SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS COORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SVEN ARLEY CASTILLO LIEVANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERIA DE SISTEMAS

NIEVA HUILA

2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS COORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SVEN ARLEY CASTILLO LIEVANO

Trabajo opción de grado como

Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERIA DE SISTEMAS

NEIVA HUILA

2020

TABLA DE CONTENIDO

Introducción 3

Escenario 1 11

Parte 1: Inicializar dispositivos 12

Paso 1: Inicializar y volver a cargar los routers y los switches 12

Parte 2: Configurar los parámetros básicos de los dispositivos 13

Paso 1: Configurar la computadora de Internet 13

Paso 2: Configurar R1 14

Paso 3: Configurar R2 16

Paso 4: Configurar R3 20

Paso 5: Configurar S1 24

Paso 6: Configurar el S3 25

Paso 7: Verificar la conectividad de la red 27

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 29

Paso 1: Configurar S1 29

Paso 2: Configurar el S3 31

Paso 3: Configurar R1 34

Paso 4: Verificar la conectividad de la red 36

Parte 4: Configurar el protocolo de routing dinámico RIPv2 37

Paso 1: Configurar RIPv2 en el R1 37

Paso 2: Configurar RIPv2 en el R2 38

Paso 3: Configurar RIP2 en el R2 40

Paso 4: Verificar la información de RIP 41

Parte 5: Implementar DHCP y NAT para IPv4 43

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 43

Paso 2: Configurar la NAT estática y dinámica en el R2 46

Paso 3: Verificar el protocolo DHCP y la NAT estática 48

Parte 6: Configurar NTP 51

Parte 7: Configurar y verificar las listas de control de acceso (ACL) 53

Paso 1: Restringir el acceso a las líneas VTY en el R2 53

Paso 2: Comando de CLI 54
Escenario 2 58
Trabajo Inicial 59
Paso 1: Configurar los parámetros básicos de los dispositivos. 59
Paso 2: Conexión física de topología de red 64
Paso 3: Configuración de direccionamiento IP 66
Parte 1: Configuración del enrutamiento 72
Paso 1: Configuración de OSPF 72
Paso 2: Configuración ruta distribuida en OSPF 74
Paso 3: Configurar ruta Sumarizada ISP 74
Parte 2: Tabla de Enrutamiento 76
Paso 1: Verificar tablas de enrutamiento 76
Paso 2: Verificar balanceo de carga 79
Paso 3: Ruta por defecto OSPF 80
Paso 4: Verificación rutas directas OSPF 80
Paso 5: Rutas Redundantes 81
Paso 6: Verificar tabla de enrutamiento ISP 81
Parte 3: Deshabilitar la propagación del protocolo OSPF. 82
Paso 1: Deshabilitar Propagación OSPF 82
Parte 4: Verificación del protocolo OSPF. 84
Paso 1: Verificar y documentar opciones de enrutamiento 84
Paso 2: Verificar y documentar base de datos OSPF 85
Parte 5: Configurar encapsulamiento y autenticación PPP 86
Paso 1: Autenticación PAT Medellin1 86
Paso 2: Autenticación CHAT Bogota1 87
Paso 1: Verificación de conexión 90
Paso 2: Configuración NAT Bogota1 91
Paso 3: Configuración NAT Medellin1 92
Parte 7: Configuración del servicio DHCP. 95
Paso 1: Configurar Bogota2 como servidor DHCP 95
Paso 2: Habilitar Broadcast Bogota3 95

Paso 3: Configurar Medellin2 como servidor DHCP.....95
Paso 4: Habilitar Broadcast Medellin3.....95
Anexo 1 – Descarga Escenarios Packet Tracer.....104

LISTA DE TABLAS

Pág.

Tabla 1. Comandos de IOS....12
Tabla 2. Direccionamiento Servidor de Internet....13
Tabla 3 – Configuración R1....15
Tabla 4 - Configuración R2....18
Tabla 5 - Configuración R3....21
Tabla 6 - Configuración S1....25
Tabla 7 - Configuración S3....26
Tabla 8 - Conectividad de la red....27
Tabla 9 - Configuración de seguridad, VLAN y routing del Switch 1....30
Tabla 10 - Configuración de VLAN, seguridad y routing de Switch 3....33
Tabla 11 - Configuración de Routing R1....35
Tabla 12 - Verificación Routing R1....36
Tabla 13 - Configuración RIPv2 en R1....38
Tabla 14 - Configuración de RIPv2 en R2....39
Tabla 15 - Configuración de RIPv3 en R2....40
Tabla 16 - Verificación de información RIP v2....41
Tabla 17 - Configuración DHCP R1 para VLAN 21 y 23....44
Tabla 18 - Configuración de NAT estática y dinámica R2....47
Tabla 19 - Verificación DHCP y NAT Estática....48
Tabla 20 - Configuración NTP....51
Tabla 21 - Configuración y Verificación de ACL....53
Tabla 22 - Comandos CLI....55
Tabla 23 - Configuración inicial dispositivos....59
Tabla 24 - Tabla de enrutamiento Escenario 2....64
Tabla 25 - Configuración direccionamiento IP....66
Tabla 26 - Configuración de OSFP....72

Tabla 27 - Configuración de ruta distribuible OSPF.....74
Tabla 28 - Ruta Sumarizada ISP 74
Tabla 29 - Deshabilitación propagación OSPF.....83
Tabla 30 - Configuración PAT Bogota1 - CHAT Medellin2 87
Tabla 32 - Configuración PAT.....92
Tabla 31 - Configuración DHCP.....95

Lista de Figuras

Pág.

Figura 1 - Topología de Red 11
Figura 2 - Verificación de eliminación VLAN Switch.....13
Figura 3 - Ping R1 a R2 28
Figura 4 - Ping R2 a R3 28
Figura 5 -Ping PC Internet a Gateway Predeterminado 29
Figura 6 - Ping S1 a VLAN 99 y VLAN 21.....36
Figura 7 - Ping S3 - VLAN 99 y VLAN 23.....37
Figura 8 - Verificación ip Protocols.....42
Figura 9 - Verificación Base de datos RIP 42
Figura 10 - Verificación RIP en ejecución 43
Figura 11 - Verificación DHCP PC-A.....48
Figura 12 - Verificación DHCP PC-C 49
Figura 13 - Verificación de conexión DHCP entre PC-A y PC-B 49
Figura 14 - Verificación de NAT 50
Figura 15 - Verificación traducción NAT R2 50
Fiigura 16 - Verificación de NTP en R1.....52
Figura 17 - Verificación ACL ADMIN-MGT.....54
Figura 18 - Verificación access-list R2 55
Figura 19 - Verificación access-list.....56
Figura 20 - Verificación ACL en Interface 56
Figura 21 - Verificación NAT Translation 57
Figura 22 - Topología Escenario 2 58
Figura 23 - Tabla de enrutamiento ISP 76
Figura 24 - Tabla de enrutamiento Medellin1.....76
Figura 25 - Tabla de enrutamiento Medellin2.....77
Figura 26 - Tabla de enrutamiento Medellin3.....77

Figura 27 - Tabla de enrutamiento Bogota1.....78
Figura 28 - Tabla de enrutamiento Bogota2.....78
Figura 29 - Tabla de enrutamiento Bogota3.....79
Figura 30 – Verificación de balanceo de carga Medellin1 - Bogota1 79
Figura 31 – Verificación ruta por defecto Medellin1 y Bogota1 80
Figura 32 - Verificación rutas directas y OSPF Medellin2 y Bogota2 81
Figura 33 - Verificación enrutamiento ISP.....82
Figura 34 - Verificación información OSPF Medellin1.....85
Figura 35 - Verificación información OSPF Bogota2.....85
Figura 36 - Verificación base de Datos OSFP Medellin1 86
Figura 37 - Verificación de Encapsulamiento y autenticación ISP 89
Figura 38 - Verificación autenticación Medellin1.....89
Figura 39 - Verificación autenticación Bogota1.....90
Figura 40 - Verificación de conexión sin NAT 91
Figura 41 - Verificación NAT Bogota1.....94
Figura 42 - Verificación NAT Medellin1.....94
Figura 43 - Verificación estado DHCP Bogota2 97
Figura 44 - Verificación estado DHCP Medellin2 98
Figura 45- Verificación DHCP PC-Medellin-LAN1.....98
Figura 46 - Verificación DHCP PC-Medellin-LAN2 99
Figura 47 - Verificación DHCP PC-Bogota-LAN1 99
Figura 48 - Verificación DHCP PC-Bogota-LAN2 100

INTRODUCCIÓN

Teniendo en cuenta la importancia de este diplomado tanto como opción de grado y ayuda para fortalecer los conocimientos adquiridos en el mismo es de vital importancia resumir que esta herramienta de trabajo en la cual venimos laborando varios ejercicios planteados y propuestos en la plataforma cisco nos permiten despejar miles de dudas las cuales nos asechan en el momento de una configuración de red puesto que en esta misma plataforma podemos salir de cualquier dudad preguntando a los apreciados instructores de la universidad los cuales están dispuestos muy amable mente a colaborarnos y ayudarnos en cualquier duda o complejidad que tengamos al momento de realizar la programación de dichas redes ya que al querer formar parte de este gran campo como lo es la ingeniería de sistemas la cual abarca muchos ámbitos específicos y no específicos al tratarse de una carrera que requiere una gran retro alimentación puesto que la tecnología cada día avanza más y es una obligación mantenernos actualizados, ya que si no lo realizamos como lo plateamos en los equipos que no son actualizados o repotenciados quedaríamos obsoletos ante esta bella carrera o profesión que decidimos hacer parte de nuestras vidas .

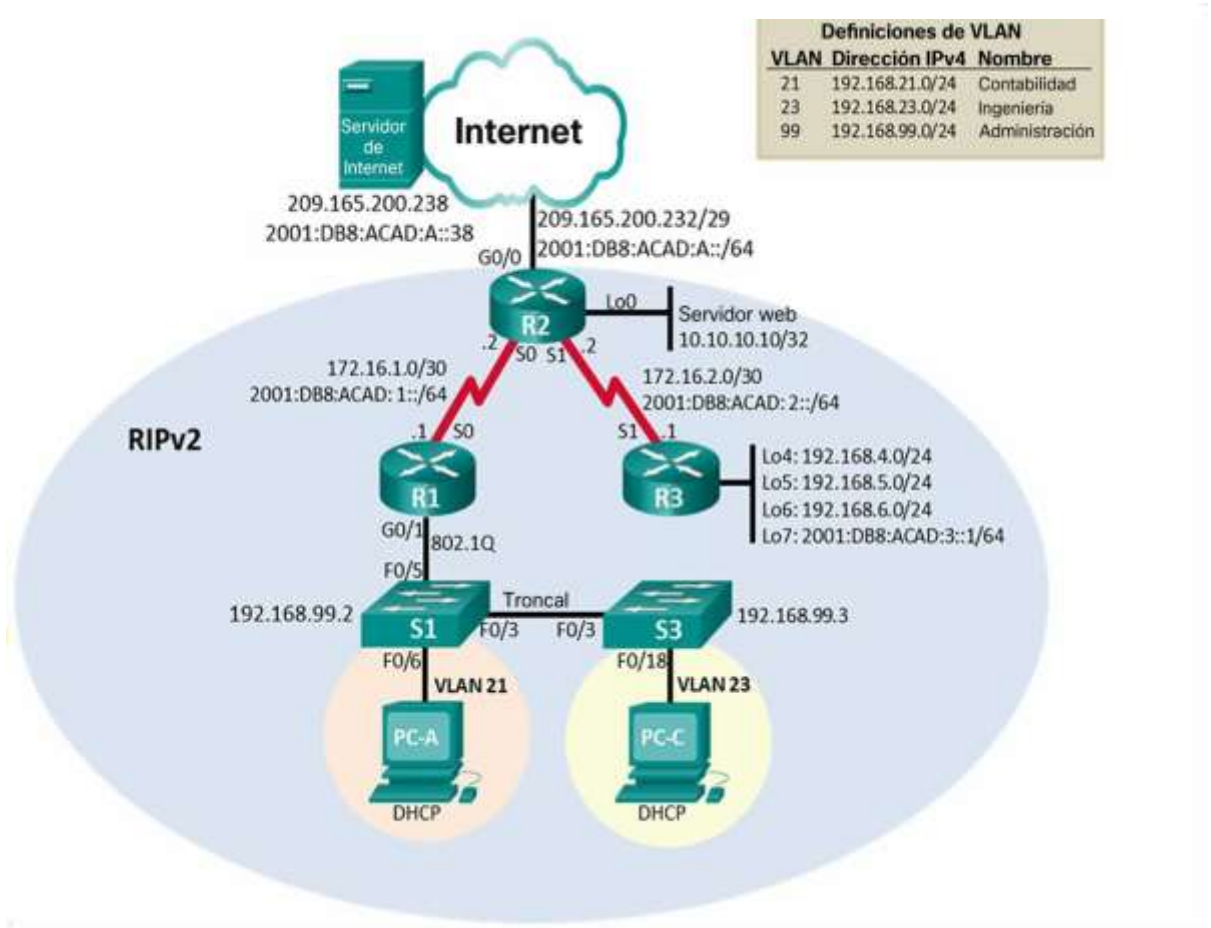
En este diplomado el cual decidimos tomar como opción de grado tenemos planteados dos casos o escenarios en el cual nosotros como estudiantes debemos desarrollar ya que son temas observados en la plataforma cisco a los cuales debemos brindar una solución con la ayudad de las herramientas facilitadas por la plataforma y las ayudas de lo los instructores o coordinadores de curso más los conocimientos adquiridos en el mismo a lo largo de este diplomado y llegando a dar la mejor solución de estos dos escenarios propuestos.

ESCENARIO 1

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

Topología

Figura 1 - Topología de



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.

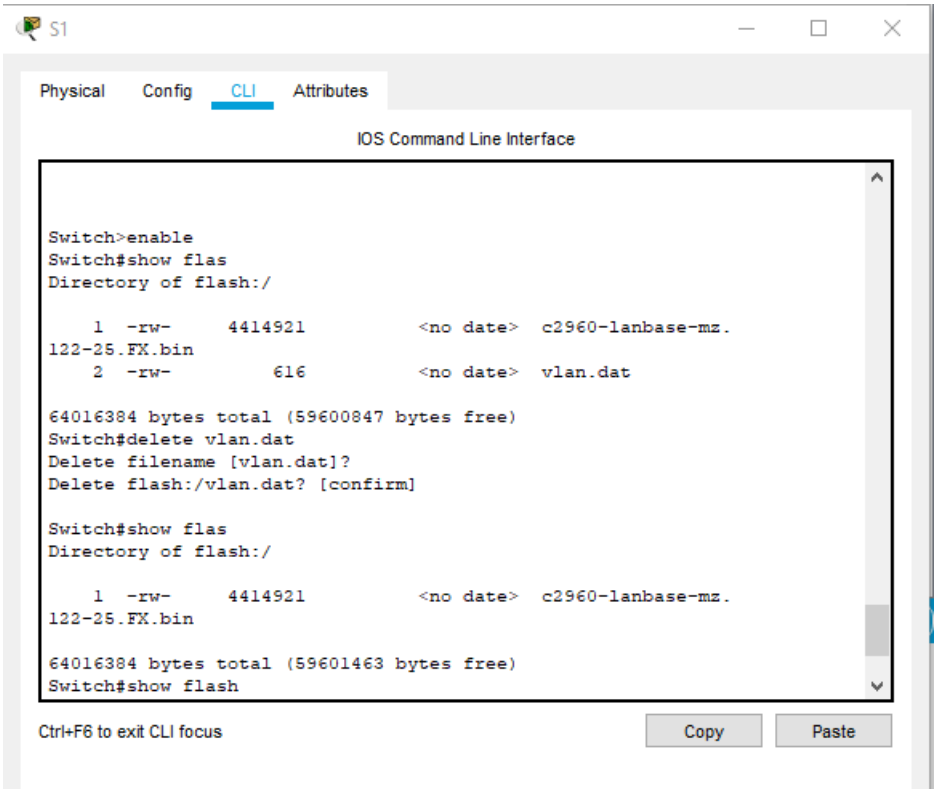
Para eliminar las configuraciones de inicio se elimina el archivo de configuración inicial para los dispositivos **startup-config** y eliminar las tablas VLAN para Routers las Base MAC para Switch, al realizar estos pasos reiniciamos el dispositivo para completar la acción

Al realizar los ejercicios de la tabla1 debemos acceder a los dispositivos en modo privilegiado y ejecutar comandos de IOS aceptando los mensajes de confirmación generados por la acción de estos.

Tabla 1. Comandos IOS

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router# erase startup-config Switch Router# delete nvram Router# delete flash:vlan.dat Router# copy running-config 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 flash: 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 flash

Figura 2 - Verificación de eliminación VLAN Switch



Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Configuración del servidor de Internet :

Realizamos la configuración de la PC-A configuramos direccionamiento IPv4 basado en la información de la tabla 2 de direccionamiento .

Tabla 2. Direccionamiento Servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248

Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Nota: de pronto 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

Configuración para R1:

Para la configuración inicial de R1 implementaremos algunas medidas de seguridad y optimizaremos el rendimiento; para proceder con las configuraciones se ingresa al modo configuración global desde ahí realizaremos la configuración del mensaje de acceso restringido para usuarios y procedemos a asignar contraseñas de seguridad al acceso modo privilegiado de consola y VTY activar el inicio de sesión con contraseñas y para concluir desactivamos la resolución de nombres (DNS).

Para evitar que algunos de estos mensajes de estado nos interrumpan el ingreso de comandos o no nos permitan la visualización de información, se configura el comando **logging synchronous** para el acceso de consola.

Llevamos a cabo la asignación de contraseñas y usamos el comando **password** el cual nos permite asignar la contraseña en texto plano, es decir, sin utilizar algoritmos de encriptación ya que refuerza la seguridad de las mismas contraseñas del dispositivo se habilita el servicio de encriptación **password-encryption**, el cual me permite encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado es **class** y para consola y VTY **cisco** usamos el comando **secret** para cifrar la contraseña de exec privilegiado y el comando **password** para los demás.

Para configurar el direccionamiento IPV4 e IPv6 de los dispositivos de la información de la topología propuesta debemos ingresar y estar dentro del modo de configuración global para poder seleccionar la interfaz e implementar la configuración, cada interfaz debe tener una dirección IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez ya configurada la interfaz tiene que quedar activa.

Se realizan las configuraciones de las rutas predeterminadas IPV4 y IPV6 las cuales me permitan enviar tráfico de red desconocido al router perimetral cuyo caso es R2 el que usaremos en las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red :: prefijo /0 e IPv6 del siguiente salto para IPv6.

Finaliza el procedimiento de configuración en modo privilegiado y procedemos a copiar la configuración actual como configuración de inicio usando el comando **copy running-config startup-config.**
Para aplicar esta configuración mencionada se ejecutan los comandos establecidos dentro de la especificación Tabla 3

Tabla 3 – Configuración R1

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

	R1(config-if)# login R1(config-if)# exit
Contraseña de acceso Telnet	R1(config)# line VTY 0 4 R1(config-if)# password cisco R1(config-if)# login R1(config-if)# exit
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Mensaje MOTD	R1(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	R1(config)# interface S 0/0/0 R1(config-if)# ip address 172.16.1.1 255.255.255.252 R1(config-if)# description R1 LAN R2 R1(config-if)# no sh R1(config-if)# exit R1(config)# ipv6 unicast-routing R1(config)# interface S 0/0/0 R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)# clock rate 2000000 R1(config-if)# no sh R1(config-if)# exit
Rutas predeterminadas	R1# show ip route R1# conf t R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)# ipv6 route ::0/64 2001:DB8:ACAD:1::2 R1(config)# end R1# copy running-config startup-config

Nota: no configure G0/1.

Paso 3: Configurar R2

Configuración de R2 :

Para iniciar la configuración inicial de R2 y R1 se implementaran algunas medidas de seguridad, como también se realizara la optimización de rendimiento; se inicia ingresando al modo configuración global y configurando un mensaje de acceso restringido para usuarios, se asigna una contraseñas de seguridad al acceso modo privilegiado de consola y VTY, activamos el inicio de sesión por contraseñas desactivamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado interrumpan el ingreso de comandos o visualización de información, configuramos el comando **logging synchronous** para el acceso de consola.

Para poder asignar las contraseñas usamos el comando **password** el cual me permite asignar contraseñas en texto plano, sin utilizar algoritmos de encriptación para aumentar la seguridad de las contraseñas en el dispositivo se habilita el servicio de encriptación **password-encryption**, el cual encriptar todas las contraseñas almacenadas en texto plano.

Las contraseñas que se van a utilizar para la configuración de exec privilegiado son: **class** para consola VTY **cisco** se usa el comando **secret** para cifrar la contraseña de exec privilegiado el comando **password** para los demás.

Para configurar el direccionamiento IPV4 e IPv6 de los dispositivos basado en la información de la topología debemos estar dentro del modo de configuración global para poder seleccionar la interfaz e implementar la configuración; cada interfaz debe tener una dirección IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez configurada la interfaz tiene que quedar activa.

