DESARROLLO DE LA PRUEBA DE HABILIDADES PRÁCTICAS CCNA APLICANDO EL SOFTWARE CISCO PACKET TRACER

ALEXANDER ELÍAS CHINCHILLA SEPÚLVEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
OCAÑA
2020

DESARROLLO DE LA PRUEBA DE HABILIDADES PRÁCTICAS CCNA APLICANDO EL SOFTWARE CISCO PACKET TRACER

ALEXANDER ELÍAS CHINCHILLA SEPÚLVEDA

Trabajo de grado presentado para optar al título de
INGENIERO DE SISTEMAS

Magister en Seguridad Informática
GUSTAVO ADOLFO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
OCAÑA
2020

NOTA DE ACEPTACIÓN

Firma del presidente de jurado

Firma del jurado

Firma del jurado

Ocaña, 21 de julio de 2020

DEDICATORIA

El presente trabajo de grado lo dedico principalmente a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de cumplir mi más anhelado sueño.

A mi Padre Rafael (en la gloria de Dios) y Madre Celina, por su amor, trabajo y sacrificio en todos mis años de vida, gracias a ellos, he logrado llegar hasta aquí y superarme en lo profesional. Ha sido un verdadero orgullo y privilegio ser su hijo, son los mejores Padres.

A mi hermana Hilda por estar siempre presente, acompañándome, apoyándome y dándome la mano incondicionalmente, gracias por brindarme tu amistad y ayuda en ésta, tan importante etapa de mi vida.

A mi amada esposa Heidy, a mis maravillosos hijos y a mis queridos hermanos.

Gracias a todos, Dios los bendiga.

AGRADECIMIENTOS

Quiero agradecer a la UNAD por esta gran oportunidad de convertirme en un profesional en el área de Ingeniería de sistemas y poder seguir creciendo en mi vida profesional.

Al Rector y administrativos del CEAD de Ocaña, siempre tan pendientes y diligentes con mi proceso académico, a todos los directores y tutores que me apoyaron en mis cursos.

En este diplomado, al tutor Gustavo Adolfo Rodríguez, gracias por sus apreciaciones y valiosas indicaciones, a mis compañeros que conocí en las diferentes regiones del país, un abrazo fraternal para todos.

Dios los bendiga.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL: (Access control list): Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición.

CHAP: (Challenge Handshake Authentication Protocol): Es un protocolo de autenticación por desafío y fue definido en la RFC 1994. Es un método de autenticación remota o inalámbrica.

DHCP: (Dynamic Host Configuration Protocol), protocolo de configuración de host dinámico de red, se utiliza en redes IP donde el dispositivo servidor DHCP fija automáticamente una dirección IP y otros valores de red, a cada host en la red para que la comunicación fluya de manera eficiente con otros puntos finales.

NAT: (Network Address Translation), especifica la traducción de direcciones entre dos redes que, por casi siempre, se efectúa en el ámbito del router. Su finalidad es enlazar redes locales con Internet y así establecer una diferencia entre dos clases de traducción de redes diferentes: Source NAT (SNAT) y Destination NAT (DNAT).

NETWORKING: En el entorno de telecomunicaciones, es un tipo red que permite a los dispositivos que pertenecen a ella, intercambiar datos. En las redes de cómputo, se pasa la información entre sí a lo largo de las conexiones de datos. Las conexiones entre los nodos se establecen a partir de los medios de comunicación, ya sea por cable o medios inalámbricos.

OSPF: (Open Shortest Path First), Abrir primero el camino más corto, es un Internal Gateway Protocol (IGP) para direccionar jerárquicamente y calcular la ruta más corta entre dos nodos.

PAT: (Port Address Translation): Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a ~64000 direcciones internas.

PPP: (Point-to-Point Protocol): Es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

RIP: (Routing Information Protocol) es un protocolo usado por algunos routers para recibir y enviar información, su finalidad es conocer por donde deberían enrutarse un paquete para lograr que éste llegue a su destino.

SLAAC: (Stateless Address Autoconfiguration), configuración automática de dirección independiente del estado, es una técnica por la cual un dispositivo de red obtiene una dirección IPv6 de unidifusión global, sin necesidad de los servicios de un servidor de DHCPv6.

VLAN: (Virtual Local Area Network), Es una técnica para establecer redes lógicas independientes dentro de una misma red física. Diferentes redes VLAN pueden existir en un solo conmutador físico o en una sola red física.

RESUMEN

La UNAD, bajo su modalidad virtual y su proceso de aprendizaje del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), se presenta como estrategia el uso del software para simular con Cisco Packet Tracer, donde podemos comprobar, virtualmente, cómo trabajan estas redes y podemos ver las diferentes clases de topología para llevar a la realidad al campo laboral cuando se nos presente en la necesidad en el entorno productivo.

En el desarrollo de los módulos CCNA1 (CCNA R&S: Introduction to Networks) y CCNA2 (CCNA R&S: Routing and Switching Essentials), se obtiene las bases teóricas y prácticas de laboratorio para el aprendizaje de la tecnología. Con los conocimientos obtenidos y puestos en práctica se busca lograr el desarrollo de la actividad final como prueba de habilidades, donde mediante los escenarios propuestos, se pone en práctica los conocimientos previamente aprendidos, realizando configuraciones como: IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2 y OSPF, 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, encapsulamiento PPP y su autenticación.

Durante la realización de las configuraciones, se probará y registrará la red mediante el uso de comandos en la Interfaz de línea de comandos (CLI) y algunos ajustes usando la interfaz gráfica de los dispositivos.

Palabras claves: Packet Tracer, Interfaz, Conectividad, tecnología CISCO.

INTRODUCCIÓN

El presente trabajo busca identificar en el estudiante, futuro profesional en sistemas, el grado de competencias y habilidades adquiridas en el Diplomado de profundización CCNA, esta práctica aportará valiosos conocimientos que mejorarán su desempeño y así ser capaz de dar solución a situaciones, en donde lo relevante es poner a prueba los niveles de comprensión y recursividad en alternativas que logren solventar problemas relacionados con aspectos de Networking.

Para esta actividad se debe solucionar e implementar dos escenarios con topologías de red propuestas, acompañado del respectivo proceso en documentación paso a paso, su correspondiente evidencia y registro de configuración requerida para cada dispositivo de la red. La verificación de conectividad y funcionamiento se llevará a cabo mediante el uso de comandos de consola como ping, traceroute, show ip route, entre otros.

Para realizar el montaje, adecuación e implementación de la red se usará el programa Packet Tracer de la empresa Cisco, es un simulador de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver los posibles inconvenientes que en su vida laborar encontrara.

Finalmente es importante destacar que con esta actividad se logra desarrollar la capacidad de configurar y administrar dispositivos de Networking con el fin de mejorar el rendimiento de la red e implementar de manera apropiada el uso de tecnologías y protocolos de conmutación y enrutamiento sobre IP, teniendo en cuenta políticas básicas de seguridad de la información.

OBJETIVOS

Objetivo general

- Desarrollar la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación y enrutamiento sobre IP, articulando políticas básicas de seguridad de la información.

Objetivos específicos

- Utilizar herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

- Identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de Routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP.

- Diseñar políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

- Configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.

- Diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NATPAT respectivamente.

PLANTEAMIENTO DEL PROBLEMA

Definición del problema

Actualmente las redes de datos de las entidades o ciudades entre sí, tienen una mayor carga de tráfico debido al uso de sistemas integrados como ERP, base de datos, voz y video, es así que la red del Proyecto, en sus escenarios, presenta varios problemas como latencia, fallas de conexión, ausencia de mecanismos de control del uso del ancho de banda, pérdida de información, y otros.

Justificación

El presente trabajo se justifica por la importancia de contar con una red que garantice el intercambio de información sin retraso alguno y de forma segura, de tal manera que coadyuve al logro de objetivos en ambos escenarios.

En el desarrollo de proyectos de redes, se utilizan tecnologías de información y comunicación para realizar sus labores diarias, es de vital importancia que los sistemas de información y específicamente la red que los conecta y comunica con internet funcionen correctamente, sin fallas, sin retrasos y garantizando la seguridad de la información que por ella fluye. Más aun, para lograr la eficiencia en la gestión pública, es necesario que los equipos, medios, y software de comunicaciones estén correctamente configurados respecto a la necesidad de la entidad, para que los funcionarios puedan laborar de la mejor manera, siendo respaldados por una red de datos confiable y rápida.

Por tanto, se requiere una solución que cumpla los requerimientos de los usuarios, y permita el normal desarrollo de sus funciones, de seguir así, continuarán los retrasos y hasta incumplimiento de los objetivos que exige cada escenario.

1 ESCENARIO 1

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

.

Figura 1. Topología propuesta para el escenario 1.

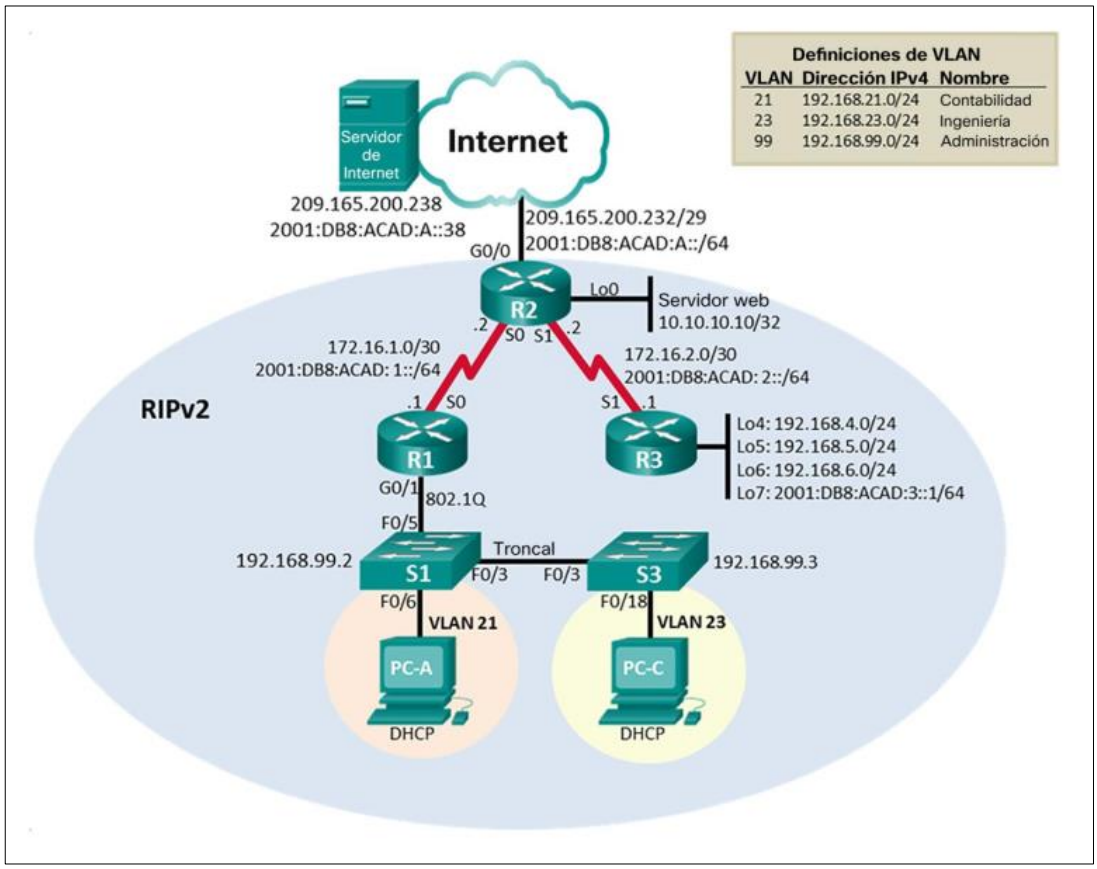
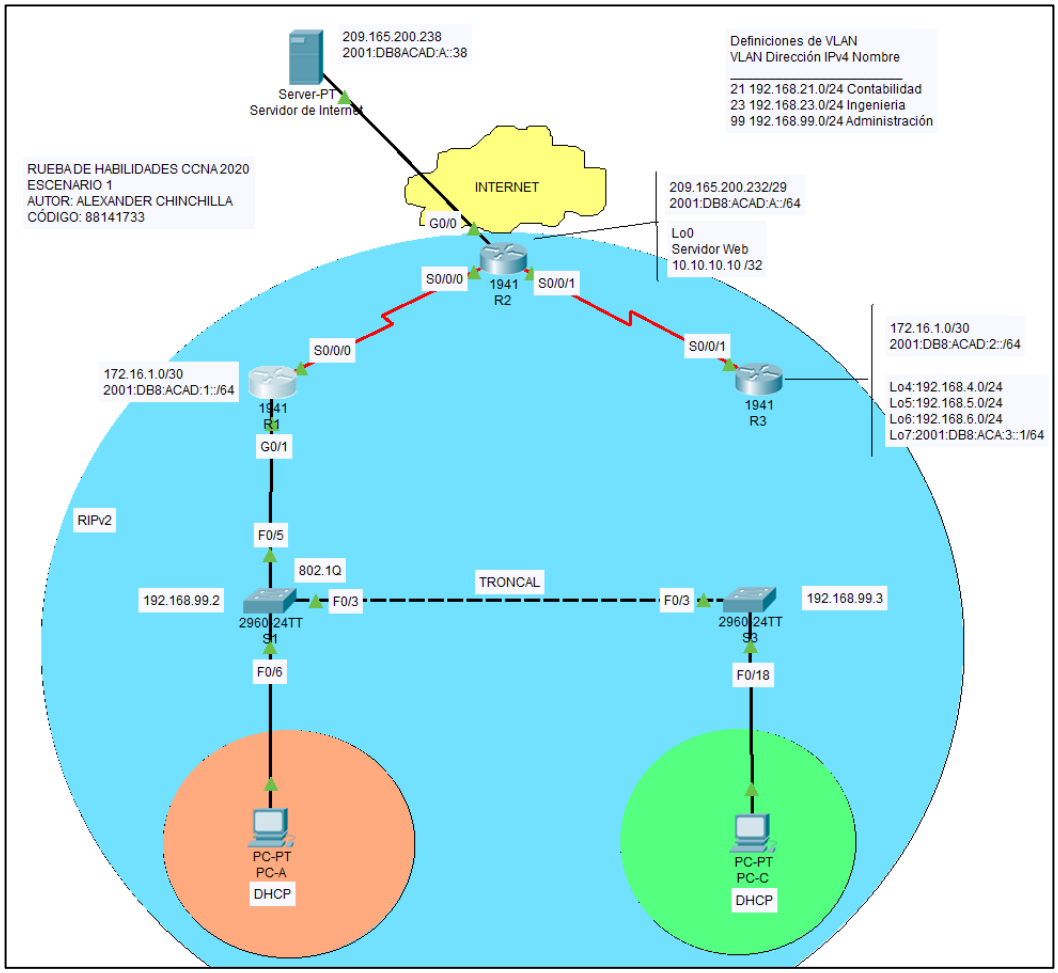


Figura 2. Diseño del escenario 1 - Topología en Packet Tracer.



1.1 Parte 1: Inicializar dispositivos

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

Para este paso, se debe eliminar la configuración de inicio y volver a cargar los dispositivos. Con las tareas de configuración, mostradas en la Tabla 1, garantizamos que los dispositivos de red no tengan datos en memoria como, base de datos VLAN u otras configuraciones preestablecidas.

