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

BRYAN ALONSO BURGOS VELASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO CCNA
BOGOTA
2020

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

BRYAN ALONSO BURGOS VELASQUEZ

TRABAJO DE GRADO INGENIERIA DE SISTEMAS

GUSTAVO RODRIGUEZ
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA
DIPLOMADO DE PROFUNDIZACION CISCO CCNA
BOGOTA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá 07, 07, 2020

Se dedica el siguiente trabajo a todos los tutores del país que hacen posible el desarrollo de la educación.

AGRADECIMIENTOS

Se dedica el siguiente trabajo a todos los tutores del país que hacen posible el desarrollo de la educación.

CONTENIDO

Pág.

1. INTRODUCCIÓN 12
2. OBJETIVOS 13
2.1 OBJETIVO GENERAL 13
2.2 OBJETIVOS ESPECÍFICOS 13
3. DESARROLLO DEL PROYECTO 14
4. ESCENARIO 1 14
4.1. Inicializar dispositivos 15
4.1.1 Configurar los parámetros básicos de los dispositivos 15
4.1.2 Configurar R1 16
4.1.3 Configurar R2 17
4.1.4 Configurar R3 18
4.1.5 Configurar S1 19
4.1.6 Configurar S3 20
4.1.7 Verificar la conectividad de la red 20
4.2 La configuración del S1 incluye las siguientes tareas 22
4.2.1 Configurar el S3 23
4.2.2 Configurar R1 24
4.2.3 Verificar la conectividad de la red 24
4.3 Configurar el protocolo de routing dinámico RIPv2 25
4.3.1 Configurar RIPv2 en el R2 26
4.3.2 Configurar RIPv2 en el R3 27
4.3.3 Verificar la información de RIP 27
4.4 Implementar DHCP y NAT para IPv4 28
4.4.1 Configurar la NAT estática y dinámica en el R2 29
4.4.2 Verificar el protocolo DHCP y la NAT estática 30
4.5 Configurar NTP 32
4.6 Restringir el acceso a las líneas VTY en el R2 33
4.6.1 Introducir comando CLI adecuado que se necesita para mostrar lo siguiente 33
5. ESCENARIO 2 35
5.1 Configuración del enrutamiento 37
5.1.1 Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática 37

5.1.2 Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF. 41

5.1.3 El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22 42

5.2 Tabla del enrutamiento 42

5.2.1 Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas 43

5.3 Deshabilitar la propagación del protocolo OSPF 45

5.3.1 Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF 45

5.4 Verificación del protocolo OSPF 45

5.4.1 Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red. 45

5.5 Configurar encapsulamiento y autenticación PPP 47

5.5.1 Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT 47

5.5.2 El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT 48

5.6 Configuración de PAT 48

5.6.1 En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), 48

5.6.2 Proceda a configurar el NAT en el router Bogotá1 y Medellin1 50

5.7 Configuración del servicio DHCP 50

5.7.1 Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan 50

5.7.2 El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2 51

5.7.3 Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan 51

5.7.4 Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2. 52

6. ENLACE DE DESCARGA ARCHIVOS PKT 53

CONCLUSIONES 54

BIBLIOGRAFÍA 55

TABLA DE ILUSTRACIONES (TABLAS)

Tabla 1 Configuración router y switch 15
Tabla 2 Configuración nube internet 15
Tabla 3 Configuración router R1 16
Tabla 4 Configuración router R2 17
Tabla 5 Configuración router R3 18
Tabla 6 Configuración S1 19
Tabla 7 Configuración S3 20
Tabla 8 Verificación de conectividad 20
Tabla 9 Configuración Vlan S1 22
Tabla 10 Configuración Vlan S3 23
Tabla 11 Configuración subinterfaz R1 24
Tabla 12 Verificación conectividad switch y R1 25
Tabla 13 Configuración RIPv2 26
Tabla 14 Configuración RIPv2 en R2 26
Tabla 15 Configuración RIPv2 en R3 27
Tabla 16 Validación RIP 28
Tabla 17 Configuración DHCP en Vlan 21 y 23 29
Tabla 18 Configuración NAT en R2 29
Tabla 19 Verificación NAT y DHCP 30
Tabla 20 Configuración NTP 32
Tabla 21 Restricción de línea VTY en R2 33
Tabla 22 Validación mediante comandos 33
Tabla 23 Direccionamiento de red 35
Tabla 24 Configuración routers Medellín, Bogotá y ISP 36
Tabla 25 Configuración direcciones Ip y Ospf en router ISP 37
Tabla 26 Configuración direcciones Ip y Ospf en router MEDELLIN1 37
Tabla 27 Configuración direcciones Ip y Ospf en router MEDELLIN2 38
Tabla 28 Configuración direcciones Ip y Ospf en router MEDELLIN3 39
Tabla 29 Configuración direcciones Ip y Ospf en router BOGOTA1 39
Tabla 30 Configuración direcciones Ip y Ospf en router BOGOTA2 40
Tabla 31 Configuración direcciones Ip y Ospf en router BOGOTA3 41
Tabla 32 Configuración ruta por defecto router BOGOTA1 y MEDELLIN1 41
Tabla 33 Configuración rutas estáticas en ISP 42
Tabla 34 Interfaces router 45
Tabla 35 Autenticación PPP routers ISP, MEDELLIN1 47
Tabla 36 Autenticación CHAP routers ISP, BOGOTA1 48
Tabla 37 Autenticación PAT routers MEDELLIN1, BOGOTA1 49
Tabla 38 Creación grupo extensiones excluidas router MEDELLIN2 y MEDELLIN3 50
Tabla 39 Configuración broadcast hacia MEDELLIN2 51
Tabla 40 Creación grupo extensiones excluidas router BOGOTA2 y BOGOTA3 51
Tabla 41 Configuración broadcast hacia MEDELLIN2 52

TABLA DE ILUSTRACIONES (ILUSTRACIÓN)

Ilustración 1 Topología escenario 1 14
Ilustración 2 Topología conectada 21
Ilustración 3 Validación conexión en router's 21
Ilustración 4 Validación en Internet pc 22
Ilustración 5 Verificación conectividad S1 y S3 25
Ilustración 6 Se ejecuta comando #show ip protocols 28
Ilustración 7 Se ejecuta comando #show ip route rip 28
Ilustración 8 Se ejecuta comando Show run 28
Ilustración 9 Validación DHCP en PC-A 31
Ilustración 10 Validación DHCP en PC-C 31
Ilustración 11 Ping PC-A y PC-C 31
Ilustración 12 Ingreso correcto servidor web 32
Ilustración 13 Validación NTP mediante #show ntp associations 32
Ilustración 14 Validación ACL mediante Router R1 33
Ilustración 15 Topología escenario 2 35
Ilustración 16 enrutamiento router ISP 43
Ilustración 17 enrutamiento router MEDELLIN1 43
Ilustración 18 enrutamiento router MEDELLIN2 43
Ilustración 19 enrutamiento router MEDELLIN3 44
Ilustración 20 enrutamiento router BOGOTA1 44
Ilustración 21 enrutamiento router BOGOTA2 44
Ilustración 22 enrutamiento router BOGOTA3 45
Ilustración 23 enrutamiento ospf MEDELLIN1 46
Ilustración 24 enrutamiento ospf MEDELLIN2 46
Ilustración 25 enrutamiento ospf MEDELLIN3 46
Ilustración 26 enrutamiento ospf BOGOTA1 46
Ilustración 27 enrutamiento ospf BOGOTA2 47
Ilustración 28 enrutamiento ospf BOGOTA3 47
Ilustración 29 ping pc's a propia red (PC1 y PC2) 49
Ilustración 30 Validación Nat en Medellin1 50
Ilustración 31 Validación Nat en Bogota1 50
Ilustración 32 Se valida DHCP en terminales de Medellín, DHCP ok 52
Ilustración 33 Se valida DHCP en terminales de Bogotá, DHCP ok 52

GLOSARIO

NETWORKING: Una red o red de datos es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos. En las redes de cómputo, dispositivos de computación conectados en red (nodos de la red) pasan los datos entre sí a lo largo de las conexiones de datos. Las conexiones (enlaces de red) entre los nodos se establecerán a partir de los medios de comunicación, ya sea por cable o medios inalámbricos.

OSPF: El protocolo Open Shortest Path First (OSPF), definido en RFC 2328 , es un Internal Gateway Protocol (IGP) que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo.

NAT: Refiere a un proceso específico que implica la reordenación de una única dirección IP en otra dirección IP, a menudo pública, mediante la alteración de la información de red y la información de dirección que se encuentra en la cabecera IP de los paquetes de datos.

RIP: Es un protocolo de puerta de enlace interna o interior utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados.

DHCP: Protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

VLAN: Método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física

SLAAC: Método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido.

RESUMEN

A través del siguiente trabajo se busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado, en el cual el estudiante dispone dos escenarios asignados.

PALABRAS CLAVE: Telecomunicaciones, GNS3, Packet tracer, Networking, topología, DHCP, NAT, OSPF, RIP, NTP, ACL.

INTRODUCCIÓN

Mediante el desarrollo del presente trabajo se pretende realizar pruebas de habilidades de CCNA en diseño e implementación de soluciones integradas lan / wan, en donde todo estudiante demostrara mediante guías de actividades, la comprensión y extensión de conocimiento en temáticas como enrutamiento, seguridad y disponibilidad y un recurso web para la empresa, manejando diferentes protocolos RIPv2, OSPFv2, OSPFv3, DHCPv4 y DHCPv6 en switches y routers, también aprenderá a diseñar e implementar NAT dinámicas y estáticas, listas de acceso bajo los protocolos IPv4 y IPv6, entre otros temas de gran importancia para afianzar conocimientos en networking.

Para el desarrollo de la presente actividad, se cuenta con aplicativos de simulación tales como Packet Tracer, Wireshark, que además de simular la creación de una red, ayudara a planear y descubrir posibles errores en la práctica real de estas actividades.