A diferencia de R1 en R2 se encuentra una interfaz virtual **loopback** la cual va a permitir por medio de la configuración IPv4 simular un servidor Web.

Se configuran rutas predeterminadas IPV4 e IPV6 en R2 que permitan acceso al Servidor de Internet usamos las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red prefijo /0 e IPv6 del siguiente salto para IPv6.

Se finaliza el procedimiento de configuración y en modo privilegiado procedemos a copiar la configuración actual como de configuración de inicio usando el comando **copy running-config startup-config.**

Para aplicar la configuración anteriormente mencionada, ejecutamos los comandos establecidos dentro de la especificación de la Tabla 4.

Tabla 4 - Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> enable Router# conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R2
Contraseña de exec privilegiado cifrada	R2(config)# enable secret class
Contraseña de acceso a la consola	R2(config)# line console 0 R2(config-if)# password cisco R2(config-if)# login R2(config-if)# exit
Contraseña de acceso Telnet	R2(config)# line VTY 0 4 R2(config-if)# password cisco R2(config-if)# login R2(config-if)# exit
Cifrar las contraseñas de texto no cifrado	R2(config)# service password-encryption
Habilitar el servidor HTTP	R2(config)# ip http server
Mensaje MOTD	R2(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	R2(config)# ip interface S 0/0/0 R2(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config-if)# description R2 LAN R1 R2(config-if)# no sh

	R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface S 0/0/0 R2(config-if)# ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)# no sh R2(config-if)# exit
Interfaz S0/0/1	R2(config)# ip interface S 0/0/1 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config-if)# ip description R2 LAN R3 R2(config-if)# no sh R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface S 0/0/1 R2(config-if)# ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)# clock rate 2000000 R2(config-if)# no sh R2(config-if)# exit.
Interfaz G0/0 (simulación de Internet)	R2(config)# ip interface G 0/0 R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)# ip description R2 LAN Servidor Web R2(config-if)# no sh R2(config-if)# exit R2(config)# ipv6 unicast-routing R2(config)# interface G 0/0 R2(config-if)# ipv6 address 2001:DB8:ACAD:A::38/64 R2(config-if)# no sh R2(config-if)# exit
Interfaz loopback 0 (servidor web simulado)	R2(config)# interface loopback 0

	R2(config-if)# ip address 10.10.10.10 255.255.255.255 R2(config-if)# description Servidor Web Simulado R2(config-if)# exit
Ruta predeterminada	R2# show ip route R2# conf t R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:A::38 R2(config)# end R2# copy running-config startup-config

Paso 4: Configurar R3

Configuración R3 :

Configuración inicial de R3 e igual que en R2 y R1 implementamos algunas medidas de seguridad y optimizamos el rendimiento; para implementar dichas medidas ingresamos al modo configuración global, configuramos un mensaje de acceso restringido para usuarios, asignamos contraseñas de seguridad al acceso modo privilegiado, de consola y VTY, activar el inicio de sesión por contraseñas y por último deshabilitamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado interfieran la entrada de comandos o visualización de información, se configura el comando **logging synchronous** para el acceso de consola.

Realizamos la asignación de contraseñas usando el comando **password** el cual permite asignar contraseñas en texto plano, para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación **password-encryption** que encripta todas las contraseñas almacenadas en texto plano.

Las contraseñas que vamos a utilizar para la configuración de exec privilegiado son class para consola y VTY **cisco** usamos el comando secret para cifrar la contraseña de exec privilegiado y el comando password para lo demás.

Se Configurar el direccionamiento IPV4 e IPv6 de los dispositivos basados en la información de la topología la configuración de cada interfaz debe tener una dirección IP y para conexiones DTE la frecuencia del reloj se establece en 2000000, una vez configurada la interfaz tiene que quedar activa.

También al igual que en R2 y R3 tenemos que configurar las interfaces virtuales **loopback** con direccionamiento IPv4 y IPv6 según la información de la topología y utilizando la primera interfaz disponible dentro de cada red

Se configuran rutas predeterminadas IPV4 e IPV6 que permitan enviar el tráfico de red desconocido al router perimetral el cual es R2; usar las rutas 0.0.0.0 con mascara 0.0.0.0 e IPv4 del siguiente salto para IPv4 y la red prefija /0 e IPv6 del siguiente salto para IPv6.

Finalizar el procedimiento de configuración y en modo privilegiado y copiar la configuración actual como de configuración de inicio usando el comando **copy running-config startup-config.**

Para aplicar la configuración mencionada anteriormente, se realizan los comandos establecidos dentro de la especificación de la Tabla 5

Tabla 5 – Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> enable Router# conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	R3(conf)# enable secret class

Contraseña de acceso a la consola	R3(config)# line console 0 R3(config-if)# password cisco R3(config-if)# login R3(config-if)# exit
Contraseña de acceso Telnet	R3(config)# line VTY 0 4 R3(config-if)# password cisco R3(config-if)# login R3(config-if)# exit l
Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	R3(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/1	R3(config)# ip interface S 0/0/1 R3(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# description R3 LAN R2 R3(config-if)# no sh R3(config-if)# exit R3(config)# ipv6 unicast-routing R3(config)# interface S 0/0/1 R3(config-if)# ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)# no sh R3(config-if)# exit
Interfaz loopback 4	R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0 R3(config-if)# exit
Interfaz loopback 5	R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0 R3(config-if)# exit
Interfaz loopback 6	R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0 R3(config-if)# exit l
Interfaz loopback 7	R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64

	R3(config-if)# exit
Rutas predeterminadas	R3# show ip route R3# conf t R3(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2 R3(config)# end R3# copy running-config startup-config

Paso 5: Configurar S1

Configuración S1:

En la configuración inicial de S1 implementamos algunas medidas de seguridad y optimizamos el rendimiento para implementar dichas medidas ingresamos al modo configuración global allí configuramos un mensaje de acceso restringido para usuarios, asignamos contraseñas de seguridad al acceso modo privilegiado, de consola y VTY 0 15, activamos el inicio de sesión por contraseñas y por último deshabilitamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado interfieran la entrada de comandos o visualización de información, se configura el comando **logging synchronous** para el acceso de consola.

Para asignar contraseñas usamos el comando **password** que permite asignar contraseñas en texto plano para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación **password-encryption** que encripta todas las contraseñas almacenadas en texto plano.

Contraseñas que vamos a utilizar para la configuración de exec privilegiado son **class** para consola y VTY **cisco** usamos el comando secret para cifrar la contraseña de exec privilegiado y el comando password para lo demás

Finalizar el procedimiento de configuración en el cual establecemos la configuración actual como de configuración de inicio.

Para aplicar la configuración mencionada anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 6

Tabla 6 - Configuración S1

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

Paso 6: Configurar S3

Configuración S3:

Configuración inicial de S3 igual que S1 implementamos algunas medidas de seguridad y optimizamos el rendimiento para implementar dichas medidas ingresamos al modo configuración global allí configuramos un mensaje de acceso restringido para usuarios, asignamos contraseñas de seguridad al acceso modo

privilegiado, de consola y VTY 0 15, activamos el inicio de sesión por contraseñas y por último deshabilitamos la resolución de nombres (DNS).

Para evitar que algunos mensajes de estado interfieran la entrada de comandos o visualización de información, se configura el comando **logging synchronous** para el acceso de consola.

Para asignar contraseñas usamos el comando **password** que permite asignar contraseñas en texto plano para reforzar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación **password-encryption** que encripta todas las contraseñas almacenadas en texto plano.

Contraseñas que vamos a utilizar para la configuración de exec privilegiado son **class** para consola y VTY **cisco** usamos el comando secret para cifrar la contraseña de exec privilegiado y el comando password para lo demás

Finalizar el procedimiento de configuración en el cual establecemos la configuración actual como de configuración de inicio.

Para aplicar la configuración mencionada anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 7

Tabla 7 - Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch> enable Switch# conf t Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)# hostname S3
Contraseña de exec privilegiado cifrada	S3(config)# enable secret class

Contraseña de acceso a la consola	S3(config)# line console 0 S3(config-if)# password cisco S3(config-if)# login S3(config-if)# exit
Contraseña de acceso Telnet	S3(config)# line VTY 0 4 S3(config-if)# password cisco S3(config-if)# login S3(config-if)# exit
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	S3(config)# banner motd “Se prohíbe el acceso no autorizado”

Paso 7: Verificar la conectividad de la red

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

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

En la tabla 8 podemos visualizar que la configuración hasta el momento está bien sin problemas

En las capturas 2, 3 y 4 podemos visualizar el resultado los pings realizados en cada dispositivo.

Tabla 8 - Conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Figura 3
R2	R3, S0/0/1	172.16.2.1	Figura 4
PC de Internet	Gateway predeterminado	209.165.200.232	Figura 5

Figura 3 - Ping R1 a R2

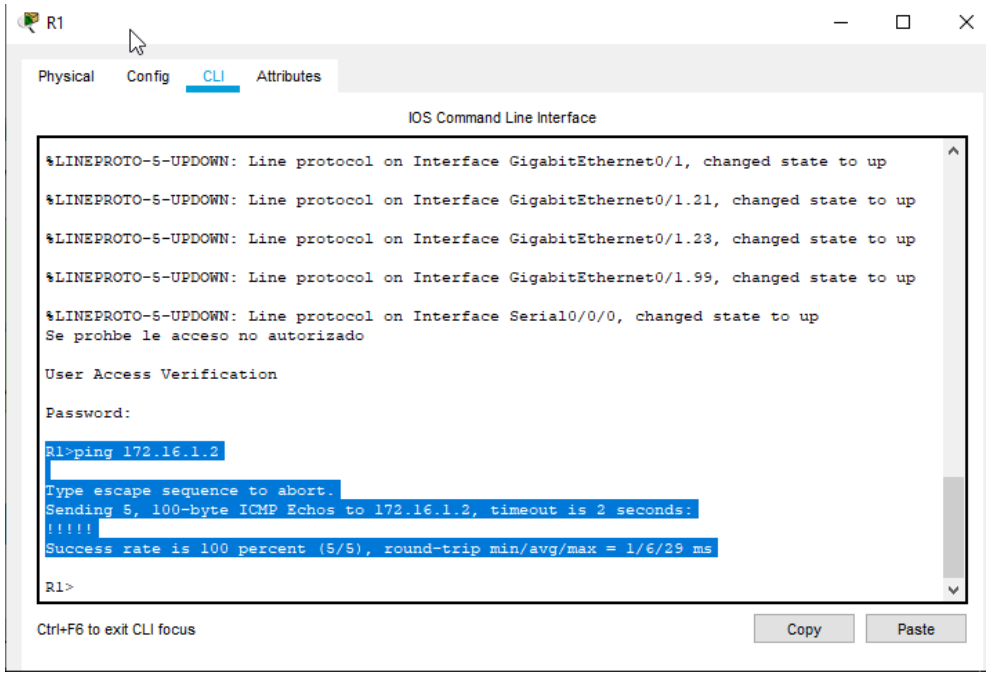


Figura 4 - Ping R2 a R3

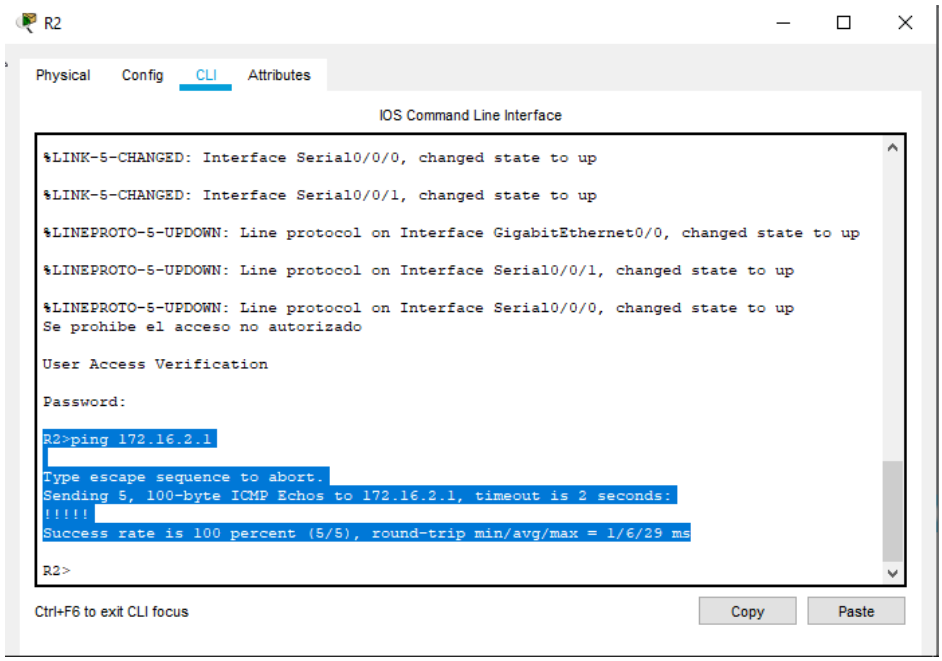
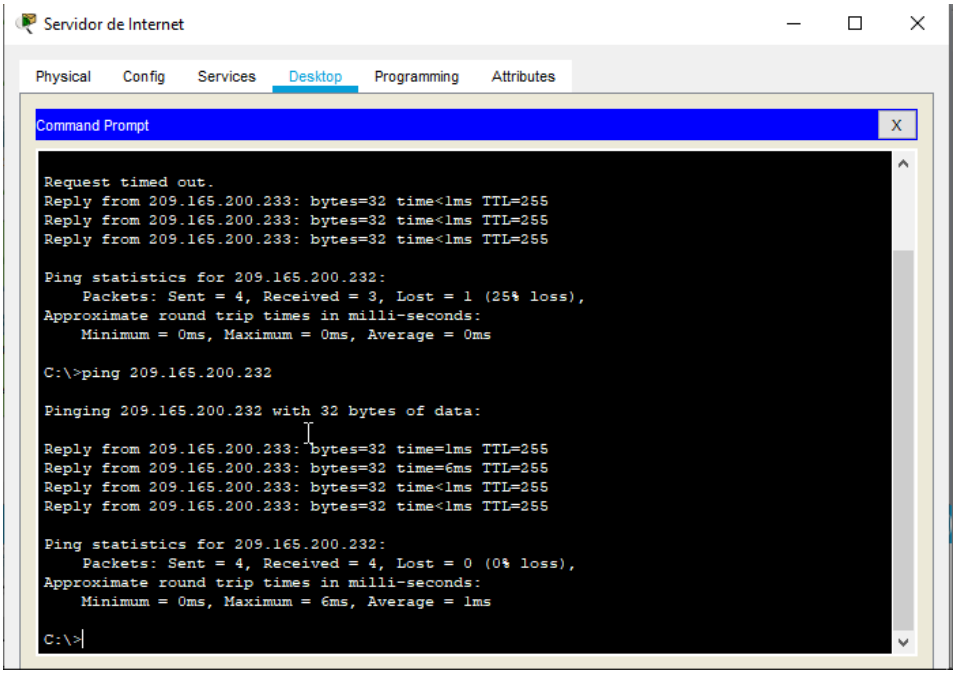


Figura 5 -Ping PC Internet a Gateway Predeterminado



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

Paso 1: Configurar S1

Configuración del S1:

Para configurar las VLAN lo primero con lo que iniciamos es crearlas en el modo de configuración global y con los comandos descritos en la columna **Especificaciones** de la Tabla 9 procedemos a crear y asignar propiedades como nombre y direccionamiento IP de administración.

Ya creadas las VLAN seleccionamos VLAN 99 como VLAN principal y asignamos la IPv4 192.168.99.3 al S1 como se muestra en la topología.

Para permitir la comunicación entre las redes del Switch y el exterior realizamos la configurar de dirección de gateway con la IPv4 192.168.99.1 cuya dirección IPv4 del siguiente salto cuyo caso es R1.

Ya creadas y configuradas las VLAN propuestas en la topología, ingresamos al modo de configuración global y seleccionar las interfaces del Switch que usaremos para conexión principal de estas redes virtuales y en las cuales vamos a configurar propiedades como descripción, direccionamiento IP y tipo de enlace; las otras interfaces del Switch solo basta con configurar el tipo de enlace.

La VLAN 1 propuesta como VLAN nativa de los enlaces troncales del Switch en las interfaces F 0/5 y F 0/3.

Para prevenir posibles intruciones de seguridad o ingresos no autorizados apagamos las interfaces no administrativas, usando el comando **interface range** para seleccionar un numero de interfaces y no tener que configurar la individual mente una por una.

Que la PC-A pertenezca a la VLAN 21 como lo muestra la topología, se asigna la interfaz de conexión F 0/6 a VLAN.

Para aplicar la configuración mencionada anteriormente, ejecutamos los comandos establecidos dentro de la especificación de la Tabla 9

Tabla 9 - Configuración de seguridad, VLAN y routing del Switch 1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1> enable S1# conf t S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config-vlan)# end S1(config)# vlan 23 S1(config-vlan)# name Ingenieria S1(config-vlan)# end S1(config)# vlan 99 S1(config-vlan)# name Administracion S1(config-vlan)# end

Asignar la dirección IP de administración.	S1(config)# interface vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)# exit
Asignar el gateway predeterminado	S1(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)# interface F 0/3 S1(config-if)# description Enlace troncal S1 – S3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Forzar el enlace troncal en la interfaz F0/5	S1(config)# interface F 0/5 S1(config-if)# description LAN S1 – R1 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native VLAN 1 S1(config-if)# end
Configurar el resto de los puertos como puertos de acceso	S1(config)# interface range F 0/6 – 24 S1(config-if-range)# switchport mode access S1(config-if-range)# exit
Asignar F0/6 a la VLAN 21	S1(config)# interface F 0/6 S1(config-if)# description S1 - VLAN 21 S1(config-if)# switchport mode access S1(config-if)# switchport access VLAN 21 S1(config-if)# exit
Apagar todos los puertos sin usar	S1(config)# interface range F 0/7 - 24 S1(config-if-range)# shutdown S1(config-if-range)# end

Paso 2: Configurar el S3

Configuración S3:

Para configurar las VLAN lo primero con lo que iniciamos es crearlas en el modo de configuración global y con los comandos descritos en la columna **Especificaciones** de la Tabla 9 procedemos a crear y asignar propiedades como nombre y direccionamiento IP de administración

Ya creadas las VLAN seleccionamos VLAN 99 como VLAN principal y asignamos la IPv4 192.168.99.3 al S1 como se muestra.

Ya permitiendo la comunicación entre las redes del Switch y el exterior configuramos la dirección de Gateway con la IPv4 192.168.99.1 la cual es la dirección IPv4 del enrutador más cercano R.

Ya creadas y configuradas las VLAN propuestas en la topología, ingresamos al modo de configuración global y seleccionar las interfaces del Switch que usaremos para conexión principal de estas redes virtuales y en las cuales vamos a configurar propiedades como descripción, direccionamiento IP y tipo de enlace; las otras interfaces del Switch solo basta con configurar el tipo de enlace.

La VLAN 1 propuesta como VLAN nativa de los enlaces troncales del Switch en las interfaces F 0/3.

Para prevenir posibles intrusiones de seguridad o ingresos no autorizados apagamos las interfaces no administrativas, usando el comando **interface range** para seleccionar un numero de interfaces y no tener que configurar la individual mente una por una.

Que la PC-A pertenezca a la VLAN 23 como lo muestra la topología, se asigna la interfaz de conexión F 0/18 a VLAN.

Para aplicar la configuración mencionada anteriormente, ejecutamos los comandos establecidos dentro de la especificación de la Tabla 10

Tabla 10 - Configuración de VLAN, seguridad y routing de Switch 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3> enable S3# conf t S3(config)# vlan 21 S3(config-vlan)# name Contabilidad S3(config-vlan)# exit S3(config)# vlan 23 S3(config-vlan)# name Ingenieria S3(config-vlan)# exit S3(config)# vlan 99 S3(config-vlan)# name Administracion S3(config-vlan)# exit
Asignar la dirección IP de administración	S3(config)# interface vlan 99 S3(config-if)# ip address 192.168.99.3 255.255.255.0 S3(config-if)# exit
Asignar el gateway predeterminado.	S3(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)# interface F 0/3 S3(config-if)# description Enlace troncal S3 - S1 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native VLAN 1 S3(config-if)# exit
Configurar el resto de los puertos como puertos de acceso	S3(config)# interface range F 0/4 – 24 S3(config-if-range)# switchport mode Access S3(config-if-range)# exit
Asignar F0/18 a la VLAN 23	S3(config)# interface F 0/18 S3(config-if)# description S3 en VLAN 23 S3(config-if)# switchport mode access S3(config-if)# switchport access VLAN 23 S3(config-if)# no shutdown

	S3(config-if)# exit
Apagar todos los puertos sin usar	S3(config)# interface range F 0/19 - 24 S3(config-if-range)# shutdown S3(config-if-range)# end

Paso 3: Configurar R1

Configuración R1:

Configuramos el enrutamiento VLAN dentro de R1 usando el tipo de enrutamiento **router-on-a-stick** la configuración es simple, solo tenemos que crear una subinterfaz por cada VLAN que vamos utilizar dentro de una interfaz.