Tabla 1. Tareas para iniciar y recargar los routers y switches.

Configuración	Especificación
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	Switch>enable Switch#erase startup-config
Volver a cargar ambos switches	Switch>enable Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show vlan brief

1.2 Parte 2: Configuración de los parámetros básicos de los dispositivos de la red

Después de garantizar que los dispositivos no tengan datos en memoria, se procede a configurarlos de acuerdo a los requerimientos del escenario 1 y listado de direccionamiento IP de la topología de red. Equipos que se configuran: 1 Servidor de Internet, 3 Routers, 2 Switches y 2 Computadoras.

1.2.1 Paso 1: Configuración del servidor de internet

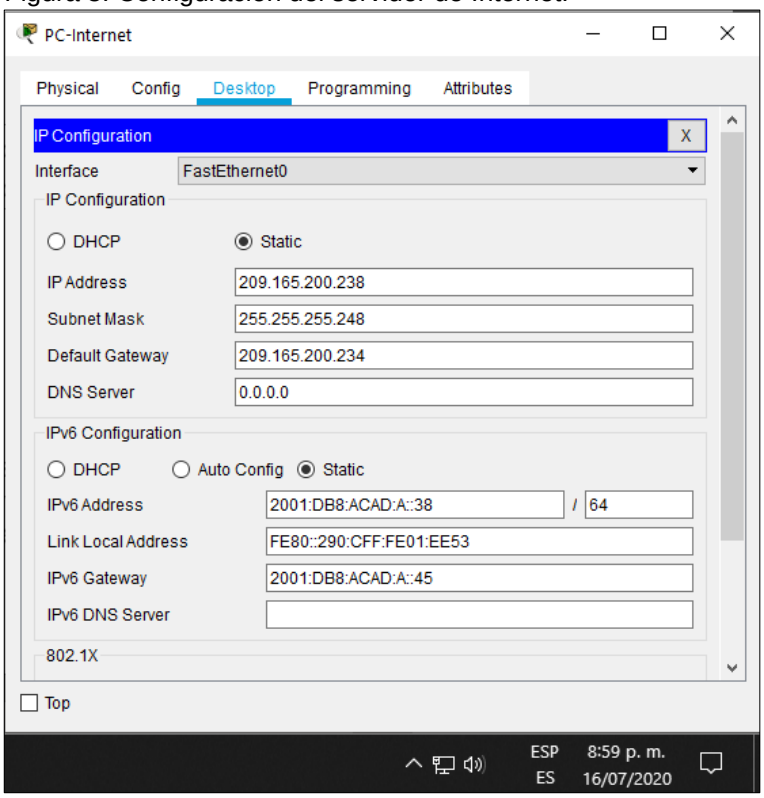
Se configura el servidor de internet con parámetros básicos de red como dirección IPv4, máscara de subred para IPv4, gateway predeterminado, dirección IPv6/subred, gateway predeterminado IPv6. La Tabla 2 muestra las tareas de configuración para la PC de Internet.

Tabla 2. Tareas de configuración para el servidor de Internet.

Configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1 No puede ser modificad

La figura 3 muestra la configuración del Servidor de internet en el simulador Packet Tracer.

Figura 3. Configuración del servidor de Internet.



1.2.2 Paso 2: Configuración de parámetros básicos del router R1

Se configura los parámetros básicos el router R1 de acuerdo a los requerimientos de la topología de red propuesta para el escenario 1, como: desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http, generar un mensaje de alerta si la contraseña ingresada es incorrecta, configurar la interfaz s0/0/0 y asignar rutas predeterminadas.

La Tabla 3 muestra las tareas de configuración para el Router R1.

Tabla 3. Tareas de configuración para el router R1.

Configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configure 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	Router>enable Router#configute terminal Router(config)#no ip domain-lookup

1.2.3 Paso 3: Configuración de parámetros básicos del router R2

Se configura los parámetros básicos el router R2 de acuerdo a los requerimientos de la topología de red propuesta para el escenario 1, como: desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http, generar un mensaje de alerta si la

contraseña ingresada es incorrecta, configurar las interfaces s0/0/0, s0/0/1, g0/0, loopback 0 y finalmente asignar rutas predeterminadas.

La Tabla 4 muestra los parámetros y tareas para la correcta configuración del Router R2.

Tabla 4. Tareas de configuración para el router R2.

Configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configure 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

Configuración	Especificación
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 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::45/64 R2(config-if)#no shutdown
Interfaz loopback 0	R2(config-if)#interface l0 R2(config-if)#description R2-web Server R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

1.2.4 Paso 4: Configuración de parámetros básicos del router R3

Se configura los parámetros básicos el router R3 de acuerdo a los requerimientos de la topología de red propuesta para el escenario 1, como: desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http, generar un mensaje de alerta si la contraseña ingresada es incorrecta, configurar las interfaces s0/0/1, loopback 4,5,6,7 y finalmente asignar rutas predeterminadas.

La Tabla 5 muestra los parámetros y tareas para la correcta configuración del Router R3.

Tabla 5. Tareas de configuración para el router R3.

Configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configute terminal Router(config)#no ip domain-lookup

Configuración	Especificación
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

1.2.5 Paso 5: Configuración de parámetros básicos del switch S1

Se configura los parámetros básicos del switch S1 de acuerdo a los requerimientos de la topología de red propuesta para el escenario 1, como: desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http, generar un mensaje de alerta si la contraseña ingresada es incorrecta.

La Tabla 6 muestra los parámetros y tareas para la correcta configuración del Switch S1.

Tabla 6. Tareas de configuración para el switch S1.

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 $Se prohíbe el acceso no autorizado.$

1.2.6 Paso 6: Configuración de parámetros básicos del switch S3

Se configura los parámetros básicos del switch S3 de acuerdo a los requerimientos de la topología de red propuesta para el escenario 1, como: desactivar DNS, nombrar el router, establecer contraseña, configurar el acceso a la consola y telnet, cifrar la contraseña, habilitar el servidor http, generar un mensaje de alerta si la contraseña ingresada es incorrecta.

La Tabla 7 muestra los parámetros y tareas para la correcta configuración del Switch S3.

Tabla 7. Tareas de configuración para el switch S3

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 $Se prohíbe el acceso no autorizado.$

1.2.7 Paso 7: Verificación de la conectividad de la red

Por medio del comando ping se comprueba si existe conectividad entre los dispositivos de la red del escenario 1.

La Tabla 8 muestra la verificación metódicamente de la conectividad entre cada dispositivo de la red.

Tabla 8. Verificación de la conectividad de la red.

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

Las figuras siguientes muestran la verificación de la conectividad entre los dispositivos de red.

Figura 4. Prueba de ping desde R1 a R2.

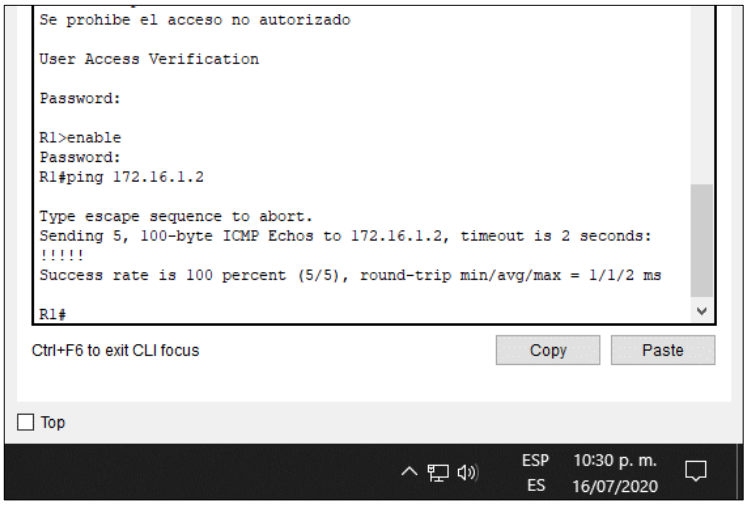


Figura 5. Prueba de ping desde R2 a R3

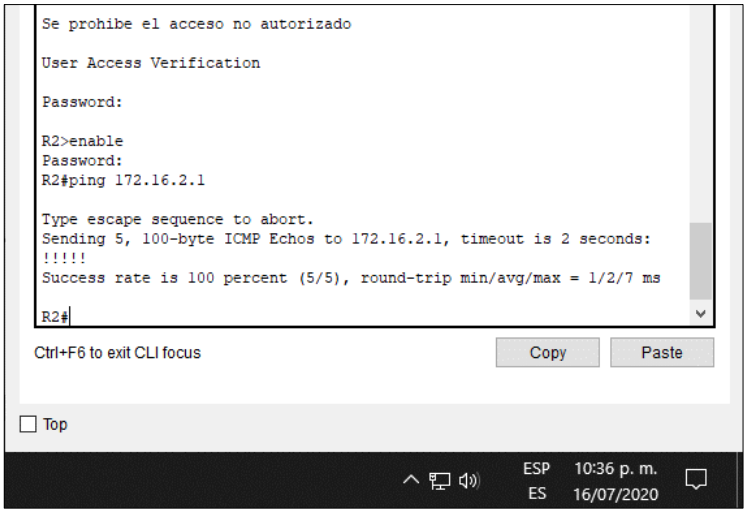
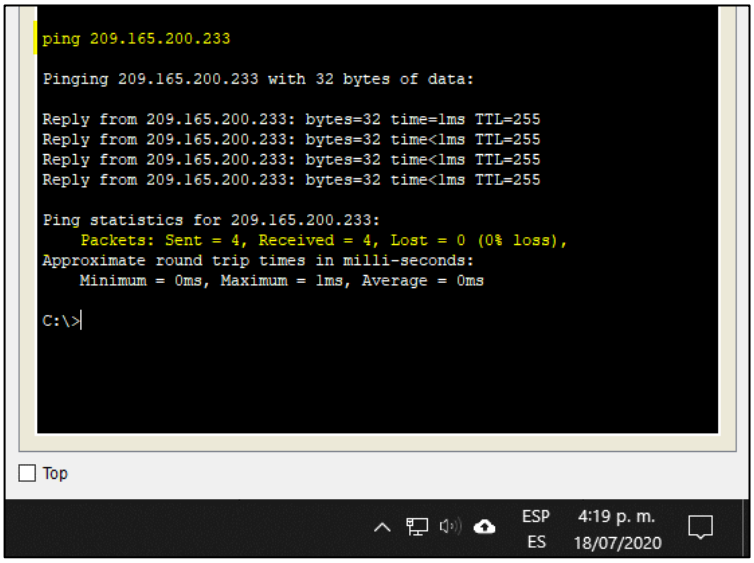


Figura 6. Ping desde la PC de internet al gateway.



1.3 Parte 3: Configuración de la seguridad del switch, las VLAN y el routing entre VLAN

1.3.1 Paso 1: Configuración de las VLAN para el switch S1

Se realiza la configuración del Switch S1 de acuerdo a la topología propuesta, asignando las VLAN 21, 23 y 99 a las áreas de Contabilidad, Ingeniería y Administración respectivamente.

La Tabla 9 muestra los parámetros y tareas para la correcta configuración de la seguridad del switch, las VLAN y el routing entre VLAN del switch S1.

Tabla 9. Tareas de configuración VLAN para S1.

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

Configuración	Especificación
	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

1.3.2 Paso 2: Configuración de las VLAN para el switch S3

Se realiza la configuración del Switch S3 de acuerdo a la topología propuesta, asignando las VLAN 21, 23 y 99 a las áreas de Contabilidad, Ingeniería y Administración respectivamente.

La Tabla 10 muestra los parámetros y tareas para la correcta configuración de la seguridad del switch, las VLAN y el routing entre VLAN del switch S3.

Tabla 10. Tareas de configuración de las VLAN para S3.

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 21	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

1.3.3 Paso 3: Configuración de las VLAN para el router R1

Se realiza la configuración del Router R1 según la topología requerida, asignando la subinterfaz 802.1Q para cada una de las VLAN 21, 23 y 99.

La Tabla 11 muestra las tareas de configuración de las subinterfaces y asignación VLAN para el router R1.

Tabla 11. Tareas de configuración de las VLAN para el router R1.

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

Configuración	Especificación
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

1.3.4 Paso 4: Verificación de la conectividad de la red

Utilizando el comando ping se comprueba o verifica que existe conectividad entre los dispositivos de red.

La Tabla 12 muestra la verificación metódicamente de la conectividad entre cada dispositivo de la red.

Tabla 12. Tabla de verificación de la conectividad de la red.

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

Figura 7. Verificación ping desde S1 a R1, VLAN 99, VLAN 21.

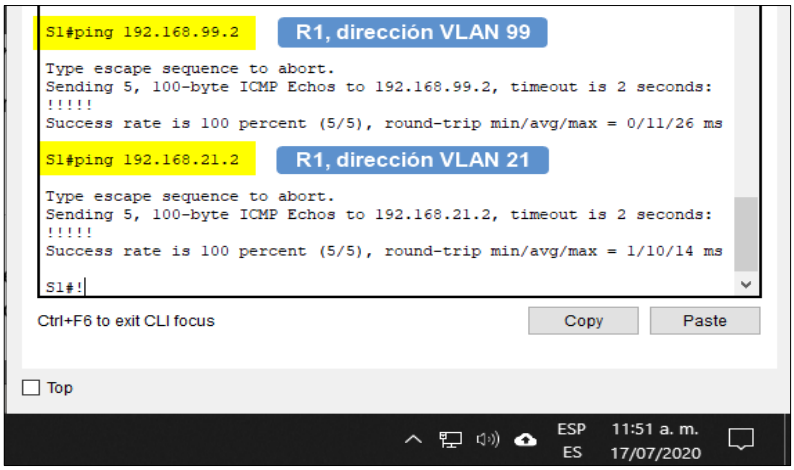
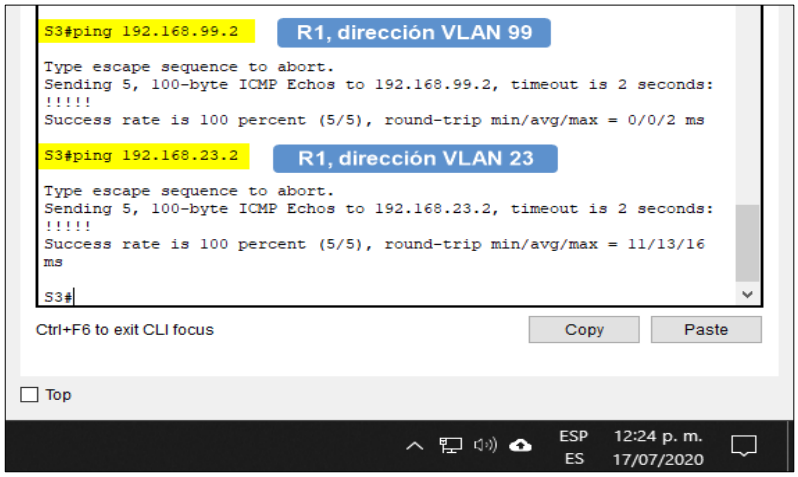


Figura 8. Verificación ping desde S1 a R1, VLAN 99, VLAN 23.



1.4 Parte 4: Configuración del protocolo de routing dinámico RIPV2

1.4.1 Paso 1: Configuración del RIPV2 en el router R1

La Tabla 13 muestra las tareas de configuración del RIPV2 para el router R1. Su finalidad es que el router pueda negociar o intercambiar datos entre las redes que estén interconectadas, esto se logra verificando o validando los saltos generados.