Estas tecnologías están fundamentadas en redes informáticas por esto es fundamental como profesionales conocer la historia y evolución de estas redes distinguir los estándares y las organizaciones que se encargan de su desarrollo y cuáles de estos tienen vigencia en las redes actuales.

OBJETIVOS

OBJETIVO GENERAL

Implementar en los escenarios habilidades ganadas a través de prácticas, teorías y simulaciones con ayuda del aplicativo cisco Packet tracert, en el cual se darán soluciones ingenieriles a las problemáticas networking.

OBJETIVOS ESPECÍFICOS

Generar topologías de red de acuerdo a casos expuestos

Mantener una red segura de acuerdo a seguridad que se le puede asignar a los diferentes dispositivos.

Verificación de conectividad en topología.

Interactuar con los diferentes dispositivos, entablando comunicación para interconectividad de redes.

DESARROLLO DEL PROYECTO

El desarrollo de este proyecto pretende solucionar dos escenarios de red, esto con la ayuda de una guía de herramientas, tutores y el software packet tracert.

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

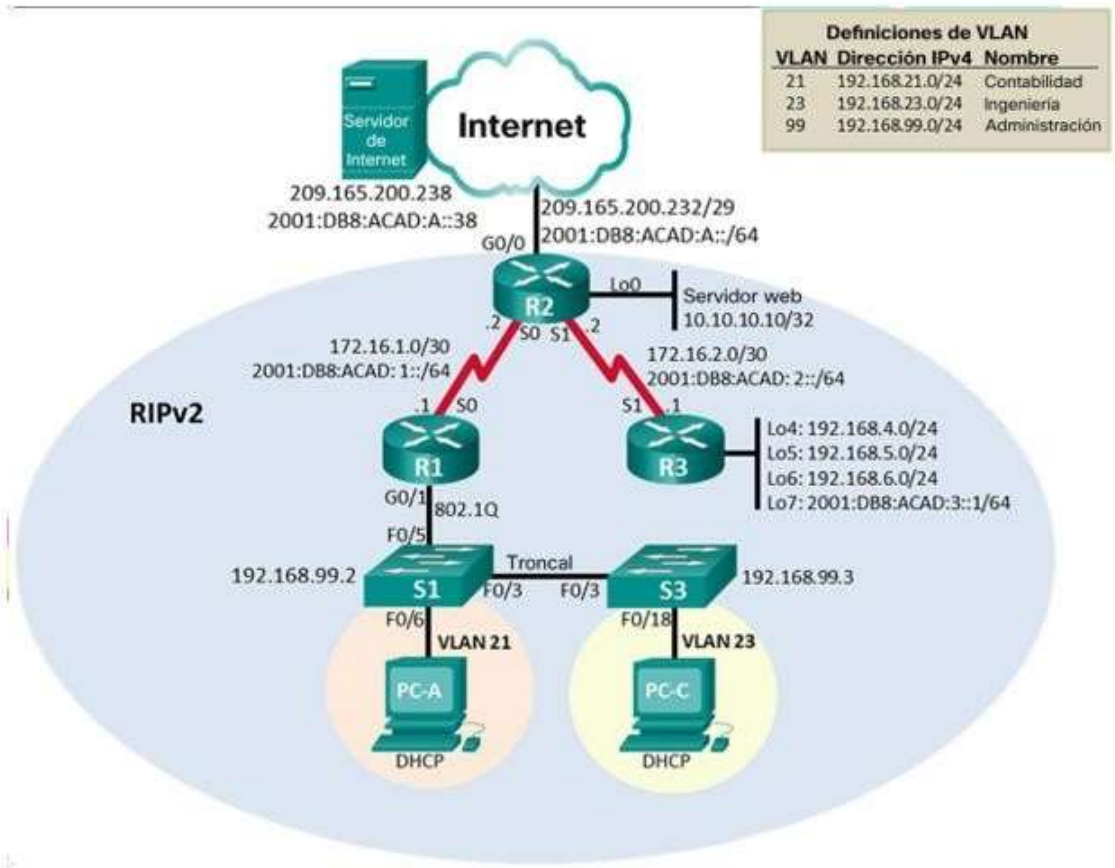


Ilustración 1 Topología escenario 1

4.1. Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Con la siguiente configuración se confirmará que los routers adquiridos no tengan datos cargados, tales como base de datos Vlan y otros.

Tabla 1 Configuración router y switch

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

Fuente propia

4.1.1 Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

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

El siguiente direccionamiento se utilizará para la nube utilizada en el escenario 1

Tabla 2 Configuración nube internet

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

Gateway predeterminado	209.165.200.234
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::45

Fuente propia

4.1.2 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Con la siguiente configuración, todos los routers tendrán parámetros de inicio tal como ingreso, alertas de intruso, claves cifradas y otros; de igual manera se inicia asignación de dirección en interfaz s0/0/0.

Tabla 3 Configuración router R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configute terminal 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 con 0 R1(config)# password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)# line vty 0 4 R1(config)# password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Mensaje MOTD	R1(config)# banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/0	R1(config)# interface s0/0/0 R1(config-if)# description R1 - R2 R1(config-if)# clock rate 128000 R1(config-if)# ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 unicast-routing R1(config)#int s0/0/0 R1(config-if)# ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown R1(config-if)#exit

Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Fuente propia

Nota: Todavía no configure G0/1.

4.1.3 Configurar R2

La configuración del R2 incluye las siguientes tareas:

Con la siguiente configuración, todos los routers tendrán parámetros de inicio tal como ingreso, alertas de intruso, claves cifradas y otros; Se establece direccionamiento ipv4 y ipv6 en router, además de configuración de internet y loopback.

Tabla 4 Configuración router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configute terminal 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 con 0 R2(config-line)# password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)# line vty 0 4 R2(config-line)# password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)# service password-encryption
Habilitar el servidor HTTP	R2(config)# Ip nat inside source static 10.10.10.10 209.165.200.229
Mensaje MOTD	R2(config)# banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/0	R2(config)#ipv6 unicast-routing R2(config)# interface se0/0 R2(config-if)# description R2-R1 R2(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config)# ipv6 address 2001:DB8:ACAD:1::2/64 R2(config)# no shutdown

Interfaz S0/0/1	R2(config)# interface se0/0/1 R2(config-if)# description R2- R3 R2(config-if)# clock rate 128000 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config)# ipv6 address 2001:db8:acad:2::2/64 R2(config-if)# no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)# interface GigabitEthernet0/0 R2(config-if)# description R2-internet R2(config-if)# Ip address 209.165.200.234 255.255.255.248 R2(config-if)# ipv6 address 2001:DB8:ACAD:A::45/64 R2(config-if)# no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)# interface l0 R2(config-if)# description R2-web Server R2(config-if)# ip address 10.10.10.1 255.255.255.0
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente propia

4.1.4 Configurar R3

La configuración del R3 incluye las siguientes tareas:

Con la siguiente configuración, todos los routers tendrán parámetros de inicio tal como ingreso, alertas de intruso, claves cifradas y otros; Se establece direccionamiento ipv4 y ipv6 en router, además de configuración en loopback.

Tabla 5 Configuración router R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configute terminal Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	R3(config)# enable secret class
Contraseña de acceso a la consola	R3(config)# line con 0 R3(config)# password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)# line vty 0 4 R3(config)# password cisco R3(config-line)#login

Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	R3(config)# banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/1	R3(config)#ipv6 unicast-routing R3(config)# interface s0/0/1 R3(config-if)# description R3-R2 R3(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# Ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)# no shutdown
Interfaz loopback 4	R3(config-if)# int lo4 R3(config-if)# ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)# int lo5 R3(config-if)# ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)# int lo6 R3(config-if)# ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)# Int lo7 R3(config-if)# Ipv6 address 2001:DB8:ACAD:3::1/64

4.1.5 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se establece configuración inicial en Switch 1, en el cual tendrán parámetros de inicio tal como ingreso, alertas de intruso, claves cifradas y otros.

Tabla 6 Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# enable Switch(config)# configure terminal 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 con 0 S1(config)# password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)# line vty 0 4 S1(config)# password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption

Mensaje MOTD	S1(config)# banner motd $Se prohíbe el acceso no autorizado.$

Fuente propia

4.1.6 Configurar S3

La configuración del S3 incluye las siguientes tareas:

Se establece configuración inicial en Switch 3, en el cual tendrán parámetros de inicio tal como ingreso, alertas de intruso, claves cifradas y otros.

Tabla 7 Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)# enable Switch(config)# configure terminal 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 con 0 S3(config)# password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)# line vty 0 4 S3(config)# password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	S3(config)# banner motd $Se prohíbe el acceso no autorizado.$

Fuente propia

4.1.7 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:

Se valida enrutamiento configurado en R1, R2 y nube, se comprueba en *Ilustración 3 e Ilustración 4,* que conectividad y configuración se encuentran correctamente asignados.