Para la VLAN de Contabilidad, Ingeniería y Administración creamos las subinterfaces .21, .23 y .99 respectivamente dentro de la interfaz de conexión o enlace troncal G 0/1.

Antes de asignar una IP a la subinterfaz, tenemos que configurarla para que funcione dentro de una VLAN específica, esto se logra usando el comando **encaptulation dot1Q ID_VLAN**. para cada una de las interfaces.

En cada Subinterfaz tenemos que configurar una descripción, y asignarla a la VLAN correspondiente y un direccionamiento IP, en cuyo caso será la primera IP disponible de la VLAN a la cual pertenezca la subinterfaz

Las descripciones de las Subinterfaces deben cumplir con las sintaxis LAN de VLAN ID

Para finalizar todas las subinterfaces deben quedar activas sin problema

Para aplicar la configuración mencionada anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 11

Tabla 11 - Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1> enable R1# conf t R1(config)# interface G 0/1.21 R1(config-subif)# encapsulation dot1Q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0 R1(config-subif)# description LAN de Contabilidad R1(config-subif)# no sh R1(config-if)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# interface G 0/1.23 R1(config-subif)# encapsulation dot1Q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0 R1(config-subif)# description LAN de Ingenieria R1(config-subif)# no sh R1(config-if)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# interface G 0/1.99 R1(config-subif)# encapsulation dot1Q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0 R1(config-subif)# description LAN Administracion R1(config-subif)# no sh R1(config-if)#exit
Activar la interfaz G0/1	R1(config)# interface G 0/1 R1(config-if)# no sh R1(config-if)#end

Paso 4: Verificar la conectividad de la red

Use el comando **ping** para probar la conectividad entre los suiches 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 en su efecto:

Tabla 12 - Verificación R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	captura 6
S3	R1, dirección VLAN 99	192.168.99.1	captura 7
S1	R1, dirección VLAN 21	192.168.21.1	captura 6
S3	R1, dirección VLAN 23	192.168.23.1	captura 7

Como se evidencia en las capturas 6 y 7, los PING a las subinterfaces de R1 se completan satisfactoria mente,

Figura 6 - Ping S1 a VLAN 99 y VLAN 21

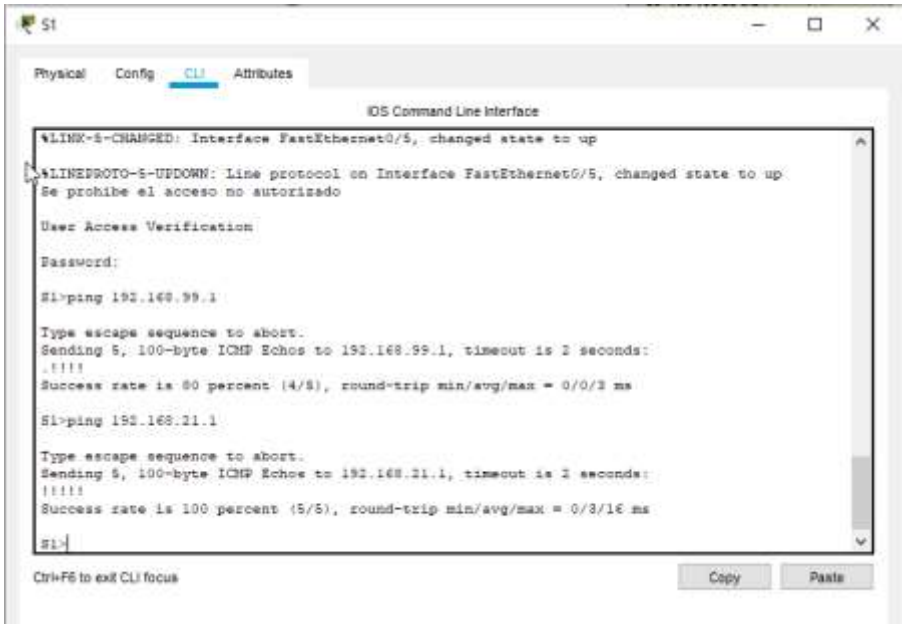
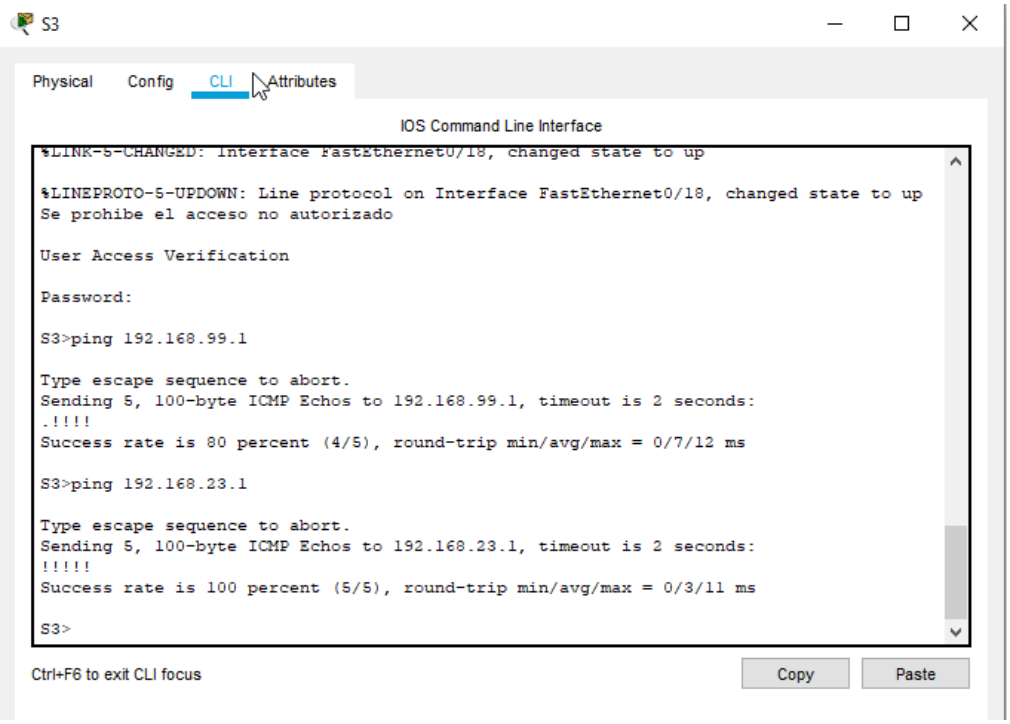


Figura 7 - Ping S3 - VLAN 99 y VLAN 23



Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Como primer paso es ingresar al modo de configuración global; por medio del comando **router rip** se habilitamos RIP y modificamos la versión del protocolo mediante el comando **versión 2**

Ya al activar y cambiar la versión del RIP vamos a pronunciar las redes con la ayuda del comando **network** seguido de la IP de la red a mostrar que para este caso son las conectadas directamente al router.

Evitando el desperdicio de ancho de banda y desperdicio de recursos evitando riesgos de seguridad que se presenten con la actualización periódica del protocolo

RIP procedemos a configurar las interfaces LAN como pasivas y No envía actualización RIP con ayuda del comando **passive-interfaces.**

Como último, para evitar que el RIP resuma automáticamente las redes utilizamos el comando no auto-summary

Para aplicar la configuración mencionada anteriormente vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 13

Tabla 13 - Configuración RIPv2 en R1

Elemento de configuración	Especificación
Configurar RIP versión 2	R1> enable R1# config t R1(config)# router rip R1(config-router)# versión 2
Anunciar las redes conectadas directamente	R1(config-router)# network 172.16.1.0 R1(config-router)# network 192.168.21.0 R1(config-router)# network 192.168.23.0 R1(config-router)# network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interface G 0/1
Desactive la sumarización automática	R1(config-router)# no auto-summary R1(config-router)# end

Paso 2: Configurar RIPv2 en el R2

Como primer paso es ingresar al modo de configuración global; por medio del comando **router rip** se habilitamos RIP y modificamos la versión del protocolo mediante el comando **versión 2**

Ya al activar y cambiar la versión del RIP vamos a pronunciar las redes con la ayuda del comando **network** seguido de la IP de la red a mostrar que para este caso son las conectadas directamente al router.

Evitando el desperdicio de ancho de banda y desperdicio de recursos evitando riesgos de seguridad que se presenten con la actualización periódica del protocolo RIP procedemos a configurar las interfaces LAN como pasivas y No envía actualización RIP con ayuda del comando **passive-interfaces.**

Como último, para evitar que el RIP resuma automáticamente las redes utilizamos el comando no auto-summary

Para aplicar la configuración mencionada anteriormente vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 14

Tabla 14 - Configuración de RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2> enable R2# config t R2(config)# router rip R2(config-router)# versión 2
Anunciar las redes conectadas directamente	R2(config-router)# network 10.10.10.10 R2(config-router)# network 172.16.1.0 R2(config-router)# network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface loopback 0

Desactive la sumarización automática.	R2(config-router)# no auto-summary R2(config-router)# end R2# copy running-config startup-config

Paso 3: Configurar RIP2 en el R2

Como primer paso es ingresar al modo de configuración global; por medio del comando **router rip** se habilitamos RIP y modificamos la versión del protocolo mediante el comando **versión 2**

Ya al activar y cambiar la versión del RIP vamos a pronunciar las redes con la ayuda del comando **network** seguido de la IP de la red a mostrar que para este caso son las conectadas directamente al router.

Evitando el desperdicio de ancho de banda y desperdicio de recursos evitando riesgos de seguridad que se presenten con la actualización periódica del protocolo RIP procedemos a configurar las interfaces LAN como pasivas y No envía actualización RIP con la ayuda del comando **passive-interfaces.**

Como último, para evitar que el RIP resuma automáticamente las redes utilizamos el comando no auto-summary

Para aplicar la configuración mencionada anteriormente vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 15

Tabla 15 - Configuración de RIPv3 en R2

Elemento o tarea de configuración	Especificación

Configurar RIP versión 2	R3> enable R3# config t R3(config)# router rip R3(config-router)# versión 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.	R2(config-router)# no auto-summary R2(config-router)# exit

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 - Verificación de información RIP v2

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 rip database
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show running-config | section rip

Como se observa en las figuras 8, 9 y 10 se puede evidenciar la información solicitada en cada una de las preguntas de la Tabla 16

Figura 8 - Verificación ip Protocolos

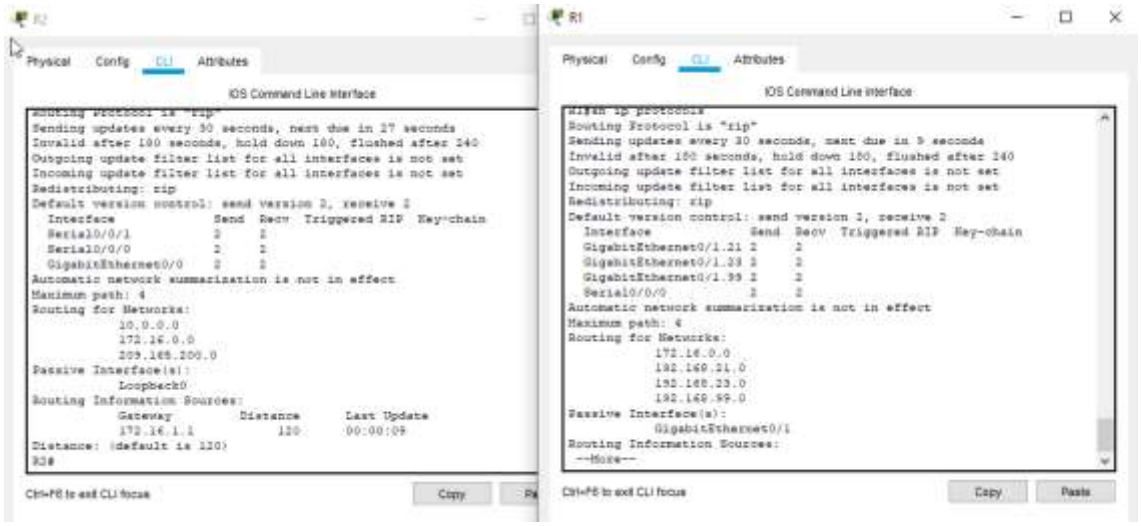


Figura 9 - Verificación Base de datos RIP

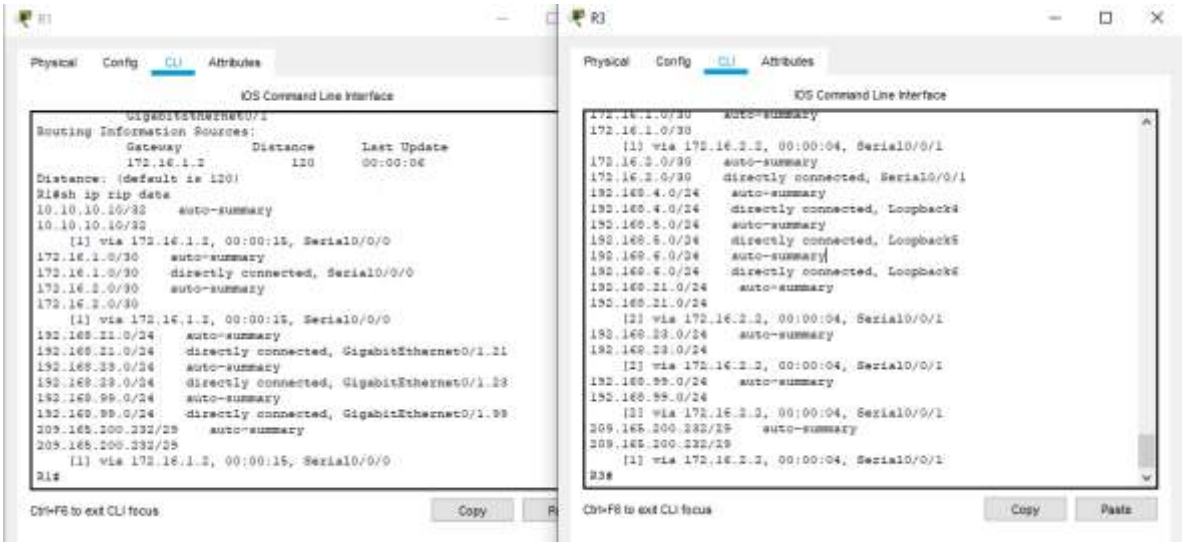
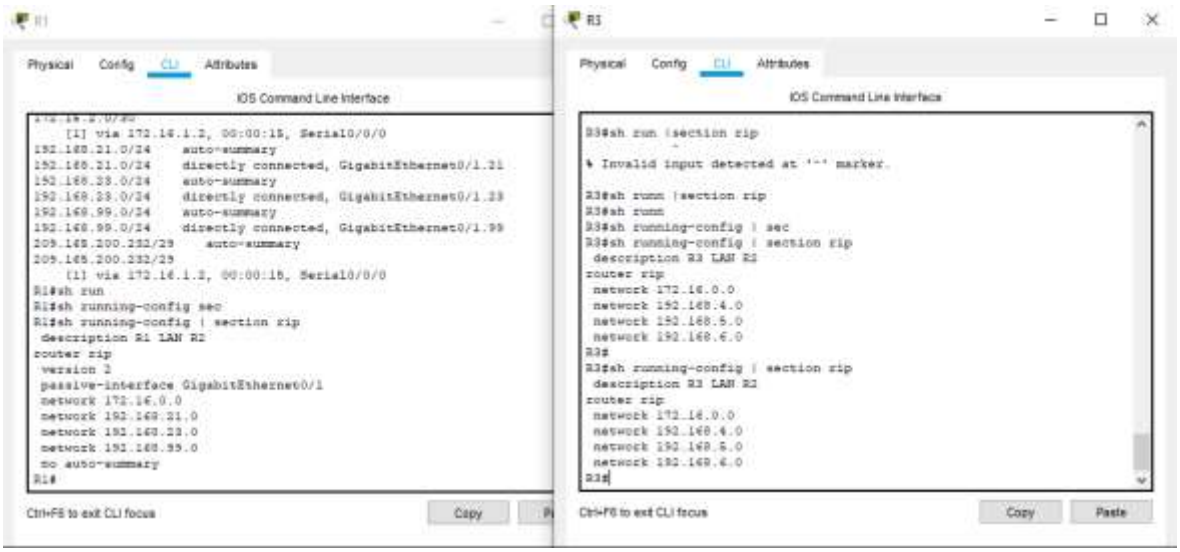


Figura 10 - Verificación RIP en ejecución



Parte 5: Implementar DHCP y NAT para IPv4

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

Cuando un router funciona como servidor DHCPv4 el mismo asigna todas las direcciones IPv4 disponibles de un conjunto de direcciones DHCP.

Ingresando al modo de configuración global configuramos R1 como servidor DHCP; para omitir las primeras 20 direcciones para las redes VLAN 21 y VLAN 23 vamos a utilizar el comando **exclude-address**

luego, configuramos un pool de direcciones para cada VLAN con estos datos:

- VLAN 21:
  - Nombre: ACCT
  - Servidor DNS: 10.10.10.10
  - Nombre de dominio: ccna-sa.com
  - Gateway: 192.168.21.1
- VLAN 23:
  - Nombre: ENGNR

- Servidor DNS: 10.10.10.10
- Nombre de dominio: ccna-sa.com
- Gateway: 192.168.23.1

Para aplicar la configuración mencionada anteriormente ejecutamos los comandos establecidos dentro de la especificación de la Tabla 17

Tabla 17 - Configuración DHCP R1 para VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1> enable R1# config t R1(config)# ip dhcp exclude-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)# ip dhcp exclude-address 192.168.23.1 192.168.23.21
Crear un pool de DHCP para la VLAN 21.	R1(config)# ip dhcp pool ACCT R1(dhcp-config)# dns-server 10.10.10.10 R1(dhcp-config)# domain-name ccna-sa.com R1(dhcp-config)# default-router192.168.21.1 R1(dhcp-config)# network 192.168.21.0 255.255.255.0 R1(dhcp-config)# exit
Crear un pool de DHCP para la VLAN 23	R1(config)# ip dhcp pool ENGNR R1(dhcp-config)# dns-server 10.10.10.10 R1(dhcp-config)# domain-nameccna-sa.com R1(dhcp-config)# default-router192.168.23.1 R1(dhcp-config)# network 192.168.23.0 255.255.255.0

	R1(dhcp-config)# exit

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

Realizamos la configuración de NAT como primero vamos a crear una cuenta de usuario dentro de una base de datos local utilizando los siguientes datos:

- Nombre de Usuario: webuser
- Clave: cisco12345
- Nivel de Privilegio 15.

Realizamos una asignación entre las direcciones locales internas y las direcciones globales internas que permitirá a un equipo de la red local mediante traducción NAT llegar al servidor de internet especifico.

Configuramos el NAT de tal forma que usamos la información proporcionada en la topología y una vez asignadas procedemos a configurar las interfaces participantes en la traducción con respecto al NAT.

Se procede a la configuración del NAT dinámico creamos una lista de acceso que me permita la traducción de las redes en R1 y un resumen de traducción de las redes LAN R3.

Para concluir la configuración vamos a utilizar un pool de direcciones publicas dentro de R1 de nombre INTERNET y un conjunto de direcciones que incluyen las IP desde la 209.165.200.225 a 209.165.200.228.