Tabla 13. Tareas de configuración RIPV2 en el router R1.

Configuración	Especificación
Configurar RIP versión 2	R1#configure terminal R1(config)#router rip R1(config-router)#version 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 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

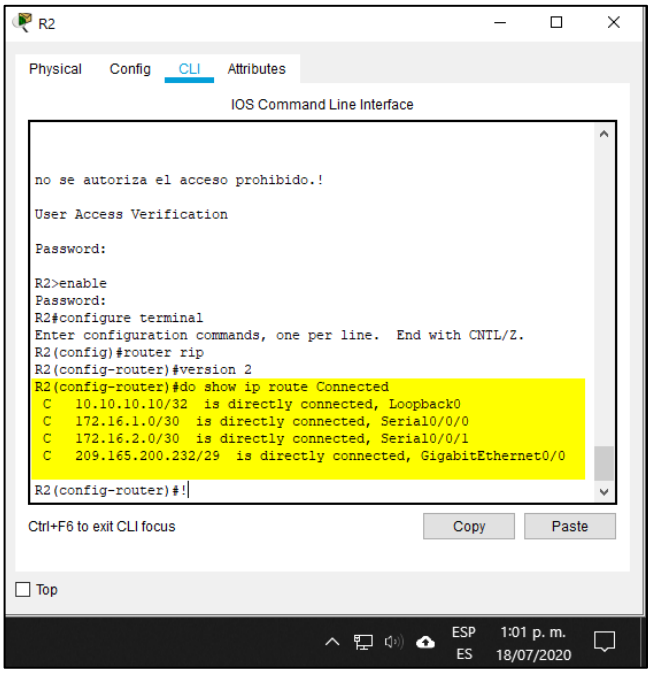
1.4.2 Paso 2: Configuración del RIPV2 en el router R2

La Tabla 14 muestra las tareas de configuración del RIPV2 para el router R2. Su finalidad es que el router pueda negociar o intercambiar datos entre las redes que estén interconectadas, esto se logra verificando o validando los saltos generados.

Tabla 14. Tareas de configuración RIPV2 en el router R2.

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

Figura 9. Verificación RIP *do show ip route connected* en R2.



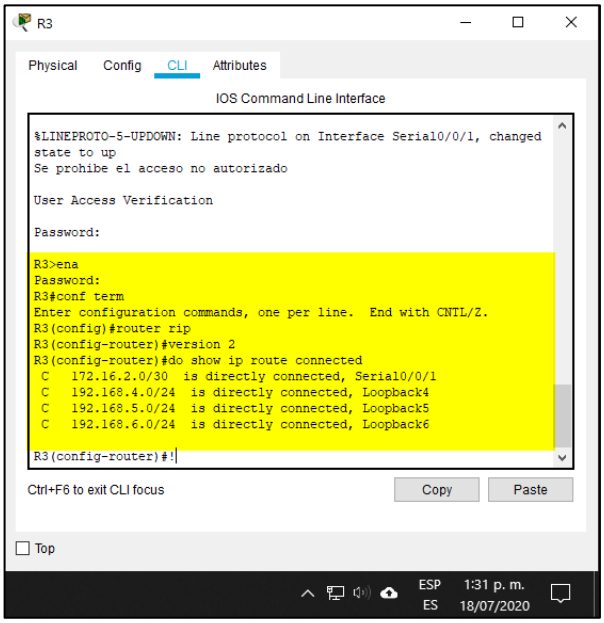
1.4.3 Paso 3: Configuración del RIPV2 en el router R3

La Tabla 15 muestra las tareas de configuración del RIPV2 para el router R3. Su finalidad es que el router pueda negociar o intercambiar datos entre las redes que estén interconectadas, esto se logra verificando o validando los saltos generados.

Tabla 15. Tareas de configuración RIPV2 en el router R3.

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

Figura 10. Verificación RIP *do show ip route connected* en R3.



1.4.4 Paso 4: Verificación de la información del protocolo de routing RIP

La Tabla 16 muestra los comandos de la CLI (interfaz de línea de comando) que se usan para comprobar o verificar que el protocolo RIP está funcionando correctamente.

Tabla 16. Comandos de la CLI para verificar la información de RIP.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del Router, las redes de routing y las interfaces pasivas configuradas en un Router?. Ver Figura 9	R1#show ip protocols
¿Qué comando muestra solo las rutas RIP? Ver Figura 10	R1#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución? Ver Figura 11	R1#show run

Figura 11. Verificación RIP *show ip protocols* en R1.

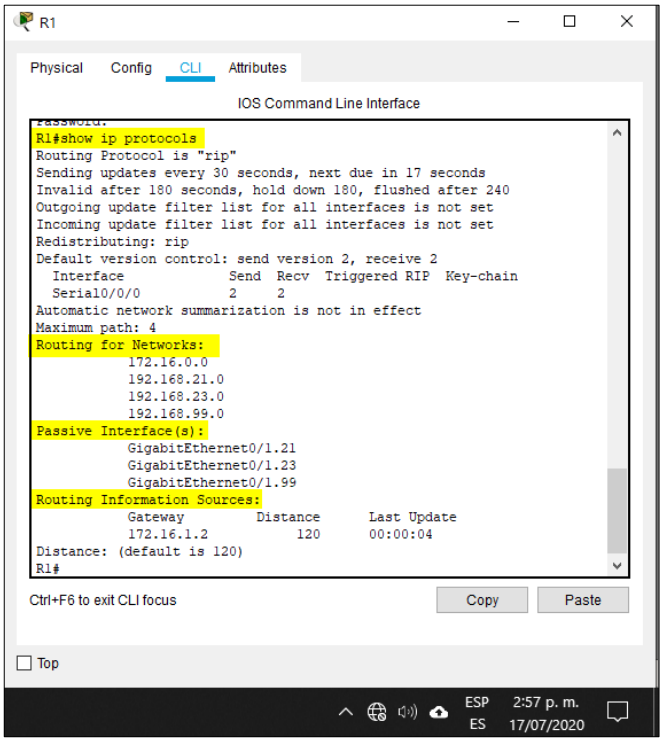


Figura 12. Verificación RIP *show ip route rip* en R1

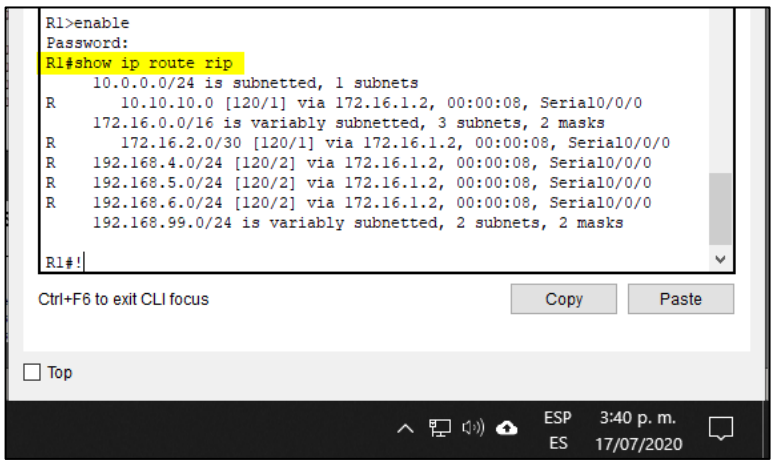
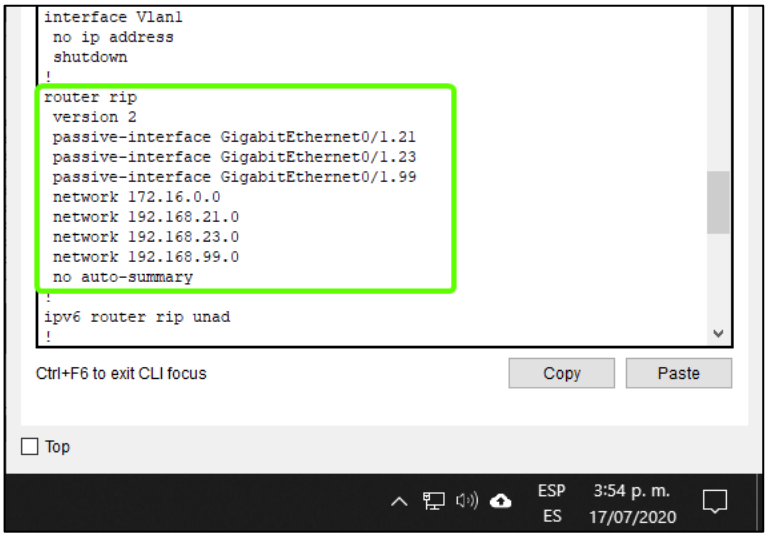


Figura 13. Verificación RIP *show run* en R1



1.5 Parte 5 : Implementación del servicio DHCP y NAT para la IPV4

1.5.1 Paso 1: Configuración del router R1 como servidor de DHCP para las VLAN 21 y 23

En este paso se configura el router R1 como servidor de DHCP para las VLAN 21 y 23 y se reservan las primeras 20 direcciones IP para las respectivas redes de áreas locales virtuales. La Tabla 17 muestra las tareas para la configuración del router R1 como servidor de DHCP para las VLAN 21 y 23.

Tabla 17. Tareas para Implementar DHCP y NAT para la IPv4.

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

1.5.2 Paso 2 : Configuración de la NAT estática y dinámica en el router R2

La siguiente configuración de R2 se efectúa para establecer las NAT estática y dinámica, creando una base de datos local para tener acceso por un usuario, se habilita el servicio HTTP y se establece una lista de acceso privada con las direcciones permitidas para ingresar. La Tabla 18 muestra las tareas para la configuración de la NAT estática y dinámica en el router R2

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

Configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#User webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (Este commando no funciona en Packet Tracer)

Configuración	Especificación
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (Este commando no funciona en Packet Tracer)
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	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

1.5.3 Paso 3: Verificación del protocolo DHCP y la NAT estática

La Tabla 19 muestra las tareas para verificar que, las configuraciones de DHCP y NAT estática, funcionan de forma correcta. Tal vez sea necesario deshabilitar el firewall[1] de los computadores para que los pings se realicen correctamente.

Tabla 19. Tareas para verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP. Ver Figura 12.	ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP. Ver Figura 13.	ok
Verificar que la PC-A pueda hacer ping a la PC-C. Ver Figura 14.	ok

[1] En el caso de computadores físicos

Prueba	Resultados
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** Ver Figura 15.	(No se pudo ingresar puesto que el comando **"ip http server"** no es soportado por Packet Tracer)

Figura 14. Verificación del servicio de DHCP en la PC-A.

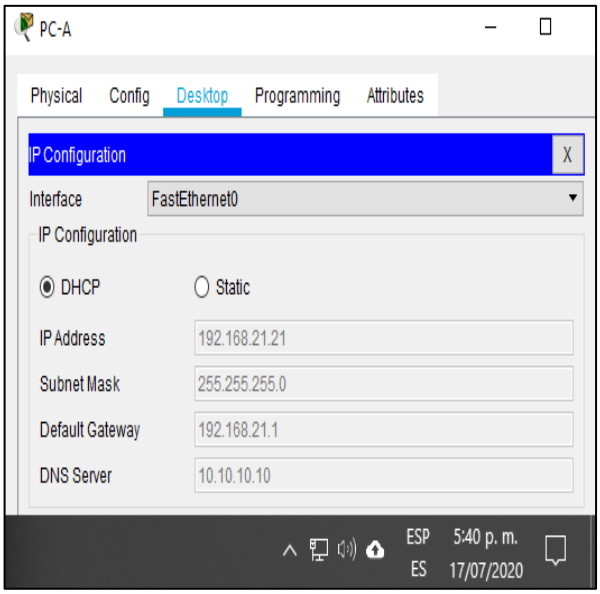


Figura 15. Verificación del servicio de DHCP en la PC-C.

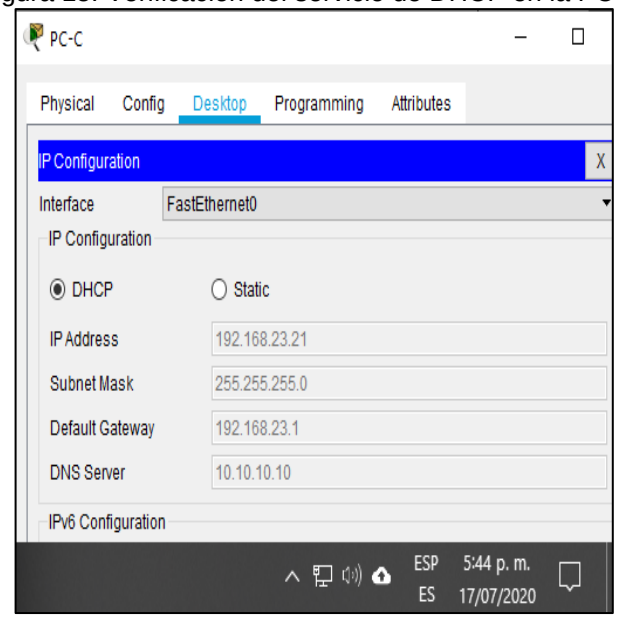


Figura 16. Verificación que la PC-A pueda hacer ping a la PC-C.

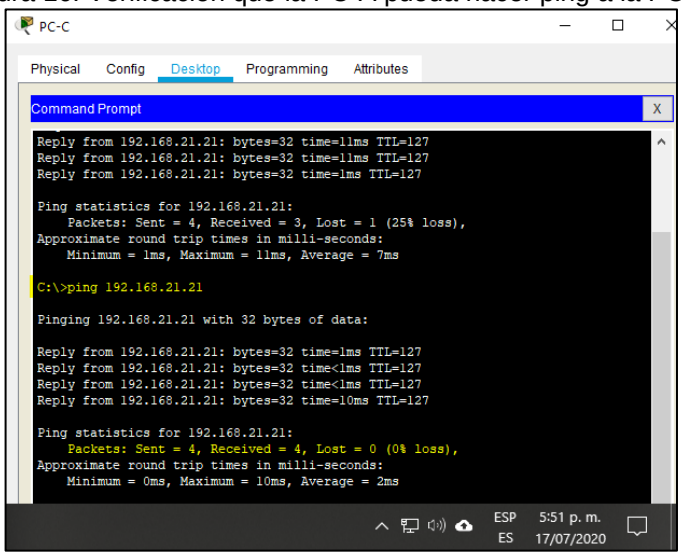
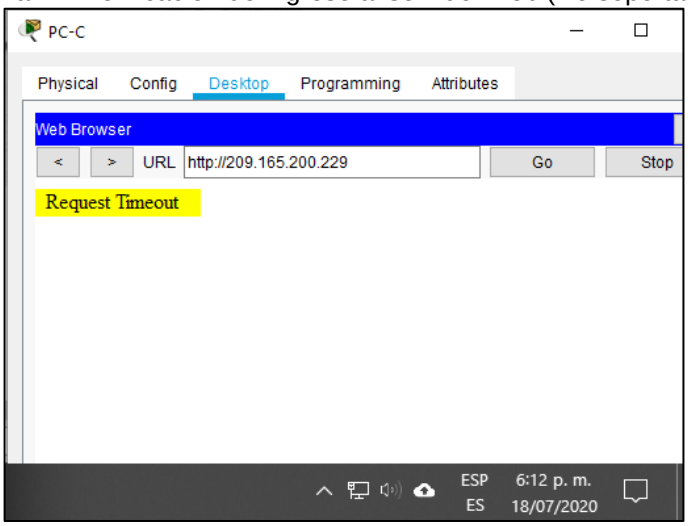


Figura 17. Verificación de ingreso al servidor web (No soportado).