Tabla 8 Verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso

R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.234	Exitoso

Fuente propia

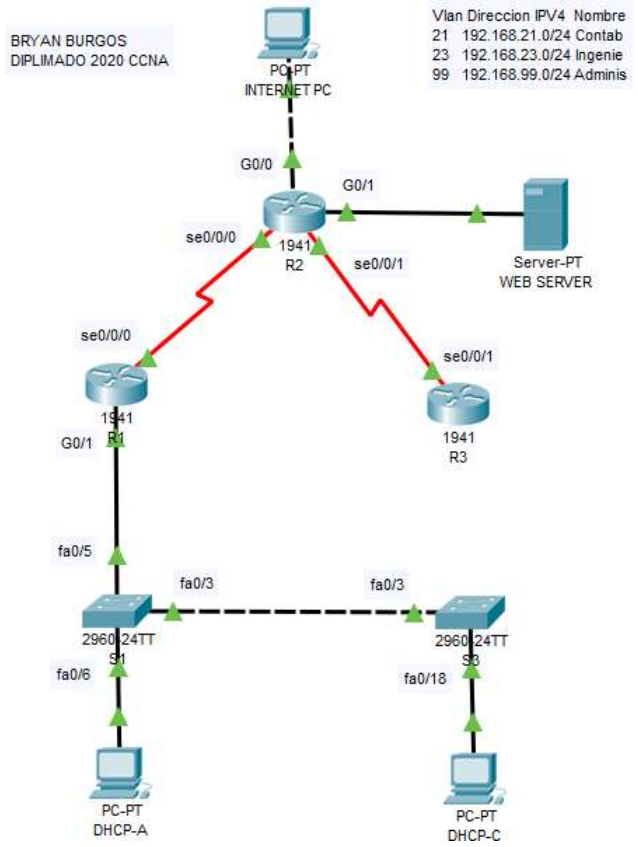


Ilustración 2 Topología conectada

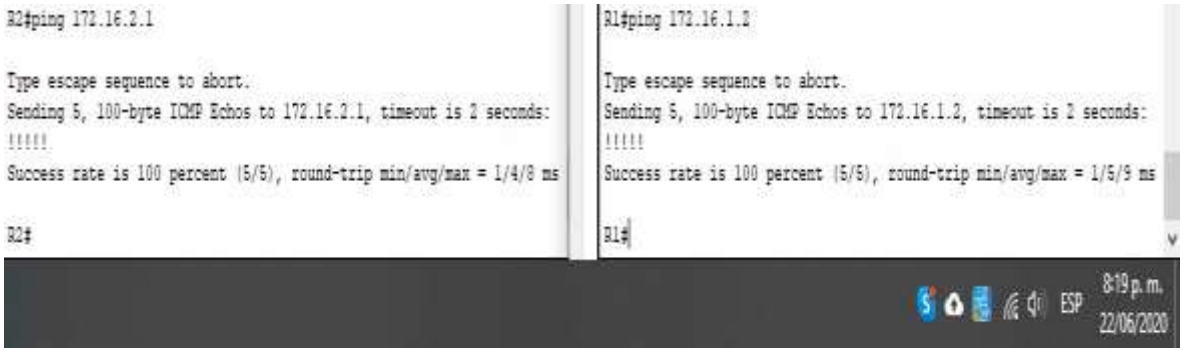


Ilustración 3 Validación conexión en router's

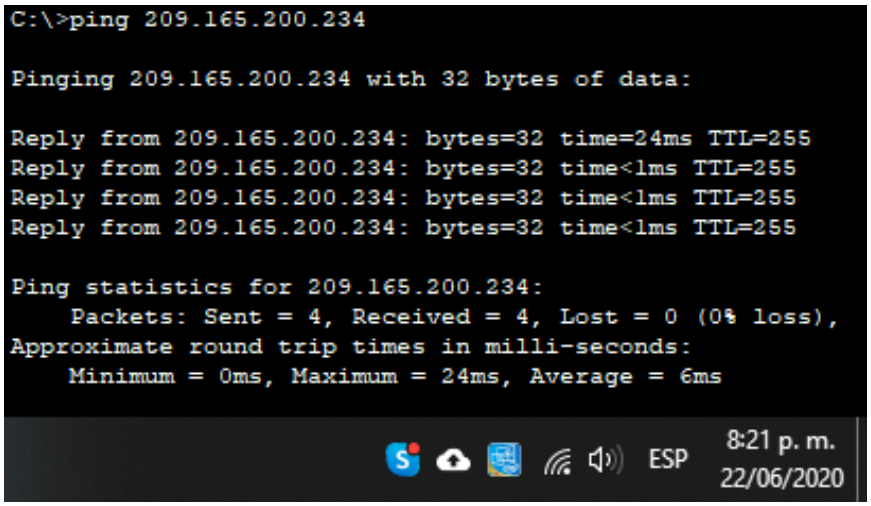


Ilustración 4 Validación en Internet pc

4.2 La configuración del S1 incluye las siguientes tareas

En la siguiente configuración en S1, se crean vlan para identificar áreas, a cada vlan se asigna su respectivo direccionamiento, así como puerta predeterminada y se configuran puertos de acceso, puertos utilizados y sin usar.

Tabla 9 Configuración Vlan S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config-vlan)# vlan 23 S1(config-vlan)# name Ingenieria S1(config-vlan)# vlan 99 S1(config-vlan)# name Administracion
Asignar la dirección IP de administración.	S1(config)# int vlan 21 S1(config)# Ip address 192.168.21.2 255.255.255.0 S1(config)# int vlan 23 S1(config)# Ip address 192.168.23.2 255.255.255.0 S1(config)# int vlan 99 S1(config)# Ip address 192.168.99.2 255.255.255.0 S1(config)# no shutdown
Asignar el gateway predeterminado	S1(config)# ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	S1(config)# int f0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1 S1(config-if)# exit
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)# int f0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)# int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if)# switch mode Access
Asignar F0/6 a la VLAN 21	S1(config-if)# interface f0/6 S1(config-if)# switchport mode access S1(config-if)# switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)# int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 S1(config)# shutdown

Fuente propia

4.2.1 Configurar el S3

La configuración del S3 incluye las siguientes tareas:

En la siguiente configuración en S3, se crean vlan para identificar áreas, a cada vlan se asigna su respectivo direccionamiento, así como puerta predeterminada y se configuran puertos de acceso, puertos utilizados y sin usar.

Tabla 10 Configuración Vlan S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)# vlan 21 S3(config-vlan)# name Contabilidad S3(config-vlan)# vlan 23 S3(config-vlan)# name Ingenieria S3(config-vlan)# vlan 99 S3(config-vlan)# name Administracion
Asignar la dirección IP de administración	S3(config)# int vlan 21 S3(config)# Ip address 192.168.21.2 255.255.255.0 S3(config)# int vlan 23 S3(config)# Ip address 192.168.23.2 255.255.255.0 S3(config)# int vlan 99 S3(config)# ip address 192.168.99.3 255.255.255.0 S3(config)# no shutdown

Asignar el gateway predeterminado.	S3(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config-if)# int f0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)# int range fa0/1-2, fa0/4-24, g0/1-2 S3(config-if)# switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if)# interface f0/18 S3(config-if)# switchport mode access S3(config-if)# switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)# interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config)# shutdown

Fuente propia

4.2.2 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se realiza configuración en R1, creando las subinterfaces de cada Vlan, esto para el enrutamiento de las mismas.

Tabla 11 Configuración subinterfaz R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)# int g0/1.21 R1(config-subif)# description contabilidad lan R1(config-subif)# encapsulation dot1q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# int g0/1.23 R1(config-subif)# description ingeniería lan R1(config-subif)# encapsulation dot1q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# int g0/1.99 R1(config-subif)# description administración lan R1(config-subif)# encapsulation dot1q 99 R1(config-subif)# ip address 192.168.99.4 255.255.255.0
Activar la interfaz G0/1	R1(config)# int g0/1 R1(config-if)# no shutdown

Fuente propia

4.2.3 Verificar la conectividad de la red

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

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

Se realiza verificación de conectividad entre dispositivo R1 y switch, dando como resultado envió de paquetes exitosos.

Tabla 12 Verificación conectividad switch y R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	Exitoso
S3	R1, dirección VLAN 99	192.168.99.2	Exitoso
S1	R1, dirección VLAN 21	192.168.21.2	Exitoso
S3	R1, dirección VLAN 23	192.168.23.2	Exitoso

Fuente propia

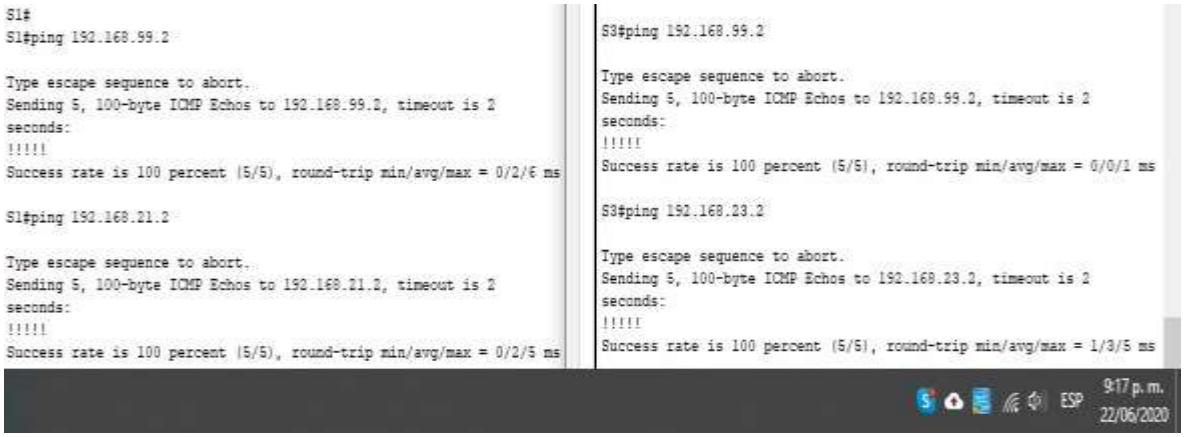


Ilustración 5 Verificación conectividad S1 y S3

4.3 Configurar el protocolo de routing dinámico RIPv2

Configurar RIPv2 en el R1
Las tareas de configuración para R1 incluyen las siguientes:

Se realiza configuración de Rip v2 en router, esto permitirá que router intercambie datos de redes que se encuentran conectados, con esto, el router calculara la ruta más corta para llegar a su destino, esto lo hace validando los saltos que genera.