Para aplicar la configuración mencionada anteriormente, vamos a ejecutar los comandos establecidos dentro de la especificación de la Tabla 18

Tabla 18 - Configuración de NAT estática y dinámica R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2> enable R2# config t 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.	R2(config)# ip nat source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)# int G 0/0 R2(config-if)# ip nat outside R2(config)#exit R2(config)# int S 0/0/0 R2(config-if)# ip nat inside R2(config)#exit R2(config)# int S 0/0/1 R2(config-if)# ip nat inside R2(config)#exit
Configurar la NAT dinámica dentro de una ACL privada	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.	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

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 DHCP y NAT Estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	captura 11
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	captura 12
Verificar que la PC-A pueda hacer ping a la PC-C	captura 13
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**	captura 14

Figura 11 - Verificación DHCP PC-A

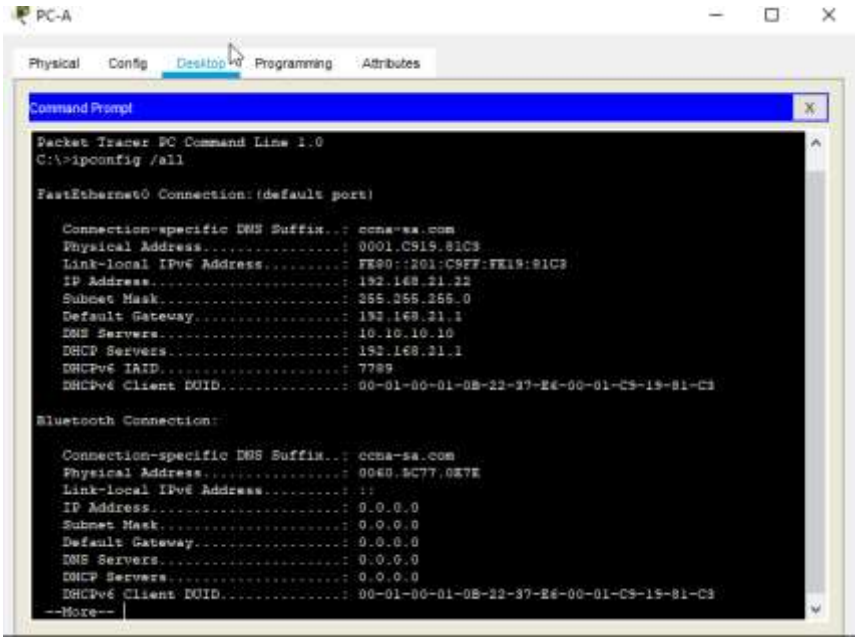


Figura 12 - Verificación DHCP PC-C

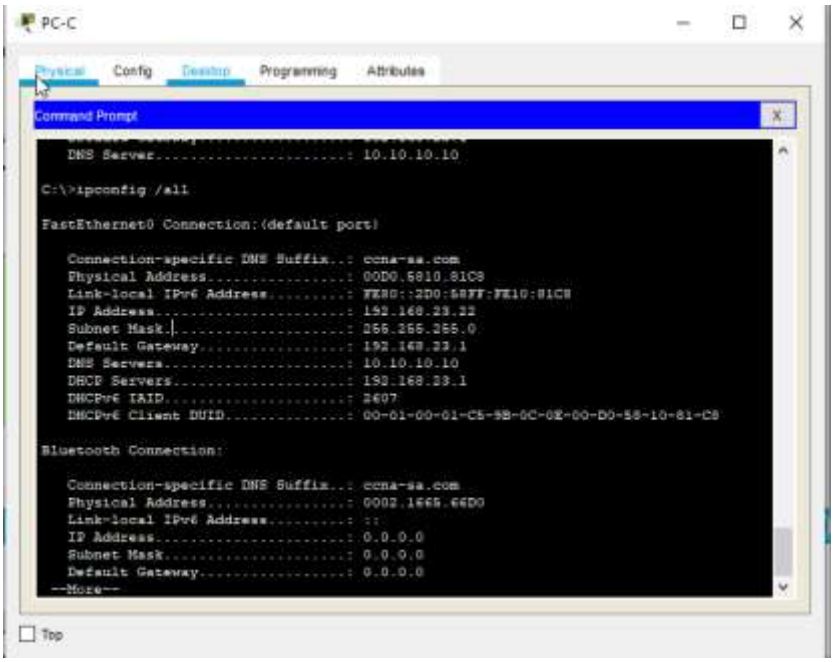


Figura 13 - Verificación de conexión DHCP entre PC-A y PC-B

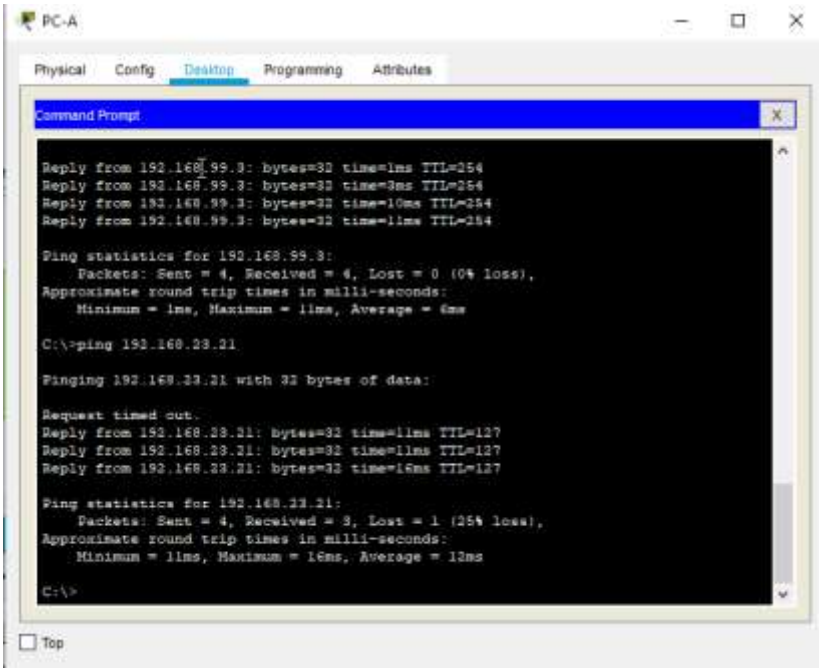


Figura 14 - Verificación de NAT

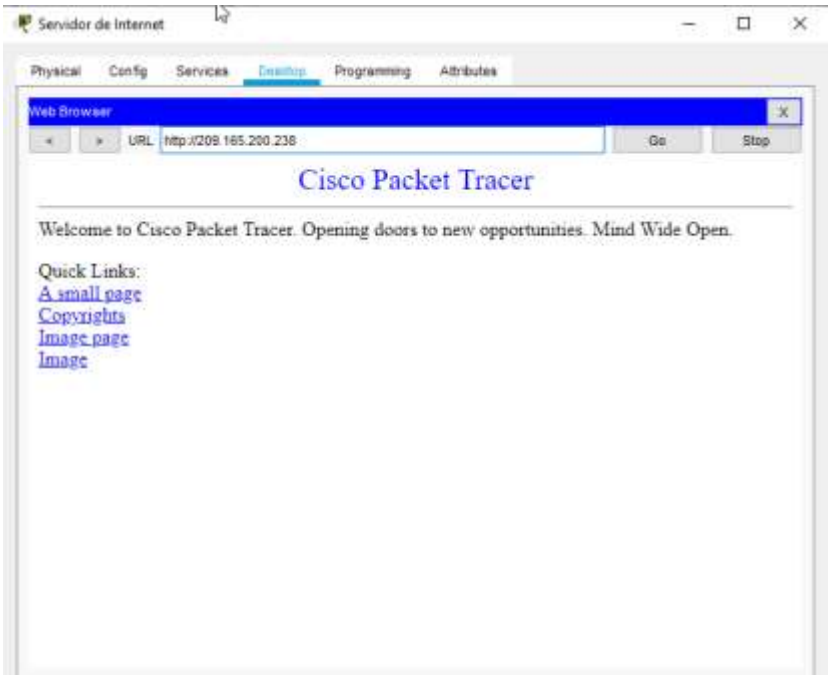
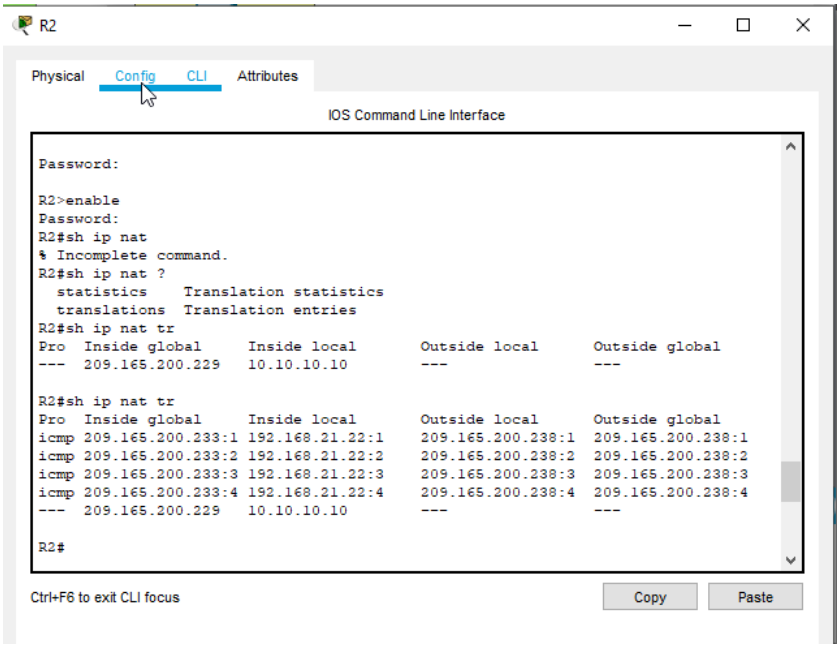


Figura 15 - Verificación traducción NAT R2



Parte 6: Configurar NTP

En esta configuración procedemos a observar el funcionamiento del protocolo de tiempo NTC; lo primero que realizaremos es configurar la hora de R2 con ayuda del comando clock set en el modo privilegiado procedemos a asignar la fecha hora 9 de julio de 2020, 7:00 a.m., y verificamos la configuración usando el comando show clock detail.

Para sincronizar la hora de los dispositivos de la red a la misma que la de R2, vamos a establecer a R2 como servidor NTP estrato 5 y utilizamos el comando ntp server para asignar en los dispositivos a R2 como servidor NTP.

Para verificar esta configuración usamos este comando **show ntp associations** que permite verificar la asociación del dispositivo al servidor NTP y el **comando show clock detail** que permite visualizar en detalle la fecha hora.

Para finalizar utilizamos el comando **show clock detail** para verificar la configuración de los dispositivos.

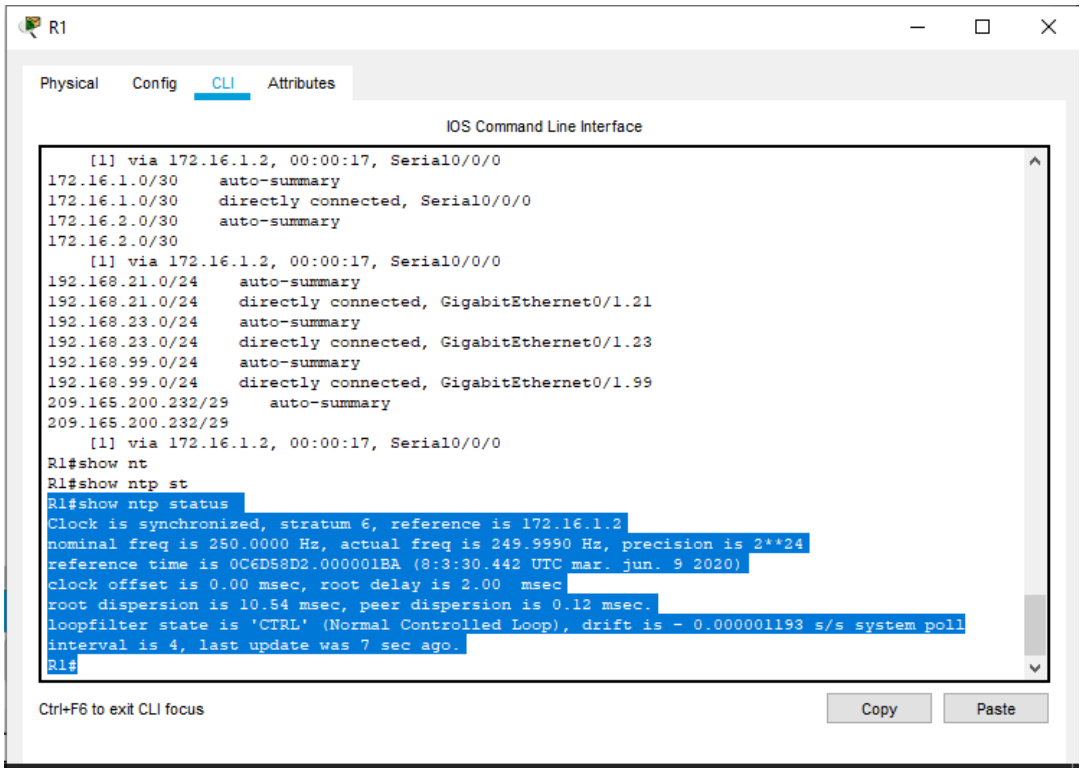
Para completar la configuración mencionada procedemos a ejecutar los comandos especificados en la tabla 20

Tabla 20 - Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2> enable R2# config t R2(config)# clock set 10:00:00 jun 9 2020
Configure R2 como un maestro NTP.	R2(config)# ntp master 5

	R2(config)# end
Configurar R1 como un cliente NTP.	R1> enable R1# config t R1(config)# ntp server 192.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)# ntp update-calendar R1(config)# end
Verifique la configuración de NTP en R1.	R1(config)# show ntp status

Figura 16 - Verificación de NTP en R1



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

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

Restringimos el acceso a las conexiones Telnet o SSH, procedemos a crear una lista de acceso permitiendo o denegando el ingreso de los equipos dentro de la red.

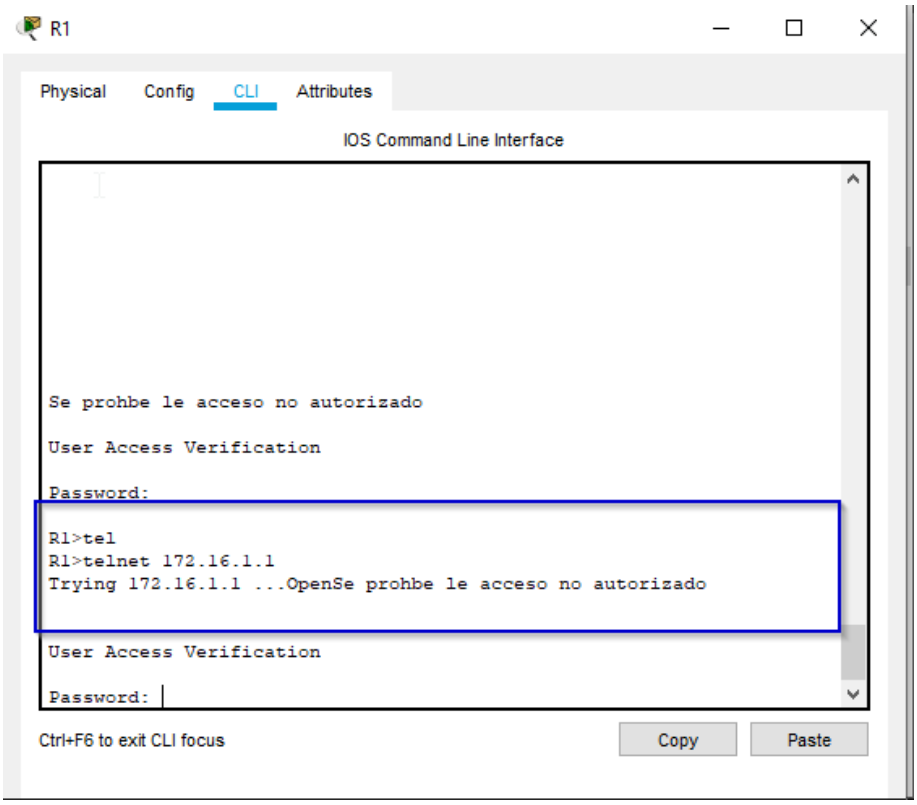
El ACL debe tener como nombre: ADMIN-MGT

Para completar la configuración ejecutamos los comandos mencionados en la Tabla 21

Tabla 21 - Configuración y Verificación de 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	R2> enable R2# conf t R2(config)# ip access-list standard ADMIN-MGT R2(config-std-nacl)# permit host 172.16.1.1 R2(config-std-nacl)# exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)# line VTY 0 15 R2(config-line)# access-class ADMIN-MGT in R2(config-line)# exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)# line VTY 0 4 R2(config-line)# access-class ADMIN-MGT in R2(config-line)# end
Verificar que la ACL funcione como se espera	Figura 11

Figura 17 - Verificación ACL ADMIN-MGT



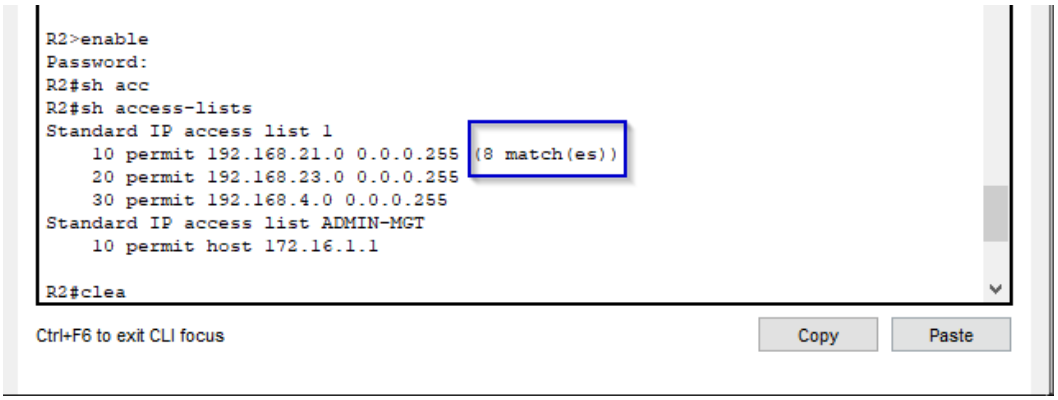
Paso 2: Comando de CLI

En el modo privilegiado procedemos a verificar la información de las listas y el comportamiento de otros protocolos como NAT ya dentro de la red; para eso utilizamos o ejecutamos los comandos descritos en las especificaciones de la Tabla 22.

Tabla 22 - Comandos CLI

Descripción del commando	Ingreso del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2> enable R2# show access-list (Figura 18)
Restablecer los contadores de una lista de acceso	R2# conf t R2(config)# clear access-list counters Ver Figura 19
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show interface S 0/0/1 Ver Figura 20
¿Con qué comando se muestran las traducciones NAT?	R2# show ip nat translations Ver Figura 21
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2# clear ip nat translation Ver Figura 22

captura 18 - Verificación access-list R2



Divisamos en la figura 19 que los contadores de la lista de acceso se reinician

Figura 19 - Verificación access-list

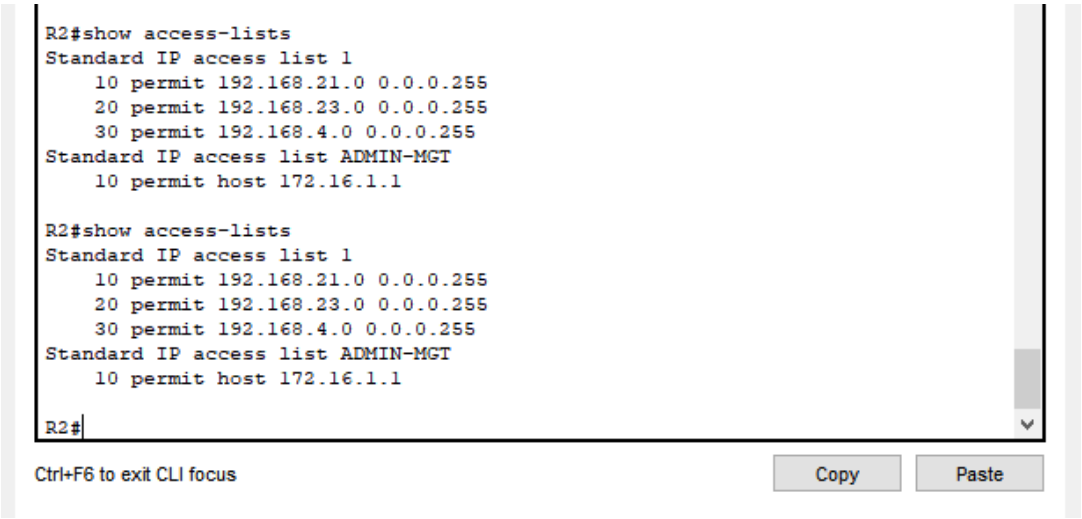


Figura 20 - Verificación ACL en Interface

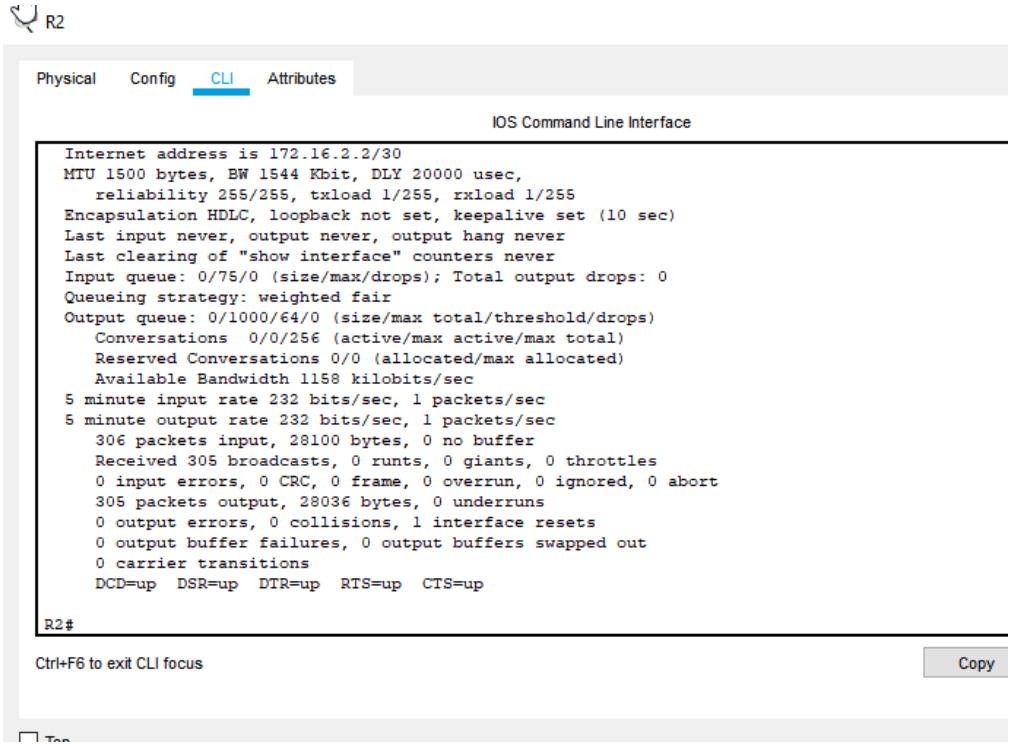
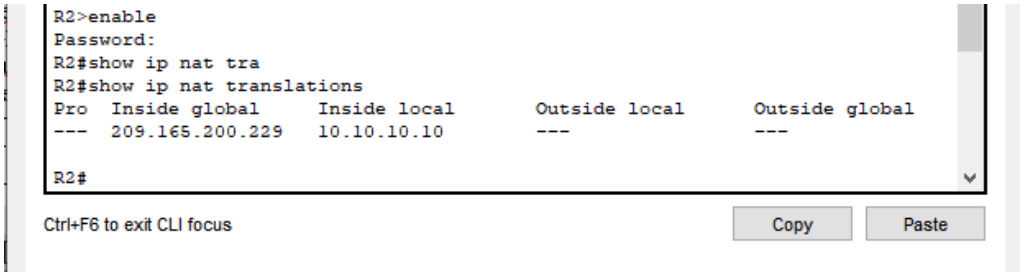


