conf t
Router(config)#hostname BOGOTA

Configuramos interfaz s0/0
BOGOTA(config)#interface Serial0/0
BOGOTA(config-if)#description BOGOTA-BOGOTA1
BOGOTA(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#shutdown

BOGOTA(config-if)#exit

Configuramos interfaz s0/1
BOGOTA(config)#interface Serial0/1
BOGOTA(config-if)#description BOGOTA-BOGOTA2
BOGOTA(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#no shu
BOGOTA(config-if)#exit

Configuramos interfaz fa0/0
BOGOTA(config)#interface fa0/0
BOGOTA(config-if)#description BOGOTA-PC1
BOGOTA(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#no shu
BOGOTA(config-if)#exit

Configuramos el Protocolo OSPF V2
BOGOTA(config-router)#router ospf
BOGOTA(config-router)#version 2
BOGOTA(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA(config-router)#no auto-summary

Comandos usados para la ruta estática en ISP:

ISP>en
ISP#conf t
ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/1
ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/1
ISP(config)#exit

Comandos usados para la ruta estática predeterminada hace la red de MEDELLIN:

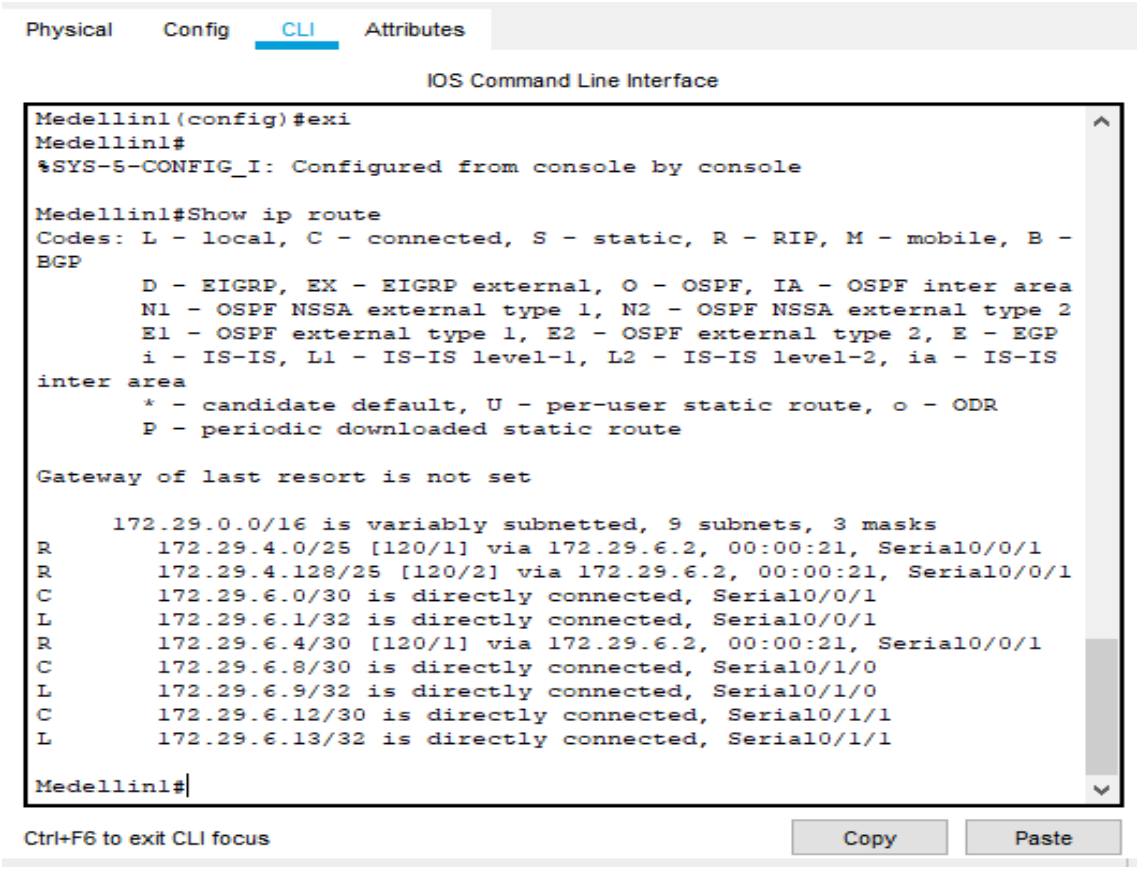
MEDELLIN1>en
MEDELLIN1#conf t

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

4.2.2 Parte 2.Tabla de enrutamiento

Enrutamiento de MEDELLIN: Desde PC2 a PC3

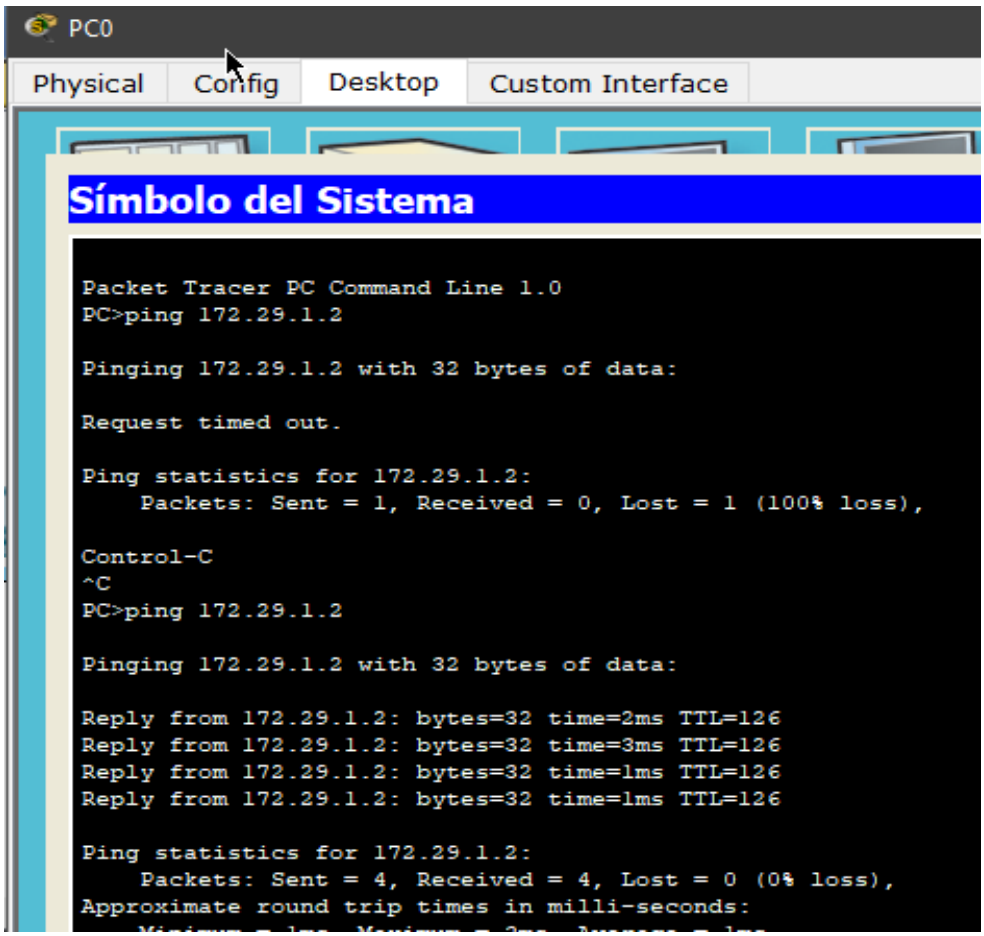