Tabla 13 Configuración RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)# router rip R1(config)# version 2
Anunciar las redes conectadas directamente	R1(config-router)# netwok 192.16.1.0 0.0.0.3 area 0 R1(config-router)# netwok 192.168.21.0 0.0.0.3 area 0 R1(config-router)# netwok 192.168.23.0 0.0.0.3 area 0 R1(config-router)# netwok 192.168.21.0 0.0.0.255 area 0 R1(config-router)# netwok 192.168.23.0 0.0.0.255 area 0 R1(config-router)# netwok 192.168.99.0 0.0.0.255 area 0 R1(config-router)# exit R1(config)#int s0/0/0 R1(config-if)#ipv6 rip unad enable R1(config-if)#exit
Establecer todas las interfaces LAN como pasivas	R1(config-router)# Passive-interface default R1(config-router)# Passive-interface g0/1.21 R1(config-router)# Passive-interface g0/1.23 R1(config-router)# Passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)# no auto-summary R1(config-router)# end

Fuente propia

4.3.1 Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Se realiza configuración de Rip v2 en router, esto permitirá que router intercambie datos de redes que se encuentran conectados, con esto, el router calculara la ruta más corta para llegar a su destino, esto lo hace validando los saltos que genera.

Tabla 14 Configuración RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)# router rip R2(config)# version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# netwok 172.16.1.0 0.0.0.3 area 0 R2(config-router)# netwok 172.16.2.0 0.0.0.3 area 0 R2(config-router)# netwok 10.10.10.10 0.0.0.255 area 0 R2(config-router)# passive-interface loopback 0 R2(config-router)# exit R2(config)#int s0/0/0 R2(config-if)#ipv6 rip unad enable

	R2(config-if)#int s0/0/1 R2(config-if)#ipv6 rip unad enable R2(config-if)#int g0/0 R2(config-if)#ipv6 rip unad enable
Desactive la sumarización automática.	R2(config-router)# no auto-summary R2(config-router)# end

Fuente propia

4.3.2 Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Se realiza configuración de Rip v2 en router, esto permitirá que router intercambie datos de redes que se encuentran conectados, con esto, el router calculara la ruta más corta para llegar a su destino, esto lo hace validando los saltos que genera.

Tabla 15 Configuración RIPv2 en R3

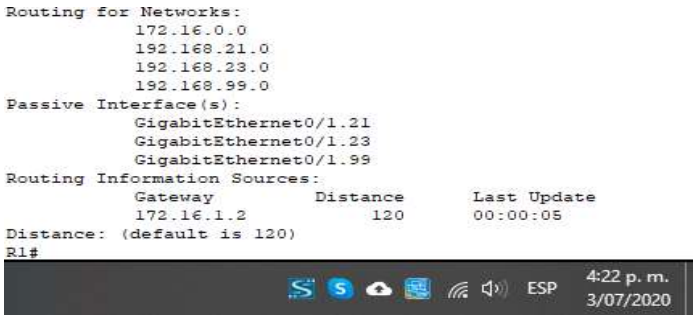
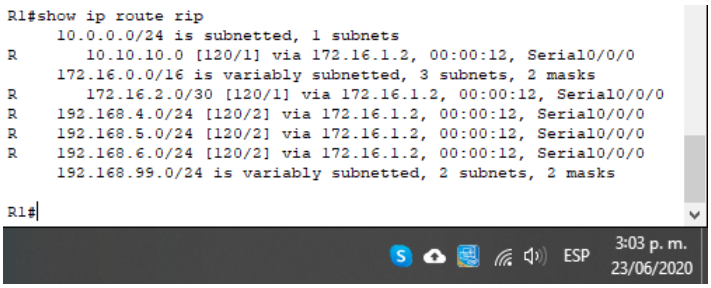
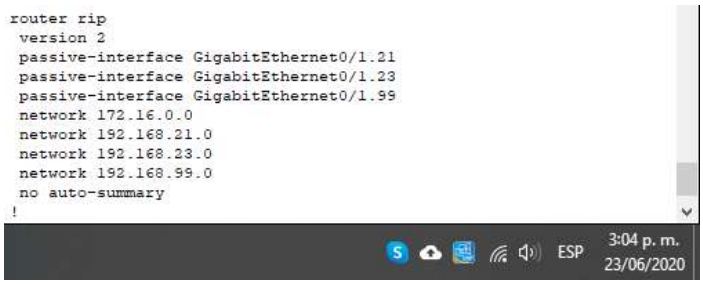
Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)# router rip R3(config)# version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)# netwok 172.16.2.0 0.0.0.3 area 0 R3(config-router)# exit R3(config)#int s0/0/1 R3(config-if)#ipv6 rip unad enable R3(config-if)#int lo7 R3(config-if)#ipv6 rip unad enable
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)# netwok 192.168.4.0 0.0.3.255 area 0 R3(config-router)# netwok 192.168.5.0 0.0.3.255 area 0 R3(config-router)# netwok 192.168.6.0 0.0.3.255 area 0 R3(config-router)# passive-interface lo4 R3(config-router)# passive-interface lo5 R3(config-router)# passive-interface lo6
Desactive la sumarización automática.	R3(config-router)# no auto-summary R3(config-router)# end

Fuente propia

4.3.3 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 Validación RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	 *Ilustración 6 Se ejecuta comando #show ip protocols*
¿Qué comando muestra solo las rutas RIP?	 *Ilustración 7 Se ejecuta comando #show ip route rip*
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	 *Ilustración 8 Se ejecuta comando Show run*

Fuente propia

4.4 Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

A continuación se crea un pool de dirección para cada vlan conectada, 21 y 23, a cada pool se proporcionará puerta de enlace, dns y dominio.

Tabla 17 Configuración DHCP en Vlan 21 y 23

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

Fuente propia

Con la configuración de nat estática, los dispositivos externos tengan acceso a dispositivos internos mediante ip publica configurada, mientras que nat dinámica la dirección interna se traduce a dirección externa 209.165.200.229.

4.4.1 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configuración NAT en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)# User webuser privilege 15 secret cisco12345 R2(config)# Nombre de usuario: webuser
Habilitar el servicio del servidor HTTP	No aplica código HTTP, router no soporta configuración

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit 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
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	R2(config)# no ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.252 R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	R2(config)# ip nat pool Internet 209.165.200.229 209.165.200.228 netmask 255.255.255.248

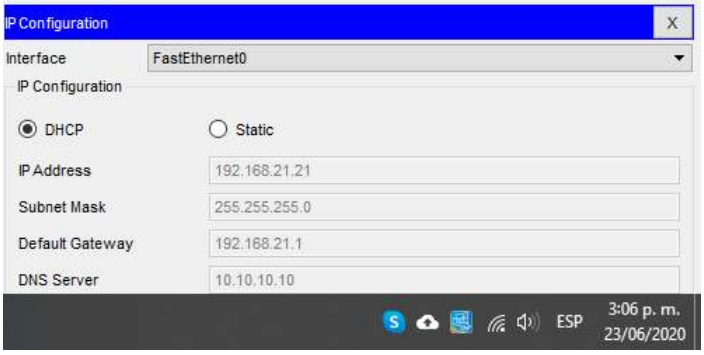
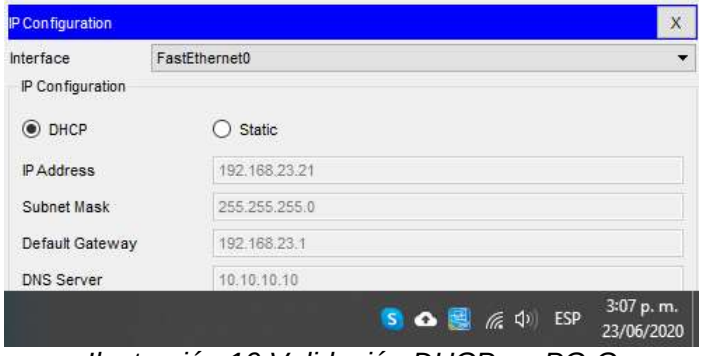
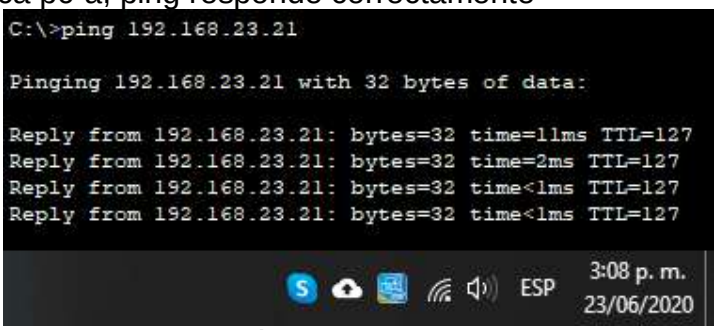
Fuente propia

4.4.2 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 NAT y DHCP

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Se realiza validación mediante símbolo del sistema del equipo, se asigna dirección por DHCP

	 *Ilustración 9 Validación DHCP en PC-A*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Se realiza validación mediante símbolo del sistema del equipo, se asigna dirección por DHCP  *Ilustración 10 Validación DHCP en PC-C*
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Se ejecuta comando ping 192.168.21.21 desde pc-ca pc-a, ping responde correctamente  *Ilustración 11 Ping PC-A y PC-C*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	El comando http server no funciono en R2, por lo tanto no puede ingresar al Router vía web, se adjunta en su lugar prueba de ping para verificar NAT funcional.

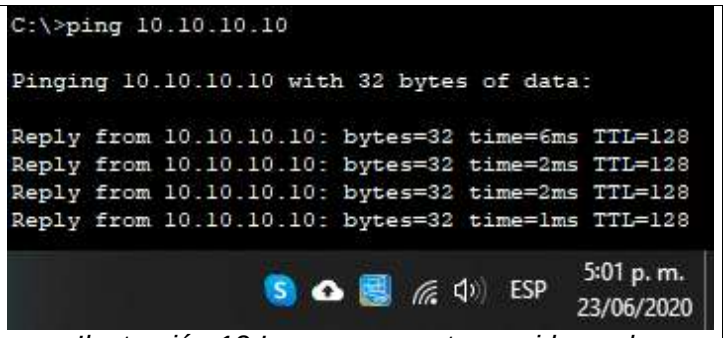


Ilustración 12 Ingreso correcto servidor web

Fuente propia

4.5 Configurar NTP

La configuración básica NTP, es un protocolo utilizado para la sincronización de relojes entre dispositivos, tal como se valida en tabla, R2 maneja un ntp maestro 5 y R1 es un cliente de R2, con esto, ntp mantiene una latencia.