Figura 21 - Verificación NAT Translation



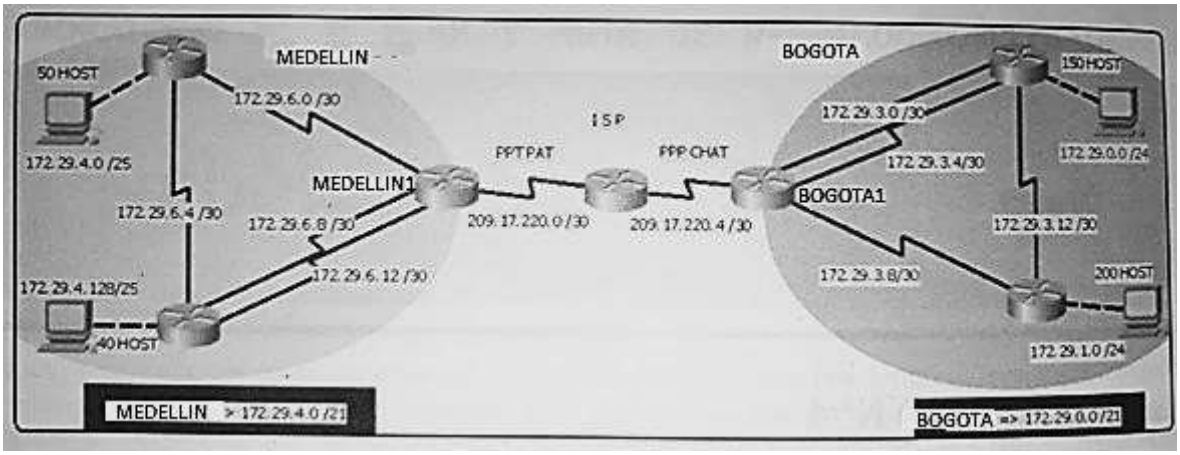
ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el

direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología

Figura 22 - Escenario 2



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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1. Configuración inicial

Trabajo Inicial

Paso 1: Configurar parámetros básicos en los dispositivos.

Configuración inicial R1 implementamos algunas medidas de seguridad y optimizamos el rendimiento; para proceder a implementar dichas medidas ingresamos al modo configuración global desde allí configuramos un mensaje de acceso restringido para usuarios y asignamos contraseñas de seguridad al acceso modo privilegiado de consola y VTY, activamos el inicio de sesión por contraseñas y por último desactivamos la resolución de nombres (DNS).

Para evitar que los mensajes de estado interfieran en la entrada de comandos o visualización de información, configuramos el comando **logging synchronous** para el acceso de consola.

En la asignación de contraseñas usamos el comando **password** que permite asignar contraseñas en texto plano, para reforzar y mejorar la seguridad de las contraseñas del dispositivo habilitamos el servicio de encriptación **password-encryption** que permite encriptar todas las contraseñas almacenadas en texto plano.

Dichas contraseñas que utilizaremos para la configuración de exec privilegiado son **class** y para consola y VTY **cisco** usamos el comando **secret** para cifrar la contraseña de exec privilegiado y el comando password para los demás.

Finalizando el procedimiento de configuración y en modo privilegiado realizamos una copiar la configuración actual como de configuración de inicio utilizando el comando **write**

La configuración mencionada anteriormente, la aplicaremos en cada uno de los dispositivos de la Tabla 23.

Tabla 23 - Configuración inicial dispositivos

Dispositivo	Configuración Básica
Medellin1	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin1 Medellin1(config)# enable secret class Medellin1(config)# line console 0 Medellin1(config-if)# password cisco Medellin1(config-if)# login Medellin1(config-if)# logging synchronous Medellin1(config-if)# exit Medellin1(config)# line VTY 0 4 Medellin1(config-if)# password cisco Medellin1(config-if)# login Medellin1(config-if)# exit Medellin1(config)# service password-encryption Medellin1(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin1(config-if)# exit Medellin1# write
Medellin2	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin2 Medellin2(config)# enable secret class Medellin2(config)# line console 0 Medellin2(config-if)# password cisco Medellin2(config-if)# login Medellin2(config-if)# logging synchronous Medellin2(config-if)# exit Medellin2(config)# line VTY 0 4 Medellin2(config-if)# password cisco Medellin2(config-if)# login

	Medellin2(config-if)# exit Medellin2(config)# service password-encryption Medellin2(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin2(config-if)# exit Medellin2# write
Medellin3	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Medellin3 Medellin3(config)# enable secret class Medellin3(config)# line console 0 Medellin3(config-if)# password cisco Medellin3(config-if)# login Medellin3(config-if)# logging synchronous Medellin3(config-if)# exit Medellin3(config)# line VTY 0 4 Medellin3(config-if)# password cisco Medellin3(config-if)# login Medellin3(config-if)# exit Medellin3(config)# service password-encryption Medellin3(config)# banner motd "Se prohíbe el acceso no autorizado" Medellin3(config-if)# exit Medellin3# write
Bogota1	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota1 Bogota1(config)# enable secret class Bogota1(config)# line console 0 Bogota1(config-if)# password cisco Bogota1(config-if)# login Bogota1(config-if)# logging synchronous

	Bogota1(config-if)# exit Bogota1(config)# line VTY 0 4 Bogota1(config-if)# password cisco Bogota1(config-if)# login Bogota1(config-if)# exit Bogota1(config)# service password-encryption Bogota1(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota1(config-if)# exit Bogota1# write
Bogota2	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota2 Bogota2(config)# enable secret class Bogota2(config)# line console 0 Bogota2(config-if)# password cisco Bogota2(config-if)# login Bogota2(config-if)# logging synchronous Bogota2(config-if)# exit Bogota2(config)# line VTY 0 4 Bogota2(config-if)# password cisco Bogota2(config-if)# login Bogota2(config-if)# exit Bogota2(config)# service password-encryption Bogota2(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota2(config-if)# exit Bogota2# write
Bogota3	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname Bogota3 Bogota3(config)# enable secret class

	Bogota3(config)# line console 0 Bogota3(config-if)# password cisco Bogota3(config-if)# login Bogota3(config-if)# logging synchronous Bogota3(config-if)# exit Bogota3(config)# line VTY 0 4 Bogota3(config-if)# password cisco Bogota3(config-if)# login Bogota3(config-if)# exit Bogota3(config)# service password-encryption Bogota3(config)# banner motd "Se prohíbe el acceso no autorizado" Bogota3(config-if)# exit Bogota3# write
ISP	Router> enable Router# conf t Router(config)# no ip domain-lookup Router(config)# hostname ISP ISP(config)# enable secret class ISP(config)# line console 0 ISP(config-if)# password cisco ISP(config-if)# login ISP(config-if)# logging synchronous ISP(config-if)# exit ISP(config)# line VTY 0 4 ISP(config-if)# password cisco ISP(config-if)# login ISP(config-if)# exit ISP(config)# service password-encryption ISP(config)# banner motd "Se prohíbe el acceso no autorizado" ISP(config-if)# exit ISP# write

Paso 2: Conexión física de topología de red

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

Tabla 24 - Tabla de enrutamiento Escenario 2

Dispositivo	Interfaz	Conexión a	Dirección IP	Máscara	Gateway
Medellin1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.1	255.255.255.252	N.A
	S0/1/0	Medellin3	172.29.6.13	255.255.255.252	N/A
	S0/1/1	Medellin3	172.16.6.9	255.255.255.252	N.A
Medellin2	S0/0/0	Medellin1	172.29.6.2	255.255.255.252	N.A
	S0/0/1	Medellin3	172.29.6.5	255.255.255.252	N.A
	G0/0	Medellin-LAN1	172.29.4.1	255.255.255.128	N.A
Medellin3	S0/0/0	Medellin1	172.16.0.14	255.255.255.252	N.A
	S0/0/1	Medellin1	172.29.6.10	255.255.255.252	N.A
	S0/1/0	Medellin2	172.29.6.6	255.255.255.252	N.A
	G0/0	Medellin-LAN2	172.29.4.129	255.255.255.128	N.A

Bogota1	S0/0/0	ISP	209.17.220.6	255.255.255.252	N.A
	S0/1/0	Bogota2	172.29.3.1	255.255.255.252	N.A
	S0/1/1	Bogota2	172.29.3.5	255.255.255.252	N.A
	S0/0/1	Bogota3	172.29.3.9	255.255.255.252	N.A
Bogota2	S0/0/0	Bogota1	172.29.3.2	255.255.255.252	N.A
	S0/0/1	Bogota1	172.29.3.6	255.255.255.252	N.A
	S0/1/0	Bogota3	172.29.3.13	255.255.255.252	N.A
	G0/0	Bogota-LAN1	172.29.0.1	255.255.255.0	N.A
Bogota3	S0/0/0	Bogota1	172.29.3.10	255.255.255.252	N.A
	S0/0/1	Bogota2	172.29.3.14	255.255.255.252	N.A
	G0/0	Bogota-LAN2	172.29.1.1	255.255.255.0	N.A
ISP	S0/0/0	Medellin1	209.17.220.1	255.255.255.252	N.A
	S0/0/1	Bogota1	209.17.220.5	255.255.255.252	N.A

PC-Medellin-LAN1	Fa0	Medellin2	DHCP	255.255.255.128	172.29.4.1
PC-Medellin-LAN2	Fa0	Medellin3	DHCP	255.255.255.128	172.29.4.129
PC-Bogota-LAN1	Fa0	Bogota2	DHCP	255.255.255.0	172.29.0.1
PC-Bogota-LAN2	Fa0	Bogota3	DHCP	255.255.255.0	172.29.1.1

Paso 3: Configuración de direccionamiento IP

Teniendo en cuenta la información de la Tabla 24 procedemos a configurar las interfaces de cada uno de los dispositivos terminando con el comando **write** utilizado para sobrescribir la configuración inicial

Tabla 25 - Configuración direccionamiento IP

Dispositivo	Configuración Direccionamiento IP
Medellin1	Medellin1> enable Medellin1#conf terminal Medellin1(config)#int S 0/0/0 Medellin1(config-if)# description Conexion a ISP Medellin1(config-if)# ip address 209.17.220.2 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/1/0 Medellin1(config-if)# description Conexion a Medellin3

	Medellin1(config-if)# ip address 172.29.6.13 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/1/1 Medellin1(config-if)# description Conexion a Medellin3 Medellin1(config-if)# ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# exit Medellin1(config)#int S 0/0/1 Medellin1(config-if)# description Conexion a Medellin2 Medellin1(config-if)# ip address 172.29.6.1 255.255.255.252 Medellin1(config-if)# clock rate 2000000 Medellin1(config-if)# no shutdown Medellin1(config-if)# end Medellin1#write
Medellin2	Medellin2> enable Medellin2#conf terminal Medellin2(config)#int S 0/0/0 Medellin2(config-if)# description Conexion a Medellin1 Medellin2(config-if)# ip address 172.29.6.2 255.255.255.252 Medellin2(config-if)# no shutdown Medellin2(config-if)# exit Medellin2(config)#int S 0/0/1 Medellin2(config-if)# description Conexion a Medellin3 Medellin2(config-if)# ip address 172.29.6.5 255.255.255.252 Medellin2(config-if)# clock rate 2000000 Medellin2(config-if)# no shutdown Medellin2(config-if)# exit Medellin2(config)#int G 0/0 Medellin2(config-if)# description Conexion LAN a PC-Medellin-LAN1

	Medellin2(config-if)# ip address 172.29.4.1 255.255.255.128 Medellin2(config-if)# no shutdown Medellin2(config-if)# end Medellin2#write Medellin2#write
Medellin3	Medellin3> enable Medellin3#conf terminal Medellin3(config)#int S 0/0/0 Medellin3(config-if)# description Conexion a Medellin1 Medellin3(config-if)# ip address 172.29.6.14 255.255.255.252 Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int S 0/0/1 Medellin3(config-if)# description Conexion a Medellin1 Medellin3(config-if)# ip address 172.29.6.10 255.255.255.252 Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int S 0/1/0 Medellin3(config-if)# description Conexion a Medellin2 Medellin3(config-if)# ip address 172.29.6.6 255.255.255.252 Medellin3(config-if)# no shutdown Medellin3(config-if)# exit Medellin3(config)#int G 0/0 Medellin3(config-if)# description Conexion LAN a PC-Medellin_LAN2 Medellin3(config-if)# ip address 172.29.4.129 255.255.255.128 Medellin3(config-if)# no shutdown Medellin3(config-if)# end Medellin3#write
Bogota1	Bogota1> enable Bogota1#conf terminal Bogota1(config)#int S 0/0/0 Bogota1(config-if)# description Conexion a ISP

	Bogota1(config-if)# ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)# no shutdown Bogota1(config-if)# exit Bogota1(config)#int S 0/1/0 Bogota1(config-if)# description Conexion a Bogota2 Bogota1(config-if)# ip address 172.29.3.1 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown Bogota1(config-if)# exit Bogota1(config)#int S 0/1/1 Bogota1(config-if)# description Conexion a Bogota2 Bogota1(config-if)# ip address 172.29.3.5 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown Bogota1(config-if)# exit Bogota1(config)#int S 0/0/1 Bogota1(config-if)# description Conexion a Bogota3 Bogota1(config-if)# ip address 172.29.3.9 255.255.255.252 Bogota1(config-if)# clock rate 2000000 Bogota1(config-if)# no shutdown Bogota1(config-if)# end Bogota1#write Bogota1#write
Bogota2	Bogota2> enable Bogota2#conf terminal Bogota2(config)#int S 0/0/0 Bogota2(config-if)# description Conexion a Bogota1 Bogota2(config-if)# ip address 172.29.3.2 255.255.255.252 Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int S 0/0/1 Bogota2(config-if)# description Conexion a Bogota1 Bogota2(config-if)# ip address 172.29.3.6 255.255.255.252

	Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int S 0/1/0 Bogota2(config-if)# description Conexion a Bogota3 Bogota2(config-if)# ip address 172.29.3.13 255.255.255.252 Bogota2(config-if)# clock rate 2000000 Bogota2(config-if)# no shutdown Bogota2(config-if)# exit Bogota2(config)#int G 0/0 Bogota2(config-if)# description Conexion LAN A PC-Bogota-LAN1 Bogota2(config-if)# ip address 172.29.0.1 255.255.255.0 Bogota2(config-if)# no shutdown Bogota2(config-if)# end Bogota2#write
Bogota3	Bogota3> enable Bogota3#conf terminal Bogota3(config)#int S 0/0/0 Bogota3(config-if)# description Conexion a Bogota1 Bogota3(config-if)# ip address 172.29.3.10 255.255.255.252 Bogota3(config-if)# no shutdown Bogota3(config-if)# exit Bogota3(config)#int S 0/0/1 Bogota3(config-if)# description Conexion a Bogota2 Bogota3(config-if)# ip address 172.29.3.14 255.255.255.252 Bogota3(config-if)# no shutdown Bogota3(config-if)# exit Bogota3(config)#int G 0/0 Bogota3(config-if)# description Conexion LAN a PC_Bogota-LAN2 Bogota3(config-if)# ip address 172.29.1.1 255.255.255.0 Bogota3(config-if)# no shutdown Bogota3(config-if)# end Bogota3# write

ISP	ISP# conf terminal ISP(config)# int S 0/0/0 ISP(config-if)# description Conexion a Medellin1 ISP(config-if)# ip address 209.17.220.1 255.255.255.252 ISP(config-if)# no shutdown ISP(config-if)# exit ISP(config)# int S 0/0/1 ISP(config-if)# description Conexion a Bogota1 ISP(config-if)# ip address 209.17.220.5 255.255.255.252 ISP(config-if)# clock rate 2000000 ISP(config-if)# no shutdown ISP(config-if)# end ISP# write

Parte 1: Configuración del enrutamiento

Paso 1: Configuración de OSPF

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

Tabla 26 - Configuración de OSFP

Dispositivo	Configuración OSPF en los Routers
Medellin1	Medellin1> enable Medellin1#conf terminal Medellin1(config)#router ospf 1 Medellin1(config-router)# router-id 1.1.1.1 Medellin1(config-router)# network 172.29.6.0 0.0.0.3 area 0 Medellin1(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medellin1(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin1(config-router)# default-information originate Medellin1(config-router)# end Medellin1# write
Medellin2	Medellin2> enable Medellin2#conf terminal Medellin2(config)#router ospf 1 Medellin2(config-router)# router-id 2.2.2.2 Medellin2(config-router)# network 172.29.6.0 0.0.0.3 area 0 Medellin2(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medellin2(config-router)# network 172.29.4.0 0.0.0.127 area 0 Medellin2(config-router)# end Medellin2#write
Medellin3	Medellin3> enable Medellin3#conf terminal Medellin3(config)#router ospf 1 Medellin3(config-router)# router-id 3.3.3.3 Medellin3(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.6.8 0.0.0.3 area 0

	Medellin3(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.4.128 0.0.0.127 area 0 Medellin3(config-router)# end Medellin3# write
Bogota1	Bogota1> enable Bogota1# conf terminal Bogota1(config)# router ospf 1 Bogota1(config-router)# router-id 4.4.4.4 Bogota1(config-router)# network 172.29.3.0 0.0.0.3 area 1 Bogota1(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota1(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota1(config-router)# default-information originate Bogota1(config-router)# end Bogota1# write
Bogota2	Bogota2> enable Bogota2#conf terminal Bogota2(config)# router ospf 1 Bogota2(config-router)# router-id 5.5.5.5 Bogota2(config-router)# network 172.29.3.0 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota2(config-router)# network 172.29.0.0 0.0.0.255 area 1 Bogota2(config-router)# end Bogota2#write
Bogota3	Bogota3> enable Bogota3# conf terminal Bogota3(config)# router ospf 1 Bogota3(config-router)# router-id 6.6.6.6 Bogota3(config-router)# network 172.29.3.4 0.0.0.3 area 1 Bogota3(config-router)# network 172.29.3.8 0.0.0.3 area 1 Bogota3(config-router)# network 172.29.1.0 0.0.0.255 area 1 Bogota3(config-router)# end Bogota3# write

Paso 2: Configuración ruta distribuida en OSPF

Los Routers Medellin1 y Bogota1 estos deberán añadir a su configuración de enrutamiento a una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Tabla 27 - Configuración de ruta distribuible OSPF

Dispositivo	Configuración Ruta Distribuida en OSPF
Medellin1	Medellin1# conf terminal 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)# end Medellin1# write
Bogota1	Bogota1# conf terminal Bogota1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota1(config)# router ospf 1 Bogota1(config-router)# default-information originate Bogota1(config)# end Bogota1# write

Paso 3: **Configurar ruta Sumarizada ISP**

Este Router ISP debe tener una ruta estática dirigida hacia cada red interna de Medellin1 y Bogota1 para este caso se sumarizan las subredes de cada uno de ellos.

Tabla 28 - Ruta Sumarizada ISP

Dispositivo	Configuración Rutas Estáticas Sumarizada a Sedes
ISP	ISP# conf terminal ISP(config)# ip route 172.29.4.0 255.255.252.0 209.17.220.2 ISP(config)# ip route 172.29.0.0 255.255.252.0 209.17.220.6

	ISP(config)# end ISP# write

Parte 2: Tabla de Enrutamiento.