Gráfica 13. Enrutamiento



Comandos usados para la ruta estática predeterminada hace la red de BOGOTA:

```
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#exit
```

Gráfica 14. Prueba de ping realizadas en la red de BOGOTÁ: Desde PC0 a PC1



4.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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.

R// Comando usados para evitar la propagación del protocolo OSPF innecesario por ciertas interfaces de cada Router de la red:

En router MEDELLIN1:
MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#router rip
MEDELLIN1(config)#versión 2
MEDELLIN1(config-router)#Passive-interface s0/1

En router MEDELLIN2:
MEDELLIN2>en
MEDELLIN2#conf t
MEDELLIN2(config)#router rip
MEDELLIN2(config)#versión 2
MEDELLIN2(config-router)#Passive-interface fa0/0

En router MEDELLIN:
MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#router rip
MEDELLIN(config)#versión 2
MEDELLIN(config-router)#Passive-interface fa0/0
MEDELLIN(config-router)#Passive-interface s0/2

En router BOGOTA1:
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#router rip
BOGOTA1(config)#versión 2
BOGOTA1(config-router)#Passive-interface s0/0

En router BOGOTA2:
BOGOTA2>en
BOGOTA2#conf t
BOGOTA2(config)#router rip
BOGOTA2(config)#versión 2
BOGOTA2(config-router)#Passive-interface fa0/0
BOGOTA2(config-router)#Passive-interface S0/2