Tabla 20 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 16:20:00 23 Jun 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Fuente propia

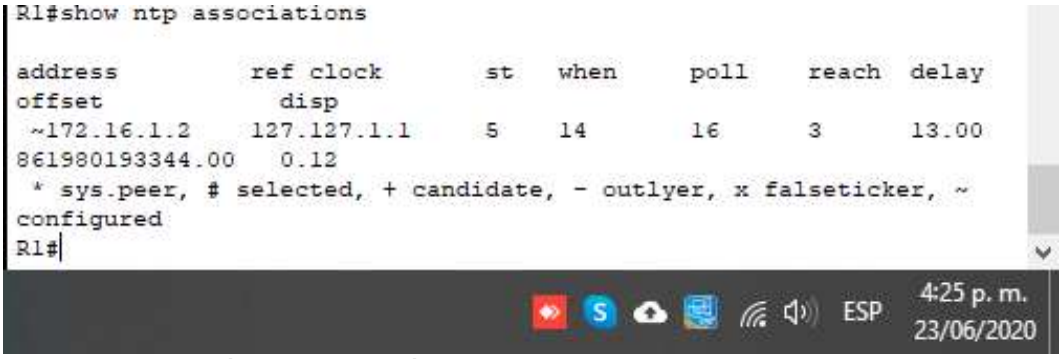


Ilustración 13 Validación NTP mediante #show ntp associations

4.6 Restringir el acceso a las líneas VTY en el R2

Se realiza configuración en R2, indicando técnica Vty que permitirá que el host pueda acceder remotamente a EXEC de R1

Tabla 21 Restricción de línea VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#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)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente propia

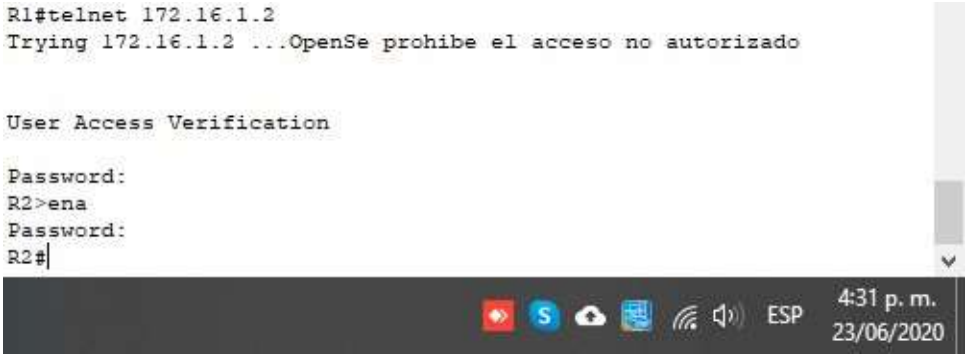


Ilustración 14 Validación ACL mediante Router R1

4.6.1 Introducir comando CLI adecuado que se necesita para mostrar lo siguiente

Tabla 22 Validación mediante comandos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Standard IP access list 1
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface buscar sh run
¿Con qué comando se muestran las traducciones NAT?	R2# show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations R2#show ip nat translations

Fuente propia

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.

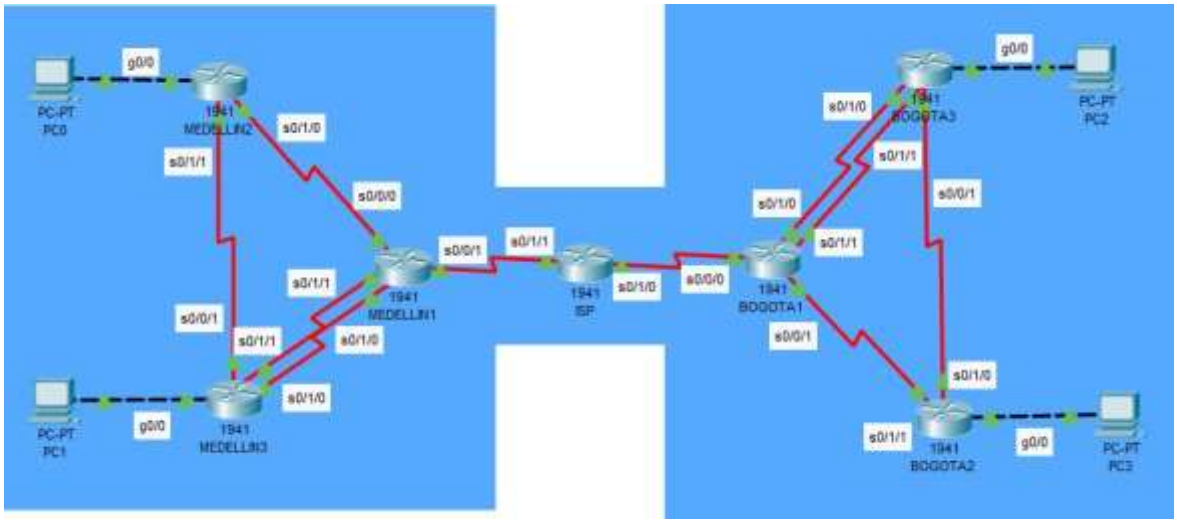


Ilustración 15 Topología escenario 2

A continuación se relaciona tabla de direccionamiento, la cual será utilizada en el escenario 2.

Tabla 23 Direccionamiento de red

DISPOSITIVO	PUERTO	DIRECCION IP	MASCARA	GATEWAY
ISP	s0/1/0	209.17.220.5	255.255.255.252	
ISP	s0/1/1	209.17.220.1	255.255.255.252	
MEDELLIN1	S0/0/1	209.17.220.2	255.255.255.252	
MEDELLIN1	S0/0/0	172.29.6.1	255.255.255.252	
MEDELLIN1	S0/1/1	172.29.6.9	255.255.255.252	
MEDELLIN1	S0/1/0	172.29.6.13	255.255.255.252	
MEDELLIN2	S0/1/0	172.29.6.2	255.255.255.252	
MEDELLIN2	S0/1/1	172.29.6.5	255.255.255.252	
MEDELLIN2	G0/0	172.29.4.1	255.255.255.128	
PC-0	FE	172.29.4.6	255.255.255.128	172.29.4.1
MEDELLIN3	S0/1/1	172.29.6.10	255.255.255.252	
MEDELLIN3	S0/1/0	172.29.6.14	255.255.255.252	

MEDELLIN3	S0/0/1	172.29.6.6	255.255.255.252	
MEDELLIN3	G0/0	172.29.4.129	255.255.255.128	
PC-1	FE	172.29.4.134	255.255.255.128	172.29.4.129
BOGOTA1	S0/0/0	209.17.220.6	255.255.255.252	
BOGOTA1	S0/1/0	172.29.3.1	255.255.255.252	
BOGOTA1	S0/1/1	172.29.3.5	255.255.255.252	
BOGOTA1	S0/0/1	172.29.3.9	255.255.255.252	
BOGOTA2	S0/1/1	172.29.3.10	255.255.255.252	
BOGOTA2	S0/1/0	172.29.3.13	255.255.255.252	
BOGOTA2	G0/0	172.29.1.1	255.255.255.0	
PC-3	FE	172.29.1.6	255.255.255.0	172.29.1.1
BOGOTA3	S0/1/0	172.29.3.2	255.255.255.252	
BOGOTA3	S0/1/1	172.29.3.6	255.255.255.252	
BOGOTA3	S0/0/1	172.29.3.14	255.255.255.252	
BOGOTA3	G0/0	172.29.0.1	255.255.255.0	
PC-2	FE	172.29.0.6	255.255.255.0	172.29.0.1

Fuente propia

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.

Se realiza configuración de routers de Bogota, Medellín y ISP en el cual se le asignan nombre, claves de seguridad, mensaje Motd, Nvram, etc.

Tabla 24 Configuración routers Medellín, Bogotá y ISP

Elemento o tarea de configuración	Especificación
Contraseña de exec privilegiado cifrada	Router(config)# enable secret class
Contraseña de acceso a la consola	Router(config)# line con 0 Router(config)# password cisco Router(config-line)#login
Contraseña de acceso Telnet	Router(config)# line vty 0 15 Router(config)# password cisco Router(config-line)#login
Cifrar las contraseñas de texto no cifrado	Router(config)# service password-encryption

Mensaje MOTD	Router(config)# banner motd #Solo personal autorizado#
Almacenar configuración en NVRAM	Router(config)# #copy running-config startup-config

Fuente propia

5.1 Configuración del enrutamiento

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

Se realiza configuración en router ISP, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso ISP enrutara por los puertos s0/1/1 y s0/1/0

Tabla 25 Configuración direcciones Ip y Ospf en router ISP

Elemento o tarea de configuración	Especificación
Interface serial 0/1/1	ISP(config)#int s0/1/1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#clock rate 4000000 ISP(config-if)#no shutdown
Interface serial 0/1/0	ISP(config-if)#int s0/1/0 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 4000000 ISP(config-if)#no shutdown

Fuente propia

Se realiza configuración en router MEDELLIN1, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso MEDELLIN1 enrutara por los puertos s0/0/0, s0/0/1, s0/1/1 y s0/1/1

Tabla 26 Configuración direcciones Ip y Ospf en router MEDELLIN1

Elemento o tarea de configuración	Especificación
Interface serial 0/0/1	MEDELLIN1(config)#int s0/0/1 MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN1(config-if)#no shutdown
Interface serial 0/0/0	MEDELLIN1(config-if)#int s0/0/0 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN1(config-if)#clock rate 4000000 MEDELLIN1(config-if)#no shutdown

Interface serial 0/1/1	MEDELLIN1(config-if)#int s0/1/1 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 4000000 MEDELLIN1(config-if)#no shutdown
Interface serial 0/1/0	MEDELLIN1(config-if)#int s0/1/0 MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)#clock rate 4000000 MEDELLIN1(config-if)#no shutdown
Ospfv2	MEDELLIN1(config)#router ospf 10 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)#passive-interface s0/0/1

Fuente propia

Se realiza configuración en router MEDELLIN2, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso MEDELLIN2 enrutara por los puertos s0/1/0, s0/1/1 y G0/0

Tabla 27 Configuración direcciones Ip y Ospf en router MEDELLIN2

Elemento o tarea de configuración	Especificación
Interface serial 0/1/1	MEDELLIN2(config)#int s0/1/1 MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN2(config-if)#clock rate 4000000 MEDELLIN2(config-if)#no shutdown
Interface serial 0/1/0	MEDELLIN2(config-if)#int s0/1/0 MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN2(config-if)#no shutdown
Interface G0/0	MEDELLIN2(config-if)#int G0/0 MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN2(config-if)#no shutdown
Ospfv2	MEDELLIN2(config)#router ospf 10 MEDELLIN2(config-router)#router-id 2.2.2.2 MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 0 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)#passive-interface g0/0

Fuente propia

Se realiza configuración en router MEDELLIN3, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso MEDELLIN3 enrutara por los puertos s0/1/0, s0/1/1, s0/0/1 y G0/0.