1.6 Parte 6 : Configuración NTP (Network Time Protocol)

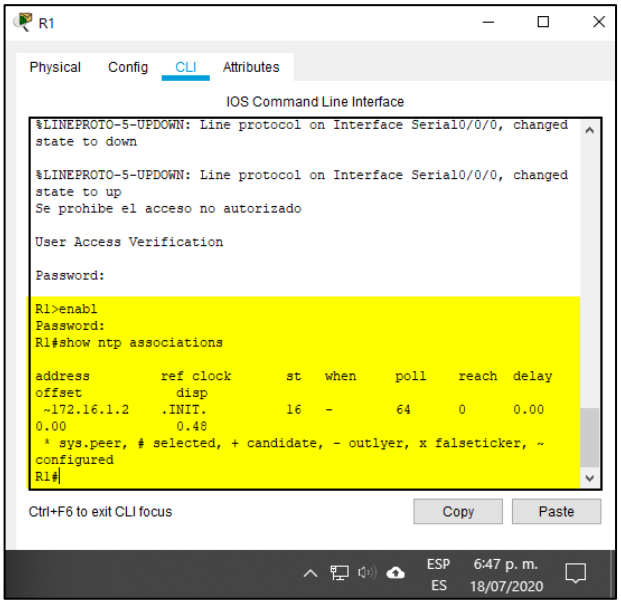
Se configura el protocolo de tiempo de red NTP, su finalidad es sincronizar los relojes de los dispositivos de la red, para completar el requerimiento del escenario 1, se establece R2 como maestro (servidor) y R1 como cliente, interactuarán y sincronizarán la hora en la red. Se realiza la verificación en la configuración de R1.

La Tabla 20 muestra las tareas de configuración del protocolo NTP en R1 y R2.

Tabla 20. Tareas de configuración NTP en R1 y R2.

Configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2#configure terminal R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1#configure terminal R1(config)#ntp server 172.16.1.2
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#show ntp associations

Figura 18. Verificación de la configuración de NTP en R1.



1.7 Parte 7: Configuración y verificación de las listas de control de acceso (ACL)

1.7.1 Paso 1 : Restringiendo el acceso a las líneas VTY en el R2

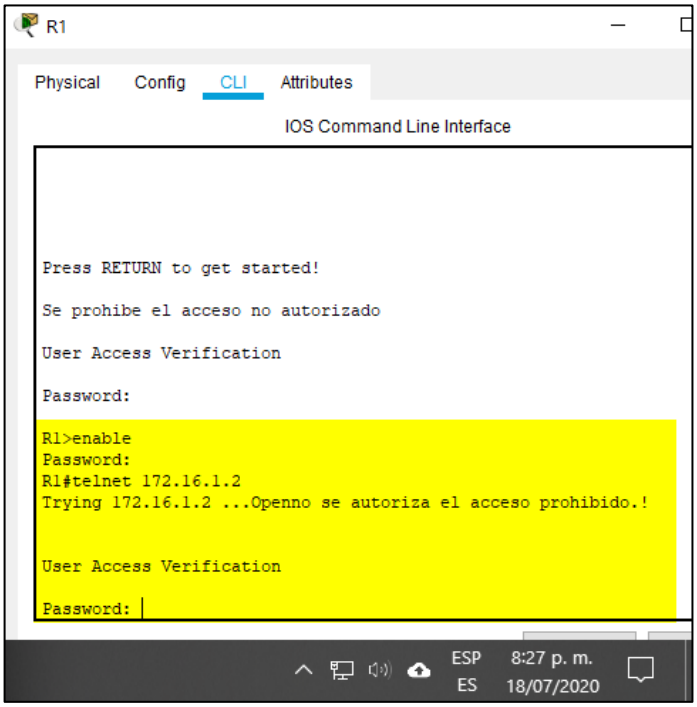
En este paso se configuran las listas de acceso con nombre para permitir que solo R1 establezca una conexión Telnet, se restringe también todo acceso a las líneas VTY. Finalmente se verifica que la configuración sea la correcta.

La Tabla 21 muestra las tareas para la configuración de la restricción de las líneas VTY en el router R2.

Tabla 21. Tareas de configuración y verificación de las 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#configure terminal 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
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Ok

Figura 19. Verificación del acceso a las líneas VTY en el router R2.



1.7.2 Paso 2 : Introducción del comando de CLI adecuado que se necesita para mostrar lo siguiente

La Tabla 22 indica los comandos adecuados para mostrar la coincidencia recibidas por una lista, restablecer los contadores, mostrar que ACL e IP que se aplica en una interfaz y por último mostrar y eliminar las traducciones NAT.

Tabla 22. Comandos de CLI para el paso 2.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear access-list counters R2#clear ip ?
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation

Figura 20. *show access list* en R2.

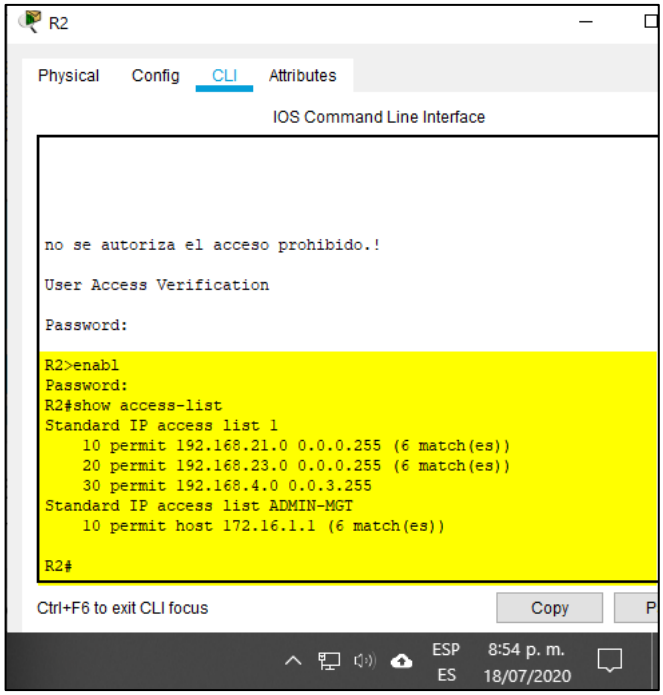


Figura 21. *show ip access-list* en R2.

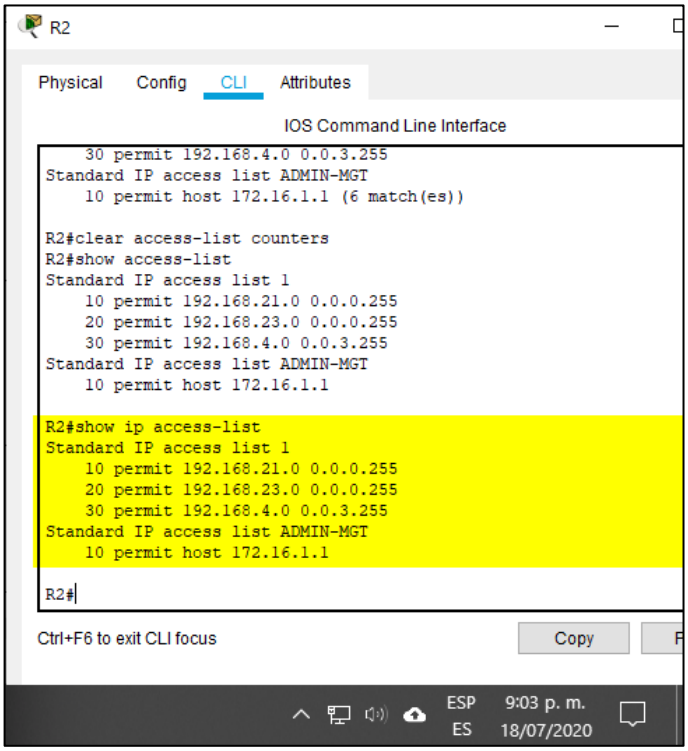


Figura 22. *show ip interface* en R2.

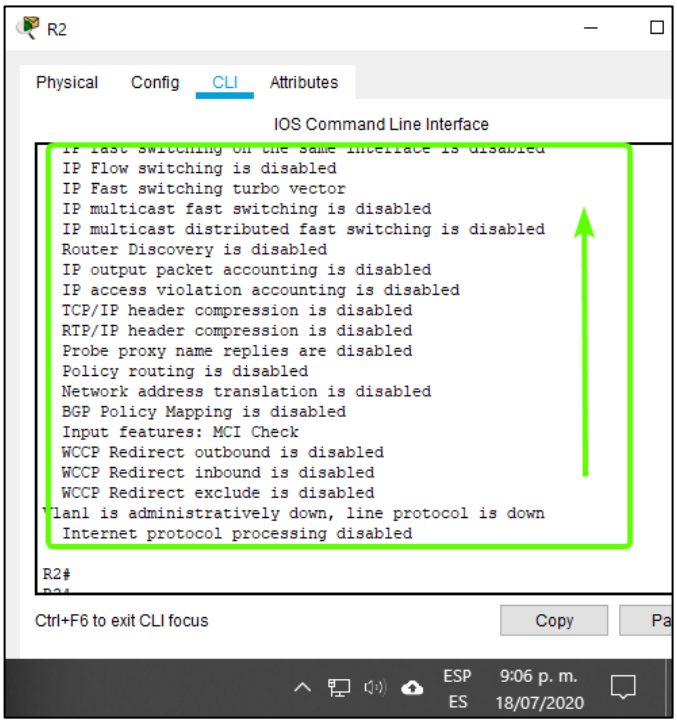


Figura 23. *show ip nat translations* en R2.

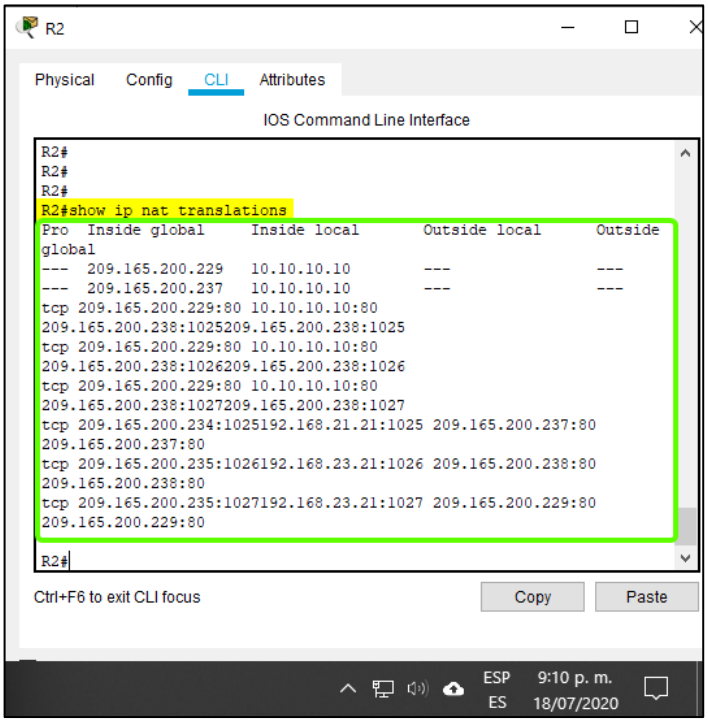


Figura 24. Prueba de ping al Servidor de Internet desde la PC-A.

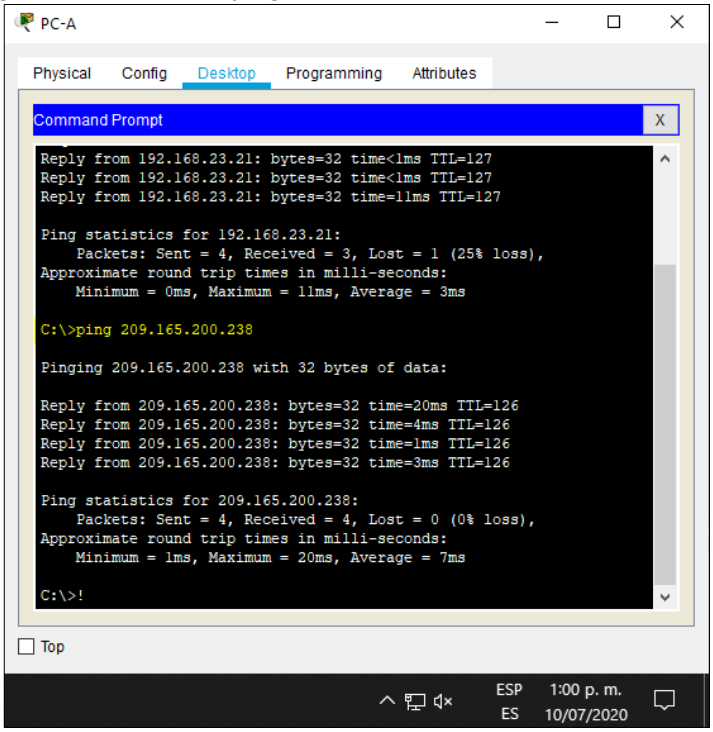


Figura 25. Prueba de ping al Servidor de Internet desde la PC-C.

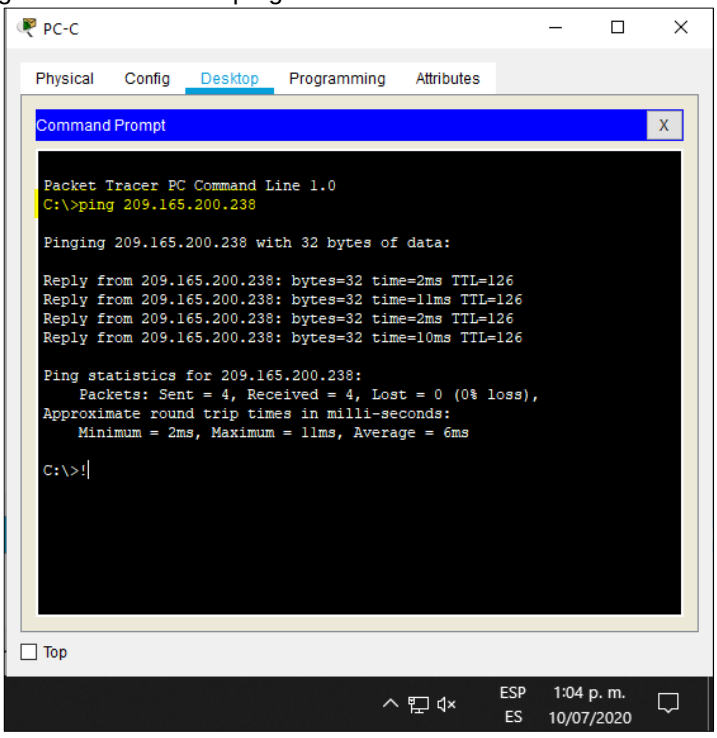


Figura 26. Prueba de acceso al Servidor de Web desde PC-A.