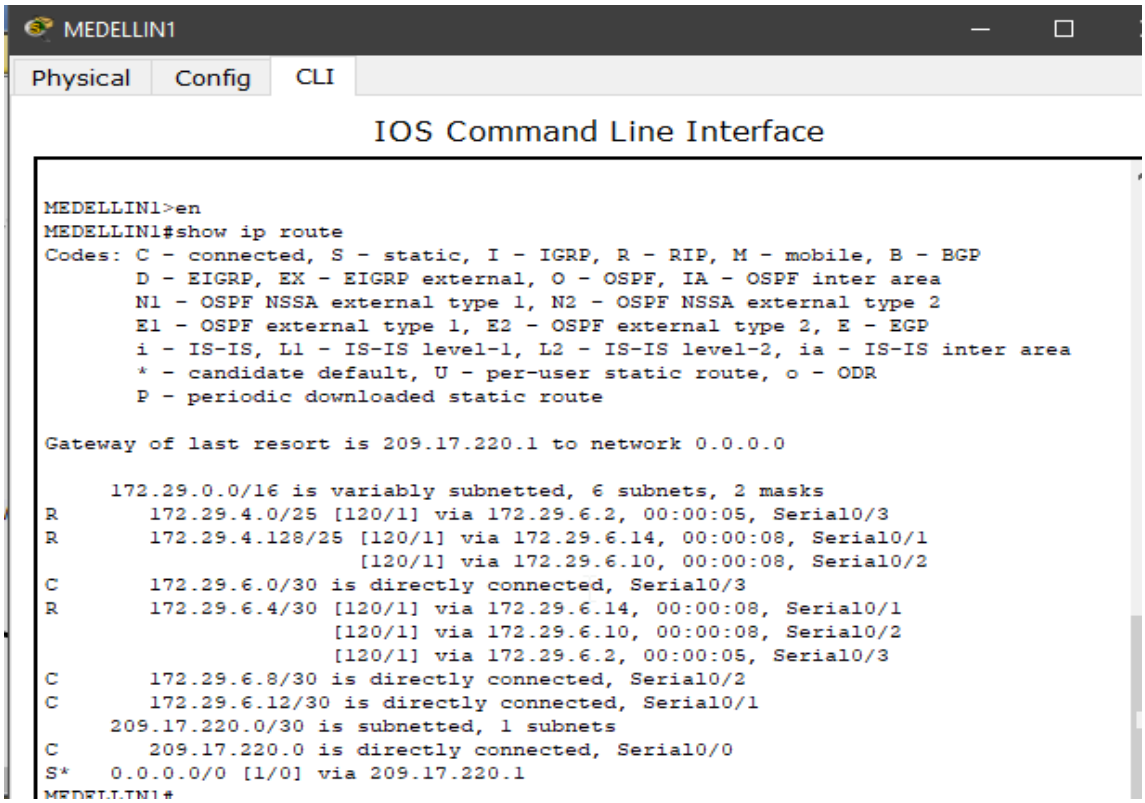
En router BOGOTA:
BOGOTA>en
BOGOTA#conf t
BOGOTA(config)# router rip
BOGOTA(config)# version 2
BOGOTA(config-router)#Passive-interface fa0/0

4.2.4 Parte 4: Verificación del protocolo OSPF.

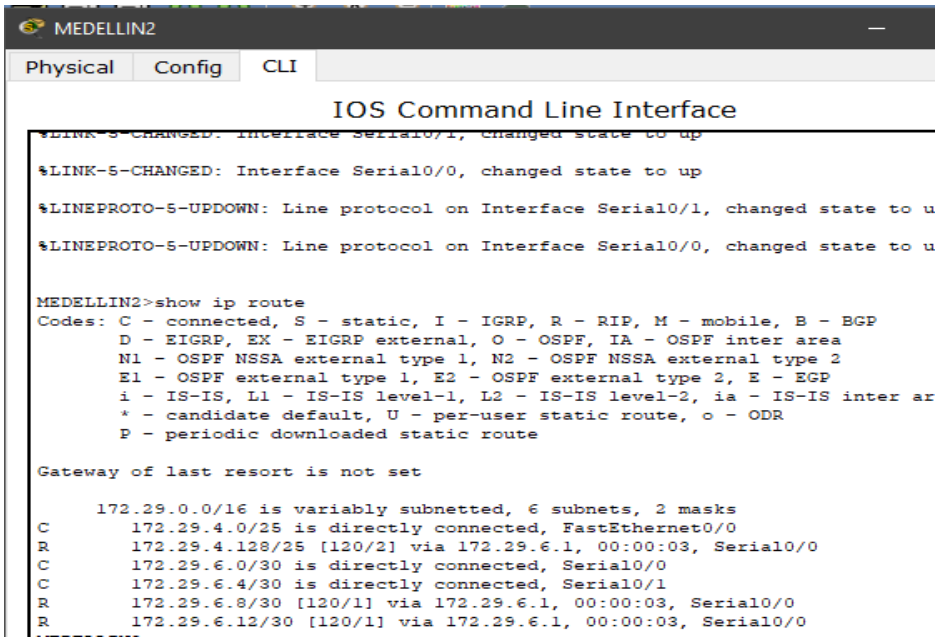
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.
b. Verificar y documentar la base de datos de OSPF de cada router, donde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

Se verifica con el comando show ip route en cada router:

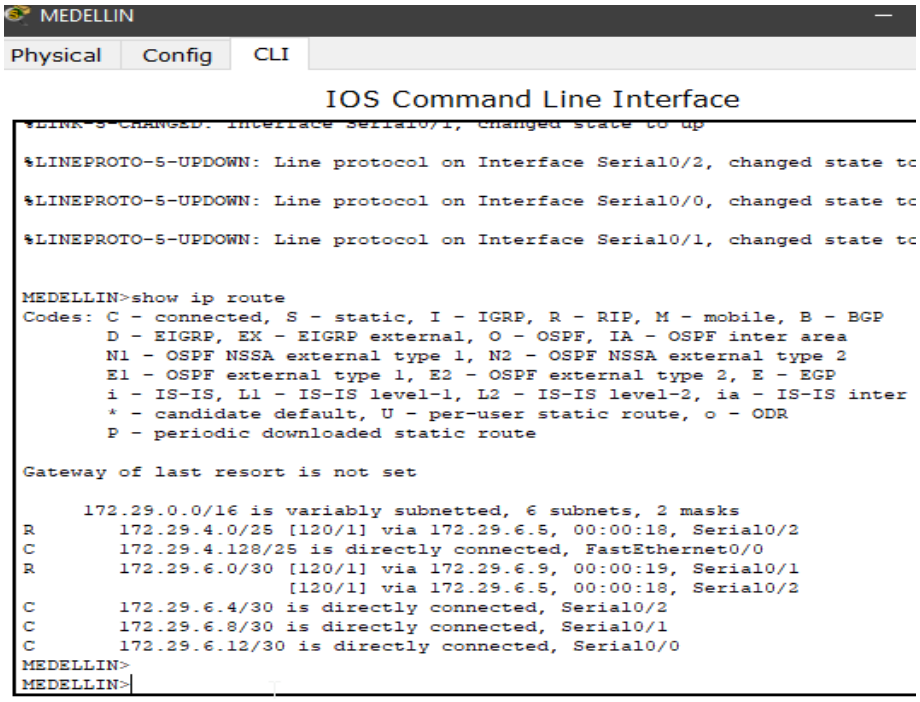
Gráfica 15. MEDELLIN1#show ip route



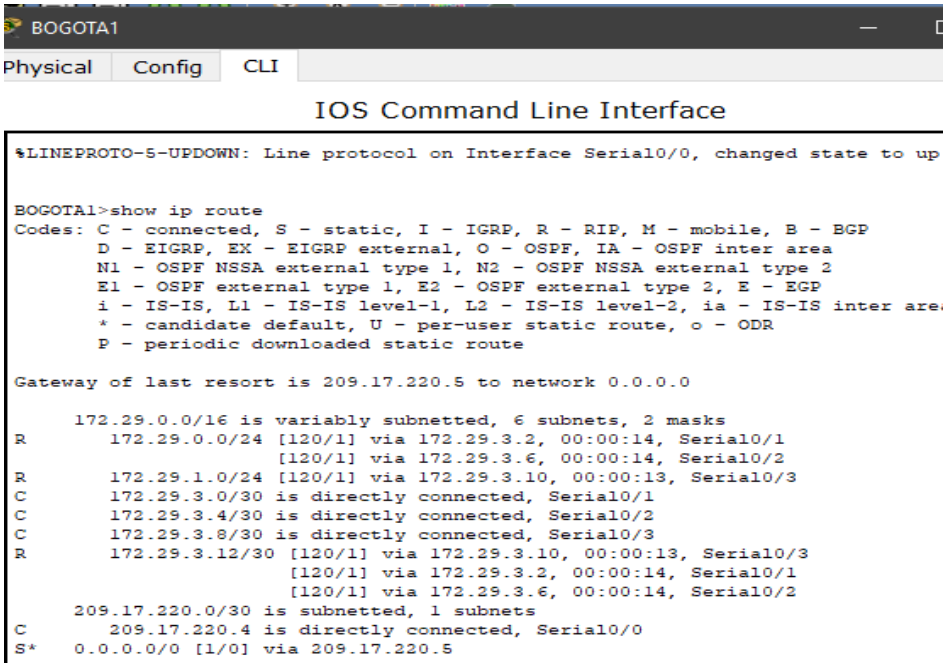
Gráfica 16. MEDELLIN2#show ip route



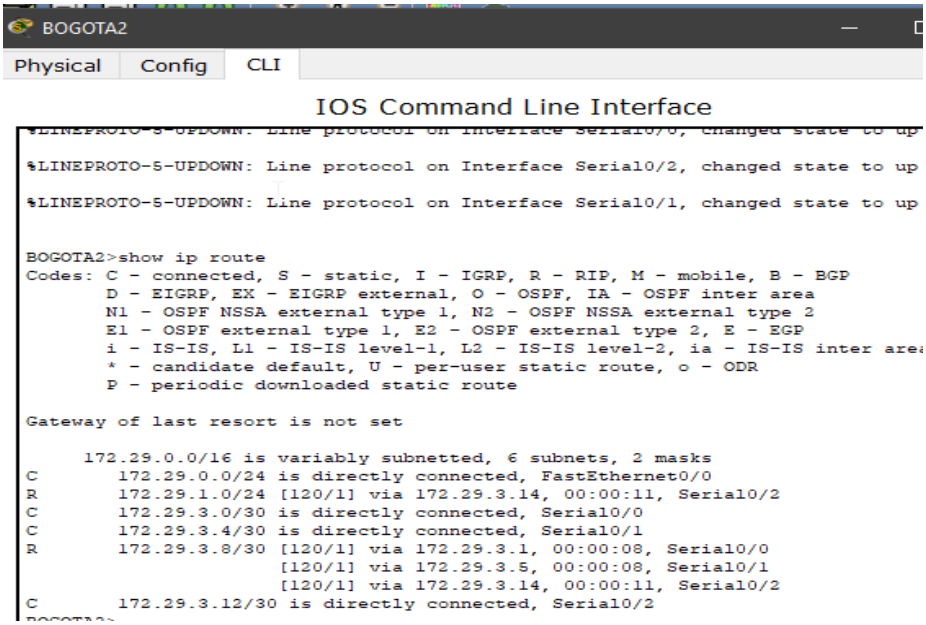
Gráfica 17. MEDELLIN#show ip route



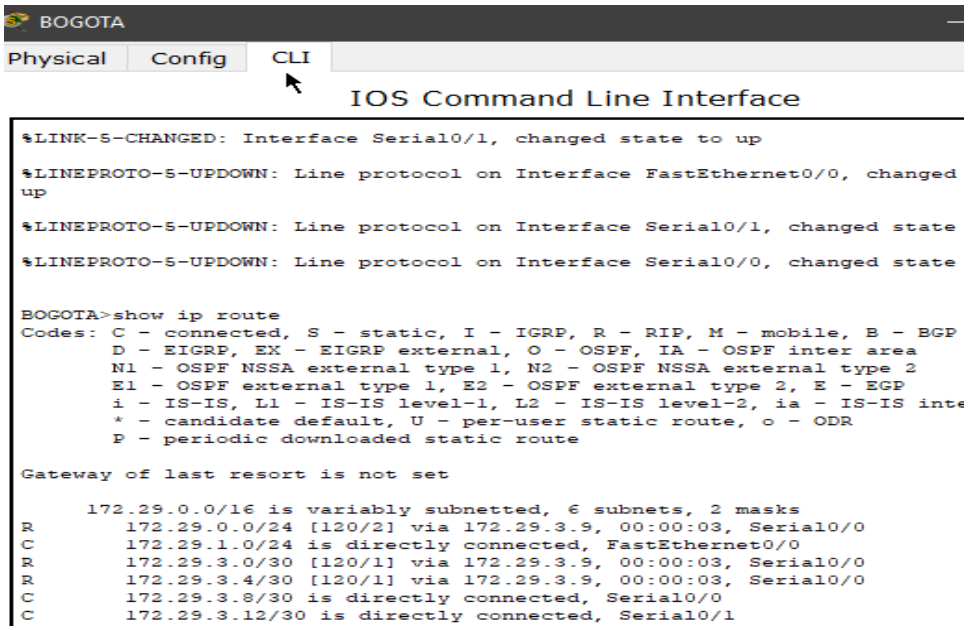
Gráfica 18. BOGOTA1# show ip route



Gráfica 19. BOGOTA2#show ip route



Gráfica 20. BOGOTA#show ip route



4.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

R// Iniciamos con la configuración de los router de ISP, MEDELLIN1 Y BOGOTA1 para que usen en ciertas interfaces el método de encapsulación PPP, para posteriormente realizar la autenticación PAT en Medellin1 y CHAT en Bogota1:

Habilitación método encapsulamiento PPP:

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#int s0/0
MEDELLIN1(config-if)#encapsulation PPP
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

BOGOTA1>en
BOGOTA1#conf t BOGOTA1(config)#int s0/0
BOGOTA1(config-if)#encapsulation PPP
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

ISP>en ISP#conf t
ISP(config)#int s0/0
ISP(config-if)#encapsulation PPP
ISP(config-if)#no shu
ISP(config-if)#exit
ISP(config)#int s0/1
ISP(config-if)#encapsulation PPP
ISP(config-if)#no shu
ISP(config-if)#exit

Habilitación autenticación PAT DE PPP entre MEDELLIN1 Y EL ISP:

Configuración PAT DE PPP en ISP CON MEDELLIN1:

ISP>en ISP#conf t
ISP(config)#username

MEDELLIN1 secret
MEDELLIN ISP(config)#int se0/0

ISP(config-if)#PPP authentication PAT
ISP(config-if)#PPP PAT sent-username
ISP password ISP
ISP(config-if)#exit

Configuración PAT de PPP en MEDELLIN1 CON ISP:

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#username ISP secret ISP
MEDELLIN1(config)#int se0/0
MEDELLIN1(config-if)#PPP authentication PAT
MEDELLIN1(config-if)#PPP PAT sent-username MEDELLIN1
password MEDELLIN
MEDELLIN1(config-if)#exit

Habilitación autenticación CHAT DE PPP entre BOGOTA1 Y EL ISP:

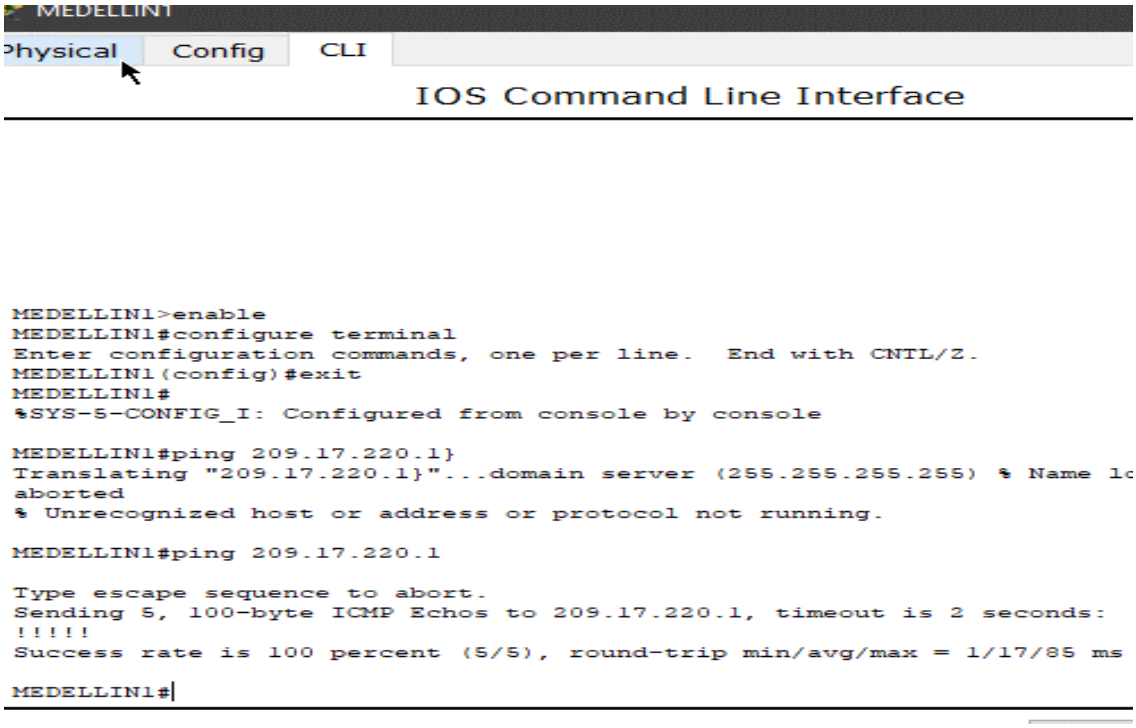
Configuración CHAT DE PPP en ISP CON BOGOTA1:

ISP>en
ISP#conf t
ISP(config)#usernameBOGOTA1 secret BOGOTA1
ISP(config)#int se0/1
ISP(config-if)#PPP authentication CHAT
ISP(config-if)#exit

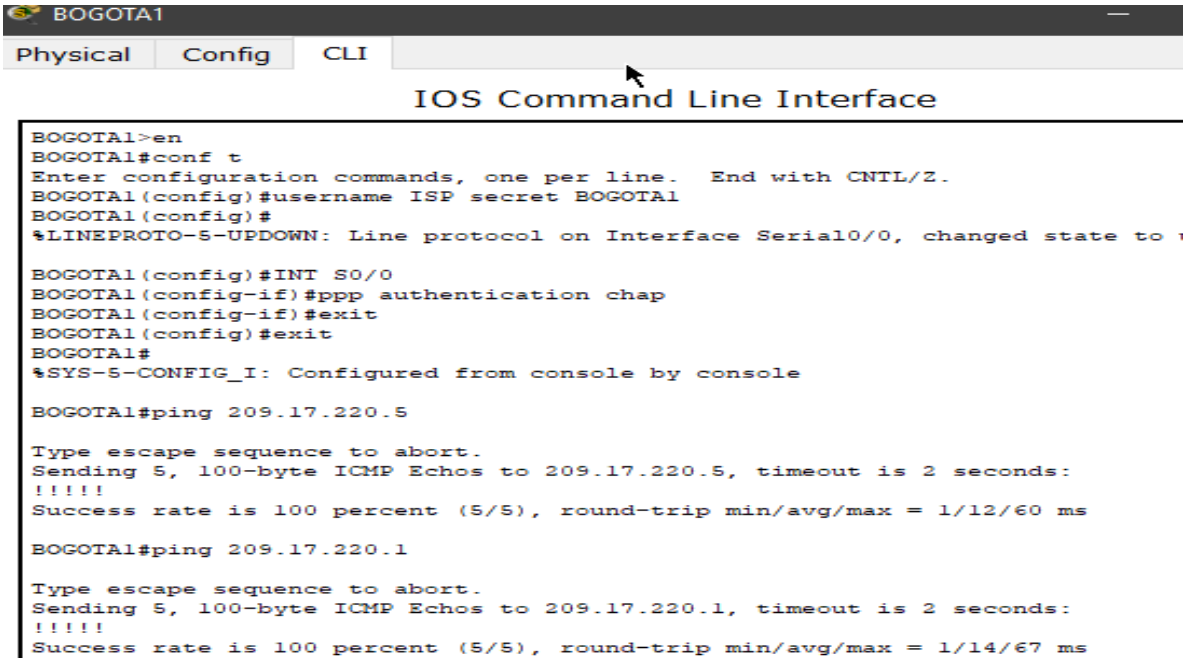
Configuración CHAT de PPP en BOGOTA1 CON ISP:

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#username ISP secret BOGOTA1
BOGOTA1(config)#int se0/0
BOGOTA1(config-if)#PPP authentication
CHAT BOGOTA1(config-if)#exit

Gráfica 21. Verificación de autenticación por PAT EN MEDELLIN Por ping hacia ISP



Gráfica 22. Verificación de autenticación por CHAP EN BOGOTA1 Por ping hacia ISP



4.2.6 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.