Tabla 28 Configuración direcciones Ip y Ospf en router MEDELLIN3

Elemento o tarea de configuración	Especificación
Interface serial 0/1/1	MEDELLIN3(config)#int s0/1/1 MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN3(config-if)#no shutdown
Interface serial 0/1/0	MEDELLIN3(config-if)#int s0/1/0 MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN3(config-if)#no shutdown
Interface serial 0/0/1	MEDELLIN3(config-if)#int s0/0/1 MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN3(config-if)#no shutdown
Interface G0/0	MEDELLIN3(config-if)#int G0/0 MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN3(config-if)#no shutdown
Ospfv2	MEDELLIN3(config)#router ospf 10 MEDELLIN3(config-router)#router-id 3.3.3.3 MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 0 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 172.29.6.8 0.0.0.3 area 0 MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN3(config-router)#passive-interface g0/0

Fuente propia

Se realiza configuración en router BOGOTA1, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso BOGOTA1 enrutara por los puertos s0/0/0, s0/1/0, s0/1/1 y s0/0/1.

Tabla 29 Configuración direcciones Ip y Ospf en router BOGOTA1

Elemento o tarea de configuración	Especificación
Interface serial 0/0/0	BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shutdown
Interface serial 0/1/0	BOGOTA1(config-if)#int s0/1/0 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252

	BOGOTA1(config-if)# clock rate 4000000 BOGOTA1(config-if)#no shutdown
Interface serial 0/1/1	BOGOTA1(config-if)#int s0/1/1 BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)# clock rate 4000000 BOGOTA1(config-if)#no shutdown
Interface serial 0/0/1	BOGOTA1(config-if)#int s0/0/1 BOGOTA1(config-if)#ip address 172.29.3.3 255.255.255.252 BOGOTA1(config-if)# clock rate 4000000 BOGOTA1(config-if)#no shutdown
Ospfv2	BOGOTA1(config)#router ospf 10 BOGOTA1(config-router)#router-id 4.4.4.4 BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA1(config-router)#passive-interface s0/0/0

Fuente propia

Se realiza configuración en router BOGOTA2, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso BOGOTA2 enrutara por los puertos s0/1/0, s0/1/1 y g0/0.

Tabla 30 Configuración direcciones Ip y Ospf en router BOGOTA2

Elemento o tarea de configuración	Especificación
Interface serial 0/1/1	BOGOTA2(config)#int s0/1/1 BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA2(config-if)#no shutdown
Interface serial 0/1/0	BOGOTA2(config-if)#int s0/1/0 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)# clock rate 4000000 BOGOTA2(config-if)#no shutdown
Interface G0/0	BOGOTA2(config-if)#int G0/0 BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA2(config-if)#no shutdown
Ospfv2	BOGOTA2(config)#router ospf 10 BOGOTA2(config-router)#router-id 5.5.5.5 BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 0 BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA2(config-router)#passive-interface g0/0

Fuente propia

Se realiza configuración en router BOGOTA3, asignando protocolo OSPF, el cual tiene como función calcular la ruta más corta entre dos nodos, en este caso BOGOTA3 enrutara por los puertos s0/0/1, s0/1/0, s0/1/1 y G0/0.

Tabla 31 Configuración direcciones Ip y Ospf en router BOGOTA3

Elemento o tarea de configuración	Especificación
Interface serial 0/0/1	BOGOTA3(config)#int s0/0/1 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shutdown
Interface serial 0/1/1	BOGOTA3(config-if)#int s0/1/1 BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA3(config-if)#no shutdown
Interface serial 0/1/0	BOGOTA3(config-if)#int s0/1/0 BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA3(config-if)#no shutdown
Interface G0/0	BOGOTA3(config-if)#int G0/0 BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA3(config-if)#no shutdown
Ospfv2	BOGOTA3(config)#router ospf 10 BOGOTA3(config-router)#router-id 6.6.6.6 BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 0 BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA3(config-router)#passive-interface g0/0

Fuente propia

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

Se realiza configuración en router BOGOTA1 y MEDELLIN1, en el cual se asigna ruta predeterminada para que estos se puedan ver por OSPF

Tabla 32 Configuración ruta por defecto router BOGOTA1 y MEDELLIN1

Elemento o tarea de configuración	Especificación
Ruta defecto MEDELLIN1	MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)#router ospf 10

	MEDELLIN1(config-router)#default-information originate
Ruta defecto BOGOTA1	BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 BOGOTA1(config)#router ospf 10 BOGOTA1(config-router)#default-information originate

Fuente propia

Con esta configuración se verifica que los router conocen una ruta por el cual se pueden ver y tener conexión a internet.

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

Sumarizacion Bogota

172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	172.29.4.0/25
172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	172.29.4.128/25
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	172.29.6.0/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	172.29.6.4/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	172.29.6.8/30172
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	172.29.6.12/30
172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	**172.29.4.0/22**

Sumarizacion Medellin

172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	172.29.0.0/24
172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	172.29.1.0/24
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	172.29.3.0/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	172.29.3.4/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	172.29.3.8/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	172.29.3.12/30
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**172.29.0.0/22**

Con la anterior tabla, es posible configurar el ISP con las direcciones 172.29.4.0 255.255.252.0 en router Medellin y Bogota

Tabla 33 Configuración rutas estáticas en ISP

Elemento o tarea de configuración	Especificación
IP estáticas	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

Fuente propia

5.2 Tabla del enrutamiento

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

Para verificar el enrutamiento se utiliza el comando #show ip route, esto se realiza en cada router configurado.

```
     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
     209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/1
L       209.17.220.1/32 is directly connected, Serial0/1/1
C       209.17.220.2/32 is directly connected, Serial0/1/1
C       209.17.220.4/30 is directly connected, Serial0/1/0
L       209.17.220.5/32 is directly connected, Serial0/1/0
C       209.17.220.6/32 is directly connected, Serial0/1/0
```

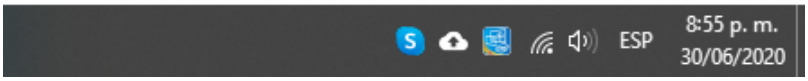


Ilustración 16 enrutamiento router ISP

```
Gateway of last resort is 209.17.220.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 00:50:20, Serial0/0/0
O       172.29.4.128/25 [110/65] via 172.29.6.10, 00:50:20, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.1/32 is directly connected, Serial0/0/0
O       172.29.6.4/30 [110/128] via 172.29.6.2, 00:50:20, Serial0/0/0
                      [110/128] via 172.29.6.10, 00:50:20, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/1/1
L       172.29.6.9/32 is directly connected, Serial0/1/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.13/32 is directly connected, Serial0/1/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/1
C       209.17.220.1/32 is directly connected, Serial0/0/1
L       209.17.220.2/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.17.220.1
```

Ilustración 17 enrutamiento router MEDELLIN1

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 00:54:21, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/1/0
L       172.29.6.2/32 is directly connected, Serial0/1/0
C       172.29.6.4/30 is directly connected, Serial0/1/1
L       172.29.6.5/32 is directly connected, Serial0/1/1
O       172.29.6.8/30 [110/128] via 172.29.6.6, 00:54:21, Serial0/1/1
                      [110/128] via 172.29.6.1, 00:54:21, Serial0/1/0
O       172.29.6.12/30 [110/128] via 172.29.6.6, 00:54:21, Serial0/1/1
                       [110/128] via 172.29.6.1, 00:54:21, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:54:21, Serial0/1/0
```

Ilustración 18 enrutamiento router MEDELLIN2

```
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.5, 00:57:40, Serial0/0/1
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.13, 00:57:40, Serial0/1/0
                      [110/128] via 172.29.6.5, 00:57:40, Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.6/32 is directly connected, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/1/1
L       172.29.6.10/32 is directly connected, Serial0/1/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.14/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:57:50, Serial0/1/0
```

Ilustración 19 enrutamiento router MEDELLIN3

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.6, 00:59:58, Serial0/1/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:59:58, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.9/32 is directly connected, Serial0/0/1
O       172.29.3.12/30 [110/128] via 172.29.3.6, 00:59:58, Serial0/1/1
                       [110/128] via 172.29.3.10, 00:59:58, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
C       209.17.220.5/32 is directly connected, Serial0/0/0
L       209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.5
```