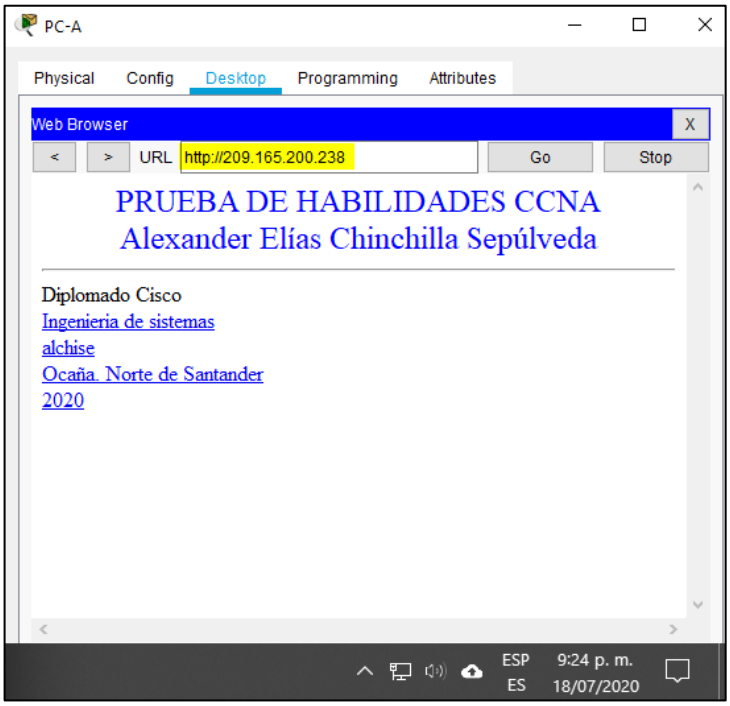
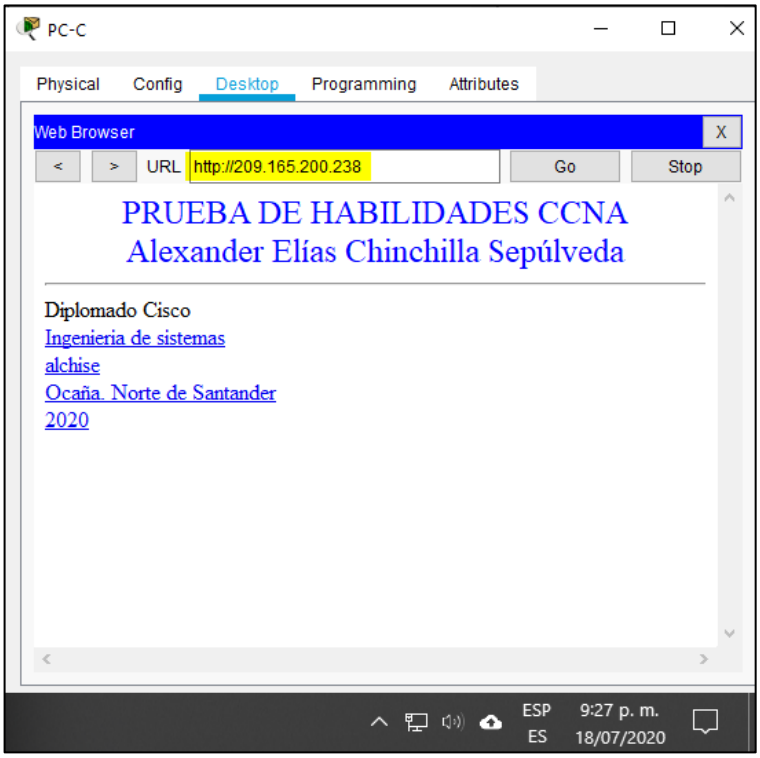


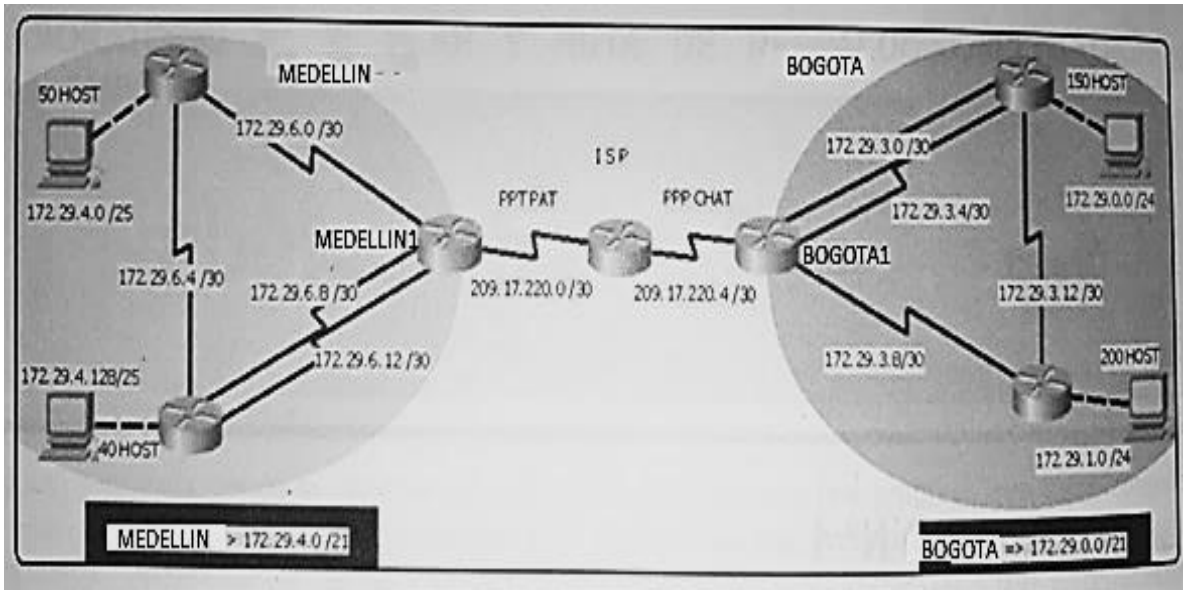
Figura 27. Prueba de acceso al Servidor de Web desde PC-C.



2 ESCENARIO 2

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

Figura 28. Topología propuesta para el 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.
Se debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Se debe habilitar NAT de sobrecarga en los Routers Bogota1 y medellin1.

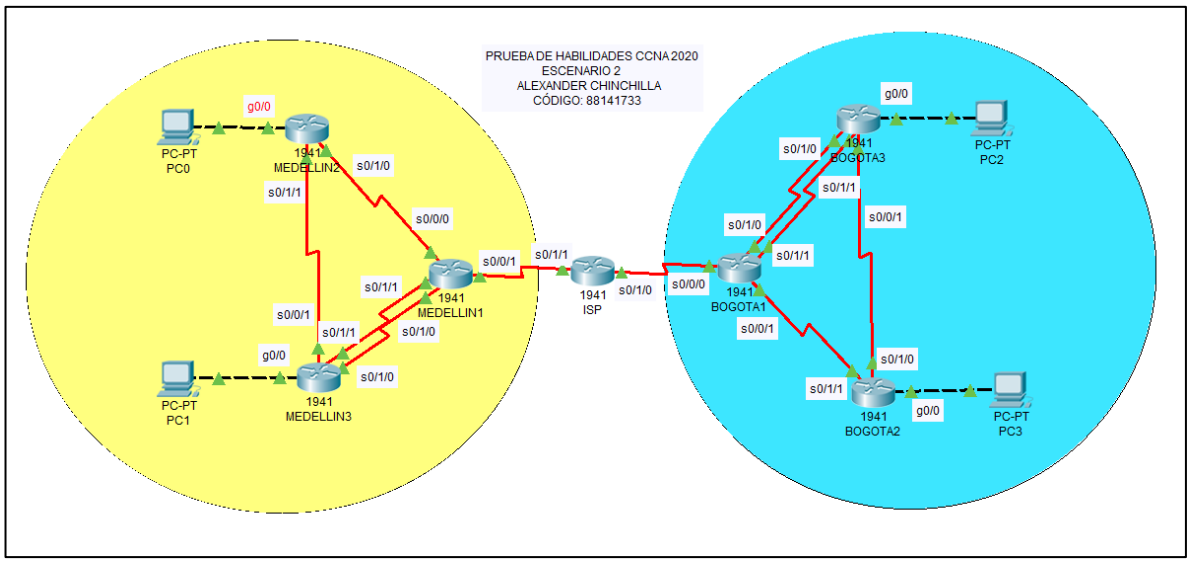
2.1 Trabajo inicial

Como trabajo inicial se debe realizar lo siguiente:

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

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

Figura 29. Diseño del escenario 2 - Topología en Packet Tracer.



2.2 Configuración básica de los dispositivos

Se configuran los routers de Bogota, Medellín e ISP con la misma configuración, haciendo salvedad que, las contraseñas en un ejercicio real deben ser diferentes, para efectos académicos, se usaran las mismas. Se configuran nombre, claves de seguridad, mensaje Motd, Nvram, entre otros.

La Tabla 23 muestra las tareas de configuración básica para los routers Medellín, Bogotá e ISP.

Tabla 23. Configuración de routers Medellín, Bogotá y ISP

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

2.3 Especificaciones de la topología de red

La Tabla 23 muestra las especificaciones para una correcta configuración de la red del escenario 2, esta información permitirá configurar el enrutamiento de los Routers.

Tabla 24. Especificaciones de la topología de red.

Dispositivo	Interfaz	Conexión a	Dirección IP	Máscara de Subred	Gateway Predeterminado
Medellin1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.13	255.255.255.252	N.A
	S0/1/0	Medellin2	172.29.6.9	255.255.255.252	N.A
	S0/1/1	Medellin3	172.29.6.1	255.255.255.252	N.A
Medellin2	S0/0/0	Medellin1	172.29.6.10	255.255.255.252	N.A
	S0/0/1	Medellin1	172.29.6.14	255.255.255.252	N.A
	S0/1/0	Medellin3	172.29.6.6	255.255.255.252	N.A
	G0/0	PCM2	**172.29.4.129**	255.255.255.192	
Medellin3	S0/0/0	Medellin1	172.29.6.2	255.255.255.252	N.A
	S0/0/1	Medellin2	172.29.6.5	255.255.255.252	N.A
	G0/0	PCM3	**172.29.4.1**	255.255.255.192	
Bogota1	S0/0/0	Bogota2	172.29.3.1	255.255.255.252	N.A
	S0/0/1	Bogota2	172.29.3.5	255.255.255.252	N.A
	S0/1/0	Bogota3	172.29.3.9	255.255.255.252	N.A
	S0/1/1	ISP	209.17.220.6	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	PCB2	**172.29.0.1**	255.255.255.0	
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	PCB3	**172.29.1.1**	255.255.255.0	
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
PCM2	Fa0	172.29.4.130	DHCP	255.255.255.192	172.29.4.129
PCM3	Fa0	172.29.4.2	DHCP	255.255.255.192	172.29.4.1
PCB2	Fa0	172.29.0.2	DHCP	255.255.255.0	172.29.0.1
PCB3	Fa0	172.29.1.2	DHCP	255.255.255.0	172.29.1.1

2.4 Configuración IP de los router del sistema de la red

La Tabla 25 muestra las tareas de configuración del direccionamiento IP que tendrá la red, se procede a asignar las IP correspondientes a cada una de las interfaces, con su respectiva máscara de subred, se establece la velocidad de envío de datos a 128000 bits por segundo.

Tabla 25. Configuración del direccionamiento IP.

Dispositivo	Configuración direccionamiento IP
ISP	ISP>enable ISP#configure terminal ISP(config)#int s0/0/0 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#no shutdown ISP(config-if)#int s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown
Medellin1	Medellin1>enable Medellin1#configure terminal Medellin1(config)#int s0/0/0 Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/0/1 Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/1/0 Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#int s0/1/1 Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252 Medellin1(config-if)#clock rate 128000

Dispositivo	Configuración direccionamiento IP
	Medellin1(config-if)#no shutdown
Medellin2	Medellin2>enable Medellin2#configure terminal Medellin2(config)#int s0/0/0 Medellin2(config-if)#ip address 172.29.6.10 255.255.255.252 Medellin2(config-if)#no shutdown Medellin2(config-if)#int s0/0/1 Medellin2(config-if)#ip address 172.29.6.14 255.255.255.252 Medellin2(config-if)#clock rate 128000 Medellin2(config-if)#no shutdown Medellin2(config-if)#int s0/1/0 Medellin2(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin2(config-if)#clock rate 128000 Medellin2(config-if)#no shutdown Medellin2(config-if)#int g0/0 Medellin2(config-if)#ip address 172.29.4.129 255.255.255.192 Medellin2(config-if)#no shutdown
Medellin3	Medellin3>enable Medellin3#configure terminal Medellin3(config)#int s0/0/0 Medellin3(config-if)#ip address 172.29.6.2 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config-if)#int s0/0/1 Medellin3(config-if)#ip address 172.29.6.5 255.255.255.252 Medellin3(config-if)#clock rate 128000 Medellin3(config-if)#no shutdown Medellin3(config-if)#int g0/0 Medellin3(config-if)#ip address 172.29.4.1 255.255.255.192 Medellin3(config-if)#no shutdown
Bogota1	Bogota1>enable Bogota1#configure terminal Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/0/1 Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/1/0 Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#int s0/1/1 Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown

Bogota2	Bogota2>enable Bogota2#configure terminal Bogota2(config)#int s0/0/0 Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252 Bogota2(config-if)#no shutdown Bogota2(config-if)#int s0/0/1 Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252 Bogota2(config-if)#clock rate 128000 Bogota2(config-if)#no shutdown 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 128000 Bogota2(config-if)#no shutdown Bogota2(config-if)#int g0/0 Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota2(config-if)#no shutdown
Bogota3	Bogota3>enable Bogota3#configure terminal Bogota3(config)#int s0/0/0 Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#int s0/0/1 Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252 Bogota3(config-if)#clock rate 128000 Bogota3(config-if)#no shutdown Bogota3(config-if)#int g0/0 Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0 Bogota3(config-if)#no shutdown

2.5 Parte 1: Configuración del enrutamiento

Configuramos el enrutamiento en la red usando el protocolo OSPF versión 2, declarando la red principal de cada uno de los routers (esto se puede hacer identificando las conexiones directas de cada uno de los routers) y desactivando la sumarización automática. En este caso no incluimos el router ISP porque tiene rutas estáticas sumarizadas (la configuración se hará posteriormente). La Tabla 26 muestra las tareas de configuración de enrutamiento OSPF versión 2.

Tabla 26. Configuración de enrutamiento OSPF versión 2

Dispositivo	Configuración OSPF en los Routers
Medellin1	Medellin1#configure terminal Medellin1(config)#router ospf 1 Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin1(config-router)#exit Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medellin1(config)#no auto-summary

Medellin2	Medellin2#configure terminal Medellin2(config)#router ospf 1 Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin2(config-router)#network 172.29.4.128 0.0.0.63 area 1 Medellin2(config-router)#default-information originate Medellin2(config-router)#no auto-summary
Medellin3	Medellin3#configure terminal Medellin3(config)#router ospf 1 Medellin3(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 1 Medellin3(config-router)#network 172.29.4.0 0.0.0.63 area 1 Medellin3(config-router)#default-information originate Medellin3(config-router)#no auto-summary
Bogota1	Bogota1#configure terminal Bogota1(config)#router ospf 1 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)#exit Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota1(config)#no auto-summary
Bogota2	Bogota2(config)#router ospf 1 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 172.29.3.12 0.0.0.3 area 1 Bogota2(config-router)#network 172.29.0.0 0.0.0.63 area 1 Bogota2(config-router)#default-information originate Bogota2(config-router)#no auto-summary
Bogota3	Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 1 Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1 Bogota3(config-router)#network 172.29.1.0 0.0.0.63 area 1 Bogota3(config-router)#default-information originate Bogota3(config-router)#no auto-summary

La condición de la red es que los routers Bogota1 y Medellín acepten un enrutamiento por defecto que se direccione al router ISP, además, de redistribuirla dentro de las publicaciones de OSPF.