R// **Iniciamos con la configuración NAT en MEDELLIN1:**

MEDELLIN1>en
MEDELLIN1#conf t

Con este comando definidos la red de los PC's que se desean que sean empleadas en el PAT"

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

Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP"

MEDELLIN1(config)#Ip nat inside source list HOST interface s0/0 overload
MEDELLIN1(config)#int s0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/2
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/3
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat translation

Iniciamos con la configuración NAT en BOGOTA1:

BOGOTA1>en
BOGOTA1#conf t

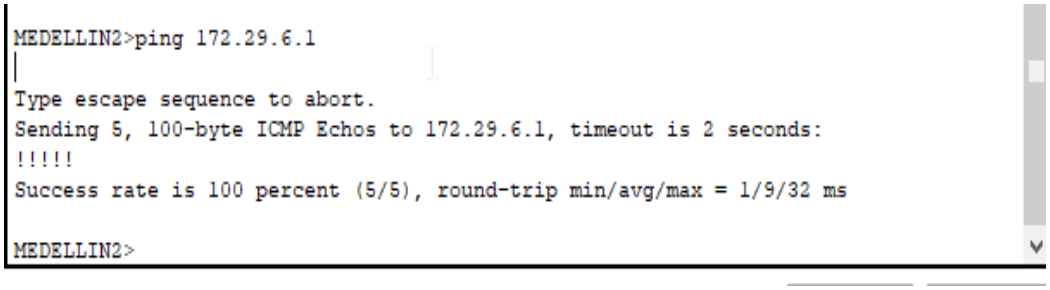
Con este comando definidos la red de los PC's que se desean que sean empleadas en el PAT"

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

Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP"

BOGOTA1(config)#Ip nat inside source list HOST interface s0/0 overload
BOGOTA1(config)#int s0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1|(config)#int s0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/2
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/3
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#exit
BOGOTA1#show ip nat translation

Gráfica 23. Verificamos ping entre MEDELLIN2 y MEDELLIN1



4.2.7 Parte 7: Configuración del servicio DHCP.

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

R// Iniciamos configurando en DHCP en el Router MEDELLIN2

MEDELLIN2>en
MEDELLIN2#conf t

-Se definen que direcciones IP no deben ser entregadas por el DHCP debido a que estas ya están siendo utilizadas.

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(dhcp-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

Definimos la red de lP's que serán arrendadas cuando el host solicite una IP.

MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128

Definimos la dirección del Gateway para los Host.

MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN2(dhcp-config)#exit

Continuamos configurando el DHCP, como el router MEDELLIN tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de MEDELLIN2:

MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#Int fa0/0
MEDELLIN(config-if)#ip helper-addres 172.29.6.5
MEDELLIN(config-if)#exit

Iniciamos configurando en DHCP en el Router BOGOTA2

```
BOGOTA2>en
BOGOTA2#conf t
```

-Se definen que direcciones IP no deben ser entregadas por el DHCP debido a que estas ya están siendo utilizadas.

```
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(dhcp-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(dhcp-config)#exit
BOGOTA2(config)#ip dhcp pool BOGOTA
```

-Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.

```
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
```

-Definimos la dirección del Gateway para los Host.

```
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
BOGOTA2(dhcp-config)#exit
```

Continuamos configurando el DHCP, como el router BOGOTA tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de BOGOTA2:

```
BOGOTA>en
BOGOTA#conf t
BOGOTA(config)#Int
fa0/0
BOGOTA(config-if)#ip helper-addres 172.29.3.13
BOGOTA(config-if)#exit
```

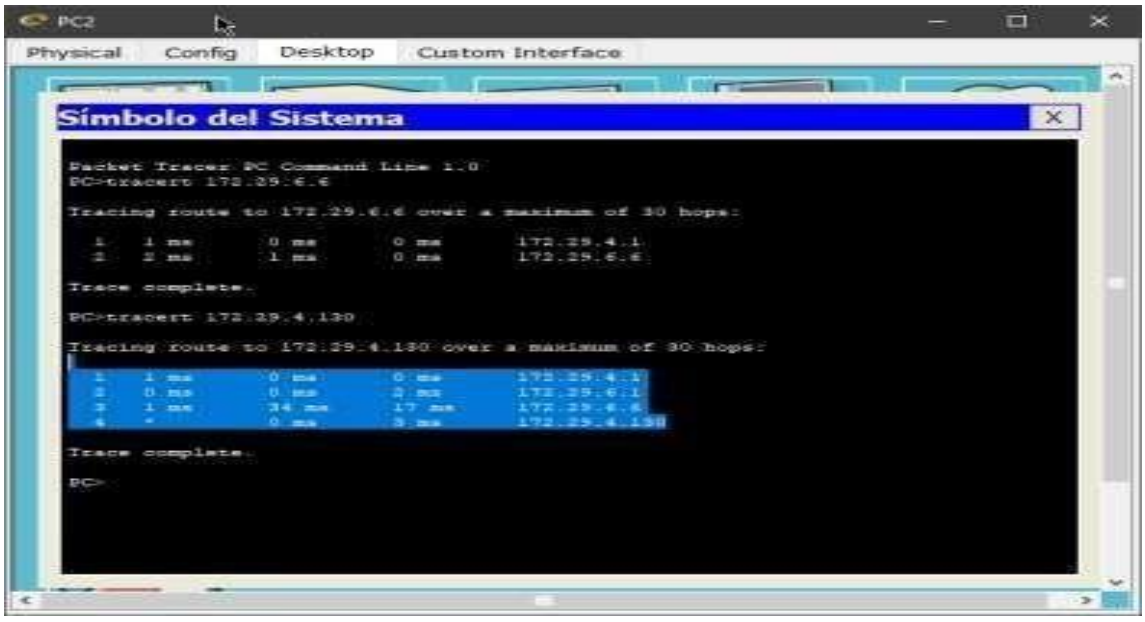
Verificamos que en el modo grafico del PC2 en la red de MEDELLIN, cuando le asignamos la configuración de ip por DHCP automáticamente le asigna