Ilustración 20 enrutamiento router BOGOTA1

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.14, 01:02:04, Serial0/1/0
C       172.29.1.0/24 is directly connected, GigabitEthernet0/0
L       172.29.1.1/32 is directly connected, GigabitEthernet0/0
O       172.29.3.0/30 [110/128] via 172.29.3.14, 01:02:04, Serial0/1/0
                      [110/128] via 172.29.3.9, 01:02:04, Serial0/1/1
O       172.29.3.4/30 [110/128] via 172.29.3.14, 01:02:04, Serial0/1/0
                      [110/128] via 172.29.3.9, 01:02:04, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/1/1
L       172.29.3.10/32 is directly connected, Serial0/1/1
C       172.29.3.12/30 is directly connected, Serial0/1/0
L       172.29.3.13/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 01:02:14, Serial0/1/1
```

Ilustración 21 enrutamiento router BOGOTA2

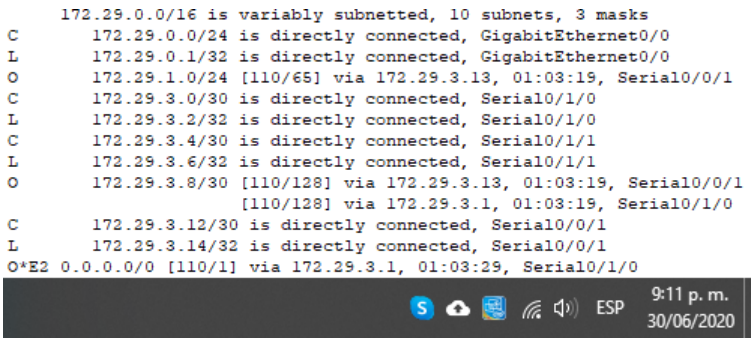


Ilustración 22 enrutamiento router BOGOTA3

5.3 Deshabilitar la propagación del protocolo OSPF.

5.3.1 Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF.

En la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 34 Interfaces router

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

Fuente propia

5.4 Verificación del protocolo OSPF.

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

Para verificar la base de datos OSPF se utiliza el comando #show ip route, este comando se ejecuta en cada router configurado.

```
Gateway of last resort is 209.17.220.1 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.2, 01:36:39, Serial0/0/0
O       172.29.4.128/25 [110/65] via 172.29.6.10, 01:36:39, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.1/32 is directly connected, Serial0/0/0
O       172.29.6.4/30 [110/128] via 172.29.6.2, 01:36:39, Serial0/0/0
                      [110/128] via 172.29.6.10, 01:36:39, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/1/1
L       172.29.6.9/32 is directly connected, Serial0/1/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.13/32 is directly connected, Serial0/1/0
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/1
C       209.17.220.1/32 is directly connected, Serial0/0/1
L       209.17.220.2/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.17.220.1
```

Ilustración 23 enrutamiento ospf MEDELLIN1

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 01:38:49, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/1/0
L       172.29.6.2/32 is directly connected, Serial0/1/0
C       172.29.6.4/30 is directly connected, Serial0/1/1
L       172.29.6.5/32 is directly connected, Serial0/1/1
O       172.29.6.8/30 [110/128] via 172.29.6.6, 01:38:49, Serial0/1/1
                      [110/128] via 172.29.6.1, 01:38:49, Serial0/1/0
O       172.29.6.12/30 [110/128] via 172.29.6.6, 01:38:49, Serial0/1/1
                       [110/128] via 172.29.6.1, 01:38:49, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 01:38:49, Serial0/1/0
```

Ilustración 24 enrutamiento ospf MEDELLIN2

```
     172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.5, 01:34:13, Serial0/0/1
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.13, 01:34:13, Serial0/1/0
                      [110/128] via 172.29.6.5, 01:34:13, Serial0/0/1
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.6/32 is directly connected, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/1/1
L       172.29.6.10/32 is directly connected, Serial0/1/1
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.14/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 01:34:23, Serial0/1/0
```

Ilustración 25 enrutamiento ospf MEDELLIN3

```
     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.0.0/24 [110/65] via 172.29.3.6, 01:41:40, Serial0/1/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 01:41:40, Serial0/0/1
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.9/32 is directly connected, Serial0/0/1
O       172.29.3.12/30 [110/128] via 172.29.3.6, 01:41:40, Serial0/1/1
                       [110/128] via 172.29.3.10, 01:41:40, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
C       209.17.220.5/32 is directly connected, Serial0/0/0
L       209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.5
```

Ilustración 26 enrutamiento ospf BOGOTA1

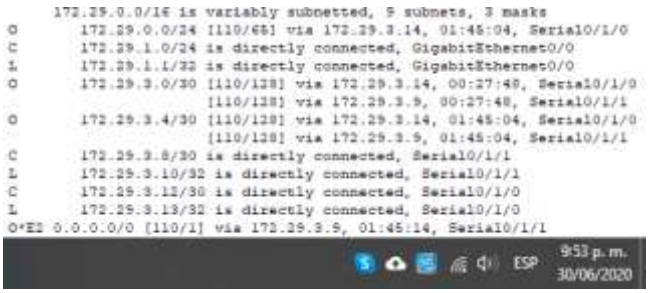


Ilustración 27 enrutamiento ospf BOGOTA2

Ilustración 28 enrutamiento ospf BOGOTA3

Los routers BOGOTA1 y MEDELLIN1 presentan similitud en cuanto a conexiones internas.

5.5 Configurar encapsulamiento y autenticación PPP.

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

Se procede a configurar la autenticación PAP entre ISP y MEDELLIN1, esto permite validar que el usuario permita demostrar su identidad para conexión.

Tabla 35 Autenticación PPP routers ISP, MEDELLIN1

Elemento o tarea de configuración	Especificación
PPP ISP	ISP(config)#username Medellin1 password cisco ISP(config)#in s0/1/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco
PPP MEDELLIN1	MEDELLIN1(config)#username ISP password cisco MEDELLIN1(config)#int s0/0/1 MEDELLIN1(config-if)#encapsulation ppp MEDELLIN1(config-if)#ppp authentication pap

	MEDELLIN1(config-if)#ppp pap sent-username Medellin1 password cisco

Fuente propia

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

Posterior a la configuración de PAP en router MEDELLIN1, se procede a configurar CHAP en router BOGOTA1, la configuración de CHAP permite validar periódicamente la identificación de clientes remotos.

Tabla 36 Autenticación CHAP routers ISP, BOGOTA1

Elemento o tarea de configuración	Especificación
CHAP ISP	ISP(config)#username Bogota1 password cisco ISP(config)#int s0/1/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap
CHAP BOGOTA1	BOGOTA1(config)#username ISP password cisco BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#encapsulation ppp BOGOTA1(config-if)#ppp authentication chap

Fuente propia

5.6 Configuración de PAT.

5.6.1 En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1),

Los routers internos de un nodo no podrán llegar hasta los routers internos al otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

Se realiza configuración PAT en router BOGOTA1 y MEDELLIN1, en el cual al enviar paquetes de un extremo a otro, este lo envía bajo un direccionamiento y PAT hace la traducción de direcciones, haciendo que llegue otra dirección.

Tabla 37 Autenticación PAT routers MEDELLIN1, BOGOTA1

Elemento o tarea de configuración	Especificación
PAT MEDELLIN1	MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/1 overload MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255 MEDELLIN1(config)#int s0/0/1 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#int s0/0/0 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#int s0/1/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#int s0/1/0 MEDELLIN1(config-if)#ip nat inside
PAT BOGOTA1	BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255 BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#int s0/1/0 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#int s0/0/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#int s0/1/1 BOGOTA1(config-if)#ip nat inside

Fuente propia

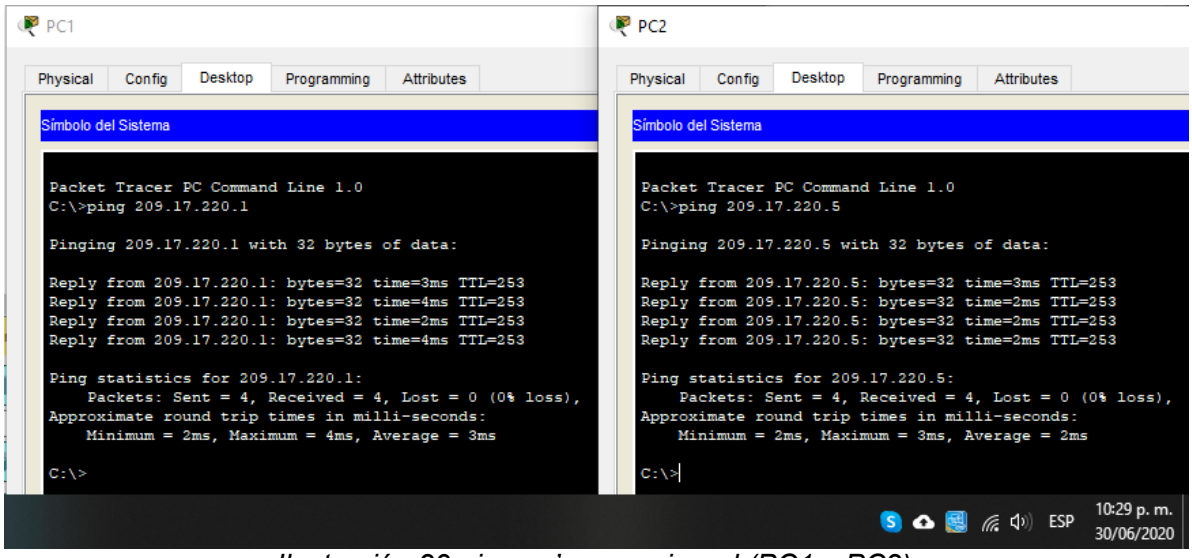


Ilustración 29 ping pc's a propia red (PC1 y PC2)

Al hacer un ping PC1 a Bogota y PC2 a Medellin, el ping no responde porque es la función de PAT. Si se desea que el pin responda, es necesario desactivar NAT.

5.6.2 Proceda a configurar el NAT en el router Bogotá1 y 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 serial 0/1/0 del router Bogotá1 y Medellín, cómo diferente puerto.