La Tabla 27 muestra las tares de configuración de las Ruta Redistribuida en OSPF.

Tabla 27. Configuración de Ruta Redistribuida en OSPF.

Dispositivo	Configuración Ruta Distribuida en OSPF
Medellin1	Medellin1#configure terminal Medellin1(config)#router ospf 1 Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 1 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 1 Medellin1(config-router)#default-information originate Medellin1(config-router)#exit
Bogota1	Bogota1#configure terminal Bogota1(config)#router ospf 1 Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 1 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)#exit

Debido a que el router ISP se comunica directamente con Medellin1 y Bogota 1, se tendrá que configurar una ruta estática que esté dirigida a la red interna de ellos, por lo tanto se realiza la sumarización de las subredes de dichos routers a /22.

La Tabla 28. Muestra las tareas de configuración de las rutas estáticas sumarizadas a Sedes.

Tabla 28. Configuración de rutas estáticas sumarizadas a Sedes.

Dispositivo	Configuración Rutas Estáticas Sumarizadas a Sedes
ISP	ISP#configure 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

2.6 Parte 2: Tabla de enrutamiento

Se verifica la tabla de enrutamiento configurada anteriormente en cada uno de los routers, se utiliza el comando “show ip route”, este comando permite ver las redes y sus rutas, además del balanceo de carga que presentan los routers.

Figura 30. Verificación de enrutamiento ISP.

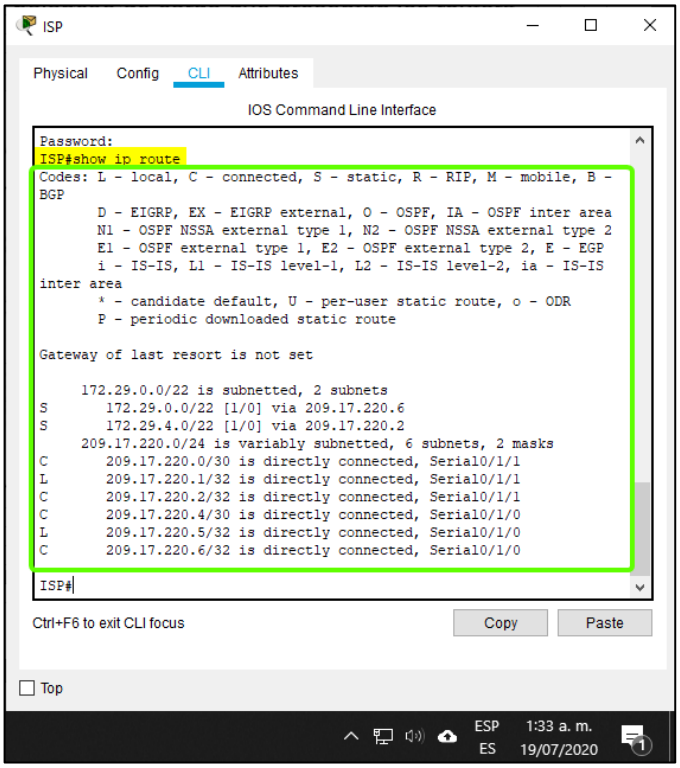


Figura 31. Verificación de enrutamiento Bogota1 y Medellin1.

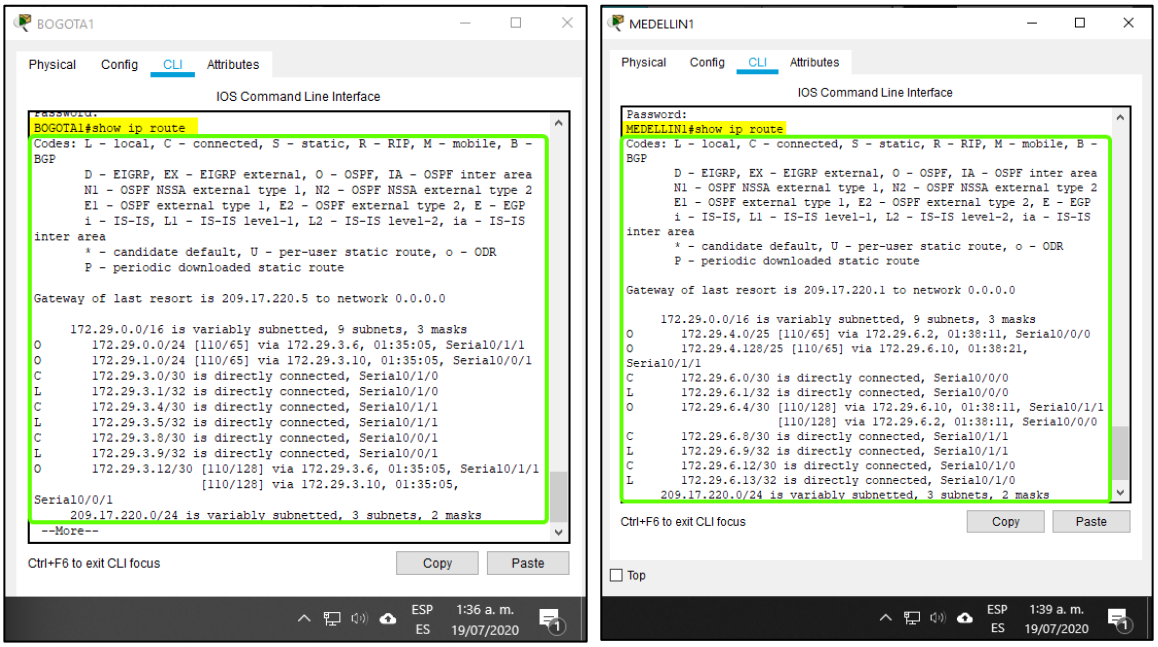


Figura 32. Verificación de enrutamiento Bogota2 y Medellin2.

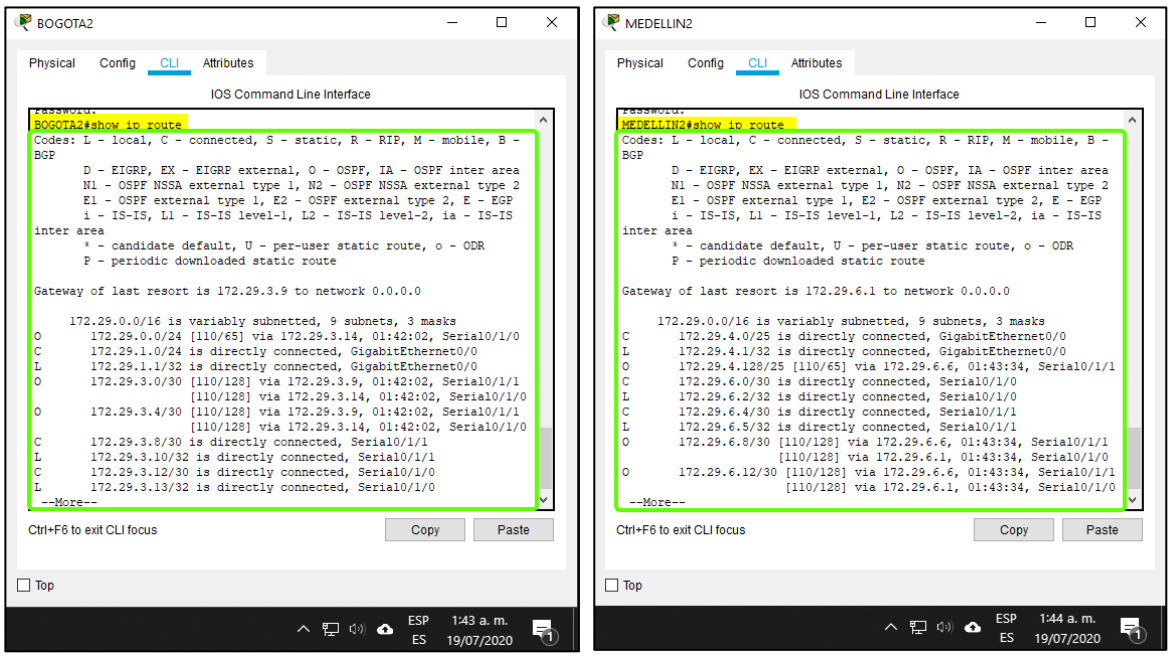
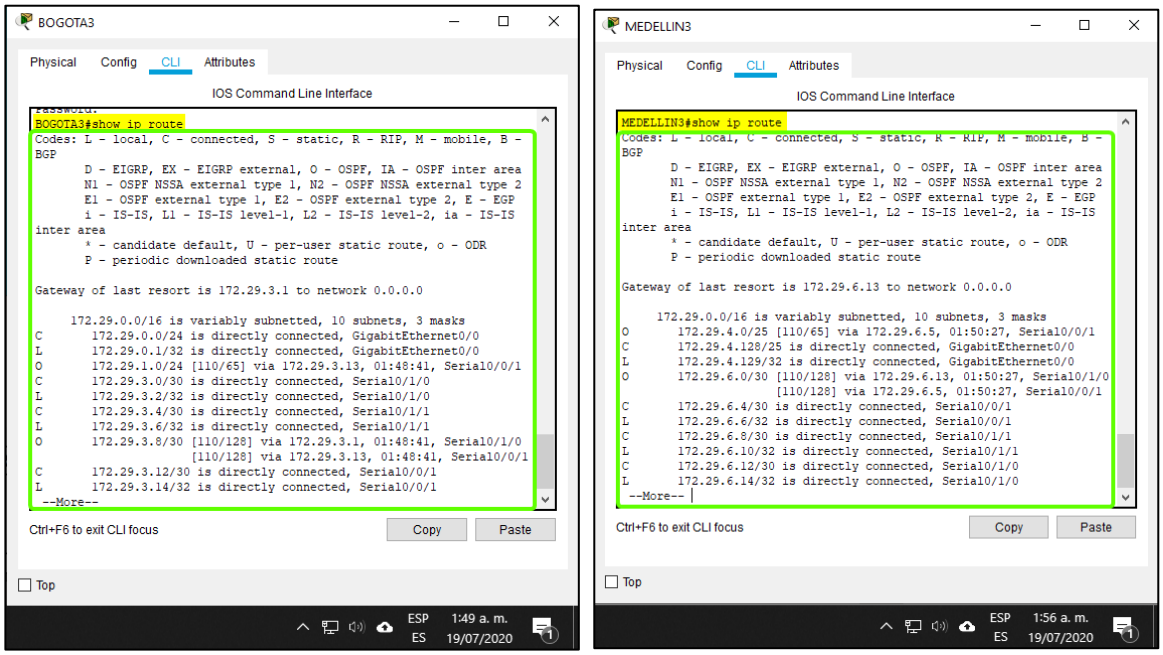


Figura 33. Verificación de enrutamiento Bogota3 y Medellin3.

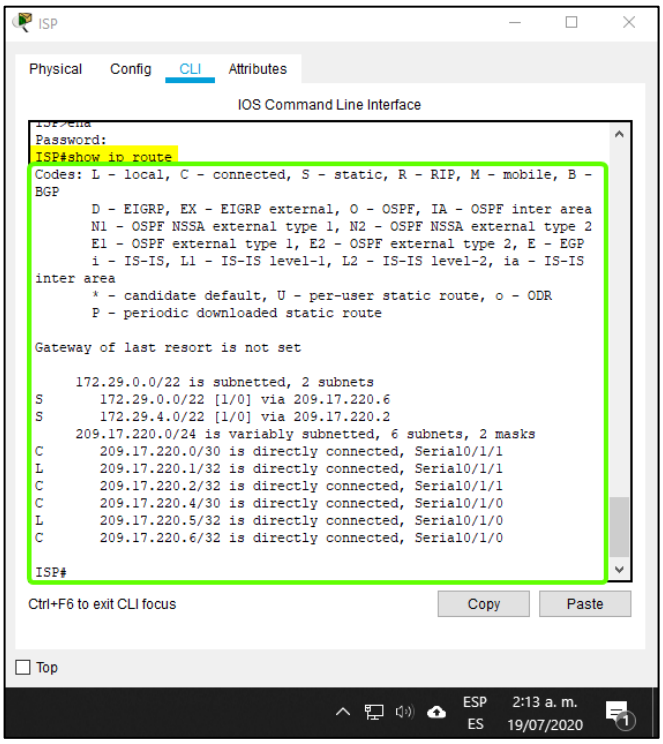


Al comparar los resultados se puede observar que en la Figura 31 existe similitud entre los routers Bogota1 y Medellín1, esto se debe a su ubicación en la red, al estar conectados directamente con el router ISP y a la ruta configurada.

En la Figura 32, comparando Medellin2 y Bogota2, se encuentran redes configuradas por OSPF y se detalla las redundancias de la ruta establecida por defecto.

El router ISP solo debe indicar las rutas estáticas que son adicionales a las directamente conectadas.

Figura 34. Rutas estáticas del router ISP.



2.7 Parte 3: Deshabilitar la propagación del protocolo OSPF.

Para no propagar las publicaciones por interfaces que no lo requieran, se debe deshabilitar el protocolo OSPF, en la Tabla 29 se muestra las interfaces de cada Router que no necesitan desactivación y la Tabla 30 muestra las tareas de configuración para desactivar el protocolo OSPF de las interfaces de router que lo necesite.

Tabla 29. Tabla de Interfaces para desactivar OSPF.

Router	Interfaz
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Tabla 30. Tareas para deshabilitar OSPF de cada Router.

Dispositivo	Tareas para deshabilitar propagación del protocolo OSPF
Bogota2	Bogota2#configure terminal Bogota2(config)#router ospf 1 Bogota2(config-router)#passive-interface g0/0 Bogota2(config-router)#end Bogota2#wr
Bogota3	Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)#passive-interface g0/0 Bogota3(config-router)#end Bogota3#wr
Medellin2	Medellin2#configure terminal Medellin2(config)#router ospf 1 Medellin2(config-router)#passive-interface g0/0 Medellin2(config-router)#end Medellin2#wr
Medellin3	Medellin3#configure terminal Medellin3(config)#router ospf 1 Medellin3(config-router)#passive-interface g0/0 Medellin3(config-router)#end Medellin3#wr

2.8 Parte 4: Verificación del protocolo OSPF

Después de terminada la configuración del protocolo OSPF, se verifican las configuraciones de interfaz pasiva y su respectiva versión. Se utiliza para esta tarea

el comando “show ip protocols”, después se verifica la base de datos de OSPF para ISP, Medellin1, Medellin2, Medellin3, Bogota1, Bogota2 y Bogota3. Se utiliza para esta tarea el comando “show ip route OSPF”, para el router ISP se usa el comando “do show ip route connected ”

Figura 35. Verificación del protocolo OSPF para Medellin1 y Bogota1.