Paso 1: **Verificar tablas de enrutamiento**

Este se verifica en la tabla de enrutamiento de cada uno de los Routers en el cual utilizamos el comando **show ip route** en cada uno para comprobar que las redes y sus rutas estén bien.

Figura 23 - Tabla de enrutamiento ISP

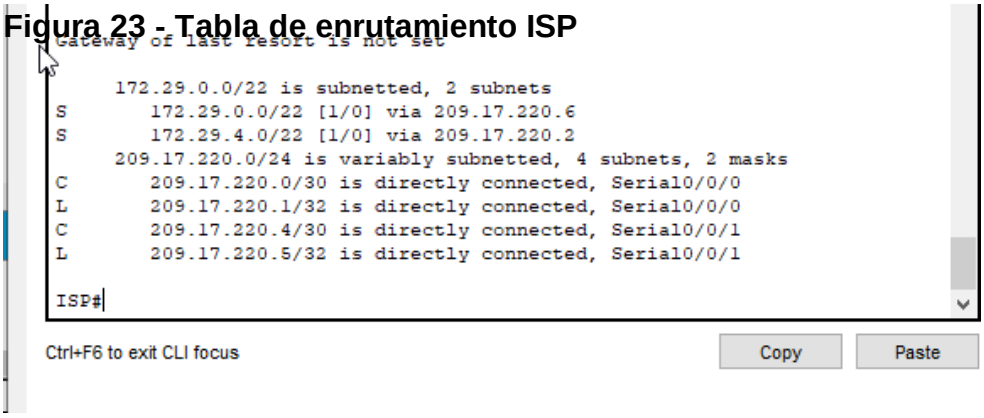


Figura 24 - Tabla de enrutamiento Medellin1

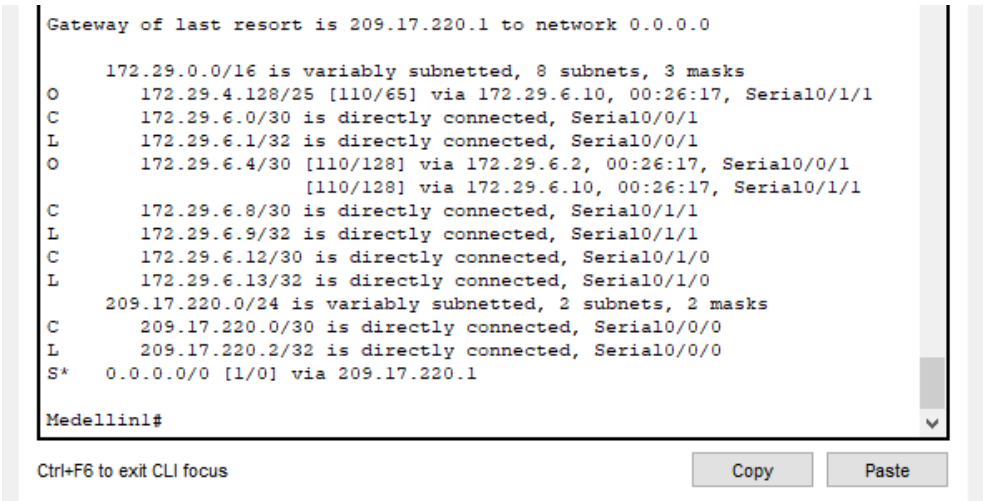


Figura 25 - Tabla de enrutamiento Medellin2

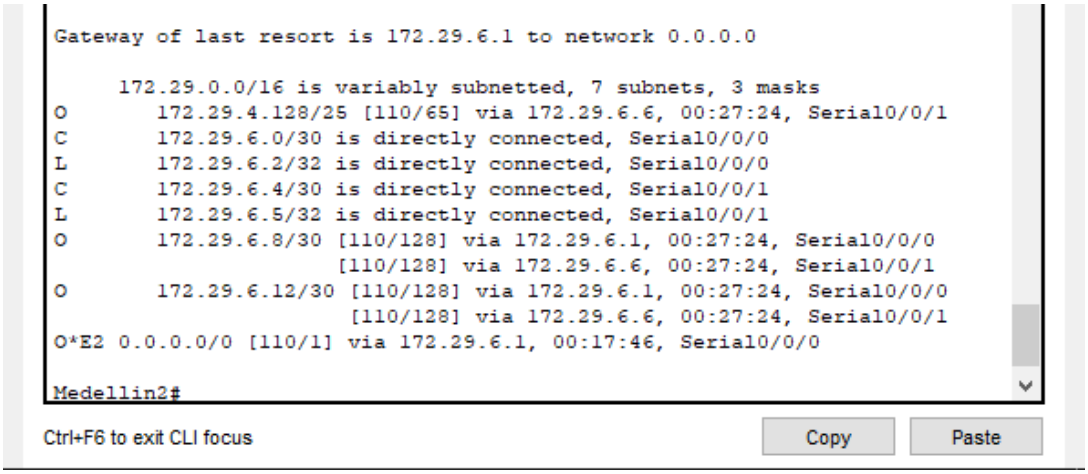


Figura 26 - Tabla de enrutamiento Medellin3

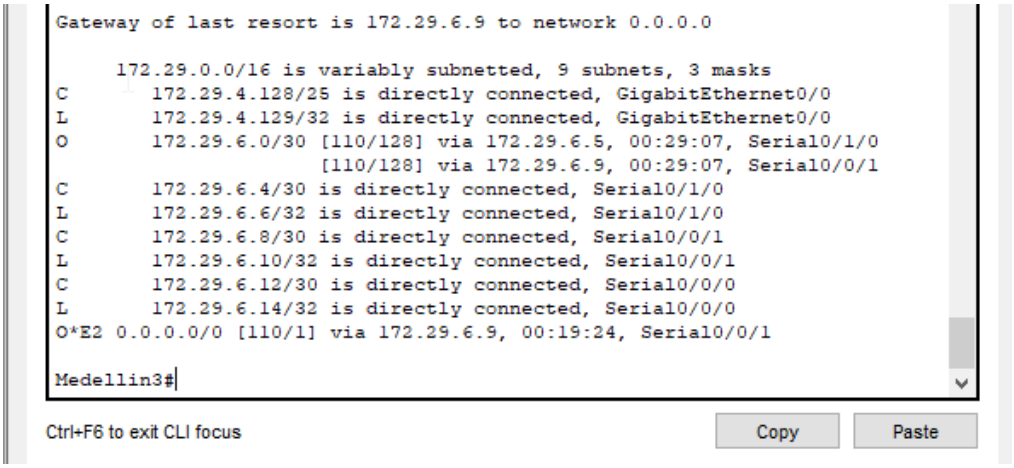


Figura 27 - Tabla de enrutamiento Bogota1

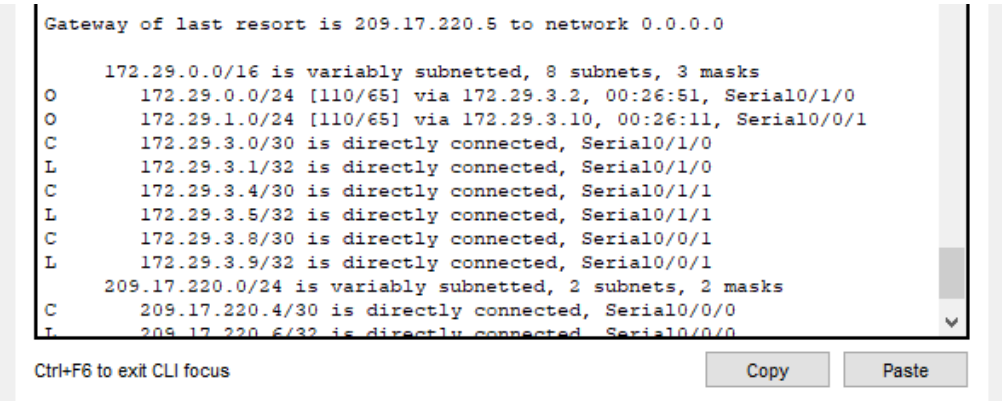


Figura 28 - Tabla de enrutamiento Bogota2

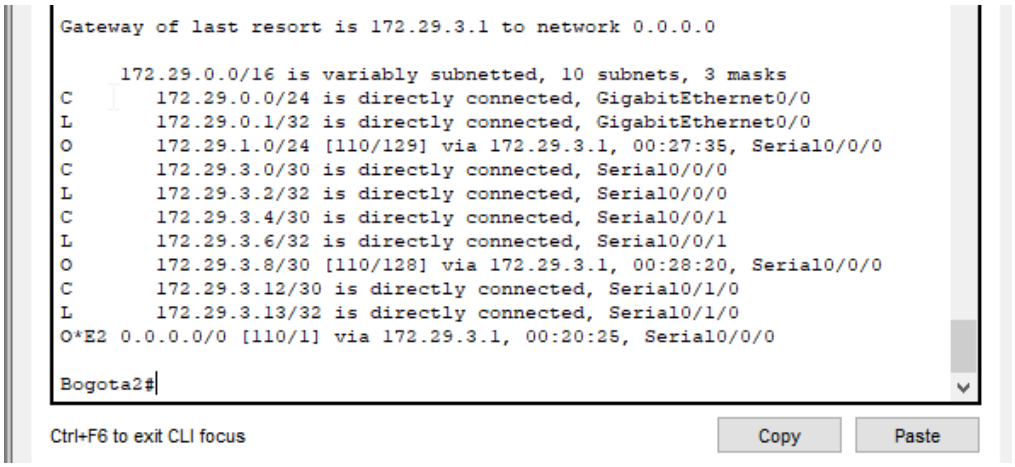
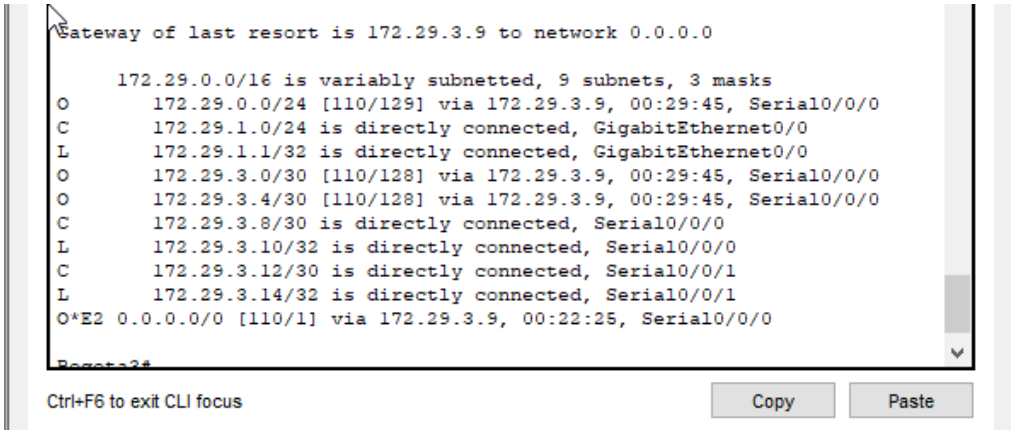


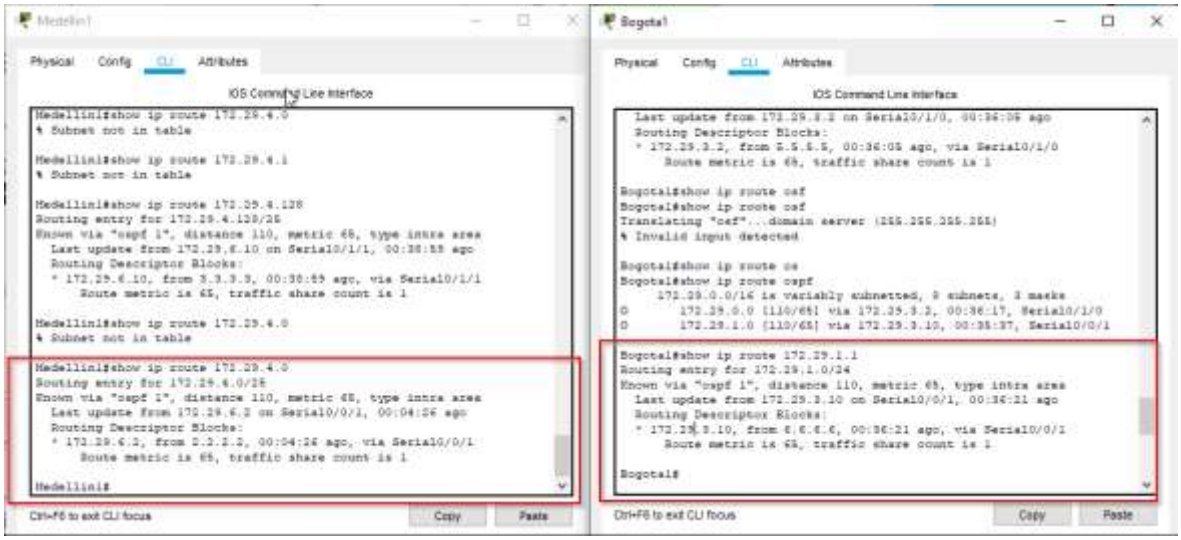
Figura 29 - Tabla de enrutamiento Bogota3



Paso 2: Verificar balanceo de carga

Probamos el balance de carga de los Routers Medellin1 y Bogota1; usando las redes LAN1 de cada area como destino final.

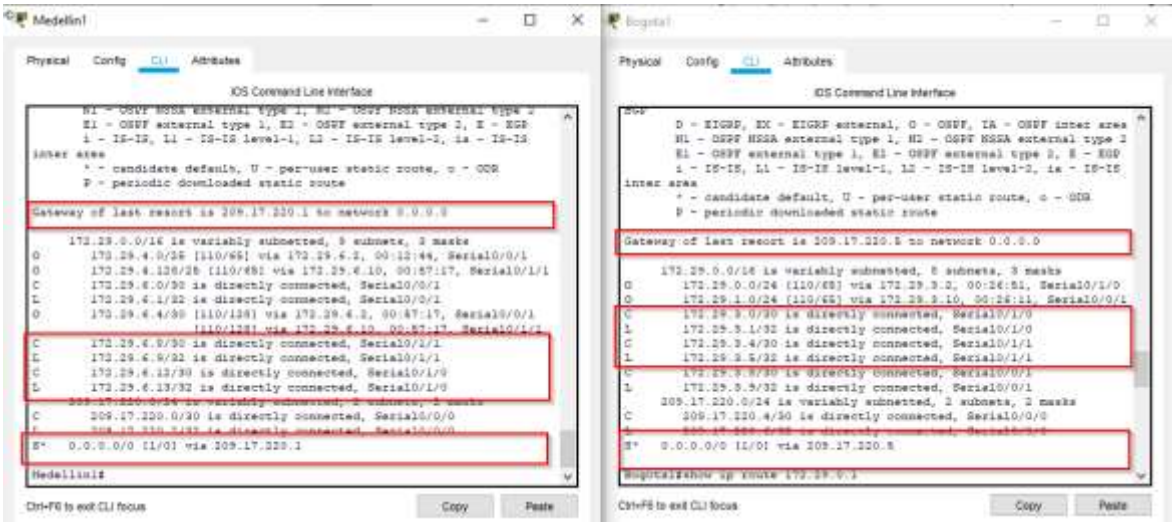
Figura 30 – Verificación de balanceo de carga Medellin1 - Bogota1



Paso 3: **Ruta por defecto OSPF**

Observamos en los Routers Medellin1 y Bogota1 una similitud por su ubicación, por tener un enlace doble de conexión hacia otro router y por la ruta por defecto manejada

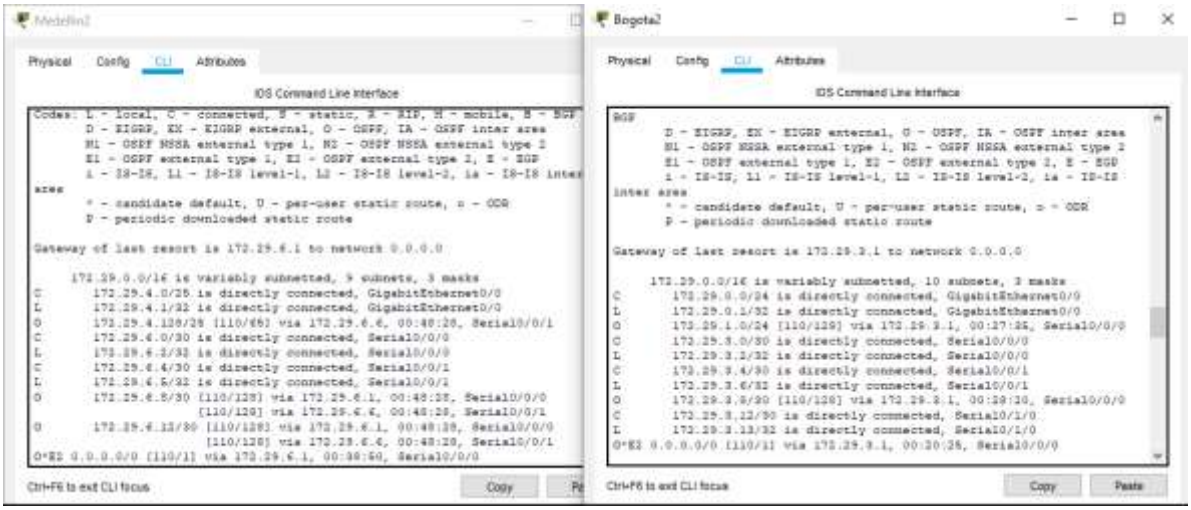
Figura 31 – Verificación ruta por defecto Medellin1 y Bogota1



Paso 4: **Verificación rutas directas OSPF**

En la captura 32. Podemos darnos cuenta que los Routers Bogota2 y Medellin2 que al igual que los Routers Medellin1 y Bogota1, reciben las actualizaciones de OSPF y las muestra directamente.

Figura 32 - Verificación rutas directas y OSPF Medellin2 y Bogota2



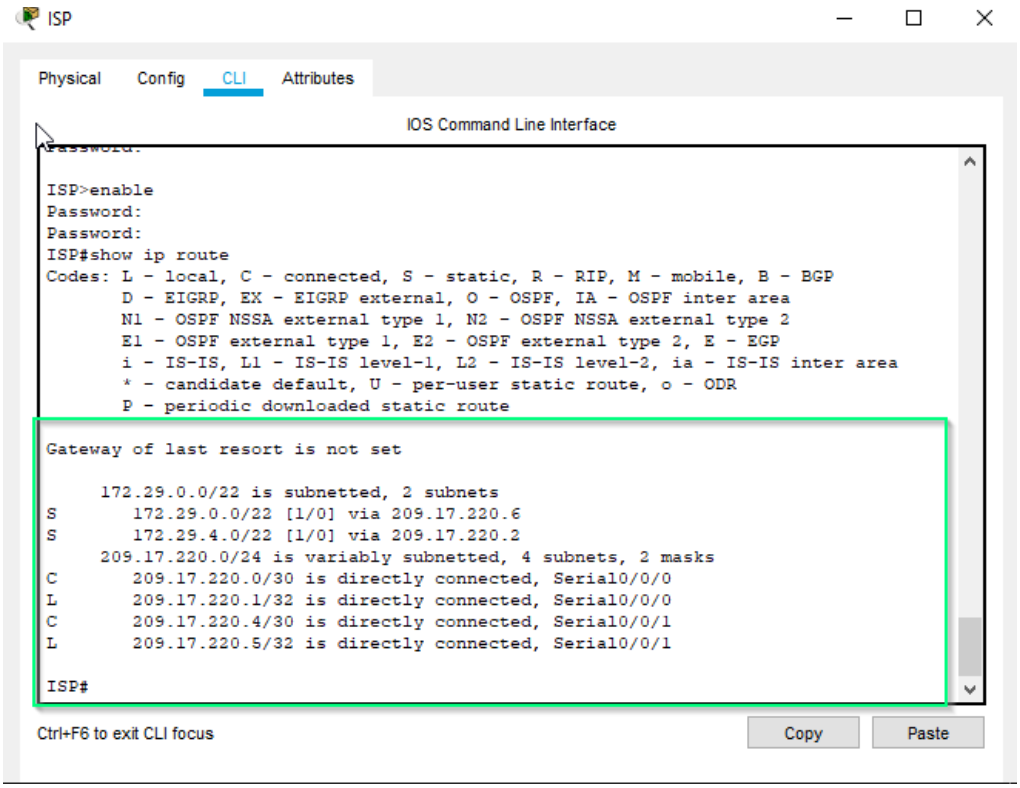
Paso 5: Rutas Redundantes

En las tablas de los Routers restantes se deben permitir las visualizaciones de las rutas redundantes para el caso de la ruta por defecto. captura 25, 26, 28 y 29

Paso 6: Verificar tabla de enrutamiento ISP

Nos fijamos que el Router ISP solo puede indicar sus rutas estáticas adicionales a las directamente conectadas ya que, en él, no se realizó ninguna configuración OSPF.