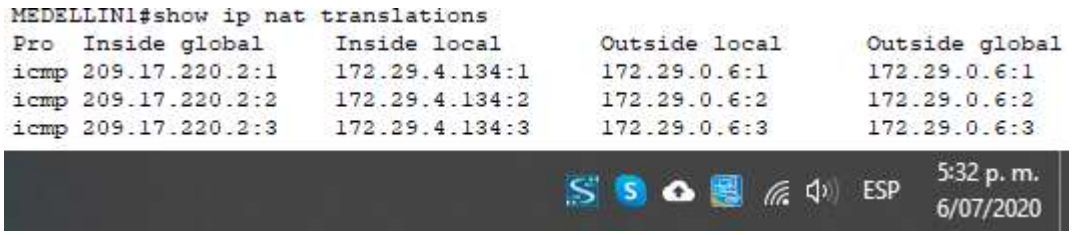


Ilustración 30 Validación Nat en Medellin1

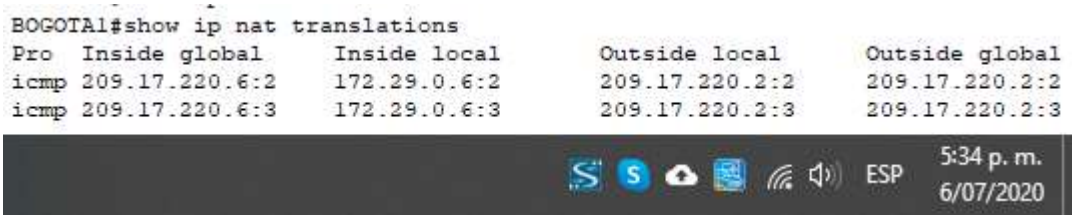


Ilustración 31 Validación Nat en Bogota1

Se puede validar en las Ilustraciones 30 y 31 que Nat funciona correctamente, haciendo que las direcciones sean traducidas en el direccionamiento.

5.7 Configuración del servicio DHCP.

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

Se realiza configuración en routers de cada extremo para que tengan DCHP excluido, asignando pool de direcciones para que terminales queden con acceso.

Tabla 38 Creación grupo extensiones excluidas router MEDELLIN2 y MEDELLIN3

Elemento o tarea de configuración	Especificación
DHCP excluido	MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133

POOL DISPONIBLE	MEDELLIN2(config)#ip dhcp pool Med2 MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.1 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp pool Med3 MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.129 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit

Fuente propia

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

Con la configuración del broadcast, el equipo terminal tiene conexión por DHCP.

Tabla 39 Configuración broadcast hacia MEDELLIN2

Elemento o tarea de configuración	Especificación
Broadcast	MEDELLIN3(config)#int g0/0 MEDELLIN3(config-if)#ip helper-address 172.29.6.5

Fuente propia

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

Se realiza configuración en routers de cada extremo para que tengan DCHP excluido, asignando pool de direcciones para que terminales queden con acceso.

Tabla 40 Creación grupo extensiones excluidas router BOGOTA2 y BOGOTA3

Elemento o tarea de configuración	Especificación
DHCP excluido	BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
POOL DISPONIBLE	BOGOTA2(config)#ip dhcp pool Bog2 BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.1.1 BOGOTA2(dhcp-config)#dns-server 8.8.8.8 BOGOTA2(dhcp-config)#ip dhcp pool Bog3

	BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.0.1 BOGOTA2(dhcp-config)#dns-server 8.8.8.8

Fuente propia

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

Con la configuración del broadcast, el equipo terminal tiene conexión por DHCP.

Tabla 41 Configuración broadcast hacia MEDELLIN2

Elemento o tarea de configuración	Especificación
Broadcast	BOGOTA3(config)#int g0/0 BOGOTA3(config-if)#ip helper-address 172.29.3.13

Fuente propia

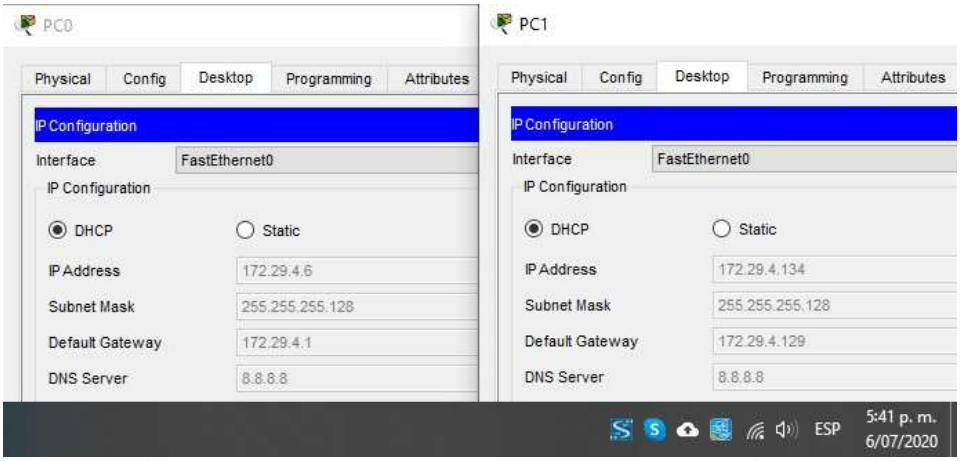


Ilustración 32 Se valida DHCP en terminales de Medellín, DHCP ok.

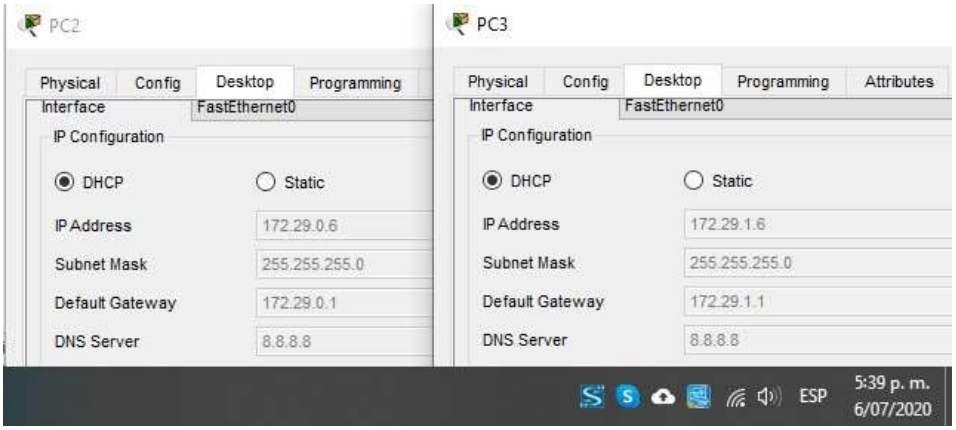


Ilustración 33 Se valida DHCP en terminales de Bogotá, DHCP ok.

ENLACE DE DESCARGA ARCHIVOS PKT.

Anexo enlace drive en el cual se encuentran alojados los dos escenarios solicitados en el trabajo final, este enlace pertenece a la herramienta Google Drive y es compartido a todo el que contenga el enlace.

Link de acceso:

https://drive.google.com/drive/folders/1gGa2Qvr5ArBux9J4kCDe1ejmyqKxegaE?usp=sharing

CONCLUSIONES

Se establece configuración efectiva en switch, routers y computadores presentados para el actual escenario, todo esto se dio gracias a las clases brindadas por cisco, en el cual fue de importante apoyo los laboratorios presentados.

Con la configuración realizada del DHCP en los router, fue posible ahorrar tiempos debido a que los equipos detectan automáticamente los rangos de direccionamiento.

Cisco packet tracer es una herramienta que permite crear redes tal cual como si se realizara físicamente, gracias a este aplicativo se pudo realizar el escenario predefinido.

Posterior a la configuración en la red, se ejecutaron comandos de verificación de las conexiones realizadas entre dispositivos, dando así alcance a los objetivos previstos.

En cada laboratorio desarrollado del diplomado CCNA, fue importante enfatizar el acceso a los router mediante usuarios y contraseñas.

Con la configuración del protocolo de red OSPF, los routers Medellin2, Medellin3, Bogorta2 y Bogota3 del escenario 2 tienen un encaminamiento jerárquico de pasarela interior, lo que permite que la red tome el camino mas corte para llegar a sus diferentes destinos.

De acuerdo a las respectivas configuraciones NAT realizadas en los routers, fue posible conservar direcciones ip y que estas se conecten a internet.

BIBLIOGRAFÍA

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

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

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

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

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

Perez, A., (2013). Redes empresariales: Todo lo que necesita saber. https://searchdatacenter.techtarget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias

CISCO. (10 de agosto de 2005). Guía de diseño de OSPF. https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Ortega, A., (2020). Direcciones de red (NAT). https://forum.huawei.com/enterprise/es/direcciones-de-red-nat-miuconhuawei/thread/628145-100235

Wikipedia. (30 de mayo de 2020). Routing Information Protocol. https://es.wikipedia.org/wiki/Routing_Information_Protocol#:~:text=El%20Protocolo%20de%20Informaci%C3%B3n%20de,las%20que%20se%20encuentran%20conectados

Networkworld. (10 SEP 2018). Qué es DHCP y cómo funciona. https://www.networkworld.es/telecomunicaciones/que-es-dhcp-y-como-funciona#:~:text=Definici%C3%B3n%20de%20DHCP,eficiente%20con%20otros%20puntos%20finales.

Wikipedia. (10 de junio de 2020). VLAN. https://es.wikipedia.org/wiki/VLAN#:~:text=Una%20VLAN%2C%20acr%C3%B3nimo%20de%20virtual,en%20una%20%C3%BAnica%20red%20f%C3%ADsica.

Walton, A. (s,f). SLAAC y DHCPv6: Introducción y Funcionamiento. https://ccnadesdecero.es/slaac-dhcpv6-funcionamiento/