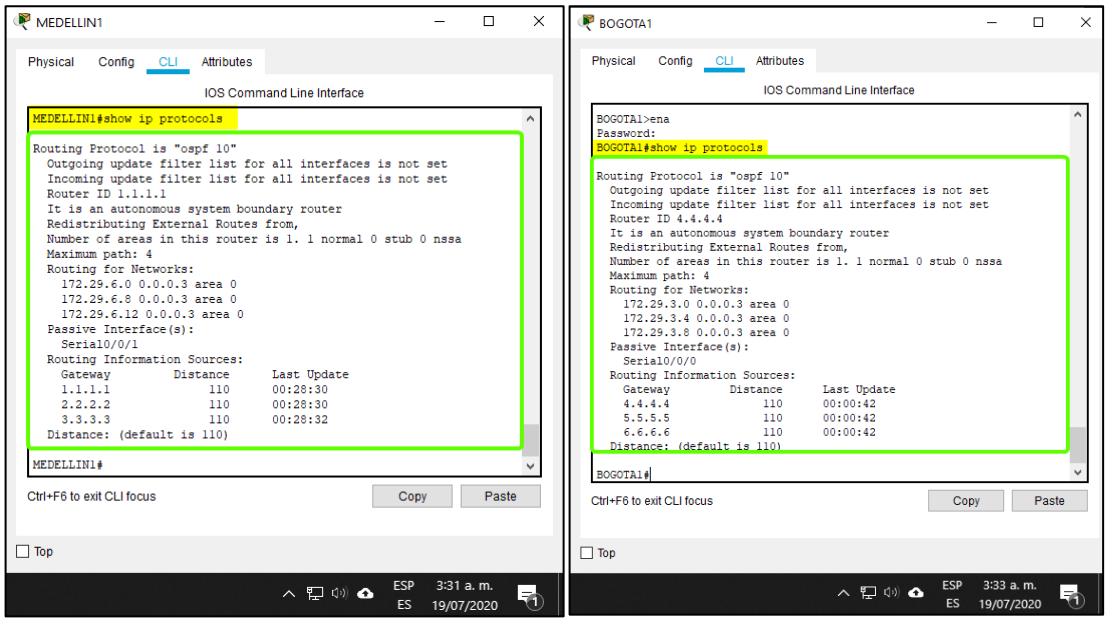


Figura 36. Verificación del protocolo OSPF para Medellin2 y Bogota2.

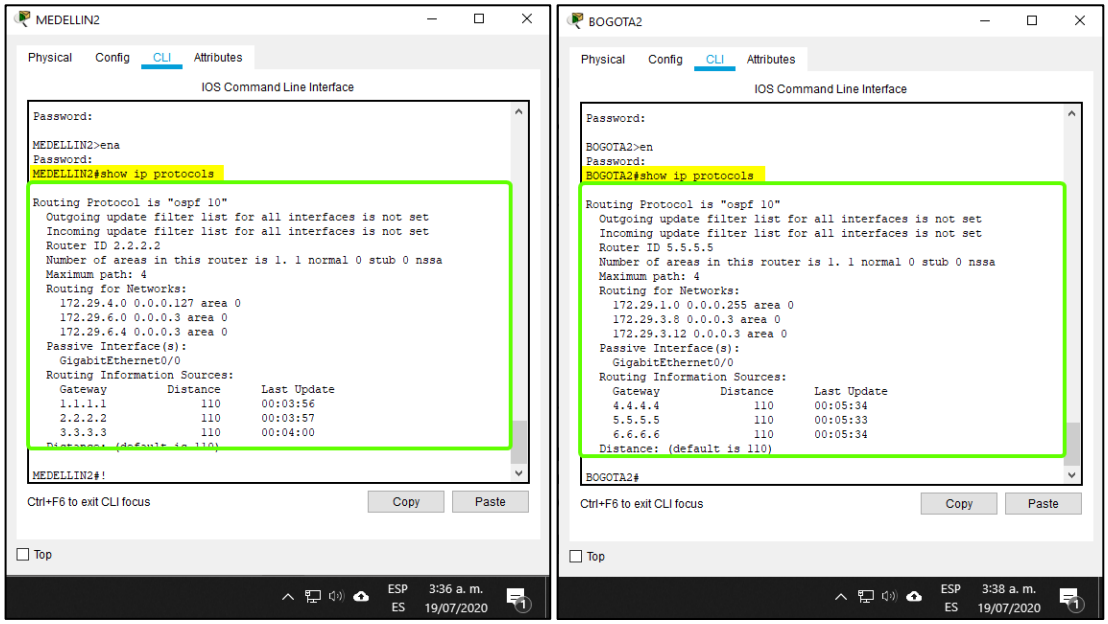


Figura 37. Verificación del protocolo OSPF para Medellin3 y Bogota3.

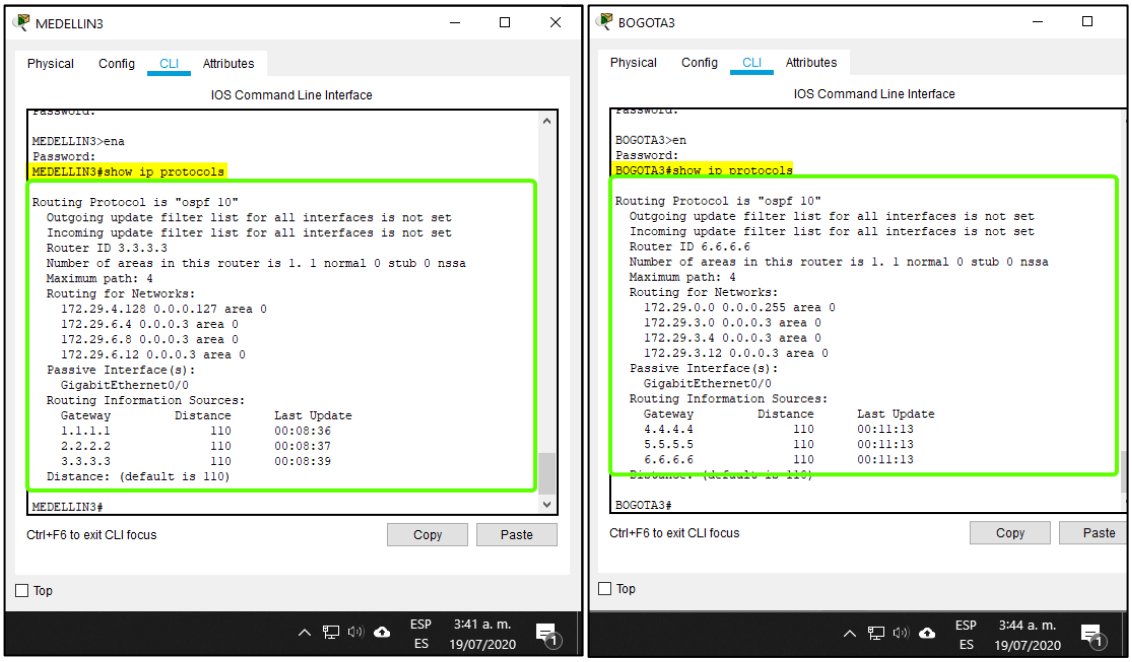


Figura 38. Verificación de la base de datos OSPF para Medellin1 y Bogota1.

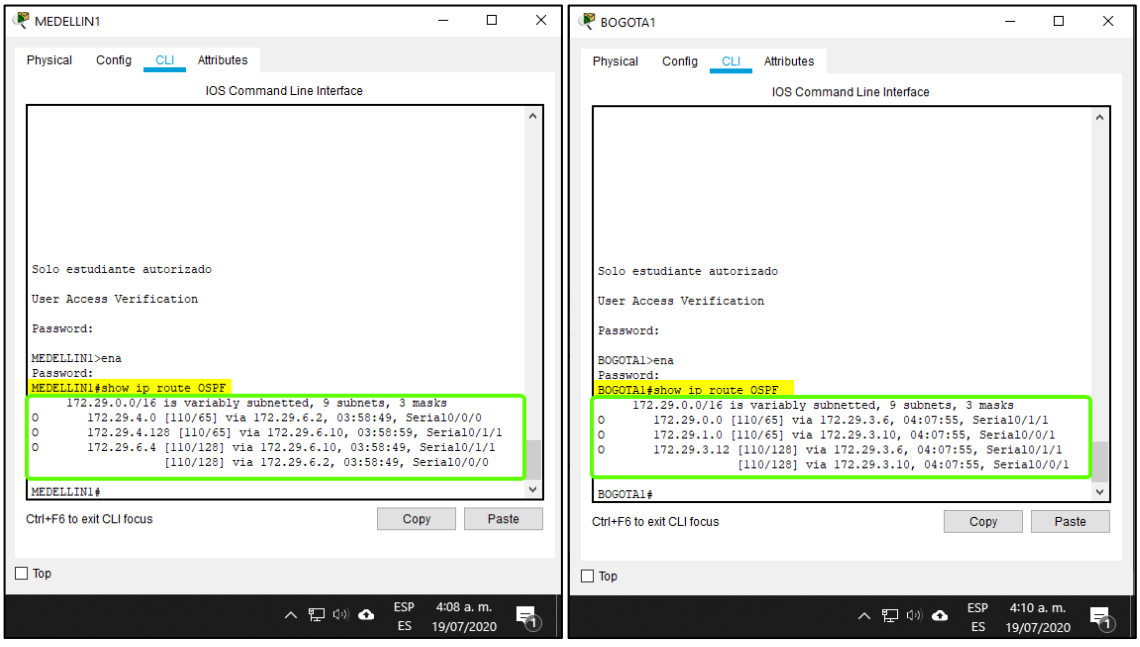


Figura 39. Verificación de la base de datos OSPF para Medellin2 y Bogota2.

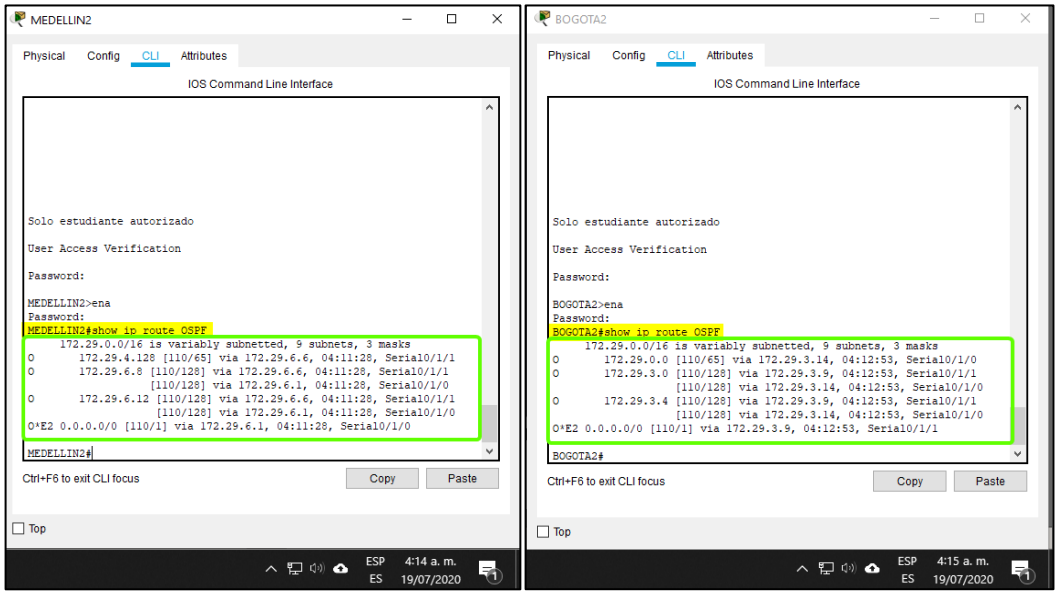


Figura 40. Verificación de la base de datos OSPF para Medellin3 y Bogota3

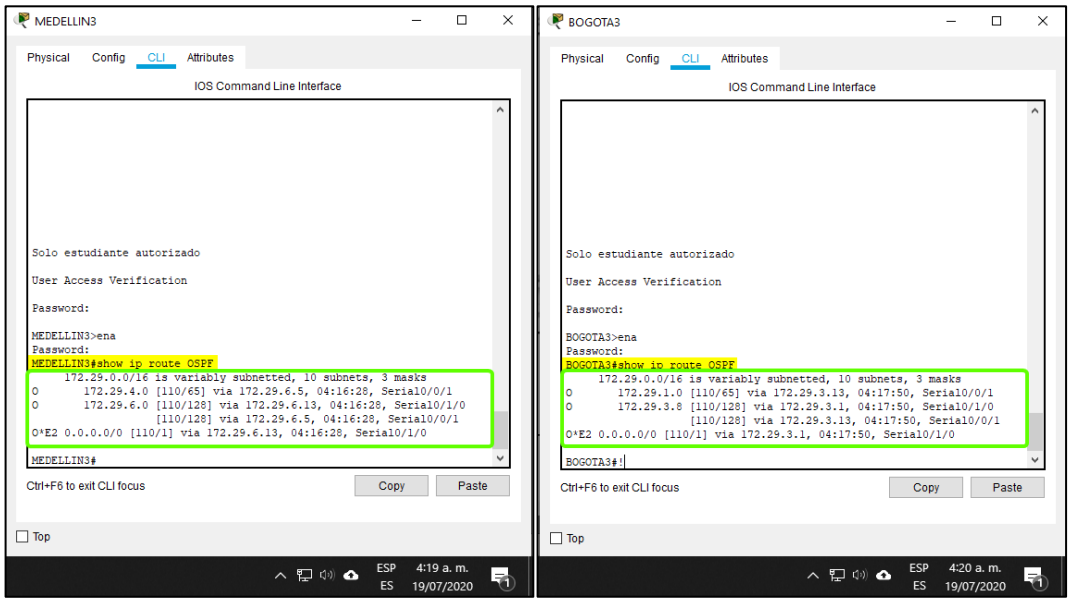
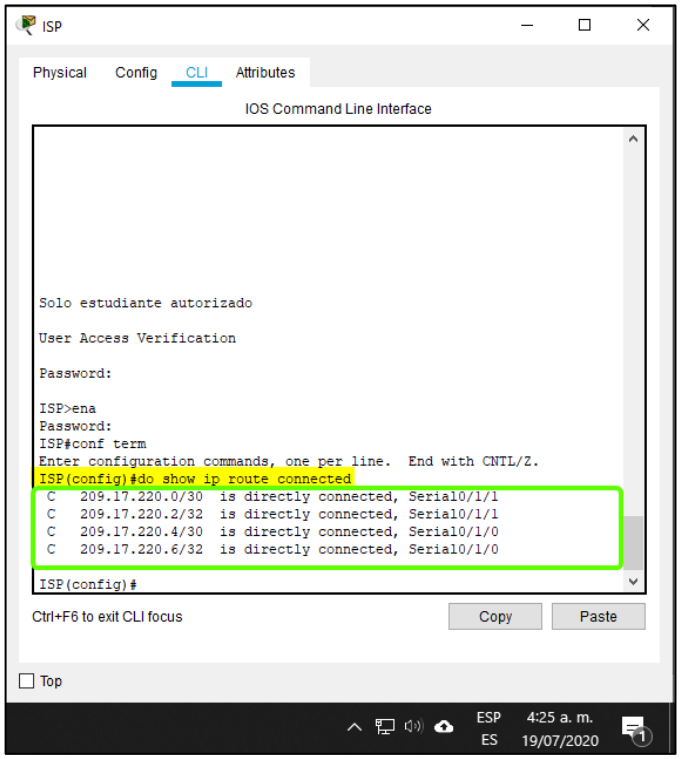


Figura 41. Verificación de la base de datos OSPF para ISP



2.9 Parte 5: Configuración del encapsulamiento y autenticación PPP

Según los requerimientos de la topología de red, se debe configurar el enlace Medellin1 con ISP mediante autenticación PAT y el enlace Bogota1 con ISP se debe configurar con autenticación CHAP.