Figura 33 - Verificación enrutamiento ISP



Parte 3: Deshabilitar la propagación del protocolo OSPF.

Paso 1: **Deshabilitar Propagación OSPF**

Procedemos a no permitir las publicaciones por interfaces deshabilitando la propagación del protocolo OSPF, esta debe deshabilitarse en los Router que tengan conexiones hacia las LAN ejecutando el comando **passive-interface** para cada una de ellas.

Tabla 29 - Des habilitación propagación OSPF

Dispositivo	Des habilitación de propagación del protocolo OSPF
Medellin1	Medellin3> enable Medellin3# conf terminal Medellin3(config)# router ospf 1 Medellin3(config-router)# passive-interface S 0/0/0 Medellin3(config-router)# end Medellin3# write
Medellin2	Medellin2> enable Medellin2# conf terminal Medellin2(config)# router ospf 1 Medellin2(config-router)# passive-interface G 0/0 Medellin2(config-router)# end Medellin2# write
Medellin3	Medellin3> enable Medellin3# conf terminal Medellin3(config)# router ospf 1 Medellin3(config-router)# passive-interface G 0/0 Medellin3(config-router)# end Medellin3# write
Bogota1	Bogota1> enable Bogota1# conf terminal Bogota1(config)# router ospf 1 Bogota1(config-router)# passive-interface S 0/0/0 Bogota1(config-router)# end Bogota1# write
Bogota2	Bogota2> enable Bogota2# conf terminal Bogota2(config)# router ospf 1 Bogota2(config-router)# passive-interface G 0/0 Bogota2(config-router)# end Bogota2# write

Bogota3	Bogota3>enable Bogota3#conf terminal Bogota3(config)# router ospf 1 Bogota3(config-router)# passive-interface G 0/0 Bogota3(config-router)#end Bogota3# write

Parte 4: Verificación del protocolo OSPF.

Paso 1: **Verificar y documentar opciones de enrutamiento**

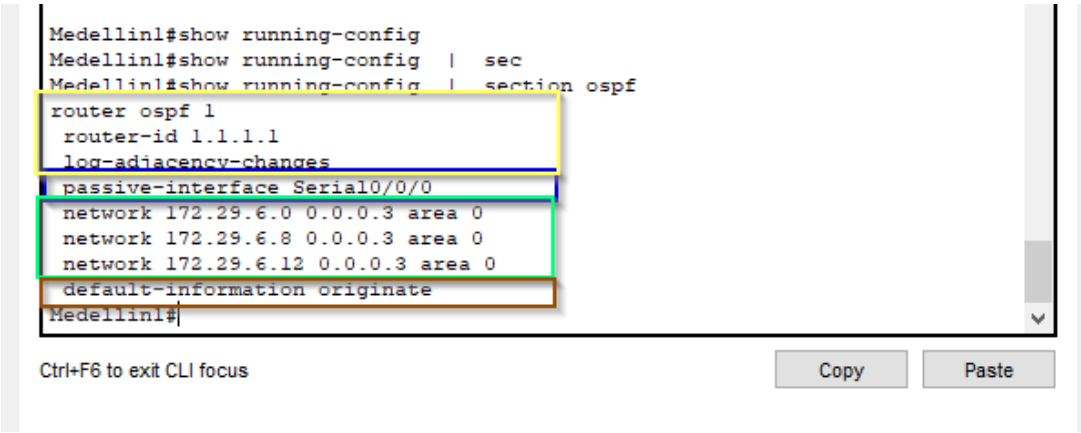
Para proceder a verificar las opciones de enrutamiento configuradas en los Routers, como el **passive interface**, la versión de OSPF y las interfaces que participan de la publicación entre otros datos procedemos a ejecutar el comando **show running-config** y reducimos la sección de OSPF tal y como se muestra en la Captura 34 y 35.

Procedemos con el comando en los routers Medellin1 captura 34 y observamos información como:

En el color amarillo tenemos la versión e identificación del router dentro de OSPF, en color azul las interfaces declaradas como pasivas, en color verde tenemos las redes presentadas dentro del router el cual tenemos configurada la interface S 0/0/0 Conexión a ISP como pasiva y en color Café default-information originate que lo que me explica que el router está enviando la información por defecto.

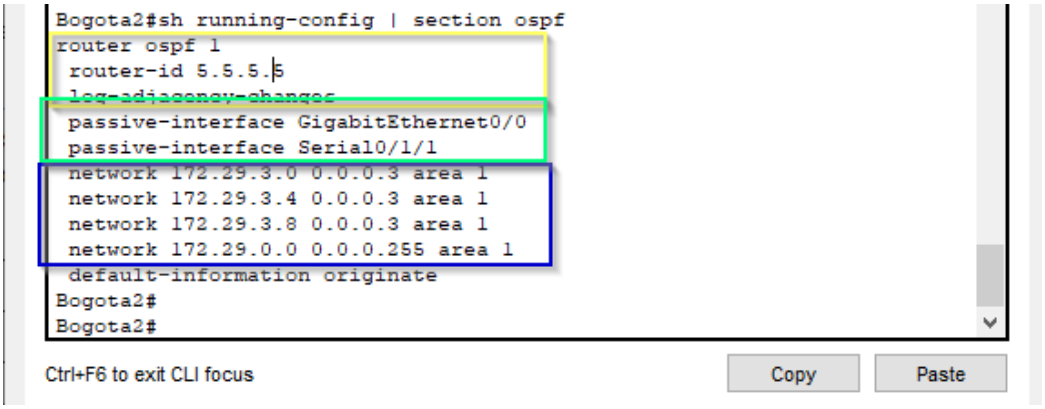
Dicha información es simple y la encontramos en cada uno de los dispositivos en los cuales tengamos o configuremos en un enrutamiento por medio del protocolo OSPF.

Figura 34 - Verificación información OSPF Medellin1



Divisamos en en la captura 35. la información del portocolo OSPF configurada para el Router Bogota2 y podemos obcerbar la misma estructura .

Figura 35 - Verificación información OSPF Bogota2

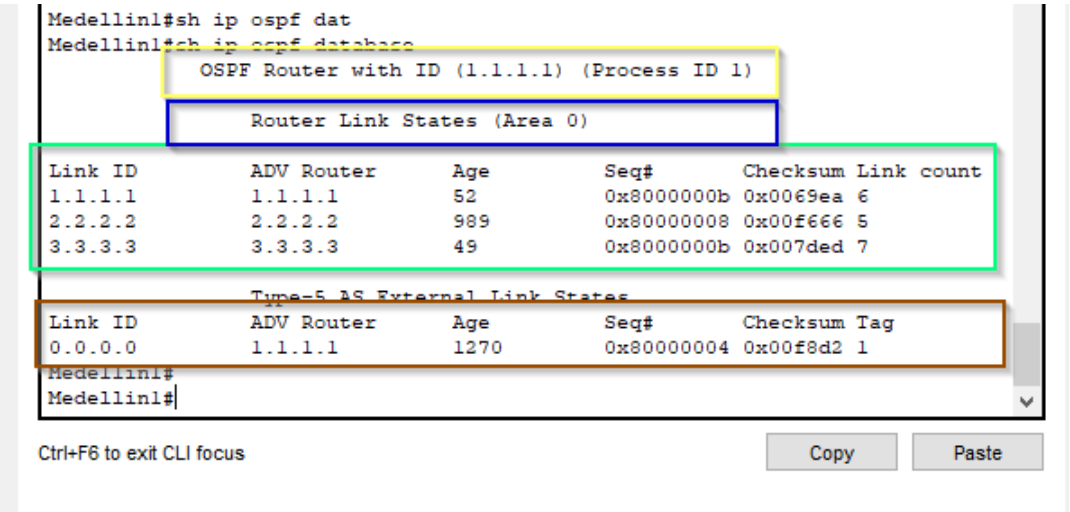


Paso 2: Verificar y documentar base de datos OSPF

Desde la base de datos OSPF del router Medellin1, captura36. Divisamos la información almacenada de la configuración de enrutamiento.

En color amarillo si nos fijamos podemos observar que tenemos la información de identificación del dispositivo y a cual proceso de enrutamiento pertenece en este caso el Router Medellin1 identificado con el ID 1.1.1.1 y que hace parte del OSPF identificado con el ID de proceso 1, en color azul encontramos el área a la cual pertenece el dispositivo, en color verde tenemos os ID de los vecinos o router conectados directamente y el tiempo de conexión y por último en color café la identificación del router perimetral.

Figura 36 - Verificación base de Datos OSFP Medellin1



Parte 5: Configurar encapsulamiento y autenticación PPP.

Paso 1: Autenticación PAT Medellin1.

Para esta configuración de verificación del enlace Medellin1 con ISP creamos un usuario a nivel local con su respectiva clave de autenticación **cisco** se configura el tipo de encapsulamiento de la interfaz (PPP) y procedemos a definir el tipo de autenticación como PAT.

Ver Tabla 30

Paso 2: Autenticación CHAT Bogota1

Para esta configuración de autenticación procedemos en el enlace Bogota1 con ISP configurando PAP que a diferencia de PPP nos permite autenticación Bidireccional.

Tabla 30 - Configuración PAT Bogota1 - CHAT Medellin2

Dispositivo	Encapsulación y Autenticación PPP
Medellin1	Medellin1> enable Medellin1# conf terminal. Medellin1(config)# username ISP password cisco Medellin1(config)# interface s0/0/0 Medellin1(config-if)# encapsulation ppp Medellin1(config-if)# ppp authentication pap Medellin1(config-if)# ppp pap sent-username ISP password cisco Medellin1(config-if)# end
Bogota1	Bogota1> enable Bogota1# conf terminal Bogota1(config)# username Bogota1 password cisco Bogota1(config)# interface s0/0/0 Bogota1(config-if)# encapsulation ppp Bogota1(config-if)# ppp authentication chap Bogota1(config-if)# end
ISP	ISP# conf terminal ISP(config)# username Medellin1 password cisco ISP(config)# interface 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)# username Bogota1 password cisco ISP(config)# interface s0/0/1 ISP(config-if)# encapsulation ppp

	ISP(config-if)# ppp authentication chap ISP(config-if)# end

figura 37 - Verificación de Encapsulamiento y

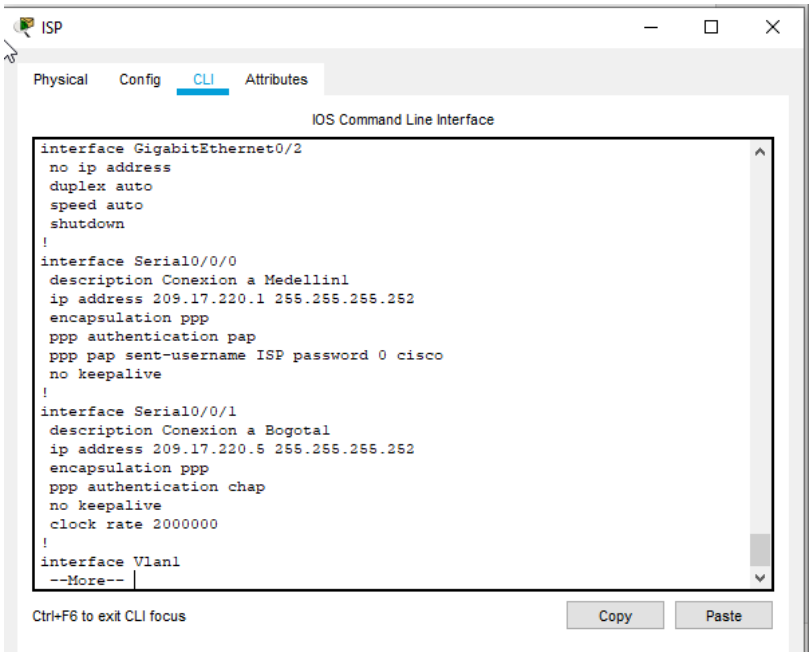


Figura 40 - Verificación autenticación Medellin1

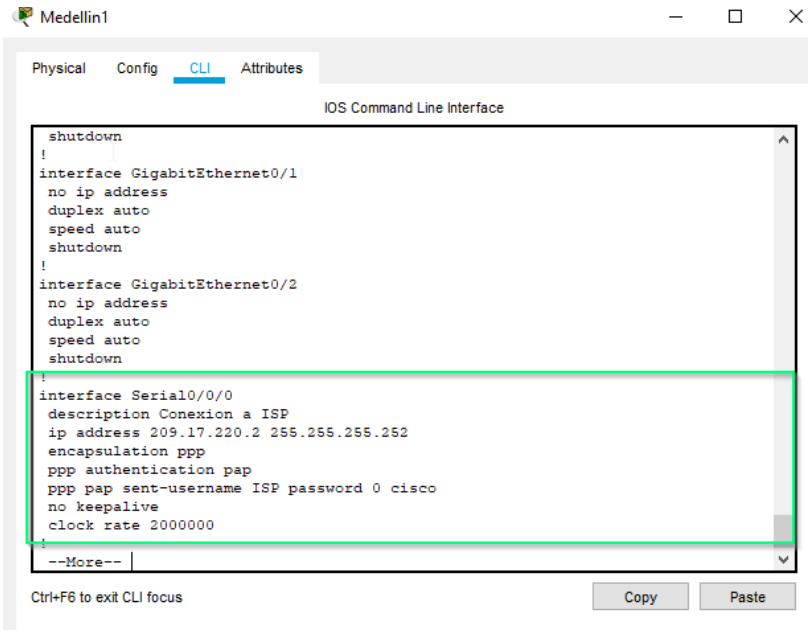
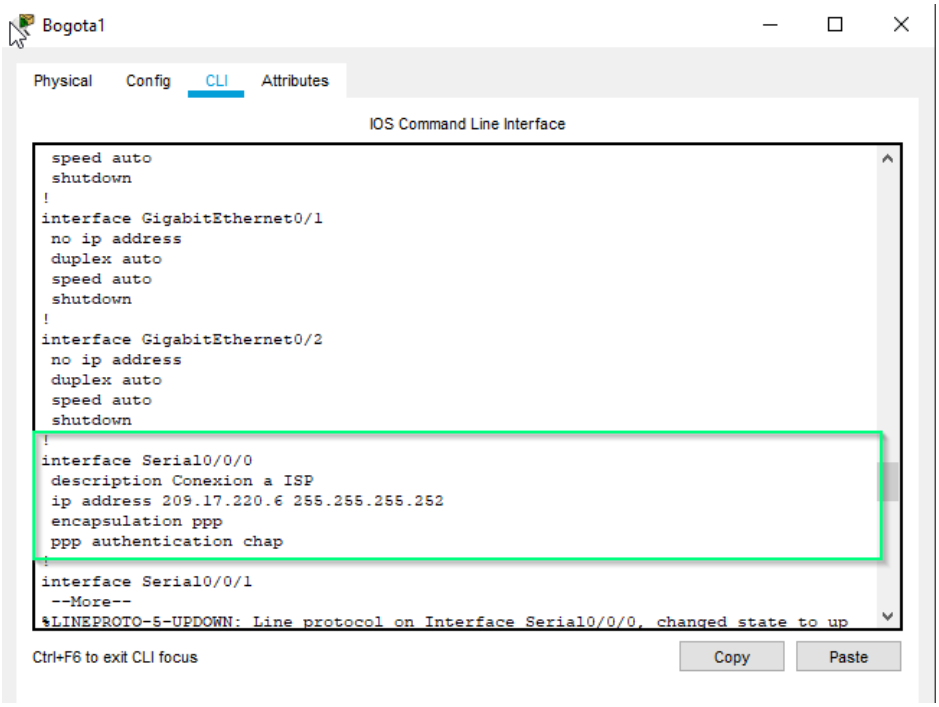


Figura 43 - Verificación autenticación Bogota1



Parte 6: Configuración de PAT.

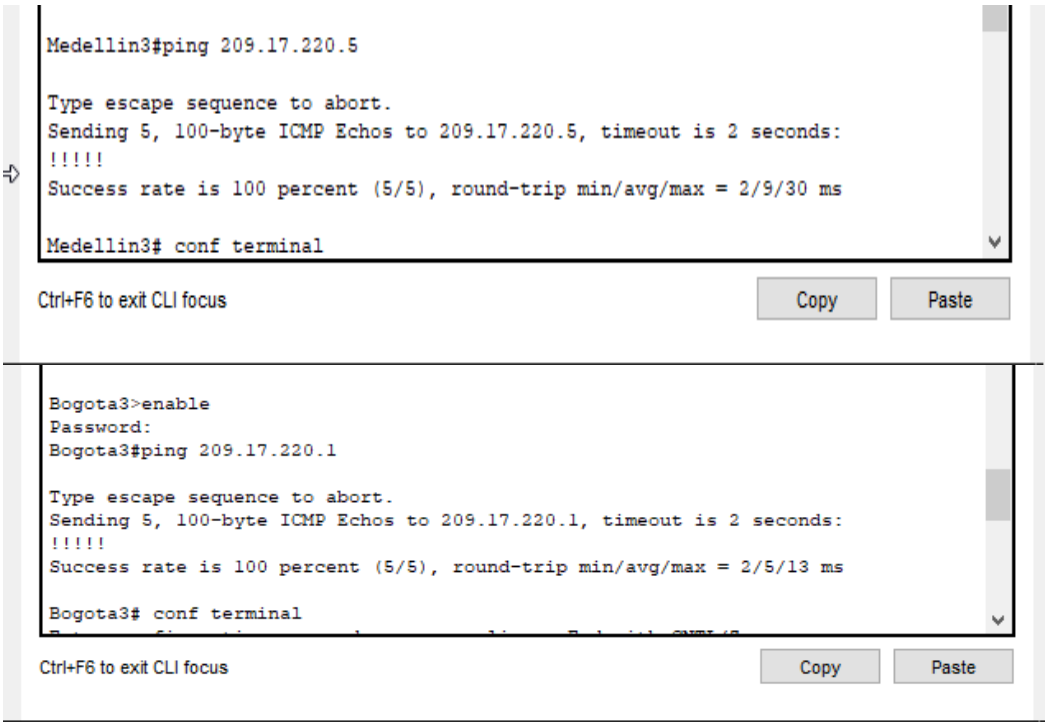
Paso 1: Verificación de conexión

En esta topología, si activamos el NAT en cada equipo de salida Medellin1 y Bogota1 los Routers internos de la ciudad no podrían llegar hasta los Routers internos en el otro extremo, sólo en el caso si existiera comunicación hasta los Routers Medellin1, ISP y Bogota1.

si tenemos 2 áreas OSPF (0, 1) configuradas, cada una llega hasta el ISP.

En la captura 40 podemos divisar el comportamiento del ping desde Medellin3 a ISP y de Bogota3 a ISP

Figura 46 - Verificación de conexión sin NAT



Paso 2: Configuración NAT Bogota1

Después de verificar lo indicado en el paso anterior procedemos a configurar el NAT en el Router Bogota1.

para proceder a verificar que la traducción de direcciones indique las interfaces de entrada y de salida, realizamos ping a la dirección y esta debe ser trasmitida automáticamente a la dirección de la interfaz serial externa del Router Bogota1, cómo en diferente puerto.

Para la lista de acceso NAT configuramos la ruta 172.29.0.0 0.0.3.255

Paso 3: Configuración NAT Medellin1

Proceda a configurar el NAT en el Router Medellin1. 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 externa del Router Medellin1, cómo diferente puerto.

Si queremos crear las nat en los routers frontera primero creamos una lista de control de acceso que me permita definir y chequear la red interna a la cual voy a permitir el acceso. paso continuo es realizar la asignación de NAT y definir los tipos de acceso de cada una de las interfaces conectadas estos dispositivos.

Para la lista de acceso NAT realizamos la configuración y la ruta Sumarizada 172.29.4.0 0.0.3.255.

Para finalizar la configuración mencionada y solicitada en los pasos 2 y 3 procedemos a utilizar los comandos especificados en laTabla 32.

Tabla 31 - Configuración PAT

Dispositivo	Configuración PAT
Medellin1	Medellin1# conf terminal Medellin1(config)# ip access-list standar LAN-Medellin Medellin1(config-std-nacl)# permit 172.29.4.0 0.0.3.255 Medellin1(config-std-nacl)# exit Medellin1(config)# ip nat inside source list LAN-Medellin interface S 0/0/0 overload Medellin1(config)# int S 0/0/0 Medellin1(config-if)# ip nat outside Medellin1(config-if)# exit Medellin1(config)# int S 0/1/0 Medellin1(config-if)# ip nat inside Medellin1(config-if)# exit Medellin1(config)# int S 0/1/1 Medellin1(config-if)# ip nat inside Medellin1(config-if)# exit

	Medellin1(config)# int S 0/0/1 Medellin1(config-if)# ip nat inside Medellin1(config-if)# end Medellin1# write
Bogota1	Bogota1>enable Bogota1#conf terminal Bogota1(config)# ip access-list standar LAN-Bogota Bogota1(config-std-nacl)# permit 172.29.0.0 0.0.3.255 Bogota1(config-std-nacl)# exit Bogota1(config)# ip nat inside source list LAN-Bogota interface S 0/0/0 overload Bogota1(config)# int S 0/0/0 Bogota1(config-if)# ip nat outside Bogota1(config-if)# exit Bogota1(config)# int S 0/1/0 Bogota1(config-if)# ip nat inside Bogota1(config-if)# exit Bogota1(config)# int S 0/1/1 Bogota1(config-if)# ip nat inside Bogota1(config-if)# exit Bogota1(config)# int S 0/0/1 Bogota1(config-if)# ip nat inside Bogota1(config-if)# end Bogota1# write

Ya configurado Medellin1 y Bogota1 podemos divisar u observar en las capturas 41 y 42 la traducción de direcciones al enviar solicitudes de conexión desde las PC internas a ISP.