una ip dentro del rango configurado anteriormente.

Gráfica 24. DHCP Medellín

Al estar el router en modo dhcp el router MEDELLIN2, le asigna aleatoriamente una ip al PC2, y podemos confirmar por un ping hacia el PC3 que la asignación es la correcta por que hay conectividad en la red, lo mismo sucede en la red de Bogota con el PC0 y el Router BOGOTA2.

Gráfica 25. Ping PC2 a PC3



Por ultimo se asignan claves de seguridad a cada router, este paso se

realiza de ultimo para agilizar el acceso a los router mientras se hacían los demás puntos.

R// Configuracipon en Router ISP:

```
ISP>en
ISP#conf t
ISP(config)#enable secret ISP
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd #Prohibido el acceso no autorizado!#
ISP(config)#exit
```

Configuracipon en Router MEDELLIN1:

```
MEDELLIN1>en
MEDELLIN1#consf t
MEDELLIN1(config)#enable secret MEDELLIN1
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN1(config)#exit
```

Configuracipon en Router MEDELLIN2:

```
MEDELLIN2>en
MEDELLIN2#conf t
MEDELLIN2(config)#enable secret MEDELLIN2
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
```

MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN2(config)#exit

Configuracipon en Router MEDELLIN:

MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#enable secret MEDELLIN
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Prohibido el acceso no
autorizado!# MEDELLIN(config)#exit

Configuracipon en Router BOGOTA1:

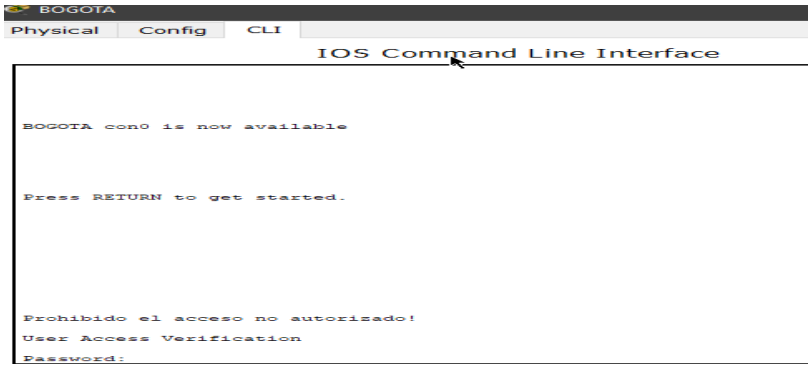
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#enable secret
BOGOTA1
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#line vty 0 4
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA1(config)#exit

Configuracipon en Router BOGOTA2:

BOGOTA2>en
BOGOTA2#conf t
BOGOTA2(config)#enable secret
BOGOTA2
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA2(config)#exit

Configuracipon en Router BOGOTA:
BOGOTA>en
BOGOTA#conf t BOGOTA(config)#enable secret BOGOTA
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Prohibido el acceso no
autorizado!#
BOGOTA(config)#exit

Gráfica 26. Routing Bogotá



5 CONCLUSIONES

Durante el desarrollo de esta prueba de habilidades práctica propuesta como fundamento para la obtención del diplomado de grado como ingeniero de sistemas, pude evidenciar los conocimientos y destrezas adquiridos en el curso ya que obtuve conocimientos básicos sobre la configuración de Routers, Switch, Servidores y demás componentes de una red, por medio de comandos que me permiten simular su configuración.

El aprendizaje como estudiante de carrera profesional en Ing. De Sistemas, el Curso de CISCO ha aportado a mis conocimientos en gran medida, gracias a eso mi perfil se vuelve más competente en el ámbito laboral y personal, gracias a que el conocimiento adquirido me abre mas puertas de trabajo para alcanzar mis objetivos y metas.

6 BIBLIOGRAFÍA

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

Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

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

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

Temática: DHCP

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

Temática: Enrutamiento Dinámico

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

Temática: Listas de control de acceso

CISCO. (2014). 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

Temática: OSPF de una sola área

CISCO. (2014). 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

Temática: Traducción de direcciones IP para IPv4

CISCO. (2014). 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