Tabla 31. Tareas de configuración del encapsulamiento y autenticación PPP.

Dispositivo	Encapsulación y Autenticación PPP
Medellin1	Medellin1#configure terminal Medellin1(config)#username ISP password cisco Medellin1(config)#int s0/0/0 Medellin1(config-if)#encapsulation ppp Medellin1(config-if)#ppp authentication chap Medellin1(config-if)#encapsulation ppp Medellin1(config-if)#ppp authentication pap Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco

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

2.10 Parte 6: Configuración de PAT

Es necesario garantizar la seguridad para cada uno de los dispositivos conectados a la red LAN de Bogotá y Medellín, Por esta razón se activa la NAT (traducción de direcciones de red). en la salida de los router Medellin1 y Bogota1. Después de activar la NAT, sólo habrá comunicación en la WAN, es decir, entre los routers Medellin1, ISP y Bogota1.

Tabla 32. Configuración NAT de Medellin1 y Bogota1.

Router	Configuración
Medellin1	Medellin1#configure terminal Medellin1(config)#ip nat inside source list 1 interface s0/0/0 overload Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255 Medellin1(config)#int s0/1/0 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int s0/0/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int s0/0/1 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int s0/1/1 Medellin1(config-if)#ip nat inside

Router	Configuración
Bogota1	Bogota1#configure terminal Bogota1(config)#ip nat inside source list 1 interface s0/1/1 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 inside 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 outside

2.11 Parte 7: Configuración del servicio DHCP

En este paso se realiza la configuración del servicio DHCP, la Tabla 33 muestra las tareas de configuración. Se configura el router Medellin2 para que sea el servidor de las 2 redes LAN y el router Medellin3 para que permita el paso de los mensajes de broadcast hacia la IP del servidor, el router Bogota1 se configura para que permita el paso de los mensajes broadcast hacia el servidor y se configuran los routers Bogota2 y Bogota3 para que tengan como servidor el router Medellin2.

Tabla 33. Tareas para la configuración DHCP según requerimientos.

Dispositivo	Configuración DHCP
Medellin2	Medellin2#configure terminal Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.3.133 Medellin2(config)#ip dhcp pool Medellin2 Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.1 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit Medellin2(config)#ip dhcp pool Medellin3 Medellin2(dhcp-config)#network 172.29.4.1 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.129 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit172.29.6.2
Medellin3	Medellin3#configure terminal Medellin3(config)#int g0/0 Medellin3(config-if)#ip helper-address 172.29.6.2

Bogota2	Bogota2#configure terminal Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 Bogota2(config)#ip dhcp pool Bogota2 Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.1.1 Bogota2(dhcp-config)#dns-server 8.8.8.8 Bogota2(dhcp-config)#ip dhcp pool Bogota3 Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.0.1 Bogota2(dhcp-config)#dns-server 8.8.8.8
	Bogota2#configure terminal Bogota2(config)#int g0/0 Bogota2(config-if)#ip helper-address 172.29.3.13

Se realiza la verificación del correcto funcionamiento del servicio de DCHP en la red.

Figura 42. Servicio de DHCP en el PCB2 y PCB3

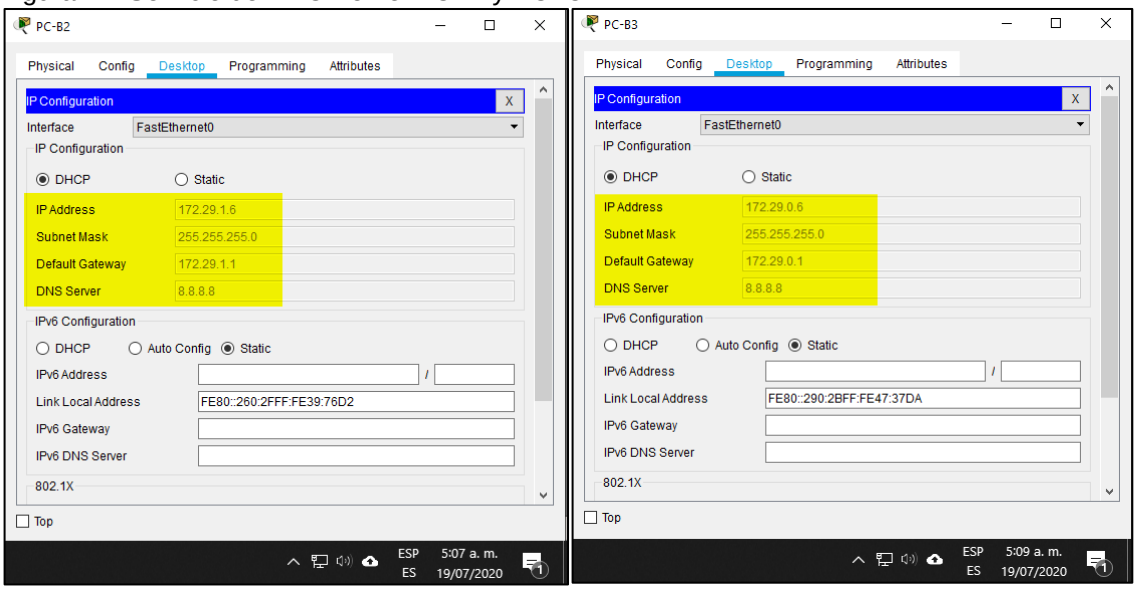
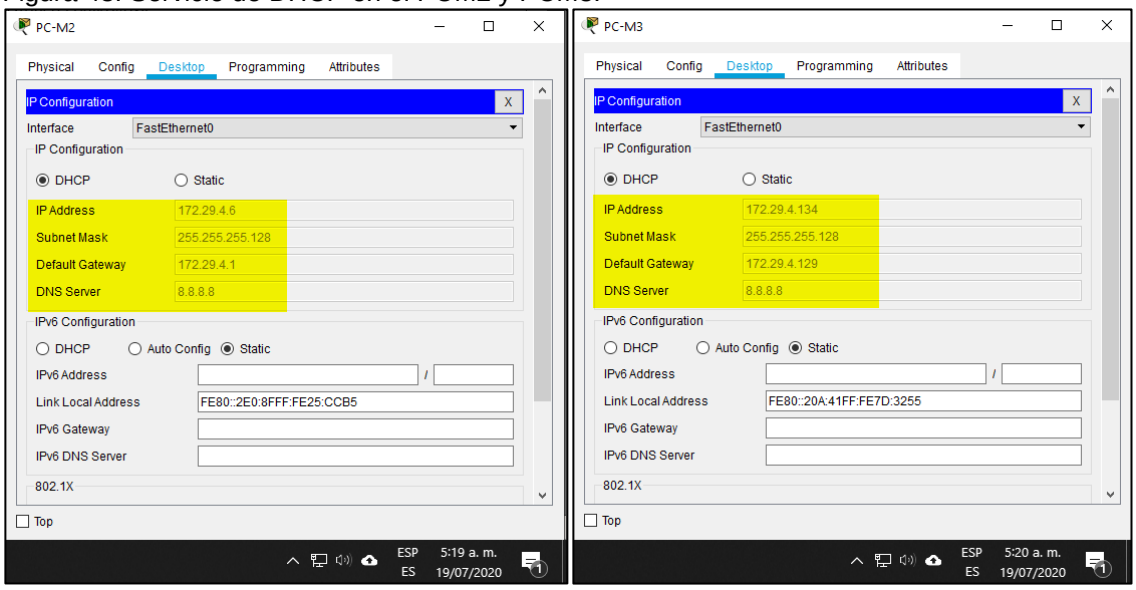


Figura 43. Servicio de DHCP en el PCM2 y PCM3.



Se, realiza la verificación de conectividad de todos los dispositivos de la red.

Figura 44. Ping de ISP a Medellin1 y Bogota1.

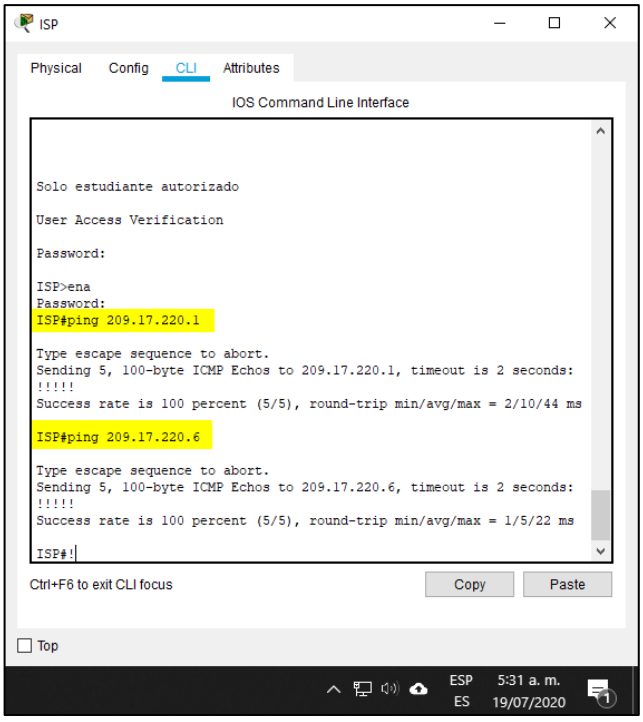


Figura 45. Ping PCB2 y PCB3 a Medellin1 IP pública.

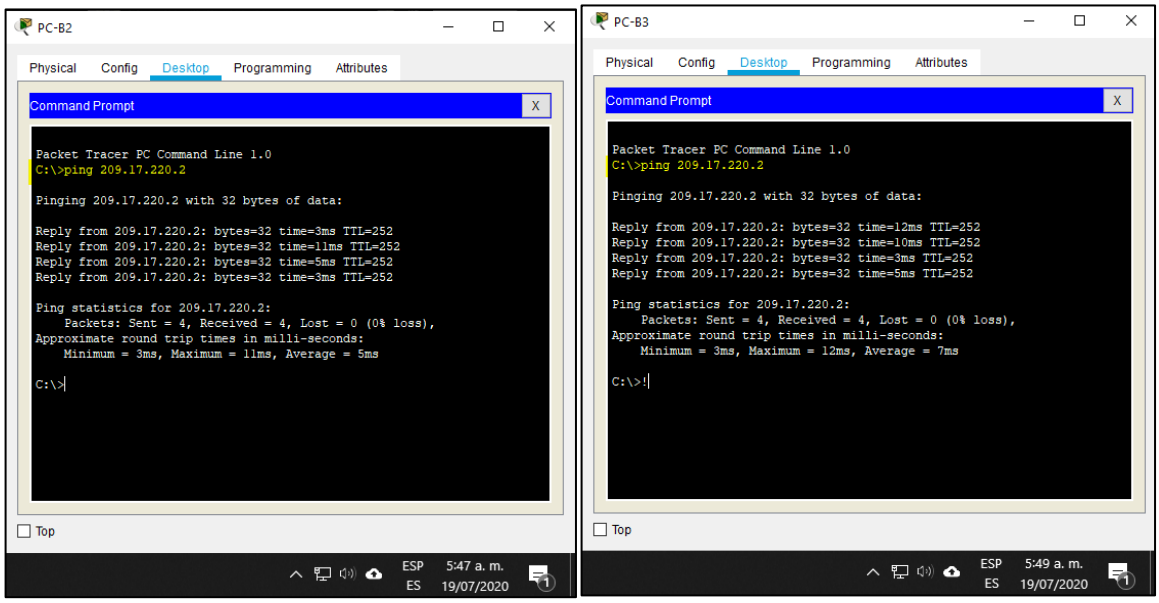
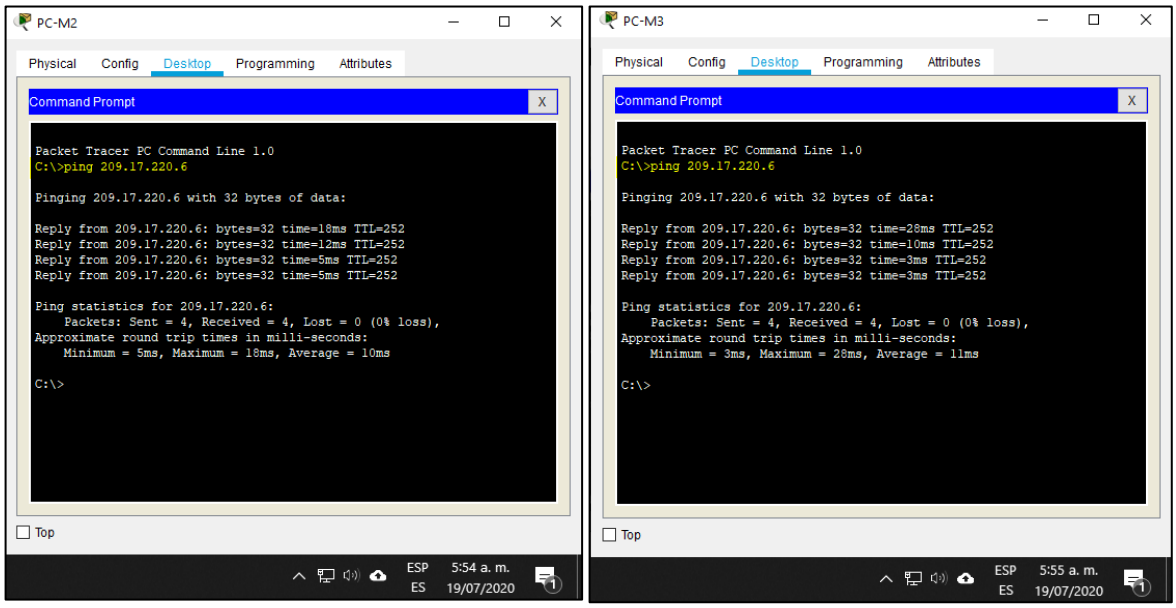


Figura 46. Ping PCM2 y PCM3 a Bogota1 IP pública



3 CONCLUSIONES

Con el desarrollo de esta prueba de habilidades se puso en práctica los conceptos vistos en el curso del diplomado de profundización cisco, estos valiosos conocimientos ayudaron a desenvolvernos y poder dar solución a los dos escenarios propuestos que, lo más probable, encontremos en la vida cotidiana o laboral.

En el primer escenario se pudo configurar una red pequeña que permitiera la conectividad IPv4 e IPv6, añadiendo 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.

Para el segundo escenario, se logró implementar el uso de OSPF como protocolo de enrutamiento, se pudo configurar las rutas por defecto redistribuidas, se habilitó el encapsulamiento PPP y su autenticación, se verificó que los routers Bogota2 y medellin2 proporcionen el servicio DHCP a su propia red LAN y a los tres routers de cada ciudad, por otra parte se logró configurar y verificar la configuración PPP en los enlaces hacia el ISP con autenticación, y finalmente, se deshabilitó el NAT de sobrecarga en los routers Bogota1 y medellin1.

Estos laboratorios de redes en los cuales se configura, se realizan pruebas, se hace seguimiento y asignación de protocolos, se lograron sacar adelante, gracias al aprendizaje adquirido en el transcurso del Diplomado de Profundización Cisco y nos servirá como punto de partida como un manual de vida informático para el crecimiento y mejoramiento como profesionales en sistemas.

BIBLIOGRAFÍA

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

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#2

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

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

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

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). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

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

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

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). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

ANEXO - ENLACES A LOS ESCENARIOS EN DRIVE

Enlace al archivo de Packet Tracer Escenario 1 – Alexander Chinchilla

Enlace al archivo de Packet Tracer Escenario 2 – Alexander Chinchilla