Figura 49 - Verificación NAT Bogota1

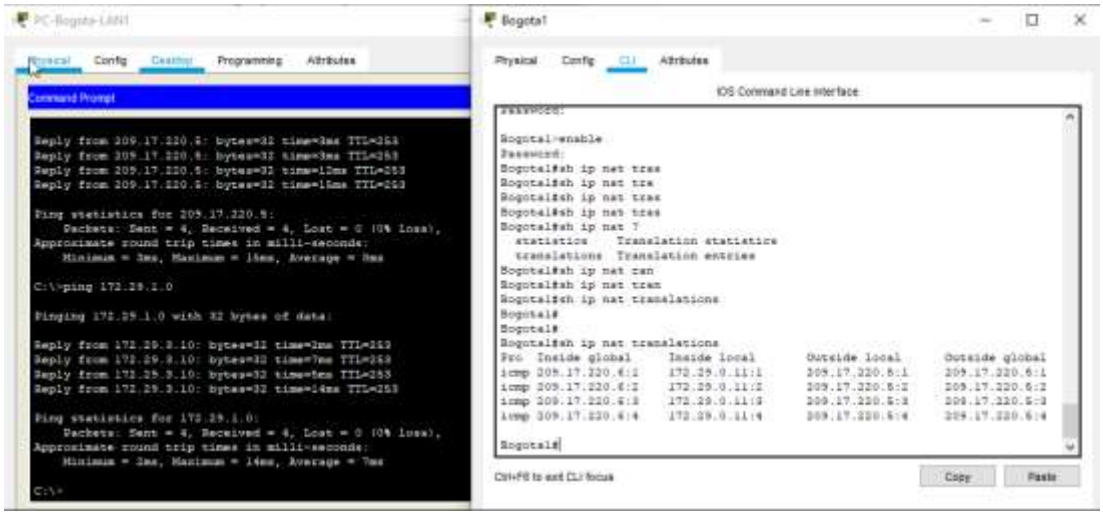
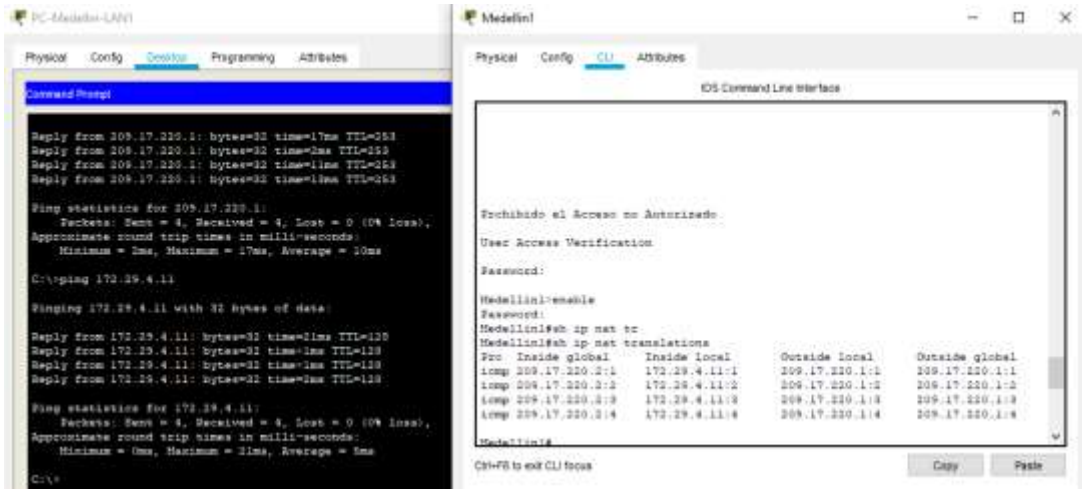


Figura 52 - Verificación NAT Medellin1



Parte 7: Configuración del servicio DHCP.

En la Tabla 31 vamos a insertar los comandos que me permiten la configuración de las configuraciones solicitadas en los pasos del 1 al 4.

Paso 1: Configurar Bogota2 como servidor DHCP

Vamos a configurar la red Bogota2 y Bogota3 donde el Router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Paso 2: Habilitar Broadcast Bogota3

El Router Bogota3 deberá habilitar el paso de los mensajes broadcast hacia la IP del Router Bogota2; para eso usaremos el comando “helper-addres”.

Paso 3: Configurar Medellin2 como servidor DHCP

Vamos a configurar la red Medellin2 y Medellin3 donde el Router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Paso 4: Habilitar Broadcast Medellin3

El Router Medellin3 deberá habilitar el paso de los mensajes Broadcast hacia la IP del Router Medellin2; para eso usaremos el comando “helper-addres”.

Tabla 32 - Configuración DHCP

Dispositivo	Configuración DHCP
Bogota2	Bogota2# conf terminal Bogota2(config)# ip dhcp excluded-address 172.29.0.1 172.29.0.10 Bogota2(config)# ip dhcp excluded-address 172.29.1.1 172.29.1.10 Bogota2(config)# ip dhcp pool Bogota-LAN1 Bogota2(dhcp-config)# network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)# default-router 172.29.0.1 Bogota2(dhcp-config)# dns-server 4.4.4.4 Bogota2(dhcp-config)# domain-name lan1.Bogota.com Bogota2(dhcp-config)# exit

	Bogota2(config)# ip dhcp pool Bogota-LAN2 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 4.4.4.4 Bogota2(dhcp-config)# domain-name lan2.Bogota.com Bogota2(dhcp-config)# end Bogota2# write
Bogota3	Bogota3> enable Bogota3# conf terminal Bogota3(config)# int G 0/0 Bogota3(config-if)# ip helper-address 172.29.0.1 Bogota3(config-if)# end Bogota3# write
Medellin2	Medellin2> enable Medellin2# conf terminal Medellin2(config)# ip dhcp excluded-address 172.29.4.1 172.29.1.10 Medellin2(config)# ip dhcp excluded-address 172.29.4.129 172.29.4.138 Medellin2(config)# ip dhcp pool Medellin-LAN1 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 4.4.4.4 Medellin2(dhcp-config)# domain-name lan1.Medellin.com Medellin2(dhcp-config)# exit Medellin2(config)# Medellin2(config)# ip dhcp pool Medellin-LAN2 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 4.4.4.4 Medellin2(dhcp-config)# domain-name lan2.Medellin.com Medellin2(dhcp-config)# end Medellin2# write

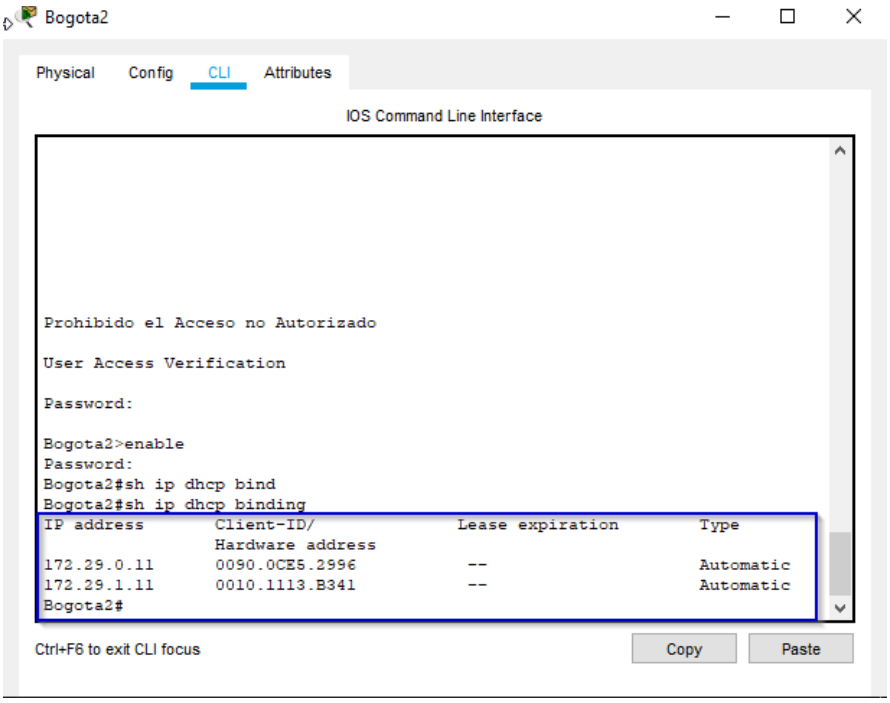
Medellin3	Medellin3> enable Medellin3# conf t Medellin3(config)# int G 0/0 Medellin3(config-if)# ip helper-address 172.29.4.1 Medellin3(config-if)# exit Medellin3(config)# write

Ya realizada dicha configuración procedemos a probar o verificar el estado del protocolo de direccionamiento DHCP con ayuda del siguiente comando **show ip dhcp binding**

En la captura 43 podemos evidenciar que hay 2 direcciones asignadas automáticamente

para las PC de las LAN 1 y 2 de la red Bogota.

Figura 55 - Verificación estado DHCP Bogota2



En la captura 44 evidenciamos al igual que en el router Bogota2, que hay 2 host conectados con direccionamiento automático, lo cual en este caso si observamos la topología vemos que son las PC de las LAN 1 y 2 de Medellin.

Figura 58 - Verificación estado DHCP Medellin2

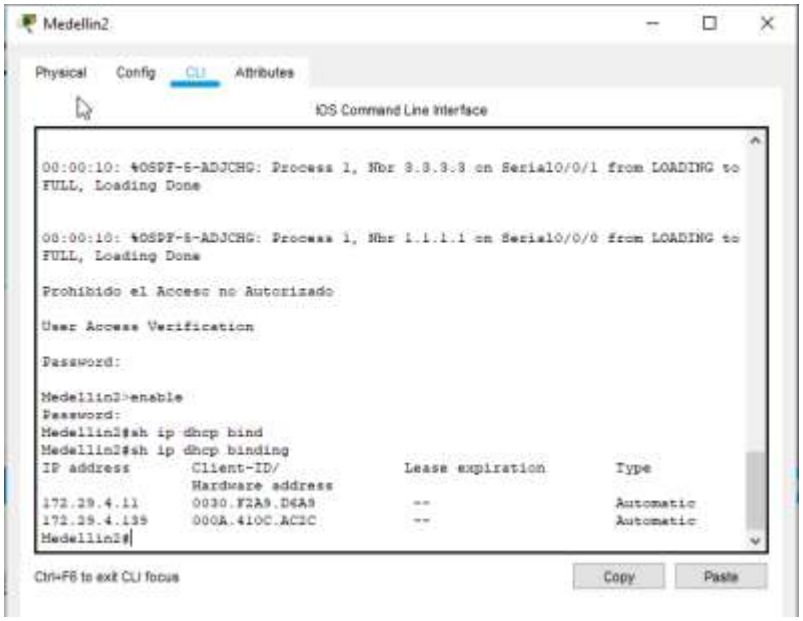


Figura 61- Verificación DHCP PC-Medellin-LAN1

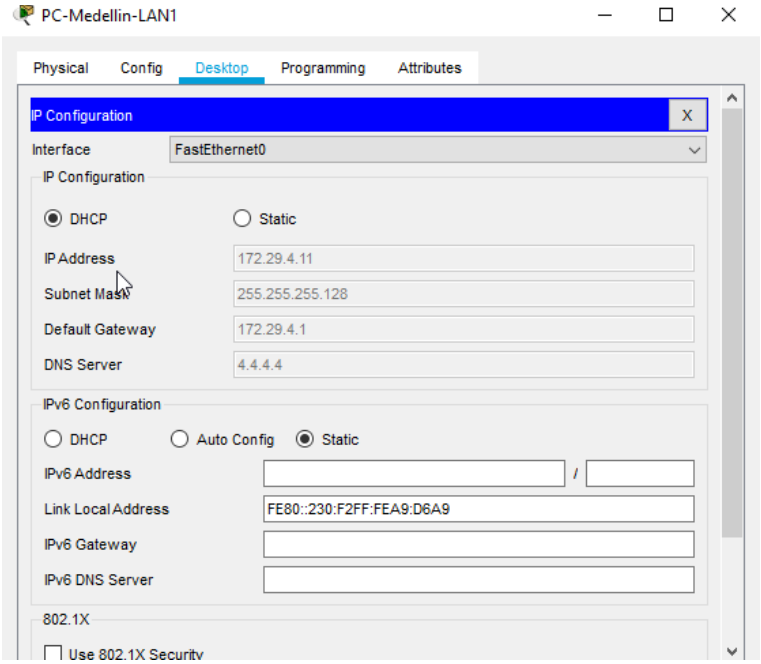


Figura 64 - Verificación DHCP PC-Medellin-LAN2

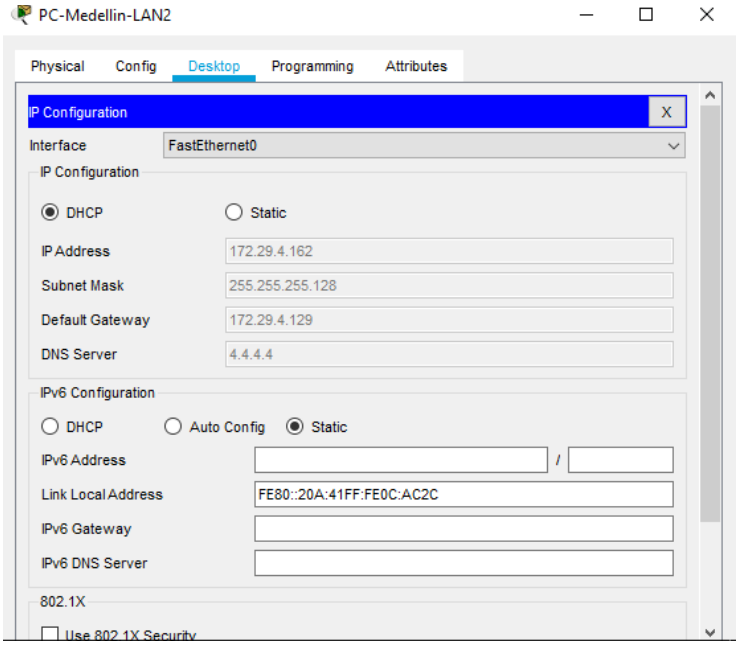


Figura 67 - Verificación DHCP PC-Bogota-LAN1

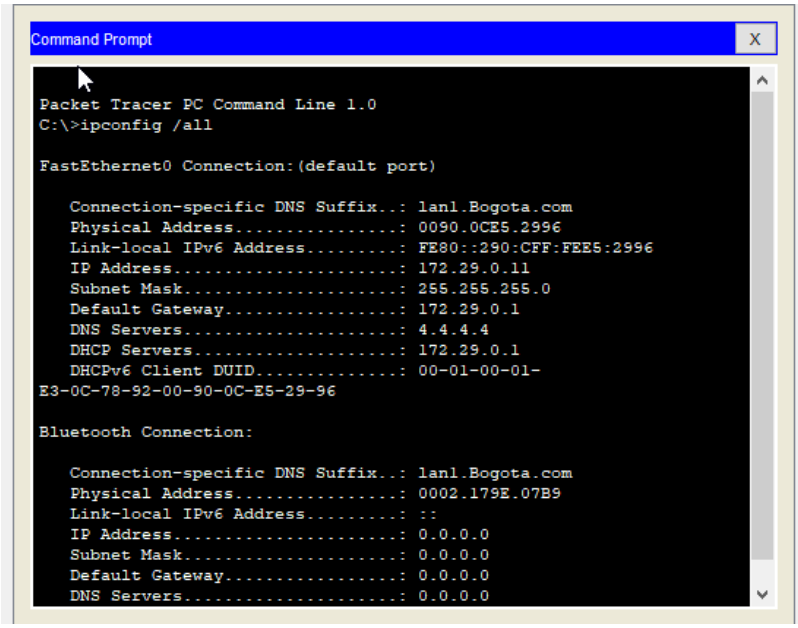
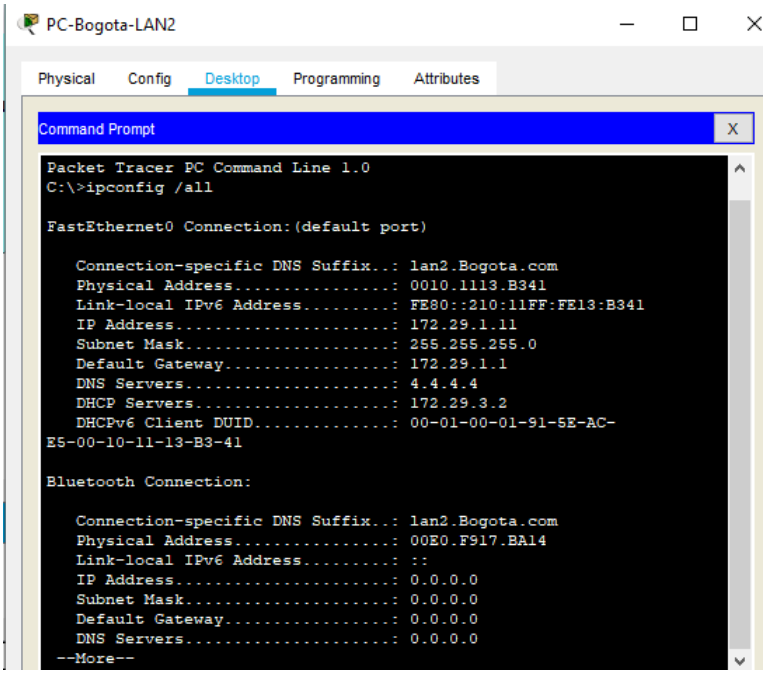


Figura 70 - Verificación DHCP PC-Bogota-LAN2



CONCLUSIONES

La configuración de un servidor de internet es de mucho cuidado y concentración al momento de realizar estos pasos puesto que con un solo error tendríamos que repetir varios procesos los cuales se pueden realizar por intranet

La configuración de enrutamiento RIP es de vital importancia en la red informática puesto que nos permite presentar las interfaces conectadas directamente.

Para la programación de un servidor es de vital importancia la asignación de contraseñas cifradas y no cifradas para seguridad de este y a su vez no permitir manipulaciones indebidas que se puedan lograr por medio de la internet o intranet

La asignación manual de direccionamiento IP en redes pequeñas resulta ser una tarea sencilla en las redes pequeñas, pero a medida que la red crece con ella nace la necesidad de automatizar el proceso de esto se deriva la necesidad o nace el proceso DHCP protocolo de configuración dinámica de host el cual permite combinar la configuración manual con la asignación dinámica, la cual nos permite una configuración de direccionamiento IP para una red de internet o telecomunicaciones

En cada escenario podemos notar la importancia de los protocolos de enrutamiento, podemos notar la diferencia entre el manejo de enrutamiento estático y dinámico y a la vez su importancia y su relevancia.

RESUMEN

En este trabajo de grado se logra afianzar de manera práctica y oportuna los conocimientos logrados o adquiridos a lo largo de este diplomado realizando simulaciones prácticas de los escenarios planteados en el mismo, con entornos corporativos solucionados llevando a cabo el uso de la plataforma CISCO.
En esta ocasión presenciamos dos escenarios en los cuales aplicamos los conocimientos adquiridos tanto en configuración y seguridad para el aseso a los mismos con protocolos de enrutamiento (RIP, OSPF) también mediante TELNET Y SSH y comunicaciones mediante los enlaces troncales, asignaciones automáticas de direcciones IP o por medio de DHCP y finalizando la traducción de direcciones de red NAT.

Palabras Claves: red de telecomunicaciones, intranet, internet, topología, interfaz

BIBLIOGRAFIA

Configuración RIP. Recuperado de: https://ccnadesdecero.es/configuracion-del-protocolo-rip/

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

Temática: Configuración de un sistema operativo de red CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

Temática: Direccionamiento IP CISCO. (2019). Direccionamiento IP Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

Temática: División de redes IP en subredes CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

ANEXO 1 – Descarga Escenarios Packet Tracer

Link de descarga escenarios:

https://drive.google.com/file/d/1fQ_N_S0kbY_jpXC972ejFKK6URDbimyX/view?usp=sharing

https://drive.google.com/file/d/1AIgXFBJjP4KFFUEHQkLsx0-5RNFiyXgy/view?usp=sharing